



Access Manager Module Settings and Operation Guide

1. Access Manager Module Settings and Operation Guide	4
1.1 List of terms used in the Access Manager Module Settings and Operation Guide	4
1.2 Access Manager Module Settings and Operation Guide. Introduction	4
1.3 Configuration of the Access Manager module	4
1.3.1 Procedure of configuring the Access Manager module	4
1.3.2 Configuring the position of the Access manager window on the screen	5
1.3.3 Rights for configuring objects in the Access Manager	6
1.3.3.1 General information about rights for objects configuring in the Access Manager	6
1.3.3.2 Specify correspondence of operator rights in the Access Manager and in the Intellect software package	7
1.3.3.3 Rights for configuring access levels in the Access manager	8
1.3.3.4 Rights for users configuring in the Access Manager	8
1.3.3.5 Rights for configuring and viewing departments in the Access Manager	8
1.3.4 Configuring readers in the Access Manager	9
1.3.4.1 Selecting control readers in the Access Manager	9
1.3.4.2 Configuring confirmation of access cards input in the Access Manager	10
1.3.5 Selecting available cameras in the Access Manager	11
1.3.6 Configuring parameters of users creation in the Access Manager	12
1.3.7 Configuring fields displaying in user accounts	12
1.3.7.1 Configuring a type of department in the Access Manager	12
1.3.7.2 Configuring availability of fields depending on operator rights in the Access Manager	14
1.4 Access Manager module interface	15
1.4.1 Departments tab	15
1.4.2 Time zones tab	16
1.4.3 Access levels tab	17
1.4.4 Regions and areas tab	18
1.5 Working with the Access Manager software module	19
1.5.1 Starting and stopping the Access Manager module	19
1.5.2 General operations with the Access Manager interface elements	20
1.5.2.1 Selecting a view of displaying objects list in the Access Manager	20
1.5.2.2 Selecting a way of sorting objects in the list	21
1.5.2.3 Change elements sizes of the Access Manager window interface	21
1.5.2.4 Key combinations for working with objects lists	22
1.5.3 Working with time zones in the Access Manager software module	22
1.5.3.1 General information about time zones in the Access Manager software module	22
1.5.3.2 Creation of a time zone in the Access Manager software module	23
1.5.3.3 Editing a time zone in the Access Manager software module	27
1.5.3.4 Search for time zone	28
1.5.3.4.1 Going to search for time zone	28
1.5.3.4.2 Working with the Search for time zone window	29
1.5.3.5 Editing holidays	30
1.5.4 Working with access levels in the Access Manager software module	32
1.5.4.1 General information about working with access levels in the Access Manager software module	32
1.5.4.2 Creation of an access level in the Access Manager software module	33
1.5.4.3 Editing an access level in the Access Manager software module	38
1.5.4.4 Going to the time zone	39
1.5.4.5 Search for access level	39
1.5.4.5.1 Going to search for access level	39
1.5.4.5.2 Working with the Search access level window	40
1.5.4.6 Managing the list of access levels	41
1.5.5 Working with departments in the Access Manager software module	44
1.5.5.1 General information about working with departments	44

1.5.5.2 Adding a department	45
1.5.5.3 Editing a department	47
1.5.5.4 Department search in the Access Manager software module	48
1.5.5.4.1 Going to department search	48
1.5.5.4.2 Working with Search for department window	49
1.5.5.5 Creating departments hierarchy	50
1.5.6 Working with users in the Access Manager software module	51
1.5.6.1 Viewing a list of users	51
1.5.6.2 Creating users in the Access Manager	51
1.5.6.3 Editing a user	53
1.5.6.3.1 Going to user editing	53
1.5.6.3.2 Setting user parameters	53
1.5.6.3.3 Assigning an access card to a user	56
1.5.6.3.4 Assigning access levels to a user	59
1.5.6.3.5 Assigning a photograph to a user in the Access Manager software module	62
1.5.6.3.6 Adding biometric parameters	66
1.5.6.3.7 Transferring a user to a different department in the Access Manager software module	67
1.5.6.4 User search in the Access Manager software module	67
1.5.6.4.1 General information about user search	67
1.5.6.4.2 Going to user search	67
1.5.6.4.3 Adding a search rule	68
1.5.6.4.4 Start of user search	71
1.5.6.5 Deleting a user in the Access Manager software module	72
1.5.6.6 Printing a user access card in the Access Manager software module	73
1.5.7 Performing Emergency Monitoring	74
1.5.7.1 General information about Emergency Monitoring	74
1.5.7.2 Card number displaying in the Event viewer window for access events	75
1.5.7.3 Viewing user profile by an access event in the Event viewer	76
1.5.7.4 Finding out the region where the user currently is	77
1.5.7.5 Viewing the list of users in the region	78
1.5.7.6 Viewing region on the Map	80
1.5.7.7 Creating, editing and deleting Area and Region objects	81
1.5.7.7.1 Creating areas	81
1.5.7.7.2 Creating regions	81
1.5.7.7.3 Editing areas and regions	82
1.5.7.7.4 Deleting areas and regions	82
1.6 Appendix 1. Description of the Access Manager interfaces	83
1.6.1 The Access Manager object settings panel	83
1.6.2 The User rights in Access Manager object settings panel	87
1.6.3 The Type of department object settings panel	90
1.7 Appendix 2. Configuring a visitor management system without the Access Manager interface window	92
1.7.1 General information on ACFA Intellect objects related to the visitor management system	92
1.7.2 Settings panel of the Department object	92
1.7.3 Settings panel of the User object	93
1.7.4 Settings panel of the Access level object	95
1.8 Appendix 3. Settings for proper operation of the Access Manager module in a distributed architecture	97

Access Manager Module Settings and Operation Guide

List of terms used in the Access Manager Module Settings and Operation Guide

User – a person whose data are processing by the Access Manager module. The Access Manager module allows processing data of visitors, vehicles and other types of users. Configuring and working of the module with different types of users are the same. In case of configuring and working with specific functions it will be additionally specified.

Operator – a person who configures and operates with the *Access Manager* module.

APB (*Antipassback*) – a control over access order. Function allows protecting from repeated use of identifier to pass in one direction.

Holiday – a non-working day. Specifying of holydays list in the system allows eliminating of defined days from time zones.

Access point – a point where access control is performed. An access point may be a door, a turnstile, a gate, or a boom barrier equipped with a reader, an electromechanical lock, or other access control devices.

Access level – right of user to access through the access point (points) depending on the time schedule. Also defines rule of arming and disarming access point. Access level can be general for all users from department and separate for one, several or all users.

Control reader – a reader which is used for card input to system.

Access Manager Module Settings and Operation Guide. Introduction

On the page:

- [Purpose of the document](#)
- [General information about the Access Manager module](#)

Purpose of the document

The *Access Manager Module Settings and Operation Guide* is a reference manual designed for *Access Manager* module configuration technicians and operators. This module is part of the *ACFA Intellect* software system.

This Guide presents the following materials:

1. general information about the *Access Manager* module;
2. *Access Manager* module settings;
3. working with the *Access Manager* module.

General information about the Access Manager module

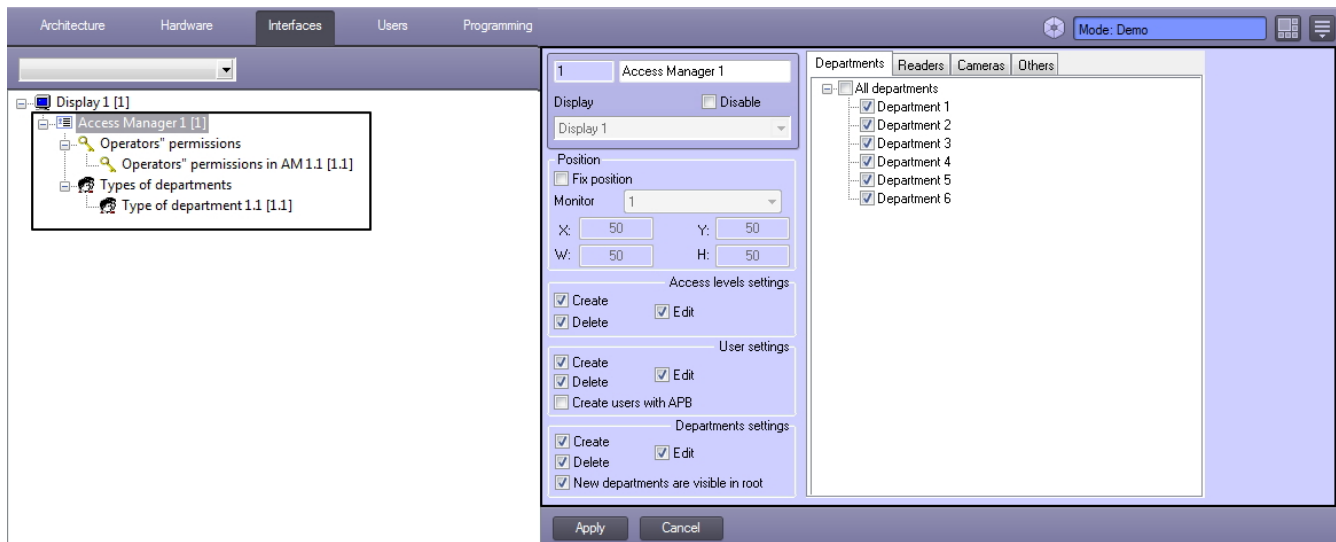
The *Access Manager* software module is a component of the *ACFA Intellect* software package and supports the following actions:

1. configure access mode of users and visitors to object with automated access control systems;
2. configure movement rules of users and visitors within object according to access levels;
3. configure operator rights to create, edit, delete and view departments;
4. configure operator rights to create, edit and delete access levels and users;
5. create and configure access levels as for each user and for all department;
6. create, configure and delete accounts of users and departments;
7. create, configure and delete time schedules and access levels;
8. print security passes for users.

Configuration of the Access Manager module

Procedure of configuring the Access Manager module

The *Access manager* module is configured on the settings panel of the **Access manager** object and on settings panels of the **User rights in Access Manager** and **Type of department** sub-objects. The **Access manager** object is created on basis of the **Display** object on the **Interfaces** tab of the **System settings** dialog window.



The *Access Manager* module is configured as follows:

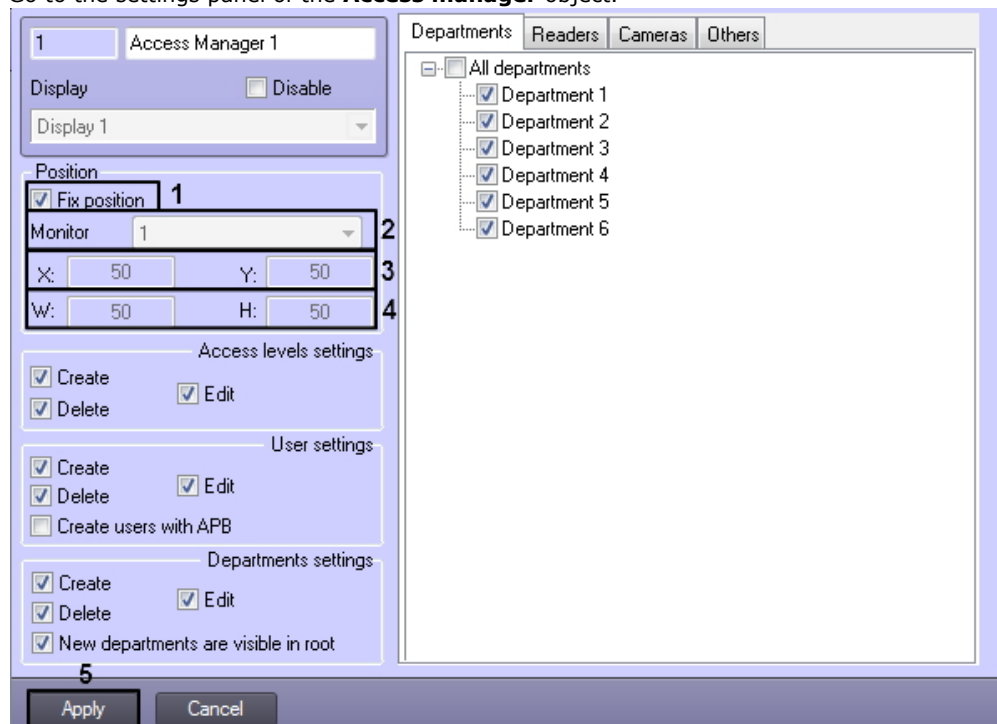
1. Configuring of location the **Access manager** window on the screen.
2. Specifying rights to configure objects in the **Access manager** window: visibility of departments, access rights for configuring access levels, users and departments.
3. Configuring of using control readers.
4. Select available cameras for input of user photos.
5. Configuring parameters of user creation.
6. Configuring of fields displaying.

Configuring the position of the Access manager window on the screen

Position of the **Access manager** window is not fixed on the screen on default and it can be changed. If it's required to specify position of the **Access manager** window on the screen eliminating possibility to change its position, do the following:

Note. When specify the fix position of the **Access manager** window on the screen, the caption bar won't display which increase the displaying area of the **Access manager** window content.

1. Go to the settings panel of the **Access manager** object.



2. Set the **Fix position** checkbox (1).
3. From the **Monitor** drop-down list select a system monitor on which the **Access Manager** window is to be displayed (2).
4. Set coordinates of the **Access Manager** window's upper left corner in the **X:** and **Y:** fields as percentage of width and height of the screen correspondingly (3).
5. Set width and height of the **Access Manager** window in the **W:** and **H:** fields as percentage of width and height of

- the screen correspondingly (4).
6. Click the **Apply** button (5).

Specifying fix position of the **Access Manager** window on the screen is completed.

Rights for configuring objects in the Access Manager

General information about rights for objects configuring in the Access Manager

Specifying rights for objects configuring allows to restrict actions available for operator of the *Access Manager* module while departments configuring, users and their access levels. Rights for objects configuring definitely correspond to user rights in the *ACFA Intellect* software package.

Rights for objects configuring in the *Access Manager* include permission or forbidding to perform the following operations with access levels, users and departments from the **Access Manager** window:

1. Create.
2. Edit.
3. Delete.



Note

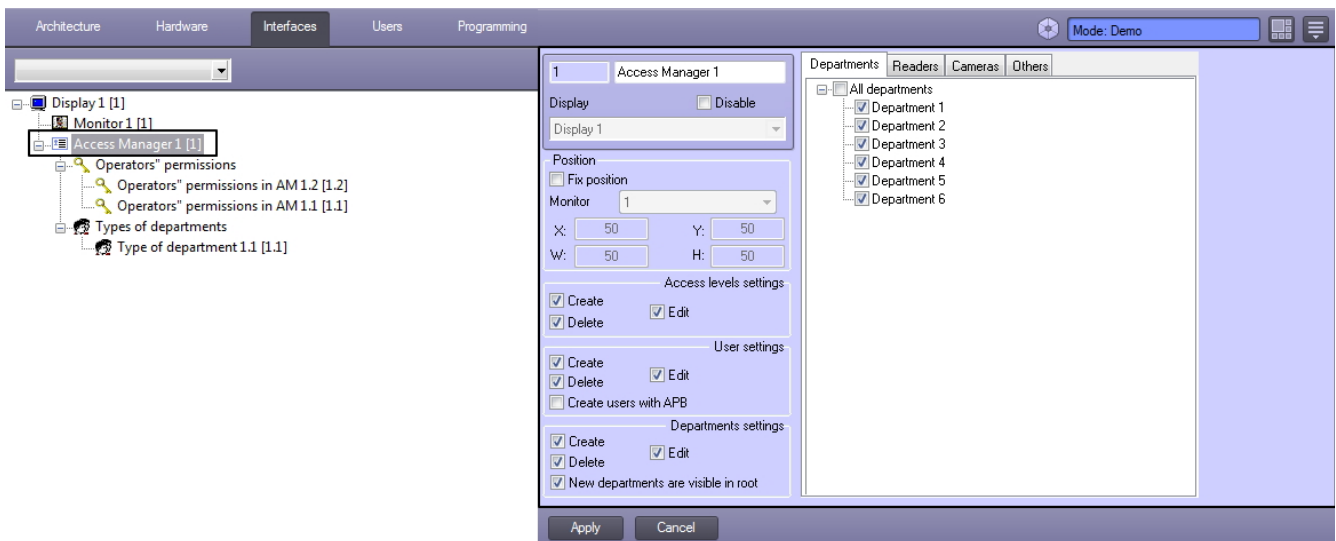
Visibility for departments is also configured in the *Access Manager* module.

All operations mentioned above are allowable for operator.

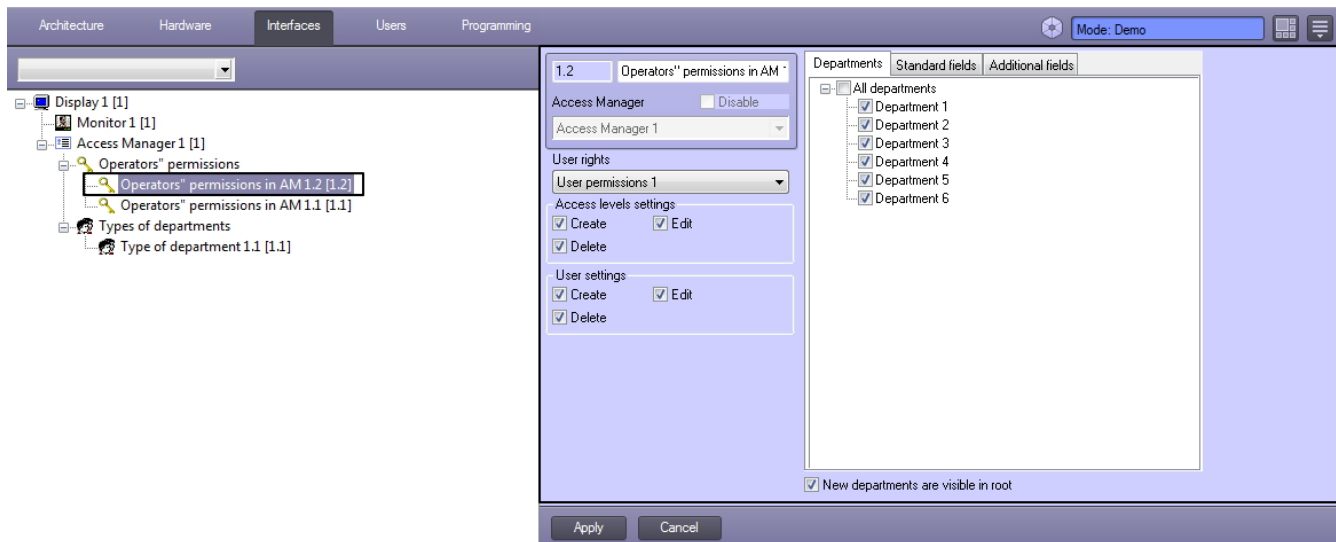
The *Access manager* software module allows specifying of common and individual rights for objects configuring.

Common rights for objects configuring have priority over individual rights. So if performing of some operation is forbidden by common rights for objects configuring, than it will be forbidden for all operators, even if it will be permitted by some individual rights.

Common rights for objects configuring are specified on the settings panel of the **Access Manager** object.



Individual rights for objects configuring are specified on the settings panel of the **User rights in Access Manager** object, which is created on the basis of the **Access Manager** object on the **Interfaces** tab of the **System settings** dialog window.



Specify correspondence of operator rights in the Access Manager and in the Intellect software package

Individual rights for objects configuring in the *Access Manager* definitely correspond to user rights in the *ACFA Intellect* software package. So only one **User rights in Access Manager** object can correspond to one **User permissions** object and vice versa.

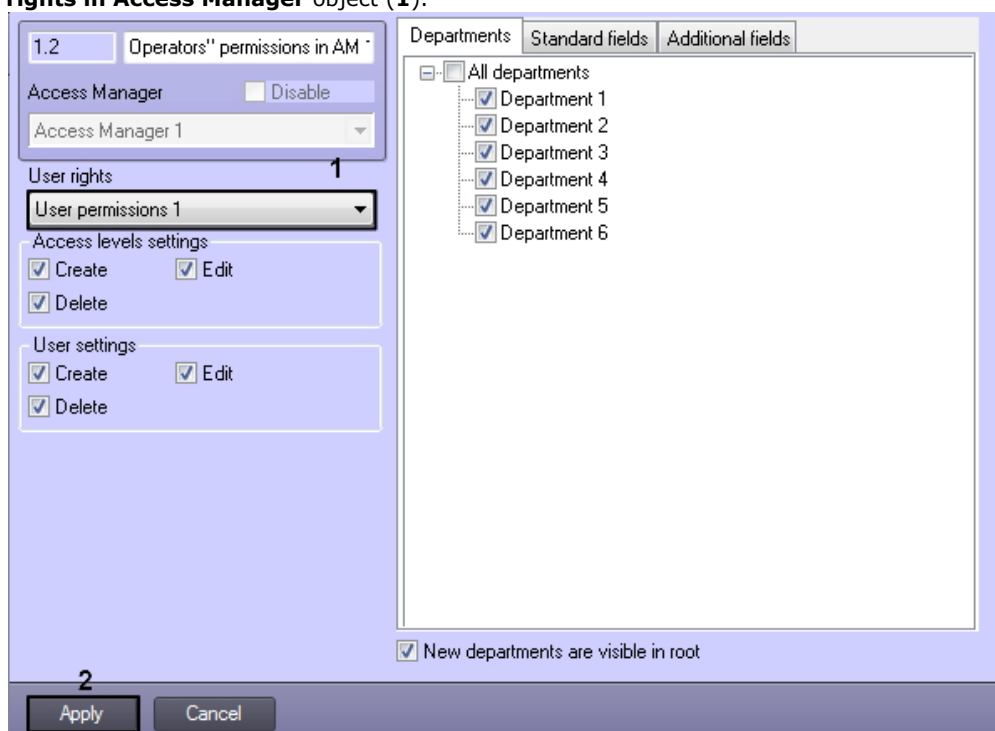


Note

If similar operator rights in the *Access Manager* should correspond to user rights in the *ACFA Intellect* software package, use the **Save** function from context menu of interface object, see [The Save function](#) section of the Intellect software package. Administrator's Guide.

To specify correspondence of operator rights in the *Access Manager* and in the *ACFA Intellect* software package, do the following:

1. Go to the settings panel of the **User rights in Access Manager** object.
2. From the **User rights** drop-down list select the **User permissions** object which is required to match to the **User rights in Access Manager** object (1).



Note

User permissions objects are created on the **Programming** tab of the **System settings** dialog window. Creating and configuring of these objects is described in the [Rights administration](#) section of the Intellect software package. Administrator's Guide. The current version of this document is available in the documentation repository

3. Click the **Apply** button (2).

Specifying correspondence of operator rights in the *Access manager* and in the *ACFA Intellect* software package is completed.

Rights for configuring access levels in the Access manager

To specify common and individual rights for configuring access levels, do the following:

1. Go to the settings panel of the **Access Manager** or **User rights in Access Manager** object.



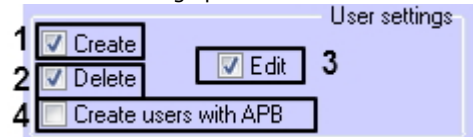
2. If it's required to forbid operators to create access levels, remove the **Create** checkbox in the **Access levels settings** group (1).
3. If it's required to forbid operators to delete access levels, remove the **Delete** checkbox in the **Access levels settings** group (2).
4. If it's required to forbid operators to edit access levels, remove the **Edit** checkbox in the **Access levels settings** group (3).

Specifying of common and individual rights for configuring access levels is completed.

Rights for users configuring in the Access Manager

To specify common or individual rights for users configuring, do the following:

1. Go to the settings panel of the **Access manager** or **User rights in Access Manager** object.



2. If it's required to forbid operators to create users, remove the **Create** checkbox in the **User settings** group (1).
3. If it's required to forbid operators to edit users, remove the **Edit** checkbox in the **User settings** group (2).
4. If it's required to forbid operators to delete users, remove the **Delete** checkbox in the **User settings** group (3).
5. If it's required to allow operators to create users with antipassback enabled, set the **Create users with APB** checkbox in the **User settings** group (4).



Note

Create users with APB checkbox is available only on the **Access manager** settings panel.

Specifying of common and individual rights for users configuring is completed.

Rights for configuring and viewing departments in the Access Manager

To specify common or individual rights for configuring and viewing departments, do the following:

1. Go to the settings panel of the **Access manager** or **User rights in Access Manager** object and open the **Departments** tab (1).

The top screenshot shows the 'Departments' tab in the Access Manager interface. On the left, there are settings for 'Access Manager 1', 'Display', 'Position', 'Monitor', 'Access levels settings', 'User settings', and 'Departments settings'. On the right, there is a tree view of departments with checkboxes for 'All departments' and 'Department 1' through 'Department 6'. The bottom screenshot shows the 'Standard fields' tab with similar settings on the left and a tree view on the right. Numbered callouts 1 through 6 highlight specific UI elements: 1. Access Manager 1 dropdown, 2. Department checkboxes, 3. Create checkbox, 4. Edit checkbox, 5. Delete checkbox, 6. New departments are visible in root checkbox.

2. Set checkboxes close to departments which should be available in the *Access Manager* interface module (2).
3. If it's required to forbid operators to create new departments, remove the **Create** checkbox (3).
4. If it's required to forbid operators to edit departments, remove the **Edit** checkbox (4).
5. If it's required to forbid operators to delete departments, remove the **Delete** checkbox (5).
6. New departments located in the root of departments hierarchy and departments replacing to the hierarchy root. On default new departments locating in the root of departments hierarchy and departments transferred to the root of hierarchy regardless of their visibility before transferring are available in the *Access Manager* interface window - the **New departments are visible in root** checkbox is set (6). If new departments and departments transferred to the root of hierarchy should be invisible in the *Access Manager* window, deselect the checkbox.



Attention!

If the **New departments are visible in root** checkbox is deselected, creation of new departments in the root of departments hierarchy will be forbidden even if the **Create** checkbox is set (3).



Note

New departments created via the *Access Manager* module on the basis of visible departments will be visible on default.

Specifying of common and individual rights for configuring and viewing departments is completed.

Configuring readers in the Access Manager

Selecting control readers in the Access Manager

It is possible to specify the list of control readers used for assigning access cards to users in the **Access Manager** interface window while configuring the *Access Manager* program module.

To select control readers, do the following:

1. Go to the settings panel of the **Access Manager** object.
2. Go to the **Readers** tab (1).

The screenshot shows the 'Access Manager 1' configuration window. The 'Readers' tab is selected, indicated by a '1' and a box. The window is divided into two main sections. The left section contains various settings: 'Display' (Disable checkbox, Display 1 dropdown), 'Position' (Fix position checkbox, Monitor 1 dropdown, X: 50, Y: 50, W: 50, H: 50), 'Access levels settings' (Create, Delete, Edit checkboxes), 'User settings' (Create, Delete, Edit checkboxes, Create users with APB checkbox), and 'Departments settings' (Create, Delete, Edit checkboxes, New departments are visible in root checkbox). The right section is a table of readers, with a '2' indicating the table area. The table has a checkbox column. The readers listed are: 'FS80 control reader 1' (checkbox unchecked), 'Gate Parking access point 1' (checkbox checked), 'Gate Parking access point 2' (checkbox checked), and 'Suprema BioMini 1' (checkbox checked). At the bottom, there are 'Apply' and 'Cancel' buttons, with a '3' indicating the 'Apply' button.

Confirm card entered by operator	
FS80 control reader 1	☐
Gate Parking access point 1	☒
Gate Parking access point 2	☒
Suprema BioMini 1	☒

3. Set checkboxes close to those readers which should be available in the **Access Manager** window while access cards input (2).

Note
Objects corresponding to control readers are created and configured on the **Hardware** tab of the **System settings** dialog window (see [Control Readers Settings Guide](#))

4. To save changes click the **Apply** button (3).

Selecting of readers is completed.

Configuring confirmation of access cards input in the Access Manager

If it's required that operator confirms assigning of access cards to user, do the following:

1. Go to the settings panel of the **Access Manager** object.

1 Access Manager 1

Display ☐ Disable
Display 1

Position
☐ Fix position
Monitor 1
X: 50 Y: 50
W: 50 H: 50

Access levels settings
☒ Create ☒ Edit
☒ Delete

User settings
☒ Create ☒ Edit
☒ Delete ☐ Create users with APB

Departments settings
☒ Create ☒ Edit
☒ New departments are visible in root

Departments 1 Readers Cameras Others

☒ Confirm card entered by operator 2

FS80 control reader 1	☐
Gate Parking access point 1	☒
Gate Parking access point 2	☒
Suprema BioMini 1	☒

3

Apply Cancel

2. Go to the **Readers** tab (1).
3. Set the **Confirm card entered by operator** checkbox (2).
4. To save changes click the **Apply** button (3).

Configuring of confirmation access cards input is completed.

Selecting available cameras in the Access Manager

The *Access Manager* program module allows specifying cameras which will be available in the **Access Manager** window for setting photos to users.

To select available cameras, do the following:

1. Go to the settings panel of the **Access Manager** object.

1 Access Manager 1

Display ☐ Disable
Display 1

Position
☐ Fix position
Monitor 1
X: 50 Y: 50
W: 50 H: 50

Access levels settings
☒ Create ☒ Edit
☒ Delete

User settings
☒ Create ☒ Edit
☒ Delete ☐ Create users with APB

Departments settings
☒ Create ☒ Edit
☒ New departments are visible in root

Departments Readers Cameras Others

Cameras	Use	Gateway
Camera 1	☒	Videogate 1
Camera 2	☒	
Camera 3	☐	

2 3

4

Apply Cancel

2. Go to the **Cameras** tab (1).
3. In the **Use** column set checkboxes close to cameras which are to be used for setting photos to users (2).



Note

Camera objects are created on the **Hardware** tab of the **System settings** dialog window. Creating and configuring **Camera** is described in the *Intellect software package. Installing and Configuring Security System Components Guide* document. Current version of this document is available in the [documentation repository](#).

- If video from camera is to be received using videogate, select the required **Videogate** object from the drop-down list in the **Gateway** column (3).



Note

The corresponding **Videogate** object should be configured for data transferring with this camera. Configuring the **Videogate** object is described in the *Intellect software package. Administrator's guide* document. Current version of this document is available in the [documentation repository](#).

- To save changes click the **Apply** button (4).

Selecting of available cameras is completed.

Configuring parameters of users creation in the Access Manager

To configure parameters of users creation, do the following:

- Go to the settings panel of the **Access Manager** object and switch to the **Others** tab (1).

- From the **Full Name** drop-down list select the way of definition duplicate user records (2):
 - Not used** – it's accepted to add users with equal full name.
 - Surname, name** – it's forbidden to add users with equal name and surname even if patronymic is differed.
 - Surname, name, patronymic** – it's forbidden to create users with equal full name.
- Set the **External ID** checkbox if you want to forbid creating users with the same external identifiers (3).
- Set the **Vehicle license plate** checkbox if you want to forbid creating users with the same vehicle plate numbers (4).
- To save changes click the **Apply** button (5).

Configuring parameters of users creation is completed.

Configuring fields displaying in user accounts

Configuring a type of department in the Access Manager

Type of department defines fields of users available to view and edit in the **Access Manager** interface window.

Default department type (**Main**), in which all main fields are available for editing and additional fields are hidden, will be available in the **Access Manager** window if department types are not created.

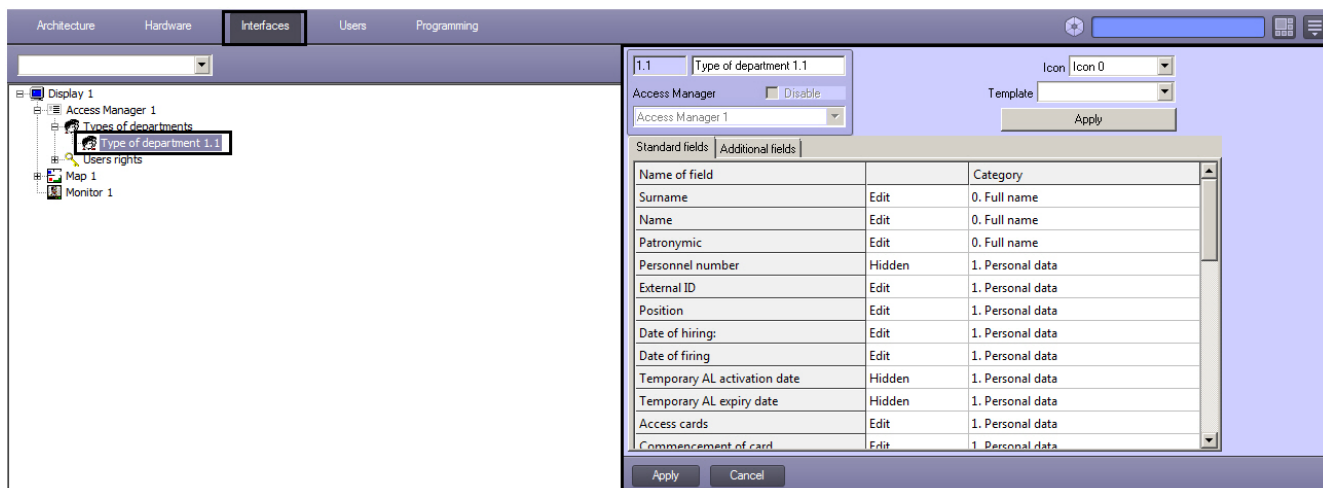


Note

Visibility of fields is defined by operator rights – see the [Configuring availability of fields depending on operator rights in the Access Manager](#) section.

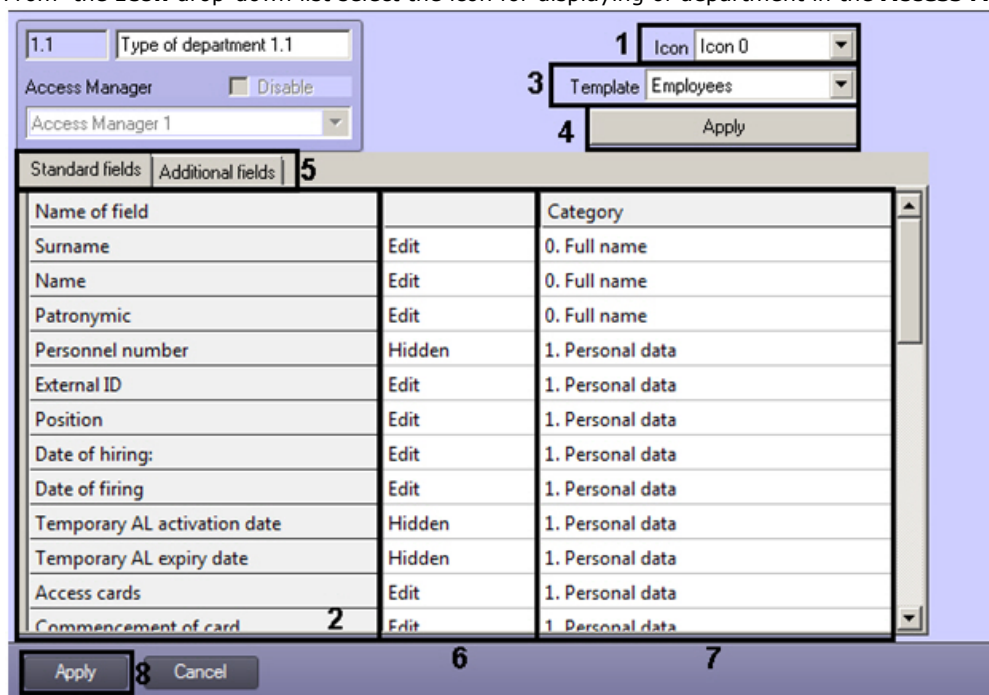
Type of department is configured on the settings panel of the **Type of department** object which is created on the basis of

the **Access Manager** object on the **Interfaces** tab of the **System settings** dialog window.



To configure type of department, do the following:

1. Go to the settings panel of the **Type of department** object.
2. From the **Icon** drop-down list select the icon for displaying of department in the **Access Manager** window (1).



3. List of available fields is displayed in the **Name of field** column (2).



Note

See description of fields in the [Setting user parameters](#) section.

4. It is possible to select template types of departments while going from the *Visitor Management System* module to the *Access manager* module and for convenience of settings of general fields availability. To perform it, do the following:
 - a. From the Template drop-down list select the required template of department type (3). Templates of following department types are available: **Employees, Visitors, Vehicle**.
 - b. Click the **Apply** button to apply the template (4). As a result values in correspondence with the selected template will be displayed in the **Standard fields** and **Additional fields** tabs (5).



Attention!

Settings of the **Type of department** object won't be saved while clicking the **Apply** button. This button only changes values of fields to the specified values in the template. To save these settings click the **Apply** button when all settings will be completed (see step 6).

5. If it's required to set visibility and availability for required fields editing manually, do the following:
 - a. In the column (6) from the drop-down list select one of the following values:

Value	Description
Hidden	The field is not displayed in the list of user parameters while viewing and editing
Read only	The field is displayed in the list of user parameters while viewing and editing but is not available for editing
Edit	The field is displayed in the list of user parameters while viewing and editing and is available for editing. Note. It is not available to edit Card issued by and Access level assigned by fields because these fields are filled in automatically by the operator data while changing/assigning access level or access card.

- b. In the **Category** column enter the name of group in which the field will be displayed in the list of users parameters in the **Access Manager** window while editing and viewing (7). Category name can be optional. If category is not specified, the field will be displayed in the **Other** category of the list of parameters.



Note

Categories in the list are sorted by alphabet. If it's required to strictly define the order of categories, use numeral prefix as for categories used in templates (see step 4).

6. To save changes click the **Apply** button (8).

Configuring of department type is completed.

Configuring availability of fields depending on operator rights in the Access Manager

The Access Manager program module allows restricting of visibility and availability for editing user fields depending on operator rights in the *Access Manager*. Prohibition on performing operation with field in operator rights has priority over availability of field for viewing and editing specified while configuring the type of department. For example, if some field is available for editing in accordance to settings of department type, but its review is forbidden by rights of some operator, than this field won't be visible to this operator. Conversely, if editing of field is allowed by operator rights in the Access manager but the field is available only for reading, than the field will be available for reading for all operators.



Note

User reregistration in the *ACFA Intellect* software is required to apply changes when rights of the current operator are changed.

To configure availability of fields depending on operator rights, do the following:

1. Go to the settings panel of the **User rights in Access Manager** object.

2. The list of all user fields is displayed on the **Standard fields** and **Additional fields** tabs (1). All user fields are hidden on default.



**Note**

See also description of fields in the [Setting user parameters](#) section.

3. In the column (2) from the drop-down list select one of the following values:

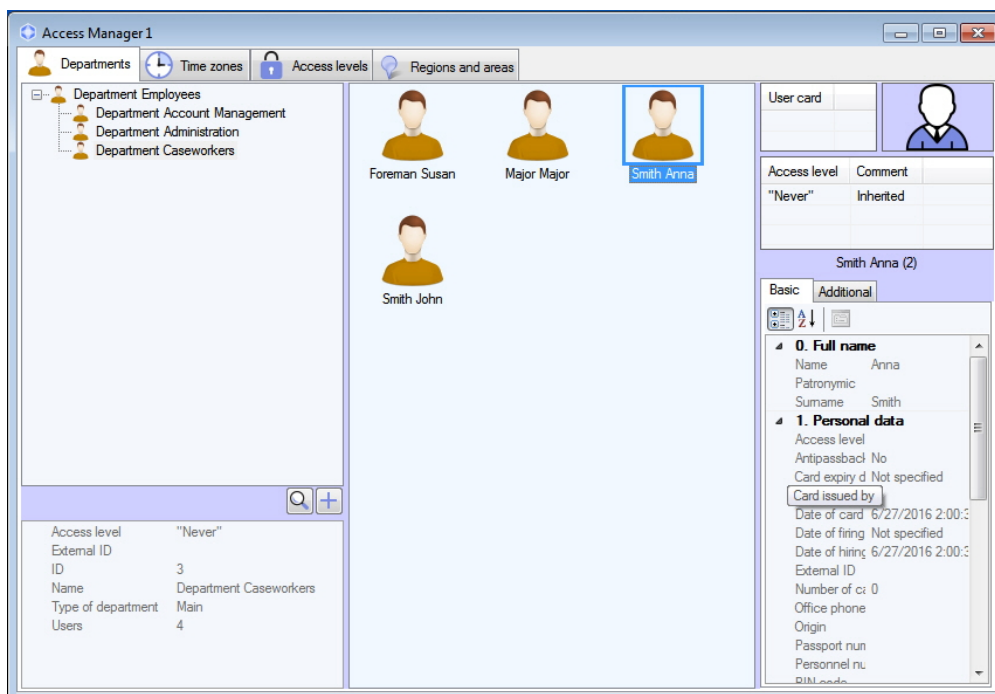
Value	Description
Hidden	The field is not displayed in the list of user parameters while viewing and editing
Read only	The field is displayed in the list of user parameters while viewing and editing but is not available for editing
Edit	The field is displayed in the list of user parameters while viewing and editing and is available for editing. Note. It is not available to edit Card issued by and Access level assigned by fields because these fields are filled in automatically by the operator data while changing/assigning access level or access card.

4. To save changes click the **Apply** button (3).

Configuring of availability fields depending on operator rights is completed.

Access Manager module interface

General view of the **Access manager** interface window is shown in the figure.

**Note**

If fix position of the window in the screen is specified, the name of the Access Manager window won't be displayed - see the [Configuring the position of the Access manager window on the screen](#) section.

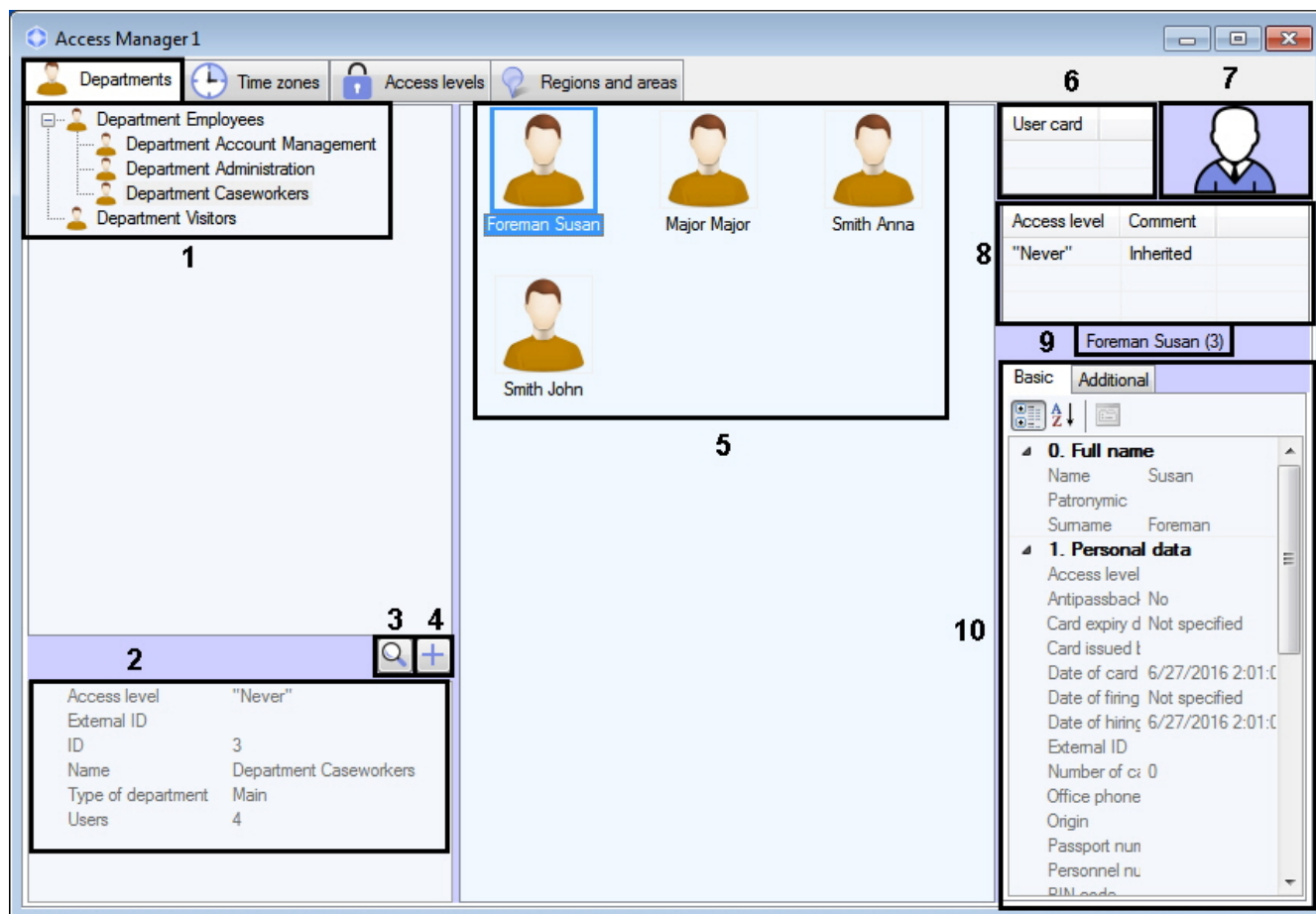
The **Access Manager** window contains three tabs:

1. **Departments** tab
2. **Time zones** tab
3. **Access levels** tab
4. **Regions and areas** tab

Description of each tab is follows.

Departments tab

Working with departments and users is performed on the **Departments** tab.

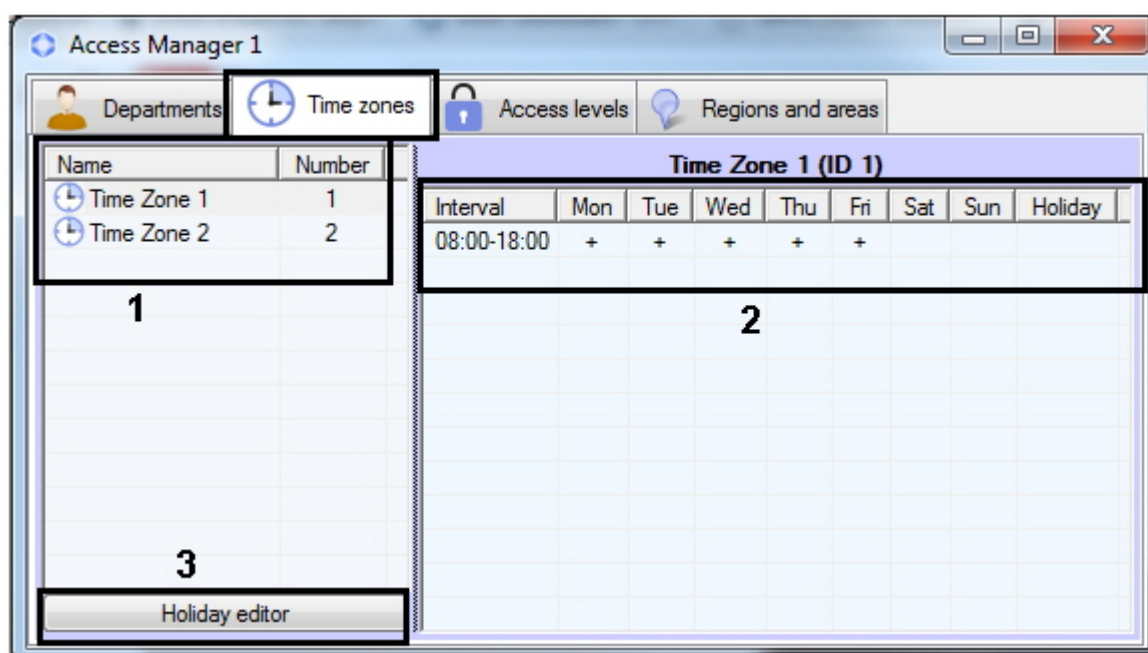


Description of **Departments** tab elements is given in the table.

Nº	Element	Description
1	Departments tree	Hierarchy structure of created departments available for viewing relying on operator rights and/or settings of the Access Manager object – see the Rights for configuring and viewing departments in the Access Manager section.
2	Department parameters	Parameters of department: ID, External ID, Name, Number of users, Type of department, Access levels. Setting and editing of department parameters is given in the Working with departments in the Access Manager software module section.
3	Search for department	Department search button – see the Department search section.
4	Add department	Button of adding a department –see the Adding a department section.
5	List of department users	List of users from the selected department.
6	List of user access cards	Displaying of the list of access cards assigned to user. See also the Assigning an access card to a user section. This list can be hidden or is not available depending on the Access card settings in operator rights and/or on the Access manager object (see the Configuring fields displaying in user accounts section)
7	User photo	Displaying of photo assigned to user. See also the Assigning a photograph to a user section.
8	List of user access levels	List of access levels assigned to user. See also the Assigning access levels to a user section. This list can be hidden or is not available depending on the Access levels settings in operator rights and/or on the Access Manager object (see the Configuring fields displaying in user accounts section)
9	User full name	Displaying of user surname, name, patronymic and its ID (in brackets).
10	User parameters	Displaying of user information. Description of fields is given in the Setting user parameters section.

Time zones tab

Working with time zones and holidays is performed on the **Time zones** tab.

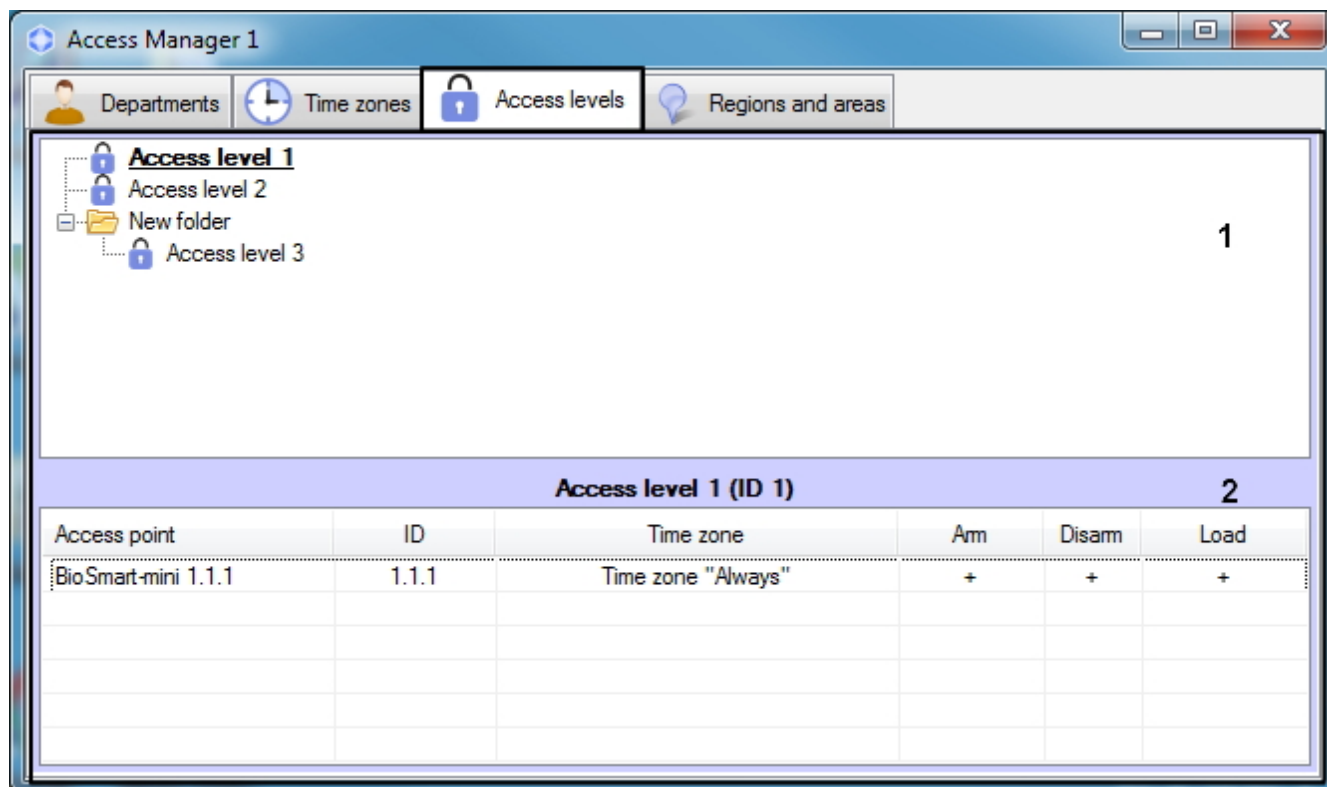


Description of **Time zones** tab elements is given in the table.

Nº	Element	Description
1	List of time zones	Names and identification numbers of time zones created in the system. The following ways of displaying time zones list are available: List , Table , Large icons . The Table view is used on default. See also the Selecting a view of displaying objects list in the Access Manager section.
2	Time zone intervals	List of intervals incoming to the time zone.
3	Holiday editor	Button opening a window of holiday editing – see the Editing holidays section.

Access levels tab

Working with user access levels is performed on the **Access levels** tab.

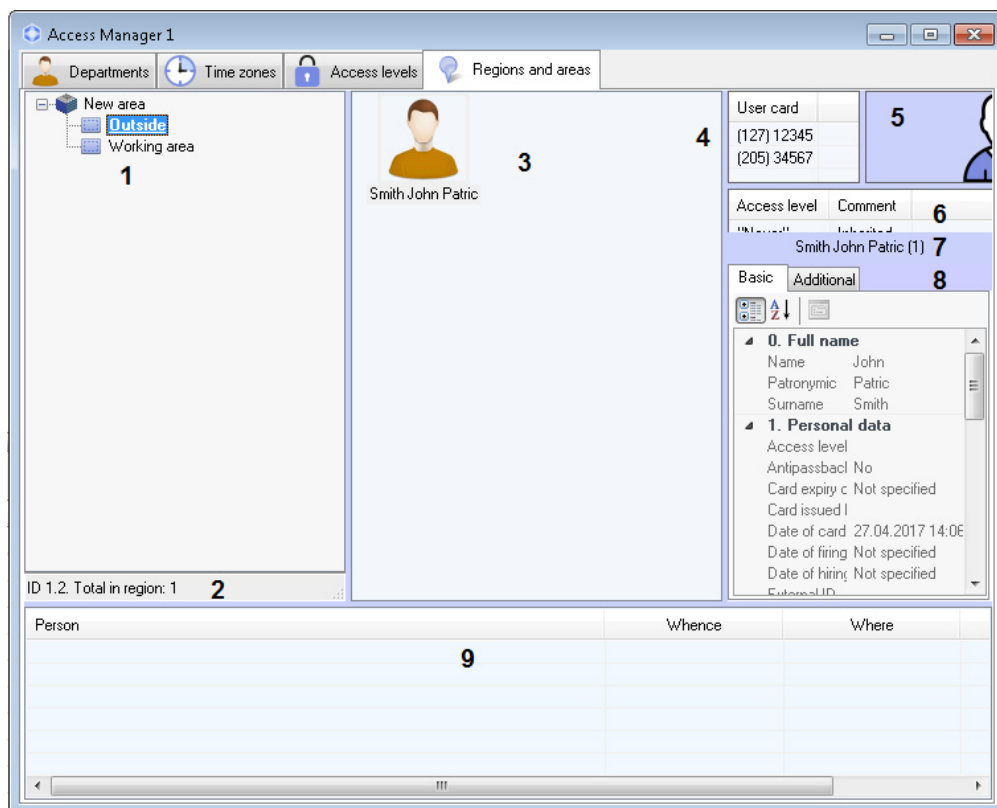


Description of **Access levels** tab elements is given in the table.

Nº	Elements	Description
1	List of access levels	List of access levels created in the system. The List view is used on default. See also the Selecting a view of displaying objects list in the Access Manager section. For details on working with the elements of the list, see Managing the list of access levels .
2	Access level parameters	Description of selected access level: list of access points with identification numbers and time zones, parameters of access point arming and disarming, sending access cards to controller after presenting access card by user. The Table view is used by default.

Regions and areas tab

The **Regions and areas** tab allows to perform Emergency Monitoring.



Description of **Regions and areas** tab elements is given in the table.

No.	Element	Description
1	Areas and regions tree	Hierarchy structure of created areas and regions in the system – see Creating, editing and deleting Area and Region objects
2	Information on the selected area or region	ID of the area/region and the current number of people in it.
3	The list of users in the region	The list of users who are currently located in the region.
4	List of user access cards	Displaying of the list of access cards assigned to user. See also the Assigning an access card to a user section. This list can be hidden or is not available depending on the Access card settings in operator rights and/or on the Access manager object (see the Configuring fields displaying in user accounts section)
5	User photo	Displaying of photo assigned to user. See also the Assigning a photograph to a user section.
6	List of user access levels	List of access levels assigned to user. See also the Assigning access levels to a user section. This list can be hidden or is not available depending on the Access levels settings in operator rights and/or on the Access Manager object (see the Configuring fields displaying in user accounts section)
7	User full name	Displaying of user surname, name, patronymic and its ID (in brackets).
8	User parameters	Displaying of user information. Description of fields is given in the Setting user parameters section.
9	Passes log	Displaying information on users passages in real-time mode.

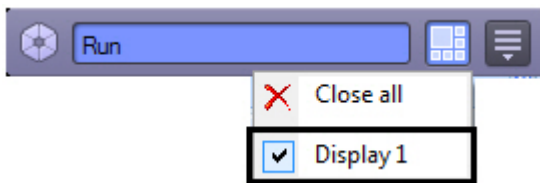
Working with the Access Manager software module

Starting and stopping the Access Manager module

The **Access manager** window is a standard interface window of the *ACFA Intellect* software window. Starting and closing of this window is performed using the **Display** menu of the main control panel.

**Note**

The **Access Manager** object is to be created on the basis of the corresponding display on the **Interface** tab to run the **Access Manager** software module.



To display the **Access Manager** interface window select the **Display** object on the basis of which the corresponding **Access manager** object is created. To hide the **Access Manager** window select the **Close all**.

General view of the Access Manager window see in the [Access Manager module interface](#) section.

To close the **Access Manager** window use the  button. So for repeat opening of this window double click the  icon in the Windows system tray. Pointing to this icon, the name of the **Access Manager** object corresponding to the **Access Manager** interface window will display.

**Note**

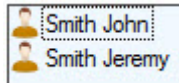
The module icon is displayed in the Windows system tray depending of the value of the *DebugLevel* setting in the *HKLM->Software->Wow6432Node->ITV->INTELLECT->Debug* branch of the Windows Registry. If this parameter is set to 0, empty or missing, the icon will not be displayed. If the parameter has a non-zero value, the icon will be displayed.

General operations with the Access Manager interface elements

Selecting a view of displaying objects list in the Access Manager

In the *Access manager* software module it's possible to configure the view of user lists, time zones and access levels. The following displaying types are available:

1. List.



2. Table.

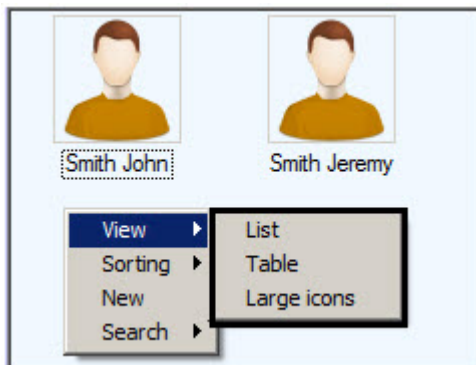
Full Name	Date of card issue	PIN c...	User locked	Antipassback
 Smith John	01.01.0001 0:00:00		No	No
 Smith Jeremy	13.04.2016 13:25:11		No	No

3. Large icons.

**Note**

The **Large icons** view is used on default for user list, times and zones and regions and areas list; **Table** and **List** views are used for access levels. The latter can not be changed.

To select the view of displaying use functional menu opened by right mouse click in free space of objects list.

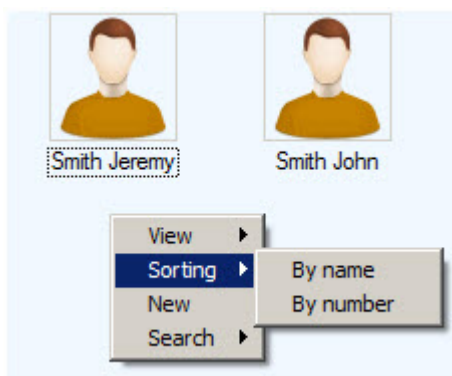


Selecting a way of sorting objects in the list

In the *Access Manager* software module it's possible to select the following ways of sorting user lists, time zones and access levels if the **List** or **Large icons** view is selected:

1. By name.
2. By number.

To select the way of sorting use functional menu opened by right mouse click in free space of objects list.

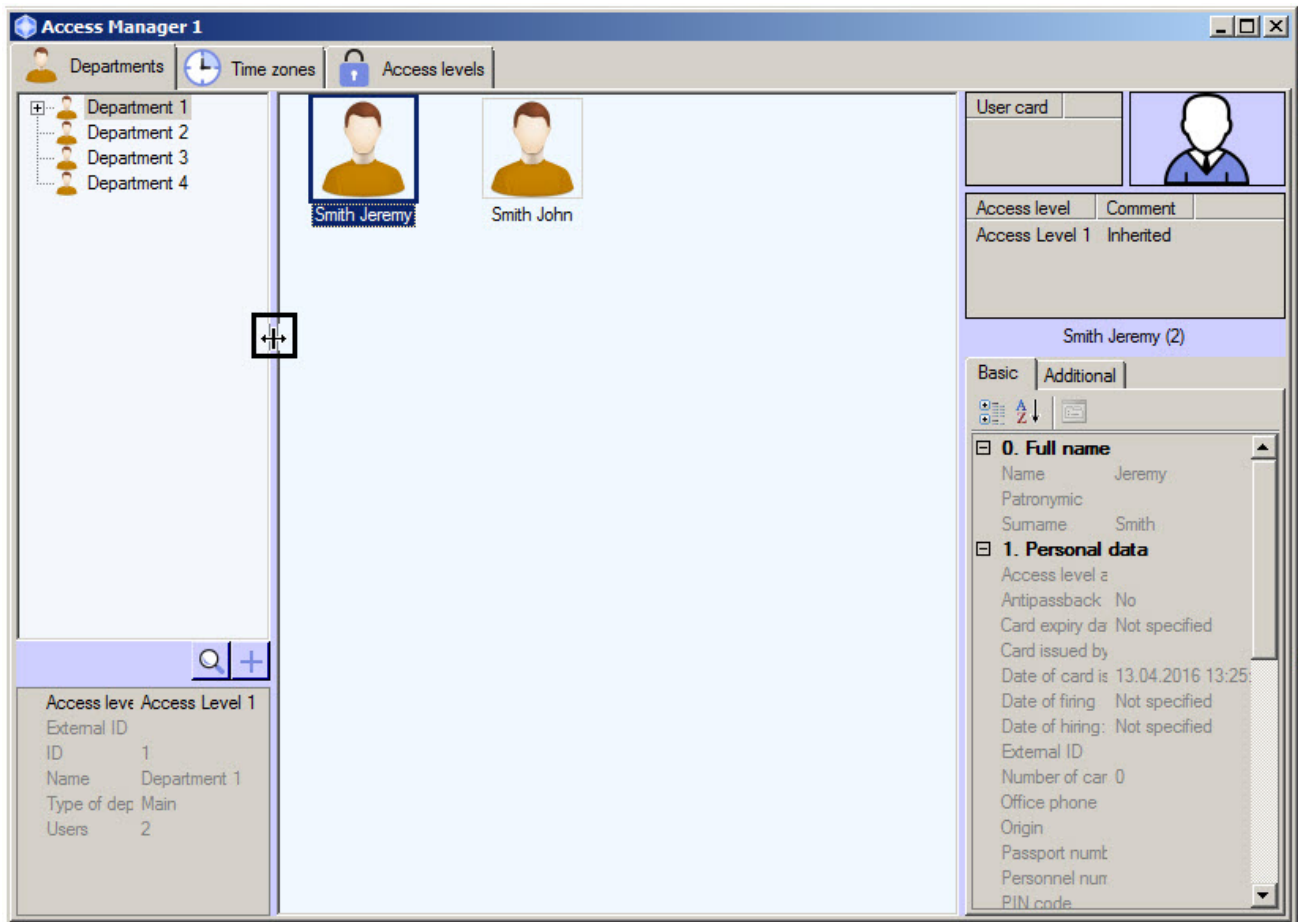


To sort values in the list by some field if the **Table** view is selected, click the left mouse button on the title of column with field name.

Full Name	Date of card issue	PIN code	User locked	Antipassback	Card expiry date
Smith Jeremy	13.04.2016 13:25:11		No	No	01.01.0001 0:00:00
Smith John	01.01.0001 0:00:00		No	No	01.01.0001 0:00:00

Change elements sizes of the Access Manager window interface

It's possible to change elements sizes of the **Access Manager** window interface using mouse. Pointing to border between interface elements of the **Access Manager** window, the cursor will be as follows.



It's possible to move the border between interface elements holding the left mouse button.

Key combinations for working with objects lists

Use key combination described in the following table while working with lists of users, time zones and access levels.

The object list is to be active for using hot keys. So before using key combination click the left mouse button on area of object list.



Note

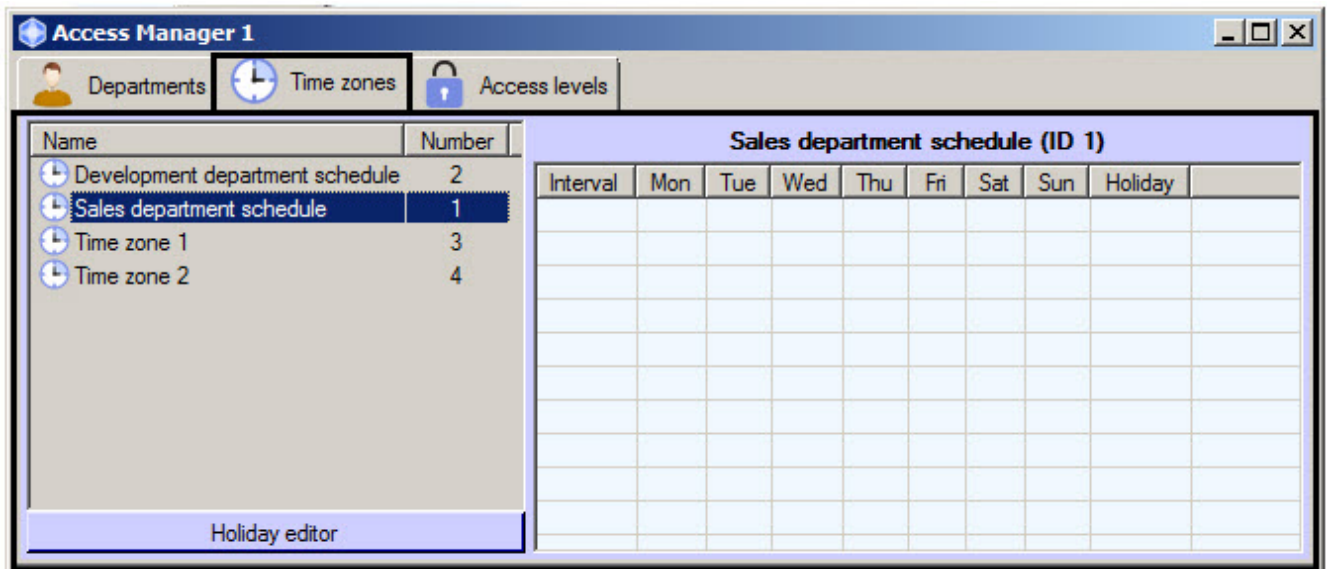
To use Ctrl+Del and Ctrl+Backspace key combinations select the object in the list.

Key combination	Description
Ctrl+F	Search for object.
Ctrl+N	Create new object.
Ctrl+Del	Delete object.
Ctrl+Backspace	

Working with time zones in the Access Manager software module

General information about time zones in the Access Manager software module

Working with time zones is performed on the **Time zones** tab of the **Access Manager** window.



Time zone is used as working schedule in the Access Manager software module. It's possible to set intervals of two types:

1. Week interval. Time interval is set for specified days of the week.
2. Intervals of shift schedule. Interval is repeated with specified period starting from the specified day.



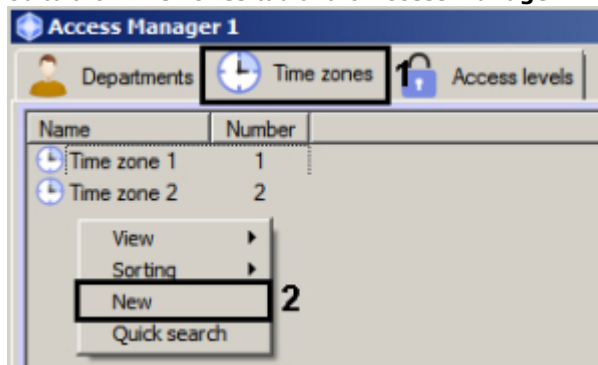
Attention!

Few types of hardware support shift schedules in spite of their supporting in the *Access Manager* software module. At most, time zones with shift intervals will be ignored by ACS integration. Exception to this case applies if integration supports operation in the "Access request" mode when hardware request the integration on access through the specified access point.

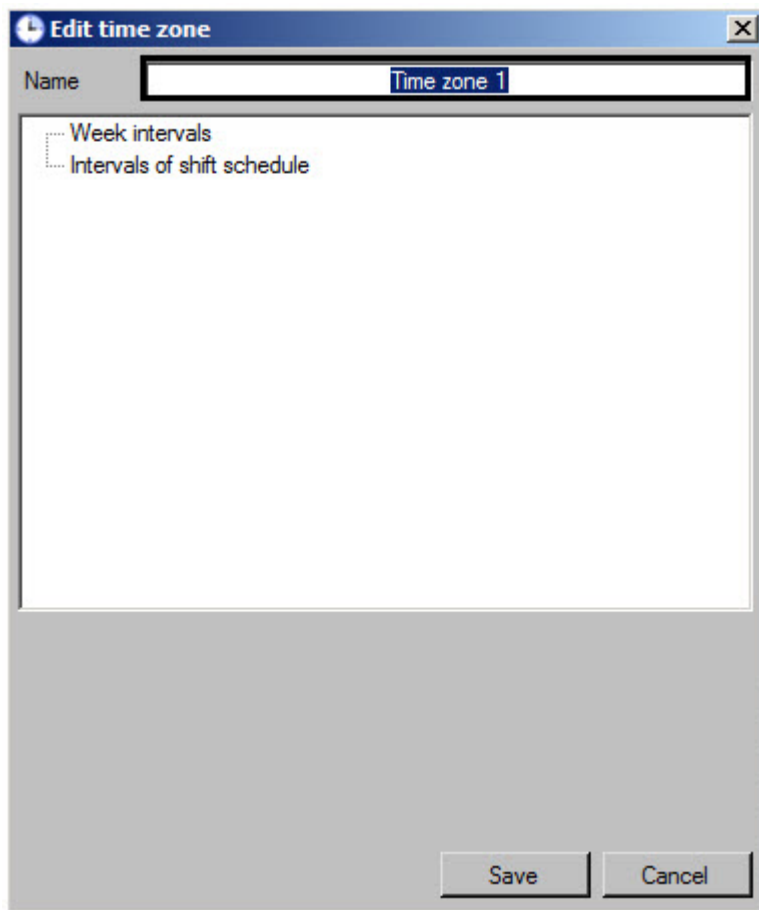
Creation of a time zone in the Access Manager software module

To create time zone, do the following:

1. Go to the **Time zones** tab of the **Access Manager** window (1).



2. Click the right mouse button in free area of time zone list. The functional menu will be opened.
3. Select the **New** item (2). The **Edit time zone** window will open.



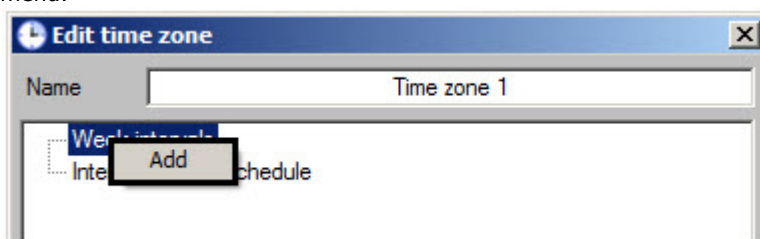
4. Enter the name of creating time zone in the **Name** field.



Note

If time zone with specified name is already exists, than the corresponding message will be displayed while saving.

5. Add week intervals to the time zone if it's required:
- Click right mouse button on the **Week intervals** line and select the **Add** item in the opened functional menu.



- New interval will be created in the **Week intervals** group. Panel of interval configuring will display at the bottom of the **Edit time zone** window.



Note

Name of the interval is a time period and specifying days in which interval operates within brackets. Apart of week days separated by commas, the following values can be specified:

- Empty interval.
- Whole week.
- Whole week and on holiday.
- On workdays.
- On workdays and on holiday.
- On the weekend and on holiday.
- On the weekend.
- Only on holiday.

- c. Enter or set using slider time of interval start in the **Start** field (1).

- d. Enter or set using slider time of interval end in the **End** field (2).
- e. Set checkboxes corresponding to days in which interval should operate (3).
- f. If it's required to eliminate holidays from the interval, set the **Holidays** checkbox (4).

Note
Working with holidays is described in the Edit holidays section.

Note
To delete interval, click right mouse button on the interval and select the **Delete** item in the opened functional menu.

- g. Repeat steps a-f for all required week intervals.
6. Add intervals of shift schedule to the time zone if it's required:
- a. Click right mouse button on the **Intervals of shift schedule** line and select the **Add** item in the opened functional menu.

- b. New interval will be created in the **Intervals of shift schedule** group. Panel of interval configuring will

display at the bottom of the **Edit time zone** window.



Note

Name of the interval is a date of interval start, time interval and period of interval repetition in days.

- c. Enter or set using slider time of interval start in the **Start** field (1).

- d. Enter or set using slider time of interval end in the **End** field (2).

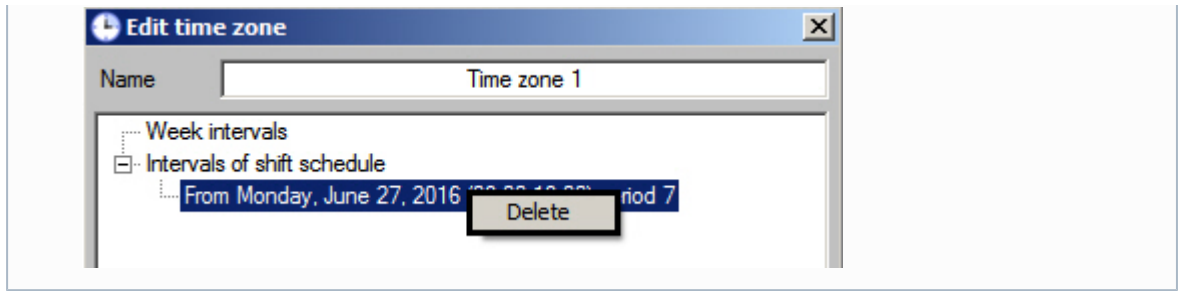
- e. Enter the start day of shift schedule in the **Start date** field using keyboard or calendar opened by  button (3).

- f. In the **Period** field using up-down buttons enter the number of days in which the interval of shift schedule will be repeated (4).



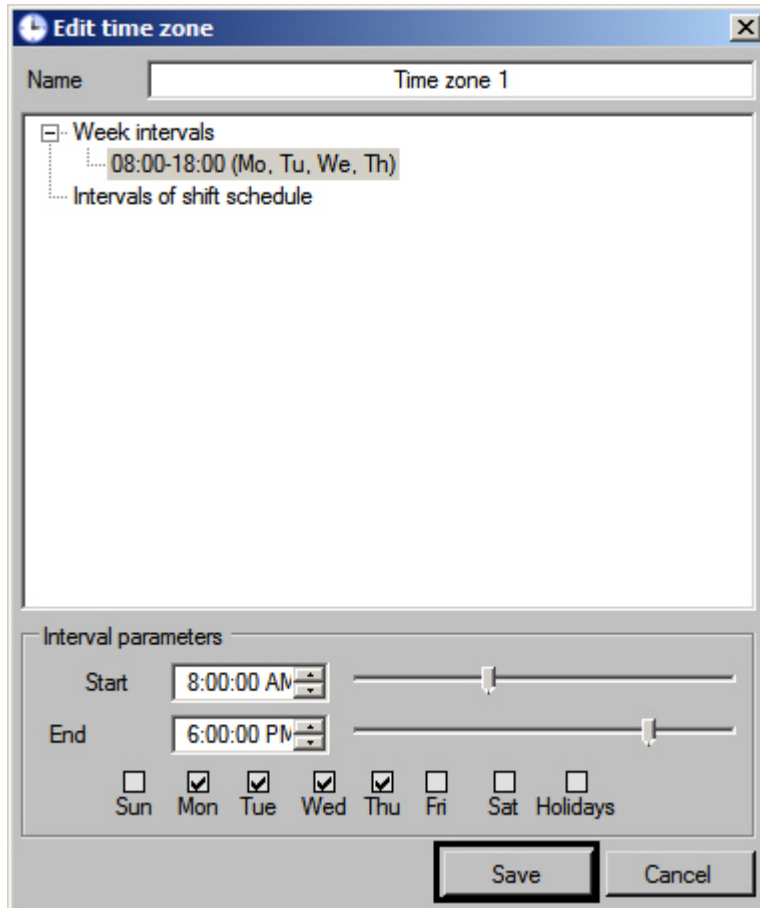
Note

To delete interval, click right mouse button on the interval and select the **Delete** item in the opened functional menu.

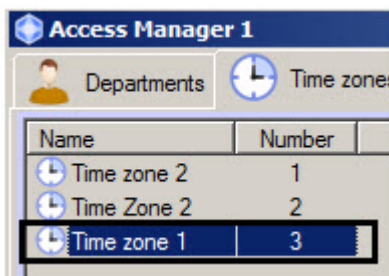


g. Repeat steps a-f for all required week intervals.

7. Click the **Save** button.



Creation of time zone is completed. Created time zone will be displayed in the list.



Editing a time zone in the Access Manager software module

Editing of time zone involves adding and deleting intervals from time zone and changing configured intervals. To start editing of time zone double click the required time zone in the list on the **Time zones** tab. As a result, the **Edit time zone** window will open.

Working with this window is the same as while creating time zone - see [Create time zone](#) section.

Also this window can be opened by double click of left mouse button on interval in the list of selected time zone. The clicked interval will be selected in the opened window.



Note

The first interval will be selected while clicking the time zone in the **Edit time zone** window

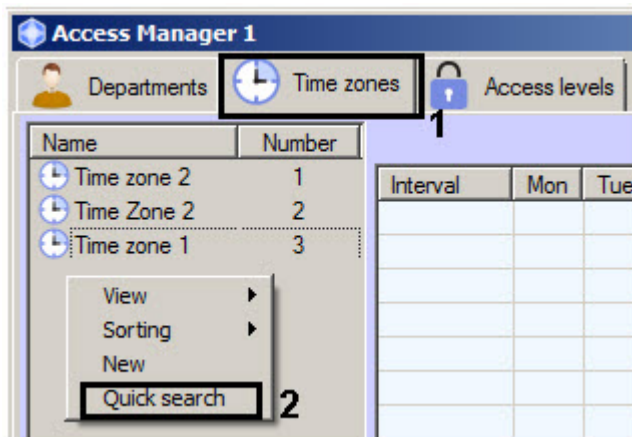
Interval	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Holiday
08:00-18:00	+	+	+	+	+			

Search for time zone

Going to search for time zone

In the *Access Manager* software module it's possible to search for time zone by name and ID. To search for time zone, do the following:

1. Go to the **Time zones** tab in the **Access Manager** window (1).



2. Click the right mouse button in free area of time zone list.
3. In the opened functional menu select the **Quick search** item. The **Search for time zone** window will open.

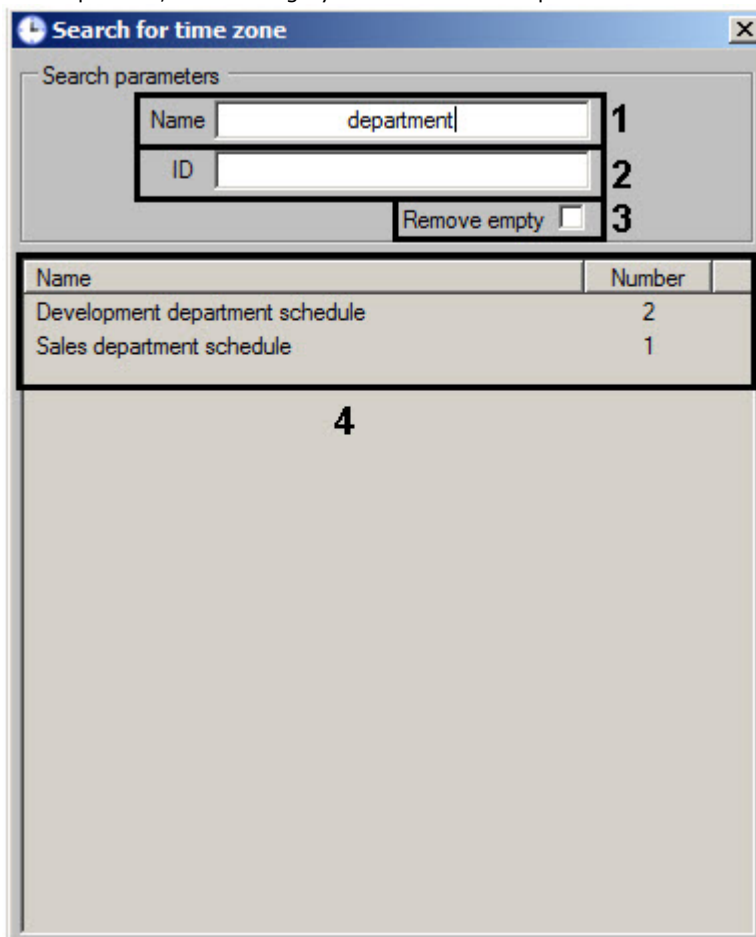
Going to search for time zone is completed. Working with the **Search for time zone** window is described in the Working with the Search for time zone window section.

Working with the Search for time zone window

The **Search for time zone** window is opened while searching for time zone (see the [Going to search for time zone](#)) or while configuring access level (see [Creation of an access level](#) section).

Working with the **Search for time zone** window is performed as follows:

1. If it's required to filter time zones by name, enter the name or its part in the **Name** field (1). If name of time zone is not specified, the filtering by this field won't be performed.



2. If it's required to filter time zones by ID, enter identical number of required time zone in the **ID** field (2). If ID is not specified the filtering by this field won't be performed.
3. If time zones without intervals are not required in search result, set the **Remove empty** checkbox (3).
4. Click the **Enter** button on the keyboard.
5. Time zones satisfying to search terms will be displayed in the table of search results (4). Search is case-insensitive. All objects corresponding fields of which contain specified values will be found.

To sort search results click the left mouse button on title of corresponding column.

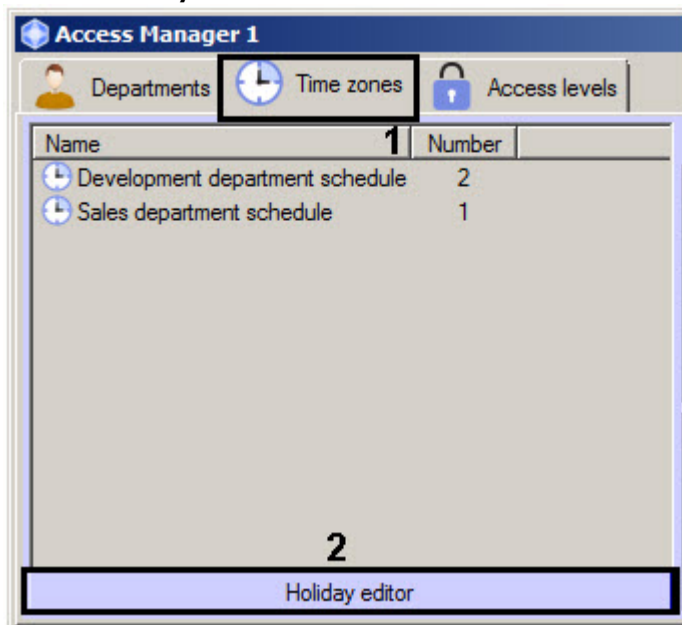
While double click on time zone, the **Search for time zone** window will be closed and corresponding time zone will be selected in the list in the **Time zones** tab or will be added to configured access level.

Search for time zone is completed.

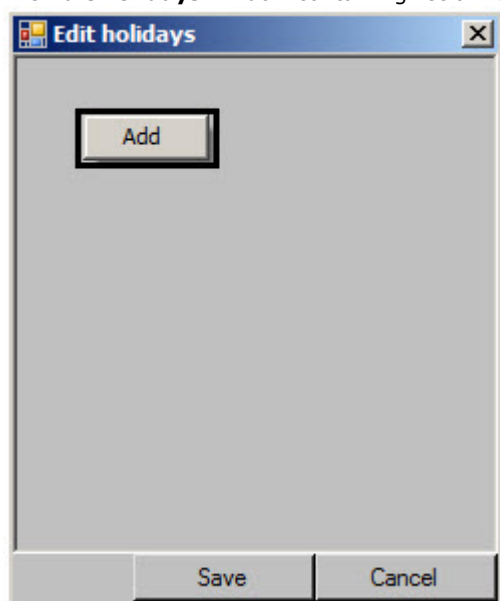
Editing holidays

To edit holidays, do the following:

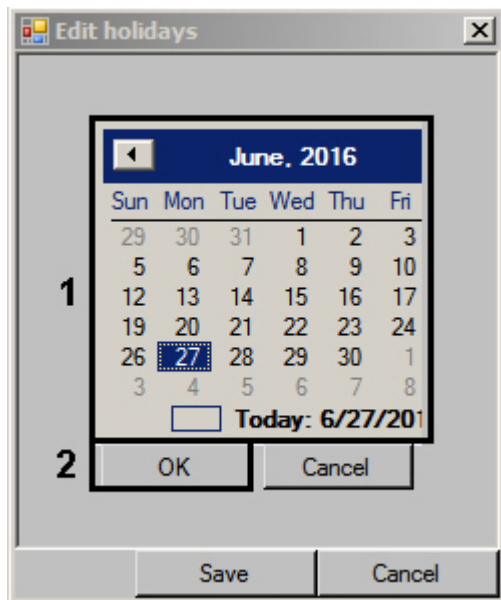
1. Go to the **Time zones** tab of the **Access manager** window.
2. Click the **Holiday editor** button.



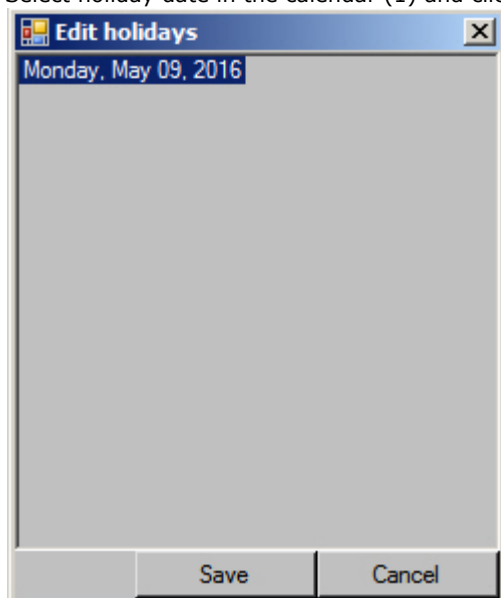
3. The **Edit holidays** window containing list of holidays will be opened.



4. To add holiday click the right mouse button in free area of holidays list and select the **Add** item in the opened functional menu. The calendar will display.



5. Select holiday date in the calendar (1) and click the **OK** button (2). The holiday will be added to the list.

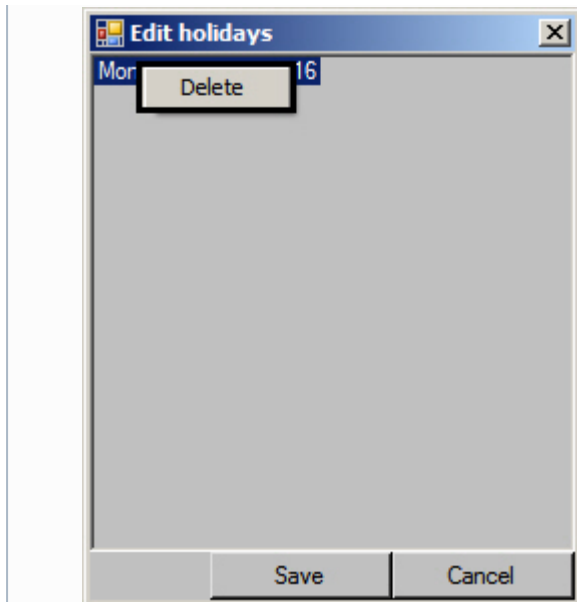


6. Repeat steps 4-5 for all required holidays.

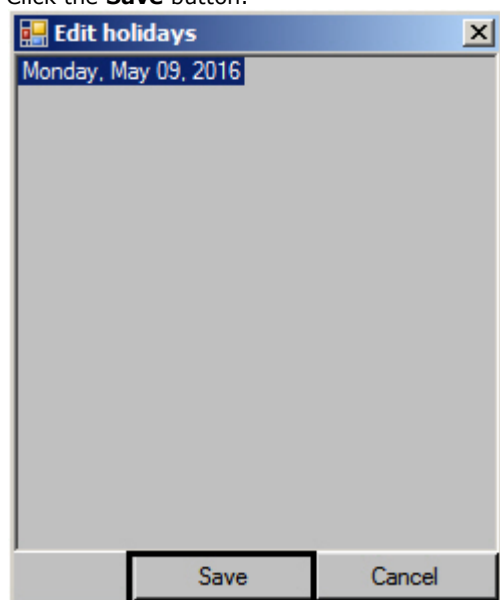


Note

To delete holiday click the right mouse button on it and select the **Delete** item in the opened functional menu.



7. Click the **Save** button.

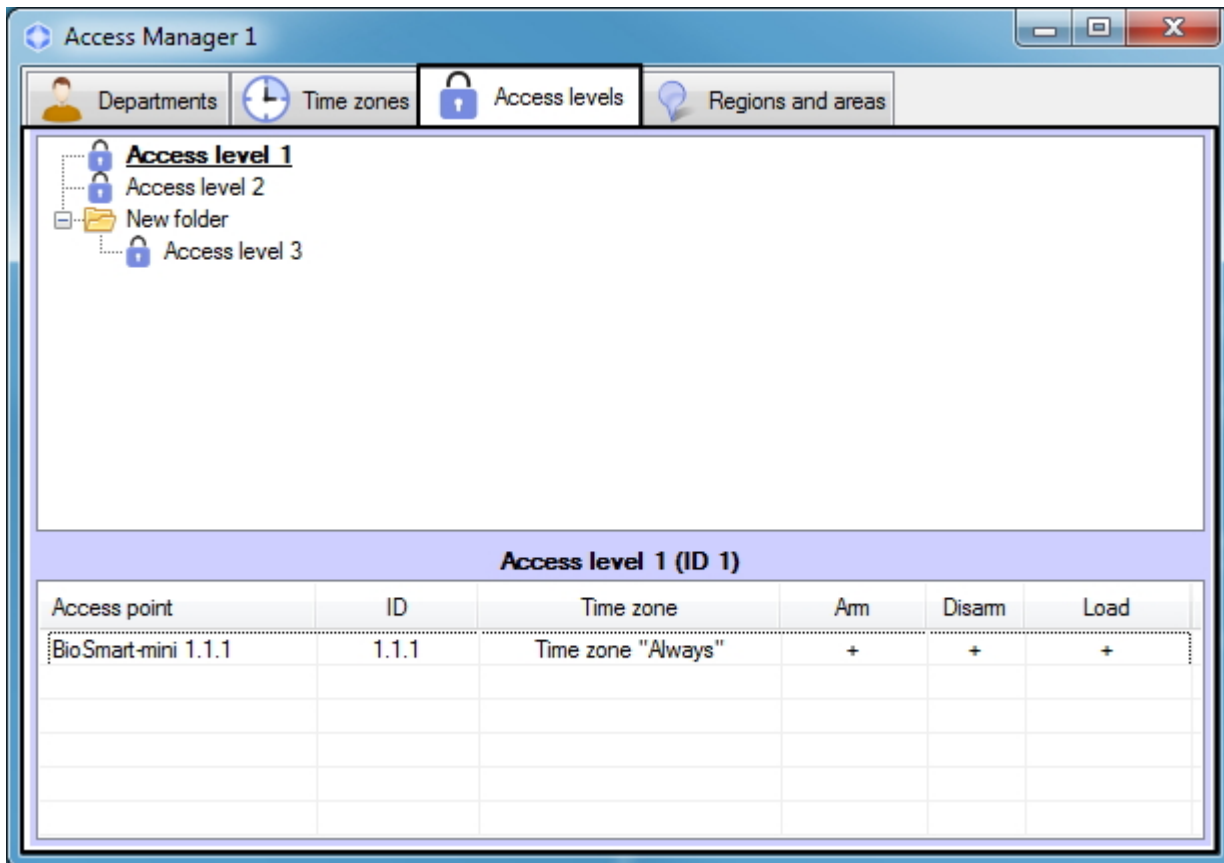


Editing of holidays is completed.

Working with access levels in the Access Manager software module

General information about working with access levels in the Access Manager software module

Working with access levels is performed on the **Access levels** tab of the **Access Manager** window.

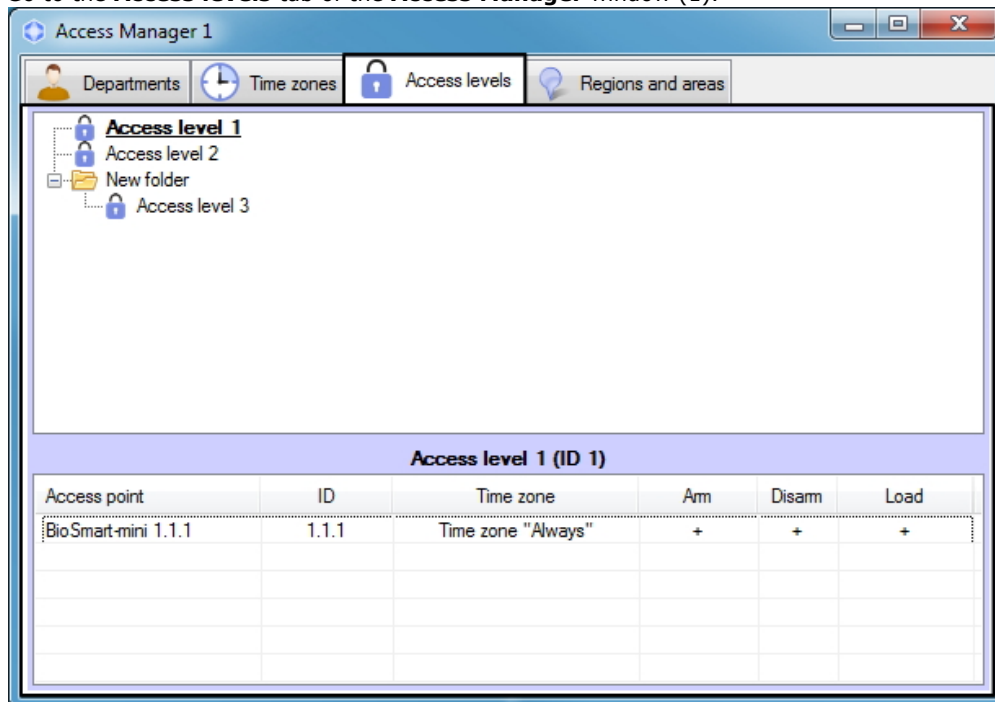


The *Access Manager* software module allows creating, editing, copying, viewing and deleting access levels. At that, possibility of creating, editing and deleting access levels can be forbidden while configuring the *Access Manager* software module - see the [Rights for configuring access levels in the Access manager](#) section.

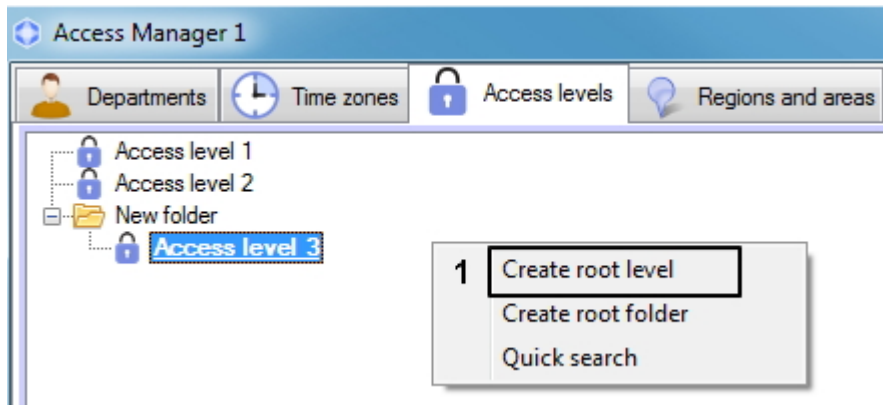
Creation of an access level in the Access Manager software module

To create access level, do the following:

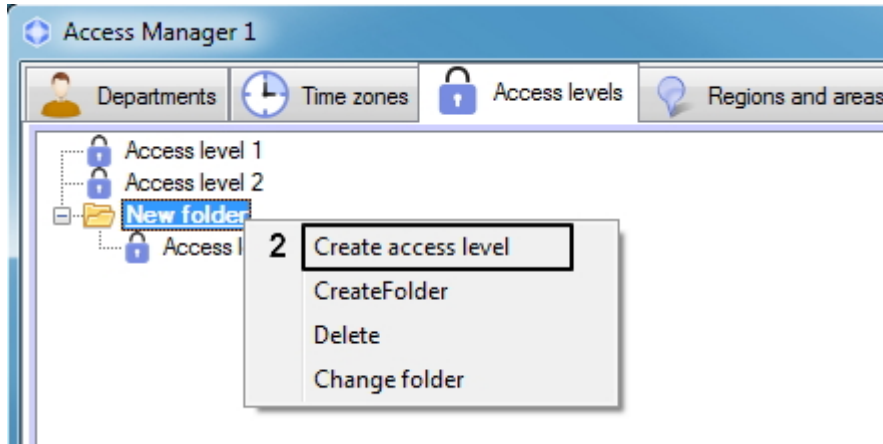
1. Go to the **Access levels** tab of the **Access Manager** window (1).



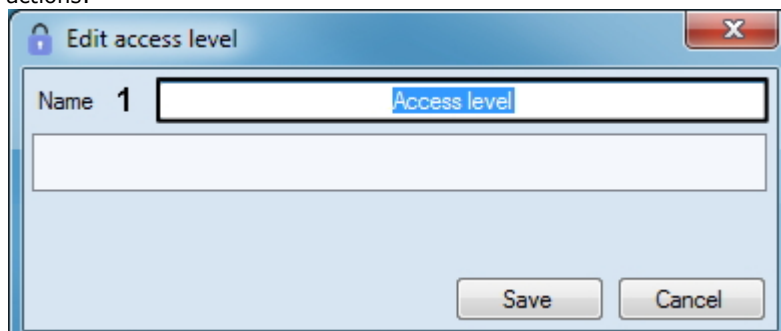
2. There are two ways to create a new access level:
 - a. Right-click in the free area of the access level list and select **Create root level** (1) in the functional menu. In this case, the access level will be created in the root list of access levels.



- b. Right-click the folder and select **Create access level** (2). In this case, the access level will be created in the selected folder.



3. If you select any of the commands, the **Edit access level** window will open, enabling you with the following actions:



- a. In the **Name** field enter name of the access level (1).

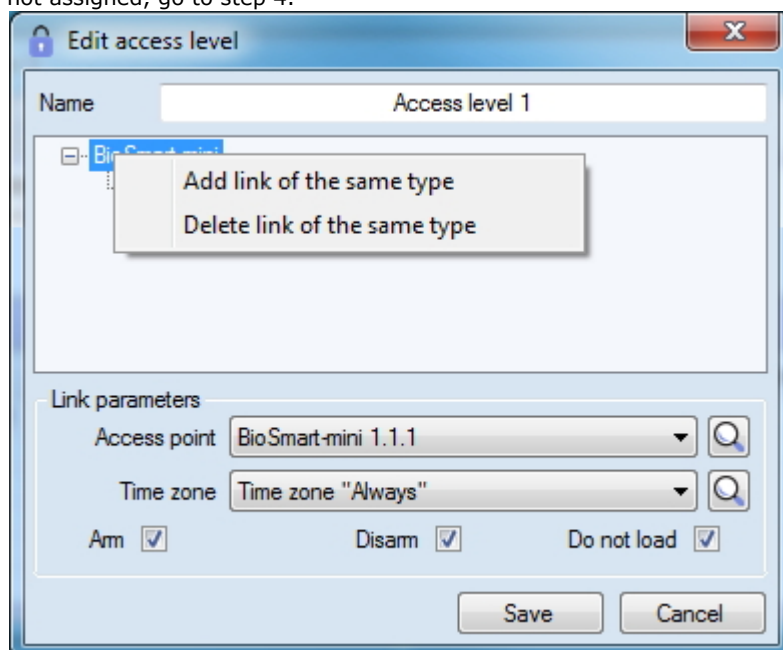


Note

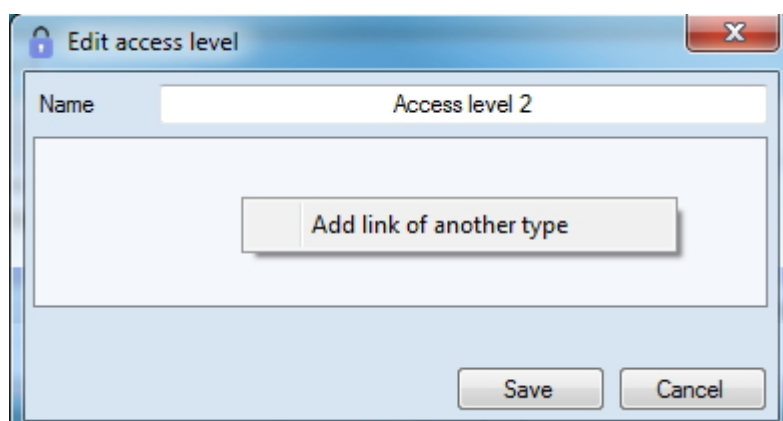
Name of access level should be unique. If access level with such name is already exists in the system, the corresponding message will display while saving and access level won't be saved.

- b. Add link between the access point and the time zone. This can be done in two ways either.
- If it's required to add link for reader of such type for which links are already exist in the list, click the right mouse button on the name of link and in the opened functional menu select the **Add link of**

the same type item and go to step 4. If there is only one access point of this type for which link is not assigned, go to step 4.



- ii. If it's required to add link for access point of new type, click the right mouse button in free area of access rules list and in the opened functional menu select the **Add link of another type** item and go to step 4. If there is only one access point for which link is not assigned, go to step 4.



Note

If links for all created readers of this type are assigned in the access level, the message about failure to create new link will display because only one link can be added for each reader.

4. When type of rule is selected, the **Search for access point** window will be opened. In this window all access point are grouped by object types in the *ACFA Intellect* software. To search for and select an access point, you must do the following:

- a. Find and select access point as follows:
 - b. Select type of access point from the **Type** drop-down list if it's required (1).
 - c. Select the location of the access point from the **Area** drop-down list if it's required (2).
 - d. Select the location of the access point from the **Region** drop-down list if it's required (3)
 - e. Enter name of access point or its part in the **Name** field if it's required (4).
 - f. Enter ID of required access point in the **ID** field if it's required (5).
 - g. The search will be performed automatically. The list of search results will be displayed below (6).
 - h. Double-clicking the required access points, thus highlighting them in bold.
 - i. Click **OK** button when access points are selected (7).
5. You will go back to the **Edit access level** window. The panel for configuring the access level will be displayed at the bottom.

6. Access point specified in the search is selected in the **Access point** drop-down list (see step 4) or the first from free access points of selected type. Select the access point through which access will be allowed with configured access level from the **Access point** drop-down list if it's required (1).

Click the  button and go to step 4 if it's required to search for access point.

7. From the **Time zone** drop-down list select time zone during which access through the selected access point will be allowed to users with configured access level (2).

Click the  button if it's required to search for required time zone - see the [Working with the Search for time zone window](#) section.



Note

Time zones are created and configured on the **Time zones** tab of the **Access Manager** window - see the [Working with time zones in the Access Manager software module](#) section. Also it's possible to use system time zones "Always" and "Never".

8. Set the **Arm** checkbox to arm access point after presenting access card by user (3).
9. Set the **Disarm** checkbox to disarm access point after presenting access card by user (4).
10. If it's not required to send access cards to controller after presenting access card by user, set the **Do not load** checkbox (5).



Attention!

Functions of arming, disarming and sending access cards should be supported by hardware.

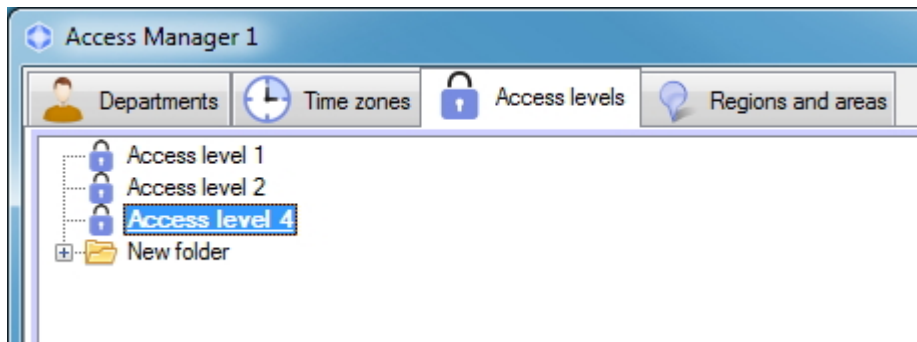


Note.

Function of the **Do not load** checkbox can differ depending on the integration module in use. For example, in PERCo-S-20 integration this checkbox enables commission mode.

11. Repeat steps 3-10 for all required links.
12. Click the **Save** button (6).

Created access level will be displayed in the list.



Creating of access level is completed.

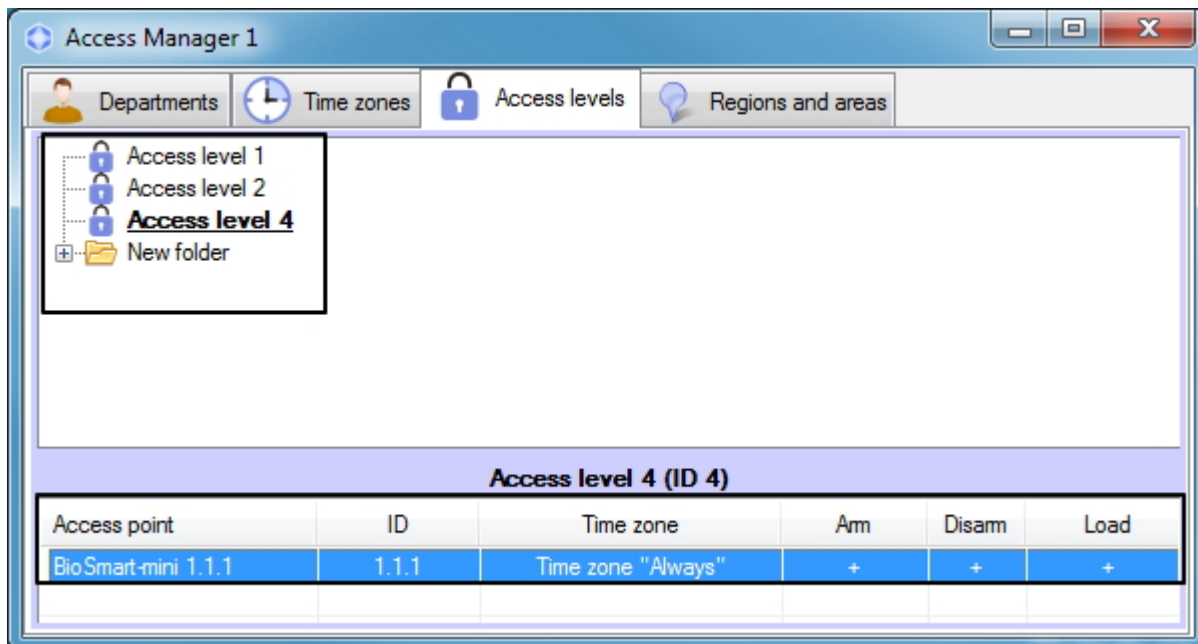
Editing an access level in the Access Manager software module

Editing of time zone involves adding, deleting and changing links. To start editing of access levels, double-click the required access level in the list on the **Access levels** tab or on the name of access point in the table of access level parameters.

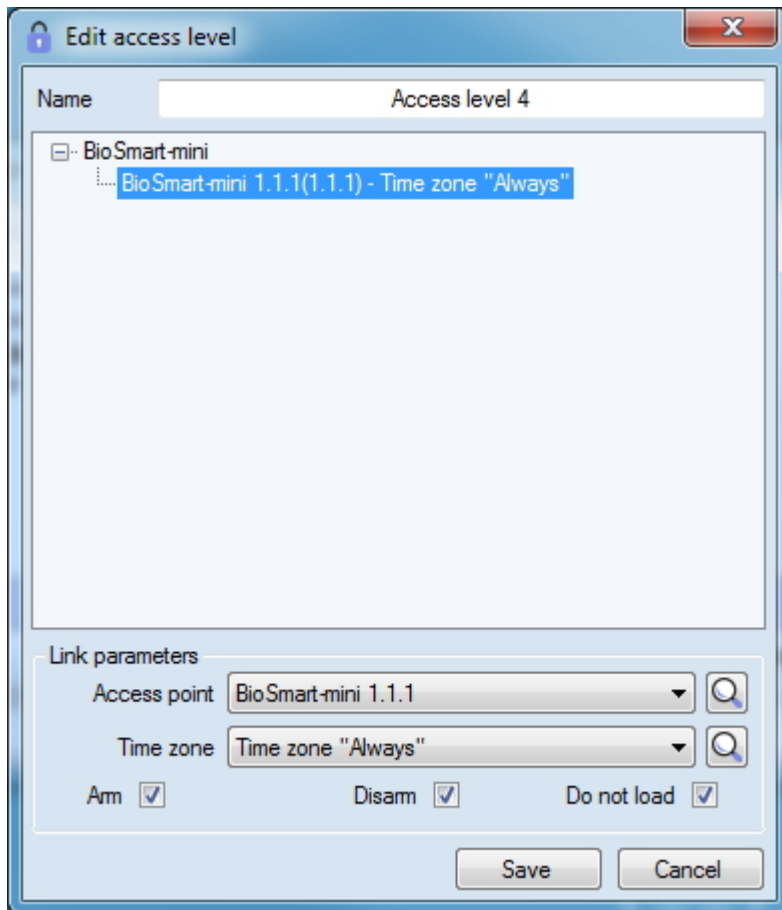


Note

The link to the corresponding access point will be selected in the opened **Edit access level** window as you click on the name of the access point. The first link will be selected while clicking the access level.

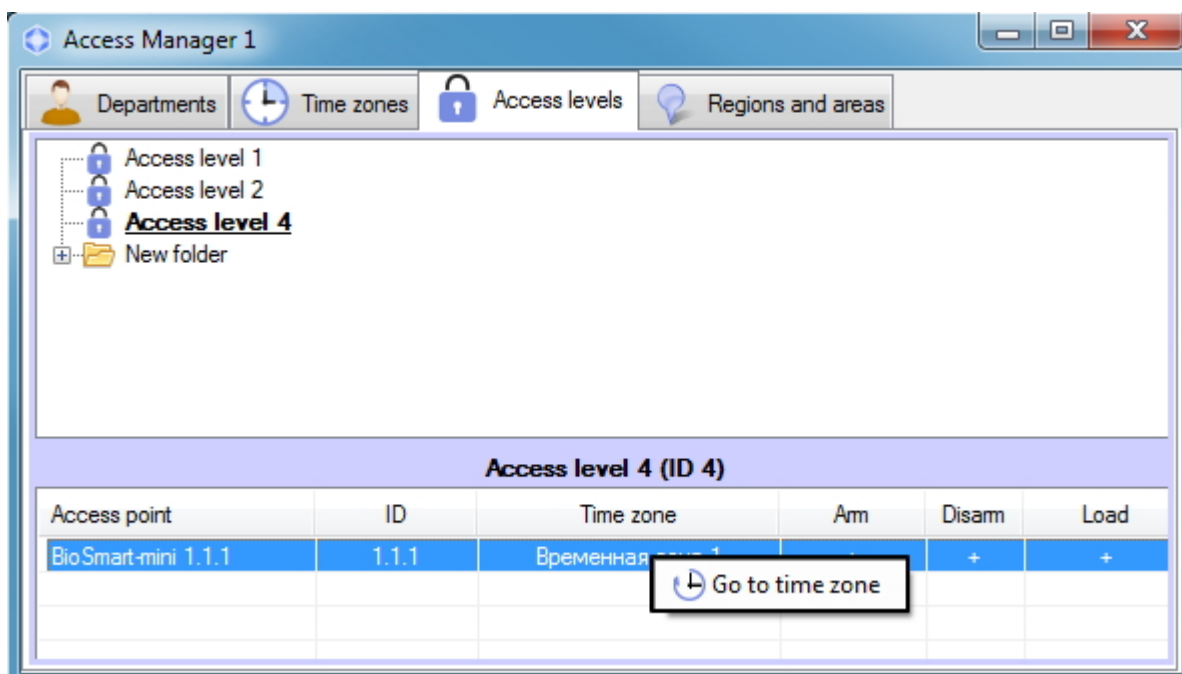


As a result the **Edit access levels** window will be opened. Working with this window is the same as while creating access level - see [Create access level](#) section.



Going to the time zone

At the bottom of the **Access levels** tab there is a list of access points added to the selected access level. If the user time zone related to the access point is not **Always** and not **Never**, it's possible to go to this time zone on the **Time zones** tab. Right-click the required access point and select **Go to time zone** in the opened functional menu.



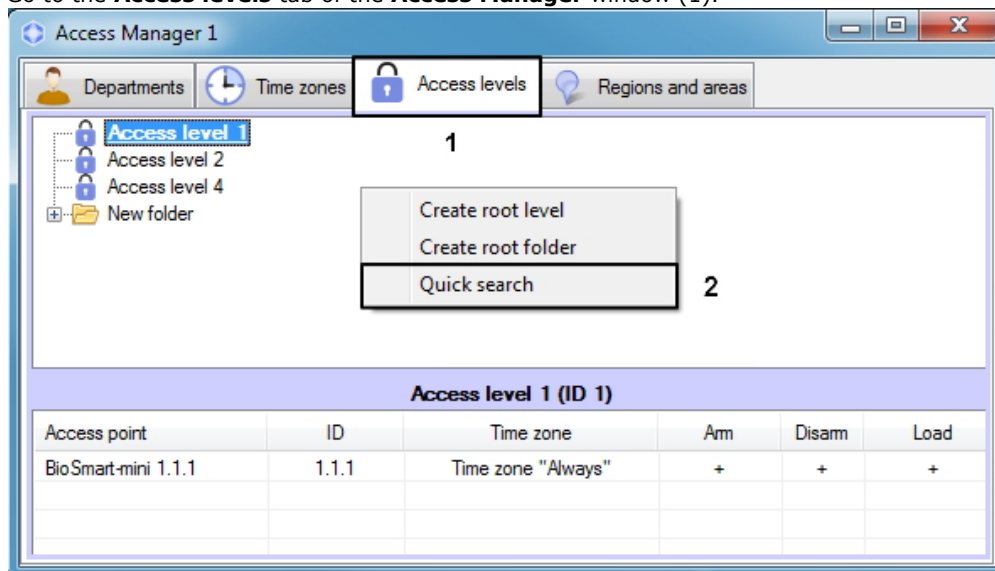
As a result, the **Time zones** tab with the required zone will be opened.

Search for access level

Going to search for access level

In the *Access Manager* software module it's possible to search for access level by name, ID and access point. To go to search for access level, do the following:

1. Go to the **Access levels** tab of the **Access Manager** window (1).



2. Click the right mouse button in free area of access levels list.
3. Select the **Quick search** item in the opened functional menu. The **Search access level** window will be opened. For details on working with the functional menu, see [Managing the list of access levels](#).

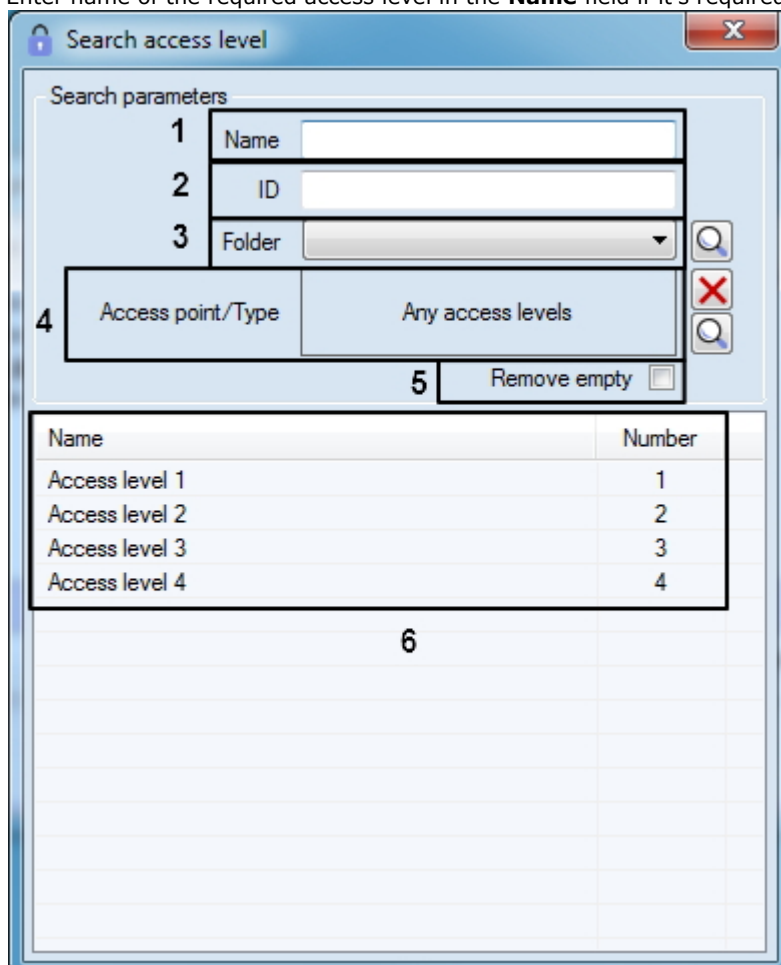
Going to search for access level is completed. Working with the **Search for access level** window is described in the [Working with the Search for access level window](#) section.

Working with the Search access level window

The **Search access level** window can be opened while searching for access level (see the [Going to search for access level](#) section), department configuring (see the [Add department](#) section), searching for department (see the [Working with Search for department window](#) section) or while user configuring (see the [Assigning access levels to a user](#) section).

Working with the **Search access level** window is performed as follows:

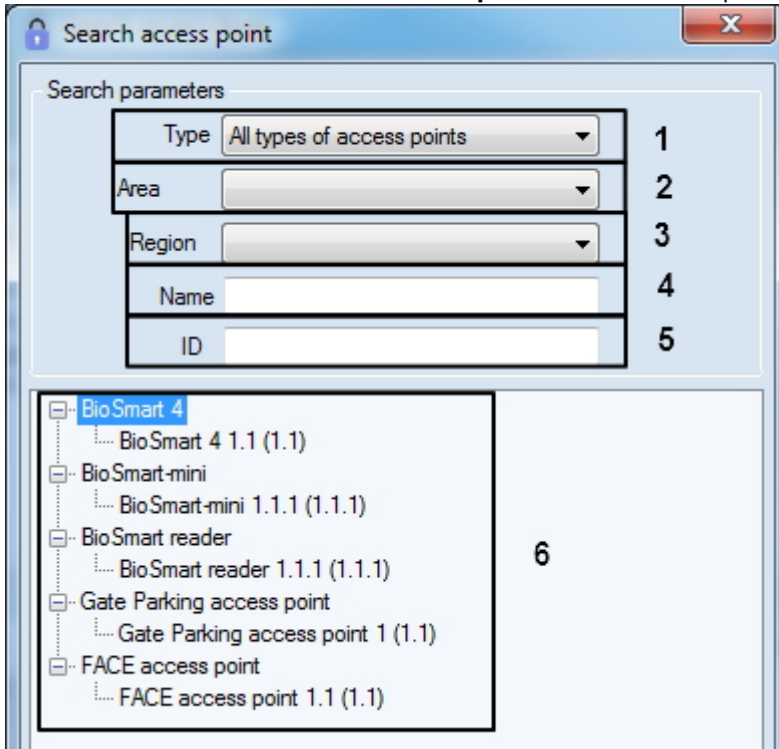
1. Enter name of the required access level in the **Name** field if it's required (1).



2. Enter the identification number of the required access level in the **ID** field if it's required (2).

3. Select the folder the level is located in from the **Folder** drop-down list if it's required (3).
4. If it's required set the list of access points which the required access levels should contain:

- a. Click the  button. The **Search access point** window will be opened.



- b. Select type of the required access point from the **Type** drop-down list if it's required (1).
- c. Select the location of the access point from the **Area** drop-down list if it's required (2).
- d. Select the location of the access point from the **Region** drop-down list if it's required (3).
- e. Specify the name of access point or its part in the **Name** field if it's required (4).
- f. Specify the identification number of the required access point in the **ID** field if it's required (5).
- g. The search will be performed automatically, and the list of search results will be displayed below (6).
- h. Double-click on the required access point in the list (6).

 Note

To clear the list of access points click the  button.

5. If it's required to remove access levels not associated to any access points from the search results, set the **Remove empty** checkbox (5).
6. Results of access levels search will be displayed in the list (6). Search is case-insensitive. All objects corresponding fields of which contain specified values will be found.

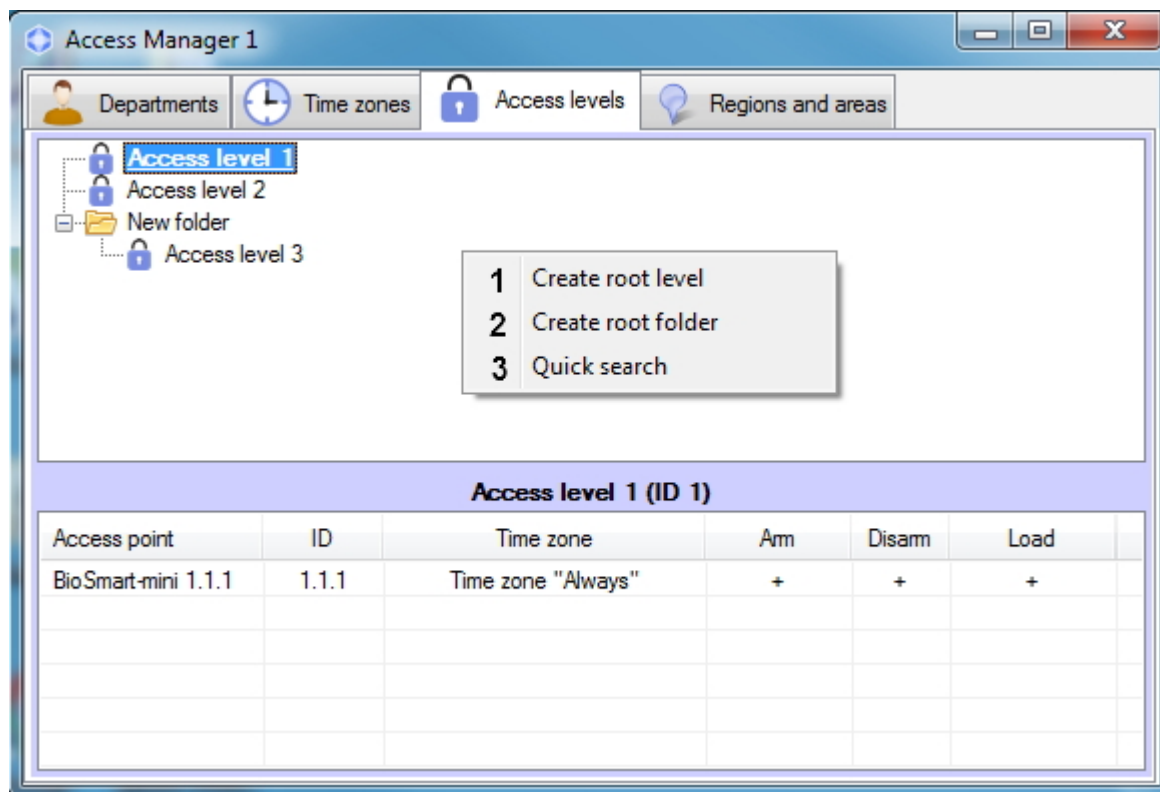
To sort search results click the left mouse button on title of corresponding column.

While double click on access level, the **Search access level** window will be closed and corresponding access level will be selected in the list in the **Access levels** tab or will be added to department or user.

Search for access level is completed.

Managing the list of access levels

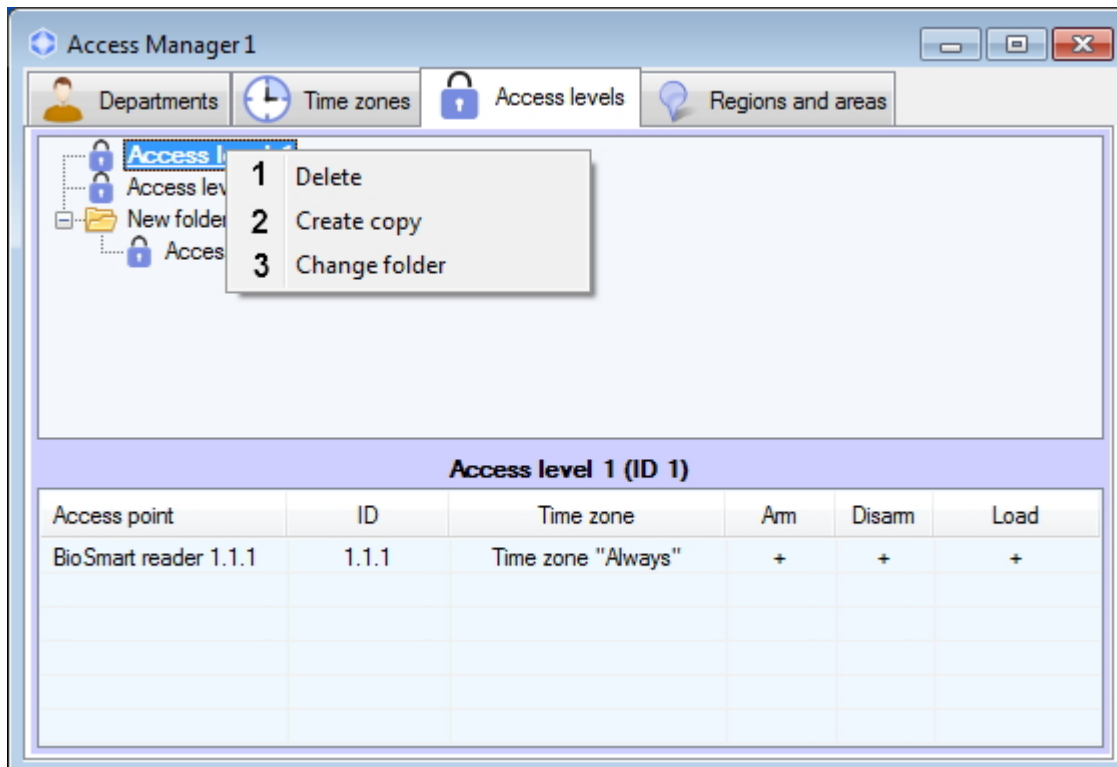
The list of access levels is managed using the context menu, invoked by clicking the right mouse button on the free space around the list.



The commands of the context menu are described in the table.

#	Command	Description
1	Create root level	Adds a new access level to the list of access levels. Clicking the menu item opens the Edit access level window. For more information on creating access levels, see Creation of an access level in the Access Manager software module .
2	Create root folder	Adds a new folder for organizing access levels in the list. Clicking the menu item opens the Folder settings window, which enables setting the name of the new folder.
3	Quick search	Opens the window for quick search of access levels in the list. Clicking the menu item opens the Quick Search window, which enables searching for access levels by different criteria. For more information on searching for access levels, see Search for access level .

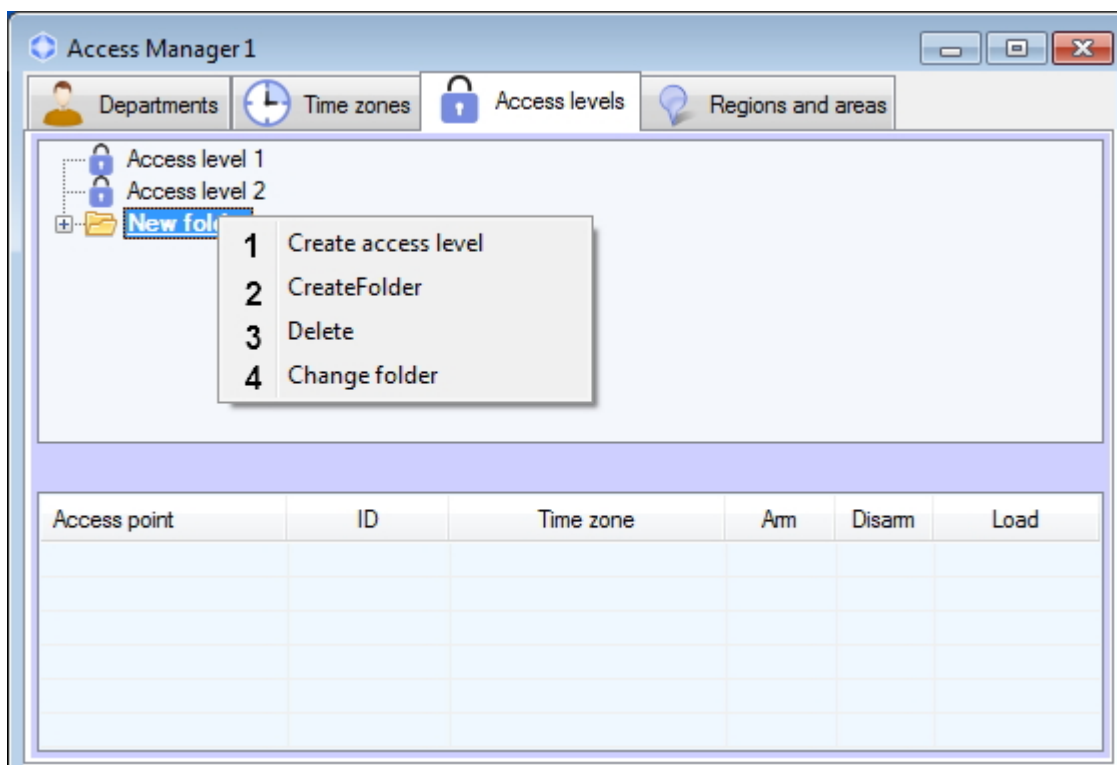
An individual access level in the root of the access level list is managed using the context menu, invoked by clicking the right mouse button on the item.



The commands of the context menu are described in the table.

#	Command	Description
1	Delete	Removes an item from the access level list after confirmation from the user.
2	Create copy	Creates a copy of the selected access level with all its settings. Clicking the menu item opens the Edit access level window, which enables editing the copy if required. For more information on editing access levels, see Editing an access level in the Access Manager software module .
3	Change folder	Moves the access level list item to the selected folder. When you select a command, the Folder search window with a tree of available folders opens.

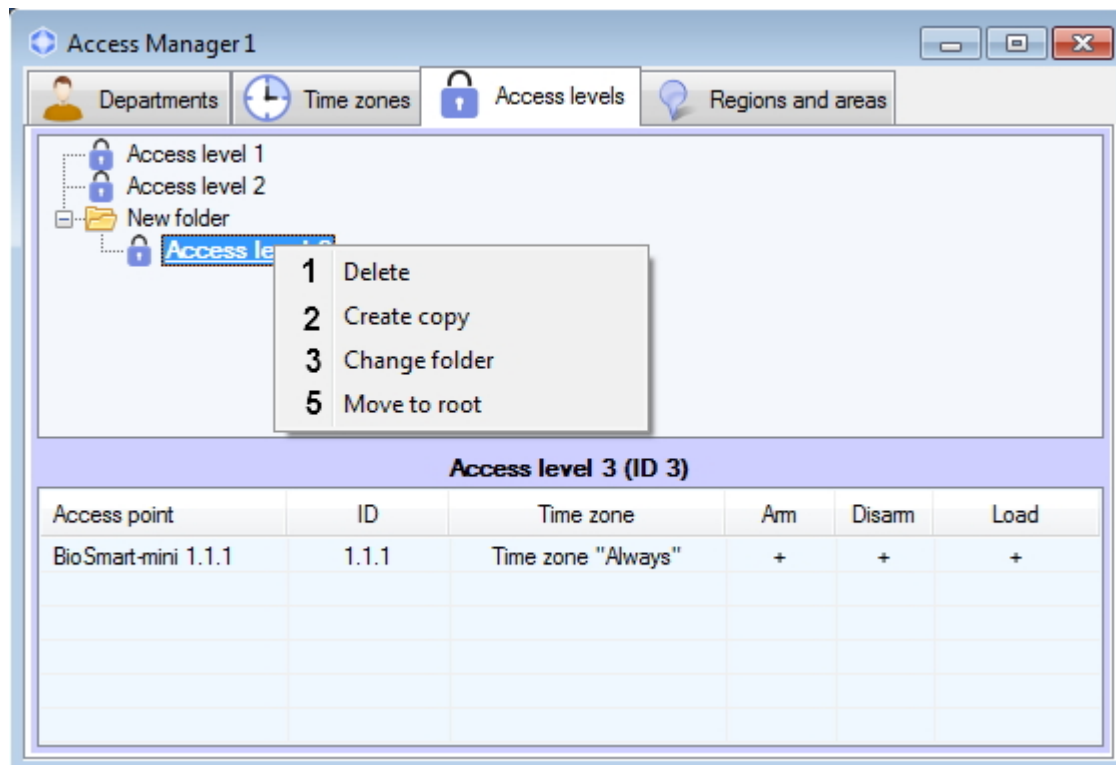
An individual folder in the access level list is managed using the context menu, invoked by clicking the right mouse button on the folder.



The commands of the context menu are described in the table.

#	Command	Description
1	Create access level	Adds a new access level to the folder. When you select a command, the Edit access level window opens. For more information on creating access levels, see Creation of an access level in the Access Manager software module .
2	Create folder	Adds a subfolder. When you select a command, the Folder settings window opens, which enables setting the name of the new folder.
3	Delete	Removes the folder and all its contents from the access level list after confirmation from the user.
4	Change folder	Moves the folder to the another folder. When you select a command, the Folder search window with a tree of available folders opens.

An individual access level within a folder is managed using the context menu, invoked by clicking the right mouse button on the access level.



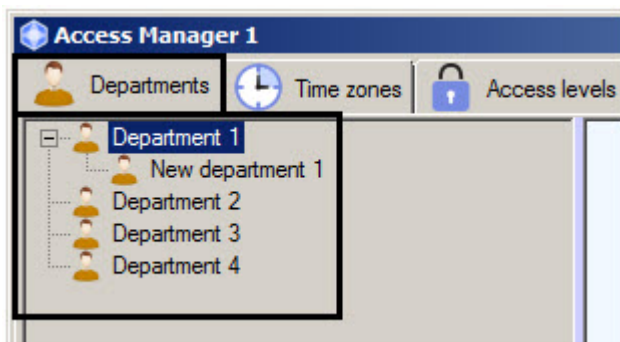
The commands of the context menu are described in the table.

#	Command	Description
1	Delete	Removes an access level from the access level list after confirmation from the user.
2	Create copy	Creates a copy of the selected access level with all its settings. Clicking the menu item opens the Edit access level window, which enables editing the copy if required. For more information on editing access levels, see Editing an access level in the Access Manager software module .
3	Change folder	Moves the access level list item to the selected folder. When you select a command, the Folder search window with a tree of available folders opens.
4	Move to root	Moves the selected access level from the folder back to the root of the access level list.

Working with departments in the Access Manager software module

General information about working with departments

Departments are organized in hierarchy structure in the *ACFA Intellect* software package. Tree of departments is displayed in the **Departments** tab of the **Access Manager** window.

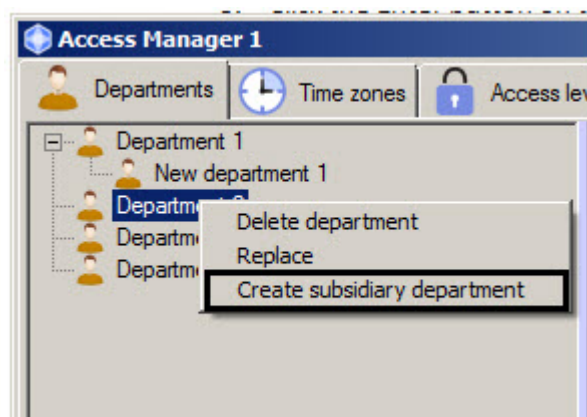
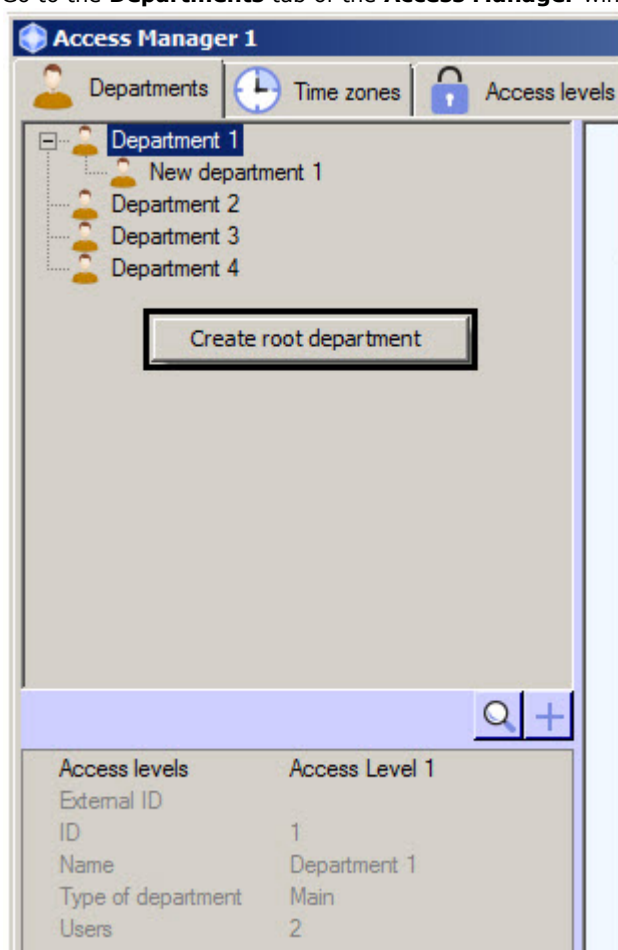


It's possible to create departments on the basis of some existed department and in the root of hierarchy. Functions of editing, deleting and viewing departments are available. Possibility of creating, editing and viewing departments can be limited while configuring the *Access Manager* software module – see the [Rights for configuring and viewing departments in the Access Manager](#) section.

Adding a department

To add department, do the following:

1. Go to the **Departments** tab of the **Access Manager** window.



2. To create department in the root of hierarchy click the right mouse button in free area of departments hierarchy and select the **Create root department** item in the opened functional menu.
To create department on the basis of existed department click the right mouse button on the required department and select the **Create subsidiary department** item.
3. The **Edit department properties** window will open.

4. Enter the department name in the **Name** field (1).



Note

Name of department should be unique. If department with such name is already exist, the corresponding message will be displayed while saving and department won't be saved.

5. In the **External ID** field enter external identical number of department (2). This field is in use if list of departments and users in the database of the *ACFA Intellect* software package is used with users database in external software due to features of used ACS integration module.
6. From the **Type of department** drop-down list select the department type (3). Types of departments are created while configuring the Access Manager software module - see the [Configuring a type of department in the Access Manager](#) section. Type of department specifies the list of visible and available for editing fields of user entering to this department. The **Main** type of department is the default type of department in the *Access Manager* module. All general user fields are visible and available for editing in this department type.
7. From the **Basic access level** drop-down list select department access level which be inherited on default by all users entering to this department (4).



Note

Use can not to inherit the department access level - see the [Configuring of department access level inheritance](#) section.



Note

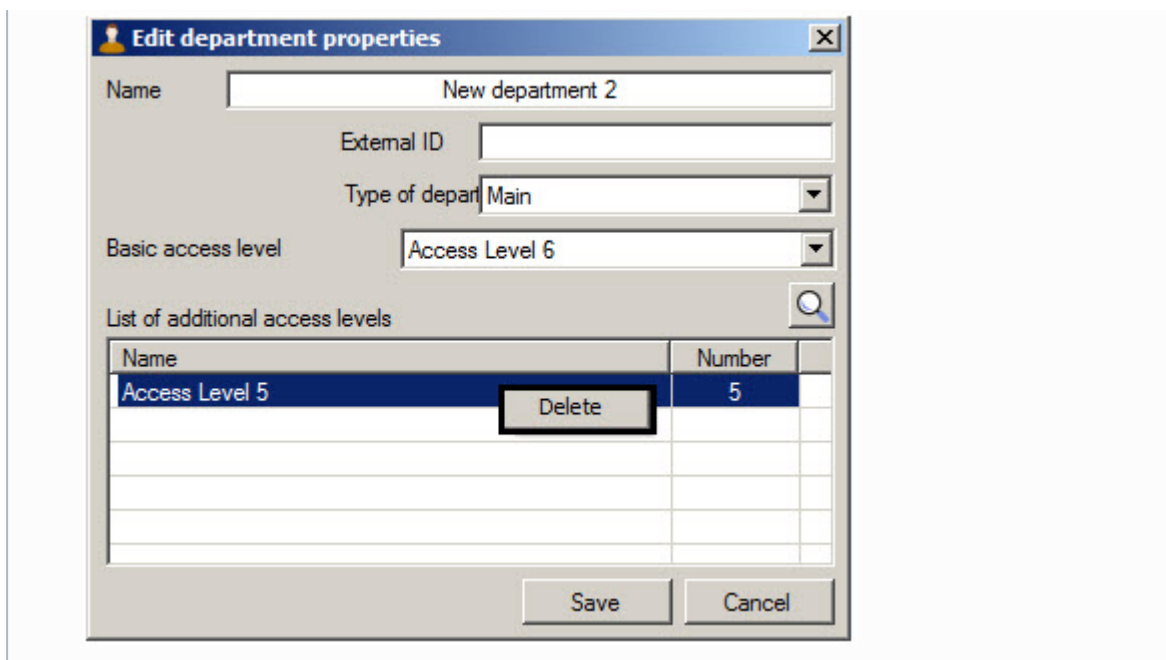
Access levels are created and configured on the **Access levels** tab of the **Access Manager** window (see the [Working with access levels in the Access manager software module](#) section). Also it's possible to use system access levels **Always** and **Never**.

8. If it's required, specify the list of additional access levels the following way:
 - a. Ensure that user access level is selected from the **Basic access level** drop-down list (i.e. not **Always** and not **Never**).
 - b. Click the **Add** button in the **List of additional access levels** table (5).
 - c. The **Search access level** window will be opened. To search for access level - see the Search for access level section.



Note

To delete the additional access level click it the right mouse button and select the **Delete** item in the opened functional menu.



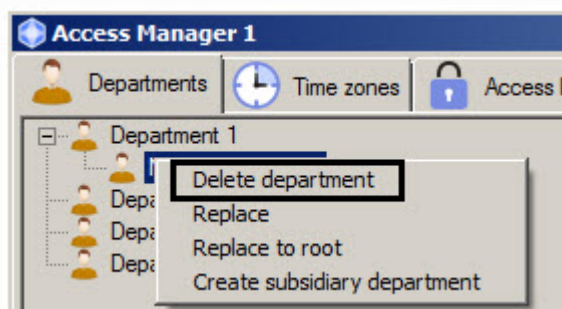
9. Click the **Save** button (5).

Department will be added to the tree.



Note

To delete department click it the right mouse button and select the **Delete department** item in the opened functional menu.



Creation of department is completed.

Editing a department

Editing a department involves changing of department parameters. To start editing a department double click the left mouse button on the name of department in a tree. The **Edit department properties** window will open. Working with this window is the same as while described in the [Adding a department](#) section.

Edit department properties

Name: Department 1

External ID:

Type of department: Main

Basic access level: Access Level 2

List of additional access levels

Name	Number
Access Level 5	5

Save Cancel

Department search in the Access Manager software module

Going to department search

In the *Access Manager* software module it's possible to search for departments by name, ID, external ID and access level.

To go to department search, do the following:

1. Go to the **Departments** tab of the **Access Manager** window (1).

Access Manager 1

Departments Time zones Access levels

Department 1
 New department 1
 Department 2
 Department 3
 Department 4

Access level: "Never"
 External ID: 5
 Name: New department 1
 Type of department: Main
 Users: 0

User card
 Access level
 Comment
 Basic Additional

2. Click the  button (2). The **Search for department** window will open.

Name	Number
Department 1	1
Department 2	2
Department 3	3
Department 4	4
New department 1	5

Going to department search is completed. Working with the Search for department is described in the [Working with Search for department window](#) section.

Working with Search for department window

Working with **Search for department** window is performed while searching for department (see the [Going to department search](#) section), replacing user from one department to another (see the [Transferring a user to a different department](#) section), and while creating departments hierarchy (see the [Creating departments hierarchy](#) section).

Working with the **Search for department** window is performed as follows:

1. Enter the complete or partial name of a department in the **Name** field if it's required (1).

2. Enter the department ID in the **ID** field if it's required (2).
3. Enter the external ID of an object in the **External ID** field if it's required (3).
4. From the **Access level** drop-down list select name of access level which is to be assigned to required department



- (4). If it's required click the button and search for access level (see the [Working with the Search access level window](#) section).
5. Click the Enter key.
6. Number of found departments will be displayed (5) and the list of departments satisfying to the specified search parameters (6). Search is case-insensitive. All objects corresponding fields of which contain specified values will be found.

To sort search results click the left mouse button on title of corresponding column.

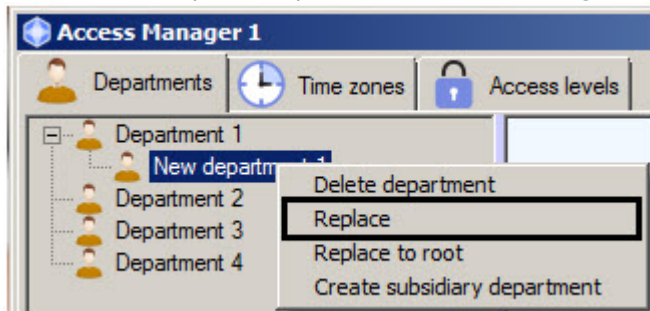
While double click on department name, the **Search for department** window will be closed and the department will be selected in the departments tree or in the form from which the **Search for department** window was opened.

Department search is completed.

Creating departments hierarchy

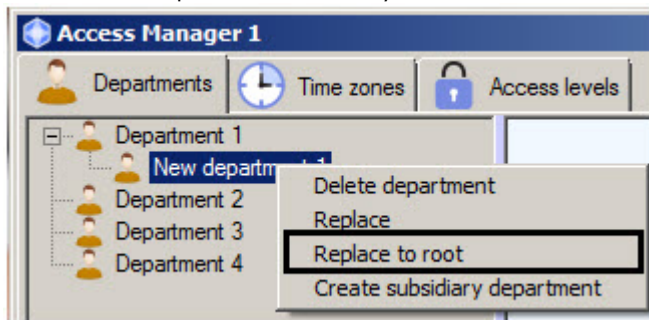
The departments hierarchy is created using the following operations:

1. Changing of parent department. Click the right mouse button on department name in the list of departments and select the **Replace** item in the opened functional menu. As a result the **Search for department** window will open to select the new parent department - see the [Working with Search for department window](#) section.



2. Replacing subsidiary department to the root of hierarchy. Click the right mouse button on department name in the list and select the **Replace to root** item in the opened functional menu. As a result the department will be places

to the root of departments hierarchy.



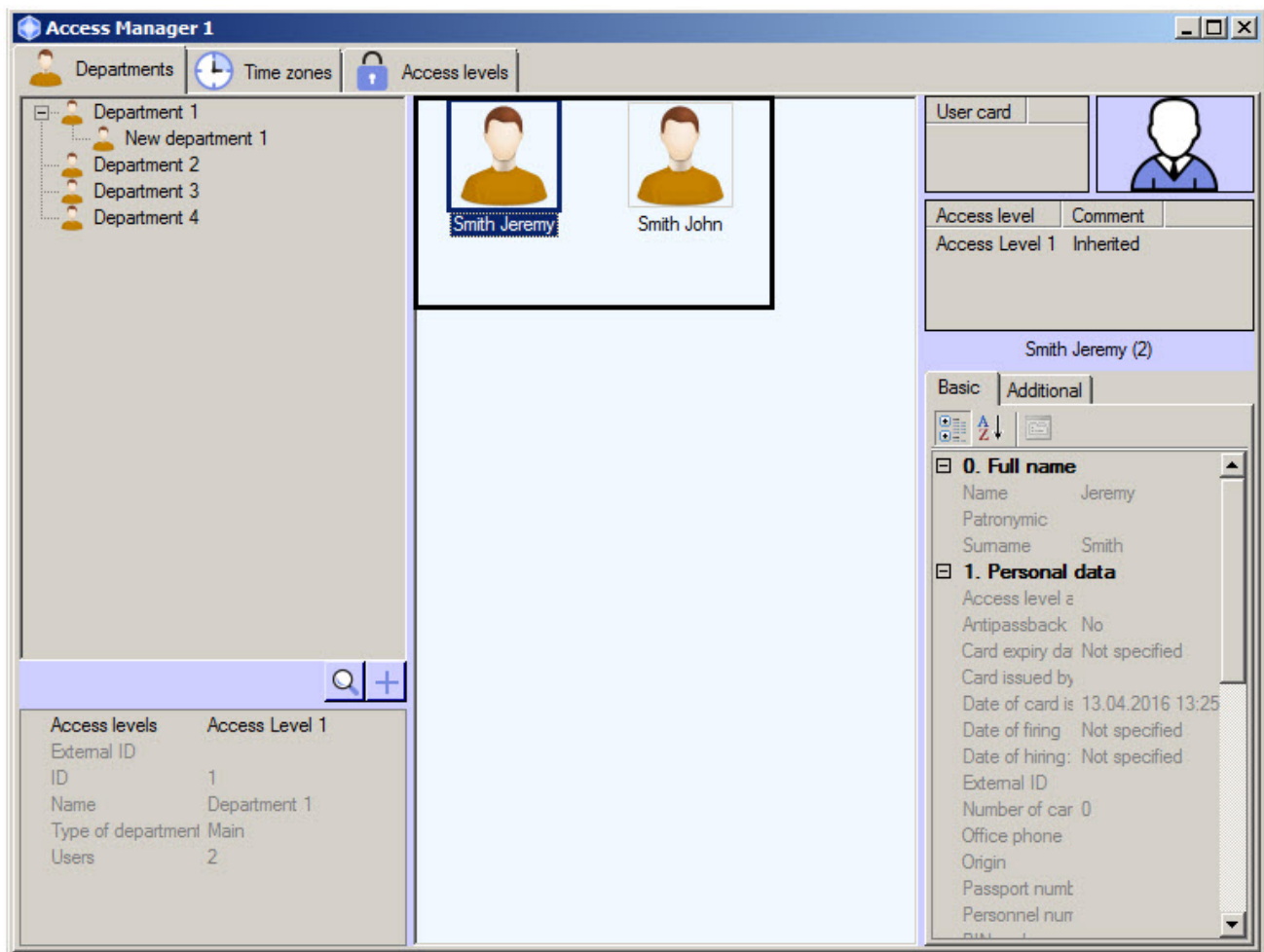
3. Change the department location by dragging it with the left mouse button holding the Ctrl key.

Note
Department replaces in hierarchy with its subsidiary departments.

Working with users in the Access Manager software module

Viewing a list of users

To view users select one of departments in the tree. A list of users included to this department will be displayed in the middle part of the **Access Manager** window.



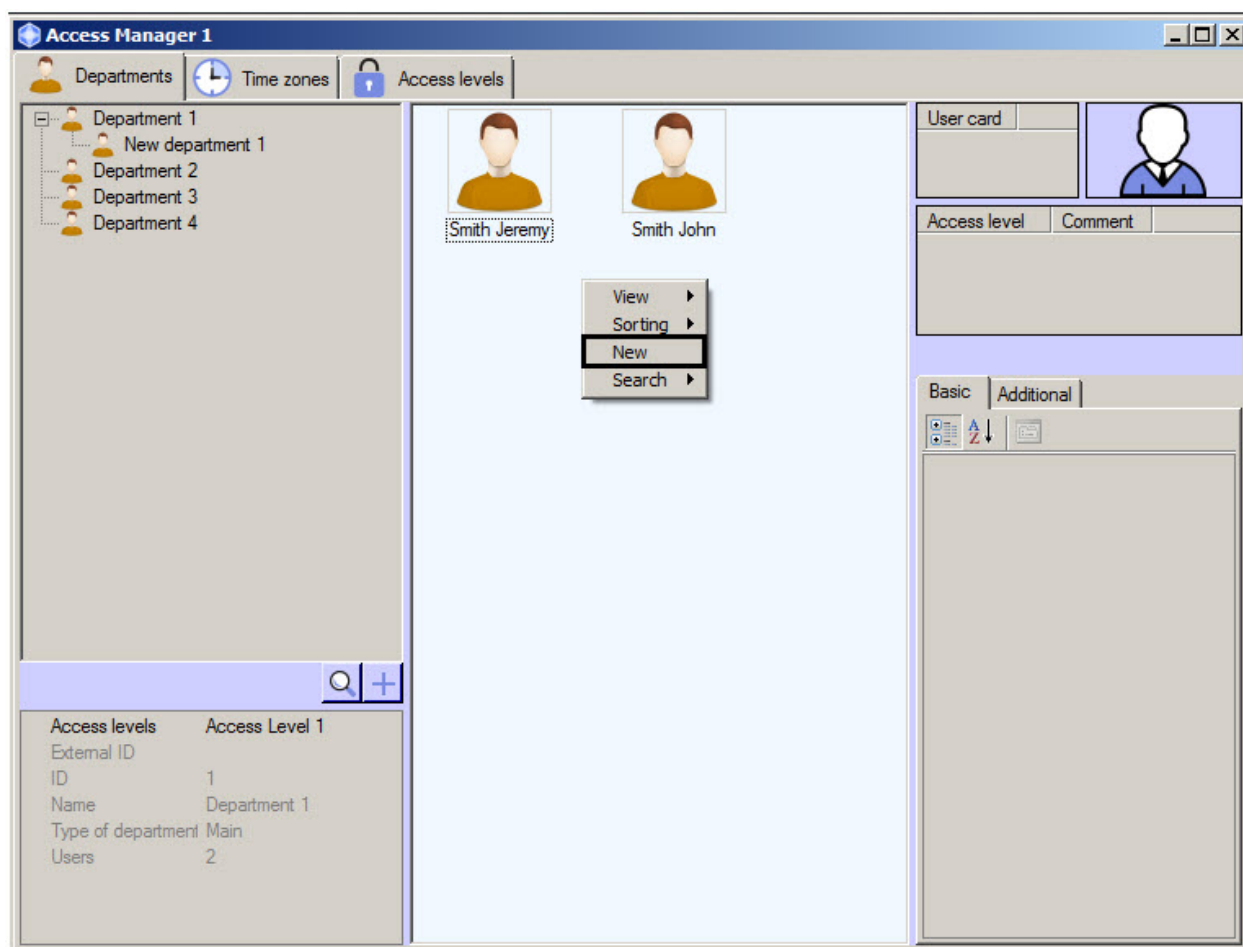
Properties of the selected user are displayed in the right part of the **Access Manager** window. On default the first user from the list will be selected while viewing the department.

Note
In case of large number of users in the department (more than 2000), displaying of users list can take for some time. Time of displaying a users list depends on computer capacity on which the **Access Manager** window is displaying.

Creating users in the Access Manager

To add a new user, do the following:

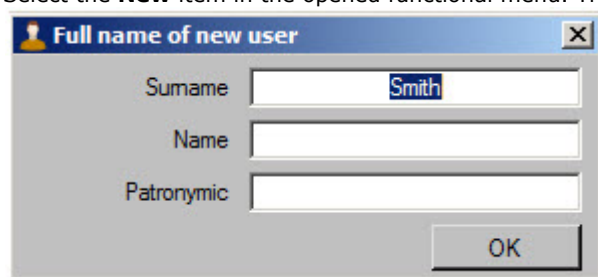
1. Open a list of user (see the [Viewing a list of users](#) section).
2. Click the right mouse button in free area of user list.



Note

Rights for users creating can be limited while configuring the *Access Manager* module. The message about missing of corresponding rights will display. See also the [Rights for users configuring in the Access Manager](#) section.

3. Select the **New** item in the opened functional menu. The **Full name of new user** window will open.

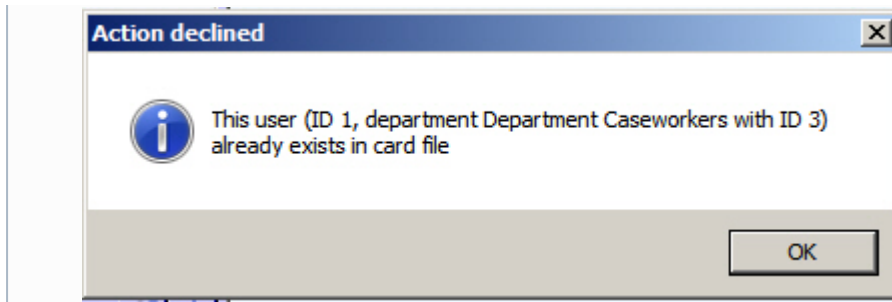


4. Enter surname, name and patronymic of creating user and click **OK** button.



Note

If criterion of records duplicate is in use and there is user with such name in the system, the error message with ID of existed user and department to which the user belongs will display. See also the [Configuring parameters of users creation in the Access Manager](#) section.



5. The **Editing. <User name> (creation)** window will display.

Further process of user creation is given in the [Editing a user](#) section.

Editing a user

Going to user editing

Going to user editing is performed while user creating (see the [Creating users in the Access Manager](#) section) or as follows:

1. Open list of users (see the [Viewing a list of users](#) section).
2. Double click the left mouse button on the required user. The **Editing. <User name> (ID)** window will open.

User card	Access level	Comment
	Access Level 1	Inherited

0. Full name

Name: Jeremy

Patronymic:

Surname: Smith

1. Personal data

Access level assigned by:

Antipassback: No

Card expiry date: Not specified

Card issued by:

Date of card issue: Cp, 13 anp 2016 13:25:11

Date of firing: Not specified

Date of hiring: Not specified

External ID:

Number of card loss: 0

Office phone:

Origin:

Passport number:

Personnel number:

PIN code:

Position:

Telephone:

Others

Ravelin Access type:

Ravelin guest card: No

Save Cancel

It's possible to do the following operations in this window:

- a. Setting user parameters
- b. Assigning access card to user
- c. Assigning access levels to user
- d. Assigning photo to user
- e. Adding biometric parameters (fingerprints)

All actions are described as follows.



Note

Rights for user editing can be limited while configuring the *Access Manager* module. The message about missing of corresponding rights will display after double click on the user name. See also the [Rights for users configuring in the Access Manager](#) section.

Fields available for editing including list of access levels and list of access cards are specified while configuring the *Access Manager* software module – see the [Configuring fields displaying in user accounts](#) section. Some fields can be hidden or not available for editing depending on settings.

Going to user editing is completed.

Setting user parameters

User parameters are specified in the **Editing. <User name> (ID)**.

Editing. Foreman Susan (3)

User card	Access level	Comment
	"Never"	Inherited

0. Full name

Name: Susan

Patronymic:

Surname: Foreman

1. Personal data

Access level assigned by:

Antipassback: No

Card expiry date: Not specified

Card issued by:

Date of card issue: Mon, 27 Jun 2016 14:01:06

Date of firing: Not specified

Date of hiring: Mon, 27 Jun 2016 14:01:06

External ID:

Number of card loss: 0

Office phone:

Origin:

Passport number:

Personnel number:

PIN code:

Position:

Telephone:

Save Cancel

There are following general user parameters in the *ACFA Intellect* software package.

Note

Note
Availability of some additional parameters depends on used integration module.

Parameter name	Parameter setting method	Default category in templates	Value range	Comment
Surname	Enter the value in the field	0. Full name	All symbols	-
Name	Enter the value in the field	0. Full name	All symbols	-
Patronymic	Enter the value in the field	0. Full name	All symbols	-
Personnel number	Enter the value in the field	1. Personal data	All symbols	-
External ID	Enter the value in the field	1. Personal data	All symbols	This field is in use if list of departments and users in the database of the <i>ACFA Intellect</i> software package is used with users database in external software due to features of used ACS integration module.
Position	Enter the value in the field	1. Personal data	All symbols	-

Date of hiring	Enter the value in the field manually or using the calendar	1. Personal data	Date in Weekday, DD mmm YYYY HH:MM:SS format	-
Date of firing	Enter the value in the field manually or using the calendar	1. Personal data	Date in Weekday, DD mmm YYYY HH:MM:SS format	-
Temporary AL activation date	Enter the value in the field manually or using the calendar	1. Personal data	Date in Weekday, DD mmm YYYY HH:MM:SS format	To use temporary access levels the Support temporary access levels object is required. This object is created on the basis of the Computer object on the Hardware tab of the System settings window
Temporary AL expiry date	Enter the value in the field manually or using the calendar	1. Personal data	Date in Weekday, DD mmm YYYY HH:MM:SS format	
Date of card issue	Enter the value in the field manually or using the calendar	1. Personal data	Date in Weekday, DD mmm YYYY HH:MM:SS format	-
Card expiry date	Enter the value in the field manually or using the calendar	1. Personal data	Date in Weekday, DD mmm YYYY HH:MM:SS format	-
Date of card issue	Enter the value in the field manually or using the calendar	1. Personal data	Date in Weekday, DD mmm YYYY HH:MM:SS format	-
Number of card loss	Enter the value in the field	1. Personal data	Numbers	-
PIN code	Enter the value in the field	1. Personal data	Numbers	-
Antipassback	Select the value from the list	1. Personal data	Yes No	Default value depends on configuring the Access Manager module – see the Configuring parameters of users creation in the Access Manager section.
User locked	Select the value from the list	1. Personal data	Yes No	Yes – user locked. Нет – user is active.
Additional information	Enter the value in the field	1. Personal data	All symbols	Enter additional information in text field opening by clicking the "down" button in the Additional information field
Driving license	Enter the value in the field	3. Vehicle	All symbols	Number of user driving license
Vehicle model	Enter the value in the field	3. Vehicle	All symbols	Model of user vehicle
Vehicle LP	Enter the value in the field	3. Vehicle	All symbols	License plate of user vehicle
Telephone	Enter the value in the field	1. Personal data	All symbols	Telephone number
Office phone	Enter the value in the field	1. Personal data	All symbols	Office phone number
E-mail address	Enter the value in the field	1. Personal data	All symbols	User e-mail address
Passport number	Enter the value in the field	1. Personal data	All symbols	Passport number of user

For visitor: from where	Enter the value in the field	4. Visitor data	All symbols	Name of organization to which the visitor belongs
For visitor: to which department	Enter the value in the field	4. Visitor data	All symbols	Department being visited
For visitor: to whom	Enter the value in the field	4. Visitor data	All symbols	Employee being visited
For visitor: purpose of visit	Enter the value in the field	4. Visitor data	All symbols	Purpose of visitor visit
For visitor: document	Enter the value in the field	4. Visitor data	All symbols	Present document of visitor identification
For visitor: registration address	Enter the value in the field	4. Visitor data	All symbols	Address of visitor registration according to place of residence
For visitor: birth place	Enter the value in the field	4. Visitor data	All symbols	Place of visitor birth
Card issued by	Automatically	1. Personal data	Operator name	Name of operator who last assigned access card to user or visitor (see the Assigning an access card to a user section)
Access level assigned by	Automatically	1. Personal data	Operator name	Name of operator who last assigned access level to user or visitor (see the Assigning access levels to a user section)

Assigning an access card to a user

General information about assigning access cards to a user

List of user access cards is displayed in the **User card** table of the **Editing. <Full name> (ID) window**.

Editing. Foreman Susan (3)

User card	Access level	Comment
(123) 7890	"Never"	Inherited

0. Full name

Name	Susan
Patronymic	
Surname	Foreman

1. Personal data

Access level assigned by	
Antipassback	No
Card expiry date	Not specified
Card issued by	Admin 1
Date of card issue	Mon, 27 Jun 2016 14:01:06
Date of firing	Not specified
Date of hiring	Mon, 27 Jun 2016 14:01:06
External ID	
Number of card loss	0
Office phone	
Origin	
Passport number	
Personnel number	
PIN code	
Position	
Telephone	

Save Cancel

The object code is specified in brackets, then the card code follows.

It is possible to assign several access cards to a user.



Attention!

Assigning several access cards to a user should be supported by hardware. If used hardware supports only one card and several cards are assigned to a user, then all cards excepting the first card will be ignored by system.

Input of card number and code while assigning access cards to a user can be performed in one of the following ways:

1. Manually.
2. Using the control reader.



Note

List of control readers used for user access cards input is specified while system configuring - see the [Selecting control readers in the Access Manager](#) section.

Input of access card number manually

To input access card number manually, do the following:

1. Go to editing a user (see the [Going to user editing](#) section).
2. Click the right mouse button in card selection area.
3. Select the **Add** item in the opened functional menu.

4. The window of input object code and card code will open.

5. Enter the object code (facility-code, room code) in the **Room code** field (1).
6. Enter the card code in the **Card number** field (2).
7. Click the **OK button** (3).

8. The card will be added to the list.



Note

To delete a card number from the list click the right mouse button on the card number and select the **Delete** item in the opened functional menu.

User card	Access level
(123) 958649	Access Level 1
(978) 1640	

Input of access card number manually is completed.

Input of card number using a control reader

To input access card number using a control reader, do the following:

1. Go to editing a user (see the [Going to user editing](#) section).
2. Click the right mouse button in card selection area.
3. Select the **From reader** item in the opened functional menu.

User card	Access
(123) 958649	Access

4. The **Access card reading** window will open.

1 Reader type Gate Parking access point 1

2 Start reading

Start reading or select another control reader

5. From the **Reader type** drop-down list select a control reader which will be used for input of access card number (1).



Note

List of accessible control readers is specified while system configuring (see the [Selecting control readers in the Access Manager](#) section).

6. Click the **Start reading** button (2). The **Access card reading** window will be as follows:

Reader type Gate Parking access point 1

Cancel reading

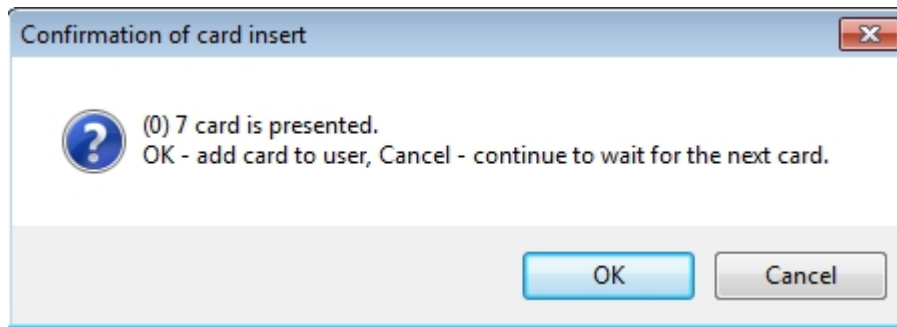
Present card to the selected control reader...



Note

To cancel access card reading click the **Cancel reading** button.

7. Present access card to the selected reader.
8. If confirmation of card input by operator is configured, the Confirmation of card input window will display. To assign presented card to a user click **OK**, to come back to step 12 click **Cancel**. See also the [Selecting control readers in the Access Manager](#) section.



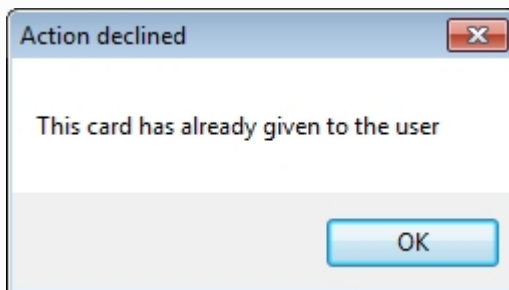
9. Then the **Access card reading** window will be closed and number of presented access card will be added to the list.

User card
(123) 958649
(13) 14572



Note

If this card is already given to the current or another user, the corresponding window will display.



Note

To delete a card number from the list click the right mouse button on the card number and select the **Delete** item in the opened functional menu.

Input of access card using a control reader is completed.

Assigning access levels to a user

General information about assigning access level to a user

List of access levels is displayed in the table of the **Editing. <User full name> (ID)** window.

User card	Access level	Comment
	Access level 2	Own
	Access level 1	Inherited

0. Full name	
Name	Anna
Patronymic	
Surname	Smith

1. Personal data	
Access level assigned by	Admin 1
Antipassback	No
Card expiry date	Not specified
Card issued by	
Date of card issue	Not specified
Date of firing	Not specified
Date of hiring:	Not specified
External ID	
Number of card loss	0
Office phone	
Origin	
Passport number	
Personnel number	
PIN code	
Position	
Telephone	

In the **Comment** column it's specified whether access level is inherited by Department (**Inherited**), temporary (**Temporary**) or assigned to a user separately (**Own**). Configuring rules of department access level inheritance is described in the [Configuring of department access level inheritance](#) section. Adding of own access levels to a user is described in the [Assigning own access level to a user](#) section. Assigning temporary access levels is described in the [Assigning temporary access level to a user](#) section.

Assigning own access level to a user

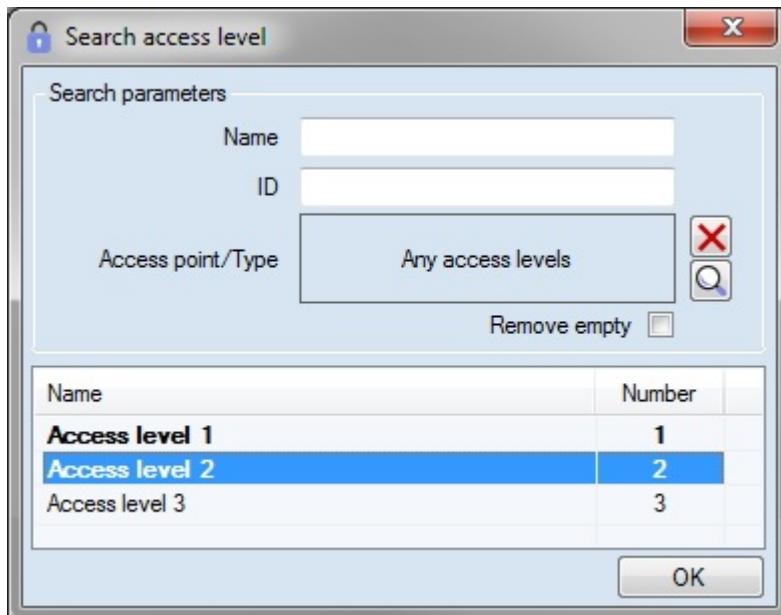
Assigning own access level is performed as follows:

- Go to editing a user (see the [Going to user editing](#) section).
- Click the right mouse button in the access levels list.

User card	Access level	Comment
(-) 0000001	"Always"	Inherited

0. Full name	
--------------	--

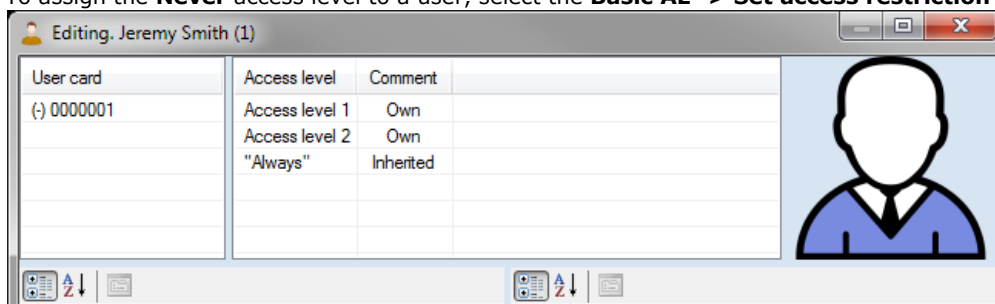
- To assign user access level select the **Basic AL -> Add** item in the opened functional menu (1). The window of access level searching will open. Search for access levels required access level (see the [Search for access level](#) section) and select any number of access levels by double-clicking them (selected levels will be highlighted in bold):



Note

If **Always** or **Never** own access levels are assigned to a user, then no other access level can be assigned.

1. To assign the **Always** access level to a user, select the **Basic AL -> Set full access** (2).
2. To assign the **Never** access level to a user, select the **Basic AL -> Set access restriction** (3).

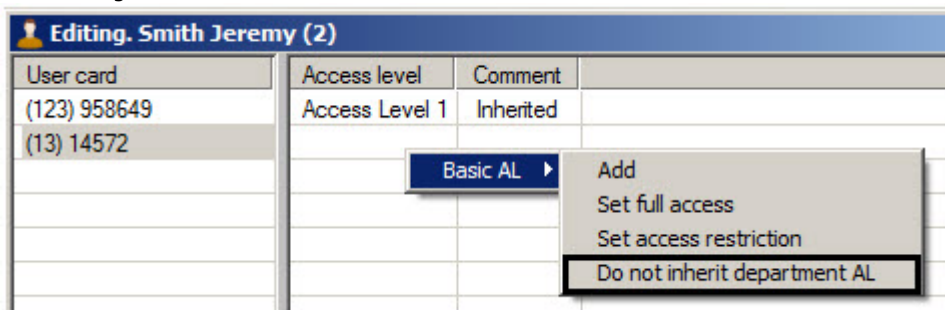


Assigning own access level to a user is completed.

Configuring of department access level inheritance

User can inherit department access level on default. If it's required not to inherit department access level (levels), do the following:

1. Go to editing a user (see the [Going to user editing](#) section).
2. Click the right mouse button in the access levels list.



3. Select the **Basic AL -> Do not inherit department AL** in the opened functional menu.



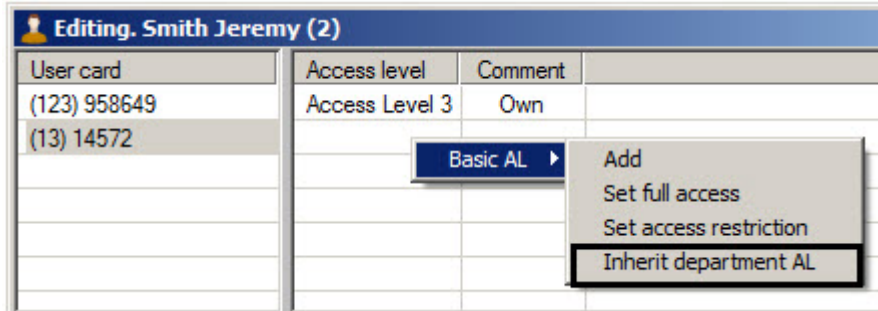
Note

It's impossible to delete inherited access level if a user haven't got own access levels. In this case it's required to assign own access level to a user and then disable inheritance of department access level – see the [Assigning own access level to a user](#) section.

As a result the inherited access level (levels) will be deleted from the list.

To restore inheritance of department access levels, do the following::

1. Click the right mouse button in access levels list.
2. Select the **Basic AL -> Inherit department AL** in the opened functional menu.



As a result the inherited access level (levels) will be added to the list.

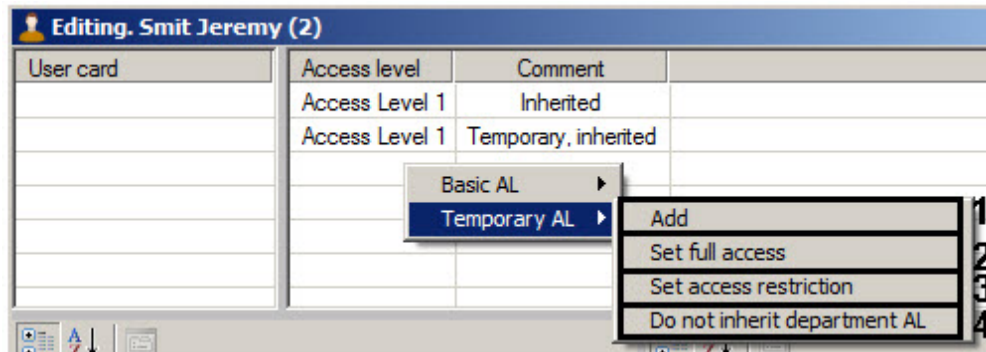
Configuring of department access level inheritance is completed.

Assigning temporary access level to a user

If the **Support of temporary access levels** object is created, start time of temporary access level and end time of temporary access levels are specified, it's possible to assign temporary access levels to a user

To assign temporary access level to a user, do the following:

1. Go to editing a user (see the [Going to user editing](#) section).
2. Click the right mouse button in the access levels list.



3. To assign user access level, select the **Temporary AL -> Add** in the opened functional menu (1).
4. The window of access level searching will open. Search for access levels and select the required access level (see the [Search for access level](#) section).



Note

If **Always** or **Never** own access levels are assigned to a user, then user access level can't be assigned.

5. To assign the **Always** access level to a user, select the **Temporary AL -> Set full access** (2).
6. To assign the **Never** access level to a user, select the **Temporary AL -> Set access restriction** (3).
7. Assigning own access level to a user is completed.
8. To disable inheritance of department temporary access level, select the **Temporary AL -> Do not inherit department AL** (4). See the [Configuring of department access level inheritance](#) section.

Assigning temporary access level to a user is completed.

Assigning a photograph to a user in the Access Manager software module

General information about assigning a photograph to a user

Assigning a photograph to a user is performed in the **Editing. <User full name> (ID)** window in one of the following ways:

1. From a file.
2. From a video camera.



Note

List of video cameras used for assigning photograph to users is specified while system configuring (see the [Selecting available cameras in the Access Manager](#) section).

Editing. Foreman Susan (3)

User card	Access level	Comment
	Access level 1	Inherited



0. Full name

Name: Susan

Patronymic:

Surname: Foreman

1. Personal data

Access level assigned by:

Antipassback: No

Card expiry date: Not specified

Card issued by:

Date of card issue: Mon, 27 Jun 2016 14:01:06

Date of firing: Not specified

Date of hiring: Mon, 27 Jun 2016 14:01:06

External ID:

Number of card loss: 0

Office phone:

Origin:

Passport number:

Personnel number:

PIN code:

Position:

Telephone:

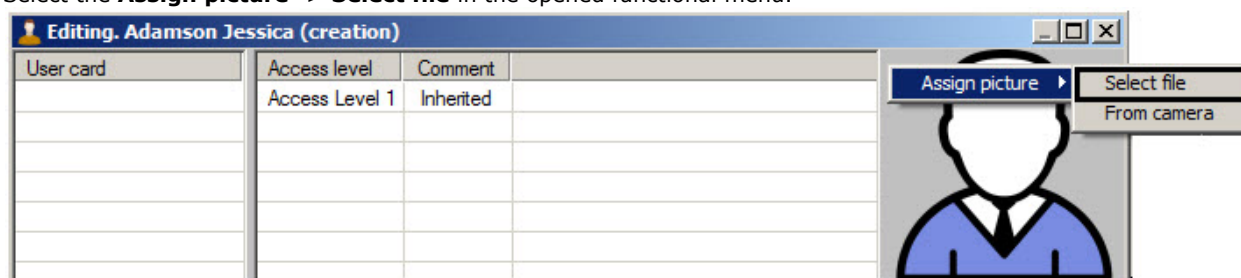
Save Cancel

Assigned photographs are storing in the <ACFA-Intellect installation directory>/Bmp/Person folder. Name of file with the user's photograph is the same as the user ID. Content of the Bmp/Person folder is synchronized on all servers of distributed system.

Assigning photograph from a file

To assign photograph from a file, do the following:

1. Go to editing a user (see the [Going to user editing](#) section).
2. Click the right mouse button in user photo area.
3. Select the **Assign picture -> Select file** in the opened functional menu.



4. The standard dialog window will be opened. Select the file with photograph.

Opened photograph will be assigned to the user.

Assigning photograph from a file is completed.

Assigning photograph from a video camera

To assign photograph from a video camera, do the following:

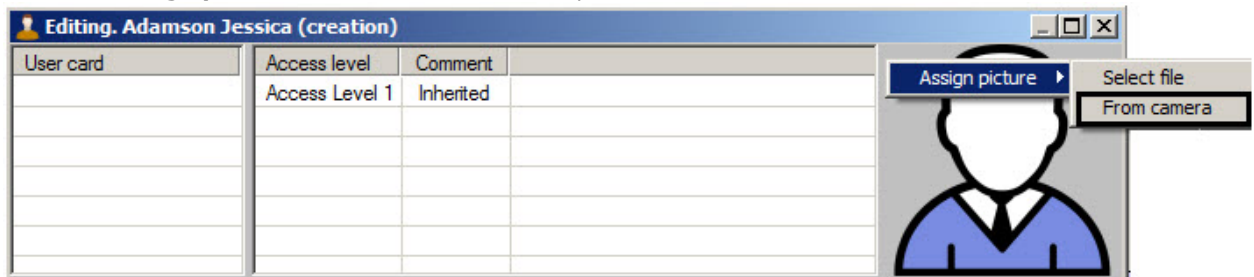


Note

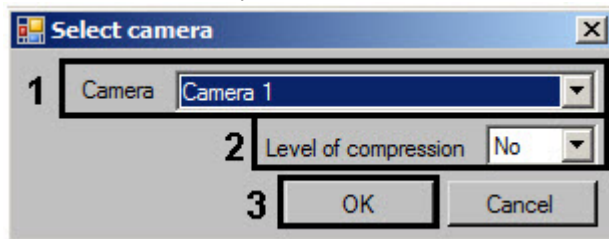
List of video camera used for assigning photographs is specified while system configuring (see the [Selecting available cameras in the Access Manager](#) section).

1. Go to editing a user (see the [Going to user editing](#) section).

2. Click the right mouse button in user photo area.
3. Select the **Assign picture -> From camera** in the opened functional menu.



4. The **Select camera** window will open.
5. From the **Camera** drop-down list select the camera from which photograph will be captured (1).



6. If it's required to change the level of video signal compression used for assigning a photograph, select from the **Level of compression** drop-down list the required level of video signal compression (2). Compression level is increasing from 0 (without compression) to 5 (maximum compression).



Note

Configuring of compression is required while using analog cameras. It's not recommended to use compression for IP-cameras.

7. Click **OK** button (3). The **Photo from camera** window will open.



8. Video from the selected video camera is displayed in the window (1).
9. If it's required selected the way of frame processing from the **Rotate and/or inverse** drop-down list (2). the following ways of frame processing are available:
 - a. Do not change (on default).
 - b. Rotate 90.
 - c. Rotate 180.
 - d. Rotate 270.
 - e. Inverse horizontally.
 - f. Rotate 90 and inverse horizontally.
 - g. Inverse vertically.
 - h. Rotate 90 and inverse vertically.
10. The frame is saving without information about camera number, time of frame receiving, without information about camera arming or disarming (it is defined by color of the frame around camera). If it's required to add this

information to the captured frame with the user image, set the **Show camera number, time of frame and security state** checkbox (3).



Note

It's recommended to configure rotation and add information to the frame before the image capturing. Changing of these settings after capturing won't lead to their disappearing from the captured frame.

11. Wait for appropriate frame with the user image and click the **Capture** button (4).
12. The received frame will display in the (5) window.
13. Click the **OK** button (6). The received frame will be assigned as the user photograph.

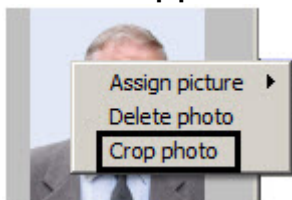
Assigning a photograph to user from a video camera is completed.

Cropping a photograph

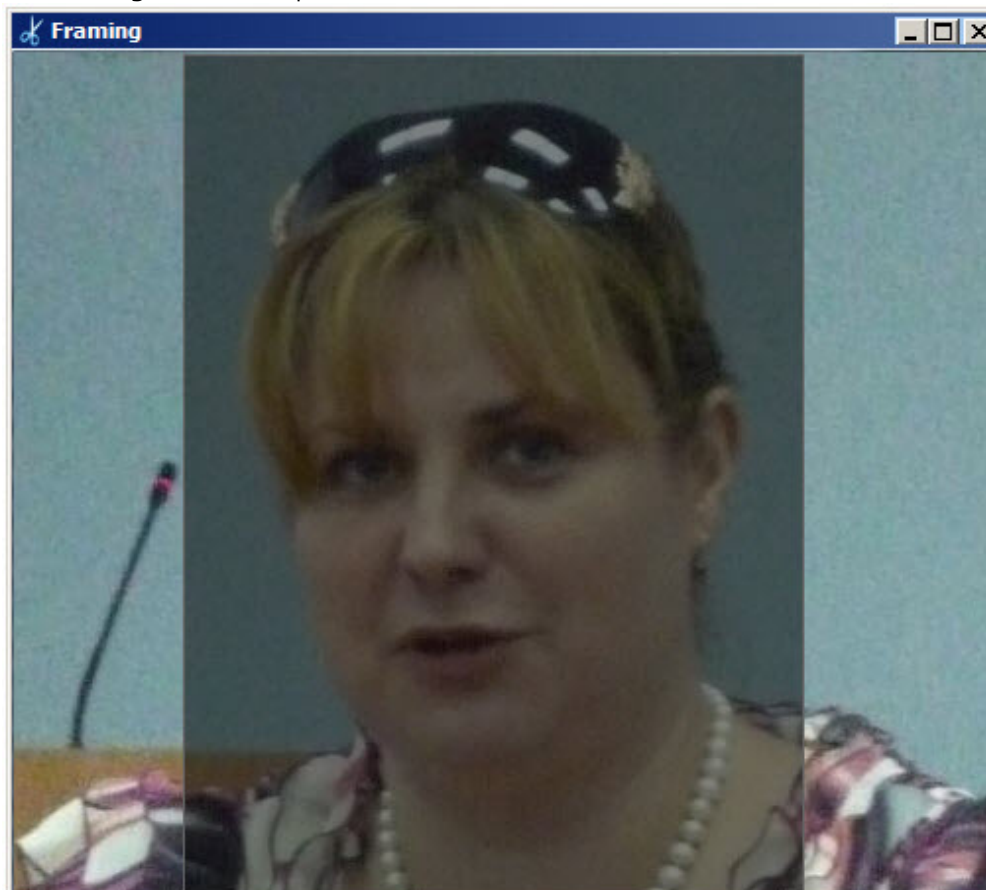
It's possible to crop the assigned photograph in the Access Manager software module.

To crop a photograph, do the following:

1. Go to editing a user (see the [Going to user editing](#) section).
2. Click the right mouse button on a photograph assigned to a user.
3. Select the **Crop photo** in the opened functional menu.



4. The **Framing** window will open.



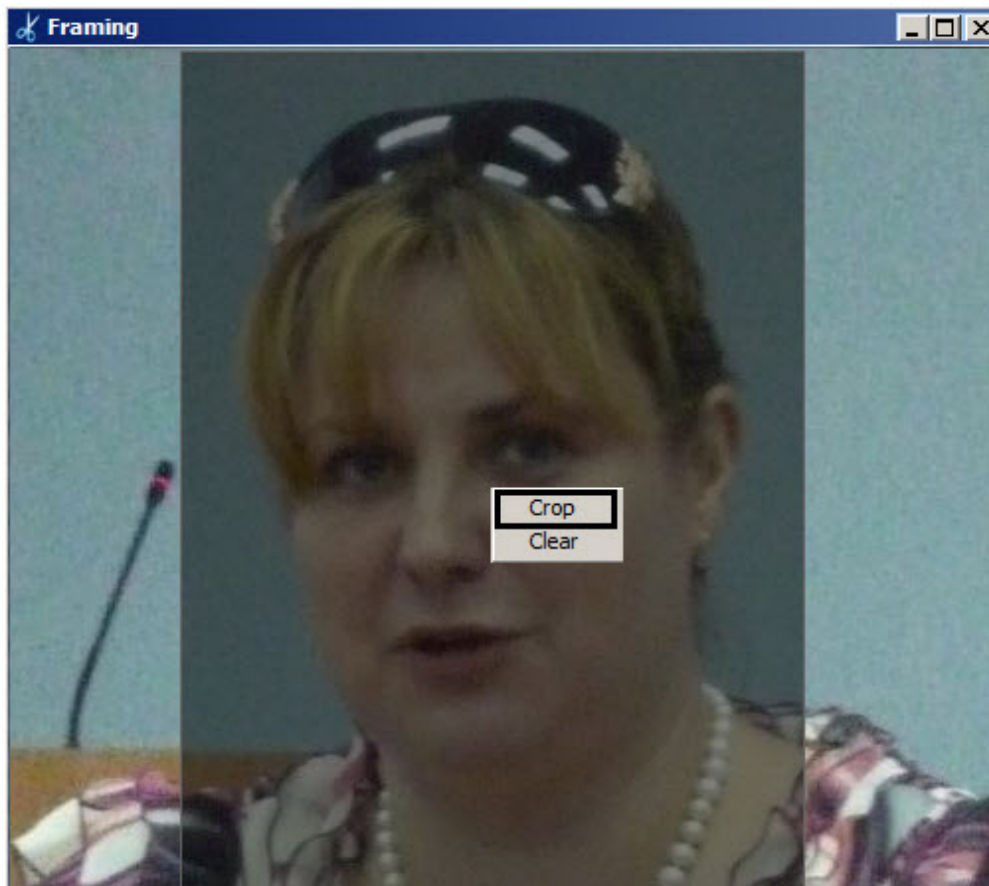
5. To select the area which should stay in the photo click the left mouse button in the required point and stretch the rectangle marking the selected area.



Note

To change the selected area click the left mouse button in the area marked by a rectangle and select the area again.

6. To delete selection click the right mouse button on the selected area and select the **Clear** item.
7. Click the right mouse button on the selected area and select the **Crop** item.



Cropping a photograph is completed.

Deleting a photograph

To delete a photograph, do the following:

1. Go to editing a user (see the [Going to user editing](#) section).
2. Click the right mouse button on a photograph assigned to a user.
3. Select the **Delete photo** in the opened functional menu.

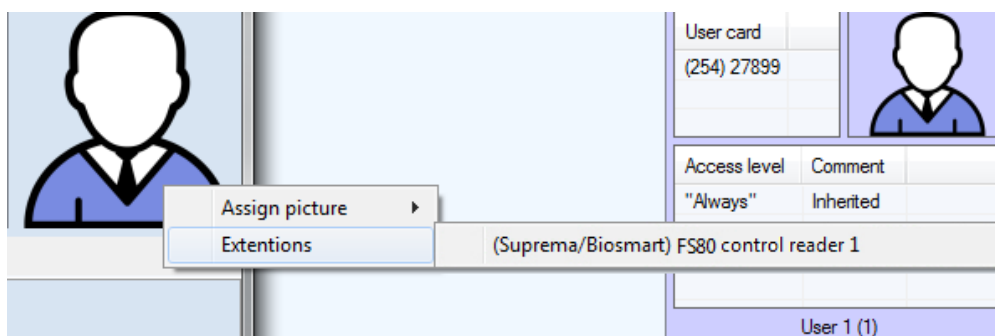


Deleting a photograph is completed.

Adding biometric parameters

Adding biometric parameters (fingerprints, palm vein patterns, etc.) is performed using control readers or biometric ACS controllers.

To add a user's fingerprints, right-click the user's photo and select **Extensions** -> **Reader**.



A dialog box for adding user biometric parameters opens. This dialog box is different for various equipment in use.

Operation in this dialog box is described in the corresponding integration module settings guide.



Note.

Select a required reader or controller while configuring *Access Manager* to make it available in the **Extensions** list – see [Selecting control readers in the Access Manager](#).

Transferring a user to a different department in the Access Manager software module

To transfer a user to a different department, do the following:

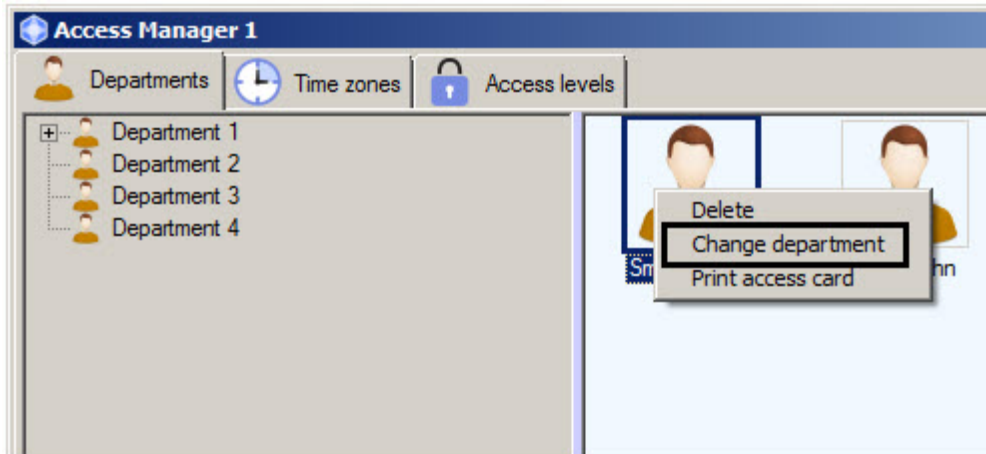
1. Go to viewing users list (see the [Viewing a list of users](#) section).
2. Click the right mouse button on the name of required user.



Note

To select several users to transfer them to a different department click them the left mouse button holding the Ctrl key.

3. Select the **Change department** item in the opened functional menu.



4. As a result the Search for department window will open. After searching select the department to which user is to be transferred (see the [Working with Search for department window](#) section).
5. As a result the user will be transferred to the selected department.

Transferring a user to a different department is completed.

User search in the Access Manager software module

General information about user search

Searching for users is performed in one of the following ways in the *Access Manager* software module:

1. By ID.
2. By surname.
3. By card.
4. By card using a control reader.
5. By access level.
6. General search.

Going to user search

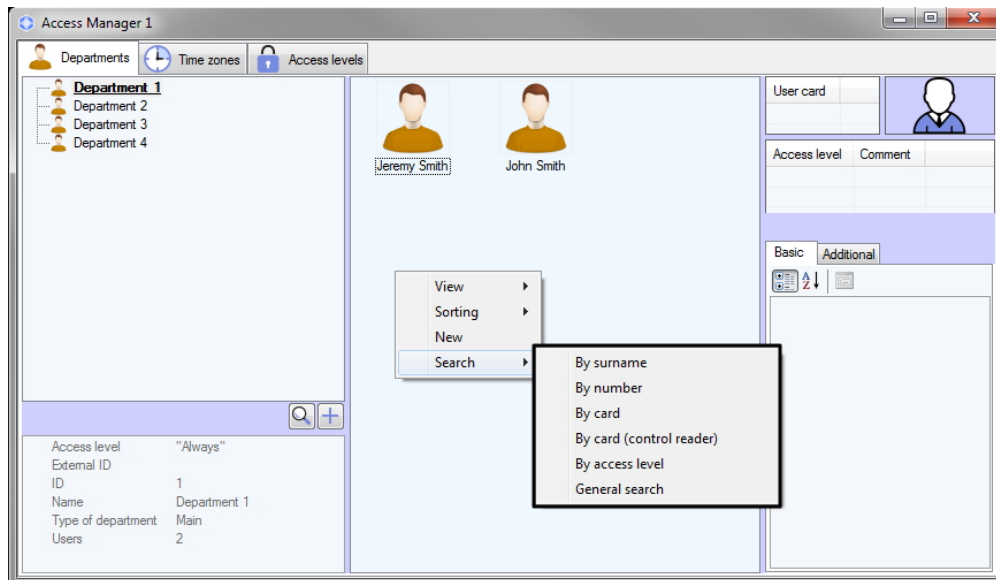
To go to user search, do the following:



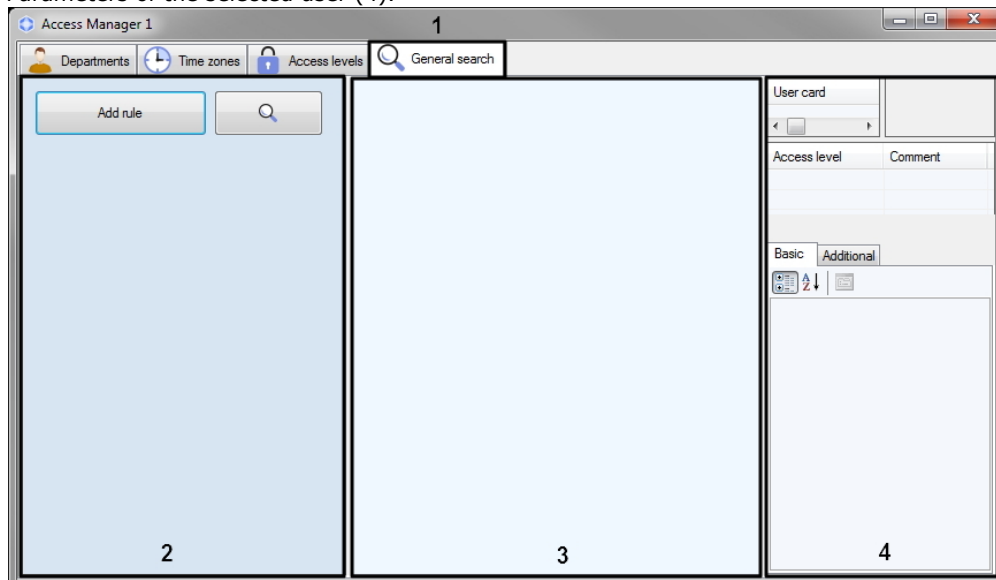
Note

Also going to user search is performed by Ctrl+F keys combination - see the [Key combinations for working with objects lists](#) section. While going to user search using the key combination, the **Search in department** tab will open where the search condition by the department will be specified.

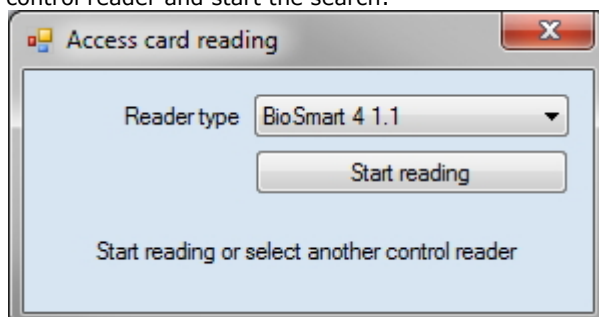
1. Go to viewing users list (see the [Viewing a list of users](#) section).
2. Click the right mouse button in free area of users list.
3. Select the **Search** item in the opened functional menu. In the opened functional menu select the required way of search - see the [General information about user search](#) section.



4. The new tab will be opened for search (1). Name of the tab depends on the selected way of search. The tab contains the following interface elements:
- List of search rules (2).
 - List of found users (3).
 - Parameters of the selected user (4).



- In case the search is performed by number, surname, card or access level, the corresponding rule will be specified in the list of rules. It's possible to add search rules to the list if it's required (see the [Adding a search rule](#) section).
- In case the search is performed by card using a control reader, a window will open, offering to select the control reader and start the search:



In the opened window, click **Start reading** and present the card to the selected reader device.

Going to user search is completed.

Adding a search rule

While searching for objects in the *Access Manager* module the following logic operators are available:

- Logic AND.
- Logic OR.

Search rules will be combined on the following way:

(Rule11 OR Rule12 OR ... OR Rule 1N) AND
(Rule21 OR Rule22 OR ...Rule 2M) AND
...
(Rule K1 OR Rule K2 OR ... OR Rule KL)

Where N, M, K, L –some integer number.

Search rules combined by OR operator are displaying in one string. Search rules combined by AND operator are displaying one over the other.

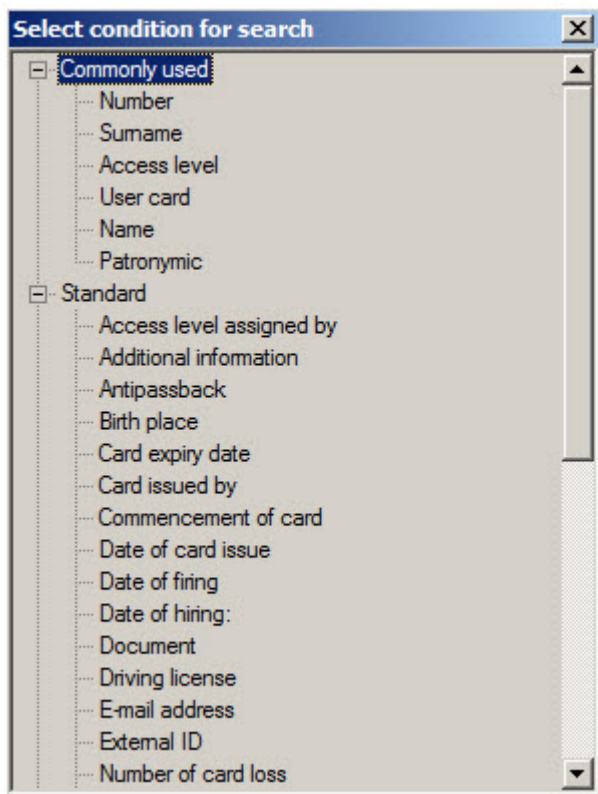
The screenshot shows a search rule configuration interface. On the left, there are three rule conditions stacked vertically, separated by 'or' operators. The first condition is 'Surname' with a dropdown set to 'Equals' and a text input containing 'Smith'. The second condition is 'Access level' with a dropdown set to 'Access Level 2' and a search icon. The third condition is 'Name' with a dropdown set to 'Equals' and a text input containing 'John'. Each condition has 'Check case' and 'Invert' checkboxes. At the bottom left is an 'Add rule' button and a search icon. On the right, there is a large grey area with an 'or' operator button at the top.

To add the search rule, do the following:

1. Go to the user search (see the [Going to user search](#) section).

This is an annotated version of the search rule configuration interface. A black box labeled '1' highlights the 'Add rule' button at the bottom left. Another black box labeled '2' highlights the 'or' operator button on the right side of the interface.

2. Click the **Add rule** button (1) to add AND rule or the **or** button (2) to add OR rule. The **Select condition for search** window will open.



3. The user parameters are listed in this window (see description in the [Setting user parameters](#) section).
4. Double click on the name of parameter by which search is to be performed.
5. The search rule by selected field will be added. Configuring of search rules differs due to type of rule. The following types of search rules are available:
 - a. Text field

- i. From the drop-down list (3) select the comparison method of a field value with specified search line.

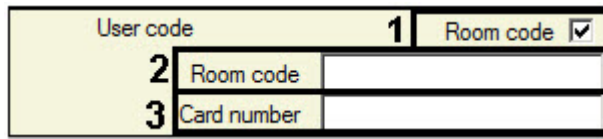
Comparison method	Description
Equals	Search for all users for which a value of the selected field is fully coincides with the specified search line.
Contains	Search for all users for which a value of the selected field contains the specified search line.
Starts with	Search for all users for which a value of the selected field starts with the specified search line
Ends with	Search for all users for which a value of the selected field ends with the specified search line

- ii. Set the **Check case** checkbox if it's required to consider symbols case while searching (4).
 - iii. Set the **Invert** checkbox if it's required to apply the negation of the specified search rule (5). It means that all users NOT satisfying to the specified search rule will be found if the checkbox is set.
 - iv. Enter the search line in the field (6).
 - b. Access level.

- i. Set the **Invert** checkbox if it's required to apply the negation of the specified search rule (1).
 - ii. Select value for search from the drop-down list (2).

To search the required access levels it's possible to click the  button. Working with windows of objects search is described in corresponding sections of this document.

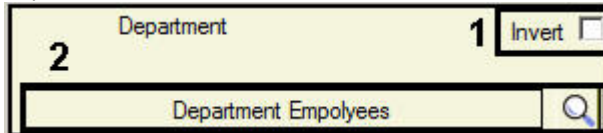
c. User card



The form for searching user cards contains three fields: 'User code' with a value of '1', 'Room code' with a checked checkbox, and 'Card number' with an empty text box. The 'Room code' field is labeled with a '2' and the 'Card number' field is labeled with a '3'.

- i. If it's not required to consider the room code, delete the **Room code** checkbox (1). As a result the **Room code** field won't be available for editing.
- ii. If it's required to use a room code while searching, enter the value in the **Room code** field (2).
- iii. Enter the required card number in the **Card number** field (3).

d. Department



The form for searching departments contains two fields: 'Department' with a value of '1' and an 'Invert' checkbox, and 'Department Employees' with a search icon. The 'Department' field is labeled with a '2'.

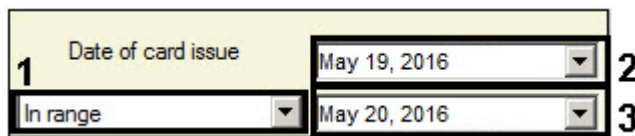
- i. Set the **Invert** checkbox if it's required to apply the negation of the specified search rule (1).
- ii. To search for required department click the  button (2). Working with windows of objects search is described in corresponding sections of this document.



Note.

Search for department is performed only if [going to user search](#) was performed by means of Ctrl+F keys.

e. Time values



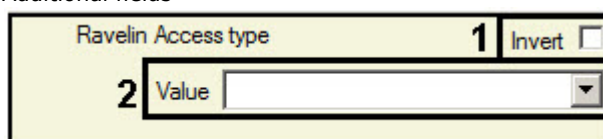
The form for searching time values contains three fields: 'Date of card issue' with a value of 'May 19, 2016' (labeled with a '1'), 'In range' with a dropdown menu (labeled with a '2'), and 'May 20, 2016' (labeled with a '3').

- i. Select the comparison method of the specified value for search with a field value:

Comparison method	Description
Equals	Search for all users for which a value of the selected field is fully coincides with the specified date.
Not equals	Search for all users for which a value of the selected field is not coincide with the specified date
Higher	Search for all users for which a value of the selected field more than specified date
Lower	Search for all users for which a value of the selected field less than specified date
In range	Search for all users for which a value of the selected field is in the specified range of dates
Out of range	Search for all users for which a value of the selected field is out of the specified range of dates

- ii. Set the date for search using the calendar (2).The selected value set the start of search interval in case of using last two comparison ways from the table.
- iii. Specify the end of search interval (3) in case of using last two comparison ways from the table.

f. Additional fields



The form for searching additional fields contains two fields: 'Ravelin Access type' with a value of '1' and an 'Invert' checkbox, and 'Value' with a dropdown menu (labeled with a '2').

- i. Set the **Invert** checkbox if it's required to apply the negation of the specified search rule (1).
- ii. Select the search value from the Value drop-down list (2).

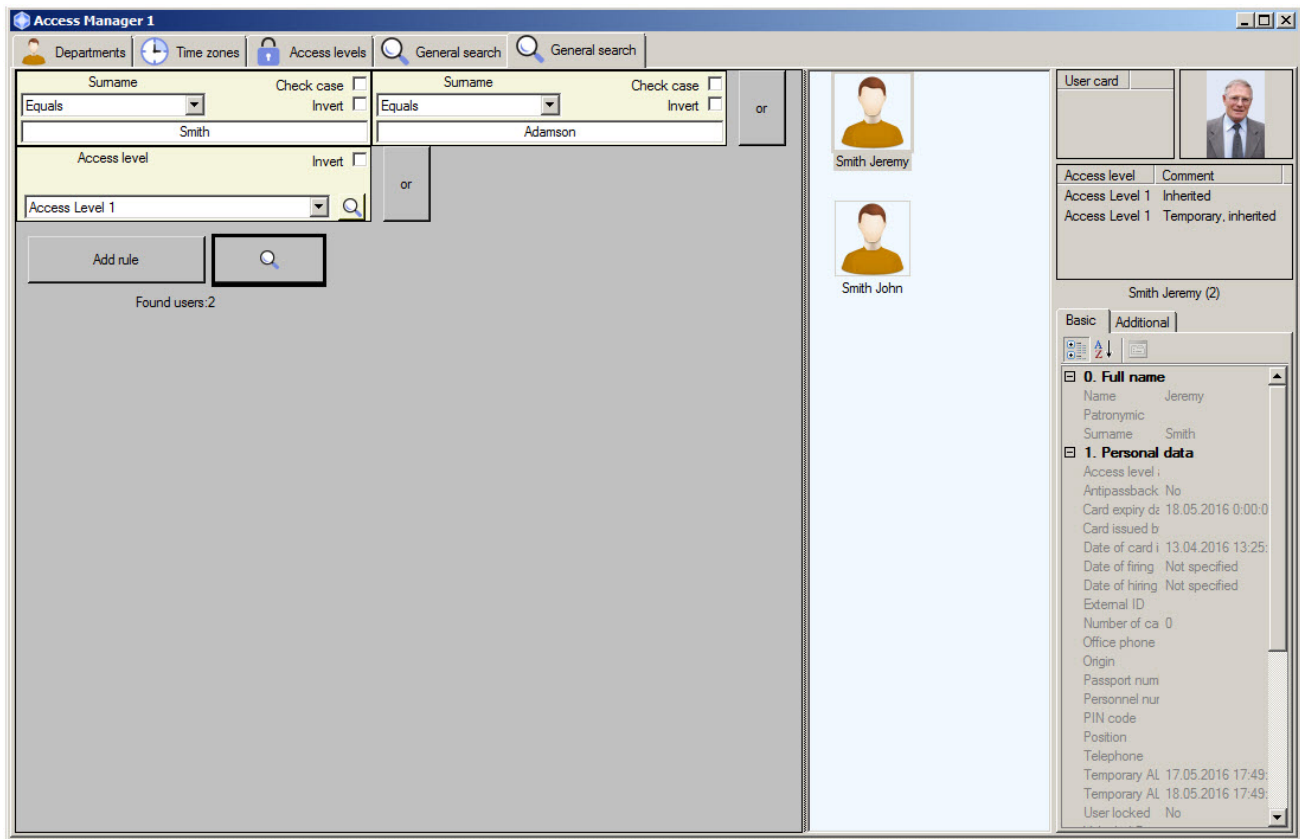
Adding a search rule is completed.

Start of user search



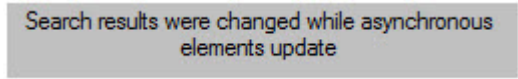
When all required search rules are specified (see the [Adding a search rule](#) section), click the button to start search.

Found users will display in the list.



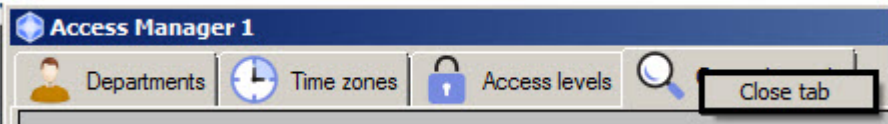
The list of found users can be changed dynamically.

Example. Search by surname was performed and several users were found. If a surname of one of found users will be changed than this user will be deleted from the search results. Conversely: if a new user will be added with a surname satisfying to the search rule, than this user will be added to the search results automatically. And the message about dynamic data changing will display in the line of search results .



Parameters of the user selected from the list are displaying in the right part of the **Access Manager** window.

To close a tab after search completion click the right mouse button on the tab name and select the **Close tab** item in the opened functional menu.



Deleting a user in the Access Manager software module

Deleting a user is performed as follows:



Note

Ctrl+Del и Ctrl+Backspace keys combination can be used apart of the given method. See the [Key combinations for working with objects lists](#) section.

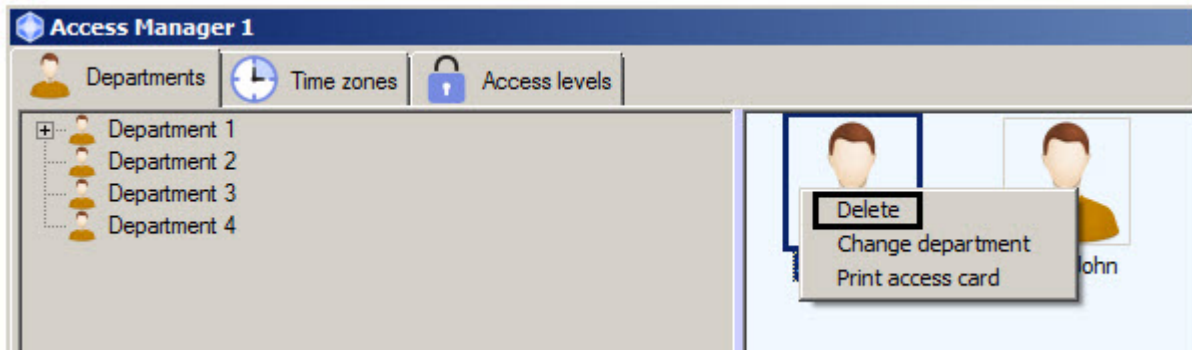
1. Go to viewing users list (see the [Viewing a list of users](#) section).
2. Click the right mouse button on a user which is to be deleted.



Note

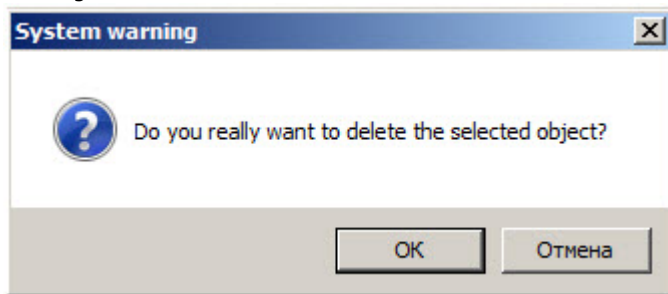
Also it's possible to select several or all users for deleting.

3. Select the **Delete** from the opened functional menu.

**Note**

Rights for deleting a user can be limited while configuring the *Access Manager* module. The message about missing the corresponding rights will be displayed. See also the [Rights for users configuring in the Access Manager](#) section.

4. The confirmation message will display. To confirm deleting of the selected user click the **OK** button. To cancel deleting click the **Cancel** button.



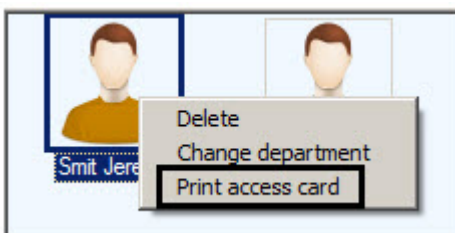
Deleting a user is completed.

Printing a user access card in the Access Manager software module

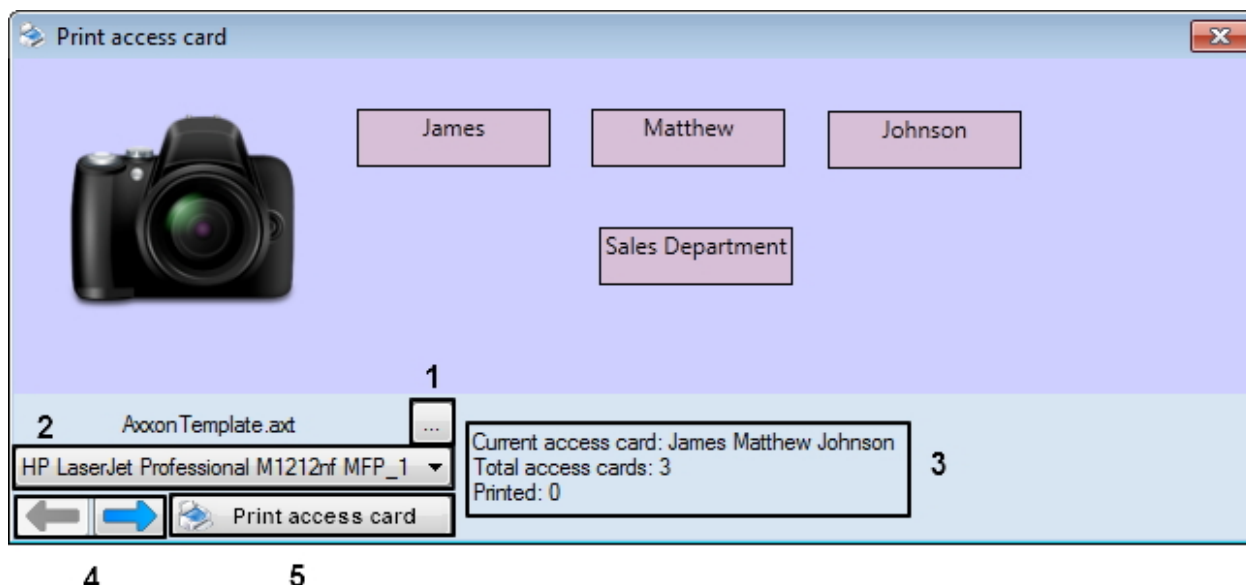
It's possible to print a user access cards in the *Access Manager* software module. A print templates creating with the help of the *Template Editor* are used (see the [Template Editor Utility Operation Guide](#)).

To print a user access card, do the following:

1. Go to viewing users list (see the [Viewing a list of users](#) section).
2. Click the right mouse button on the name of required user, or select several user by clicking on them while holding **Ctrl**.
3. Select the **Print access card** item in the opened functional menu.



4. The **Print access card** window will open.



5. Press the button (1) to select the template to print the access card.



Примечание.

Templates are created using the *Template Editor* utility - see the [Template Editor Utility Operation Guide](#).

Note: To create a template file that can be uploaded to **Access Manager**, you must manually run the *Edit or Wpf.exe* utility from the *Modules* folder in the *Intellect* installation directory.

6. From the drop-down list (2), select the printer that will be used from the list of available printers.
7. The interface displays the information on the status of printing (3).
8. The buttons (4) enable switching between users for whom the access cards are being printed, if there are several of them.
9. To print an access card, click the **Print card** button (5). The **Access Manager** module will automatically create a print queue and send the cards to the selected printer.



Note

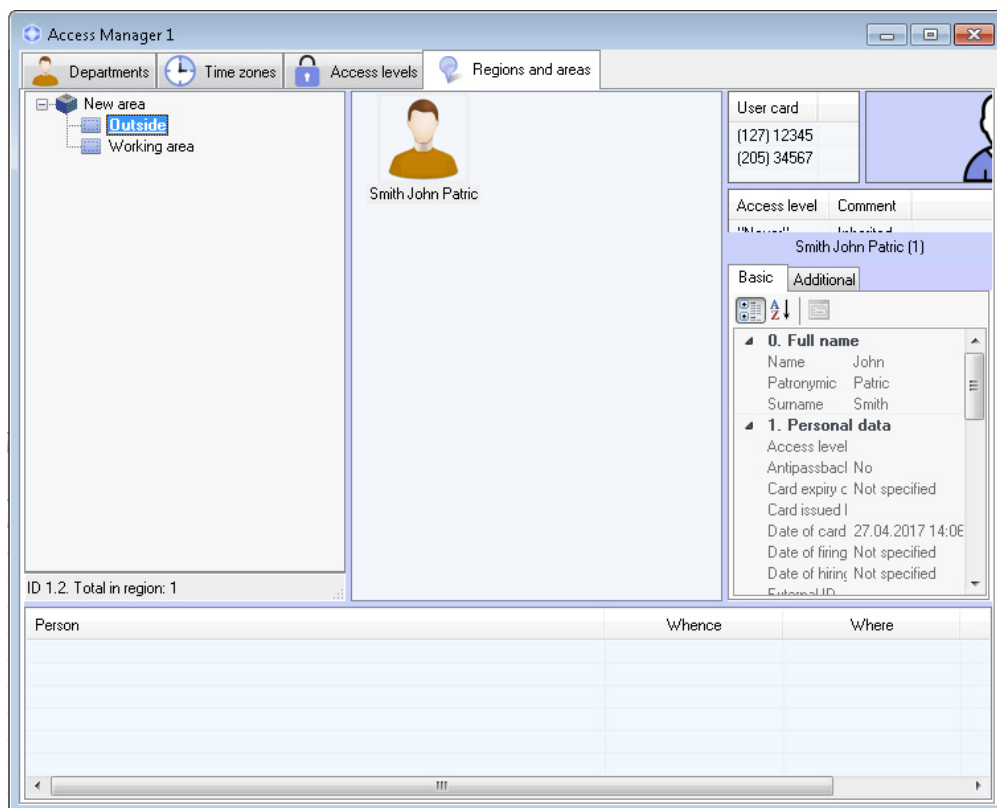
If a template was sent for printing, the *Access Manager* module will generate the "Print access card" event. A user full name, its ID, name of computer from which access card was printed and person initiated printing (operator working with the *Access Manager* module) will be specified in event parameters

Printing a user access card is completed.

Performing Emergency Monitoring

General information about Emergency Monitoring

Emergency monitoring is performed on the **Regions and areas** tab of the **Access Manager** window.



The Emergency monitoring includes the following features:

1. Switch over from access-related events in the *Event viewer* window to the user profile in the *Access manager* window (see [Viewing user profile from an access event in the Access Manager window](#)).
2. Find out the region where user is currently located (see [Finding out the region where the user currently is](#)).
3. Find out user list in the specified region (see [Viewing the list of users in the region](#)).
4. Switch over to the specified region on the *Intellect* software Map (see [Viewing region on the Map](#)).

At switching between interfaces (e.g. from the *Map* to the *Access Manager*, or from the *Event Viewer* to the *Access Manager*, or backwards), an interface object created on the basis of the same **Display** object as the source interface is selected for transition.

Configuration of the **Map**, **Event Viewer**, **Display**, **Area**, **Region** objects is described in the *Intellect software. Administrator's Guide*. Operation of these interface objects is described in the *Intellect software. Operator's Guide*. The most recent versions of these documents are available in the [AxxonSoft documentation repository](#).

Creating, editing and deletion of the **Area** and **Region** objects in **Access Manager** is also possible – see [Creating, editing and deleting Area and Region objects](#).

Card number displaying in the Event viewer window for access events

Facility code and card number of the user related to the access event is displayed in the **Card** column of the **Event viewer** window.

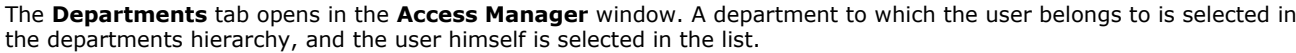


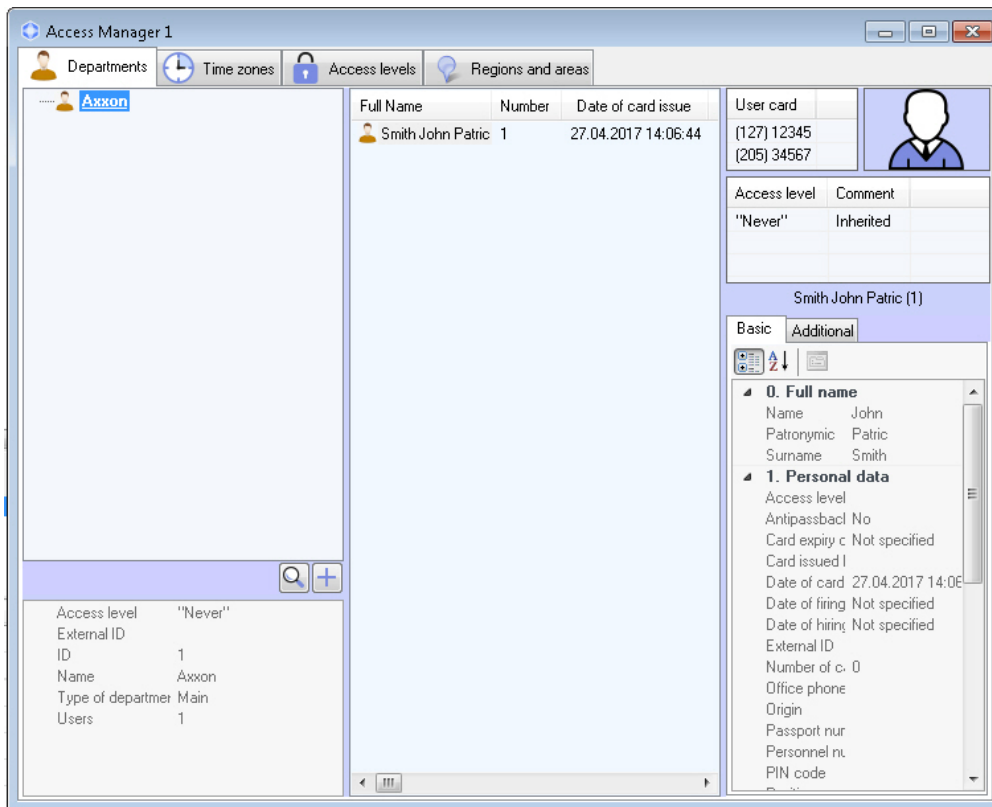
Note.

This column can be disabled according to the **Event Viewer** object settings – see [Administrator's Guide](#), the [Event viewer parameters](#) section. The most relevant version of this document is available in the [AxxonSoft documentation repository](#).



To view user profile in the Access Manager right-click on the corresponding event in the **Event viewer** window and select the **Show in AC department** menu item.





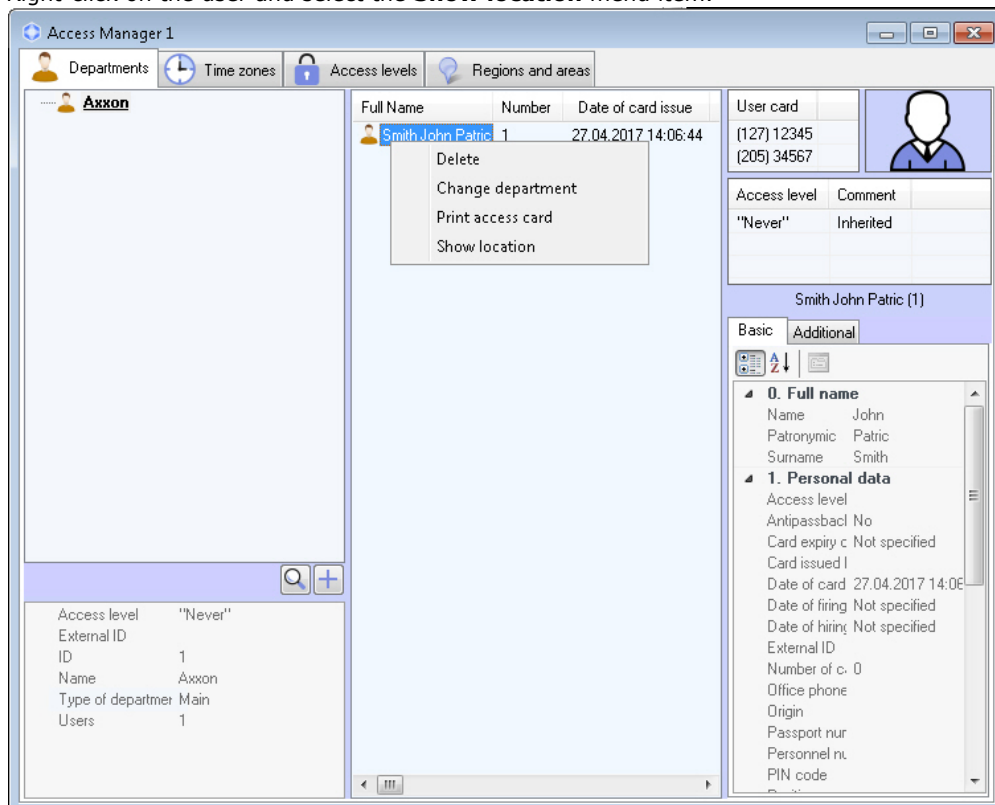
Note.

It is also possible to find out the user current location – see [Finding out the region where the user currently is](#).

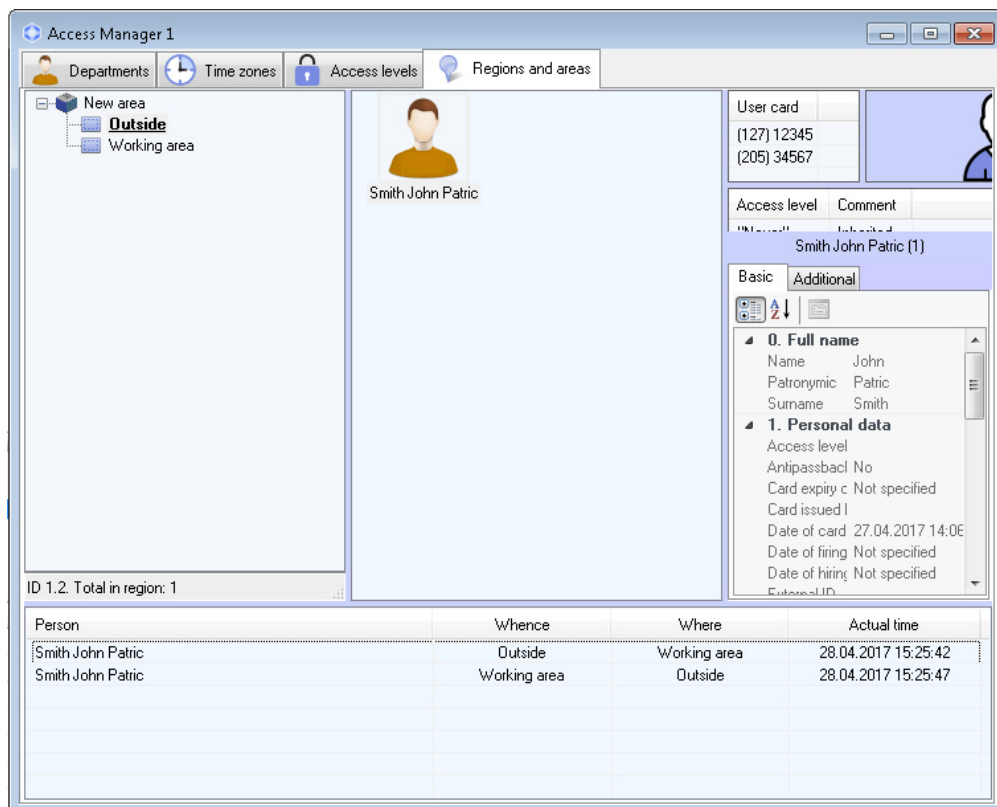
Finding out the region where the user currently is

To find out the user current location, do the following:

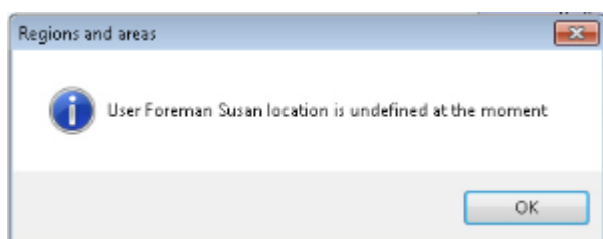
1. Find the user on the Departments tab manually or perform the user search (see [User search in the Access Manager software module](#)).
2. Right-click on the user and select the **Show location** menu item.



3. The **Regions and areas** tab opens. The region where the user is currently located is selected in the regions and areas hierarchy while the user himself is selected in the list of persons located in this region.



If the user location is undefined, the corresponding message is displayed.

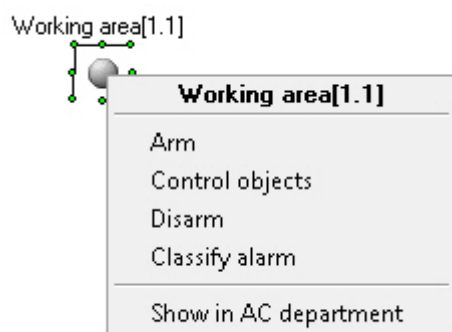


Defining the user current location is completed.

Viewing the list of users in the region

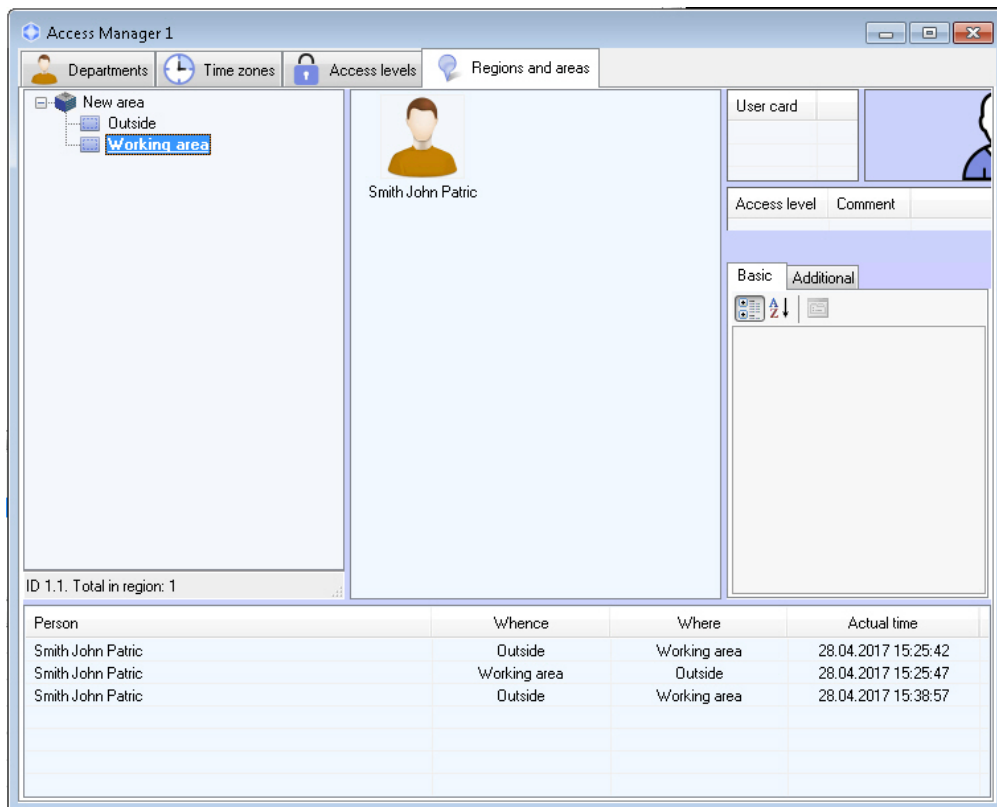
Switch to viewing users in the region in one of the following ways:

1. From the *ACFA-Intellect* Map, if the region is added to the Map. For that, right-click on the region and select the **Show in the Access Manager** menu item.



2. Select the region manually in the **Regions and areas** tab of the **Access Manager** window.

As a result, the list of users in the selected region is displayed. The information panel in the lower part of the regions and areas hierarchy displays the identifier of the selected region or area and the number of users, that are currently located in this region or area.



In the lower part off the **Regions and areas** tab there is a log of passes of all users registered in the system. The list of users in the region is displayed on real-time basis, while the passes of users between regions are displayed in the log.



Note.

This data on passes is given for information only, it is not recorded in a separate database.

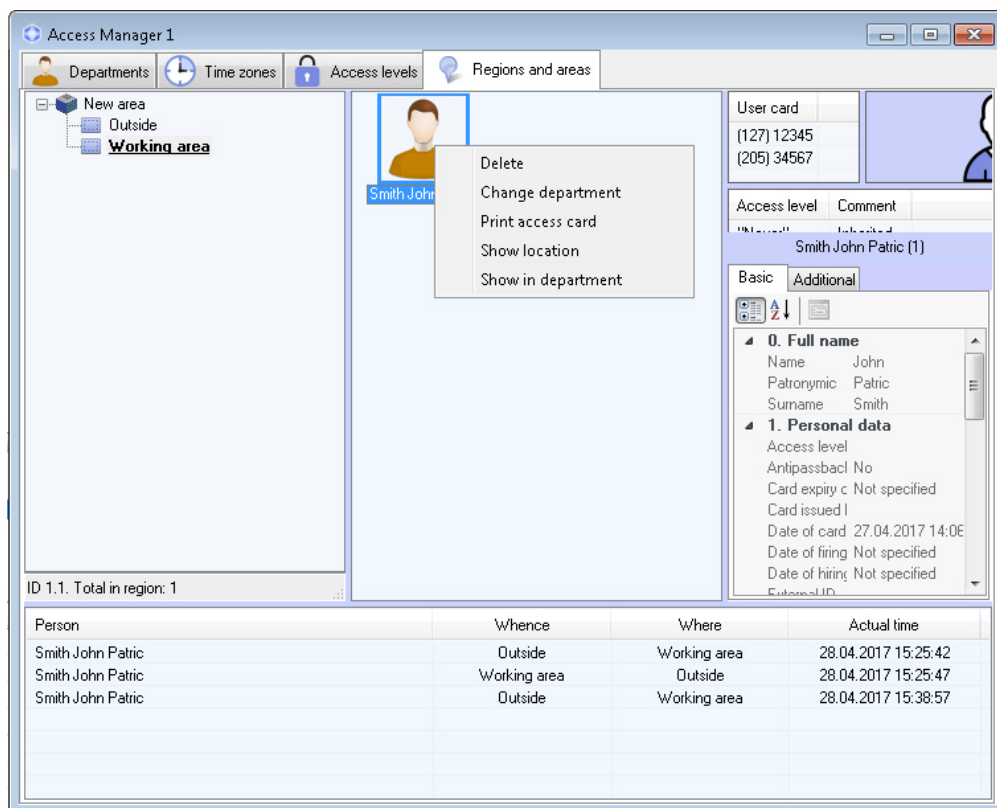
To view the passed user in the current region on the **Regions and areas** tab, right-click on the required event and select the **Show location** item in the menu opened. To view the passed user in his or her department on the **Departments** tab, select the **Show in department** item in the above menu

Person	Whence	Where	Actual time
Smith John Patric	Outside	Working area	28.04.2017 15:25:42
Smith John Patric	Working area	Outside	28.04.2017 15:25:47
Smith John Patric	Outside	Working area	28.04.2017 15:38:57

Show location
Show in department

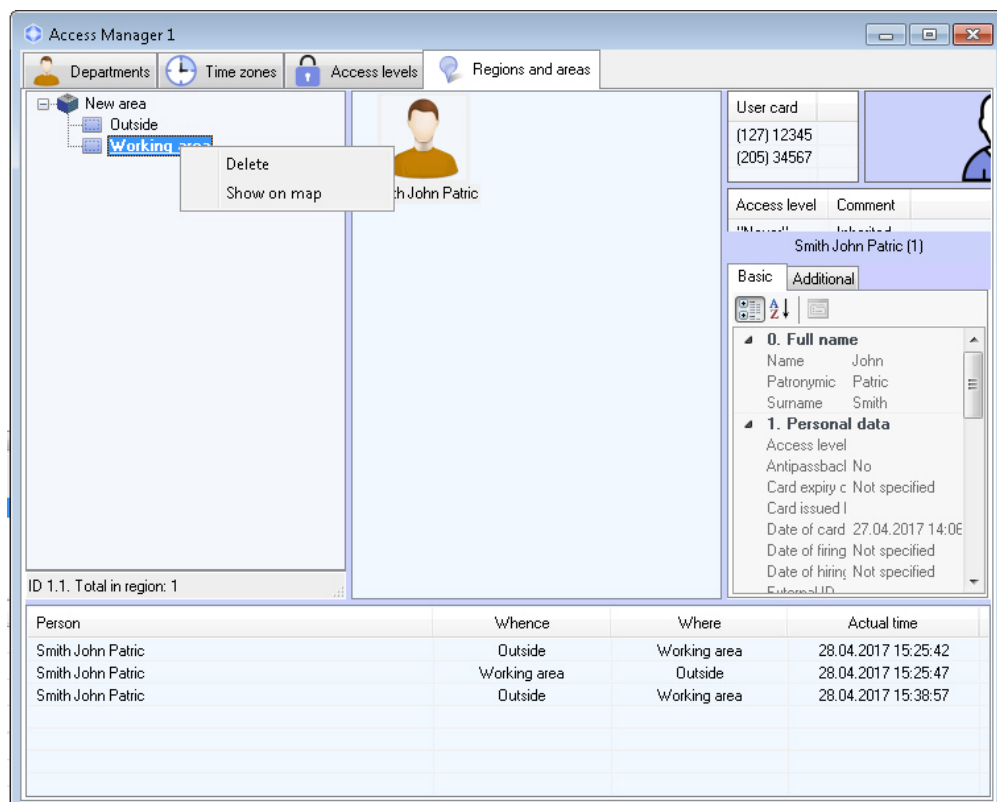
On th **Regions and areas** tab the same actions with a user as in the **Departments** tab are available (see [Working with users in the Access Manager software module](#)).

To view the user profile on the **Departments** tab, select the **Show in department** item in the user functional menu.

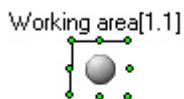


Viewing region on the Map

To view a region on the Map, right click on the corresponding object in the hierarchy and select the **Show on map** item in the menu opened.



As a result, the region is selected in the Map window and the region icon blinks twice.



Creating, editing and deleting Area and Region objects



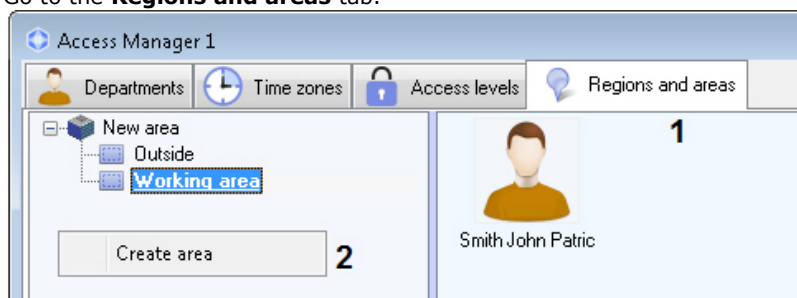
Note.

Creating, editing and deleting areas and regions can be done without using the Access Manager with the tools of the base *Intellect* software. See *Intellect software. Administrator's Guide*. The most recent version of this document is available in the [AxxonSoft documentation repository](#)

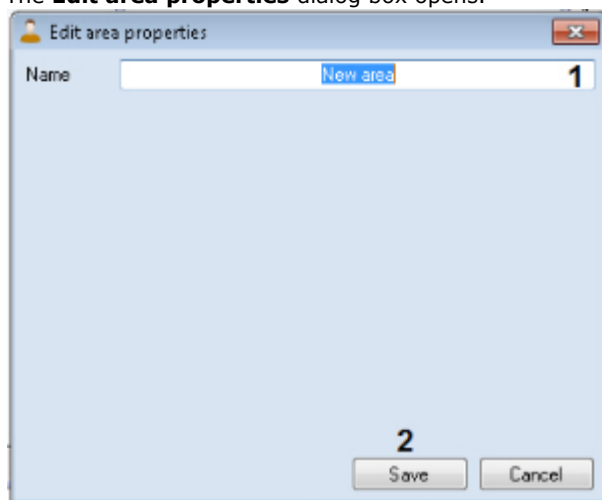
Creating areas

An **Area** object is created in the following order:

1. Go to the **Regions and areas** tab.



2. Right-click in the regions hierarchy area free from objects.
3. In the menu opened select the **Create area** item.
4. The **Edit area properties** dialog box opens.



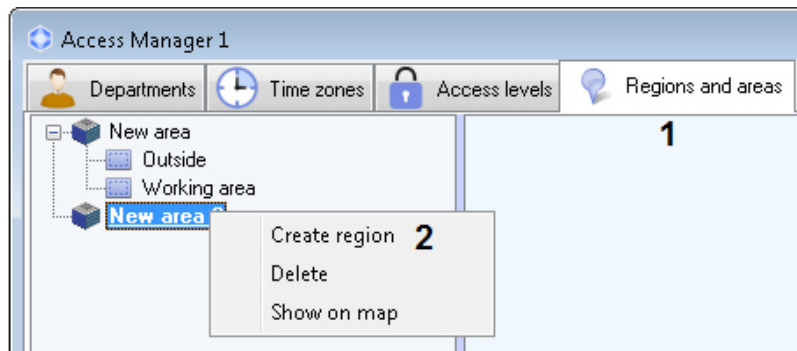
5. In the **Name** field enter the name of the created **Area** object (1).
6. Click **Save** (2).

The area is created.

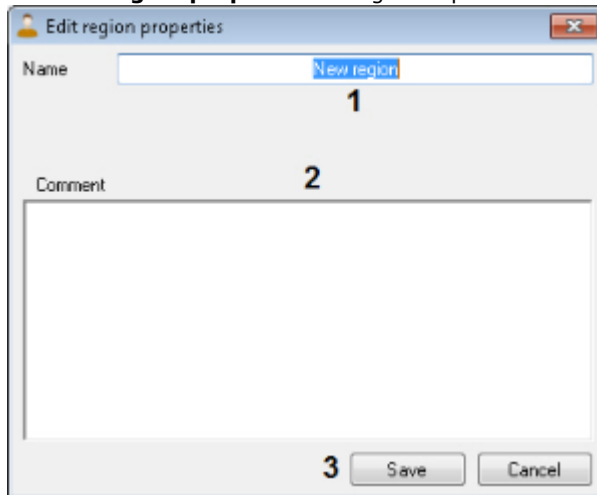
Creating regions

The region is created in the following order:

1. Go to the **Regions and areas** tab.



2. Right-click on the area under which the region is to be created.
3. In the menu opened select the **Create region** item.
4. The **Edit region properties** dialog box opens.



5. In the **Name** field enter the name of the created **Region** object (1).
6. In the **Comment** field enter description of the created region if necessary (2).
7. Click **Save** (3).

The region is created.

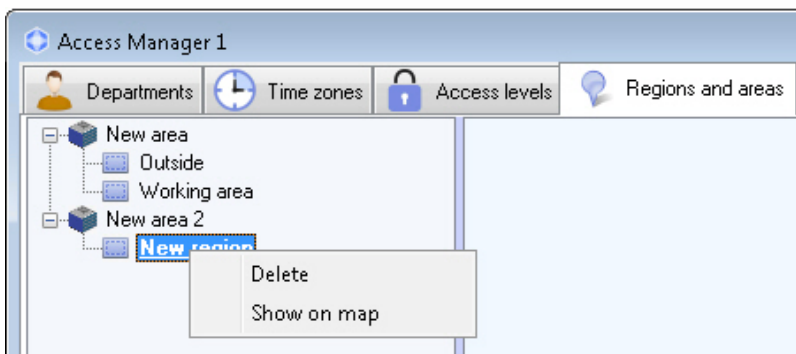
Editing areas and regions

To edit area or region, double-left-click on it.

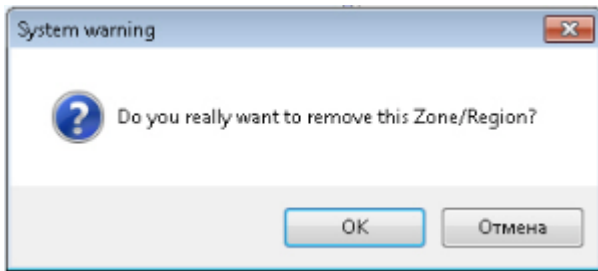
The **Edit area properties/Edit region properties** dialog box opens. Working with this dialog box is described in the [Creating areas](#) or [Creating regions](#) section correspondingly.

Deleting areas and regions

To delete an area or region, right-click on it and select the **Delete** menu item.



The **System warning** dialog box opens. Click **OK** to delete the **Area** or **Region**, or **Cancel** to abort the operation.



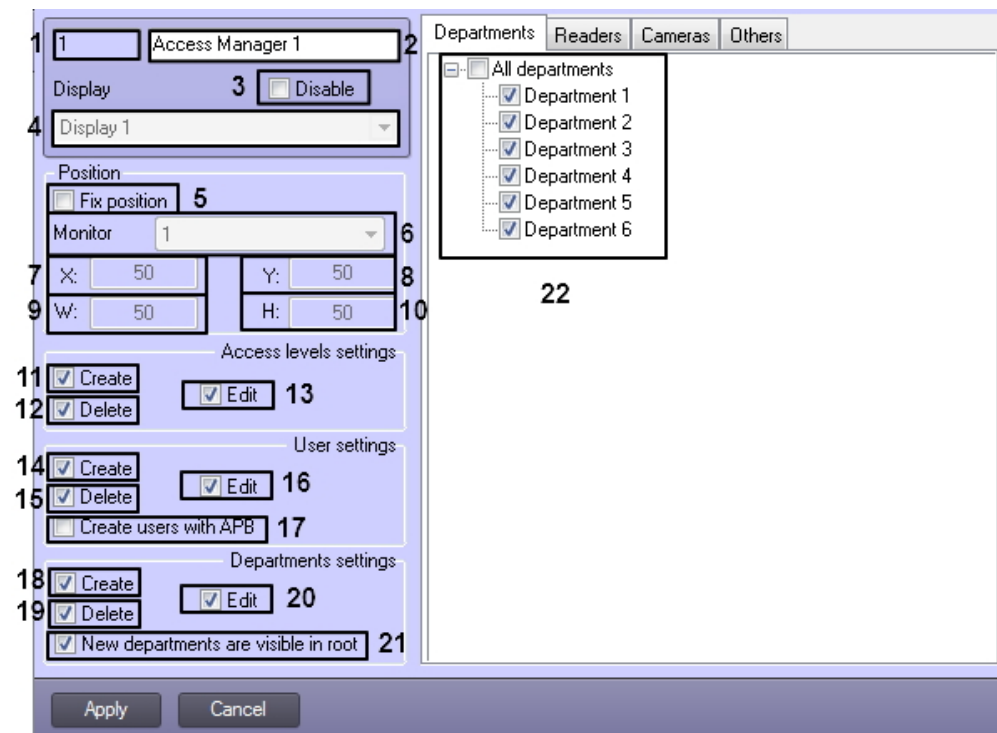
When you delete an area, all the child regions in it are deleted.

Deleting area or region is completed.

Appendix 1. Description of the Access Manager interfaces

The Access Manager object settings panel

The figure shows the **Access Manager** interface object settings panel.



Departments tab

1

Access Manager 1

Display

☐ Disable

Display 1

Position

☐ Fix position

Monitor

1

X:

50

Y:

50

W:

50

H:

50

Access levels settings

☒ Create

☒ Delete

☒ Edit

User settings

☒ Create

☒ Delete

☒ Edit

☐ Create users with APB

Departments settings

☒ Create

☒ Delete

☒ Edit

☒ New departments are visible in root

Apply

Cancel

Departments

Readers

Cameras

Others

☐ Confirm card entered by operator

23

FS80 control reader 1	☐
Gate Parking access point 1	☒
Gate Parking access point 2	☒
Suprema BioMini 1	☒

24

Readers tab

1

Access Manager 1

Display

☐ Disable

Display 1

Position

☐ Fix position

Monitor

1

X:

50

Y:

50

W:

50

H:

50

Access levels settings

☒ Create

☒ Delete

☒ Edit

User settings

☒ Create

☒ Delete

☒ Edit

☐ Create users with APB

Departments settings

☒ Create

☒ Delete

☒ Edit

☒ New departments are visible in root

Apply

Cancel

Departments

Readers

Cameras

Others

Cameras	Use	Gateway
Camera 1	☒	Videogate 1
Camera 2	☒	
Camera 3	☐	

25 26 27

Cameras tab

Others tab

The following table shows the elements in the **Access Manager** settings panel.

Nº	Parameter name	Parameter setting method	Description	Data type	Default value	Value range
1	ID field	Automatically	Displays the identification number of the Access Manager interface object in the system	Whole nonnegative number	-	Depends on number of accessible Access Manager objects in the system
2	Name field	Setting the value in the field	Sets the number of the Access Manager object in the system	Latin, Cyrillic and special symbols	Access Manager	Case-insensitive character string (letters, digits, special symbols excepting > and <). From 1 to 60 symbols
3	Disable checkbox	Settings checkbox	Sets the Access Manager object state in the system (enabled or disabled)	Boolean type	No	Yes – the Access Manager object is not used in the system. No – the Access Manager object is used and active
4	Display drop-down list	Selecting the value in the list	Sets the Display parent object for the Access Manager object	Name of created Display objects	Parent Display name	Depends on the number of the Display objects
Position group						
5	Fix position checkbox	Settings checkbox	Is used if it's required to specify coordinates of the Access Manager window and forbid its moving	Boolean type	No	Yes – position of the Access Manager window is fixed. No – position of the Access Manager window can be changed.
6	Monitor drop-down list	Selecting the value in the list	Sets the number of monitor on which the Access Manager window will be displayed	List of accessible computer monitors	Monitor 1	Depends on the number of connected computer monitors
7	X:	Setting the value in the field	Sets X coordinate of the upper left corner of the Access Manager window	% of screen width	0	From 0 to M*100, where M is a number of computer monitors
8	Y:	Setting the value in the field	Sets Y coordinate of the upper left corner of the Access Manager window	% of screen height	0	From 0 to M*100, where M is a number of computer monitors
9	W:	Setting the value in the field	Sets the Access Manager window width	% of screen width	0	From 0 to M*100, where M is a number of computer monitors

10	H:	Setting the value in the field	Sets the Access Manager window height	% of screen height	0	From 0 to M*100, where M is a number of computer monitors
Access level settings group						
11	Create checkbox	Settings checkbox	Sets possibility to create access levels in the Access Manager window	Boolean type	Yes	Yes – creating access levels from the Access Manager window is allowed. No – creating access levels from the Access Manager window is forbidden.
12	Delete checkbox	Settings checkbox	Sets possibility to delete access levels in the Access Manager window	Boolean type	Yes	Yes – deleting access levels from the Access Manager window is allowed. No – deleting access levels from the Access Manager window is forbidden.
13	Edit checkbox	Settings checkbox	Sets possibility to edit access levels in the Access Manager window	Boolean type	Yes	Yes – editing access levels from the Access Manager window is allowed. No – editing access levels from the Access Manager window is forbidden.
User settings group						
14	Create checkbox	Settings checkbox	Sets possibility to create users in the Access Manager window	Boolean type	Yes	Yes – creating users from the Access Manager window is allowed. No – creating users from the Access Manager window is forbidden.
15	Delete checkbox	Settings checkbox	Sets possibility to delete users in the Access Manager window	Boolean type	Yes	Yes – deleting users from the Access Manager window is allowed. No – deleting users from the Access Manager window is forbidden.
16	Edit checkbox	Settings checkbox	Sets possibility to edit users in the Access Manager window	Boolean type	Yes	Yes – editing users from the Access Manager window is allowed. No – editing users from the Access Manager window is forbidden.
17	Create users with APB checkbox	Settings checkbox	Sets default value for antipassback parameter	Boolean type	No	Yes – users are created with antipassback on default. No – users are created without antipassback on default.
Departments settings group						
18	Create checkbox	Settings checkbox	Sets possibility to create departments in the Access Manager window	Boolean type	Yes	Yes – creating departments from the Access Manager window is allowed. No – creating departments from the Access Manager window is forbidden.
19	Delete checkbox	Settings checkbox	Sets possibility to delete departments in the Access Manager window	Boolean type	Yes	Yes – deleting departments from the Access Manager window is allowed. No – deleting departments from the Access Manager window is forbidden.
20	Edit checkbox	Settings checkbox	Sets possibility to edit departments in the Access Manager window	Boolean type	Yes	Yes – editing departments from the Access Manager window is allowed. No – editing departments from the Access Manager window is forbidden.

21	New departments are visible in root checkbox	Settings checkbox	Sets availability of new created departments in the Access Manager hierarchy root	Boolean type	Yes	Yes – new departments are available in the Access Manager hierarchy root No – new departments are not available in the Access Manager hierarchy root
Departments tab						
22	Departments tree	Settings checkbox	Sets available departments in the Access Manager window	Boolean type	Set of boolean variables	Department will be available in the Access Manager window if checkbox is set close to it
Readers tab						
23	Confirm card entered by operator checkbox	Settings checkbox	Sets requirement to confirm card code entering by operator	Boolean type	No	Yes – operator confirmation is required to assign access card to user. No –operator confirmation is not required to assign access card to user.
24	List of readers	Settings checkbox	Sets list of control readers used for entering user access cards	List of created reader objects in the system	Set of boolean variables	The reader will be available to enter user access card if checkbox is set close to it
Cameras tab						
25	Cameras column	Automatically	Displays list of Camera objects created on the Hardware tab of the System settings dialog window	List of created Camera objects in the system	Names of Camera objects	Depends on number of accessible Camera objects in the system
26	Use checkbox	Settings checkbox	Sets possibility to use camera for assigning photo to user in the Access Manager window	Boolean type	No	Yes – camera can be used for assigning photo. No – camera can't be used for assigning photo
27	Gateway drop-down list	Selecting the value in the list	Sets the Gateway object used for receiving video signal from camera	List of created Gateway objects in the system	Names of Gateway objects	Depends on number of accessible Gateway objects in the system
Others tab						
28	Full name drop-down list	Selecting the value in the list	Sets the way of defining of users record duplicates by name, surname, patronymic	List of available combinations	Not used	Not used – adding users with the same full name is allowed. Surname, name – adding users with the same name and surname and different patronymic is forbidden. Surname, name, patronymic – creating users with the same full name is forbidden.
29	External ID checkbox	Settings checkbox	Indicates whether the users records should be checked for external ID duplicates	Boolean type	No	Yes – creating users with the same external ID is forbidden. No – creating users with the same external ID is allowed.
30	Vehicle license plate checkbox	Settings checkbox	Indicates whether the users records should be checked for vehicle licence plate number duplicates	Boolean type	No	Yes – creating users with the same license plate number is forbidden. No – creating users with the same license plate number is allowed.
31	Module version field	Automatically	Displays the current version number	Number	Current version number	Depands on the current version of the module.

The User rights in Access Manager object settings panel

The figure shows the **User rights in Access Manager** interface object settings panel.

1.1 User rights in Access Manager

Access Manager ☐ Disable

Access Manager 1

User rights

User permissions 1

Access levels settings

☒ Create ☒ Edit

☒ Delete

User settings

☒ Create ☒ Edit

☒ Delete

Departments Standard fields Additional fields

☐ All departments

- ☒ Department 1
 - ☒ New department 1
- ☒ Department 2
- ☒ Department 3
- ☒ Department 4

☒ Create ☒ Edit ☒ Delete

☒ New departments are visible in root

Apply Cancel

Departments tab

1.1 User rights in Access Manager

Access Manager ☐ Disable

Access Manager 1

User rights

User permissions 1

Access levels settings

☒ Create ☒ Edit

☒ Delete

User settings

☒ Create ☒ Edit

☒ Delete

Departments Standard fields Additional fields

Name of field	
Surname	Hidden
Name	Hidden
Patronymic	Hidden
Personnel number	Hidden
External ID	Hidden
Position	Hidden
Date of hiring:	Hidden
Date of firing	Hidden
Temporary AL activation date	Hidden
Temporary AL expiry date	Hidden
Access cards	Hidden
Commencement of card	Hidden
Card expiry date	Hidden
Date of card issue	Hidden
Number of card loss	Hidden
PIN code	Hidden
Access levels	Hidden

☒ New departments are visible in root

Standard fields tab



Note

The list of fields displaying in the **Additional fields** tab depends on used integration module.

The following table shows the elements in the **User rights in Access Manager** settings panel.

№	Parameter name	Parameter setting method	Description	Data type	Default value	Value range
1	ID field	Automatically	Displays identical number of the User rights in Access Manager interface object in the system	Whole nonnegative number	-	Depends on number of accessible User rights in Access Manager objects in the system
2	Name field	Setting the value in the field	Sets the number of the User rights in Access Manager object in the system	Latin, Cyrillic and special symbols	User rights in Access Manager	Case-insensitive character string (letters, digits, special symbols excepting > and <). From 1 to 60 symbols
3	Disable checkbox	Settings checkbox	Sets the User rights in Access Manager object state in the system (enabled or disabled)	Boolean type	No	Yes – the User rights in Access Manager object is not used in the system. No – the User rights in Access Manager object is used and active
4	Access Manager drop-down list	Selecting the value in the list	Sets the Access Manager parent object for the User rights in Access Manager object	Names of acceptable Access Manager objects in the system	Name of the Access Manager parent object	Depends on number of Access Manager objects in the system
User rights group						
5	User rights drop-down list	Selecting the value in the list	Sets user rights in the <i>ACFA-Intellect</i> software package, corresponding to the configured User rights in Access Manager object	Name of created User permissions objects	Depends on created User permissions objects	Depends on created User permissions objects
Access level settings group						
6	Create checkbox	Settings checkbox	Sets possibility to create access levels in the Access Manager window while working with configured operator rights	Boolean type	Yes	Yes – creating access levels from the Access Manager window is allowed. No – creating access levels from the Access Manager window is forbidden.
7	Delete checkbox	Settings checkbox	Sets possibility to delete access levels in the Access Manager window while working with configured operator rights	Boolean type	Yes	Yes – deleting access levels from the Access Manager window is allowed. No – deleting access levels from the Access Manager window is forbidden
8	Edit checkbox	Settings checkbox	Sets possibility to edit access levels in the Access Manager window while working with configured operator rights	Boolean type	Yes	Yes – editing access levels from the Access Manager window is allowed. No – editing access levels from the Access Manager
User settings group						
9	Create checkbox	Settings checkbox	Sets possibility to create users in the Access Manager window while working with configured operator rights	Boolean type	Yes	Yes – creating users from the Access Manager window is allowed. No – creating users from the Access Manager window is forbidden.

10	Delete checkbox	Settings checkbox	Sets possibility to delete users in the Access Manager window while working with configured operator rights	Boolean type	Yes	Yes – deleting users from the Access Manager window is allowed. No – deleting users from the Access Manager window is forbidden
11	Edit checkbox	Settings checkbox	Sets possibility to edit users in the Access Manager window while working with configured operator rights	Boolean type	Yes	Yes – editing users from the Access Manager window is allowed. No – editing users from the Access Manager window is forbidden.
Without group						
12	New departments are visible in root checkbox	Settings checkbox	Sets availability of new created departments in the Access Manager hierarchy root	Boolean type	Yes	Yes – new departments are available in the Access Manager hierarchy root No – new departments are not available in the Access Manager hierarchy root
Departments tab						
13	Departments tree	Settings checkbox	Sets available departments in the Access Manager window while working with configured operator rights	Boolean type	Set of boolean variables	Department will be available in the Access Manager window if checkbox is set close to it.
14	Create checkbox	Settings checkbox	Sets possibility to create departments in the Access Manager window while working with configured operator rights	Boolean type	Yes	Yes – creating departments from the Access Manager window is allowed. No – creating departments from the Access Manager window is forbidden.
15	Delete checkbox	Settings checkbox	Sets possibility to delete departments in the Access Manager window while working with configured operator rights	Boolean type	Yes	Yes – deleting departments from the Access Manager window is allowed. No – deleting departments from the Access Manager window is forbidden.
16	Edit checkbox	Settings checkbox	Sets possibility to edit departments in the Access Manager window	Boolean type	Yes	Yes – editing departments from the Access Manager window is allowed. No – editing departments from the Access Manager window is forbidden.
Standard fields tab						
17	Name of field column	Automatically	List of available user fields	-	-	See the Setting user parameters section
18	Field availability for viewing and editing	Selecting the value in the list	Sets availability of field for viewing and editing	Accessible types of field availability	Hidden	Hidden Read only Edit

The Type of department object settings panel

The figure shows the **Type of department** interface object settings panel.

1.1 Type of department 1.1

Access Manager ☐ Disable

Access Manager 1

Icon Icon 0

Template

Apply

Name of field	Edit	Category
Surname	Edit	0. Full name
Name	Edit	0. Full name
Patronymic	Edit	0. Full name
Personnel number	Hidden	1. Personal data
External ID	Edit	1. Personal data
Position	Edit	1. Personal data
Date of hiring:	Edit	1. Personal data
Date of firing	Edit	1. Personal data
Temporary AL activation date	Hidden	1. Personal data
Temporary AL expiry date	Hidden	1. Personal data
Access cards	Edit	1. Personal data
Commencement of card	Edit	1. Personal data
Card expiry date	Hidden	
Date of card issue	Hidden	



Note

The list of fields displaying in the **Additional fields** tab depends on used integration module.

The following table shows the elements in the **Type of department** settings panel.

Nº	Parameter name	Parameter setting method	Description	Data type	Default value	Value range
1	ID field	Automatically	Displays identical number of the Type of department interface object in the system	Whole nonnegative number	-	Depends on number of accessible Type of department objects in the system
2	Name field	Setting the value in the field	Sets the number of the Type of department object in the system	Latin, Cyrillic and special symbols	Type of department	Case-insensitive character string (letters, digits, special symbols excepting > and <). From 1 to 60 symbols
3	Disable checkbox	Settings checkbox	Sets the Type of department object state in the system (enabled or disabled)	Boolean type	No	Yes – the Type of department object is not used in the system. No – the Type of department object is used and active
4	Access Manager drop-down list	Selecting the value in the list	Sets the Access Manager parent object for the Type of department object	Names of acceptable Access Manager objects in the system	Name of the Access Manager parent object	Depends on number of Access Manager objects in the system
Without group						
5	Icon drop-down list	Selecting the value in the list	Sets icon used for displaying department in the tree of the Access manager window	Name of accessible icons	Icon 0	Icon 0 – Icon 29
6	Template drop-down list	Selecting the value in the list	Sets fields available for viewing and editing for some users category	Name of accessible templates	-	Employees Vehicle Visitors
7	Apply button	Clicking the button	Applying the selected template	-	-	-
Standard fields tab						

8	Name of field column	Automatically	List of available user fields	-	-	See the Setting user parameters section
9	Field availability for viewing and editing	Selecting the value in the list	Sets availability of field for viewing and editing	Accessible types of field availability	Hidden	Hidden Read only Edit
10	Category field	Setting the value in the field	Sets name of a category in which field will display on the Access Manager user panel	Latin, Cyrillic and special symbols	-	Any character string

Appendix 2. Configuring a visitor management system without the Access Manager interface window

General information on ACFA Intellect objects related to the visitor management system

Some of the *ACFA Intellect* software objects can be used to set up the visitor management system without the *Visitor Management System* window, namely:

1. **User** and **Department** objects created on the **Users** tab of the **System settings** dialog box.
2. **Access level** and **Time zone** (which corresponds both to time zone and shift work in the VMS) objects created on the **Programming** tab of the **System settings** dialog box.



Note.

Settings panel of the **Time zone** object is described in the [Intellect software. Administrator's Guide](#) for this object is used in the *Intellect* software not only for setting up the visitor management system but also for other purposes.

Most of the settings in the settings panels of these objects duplicate the respective settings of the *Visitor Management System* objects. Thus, the setting of the listed objects is designed to operate in the absence of the *Visitor Management System* module in the system (if the module is not purchased). However, as practice shows, the *Visitor Management System* module provides a much more user-friendly interface to perform similar tasks and also has an enhanced functionality, so it is recommended to use the *Visitor Management System* module.

Settings panel of the Department object

The picture shows the settings panel of the **Department** object.

The table gives the description of the **Department** object settings.

#	Parameter name	Method for setting the parameter value	Parameter description	Default value	Value range
1	Identification number field	Automatically	Shows the identification number of the Department object in the system	-	Depends on number of Department objects in the system

2	Name field	Enter the value in the field	Sets the name of the Department object in the system	Department	A line representing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive. Number of symbols – from 1 to 60.
3	Disable checkbox	Is set in a checkbox	Sets the status (enabled/disabled) of the Department object in the system	False	True - the Department object is enabled and in use False - the Department object is disabled and not in use
The Access control group					
4	Access level dropdown list	Is selected in the list	Sets the department's access level	-	The list of Access level objects created in <i>ACFA Intellect</i> (on the Programming tab or via the VMS) and also Full access and Access forbidden levels.
5	List of access levels	Is selected in the list. To add a new row in the table click left mouse button in any empty space of the table and press "down" arrow on the keyboard.	Sets the department's access level list	-	The list of Access level objects created in <i>ACFA Intellect</i> (on the Programming tab or via the VMS)
The "Rubezh" subsystem group					
6	Region dropdown list	Is selected in the list	Sets the Region object for the <i>Rubeg-07 ACS</i> (discontinued)	-	The list of Region objects in the <i>ACFA Intellect</i> software
7	Access level dropdown list	Is selected in the list	Sets the access level for the <i>Rubeg-07 ACS</i> (discontinued)	-	The list of Access level objects created in <i>ACFA Intellect</i> (on the Programming tab or via the VMS) and also Full access and Access forbidden levels.

Settings panel of the User object

The pictures show the settings panel of the **User** object.

The screenshot displays the settings panel for a User object. It includes fields for Name (1), Department (2), a Disable checkbox (3), and a Department dropdown (4). Below these is the "Rubezh" subsystem section with Rights for regions management (5), Access level (6), and Group (7) dropdowns. The bottom section contains checkboxes for User locked (8) and Antipassback (9), followed by input fields for Object code (10), PIN (11), Permanent card (12), Temporary card (13), and Valid till (14). On the right, the "Additional cards" table (15) shows columns for Object code and Card, with a sample entry (16). At the bottom are tabs for Access control and Access Levels.

Settings panel of the **User** object The **Access control** tab.

1 User 1

Department ☐ Disable

Department 1

"Rubezh" subsystem

Rights for regions management

Access level

Group

Additional info

Access type: List 17

A.L.	Date1	Time1	Date2	Time2
Access Level 1 18	01-01-01 19	0:00:00 19	09-05-45 20	00:00:20 20

Access control Access Levels

Settings panel of the **User** object The **Access levels** tab.

The table gives the description of the **User** object settings.

#	Parameter name	Method for setting the parameter value	Parameter description	Default value	Value range
1	Identification number field	Automatically	Shows the identification number of the User object in the system	-	Depends on number of User objects in the system
2	Name Field	Enter the value in the field	Sets the name of the User object in the system	User	A line representing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive. Number of symbols – from 1 to 60. Do not use rs as username when registering Operator accounts as this name is used by default in <i>Intellect Web Report System</i> .
3	Disable Check box	Is set in a checkbox	Sets the status (enabled/disabled) of the User object in the system	False	True - the User object is enabled and in use False - the User object is disabled and not in use
4	Department dropdown list	Is selected in the list	Sets the parent Department object for this User object	Name of the parent Department object	Depends on number of Department objects in the system
5	Additional info field	Enter the value in the field	Additional user information	-	A line representing a sequence of any symbols
The " Rubezh " subsystem group					
6	Rights for region management dropdown list	Is selected in the list	Sets the permissions for the <i>Rubeg-07 ACS</i> (discontinued) regions management	-	0 - 16
7	Access level dropdown list	Is selected in the list	Sets the access level for the <i>Rubeg-07 ACS</i> (discontinued)	-	The list of Access level objects created in <i>ACFA Intellect</i> (on the Programming tab or via the VMS) and also Full access and Access forbidden levels.
The Access control tab					
8	User locked checkbox	Is set in a checkbox	Is set if the user is to be locked.	False	True – the user is locked. False – the user is active.

9	Antipassback checkbox	Is set in a checkbox	Is set if the user is not allowed to go twice through the reader in the same direction.	False	True – anti-passback enabled. False – anti-passback disabled.
10	Object code field	Enter the value in the field	Facility code of the user's access card	-	Depends on the type of cards in use.
11	PIN field	Enter the value in the field	PIN-code of the user's access card	-	Depends on the ACS in use
12	Permanent card field	Enter the value in the field	User's access card number	-	Depends on the type of cards in use.
13	Temporary card field	Enter the value in the field	User's temporary access card number	-	Depends on the type of cards in use.
14	Valid till field	Enter the value in the field	Date the user's access card expires (which is specified in the Permanent card field)	-	Date in DD.MM.YYYY format
Additional cards table					
Note. In the Visitor Management System, the additional cards are specified separated by spaces after the parameters of the main card. The functionality of assigning users additional cards is to be supported by the hardware.					
15	Object code field	Enter the value in the field	Facility code of the user's additional access card	-	Depends on the type of cards in use.
16	Card code field	Enter the value in the field	Number of the user's additional access card	-	Depends on the type of cards in use.
The Access levels tab.					
17	Access type dropdown list	Is selected in the list	Sets the way of choosing access level for user	-	Group - the employee is assigned the access level of the department Access forbidden - the employee is not allowed to access, even if the department assigned a different access level, allowing access Full access - the employee has a full access , even if the department assigned a restricted access level List - the employee is assigned a list of access levels having priority over the department access level.
18	A.L. dropdown list	Is selected in the list	Can be used if the List value is selected in the Access type list. Sets the user's access level list	-	The list of Access level objects created in <i>ACFA Intellect</i> (on the Programming tab or via the VMS)
19	Date1 and Time1 fields	Enter the value in the field	Allow to set the beginning date of the temporary access level.	-	Date in DD-MM-YY and time in HH:MM:SS format.
20	Date2 and Time2 fields	Enter the value in the field	Allow to set the ending date of the temporary access level.	-	Date in DD-MM-YY and time in HH:MM:SS format.

Settings panel of the Access level object

The picture shows the settings panel of the **Access level** object.

The table gives the description of the **Access level** object settings.

#	Parameter name	Method for setting the parameter value	Parameter description	Default value	Value range
1	Identification number field	Automatically	Shows the identification number of the Access level object in the system	-	Depends on number of Access level objects in the system
2	Name field	Enter the value in the field	Sets the name of the User object in the system	Access level	A line representing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive. Number of symbols – from 1 to 60.
3	Disable checkbox	Is set in a checkbox	Sets the status (enabled/disabled) of the Access level object in the system	False	True - the Access level object is enabled and in use False - the Access level object is disabled and not in use
4	Access point dropdown list	Is selected in the list	Card reader through which the employees are performing access	-	Depends on the readers created in the system
5	Time zone dropdown list	Is selected in the list	Time zone, during which the access will be allowed through the corresponding access point	-	Always Never The list of Time zone objects created in the system
6	Arm checkbox	Is set in a checkbox	Enables arming of access point after presenting access card by user. <i>Note. This function should be supported by hardware.</i>	False	True – access point is armed after presenting access card by user False – access point is not armed after presenting access card by user
7	Disarm checkbox	Is set in a checkbox	Enables disarming of access point after presenting access card by user. <i>Note. This function should be supported by hardware.</i>	False	True – access point is disarmed after presenting access card by user False – access point is not disarmed after presenting access card by user

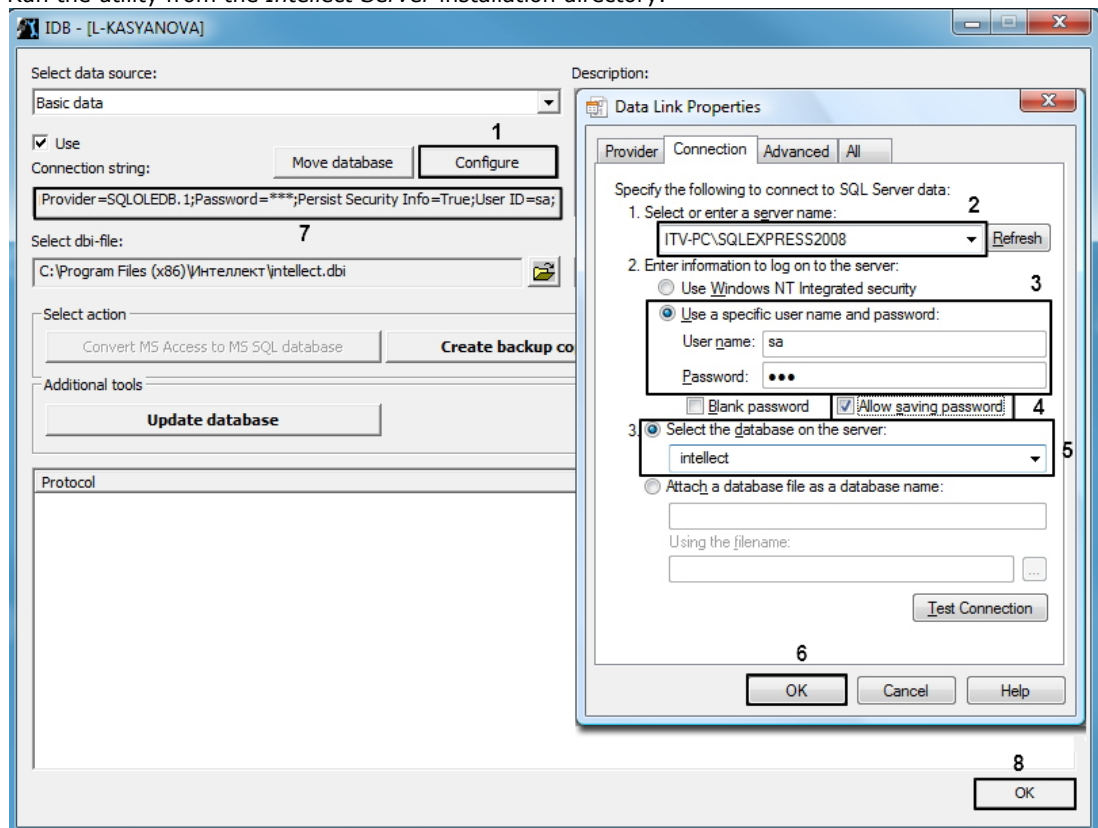
8	Transmit cards checkbox	Is set in a checkbox	Enables sending access cards to controller after presenting access card by user. <i>Note. This function should be supported by hardware.</i> <i>Function of this checkbox can differ depending on the integration module in use. For example, in PERCo-S-20 integration this checkbox enables commission mode.</i>	False	True – access cards are sent to controller after presenting access card by user. False – access cards are not sent to controller after presenting access card by user.
---	--------------------------------	----------------------	--	-------	---

Appendix 3. Settings for proper operation of the Access Manager module in a distributed architecture

The *Access Manager* module loads the components required for its proper operation directly from the SQL Server database of the *Intellect Server*. This causes some problems for module operation in distributed architectures, based on a variety of combinations between the *Intellect Server*, the *Remote Admin Workstation*, and the *Client* (see [Configuration of distributed architecture](#)).

In particular, attempting to run the *Access Manager* module remotely from a computer with a *Client* installation leads to inability of the *Access Manager* to display the objects, which are loaded from the *Intellect Server DB*, e.g. the lists of users and departments. In order to circumvent this issue, the distributed architecture administrator is recommended to do the following:

1. **On the computer with a *Client* installation:**
 - a. Install the SQL Server database server. Thus, the SQL Server on a computer with a *Client* installation will be able to connect to the SQL Server on the computer with an *Intellect Server* installation.
 - b. Ensure SQL Server authentication through the base **sa** account.
 - c. Ensure uninterrupted connection of the SQL Server on the computer with a *Client* installation to the SQL Server on the computer with the *Intellect Server* installation.
2. **On the computer with an *Intellect Server* installation and the *Access Manager* module:**
 - a. Configure SQL Server to allow remote connections.
 - b. Ensure SQL Server authentication through the base **sa** account.
 - c. Configure the *Intellect Server* connection to its database using the **idb.exe** utility. For this, you must perform the following actions:
 - i. Run the utility from the *Intellect Server* installation directory.



- ii. In the utility interface, click the **Configure** button (1). The database connection window will open.
- iii. In the **Select or enter a server name** field, type the name or IP address of the SQL server used to for database management (2).



Note

Please note that you must specify the explicit name or IP address of the machine on which the database is installed. The format (local)\SQLEXPRESS would be incorrect.

- iv. In the **Enter the information to log on to the server** settings section, check **Use a specific user name and password**. In the **User name** field enter **sa**. In the **Password** field, enter the password for the **sa** user. (3)



Note

Note that accounts other than **sa** are not allowed.

- v. Set the **Allow saving password** checkbox (4).



Note

This step is also mandatory.

- vi. Set the **Select the database on the server** selector and choose **intellect** from the drop-down list (5).
- vii. Click **OK** to save the connection settings (6). The parameters will be displayed in the **Connection string** field in **idb.exe** (7).
- viii. Click **OK** in **idb.exe** to save the changes.

Setting up the proper operation of the *Access Manager* module in a distributed architecture is complete.