ACFA Intellect

Access Manager Module Settings and Operation Guide

Last update 08/02/2022

Table of contents

1 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.

2 Access Manager Module Settings and Operation Guide. Introduction

On the page:

2.1 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.

2.2 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.

3 Licensing policy for Access Manager

If you acquire 1 license for this module, it will allow you to use any number of **Access Manager** objects on any number of computers (Servers/RAWs and Clients). The same license also opens **Access Manager reports** object under **Web Report System** object so that you could use corresponding reports after *Intellect Web Report System* installation (for more information, see the Intellect Web Report System. User Guide) . In addition, the license allows the use of all integrated control readers (see the Control Readers Settings Guide).

4 Configuration of the Access Manager module

4.1 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 **Operators'' permissions in AM** and **Type of department** sub-objects.

The *Access Manager* module is configured in the following order:

1. Procedure of configuring the Access Manager module
2. Rights for configuring and accessing objects in Access Manager
3. Configuring access cards
4. Configuring control readers in the Access Manager
5. Configuring the prohibition of new user parameter duplicates in Access Manager
6. Configuring the interaction with the FACE Intellect Face recognition server
7. Configuring fields displaying in user accounts

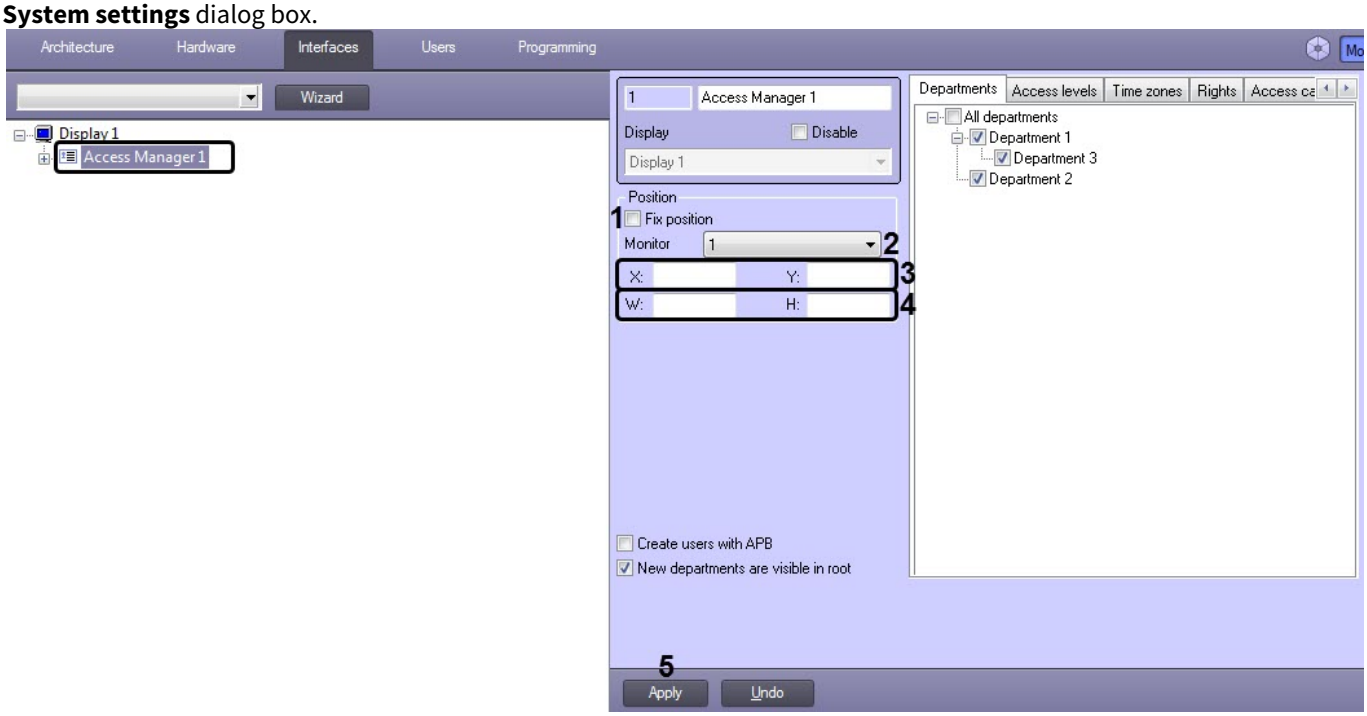
4.2 Configuring the position of the Access manager window on the screen

By default, the position of the **Access manager** window is not fixed on the screen and it can be changed. When setting up the system, you can specify the position of the **Access manager** window on the screen and eliminate the possibility to change it.

> **Note.**
>
> If you specify the fixed position of the **Access manager** window on the screen, the caption bar won't display which increases the displaying area of the **Access manager** window content.

To configure the position of the **Access manager** window on the screen, do the following:

1. Go to the settings panel of the **Access manager** object created under the **Display** object on the **Interfaces** tab of the **System settings** dialog box.



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

4.3 Rights for configuring and accessing objects in Access Manager

4.3.1 General information about rights for objects configuring and accessing in Access Manager

Specifying rights for objects configuring and accessing allows you to restrict actions available for operator of the *Access Manager* module while departments configuring, users, access levels, time zones, areas, and partitions. 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:

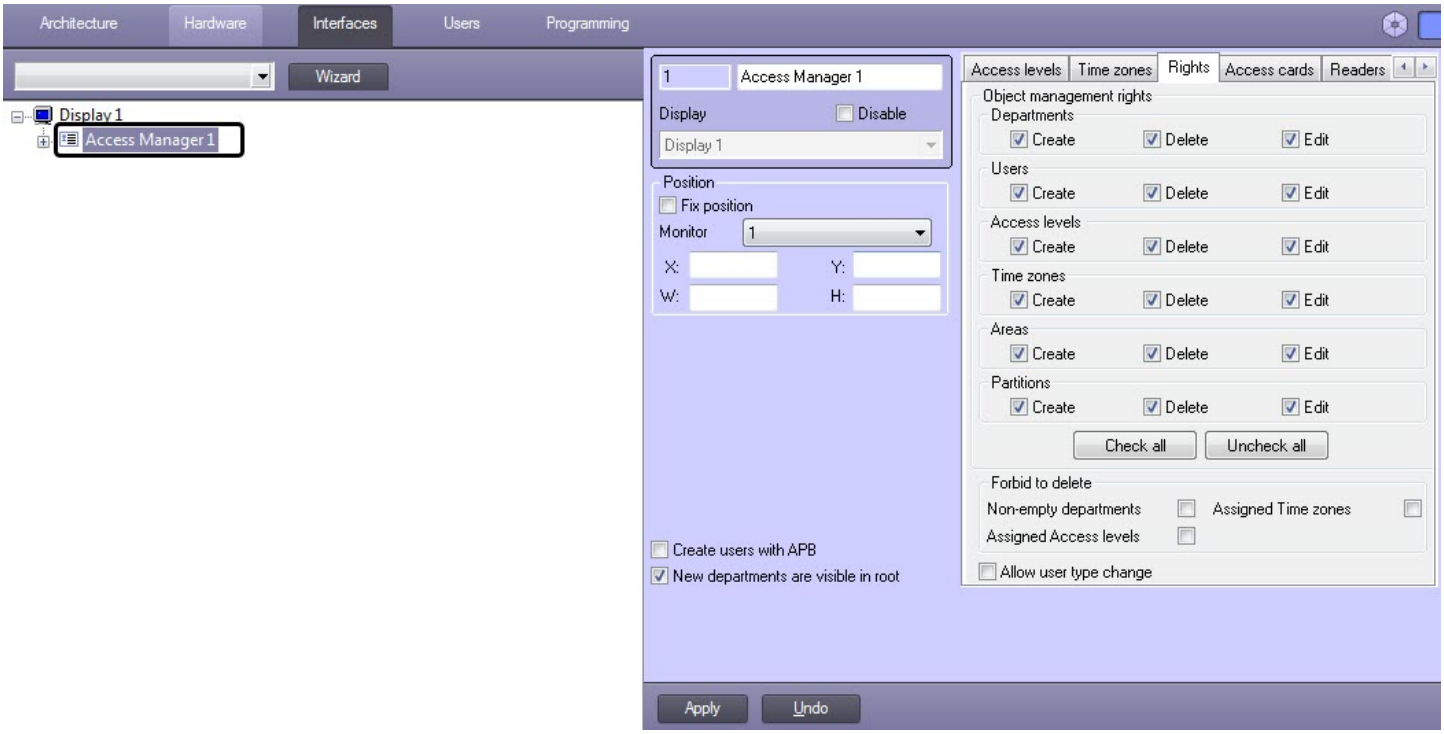
1. Create.
2. Edit.
3. Delete.

For departments, access levels and time zones, the permission to access these objects is additionally configured in the *Access Manager* module interface.

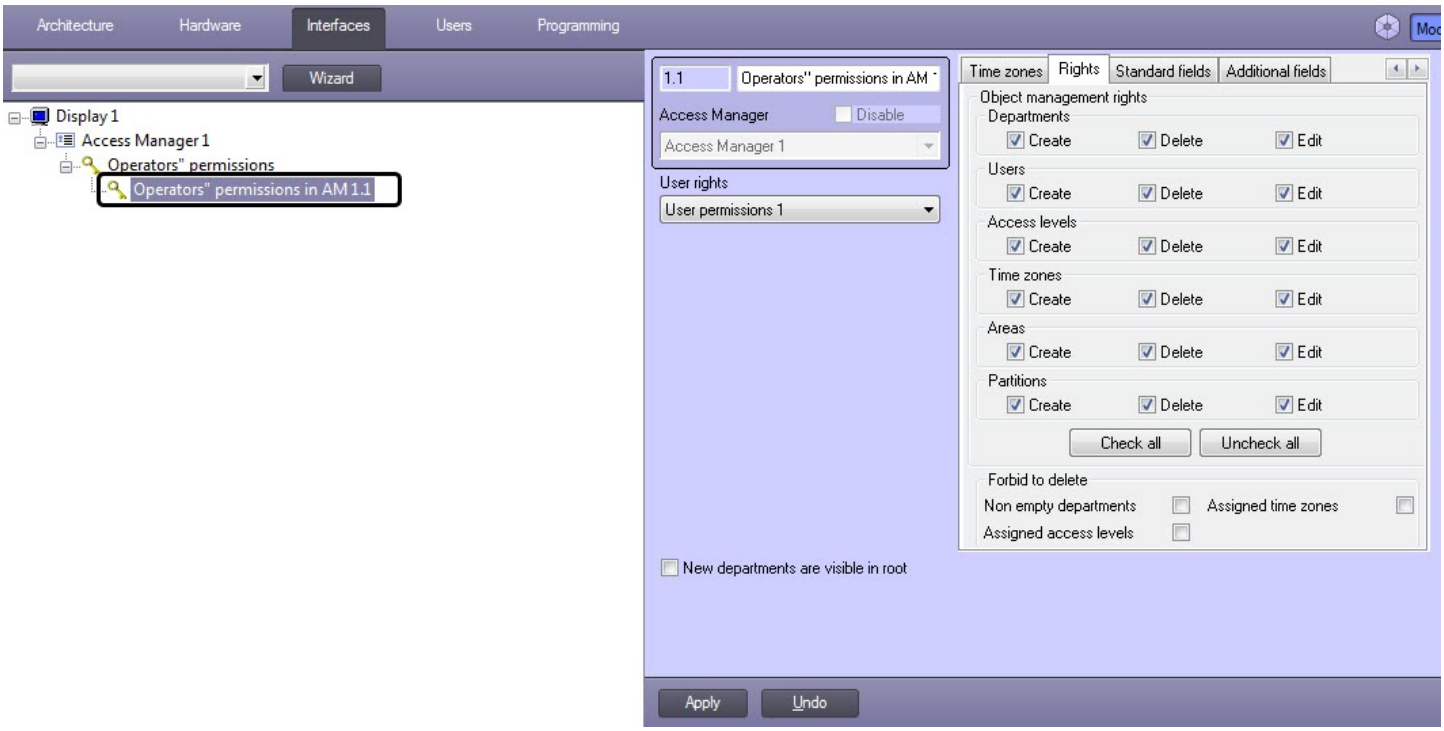
The *Access manager* software module allows you to set common and individual rights for objects configuring. By default, all of the above operations are prohibited in the *Access Manager* module.

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 configuration are specified on the **Rights** tab of the **Access Manager** object settings panel, which is created under the **Display** object on the **Interfaces** tab of the **System settings** dialog box.



Individual rights for objects configuring are specified on the **Rights** tab of the **Operators' permissions in AM** object settings panel, which is created on the basis of the **Access Manager** object.



4.3.2 Configuring the correspondence of operator permissions in Access Manager and in Intellect

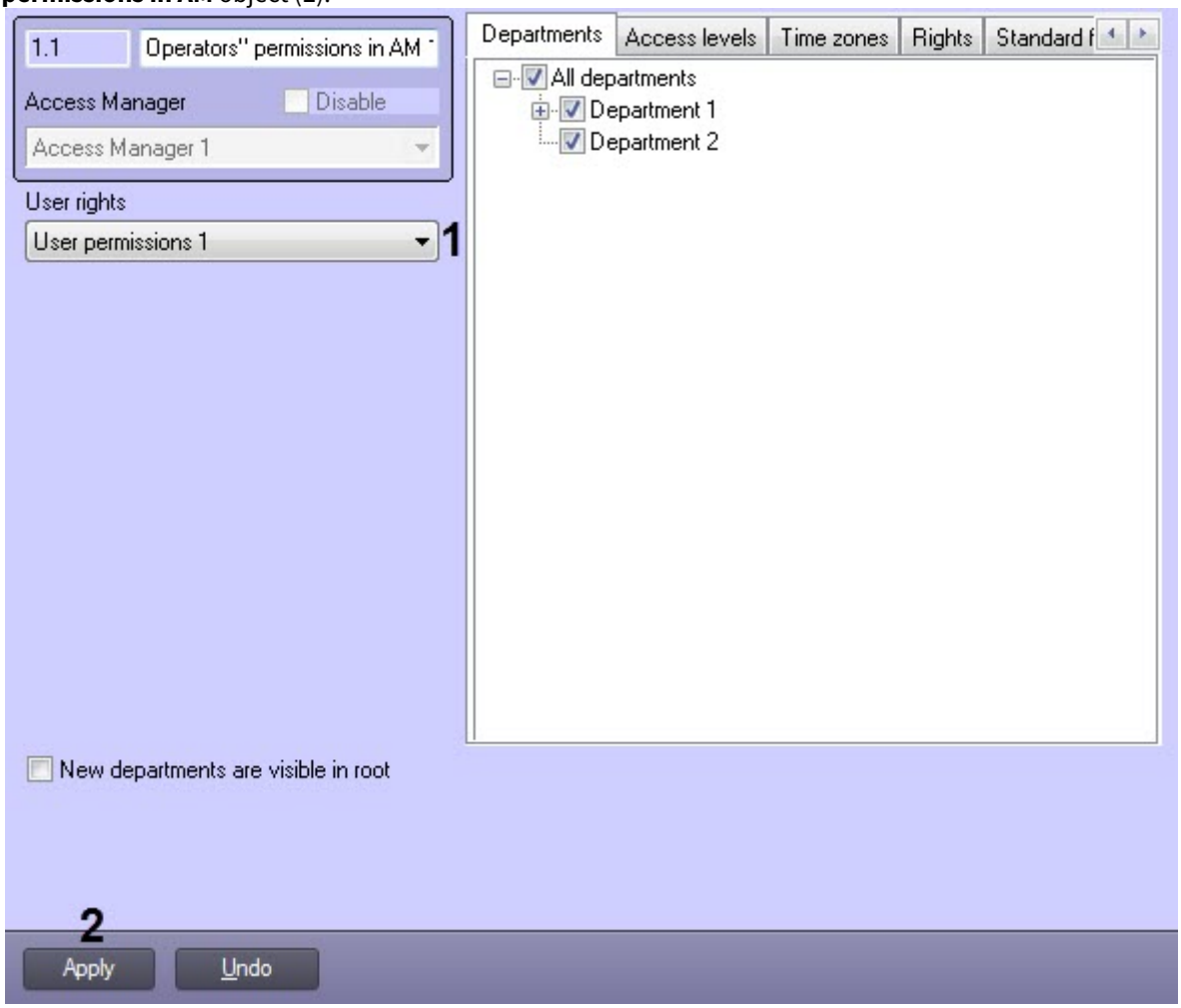
Individual rights for objects configuring in the *Access Manager* definitely correspond to user rights in the *ACFA Intellect* software package. So only one **Operators' permissions in AM** object can correspond to one **User permissions** object and vice versa.

> **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 **Operators' permissions in AM** object.

2. From the **User rights** drop-down list select the **User permissions** object which is required to match to the **Operators' permissions in AM** 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

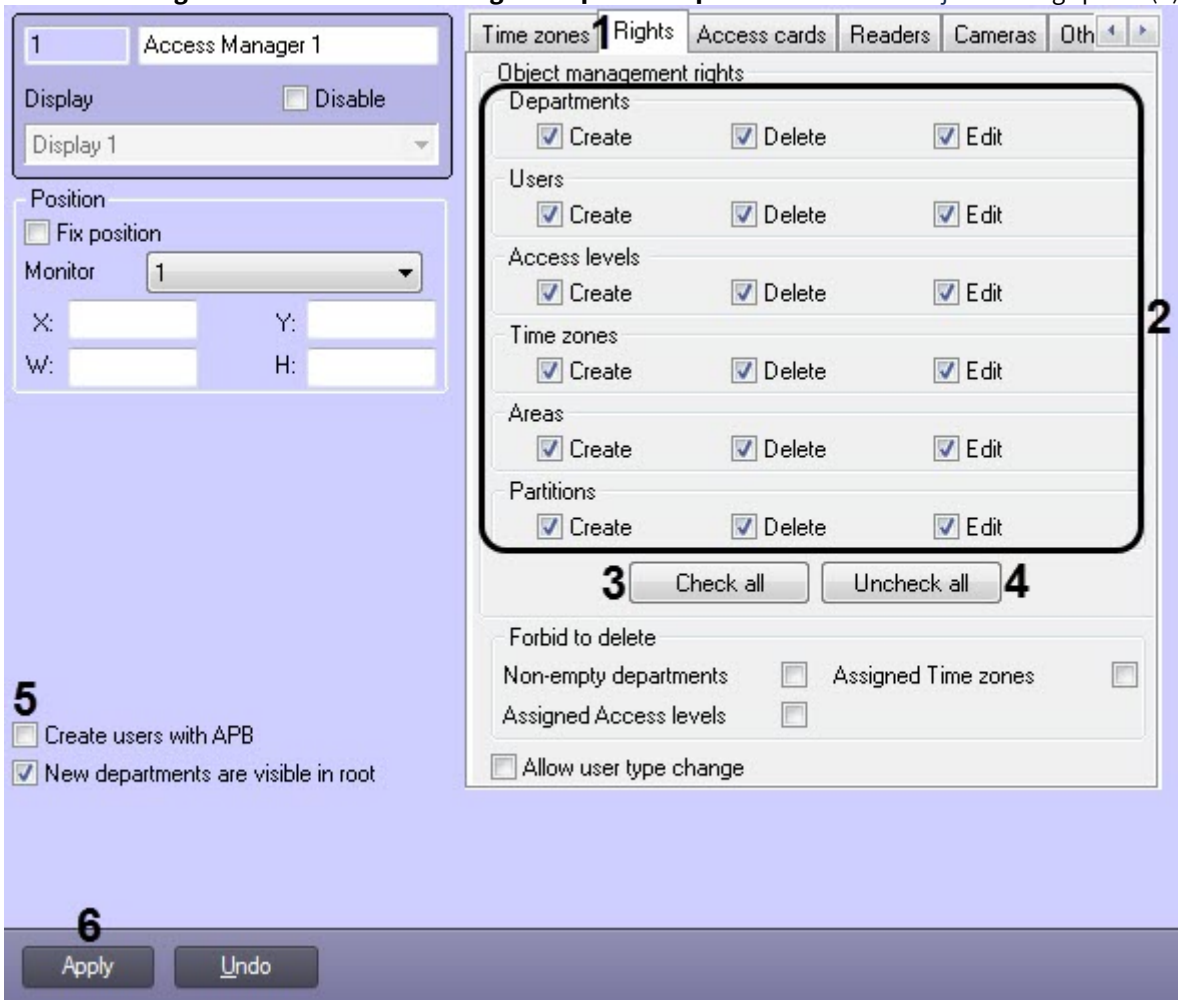
3. Click the **Apply** button (**2**).

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

4.3.3 Configuring the object management rights

Configure common or individual rights for managing objects as follows:

1. Go to the the **Rights** tab of the **Access Manager** or **Operators' permissions in AM** object settings panel (**1**).



2. In the **Departments**, **Users**, **Access levels**, **Time zones**, **Areas** and **Partitions** groups:
   a. Set the **Create** checkbox to allow the operators to create the corresponding objects in the **Access Manager** interface window.
   b. Set the **Delete** checkbox to allow the operators to delete the corresponding objects in the **Access Manager** interface window.
   c. Set the **Edit** checkbox to allow the operators to edit the corresponding objects in the **Access Manager** interface window.
3. Click the **Check all** button (**3**) to check all the boxes in the **Object management rights** group (**2**).
4. Click the **Uncheck all** button (**4**) to uncheck all the boxes in the **Object management rights** group (**2**).
5. If it is required to allow operators to create users with antipassback enabled, set the **Create users with APB** checkbox (**5**).

> **Note**
>
> The **Create users with APB** checkbox is available only on the **Access Manager** settings panel.

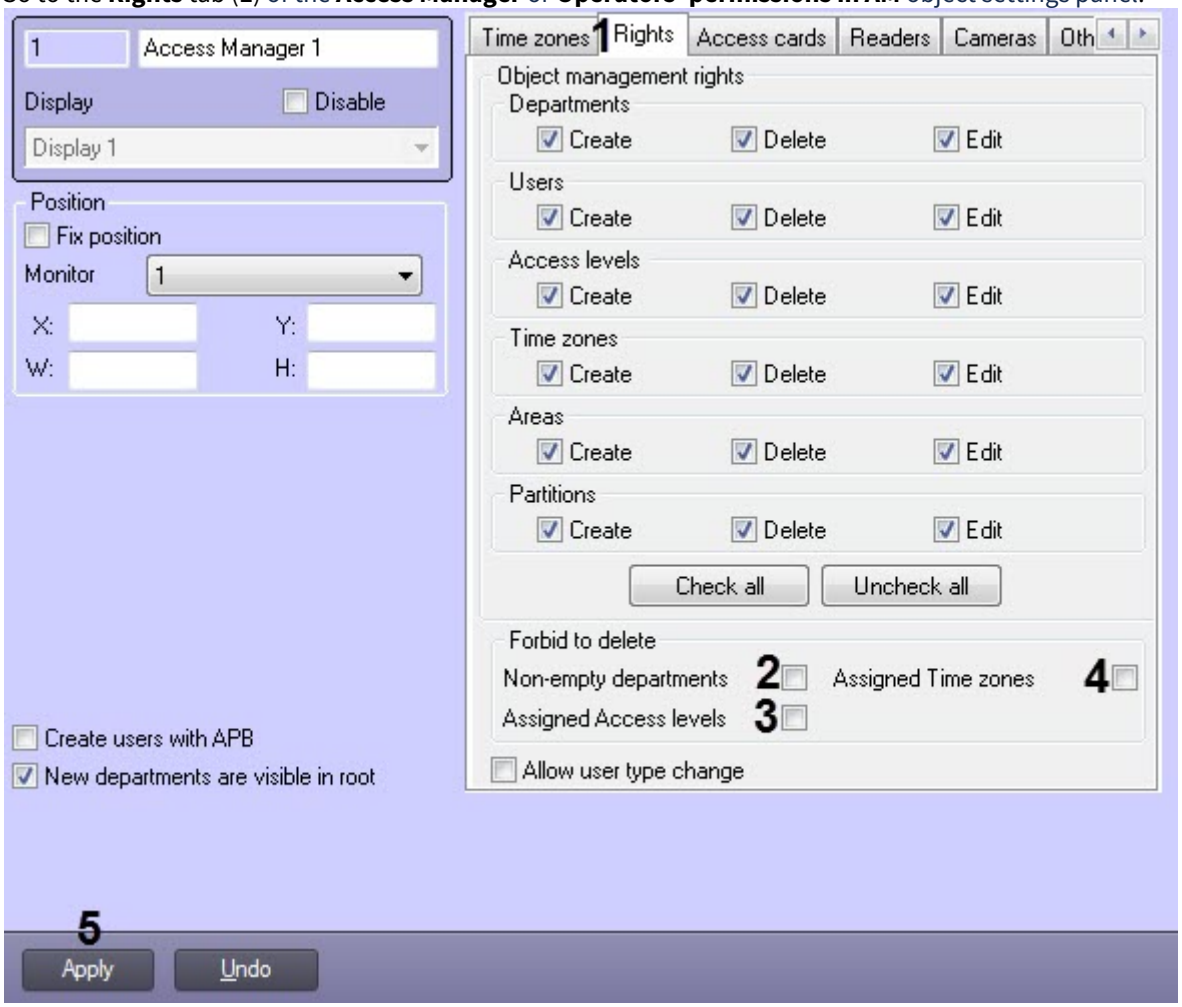
6. Click the **Apply** button (**6**) to save the changes.

The common or individual rights for managing objects are now configured.

4.3.4 Setting the prohibition of deleting non-empty departments, assigned ALs and TZs

Set the prohibition of deleting non-empty departments, assigned access levels (ALs) and time zones (TZs) as follows:

1. Go to the **Rights** tab (**1**) of the **Access Manager** or **Operators' permissions in AM** object settings panel.



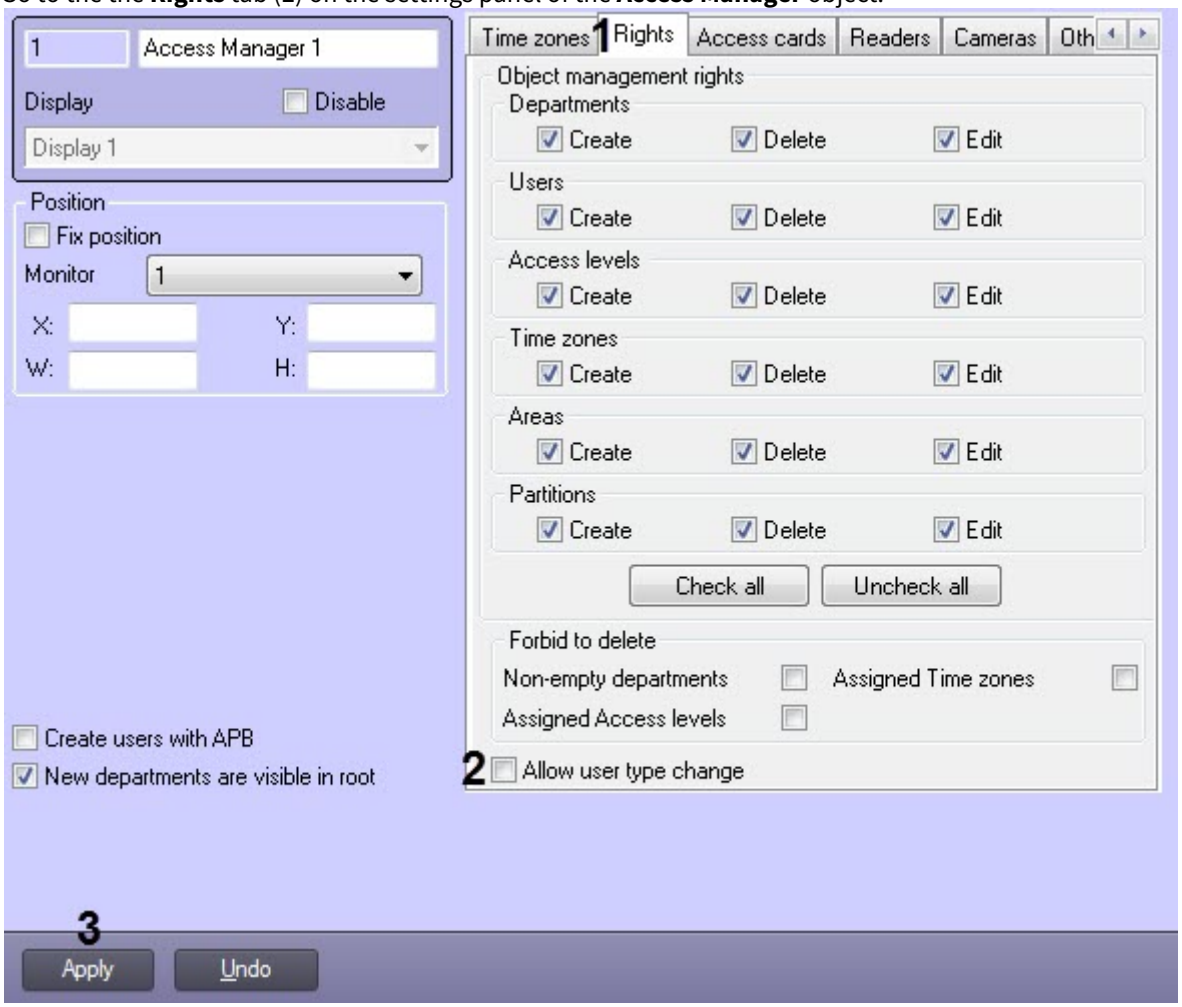
2. Set the **Non-empty departments** checkbox to forbid deletion of the departments in which there are users (**2**).
3. Set the **Assigned Access levels** checkbox to forbid deletion of the access levels assigned to departments or users (**3**).
4. Set the **Assigned Time zones** checkbox to forbid deletion of time zones used in access levels (**4**).
5. Click **Apply** to save settings (**5**).

Setting the prohibition of deleting non-empty departments, assigned ALs and TZs is completed.

4.3.5 Configuring the permission to change user type

The permission to change the user type is configured as follows:

1. Go to the the **Rights** tab (**1**) on the settings panel of the **Access Manager** object.



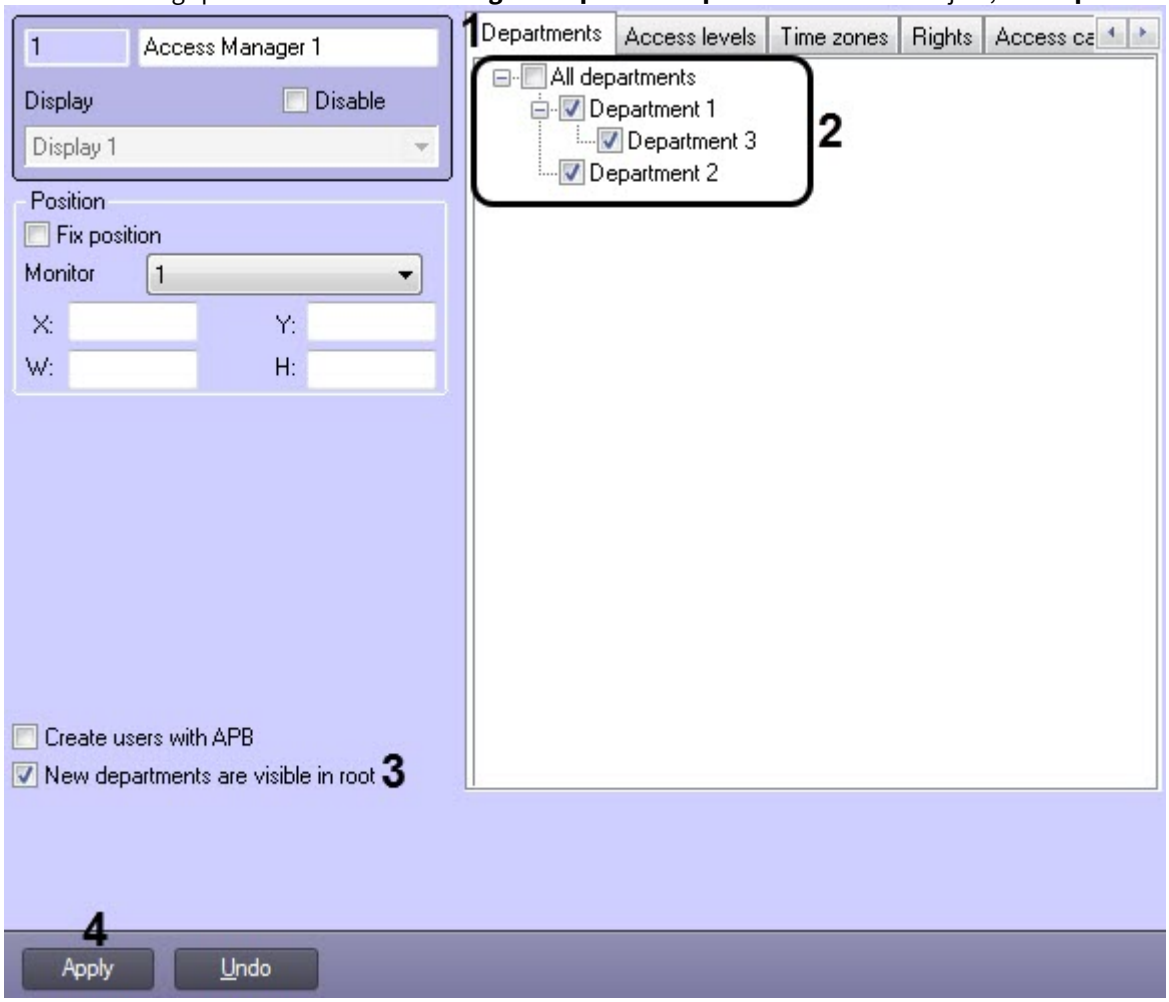
2. Set the **Allow user type change** checkbox (**2**) to enable the ability to change the user type (see Changing a user type).
3. Click the **Apply** button (**3**) to save the settings.

The permission to change user type is now configured.

4.3.6 Rights for accessing the departments in the Access Manager

To specify common or individual rights for accessing the departments, do the following:

1. Go to the settings panel of the **Access manager** or **Operators'' permissions in AM** object, the **Departments** tab (**1**).



2. Set checkboxes for the departments which should be available in the *Access Manager* interface module (**2**).
3. By default, new departments located 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 (**3**). 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.

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

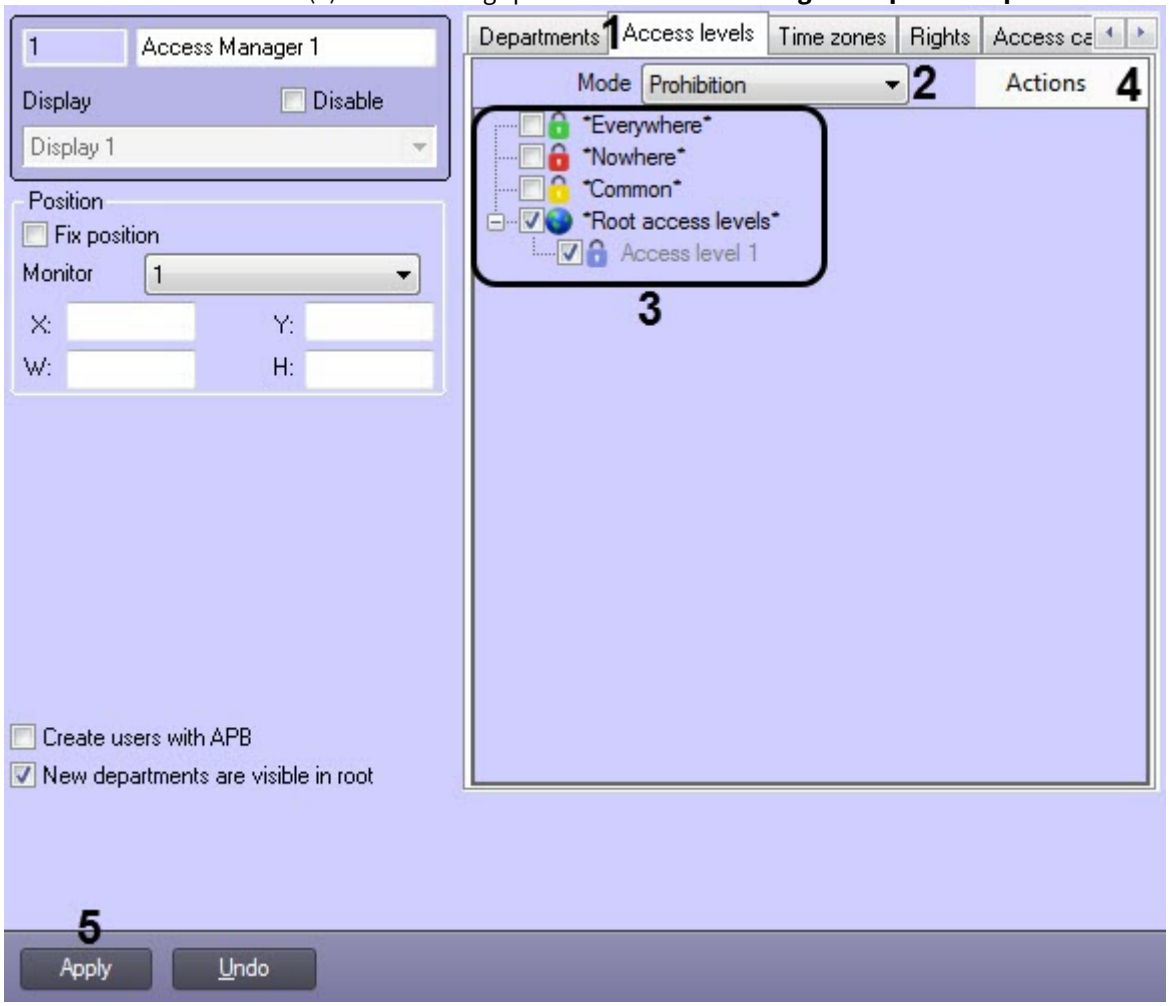
> **Note**
>
> New departments created via the *Access Manager* module on the basis of visible departments will be visible on default.

Specifying of common and individual rights for accessing the departments is completed.

4.3.7 Rights for accessing the access levels in Access Manager

To specify common or individual rights for accessing the access levels, do the following::

1. Go to the **Access levels** tab (**1**) on the settings panel of the **Access Manager** or **Operators' permissions in AM** object.



2. In the **Mode** drop-down list (**2**) select the required mode:
   - **Prohibition** - restrict the access
   - **Permission** - allow the access
3. Set the checkboxes (**3**) next to the required values:
   - **"Everywhere"** - access to the predefined access level "Everywhere".
   - **"Nowhere"** - access to the predefined access level "Nowhere".
   - **"Common"** - access inherited from the department access level.
   - **"Root access levels"** - set the checkbox to select all access levels in *Intellect* or expand the list and set the checkboxes only for the required access levels.

   > **Note**
   >
   > Use the **Actions** button (**4**) to select and deselect all items, minimize and expand all drop-down lists, and search for access levels or folders.

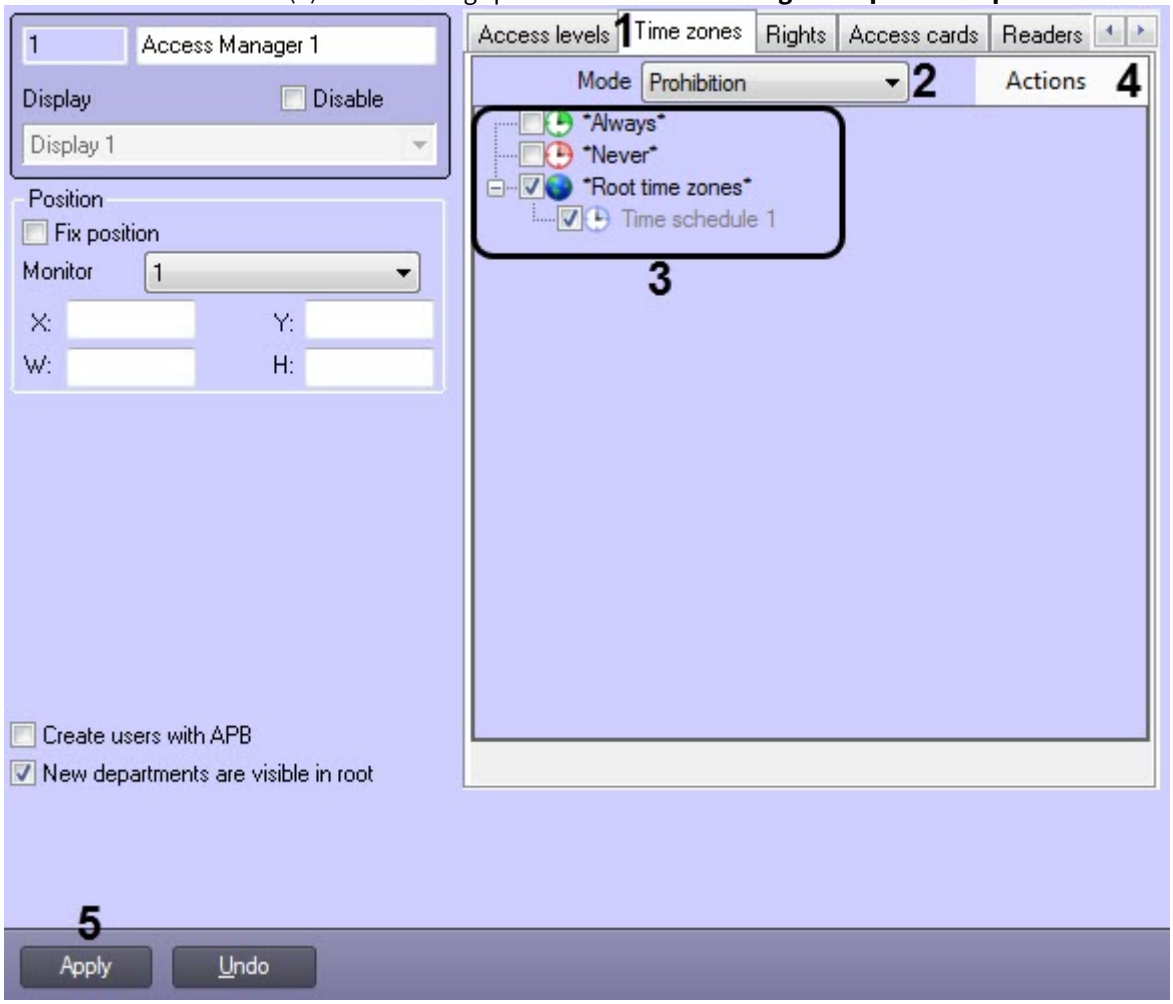
4. Click **Apply** to save settings (**5**).

Specifying common and individual rights for accessing the access levels is completed.

4.3.8 Rights for accessing the time zones in Access Manager

To specify common and individual rights for accessing the time zones, do the following:

1. Go to the **Time zones** tab (**1**) on the settings panel of the **Access Manager** or **Operators'' permissions in AM** object.



2. In the **Mode** drop-down list (**2**) select the required mode:
   - **Prohibition** - restrict the access.
   - **Permission** - allow the access.
3. Set the checkboxes (**3**) next to the required values:
   - **"Always"** - access to the predefined time zone "Always".
   - **"Never"** - access to the predefined time zone "Never".
   - **"Root time zones"** - set the checkbox to select all time zones in *Intellect* or expand the list and set the checkboxes only for the required time zones.

   > **Note**
   >
   > Use the **Actions** button (**4**) to select and deselect all items, minimize and expand all drop-down lists, and search for time zones or folders.

4. Click **Apply** to save settings (**5**).

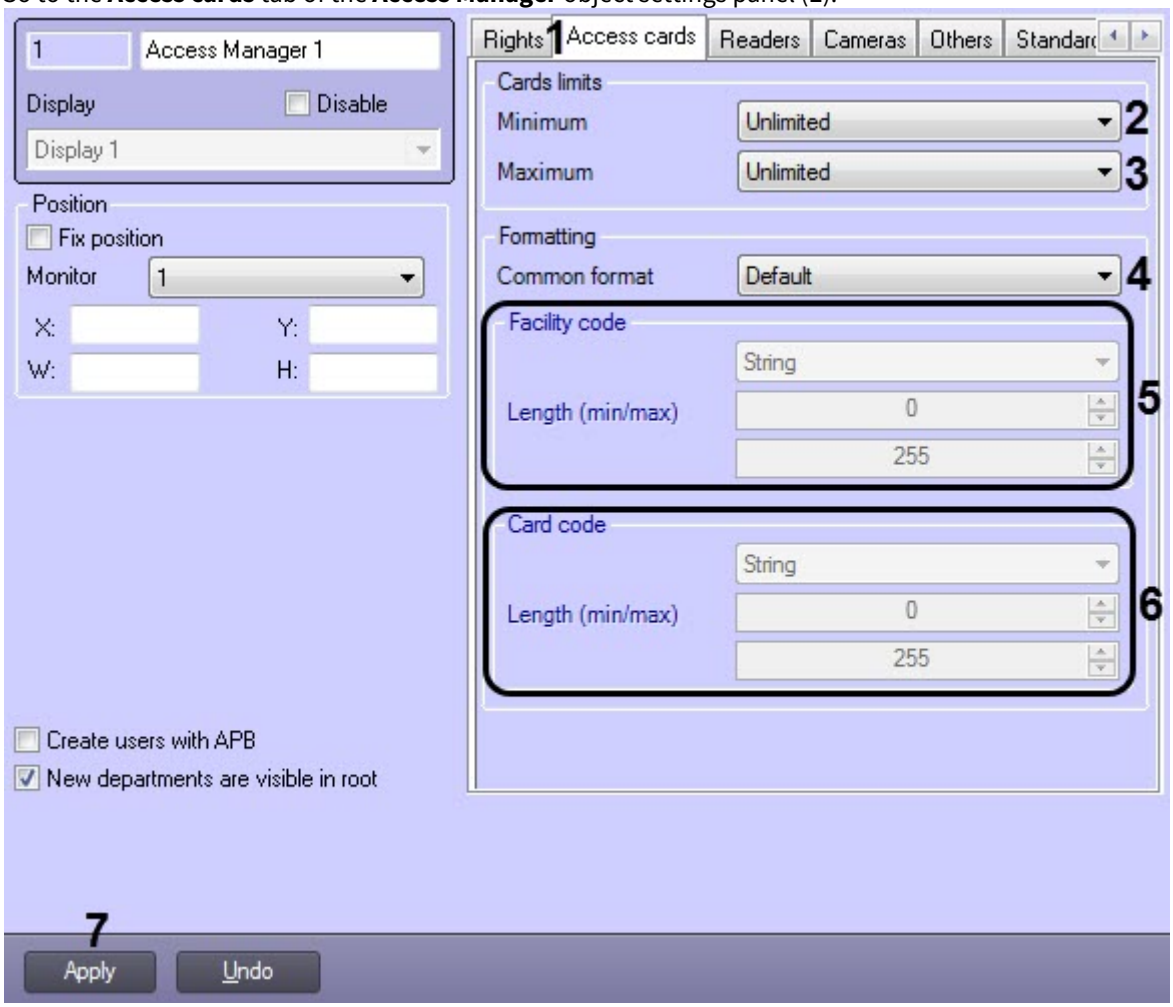
Specifying common and individual rights for accessing the time zones is completed.

4.4 Configuring access cards

Configuring access cards allows you to set the required number and format of user access cards (see Assigning an access card to a user).

Access cards are configured as follows:

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



2. In the **Cards limits** group from the **Minimum** drop-down list (**2**), select the minimum number of access cards that should be assigned to the user.
   - from **1** to **5** - if the specified number of access cards is not assigned to the user, then this user cannot be saved in the **Access Manager** interface object.
   - **Unlimited** - an unlimited number of access cards can be assigned to the user.
   - **Prohibited** - the user cannot be assigned access cards. Buttons and functional menu for assigning access cards will be inactive in the **Access Manager** interface object.
3. In the **Cards limits** group from the **Maximum** drop-down list (**3**), select the maximum number of access cards that should be assigned to the user.
   - from **1** to **5** - if the user is assigned more than the specified number of access cards, then this user cannot be saved in the **Access Manager** interface object.
   - **Unlimited** - an unlimited number of access cards can be assigned to the user.
   - **Prohibited** - the user cannot be assigned access cards. Buttons and functional menu for assigning access cards will be inactive in the **Access Manager** interface object.

   > **Note**
   >
   > - If at least one **Minimum** or **Maximum** parameter has the **Prohibited** value, the buttons and the functional menu for assigning access cards in the **Access Manager** interface object will be inactive.
   > - If the **Prohibited** value is set, and the user is assigned an access card without using the **Access Manager** interface window (see Appendix 2. Configuring a visitor management system without the Access Manager interface window), then this user cannot be saved in the **Access Manager** interface object until the card is removed from them.

4. In the **Formatting** group from the **Common format** drop-down list (**4**) select the access cards format:

Attention!

If the following access cards restrictions are violated, the user cannot be saved in the **Access Manager** interface object.

- **Default** - allows setting an arbitrary value for the facility code and card code. Any letters, numbers and symbols are allowed except: <| >.
- **Wiegand26** - allows entering a 1-byte facility code (from 0 to 255), and a 2-byte card code (from 0 to 65535).
- **Wiegand32** - allows entering a 2-byte facility code (from 0 to 65535), and a 2-byte card code (from 0 to 65535).
- **Wiegand26** (code only) - the facility code cannot be set, only a 3-byte card code is set (from 0 to 16777215).
- **Wiegand32** (code only) - the facility code cannot be set, only a 4-byte card code is set (from 0 to 4294967295).
- **TouchMemory** - the facility code cannot be set, only the 8-byte card code is set. The format is hexadecimal, characters A, B, C, D, E, F are allowed. The code should be 8 characters or longer. If the entered card code is less than 8 characters long, the the higher order digits are filled with zeros.
- **Hikvision** - the *Hikvision* ACS format. It always has a fixed H character in the facility code. The card code is specified by a string with a maximum length of 32 characters.
- **Configurable** - allows setting the parameters of the facility code (**5**) and card code (**6**).
  - **Fixed character** - the specified single character will always be hard-coded, which cannot be changed in the **Access Manager** interface object.
  - **String** - allows entering a string of 0 to 255 characters.
  - **Numeric** - allows entering only numbers from 0 to 4294967295.
  - **Hexadecimal** - allows entering numbers in HEX format (numbers and symbols A, B, C, D, E, F) from 0 to 8 bytes long.
  - **Fixed number** - similar to **Fixed character**, but instead of a character, a number between 0 and 4294967295 is used.
  - **Regular template** - allows defining an access card template with specified restrictions, lengths and value ranges.

    Note

    An example of some service characters for regular expressions:
    - **^** is the beginning of the regular expression. A line opening.
    - **$** is the end of the regular expression. A line closing.
    - **.** is any single character.

    On the site https://regex101.com you can find a complete list of service characters for regular expressions, as well as to check the accuracy of a regular expression.

    Example 1:
    For the facility code, it is necessary to limit the range of entered numbers from 1 to 3. The amount of numbers should be not more than 4. Other characters and numbers are not allowed.
    Template:

    ```
    ^[1-3]{4}$
    ```

    Example 2:
    For a card code, it is necessary to limit the code length to 8 characters, at least 1 character for input. In this case, it is allowed to enter uppercase Latin letters A, B, C, D, E, F.
    Template:

    ```
    ^[(A-F),(0-9)]{1,8}$
    ```

5. Click the **Apply** button (**7**) to save the settings.

Configuring access cards is complete.

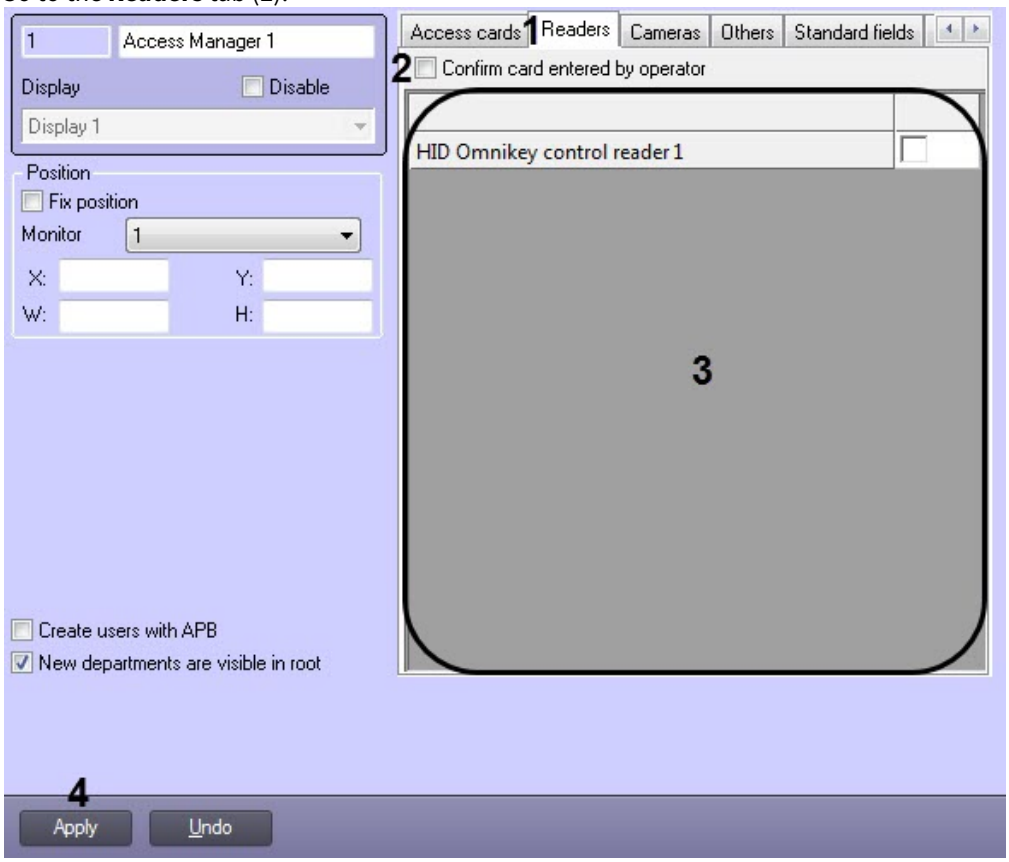
4.5 Configuring control readers in the Access Manager

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

> **Note**
>
> Any reader from the ACS integration modules (see ACS integration modules), FSA/ACS (see ACFA Systems integration modules) can act as a control reader, as well as the control readers themselves from the control reader integration modules (see Control Readers Settings Guide).

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**).



3. Set the **Confirm card entered by operator** checkbox (**2**) if it's required that operator confirms assigning of access cards to user.
4. Set checkboxes for those readers which should be available in the **Access Manager** window while access cards or biometric data input (**3**).
5. To save changes click the **Apply** button (**4**).

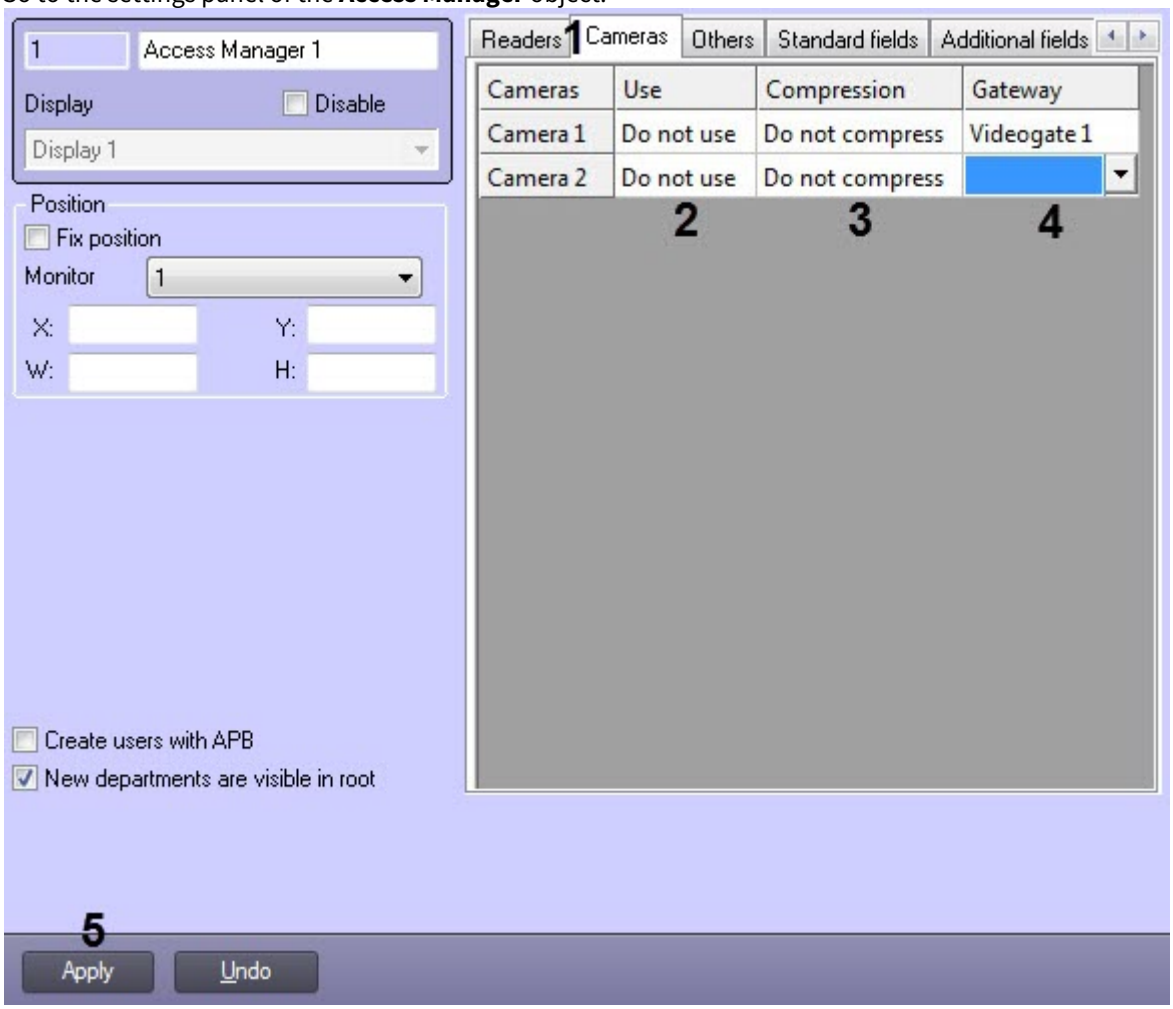
Configuring a control readers in the *Access Manager* is completed.

4.6 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.



2. Go to the **Cameras** tab (**1**).
3. In the **Use** column, from the drop-down list, select the camera stream (**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.

4. In the **Compression** column, from the drop-down list, select the video stream compression level (**3**).
5. If video from camera is to be received using videogate, select the required **Videogate** object from the drop-down list in the **Gateway** column (**4**).

> **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.

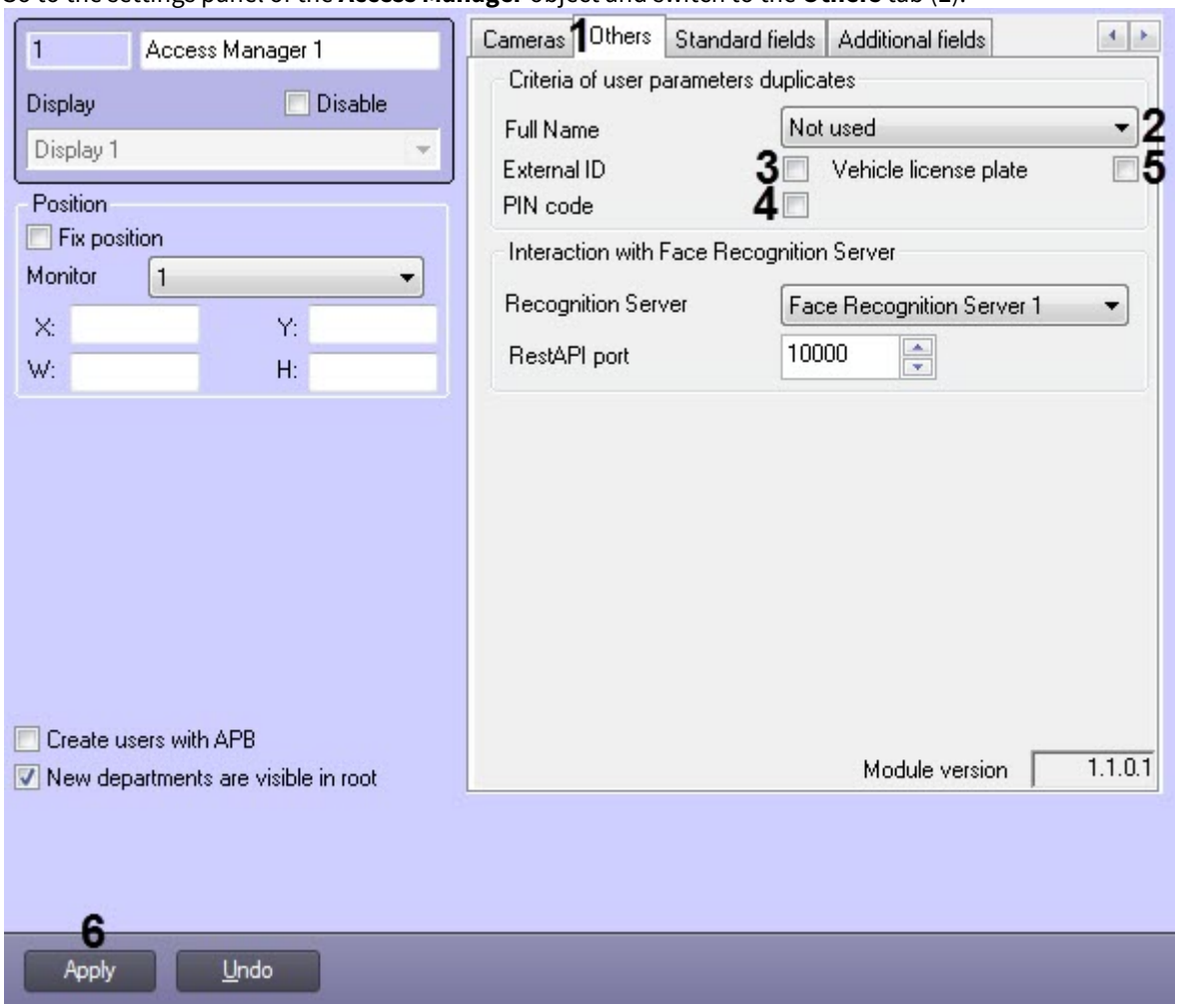
6. To save changes click the **Apply** button (**5**).

Selecting of available cameras is completed.

4.7 Configuring the prohibition of new user parameter duplicates in Access Manager

Configure the prohibition of duplicate parameters for new users as follows:

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



2. From the **Full Name** drop-down list (2) select a method for identifying duplicate user records:
   a. **Not used** – it's accepted to add users with equal full name.
   b. **Surname, name** – it's forbidden to add users with equal name and surname even if patronymic is differed.
   c. **Surname, name, patronymic** – it's forbidden to create users with equal full name.
3. Set the **External ID** checkbox if you want to forbid creating users with the same external identifiers (**3**).
4. Set the **PIN code** checkbox if you want to forbid creating users with the same PIN codes (**4**).
5. Set the **Vehicle license plate** checkbox if you want to forbid creating users with the same vehicle plate numbers (**5**).
6. To save changes click the **Apply** button (**6**).

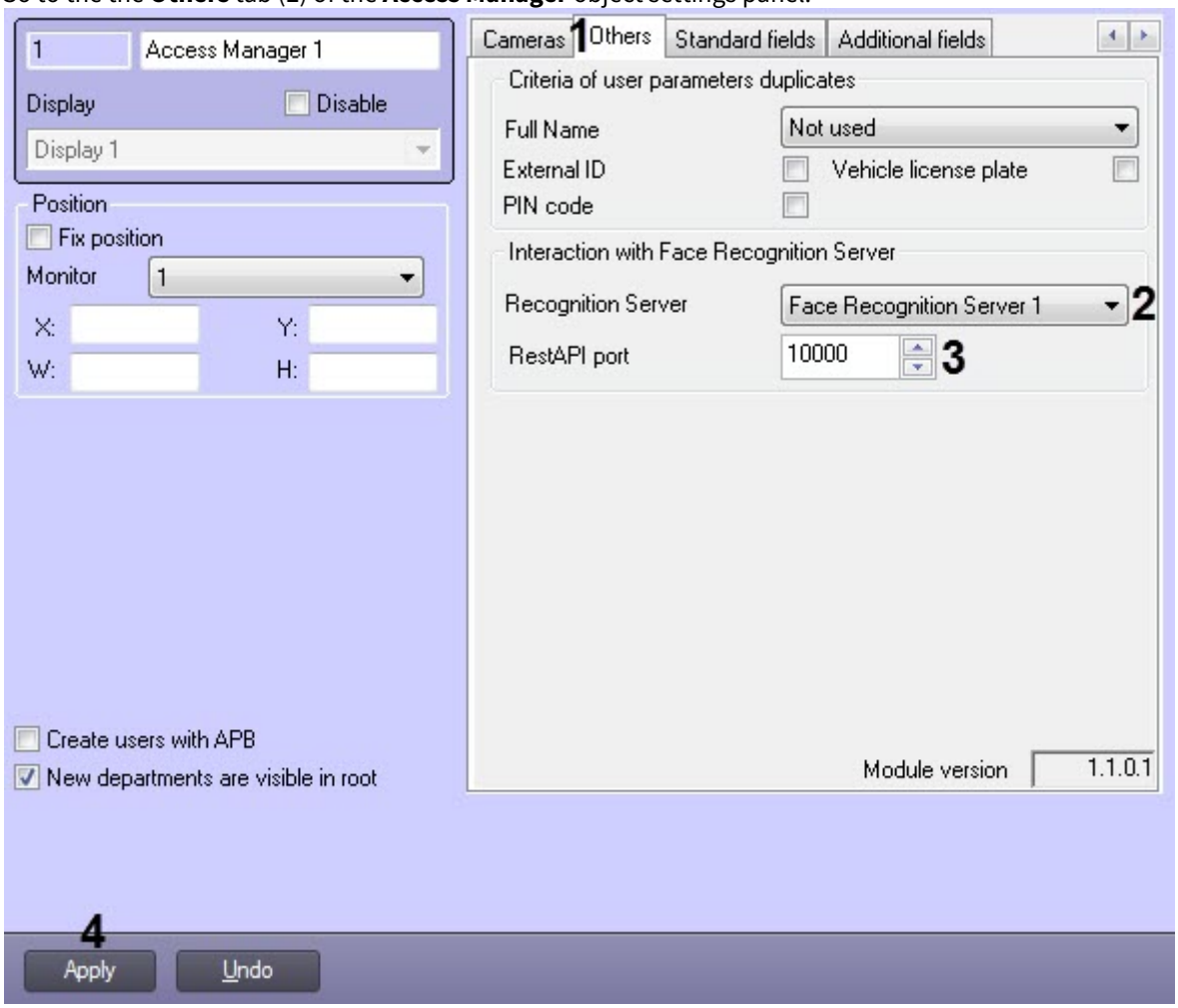
Configuring the prohibition of duplicate parameters for new users is completed.

4.8 Configuring the interaction with the FACE Intellect Face recognition server

Configuring the interaction with the *FACE Intellect* Face recognition server allows to check the quality of a recognized face before assigning it to the user.

The interaction with the Face recognition server is configured as follows:

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



2. From the **Recognition Server** drop-down list (**2**), select the Face Recognition Server (for details, see Face-Intellect. Administrator Guide), which will check the quality of photos that are being added.
3. In the **RestAPI port** field (**3**), specify the port used for connecting to the Face Recognition Server. The default value is **10000**.
4. Click the **Apply** button (**4**) to save the settings.

The interaction with the *FACE Intellect* Face recognition server is now configured.

4.9 Configuring fields displaying in user accounts

4.9.1 Configuring Main department type

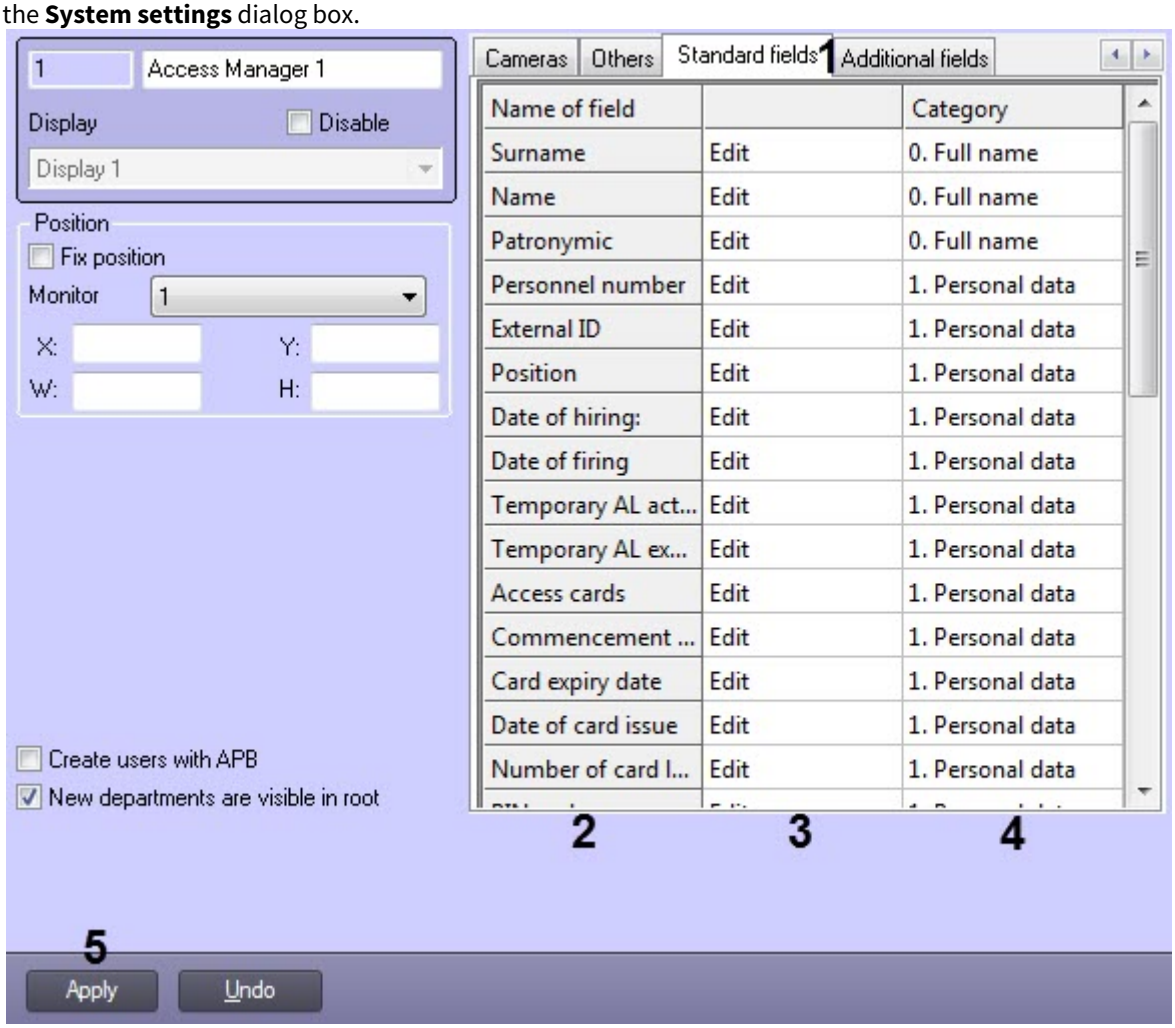
The **Main** department type defines fields of the user profile available in **Access Manager** for view and edit by default.

> **Note.**
>
> Fields visibility can also be restricted by **Type of department** and/or **Operators' permissions in AM** objects – see Configuring a type of department in the Access Manager and Configuring availability of fields depending on operator rights in the Access Manager.

> **Note.**
>
> Fields visibility configured in the **Main** type of department is applied if **Main** type is selected for the department while editing in the **Access Manager** (see Editing a department).

Configure the Main department type as follows:

1. Go to the **Access manager** object settings panel. The object is created under the **Display** object on the Interfaces tab of the **System settings** dialog box.



2. Go to the **Standard fields** or **Additional fields** tab (**1**).
3. Available fields are shown in the **Name of field** column (**2**).

> **Note.**
>
> See Setting user parameters for details on the fields.

4. Set visibility and editability of each field as necessary. For that:
   a. Select one of the following values in the (**3**) column:

Value	Description
Hidden	The field is not displayed in the list while editing or viewing user
Read only	The field is displayed in the list while editing or viewing user but is not editable
Edit	The field is displayed in the list while editing or viewing user band is editable. *Note. The **Card issued by** and **Access level assigned by** fields are always not editable as so as these fields are automatically filled with the name of the Operator assigning/changing card or access level.*

   b. Enter name of the group to display the field in the list of user's parameters in the **Access Manager** interface window in the **Category** column (**4**). Category name is arbitrary. If it is not specified, the parameter is shown in **Other** group.

> **Note.**

Categories are sorted alphabetically. Use number prefixes in the name to set strict order of sorting.

5. Click **Apply** to save settings (**5**).

Configuring the **Main** department type is completed.

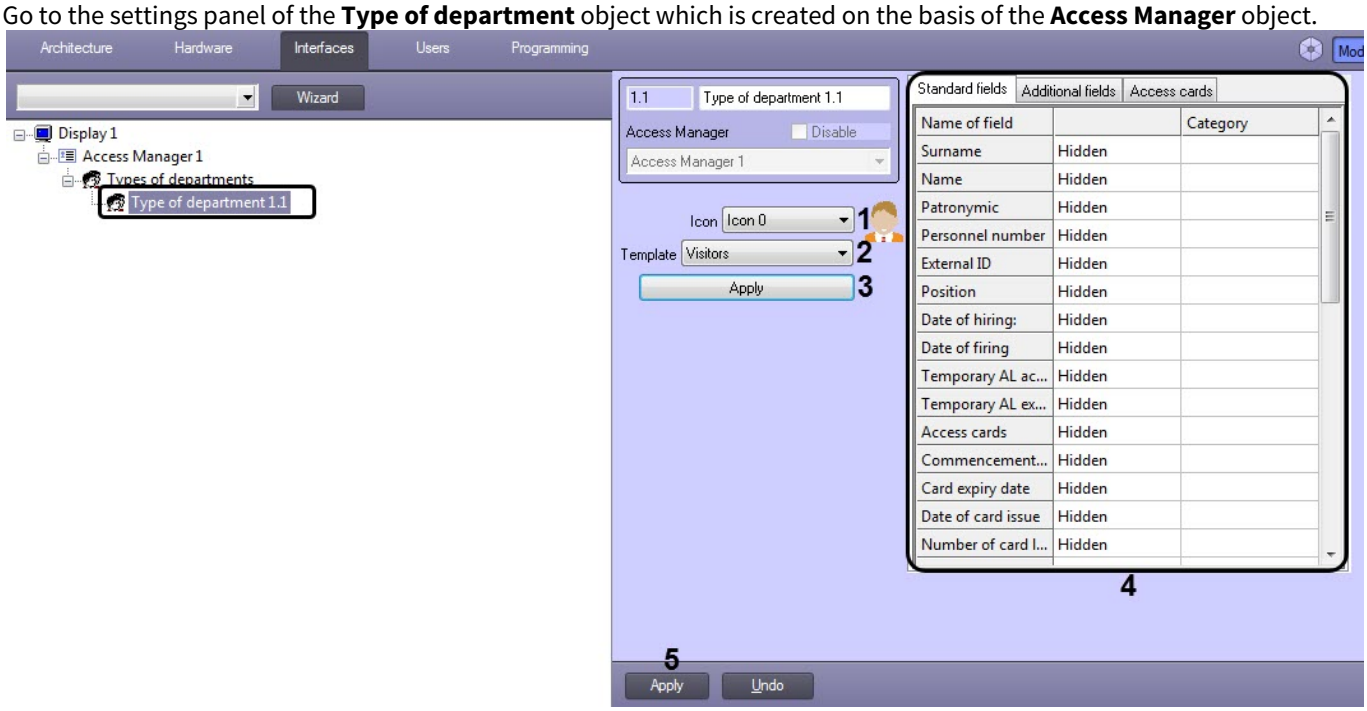
4.9.2 Configuring a type of department in the Access Manager

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

> **Note**
>
> Visibility of fields is defined by operator rights – see the Configuring availability of fields depending on operator rights in the Access Manager section.

To configure type of department, do the following:

1. Go to the settings panel of the **Type of department** object which is created on the basis of the **Access Manager** object.



2. From the **Icon** drop-down list (**1**) select the icon for displaying of department in the **Access Manager** window.
3. 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 (**2**) 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 (**3**). As a result values in correspondence with the selected template will be displayed in the **Standard fields** and **Additional fields** tabs.

> **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.

4. If it's required to set visibility and availability for required fields editing manually, do the following:
   a. In the column (**4**) 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.

> **Note**
>
> See also the description of fields in the Setting user parameters section.

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. 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.

5. If it is necessary for this type of department to have its own parameters of access cards, make the appropriate settings on the **Access cards** tab (**4**) (for details, see Configuring access cards).
6. To save changes, click the **Apply** button (**5**).

Configuring of department type is completed.

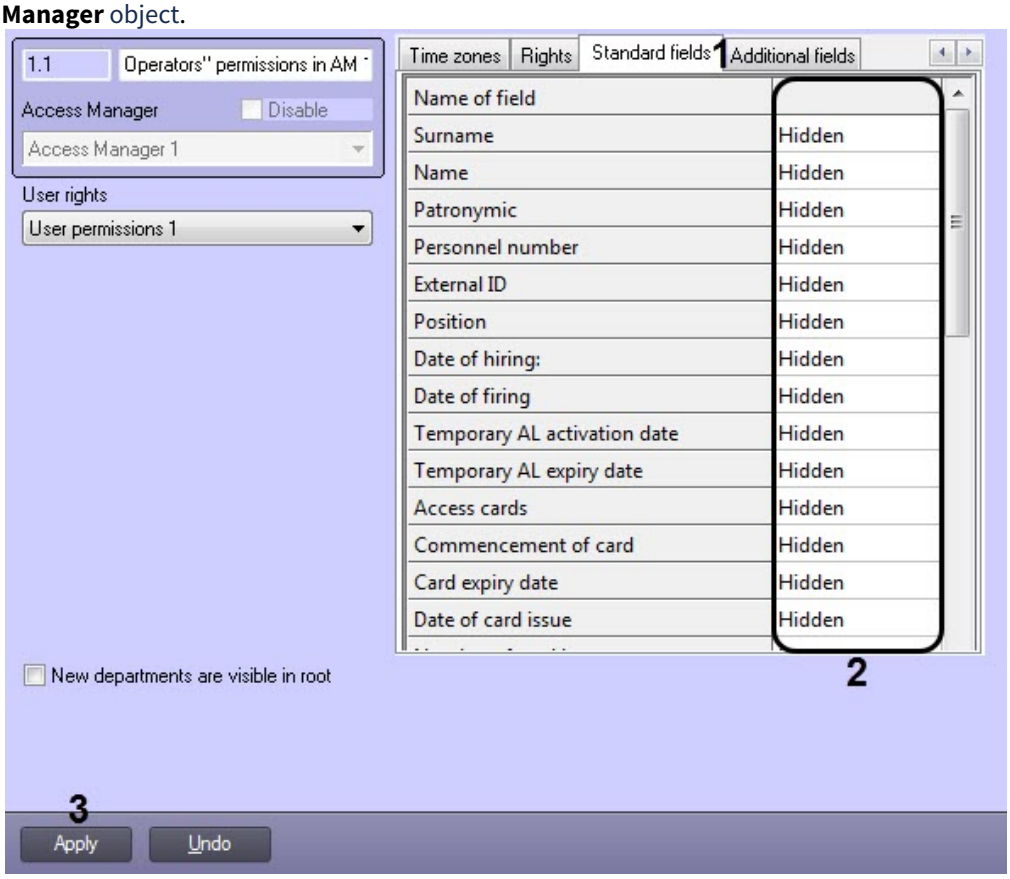
4.9.3 Configuring availability of fields depending on operator rights in the Access Manager

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 **Operators'' permissions in AM** object, which is created on the basis of the **Access Manager** object.



2. Select the required tab: **Standard fields** or **Additional fields** (**1**). By default, all user fields are hidden.

> **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:

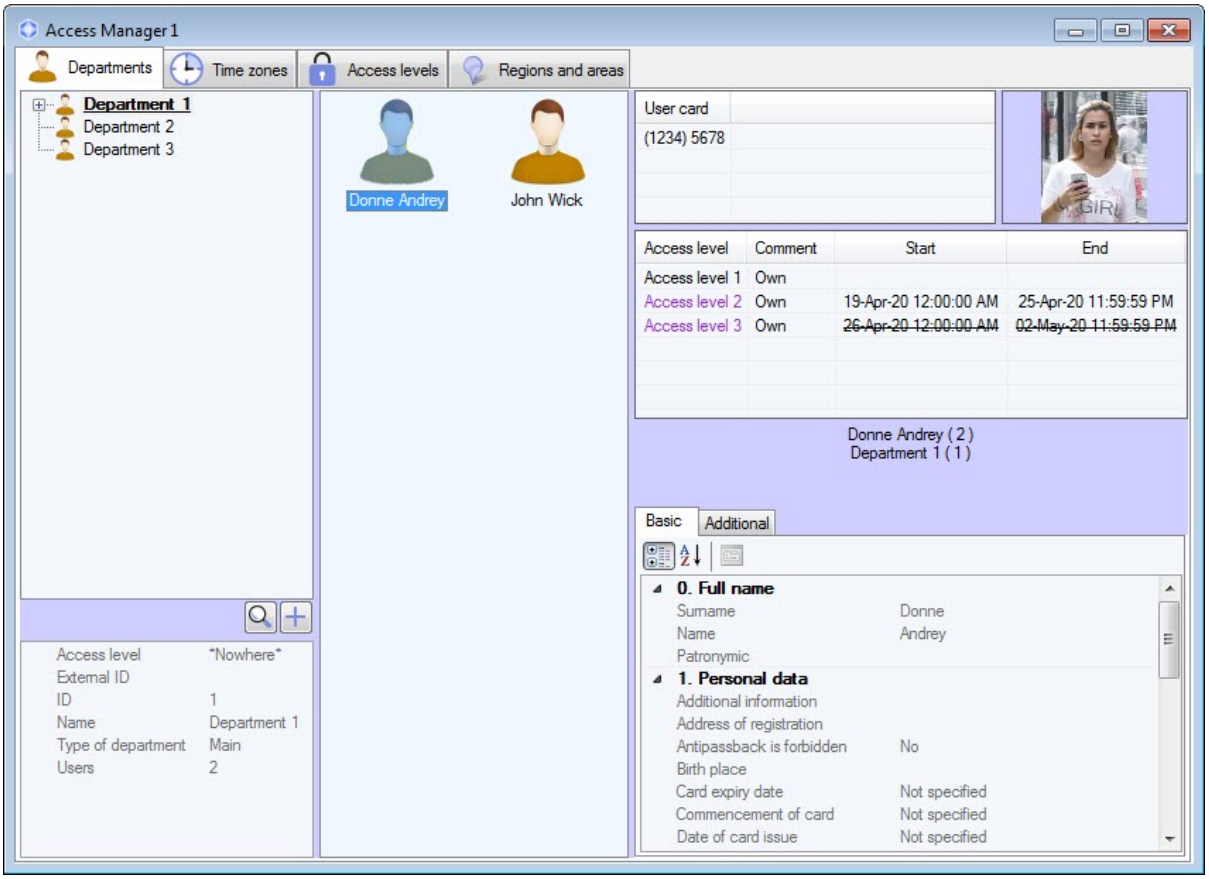
Value	Description
Hidden	The field is not displayed in the list of user parameters while viewing and editing
Read only	The field is displayed in the list of user parameters while viewing and editing but is not available for editing
Edit	The field is displayed in the list of user parameters while viewing 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.

5 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.

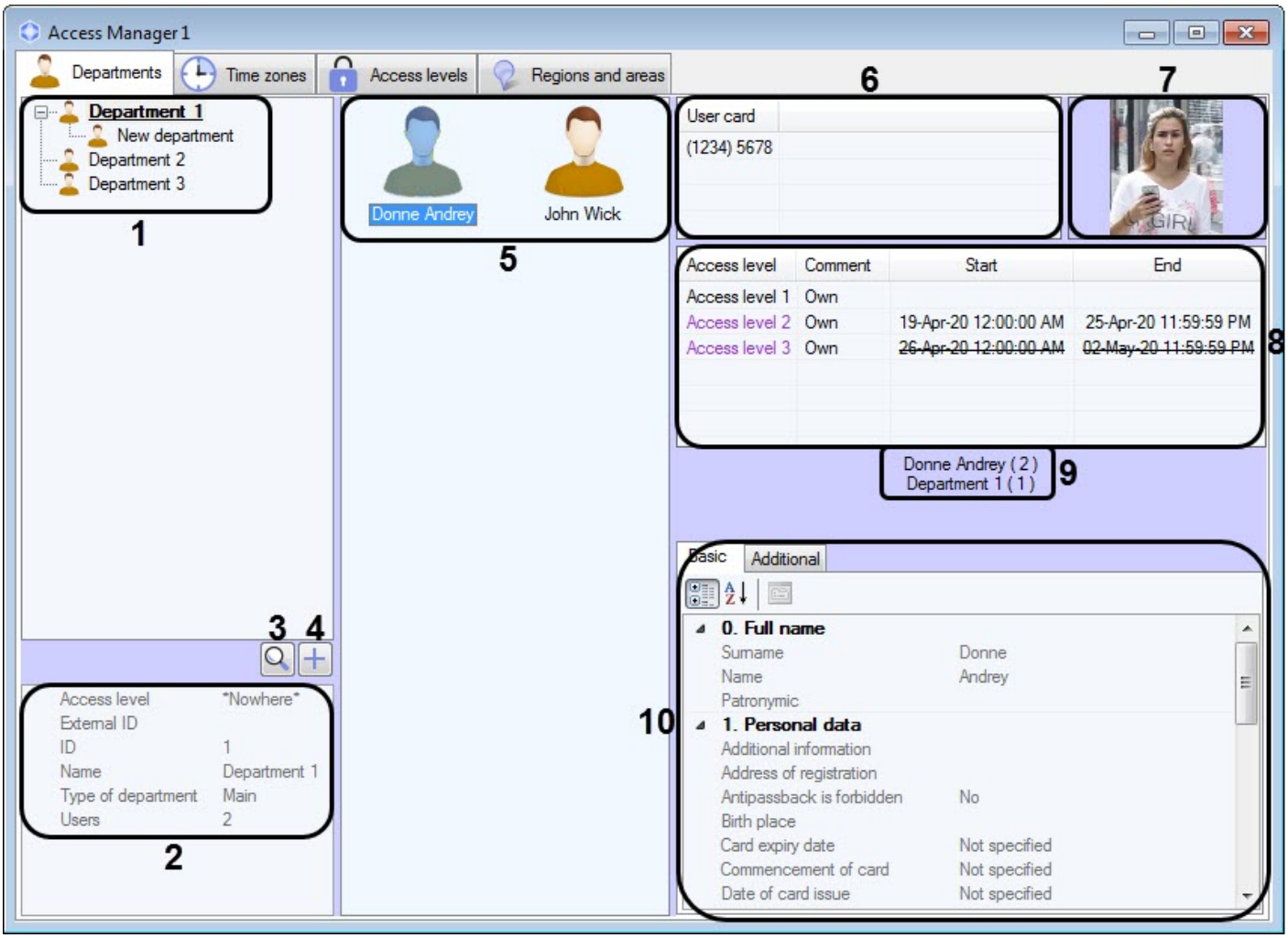
The **Access Manager** window contains three tabs:

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

Description of each tab is follows.

5.1 Departments tab

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



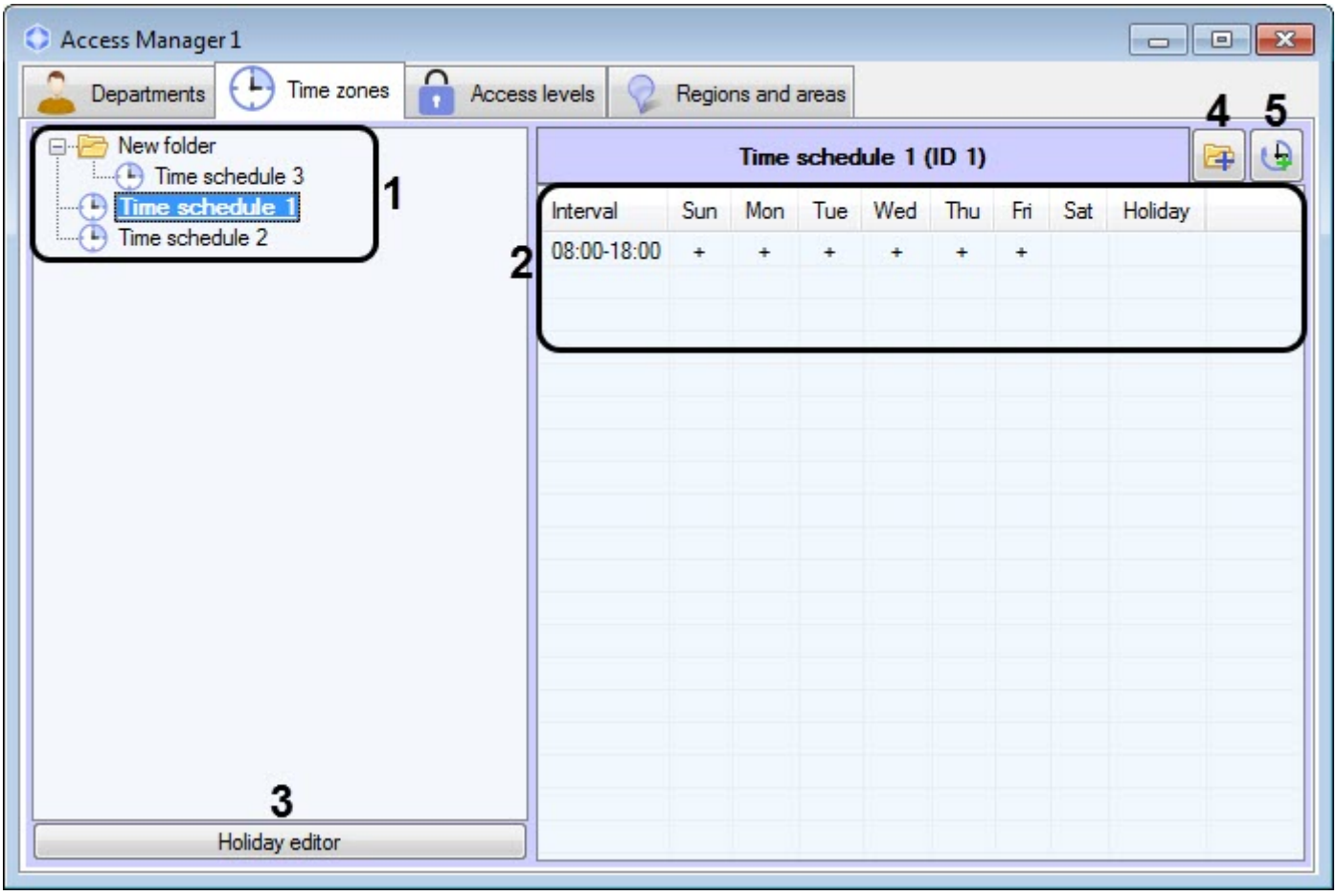
Description of **Departments** tab elements is given in the table.

№	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 accessing the 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. Temporary access levels are highlighted in color, and the date and time of validity of the temporary access level will be displayed in the **Start** and **End** columns next to them. The crossed out date and time of the temporary access level validity indicate that this temporary access level is not valid at the moment. 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.

5.2 Time zones tab

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



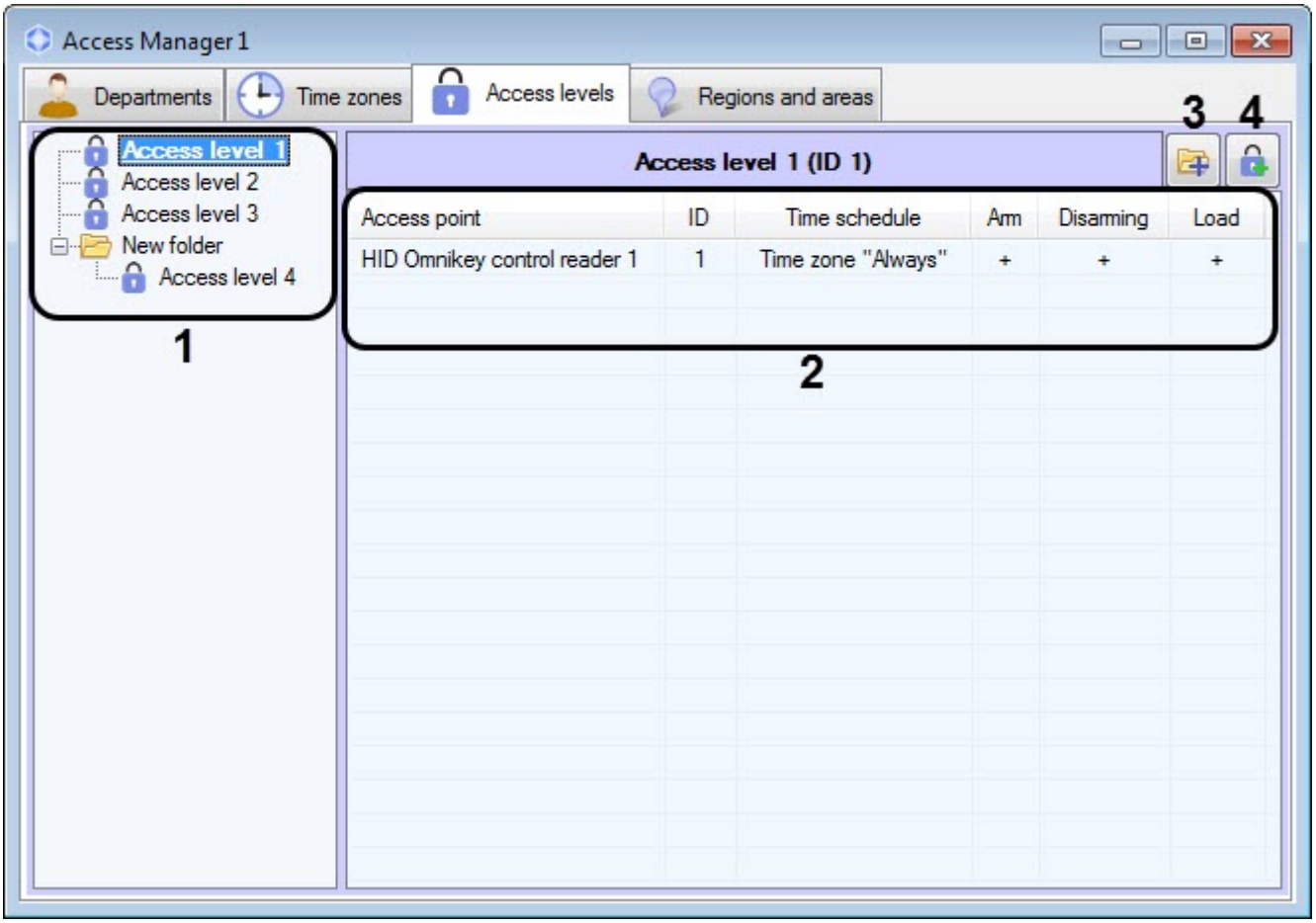
Description of **Time zones** tab elements is given in the table.

№	Element	Description
1	List of time zones and folders	Names of time zones and folders 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.
4	Create a folder in root	Button opening a window for creating a folder in the root - see the Managing the list of time zones section.
5	Create a time zone in root	Button opening a window for creating a time zone in the root - see the Creation of a time zone in the Access Manager software module section.

5.3 Access levels tab

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



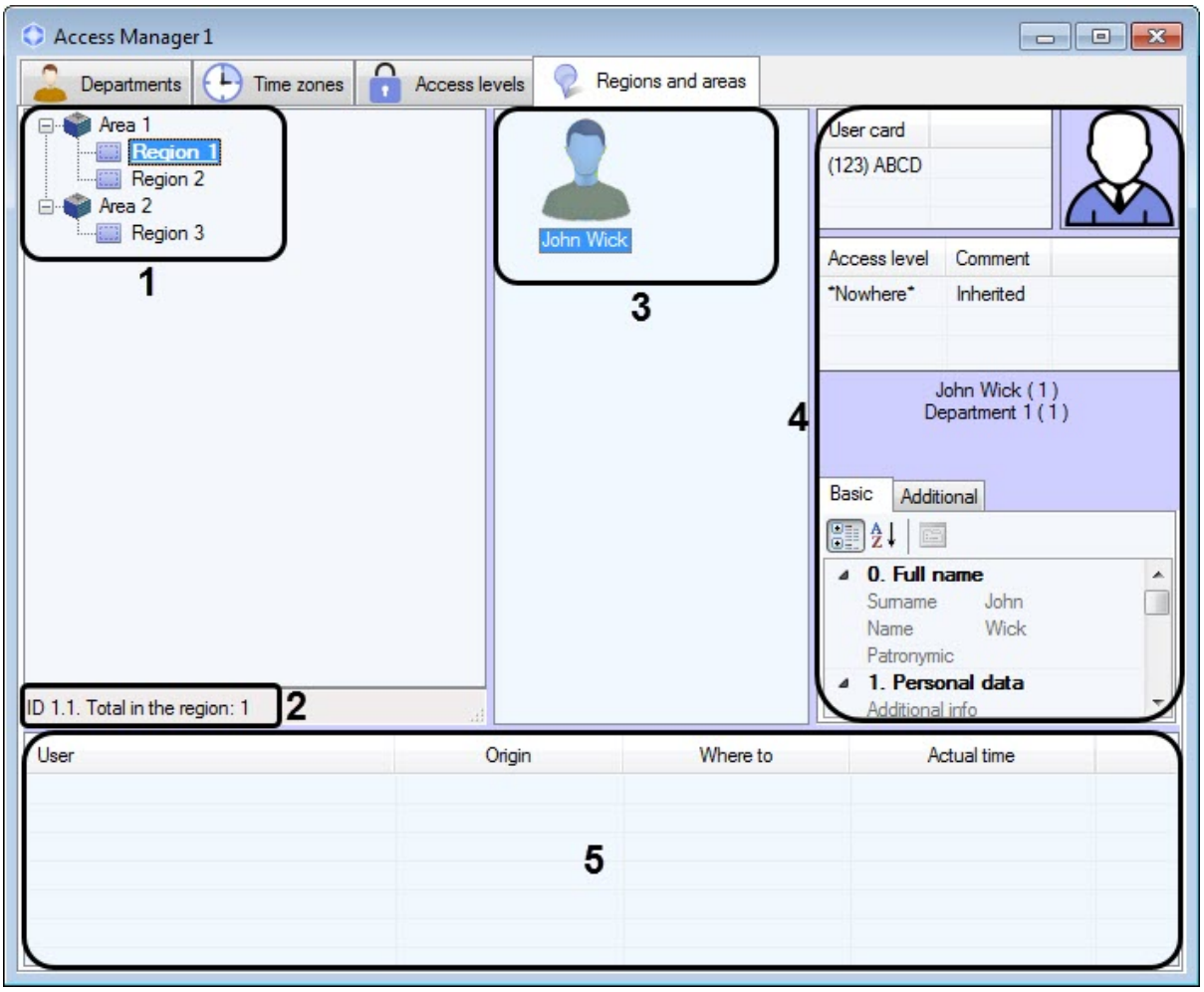
Description of **Access levels** tab elements is given in the table.

№	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.
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.
4	Create a folder in root	Button opening a window for creating a folder in the root - see the Managing the list of time zones section.
5	Create a time zone in root	Button opening a window for creating a time zone in the root - see the Creation and deletion of a time zone in the Access Manager software module section.

5.4 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	User parameters	See the Departments tab section.

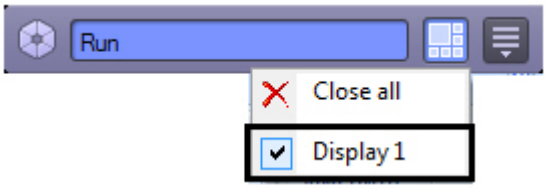
5	Passes log	Displaying information on users' passages in real time.

6 Working with the Access Manager software module

6.1 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.

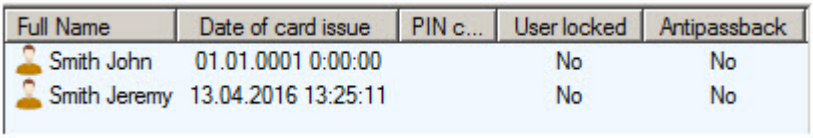
6.2 General operations with the Access Manager interface elements

6.2.1 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.

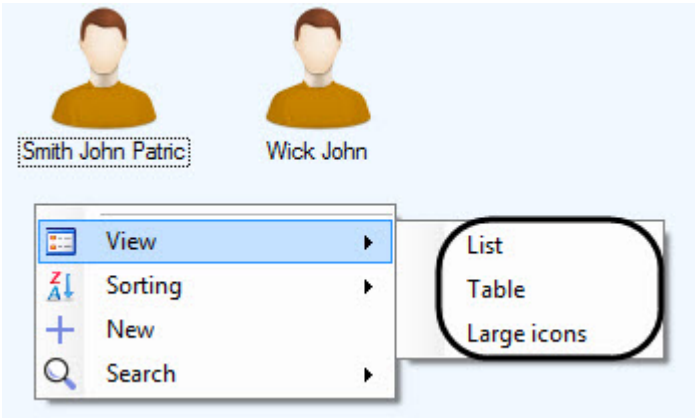
2. Table.



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 or any user.

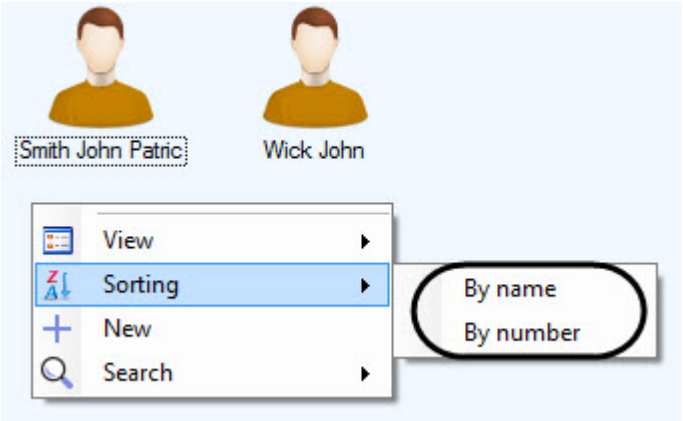


6.2.2 Selecting a way of sorting objects in the list

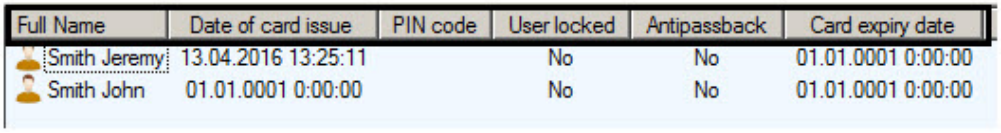
In the *Access Manager* software module it's possible to select the following ways of sorting user lists, time zones and access levels if the **List** or **Large icons** view is selected:

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 or any user.



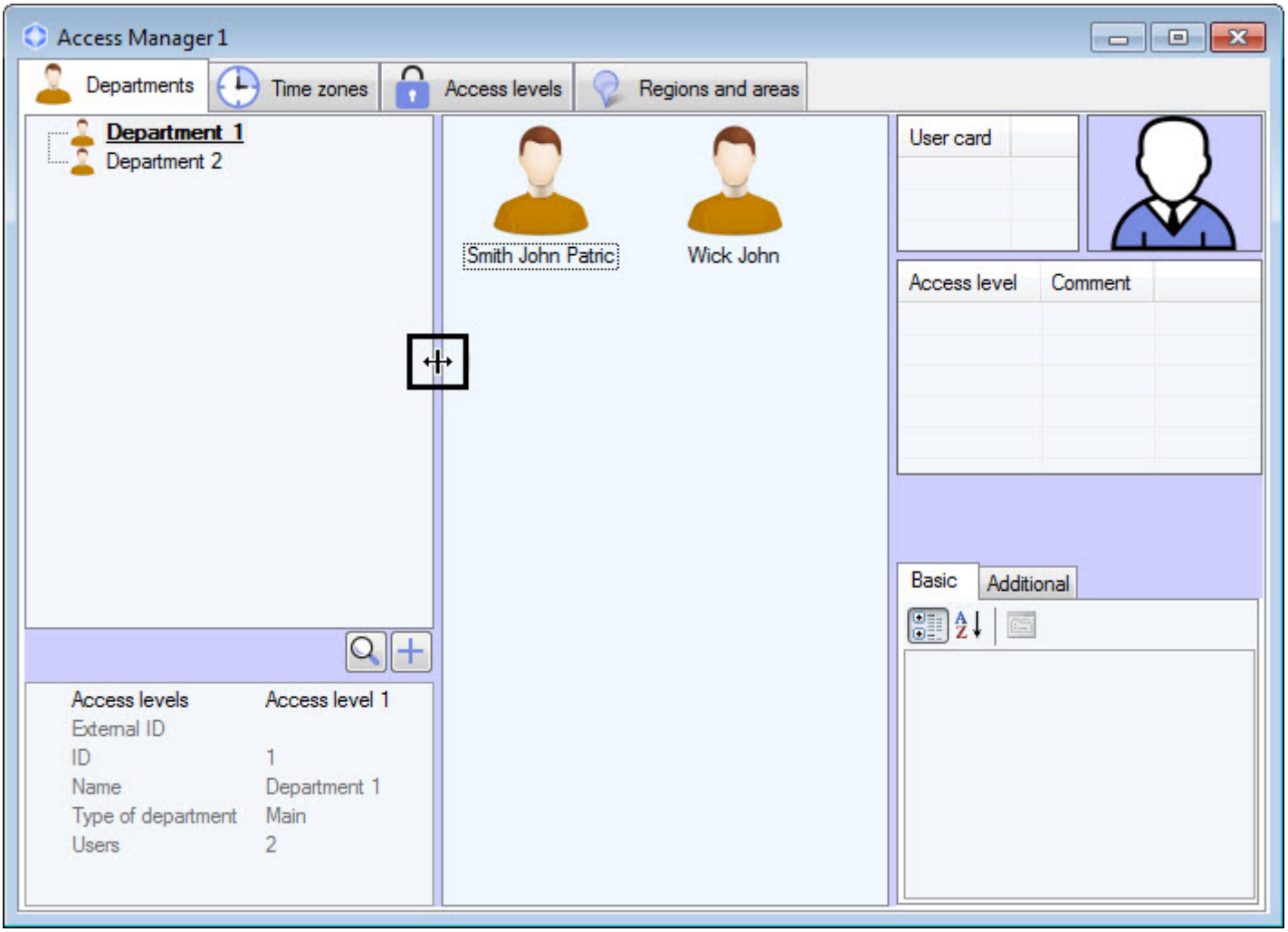
To sort values in the list by some field if the **Table** view is selected, click the left mouse button on the title of column with field name.



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

6.2.3 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.

6.2.4 Keyboard shortcuts for working with interface elements

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

To use the keyboard shortcut, the list of objects should be active. So before using the keyboard shortcut, left-click in the area of the objects list.

Keyboard shortcut	**Description**
Ctrl+F	Search for object
Ctrl+N	Create new object
Ctrl+Del Ctrl+Backspace	Delete an object. To use this shortcut, select an object in the list
Ctrl+Shift+M	Show/hide the user control panel in the **Departments** tab (see Viewing a list of users)

Ctrl+A	Select all users in the department / in search results / in the region
Ctrl+left mouse button	Select multiple objects one by one. To use this shortcut, press the Ctrl key and, without releasing it, select each required object by clicking the left mouse button
Shift+left mouse button	Select a group of objects. To use this shortcut, press the SHIFT key and, without releasing it, select the first and last object of the group by clicking the left mouse button. All objects in between will be selected automatically

Modal windows, with a few exceptions, are closed by pressing the Esc key.

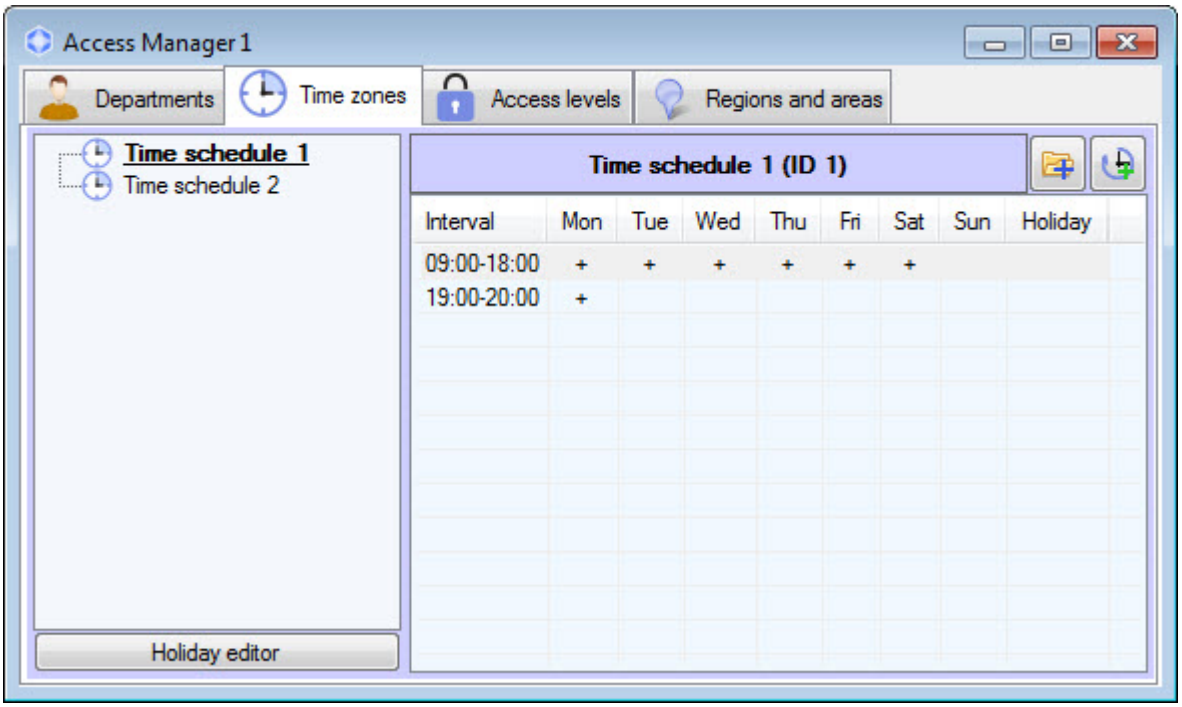
Note

For example, the Esc key cannot be used to close the user photo assignment window.

6.3 Working with time zones in the Access Manager software module

6.3.1 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.



The Access Manager software module allows you to create, edit, copy, view, and delete time zones. At the same time, the ability to create, edit and delete time zones may be prohibited when configuring the Access Manager software module - see Rights for accessing the time zones in Access Manager.

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.

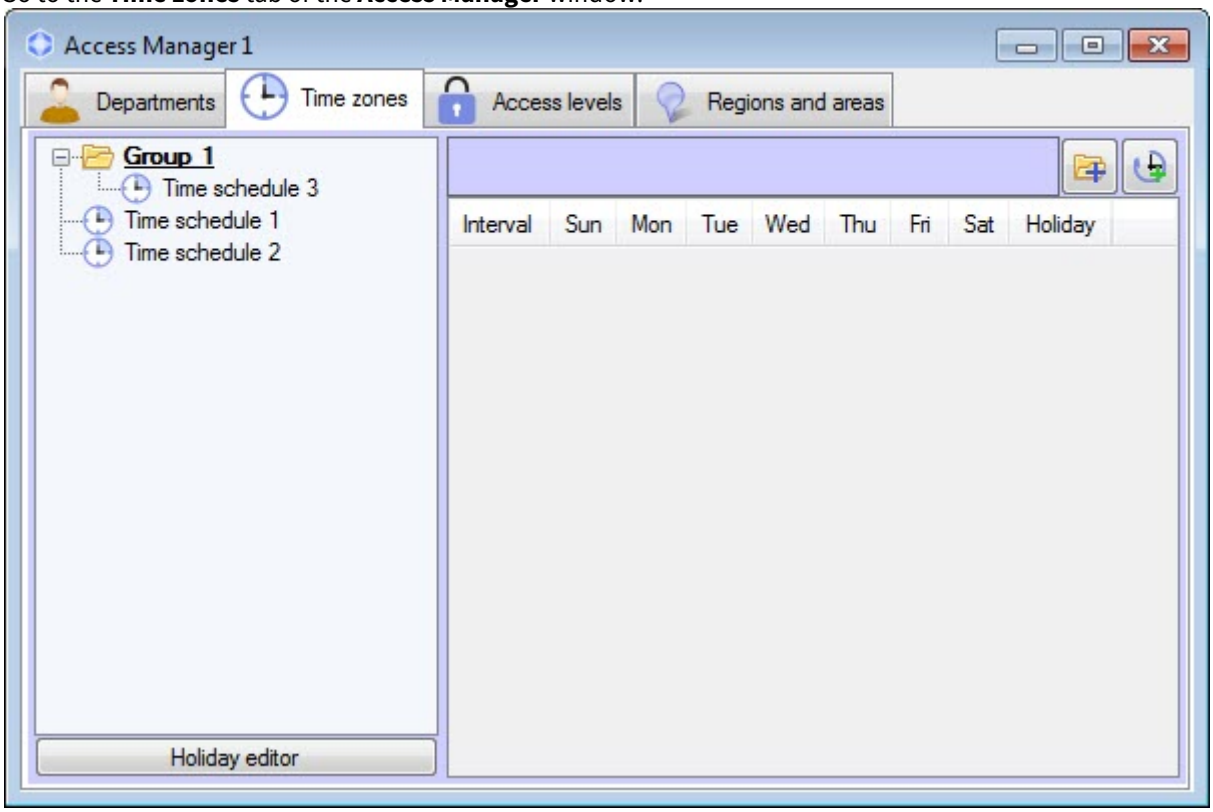
Attention!

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.

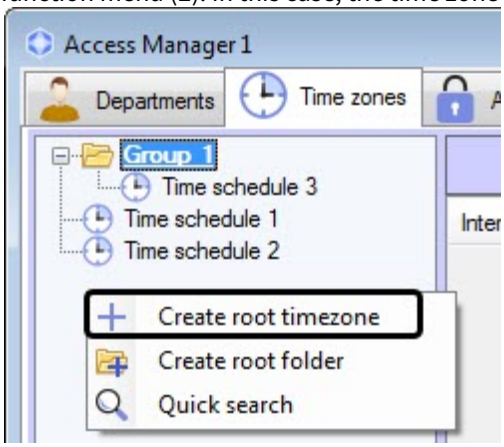
6.3.2 Creation of a time zone in the Access Manager software module

To create a time zone, do the following:

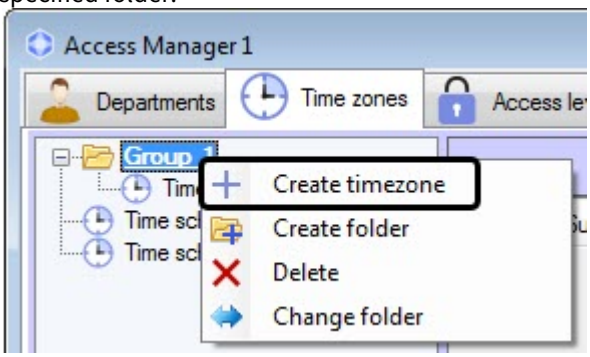
1. Go to the **Time zones** tab of the **Access Manager** window.



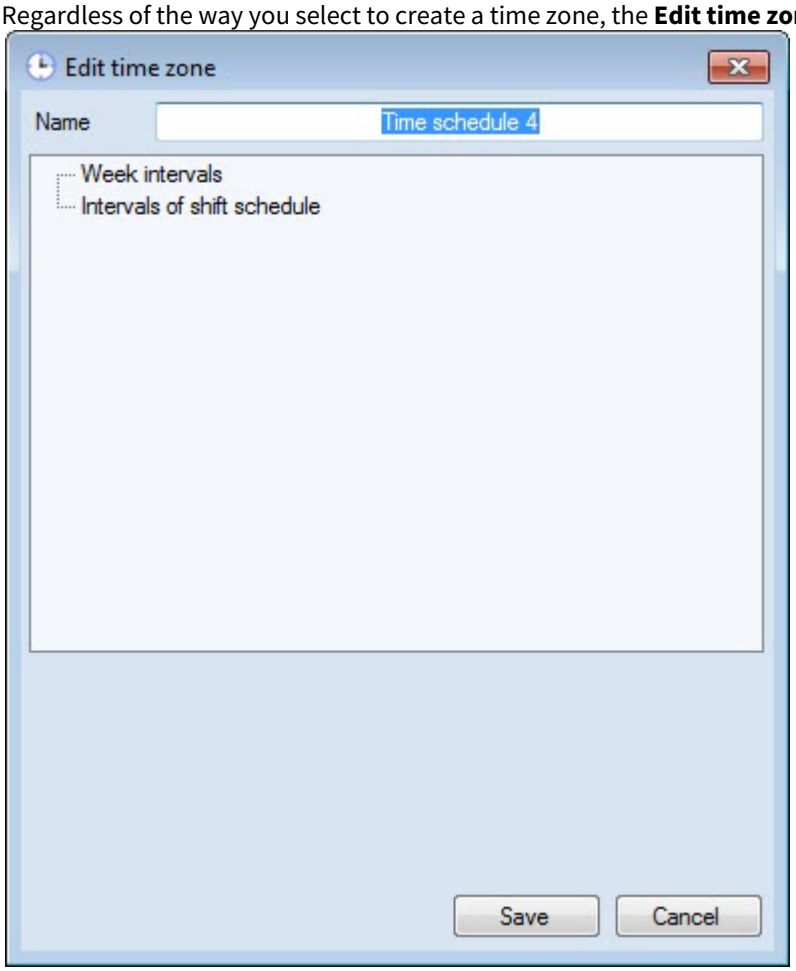
2. There are two ways to create a new time zone:
   a. Right-click in the free area of the list of time zones and select the **Create root time zone** item in the opened function menu (**1**). In this case, the time zone will be created in the common list of time zones.



b. Right-click on the folder and select the **Create timezone** item (**2**). In this case, the time zone will be created in the specified folder.



3. Regardless of the way you select to create a time zone, the **Edit time zone** window will open.

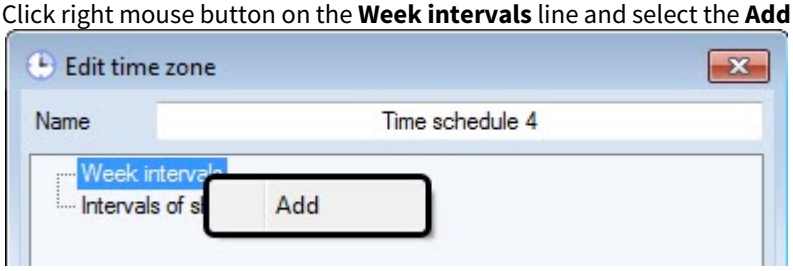


4. Enter the name of creating time zone in the **Name** field.

> **Note**
>
> The name should be unique. If a time zone with this name has already been created in the system, then while saving, a corresponding message will be displayed and the zone will not be saved. Also, the name should not contain the following characters: < | >.

5. Add week intervals to the time zone if it's required:

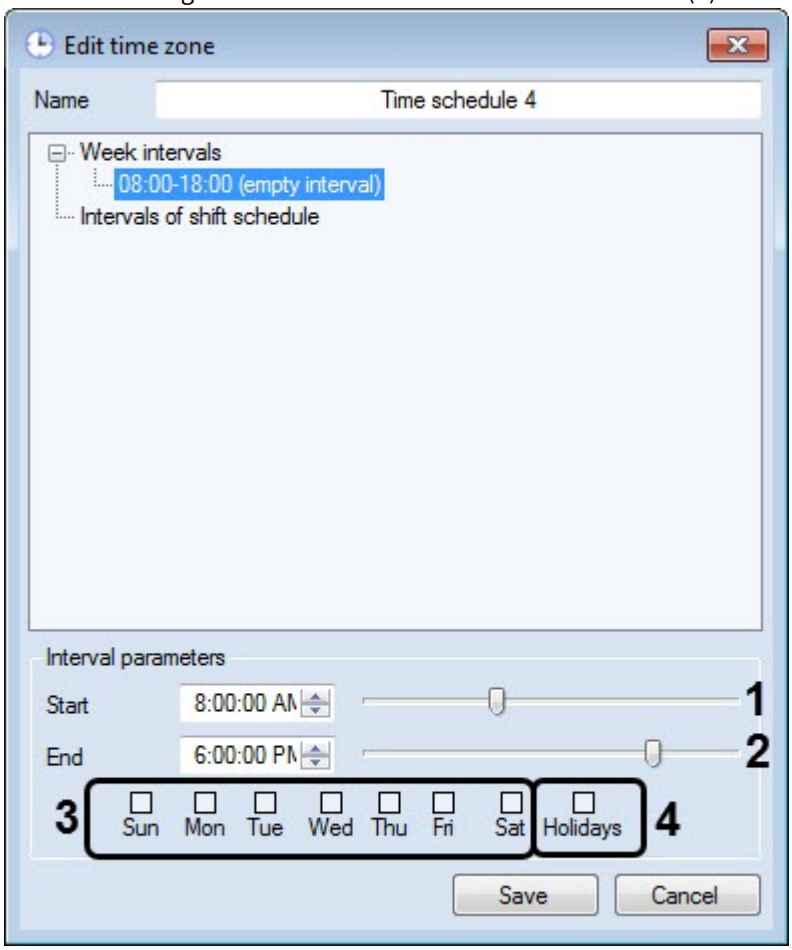
a. Click right mouse button on the **Week intervals** line and select the **Add** item in the opened functional menu.



b. 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:
> 1. Empty interval.
> 2. Whole week.
> 3. Whole week and on holiday.
> 4. On workdays.
> 5. On workdays and on holiday.
> 6. On the weekend and on holiday.
> 7. On the weekend.
> 8. Only on holiday.

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

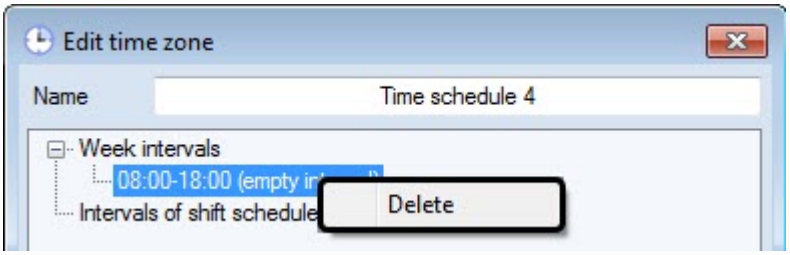


d. Enter or set using slider time of interval end in the **End** field (**2**).

e. Set checkboxes corresponding to days in which interval should operate (**3**).

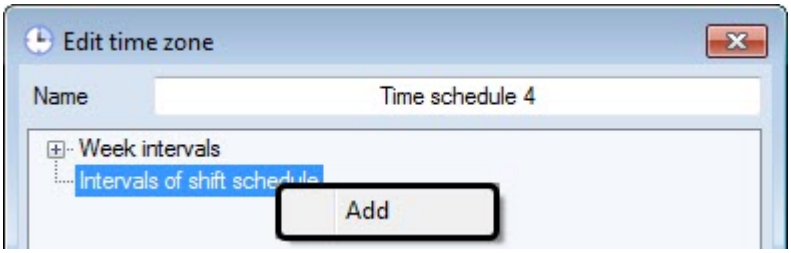
f. If it's required to eliminate holidays from the interval, set the **Holidays** checkbox (**4**).

> **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.

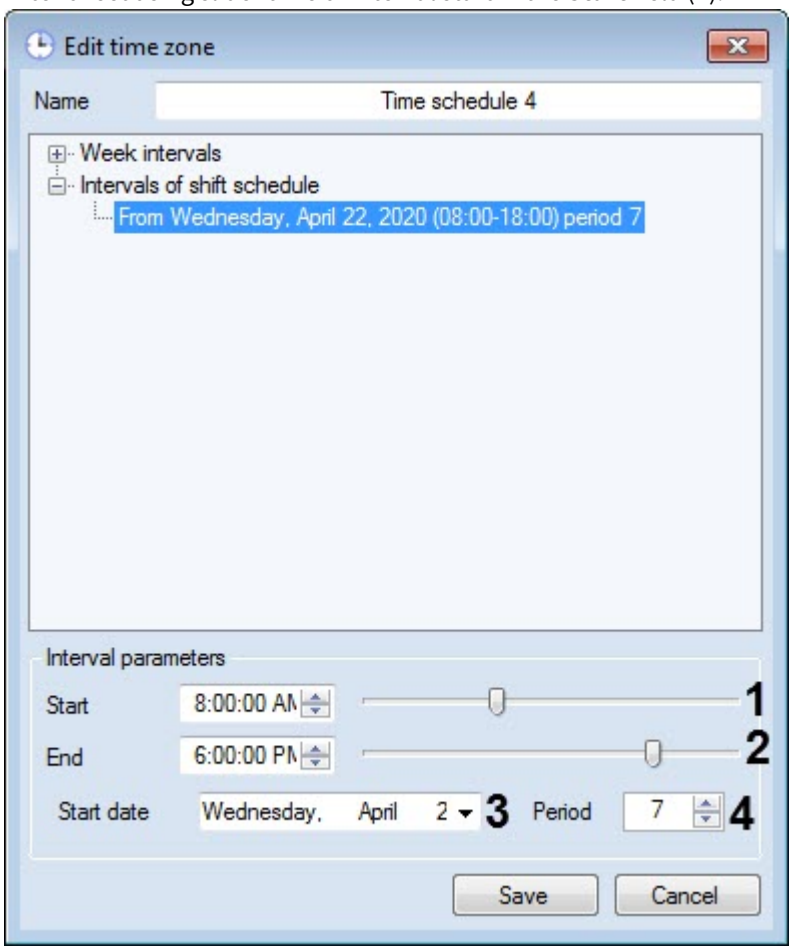
6. Add intervals of shift schedule to the time zone if it's required:
   a. Click right mouse button on the **Intervals of shift schedule** line and select the **Add** item in the opened functional menu.



   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.

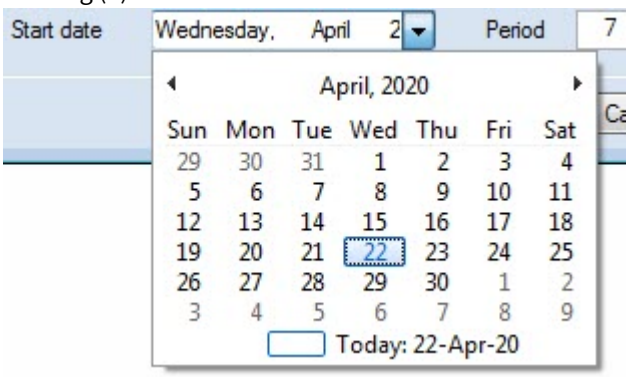
> **Note**
>
> Name of the interval is a date of interval start, time interval and period of interval repetition in days.

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



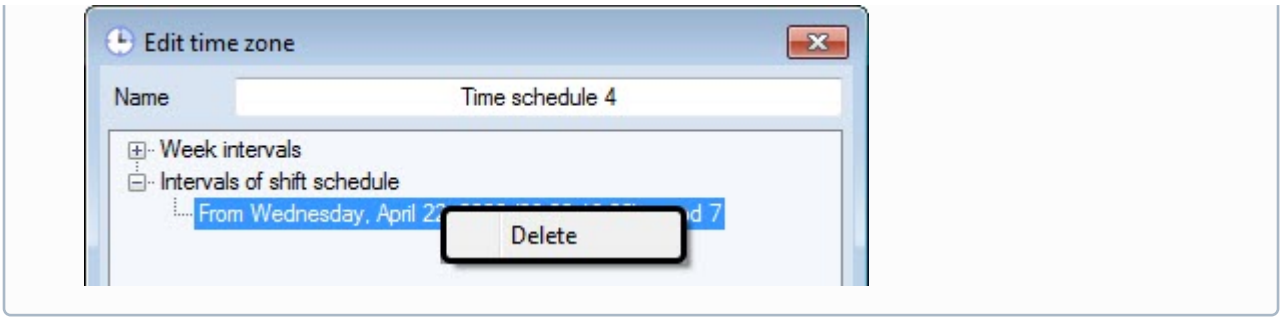
d. Enter or set using slider time of interval end in the **End** field (**2**).

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



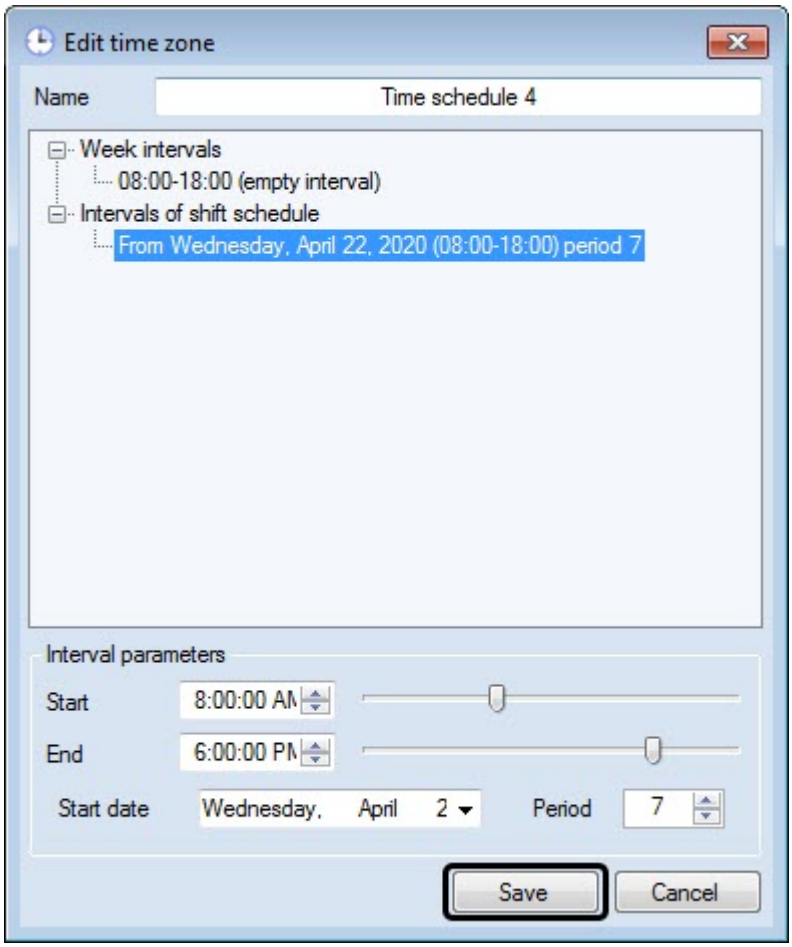
f. In the **Period** field using up-down buttons enter the number of days in which the interval of shift schedule will be repeated (**4**).

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

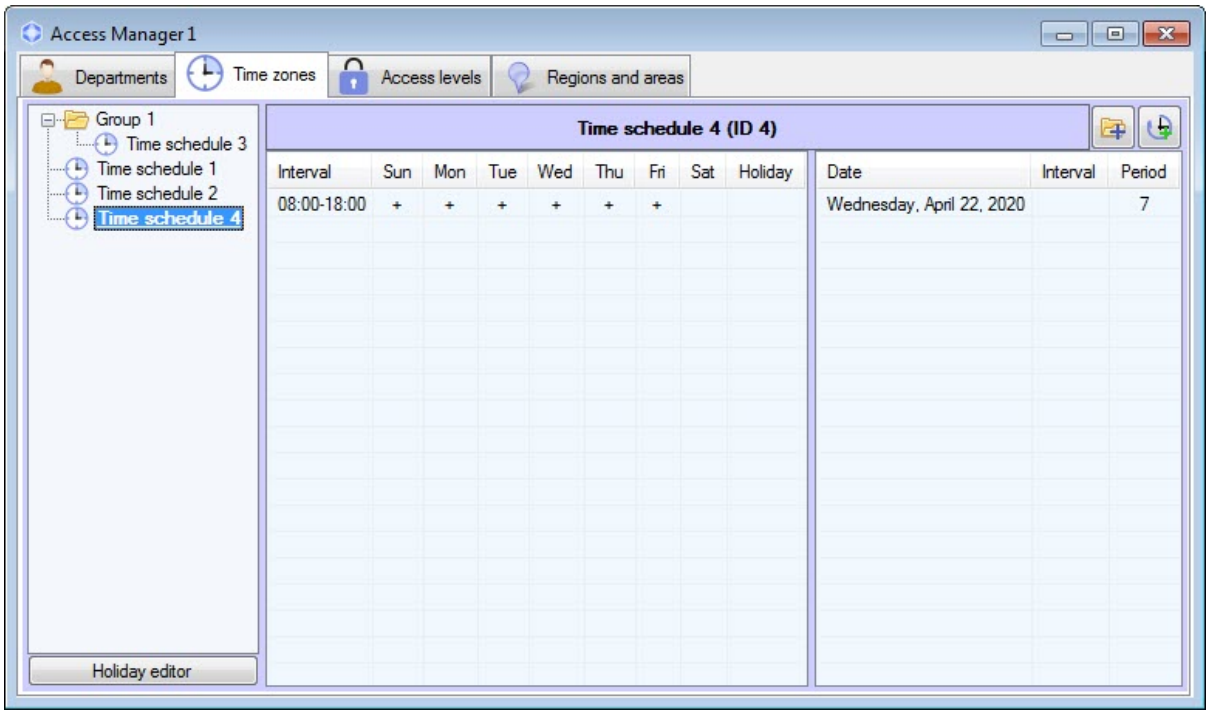


g. Repeat steps a-f for all required week intervals.

7. Click the **Save** button.



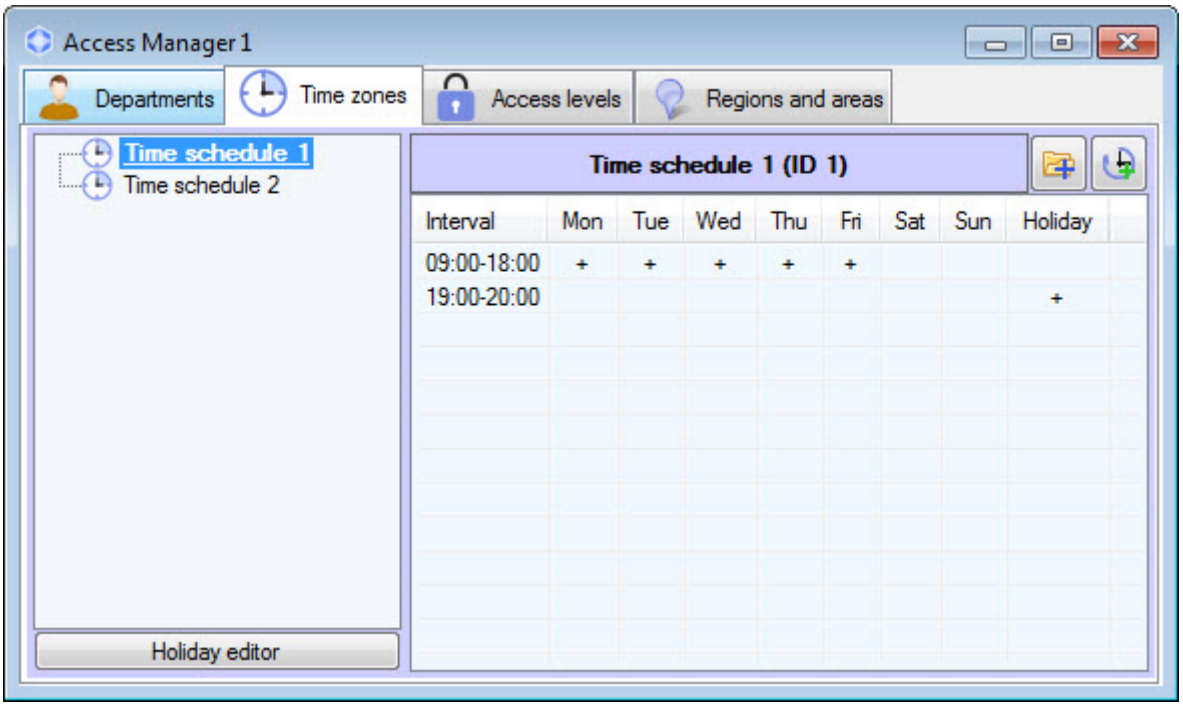
As a result, the created time zone will be displayed in the time zone list.



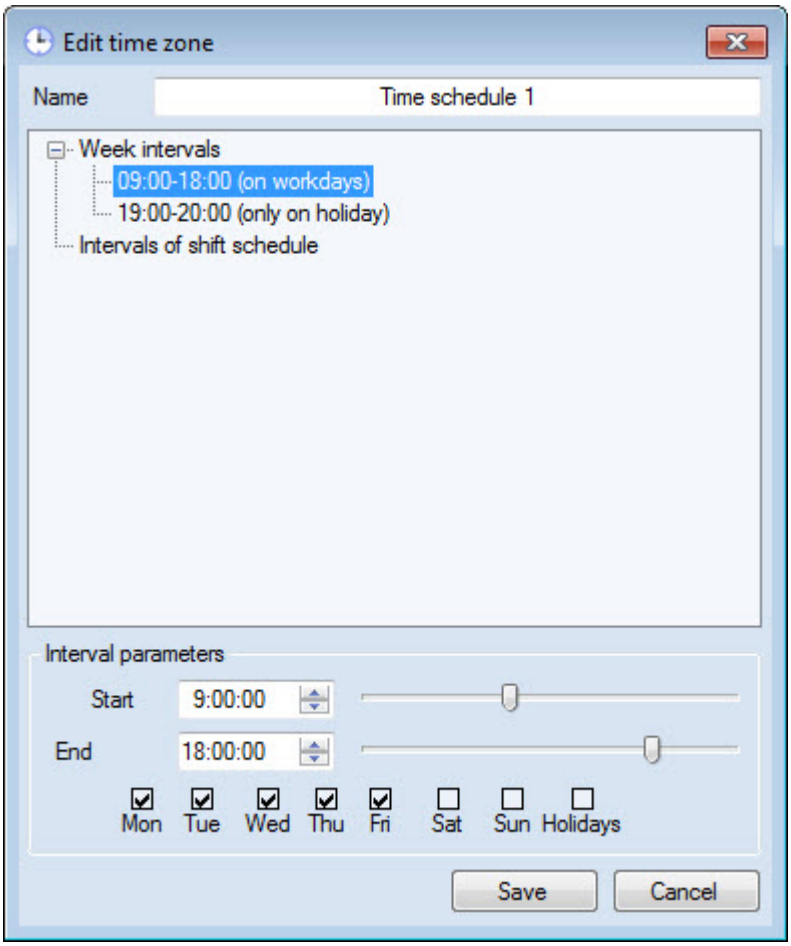
6.3.3 Editing a time zone in the Access Manager software module

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.

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. Working with this window is the same as while creating time zone - see Create time zone section.

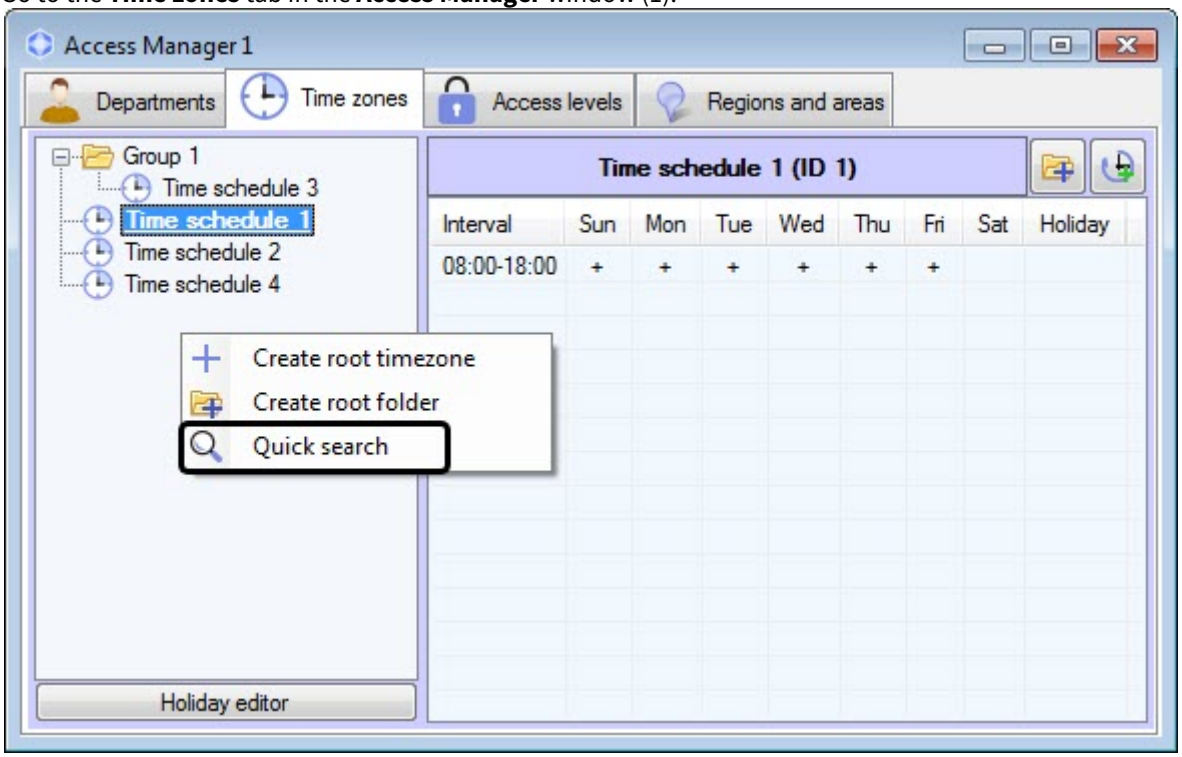


6.3.4 Search for time zone

6.3.4.1 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.

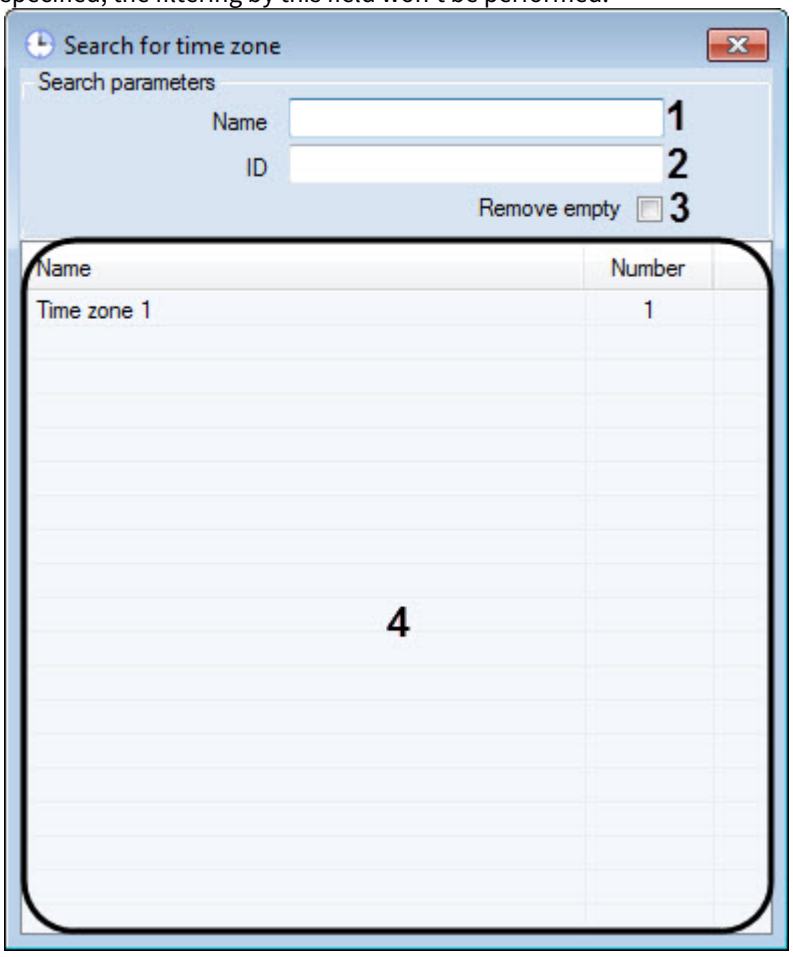
Going to search for time zone is completed. Working with the **Search for time zone** window is described in the Working with the Search for time zone window section.

6.3.4.2 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.

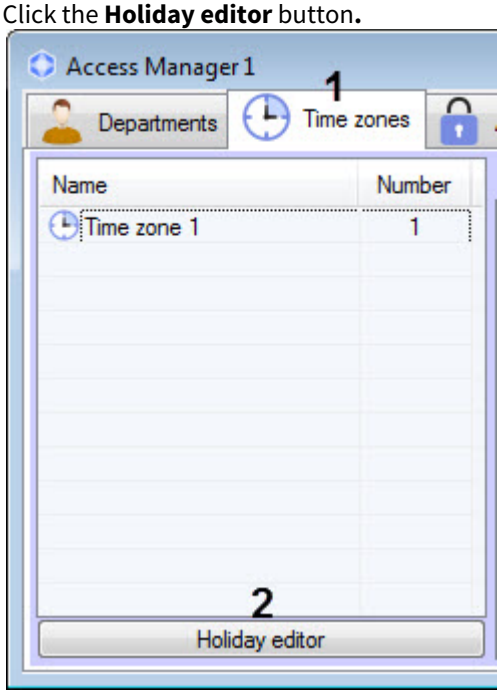
Search for time zone is completed.

6.3.5 Editing holidays

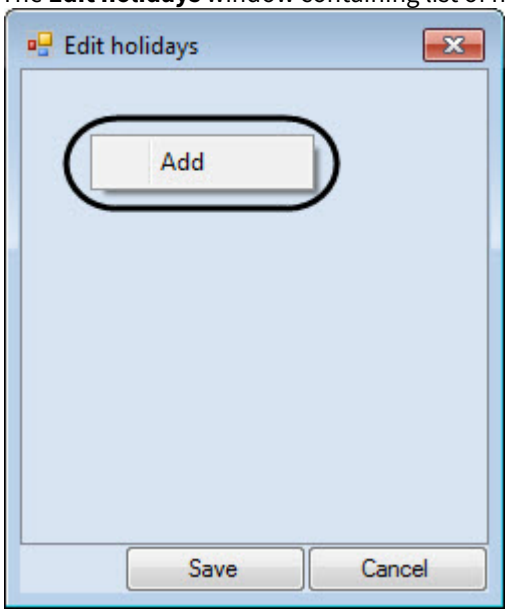
To edit holidays, do the following:

1. Go to the **Time zones** tab of the **Access manager** window.

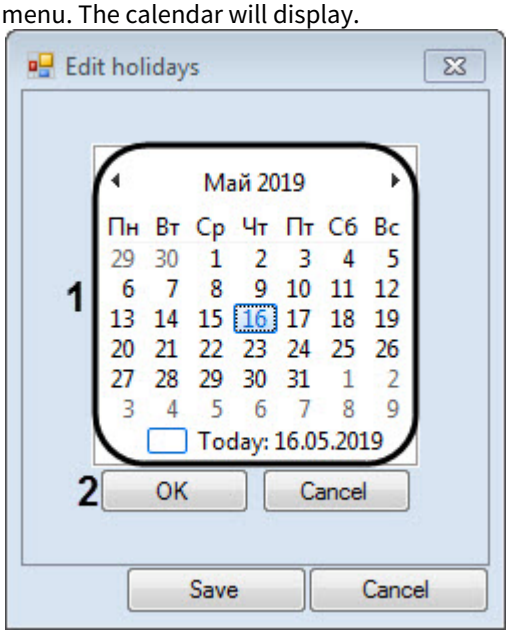
2. Click the **Holiday editor** button**.**



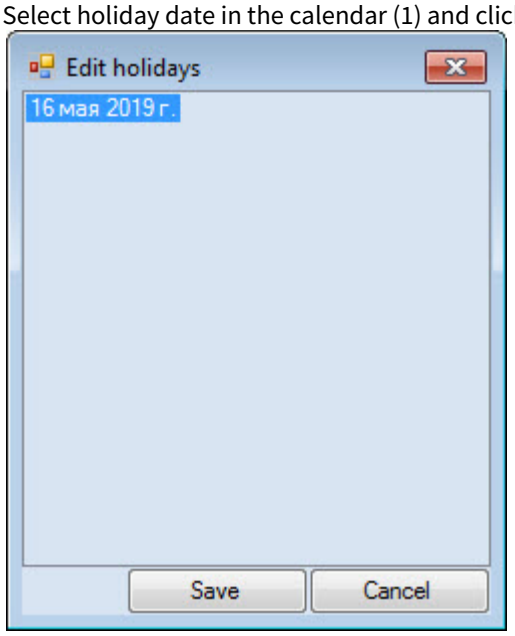
3. The **Edit holidays** window containing list of holidays will be opened.



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.

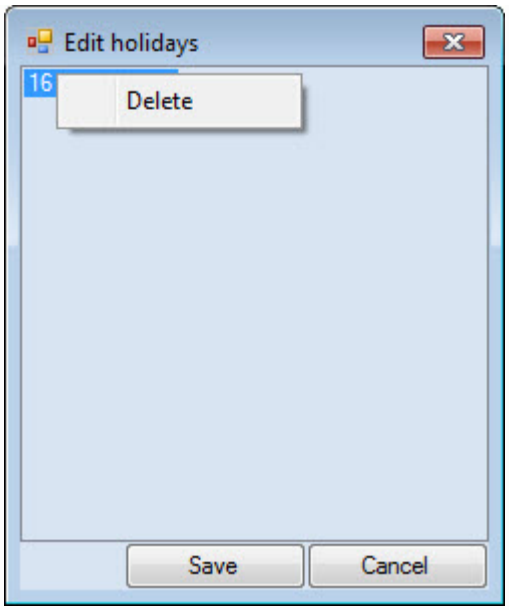


5. Select holiday date in the calendar (1) and click the **OK** button (2). The holiday will be added to the list.

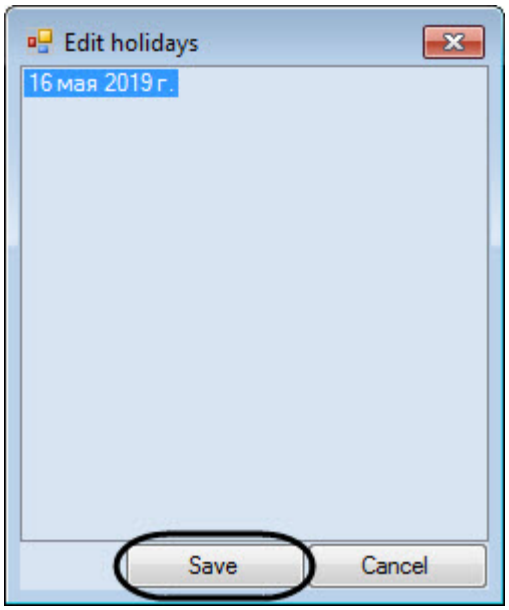


6. Repeat steps 4-5 for all required holidays.

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



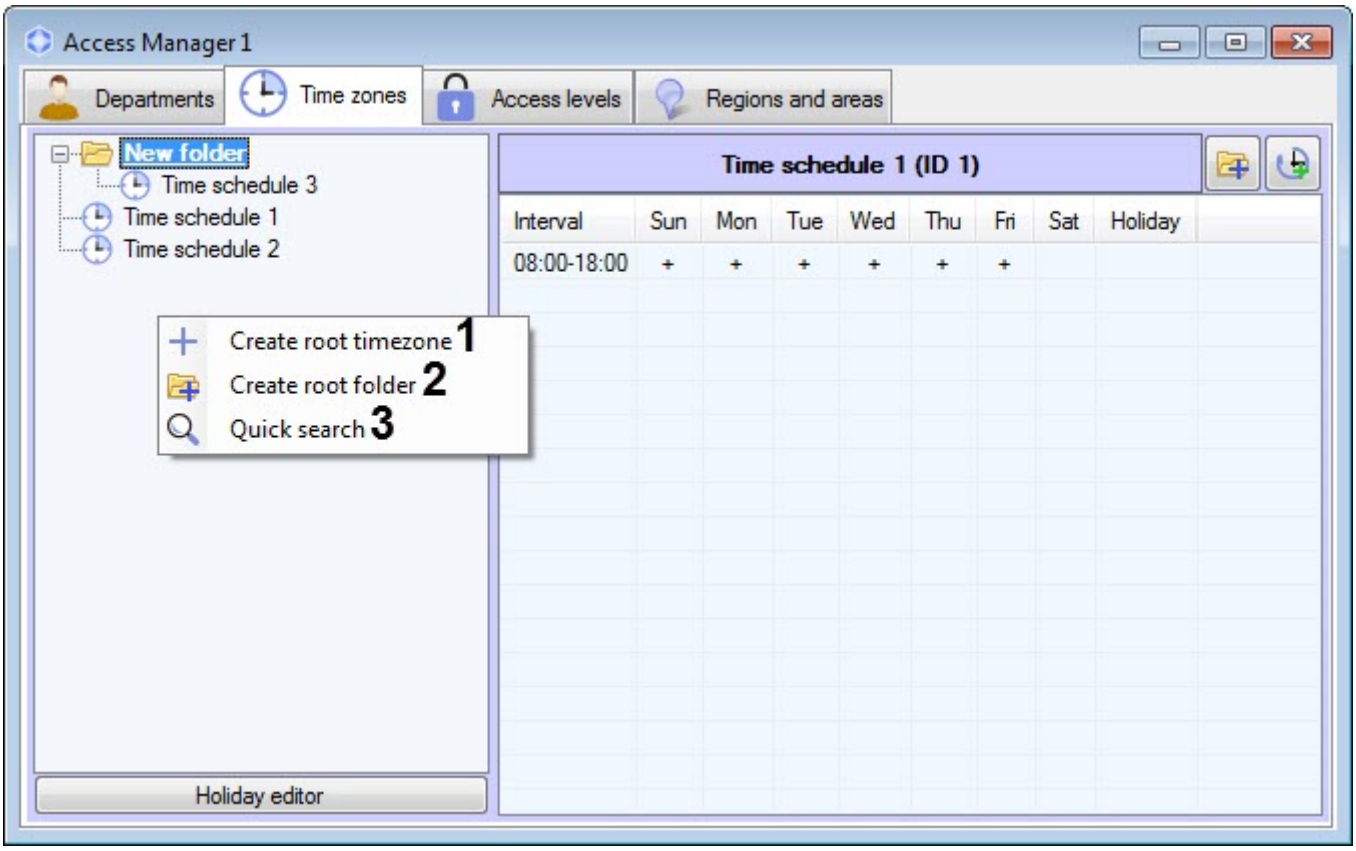
7. Click the **Save** button.



Editing of holidays is completed.

6.3.6 Managing the list of time zones

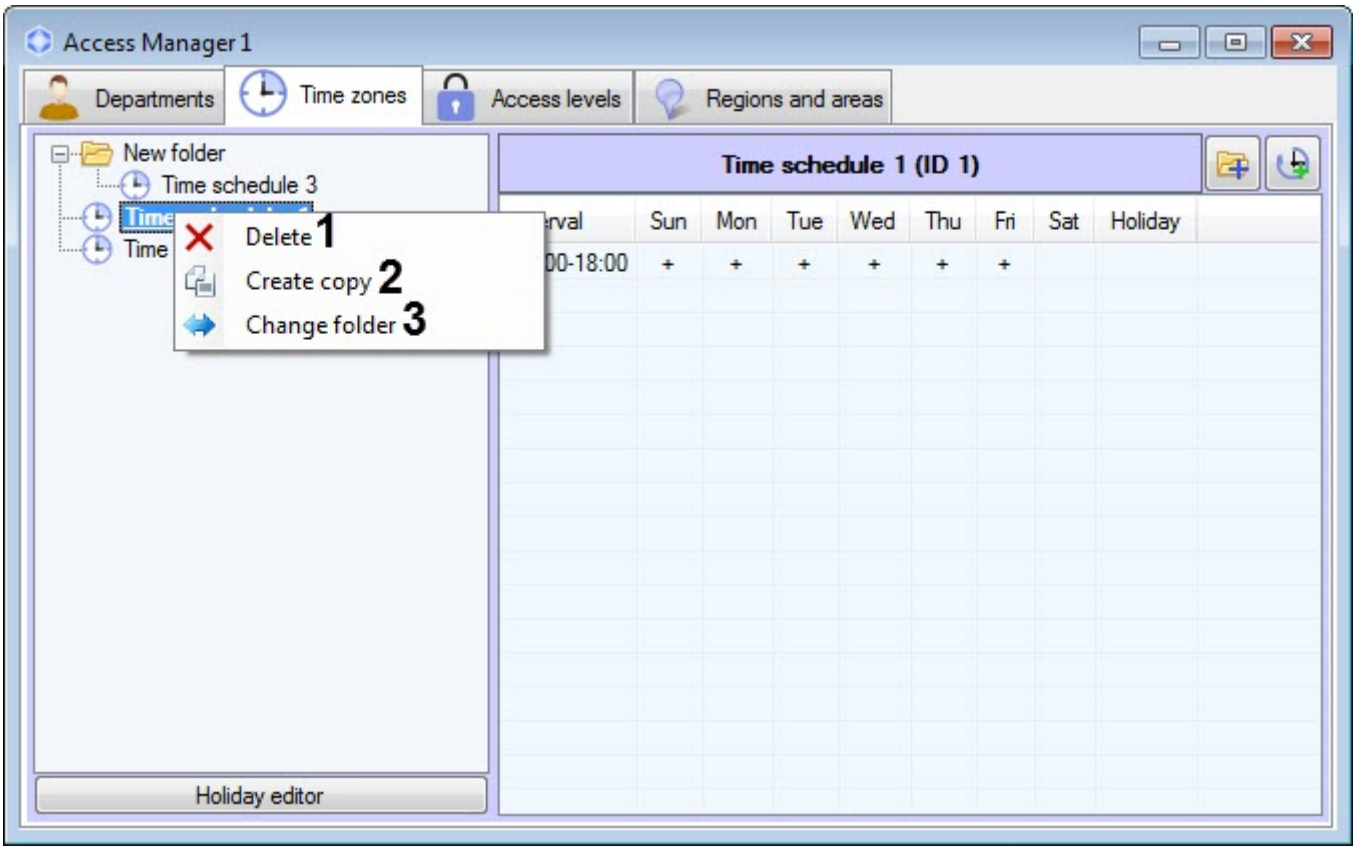
The list of time zones is managed in the *Access Manager* using the context menu, invoked by right-clicking in the free area of the list of time zones.



The context menu commands are described in the table.

№	Command	Description
1	Create root timezone	Adds a new time zone to the list of time zones. When you select this command, the **Edit time zone** window opens, where you can specify a name for a new time zone and add week intervals/intervals of shift schedule to it. For details on creating a time zone, see Creation of a time zone in the Access Manager software module.
2	Create root folder	Adds a folder for grouping time zones to the list of time zones. When you select this command, the **Folder options** window opens, where you can specify a name for the new folder.
3	Quick search	Launches the quick search window for time zones in the list. When you select this command, the **Search for time zone** window opens, where you can search for time zones by various criteria. For details on searching time zones, see Search for time zone.

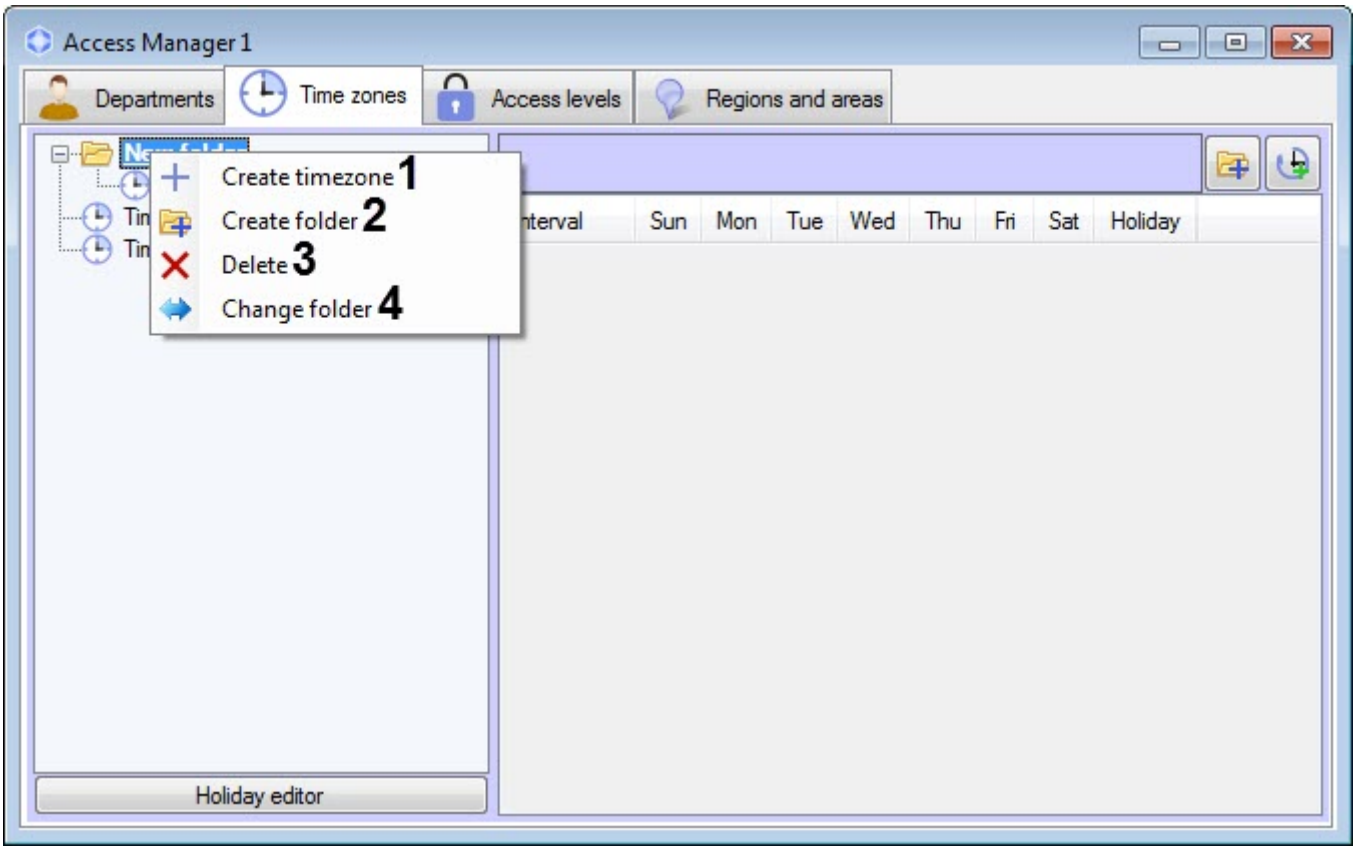
A separate time zone in the root of the list of time zones is managed using the context menu invoked by right-clicking on the time zone.



The context menu commands are described in the table.

№	Command	Description
1	Delete	Deletes the time zone after confirmation from the user. If deletion of assigned time zones is forbidden (see Setting the prohibition of deleting non-empty departments, assigned ALs and TZs), then the time zone can only be deleted if it is not assigned to any access level. When you try to delete an assigned time zone, the **Invalid operation** warning is displayed indicating access levels to which the time zone is assigned.
2	Create copy	Copies the selected time zone. When you select this command, the **Edit time zone** window opens, where you can modify the copy, if necessary. For details on editing a time zone, see Editing a time zone in the Access Manager software module.
3	Change folder	Moves the time zone to the selected folder. When you select this command, the **Search for folder** window opens with a tree of available folders. After you select the required folder, press the Enter key on the keyboard or the **OK** button in the folder selection window.

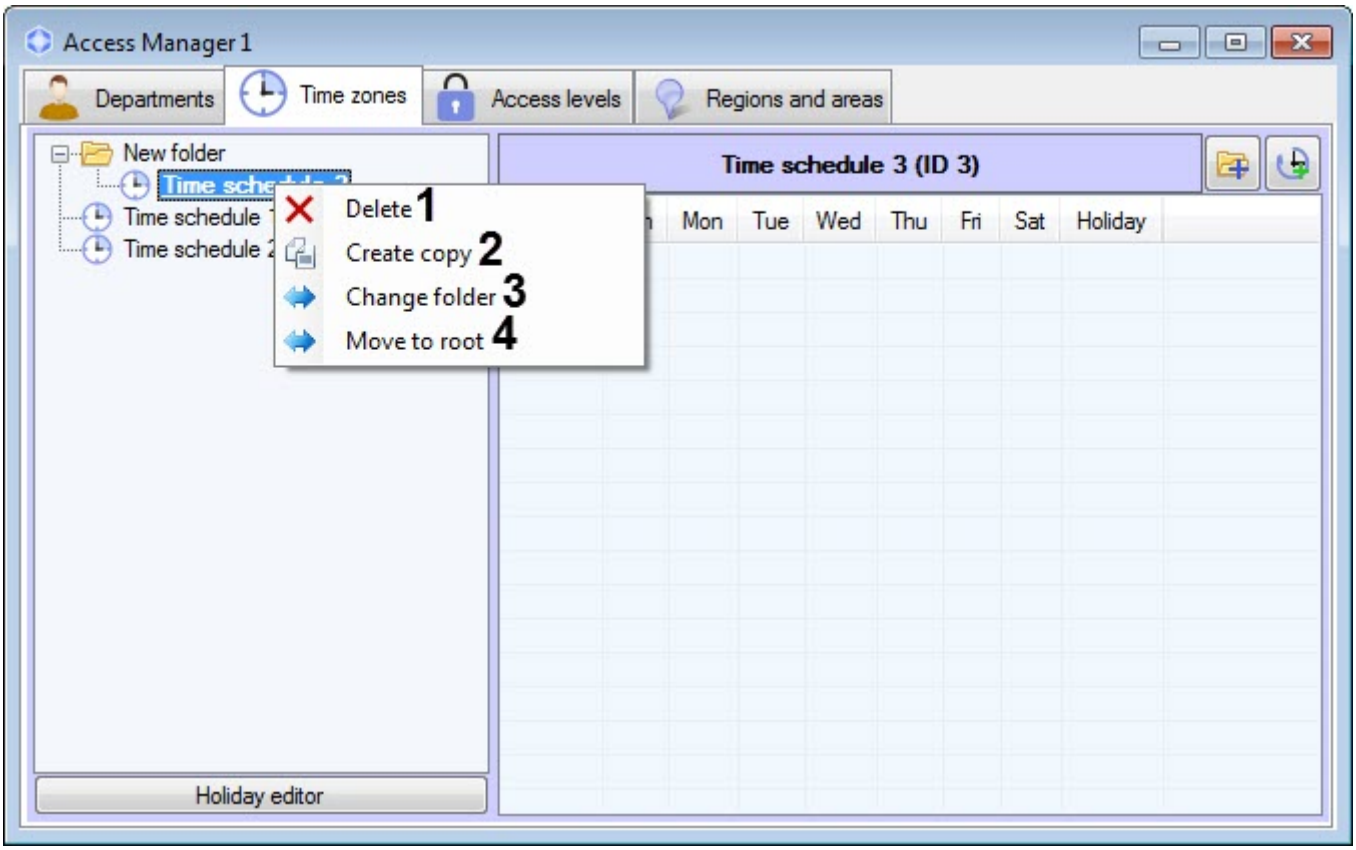
An individual folder in the list of time zones is managed using the context menu invoked by right-clicking on the folder.



The context menu commands are described in the table.

№	Command	Description
1	Create timezone	Adds a new time zone to the folder. When you select this command, the **Edit time zone** window opens, where you can specify a name for a new time zone and add week intervals/intervals of shift schedule to it. For details on creating and editing a time zone, see Creation of a time zone in the Access Manager software module.
2	Create folder	Adds a subfolder. When you select this command, the **Folder options** window opens, where you can specify a name for the new folder.
3	Delete	Deletes the folder after confirmation from the user. If deletion of assigned time zones is forbidden (see Setting the prohibition of deleting non-empty departments, assigned ALs and TZs), then the time zone can only be deleted if it is not assigned to any access level. When you try to delete an assigned time zone, the **Invalid operation** warning is displayed indicating access levels to which the time zone is assigned.
4	Change folder	Moves the folder to the selected folder. When you select this command, the **Search for folder** window opens with a tree of available folders. After you select the required folder, press the Enter key on the keyboard or the **OK** button in the folder selection window.

A separate time zone located inside a folder is managed using the context menu invoked by right-clicking on the time zone.



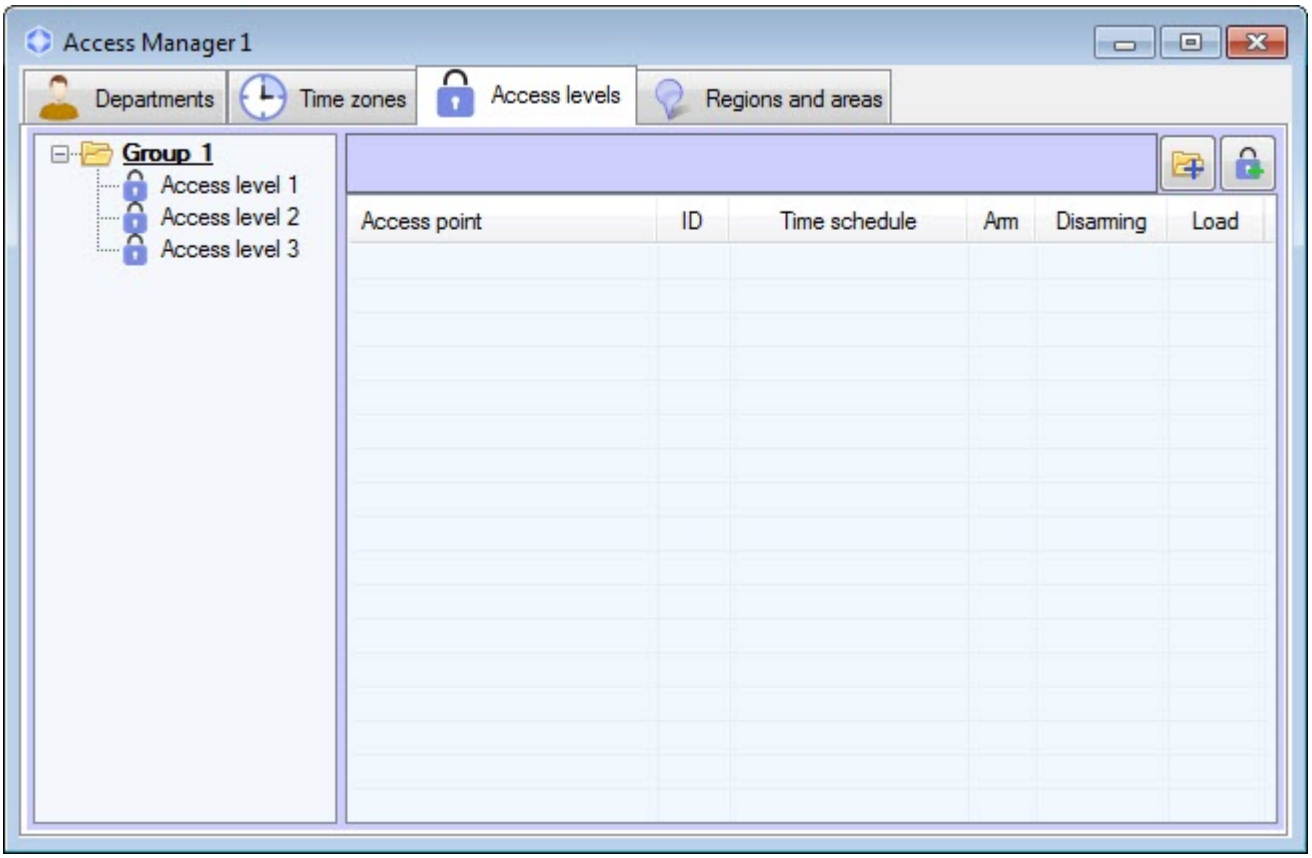
The context menu commands are described in the table.

№	Command	Description
1	Delete	Deletes the time zone after confirmation from the user. If deletion of assigned time zones is forbidden (see Setting the prohibition of deleting non-empty departments, assigned ALs and TZs), then the time zone can only be deleted if it is not assigned to any access level. When you try to delete an assigned time zone, the **Invalid operation** warning is displayed indicating access levels to which the time zone is assigned.
2	Create copy	Copies the selected time zone. When you select this command, the **Edit time zone** window opens, where you can modify the copy, if necessary. For details on editing a time zone, see Editing a time zone in the Access Manager software module.
3	Change folder	Moves the folder to the selected folder. When you select this command, the **Search for folder** window opens with a tree of available folders. After you select the required folder, press the Enter key on the keyboard or the **OK** button in the folder selection window.
4	Move to root	Moves the time zone from the folder to the root of the time zone list.

6.4 Working with access levels in the Access Manager software module

6.4.1 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.

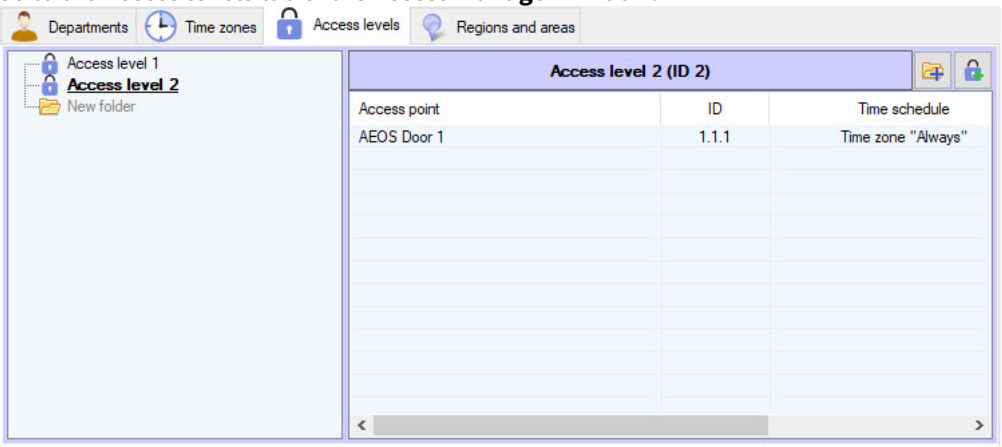


The *Access Manager* software module allows creating, editing, copying, viewing and deleting access levels. At that, possibility of creating, editing and deleting access levels can be forbidden while configuring the *Access Manager* software module - see the Rights for accessing the access levels in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

6.4.2 Creating access levels

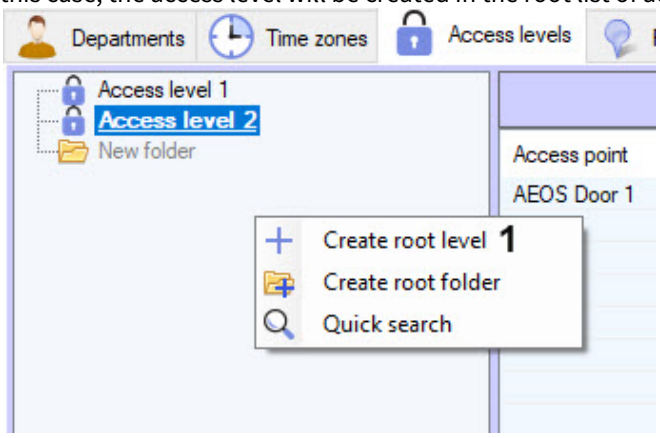
To create access level, do the following:

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

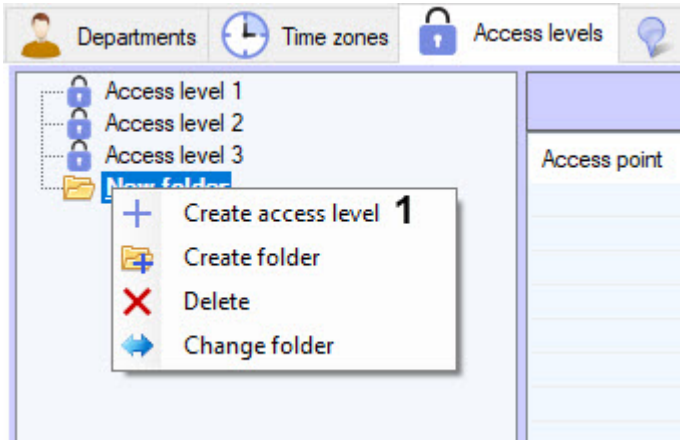


2. There are two ways to create a new access level:

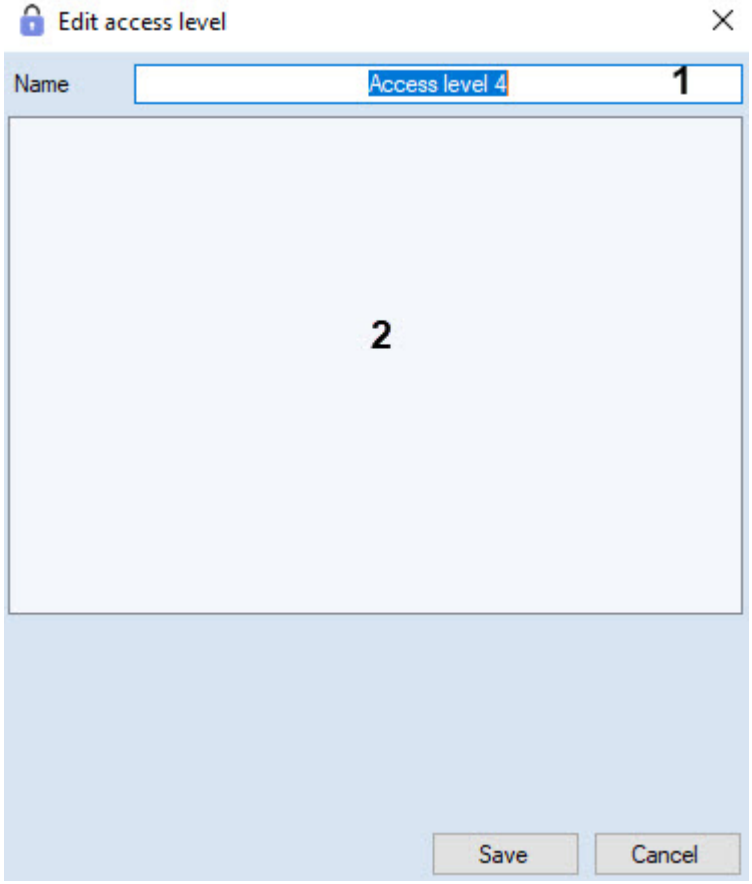
a. Right-click in the free area of the access level list and select **Create root level** item (**1**) in the functional menu. In this case, the access level will be created in the root list of access levels.



b. Right-click the folder and select **Create access level** item (**1**). 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:

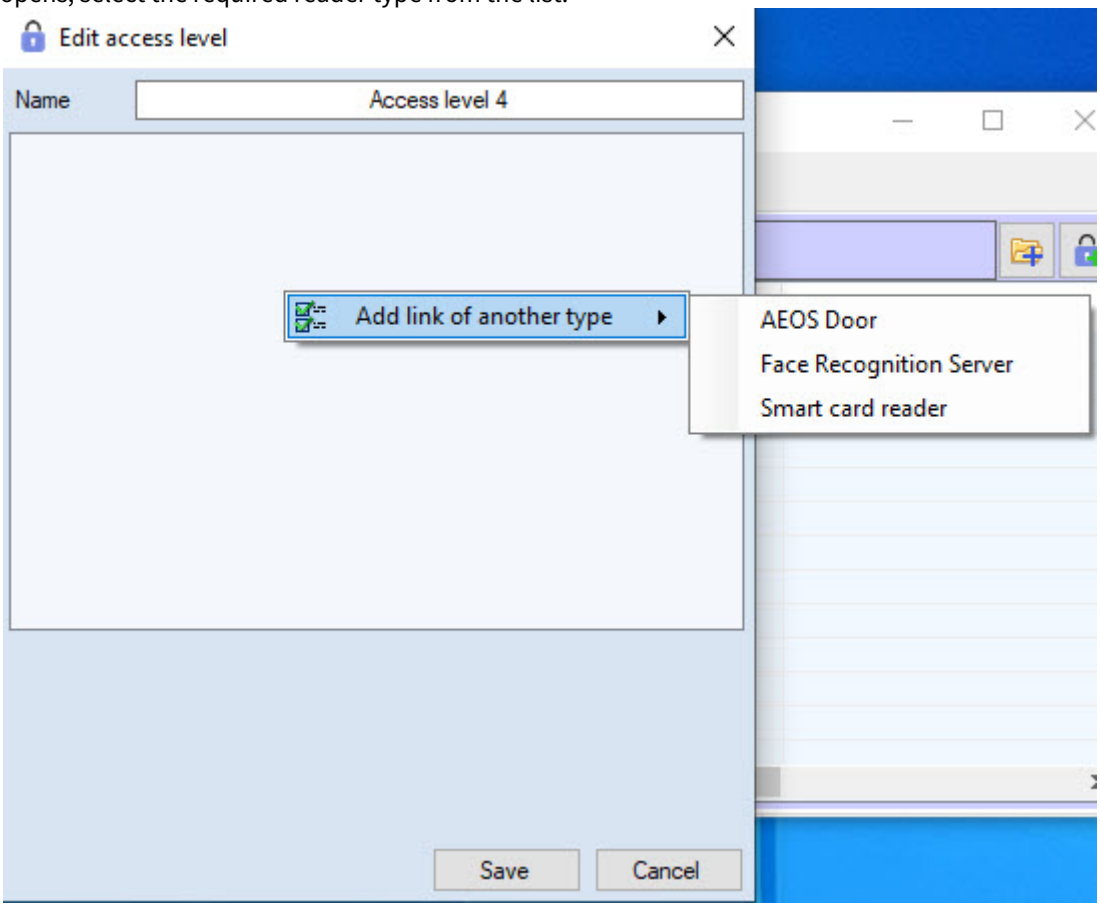


   a. In the **Name** field (**1**), enter name of the access level.

   > **Note**
   >
   > The name should be unique. If an access level with the same name has already been created in the system, then the attempt to save will fail and a corresponding message will be displayed. Also, the name should not contain the following characters: < | >.

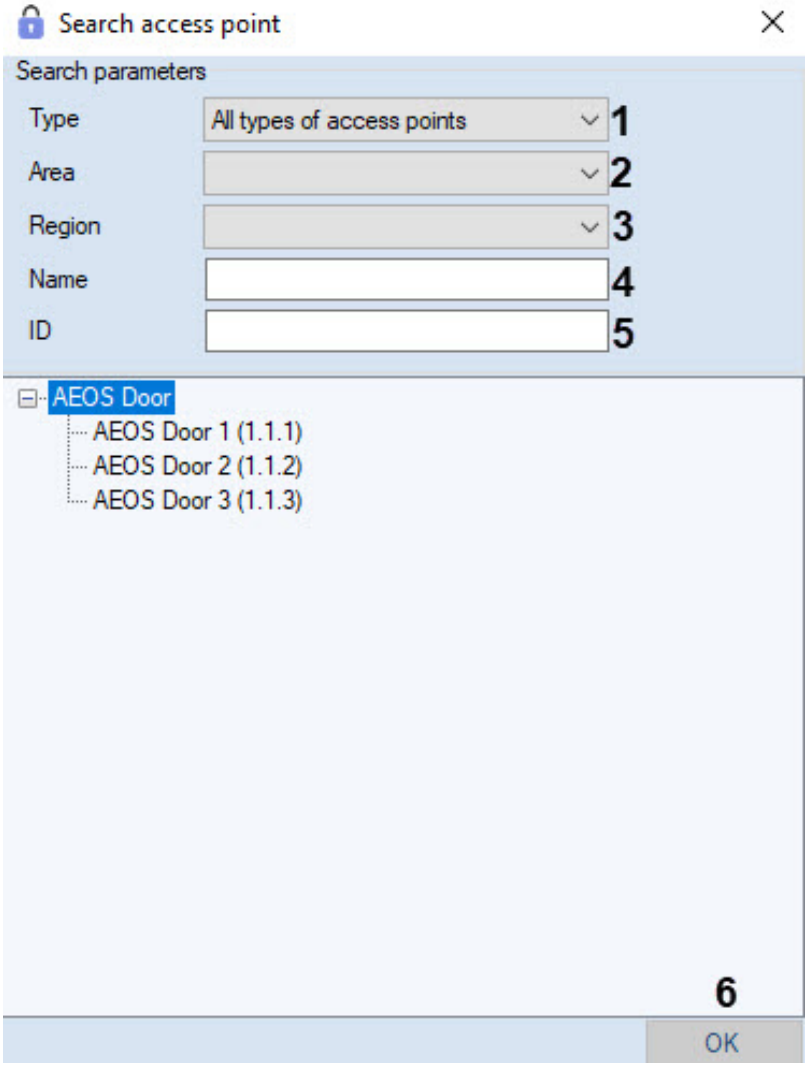
   b. In the free area of the list of access rules (**2**), add a rule that links the access point with the time zone:

i. Right-click on a free area of the list of access rules and in the **Add link of another type** functional menu that opens, select the required reader type from the list.



ii. If there is only one access point of this type, or if there is only one available access point from several access points of the same type, then it will be added automatically.

iii. If there are several access points of this type, then the **Search access point** window will open, which will display all available access points of this type.



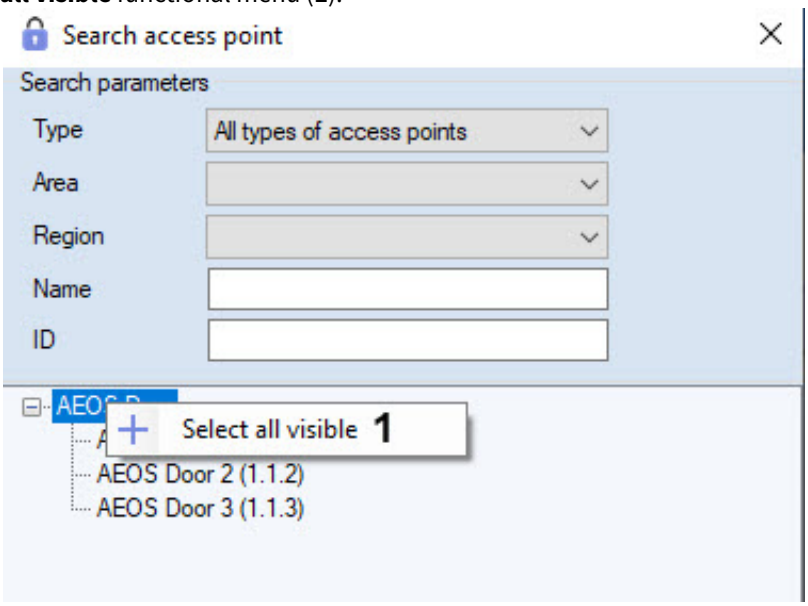
iv. To search and select an access point, do the following:

> **Note**
>
> The suitable access points are searched automatically as you specify the search parameters.

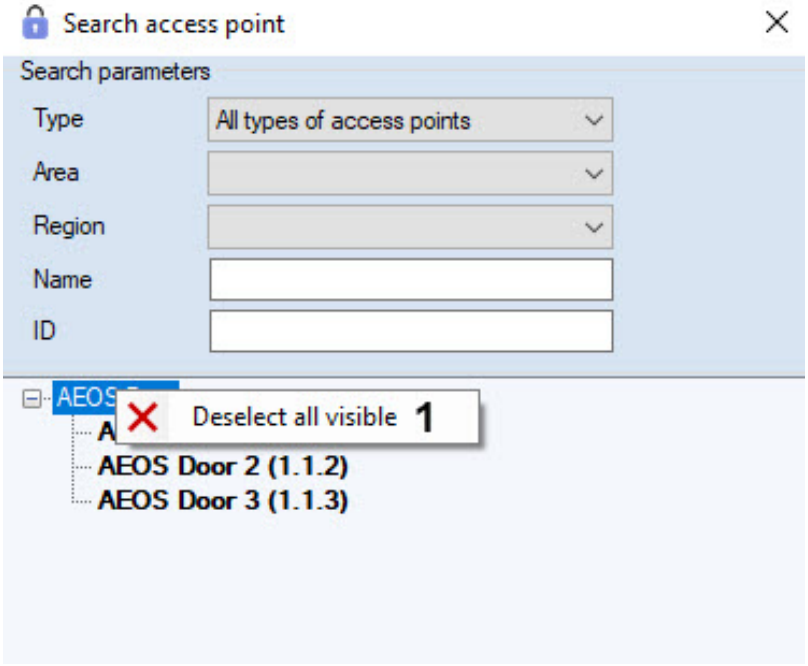
1. Select type of access point from the **Type** drop-down list if it's required (**1**).
2. Select the location of the access point from the **Area** drop-down list if it's required (**2**).
3. Select the location of the access point from the **Region** drop-down list if it's required (**3**).
4. Enter name of access point or its part in the **Name** field if it's required (**4**).
5. Enter ID of required access point in the **ID** field if it's required (**5**).
6. After completing the selection of access points, click the **OK** button (**6**).

v. To select an access point from the list of available access points, double-click on the required object.

vi. To select all available access points of this type at once, right-click on the parent object to open the **Select all visible** functional menu (**1**).



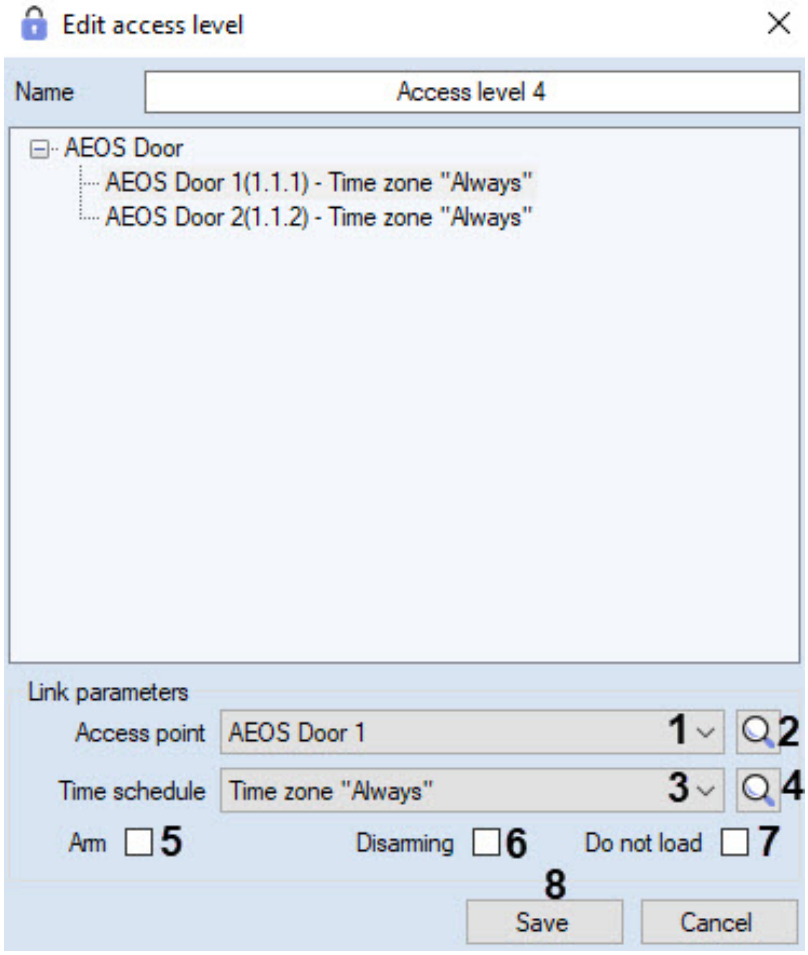
vii. You can deselect all selected access points by right-clicking on the parent object to open the **Deselect all visible** functional menu (**1**).



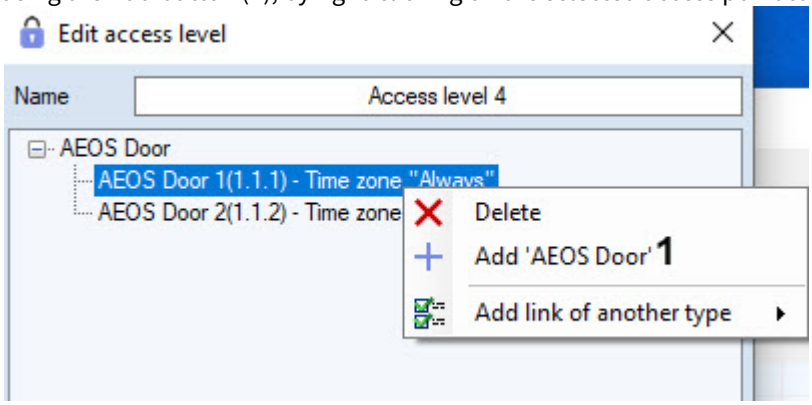
Note

- **Select all visible** and **Deselect all visible** commands can be applied only to those access points that are currently displayed in the list of access points.
- Selected access points are highlighted in bold in the list.

4. You will go back to the **Edit access level** window. The panel for configuring the access level will be displayed at the bottom.



5. Access point specified in the search is selected in the **Access point** drop-down list (**1**). You can change it if necessary.
6. If it is necessary to search for access point, click the button and go to step 3bii. You can also open the search window using the **Add** button (**1**), by right-clicking on the selected access point to open the context menu.



7. From the **Time schedule** drop-down list (**3**), select time zone during which access through the selected access point will be allowed to users with configured access level.
8. If it is necessary to search for time zone, click the button (**4**) (see Working with the Search for time zone window).

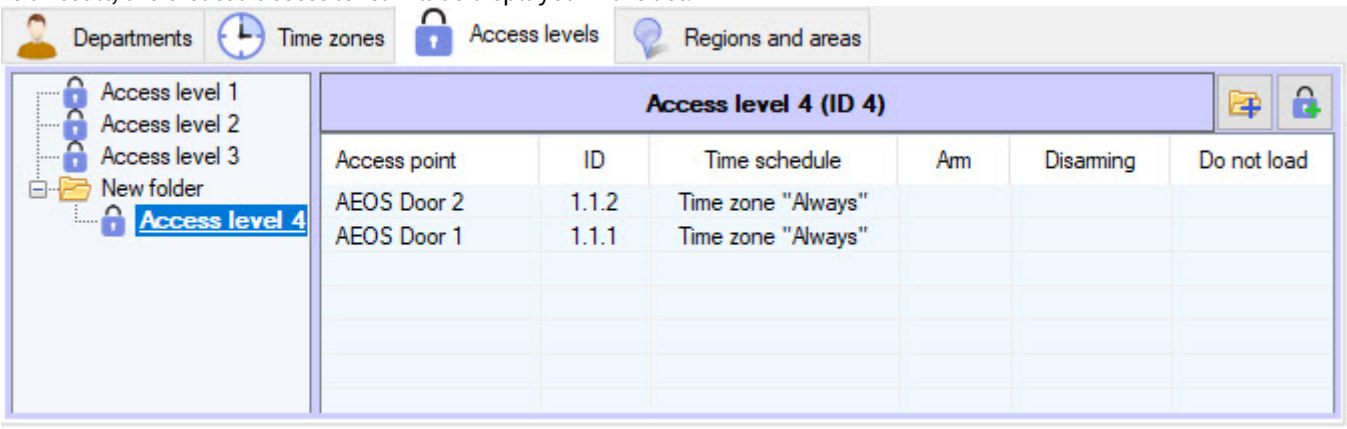
> **Note**
>
> Time zones are created and configured on the **Time zones** tab of the **Access Manager** window - see the Working with time zones in the Access Manager software module section. Also it's possible to use system time zones "Always" and "Never".

9. Set the **Arm** checkbox to arm access point after presenting access card by user (**5**).
10. Set the **Disarming** checkbox to disarm access point after presenting access card by user (**6**).
11. If it's not required to send access cards to controller after presenting access card by user, set the **Do not load** checkbox (**7**).

> **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.

12. Repeat steps 3-11 for all required links.
13. Click the **Save** button (**8**).
    As a result, the created access level will be displayed in the list.



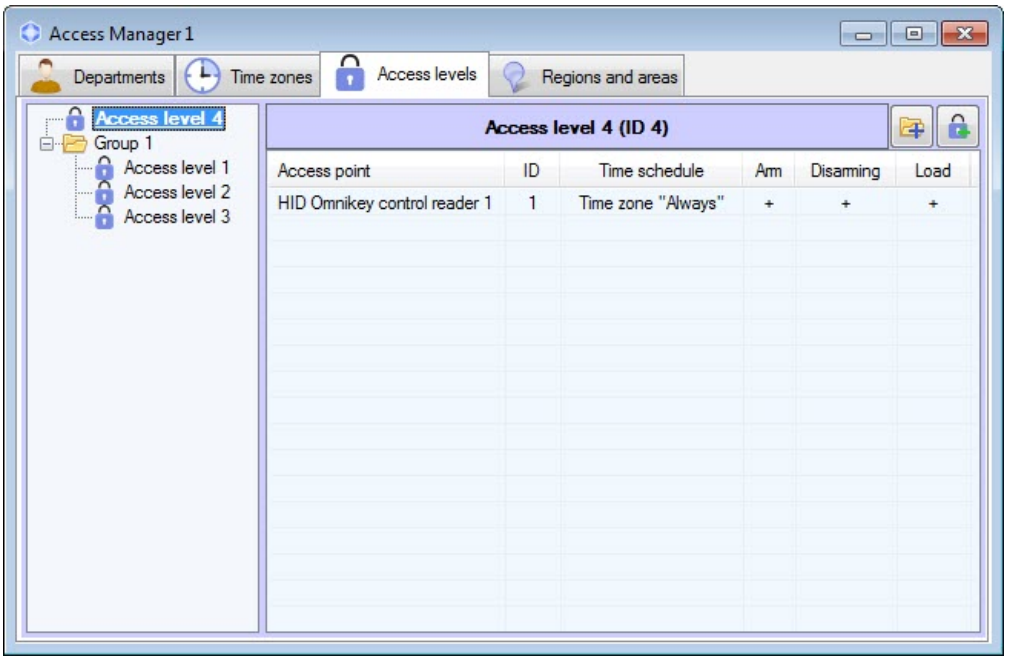
> **Attention!**
>
> When the user configuration is written to the controller/terminal, only those users will be written whose access level contains at least one access point of the corresponding controller/terminal. For example, if a user has an access point of terminal 1 specified in the access levels, but no access point of terminal 2 is specified, then this user will be written only to terminal 1.

The creation of the access level is complete.

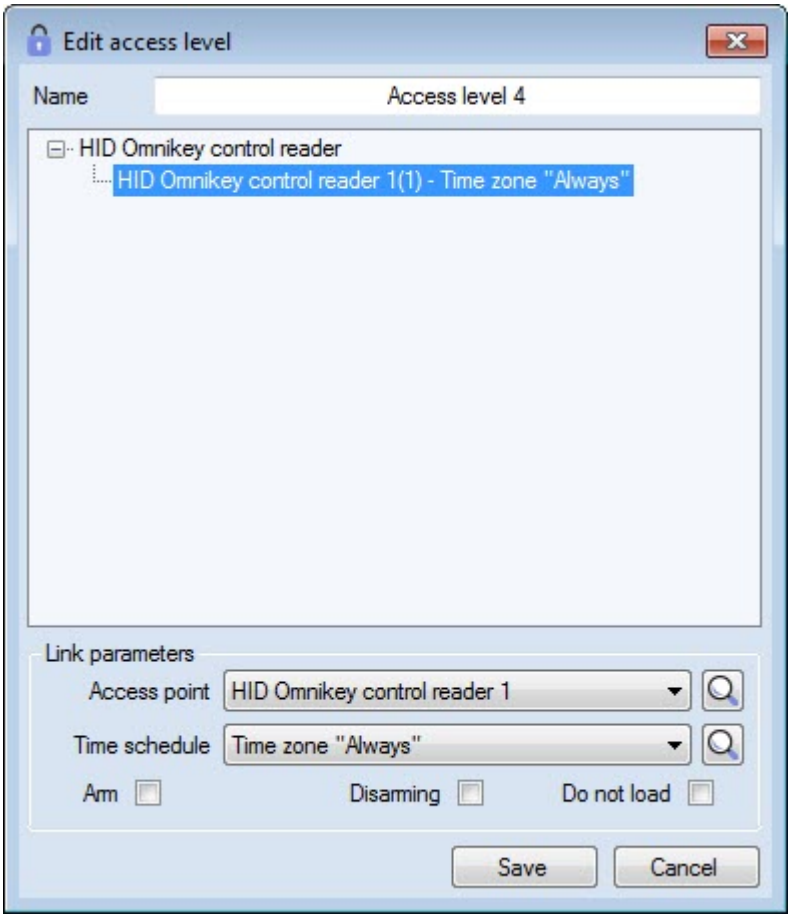
6.4.3 Editing an access level in the Access Manager software module

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.

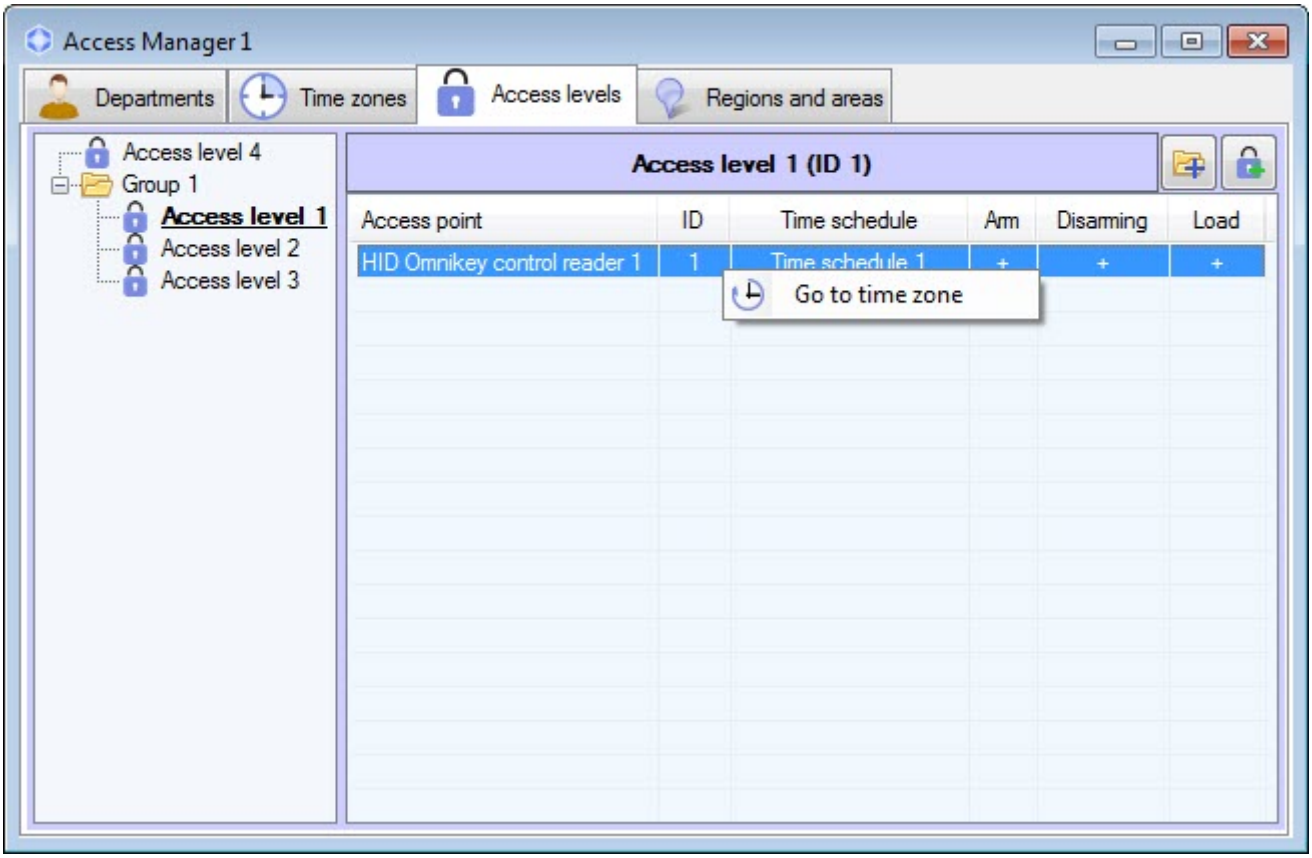


As a result the **Edit access levels** window will be opened. Working with this window is the same as while creating access level - see Create access level section.



6.4.4 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.



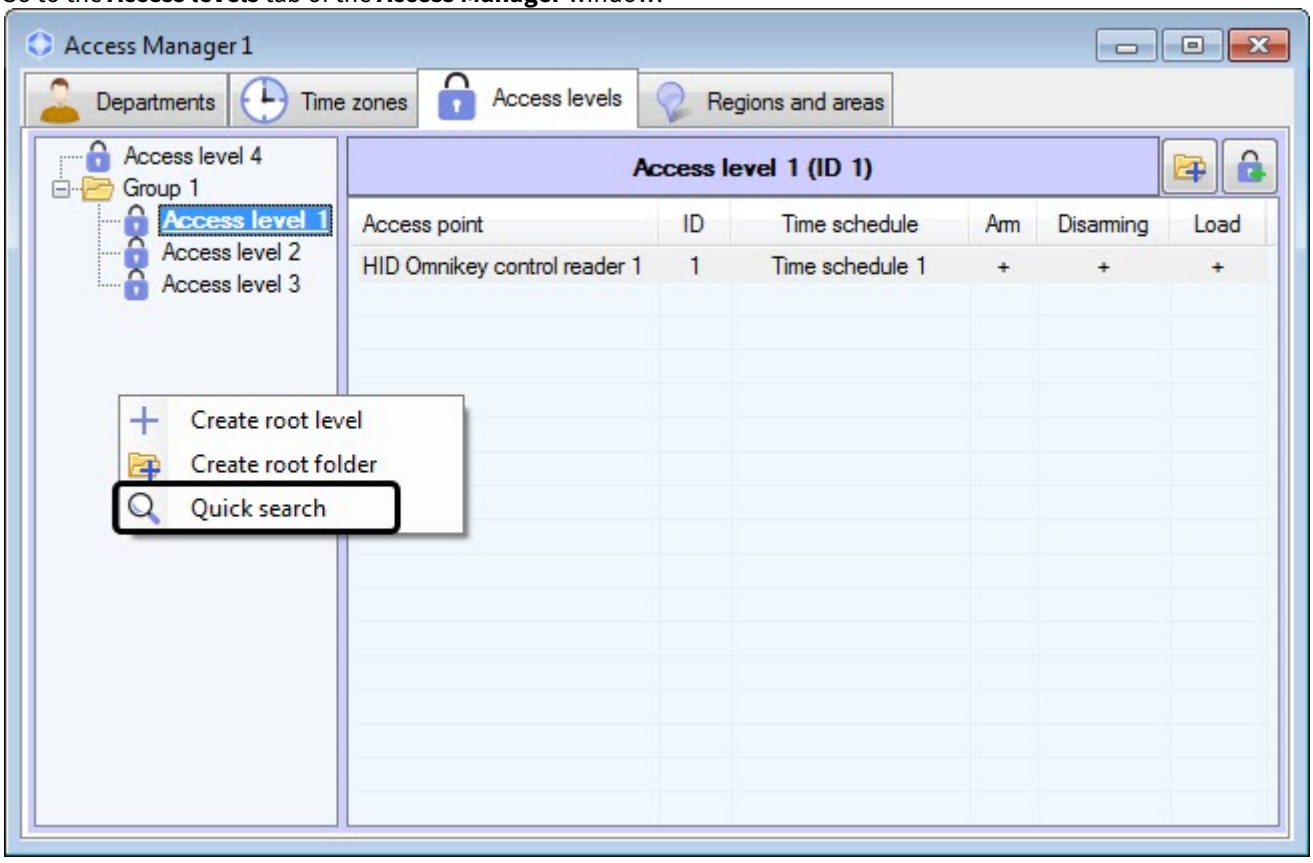
As a result, the **Time zones** tab with the required zone will be opened.

6.4.5 Search for access level

6.4.5.1 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.



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 woking with the functional menu, see Managing the list of access levels.

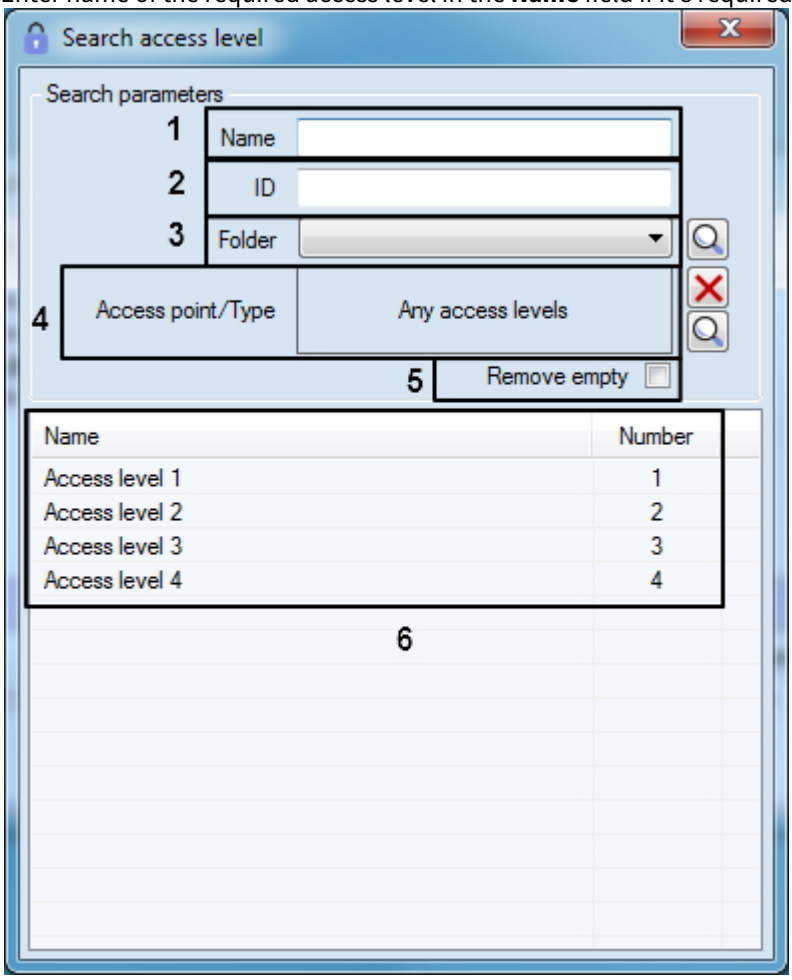
Going to search for access level is completed. Working with the **Search for access level** window is described in the Working with the Search for access level window section.

6.4.5.2 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).

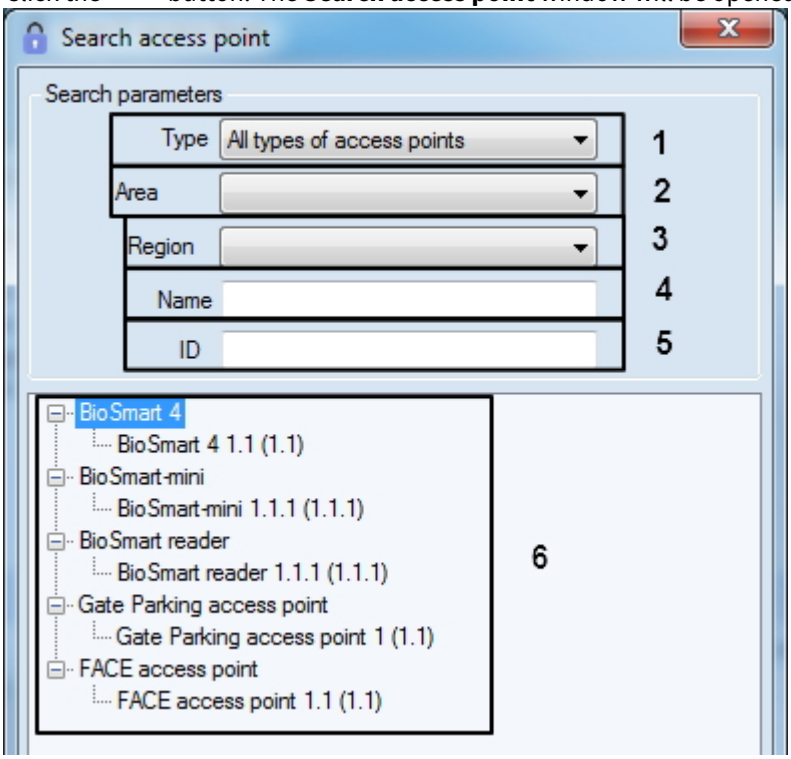
Working with the **Search access level** window is performed as follows:

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.

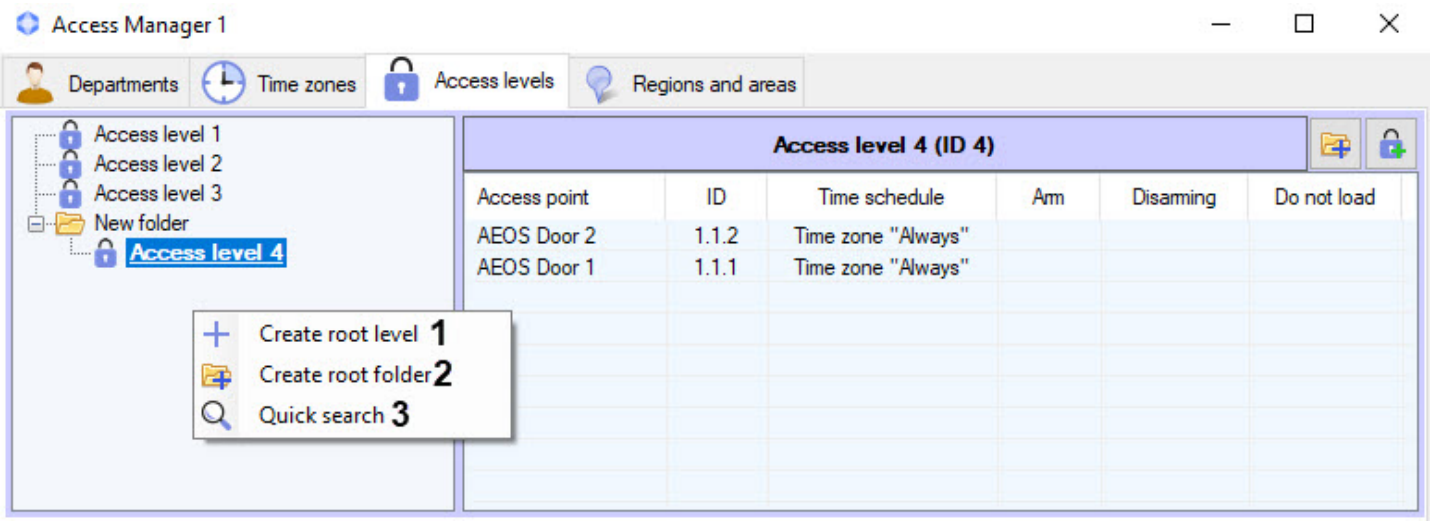
To sort search results click the left mouse button on title of corresponding column.

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.

6.4.6 Managing the list of access levels

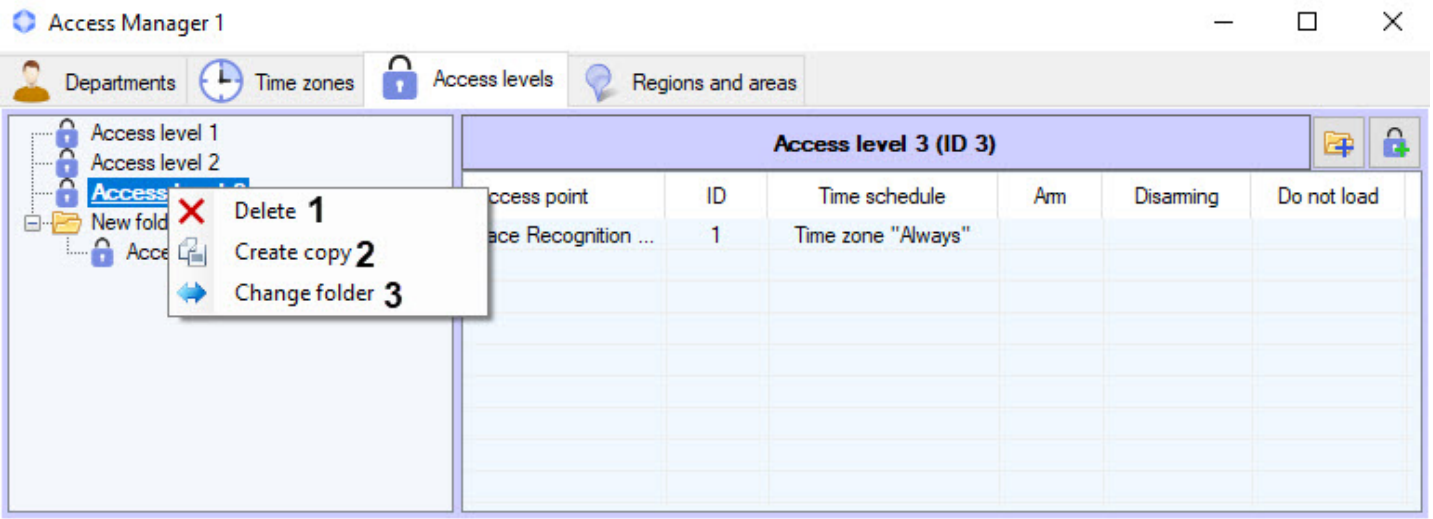
The list of access levels is managed using the context menu, invoked by clicking the right mouse button on the free space around the list.



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 Creating access levels.
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.

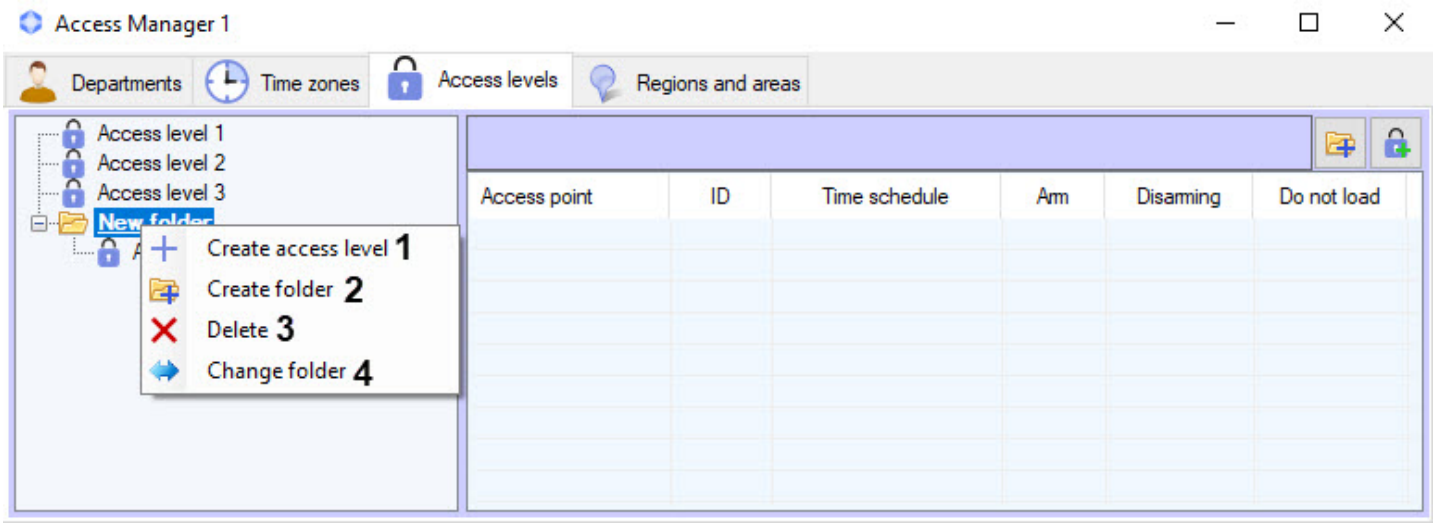


The commands of the context menu are described in the table.

#	Command	Description

1	Delete	Removes an item from the access level list after confirmation from the user. If deletion of assigned access levels is forbidden (see Setting the prohibition of deleting non-empty departments, assigned ALs and TZs), the access level can only be deleted if it is not assigned to any user. When you try to delete an assigned access level, the **Invalid operation** warning is displayed indicating users to which the access level is assigned.
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. After you select the required folder, press the Enter key on the keyboard or the **OK** button in the folder selection window.

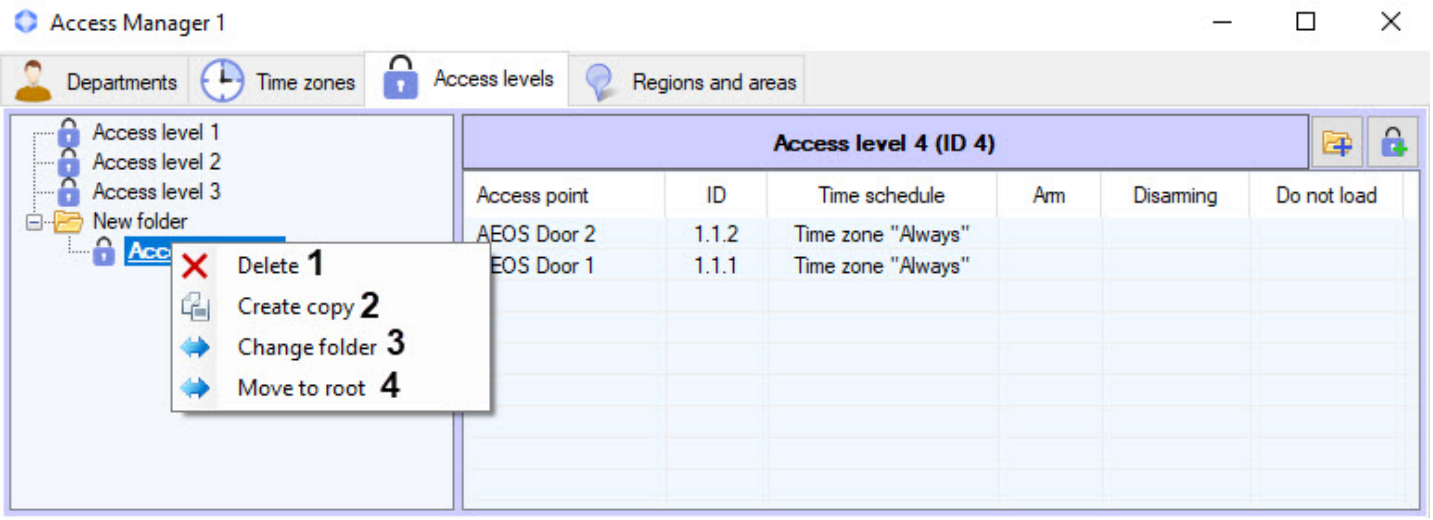
An individual folder in the access level list is managed using the context menu, invoked by clicking the right mouse button on the folder.



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 Creating access levels.
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. If deletion of assigned access levels is forbidden (see Setting the prohibition of deleting non-empty departments, assigned ALs and TZs), the access level can only be deleted if it is not assigned to any user. When you try to delete an assigned access level, the **Invalid operation** warning is displayed indicating users to which the access level is assigned.
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. After you select the required folder, press the Enter key on the keyboard or the **OK** button in the folder selection window.

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



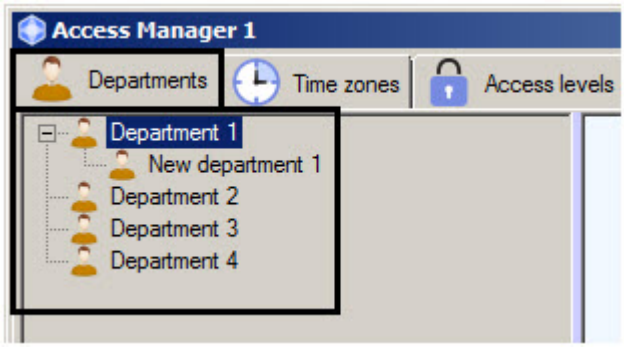
The commands of the context menu are described in the table.

#	Command	Description
1	Delete	Removes an access level from the access level list after confirmation from the user. If deletion of assigned access levels is forbidden (see Setting the prohibition of deleting non-empty departments, assigned ALs and TZs), the access level can only be deleted if it is not assigned to any user. When you try to delete an assigned access level, the **Invalid operation** warning is displayed indicating users to which the access level is assigned.
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. After you select the required folder, press the Enter key on the keyboard or the **OK** button in the folder selection window.
4	Move to root	Moves the selected access level from the folder back to the root of the access level list.

6.5 Working with departments in the Access Manager software module

6.5.1 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.

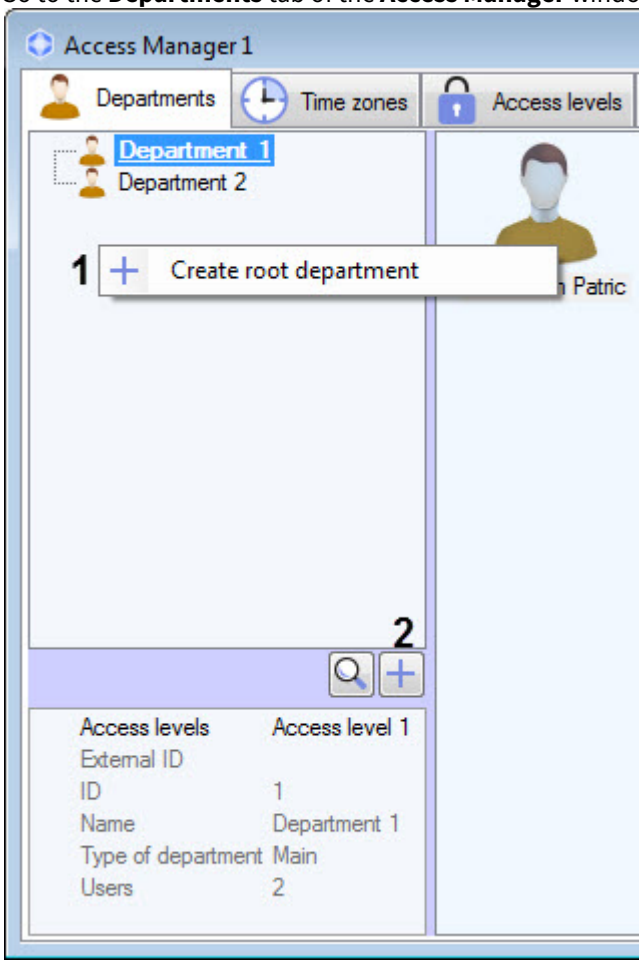


It's possible to create departments on the basis of some existed department and in the root of hierarchy. Functions of editing, deleting and viewing departments are available. Possibility of creating, editing and viewing departments can be limited while configuring the *Access Manager* software module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

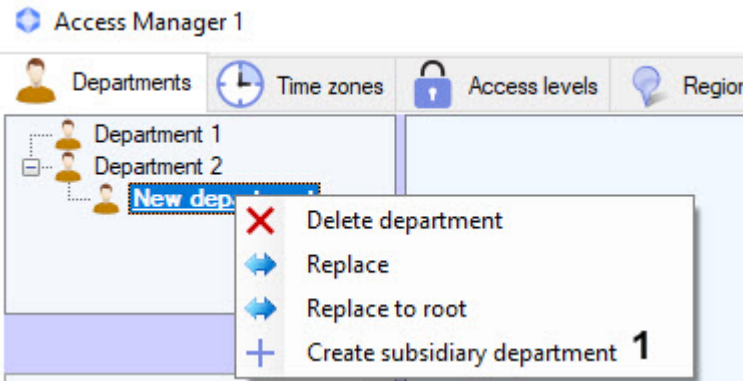
6.5.2 Adding and deleting a department

To add department, do the following:

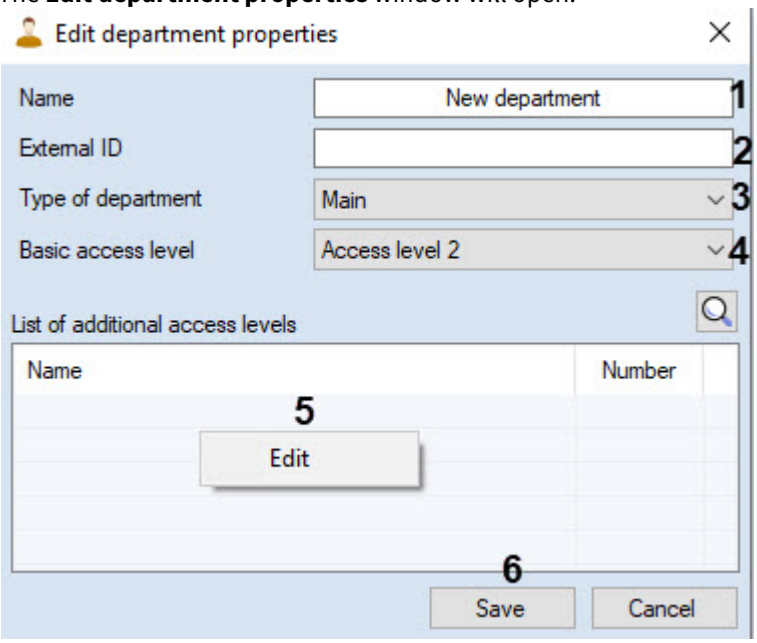
1. Go to the **Departments** tab of the **Access Manager** window.



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 (**1**) or click the  button (**2**).
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 (**1**).



3. The **Edit department properties** window will open.



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

> **Note**
>
> The name should be unique. If an access level with this name has already been created in the system, then while saving, a corresponding message will be displayed and the department will not be saved. Also, the name should not contain the following characters: < | >.

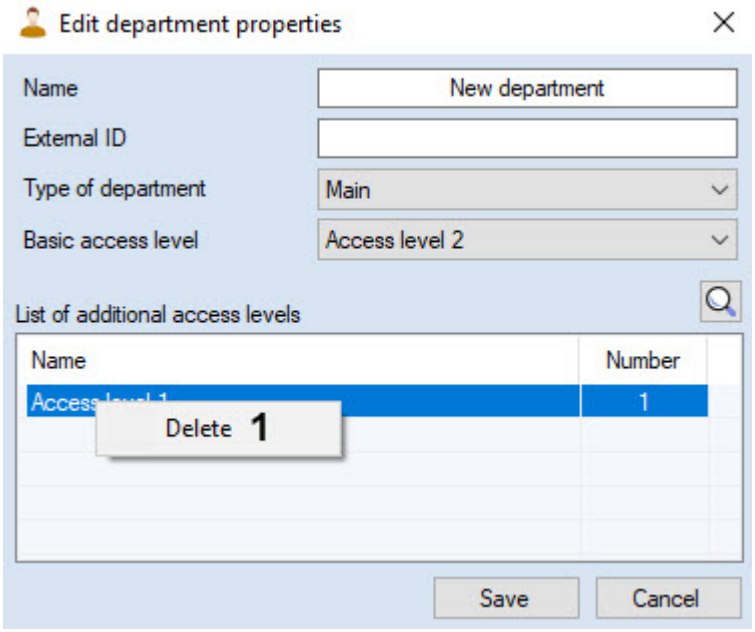
5. In the **External ID** field enter external identical number of department (2). This field is required if, due to the peculiarities of the ACS integration module, the list of departments and users in the database of the *ACFA Intellect* software package is used together with users database in external software.
6. From the **Type of department** drop-down list select the required 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 only default type of department in the *Access Manager* module (see Configuring Main 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 the 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 **Edit** 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.

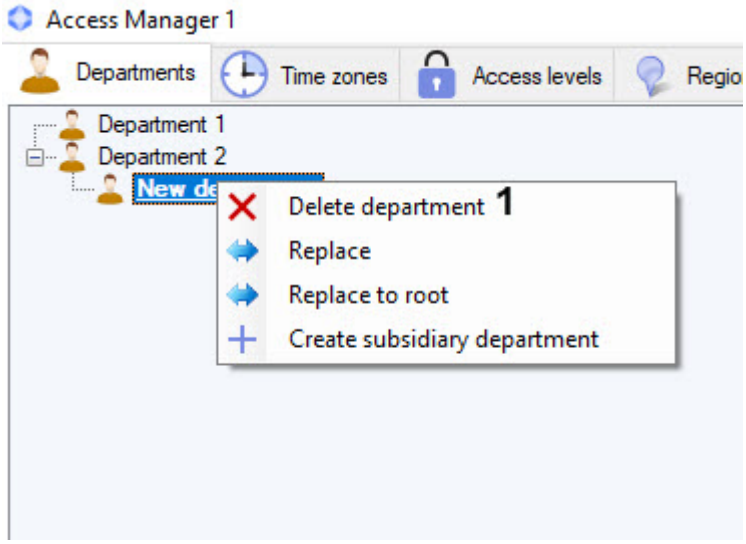
> **Note**
>
> To delete the additional access level click it the right mouse button and select the **Delete** item in the opened functional menu.



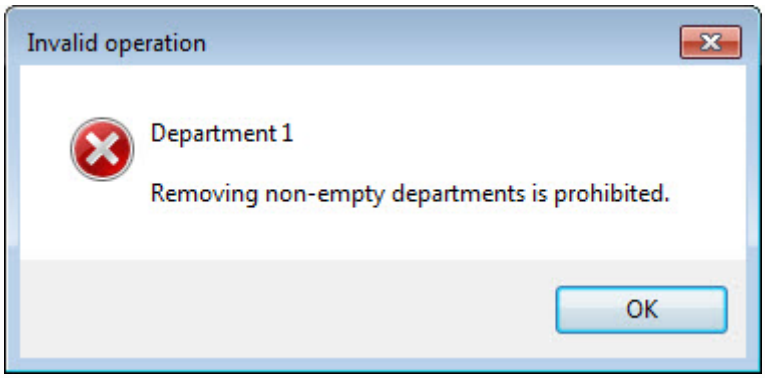
9. Click the **Save** button (5) or the Enter key on the keyboard.

Department will be added to the tree.

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

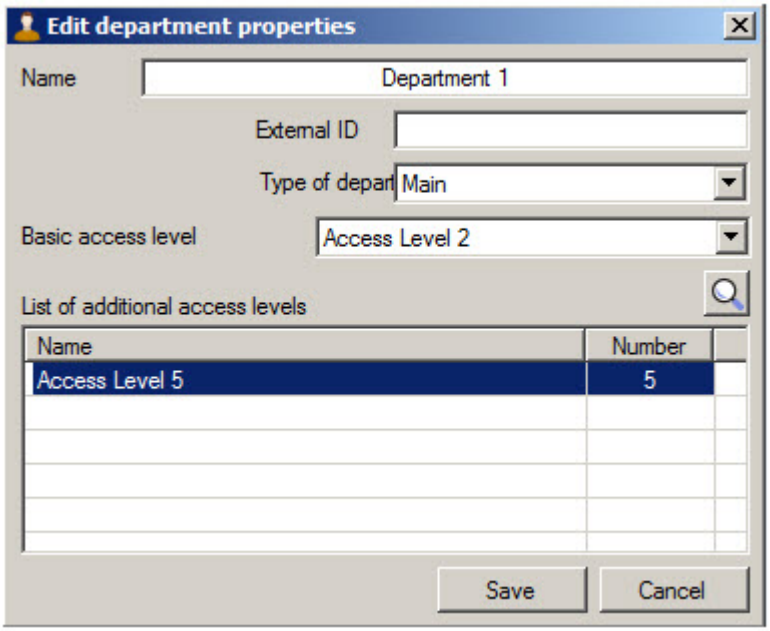


> **Note**
>
> If deletion of non-empty departments is prohibited, the department can only be deleted if there are no users in it (see Setting the prohibition of deleting non-empty departments, assigned ALs and TZs). When you try to delete a non-empty department, the **Invalid operation** warning is shown.



6.5.3 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 and deleting a department section.



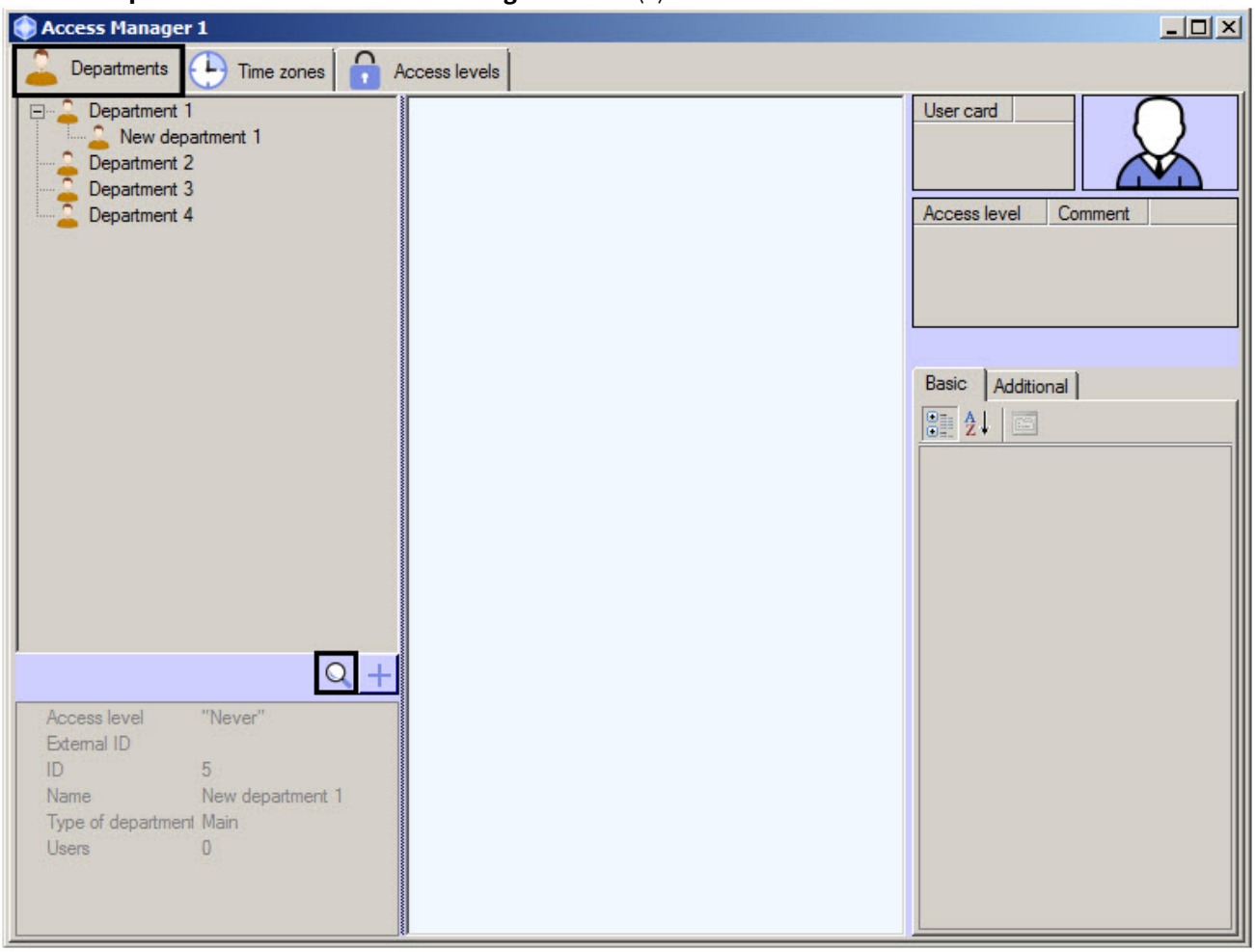
6.5.4 Department search in the Access Manager software module

6.5.4.1 Going to department search

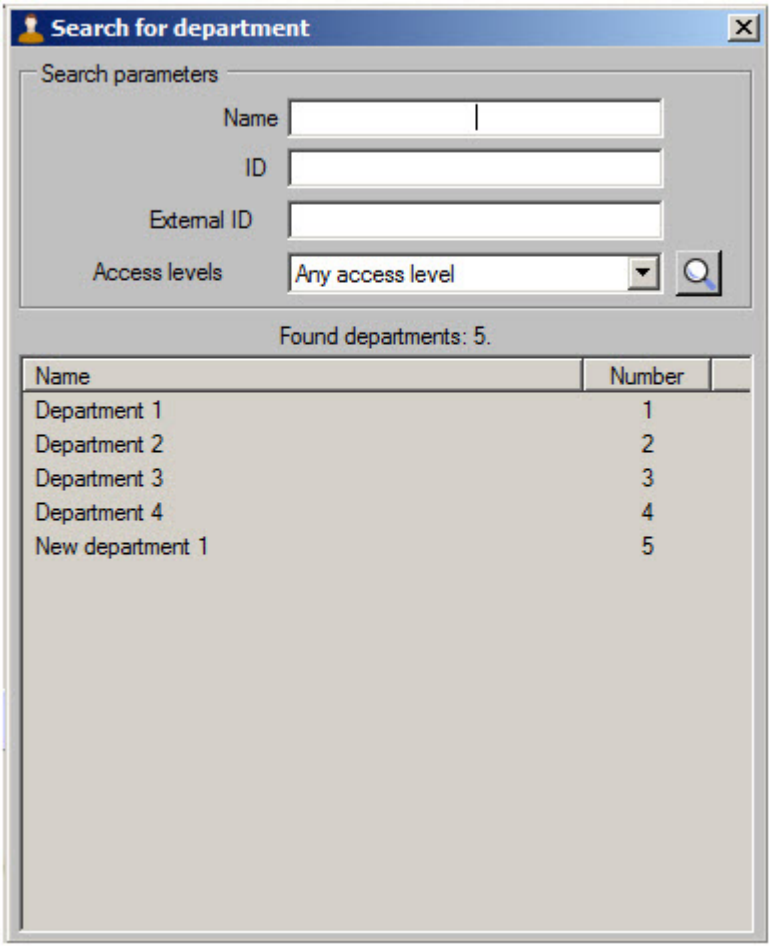
In the *Access Manager* software module it's possible to search for departments by name, ID, external ID and access level.

To go to department search, do the following:

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



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



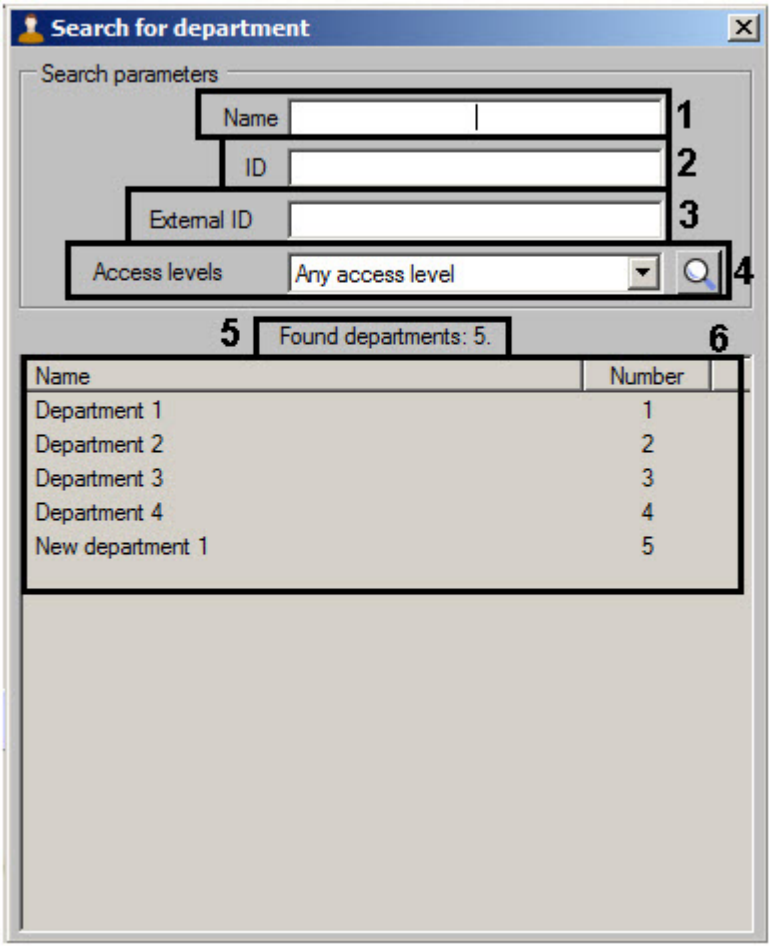
Going to department search is completed. Working with the Search for department is described in the Working with Search for department window section.

6.5.4.2 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.

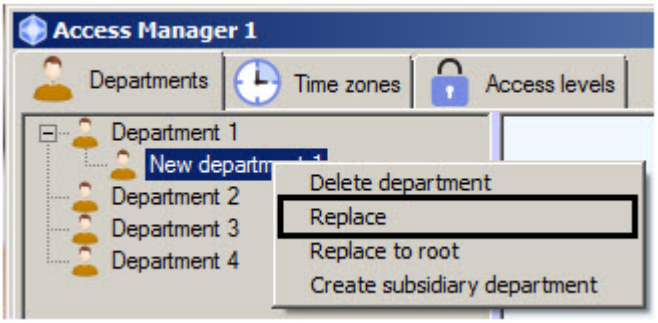
Department search is completed.

6.5.5 Creating departments hierarchy

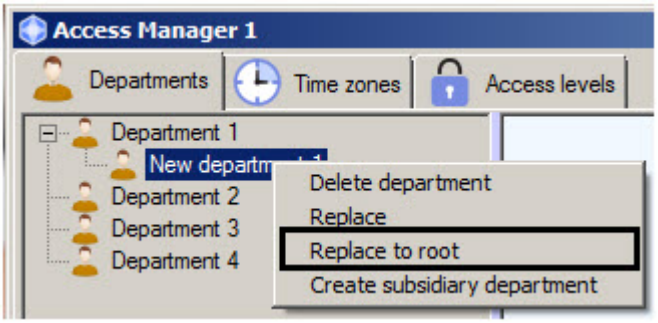
The departments hierarchy is created using the following operations:

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.



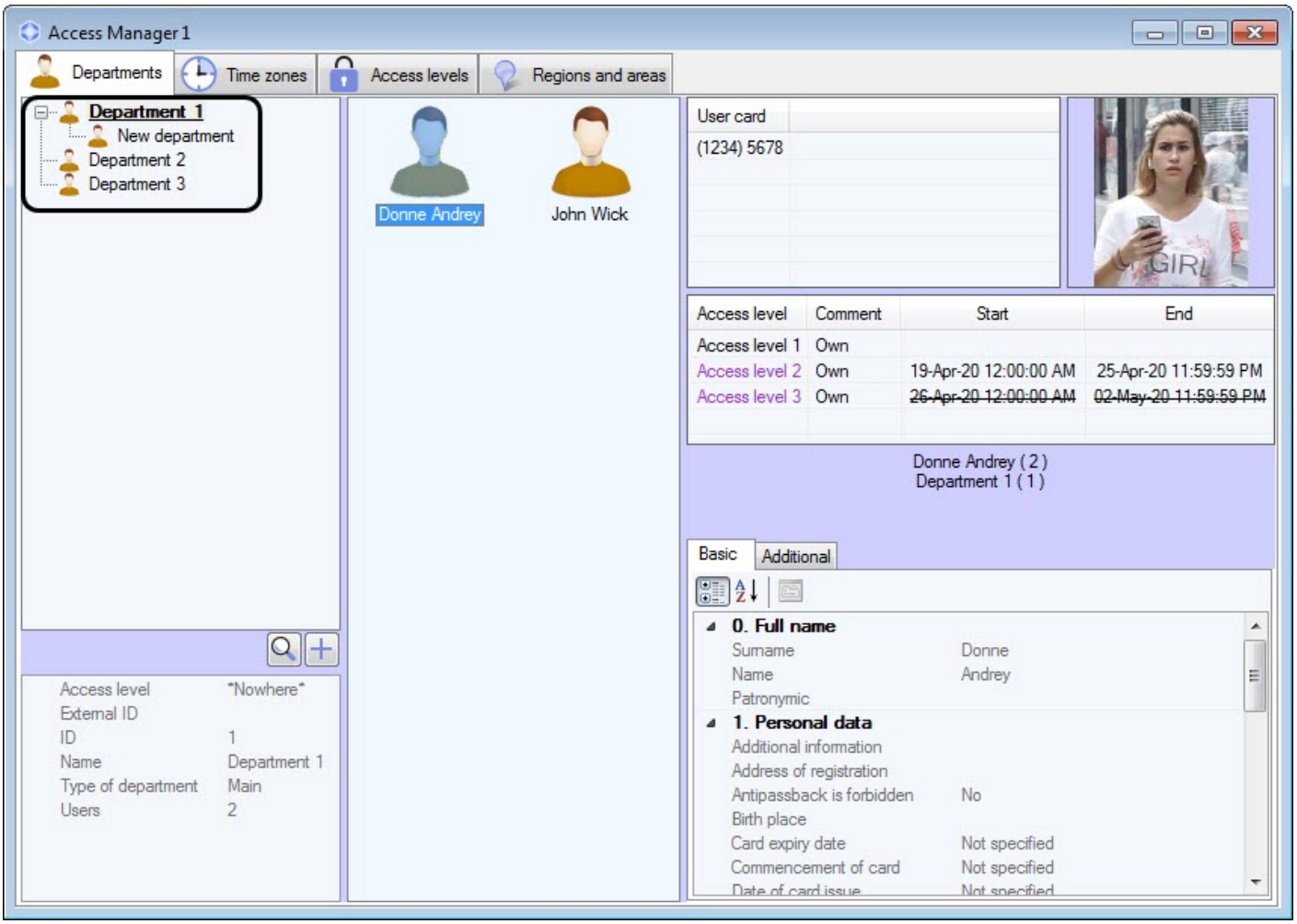
3. Change the department location by dragging it with the left mouse button holding the Ctrl key.

> **Note**
>
> Department replaces in hierarchy with its subsidiary departments.

6.6 Working with users in the Access Manager software module

6.6.1 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.



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.

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.

Press the key combination Ctrl+Shift+M, and the user control panel will be displayed at the bottom of the window:

- **Search** (**1**) - User search in the Access Manager software module.
- **Delete** (**2**) - Deleting a user in the Access Manager software module.
- **New** (**3**) - Creating users in the Access Manager.

Note

To hide this panel, press the key combination Ctrl+Shift+M again.

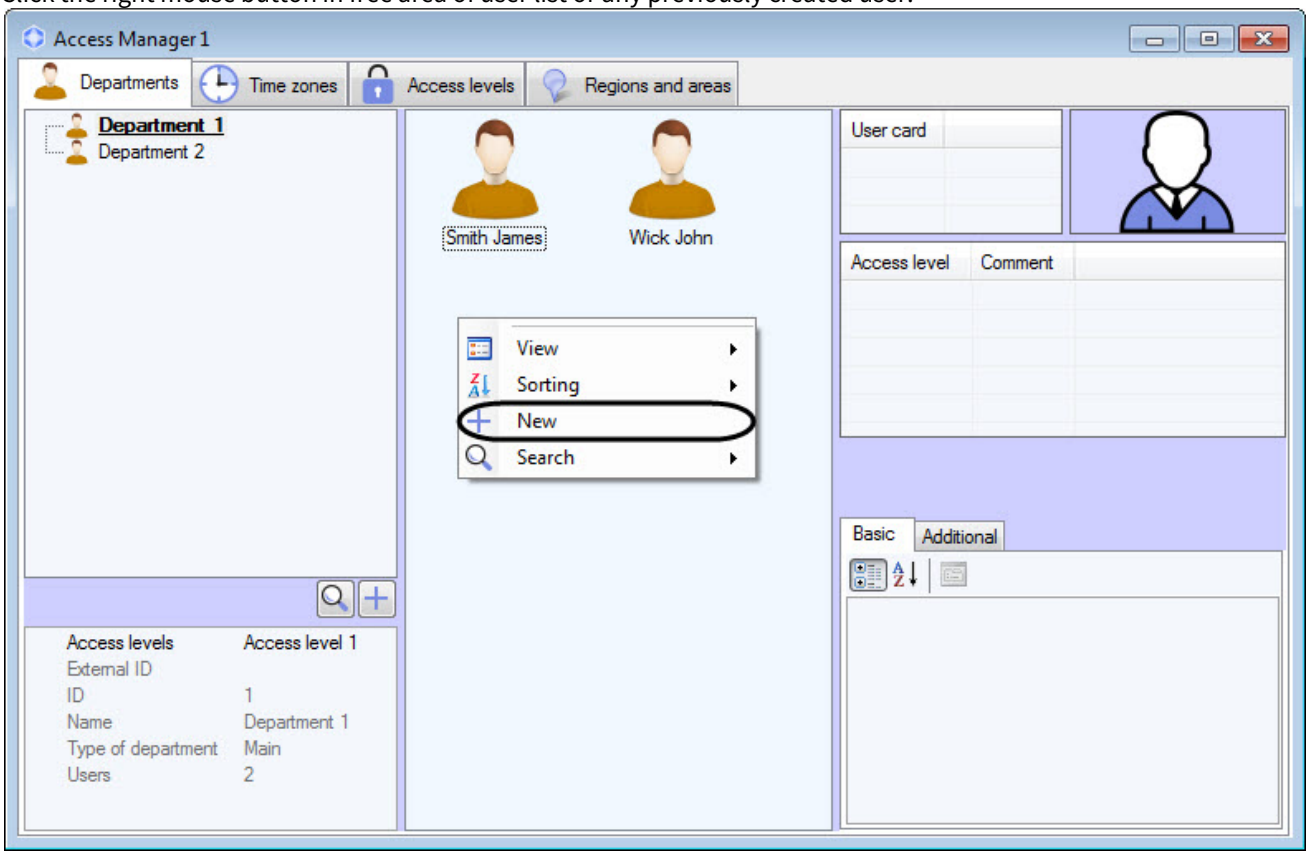
6.6.2 Creating users in the Access Manager

To add a new user, do the following:

Note

In addition to the method described below, you can also create new users by clicking the **New** button on the user control panel (see Viewing a list of users).

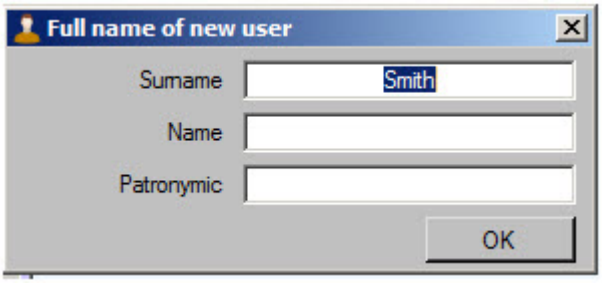
1. Open a list of users (see Viewing a list of users).
2. Click the right mouse button in free area of user list or any previously created user.



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 Configuring the object management rights section.

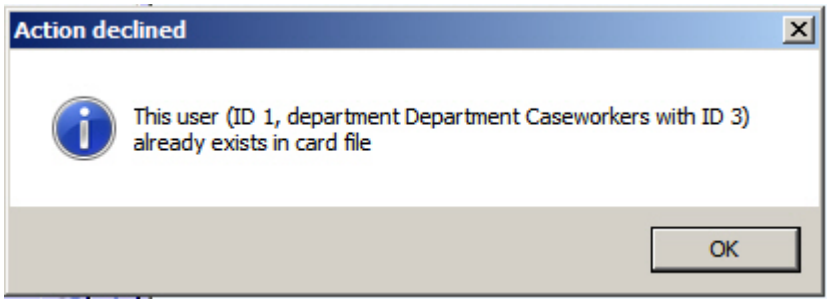
3. Select the **New** item in the opened functional menu. The **Full name of new user** window will open.



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

Note

- Surname, name and patronymic should not contain the following characters: < | >.
- 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 the prohibition of new user parameter duplicates in Access Manager section.



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

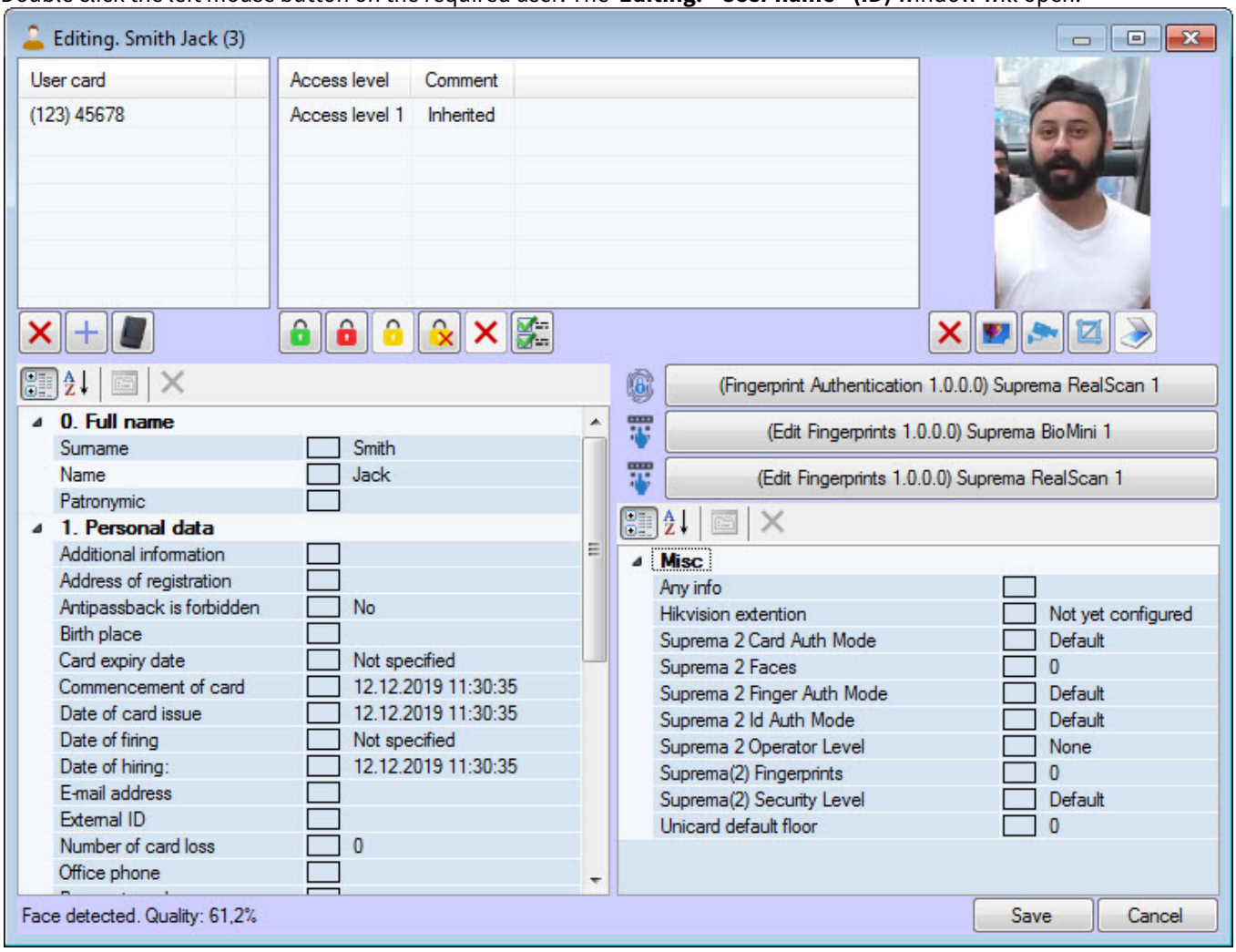
Further process of user creation is given in the Editing a user section.

6.6.3 Editing a user

6.6.3.1 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.



It is 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).
f. Opening a folder with user documents.
g. Adding extension buttons.

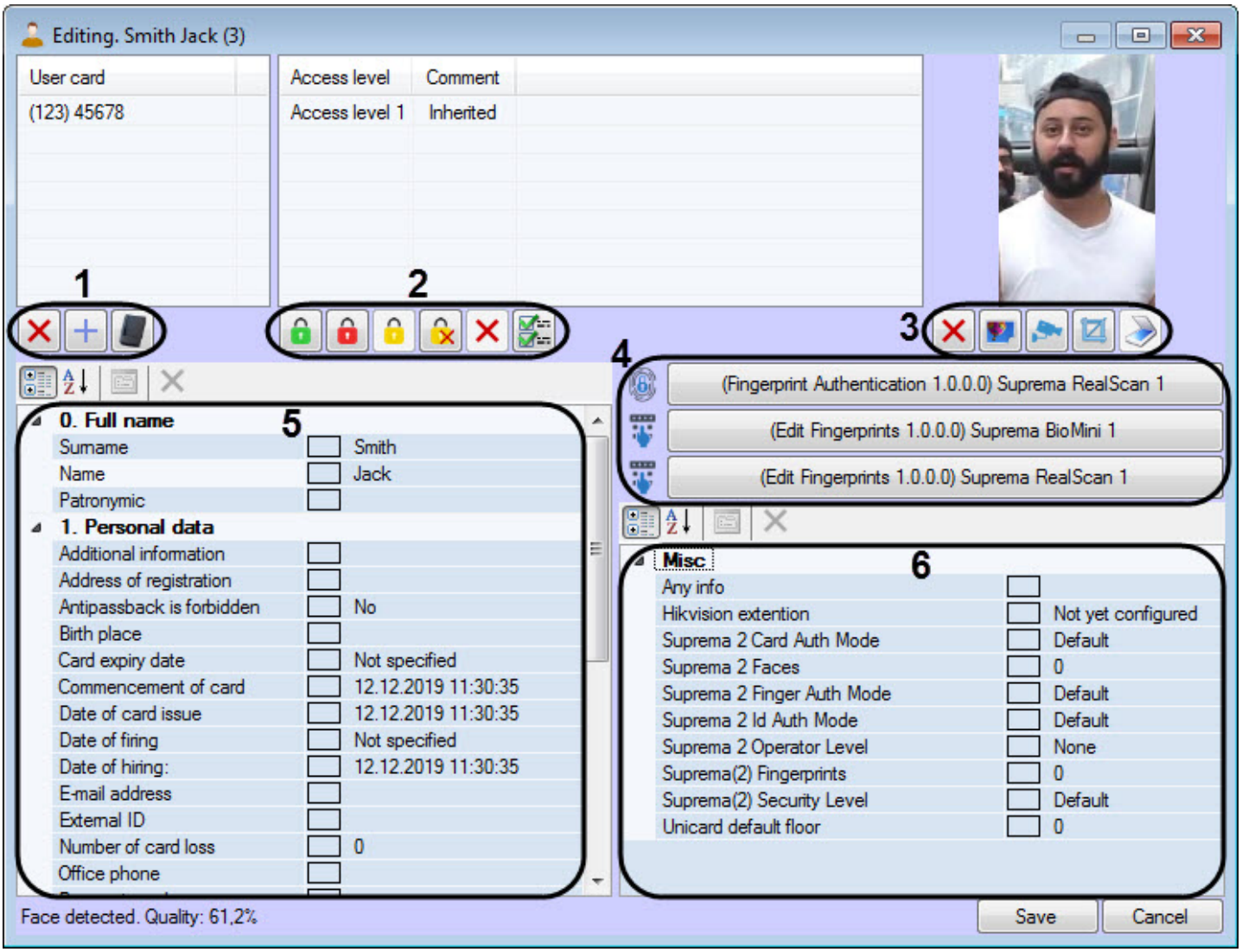
All actions are described as follows.

> **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 Configuring the object management rights section.

Going to user editing is completed.

6.6.3.2 Setting user parameters

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



The button panel (**1**) allows performing the following actions:

-  - delete the selected user card (see Deleting of access card).
-  - add a user card manually (see Manual input of access card number).

-  - add a user card using the control reader (see Input of card number using a control reader).

The button panel (**2**) allows performing the following actions:

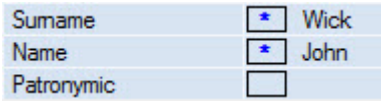
-  - set full access (see Assigning Own access level to a user).
-  - prohibit the access (see Assigning Own access level to a user).
-  - enable the department access level inheritance (see Configuring the department access level inheritance).
-  - disable the department access level inheritance (see Configuring the department access level inheritance).
-  - delete **Own** access level (see Assigning Own access level to a user).
-  - edit access level (see Assigning Own access level to a user).

The button panel (**3**) allows performing the following actions:

-  - delete the photo assigned to the user (see Deleting a photograph).
-  - assign the user a photo from the file (see Assigning photograph from a file).
-  - assign the user a photo from the camera (see Assigning a photograph from a video camera).
-  - crop the photo assigned to the user (see Cropping a photograph).
-  - this button is used only in the Russian version of *ACFA Intellect*, and is inactive in the English version.

The button panel (**4**) allows you to add biometric parameters to users (see Adding biometric parameters).

In the fields (**5**) and (**6**), a rectangle is displayed next to each field. When the field is changed, the "*****" sign is displayed in the rectangle until the user editing window is opened again.



> **Note**
>
> 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.

The following **Standard fields** are displayed in the field (**5**):

Parameter name	Parameter setting method	Default category in templates	Value range	Comme
Surname	Enter the value in the field	0. Full name	Any characters except: < | >	-
Name	Enter the value in the field	0. Full name	Any characters except: < | >	-
Patronymic	Enter the value in the field	0. Full name	Any characters except: < | >	-
Additional information	Enter the value in the field	1. Personal data	Any characters except: < | >	Enter a When y
Access level assigned by	Automatically	1. Personal data	Operator name	Name o

Address of registration				
Antipassback is forbidden	Select the value from the list	1. Personal data	Yes No	Default
Birth place	Enter the value in the field	1. Personal data	Any characters except: < | >	Place o
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	If the co
Card issued by	Automatically	1. Personal data	Operator name	Name o
Commencement of card	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	-
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	-
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	-
E-mail address	Enter the value in the field	1. Personal data	Any characters except: < | >	User e-r
External ID	Enter the value in the field	1. Personal data	Any characters except: < | >	This fiel
Number of card loss	Enter the value in the field	1. Personal data	Numbers	-
Office phone	Enter the value in the field	1. Personal data	Any characters except: < | >	Office p
Passport number	Enter the value in the field	1. Personal data	Any characters except: < | >	Passpo
Personnel number	Enter the value in the field	1. Personal data	Any characters except: < | >	-
PIN code	Enter the value in the field	1. Personal data	Numbers	-
Position	Enter the value in the field	1. Personal data	Any characters except: < | >	-
Telephone	Enter the value in the field	1. Personal data	Any characters except: < | >	Telepho
User locked	Select the value from the list	1. Personal data	Yes No	Yes – us No – us
Driving license	Enter the value in the field	3. Vehicle	Any characters except: < | >	Numbe
Vehicle LP	Enter the value in the field	3. Vehicle	Any characters except: < | >	License Server I
Vehicle model	Enter the value in the field	3. Vehicle	Any characters except: < | >	Model o

Document	Enter the value in the field	4. Visitor data	Any characters except: < | >	Present
Origin	Enter the value in the field	4. Visitor data	Any characters except: < | >	Name o
Purpose of visit	Enter the value in the field	4. Visitor data	Any characters except: < | >	Purpos
To which department	Enter the value in the field	4. Visitor data	Any characters except: < | >	Departr
To whom	Enter the value in the field	4. Visitor data	Any characters except: < | >	Employ

The following **Additional fields** are displayed in the field (**6**):

Parameter name	**Parameter setting method**	**Default category in templates**	**Value range**	**Comment**
Apollo SDK v.3 extension	Configurating	Misc	Unconfigured Configured	(see ApolloSDK v.3 Integration Module Settings Guide).
Galaxy Dual	Select the value from the list		Yes No	(see Honeywell Galaxy Dimension Integration Module Settings Guide).
Galaxy Dual Access	Select the value from the list		Yes No	
Galaxy Dual Focus	Select the value from the list		Yes No	
Galaxy Duress	Select the value from the list		Yes No	
Galaxy Group Choice	Select the value from the list		Yes No	
Galaxy Keypad	Enter the value in the field		NONE 10-51	
Galaxy Menu Choice	Select the value from the list		Yes No	
Galaxy Menu Level	Select the value from the list		1.0 2.1 2.3 2.4 2.5 3.6	
Galaxy Menu Option	Select the value from the list		NONE 11-71	

Galaxy Pin Change	Select the value from the list	Yes No	
Galaxy Tag Link	Enter the value in the field	Numbers	
Galaxy Temp Code	Enter the value in the field	Numbers	
Galaxy Template	Enter the value in the field	Numbers	
Galaxy Timer Schedule	Enter the value in the field	Numbers	
Group number	Enter the value in the field	Numbers	-
Hikvision extension	Configurating	Unconfigured Configured	(see Hikvision Integration Module Configuration and Operation Guide).
Level in first card mode	Enter the value in the field	Numbers	-
Ravelin Access type	Select the value from the list	Card only Master card Card and pin Slave card	(see Gate Integration Module Setup and User Guide).
Ravelin guest card	Select the value from the list	Yes No	
Soyal Access type	Select the value from the list	Card only Card or PIN Card and PIN Access denied	(see Soyal Integration Module Settings Guide).
Soyal Can pass in and out	Select the value from the list	Yes No	
Soyal Card Level	Select the value from the list	0-10	
Soyal Patrol card	Select the value from the list	Yes No	
Soyal PWD change available	Select the value from the list	Yes No	

Suprema 2 Card Auth Mode	Select the value from the list	Default Only Card Card And Fingerprint Card And Pin Fingerprint Or Pin After Card Card And Fingerprint and Pin Cannot Use	(see Suprema 2 Settings Guide).
Suprema 2 Faces	Automatically	Numbers	
Suprema 2 Finger Auth Mode	Select the value from the list	Default Only Fingerprint Fingerprint And Pin Cannot Use	
Suprema 2 Id Auth Mode	Select the value from the list	Default Fingerprint After Id Pin After Id Fingerprint Or Pin After Id Fingerprint And Pin After Il Cannot Use	
Suprema 2 Operator Level	Select the value from the list	None Admin System settings User information	
Suprema Bypass Card	Select the value from the list	Yes No	
Suprema(2) Fingerprints	Automatically	Numbers	
Suprema(2) Security Level	Select the value from the list	Default Lower Low Normal Hight Higher	
Unicard code	Enter the value in the field	Any characters except: < | >	(see Unicard Integration Module Settings Guide).

Unicard default floor	Enter the value in the field		Numbers	
Unicard disabled	Enter the value in the field		Numbers	
VertX-Edge Access mode	Select the value from the list		Card or "Card and PIN" Card only PIN only Card only and PIN only	(see HID Integration Module Settings Guide).
VertX-Edge Escort	Enter the value in the field		Any characters except: < | >	
VertX-Edge Exempt PIN	Select the value from the list		Yes No	
VertX-Edge Extended access	Select the value from the list		Yes No	
VertX-Edge PIN commands	Select the value from the list		Yes No	
Group number	Enter the value in the field		Numbers	(see ZK Teco Integration Module Settings Guide).
Level in first card mode	Enter the value in the field		Numbers	

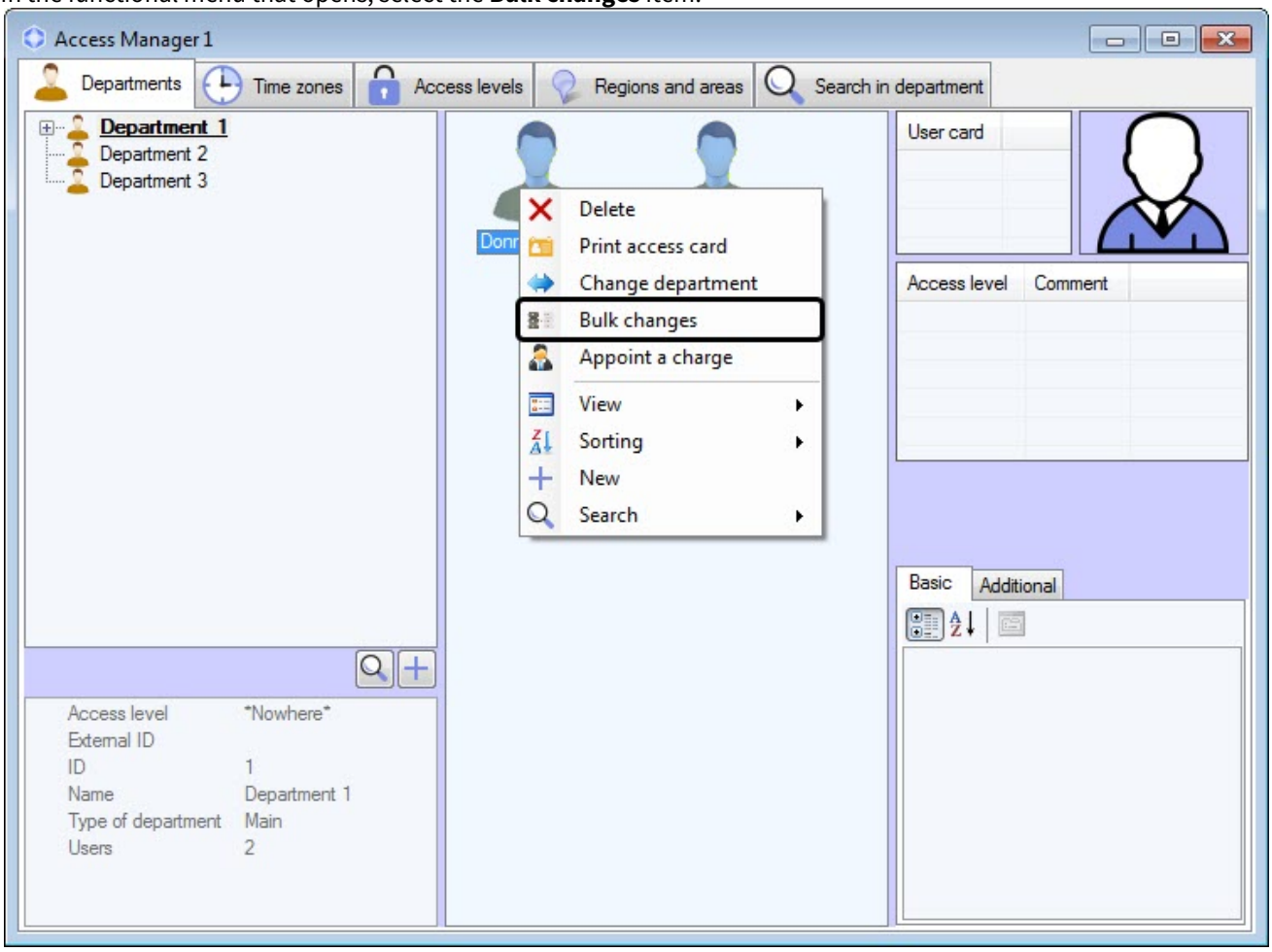
6.6.3.2.1 Bulk editing of users

Bulk editing of users is performed as follows:

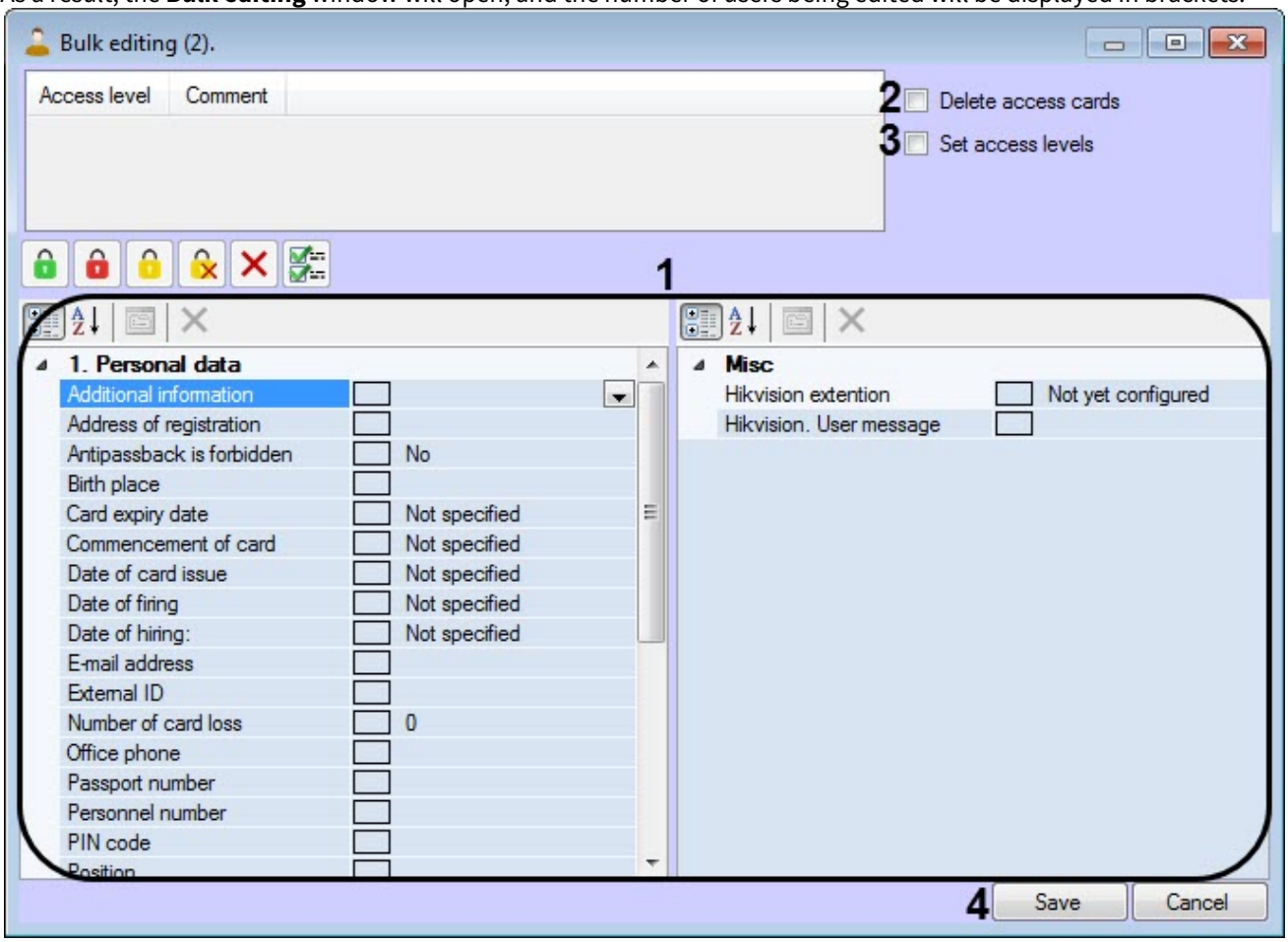
1. Go to viewing the list of users (see Viewing a list of users).
2. Select several users to be edited and right-click on the name of any of the selected users.

> **Note**
>
> You can select several users by using the mouse or keyboard shortcuts (see Keyboard shortcuts for working with interface elements)

3. In the functional menu that opens, select the **Bulk changes** item.



4. As a result, the **Bulk editing** window will open, and the number of users being edited will be displayed in brackets.

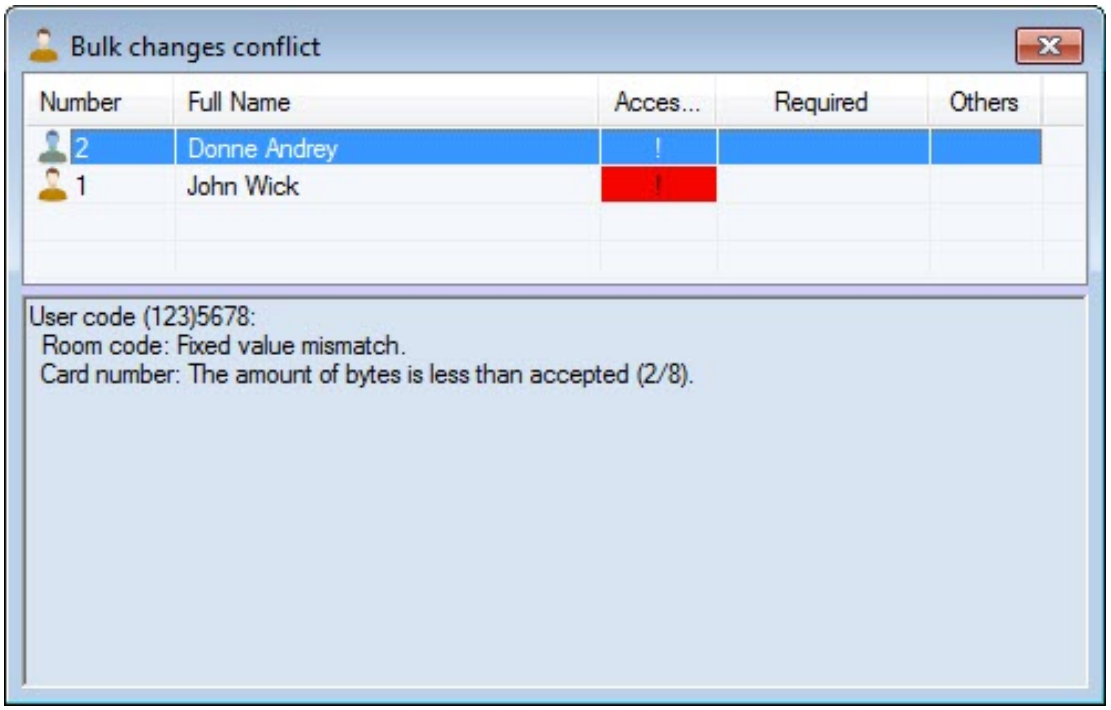


5. Set the standard and additional fields (**1**), which will be the same for all selected users (see Setting user parameters).
6. Set the **Delete access cards** checkbox (**2**) if it is necessary to delete all existing access cards from the selected users.

> **Attention!**
>
> The deletion of access cards for all selected users cannot be undone.

7. Set the **Set access levels** checkbox (**3**) if it is necessary to allow assigning access levels that are the same for all selected users. The procedure of assigning access levels to several users is the same as for one user (see Assigning access levels to a user).
8. Click the **Save** button (**4**) to apply the changes.

> **Attention!**
>
> If the selected users have an access card in a format that differs from the access card format specified in the **Access Manager** object settings (see Configuring access cards), then a list of all users with such cards will be displayed, indicating the cause of the conflict. Changes will not be saved until all conflicts are resolved. If the **Delete access cards** checkbox is set, then the changes can be saved.

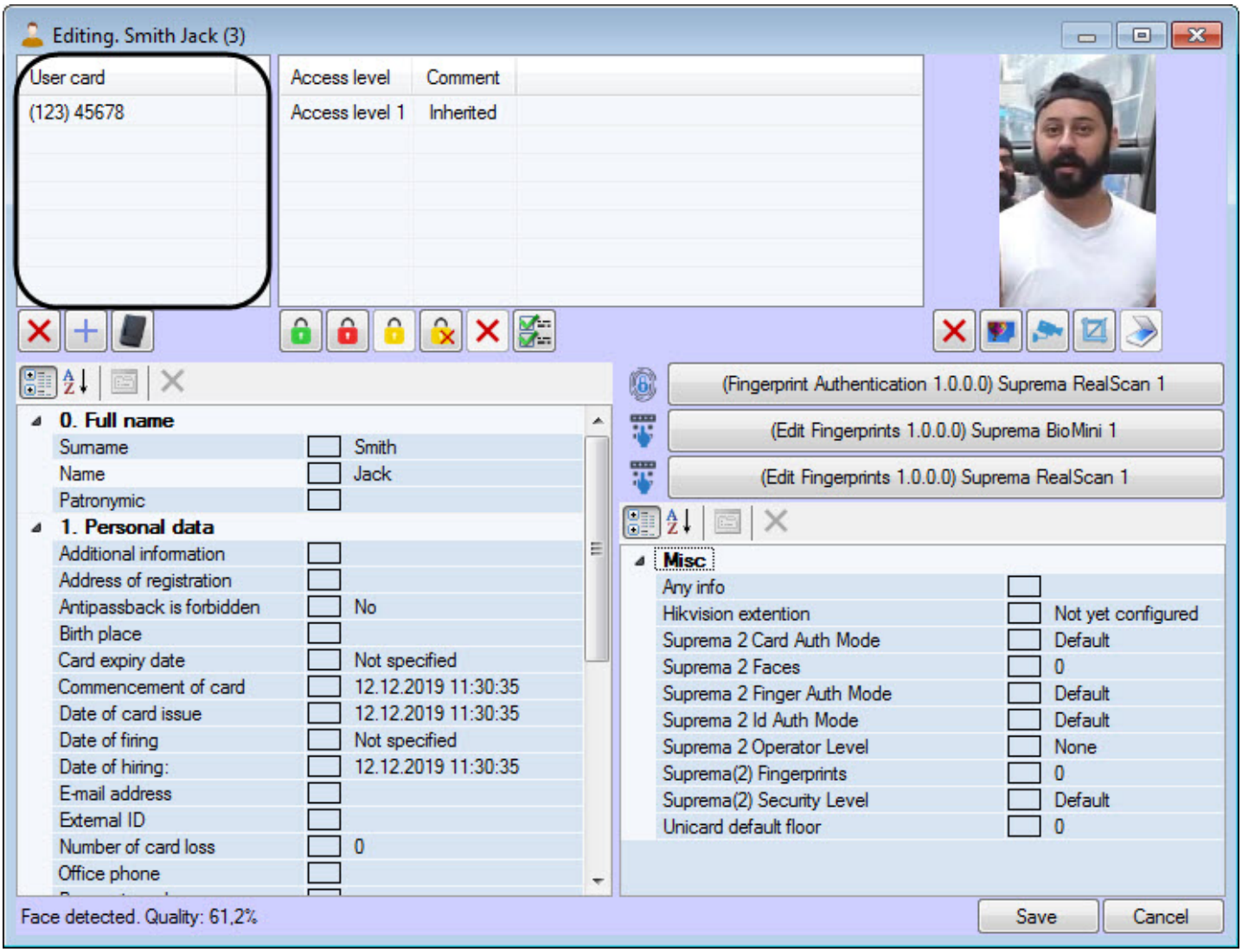


Bulk editing of users is complete.

6.6.3.3 Assigning an access card to a user

6.6.3.3.1 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**.



The object code is specified in brackets, then the card code follows. The access cards format is set in the **Access Manager** object settings (see Configuring access cards).

Several access cards can be assigned to one user.

Attention!

Assigning multiple access cards to a user should be supported by hardware and by the corresponding integration module. If used hardware/integration module supports only one card, and multiple cards are assigned to a used, then all cards excepting the first card will be ignored by system.
Support for multiple user access cards has been tested in the following integration modules: Noder, ApolloSDK v.3, SDK Orion v.2, PERCo-S-20, PERCo-S-20 v.2, AccessNet (ABC), Forteza, ParsecNet 3. For information on others integration modules, please contact the AxxonSoft technical support.

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.

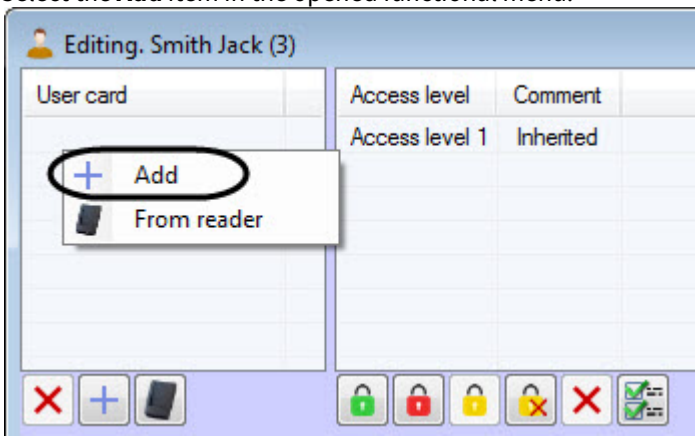
Note

List of control readers used for user access cards input is specified while system configuring - see the Configuring control readers in the Access Manager section.

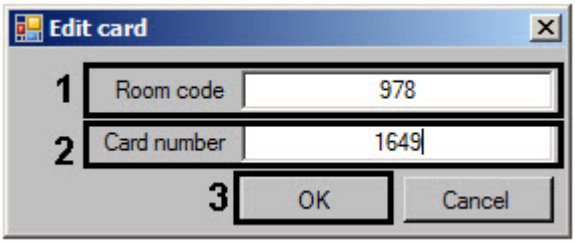
6.6.3.3.2 Manual input of access card number

To input access card number manually, do the following:

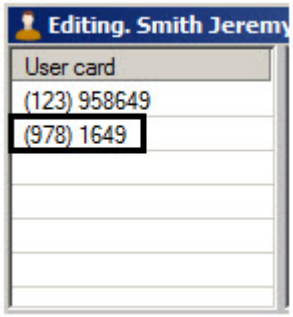
1. Go to editing a user (see the Going to user editing section).
2. Click the right mouse button in card selection area.
3. Select the **Add** item in the opened functional menu.



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.



Input of access card number manually is completed.

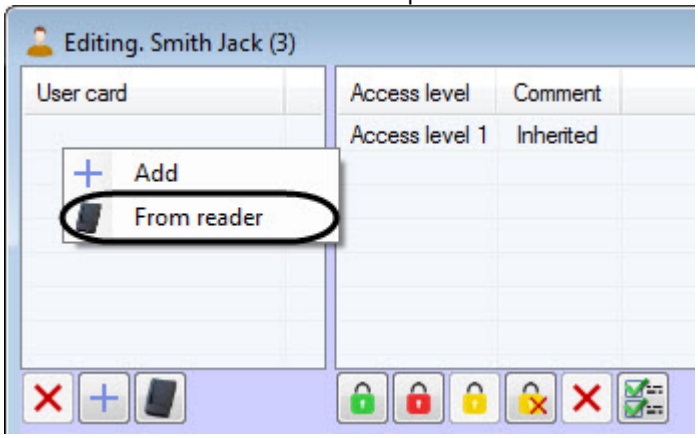
> **Note**
>
> You also can input access card number manually using the corresponding buttons (see Setting user parameters).

6.6.3.3.3 Input of card number using a control reader

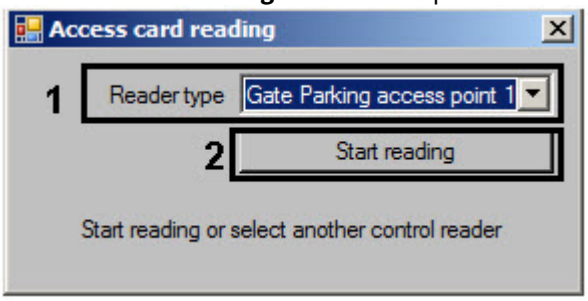
To input access card number using a control reader, do the following:

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.



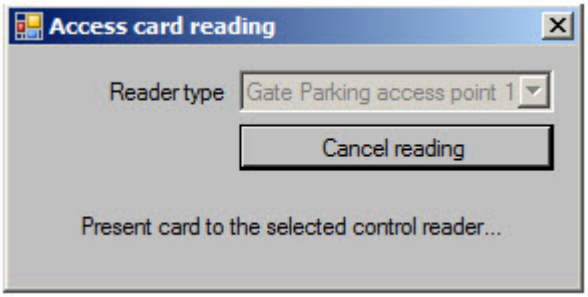
4. The **Access card reading** window will open.



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 Configuring control readers in the Access Manager section).

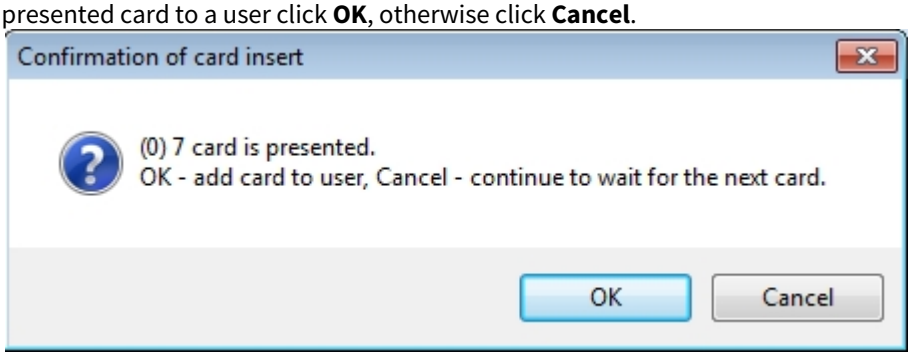
6. Click the **Start reading** button (**2**). The **Access card reading** window will be as follows:



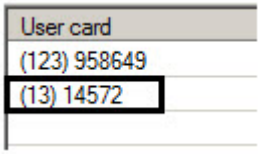
> **Note**
>
> To cancel access card reading click the **Cancel reading** button.

7. Present access card to the selected reader.

8. If confirmation of card input by operator is configured, the **Confirmation of card insert** window will display. To assign presented card to a user click **OK**, otherwise click **Cancel**.

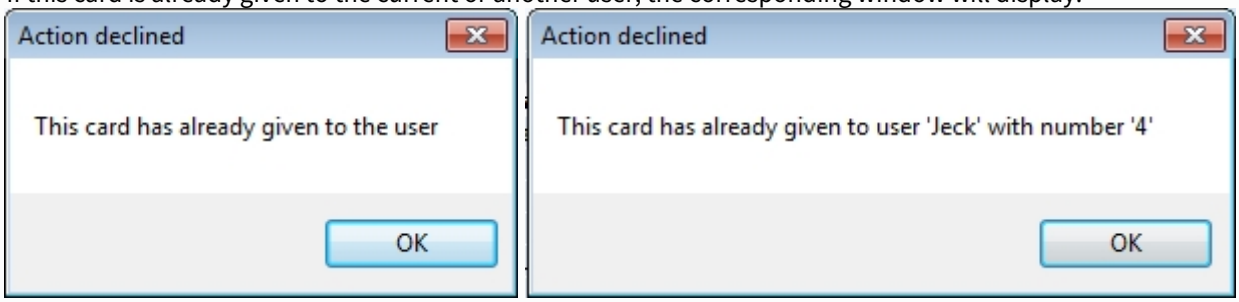


9. Then the **Access card reading** window will be closed and number of presented access card will be added to the list.



Note

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



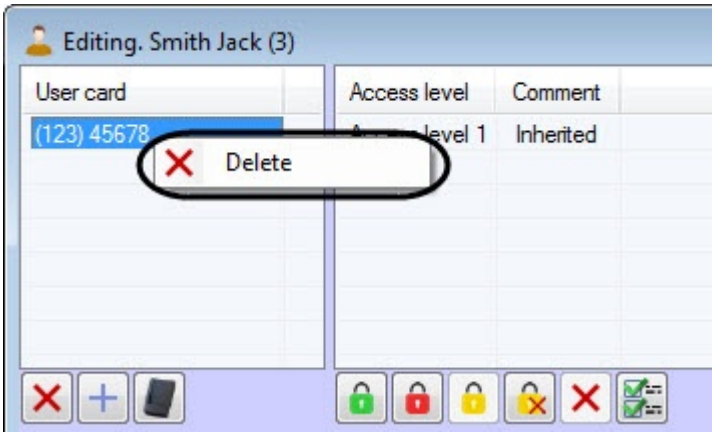
Input of access card using a control reader is completed.

Note

You can also input access card number using a control reader using the corresponding buttons (see Setting user parameters).

6.6.3.3.4 Deleting of access card

To remove a card number from the list, right-click on the card number in the list and select the **Delete** item in the opened functional menu.

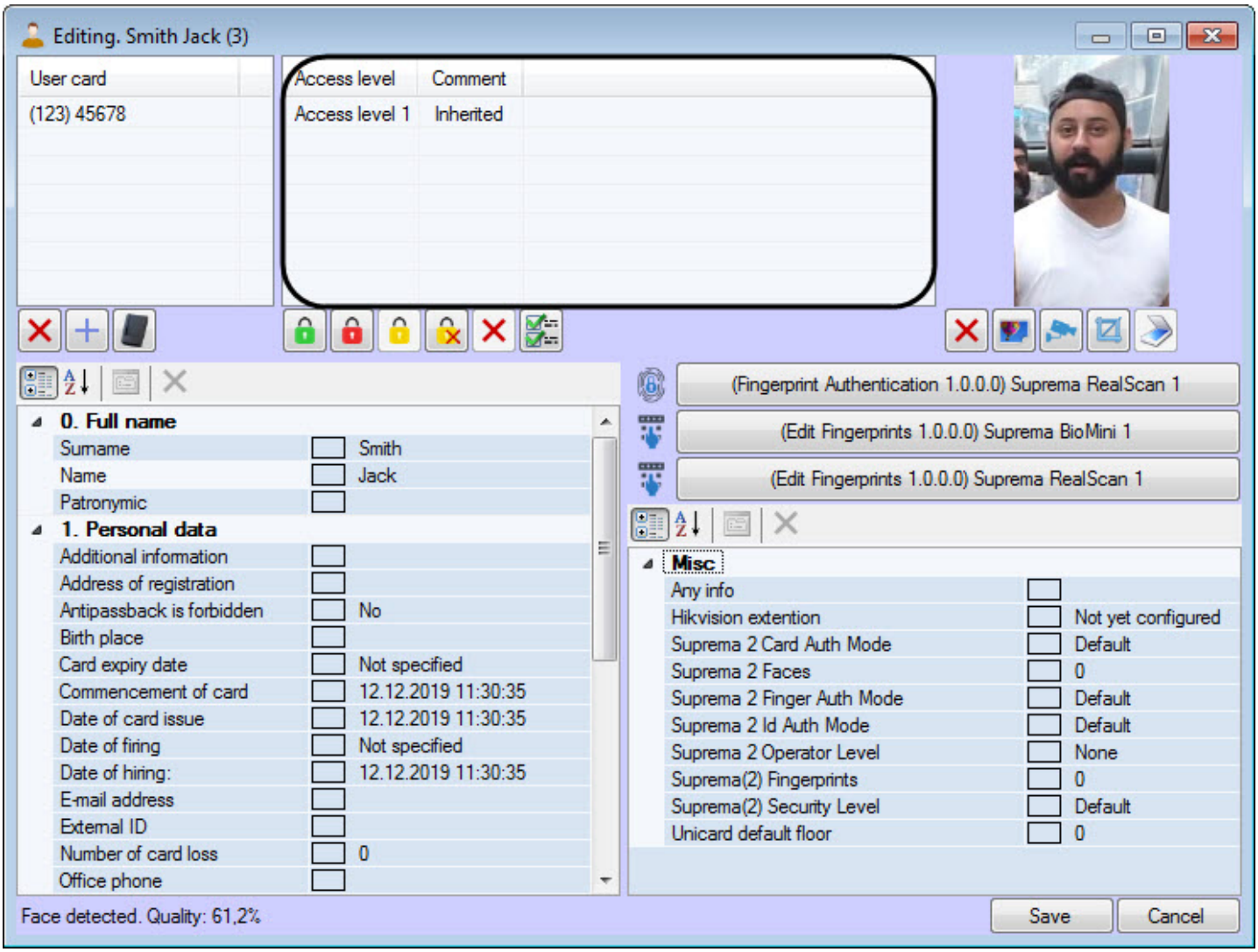


> **Note**
>
> You can also remove a card number from the list using the corresponding buttons (see Setting user parameters).

6.6.3.4 Assigning access levels to a user

6.6.3.4.1 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.



In the **Comment** column it's specified whether access level is inherited from Department (**Inherited**) or assigned to a user separately (**Own**). Configuring rules of department access level inheritance is described in the Configuring the 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.

Several access levels can be assigned to a single user.

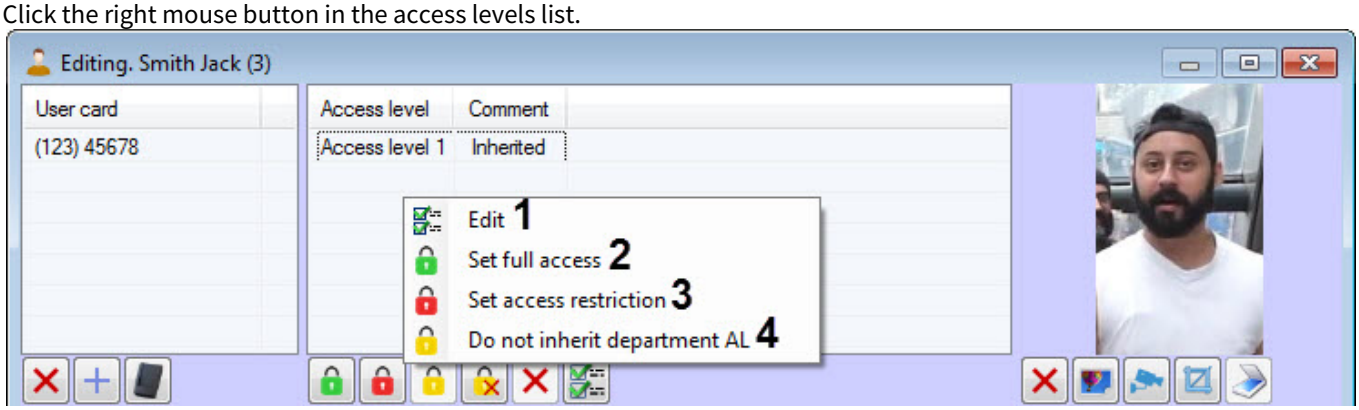
> **Attention!**
>
> The assignment of several access levels to a single user should be supported by hardware and by an appropriate integration module. If several access levels are assigned to a user, but the ACS equipment or the integration module supports only one access level, then all levels except the first one in the list will be ignored by the system.

The support for several user access levels has been tested in the following integration modules: ApolloSDK v.3, Elsys, ParsecNet, HID, Suprema, Salto, Perco S20 v.2, BioSmart2, Noder. For information on other integration modules, please contact the AxxonSoft technical support.

6.6.3.4.2 Assigning Own access level to a user

Assigning Own access level is performed as follows:

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. In the functional menu that opens:
   - To assign the **Own** access level to a user, select the **Edit** item (**1**). The **Search access level** window opens. In this window, select one or several access levels (see Working with the Search access level window).

     Attention!

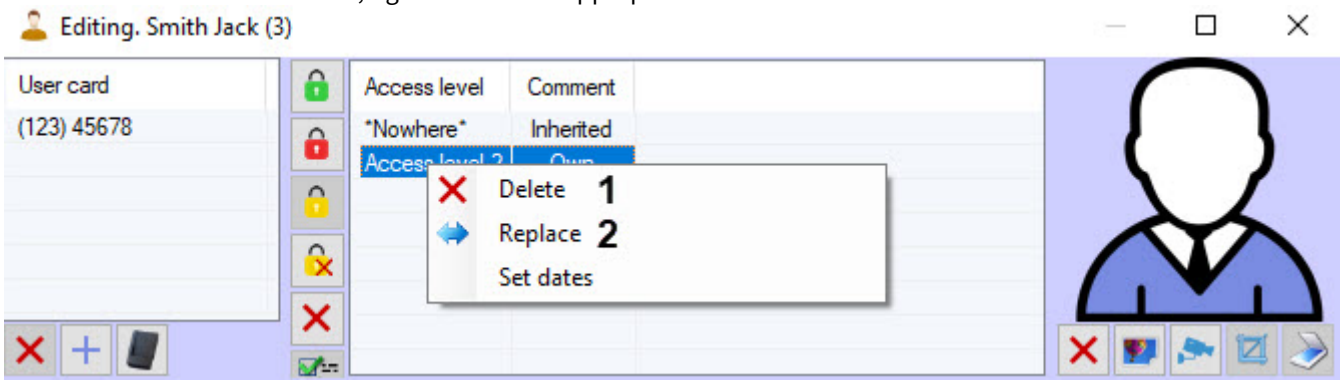
     If **Always** or **Never** Own access levels are inherited to a user, then the selected **Own** access levels will be ignored.

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

     Note.

     If **Always** or **Never** access level is assigned to a user, then all other access levels will be deleted.

   - If you disable the access level inheritance from a department by selecting the **Do not inherit department AL** item (**4**), the user will also be assigned the **Own** access level (for details, see Configuring the department access level inheritance)
4. To remove the **Own** access level, right-click on the appropriate access level and select **Delete**.



Note

If the user has only one **Own** access level, then when it is deleted, the access level inheritance from a department will be enabled.

5. To replace one access level (**Own**) with another, right-click on the corresponding access level and select **Replace** (**2**). The **Search access level** window opens. In this window, select one or several access levels (see Working with the Search access level window).

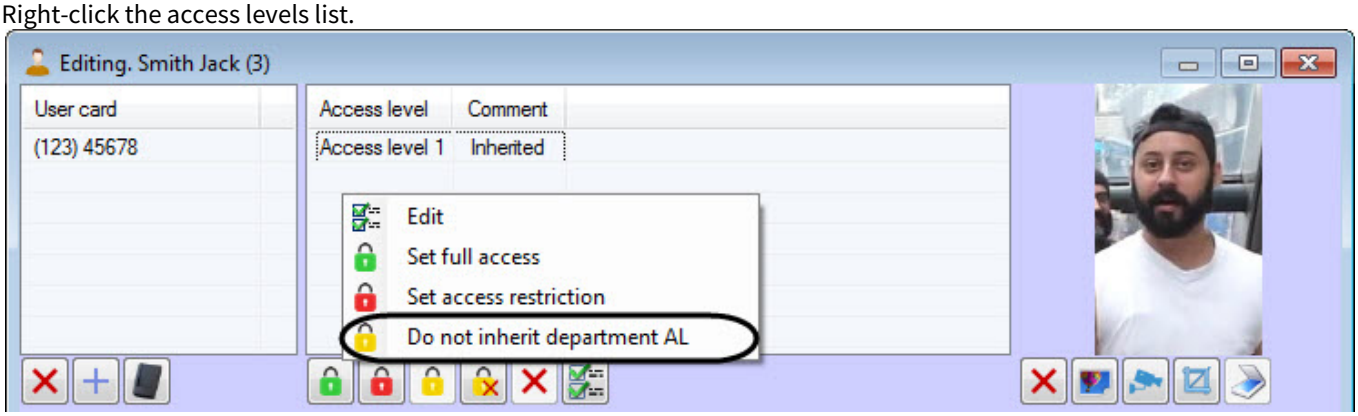
Assigning **Own** access level to a user is completed.

> **Note**
>
> You can perform all the actions described above using the corresponding buttons (see Setting user parameters).

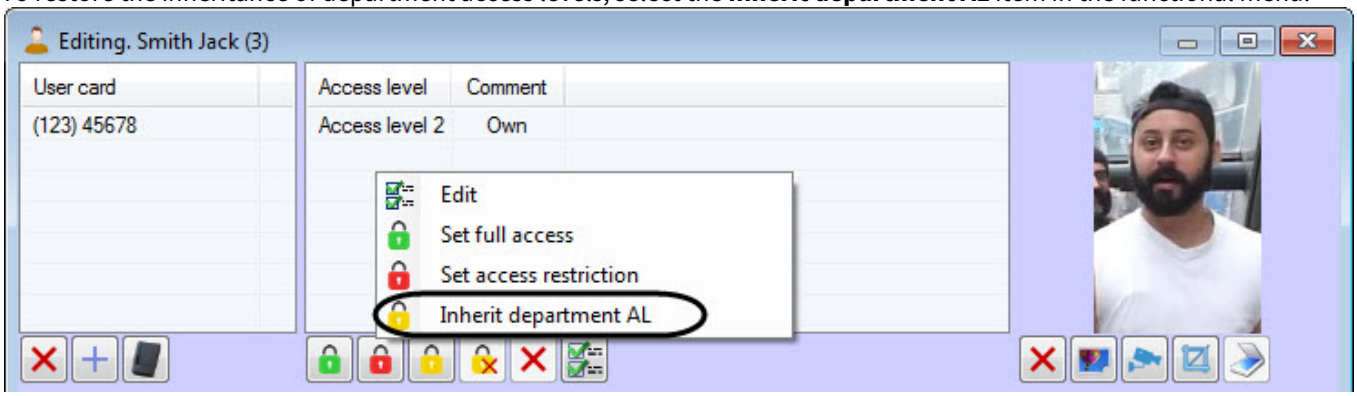
6.6.3.4.3 Configuring the department access level inheritance

By default, the user inherits the department access level. If it's required not to inherit the department access level, do the following:

1. Go to editing a user (see the Going to user editing section).
2. Right-click the access levels list.



3. Select the **Do not inherit department AL** item in the opened functional menu. If the user does not have any other access levels assigned except the inherited, the **Search access level** window will be opened. In that window, select one or several access levels (see Working with the Search access level window). As a result, the inherited access level will be removed from the list.
4. To restore the inheritance of department access levels, select the **Inherit department AL** item in the functional menu.



Configuring of department access level inheritance is completed.

> **Note**
>
> You can perform all the actions described above using the corresponding buttons (see Setting user parameters).

6.6.3.4.4 Assigning temporary access level to a user

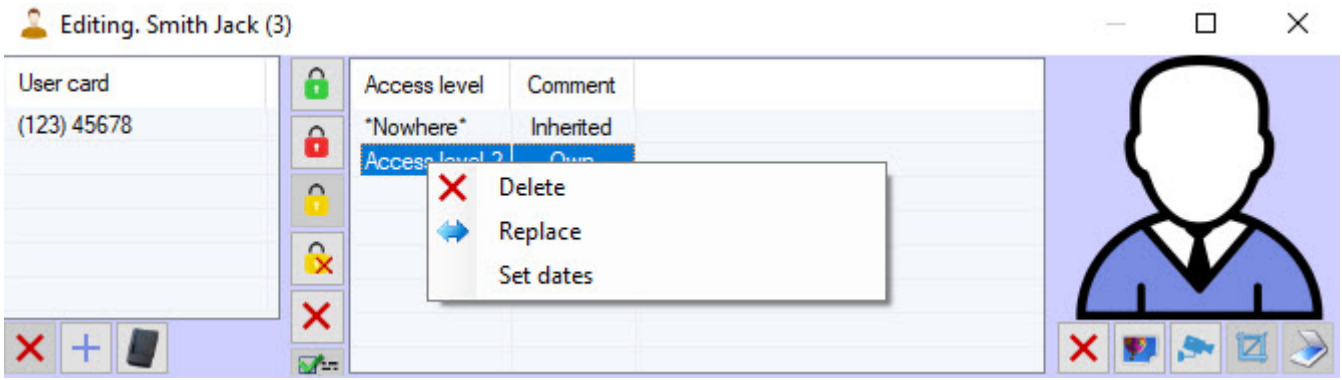
> **Attention!**

A user can be assigned a temporary access level only if the **Temporary Access Levels** object (service module) is created in the hardware tree.

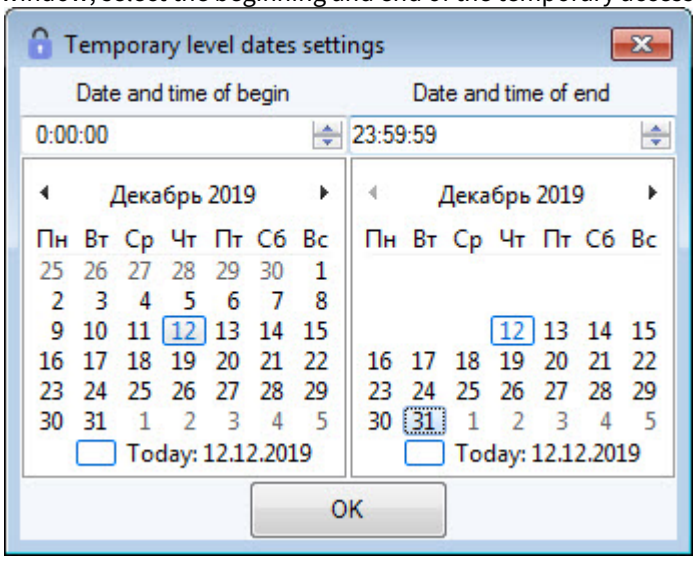
To assign temporary access level to a user, do the following:

1. Go to editing a user (see the Going to user editing section).
2. Right-click the required access level (**Own**) which should be made temporary (see Assigning Own access level to a user).

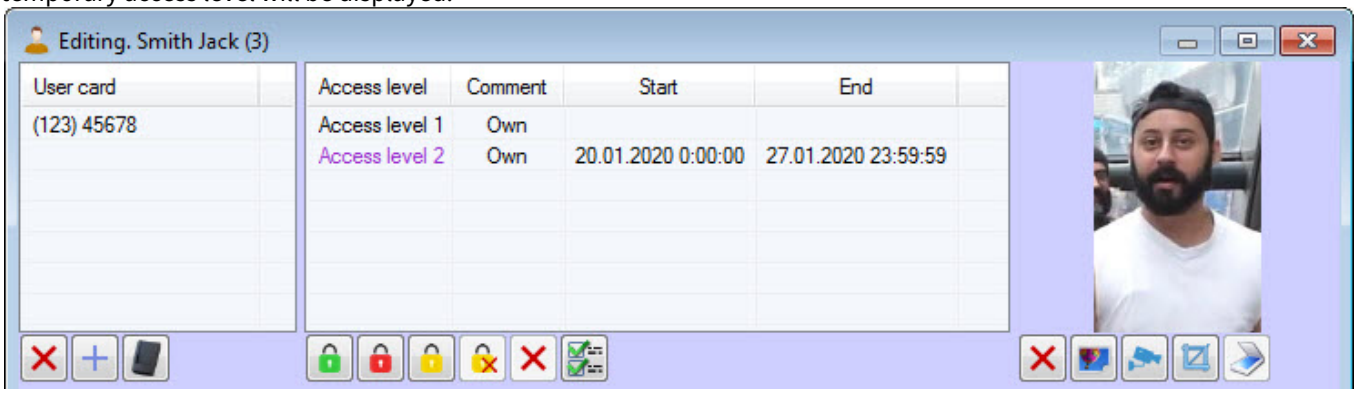
> **Note**
>
> You can also select several access levels (**Own**): for example, by selecting them with the mouse or by using keyboard shortcuts (see Keyboard shortcuts for working with interface elements).



3. In the opened functional menu, select the **Set dates** item. The **Temporary level dates settings** window opens. In that window, select the beginning and end of the temporary access level and click **OK**.



4. As a result, this access level will become temporary. In the **Start** and **End** columns next to it the date and time of the temporary access level will be displayed.



If the date and time of validity of the temporary access level has already expired or has not yet started, then the date and time of validity of the temporary access level will be crossed out.

Access level	Comment	Start	End
Access level 1	Own		
Access level 2	Own	19-Apr-20 12:00:00 AM	25-Apr-20 11:59:59 PM
Access level 3	Own	~~26-Apr-20 12:00:00 AM~~	~~02-May-20 11:59:59 PM~~

Note

You can delete temporary access levels in the same way as **Own** access levels (see Assigning Own access level to a user).

Assigning temporary access level to a user is completed.

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

6.6.3.5.1 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.

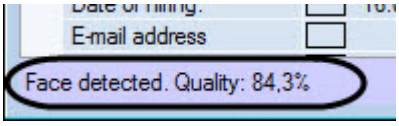
Note

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).

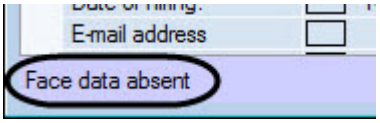
Assigned photographs are stored in the *<ACFA-Intellect installation directory>*/Bmp/Person folder. Name of file with the user's photograph is the same as the user ID. Content of the Bmp/Person folder is synchronized on all servers of distributed system.

It is possible to check the quality of an image before saving the assigned photo. To do this, it is necessary to configure the interaction with the *FACE Intellect* Face recognition server (see Configuring the interaction with the FACE Intellect Face recognition server.

As a result, after a user's photo is added, a message about face detection and its quality will be displayed in the lower left corner of the user parameters editing window, if this face meets the requirements specified on the **Face recognition server** object settings panel.



If the face does not meet the requirements specified on the **Face recognition server** object settings panel, the **Face data absent** message will be displayed. In this case, it is recommended to repeat the process of adding a user's photo by selecting another photo or selecting a new image from the camera.



It is also possible to automatically synchronize the users of the *Access Manager* module with the *FACE Intellect* reference face database (see Appendix 6. Face synchronization module).

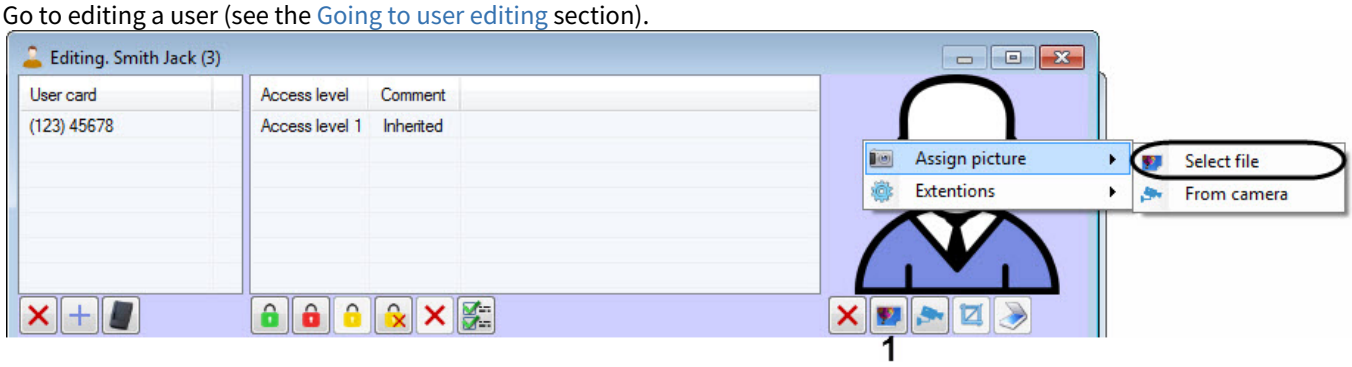
Note

If the quality of the face photo does not meet the requirements specified on the **Face recognition server** object settings panel, then this user will not be synchronized.

6.6.3.5.2 Assigning a 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  button (**1**). As a result, the standard Windows dialog window will be opened. In this window, select a file with a photo, which will be assigned to the user.

> **Note**
>
> You can also assign a photo to the user by right-clicking on the user's photo area and selecting **Assign picture -> Select file** in the opened functional menu.

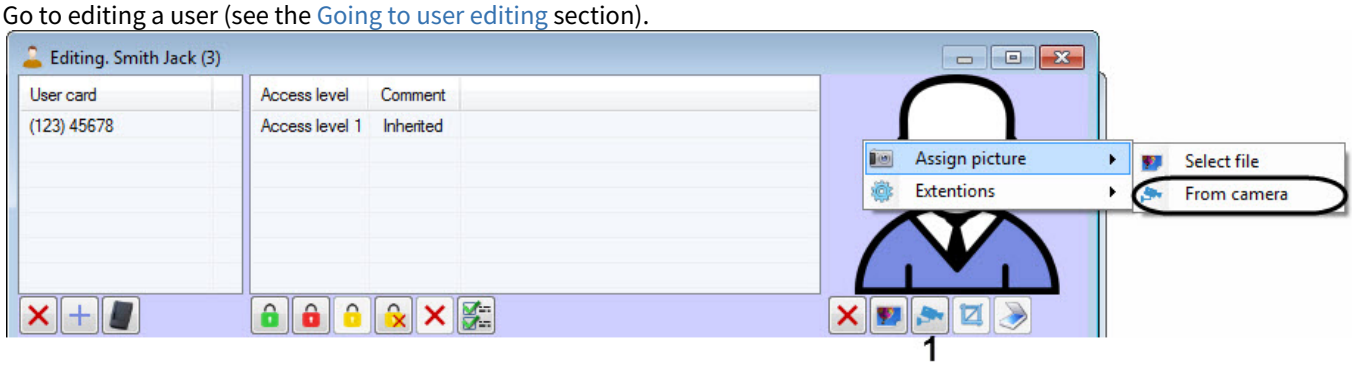
Assigning photograph from a file is completed.

6.6.3.5.3 Assigning a photograph from a video camera

To assign a 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).

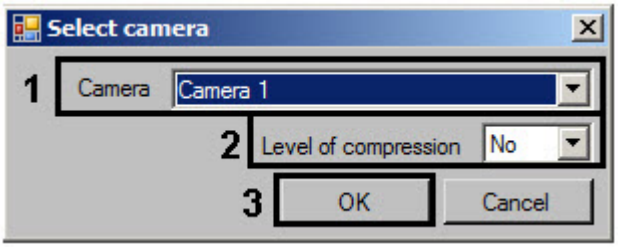
1. Go to editing a user (see the Going to user editing section).



2. Click the  button (**1**). As a result, the **Select camera** window will open.

> **Note**
>
> You can also open the **Select camera** window by right-clicking on the user's photo area and selecting **Assign picture -> From camera** in the opened functional menu.

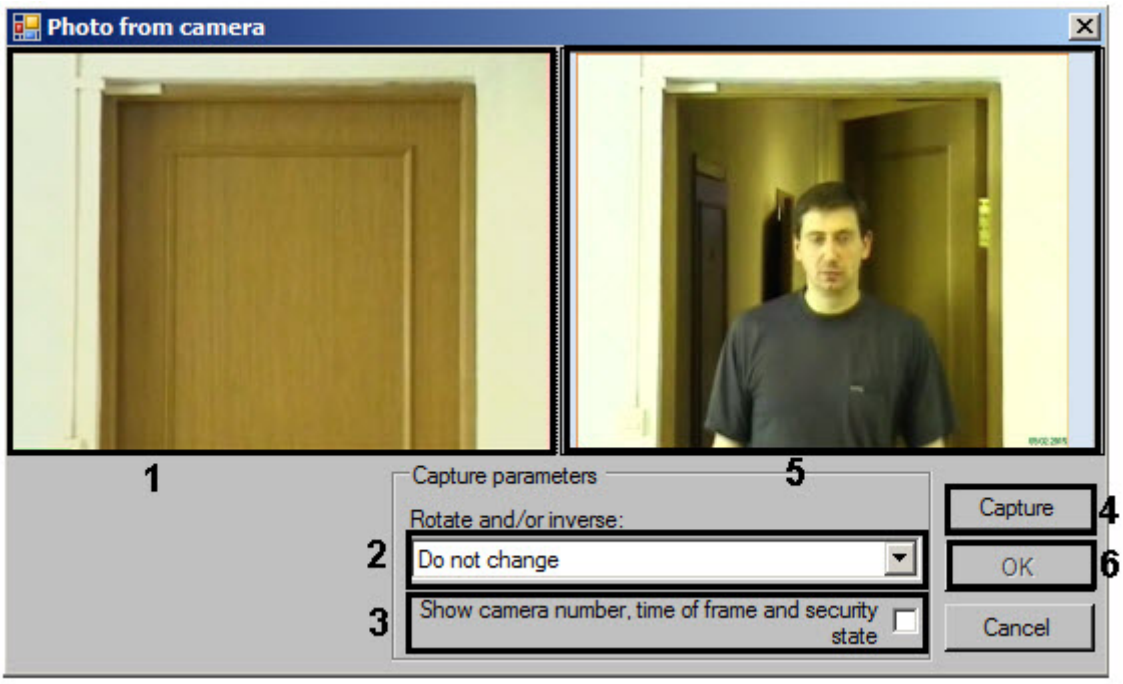
3. From the **Camera** drop-down list select the camera from which photograph will be captured (**1**).



4. 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.

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



6. Video from the selected video camera is displayed in the window (**1**).
7. 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.
8. 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.

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

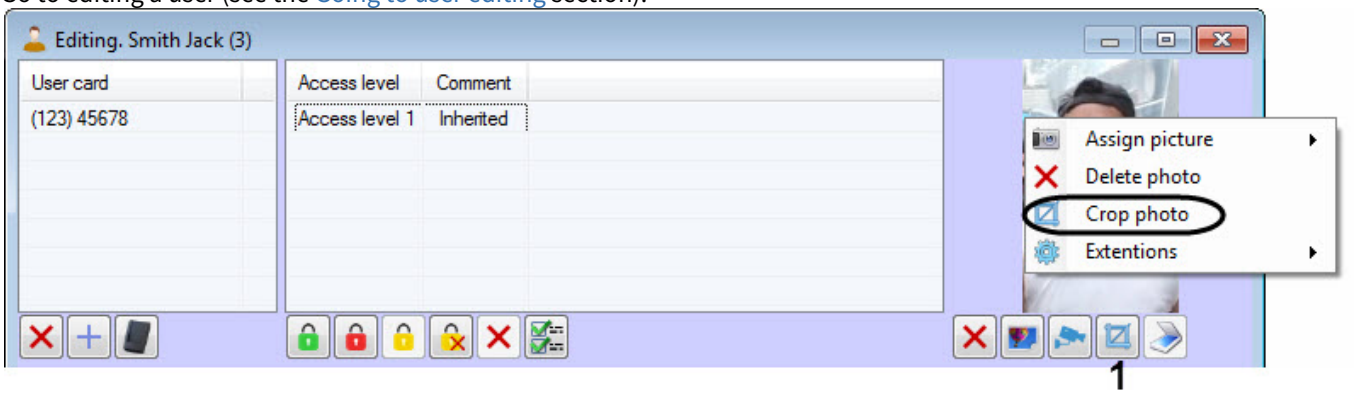
Assigning a photograph to user from a video camera is completed.

6.6.3.5.4 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  button (**1**). As a result, the **Framing** window will open

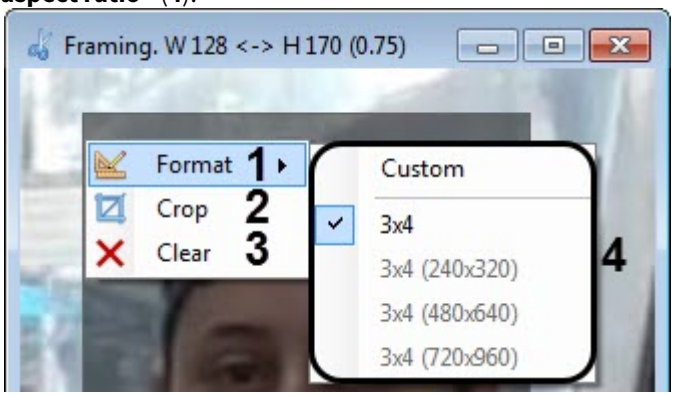
> **Note**
>
> You can also open the **Framing** window by right-clicking on the user's photo area and selecting **Crop photo** from the opened functional menu.

3. Select the area which should remain in the photo. To do this, left-click the required point and stretch the rectangle marking the selected area. The selected area can be moved by holding down the left mouse button on the rectangle.

Note

In the upper part of the **Framing** window displays the width "W" and height "H" in pixels, and the aspect ratio of the selected area in parentheses.

4. To select the preset size of the resulting photo or the aspect ratio of the rectangle, right-click, either on the selected area, or in the area not marked by the rectangle, and in the opened function menu select **Format** (**1**) → **<required size or aspect ratio>** (**4**).



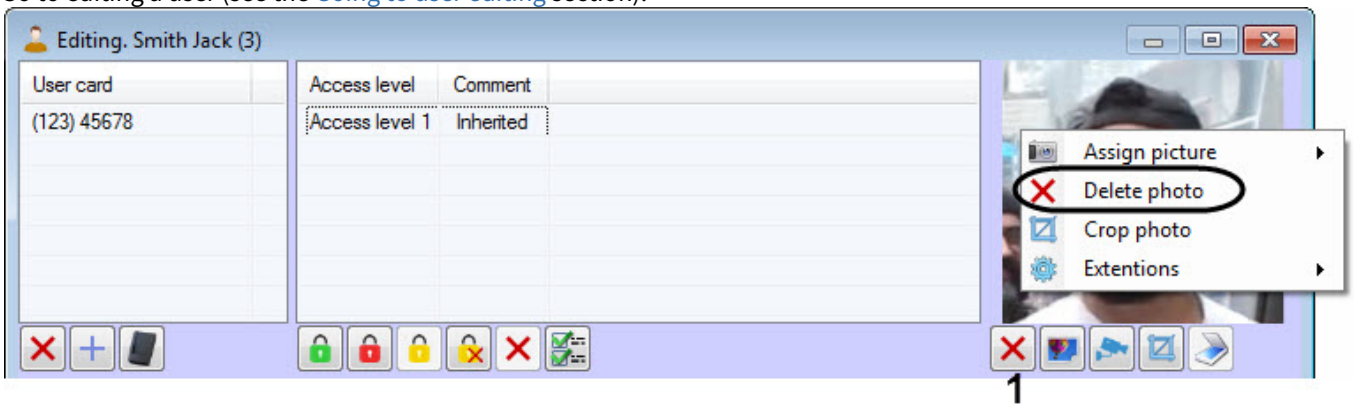
5. To delete the selected area, left-click on the area not marked by the rectangle and make the selection again. Or right-click on the selected area and select **Clear** (**3**) in the opened function menu.
6. To confirm cropping of the photo, right-click on the selected area and select **Crop** (**2**) in the opened functional menu.

Cropping a photograph is completed.

6.6.3.5.5 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  button (**1**).

> **Note**
>
> You can also delete a photo of the user by right-clicking on the user's photo area and selecting **Delete photo** in the opened functional menu.

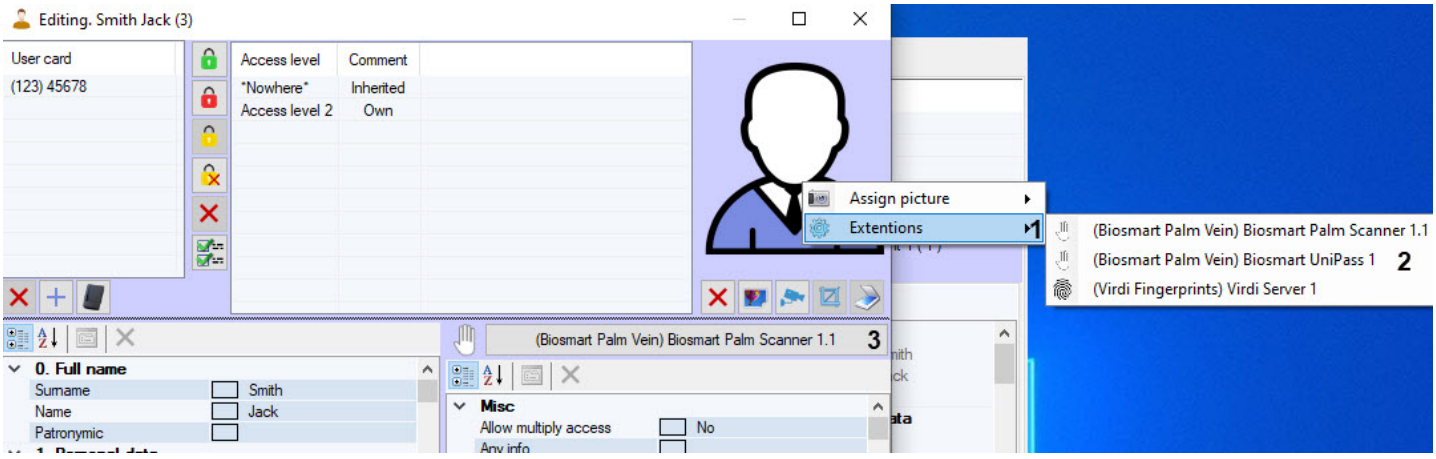
Deleting a photograph is completed.

6.6.3.6 Adding biometric parameters

Adding biometric parameters (faces, fingerprints, etc.) is performed using control readers or biometric ACS terminals.

To add a user's biometric parameters, do the following:

1. Right-click on the user's photo and hover over the **Extensions** item (**1**).
2. Select a biometric reader from the list (**2**).
3. If an extension button is added, then instead of the first 2 steps, you can click this button (**3**).



As a result, a dialog box for adding user biometric parameters opens. This dialog box differs depending on the equipment used. Operation in this dialog box is described in the documentation for the corresponding ACS integration module (see ACS integration modules), as well as in the documentation for the corresponding control reader integration module (see Control Readers Settings Guide).

> **Note.**
>
> In order for a reader or controller to be available for selection in the **Extensions** list, it is necessary to select it when configuring the *Access Manager* module – see Configuring control readers in the Access Manager.

By default, extension buttons are hidden. To add (or remove) extension buttons:

1. Right-click on the user's photo and hover over the **Extensions** item (**1**).
2. Holding down the Shift key, click on the extension from the list (**2**).

As a result, the button with the selected biometric reader (**3**) will be added to the area under the user's photo.

To remove the extension button, follow the same steps.

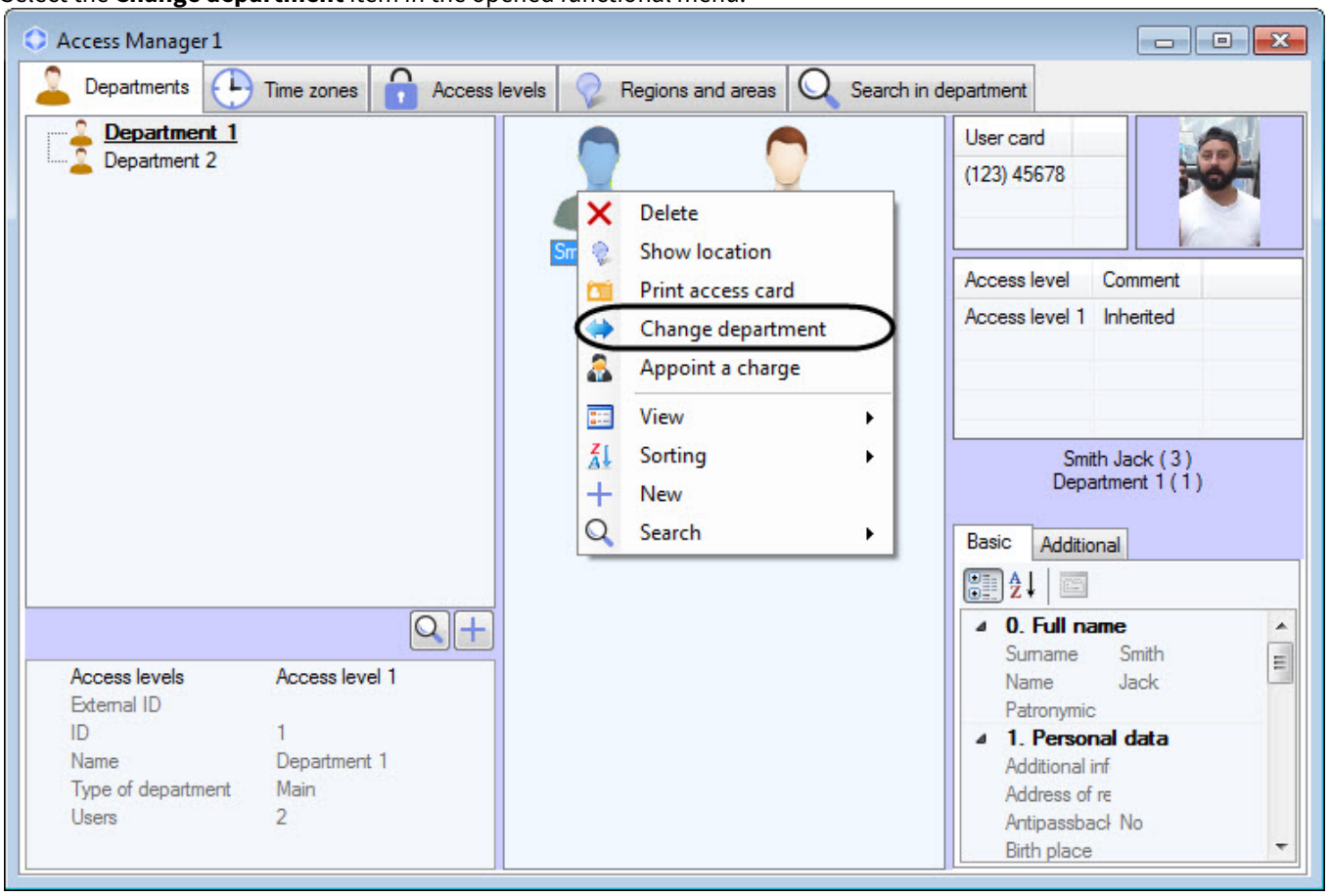
6.6.3.7 Transferring a user to a different department in the Access Manager software module

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**
>
> You can also select several users: for example, by selecting them with the mouse or by using keyboard shortcuts (see Keyboard shortcuts for working with object lists).

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.

6.6.3.8 Changing a user type

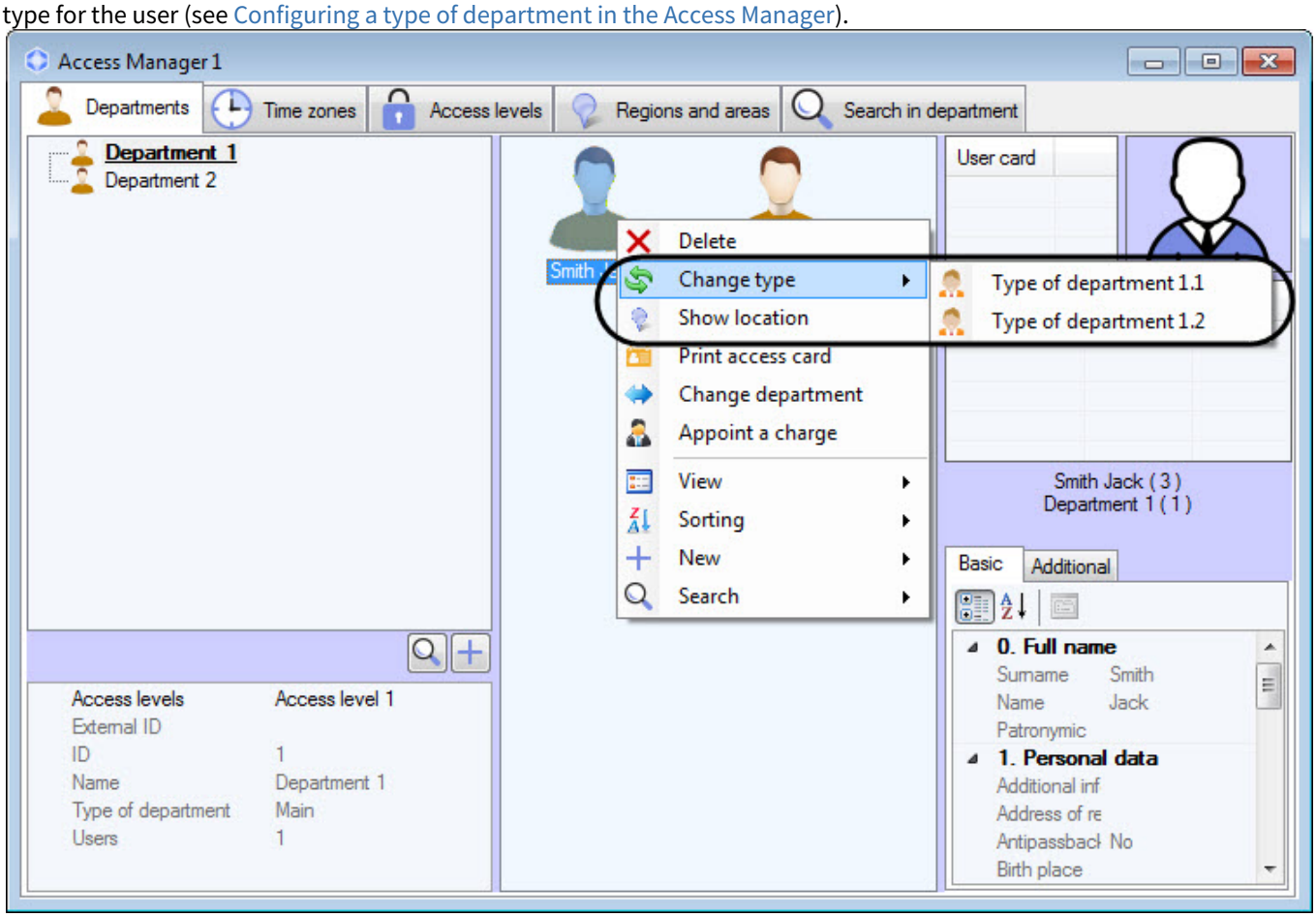
> **Attention!**
>
> You can change the user type only if it is allowed (see Configuring the permission to change user type).

Change user type as follows:

1. Go to viewing the list of users (see Viewing a list of users).
2. Right-click on the name of the required user.

> **Note**
>
> You can also select several users: for example, by selecting them with the mouse or by using keyboard shortcuts (see Keyboard shortcuts for working with object lists).

3. In the function menu that opens, select the **Change type** item and in the drop-down list select the required department type for the user (see Configuring a type of department in the Access Manager).



4. As a result, the user type will be changed.

Changing a user type is now completed.

6.6.4 User search in the Access Manager software module

6.6.4.1 General information about user search

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

1. By surname.
2. By number.

3. By card.
4. By card (control reader).
5. By access level.
6. General search.

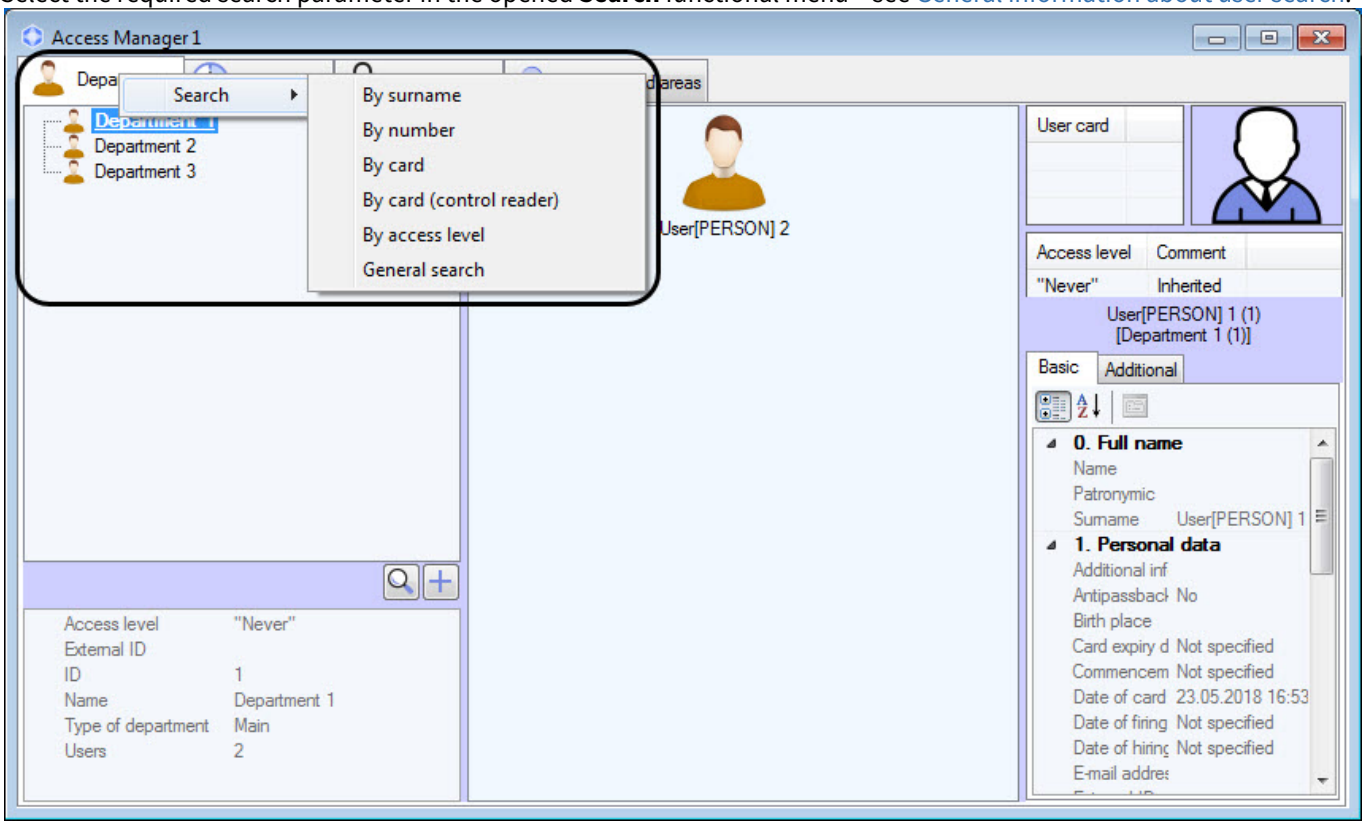
6.6.4.2 Going to user search

Go to the user search using one of the following ways.

> **Note**
>
> In addition to the method described below, you can also use the **Search** button on the user control panel (see Viewing a list of users).

The first way:

1. Right-click the **Departments** tab.
2. Select the required search parameter in the opened **Search** functional menu – see General information about user search.

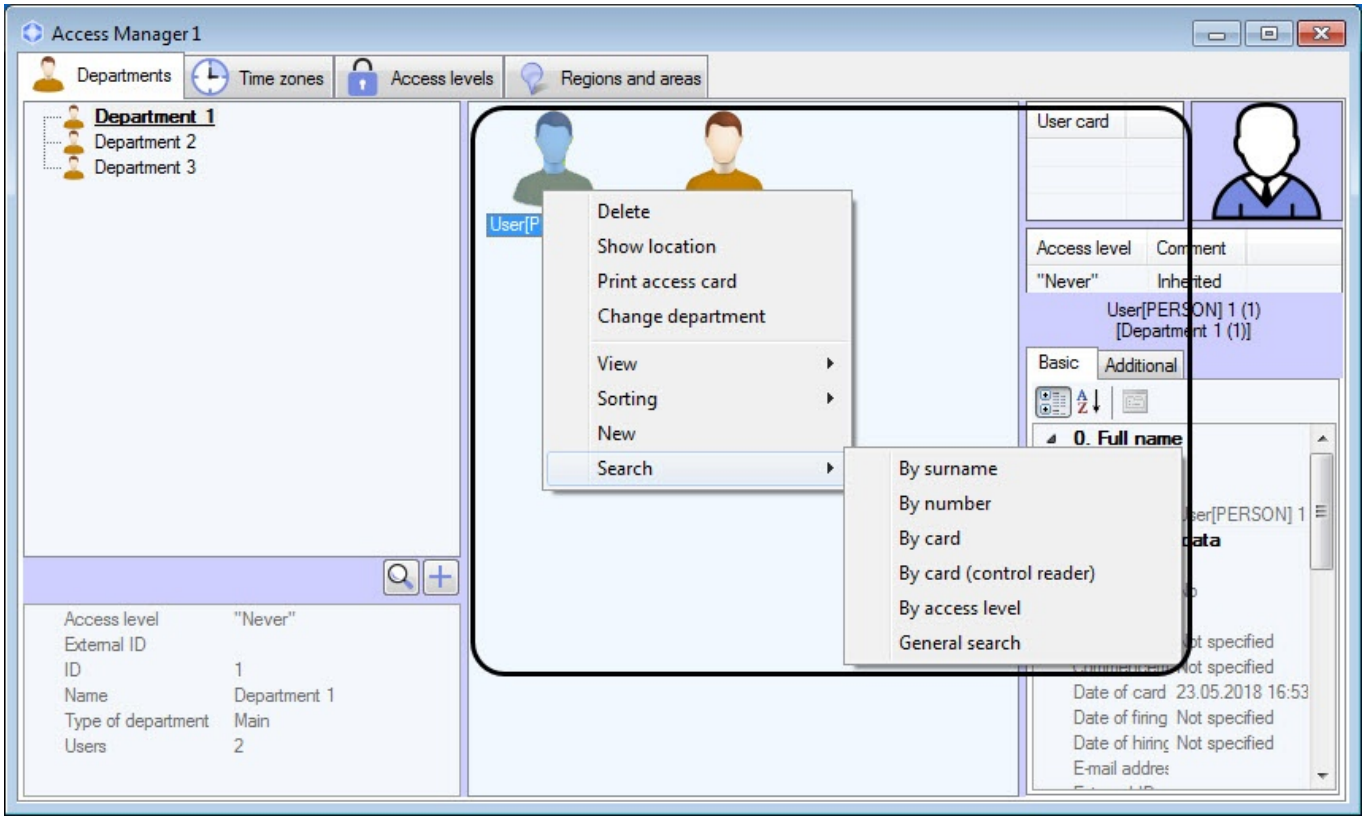


The second way:

1. Go to viewing users list (see Viewing a list of users).
2. Right-click the free area in the users list or right-click the user.

> **Note**
>
> Also going to user search is performed by Ctrl+F keys combination - see Keyboard shortcuts for working with interface elements. 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.

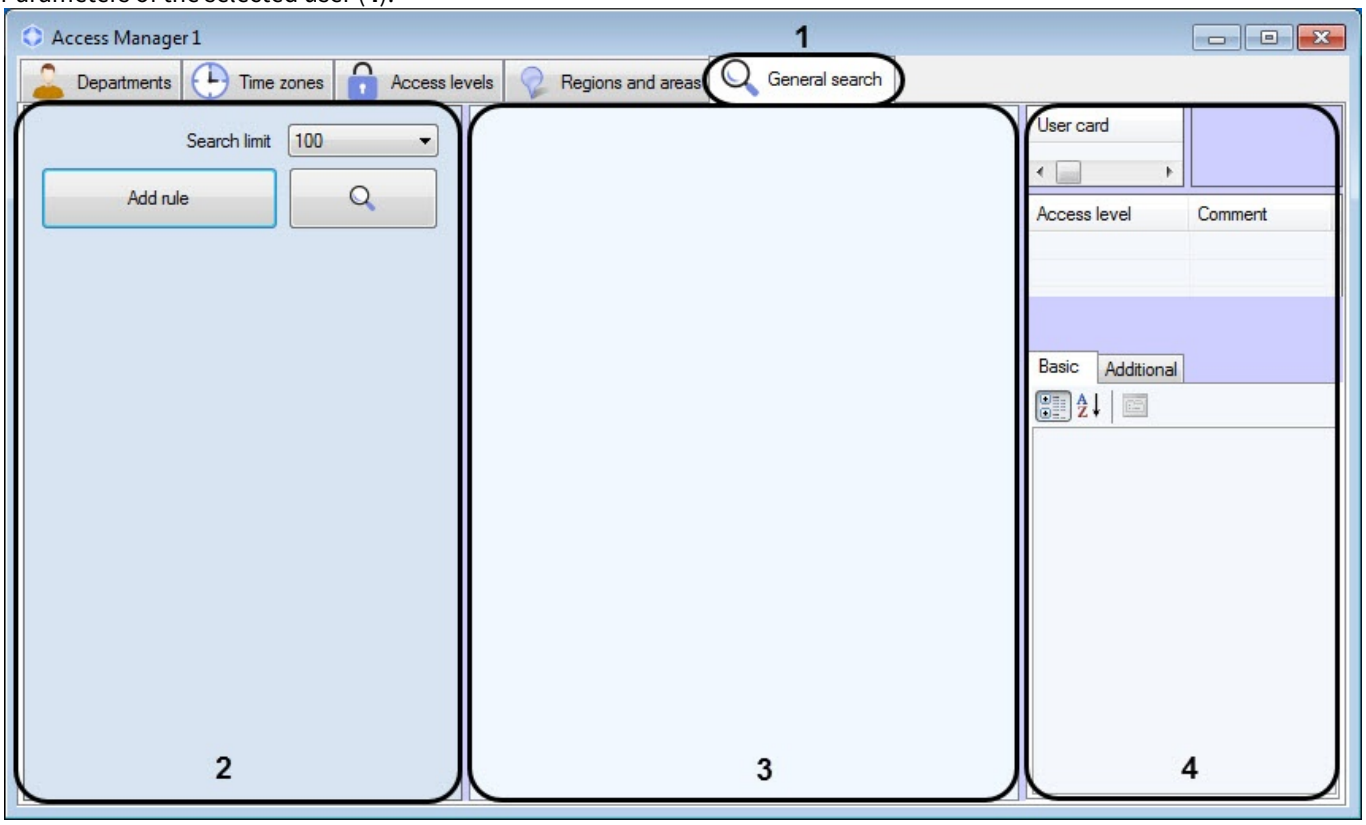
3. Select the **Search** item in the opened functional menu**.** In the opened functional menu select the required way of search - see General information about user search.



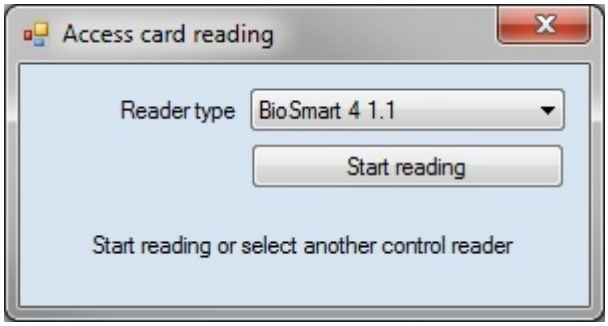
As a result, the new tab will be opened for search (**1**). The name of the tab depends on the selected way of search. The tab contains the following interface elements:

1. List of search rules (**2**).
2. List of found users (**3**).

3. Parameters of the selected user (**4**).



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).
5. 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.

6.6.4.3 Adding a search rule

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

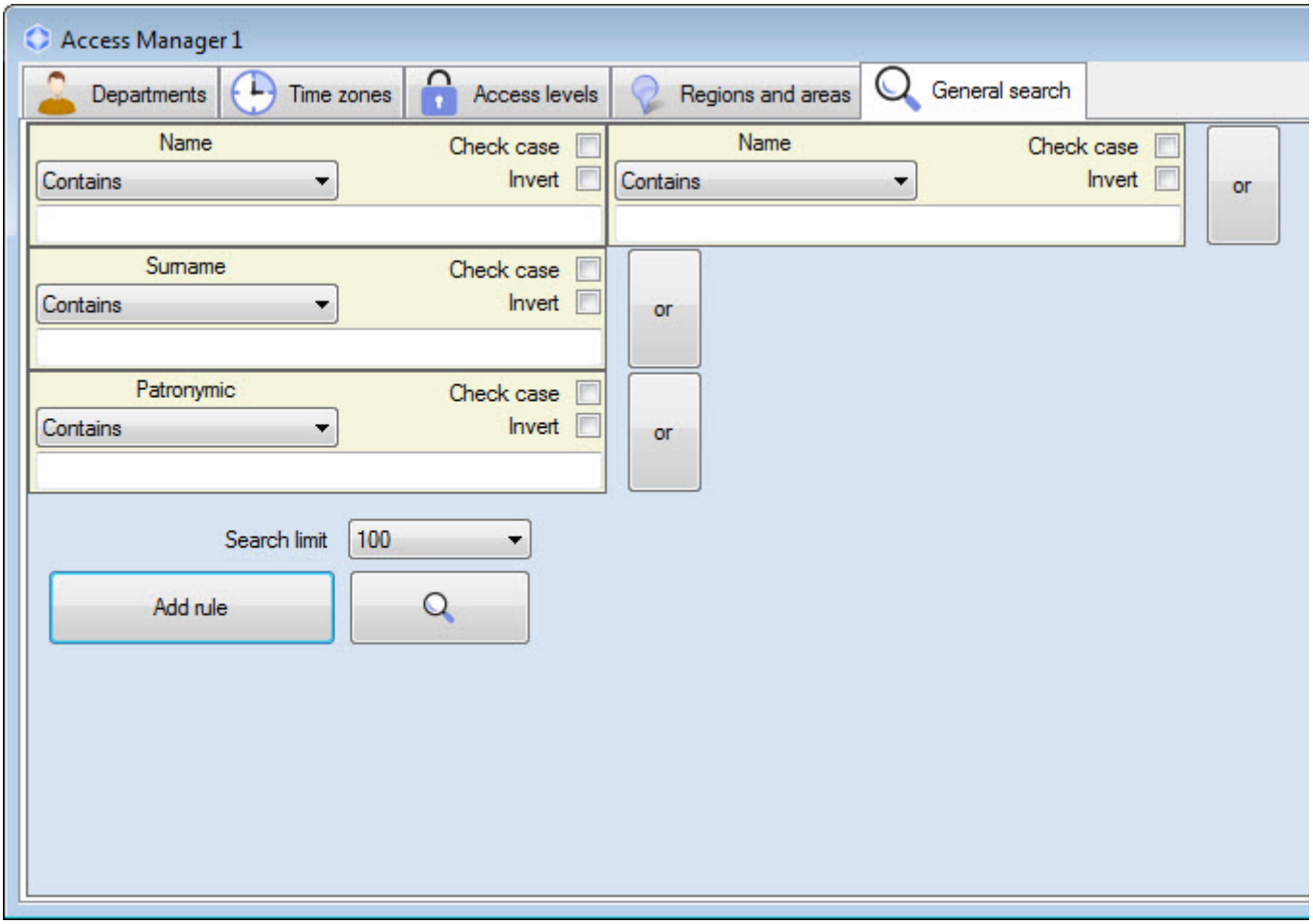
1. Logic AND.
2. Logic OR.

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)
```

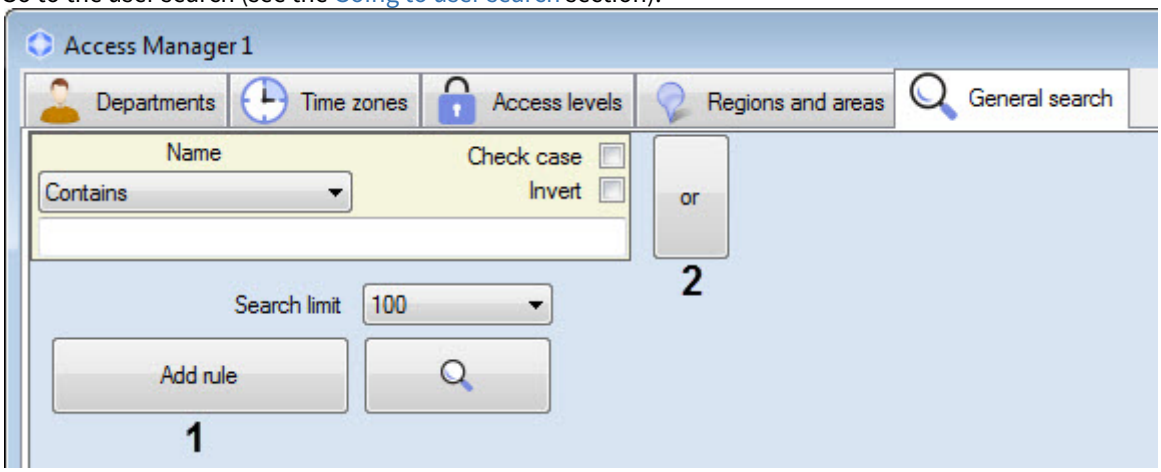
Where N, M, K, L –some integer number.

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

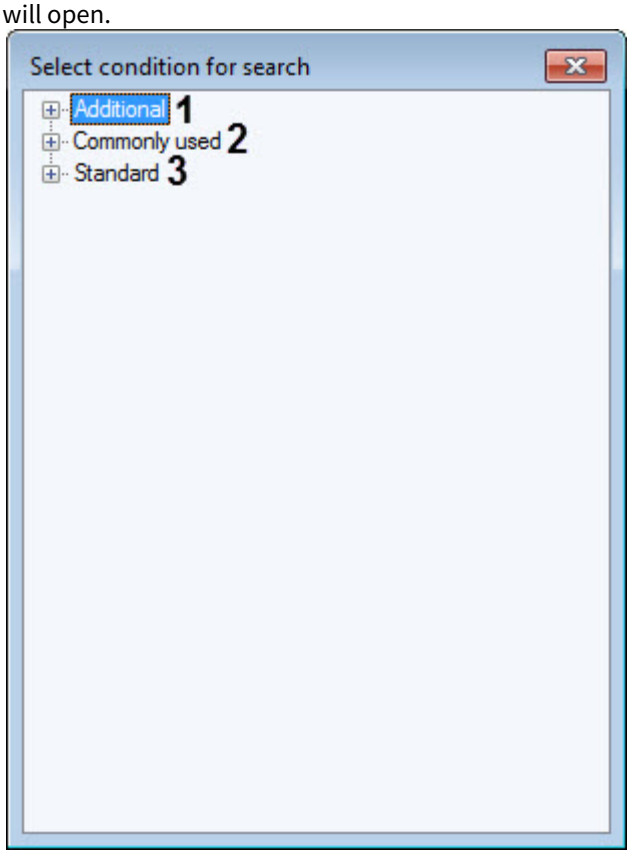


To add the search rule, do the following:

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



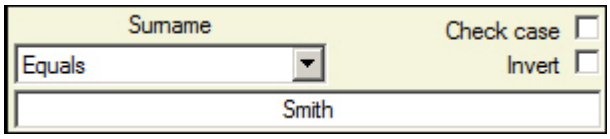
2. Click the **Add rule** button (1) to add AND rule or the **or** button (2) to add OR rule. The **Select condition for search** window will open.



   a. The **Additional** group (1) contains the criteria for filtering by additional user parameters.
   b. The **Commonly used** group (2) group contains the frequently used criteria for filtering by user parameters, and the **Time in the region** criterion, which is used for searching the users by the time they were present or absent in the selected region.
   c. The **Standard** group (3) contains the criteria for filtering by the standard user parameters.

> **Note**
>
> For the details on the user parameters description, see Setting user parameters.

3. Double click on the name of parameter by which search is to be performed.
4. 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

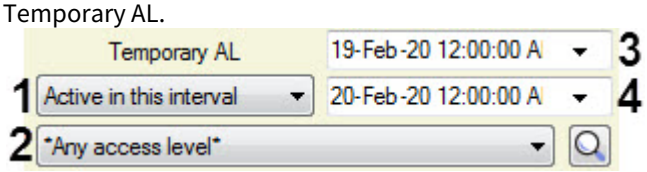
Ends with	Search for all users for which a value of the selected field ends with the specified search line

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.

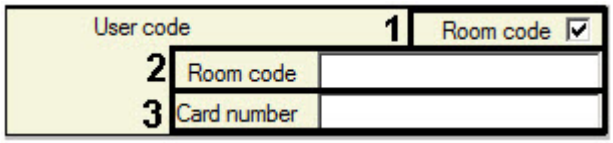
i. Set the **Invert** checkbox if it's required to apply the negation of the specified search rule (1).
ii. Select value for search from the drop-down list (2). To search the required access levels it's possible to click the  button. Working with windows of objects search is described in corresponding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

c. Temporary AL.



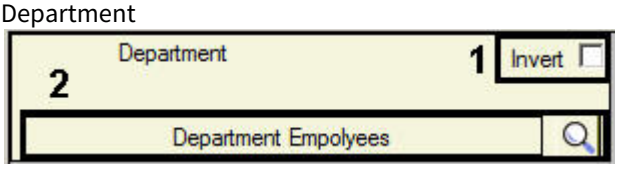
i. Select the search criteria from the drop-down list (**1**):
    1. **Activation date** - the start date of the temporary access level.
    2. **Active on this day** - the date between the start and end of the temporary access level.
    3. **Active in this interval** - the selected interval between the start and end of the temporary access level. If the interval includes a day when the temporary access level is not valid, then the search will have no results.
ii. Select the search criteria from the drop-down list (**2**). You can also click on the  button to search for the required temporary access level. Working with object search windows is described in the corresponding sections of this document.
iii. Use the calendar to set the search date (**3**).
iv. If **Active in this interval** is selected, set the end of the interval for the search (**4**).

d. User card



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).

e. Department

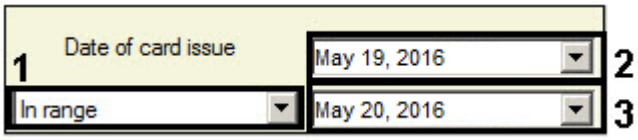


i. Set the **Invert** checkbox if it's required to apply the negation of the specified search rule (1).
ii. To search for required department click the  button (2). Working with windows of objects search is described in corresponding sections of this document.

> **Note.**

> Search for department is performed only if going to user search was performed by means of Ctrl+F keys.

f. Time values



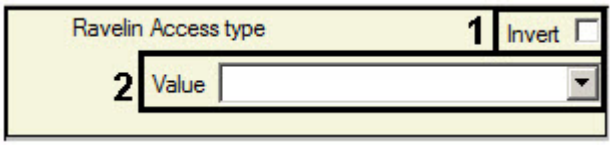
i. Select the comparison method of the specified value for search with a field value:

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.

g. Additional fields



i. Set the **Invert** checkbox if it's required to apply the negation of the specified search rule (1).

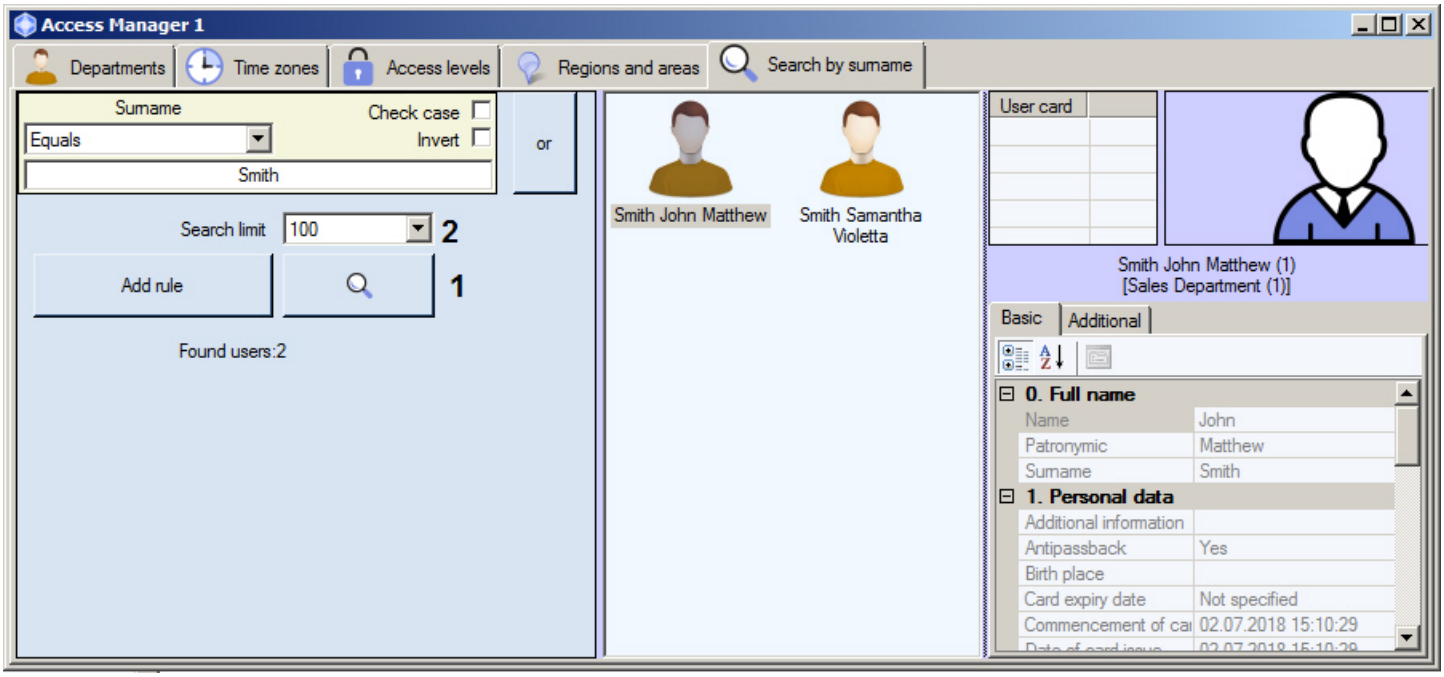
ii. Select the search value from the Value drop-down list (2).

Adding a search rule is completed.

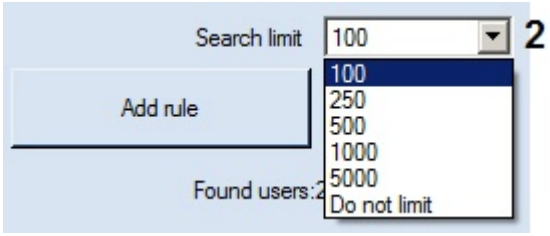
6.6.4.4 Start of user search

When all required search rules are specified (see the Adding a search rule section), click the  button to start search (**1**).

Found users will be displayed in the list.

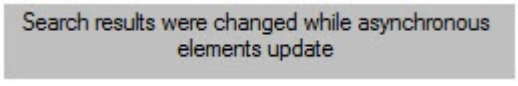


Number of users in the search result list can be limited. To change the limit, select the required number of users displayed from the **Search limit** drop-down list (**2**).



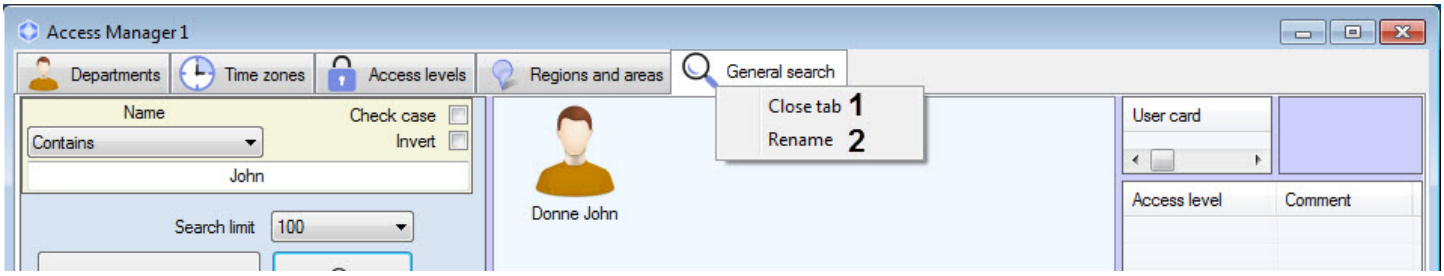
The list of found users can be changed dynamically.

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 displayed in the right part of the **Access Manager** window.

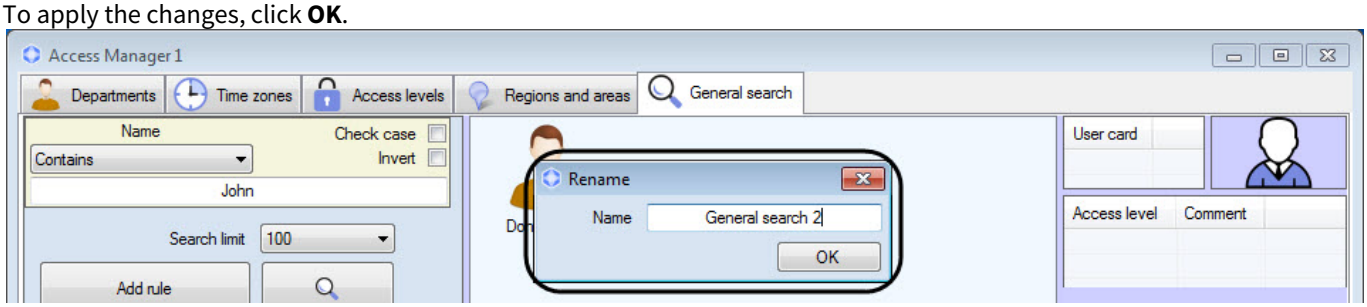
To close a tab after search completion click the right mouse button on the tab name and select the **Close tab** (**1**) item in the opened functional menu.



The search tab name can be changed. To rename it, do the following:

1. Right-click the tab name and select **Rename** (**2**) from the menu.

2. In the opened dialog box, in the **Name** field, enter the new name for the search tab.
3. To apply the changes, click **OK**.



Note.

The search tab with all conditions set is saved at *Access Manager* restart for the logged in *Intellect* user.

6.6.5 Deleting a user in the Access Manager software module

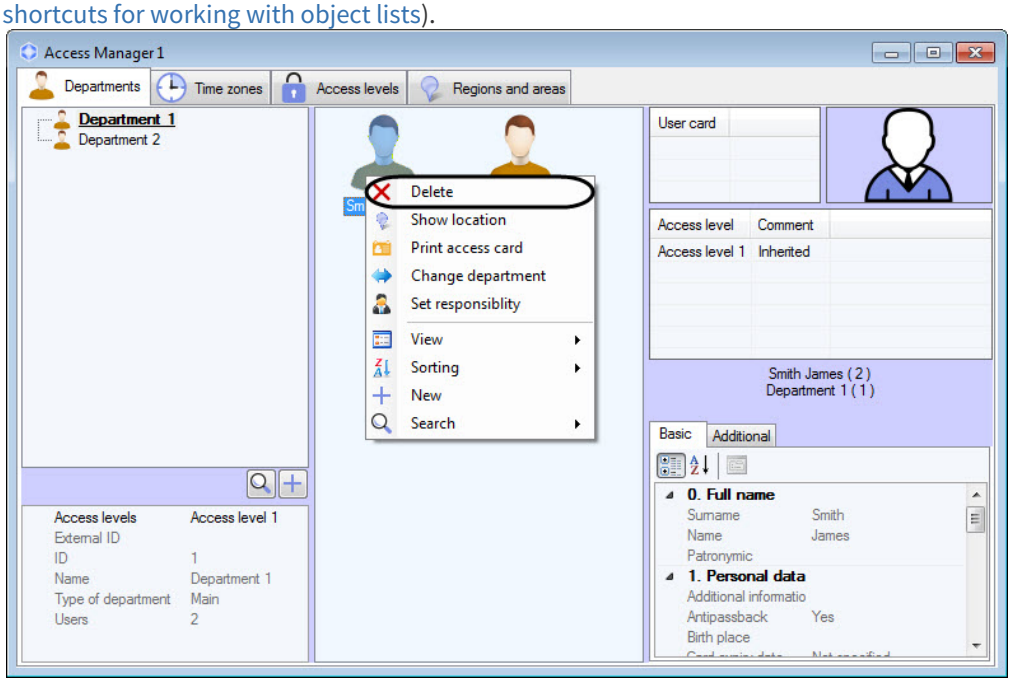
Deleting a user is performed as follows:

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

You can also select several users: for example, by selecting them with the mouse or by using keyboard shortcuts (see Keyboard shortcuts for working with object lists).

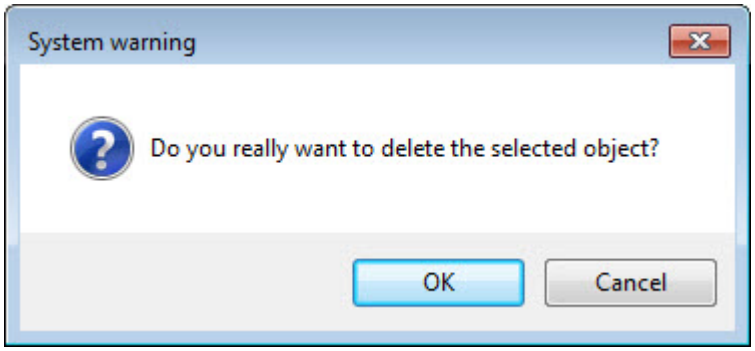
3. In the opened functional menu, select **Delete** or use the keyboard shortcut Ctrl+Del and Ctrl+Backspace (see Keyboard shortcuts for working with object lists).



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 Configuring the object management rights 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.

6.6.6 Printing a user access card in the Access Manager software module

> **Attention!**
>
> To ensure the correct printing of the user access cards, set the Windows screen scale to the default value (see Change the size of text in Windows 10).

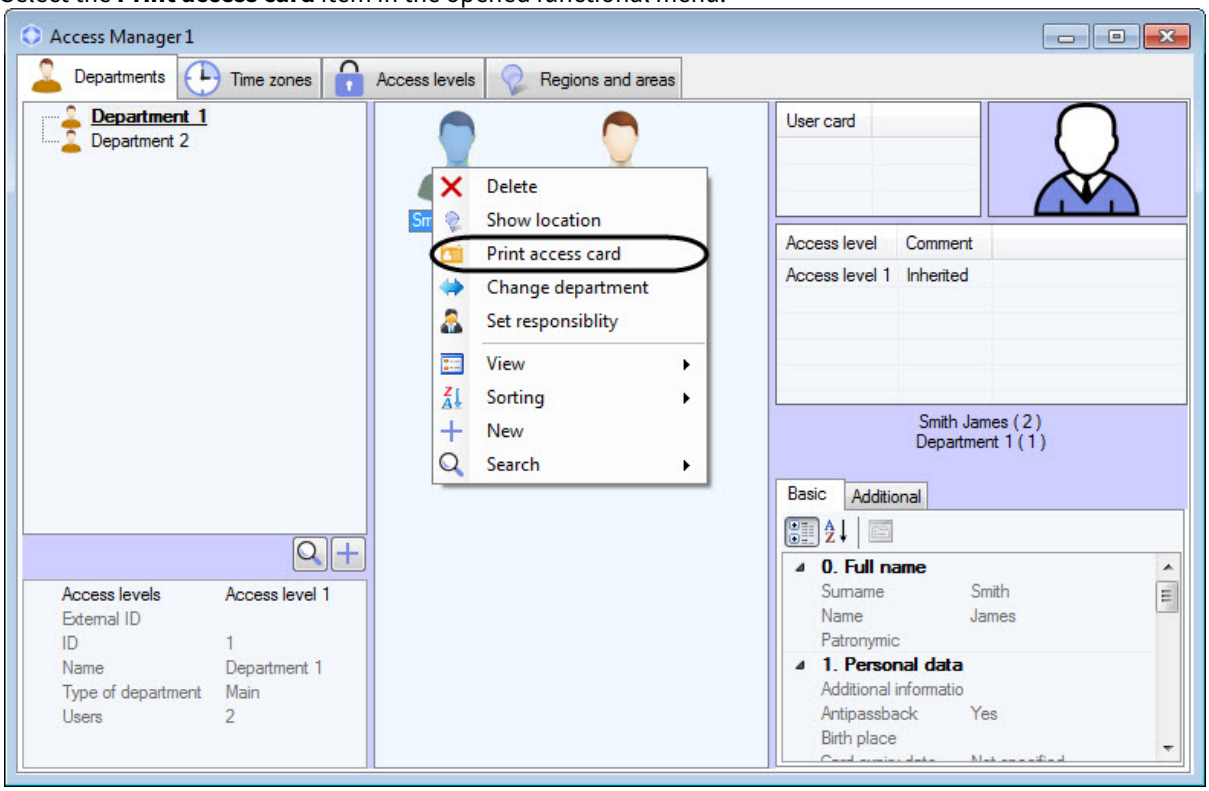
You can print user access cards in the *Access Manager* software module.

To print a user access card, do the following:

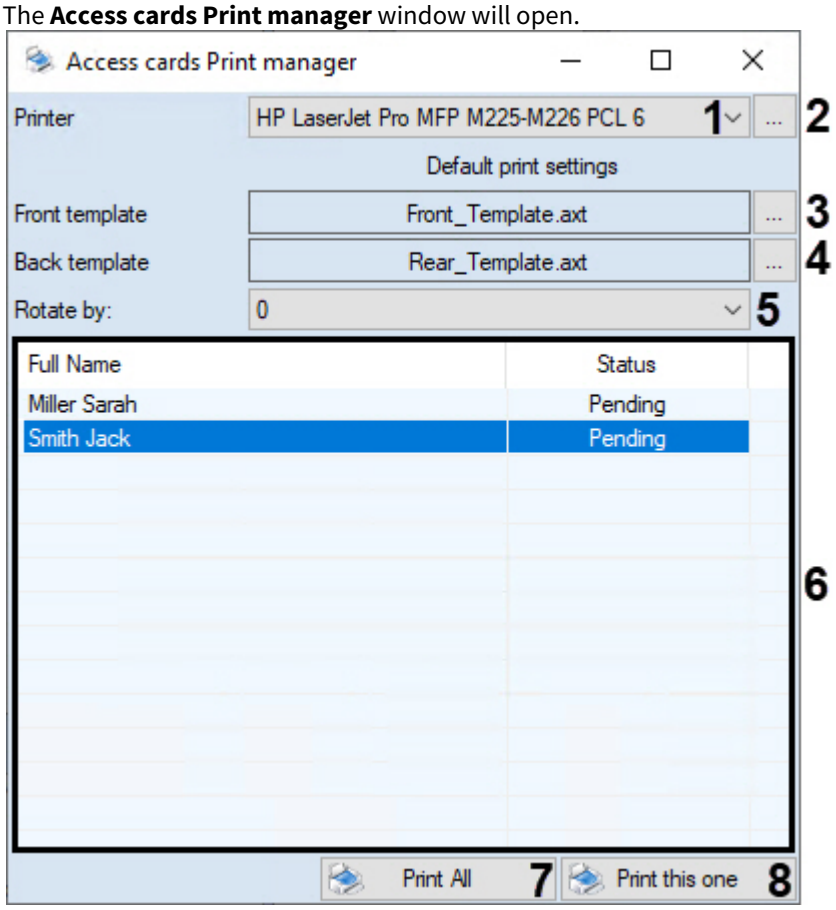
1. Go to viewing users list (see the Viewing a list of users section).
2. Right-click on the name of required user.

> **Note**
>
> You can also select several users: for example, by selecting them with the mouse or by using keyboard shortcuts (see Keyboard shortcuts for working with object lists).

3. Select the **Print access card** item in the opened functional menu.



4. The **Access cards Print manager** window will open.



5. From the **Printer** drop-down list (**1**), select the printer that will be used for printing. Click the (**2**) button if it is necessary to change the print settings for the selected printer.
6. Click the (**3**) button to select the front template of the access card. For duplex printing, click the (**4**) button to select the back template.

> **Note.**
>
> 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 should manually run the *EditorWpf.exe* utility from the *Modules* folder in the *Intellect* installation directory.

> **Note.**
>
> If the template has a bar code which is not shown in the preview, make sure that the suitable code format is selected – see Barcode object properties.

7. Select rotation angle in the (**5**) drop-down list to rotate template on the printed list by **0, 90, 180** or **270** degrees.

> **Note.**
>
> Rotation angle can also be set via **RotateAngle** registry key (see Registry keys reference guide for more details on the key and Working with Windows OS registry for details on how to operate the registry.

8. The list (**6**) displays all users for whom the access cards will be printed, as well as information on the status of printing. To preview the access card template, double-click on the required user. This will open the **Print Preview** window.
9. To print access cards for all users, click **Print All** (**7**). The **Access Manager** module will automatically create print queue and send access cards to the selected printer.
10. To print an access card for only one user, select the required user from the list (**6**) and click the **Print this one** button (**8**). The **Access Manager** module will automatically create a print queue and send the card 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.

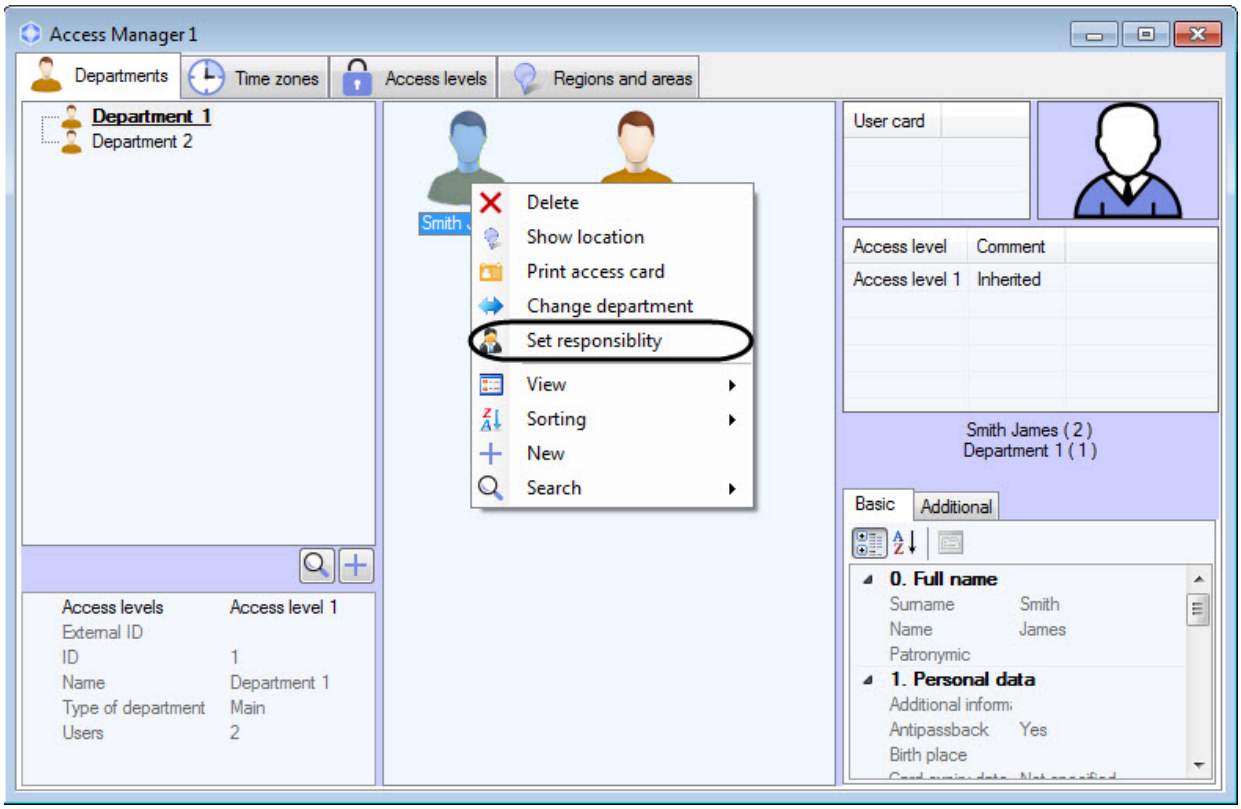
6.6.7 Assigning a user responsible for the region

It is possible to assign a user responsible for the region in the *Access Manager* software module.

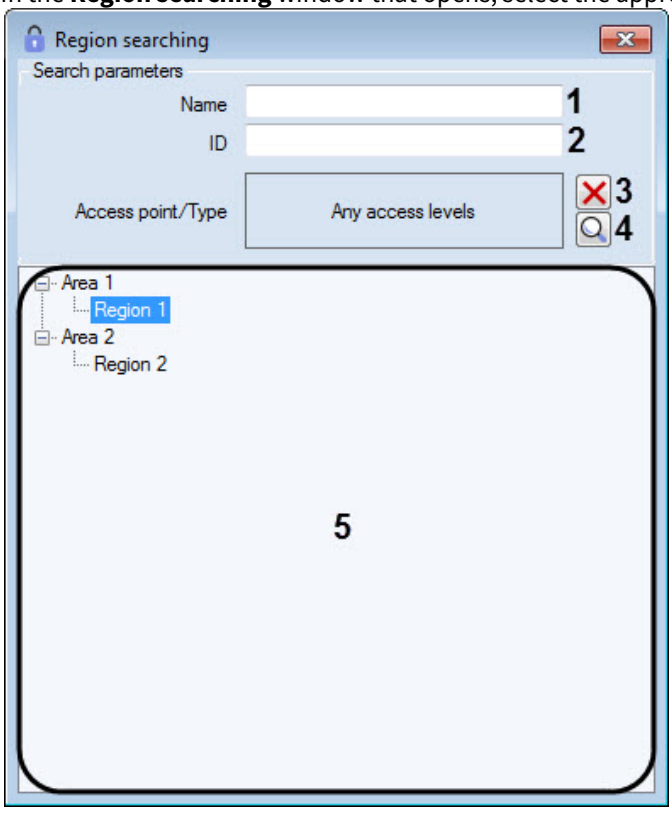
To assign a responsible user, do the following:

1. Go to the list of users (see Viewing a list of users).
2. Right-click on the name of the required user and select the **Set responsibility** item in the functional menu that opens.

> **Note**
>
> You can also select several users: for example, by selecting them with the mouse or by using keyboard shortcuts (see Keyboard shortcuts for working with object lists).

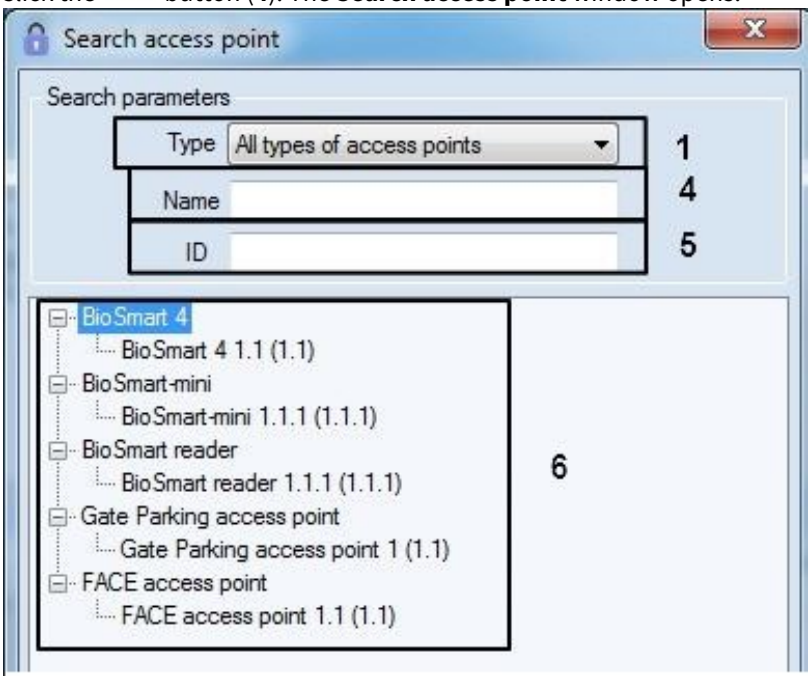


3. In the **Region searching** window that opens, select the appropriate region.



4. If necessary, specify the name of the required region in the **Name** field (**1**).
5. If necessary, enter the identifier of the required region in the **ID** field (**2**).
6. If necessary, specify a list of access points that should be included in the required region, as follows:

a. Click the button (**4**). The **Search access point** window opens.



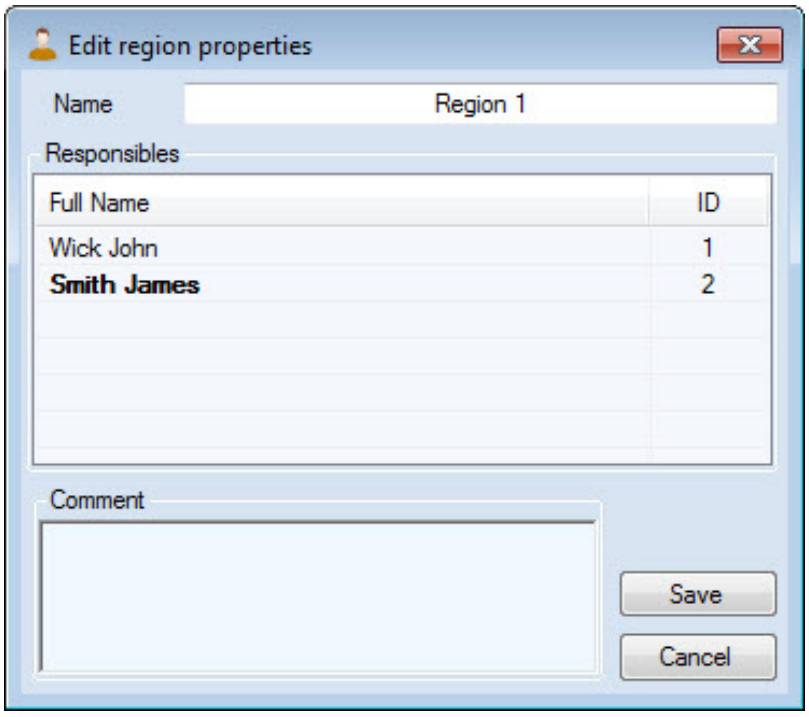
b. If necessary, select the access point type from the **Type** drop-down list (**1**).
c. If necessary, specify the access point name or its part in the **Name** field (**4**).
d. If necessary, specify the access point identifier in the **ID** field (**5**).
e. As a result, a list of search results satisfying the specified parameters will be displayed (**6**).
f. Double-click the necessary access point.

> **Note**
>
> To clear the list of access points, click the button (**3**).

Region search results will be displayed in the list (**5**). The search is case insensitive.

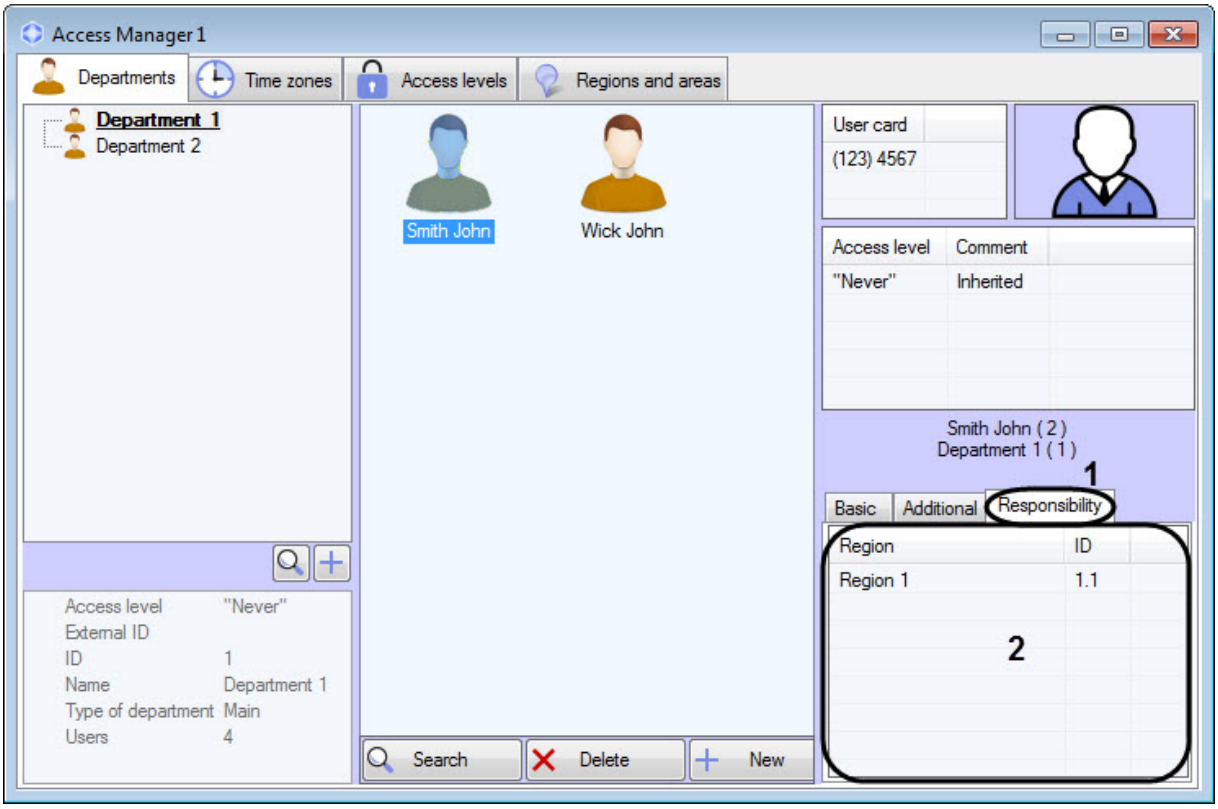
7. Double-click the necessary region. As a result, you will be taken to editing the region properties (see Creating and editing regions).

> **Note**
>
> The user that is currently being assigned responsible is highlighted in bold.



8. Click **Save** to confirm the assignment of the selected user responsible for the region.

The user who is responsible for the region will have the **Responsibility** tab (**1**). On this tab, a list of regions for which the corresponding user is responsible will be displayed (**2**).

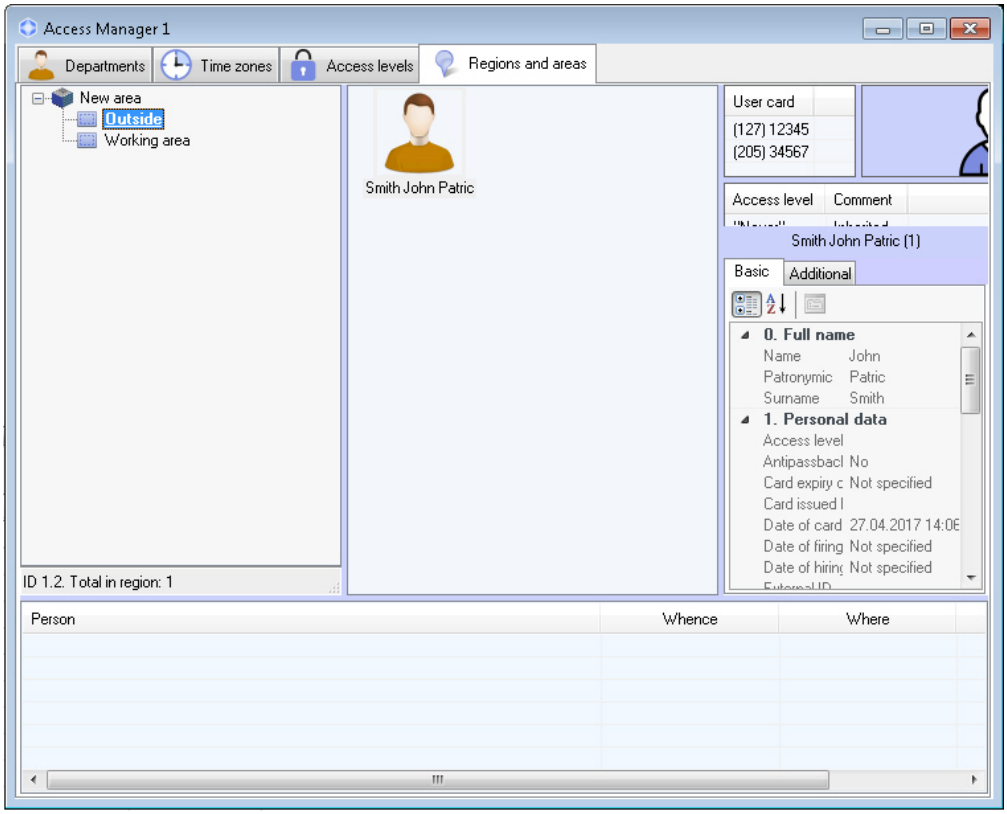


Assigning a user responsible for the region is now complete.

6.7 Performing Emergency Monitoring

6.7.1 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.

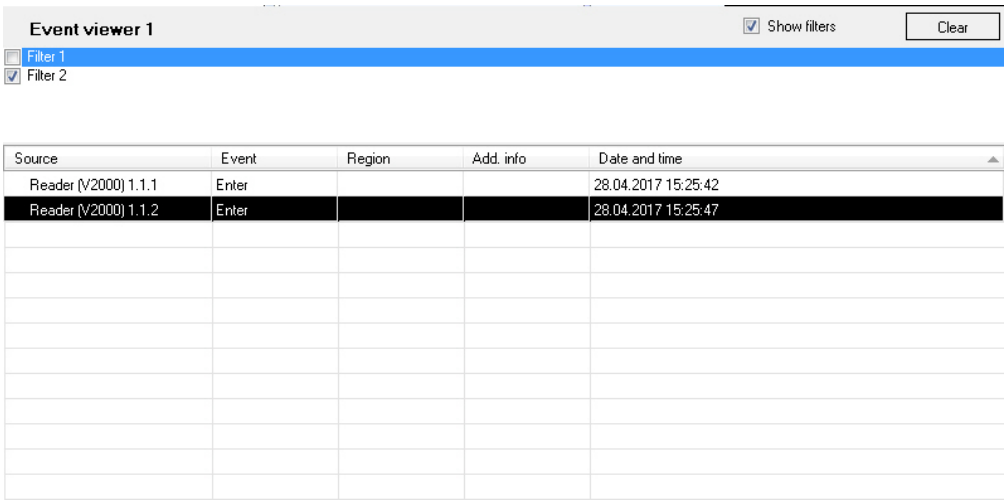
Creating, editing and deletion of the **Area** and **Region** objects in **Access Manager** is also possible – see Creating, editing and deleting Area and Region objects.

6.7.2 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.

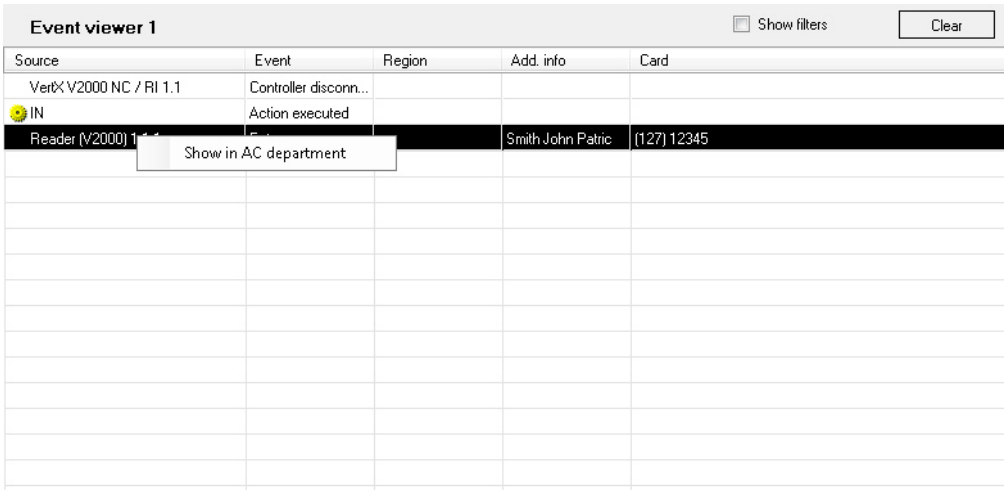
This column can be disabled according to the **Event Viewer** object settings – see Administrator's Guide, the Event viewer parameters section. The most relevant version of this document is available in the AxxonSoft documentation repository.



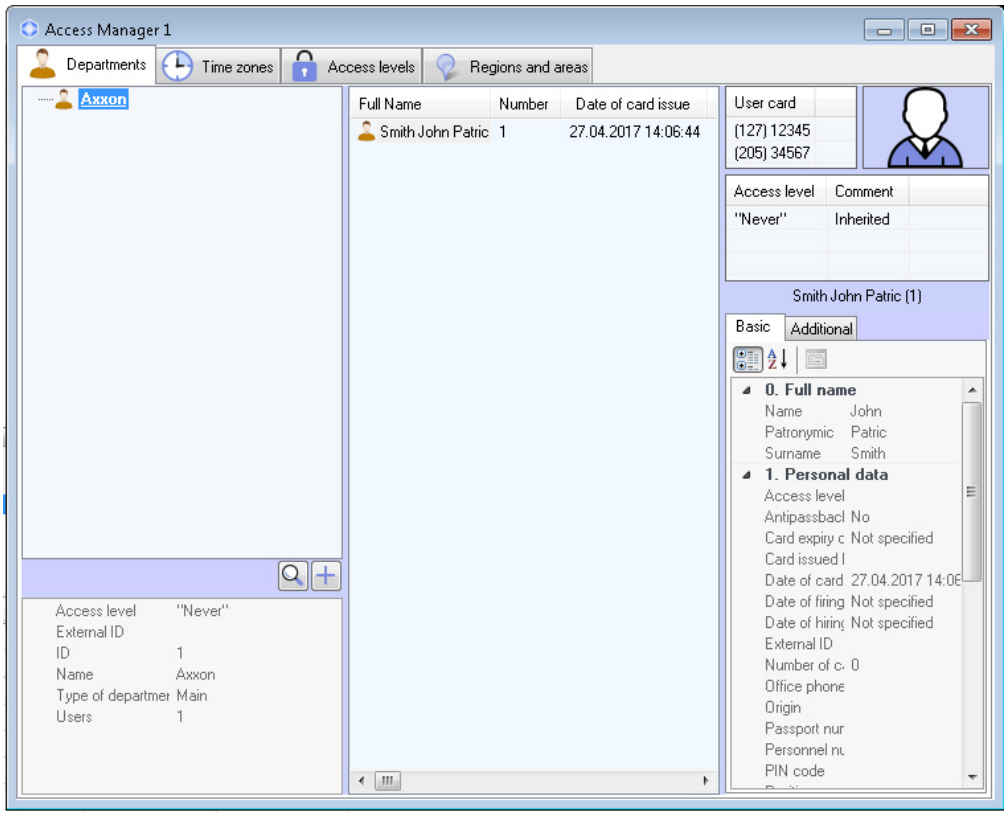
6.7.3 Viewing user profile by an access event in the Event viewer

Switching to the user profile in the Access Manager from Event viewer is possible for **Entrance** (ACCESS_IN) and **Exit** (ACCESS_OUT1) events.

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.



The **Departments** tab opens in the **Access Manager** window. A department to which the user belongs to is selected in the departments hierarchy, and the user himself is selected in the list.



Note.

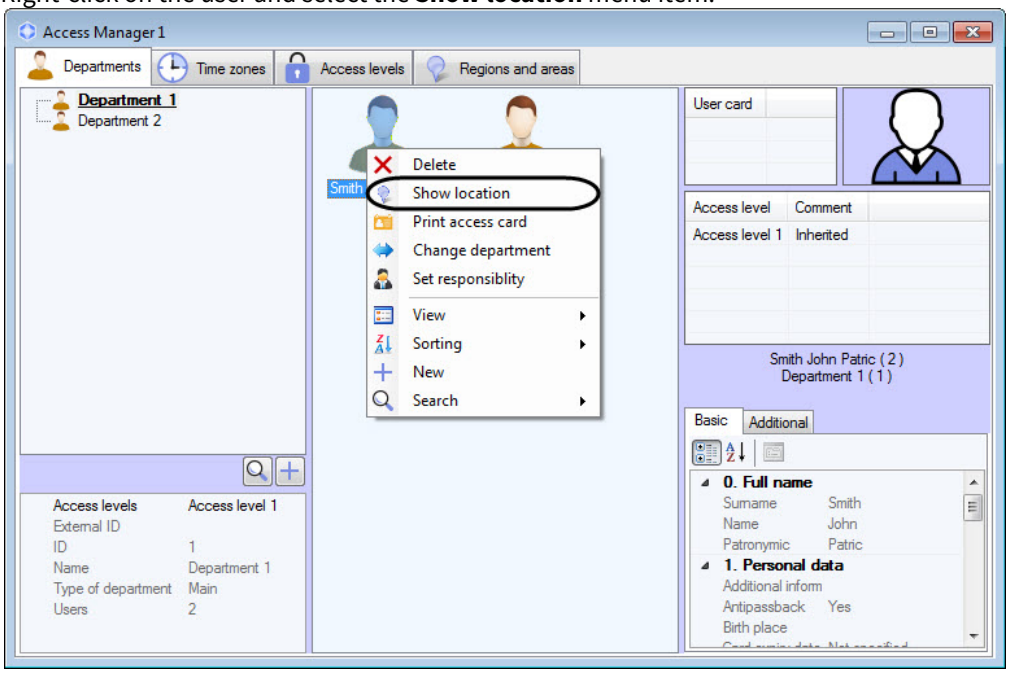
It is also possible to find out the user current location – see Finding out the region where the user currently is.

6.7.4 Finding out the region where the user currently is

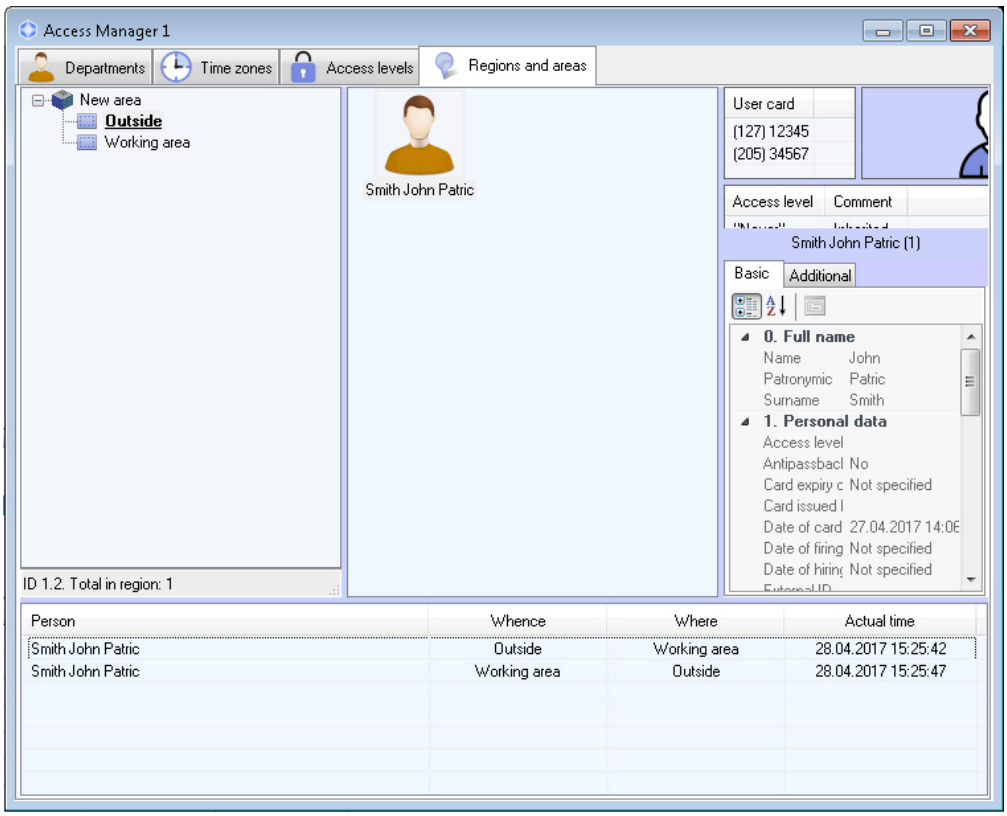
To find out the user current location, do the following:

1. Find the user on the Departments tab manually or perform the user search (see User search in the Access Manager software module).

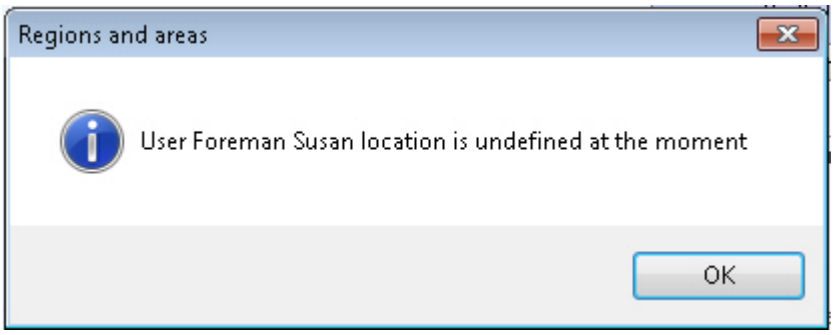
2. Right-click on the user and select the **Show location** menu item.



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.

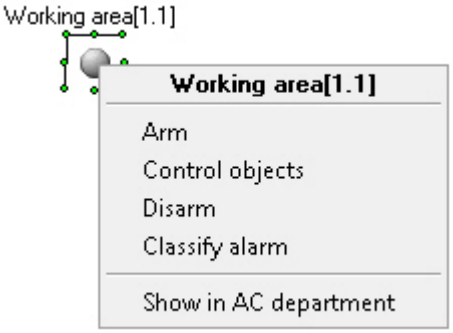


Defining the user current location is completed.

6.7.5 Viewing the list of users in the region

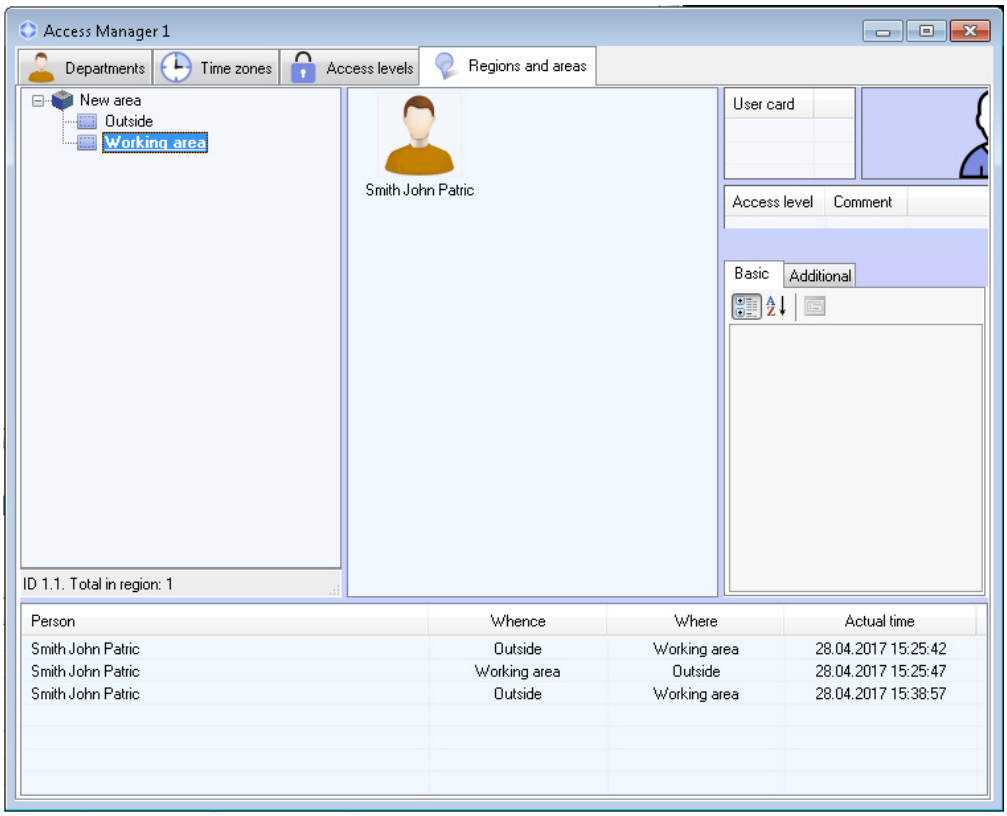
Switch to viewing users in the region in one of the following ways:

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.

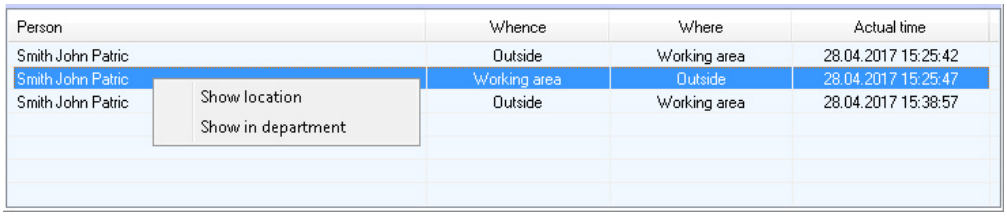
As a result, the list of users in the selected region is displayed. The information panel in the lower part of the regions and areas hierarchy displays the identifier of the selected region or ares and the number of users, that are currently located in this region or ares.



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.

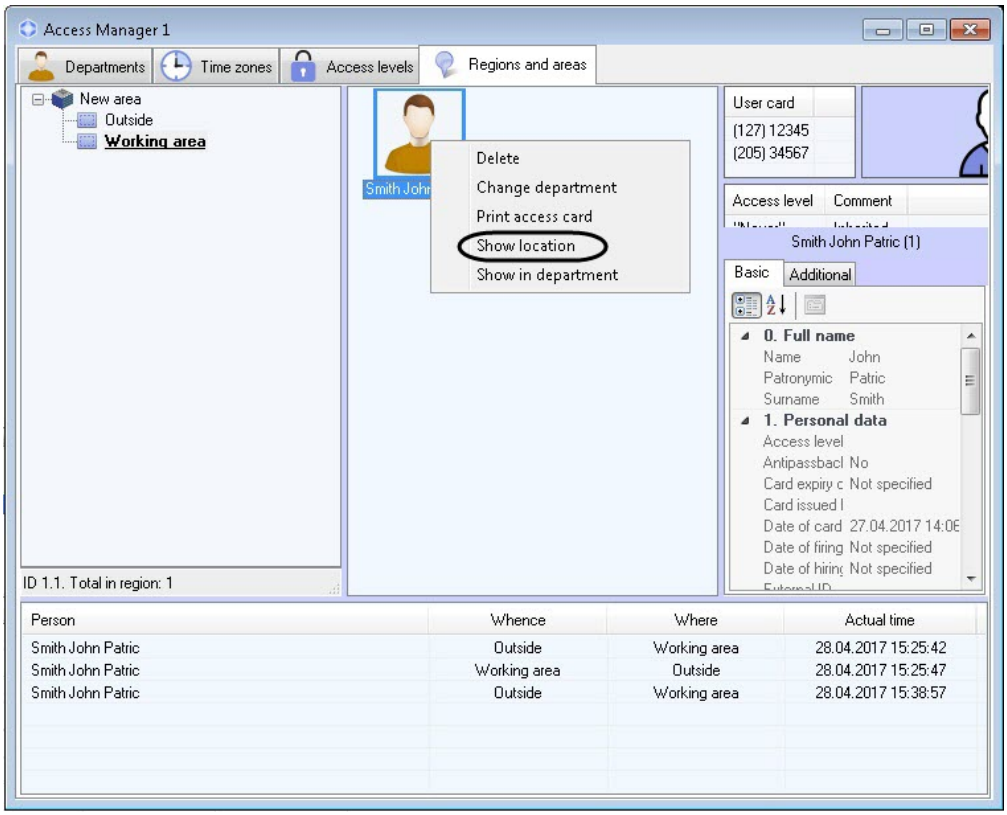
> **Note.**
>
> This data on passes is given for information only, it is not recorded in a separate database.

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



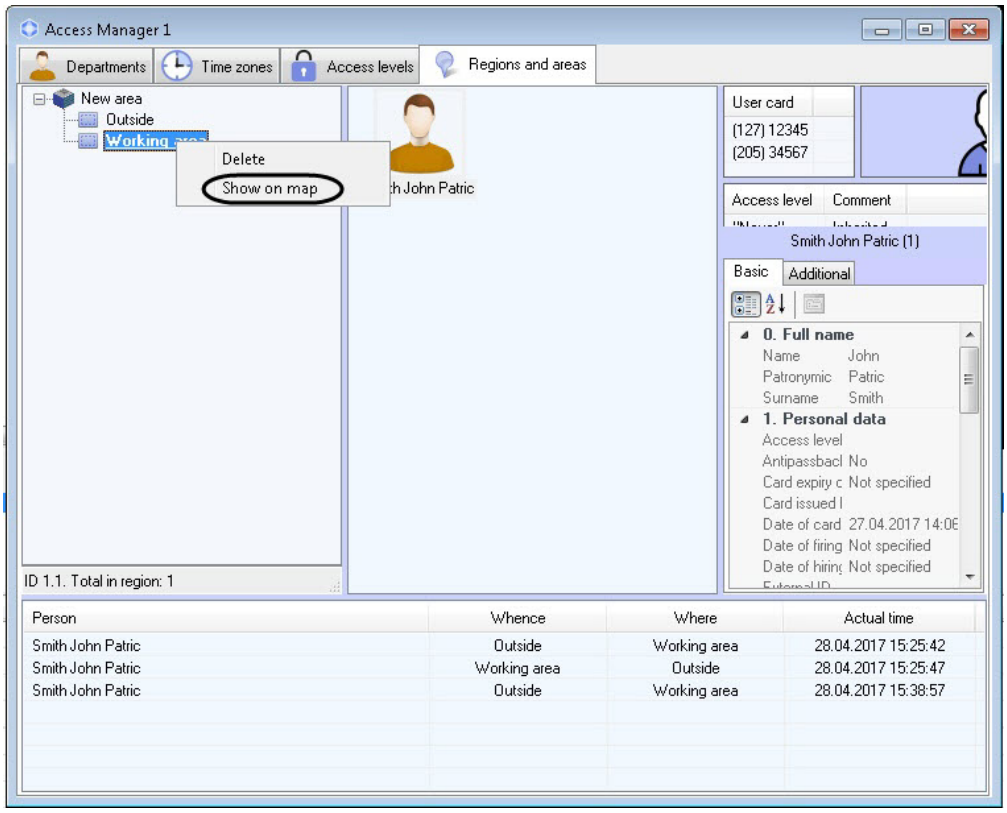
On the **Regions and areas** tab the same actions with a user as in the **Departments** tab are available (see Working with users in the Access Manager software module).

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



6.7.6 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.

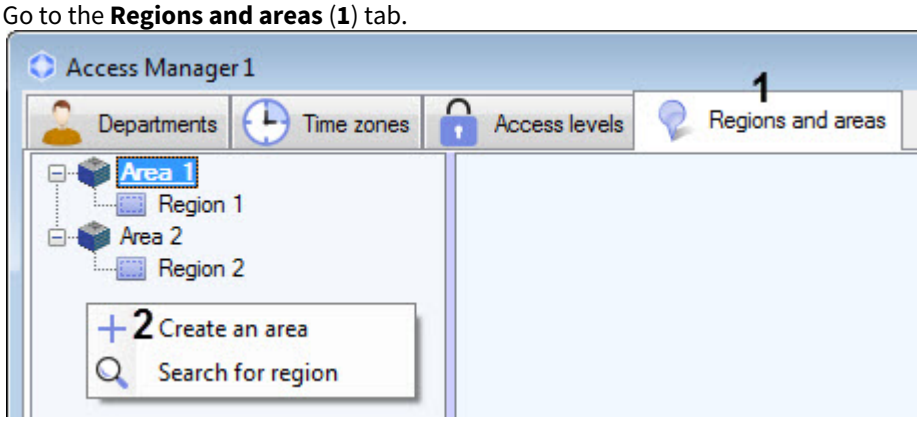
6.7.7 Creating, editing and deleting Area and Region objects

> **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

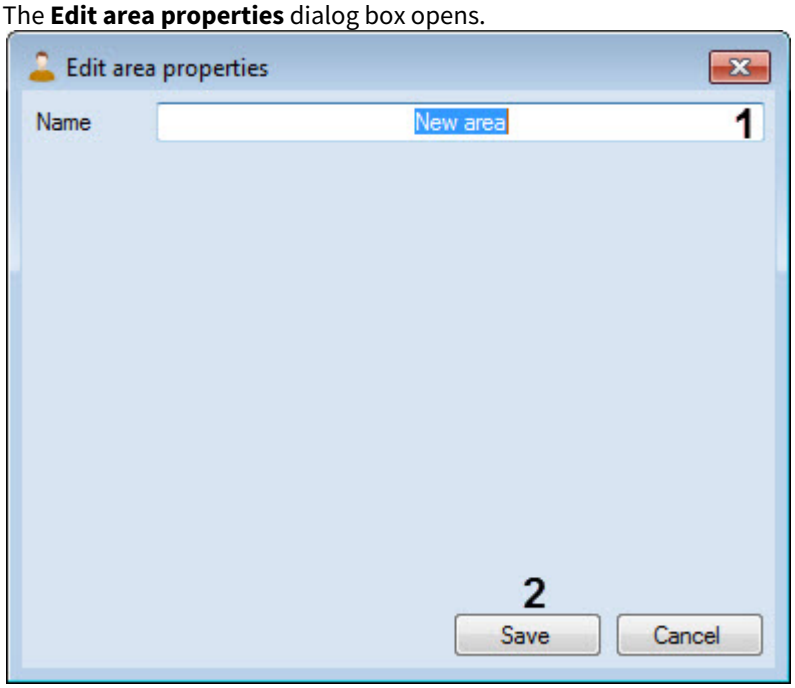
6.7.7.1 Creating areas

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

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



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



5. In the **Name** field enter the name of the area.

> **Note**
>
> The name should be unique. If an area with this name has already been created in the system, then while saving, a corresponding message will be displayed and the area will not be saved. Also, the name should not contain the following characters: < | >.

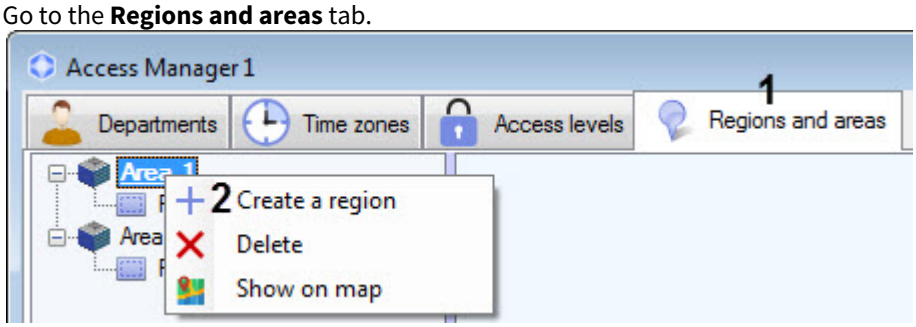
6. Click **Save** (**2**).

The area is created.

6.7.7.2 Creating and editing regions

To create or edit the region, do the following:

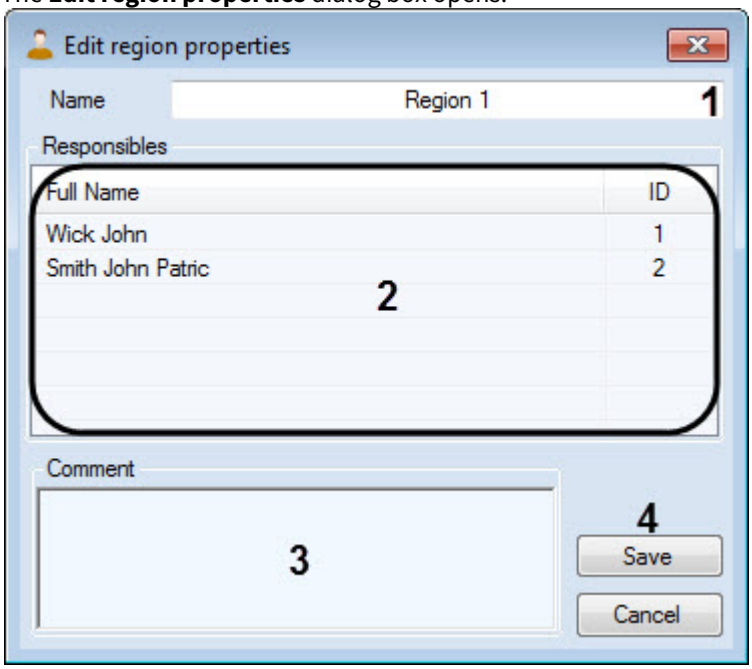
1. Go to the **Regions and areas** tab.

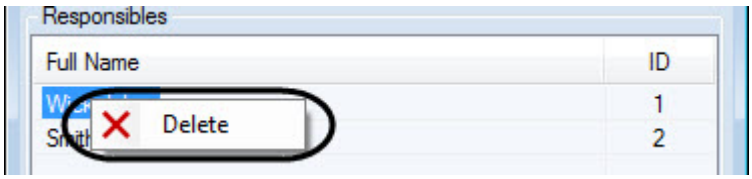


2. Right-click on the area under which the region is to be created.
3. In the menu that opens, select the **Create a region** item.

> **Note**
>
> To edit an existing region, double left-click the corresponding region.

4. The **Edit region properties** dialog box opens.





5. In the **Name** field (**1**), enter the region name.

> **Note**
>
> The name should be unique. If a region with this name has already been created in the system, then while saving, a corresponding message will be displayed and the region will not be saved. Also, the name should not contain the following characters: < | >.

6. In the **Responsibles** area (**2**), a list of users who are assigned responsible for this region is displayed (see Assigning a user responsible for the region).
7. To remove a user from the list of responsible users, right-click on the user and click the **Delete** button.

> **Note**
>
> You can select multiple users.

8. If necessary, in the **Comment** field (**3**), enter the region description.
9. Click **Save** (**4**).

The region is created or edited.

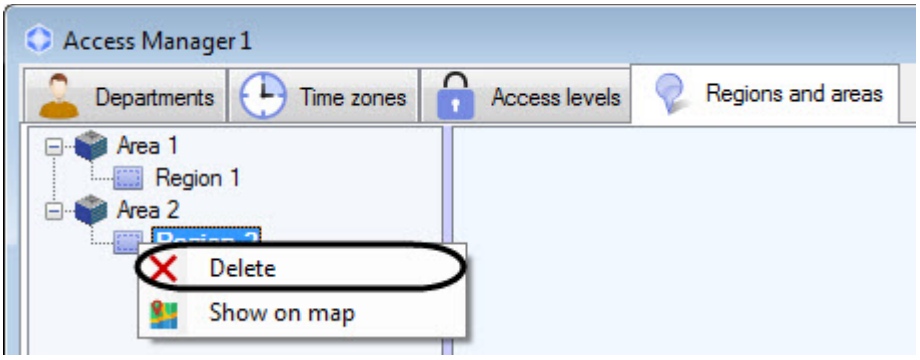
6.7.7.3 Editing areas and regions

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

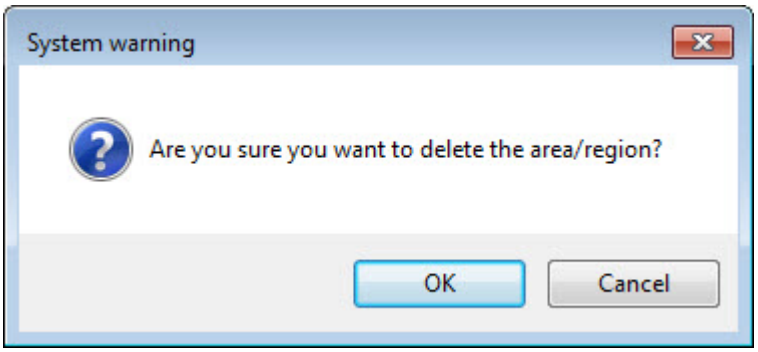
The **Edit area properties/Edit region properties** dialog box opens. Working with this dialog box is described in the Creating areas or Creating and editing regions section correspondingly.

6.7.7.4 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.



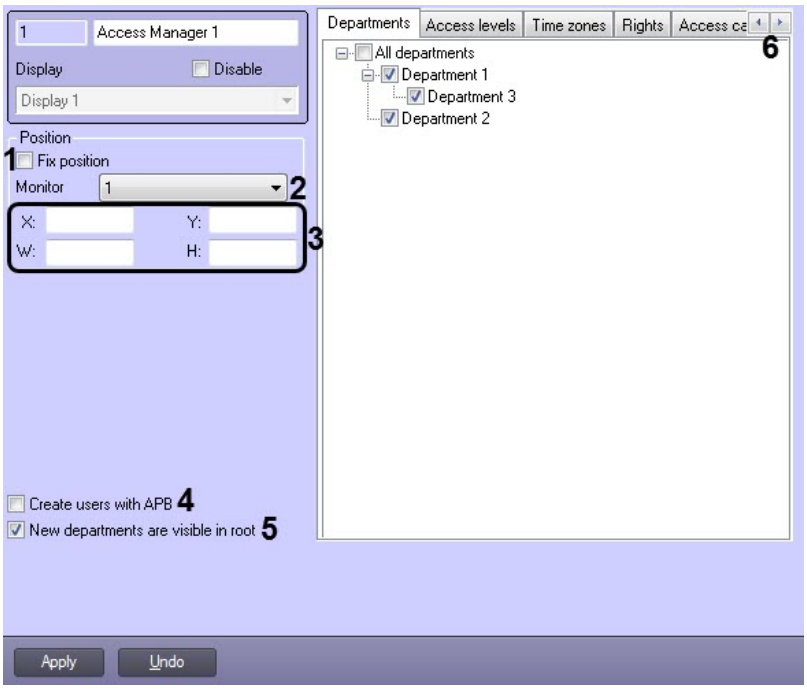
When you delete an area, all the child regions in it are deleted.

Deleting area or region is completed.

7 Appendix 1. Description of the Access Manager interfaces

7.1 The Access Manager object settings panel

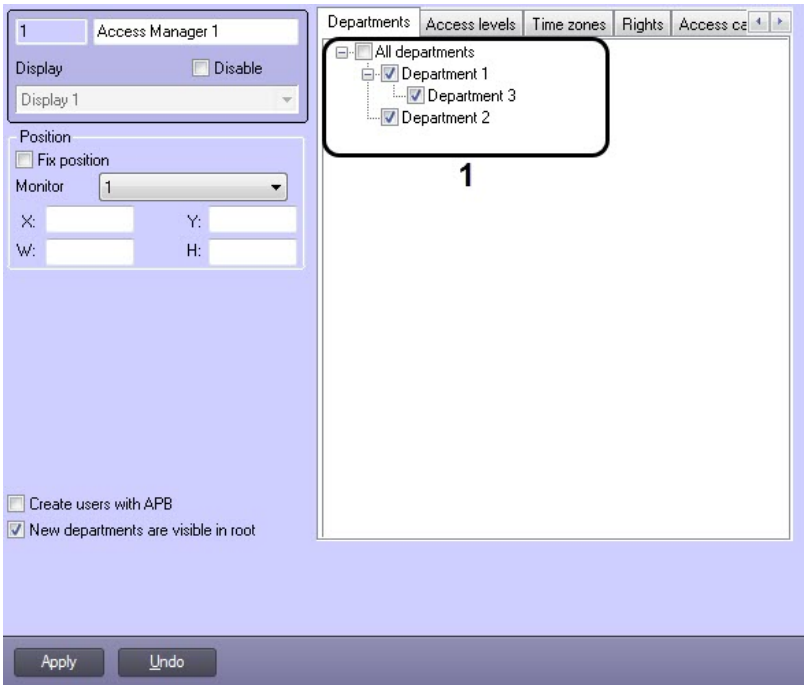
The figure shows the **Access Manager** interface object settings panel.



№	Parameter name	Parameter setting method	Description	Data type	Default value	Value range
The **Position** group						
1	**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.
2	**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
3	**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
	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
	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

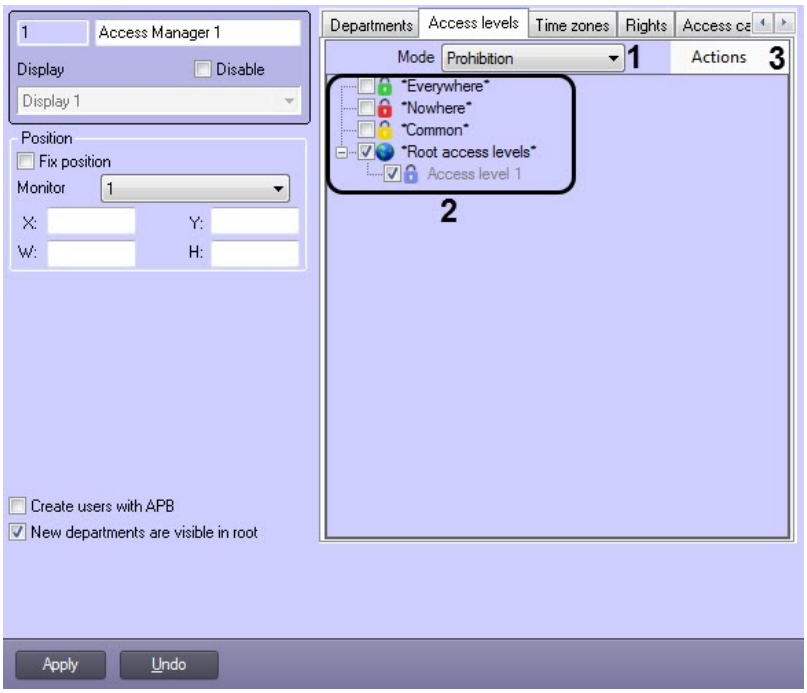
	H:	Setting the value in the field	Sets the **Access Manager** window height	% of screen height	0	From 0 to M*100, where M is a number of computer monitors
Out of groups						
4	**Create users with APB** checkbox	Checkbox	Sets the default setting for the user antipassback parameter	Boolean type	No	**Yes** - by default, the users are created with enabled antipassback **No** - by default, the users are created with disabled antipassback
5	**New departments are visible in root** checkbox	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
6	Tab navigation buttons	Click the button	Buttons switch the active tab	-	-	-

Departments tab



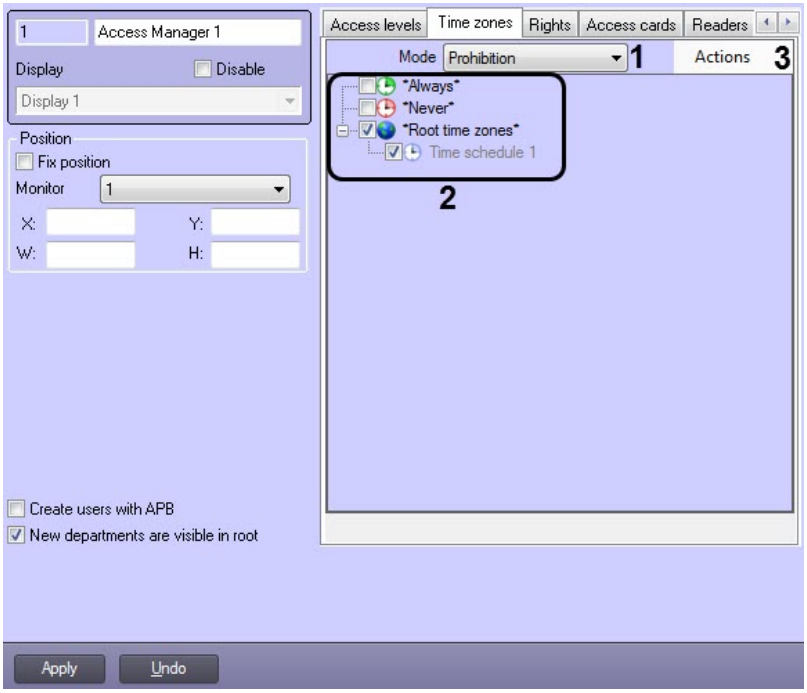
№	Parameter name	Parameter setting method	Description	Data type	Default value	Value range
1	Departments tree	Settings checkbox	Sets available departments in the **Access Manager** window	Boolean type	Set of boolean variables	Department will be available in the **Access Manager** window if checkbox is set close to it

Access levels tab



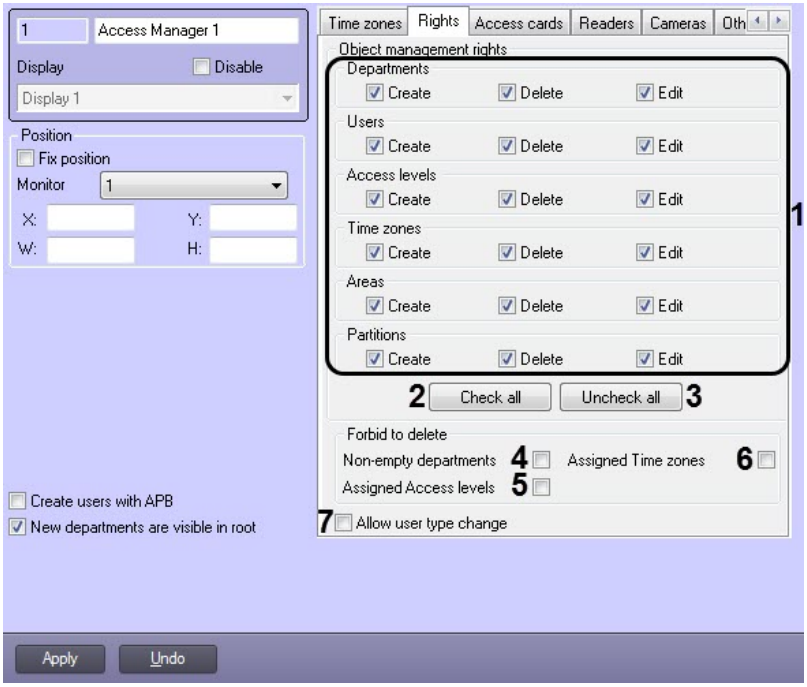
№	Parameter name	Parameter setting method	Description	Data type	Default value	Value range
1	**Mode** drop-down list	Selecting the value in the list	Sets the access restriction mode for access levels in the **Access Manager** interface object	-	Prohibition	**Prohibition** - restrict the access **Permission** - allow the access
2	Access levels tree	Checkbox	Specifies the access levels, the access to which should be configured	Boolean type	A set of boolean variables	If the checkbox is set for the access level, the selected access restriction mode will be applied to it in the **Access Manager** interface object
3	**Actions** button	Selecting the value in the list	Opens a list of actions for managing the access levels tree	-	-	**Minimize** - minimizes all access levels in the tree **Expand** - expands all access levels in the tree **Select all** - sets the checkboxes for all access levels **Remove all** - removes checkboxes for all access levels **Search** - opens the Access level or folder search window for access level or folder searching by the name or identifier

Time zones tab



№	Parameter name	Parameter setting method	Description	Data type	Default value	Value range
1	**Mode** drop-down list	Selecting the value in the list	Sets the access restriction mode for time zones in the **Access Manager** interface object	-	Prohibition	**Prohibition** - restrict the access **Permission** - allow the access
2	Time zones tree	Checkbox	Specifies the time zones, the access to which should be configured	Boolean type	A set of boolean variables	If the checkbox is set for the time zone, the selected access restriction mode will be applied to it in the **Access Manager** interface object
3	**Actions** button	Selecting the value in the list	Opens a list of actions for managing the time zones tree	-	-	**Minimize** - minimizes all time zones in the tree **Expand** - expands all time zones in the tree **Select all** - sets the checkboxes for all time zones **Remove all** - removes checkboxes for all time zones **Search** - opens the Time zone or folder search window for time zone or folder searching by the name or identifier

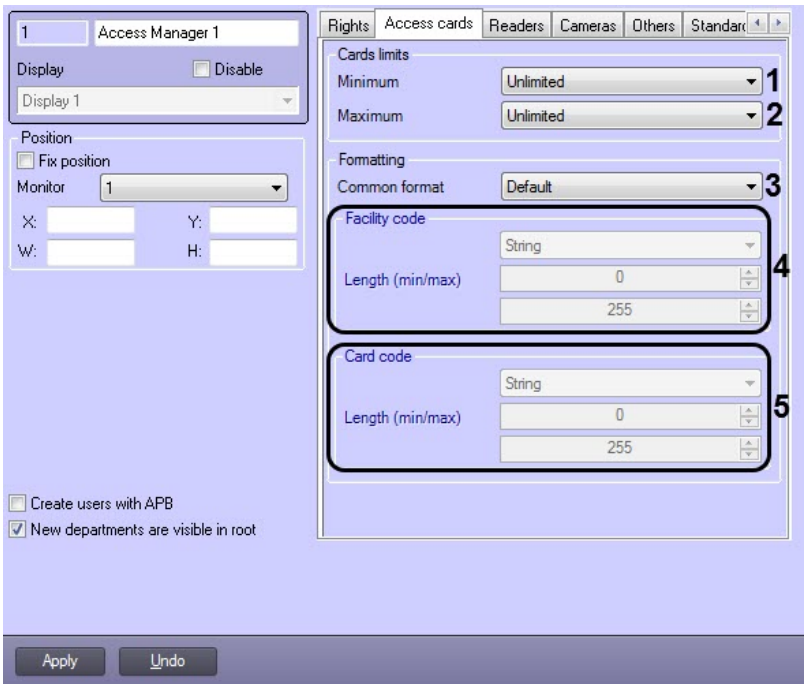
Right tab



№	Parameter name	Parameter setting method	Description	Data type	Default value	Value range
Object management rights group						
1	**Create** checkbox	Checkbox	Sets possibility to create the corresponding object in the **Access Manager** window	Boolean type	Yes	**Yes** – creating the corresponding object from the **Access Manager** window is allowed. **No** – creating the corresponding object from the **Access Manager** window is forbidden.
	Delete checkbox	Checkbox	Sets possibility to delete the corresponding object in the **Access Manager** window	Boolean type	Yes	**Yes** – deleting the corresponding object from the **Access Manager** window is allowed. **No** – deleting the corresponding object from the **Access Manager** window is forbidden.
	Edit checkbox	Checkbox	Sets possibility to edit the corresponding object in the **Access Manager** window	Boolean type	Yes	**Yes** – editing the corresponding object from the **Access Manager** window is allowed. **No** – editing the corresponding object from the **Access Manager** window is forbidden.
2	**Check all** button					
3	**Uncheck all** button					
Forbid to delete group						
4	**Non-empty departments** checkbox	Settings checkbox	Forbids to delete departments if there are users in them	Boolean type	No	**Yes** – non-empty departments cannot be deleted. **No** – non-empty departments can be deleted.
5	**Assigned Access Levels** checkbox	Settings checkbox	Forbids to delete access levels if they are assigned to user(s)	Boolean type	No	**Yes** – assigned access levels cannot be deleted. **No** – assigned access levels can be deleted.

6	**Assigned Time Zones** checkbox	Settings checkbox	Forbids to delete time zones if they are assigned to access levels	Boolean type	No	**Yes** – assigned time zones cannot be deleted. **No** – assigned time zones can be deleted.
Out of groups						
7	**Allow user type change** checkbox	Settings checkbox	Enables the ability to change the user type	Boolean type	No	**Yes** – the user type change is allowed. **No** – the user type change is not allowed.

Access cards tab

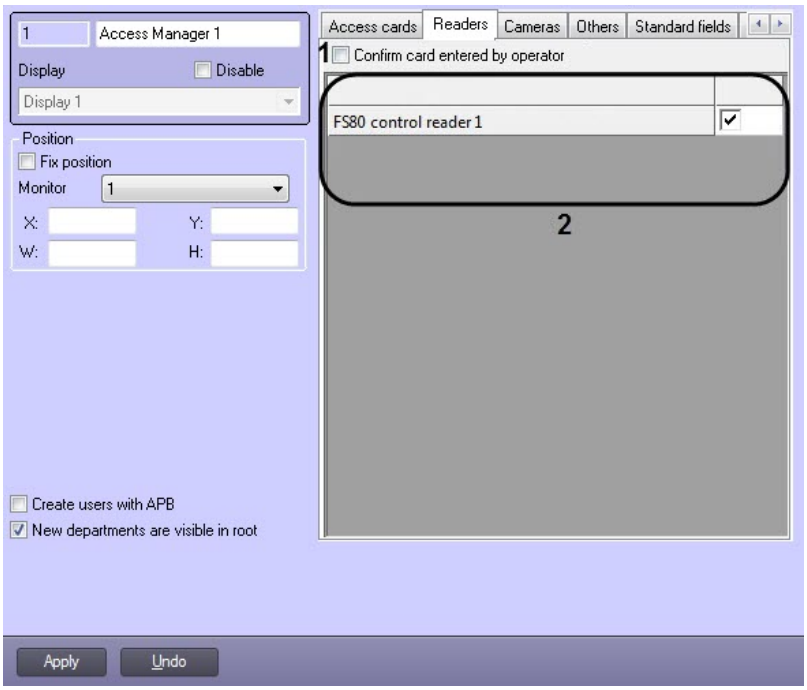


№	Parameter name	Parameter setting method	Description	Data type	Default value	Value range
1	**Minimum** drop-down list	Selecting the value in the list	Sets the minimum number of access cards that should be assigned to the user	List of values	Unlimited	• from **1** to **5** - if the specified number of access cards is not assigned to the user, then this user cannot be saved in the **Access Manager** interface object. • **Unlimited** - an unlimited number of access cards can be assigned to the user. • **Prohibited** - the user cannot be assigned access cards. Buttons and functional menu for assigning access cards will be inactive in the **Access Manager** interface object.
2	**Maximum** drop-down list	Selecting the value in the list	Sets the maximum number of access cards that should be assigned to the user	List of values	Unlimited	• from **1** to **5** - if the user is assigned more than the specified number of access cards, then this user cannot

						be saved in the **Access Manager** interface object. • **Unlimited** - an unlimited number of access cards can be assigned to the user. • **Prohibited** - the user cannot be assigned access cards. Buttons and functional menu for assigning access cards will be inactive in the **Access Manager** interface object.
3	**Common format** drop-down list	Selecting the value in the list	Sets the access cards format	List of values	Default	• **Default** - allows setting an arbitrary value for the facility code and card code. Any letters, numbers and symbols are allowed except: <| >. • **Wiegand26** - allows entering a 1-byte facility code (from 0 to 255), and a 2-byte card code (from 0 to 65535). • **Wiegand32** - allows entering a 2-byte facility code (from 0 to 65535), and a 2-byte card code (from 0 to 65535). • **Wiegand26** (code only) - the facility code cannot be set, only a 3-byte card code is set (from 0 to 16777215). • **Wiegand32** (code only) - the facility code cannot be set, only a 4-byte card code is set (from 0 to 4294967295). • **TouchMemory** - the facility code cannot be set, only the 8-byte card code is set. The format is hexadecimal, characters A, B, C, D, E, F are allowed. The code should be 8 characters or longer. If the entered card code is less than 8 characters long, the the higher order digits are filled with zeros. • **Hikvision** - the *Hikvision* ACS format. It always has a fixed H character in the facility code. The card code is specified by a string with a maximum length of 32 characters. • **Configurable** - allows setting the parameters of the facility code (**4**) and card code (**5**). • **Fixed character** - the specified single character will always be hard-coded, which

						cannot be changed in the **Access Manager** interface object. • **String** - allows entering a string of 0 to 255 characters. • **Numeric** - allows entering only numbers from 0 to 4294967295. • **Hexadecimal** - allows entering numbers in HEX format (numbers and symbols A, B, C, D, E, F) from 0 to 8 bytes long. • **Fixed number** - similar to **Fixed character**, but instead of a character, a number between 0 and 4294967295 is used. • **Regular template** - allows defining an access card template with specified restrictions, lengths and value ranges.

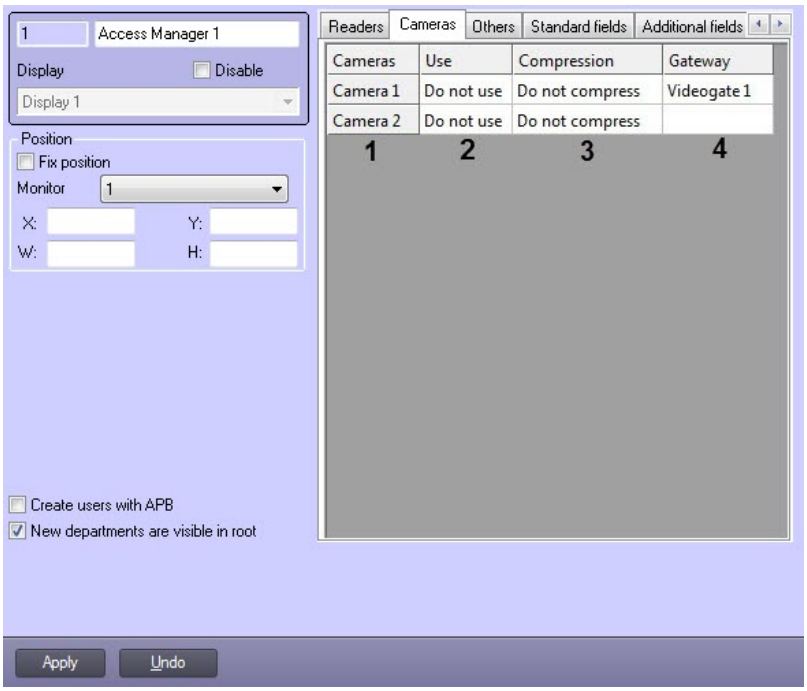
Readers tab



№	Parameter name	Parameter setting method	Description	Data type	Default value	Value range

1	**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.
2	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

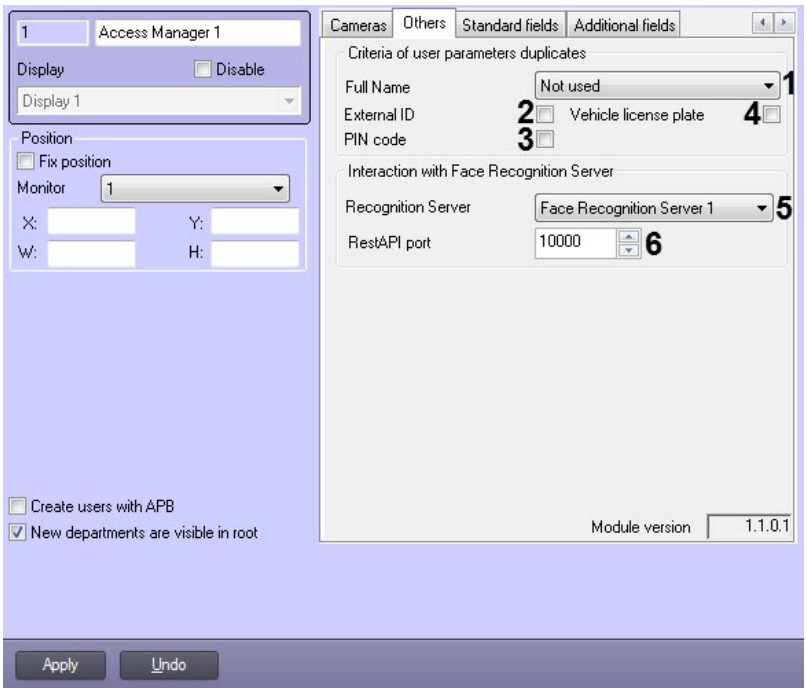
Cameras tab



№	Parameter name	Parameter setting method	Description	Data type	Default value	Value range
1	**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
2	**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
3	**Compression** drop-down list	Selecting the value in the list	Sets the compression level of the selected video stream	-	Do not compress	**Do not compress** - compression of the camera video stream is disabled **Level 1** - the lowest level of video stream compression .... **Level 5** - the highest level of video stream compression

4	**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

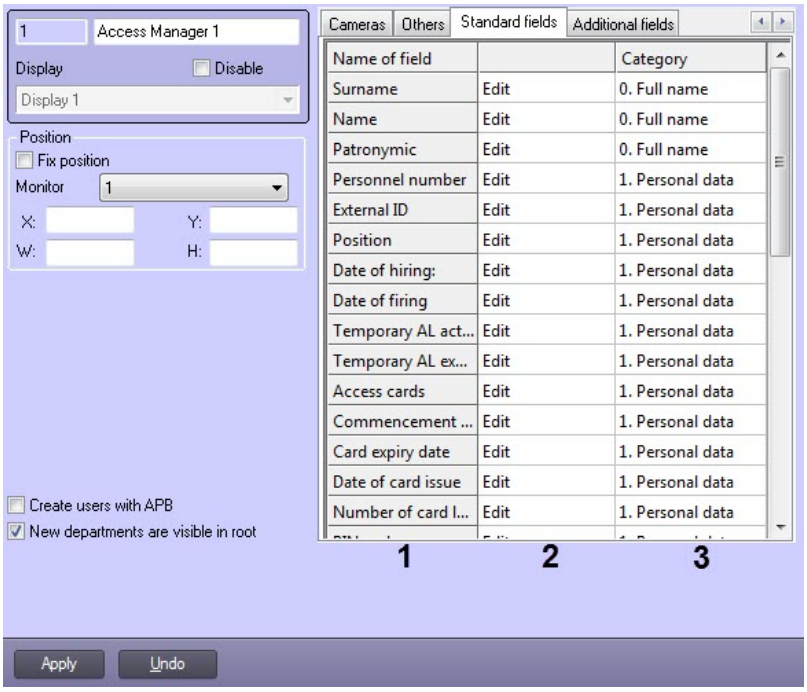
Others tab



№	Parameter name	Parameter setting method	Description	Data type	Default value	Value range
1	**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.
2	**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.
3	**PIN code** checkbox	Settings checkbox				
4	**Vehicle license plate** checkbox	Settings checkbox	Indicates whether the users records should be checked for vehicle license 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.
5	**Recognition Server** drop-down list	Selecting the value in the list	Displays a list of **Face Recognition Server** objects created on the **Hardware** tab of the **System Settings** dialog box	List of **Face Recognition Server** objects created in the system	-	Depends on number of accessible **Face Recognition Server** objects in the system

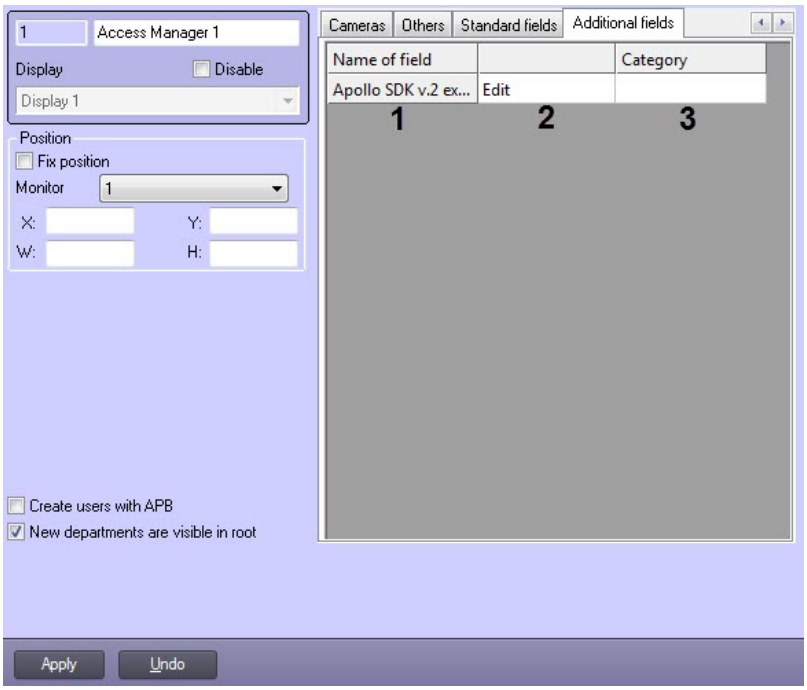
6	**RestAPI port** field	Setting the value in the field	Specifies the communication port to connect to the Face Recognition Server through the REST API. By default, it is necessary to set the **10000** value.	Number	0	-

Standard fields tab



№	Parameter name	Parameter setting method	Description	Data type	Default value	Value range
1	**Name of field** column	Automatic	Displays a list of standard user fields	-	Names of standard user fields	-
2	Drop-down list	Selecting the value in the list	Specifies the permissions to edit, specify, or hide the standard fields from the **Access Manager** interface object	-	Depends on the standard field	**Edit** - the field is displayed in the list of user parameters while viewing and editing and is available for editing **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 **Mandatory** - this field is displayed and is required when creating a new user
3	**Category** column	Setting the value in the field	Specifies the name of the category to which the standard field belongs	-	Depends on the standard field	Any value

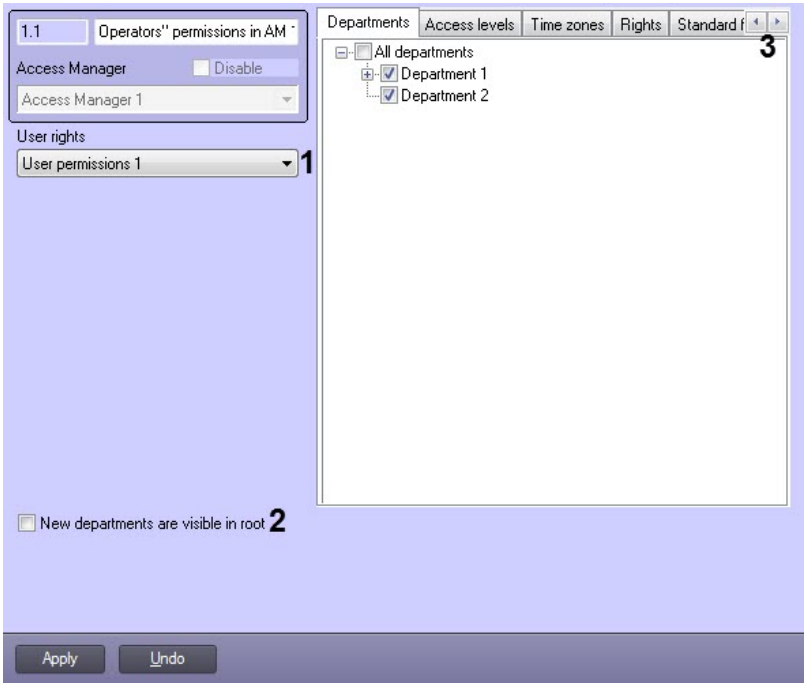
Additional fields tab



№	Parameter name	Parameter setting method	Description	Data type	Default value	Value range
1	**Name of field** column	Automatic	Displays a list of additional user fields	-	Names of additional user fields	-
2	Drop-down list	Selecting the value in the list	Specifies the permissions to edit, specify, or hide the additional fields from the **Access Manager** interface object	-	Depends on the additional field	**Edit** - the field is displayed in the list of user parameters while viewing and editing and is available for editing **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 **Mandatory** - this field is displayed and is required when creating a new user
3	**Category** column	Setting the value in the field	Specifies the name of the category to which the additional field belongs	-	Depends on the additional field	Any value

7.2 The Operators'' permissions in AM object settings panel

The figure shows the **Operators'' permissions in AM** interface object settings panel.



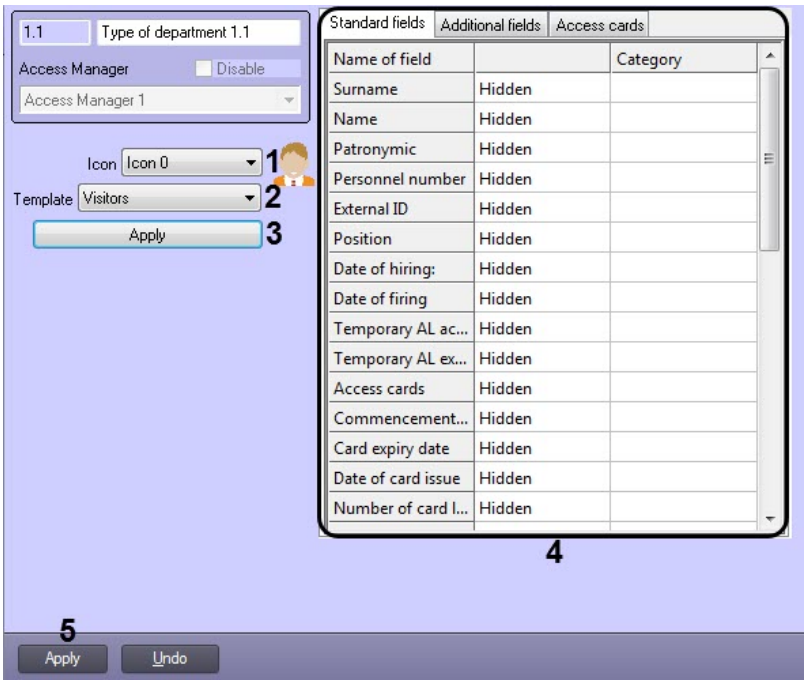
The following table shows the elements in the **Operators'' permissions in AM** settings panel.

№	Parameter name	Parameter setting method	Description
User rights group			
1	**User rights** drop-down list	Selecting the value in the list	Sets user rights in the *ACFA-Intellect* software package, corresponding to the configured **Operators'' permissions in AM** object
Without group			
2	**New departments are visible in root** checkbox	Setting the checkbox	Sets availability of new created departments in the **Access Manager** hierarchy root
3	Tab navigation buttons	Click the button	Buttons switch the active tab

The **Departments**, **Access levels**, **Time zones**, **Rights**, **Standard fields** and **Additional fields** tabs are similar to the tabs on the settings panel of the **Access Manager** object (see The Access Manager object settings panel).

7.3 The Type of department object settings panel

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



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

№	Parameter name	Parameter setting method	Description	Data type	Default value	Value range
1	**Icon** drop-down list	Selecting the value from the list	Sets icon used for displaying department in the tree in the **Access Manager** window	Name of accessible icons	Icon 0	Icon 0 – Icon 29
2	**Template** drop-down list	Selecting the value from the list	Sets fields available for viewing and editing typical for some users category	Name of accessible templates	-	Employees Vehicle Visitors
3	**Apply** button	Clicking the button	Applying the selected template	-	-	-
4	Group of tabs	-	Access to the **Standard fields**, **Additional fields** for setting the visibility of user fields, as well as access to the **Access cards** to configure the parameters of access cards of this type of department	-	-	-

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

8.1 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:

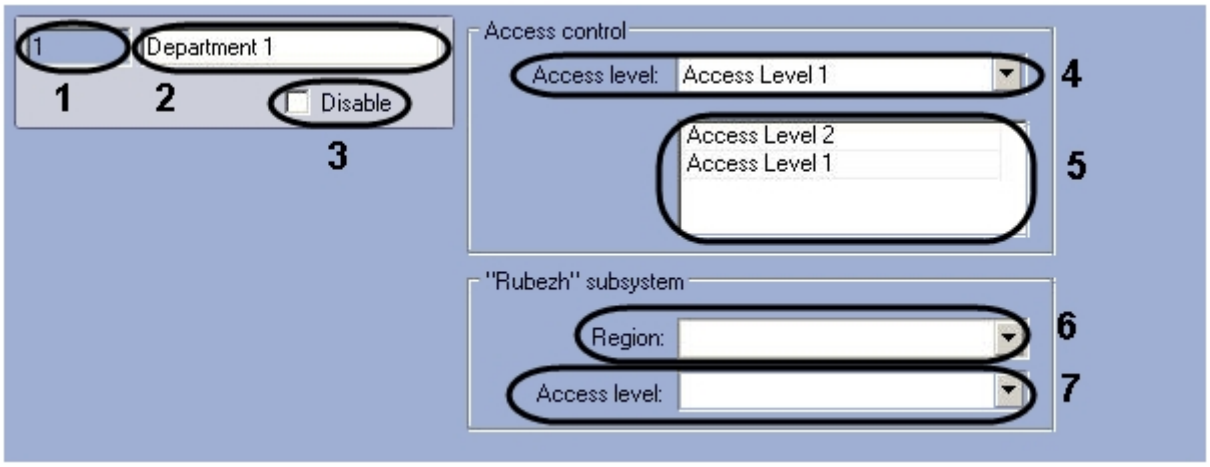
1. **User** and **Department** objects created on the **Users** tab of **the System settings** dialog box.
2. **Access level** and **Time zone** (which corresponds both to time zone and shift work in the VMS) objects created on the **Programming** tab of the **System settings** dialog box.

> **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.

8.2 Settings panel of the Department object

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



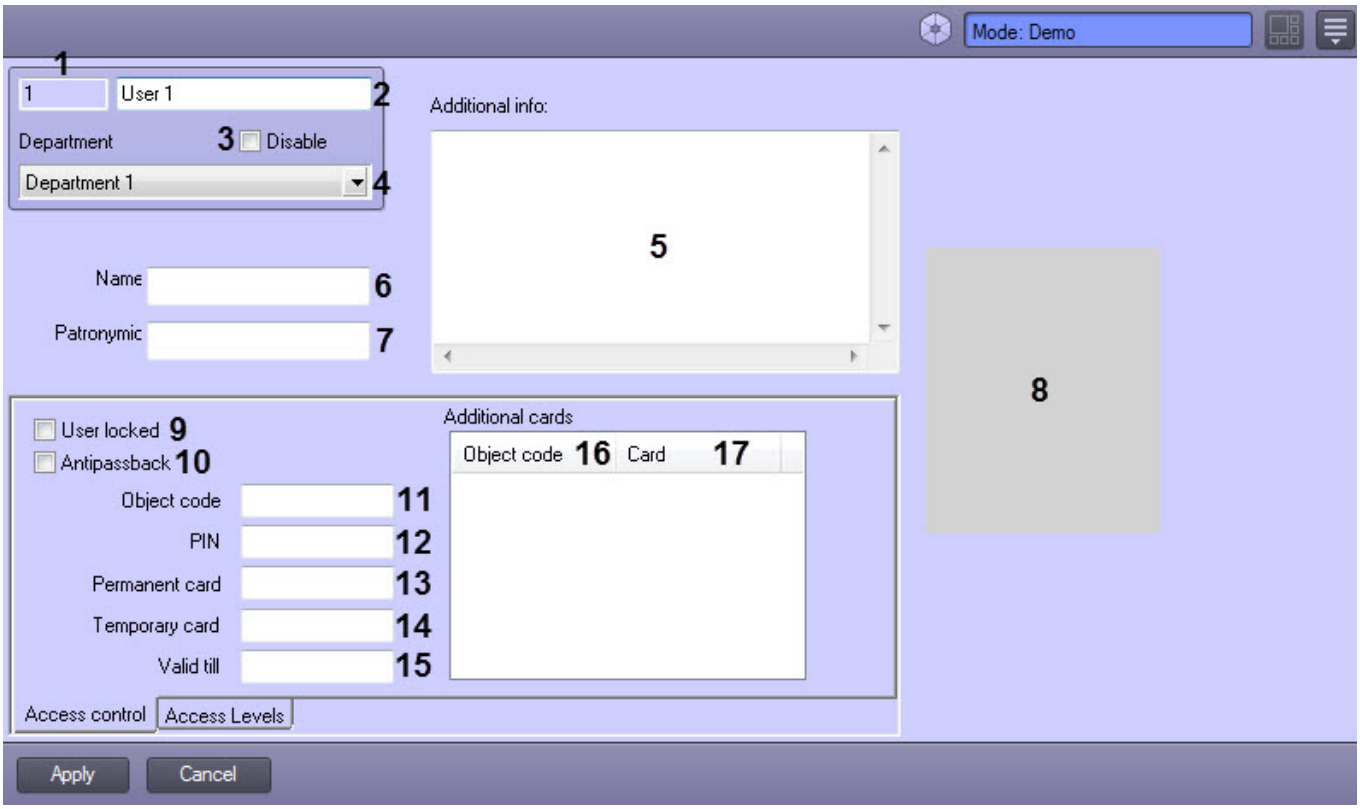
The table gives the description of the **Department** object settings.

#	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

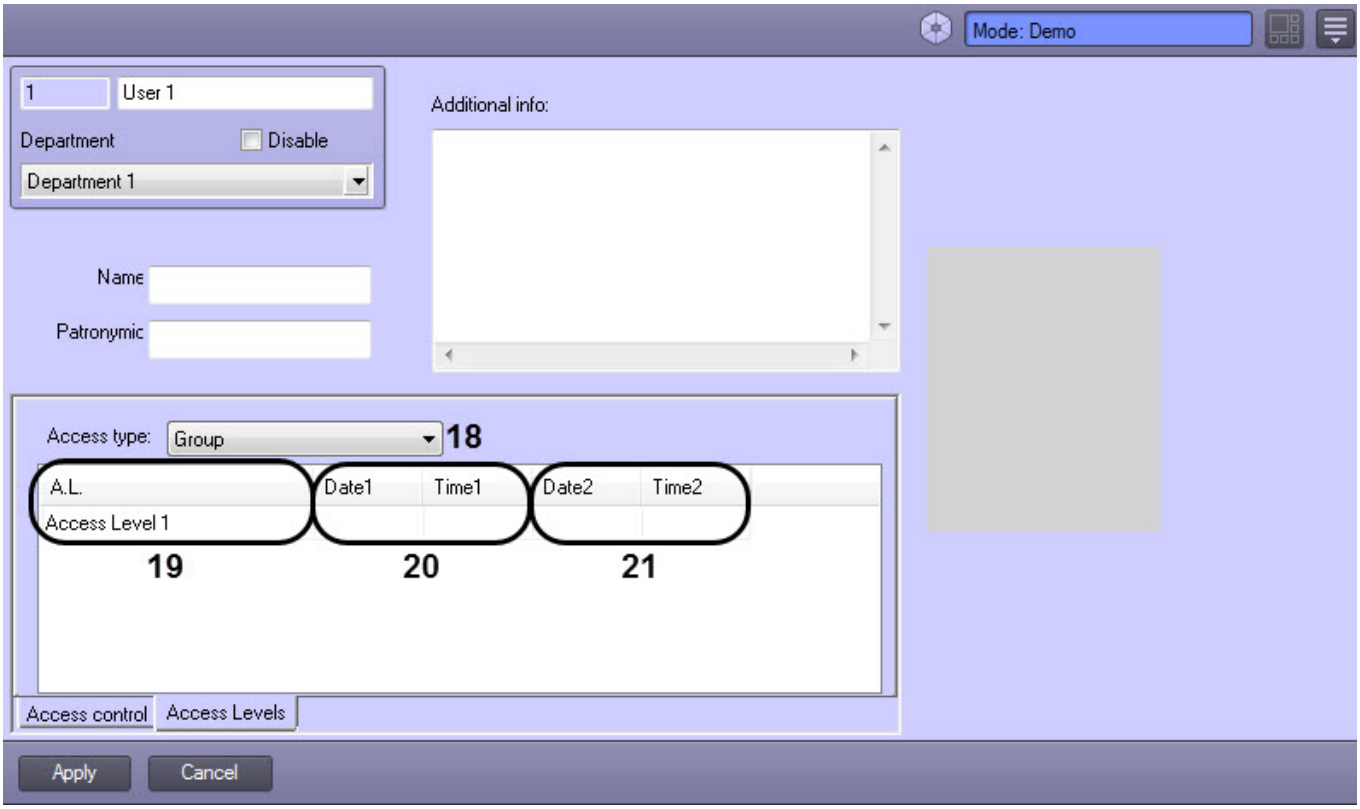
#	Parameter name	Method for setting the parameter value	Parameter description	Default value	Value range
					characters except < | > symbols), not case-sensitive. Number of symbols – from 1 to 60.
3	**Disable** checkbox	Is set in a checkbox	Sets the status (enabled/ disabled) of the **Department** object 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 *ACFA Intellect* (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 *ACFA Intellect* (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 *Rubeg-07 ACS* (discontinued)	-	The list of **Region** objects in the *ACFA Intellect* software
7	**Access level** dropdown list	Is selected in the list	Sets the access level for the *Rubeg-07 ACS* (discontinued)	-	The list of **Access level** objects created in *ACFA Intellect* (on the **Programming** tab or via the VMS) and also **Full access** and **Access forbidden** levels.

8.3 Settings panel of the User object

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



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



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

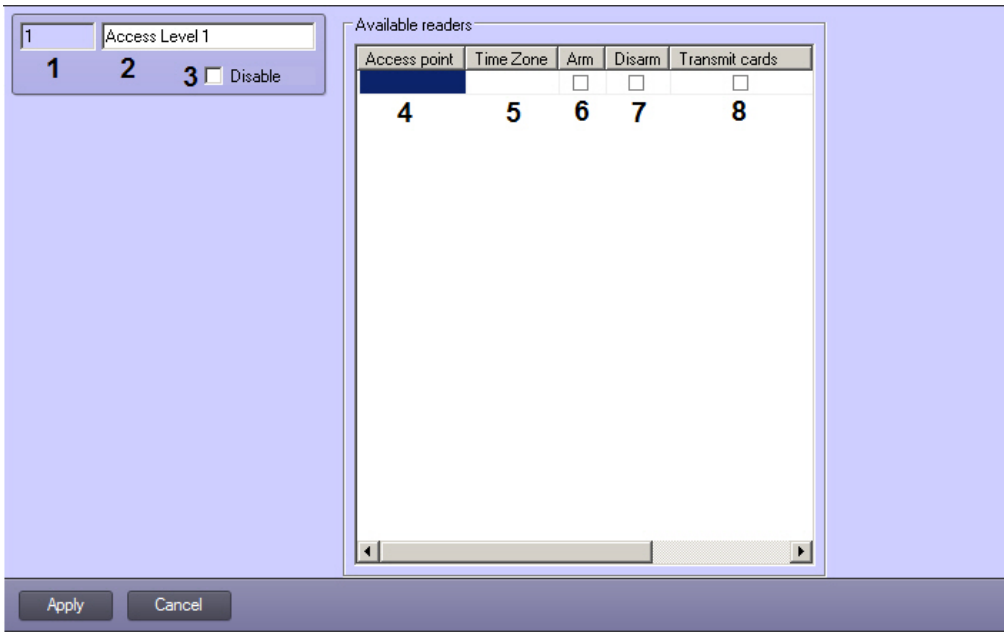
The table gives the description of the **User** object settings.

#	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	**Surname** field	Enter the value in the field	Sets the surname of the **User** object in the system	User	A line representing a sequence of any symbols (letters, digits, service characters except < | > 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 *Intellect Web Report System*.
3	**Disable** Checkbox	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
6	**Name** field	Enter the value in the field	Sets the name of the **User** object in the system	-	A line representing a sequence of any symbols (letters, digits, service characters except < | > symbols), not case-sensitive. Number of symbols – from 0 to 255.
7	**Patronymic** field	Enter the value in the field	Sets the patronymic of the **User** object in the system	-	A line representing a sequence of any symbols (letters, digits, service characters except < | > symbols), not case-sensitive. Number of symbols – from 0 to 255.
8	**User photo** area	-	Displays a user's photo	-	-
The **Access control** tab					
9	**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.
10	**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.
11	**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.
12	**PIN** field	Enter the value in the field	PIN-code of the user's access card	-	Depends on the ACS in use

#	Parameter name	Method for setting the parameter value	Parameter description	Default value	Value range
13	**Permanent card** field	Enter the value in the field	User's access card number	-	Depends on the type of cards in use.
14	**Temporary card** field	Enter the value in the field	User's temporary access card number	-	Depends on the type of cards in use.
15	**Valid till** field	Enter the value in the field	Day inclusive, until which the user's access card is valid (which is indicated in the **Permanent card** field). The card will expire on the next day at 00:00 from the specified date	-	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.					
16	**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.
17	**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.					
18	**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.
19	**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 *ACFA Intellect* (on the Programming tab or via the VMS)
20	**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.
21	**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.

8.4 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 except < | > 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. *Note. This function should be supported by hardware.*	False	**True** – access point is armed after presenting access card by user **False** – access point is not armed after presenting access card by user

#	Parameter name	Method for setting the parameter value	Parameter description	Default value	Value range
7	**Disarm** checkbox	Is set in a checkbox	Enables disarming of access point after presenting access card by user. *Note. This function should be supported by hardware.*	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. *Note. This function should be supported by hardware.* *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.*	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.

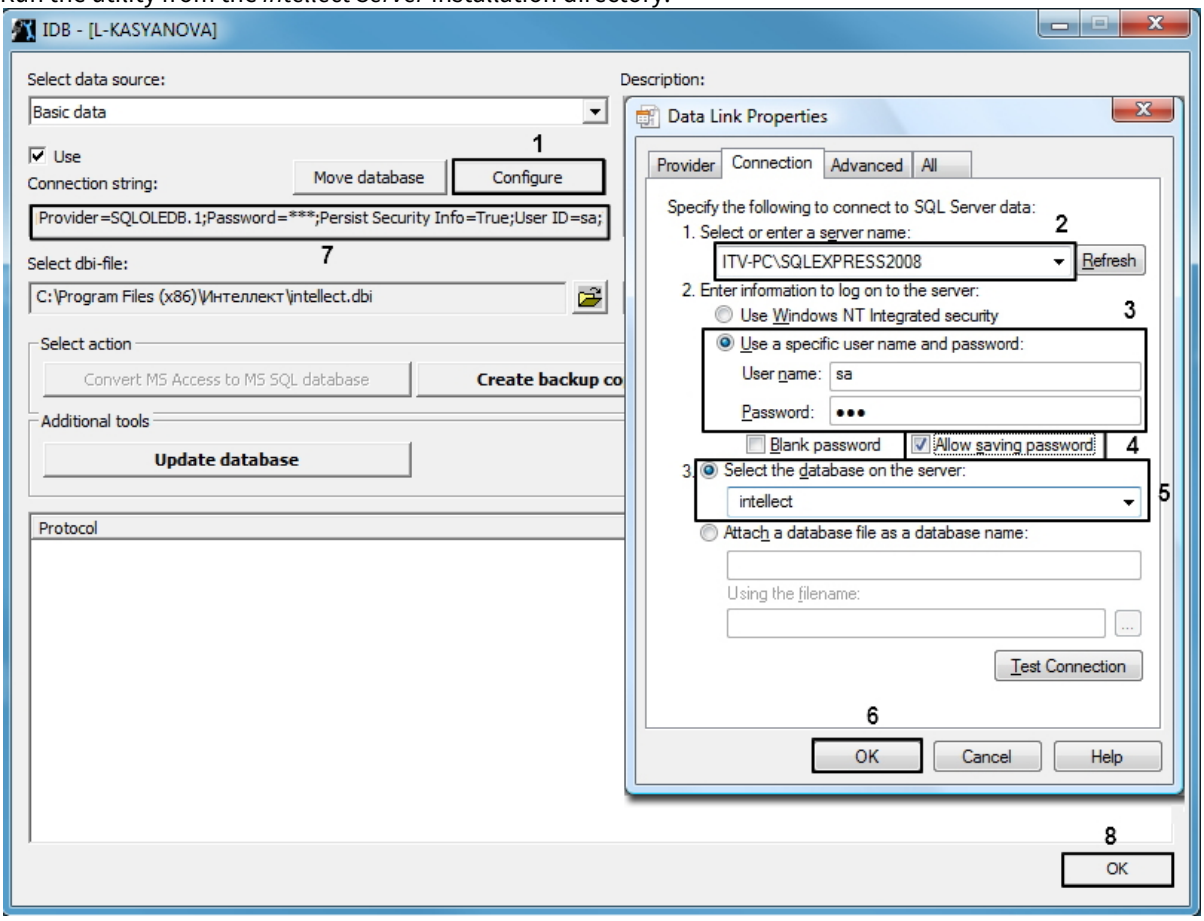
9 Appendix 3. Settings for proper operation of the Access Manager module in a distributed architecture

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.

10 Appendix 4. Creating additional fields for the User object

You can create additional fields for the User object which are used in the Access Manager Module (see Working with users in the Access Manager software module).

Additional fields are created using the text editor that allows you to view and edit the ASCII text encoding.

To create additional fields for the User object, do the following:

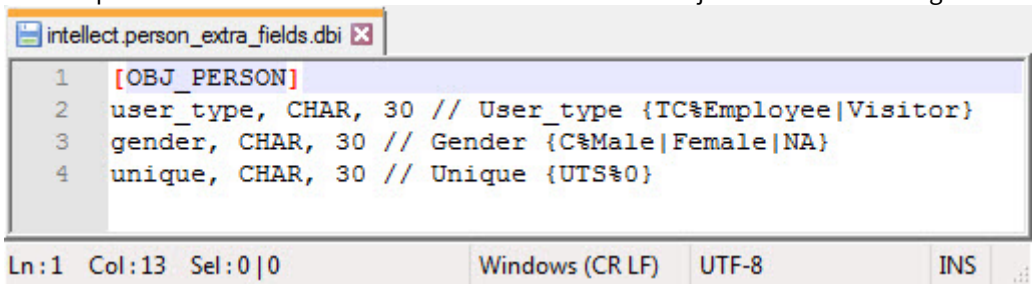
1. In the Intellect installation directory, for example **C:\Program Files (x86)\Intellect** create a .dbi text document, for example **intellect.person_extra_fields.dbi**.
2. Open the created .dbi file in the text editor.

   > **Attention!**
   >
   > Before you enter any data, make sure that the UTF-8 text encoding is selected. Otherwise, when adding additional fields to the database, the text will be recognized incorrectly.

3. In the first line of the text document, enter **[OBJ_PERSON]**.
4. In subsequent lines, specify the additional fields parameters, namely:
   a. Enter the **field name** that will be saved in the database, the **field data type**, and the **field size** separated by a comma.
   b. Specify the field description after a double slash "**//**": enter the field name that will be displayed in the **Access Manager** interface window, and set the field behavior pattern. In general, the description of the field is as follows: "Type {TC% value1 | valueN}", where:

Name	Description
Type	The field name displayed in the Access Manager interface window.
{	Beginning of the field behavior pattern
T	The field will be editable, the entered value will be saved.
C	The field will be a drop-down list.
%	The predefined field value names are listed after the % sign. *Note. If you specify %EMPTY, there will be no predefined values.*
value1, valueN	The predefined field value names
|	Separation of the predefined field values
UTS%0	The field will be editable with a unique value. If the user tries to enter a value which is already specified by other User, the warning will be displayed saying that the user with ID = "" already specified this value
}	End of the field behavior pattern

An example of the .dbi file with additional fields for the User object is shown in the figure below:



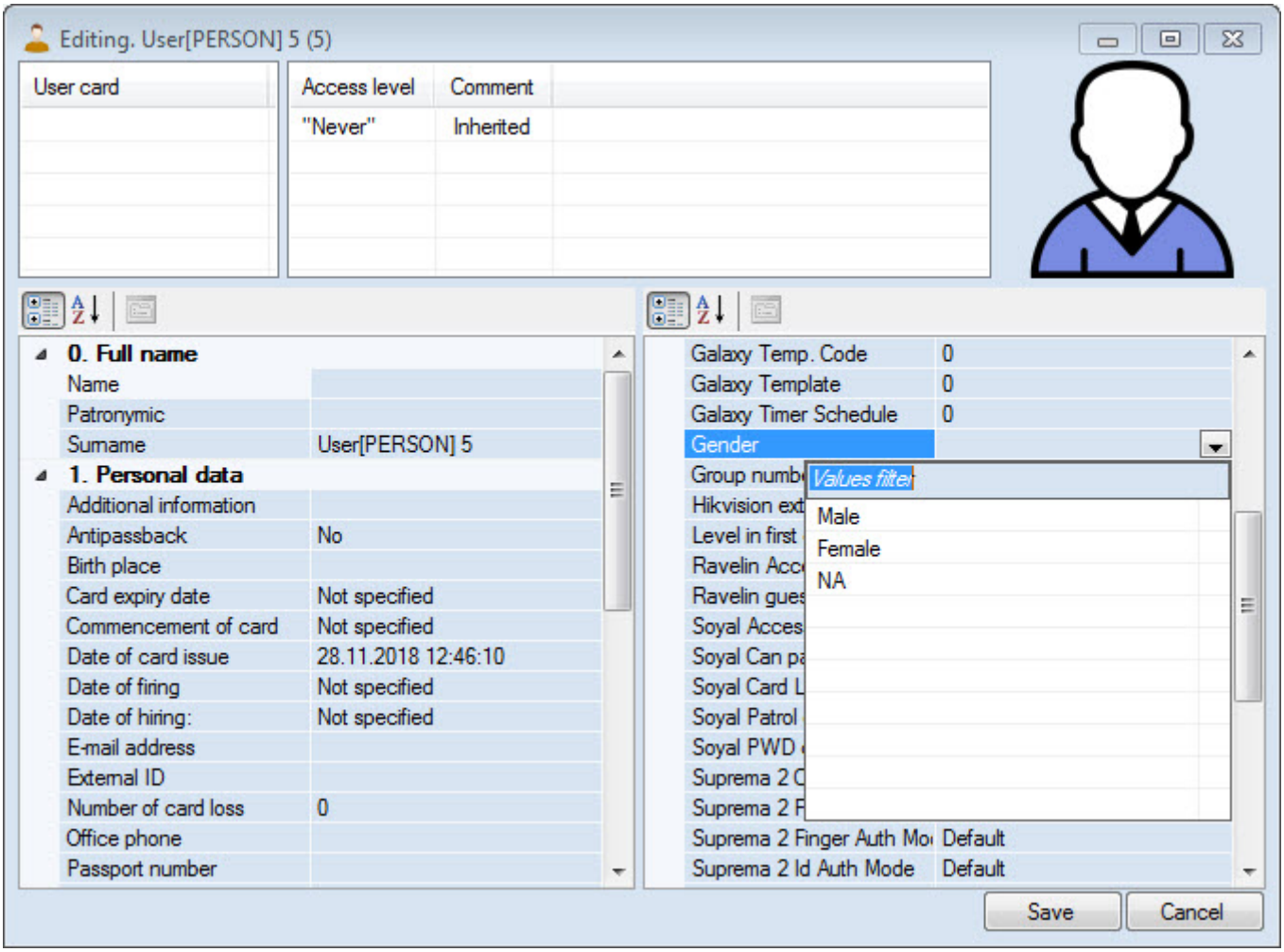
5. After you create the additional fields, save the changes.

   > **Attention!**

> After you save the .dbi file, it is necessary to update the main database. To do this, use the idb.exe utility (see The idb.exe utility for converting databases, selecting database templates and making backup copies of databases).

As a result, the created fields will be available on the settings panel of the **Access Manager** object on the **Additional fields** tab (see Configuring Main department type).

Depending on the visibility and accessibility for editing the fields, as well as the specified category, the corresponding additional fields will be displayed in the **Access Manager** interface window.



Creating additional fields for the User object is complete.

11 Appendix 5. Creating a single photograph database

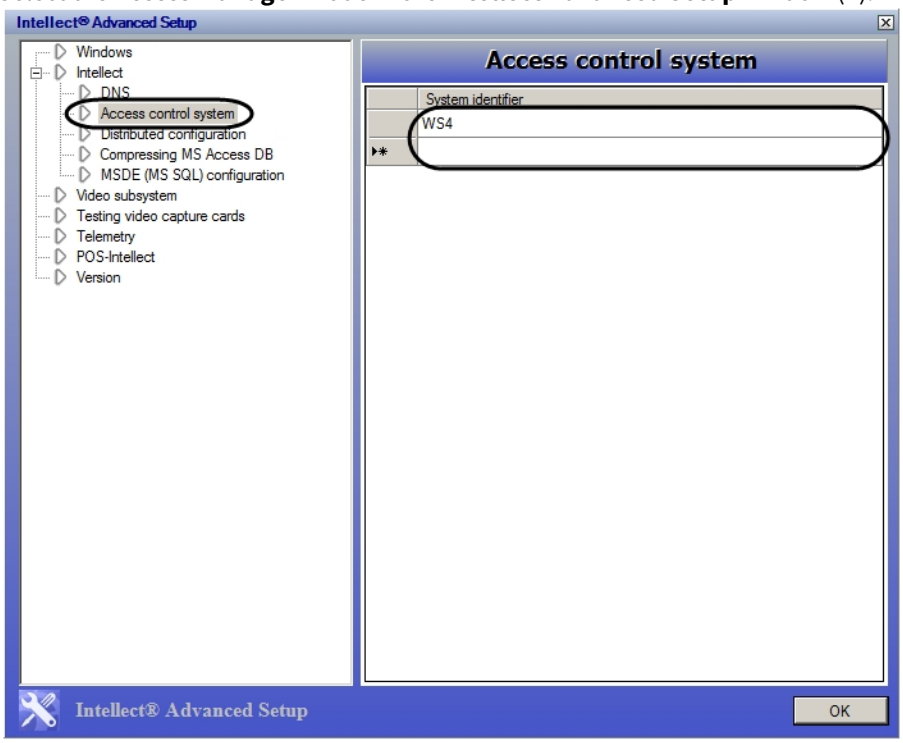
The *ACFA Intellect* Software System supports storing user photographs on several computers.

The *ACFA Intellect* Software System's advanced settings utility tweaki.exe is used to create a single photograph database. There are two ways to launch the tweaki.exe utility:

1. From the Windows **Start** menu: **Start** ->**All Programs** ->**Intellect** ->**Utilities** ->**Advanced settings**.
2. From the **Tools** folder of the *ACFA Intellect* Software System's installation directory: <Intellect installation directory>\Tools\tweaki.exe .

To configure the creation of a single photograph database, do the following:

1. Select the **Access Manager** mode in the **Intellect Advanced Setup** window (**1**).



2. In the **System identifier** column, enter the names of the Servers/RAWs that will store the photographs assigned by a user using the *Access Manager* module (**2**).

> **Note:**
>
> The specified Servers/RAWs must be connected to the *Intellect* Server to which photos from *Access Manager* are added. Detailed information about configuring server connections is given in Intellect Software System: Administrator's Guide. However, the *Access Manager* module does not have to be installed on the specified computers. Do not add Clients to the list.

> **Note:**
>
> Only photographs that have been newly added using the *Access Manager* module will be placed on the specified computers. Photographs added to the system before the configuration of the creation of a single photograph database will not be distributed to these computers.

> **Note:**
>
> Photographs will be stored on both the computers specified using the tweaki.exe utility as well as the computer from which photographs are added. Added photographs are stored in: <Intellect installation directory>\Bmp\Person.

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

This completes the process of configuring the creation of a single photograph database.

12 Appendix 6. Face synchronization module

12.1 General information about the Face synchronization module and its licensing

The Face synchronization module is designed to automatically synchronize the users of the *Access Manager* module who have photos with the *FACE Intellect* reference face database (see Face Intellect, Working with the reference face database).

The Face synchronization module allows you to do the following:

1. Automatically create a face in the reference face database when you assign a photograph to the user in the *Access Manager* module.
2. Automatically change the face image in the reference face database when you change a user's photo in the *Access Manager* module.
3. Automatically delete a face from the reference face database when you delete a user's photo in the *Access Manager* module.
4. Automatically delete a user in the *Access Manager* module when you delete a face from the reference face database.

Attention!

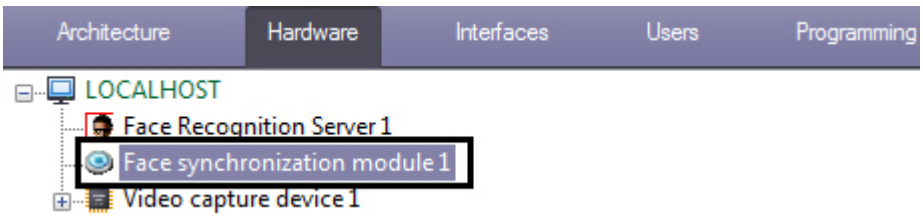
In case you create users in the *Face-Intellect* database using the **Face recognition and search** interface object (see Adding images to the reference face database), the correct synchronization of faces is not guaranteed.

Protection

The Face synchronization module is provided free of charge upon purchase of the *Access Manager*/*Visitor Management System* module.

12.2 Activation of the Face synchronization module

To activate the Face synchronization module, create the **Face synchronization module** object based on the **Computer** object on the **Hardware** tab of the **System settings** dialog window.

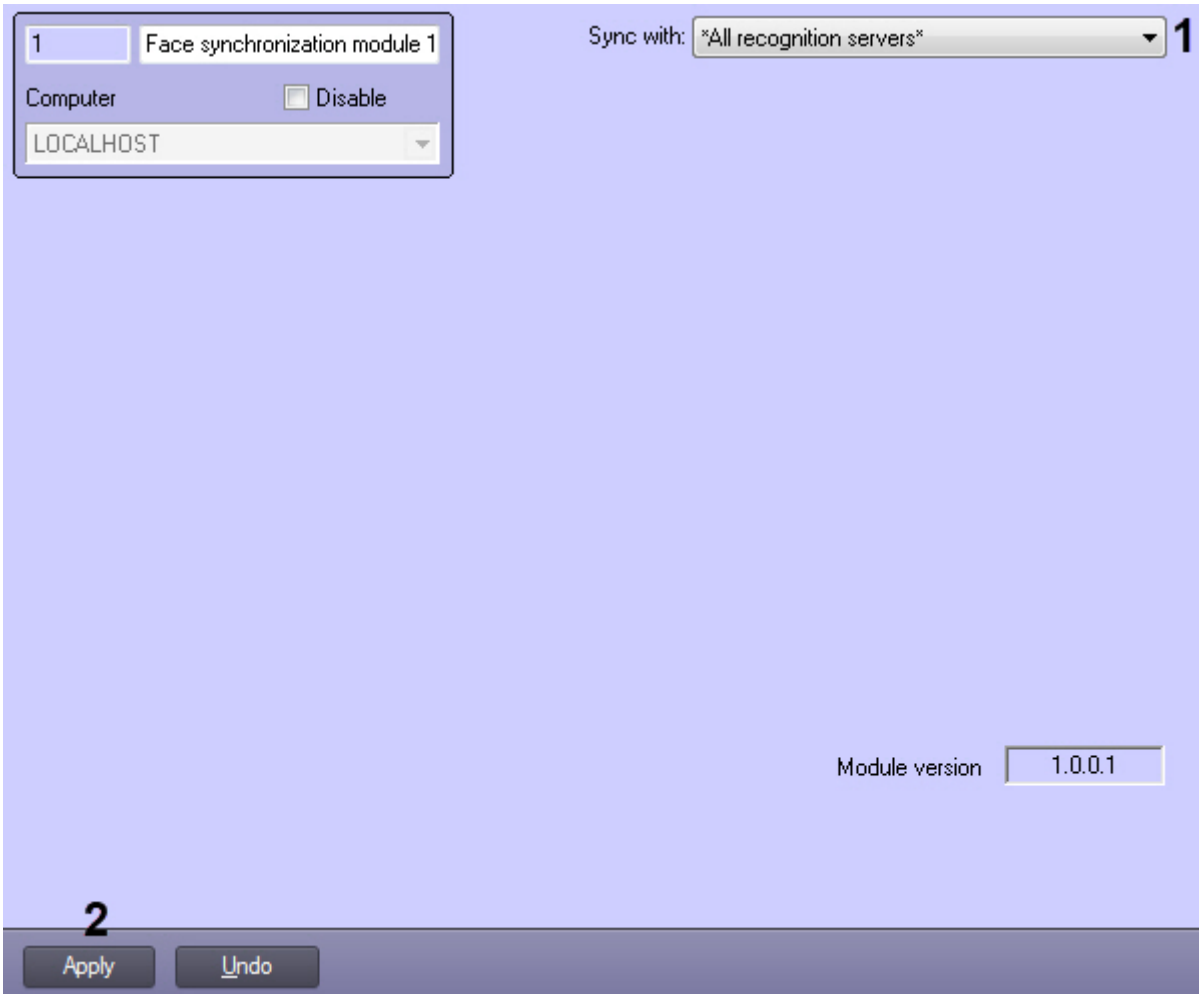


12.3 Configuring the Face synchronization module

On the page:

12.3.1 Selecting the Face Recognition Servers for synchronization

The selection of Face Recognition Servers with which faces will be automatically synchronized is carried on the **Face synchronization module** object settings panel.



In the **Synch with** drop-down list (**1**), select the required Face Recognition Server. If you select the value **All recognition servers** will be synchronized with all Face Recognition Servers in the distributed system.

> **Note**
>
> In the **Module version** field is displayed the current version of the Face synchronization module.

12.3.2 Selecting the Face Recognition Servers in the Access Manager module

To receive events about the impossibility of adding a photo to the Face Recognition Server due to its poor quality, you must specify the corresponding Face Recognition Servers as control readers on the *Access Manager* module settings panel (see Configuring control readers in the Access Manager).

13 Appendix 7. Additional features of Access Manager module

13.1 Event generation when a photo is assigned to a user

It is possible to generate an event with the captured frame image when a photo is assigned to a user from a camera (see Assigning a photograph from a video camera).

> **Attention!**
>
> The **account_manager.run.config** file should be configured on the same computer on which you are planning to work with the *Access Manager* module.
> After you make changes to the **account_manager.run.config** file, it is necessary to restart *ACFA-Intellect*.

1. Go to the *<Intellect* installation directory>\Modules\ path.
2. Open the **account_manager.run.config** file for editing.
3. Add the following lines to the **applicationSettings** group:

```
<setting name="NotifyInitialPhoto" serializeAs="String">
    <value>True</value>
</setting>
```

account_manager.run.config

```
 8      <applicationSettings>
 9          <RunModule.account_manager_run.Properties.Settings>
10              <setting name="CommonBackground" serializeAs="String">
11                  <value>206, 206, 255</value>
12              </setting>
13              <setting name="ControlsBackground" serializeAs="String">
14                  <value>244, 247, 252</value>
15              </setting>
16              <setting name="FormsBackground" serializeAs="String">
17                  <value>215, 228, 242</value>
18              </setting>
19              <setting name="SettingsBackground" serializeAs="String">
20                  <value>AliceBlue</value>
21              </setting>
22              <setting name="ScanifyAPIEnabled" serializeAs="String">
23                  <value>False</value>
24              </setting>
25              <setting name="AutoCropFrame" serializeAs="String">
26                  <value />
27              </setting>
28              <setting name="NotifyInitialPhoto" serializeAs="String">
29                  <value>True</value>
30              </setting>
31          </RunModule.account_manager_run.Properties.Settings>
32      </applicationSettings>
33  </configuration>
```

4. Save the changes to the **account_manager.run.config** file.

As a result, when a photo is assigned to a user from a camera, an event will be generated:

```
PERSON|id|NOTIFY_PHOTO|core_global<0>,base64<>
```

where id is the identifier of the user to whom the photo is assigned, and base64 is the jpeg image in Base64 format.