Guide for configuring and working with the Access Manager module

ACFA PSIM 1.10

Last update 24/04/2026

Table of Contents

1 List of used terms and abbreviations

User is 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, in addition to the data of company users. Configuration and operation of the module with different types of users are the same. When it comes to configuring and working with features specific to individual categories, this is specified separately.

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

APB (*Antipassback*) is a feature of the system that enables protection against ID reuse in one direction..

Holiday is a non-working day. Specifying a list of holidays in the system allows you to exclude certain days from time zones.

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

Access level is a right of a user to access through an access point (points) depending on the time zone. Access level also determines the rules of arming and disarming an access point. Access level can be common for all users from a department and separate for one, several, or all users.

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

2 Introduction into the Guide for configuring and working with the Access Manager integration module

On the page:

2.1 Purpose of the document

The *Guide for configuring and working with the Access Manager integration module* is a reference manual for configuration technicians and operators of the *Access Manager* module. This module is a part of *ACFA PSIM*.

This Guide has the following materials:

1. General information about the *Access Manager* module.
2. Configuration of the *Access Manager* module.
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 *ACFA PSIM* and allows you to perform the following actions:

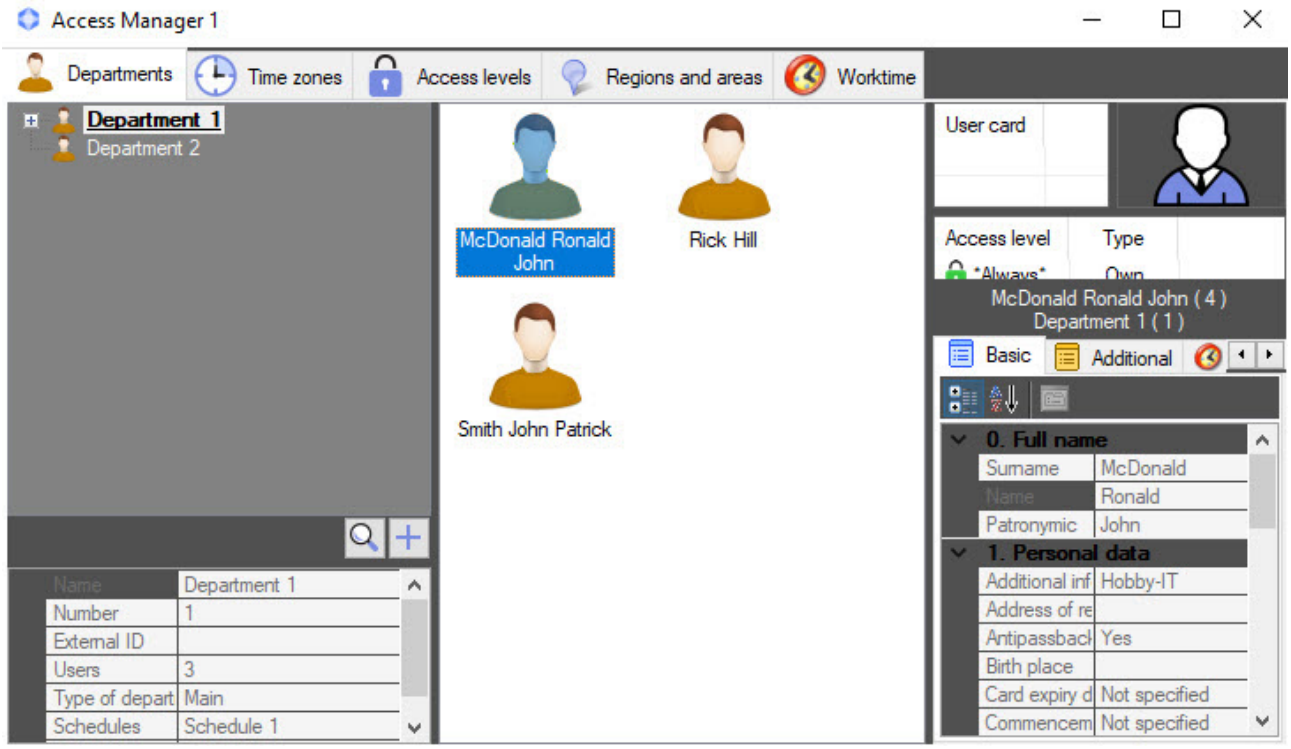
1. Configure the access mode of employees and visitors to the facility with automated access control systems.
2. Configure the movement rules of employees and visitors within the facility according to access levels.
3. Configure the operators' permissions in AM to create, edit, delete, and view departments.
4. Configure the operators' permissions in AM to create, edit, and delete access levels and users.
5. Create and configure access levels for each user and a entire department.
6. Create, configure, and delete accounts of users and departments.
7. Create, configure, and delete time zones and access levels.
8. Print electronic security passes for employees and visitors to the facility with automated access control systems.
9. Synchronize the users with added photos in *Access Manager* with the reference face database of *Face PSIM*.
10. View the personnel structure of the company for each departments and get information on each employee.
11. Generate schedules and work schemes with different periods and assign these individually to an employee or entire department.
12. Keep records of employees' exculpatory and overtime documents.
13. Calculate the total work hours for each employee of the department and present the results as a table.
14. Create a report on the total work hours by employees.

3 Licensing of the Access Manager module

One license for this module allows you to use any number of the **Access Manager** objects on any number of computers. The same license also allows you to create **Access Manager reports** and **Time and Attendance reports** objects on the basis of the **Web Report System** parent object (for more information, see WEB Report System PSIM. User Guide). In addition, the license allows the use of all integrated control readers (see Control Readers Settings Guide).

4 Interface of the Access Manager module

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



Note

- If the position of the window on the screen is fixed, the title bar of the **Access Manager** window isn't displayed—see the Configuring the position of the Access manager window on the screen.
- To add the **Worktime** tab to the **Access Manager** interface window, first you need to connect this subsystem: create the **Worktime support** object on the basis of the **Access Manager** object on the **Interfaces** tab of the **System settings** window (see Configuring the Worktime subsystem).

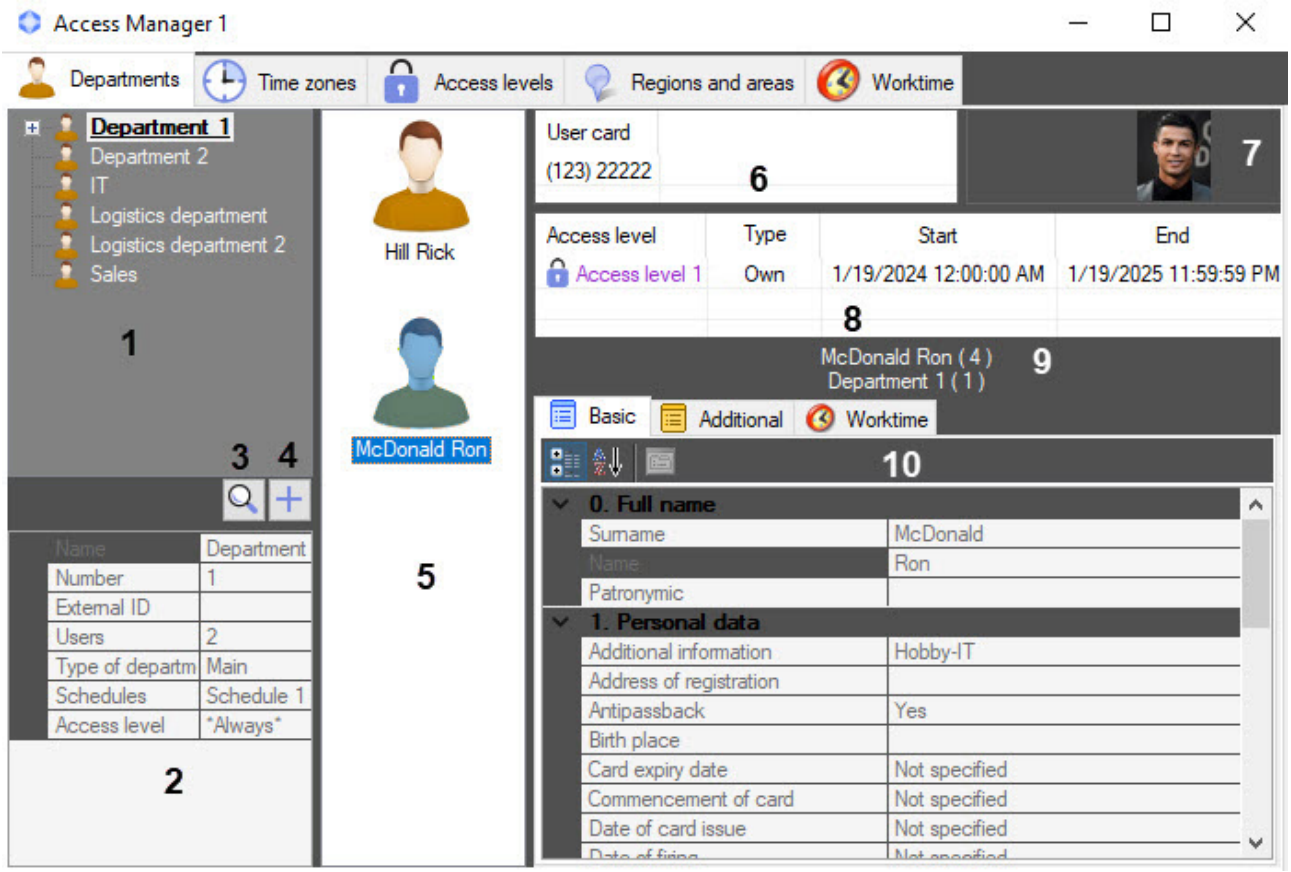
The **Access Manager** window contains the following tabs:

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

For the description of each tab, see the sections below.

4.1 The Departments tab

You can work with departments and users on the **Departments** tab.



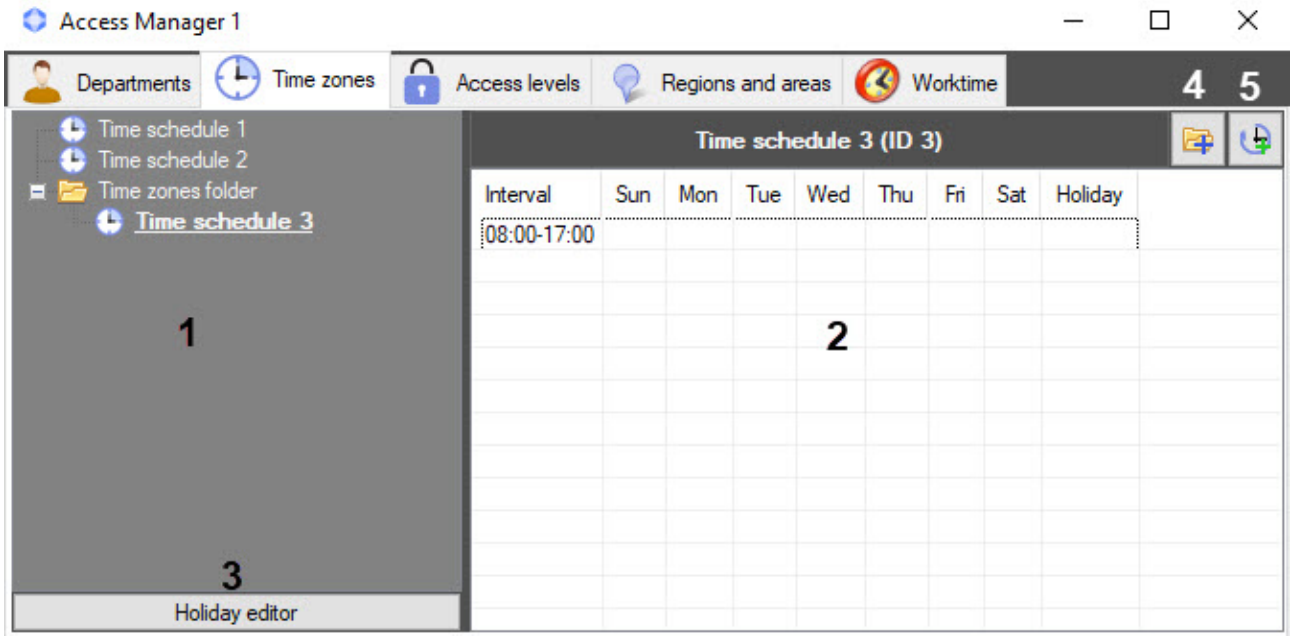
Description of the elements of the **Departments** tab is given in the table.

№	Element	Description
1	Departments tree	Hierarchy structure of created departments available for viewing depending on operator rights and/or settings of the **Access Manager** object (see the Rights to access departments in the Access Manager)
2	Department parameters	Parameters of a department: ID, External ID, Name, Number of users, Type of department, Access levels. For the information on how to set and edit department parameters, see Working with departments in the Access Manager software module
3	Search for department	Department search button (see Department search in the Access Manager software module)

4	Add department	Button to add a department (see Adding and deleting a department)
5	List of department users	List of users from the selected department
6	List of user access cards	List of access cards assigned to a user. See also Assigning an access card to a user. This list can be hidden or unavailable depending on the **Access card** settings in operator rights and/or on the **Access manager** object (see Configuring fields displaying in user accounts)
7	User photo	Photo assigned to a user. See also Assigning a photograph to a user
8	List of user access levels	List of access levels assigned to a user. Temporary access levels are highlighted in color, and the date and time of validity of the temporary access level are 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 isn't valid at the moment. See also Assigning access levels to a user. This list can be hidden or unavailable depending on the **Access levels** settings in operator rights and/or on the **Access Manager** object (see Configuring fields displaying in user accounts)
9	User's full name and their department	User surname, name, patronymic, their ID (in brackets), and the department they belong to
10	User parameters	User information. For the description of fields, see Specifying user parameters

4.2 The Time zones tab

You can work with time zones and holidays on the **Time zones** tab.

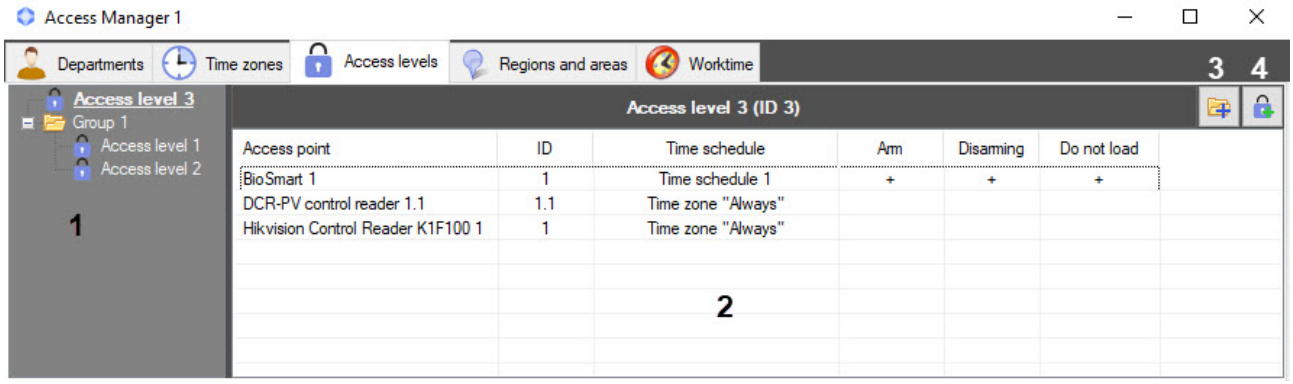


Description of the elements of the **Time zones** tab is given in the table.

№	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 by default. See also Selecting a view of displaying objects list in the Access Manager
2	Time zone intervals	List of intervals included in the time zone
3	The **Holiday editor** button	Button opens the **Edit holiday** window (see Editing holidays)
4	Button to create a folder in the root	Button opens a window for creating a folder in the root (see Managing a list of time zones)
5	Button to create a time zone in the root	Button opens a window for creating a time zone in the root (see Creating a time zone in the Access Manager software module)

4.3 The Access levels tab

You can work with the user access levels on the **Access levels** tab.

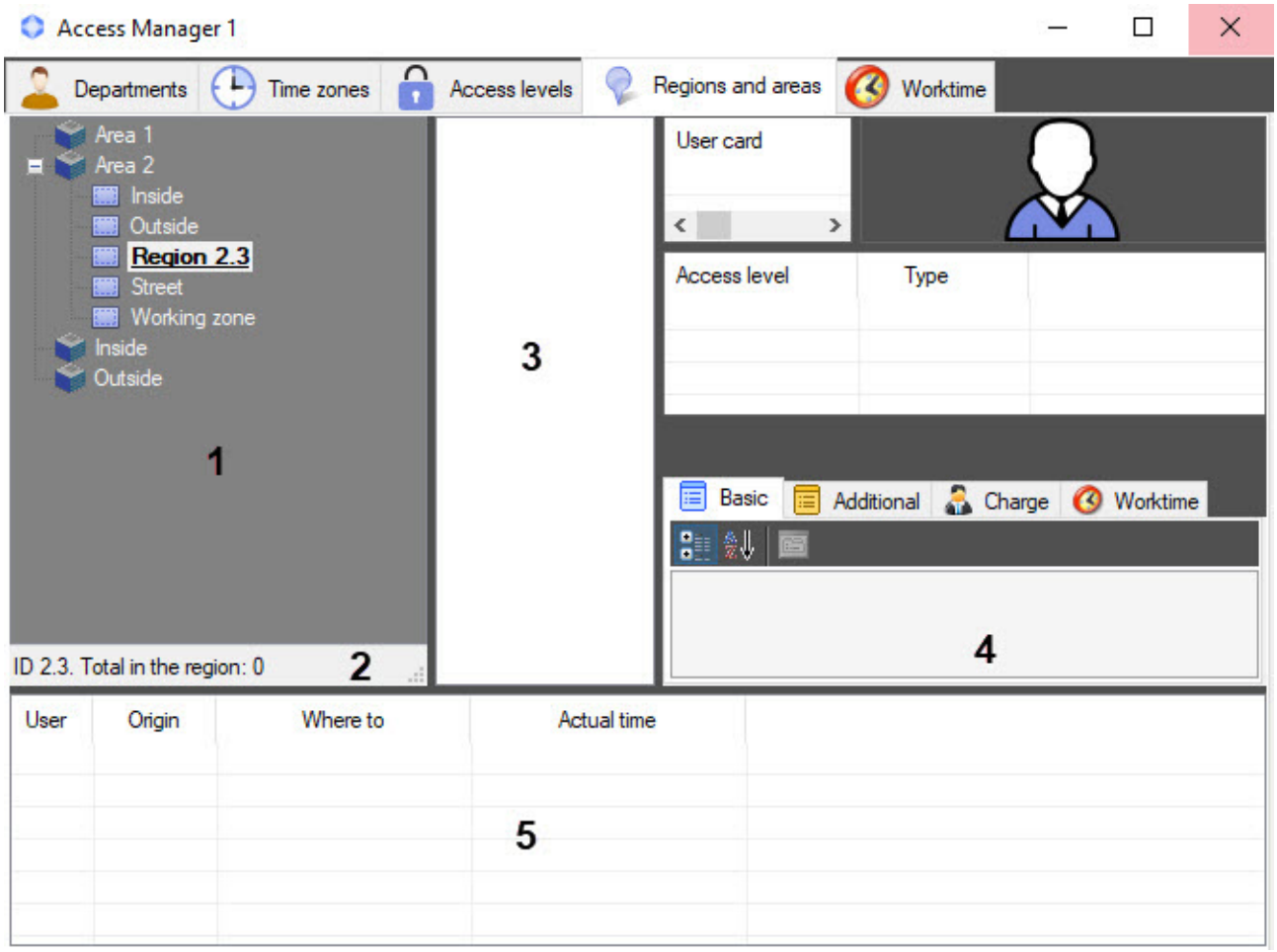


Description of the elements of the **Access levels** tab is given in the table.

№	Elements	Description
1	List of access levels	List of access levels created in the system. The **List** view is used by default. See also Selecting a view of displaying objects list in the Access Manager
2	Access level parameters	Description of the 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 a user. The **Table** view is used by default
3	Button to create a folder in the root	Button opens a window for creating a folder in the root (see Managing a list of time zones)
4	Button to create a time zone in the root	Button opens a window for creating a time zone in the root (see Creating a time zone in the Access Manager software module)

4.4 The Regions and areas tab

The **Regions and areas** tab allows you to perform emergency monitoring.

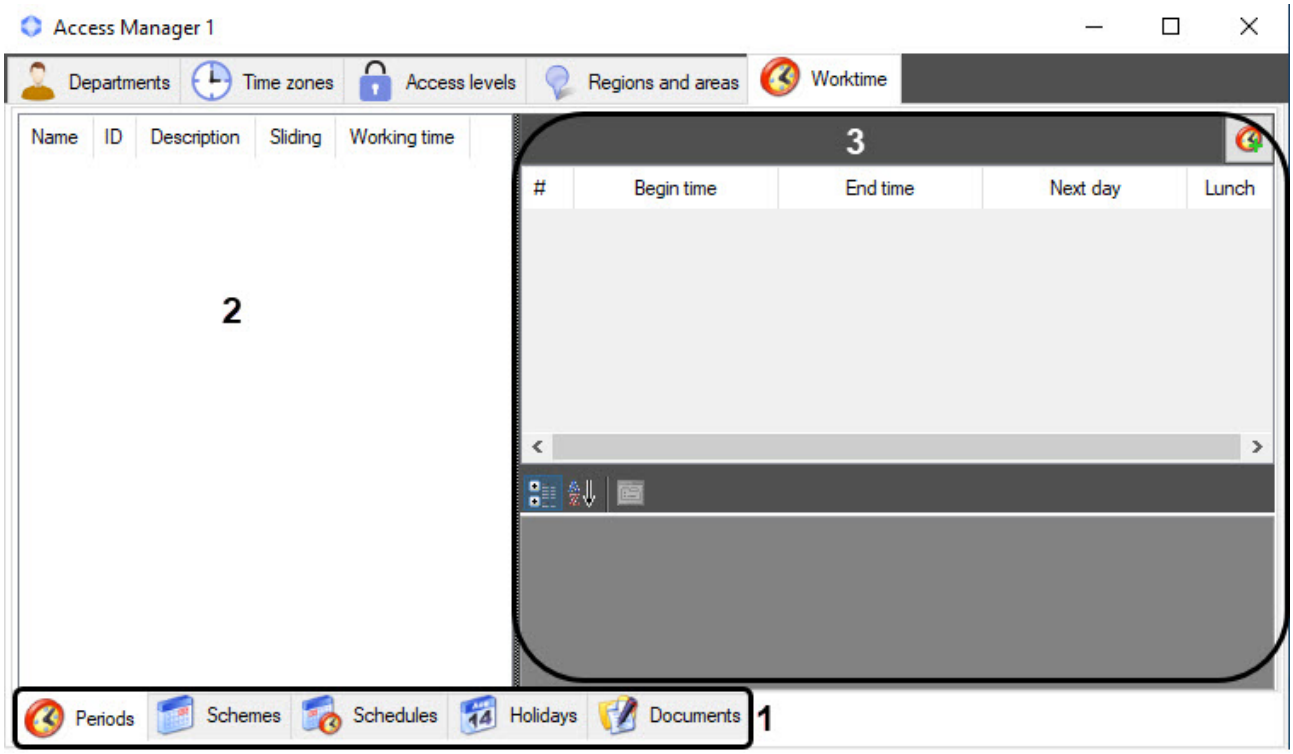


Description of the elements of the **Regions and areas** tab is given in the table.

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 selected in the tree and the current number of people in it
3	The list of users in the region	List of users who are currently located in the region
4	User parameters	See The Departments tab
5	Access log	Information on users' access in real time

4.5 The Worktime tab

On the **Worktime** tab, you can view the information about the personnel structure of an organization by department and by each employee, create and assign work schedules and work schemes with different work periods to employees and departments, keep record of employees' exculpatory and overtime documents, calculate the total working time of each employee and present the results as a table, generate reports on the total working time of employees.



The navigation bar (**1**) is used to switch between the menu items of the *Time and Attendance* subsystem.

The information field (**2**) displays information on the objects existing in the system of the *Time and Attendance* subsystem.

The properties panel (**3**) displays the parameters of the objects from the area (**2**).

For more information about the interface elements of the **Worktime** tab, see The main elements of the Worktime tab.

5 Configuration of the Access Manager module

5.1 Procedure of configuring the Access Manager module

You can configure the *Access Manager* module on the settings panel of the **Access manager** object that is created on the basis of the **Display** object on the **Interfaces** tab of the **System settings** window, and on the settings panels of the **Operators' permissions in AM** and **Type of department** child objects.

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

1. Rights for configuring and accessing objects in Access Manager.
2. Configuring access cards.
3. Configuring control readers in the Access Manager.
4. Configuring the prohibition of duplicates of new user parameters in the Access Manager.
5. Configuring the interaction with the Face PSIM Face Recognition Server.
6. Configuring fields displaying in user accounts.
7. Configuring the Worktime subsystem.
8. Configuring the ABBYY PassportReader SDK module.

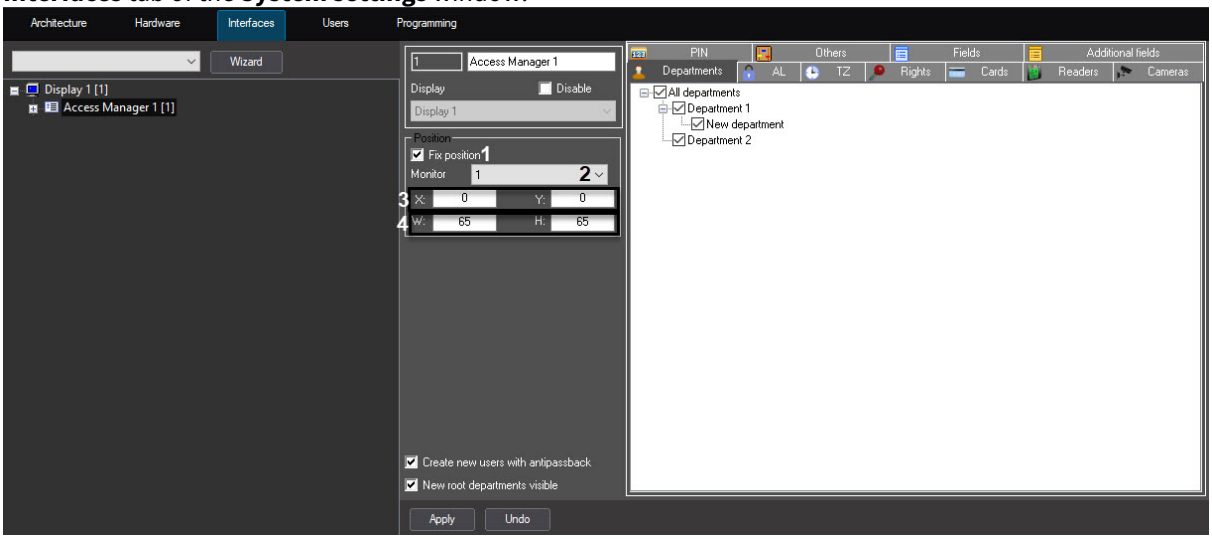
5.2 Configuring the position of the Access manager window on the screen

By default, the position of the **Access manager** window isn't fixed, and you can move it on the screen. When configuring 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 isn't displayed, which increases the display 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 on the basis of the **Display** object on the **Interfaces** tab of the **System settings** window.



2. Set the **Fix position** checkbox (**1**).

3. From the **Monitor** drop-down list, select a computer monitor on which the **Access Manager** window will be displayed (**2**).
4. Specify the coordinates of the top left corner of the **Access Manager** window in the **X** and **Y** fields as percentage of width and height of the screen correspondingly (**3**).
5. Specify the 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.

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

5.3 Rights for configuring and accessing objects in Access Manager

5.3.1 General information about rights to configure and access objects in Access Manager

Specifying the rights to configure and access objects allows limiting the actions available for an operator of the *Access Manager* module when you configure departments, users, access levels, time zones, areas, and regions. Rights to configure objects in *Access Manager* correspond to the user rights in *ACFA PSIM*.

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

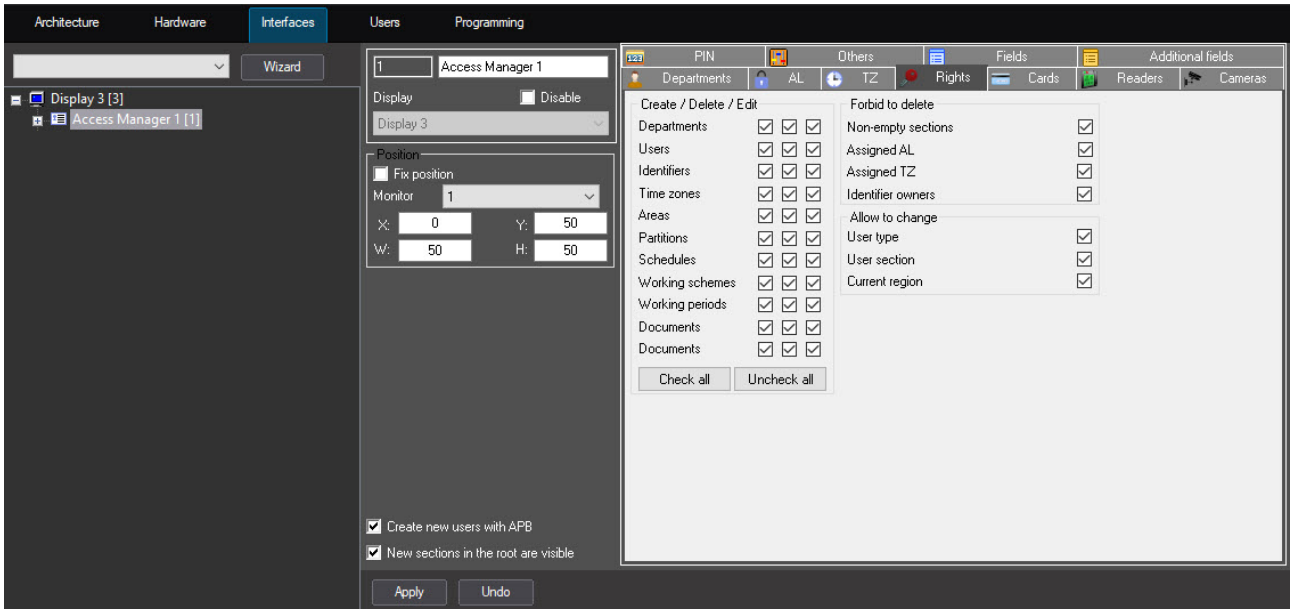
1. Create.
2. Edit.
3. Delete.

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

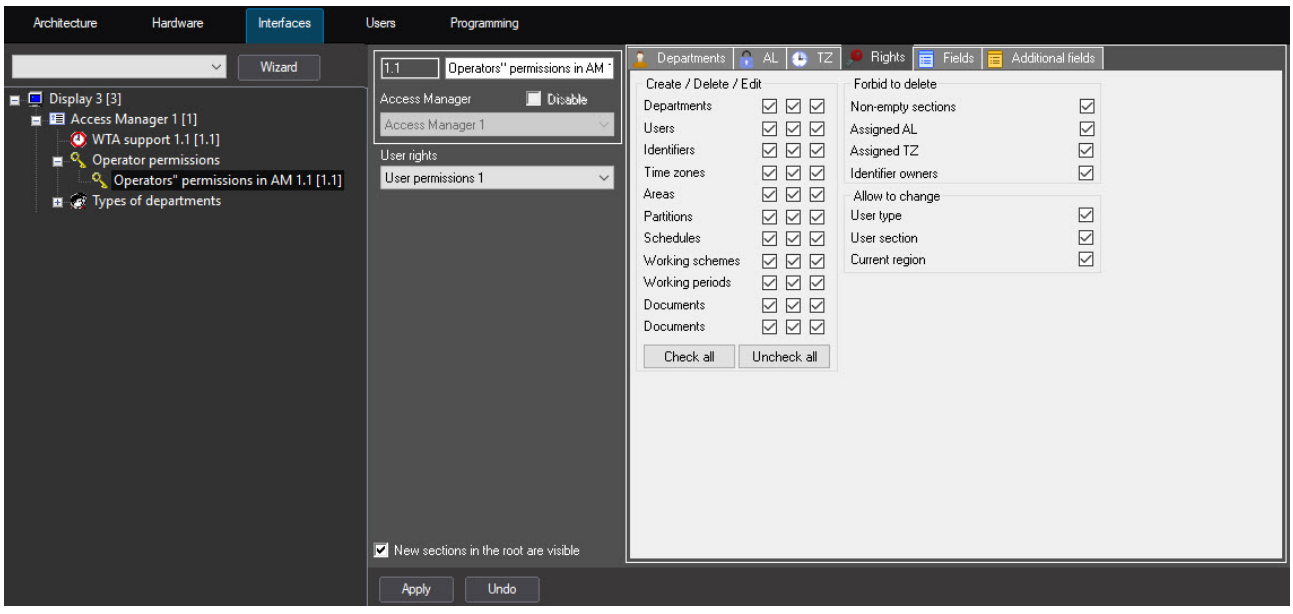
The *Access Manager* software module allows setting the common and individual rights to configure objects. By default, all the above operations are prohibited in the *Access Manager* module.

The common rights to configure objects have a priority over the individual rights. It means that if some operation is prohibited by the common rights to configure objects, then this operation is unavailable for all operators, even if it is permitted by some individual rights.

You can specify the common rights to configure objects on the **Rights** tab on the settings panel of the **Access Manager** object that is created on the basis of the **Display** object on the **Interfaces** tab of the **System settings** window.



You can specify the individual rights to configure objects on the **Rights** tab on the settings panel of the **Operators" permissions in AM"** object that is created on the basis of the **Access Manager** object.



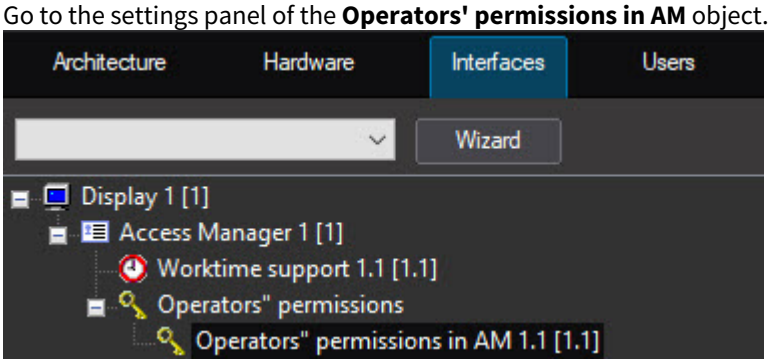
5.3.2 Configuring the correspondence between operator's permissions in the Access Manager and in Axxon PSIM

Individual rights to configure objects in the *Access Manager* correspond to user rights in *ACFA PSIM*. It means that one **Operators' permissions in AM** object can correspond to one **User permissions** object and vice versa.

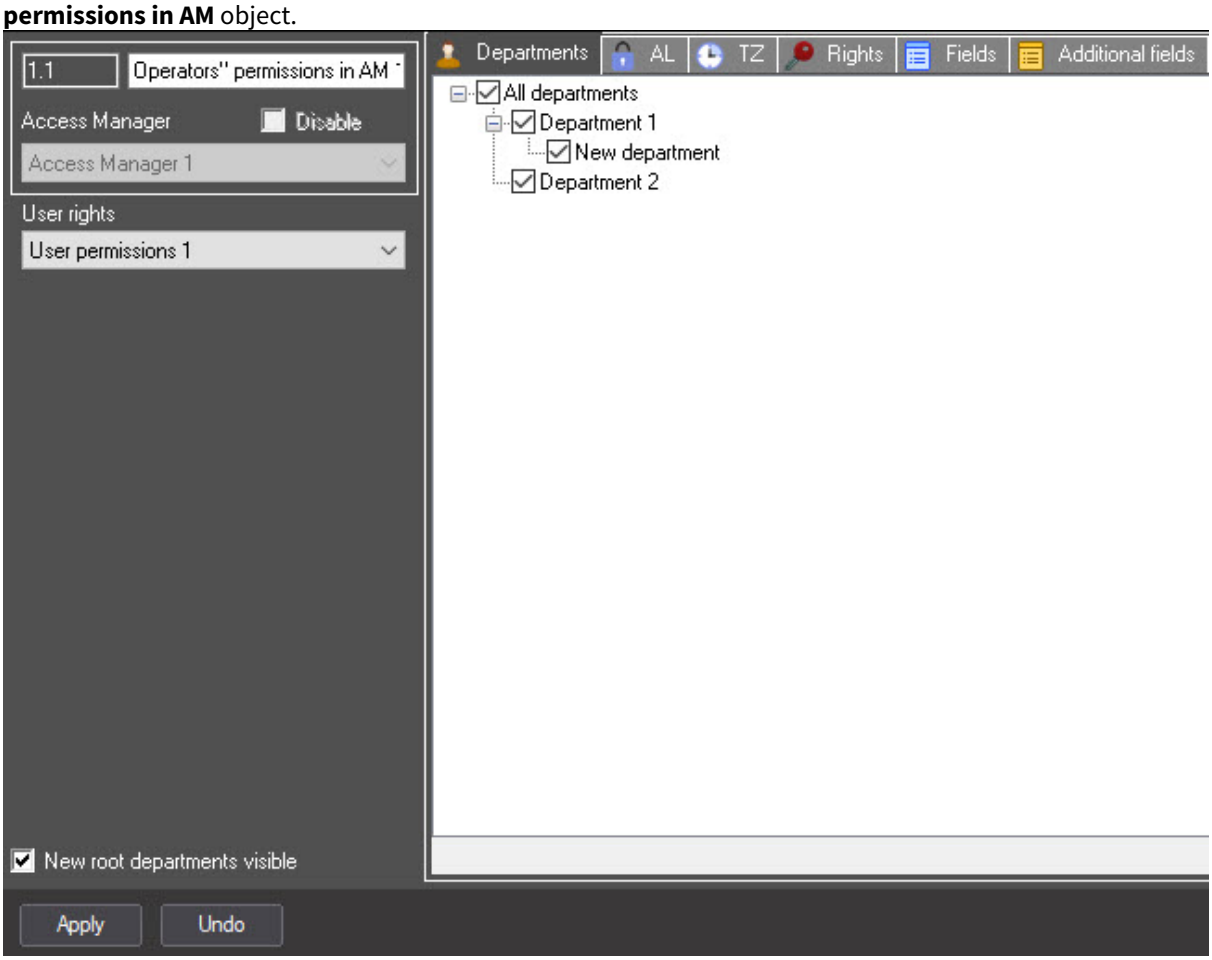
> **Note**
>
> If similar operator rights in the *Access Manager* must correspond to user rights in *ACFA PSIM*, use the **Save** function from the context menu of the interface object (see The Save function)

To specify correspondence of operator's rights in the *Access Manager* and in *ACFA PSIM*, 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 that must match the **Operators' permissions in AM** object.



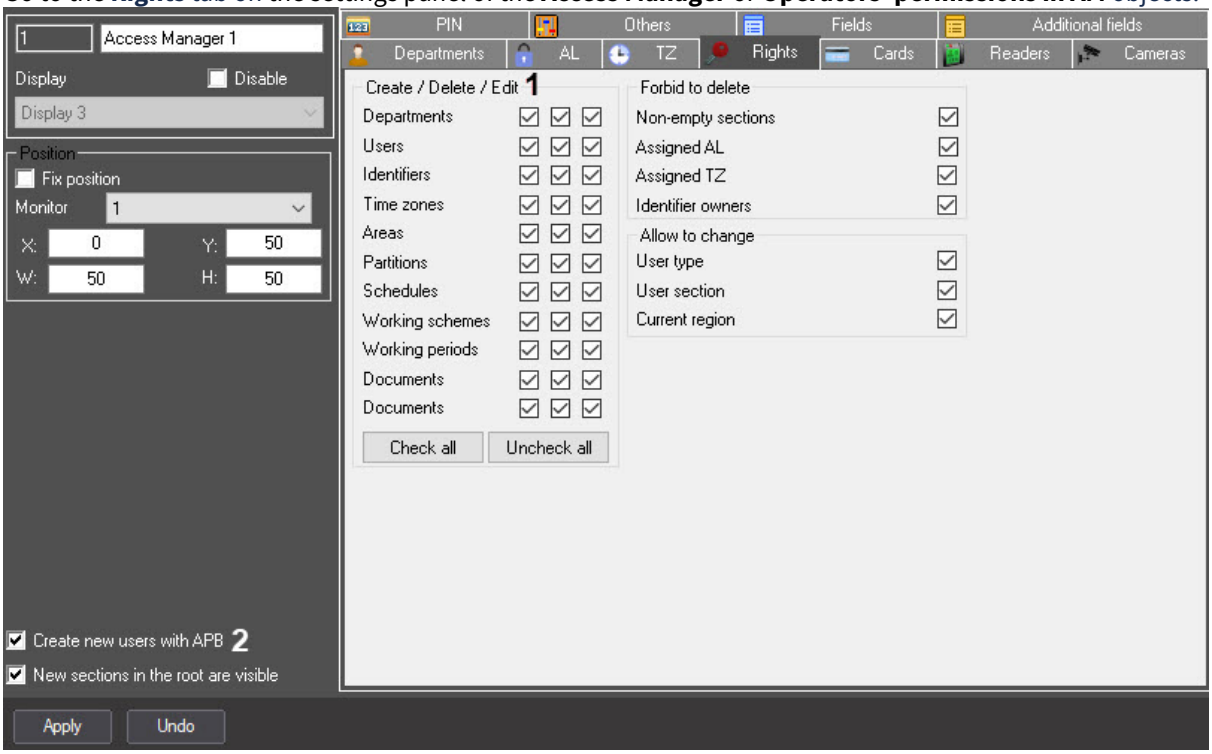
> **Note**
>
> The **User permissions** objects are created on the **Users** tab of the **System settings** dialog window. Creation and configuration of these objects is described in Rights administration.

3. Click the **Apply** button.

5.3.3 Configuring the rights to manage objects in Access Manager

To configure the common or individual rights for managing objects, do the following:

1. Go to the **Rights** tab on the settings panel of the **Access Manager** or **Operators' permissions in AM** objects.



2. In the **Create/Delete/Edit** group (**1**) for the **Departments**, **Users**, **Identifiers**, **Time zones**, **Areas**, **Partitions**, **Schedules**, **Working schemes**, **Working periods**, **Documents**, **Documents** objects:
   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 to set all the checkboxes in the **Create/Delete/Edit** group (**1**).
4. Click the **Uncheck all** button to clear all the checkboxes in the **Create/Delete/Edit** group (**1**).
5. If you want to allow operators to create users with the enabled antipassback option, set the **Create new users with APB** checkbox (**2**).

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

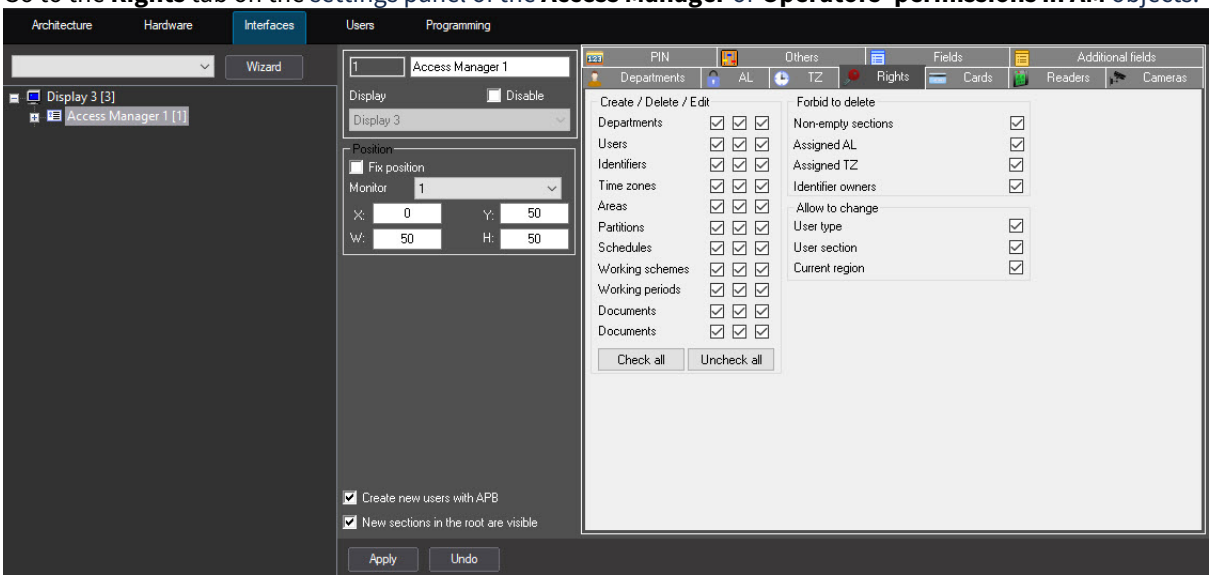
6. Click the **Apply** button to save the changes.

Configuring the rights to manage objects is complete.

5.3.4 Forbid to delete non-empty departments, assigned access levels, time zones, and identifier owners

To forbid deleting the non-empty departments, assigned access levels, time zones, and identifier owners, do the following:

1. Go to the **Rights** tab on the settings panel of the **Access Manager** or **Operators' permissions in AM** objects.



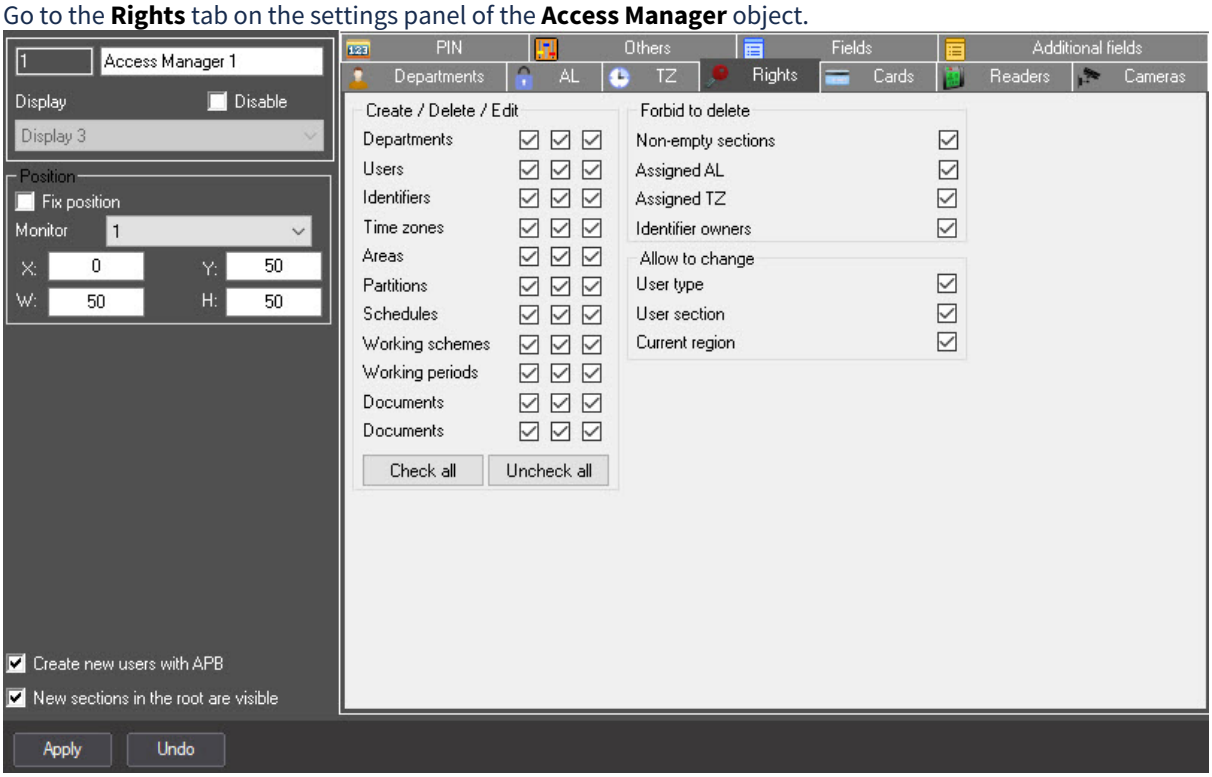
2. In the **Forbid to delete** group:
   a. Set the **Non-empty section** checkbox to forbid deleting the departments that contain users.
   b. Set the **Assigned AL** checkbox to forbid deleting the access levels assigned to any department or user.
   c. Set the **Assigned TZ** checkbox to forbid deleting the time zones assigned to any access level.
   d. Set the **Identifier owners** checkbox to forbid deleting the user data that has an identifier.
3. Click the **Apply** button to save the settings.

Forbidding the deletion of the non-empty departments, assigned access levels, time zones, and identifier owners is complete.

5.3.5 Configuring the rights to change user type, user department, and current region

To configure the rights to change the user type, user department, and current region, do the following:

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



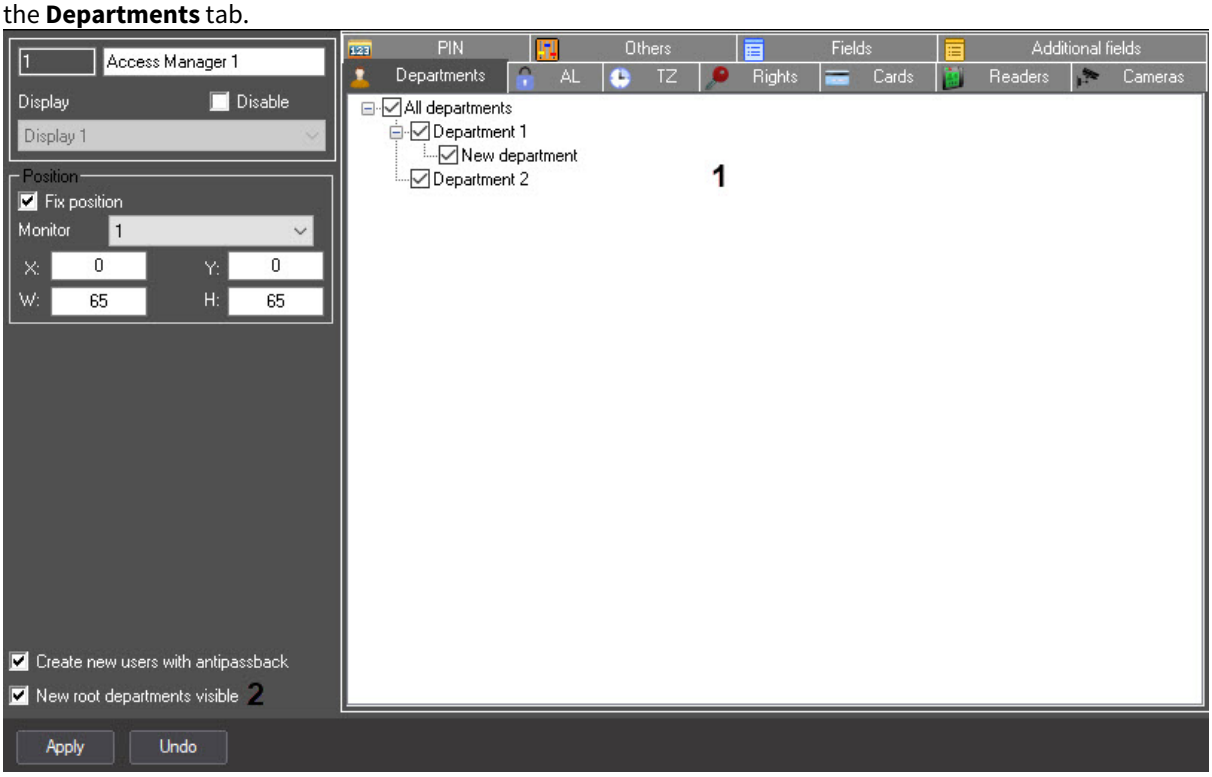
2. In the **Allow to change** group:
   a. Set the **User type** checkbox to allow changing the user type (see Changing a user type).
   b. Set the **User section** checkbox to allow transferring a user to another department (see Transferring a user to a different department in the Access Manager software module).
   c. Set the **Current region** checkbox to allow changing the current region of a user.
3. Click the **Apply** button to save the settings.

Configuring the rights to change the user type, user department, and current region is complete.

5.3.6 Rights to access departments in the Access Manager

To specify common or individual rights to access departments, do the following:

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



2. Set checkboxes next to the departments that must be available in the interface of the *Access Manager* module (**1**).
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 root departments visible** checkbox is set (**2**). If new departments and departments transferred to the root of hierarchy must be invisible in the *Access Manager* window, clear the checkbox.

> **Attention!**
>
> If the **New root departments visible** checkbox is clear, creation of new departments in the root of departments hierarchy is forbidden.

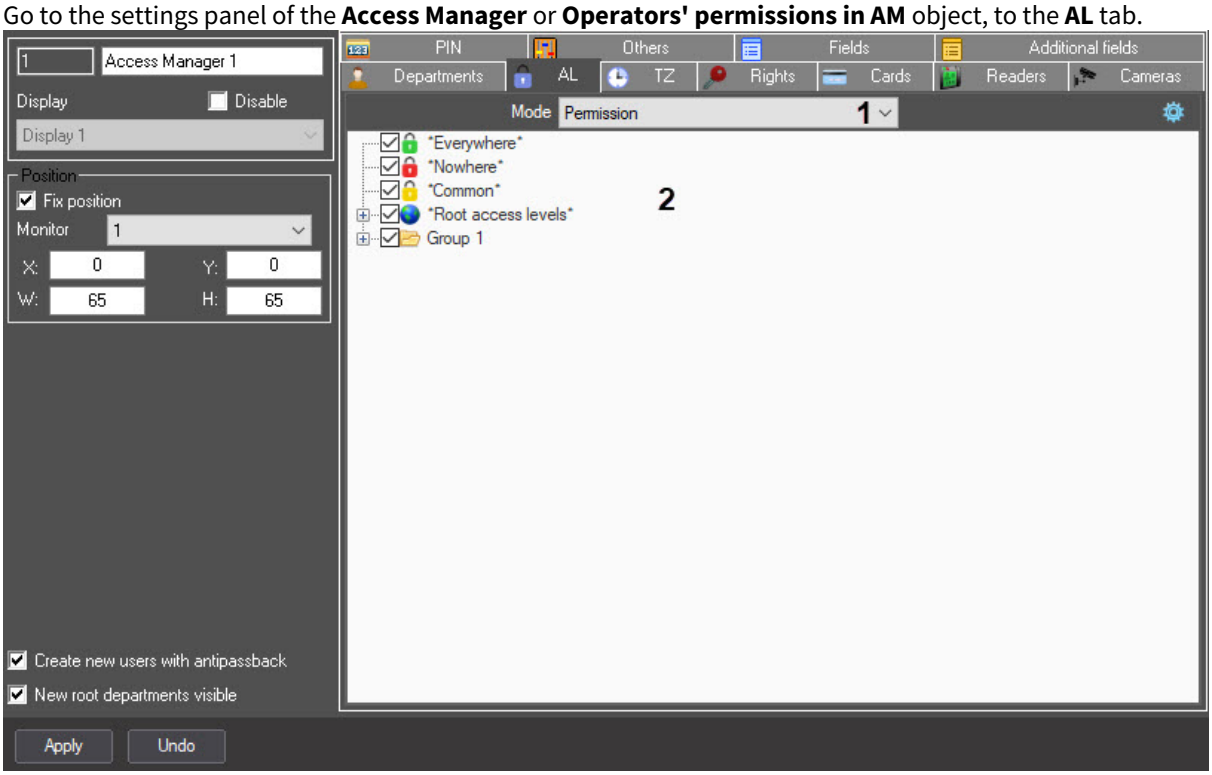
4. Click the **Apply** button.

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

5.3.7 Rights to access the access levels in the Access Manager

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

1. Go to the settings panel of the **Access Manager** or **Operators' permissions in AM** object, to the **AL** tab.



2. From the **Mode** drop-down list (**1**), select the required mode:
   - **Prohibition**—restrict the access;
   - **Permission**—allow the access.
3. Set the checkboxes (**2**) 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 *Axxon PSIM* or expand the list and set the checkboxes only next to the required access levels.

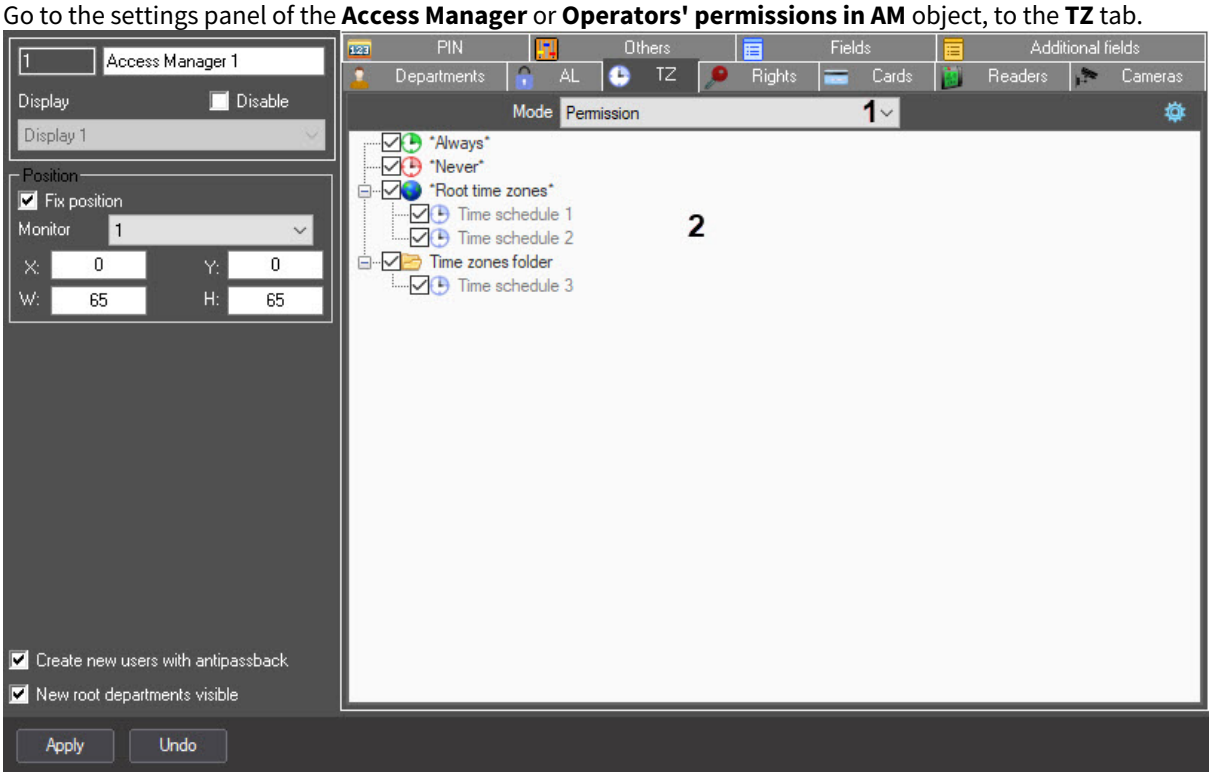
   > **Note**
   >
   > Use the button to set and clear all checkboxes, minimize and expand all drop-down lists, and search for access levels or folders.

4. Click the **Apply** button to save the settings.

5.3.8 Rights to access the time zones in the Access Manager

To specify common and individual rights to access the time zones, do the following:

1. Go to the settings panel of the **Access Manager** or **Operators' permissions in AM** object, to the **TZ** tab.



2. From the **Mode** drop-down list (**1**), select the required mode:
   - **Prohibition**—restrict the access;
   - **Permission**—allow the access.
3. Set the checkboxes (**2**) 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 *Axxon PSIM* or expand the list and set the checkboxes only next to the required time zones.

   > **Note**
   >
   > Use the button to set or clear all checkboxes, minimize and expand all drop-down lists, and search for time zones or folders.

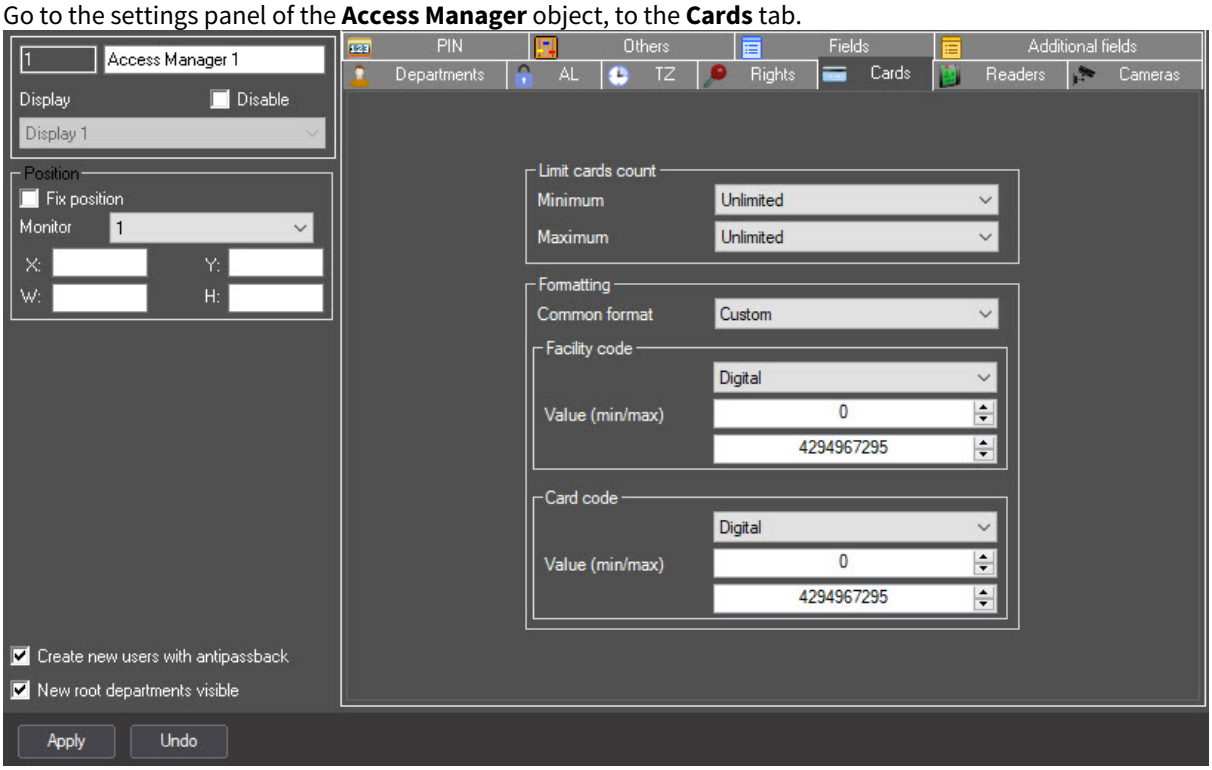
4. Click the **Apply** button to save the settings.

5.4 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).

To configure access cards, do the following:

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



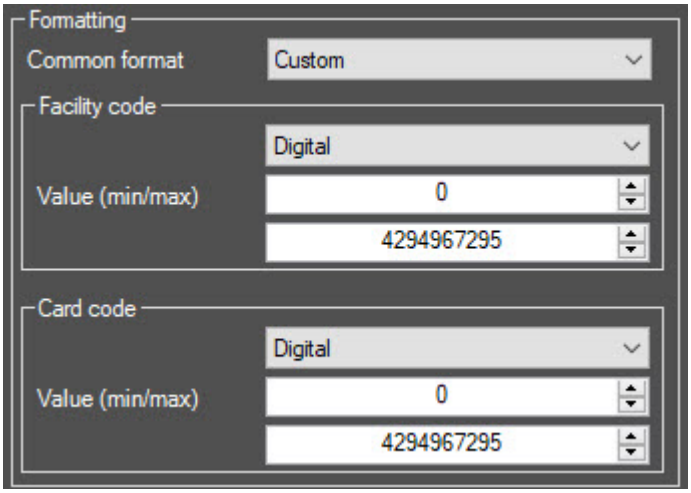
2. In the **Limit cards count** group, from the **Minimum** drop-down list, select the minimum number of access cards that must be assigned to a user.
   - from 1 to 10—if the specified number of access cards is not assigned to a user, then this user cannot be saved in the **Access Manager** interface object.
   - **Unlimited**—an unlimited number of access cards can be assigned to a user.
   - **Prohibited**—user cannot be assigned access cards. Buttons and function menu for assigning access cards are inactive in the **Access Manager** interface object.

3. In the **Limit cards count** group, from the **Maximum** drop-down list, select the maximum number of access cards that must be assigned to a user.
   - from 1 to 10—if a 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 a user.
   - **Prohibited**—user cannot be assigned access cards. Buttons and function menu for assigning access cards are inactive in the **Access Manager** interface object.

   Note

   If at least one **Minimum** or **Maximum** parameter has the **Prohibited** value, the buttons and the function menu for assigning access cards in the **Access Manager** interface object are inactive.

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



Attention!

If the following access cards restrictions are violated, 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 characters 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 must 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 and card code.
  - **Fixed character**—the specified single character is always 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 characters 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 setting 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 website 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 must be no 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 to save the settings.

5.5 Configuring control readers in the Access Manager

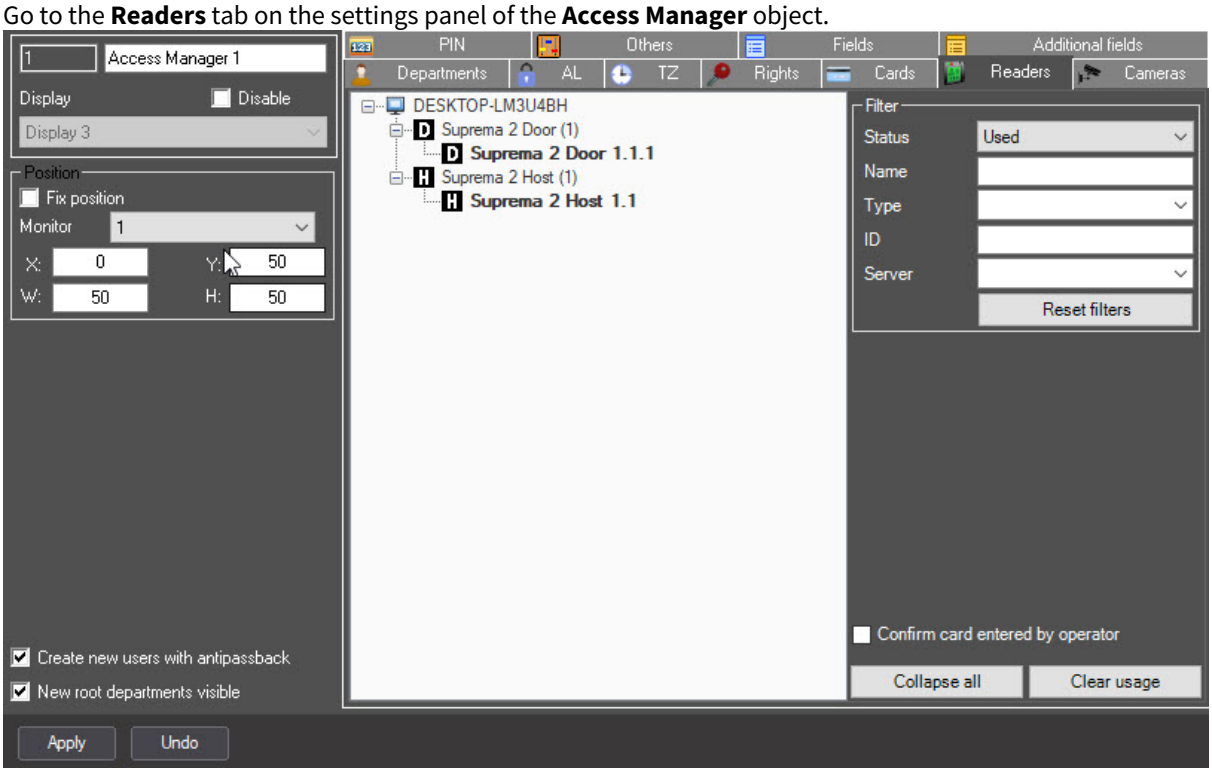
When you configure the *Access Manager* module, you can specify the list of control readers used for assigning access cards or adding biometric parameters of users in the **Access Manager** interface window.

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 from the control reader integration modules (see Control Readers Settings Guide).

To select control readers, do the following:

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



2. If you want the operator to confirm the assignment of access cards to a user, set the **Confirm card entered by operator** checkbox.
3. If necessary, in the **Filter** group, filter the cameras that are used in the *Access Manager* to assign photos to a user.
    a. To filter by status, from the **Status** drop-down list, select the camera status: **Used**, **Not used**, **Any**.
    b. To filter by name, enter the camera name in the **Name** field. The search starts from the first character.
    c. To filter by ID, enter the camera ID in the **ID** field.
    d. To filter by server, select the required server from the **Server** drop-down list.
    e. Select one or more control readers with a double click.

    Note

    To collapse the structure of control readers, click the **Collapse all** button. To deselect the readers, click the **Clear usage** button. To reset the filters and the search result, click the **Reset filters** button.

4. Click the **Apply** button to save the changes.

Note

If you don't select any reader, all readers in the system are displayed (the **Any** status).
If you select at least one reader, the status automatically change to **Used** the next time you open the tab.

Configuring control readers in the *Access Manager* is complete.

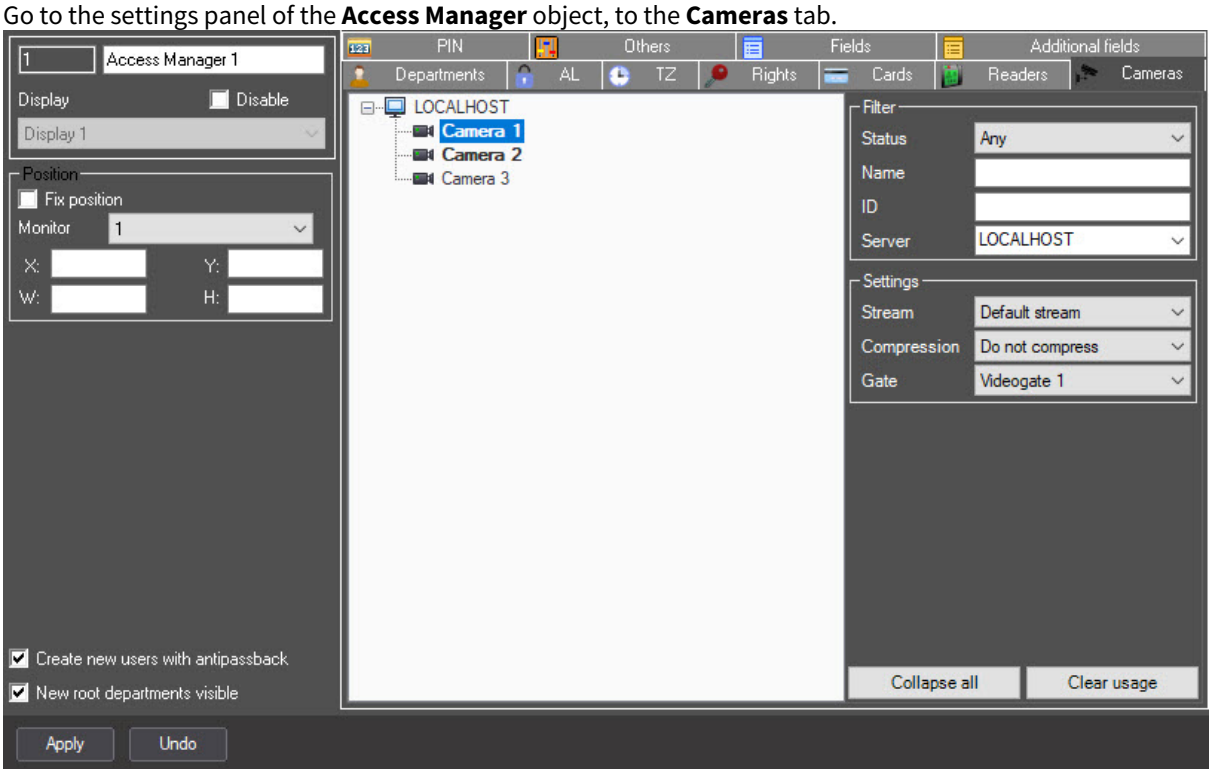
5.6 Selecting and configuring cameras in the Access Manager

On the page:

The *Access Manager* program module allows you to specify cameras that will be available in the **Access Manager** window to assign photos to users and to configure these cameras.

5.6.1 Selecting available cameras

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



2. In the **Filter** group, filter the cameras that you want to use in the *Access Manager* to assign photos to users:
   a. filter by status by selecting camera status from the **Status** drop-down list: **Any**, **Used**, **Unused**.
   b. filter by name by entering camera name in the **Name** field. The search starts with the first character.
   c. filter by ID by entering camera ID in the **ID** field.
   d. filter by server by selecting the required server from the **Server** drop-down list.
3. To collapse the camera structure, click the **Collapse all** button. To delete filtering results, click the **Clear usage** button.
4. Click the **Apply** button.

A list of cameras that are available in the **Access Manager** window to assign photos to users is specified.

5.6.2 Configuring a camera

1. Select a camera that you want to configure.

   > **Note**
   >
   > **Camera** objects are created on the **Hardware** tab of the **System settings** dialog window. Creating and configuring **Camera** is described in the *Axxon PSIM software package. Installing and Configuring Security System Components Guide* document. Current version of this document is available in the documentation repository.

2. From the **Stream** drop-down list, select camera stream.
3. From the **Compression** drop-down list, select video stream compression level.
4. If video from camera must be received via Videogate, select the required **Videogate** object from the **Gate** drop-down list.

   > **Note**
   >
   > The corresponding **Videogate** object must be configured for data transferring with this camera. Configuring the **Videogate** object is described in the *Axxon PSIM software package. Administrator's guide* document. Current version of this document is available in the documentation repository.

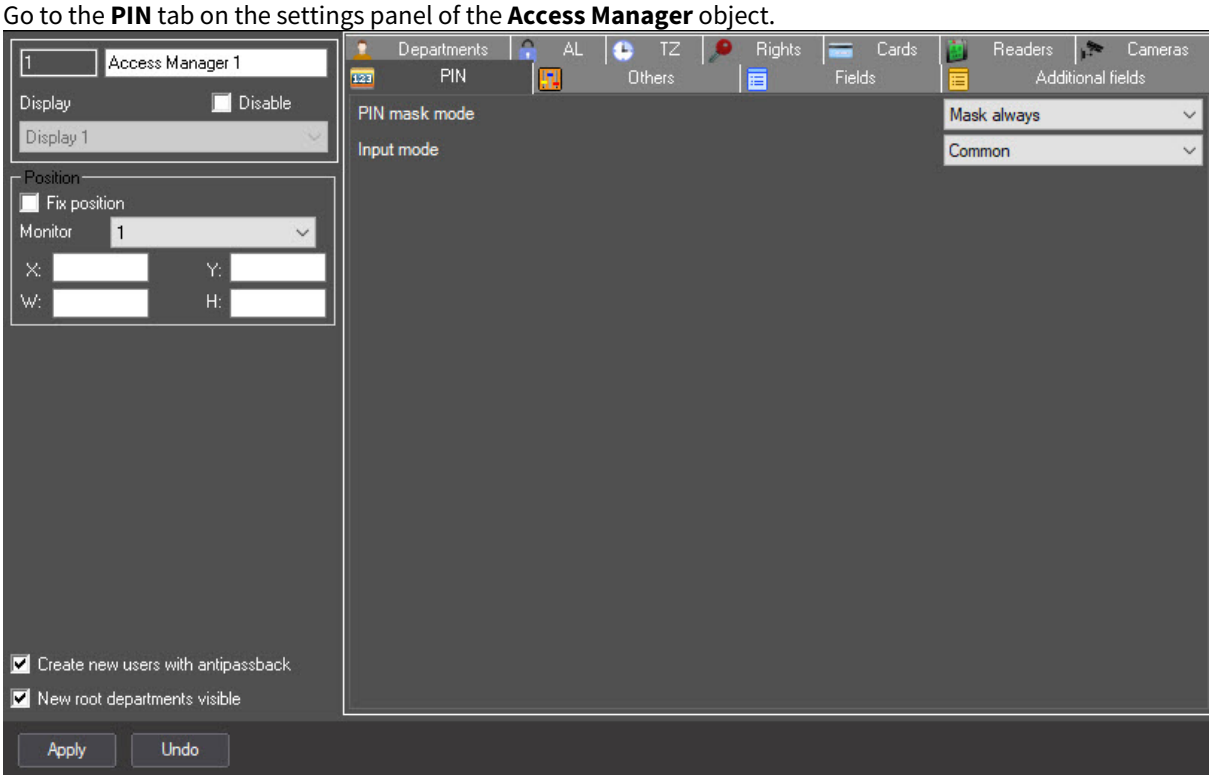
5. Click the **Apply** button to save the settings.

5.7 Configuring the user PIN code

Configuring the user PIN code allows you to set its format and perform the necessary checks to increase the reliability and security of access.

To configure the user PIN code, do the following:

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



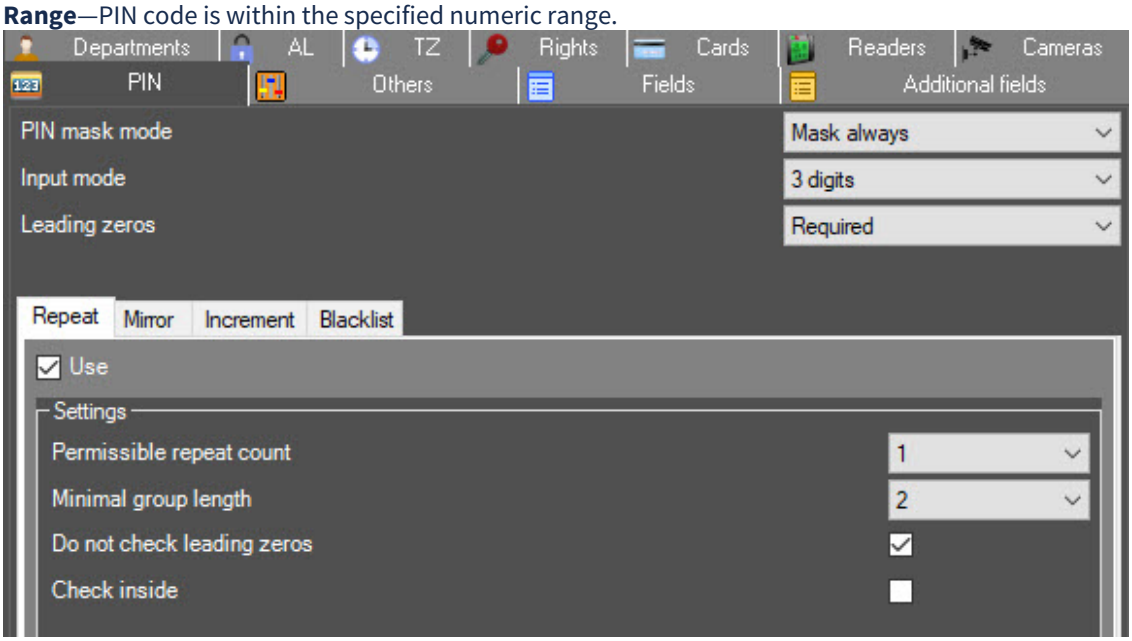
2. From the **PIN mask mode** drop-down list, select the mask mode of the user PIN code:
   - **Do not mask**—PIN code isn't masked with dots;
   - **Mask view**—PIN code is masked with dots when reading user data;
   - **Mask always**—PIN code is always masked with dots.
3. From the **Input mode** drop-down list, select the input mode of the user PIN code, further settings depend on it:
   a. **Common**—any variant of the PIN code is allowed. It is allowed to enter symbols, letters and numbers. If you select this mode, you can go to step 10 to apply the settings.

      Note

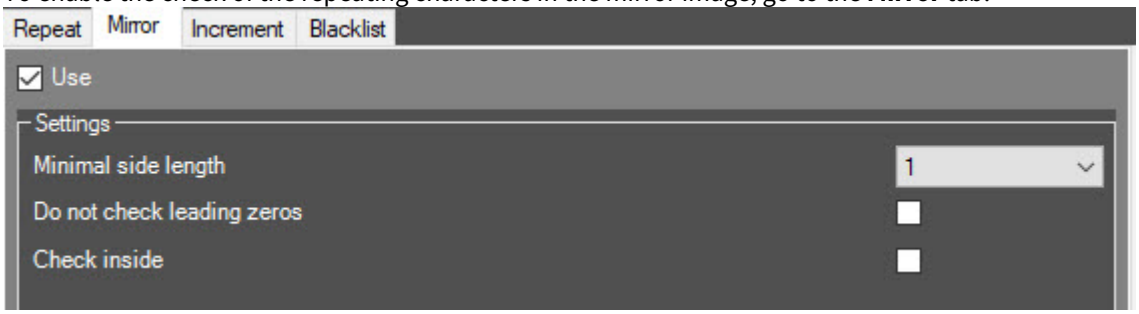
      All further settings are made for all modes except for the **Common** mode.

   b. **3 digits**—PIN code must contain three digits.
   c. ...
   d. **9 digits**—PIN code must contain nine digits.

e. **Range**—PIN code is within the specified numeric range.



4. From the **Leading zeros** drop-down list, select the mode of setting zeros at the beginning of the PIN code:
   a. **Ignore**—leading zeros aren't considered as characters.
   b. **Required**—leading zeros are considered as characters.
   c. **Auto**—leading zeros are entered automatically, completing the PIN code to the required number of characters.
5. To enable the required PIN checks, go to the corresponding **Repeat**, **Mirror**, **Increment**, **Blacklist** tab and set the **Use** checkbox.
6. To enable the check of the repeating characters, go to the **Repeat** tab.
   a. From the **Permissible repeat count** drop-down list, select the maximum number of allowed character repetitions in the PIN code. The range of values depends on the input mode selected in step 3.
   b. From the **Minimal group length** drop-down list, select the number of characters in the group to search for repetitions. The range of values depends on the input mode selected in step 3.
   c. Set the **Do not check leading zeros** checkbox to disregard leading zeros when searching for repetitions. By default, the checkbox is clear.
   d. Set the **Check inside** checkbox to search for repetitions in the entire PIN code. By default, the checkbox is clear.
7. To enable the check of the repeating characters in the mirror image, go to the **Mirror** tab.



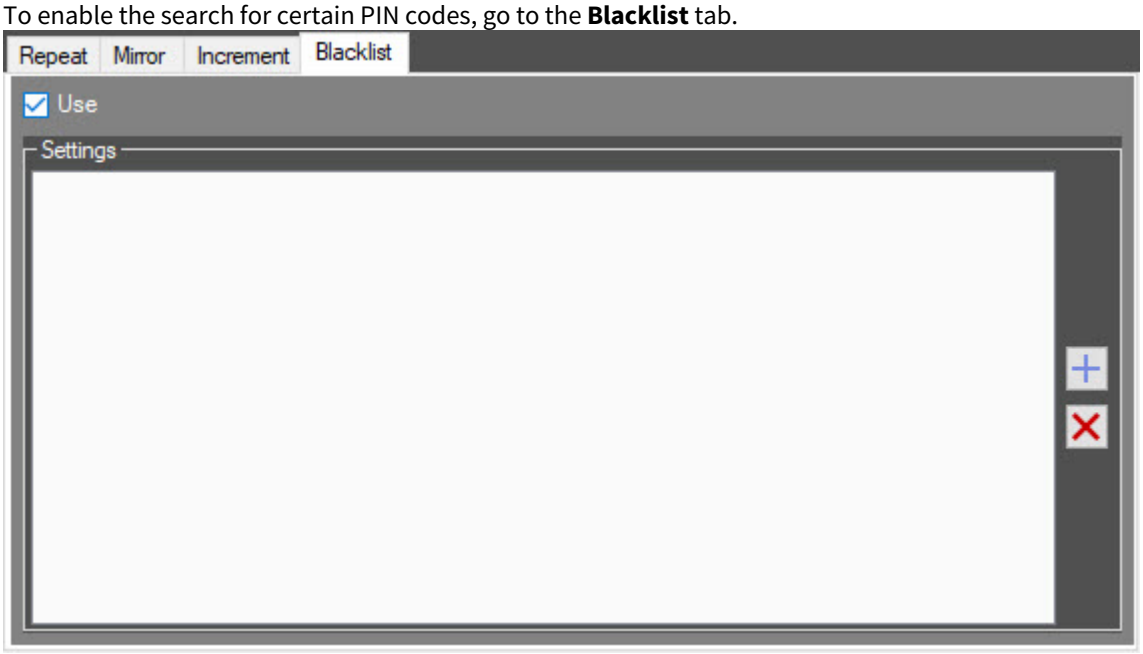
   a. From the **Minimal side length** drop-down list, select the number of characters in the group to search for repetitions in the mirror image. The range of values depends on the input mode selected in step 3.
   b. Set the **Do not check leading zeros** checkbox to disregard leading zeros when searching for repetitions in the mirror image. By default, the checkbox is clear.

c. Set the **Check inside** checkbox to search for repetitions in the entire PIN code in the mirror image. By default, the checkbox is clear.

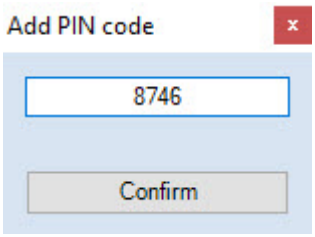
8. To enable the check of increasing and decreasing character sequences in the PIN code, go to the **Increment** tab.

a. From the **Permissible 'stair' length** drop-down list, select the number of characters in increasing/decreasing order from which the search will be performed. The range of values depends on the input mode selected in step 3.
b. From the **Checking mode** drop-down list, select the type of check:
   i. **Both**—sequences of characters are checked in increasing (increment) and decreasing (decrement) order.
   ii. **Increment**—sequences of characters are checked in increasing order.
   iii. **Decrement**—sequences of characters are checked in decreasing order.
c. Set the **Do not check leading zeros** checkbox to disregard leading zeros when searching for sequences of characters in increasing and decreasing order. By default, the checkbox is clear.
d. Set the **Check inside** checkbox to search for sequences of characters in increasing and decreasing order in the entire PIN code. By default, the checkbox is clear.

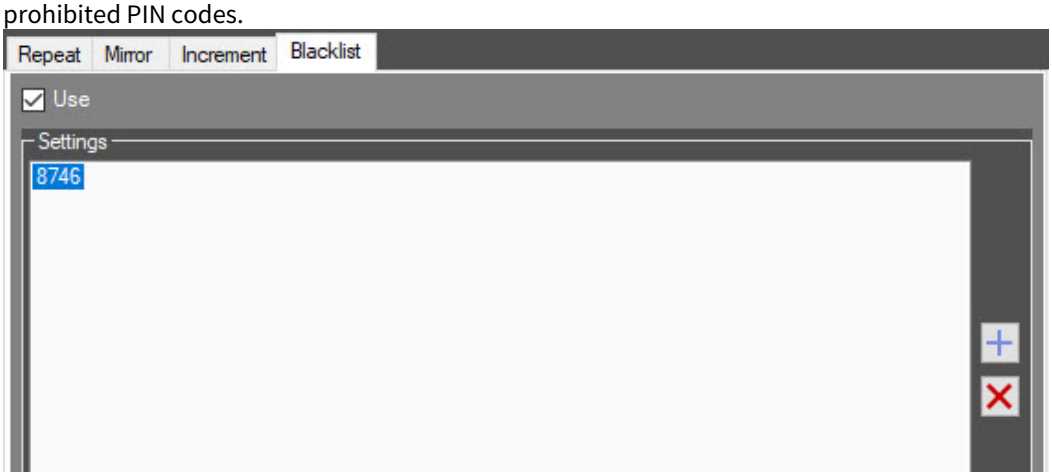
9. To enable the search for certain PIN codes, go to the **Blacklist** tab.



a. To add a PIN code to the blacklist, click the button. The **Add PIN code** window will open.



i. Enter the required PIN code in the blank field.
ii. Click the **Confirm** button. As a result, the specified PIN code will be added to the list of prohibited PIN codes.



Note

To remove the PIN code from the blacklist, click the button.

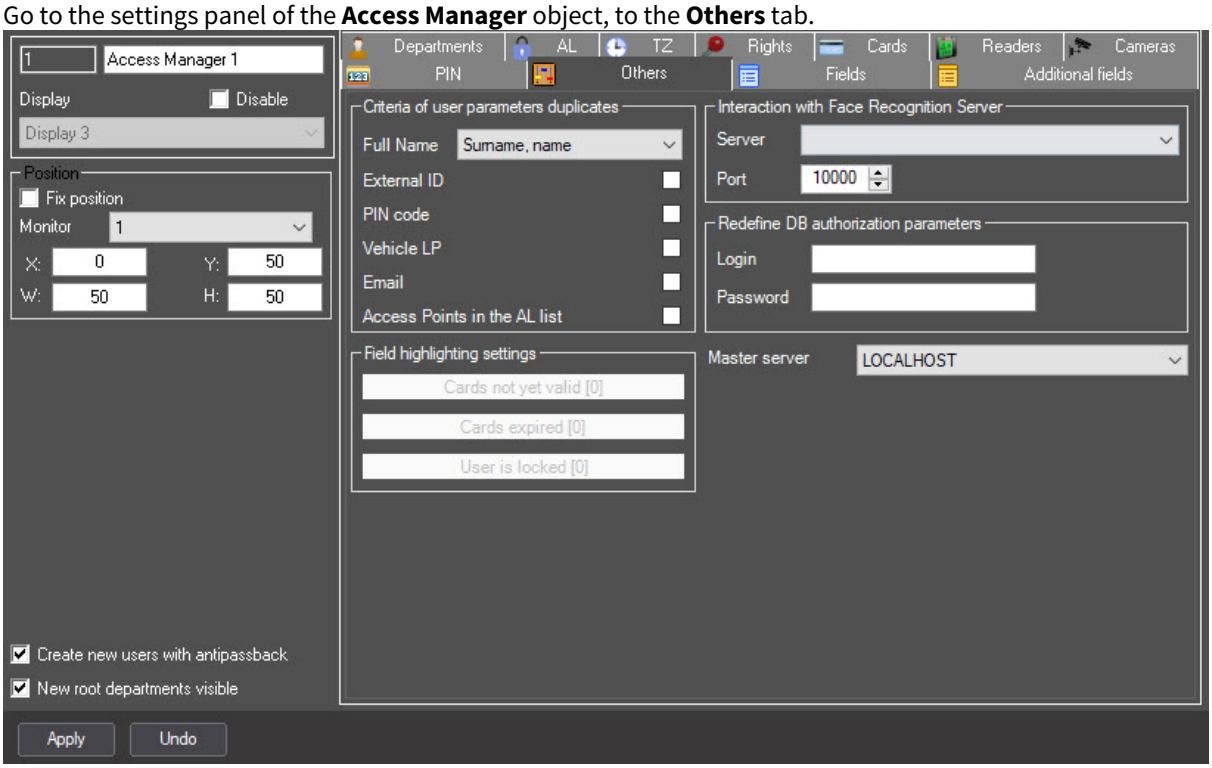
10. Click the **Apply** button to save the settings.

Configuring the user PIN code is complete.

5.8 Configuring the prohibition of duplicates of new user parameters in the Access Manager

To configure the prohibition of duplicate parameters for new users, do the following:

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



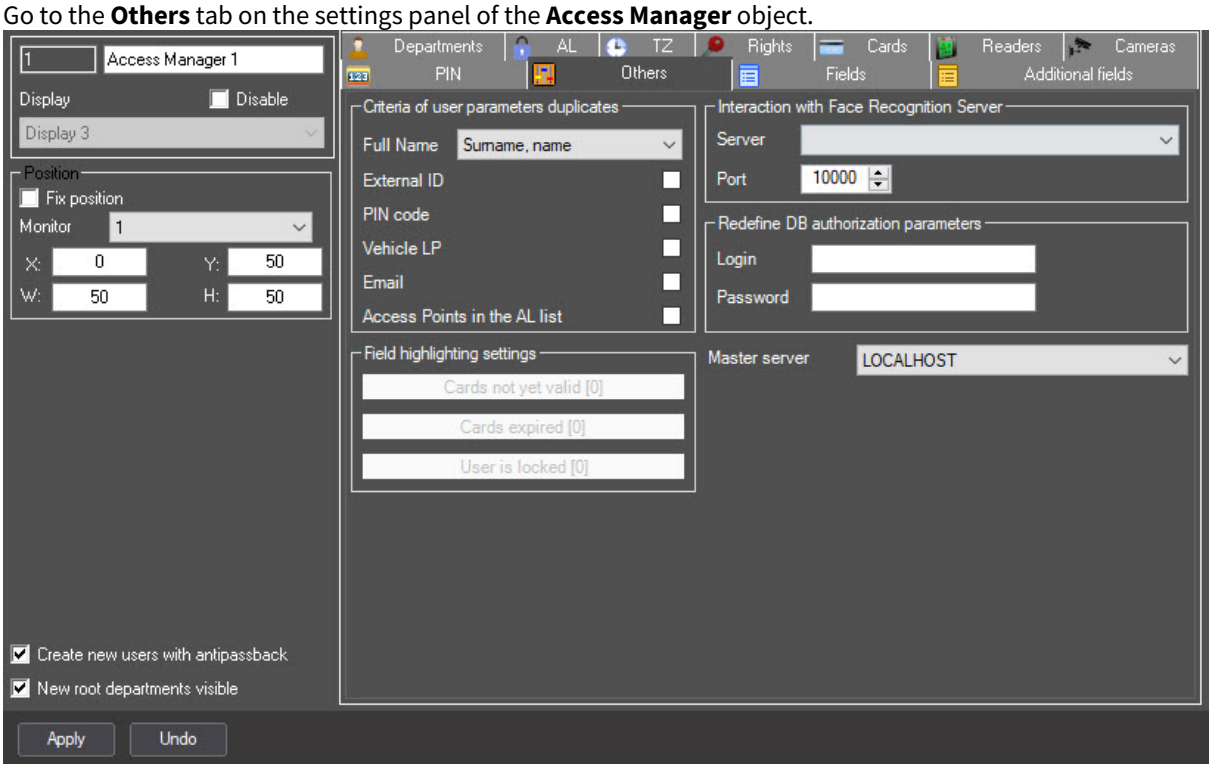
2. From the **Full Name** drop-down list, select a method for identifying duplicate user records:
   a. **Not used**—you can add users with the same full name.
   b. **Surname, name**—you cannot add users with the same name and surname even if patronymic is differed.
   c. **Surname, name, patronymic**—you cannot add users with the same full name.
3. Set the **External ID** checkbox to prohibit creating users with the same external identifiers.
4. Set the **PIN code** checkbox to prohibit creating users with the same PIN codes.
5. Set the **Vehicle LP** checkbox to prohibit creating users with the same vehicle license plates.
6. Set the **Email** checkbox to prohibit creating users with the same email address.
7. Set the **Access Points in the AL list** checkbox to prohibit creating users who have access levels with the same access points. If the checkbox is set, such a user cannot be created and the event of access level conflict appears in the *Event Viewer*.
8. Click the **Apply** button to save the settings.

5.9 Configuring the blocking of the Access Manager when the main server is unavailable

In a distributed architecture in which there are many Client workstations with the *Access Manager* module installed, it is important to keep the Clients up and running when the main (master) server is down. However, changes made on the Client workstations when the master server is down can result in misconfiguration of users, duplication, overrides, and other problems. To prevent this, in the *Access Manager* module, you can specify a server that, when down, will block the *Access Manager* on all servers on which this option is set. After the connection to the master server is restored, the work of the *Access Manager* module on the Client workstations will fully resume.

To enable the blocking of the *Access Manager* module for the Client workstations when the master server is unavailable, do the following:

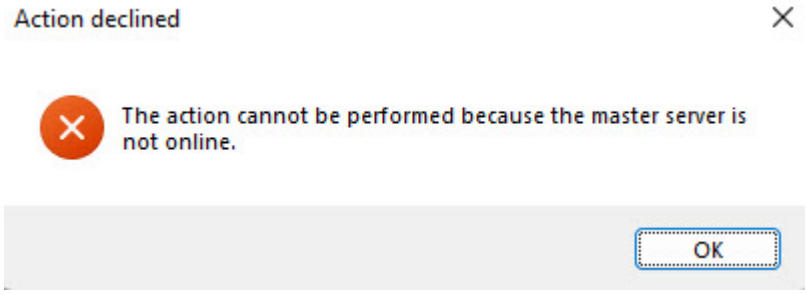
1. Go to the **Others** tab on the settings panel of the **Access Manager** object.



2. From the **Master server** drop-down list, select the master server.
3. Click the **Apply** button to save the settings.

Configuring the blocking of the *Access Manager* module for the Client workstations when the master server is unavailable is complete.

When you try to make any changes, a system message is displayed stating that the master server is unavailable.

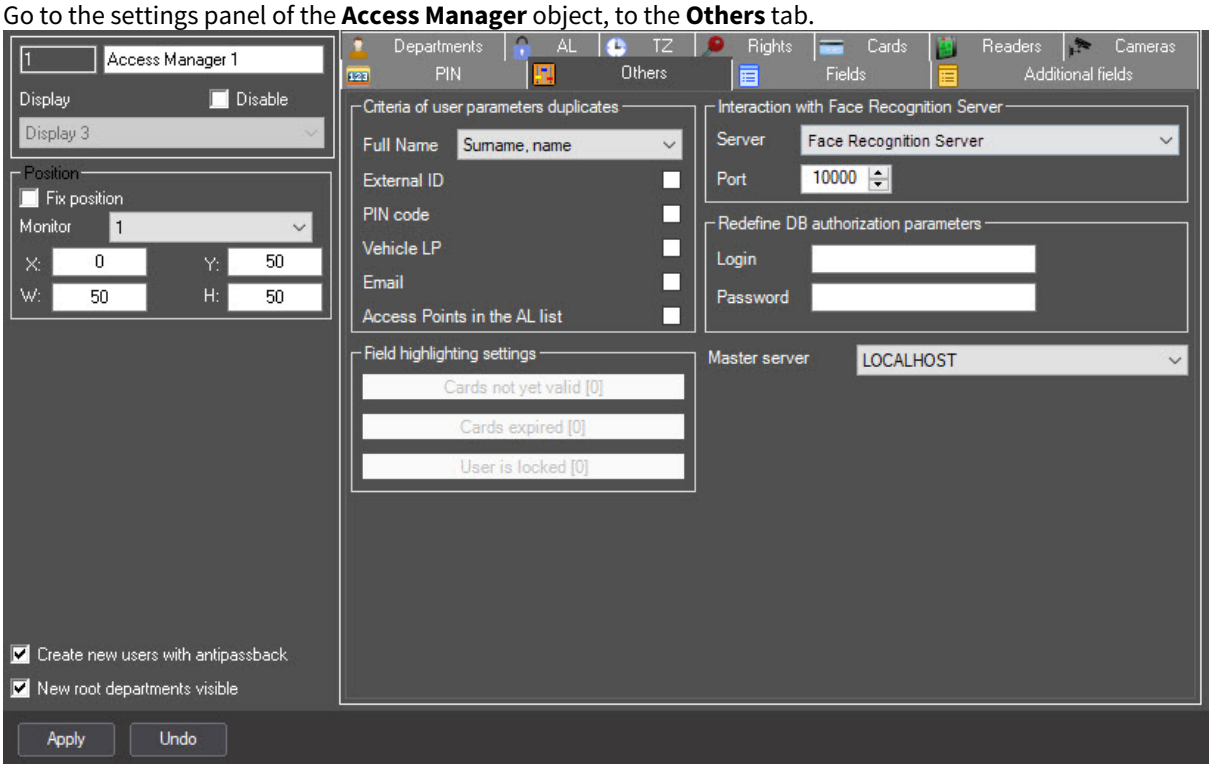


5.10 Configuring the interaction with the Face PSIM Face Recognition Server

Configuring the interaction with the *Face PSIM* Face Recognition Server allows you to check the quality of a recognized face before assigning it to a user.

To configure the interaction with the Face Recognition Server, do the following:

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



2. In the **Interaction with Face Recognition Server** group, from the **Server** drop-down list, select the Face Recognition Server (for details, see *Face PSIM*. Administrator's Guide) that will check the quality of user photos that you add.
3. In the **Port** field, specify the port used for connecting to the Face Recognition Server. The default value is **10000**.
4. Click the **Apply** button to save the settings.

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

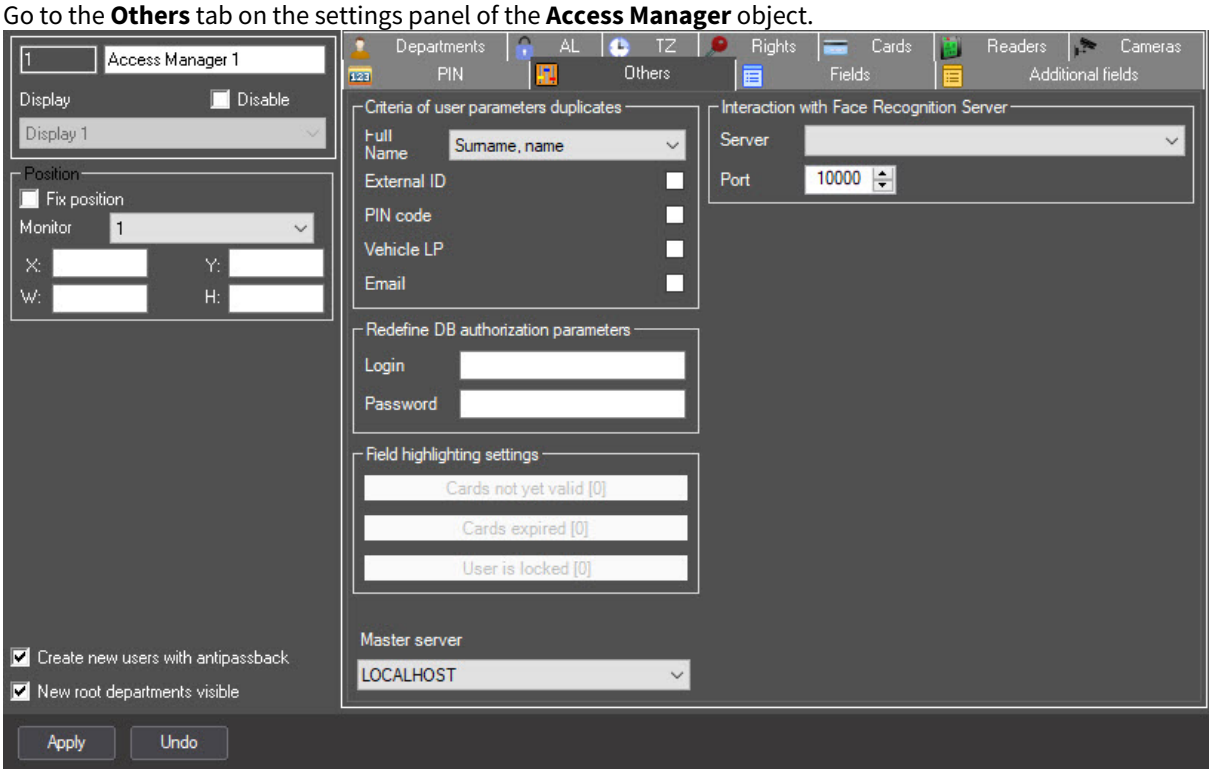
5.11 Highlighting user access cards

In the *Access Manager*, you can highlight the following groups of access cards:

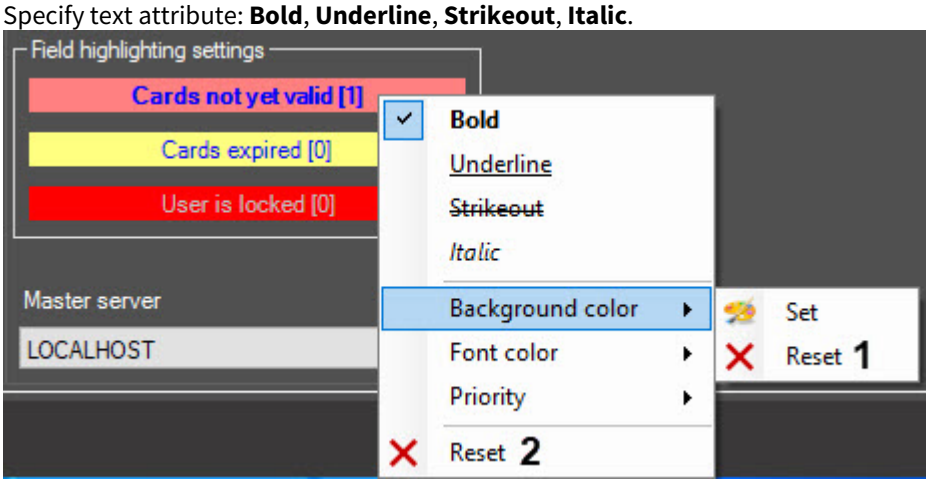
- Cards not yet valid,
- Cards expired,
- User is locked.

To highlight access cards, do the following:

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



2. Right-click the **Cards not yet valid [0]**, **Cards expired [0]**, **User is locked [0]** button.
3. In the menu that opens, select an option to highlight an access card:
   a. Specify text attribute: **Bold**, **Underline**, **Strikeout**, **Italic**.



   b. Specify the **Background color** and **Font color** by clicking **Set**, to cancel the action, click **Reset** (**1**).
   c. From the **Priority** drop-down list, select the priority level of highlighting a group of access cards in the range from 0 (default) to 4. Priority is displayed in square brackets. It is used when an access card is assigned to two groups at the same time.

> **Note**
>
> To cancel all changes, click **Reset** (**2**).

4. Click the **Apply** button to save the changes.

Highlighting user access cards is complete.

5.12 Configuring fields displaying in user accounts

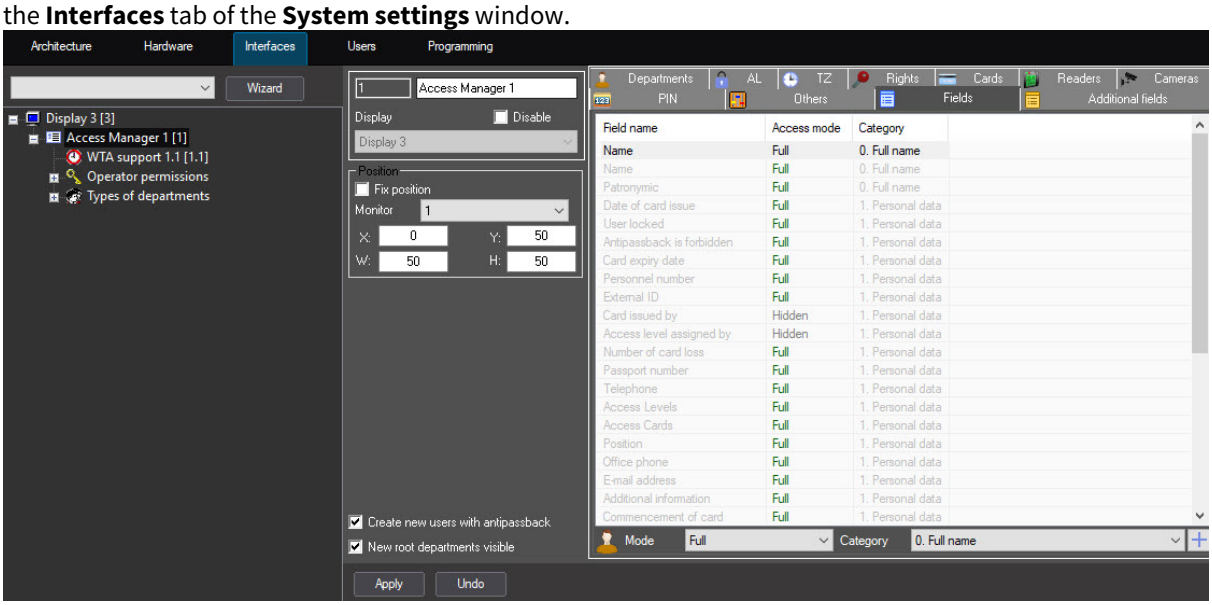
5.12.1 Configuring the Main department type

The **Main** department type determines the user fields available in the **Access Manager** for viewing and editing by default.

> **Note**
>
> Fields visibility can also be determined by the **Type of department** and **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).
> Fields visibility of the **Main** department type is only taken into account if the **Main** department type is selected in the **Access Manager** interface window when you edit department properties (see Editing a department).
> You can sort alphabetically any column of the **Fields** and **Additional fields** tabs by clicking its name.

To configure the **Main** department type, do the following:

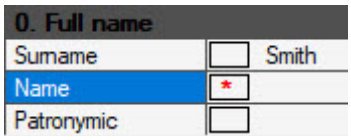
1. Go to the settings panel of the **Access Manager** object that is created on the basis of the **Display** object on the **Interfaces** tab of the **System settings** window.



2. Go to the **Fields** or **Additional fields** tab.
3. Available fields are displayed in the **Field name** column.

> **Note**
>
> For the description of fields, see Specifying user parameters.

4. If necessary, specify the access mode and category for the required fields manually. For this:
   a. Select a user field for editing.
   b. From the **Mode** drop-down list, select the access mode to the user field.

Value	Description
Hidden	Field isn't displayed in the list of user parameters when viewing and editing
Read only	Field is displayed in the list of user parameters when viewing and editing, but it isn't editable
Edit	Field is displayed in the list of user parameters when viewing and editing, and it is editable. *Note. The **Card issued by** and **Access level assigned by** fields are always not editable as these fields are automatically filled with the name of the Operator when assigning/ changing card or access level*
Required	Field is mandatory when creating and editing a user in the *Access Manager* module. Field that isn't filled in is highlighted with red asterisks 

c. From the **Category** drop-down list, select the name of the user parameter group in the **Access Manager** interface window in which the field will be displayed during editing and viewing. The name of the category can be arbitrary. Categories that exist in the system are **0. Full name**, **1. Personal data**, **3. Vehicle**, **4. Visitor data**. If you don't specify a category, the field will be displayed in the parameter list in the **Others** category.

> **Note**
>
> Categories in the parameter list are sorted alphabetically. Use number prefixes in the name to set strict order of sorting.

5. To add a category, click the  button.
6. Click the **Apply** button to save the setting.

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

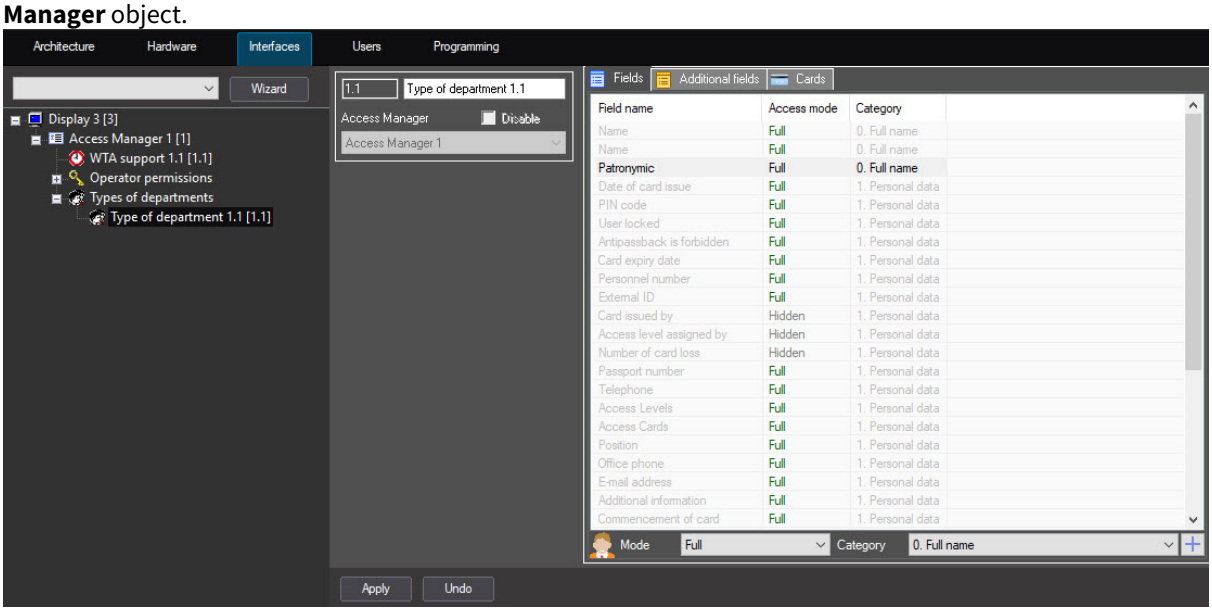
5.12.2 Configuring a type of department in the Access Manager

Type of department determines the user fields available for viewing and editing in the **Access Manager** interface window.

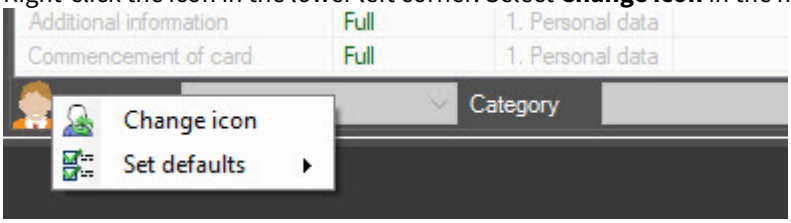
> **Note**
>
> Visibility of the fields is also determined by operator rights (see Configuring availability of fields depending on operator rights in the Access Manager).
> You can sort alphabetically any column of the **Fields** and **Additional fields** tabs by clicking its name.

To configure a type of department, do the following:

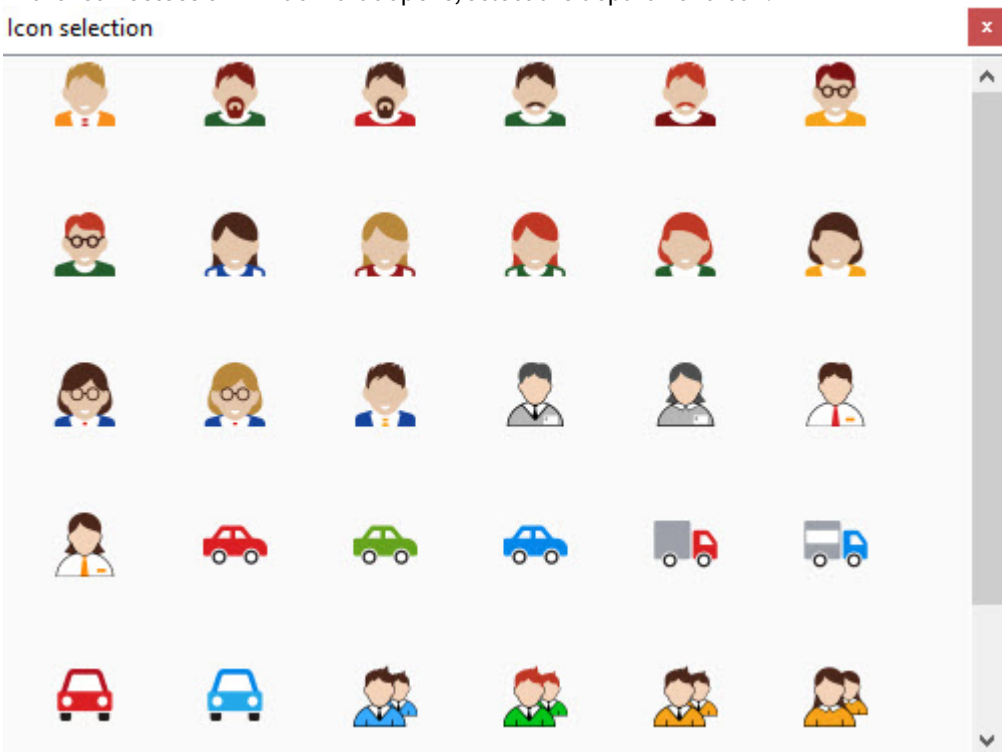
1. Go to the settings panel of the **Type of department** object that is created on the basis of the **Access Manager** object.



2. You can change the department icon in the **Access Manager** window. For this, do the following:
   a. Right-click the icon in the lower left corner. Select **Change icon** in the menu.



   b. In the **Icon selection** window that opens, select the department icon.



3. For convenience of configuring the availability of the main fields, select template types of departments. For this, do the following:
    a. Right-click the icon in the lower left corner. Select **Set defaults** in the menu.
    b. Select the template of the department type. Templates of the following department types are available: **Employees, Visitors, Vehicle**. As a result, the **Fields** and **Additional fields** tabs will contain values according to the selected template.
4. If necessary, specify the access mode and category for the required fields manually. For this, do the following:
    a. Select a user field for editing.
    b. From the **Mode** drop-down list, select the access mode to the user field.

Value	Description
Hidden	Field isn't displayed in the list of user parameters when viewing and editing
Read only	Field is displayed in the list of user parameters when viewing and editing, but it isn't editable
Edit	Field is displayed in the list of user parameters when viewing and editing, and it is editable. *Note. The **Card issued by** and **Access level assigned by** fields are always not editable as these fields are automatically filled with the name of the Operator when assigning/changing card or access level*
Mandatory	Field is mandatory when creating and editing a user in the *Access Manager* module. Field that isn't filled in is highlighted with red asterisks 

> **Note**
>
> See the description of fields in Specifying user parameters.

    c. From the **Category** drop-down list, select the name of the user parameter group in the **Access Manager** interface window in which the field will be displayed during editing and viewing. The name of the category can be arbitrary. Categories that exist in the system are **0. Full name**, **1. Personal data**, **3. Vehicle**, **4. Visitor data**. If you don't specify a category, the field will be displayed in the parameter list in the **Others** category.

> **Note**
>
> Categories in the parameter list are sorted alphabetically. Use number prefixes in the name to set strict order of sorting like in templates.

5. To add a category, click the  button.

6. If it is necessary for this type of department to have its own parameters of access cards, make the appropriate settings on the **Cards** tab (see Configuring access cards).
7. Click the **Apply** button to save the settings.

Configuring a type of department is complete.

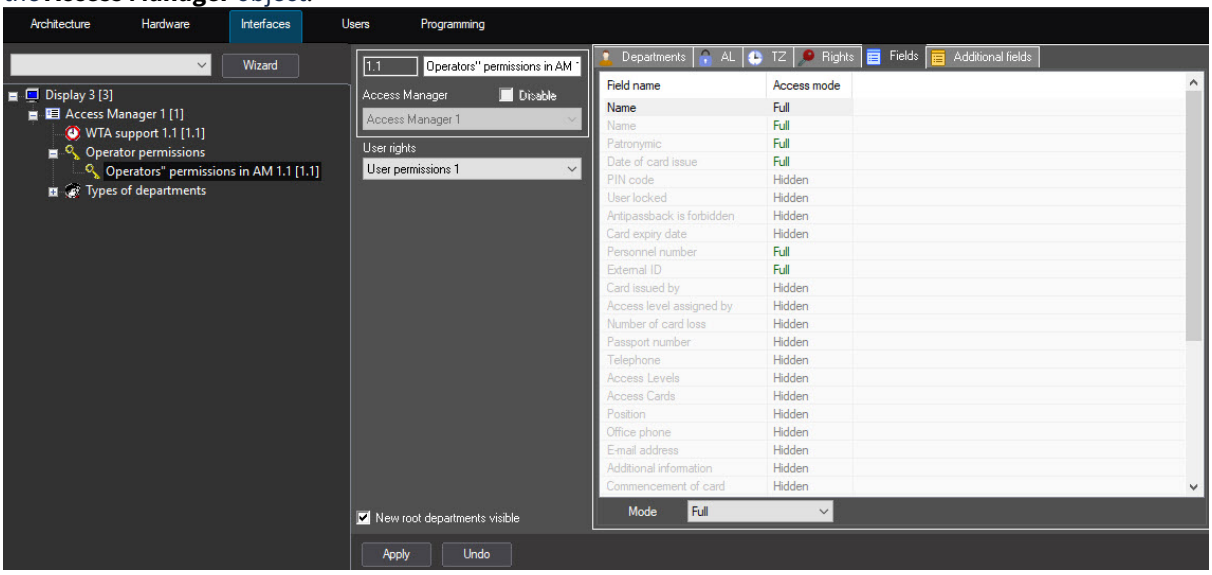
5.12.3 Configuring availability of fields depending on operator rights in the Access Manager

The *Access Manager* module allows you to limit the visibility and availability of user fields for editing depending on operator's rights in the *Access Manager*. The prohibition to perform an operation with a field in operator's rights has priority over availability of field for viewing and editing specified when configuring the type of department. For example, if some field is available for editing according to the settings of the department type, but its viewing is forbidden by the rights of a certain operator, then this field won't be visible to this operator. The opposite is also true: if editing of field is allowed by operator's rights in the *Access Manager,* but the field is available only for reading, then the field will be available for reading for all operators regardless of their rights.

> **Note**
>
> When you change the rights of the current operator, you must re-register the user in *ACFA PSIM* to apply the changes.

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

1. Go to the settings panel of the **Operators'' permissions in AM** object that is created on the basis of the **Access Manager** object.



2. Select the required tab: **Fields** or **Additional fields**. By default, all user fields are hidden.

> **Note**
>
> You can sort alphabetically any column of the **Fields** and **Additional fields** tabs by clicking its name.
> See the description of fields in Specifying user parameters.

3. Select a user field for editing.
4. From the **Mode** drop-down list, select the access mode to the user field.

Value	Description
Hidden	Field isn't displayed in the list of user parameters when viewing and editing
Read only	Field is displayed in the list of user parameters when viewing and editing, but it isn't editable
Edit	Field is displayed in the list of user parameters when viewing and editing, and it is editable. *Note. The **Card issued by** and **Access level assigned by** fields are always not editable as these fields are automatically filled with the name of the Operator when assigning/changing card or access level*
Mandatory	Field is mandatory when creating and editing a user in the *Access Manager* module. Field that isn't filled in is highlighted with red asterisks 

5. Click the **Apply** button to save the settings.

Configuring availability of fields depending on operator's rights is complete.

5.13 Configuring the ABBYY PassportReader SDK module

On the page:

5.13.1 General information about the ABBYY PassportReader SDK module

The *ABBYY PassportReader SDK* module is used to fill out the users parameters in the *Access Manager* module automatically after the images of the identification documents are recognized (passport, driver's license, passport for traveling abroad, birth certificate, and so on), including the images of the identification documents of some CIS

countries (Azerbaijan, Belarus, Kazakhstan, Kyrgyzstan, Tajikistan, Uzbekistan) and foreign passports of any country (MRZ analyzed) from the scanner or hard disk.

Manufacturer:	ABBYY www.ABBYY.com
SDK version:	1.5.2

5.13.2 Configuration procedure

To configure the *ABBYY PassportReader SDK* module, do the following:

1. Create and configure the *Access Manager* module.
2. Open the **account_manager.run.config** file for editing. The file is created in the *<Axxon PSIM installation directory>Modules* folder after the first start of the *Access Manager* module.
3. Set the value of the **AbbyyAPIEnabled** key to **True.** The default value is **False**.

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

4. Save the changes in the edited **account_manager.run.config** file.
5. Install the 32-bit version of the *ABBYY PassportReader* SDK.

> **Note**
>
> Contact the manufacturer about licensing and downloading the *ABBYY PassportReader* SDK distribution.

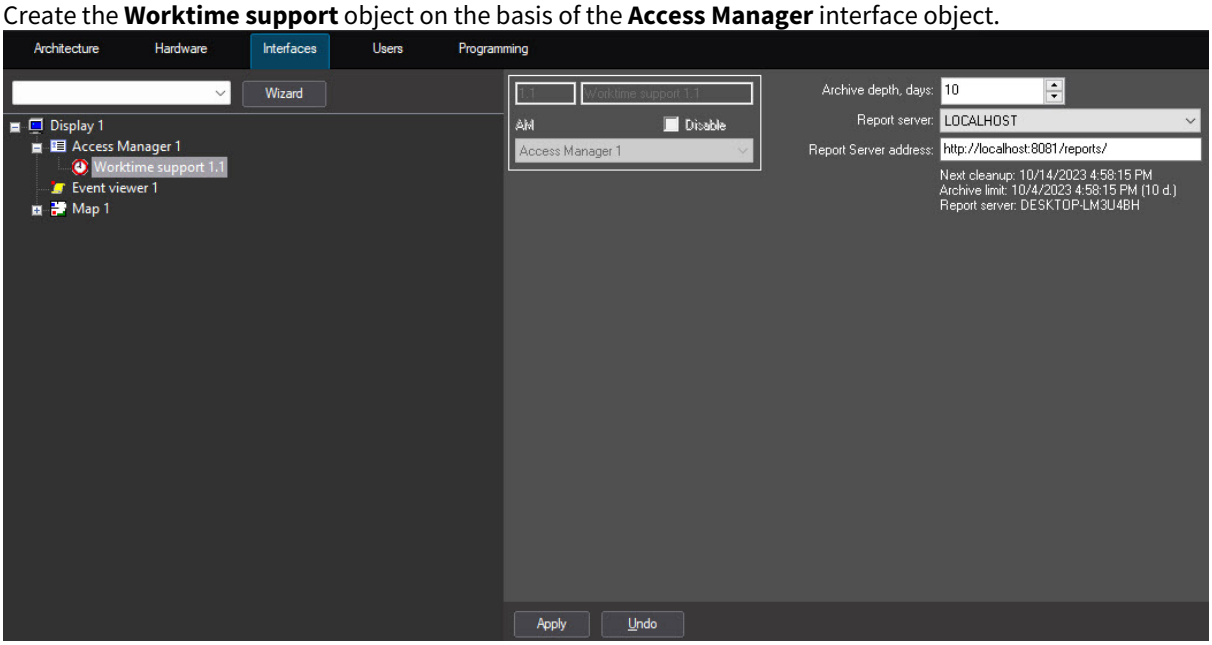
6. Restart *ACFA PSIM.*
7. As a result, the button for accessing the *ABBYY PassportReader SDK* module becomes active in the *Access Manager* module (see Filling out the user parameters using the ABBYY PassportReader SDK module).

Configuring the *ABBYY PassportReader SDK* module is complete.

5.14 Configuring the Worktime subsystem

For the correct operation of the *Worktime* subsystem, do the following in the specified order and in full:

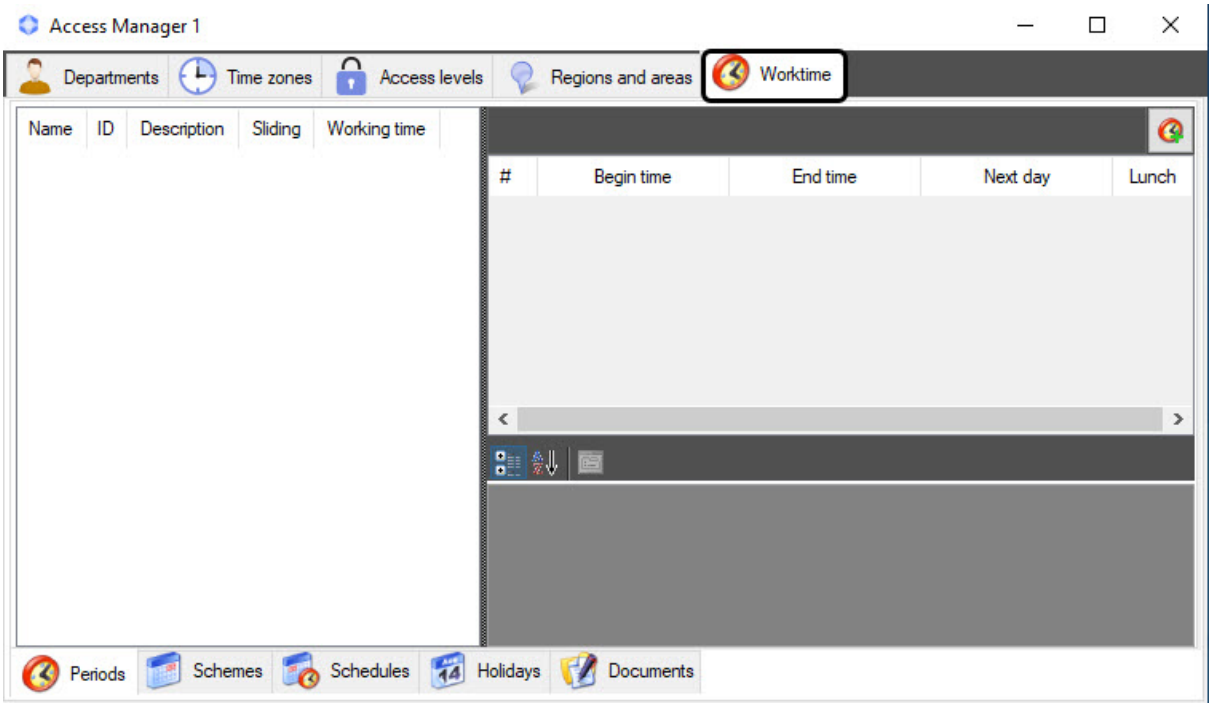
1. Create the **Worktime support** object on the basis of the **Access Manager** interface object.



2. Go to the settings panel of the **Worktime support** object.
3. In the **Archive depth, days** field, specify the time of storing the events archive in days, after which the event is deleted from the archive. If you leave 0 (the default value), the archive won't be automatically cleared.
4. From the **Report server** drop-down list, select the computer on which you created the **Time and Attendance reports** object (part of the *WEB Report System PSIM*) and whose database contains all information about access.
5. In the **Report Server address** field, specify the server address of the *WEB Report System PSIM.* For the information about configuring and working with the system, see WEB Report System PSIM. User Guide.

> **Note**
>
> If the server of the *WEB Report System PSIM* has a static ip, and you plan to generate reports from another subnetwork, you must explicitly specify the IP address of the server of the *WEB Report System PSIM.*

6. Click the **Apply** button to save the changes.
7. Restart *ACFA PSIM*.
   After that, the **Worktime** tab will appear in the **Access Manager** interface window.



8. Update the database using the UpdateDB Utility.
9. Configure the regions for the ACS Readers (see Appendix 1. Configuring Regions for the ACS Readers to work with the Time and Attendance subsystem).
10. Create and configure:

> **Note**
>
> We recommend that you read The Worktime tab of the Access Manager interface window.

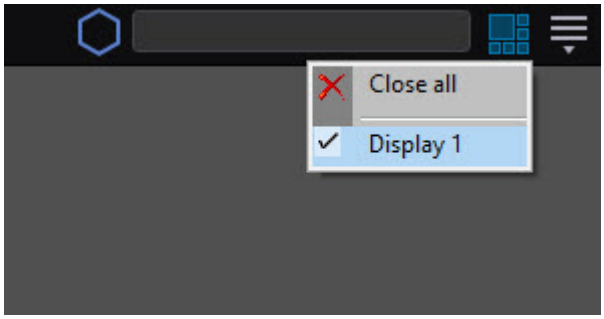
    a. Create work periods (see Work periods).
    b. Create work schemes (see Work schemes).
    c. Create work schedules (see Work schedules).
    d. If necessary, configure holidays (see Holidays).
    e. If necessary, create and configure documents (see Documents).
11. Assign work schedules to departments (see Assigning a work schedule to a department).
12. Assign work schedules to employees (see Assigning a work schedule to a user).
13. Assign documents to employees (see Assigning documents to a user).
14. Configure the WEB *Report System PSIM* (see Working with the reports).
15. To account for employee passes made before configuring the *Worktime* subsystem, use the UpdateDB Utility and re-account the databases (see Starting and working with the UpdateDB Utility).

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 *ACFA PSIM*. You can open and close this window using the **Display** menu of the main control panel.

> **Note**
>
> In order to be able to run the *Access Manager* software module, you must create the **Access Manager** object on the basis of the corresponding display on the **Interfaces** tab.



To display the **Access Manager** interface window, select in the menu 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** menu item.

General view of the **Access Manager** window see in Interface of the Access Manager module.

To close the **Access Manager** window, use the  button. In this case, to reopen the window, double-click the  icon in the Windows taskbar. If you hover the mouse cursor over this icon, the name of the **Access Manager** object corresponding to the **Access Manager** interface window is displayed.

> **Note**
>
> The module icon is displayed in the Windows taskbar depending of the value of the *DebugLevel* setting in the *HKLM → Software → Wow6432Node → AxxonSoft → PSIM → Debug* branch of the Windows registry. If this parameter is set to 0, empty or missing, the icon won't be displayed in the taskbar. 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, you can configure the view of user lists, time zones and access levels. The following types of display are available:

1. List.

2. Table.

Full Name	Number	Date of card issue	PIN code	User locked	Antipassback	Card expiry date
Hill Rick	2	Not specified		No	No	Not specified
McDonald Ronald John	4	Not specified		No	Yes	Not specified
Smith Patrick	1	Not specified		No	Yes	12/12/2023 12:00:00 AM

3. Large icons.

Note

By default, the **Large icons** view is used for the user list, times zones, regions, and access levels. The **Table** and **List** views are used for access levels. You cannot change the view in the access level list.

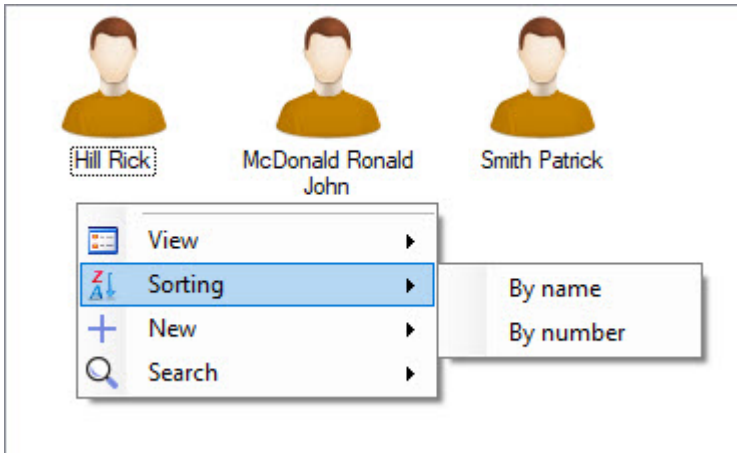
You can select the view of display in the function menu that opens when you right-click in the free space of objects list or any user.

6.2.2 Selecting a method of sorting objects in the list

When you select the **List** and **Large icons** view in the *Access Manager,* you can select the following methods of sorting user lists, time zones and access levels:

1. By name.
2. By number.

You can select a method of sorting in the function menu that opens when you right-click in the free space of objects list or any user.

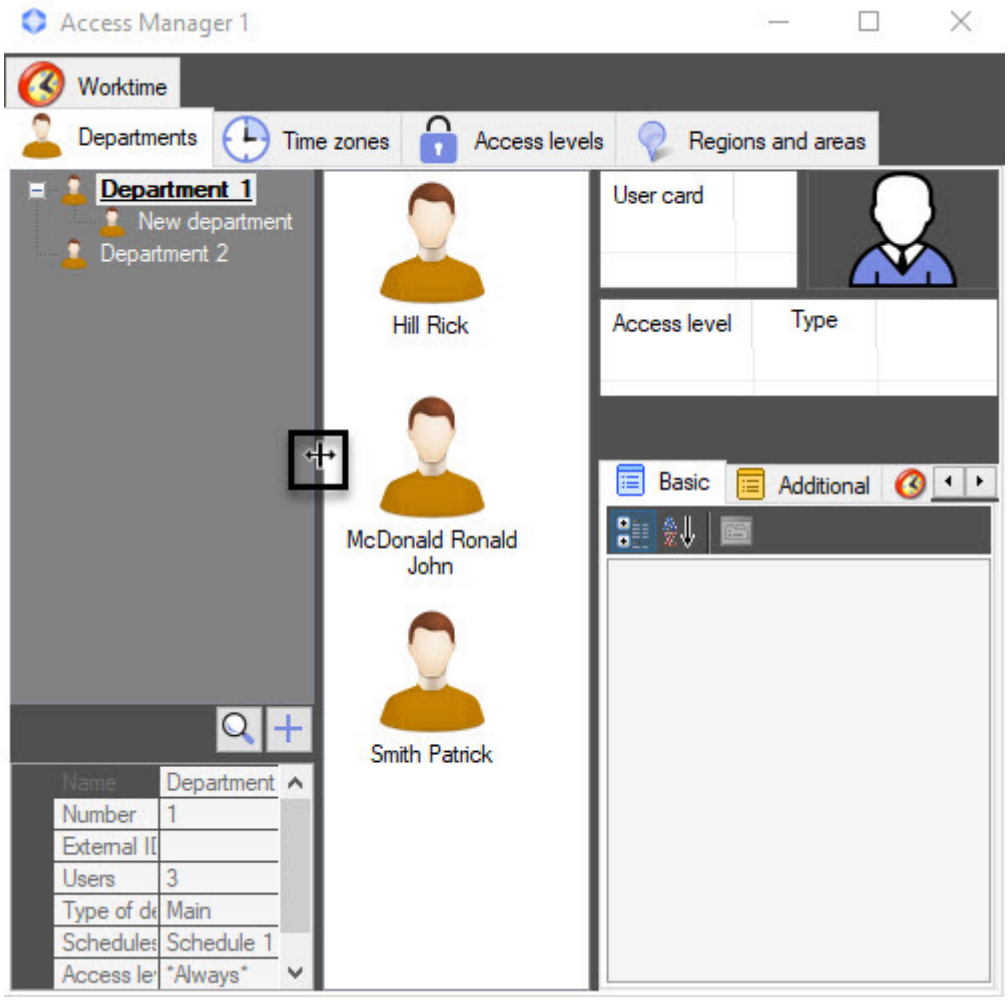


When you select the **Table** view, you can sort the values in the list by clicking the header of the corresponding column.

Full Name	Number	Date of card issue	PIN code	User locked	Antipassback	Card expiry date
Smith Patrick	1	Not specified		No	Yes	12/12/2023 12:00:00 AM
Hill Rick	2	Not specified		No	No	Not specified
McDonald Ronald John	4	Not specified		No	Yes	Not specified

6.2.3 Changing the size of interface elements of the Access Manager window

You can change the size of the interface elements of the **Access Manager** window using the mouse. When you hover the mouse cursor over the border between the interface elements of the **Access Manager** window, the cursor takes the form shown in the figure.



You can drag the border between interface elements by holding down 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.

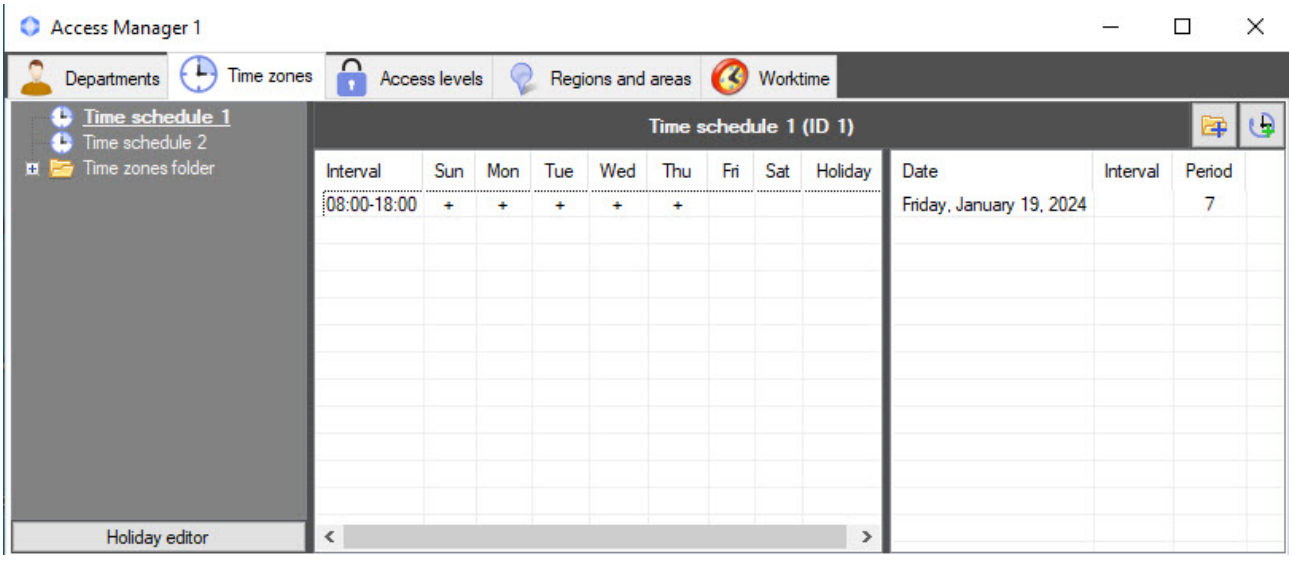
Note

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

You can work with time zones in 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, you can forbid to create, edit, and delete time zones when configuring the *Access Manager* software module (see Rights to access the time zones in the Access Manager).

Time zone is used as time schedule in the *Access Manager* software module. You can set intervals of two types in a time zone:

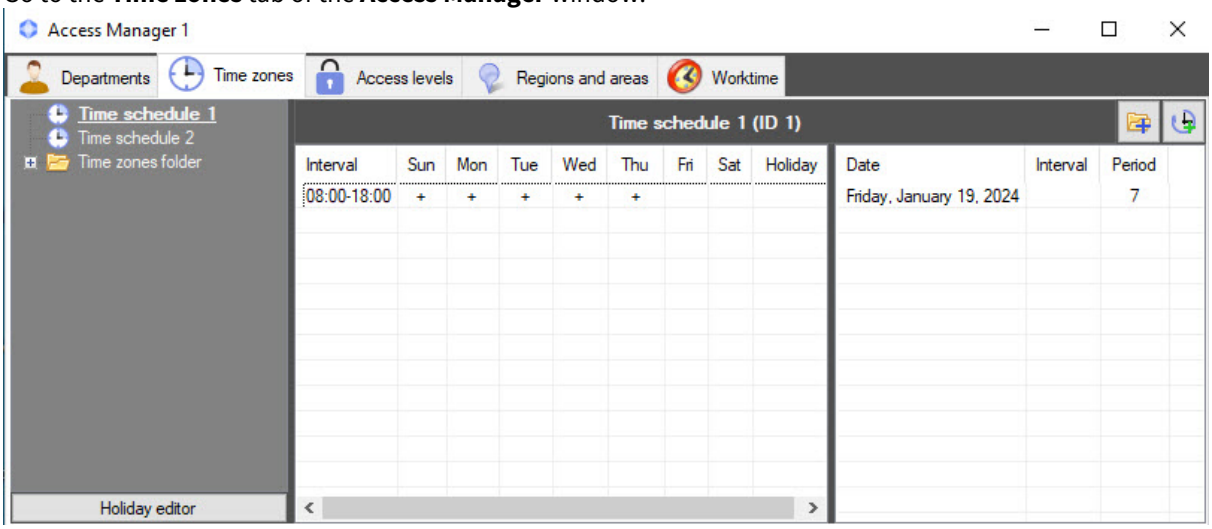
1. Week interval. Time interval is set for specified days of the week.
2. Intervals of shift schedule. Interval is repeated with specified period starting from the specified day.

> **Attention!**
>
> Despite the support for shift schedules in the *Access Manager* software module, few types of hardware support such schedules. In many cases, time zones with shift intervals will be ignored by ACS integrations. The only exception can be those integrations that support operation in the "Access request" mode, in which the hardware requests the integration module to allow access through a certain access point. In this case it is possible to process the check by a complex time zone containing shift schedules.

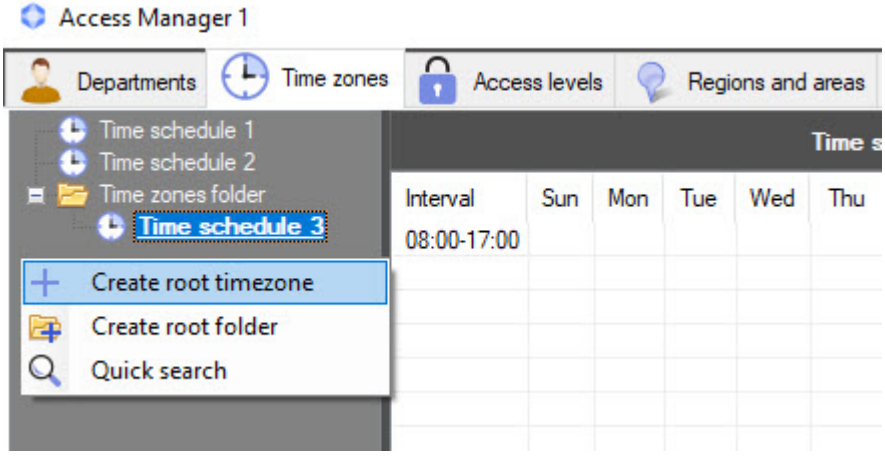
6.3.2 Creating a time zone in the Access Manager software module

To create a time zone, do the following:

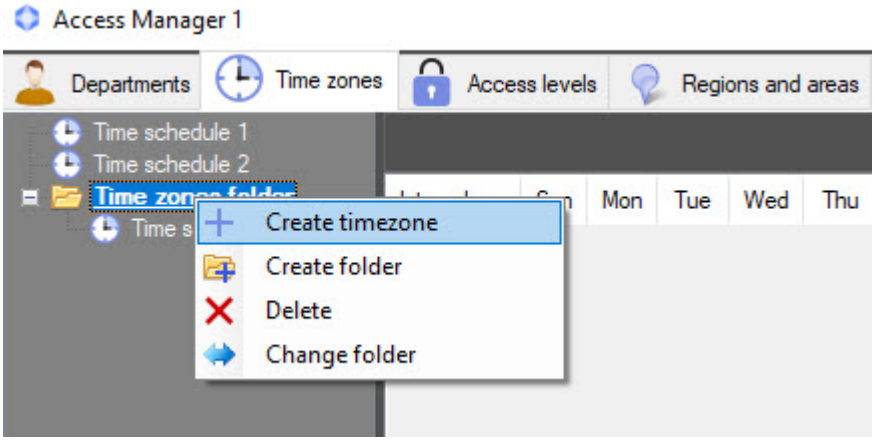
1. Go to the **Time zones** tab of the **Access Manager** window.



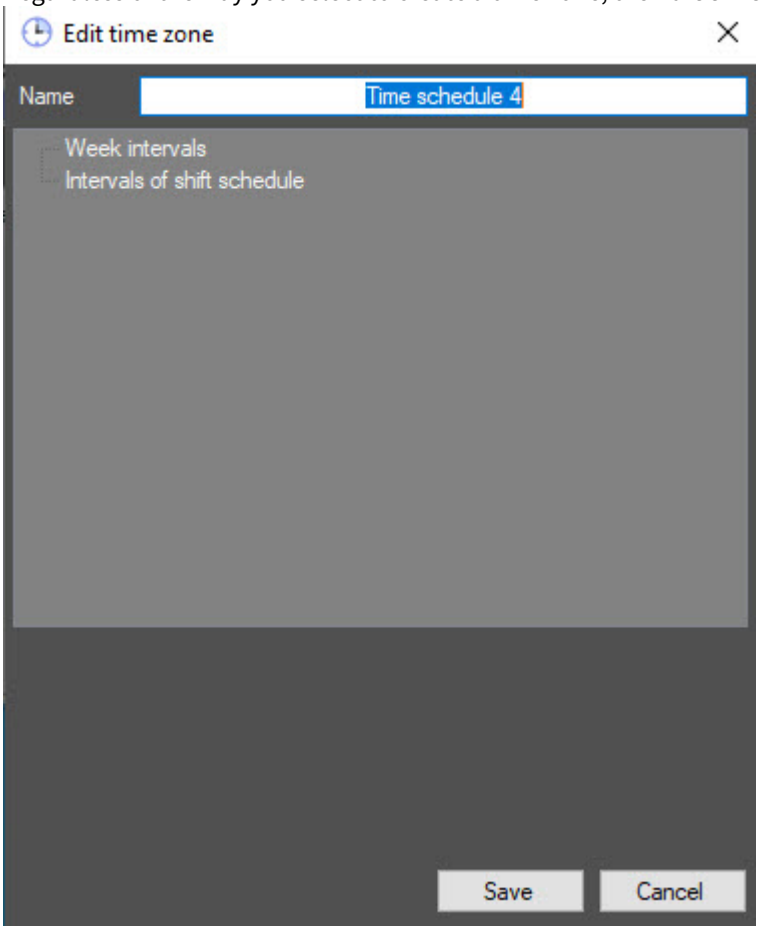
2. There are two ways you can create a new time zone:
   a. Right-click in the free area of the list of time zones and select the **Create root timezone** item in the function menu. In this case, a time zone will be created in the common list of time zones.



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



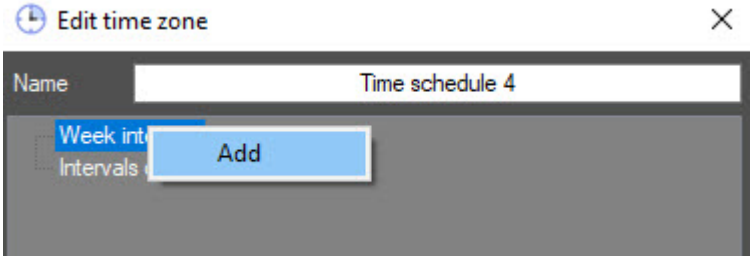
3. Regardless of the way you select to create a time zone, the **Edit time zone** window opens.



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

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

5. If necessary, add week intervals to the time zone:
   a. Right-click the **Week intervals** line and select the **Add** item in the function menu.



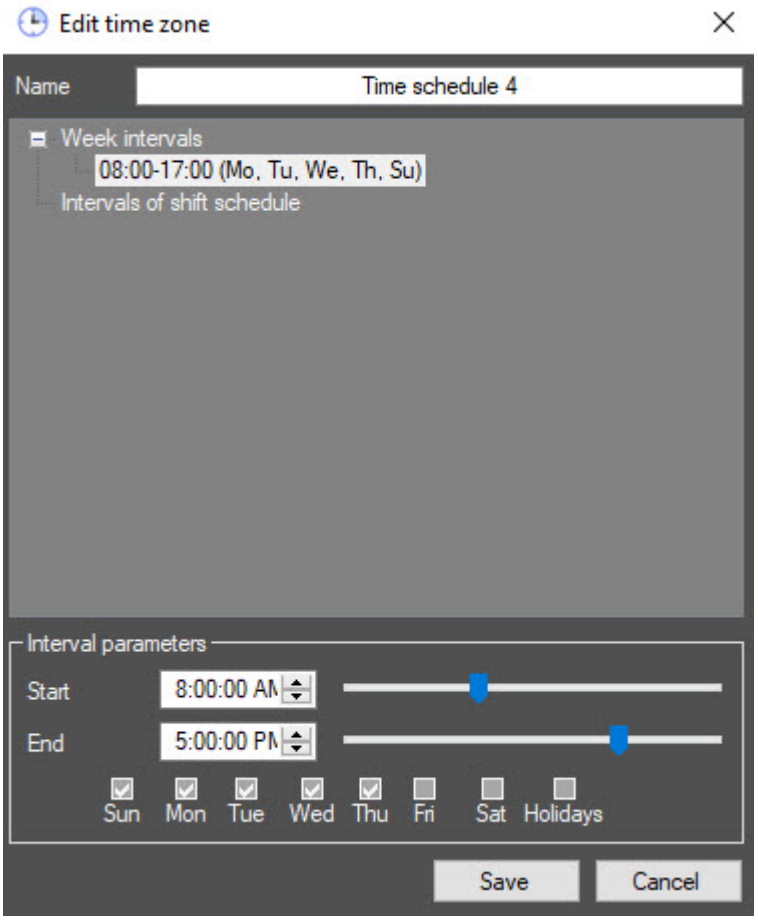
   b. New interval will be created in the **Week intervals** group. Panel for configuring an interval will display at the bottom of the **Edit time zone** window.

> **Note**

Name of the interval is a time period and days in which interval operates in brackets. In addition to days of the week separated by commas, you can specify the following values:

i. Empty interval.
ii. Whole week.
iii. Whole week and on holiday.
iv. On workdays.
v. On workdays and on holiday.
vi. On the weekend and on holiday.
vii. On the weekend.
viii. Only on holiday.

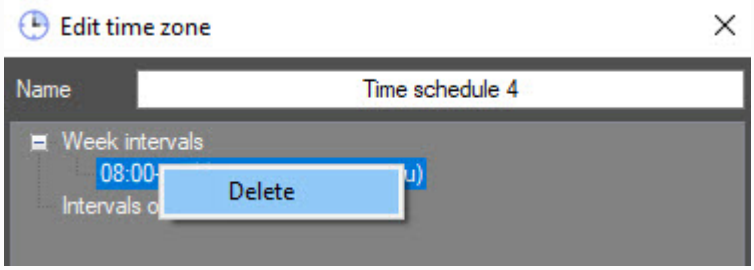
c. In the **Start** field, enter or set using a slider time of interval start.



d. In the **End** field, enter or set using a slider time of interval end.
e. Set checkboxes next to the days on which interval must operate.
f. Set the **Holidays** checkbox, if it's required to include holidays in the interval. Working with holidays is described in Editing holidays.

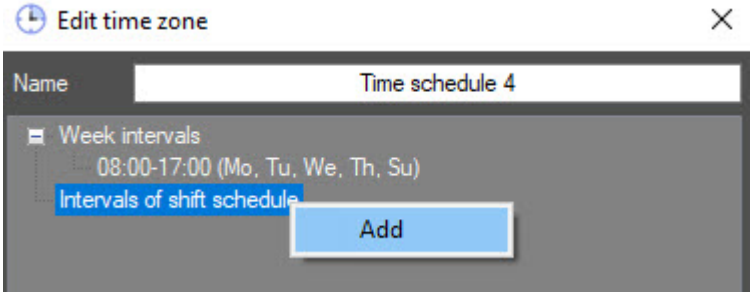
Note

To delete an interval, right-click the interval and select the **Delete** item in the function menu.



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

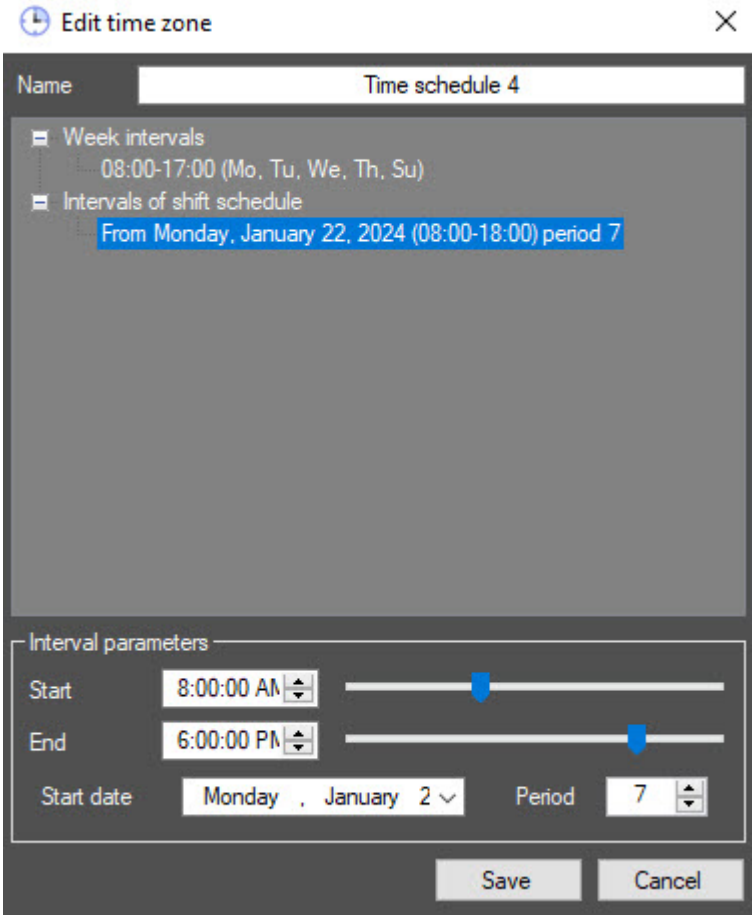
6. If necessary, add intervals of shift schedule to the time zone:
   a. Right-click the **Intervals of shift schedule** line and select the **Add** item in the function menu.



   b. A new interval will be created in the **Intervals of shift schedule** group. Panel for configuring an interval will display at the bottom of the **Edit time zone** window.

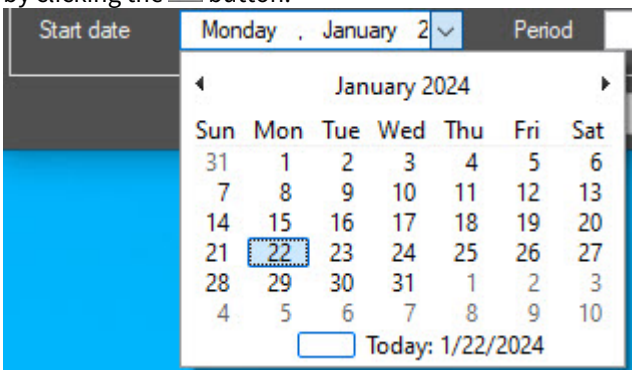
> **Note**
>
> Name of the interval is a date of interval start, time interval and period of interval repetition in days.

c. In the **Start** field, enter or set using a slider time of interval start.



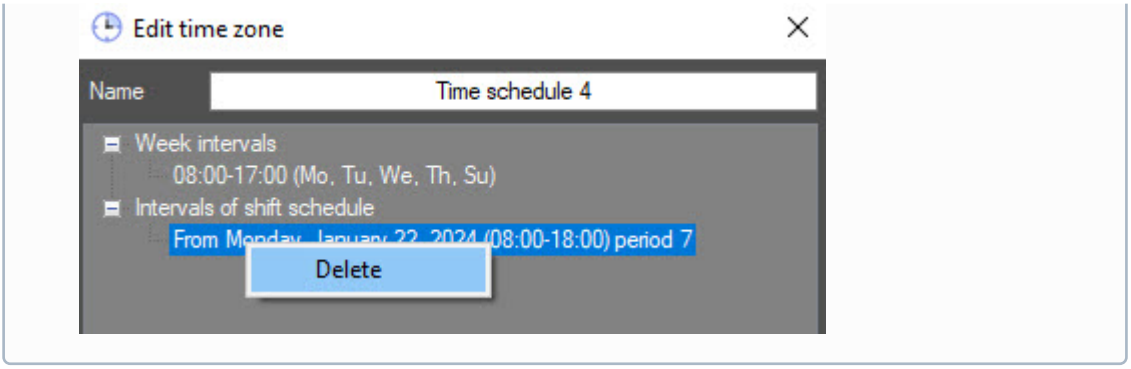
d. In the **End** field, enter or set using a slider time of interval end.

e. In the **Start date** field, enter the start day of shift schedule, using a keyboard or calendar that opens by clicking the button.



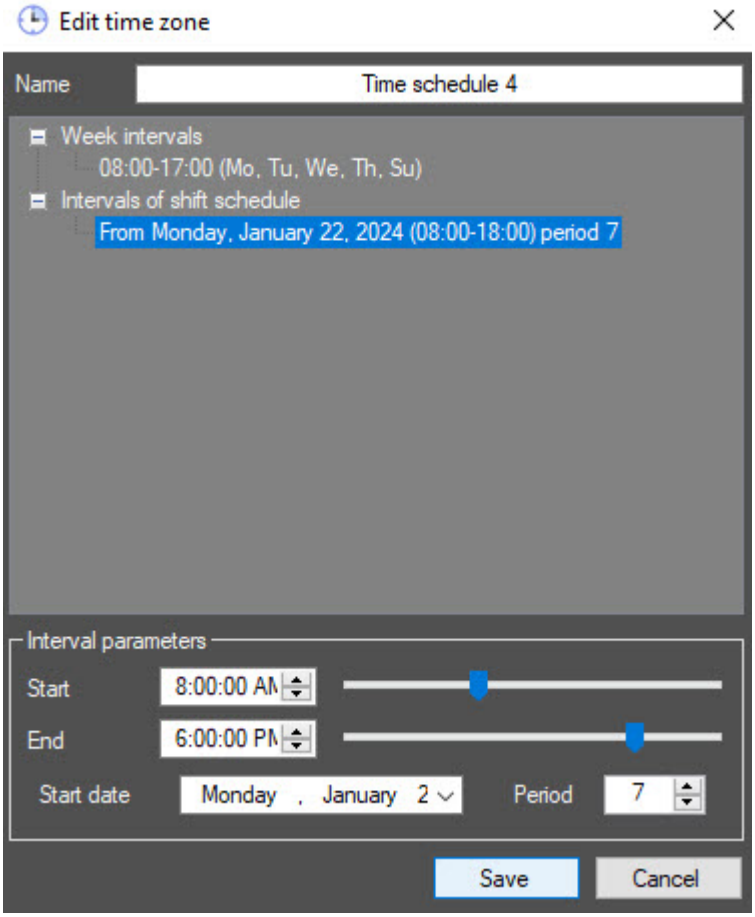
f. In the **Period** field, specify the number of days in which the interval of shift schedule will be repeated.

> **Note**
>
> To delete an interval of shift schedule, right-click the interval and select the **Delete** item in the function menu.

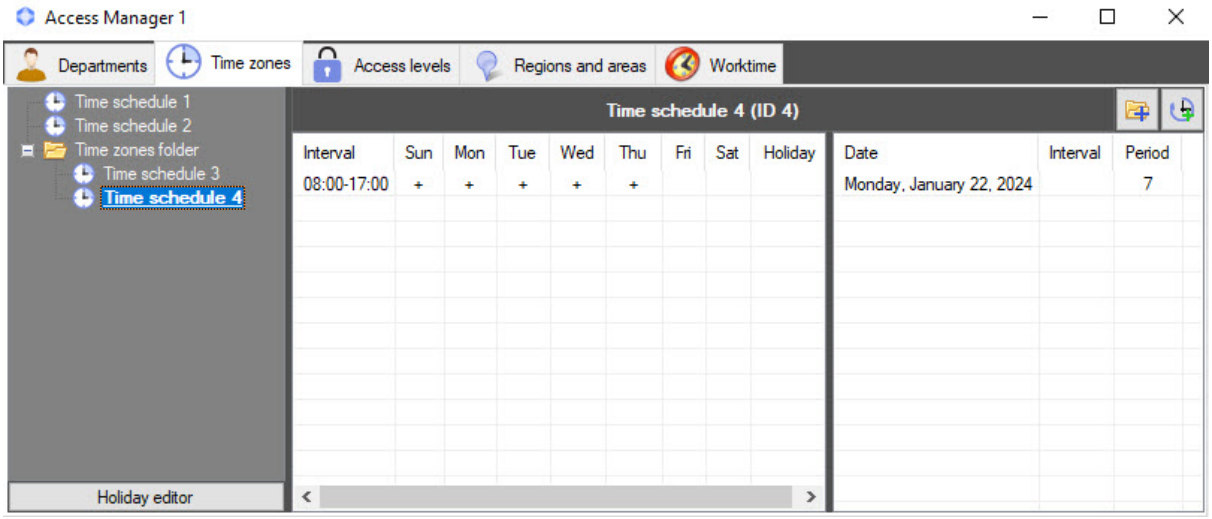


g. Repeat steps a-f for all required intervals of shift schedule.

7. Click the **Save** button.



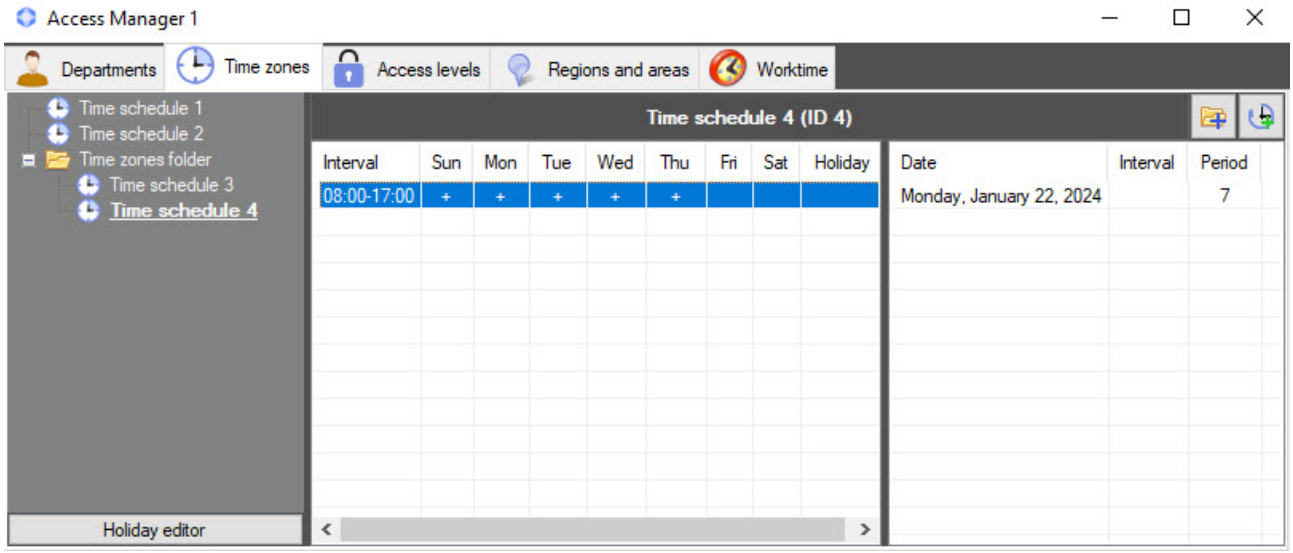
As a result, the created time zone will be displayed in the time zone list.



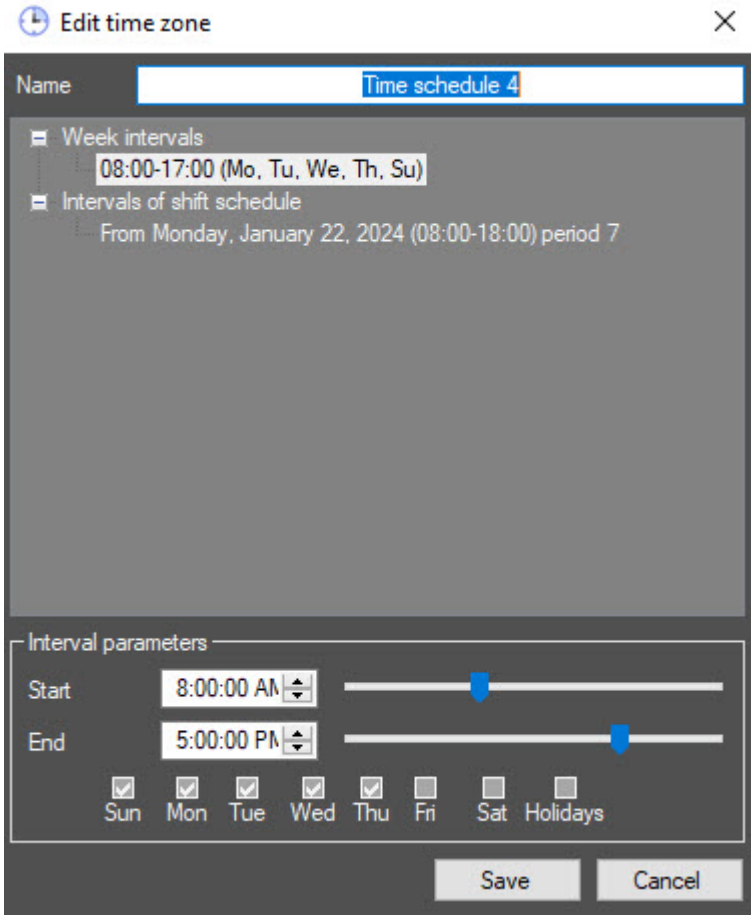
6.3.3 Editing a time zone in the Access Manager software module

Editing a time zone involves adding and deleting intervals from time zone and changing configured intervals. To edit a time zone, double-click the required time zone in the list on the **Time zones** tab. As a result, the **Edit time zone** window opens.

You can also open this window by double-clicking an interval in the list of intervals of the selected time zone.



The interval you clicked is selected in the window that opens. Working with this window is the same as when creating a time zone (see Creating a time zone in the Access Manager software module).

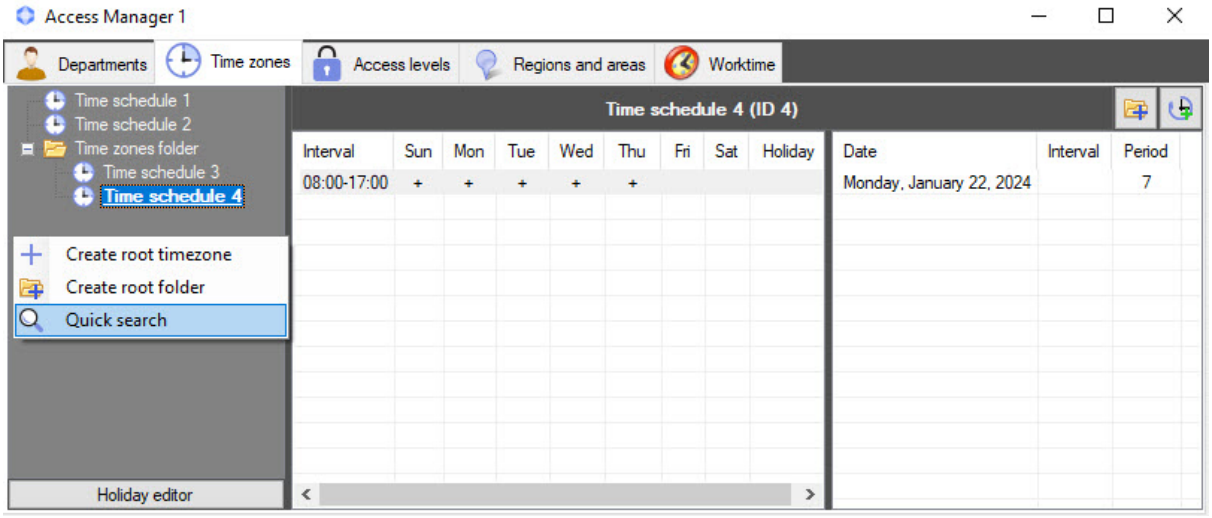


6.3.4 Searching for a time zone

Going to search for a time zone

In the *Access Manager* software module, you can search for a time zone by name and ID. To search for a time zone, do the following:

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



2. Right-click in the free area of time zone list.
3. In the function menu, select the **Quick search** item. The **Search for time zone** window opens.

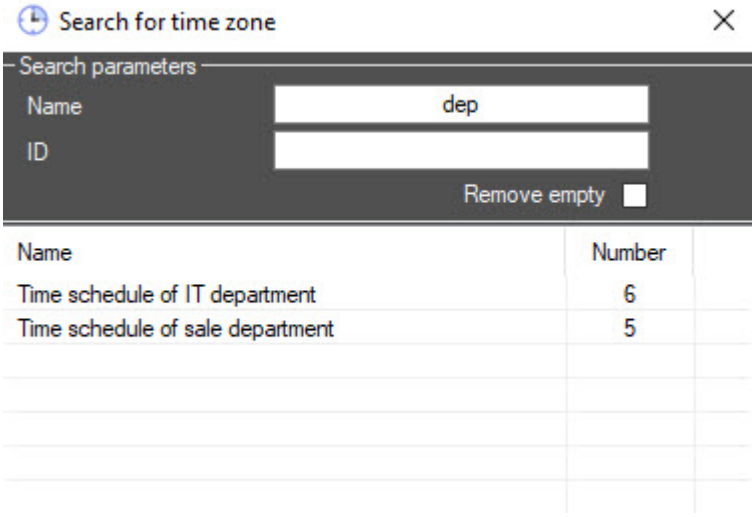
Going to search for a time zone is completed. Working with the **Search for time zone** window is described in Working with the Search for time zone window.

Working with the Search for time zone window

You can open the **Search for time zone** window when searching for a time zone (see Going to search for a time zone) or when configuring an access level (see Creating access levels).

You can work with the **Search for time zone** window as follows:

1. To search for a time zone by its name, enter the name or its part in the **Name** field. If the name of a time zone isn't specified, the search by this field won't be performed.



2. To search for a time zone by its ID, enter the identifier of the required time zone in the **ID** field. If ID isn't specified, the search by this field won't be performed.
3. To exclude from the search the time zones with no intervals added, set the **Remove empty** checkbox.
4. Press the **Enter** key on the keyboard.
   The search results table will display time zones that meet the specified search criteria. The search is case-insensitive. All objects containing the specified values will be found.

To sort search results, left-click the header of the corresponding column.

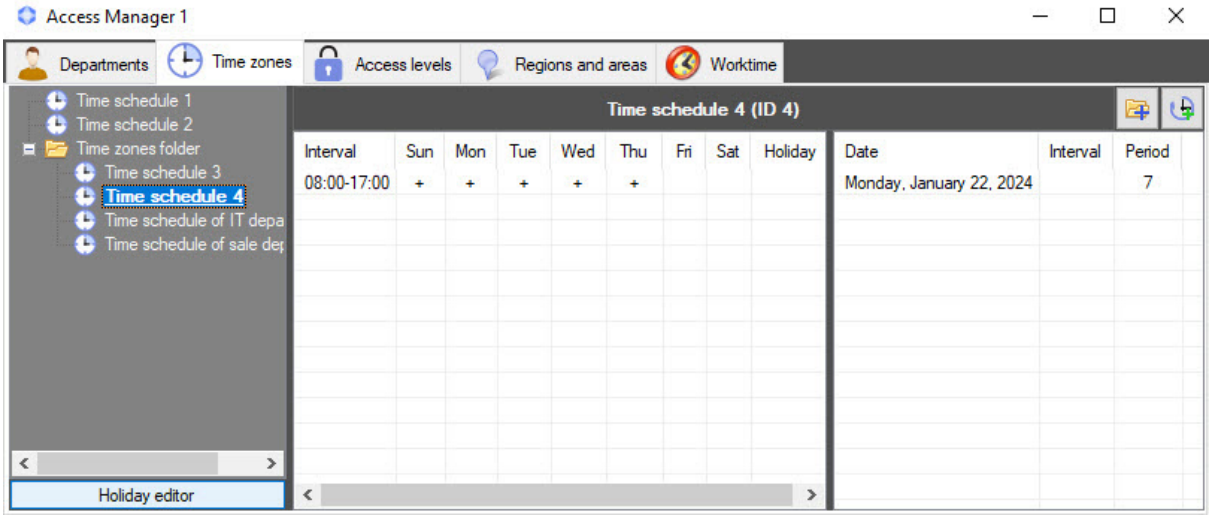
When you double-click a time zone, the **Search for time zone** window will be closed, and the corresponding time zone will be selected in the list in the **Time zones** tab or will be added to a configured access level.

Search for a time zone is completed.

6.3.5 Editing holidays

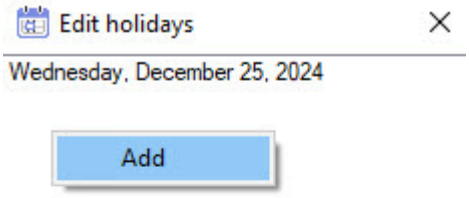
To edit a holiday list, do the following:

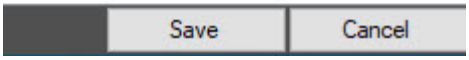
1. Go to the **Time zones** tab of the **Access manager** window.
2. Click the **Holiday editor** button**.**



The **Edit holidays** window containing a list of holidays opens.

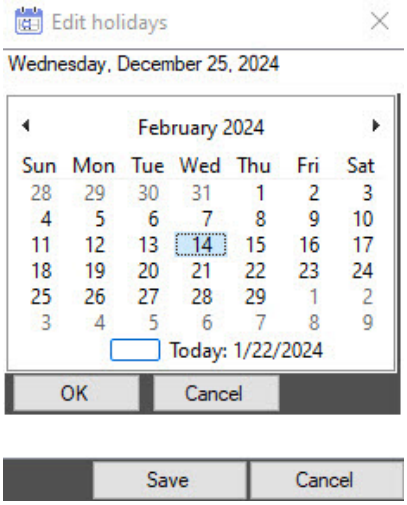
3. To add a holiday, right-click in the free area of holiday list and select the **Add** item in the function menu.



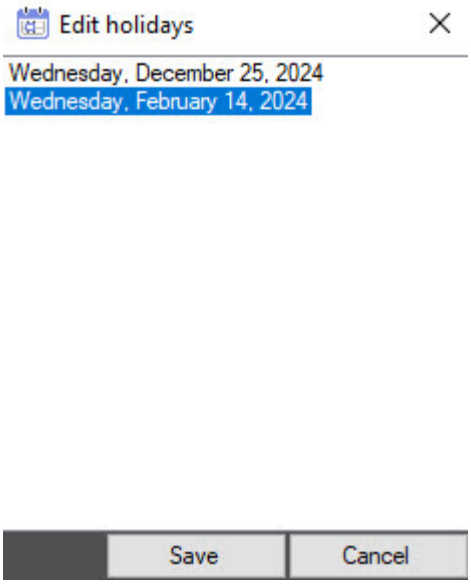


The calendar opens.

4. Select a holiday date in the calendar and click the **OK** button.

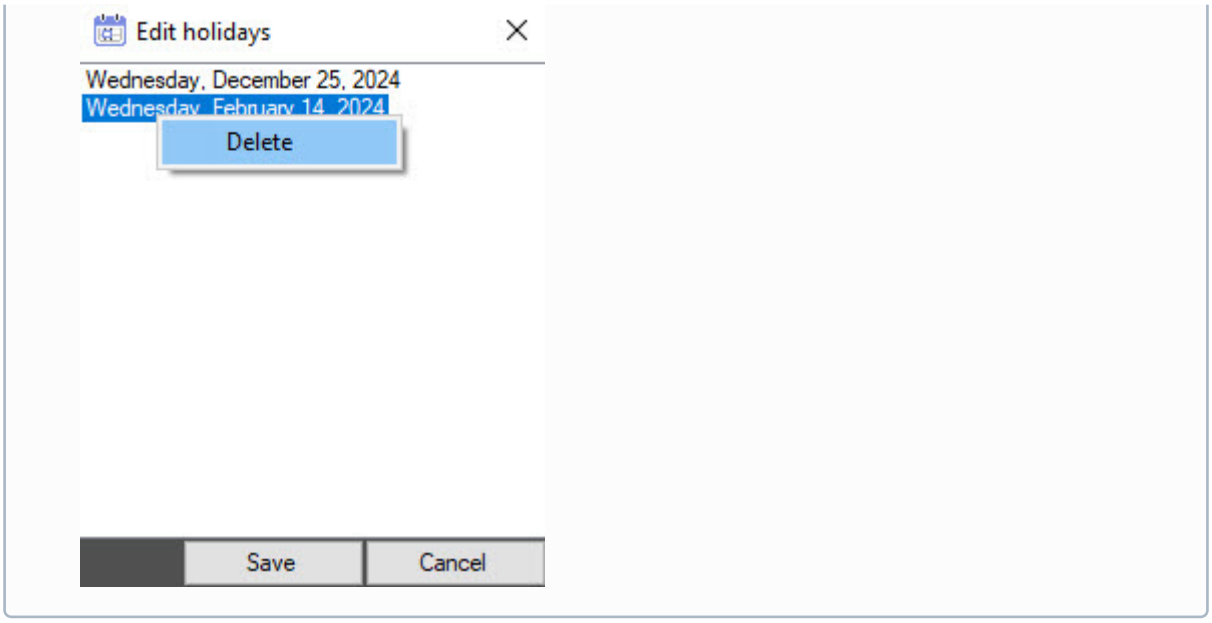


The holiday will be added to the list.

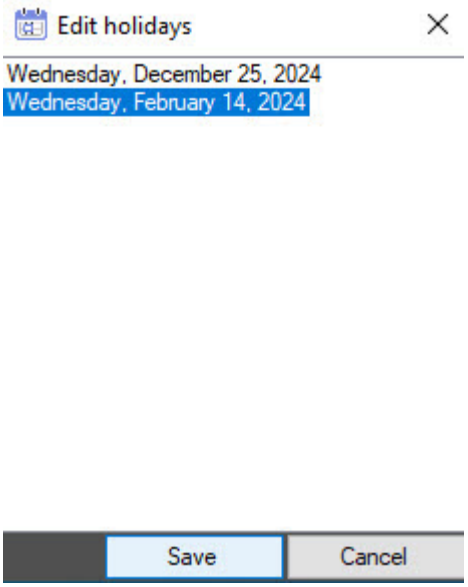


5. Repeat steps 4-5 for all required holidays.

> **Note**
>
> To delete a holiday, right-click it and select the **Delete** item in the function menu.



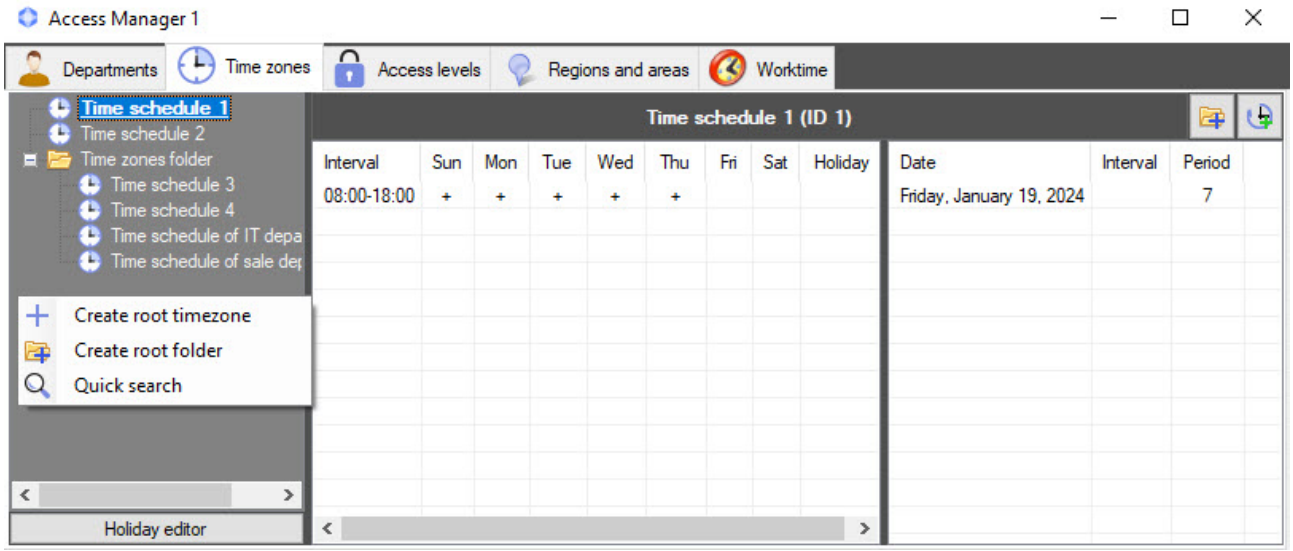
6. Click the **Save** button.



Editing holidays is completed.

6.3.6 Managing a list of time zones

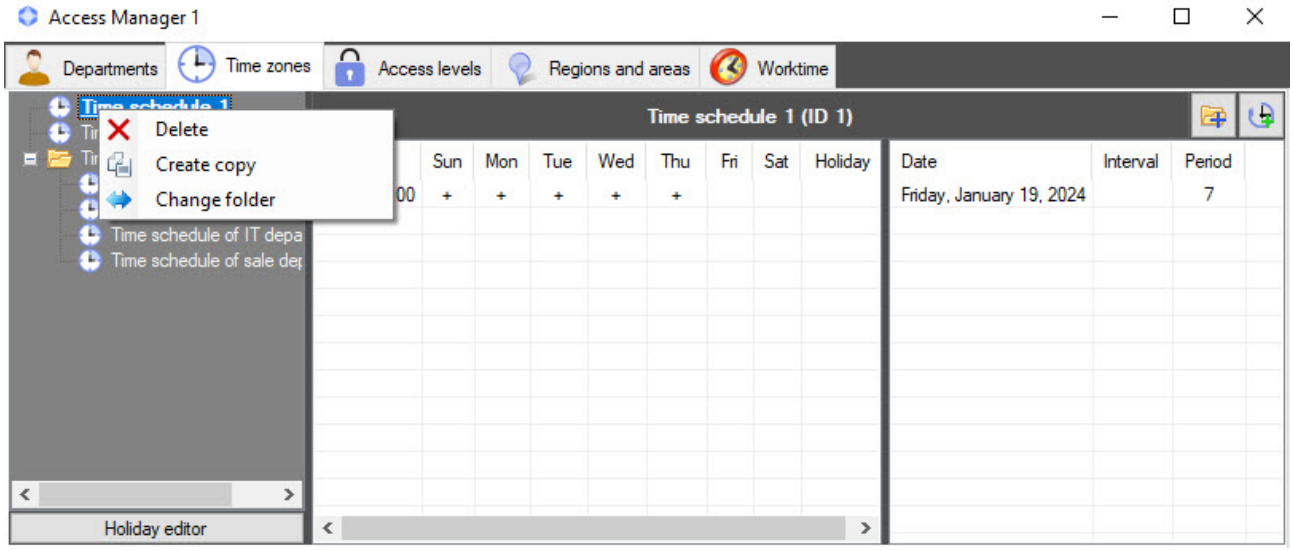
You can manage a list of time zones in the *Access Manager* using the context menu that opens when you right-click in the free area of the list of time zones.



The commands of the context menu described in the table.

Command	Description
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 Creating a time zone in the Access Manager software module
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
Quick search	Opens a window for quick search 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 Searching for a time zone

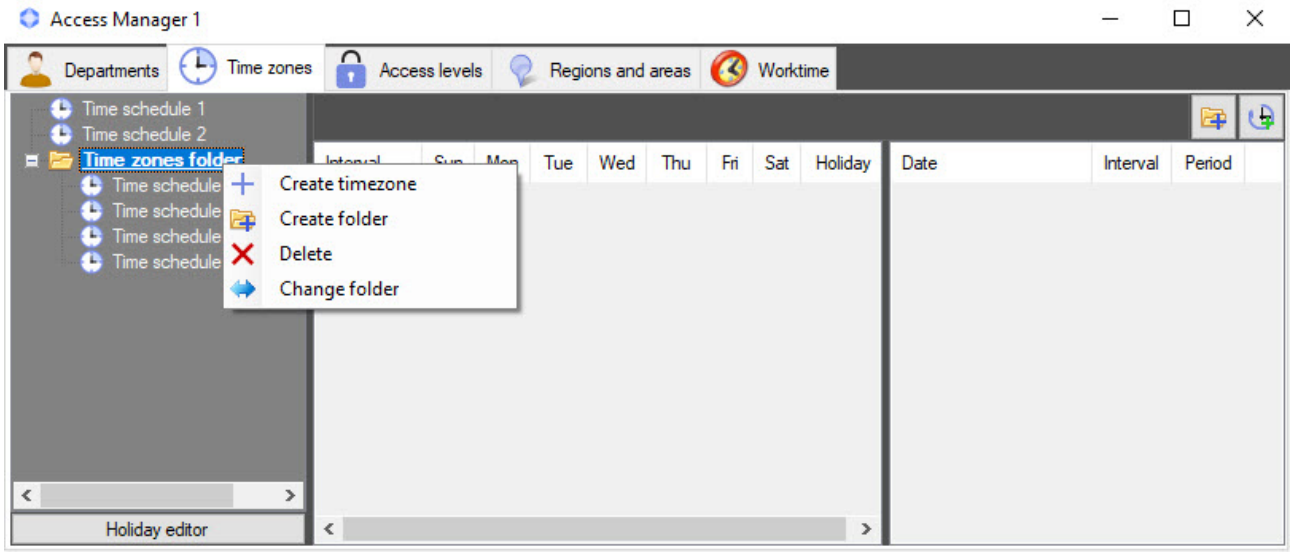
You can manage a separate time zone in the root of the list of time zones using the context menu that opens when you right-click a time zone.



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

Command	Description
Delete	Deletes a time zone after confirmation from the user. If deletion of an assigned time zones is forbidden (see Forbid to delete non-empty departments, assigned access levels, time zones, and identifier owners), then a 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
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
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

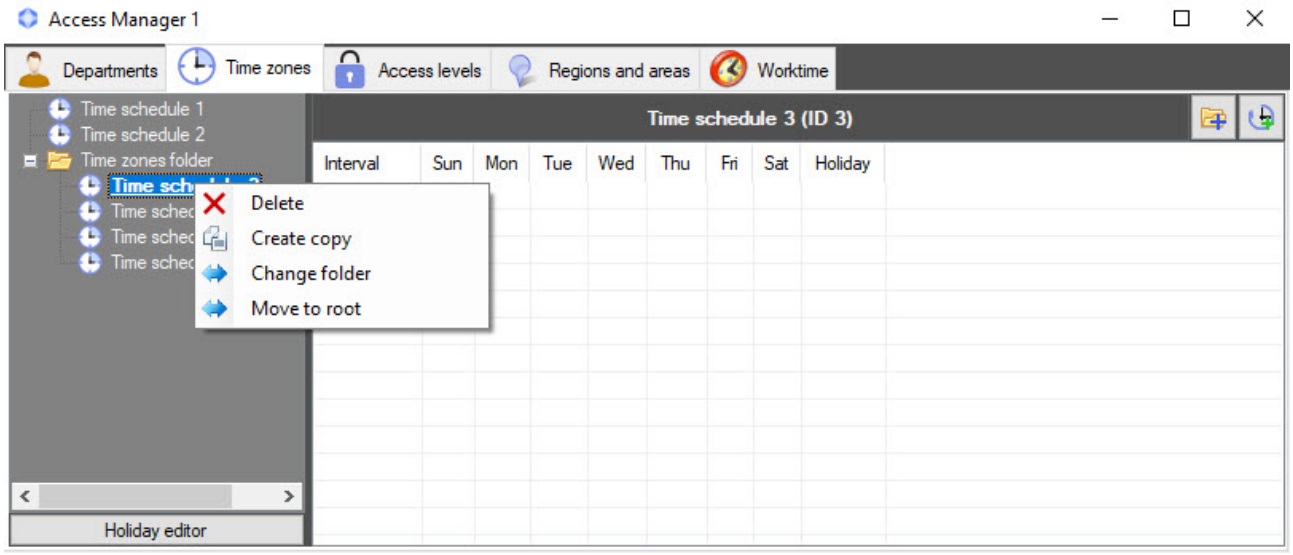
You can manage an individual folder in the list of time zones using the context menu that opens when you right-click the folder.



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

Command	Description
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 Creating a time zone in the Access Manager software module
Create folder	Adds a subfolder. When you select this command, the **Folder options** window opens, where you can specify a name for a new folder
Delete	Deletes the folder after confirmation from the user. If deletion of assigned time zones is forbidden (see Forbid to delete non-empty departments, assigned access levels, time zones, and identifier owners), 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
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

You can manage a separate time zone located inside a folder, using the context menu that opens when you right-click a time zone.



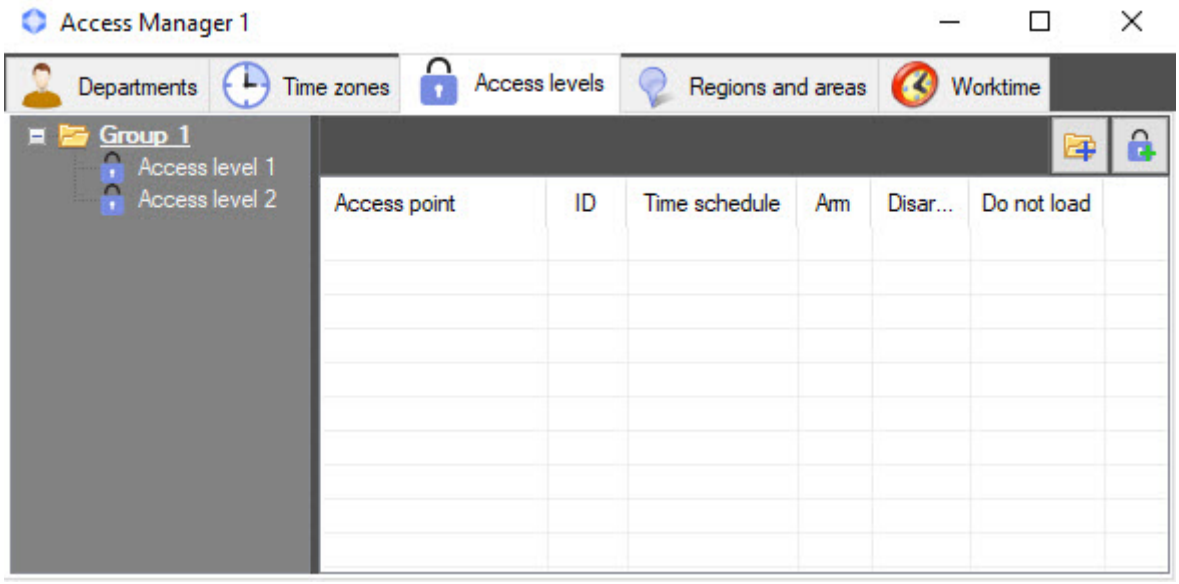
The commands of the context menu are described in the table.

Command	Description
Delete	Deletes the time zone after confirmation from the user. If deletion of an assigned time zones is forbidden (see Forbid to delete non-empty departments, assigned access levels, time zones, and identifier owners), 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
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
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
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

You can work with access levels on the **Access levels** tab in the **Access Manager** window.

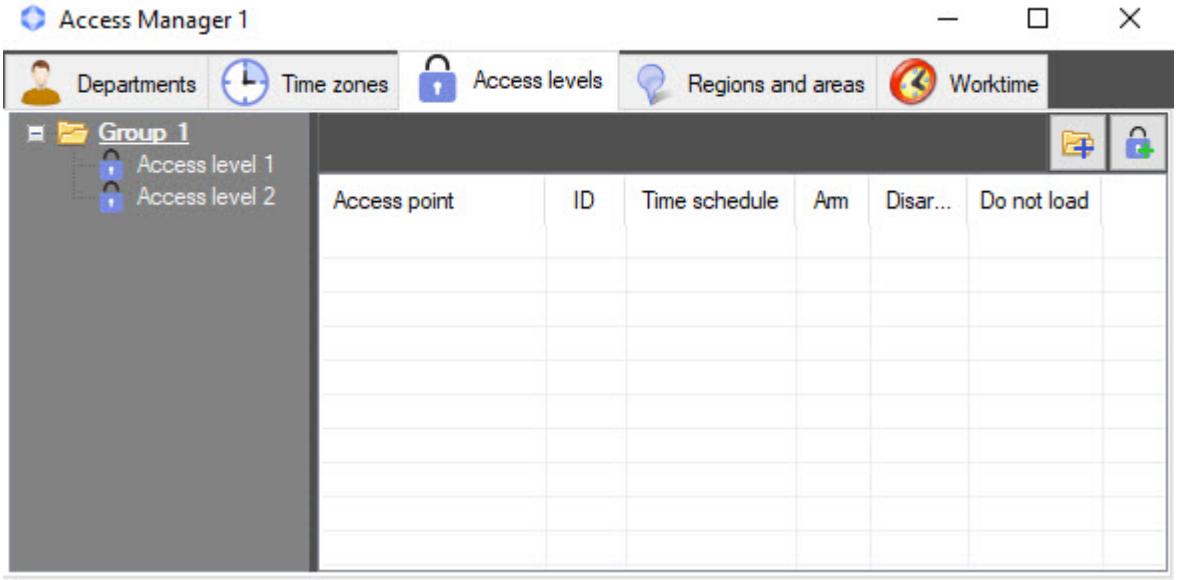


The *Access Manager* software module allows creating, editing, copying, viewing, and deleting access levels. The possibility of creating, editing and deleting access levels can be forbidden when configuring the *Access Manager* software module—see Rights to access the access levels in the Access Manager.

6.4.2 Creating access levels

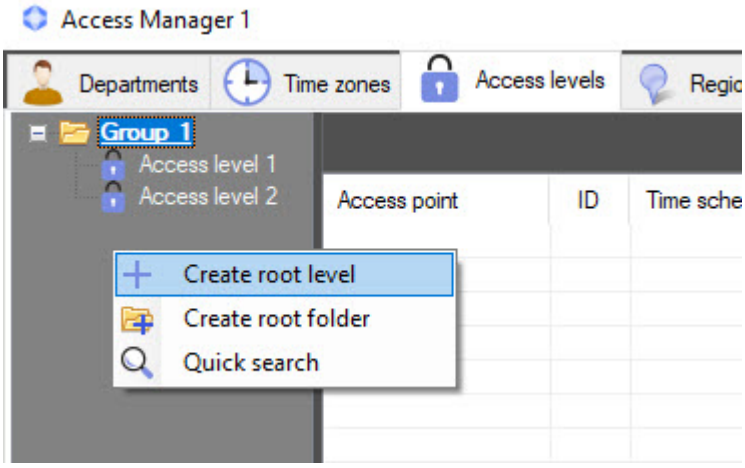
To create an access level, do the following:

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

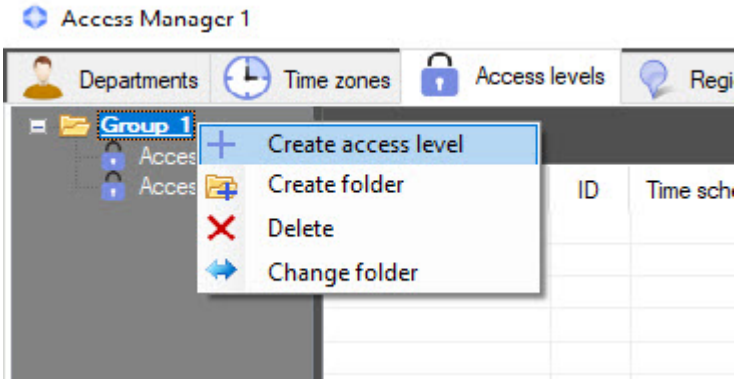


2. There are two ways you can create a new access level:

a. Right-click in the free area of the access level list and select **Create root level** item in the function 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. In this case, the access level will be created in the selected folder.



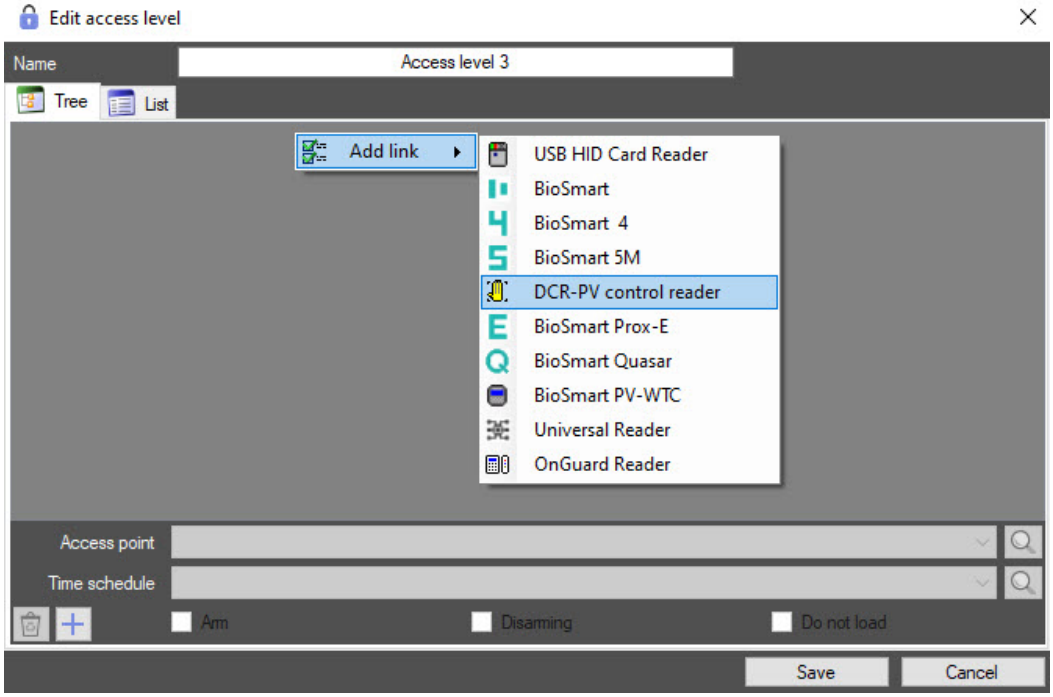
3. If you select any of the commands, the **Edit access level** window will open. In the window, do the following:

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

   > **Note**
   >
   > The name must 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 must not contain the following characters: < | >.

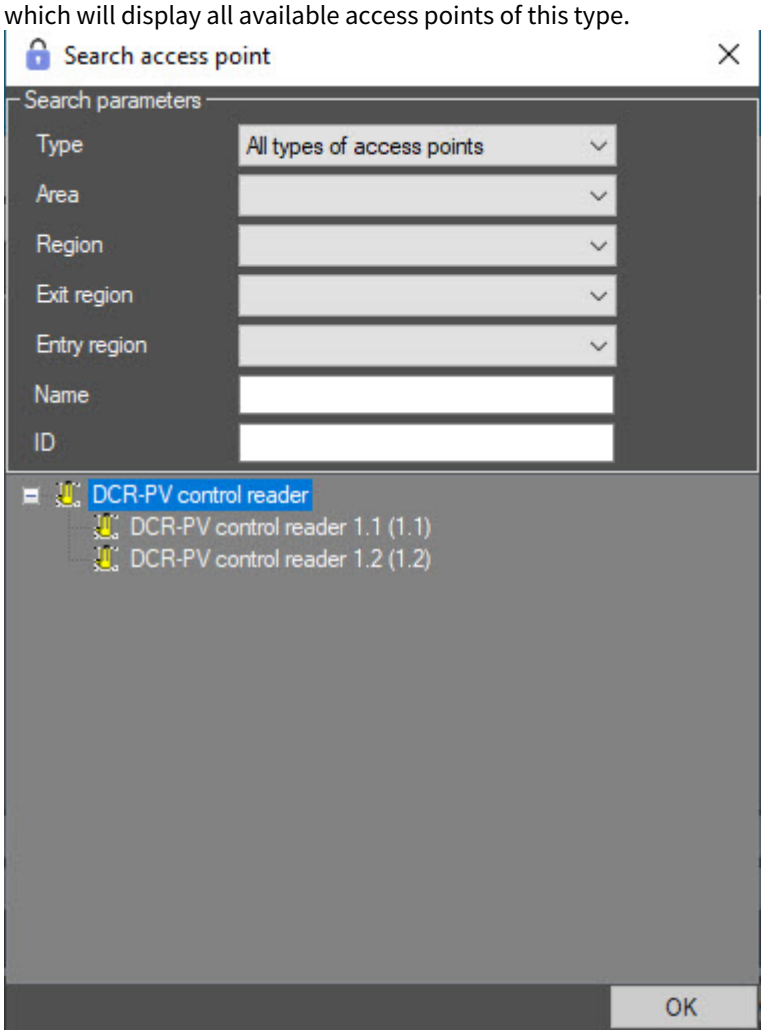
   b. In the free area of the list of access rules, add a rule that links the access point with the time schedule:

i. Right-click in a free area of the list of access rules and in the **Add link** function 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.

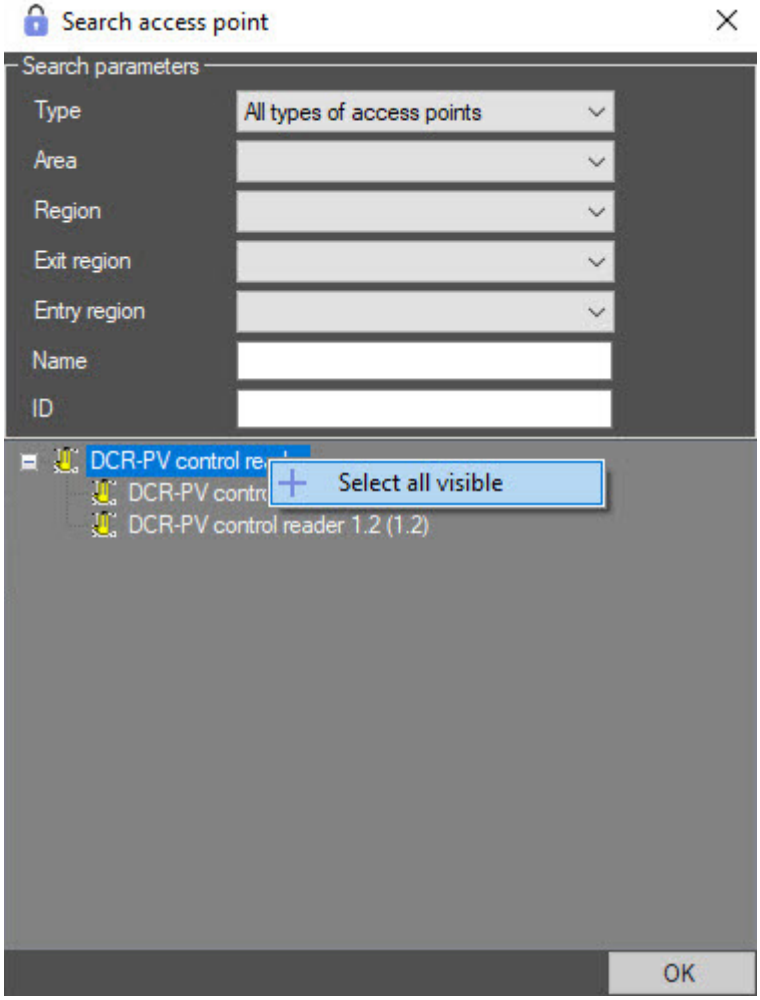
iii. If there are several access points of this type, then the **Search access point** window will open, which will display all available access points of this type.



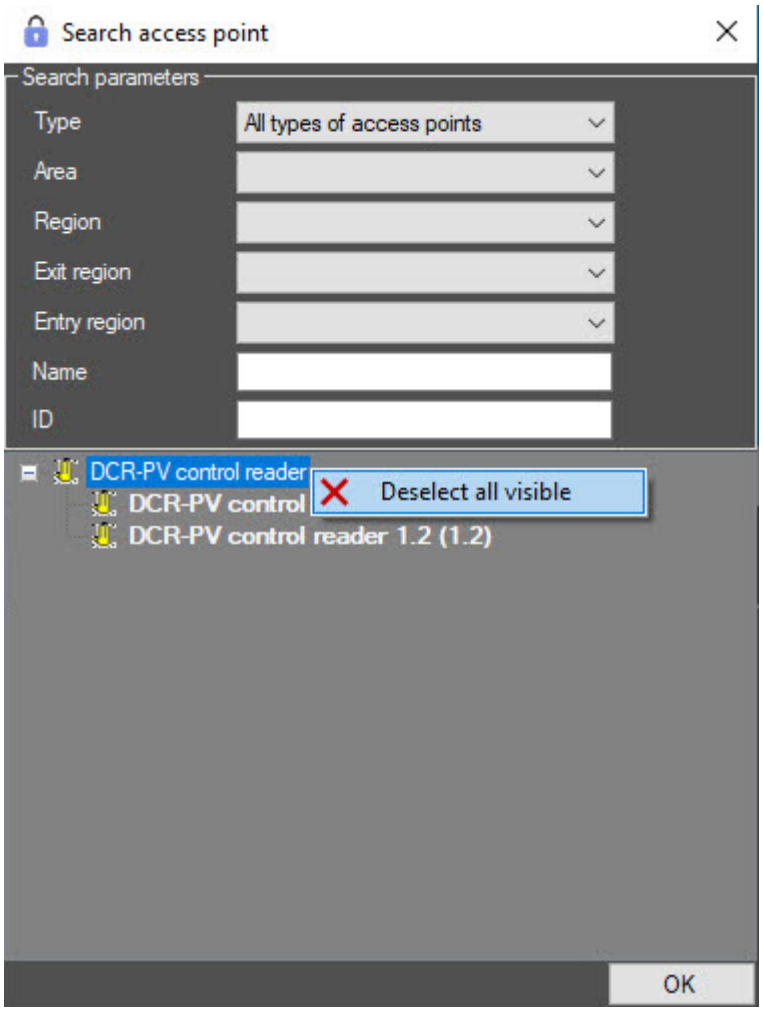
iv. The suitable access points are searched automatically as you specify the search parameters. The search is case insensitive. To search and select an access point, do the following:
   - Select type of access point from the **Type** drop-down list. The default value is **All types of access points**.
   - Select the value from the **Area** drop-down list to search for an access point by area.
   - Select the value from the **Region** drop-down list to search for an access point by region.
   - Select the value from the **Exit region** drop-down list to search for an access point by exit region.
   - Select the value from the **Entry region** drop-down list to search for an access point by entry region.
   - Enter the name of the access point or its part in the **Name** field to search for an access point by its name.
   - Enter the ID of the access point in the **ID** field to search for an access point by its ID.
   - After completing the selection of access points, click the **OK** button.

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

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



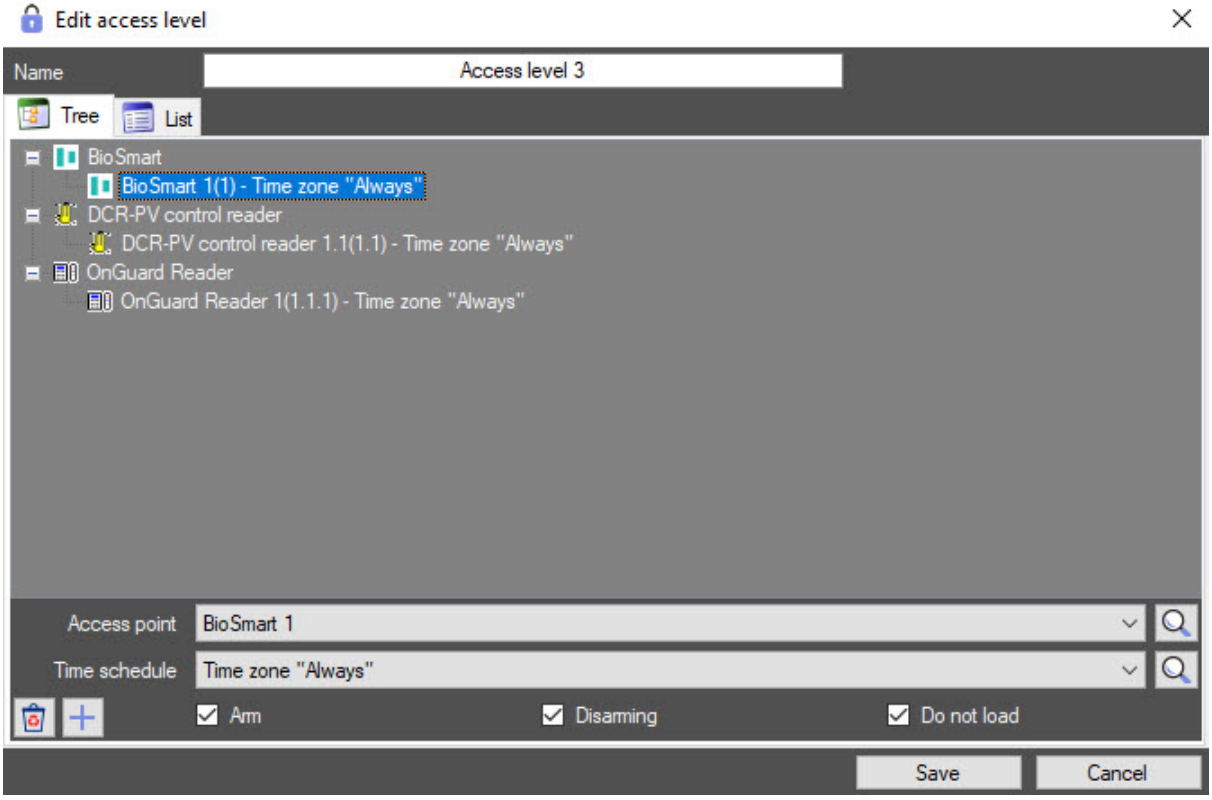
vii. You can deselect all selected access points by right-clicking the parent object to open the **Deselect all visible** function menu.



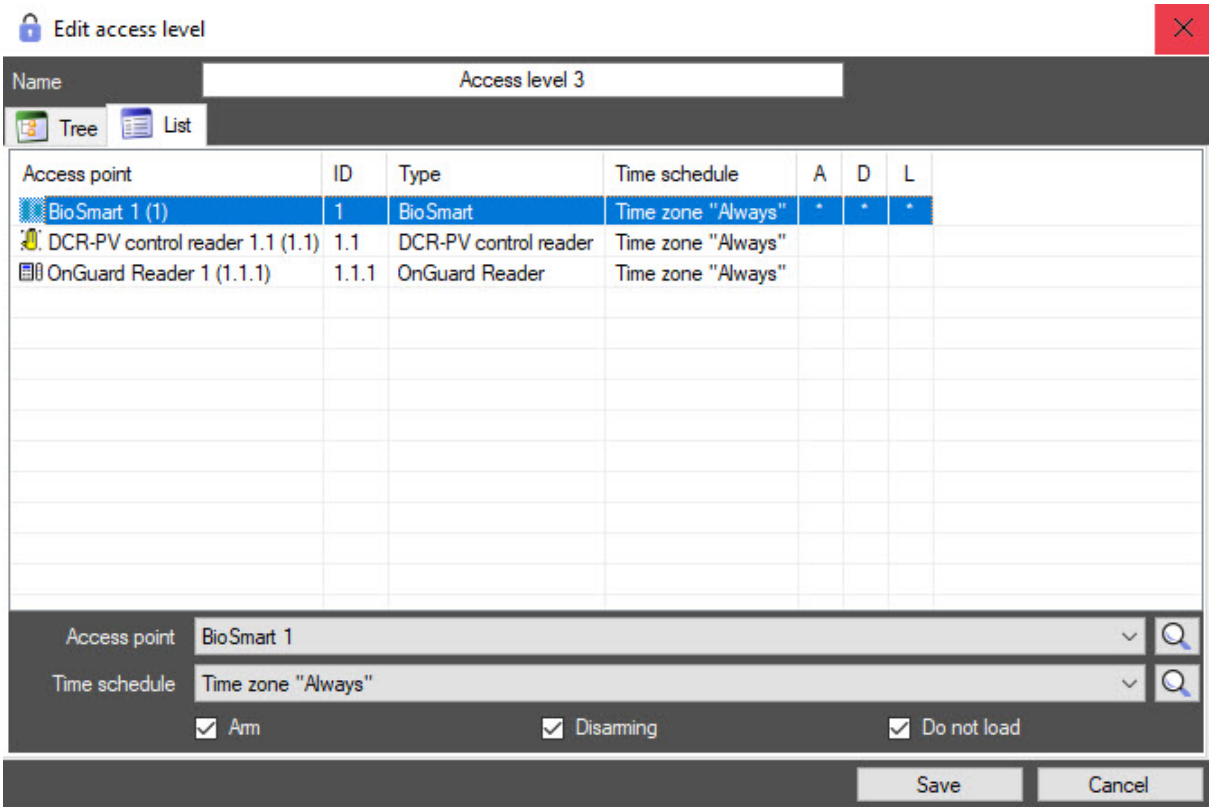
Note

- The **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.
   Access levels have two types of display: **Tree** and **List**.
   The tree of access levels looks like this.

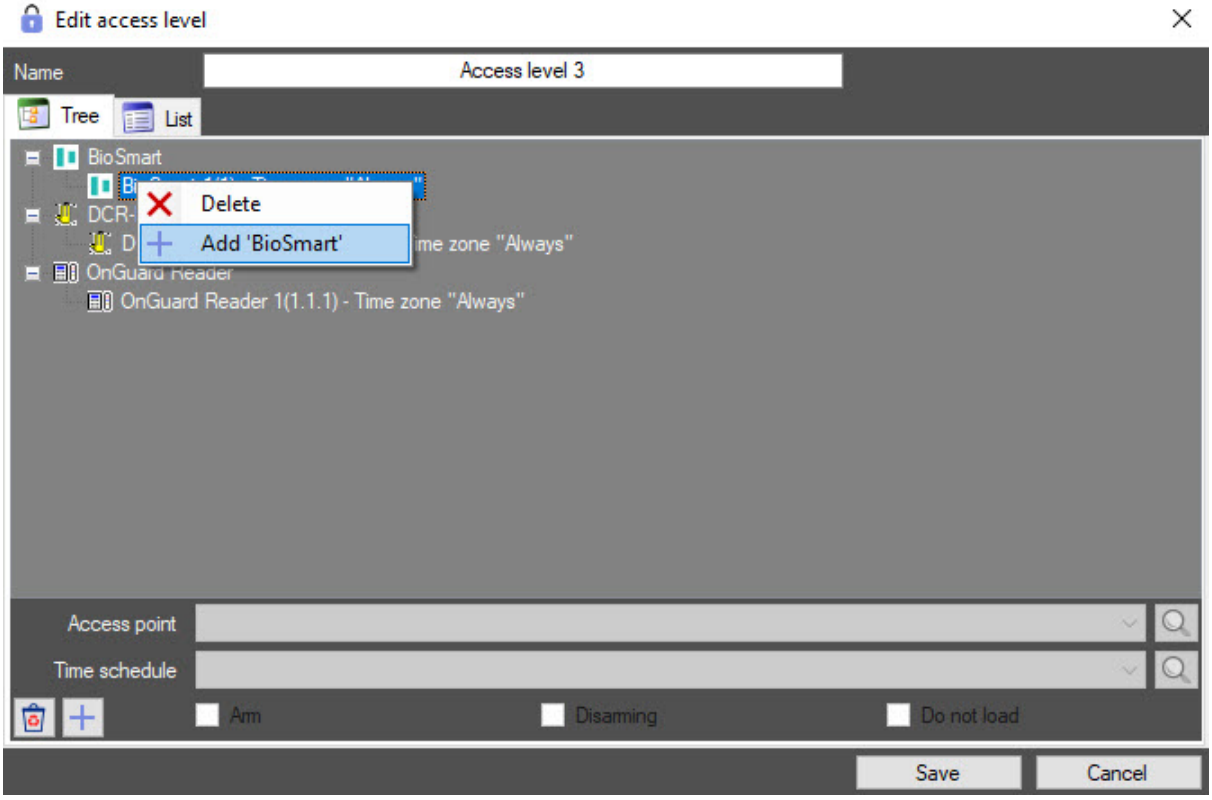


The list of access levels looks like this.



5. Access point is selected in the **Access point** drop-down list. You can change it if necessary.

6. If you want to search for an access point, click the button (the **Search access point** window will open) and go to step 3bii. You can also open the search window using the **Add** button or by right-clicking the selected access point to open the context menu.



> **Note**
>
> To delete all selected access points, click the button.

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

> **Note**
>
> Time schedules are created and configured on the **Time zones** tab of the **Access Manager** window —see Working with time zones in the Access Manager software module. You can also use the system time zones "Always" and "Never".

9. Set the **Arm** checkbox to arm the access point after a user presents an access card.
10. Set the **Disarming** checkbox to disarm the access point after a user presents an access card.
11. If it's not required to send access cards to a controller after a user presents an access card, set the **Do not load** checkbox.

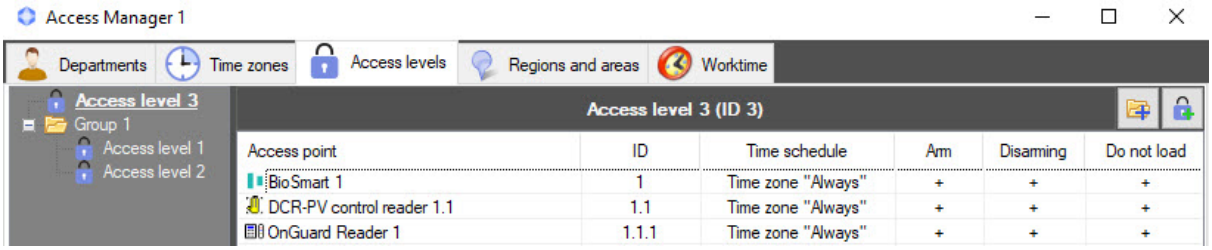
> **Attention!**

Functions of arming, disarming and sending access cards to a controller must be supported by hardware.

Note

Function of the **Do not load** checkbox can differ depending on the integration module that you 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. As a result, the created access level will be displayed in the list of access levels.



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.

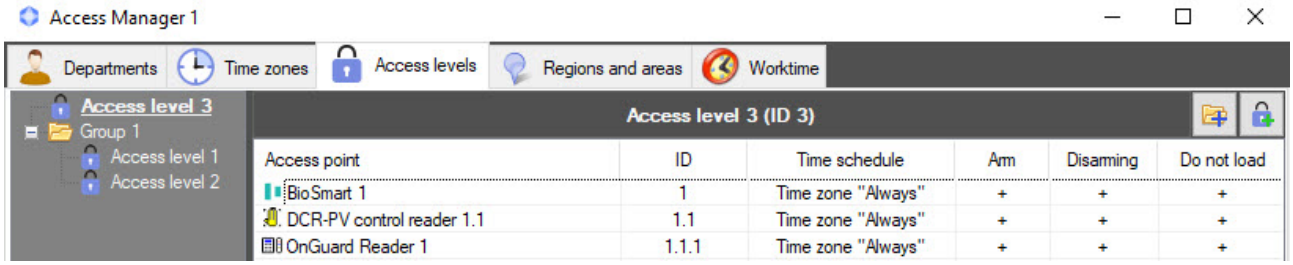
The creation of the access level is complete.

6.4.3 Editing an access level in the Access Manager software module

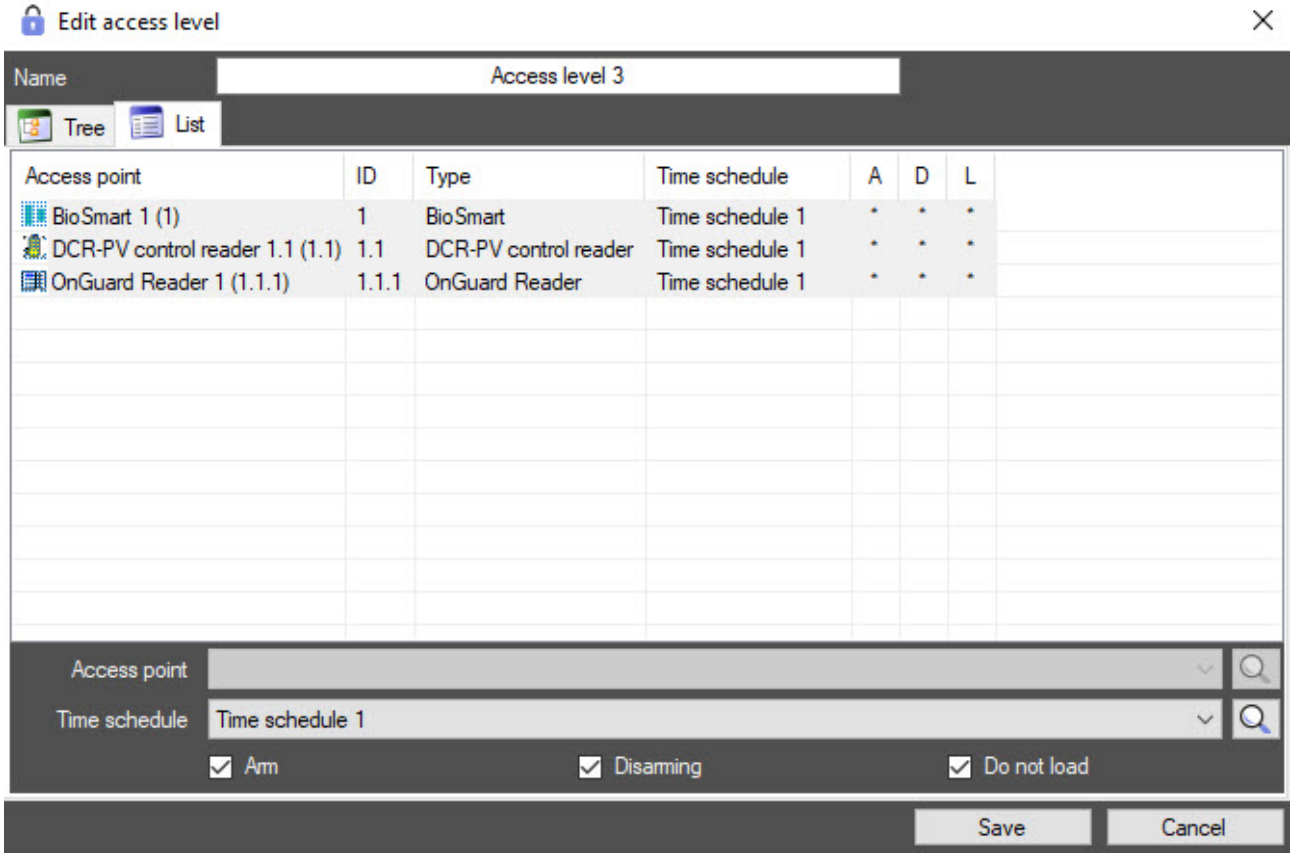
Editing an access level includes adding, deleting and changing links. To edit an access level, double-click the required access level in the list on the **Access levels** tab or double-click the name of access point in the table of access level parameters.

Note

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



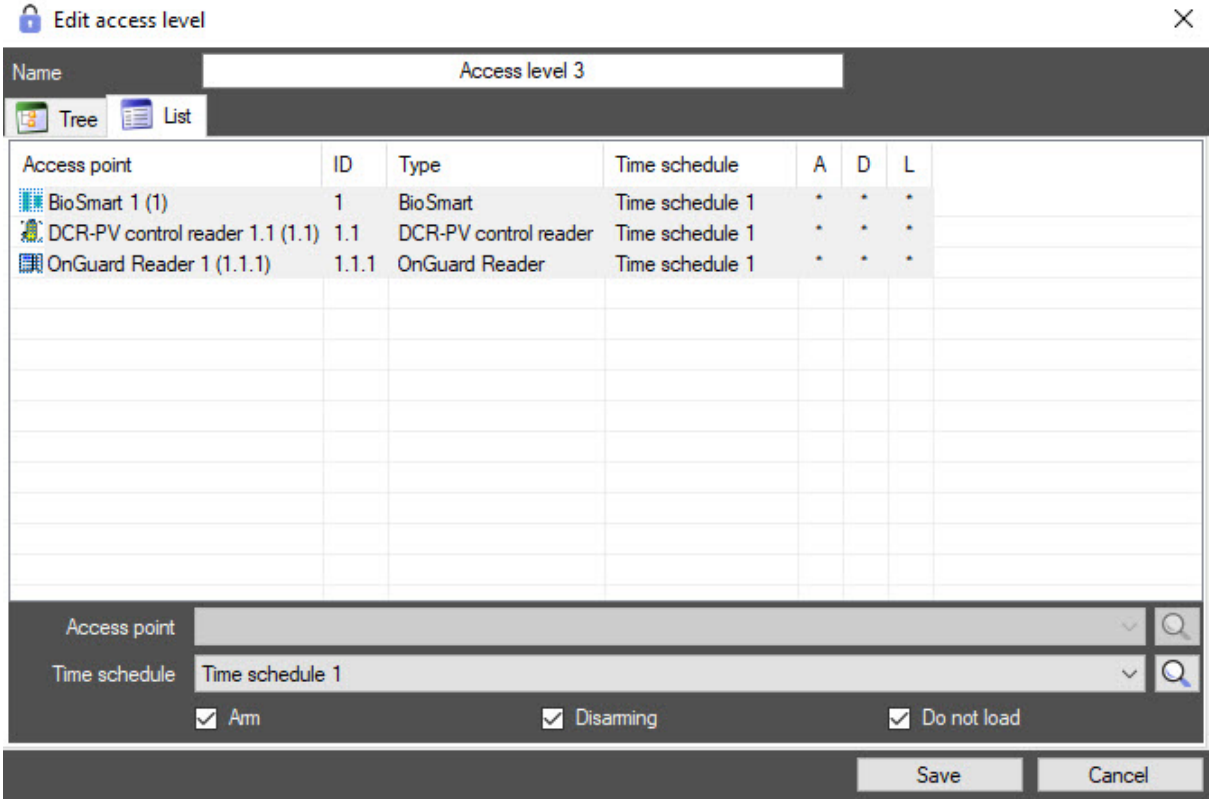
As a result, the **Edit access levels** window will open. You can work with this window the same as when creating an access level—see Create access level.



In *ACFA PSIM*, you can assign one time schedule to several access points. To do this, do the following:

1. In the **Edit access level** window, select the **List** option of data display.
2. Hold down the Shift key and select all access points that you want to edit.

3. From the **Time schedule** drop-down list, select the required time schedule. As a result, this time schedul will be assigned to all selected access points.

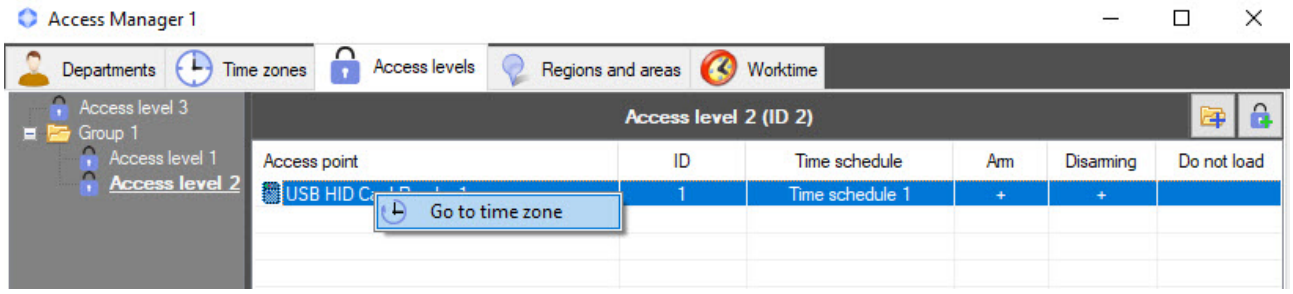


4. Click the **Save** button to save the changes.

Assigning a time schedule to several access points is complete.

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 is associated with the access point (not **Always** or **Never**), you can go to this time zone on the **Time zones** tab. Right-click the required access point and select **Go to time zone** in the function menu.



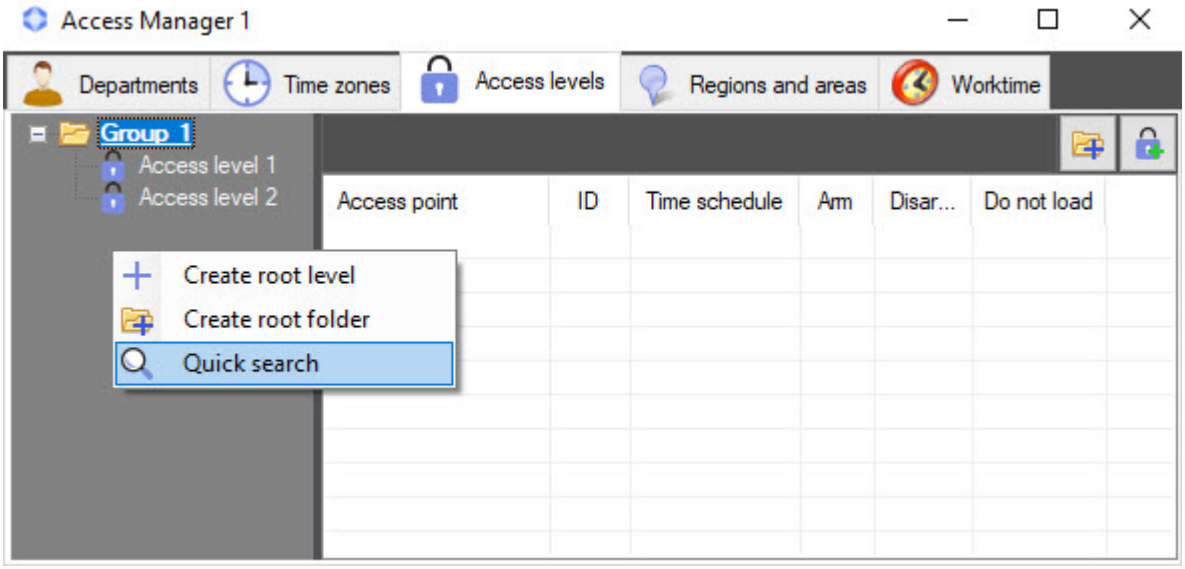
As a result, the **Time zones** tab will open with the required zone selected.

6.4.5 Search for access level

Going to search for an access level

In the *Access Manager* software module, you can search for access level by name, ID and access point. To go to search for an access level, do the following:

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



2. Right-click in a free area of access levels list.
3. Select the **Quick search** item in the function menu. For details on working with the function menu of the **Access levels** tab, see Managing the list of access levels.
4. The **Search access level** window will open.

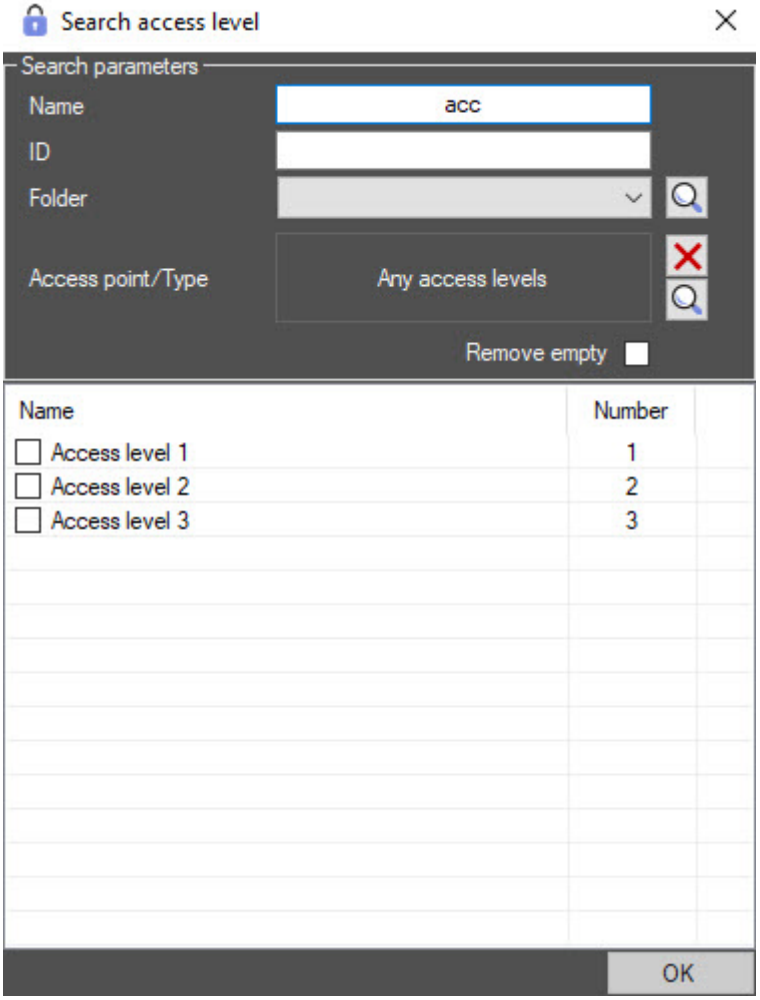
Going to search for an access level is completed. Working with the **Search for access level** window is described in Working with the Search for access level window.

Working with the Search access level window

You can open the **Search access level** window when searching for an access level (see Going to search for an access level), when configuring a department (see Adding and deleting a department), when searching for a department (see Working with the Search for department window), or when configuring a user (see Assigning access levels to a user).

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

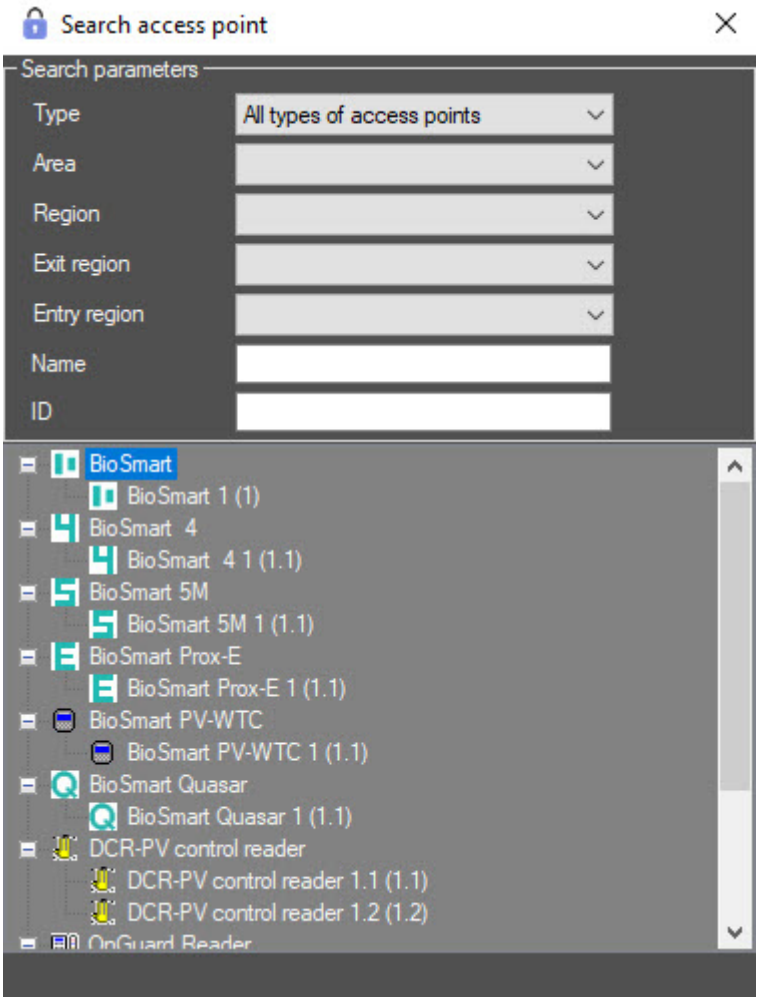
1. To search by the name, enter the name of the required access level or part of the name in the **Name** field. The search starts with the first character.



2. To search by the ID, enter the identification number of the required access level in the **ID** field.
3. To search by the folder in which the access level is located, select the folder from the **Folder** drop-down list.

   You can also use the search by clicking the  button to the right of this list.
4. You can find the access level by the access point that belongs to it:

a. Click the button to the right of the **Access point/Type** button. The **Search access point** window will open.



b. Select type of the access point from the **Type** drop-down list.
c. Select the value from the **Area** drop-down list to search for an access point by area.
d. Select the value from the **Region** drop-down list to search for an access point by region.
e. Select the value from the **Exit region** drop-down list to search for an access point by exit region.
f. Select the value from the **Entry region** drop-down list to search for an access point by entry region.
g. Enter the name of the access point or its part in the **Name** field to search for an access point by its name.
h. Enter the ID of the access point in the **ID** field to search for an access point by its ID.
i. To search for access points that meet the specified parameters, press the Enter key on the keyboard. The list of search results will be displayed below.
j. Double-click the required access point in the list.

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

5. To remove access levels not associated with any access points from the search results, set the **Remove empty** checkbox.

6. Press the Enter key on the keyboard.
7. Results of the access levels search will be displayed in the list. The search is case insensitive. All objects, the corresponding fields of which contain the specified values will be found.

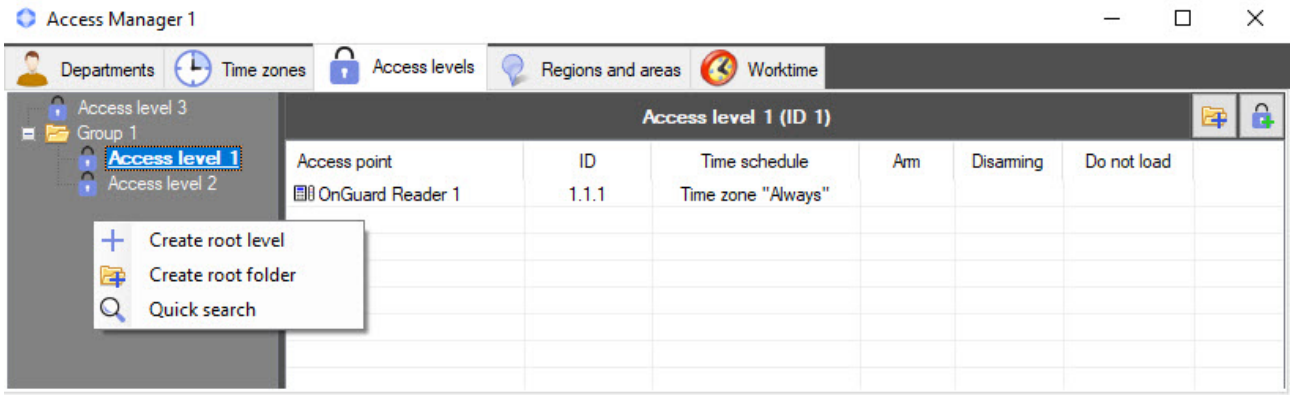
To sort the search results, left-click the header of corresponding column.

When double-clicking an access level, the **Search access level** window will be closed and the corresponding access level will be selected in the list in the **Access levels** tab, or will be added to a department or a user.

Search for an access level is completed.

6.4.6 Managing the list of access levels

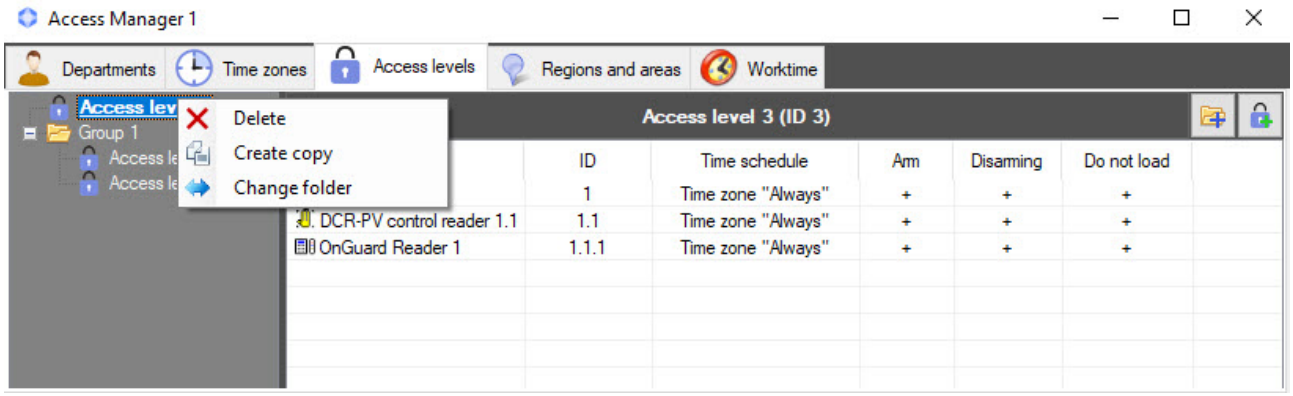
You can manage the list of access levels in the *Access Manager* using the menu that opens when you right-click in the free area of the access level list.



The commands of the menu are described in the table.

Command	Description
Create root level	Adds a new access level to the list of access levels. When you select this command, the **Edit access level** window opens. This window allows you to name a new level and create links to access points and time zones. For more information on creating and editing an access level, see Creating access levels
Create root folder	Adds a new folder to the list for grouping access levels. When you select this command, the **Folder settings** window opens. This window allows you to name a new folder
Quick search	Opens the window for quick search for access levels in the list. When you select this command, the **Quick Search** window opens. This window allows you to search for access levels by different criteria. For more information on searching for access levels, see Search for access level

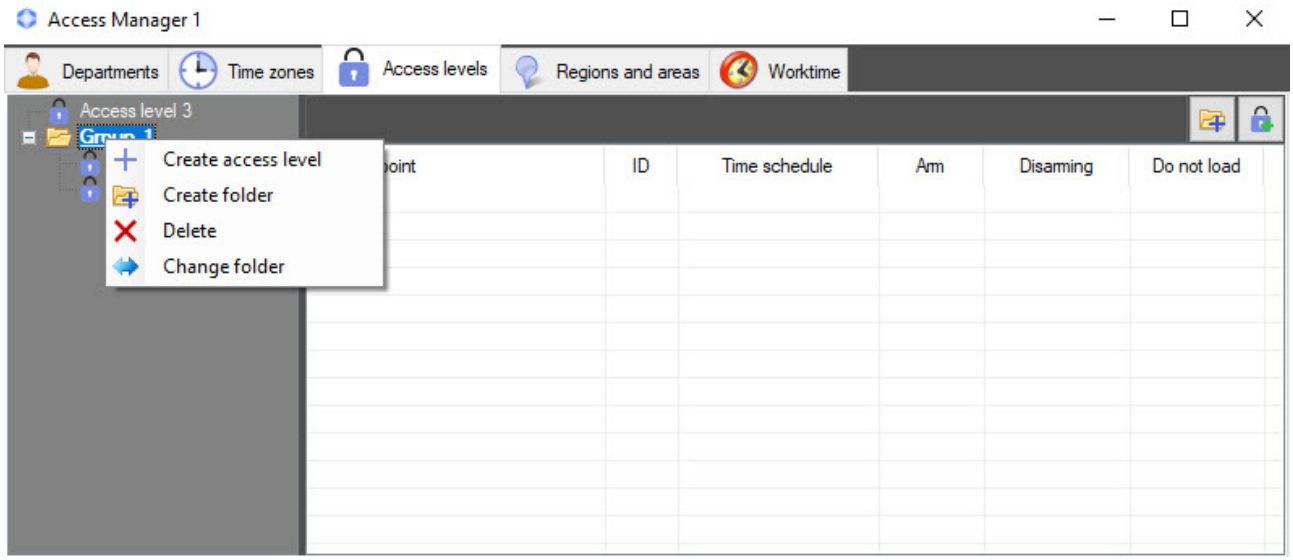
You can manage an individual access level in the root of the access level list using the menu that opens when you right-click an access level.



The commands of the menu are described in the table.

Command	**Description**
Delete	Deletes an access level after confirmation from a user. If deletion of assigned access levels is forbidden (see Forbid to delete non-empty departments, assigned access levels, time zones, and identifier owners), the access level can only be deleted if it is not assigned to any user or department. When you try to delete an access level assigned to a user or department, the **Invalid operation** warning is displayed indicating a user or deparment to which the access level is assigned
Create copy	Creates a copy of the selected access level with all its settings. When you select this command, the **Edit access level** window opens. This window allows you to edit a copy if required. For more information on editing access levels, see Editing an access level in the Access Manager software module
Change folder	Moves an access level to the selected folder. When you select this command, the **Folder search** window opens. This window contains 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

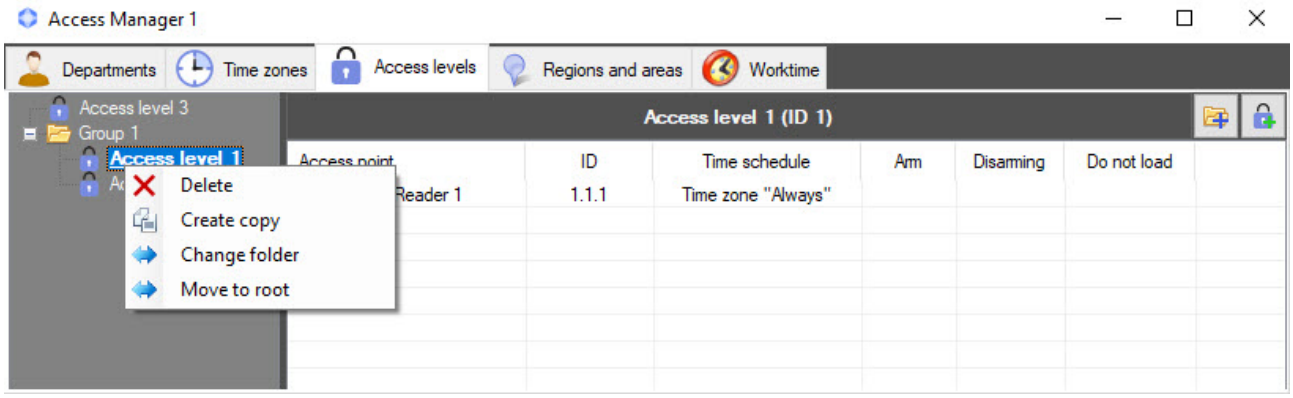
You can manage an individual folder in the access level list using the menu that opens when you right-click the folder.



The commands of the menu are described in the table.

Command	Description
Create access level	Adds a new access level to the folder. When you select this command, the **Edit access level** window opens. This window allows you to name a new level and create links to access points and time zones. For more information on creating and editing an access level, see Creating access levels
Create folder	Adds a subfolder. When you select this command, the **Folder settings** window opens. This window allows you to name a new folder
Delete	Deletes an access level after confirmation from a user. If deletion of assigned access levels is forbidden (see Forbid to delete non-empty departments, assigned access levels, time zones, and identifier owners), the access level can only be deleted if it is not assigned to any user or department. When you try to delete an access level assigned to a user or department, the **Invalid operation** warning is displayed indicating a user or deparment to which the access level is assigned
Change folder	Moves the folder to the selected folder. When you select this command, the **Folder search** window opens. This window contains 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

You can manage an individual access level within a folder using the menu that opens when you right-click an access level.



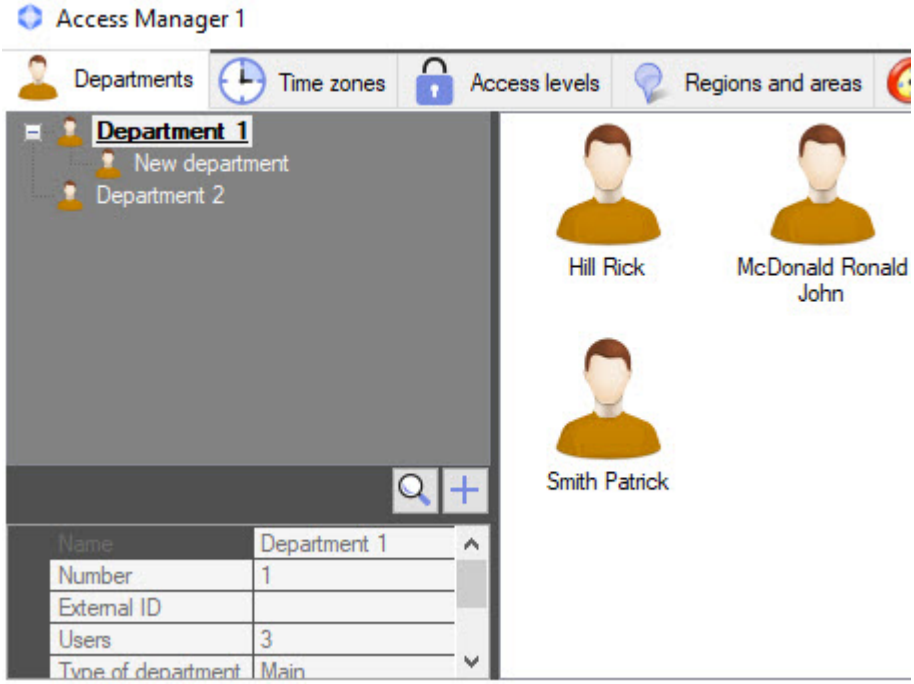
The commands of the menu are described in the table.

Command	Description
Delete	Deletes an access level after confirmation from a user. If deletion of assigned access levels is forbidden (see Forbid to delete non-empty departments, assigned access levels, time zones, and identifier owners), the access level can only be deleted if it is not assigned to any user or department. When you try to delete an access level assigned to a user or department, the **Invalid operation** warning is displayed indicating a user or deparment to which the access level is assigned
Create copy	Creates a copy of the selected access level with all its settings. When you select this command, the **Edit access level** window opens. This window allows you to edit a copy if required. For more information on editing access levels, see Editing an access level in the Access Manager software module
Change folder	Moves the access level to the selected folder. When you select this command, the **Folder search** window opens. This window contains 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
Move to root	Moves the selected access level from the folder 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 in the Access Manager

In *ACFA PSIM*, departments have a hierarchical structure. The tree of departments is displayed on the **Departments** tab of the **Access Manager** window.



You can create departments on the basis of any existing 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 when configuring the *Access Manager* software module—see Rights to access departments in the Access Manager.

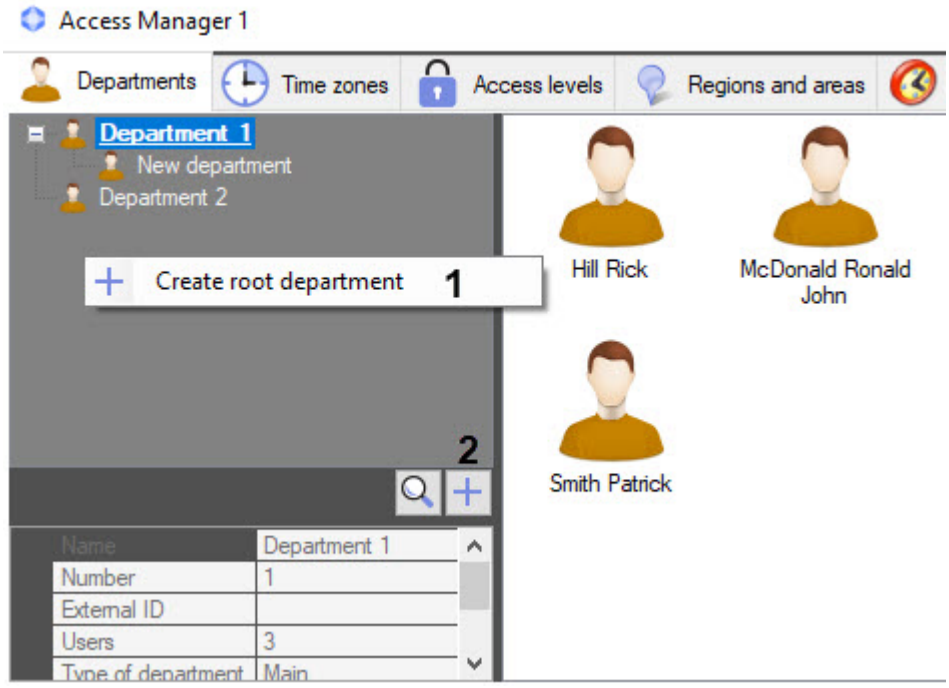
6.5.2 Adding and deleting a department

On the page:

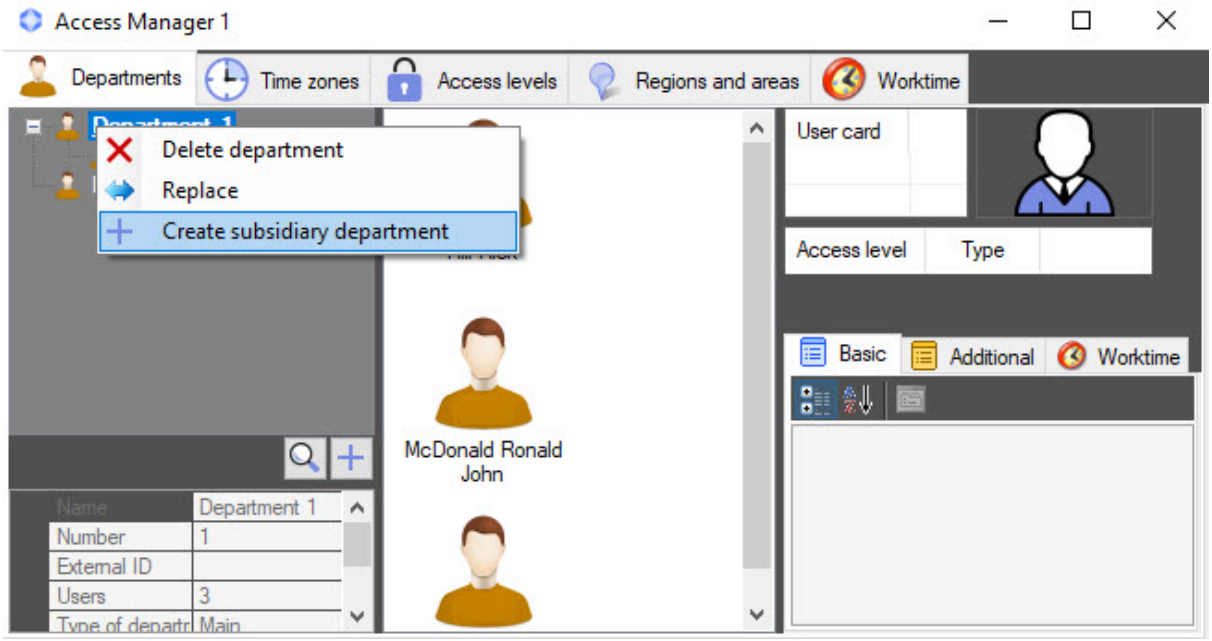
Adding a department

To add a department, do the following:

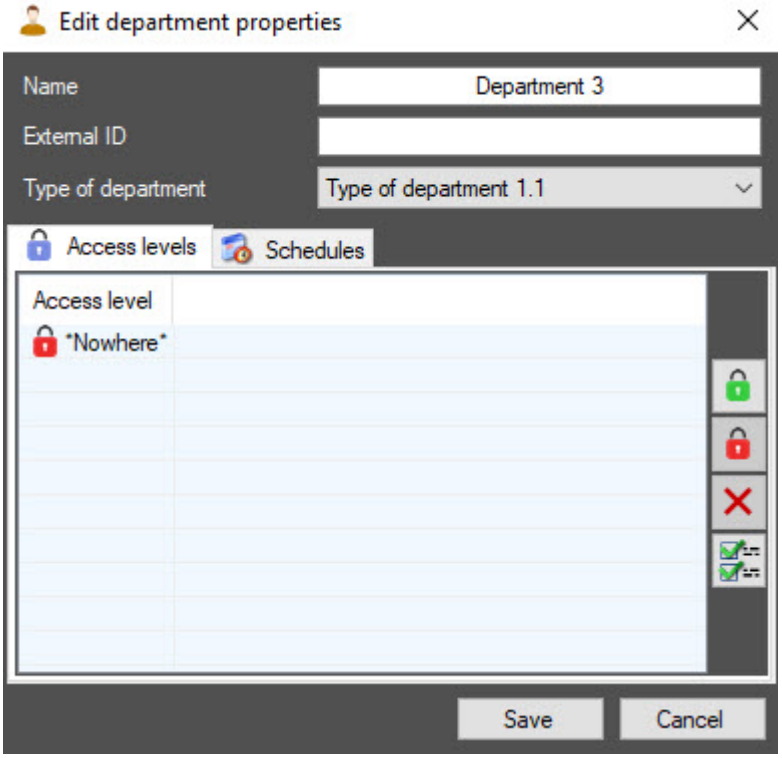
1. Go to the **Departments** tab of the **Access Manager** window.



2. To create a department in the root of hierarchy, right-click in a free area of departments hierarchy and select the **Create root department** item in the function menu (**1**) or click the button (**2**).
To create a department on the basis of an existed department, right-click the required department and select the **Create subsidiary department** item.



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

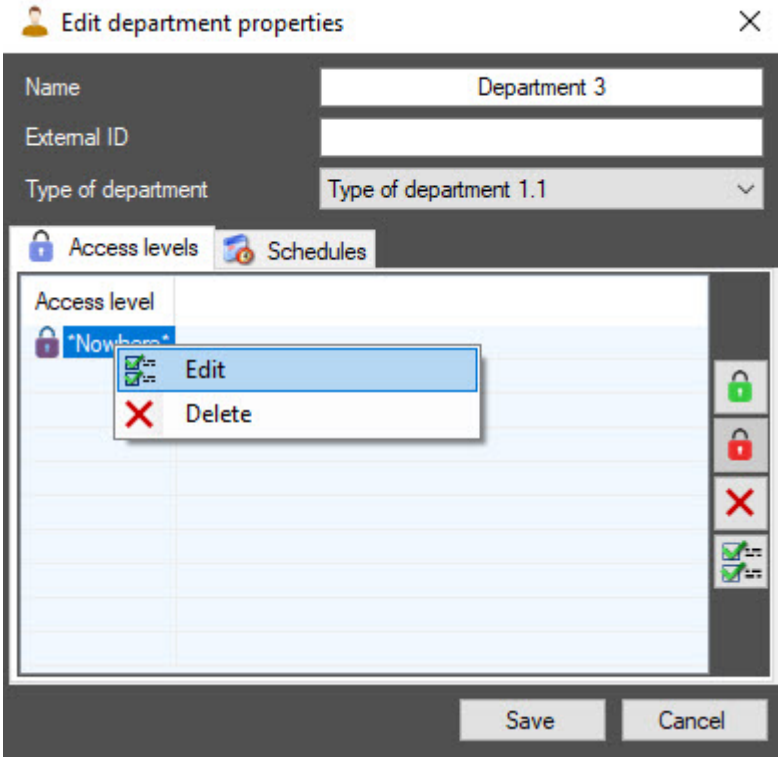


3. Enter the department name in the **Name** field.

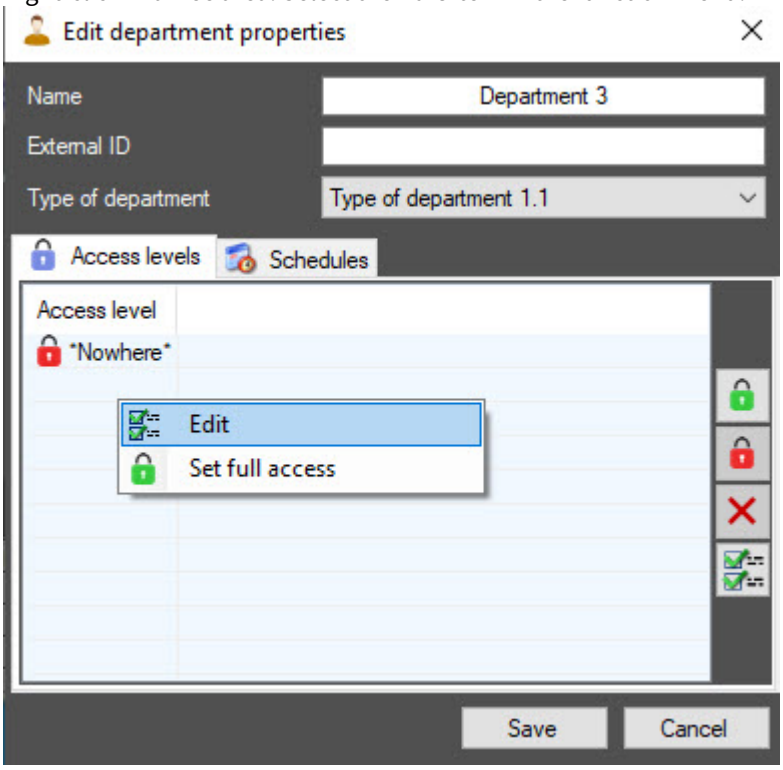
> **Note**
>
> The name must be unique. If a department with the same name has already been created in the system, then the attempt to save will fail and a corresponding message will be displayed. Also, the name must not contain the following characters: < | >.

4. In the **External ID** field, enter the external identification number of a department. This field is required if, due to the peculiarities of the ACS integration module, the list of departments and users in the database of *ACFA PSIM* is used together with the users database in the external software.
5. From the **Type of department** drop-down list, select the required type. Types of departments are created when configuring the Access Manager software module—see Configuring a type of department in the Access Manager. Type of department specifies the list of visible and available for editing fields of user belonging to this department. The **Main** type of department is the only default type of department in the *Access Manager* module (see Configuring the Main department type).
6. Open the **Search access level** window for the department being edited in one of the following ways.

a. Right-click the access level. Select the **Edit** item in the function menu.

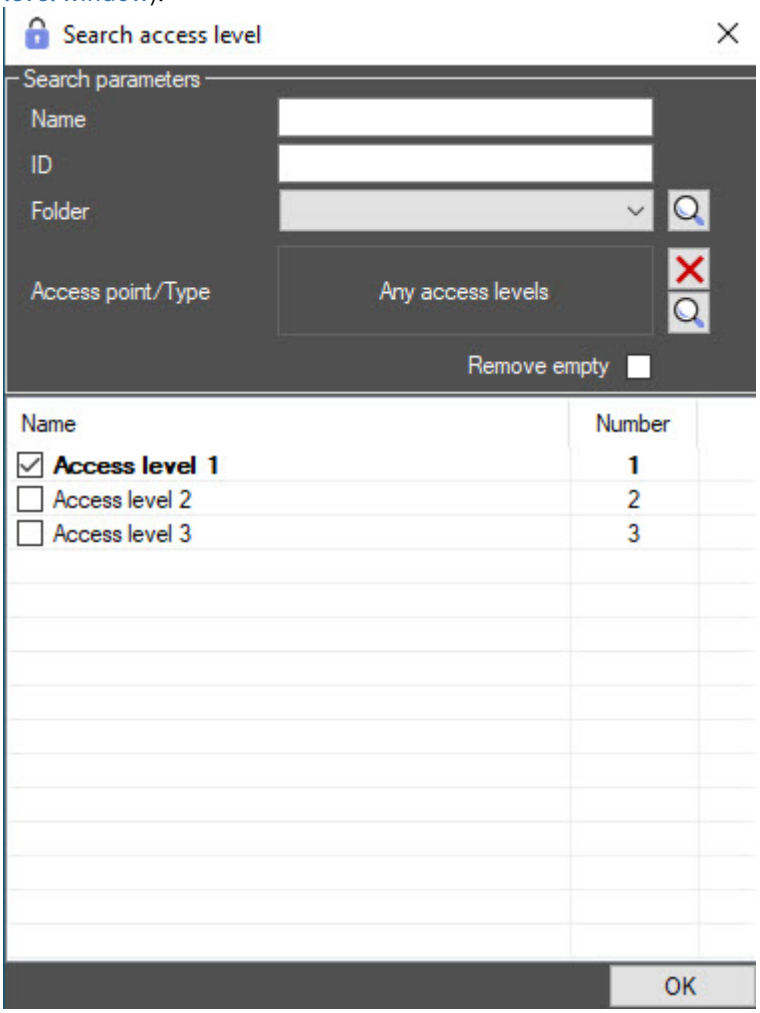


b. Right-click in a free area. Select the **Edit** item in the function menu.



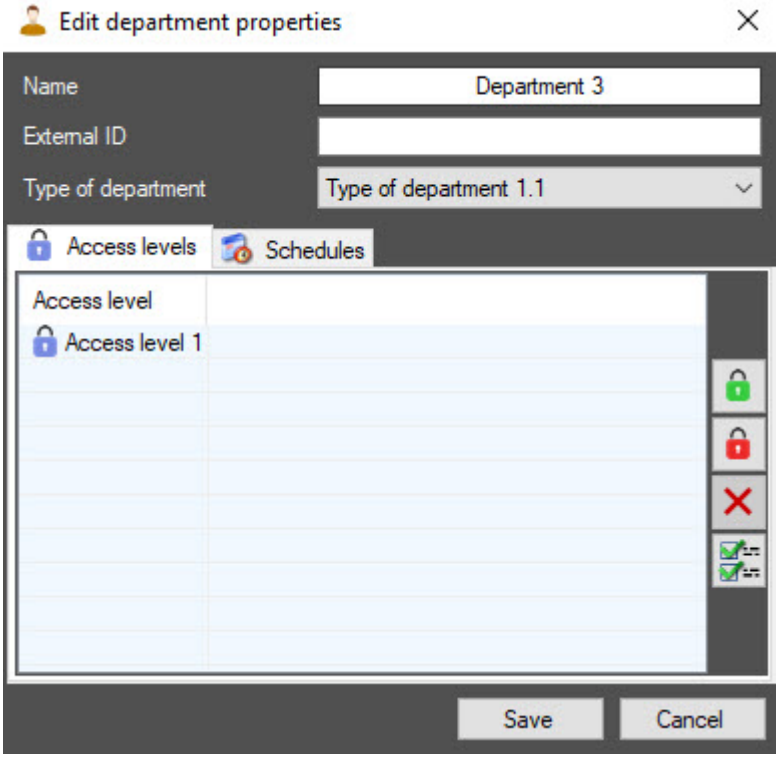
c. In the **Edit department properties** window, click the  button.

7. Select the required access levels in the **Search access level** window (see Working with the Search access level window).

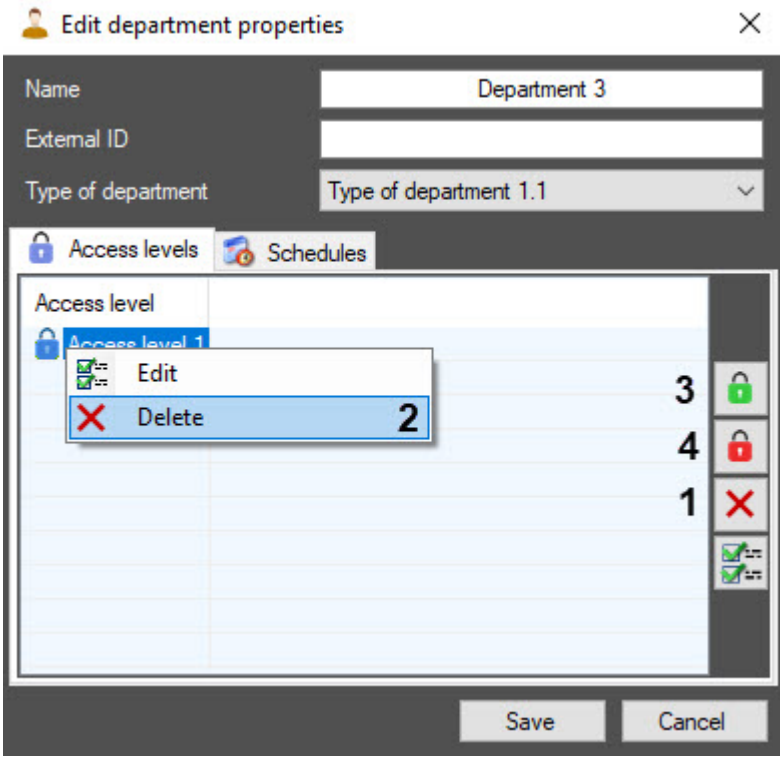


8. Click the **OK** button. As a result, the selected access levels will be displayed in the **Edit department properties** window. Also, the access levels of the department will be inherited by all users belonging to the

department after you save the settings.



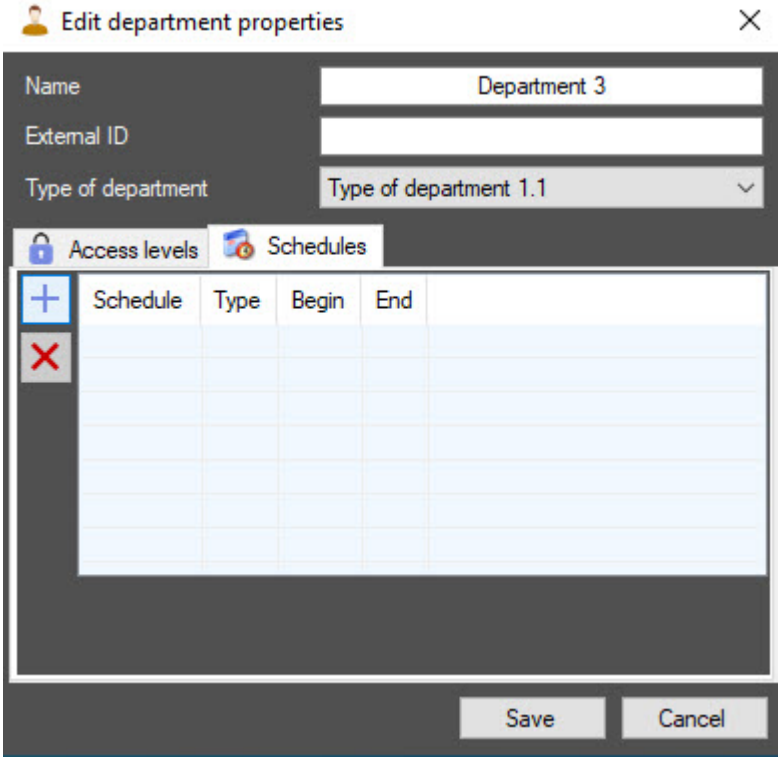
9. To delete an access level, select the required level and click the  button (**1**) on the panel to the right, or right-click the level that you want to delete and select the **Delete** item in the function menu (**2**).



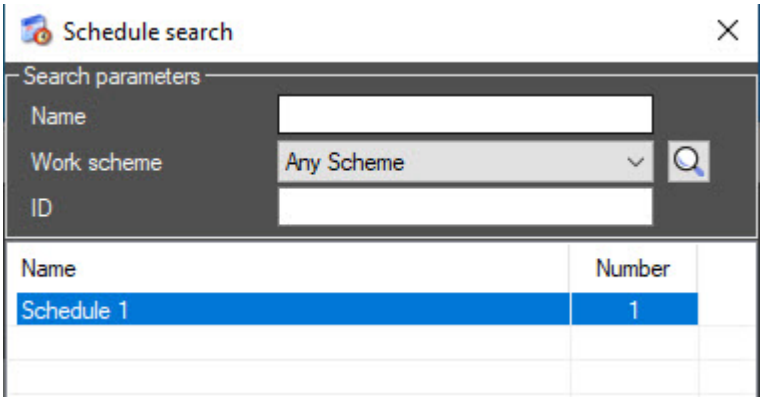
10. To assign the **Always** and **Never** system access levels to a department, click the  button (**3**) to set full access, or click the  button (**4**) to deny access.

> **Note**
>
> A department must have at least one access level, so you cannot delete the last remaining level.
> User may not inherit the access level of a department—see Configuring the department access level inheritance.
> You can create and configure access levels on the **Access levels** tab of the **Access Manager** window (see Working with access levels in the Access manager software module). You can also use the **Always** and **Never** system access levels.

11. Assign schedules to a department.
    a. Go to the **Schedules** tab.

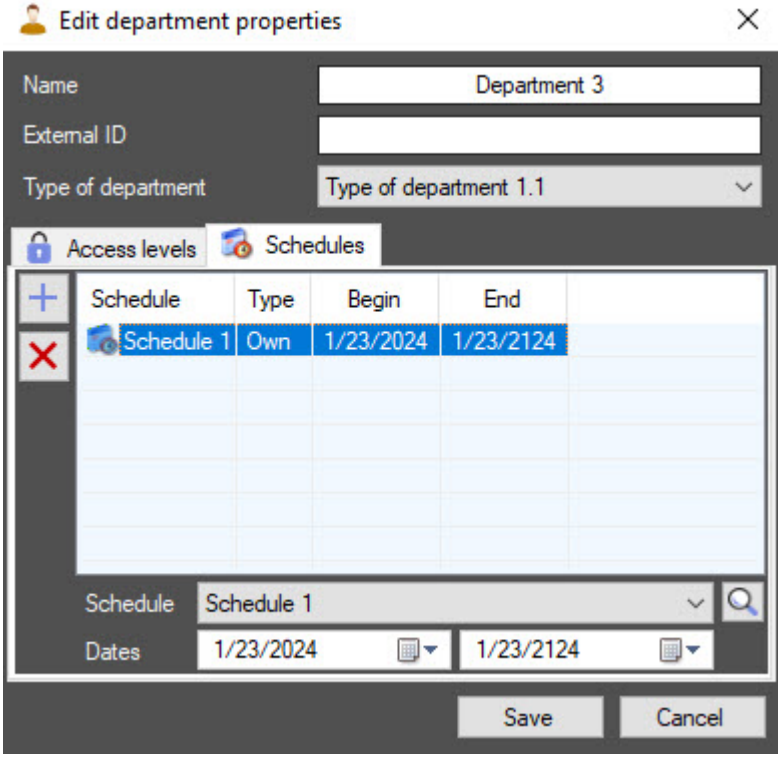


    b. Click the  button to search for schedules.
    c. In the **Schedule search** window, double-click to select the required schedule that will be assigned to a department. You must create the schedules beforehand in the *Access Manager* module (see Work schedules).



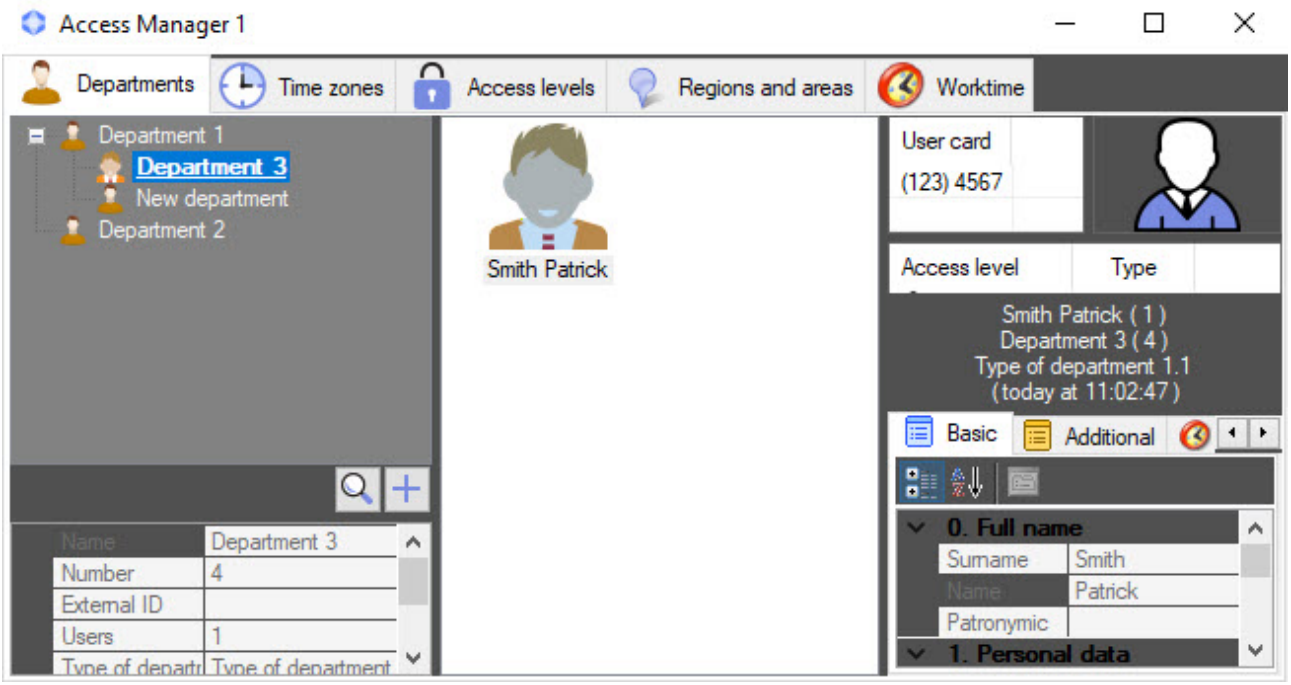
As a result, the selected schedule will be displayed in the **Edit department properties** window.

12. If necessary, change the settings of the department schedule (see Assigning a work schedule to a department).



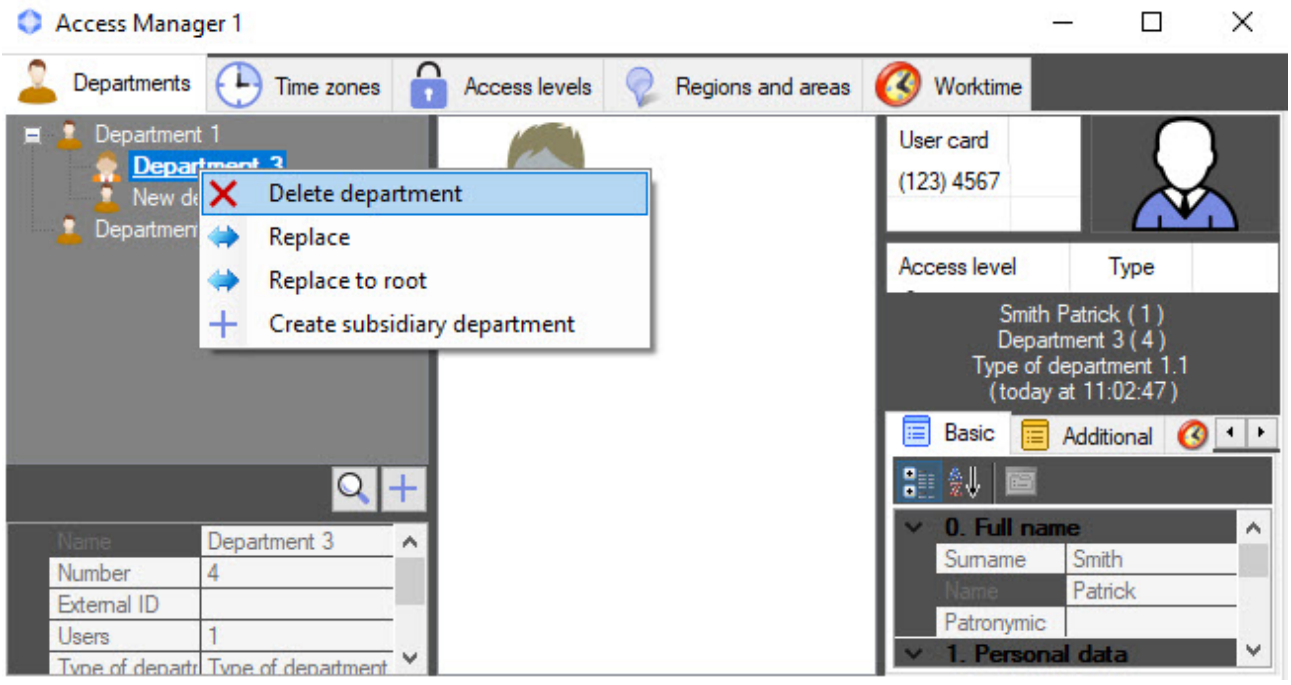
13. Click the **Save** button to save the settings.

Department will be added to the tree.



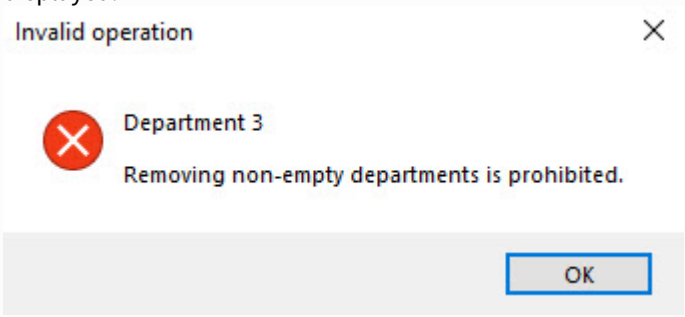
Deleting a department

To delete a department, right-click it and select the **Delete department** item in the function menu.



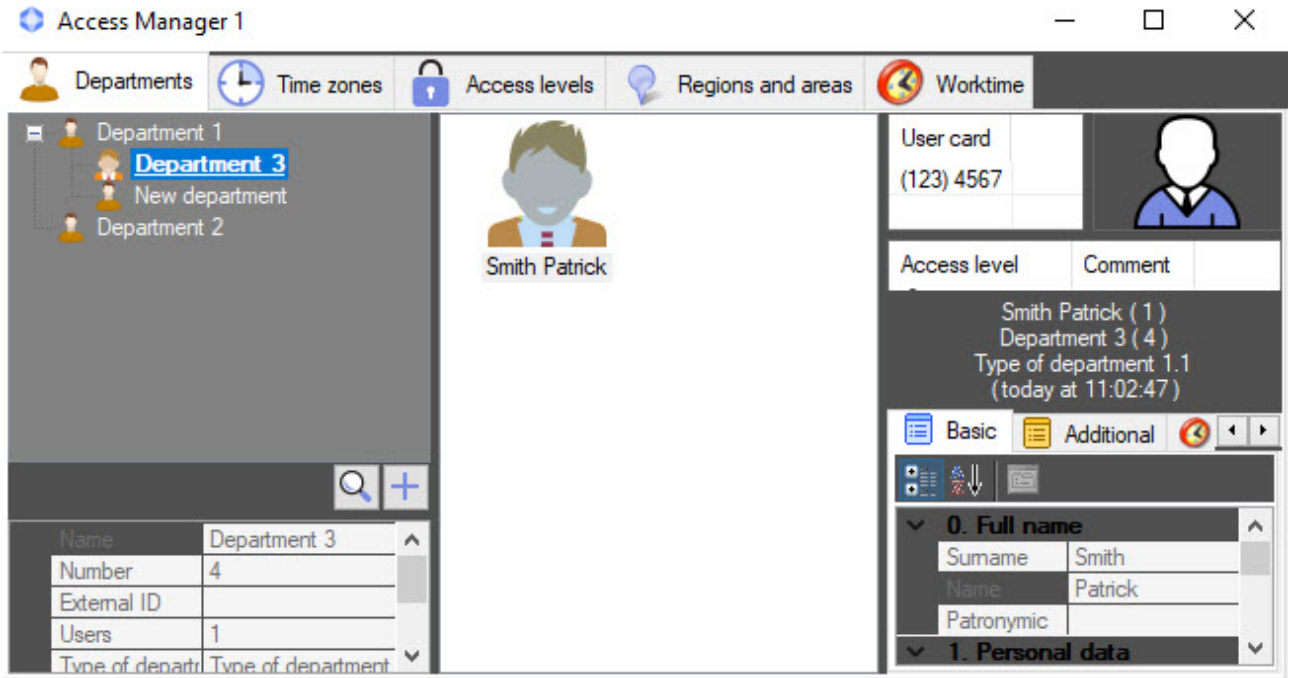
Note

If deletion of non-empty departments is prohibited (see Forbid to delete non-empty departments, assigned access levels, time zones, and identifier owners), you can delete the department only if there are no users in it. If you try to delete a non-empty department, the **Invalid operation** warning will be displayed.

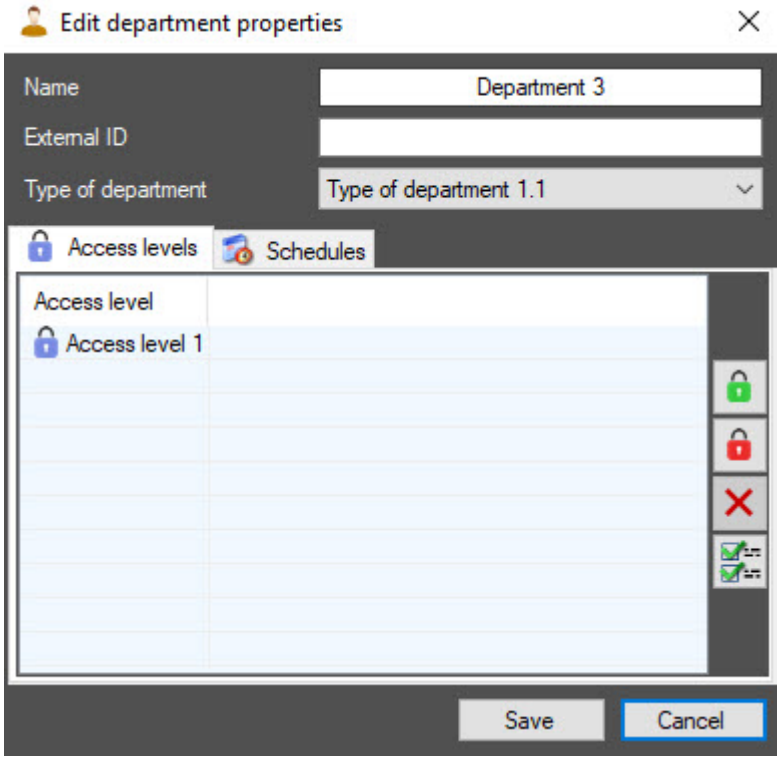


6.5.3 Editing a department

Editing a department involves changing the department parameters. To edit a department, double-click the name of the department in a department tree on the **Departments** tab of the **Access Manager** interface window.



The **Edit department properties** window will open. You can work with this window in the same way as described in Adding and deleting a department.



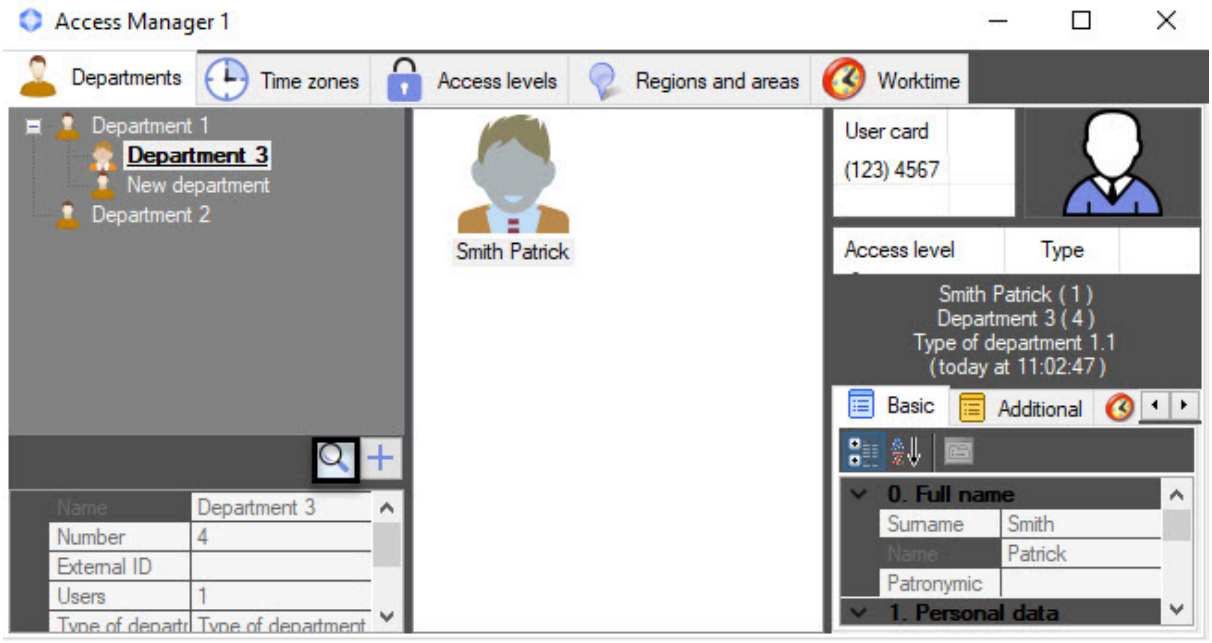
6.5.4 Department search in the Access Manager software module

Going to department search

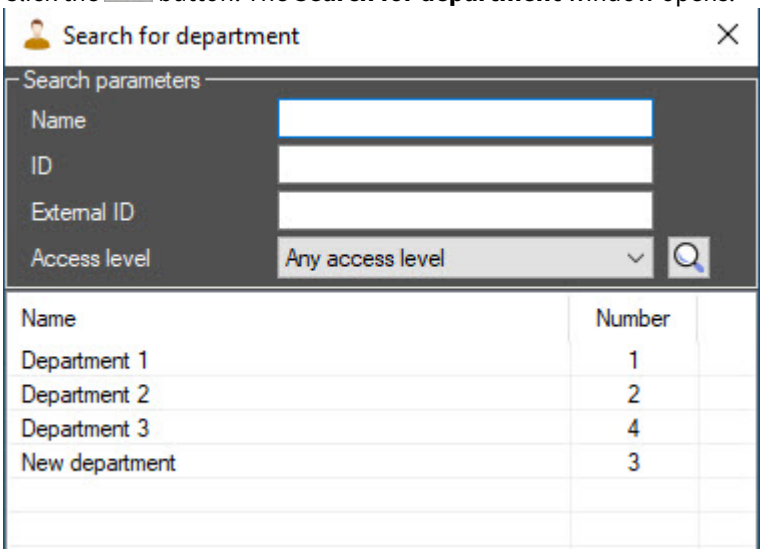
In the *Access Manager* software module, you can search for departments by name, ID, external ID, and access level.

To go to department search, do the following:

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



2. Click the  button. The **Search for department** window opens.



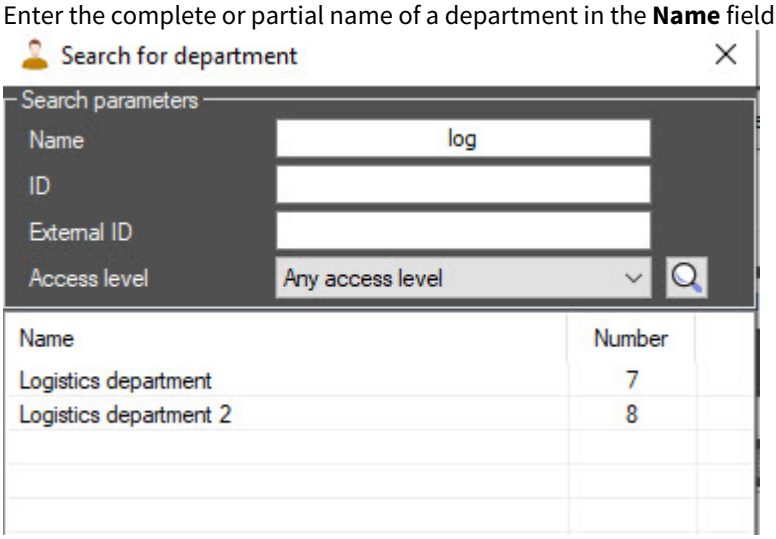
Going to the department search is complete. For the information on how to work with the **Search for department** window, see Working with the Search for department window.

Working with the Search for department window

You can work with the **Search for department** window when searching for a department (see Going to department search), transferring a user from one department to another (see Transferring a user to a different department), and when creating departments hierarchy (see Creating department's hierarchy).

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.



2. Enter the department ID in the **ID** field.
3. Enter the external ID of an object in the **External ID** field.
4. From the **Access level** drop-down list, select the name of an access level which is assigned to the required department. You can also search for an access level. Click the  button and search for an access level (see Working with the Search access level window).
5. Click the Enter key on the keyboard. As a result, a list of departments that meet the specified search parameters will be displayed. Search is case-insensitive. All objects, the corresponding fields of which contain the specified values will be found.

To sort the search results, click the header of the corresponding column.

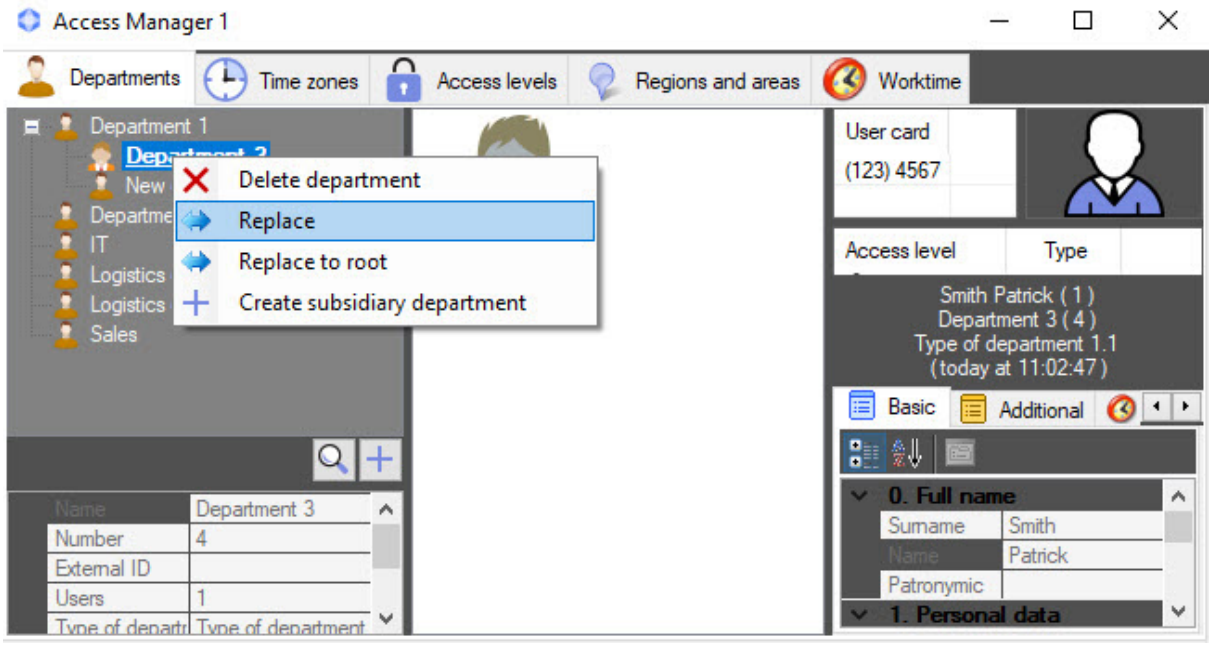
When you double click the department name in the search results, the **Search for department** window will be closed, and the department will be selected in the departments tree or in the form from which the **Search for department** window was opened.

6.5.5 Changing the departments hierarchy in the Access Manager

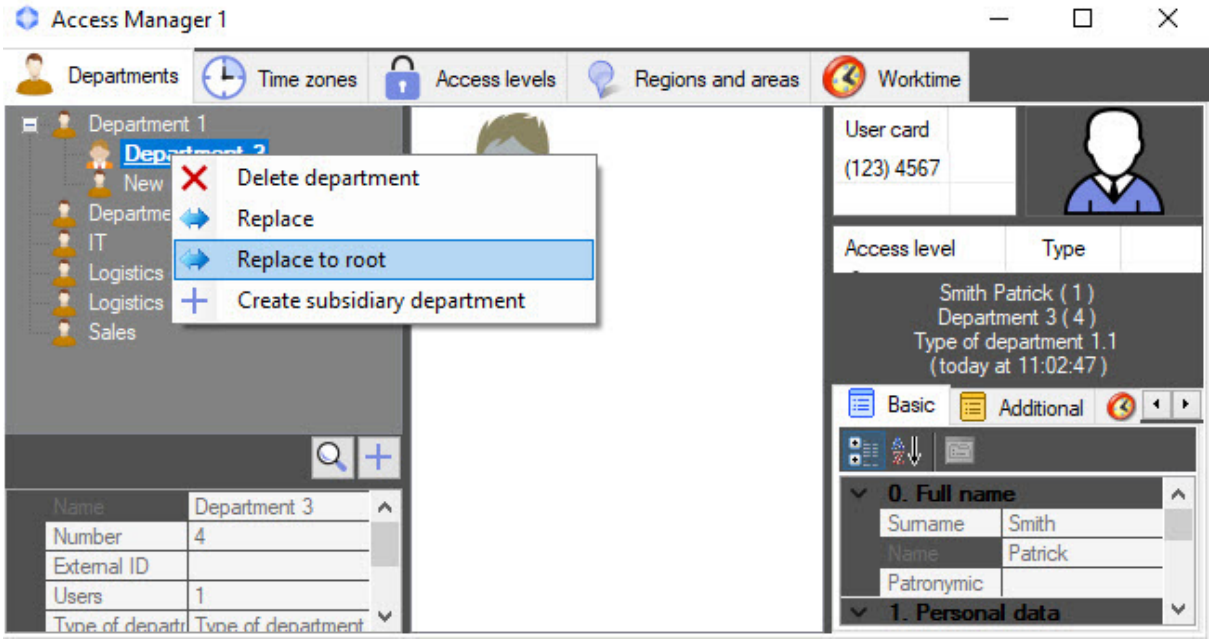
You can change the departments hierarchy using the following operations:

1. Changing the parent department. Right-click the department name in the departments tree and select the **Replace** item in the function menu. As a result, the **Search for department** window will open to select a

new parent department (see Working with the Search for department window).



2. Replacing subsidiary department to the root of hierarchy. Right-click department name in the departments tree and select the **Replace to root** item in the function menu. As a result, the department will be replaced to the root of the departments hierarchy.



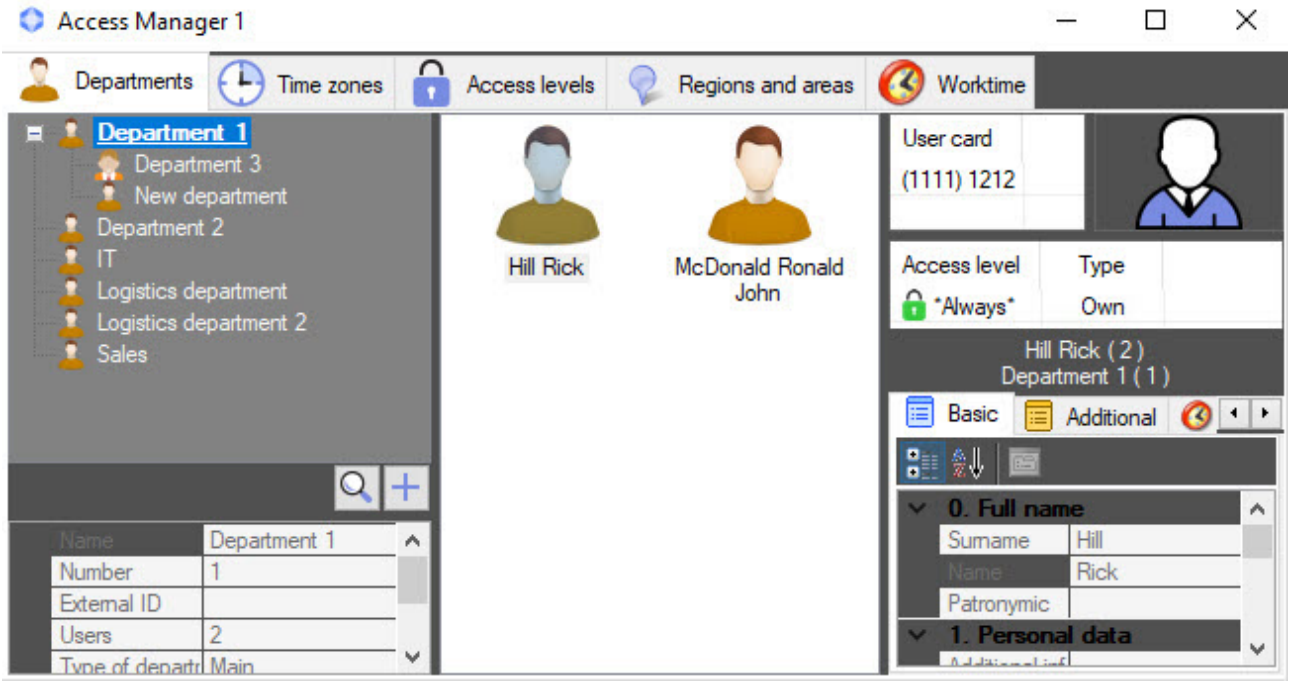
3. Change the department location in the hierarchy by dragging it with the left mouse button while holding down the Ctrl key.

> **Note**
>
> Subsidiary departments are replaced with their parent deparment in the hierarchy.

6.6 Working with users in the Access Manager software module

6.6.1 Viewing a list of users

To view a list of users, select one of the departments in the department hierarchy. A list of users included in this department is displayed in the middle part of the **Access Manager** interface window.



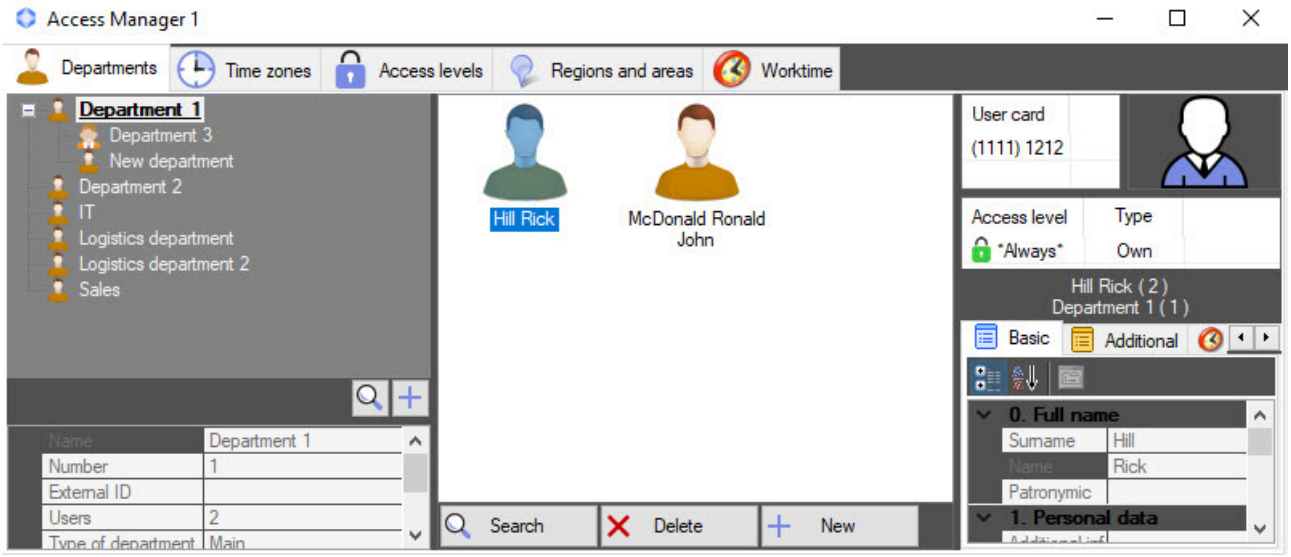
Note

When the number of users in a department is large (more than 2000), it can take some time to display the list of users, which depends on computer performance.

When you select a user in the list, user properties are displayed in the right part of the **Access Manager** window. By default, the first user from the list is selected when you view the department.

When you press the key combination **Ctrl+Shift+M**, the user control panel is displayed at the bottom of the window:

- **Search**—User search in the Access Manager software module.
- **Delete**—Deleting a user in the Access Manager software module.
- **New**—Creating a user in the Access Manager.



Note

To hide the user control panel, press the key combination **Ctrl+Shift+M** again.

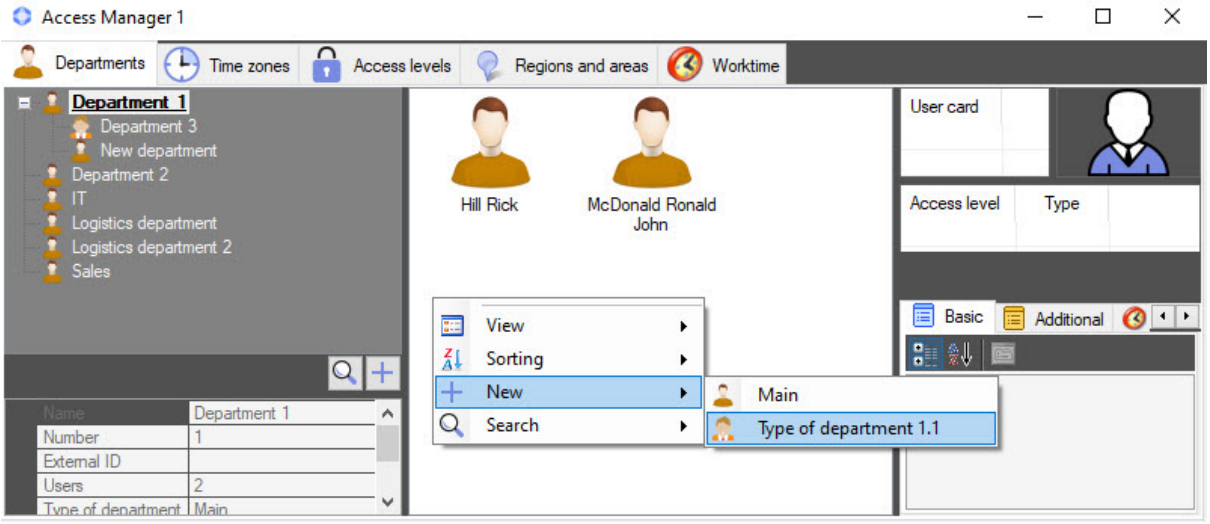
6.6.2 Creating a user in the Access Manager

To add a new user, do the following:

Note

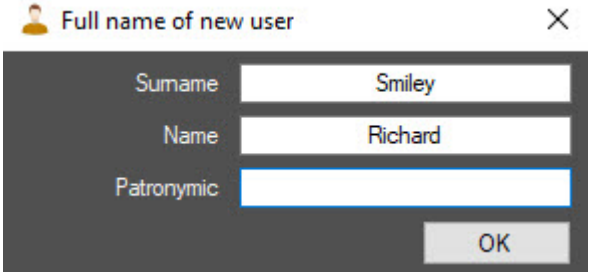
In addition to the method described below, you can also create new users by clicking the **New** button on the user control panel (see Viewing a list of users).

1. Open a list of users (see Viewing a list of users).
2. Right-click in a free area of the user list or any previously created user.



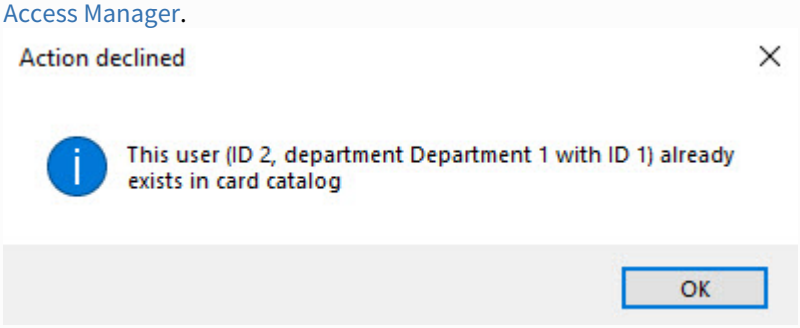
> **Note**
>
> Rights to create users can be limited when you configure the *Access Manager* module. The message about the lack of corresponding rights is displayed. See also Configuring the rights to manage objects in Access Manager.

3. Select the **New** item in the function menu. The **Full name of new user** window opens.



4. Enter the surname, name, and patronymic of a new user.
5. Click the **OK** button.

> **Note**
>
> - Surname, name, and patronymic must not contain the following characters: < | >.
> - If a duplicate record check is enabled and there is a user with such a name in the system, the error message with the ID of an existing user and department to which the user belongs is displayed. See also Configuring the prohibition of duplicates of new user parameters in the Access Manager.



6. The **Editing. <User name> (creation)** window opens.

The further process of user creation is described in Editing a user.

Creation of a new user is complete.

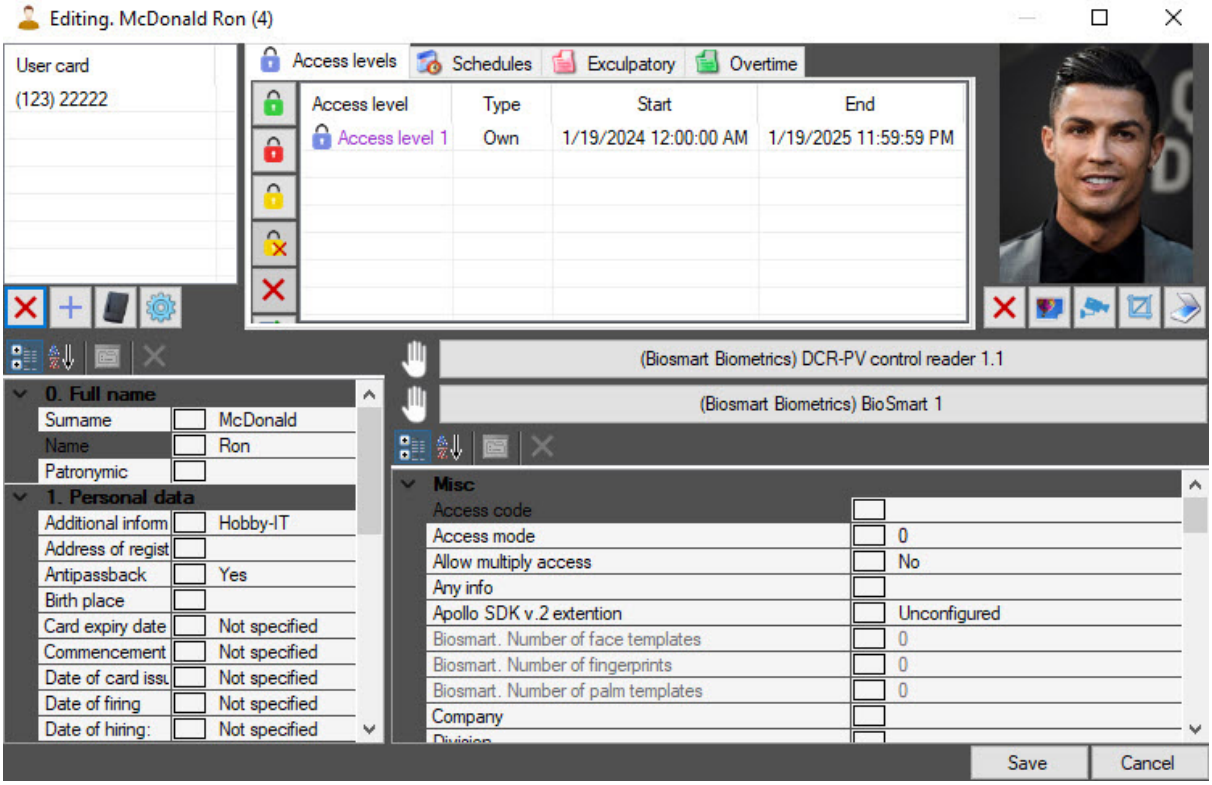
6.6.3 Editing a user

Going to user editing

You can go to user editing when you create a user (see Creating a user in the Access Manager) or as follows:

1. Open a list of users (see Viewing a list of users).

2. Double-click the required user. The **Editing. <User name> (ID)** window opens.



In this window, you can do the following:

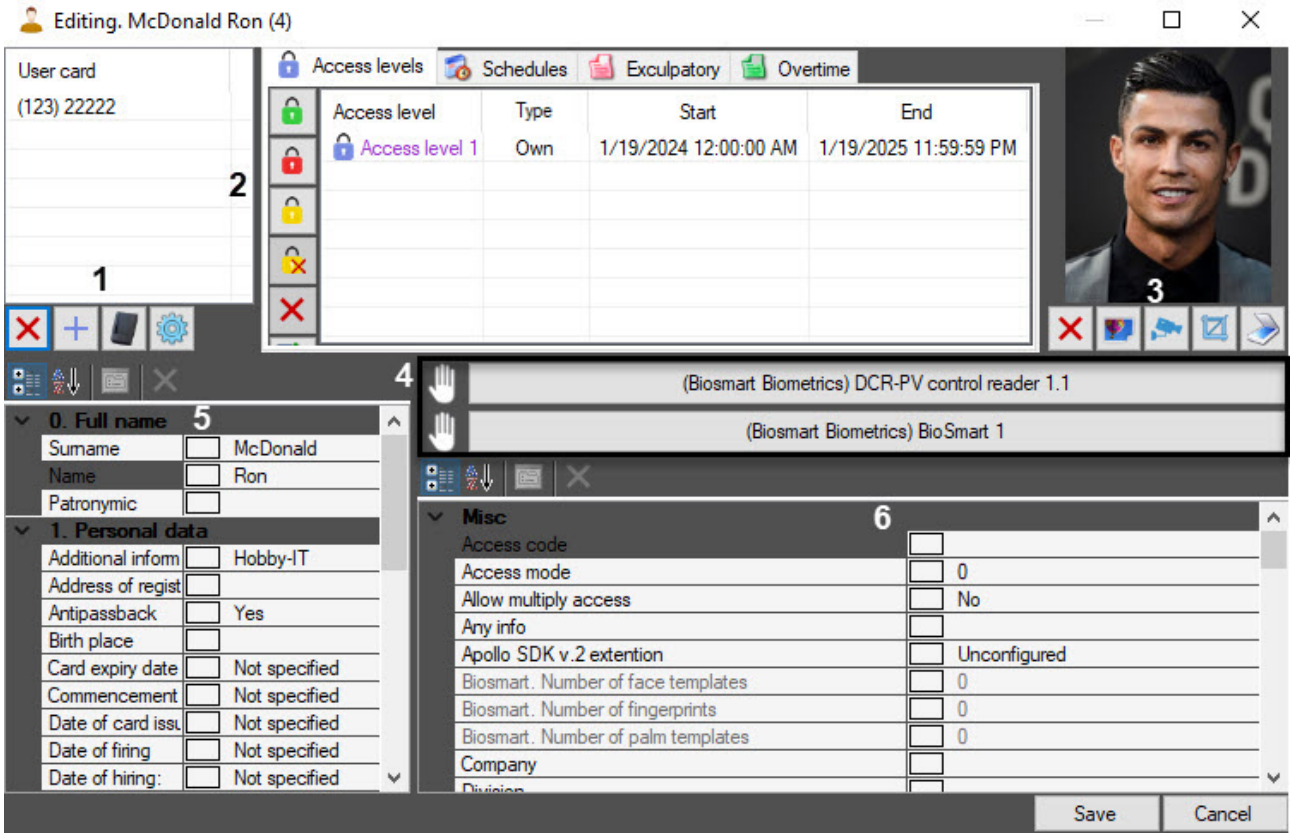
a. Set user parameters.
b. Assign an access card to a user.
c. Assign access levels to a user.
d. Assign a photo to a user.
e. Add biometric parameters (fingerprints).
f. Open a folder with user documents.
g. Add extension buttons.

These actions are described in the sections below.

> **Note**
>
> Rights for user editing can be limited when you configure the *Access Manager* module. In this case, the message about the lack of corresponding rights is displayed after you double-click the user name. See also Configuring the rights to manage objects in Access Manager.

Specifying user parameters

You can specify user parameters in the **Editing. <User name> (ID)** window.



The button panel (**1**) allows you to perform the following actions:

- —delete the selected user card (see Deleting a user access card);
- —add a user card manually (see Manual input of access card number);
- —add a user card using a control reader (see Entering an access card number using a control reader);
- —use the user card manager.

The button panel (**2**) allows you to perform 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 the **Own** access level (see Assigning Own access level to a user).
- —edit access level (see Assigning Own access level to a user).

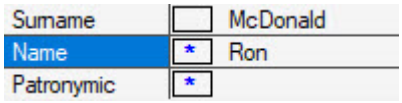
The button panel (**3**) allows you to perform the following actions:

- —delete a photo assigned to a user (see Deleting a photo).
- —assign a photo from a file to a user (see Assigning photograph from a file).
- —assign a photo from the camera to a user (see Assigning a photo to a user from a camera).
- —crop a user photo (see Cropping a photo).
- —specify user parameters using the *ABBYY PassportReader SDK* module (see Filling out the user parameters using the ABBYY PassportReader SDK module).

> **Note**
>
> By default, the button is inactive. To activate it, you must configure the *ABBYY PassportReader SDK* module (see Configuring the ABBYY PassportReader SDK module).

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

In the areas (**5**) and (**6**), a rectangle is displayed next to each field. When you change the field, the "*****" character is displayed in the rectangle until you open the user editing window again.



> **Note**
>
> Fields available for editing including a list of access levels and a list of access cards are specified while configuring the *Access Manager* software module—see Configuring fields displaying in user accounts. Some fields can be hidden or not available for editing depending on settings.

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

Parameter name	**Method of setting the parameter value**	**Default category in templates**	**Possible values**	**Comment**
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 additional information in text field that opens by clicking the "down" button in the **Additional information** field. When you hover the mouse cursor over a user's photo, a pop-up window with the full content of this field is displayed
Access level assigned by	Automatically	1. Personal data	Operator name	Name of the operator who last assigned access level to a user or visitor (see Assigning access levels to a user)
Address of registration				
Antipassback	Select the value from the list	1. Personal data	Yes No	Default value depends on configuring the *Access Manager* module—see Configuring the prohibition of duplicates of new user parameters in the Access Manager
Birth place	Enter the value in the field	1. Personal data	Any characters except: < | >	Place of user birth
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 controller does not support time recording, the card stops working the next day at 00:00 from the specified date
Card issued by	Automatically	1. Personal data	Operator name	Name of the operator who last assigned access card to a user or visitor (see Assigning an access card to a user)
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 email address
External ID	Enter the value in the field	1. Personal data	Any characters except: < | >	This field is used if list of departments and users in the database of *ACFA PSIM* is used with users database in external software due to features of used ACS integration module
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 phone number
Passport number	Enter the value in the field	1. Personal data	Any characters except: < | >	User passport number
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	Depending on the selected value in the **Mask PIN code** field in the *Access Manager*, the PIN code can be: • Always masked with dots. • Masked while reading user data. • Not masked 
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: < | >	Telephone number
User locked	Select the value from the list	1. Personal data	Yes No	Yes—user locked No—user is active
Driving license	Enter the value in the field	3. Vehicle	Any characters except: < | >	Number of user driving license
Vehicle LP	Enter the value in the field	3. Vehicle	Any characters except: < | >	License plate of user vehicle. Several license plates can be specified divided by space. Access by license plate is also enabled in this case when *ACFA PSIM* is set up for operation with *Virtual Access Server* module (see Virtual Access Server Integration Module Configuration and Operation Manual)
Vehicle model	Enter the value in the field	3. Vehicle	Any characters except: < | >	Model of user vehicle
Document	Enter the value in the field	4. Visitor data	Any characters except: < | >	Presented document of visitor identification
Origin	Enter the value in the field	4. Visitor data	Any characters except: < | >	Name of organization to which the visitor belongs
Purpose of visit	Enter the value in the field	4. Visitor data	Any characters except: < | >	Purpose of visitor visit

To which department	Enter the value in the field	4. Visitor data	Any characters except: < | >	Department being visited
To whom	Enter the value in the field	4. Visitor data	Any characters except: < | >	Employee being visited

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

Parameter name	**Method of setting the parameter value**	**Default category in templates**	**Possible values**	**Comment**
Access code	Enter the value in the field	Misc		
Access mode	Enter the value in the field		Numbers	
Add or remove mobile card in background	Select the value from the list		+1 0 X	
Allow multiple access	Select the value from the list		Yes No	
Any info	Enter the value in the field		Any characters except: < | >	
Apollo SDK	Configurating		Unconfigured Configured	Used together with the ApolloSDK integration module (see ApolloSDK Integration Module Settings Guide)
Biosmart. Number of face templates	Automatically		Automatically	Used together with the Biosmart integration module (see Guide for configuring and working with the BioSmart integration module)

Biosmart. Number of face fingerprints	Automatically	Automatically	
Biosmart. Number of palm templates	Automatically	Automatically	
Company	Enter the value in the field	Any characters except: < | >	
Division	Enter the value in the field	Any characters except: < | >	
Galaxy Dual	Select the value from the list	Yes No	Used together with the Honeywell Galaxy Dimension integration module (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 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	
Hikvision extension	Configurating	Not yet configured Configured	Used together with the Hikvision integration module (see Hikvision Integration Module Configuration and Operation Guide)
Hikvision. User message	Enter the value in the field	Any characters except: < | >	
Max login count	Enter the value in the field	Numbers	
Max pick up count	Enter the value in the field	Numbers	

OnGuard ID	Automatically	Numbers	Used together with the OnGuard integration module (see Guide for configuring and working with the OnGuard integration module)
Ravelin Access type	Select the value from the list	Card only Master card Card and pin Slave card	Used together with the Gate integration module (see Gate Integration Module Setup and User Guide)
Ravelin guest card	Select the value from the list	Yes No	
Sigur wiegand	Select the value from the list	Common W26 W34 W58 W58DEC	Used together with the Sigur integration module (see Sigur integration module configuration and operation manual)
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	Used together with the Suprema 2 integration module (see Guide for configuring and working with the Suprema 2 integration module)

Suprema 2 Ex Card Auth Mode	Select the value from the list	Default Card Card → Face Card → Fingerprint Card → Pin Card → Face or Fingerprint Card → Face or Pin Card → Fingerprint or Pin Card → Face or Fingerprint or Pin Card → FaceFingerprint Card → Face → Pin Card → Fingerprint → Face Card → Face or Fingerprint → Pin Card → Face → Fingerprint or Pin Card → Fingerprint → Face or Pin Cannot Use
Suprema 2 Ex Face Auth Mode	Select the value from the list	Default Face Face → Fingerprint Face → Pin Face → Fingerprint or Pin Face → Fingerprint → Pin Cannot Use

Suprema 2 Ex Finger Auth Mode	Select the value from the list	Default Fingerprint Fingerprint → Face Fingerprint → Pin Fingerprint → Face or Pin Fingerprint → Face → Pin Cannot Use
Suprema 2 Ex Id Auth Mode	Select the value from the list	Default Id → Face Id → Fingerprint Id → Pin Id → Face or Fingerprint Id → Face or Pin Id → Fingerprint or Pin Id → Face or Fingerprint or Pin Id → Face → Fingerprint Id → Face → Pin Id → Fingerprint → Face Id → Fingerprint → Pin Id → Face or Fingerprint → Pin Id → Face → Fingerprint or Pin Id → Fingerprint → Face or Pin Cannot Use
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 2 QR Code	Automatically	Value of the QR code assigned to the user	
Suprema(2) Fingerprints	Automatically	Numbers	
Suprema(2) Security Level	Select the value from the list	Default Lower Low Normal Hight Higher	
Texecom config bitmap	Automatically	Numbers	Used together with the Texecom integration module (see Texecom Integration Module Settings Guide)
Texecom modifiers bitmap	Automatically	Numbers	
Texecom user locked by	Automatically	Numbers	

Texecom user name	Enter the value in the field	Any characters except: < | >	
Unicard code	Enter the value in the field	Any characters except: < | >	Used together with the Unicard integration module (see Unicard Integration Module Settings Guide)
Unicard default floor	Enter the value in the field	Numbers	
Unicard disabled	Select the value from the list	Yes No	
UProx Identifier	Enter the value in the field	Numbers	See Control Readers Settings Guide
UProx Passage at any time	Select the value from the list	Yes No	
UProx Passage through locked door	Select the value from the list	Yes No	
UProx Right to cancel alarm	Select the value from the list	Yes No	
VertX-Edge Access mode	Select the value from the list	Card or "Card and PIN" Card only PIN only Card only and PIN only	Used together with the HID integration module (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	
Virdi. Options	Configurating		Not yet configured Configured	Used together with the Virdi integration module (see Virdi Integration Module Settings Guide)
ZKTeco: User privilage	Select the value from the list		User Administrator	Used together with the ZK Teco integration module (see ZK Teco Integration Module Settings Guide)

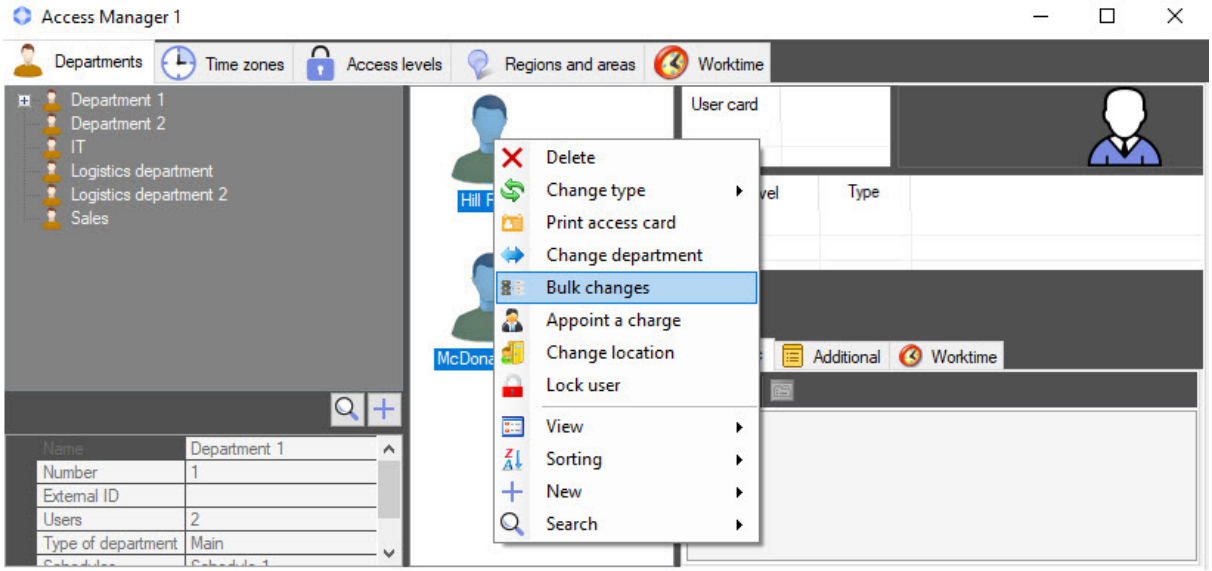
Bulk editing of users

To edit users in bulk, do the following:

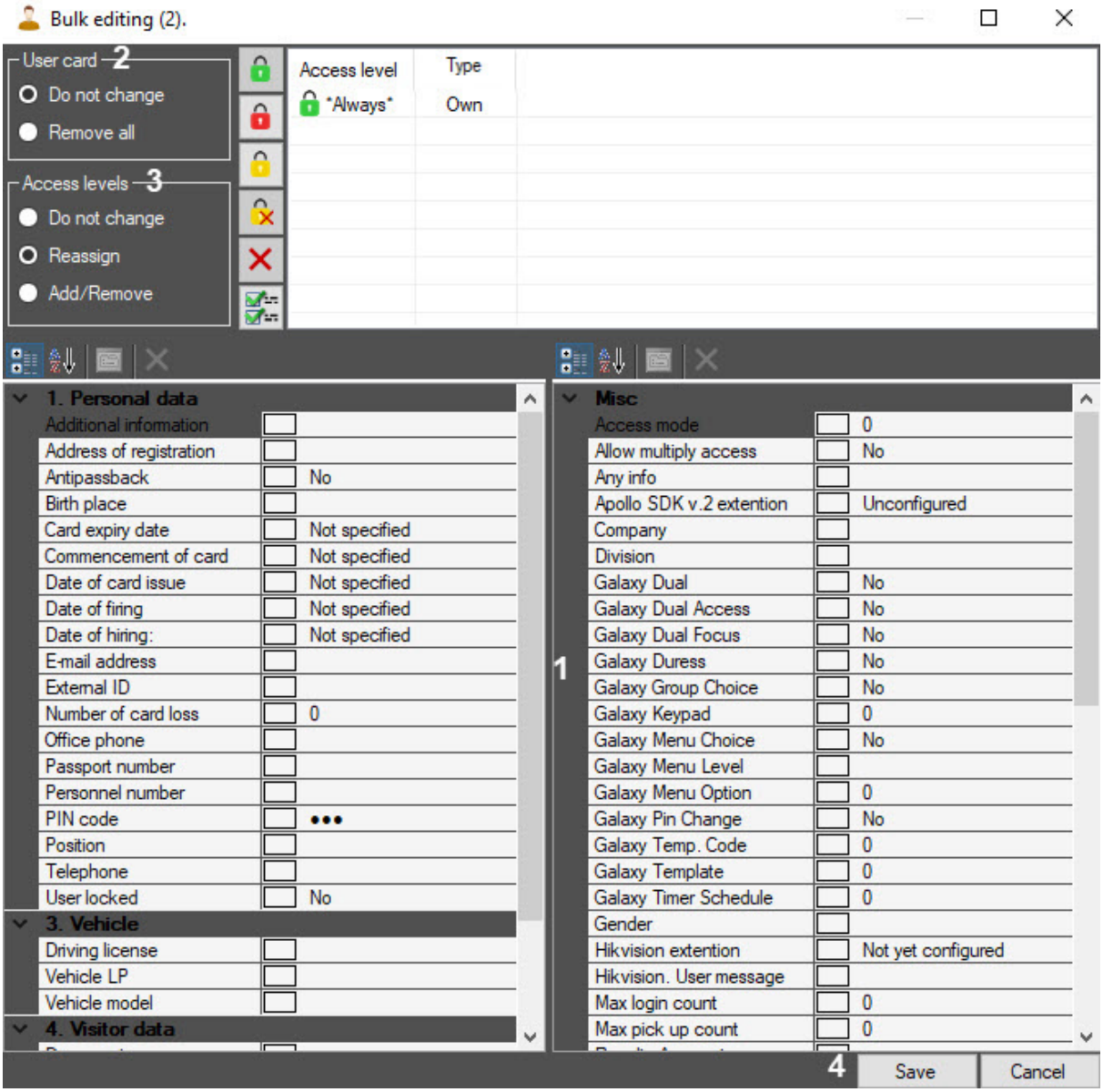
1. Go to viewing the list of users (see Viewing a list of users).
2. Select several users that you want to edit and right-click the name of any selected user.

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

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



As a result, the **Bulk editing** window opens, and the number of users being edited is displayed in brackets.

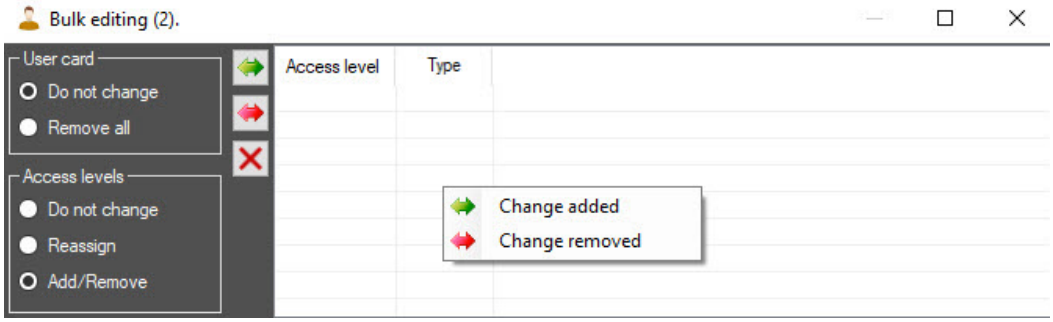


4. Specify the standard and additional fields (**1**) that are the same for all selected users (see Specifying user parameters).
5. In the **User card** group (**2**), select the **Remove all** option to delete all existing access cards from the selected users. If you don't want to change the access cards, select the **Do not change** option.

> **Attention!**
>
> You cannot cancel the deletion of access cards for all selected users.

6. In the **Access levels** group (**3**), select:
   a. the **Do not change** option if you don't want to change the access level.
   b. the **Reassign** option if you want to edit the access level of the selected users (see Assigning access levels to a user).
   c. the **Add/Remove** option if you want to add an access level or remove an existing access level.
      i. Open the function menu by right-clicking the list of access levels to the right.

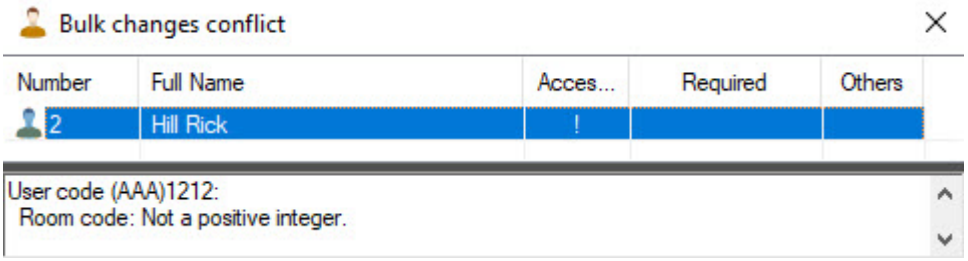
ii. To add a new access level to all selected users, select the **Change added** item. To remove an access level, select the **Change removed** item.



iii. In the **Search access level** window, select the required level (see Working with the Search access level window).

7. Click the **Save** button (**4**) to apply the changes.

> **Attention!**
>
> If the selected users have access cards 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 is displayed, indicating the cause of the conflict. Changes will not be saved until all conflicts are resolved. Changes can be saved if you select the **Remove all** option in the **User card** group.



Bulk editing of users is complete.

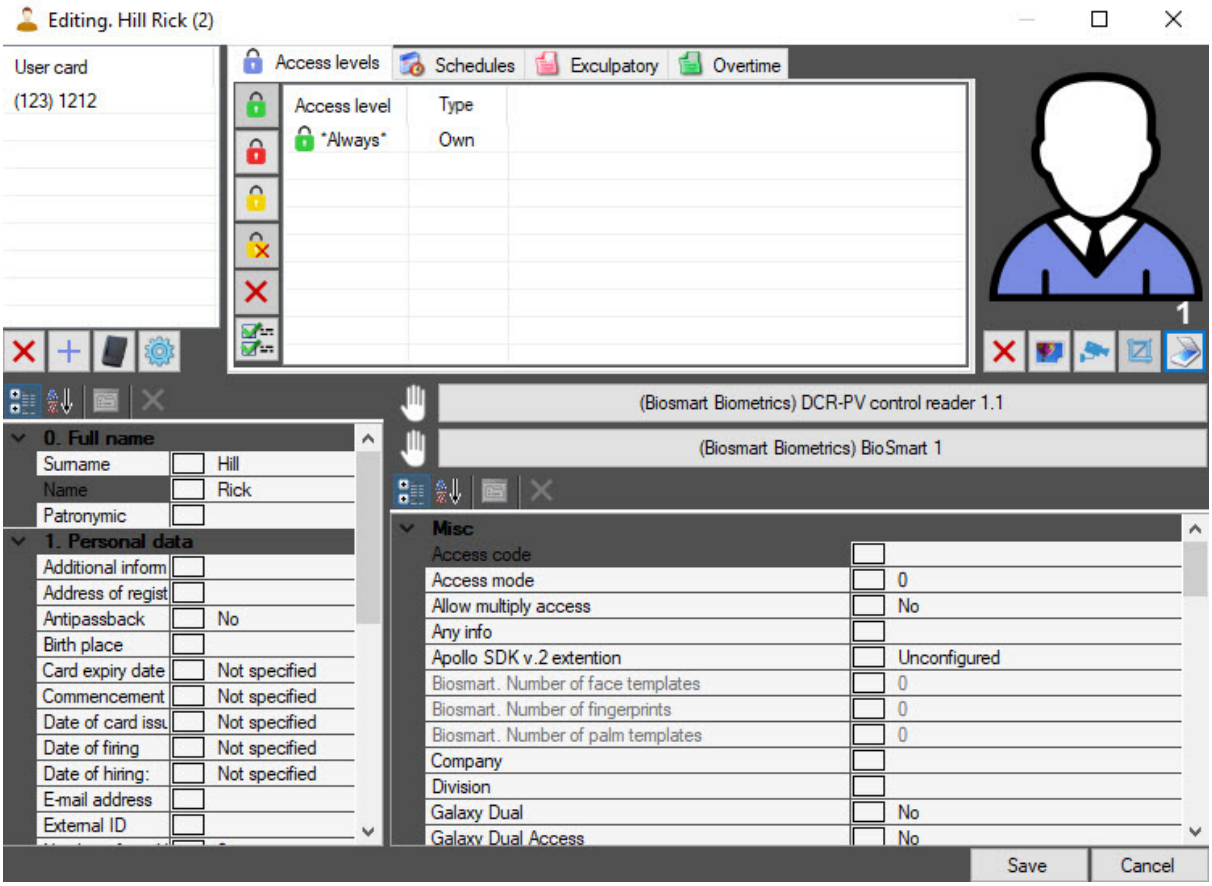
Filling out the user parameters using the ABBYY PassportReader SDK module

The *ABBYY PassportReader SDK* module is used to fill out the users parameters in the *Access Manager* module automatically after the images of the identification documents are recognized (passport, driver's license, passport for traveling abroad, birth certificate, and so on), including the images of the identification documents of some CIS countries (Azerbaijan, Belarus, Kazakhstan, Kyrgyzstan, Tajikistan, Uzbekistan) and foreign passports of any country (MRZ analyzed) from the scanner or hard disk.

The *ABBYY PassportReader SDK* module allows you to recognize user information from images downloaded from a file or obtained using any configured scanner that is connected to the computer.

To set the user parameters using the *ABBYY PassportReader SDK* module, do the following:

1. Go to user editing (see Going to user editing).



2. Click the  button (**1**). As a result, the **Document recognition** window opens.

> **Note**
>
> If this button is inactive, check if the *ABBYY PassportReader SDK* module is configured correctly (see Configuring the ABBYY PassportReader SDK module).

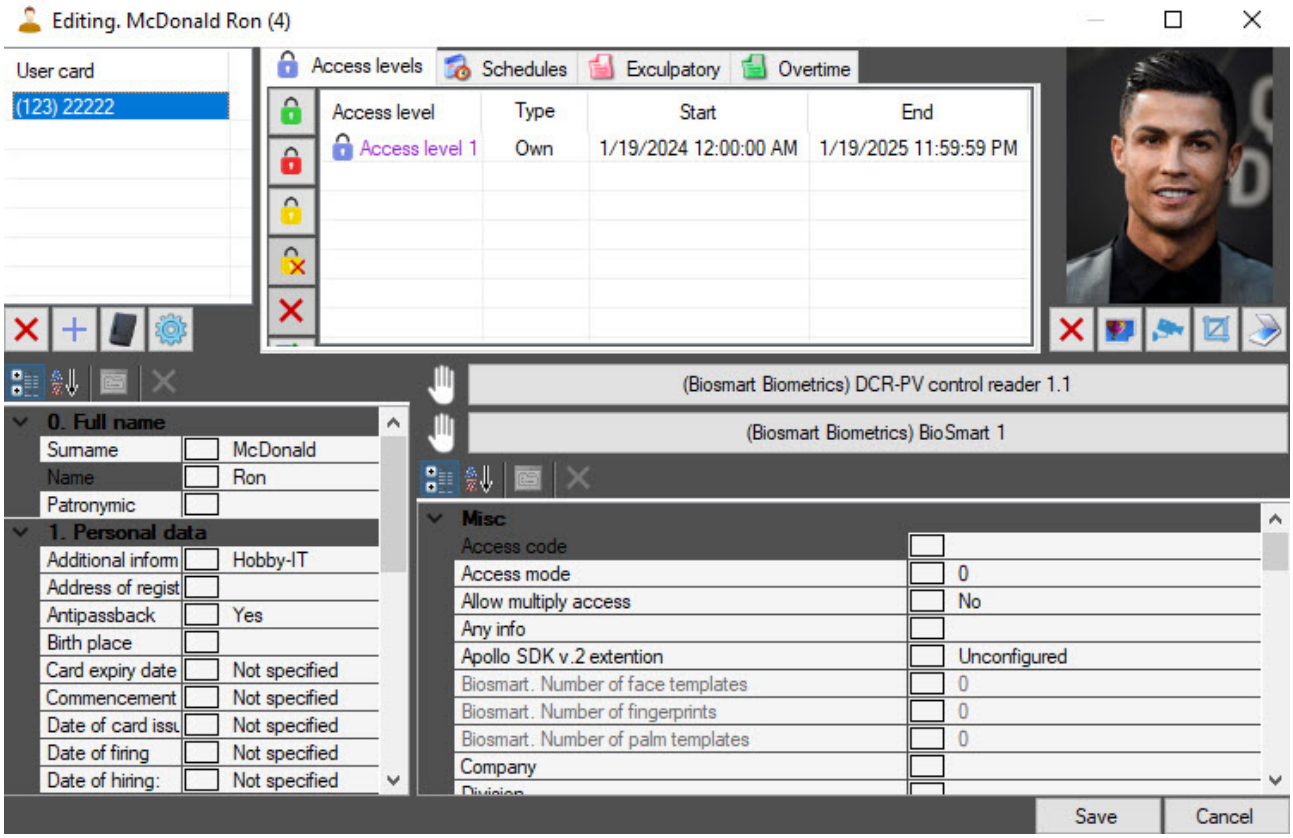
3. Select the way you want the passport information to be provided:
   - Click the **Scan** button if you want to scan the document using the scanner selected by default in Windows OS (see Windows hardware settings). When you click this button, the pre-scan of the document starts.
   - Click the **From file** button if you want to download a photo of the document from a file. When you click this button, the standard open file dialog window opens, in which you need to select the corresponding photo of the first page of the document that you want to download.
4. When working with the *ABBYY PassportReader SDK* module, you can do the following:
   a. Select a printer.
   b. Rotate the scanned image, selecting the necessary value from the **Rotate** drop-down list:
      i. **Do not change**
      ii. **Rotate right**
      iii. **Rotate left**
      iv. **Rotate 180°**.
   c. Select the type of the document.
   d. Display the license serial number and the number of the remaining recognitions. The number of the remaining recognitions in the license is specified after the word **activated**.

The values in the fields that are marked red are offered to the operator to double-check and, if necessary, make changes to them. After the operator checks and makes changes to them, the field turns green, which means that the field has been checked.

Assigning an access card to a user

General information about assigning access cards to a user

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



The object code is specified in brackets; next is the card code. You can set the format of the access card in the **Access Manager** object settings (see Configuring access cards).

You can assign several access cards to one user.

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

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

1. Manually.

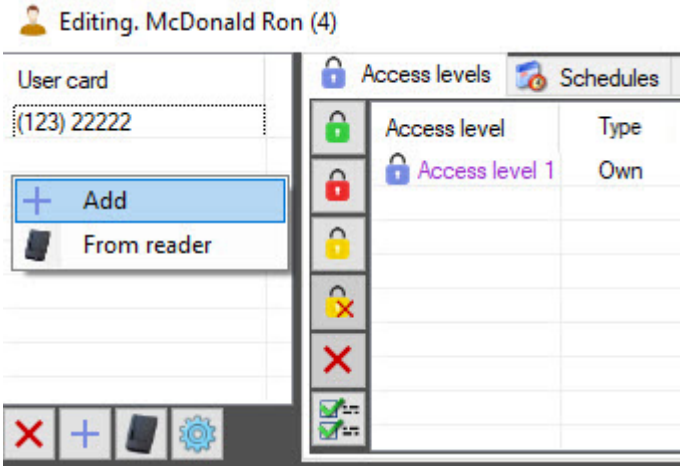
2. Using the control reader.

> **Note**
>
> The list of control readers used for user access card input is specified when configuring the system—see Configuring control readers in the Access Manager.

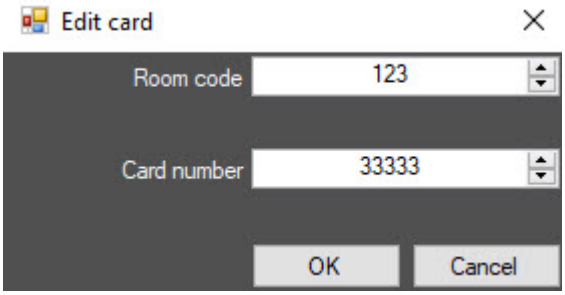
Manual input of access card number

To input access card number manually, do the following:

1. Go to user editing (see Going to user editing).
2. Right-click the list of cards area.
3. Select the **Add** item in the function menu.

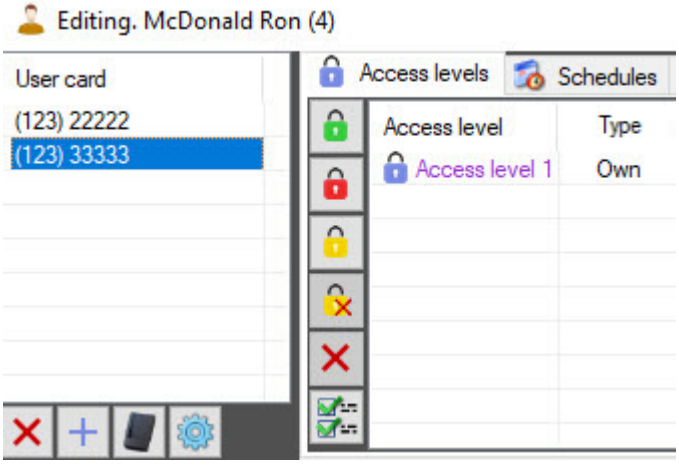


Window for inputting object code and card code opens.



4. Enter the object code (facility code, room code) in the **Room code** field.
5. Enter the card code in the **Card number** field.
6. Click the **OK** button.

7. The card is added to the list.



Manual input of the access card number is complete.

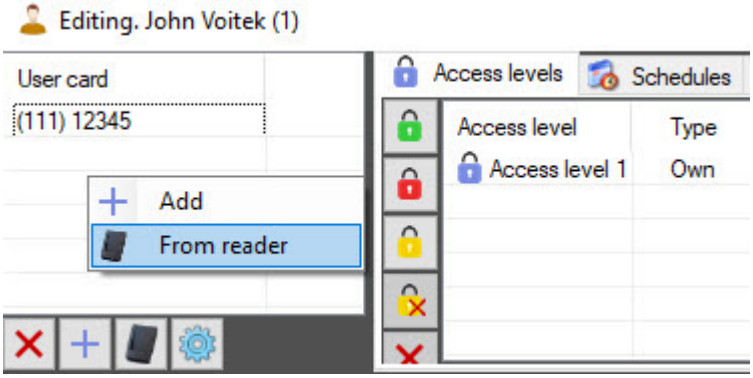
> **Note**
>
> You can also input the access card number manually using the corresponding buttons (see Specifying user parameters).

Entering an access card number using a control reader

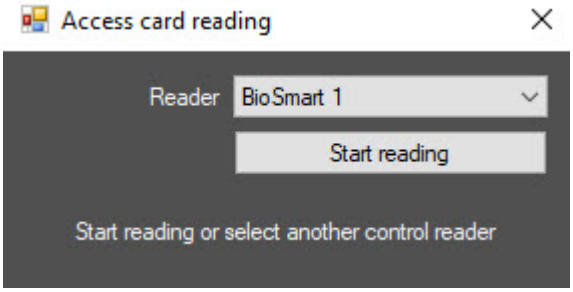
> **Note**
>
> You can enter an access card number using a control reader by clicking the corresponding button  (see Specifying user parameters).

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

1. Go to user editing (see Going to user editing).
2. Right-click the card list area.
3. In the function menu, select the **From reader** item.



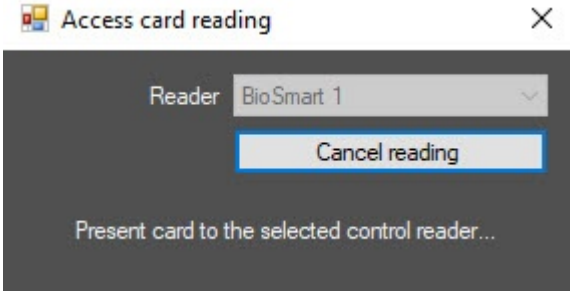
The **Access card reading** window opens.



4. From the **Reader** drop-down list, select a control reader that is used for entering the access card number.

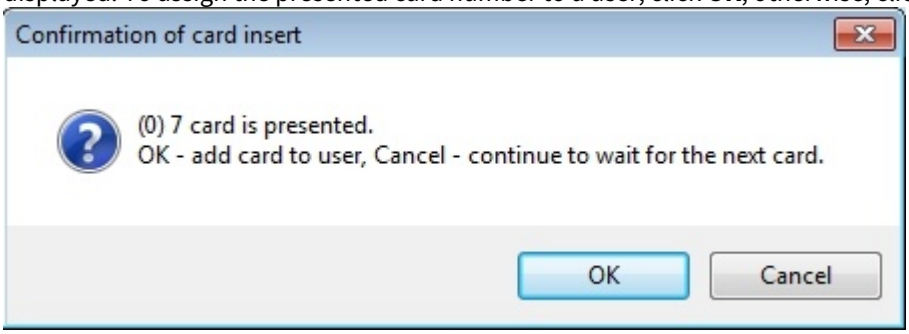
> **Note**
>
> The list of available control readers is specified when configuring the system (see Configuring control readers in the Access Manager).

5. Click the **Start reading** button. The **Access card reading** window will look like this:

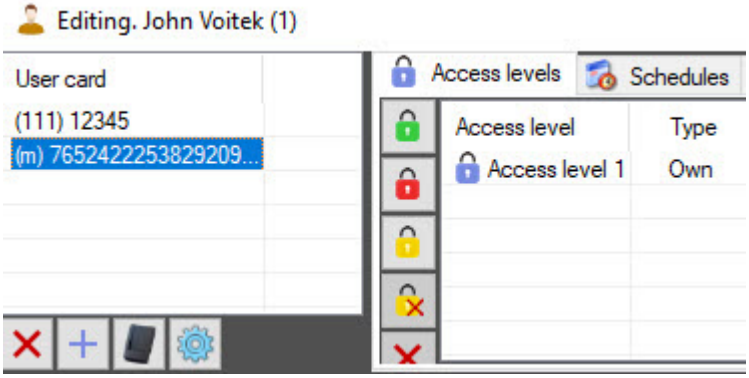


> **Note**
>
> To cancel the reading of an access card, click the **Cancel reading** button.
> If you select *Universal Reader*, when you click the **Start reading** button, a settings window opens. For the description of settings, see Entering an access card number using a universal reader.

6. Bring the access card to the selected reader.
7. If confirmation of card insert by operator is configured, the **Confirmation of card insert** window is displayed. To assign the presented card number to a user, click **OK**, otherwise, click **Cancel**.

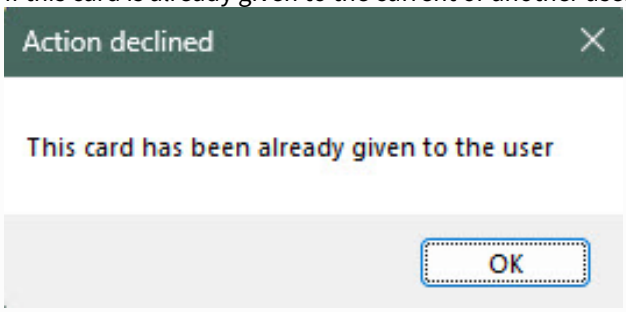


8. The **Access card reading** window closes, and the number of the presented access card is added to the list.



Note

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



9. To save the changes, click the **Save** button in the user editing window.

Entering an access card using a control reader is complete.

Entering an access card number using a universal reader

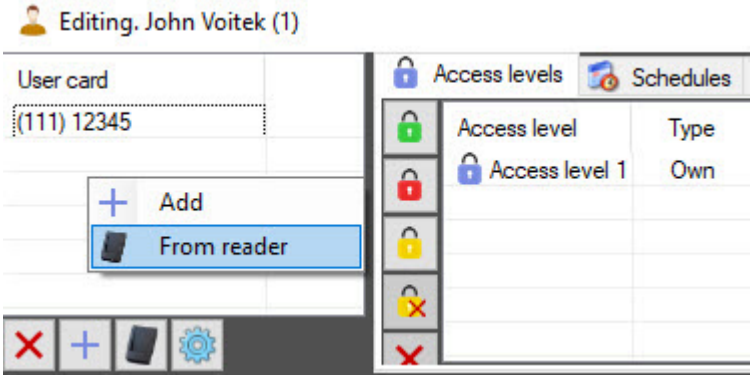
Note

You can enter an access card number using a universal reader by clicking the corresponding button  (see Specifying user parameters).

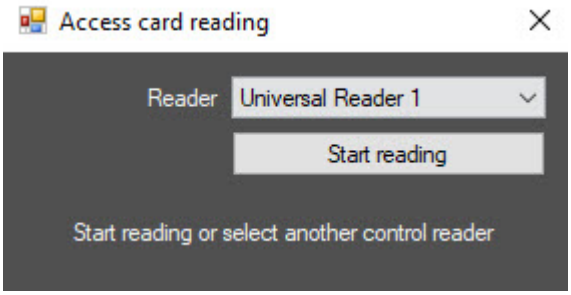
To enter an access card number using a universal reader, do the following:

1. Go to user editing (see Going to user editing).
2. Right-click the card list area.

3. In the function menu, select the **From reader** item.



The **Access card reading** window opens.



4. From the **Reader** drop-down list, select **Universal Reader** that is used for entering the access card number.

> **Note**
>
> You must create and configure a universal reader (see Configuring a universal reader).
> The list of available control readers is specified when configuring the system (see Configuring control readers in the Access Manager).

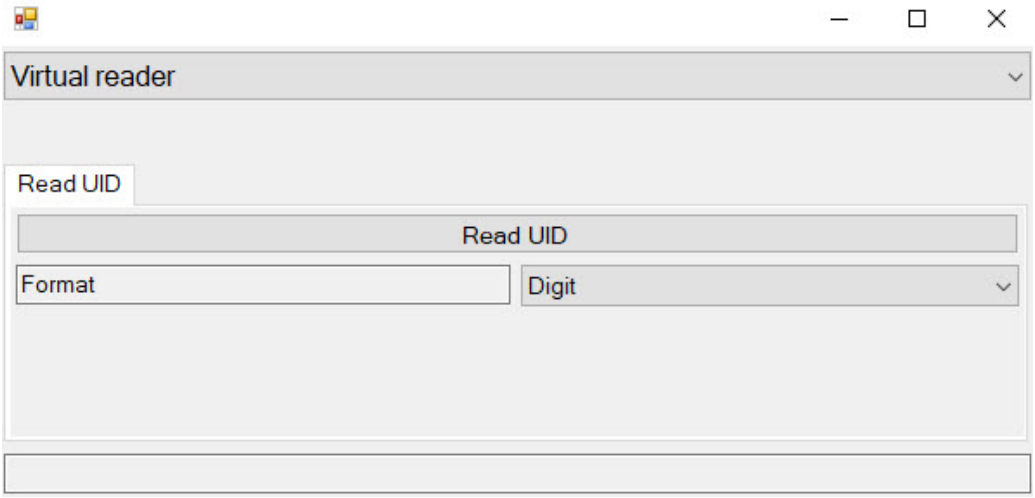
5. Click the **Start reading** button.

> **Note**
>
> If the **Auto-read** checkbox is clear (see Configuring a universal reader), when you click the **Start reading** button, a settings window opens (see below). If the **Auto-read** checkbox is set, an access card must be presented at once, the settings window doesn't open.

You can work with a universal reader via *Virtual reader*.

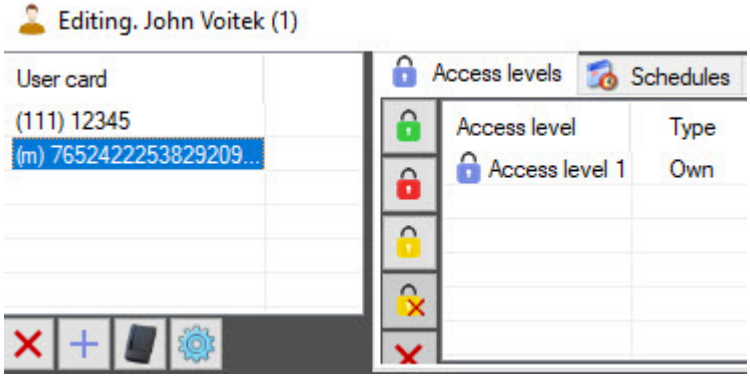
a. Select a *Virtual reader*.

i. From the **Format** drop-down list, select the required card format: **Digit**, **HEX**, **W24**, **W32**.



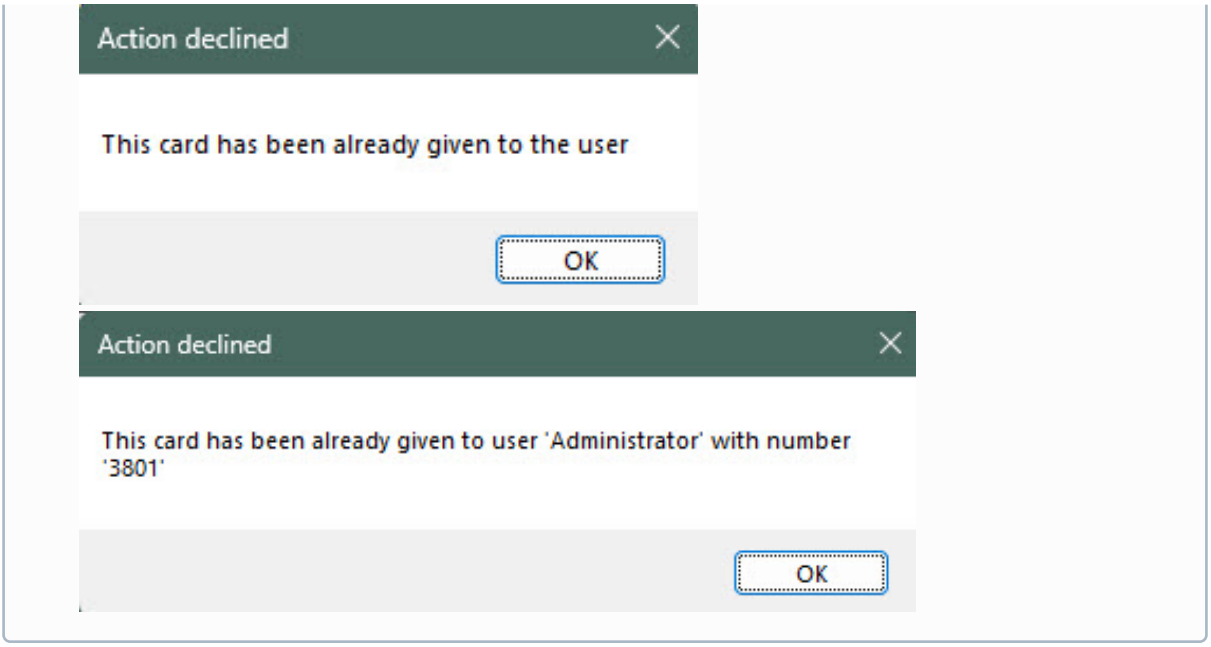
ii. Click the **Read UID** button. The process of reading the number of an access card starts.

6. The number of the presented access card is added to the list of the user's cards.



Note

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

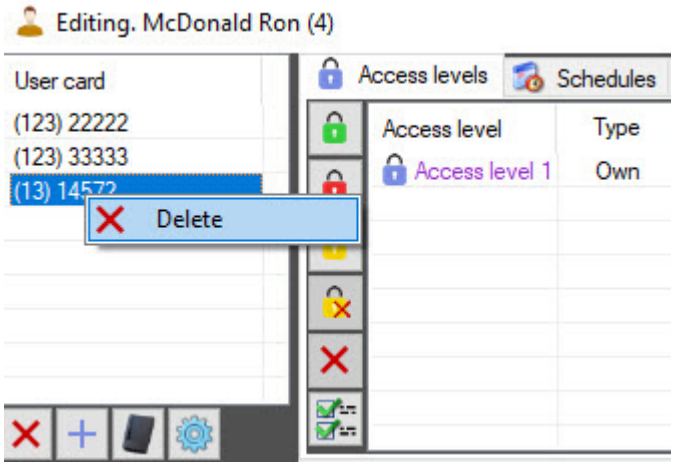


7. To save the changes, click the **Save** button in the user editing window.

Entering an access card using a universal reader is complete.

Deleting a user access card

To delete a card number from the list, right-click the card number in the list and select the **Delete** item in the function menu.



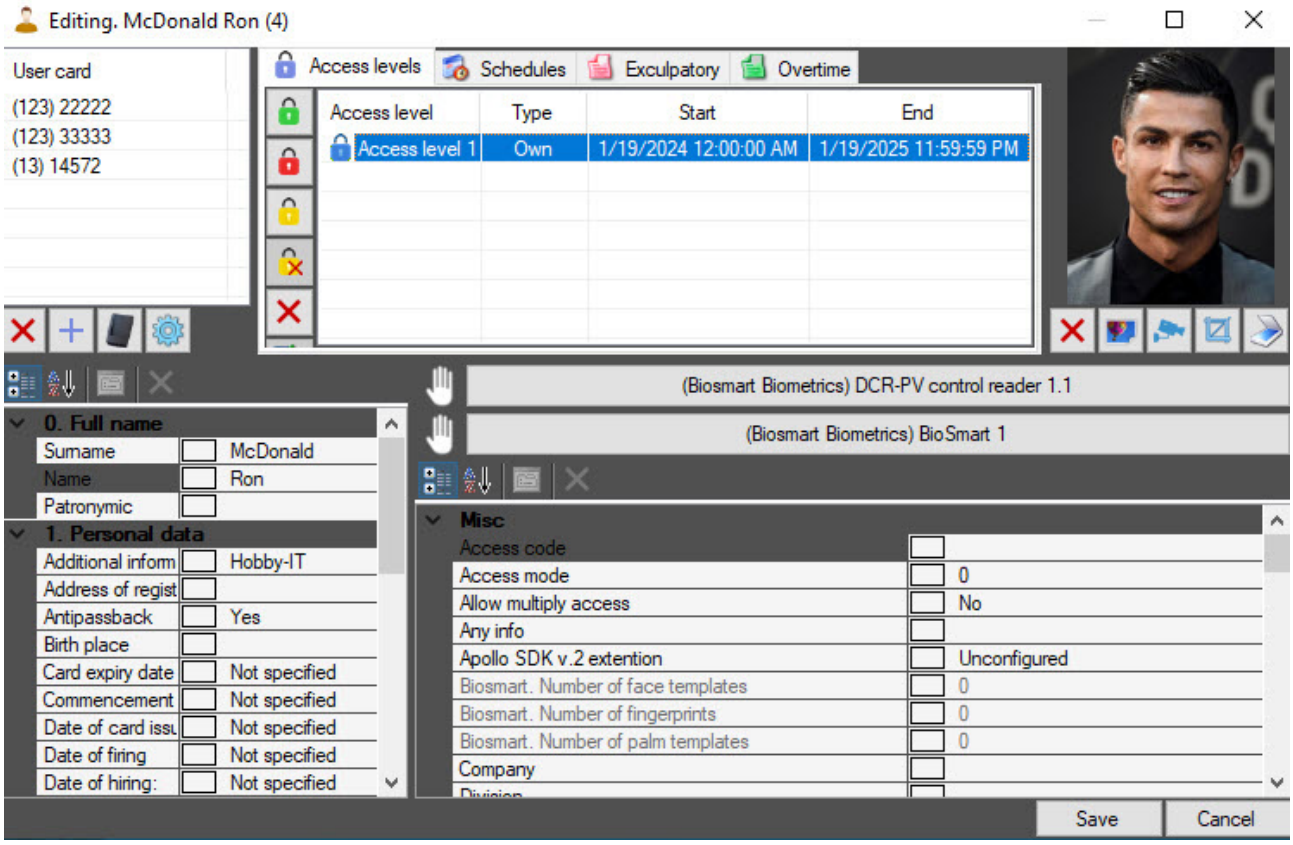
Note

You can also delete a card number using the corresponding button (see Specifying user parameters).

Assigning access levels to a user

General information about assigning access level to a user

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



The **Comment** column specified whether the access level is inherited from Department (**Inherited**) or assigned to a user separately (**Own**). Configuring the rules of department access level inheritance is described in Configuring the department access level inheritance. Adding access levels to a user (**Own**) is described in Assigning Own access level to a user.

You can assign several access levels to a single user.

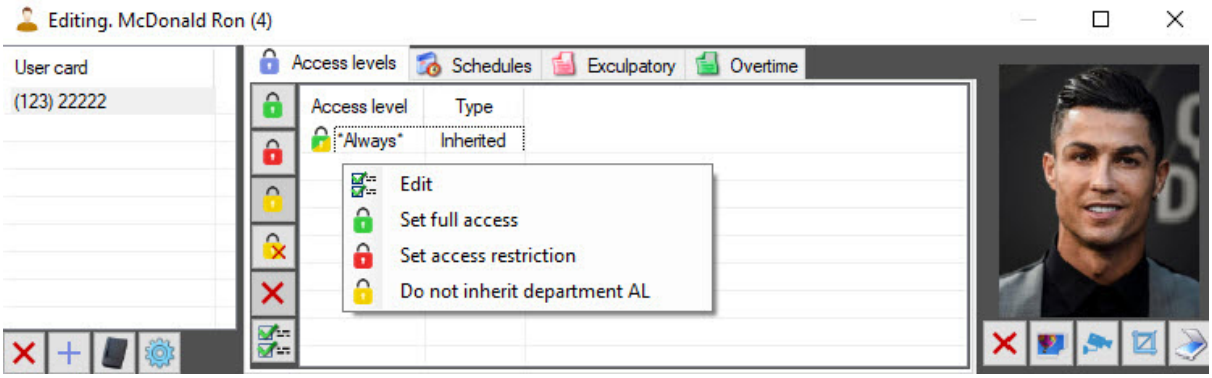
> **Attention!**
>
> The assignment of several access levels to a single user must be supported by hardware and by an appropriate integration module. If several access levels are assigned to a user, but the ACS hardware or the integration module supports only one access level, then all levels, except the first one in the list, are ignored by the system.
> The support for several user access levels has been tested in the following integration modules: ApolloSDK, Elsys, ParsecNet, HID, Suprema, Salto, Perco S20 v.2, BioSmart2, Noder. For information on other integration modules, please contact AxxonSoft technical support.

Assigning Own access level to a user

To assign a user **Own** access level, do the following:

1. Go to user editing (see Going to user editing).

2. Right-click the access levels list.



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

     Attention!

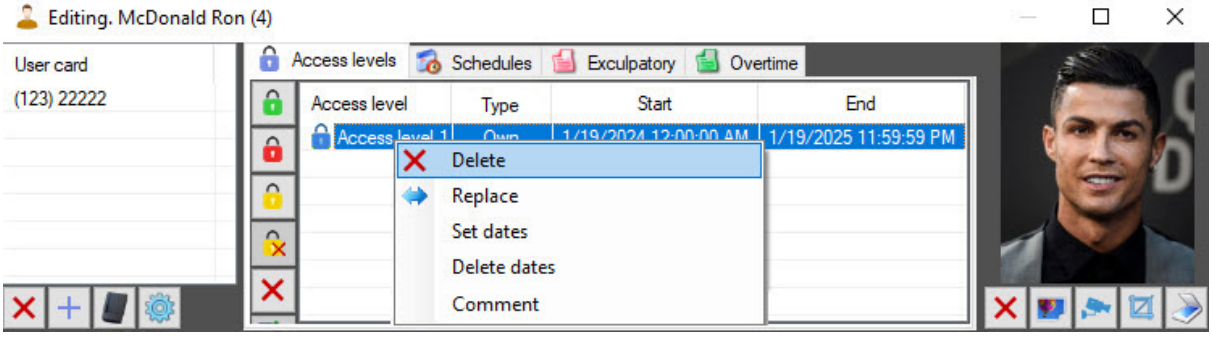
     If **Always** or **Never** access levels are inherited, then the added **Own** access levels are ignored.

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

     Note

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

   - If you disable the department access level inheritance by selecting the **Do not inherit department AL** item, the user is also assigned the **Own** access level (see Configuring the department access level inheritance)
4. To delete the **Own** access level, right-click the required access level and select **Delete**.

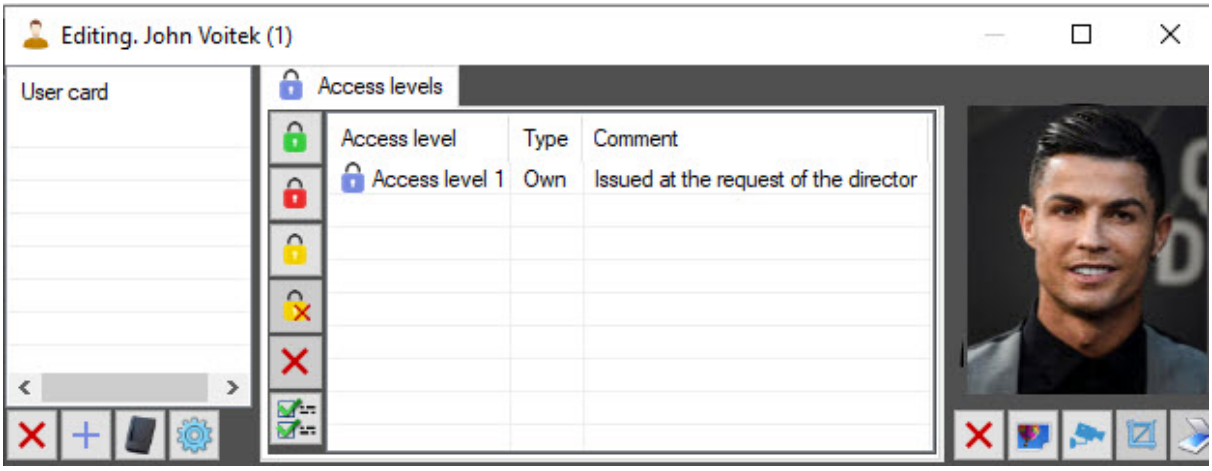


Note

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

5. To replace one access level (**Own**) with another, right-click the corresponding access level and select **Replace**. The **Search access level** window opens. In this window, select one or several access levels (see Working with the Search access level window).
6. To add a comment to the **Own** access level, right-click the corresponding access level and select **Comment**. Enter the comment in the form that opens, and click the **OK** button. This comment is displayed in the table

of user access levels.



Note

You can add a comment to the **Own** access level only that isn't inherited from a department and isn't the **Always** or **Never** system access level.

Assigning the **Own** access level to a user is complete.

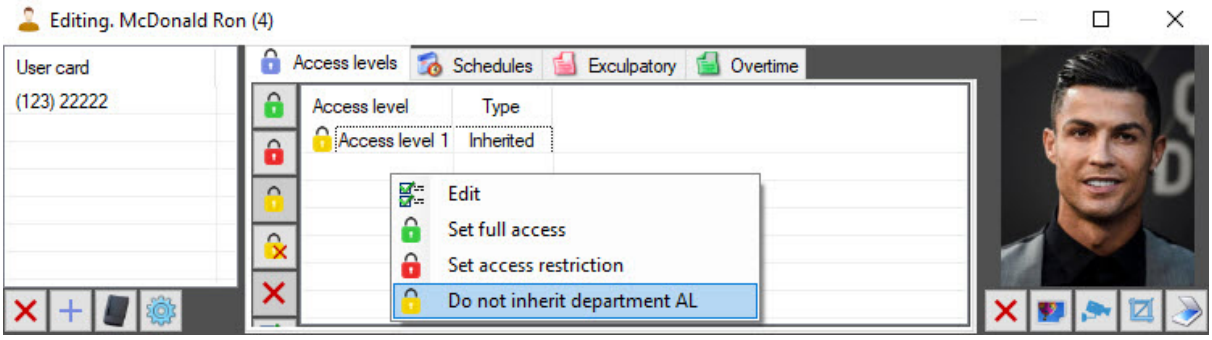
Note

You can perform all the actions described above using the corresponding buttons (see Specifying user parameters).

Configuring the department access level inheritance

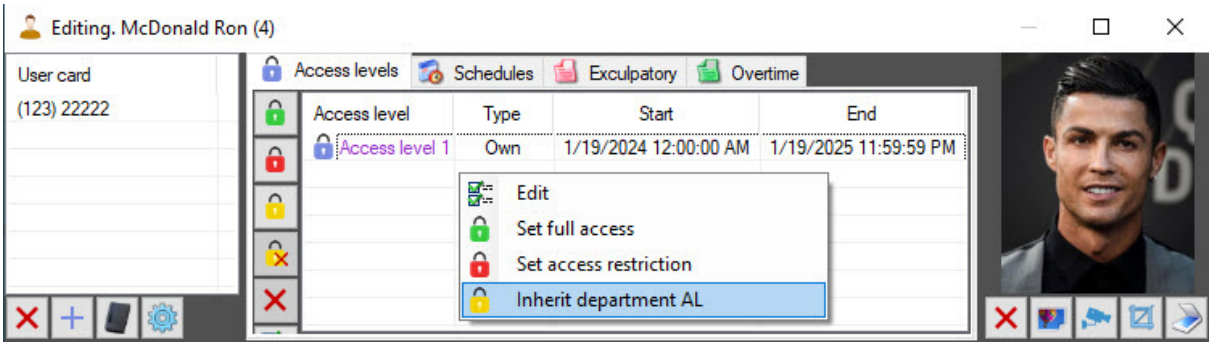
By default, the user inherits the department access level. If it's required not to inherit the department access level, do the following:

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



3. In the function menu, select the **Do not inherit department AL** item. If a user doesn't have any other access levels assigned except the inherited one, the **Search access level** window opens. In this window, select one or several access levels (see Working with the Search access level window). As a result, the inherited access level is deleted from the list.

4. To restore the inheritance of department access levels, select the **Inherit department AL** item in the function menu.



Configuring of department access level inheritance is completed.

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

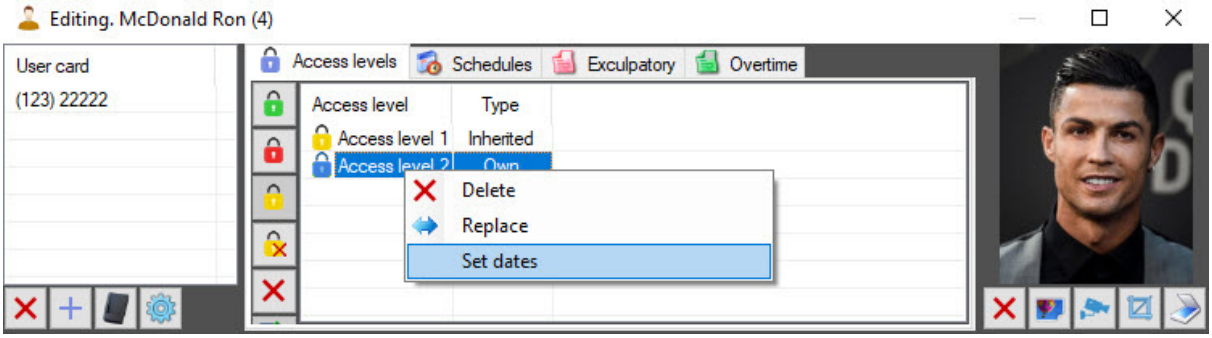
Assigning a temporary access level to a user

> **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.

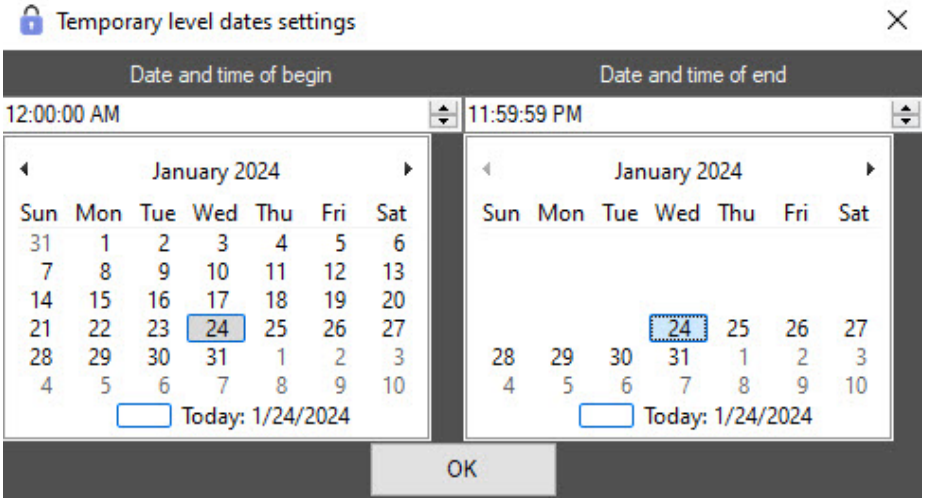
To assign a temporary access level to a user, do the following:

1. Go to user editing (see Going to user editing).
2. Right-click the required access level (**Own**) that you want to make a temporary one (see Assigning Own access level to a user).

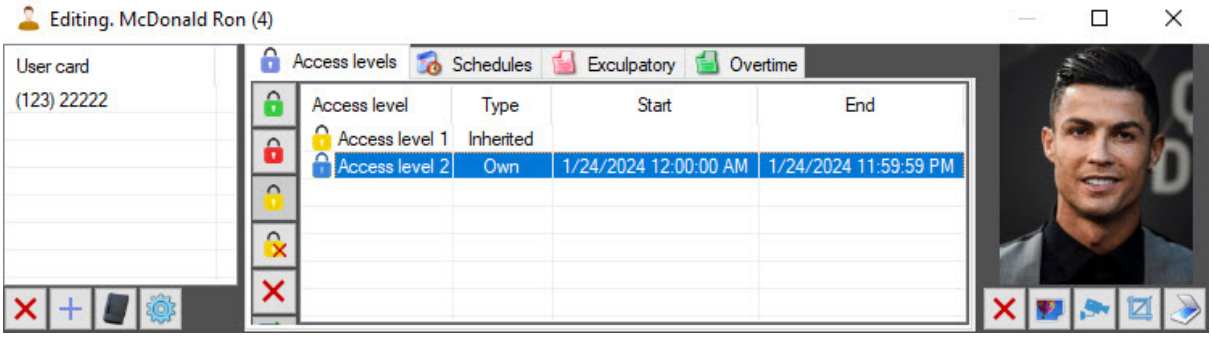
> **Note**
>
> You can also select several access levels (**Own**): for example, by selecting them with the mouse or by using keyboard shortcuts (see Keyboard shortcuts for working with interface elements).



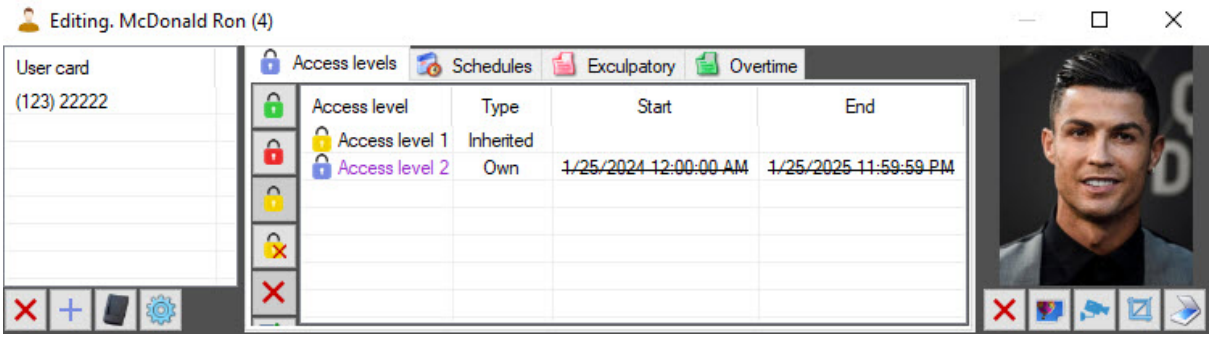
3. In the function menu, select the **Set dates** item. The **Temporary level dates settings** window opens. In that window, select the beginning and end of the temporary access level and click **OK**.



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



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



Note

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

Assigning a temporary access level to a user is complete.

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

General information about assigning a photograph to a user

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

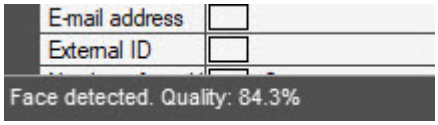
1. From a file.
2. From a video camera.

> **Note**
>
> List of video cameras used for assigning photograph to users is specified while system configuring (see the Selecting and configuring cameras in the Access Manager section).

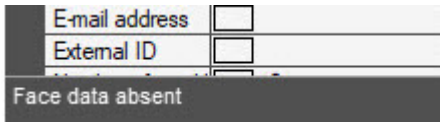
Assigned photographs are stored in the *<ACFA PSIM* installation directory>/Bmp/Person folder. Name of the file with the user's photograph is the same as the user ID. Content of the Bmp/Person folder is synchronized on all servers of distributed system.

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 PSIM* Face recognition server (see Configuring the interaction with the Face PSIM 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 PSIM* reference face database (see Appendix 5. Face synchronization module).

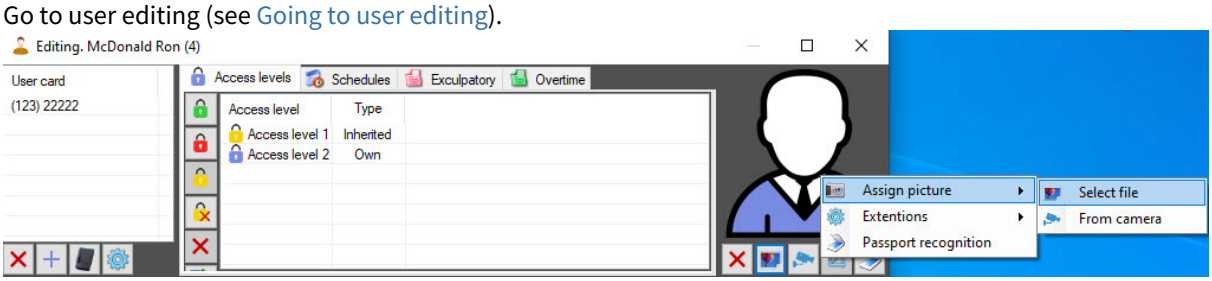
> **Note**
>
> If the quality of the face photo does not meet the requirements specified on the **Face recognition server** object settings panel, then this user will not be synchronized.

You can check the quality of the already assigned user photos using the CHECK_QUALITY_START command (for details, see FIRSERVER commands, Examples of frequently used scripts). This check is used, for example, in two-factor verification (see Configuring two-step verification).

Assigning a photo to a user from a file

To assign a photo to a user from a file, do the following:

1. Go to user editing (see Going to user editing).



2. Click the  button.
3. In the standard Windows dialog window, select a file with a photo that will be assigned to the user.

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

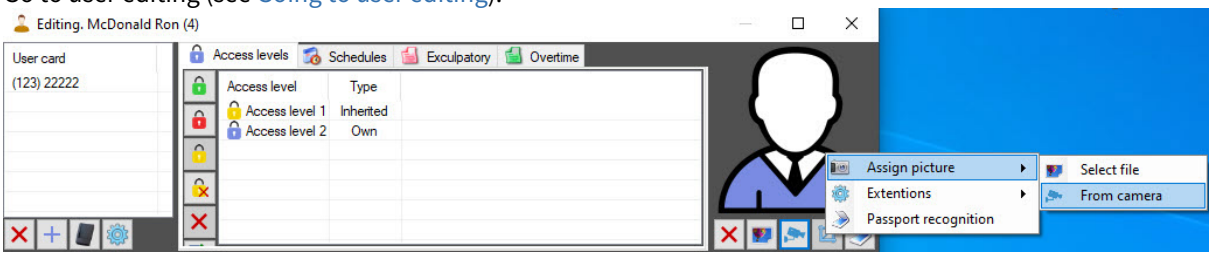
Assigning a photo to a user from a file is complete.

Assigning a photo to a user from a camera

To assign a photo from a camera, do the following:

> **Note**
>
> The list of cameras used for assigning photos is specified when you configure the system (see Selecting and configuring cameras in the Access Manager).

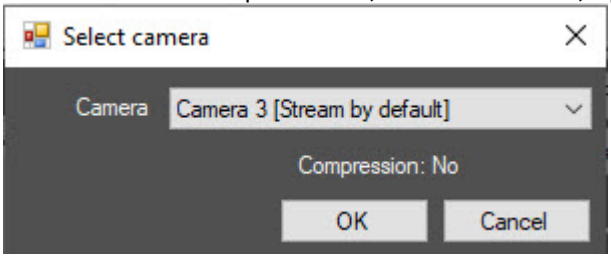
1. Go to user editing (see Going to user editing).



2. Click the  button. The **Select camera** window opens.

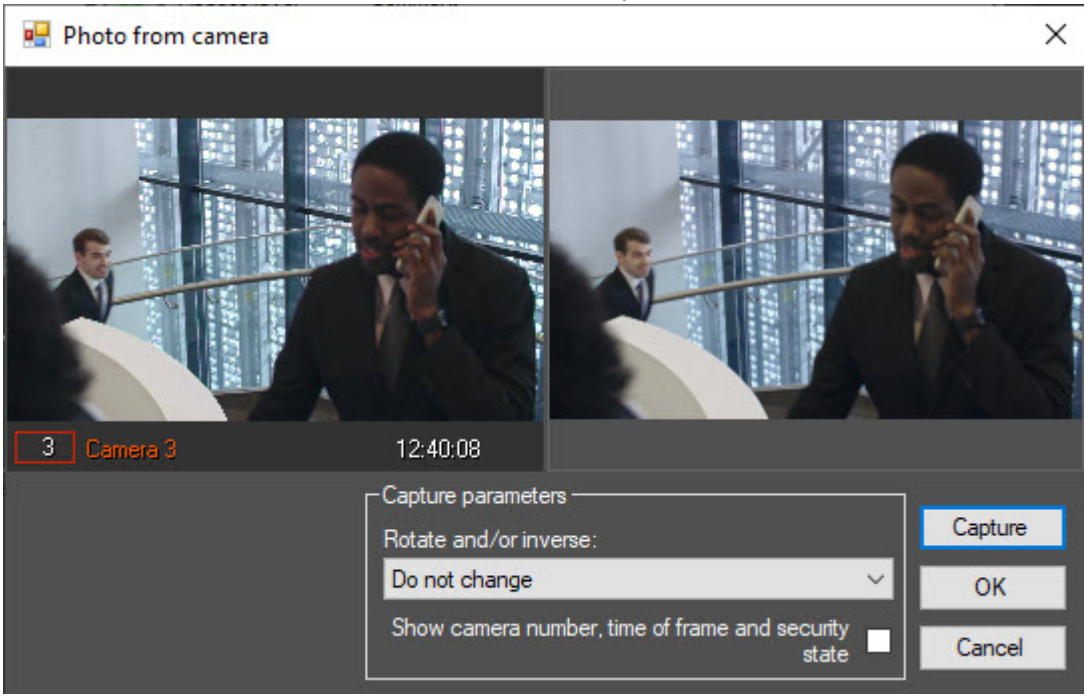
> **Note**
>
> You can also open the **Select camera** window by right-clicking the user's photo area and selecting **Assign picture** → **From camera** in the function menu.

3. From the **Camera** drop-down list, select the camera, a photo from which you want to assign to a user.



> **Note**
>
> You can specify the compression level of the video signal used for assigning a photo on the **Cameras** tab on the settings panel of the **Access Manager** object. From the **Compression** drop-down list, select the required level of video signal compression. Compression level increases from 0 (no compression) to 5 (maximum compression) (see Selecting and configuring cameras in the Access Manager).
> Configuration of compression is relevant if you use analog cameras. We don't recommend using compression for IP cameras.

4. Click the **OK** button. The **Photo from camera** window opens.



5. Video from the selected video camera is displayed in the left part of the window.
6. If necessary, select the method of frame processing from the **Rotate and/or inverse** drop-down list. The following methods of frame processing are available:
   a. Do not change (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.
7. By default, the frame is saved without the information about camera number, time the frame was received, and without the information about whether the camera is armed or disarmed (the latter is determined by the color of the frame around the camera). If you want to add this information to the captured frame with the user image, set the **Show camera number, time of frame and security state** checkbox.

> **Note**
>
> Rotation and superimposition of camera data on the image must be specified before capturing the image, because changing the settings after capturing doesn't affect the already captured frame.

8. Wait for the appropriate frame with the user image and click the **Capture** button.
9. The captured frame is displayed in the right part of the window.
10. Click the **OK** button. The received frame is assigned as the user photo.

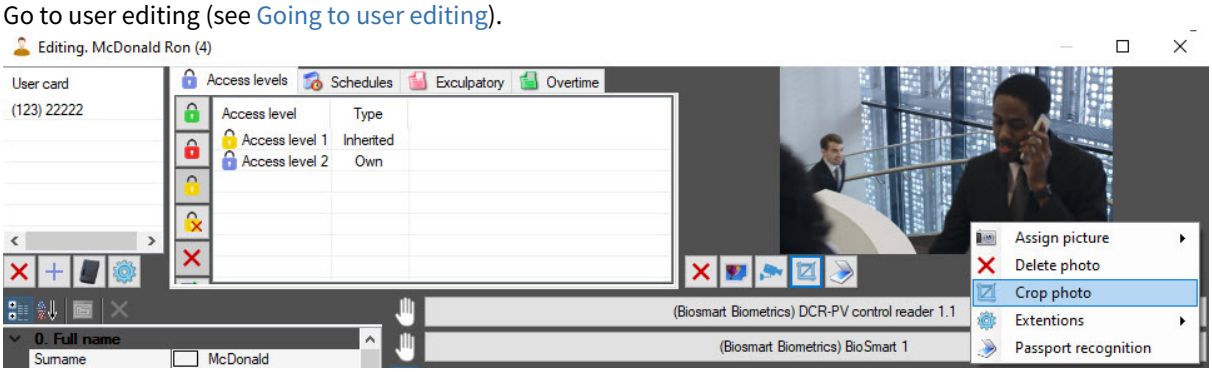
Assigning a photo to a user from a camera is complete.

Cropping a photo

In the *Access Manager* software module, you can crop a photo assigned to a user.

To crop a photo, do the following:

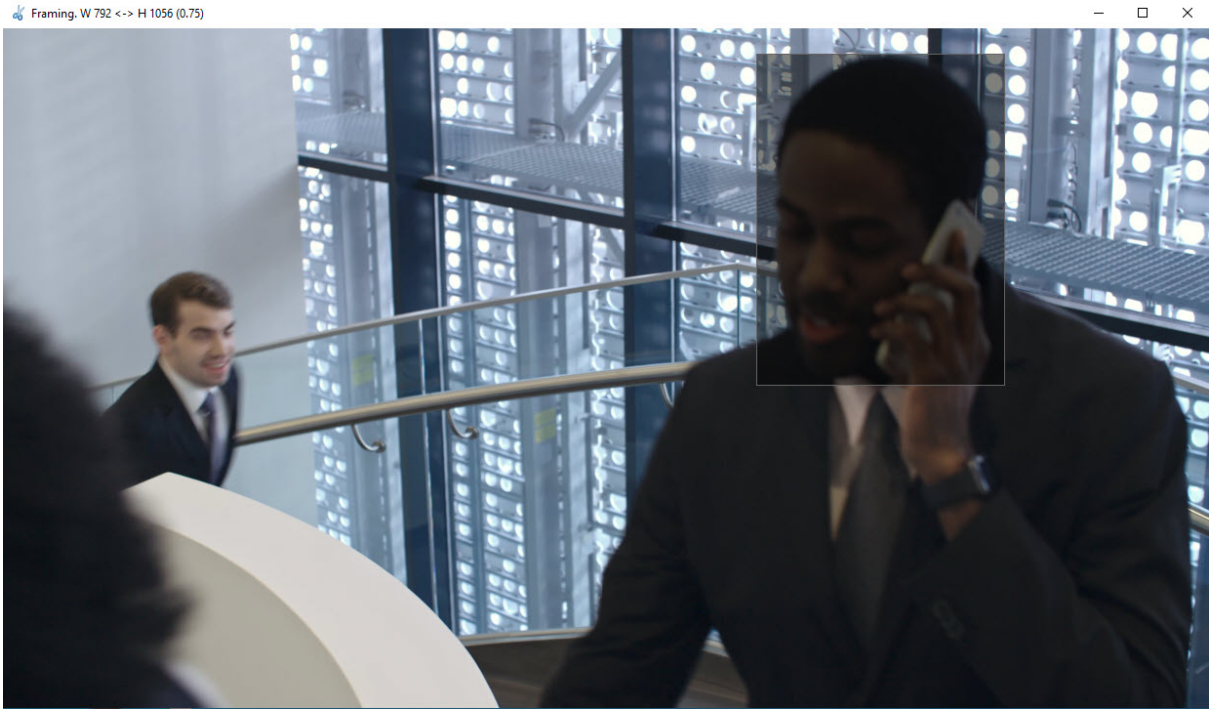
1. Go to user editing (see Going to user editing).



2. Click the  button. As a result, the **Framing** window opens.

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

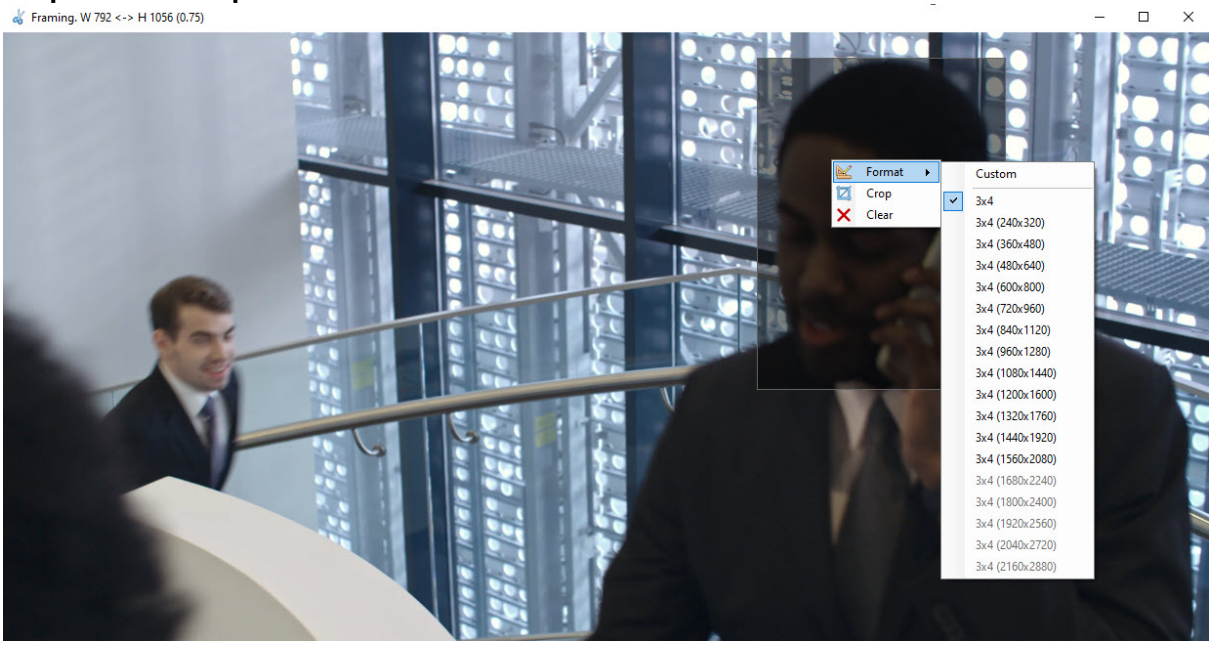
3. Select the area that you want to leave on the photo. To do this, left-click the required point and stretch the rectangle marking the selected area. You can move the selected area by holding down the left mouse button on the rectangle.



Note

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 the selected area or the area not marked by the rectangle, and in the function menu, select **Format** → **<required size or aspect ratio>**.



5. To delete the selected area, left-click the area not marked by the rectangle and make the selection again. Or right-click the selected area and select **Clear** in the function menu.

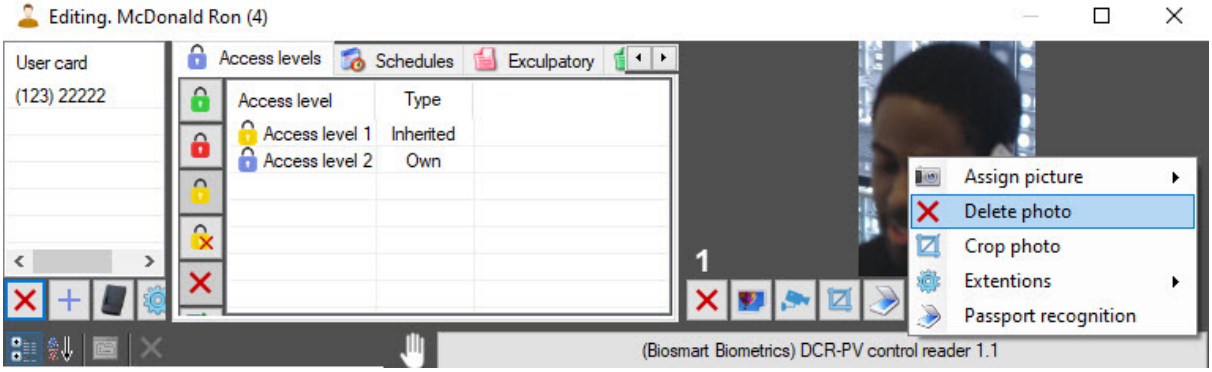
6. To confirm cropping of the photo, right-click the selected area and select **Crop** in the function menu.
7. To save the changes, click the **Save** Save button in the user editing window.

Cropping a photo is complete.

Deleting a photo

To delete a user photo, do the following:

1. Go to user editing (see Going to user editing).



2. Click the button (**1**).

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

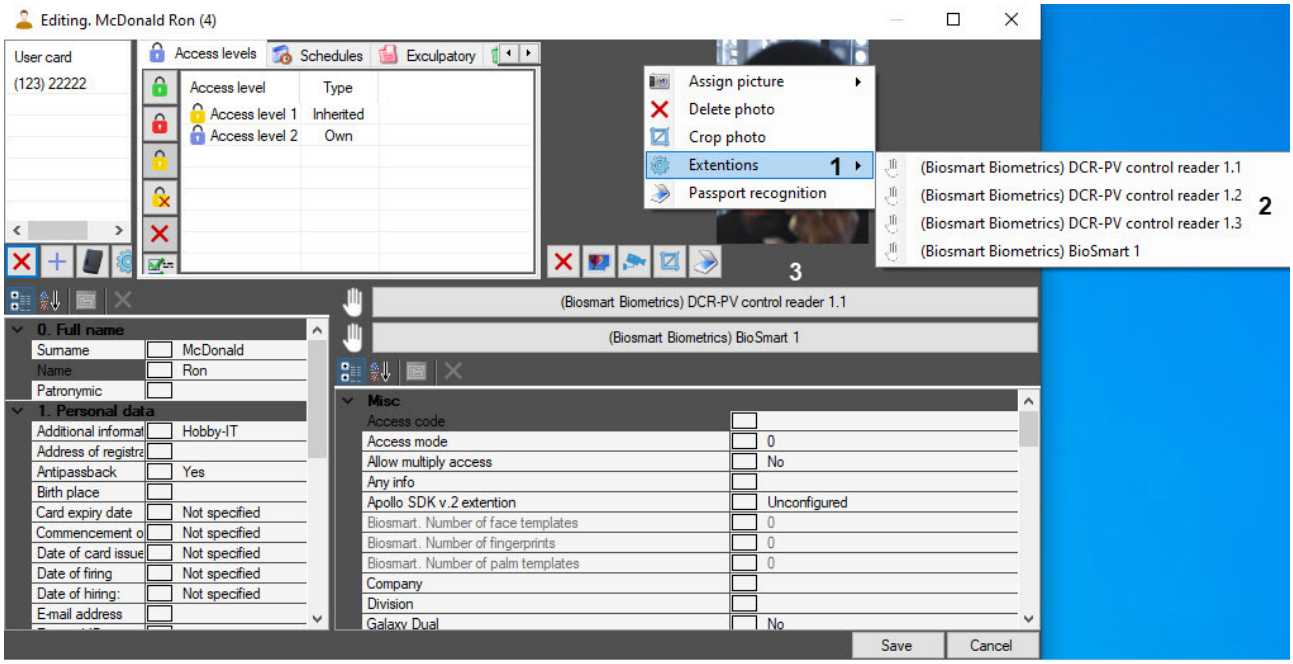
Deleting a user photo is complete.

Adding biometric parameters

You can add biometric parameters (faces, fingerprints, and so on) using control readers or biometric ACS terminals.

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

1. Right-click the user's photo and hover the mouse cursor 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 two steps, you can click this button (**3**).



As a result, a dialog window for adding user biometric parameters opens. This dialog window differs depending on the hardware that you use. Working with 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, you must 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, do the following:

1. Right-click the user's photo and hover the mouse cursor over the **Extensions** item (**1**).
2. Holding down the Shift key, click the extension from the list (**2**). As a result, the button with the selected biometric reader (**3**) is added to the area below the user's photo.

To remove the extension button, follow the same steps.

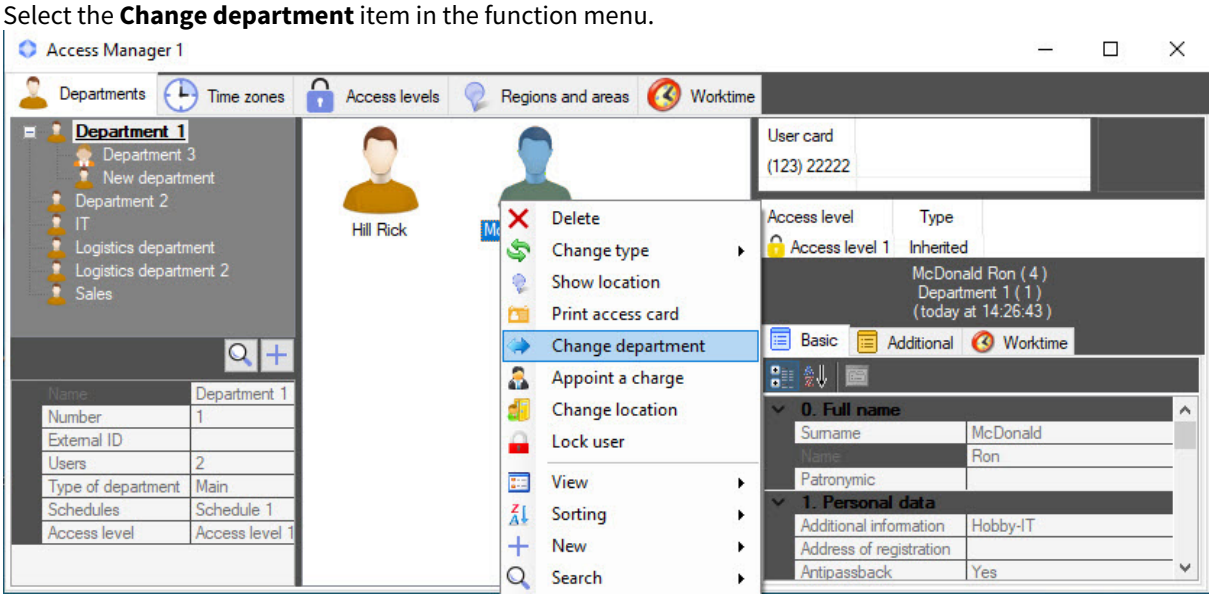
Transferring a user to a different department in the Access Manager software module

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

1. Go to viewing a list of users (see Viewing a list of users).
2. Right-click 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 interface elements).

3. Select the **Change department** item in the function menu.



4. In the **Search for department** window, select a department to which you want to transfer a user (see Working with the Search for department window).
   As a result, a user will be transferred to the selected department.

Transferring a user to a different department is completed.

Changing a user type

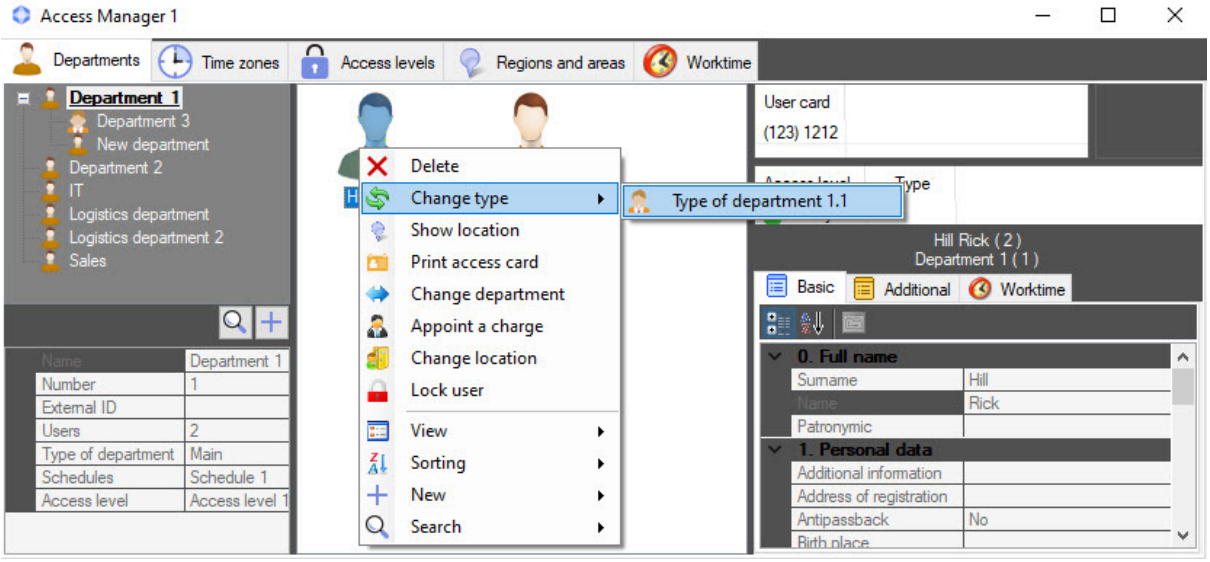
> **Attention!**
>
> You can change a user type only if you have the required permissions (see Configuring the rights to change user type, user department, and current region).

Change a user type as follows:

1. Go to viewing a list of users (see Viewing a list of users).
2. Right-click 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 interface elements).

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, a user type is changed.

Changing a user type is now completed.

Folder with user documents

Pre-configuring a folder with user documents

To be able to work with a user's network or local folder, do the following:

1. In the <Axxon PSIM installation directory>/Modules folder, open the **account_manager.run.config** file, and specify the path to the local or network folder in it.

```
</setting>
<setting name="NetworkFolder" serializeAs="String">
    <value />
</setting>
```

   a. If it is a local folder, the path to the folder must look like this:

```
</setting>
<setting name="NetworkFolder" serializeAs="String">
    <value>C:\InOut</value>
</setting>
```

   b. If it is a network folder, the path to the folder must look like this:

```
</setting>
<setting name="NetworkFolder" serializeAs="String">
    <value>\\DESKTOP-LM3U4BH\Users\Jane\Desktop\Shara</value>
</setting>
```

2. Save the **account_manager.run.config** file before closing it.

Pre-configuring a folder with user documents is complete.

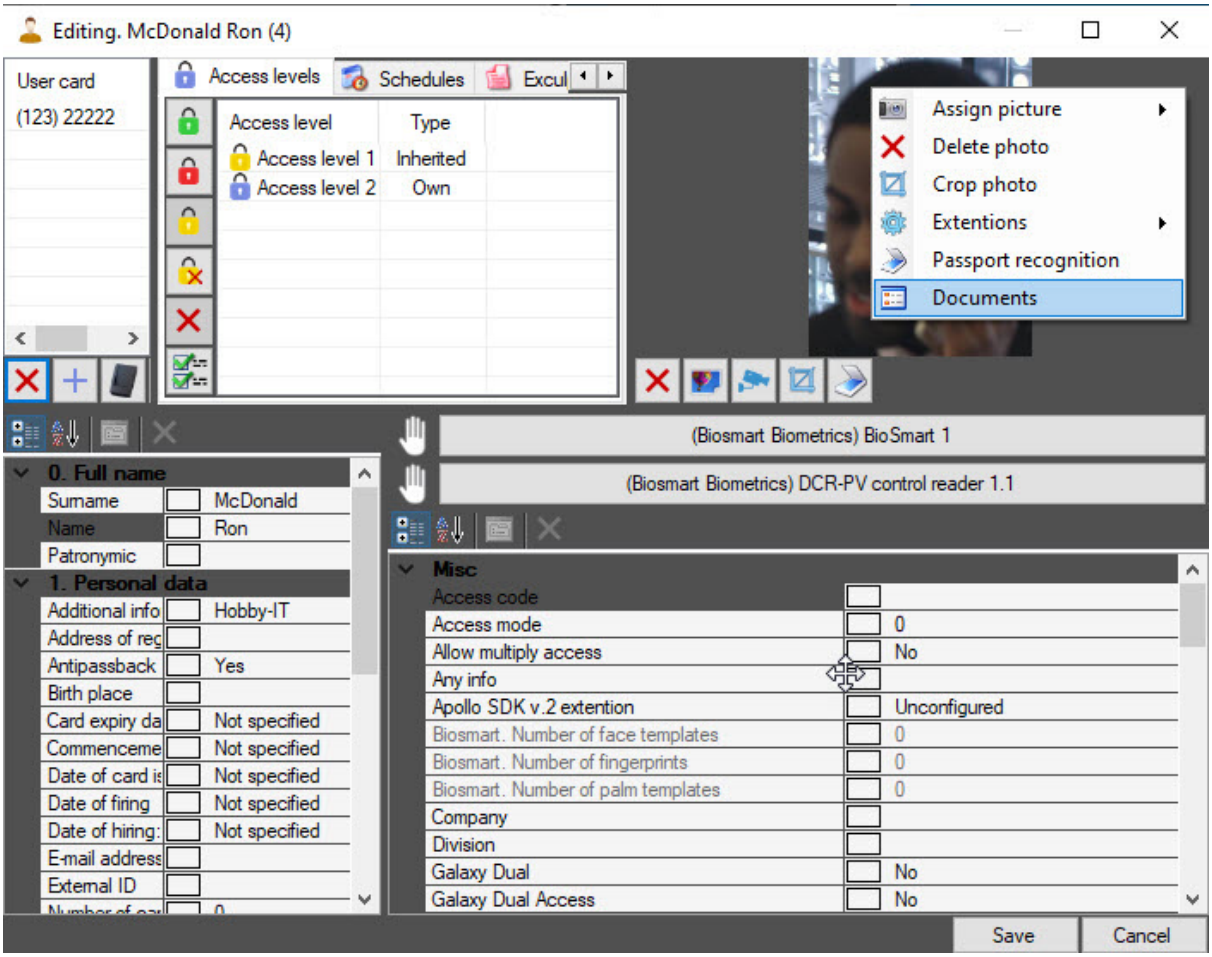
Note

A local or network folder must be created beforehand.

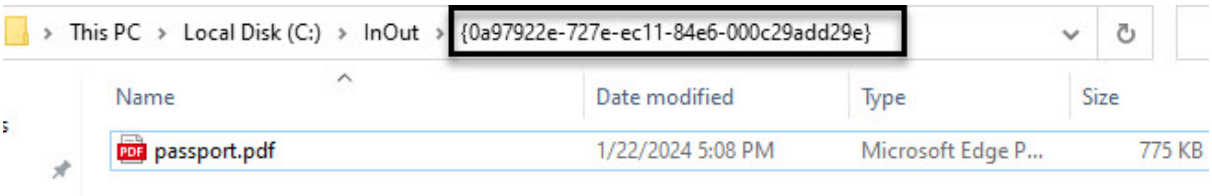
Opening a folder with user documents

To open a folder with user documents or a file from a folder with user documents, do the following:

1. Go to user editing (see Going to user editing).
2. Right-click the user photo.
3. Select the **Documents** item in the menu.



A folder with user documents looks like this:

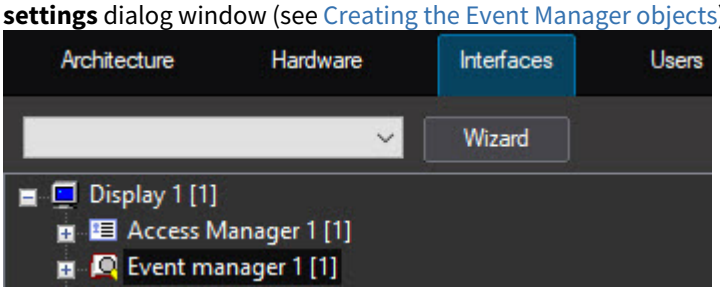


Opening a folder with user documents is complete.

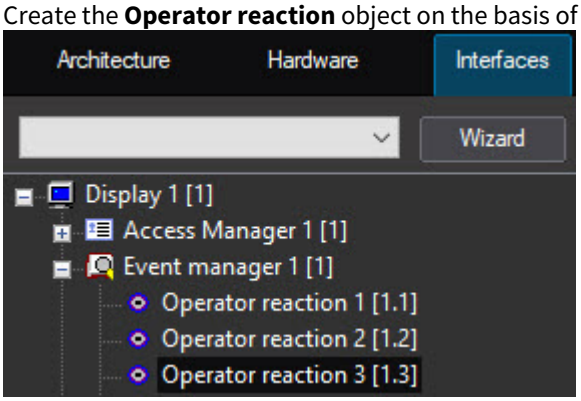
Configuring a quick opening of a folder with user documents or user file

To configure a quick opening of a folder with user documents or user file, do the following:

1. Create the **Event manager** object on the basis of the **Display** object on the **Interfaces** tab of the **System settings** dialog window (see Creating the Event Manager objects).

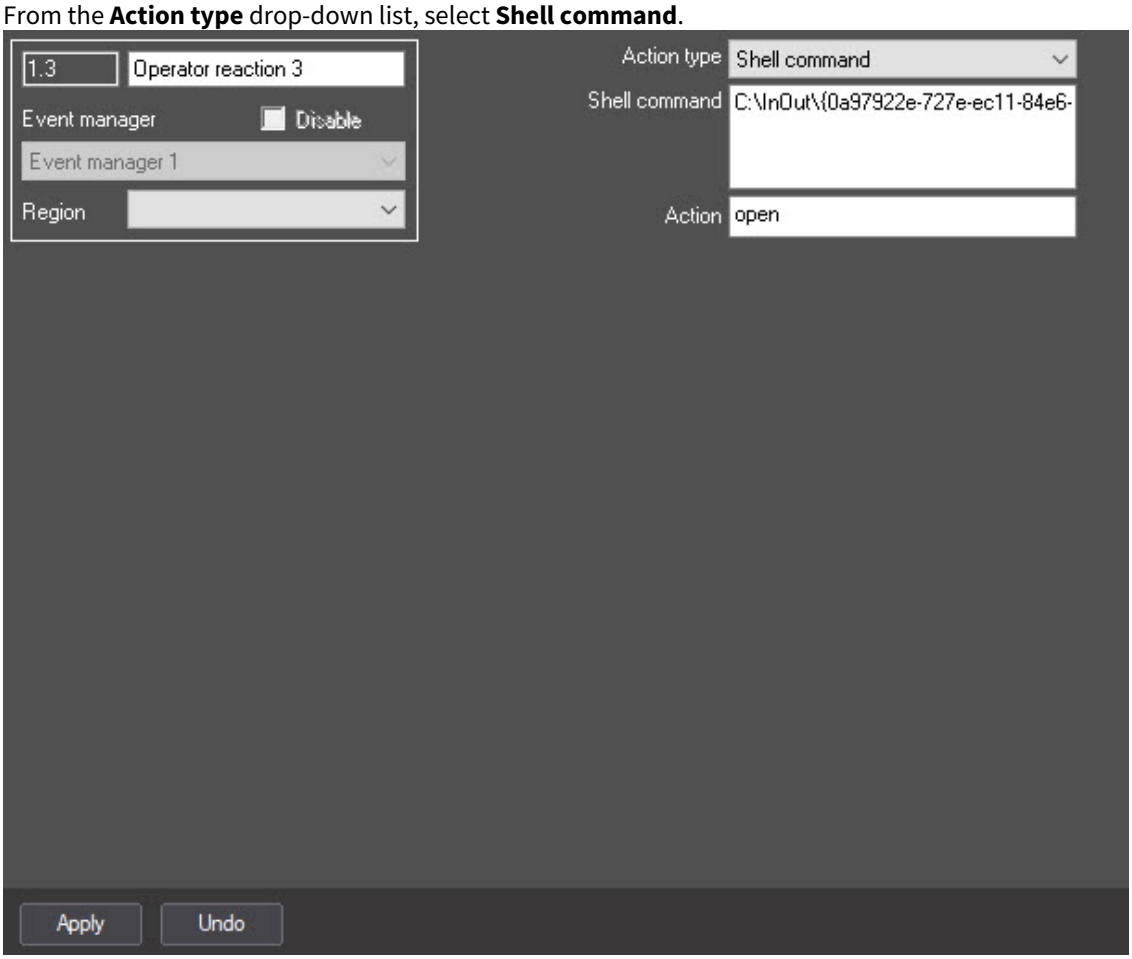


2. Create the **Operator reaction** object on the basis of the **Event manager** object.



3. Go to the settings panel of the **Operator reaction** object.

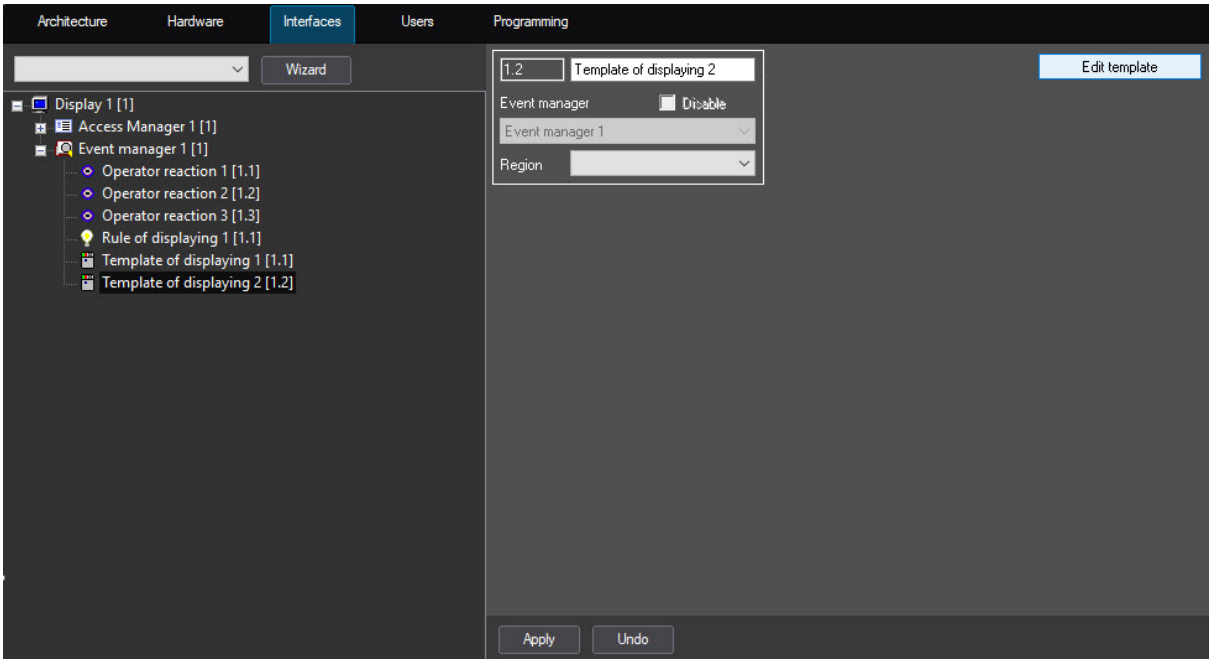
a. From the **Action type** drop-down list, select **Shell command**.



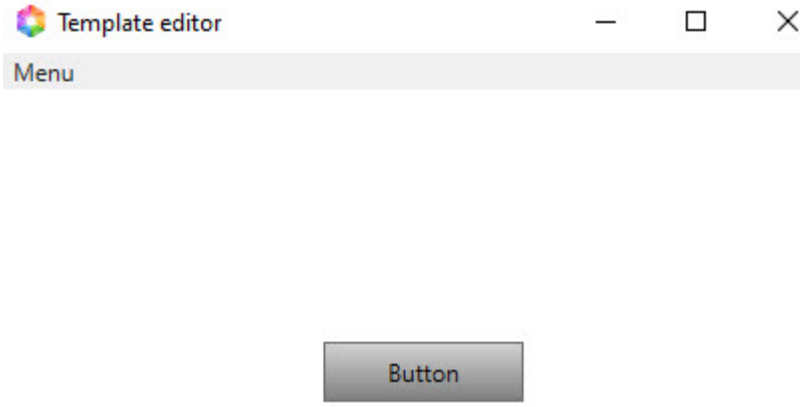
b. In the **Shell command** fieled, enter the path to the user's folder (see Pre-configuring a folder with user documents).
   If you want to open a file quickly, you must add the file name and its extension to the folder path:
   - for network folder: \\path_to_network_folder\{person_guid}\file_name_with_extension, for example, \\Jane\Shara\{dcf73f47-ed57-ec11-be7c-38d547783445}\passport.pdf
   - for local folder: path_to_local_folder\{person_guid}\file_name_with_extension, for example, D:\InOut\{dcf73f47-ed57-ec11-be7c-38d547783445}\passport.pdf

c. In the **Action** field, enter **open**.
d. Click the **Apply** button.

4. Create the **Template of displaying** object on the basis of the **Event manager** object (see Configuring templates of displaying).

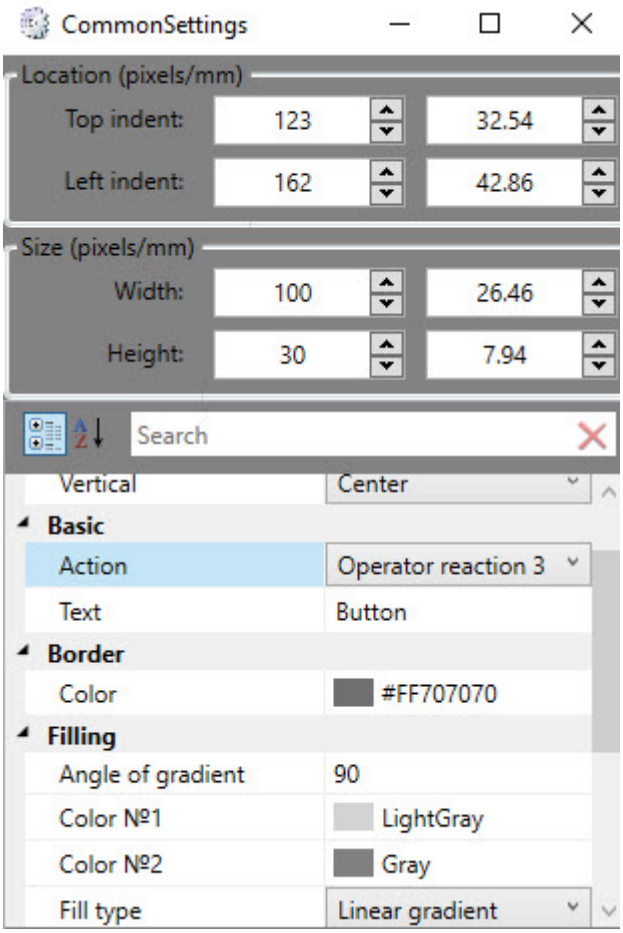


5. On the settings panel of the **Template of displaying** object, click the **Edit template** button. The **Template editor** window opens.
6. In the **Template editor** window, add the **Button** element (see Template Editor Utility Operation Guide).



> **Note**
>
> You can create the required number of buttons.

7. In the **Template editor** window, click the button to open the settings window.
8. In the settings window, from the **Action** drop-down list, select the **Operator reaction** object created in step 3.



9. Save the template before closing the window.
When an event is received, a template with a button is displayed. When you click the button, a folder or file opens if its name and extension were specified in the path.

> **Attention!**
>
> A folder with user documents or user file opens only for those events that contain the user ID. For other events, a folder or file doesn't open.

Configuring a quick opening of a folder with user documents or user file is complete.

6.6.4 User search in the Access Manager software module

General information about user search

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

1. By surname.
2. By number.
3. By card.
4. By card (control reader).
5. By access level.
6. General search.

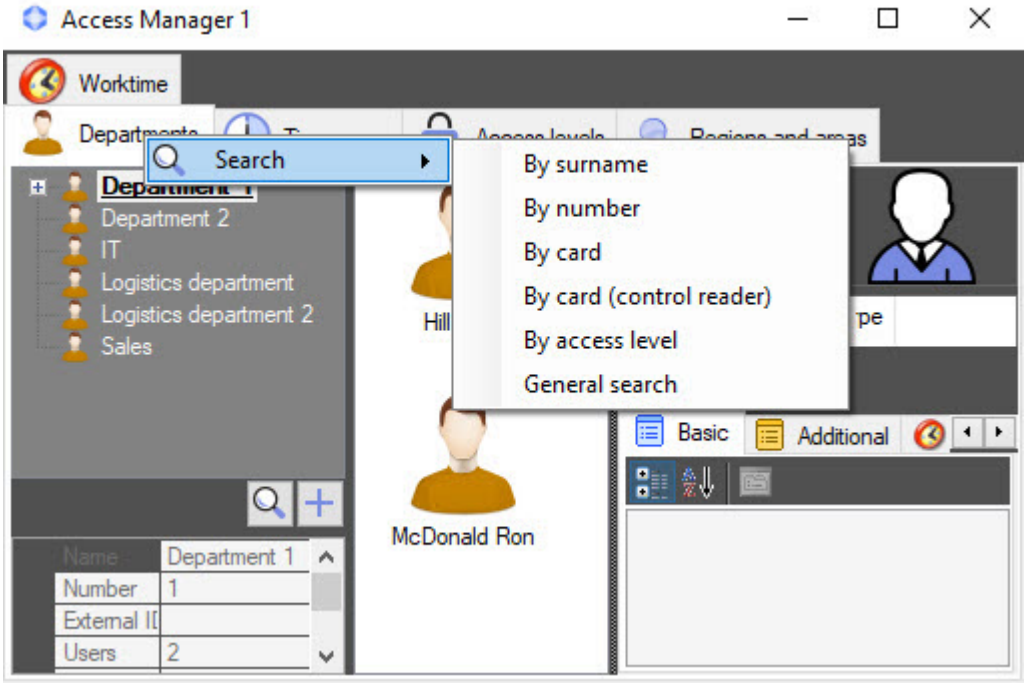
Going to user search

You can go to user search in 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 method:

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

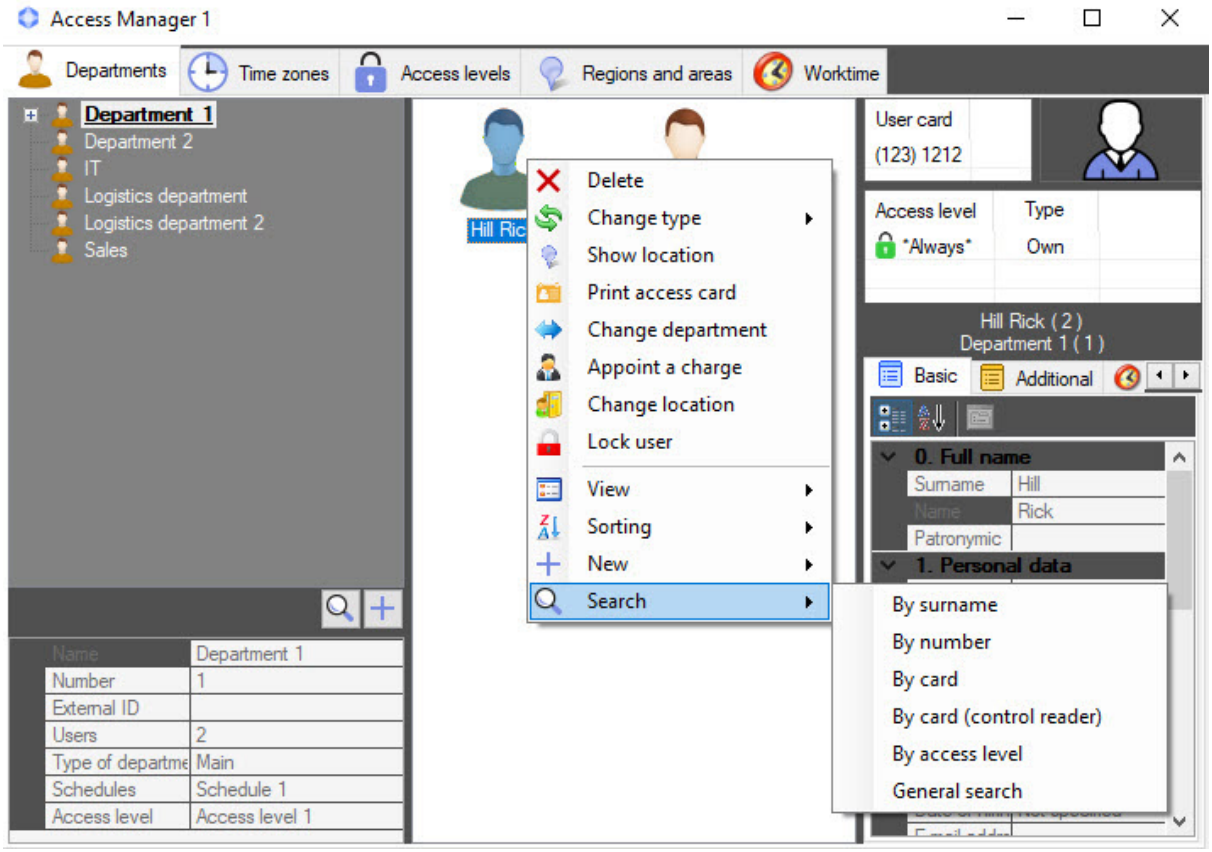


The second method:

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

> **Note**
>
> You can also go to user search using the Ctrl+F keyboard shortcut—see Keyboard shortcuts for working with interface elements. The **Search in department** tab opens, in which the search condition by the department is specified.

3. In the **Search** function menu, select the required method of search—see General information about user search.

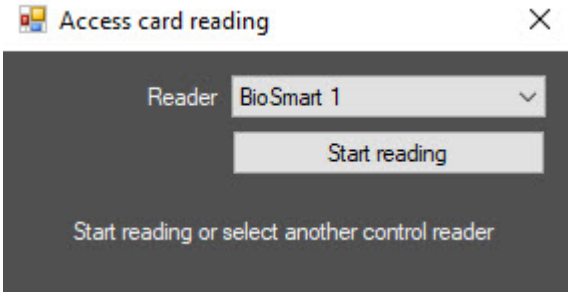


As a result, a new search tab opens (**1**). The name of the tab depends on the selected method of search. The tab contains the following interface elements:

1. List of search rules (**2**).
2. List of found users (**3**).
3. Parameters of the selected user (**4**).

4. If you search by number, surname, card or access level, the corresponding rule will be specified in the list **2**. You can add search rules to the list if it's required (see Adding a search rule).

5. If you search by card using a control reader, the **Access card reading** window opens:



   a. From the **Reader** drop-down list, select the control reader.
   b. Click the **Start reading** button.
   c. Bring the user's card to the selected reader.

Going to user search is complete.

Adding a search rule

When searching for objects in the *Access Manager* module, you can use the following logic operators:

1. Logic AND.
2. Logic OR.

Search rules are combined according to the following principle:

(Rule11 OR Rule12 OR ... OR Rule 1N) AND

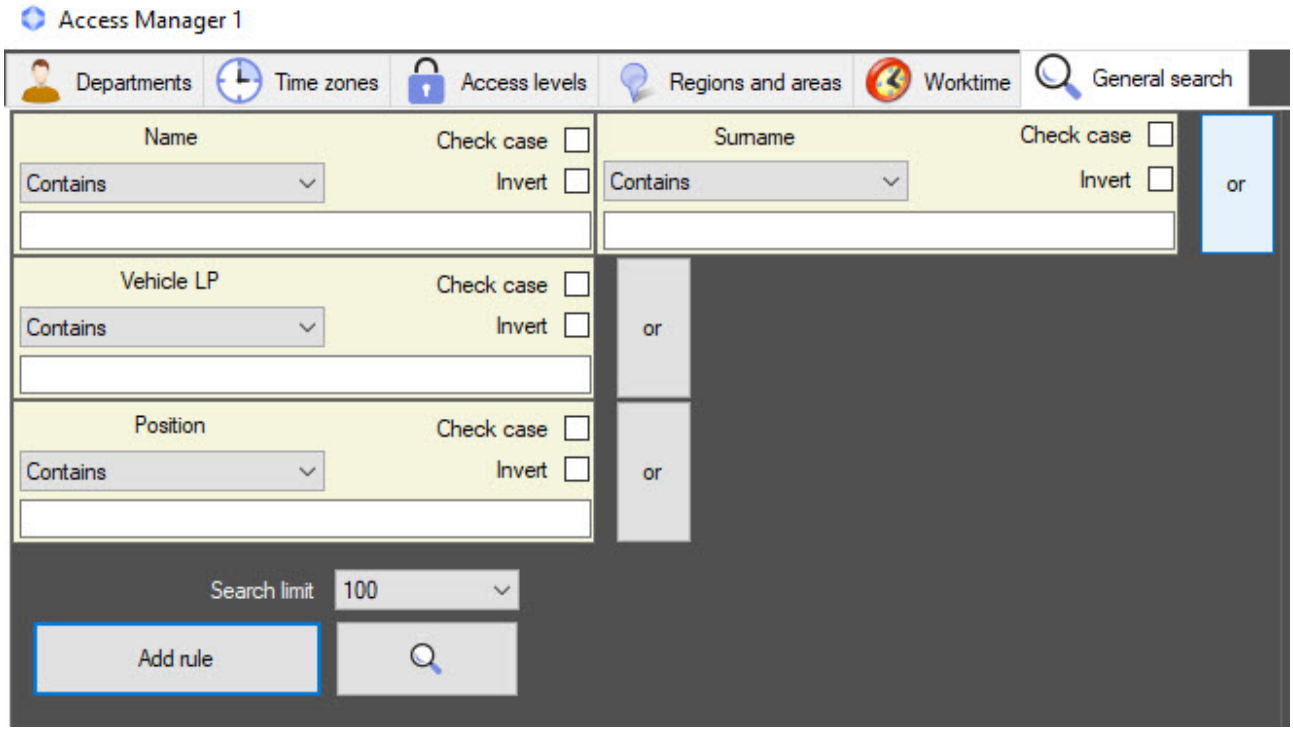
(Rule21 OR Rule22 OR ...Rule 2M) AND

...

(Rule K1 OR Rule K2 OR ... OR Rule KL)

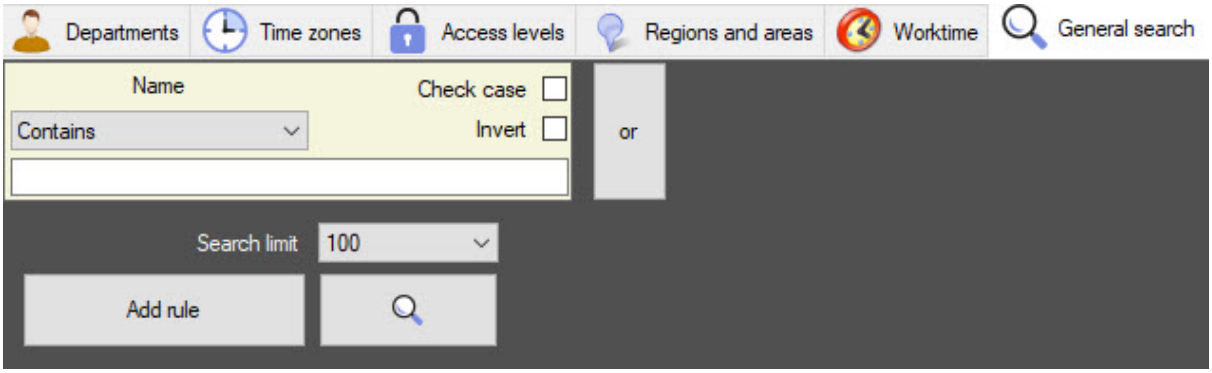
Where N, M, K, L are arbitrary integers.

In the **Access Manager** window, the search rules combined by the OR operator are displayed in one string. The search rules combined by the AND operator are displayed under each other.

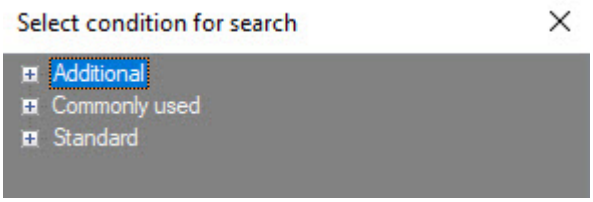


To add a search rule, do the following:

1. Go to the user search (see Going to user search).
2. Click the **Add rule** button to add the AND rule or the **or** button to add the OR rule.



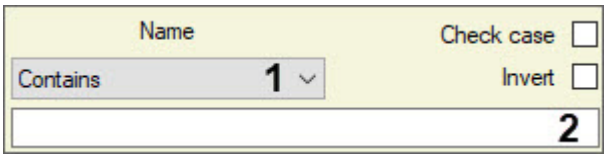
The **Select condition for search** window opens.



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

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

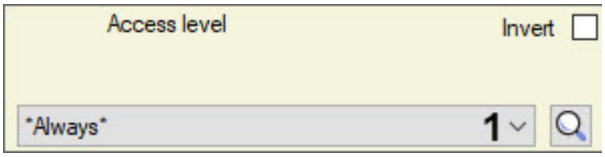
3. Select the search parameter by double-clicking its name.
   The search rule by selected field is added. Configuring the search rules differs depending on the type of the rule. The following types of search rules are available:
   a. Text field



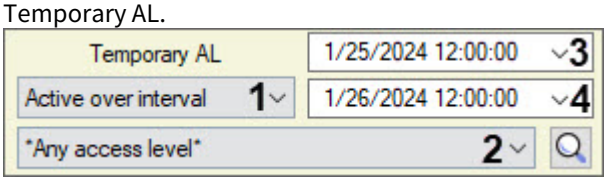
      i. From the drop-down list (**1**), select the comparison method of a field value with the specified search line.

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

      ii. Set the **Check case** checkbox if you want the search to be case-sensitive.
      iii. Set the **Invert** checkbox if you want to apply the negation of the specified search rule. if you set this checkbox, all users who don't meet the specified search condition will be found.
      iv. Enter the search line in the field (**2**).
   b. Access level.



      i. Set the **Invert** checkbox if it's required to apply the negation of the specified search rule.
      ii. Select value for search from the drop-down list (**1**) or click the button. Working with the search window is described in Working with the Search access level window.
   c. Temporary AL.

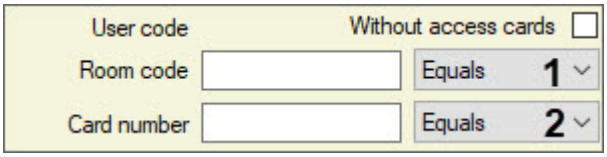


      i. Select the search criteria from the drop-down list (**1**):
         1. **Activation date**—the start date of the temporary access level.

2. **Active on this day**—the date between the start and end of the temporary access level.
3. **Active over interval**—the interval that falls entirely between the start and end of the temporary access level. If the interval includes a day when the temporary access level isn't valid, the search will have no results.
4. **Active in this interval**—the interval that falls at least partially between the start and end of the temporary access level.

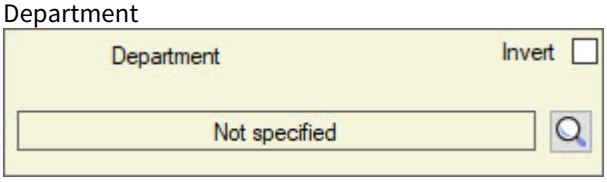
ii. Select the search criteria from the drop-down list (**2**). You can also click the button to search for the required temporary access level. Working with the search window is described in Working with the Search access level window.
iii. Use the calendar to set the search date (**3**).
iv. If you select **Active in this interval** or **Active over interval**, set the end of the interval for the search (**4**).

d. Access card:



i. Set the **Without access card** checkbox if user doesn't have an access card. As a result, other fields of the **User code** condition become unavailable for editing.
ii. In the **Room code** field, enter the required room code.
iii. From the drop-down list (**1**), select the comparison method of a field value with the specified search line similar to step 3ai.
iv. In the **Card number** field, enter the required number of the access card.
v. From the drop-down list (**2**), select the comparison method of a field value with the specified search line similar to step 3ai.

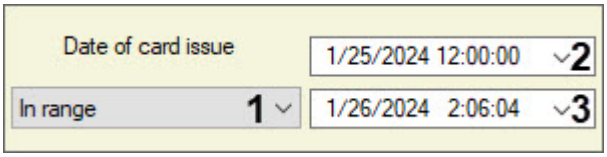
e. Department



i. Set the **Invert** checkbox if it's required to apply the negation of the specified search rule.
ii. To search for required department, click the button. Working with the search window is described in Working with the Search for department window.

> **Note**
>
> You can search for department only if you performed user search by pressing the Ctrl+F keys.

f. Time values:



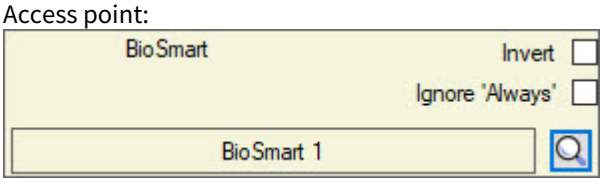
i. Select the comparison method of the specified value for search with a field value (**1**):

Comparison method	Description

Equals	Search for all users for who the value of the selected field is fully coincides with the specified date
Not equals	Search for all users for who the value of the selected field is not coincide with the specified date
Higher	Search for all users for who the value of the selected field is higher than the specified date
Lower	Search for all users for who the value of the selected field is lower than the specified date
In range	Search for all users for who the value of the selected field is in the specified range of dates
Out of range	Search for all users for who the value of the selected field is out of the specified range of dates

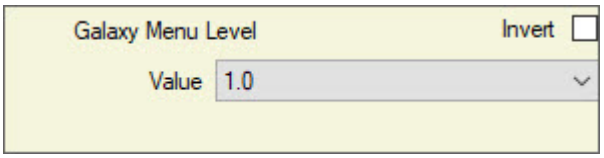
ii. Set the date for search using the calendar (**2**). If you use the last two comparison methods from the table, the selected value sets the start of search interval.
iii. If you use the last two comparison methods from the table, specify the end of search interval (**3**).

g. Access point:



i. Set the **Invert** checkbox if it's required to apply the negation of the specified search rule.
ii. Set the **Ignore 'Always'** checkbox to select users whose access level differs from **Always**.
iii. Click the button to select the search value. Working with the access point search window is described in Working with the Search access level window.

h. Additional fields:



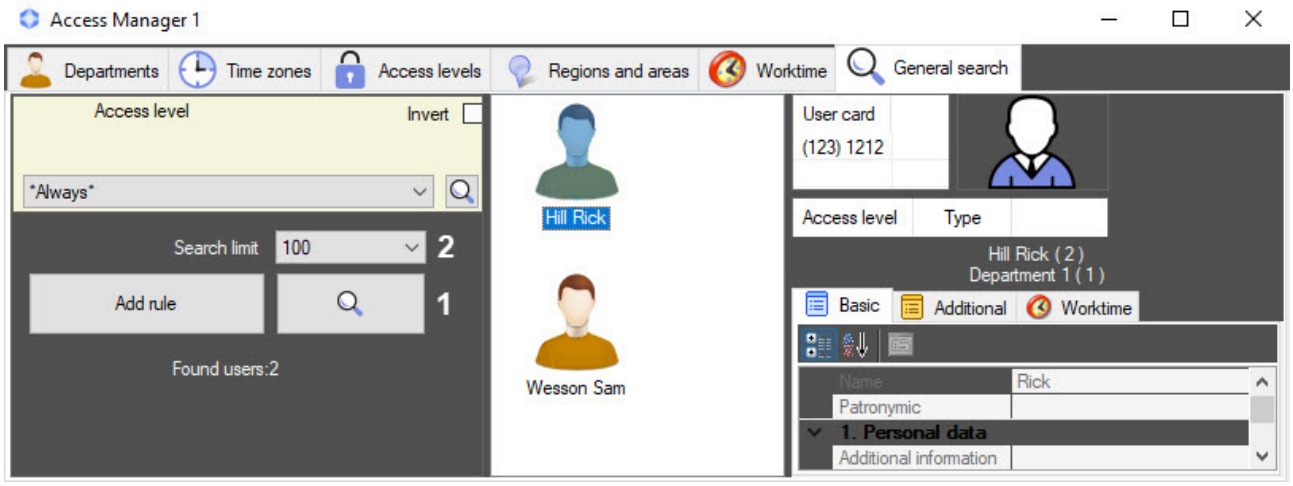
i. Set the **Invert** checkbox if it's required to apply the negation of the specified search rule.
ii. From the **Value** drop-down list, select the search value.

Adding a search rule is completed.

Starting user search

After you specify all required search rules (see Adding a search rule), click the button to start the search (**1**).

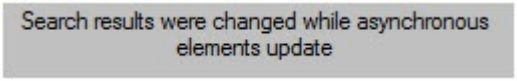
Found users are displayed in the list.



You can limit the number of users in the search result list. To change the limit, select the required maximum number of users displayed from the **Search limit** drop-down list (**2**): **100** (default), **250**, **500**, **1000**, **5000**. If you don't want to limit the number of users, select **Do not limit**.

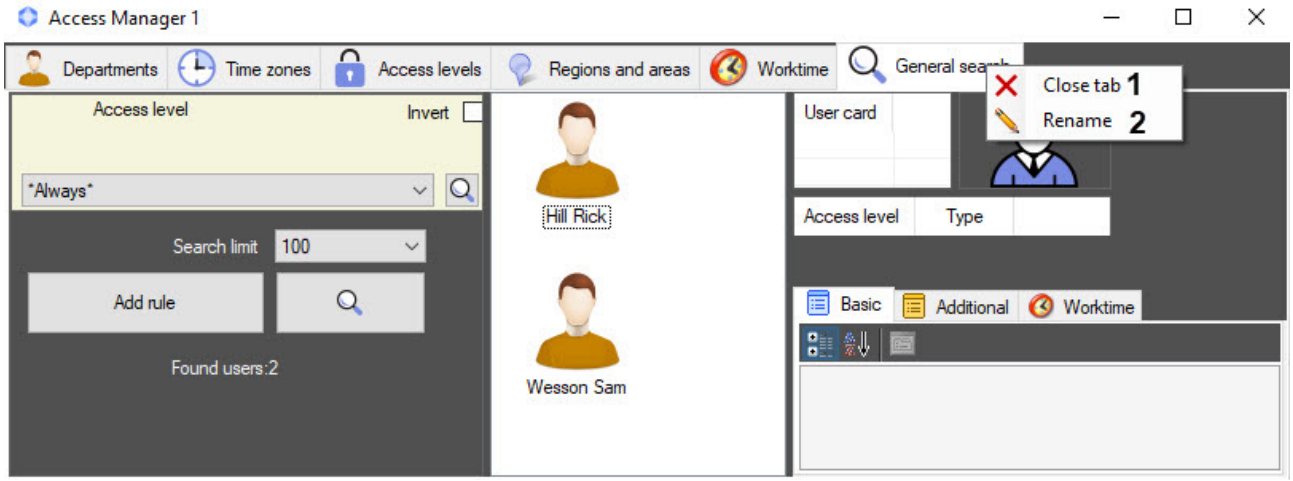
The list of found users can be changed dynamically.

Example. You searched for a user by surname, and several users were found. If a surname of one of the found users is changed so that it no longer matches the filter, the user is removed from the search results. The opposite is also true: if a new user with a surname that matches the search rule appears, they are automatically added to the search result list. In this case, the search result line displays the message about dynamic data change.



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

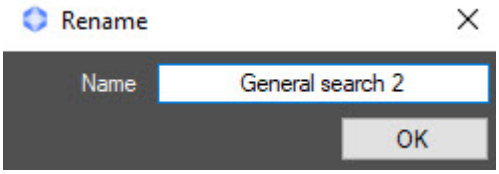
To close the tab after search completion, right-click the tab name and select the **Close tab** (**1**) item in the function menu.



You can rename the search tab. To rename it, do the following:

1. Right-click the tab name and select **Rename** (**2**) from the menu.
2. The **Rename** window opens. In the **Name** field, enter a new name for the search tab.

3. To apply the changes, click **OK**.



> **Note**
>
> The search tab with all search rules and a name is saved for the current user of *Axxon PSIM* even after you restart the *Access Manager* module.

User search is complete.

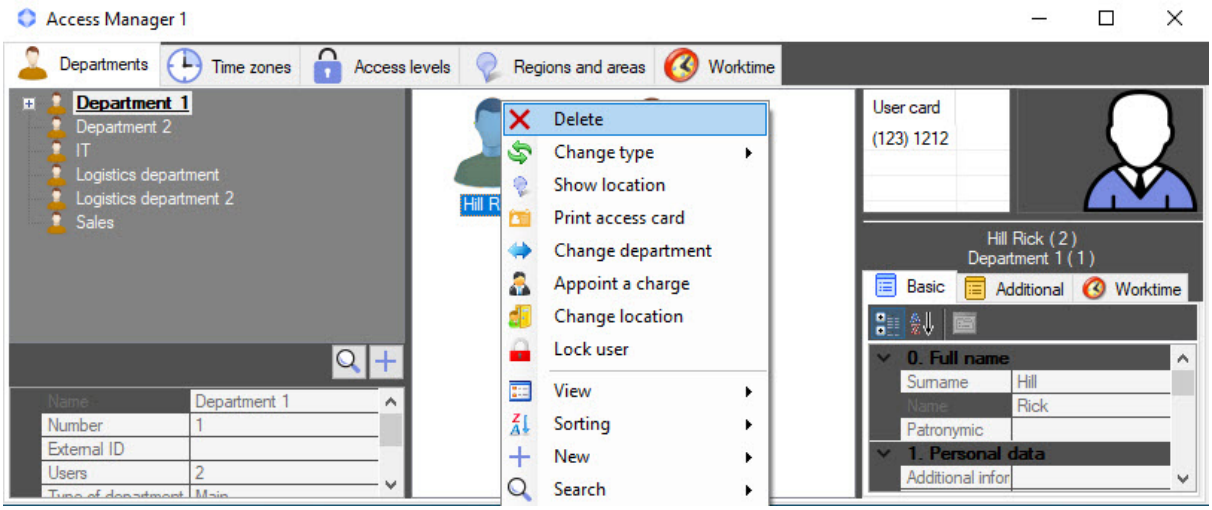
6.6.5 Deleting a user in the Access Manager software module

To delete a user, do the following:

1. Go to viewing a list of users (see Viewing a list of users).
2. Right-click the user you want to delete.

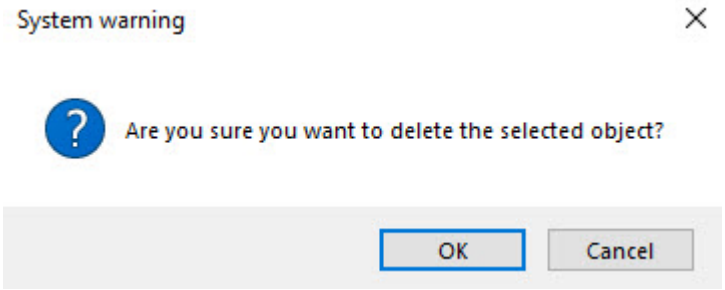
> **Note**
>
> You can also select several users by selecting them with the mouse or by using keyboard shortcuts (see Keyboard shortcuts for working with object lists).

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



> **Note**
>
> Rights for deleting a user can be limited when you configure the *Access Manager* module. In this case, the message about the lack of corresponding rights is displayed. See also Configuring the rights to manage objects in Access Manager.

4. The confirmation message is displayed. To confirm the deletion of the selected user, click the **OK** button. To cancel the action, click the **Cancel** button.



Deleting a user is complete.

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).

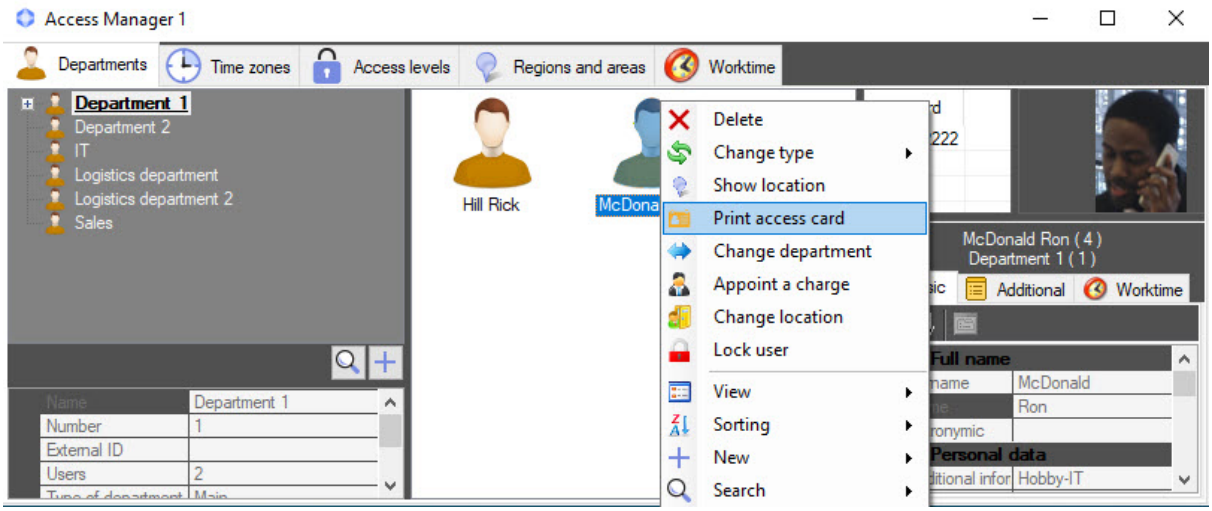
You can print user access cards in the *Access Manager* software module.

To print a user access card, do the following:

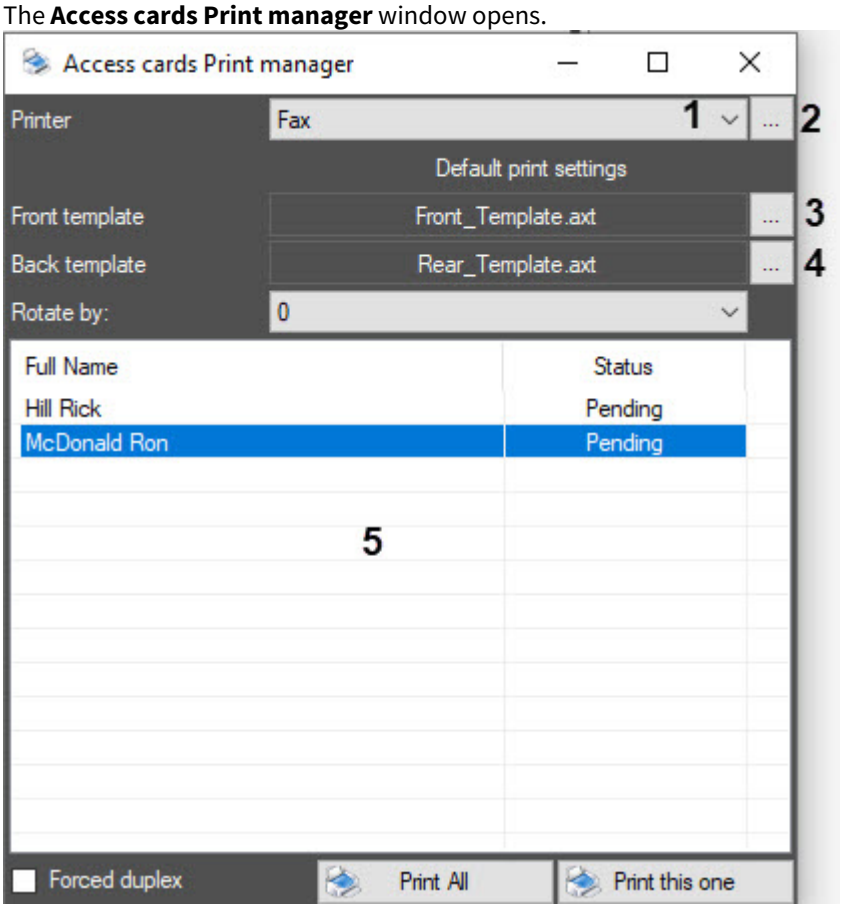
1. Go to viewing a list of users (see Viewing a list of users).
2. Right-click the name of the required user.

> **Note**
>
> You can also select several users 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 function menu.



4. The **Access cards Print manager** window opens.



5. From the **Printer** drop-down list (**1**), select the printer that is used for printing.
6. Click the (**2**) button if it is necessary to change the print settings for the selected printer.
7. Click the (**3**) button to select the front template of the access card.
8. For duplex printing, click the (**4**) button to select the back template.
9. If your printer supports duplex printing but doesn't allow you to set it up at step 5, set the **Forced duplex** checkbox.

> **Note**
>
> You can create templates using the *Template Editor* utility—see the Template Editor Utility Operation Guide.
> To create a template file that can be uploaded to *Access Manager*, you must manually run the *EditorWpf.exe* utility from the *Modules* folder in the *Axxon PSIM* installation directory.
> If the template has a barcode that isn't displayed in the preview window, make sure that you selected the correct format of a code—see Barcode object properties.

10. From the **Rotate by** drop-down list, select the rotation angle to rotate the template on the printed list by **0**, **90**, **180**, or **270** degrees.

> **Note**
>
> You can change the rotation angle in the Windows OS registry using the **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).

11. The list (**5**) displays all users for whom the access cards will be printed, as well as information on the status of printing.
12. To preview the access card template, double-click the required user. The **Print Preview** window opens.
13. To print access cards for all users, click **Print All**. The *Access Manager* module automatically creates a print queue and sends access cards to the selected printer.
14. To print an access card for only one user, select the required user from the list (**5**) and click the **Print this one** button. The *Access Manager* module automatically creates a print queue and sends the card to the selected printer.

> **Note**
>
> If a template is sent for printing, the *Access Manager* module generates the "Print access card" event. A user's full name, their ID, the name of the computer from which the access card was printed, and the person who initiated printing (operator working with the *Access Manager* module) are specified in the event parameters.
> You can print templates from several printers at the same time using a script described in Appendix 7. Script for printing templates.

Printing a user access card is complete.

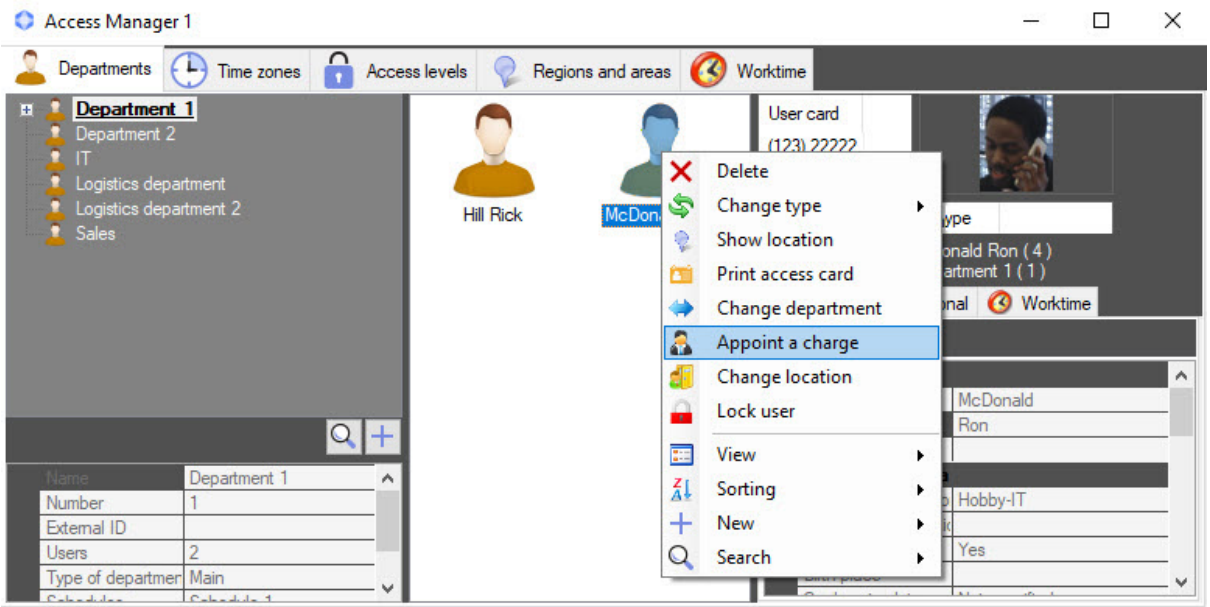
6.6.7 Appointing a user in charge of a region

You can appoint a user in charge of a region in the *Access Manager* software module.

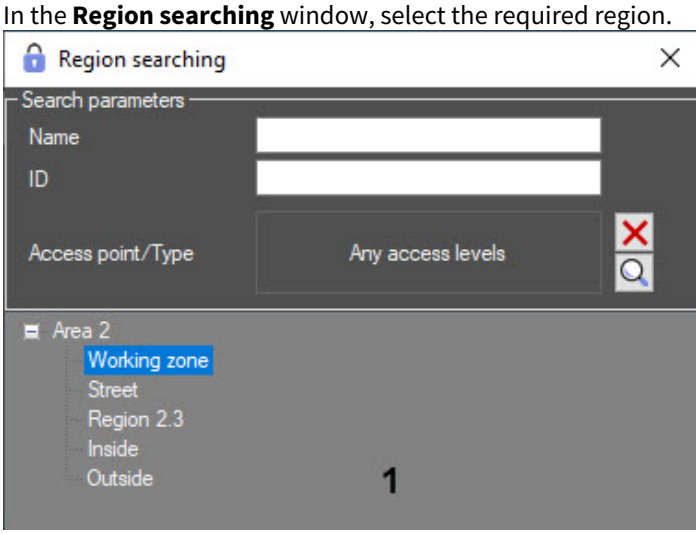
To appoint a charge, do the following:

1. Go to viewing a list of users (see Viewing a list of users).
2. Right-click the name of the required user and select the **Appoint a charge** item in the function menu.

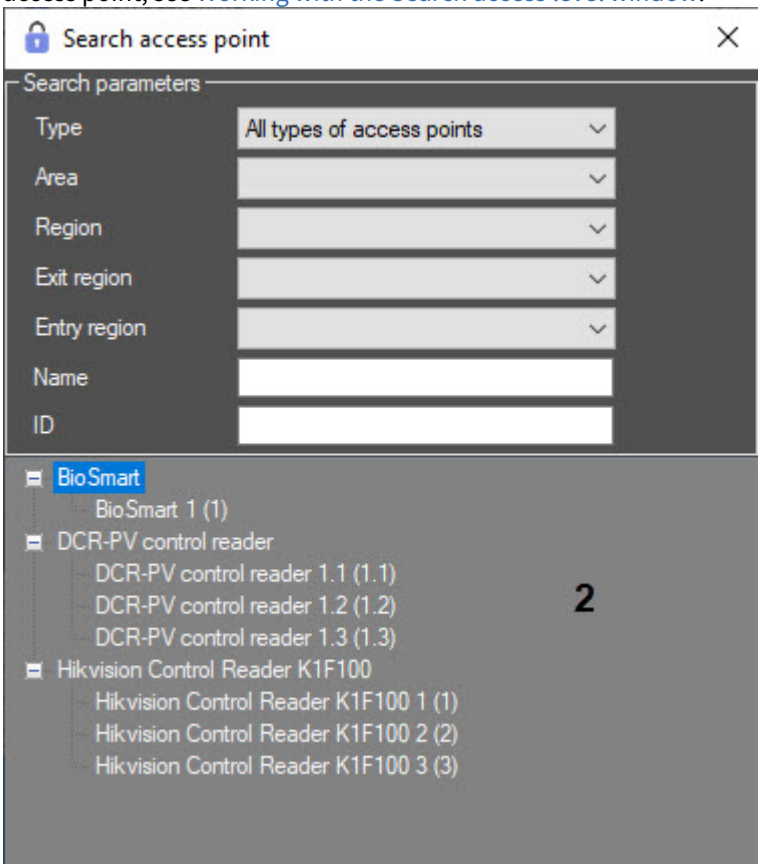
> **Note**
>
> You can also select several users: for example, by selecting them with the mouse or by using keyboard shortcuts (see Keyboard shortcuts for working with interface elements).



3. In the **Region searching** window, select the required region.



4. If necessary, specify the name of the required region in the **Name** field.
5. If necessary, enter the identifier of the required region in the **ID** field.
6. If necessary, specify a list of access points that must be included in the required region, as follows:
   a. Click the  button. The **Search access point** window opens. For more information on searching an access point, see Working with the Search access level window.



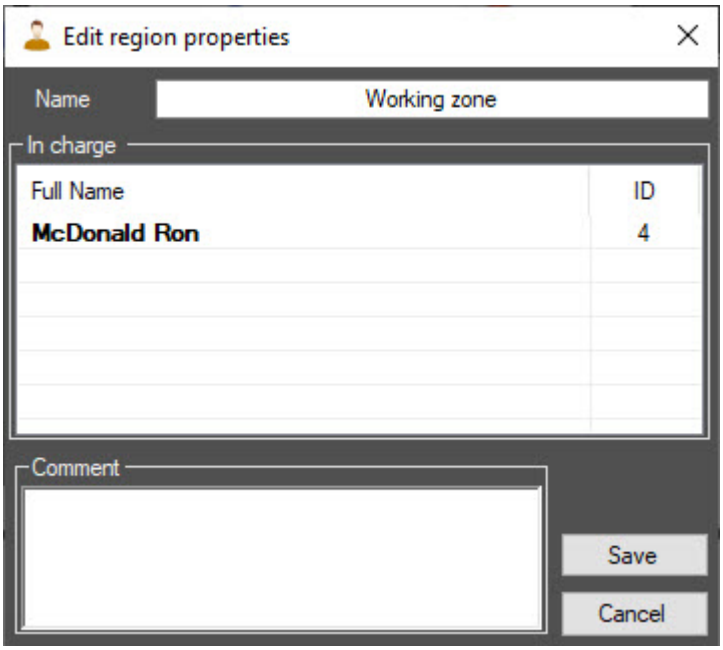
   As a result, a list of search results that meets the specified search parameters is displayed (**2**).
   b. Double-click the necessary access point.

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

Region search results will be displayed in the list (**1**) of the **Region searching** window. The search is case-insensitive.

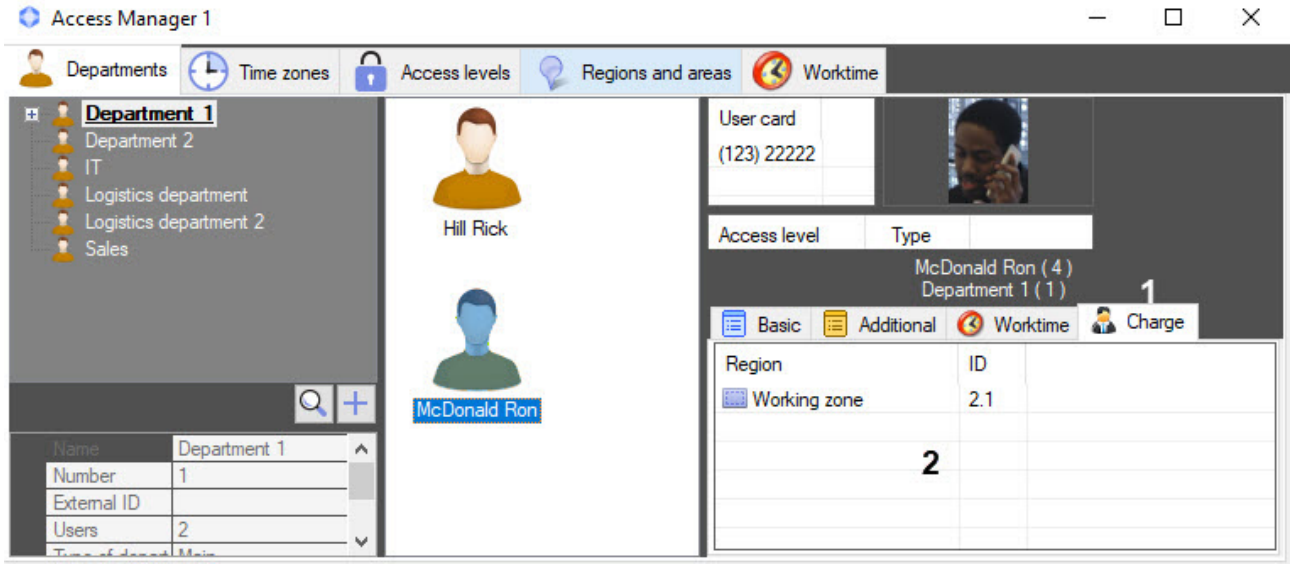
7. Double-click the necessary region. As a result, you go to editing the region properties (see Creating and editing regions).

> **Note**
>
> The user that is currently being appointed in charge is highlighted in bold.



8. Click **Save** to appoint the selected user in charge of the region.

The user who is in charge of the region has the **Charge** tab (**1**). On this tab, a list of regions of which the corresponding user is in charge is displayed (**2**).

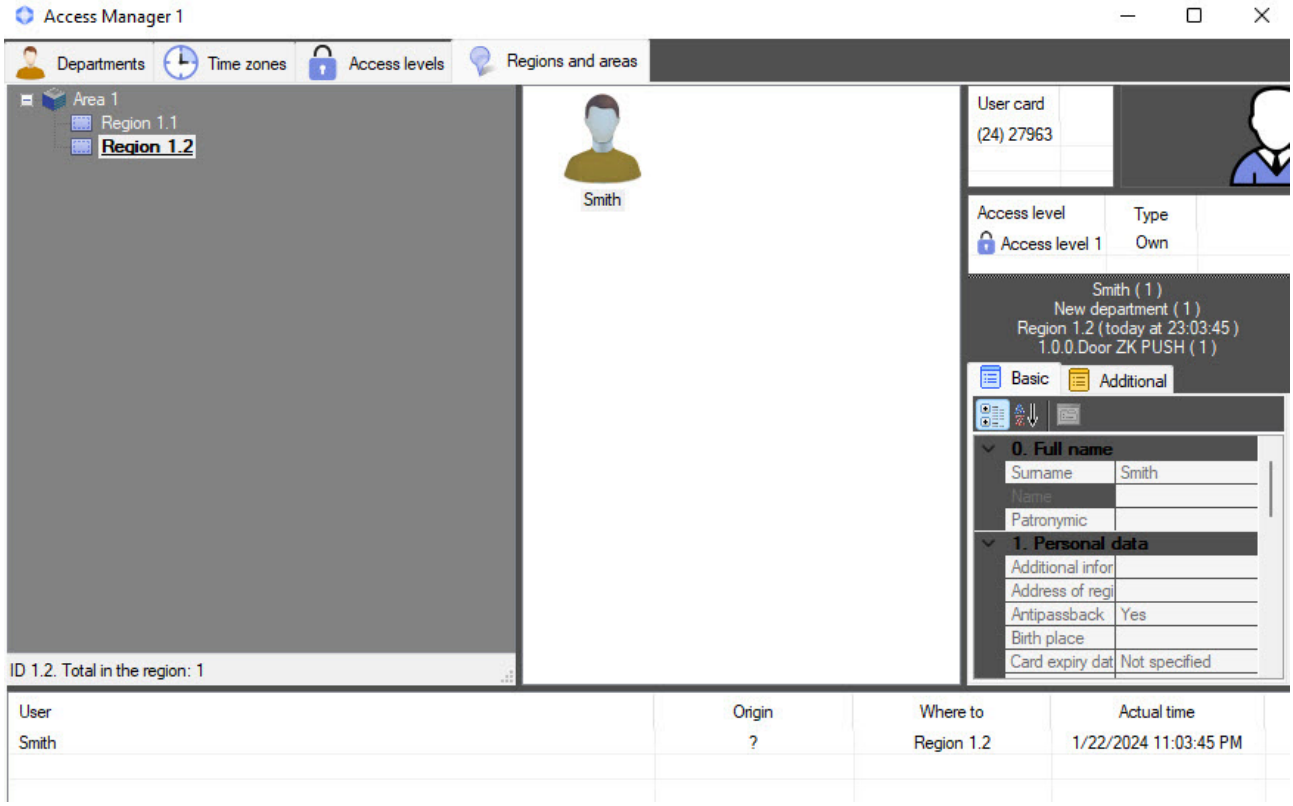


Appointing a user in charge of the region is now complete.

6.7 Working with 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 Event Viewer).
2. Find out the region where the user is currently located (see Finding out the region where the user is located).
3. View the list of users in the specified region (see Viewing the list of users in the region).
4. Switch over to the specified region on the *Axxon PSIM Map* (see Viewing region on the map).

When you switch between interfaces (for example, from the *Map* to the *Access Manager*, or from the *Event Viewer* to the *Access Manager*, and back), an interface object created on the basis of the same **Display** object as the source interface is selected for transition.

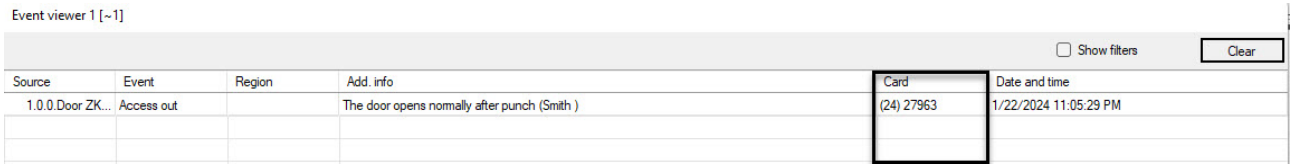
Configuration of the **Map**, **Event Viewer**, **Display, Area, Region** objects is described in the *Axxon PSIM software. Administrator's Guide*. Operation of these interface objects is described in the *Axxon PSIM software. Operator's Guide.* The most recent versions of these documents are available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

You can also create, edit, and delete the **Area** and **Region** objects in the **Access Manager** window (see Creating, editing and deleting Area and Region objects).

6.7.2 Displaying card number for access events in the Event viewer

Facility code and user card number with which an access event is associated are displayed in the **Card** column of the **Event viewer** window.

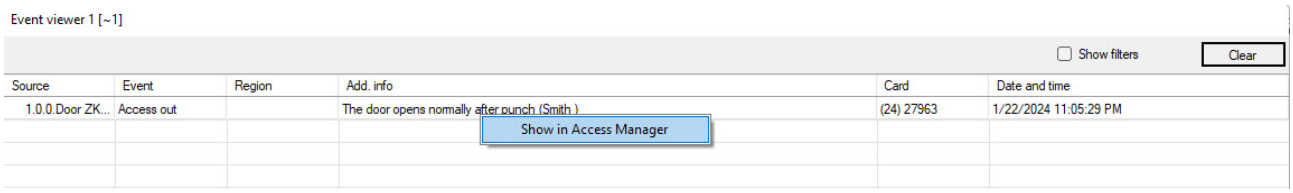
> **Note**
>
> You can disable the display of this column when configuring the **Event viewer** object (see Event viewer parameters).



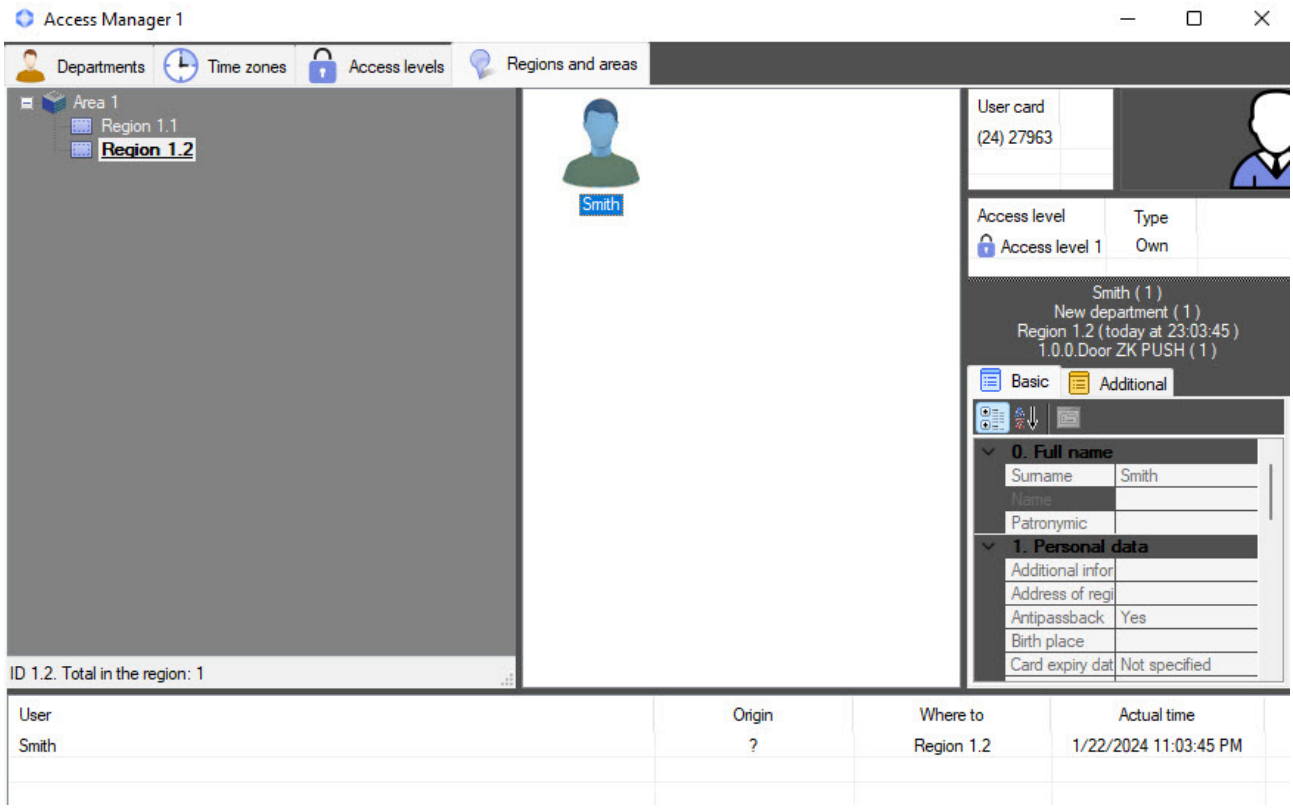
6.7.3 Viewing user profile by access events in the Event viewer

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

To view a user profile in the *Access Manager*, right-click the corresponding event in the **Event viewer** window and select the **Show in Access Manager** item.



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



Note

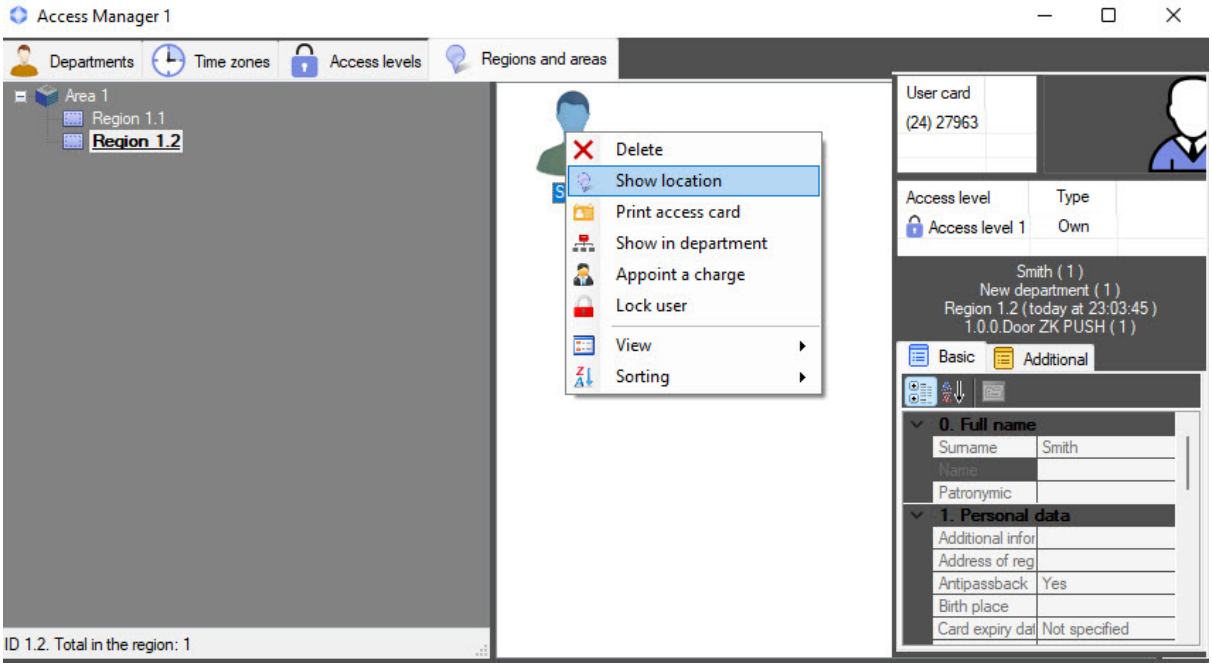
You can also find out the user's current location (see Finding out the region where the user is located).

6.7.4 Finding out the region where the user is located

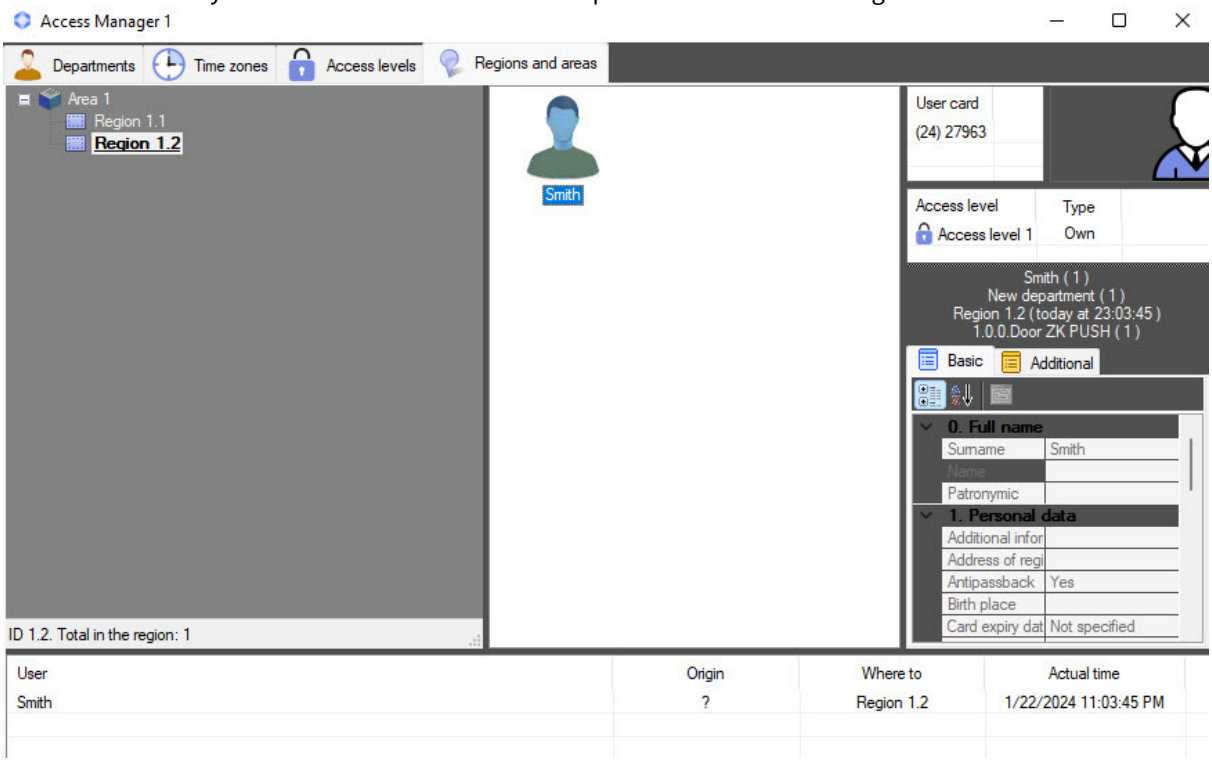
To find out the user's current location, do the following:

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

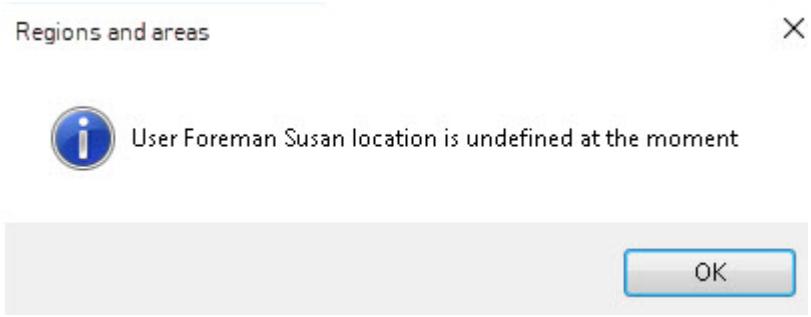
2. Right-click the user and select the **Show location** item.



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



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

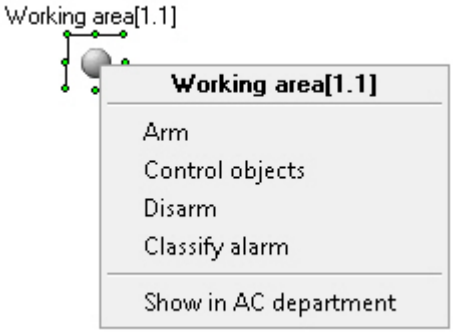


Finding out the user's current location is complete.

6.7.5 Viewing the list of users in the region

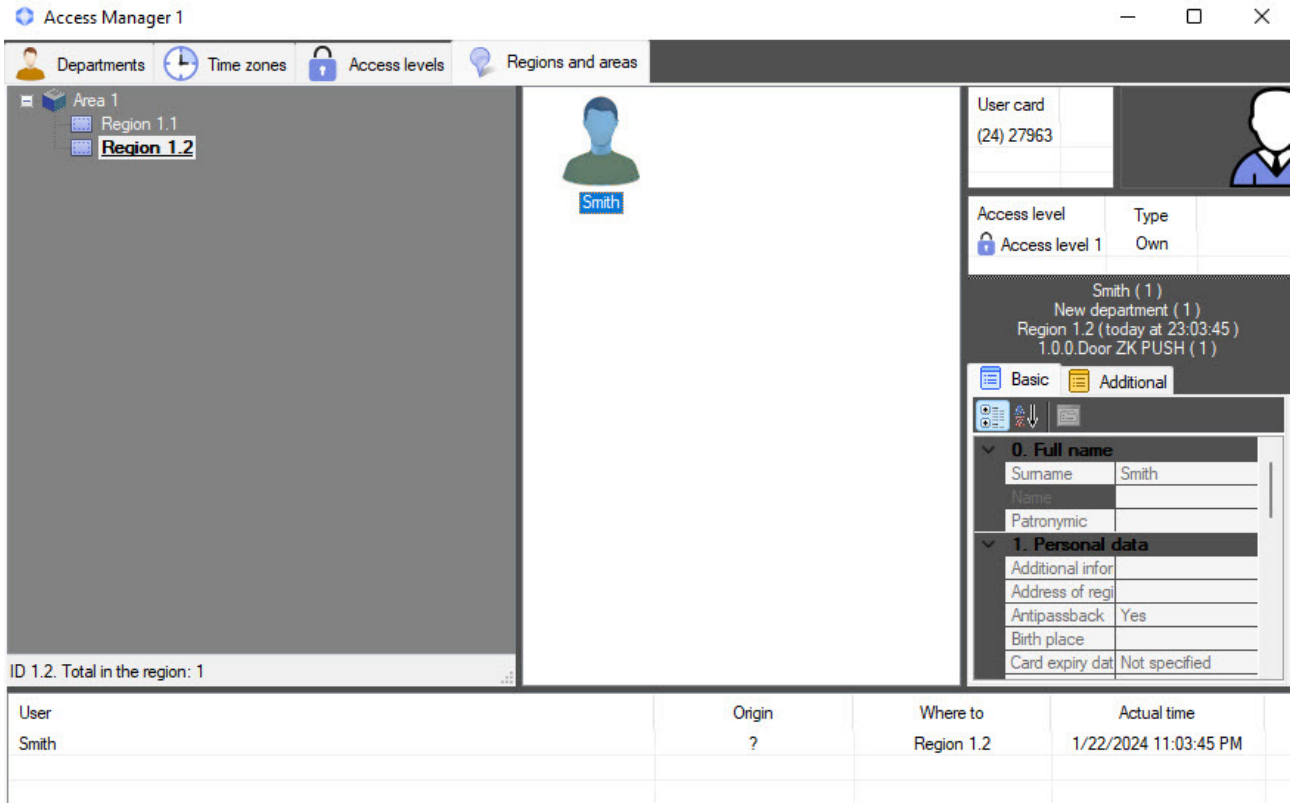
You can view users in the region in one of the following ways:

1. From the *ACFA PSIM* Map, if the region is added to the Map. For that, right-click the region and select the **Show in AC department** item.



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

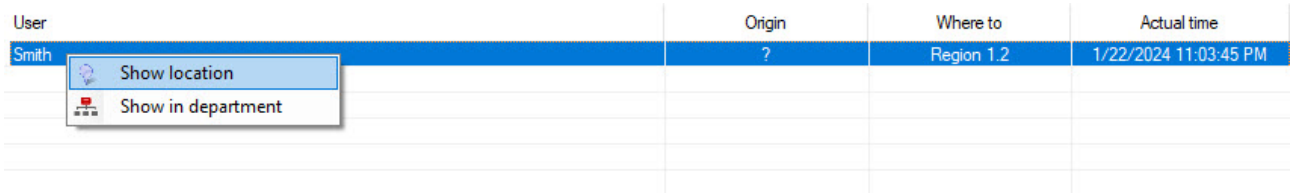
As a result, the list of users in the selected region is displayed. The information panel in the lower part of the regions and areas hierarchy displays the identifier of the selected region or area and the number of users that are currently located in this region or area.



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

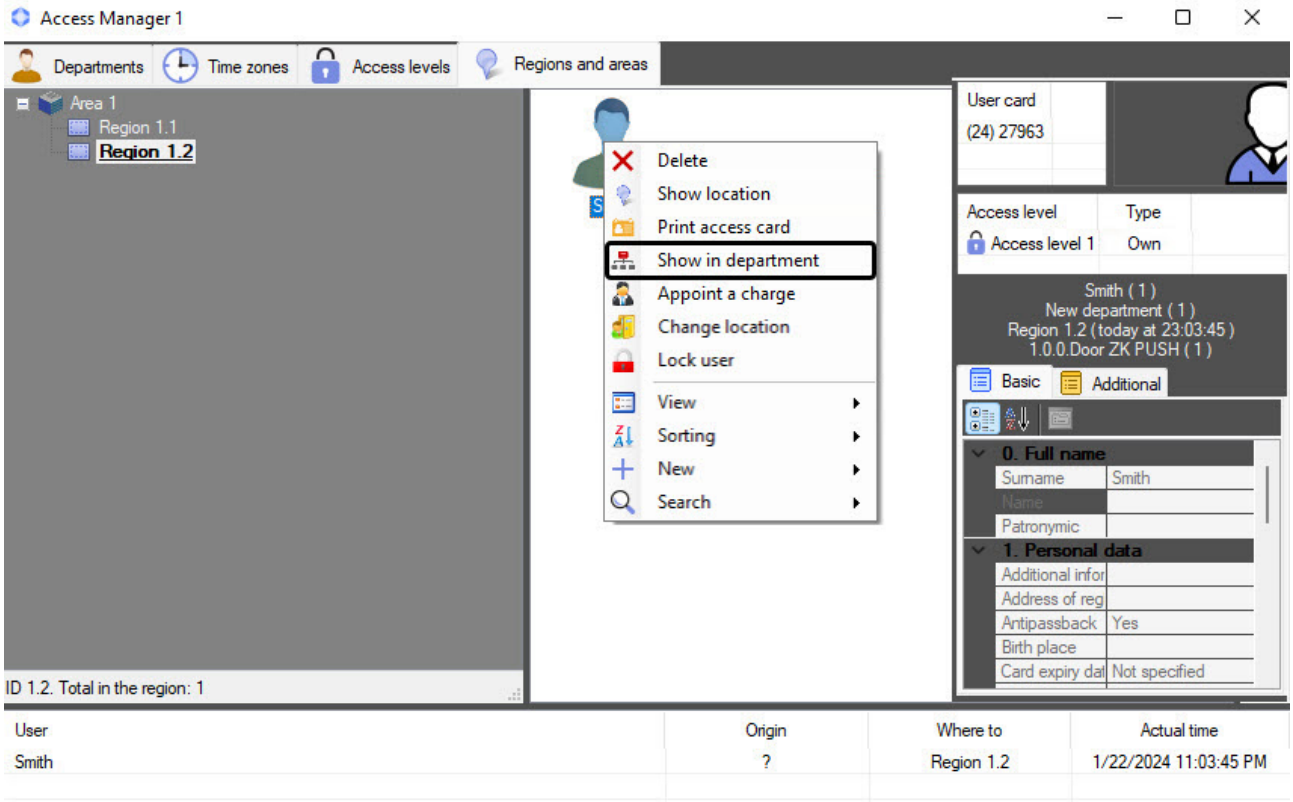
> **Note.**
>
> This data on access is given for information only, it is not recorded to a separate database.

To view the user who accessed in the current region, on the **Regions and areas** tab, right-click the required event and select the **Show location** item. To view the user in the department on the **Departments** tab, select the **Show in department** item.



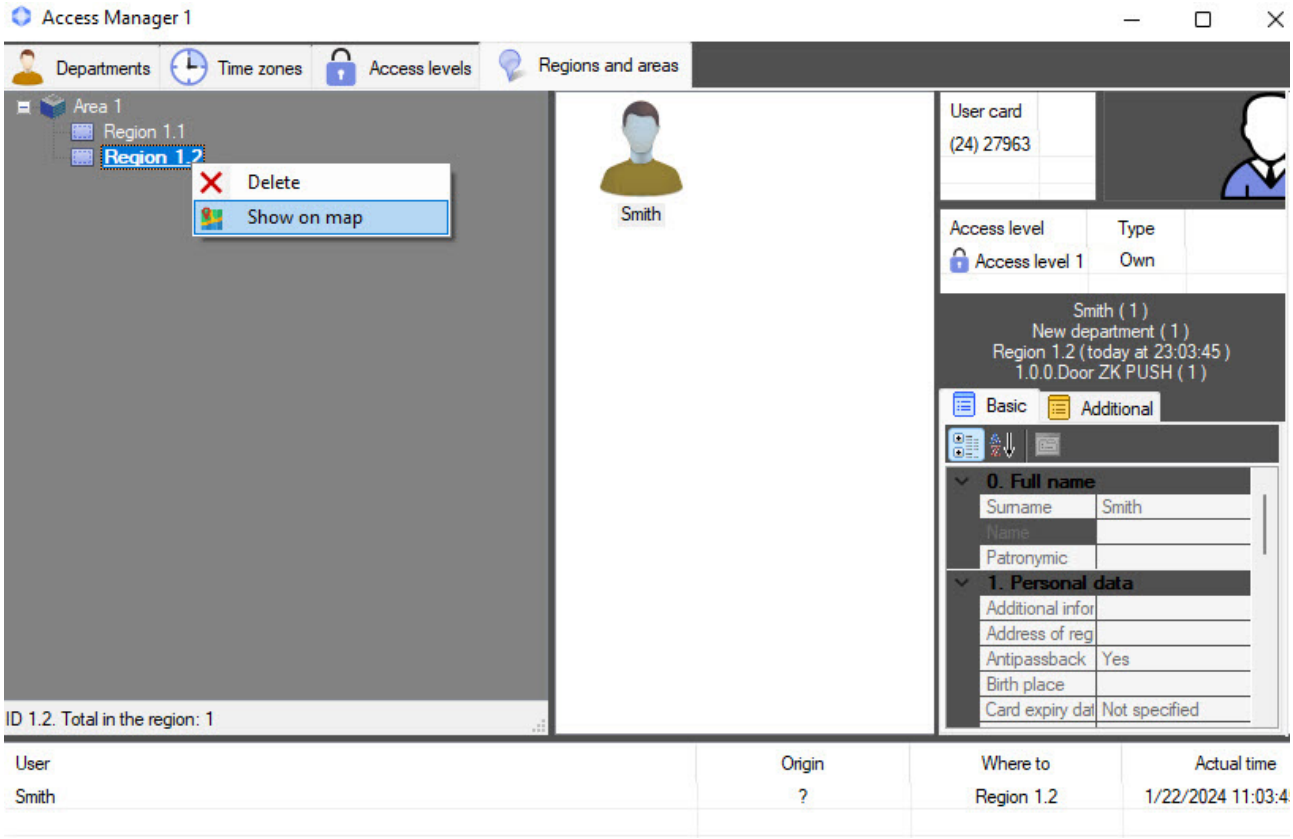
On the **Regions and areas** tab, the same actions with a user as in the **Departments** tab are available (see Working with users in the Access Manager software module).

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



6.7.6 Viewing region on the map

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



As a result, the region is selected in the map window, and the region icon blinks several times.

6.7.7 Creating, editing and deleting Area and Region objects

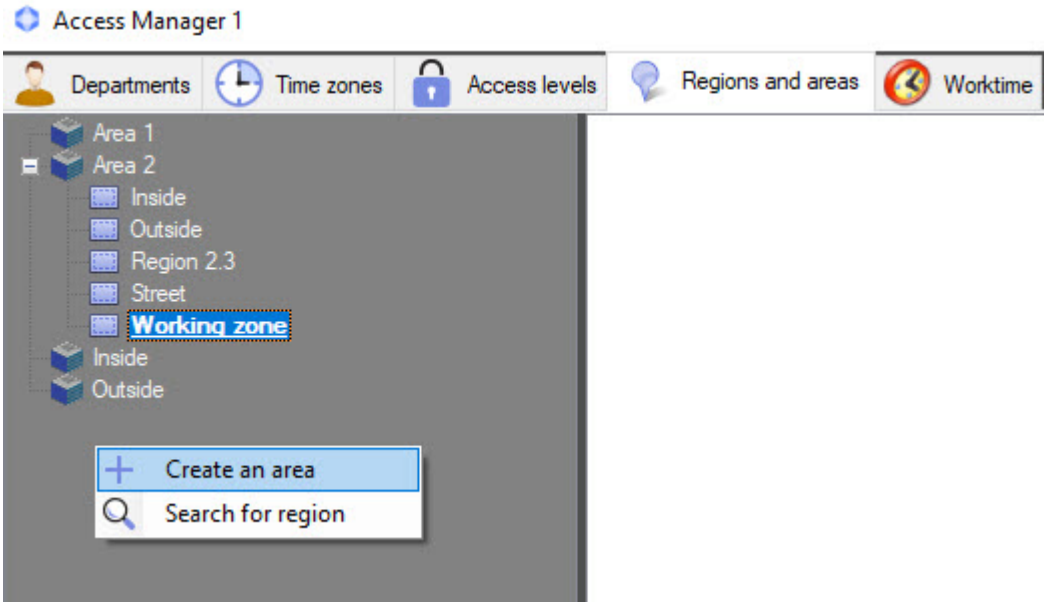
Note.

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

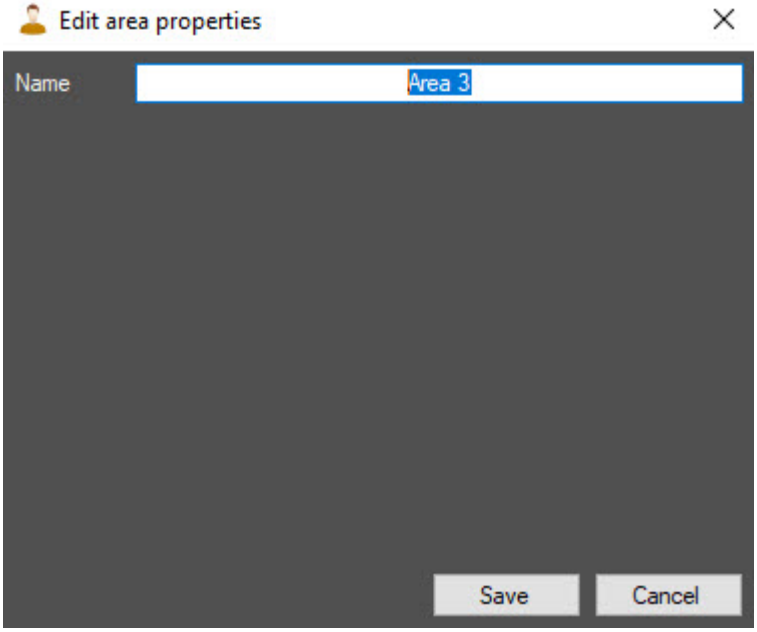
Creating areas

To create an area, do the following:

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



2. Right-click in the regions tree in the area free from any objects.
3. In the menu, select the **Create an area** item.
4. The **Edit area properties** window opens.



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

> **Note**
>
> Name must be unique. If an area with this name has already been created in the system, then when saving, a corresponding message is displayed and the area isn't saved. Also, the name must not contain the following characters: < | >.

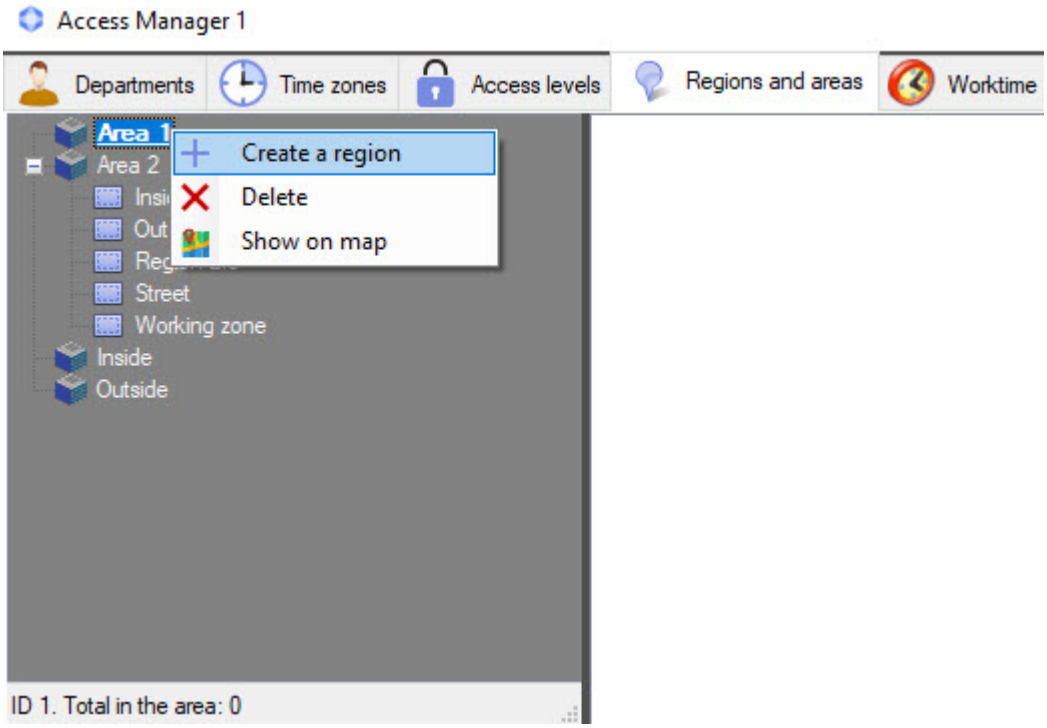
6. Click the **Save** button.

The area is created.

Creating and editing regions

To create or edit a region, do the following:

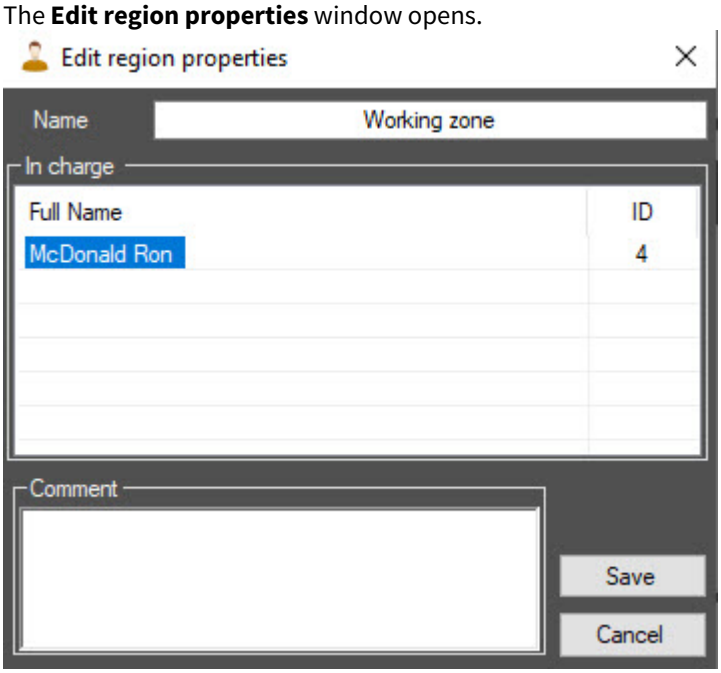
1. Go to the **Regions and areas** tab.



2. Right-click the area on the basis of which you want to create a region.
3. In the menu, select the **Create a region** item.

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

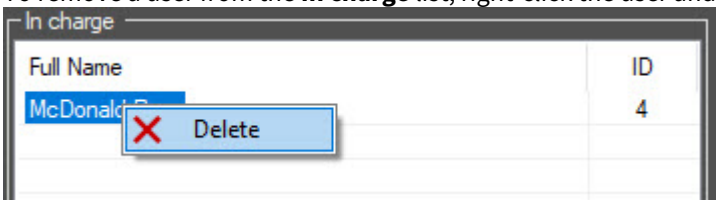
The **Edit region properties** window opens.



4. In the **Name** field, enter the region name.

> **Note**
>
> Name must be unique. If a region with this name has already been created in the system, then when saving, a corresponding message is displayed and the region isn't saved. Also, the name must not contain the following characters: < | >.

5. In the **In charge** area, a list of users who are in charge of this region is displayed (see Appointing a user in charge of a region).
To remove a user from the **In charge** list, right-click the user and click the **Delete** button.



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

6. If necessary, in the **Comment** field, enter the region description.
7. Click the **Save** button.

Editing areas and regions

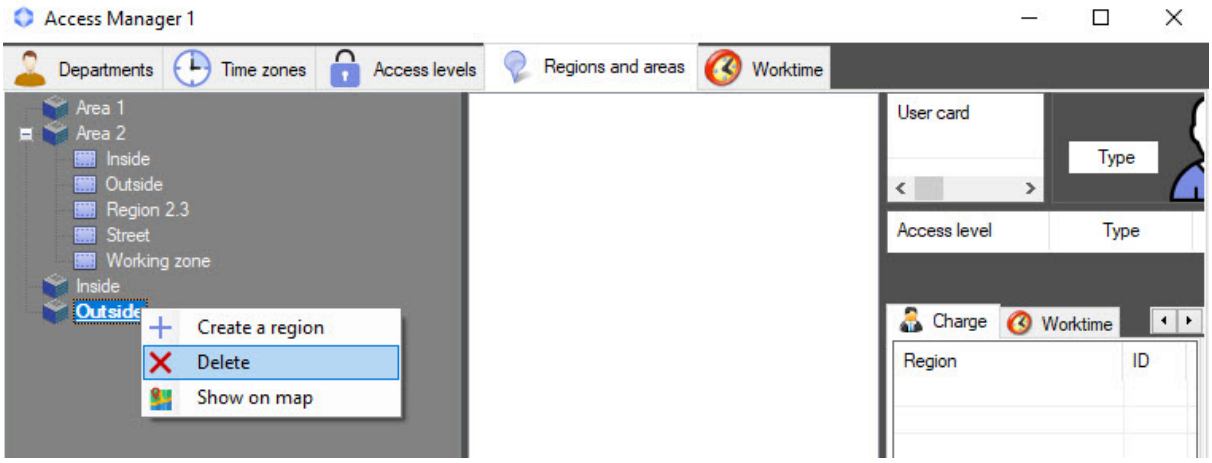
To edit an area or region, double-click it.

The **Edit area properties/Edit region properties** window opens. For the information on working with this window, see Creating areas or Creating and editing regions.

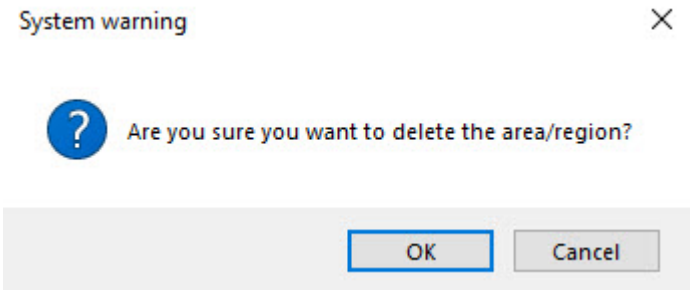
Deleting areas and regions

To delete an area or region, do the following:

1. Right-click it.



2. Select the **Delete** menu item.
3. In the **System warning** window, click the **OK** button to delete an **Area** or **Region**. Click the **Cancel** button to cancel the operation.



> **Note**
>
> When you delete an area, all the child regions in it are deleted as well.

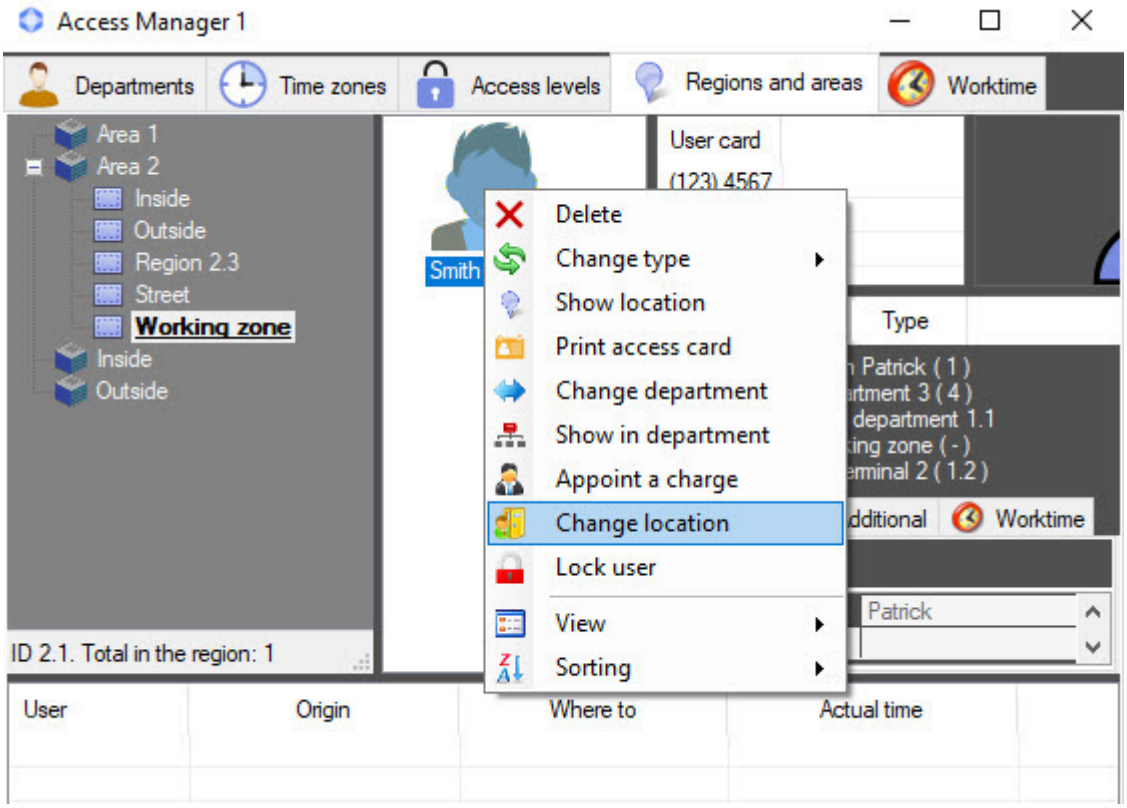
Deleting an area or region is complete.

6.7.8 Changing the current location of a user

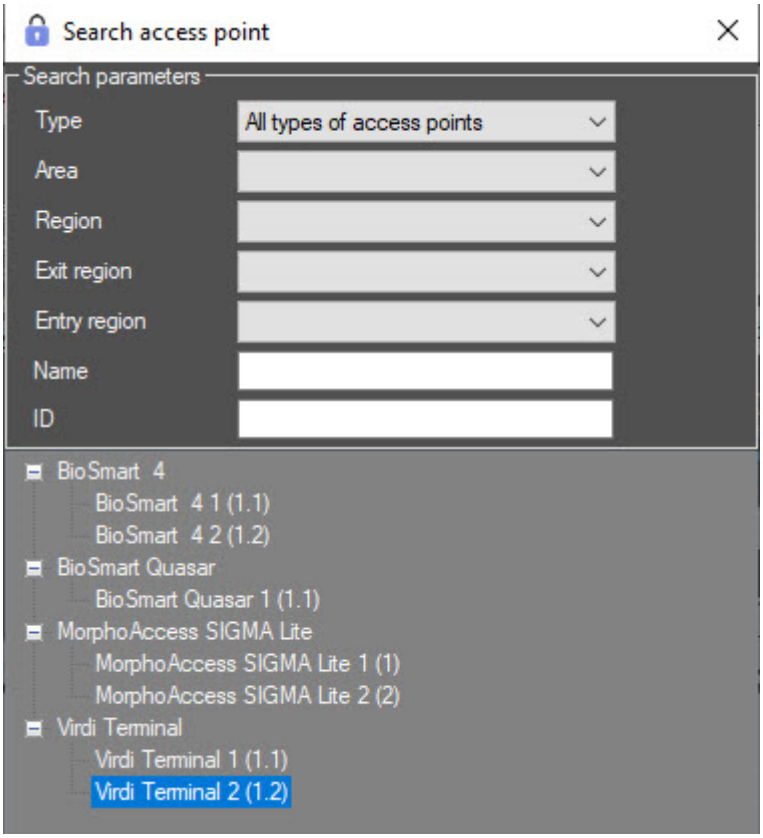
In *ACFA PSIM*, you can move a user to a different region manually if their location differs from what the system shows. To do this, do the following:

1. Go to the **Regions and areas** tab of the **Access Manager** interface window.

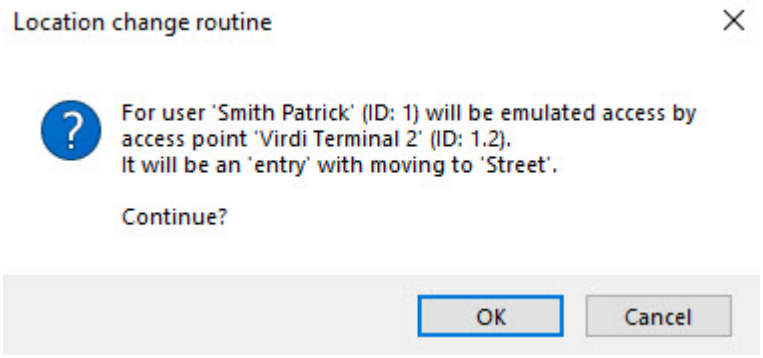
2. Right-click the user whose current location you want to change, and in the function menu, select **Change location**.



3. In the **Search access point** window, double-click the required point in the object tree or use the search to select the point through which the access will be emulated (see Working with the Search access level window). If only one access point is available, the selection window doesn't open.

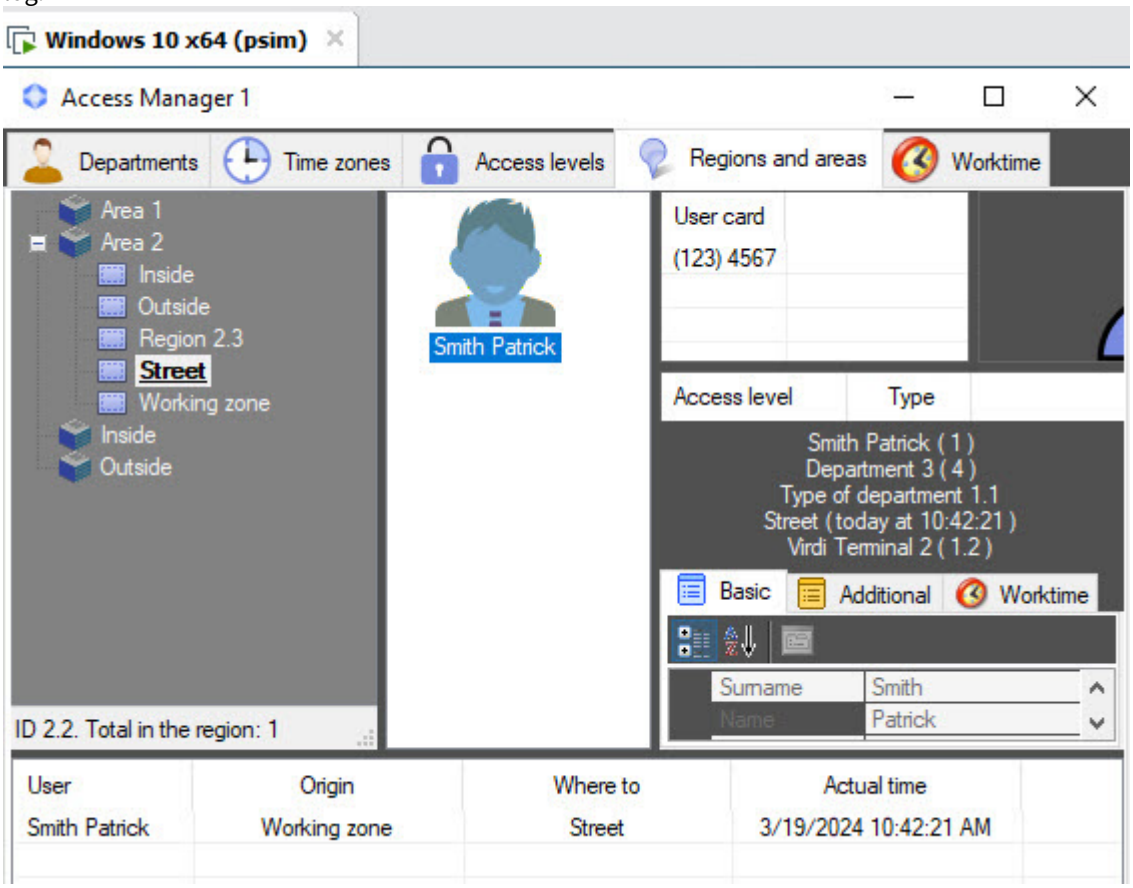


4. Confirm the change of user location by clicking **OK** in the **Location change routine** window.



As a result, the current location of a user changes, and an entry about this event is displayed in the access

log.



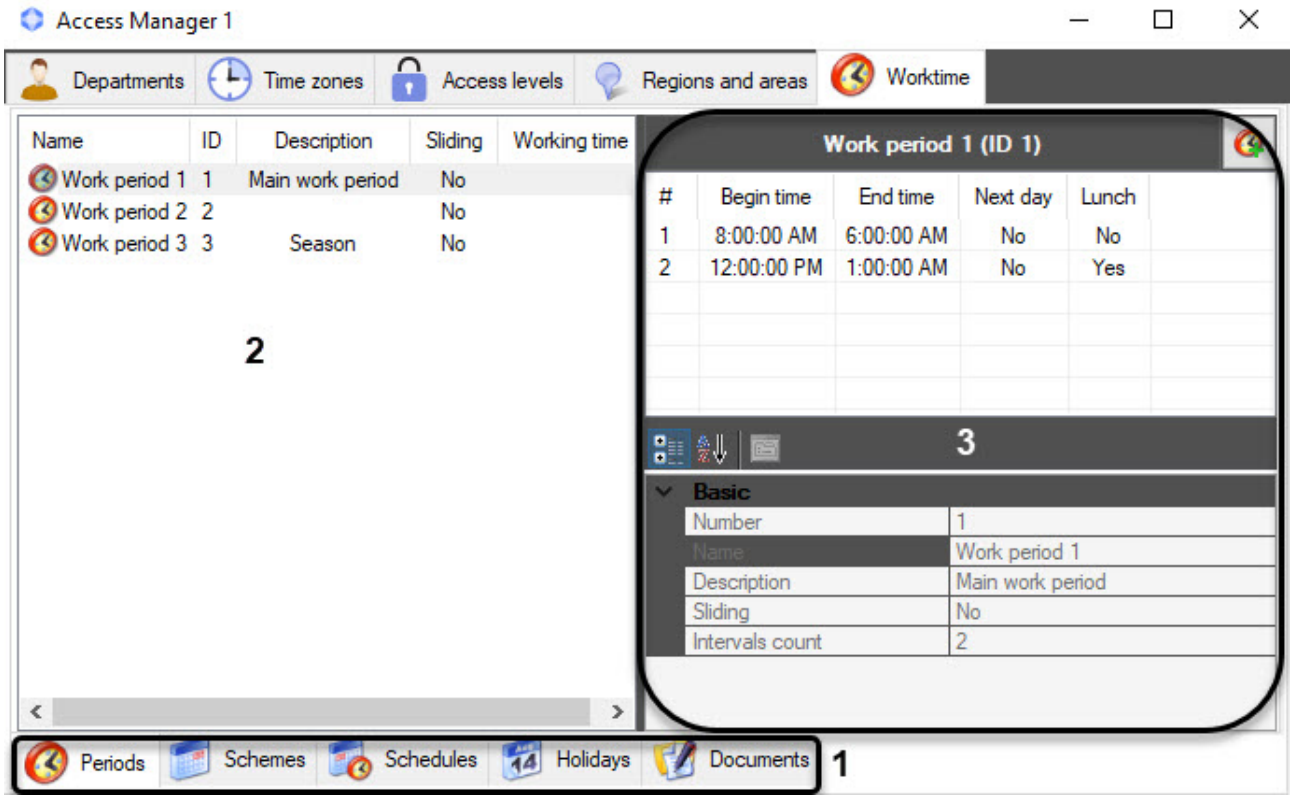
Changing the current location of a user is complete.

6.8 Working with the Time and Attendance subsystem

6.8.1 The Worktime tab of the Access Manager interface window

The main elements of the Worktime tab

The **Worktime** tab of the **Access Manager** interface window consists of three interactive parts. When you switch between the menu items (**1**), the contents of the information field (**2**) and the properties panel (**3**) changes.



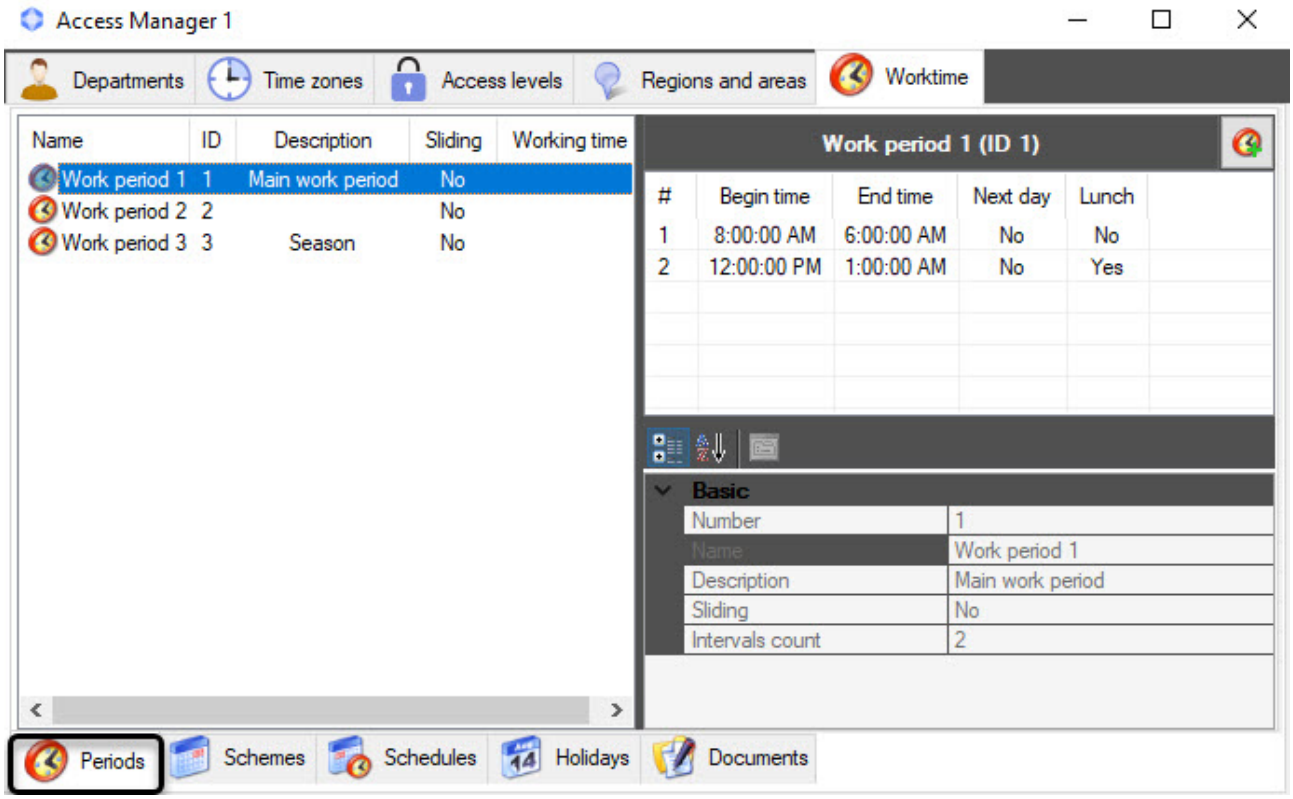
The navigation bar (**1**) is located in the lower left part of the window and used to switch between the menu items of the *Time and Attendance* subsystem.

The information field (**2**) is located in the central left part of the window and displays information on the objects existing in the system of the *Time and Attendance* subsystem.

The properties panel (**3**) is located in the right part of the window. It displays the parameters of the objects from the area (**2**).

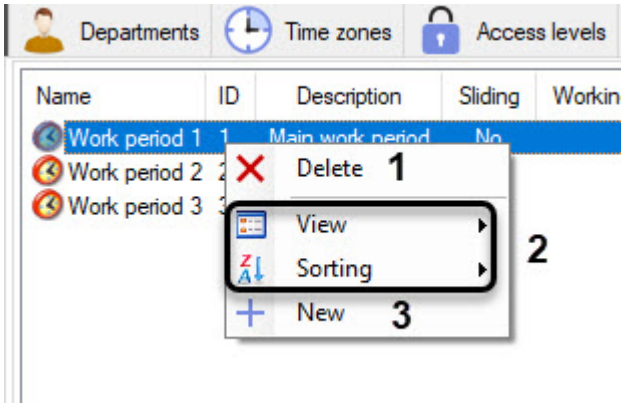
The Periods menu of the Worktime tab

To go to the **Periods** menu, select it on the navigation bar at the bottom of the **Worktime** tab of the **Access Manager** interface window.



The main elements of the **Periods** menu are described in The main elements of the Worktime tab.

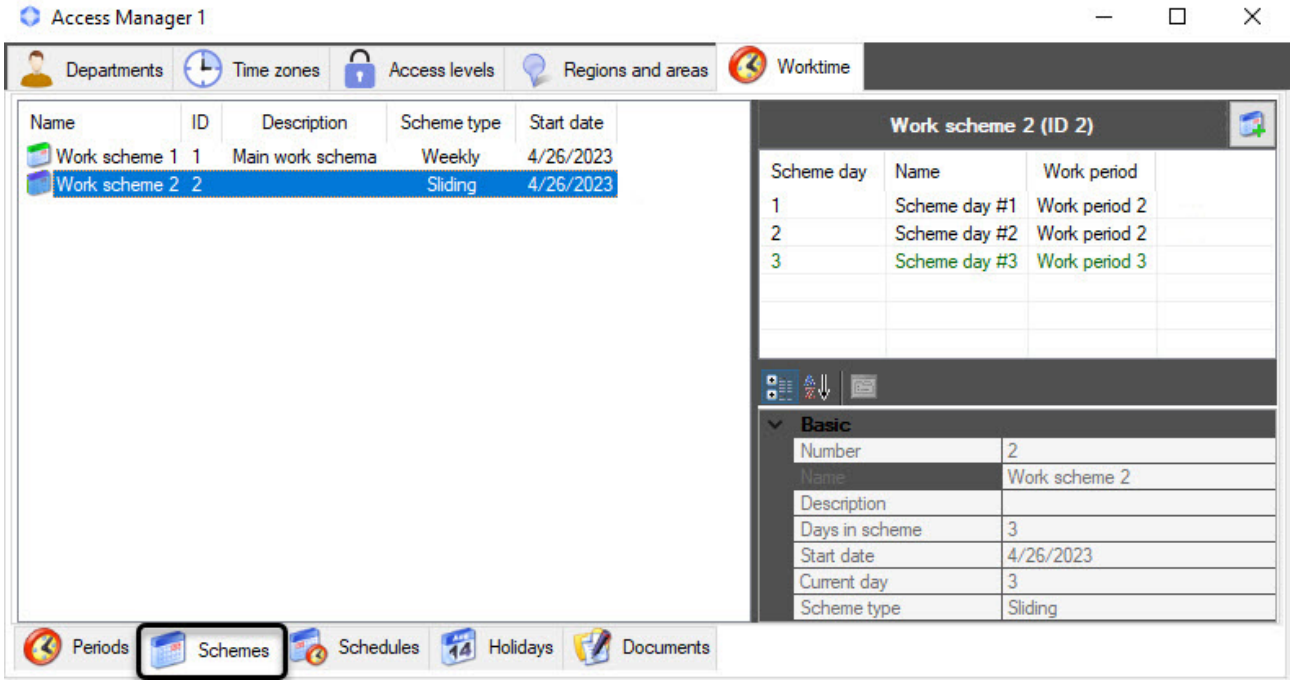
When you right-click a work period, the context menu appears, which includes the following actions:



1. **Delete** (**1**)—delete work period (see Work periods).
2. **View** and **Sorting** (**2**)—these actions with interface elements, common to the whole *Access Manager* module, are described in General operations with the Access Manager interface elements.
3. **New** (**3**)—create a new work period (see Work periods).

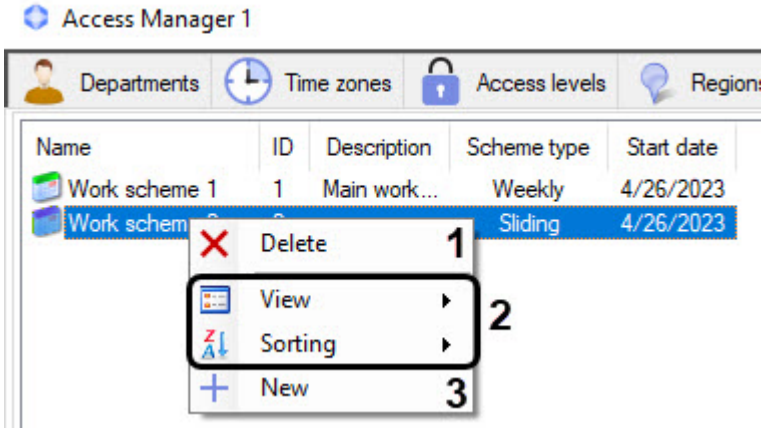
The Schemes menu of the Worktime tab

To go to the **Schemes** menu, select it on the navigation bar at the bottom of the **Worktime** tab of the **Access Manager** interface window.



The main elements of the **Schemes** menu are described in The main elements of the Worktime tab.

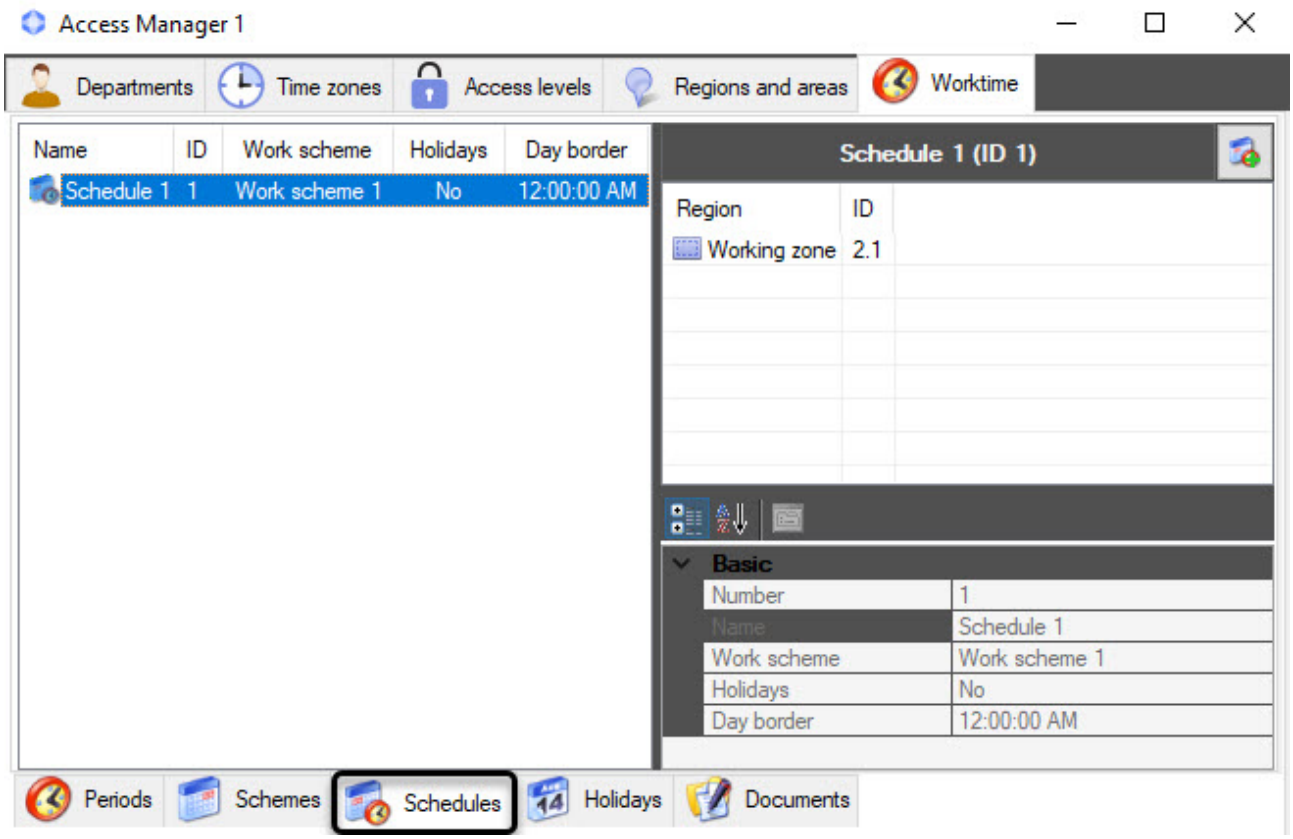
When you right-click a work scheme, the context menu appears, which includes the following actions:



1. **Delete** (**1**)—delete work scheme (see Work schemes).
2. **View** and **Sorting** (**2**)—these actions with interface elements, common to the whole *Access Manager* module, are described in General operations with the Access Manager interface elements.
3. **New** (**3**)—create a new work scheme (see Work schemes).

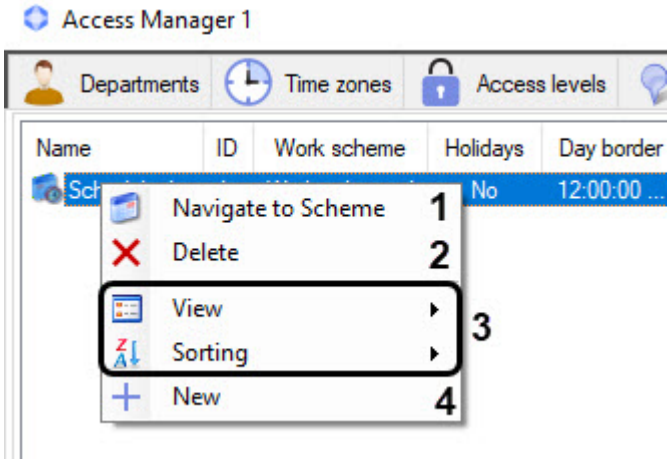
The Schedules menu of the Worktime tab

To go to the **Schedules** menu, select it on the navigation bar at the bottom of the **Worktime** tab of the **Access Manager** interface window.



The main elements of the **Schedules** menu are described in The main elements of the Worktime tab.

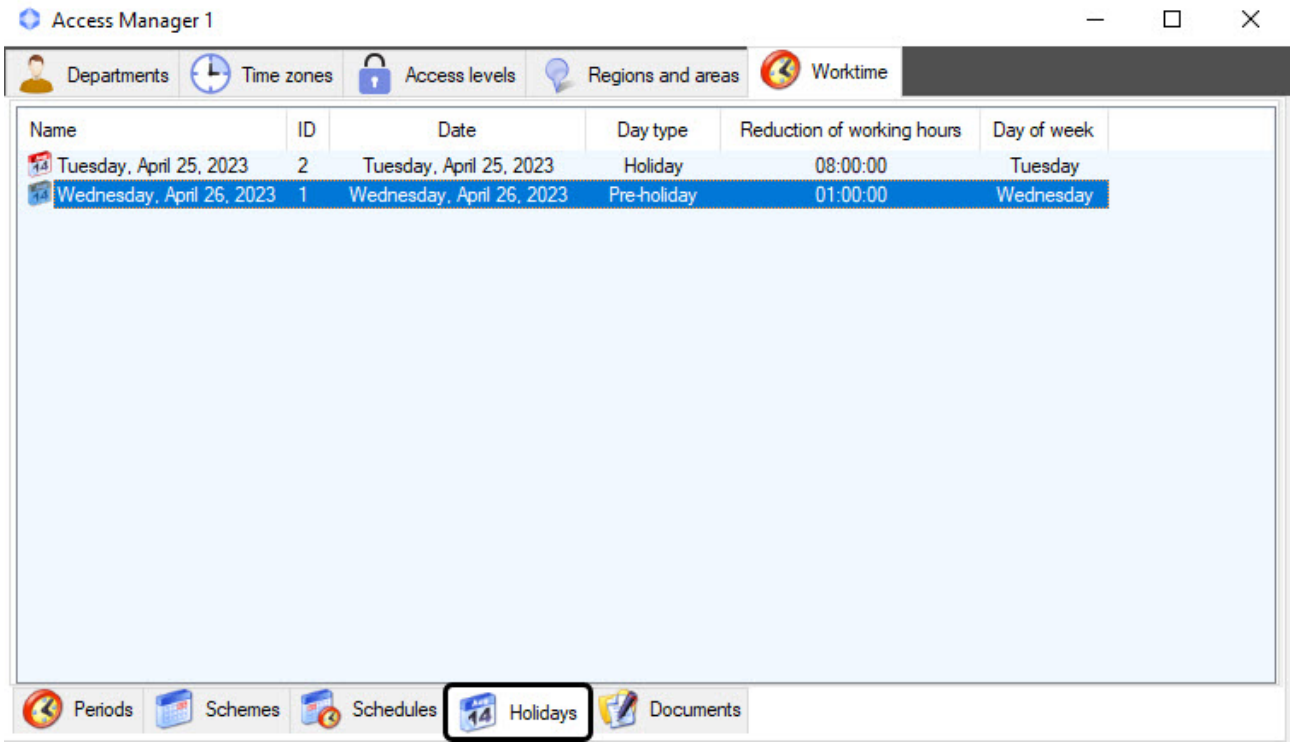
When you right-click a work schedule, the context menu appears, which includes the following actions:



1. **Navigate to Scheme** (**1**)—go to the work scheme that is the basis of this schedule.
2. **Delete** (**2**)—delete work schedule (see Work schedules).
3. **View** and **Sorting** (**3**)—these actions with interface elements, common to the whole *Access Manager* module, are described in General operations with the Access Manager interface elements.
4. **New** (**4**)—create a new work schedule (see Work schedules).

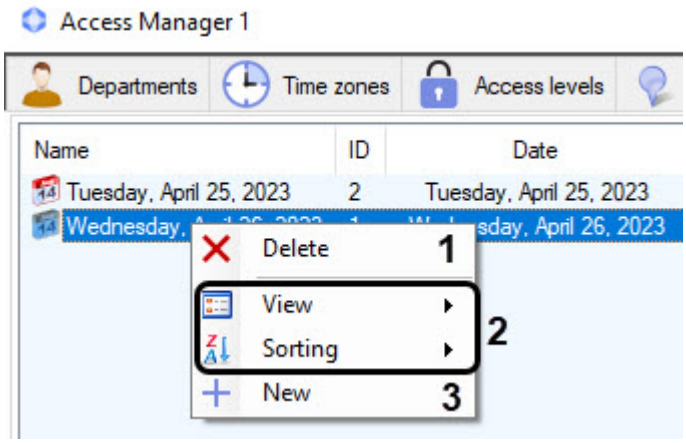
The Holidays menu of the Worktime tab

To go to the **Holidays** menu, select it on the navigation bar at the bottom of the **Worktime** tab of the **Access Manager** interface window.



The window of the **Holidays** menu consists of a navigation bar and an information field. For details, see The main elements of the Worktime tab.

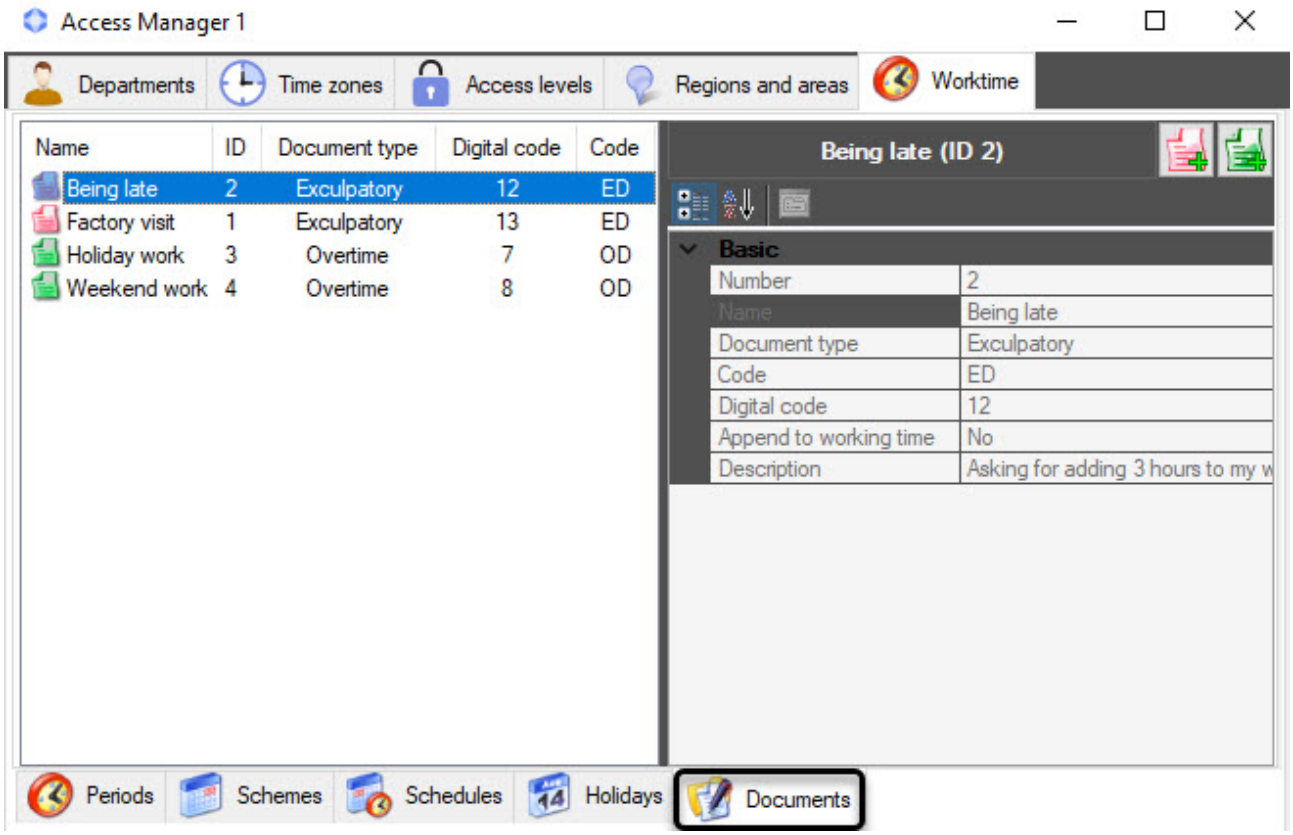
When you right-click a holiday, the context menu appears, which includes the following actions:



1. **Delete** (**1**)—delete holiday (see Holidays).
2. **View** and **Sorting** (**2**)—these actions with interface elements, common to the whole *Access Manager* module, are described in General operations with the Access Manager interface elements.
3. **New** (**3**)—create a new holiday (see Holidays).

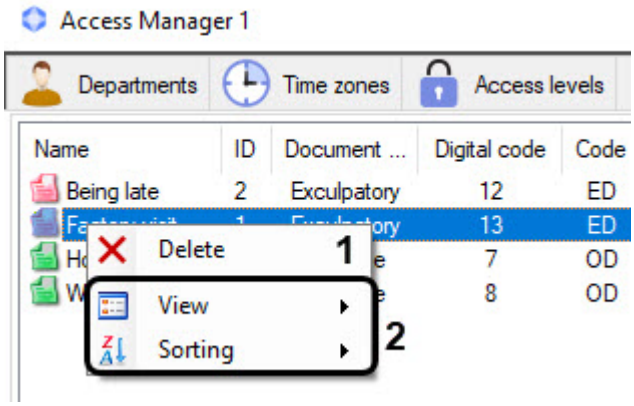
The Documents menu of the Worktime tab

To go to the **Documents** menu, select it on the navigation bar at the bottom of the **Worktime** tab of the **Access Manager** interface window.



The main elements of the **Documents** menu are described in The main elements of the Worktime tab.

When you right-click a document, the context menu appears, which includes the following actions:



1. **Delete** (**1**)—delete document (see Documents).
2. **View** and **Sorting** (**2**)—these actions with interface elements, common to the whole *Access Manager* module, are described in General operations with the Access Manager interface elements.

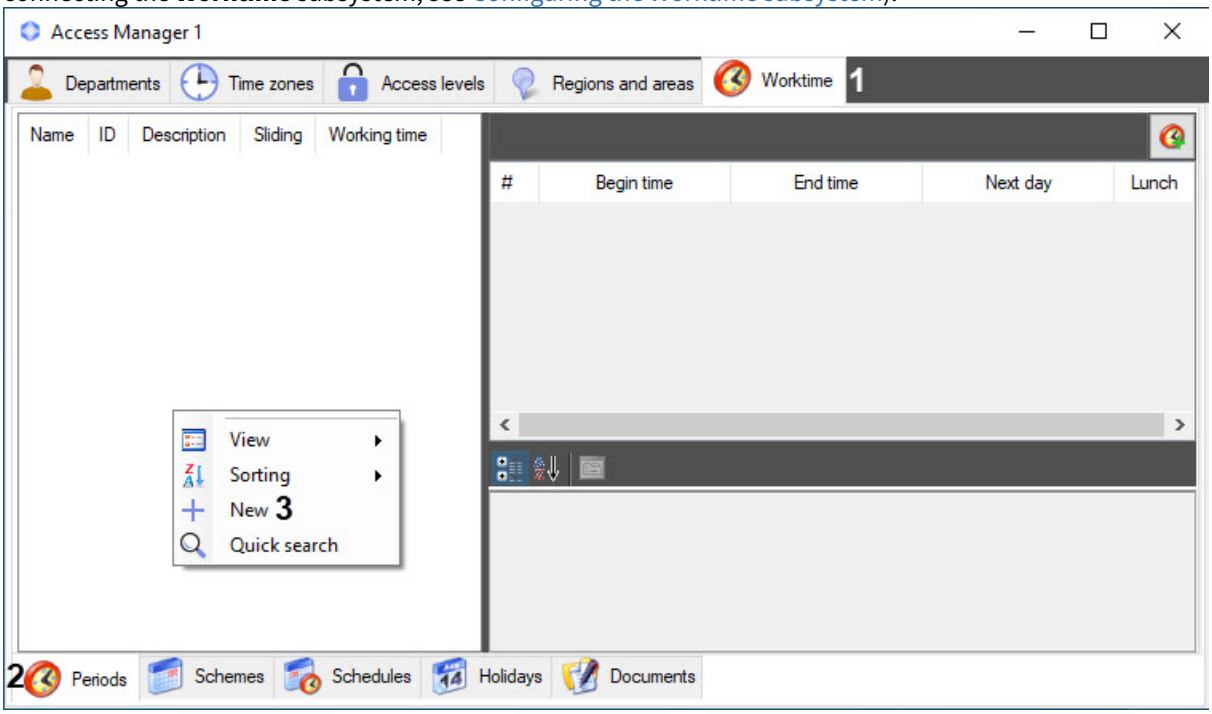
6.8.2 Work periods

On the page:

To work with the *Time and Attendance* subsystem, you need to create and configure work periods.

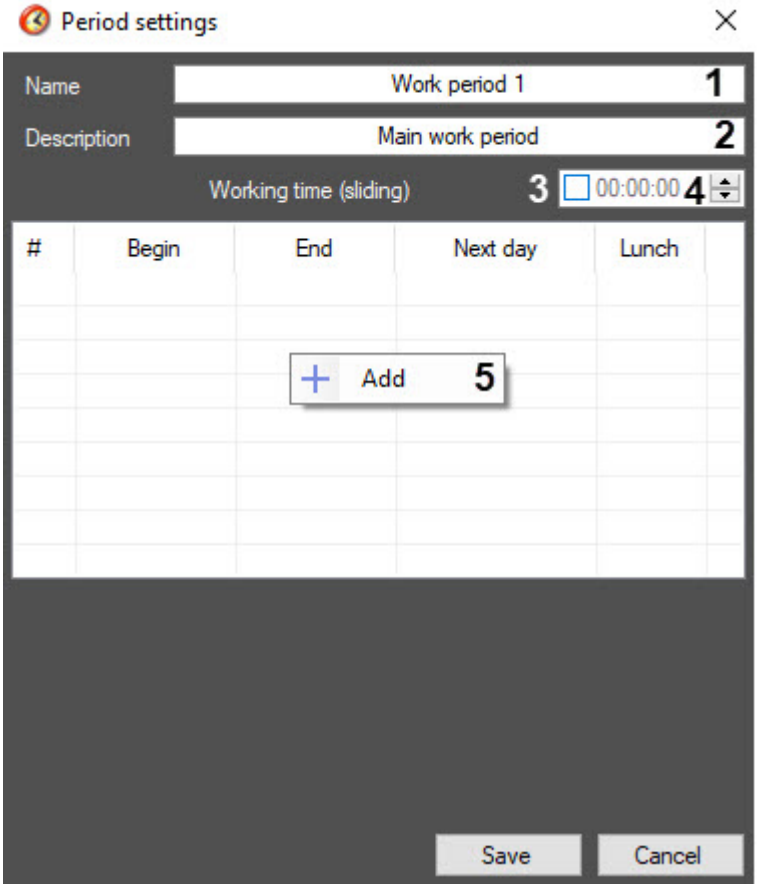
Creating work periods

1. Go to the **Worktime** tab (**1**) of the **Access Manager** interface window (For more information about connecting the **Worktime** subsystem, see Configuring the Worktime subsystem).



2. Go to the **Periods** menu (**2**).
3. Right-click the empty space on the left side of the window to open the context menu.

4. In the context menu, select **New** (**3**). The **Schedule settings** form will open.

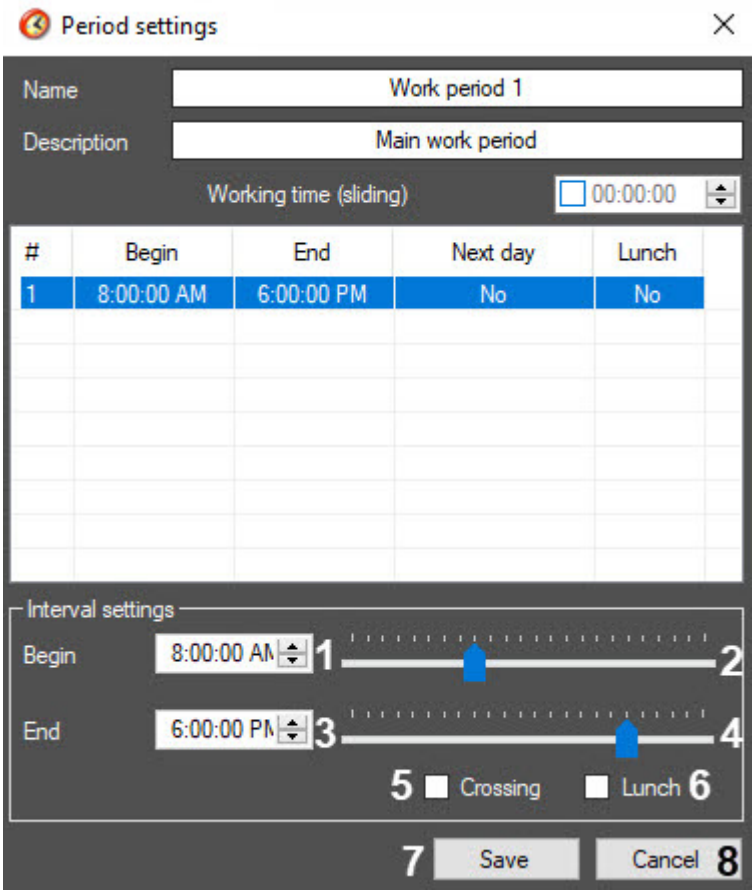


5. In the **Name** field (**1**), enter the name of the work period.
6. In the **Description** field (**2**), enter the description of the work period.
7. Set the **Working time (sliding)** checkbox (**3**), if sliding work schedule is used.

> **Note**
>
> Sliding schedule implies unregulated time of an employee at the workplace, but in a certain time interval of the work shift.

8. In the **Working time (sliding)** field (**4**), enter the employee sliding working time in the HH:MM:SS format.
9. To add work intervals, right-click an empty space in the central part of the form and select **Add** (**5**) in the context menu.

10. Enter the interval settings:

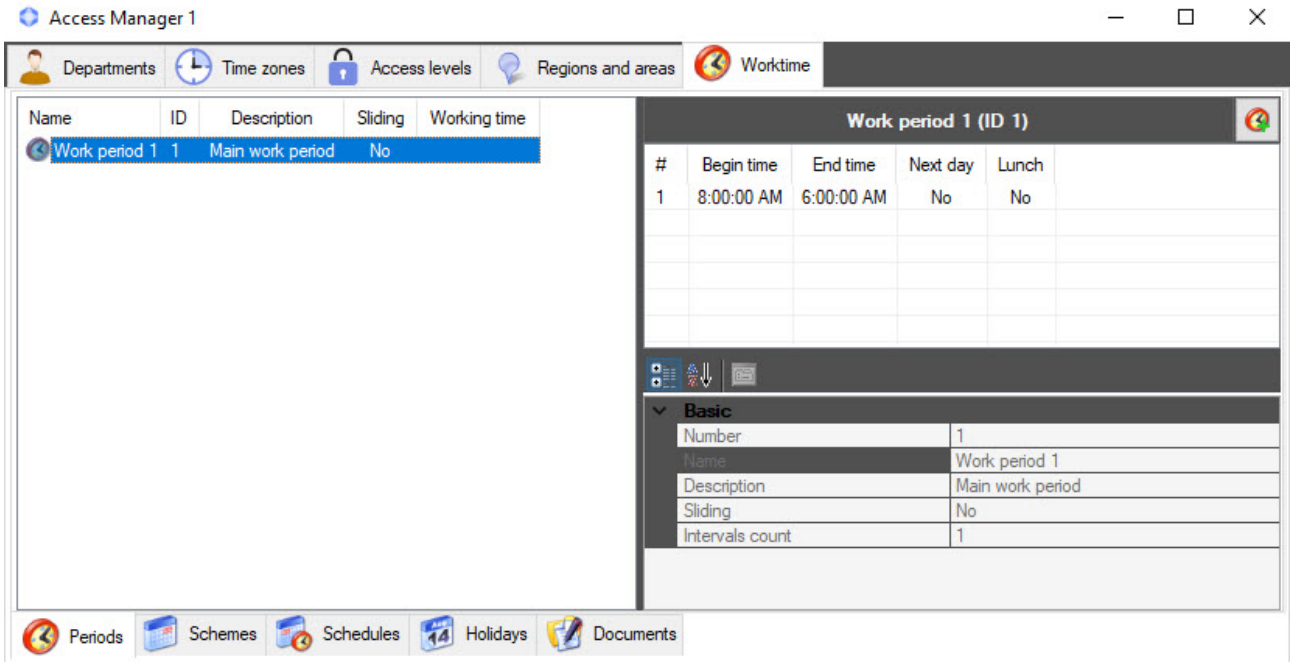


a. In the **Begin** field (**1**), enter the start time of the work interval in the HH:MM:SS format, or select it with the slider (**2**).
b. In the **End** field (**3**), enter the end time of the work interval in the HH:MM:SS format, or select it with the slider (**4**).
c. Set the **Crossing** checkbox (**5**), if the start of the work interval is on the current day and the end is the next day. If the start time of the work interval is longer than the end time, the **Crossing** checkbox will be set automatically.
d. Set the **Lunch** checkbox (**6**), so that the employee's presence at work isn't taken into account when calculating the work period. If the checkbox isn't set, the employee's presence is included in the calculation. To add a lunch break, you need to create a second work interval in which the **Lunch** checkbox will be set (see Examples of work periods).

> **Attention!**
>
> To create correct Time and Attendance reports, it is necessary that only one work interval with the clear **Lunch** checkbox is set (see Working with Time and Attendance reports).

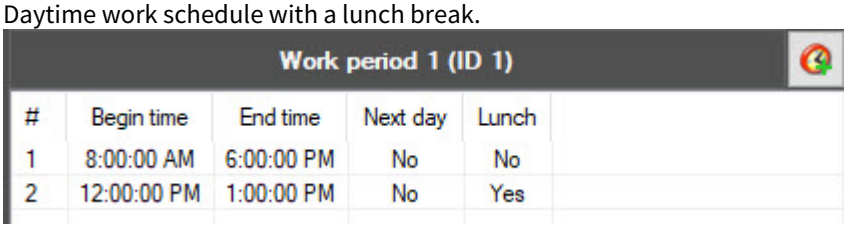
e. Click the **Save** button (**7**) to save the changes. Click the **Cancel** button (**8**) to cancel the changes.

Creating a work period is complete. The created work period will appear in the information field and in the properties panel of the **Periods** menu on the **Worktime** tab of the **Access Manager** interface window.

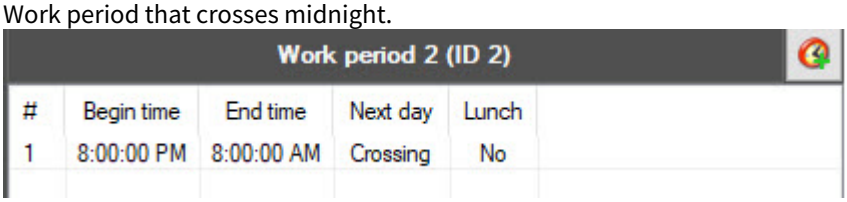


Examples of work periods

1. Daytime work schedule with a lunch break.

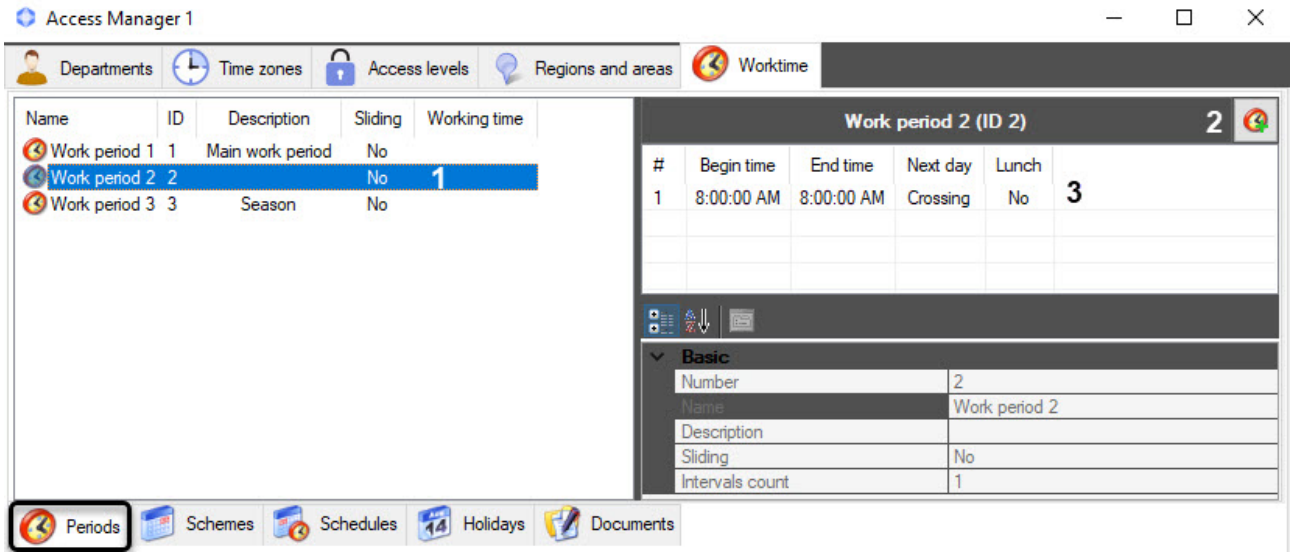


2. Work period that crosses midnight.



Editing work periods

To edit a work period saved in the system, go to the **Periods** menu on the **Worktime** tab of the **Access Manager** interface window and use one of three methods:



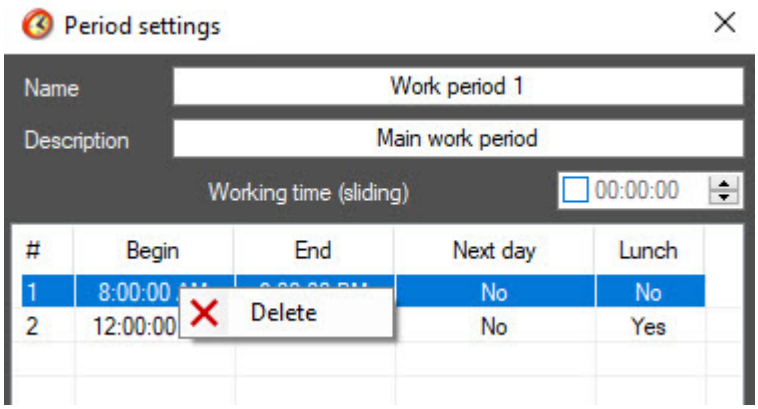
1. In the information field, double-click the period you want to change (**1**).
2. Select the period you want to change, and on the properties panel, click the  button (**2**).
3. Double-click the selected period on the properties panel (**3**).

As a result, the window for editing work period will open.

Deleting work intervals and periods

Deleting work intervals

To delete a work interval saved in the system, do the following:



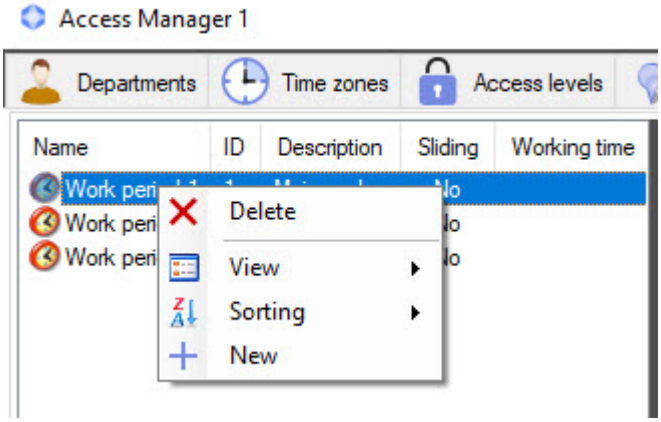
1. Go to the **Periods** menu on the **Worktime** tab of the **Access Manager** interface window.
2. Open the **Schedule settings** form.
3. Right-click the work interval you want to delete to open the context menu.
4. Select **Delete** in the context menu.

The work interval is deleted.

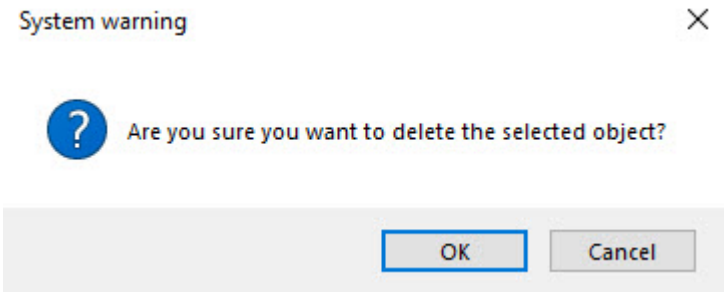
Deleting work periods

To delete a work period saved in the system, do the following:

1. Go to the **Periods** menu on the **Worktime** tab of the **Access Manager** interface window.



2. Right-click the work period you want to delete to open the context menu.
3. Select **Delete** in the context menu.
4. Click the **OK** button in the system warning message.



The work period is deleted.

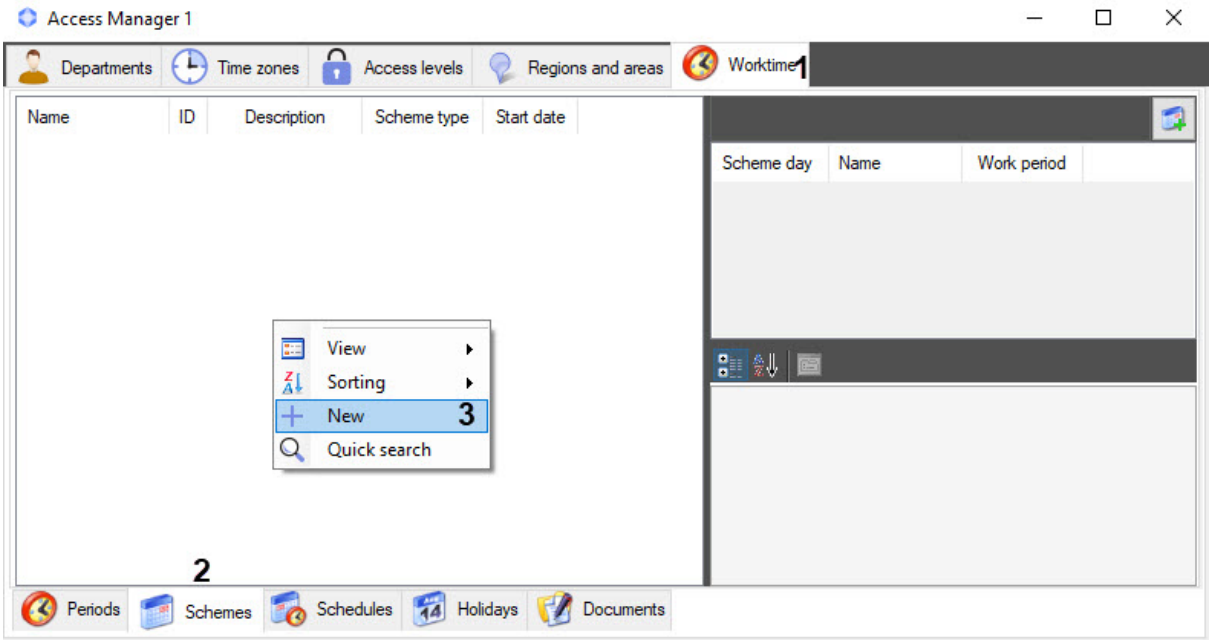
6.8.3 Work schemes

On the page:

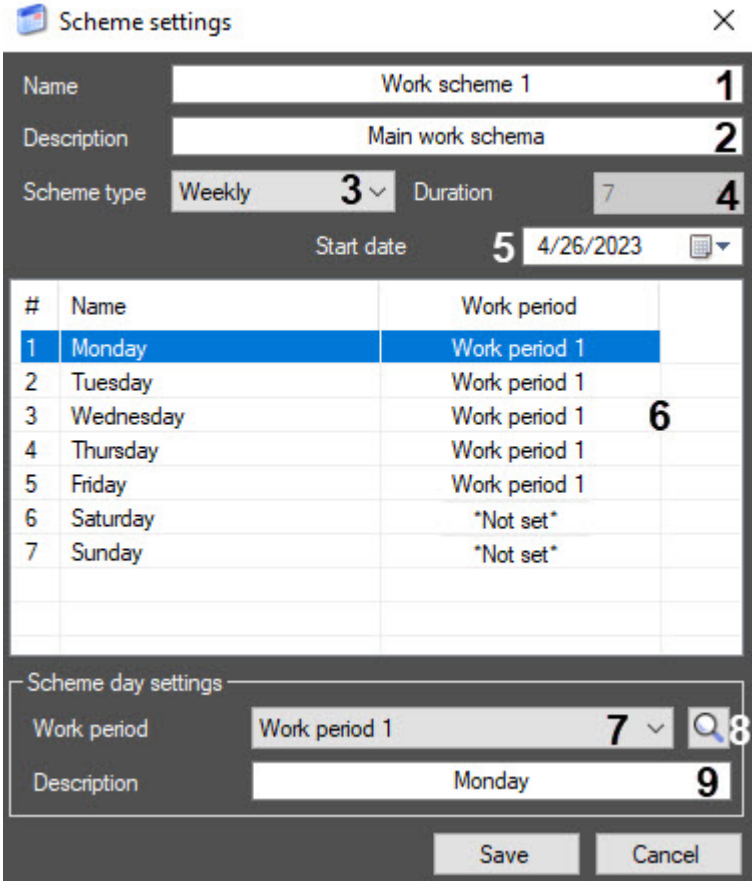
To work with the *Time and Attendance* subsystem, you need to create and configure work schemes.

Creating work schemes

1. Go to the **Worktime** tab (**1**) of the **Access Manager** interface window (For more information about connecting the **Worktime** subsystem, see Configuring the Worktime subsystem).

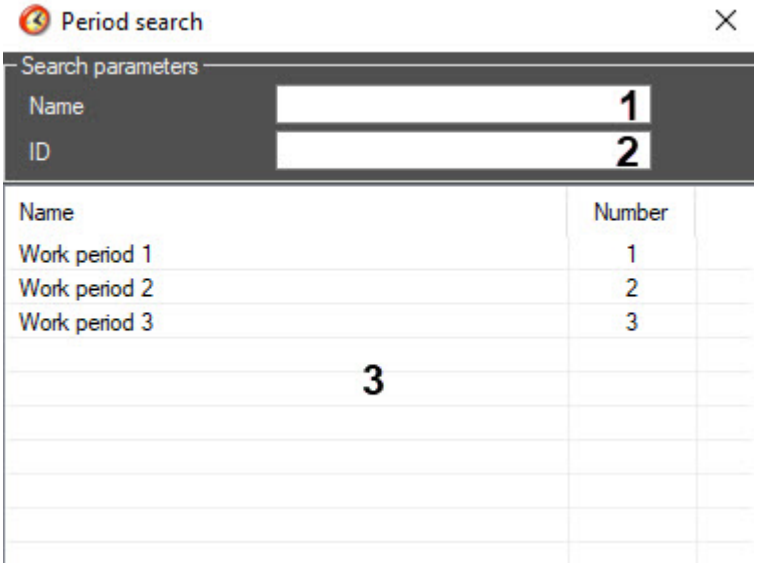


2. Go to the **Schemes** menu (**2**).
3. Right-click the empty space on the left side of the window to open the context menu.
4. In the context menu, select **New** (**3**). The **Scheme settings** form will open.



5. In the **Name** field (**1**), enter the name of the scheme.
6. In the **Description** field (**2**), enter the description of the scheme.

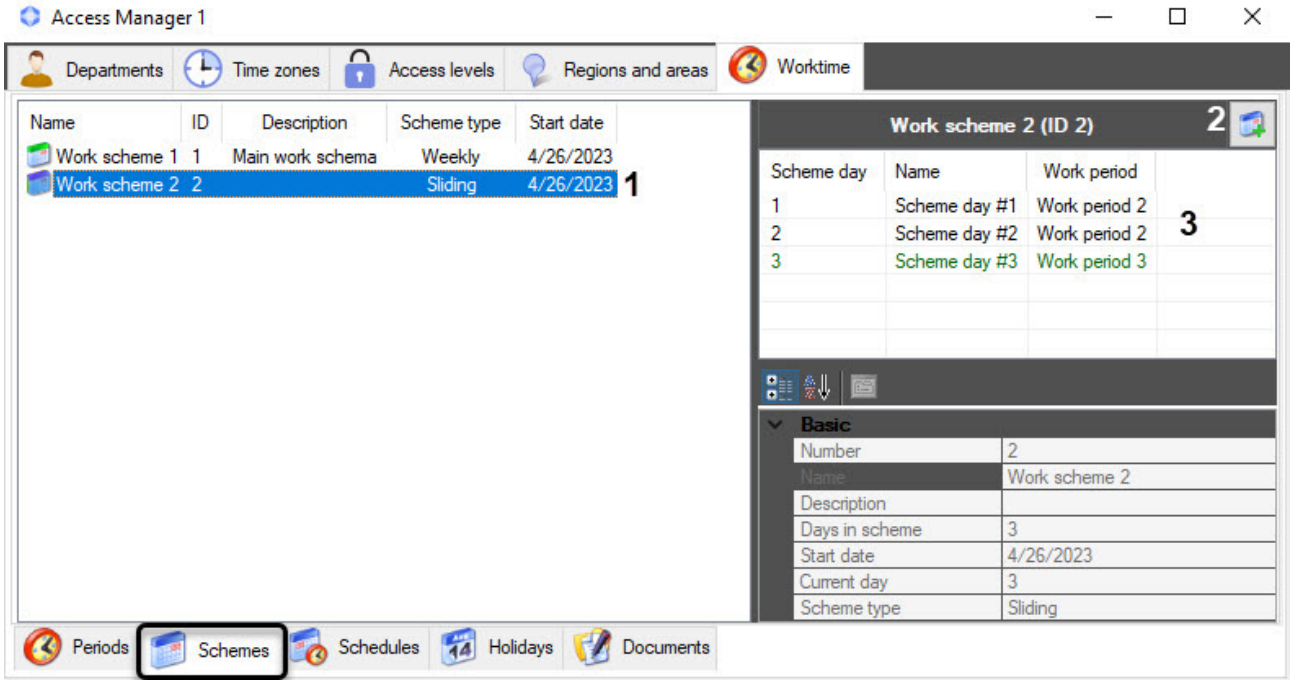
7. From the **Scheme type** drop-down list (**3**), select the type of a scheme you want to use. The scheme type determines the duration of the scheme in days (**4**). There are three types of scheme available:
    a. **Weekly**—the duration of the scheme is seven days.
    b. **Sliding**—the duration of the scheme is set manually.
    c. **Monthly**—the duration of the scheme is 31 days.
8. If you selected the **Sliding** scheme type, in the **Duration** field (**4**), enter the duration of the scheme in days.
9. In the **Start date** field (**5**), set the start date of the work scheme by clicking the button and opening a calendar, or enter the start date manually in the DD.MM.YYYY format.
10. Set the parameters for each day of the work scheme:
    a. For each scheme day in table (**6**) assign a work period by selecting it from the **Work period** drop-down list (**7**) or by using the search button (**8**). When you click the button, the **Period search** window will open, where you can select a work period from the list (**3**) or search it by parameters:



        i. In the **Name** field (**1**), enter the work period name to search by it. The search starts with the first character.
        ii. In the **ID** field (**2**), enter the work period ID to search by it.
    b. If necessary, in the **Description** field (**9**), enter a description of the scheme day.
11. Click the **Save** button to save all changes.

Editing work schemes

To edit a work scheme saved in the system, go to the **Schemes** menu on the **Worktime** tab of the **Access Manager** interface window and use one of three methods:



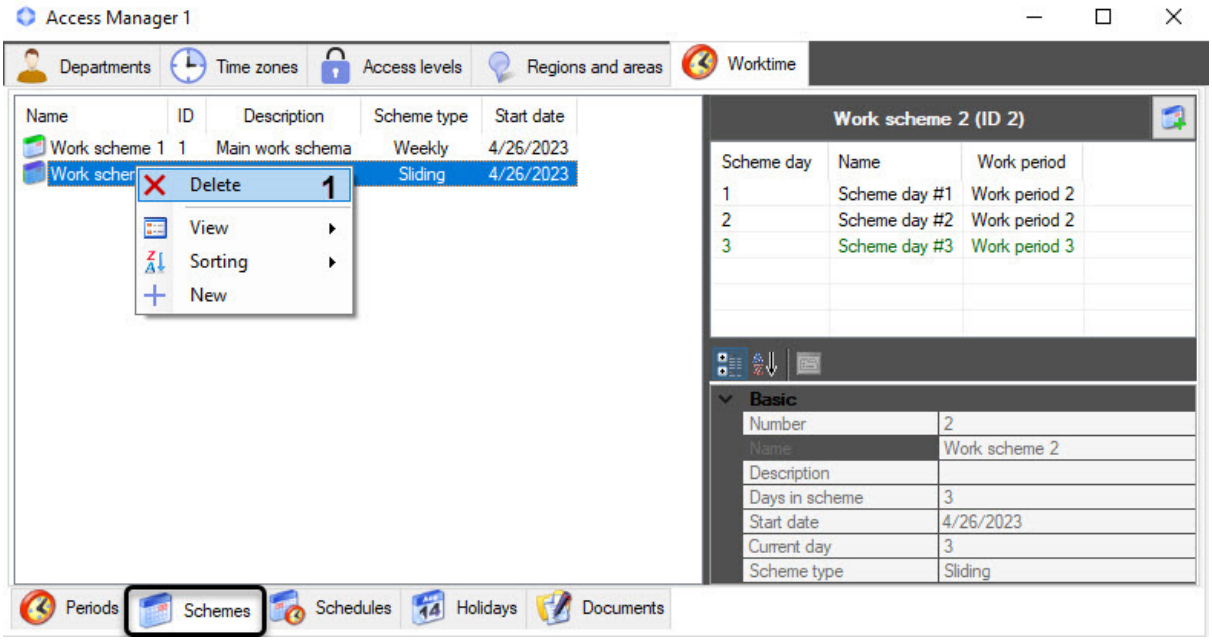
1. In the information field, double-click the work scheme you want to change (**1**).
2. Select the work scheme you want to change, and on the properties panel, click the  button (**2**).
3. Double-click any day of the selected work scheme on the properties panel (**3**).

As a result, the window for editing work scheme will open.

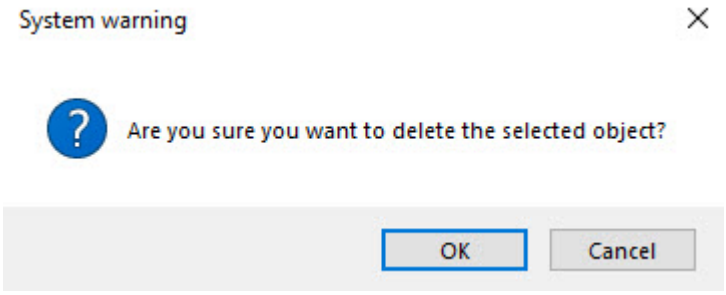
Deleting work scheme

To delete a work scheme saved in the system, do the following:

1. Go to the **Schemes** menu on the **Worktime** tab of the **Access Manager** interface window.



2. Right-click the work scheme you want to delete to open the context menu.
3. Select **Delete** (**1**) in the context menu.
4. Click the **OK** button in the system warning message.



The work scheme is deleted.

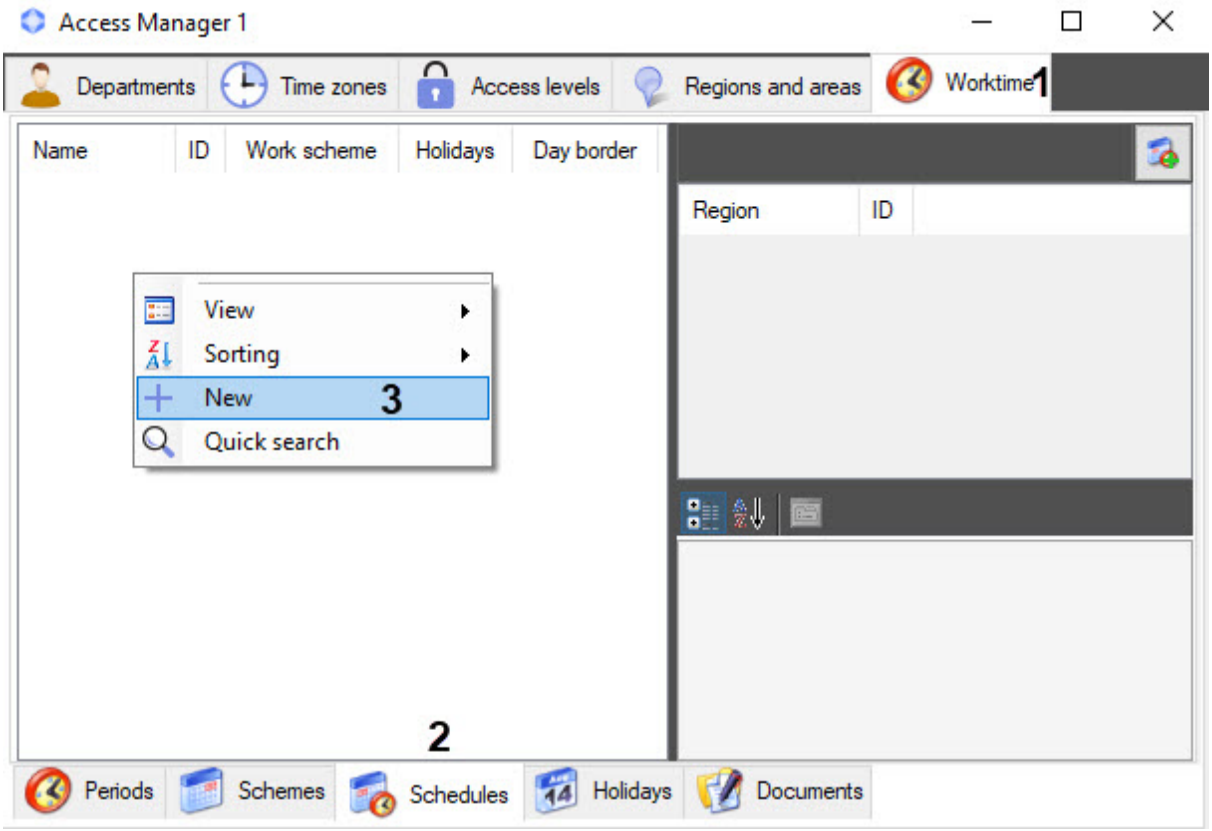
6.8.4 Work schedules

On the page:

To work with the *Time and Attendance* subsystem, you need to create and configure work schedules.

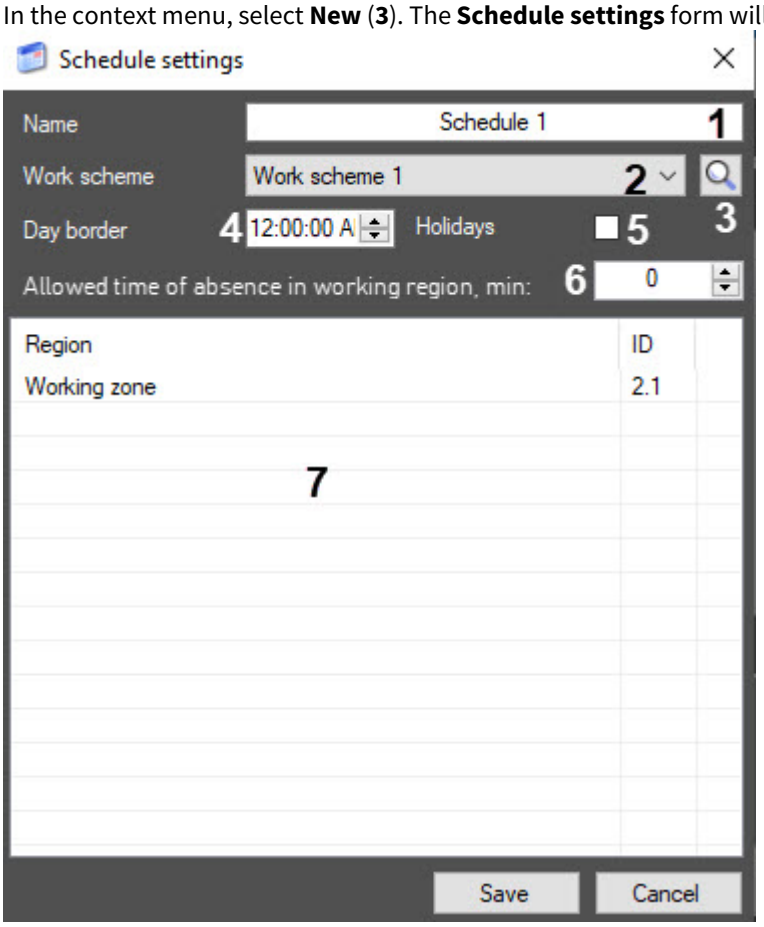
Creating work schedules

1. Go to the **Worktime** tab (**1**) of the **Access Manager** interface window (For more information about connecting the **Worktime** subsystem, see Configuring the Worktime subsystem).

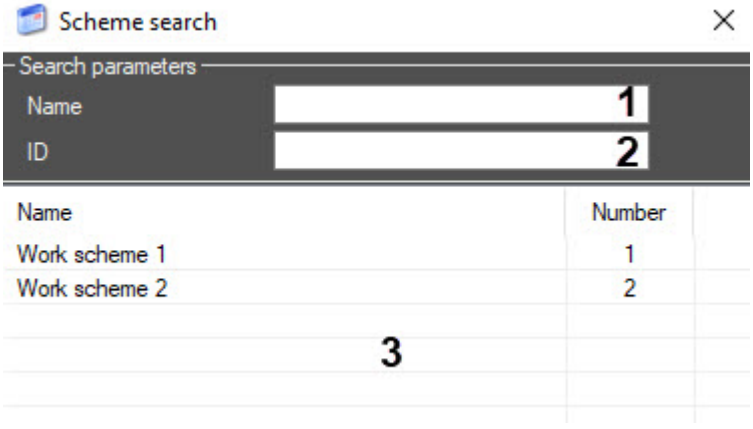


2. Go to the **Schedules** menu (**2**).
3. Right-click the empty space on the left side of the window to open the context menu.

4. In the context menu, select **New** (**3**). The **Schedule settings** form will open.

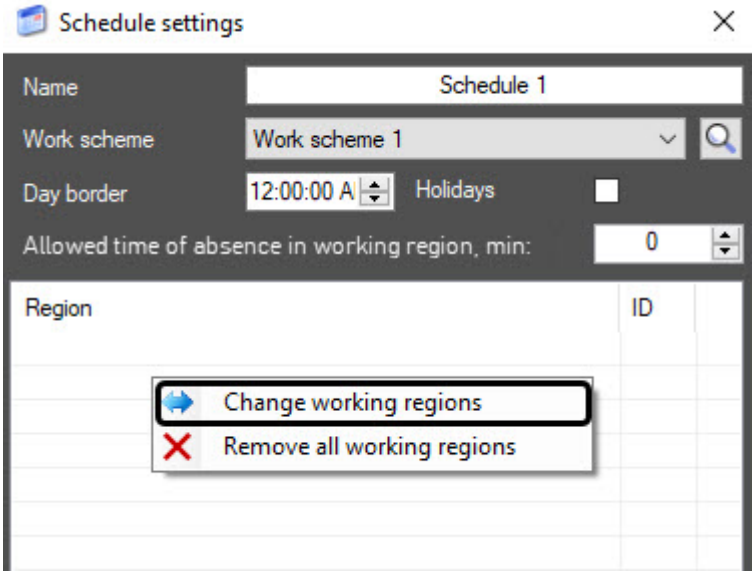


5. In the **Name** field (**1**), enter the name of the work schedule.
6. From the **Work scheme** drop-down list (**2**), select a work scheme for the schedule, or use the search button (**3**). The **Scheme search** window will open, in which you can double-click to select the required work scheme in the area (**3**), or search by parameters:

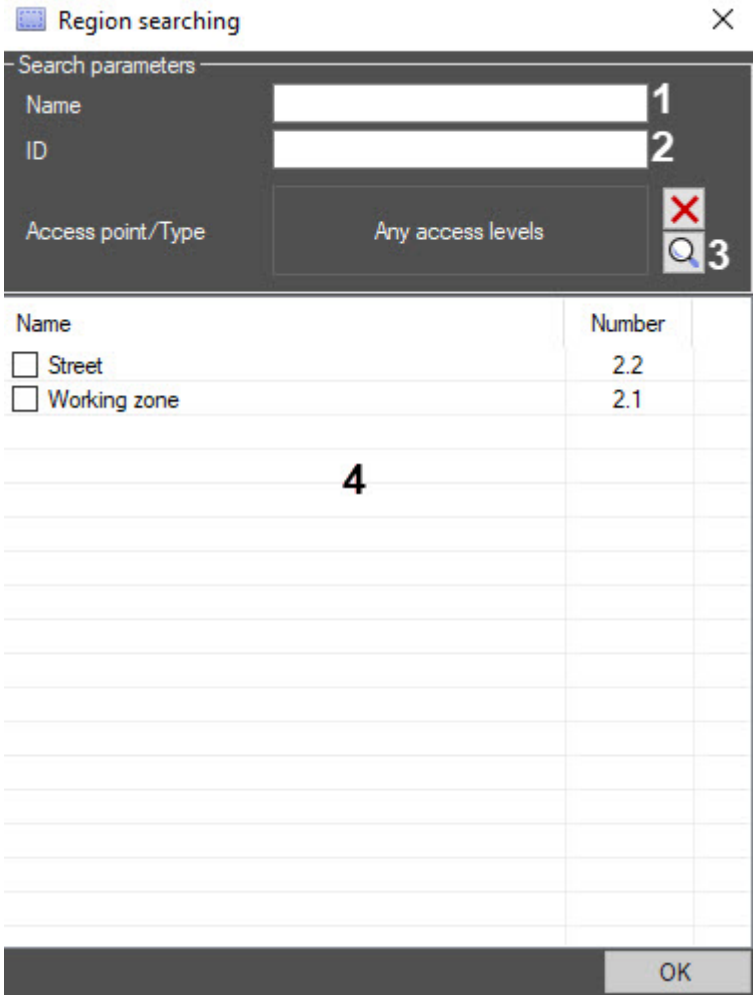


   a. In the **Name** field (**1**), enter the work scheme name to search by it. The search starts with the first character.
   b. In the **ID** field (**2**), enter the work scheme ID to search by it.
7. In the **Day border** field (**4**), enter the time in the HH:MM:SS format from which the day begins.
8. Set the **Holidays** checkbox (**5**) to include holidays in this work schedule (see Holidays).

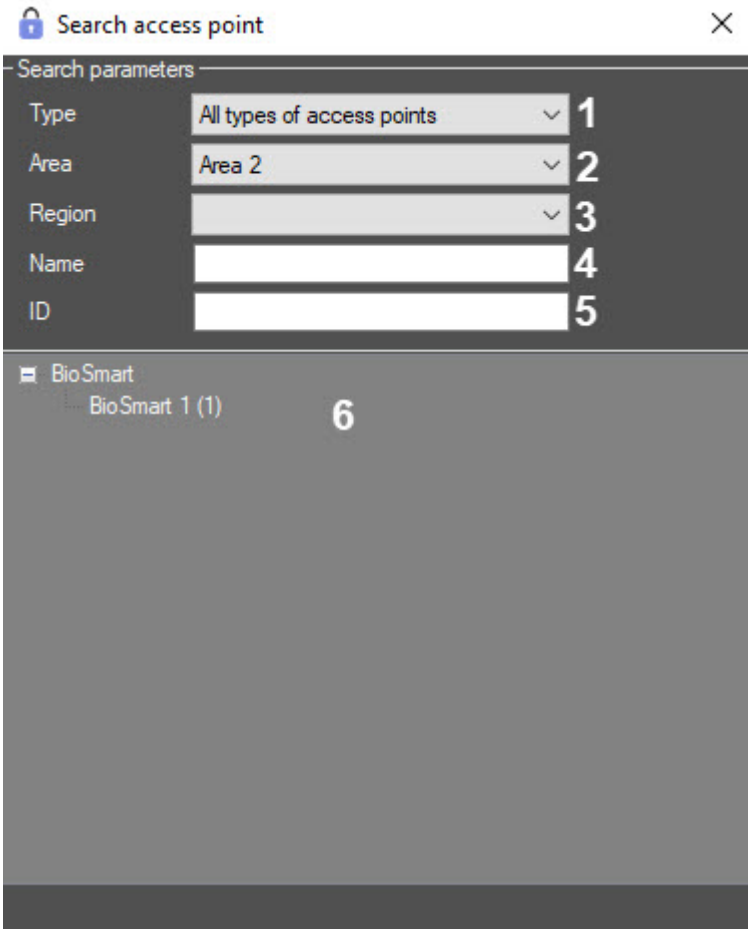
9. In the **Allowed time of absence in working region, min** (**6**) field, enter the time in minutes of an employee absence from work (in the area determined by the **Region** object) that won't be considered as leaving work. In case when an employee is absent from the workplace for longer than the allowed time, the whole period is considered as absence from the working region. The default value is **0**, i.e., any time an employee is out of the working region is considered an absence from work.
10. To add working regions, right-click the empty space in the form and in the context menu, select **Change working regions** (see Appendix 1. Configuring Regions for the ACS Readers to work with the Time and Attendance subsystem).



11. As a result, the **Region searching** window will open. Double-click to select the required working region in the area (**4**) or search by parameters:

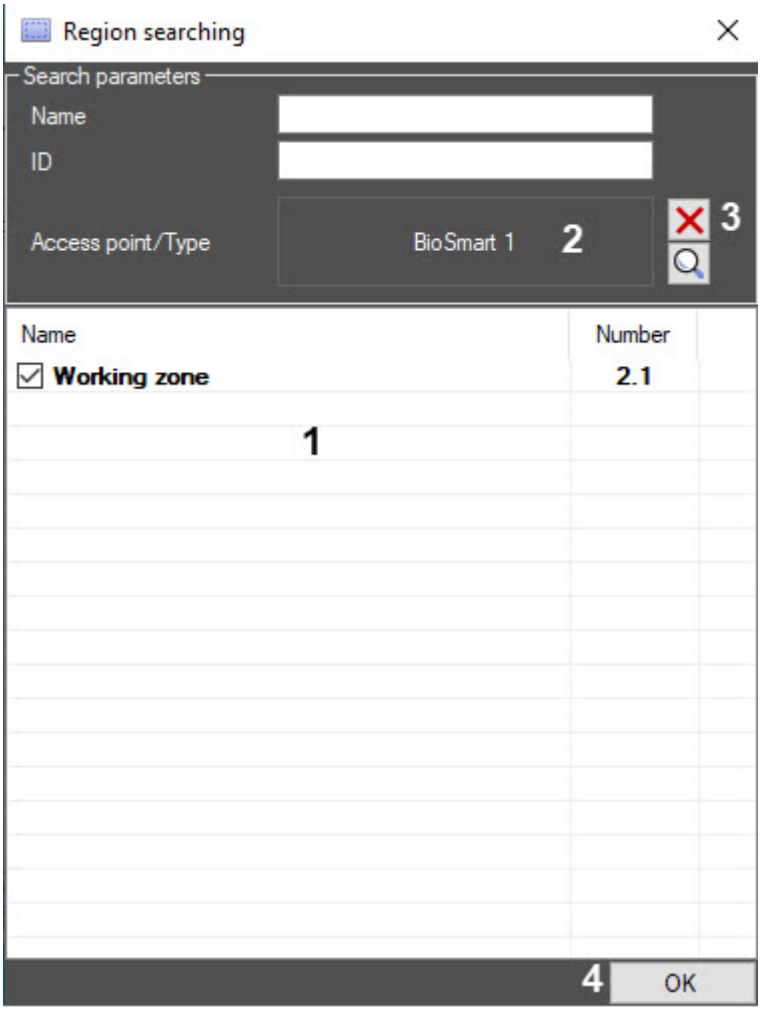


a. In the **Name** field (**1**), enter the working region name to search by it. The search starts with the first character.
b. In the **ID** field (**2**), enter the working region ID to search by it.
c. Click the search button (**3**) to search the region by the access point. In the **Search access point** window, double-click to select the required access point in the area (**6**), or fill out the search parameters:



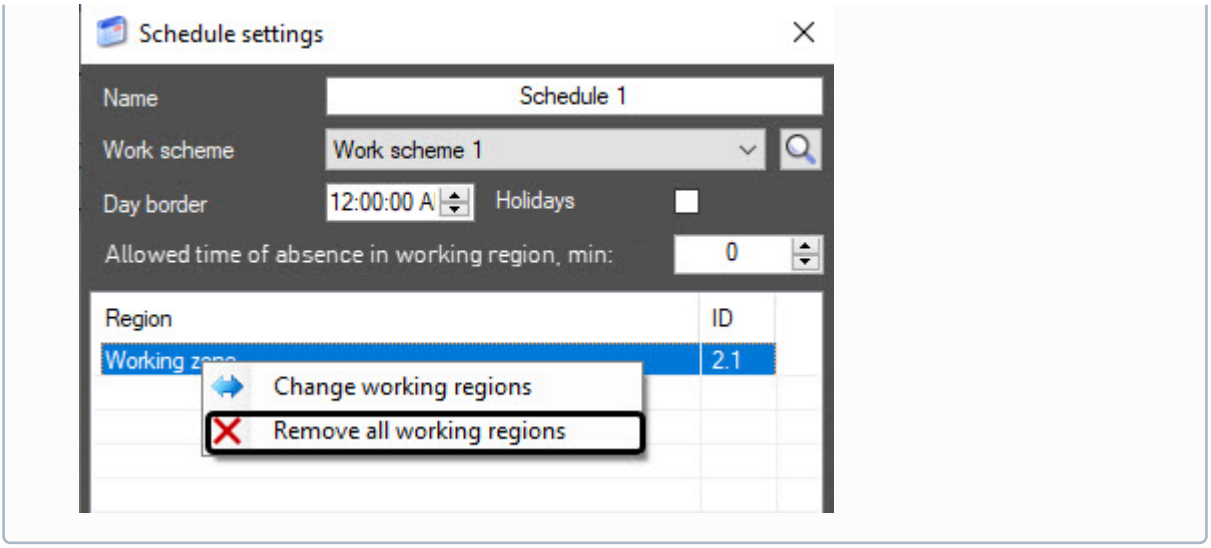
i. From the **Type** drop-down list (**1**), select the type of the access point.
ii. From the **Area** drop-down list (**2**), select the area to which the access point belongs.
iii. From the **Region** drop-down list (**3**), select the region to which the access point belongs.
iv. In the **Name** field (**4**), enter the name of the access point. The search starts with the first character.
v. In the **ID** field (**5**), enter the ID of the access point.
After you select the access point, the **Search access point** window will close.

12. In the **Region searching** form, in the area (**1**), a region will appear to which the selected access point belongs in the area (**2**). To cancel the selected access point, click the button (**3**).



13. Set the checkbox next to the required region and click the **OK** button (**4**). After that the **Region searching** form will close.
14. In the **Schedule settings** form, the selected region will be displayed in the area (**7**). Click the **Save** button to save the changes.

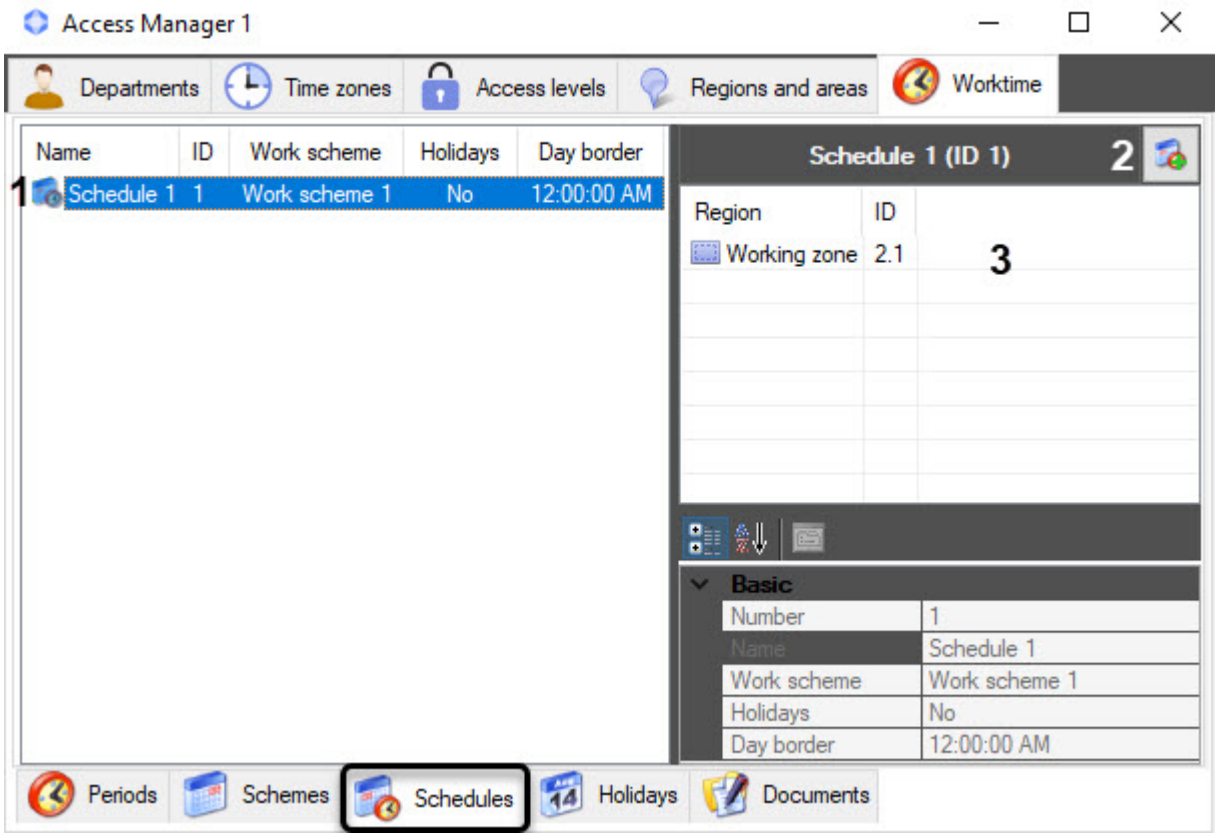
> **Note**
>
> - Assigning working regions to each work schedule is mandatory.
> - The number of working regions that will be included in this work schedule is unlimited.
> - You can delete only all working regions. To do this, in the **Schedule settings** window, right-click any region and in the context menu, select **Remove all working regions**.



The work schedule is created and configured.

Editing work schedules

To edit a work schedule saved in the system, go to the **Schedules** menu on the **Worktime** tab of the **Access Manager** interface window and use one of three methods:



1. In the information field, double-click the work schedule you want to change (**1**).

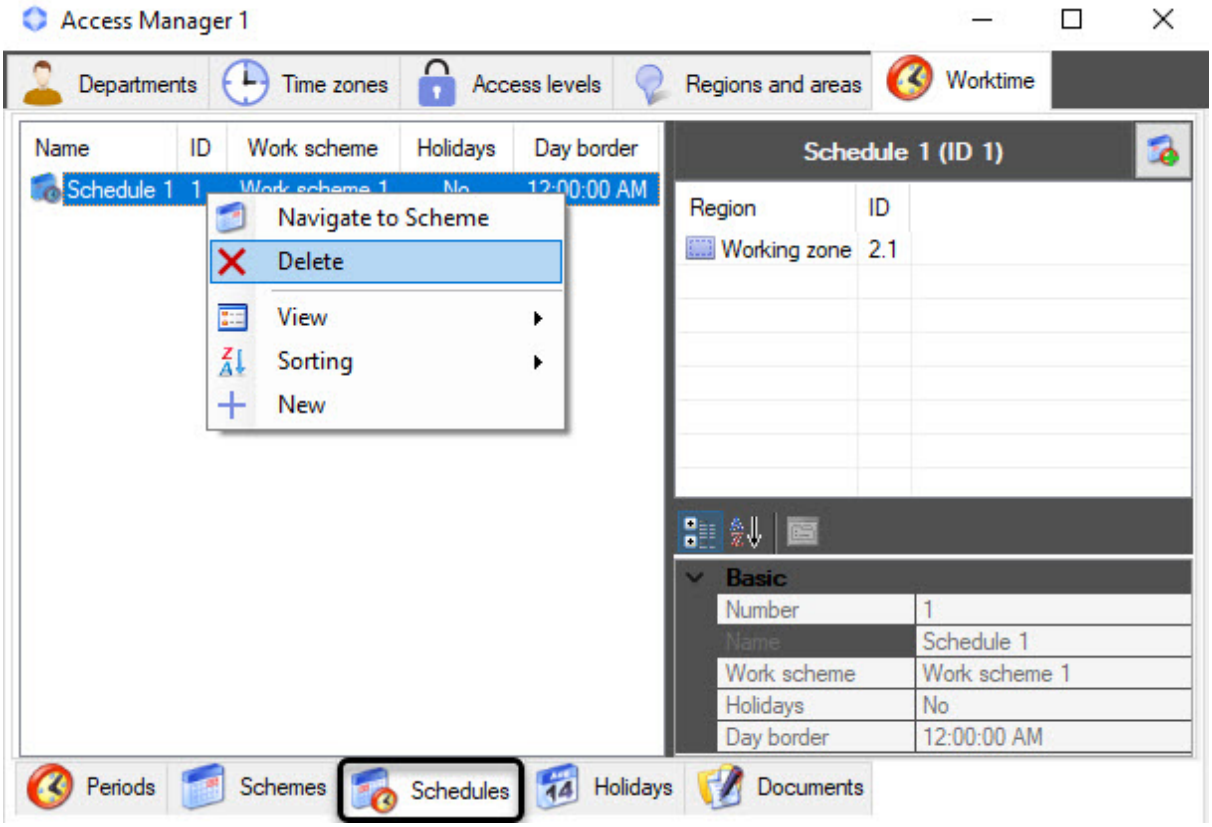
2. Select the work schedule you want to change, and on the properties panel, click the  button (**2**).
3. Double-click the selected working region on the properties panel (**3**).

As a result, the window for editing work schedule will open.

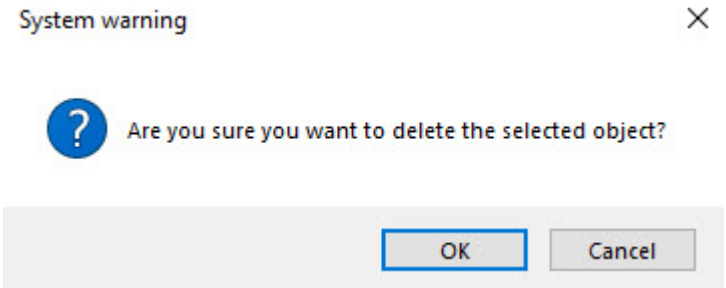
Deleting work schedules

To delete a work schedule saved in the system, do the following:

1. Go to the **Schedules** menu on the **Worktime** tab of the **Access Manager** interface window.



2. Right-click the work schedule you want to delete to open the context menu.
3. Select **Delete** in the context menu.
4. Click the **OK** button in the system warning message.



The work schedule is deleted.

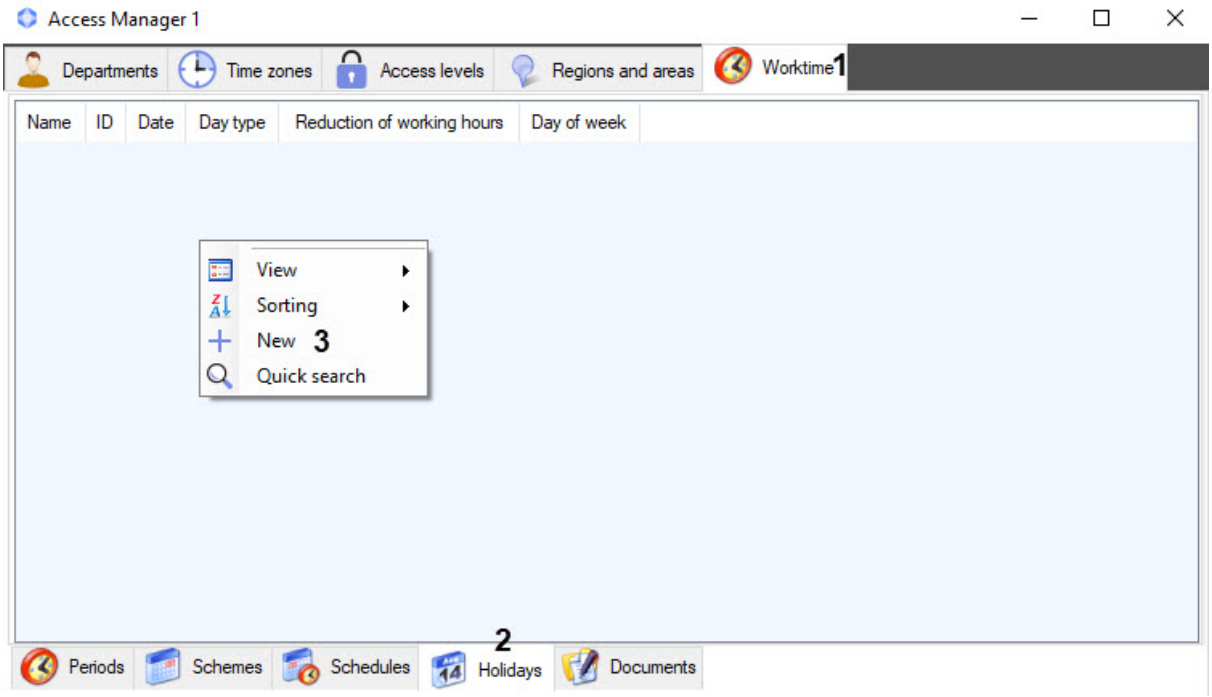
6.8.5 Holidays

On the page:

To work with the *Time and Attendance* subsystem, you need to create and configure holidays.

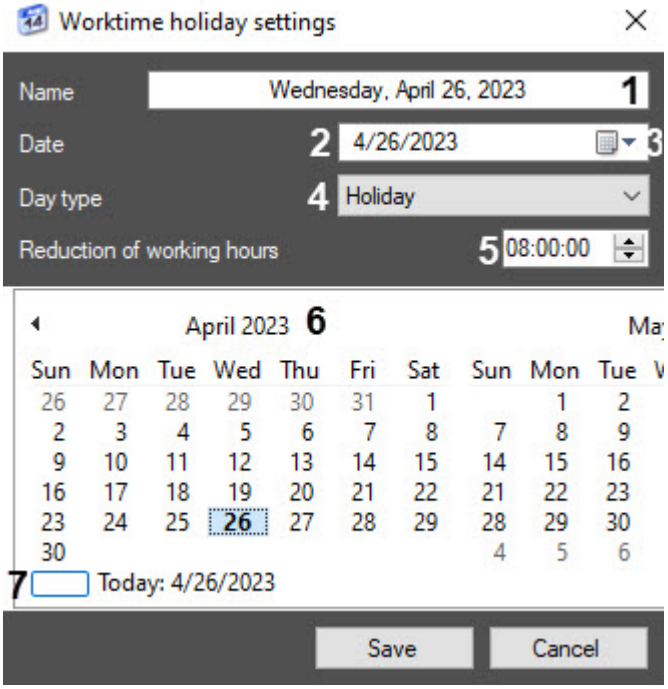
Creating holidays

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



2. Go to the **Holidays** menu (**2**).
3. Right-click the empty space on the left side of the window to open the context menu.

4. In the context menu, select **New** (**3**). The **Worktime holiday settings** form will open.



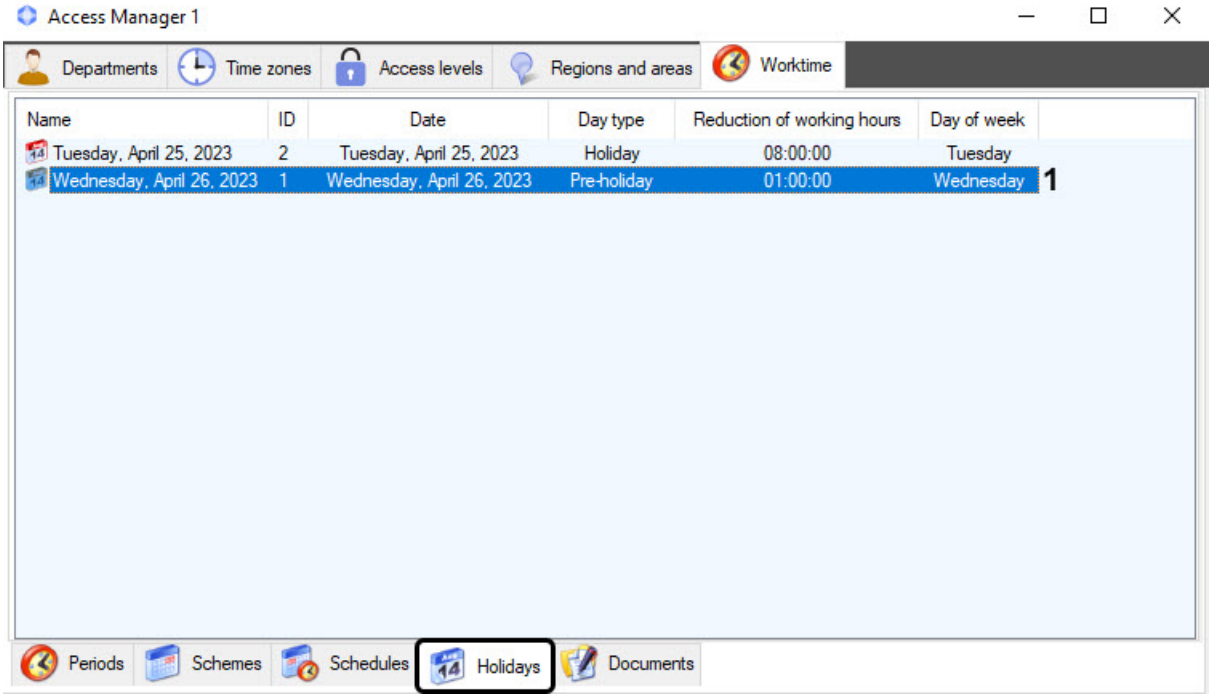
5. In the **Name** field (**1**), enter the name of the holiday. The default name is the current date.
6. In the **Date** field (**2**), enter the date using the calendar that opens when clicking the button (**3**), or by clicking the required date in the area (**6**). The current date is specified in the area (**7**).
7. From the **Day type** drop-down list (**4**), select **Holiday** (usually non-working day) or **Pre-holiday** (working hours are usually reduced by a set time) day type.
8. In the **Reduction of working hours** field (**5**), specify the time in the HH:MM:SS format by which the working day will be reduced. The default value is 8:00:00, i.e., eight hours.
9. Click the **Save** button to save the changes.

Creating holidays is complete.

Editing holidays

To edit a holiday saved in the system, do the following:

1. Go to the **Holidays** menu on the **Worktime** tab of the **Access Manager** interface window.



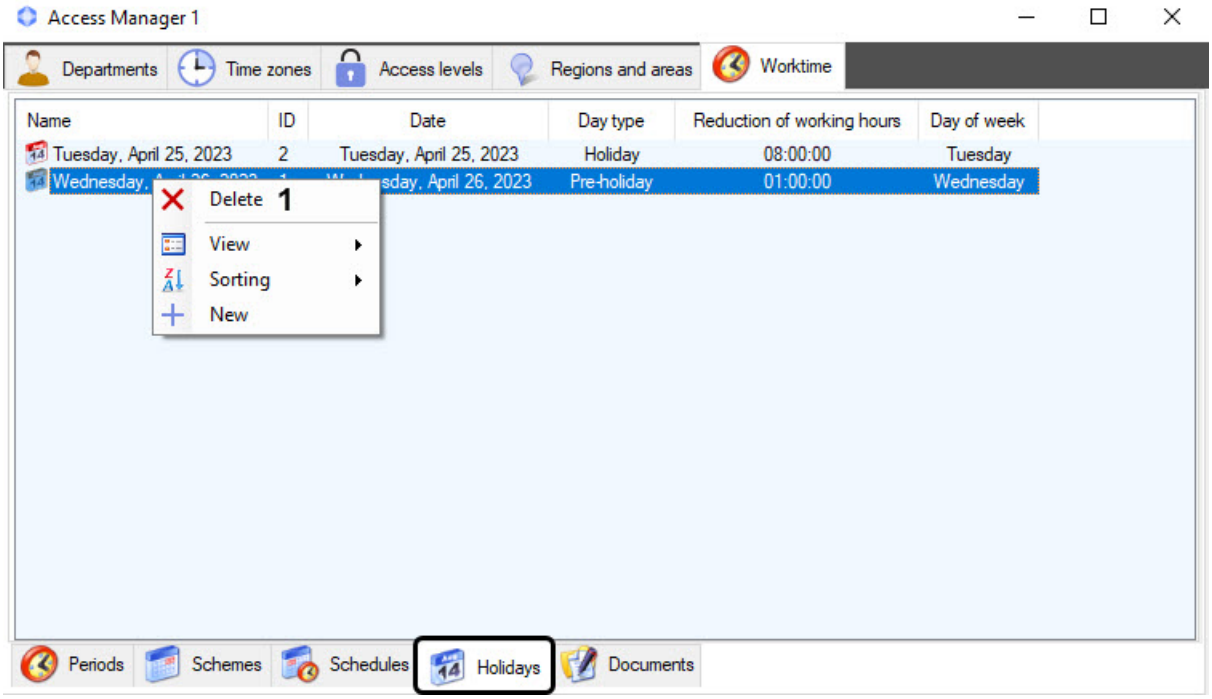
2. In the information field, double-click the holiday you want to change (**1**).

As a result, the window for editing a holiday will open.

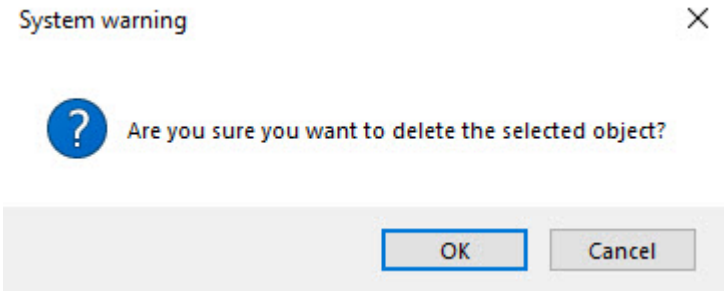
Deleting holidays

To delete a holiday saved in the system, do the following:

1. Go to the **Holidays** menu on the **Worktime** tab of the **Access Manager** interface window.



2. Right-click the holiday you want to delete to open the context menu.
3. Select **Delete** (**1**) in the context menu.
4. Click the **OK** button in the system warning message.



The holiday is deleted.

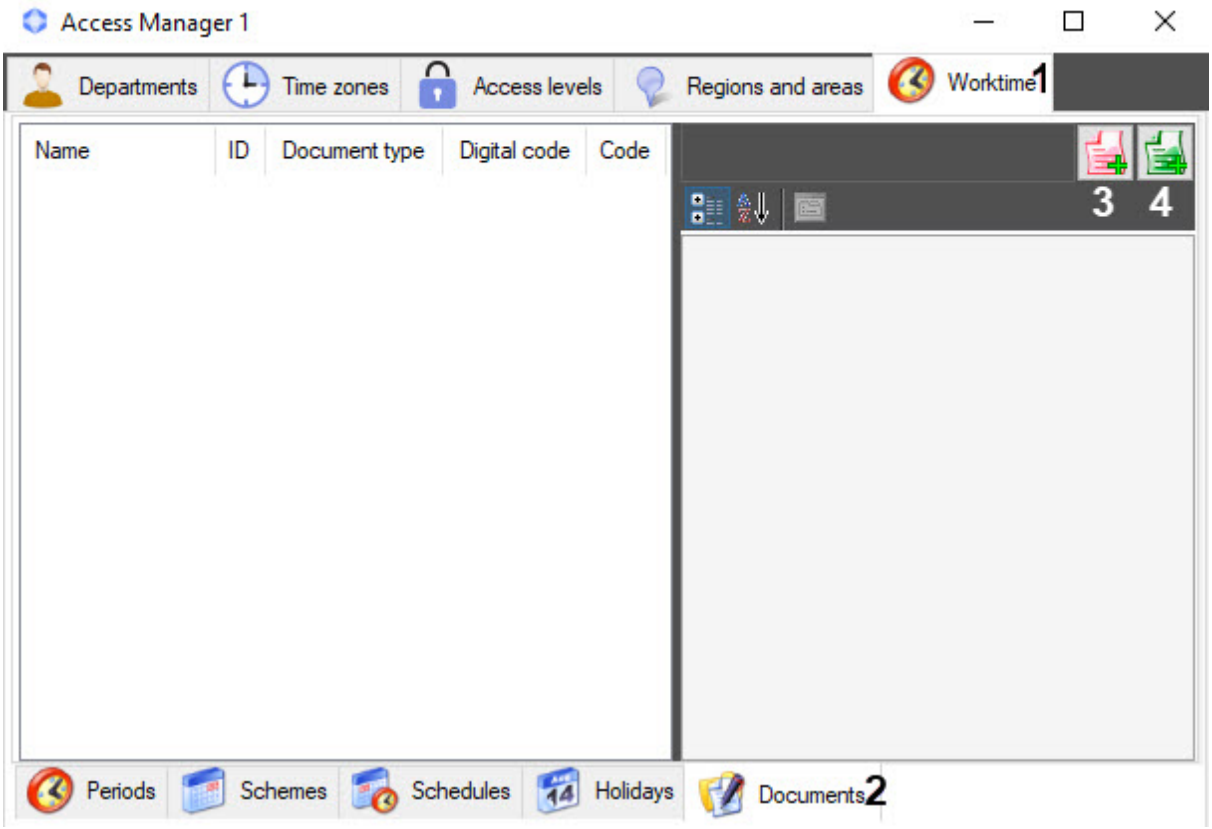
6.8.6 Documents

On the page:

You can create exculpatory and overtime documents in the *Time and Attendance* subsystem.

Creating documents

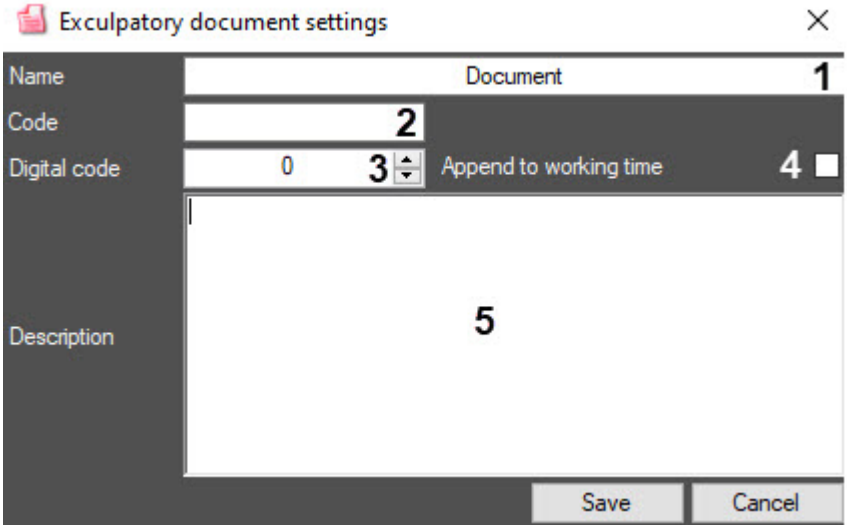
1. Go to the **Worktime** tab (**1**) of the **Access Manager** interface window (For more information about connecting the **Worktime** subsystem, see Configuring the Worktime subsystem).



2. Go to the **Documents** menu (**2**).
3. To create an exculpatory document, click the  button (**3**). To create an overtime document, click the  button (**4**).
   As a result, the window for editing a corresponding document will open.

Creating an exculpatory document

1. In the **Exculpatory document settings** window, in the **Name** field (**1**), enter the name of the document.

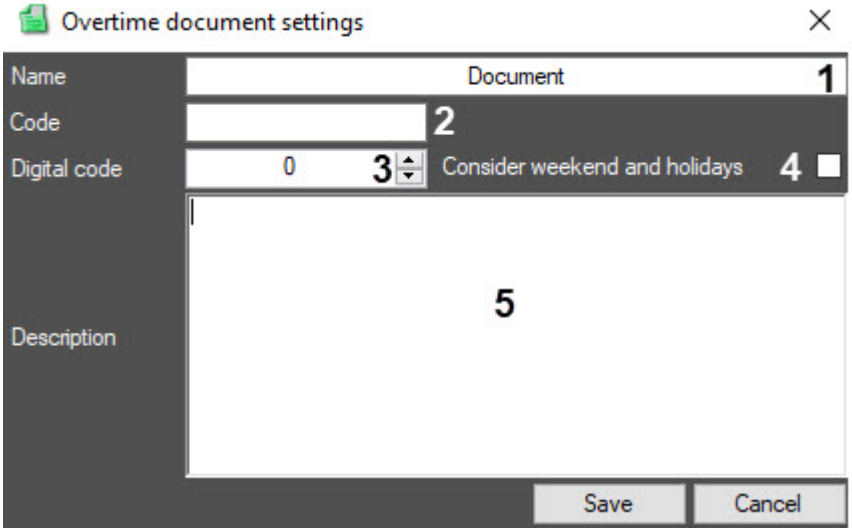


2. In the **Code** field (**2**), enter a letter code (or a second digital code) of the document.

3. In the **Digital code** field (**3**), enter a unique digital code of the document.
4. Set the **Append to working time** checkbox (**4**) to add the time of an employee absence from the workplace to the total working time.
5. In the **Description** field (**5**), add a comment to the document.
6. Click the **Save** button to save the exculpatory document.

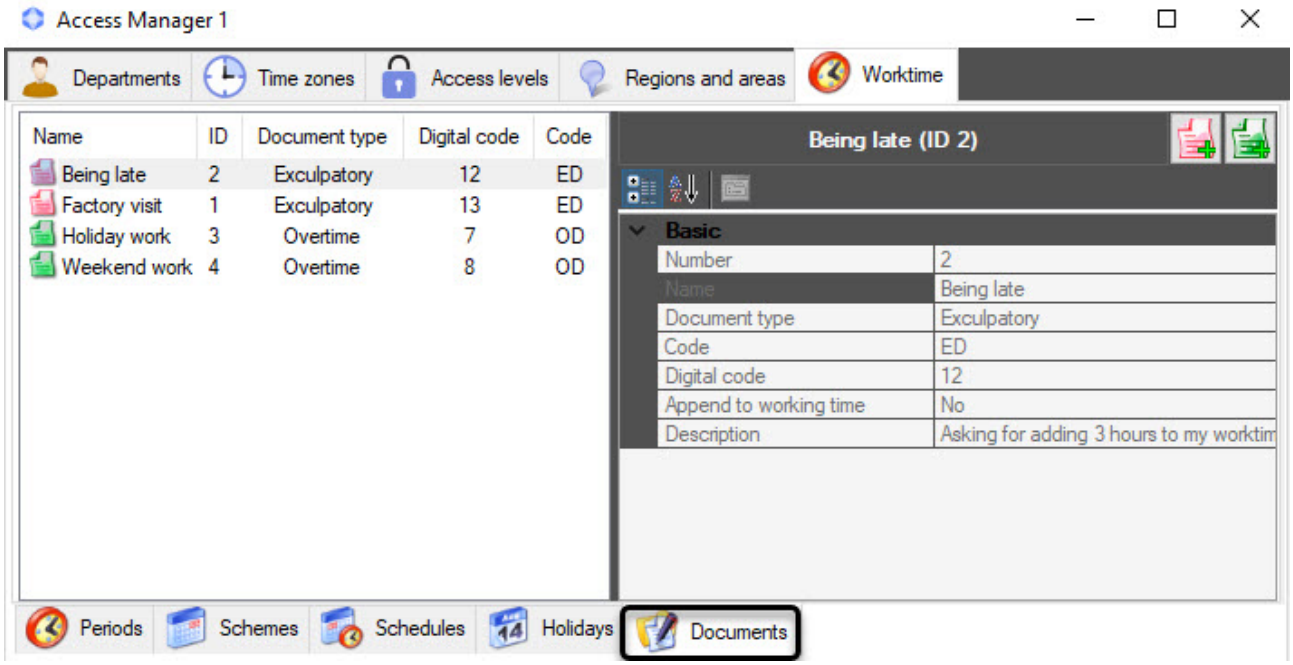
Creating an overtime document

1. In the **Overtime document settings** window, in the **Name** field (**1**), enter the name of the document.



2. In the **Code** field (**2**), enter a letter code (or a second digital code) of the document.
3. In the **Digital code** field (**3**), enter a unique digital code of the document.
4. Set the **Consider weekend and holidays** checkbox (**4**), so that when an employee works on weekend or holiday, this time is considered as working time.
5. In the **Description** field (**5**), add a comment to the document.
6. Click the **Save** button to save the overtime document.

After saving, the document will be displayed in the information field of the **Documents** menu on the **Worktime** tab of the **Access Manager** interface window.

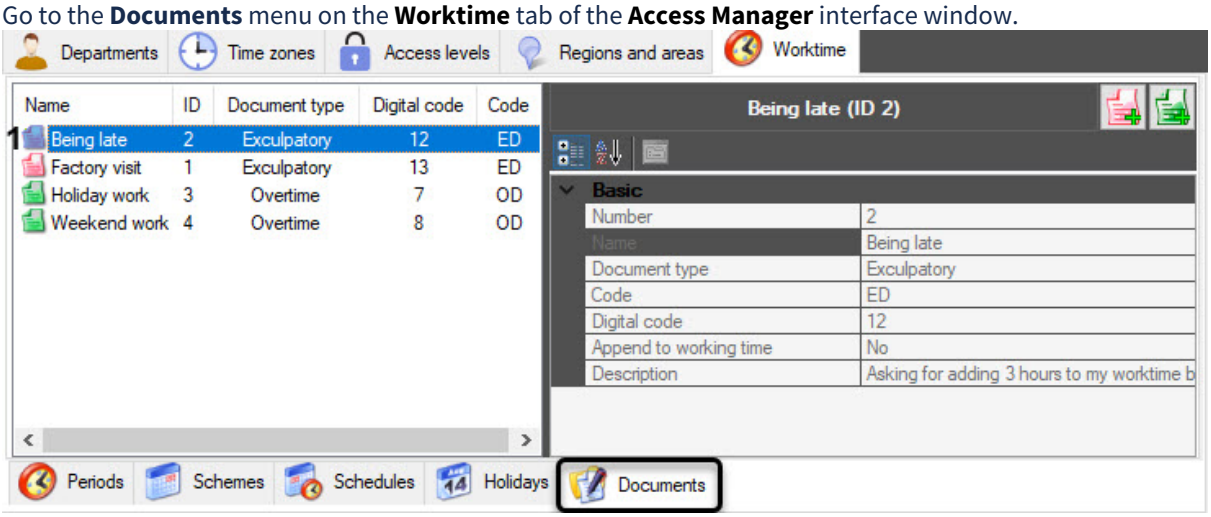


Creating documents is complete.

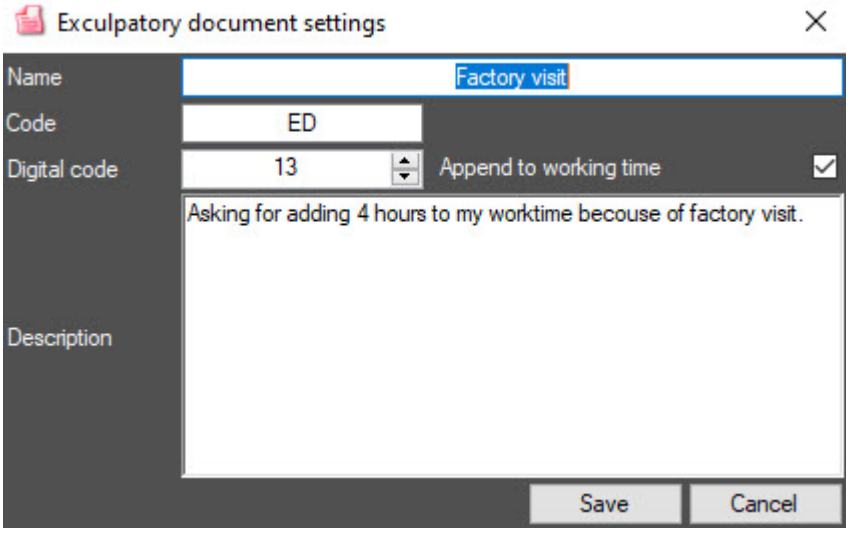
Editing documents

To edit an exculpatory and overtime document saved in the system, do the following:

1. Go to the **Documents** menu on the **Worktime** tab of the **Access Manager** interface window.



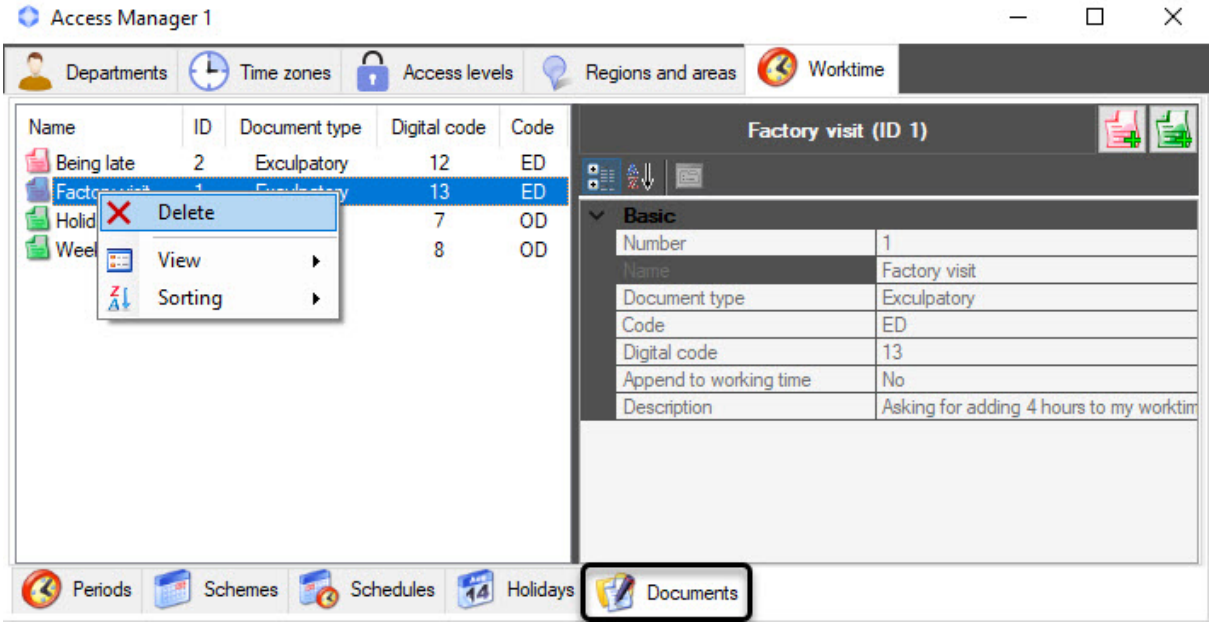
2. In the information field, double-click the document you want to change (**1**).
   As a result, the **Exculpatory document settings** window will open.



Deleting documents

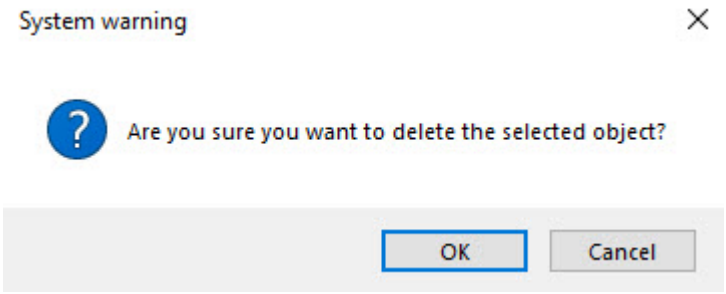
To delete an exculpatory and overtime document saved in the system, do the following:

1. Go to the **Documents** menu on the **Worktime** tab of the **Access Manager** interface window.



2. Right-click the document you want to delete to open the context menu.
3. Select **Delete** in the context menu.

4. Click the **OK** button in the system warning message.

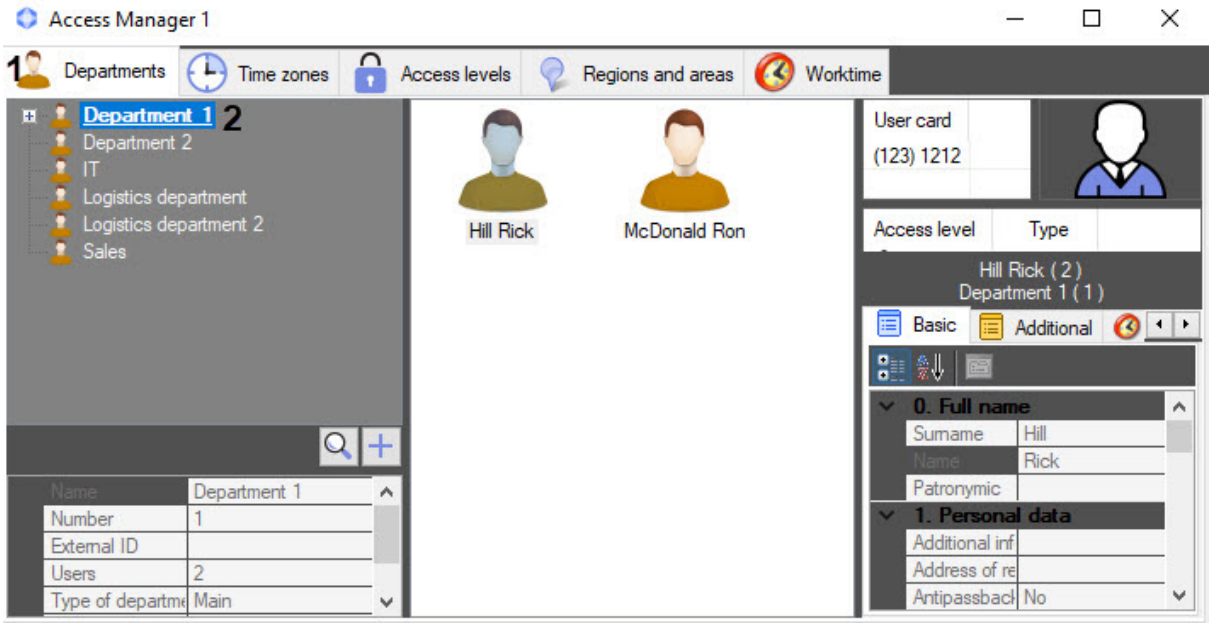


The document is deleted.

6.8.7 Assigning a work schedule to a department

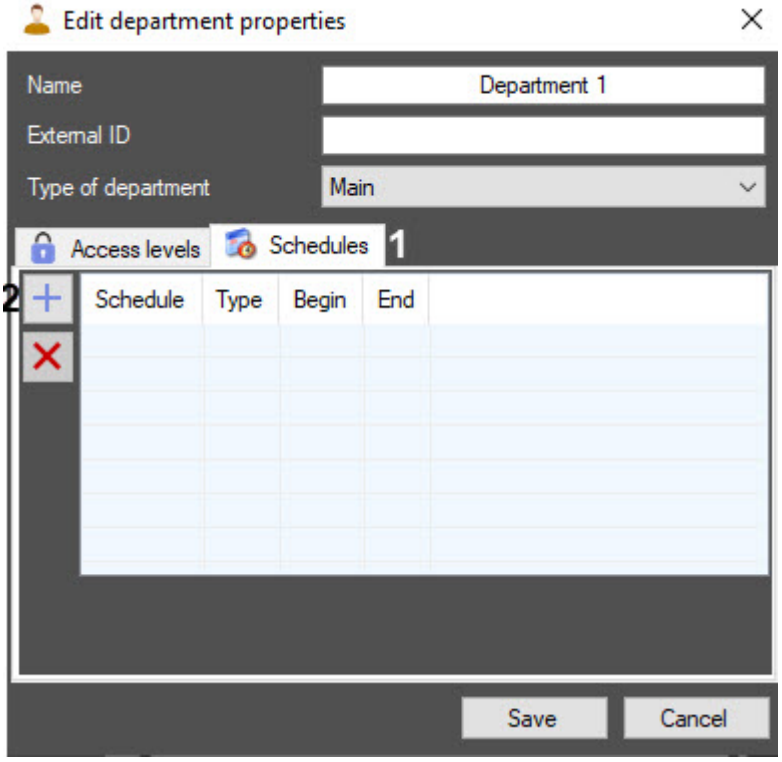
You can add a work schedule to a department in the *Time and Attendance* subsystem. To do this, do the following:

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

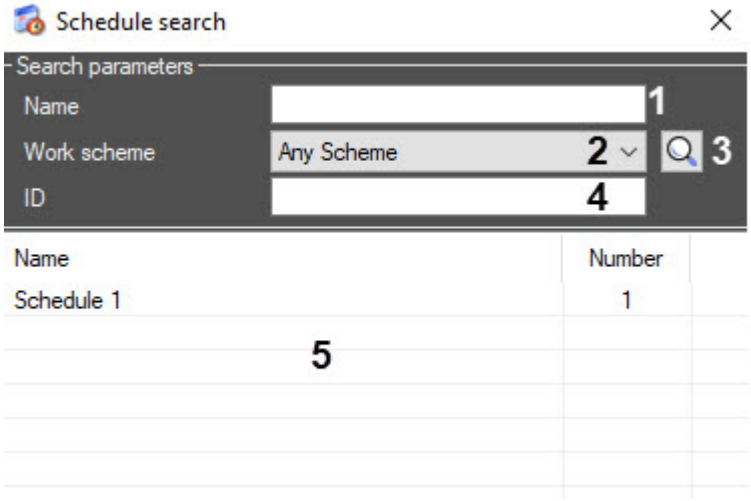


2. Double-click the required department (**2**) to open the **Edit department properties** window.

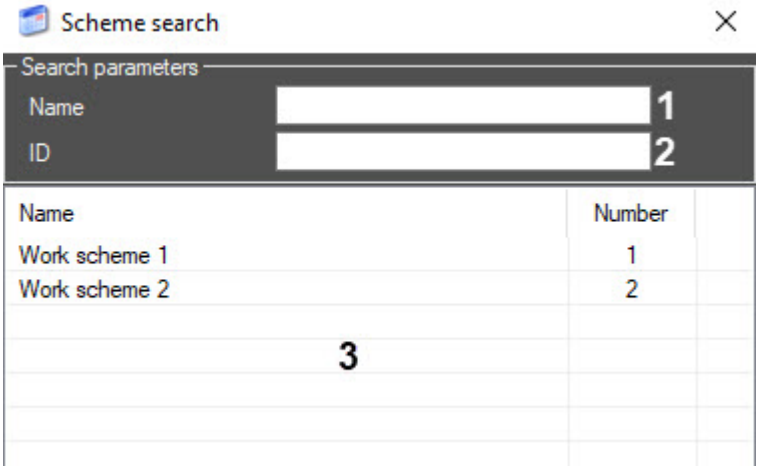
3. In the **Edit department properties** window, go to the **Schedules** tab (**1**).



4. To add a work schedule to a department, click the  button (**2**). As a result, the **Schedule search** window opens.

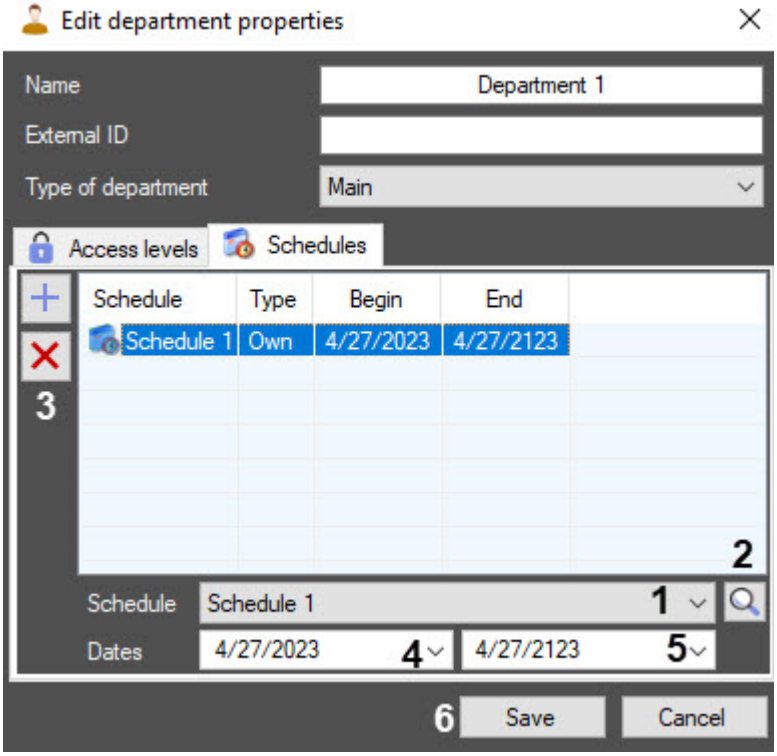


5. In the **Schedule search** window, double-click to select the required schedule in the area (**5**) or search by parameters:
   a. In the **Name** field (**1**), enter the work schedule name to search by it. The search starts with the first character.
   b. In the **ID** field (**4**), enter the work schedule ID to search by it.
   c. To search by the work scheme, in the **Work scheme** drop-down list (**2**), select the required work scheme or click the  button (**3**).
   As a result, the **Scheme search** window opens. Select the required scheme in the area (**3**) or search by parameters:



i. In the **Name** field (**1**), enter the work scheme name to search by it. The search starts with the first character.
ii. In the **ID** field (**2**), enter the work scheme ID to search by it.

6. In the **Edit department properties** window, from the **Schedule** drop-down list (**1**), select the required work schedule, or use the search button (**2**) to open the **Schedule search** window (see step 5).

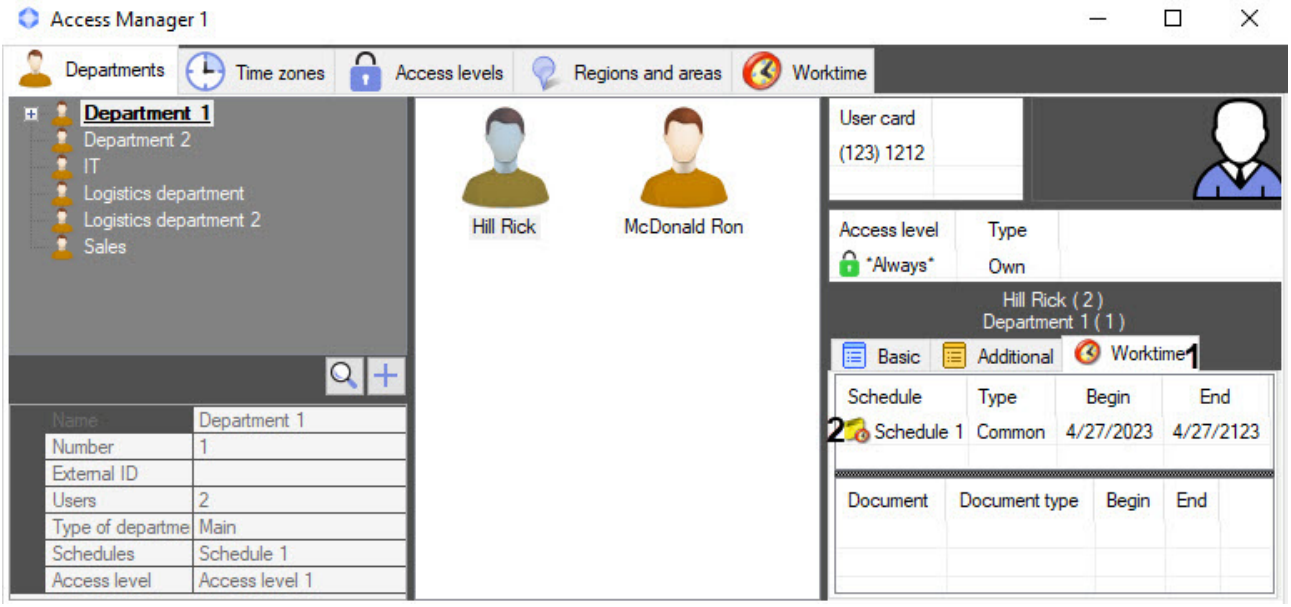


7. Open the calendar by clicking the button. Set the start date (**4**) and end date (**5**) of the work schedule. By default, the start date is the current date, and the end date is the current date plus 100 years.

> **Note**
>
> To delete a schedule, select it and click the button.

8. Click the **Save** button (**6**) to save the changes.

The work schedule for a department is added to the **Worktime** tab (**1**) of the properties panel of the departments to the schedule list (**2**).

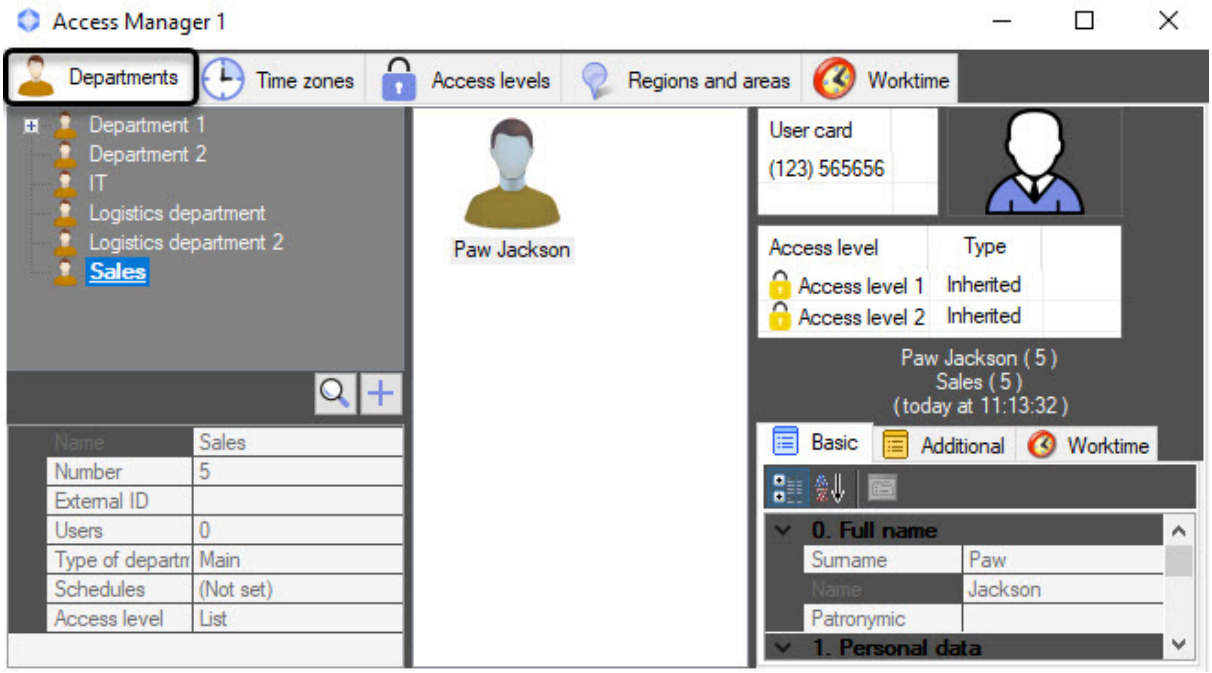


By default, the work schedule that is assigned to a department is inherited by all users who belong to it. For employees who belong to child departments, the work schedule must be set additionally (see Assigning a work schedule to a user).

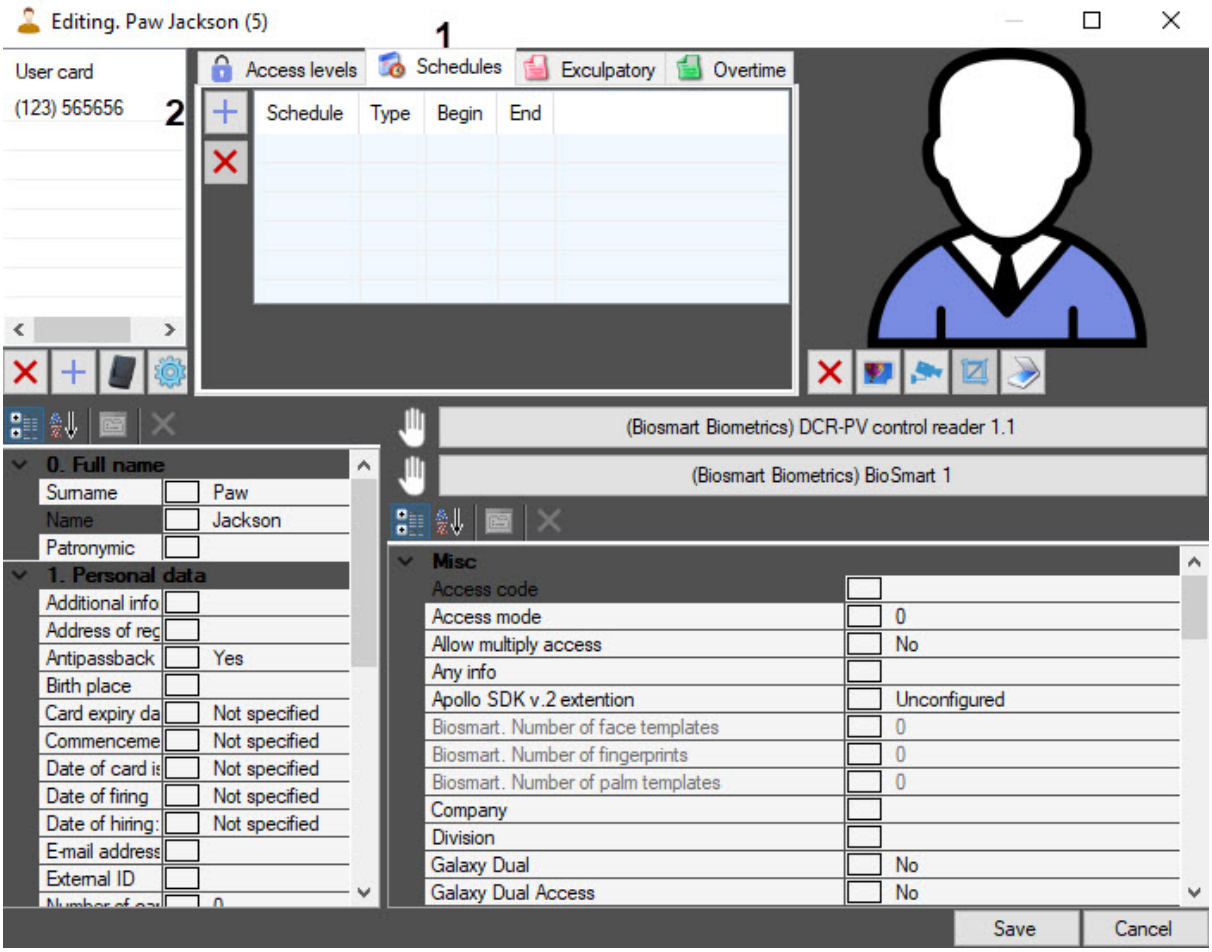
6.8.8 Assigning a work schedule to a user

The work schedule that is assigned to a department is inherited by all users who belong to it. For employees who belong to child departments, the work schedule must be set additionally. To do this, do the following:

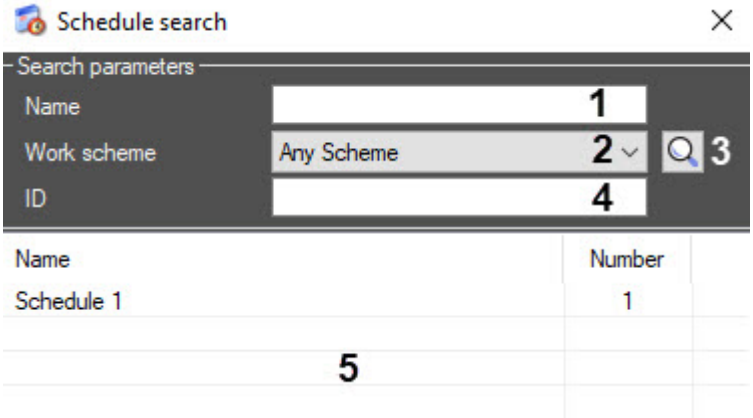
1. Go to the **Departments** tab of the **Access Manager** interface window.



2. Double-click the required user to open their editing window.

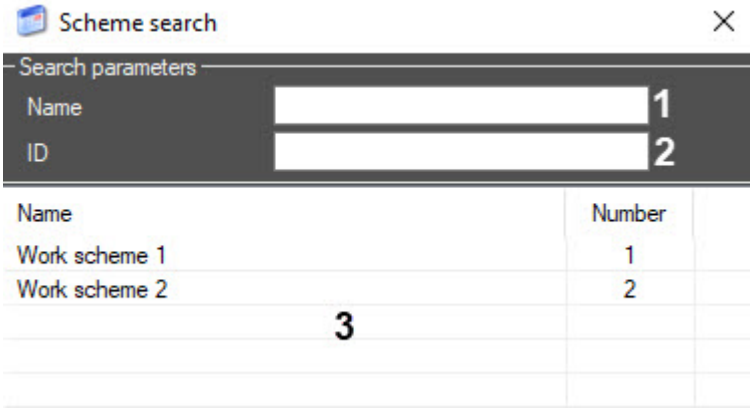


3. In the user editing window, go to the **Schedules** tab (**1**).
4. To add a work schedule, click the  button (**2**). As a result, the **Schedule search** window opens.



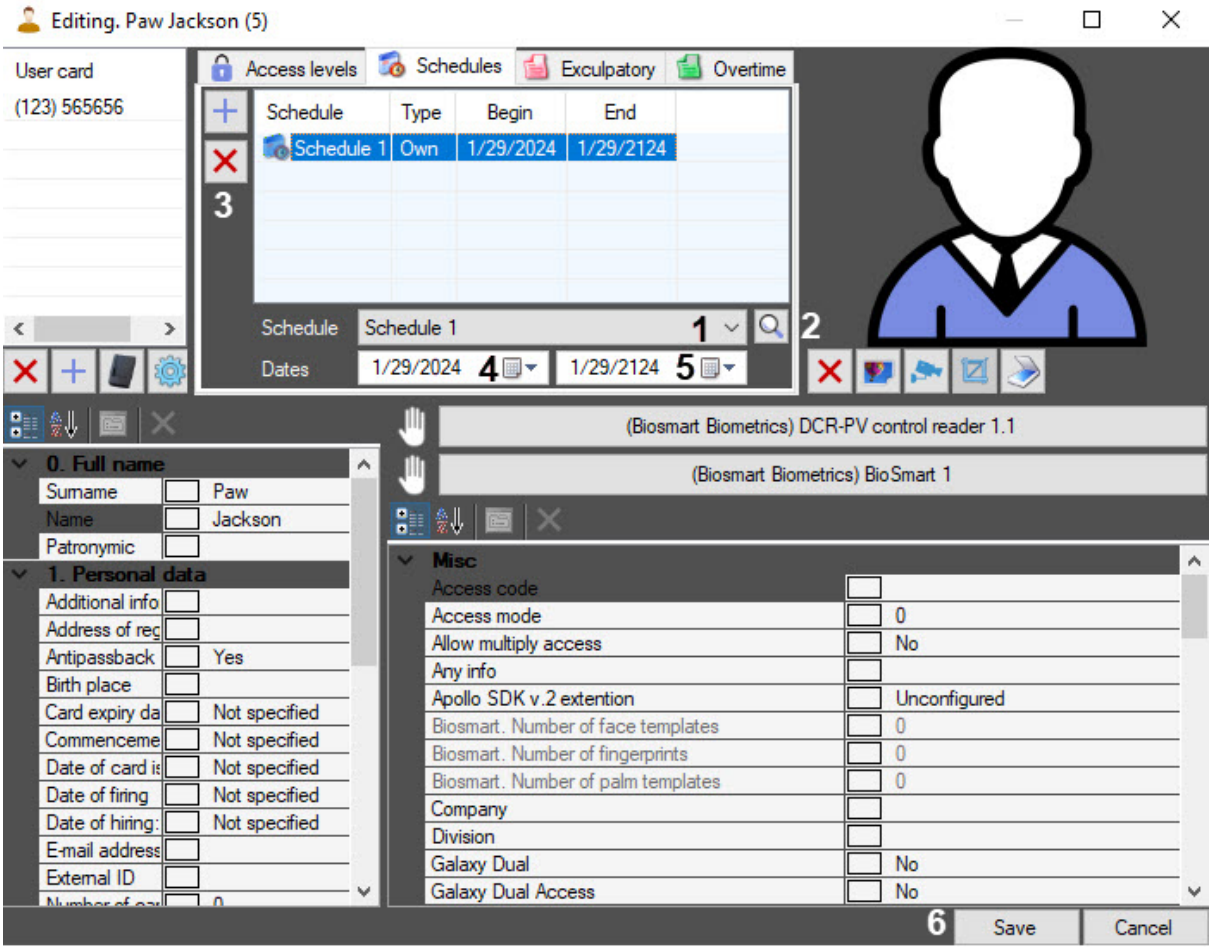
5. In the **Schedule search** window, double-click to select the required schedule in the area (**5**) or search by parameters:
   a. In the **Name** field (**1**), enter the work schedule name to search by it. The search starts with the first character.
   b. In the **ID** field (**4**), enter the work schedule ID to search by it.

c. To search by the work scheme, in the **Work scheme** drop-down list (**2**), select the required work scheme or click the button (**3**). As a result, the **Scheme search** window opens. Select the required scheme in the area (**3**) or search by parameters:



i. In the **Name** field (**1**), enter the work scheme name to search by it.
ii. In the **ID** field (**2**), enter the work scheme ID to search by it.

6. In the user editing window, from the **Schedule** drop-down list (**1**), select the work schedule, or click the button to open the **Schedule search** window (see steps 4-5).

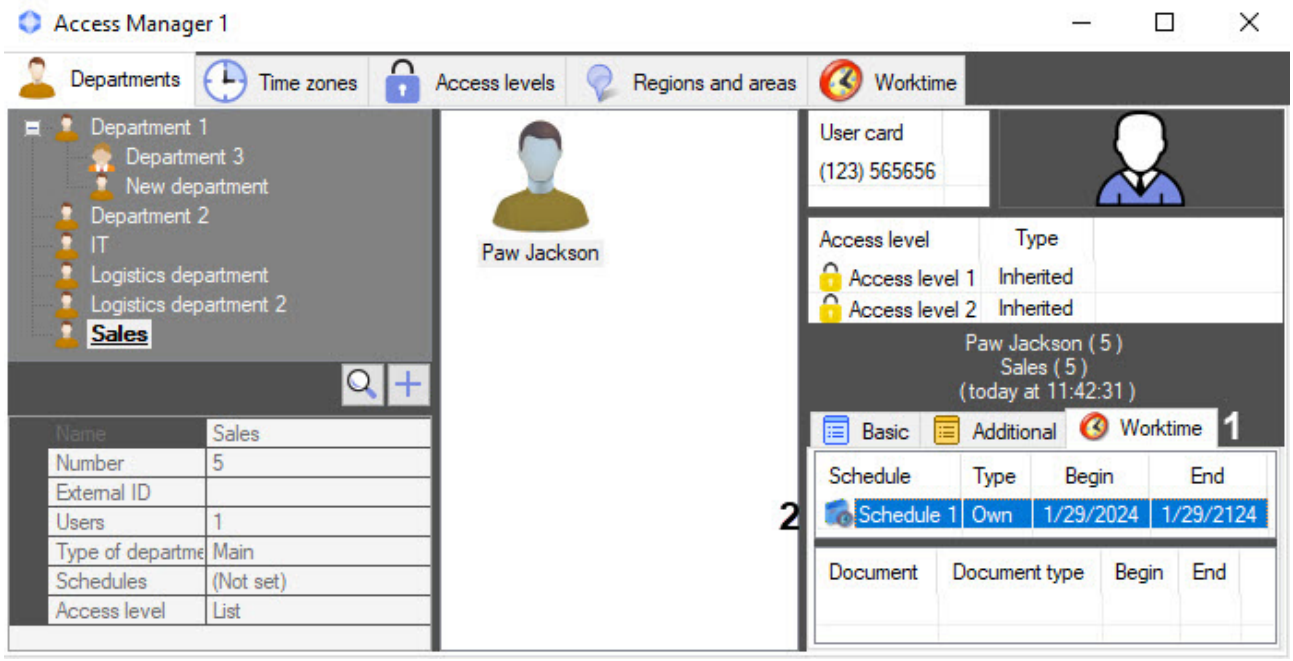


7. Open the calendar by clicking the button. Set the start date (**4**) and end date (**5**) of the work schedule. By default, the start date is the current date, and the end date is the current date plus 100 years.

> **Note**
>
> To delete a schedule, select it and click the button.

8. Click the **Save** button (**6**) to save the changes.

The work schedule for a user is added to the **Worktime** tab (**1**) of the properties panel of a user to the schedules list (**2**).

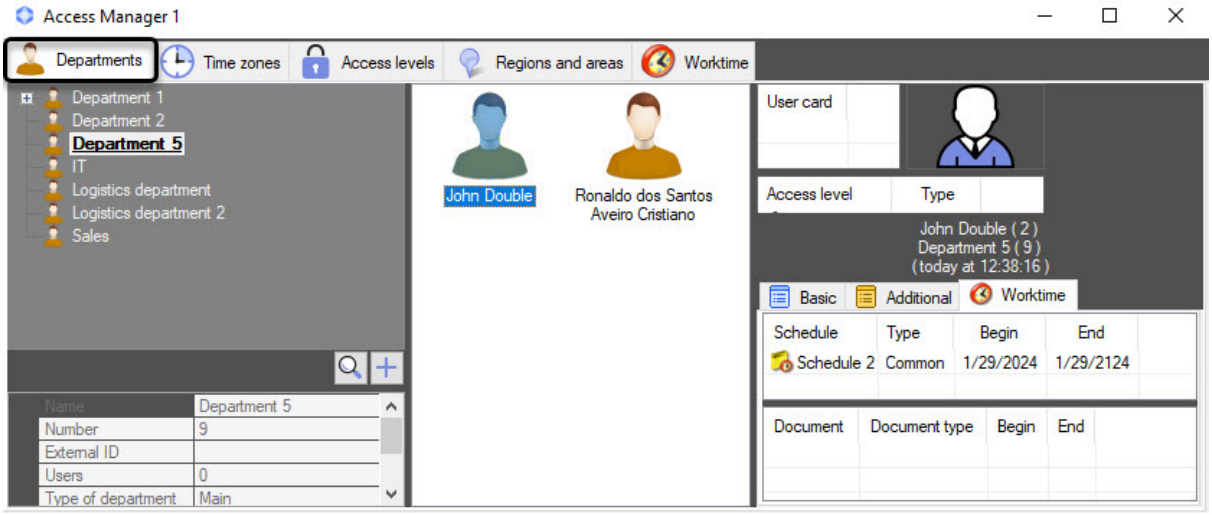


6.8.9 Assigning documents to a user

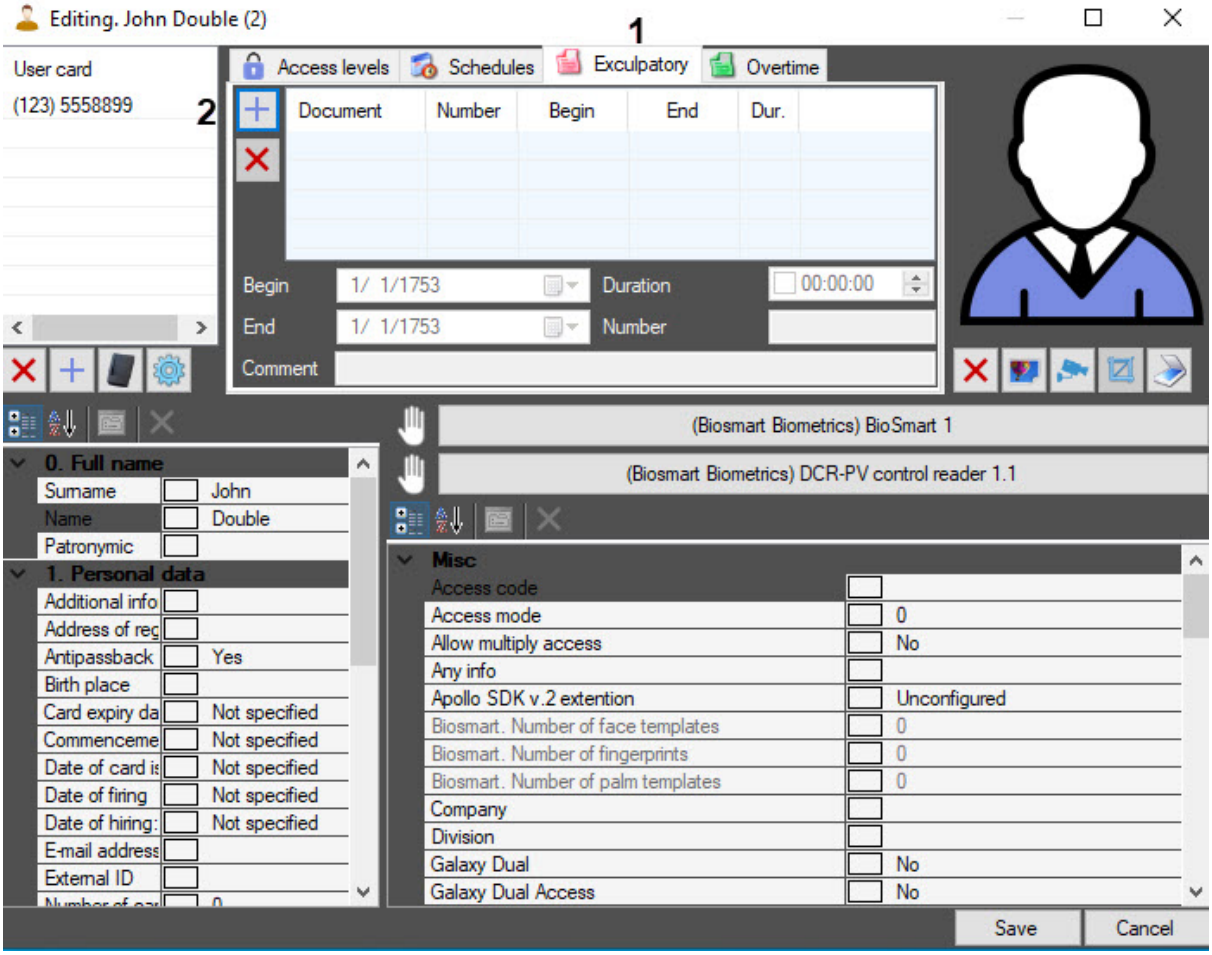
Assigning exculpatory documents to a user

In order for an exculpatory document to be taken into account in calculations and displayed in reports, it must be added to a user. To do this, do the following:

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

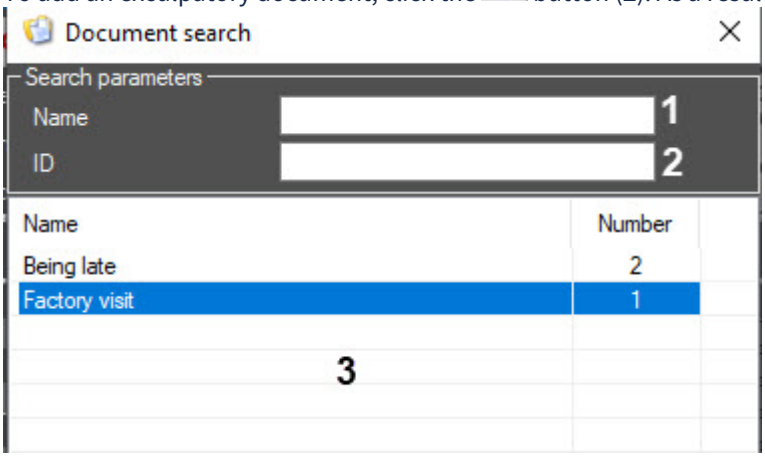


2. Double-click to open the editing window of the user to whom the document is added.

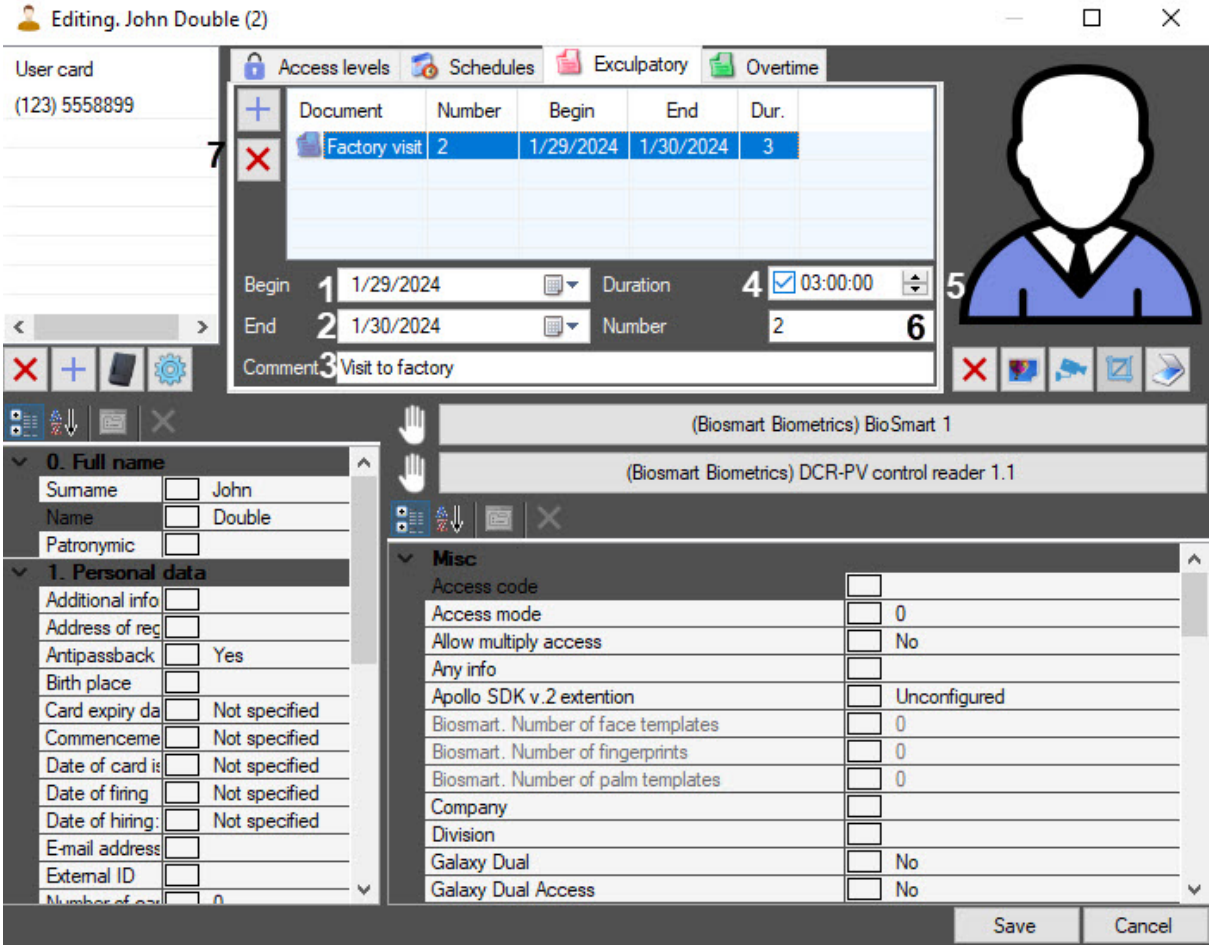


3. In the editing window, go to the **Exculpatory** tab (**1**).

4. To add an exculpatory document, click the + button (**2**). As a result, the **Document search** window opens.



5. Select the required document from the list in the area (**3**) or search by parameters:
   a. In the **Name** field (**1**), enter the document name to search by it. The search starts with the first character.
   b. In the **ID** field (**2**), enter the document ID to search by it.
6. For the added exculpatory document:

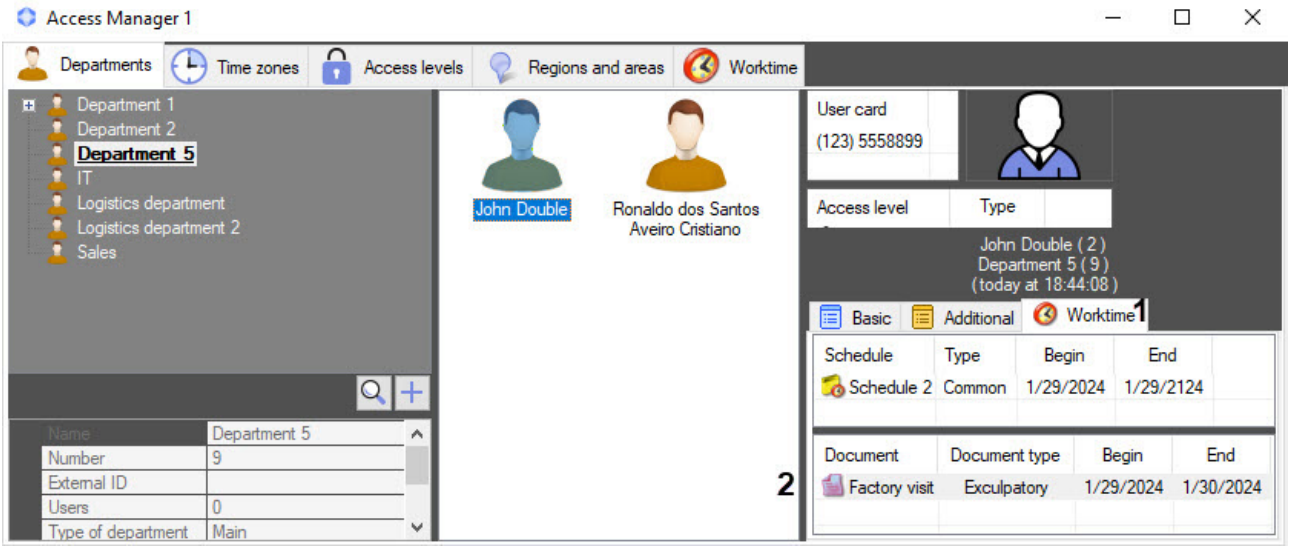


a. In the **Begin** (**1**) and **End** (**2**) fields, specify the begin date and end date of the exculpatory document, using the calendar that opens by clicking the button.
b. If necessary, in the **Comment** field (**3**), enter a comment.
c. Set the **Duration** checkbox (**4**) and specify the time interval in the HH:MM:SS format (**5**) so that this time is also counted as working time.
d. In the **Number** field (**6**), enter the ID of the document.

> **Note**
>
> To delete a document, click the button (**7**).

7. Click the **Save** button to save the changes.

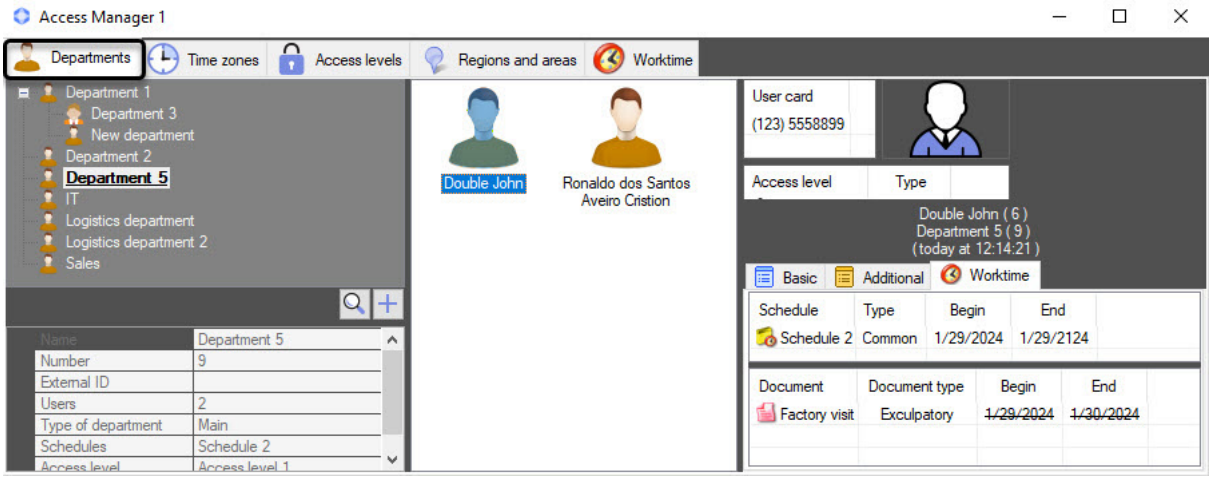
The user exculpatory document is added to the **Worktime** tab (**1**) of the user properties panel to the document list (**2**).



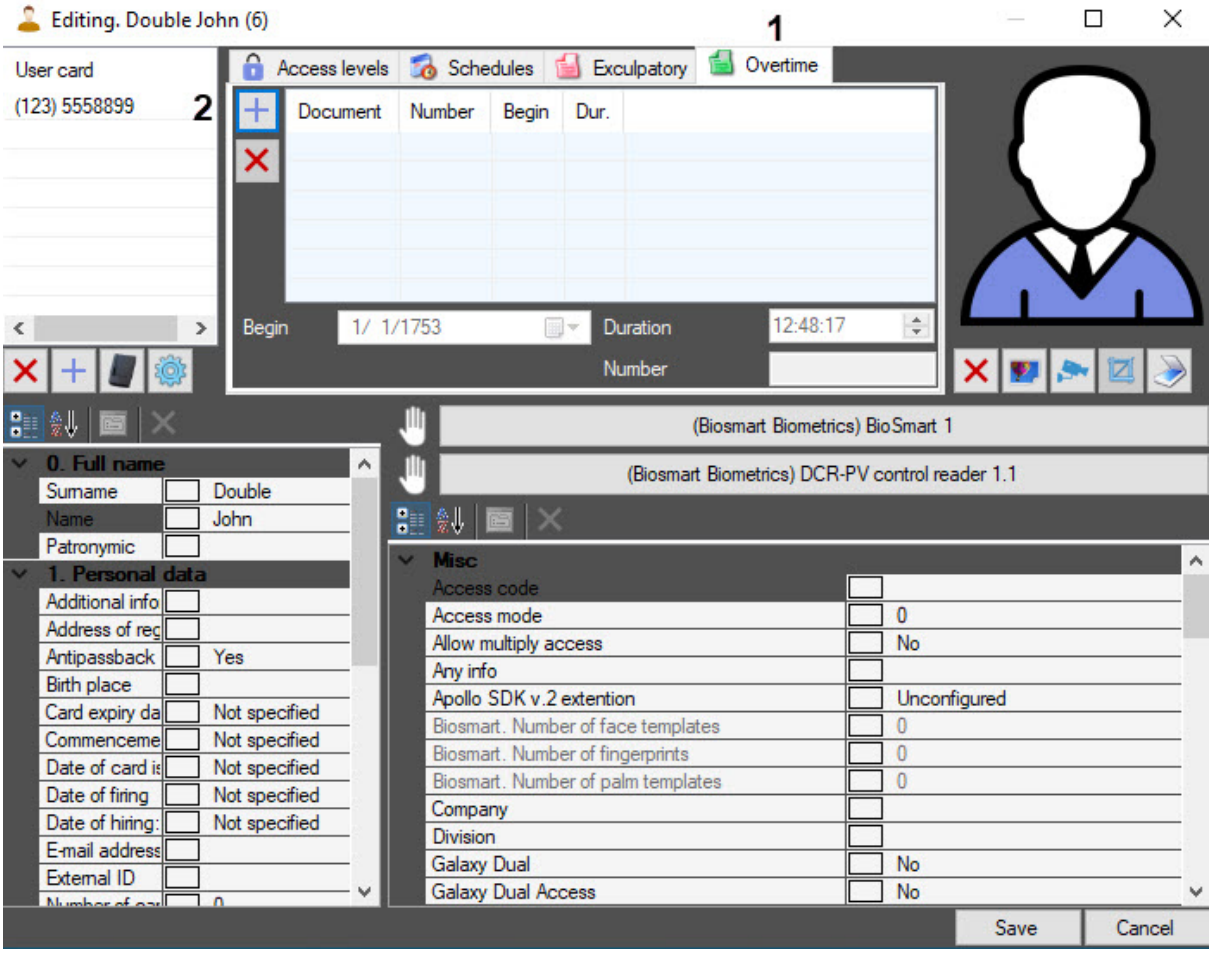
Assigning overtime documents to a user

In order for an overtime document to be taken into account in calculations and displayed in reports, it must be added to a user. To do this, do the following:

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

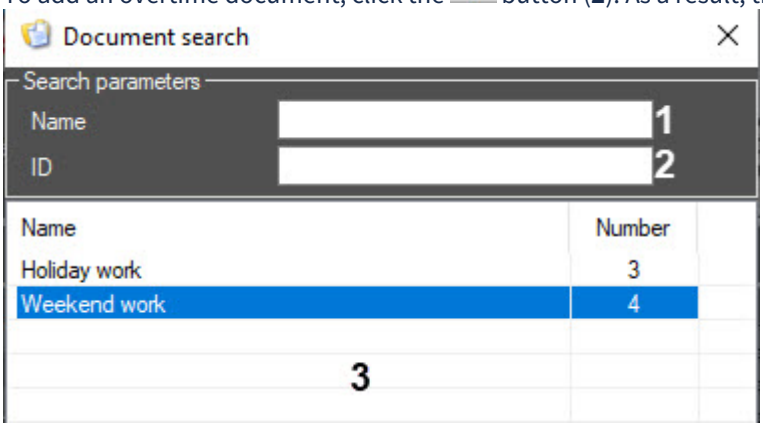


2. Double-click to open the editing window of the user to whom the document is added.

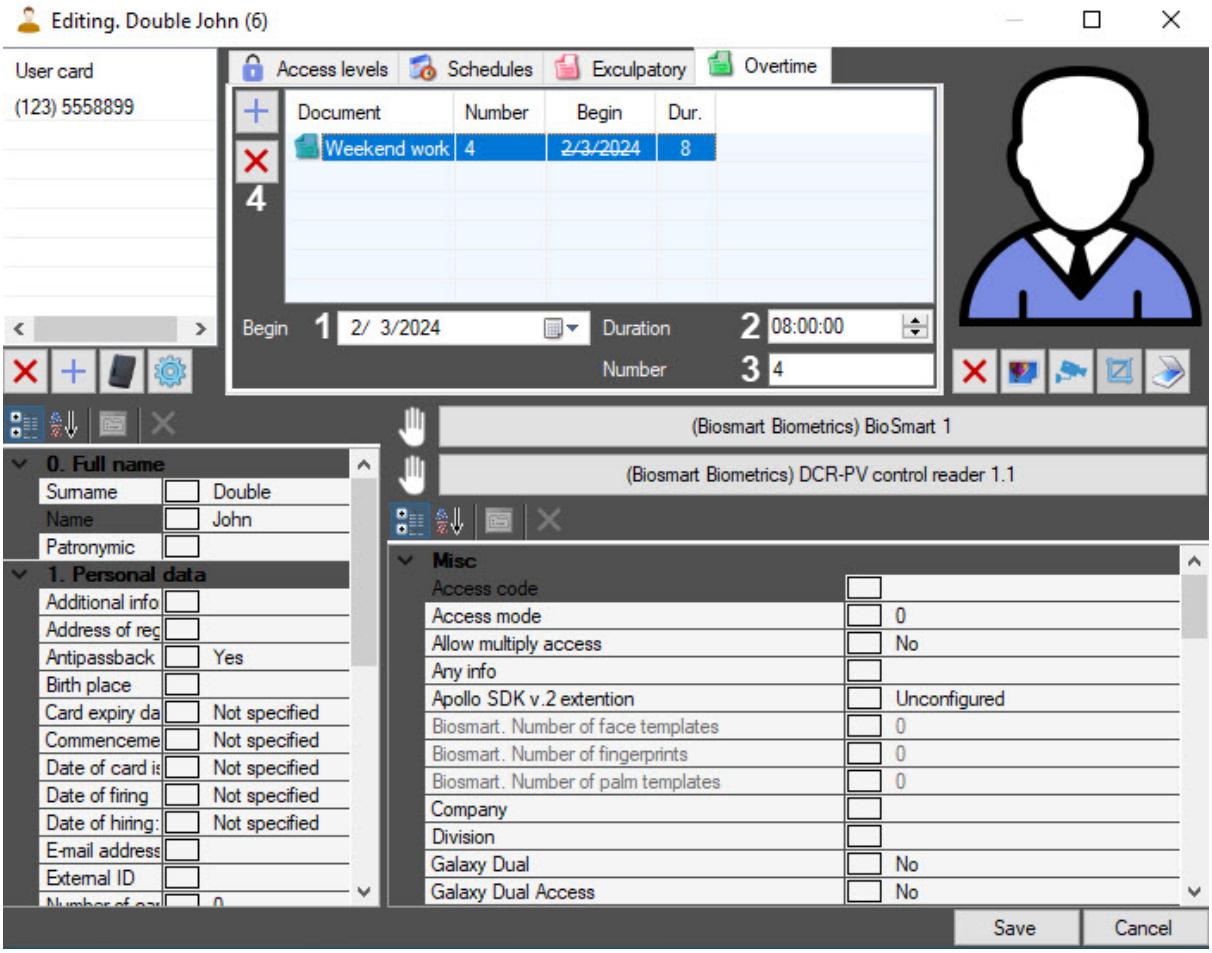


3. In the editing window, go to the **Overtime** tab (**1**).

4. To add an overtime document, click the + button (**2**). As a result, the **Document search** window opens.



5. Select the required document from the list in the area (**3**) or search by parameters:
   a. In the **Name** field (**1**), enter the document name to search by it. The search starts with the first character.
   b. In the **ID** field (**2**), enter the document ID to search by it.
6. For the added overtime document:



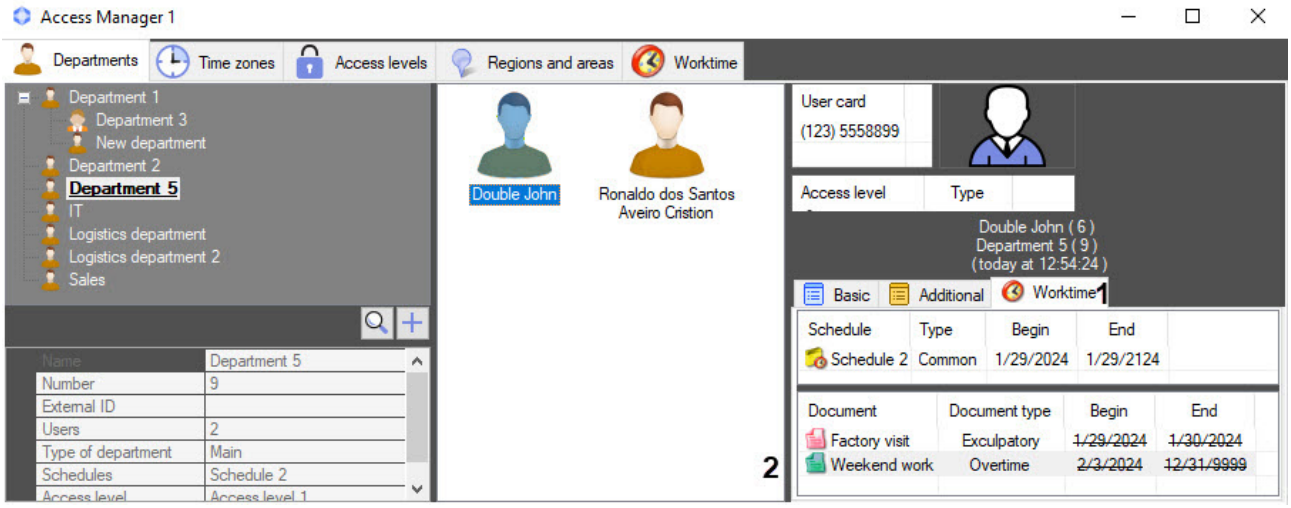
   a. In the **Begin** field (**1**), specify the begin date of the overtime document, using the calendar that opens by clicking the ⌄ button.

b. In the **Duration** field (**2**), specify the time interval in the HH:MM:SS format so that this time is also counted as working time.
c. In the **Number** field (**3**), enter the ID of the document.

> **Note**
>
> To delete a document, click the  button (**4**).

7. Click the **Save** button to save the changes.

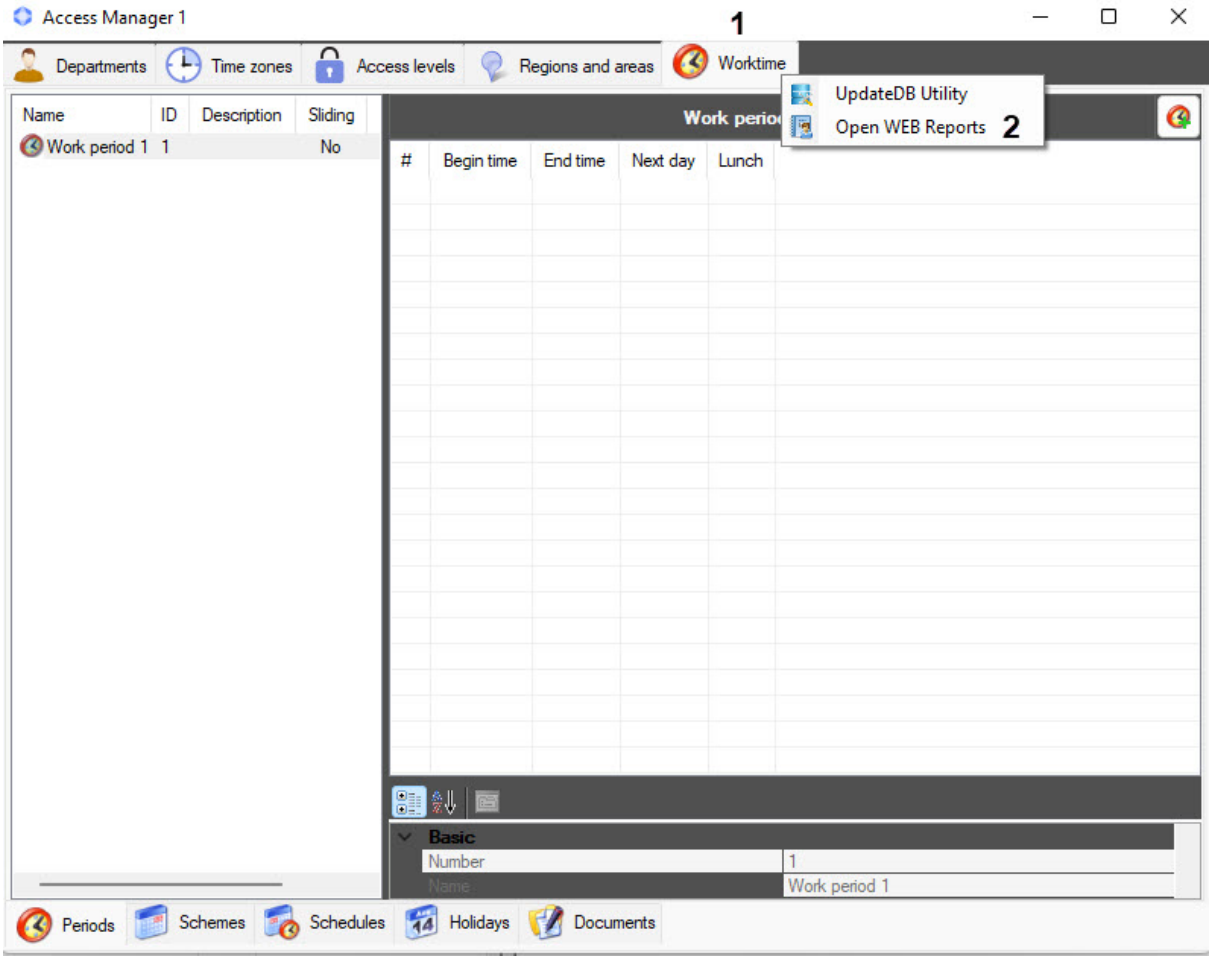
The user overtime document is added to the **Worktime** tab (**1**) of the user properties panel to the document list (**2**).



6.8.10 Working with the reports

In the *Worktime* subsystem, you can run the *WEB Report System* (if it is installed). For this, do the following:

1. Go to the **Worktime** tab (**1**).

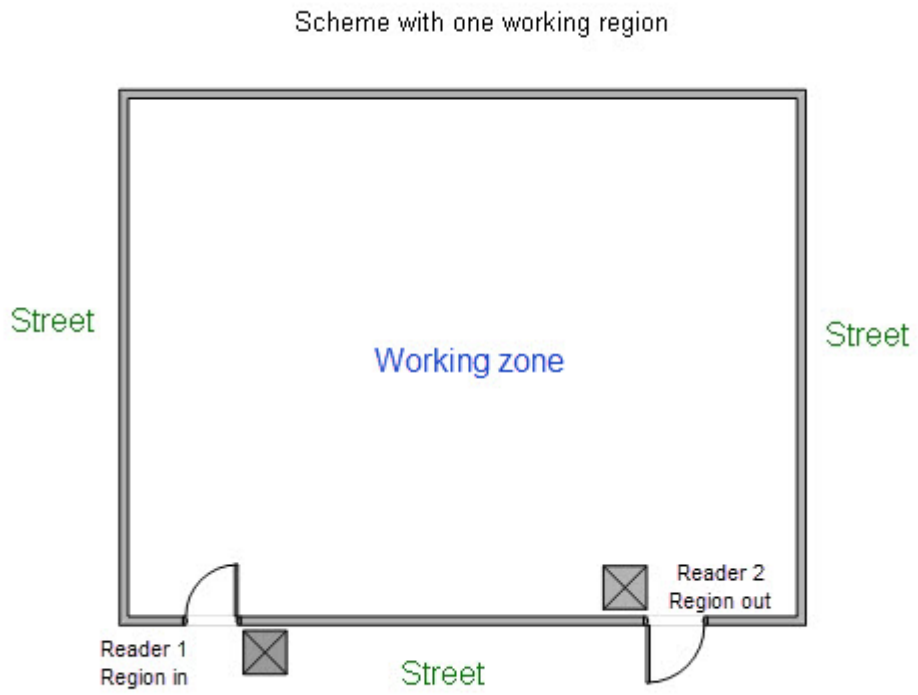


2. Right-click to open the context menu of the tab.
3. Select the **Open WEB Reports** menu item (**2**). For the information about configuring and working with the system, see WEB Report System PSIM. User Guide.
   As a result, you will go to the link specified in the **Report Server address** field when configuring the **Worktime support** object (see Configuring the Worktime subsystem).

> **Note**
>
> If many events are stored in the *ACFA PSIM* database, the performance of the *WEB Report System* may be low when generating the Worktime and general protocol reports. To improve the performance of the subsystem, it is recommended to use the **Remote Protocol Connector** utility (see Appendix 3. Working with the Remote Protocol Connector utility).

6.8.11 Appendix 1. Configuring Regions for the ACS Readers to work with the Time and Attendance subsystem

There is a scheme with one working region.



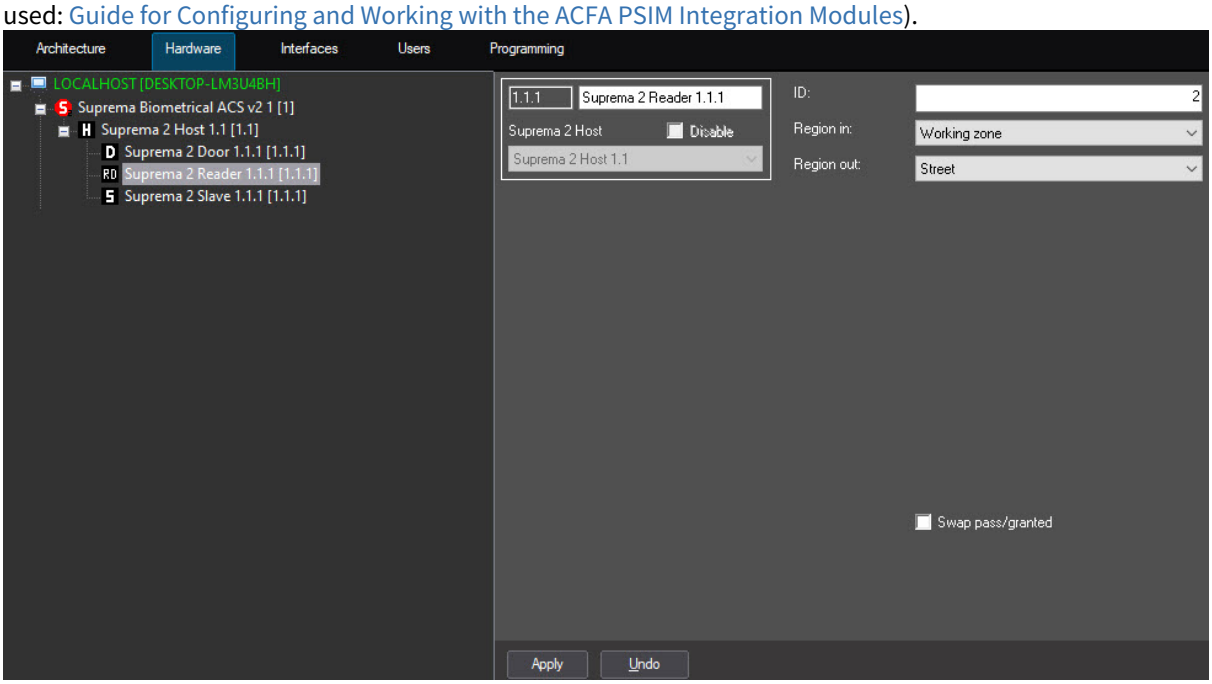
In this case, the following settings must be made in *ACFA PSIM*:

1. Create two **Region** objects corresponding to the working zone and street. The **Region** objects are created on the basis of the **Area** object on the **Programming** tab of the **System settings** dialog box. Let's call them Street and Working zone.

> **Note**
>
> You can also create regions using the *Access Manager* module (see Creating, editing and deleting Area and Region objects).

2. Configure the readers of the used ACS by specifying the created **Region** objects in the **Region in** and **Region out** fields in accordance with the installation place of the configured reader: at the entrance or exit of the room (for more information on assigning a region to readers, see the manual for the integration module

used: Guide for Configuring and Working with the ACFA PSIM Integration Modules).

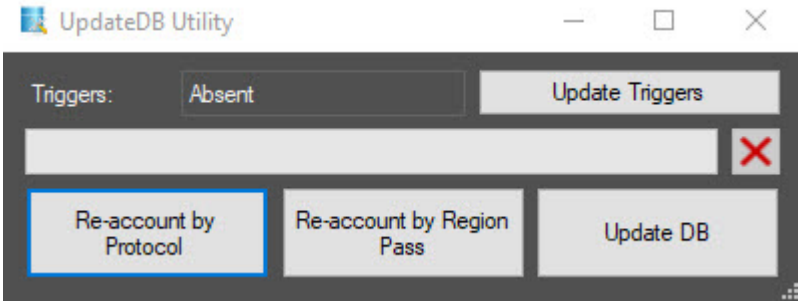


6.8.12 Appendix 2. The UpdateDB Utility

The UpdateDB Utility is used to update and re-account the *Axxon PSIM* database after the installation of the *Time and Attendance* subsystem that is a part of the *Access Manager* module. During the *Axxon PSIM* database update, using the UpdateDB Utility, the following operations are performed:

- the stored procedures and triggers are installed;
- the tables necessary for the correct operation of the *Time and Attendance* subsystem are created and updated.

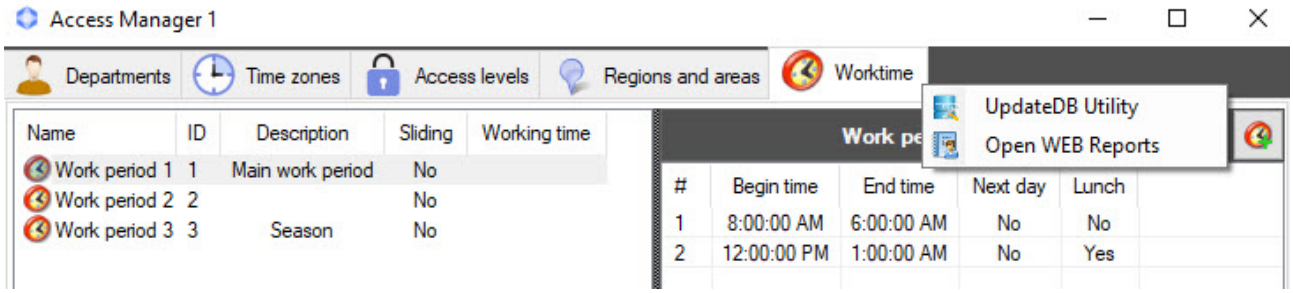
The UpdateDB Utility has the following interface:



Starting and working with the UpdateDB Utility

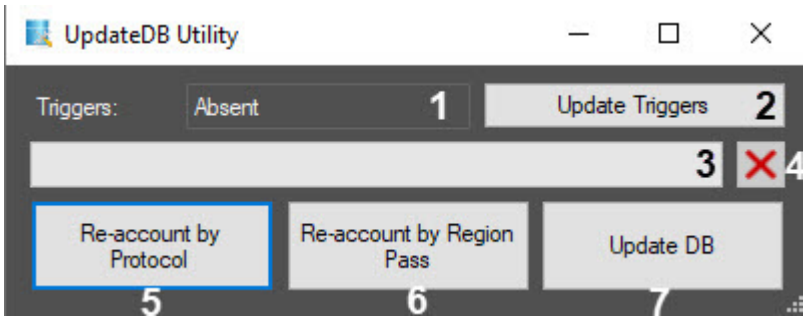
Starting the UpdateDB Utility

You can start the UpdateDB Utility by right-clicking the **Worktime** tab in the **Access Manager** interface window.



As a result, the **UpdateDB Utility** window will open.

Working with the UpdateDB Utility

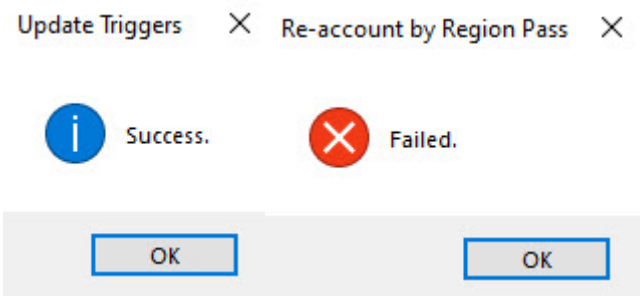


You can work with the UpdateDB Utility as follows:

1. The **Triggers** area (**1**) displays triggers. If necessary, for example, when upgrading to a newer version of *ACFA PSIM*, you must update the triggers by clicking the **Update Triggers** button (**2**). The progress is displayed in the area (**3**). To cancel the action, click the button (**4**).
2. To update the database, click the **Update DB** button (**7**). Both triggers and stored procedures, required for the correct operation of the subsystem, are updated. You need to do this once when connecting the *Time and Attendance* subsystem. The progress is displayed in the area (**3**). To cancel the action, click the button (**4**).
3. If it is necessary to take into account the passes made before configuring the *Time and Attendance* subsystem, after starting the *Time and Attendance* subsystem in *Axxon PSIM*, re-account the database using the **Re-account by Protocol** (**5**) and **Re-account by Region Pass** (**6**) buttons. The progress is displayed in the area (**3**). To cancel the action, click the button (**4**).

> **Attention!**
>
> It is strongly not recommended to use the re-account buttons without recommendations of AxxonSoft technical support specialists!
> When you click the **Re-account by Protocol** button (**5**), the dbo.Region_Enter_Exit table is completely cleared and filled out again depending on the pass information currently contained in the dbo.protocol table.
> When you click the **Re-account by Region Pass** button (**6**), the dbo.Region_Enter_Exit table is completely cleared and filled out again depending on the pass information currently contained in the dbo.Region_pass table.
> **Attention!** Because of the different depth of the event archive of these tables, there is a risk of data loss when clearing the dbo.Region_Enter_Exit table.

If the update (re-account) succeeds or fails, the corresponding message appears: about success in the first case and failure in the second case.



Note

If the reaccounting is completed with an error, we recommend increasing the time for waiting for the system response by changing the value of the **RecalcTimeoutInSec** parameter in the account_manager_run.config file. The default value is **600** seconds.

4. Click the **OK** button in the message window.
5. To close the **UpdateDB Utility** window, click the button in the top right corner of the form.

Working with the UpdateDB Utility is complete.

Note

By default, only the passes that were made after the installation and configuration of the *Time and Attendance* subsystem are taken into account.

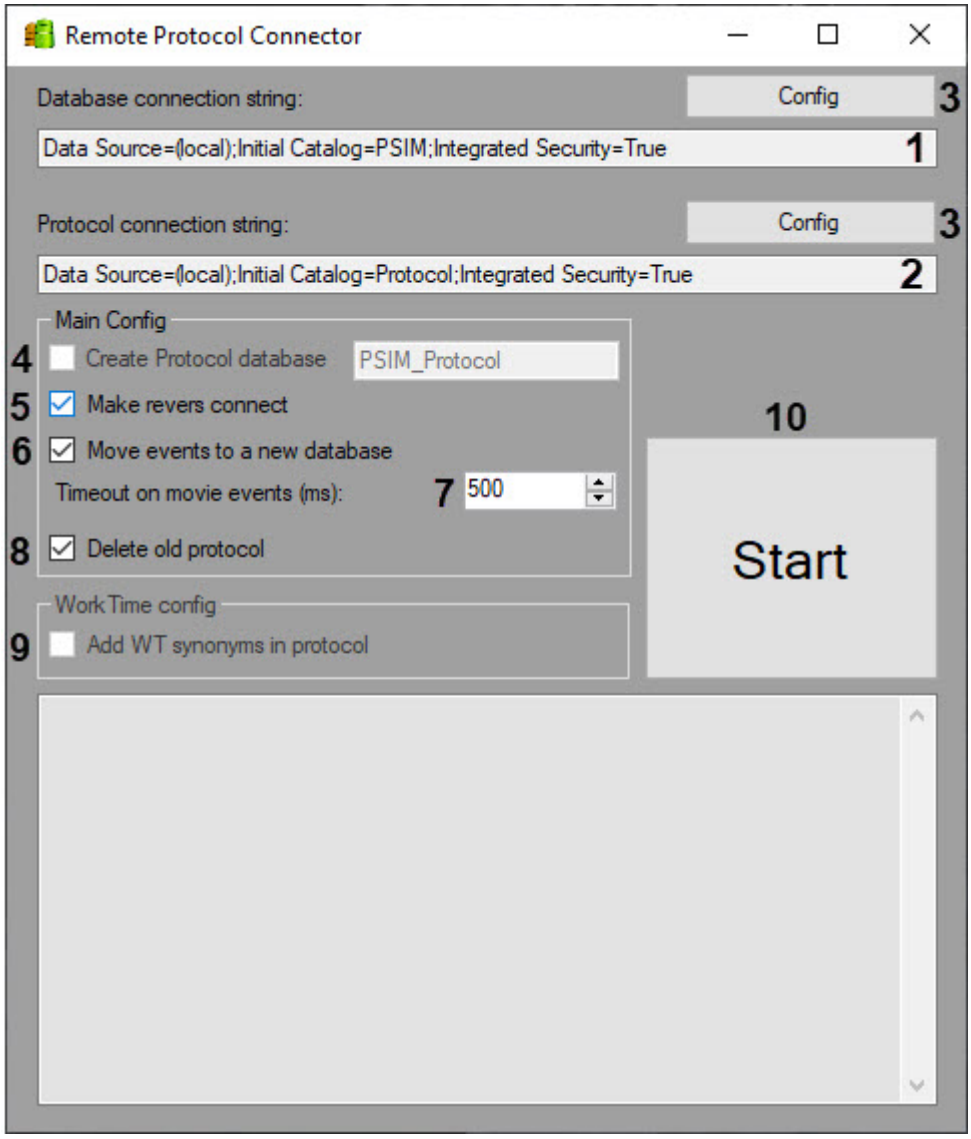
6.8.13 Appendix 3. Working with the Remote Protocol Connector utility

The **Remote Protocol Connector** utility is used to improve the system performance by optimizing the work with the database when generating general and Worktime reports by event protocol, both in the *Time and Attendance* subsystem and in the Axxon PSIM WEB Report System.

The utility enables the following actions:

1. Migrate the events protocol into a separate database.
2. Create a protocol database.
3. Transfer data from the old protocol table to a new one in a separate database.
4. Delete the old protocol table.
5. Create synonyms for a new protocol database, which will enable the work of the *Time and Attendance* subsystem.

The utility is located in the /Axxon PSIM/ Tools folder.

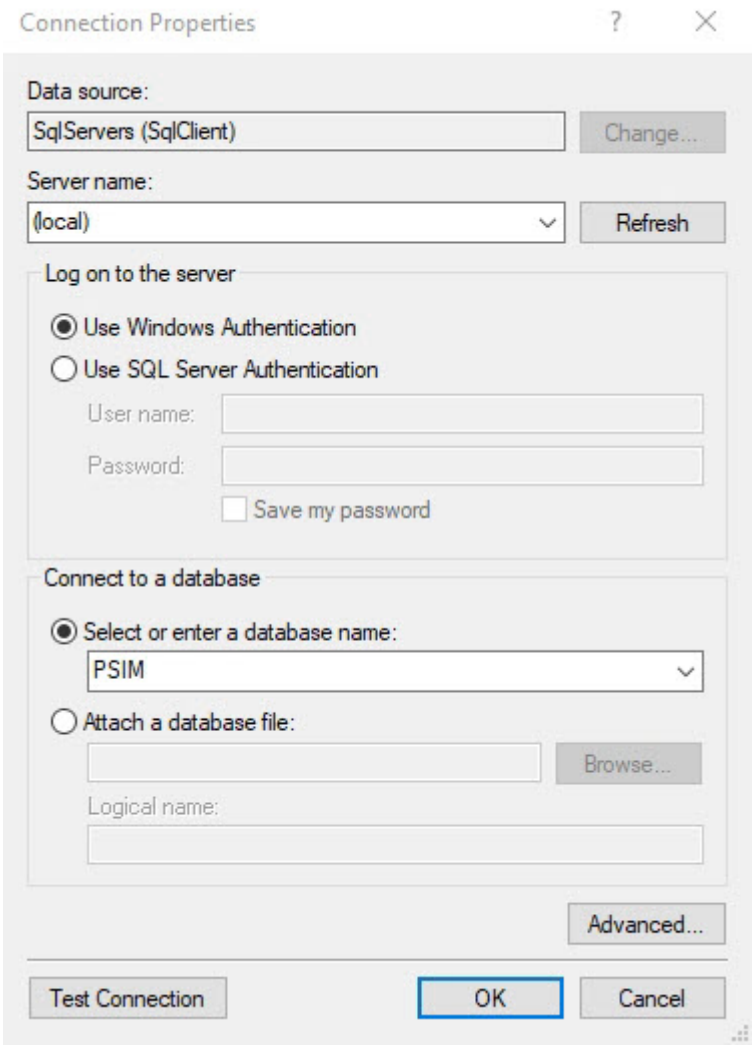


Attention!

Before starting to work with the utility, *Axxon PSIM* must be shut down.

To work with the utility, do the following:

1. In the **Database connection string** field (**1**), specify the path to the *Axxon PSIM* database.
2. In the **Protocol connection string** field (**2**), specify the path to the events protocol table.
   The **Config** button (**3**) for both fields enables automatic generation of connection strings to the database and to the protocol table. When you click the button, the connection settings window opens, where you can select the server name and the name of the database or table.



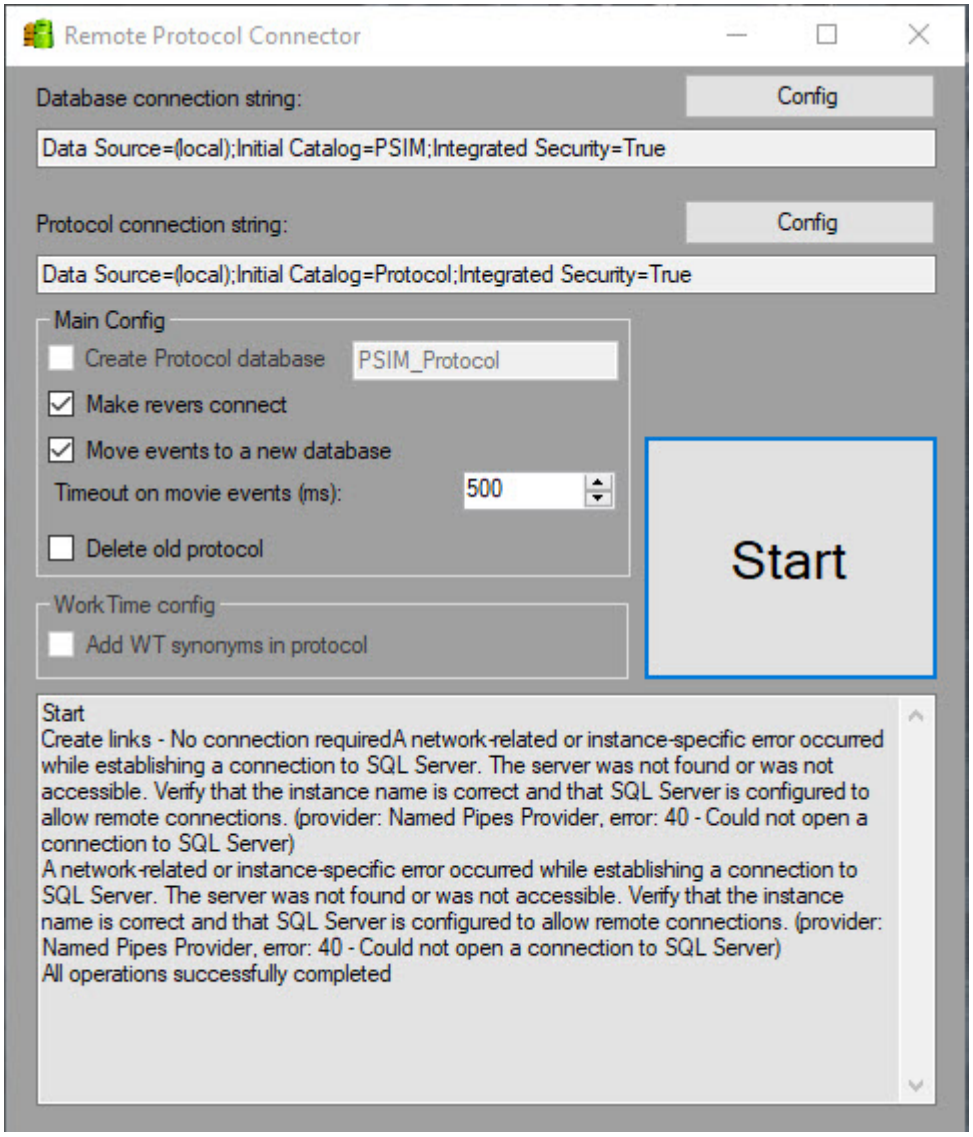
3. Set the **Create Protocol database** checkbox (**4**) if you want to create a separate database for the events protocol. By default, the name of the database is *PSIM_Protocol*, however, it can be changed.
4. Set the **Make revers connect** checkbox (**5**) if you want to keep the old event protocol table, but associate it with the new database that will be created by the utility.
5. Set the **Move events to a new database** checkbox (**6**) if you want to migrate all entries from the old event protocol table to the new database.
6. In the **Timeout on movie events (ms)** (**7**), specify the timeout for transferring entries in milliseconds (if the event transfer setting is enabled).
7. Set the **Delete old protocol** checkbox (**8**) if you do not want to save the old event table.

   Note

   It is recommended to migrate the events to a new database beforehand.

8. Set the **Add WT synonyms in protocol** checkbox (**9**) if you want to transfer the links of the old event protocol table to the other *Time and Attendance* tables to the new database.
9. Click the **Start** button (**10**) to run the utility.

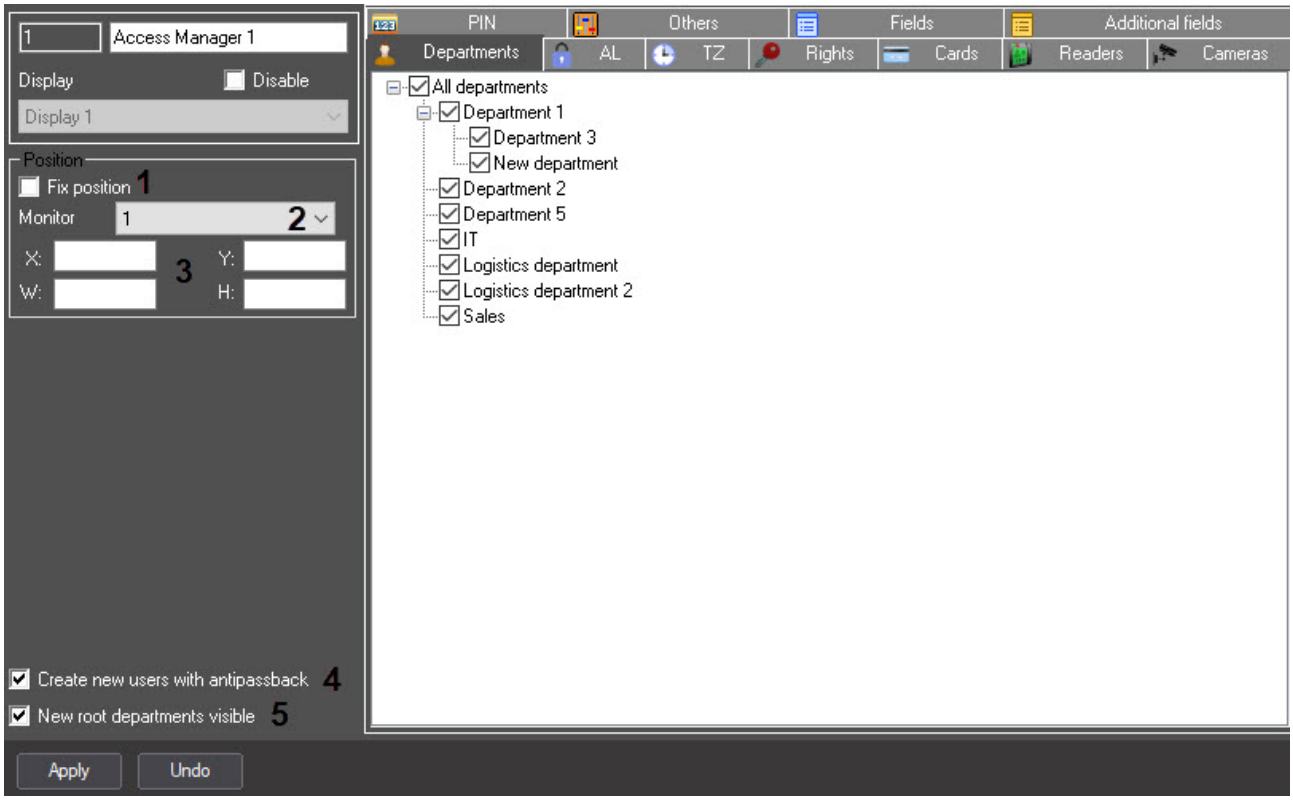
The migration progress and possible errors will be displayed in the field below the settings panel.


Remote Protocol Connector
Database connection string:
Config
Data Source=(local);Initial Catalog=PSIM;Integrated Security=True
Protocol connection string:
Config
Data Source=(local);Initial Catalog=Protocol;Integrated Security=True
Main Config
Create Protocol database
PSIM_Protocol
Make revers connect
Move events to a new database
Timeout on movie events (ms):
500
Delete old protocol
Start
Work Time config
Add WT synonyms in protocol
Start
Create links - No connection requiredA network-related or instance-specific error occurred while establishing a connection to SQL Server. The server was not found or was not accessible. Verify that the instance name is correct and that SQL Server is configured to allow remote connections. (provider: Named Pipes Provider, error: 40 - Could not open a connection to SQL Server)
A network-related or instance-specific error occurred while establishing a connection to SQL Server. The server was not found or was not accessible. Verify that the instance name is correct and that SQL Server is configured to allow remote connections. (provider: Named Pipes Provider, error: 40 - Could not open a connection to SQL Server)
All operations successfully completed

7 Appendix 1. Description of the Access Manager interfaces

7.1 The settings panel of the Access Manager object

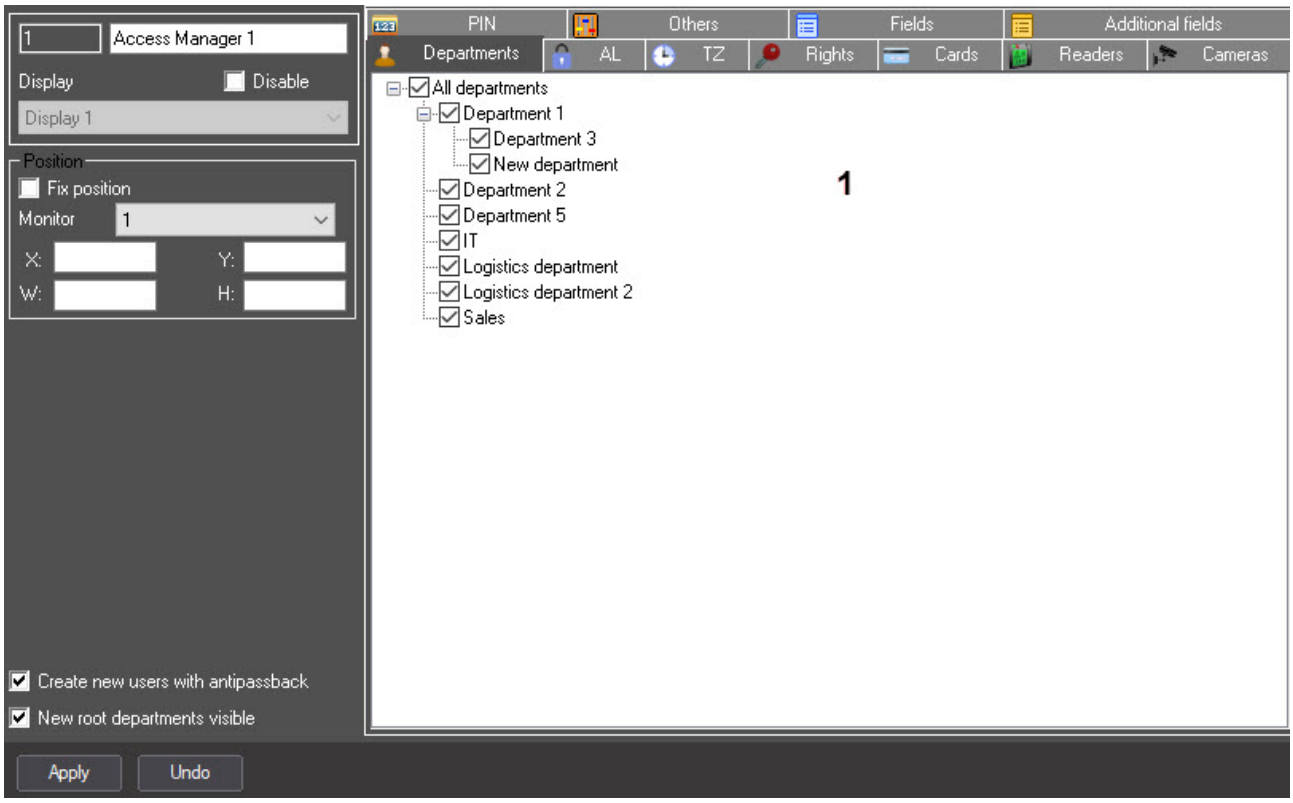
The settings panel of the **Access Manager** interface object is shown in the figures.



№	Parameter name	Method of setting the parameter value	Parameter description	Representation	Default value	Value range
The **Position** group						
1	The **Fix position** checkbox	Set the checkbox	Set the checkbox if you want to specify the coordinates and the size of the **Access Manager** window on the screen and prohibit its movement	Boolean type	Clear	**Set**—position of the **Access Manager** window is fixed **Clear**—position of the **Access Manager** window can be changed

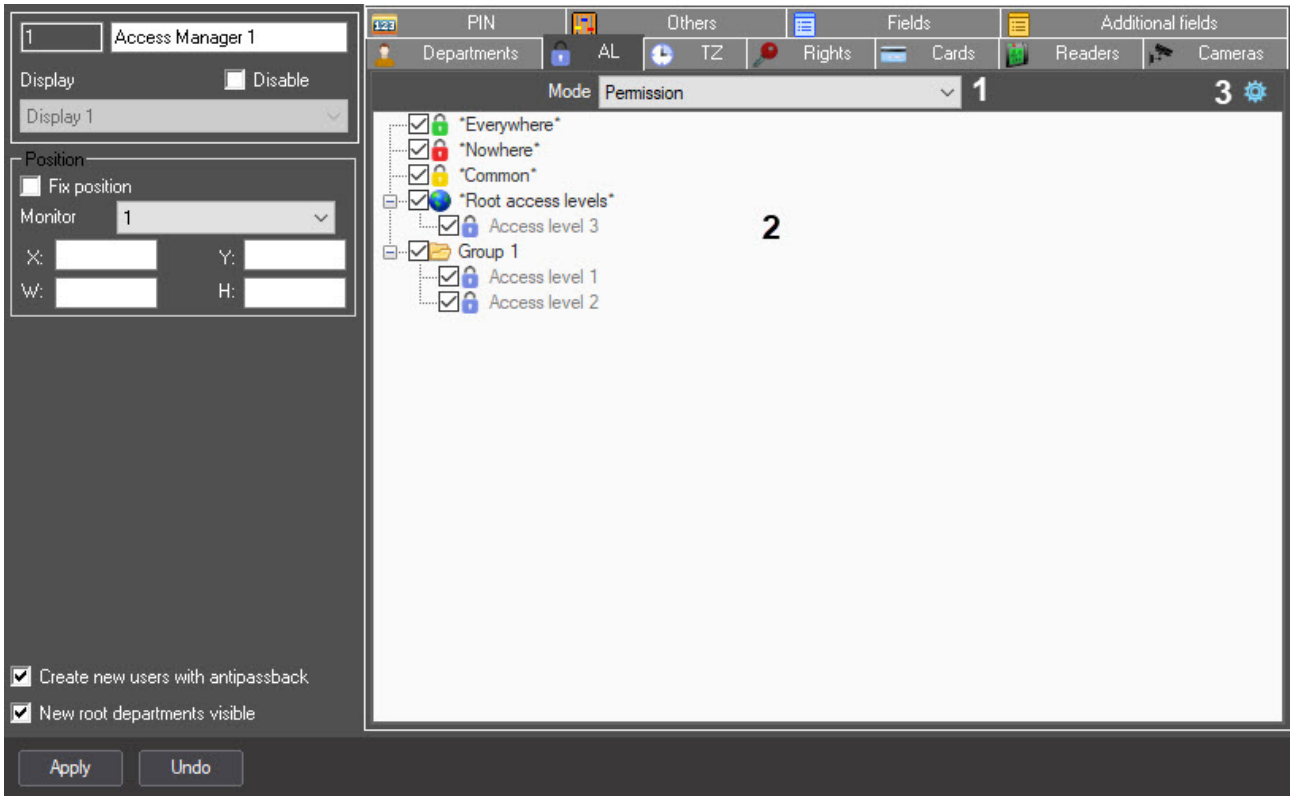
2	The **Monitor** drop-down list	Select the value from the list	Sets the number of the monitor on which the **Access Manager** window must be displayed	List of available computer monitors	Monitor 1	Depends on the number of the connected computer monitors
3	The **X** field with list	Enter the value in the field	Sets the coordinate of the upper left corner of the **Access Manager** window along the horizontal X axis	% of screen width	0	From 0 to M*100, where M is a number of installed (computer) monitors
	The **Y** field with list	Enter the value in the field	Sets the coordinate of the upper left corner of the **Access Manager** window along the vertical Y axis	% of screen height	0	From 0 to M*100, where M is a number of installed (computer) monitors
	The **W** field with list	Enter the value in the field	Sets the width of the **Access Manager** window	% of screen width	0	From 0 to M*100, where M is a number of installed (computer) monitors
	The **H** field with list	Enter the value in the field	Sets the height of the **Access Manager** window	% of screen height	0	From 0 to M*100, where M is a number of installed (computer) monitors
Out of the group						
4	The **Create new users with antipassback** checkbox	Set the checkbox	Sets the default value for the user antipassback parameter	Boolean type	Clear	**Set**—by default, the users are created with enabled antipassback **Clear**—by default, the users are created with disabled antipassback
5	The **New root departments visible** checkbox	Set the checkbox	Determines the availability of the created departments in the **Access Manager** that are located in the root of the hierarchy	Boolean type	Set	**Set**—new departments created in the root of the hierarchy are available in the **Access Manager** **Clear**—new departments created in the root of the hierarchy aren't available in the **Access Manager**

The **Departments** tab



№	Parameter name	Method of setting the parameter value	Parameter description	Representation	Default value	Value range
1	Departments tree	Set the checkbox	Sets the departments available in the **Access Manager** window	Boolean type	Set of the boolean variables	Department will be available in the **Access Manager** window if you set the checkbox next to it

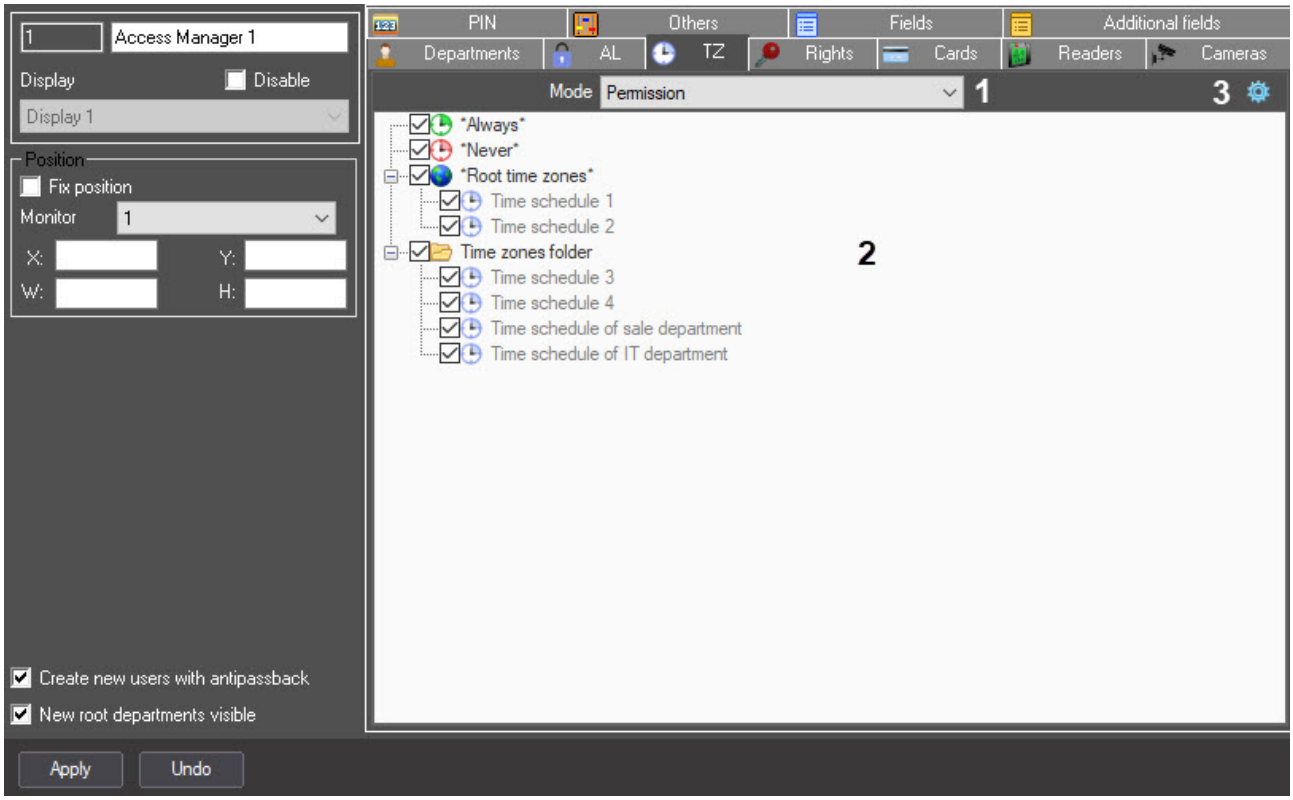
The **AL** tab



№	Parameter name	Method of setting the parameter value	Parameter description	Representation	Default value	Value range
1	The **Mode** drop-down list	Select the value from the list	Sets the access restriction mode to the access levels in the **Access Manager** interface object	NA	Prohibition	**Prohibition**— restrict the access to the selected access levels **Permission**—allow the access to the selected access levels
2	Access levels tree	Set the checkbox	Specifies the access levels, the access to which must be configured	Boolean type	Set of the 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

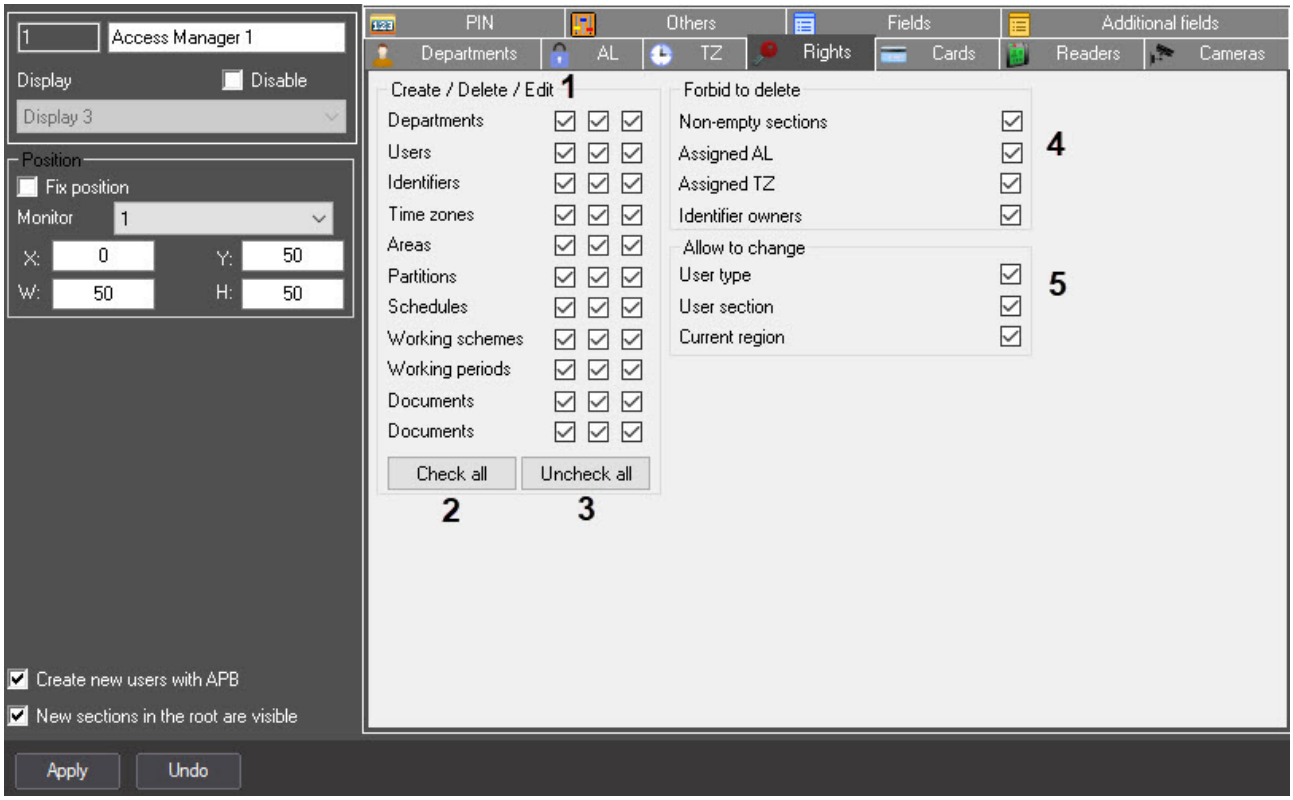
3	The action button	Select the value from the list	Opens a list of actions for managing the access levels tree	NA	NA	**Minimize**—minimizes all access levels in the tree **Expand**—expands all access levels in the tree **Select all**—sets the checkboxes for all access levels **Remove all**—clears checkboxes for all access levels **Search**—opens the **Access level search** window or a folder for searching the access level or a folder for searching by the name or identifier

The **TZ** tab



№	Parameter name	Method of setting the parameter value	Parameter description	Representation	Default value	Value range
1	The **Mode** drop-down list	Select the value from the list	Sets the access restriction mode to the time zones in the **Access Manager** interface object	NA	Prohibition	**Prohibition**—restrict the access to the selected time zones **Permission**—allow the access to the selected time zones
2	Time zones tree	Set the checkbox	Specifies the time zones, the access to which must be configured	Boolean type	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	The action button	Select the value from the list	Opens a list of actions for managing the time zones tree	NA	NA	**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**—clears the checkboxes for all time zones **Search**—opens the **Time zone search** window or a folder for searching the time zone or a folder searching by name identifier

The **Right** tab

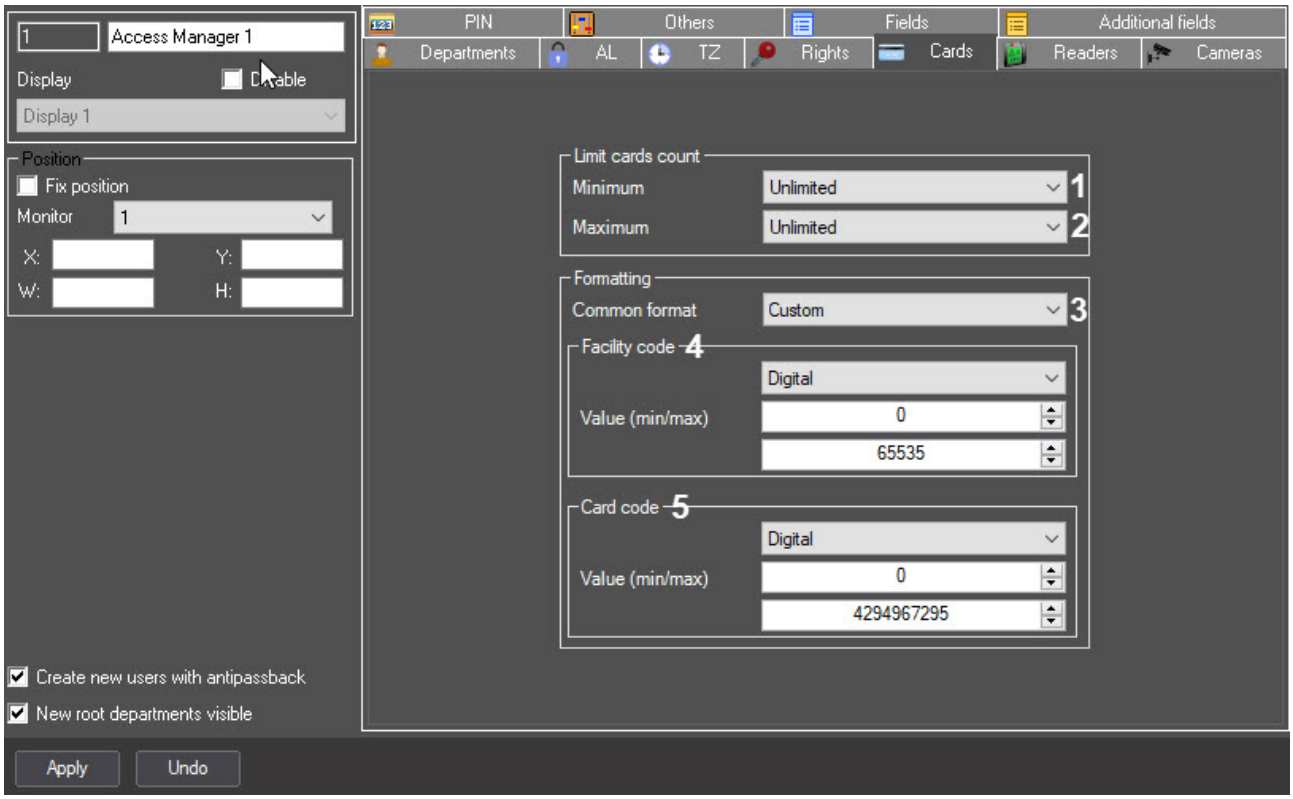


№	Parameter name	Method of setting the parameter value	Parameter description	Representation	Default value	Value range
The **Create** / **Delete** / **Edit** group						
1	The **Create** checkbox	Set the checkbox	Creates the corresponding object in the **Access Manager** window	Boolean type	Set	**Set**—creating the corresponding object from the **Access Manager** window is allowed **Clear**—creating the corresponding object from the **Access Manager** window is forbidden

	The **Delete** checkbox	Set the checkbox	Deletes the corresponding object in the **Access Manager** window	Boolean type	Set	**Set**—deleting the corresponding object from the **Access Manager** window is allowed **Clear**—deleting the corresponding object from the **Access Manager** window is forbidden
	The **Edit** checkbox	Set the checkbox	Edits the corresponding object in the **Access Manager** window	Boolean type	Set	**Set**—editing the corresponding object from the **Access Manager** window is allowed **Clear**—editing the corresponding object from the **Access Manager** window is forbidden
2	The **Check all** button	Click the button	Sets all checkboxes in the **Create / Delete / Edit** group	NA	NA	NA
3	The **Uncheck all** button	Click the button	Clears all checkboxes in the **Create / Delete / Edit** group	NA	NA	NA
The **Forbid to delete** group						
4	The **Non-empty departments** checkbox	Set the checkbox	Forbids to delete departments which cotain users	Boolean type	Clear	**Set**—non-empty departments cannot be deleted **Clear**—non-empty departments can be deleted
	The **Assigned AL** checkbox	Set the checkbox	Forbids to delete access levels if they are assigned to any user or department	Boolean type	Clear	**Set**—assigned access levels cannot be deleted **Clear**—assigned access levels can be deleted
	The **Assigned TZ** checkbox	Set the checkbox	Forbids to delete time zones if they are assigned to any access level	Boolean type	Clear	**Set**—assigned time zones cannot be deleted **Clear**—assigned time zones can be deleted
The **Allow to change** group						

5	The **User type** checkbox	Set the checkbox	Allows changing the user type	Boolean type	Clear	**Set**—the user type change is allowed **Clear**—the user type change isn't allowed
	The **User department** checkbox	Set the checkbox	Allows changing the user department	Boolean type	Clear	**Set**—the user department change is allowed **Clear**—the user department change isn't allowed
	The **Current region** checkbox	Set the checkbox	Allows changing the current region	Boolean type	Clear	**Set**—the current region change is allowed **Clear**—the current region change isn't allowed

The **Cards** tab



№	Parameter name	Method of setting the parameter value	Parameter description	Representation	Default value	Value range
The **Limit cards count** group						

1	The **Minimum** drop-down list	Select the value from the list	Sets the minimum number of access cards that must be assigned to the user	List of values of the minimum number of access cards of a user	Unlimited	• from **1** to **10**—if the specified number of access cards isn't 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 function menu for assigning access cards will be inactive in the **Access Manager** interface object

2	The **Maximum** drop-down list	Select the value from the list	Sets the maximum number of access cards that must be assigned to the user	List of values of the maximum number of access cards of a user	Unlimited	• from **1** to **10**—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 function menu for assigning access cards will be inactive in the **Access Manager** interface object
The **Formatting** group						

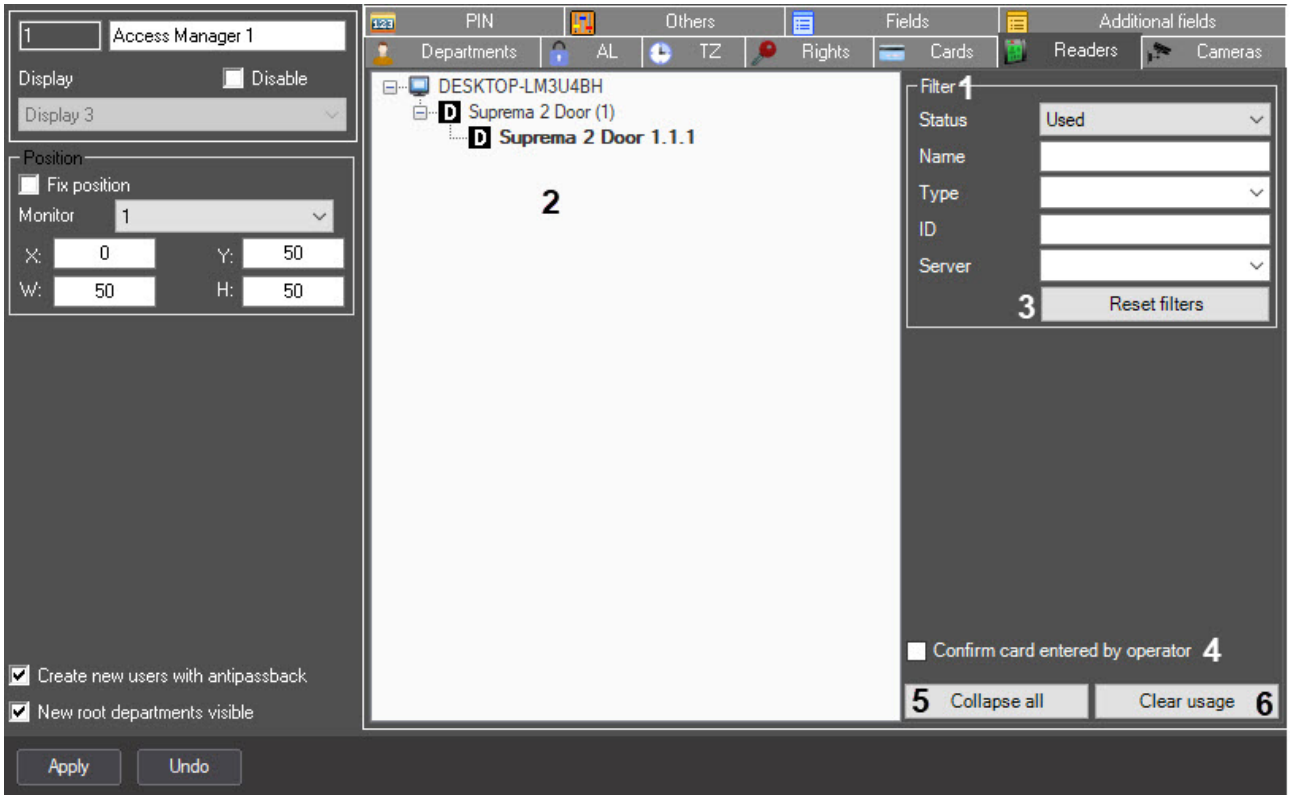
3	The **Common format** drop-down list	Select the value from the list	Sets the format of access cards	List of values of access cards formats	Default	• **Default**—allows setting an arbitrary value for the facility code and card code. Any letters, digits and characters are allowed • **Wiegand26**—allows entering a 1-byte facility code (from 0 to 255), and a 2-byte card code (from 0 to 65535). If the limit of the code length is exceeded, the user cannot be saved • **Wiegand32**—allows entering a 2-byte facility code (from 0 to 65535), and a 2-byte card code (from 0 to 65535). If the limit of the code length is exceeded, the user cannot be saved • **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 must be eight characters or longer. If the entered card code is less than eight characters long, 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 digits from 0 to 4294967295 • **Hexadecimal**—allows entering digits in HEX format (digits and characters A, B, C, D, E, F) from 0 to 8 bytes long

						• **Fixed number**—similar to **Fixed character**, but instead of a character, a digit between 0 and 4294967295 is used • **Regular template**—allows defining an access card template with specified restrictions, lengths and value ranges

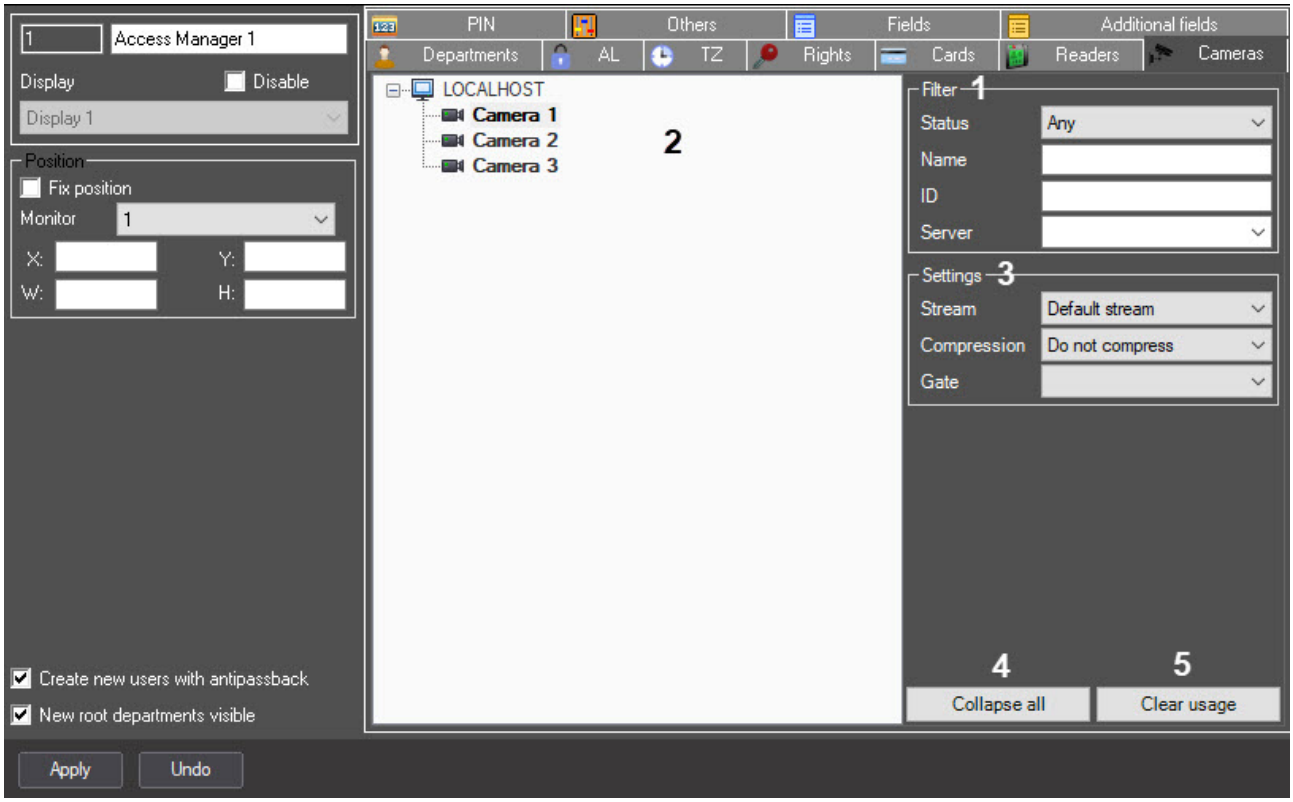
The **Readers** tab



№	Parameter name	Method of setting the parameter value	Parameter description	Representation	Default value	Value range
1	The **Filter** group					
	The Status drop-down list	Select the value from the list	Displays a list of control reader statuses to search by the value of this field	List of control reader statuses	Any	**Any**—all control readers created in the system **Used**—only used control readers **Not used**—only control readers that aren't used
	The **Name** field	Enter the value in the field	Sets the name of the control reader to search by the value of this field	Latin and Cyrillic alphabet, digits 0-9	NA	NA

	The **ID** field	Enter the value in the field	Sets the unique identifier of the control reader to search by the value of this field	Sequence of numbers	NA	NA
	The Server drop-down list	Select the value from the list	Sets the name of the server to search by the value of this field	List of the **Server** objects	NA	Depends on the number of the **Server** objects
2	List of control readers	Automati cally	Displays the list of control readers used for entering user access cards from the **Access Manager**	List of readers filtered in step 1	NA	If you select the reader, it is available for entering the user access card or entering the user biometric data
3	The **Reset filters** button	Click the button	Resets filters and search result	NA	NA	NA
4	The **Confirm card entered by operator** checkbox	Set the checkbox	Sets the necessity to confirm the card code entered by an operator	Boolean type	Clear	**Set**—operator confirmation is required to assign access card to a user **Clear**—operator confirmation isn't required to assign access card to a user
5	The **Collapse all** button	Click the button	Collapses the list of readers	NA	NA	NA
6	The **Clear usage** button	Click the button	Resets the settings of the control reader list to the default values	NA	NA	NA

The **Cameras** tab

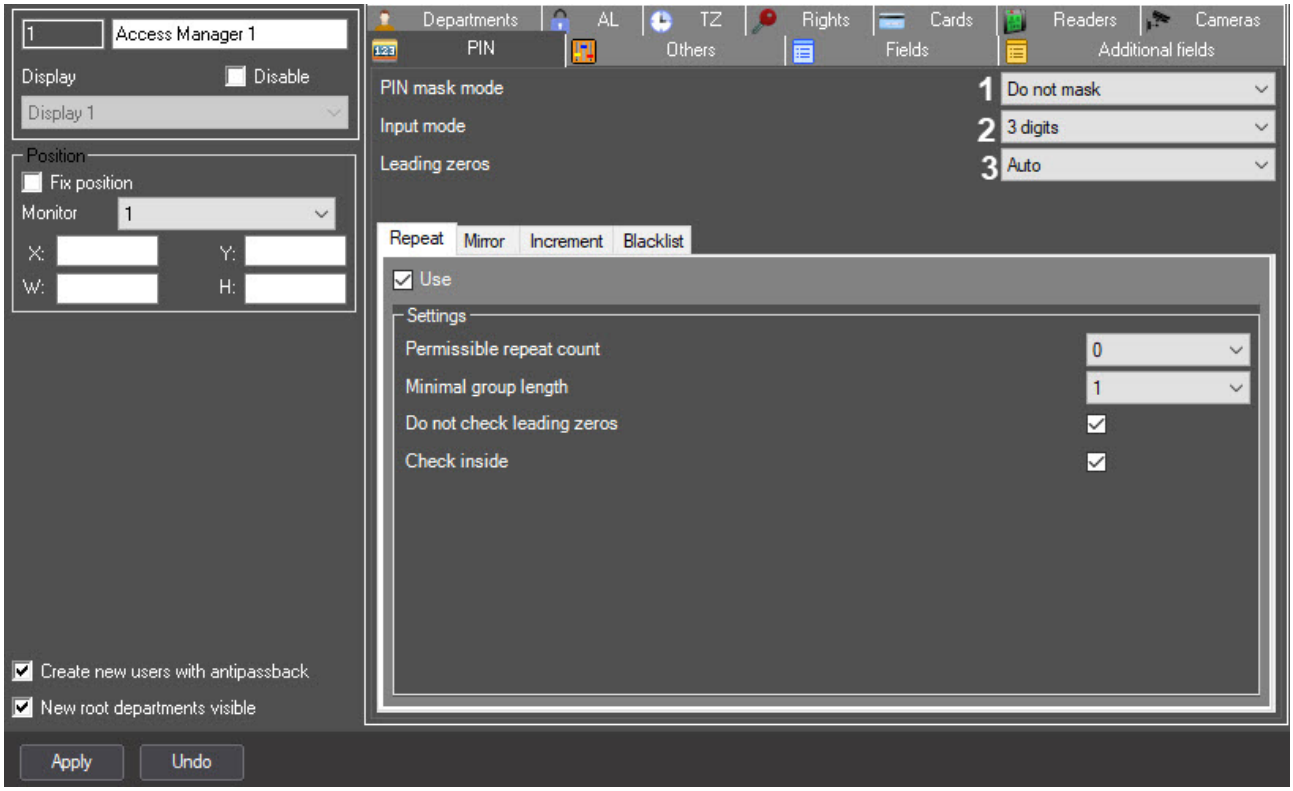


№	Parameter name	Method of setting the parameter value	Parameter description	Representation	Default value	Value range
The **Filter** group						
1	The **Status** drop-down list	Select the value from the list	Displays the list of statuses of the **Camera** object to search by the value of this field	List of statuses of the **Camera** object	Unused	**Any**—all cameras created in the system **Used**—only cameras that are used **Unused**—only cameras that aren't used
	The **Name** field	Enter the value in the field	Sets the name of the camera to search by the value of this field	Latin and Cyrillic alphabet, digits 0-9	NA	NA

	The **ID** field	Enter the value in the field	Sets a unique camera identifier to search by the value of this field	Sequence of numbers	NA	NA
	The **Server** drop-down list	Select the value from the list	Sets the name of the server to search by the value of this field	List of the **Server** objects	NA	Depends on the number of the **Server** objects
2	The **Cameras** object tree	Automatically	Displays the list of the **Camera** objects	List of the **Camera** objects filtered in step 1	NA	Depends on the number of the **Camera** objects filtered in step 1
The **Settings** group						
3	The **Stream** drop-down list	Select the value from the list	Sets the camera stream that will be used to assign photos to users	NA	Do not use	**Do not use**—camera cannot be used to input a photo **Default stream**—the default stream of a camera will be used **Stream #1**—the first stream of a camera will be used **Stream #2**—the second stream of a camera will be used **Stream #3**—the third stream of a camera will be used **Stream #4**—the forth stream of a camera will be used

	The **Compression** drop-down list	Select the value from the list	Sets the compression level of the selected video stream	List of compression options	Do not compress	**Do not compress**—compression of the camera video stream is disabled **Level 1**—the lowest level of the video stream compression .... **Level 5**—the highest level of the video stream compression
	The **Gate** drop-down list	Select the value from the list	Sets the **Videogate** object that must be used for receiving video signal from a camera	List of the **Videogate** objects created in the system	NA	Depends on the number of the **Videogate** objects created in the system
4	The **Collapse all** button	Click the button	Collapses the list of cameras	NA	NA	NA
5	The **Clear usage** button	Click the button	Resets all camera settings to the default values	NA	NA	NA

The **PIN** tab



№	Parameter name	Method of setting the parameter value	Parameter description	Representation	Default value	Value range
1	The **PIN mask mode** drop-down list	Select the value from the list	Sets the mask mode of the PIN code	List of options for PIN code masking	Mask always	**Do not mask**—PIN code isn't masked with dots **Mask view**—PIN code is masked with dots when you read user data **Mask always**—PIN code is always masked with dots

2	The **Input mode** drop-down list	Select the value from the list	Sets the input mode of the PIN code	List of PIN code input modes	Common	**Common**—any variant of the PIN code is allowed. You can enter symbols, letters and numbers. If you select this mode, no further settings are required **3 digits**—PIN code must contain three digits. ... **9 digits**—PIN code must contain nine digits. **Range**—PIN code is within the specified numeric range
3	The **Leading zeros** drop-down list	Select the value from the list	Sets the mode of setting zeros at the beginning of the PIN code. The setting is made for all modes except for the common mode	List of modes for setting zeros at the beginning of the PIN code	Ignore	**Ignore**—leading zeros aren't considered as characters **Required**—leading zeros are considered as characters **Auto**—leading zeros are entered automatically, completing the PIN code to the required number of characters

The **Repeat** tab

1	The **Use** checkbox	Set the checkbox	Enables the required PIN check	Boolean type	Clear	**Set**—the required check is enabled **Clear**—the required check is disabled
2	The **Permissible repeat count** drop-down list	Select the value from the list	Sets the maximum number of allowed character repetitions in the PIN code	Digits 0–7	0	Depends on the selected input mode
3	The **Minimal group length** drop-down list	Select the value from the list	Sets the number of characters in the group to search for repetitions	Digits 1–8	1	Depends on the selected input mode
4	The **Do not check leading zeros** checkbox	Set the checkbox	Doesn't considers the leading zeros as characters when you enter the PIN code	Boolean type	Clear	**Set**—leading zeros aren't considered **Clear**—leading zeros are considered
5	The **Check inside** checkbox	Set the checkbox	Enables the corresponding search in the entire PIN code (not only from the begining)	Boolean type	Clear	**Set**—search is performed in the entire PIN code (not only from the begining) **Clear**—search is performed only from the beginning

The **Mirror** tab

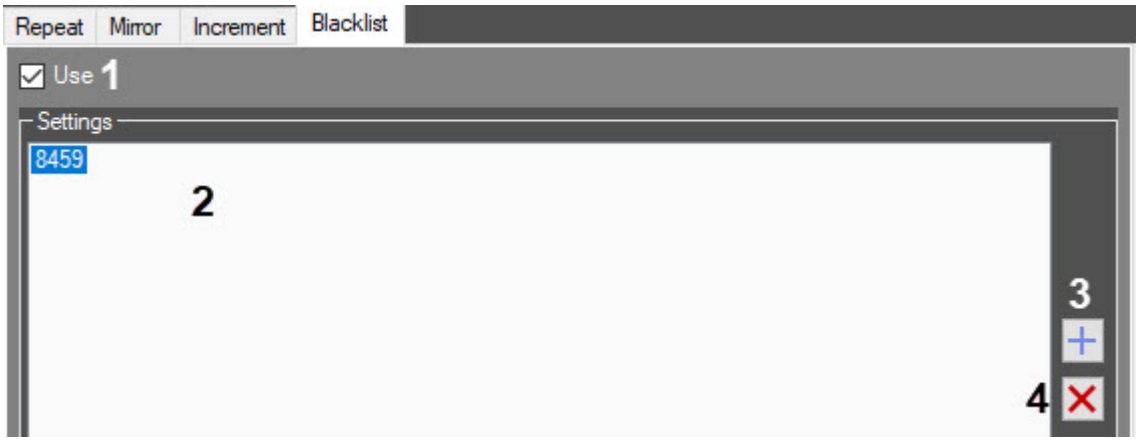
1	The **Use** checkbox	Set the checkbox	Enables the required PIN check	Boolean type	Clear	**Set**—the required check is enabled **Clear**—the required check is disabled
2	The **Minimal side length** drop-down list	Select the value from the list	Sets the number of characters in the group to search for repetitions in the mirror image	Digits 1–8	1	Depends on the selected input mode
3	The **Do not check leading zeros** checkbox	Set the checkbox	Doesn't considers the leading zeros as characters when you enter the PIN code	Boolean type	Clear	**Set**—leading zeros aren't considered **Clear**—leading zeros are considered
4	The **Check inside** checkbox	Set the checkbox	Enables the corresponding search in the entire PIN code (not only from the begining)	Boolean type	Clear	**Set**—search is performed in the entire PIN code (not only from the begining) **Clear**—search is performed only from the beginning

The **Increment** tab

1	The **Use** checkbox	Set the checkbox	Enables the required PIN check	Boolean type	Clear	**Set**—the required check is enabled **Clear**—the required check is disabled
2	The **Permissible 'stair' length** drop-down list	Select the value from the list	Sets the number of characters in increasing/ decreasing order from which the search will be performed	Digits 1–8	1	Depends on the selected input mode
3	The **Checking mode** drop-down list	Select the value from the list	Sets the checking mode of the PIN code character sequence	List of checking modes of the PIN code character sequence	Both	**Both**—sequences of characters are checked in increasing (increment) and decreasing (decrement) order **Increment**—sequences of characters are checked in increasing order **Decrement**—sequences of characters are checked in decreasing order

4	The **Do not check leading zeros** checkbox	Set the checkbox	Doesn't considers the leading zeros as characters when you enter the PIN code	Boolean type	Clear	**Set**—leading zeros aren't considered **Clear**—leading zeros are considered
5	The **Check inside** checkbox	Set the checkbox	Enables the corresponding search in the entire PIN code (not only from the begining)	Boolean type	Clear	**Set**—search is performed in the entire PIN code (not only from the begining) **Clear**—search is performed only from the beginning

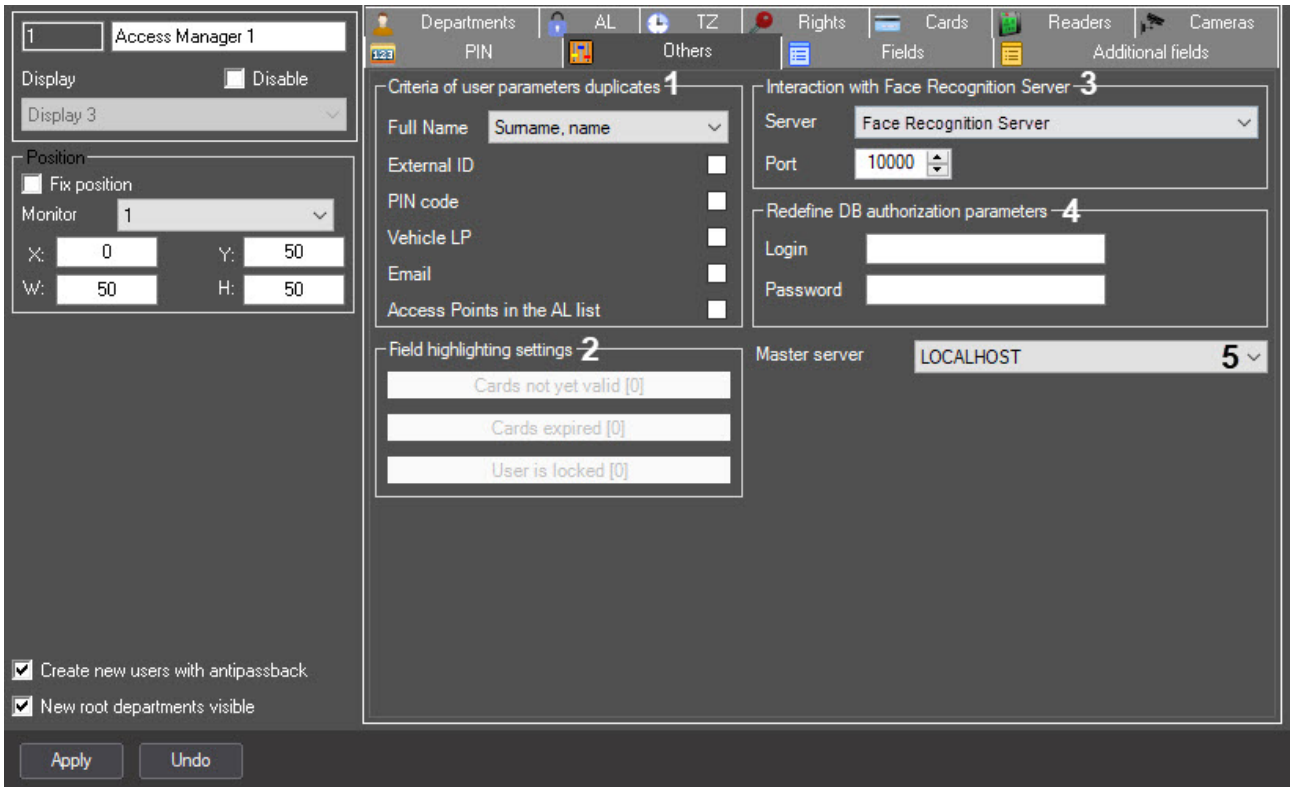
The **Blacklist** tab



1	The **Use** checkbox	Set the checkbox	Enables the required PIN check	Boolean type	Clear	**Set**—the required check is enabled **Clear**—the required check is disabled
2	List of PIN codes	Using the **Add** button	Contains the list of PIN codes prohibited for use	String	NA	NA
3	The Add button	Click the button	Opens the form for adding the PIN code to the blacklist	NA	NA	NA

4	The Delete button	Click the button	Removes the PIN code from the blacklist	NA	NA	NA

The **Others** tab



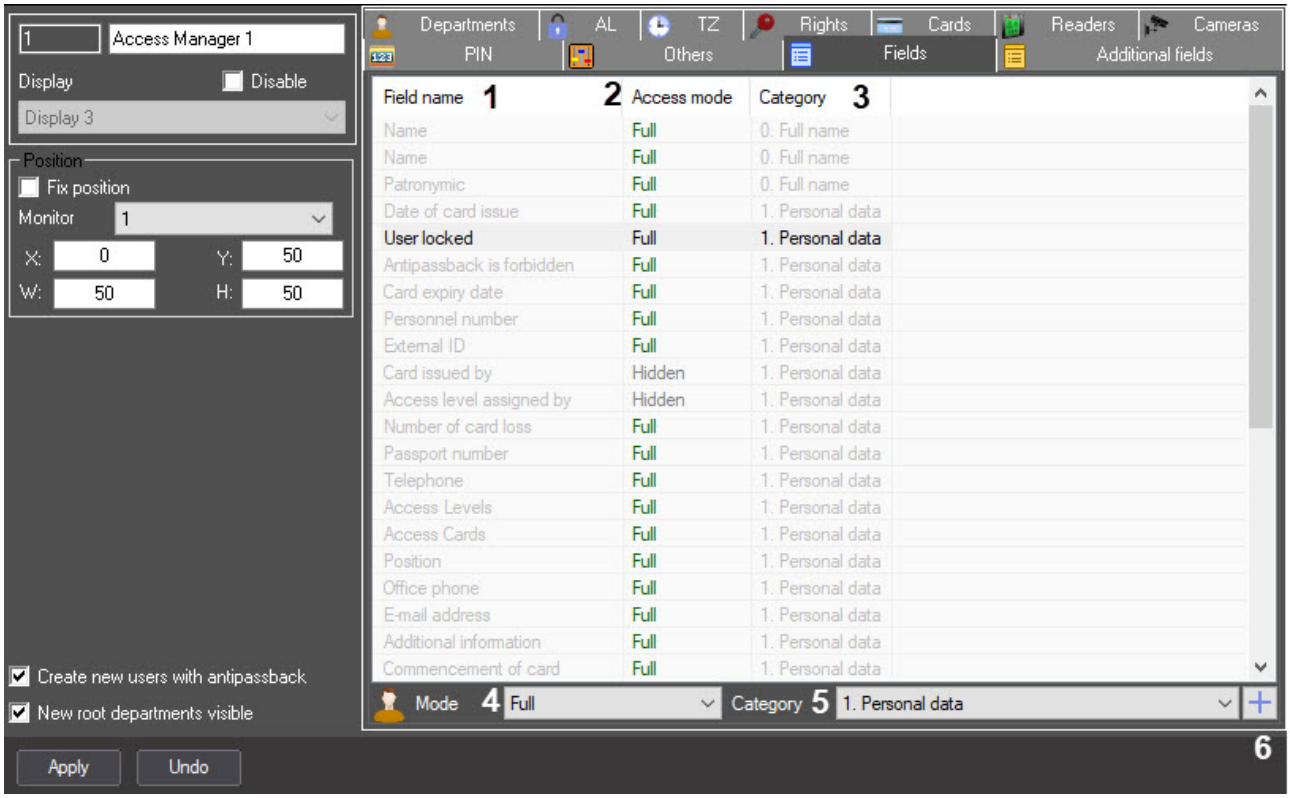
№	Parameter name	Method of setting the parameter value	Parameter description	Representation	Default value	Value range
1	The **Criteria of user parameters duplicates** group					

	The **Full name** drop-down list	Select the value from the list	Displays a list of criteria for restricting duplicate user parameters by name, surname, patronymic	List of available combinations	Not used	**Not used**—added users aren't checked for duplicate name, surname, patronymic **Surname, name**—added users are checked for duplicate name and surname **Surname, name, patronymic**—added users are checked for duplicate name, surname, patronymic
	The **External ID** checkbox	Set the checkbox	Checks the added users for duplicate external ID	Boolean type	Clear	**Set**—added users are checked for duplicate external ID **Clear**—added users aren't checked for duplicate external ID
	The **PIN code** checkbox	Set the checkbox	Checks the added users for duplicate PIN code	Boolean type	Clear	**Set**—added users are checked for duplicate PIN code **Clear**—added users aren't checked for duplicate PIN code
	The **Vehicle LP** checkbox	Set the checkbox	Checks the added users for duplicate license plates	Boolean type	Clear	**Set**—added users are checked for duplicate license plates **Clear**—added users aren't checked for duplicate license plates
	The **Email** checkbox	Set the checkbox	Checks the added users for duplicate emails	Boolean type	Clear	**Set**—added users are checked for duplicate emails **Clear**—added users aren't checked for duplicate emails

	The **Access Points in the AL list** checkbox	Set the checkbox	Checks the added users for duplicate access points included in the access level	Boolean type	Clear	**Set**—added users are checked for duplicate access points included in the access level **Clear**—added users aren't checked for duplicate access points included in the access level
2	The **Field highlighting settings** group					
	The **Cards not yet valid [0]** button	Click the button	Enables the color highlighting of the **Cards not yet valid** field	NA	NA	NA
	The **Cards expired [0]** button	Click the button	Enables the color highlighting of the **Cards expired** field	NA	NA	NA
	The User is locked [0] button	Click the button	Enables the color highlighting of the **User is locked** field	NA	NA	NA
3	The **Interaction with Face Recognition Server** group					
	The **Server** drop-down list	Select the value from the list	Displays the list of the **Face Recognition Server** objects created on the **Hardware** tab of the **System settings** window	List of the **Face Recognition Server** objects created in the system	NA	Depends on the **Face Recognition Server** objects created in the system
	The **Port** field	Enter the value in the field	Sets the communication port to connect to the face recognition server via the REST API. The default value is **10000**	Sequence of numbers	0	NA
4	The **Redefine DB authorization parameters** group—this group of settings is currently rudimentary					

5	The **Master server** drop-down list	Select the value from the list	Displays the list of the **Server** objects	List of the **Server** objects	NA	Depends on the number of the created **Server** objects

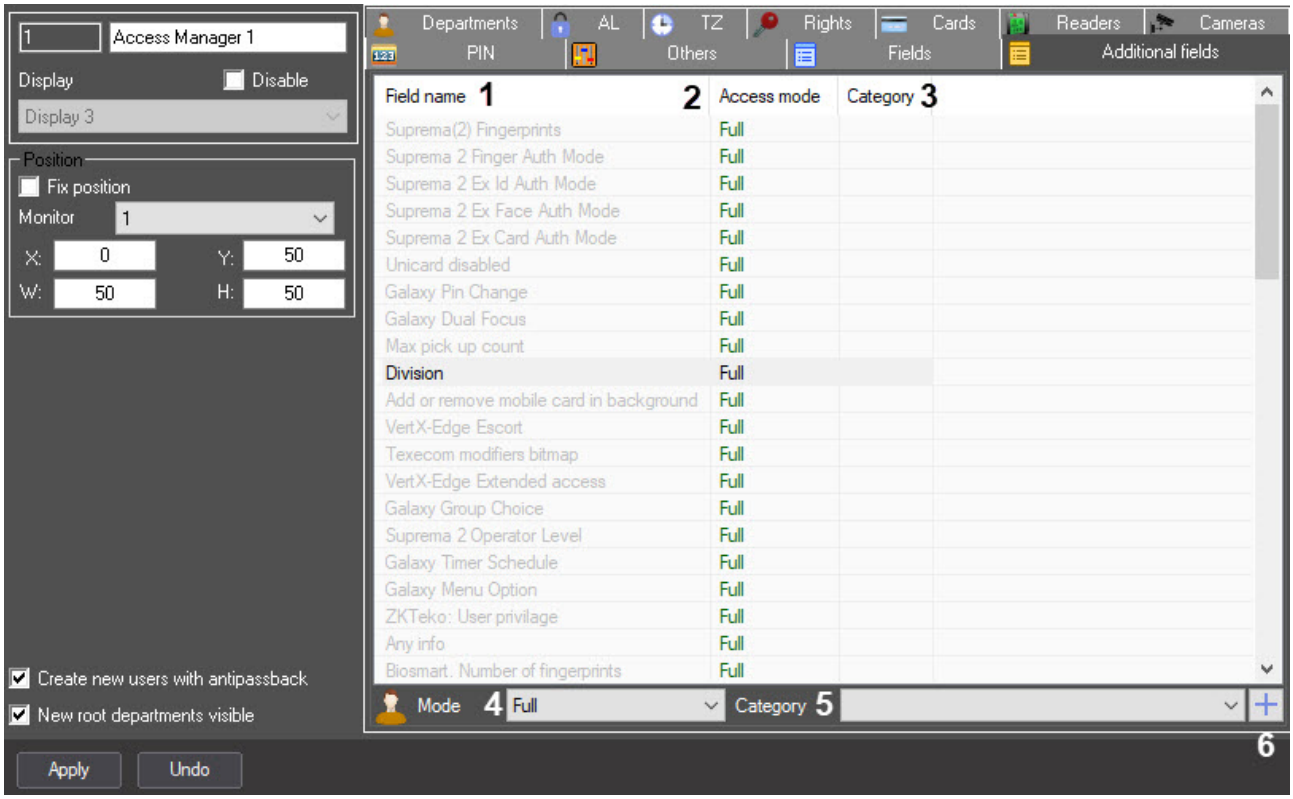
The **Fields** tab



№	Parameter name	Method of setting the parameter value	Parameter description	Representation	Default value	Value range
1	The **Field name** column	Automatically	Displays the list of the standard user fields	List of the standard user fields	NA	List of fields depends on the used integration modules

2	The **Access mode** column	Automatically	Displays the list of assigned access modes for the standard user fields	List of assigned access modes for the standard user fields	NA	NA
3	The **Category** column	Automatically	Displays the list of category names to which the standard fields belong	List of the category names to which the standard fields belong	NA	NA
4	The **Mode** drop-down list	Select the value from the list	Assigns the mode of working with the standard user fields in the **Access Manager** interface object	List of the access modes of the standard user field created in the system	Depends on the standard user field	**Edit**—the field is displayed with the ability of editing **Hidden**—the field is hidden **Read only**—the field is displayed without the ability of editing **Mandatory**—this field is mandatory when you create and edit a user in the *Access Manager* module. If you don't fill out the parameter, the field is highlighted with red asterisks
5	The **Category** drop-down list	Select the value from the list	Assigns a category to a standard user field	List of the category names of the standard user field created in the system	Depends on the standard user field	0. Full name 1. Personal data 3. Vehicle 4. Visitor data
6	Button for adding a category	Click the button	Adds a category of a standard user field	NA	NA	NA

The **Additional fields** tab

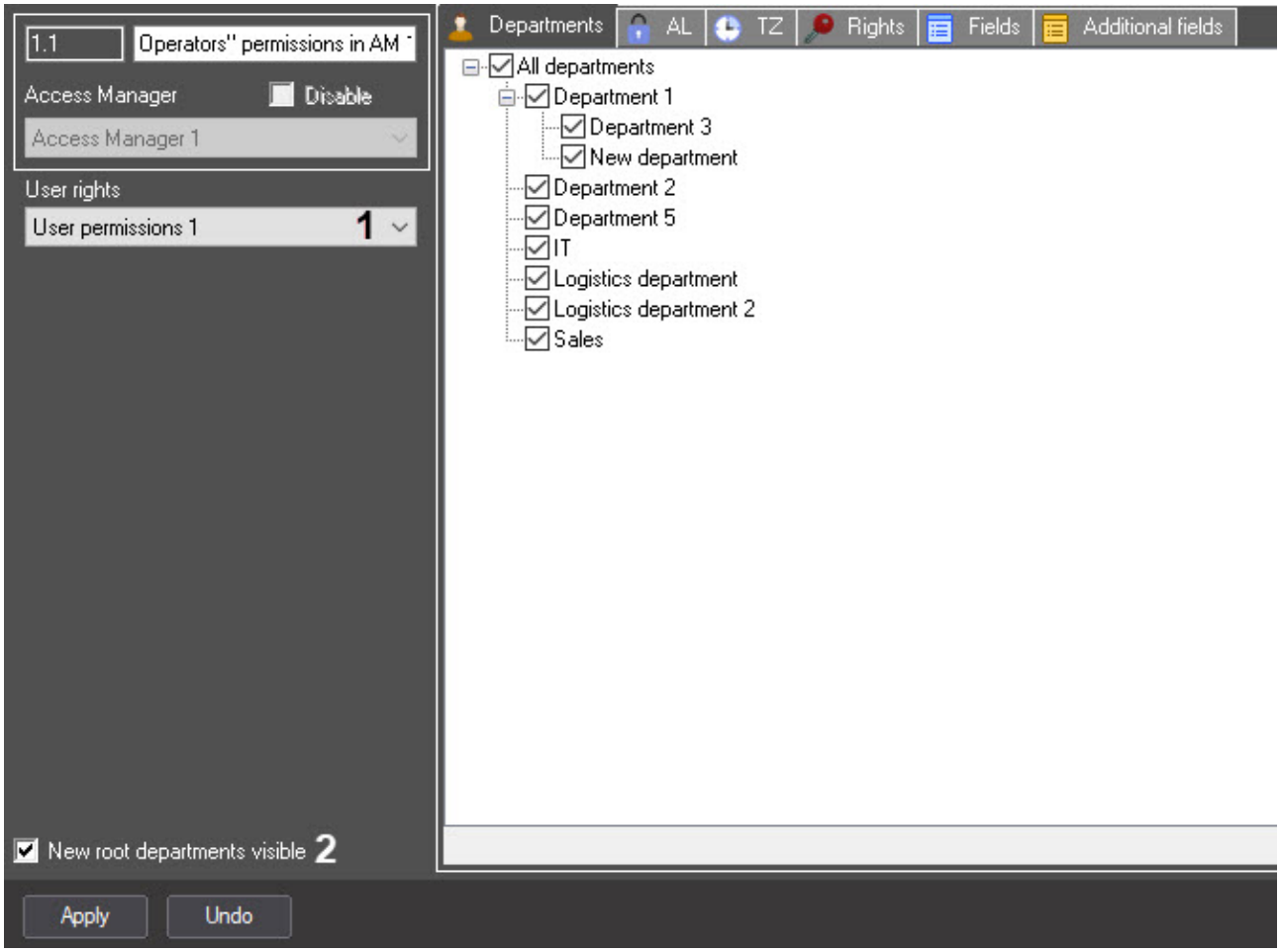


№	Parameter name	Method of setting the parameter value	Parameter description	Representation	Default value	Value range
1	The **Field name** column	Automatically	Displays the list of additional user fields	List of additional user fields	NA	List of fields depends on the used integration modules
2	The **Access mode** column	Automatically	Displays the list of assigned access modes for additional user fields	NA	NA	NA
3	The **Category** column	Automatically	Displays the list of category names to which the additional fields belong	NA	NA	NA

4	The **Mode** drop-down list	Select the value from the list	Assigns the mode of working with additional user fields in the **Access Manager** interface object	List of the access modes of the additional user field created in the system	Depends on the additional user field	**Edit**—the field is displayed with the ability of editing **Hidden**—the field is hidden **Read only**—the field is displayed without the ability of editing **Mandatory**—this field is mandatory when you create and edit a user in the *Access Manager* module. If you don't fill out the parameter, the field is highlighted with red asterisks
5	The **Category** drop-down list	Select the value from the list	Assigns a category to an additional user field	List of the category names of the additional user field created in the system	NA	NA
6	Button for adding a category	Click the button	Adds a category of an additional user field	NA	NA	NA

7.2 The settings panel of the Operators' permissions in AM object

The settings panel of the **Operators'' permissions in AM** interface object is shown in the figure.



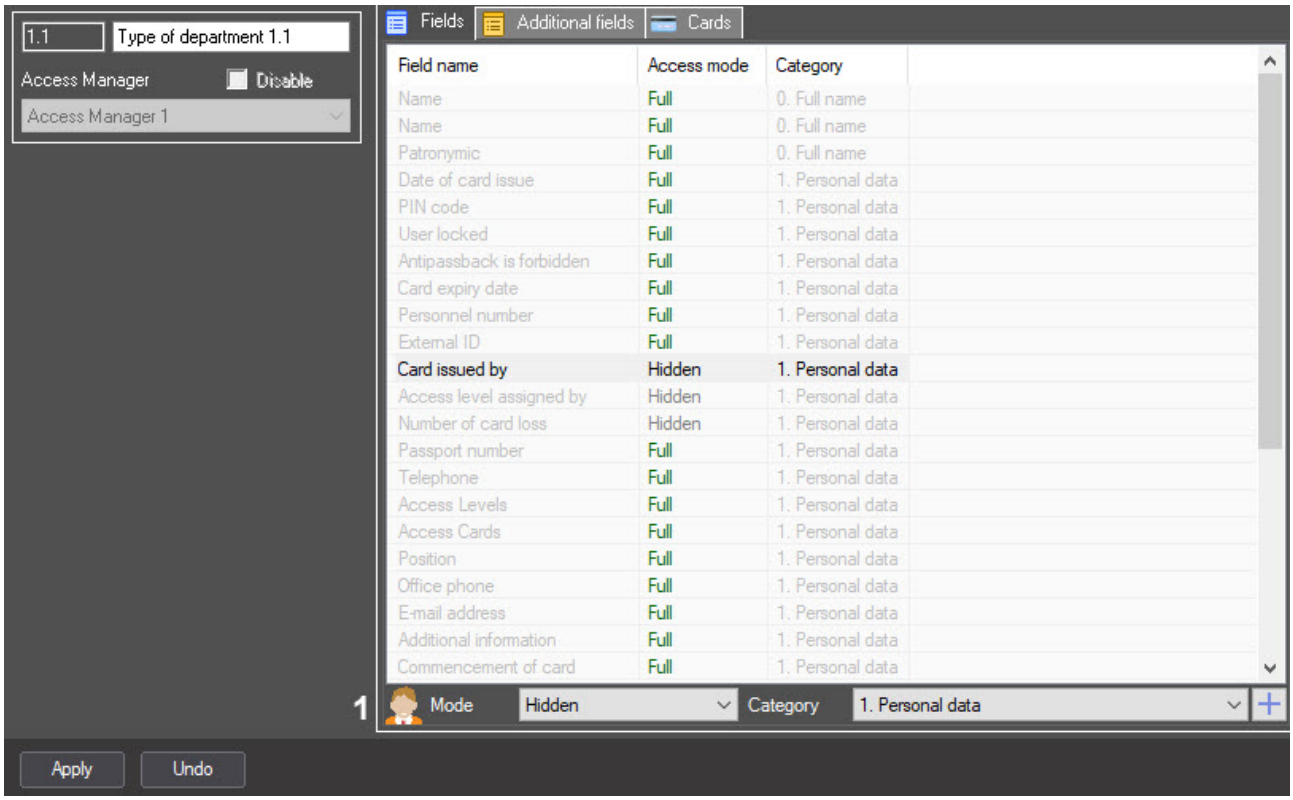
№	Parameter name	Method of setting the parameter value	Parameter description	Representation	Default value	Value range
The **User rights** group						
1	**User rights**	Select the value from the list	Sets the user rights in *ACFA PSIM*, corresponding to the **Operators' permissions in AM** object that is being configured	Name the **User permissions** objects registered in the system	Depends on the **User permissions** objects created in the system	Depends on the **User permissions** objects created in the system
Outside groups						

2	**New root departments visible**	Set the checkbox	Sets the availability of newly created departments in the **Access Manager** located in the root of the hierarchy	Boolean type	Set	**Set**—new departments are available in the **Access Manager** hierarchy root **Clear**—new departments are not available in the **Access Manager** hierarchy root

The **Departments**, **AL**, **TZ**, **Rights**, **Fields**, and **Additional fields** tabs are similar to the tabs on the settings panel of the **Access Manager** object (see The settings panel of the Access Manager object).

7.3 The settings panel of the Type of department object

The settings panel of the **Type of department** interface object is shown in the figure.



Right-click the icon (**1**) to open the menu in which you can change the icon for displaying the department in the **Access Manager** window and select the department type template (see Configuring a type of department in the Access Manager).

The **Fields**, **Additional fields** and **Cards** tabs are similar to the tabs on the settings panel of the **Access Manager** object (see The settings panel of the Access Manager object).

8 Appendix 2. Configuring the correct operation of the Access Manager module in a distributed system

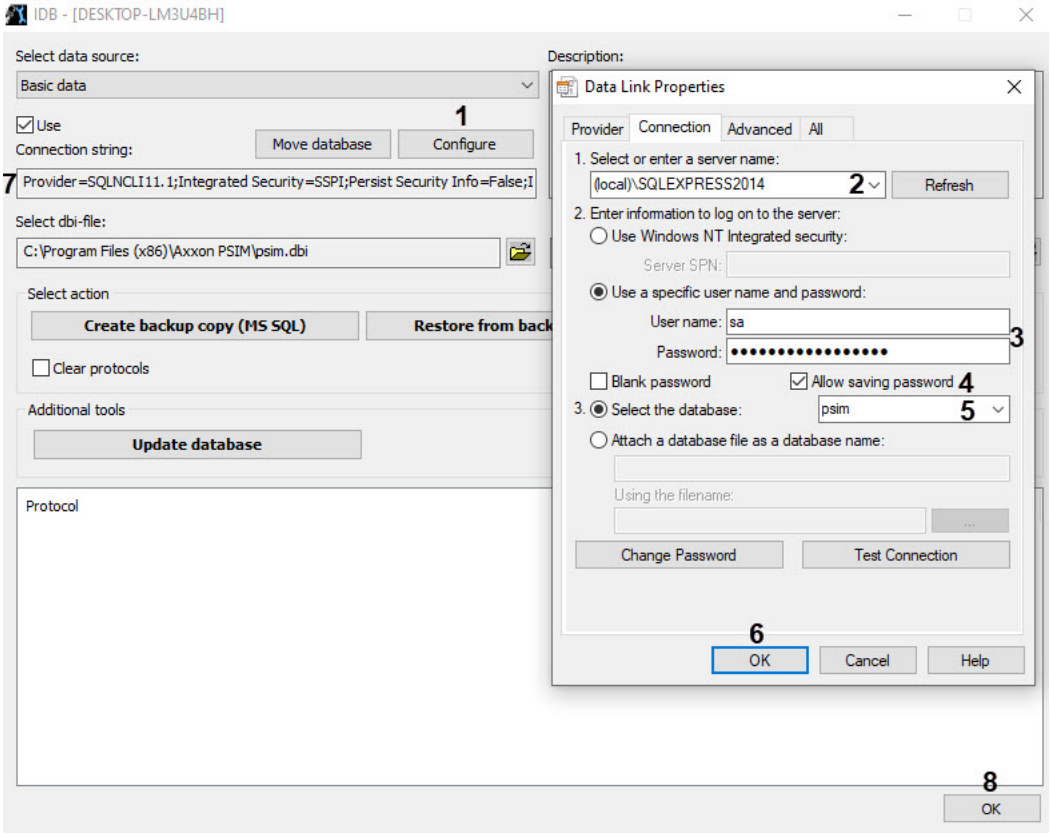
The *Access Manager* module gets the objects required for its operation directly from the SQL Server database of the *Axxon PSIM* Server. This causes some issues for the module operation in distributed systems, based on a variety of combinations between the *Axxon PSIM* Server, the Remote Administrator's workstation, and the Remote Client (see Configuration of distributed architecture).

In particular, when you try to run the *Access Manager* module remotely from a computer with a Remote Client, the *Access Manager* will not display the objects, which are loaded from the database of the *Axxon PSIM* Server, e.g. the lists of users and departments. In order to eliminate this issue, when configuring the distributed system, the administrator should do the following:

1. On the computer with the installed Remote Client:
    a. Install the OLE DB Driver for SQL SERVER driver by selecting the msoledbsql file that is located in the redist folder in the installation directory according to the language and bitness of the Remote Client, or fully install the SQL Server. Thus, the SQL Server on the computer with the installed Remote Client will be able to connect to the SQL Server on the computer with the *Axxon PSIM* Server.
    b. Ensure the SQL Server authentication through the base **sa** account.
    c. Ensure uninterrupted connection of the SQL Server on the computer with the installed Remote Client to the SQL Server on the computer with the installed *Axxon PSIM* Server.

2. On the computer with the installed *Axxon PSIM* Server and the *Access Manager* module:
    a. Configure the SQL Server to allow remote connections.
    b. Ensure the SQL Server authentication through the base **sa** account.
    c. Configure the *Axxon PSIM* Server connection to its database using the idb.exe utility. For this, do the following:

i. Run the utility from the *Axxon PSIM* 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 (**2**), enter the name or the IP address of the SQL server used to for database management.

> **Note**
>
> Note that you must specify the explicit name or the 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 (**3**), select the **Use a specific user name and password** radio button. In the **User name** field enter **sa**. In the **Password** field, enter the password for the **sa** user.

> **Note**
>
> Note that user names other than **sa** are not allowed.

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

> **Note**
>
> This step is mandatory.

vi. Select the **Select the database on the server** radio button and select **psim** from the drop-down list (**5**).

vii. Click the **OK** button to save the connection parameters (**6**). The parameters will be displayed in the **Connection string** field (**7**) in the idb.exe utility interface.
viii. Click the **OK** button (**8**) in the idb.exe utility interface to save the changes.

Configuring the correct operation of the *Access Manager* module in a distributed system is complete.

9 Appendix 3. Creating additional fields for the User object

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

You can create additional fields using the text editor that allows you to view and edit the ASCII text encoding.

9.1 Structure of additional fields in .dbi

Additional fields for the **User** object are divided into two groups:

1. The base field with the default processing has the following structure: (db_name), (db_type) // (description).
   Example: is_guest, BIT // Guest key.
   The default processing depends on the data type (see Supported SQL data types).
2. The base field with special processing has the following structure: (db_name), (db_type) // (description) {(fmt)%(prms)}.
   Example: job_title, CHAR, 20 // Position{C%Waiter|Cashier|Storekeeper}.

> **Attention!**
>
> a. The **db_name** structural element cannot be empty and must not match the existing standard user fields, because this disrupts the general logic of the *Access Manager* module and leads to failures and data loss.
> b. The **description** structural element cannot be empty because it is also the name of an additional field displayed in the *Access Manager* interface window; otherwise, it is ignored by the system.
> c. The **fmt** structural element must be one of a fixed set of modifiers (see Field formats with special processing). If a modifier not from the set is specified or the parameters (**prms**) are specified incorrectly, the field is processed by default according to its type (see Supported SQL data types).

9.2 Supported SQL data types

SQL data type	Representation	Default processing
BIT	Boolean	Drop-down list with Yes/No values
INTEGER Range (-2147483648; 2147483647)	Integer	Numeric field with increment/decrement and manual input option
SMALLINT Range: from -32768 to 32767, values outside the range aren't updated in the database		
DATETIME	DateTime	Calendar with date and time selection options

SQL data type	Representation	Default processing
CHAR The maximum size must be specified (example: 'CHAR, 30')	String	Text field
TEXT		

9.3 Field formats with a special processing

Format	Description	Syntax
C	A drop-down list with a predefined and fixed set of possible values. *Note. The type in the database can also be numeric, in which case the entire set of values must be numeric*	{C%value1|value2|...|valueN} Example: {C%Waiter|Cashier|Storekeeper|Security}
CT	A drop-down list where you can enter arbitrary values. The logic is similar to the C format, but it allows you to manually fill the field with text if necessary. It is used if the full list of possible values is too large, but there are few most frequently used options (they are predefined)	{CT%value1|value2|...|valueN} Example: {CT%Tokyo|Paris}
CCI	A drop-down list with predefined values and an option to generate events on saving. It is used if changes in key user parameters need to be logged in the database or "intercepted" by the Event Manager/script. It is recommended to make this field mandatory. *Note. The event is generated if the given user was saved after changing the field, and the event is not generated when new users are currently created. The event that was edited is generated for the Access Manager module object. To see this event in the Event Viewer or use it in the Event Manager, add these events to the Access Manager object in the DDI file of the Access Manager module*	{CCI%Descr1(EVENT1)|Descr2(EVENT2)|...|| DescrN(EVENTN)} Example: {CCI%Issued(CARD_ISSUED)| Lost(CARD_LOST)|Broken(CARD_BROKEN)}

Format	Description	Syntax
S	A numeric field with increment/decrement and manual input option. *Note. If a numeric data type is selected for a field in the database, then it is necessary to take into account the minimum and maximum values in accordance with the ranges in the syntax*	{S%0} or {S%min|max} Example 1: {S%0}—range of values: min -2147483648, max 2147483647 Example 2: {S%100|999}—range of values: min 100, max 999
U	This format is internal and cannot be used to generate additional fields	-
UT	A unique text with validation (checking for compliance with certain requirements) using a regular expression template. It is a convenient customization tool, but it requires technical knowledge in writing regular expressions. The text entered by the operator is checked against the template, and only if it matches the template can the field value be changed. Also, when saving a user, the uniqueness of the entered value is checked: there cannot be two users with the same value for this field	{UT%pattern_base64} Example: {UT%XlvQkNCS0JXQmtCc0J3QntCg0KHQotCj0KVdXGR7M31b0JDQktCV0JrQnNCd0J7QoNCh0KLQo9ClXXsyfVxkezIsM30k} The text encoded in Base64 format contains the following template (for the English version of the product): ^[A-Z]\d{3}-\d{3}-\d{2}-\d{3}-\d$. This template allows you to check the entry of a car license plate in the state of Florida: • F031-469-45-999-5—matches the template, • F 31-469 45-A99-5—does not match the template Advanced format options: • With an additional text masking during reading (masked only while reading user data). Example: {UT%MR|XjR7NX0k} The text encoded in Base64 format contains the 44444 template. • With an additional permanent text masking (always masked). Example: {UT%MA|XjR7NX0k} The text encoded in Base64 format contains the 44444 template

Format	Description	Syntax
TC	A non-unique text that contains predefined values, with the option to add new values. It allows you to supplement the set of text values as necessary and re-select values from the list. It can have a fixed set of predefined values. *Note. Before you edit a field, you must collect all variants of the value of this field from all users, eliminate the duplicates, and add values to the list of predefined values, if any. Therefore:* *1) If you want to remove a certain cached value from this list, you need to clear or change it for all users who have this value set in their fields.* *2) If you save a value with an error, it will be cached along with other values. That is, the options "bucket", "buc ket", "bUcket" or "buket" will end up in the cache and can appear in the list of available values*	{TC%EMPTY} or {TC%value1|value2|...|valueN} Example 1: {TC%EMPTY}—no predefined values. Example 2: {TC%Engineer|Medic|Accountant}
TL	A text with a limited length. *Note. It is necessary to make sure that the field type in the database does not exceed the allowed length. The example above requires TEXT or CHAR, 10 (or more)*	{TL%length} Example: {TL%10}—the line length is limited to 10 characters
RO	An arbitrary readonly field. It is used, for example, to display data when importing users from an external system or if this field is filled in with a script when manual input by the operator is prohibited. *Note. This format is similar to the normal text field, which is used in the Access Manager by default and marked as "Read Only". The difference is that this field remains non-editable even if it is marked as editable. It also has a default value*	{RO%def_value} Example: {RO%Not specified}

9.4 Creating additional fields for the **User** object

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

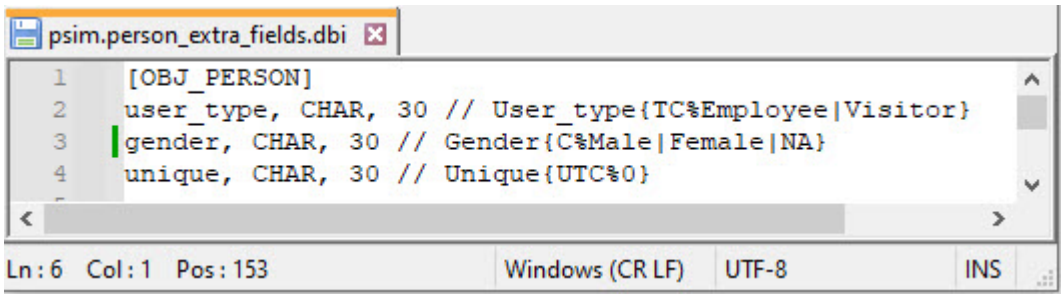
1. In the *Axxon PSIM* installation directory, for example, **C:\Program Files (x86)\Axxon PSIM** create a .dbi text document, for example, **psim.person_extra_fields.dbi**.
2. Open the created .dbi file in the text editor.

   > **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:
   a. Separated by commas, enter the field name (**db_name**) that will be saved in the database, the field data type (**db_type**) with the maximum field size, if required—see Supported SQL data types.
   b. Using a double slash "**//**", indicate the field description (**description**) that will be displayed in the interface window of the *Access Manager*.
   c. If necessary, set the field behavior pattern by indicating the beginning and end using curly braces "**{ }**".
5. Save the changes.

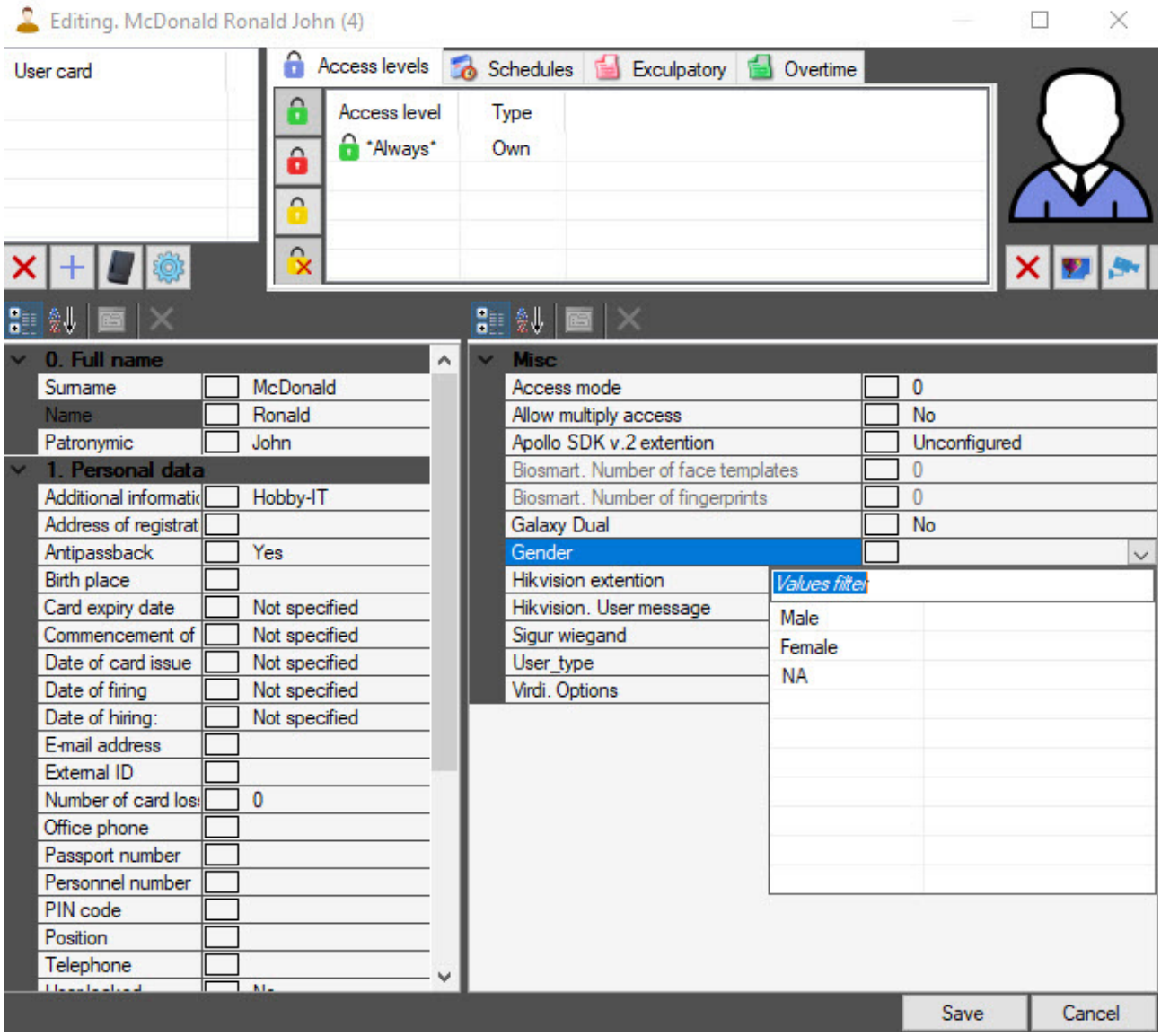
   > **Attention!**
   >
   > After you save the .dbi file, it is necessary to update the main database. To do this, use the idb.exe utility (see The idb.exe utility for converting databases, selecting database templates and making backup copies of databases).

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



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 the Main department type).

In the interface window of the **Access Manager**, in the area of additional fields, the corresponding additional fields will be displayed depending on the configured visibility and availability of fields for editing, as well as the specified category.



9.5 Basic structural elements of the additional field of the **User** object

Indication	Description
db_name	The additional field name (db_name) that is saved in the database
db_type	Data type (db_type) of the additional field, size (if required, see Supported SQL data types)
description	Name of the additional field displayed in the **Access Manager** interface window
fmt	A modifier from the set (see Field formats with special processing)

Indication	Description
prms	Field value parameters, entered using parentheses ()
{	Beginning of the behavior template of the additional field
%	After the %, the names of the predefined values of the additional field are listed. *Note. If you specify %EMPTY, there will be no predefined values*
value1, valueN	Names of predefined values of the additional field
|	Separation of predefined values of the additional field
length	Limit of the line length
def_value	Default value
}	End of the behavior template of the additional field

Creating additional fields for the **User** object is complete.

10 Appendix 4. Creating a single photo database

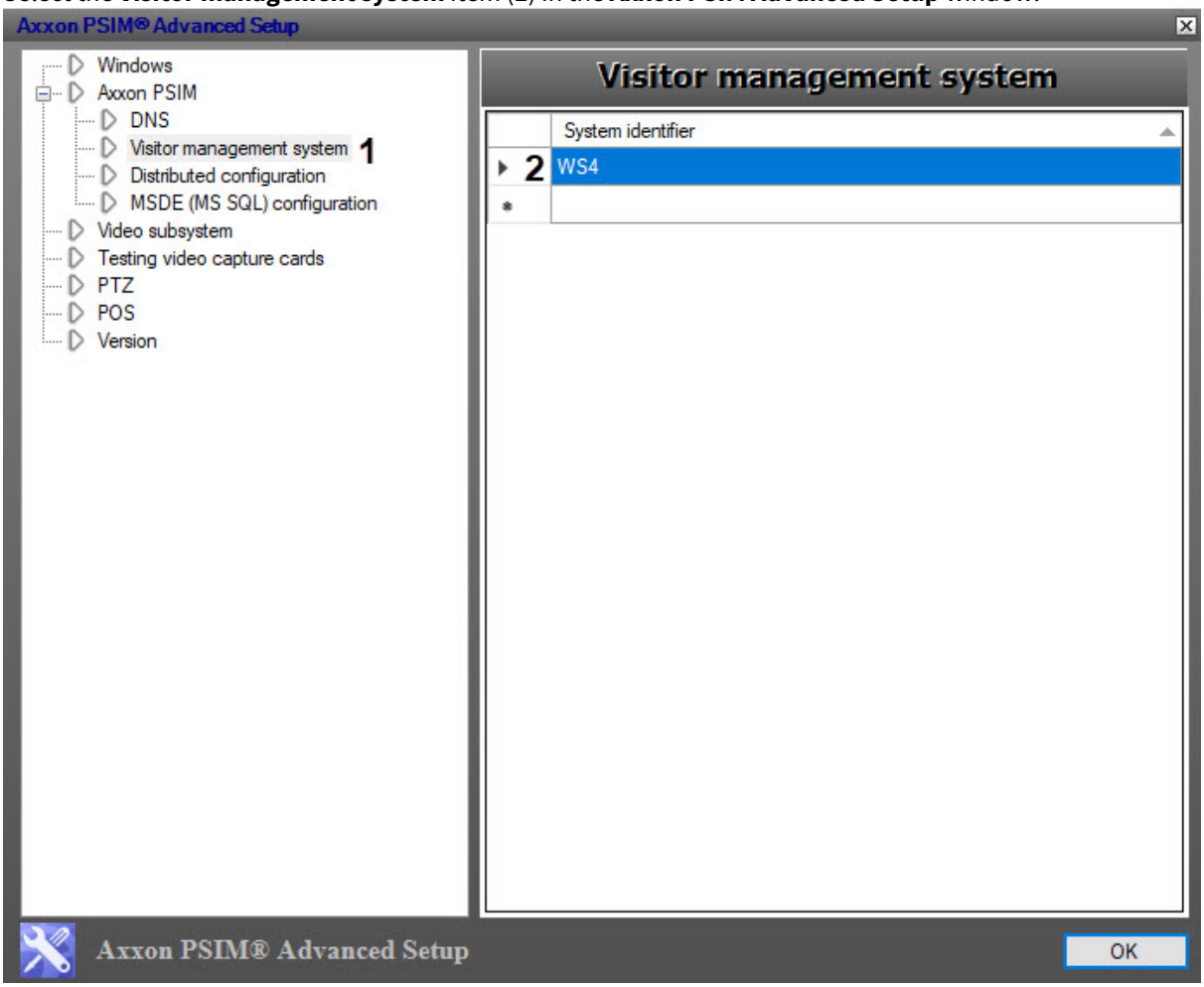
ACFA PSIM supports storing user photos on several computers.

ACFA PSIM advanced settings utility tweaki.exe is used to create a single photo database. There are two ways to launch the tweaki.exe utility:

1. From the Windows **Start** menu: **Start** → **All Programs** → **Axxon PSIM** → **Utilities** → **Advanced settings utility**.
2. From the **Tools** folder of *ACFA PSIM* installation directory: <*Axxon PSIM* installation directory>\Tools\tweaki.exe.

To create a single photo database, do the following:

1. Select the **Visitor management system** item (**1**) in the **Axxon PSIM Advanced Setup** window.



2. In the **System identifier** column (**2**), enter the names of the Servers/RAWs that will store the photos assigned to users using the *Access Manager* module.

> **Note**
>
> The specified Servers/RAWs must be connected to the *Axxon PSIM* Server to which photos from *Access Manager* are added. Detailed information about configuring server connections is given in 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 photos assigned to users via the *Access Manager* module will be sent to the specified computers. Photos added to the system before the photo database was formed won't be sent.

> **Note**
>
> Photos will be stored not only on the computers specified using the tweaki.exe utility, but also on the computer from which the photos are sent. The added photos are stored in the *<Axxon PSIM* installation directory>\Bmp\Person folder.

3. Click the **OK** button.

11 Appendix 5. Face synchronization module

11.1 General information about the Face synchronization module and its licensing

The *Face synchronization* module is used to automatically synchronize the users of the *Access Manager* module who have photos with the *Face PSIM* reference face database (see 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 photo to a user in the *Access Manager* module.
2. Automatically change a 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.

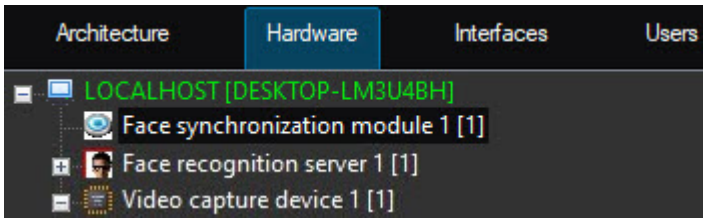
> **Attention!**
>
> In case you create users in the *Face PSIM* database using the **Face recognition and search** interface object (see Adding images to the reference face database), the correct synchronization of faces is not guaranteed.

Module licensing

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

11.2 Activation of the Face synchronization module

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

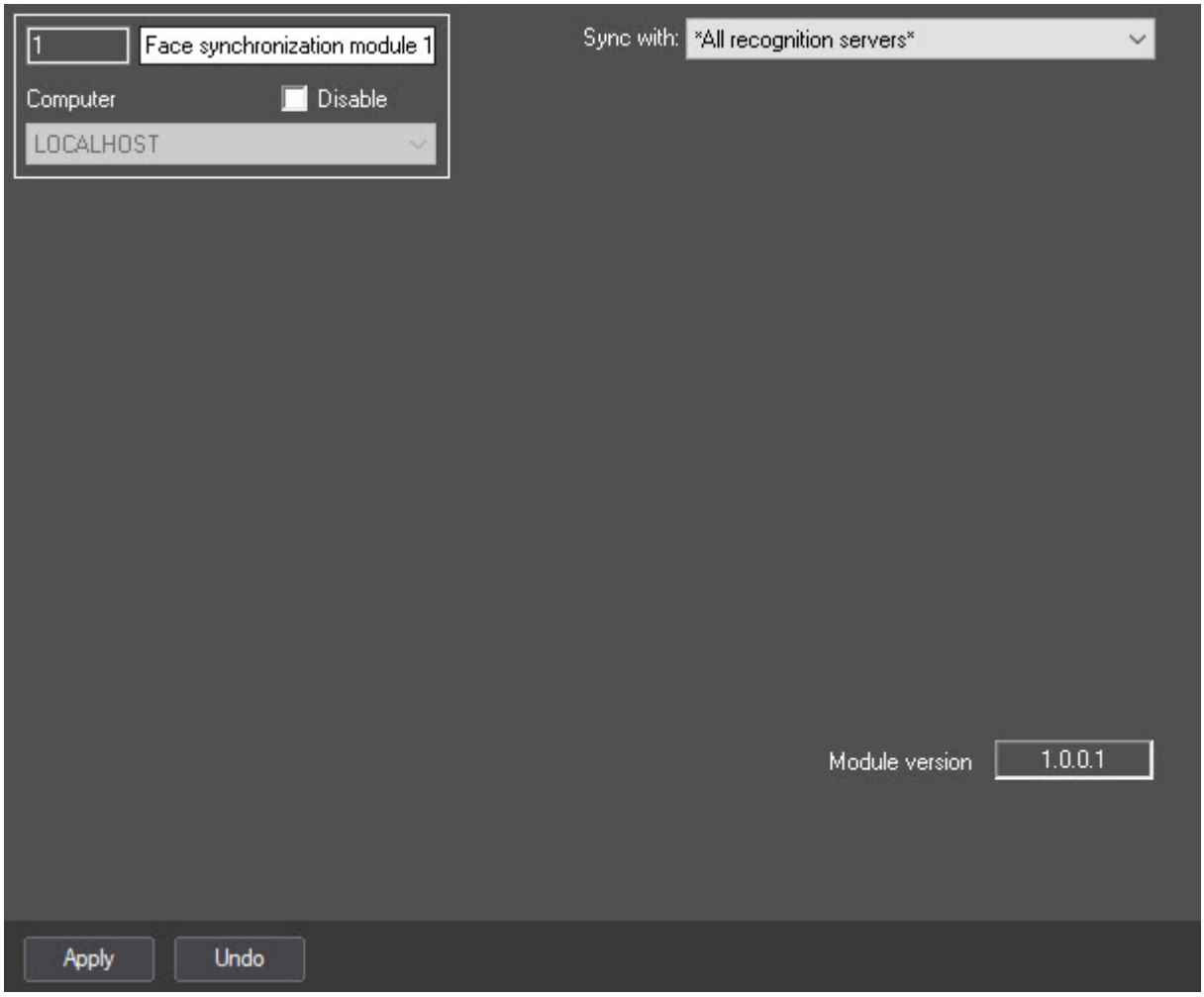


11.3 Configuring the Face synchronization module

On the page:

11.3.1 Selecting the Face Recognition Server for synchronization

You can select the Face Recognition Server with which user faces will be automatically synchronized on the settings panel of the **Face synchronization module** object.



1. From the **Synch with** drop-down list, select the required Face Recognition Server. If you select the **All recognition servers** value, faces will be synchronized with all Face Recognition Servers in the distributed system.
2. Click the **Apply** button to save the changes.

11.3.2 Selecting the Face Recognition Server 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 settings panel of the *Access Manager* module (see Configuring control readers in the Access Manager).

Configuring the *Face synchronization* module is complete.

12 Appendix 6. Additional features of Access Manager module

12.1 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 photo to a user from a 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 PSIM*.

1. Go to the *<Axxon PSIM* 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

```
    <applicationSettings>
        <RunModule.account_manager_run.Properties.Settings>
            <setting name="CommonBackground" serializeAs="String">
                <value>206, 206, 255</value>
            </setting>
            <setting name="ControlsBackground" serializeAs="String">
                <value>244, 247, 252</value>
            </setting>
            <setting name="FormsBackground" serializeAs="String">
                <value>215, 228, 242</value>
            </setting>
            <setting name="SettingsBackground" serializeAs="String">
                <value>AliceBlue</value>
            </setting>
            <setting name="ScanifyAPIEnabled" serializeAs="String">
                <value>False</value>
            </setting>
            <setting name="AutoCropFrame" serializeAs="String">
                <value />
            </setting>
            <setting name="NotifyInitialPhoto" serializeAs="String">
                <value>True</value>
            </setting>
        </RunModule.account_manager_run.Properties.Settings>
    </applicationSettings>
</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.

13 Appendix 7. Script for printing templates

On the page:

13.1 General information about scripts

For the description of objects and programming methods necessary for developing scripts in *Axxon PSIM*, see Guide for creating scripts (programming).

13.2 Script for printing a template

In the *Access Manager* module, you can print templates from several printers at the same time using a script.

Script for printing a template looks like this:

```
DoReactStr("AM","1","EXTERNAL_PRINT","person_id<>,template_path<>,target_slave<>,target_device<>");
```

Parameters:

- AM—the *Access Manager* module that you use,
- 1—id of the *Access Manager* module that you use,
- person_id<>—id of the user for whom you want to print a template,
- template_path<>—path to the template file for printing,
- target_slave<>—slave device (computer) that you use,
- target_device<>—name of the printer as it is displayed in the **Devices and Printers** section of the OS settings.

You can print templates from several printers at the same time if printers have the last saved settings that are the same for all devices, for this:

1. All printers belonging to the same *Access Manager* module must be the same (one driver).
2. All printers belonging to the same *Access Manager* module are installed in the system (visible in the OS).

Example of a script for printing a template:

```
DoReactStr("AM","1","EXTERNAL_PRINT","person_id<3>,template_path<D:\AxxonTemplate.axt>,target_slave<A-KING>,target_device<Microsoft Print to PDF>");
```