Hikvision Integration Module Configuration and Operation Guide

ACFA PSIM 1.1

Last update 05/03/2024

Table of Contents

1 List of terms used in the Hikvision Integration Module Configuration and Operation Guide

Access Control System (ACS) is a hardware and software suite for selective restriction of access to a certain site or area.

Server is a computer that hosts the **Server** version of *Axxon PSIM*.

Hikvision ACS Controllers are electronic devices that monitor and manage access points.

Reader is an electronic device that enters user credentials into the ACS.

Passing time is a time interval for the user passing through the access point under normal operating conditions. After passing time expires, the access point is blocked automatically.

Access point is a location where granting access is electronically controlled. An access control point can be a door, turnstile, gate or barrier equipped with a reader, an electromechanical lock, and/or other means of access control.

Time zone is a set of time intervals within each day of a time cycle (1 to 366 days), as well as time intervals during specific dates. Time zones determine the access schedule to the protected facility.

2 Introduction into the Hikvision Integration Module Configuration and Operation Guide

On the page:

2.1 The purpose of this document

The *Hikvision Integration Module Configuration and Operation Guide* is a reference guide for *Hikvision* integration module configuration specialists. This module is a part of *ACFA PSIM*.

This document contains the following information:

1. General information on the *Hikvision* integration module.
2. Configuring the *Hikvision* integration module.
3. Operating the *Hikvision* integration module.

2.2 General information on the Hikvision integration module

The *Hikvision* integration module is a part of *ACFA PSIM* and used to perform the following functions:

1. Configuration of the *Hikvision* ACS and connected Hikvision readers.
2. Communcation between the *Hikvision* ACS and *ACFA PSIM* for monitoring and management.

Note

For detailed information on the *Hikvision* ACS, refer to the official documentation for this device on the manufacturer's website.

Before you start configuring the *Hikvision* Integration module, do the following:

1. Install *Hikvision* hardware on the protected facility (refer to the official *Hikvision* ACS installation manual);
2. Connect the *Hikvision* ACS to the *ACFA PSIM* Server (refer to the most recent version of the *Hikvision* module official documentation).

3 Supported hardware and licensing of the Hikvision module

Manufacturer	Hikvision USA 18639 Railroad Street, City of Industry, California 91748 Tel: +1-909-895-0400 Toll Free: +1-866-200-6690 (U.S. and Canada only) Technical Support: tel: 909-612-9039 or email: techsupport.usa@hikvision.com Sales: sales.usa@hikvision.com http://www.hikvision.com/us/
Integration type	SDK
Hardware connections	Ethernet, RS-485

Supported hardware

Hardware	Function
DS-K26x and DS-K28x series controllers, where **x** is the number of doors supported (for example, DS-K2602, DS-K2804)	Access controller
DS-KVx series call panels, where **x** is the second part of the name of the call panel (for example, DS-KV8102-IP)	Call panel
DS-K1T605x, DS-K1T606x, DS-K1T671x, DS-K5603x access control terminals, where **x** is the version. All other Hikvision terminals are also supported	Access control terminal

Module licensing

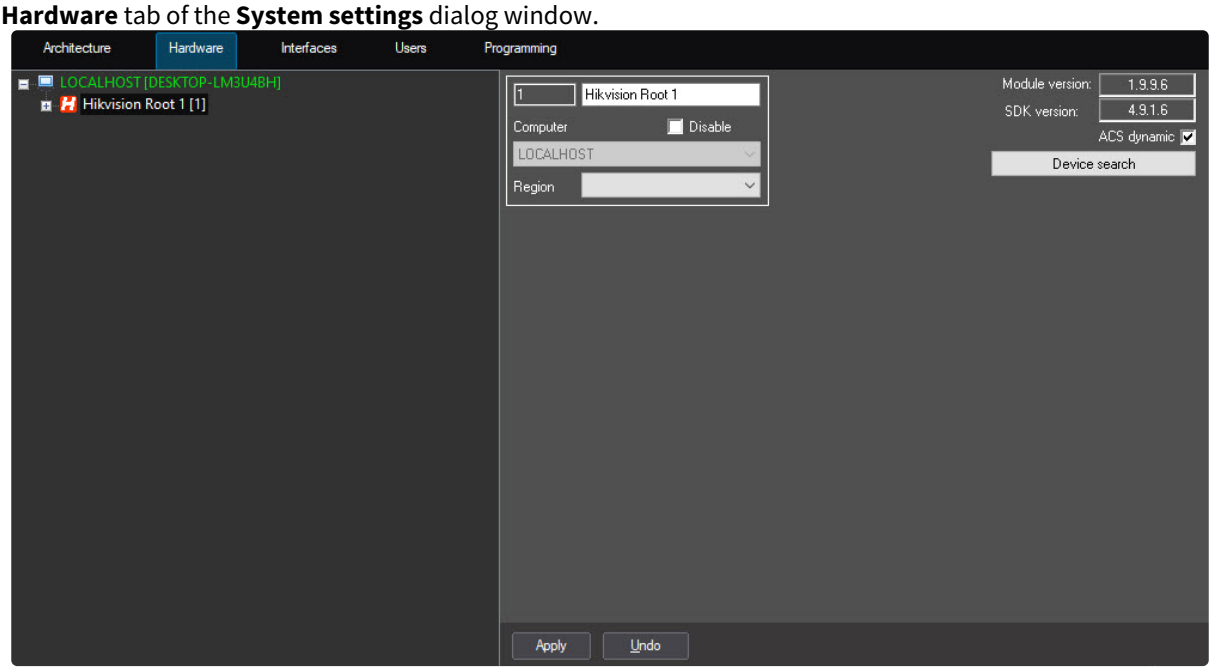
Per 1 controller/terminal.

4 Configuring the Hikvision integration module

4.1 Configuring the Hikvision parent object

To configure the *Hikvision* parent object, do the following:

1. Go to the settings panel of the **Hikvision Root** object created on the basis of the **Computer** object on the **Hardware** tab of the **System settings** dialog window.

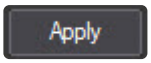


2. Set the **ACS dynamic** 

checkbox to automatically send any changes to employees, access control or time schedule to the corresponding *Hikvision* controllers.
3. Click the **Device search** 

button to find all *Hikvision* devices connected to the Server and automatically build the hardware tree.

> **Note**
>
> For the device search to work, you must install the manufacturer's SADP utility beforehand.

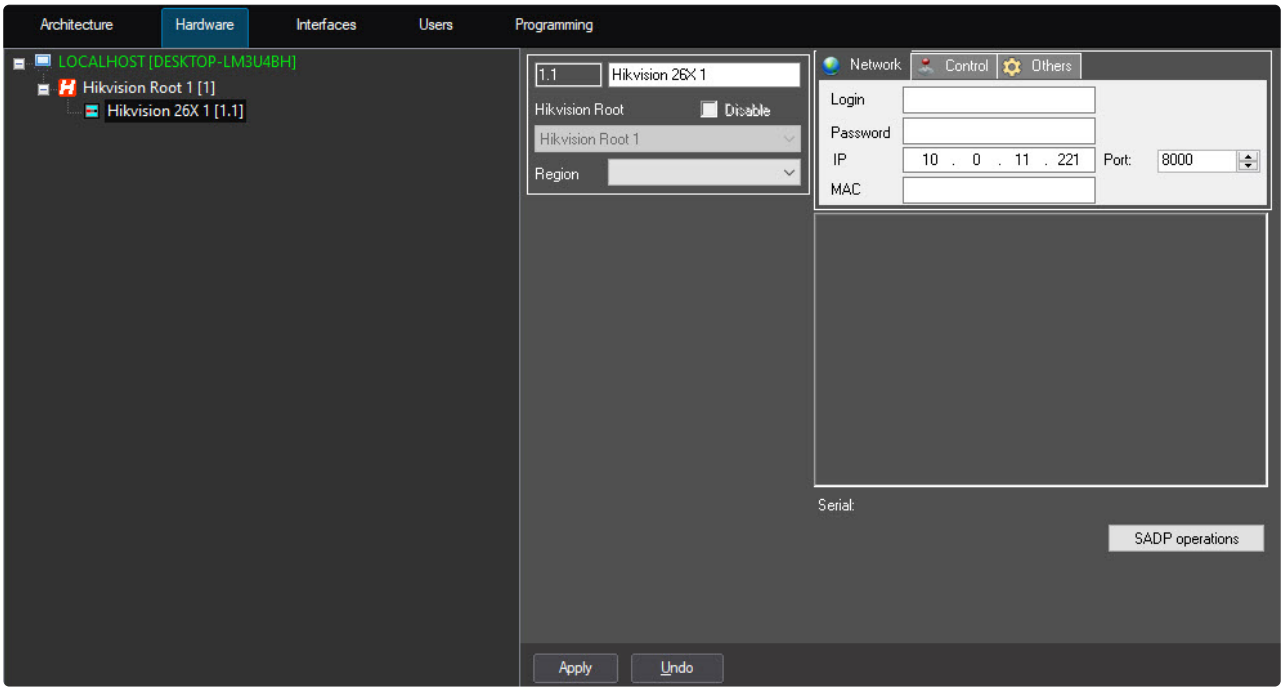
4. Click the **Apply** 

button to save the settings.

4.2 Configuring the Hikvision controller/terminal

> **Note**
>
> Configuration of the *Hikvision* controller/terminal will be illustrated by an example of the Hikvision DS-K26x series controller. You can configure other *Hikvision* controllers/terminals in the similar way.

You can configure the *Hikvision* controller on the settings panel of the **Hikvision 26X** object that is created on the basis of the **Hikvision Root** parent object.

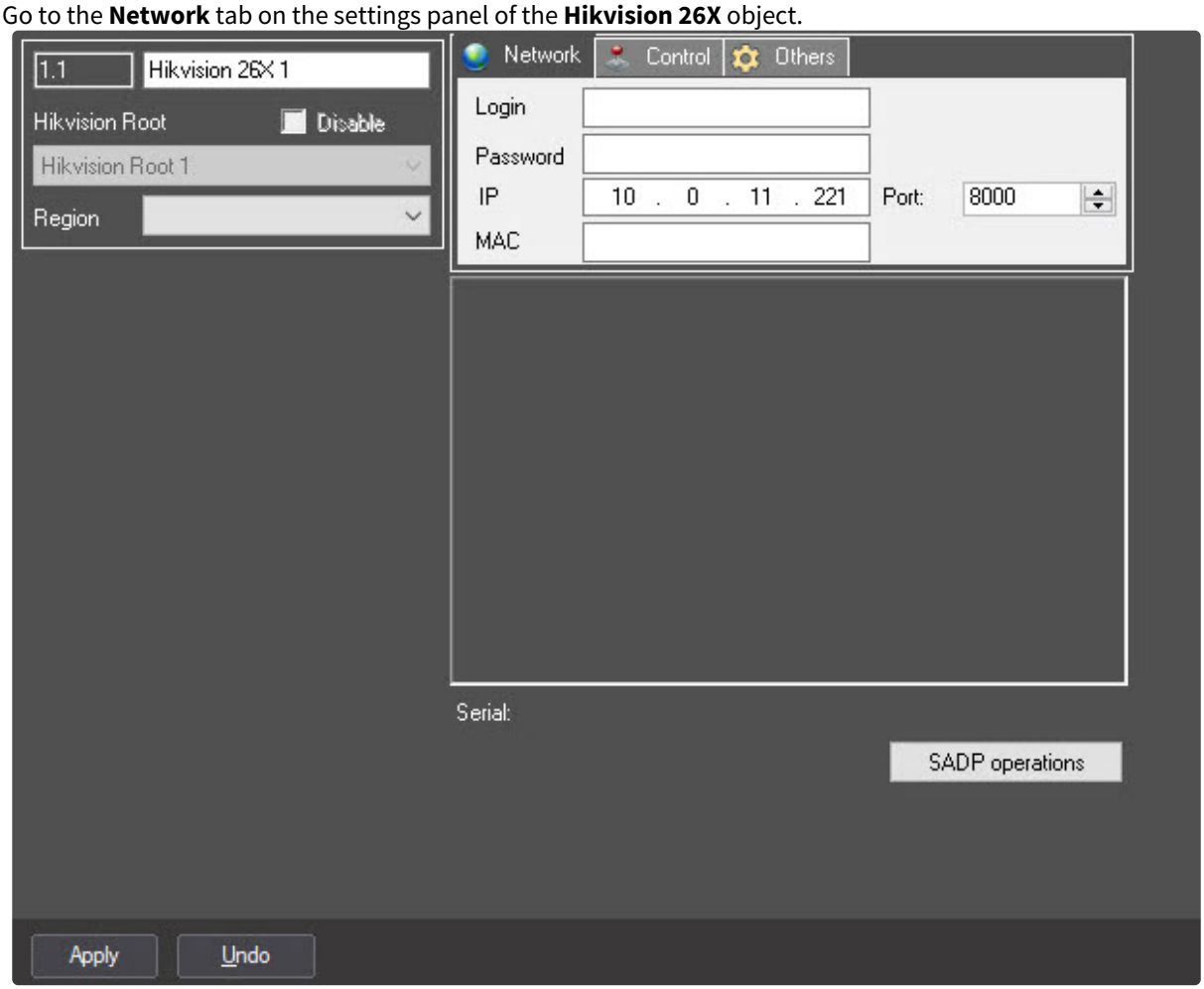


4.2.1 Network settings of the Hikvision controller/terminal

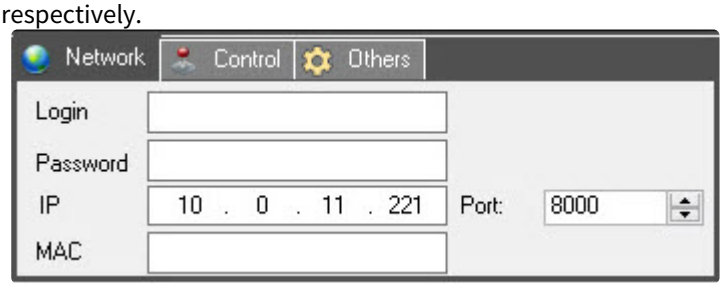
> **Note**
>
> The network settings of the *Hikvision* controller/terminal will be illustrated by an example of the Hikvision DS-K26x series controller. You can configure the network settings of other *Hikvision* controllers/terminals in the similar way.

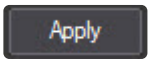
To configure the network settings of the *Hikvision* controller, do the following:

1. Go to the **Network** tab on the settings panel of the **Hikvision 26X** object.



2. In the **Login** and **Password** fields, enter the login and password to connect the *Hikvision* controller, respectively.



3. In the **IP**, **Port** and **MAC** fields, enter the IP address, connection port and MAC address of the *Hikvision* controller. If you added the device using the **Device search** button (see Configuring the Hikvision parent object), these fields will fill in automatically.
4. Click the **Apply** 

button to save the network settings. As a result, an objects tree corresponding to the configuration of the *Hikvision* controller will be created.

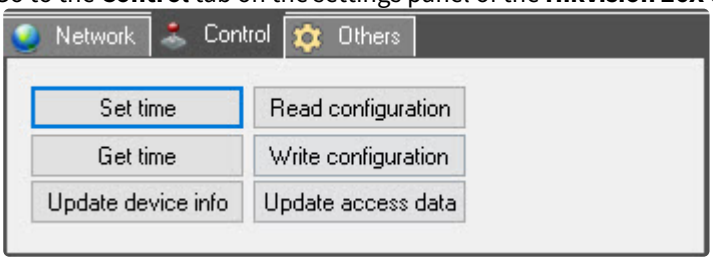
> **Note.**
>
> If the connection to the device is successful, the **Device information** blank area below the **Network**, **Control** and **Others** tabs will display information on this controller.

4.2.2 Managing the configuration of the Hikvision controller/terminal

> **Note**
>
> Configuration management of the *Hikvision* controller/terminal will be illustrated by an example of the Hikvision DS-K26x series controller. You can manage the configuration of other *Hikvision* controllers/terminals in the similar way.

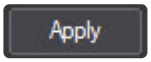
To manage the configuration of the *Hikvision* controller, do the following:

1. Go to the **Control** tab on the settings panel of the **Hikvision 26X** object.



2. Click the **Set time** button to set the current computer time in the *Hikvision* controller.
3. Click the **Get time** button to get the current time of the *Hikvision* controller.
4. Click the **Update device info** button to update the information about the controller in the **Device information** area.
5. Click the **Read configuration** button to read the configuration of the *Hikvision* controller.
6. Click the **Write configuration** button to write the current configuration into the controller. The user photos assigned using the *Access Manager* module (see Assigning a photograph to a user in the Access Manager software module) are also written to the access control terminals. These photos are used as face templates (see Adding the Hikvision face template).

   > **Note**
   >
   > Write the current configuration into the *Hikvision* controller after each change made to the controller configuration.

7. Click the **Update access data** button to update access levels in the *Hikvision* controller.
8. Click the **Apply** 

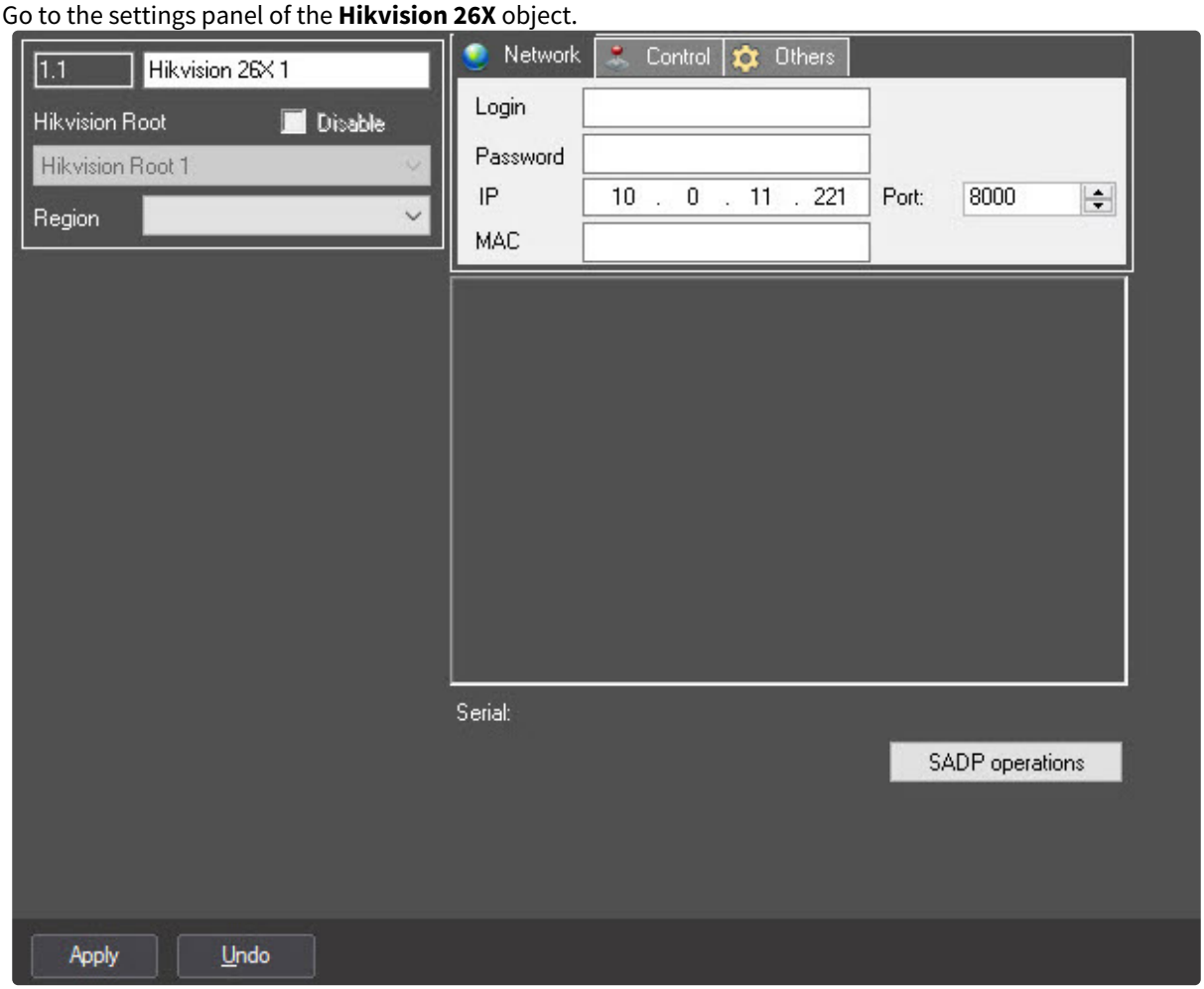
button to save the settings.

4.2.3 Hikvision SADP settings

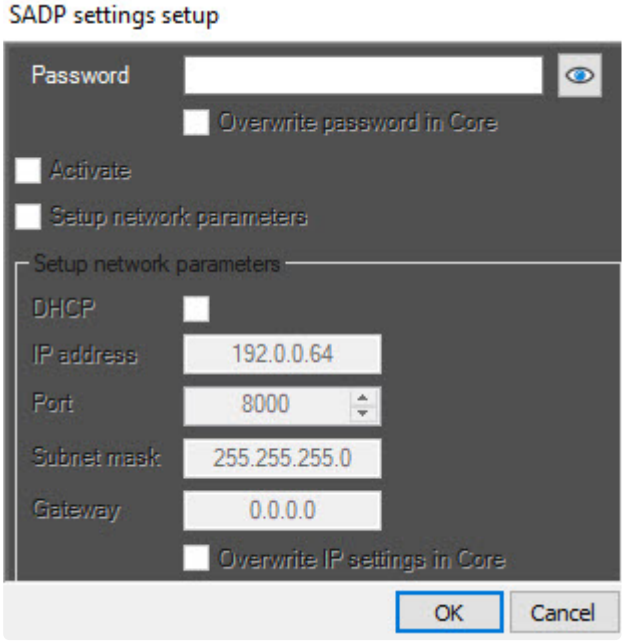
> **Note**
>
> The SADP settings of the *Hikvision* controller will be illustrated by an example of the Hikvision DS-K26x series controller. You can configure the SADP settings of other *Hikvision* controllers/terminals in the similar way.

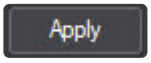
To configure the *Hikvision* SADP, do as follows:

1. Go to the settings panel of the **Hikvision 26X** object.



2. Click the **SADP operations**  button. The **SADP settings setup** window will open.



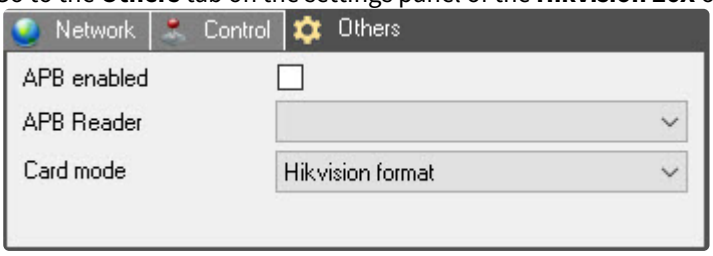
3. In the **Password** field, enter a new password for the *Hikvision* controller.
4. Set the **Overwrite password in Core** checkbox to automatically overwrite the old password in ACFA *PSIM* with the new one, otherwise you need to do it manually (see Network settings of the Hikvision controller/terminal).
5. Set the **Activate** checkbox to activate the controller in case it has been reset to factory settings. The password entered on step 3 becomes the master password for the *Hikvision* controller.
6. Set the **Setup network parameters** checkbox to enable changing the network settings.
7. Set the **DHCP** checkbox to enable DHCP.
8. In the **IP address** field, enter the new IP address of the *Hikvision* controller.
9. In the **Port** field, enter a new connection port number of the *Hikvision* controller.
10. In the **Subnet mask** field, specify the mask for a subnet in which the *Hikvision* controller will be located.
11. In the **Gateway** field, specify the connection gateway of the *Hikvision* controller.
12. Set the **Overwrite IP settings in Core** checkbox to automatically overwrite the old network settings in ACFA *PSIM,* otherwise you need to do it manually (see Network settings of the Hikvision controller/terminal).
13. Click the **OK** button to save the SADP settings.
14. Click the **Apply** 

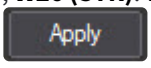
button on the settings panel of the *Hikvision* controller to save the changes.

4.2.4 Advanced settings of a Hikvision controller/terminal

> **Note**
>
> The advanced settings of the *Hikvision* controller/terminal will be illustrated by an example of the Hikvision DS-K26x series controller. You can configure the advanced settings of other *Hikvision* controllers/terminals in the similar way.
> Advanced settings are not available for the *Hikvision KV* series call panels, such as DS-KV8102-IP.

To configure the advanced settings of the *Hikvision* controller, do the following:

1. Go to the **Others** tab on the settings panel of the **Hikvision 26X** object.


2. Set the **APB enabled** checkbox to enable the anti-passback monitoring.
3. From the **APB Reader** drop-down list, select the starting reader for the anti-passback monitoring.
4. From the **Card mode** drop-down list, select the supported format of the access card: **Hikvision format** (default), **W26 (STR)**. **W26 (DEC)**. **W32 (STR)**. **W32 (DEC)**, **Mifare**.
5. Click the **Apply** 

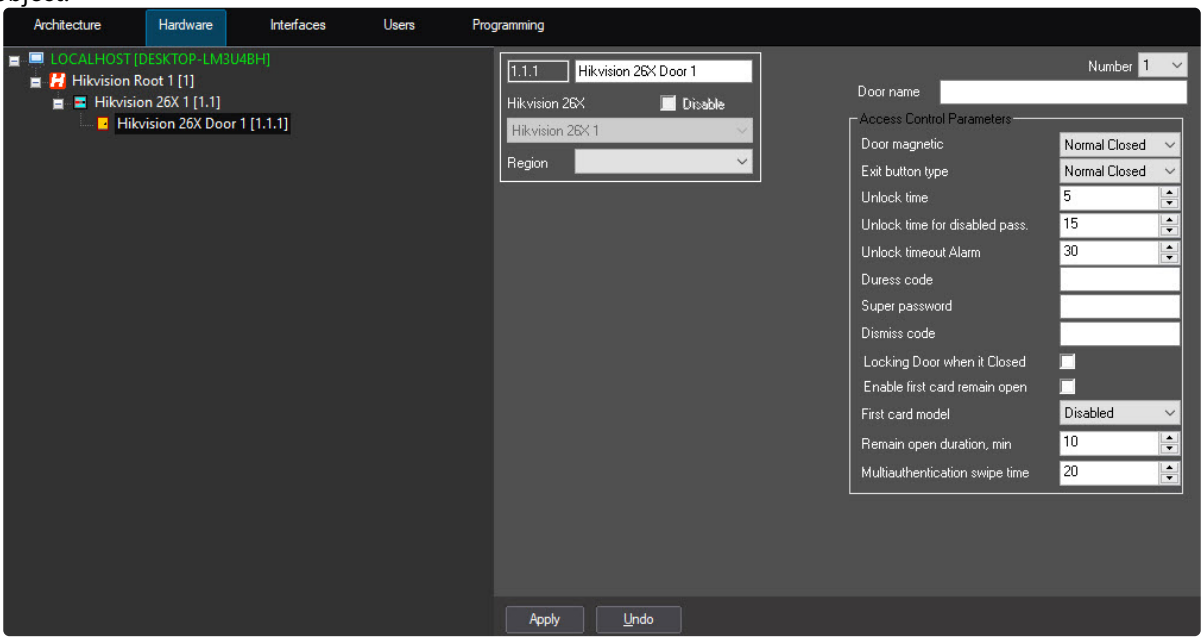
button.

4.3 Configuring the Hikvision door

> **Note**
>
> The *Hikvision* door configuration options depend on the *Hikvision* controller/terminal model. The *Hikvision* door configuration will be illustrated by an example of the Hikvision DS-K26x series controller.

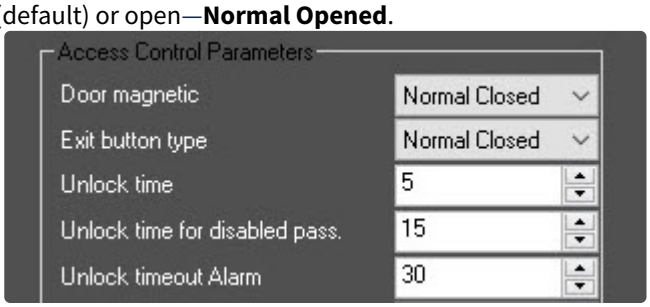
To configure the *Hikvision* door, do the following:

1. Go to the settings panel of the **Hikvision 26X Door** object that is created on the basis of the **Hikvision 26X** object.



2. From the **Number** drop-down list, select the number corresponding to the door number in the *Hikvision* controller.

3. In the **Door name** field, enter the name of the door that will be displayed in *ACFA PSIM* during further readings of the *Hikvision* controller configuration.
4. From the **Door magnetic** drop-down list, select which door state is a normal state: closed—**Normal Closed** (default) or open—**Normal Opened**.



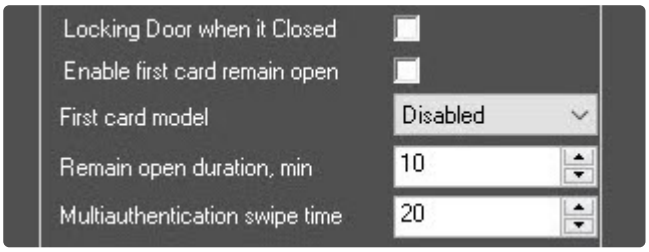
5. From the **Exit button type** drop-down list, select the exit button type: normally closed—**Normal Closed** (default) or normally open—**Normal Opened**.
6. In the **Unlock time** field, enter the time in seconds after which the unlocked door will be locked again.
7. In the **Unlock time for disabled pass** field, enter the time during which the door will be opened for users who have the **Disabled** card type.
8. In the **Unlock timeout Alarm** field, enter the time in seconds after which an alarm will be initiated if the door wasn't closed.

9. In the **Duress code** field, enter the duress code for opening the door by an employee under duress. The duress alarm will be initiated. The duress code must consist of four to eight digits.

10. In the **Super password** field, enter the super password that can be used to open this door. The super password must consist of four to eight digits.

> **Note**
>
> **Duress code** and **Super password** must be different from each other and from the authentication password.

11. In the **Dismiss code** field, enter the dismiss code that can be used to disable the card readers of this door. The dismiss code must consists of four to eight digits.
12. Set the **Locking Door when it Closed** checkbox if you want to lock the door immediately after closing it. If the checkbox is clear, the door will be locked after the **Unlock time** time expires (see step 6). By default, the checkbox is clear.



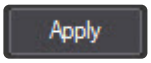
13. Set the **Enable first card remain open** checkbox if you want to use the first card model. By default, the checkbox is clear.

> **Note**
>
> You can set several first cards for one door. The door will be available for other users with any authorization type only after the first card is swiped.

14. From the **First card model** drop-down list, select the first card model: **Disabled**, **Normal Open** or **Authorization**.
    a. **Disabled**—disables the first card model.
    b. **Normal Open**—when the first card is swiped, the door remains open for the time specified in the **Remain open duration, min** field (see step 15).
    c. **Authorization**—any kind of authentication (except for super card, super password and duress card/code authentication) is accepted only after the first card is authorized.

> **Note**
>
> The first card authorization is valid for the current day only. The authorization expires in 24 hours on the current day. Re-swipe the same first card to disable the first card model.

15. In the **Remain open duration, min** field, enter the time in minutes during which the door remains open after the first card is swiped with the **Normal Open** model. The default value is 10 minutes.
16. In the **Multiauthentication swipe time** field, enter the maximum time between card reading/password entry and other authentication methods when using a multiple card configuration (see Configuring multiple Hikvision cards).

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

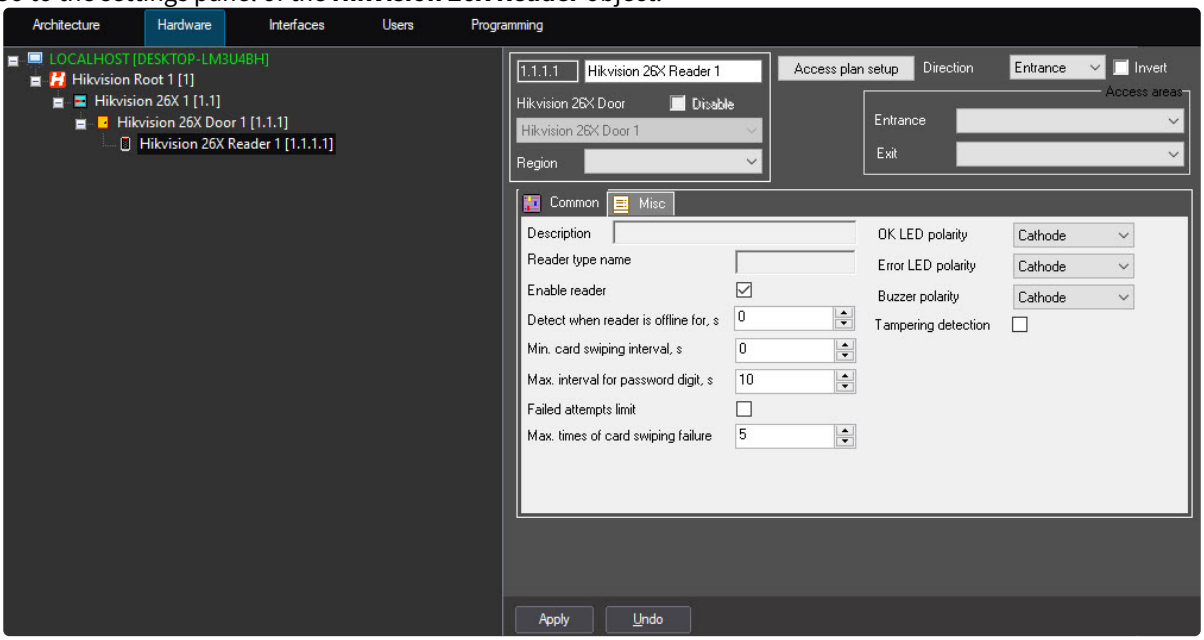
4.3.1 Configuring the Hikvision reader

> **Note**
>
> The *Hikvision* reader configuration options depend on the *Hikvision* controller/terminal model. The *Hikvision* reader configuration will be illustrated by an example of the Hikvision DS-K26x series controller.

Common settings of the Hikvision reader

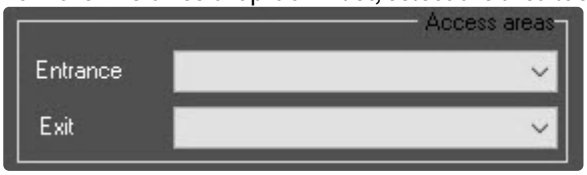
To configure the common settings of the *Hikvision* reader, do the following:

1. Go to the settings panel of the **Hikvision 26X Reader** object.



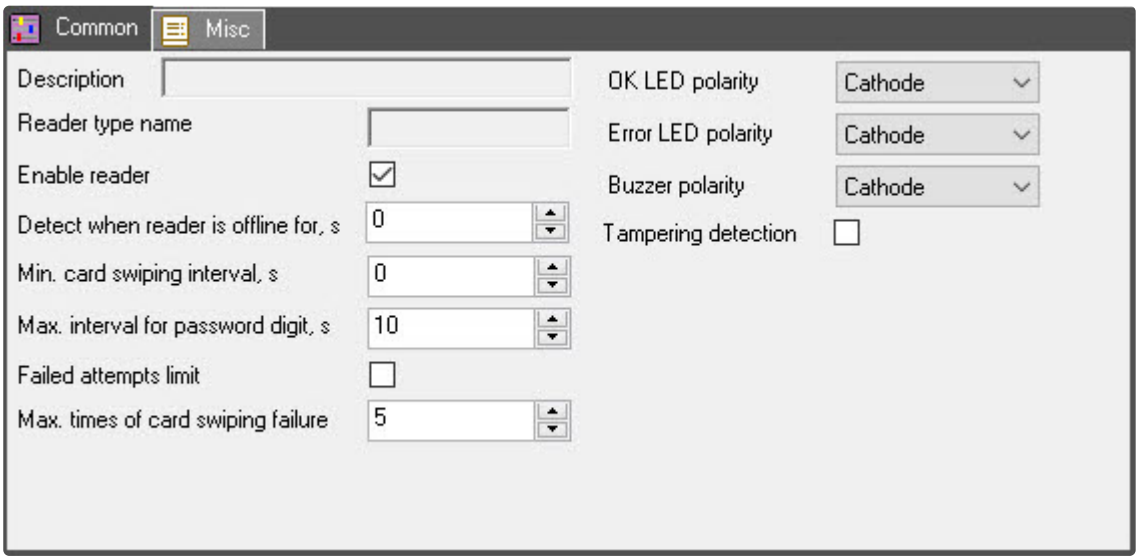
2. From the **Direction** drop-down list, select the direction of access through the reader: **Exit** or **Entrance**.

3. Set the **Invert** checkbox to enable the inverted (reverse) entrance. By default, the checkbox is clear.
4. From the **Entrance** drop-down list, select the area located on the exit side of the door.



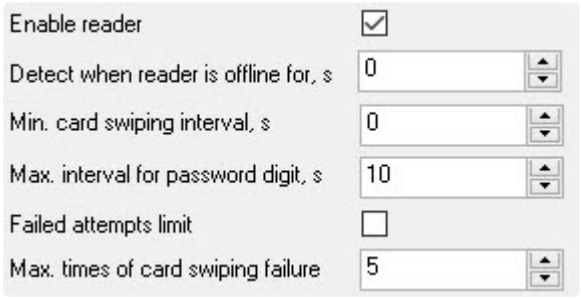
5. From the **Exit** drop-down list, select the area located on the entry side of the door.

6. Go to the **Common** tab.



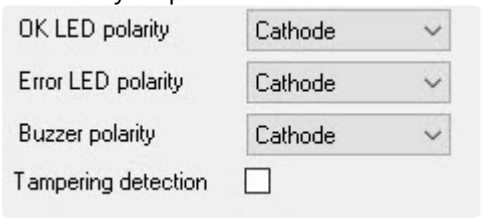
7. The **Description** field displays a description of the reader. You cannot edit this field.

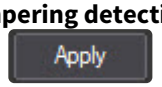
8. The **Reader type name** field displays the name of the reader type. You cannot edit this field.
9. Set the **Enable reader** checkbox to enable the reader.



10. In the **Detect when reader is offline for, s** field, specify the time in seconds, after which the reader will turn off when the connection with the *Hikvision* controller is lost.
11. In the **Min. card swiping interval, s** field, specify the minimum time in seconds in the range from 0 to 255 seconds, during which the repeated card swiping will be invalid.
12. In the **Max. interval for password digit, s** field, specify the time interval in seconds between two digits when entering the password on the reader. If the time interval between pressing two digits exceeds the specified value, all previously entered digits will be automatically cleared.
13. Set the **Failed attempts limit** checkbox if you want to generate an alarm when the number of card swiping attempts exceeds the number specified in the **Max. times of card swiping failure** field.
14. In the **Max. times of card swiping failure** field, enter the number of card swiping attempts, after exceeding which an alarm will be generated if the **Failed attempts limit** checkbox is set.

15. From the **OK LED polarity** drop-down list, select the polarity of the reader's buzzer when the card is successfully swiped.



16. From the **Error LED polarity** drop-down list, select the polarity of the reader's buzzer when the card isn't successfully swiped.
17. From the **Buzzer polarity** drop-down list, select the polarity of the reader's buzzer.
18. Set the **Tampering detection** checkbox to detect unauthorized access to the reader.
19. Click **Apply**  button.

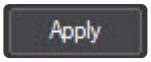
Additional settings of the Hikvision reader

To configure the additional settings of the *Hikvision* reader, do the following:

1. Go to the **Misc** tab on the settings panel of the **Hikvision 26X Reader** object.

2. Set the **Connected by RS485** checkbox if the reader is connected through the RS-485 interface.
3. Set the **Control reader** checkbox if it is necessary to assign the code from this reader to the employee in the *Access Manager* module when issuing a card.

> **Note**
>
> Make sure to select the *Hikvision* door to which the reader is connected on the **Readers** tab in the settings of the *Access Manager* module (see Access Manager Module Settings and Operation Guide).

4. Click the **Apply**  button.

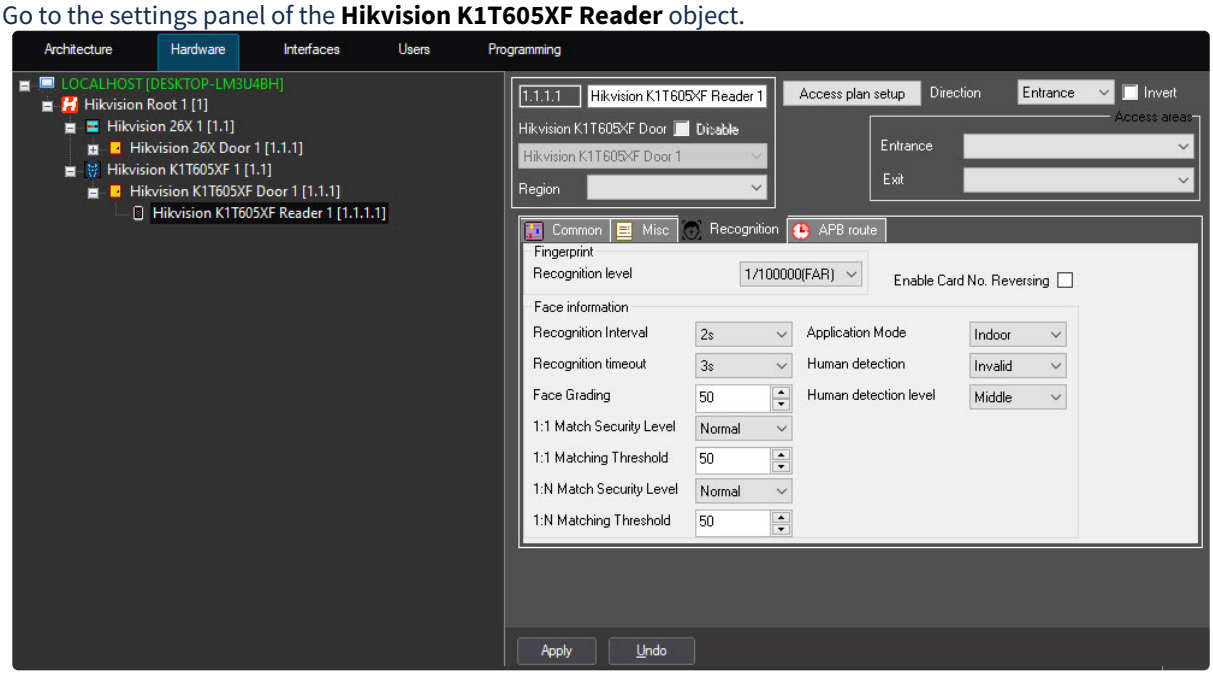
Recognition settings of the Hikvision reader

Recognition settings of the *Hikvision* reader are available for access control terminals that have both a face scanner and a built-in fingerprint reader.

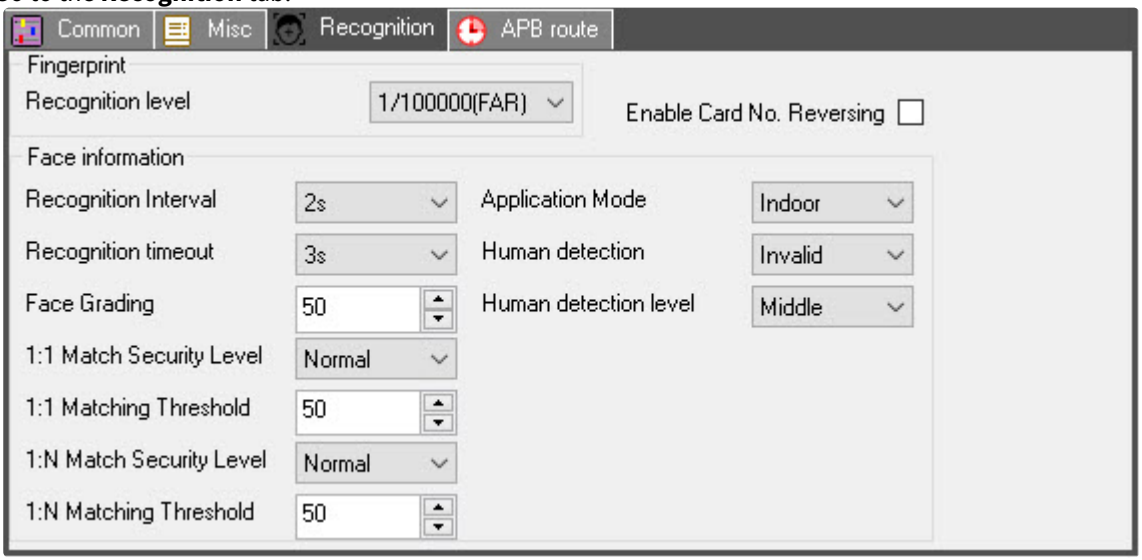
> **Note**
>
> Recognition settings of the *Hikvision* reader will be illustrated by an example of the Hikvision DS-K1T605MF access control terminal. You can configure the recognition settings of a reader of other *Hikvision* terminals in the similar way.

To configure the recognition settings of the *Hikvision* reader, do the following:

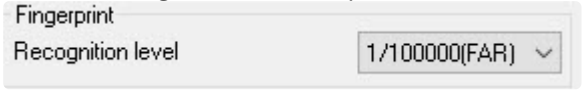
1. Go to the settings panel of the **Hikvision K1T605XF Reader** object.



2. Go to the **Recognition** tab.



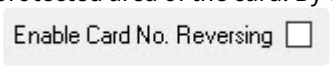
3. From the **Recognition level** drop-down list, select the recognition level:



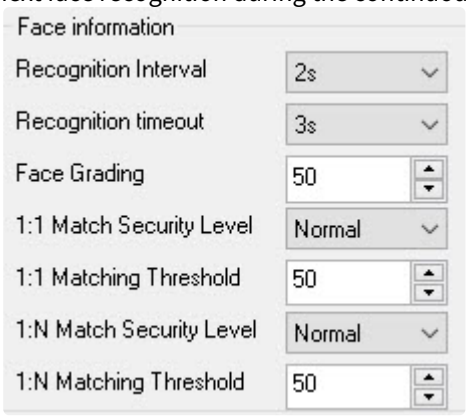
- **1/1000(FAR)**.
- **1/100000(FAR)**.
- **1/1000000(FAR)**.
- **3/100000(FAR)**.
- **3/1000000(FAR)**.

> **Note**
>
> The higher the recognition level, the lower the probability of false identification.

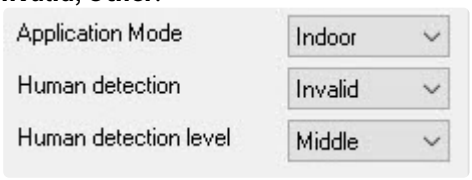
4. Set the **Enable Card No. Reversing** checkbox to enable the ability to read the information from the protected area of the card. By default, the checkbox is clear.

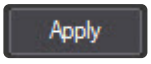


5. From the **Recognition Interval** drop-down list, select the time interval in seconds between the previous and next face recognition during the continuous operation in the range from 1 to 10. The default value is **2s**.



6. From the **Recognition timeout** drop-down list, select the time in seconds in the range from 1 to 20, after which the connection with the *Axxon PSIM* Server is broken if there is no recognition. The default value is **3s**.
7. In the **Face Grading** field, specify the minimum acceptable image quality for face recognition in percent. The default value is **50%**.
8. From the **1:1 Match Security Level** drop-down list, select the verification quality level if only one type of authentication is used: **Normal**, **High**, or **Higher**.
9. In the **1:1 Matching Threshold** field, specify the maximum allowable variation from the **1:1 Match Security Level** value if only one type of authentication is used. The default value is **50%**.
10. From the **1:N Match Security Level** drop-down list, select the verification quality level if several types of authentication are used: **Normal**, **High**, or **Higher**.
11. In the **1:N Matching Threshold** field, specify the maximum allowable variation from the **1:N Match Security Level** value if several types of authentication are used. The default value is **50%**.
12. From the **Application Mode** drop-down list, select the application mode of the *Hikvision* reader: **Indoor**, **Invalid**, **Other**.



13. From the **Human detection** drop-down list, select if the detection of live faces is used: **Invalid** (default), **Disable**, **Enable**.
14. From the **Human detection level** drop-down list, select the level of human recognition: **Invalid**, **Low**, **Middle**, **High**.
15. Click the **Apply** 

button.

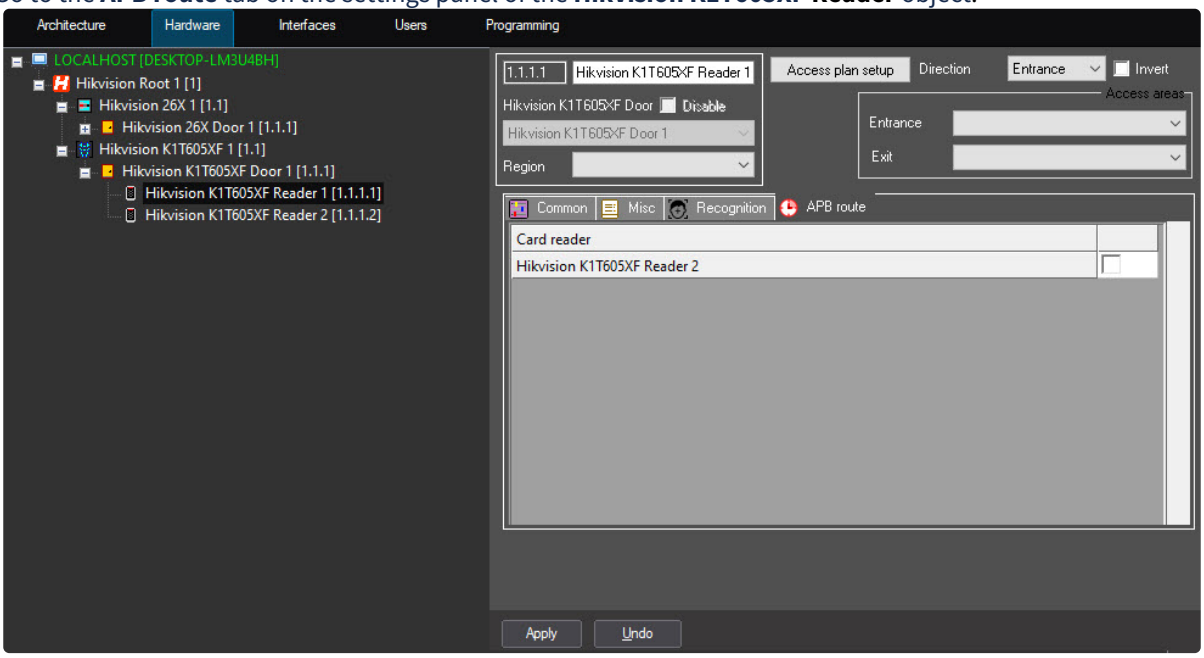
Anti-passback settings of the Hikvision reader

Configuring the anti-passback of the *Hikvision* reader is available only for the access control terminals. To configure the anti-passback, do the following:

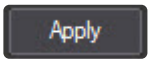
> **Note**

Anti-passback settings of the *Hikvision* reader will be illustrated by an example of the Hikvision DS-K1T605MF access control terminal. You can configure the anti-passback settings of a reader of other *Hikvision* terminals in the similar way.

1. Go to the **APB route** tab on the settings panel of the **Hikvision K1T605XF Reader** object.



2. In the list of readers, set the checkboxes next to those readers for which you want to set the anti-passback control.

3. Click the **Apply** 

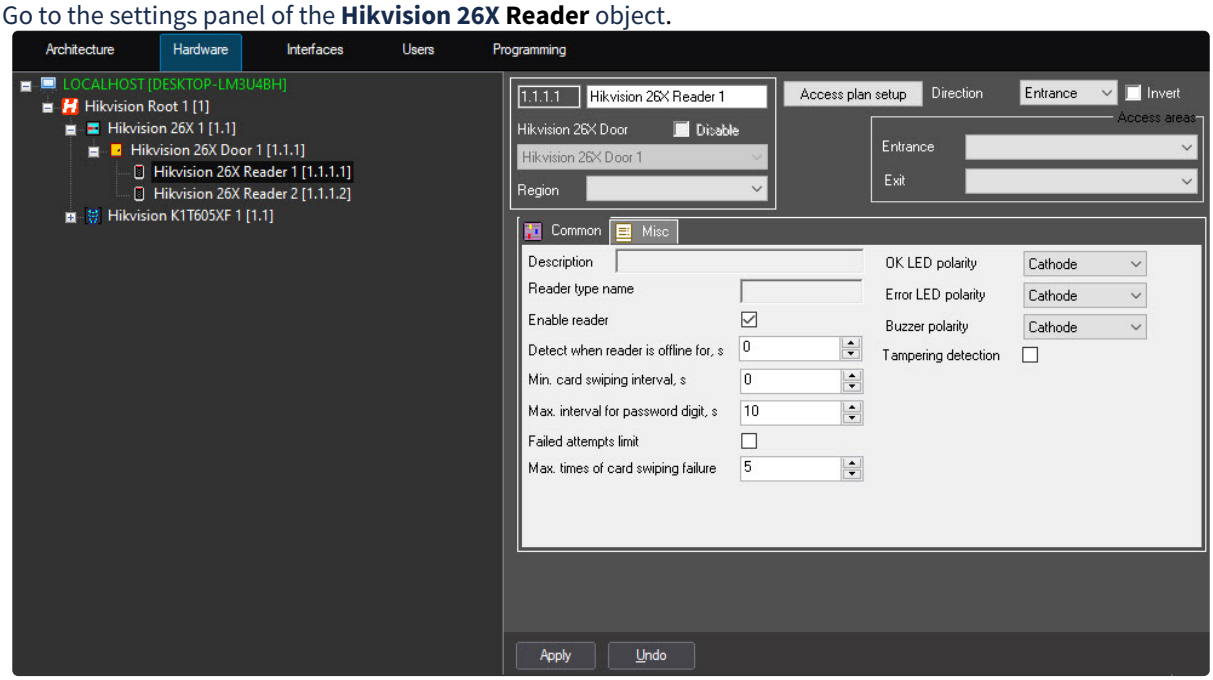
button to save the settings.

Access plan settings of the Hikvision reader

> **Note**
>
> Access plan configuration of the *Hikvision* reader will be illustrated by an example of the Hikvision DS-K26x series controller. You can configure readers of other *Hikvision* controllers/terminals in the similar way.

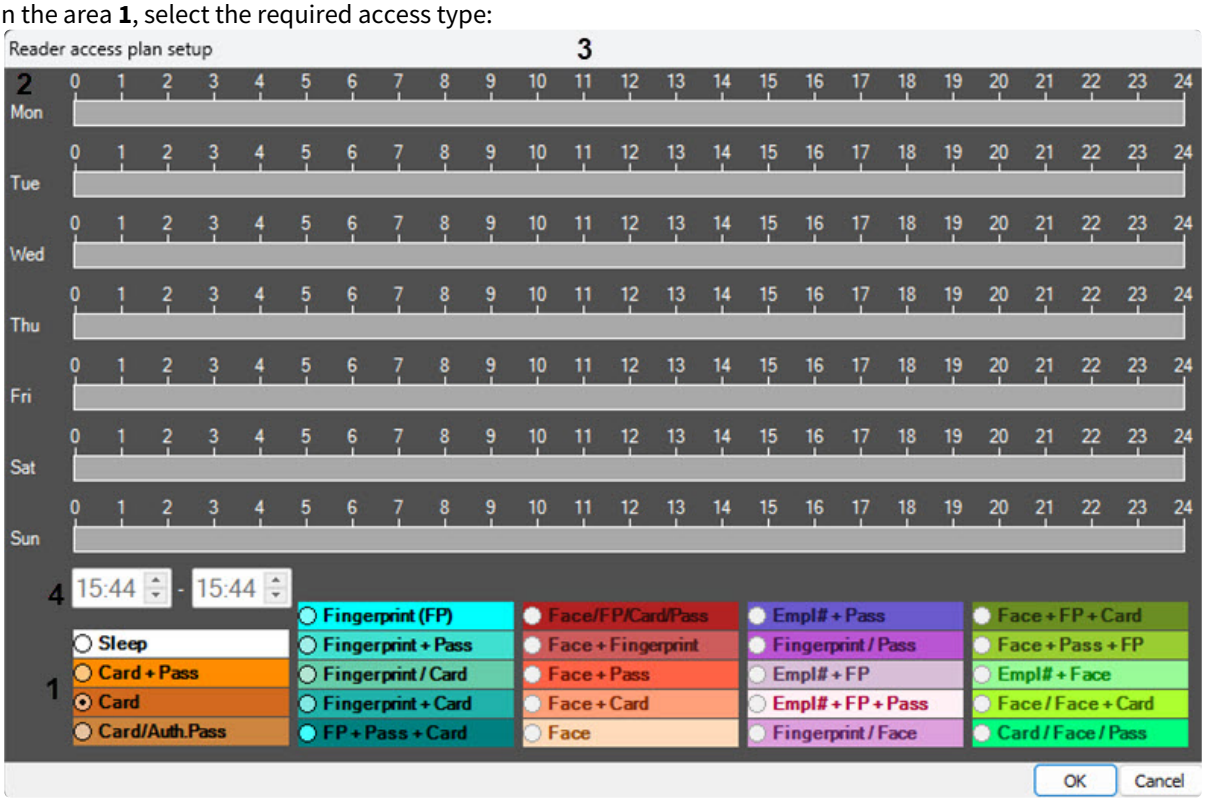
To configure the access plan of the *Hikvision* reader, do the following:

1. Go to the settings panel of the **Hikvision 26X Reader** object.



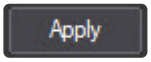
2. Click the **Access plan setup**  button. The **Reader access plan setup** window will open.

3. In the area **1**, select the required access type:



   a. **Sleep**—sleep mode. If you select this mode, the reader won't operate.
   b. **Card + Pass**—first you need to swipe the card and then enter the password, only then the access will be granted.
   c. **Card**—you need to swipe the card, after that the access will be granted.

d. **Card/Auth.Pass**—you can either swipe the card or enter the password to access.

4. In the column **2**, select the day of the week, and using the mouse, set the time interval for this access type in the corresponding line in the area **3**.
5. If necessary, adjust the time interval in the area **4**, where the left field indicates the beginning time, and the right field indicates the ending time of this time interval.
6. Click the **OK** button to save the changes and return to the settings panel of the *Hikvision* reader.
7. Click the **Apply** 

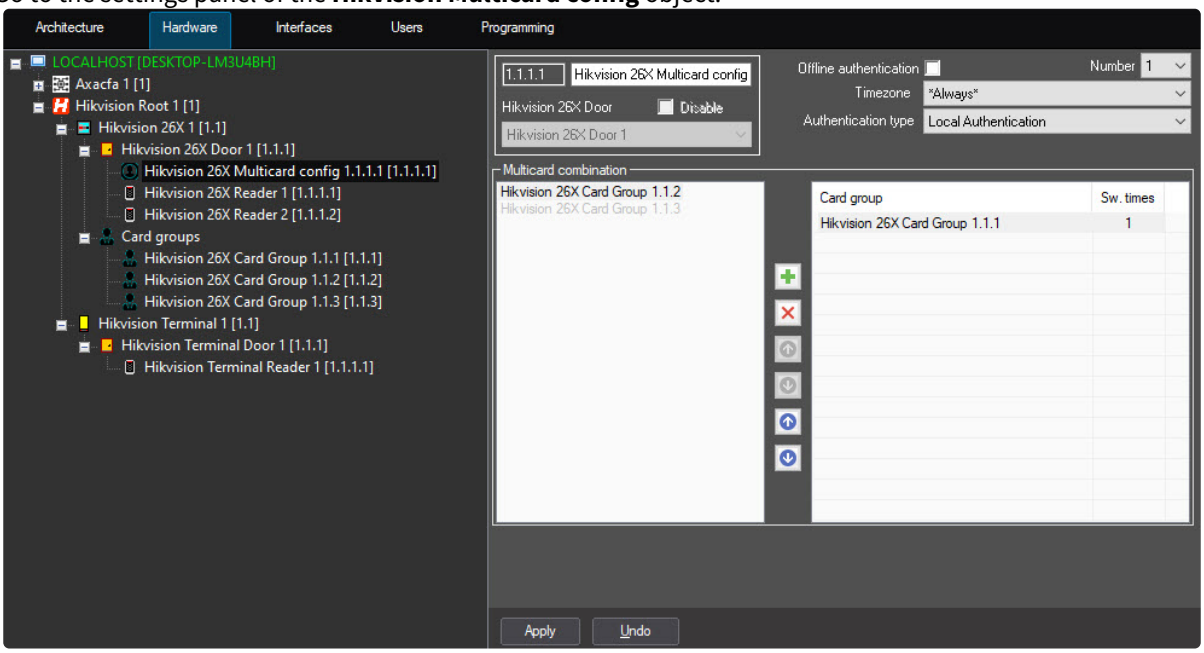
button on the settings panel of the reader.

4.3.2 Configuring multiple Hikvision cards

> **Note**
>
> The ability to configure multiple *Hikvision* cards depends on the *Hikvision* controller/terminal model. Configuration of multiple *Hikvision* cards will be illustrated by an example of the Hikvision DS-K26x series controller.
> You must configure *Hikvision* card groups beforehand (see Configuring the Hikvision card groups).

To configure multiple *Hikvision* cards, do the following:

1. Go to the settings panel of the **Hikvision Multicard config** object.

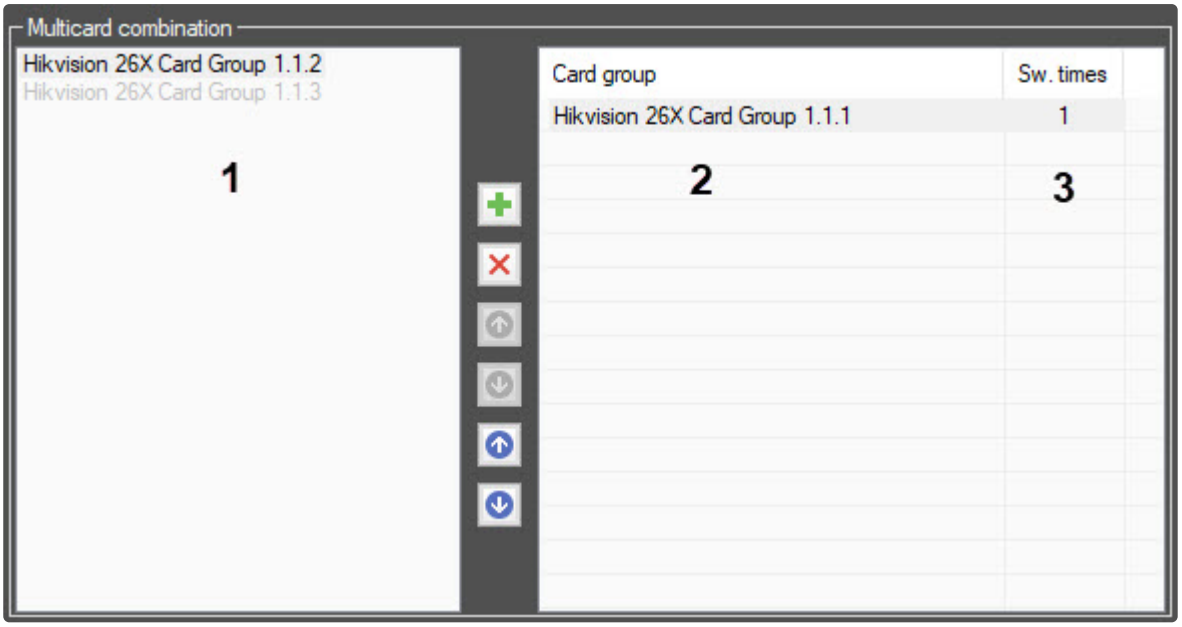


2. Set the **Offline authentication** checkbox to enable authentication using **Super Password** when the access point is offline.

3. From the **Number** drop-down list, select the configuration number from **1** to **20** corresponding to the configuration number in the *Hikvision* controller.
4. From the **Timezone** drop-down list, select a time zone.
5. From the **Authentication type** drop-down list, select the authentication type:

a. **Local Authentication**—to access, you need to present only the required identifiers (cards). You can add up to eight card groups to this authentication type.
b. **Local Auth. and Remotely Open**—after you present identifiers, an operator will receive a request for remote opening. You can add up to seven card groups to this authentication type.
c. **Local Auth. and Super Password**—to access, you need to present identifiers and then enter the **Super Password**.

6. To add a card group to the **Card group** column (**2**), select a group in the **Multicard combination** area (**1**) and click the button.



7. To remove a group from the **Card group** column (**2**), select the required group and click the button.
8. Use the and buttons to move a card group within the **Card group** column (**2**).
9. Use the and buttons to change the number of different card swipes required for granting access in the **Sw. times** column (**3**).

> **Note**
>
> The maximum time between card readings/password entries and other authorization methods must not exceed the time specified in the **Multiauthentication swipe time** field (see Configuring the Hikvision door).

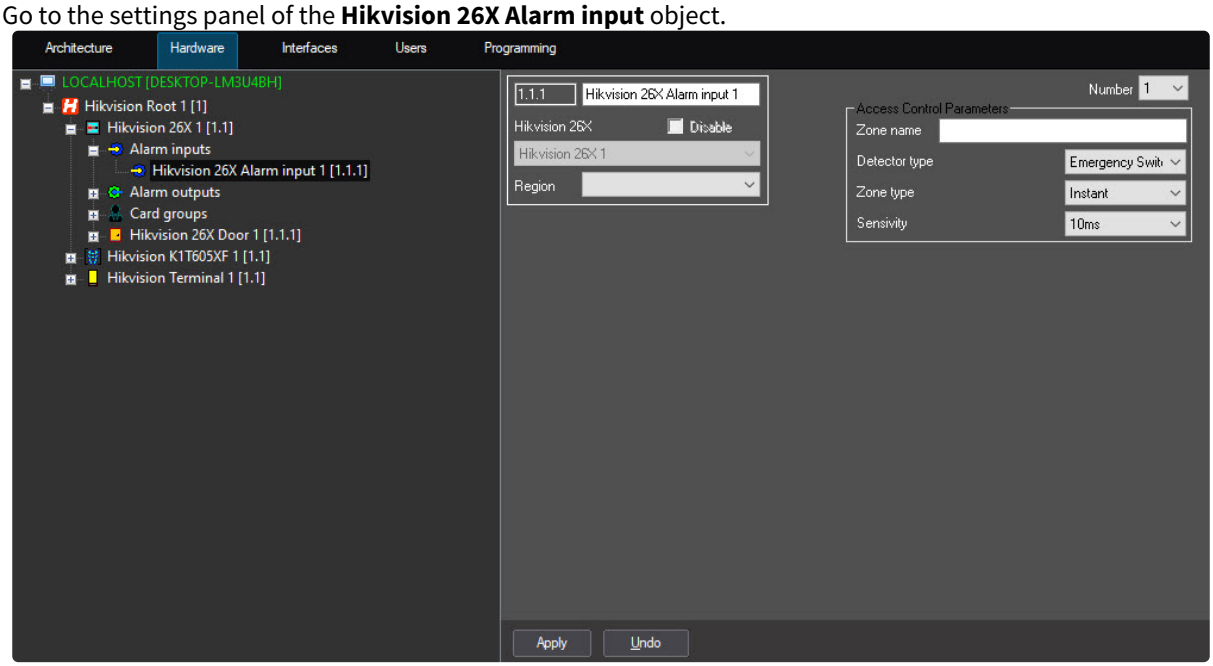
10. Click the **Apply** button.

4.4 Configuring the Hikvision alarm input

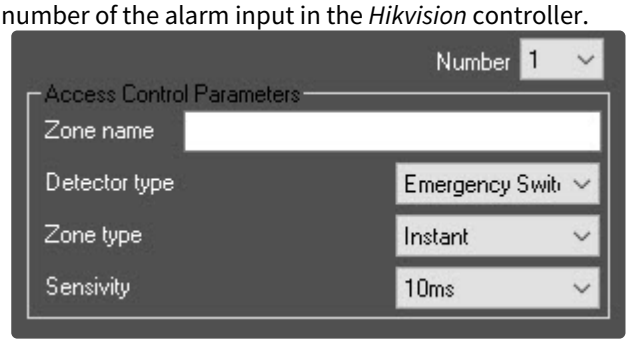
> **Note**
>
> *Hikvision* alarm input configuration options depend on *Hikvision* controller/terminal model. Configuration of the *Hikvision* alarm input will be illustrated by an example of the Hikvision DS-K26x series controller.

To configure the *Hikvision* alarm input, do the following:

1. Go to the settings panel of the **Hikvision 26X Alarm input** object.

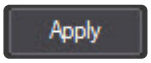


2. From the **Number** drop-down list, in the range from 1 to 4, select the number that corresponds to the number of the alarm input in the *Hikvision* controller.



3. In the **Zone name** field, enter the name of the alarm input that will be displayed in *Axxon PSIM* during subsequent readings of the controller configuration.
4. From the **Detector type** drop-down list, select the detector type:
   a. **Emergency Switch**—emergency switch detector (default).
   b. **Door Magnetic**—door magnetic detector.
   c. **Smoke**—smoke detector.
   d. **Active Infrared**—active infrared detector.
   e. **Passive Infrared**—passive infrared detector.
   f. **Glass Break**—glass break detector.
   g. **Vibration**—vibration detector.
   h. **Dual Tech. PIR**—Dual Technology PIR detector.
   i. **Triple Tech. PIR**—Triple Technology PIR detector.
   j. **Humidity**—humidity detector.
   k. **Temperature**—temperature detector.
   l. **Combustible Gas**—combustible gas detector.
   m. **Other Detector**—other detector.
5. From the **Zone type** drop-down list, select the zone type:
   a. **Instant**—instant zone (default).
   b. **24 Hours**—permanent zone.
   c. **Door Emg. open**—open emergency door zone.

d. **Door Emg. shutdown**—shutdown emergency door zone.
e. **Shield zone**—protected zone.

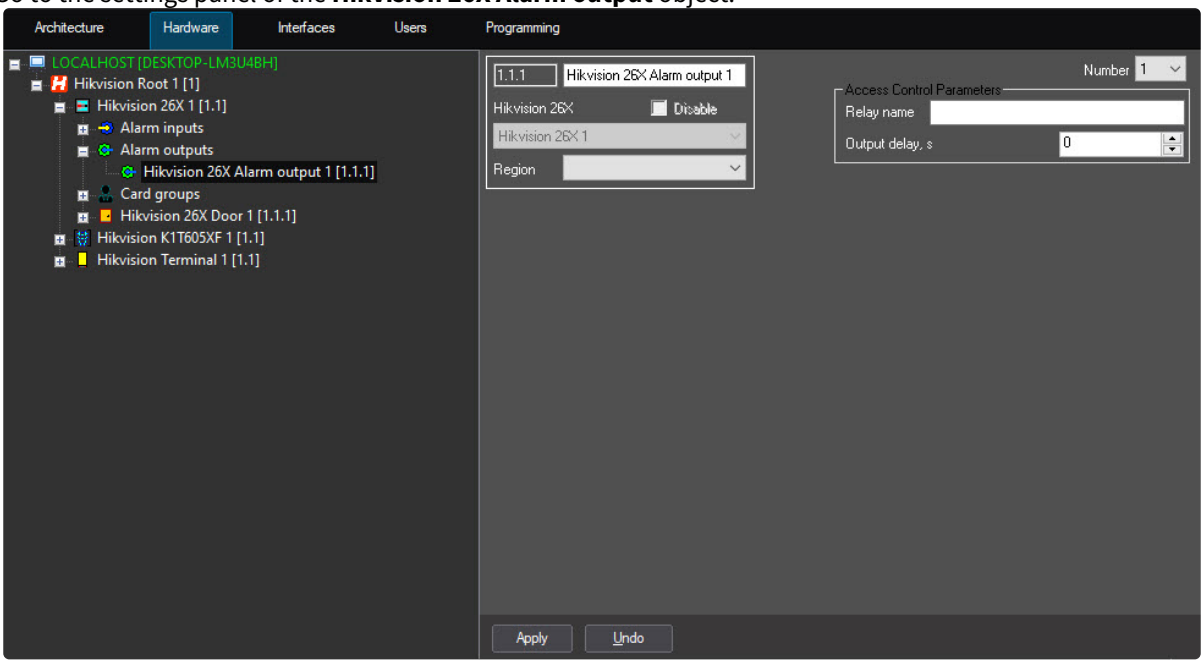
6. From the **Sensivity** drop-down list, select the sensivity value in milliseconds: **10ms** (default), **250ms**, **500ms**, **750ms**.
7. Click the **Apply**  button.

4.5 Configuring the Hikvision alarm output

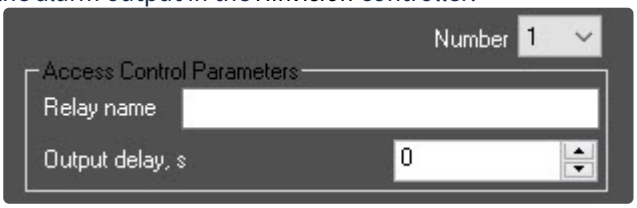
> **Note**
>
> *Hikvision* alarm output configuration options depend on *Hikvision* controller/terminal model. Configuration of the *Hikvision* alarm output will be illustrated by an example of the Hikvision DS-K26x series controller.

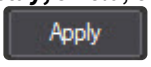
To configure the *Hikvision* alarm output, do the following:

1. Go to the settings panel of the **Hikvision 26X Alarm output** object.



2. In the **Number** drop-down list, in the range from 1 to 4, select the number that corresponds to the number of the alarm output in the *Hikvision* controller.



3. In the **Relay name** field, enter the name of the alarm output that will be displayed in *Axxon PSIM* during subsequent readings of the controller configuration.
4. In the **Output delay, s** field, enter the delay time of the alarm output in seconds.
5. Click the **Apply**  button.

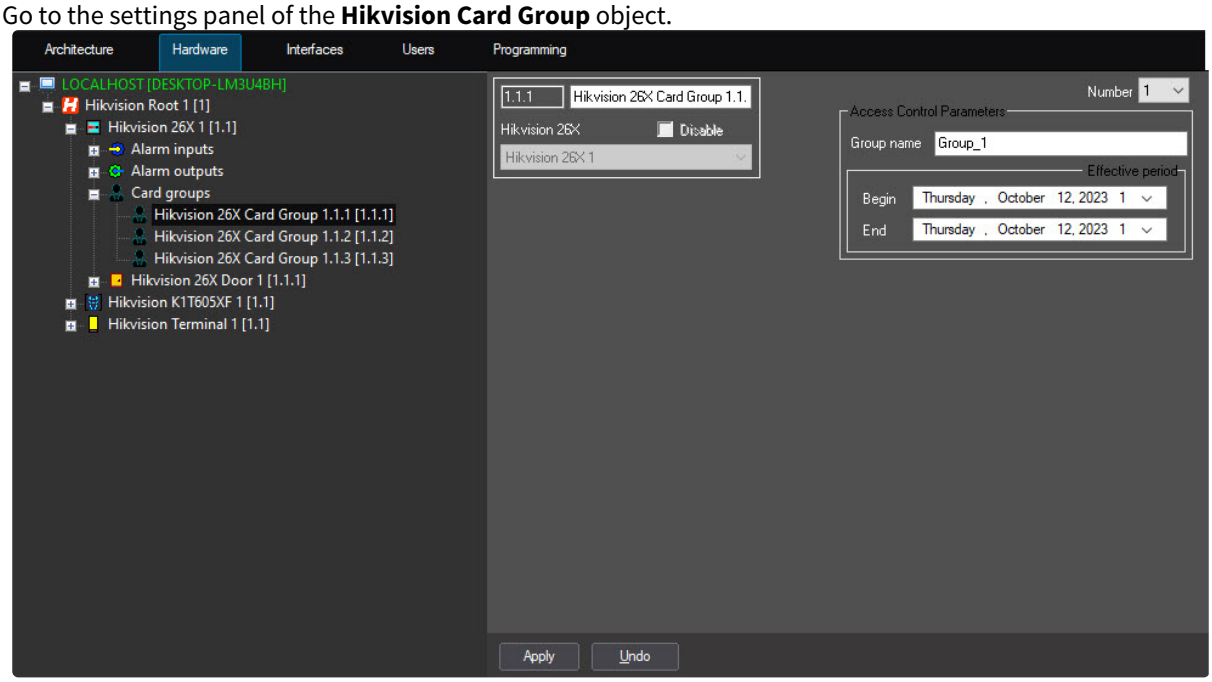
4.6 Configuring the Hikvision card groups

The **Hikvision Card Group** object is used for grouping cards when configuring the *Hikvision* multiple cards (see Configuring multiple Hikvision cards).

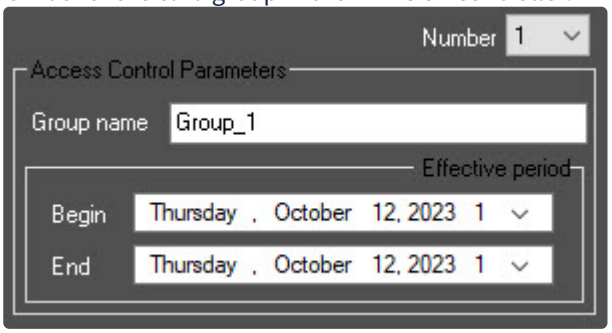
> **Note**
>
> *Hikvision* card groups configuration options depend on *Hikvision* controller/terminal model. Configuration of the *Hikvision* card groups will be illustrated by an example of the Hikvision DS-K26x series controller.

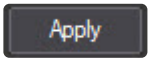
To configure the *Hikvision* card groups, do the following:

1. Go to the settings panel of the **Hikvision Card Group** object.



2. From the **Number** drop-down list, in the range from 1 to 32, select the number that corresponds to the number of the card group in the *Hikvision* controller.



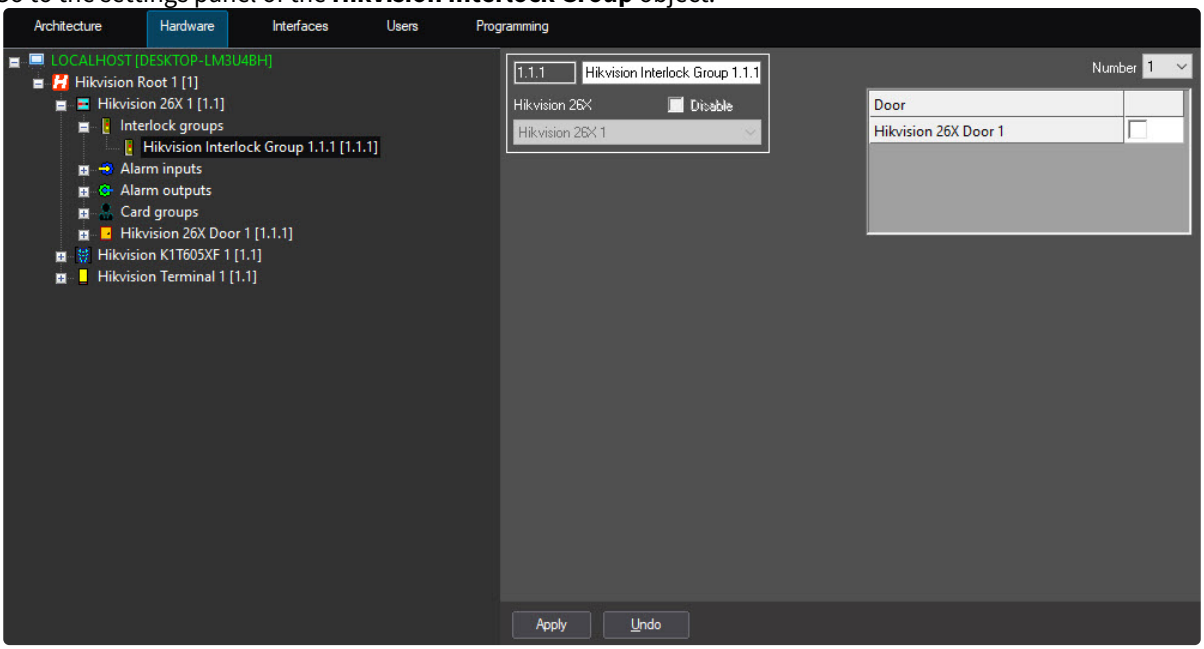
3. In the **Group name** field, enter the card group name.
4. In the **Begin** field, use the button to specify the beginning of the effective period of the card group. The effective period depends on the specified end period. It is recommended to first specify the correct end date of the card group period (see step 5).
5. In the **End** field, use the button to specify the end of the effective period of the card group.
6. Click the **Apply**  button to save the settings.

4.7 Configuring the Hikvision interlock group

> **Note**
>
> *Hikvision* interlock group configuration options depend on *Hikvision* controller/terminal model. Configuration of the *Hikvision* interlock group will be illustrated by an example of the Hikvision DS-K26x series controller.

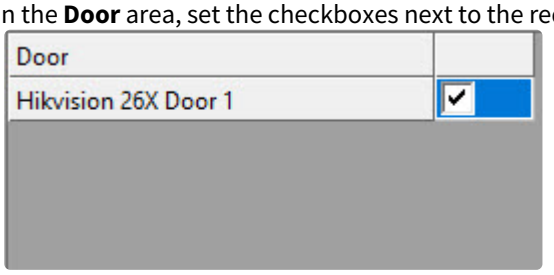
To configure the *Hikvision* interlock group, do the following:

1. Go to the settings panel of the **Hikvision Interlock Group** object.

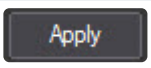


2. From the **Number** 

drop-down list, in the range from 1 to 4, select the number that corresponds to the number of the interlock group in the *Hikvision* controller.
3. In the **Door** area, set the checkboxes next to the required *Hikvision* doors.



> **Note**
>
> To open one of the doors, other doors must be closed. This means that only one door in the interlock group can be opened at a time.

4. Click the **Apply** 

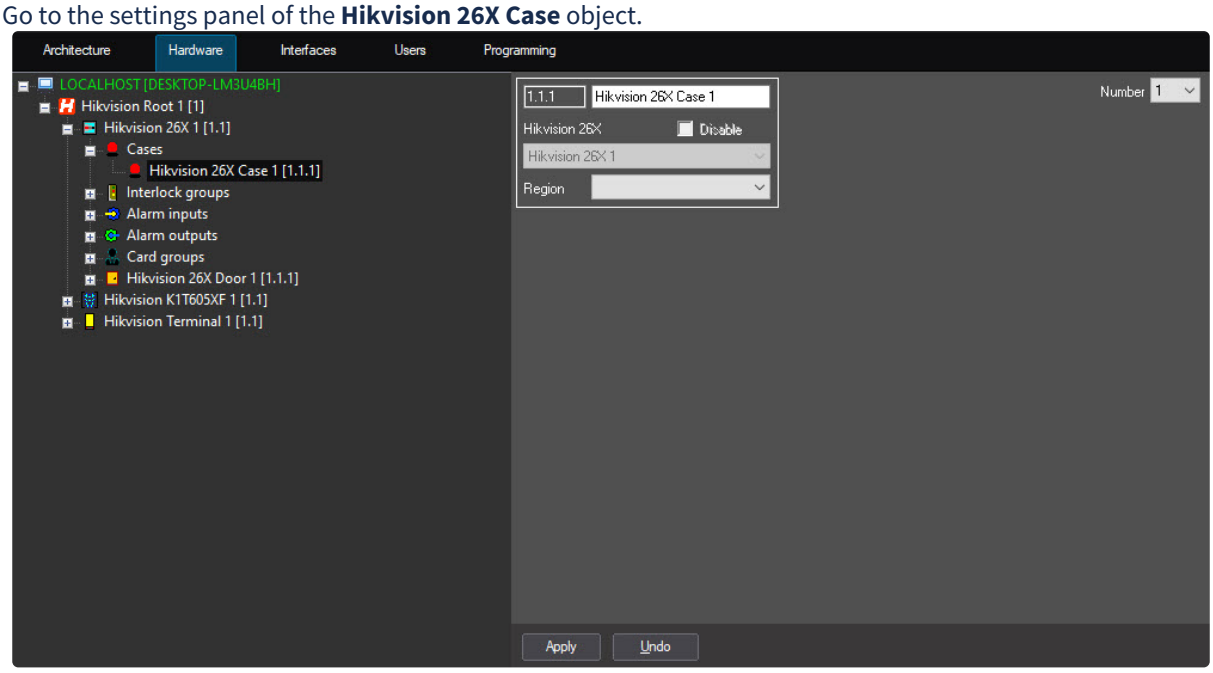
button to save the settings.

4.8 Configuring the Hikvision case

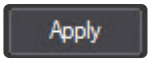
> **Note**
>
> *Hikvision* case configuration options depend on *Hikvision* controller model. Configuration of the *Hikvision* case will be illustrated by an example of the Hikvision DS-K26x series controller.

To configure the *Hikvision* case, do the following:

1. Go to the settings panel of the **Hikvision 26X Case** object.



2. From the **Number** 

drop-down list, select the number of the case input in the range from 1 to 8.
3. Click the **Apply** 

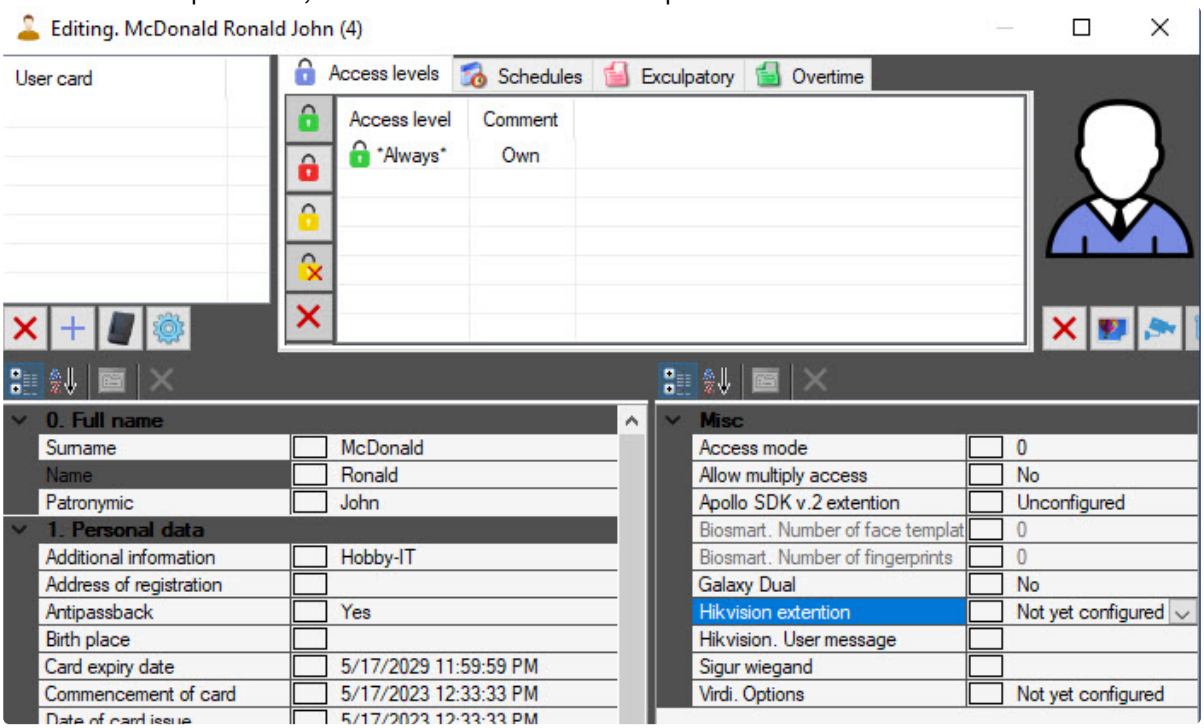
button to save the settings.

4.9 Configuring the Hikvision user cards

To configure the *Hikvision* user cards, do the following:

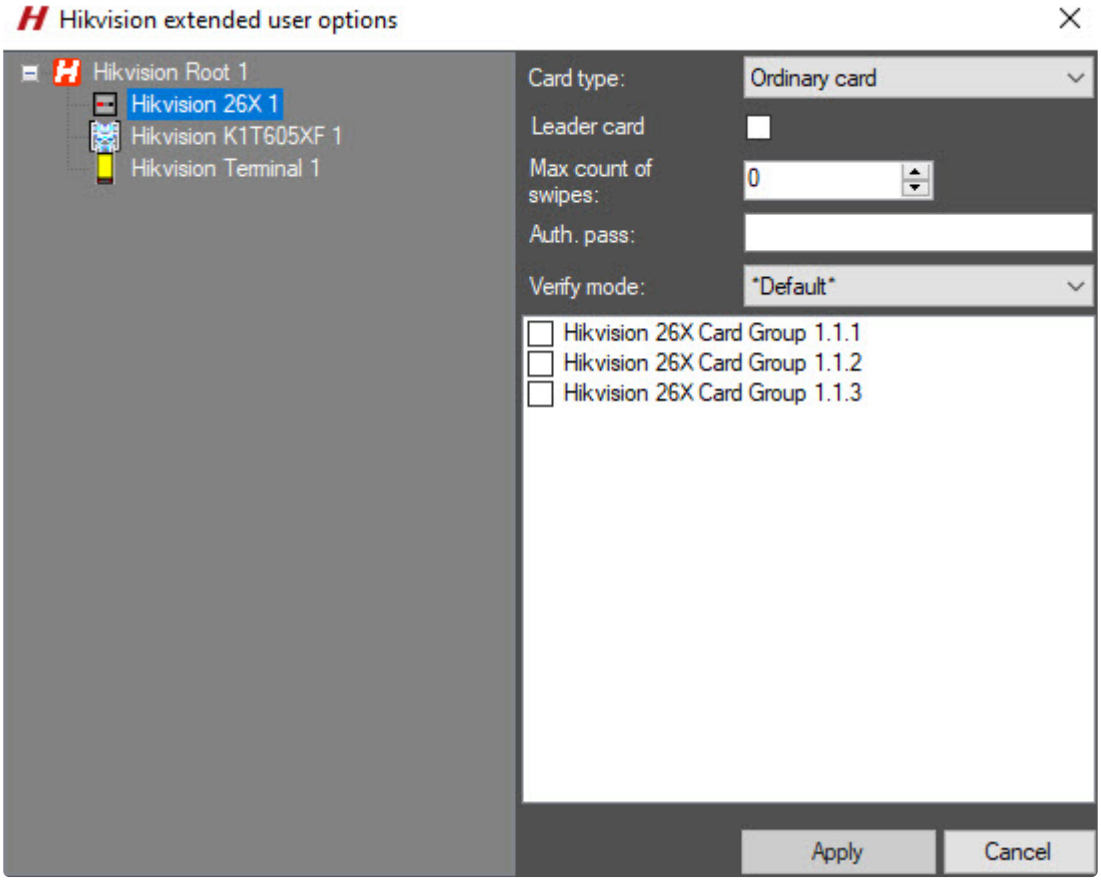
1. Go to the user editing in the *Access Manager* module (see Going to user editing).

2. In the advanced options tab, select the **Hikvision extention** parameter and click the button.

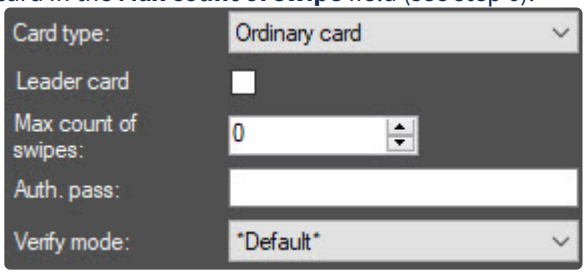


The **Hikvision extended user options** window opens.

> **Note**
>
> If the **Hikvision extention** parameter isn't displayed, enable it for user accounts (Configuring fields displaying in user accounts).



3. Select the required *Hikvision* controller from the objects tree.
4. From the **Card type** drop-down list, select the card type:
    a. **Invalid**—expired card.
    b. **Ordinary card**—standard card type.
    c. **Disabled card**—swiping this type of card prevents the door from locking for a time interval specified by the **Unlock Time for Disabled Pass** parameter (see Configuring the Hikvision door).
    d. **Blacklist card**—when a blacklisted card is swiped, a system event is generated without granting access.
    e. **Patrol card**—this type of cards can be used by supervisors.
    f. **Stress card**—if a user is under duress, this card opens the door and generates a duress alarm.
    g. **Super card**—this card opens all doors of a given controller/terminal within an active time zone specified for user's access level.
    h. **Visitor card**—the card is intended for visitors. You can set the maximum number of swipes for this card in the **Max count of swipe** field (see step 6).

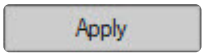
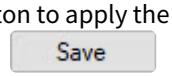


5. Set the **Leader card** checkbox (**2**) if it is necessary to activate all readers connected to this controller/terminal by the first card swipe through any of the readers.

6. Set a limit for a number of **Visitor card** swipes in the **Max count of swipe** field. The maximum number of swipes must be in the range from **0** to **255**. The **0** value means that there are no restrictions on the number of swipes.
7. Specify a card password in the **Auth. pass** field. The password consists of 4 to 8 digits. The availability of this parameter setting depends on the *Hikvision* controller/terminal model.
8. From the **Verify mode** drop-down list, select the mode in which the user's card works.

   > **Note**
   >
   > For the correct operation, the device must support the selected verification mode.

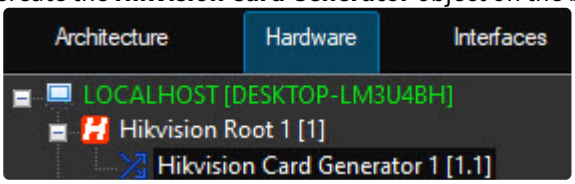
9. In the card group area, select the required card groups by setting the checkboxes next to them. The availability of this parameter setting depends on the *Hikvision* controller/terminal model.

10. Click the **Apply**  button to apply the settings and return to the user editing menu.
11. In the user editing menu, click the **Save**  button to save the changes.

4.10 Creating the Hikvision access cards

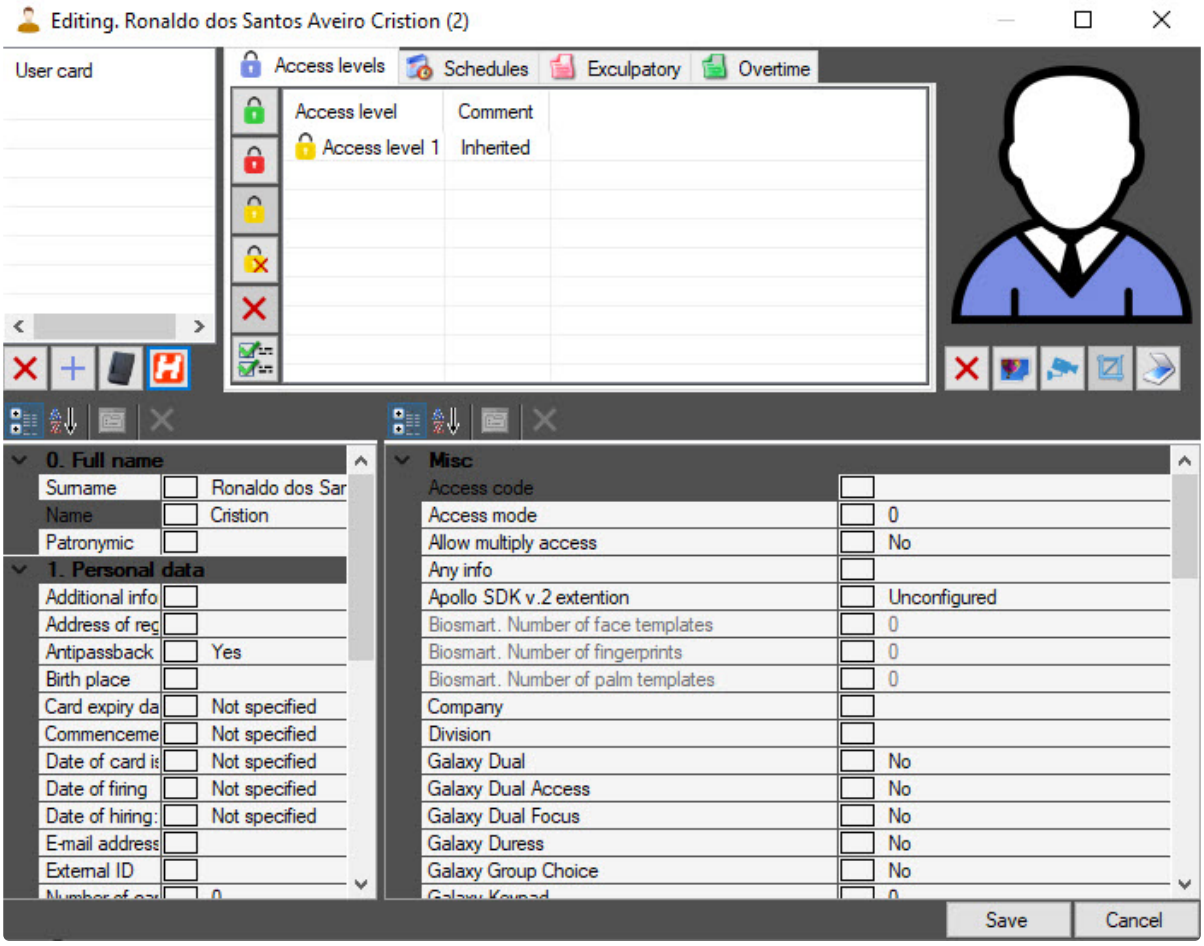
In *ACFA PSIM*, you can create the *Hikvision* access cards. To generate a *Hikvision* access card, do the following:

1. Create the **Hikvision Card Generator** object on the basis of the *Hikvision Root* object.

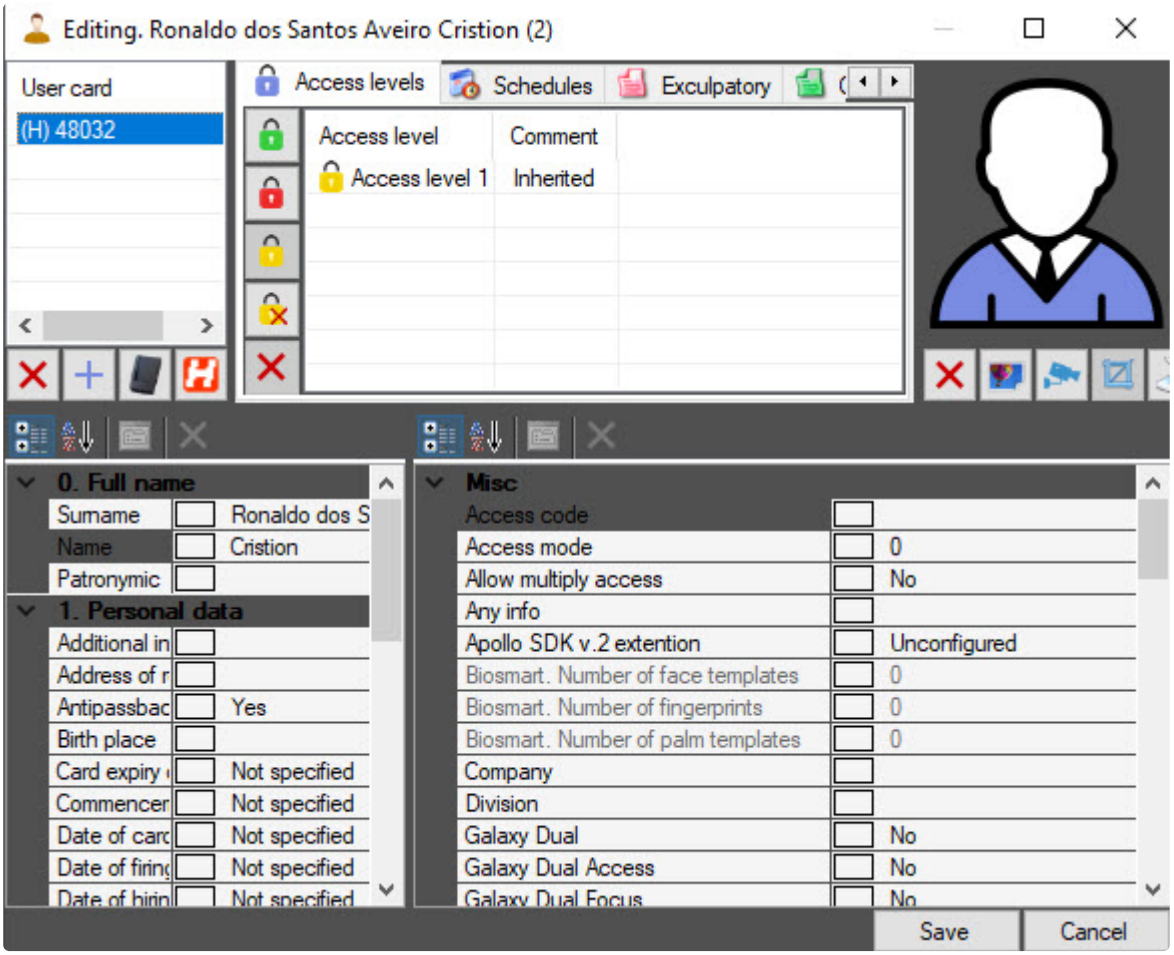


2. Select the Hikvision card generator as a reader on the settings panel of the *Access Manager* module (see Configuring control readers in the Access Manager).
3. In the **Access Manager** interface object, open the user editing window (Going to user editing).

   The **Hikvision Card Generator**  button will be available.



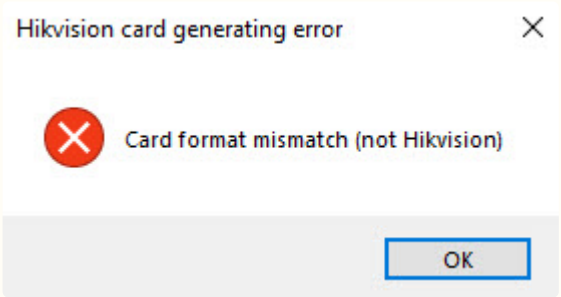
4. Click the **Hikvision Card Generator** button.
   As a result, a *Hikvision* access card will be created.



5. Click the **Save** button.

Attention!

The access card format set in the *Access Manager* module must match the *Hikvision* card format, otherwise an error message will be displayed (for more information on the formats of access cards, see Configuring access cards).



The *Hikvision* access card is created.

5 Hikvision integration module operation

5.1 General information on Hikvision integration module operation

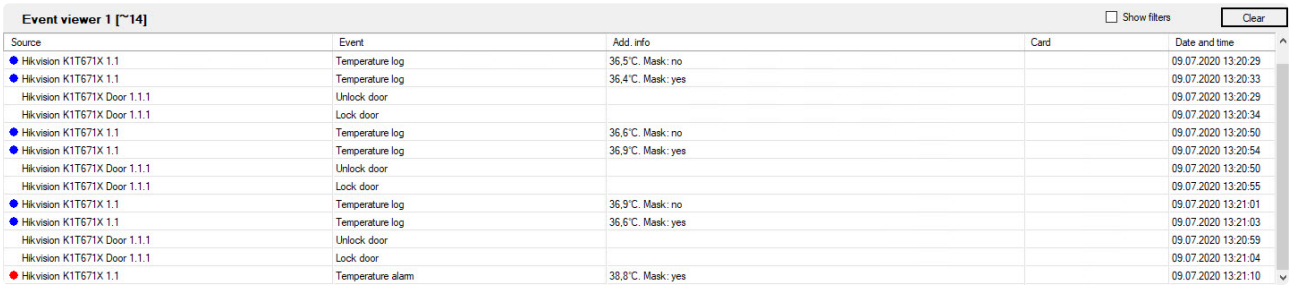
The following interface objects are used for *HikVision* integration module operation:

1. **Map**.
2. **Event viewer**.

For a detailed description of configuring these interface objects, see Axxon PSIM Administrator's Guide.

For a detailed description of working with these interface objects, see Axxon PSIM Operator's Guide.

Access control terminals DS-K5604A-3XF/V and DS-K1T671TM-3XF allow you to measure body temperature and determine the presence/absence of a mask on the user's face. The corresponding events are displayed in the **Event viewer** interface object only if these settings are configured on the terminal (for details, see the manufacturer's documentation).



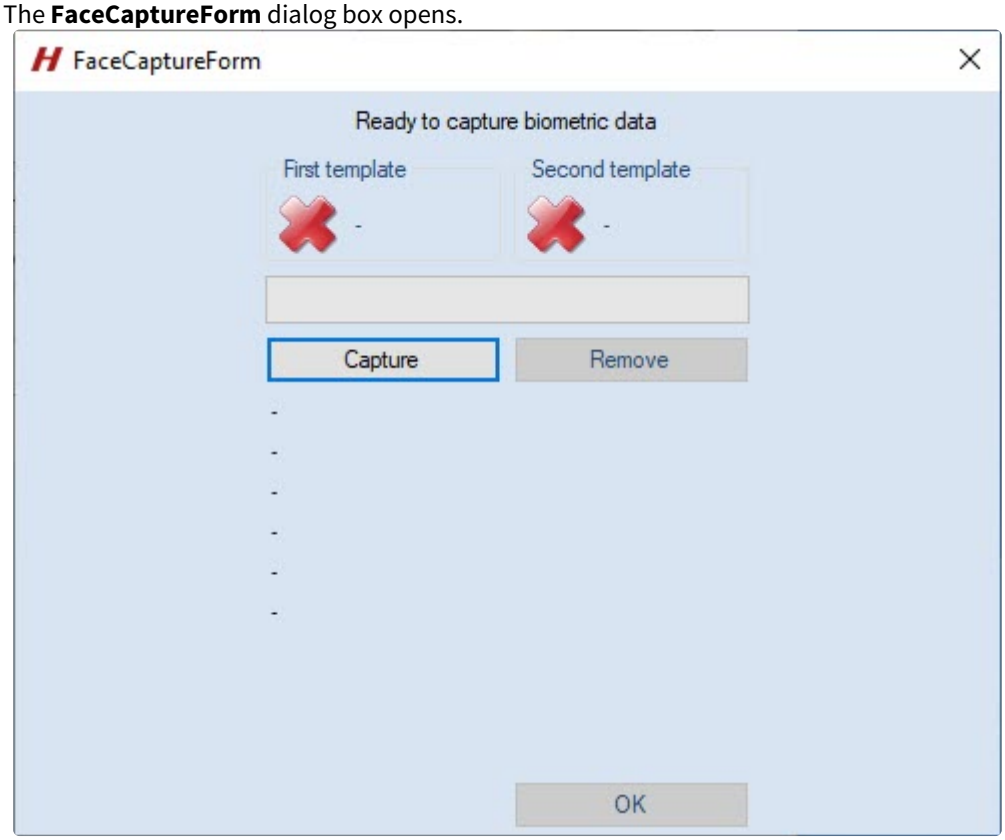
5.2 Adding the Hikvision biometric parameters

5.2.1 Adding the Hikvision face template

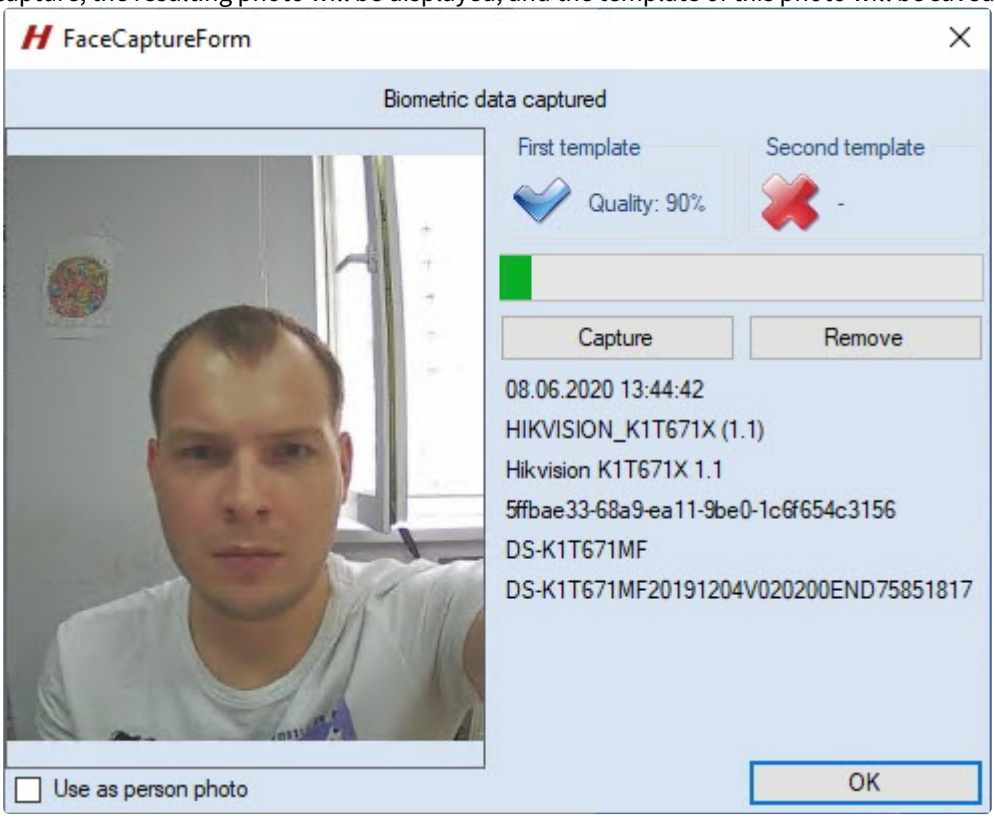
To add a *Hikvision* face template to the *Access Manager* module, do the following:

1. Go to adding biometric data in the **Access Manager** window (see Adding biometric parameters).
2. Select the extension **(Hikvision Face) <Terminal Name>** that corresponds to a terminal with a biometric face reader.

3. The **FaceCaptureForm** dialog box opens.



4. Click the **Capture** button. Then follow the instructions on the terminal screen. In case of successful face capture, the resulting photo will be displayed, and the template of this photo will be saved.



5. To use the resulting photo as a user photo, set the **Use as person photo** checkbox (see Assigning a photograph to a user in the Access Manager software module).

> **Attention!**
>
> It is highly recommended to set the **Use as person photo** checkbox so that the photo can be added to other terminals. Otherwise, the photo will be added only to the terminal from which the face was captured, and the face caption will be deleted during the next addition of access parameters.

6. To delete a face template, click the **Remove** button.
7. Click **OK** to save the face template.

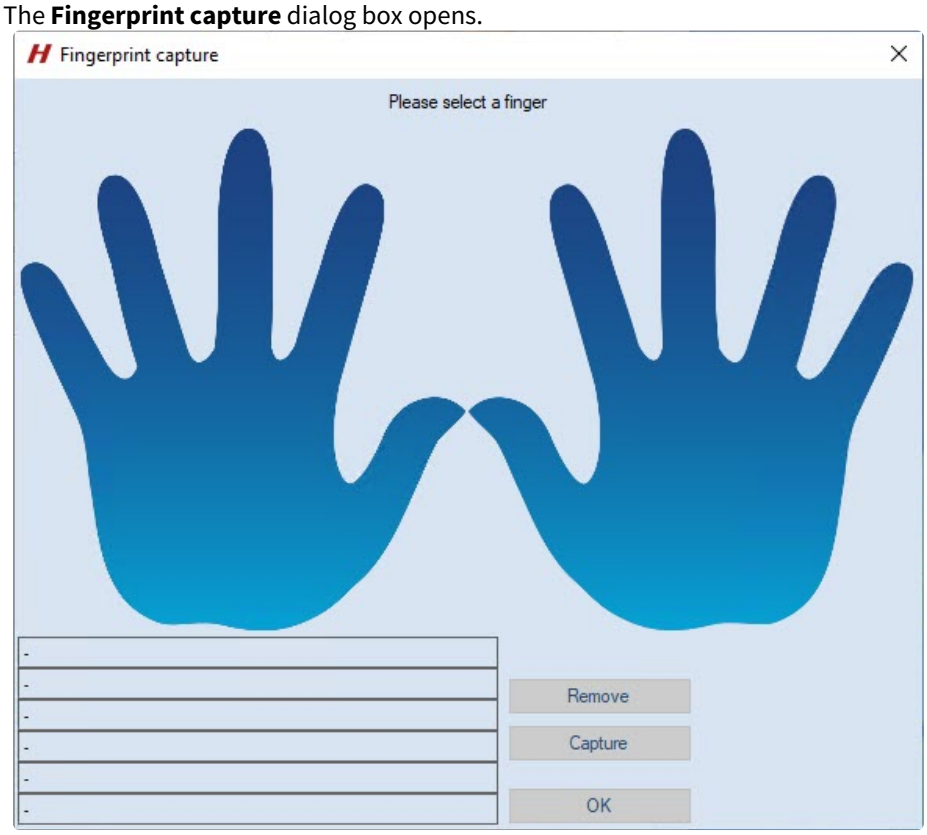
The *Hikvision* face template is added.

5.2.2 Adding the Hikvision fingerprints

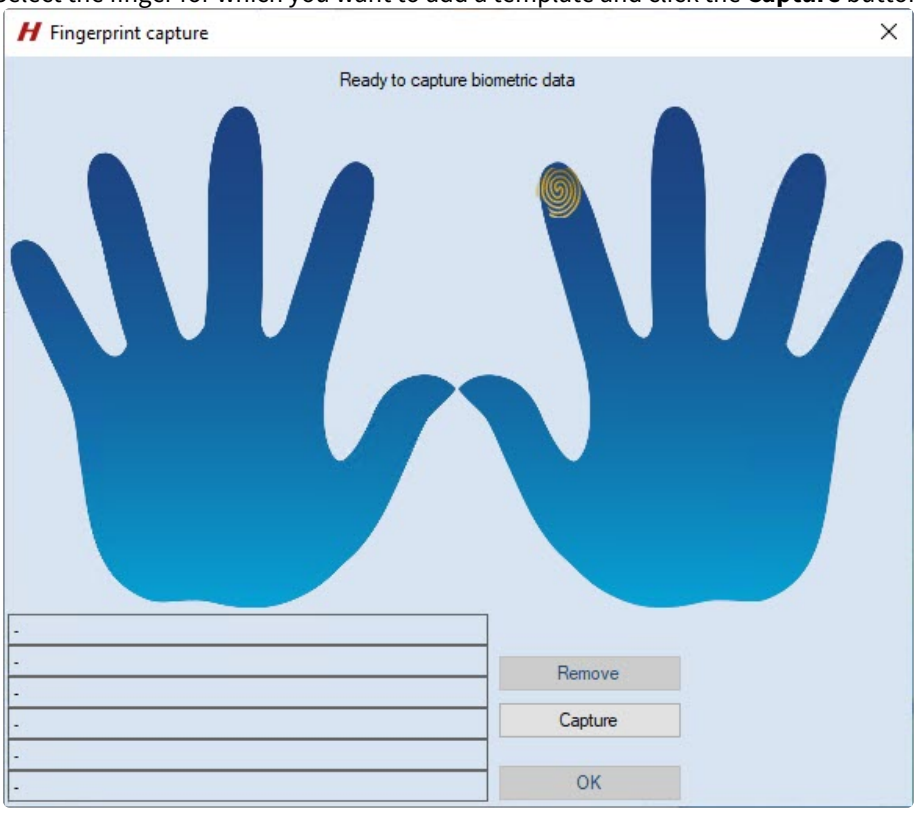
To add the *Hikvision* fingerprint templates to the *Access Manager* module, do the following:

1. Go to adding biometric data in the **Access Manager** window (see Adding biometric parameters).
2. Select the extension **(Hikvision Fingerprint) <Controller/terminal name>** that corresponds to the controller with the biometric fingerprint reader connected to it or to the terminal.

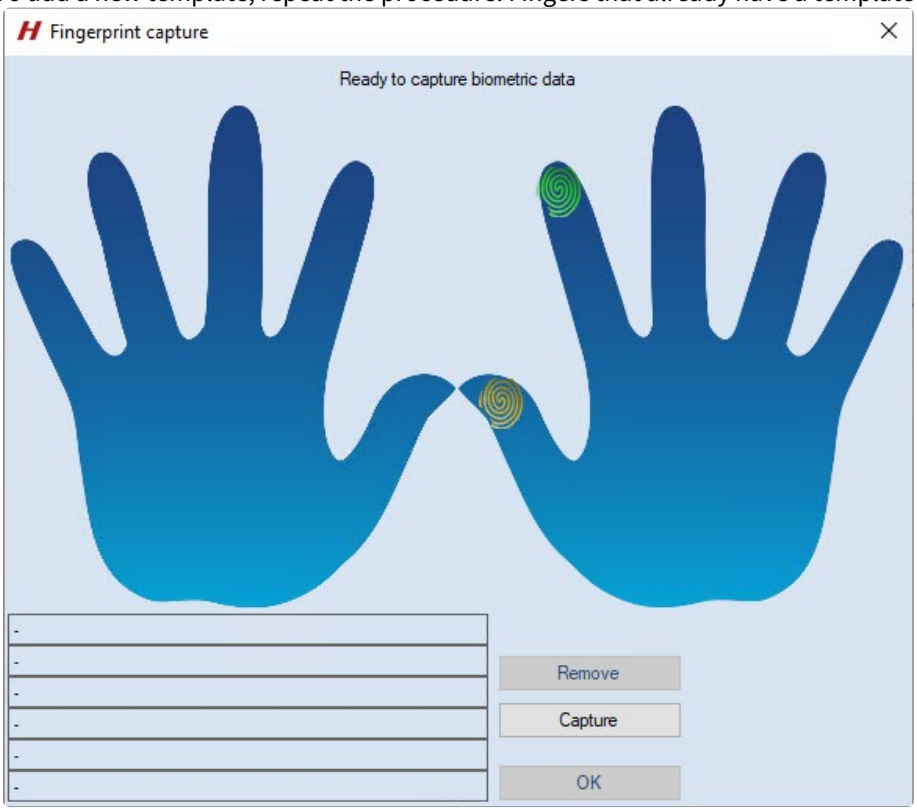
3. The **Fingerprint capture** dialog box opens.



4. Select the finger for which you want to add a template and click the **Capture** button.



5. Then put your finger on the reader several times. In case of successful capture, the fingerprint template will be automatically saved in the controller/terminal.
6. To add a new template, repeat the procedure. Fingers that already have a template are highlighted in green.



7. To delete a previously added template, select your finger and click the **Remove** button.

The *Hikvision* fingerprint templates are now added.

5.3 Managing a Hikvision controller/terminal/call panel

In the **Map** interactive window, you can manage only *Hikvision* KV series call panels using the function menu of the **Hikvision KVx** object. You cannot manage *Hikvision* controllers and terminals in the **Map** window.

The function menu of the **Hikvision KVx** object looks like this:

Description of the function menu commands of the **Hikvision KVx** object is given in the table.

Function menu command	Function
Open	Opens the door

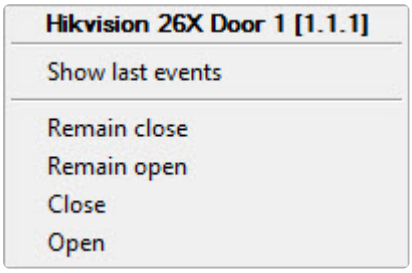
The state images are the same for all *Hikvision* controllers/terminals/call panels. The following states are possible:

	Battery low
	Link lost
	Network supply
	Battery supply
	Link ok

5.4 Managing a Hikvision door

> **Note**
>
> Management of a *Hikvision* door will be illustrated by an example of the Hikvision DS-K26x series controller. You can manage doors of other *Hikvision* controllers/terminals in the similar way.

You can manage the *Hikvision* door in the **Map** interactive window using the function menu of the **Hikvision 26X Door** object.



Description of the function menu commands of the *Hikvision* door is given in the table.

Function menu command	Function
Remain close	Changes the door state from normal to closed
Remain open	Changes the door state from normal to open
Close	Locks the door
Open	Opens the door

The following door states are possible:

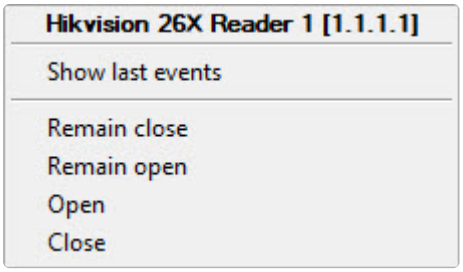
> **Note**
>
> The door state images are the same for all *Hikvision* controllers/terminals.

	Normal
	Permanent closed
	Permanent opened
	Sleep
	Lock exception
	Lock break
	Lock short
	Magnet exception
	Magnet break
	Magnet short
	Link lost

5.5 Managing a Hikvision reader

> **Note**
>
> Management of the *Hikvision* reader will be illustrated by an example of the Hikvision DS-K26x series controller. You can manage readers of other *Hikvision* controllers/terminals in the similar way.

You can manage the *Hikvision* reader in the **Map** interactive window using the function menu of the **Hikvision 26X Reader** object. Actually, you will manage the door of the reader. This is done for your convenience.



Description of the function menu commands of the *Hikvision* reader is given in the table.

Function menu command	Function
Remain close	Changes the state of the reader door from normal to closed
Remain open	Changes the state of the reader door from normal to open
Open	Opens the door
Close	Locks the door

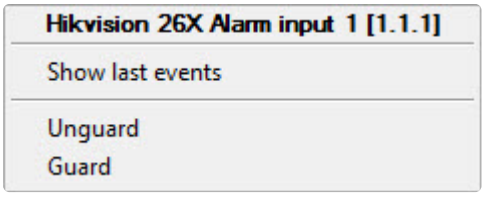
The reader state images are the same for all *Hikvision* controllers/terminals. The following reader states are possible:

	Mode: map
	Mode: other
	Offline
	Tampering

5.6 Managing a Hikvision alarm input

> **Note**
>
> Management of a *Hikvision* alarm input will be illustrated by an example of the Hikvision DS-K26x series controller. You can manage alarm inputs of other *Hikvision* controllers/terminals in the similar way.

You can manage a *Hikvision* alarm input in the **Map** interactive window using the function menu of the **Hikvision 26X Alarm input** object.



The alarm input state images are the same for all *Hikvision* controllers/terminals. Description of the function menu commands of the *Hikvision* alarm input is given in the table.

Function menu command	Function
Unguard	Disarming
Guard	Arming

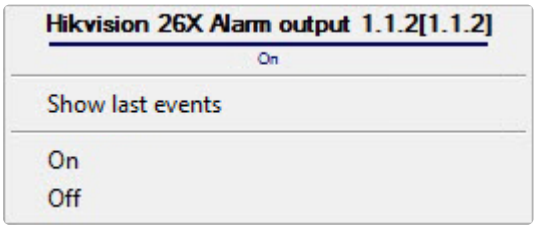
The following alarm input states are possible:

	Armed
	Disarmed
	Alarm

5.7 Managing a Hikvision alarm output

> **Note**
>
> Management of a *Hikvision* alarm output will be illustrated by an example of the Hikvision DS-K26x series controller. You can manage alarm outputs of other *Hikvision* controllers/terminals in the similar way.

You can manage a *Hikvision* alarm output in the **Map** interactive window using the function menu of the **Hikvision 26X Alarm output** object.



Description of the function menu commands of the *Hikvision* alarm output is given in the table.

Function menu command	**Function**
On	Enable the output
Off	Disable the output

The alarm output state images are the same for all *Hikvision* controllers/terminals.

	On
	Off

5.8 Managing a Hikvision case

You cannot manage cases of the *Hikvision* controllers and terminals in the **Map** window.

The case state images are the same for all *Hikvision* controllers/terminals. The following case states are possible:

	Off
	On