ACFA Intellect

Hikvision Integration Module Configuration and Operation Guide

Last update 24/05/2022

Table of contents

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

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

Server: a computer that hosts the **Server** version of the *Intellect* PSIM software.

Hikvision ACS Controller: an electronic device that monitors and manages access points.

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

Passing time: 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: 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: 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 zone: a set of time intervals within each day of a time cycle (1 to 366 days), as well as time intervals during specific dates.

2 Introduction in the Hikvision Integration Module Configuration and Operation Guide

On the page:

2.1 The purpose of this Guide

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

This Guide contains information about the following topics:

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 the *ACFA Intellect* integration module responsible for the following functions:

1. configuration of the *Hikvision* ACS and connected Hikvision readers.
2. interoperability between the *Hikvision* ACS and the *ACFA Intellect* for monitoring and management.

Note

For detailed information on the *Hikvision* ACS, you can visit the manufacturer's website.

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

1. install *Hikvision* hardware onsite (refer to the official *Hikvision* ACS installation manual);
2. connect the *Hikvision* ACS to the *ACFA Intellect* server (refer to the most recent version of the *Hikvision* module operations manual).

3 Hardware compatibility 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

Hardware connections

Equipment	Purpose
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

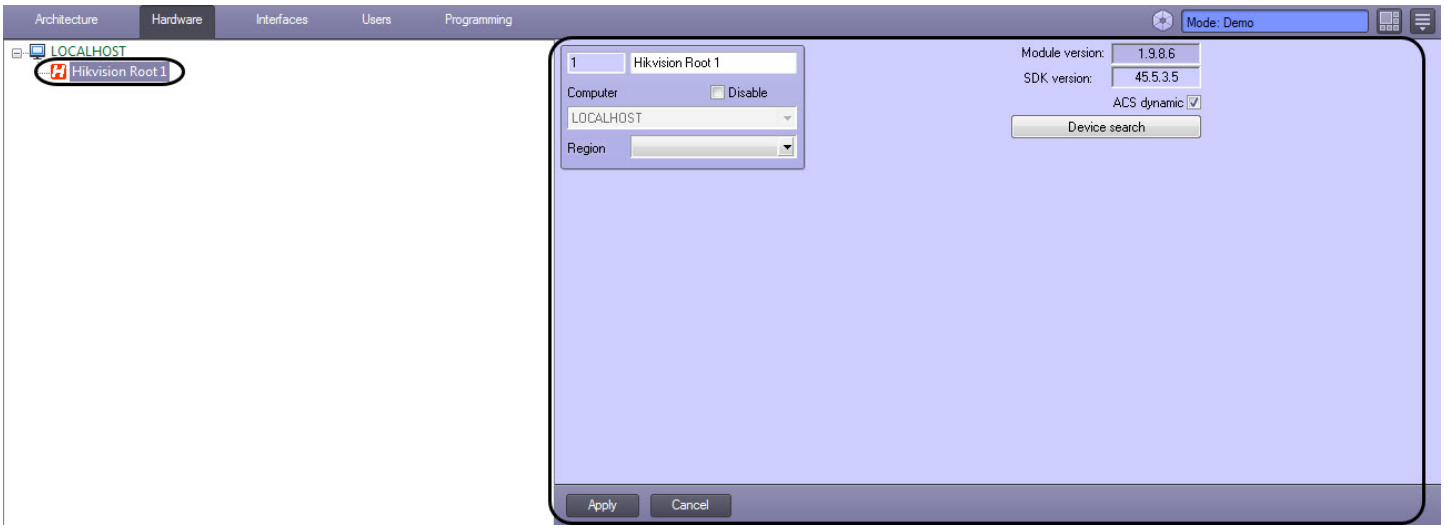
Software Licensing

Per 1 controller/terminal.

4 Configuring the Hikvision integration module

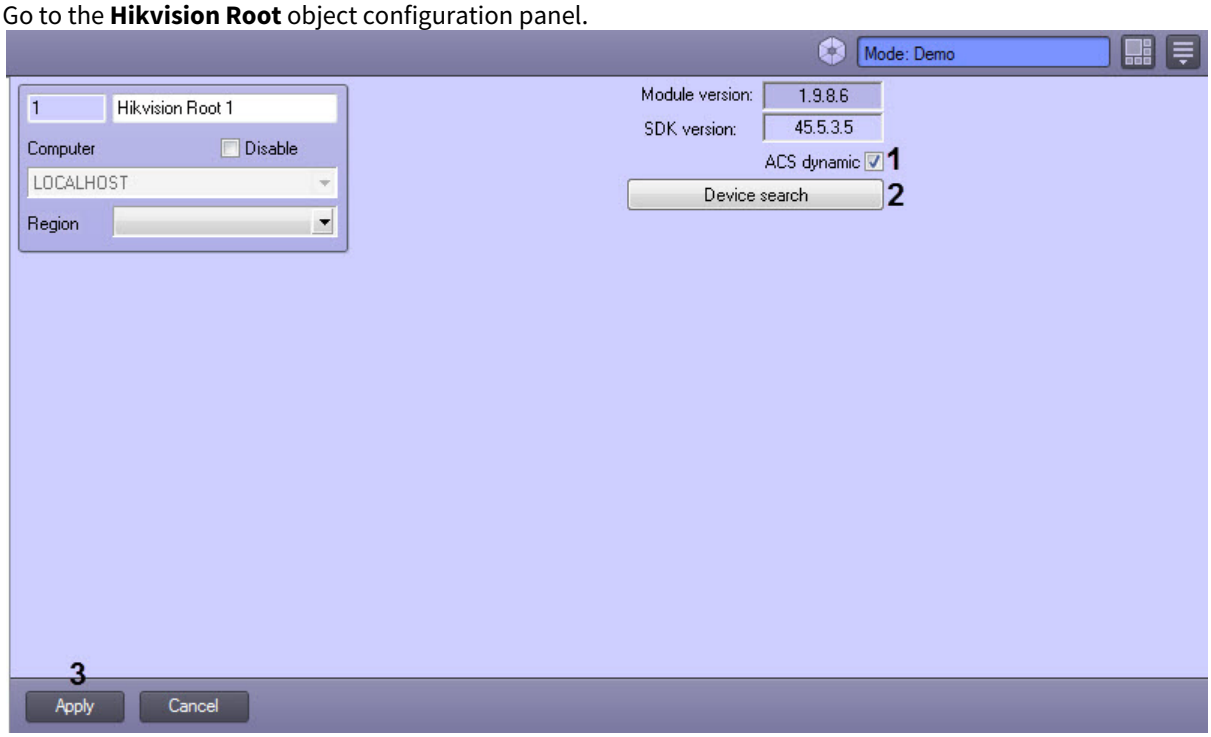
4.1 Setting up the Hikvision ACS connection

You can set up the connection to the *Hikvision* ACS via the **Hikvision Root** object configuration panel. This object is created under a parent **Computer** object via the **Settings** dialog box on the **Hardware** tab.



How to configure the *Hikvision* ACS connection:

1. Go to the **Hikvision Root** object configuration panel.



2. Check the **ACS Dynamic** (**1**) box to enable automatic synchronization of any changes in card users' base, access rules and/or time zones with relevant controllers.
3. Click the **Device Search** button (**2**) button to start searching for connected controllers. As the result of the search, Hikvision controller objects corresponding to each discovered device are automatically created in the object tree.

> **Note.**
>
> Download the SADP tool from the manufacturer's web site and install it to make sure all connected controllers could de discovered.

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

The *Hikvision* ACS connection is now configured.

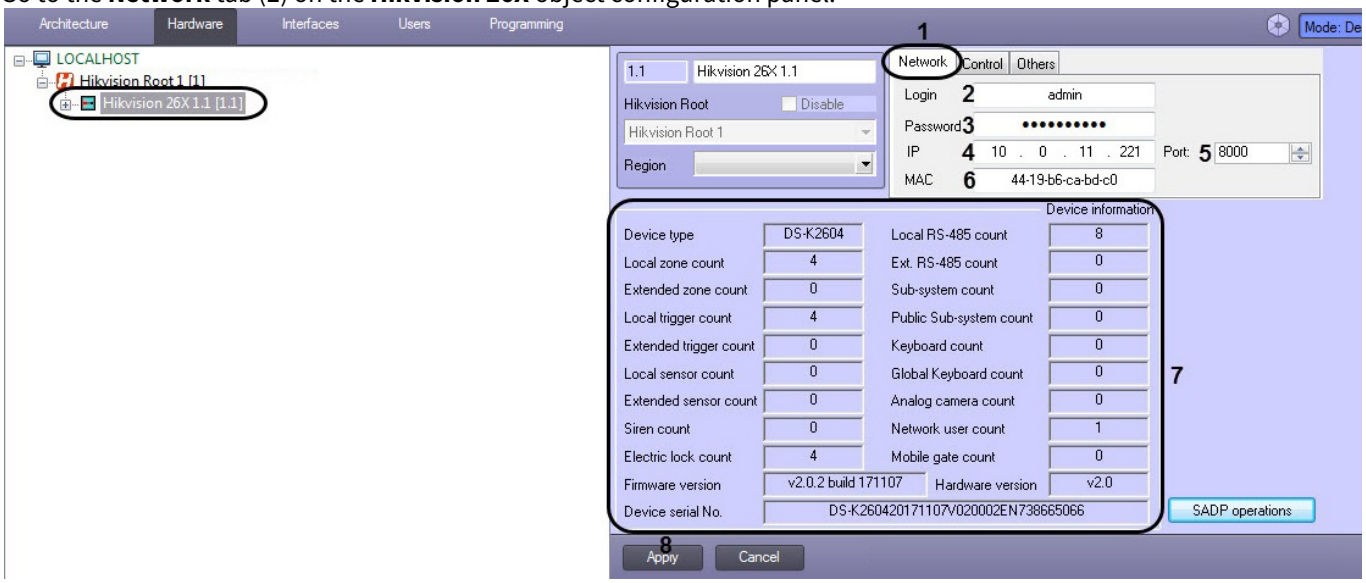
4.2 Configuring the Hikvision access controller

4.2.1 Network settings of the Hikvision controller

> **Note**
>
> The network settings of the *Hikvision* controller will be illustrated by an example of the *Hikvision 26X* controller. Network settings for other *Hikvision* controllers are similar.

To set network parameters for a *Hikvision* controller, do the following:

1. Go to the **Network** tab (**1**) on the **Hikvision 26X** object configuration panel.



2. In the **Login** (**2**) field, enter the login for the *Hikvision* controller.
3. In the **Password** field (3), enter the password for the *Hikvision* controller.
4. In the **IP** field (**4**), specify the IP address of the *Hikvision* controller.
5. In the **Port** field (**5**), specify the communication port number of the *Hikvision* controller.
6. In the **MAC** field (**6**), specify the MAC address of the *Hikvision* controller.

> **Note.**
>
> The **IP, Port**, and **MAC** fields are filled in automatically if controller is added automatically.

7. In case of a successful connection, you will see detailed information on the controller in the **Device information** pane (**7**).
8. Click **Apply** button (**8**).

> **Note.**
>
> The objects tree corresponding to the *Hikvision* controller configuration is created after you click the **Apply** button.

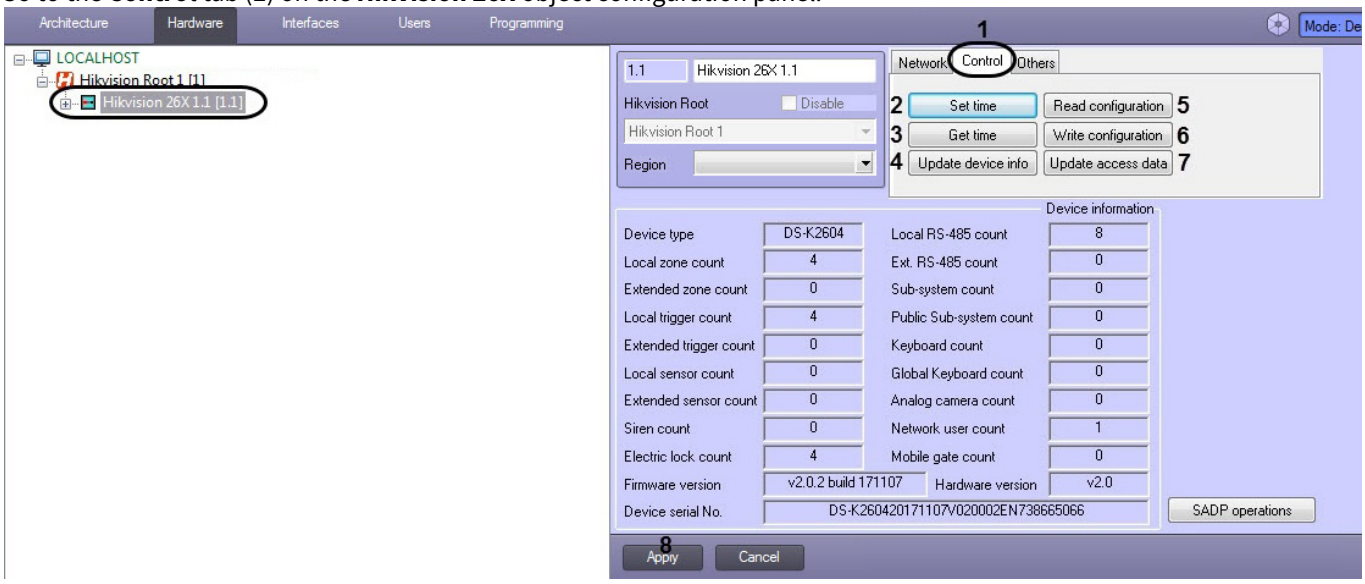
The network settings of the *Hikvision* controller are now complete.

4.2.2 Configuring the Hikvision controller

> **Note**
>
> The configuration of the *Hikvision* controller will be illustrated by an example of the *Hikvision 26X* controller. The configuration of other *Hikvision* controllers is similar.

To configure a *Hikvision* controller, do the following:

1. Go to the **Control** tab (**1**) on the **Hikvision 26X** object configuration panel.



2. Press the **Set Time** button (**2**) to set the controller's on-board clock to the current time of your server.
3. Press the **Get Time** button (**3**) to get the controller's on-board clock value.
4. Press the **Update Device Info** button (**4**) to update the controller data in the **Device information** pane.
5. Click the **Read Configuration** button (**5**) to read the controller configuration data.
6. Press the **Write Configuration** button (**6**) to write the current configuration data 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 data into the controller after each change made to configuration in *ACFA Intellect*.

7. Click **Update Access Data** button (**7**) to update access levels data stored in the controller.
8. Click the **Apply** button (**8**) to save your settings.

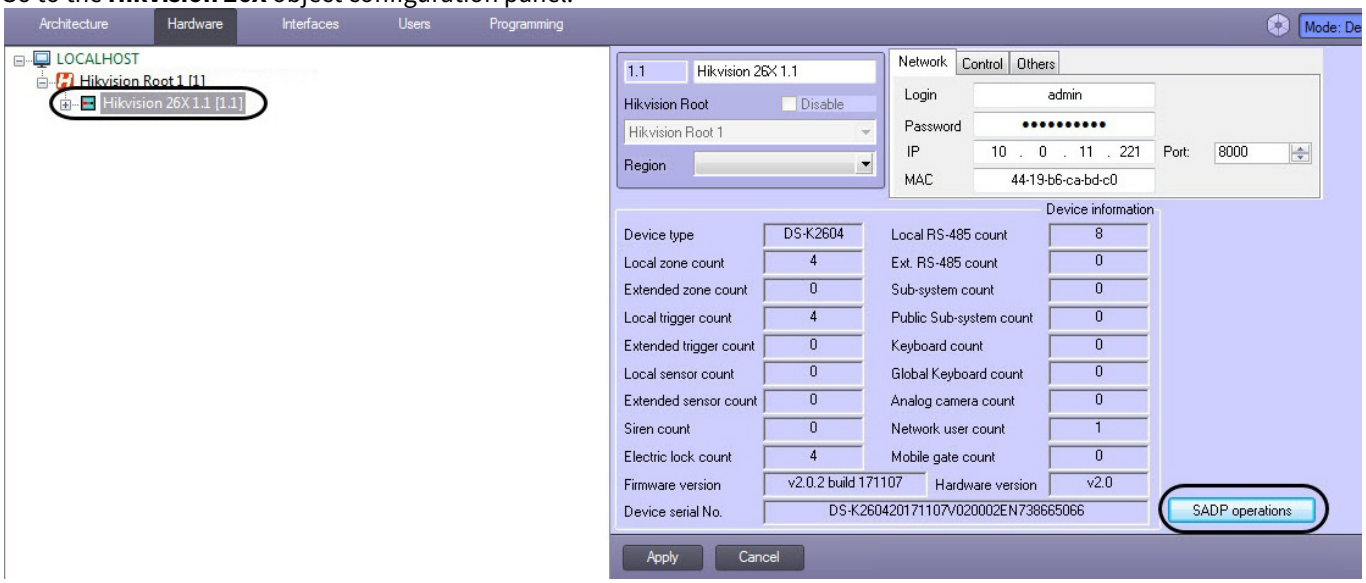
The *Hikvision* controller is now configured.

4.2.3 Hikvision SADP settings

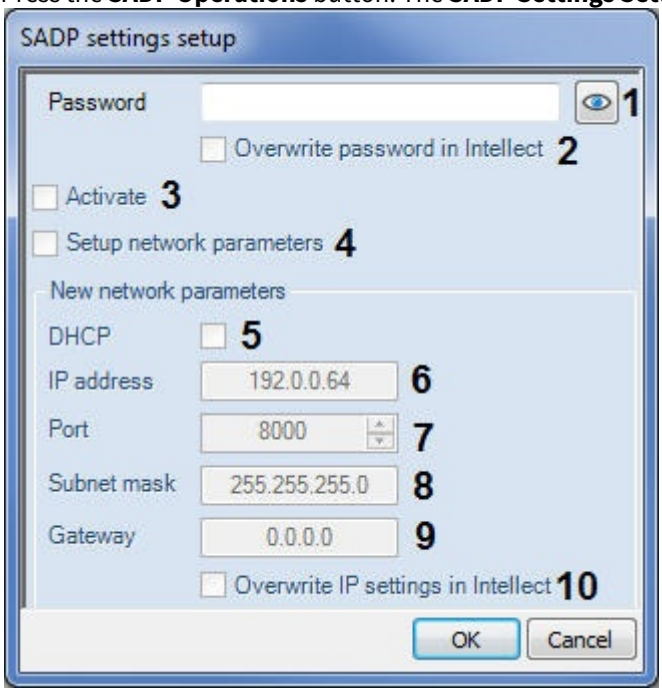
> **Note**
>
> The SADP settings of the *Hikvision* controller will be illustrated by an example of the *Hikvision 26X* controller. SADP settings for other *Hikvision* controllers are similar.

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

1. Go to the **Hikvision 26X** object configuration panel.



2. Press the **SADP Operations** button. The **SADP Settings Setup** window opens.



3. In the **Password** field (**1**), enter a new password for the *Hikvision* controller.
4. Check the **Overwrite Password in Intellect** (**2**) box to automatically overwrite the old password in the ACFA *Intellect* integration module with the new one; otherwise you need to do it manually (refer to Network settings of the Hikvision controller).
5. Check the **Activate** (**3**) box 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. Check the **Setup Network Parameters** (**4**) box to enable changing network settings.
7. Check the **DHCP** box (**5**) to enable DHCP.
8. In the **IP address** field (**6**), enter the new IP address of the *Hikvision* controller.
9. In the **Port** field (**7**), enter a new connection port number for the *Hikvision* controller.
10. In the **Subnet mask** field (**8**), specify the mask for a subnet where the *Hikvision* controller will be located.
11. In the **Gateway** field (**9**), specify the connection gateway for the *Hikvision* controller.
12. Check the **Overwrite IP Settings in Intellect** box (**10**) to automatically overwrite the old network settings in the ACFA *Intellect* integration module; otherwise you need to do it manually (refer to Network settings of the Hikvision controller).
13. Click the **OK** button to apply the settings.

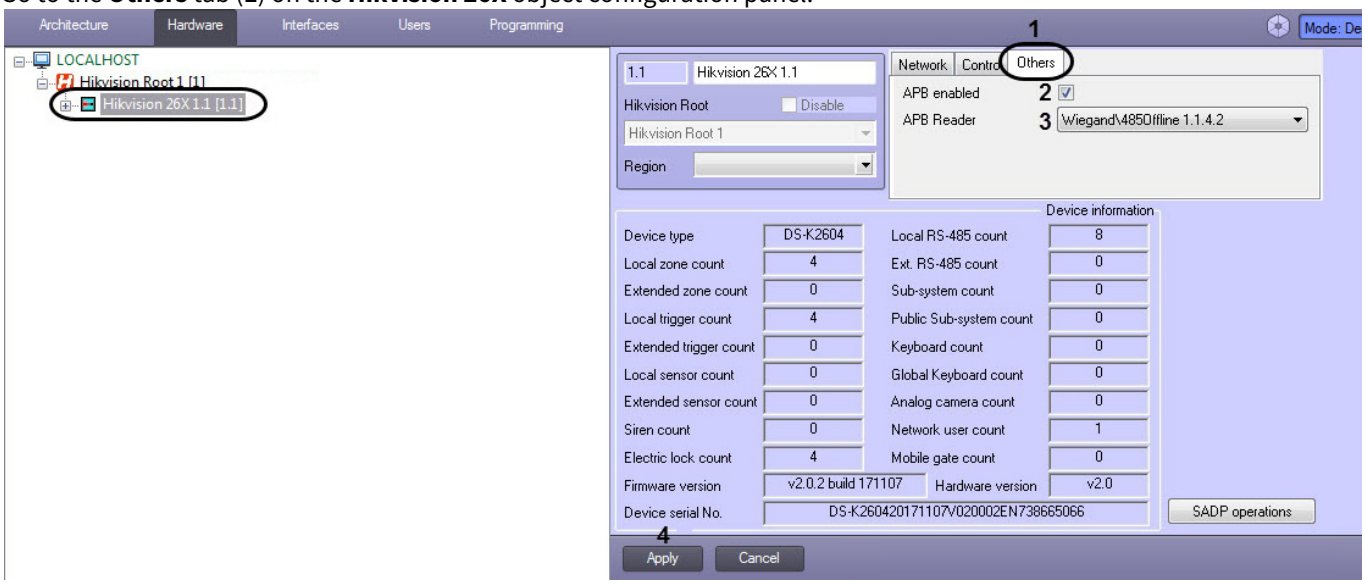
Hikvision SADP settings are now configured.

4.2.4 Advanced settings for a Hikvision controller

> **Note**
>
> The advanced settings of the *Hikvision* controller will be illustrated by an example of the *Hikvision 26X* controller. Advanced settings for other *Hikvision* controllers are similar.
> Advanced settings are not available for *Hikvision KV* series panels, such as *DS-KV8102-IP*.

To perform an advanced setup of a *Hikvision* controller, do the following:

1. Go to the **Others** tab (**1**) on the **Hikvision 26X** object configuration panel.



2. Check the **APB Enabled** box (**2**) to enable Anti-Passback monitoring.
3. From the **APB Reader** (**3**) drop-down list, select the starting reader for Anti-Passback monitoring.
4. Click **Apply** button (**4**).

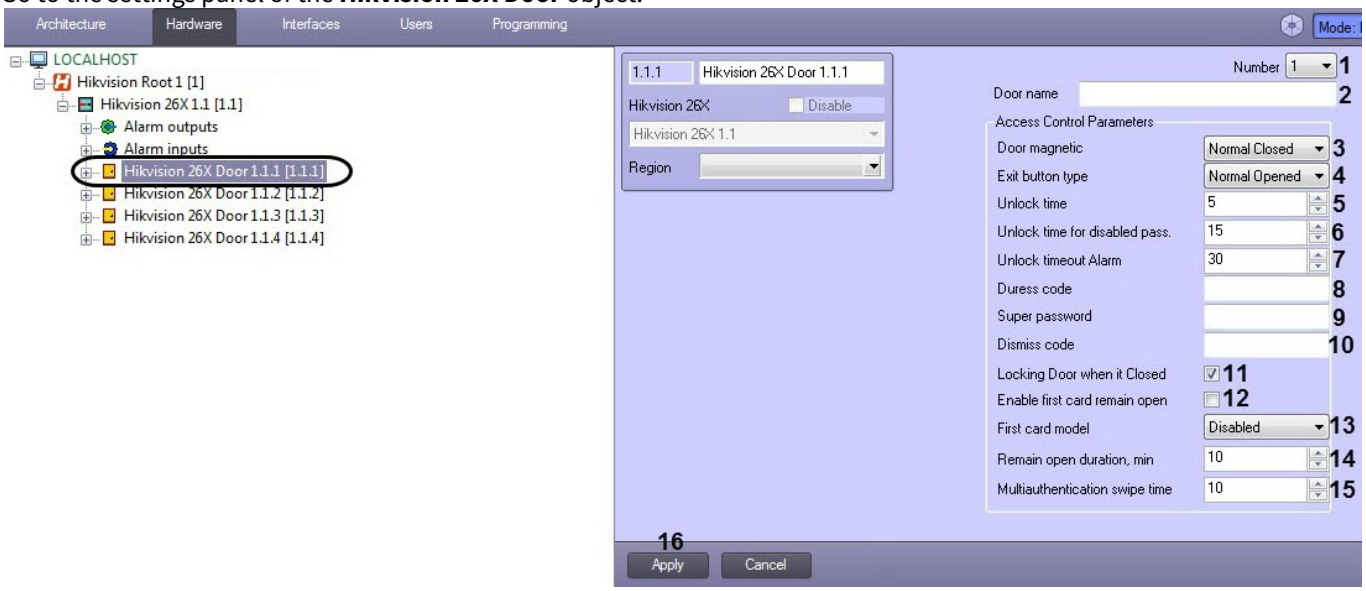
Advanced setup of the *Hikvision* controller is now complete.

4.3 Configuring the Hikvision door

> **Note**
>
> *Hikvision* door configuration options depend on the *Hikvision* controller model. *Hikvision* door configuration will be illustrated by an example of the *Hikvision 26X* controller. Door configuration for other *Hikvision* controllers is similar.

You can configure the *Hikvision* door as follows:

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



2. In the **Number** drop-down list (**1**), you see the door ID number assigned by the *Hikvision* controller. You can not change this value.
3. In the **Door Name** field (**2**), you can set the name of the door under which it will further appear in the ACFA *Intellect* integration module.
4. Select a door's default state from the **Door Magnetic** drop-down list (**3**): **Normal Closed** for normally closed or **Normal Opened** for normally open.
5. Select a push-to-exit button type from the **Exit button type** (**4**) drop-down list: **Normal Closed** for normally closed or **Normal Opened** for normally open.
6. In the **Unlock Time** (**5**) field, you can set a time interval after which the door will be automatically re-locked.
7. In the **Unlock Time for Disabled Pass** field (**6**), you can set a time interval during which the door will be opened for any **Disabled** card holder.
8. In the **Unlock Timeout Alarm** field (**7**), you can set a time interval after which an alarm is initiated if the door is still open.
9. In the **Duress Code** field (**8**), you can set a code to be applied when accessing the door under duress. This code opens the door while triggering the duress alarm. The duress code consists of 4 to 8 digits.
10. In the **Super password** field (**9**), you can set a super password for this door. The super password consists of 4 to 8 digits.

> **Note.**
>
> **Duress Code** and **Super password** shall not match each other or authentication password.

11. In the **Dismiss Code** field (**10**), you can set a code for turning off all card readers associated with this door. The Dismiss code consists of 4 to 8 digits.
12. Check the **Locking Door When it Closed** box (**11**) if the door has to be locked immediately after its closing. If the box is left unchecked, the door will be locked after the **Unlock Time** interval expires (see Step 6).
13. Check the **Enable First Card Remain Open** box (**12**) if you want to set the door to first card mode.

> **Note.**
>
> Several First Cards can be set for one door. The door is available for other users with any authorization type after the first card is swiped only.

14. From the **First Card Mode** drop-down list (**13**), select **Disabled**, **Normal Open** or **Authorization**.
Disabled turns off the first card mode.
Normal Open sets the door to remain open for the time interval specified in the Remain Open Duration, min field (see step 15).
Authorization sets the access point to accept any kind of authentication (except for super card, super password and duress card/code) only after the first card is authorized.

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

15. In the **Remain Open Duration, min** field (**14**), you can set the time interval during which the door will remain open after the first card is read in **Normal Open** mode.
16. In the **Multiauthentication Swipe Time** field (**15**), you can set a time-out interval between access requests in multiple card configuration (see Setting up multiple Hikvision cards).
17. Click the **Apply** button (**16**) to save your settings.

The *Hikvision* door is now configured.

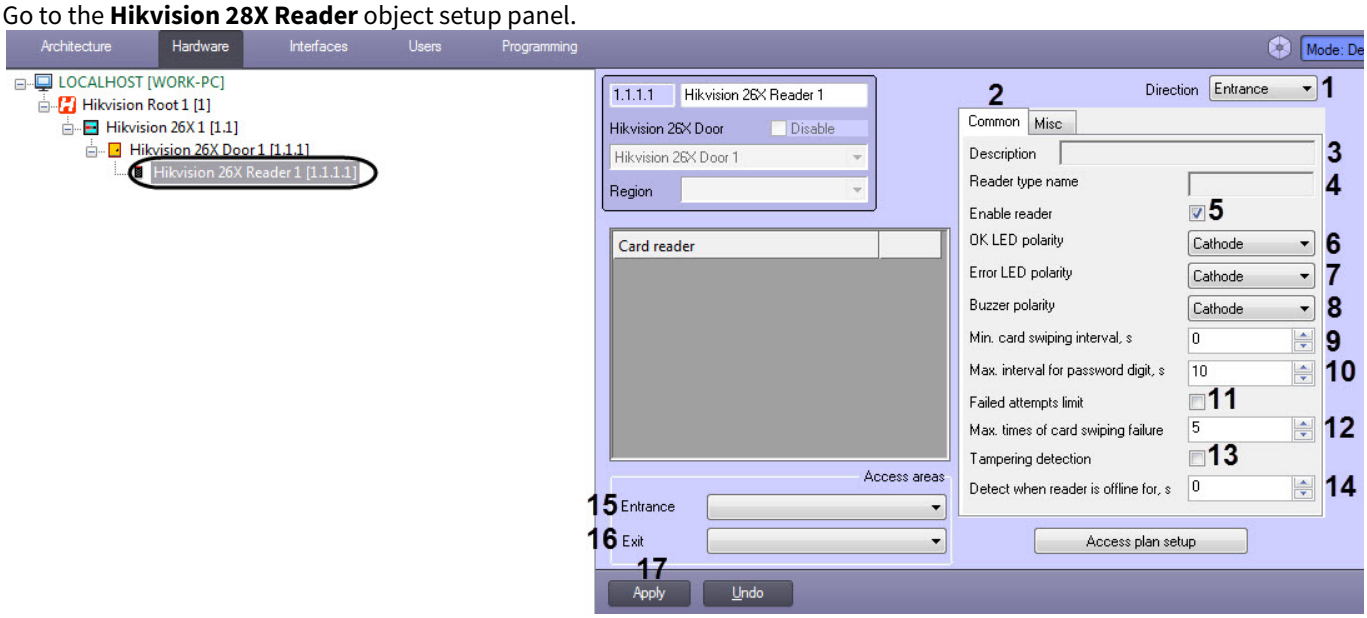
4.3.1 Configuring the Hikvision reader

> **Note**
>
> *Hikvision* reader configuration options depend on the *Hikvision* controller model. *Hikvision* reader configuration will be illustrated by an example of the *Hikvision 26X* controller.

4.3.1.1 Common settings of Hikvision reader

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

1. Go to the **Hikvision 28X Reader** object setup panel.



2. From the **Direction** drop-down list (**1**), select the reader's direction: **Exit** or **Entrance**.
3. Go to the **Common** tab (**2**).
4. The **Description** field (**3**) displays a brief description of the reader.
5. The reader type is displayed in the **Reader type name** field (**4**).
6. Check the **Enable reader** box (**5**) to activate the reader.
7. From the **OK LED polarity** drop-down list (**6**), select the buzzer's polarity on a successful card swipe.
8. From the **Error LED polarity** drop-down list (**7**), select the buzzer's polarity on a successful card swipe.
9. From the **Buzzer polarity** drop-down list (**8**), select a reader buzzer's polarity.
10. In the **Min. card swiping interval, s** field (**9**), specify the minimum time interval between two consecutive card swipes. You can set the interval from 0 to 255 seconds.
11. In the **Max. interval for password digit, s** field (**10**), specify the timeout interval between consecutive pressings of numeric keys while entering the password. If the time interval exceeds the timeout value, all previous entries are cancelled.

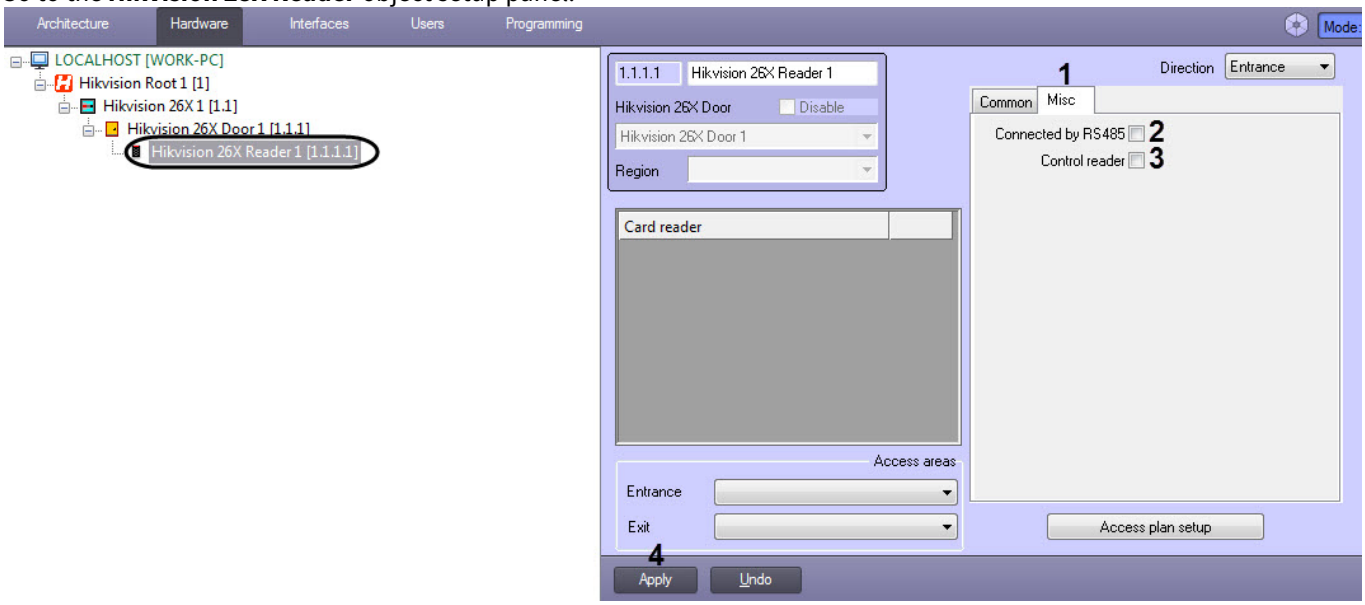
12. Check the **Failed attempts limit** box (**11**) to automatically generate an alarm in case of exceeding the permitted number of card swipes set in the **Max. times of card swiping failure** field (**12**).
13. In the **Max. times of card swiping failure** field (**12**), set the critical number of consecutive card swipes to generate an alarm if the **Failed attempts limit** box (**11**) is checked.
14. Check the **Tampering detection** box (**13**) to enable the detection of device tampering attempts.
15. In the **Detect when reader is offline for, s** field (**14**) field, specify the timeout interval to de-activate the reader on lost connection to the *Hikvision* controller.
16. From the **Entrance** drop-down list (**15**), select the section located on the door entry side.
17. From the **Exit** drop-down list (**16**), select the section located on the exit side of the door.
18. Click **Apply** button (**17**).

The *Hikvision* reader common settings are now configured.

4.3.1.2 Additional settings of Hikvision reader

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

1. Go to the **Hikvision 28X Reader** object setup panel.



2. Go to the **Misc** tab (**1**).
3. Set the **Connected by RS485** checkbox (**2**) if the reader is connected through the RS-485 interface.
4. Set the **Control reader** checkbox (**3**) 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 check the *Hikvision* door to which the reader is connected on the **Readers** tab of the **Access Manager** object settings panel (see Access Manager Module Settings and Operation Guide).

5. Click **Apply** (**4**).

The *Hikvision* reader additional settings are now configured.

4.3.1.3 Recognition settings of Hikvision reader

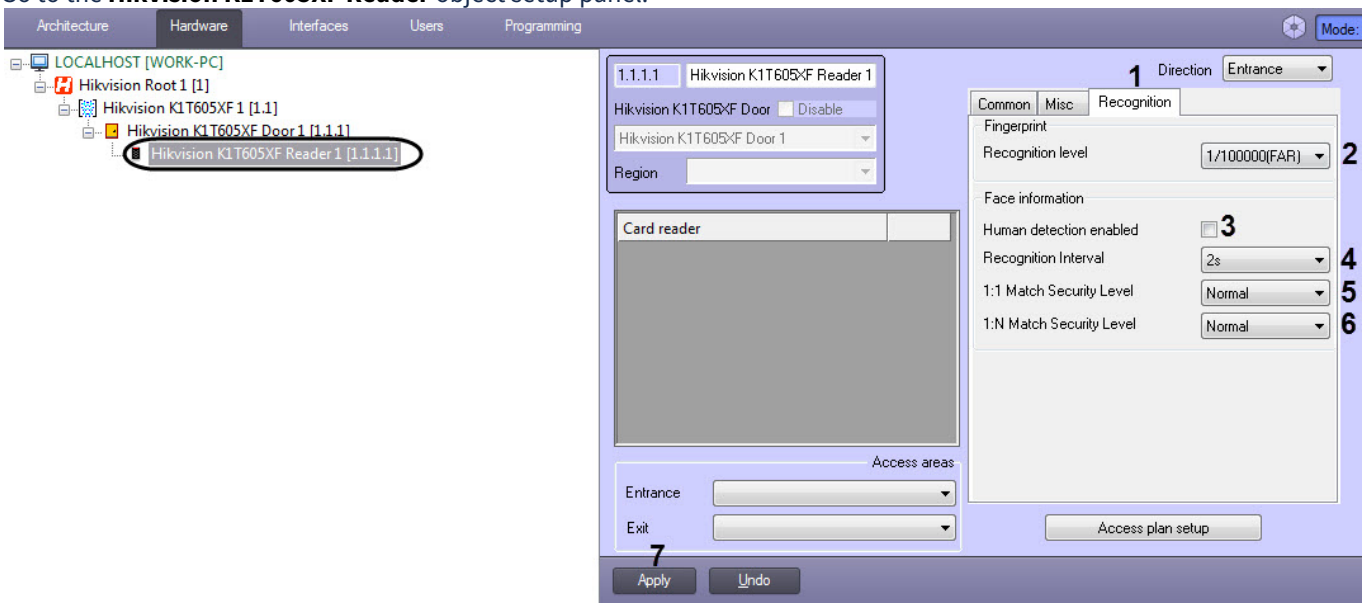
Recognition settings of *Hikvision* reader are available for access control terminals that contain both a face scanner and a built-in fingerprint reader.

> **Note**

> Recognition settings of *Hikvision* reader will be illustrated by an example of the *Hikvision K1T605XF* access control terminal. Network settings for other *Hikvision* terminals are similar.

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

1. Go to the **Hikvision K1T605XF Reader** object setup panel.



2. Go to the **Recognition** tab (**1**).
3. From the **Recognition level** drop-down list (**2**), 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.

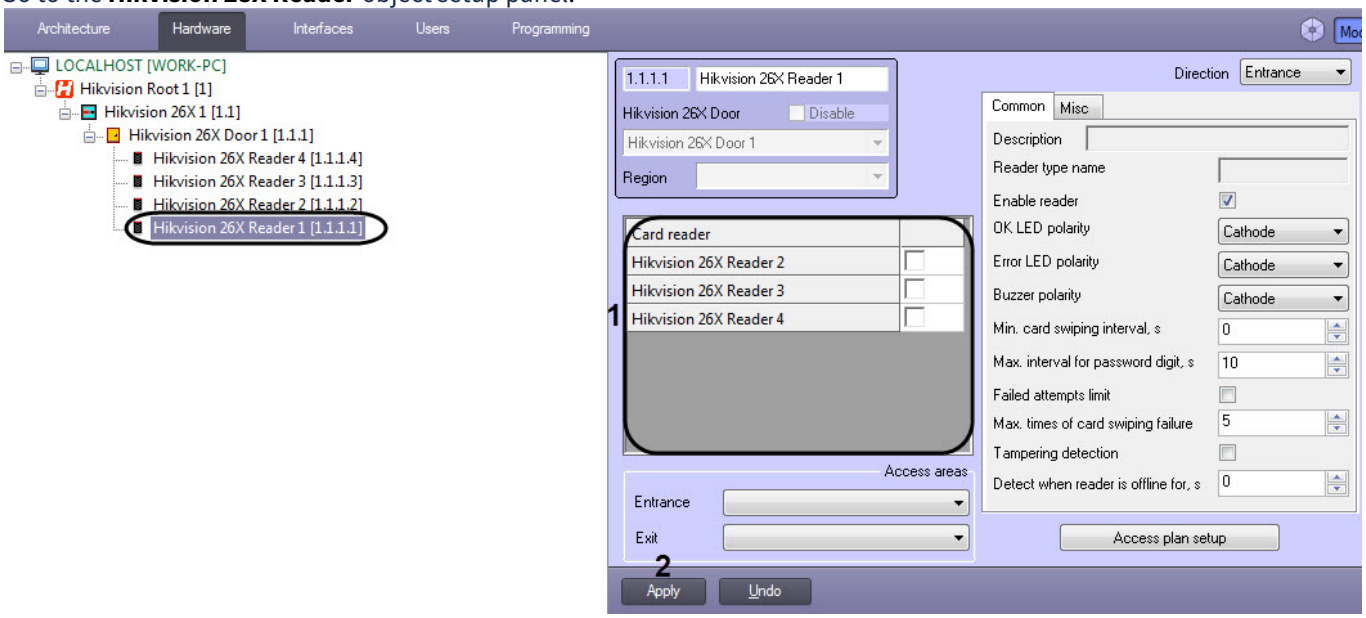
4. Set the **Human detection enabled** checkbox (**3**) to enable the detection of live faces.
5. From the **Recognition Interval** drop-down list (**4**), select the time interval in seconds between the previous and next face recognition during the continuous operation: from **1s** to **10s**.
6. From the **1:1 Match Security Level** drop-down list (**5**), select the verification quality level if only one type of authentication is used: **Normal**, **High**, or **Higher**.
7. From the **1:N Match Security Level** drop-down list (**6**), select the authentication quality level if several authentication types are used: **Normal**, **High**, or **Higher**.
8. Click the **Apply** button (**7**).

The *Hikvision* reader recognition settings are now configured.

4.3.1.4 Anti-passback settings of Hikvision Reader

To configure the *Hikvision* reader anti-passback settings, do the following:

1. Go to the **Hikvision 28X Reader** object setup panel.



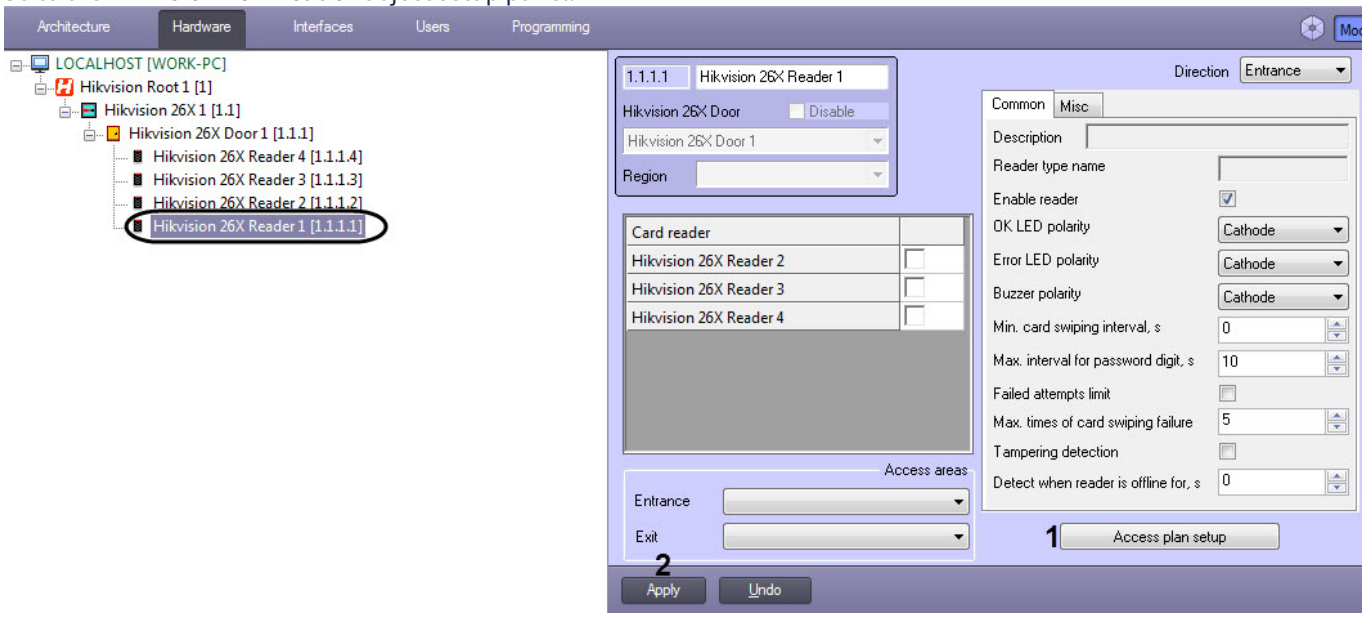
2. In the **Card reader** panel (**1**), select the checkboxes for the readers for which the anti-passback control will be set.
3. Click the **Apply** (**2**) button to save the settings.

The anti-passback settings of *Hikvision* reader are now configured.

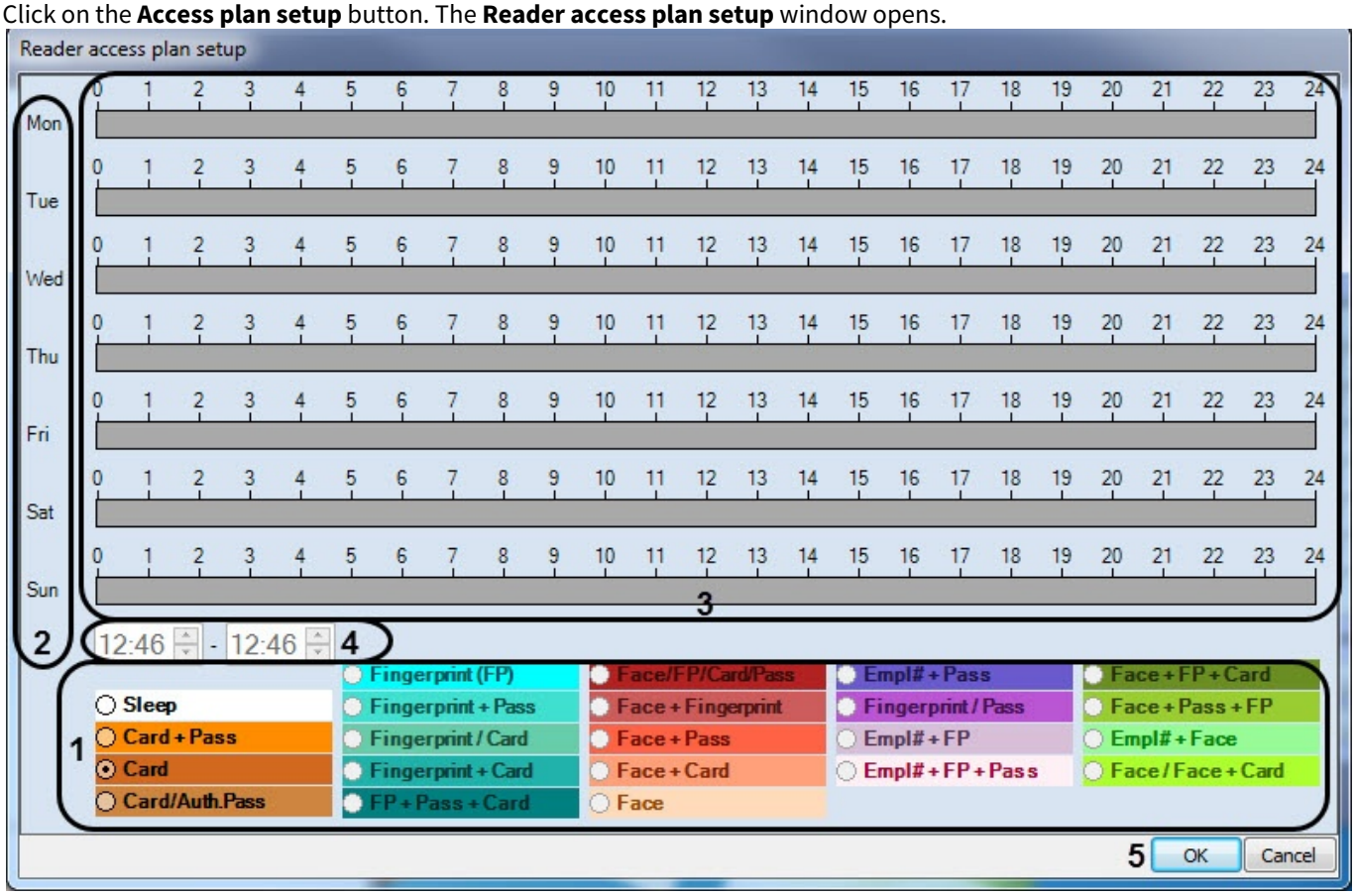
4.3.1.5 Access plan settings of Hikvision reader

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

1. Go to the **Hikvision 28X Reader** object setup panel.



2. Click on the **Access plan setup** button. The **Reader access plan setup** window opens.



3. In the area (1), set the required access type.

> **Note.**
>
> The **Sleep** access type stands for the sleep mode. The reader is not operable in this mode.
> The **Card + Pass** access type means that you first need to swipe the card and then enter the password, only then the access is granted.
> The **Card/Auth.Pass** access type means that you can swipe the card OR enter the password to access.

4. In 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 area (**3**).
5. If necessary, adjust the time interval in area (**4**), where the left field indicates the beginning time, and the right field indicates the ending time of this time interval.
6. Click **OK** (**5**) to save the settings.
7. Click **Apply** (**2**).

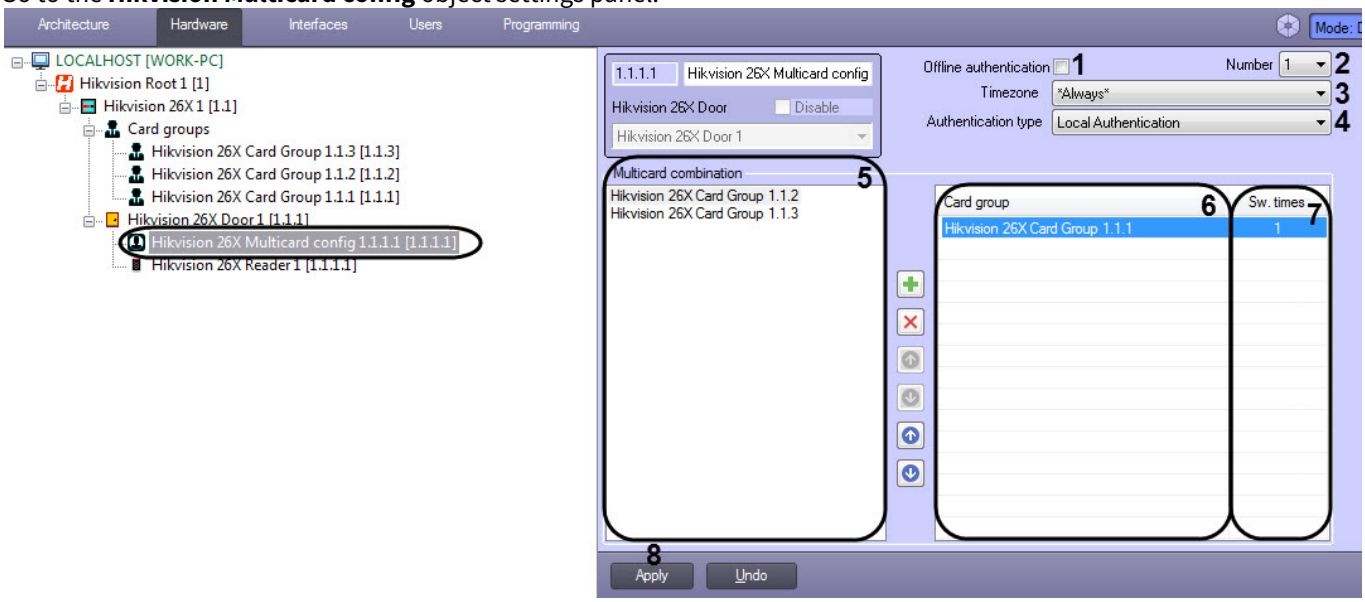
The access plan settings of the *Hikvision* reader are now configured.

4.3.2 Setting up multiple Hikvision cards

> **Note.**
>
> The ability to configure multiple *Hikvision* cards depends on the *Hikvision* controller model. Configuring multiple *Hikvision* cards will be illustrated by an example of the *Hikvision 26X* controller.
> Set up *Hikvision* card groups before setting up the multicard configuration (see Configuring the Hikvision card groups).

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

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



2. Check the **Offline authentication** box (**1**) to enable authentication using **Super Password** for an autonomous access point.
3. From the **Number** drop-down list (**2**), select a configuration ID number (**1** to **20**) corresponding to configuration's ID in the Hikvision controller.
4. Select a time zone from the **Timezone** drop-down list (**3**).
5. Select an authentication type from the **Authentication type** (**4**) drop-down list:
    a. **Local Authentication** is performed by regular user IDs (cards). You can link up to 8 card groups with this authentication type.
    b. **Local Auth. and Remotely Open** authentication automatically passes local ID check results to a remote operator for taking access decision. You can link up to 7 card groups with this authentication type.
    c. **Local Auth. and Super Password** authentication extends local ID check with the request for **Super Password**.
6. To add a card group to the **Card group** column (**6**), select a group in the **Multicard combination** (**5**) panel and press the button  .
7. To remove a group from the **Card group** column (**6**), select it and click the button  .
8. Use the  and  buttons to move a card group within the **Card group** column (**6**).
9. In the **Sw. times** column (**7**), you can use the  and  buttons to change the number of different card swipes required for granting access.

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

10. Click **Apply** (**8**).

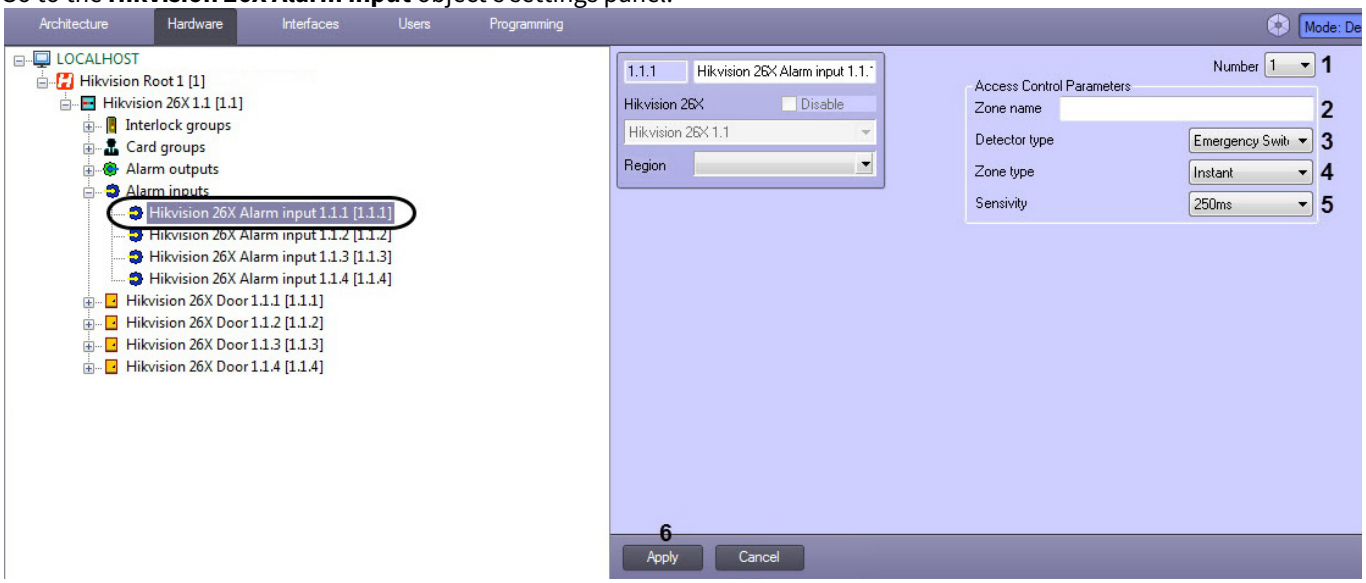
The *Hikvision* multicard configuration is now complete.

4.4 Configuring the Hikvision alarm input

> **Note**
>
> *Hikvision* alarm input configuration options depend on *Hikvision* controller model. Configuring the Hikvision alarm input will be illustrated by an example of a *Hikvision 26X* controller.

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

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



2. In the **Number** drop-down list (**1**), you see the alarm input's ID number corresponding to its ID in the *Hikvision* controller. You can not change this value.
3. In the **Zone name** field (**2**), enter the alarm input name under which it will further appear in the *Intellect* PSIM.
4. Select a detector type from the **Detector type** drop-down list (**3**):

Emergency Switch	Emergency switch sensor
Door Magnetic	Door Magnetic
Smoke	Smoke sensor
Active Infrared	Active infrared sensor
Passive Infrared	Passive infrared sensor
Glass Break	Glass break sensor
Vibration	Vibration sensor
Dual Tech.PIR	Dual technology PIR sensor
Dual technology PIR sensor	Triple technology PIR sensor
Humidity	Humidity sensor
Temperature	Temperature sensor
Combustible Gas	Flammable gas sensor
Other Detector	Other type of sensor

5. Select a zone type from the **Zone type** drop-down list (**4**):

Instant	Instant zone
24 Hours	Permanently controlled zone
Door Emg. open	Open emergency door zone
Door Emg. shutdown	Inactive emergency door zone
Shield Zone	Protected zone

6. From the **Sensivity** drop-down list (**5**), select a sensivity value in milliseconds: **10ms**, **250ms**, **500ms**, **750ms**.

7. Click the **Apply** button (**6**).

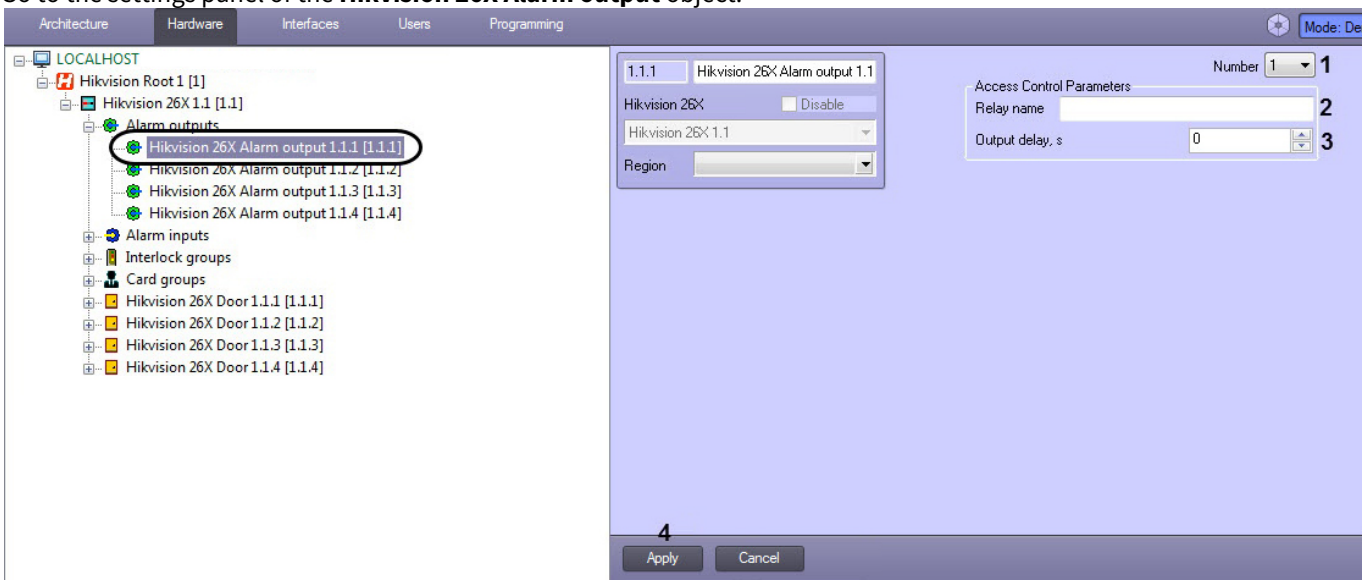
The *Hikvision* alarm input is now configured.

4.5 Configuring the Hikvision alarm output

> **Note**
>
> *Hikvision* alarm output configuration options depend on *Hikvision* controller model. Configuring the Hikvision alarm output will be illustrated by an example of a *Hikvision 26X* 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 (**1**), you see the alarm output's ID number corresponding to its ID in the *Hikvision* controller. You can not change this value.
3. In the **Relay name** field (**2**), enter the alarm output name under which it will further appear in the *Intellect* PSIM.
4. In the **Output delay, s** field (**3**), enter the desired delay time for your alarm output.
5. Click **Apply** button (**4**).

The *Hikvision* alarm output is now configured.

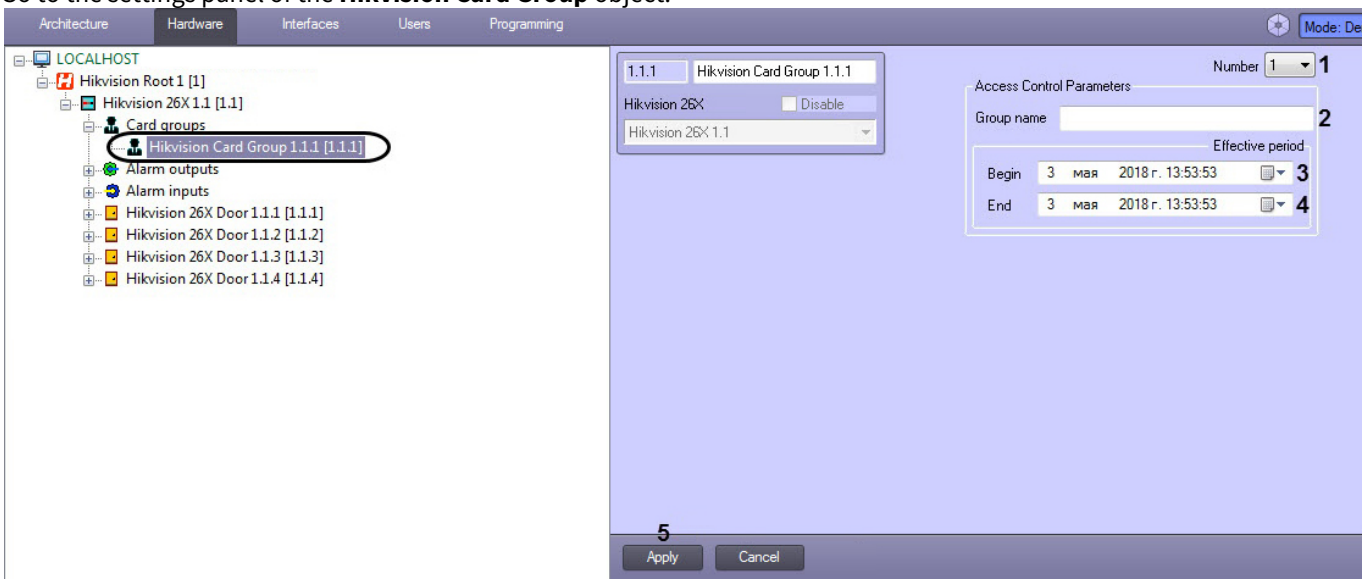
4.6 Configuring the Hikvision card groups

The **Hikvision Card Group** object is intended for grouping cards when setting up the *Hikvision* multiple card configuration (see Setting up multiple Hikvision cards).

> **Note**
>
> *Hikvision* card groups configuration options depend on *Hikvision* controller model. Configuring the *Hikvision* card groups will be illustrated by an example of a *Hikvision 26X* 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 (**1**) , select ID numbers of card groups (from **1** to **32**) corresponding to their ID numbers in the *Hikvision* controller.
3. In the **Group name** field (**2**), enter the card group names.
4. In the **Begin** field (**3**), use the button to set the activation time for each card group.

> **Note.**
>
> The beginning of the card group period can not be set after the end of the card group period. It is recommended to set the valid end date for the card group period first (see step 5).

5. In the **End** field (**4**), use the button to set the de-activation time for each card group.

> **Note.**
>
> The end of the card group period can not be set before the start of it.

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

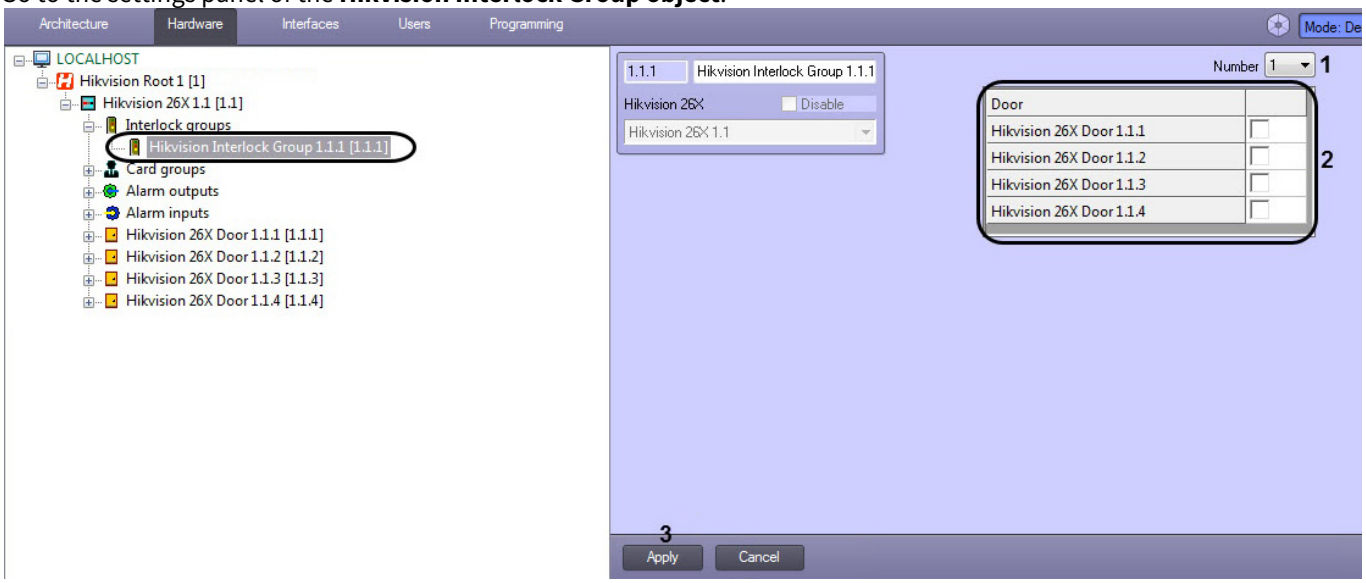
The *Hikvision* card groups are now configured.

4.7 Configuring the Hikvision interlock group

> **Note**
>
> *Hikvision* interlock group configuration options depend on *Hikvision* controller model. Configuring the *Hikvision* interlock group will be illustrated by an example of a *Hikvision 26X* 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 (**1**), select the interlock group number ID corresponding to this group's ID in the *Hikvision* controller.
3. In the **Door** panel (**2**), check the boxes for the relevant *Hikvision* doors.

> **Note.**
>
> All doors are to be closed to open one of them. This means that only one door in the interlock group can be opened at a time.

4. Click the **Apply** button (**3**) to save the settings.

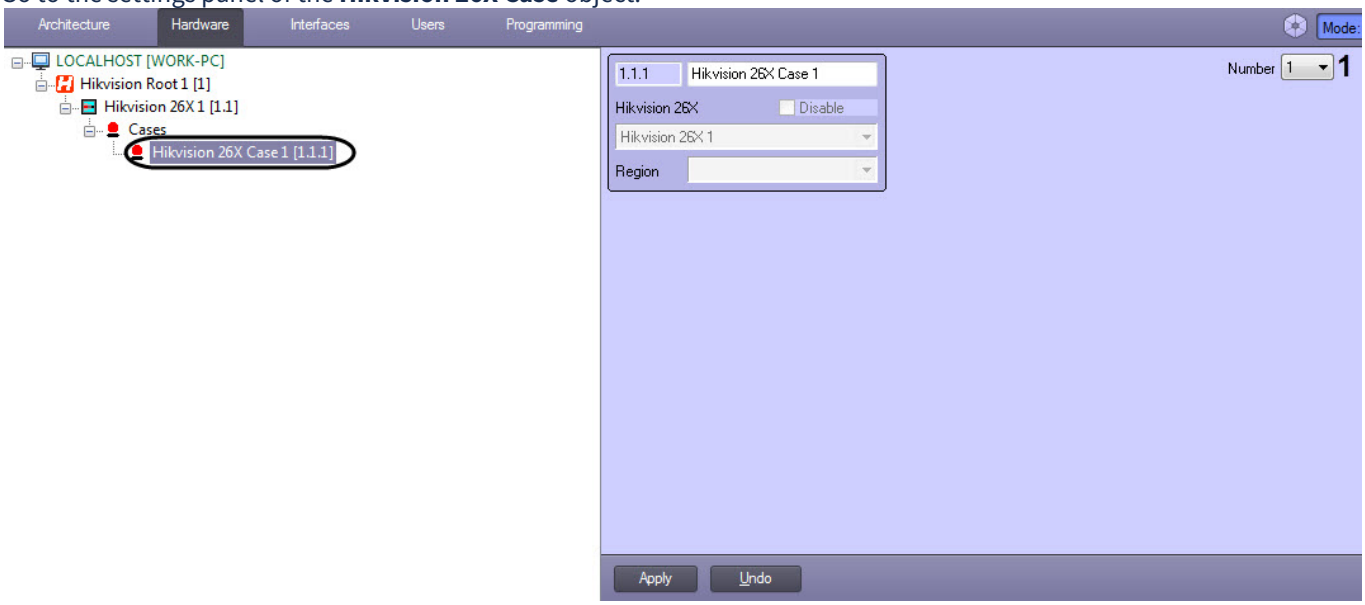
The *Hikvision* interlock group is now configured.

4.8 Configuring the Hikvision case

> **Note**
>
> *Hikvision* case configuration options depend on *Hikvision* controller model. Configuring the *Hikvision* case will be illustrated by an example of a *Hikvision 26X* controller.

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

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



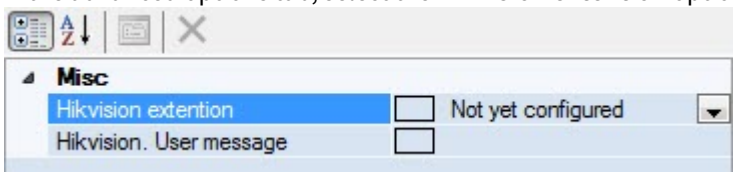
2. From the **Number** drop-down list (**1**), select the event input number: from **1** to **8**.
3. Click the **Apply** button to save the settings.

The *Hikvision* case is now configured.

4.9 Configuring the Hikvision user cards

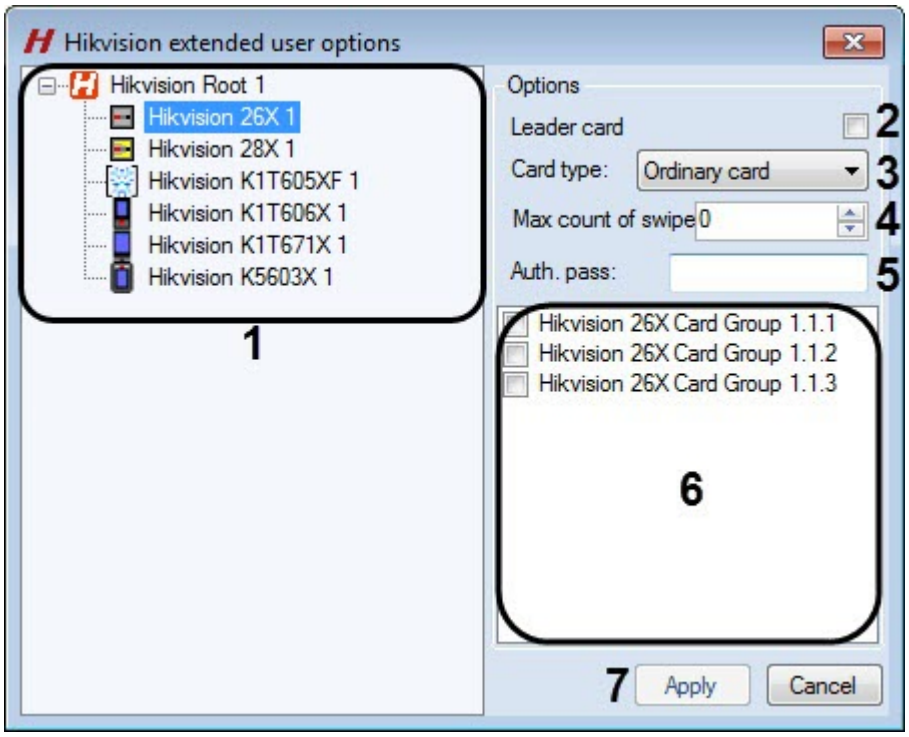
To configure the *Hikvision* user cards, do the following:

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** option and click the button.



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

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



3. Select the required *Hikvision* controller from the object tree (**1**).
4. Set the **Leader card** checkbox (**2**) if it is necessary to activate all readers connected to this controller by the first card swipe through any of the readers.
5. From the **Card type** drop-down list (**3**), select the card type:

Invalid	Invalid card
Ordinary card	Normal card
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).
Blacklist card	When a blacklisted card is swiped, a system event is generated without granting access
Patrol card	This type of cards can be used by supervisors
Stress card	If a user is under duress, this card opens the door and generates a duress alarm
Super card	This card opens all doors of a given controller within a time zone defined by user's access level
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).

6. Set a limit for a number of **Visitor card** swipes in the **Max count of swipe** field (**4**).

> **Note.**
>
> 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 (**5**). The password consists of 4 to 8 digits.

> **Note**
>
> The availability of this parameter setting depends on the *Hikvision* controller model.

8. Check the boxes for the required card groups in the (**6**) field.

> **Note**
>
> The availability of this parameter setting depends on the *Hikvision* controller model.

9. Click the **Apply** button (**7**) to save the changes.

The *Hikvision* user cards are now configured.

5 Hikvision integration module operation

5.1 General information on Hikvision integration module operation

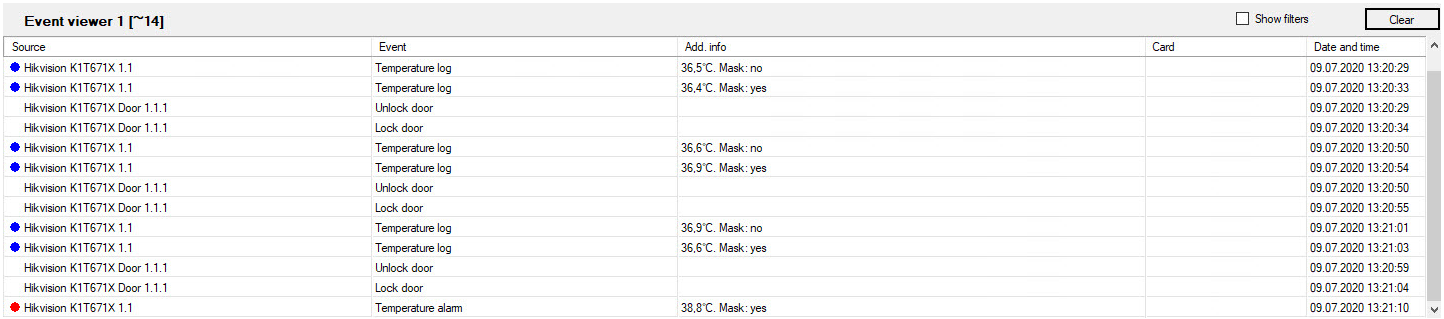
The following interface objects are used for HikVision integration module operation:

1. **Map**;
2. **Event Log**.

For detailed description of configuring these interface objects, please refer to the Intellect PSIM Administrator's Guide.

For detailed description of using these interface objects, please refer to the Intellect 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 options are configured on the terminal (for details, see the manufacturer's documentation).



Source	Event	Add. info	Card	Date and time
Hikvision K1T671X 1.1	Temperature log	36,5°C. Mask: no		09.07.2020 13:20:29
Hikvision K1T671X 1.1	Temperature log	36,4°C. Mask: yes		09.07.2020 13:20:33
Hikvision K1T671X Door 1.1.1	Unlock door			09.07.2020 13:20:29
Hikvision K1T671X Door 1.1.1	Lock door			09.07.2020 13:20:34
Hikvision K1T671X 1.1	Temperature log	36,6°C. Mask: no		09.07.2020 13:20:50
Hikvision K1T671X 1.1	Temperature log	36,9°C. Mask: yes		09.07.2020 13:20:54
Hikvision K1T671X Door 1.1.1	Unlock door			09.07.2020 13:20:50
Hikvision K1T671X Door 1.1.1	Lock door			09.07.2020 13:20:55
Hikvision K1T671X 1.1	Temperature log	36,9°C. Mask: no		09.07.2020 13:21:01
Hikvision K1T671X 1.1	Temperature log	36,6°C. Mask: yes		09.07.2020 13:21:03
Hikvision K1T671X Door 1.1.1	Unlock door			09.07.2020 13:20:59
Hikvision K1T671X Door 1.1.1	Lock door			09.07.2020 13:21:04
Hikvision K1T671X 1.1	Temperature alarm	38,8°C. Mask: yes		09.07.2020 13:21:10

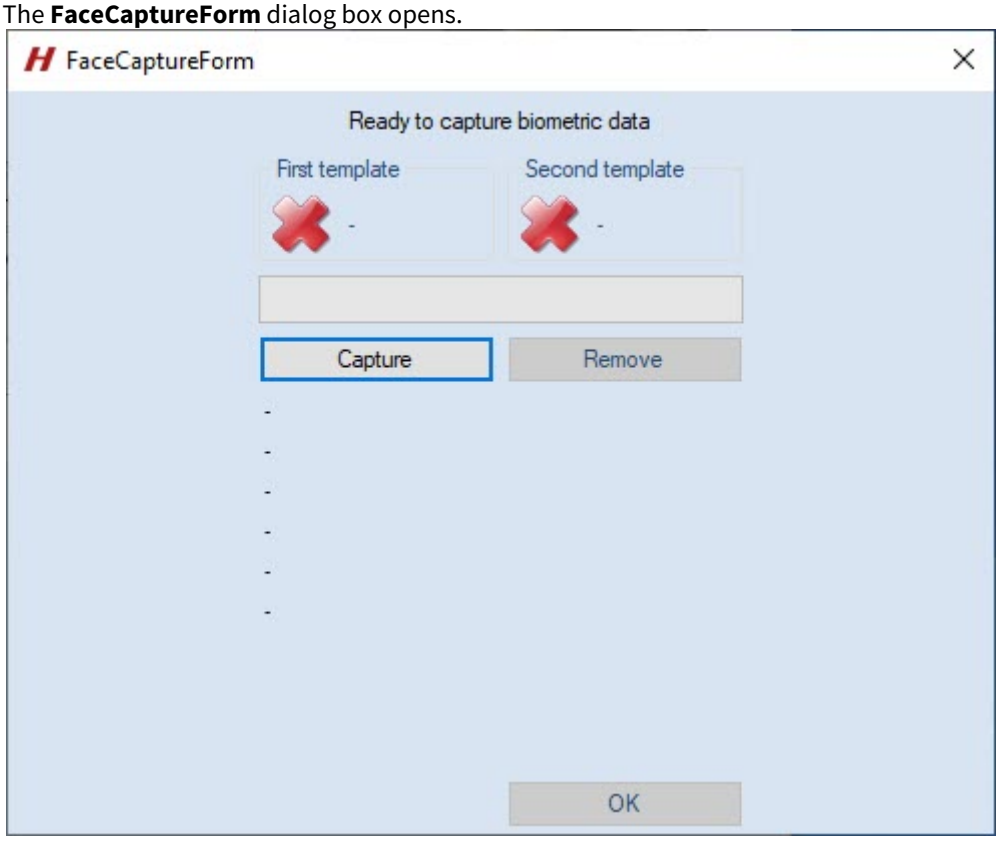
5.2 Adding the Hikvision biometric parameters

5.2.1 Adding the Hikvision face template

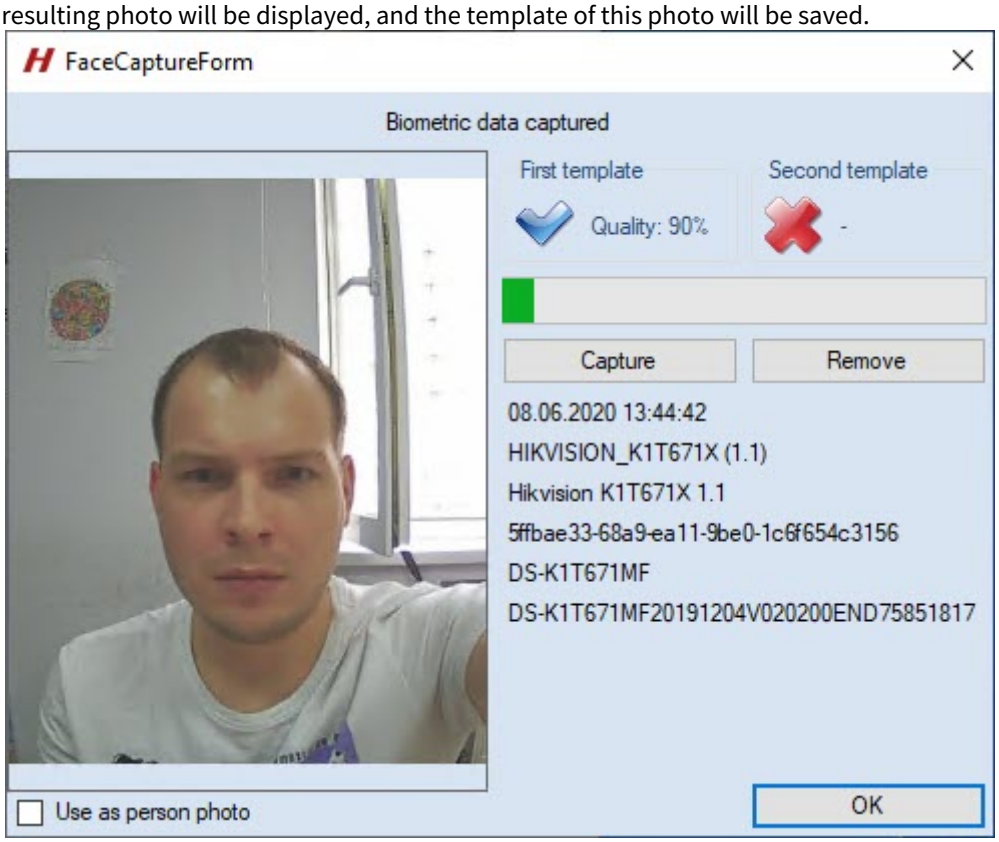
To add a *Hikvision* face template in the *Access Manager* module, do the following:

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 in the terminal from which the face was captured, and the face caption will be deleted during the next addition of access parameters.

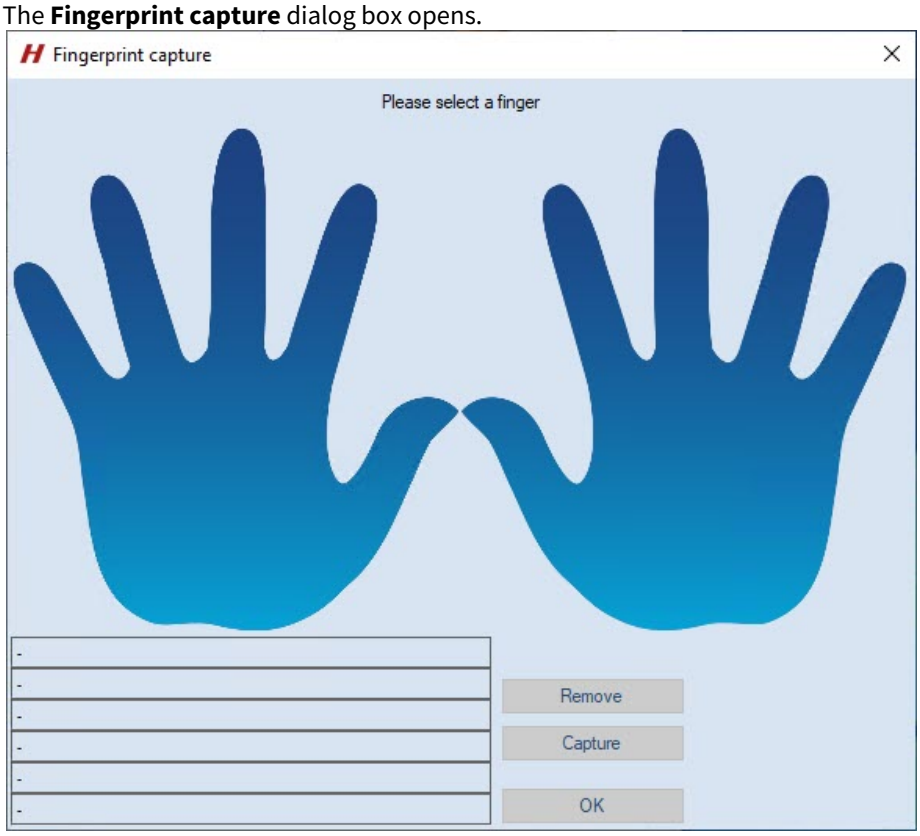
6. To delete a face template, click the **Remove** button.
7. Click **OK** to save the face template.

The *Hikvision* face template is added.

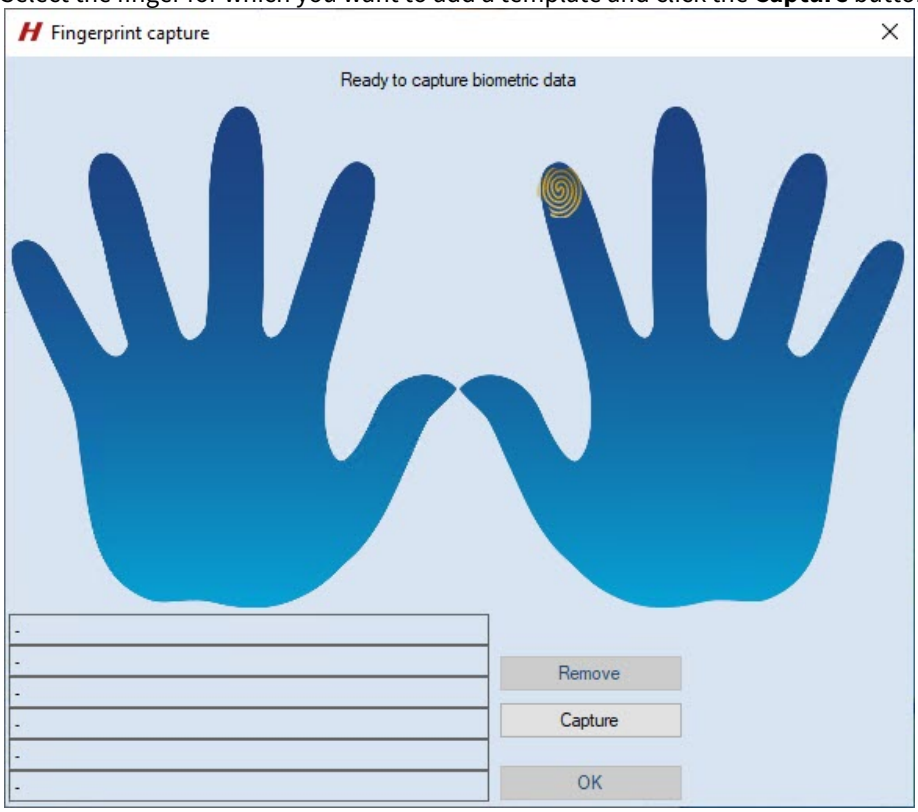
5.2.2 Adding the Hikvision fingerprints

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

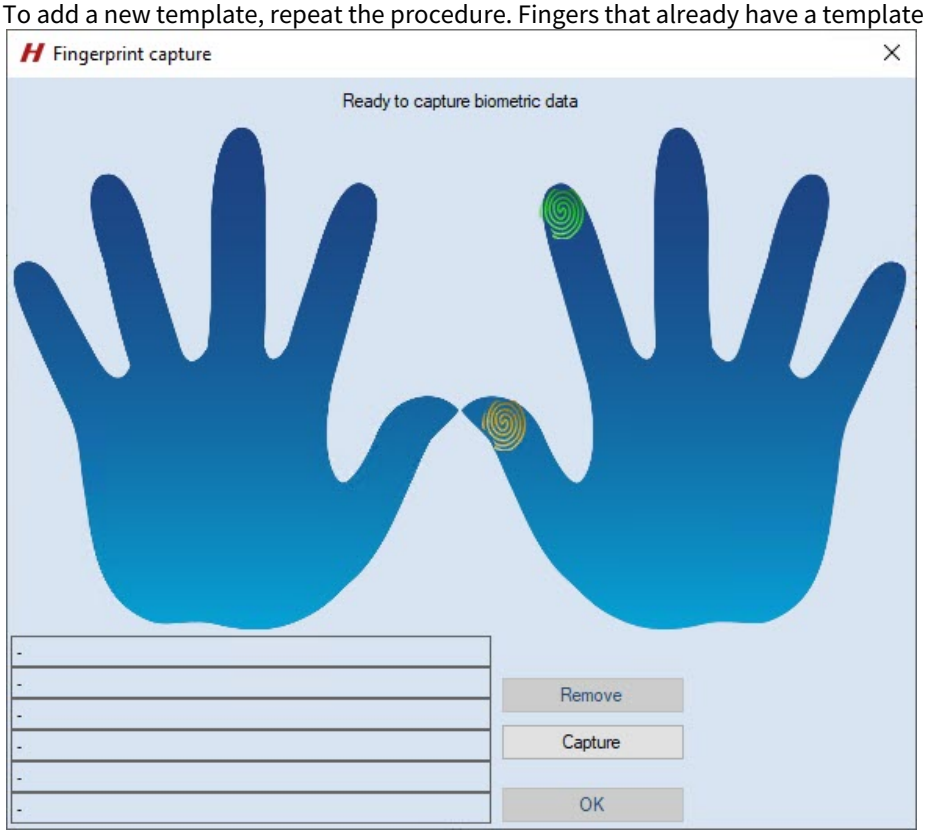
1. Go to adding biometric data in the **Access Manager** window (see Adding biometric parameters).
2. Select the extension **(Hikvision Fingerprint) <Controller/terminal name>** that corresponds to the controller with the biometric fingerprint reader connected to it, or to the terminal.
3. The **Fingerprint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

> **Note.**
>
> The *Hikvision* controllers can not be controlled from the **Map**.

The *Hikvision KV* series panel is managed in the **Map** interactive window using the **Hikvision KVx** object functional menu:

The **Hikvision KVx** object functional menu commands description is given in the table.

Menu command	Function performed
Open	Open

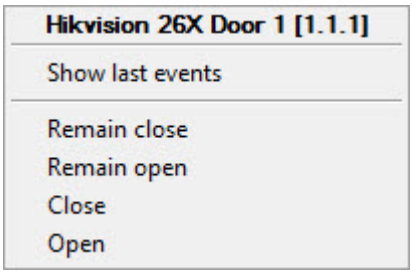
There can be the following states:

> **Note**
>
> The status images are the same for all *Hikvision* controllers/panels.

	Battery low
	Connection lost
	Mains powered
	Battery powered

5.4 Managing a Hikvision door

> **Note.**
>
> Managing a *Hikvision* door is described by example of the **Hikvision 26X** controller's door. Managing other *Hikvision* controllers' doors is performed in the same way.



The description of the commands of the functional menu of the *Hikvision* door is given in the table.

Menu item	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

Door states can be as follows:

> **Note**
>
> Door status images are the same for all *Hikvision* controllers.

	Normal
	Permanently closed
	Permanently open
	Standby
	Locking disabled

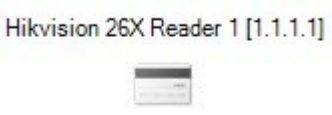
	Locking failure
	Always locked
	Magnetic sensor disabled
	Magnetic sensor failure
	Magnetic sensor shorted

5.5 Managing a Hikvision reader

> **Note.**
>
> The *Hikvision* reader is not controlled from the **Map**.

Reader states can be as follows:

> **Note**
>
> Reader status images are the same for all *Hikvision* controllers.

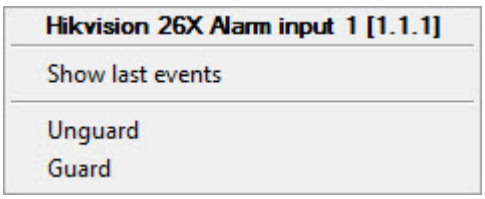
	Mode: map
	Mode: other

	Offline
	Tampering

5.6 Managing a Hikvision alarm input

> **Note**
>
> Managing a *Hikvision* alarm input is described by example of the **Hikvision 26X** controller's alarm input. Managing other *Hikvision* controller's alarm inputs is performed in the same way.

The *Hikvision* alarm input is managed in the **Map** interactive window using the **HikVision 26X Alarm input** object's functional menu.

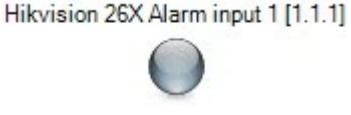


Hikvision alarm input menu commands are described in the following table.

Menu item	Function
Unguard	Disarming
Guard	Arming

Alarm input states can be as follows:

> **Note**
>
> Alarm input status images are the same for all *Hikvision* controllers.

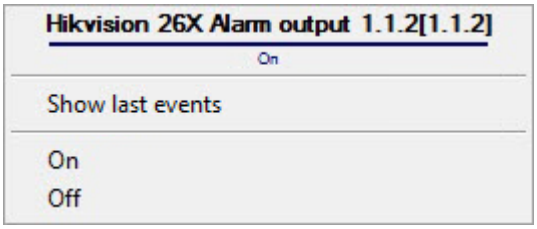
	Armed
	Disarmed

Hikvision 26X Alarm input 1 [1.1.1] 	Alarm

5.7 Managing a Hikvision alarm output

> **Note.**
>
> Managing a *Hikvision* alarm output is described by example of the **Hikvision 26X** controller's alarm output. Managing other *Hikvision* controllers' alarm outputs is performed in the same way.

The *Hikvision* alarm output is managed in the **Map** interactive window using the **HikVision 26X Alarm output** object's functional menu.



Hikvision alarm output menu commands are described in the following table.

Menu item	Function
On	Enable
Off	Disable

Alarm input states can be as follows:

> **Note**
>
> Alarm output status images are the same for all *Hikvision* controllers.

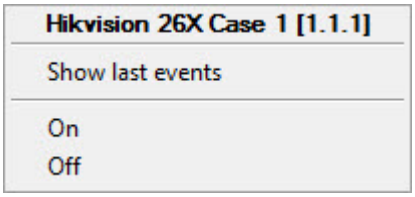
Hikvision 26X Alarm output 1 [1.1.1] 	Active
Hikvision 26X Alarm output 1 [1.1.1] 	Inactive

5.8 Managing a Hikvision case

> **Note**

Managing a *Hikvision* case is described by example of the **Hikvision 26X** controller's case. Managing other *Hikvision* controllers' cases is performed in the same way.

The *Hikvision* case is managed in the **Map** interactive window using the **HikVision 26X Case** object's functional menu.



Hikvision case menu commands are described in the following table.

Menu item	Function
On	Enable
Off	Disable

Hikvision case states can be as follows:

Note

Case status images are the same for all *Hikvision* controllers.

	Off
	On