ACFA Intellect

Hikvision Integration Module Settings Guide

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, gaty 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.

Introduction in the Hikvision Integration Module Configuration and Operation Guide

On the page:

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.

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).

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	Characterization
DS-K2604	Access controller	Up to 100,000 card records are supported Up to 300,000 events are supported Physical interfaces: Ethernet, RS-485 Readers can be connected via RS-485 or Wiegand (w26/w34) Up ro 8 readers can be connected via RS-485 and up to 4 via Wiegand 21 Alarm Inputs 8 Alarm Outputs
DS-K2804	Access controller	Number of supported card records: up to 10,000 Number of supported events: up to 50,000 Ethernet interface Wiegand interface (w26/w34) Up to 4 readers can be connected via Wiegand 12 Alarm Inputs 8 Alarm Outputs
DS-K1F100-D8E	Card reader	Operating frequency: 13.56MHz /125kHz Operating range: 10 to 30mm Supported card formats: Mifare, CPU, PSAM, ID and EM

DS-K1802E	Card reader	Operating frequency: 125MHz. Operating range: 30 to 50mm. Card format: EM-MARINE Communication protocol: Wiegand (w25/w37) Only for DS-K28xx series controllers
DS-K1107E	Card reader	Operating frequency: 125MHz. Operating range: 30 to 50mm. Communication protocols: Wiegand (w25/w37), RS-485 Supported card format: EM-MARINE
DS-K1802MK	Card reader	Operating frequency: 13.56MHz Operating range: 30-50mm Communication protocol: Wiegand (w25/w37) Card format: Mifare Only for DS-K28xx series controllers
DS-K1107MK	Card reader	Operating frequency: 13.56MHz Operating range: 30 to 50mm. Communication protocols: Wiegand (w26/w34), RS-485. Card format: Mifare Only for DS-K28xx series controllers

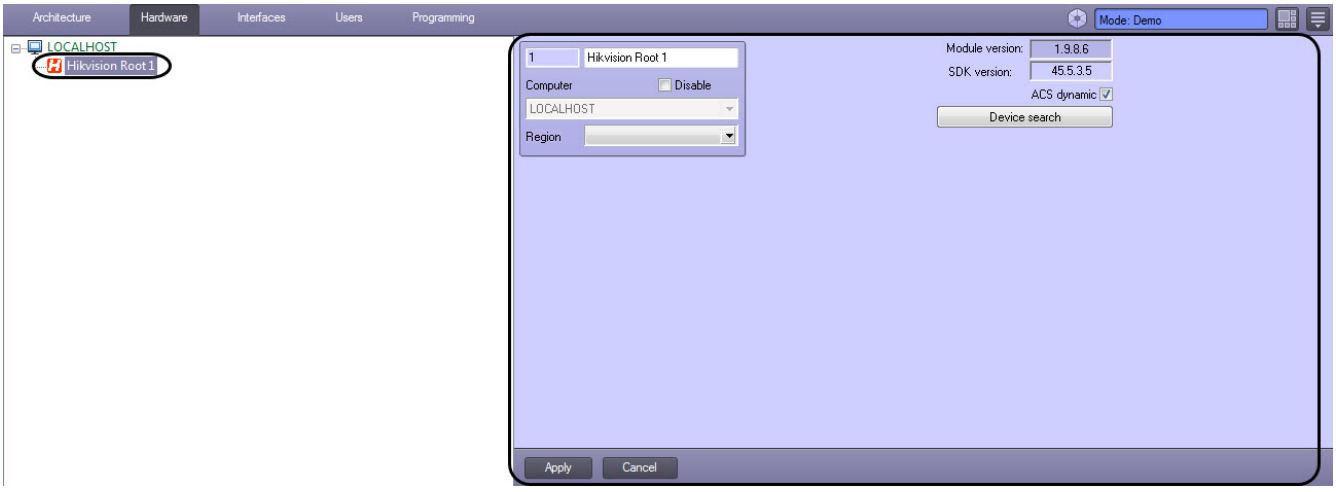
Software Licensing

Per reader

Configuring the Hikvision integration module

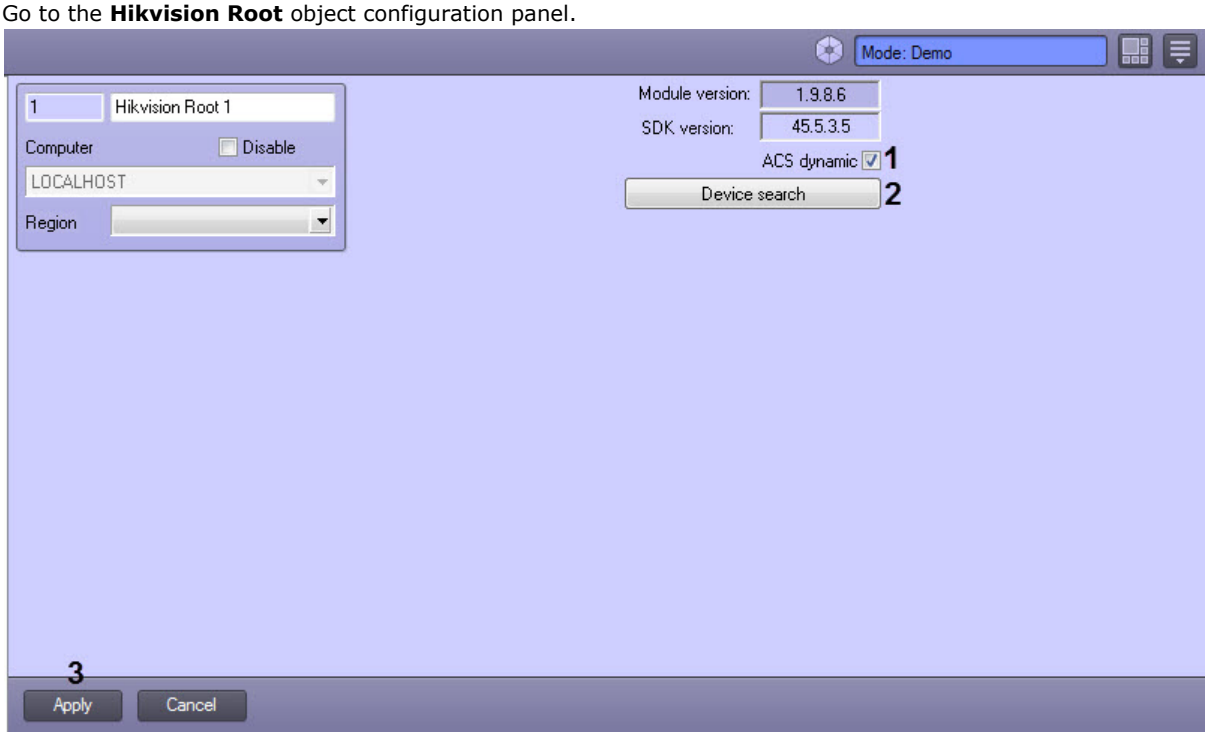
Setting up the Hikvision ACS connection

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.

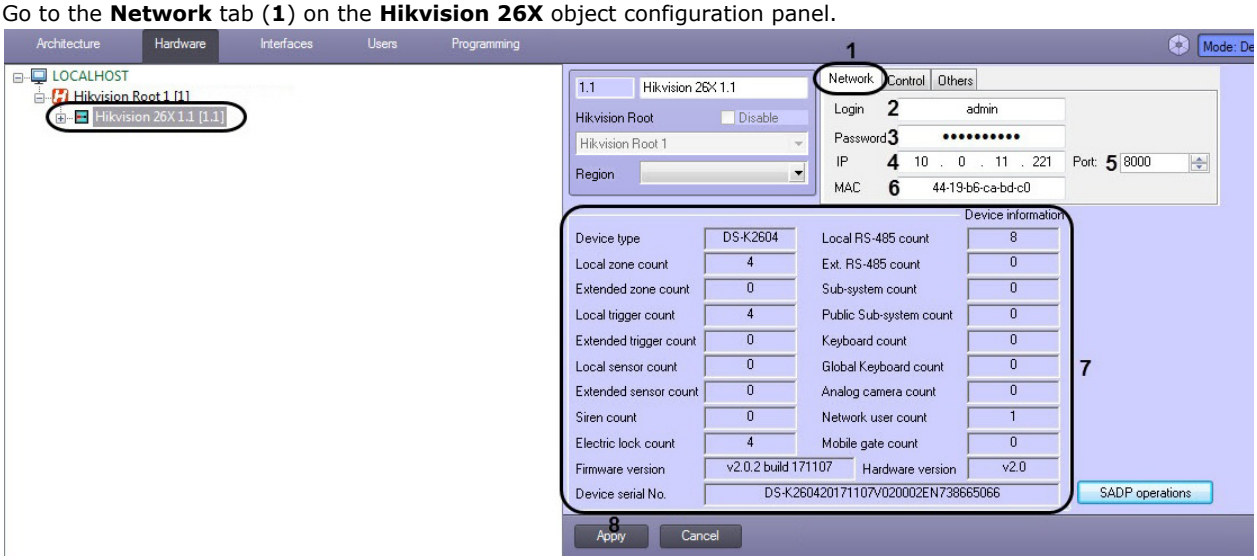
Configuring the Hikvision access controller

Network settings of the Hikvision controller

You can configure network settings of a *Hikvision* controller on the **Hikvision 26X** or **Hikvision 28X** object's configuration panel. You can create these objects under a parent **Computer** object using the **Settings** dialog box on the **Hardware** tab, or it can be created automatically (refer to Setting up the Hikvision ACS connection). As an example of *Hikvision* controller settings, let's consider a *Hikvision 26X* controller.

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.

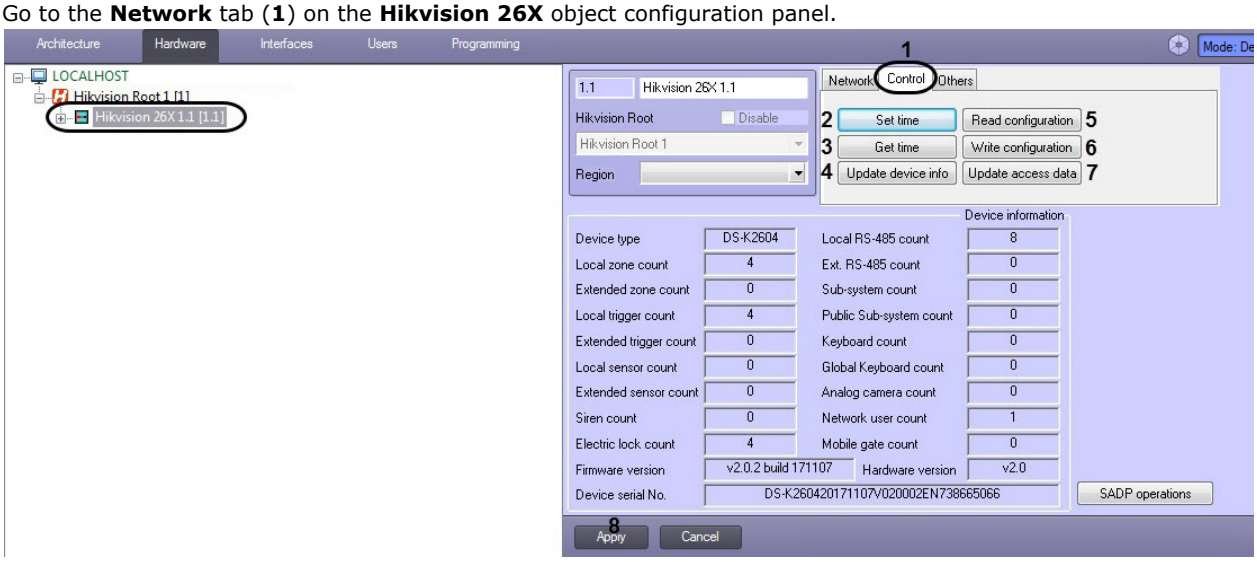
The network settings of the *Hikvision* controller are now complete.

Configuring the Hikvision controller

You can configure of a *Hikvision* controller via the **Hikvision 26X** or **Hikvision 28X** object configuration panel. You can create these objects under a parent **Computer** object using the **Settings** dialog box on the **Hardware** tab, or it can be created automatically (see Setting up the Hikvision ACS connection). As an example of *Hikvision* controller configuration management, let's consider a *Hikvision 26X* controller.

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

1. Go to the **Network** 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.

> **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.

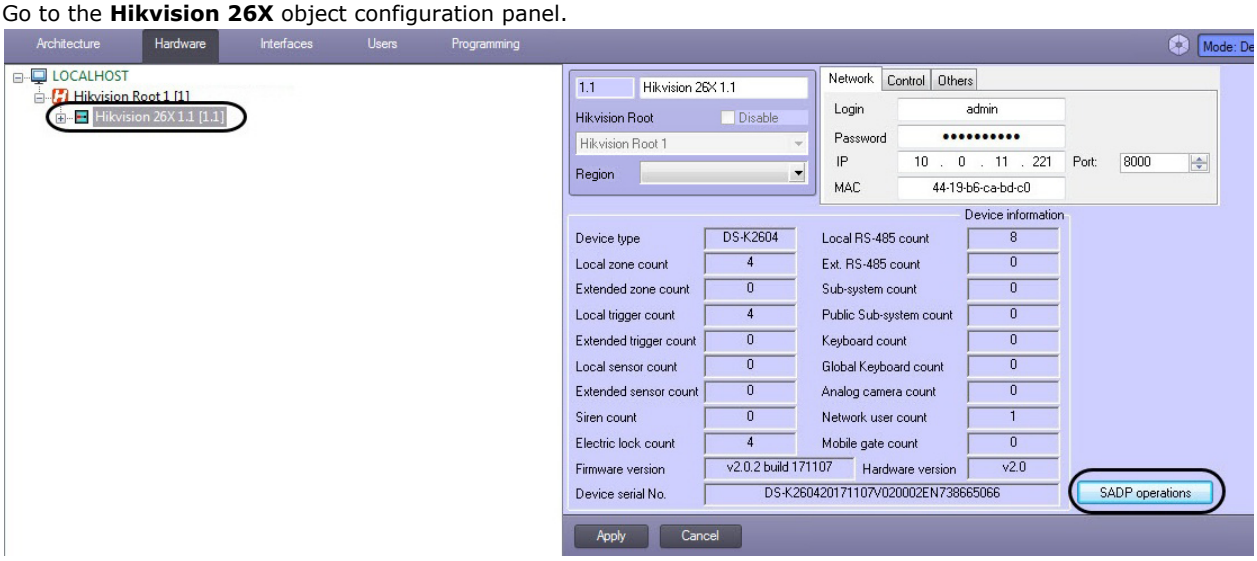
The *Hikvision* controller is now configured.

Hikvision SADP settings

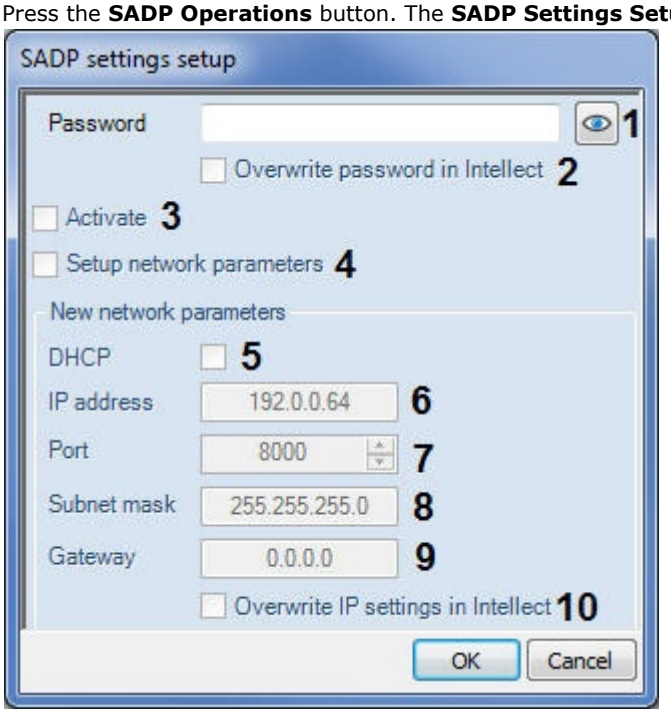
The *Hikvision* SADP is configured via the **HikVision 26X** or **HikVision 28X** object configuration panel. As an example of *Hikvision* SADP configuration, let's consider a *Hikvision 26X* controller.

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.

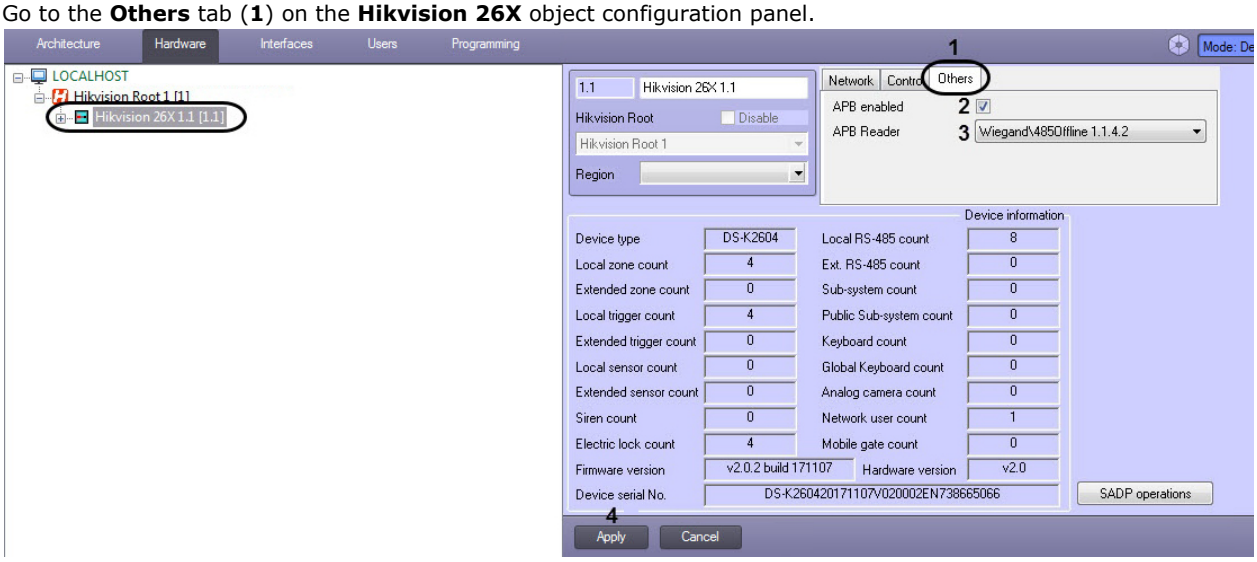
Hikvision SADP settings are now completed.

Advanced settings for a Hikvision controller

Advanced settings for the *Hikvision* controller are available via the **Hikvision 26X** or **Hikvision 28X** object configuration panel. You can create these objects under a parent **Computer** object using the **Settings** dialog box on the **Hardware** tab, or it can be created automatically (see Setting up the Hikvision ACS connection). As an example of *Hikvision* controller advanced settings, let's consider a *Hikvision 26X* controller.

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.

Configuring the Hikvision door

You can configure a *Hikvision* door via the settings panel of the **Hikvision door** object, which is automatically created on the basis of **Hikvision 26X** or **Hikvision 28X** object after reading the configuration of the corresponding controller (refer to Network settings of the Hikvision controller and Network settings of the Hikvision controller). As an example of *Hikvision* door configuration, let's consider a door created on the basis of the **Hikvision 26X** object.

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 the Hikvision multicard configuration).
17. Click the **Apply** button (**16**) to save your settings.

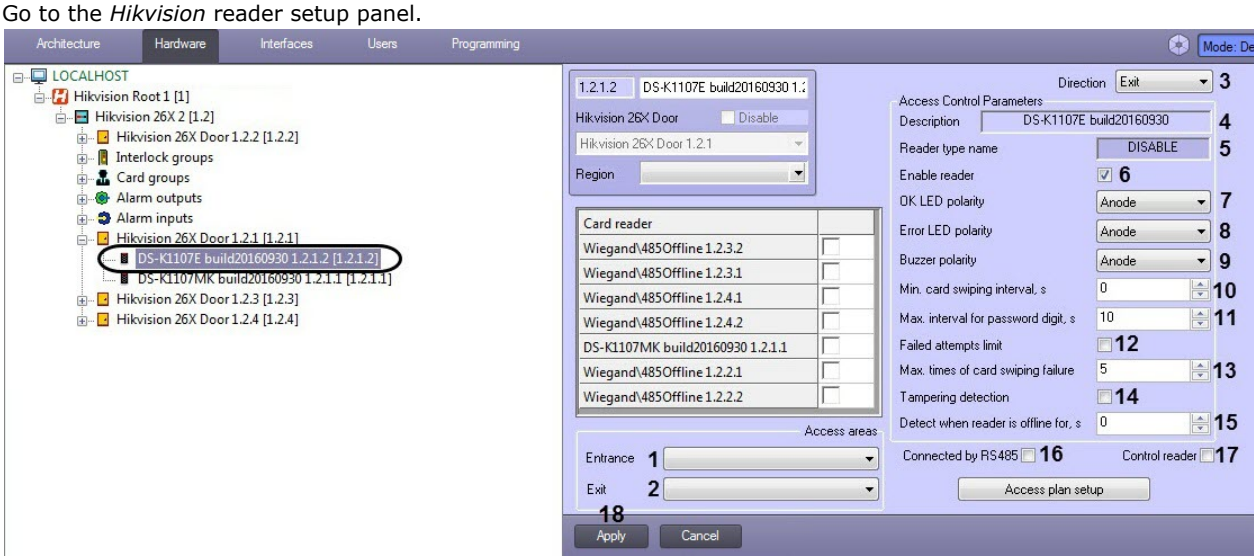
The *Hikvision* door is now configured.

Configuring a Hikvision reader

You can configure a *Hikvision* reader via the settings panel of the *Hikvision* reader object, which is automatically created on the basis of **Hikvision 26X** or **Hikvision 28X** object after reading the configuration from the corresponding controller (see Network settings of the Hikvision controller and Configuring the Hikvision controller). As an example of *Hikvision* reade r configuration, let's consider a *Hikvision* reader connected to a **Hikvision 26X** controller.

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

1. Go to the *Hikvision* reader setup panel.



2. In the **Direction** drop-down list (**3**), you see the reader's direction: **Exit** or **Entrance**. You can not change this value.
3. The **Description** field (**4**) contains a brief description of the reader.
4. The reader type is displayed in the **Reader Type Name** field (**5**).
5. Check the **Enable Reader** box (**6**) to activate the reader.
6. From the **OK LED Polarity** drop-down list (**7**), select the buzzer's polarity on a successful card swipe.
7. From the **Error LED Polarity** drop-down list (**8**), select the buzzer's polarity on a successful card swipe.
8. From the **Buzzer Polarity** drop-down list (**9**), select a reader buzzer's polarity.
9. In the **Min. Card Swiping Interval, s** field (**10**), specify the minimum time interval between two consecutive card swipes. You can set the interval from 0 to 255 seconds.
10. In the **Max. Interval for Password Digit, s** field (**11**), 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.
11. Check the **Failed Attempts Limit** box (**12**) 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** (**13**).
12. In the **Max Times of Card Swiping Failure** field (**13**), set the critical number of consecutive card swipes to generate an alarm if the Failed Attempts Limit box (**12**) is checked.
13. Check the **Tampering Detection** box (**14**) to enable the detection of device tampering attempts.
14. In the **Detect When Reader Is Offline for, s** field (**15**) field, specify the timeout interval to de-activate the reader on lost connection to the *Hikvision* controller.
15. Check the **Connected by RS485** box (**16**) if the reader is connected through the RS-485 interface.
16. Check the **Control Reader** box (**17**) if you want the reader to assign card codes in the *Access Manager* module.

> **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).

17. Click **Apply** button (**18**).

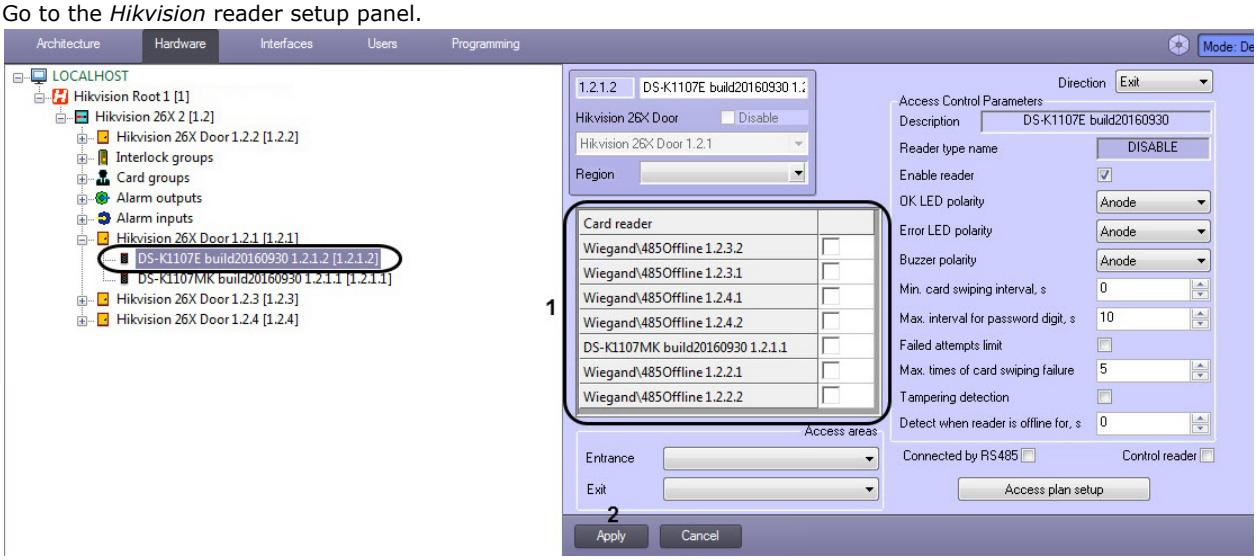
The *Hikvision* reader is now configured .

Configuting the Hikvision Anti-Passback

You can configure *Hikvision* anti pass-back via the *Hikvision* reader's setup panel (see Configuring a Hikvision reader). As an example of the *Hikvision* anti pass-back configuration, let's consider a *Hikvision* reader connected to a *Hikvision 26X* controller.

To configure the *Hikvision* anti pass-back, do the following:

1. Go to the *Hikvision* reader setup panel.



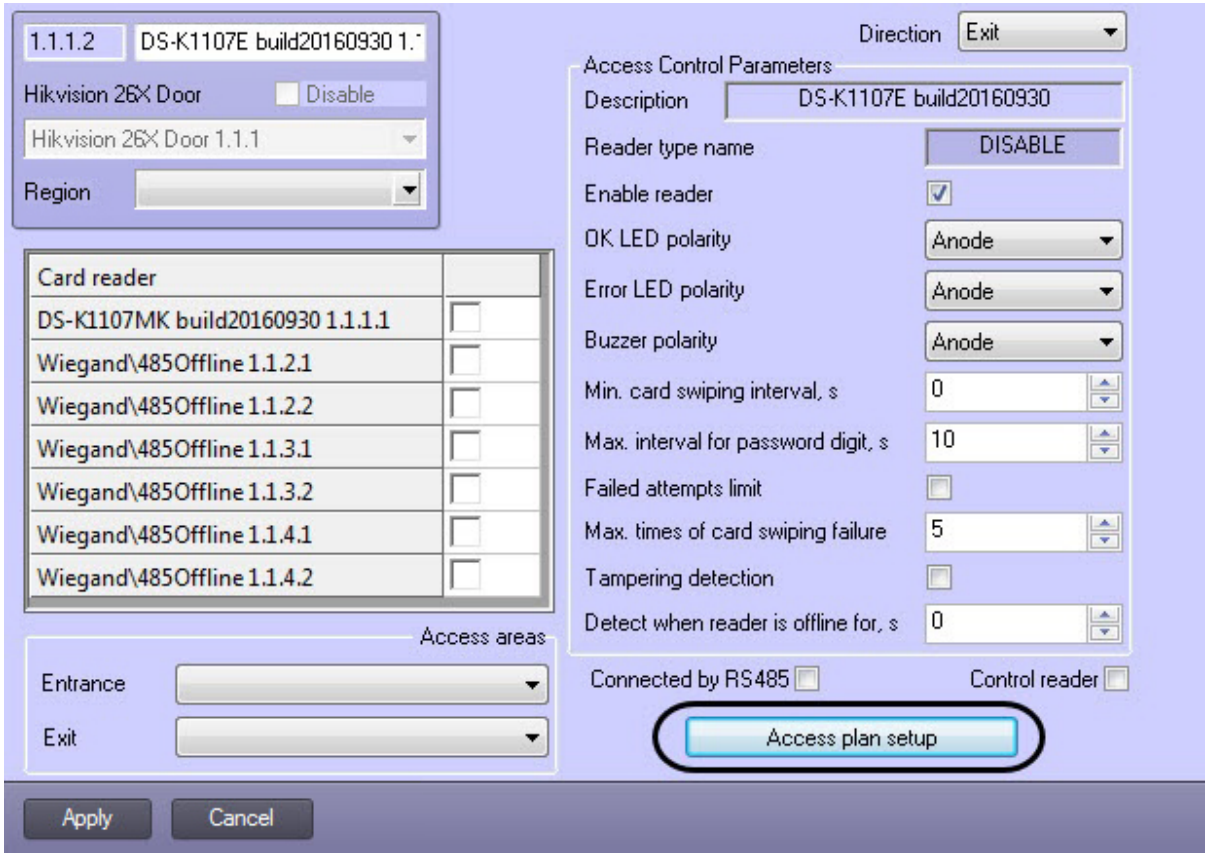
2. In the **Card reader** pane (**1**), check the boxes for the readers where the anti pass-back monitoring is required.
3. Click the **Apply** (**2**) button to save your settings.

The *Hikvision* Anti-Passback is now configured.

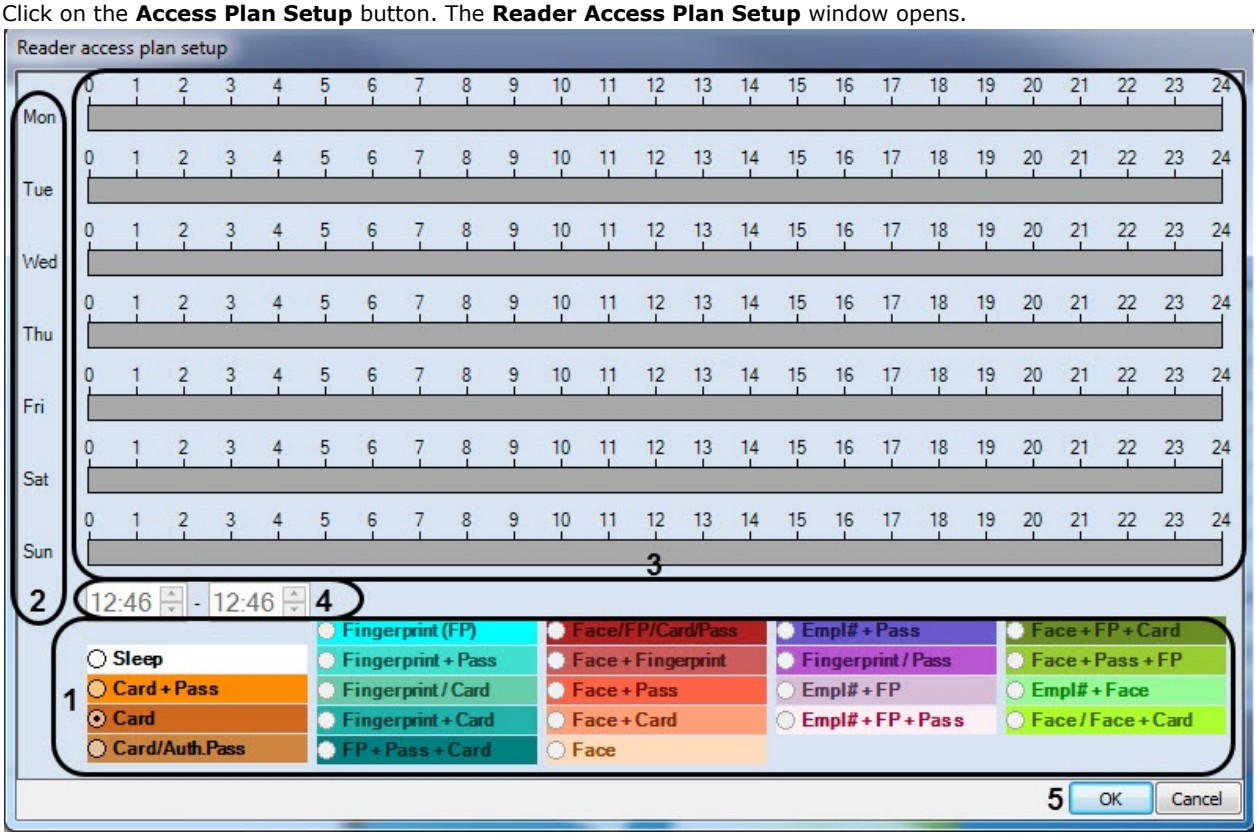
Setting up an access schedule

To set up an access schedule for a *Hikvision* reader, do the following:

1. Go to the settings panel of the **Hikvision 26X** Reader or **Hikvision 28X** Reader.



2. Click on the **Access Plan Setup** button. The **Reader Access Plan Setup** window opens.



3. Set the schedule in the **Reader Access Plan** window:
    1. Set your required access schedule in the corresponding pane (**1**).

> **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.

2. In the week day's column (**2**), use your mouse to set the required time slot (**3**).
3. You can edit the time values for each slot (4): starting time in the left field and ending time on the right.
4. Repeat steps 3a — 3c as necessary.

4. Click the OK (**5**) button to save your settings.

The access schedule for the *Hikvision* reader is now configured.

Setting up the Hikvision multicard configuration

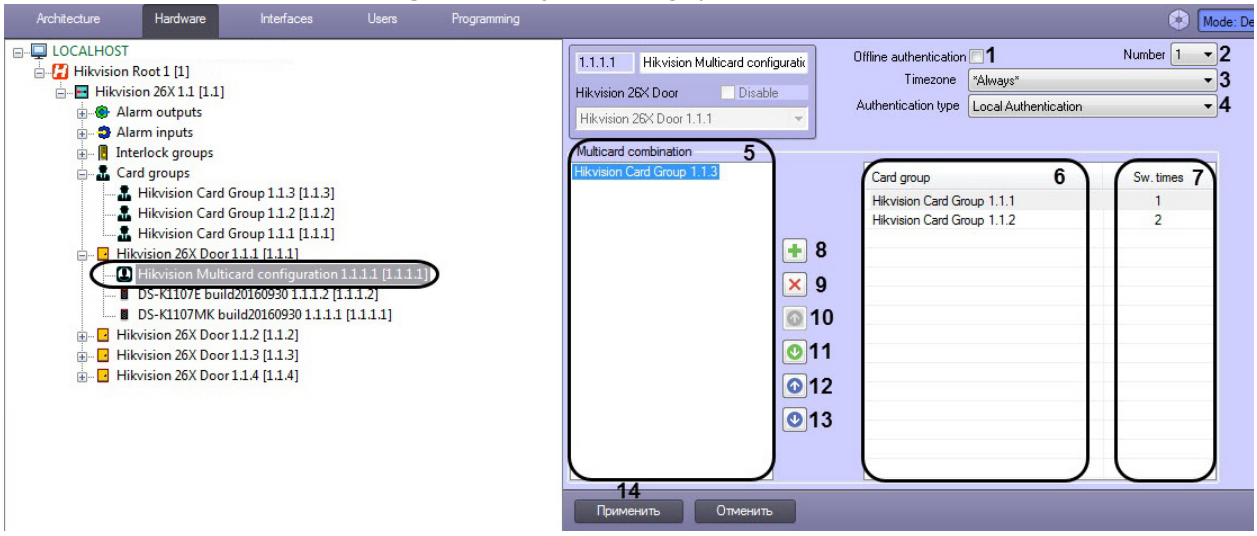
Note.

Set up *Hikvision* card groups before setting up the multicard configuration (see Configuring Hikvision card groups).

You can configure multiple *Hikvision* cards via the **Hikvision Multicard configuration** object's configuration panel; you can create this object on the basis of the **Hikvision 26X Door** object, or it can be created automatically after reading the configuration from the corresponding controller (see Network settings of the Hikvision controller and Configuring the Hikvision controller).

To set up a *Hikvision* multiple card configuration, do the following:

1. Go to the **Hikvision Multicard Configuration** object's 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:
    1. **Local authentication** is performed by regular user IDs (cards). You can link up to 8 card groups with this authentication type.
    2. **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.
    3. **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 Configuration** (**5**) pane and press the button  (**8**).
7. To remove a group from the **Card Group** column (**6**), select it and click the button  (**9**).
8. Use the  (**10**) and  (**11**) buttons to move a card group within the **Card Group** column (**6**).
9. In the **Sw. Times** column(**7**), you can use the  (**12**) and  (**13**) 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).

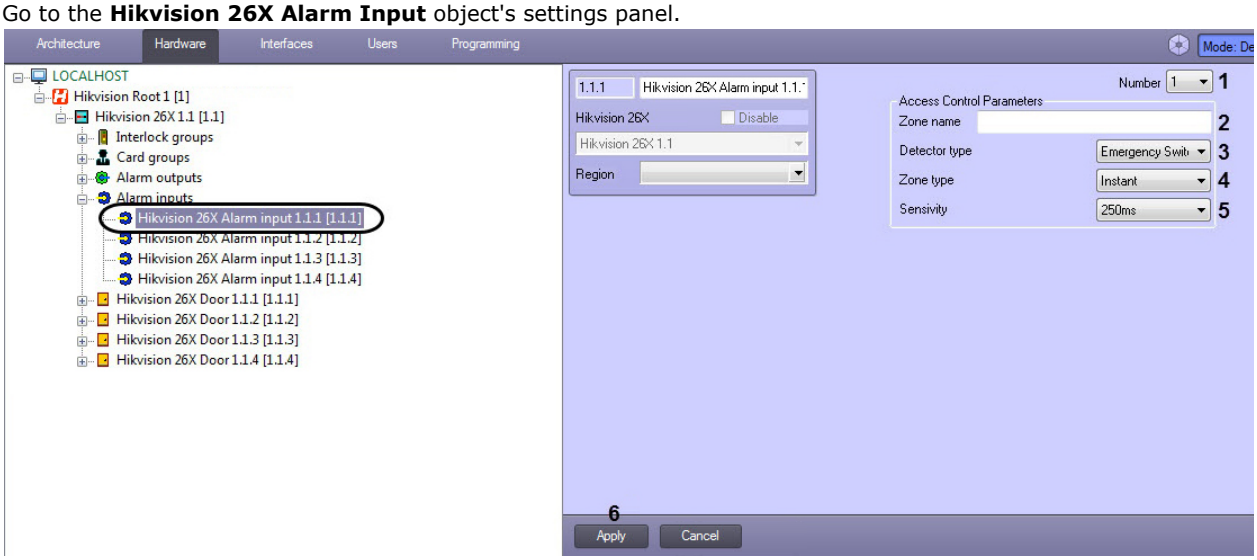
Hikvision multi-card configuration is now complete.

Configuring the Hikvision alarm input

You can configure a *Hikvision* alarm input via the settings panel of the **Hikvision 26X Alarm Input** object, which is created automatically on the basis of **Hikvision 26X** object after reading the configuration from the corresponding controller (see Network settings of the Hikvision controller and Configuring the Hikvision 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** (**2**) field, 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 **Apply** button (**6**).

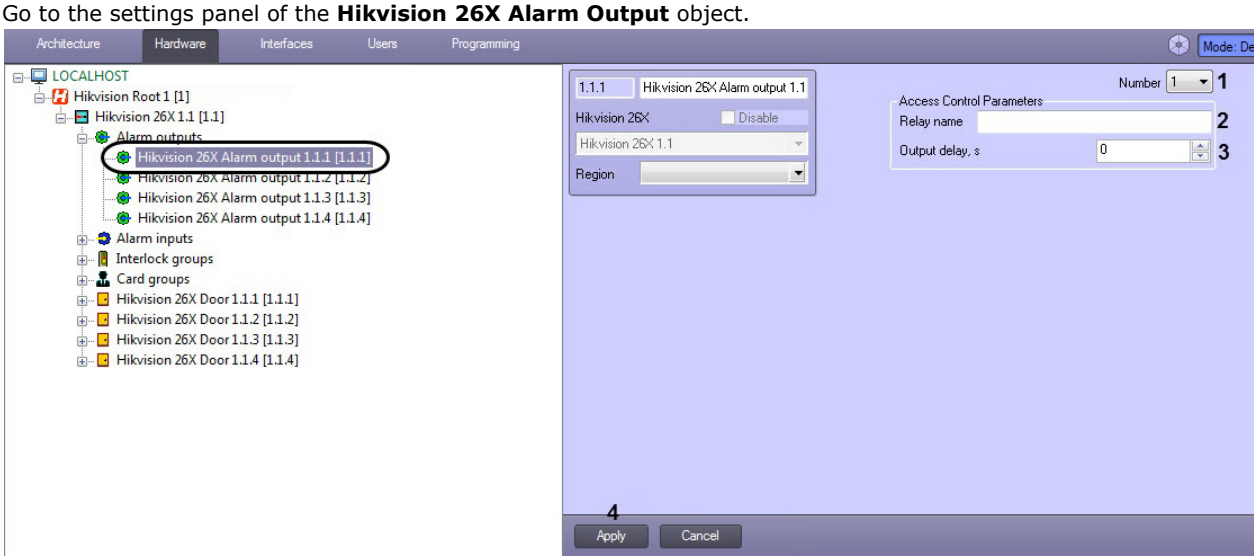
The *Hikvision* alarm input is now configured.

Configuring the Hikvision alarm output

You can configure a *Hikvision* alarm output via the settings panel of the *Hikvision* alarm output object, which is automatically created on the basis of **Hikvision 26X** or **Hikvision 28X** object after reading the configuration from the corresponding controller (see Network settings of the Hikvision controller and Configuring the Hikvision controller). As an example of *Hikvision* alarm output configuration, let's consider an alarm output created on the basis of the **Hikvision 26X** object.

You can configure the *Hikvision* alarm output as follows:

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* c ontroller. You can not change this value.
3. In the **Relay Name** (**2**) field, 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**).

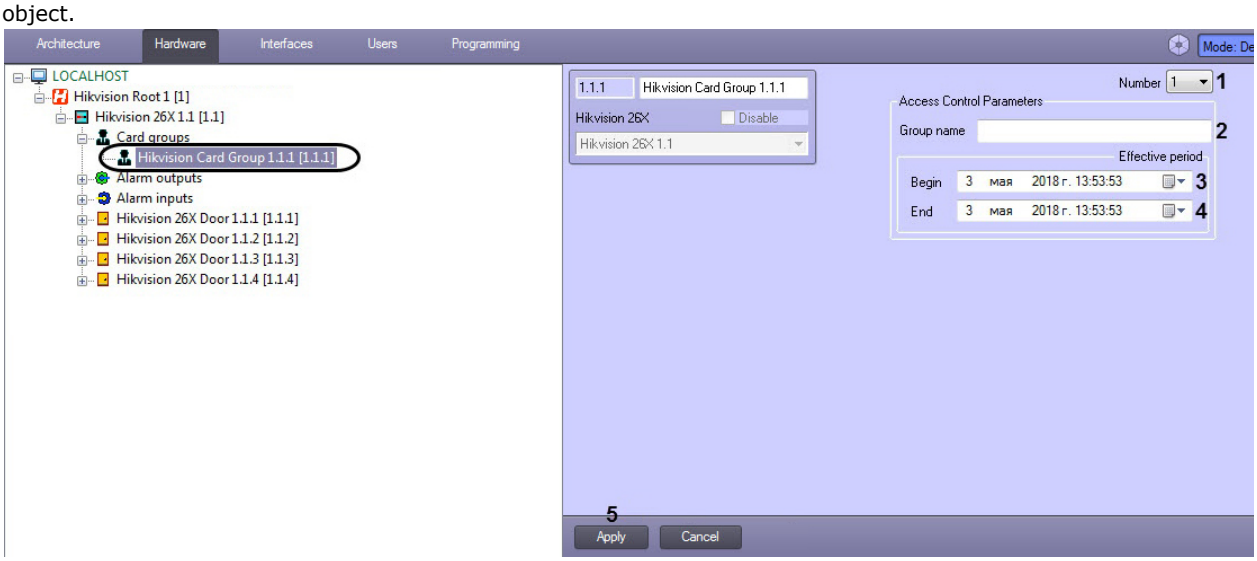
The *Hikvision* alarm output is now configured.

Configuring Hikvision card groups

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

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

1. Go to the settings panel of the **Hikvision Card Group** object , which is created on the basis of the **Hikvision 26X** 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.

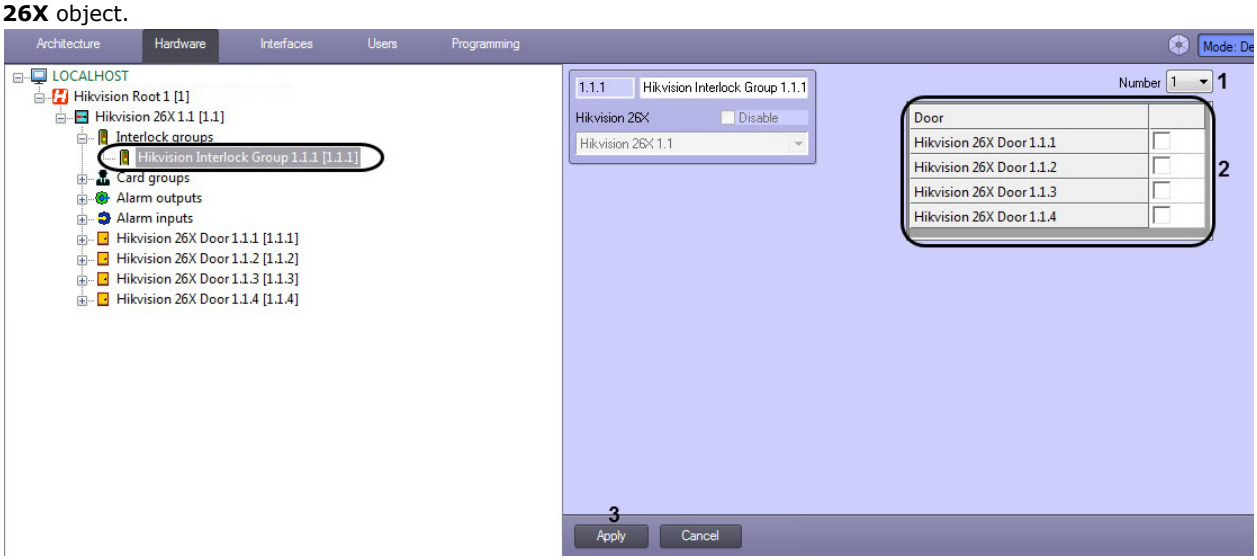
6. Click the **Apply** button (**5**) to save your settings.

The *Hikvision* card groups are now configured.

Setting up Hikvision interlock groups

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

1. Go to the settings panel of the **Hikvision Interlock Group object** , which is created on the basis of the **Hikvision 26X** 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** pane (**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.

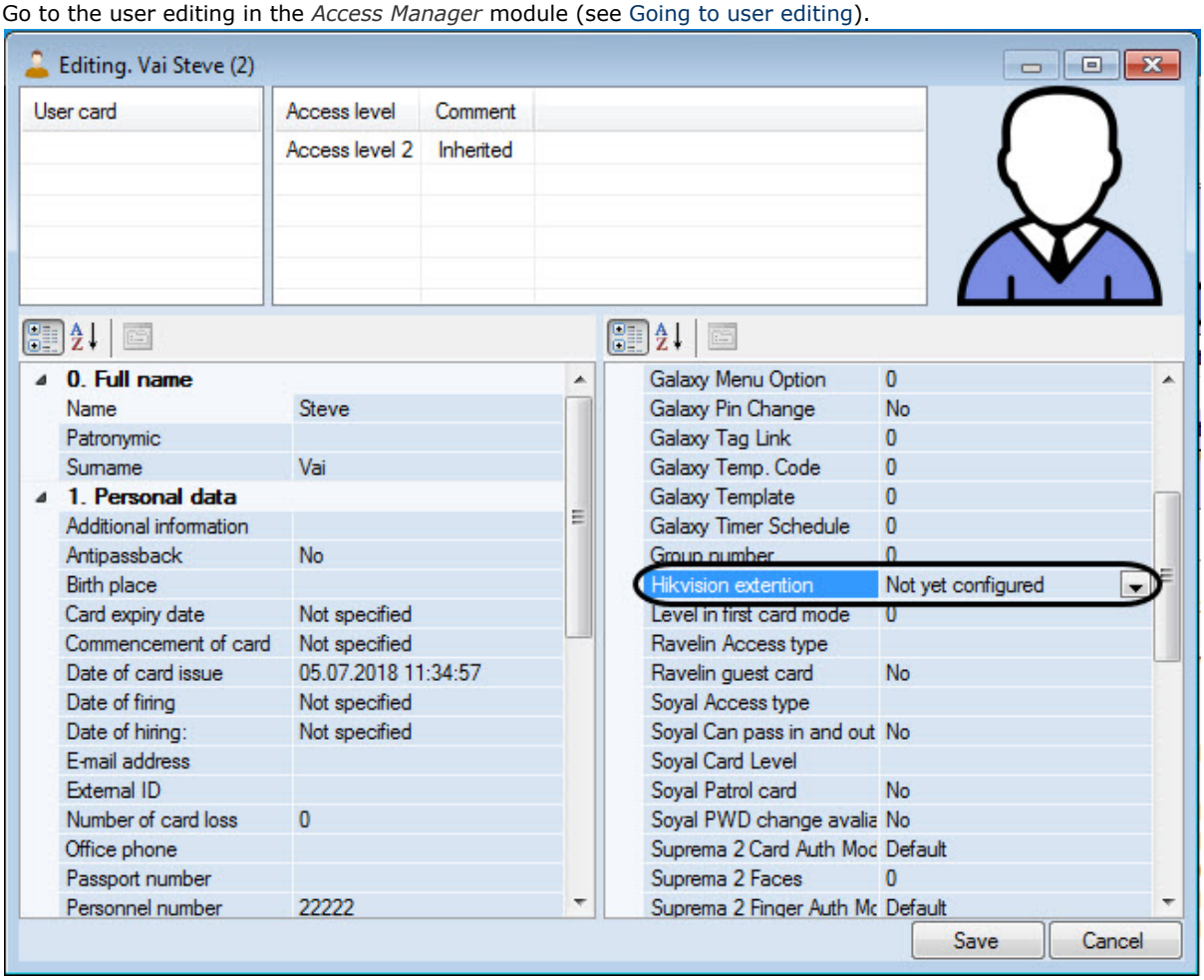
4. Click the **Apply** button (**3**) to save your settings.

The *Hikvision* interlock group is now configured.

Configuring Hikvision user cards

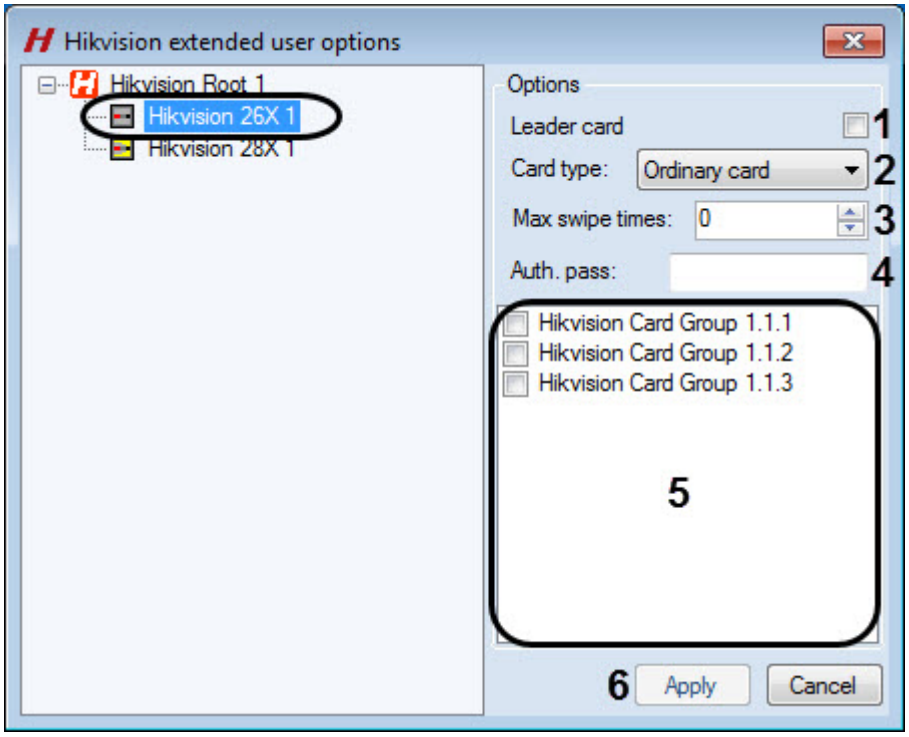
To configure *Hikvision* user cards, do the following:

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 desired controller from the object tree in the **Hikvision Extended User Options** window.
4. Check the **First Card** box (**1**) if you need 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 (**2**), 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 map is intended for visitors. You can set the maximum number of swipes for this card in the **Max Swipe Time**s field (see step 6).

6. Set a limit for a number of **Visitor card** swipes in the **Max Swipe Times** field (**3**).

> **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's password in the **Auth. Pass** field (**4**). The password consists of 4 to 8 digits.
8. Check the boxes for the required card groups in the (**5**) field.
9. Click the **Apply** button (**6**) to save the changes.

The *Hikvision* user cards are now configured.

Hikvision integration module operation

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 software operations manual

For detailed description of using these interface objects, please refer to the Intellect PSIM software operations manual.

Managing the Hikvision controller

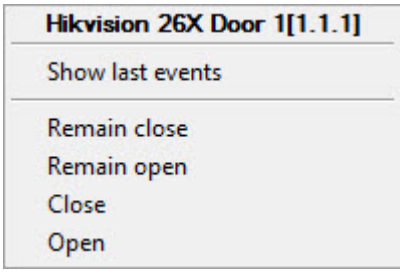
> **Note.**
>
> The *Hikvision* controller is not controlled from the **Map**.

Controller states can be as follows:

	Battery low
	Connection lost
	Mains powered
	Battery powered

Managing a Hikvision door

> **Note.**
>
> Managing a *Hikvision* door is described for the **Hikvision 26X** controller's door. Managing the door of the **HikVisi on 28X** controller 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:

	Normal
	Permanently closed
	Permanently open
	Standby
	Locking disabled
	Locking failure
	Always locked
	Magnetic sensor disabled
	Magnetic sensor failure
	Magnetic sensor shorted

Managing Hikvision reader

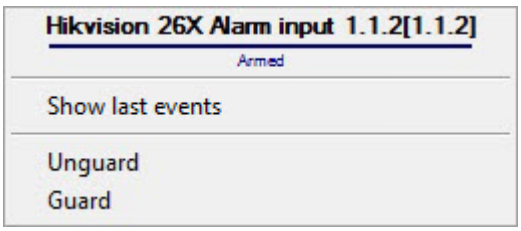
> **Note.**
>
> The *Hikvision* reader is not controlled from the **Map**.

Reader states can be as follows:

	Mode: map
	Mode: other
	Offline
	Tampering

Managing Hikvision alarm input

The *Hikvision* alarm input is managed through the **Map** 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:

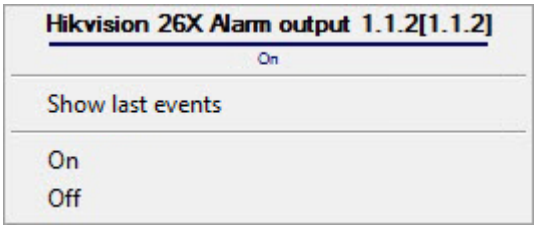
	Armed

	
	Disarmed
	Alarm

Managing Hikvision alarm output

> **Note.**
>
> Managing a *Hikvision* alarm output is described for the **Hikvision 26X** controller's alarm output. Managing the alarm output of the **HikVision 28X** controller is performed in the same way.

The *Hikvision* alarm output is managed through the **Map** 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:

	Active
	Inactive