HIKVISION

EUROPEAN TECHNICAL CENTER

FIRMWARE RELEASE NOTE

DS-K260X series Access Controller V2.0.2_Build171107 Release Notes (2017-12-02)

Device Model: DS-K2601/DS-K2602/ DS-K2604	Firmware Version:	V2.0.2_Build171107
	SDK Version:	V5.3.1.35_build20170911
	Client version	V2.6.5.6 build20171016

Reason of Upgrade

Added or modified functions, enhance products quality and meet customers' requirements.

Note

IMPORTANT! When upgrading DS-K260X series access controller from V1.1.1 to V2.0.2, the controller buzzer will keep sounding for approximately 5 minutes after restart, please do not power off and let it finish the upgrade process. If you reboot the device while buzzing, please do initialization via the onboard jumper.

Main Features

i. Mifare M1 Card Encryption

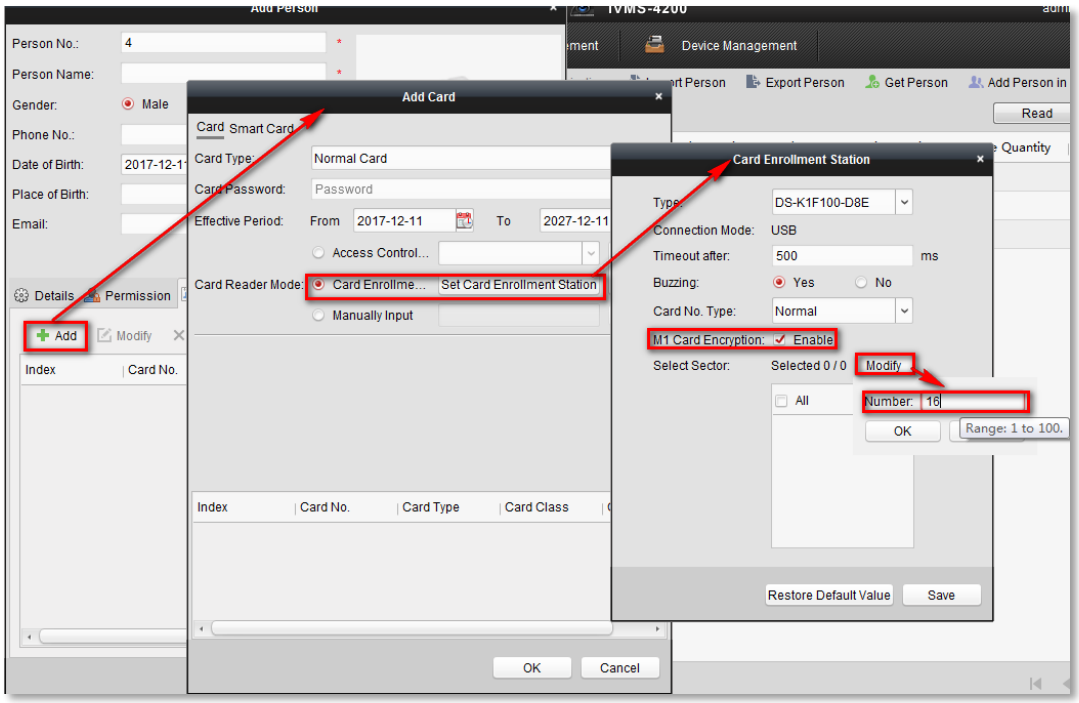
A private encryption method that provides higher protection against card coping by writing specific information on its sectors:

1. Card readers and card enrollment station should be in the following version:

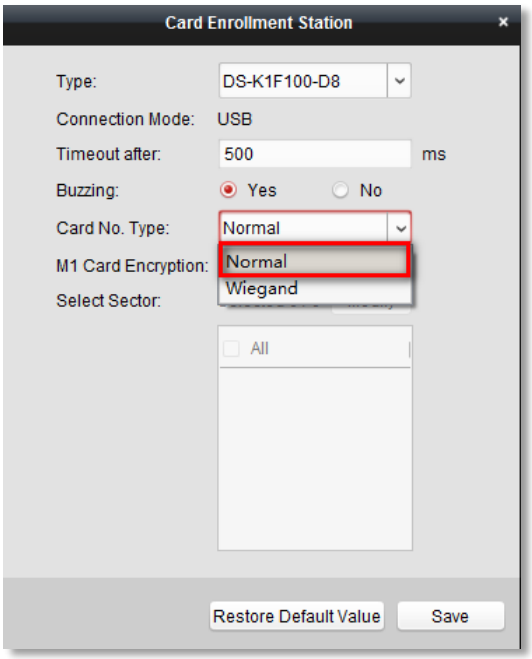
Device	Model	Firmware
Card Reader	DS-K1101/2/3/4/7/8 series	V2.0.1_171107
Card Enrollment Station	DS-K1F100-D8E/DS-K1F180-D8E	V2.1.0_171017

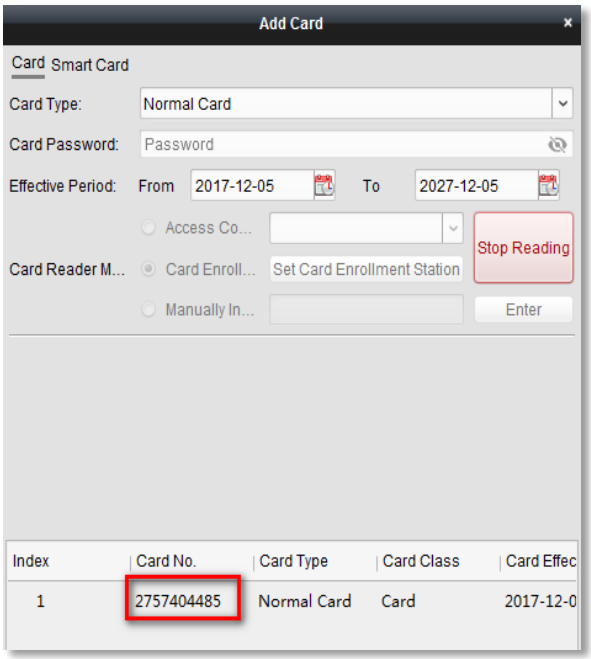
Note: the required firmware can be found on EU download portal following this link

M1 Card Encryption needs to be enabled in Add person->Add Card->Set Card Enrolment Station. The supported Hikvision M1 card, model IC S50 is made up of 16 sectors (Sector 0 – Sector 15), so the ***Select Sector*** should be no more than 16

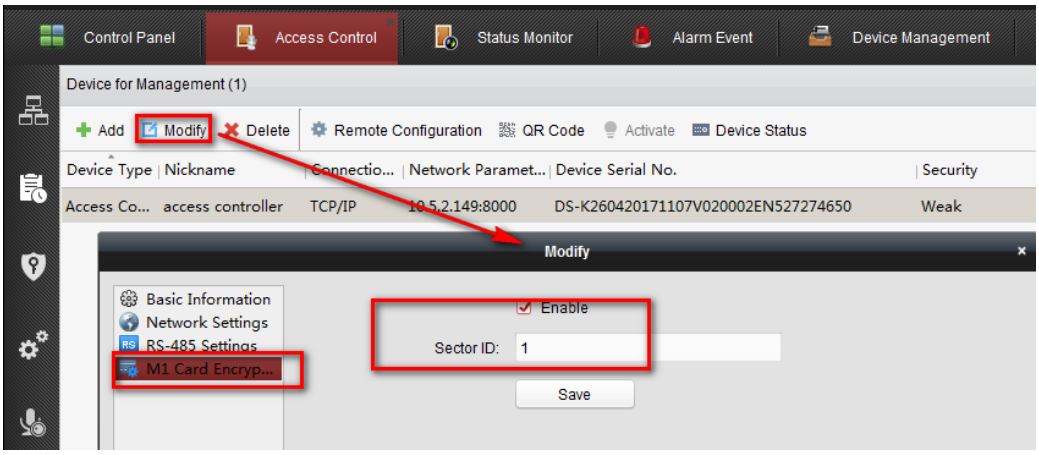


2. For ***Card No. Type***, options are ***Normal*** and ***Wiegand***. In M1 Card Encryption mode only ***Normal*** type should be used which means that 10-digit card No. is displayed in iVMS-4200 client. In this mode the card readers should be connected via RS- 485;





3. Enable ***M1 Card Encryption*** and set ***Sector ID*** on the access controller in device management;



Notice:

- For higher security, customers should enable encryption on all card sectors except the one that is used for ***Based on Card Cross-Controller Anti-Pass Back*** function (See below);
- ***M1 Card Encryption*** is only supported for readers with RS485 wiring;

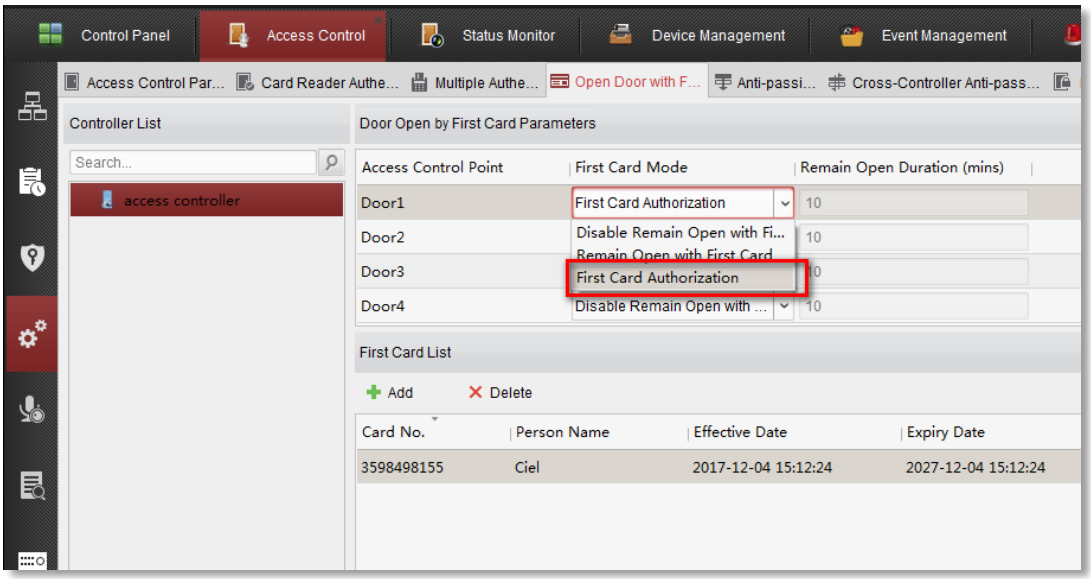
ii. Open Door with First Card

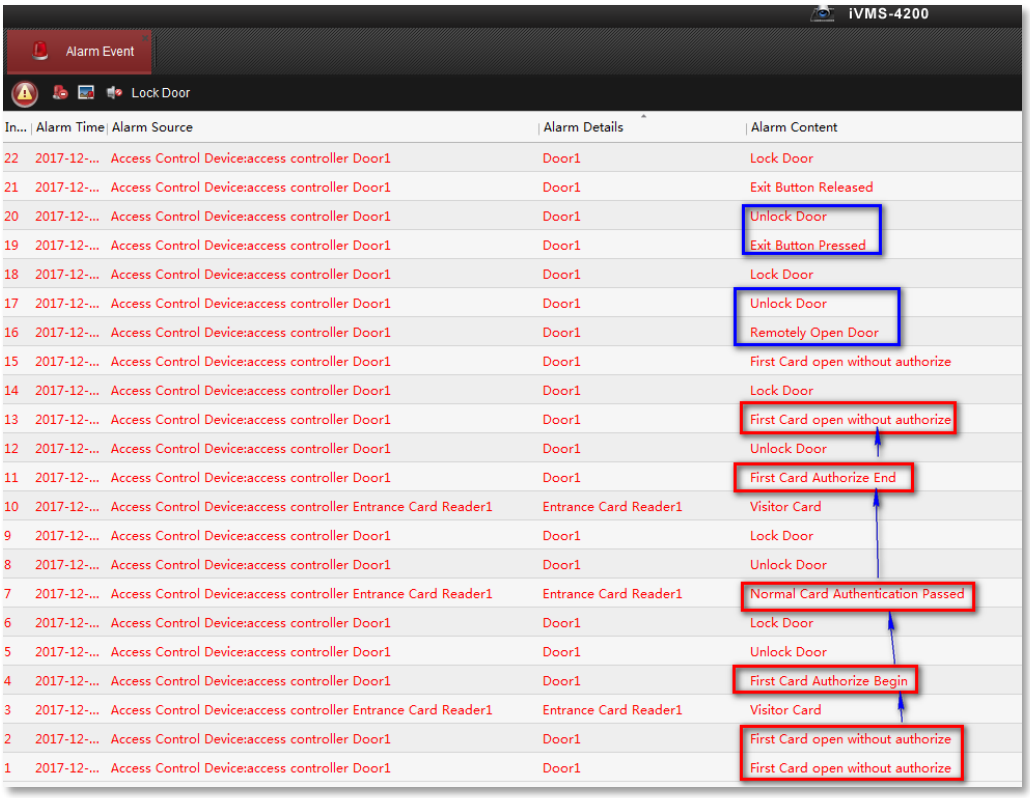
(1) **First Card Authorization** – if enabled the door will allow access to valid users only after a card/user added to ***First Cards List*** has authorized on the reader.

To enable this function for an access control point select ***First Card*** **Authorization** option from the drop down menu in the ***First Card Mode***.

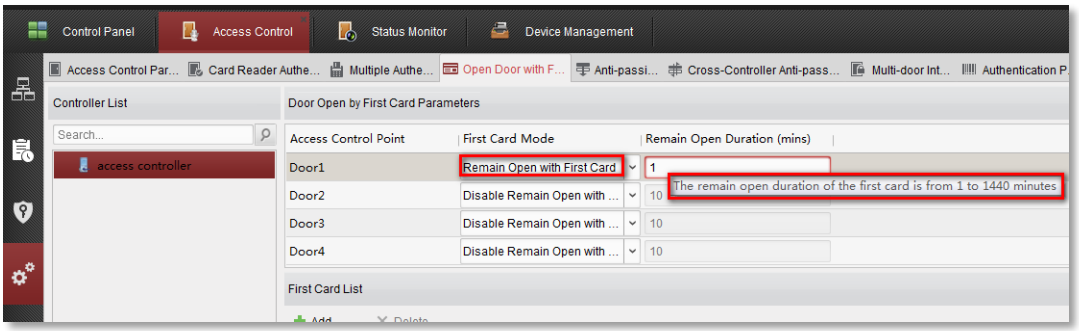
Swiping the First Card will enter **First Card Authentication** mode and all valid users will be able to access the door, swiping it again will exit **First Card Authentication** mode and only ***Super Card/Duress Card*** and ***Remote Open*** and pressing ***Exit Button*** can open the door.

Notice: The first card authorization is effective only on the current day. The authorization will expire after 24:00 on the current day.





(2) Remain Open with First Card – the door will remain open for the configured time duration after a card/user in **First Card List** is swiped.

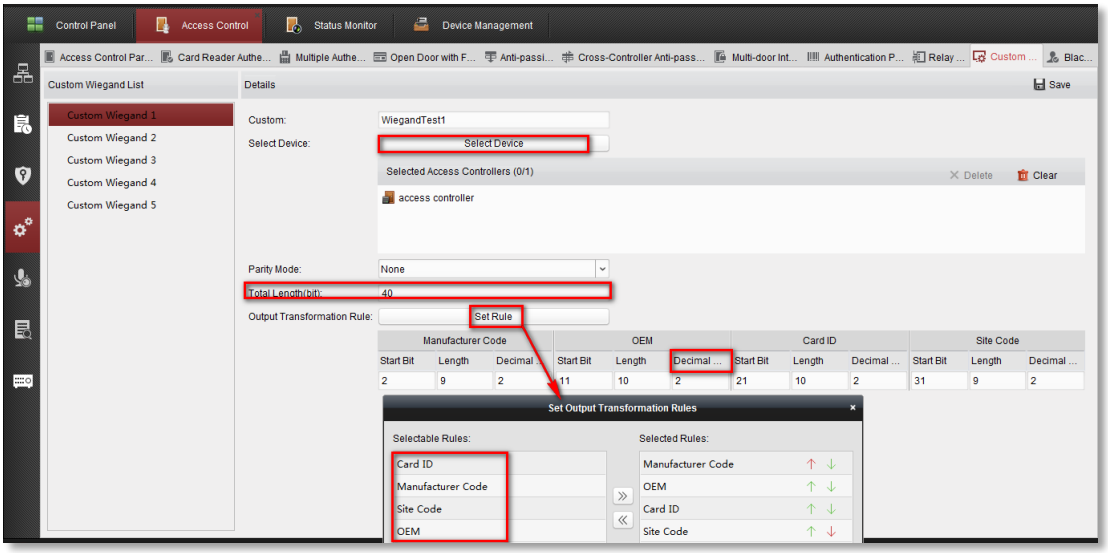


(3) Disable Remaining Open with First Card: Disable the function.

iii. Custom Wiegand:

Up to 5 Custom Wiegand protocols can be created for 3rd party readers compatibility;

1. Parameters:



(1) ***Total Length(bit)***: the length of binary data which the card reader send to the controller;

(2) **Output Transformation Rule**: Card No. consists of several different parts, such as ***Manufacturer Code***, ***OEM***, ***Site Code*** and ***Card ID***. Each part is converted independently into decimal number, and then combined together in sequence to get the card No.

(3) ***Decimal Digit***:

Example: the length of ***Card ID*** is 10 and we set ***Decimal Digit*** 2:

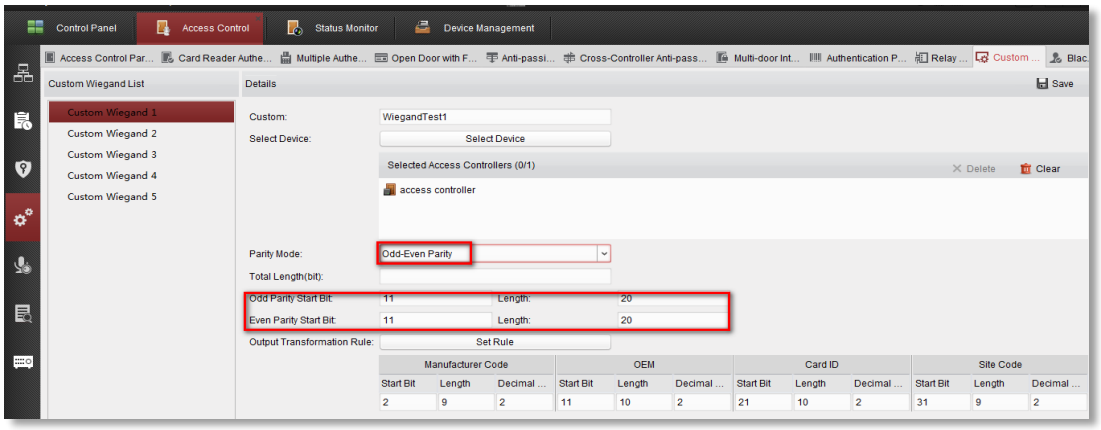
If the Card ID is 1111111111 in binary, which means it is 1023 in decimal, so the effective data is 23;

If the Card ID is 0000011111 in binary, which means it is 31 in decimal, so the effective data is 31;

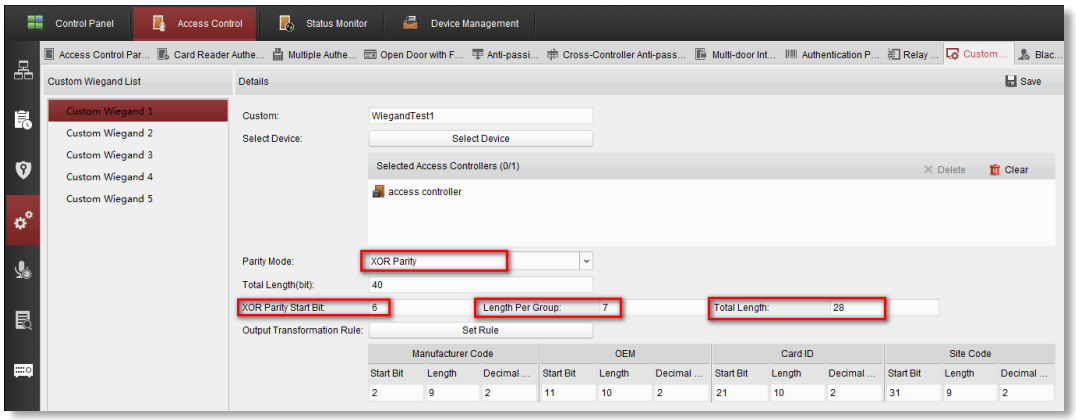
If the Card ID is 0000000001 in binary, which means it is 1in decimal, so the effective data is 01;

2. Parity Mode: Odd-Even Parity, XOR Parity and None

(1) Odd-Even Parity:



(2) XOR Parity



Length Per Group: the length of XOR cipher;

Total Length: the length of validated data, which does not include the length of XOR parity;

Notice:

Total Length (bit) = [(XOR Parity Start Bit) - 1] + (Total Length) + (non- validated data) + (length of XOR cipher);

Total Length = (Integer A) * (Length per Group), the length of validated data;

(Total Length (bit) - (XOR Parity Start Bit) + 1 - (Total Length) ≥ (Length Per Group).

Notice: not supported Custom Wiegand 26/34

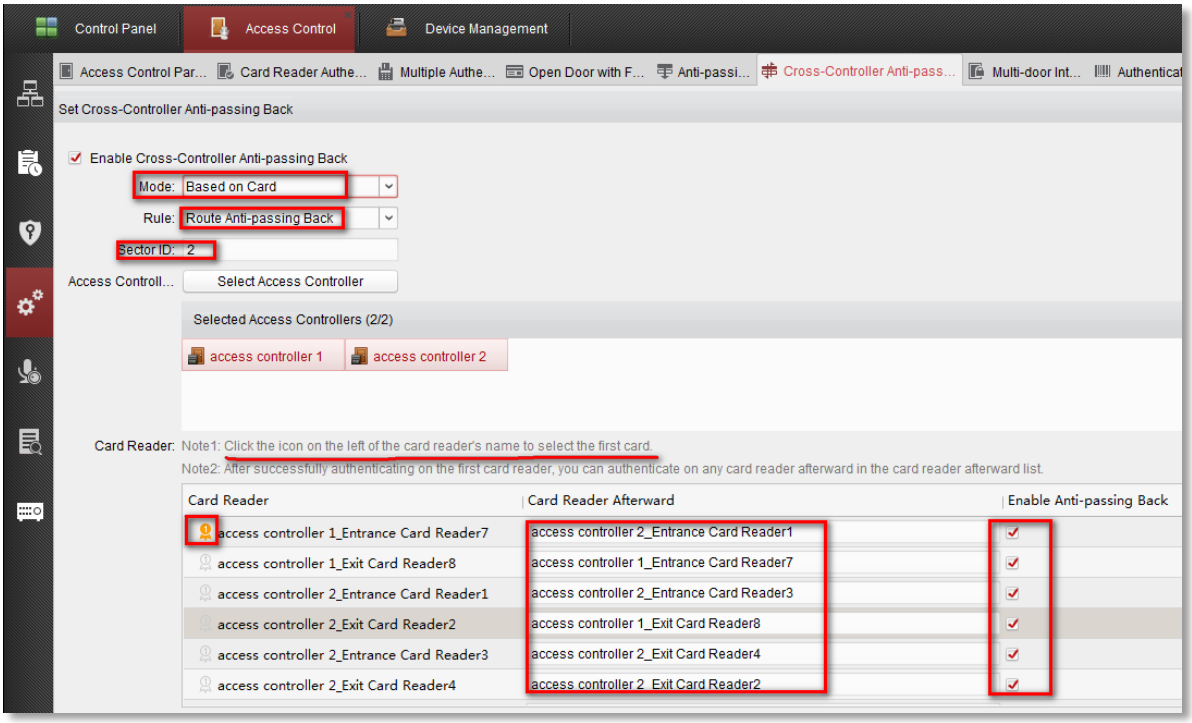
iv. Cross-Controller Anti-Pass Back

Innovative function that allows the controllers to communicate between each other on the LAN in ***Based on Network*** mode or via the logs in the user cards in ***Based on Card*** mode in order to detect anti-pass back violation without relying on unstable PC server or expensive master controller (control panel).

Both ***Based on Card*** and ***Based on Network*** modes supports ***Route Anti-passing Back*** and ***Entrance/Exit Anti-passing Back***;

1. ***Based on Card*** Cross-Controller Anti-passing Back – APB violation is judged according to the logs written on the card by the last controller. Only M1 Mifare cards are supported.

   (1) ***Route Anti-passing Back*** – users have to pass through a predefined route of doors:



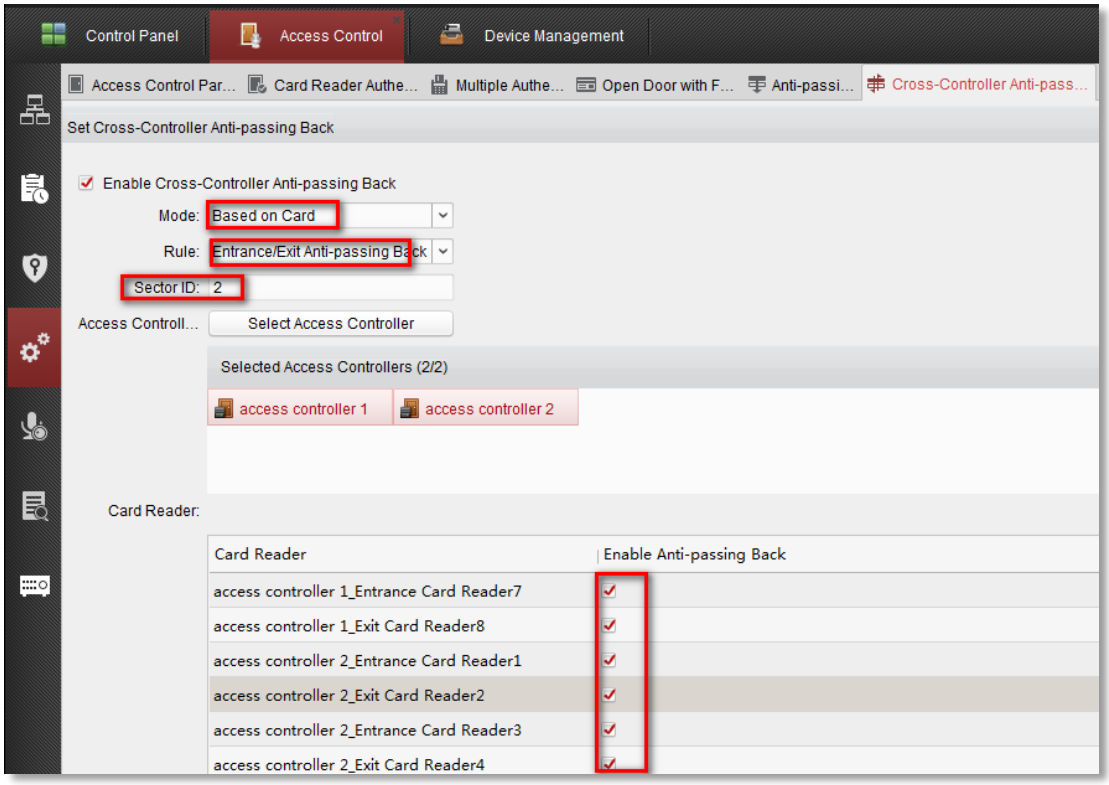
Notice：For ***Based on Card*** Cross-Controller Anti-passing Back:

a) Supported for readers connected via RS-485;

b) Please hold the card for 1 second when swiping;

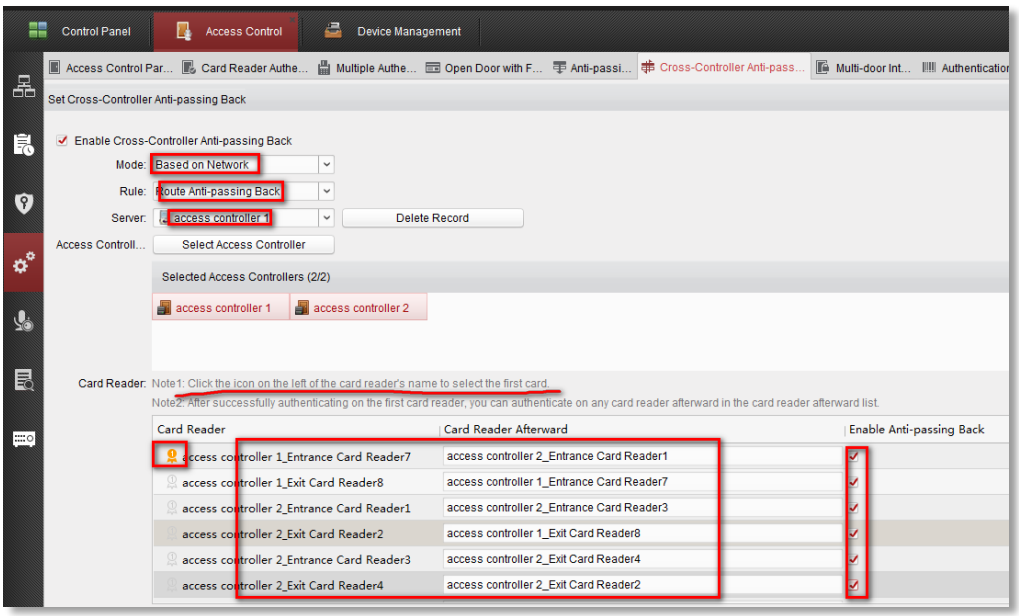
c) On an access control point with a reader included in Anti-passing Back, ***Multiple Authentication function*** cannot be enabled;

(2) ***Entrance/Exit Anti-passing Back*** – users can enter and exit every door included in the APB without any predefined route:



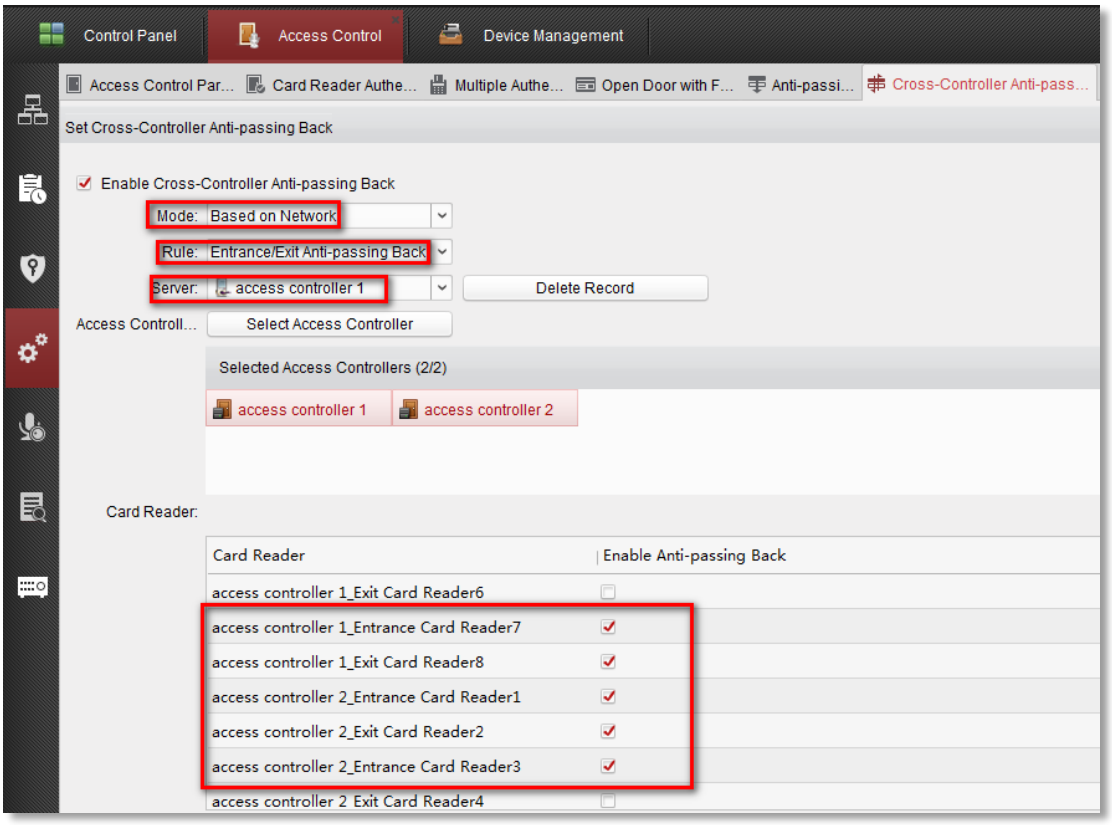
2. ***Based on Network*** Cross-Controller Anti-passing Back – a controller is selected as a server that judge the APB violation and rest of the controller are connected to it. All types of cards and readers methods are supported.

(1) Route Anti-passing Back - users have to pass through a predefined route of doors:



The icon  means this card reader is the ***First Card Reader;***

(2) ***Entrance/Exit Anti-passing Back*** - users can enter and exit every door included in the APB without any predefined route:

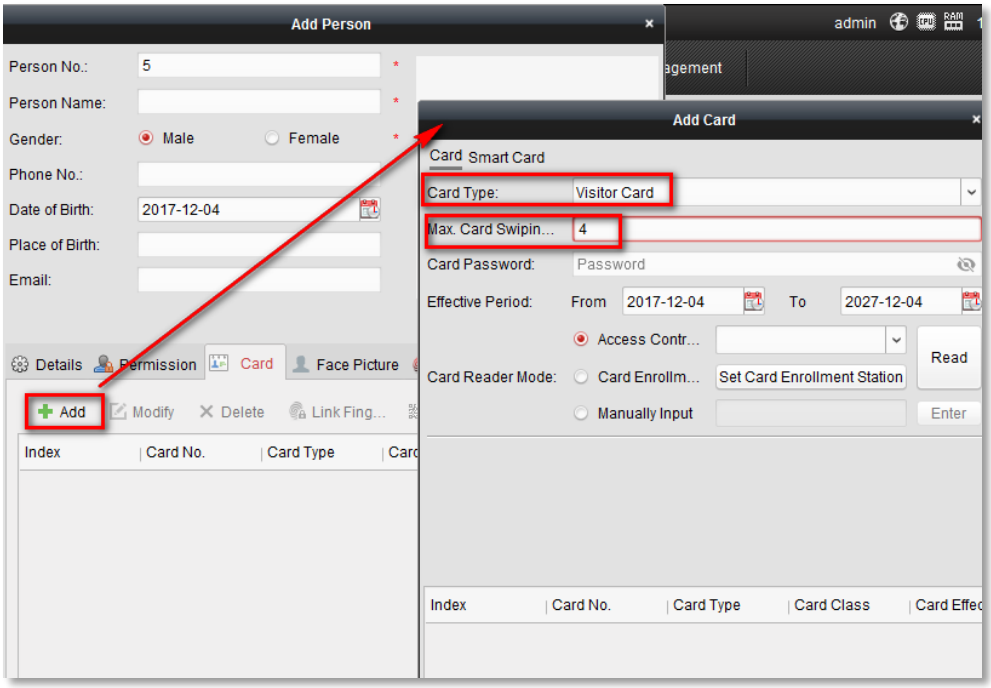


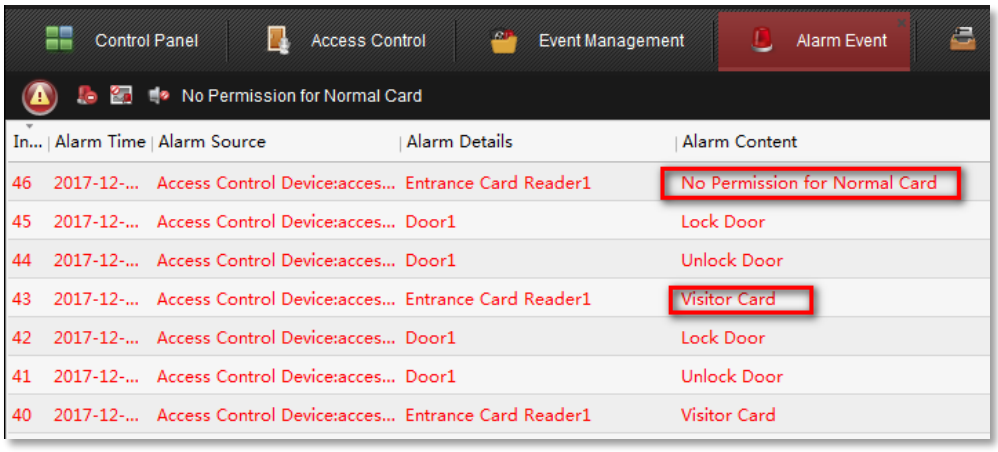
Notice:

1. Cross-Controller Anti-passing Back supports 64 DS-K260X series access controllers at most (baseline iVMS-4200 client can manage up to 16 devices and 64 access control points), and up to 128 card readers;
2. For ***Route Anti-passing Back***, the number of ***Card Reader Afterward*** should be less than 16;
3. For ***Based on Network*** Cross-Controller Anti-passing Back, the server can store 5000 anti-passing records.
4. ***Delete Record option*** is used to reset manually user/card APB status.

Modified Functions

i. DS-K260X series access controller can store up to 97,000 ***Normal Card***, 3,000 ***Visitor Card*** where the ***Max. Card Swiping Times*** can be limited in the range of 1 – 255 and 0 means swiping times are unlimited;



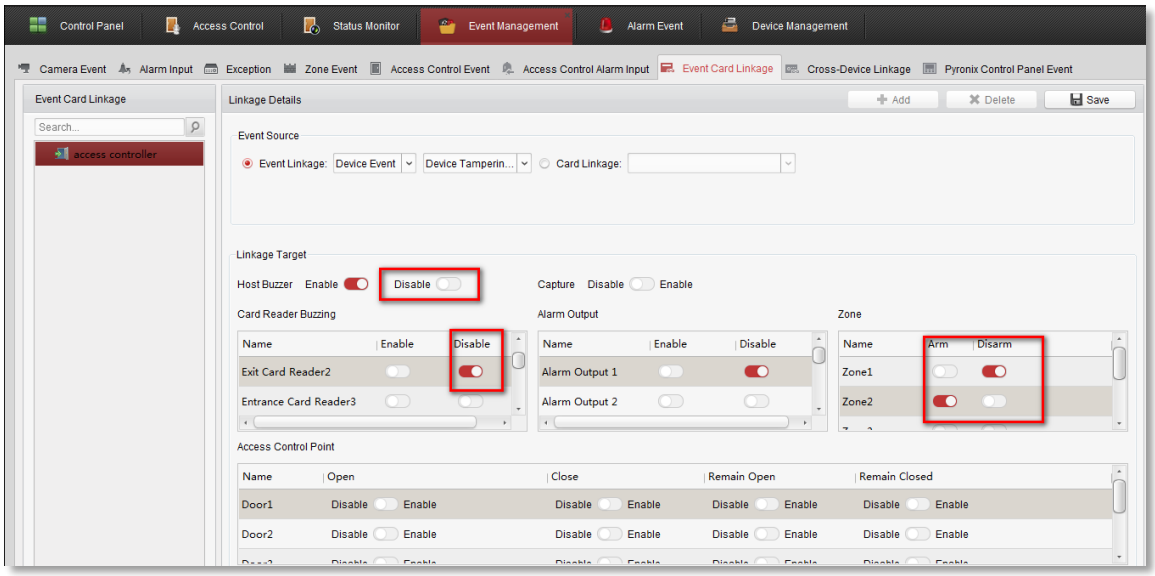


ii. Supports up to 500 ***Authentication Passwords*** that cannot be the repeated or the same as ***Super Password/Dismiss Code/Duress Code***;

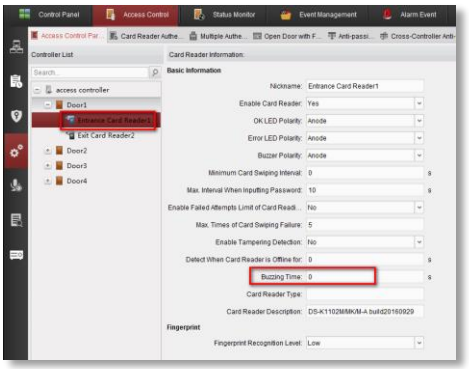
iii. For one access controller, ***Anti-passing Back*** and ***Multi-door Interlocking*** can exist at the same time;

iv. ***Multiple Authentication***: supported up to 20 Authentication Groups;

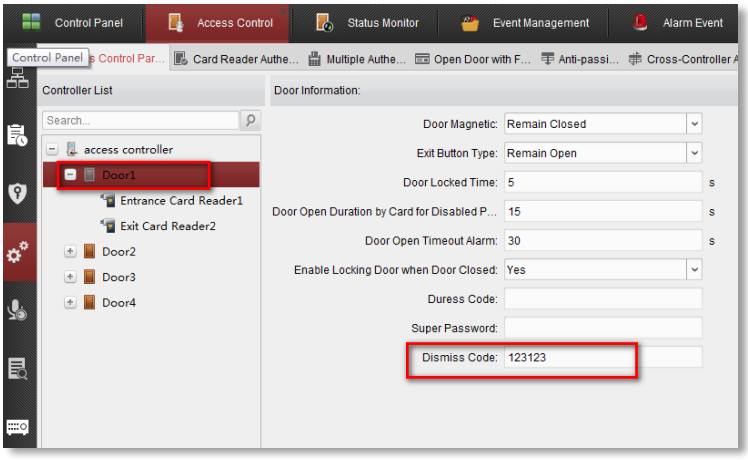
v. In ***Event Management*** -> ***Event Card Linkage*** interface is added ***Disable*** button that can disable Controller/Card Reader buzzing or disarm zones on event occurrence.



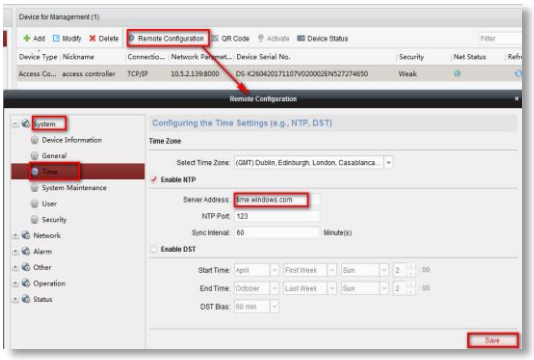
1. Host Buzzer time: 20S by default;
2. Card Reader Buzzing: Buzzing Time 0 – 5999 (0 means buzzing all the time);

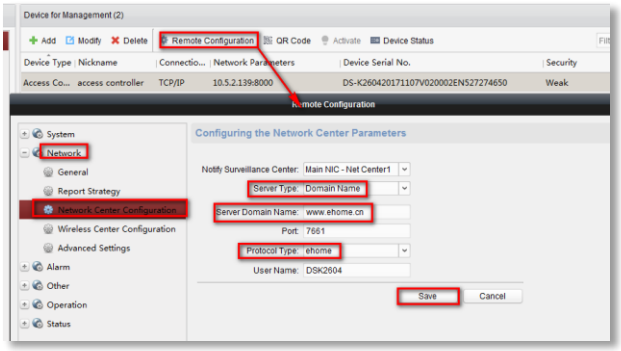


3. Dismiss Code: input dismiss code to cancel card reader buzzing or host buzzing alarm;

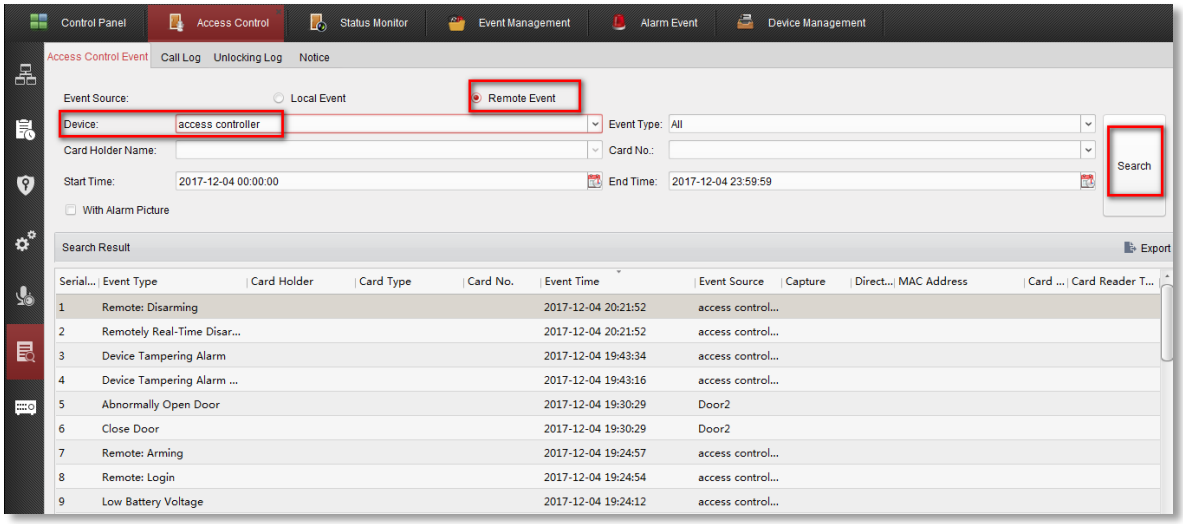


vi. Supports entering domain name (64 byte) for E-home and NTP;

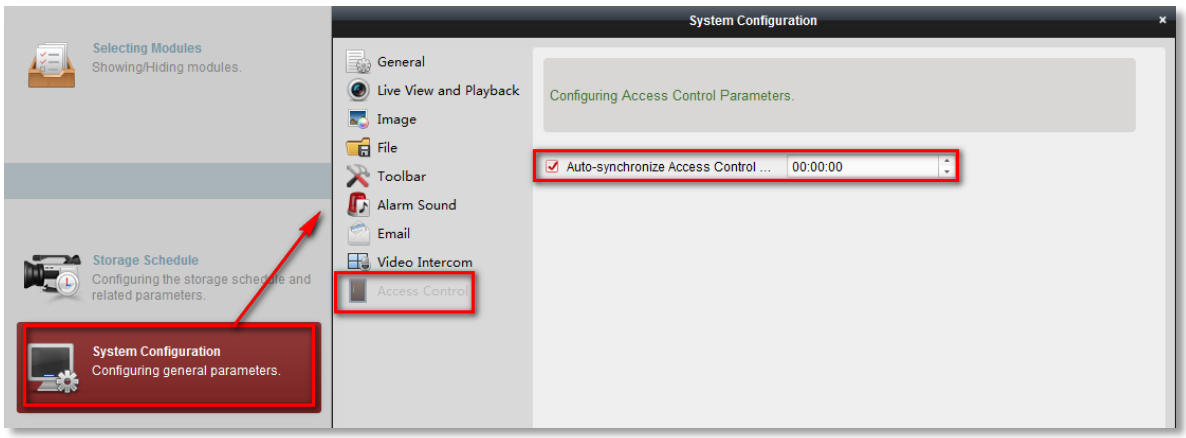




vii. Remote Event: supports getting access control records from the device event buffer

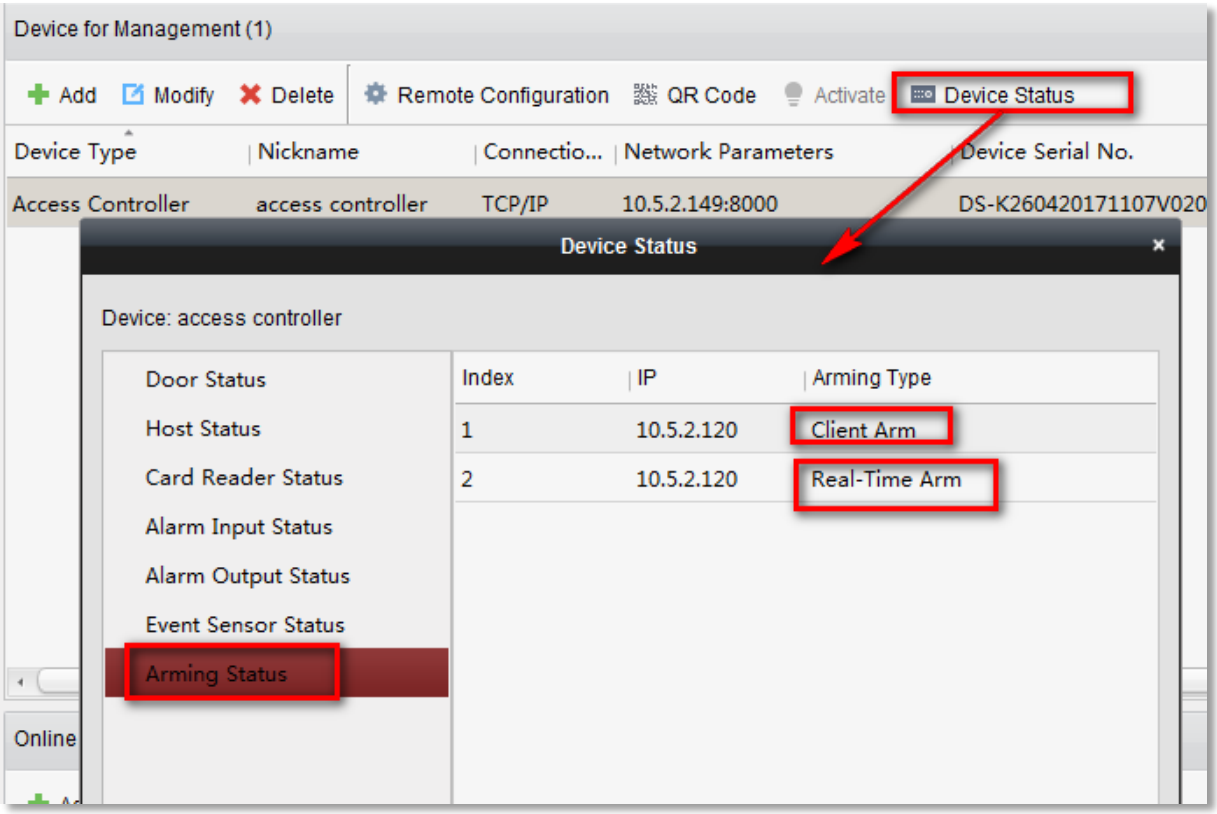


viii. Auto-synchronize Access Control Events: You can set the time so that the system will get the access control events which are not uploaded to the client from the access control device and save them to the client's database.

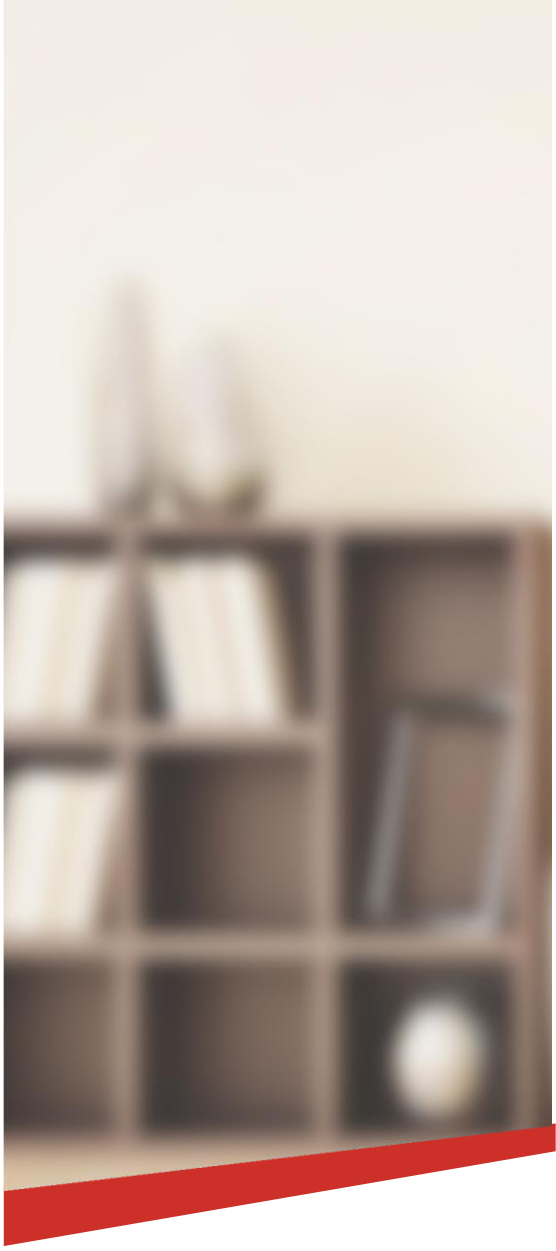


ix. DS-K260X series access controller supports DS-K1201 series fingerprint card reader;

x. Check device arming status on client;



xi. Support IP Conflict Detection Alarm: once in conflict, DS-K260X series access controller will beep like "Bi --- Bi --- Bi --- Bi-Bi " , three minutes again;



Customer Impact and Recommended Action

This new firmware upgrade is to improve product performance, and will take effect automatically after upgrading from previous versions. We'd like to inform you for the above changes. Also, we are sorry for any possible inconvenience of use-habit changes caused by this action.

For questions or concerns, please contact our local technical support team.

Note:

- Hikvision has all rights to alter, modify and cancel this notice.
- Hikvision doesn't give any guarantee for old models' stock.
- Hikvision is not liable for any typing or printing errors.
- For special model's change details, please contact our local technical support team.

Hikvision Digital Technology CO., Ltd.
No. 555 Qianmo Road, Binjiang District, Hangzhou
310052, China
Tel: +86-571-8807-5998
FAX: +86-571-8993-5635