



EUROPEAN TECHNICAL CENTER
FIRMWARE RELEASE NOTE

DS-K1T105/200/201 series Access Control Terminal

V2.0.0_Build180104 Release Notes (2018-03-30)

Device Model: DS- K1T105/200/201MF/EF(- C)	Firmware Version:	V2.0.0_Build180104
	SDK Version:	V5.3.1.35_build20170911
	Client version	V2.7.0.6 build20171212

Reason of Upgrade

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

Main Features

- i. **Change to Hikvision own developed fingerprint module (For DS-K1T201MF/EF(-C)):**
 1. Recognition speed and accuracy improved: 1:3000 < 1S & 1:5000 < 1.5S;
 2. Max. capacity of up to 5000 fingerprints;
- ii. **Support device activation locally:**



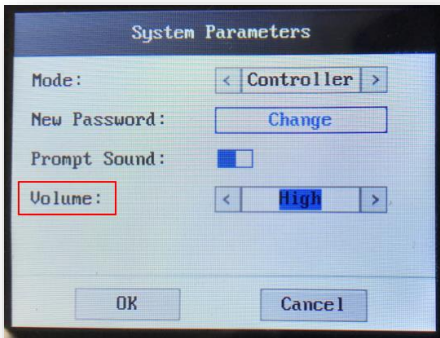
- iii. **Four new device status icons on main interface:**



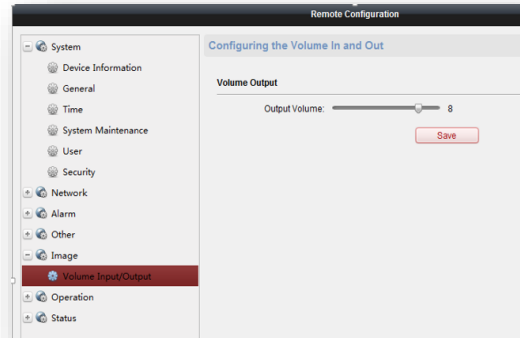
1. Network status: Connected or Abnormal (will show red '!');
2. Arming status: Armed or Disarmed (will show red '!');
3. Ehome status: connected or disconnected (will show red '!');
4. Wi-Fi signal status : excellent, good, normal, weak, no signal.

iv. Support adjusting Speaker Volume:

1. Local:

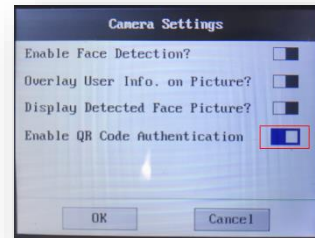
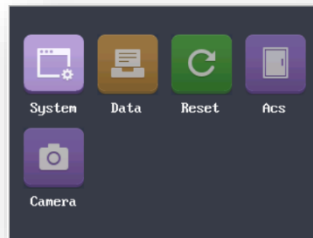
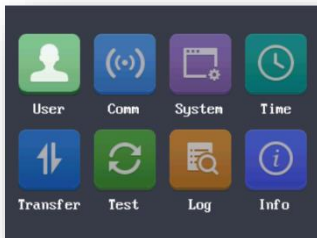


2. iVMS-4200 Client (click Remote Configuration):

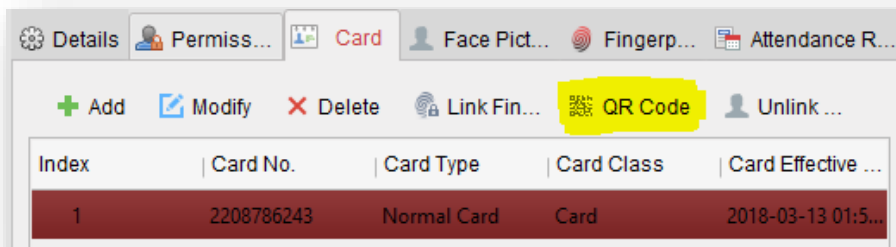


v. Support QR Code Authentication:

1. Enable this functionality as following:



2. Generate a QR code for a user card in iVMS access control module -> Person and Card tab



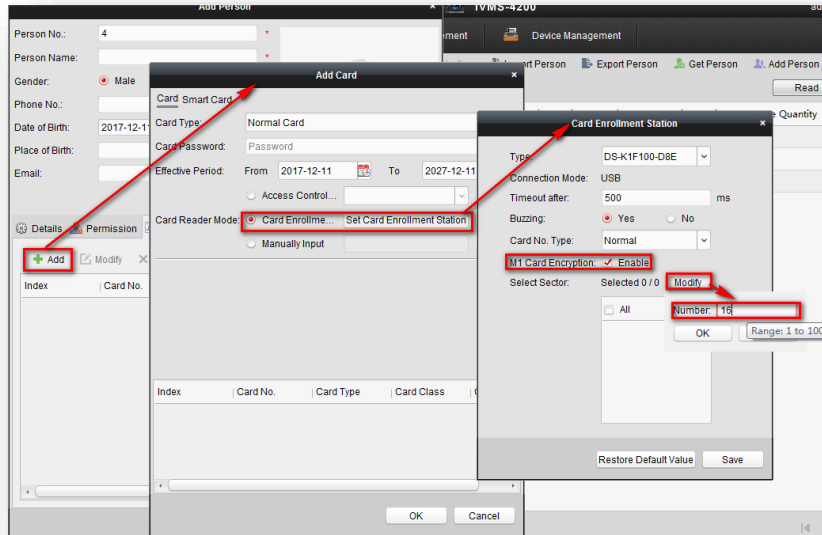
3. Press and hold 'F1' button on the terminal to enable camera and present the QR code.

vi. Mifare M1 Card Encryption – method for increasing Mifare card protection against copying

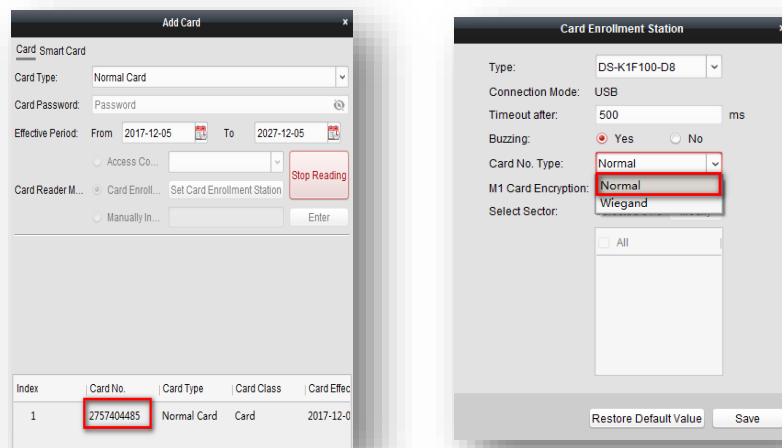
1. Card reader and card enrollment station should be in following firmware version:

Device	Model	Firmware
Card Reader (external)	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

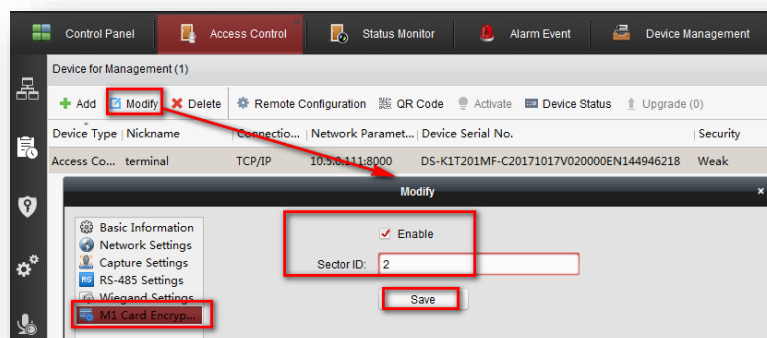
2. Enable **M1 Card Encryption** in iVMS access control module->Person and Card tab->User options->Add Card->Set Card Enrolment Station. Click Modify to select the sector where the encryption code will be written. Hikvision Mifare M1 card model IC S50 has 16 sectors (Sector 0 – Sector 15), so the **Select Sector** option should be no more than 16.



3. For **Card No. Type**, set **Normal** (M1 Card Encryption function supports only **Normal** type). **Normal** means 10-digit card No. on iVMS-4200 client and in this case card reader should be connected to the terminal only via RS-485 interface;



4. In device management click Modify and Enable **M1 Card Encryption** on the terminal and set the same **Sector ID** as in the enrolment station;



Notice:

1. For higher security, it is suggested to enable encryption for all sectors except for the one that is used for Base on Card Cross-Controller Anti-passing Back function in 260X series controllers;
2. M1 Card Encryption is only for RS-485 connected readers;
3. Instruction on how to upgrade enrolment station can be found on [this link](#);

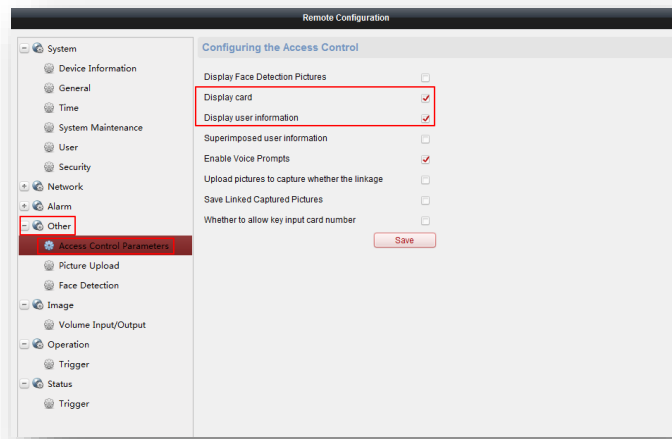
Modified Functions

i. Optimize the UI interface of the authentication screen

1. Show green '✓' on successful authentication (show '✓' only for the last authentication method if the device is in multi-authentication mode);
2. Show red '✗' when authentication has failed;

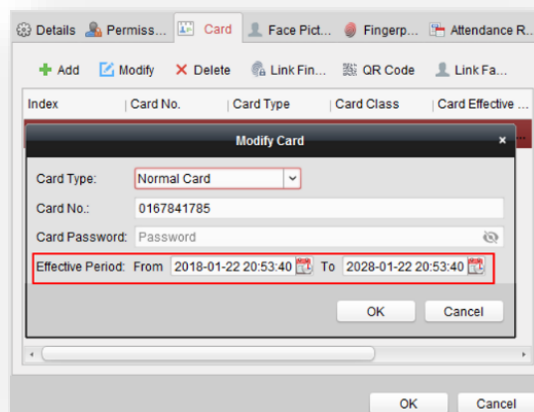


3. Show card holder's Name or card NO. on the display. Enable in Remote configuration on iVMS;

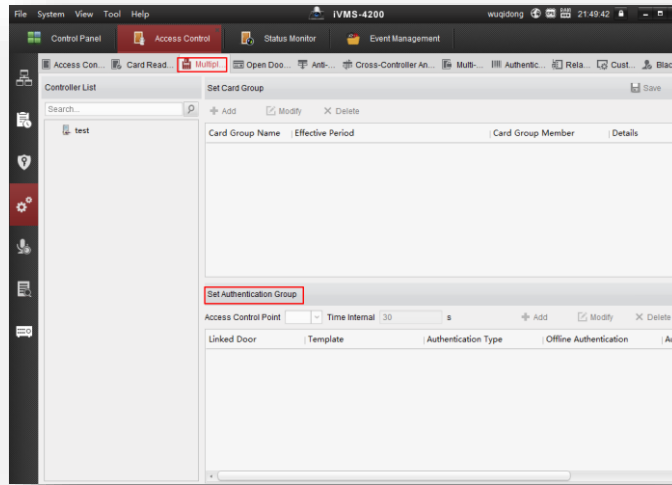


Note: If the device is working in Access Control Terminal mode, it is suggested to upload permission information to DS-K1T20X access control terminals from iVMS-4200 Client;

ii. Card effective period can be set to minutes;

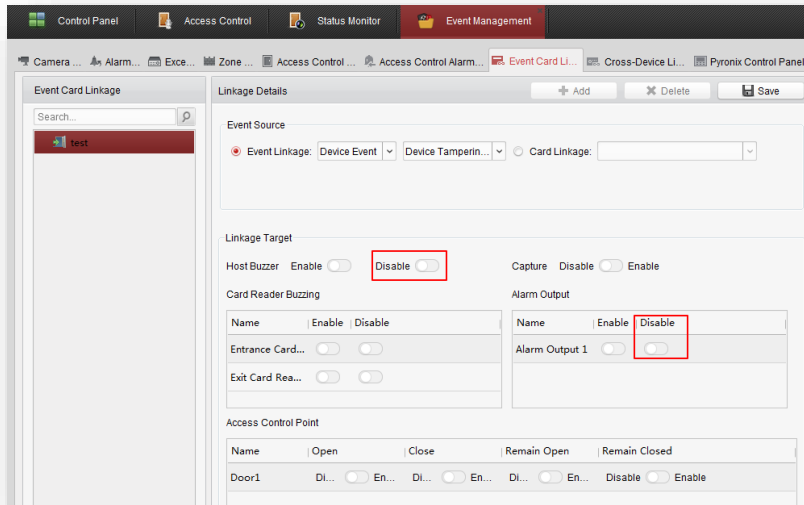


- iii. **Multiple Authentication:** support up to 20 Authentication Groups. A member of each authentication group should present his credential to the terminal in order to unlock the door. Confirmation from iVMS operator or super card can be set.

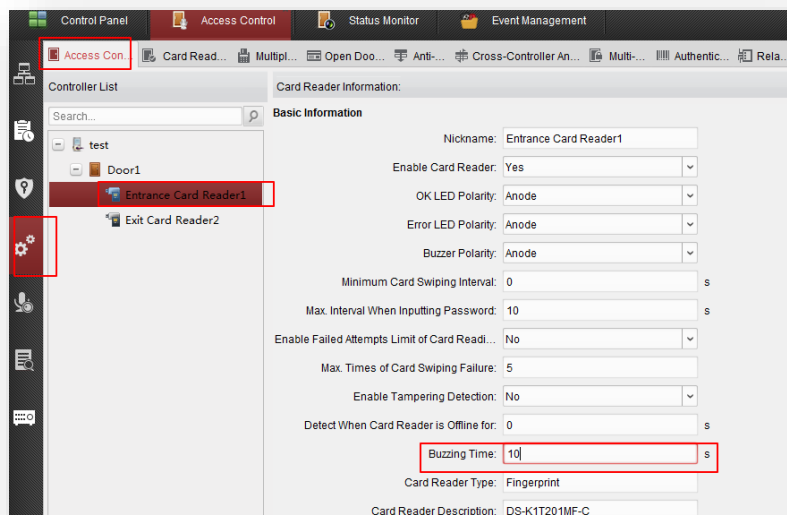


- iv. In **Event Management** -> **Event Card Linkage** interface is available new **Disable** button for Host Buzzer/Card Reader Buzzing;

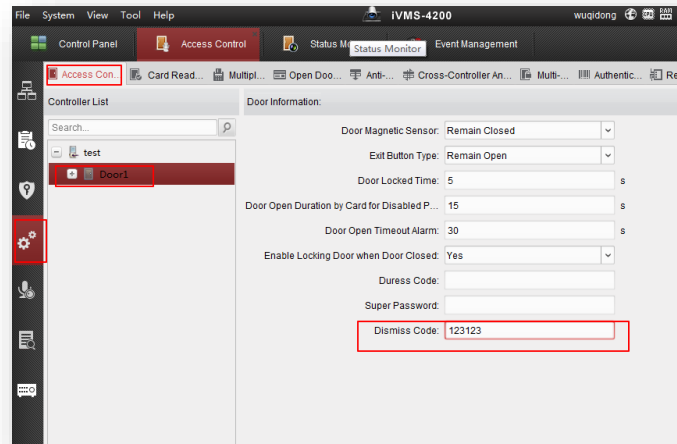
1. Host Buzzer is 20S by default;



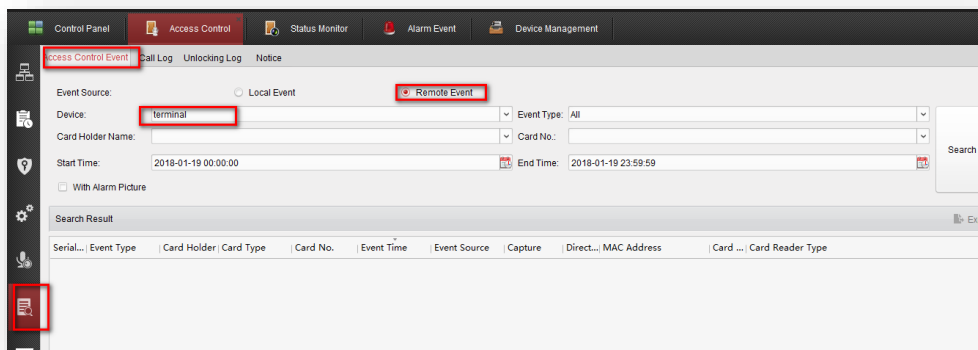
2. Card reader buzzing time can be set from 0 – 5999 (0 means buzzing all the time);



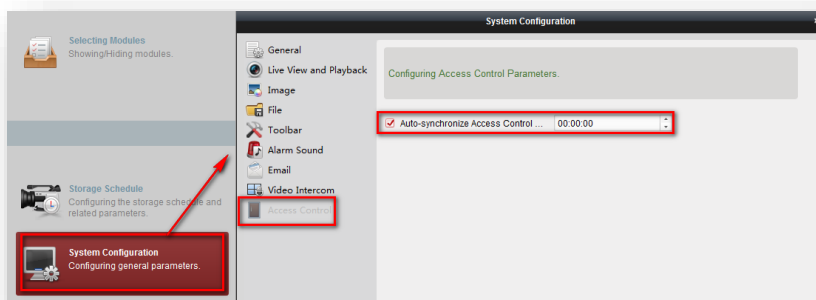
3. Dismiss Code: input dismiss code followed by # on the terminal/reader to stop card buzzing or host buzzing. This action will not unlock the door.



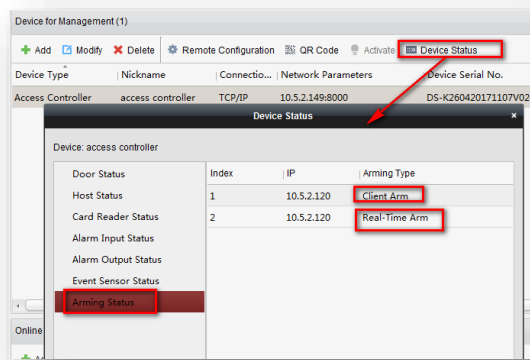
- v. **Remote Event:** support obtaining access control event logs from the terminal instead of iVMS database



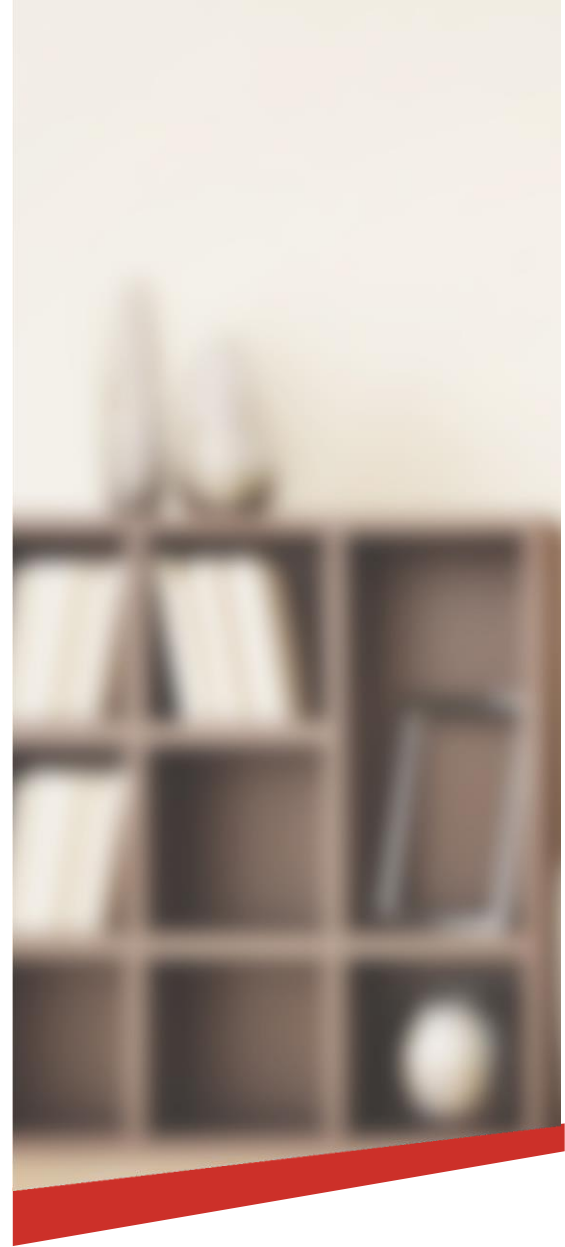
- vi. **Auto-synchronize Access Control Events** – suitable to fetch device events in case the device was armed by another iVMS.



- vii. **Check device arming status on client** – in device management click on the device and press device status button to see which client is receiving the events of the device.



- viii. **Support IP Conflict Alarm:** once occurred, the access controller terminal buzzer will beep like “Bi --- Bi --- Bi --- Bi-Bi ”, every three minutes;



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 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