

A large, stylized graphic of a fingerprint sensor. It features concentric circular patterns in shades of gray and red. In the center, there is a white crosshair-like reticle with three white dots above it. To the left of the main circle, there is a smaller, separate graphic showing several horizontal red dashed lines and a vertical red dashed line intersecting them.

HIKVISION

Fingerprint Time Attendance Terminal

User Manual

V1.0

UD02461B

User Manual

©2016 Hangzhou Hikvision Digital Technology Co., Ltd.

This Manual is intended for users of the series below:

Name	Model
Fingerprint Time Attendance Terminal	DS-K1A801F
	DS-K1A801MF
	DS-K1A801EF

It includes instructions on how to use the Product. The software embodied in the Product is governed by the user license agreement covering that Product.

About this Manual

This Manual is subject to domestic and international copyright protection. Hangzhou Hikvision Digital Technology Co., Ltd. ("Hikvision") reserves all rights to this manual. This manual cannot be reproduced, changed, translated, or distributed, partially or wholly, by any means, without the prior written permission of Hikvision.

Trademarks

HIKVISION and other Hikvision marks are the property of Hikvision and are registered trademarks or the subject of applications for the same by Hikvision and/or its affiliates. Other trademarks mentioned in this manual are the properties of their respective owners. No right of license is given to use such trademarks without express permission.

Legal Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, IS PROVIDED "AS IS", WITH ALL FAULTS AND ERRORS, AND HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF THIRD PARTY. IN NO EVENT WILL HIKVISION, ITS DIRECTORS, OFFICERS, EMPLOYEES, OR AGENTS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA OR DOCUMENTATION, IN CONNECTION WITH THE USE OF THIS PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

SURVEILLANCE LAWS VARY BY JURISDICTION. PLEASE CHECK ALL RELEVANT LAWS IN YOUR JURISDICTION BEFORE USING THIS PRODUCT IN ORDER TO ENSURE THAT YOUR USE CONFORMS THE APPLICABLE LAW. HIKVISION SHALL NOT BE LIABLE IN THE EVENT THAT THIS PRODUCT IS USED WITH ILLEGITIMATE PURPOSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

Support

Should you have any questions, please do not hesitate to contact your local dealer.

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC compliance: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.

FCC Conditions

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation

EU Conformity Statement



This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the RE Directive 2014/53/EU, the EMC Directive 2014/30/EU, the RoHS Directive 2011/65/EU.



2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info.

2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see: www.recyclethis.info.

Industry Canada ICES-003 Compliance

This device meets the CAN ICES-3 (B)/NMB-3(B) standards requirements.

This device complies with Industry Canada licence-exempt RSS standard(s).

Operation is subject to the following two conditions:

- (1) this device may not cause interference, and
- (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radioexempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

- (1) l'appareil ne doit pas produire de brouillage, et
- (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut

fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.

Cet équipement doit être installé et utilisé à une distance minimale de 20 cm entre le radiateur et votre corps.

Safety Instruction

These instructions are intended to ensure that user can use the product correctly to avoid danger or property loss.

The precaution measure is divided into **Warnings** and **Cautions**:

Warnings: Neglecting any of the warnings may cause serious injury or death.

Cautions: Neglecting any of the cautions may cause injury or equipment damage.

	
Warnings Follow these safeguards to prevent serious injury or death.	Cautions Follow these precautions to prevent potential injury or material damage.



Warnings

- All the electronic operation should be strictly compliance with the electrical safety regulations, fire prevention regulations and other related regulations in your local region.
- Please use the power adapter, which is provided by normal company. The power consumption cannot be less than the required value.
- Do not connect several devices to one power adapter as adapter overload may cause over-heat or fire hazard.
- Please make sure that the power has been disconnected before you wire, install or dismantle the device.
- When the product is installed on wall or ceiling, the device shall be firmly fixed.
- If smoke, odors or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the device yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)



Cautions

- Do not drop the device or subject it to physical shock, and do not expose it to high electromagnetism radiation. Avoid the equipment installation on vibrations surface or places subject to shock (ignorance can cause equipment damage).
- Do not place the device in extremely hot (refer to the specification of the device for the detailed operating temperature), cold, dusty or damp locations, and do not expose it to high electromagnetic radiation.
- The device cover for indoor use shall be kept from rain and moisture.
- Exposing the equipment to direct sun light, low ventilation or heat source such as heater or radiator is forbidden (ignorance can cause fire danger).
- Do not aim the device at the sun or extra bright places. A blooming or smear may occur otherwise (which is not a malfunction however), and affecting the endurance of sensor at the same time.

- Please use the provided glove when open up the device cover, avoid direct contact with the device cover, because the acidic sweat of the fingers may erode the surface coating of the device cover.
- Please use a soft and dry cloth when clean inside and outside surfaces of the device cover, do not use alkaline detergents.
- Please keep all wrappers after unpack them for future use. In case of any failure occurred, you need to return the device to the factory with the original wrapper. Transportation without the original wrapper may result in damage on the device and lead to additional costs.
- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.

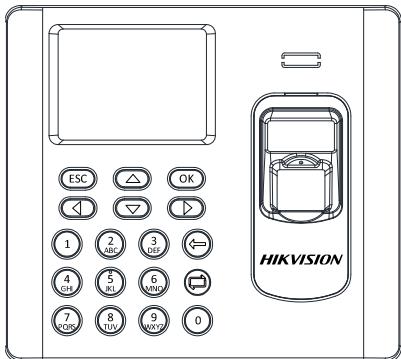
Contents

Chapter 1 Overview.....	3
1.1 Introduction	3
1.2 Main Features	3
1.3 Appearance	4
1.4 Keypad Description	5
Chapter 2 Installation	6
2.1 Wall Mounting.....	6
2.2 Wall Mounting with Mounting Plate	7
Chapter 3 Basic Operation	8
3.1 Device Activation	8
3.1.1 Activating via SADP Software.....	9
3.1.2 Activating via Client Software	10
3.2 Login.....	13
3.3 Parameters Configuration.....	13
3.3.1 Communication Settings.....	13
3.3.2 System Settings	15
3.3.3 Setting Time	20
3.4 User Management	20
3.4.1 Adding User.....	21
3.4.2 Managing the User.....	24
3.5 Department Management	25
3.5.1 Editing and Resetting the Department	25
3.5.2 Searching the Department.....	26
3.5.3 Resetting the Department	27
3.6 Shift Management	27
3.6.1 Normal Shift	28
3.6.2 Man-Hour Shift	29
3.7 Holiday Management.....	31
3.7.1 Adding the Holiday.....	31
3.7.2 Searching the Holiday	31
3.7.3 Editing and Deleting the Holiday	31
3.8 Shift Schedule Management.....	32
3.8.1 Scheduling Shift by Department	32
3.8.2 Scheduling Shift by Individual.....	34
3.9 Other Management	36
3.9.1 Report Management.....	36
3.9.2 Data Transfer	38
3.9.3 Searching the Log	39
3.9.4 Testing	40
3.9.5 System Information.....	42
Chapter 4 Client Operation	44
4.1 Overview of Access Control System.....	44
4.1.1 Description	44
4.1.2 Configuration Flow.....	44
4.2 Device Management.....	45

4.2.1 Controller Management.....	45
4.2.2 Access Control Point Management.....	60
4.3 Permission Management	62
4.3.1 Person Management.....	62
4.3.2 Card Management	65
4.3.3 Schedule Template	68
4.3.4 Door Status Management	72
4.3.5 Interact Configuration.....	74
4.3.6 Access Permission Configuration	77
4.3.7 Advanced Functions.....	82
4.4 Attendance Management	86
4.4.1 Shift Group Management	86
4.4.2 Shift Management	88
4.4.3 Holiday Management.....	91
4.4.4 Shift Schedule Management.....	92
4.4.5 Attendance Check Point Management	93
4.4.6 Adjustment Management.....	94
4.4.7 Card Swiping Log Query	99
4.4.8 Statistic Analysis.....	99
4.4.9 Parameters Configuration	101
4.4.10 Data Management	101
4.5 Checking Status and Event	102
4.5.1 Status Monitor	102
4.5.2 Access Control Event.....	104
4.5.3 Event Search.....	104
4.6 System Maintenance.....	105
4.6.1 Log Management	105
4.6.2 System Configuration	108
Chapter 5 Appendix.....	112
5.1 Tips for Scanning Fingerprint	112
5.2 Attendance Record Delete Rule	113
5.2.1 Enabling Record Delete	113
5.2.2 Disabling Record Delete	113
5.3 Attendance Performance	114
5.4 Attendance Report Table	115
5.4.1 Description of Attendance Report File Name	115
5.4.2 Attendance Report Table Description	116

Chapter 1 Overview

1.1 Introduction



DS-K1A801 Series Fingerprint Time Attendance Terminal is designed with a 2.8-inch LCD display screen. It supports swiping card or scanning fingerprint for attendance, generating the attendance report automatically. Offline operation, wired network (TCP/IP) and wireless network transmission modes are supported as well.

1.2 Main Features

- 2.8-inch LCD display screen
- Transmission modes of wired network (TCP/IP) and wireless network
- Max. 3,000 users, 3,000 fingerprints and 100,000 access control events records storage
- Configure attendance type by device or by person
- Locally add the user information (User Name, Card No., Fingerprint, etc.), and configure the shift, shift schedule and the attendance rule
- Max. 32 normal shifts, 32 man-hour shifts and 32 holiday schedules
- Set the shift schedule by department or by person
- Generate the attendance report automatically via the device and the client software
- Export the report and upgrade the device via the USB disk.
- Inputting Chinese characters, upper-case and lower-case letters, numbers and symbols is available
- Hint for full report memory
- Authenticate via ID No. + password, card or fingerprint for the admin
- Different authentication types according to different device models:
 1. Fingerprint (DS-K1A801F)
 2. EM card reading and fingerprint (DS-K1A801EF)
 3. Mifare card reading and fingerprint (DS-K1A801MF)

1.3 Appearance

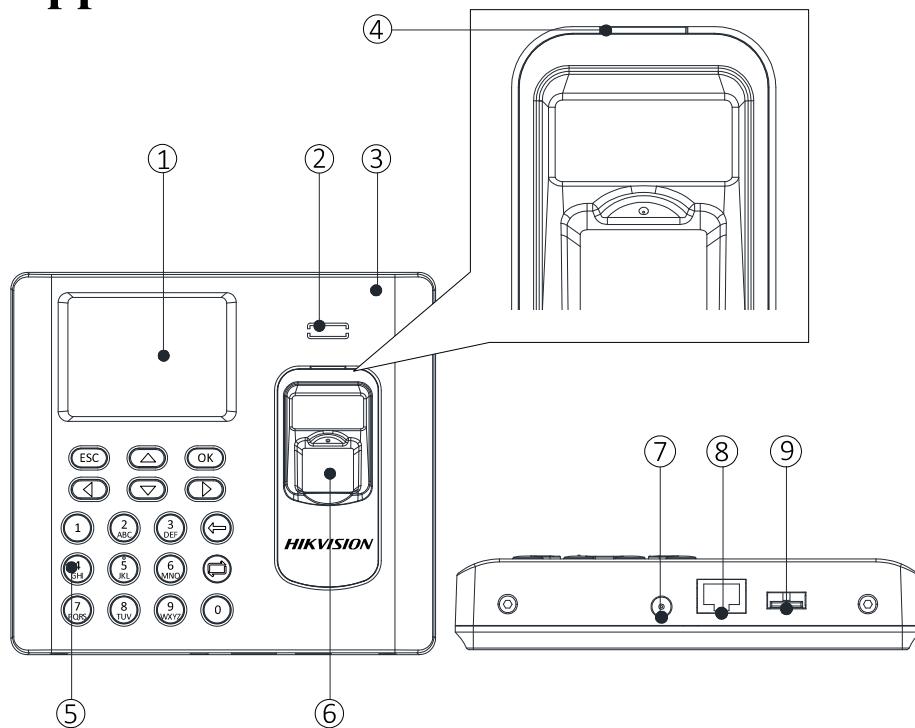


Table 1. 1 Description of DS-K1A801 Series Model

No.	Description
1	2.8-inch LCD Display Screen
2	Loudspeaker
3	Front Cover
4	Indicator
5	Keypad
6	Fingerprint Reading Module
7	12V Power Interface
8	Ethernet Port
9	USB Interface

1.4 Keypad Description



Table 1. 2 Keypad Description

No.	Description
1	Exiting Key: Press the button to exit the menu.
2	Direction Keys: Use \triangle , ∇ , \leftarrow , \rightarrow to move the cursor in the menu.
3	Numeric Keys/Letter Keys: Press to input numbers or letters.
4	Confirming Key: Press to confirm operations. Press and hold the key for 3s to login the main interface.
5	Deleting Key: Delete the contents in the textbox.
6	Editing Key: Press to enter the editing status. Press to shift among Chinese, numbers/lowercases, numbers/uppercases and symbols.

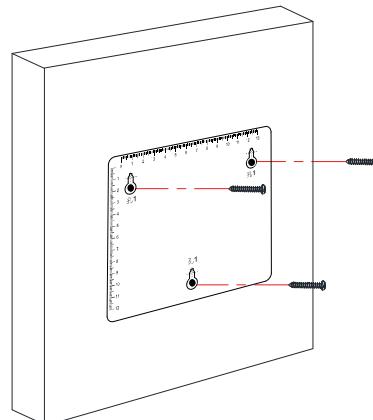
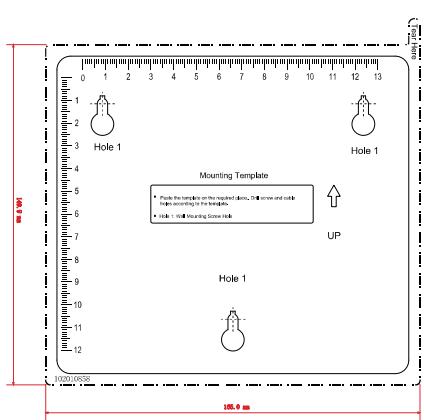
Chapter 2 Installation

2.1 Wall Mounting

Steps:

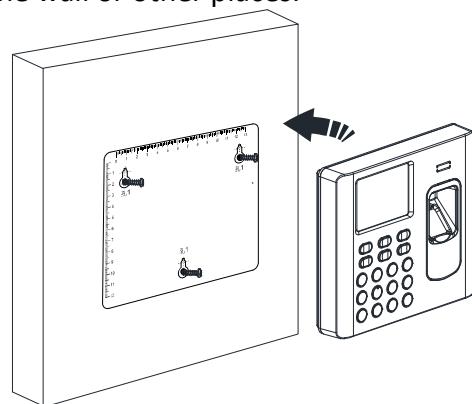
1. Drill holes on the wall or other places according to the mounting template (supplied).

Note: The minimum bearing weight of the wall or other places should be three times heavier than the device weight.



2. Insert the screw sockets of the setscrews in the drilled holes.
3. Fix and fasten the screws in the sockets on the wall or other places.

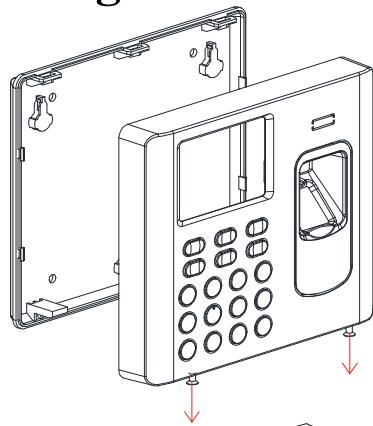
4. Align the three holes on the device plate with the fixed screws and hang the device on the wall.



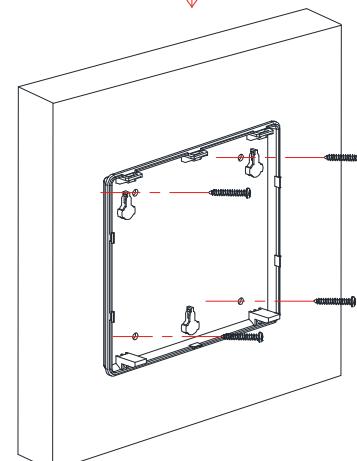
2.2 Wall Mounting with Mounting Plate

Steps:

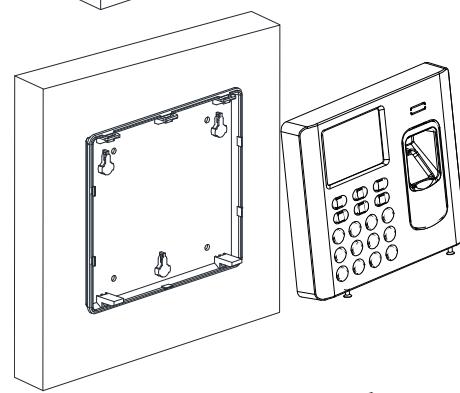
1. Remove the two screws at the bottom of the front cover and remove the back cover.



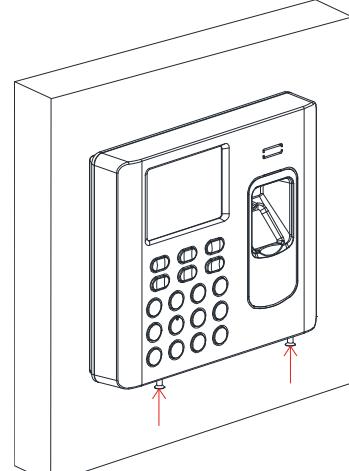
2. Align the back cover on the level on the wall or other places.
3. Drill through the holes at the four corners of the back cover.
4. Insert the screw sockets of the setscrews in the drilled holes.
5. Fasten the screws in the sockets to fix the back cover on the wall or other places.



6. Align the front cover to the back cover and buckle them together.

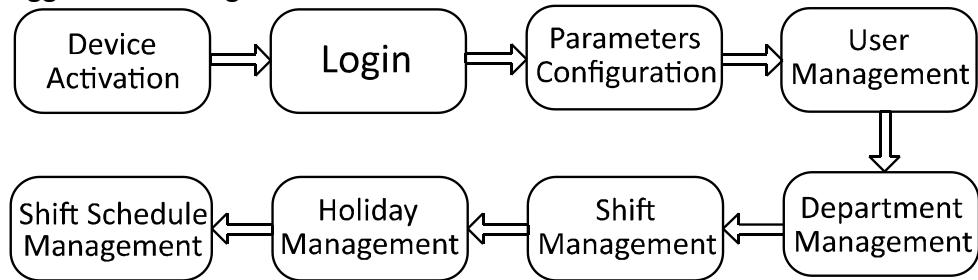


7. Fix and fasten the screws at the bottom of the front cover.



Chapter 3 Basic Operation

The suggested working flow is as follows:



Device Activation: Activate the device before first using.

Login: Hold the OK key for 3s to login the device main interface.

Parameters Configuration: Configure the communication, the system, and the time.

User Management: Add, edit and delete the users.

Department Management: Edit the default department.

Shift Management: Configure the normal shift and the man-hour shift.

Holiday Management: Configure the holiday.

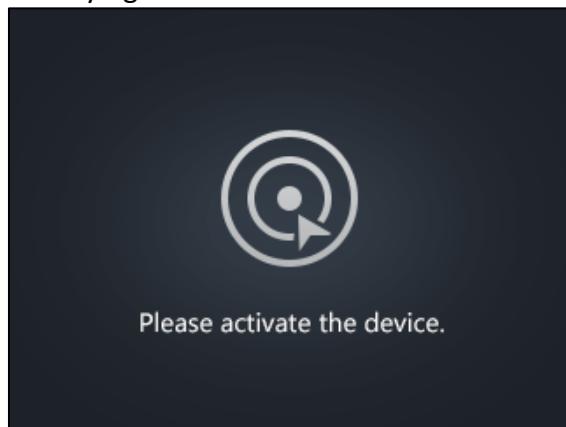
Shift Schedule Management: Schedule by department or by individual.

Note: The device has configured the default department, the default shift, the default shift schedule and the default system information. You are able to use the device directly after adding the user.

3.1 Device Activation

Purpose:

You should activate the device before the first login. After powering on, the system will switch to activate notifying interface.



Activation via SADP and activation via the iVMS-4200 Client Software are supported.

The default values of the terminal are as follows:

- The default IP address: 192.0.0.64
- The default port No.: 8000
- The default user name: admin

3.1.1 Activating via SADP Software

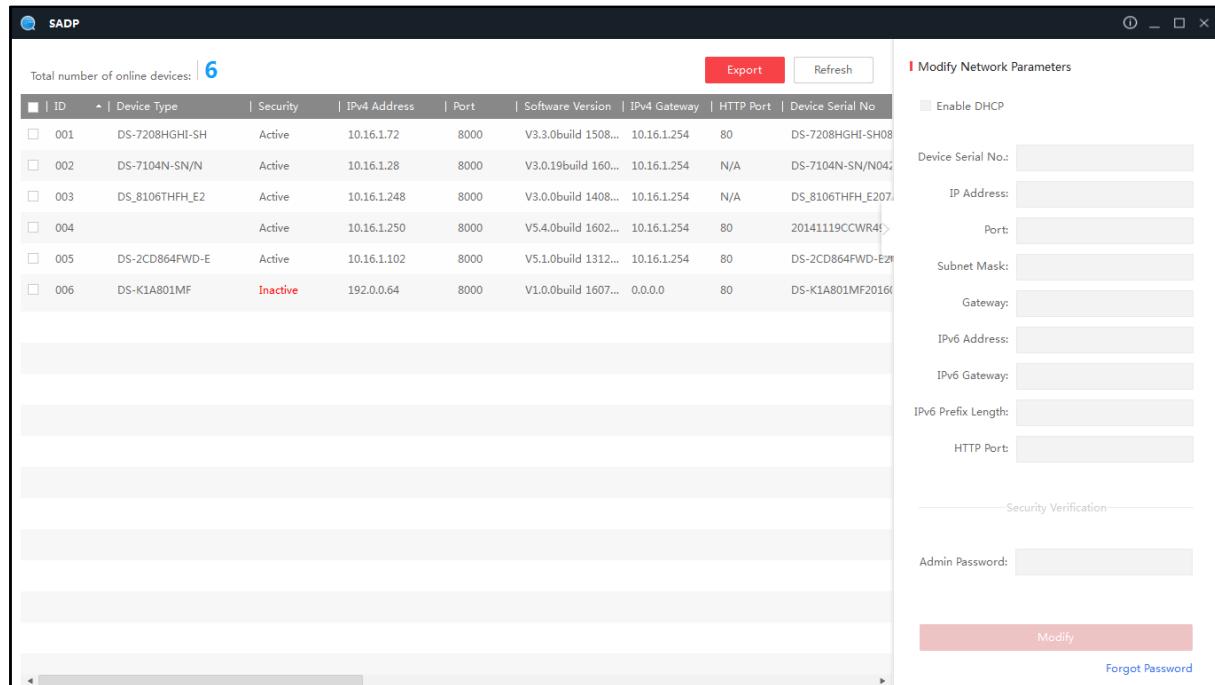
Purpose:

SADP software is used for detecting the online device, activating the device, and resetting the device password.

Steps:

1. Get the SADP software from the supplied disk or the official website. Install and run the software.

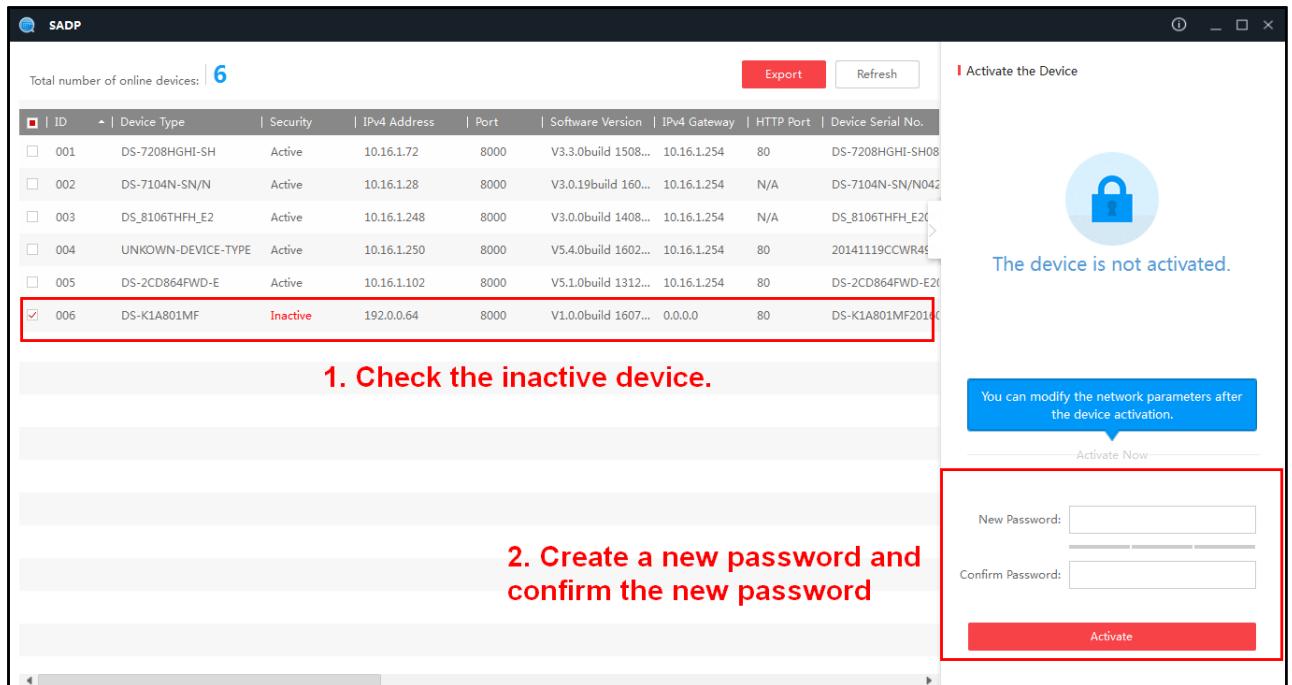
Note: Go to http://www.hikvision.com/en/tools_82.html to download the SADP software.



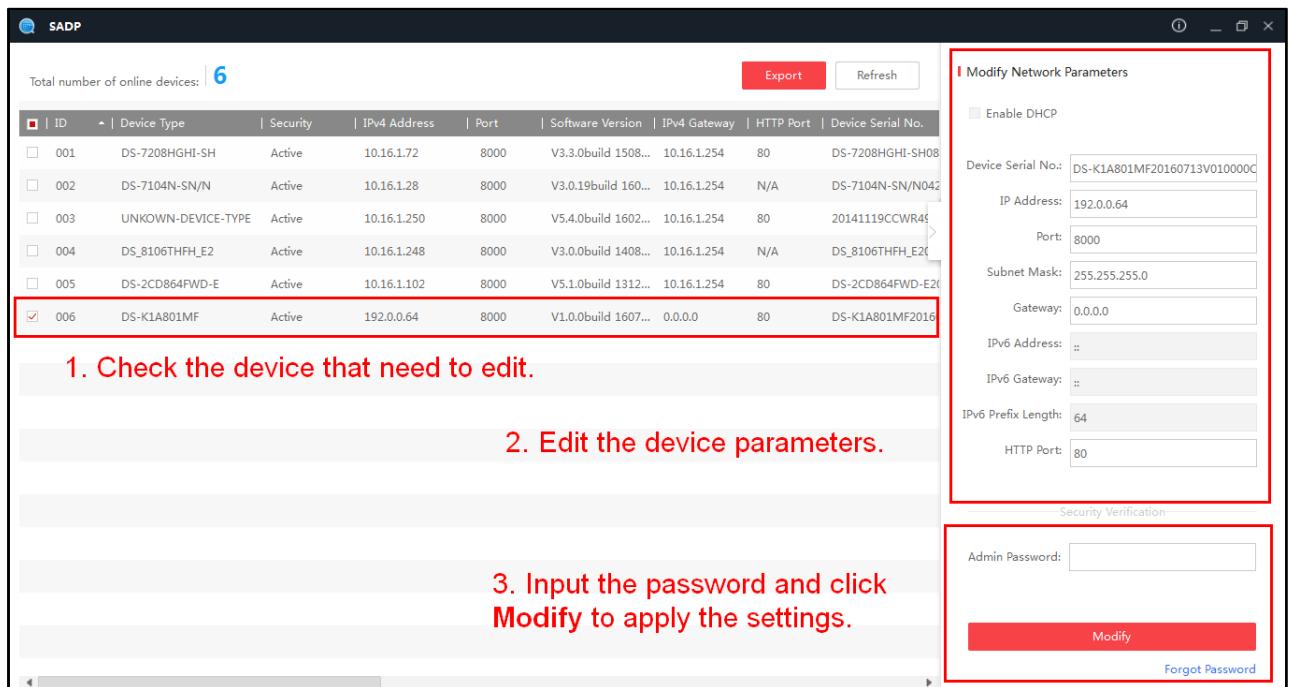
2. Check the inactive device from the device list.
3. Create a password in the right side of the interface and confirm the password.



STRONG PASSWORD RECOMMENDED— We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.



4. Click **Activate**. The device will be active.
Or click **Fresh** to fresh the device status.
 5. Check the device and manually edit the device IP address, Port No., Subnet Mask, Gateway, etc. Or check DHCP to enable DHCP.
 6. Input the password and click **Modify** to apply the settings.
- Note:** The device IP address should be the same with the PC's.



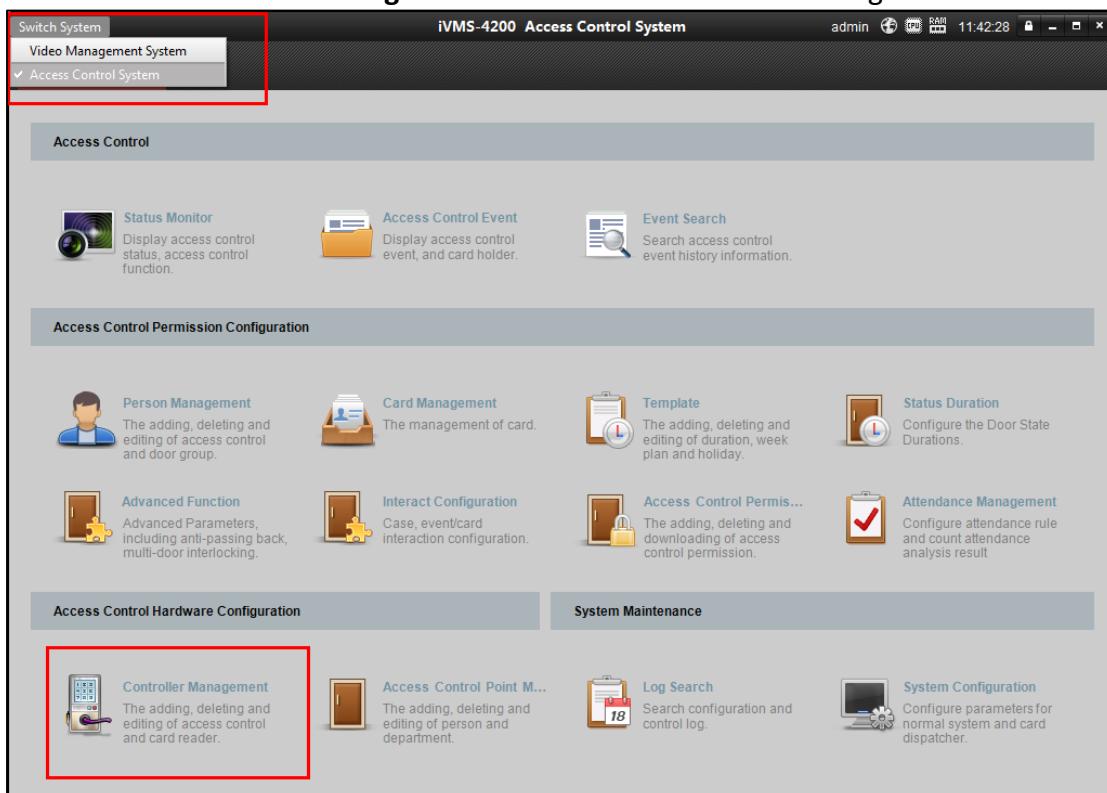
3.1.2 Activating via Client Software

Purpose:

The client software is versatile video management software for multiple kinds of devices.

Steps:

1. Get the client software from the supplied disk or the official website. Install and run the client software.
- Note:** Go to http://www.hikvision.com/en/Tools_84.html to download the client software.
2. Click **Switch System -> Access Control System** at the upper left corner of the interface to enter the Access Control System interface.
3. Click **Controller Management** to enter the Controller Management interface.



You can check the online device, as shown in the figure displayed below:

Device Managed (0)						
Add Device		Edit	Delete	Bulk Time...	Status	Remote Co...
Name	Type	Connection M...		IP	Port	Baud Rate
		Port	Dial-up	Connection St...	Refresh	

Online Devices (1)						
Add to Client		Add All Device	Edit Network...	Reset P...	Activate	Filter
Name	Type	IP	Port	Activated	Added	
44-19-b6-c5-cb-a6	Access Controller_DS-K1A801MF	192.0.0.64	8000	No	No	

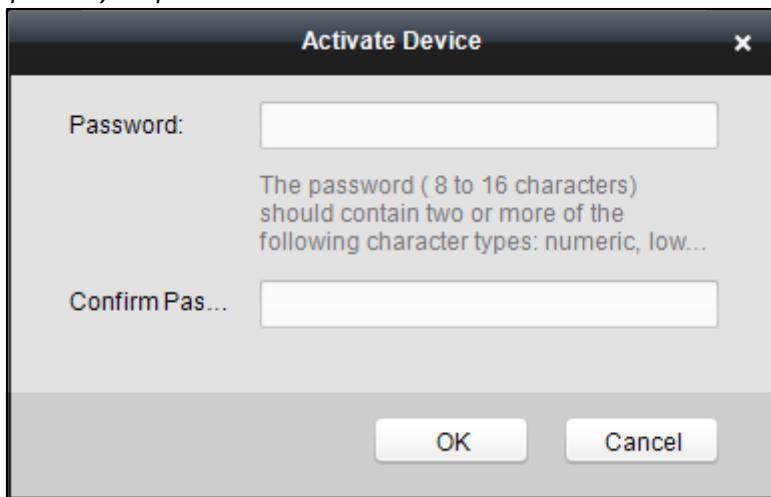
4. Select an inactive device from the device list.
5. Click **Activate** to pop up the Activation interface.

Online Devices (1)					
Name	Type	IP	Port	Activated	Added
44-19-b6-c5-cb-a6	Access Controller_DS-K1A801MF	192.0.0.64	8000	No	No

6. Create a password and confirm the new password.

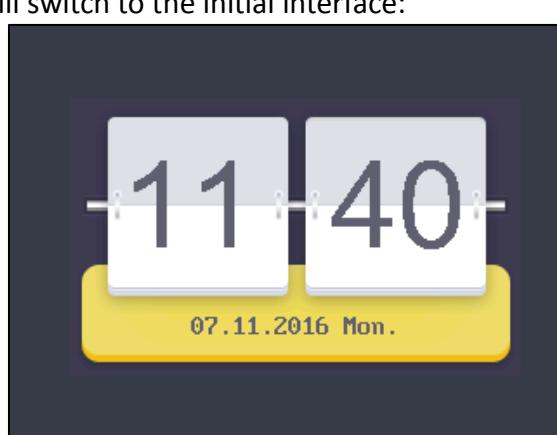


STRONG PASSWORD RECOMMENDED— We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.



7. Click **OK** to start activate.
8. Click **Edit Network...** to configure the device IP address, mask address, gateway address, port No.
9. Input the password and click **OK** to apply.

Note: The device IP address should be the same with the PC.
The device will switch to the initial interface:

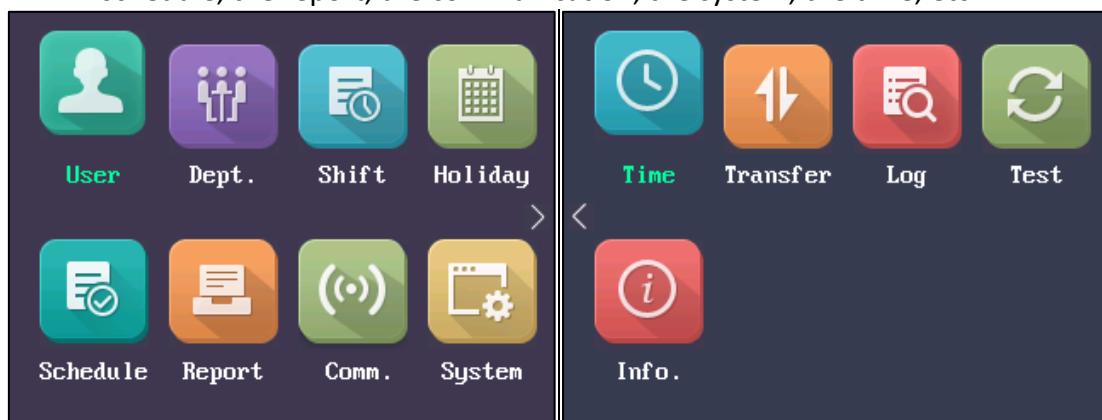


3.2 Login

Steps:

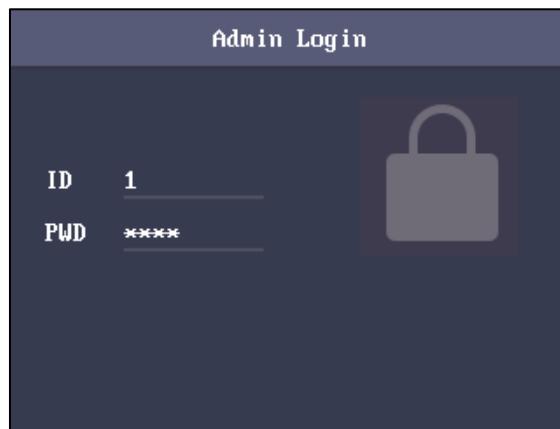
1. For the first time login, long-press the OK key for 3s to enter the main interface.

You can manage the user, the department, the shift, the holiday, the shift schedule, the report, the communication, the system, the time, etc.



If you have configured the admin in the User interface, then

- 1) Long-press OK key to enter the Admin Login interface.
- 2) Enter the admin ID No. and password, scan the fingerprint or swipe the card to enter the main interface.

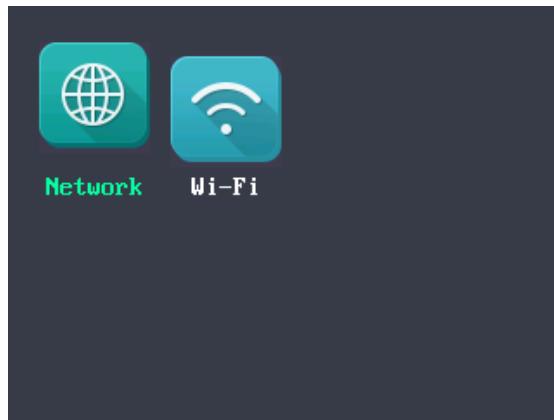


3.3 Parameters Configuration

3.3.1 Communication Settings

Purpose:

You can set the network parameters and the Wi-Fi.



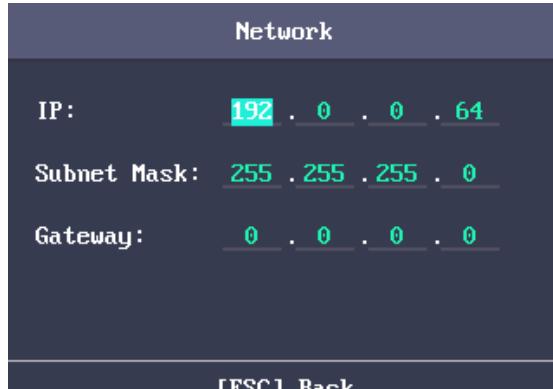
Setting Network

You can set the device network parameters, including the IP address, the subnet mask and the gateway address.

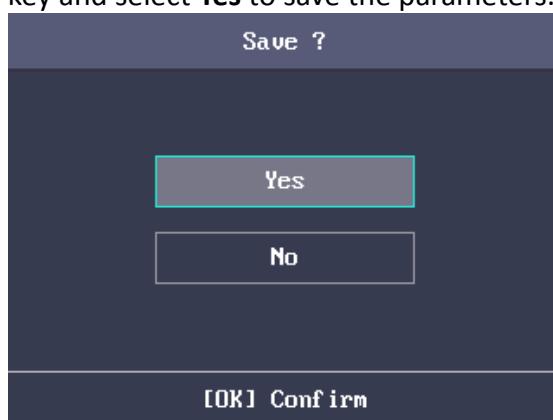
Steps:

1. Move the cursor to the **Network** and press the OK key to enter the Network interface.
2. Edit the IP address, the subnet mask and the gateway.

Note: The IP address should be the same with the PC's.



3. Press the ESC key and select **Yes** to save the parameters.



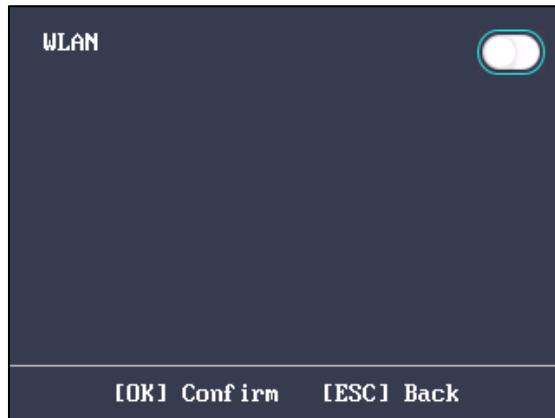
Setting Wi-Fi

Purpose:

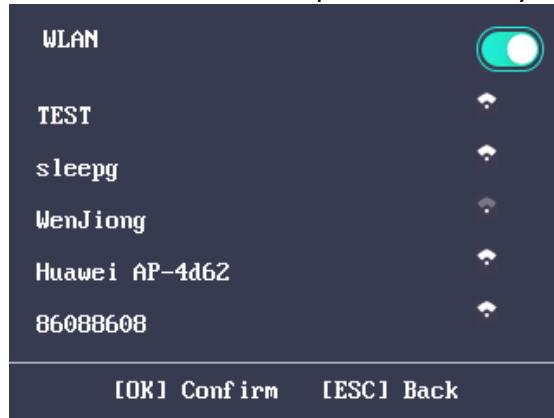
You can enable the Wi-Fi and configure the Wi-Fi parameter.

Steps:

- Move the cursor to the **Wi-Fi**, and press the OK key to enter the Wi-Fi interface.



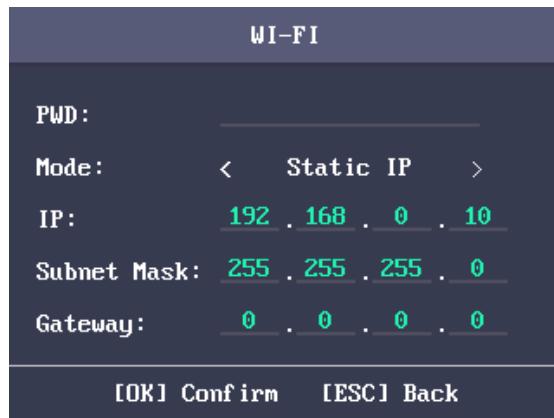
- Move the cursor to the icon and press the OK key to enable the WLAN.



- Select a network and press the OK key to enter the Wi-Fi Setting interface.

- Input the Wi-Fi password, and configure the IP mode the IP address, the subnet mask and the gateway.

Note: The password supports numbers, uppercase letters, lowercase letters and symbols.

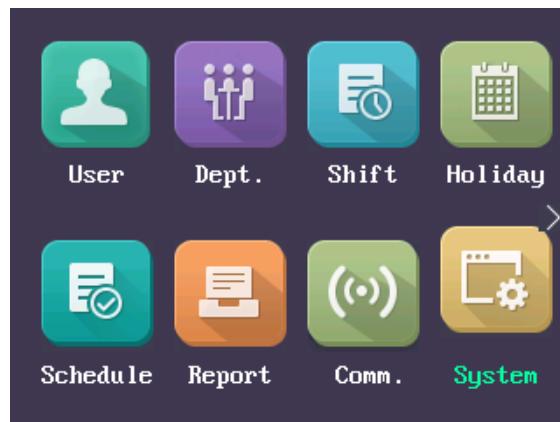


- Press the ESC key and select **Yes** to save the parameters and exit the interface.

3.3.2 System Settings

Purpose:

You are able to set the system parameters, manage the data, restore default parameters and upgrade the device.



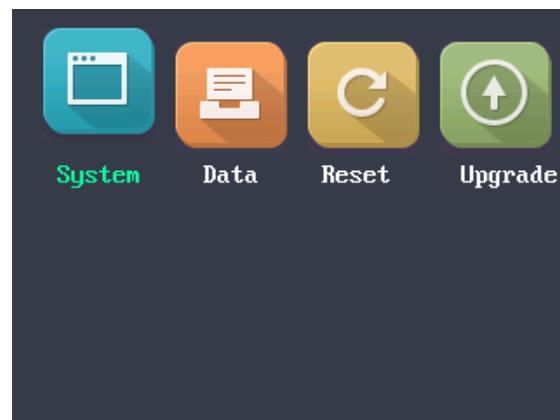
Setting System Parameters

Purpose:

Set the system parameters, including the device time format, the keypad sound, the voice prompt, the volume, the sleeping, the attendance repeating time interval, the attendance record prompt and the authentication mode.

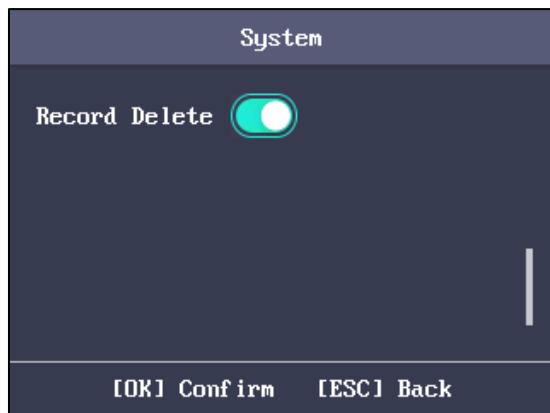
Steps:

1. Move the cursor to **System** and press the OK key to enter the System interface.



2. Edit the parameters.

System		System	
Time Format: < MM.DD.YYYY >		Sleeping: 30 min	
Keypad Sound: <input checked="" type="checkbox"/>		Interval: 0 s	
Voice Prompt: <input checked="" type="checkbox"/>		Record over 99 %, Pop up Promp.	
Voice Volume: < Medium >		Auth Mode: < Card / FP >	
[OK] Confirm [ESC] Back		[OK] Confirm [ESC] Back	



- Time Format:** MM/DD/YYYY, MM.DD.YYYY, DD-MM-YYYY, DD/MM/YYYY, DD.MM.YYYY, YYYYMMDD, YYYY-MM-DD, YYYY/MM/DD, YYYY.MM.DD and MM-DD-YYYY are available.
- Keypad Sound:** Move the cursor to or and press the OK key to enable or disable the keypad sound.
- Voice Prompt:** Move the cursor to or and press the OK key to enable or disable the prompt audio.
- Note:** The icon represents the keypad sound is enabled.
- The icon represents the keypad sound is disabled.
- Voice Volume:** High, Medium and low can be selected.
- Sleeping:** Set the device sleeping waiting time (Minute). If you set the sleeping time to 30min, the device will sleep after 30 min without any operation.
- Note:** If you set the sleeping time to 0, the device will not sleep.
- Interval:** Set the attendance repeating time interval (Second) of a person. The attendance is invalid if you swipe the card repeatedly within the time interval. (Set the authentication mode to Card).
- Note:** The time interval should be between 0 and 255s.
- Record over Threshold Prompt:** If the attendance record memory reaches the configured value, the system will pop up a prompt to remind you.
- Authentication Mode:** The authentication mode can be switched among "card/fingerprint", "card", "fingerprint", "card & password", "card & fingerprint", "fingerprint & password", "card & fingerprint" and "password", and "card/password (The password here refers to the card ID No. and the user password)".
- Record Delete:** When the function is enabled, the terminal will delete the first 3000 attendance records when the memory is full, in order to save the new attendance records. By default, the function is enabled. See *Section 5.2 Attendance Record Delete Rule*.

3. Press the ESC key and select Yes to save the settings and exit the interface.

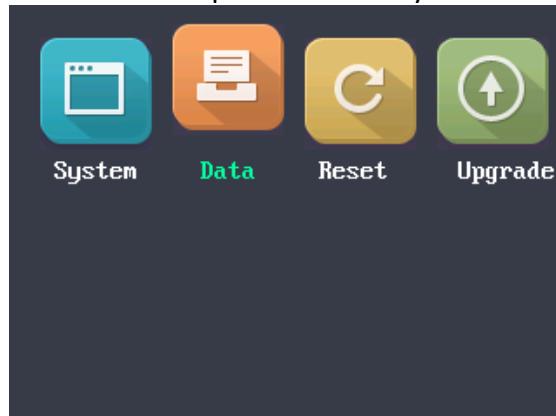
Managing Data

Purpose:

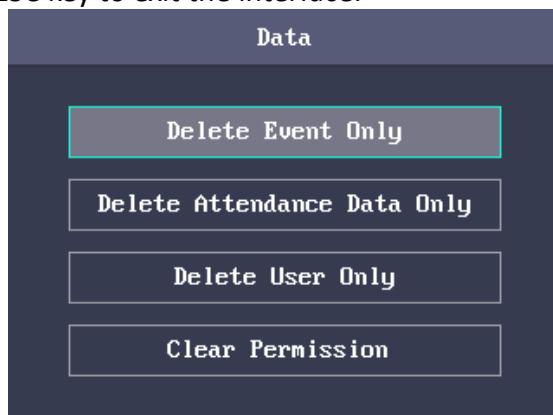
You are able to delete the storage data of the device, including the event, the attendance data, the user, and the permission.

Steps:

1. Move the cursor to **Data** and press the OK key to enter the Data interface.



2. Select a data type and press the OK key to delete.
Or press the ESC key to exit the interface.



Delete Event Only: Delete all recorded events in the device.

Delete Attendance Data Only: Delete all attendance data in the device.

Data Only:

<p>Delete Attendance Data</p> <p>Delete By Time (highlighted in blue)</p> <p>Delete All</p> <p>[OK] Confirm [ESC] Back</p>	<p>Input Time</p> <p>Press OK to delete records</p> <p>before 2016 Y 7 M 1 D</p> <p>[OK] Confirm [ESC] Back</p>
---	---

Figure 3. 1 Delete Attendance Data Interface

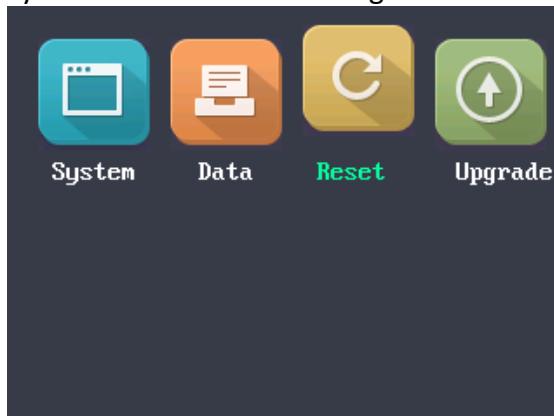
Delete User Only: Delete all user data in the device, including the attendance records.

Clear Permission: Clear the admin management permission. The admin will turn to the normal user. The user will not be deleted.

Restoring Settings

Purpose:

You can restore Factory Defaults or Default Settings.



Steps:

1. Move the cursor to **Reset** and press the OK key to enter the Reset interface.



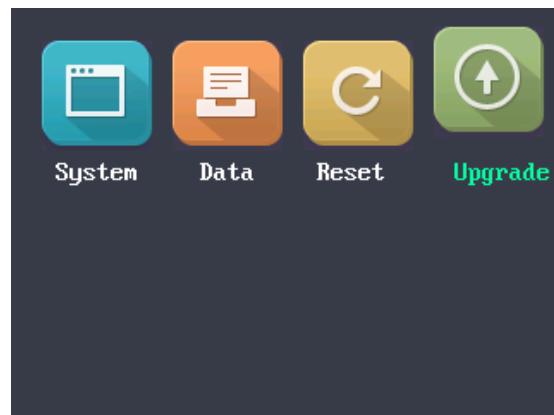
2. Select **Factory Defaults** or **Default Settings**.

Factory Defaults: All parameters of the device will restore to the factory condition.

Default Settings: All parameters, excluding the communication parameters and the remote user management, will restore to the factory condition.

Upgrading Device

The system can automatically read the upgrading file from the plugged USB disk to upgrade the device.



Notes:

- The upgrading file should be put in the root directory.
- The upgrading file name in the USB disk should be digicap.dav.

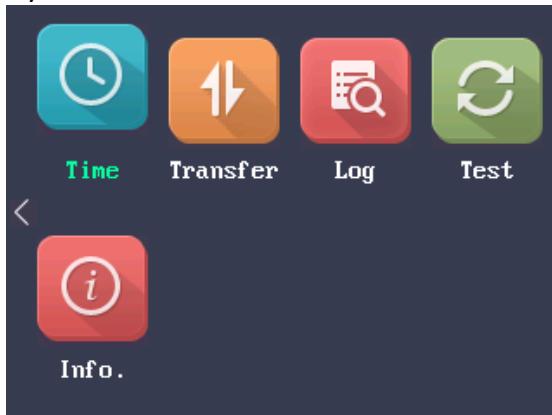
3.3.3 Setting Time

Purpose:

You are able to set the device time and the DST.

Steps:

1. Move the cursor to **Time** in the main interface.
2. Press the OK key to enter the Time interface.



3. Edit the parameters.

Date: The displayed date on the device.

Time: The displayed time on the device.

DST: Select to enable or disable the DST. When the DST is enabled, you can set the DST bias time, the start time and the end time.

- **DST Bias:** you can select 30min, 60min, 90min and 120min.
- **Start:** Set the start time of the DST.
- **End:** Set the end time of the DST.

Time									
Date:	2016	Y	08	M	18	D	<	Mon	>
Time:	14	H	26	M	58	S	02	:	00
DST:	< Disable >								
DST Bias:	< 60 >								
[OK] Confirm					[ESC] Back				
Start: 05 (M) 2 (W) < Mon >					End: 11 (M) 5 (W) < Mon >				
02 : 00					02 : 00				

4. Press the ESC key and select **Yes** to save the settings and exit the interface.

3.4 User Management

Purpose:

You are able to add, edit, delete and search the user.

Move the cursor to **User** in the main interface and press the OK key to enter the User interface.



3.4.1 Adding User

You can add users by editing the ID No., the user name, the card No. You can also scan the user fingerprint, set the password, the department, the role and the authentication mode.

Steps:

1. Press the ▶ key to enter the New (new user) interface and input the ID No.

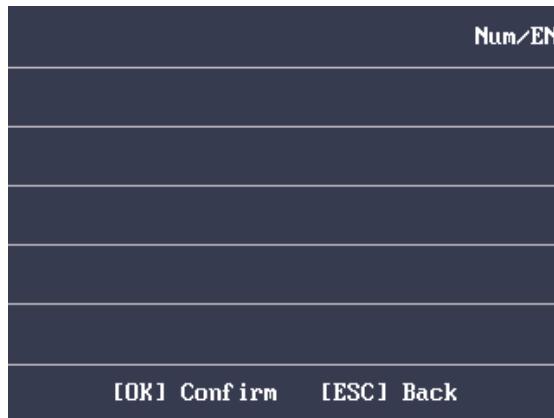
Notes:

- The ID No. refers to the user attendance serial No.
- The ID No. should be between 1 and 99999999 and should not start with 0.
- The ID No. can be used for once.
- By default, the ID No. will be increased in sequence.

User	New	
ID: 1	PWD: Set	None
Name: _____	Dept.: Select	Company
Card: 1	Role: < User >	
FP: Register FP : 0	Auth Mode: < Controller >	
[OK] Confirm [ESC] Back		

2. Enter the new user name.

- 1) Press key to enter the editing interface. Press key to shift input mode. Chinese, Digits/Lowercase Letters, Digits/Uppercase Letters and symbols are supported.
- 2) Enter the use name and press the OK key to confirm and exit the interface.



Notes:

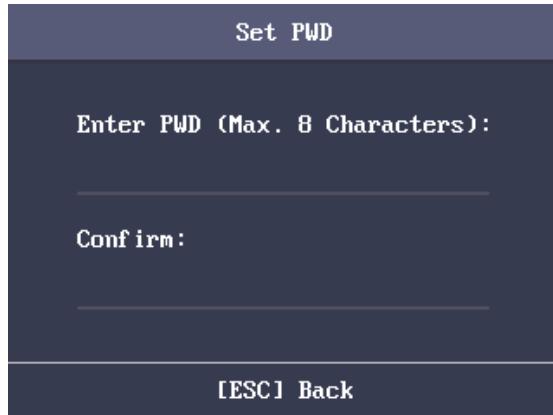
- Digits, uppercase letters, lowercase letters, Chinese characters and symbols are supported.
 - The user name supports up to 32 characters.
 - Each user name can be used for once.
3. Enter the card No.
- Notes:**
- The card No. is required.
 - The card No. can start with 0 when it contains more than one numbers. E.g. 012345.
 - The card No. can be used for once.
 - The device of DS-K1A801F model supports manually entering the card No. The device of DS-K1A801MF and DS-K1A801EF model supports manually entering card No. and swiping card to get the card No.
4. Move the cursor to **Register** and press the OK key scan the fingerprint.
Place the finger on the scanner, rise and confirm your fingerprint by following the voice prompt.

Notes:

- The same fingerprint cannot be repeatedly registered.
- The same ID No. supports adding up to 10 fingerprints.
- The device supports the optical fingerprint recording.
- You can also scan the fingerprint via the external device and apply the fingerprint to the device by the client software.
- For detailed information about scanning the fingerprint, see *Section 5.1 Tips for Scanning Fingerprint*.



5. Move the cursor to **Set** and press the OK key to edit the user password.
- 1) Enter the password and confirm the password in the Set Password interface.



- 2) Press the ESC key and select **Yes** to save the password.
- Note:** Up to 8 digits can be entered.
6. Move the cursor to **Select** and press the OK key to select a department.



- Note:** For detailed information about editing the department, see *Section 3.5.1 Editing and Resetting the Department*.
7. Move the cursor and press the OK key to select the user role.
- Admin:** The admin has all permissions to operate the device.
- User:** The user can check attendance in the initial interface.

Notes:

- All people can enter the main interface to operate if there is no Admin configured.
- After configuring the admin, you have to authorize the admin ID to enter the main interface.
- You can use the USB interface to import the user information. For details, see *Section 2 The USB disk memory should be from 1G to 32G*. Make sure the free space of the USB disk is more than 512M.
- For details about the exported tables descriptions, see *Section 5.4 Attendance Report Table*.
- Data Transfer.

8. Move the cursor to select an authorize mode.

You can select Card/Fingerprint, Card, Fingerprint, Card & Password, Card and Fingerprint, Fingerprint & Password, Card & Fingerprint & Password,

- Card/Password (The password here refers to the card ID No. and the user password), and Controller.
- Press the ESC key and select **Yes** to save the settings and exit the interface.

3.4.2 Managing the User

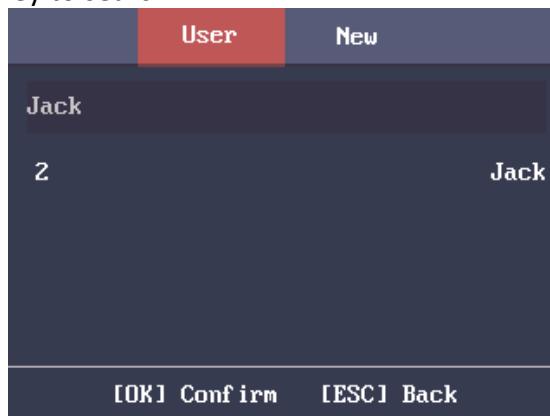
Searching the User

Purpose:

Enter the user ID No. or the user name to search the target user.

Steps:

- Enter the user ID or the user name in the searching bar of the user list interface,
- Press the OK key to search.



Editing the User

Steps:

- Select a target user in the user list and press the OK key.
- Select **Edit User** in the User Configuration interface.



- Follow *Section 3.4.1 Adding User* to edit the user information.
 - Press the ESC key and select **Yes** to save the settings and exit the interface.
- Note:** The user ID cannot be edited.

Deleting Operation

Steps:

- Select the target user for deleting in the User interface.
- Press the OK key to enter the configuration interface.

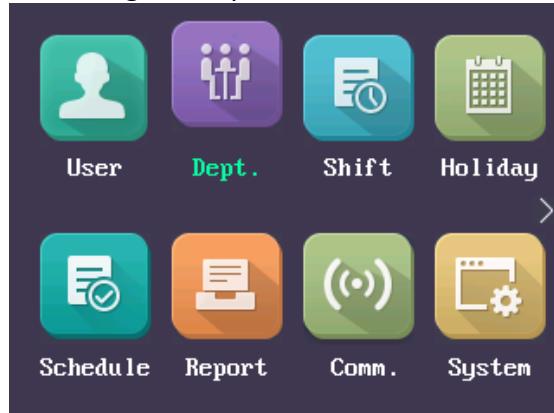


3. Select **Delete User** and press the OK key to delete the target user. The linked user information will be deleted.
Or press **Delete Password** and press the OK key to delete the target user password.
Or press **Clear Fingerprint** and press the OK key to clear the target user fingerprint.
Or press **Clear Card** and press the OK key to delete the user card No.

3.5 Department Management

Purpose:

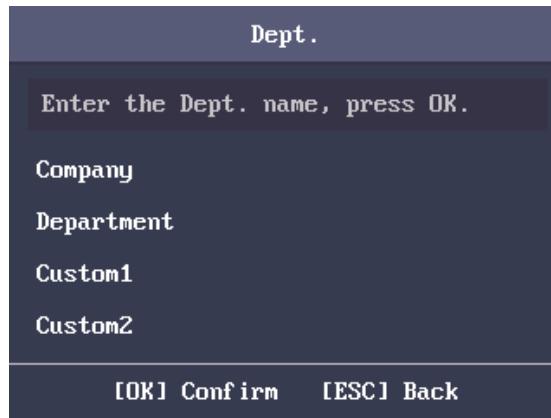
Editing, searching and resetting the department are available.



3.5.1 Editing and Resetting the Department

Steps:

1. Select a target department to edit.



2. Press the OK key to enter the configuration interface.



3. Select **Edit** and press the OK key.
4. Edit the department name, the shift type and the shift name.
5. Press the ESC key and select **Yes** to save the settings and exit the interface.

Notes:

- The department name supports numbers, uppercase letters, lowercase letters, Chinese characters and symbols.
- The department name supports up to 32 characters.
- You can configure the shift in the Shift Management. For detailed information, see *Section 3.6 Shift Management*.
- By default, the system contains 32 departments.

You can also select **Reset** to reset the settings.



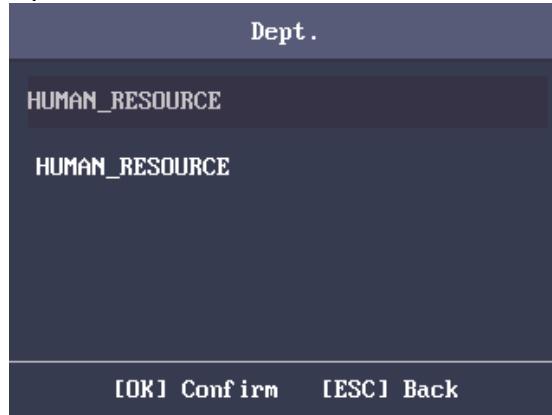
3.5.2 Searching the Department

Purpose:

Search the target department by entering the department name.

Steps:

1. Enter the target department name in the searching bar of the department list interface.
2. Press the OK key to search.



3.5.3 Resetting the Department

Purpose:

Reset all parameters of the target department to the default ones.

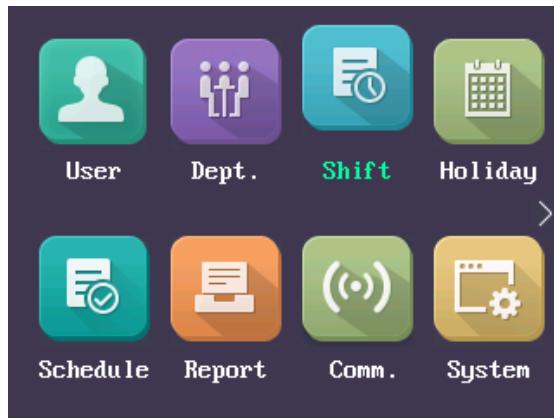


3.6 Shift Management

Purpose:

The normal shift and the man-hour shift are available to be configured. You can set the attendance rule and the attendance checking times in the normal shift. You can also set the working hours per day in the man-hour shift.

The normal shift can be applied to the normal attendance situation, while the man-hour shift can be applied to the situation with flexible working hours.



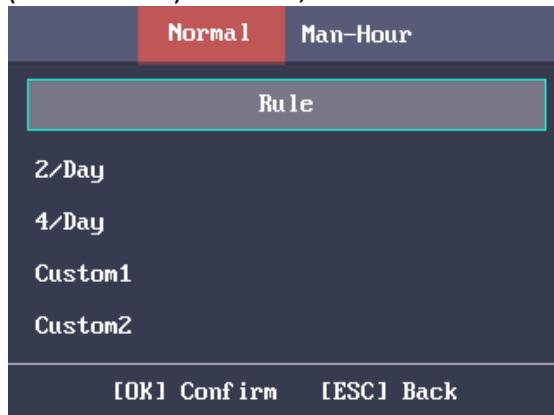
Note: Support up to 32 normal shifts and 32 man-hour shifts.

3.6.1 Normal Shift

Setting the Attendance Rule

Steps:

1. In the Normal (Normal Shift) interface, select **Rule**.



2. Configure the attendance rule.

On-work Advanced Time: The allowable early duration to go to work.

Latest On-Work Check Time: The allowable late duration to go to work.

Absence Time (Late): The late arrival threshold duration.

Off-Work Early Time: The allowable early duration to get off work.

Latest Off-Work Check Time: The allowable late duration to get off work.

Absence Time (Early Leave): The early leave threshold duration.

<p>Rule</p> <p>(Time Range: 0 to 1440 m.)</p> <p>On-Work Advanced Time: <input type="text" value="0"/></p> <p>Latest On-Work Check Time: <input type="text" value="0"/></p> <p>Absence Time (Late): <input type="text" value="0"/></p> <p>Off-Work Early Time: <input type="text" value="0"/></p> <p>[ESC] Back</p>	<p>Rule</p> <p>Latest Off-Work Check Time: <input type="text" value="0"/></p> <p>Absence Time (Early Leave): <input type="text" value="0"/></p> <p>[ESC] Back</p>
--	--

3. Press the ESC key and select **Yes** to save the settings and exit the interface.

Notes:

- Unit: minute.
- The available time range is from 0 to 1440 minutes.

Setting Normal Shift Attendance**Steps:**

1. Select an attendance type in the Normal (Normal Shift) interface.

Notes:

- By default, the normal shift type includes 2/Day (2 times per day), 4/Day (4 times per day), and 30 custom types.
- The following steps will take Custom 1 as an example.

2. Select **Edit** and press the OK key to enter the Edit Shift interface.



3. Edit the shift name, and the period in order.

Edit Shift		Edit Shift	
Shift No.	1	Period 3:	0 : 0 - 0 : 0
Name:	2/Day	Period 4:	0 : 0 - 0 : 0
Period 1:	9 : 30 - 17 : 30		
Period 2:	0 : 0 - 0 : 0		
[ESC] Back		[ESC] Back	

Notes:

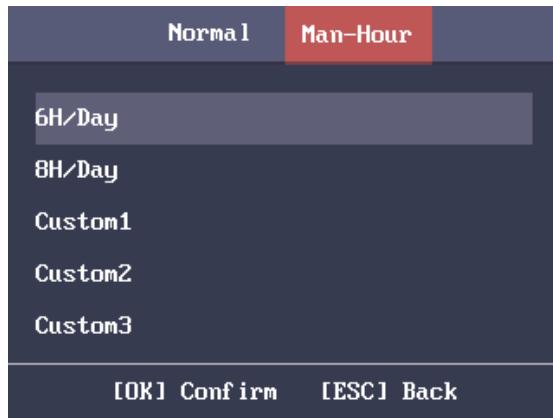
- The shift No. cannot be edited.
- The shift name supports numbers, uppercase letters, lowercase letters, Chinese characters and symbols.
- The shift name supports up to 32 characters.
- Up to 4 time periods can be edited.

You can also select **Reset** to reset the settings.

4. Press the ESC key and select **Yes** to save the settings and exit the interface.

3.6.2 Man-Hour Shift**Steps:**

1. Press the key to enter the Man-Hour interface.



2. Select a man-hour shift type in the list.

Notes:

- By default, the man-hour shift type includes 6H/Day (6 hours per day), 4H/Day (4 hours per day), and 30 custom types.
- The following steps will take Custom 1 as an example.

3. Press the OK key to enter the Man-Hour Shift configuration interface.



4. Select **Edit** to enter the Edit Shift interface.

You can edit the shift name, the shift duration (work duration), the latest time on-work and the break time.

Edit Shift	
Shift No.	1
Name:	6H/Day
Duration:	6 : 0 (H : M)
Latest Time:	10 : 30 (On-Work)
[ESC] Back	
Edit Shift	
Break 1:	12 : 30 - 13 : 30
Break 2:	0 : 0 - 0 : 0
Break 3:	0 : 0 - 0 : 0
[ESC] Back	

Notes:

- The shift No. cannot be edited.
- The break time will not be counted into the working hour.
- If the Latest Time (On-Work) is set to 0, the Latest Time function will not be enabled.

You can also select **Reset** and press the OK key to reset the settings.

- Press the ESC key and select Yes to save the settings and exit the interface.

3.7 Holiday Management

Purpose:

You are able to configure the attendance holiday. The attendance will not be recorded during the holiday.

3.7.1 Adding the Holiday

Steps:

- In the Holiday interface, press the key to enter the New (New Holiday) interface.

Holiday	New
No. :	<u>2</u>
Name :	
Start :	<u>2016</u> Y <u>1</u> M <u>1</u> D
End :	<u>2016</u> Y <u>1</u> M <u>3</u> D
[ESC] Back	

- Enter the holiday No., the holiday name, the holiday start time and the end time.
- Press the ESC key and select Yes to save the settings and exit the interface. The new holiday will be displayed in the Holiday list.

Holiday	New
Enter the holiday name, press OK .	
<u>National_Day</u>	
[OK] Confirm	[ESC] Back

3.7.2 Searching the Holiday

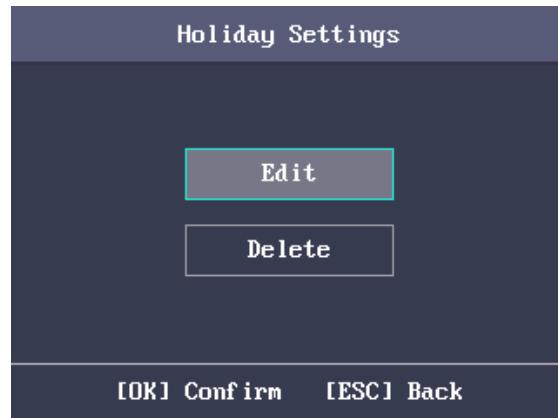
Steps:

- In the Holiday List interface, enter the target holiday name.
- Press the OK key to search.

3.7.3 Editing and Deleting the Holiday

Steps:

- Select a target holiday in the Holiday List interface to enter the Holiday Settings interface.

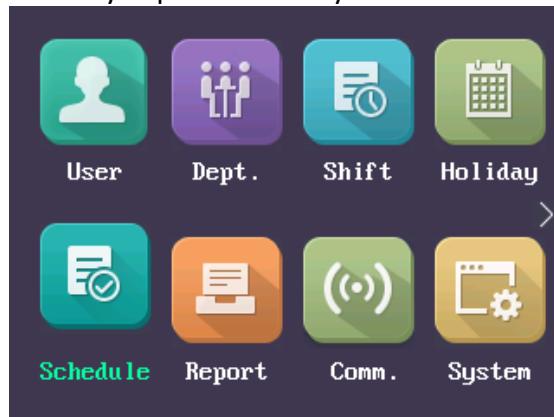


2. Select **Edit** and follow the steps in *Section 3.7.1 Adding the Holiday* to edit the holiday information.
Or select **Delete** and press the OK key to delete the holiday.
3. Press the ESC key and select **Yes** to save the settings and exit the interface.

3.8 Shift Schedule Management

Purpose:

Configure the shift schedule by department or by individual.



3.8.1 Scheduling Shift by Department

Before you start:

1. Edit the department. For detailed information, see *Section 3.5 Department Management*.
2. Configure the normal shift or the man-hour shift. For detailed information, see *Section 3.6 Shift Management*.

Steps:

1. Select a target department in the By Dept. (Schedule by Department) interface.

By Dept.	By Indiv.
Company	2/Day
Department	2/Day
Custom1	2/Day
Custom2	2/Day
Custom3	2/Day
[OK] Confirm	[ESC] Back

2. Press the OK key to enter the Schedule Shift by Dept. interface.

<p style="text-align: center;">Schedule Shift by Dept.</p> <p>Dept. Name: Company</p> <p>Set Shift: Set Shift</p> <p>Start: 2000 Y 1 M 1 D</p> <p>End: 2037 Y 12 M 31 D</p> <p style="text-align: center;">[OK] Confirm [ESC] Back</p>	<p style="text-align: center;">Schedule Shift by Dept.</p> <p>Add Holiday: Select Holiday</p> <p style="text-align: center;">[OK] Confirm [ESC] Back</p>
---	---

3. Move the cursor to **Set Shift** and press the OK key to enter the Set Shift interface.

1) Select the shift type and the shift times.

<p style="text-align: center;">Set Shift</p> <p>Mon.: < Normal > < 2/Day ></p> <p>Tue.: < Normal > < 2/Day ></p> <p>Wed.: < Normal > < 2/Day ></p> <p>Thu.: < Normal > < 2/Day ></p> <p>Fri.: < Normal > < 2/Day ></p> <p style="text-align: center;">[OK] Confirm [ESC] Back</p>	<p style="text-align: center;">Set Shift</p> <p>Sat.: < Normal > < 2/Day ></p> <p>Sun.: < Normal > < 2/Day ></p> <p style="text-align: center;">[OK] Confirm [ESC] Back</p>
---	---

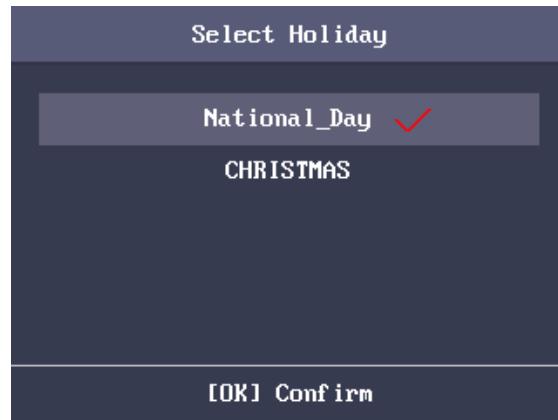
Notes:

- You can set the shift from Monday to Sunday.
- The shift types include None, Normal, and Man-Hour.

2) Press the ESC key and select Yes to save the settings and exit the interface.

4. Set the schedule start time and the end time.

5. Move the cursor to **Select Holiday** and press the OK key.



- 1) Select a target holiday.
- 2) Press the ESC key and select **Yes** to save the settings and exit the interface.
Notes: The attendance will not be recorded during the holiday.
6. Press the ESC key and select **Yes** to save the settings and exit the interface.
Note: The department name cannot be edited.

3.8.2 Scheduling Shift by Individual

Up to 32 individual shifts can be added.

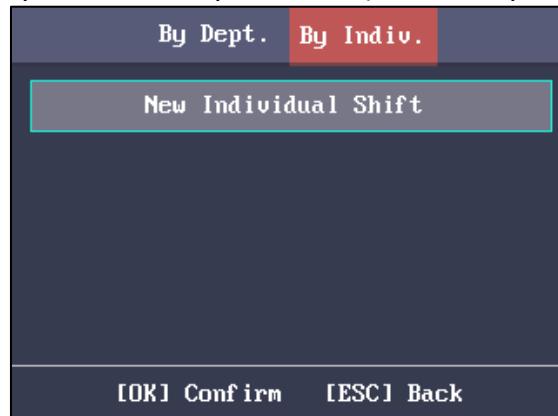
Adding New Individual Shift

Before you start:

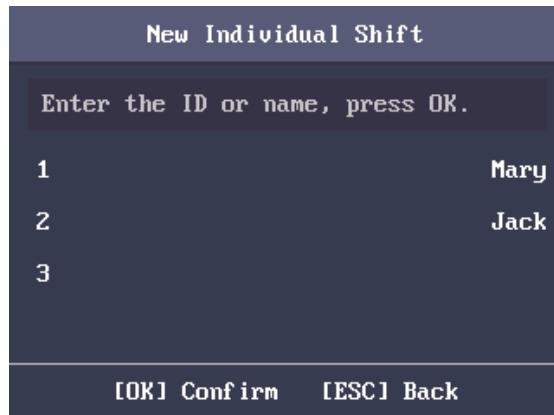
1. Add the user. For detailed information, see *Section 3.4 User Management*.
2. Configure the normal shift or the man-hour shift. For detailed information, see *Section 3.6 Shift Management*.

Steps:

1. Press the ▶ key to enter the By Individual (Schedule by Individual) interface.



2. Select **New Individual Shift** and press the OK key to enter New Individual Shift interface.



3. Select an individual in the list and press the OK key to enter the Individual Shift Settings interface.

Individual Shift Settings		Schedule Shift by Dept.	
ID:	1	Add Holiday:	Select Holiday
Set Shift:	Set Shift		
Start:	2000 Y 1 M 1 D		
End:	2037 Y 12 M 31 D		
[OK] Confirm [ESC] Back		[OK] Confirm [ESC] Back	

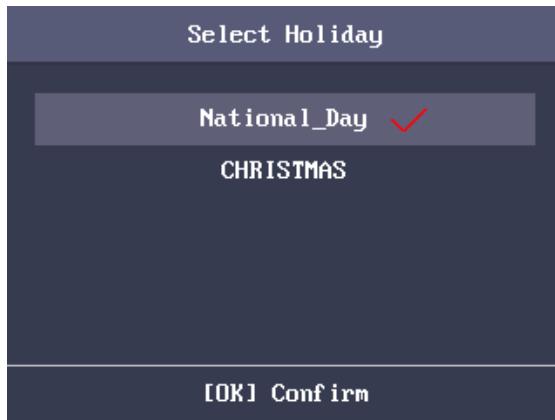
4. Move the cursor to **Set Shift** and press the OK key to enter the Set Shift interface.
- 1) Select the shift types and the shift times.

Set Shift		Set Shift	
Mon.: < Normal > < 2/Day >		Sat.: < Normal > < 2/Day >	
Tue.: < Normal > < 2/Day >		Sun.: < Normal > < 2/Day >	
Wed.: < Normal > < 2/Day >			
Thu.: < Normal > < 2/Day >			
Fri.: < Normal > < 2/Day >			
[OK] Confirm [ESC] Back		[OK] Confirm [ESC] Back	

Notes:

- You can set the shift from Monday to Sunday.
- The shift types include None, Normal, and Man-Hour.

- 2) Press the ESC key and select **Yes** to save the settings and exit the interface.
5. Set the start time and the end time in the Individual Shift Settings interface.
6. Select **Select Holiday** and press the OK key to enter the Select Holiday interface.



- 1) Select a target holiday.
- 2) Press the ESC key and select **Yes** to save the settings and exit the interface.
Note: The attendance will not be recorded during the holiday.

7. Press the ESC key and press the OK key to save the settings and exit the interface.

Editing and Deleting Individual Shift

Steps:

1. Select an individual shift in the By Individual (Schedule by Individual) interface.
2. Select **Edit** and press the OK key to enter the Individual Shift Settings interface.
Follow *Adding New Individual Shift* in *Section 3.8.2 Scheduling Shift by Individual* to edit the shift.

Or select **Delete** to delete the selected individual shift.

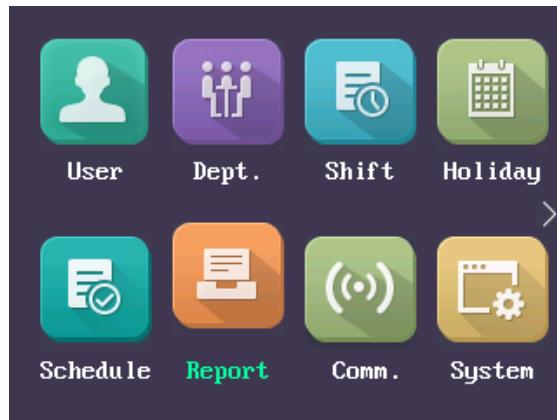


3.9 Other Management

3.9.1 Report Management

Purpose:

You are able to export the attendance report, the attendance report, the abnormal attendance record and the attendance management schedule.

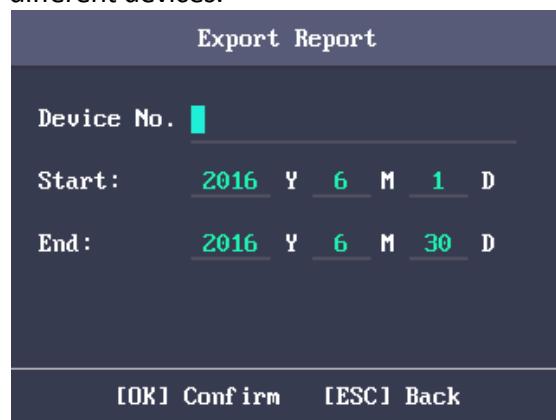


Steps:

1. Insert a USB disk to the USB interface.
Note: The device will automatically check the USB disk memory. If there is no enough space for exporting, a prompt will be displayed.
1. Select **Attendance Record/Attendance Report/Abnormal Attendance Record** in the Report interface.



2. Edit the device No. the start time and the end time in the Export Report interface
Note: You should customize the device No. The device No. is for differentiating the reports of different devices.



Or select **Attendance Management Schedule** in the Report Management interface to export the Shift Settings Table, the Normal Shift Schedule table and the Man-Hour Shift Schedule table directly.

3. Press the OK key to export. The exported file will be saved in the USB disk in Excel format.

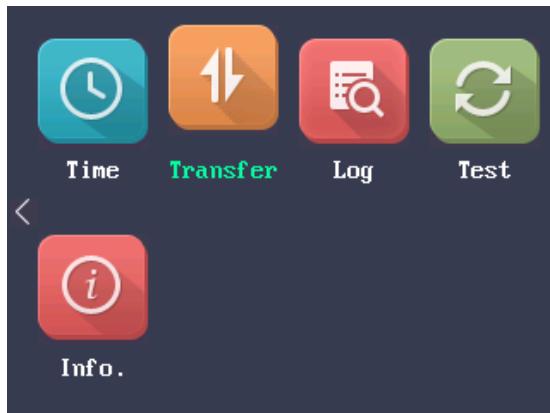
Notes:

- Support the USB disk of FAT32 format.
- The USB disk memory should be from 1G to 32G. Make sure the free space of the USB disk is more than 512M.
- For details about the exported tables descriptions, see *Section 5.4 Attendance Report Table*.

3.9.2 Data Transfer

Purpose:

You can export the attendance parameters and the attendance data. You can also import the attendance parameters from the USB disk.



Exporting Parameters and Data

Steps:

1. Insert the USB disk to the USB interface.
Note: The device will automatically check the USB disk memory. If there is no enough space for exporting, a prompt will be displayed.
2. In the Export interface, select **Export Attendance Para** (Export Attendance Parameters) or **Export Attendance Data**.



3. Press the OK key, the attendance parameters or the attendance data will be saved in the USB disk.

Notes:

- When the USB disk is full, the device will pop up a prompt. You have to change another one to continuing exporting.
- Support the USB disk of FAT32 format.
- The USB disk memory should be from 1G to 32G.

Importing Attendance Parameters

Steps:

1. Insert the USB disk to the USB interface.
2. Press the  key to enter the Import interface and select **Import Attendance Para** (Import Attendance Parameters).



3. Press the OK key to import.

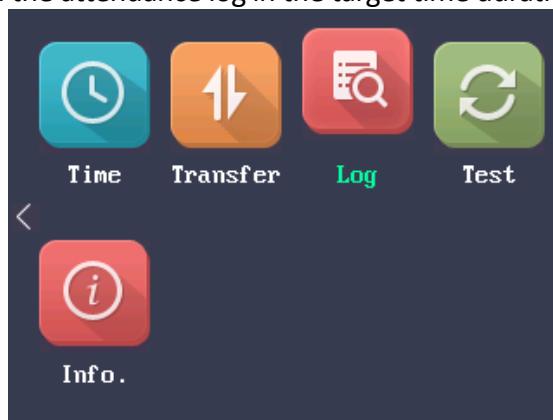
Notes:

- Support the USB disk of FAT32 format.
- The file for importing should be in the root directory.

3.9.3 Searching the Log

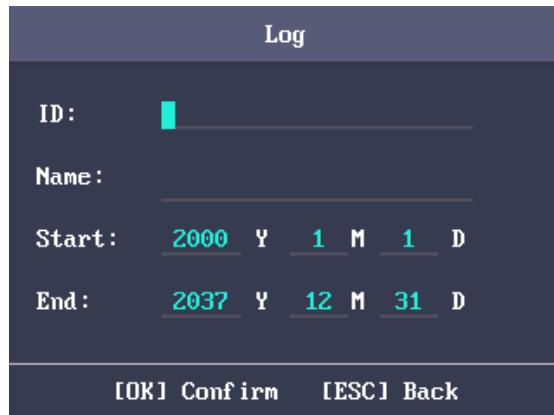
Purpose:

You are able to search the attendance log in the target time duration of the target ID No.



Steps:

1. Enter the ID No. in the Log (Log Search) interface.
2. Move the cursor the Name, the corresponding name will be displayed automatically.
Or enter the name and move the cursor to the ID No., the corresponding ID No. will be displayed automatically.



3. Enter the target log start time and the end time.
4. Press the OK key to search. The interface will display the log search result.

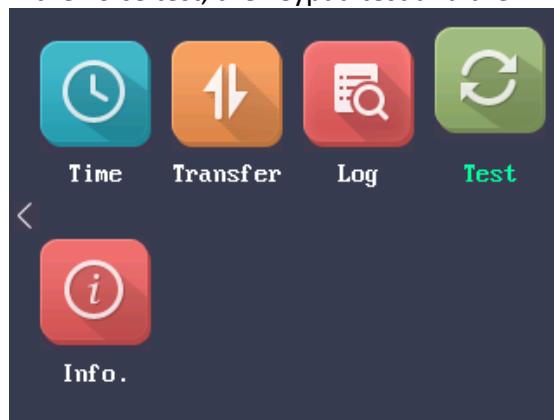
ID:	Time:	Reader ID:
1	2016-07-18-16-11	1

[ESC] Back

3.9.4 Testing

Purpose:

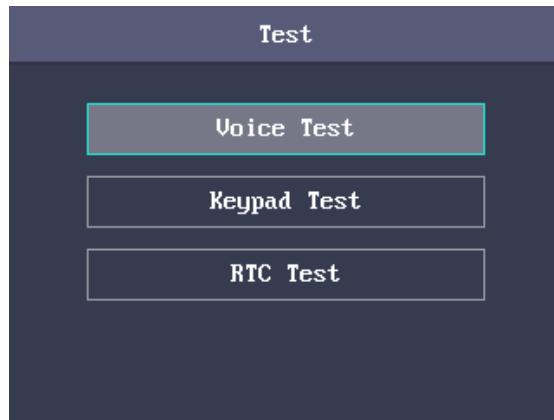
You are able to perform the voice test, the keypad test and the RTC test.



Voice Test

Steps:

1. Select **Voice Test** in the Test interface.



2. Press the OK key. If the device voice is working properly, you are able to hear "Voice Test Success".

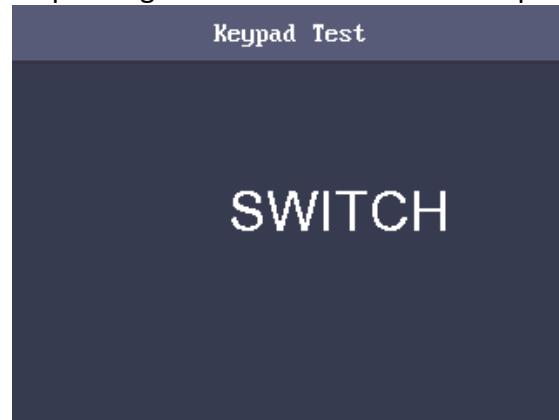
Keypad Test

Steps:

1. Select **Keypad Test** in the Test interface.



2. Press the OK button to start testing. If the keypad test succeeds, the screen will display the corresponding numbers or functions of the pressed key.



RTC Test

Steps:

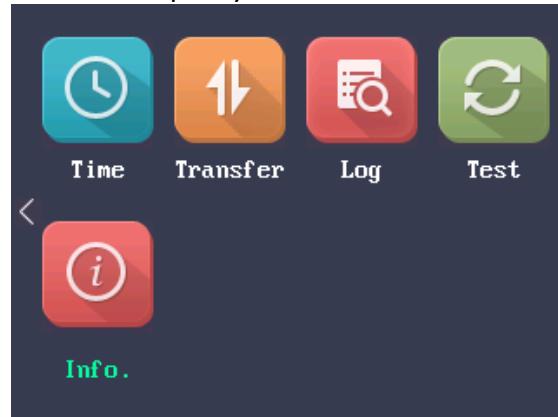
1. Select **RTC Test** in the Test interface.



2. Press the OK key to enter the RTC Test interface. If the test succeeds, the screen will display the synchronization time.

3.9.5 System Information

You are able to check the device capacity and the device information.



Checking the Capacity

Check the user capacity and the fingerprint capacity in the device.



User Capacity: The maximum user amount that can be configured.

Note: The default maximum user amount is 3,000.

Fingerprint Capacity: The maximum fingerprint amount.

Note: The default maximum fingerprint amount is 3,000.

Checking the Device Information

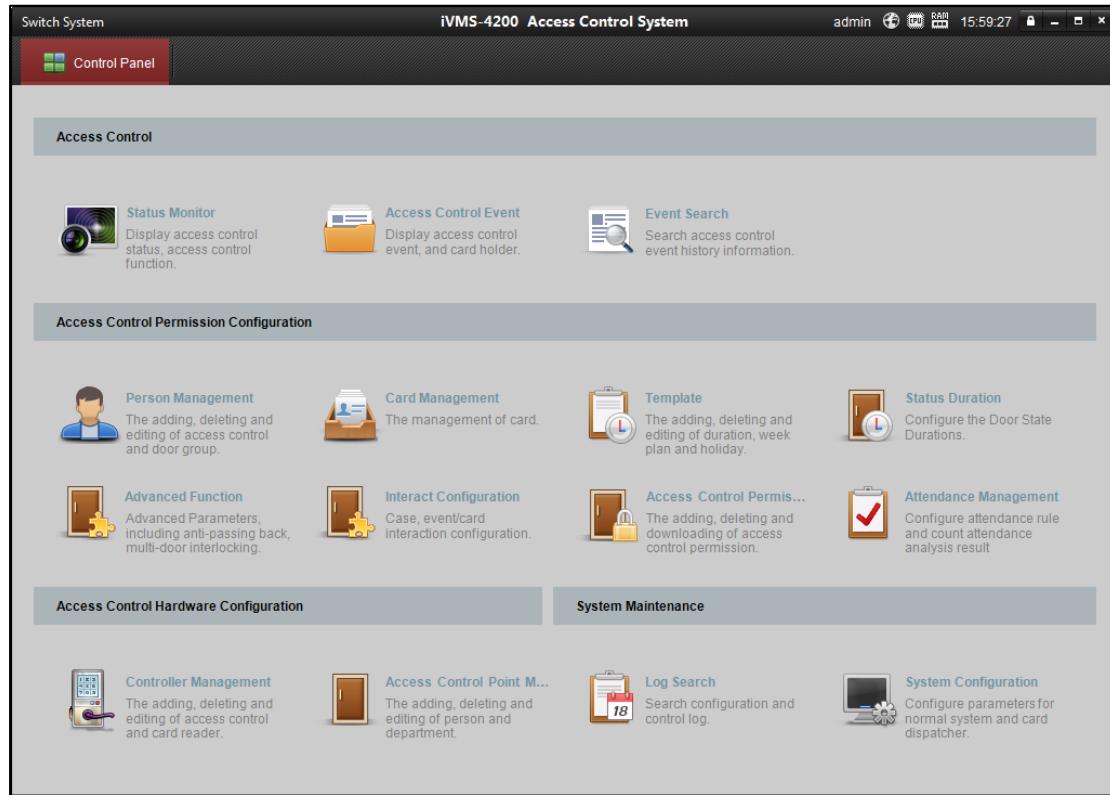
In the Device interface, you are able to check the device name, the device serial No., the MAC address, the firmware, the hardware and the production data.

Capacity	Device
Device Name:	T&A Controller
Serial No.:	[REDACTED]
MAC Address:	[REDACTED]
Firmware:	V1.0.0 [REDACTED]
Hardware:	[REDACTED]
Production Date:	[REDACTED]

Chapter 4 Client Operation

4.1 Overview of Access Control System

Click Switch **System-> Access Control System** on the menu bar to enter the Access Control System.



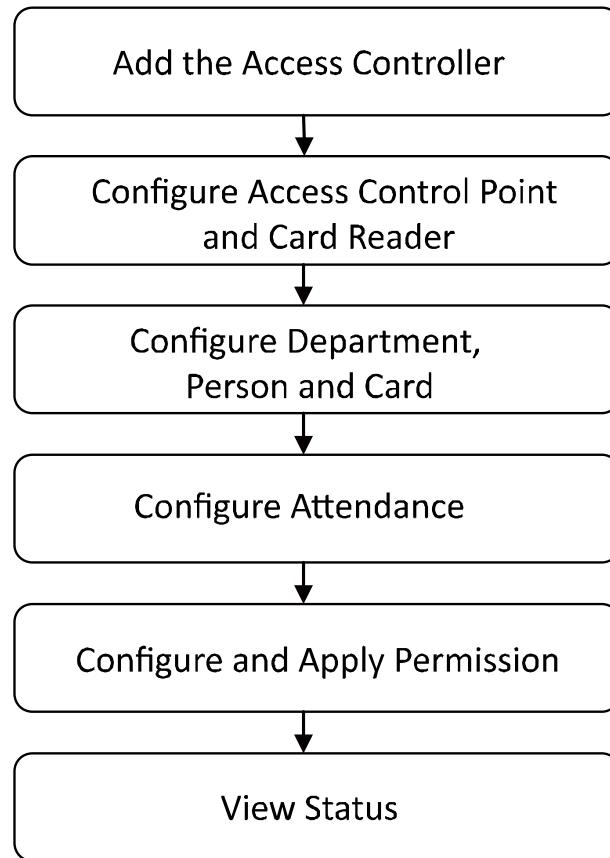
4.1.1 Description

The Access Control System is a client of configuring permission of door access. It provides multiple functionalities, including access controller management, person/card management, permission configuration, door status management, attendance management, event search, etc.

This user manual describes the function, configuration and operation steps of Access Control Client. To ensure the properness of usage and stability of the client, please refer to the contents below and read the manual carefully before installation and operation.

4.1.2 Configuration Flow

Refer to the following flow chart for the configuration order.



4.2 Device Management

4.2.1 Controller Management

Click the  icon to enter the controller management interface.

The screenshot shows the 'Controller Management' interface. At the top, there is a header with buttons for 'Add Device', 'Edit', 'Delete', 'Bulk Time Adj...', 'Status', 'Remote Config...', 'Refresh', and 'Filter'. Below this is a table titled 'Device Managed (1)' with one row:

Name	Type	Connection Mode	IP	Port	Baud Rate	Dial-up	Connection Status	Refresh
123	Access Controller_DS-K1T200E...	TCP/IP	10.17.138.232	80...	1	Online		

At the bottom, there is another section titled 'Online Devices (0)' with buttons for 'Add to Client', 'Add All Device', 'Edit Network...', 'Reset P...', 'Activate', 'Refresh', and 'Filter'. This section also contains a table with columns for Name, Type, IP, Port, Activated, and Added.

The interface is divided into 2 parts: device management and online device detection.

Device Management:

Manage the access control devices, including adding, editing, deleting, and batch time synchronizing functions.

Online Device Detection:

Automatically detect online devices in the same subnet with the access control server, and the detected devices can be added to the server in an easy way.

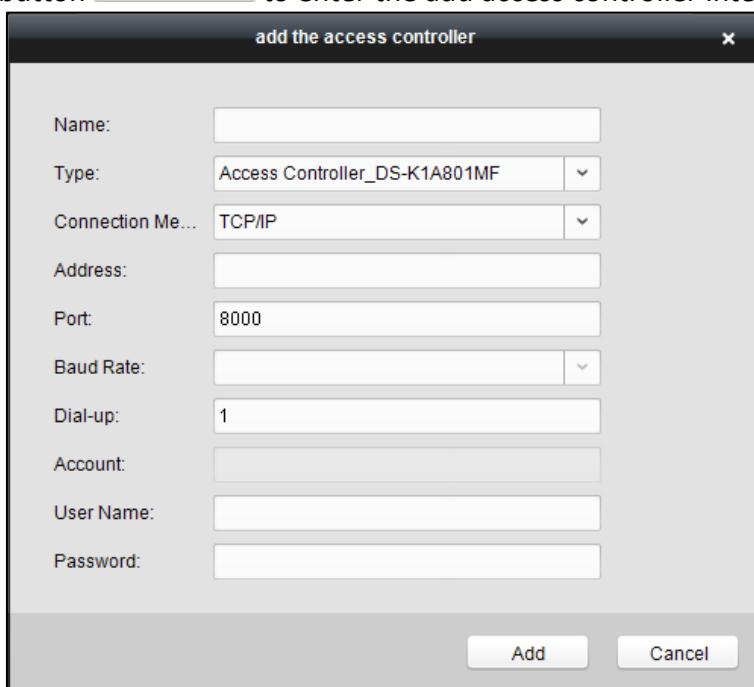
Note: The control client can manage 16 access controllers at most.

Device Management

Adding Controller

Steps:

1. Click the button  **Add Device** to enter the add access controller interface.



2. Input the device name.
 3. Select the access controller type in the dropdown list.
 4. Select the connection mode in the dropdown list: TCP/IP, or COM port.
TCP/IP: Connect the device via the network.
 5. Set the parameters of connecting the device.
If you choose to connect the device via network, you should input the IP address and port No. of the device, and set the Dial-up value to 1.
 6. Click the  **Add** button to finish adding.
- You can click **Status** to check the detailed status of the controller, and click **Remote Configuration** to configure the settings of the controller.

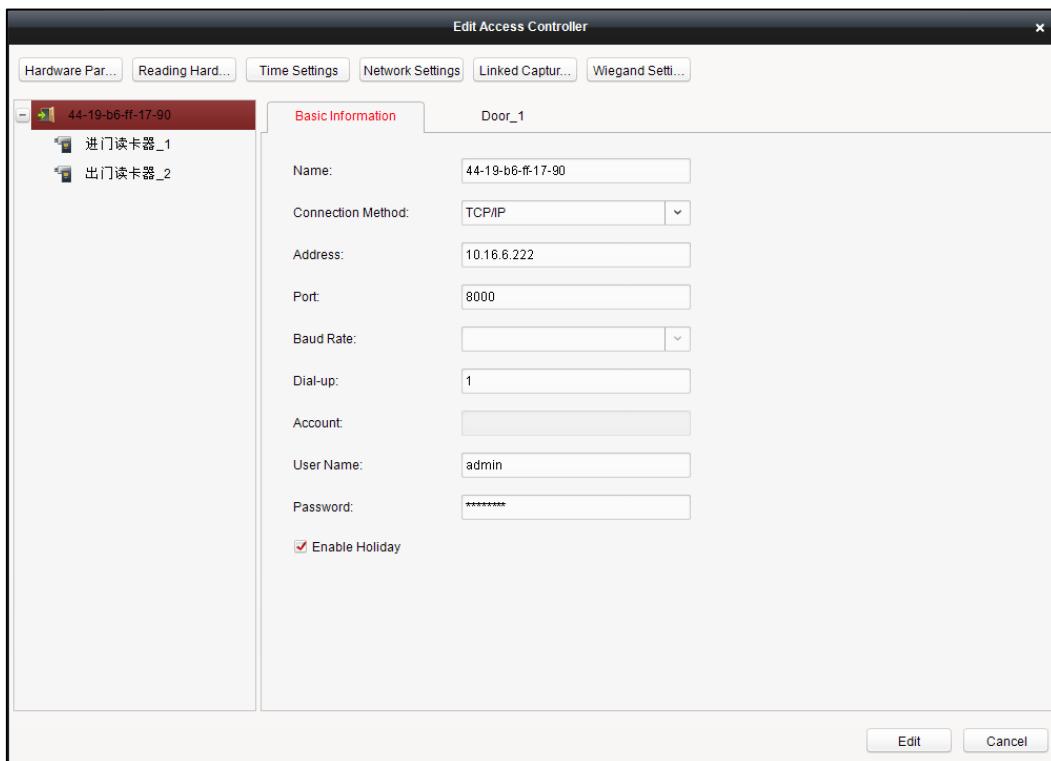
Editing Device (Basic Information)

Purpose:

After adding the device, some advanced parameters can be configured in the editing device interface, e.g. downloading hardware parameters, reading hardware parameters, time synchronizing, configuring access point, etc.

Steps:

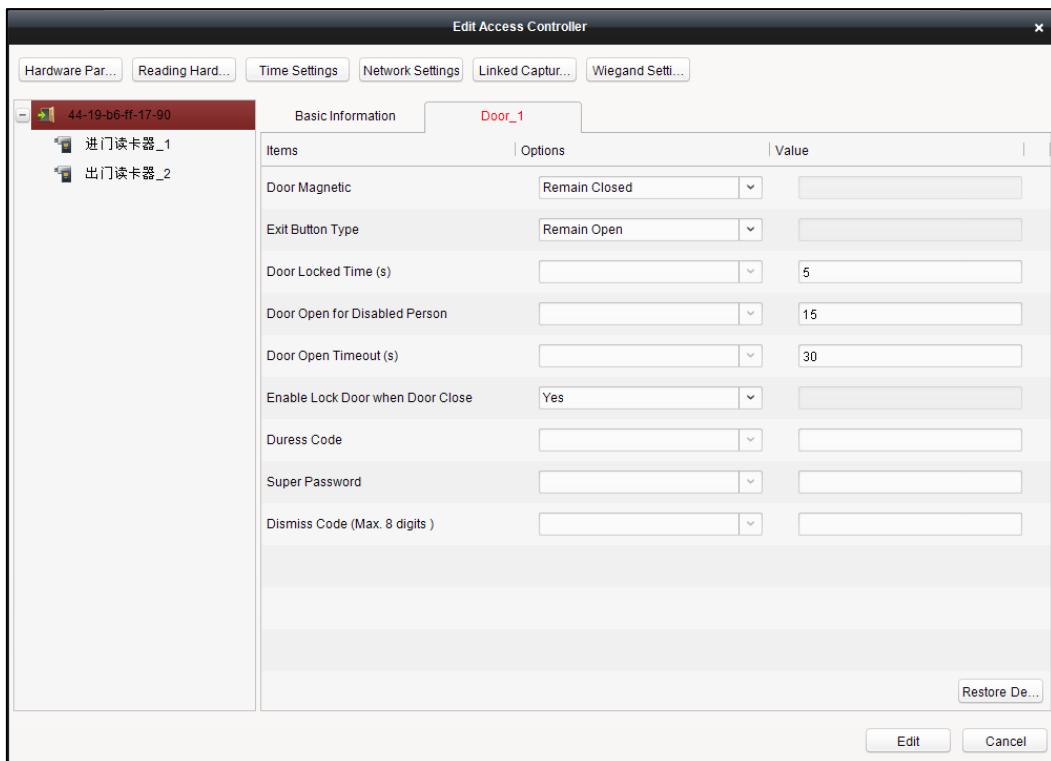
1. In the device list, click **Edit** button to edit the information of the selected added device.



2. Edit the basic parameters of the device on your demand, which are the same as the ones when adding the device.
3. (Optional) Check the checkbox of **Enable Holiday** to enable the holiday parameters when downloading permissions.
4. Click the **Edit** button to finish editing.
5. Click the **Hardware Parameters Downloading** button to download the updated parameters to the local memory of the device.

Note: Capture function is not supported.

Editing Device (Door Information)

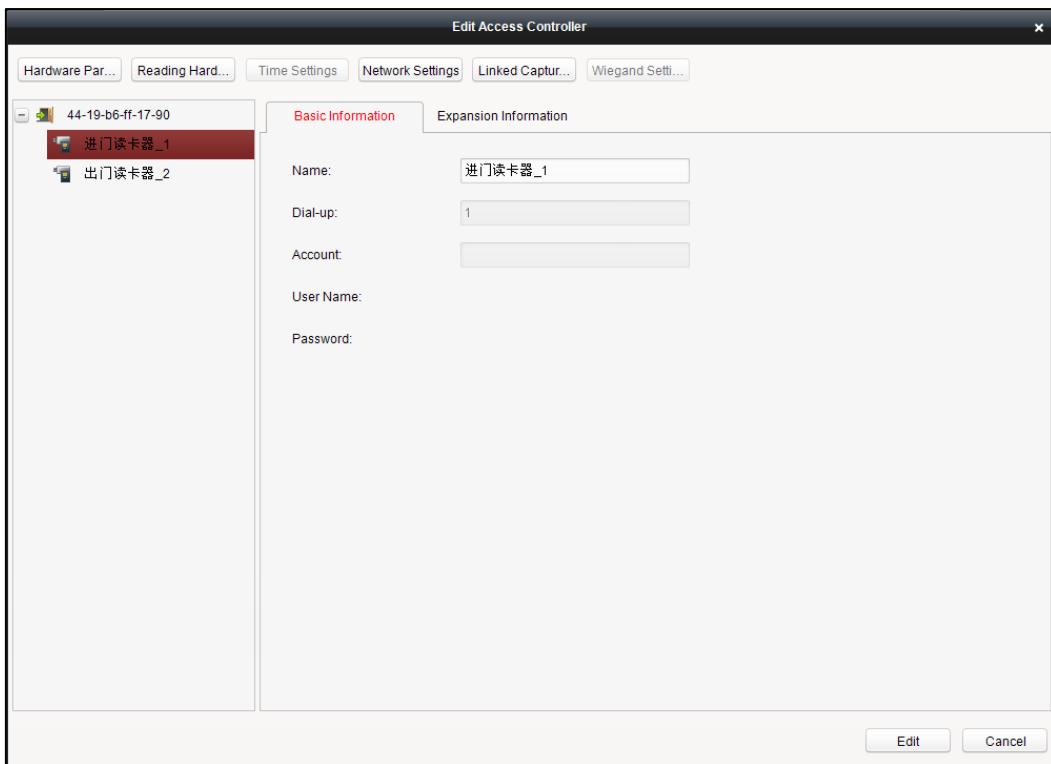


Steps:

- In the editing interface, click the **Door_1** button to edit the information of the selected door.
 - Door Magnetic:** The Door Magnetic is in the status of **Remain Closed** (excluding special conditions).
 - Exit Button Type:** The Exit Button Type is in the status of **Remain Open** (excluding special conditions).
 - Door Locked Time(s):** After swiping the normal card and relay action, the timer for locking the door starts working.
 - Door Open for Disabled Person:** The door magnetic can be enabled with appropriate delay after disabled person swipes the card.
 - Door Open Timeout(s):** The alarm can be triggered if the door has not been closed.
 - Enable Lock Door when Door Close:** This function has not been supported yet.
 - Duress Code:** The door can open by inputting the duress code when there is a duress. At the same time, the access system can report the duress event.
 - Super Password:** The specific person can open the door by inputting the super password.
- Click the **Restore Default Value** to restore all parameters into default settings.
- Click the **Edit** button to save parameters.
- Click the **Hardware Parameters Downloading** button to download the updated parameters to the local memory of the device.

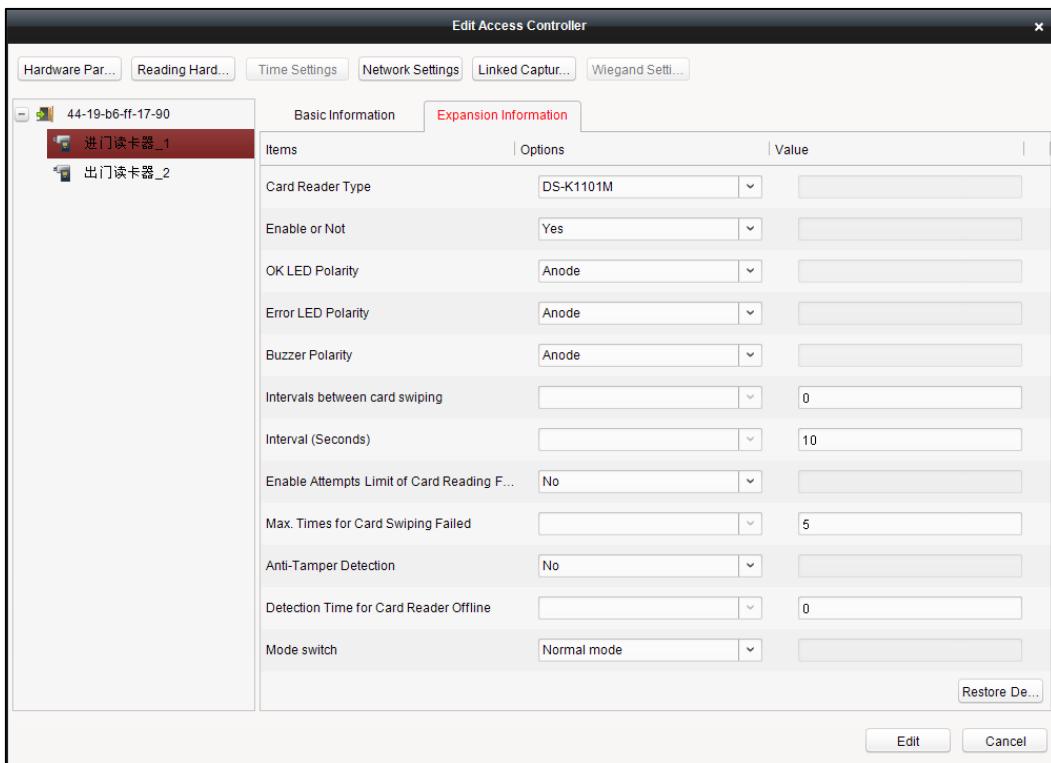
Note: The attendance device does not support the function.

Editing Device (Card Reader Information)



Steps:

1. In the device list, select a card reader name to enter into the card reader information editing interface.
2. Click the **Basic Information** button to edit the basic information about the card reader.
3. Click the **Expansion Information** button to edit the expansion information about the card reader.



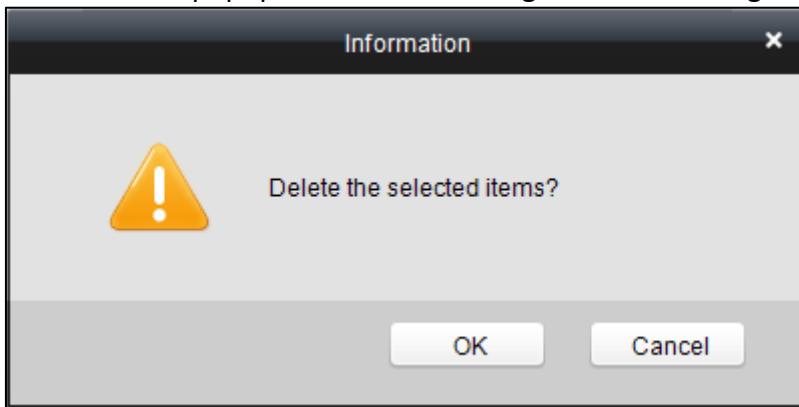
4. Click the **Edit** button to save parameters.

5. Click the **Hardware Parameters Downloading** button to download the updated parameters to the local memory of the device.

Deleting Device

Steps:

1. In the device list, select a device by clicking it, or select multiple devices by pressing Ctrl button on your keyboard and clicking them one by one.
2. Click the  button to delete the selected device(s).
3. Click **OK** button in the popup confirmation dialog to finish deleting.



Bulk Time synchronization

Steps:

1. In the device list, select a device by clicking it, or select multiple devices by pressing Ctrl button on your keyboard and clicking them one by one.
2. Click the **Bulk Time Adjustment** button to start time synchronization.
A message box will pop up on the lower-right corner of the screen when the time synchronization is completed.

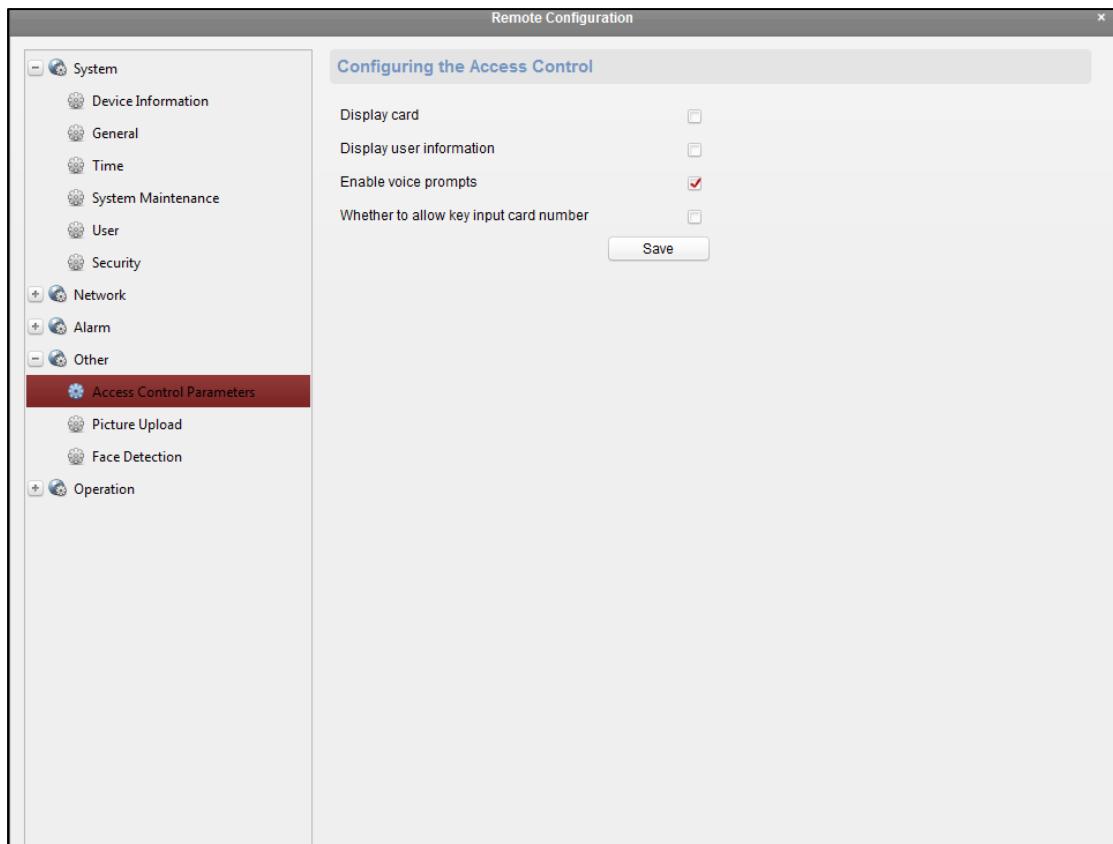
Status

In the device list, you can click **Status** button to enter view the status.

- 1) **Door Status:** The status of the connected door.
- 2) **Host Status:** The status of the host, including Storage Battery Power Voltage, Device Power Supply Status, Multi-door Interlocking Status, Anti-passing Back Status, Host Anti-Tamper Status.
- 3) **Card Reader Status:** The status of card reader.
- 4) **Alarm Input Status:** The alarm input status of each port.
- 5) **Alarm Output Status:** The alarm output status of each port.
- 6) **Event Sensor Status:** The event status of each port.

Remote Configuration

In the device list, you can click **Remote Configuration** button to enter the remote configuration interface. You are able to configure the voice prompt function.



Attendance Configuration

Purpose:

You are able to remotely configure the device shift, holiday and shift schedule.

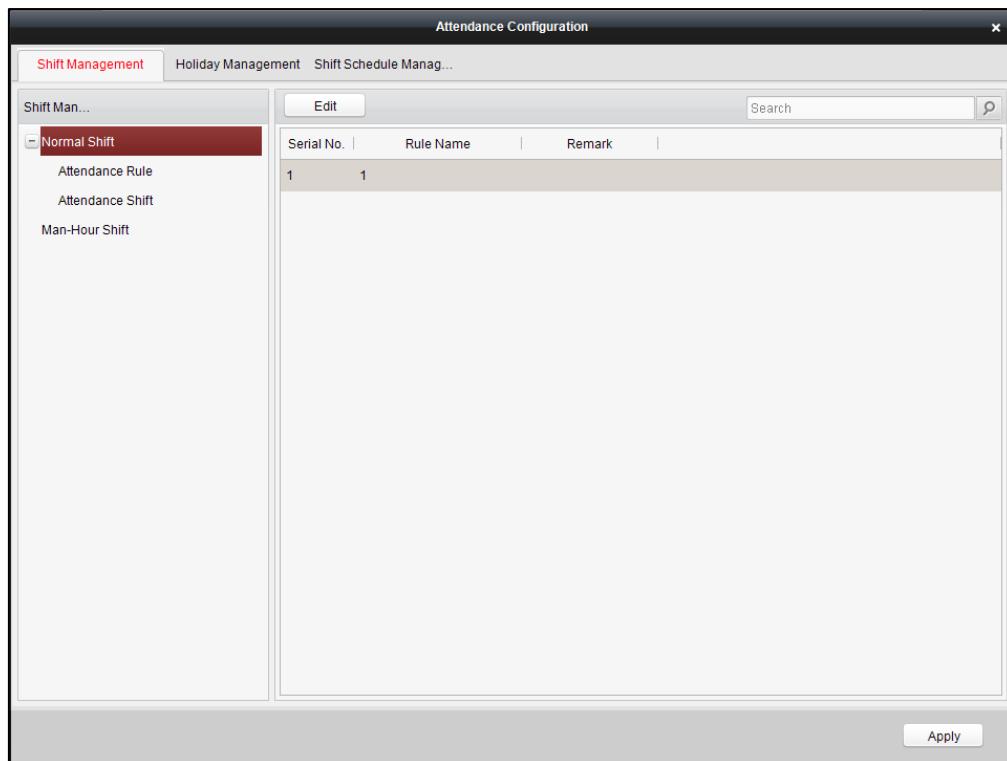
- **Shift Management**

You are able to add, delete and edit the shift.

1) Editing Normal Shift

Steps:

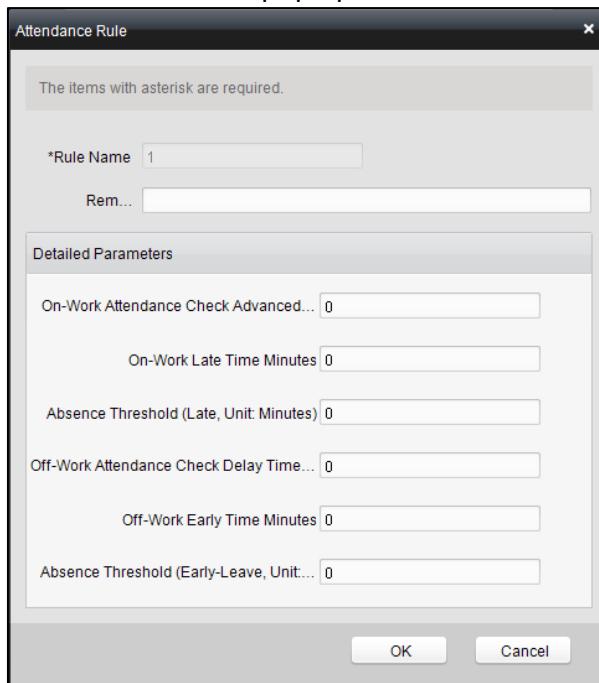
1. Click the Shift Group tab to enter the following page.



2. Click **Attendance Rule** in the Shift Management List, and click the attendance rule on the right of the interface.

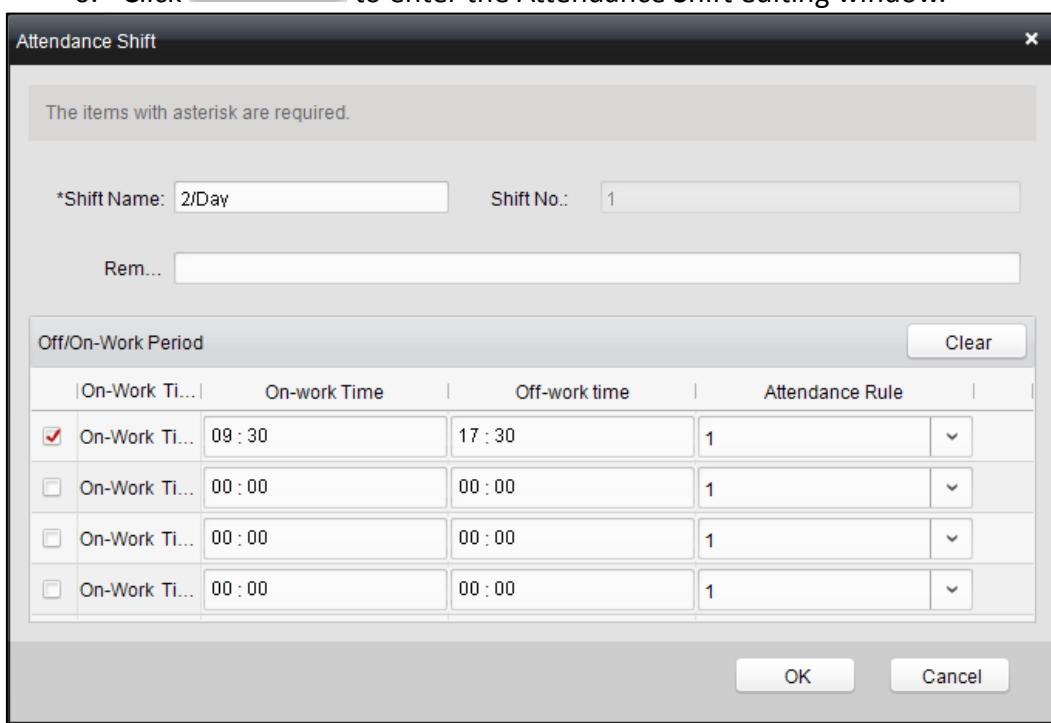
Note: There is one default attendance rule.

3. Click **Edit** button to pop up the Attendance Rule window.



4. Configure the parameters and click the **OK** button to confirm editing.
5. Click Attendance Shift in the Shift Management list and select a shift on the right side of the interface.

6. Click **Edit** to enter the Attendance Shift editing window.



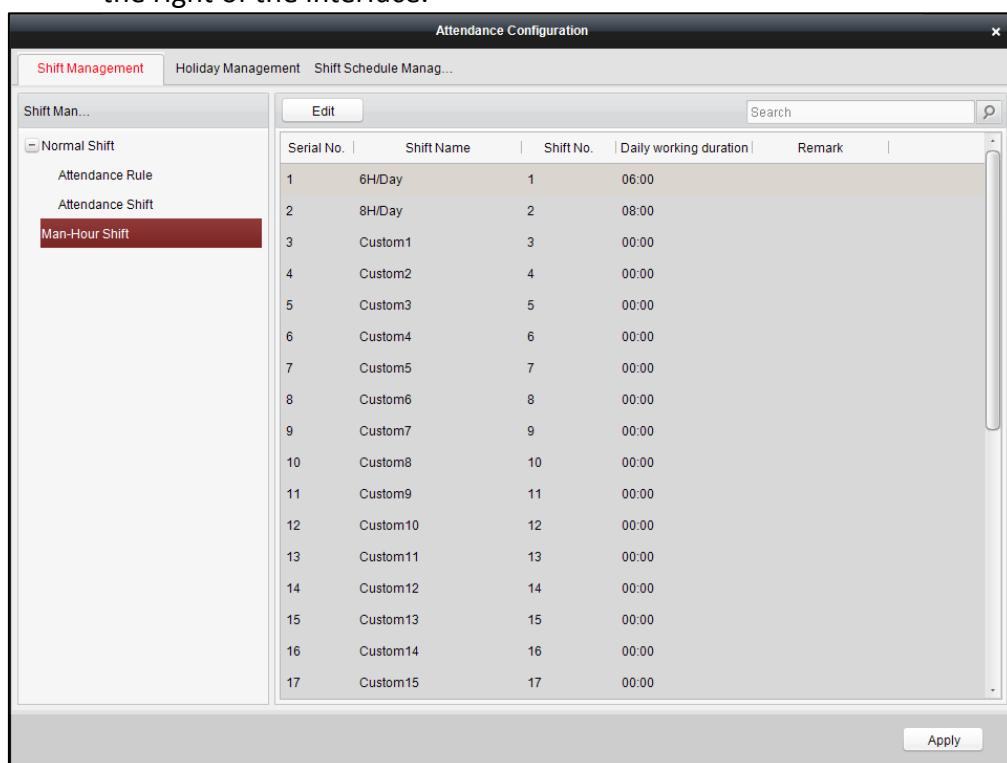
7. Configure the parameters in the window and click **OK** to confirm editing.

8. Click **Apply** to apply the parameters to the device.

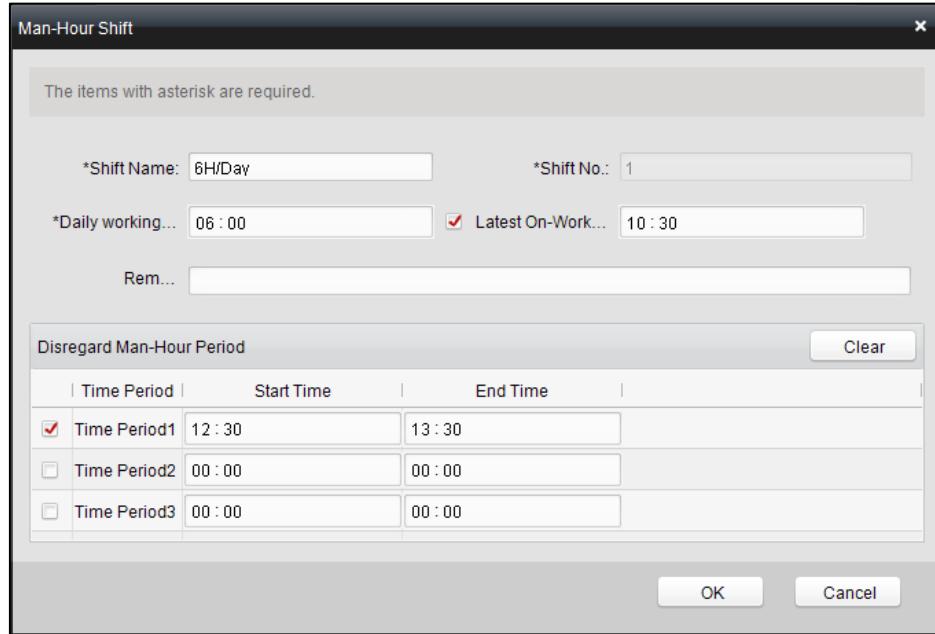
2) Editing Man-Hour Shift

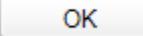
Steps:

1. Click "Man-Hour Shift" in the Shift Management List and click a shift on the right of the interface.



2. Click .
3. Configure the man-hour shift parameters in the pop-up window.

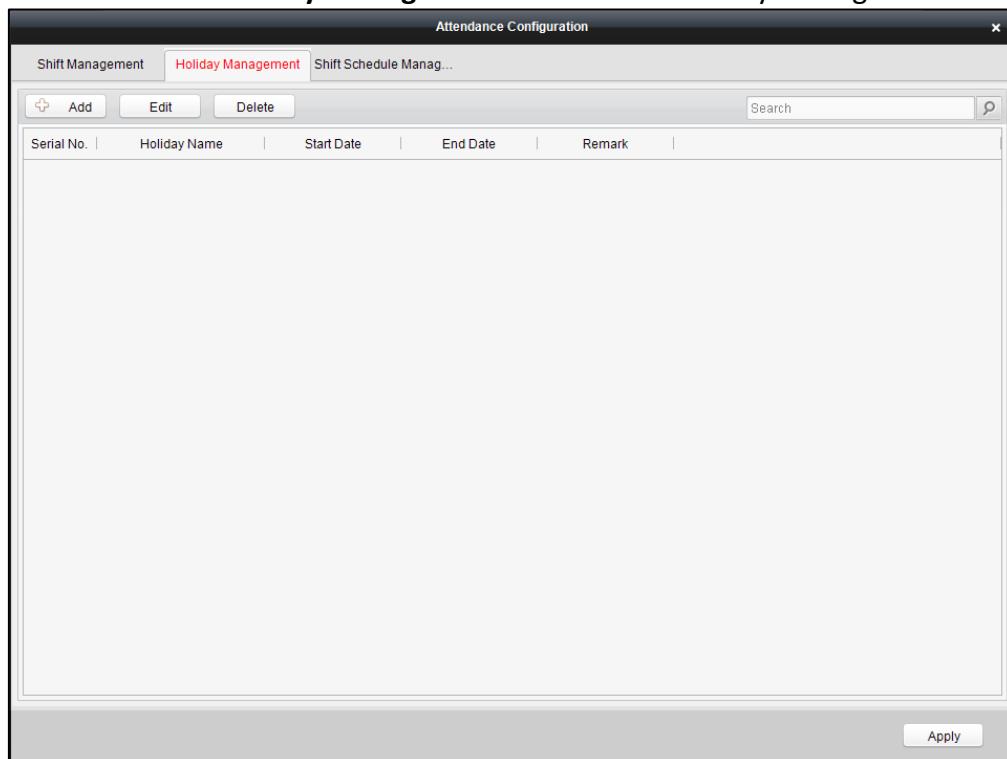


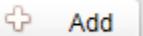
4. Click  to confirm editing.

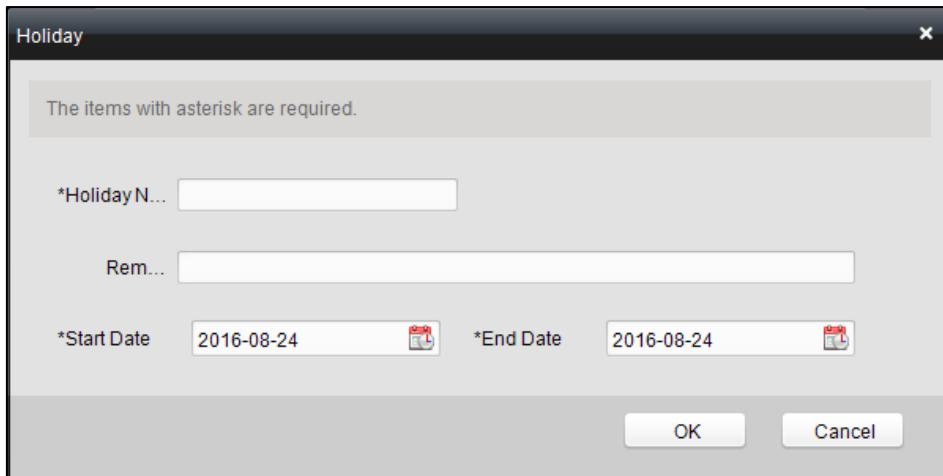
- **Holiday Management**

Steps:

1. Click **Holiday Management** to enter the Holiday Management tab.



2. Click  to enter the Holiday management window.
3. Edit the holiday name, the holiday start time and the end time.



4. Click **OK** to add the holiday.
5. Click **Apply** to apply the parameters to the device.
Or select a holiday in the holiday list and click **Edit** to edit the holiday.
Or select a holiday and click **Delete** to delete the holiday.

- **Shift Schedule Management**

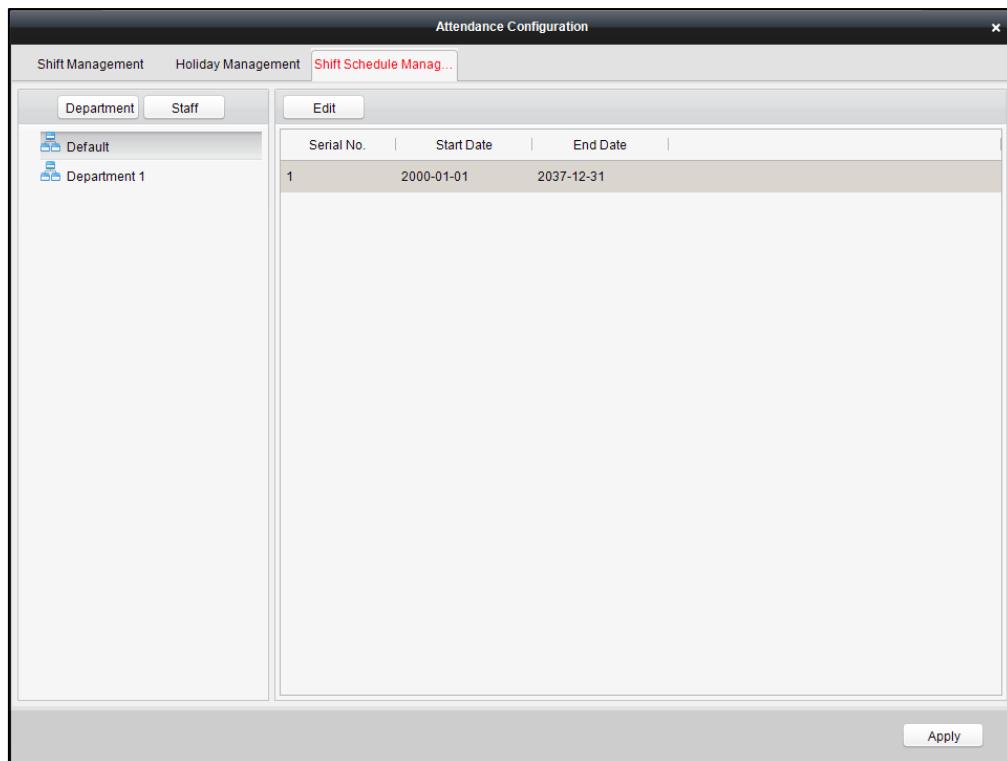
Schedule by Department

Before you start:

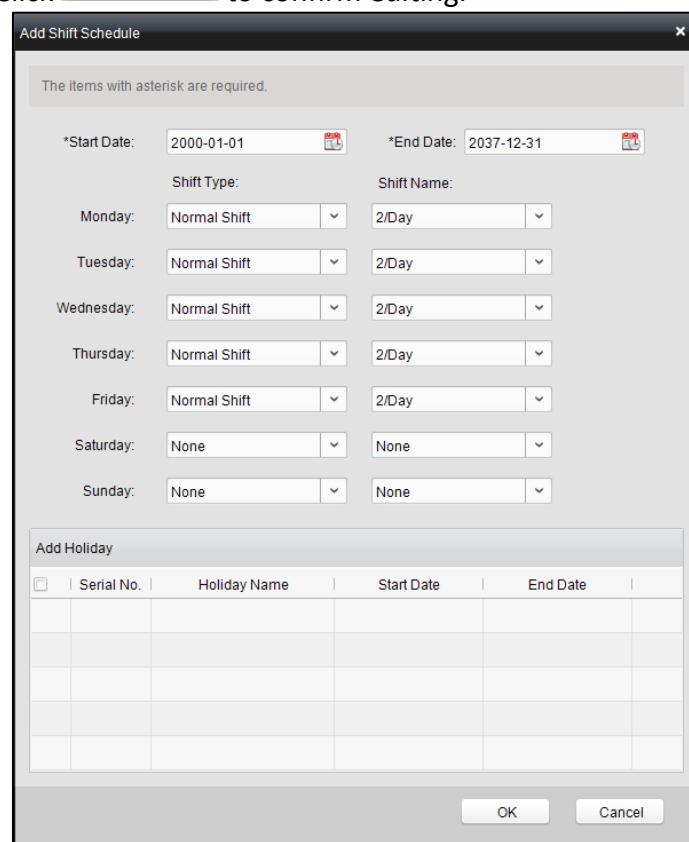
Add department before manage the shift schedule. For details, see *Section 4.3.1 Person Management*.

Steps:

1. Click Shift Schedule Management to enter the Shift Schedule Management tab and click **Department**.



2. Select a department in the department list and click the default shift on the right of the interface.
3. Click **Edit** and configure the shift schedule parameters in the pop-up window.
4. Click **OK** to confirm editing.



5. Click  **Apply**, and apply permissions in the permission management to apply configurations to the device. For details, see *Section 4.3 Permission Management*.

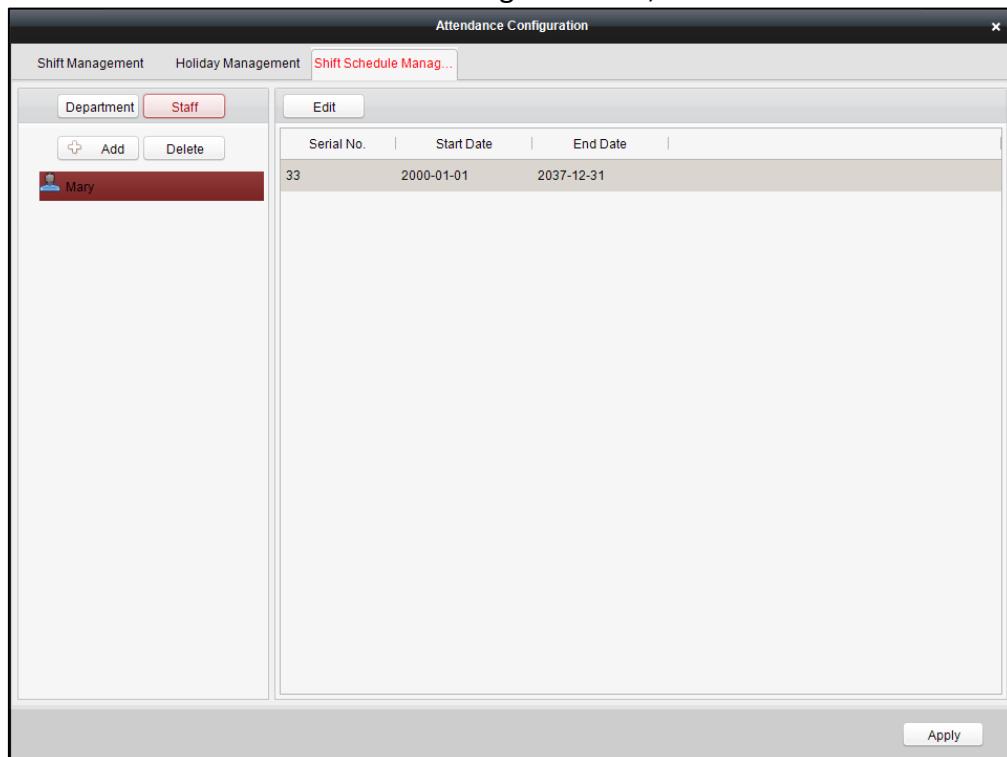
Schedule by Person

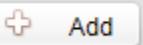
Before you start:

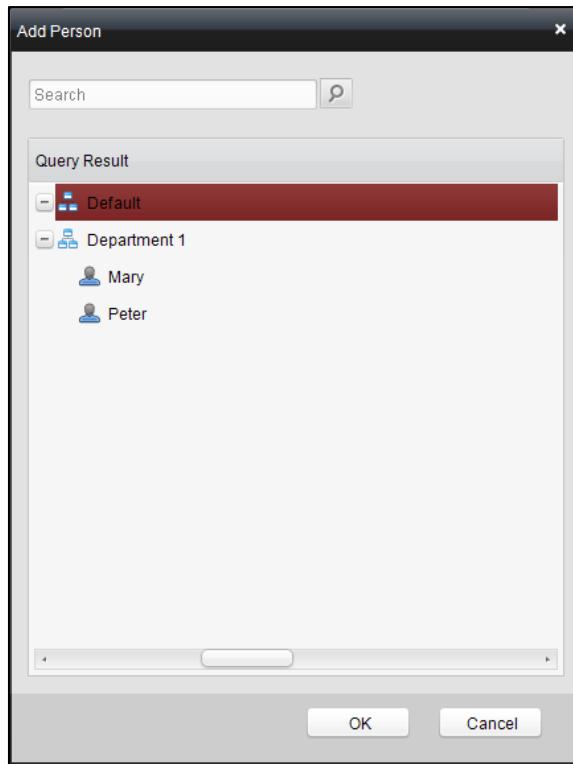
Add persons in the Person Management before you scheduling by person.

Steps:

1. In the Shift Schedule Management tab, click  **Staff**.

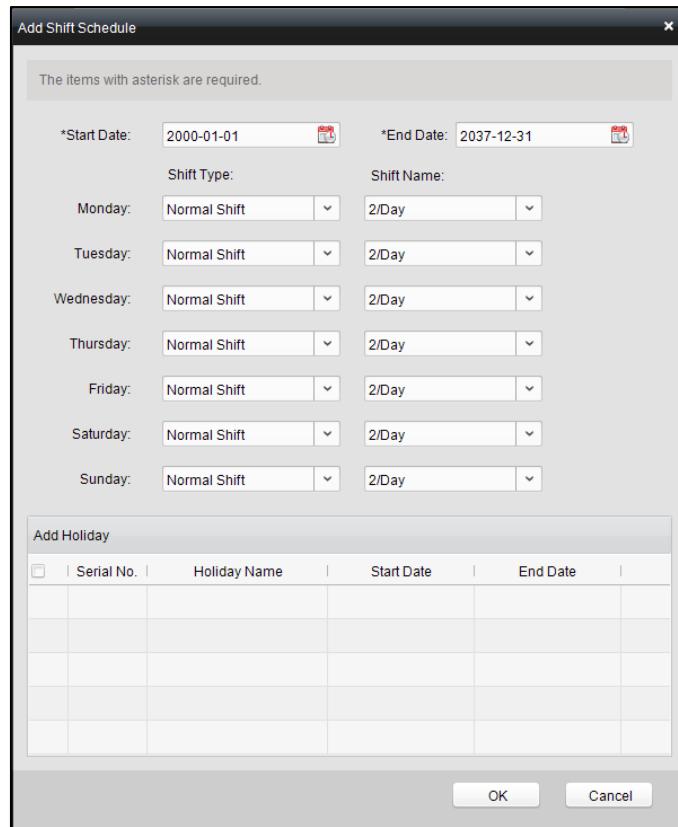


2. Click  **Add** and select the person in the pop-up window and click  **OK**.



You can also select the person in the person list and click **Delete** to delete the person.

3. Select the person in the person list and select the default schedule on the right of the interface.
4. Click **Edit** and configure the parameters in the pop-up window.



5. Click **OK** to confirm editing.
6. Click **Apply**, and apply permissions in the permission management to apply configurations to the device. For details, see *Section 4.3 Permission Management*.

Setting Wiegand

Purpose:

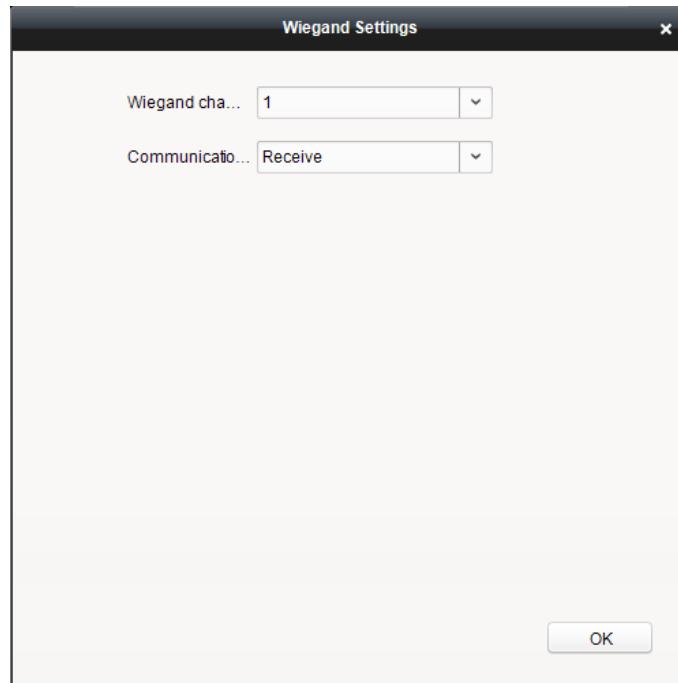
You can set the Wiegand channel and the communication mode.

Steps:

1. In the Edit Access Controller interface, click the **Wiegand Settings** button to enter the Wiegand Settings interface.
2. Select the Wiegand channel and the communication mode in the dropdown list.
3. Click **OK** to save the settings.

Notes:

- After changing the communication direction, the device will be rebooted. A prompt will be pop-up after changing the communication direction.
- The attendance device does not support the function.



4.2.2 Access Control Point Management

Click the icon on the control panel to enter the door management interface.

A screenshot of the Access Control Point Management interface. On the left, there's a sidebar with "Add Group" and "Delete Gro...". Below it is a tree view with groups: Test_1 (selected), Test_2, Test_3, and Test_4. On the right, a main panel shows a table titled "Access Control Point under Group Test_1". The table has columns: Name, Belong to Controller, Door Camera, and Position. One row is visible: 123_Door1, 123, 1. There are also "Import", "Edit", and "Delete" buttons at the top of the main panel.

Group Management

The doors can be added to different groups to realize the centralized management.

Door Management

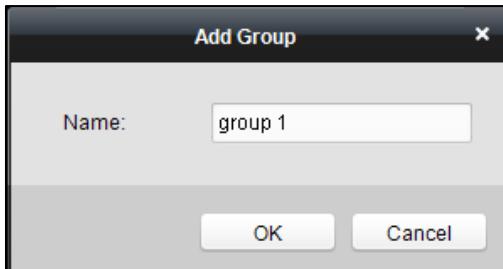
Manage the specific door under the door group, including importing, editing and deleting door.

Group Management

Adding Group

Steps:

1. Click the  button to pop up the Add Group dialog.



2. Input the group name in the text field and click the  button to finish adding.

Note: Multi-level groups are not supported yet.

Editing Group

Steps:

Double-click the group or right-click the group and select Edit in the right-click menu.

Deleting Group

To delete a group, three ways are supported.

- Click to select a group and click the  button.
- Right-click a group and select Delete in the popup menu.
- Move the mouse onto the group and click  icon of it.

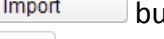
And then click the OK button in the popup window.

Access Control Point Management

Access control points under the group can also be edited, refer to the following instructions.

Importing Access Control Point

Steps:

1. Click the  button to pop up the access control point importing interface.
2. Select a access control point to import by clicking it.
3. Click to select a group in the right side bar to import to.
4. Click  button to import the selected access control points or click  to import all the available access control points.

Notes:

- You can click  button on the upper-right corner of the window to create a new group.
- The control client can manage 16 access control points at most.

Editing Access Control Point

Steps:

1. Click to select a access control point in the list and click the  button to edit the access control point.
2. Edit the Door Name and Position.
3. Click  button to finish editing.

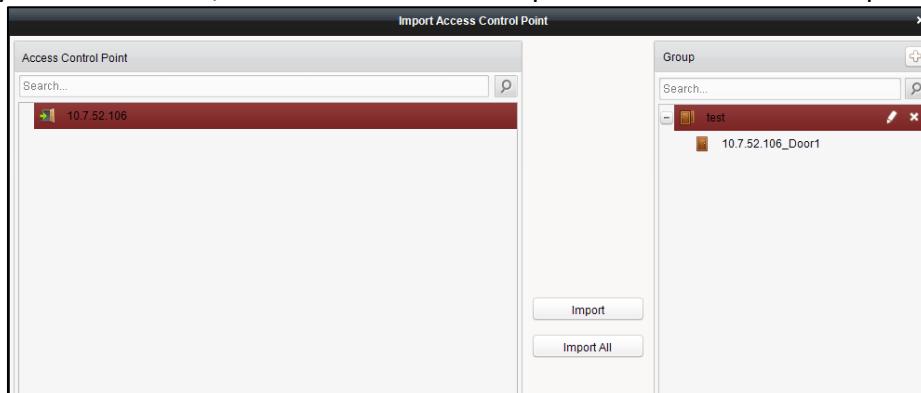
Note: you can also enter the Edit interface by double clicking the door from the list.

Deleting Access Control Point

Several ways are supported to delete the access control point, as shown below.

- ◆ Click to select a group in the group list, select door(s) under it, and click  button.
- ◆ Click to select a group in the group list, and click  button to delete all access control points under the group.
- ◆ Move the mouse onto a group in the group list, and click  button to delete all access control points under the group.

Note: you can also edit/delete a door on the Import Access Control Point panel.

**Steps:**

1. Select a control point on the **Group** panel.
2. Click the  /  icon to enter the **Edit Access Control Point** panel or to delete the control point.

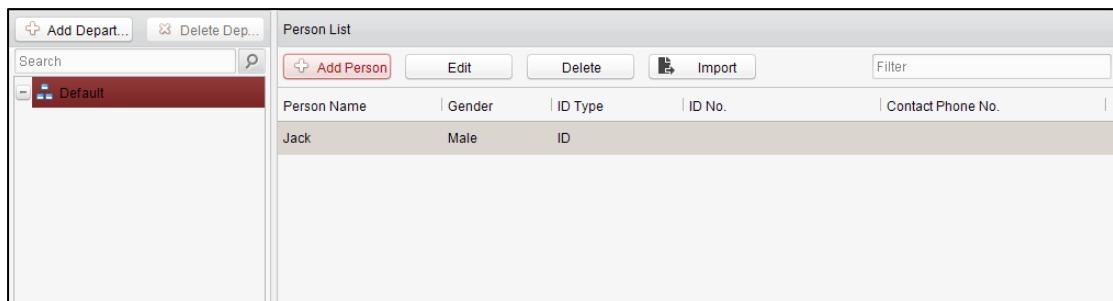
4.3 Permission Management

4.3.1 Person Management



Click the  icon on the control panel of the software.

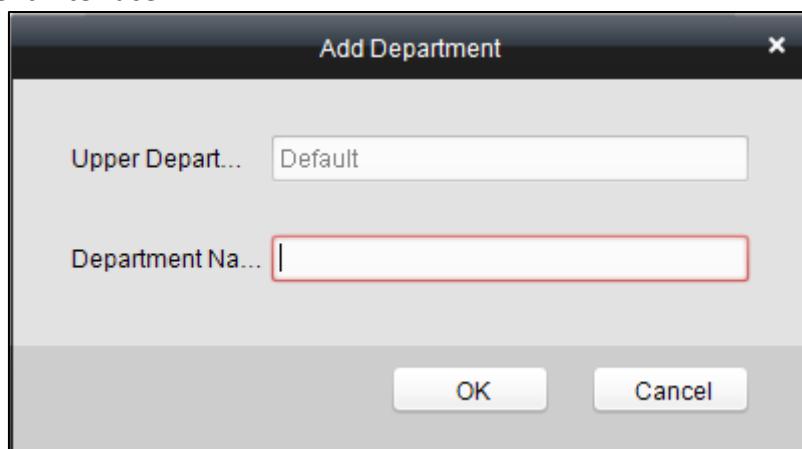
Adding, editing, deleting and filtering of the department and person are supported in this interface.



Department Management

Steps:

1. In the department list, click button to pop up the adding department interface.



Notes:

- Multi-level department system can be created. Click a department as the upper-level department and click button, and then the added department will be the sub-department of it.
 - Up to 10 levels can be created.
2. You can double-click an added department to edit its name.
 3. You can click to select a department, and click the button to delete it.

Notes:

- The lower-level departments will be deleted as well if you delete a department.
- Make sure there is no person added under the department, or the department cannot be deleted.

Person Management

Note: In the person management interface, double-click the person name or click the **Edit** button to edit the person information.

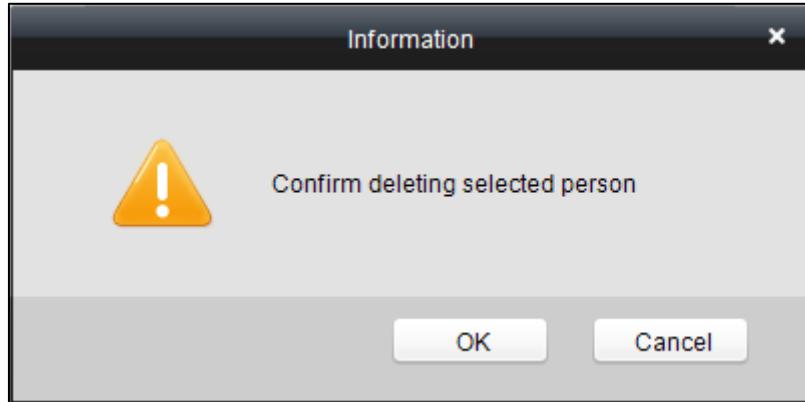
In the person management interface, click the **Delete** button to delete the person. Up to 2000 persons can be added.

● Inputting General Information

Steps:

1. Select a department in the list and click the in the person

- infoarmation list to pop up the adding person interface.
2. Input the Person Name (required), Gender, ID Card, etc., upload the photo of the person and click the  icon to finish adding.
Note: The format of the photo should be .jpg, or .jpeg.
 3. You can double-click an added person to edit its information.
 4. You can click to select a person, and click the  button to delete it.

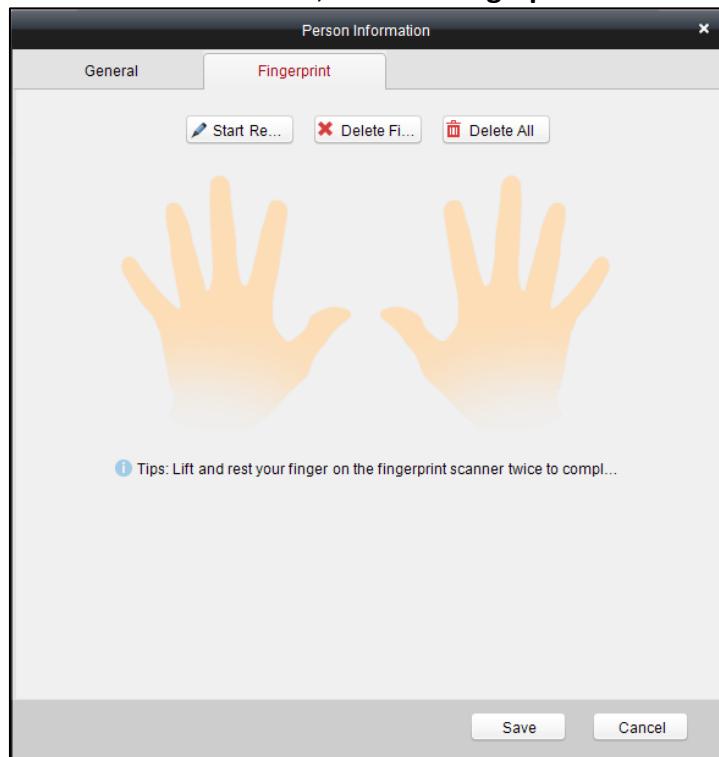


If a card is associated with the current person, the association will be invalid after the person is deleted.

● Inputting Fingerprint

Steps:

1. In the personal information interface, click the **Fingerprint** button.



2. Click the **Start Register** button, and select the fingerprint to be input.
3. Click the **Save** button to save the parameter.

Note: Click the **Delete Fingerprint** button to delete the fingerprint.

Click the **Delete All** button to clear all fingerprints input.

4.3.2 Card Management

Click  on the control panel of the software to enter the card management interface.



The cards are divided into 3 types: Blank Card, Normal Card, and Lost Card.

Blank Card: A card has not been issued with a person.

Normal Card: A card is issued with a person and is under normal using.

Lost Card: A card is issued with a person and is reported as lost.

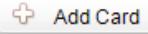
Blank Card

- Adding Card

Before you start:

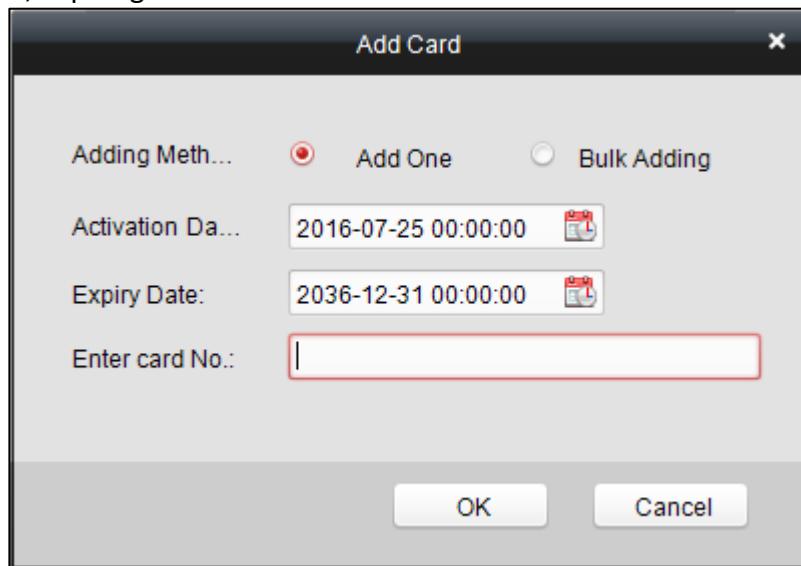
Make sure a card dispenser is connected to the PC and is configured already. Refer to the section of *Card Dispenser Configuration* for details.

Steps:

1. Click the  button to add cards.
2. Two modes of adding cards are supported.

Adding Single Card

Choose the Single Add as the adding mode by clicking the to and input the Start Date, Expiring Date and Card No. in the text field.



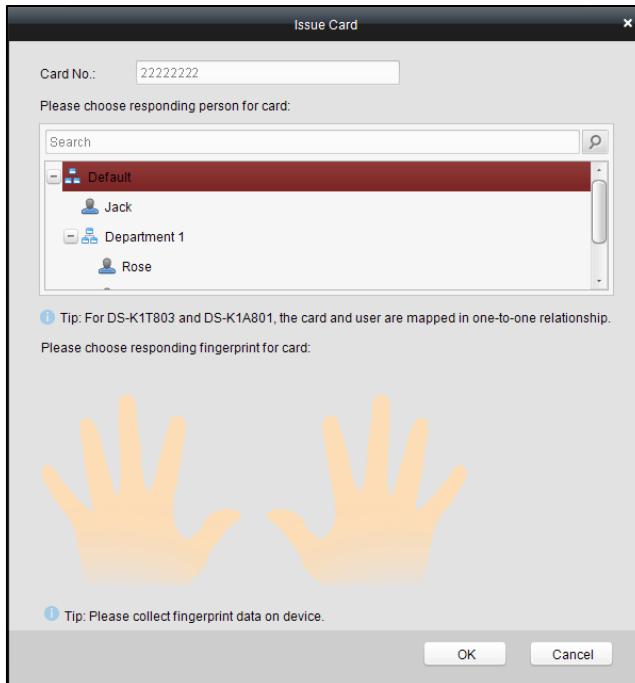
Batch Adding Cards

Choose the **Bulking Adding** as the adding mode by clicking the to and input the activation date, expiry date, start card No. and last card No. in the corresponding text fields.

Note: The start card No. and the last card No. should be the with same length.

E.g., the last card No. is 234, then the start card No. should be like 028.

3. Click the button to finish adding.
 4. Click an added blank card in the list and click button to issue the card with a person.
- Note:** you can double click the blank card in the card list to enter the **Issue Card** Page.



5. Click to choose a person on your demand in the popup dialog box, select a fingerprint, and click to finish.

Notes:

- The issued card will disappear from the Blank Card list, you can check the card information in the Normal Card list.
- Up to 2000 cards can be added.
- For the DS-K1A801 device and the DS-K1T803 device, the card and the user are mapped in one-to-one relationship.

● Deleting Card

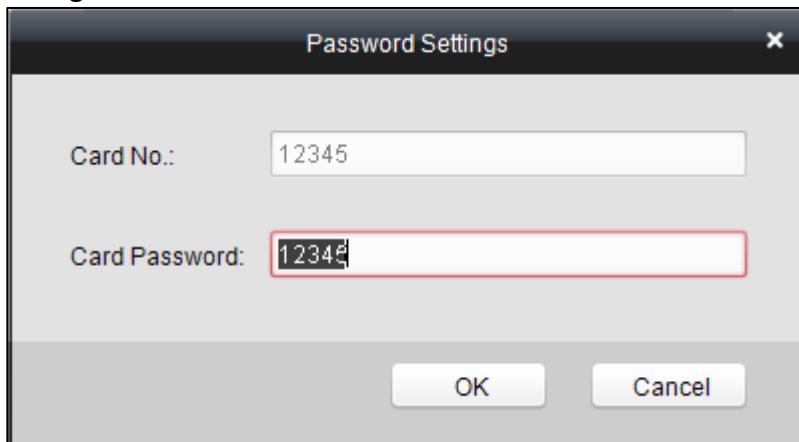
You can click an added blank card in the list and click button to delete the selected card.

Normal Card

Click the Normal tab in the card management interface to show the Normal Card list. You can view all the issued card information, including card No., card holder, and the department of the card holder.

Empty Card	Normal Card	Card Reported Loss
Normal Card List		
Card Change	Return Card	Report Card L...
Card No.	Status	Card Holder Name
0001	Normal Card	Lela
0002	Normal Card	Olivia
0003	Normal Card	Shanna
0004	Normal Card	Sam
0005	Normal Card	Lemon

- ◆ Click to select a card and click the **Card Change** button to change the associated card for card holder. Select another card in the popup window to replace the current card.
- ◆ Click to select an issued card and click the **Return Card** button to cancel the association of the card, then the card will disappear from the Normal Card list, which you can find it in the Blank Card list.
- ◆ Click to select an issued card and click the **Report Card Loss** button to set the card as the Lost Card, that is, an invalid card.
- ◆ Click to select an issued card and click the **Password Settings** button to set the password for the card, set the password in the text field and click the **OK** button to finish setting.



Note: The password will be required when the card holder swiping the card to get enter to or exit from the door if you enable the card&password authentication on the advanced configuration page.

Lost Card

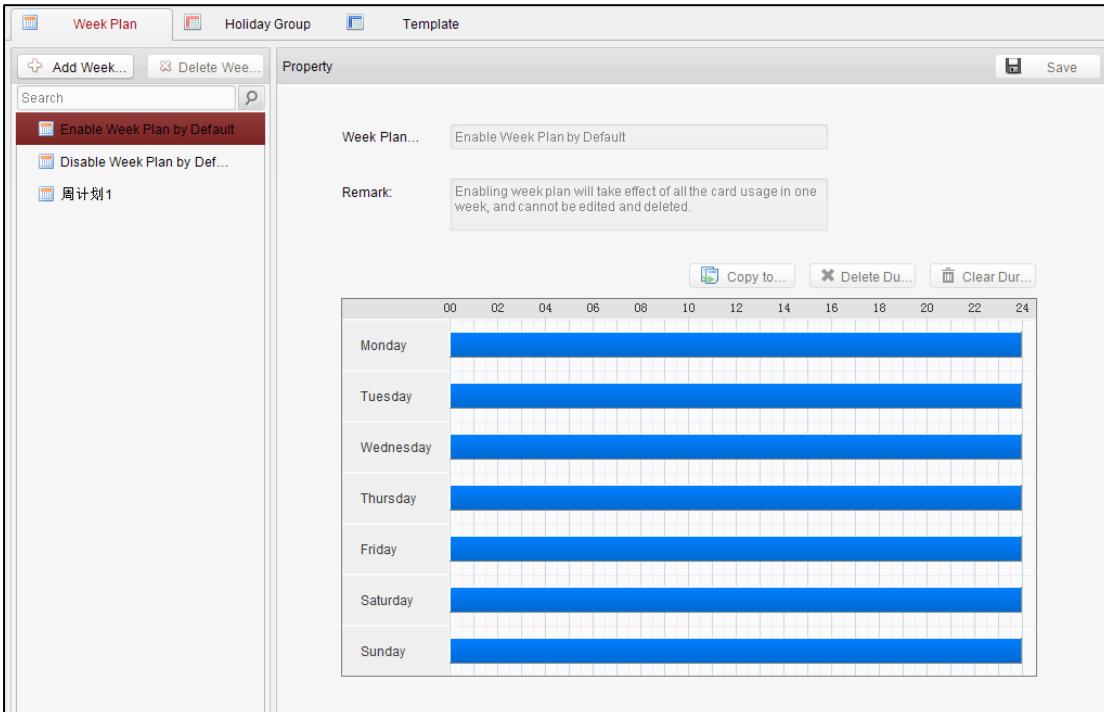
Click the Card Reported Loss tab in the card management interface to show the Lost Card list. You can view all the lost card information, including card No., card holder, and the department of the card holder.

Empty Card	Normal Card	Card Reported Loss		
Card Loss List				
Cancel Card L... Card Replace... Filter				
Card No.	Status	Replace card?	Card Holder Name	Department
12345	Card Reported Loss	No	Jack	Default

- ◆ Click the **Cancel Card Loss** button to resume the card to the normal card.
- ◆ Click the **Card Replacement** button to issue a new card to the card holder replacing for the lost card. Select another card in the popup window as the new card and the predefined permissions of the lost card will be copied to the new one automatically.

4.3.3 Schedule Template

Click  **Template** on the control panel of the software to enter the schedule template interface.



The screenshot shows the 'Template' interface with the following details:

- Week Plan:** A list on the left includes 'Add Week...', 'Delete Week...', 'Enable Week Plan by Default' (which is selected), 'Disable Week Plan by Def...', and a custom plan named '周计划1'.
- Property:** On the right, there's a 'Save' button and a 'Remark' section stating: "Enabling week plan will take effect of all the card usage in one week, and cannot be edited and deleted."
- Schedule Grid:** Below the property is a grid for defining weekly schedules. It shows a 7-day week from Monday to Sunday, with time slots from 00 to 24. Each day has a solid blue bar spanning the entire 24-hour period, indicating that the system is set to active 24/7 for all days.

There are 3 settings in this interface: Week Plan, Holiday Plan, and Template.

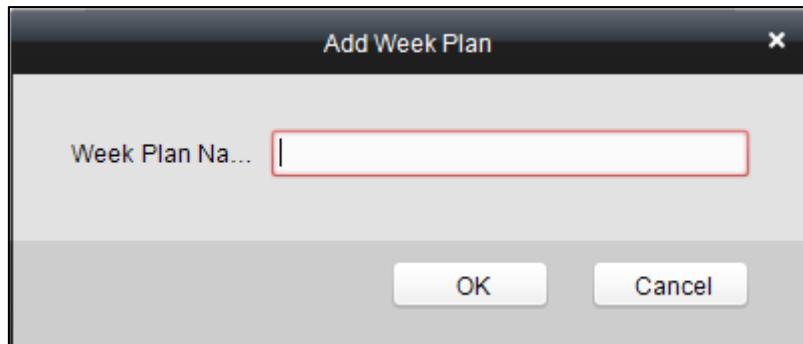
Setting Week Plan

● Adding Week Plan

System defines 2 kinds of week plan by default, Enable Week Plan by Default and Disable Week Plan by Default. You can define custom plans on your demand.

Steps:

1. Click the **Add Week Plan** button to pop up the adding plan interface.



2. Input the name of week plan and click the **OK** button to add the week plan.
3. Select a week plan in the plan list on the left-side of the window to edit.
4. Click and drag your mouse on a day to draw a blue bar on the schedule, which means in that period of time, the configured permission is activated.
5. Repeat the above step to configure other time periods.
Or you can select a configured day and click the **Copy to Week** button to copy the same settings to the whole week.

- **Deleting Week Plan**

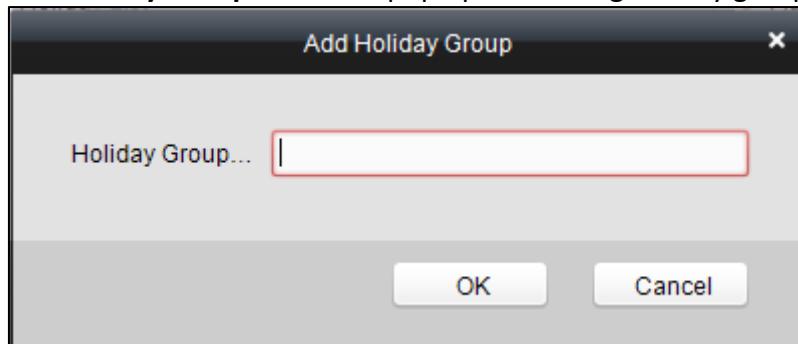
- ◆ Click to select a configured duration and click the **Delete Duration** button to delete it.
- ◆ Click the **Clear Duration** button to clear all the configured durations, while the week plan still exists.
- ◆ Click the **Delete Week Plan** button to delete the week plan directly.

Setting Holiday Group

- **Adding Holiday Group**

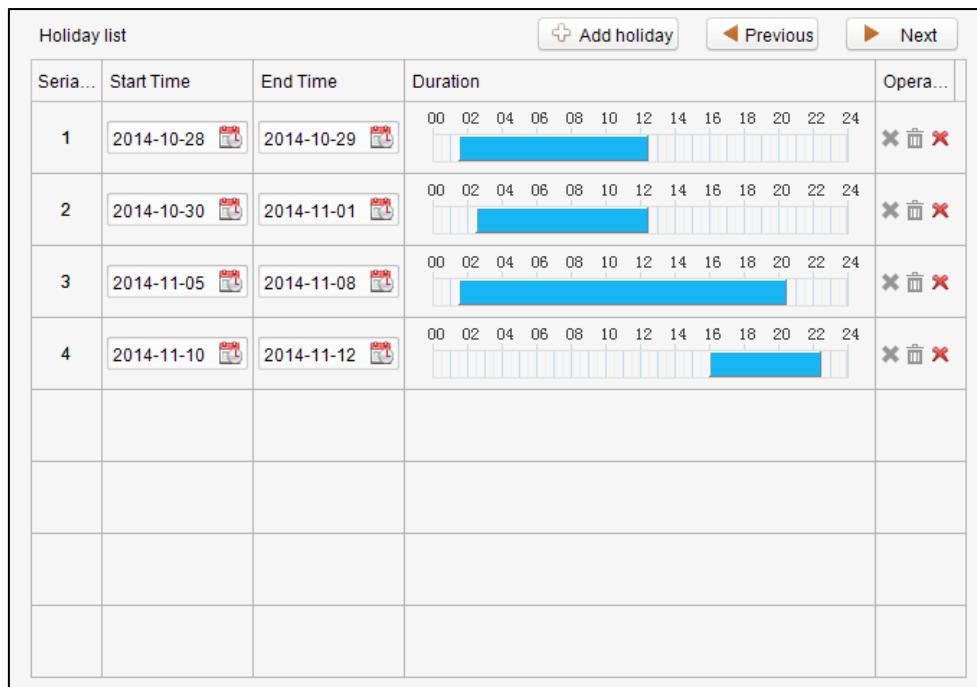
Steps:

1. Click the **Add Holiday Group** button to pop up the adding holiday group interface.



2. Input the name of holiday group in the text filed and click the **OK** button to add the holiday group.
3. Click the **+ Add Holiday** icon to add a holiday in the holiday list and configure the duration of the holiday.

Note:At most 16 holiday periods can be added.



- 1) Click and drag your mouse on a day to draw a blue bar on the schedule, which means in that duration, the configured permission is activated.
 - 2) Click to select a configured duration and click  to delete it.
 - 3) Click the  to clear all the configured durations, while the holiday still exists.
 - 4) Click the  to delete the holiday directly.

4. Click the  **Save** button to save the settings.

Note: The holidays cannot be overlapped with each other.

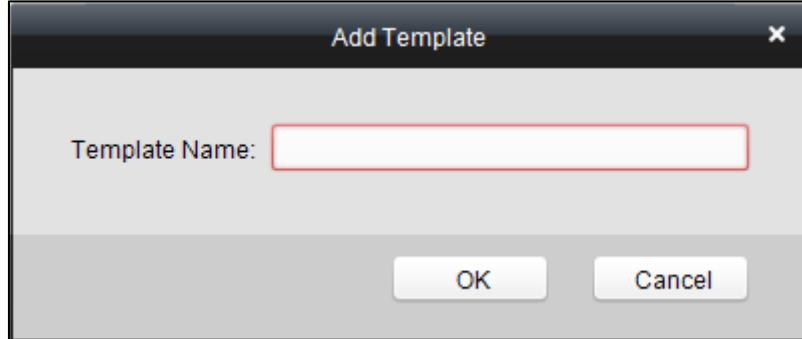
The schedule consists of week m

The schedule consists of week plan and holiday group, you can only choose which plan and group to enable in the schedule template configuration interface. Configure the week plan and holiday group before configuring the schedule template.

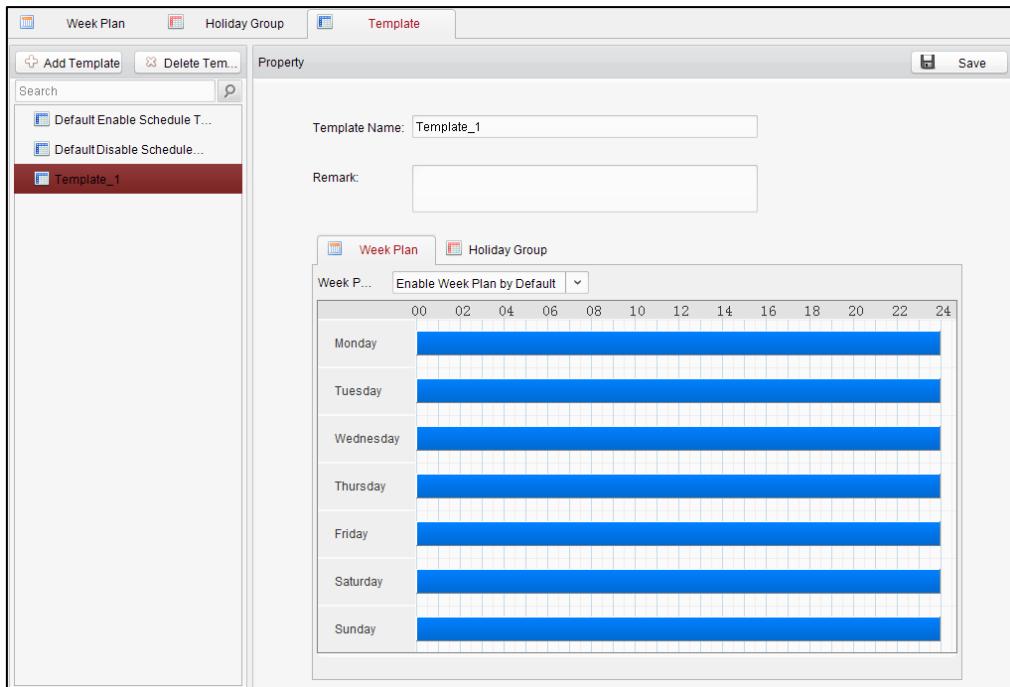
Note: The priority of holiday group schedule is higher than the week plan.

Steps:

1. Click Add Template to pop up the adding schedule interface.

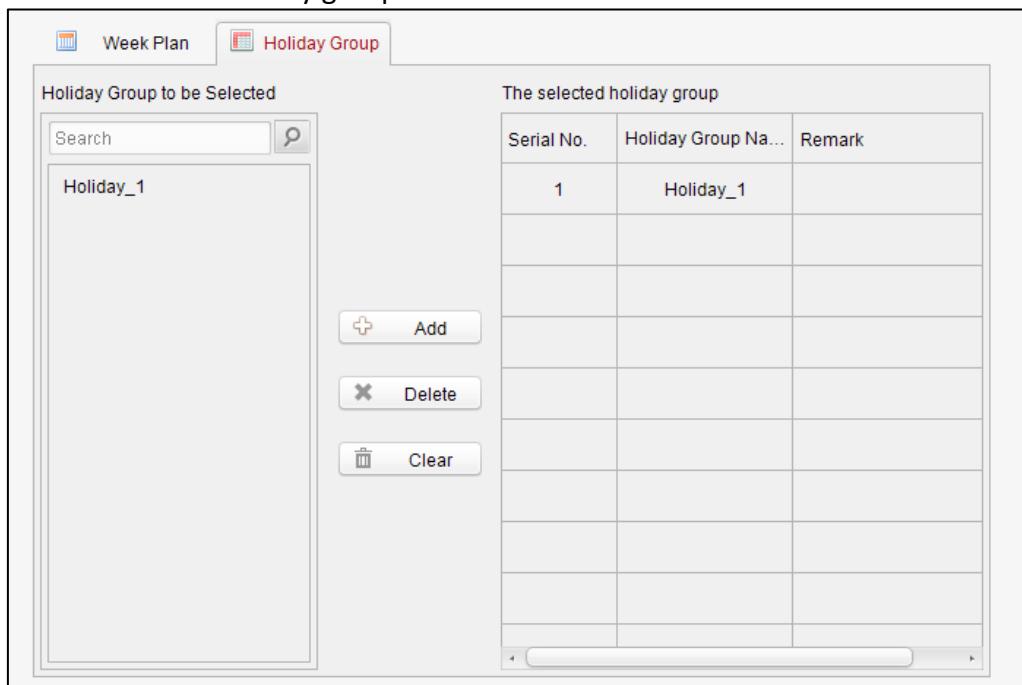


2. Input the name of schedule in the text field and click the  button to add the schedule.
 3. Select a week plan you want to apply to the schedule.
Click the Week Plan tab and select a plan in the dropdown list.



4. Select holiday groups you want to apply to the schedule.

Note:At most 4 holiday groups can be added.



- ◆ Click to select a holiday group in the left-side list and click  Add to add it.
 - ◆ Click to select an added holiday group in the right-side list and click  Delete to delete it.
 - ◆ Click  Clear to delete all the added holiday groups.

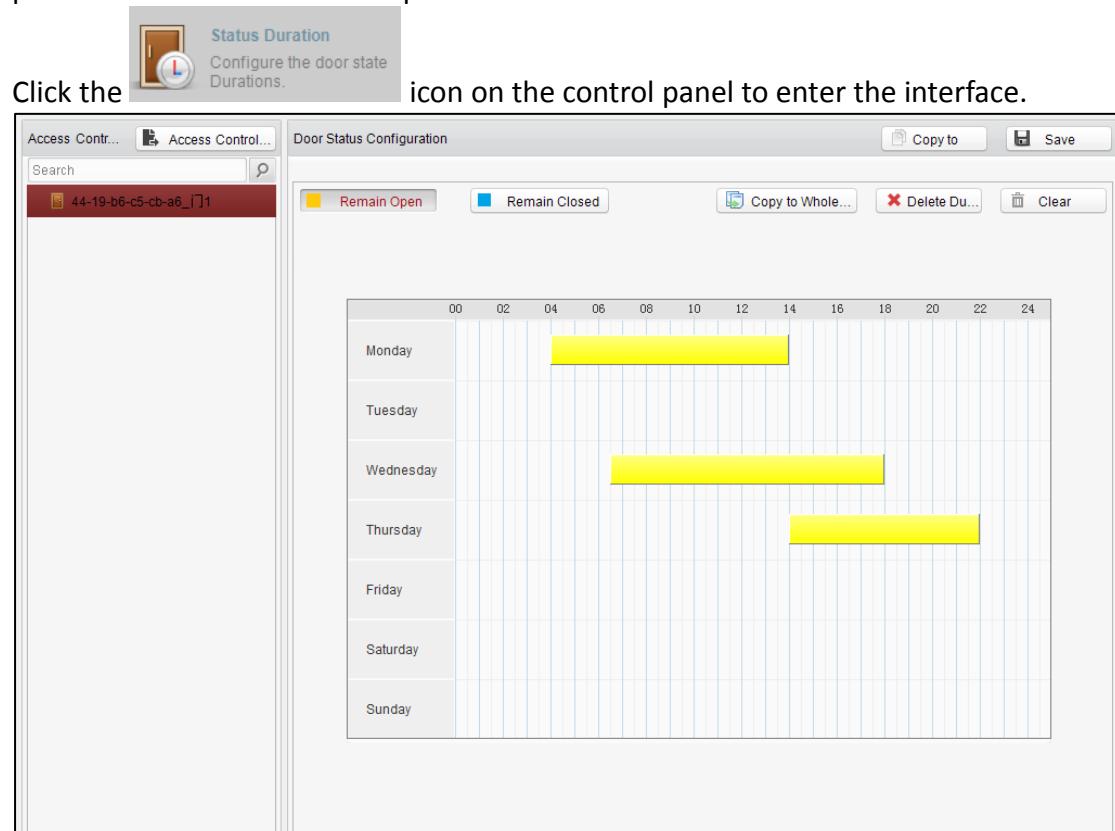
5. Click Save to save the settings.

Note: The attendance device does not support schedule template..

4.3.4 Door Status Management

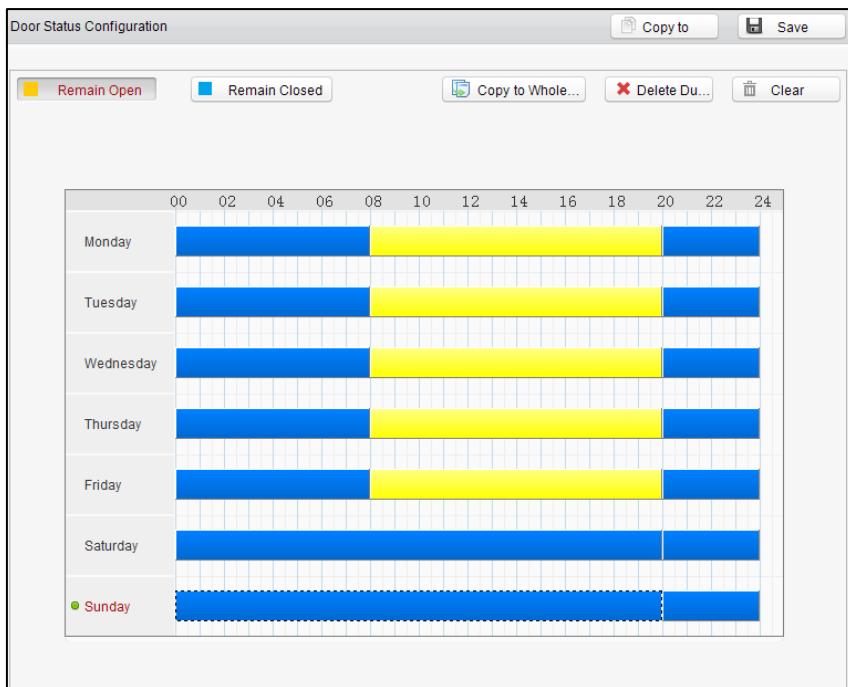
Purpose:

The function of **Door Status Management** allows you to schedule weekly time periods for a door to remain open or closed.



Steps:

1. Enter the Door Status Management page.
2. Click and select a door from the door list on the left side of the page.
3. Draw a schedule map.
 - 1) Select a door status brush **Remain Open** / **Remain Closed** on the upper-left side of the **Door Status Settings** panel.
Remain open: the door will keep open during the configured time period.
 The brush is marked as yellow.
Remain Closed: the door will keep closed during the configured duration.
 The brush is marked as blue.
 - 2) Click and drag the mouse to draw a color bar on the schedule map to set the duration.

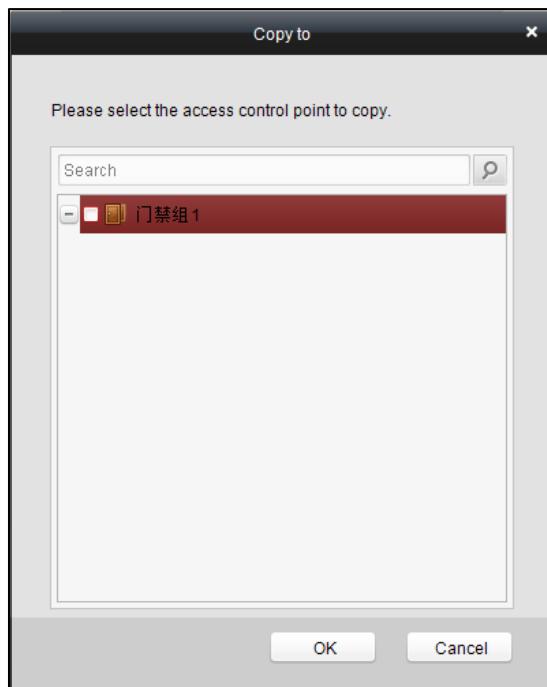


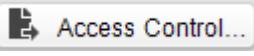
Notes

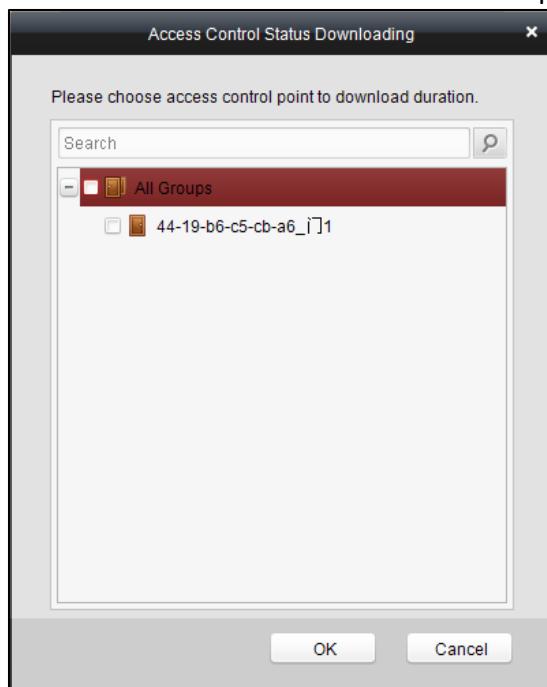
- The min. segment of the schedule is 30min.
- You can copy the configured time periods of a day to the whole week.

Steps:

1. Select a day which has already been configured.
2. Click on to copy the time periods to the whole week.
4. Edit the schedule map.
 - **Edit Duration:**
Click and drag the color bar on the schedule map and you can move the bar on the time track.
Click and drag the mouse on the ends of the color bar and you can adjust the length of the bar.
 - **Delete a Duration:**
Click and select a color bar and click to delete the time period.
 - **Clear All Durations:**
Click to clear all configured durations on the schedule map.
5. Click on to save the settings.
6. You can copy the schedule to other doors by clicking on and select the required doors.



7. Click  to enter the Download Door State page.

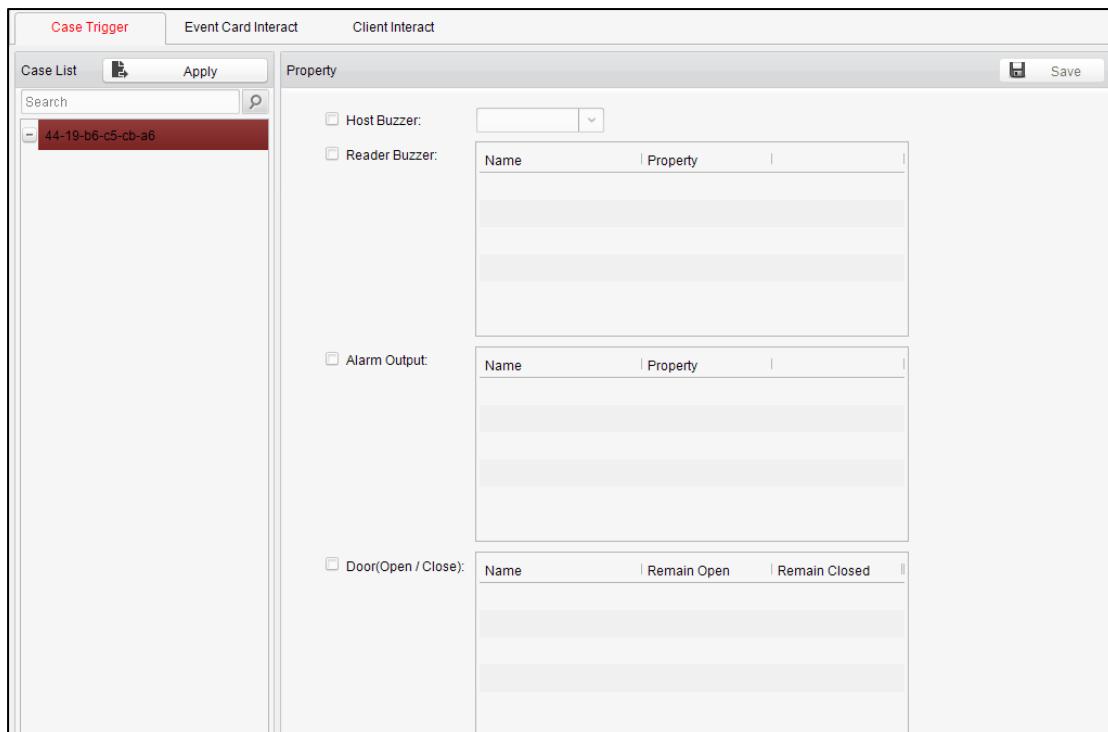


8. Select a control point and click **OK** to download the settings to the system.

Note: The attendance device does not support the function.

4.3.5 Interact Configuration

 **Interact Configuration**
Case, event/card interaction configuration.
Click  on the control panel of the software to enter the interact configuration interface.



In this interface, you can set alarm linkage modes of the access host, including case trigger, event card interact, and client interact.

Case Trigger

Purpose:

The case (refer to the triggers of the controller) can be linked to some actions (e.g., alarm output, host buzzer) when it is triggered.

Steps:

1. Click the Case Trigger tab to enter the case trigger interface, and select a case.
2. Check the checkbox of the corresponding linkage actions and set the property as **Trigger** to enable this function.
 - Host Buzzer:** The audible warning of controller will be triggered.
 - Reader Buzzer:** The audible warning of card reader will be triggered.
 - Alarm Output:** The alarm output will be triggered for notification.
 - Door (Open/Close):** The door will be open or closed when the case is triggered.
3. Click the **Save** button.
4. Click the **Apply** button to take effect of the new settings.

Note: The Door cannot be configured as open or closed at the same time.

Event Card Interact

In the Interact Configuration interface, click the **Event Card Interact** button to enter the settings interface.

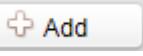
● **Event Linkage**

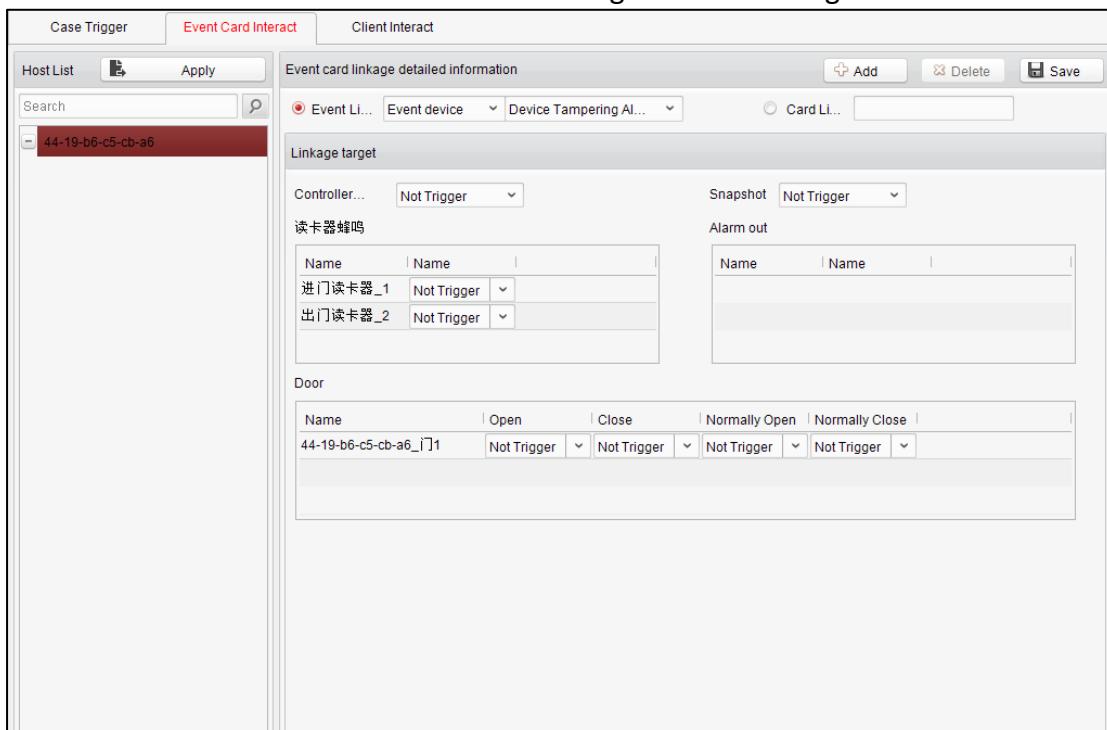
In the Event Interact interface, the linkage alarm action, after triggering alarm event, can be set. The alarm event can be divided into four types: event device, event input alarm, door event, and card reader event.

Steps:

1. Click the Event Card Interact tab to enter the event card interface

2. Select the host to be set from the host list.

3. Click the  button to start setting the event linkage.



4. Click the radio button of the event linkage, and select the event type from the dropdown list.

5. Set the linkage target, and set the property as **Trigger** to enable this function.

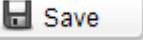
Host Buzzer: The audible warning of controller will be triggered.

Snapshot: The real-time capture will be triggered.

Reader Buzzer: The audible warning of card reader will be triggered.

Alarm Output: The alarm output will be triggered for notification.

Door: The door status of open, close, normally open, and normally close will be triggered.

6. Click the  button to save parameters.

7. Click the **Apply** button to download the updated parameters to the local memory of the device.

Notes:

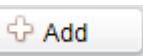
- The door status of open, close, normally open, and normally close cannot be triggered at the same time.
- The attendance device does not support opening door, closing door and capturing.

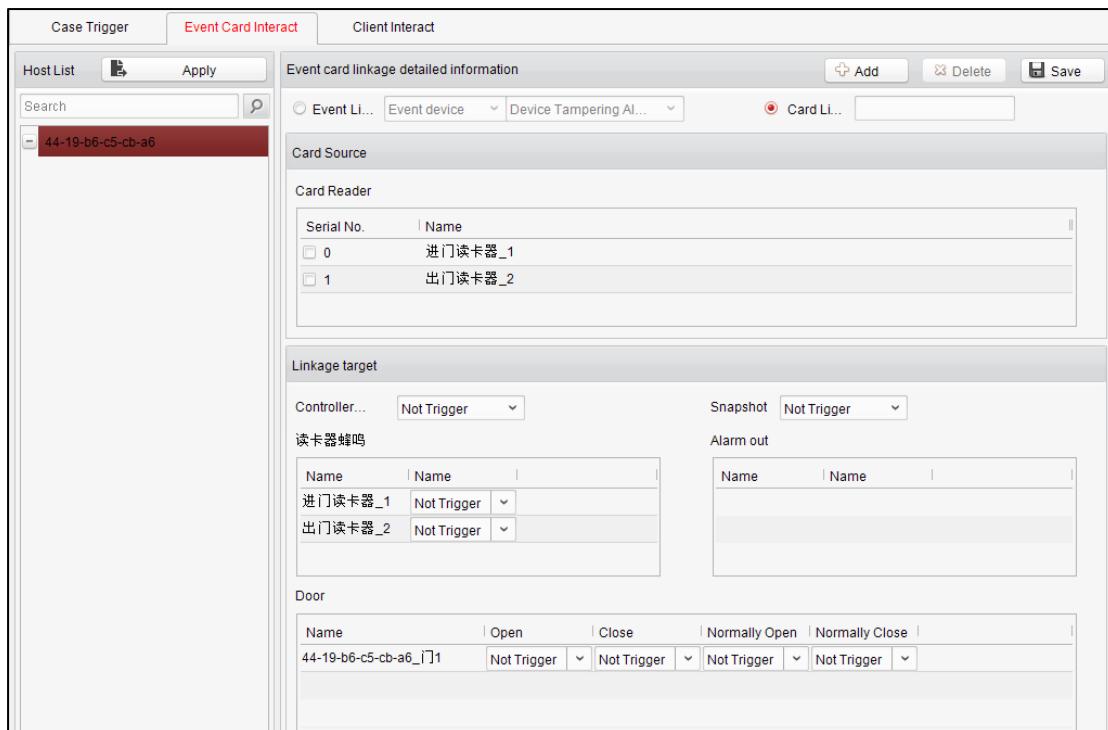
● Card Linkage

In the Event Interact interface, the linkage alarm action, after triggering the card number, can be set.

Steps:

- Click the Card Event Interact tab to enter the event card interface
- Select the host to be set from the host list.

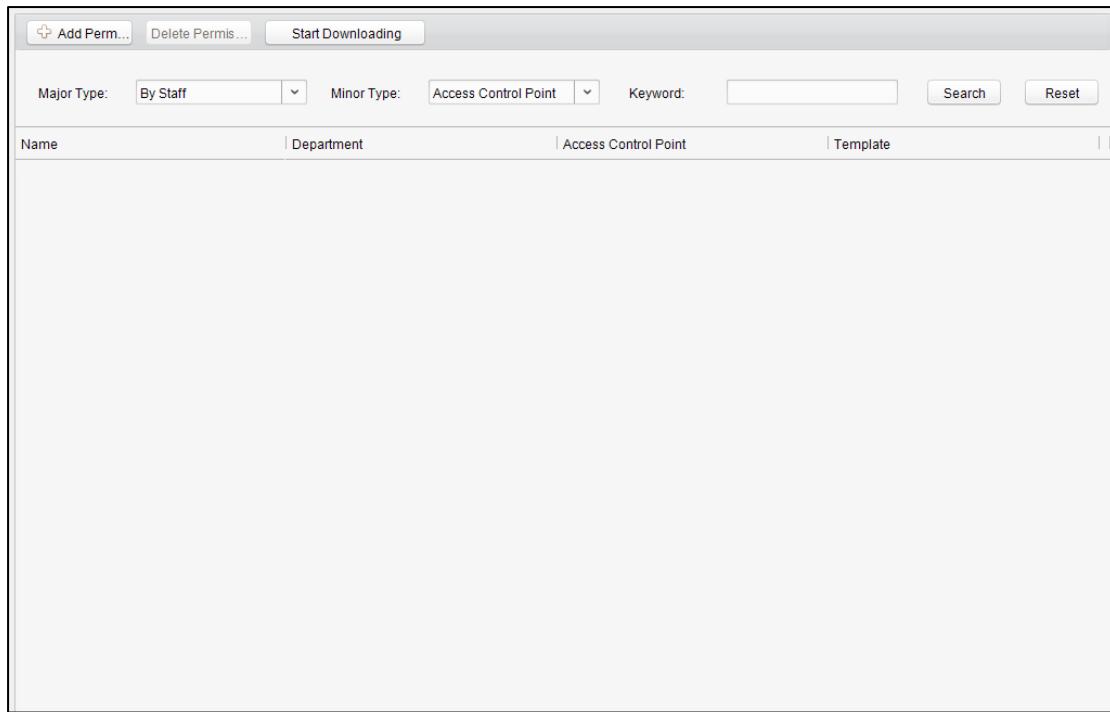
3. Click the  button to start setting the event linkage.



4. Click the radio button of card linkage, and input the card number.
 5. Select the event source, and check the checkbox of the card reader's serial number.
 6. Set the linkage target, and set the property as **Trigger** to enable this function.
Controller Buzzer: The audible warning of controller will be triggered.
Snapshot: The real-time capture will be triggered.
Reader Buzzer: The audible warning of card reader will be triggered.
Alarm Output: The alarm output will be triggered for notification.
Door: The door status of open, close, normally open, and normally close will be triggered.
 7. Click the **Save** button to save parameters.
 8. Click the **Apply** button to download the updated parameters to the local memory of the device.
- Note:** The door status of open, close, normally open, and normally close cannot be triggered at the same time.

4.3.6 Access Permission Configuration

Click the icon on the control panel to enter the interface.



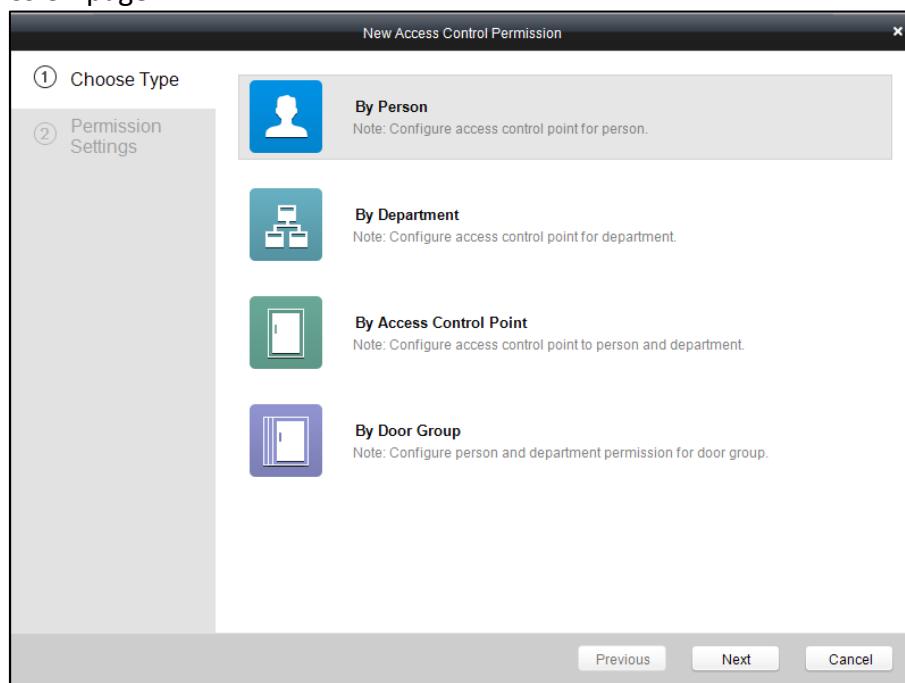
Access Permission Settings

Purpose:

You can allocate permission for people/department to enter/exist the control points (doors) in this section.

Steps:

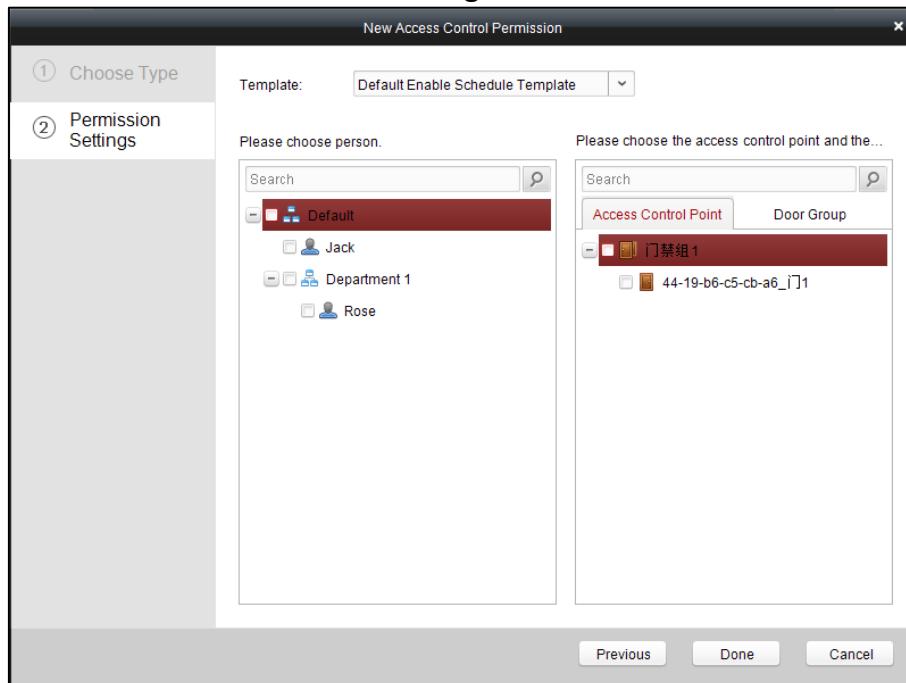
1. Enter the **Permission** page.
2. Click on icon on the upper-left side of the page to enter the **Add Permission** page.



3. Select an adding type in the **Select Type** interface.
 - ◆ **By Person:** you can select people from the list to enter/exit the door.

- ◆ **By Department:** You can select departments from the list to enter/exit the door. Once the permission is allocated, all the people in this department will have the permission to access the door.
- ◆ **By Access Control Point:** You can select doors from the door list for people to enter/exit.
- ◆ **By Door Group:** You can select groups from the door list for people to enter/exit. The permission will take effect on the door in this group.

4. Click **Next** to enter the **Permission Settings** interface.



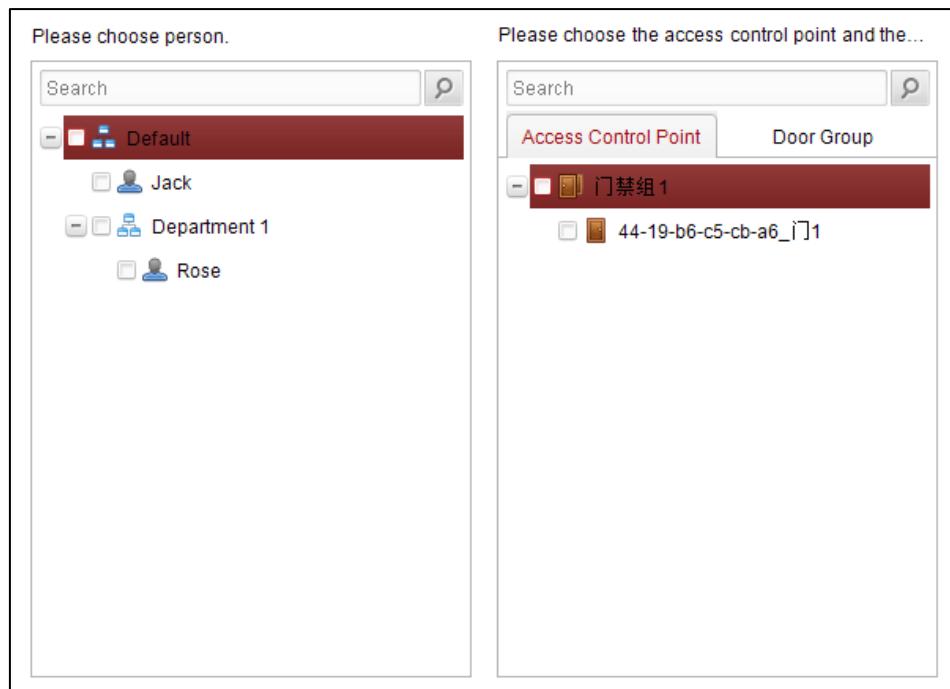
5. Click on the dropdown menu to select a schedule template for the permission.



Note: The schedule template must be configured before any permission settings.

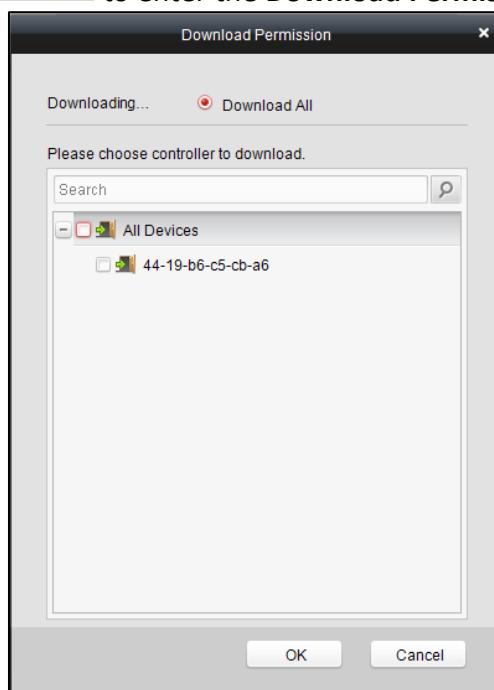
Refer to *Section 4.3.3 Schedule Template* for detailed configuration guide.

6. Select people/department and corresponding doors/door groups from the appropriate lists.

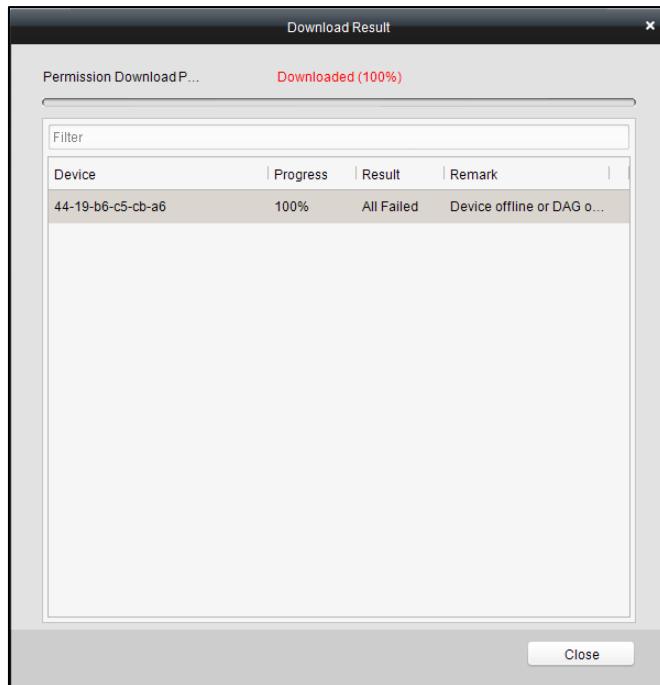


Note: The lower-level of department will also be selected if the highest-level of department is selected,

7. Click the **Done** button to complete the permission adding.
8. Click **Start Downloading** to enter the **Download Permission** page.



9. Select a control point and click the **OK** button, to enter the download result interface, to download the permission to the device.



Access Permission Searching

Purpose:

After the permission settings being completed, you can search and view permission assigning condition on the searching interface.

Steps:

1. Enter the **Permission** page.

2. Enter the search criteria (main type/minor type/Keyword).
3. Click **Search** to get the search results.

Name	Department	Access Control Point	Template
Lela	Market Department	123_Door1	Template_1
Olivia	Market Department	123_Door1	Template_1
Shanna	Market Department	123_Door1	Template_1
Sam	Market Department	123_Door1	Template_1
Lemon	Market Department	123_Door1	Template_1

Note: You can click **Reset** on the search criteria panel to clear all the displayed search results.

Permission Deleting

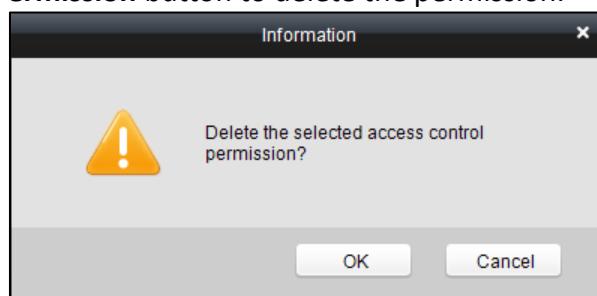
Steps:

1. Follow steps 1-3 in the Permission Searching section to search for the permission

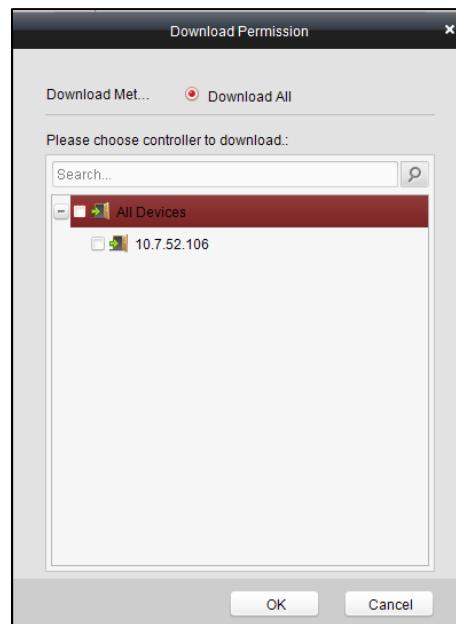
- needs to be deleted.
2. Select the permission from the results list.

Name	Department	Access Control Point	Template
Lela	Market Department	123_Door1	Template_1
Olivia	Market Department	123_Door1	Template_1
Shanna	Market Department	123_Door1	Template_1
Sam	Market Department	123_Door1	Template_1
Lemon	Market Department	123_Door1	Template_1

- Note:** you can press the Ctrl or Shift key on the keyboard to select multiple items.
3. Click the **Delete Permission** button to delete the permission.



4. Click **Start Downloading** to enter the **Download Permission** page.



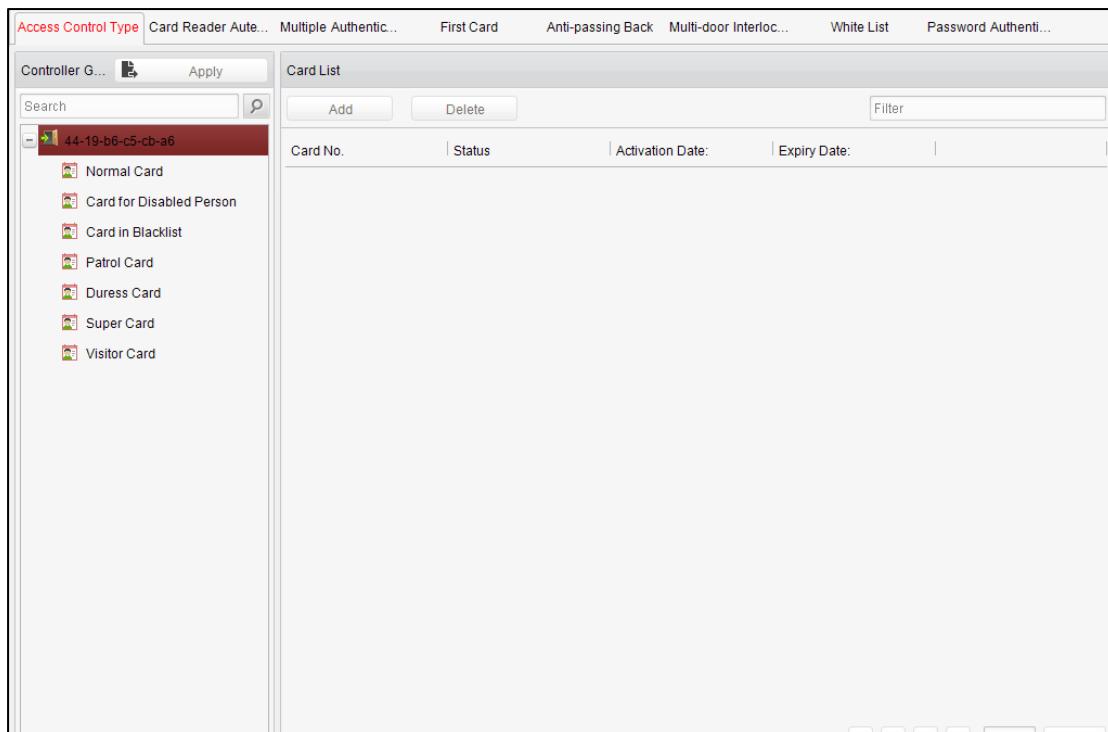
5. Select a control point and click the **OK** button to download the deletion operation to the device.

4.3.7 Advanced Functions

Purpose:

The advanced functions of the access control system can be configured.

Click the icon on the control panel to enter the interface.



Access Control Type

Purpose:

The added cards can be assigned with different card type for the corresponding usage.

Steps:

1. Click **Access Control Type** tab and select a card type.

Normal Card: By default, the card is set as normal card.

Card for Disabled Person: The door will remain open for the configured time period for the cardholder.

Card in Blacklist: The card swiping action will be uploaded and the door cannot be opened.

Patrol Card: The card swiping action can be used for checking the working status of the inspection staff. The access permission of the inspection staff is configurable.

Duress Card: The card swiping action will be uploaded.

Super Card: The card is valid for all the doors of the controller during the configured schedule.

Visitor Card: The card is assigned for visitors.

2. Click **Add** and select the available card.
3. Click **OK** to confirm assigning the card(s) to the selected card type.
4. Click the **Apply** button to take effect of the new settings.

Notes:

- You can click **Delete** to remove the card from the card type and the card can be available for being re-assigned.
- The attendance device only supports the normal card.

Card Reader Authentication

Purpose:

You can only open the door by both swiping card and entering the password during the set time periods.

Notes:

- For this authentication mode, the card swiping operation cannot be replaced by entering the card No..
- For password settings, please refer to *Section 4.3.2 Card Management*.

Steps:

1. Click **Card Reader Authentication** tab and select a card reader.
2. Select a card reader authentication type from the dropdown list.

Fingerprint: The door can open by only inputting the fingerprint.

Swipe Card: The door can open by only swiping the card.

Fingerprint/Swipe Card: The door can open by inputting the fingerprint or swiping the card.

Swipe Card/Password: The door can open by inputting the ID No. and password, or swiping the card.

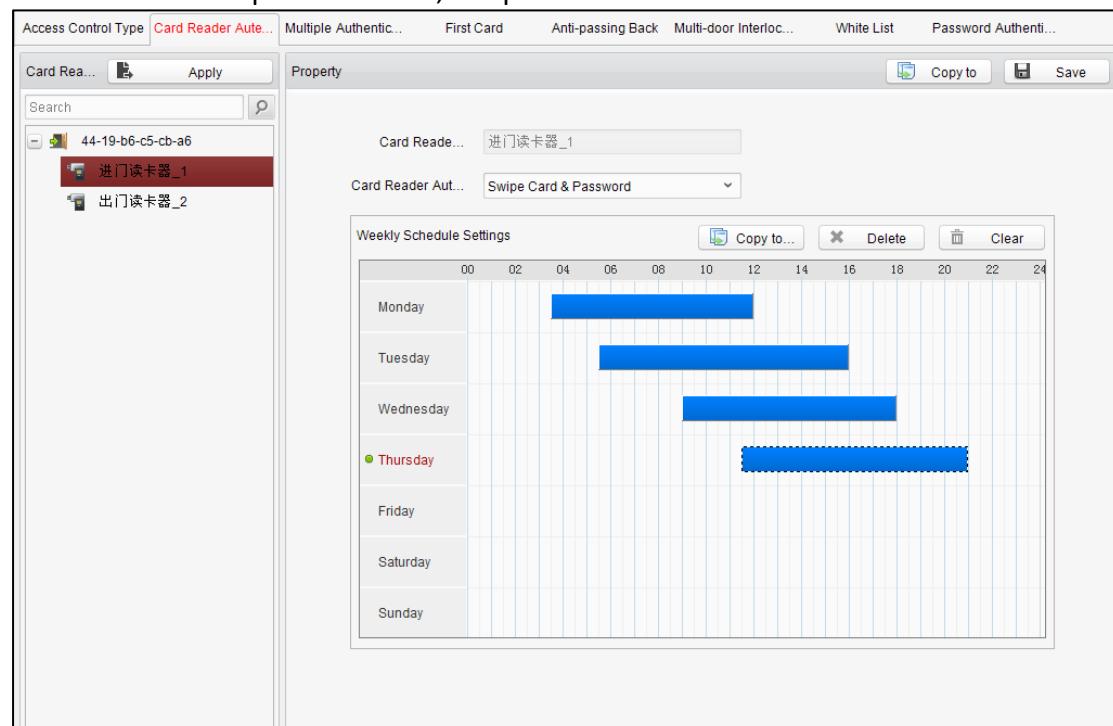
Fingerprint Password: The door can open by both inputting the password and inputting the fingerprint.

Swipe Card Password: The door can open by both inputting the password and swiping the card.

Fingerprint Swipe Card: The door can open by both inputting the fingerprint and swiping the card.

Fingerprint Swipe Card Password: The door can open by both inputting the fingerprint, inputting the password, and swiping the card.

3. Click and drag your mouse on a day to draw a blue bar on the schedule, which means in that period of time, the password authentication is valid.



4. Repeat the above step to set other time periods.

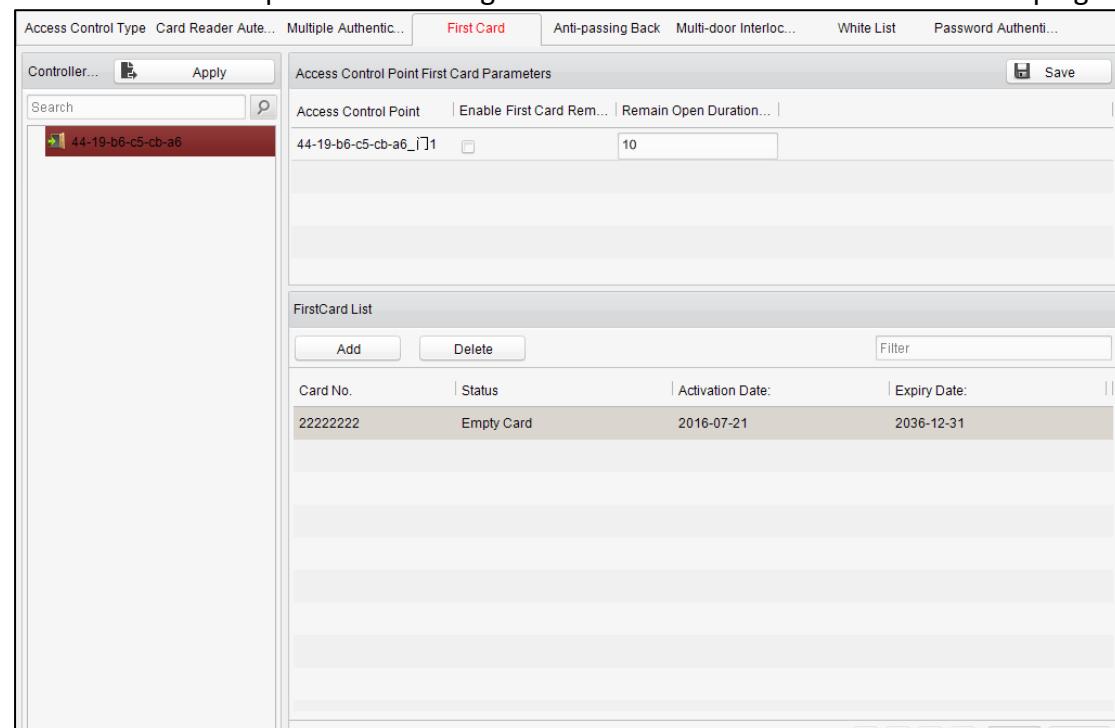
Or you can select a configured day and click the **Copy to Week** button to copy the same settings to the whole week.

- You can click the **Delete** button to delete the selected time period or click the **Clear** button to delete all the configured time periods.
5. (Optional) Click the **Copy to** button to copy the settings to other card readers.
 6. Click the **Save** button to save parameters.
 7. Click the **Apply** button to take effect of the new settings.

First Card

Purpose:

The door remains open for the configured time duration after the first card swiping.



Steps:

1. Click **First Card** and select an access control point.
2. Check the checkbox of **Enable First Card Remain Open** to enable this function.
3. In the **Remain Open Duration** (min), input the time duration for remaining open the door.
4. Click **Add** and select the cards to add as first card for the door and click the **OK** button.
5. Click **Save** and then click **Apply** to take effect of the new settings.

Note: The attendance device does not support the function.

Anti-Passing Back

Purpose:

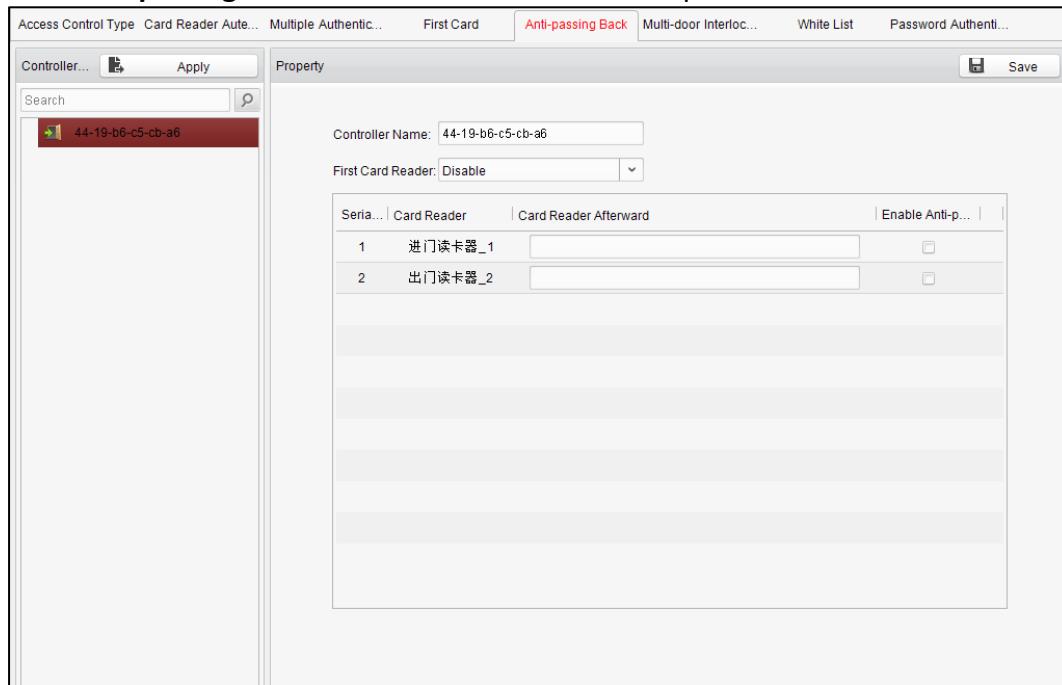
In this mode, you can only pass the access control system according to the specified path.

Note: Either the anti-passing back or multi-door interlocking can be configured for an access controller at the same time.

Setting the Path of Swiping Card (Card Reader Order)

Steps:

1. Click **Anti-passing Back** and select an access control point.



2. You can set the name for the controller and select the card reader as the beginning of the path.
3. In the list, click the text field of **Card Reader Afterward** and select the linked card readers.

Example: If you select Reader In_01 as the beginning, and select Reader In_02, Reader Out_04 as the linked card readers. Then you can only get through the access control system by swiping the card in the order as Reader In_01, Reader In_02 and Reader Out_04.

4. Check the checkbox of **Enable Anti-Passing back**.
5. Click **Save** and then click **Apply** to take effect of the new settings.

Note: The attendance device does not support the function.

4.4 Attendance Management

Purpose:

After adding the device and person, you can set the person shift, set the holiday, manage the person attendance and view the card swiping log.

Click icon on the control panel to enter the Attendance Configuration interface.

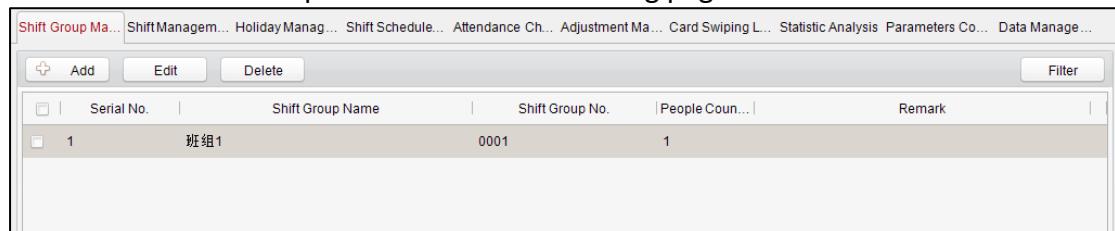
4.4.1 Shift Group Management

Purpose:

On the shift group management interface, you can add, edit, and delete shift groups for attendance management.

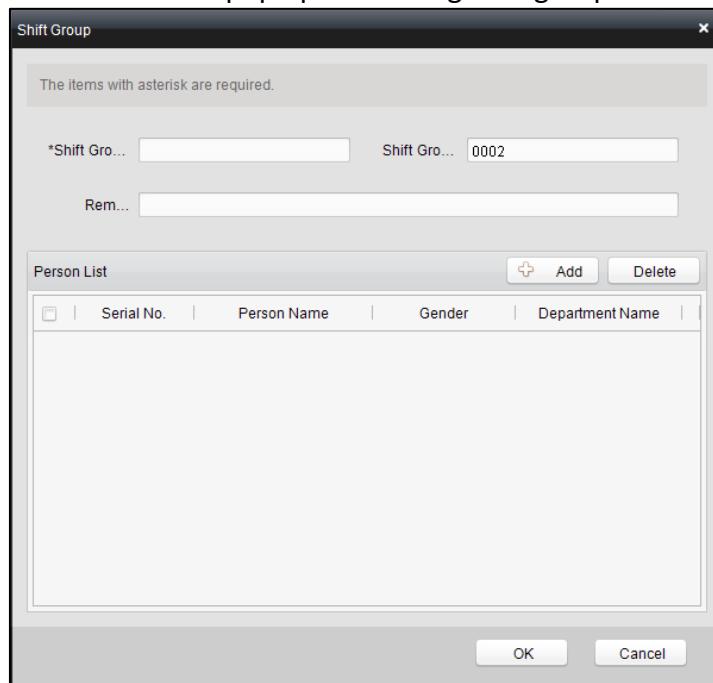
Steps:

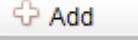
- Click the Shift Group tab to enter the following page.

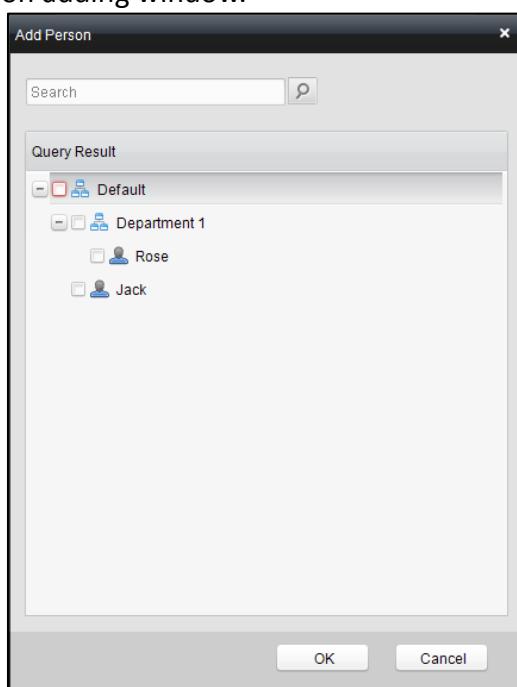


The screenshot shows a software interface titled "Shift Group Ma...". The main window displays a table with columns: Serial No., Shift Group Name, Shift Group No., People Count..., and Remark. A single row is present with values: 1, 班组1, 0001, 1, and an empty remark field. Below the table are buttons for Add, Edit, Delete, and Filter.

- Click  button to pop up the adding shift group window.



- Enter the shift group name, and add  button on the person list area to pop up the person adding window.



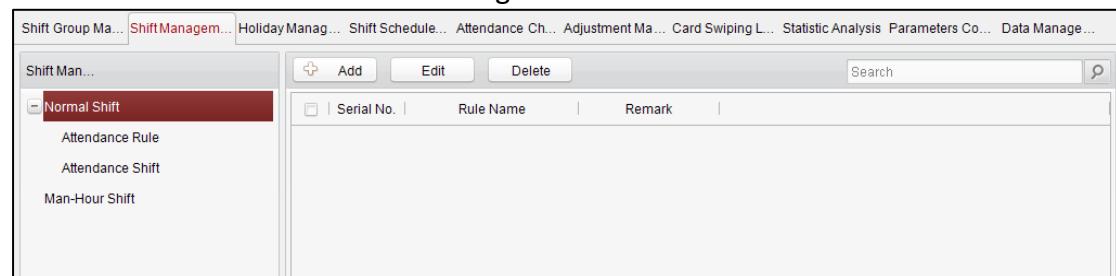
4. Check the checkbox to select the person and click and return to the shift group settings interface.
To delete the added person, check the person from the person list, and click button.
5. Click button to complete the operation.
6. You can edit or delete the added shift groups by clicking or .

Notes:

- After deleting the shift group, the shift schedule of the shift group will be deleted as well. For details about shift schedule, refer to *Section 4.4.4 Shift Schedule Management*.
- If the person has been added to one shift group, he/she cannot be added to other shift groups.

4.4.2 Shift Management

Click **Shift** tab to enter the shift management interface.



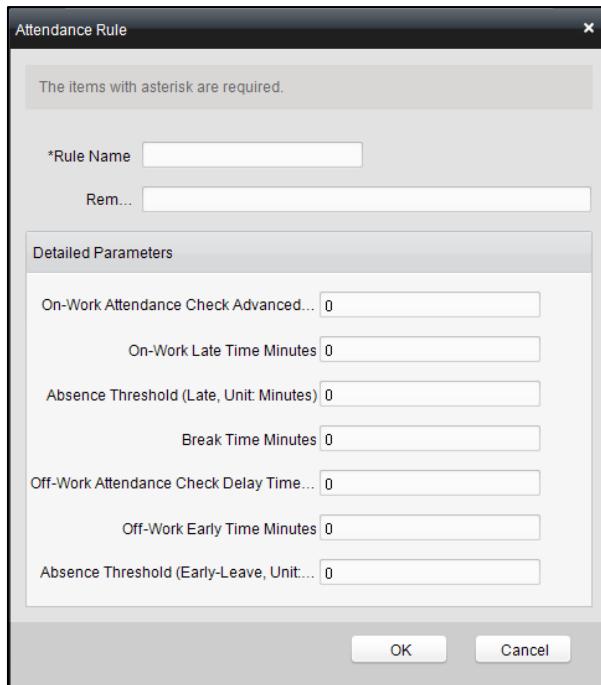
There are two kinds of shifts in this interface: **Normal Shift**, and **Man-Hour Shift**.

Normal Shift

❖ Setting Attendance Rule

Steps:

- Click **Attendance Rule** to set the rule for the attendance management.
- Click to pop up the following dialog box.



3. Set a rule name.
4. Set detailed parameters for the attendance rule according to actual needs.
5. Click to save the rule.
6. (Optional) You can edit or delete the rule by clicking or .

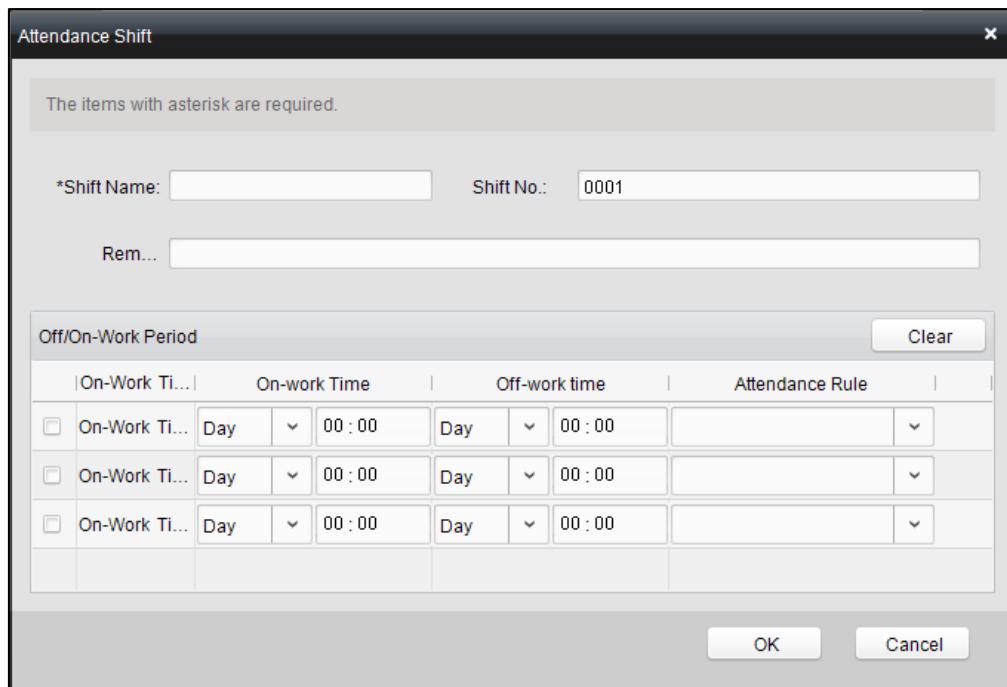
Notes:

- After deleting the rule, the normal attendance shift which has enabled the rule will be deleted as well.
- If the shift which has enabled the rule has already set the shift schedule, the shift will not be deleted.

❖ **Setting Attendance Shift**

Steps:

1. Click **Attendance Shift** to set the normal attendance shift.
2. Click to pop up the attendance shift setting window.

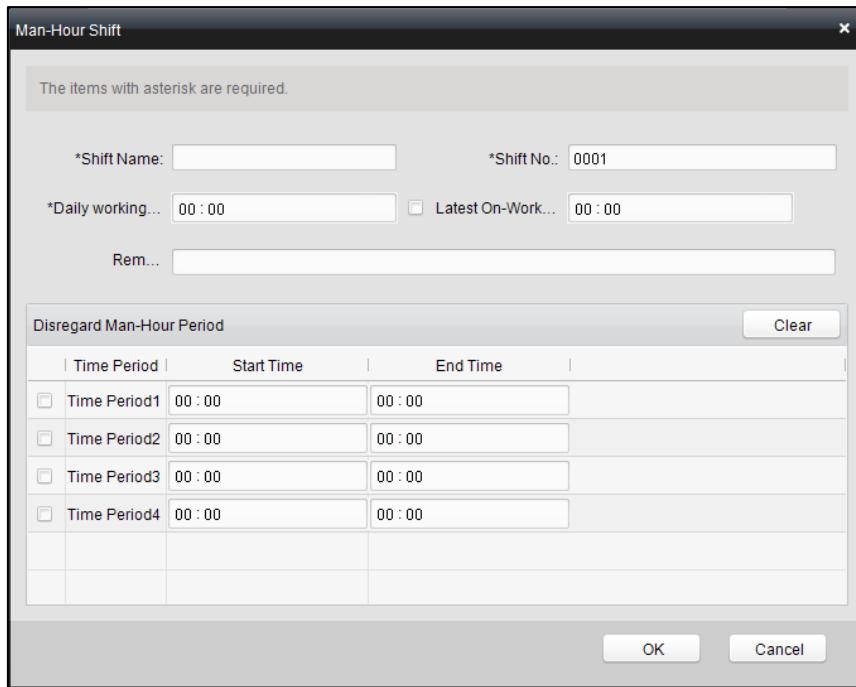


3. Set a shift name.
 4. Set on-work duration for the shift, and select the attendance rule from the dropdown list.
 5. Click **OK** to complete the operation.
 6. (Optional) You can edit or delete the shift by clicking **Edit** or **Delete**.
- Note:** After deleting the shift, its shift schedule will be deleted as well. For details about shift schedule, refer to *Section 4.4.4 Shift Schedule Management*.

Man-Hour Shift

Steps:

1. Click **Man-Hour Shift** to set the man-hour shift details.
2. Click **Add** to pop up the man-hour shift setting window.



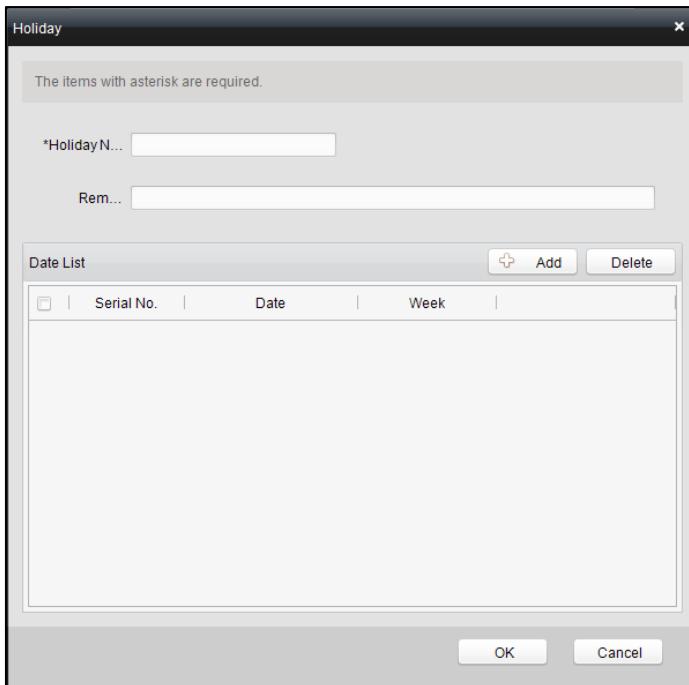
3. Set a shift name, and daily work duration.
 4. (Optional) Check the checkbox of latest on-work time, and set the latest on-work time.
 5. (Optional) Set the durations excluded from man-hour duration.
 6. Click **OK** to complete the operation.
 7. (Optional) You can edit or delete the shift by clicking **Edit** or **Delete**.
- Note:** After deleting the shift, its shift schedule will be deleted as well. For details about shift schedule, refer to *Shift Schedule Management*.

4.4.3 Holiday Management

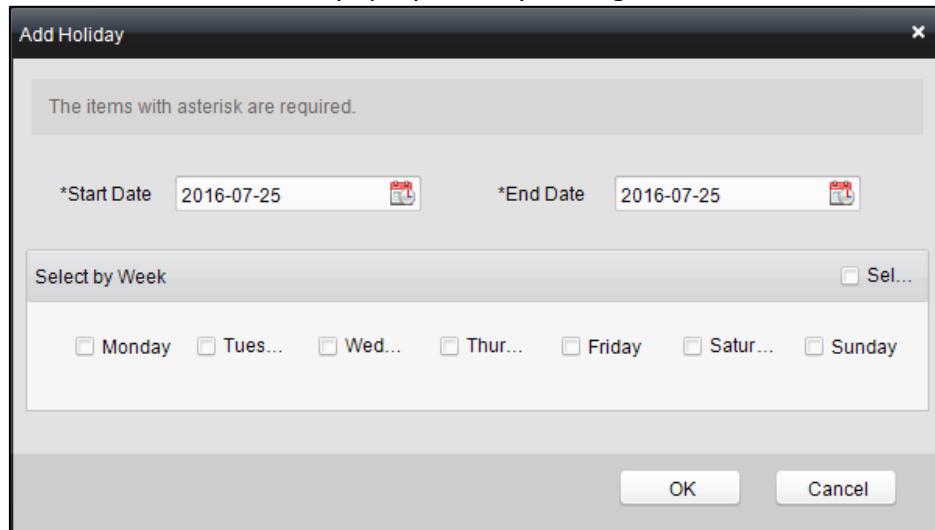
Steps:

1. Click **Holiday** tab to enter the holiday management interface.

2. Click **Add** button to pop up the holiday setting window.



- Click button to pop-up holiday adding window.



- Set the start date and end date, select the date of week, and click .

- Click to save the settings.

4.4.4 Shift Schedule Management

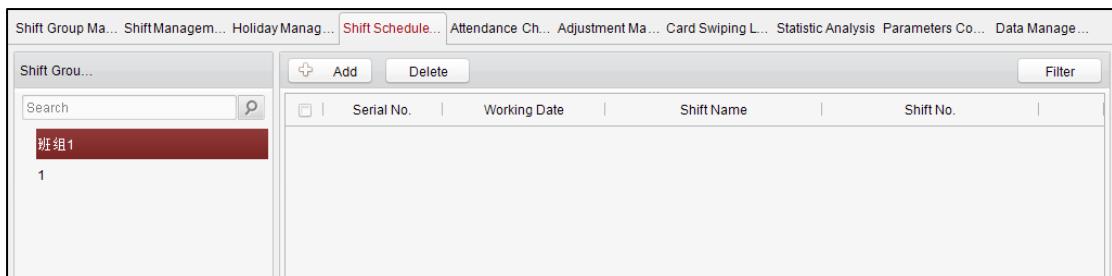
Purpose:

After setting the shift group and the corresponding shift and shift rule, you can set the shift schedule for the shifts.

Steps:

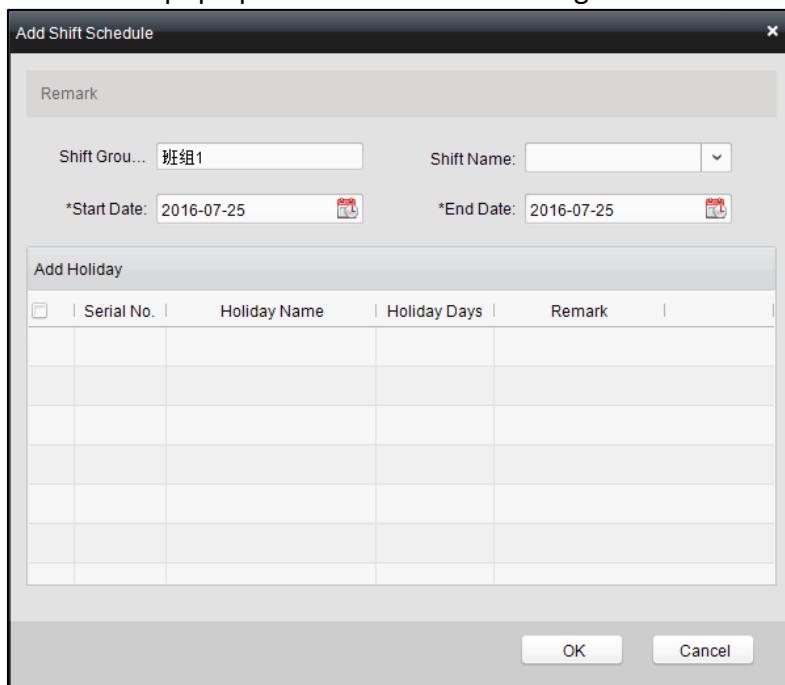
- Click the Shift Schedule tab to enter the shift schedule management interface.

Fingerprint Time Attendance Terminal



2. Select the shift group from the list on the left.

3. Click to pop up the shift schedule settings window.



4. Select the shift name from the drop-down list and set the start data and end data.

(Optional) You can check the checkbox of holiday to add the holiday shift.

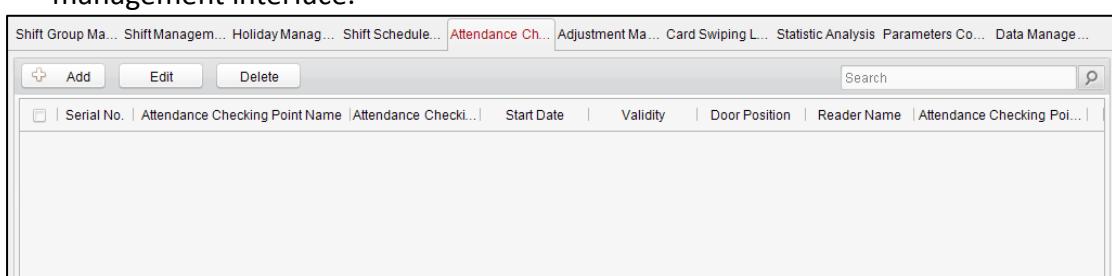
Click button to complete the operation.

5. Click to save the settings.

4.4.5 Attendance Check Point Management

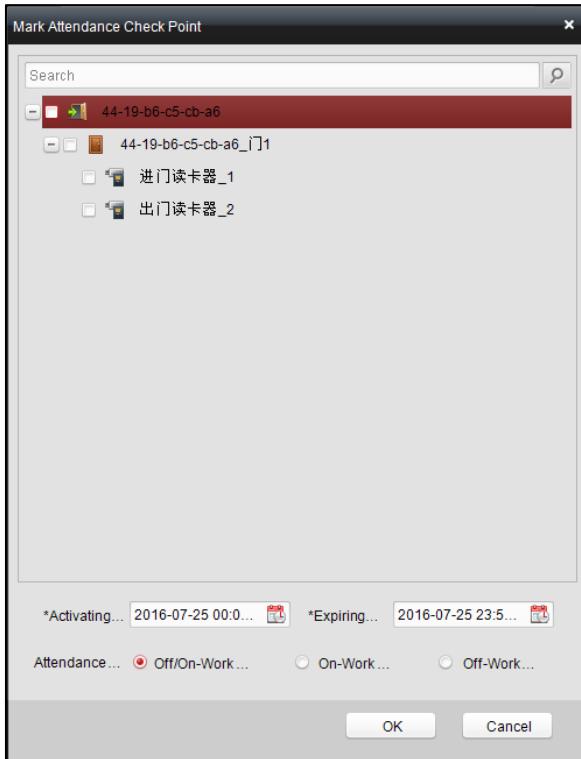
Steps:

1. Click the Attendance Check Point tab to enter the attendance check point management interface.



2. Click to pop up the adding attendance check point interface as

follows.



Check the select the card reader of the access control point and set the start date and the end date.

Select the check point type.

Click **OK** to save the adding.

The added check points will be displayed in the attendance check point list.

3. You can check the checkbox of a check point, and click **Edit** to pop up the attendance check point editing window.
You can edit the attendance check point name, start date, end date, and check point type, controller name, door position, and card reader name.
- Click **OK** to complete the operation.
4. You can check the checkbox of a check point and click **Delete** to delete the added check point.

4.4.6 Adjustment Management

Click the Adjustment tab to enter the adjustment management interface.

In this module, **Reason Management** and **List Management** can be realized.

Reason Management

✧ **Leave**

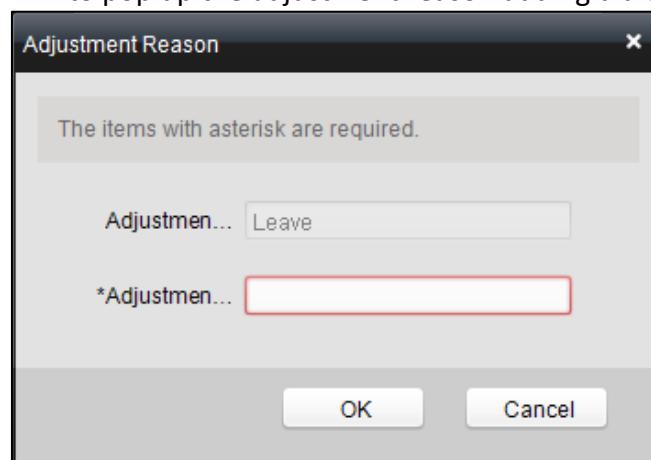
You can add, edit, and delete reasons for leave on the leave interface.

Steps:

1. Click **Leave** tab to enter the leave interface.

<input type="checkbox"/>	Serial No.	Reason Management
<input type="checkbox"/>	1	Personal Leave
<input type="checkbox"/>	2	Sick Leave
<input type="checkbox"/>	3	Marriage Leave
<input type="checkbox"/>	4	Bereavement Leave
<input type="checkbox"/>	5	Family Reunion Leave
<input type="checkbox"/>	6	Annual Leave
<input type="checkbox"/>	7	Maternity Leave
<input type="checkbox"/>	8	Paternity Leave

2. Click  **Add** to pop up the adjustment reason adding dialog box.



3. Enter the adjustment reason, and click  **OK** to save the adding.

Notes:

- The default adjustment reasons include leave for personal affairs, sick leave, marriage leave, funeral leave, home leave, annual leave, maternity leave, and paternity leave.
- You can check the checkbox of a reason and click  **Edit** to edit the reason, and click  **Delete** to delete the reason.

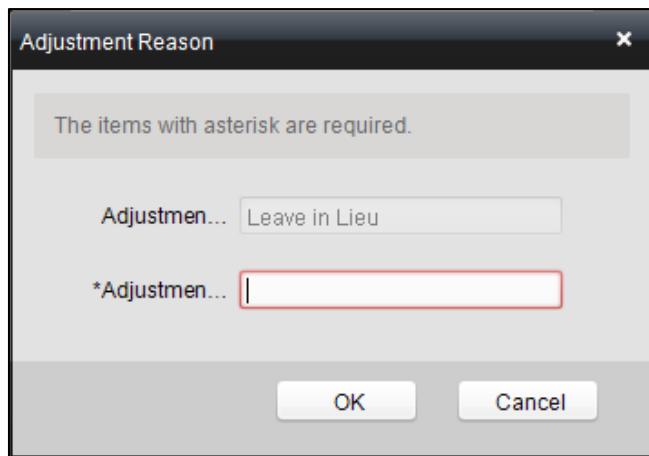
✧ **Leave in Lieu**

Steps:

1. Click **Leave in Lieu** tab to enter the leave-in-lieu interface.

<input type="checkbox"/>	Serial No.	Reason Management
<input type="checkbox"/>	1	Overtime Exchange Holiday
<input type="checkbox"/>	2	Business Trip Exchange Holiday

2. Click  **Add** to pop up the adjustment reason adding dialog box.



- Enter the adjustment reason, and click **OK**.

Notes:

- The default adjustment reasons for leave in lieu include overtime, and business trip.
- You can check the checkbox of a reason and click **Edit** to edit the reason, and click **Delete** to delete the reason.

✧ **Overtime**

Steps:

- Click the Overtime tab to enter the overtime interface.

		Add	Edit	Delete	Search	Print
		Reason Management				
<input type="checkbox"/>	1	Work Demand				
<input type="checkbox"/>	2	Workday Overtime				
<input type="checkbox"/>	3	Off Day Overtime				
<input type="checkbox"/>	4	Holiday Overtime				

- Click **Add** to pop up the adjustment reason adding dialog box.

- Enter the adjustment reason, and click **OK**.

Notes:

- The default adjustment reasons for overtime include work requirement, working day overtime, rest day overtime, and holiday overtime.
- You can check the checkbox of a reason and click **Edit** to edit the reason, and click **Delete** to delete the reason.

✧ **Card Replacement**

Steps:

- Click the Card Replacement tab to enter the following interface.

<input type="checkbox"/>	Serial No.	Reason Management
<input type="checkbox"/>	1	Forget to Swipe Card
<input type="checkbox"/>	2	Card Loss
<input type="checkbox"/>	3	Device Fault
<input type="checkbox"/>	4	Shift Rearrangement
<input type="checkbox"/>	5	Business Trip

2. Click  **Add** to pop up the adjustment reason adding dialog box.

3. Enter the adjustment reason, and click  **OK**.

Notes:

- The default adjustment reasons for card replacing include forget to swipe card, attendance card lost, device fault, shift adjustment, and business trip.
- You can check the checkbox of a reason and click  **Edit** to edit the reason, and click  **Delete** to delete the reason.

List Management

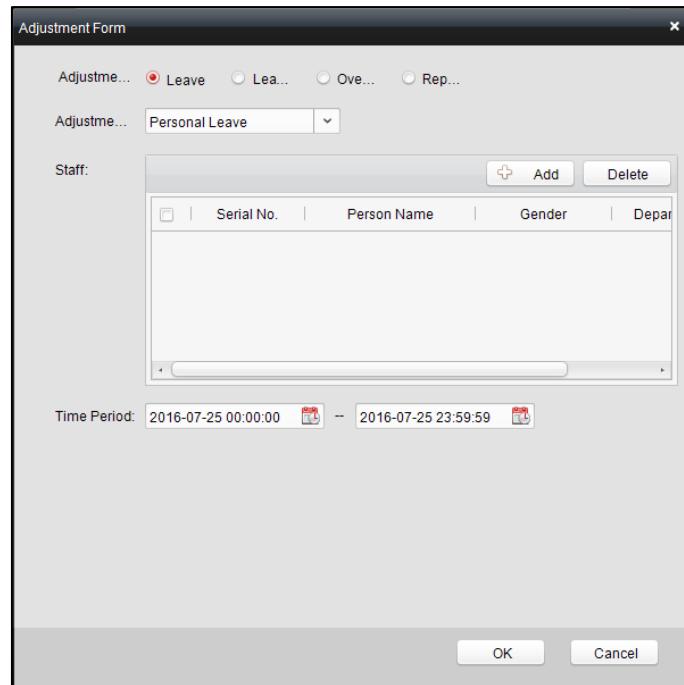
❖ **Enabled List**

Steps:

1. Click **Enabled List** tab to enter the enabled list interface.

<input type="checkbox"/>	Serial No.	Form No.	Person Name	Department Name	Start Time	End Time	Filter

2. Click  **Add** button to add an attendance management form.

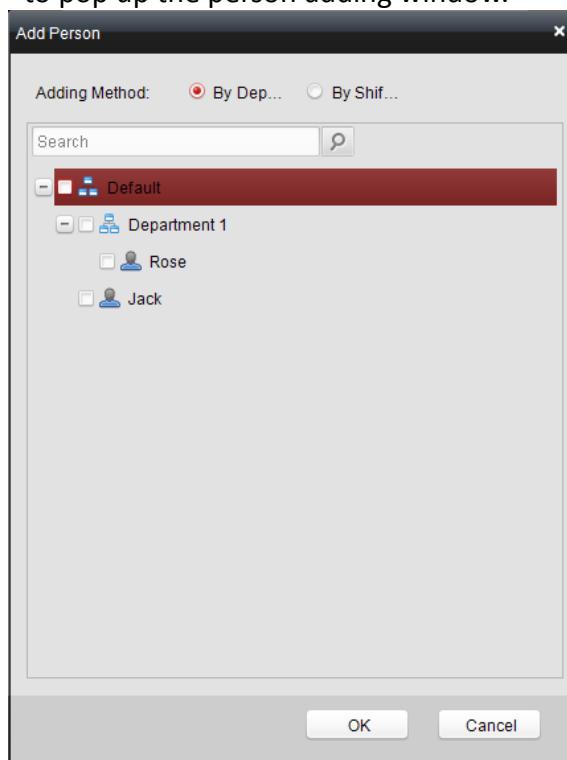


3. Select the adjustment type: leave, leave in lieu, overtime, and card replacement.

Leave, Leave in Lieu, and Overtime

- 1) Select the adjustment reason from the drop-down list.

- 2) Click to pop up the person adding window.



- 3) Select the adding type as by department or by shift group. Select the person and click .

- 4) Set the time duration.

❖ **Disabled List**

Steps:

1. In the Enabled List interface, check the checkbox of a piece of enabled list and click **Disable** to disable the list.
2. Click Disabled tab and the disabled list will be listed on the disabled interface.

3. You can check the checkbox and click **Delete** to delete the disabled list.

4.4.7 Card Swiping Log Query

Click **Swiping Log** tab to enter the card swiping log searching and viewing interface.

You can search the card swiping log by two query types: **By Shift Group**, and **By Department**.

Input other search conditions and click **Search** to start query the card swiping log.

4.4.8 Statistic Analysis

Press the Statistic Analysis tab to enter the statistic analysis interface.

On the statistic analysis interface, you can search the attendance analysis table, attendance result statistic table, and attendance rate statistic table.

Attendance Analysis Table

Press the Attendance Analysis Table tab to enter the attendance analysis interface.

The screenshot shows the 'Attendance Analysis Table' tab selected in a software interface. The left sidebar has tabs for 'Attendance Analysis Table', 'Attendance Result Statistic Table', and 'Attendance Rate Statistic Table'. The main area has search filters for 'Shift Type' (Normal Shift), 'Department' (Default), 'Start Date' (2015-11-12 00:00:00), and 'End Date' (2015-11-12 23:59:59). Below the filters is an 'Export' button. The results table is titled 'Attendance Analysis Table' and shows data for a single employee P1. The columns include Name, Department, Date, Shift Name, Time Period, On-Work Attendance Checking Time, and Off-Work Attendance Checking Time. The data row for P1 shows Default as the department, 2015-11-12 as the date, Normal Shift1 as the shift name, 1 as the time period, 2015-11-12 08:30:48 as the on-work checking time, and No as the off-work checking time.

Notes:

- You can search the attendance statistics by different shift type: Normal Shift, or Man-Hour Shift.
- You can search the attendance statistics by department.
- You can search the attendance statistics by start date and end date.

Attendance Result Statistic Table

Press the Attendance Result Statistic Table tab to enter the attendance result analysis interface.

The screenshot shows the 'Attendance Result Statistic Table' tab selected in a software interface. The left sidebar has tabs for 'Attendance Analysis Table', 'Attendance Result Statistic Table', and 'Attendance Rate Statistic Table'. The main area has search filters for 'Shift Type' (Normal Shift), 'Department' (Default), 'Start Date' (2015-11-12 00:00:00), and 'End Date' (2015-11-12 23:59:59). Below the filters is an 'Export' button. The results table is titled 'Attendance Result Statistic Table' and shows data for a single employee P1. The columns include Name, Department, Required Attendance, Actual Attendance, Attendance Rate, Late Times, and Early-Leave Times. The data row for P1 shows Default as the department, 1 as the required attendance, 1 as the actual attendance, 100.00% as the attendance rate, 0 as the late times, and 0 as the early-leave times.

Notes:

- You can search the attendance result statistics by different shift type: Normal Shift, or Man-Hour Shift.
- You can search the attendance result statistics by department.
- You can search the attendance result statistics by start date and end date.

Attendance Rate Statistic Table

Press the Attendance Rate Statistic Table tab to enter the attendance rate analysis interface.

Name	Department	Date	Shift Name	Day Required At...	Day Actual Atten...	Day Attendance
P1	Default	2015-11-12	Normal Shift1	1	1	100.00%

Notes:

- You can search the attendance rate statistics by different shift type: Normal Shift, or Man-Hour Shift.
- You can search the attendance rate statistics by department.
- You can search the attendance rate statistics by start date and end date.

4.4.9 Parameters Configuration

Steps:

1. Click the Parameters Configuration tab to enter the parameters configuration interface.

2. Select the attendance effecting type, data saving time, data expiring prompt.
3. Set the attendance checking log clearing time.
4. Click **Save** to save the parameters.

4.4.10 Data Management

Steps:

1. Click the Data Management tab to enter the data management interface.

2. Select the date and time period for calculation and click **Calculate Attendance Data** to start calculating the attendance data.
3. After calculation, you can also export and import the attendance data.

4.5 Checking Status and Event

Purpose:

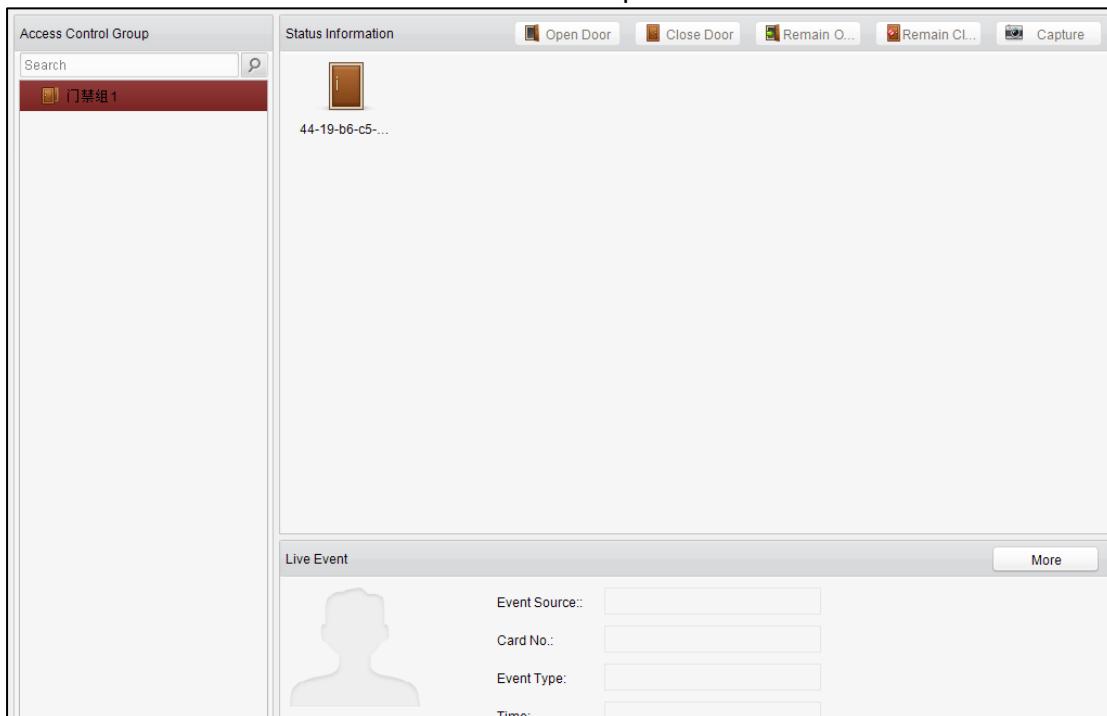
In this section, you are able to anti-control the status of the door and to check the event report of the control point.

4.5.1 Status Monitor

Purpose:

You can anti-control the door status and check the real-time access event information for the control point.

Click the  icon on the control panel to enter the interface.



Access Anti-control

Purpose:

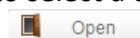
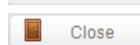
You can control the status for a single control point (a door) in this section.

Steps:

1. Enter the status monitor page.



2. Click on the icon 

 : Click on the button to open the door once.
 : Click on the button to close the door once.

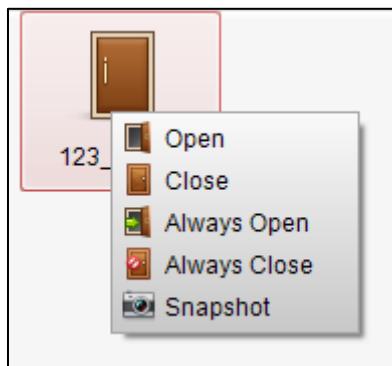
 : Click on the button to keep the door open.

 : Click on the button to keep the door closed.

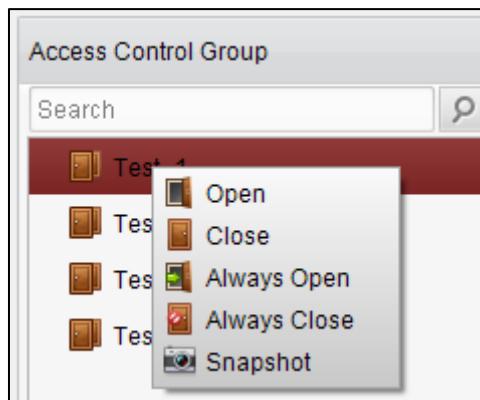
Note: Do not support the Capture function.



4. You can also right click the icon and to select a status for the door.



5. (Optional) Right click on a group in the Group list and to select a door status for the group.



Notes:

- If the status is selected as **Remain Open/Remain Closed**, the door will keep open/ closed until a new anti-control command being made.
- The function of picture capturing cannot be realized until the storage server is installed.
- Do not support the Capture function.

Access Status

The door status will be represented instantly by the change of icon on the **Access Information** panel if the access event is triggered or an anti-control command is made.



Note: The attendance device does not support the function.

Real-Time Event

You can check the Real-time information of the access event on this panel. Click **More** to enter the Access Event page to view more event information.

The screenshot shows a "Live Event" panel with a placeholder user profile icon. Below it are four input fields: "Event Source:", "Card No.", "Event Type:", and "Time:". A "More" button is located in the top right corner.

4.5.2 Access Control Event

Purpose:

You can view real-time access event (such as swiping to open the door, unrecognized card number, duration group error, etc.) information in this section.

Click the icon on the control panel to enter the interface.

The screenshot shows the "Access Control Event Information" interface. On the left is a large list area with a header row containing columns for Serial Number, Event Type, Card Holder, Card Type, Card No., Event Time, Event Source, and Direction. On the right is a "Card Holder Information" panel displaying a placeholder user profile and several input fields: Person No., IC Card No., Belong to..., Contact No., and Contact Ad... .

Steps:

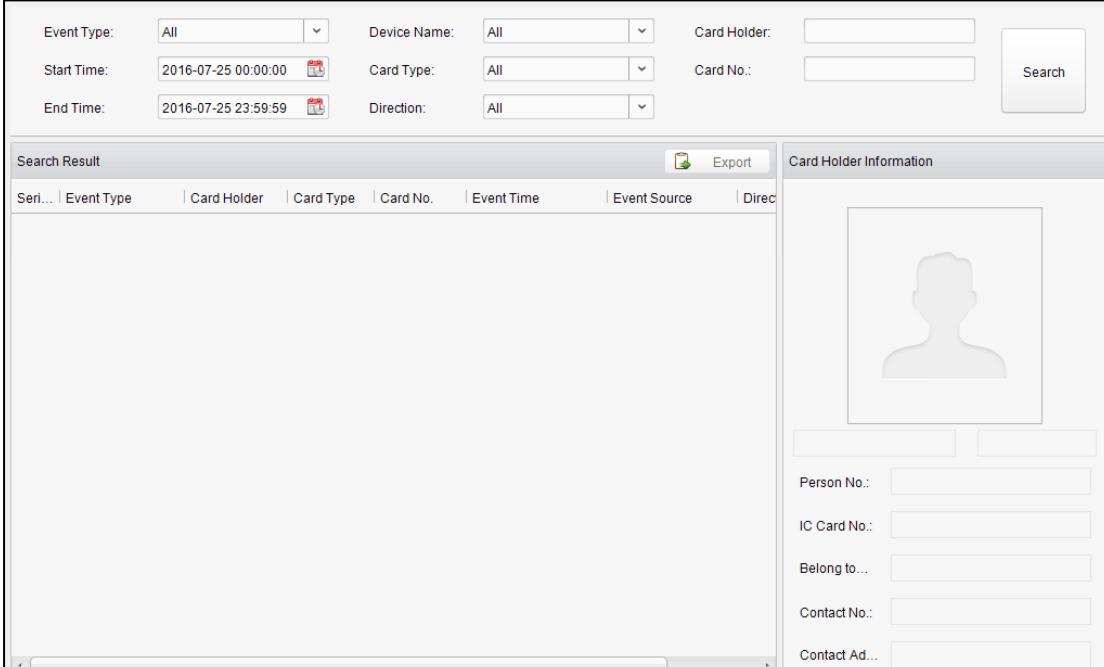
1. Enter the access event page.
2. View the event information in the event list.
3. Click on an event to view the information of the card holder on the **Person Information** panel on the left side of the page.

4.5.3 Event Search

Purpose:

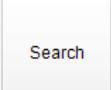
You can search historical access event according to the search criteria (such as event type, name of the person, card No. or start/end time) in this section.

Click the  icon on the control panel to enter the interface.



The screenshot shows the 'Event Search' interface. At the top, there are search filters: Event Type (All), Device Name (All), Card Holder (empty), Start Time (2016-07-25 00:00:00), End Time (2016-07-25 23:59:59), Card Type (All), Card No. (empty), and Direction (All). Below the filters is a 'Search' button. To the right is a 'Card Holder Information' panel featuring a placeholder profile picture and fields for Person No., IC Card No., Belong to..., Contact No., and Contact Ad... .

Steps:

1. Enter the event search page.
 2. Enter the search criteria (event type/ person name/ card No/ start &end time).
- 
3. Click **Search** to get the search results.
 4. View the event information in the event list.
 5. Click on an event to view the information of the card holder on the **Person Information** panel on the left side of the page.

4.6 System Maintenance

4.6.1 Log Management

Purpose:

The log files of the Access Control System and the devices that connected to the Access Control System can be searched for checking.

Click the  icon on the control panel to open the Log Search page.

Configuration Logs Searching

Purpose:

The Configuration Log files of the Access Control System can be searched by time ,including One-card Configuration, Access Control Configuration, Downloading Permission and System Configuration.

Steps:

1. Open the Log Search page.
2. Select the radio button of Configuration Logs.
3. Select the Operation Type of log files.
4. Click the icon to specify the start time and end time.
5. Click **Search**. The matched log files will display on the list.

You can check the operation time, log type and other information of the logs.

Note: Please narrow the search condition if there are too many log files.

Control Logs Searching

Purpose:

The Control Log files of the Access Control System can be searched by time ,including Access Control and Log Search.

Steps:

1. Open the Log Search page.
2. Select the radio button of Control Logs.
3. Select the Operation Type of log files.
4. Click the icon to specify the start time and end time.
5. Click **Search**. The matched log files will display on the list.

You can check the operation time, log type and other information of the logs.

Note: Please narrow the search condition if there are too many log files.

Searching Configuration Log

Searching One-card Configuration Logs

Purpose:

The One-card Configuration Log files include departments, persons and cards log files. One-card Configuration of the Access Control System can be operated as adding ,modifying and deleting logs.

Steps:

1. Open the Log Search page.
2. Select the radio button of Configuration Logs.
3. Select the operation type as One-card Configuration.
4. Click the icon  to specify the start time and end time.
5. Click **Search**. The matched log files will display on the list.

You can check the operation time, log type and other information of the logs.

Note: Please narrow the search condition if there are too many log files.

Searching Access Control Configuration Logs

Purpose:

The Access Control Configuration Log files include Access Control devices log files. Access Control Configuration of the Access Control System can be operated as adding, modifying and deleting door groups or doors and access control device permission operations.

Steps:

1. Open the Log Search page.
2. Select the radio button of Configuration Logs.
3. Select the operation type as Access Control Configuration.
4. Click the icon  to specify the start time and end time.
5. Click **Search**. The matched log files will display on the list.

You can check the operation time, log type and other information of the logs.

Note: Please narrow the search condition if there are too many log files.

Searching Downloading Permission Logs

Purpose:

The Downloading Permission Log files include downloading permission log files, and no record for downloading permission failure log files.

Steps:

1. Open the Log Search page.
2. Select the radio button of Configuration Logs.
3. Select the operation type as Downloading Permission.
4. Click the icon  to specify the start time and end time.
5. Click **Search**. The matched log files will display on the list.

You can check the operation time, log type and other information of the logs.

Note: Please narrow the search condition if there are too many log files.

Searching System Configuration Logs

Purpose:

The System Configuration Log files of the Access Control System can be searched as system configuration interface log files.

Steps:

1. Open the Log Search page.
2. Select the radio button of Configuration Logs.

3. Select the operation type as System Configuration Logs.
4. Click the icon  to specify the start time and end time.
5. Click **Search**. The matched log files will display on the list.
You can check the operation time, log type and other information of the logs.

Note: Please narrow the search condition if there are too many log files.

Searching Control Log

Searching Access Control Logs

Purpose:

The Access Control Log files of the Access Control System include door groups and doors access control logs and door on/off control log files.

Steps:

1. Open the Log Search page.
2. Select the radio button of Control Logs.
3. Select the operation type as Access Control Logs.
4. Click the icon  to specify the start time and end time.
5. Click **Search**. The matched log files will display on the list.
You can check the operation time, log type and other information of the logs.

Note: Please narrow the search condition if there are too many log files.

Log Search

Purpose:

The Log Search of the Access Control System include informations for configuration log files and control log files.

Steps:

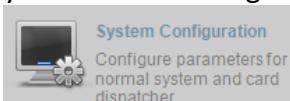
1. Open the Log Search page.
2. Select the radio button of Control Logs.
3. Select the operation type as Log Search.
4. Click the icon  to specify the start time and end time.
5. Click **Search**. The matched log files will display on the list.
You can check the operation time, log type and other information of the logs.

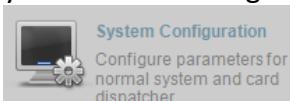
Note: Please narrow the search condition if there are too many log files.

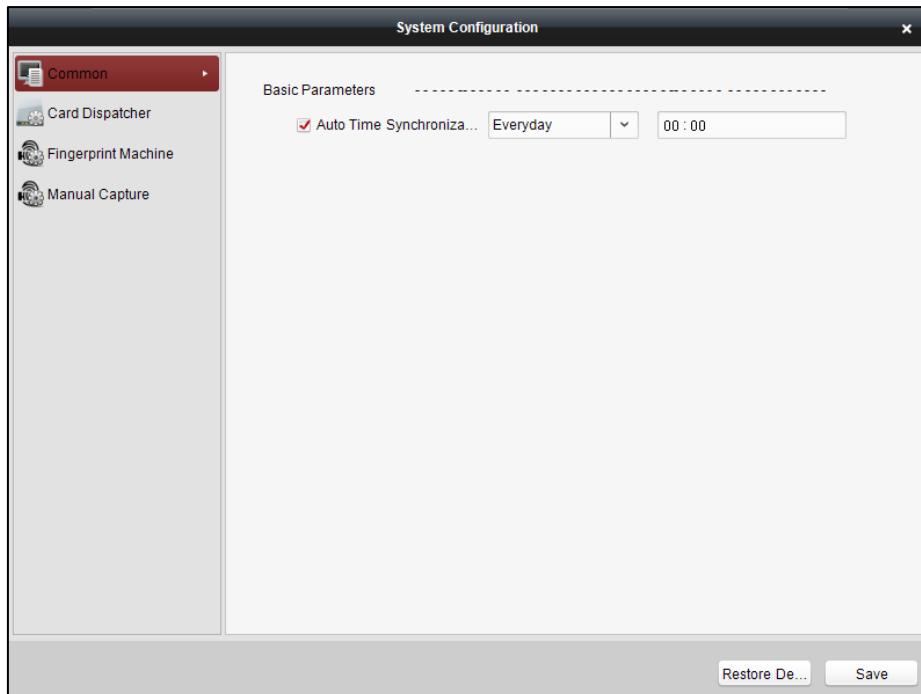
4.6.2 System Configuration

Purpose:

The general parameters, Auto Time Adjustment and Card Reader of the Access Control System can be configured.



Click the  icon on the control panel to open the System Configuration page.



Auto Time Synchronization

The Auto Time Synchronization of the Access Control System can operate auto time adjustment to all access control devices of the Access Control System according to specified period and time.

Card Reader Configuration

The Card Reader Configuration is for Access Control System to read the card by setting Card Reader parameters. For now D8E-U-A-III and DS-K1F100-M card reader types are supported.

Fingerprint Machine

The Fingerprint Machine is for Access Control system to collect fingerprints.

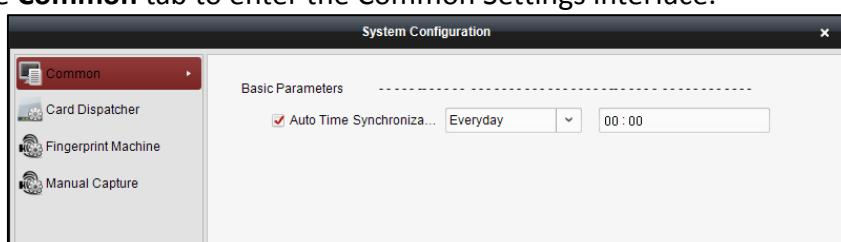
Manual Capture Configuration

The Manual Capture Configuration is for Access Control system to take photos remotely.

Auto Time Synchronization

Steps:

1. Open the System Configuration page.
2. Click the **Common** tab to enter the Common Settings interface.



3. Tick the checkbox to enable Auto Time Synchronization.
4. Select the matched day and input the time to operate the time adjustment.
5. Click **Save** to save the settings.

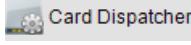
Note: You can click **Restore De...** (Restore Default Value) to restore the defaults of all the local configurations.

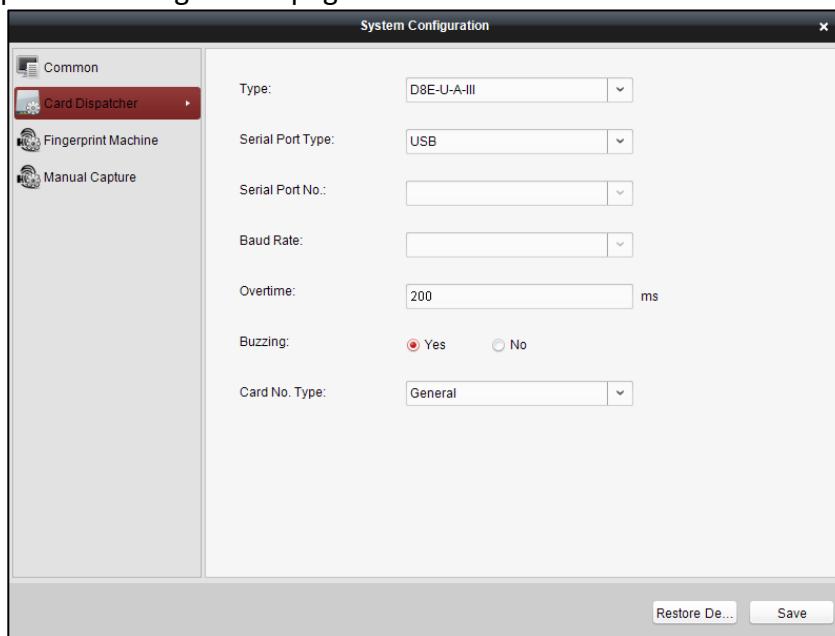
Card Dispenser Configuration

Purpose:

The Card Reader Configuration of the Access Control System can configure device type, connection mode, serial port, baud rate and other parameters of the Card Reader Configuration.

Steps:

1. Click the  Card Dispatcher icon on the System Configuration interface to open the Card Dispatcher Configuration page.



2. Select the device type, serial port type, serial port, baud rate, and other parameters of the Card Dispatcher.
3. Click the save button to save the settings.

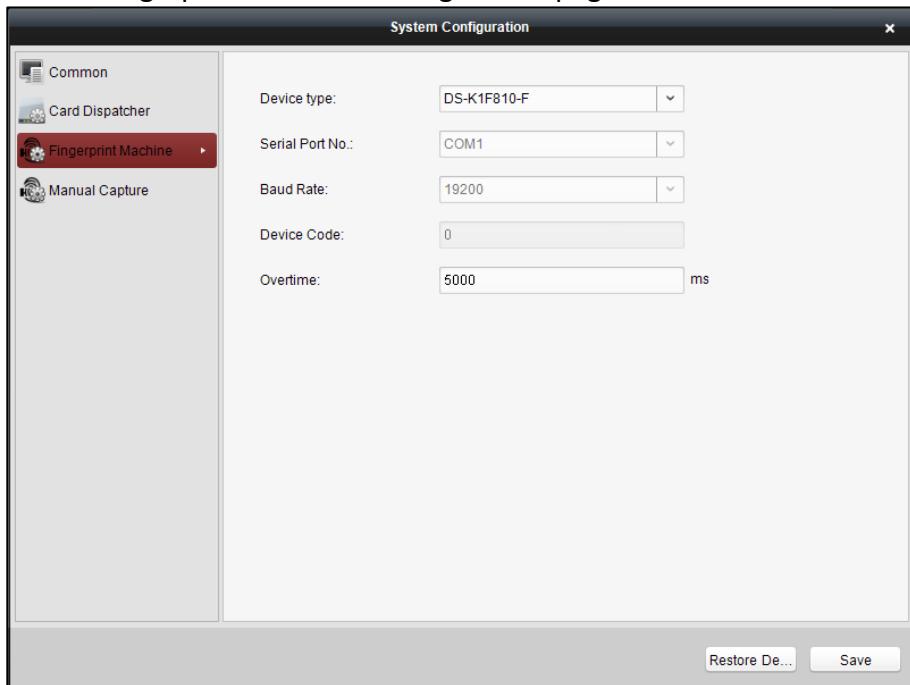
Note:

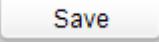
- **Configuration Instruction**
 - DS-K1F100-M:** select Serial Port Mode as accessing mode (currently only support serial port mode), the serial port NO. is the COM port NO. of the computer. Set other parameters as default.
 - D8E-U-A-III:** select USB Mode as accessing mode (currently only support USB mode). Set other parameters as default.
- It is supported using card type as regular and Wiegand.
- When the BEEP is selected as “YES”, the audio will be off when you click the “SAVE” if the Card Reader Configuration is set wrong; the audio will be on when you click the **Save** and when you insert the card reader if the configuration is set correct.
- You can click **Restore De...** (Restore Default Value) to restore the defaults of all the local configuration.

Fingerprint Machine Configuration

Steps:

1. Click the  icon on the System Configuration interface to open the Fingerprint Machine Configuration page.



2. Select the device type, serial port number, baud rate, device code, and overtime parameters of the fingerprint machine.
3. Click  to save the settings.

Note:

- It is supported using device type as Optical Fingerprint Collecting Instrument.
- The serial port number should correspond to the serial port number of PC.
- The baud rate should be called according to the external fingerprint card dispatcher. The default value is 19200.
- Overtime refers to the valid fingerprint collecting time. If the user does not input a fingerprint or inputs a fingerprint unsuccessfully, the device will indicate that the fingerprint collecting is over.
- You can click  (Restore Default Value) to restore the defaults of all local settings.

Chapter 5 Appendix

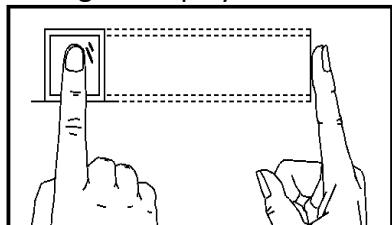
5.1 Tips for Scanning Fingerprint

Recommended Finger

Forefinger, middle finger or the third finger.

Correct Scanning

The figure displayed below is the correct way to scan your finger:

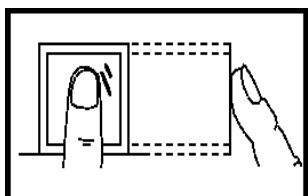


You should press your finger on the scanner horizontally. The center of your scanned finger should align with the scanner center.

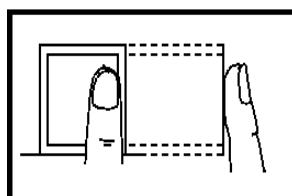
Incorrect Scanning

The figures of scanning fingerprint displayed below are wrong:

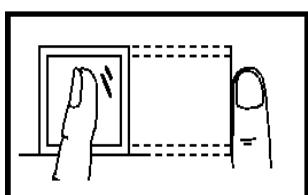
Vertical



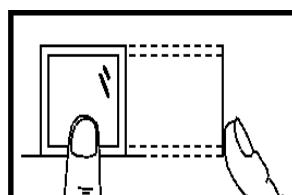
Edge I



Side



Edge II



Environment

The scanner should avoid direct high light, high temperature, humid conditions and rain.

When it is dry, the scanner may not recognize your fingerprint successfully. You can blow your finger and scan again after drying the finger.

Others

If your fingerprint is shallow, or it is hard to scan your fingerprint, we recommend you to use other authentication methods.

If you have injuries on the scanned finger, the scanner may not recognize. You can change another finger and try again.

5.2 Attendance Record Delete Rule

5.2.1 Enabling Record Delete

You are able to configure the percentage of the attendance record over threshold prompt.

- 1) When the record reaches the threshold, an alarm of the attendance record over limit value will be displayed on device screen. The alarm information is: Log will be full, export the report. Card authentication is available. The interface will be back to the alarm interface after authenticating.
- 2) When the record is full, an alarm of the attendance record over limit value will be displayed on the device screen. The alarm information is: Log is full, export the report. Card authentication is available. And the first 3000 attendance records will be deleted automatically. The interface will be back to the alarm interface after authenticating.
- 3) Deleting by time and deleting all are available when deleting the attendance records.

5.2.2 Disabling Record Delete

You are able to configure the percentage of the attendance record over threshold prompt.

- 1) When the record reaches the threshold, an alarm of the attendance record over limit value will be displayed on device screen. The alarm information is: Log will be full, export the report. Card authentication is available. The interface will be back to the alarm interface after authenticating.
- 2) When the record is full, an alarm of the attendance record over limit value will be displayed on the device screen. The alarm information is: Log is full, export the report. Card authentication is available. And there will be no new attendance records added. The interface will be back to the alarm interface after authenticating.
- 3) Deleting by time and deleting all are available when deleting the attendance records.

5.3 Attendance Performance

Content	Maximum Configurable Parameters
Department	32
Normal Shift	32
Man-Hour Shift	32
Holiday	32
Holiday Group	64
Schedule by Department	32
Schedule by Individual	32

5.4 Attendance Report Table

5.4.1 Description of Attendance Report File Name

File Name Rule

att_Report Type_dev_Device No._Date_Time.xls

Report Type

abnormal: The Abnormal Attendance Record table.

abnormal2: When the row of the Abnormal Attendance Record table is more than 65000, the record will be export in two tables. Here abnormal2 refers to the second table.

summary: The Attendance Report table.

record: The Attendance Record table.

schedule_cfg: The shift schedule configuration table.

ord_class: The normal shift configuration table.

work_class: The man-hour shift configuration table.

Device No.

A serial of numbers from 0 to 8.

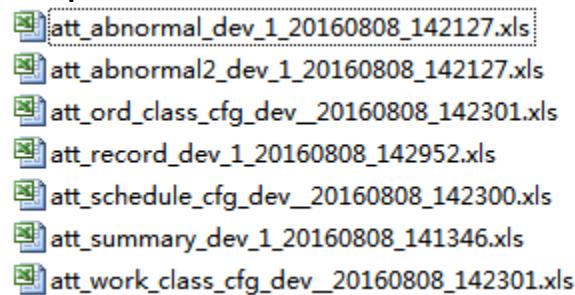
Date

YYYYMMDD

Time

HHMMSS

Example



5.4.2 Attendance Report Table Description

Shift Settings Table							
Special Shift: 1-1 Normal Shift1 2-1 Man-Hour Shift1 0 No Shift 3Holiday							
Date			2016/4/10				
Employee ID	Name	Department	1	2	3	4	5

Shift Settings Table: All users shift schedule information for a period will be displayed in this table. You are able to set the shift information and the holiday (No attendance recorded during the holiday) in shift schedule configuration.

1. ID No.: The user's ID No.
2. Name: The user's name.
3. Department: The department of the user.
4. Header: The number from 1 to 31 refers to the shift schedule days. For example: If entering 2016.8.26 to 2016.9.15, header 1 refers to the shift schedule information in 2016.8.26.

Normal Shift Schedule					
Shift No.	Shift Name	Period 1		Period 2	
		On Work	Off Work	On Work	Off Work

Normal Shift Table: Up to 4 periods can be configured in normal shift configuration. You are able to take attendance according to the configured period.

For example: If set Period 1 to 9:00 (On Work) and 17:00 (Off Work), it is effective for the user to take attendance between 9:00 and 17:00.

Combining with the attendance rule, you are able to set multiple attendance types.

Man-Hour Shift Schedule					
Shift No.	Shift Name	Duration	Latest On-Work Time	Break Period 1	
				Start	End

Man-Hour Shift Table: Set the Man-Hour Shift working duration. If set the Latest On-Work Time to 0, all users are attendant. If set the Latest On-Work Time to more than 0, the user will be absent by taking attendance after the configured time. The Break Period will not be configured in the man-hour shift.

For example: If set the working duration to 6 hours, the on-work time to 09:00, the off-work time to 17:00 and the break period 1 to 12:00 to 13:00, the user actual working hour is 17:00 - 09:00 - (13:00 - 12:00).

Fingerprint Time Attendance Terminal

Abnormal Attendance Record						
Date: 2016/04/01 ~2016/04/30						
Employee ID	Name	Department	Date	Period 1		Period 2
				On Work	Off Work	On Work

Abnormal Attendance Record Table: Calculate the abnormal attendance according to the attendance records and the shift schedule configuration.

1. Employee ID: The user's ID No.
2. Name: The user's name.
3. Department: The department of the user.
4. Date: the date of the data generated.
5. Period 1 to Period 4: Up to 4 periods can be configured. It records the attendance time of each user every day.
6. Late (Minute): The on-work attendance time is later than the normal on-work time.
7. Early Leaving (Minute): The off-work attendance time is earlier than the normal off-work time.
8. Absence (Minute): No normal working hour.
9. Total: The normal working hour of the day.

Attendance Record											
Attendance Checking Time: 2016/04/01~2016/04/30 Tabulation Time: 2016/04/30											#
1	2	3	4	5	6	7	8	9	10		#
Employee ID: 1	Name: 111						Department: aaa				
Employee ID: 2	Name: 222						Department:				
bbb											

Attendance Record Table: Input the start time and the end time to export the effective attendance data during the configured duration.

1. Header: The number from 1 to 31 refers to the shift schedule days.
For example: If entering 2016.8.26 to 2016.9.15, header 1 refers to the shift schedule information in 2016.8.26.
2. Employee ID: The user's ID No.
3. Name: The user's name.
4. Department: The user's department.

Attendance Report						
Counting Date: 2016/04/01 ~2016/04/30						
Employee ID	Name	Department	Duration (Hour:Munite)		Late	
			Standard	Actual	Frequency	Minute
1	111	aaa	12:00	11:00	1	20

2	222	bbb	12:00	11:00	1	30
---	-----	-----	-------	-------	---	----

Attendance Report Table: Enter the start time and the end time to calculate the user attendance information via the shift information and the holiday information according to the shift schedule configuration.

1. Employee ID: The user's ID No.
2. The user's name.
3. Department: The user's department.
4. Duration:

Standard: Total standard working hours in the duration.

Actual: Total actual working hours in the duration.

$$\text{Actual Hours} = \text{Standard Value} - \text{Late Hours} - \text{Early Leaving Hours}$$

5. Late: The on-work attendance time is later than the normal on-work time.

Frequency: Late arriving for no more than once every day.

Minute: All late arriving minutes in the duration.

6. Early Leaving: The off-work attendance time is earlier than the normal off-work time.

Frequency: Early leaving for no more than once every day.

Minute: All early leaving minutes in the duration.

7. Over Time: No records.

8. Attendance Days:

Standard: Standard attendance days in a duration, excluding the holidays and the days without shift schedule.

Actual: Actual attendance days in a duration. Actual Days = Standard Days - Absent Days

9. Business: No records.

10. Absence: Do not take attendance in the normal working days.

11. Leave: No records.

1000001060829



First Choice for Security Professionals

HIKVISION | www.hikvision.com