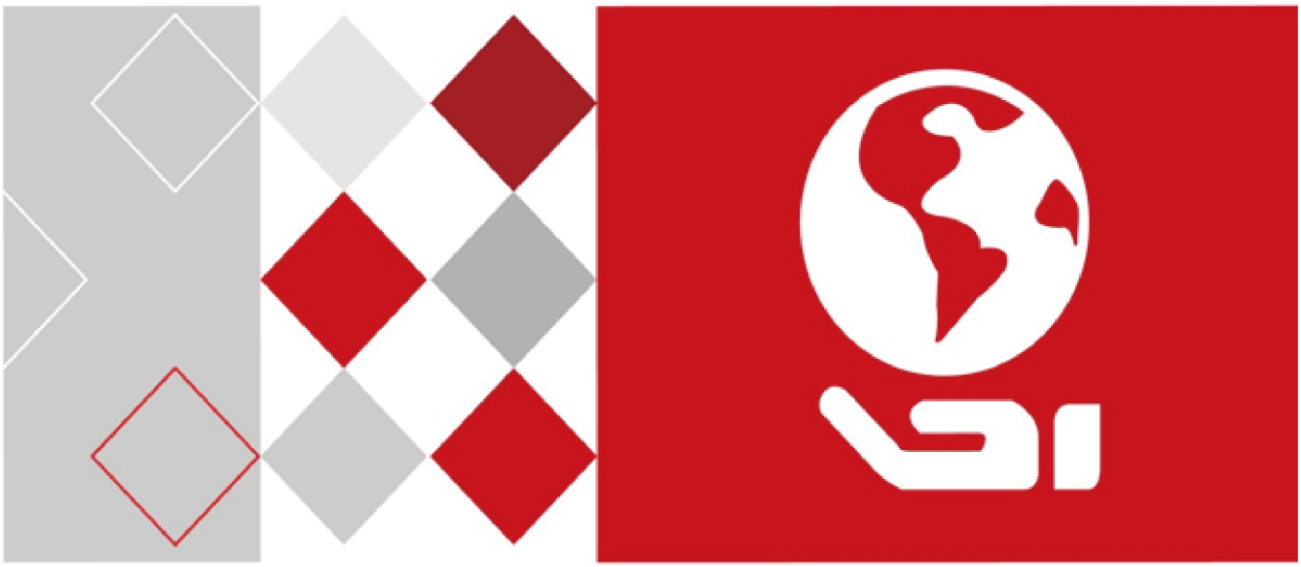
HIKVISION



Fingerprint Time Attendance Terminal

User Manual

UD06737B

User Manual

This manual is applied for fingerprint time attendance terminal.

Name	Model	Note
Fingerprint Time Attendance Terminal	DS-K1A801F	Without Battery
	DS-K1A801MF	
	DS-K1A801EF	
	DS-K1A801F-1	
	DS-K1A801MF-1	
	DS-K1A801EF-1	
	DS-K1A801F-B	With Battery
	DS-K1A801MF-B	
	DS-K1A801EF-B	
	DS-K1A802F	Without Battery
	DS-K1A802F-1	
	DS-K1A802MF	
	DS-K1A802MF-1	
	DS-K1A802EF	
	DS-K1A802EF-1	
	DS-K1A802F-B	With Battery
	DS-K1A802MF-B	
	DS-K1A802EF-B	

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

Trademarks

Disclaimer

REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. OUR COMPANY 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, OUR COMPANY 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. OUR COMPANY 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**

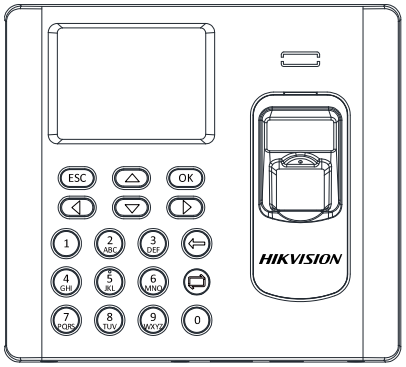
- Do not drop the device or subject it to physical shock, and do not expose it to high electromagnetism radiation. Avoid the equipment installation on vibrations surface or places subject to shock (ignorance can cause equipment damage).
- Do not place the device in extremely hot (refer to the specification 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.

Table of Contents

Chapter 1Overview

1.1 Introduction



DS-K1A801 Series and DS-K1A802 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. (The models with -1 do not support the wireless network function.)

1.2 Main Features

1.2.1 DS-K1A801F/MF/EF, DS-K1A801F/MF/EF-B, DS-K1A802F/MF/EF and DS-K1A802F/MF/EF-B 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 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
- Up to 4 login methods for admin:
  1) Login via fingerprint, employee ID No. + password, or device password for DS-K1A801F, DS-K1A801-B, DS-K1A802F and DS-K1A802F-B
  2) Login via fingerprint, employee ID No. + password, device password or card for DS-K1A801MF/EF, DS-K1A801MF/EF-B, DS-K1A802MF/EF, and DS-K1A802 MF/EF-B
- Different authentication types according to different device models:
  1. Fingerprint (DS-K1A801F/DS-K1A801F-B/DS-K1A802F/DS-K802F-B)

2. EM card reading and fingerprint
   (DS-K1A801EF/DS-K1A801EF-B/DS-K1A802EF/DS-K802EF-B)
3. Mifare card reading and fingerprint
   (DS-K1A801MF/DS-K1A801MF-B/DS-K1A802MF/DS-K802MF-B)

- The model DS-K1A801F-B, DS-K1A801EF-B and DS-K1A801MF-B support power supply by lithium battery. When the main power is off, the system will change the power supply method to lithium battery supply automatically
- Check the device running status via the Watchdog. When exceptional status occurs, the device will reboot automatically
- Remotely control via the iVMS-4200 client software
- Remotely collecting fingerprints is available
- The third party arming is available.
- Supports transmitting data via Hik EHome to realize the whole network transmitting.
- Activates via device.

1.2.2 DS-K1A801F/MF/EF-1 and DS-K1A802F/MF/EF-1 Features

- 2.8-inch LCD display screen
- Transmission modes of wired network (TCP/IP)
- Max. 800 users, 800 fingerprints and 800 access control events 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
- Up to 4 login methods for admin:
  1) Login via fingerprint, employee ID No. + password, or device password for DS-K1A801F-1 and DS-K1A802F-1
  2) Login via fingerprint, employee ID No. + password, device password or card for DS-K1A801MF/EF-1 and DS-K1A802 MF/EF-1
- Different authentication types according to different device models:
  1. Fingerprint (DS-K1A801F-1 Series and DS-K1A802F-1)
  2. EM card reading and fingerprint (DS-K1A801EF-1 Series and DS-K1A802EF-1 Series)
  3. Mifare card reading and fingerprint (DS-K1A801MF-1 Series and DS-K1A802MF Series)

- Check the device running status via the Watchdog. When exceptional status occurs, the device will reboot automatically
- Remotely control via the iVMS-4200 client software
- Remotely collecting fingerprints is available
- The third party arming is available.
- Supports transmitting data via Hik EHome to realize the whole network transmitting.
- Activates via device.

1.3 Appearance

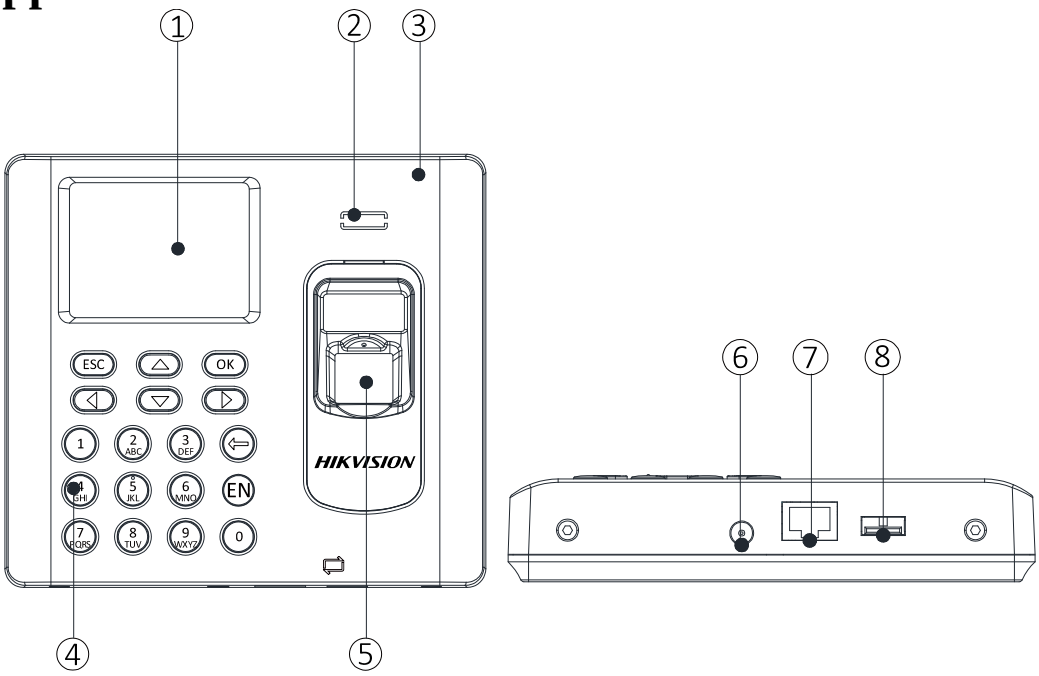


Table 1-1 Description of DS-K1A801 Series Model

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

1.4 Keypad Description

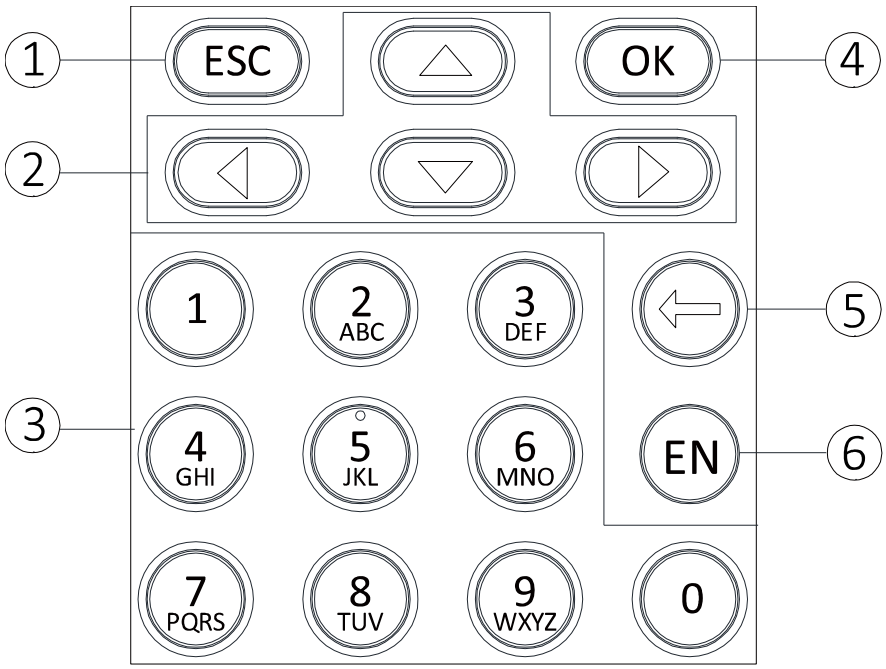


Table 1-2 Description of Keys

No.	Description
1	**Exiting Key:** Press the button to exit the menu.
2	**Direction Keys:** Use △, ▽, ◁, ▷ to move the cursor in the menu.
3	**Numeric Keys/Letter Keys:** • Press to input numbers or letters. • Long press Key 6 for 3s to enter One-Touch Wi-Fi Settings mode. You can set the Wi-Fi for the device via the App on the phone. Press Key 6 again to exit the mode after setting Wi-Fi completely. ***Note:*** The models with -1 do not support One-Touch Wi-Fi Settings mode.
4	**OK Key:** Press to confirm operations. Press and hold the key for 3s to login the main interface.
5	**Deleting Key:** • Press to delete the letters or numbers one by one in the textbox. • Long-press to clear all contents in the textbox. • If the device model contains "-B", long-press the deleing key for 2s to enter the powering off interface. Press the **OK** key to power off.
6	**Editing Key:** Press to enter the editing status. Press to shift among numbers/lowercases, numbers/uppercases and symbols. ***Note:*** There are two kinds of Editing Key icons: EN or .

Chapter 2Installation

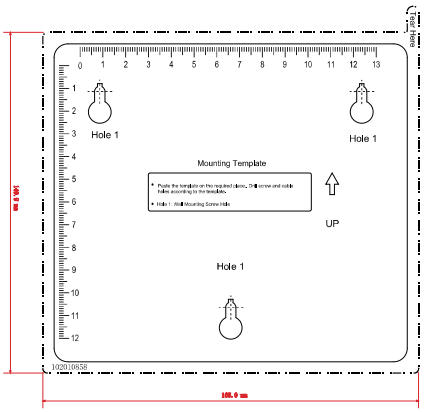
2.1 Wall Mounting

Steps:

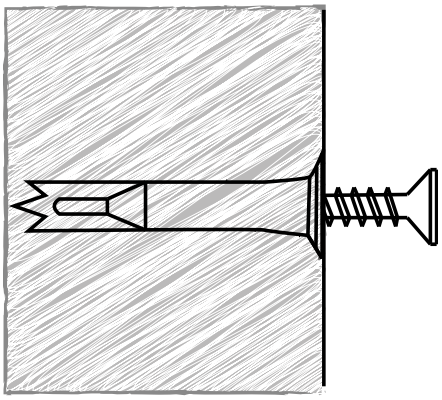
1. Drill holes on the wall or other places according to the mounting template (supplied).

   Notes:

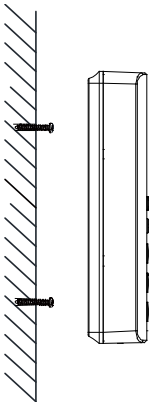
   - The minimum bearing weight of the wall or other places should be three times heavier than the device weight.
   - The length and the width will be 2 to 3mm smaller than the actual device's.



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. (Up to 5.5 mm should be reserved for the hanging the device when fix and fasten the screws.)



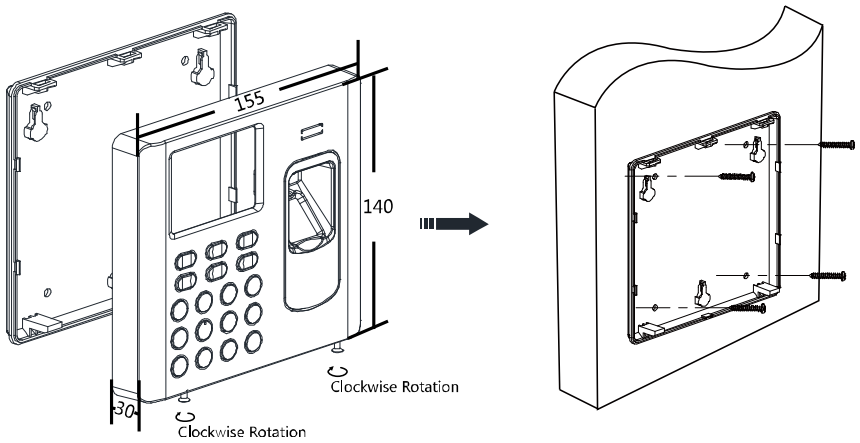
4. Align the three holes on the device plate with the fixed screws and hang the device on the wall.



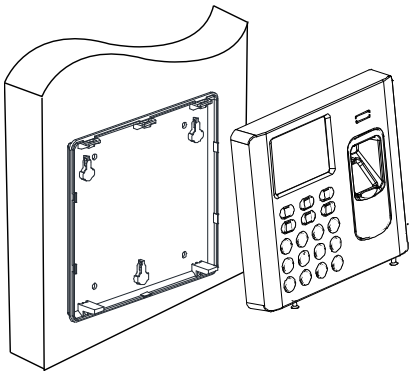
2.2 Wall Mounting with Mounting Plate

Steps:

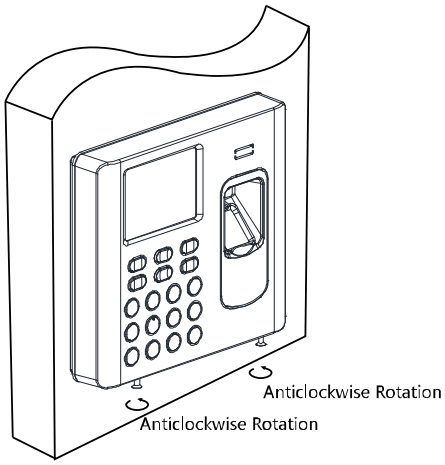
1. Remove the two screws at the bottom of the front cover and remove the back cover.



2. Align the back cover on the 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.

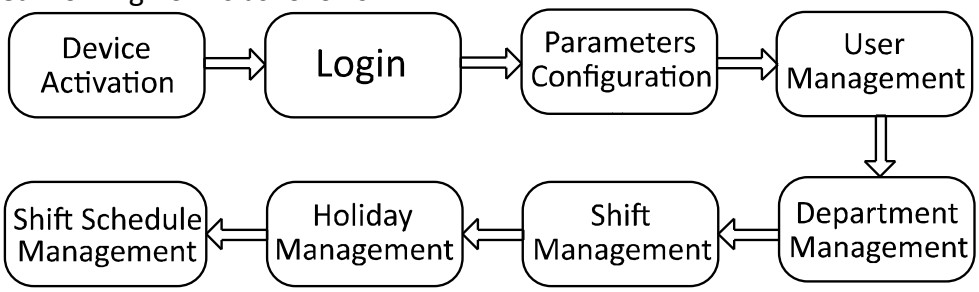


5. Fasten the screws in the sockets to fix the back cover on the wall or other places.
6. Align the front cover to the back cover and buckle them together.
7. Fasten the screws at the bottom of the front cover.



Chapter 3Basic 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 Device Activation interface.

Activation via the device, SADP tool and the iVMS-4200 client software are supported.

The default values of the terminal are as follows:

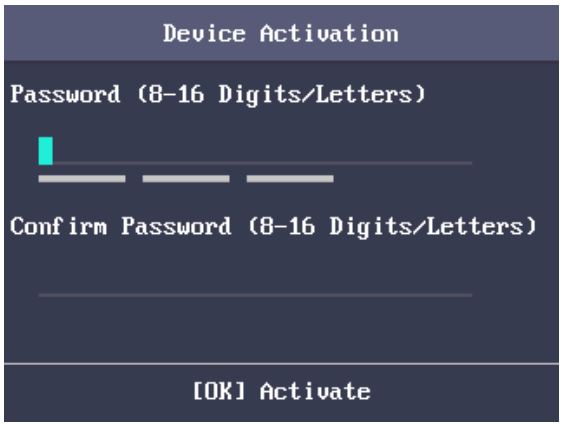
- The default IP address: 192.0.0.64
- The default port No.: 8000
- The default user name: admin

3.1.1 Activating via Device

If the device is not activated before first login, the system will enter the Device Activation interface after powering on.

Steps:

1. Create a device password for activation.



2. Confirm the password.
3. Press the OK key to activate the device.

Note: For details about entering and operating the input method, see *Appendix B Input Method Operation*.

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.*

3.1.2 Activating via SADP Software

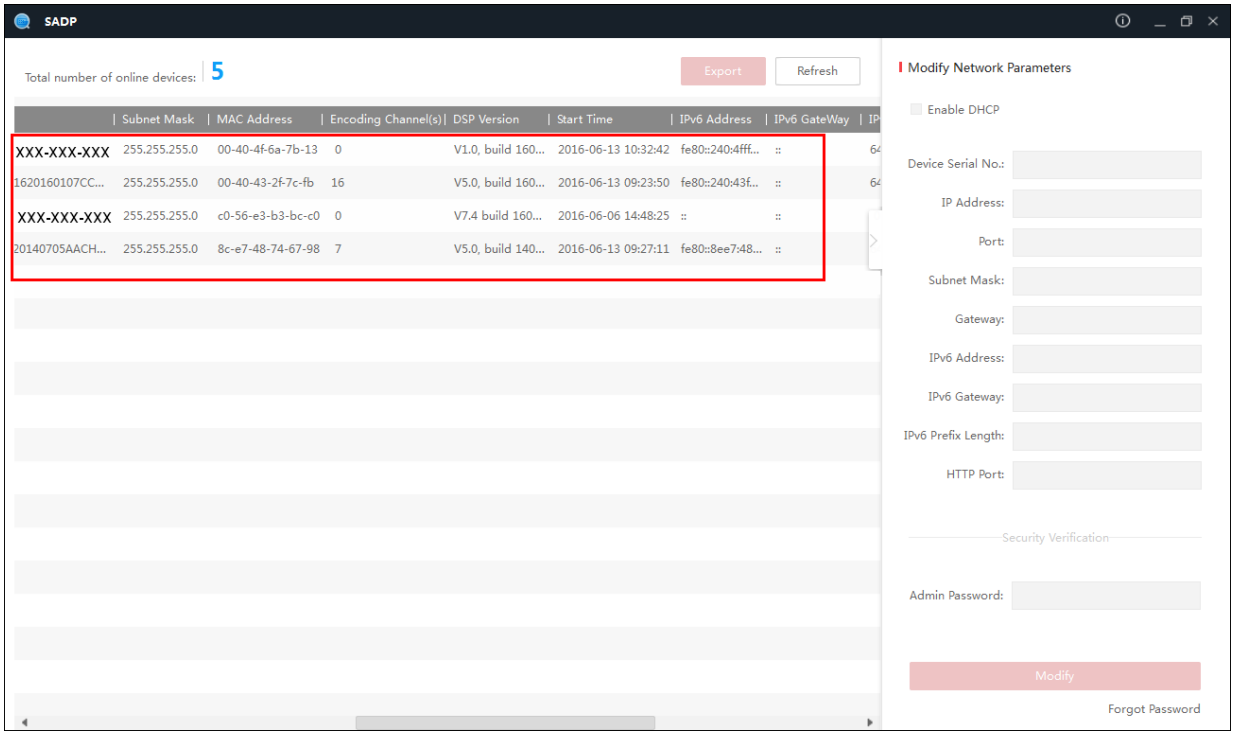
Purpose:

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

Get the SADP software from the supplied disk or the official website, and install the SADP according to the prompts. Follow the steps to activate the control panel.

Steps:

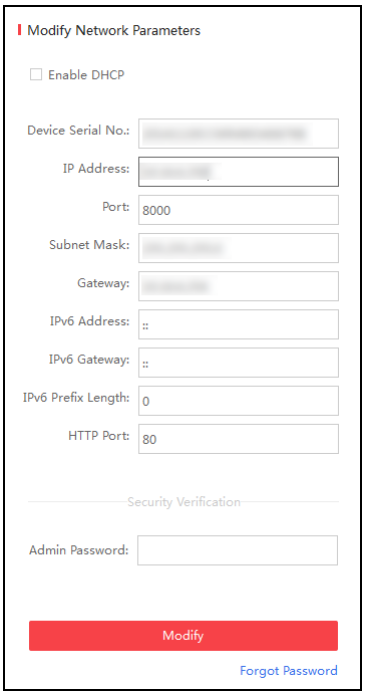
1. Run the SADP software to search the online devices.
2. Check the device status from the device list, and select an inactive device.



3. Create a password and input the password in the password field, 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** to save the password.
5. Check the activated device. You can change the device IP address to the same network segment with your computer by either modifying the IP address manually or checking the checkbox of Enable DHCP.



6. Input the password and click the **Modify** button to activate your IP address modification.

3.1.3 Activating via Client Software

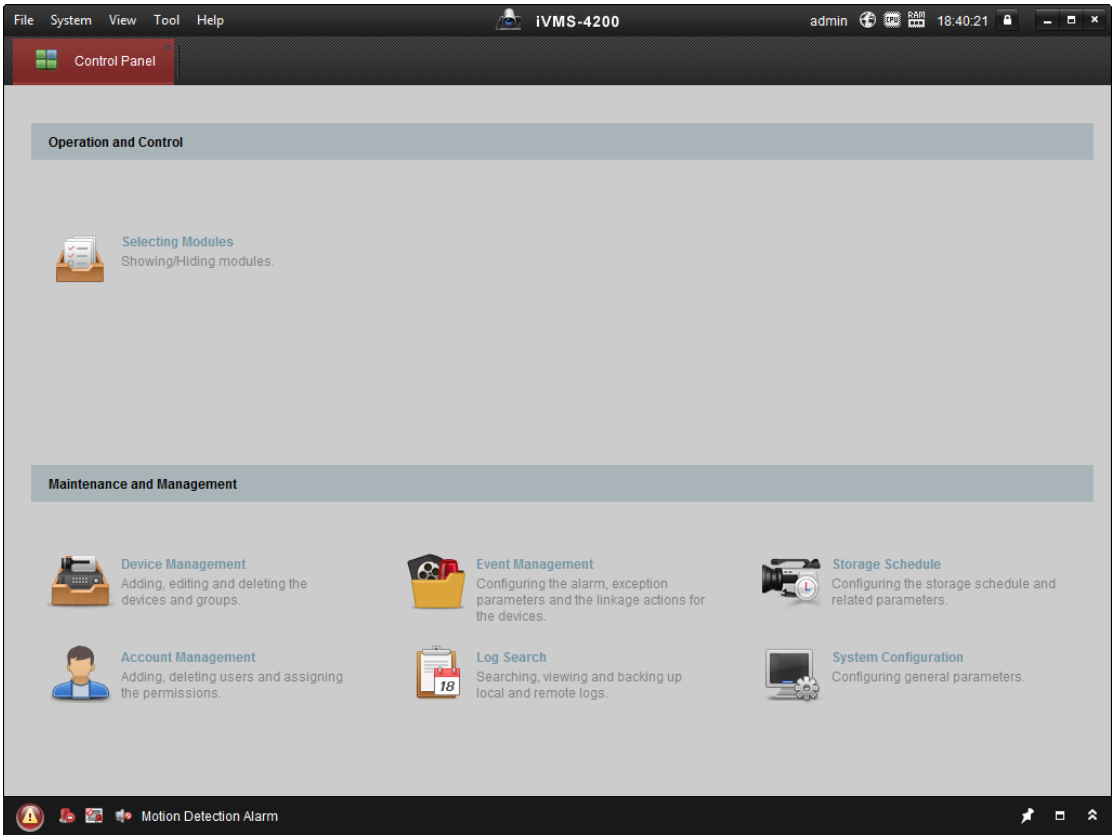
Purpose:

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

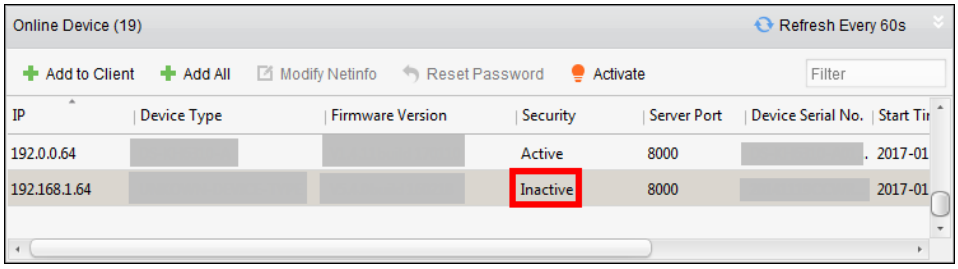
Get the client software from the supplied disk or the official website, and install the software according to the prompts. Follow the steps to activate the control panel.

Steps:

1. Run the client software and the control panel of the software pops up, as shown in the figure below.



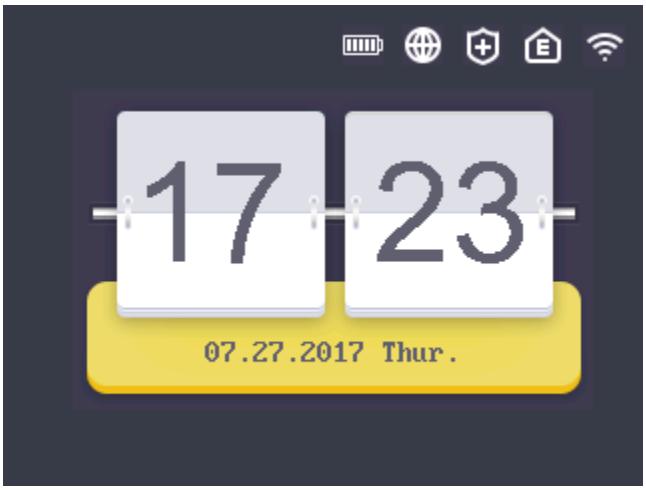
2. Click **Device Management** to enter the Device Management interface.
3. Check the device status from the device list, and select an inactive device.



4. Check the device status from the device list, and select an inactive device.
5. Click the **Activate** button to pop up the Activation interface
6. In the pop-up window, create a password in the password field, 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.*

7. Click **OK** button to start activation.
8. Click the **Modify Netinfor** button to pop up the Network Parameter Modification interface.
9. Change the device IP address to the same network segment with your computer by either modifying the IP address manually.
10. Input the password and click the **OK** button to save the settings.
    You will enter the initial interface.



Notes:

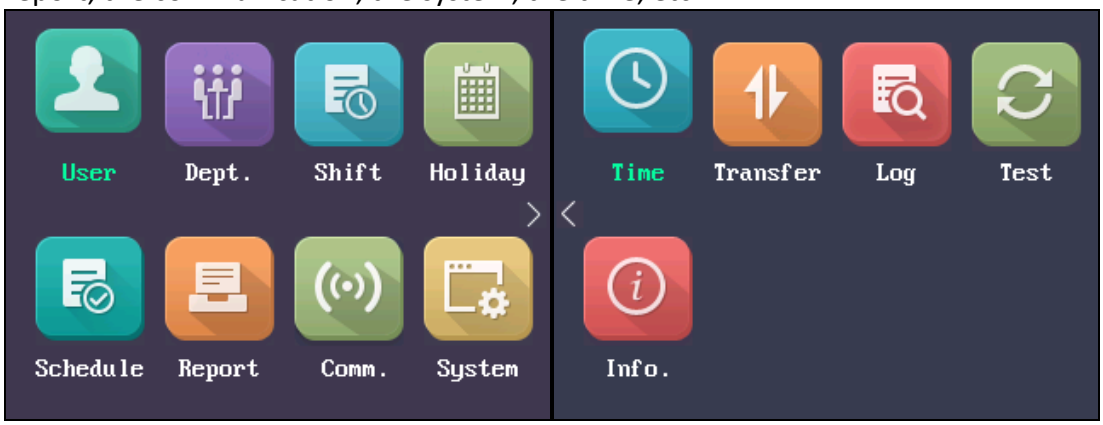
- In the initial interface, the icons , , , , and at the upper-right corner represents network is online, network is armed, EHome is online. If the network is offline, network is not armed, and EHome is offline, there will be on the icon. When the Wi-Fi is not connected, the Wi-Fi icon will have no color inside.
- You should add the device via EHome protocol in iVMS-4200 client software, and the EHome icon will be displayed as online. See Section 4.4.1 Adding Access Control Device to add device via EHome protocol;
- You should arm the device via iVMS-4200 client software, and the Arming icon will be displayed as armed. See Section 4.13 Arming Control for more information.

- The picture displayed above is the initial interface. It may vary according to different models: If the device model contains -1, the interface will not contain the Wi-Fi icon; If the device model contains –B, the interface will contain the battery icon.

3.2 Login

Steps:

1. For the first time login, long-press the OK key for 3s and input the device password (the password for activation) 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, for different device models, there are different login methods:

   DS-K1A801F Series and DS-K1A802F Series

   1) Long-press OK key for 3s to enter the Login interface.
   2) Move the cursor to select FP, Employee ID & PWD, or Device PWD.
   3) Press the OK key.
   4) Scan the fingerprint, input the employee ID and the password, or input the device password to enter the main interface.

   DS-K1A801MF/EF Series and DS-K1A802MF/EF Series

   1) Long-press OK key for 3s to enter the Login interface.
   2) Move the cursor to select FP, Card, Employee ID & PWD, or Device PWD.
   3) Press the OK key.
   4) Scan the fingerprint, input the card No., input the employee ID and the password, or input the device password to enter the main interface.

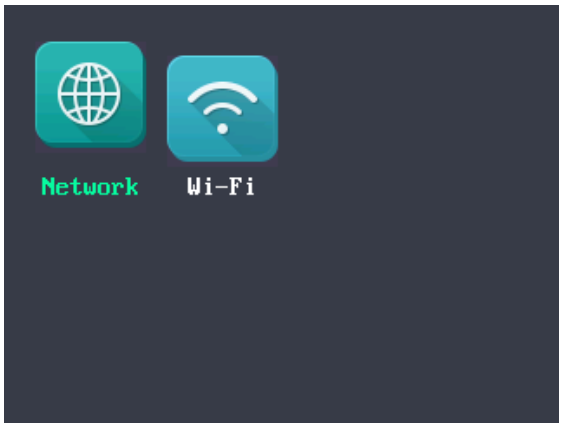
   Note: For details about entering and operating the input method, see *Appendix B Input Method Operation*.

3.3 Parameters Configuration

3.3.1 Communication Settings

Purpose:

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



Note: The picture displayed above is the Communication Settings interface. The models with -1 does not support Wi-Fi function. And the Wi-Fi module's icon will not be displayed in the interface.

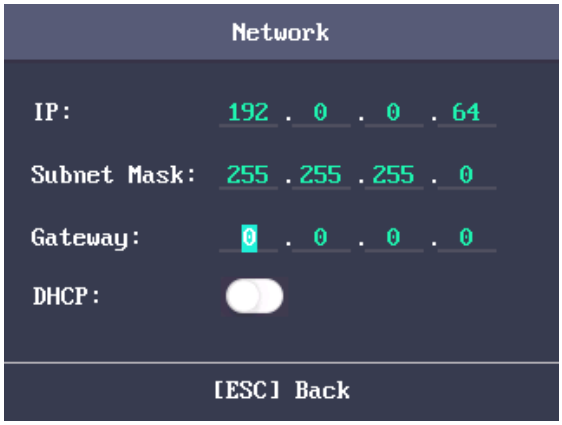
Setting Network

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

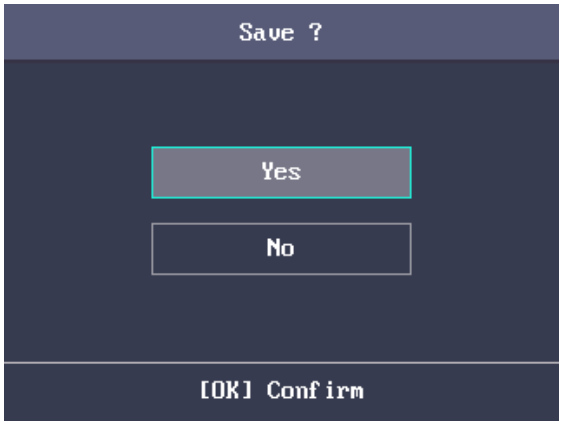
Steps:

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, the gateway and the DHCP.

   Note: The device's IP address and the PC's should be in the same network segment.



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



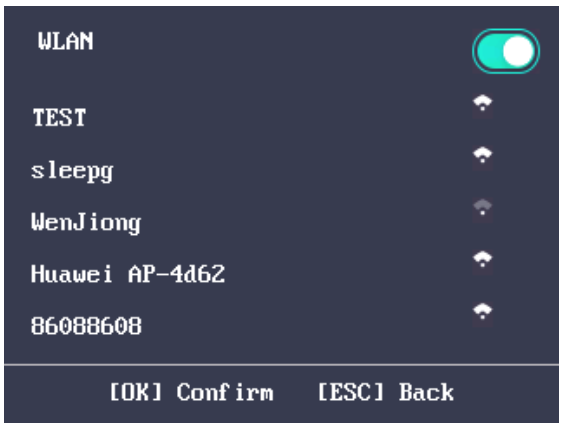
Setting Wi-Fi

Purpose:

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

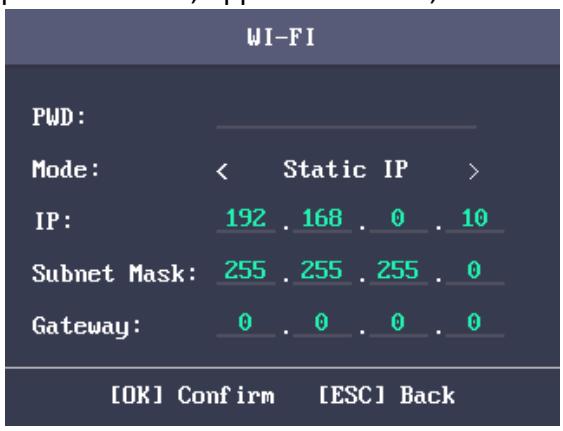
Steps:

1. Move the cursor to the **Wi-Fi**, and press the OK key to enter the Wi-Fi interface.
2. By default the WLAN is enabled. If the WLAN is note enabled, move the cursor to the icon  and press the OK key to enable the WLAN.



3. Select a network and press the OK key to enter the Wi-Fi Setting interface.
4. 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.

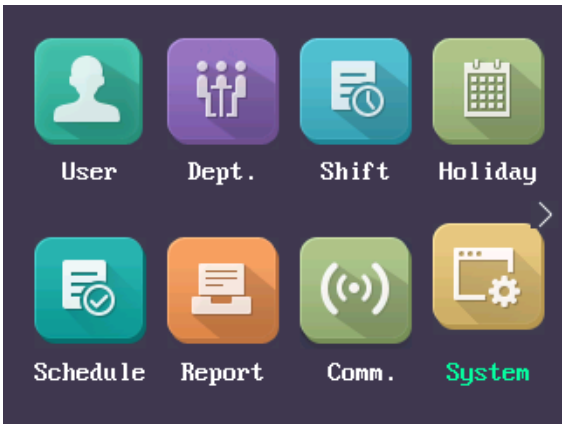


5. Press the ESC key and select **Yes** to save the parameters and exit the interface.

3.3.2 System Settings

Purpose:

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



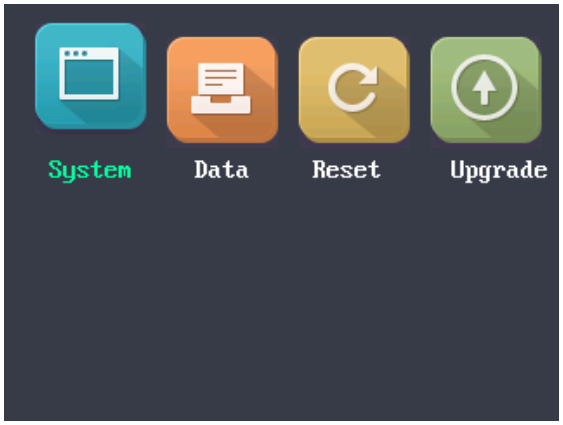
Setting System Parameters

Purpose:

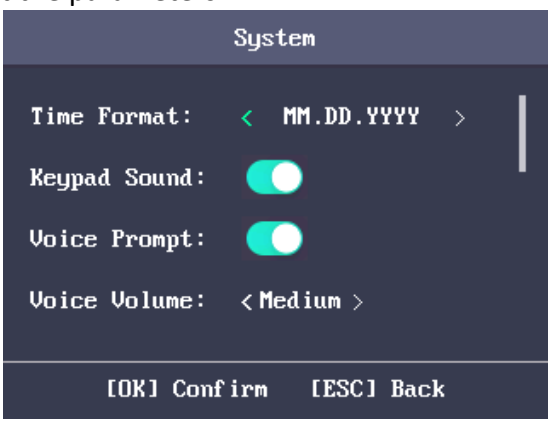
Set the system parameters, including the device time format, the keypad sound, the voice prompt, the volume, the sleeping, the attendance repeating time interval, the attendance record prompt and the authentication mode.

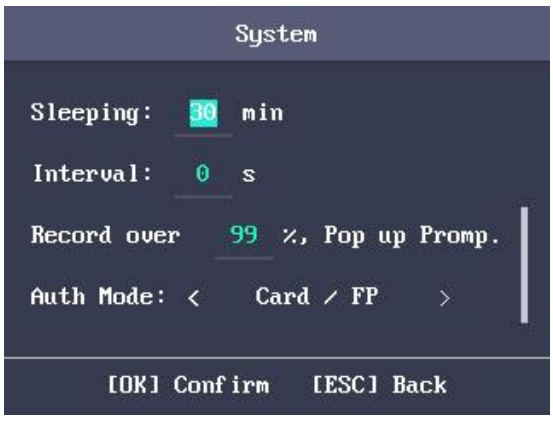
Steps:

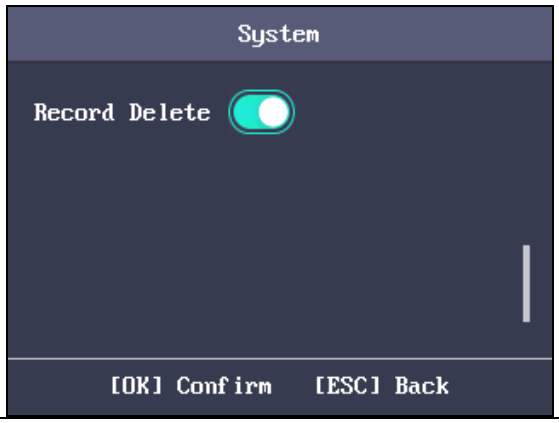
1. Move the cursor to **System** and press the OK key to enter the System interface.



2. Edit the parameters.







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. ***Note:*** The maximum attendance record memory is 150,000.
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 reaches the configure threshold, in order to save the new attendance records. By default, the function is enabled. *See Appendix C Attendance Record Delete Rule*.

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

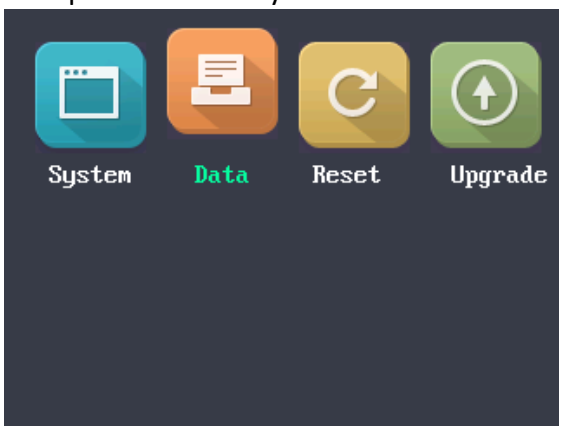
Managing Data

Purpose:

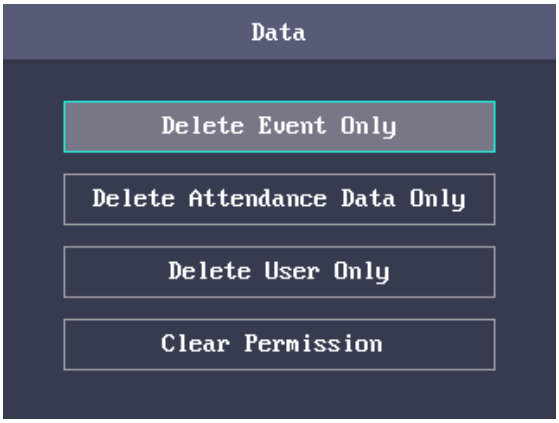
You are able to delete the storage data of the device, including the event, the attendance data, the user, and the permission.

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.



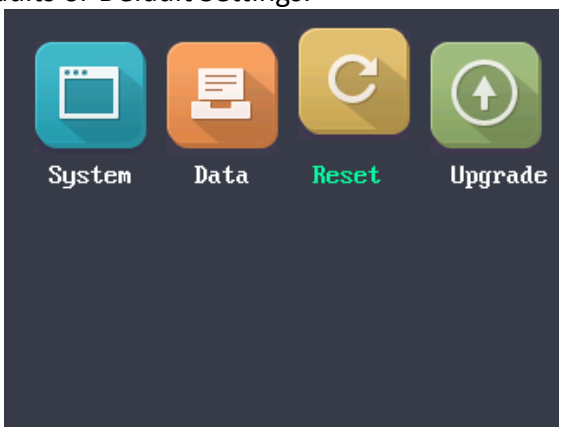
Delete Event Only:	Delete all recorded events in the device.
Delete Attendance Data Only:	Delete all attendance data in the device.

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:

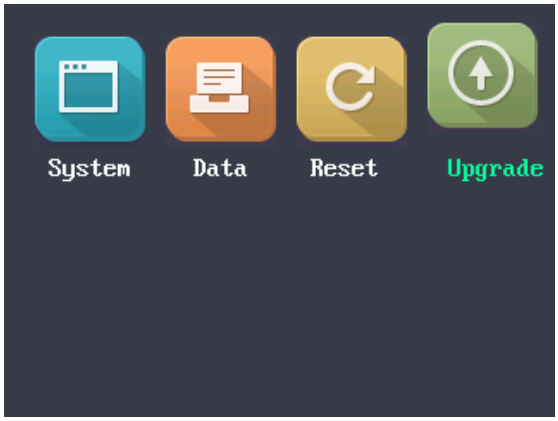
1. Move the cursor to **Reset** and press the OK key to enter the Reset interface.

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 read the upgrading file from the plugged USB disk. Press **OK** 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.

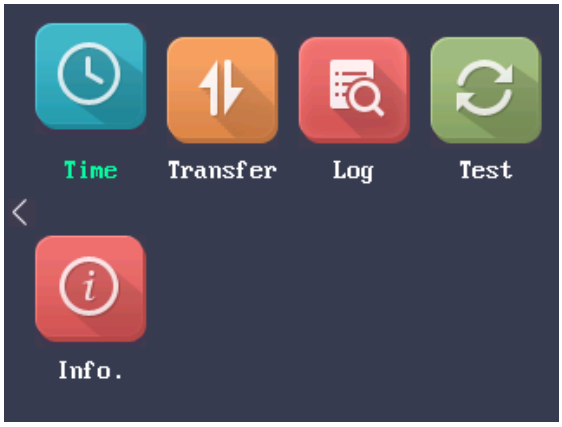
3.3.3 Setting Time

Purpose:

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

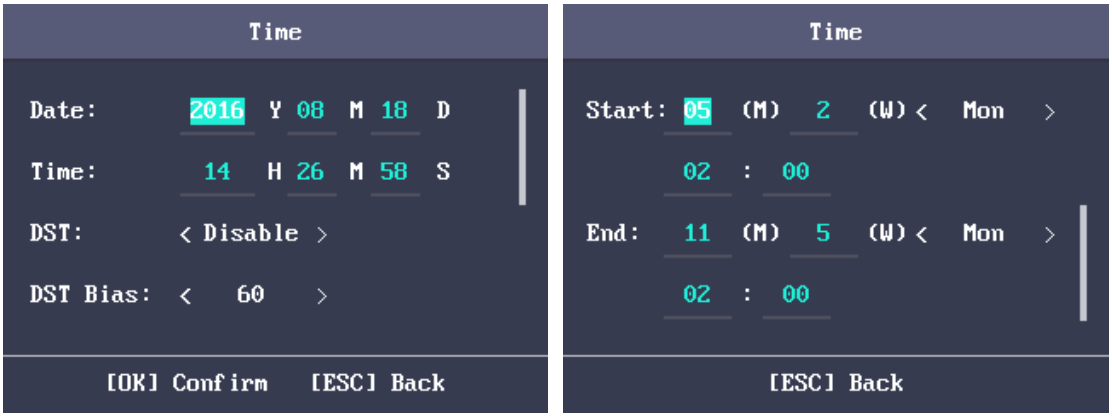
Steps:

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.



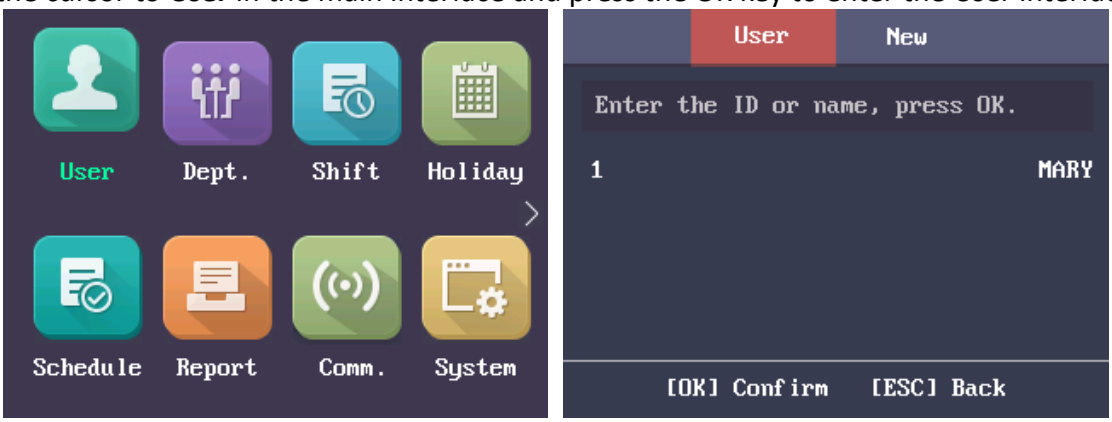
4. Press the ESC key and select **Yes** to save the settings and exit the interface.

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.



3.4.4 Adding User

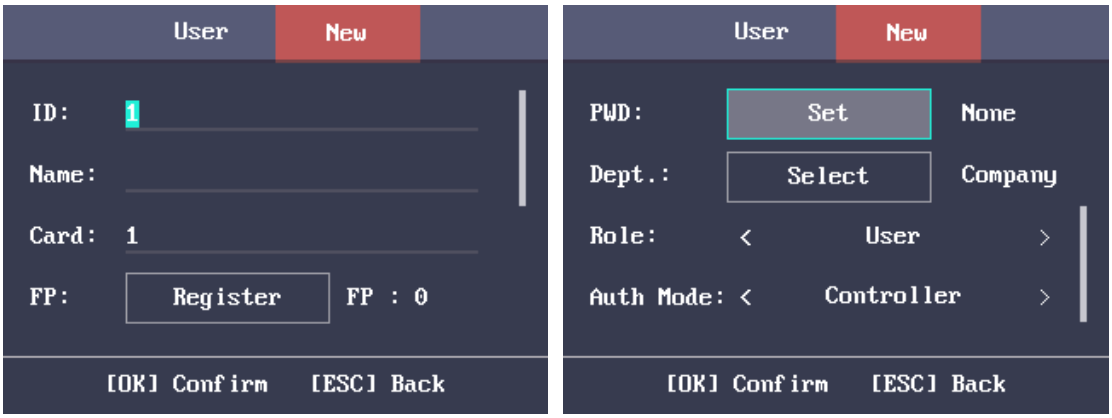
You can add users by editing the ID No., the user name, the card No. You can also scan the user fingerprint, set the password, the department, the role and the authentication mode.

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.



2. Enter the new user name.

   Notes:

   - For details about using the input method, see *Appendix B Input Method Operation*.
   - The user name supports up to 32 characters.
   - Each user name can be used for once.

3. Enter the card No.

   Notes:

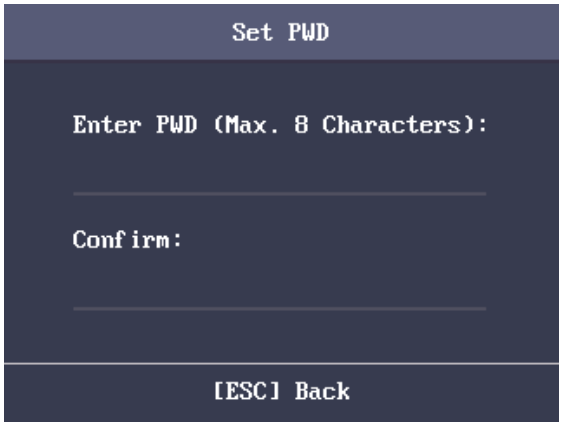
   - The card No. is required.
   - The card No. can be 0.
   - The card No. can start with 0 when it contains more than one numbers. E.g. 012345.
   - The card No. can be used for once.
   - The device of DS-K1A801F series supports manually entering the card No. The device of DS-K1A801MF series and DS-K1A801EF series support 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 *Appendix A Tips for Scanning Fingerprint.*

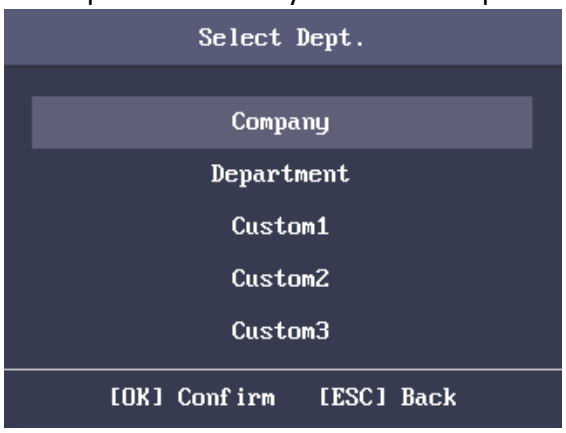
5. Move the cursor to **Set** and press the OK key to edit the user password.
   1) Enter the password and confirm the password in the Set Password interface.



   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 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 user the USB interface to import the user information. For details, see *Appendix B Input Method Operation*.

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

3.4.5 Managing User

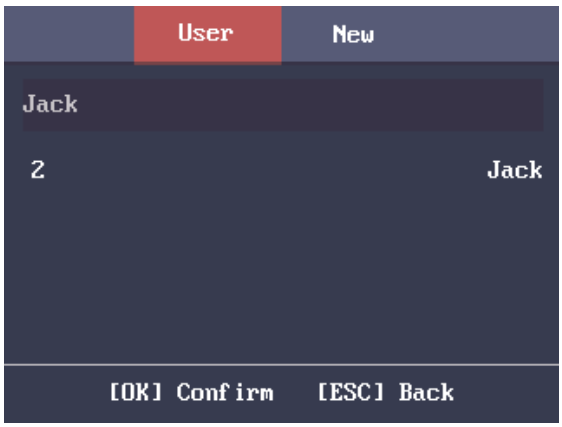
Searching User

Purpose:

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

Steps:

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



Editing User

Steps:

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

3. Follow *Section 3.4.4 Adding User* to edit the user information.
4. 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:

1. Select the target user for deleting in the User interface.
2. 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.

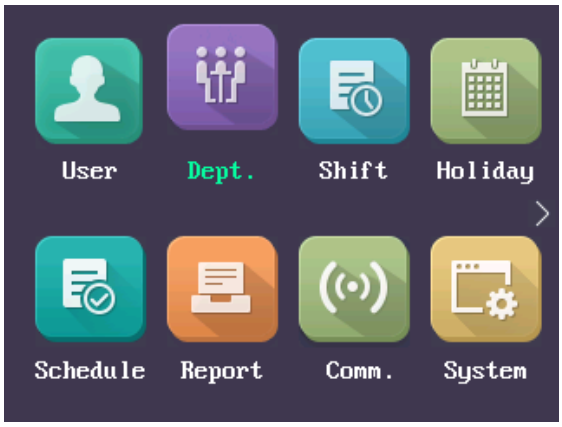
   Or press **Clear Fingerprint** and press the OK key to clear the target user fingerprint.

   Or press **Clear Card** and press the OK key to delete the user card No.

3.5 Department Management

Purpose:

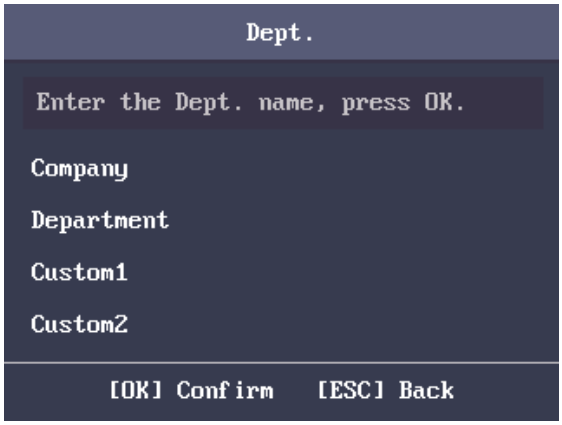
Editing, searching and resetting the department are available.



3.5.1 Editing and Resetting 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.
- For details about using the input method, see *Appendix B Input Method Operation*.

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

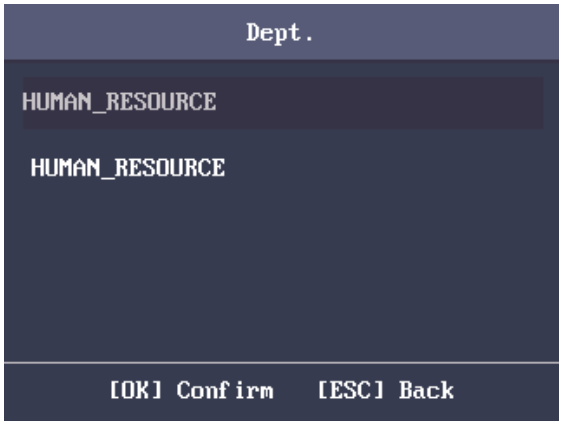
3.5.2 Searching Department

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 Department

Purpose:

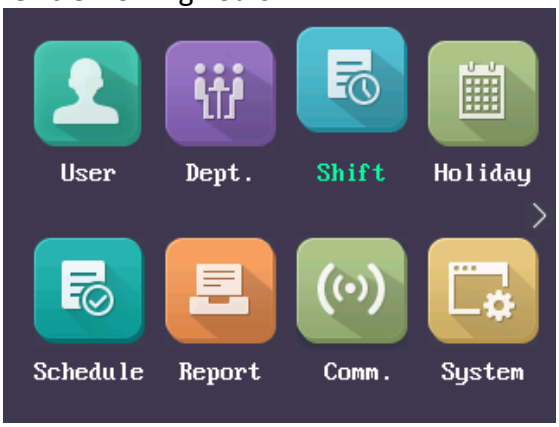
Reset all parameters of the target department to the default ones.

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.



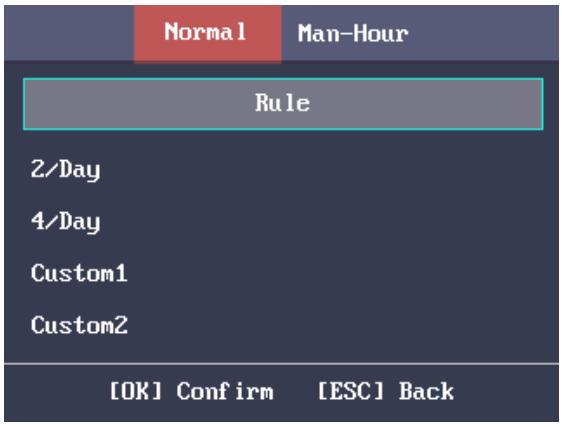
Note: Support up to 32 normal shifts and 32 man-hour shifts.

3.6.4 Normal Shift

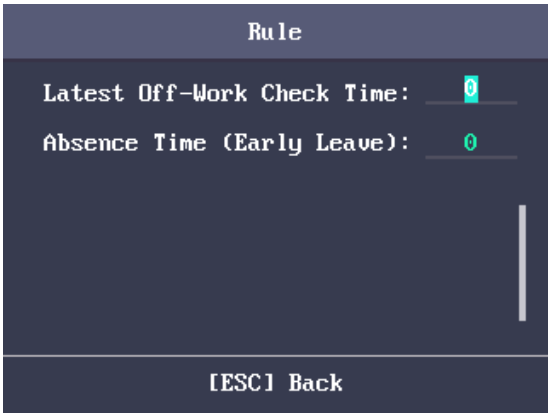
Setting Attendance Rule

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.

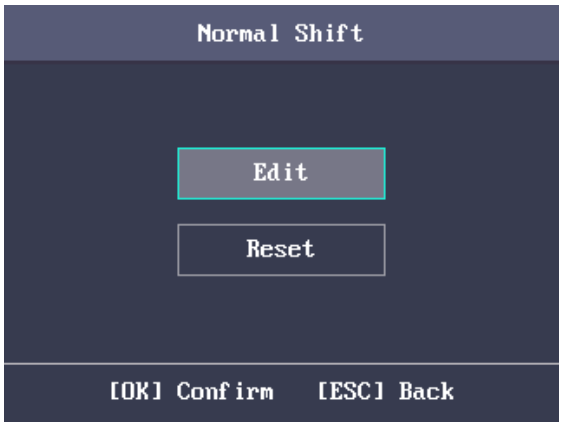


3. Press the ESC key and select **Yes** to save the settings and exit the interface.
   Notes:
   - Unit: minute.
   - The available time range is from 0 to 1440 minutes.

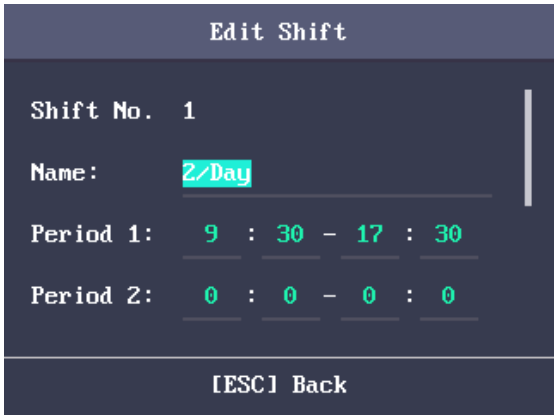
Setting Normal Shift Attendance

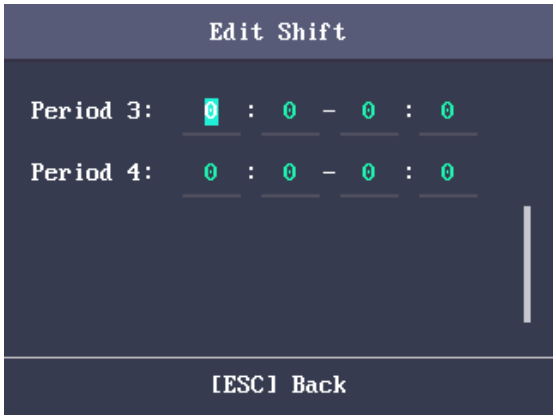
Steps:

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.





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.
- For details about using the input method, see *Appendix B Input Method Operation*.

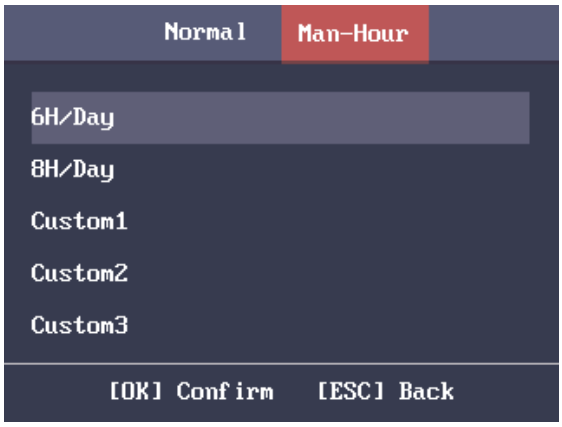
You can also select **Reset** to reset the settings.

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

3.6.5 Man-Hour Shift

Steps:

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

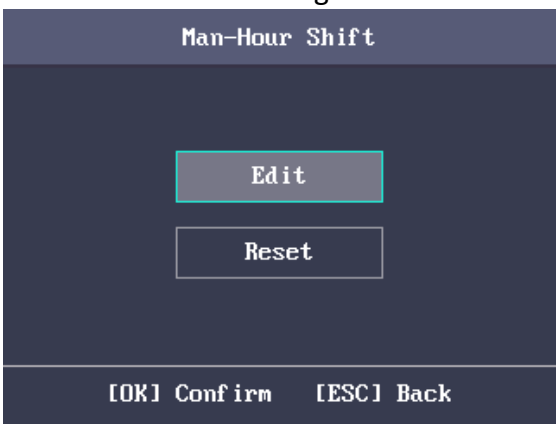


2. Select a man-hour shift type in the list.

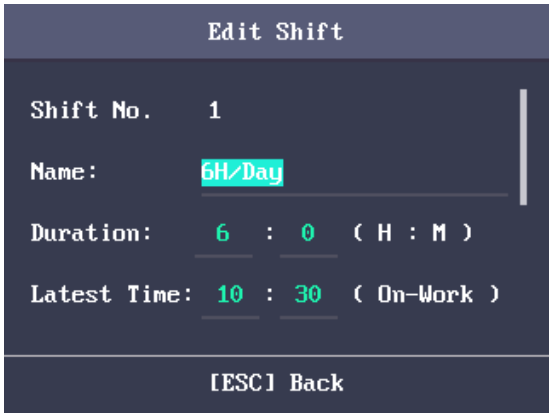
Notes:

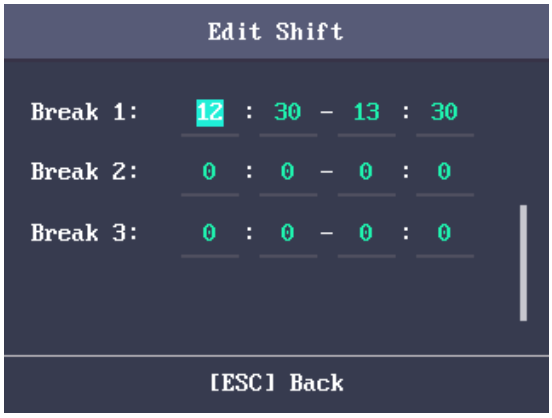
- By default, the man-hour shift type includes 6H/Day (6 hours per day), 4H/Day (4 hours per day), and 30 custom types.
- The following steps will take Custom 1 as an example.

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.





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.

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

3.7 Holiday Management

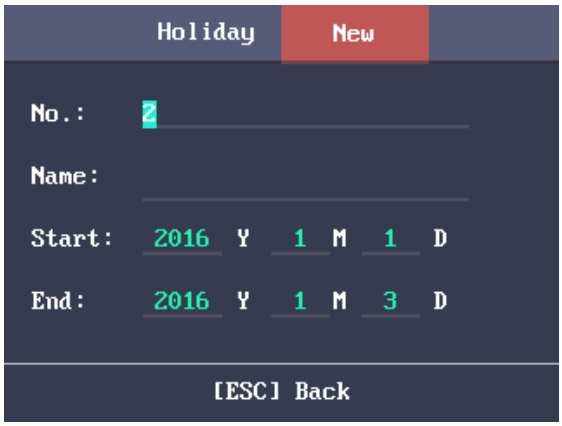
Purpose:

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

3.7.6 Adding Holiday

Steps:

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



2. Enter the holiday No., the holiday name, the holiday start time and the end time.
3. 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.

3.7.7 Searching Holiday

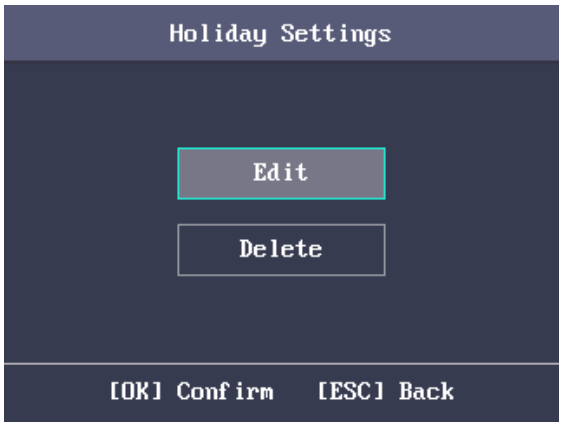
Steps:

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

3.7.8 Editing and Deleting Holiday

Steps:

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

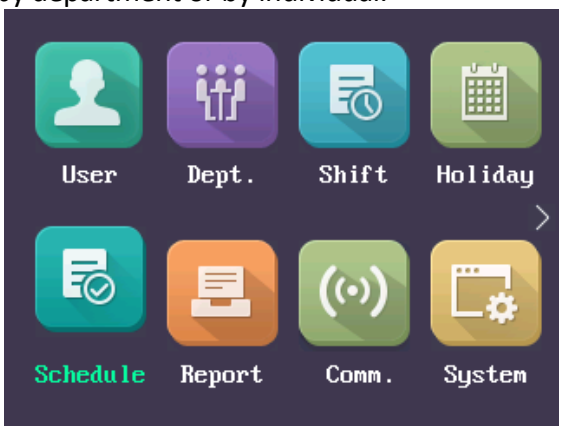


2. Select **Edit** and follow the steps in *Section 3.7.6 Adding Holiday* to edit the holiday information. Or select **Delete** and press the OK key to delete the holiday.
3. Press the ESC key and select **Yes** to save the settings and exit the interface.

3.8 Shift Schedule Management

Purpose:

Configure the shift schedule by department or by individual.



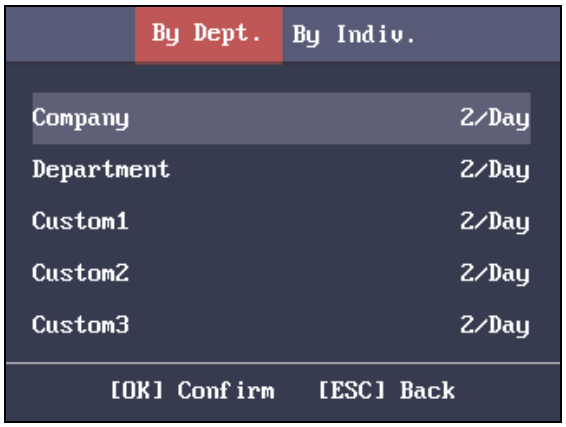
3.8.9 Scheduling Shift by Department

Before you start:

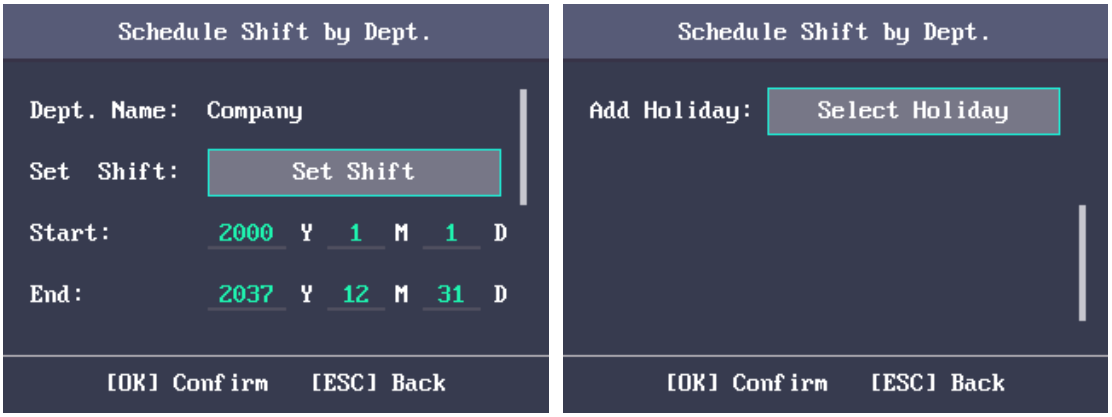
1. Edit the department. For detailed information, see *Section 3.5 Department Management*.
2. Configure the normal shift or the man-hour shift. For detailed information, see *Section 3.6 Shift Management*.

Steps:

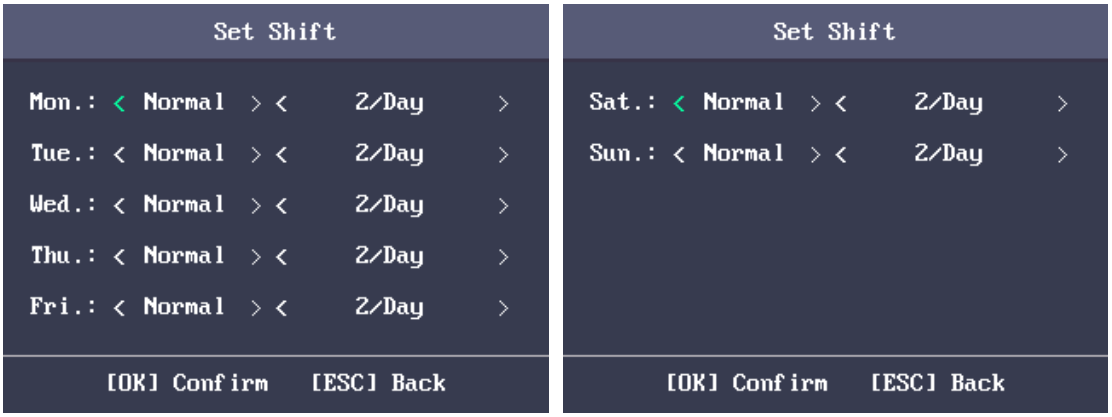
1. Select a target department in the By Dept. (Schedule by Department) interface.



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



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.



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.

3.8.10 Scheduling Shift by Individual

Up to 32 individual shifts can be added.

Adding New Individual Shift

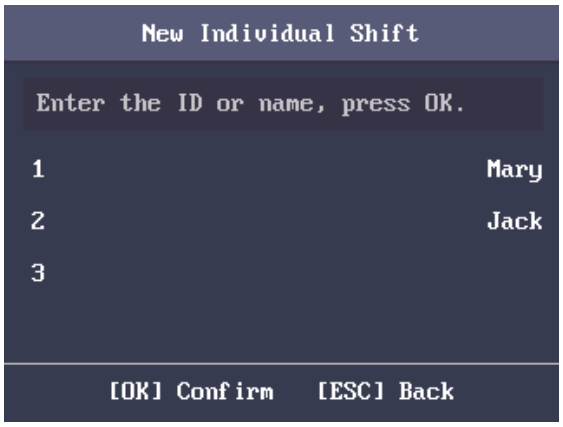
Before you start:

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*.

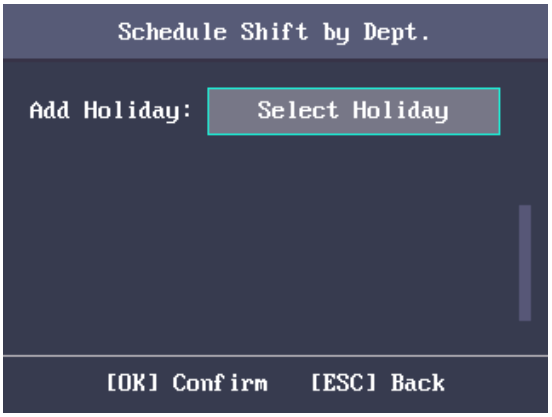
Steps:

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

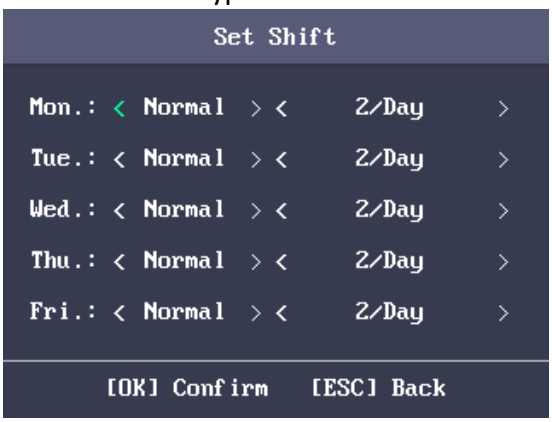
2. Select **New Individual Shift** and press the OK key to enter New Individual Shift interface.

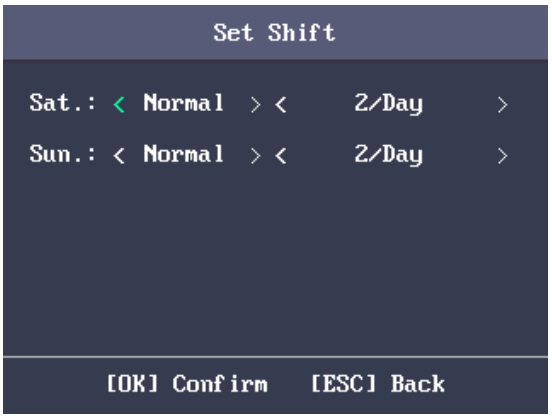


3. Select an individual in the list and press the OK key to enter the Individual Shift Settings interface.



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.





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.

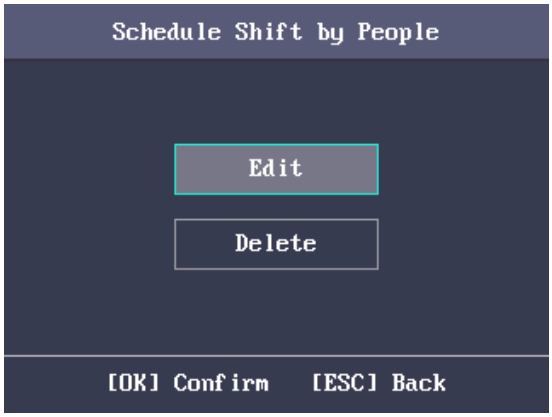
1) Select a target holiday.
2) Press the ESC key and select **Yes** to save the settings and exit the interface.
   Note: The attendance will not be recorded during the holiday.

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 3.8.10 Scheduling Shift by Individual* to edit the shift.
   Or select **Delete** to delete the selected individual shift.

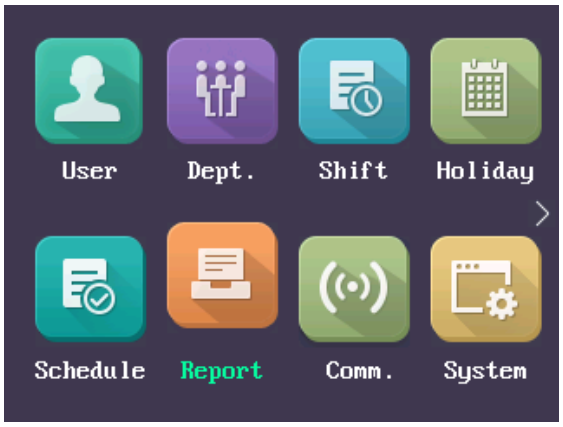


3.9 Other Management

3.9.1 Report Management

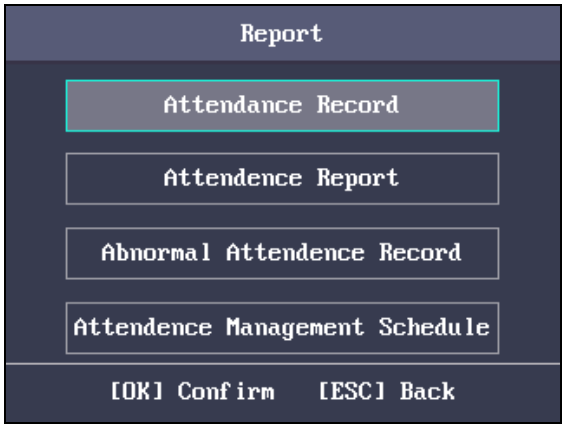
Purpose:

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

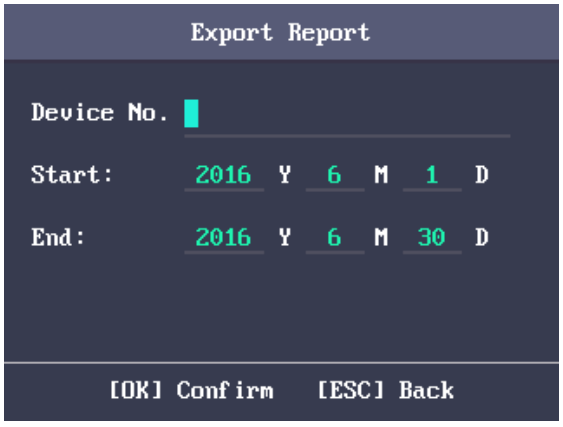


Steps:

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



3. 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.

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

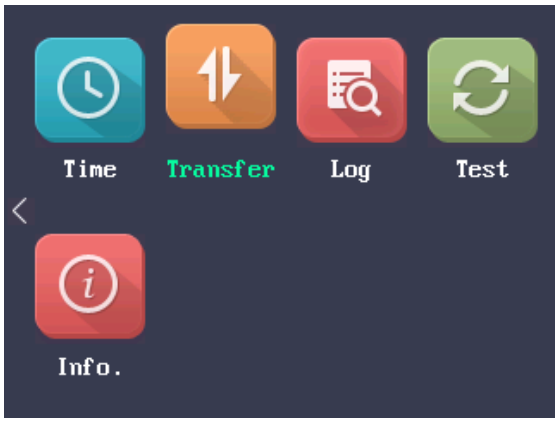
Notes:

- Support the USB disk in 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 Appendix E 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.

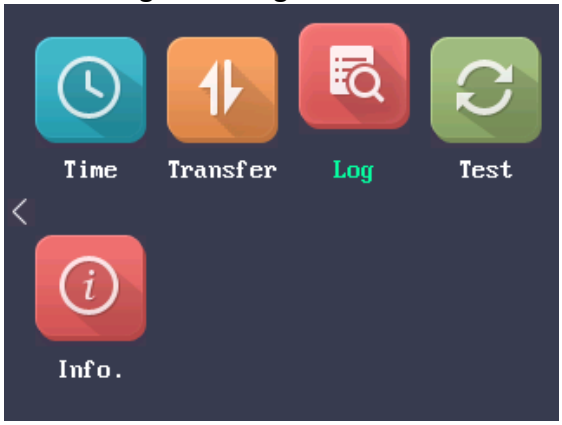
Notes:

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

3.9.3 Searching the Log

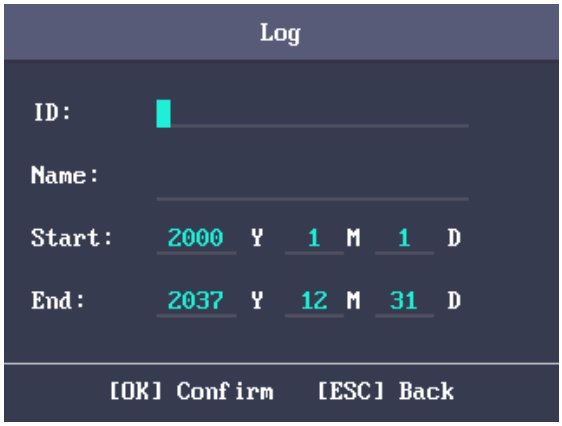
Purpose:

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

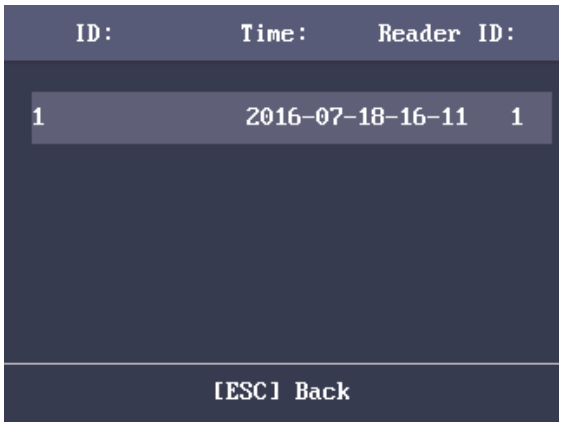


Steps:

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.



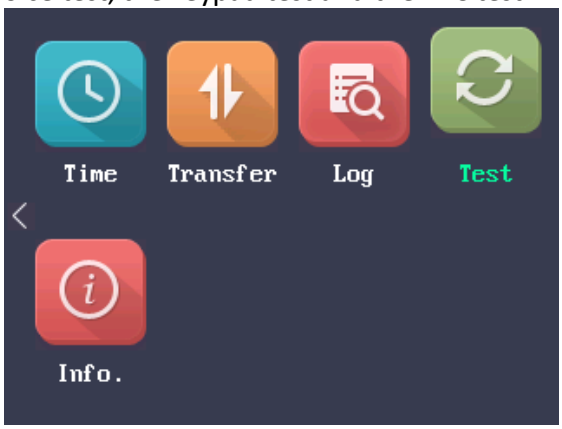
3. Enter the target log start time and the end time.
4. Press the OK key to search. The interface will display the log search result.



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

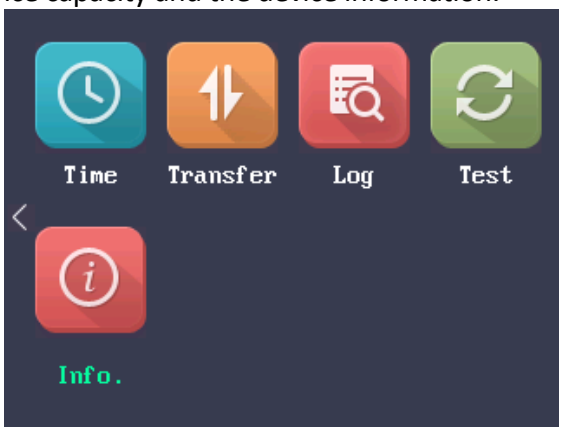
Steps:

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.

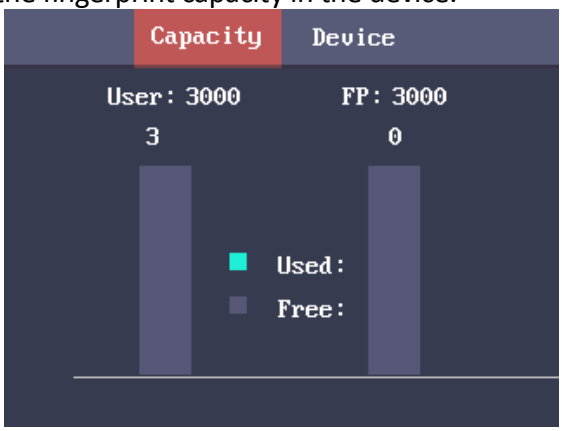
3.9.5 System Information

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



Checking 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 Device Information

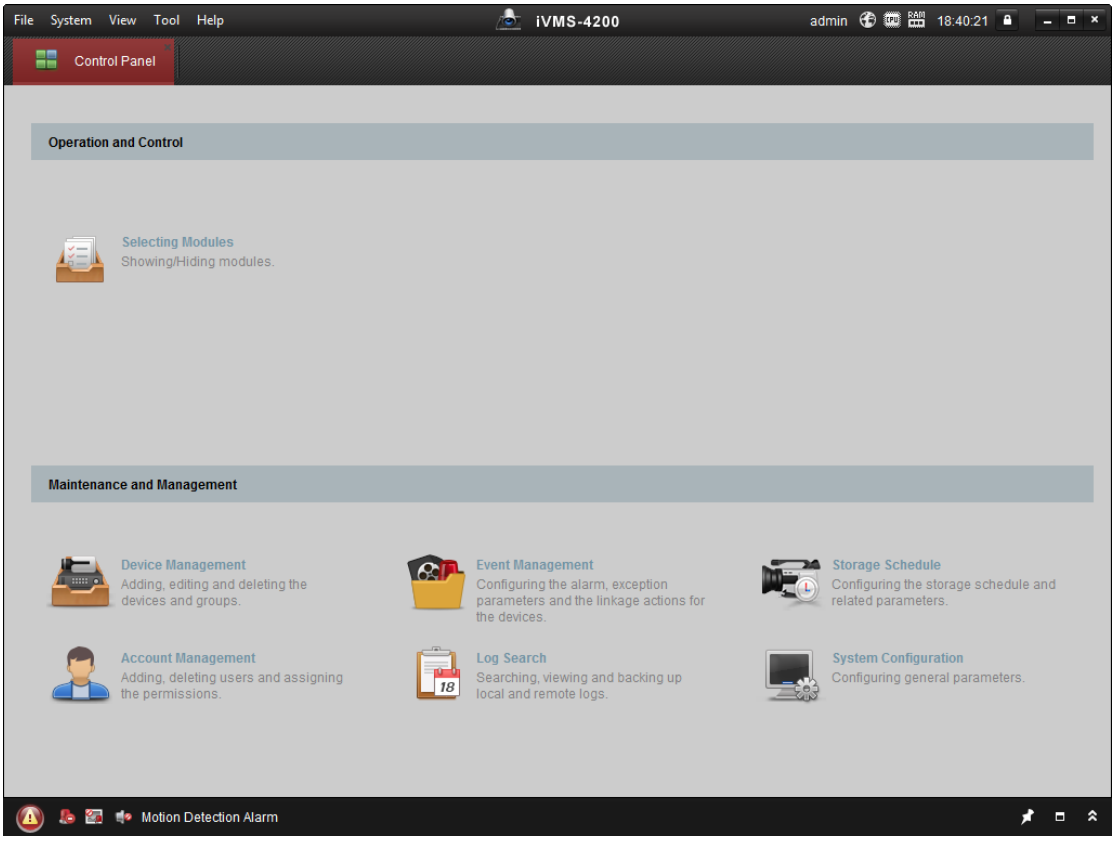
In the Device interface, you are able to check the device name, the device serial No., the MAC address, the firmware, the hardware and the production data.

Chapter 4Client Operation

You can set and operate the access control devices via the client software. This chapter will introduce the access control device related operations in the client software. For integrated operations, refer to *User Manual of iVMS-4200 Client Software*.

4.1 Function Module

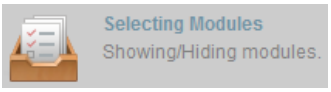
Control Panel of iVMS-4200:



Menu Bar:

File	**Open Image File**	Search and view the captured pictures stored on local PC.
	Open Video File	Search and view the video files recorded on local PC.
	Open Log File	View the backup log files.
	Exit	Exit the iVMS-4200 client software.
System	**Lock**	Lock screen operations. Log in the client again to unlock.
	Switch User	Switch the login user.
	Import System Config File	Import client configuration file from your computer.
	Export System Config File	Export client configuration file to your computer.
	Auto Backup	Set the schedule for backing up the database including person, attendance data, and permission data automatically.

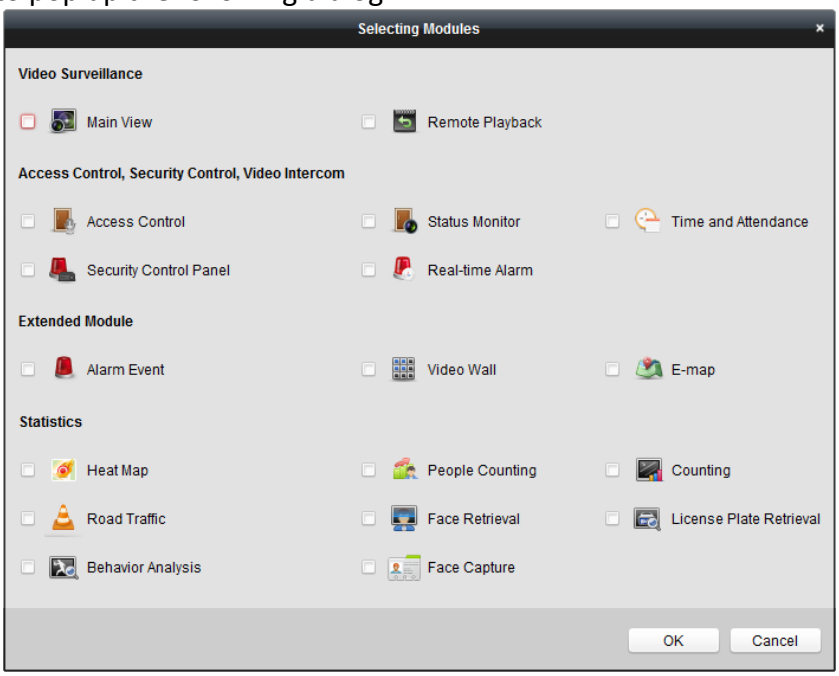
View	**1024*768**	Display the window at size of 1024*768 pixels.
	1280*1024	Display the window at size of 1280*1024 pixels.
	1440*900	Display the window at size of 1440*900 pixels.
	1680*1050	Display the window at size of 1680*1050 pixels.
	Maximize	Display the window in maximum mode.
	Control Panel	Enter Control Panel interface.
	Main View	Open Main View page.
	Remote Playback	Open Remote Playback page.
	Access Control	Enter the Access Control Module.
	Status Monitor	Enter the Status Monitor Module.
	Time and Attendance	Enter the Time and Attendance Module.
	Security Control Panel	Enter the Security Control Panel Module.
	Real-time Alarm	Enter the Real-time Alarm Module.
	Video Wall	Open Video Wall page.
	E-map	Open E-map page.
	Auxiliary Screen Preview	Open Auxiliary Screen Preview window.
Tool	**Device Management**	Open the Device Management page.
	Event Management	Open the Event Management page.
	Storage Schedule	Open the Storage Schedule page.
	Account Management	Open the Account Management page.
	Log Search	Open the Log Search page.
	System Configuration	Open the System Configuration page.
	Broadcast	Select camera to start broadcasting.
	Device Arming Control	Set the arming status of devices.
	Alarm Output Control	Turn on/off the alarm output.
	Batch Wiper Control	Batch starting or stopping the wipers of the devices.
	Batch Time Sync	Batch time synchronization of the devices.
	Player	Open the player to play the video files.
	Message Queue	Display the information of Email message to be sent.
Help	**Open Video Wizard**	Open the video guide for the video surveillance configuration.
	Open Video Wall Wizard	Open the guide for the video wall configuration.
	Open Security Control Panel Wizard	Open the guide for the security control panel configuration.
	Open Access Control and Video Intercom Wizard	Open the guide for the access control and video intercom configuration.
	Open Attendance Wizard	Open the guide for the time and attendance configuration.
	User Manual (F1)	Click to open the User Manual; you can also open the User Manual by pressing **F1** on your keyboard.
	About	View the basic information of the client software.
	Language	Select the language for the client software and reboot the software to activate the settings.

For the first time running the software, you can click 

on the control panel to select the modules to display on the Operation and Control area of the control pane.

Steps:

1. Click  to pop up the following dialog.



2. Check the module checkboxes to display them on the control panel according to the actual needs.
3. Click **OK** to save the settings.

Notes:

- After adding the access control device in Device Management module, the Access Control, Status, and Time and Attendance module will be displayed on the control panel automatically.
- After adding the security control panel in Device Management module, the Security Control Panel and Real-time Alarm modules will be displayed on the control panel automatically.

The iVMS-4200 client software is composed of the following function modules:

	The Main View module provides live view of network cameras and video encoders, and supports some basic operations, such as picture capturing, recording, PTZ control, etc.
	The Remote Playback module provides the search, playback, export of video files.
	The Access Control module provides managing the organizations, persons, permissions, and advanced access control functions. Provides video intercom function.
	The Status Monitor module provides monitoring and controlling the door status, viewing the real-time card swiping records and access control events.

	The Time and Attendance module provides setting the attendance rule for the employees and generating the reports.
	The Security Control Panel module provides operations such as arming, disarming, bypass, group bypass, and so on for both the partitions and zones.
	The Real-time Alarm module provides displaying the real-time alarm of security control panel, acknowledging alarms, and searching the history alarms.
	The Alarm Event module displays the alarm and event received by the client software.
	The Video Wall module provides the management of decoding device and video wall and the function of displaying the decoded video on video wall.
	The E-map module provides the displaying and management of E-maps, alarm inputs, hot regions and hot spots.
	The Device Management module provides the adding, modifying and deleting of different devices and the devices can be imported into groups for management.
	The Event Management module provides the settings of arming schedule, alarm linkage actions and other parameters for different events.
	The Storage Schedule module provides the schedule settings for recording and pictures.
	The Account Management module provides the adding, modifying and deleting of user accounts and different permissions can be assigned for different users.
	The Log Search module provides the query of system log files and the log files can be filtered by different types.
	The System Configuration module provides the configuration of general parameters, file saving paths, alarm sounds and other system settings.

The function modules are easily accessed by clicking the navigation buttons on the control panel or by selecting the function module from the **View** or **Tool** menu.

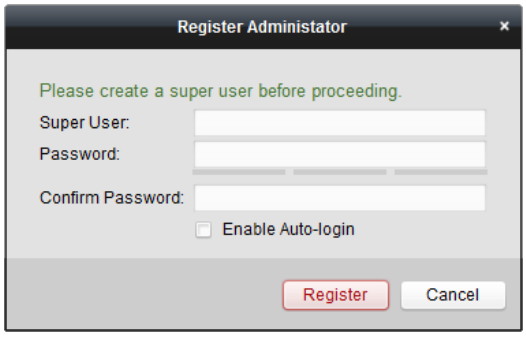
You can check the information, including current user, network usage, CPU usage, memory usage and time, in the upper-right corner of the main page.

4.2 User Registration and Login

For the first time to use iVMS-4200 client software, you need to register a super user for login.

Steps:

1. Input the super user name and password. The software will judge password strength automatically, and we highly recommend you to use a strong password to ensure your data security.
2. Confirm the password.
3. Optionally, check the checkbox **Enable Auto-login** to log into the software automatically.
4. Click **Register**. Then, you can log into the software as the super user.

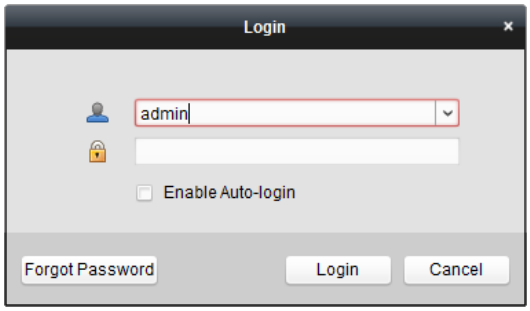


- *A user name cannot contain any of the following characters: / \ : * ? " < > |. And the length of the password cannot be less than 6 characters.*
- *For your privacy, we strongly recommend changing the password to something of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product.*
- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*

When opening iVMS-4200 after registration, you can log into the client software with the registered user name and password.

Steps:

1. Input the user name and password you registered.
   Note: If you forget your password, please click **Forgot Password** and remember the encrypted string in the pop-up window. Contact your dealer and send the encrypted string to him to reset your password.
2. Optionally, check the checkbox **Enable Auto-login** to log into the software automatically.
3. Click **Login**.



After running the client software, you can open the wizards (including video wizard, video wall wizard, security control panel wizard, access control and video intercom wizard, and attendance wizard), to guide you to add the device and do other settings and operations. For detailed configuration about the wizards, please refer to the *Quick Start Guide of iVMS-4200*.

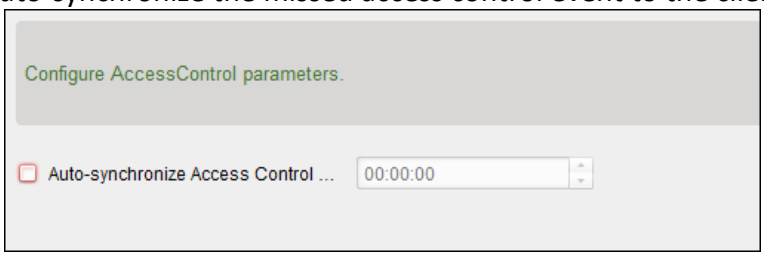
4.3 System Configuration

Purpose:

You can synchronize the missed access control events to the client.

Steps:

1. Click **Tool** – **System Configuration**.
2. In the System Configuration window, check the **Auto-synchronize Access Control Event** checkbox.
3. Set the synchronization time.
   The client will auto-synchronize the missed access control event to the client at the set time.



4.4 Access Control Management

Purpose:

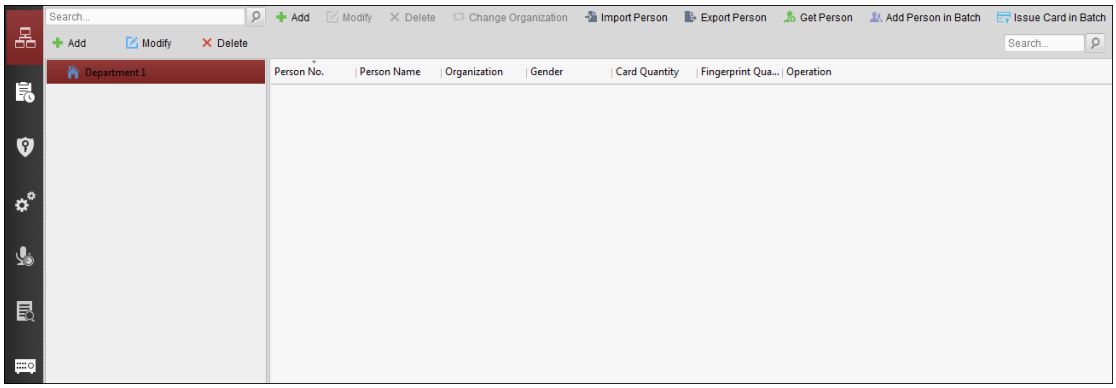
The Access Control module is applicable to access control devices and video intercom. It provides multiple functionalities, including person and card management, permission configuration, access control status management, video intercom, and other advanced functions.

You can also set the event configuration for access control and display access control points and zones on E-map.

Note: For the user with access control module permissions, the user can enter the Access Control module and configure the access control settings.

Click  in the control panel, and check **Access Control** to add the Access Control module to the control panel.

Click  to enter the Access Control module.



Before you start:

For the first time opening the Access Control module, the following dialog will pop up and you are required to select the scene according to the actual needs.

You can select the scene as **Non-residence** and **Residence**.

Non-residence: You can set the attendance rule when adding person, while set the access control parameters.

Residence: You cannot set the attendance rule when adding person.

Note: Once the scene is configured, you cannot change it later.

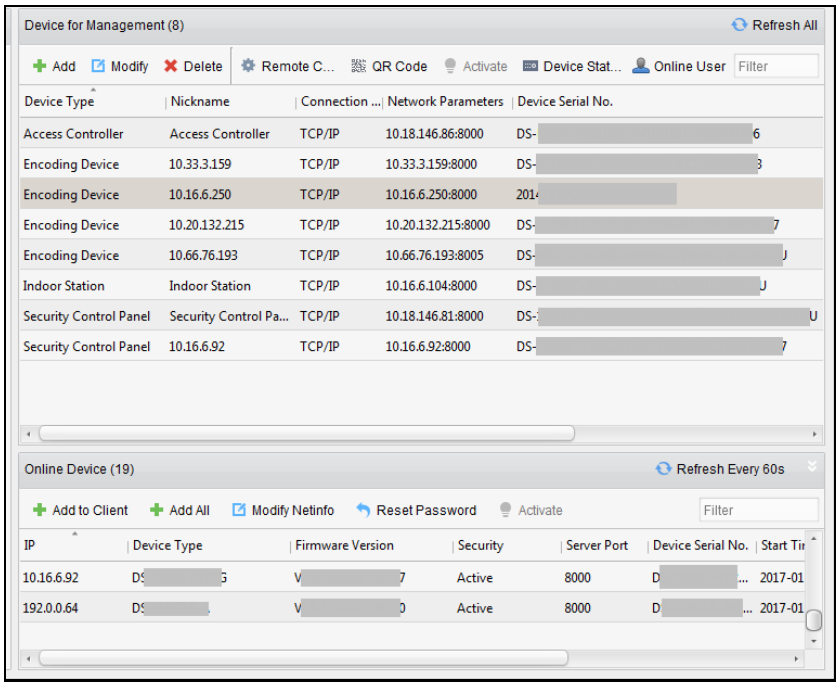
The Access Control module is composed of the following sub modules.

	Person and Card	Managing the organizations, persons, and assigning cards to persons.
	Schedule and Template	Configuring the week schedule, holiday group, and setting the template.
	Permission	Assigning access control permissions to persons and applying to the devices.
	Advanced Function	Providing advanced functions including access control parameters settings, card reader authentication, opening door with first card, anti-passing back, multi-door interlocking, and authentication password.
	Video Intercom	Video intercom between client and resident, searching the dial log, and releasing notice.
	Search	Searching history events of access control; Searching call logs, unlocking logs, and released notices.
	Device Management	Managing the access control devices and video intercom devices.

Note: In this chapter, we only introduce the operations about access control.

4.4.1 Adding Access Control Device

Click in the Access Control module to enter the following interface.



Note: After adding the device, you should check the device arming status in **Tool** – **Device Arming Control**. If the device is not armed, you should arm it, or you will not receive the real-time events via the client software. For details about device arming control, refer *4.13 Arming Control*.

Creating Password

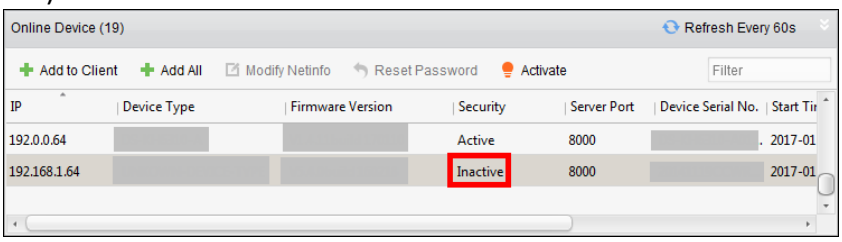
Purpose:

For some devices, you are required to create the password to activate them before they can be added to the software and work properly.

Note: This function should be supported by the device.

Steps:

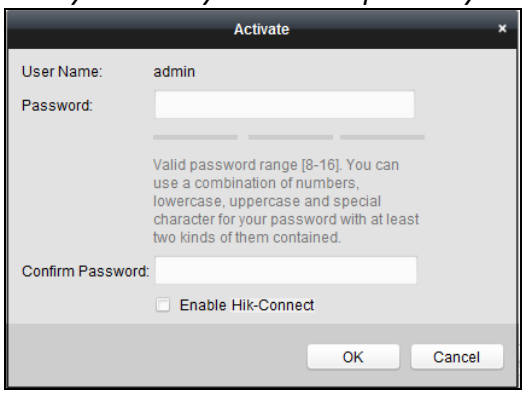
1. Enter the Device Management page.
2. On the **Device for Management** or **Online Device** area, check the device status (shown on **Security** column) and select an inactive device.



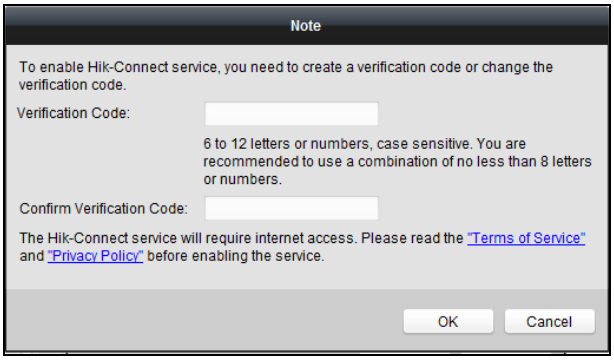
3. Click the **Activate** button to pop up the Activation interface.
4. Create a password in the password field, and confirm the password.

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,*

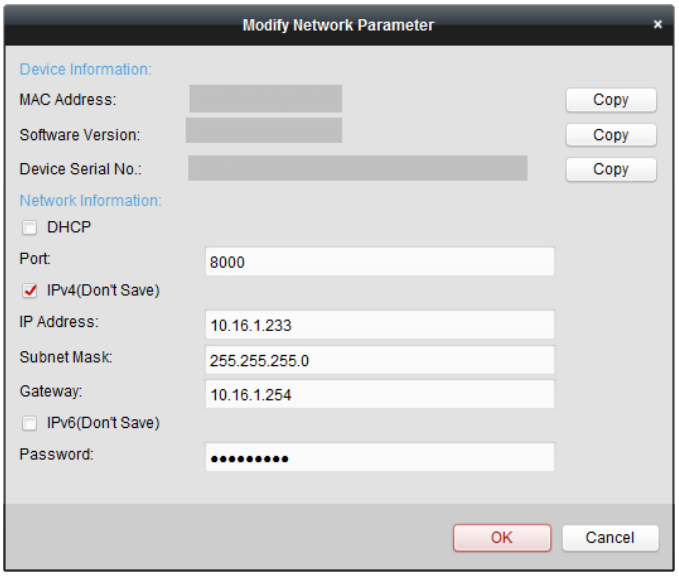
resetting the password monthly or weekly can better protect your product.



5. (Optional) Enable Hik-Connect service when activating the device if the device supports.
   1) Check **Enable Hik-Connect** checkbox to pop up the Note dialog.



   2) Create a verification code.
   3) Confirm the verification code.
   4) Click **Terms of Service** and **Privacy Policy** to read the requirements.
   5) Click **OK** to enable the Hik-Connect service.
6. Click **OK** to activate the device.
   A “The device is activated.” window pops up when the password is set successfully.
7. Click **Modify Netinfo** to pop up the Modify Network Parameter interface.
   Note: This function is only available on the **Online Device** area. You can change the device IP address to the same subnet with your computer if you need to add the device to the software.
8. Change the device IP address to the same subnet with your computer by either modifying the IP address manually or checking the checkbox of DHCP.
9. Input the password set in step 4 and click **OK** to complete the network settings.

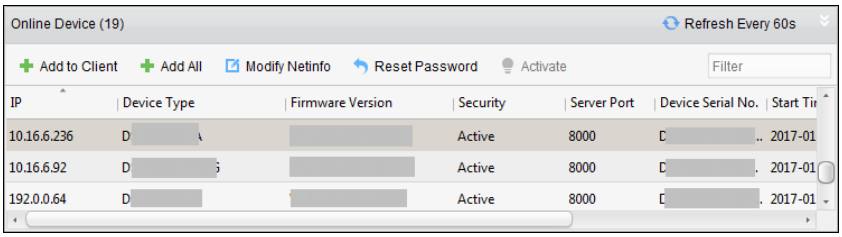


Adding Online Device

Purpose:

The active online devices in the same local subnet with the client software will be displayed on the **Online Device** area. You can click the **Refresh Every 60s** button to refresh the information of the online devices.

Note: You can click to hide the **Online Device** area.



Steps:

1. Select the devices to be added from the list.

   Note: For the inactive device, you need to create the password for it before you can add the device properly. For detailed steps, see *3.1 Device Activation*.
2. Click **Add to Client** to open the device adding dialog box.
3. Input the required information.

   Nickname: Edit a name for the device as you want.

   Address: Input the device's IP address. The IP address of the device is obtained automatically in this adding mode.

   Port: Input the device port No. The default value is *8000*.

   User Name: Input the device user name. By default, the user name is *admin*.

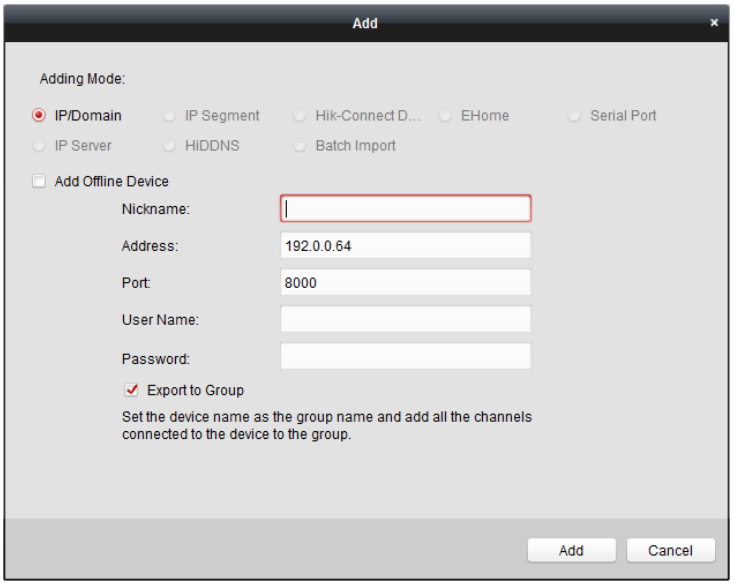
   Password: Input the device password.

   The password strength of the device can be checked by the software. For your privacy, we strongly recommend changing the password to something 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. Optionally, check the **Export to Group** checkbox to create a group by the device name.
   You can import all the channels of the device to the corresponding group by default.
   Note: iVMS-4200 also provides a method to add the offline devices.
   1) Check the **Add Offline Device** checkbox.
   2) **I**nput the required information, including the device channel number and alarm input number.
   3) Click **Add**.

   When the offline device comes online, the software will connect it automatically.
5. Click **Add** to add the device.

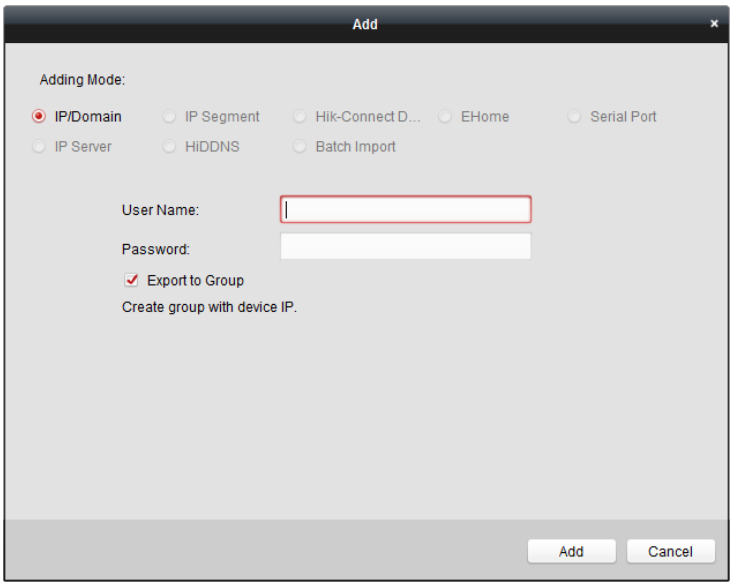


➢ Adding Multiple Online Device

If you want to add multiple online devices to the client software, click and hold *Ctrl* key to select multiple devices, and click **Add to Client** to open the device adding dialog box. In the pop-up message box, enter the user name and password for the devices to be added.

➢ Adding All Online Devices

If you want to add all the online devices to the client software, click **Add All** and click **OK** in the pop-up message box. Then enter the user name and password for the devices to be added.



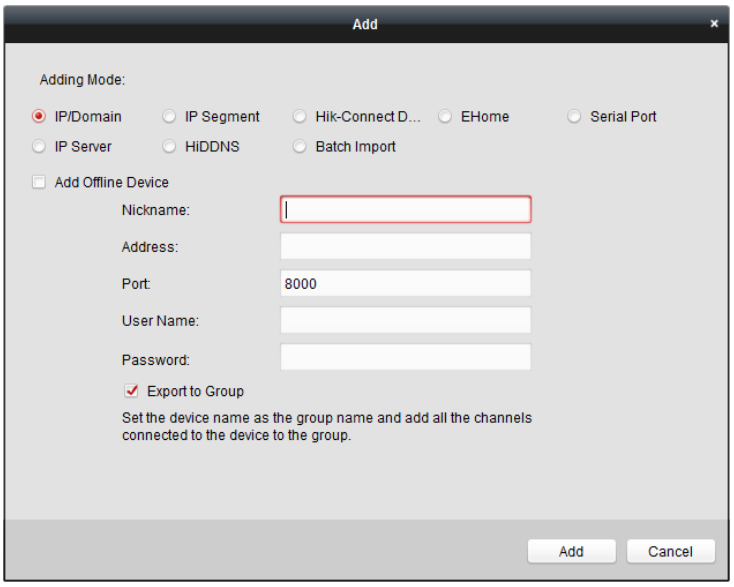
Adding Devices by IP or Domain Name

Steps:

1. Click **Add** to open the device adding dialog box.
2. Select **IP/Domain** as the adding mode.
3. Input the required information.
   Nickname: Edit a name for the device as you want.
   Address: Input the device's IP address or domain name.
   Port: Input the device port No.. The default value is *8000*.
   User Name: Input the device user name. By default, the user name is *admin*.
   Password: Input the device password.

   The password strength of the device can be checked by the software. For your privacy, we strongly recommend changing the password to something 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. Optionally, check the **Export to Group** checkbox to create a group by the device name.
   You can import all the channels of the device to the corresponding group by default.
   Note: iVMS-4200 also provides a method to add the offline devices.
   1) Check the **Add Offline Device** checkbox.
   2) **I**nput the required information, including the device channel number and alarm input number.
   3) Click **Add**.

   When the offline device comes online, the software will connect it automatically.
5. Click **Add** to add the device.



Adding Devices by IP Segment

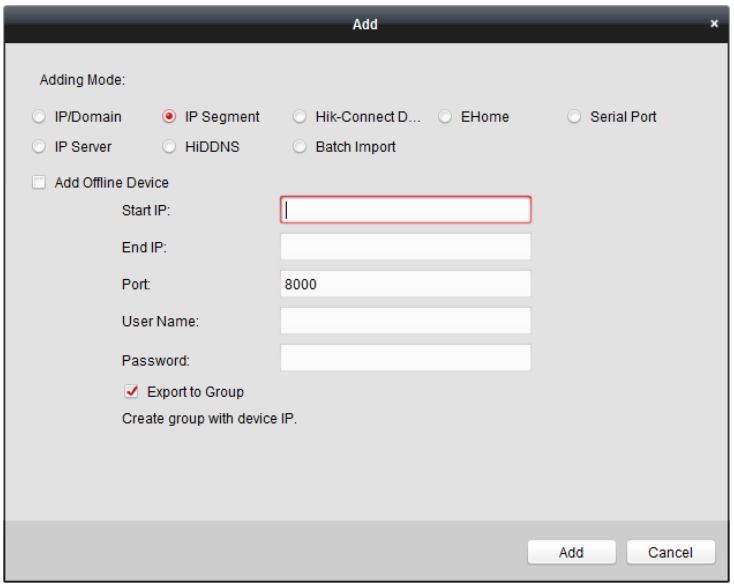
Steps:

1. Click **Add** to open the device adding dialog box.
2. Select **IP Segment** as the adding mode.
3. Input the required information.
   Start IP: Input a start IP address.
   End IP: Input an end IP address in the same network segment with the start IP.
   Port: Input the device port No.. The default value is *8000*.
   User Name: Input the device user name. By default, the user name is *admin*.
   Password: Input the device password.

   The password strength of the device can be checked by the software. For your privacy, we strongly recommend changing the password to something 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. Optionally, check the **Export to Group** checkbox to create a group by the device name.
   You can import all the channels of the device to the corresponding group by default.
   Note: iVMS-4200 also provides a method to add the offline devices.
   1) Check the **Add Offline Device** checkbox.
   2) **I**nput the required information, including the device channel number and alarm input number.
   3) Click **Add**.

   When the offline device comes online, the software will connect it automatically.
5. Click **Add**.
   You can add the device which the IP address is between the start IP and end IP to the device

list.



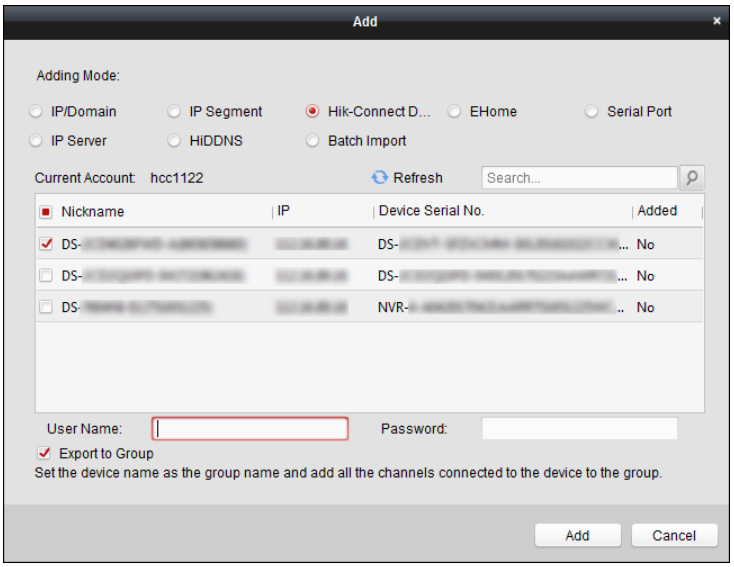
Adding Devices by Hik-Connect Domain

Purpose:

You can add the devices connected via Hik-Connect by inputting the Hik-Connect account and password.

Before you start: Add the devices to Hik-Connect account via iVMS-4200, iVMS-4500 Mobile Client, or Hik-Connect first. For details about adding the devices to Hik-Connect account via iVMS-4200, refer to *the User Manual of iVMS-4200 Client Software.*

1. Log into the Hik-Connect account. For details, refer to *User Manual of iVMS-4200 Client Software.*
2. Click **Hikvision Device -> Add** to open the device adding dialog.
1. Select **Hik-Connect Domain** as the adding mode.
   The device(s) under the Hik-Connect account will display.
2. (Optional) Click **Refresh** to refresh the device list.
3. (Optional) Input keyword of the device name in the **Search** field to search the device(s).
4. Check the checkbox(es) to select the device(s).
5. Input the device user name and the device password in the **User Name** field and **Password** field respectively.



Notes:

- The device user name is *admin* by default.
- The device password is created when you activate the device. For details, refer to *Chapter 3.1* Device Activation.

6. (Optional) Check the **Export to Group** checkbox to create a group by the device name. You can import all the channels of the device to the corresponding group by default.
7. Click **Add** to add the device to the local client.

Adding Devices by EHome Account

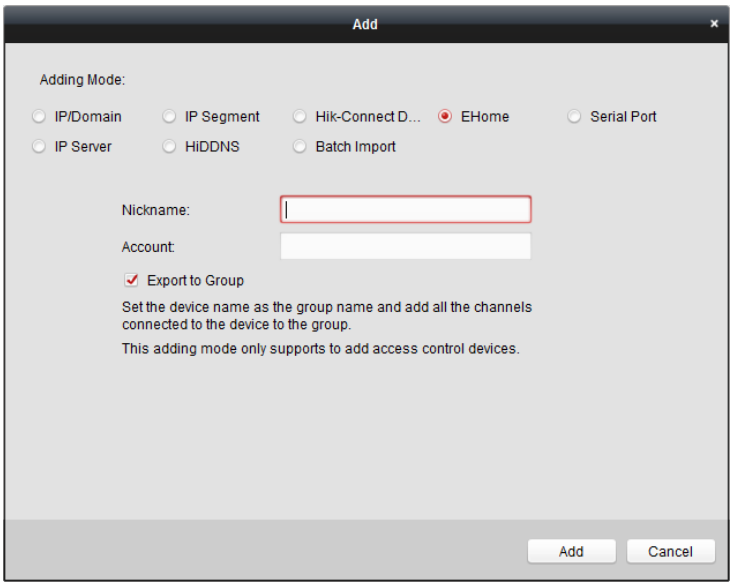
Purpose:

You can add access control device connected via EHome protocol by inputting the EHome account.

Before you start: Set the network center parameter first. For details, refer to *Chapter 4.4.4 Network Settings.*

Steps:

1. Click **Add** to open the device adding dialog box.
2. Select **EHome** as the adding mode.



3. Input the required information.
   Nickname: Edit a name for the device as you want.
   Account: Input the account name registered on EHome protocol.
4. Optionally, check the **Export to Group** checkbox to create a group by the device name.
   You can import all the channels of the device to the corresponding group by default.
   Note: iVMS-4200 also provides a method to add the offline devices.
   1) Check the **Add Offline Device** checkbox.
   2) **I**nput the required information, including the device channel number and alarm input number.
   3) Click **Add**.

   When the offline device comes online, the software will connect it automatically.
5. Click **Add** to add the device.

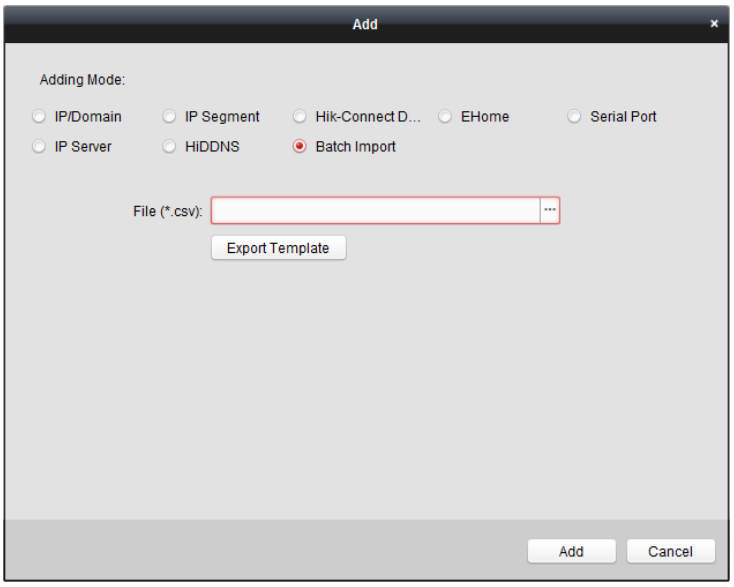
Importing Devices in Batch

Purpose:

The devices can be added to the software in batch by inputting the device information in the pre-defined CSV file.

Steps:

1. Click **Add** to open the device adding dialog box.
2. Select **Batch Import** as the adding mode.



3. Click **Export Template** and save the pre-defined template (CSV file) on your PC.
4. Open the exported template file and input the required information of the devices to be added on the corresponding column.

   Nickname: Edit a name for the device as you want.

   Adding Mode: You can input 0, 2, 3, 4, 5, or 6 which indicated different adding modes. 0 indicates that the device is added by IP address or domain name; 2 indicates that the device is added via IP server; 3 indicates that the device is added via HiDDNS; 4 indicates that the device is added via EHome protocol; 5 indicates that the device is added by serial port; 6 indicates that the device is added via Hik-Connect Domain.

   Address: Edit the address of the device. If you set 0 as the adding mode, you should input the IP address or domain name of the device; if you set 2 as the adding mode, you should input the IP address of the PC that installs the IP Server; if you set 3 as the adding mode, you should input *www.hik-online.com*.

   Port: Input the device port No.. The default value is *8000*.

   Device Information: If you set 0 as the adding mode, this field is not required; if you set 2 as the adding mode, input the device ID registered on the IP Server; if you set 3 as the adding mode, input the device domain name registered on HiDDNS server; if you set 4 as the adding mode, input the EHome account; if you set 6 as the adding mode, input the device serial No.

   User Name: Input the device user name. By default, the user name is *admin*.

   Password: Input the device password.

   The password strength of the device can be checked by the software. For your privacy, we strongly recommend changing the password to something 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.

   Add Offline Device: You can input 1 to enable adding the offline device, and then the software will automatically connect it when the offline device comes online. 0 indicates disabling this

function.

Export to Group: You can input 1 to create a group by the device name (nickname). All the channels of the device will be imported to the corresponding group by default. 0 indicates disabling this function.

Channel Number: If you set 1 for Add Offline Device, input the channel number of the device. If you set 0 for Add Offline Device, this field is not required.

Alarm Input Number: If you set 1 for Add Offline Device, input the alarm input number of the device. If you set 0 for Add Offline Device, this field is not required.

Serial Port No.: If you set 5 as the adding mode, input the serial port No. for the access control device.

Baud Rate: If you set 5 as the adding mode, input the baud rate of the access control device.

DIP: If you set 5 as the adding mode, input the DIP address of the access control device.

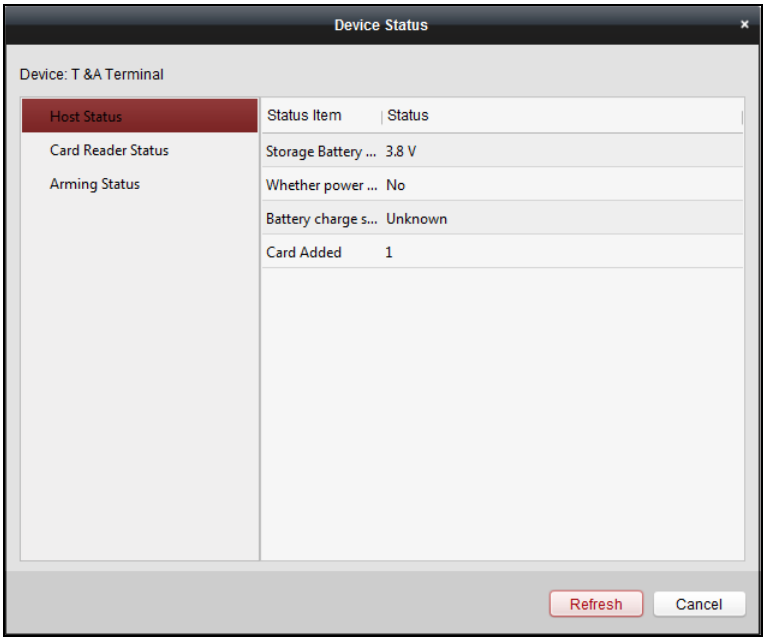
Hik-Connect Account: If you set 6 as the adding mode, input the Hik-Connect account.

Hik-Connect Password: If you set 6 as the adding mode, input the Hik-Connect password.

5. Click ··· and select the template file.
6. Click **Add** to import the devices.

4.4.2 Viewing Device Status

In the device list, you can select the device and then click **Device Status** button to view its status.



Note: The interface may different from the picture displayed above. Refer to the actual interface when adopting this function.

Host Status: The status of the host, including Storage Battery Power Voltage, Device Power Supply Status, Multi-door Interlocking Status, Anti-passing Back Status, and Host Anti-Tamper Status.

Card Reader Status: The status of card reader.

Arming Status: The status of the device.

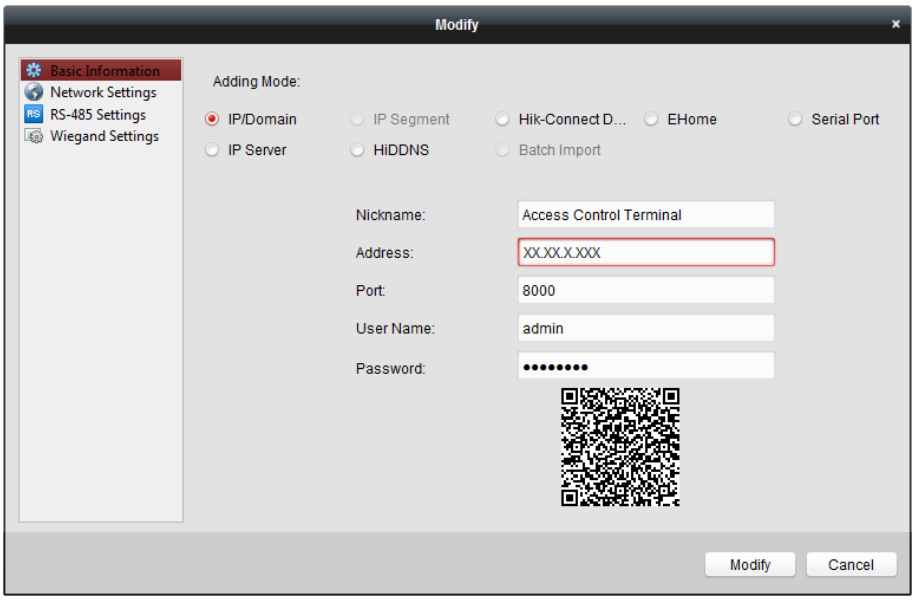
4.4.3 Editing Basic Information

Purpose:

After adding the access control device, you can edit the device basic information.

Steps:

1. Select the device in the device list.
2. Click **Modify** to pop up the modifying device information window.
3. Click **Basic Information** tab to enter the Basic Information interface.



4. Edit the device information, including the adding mode, the device name, the device IP address, port No., user name, and the password.

4.4.4 Network Settings

Purpose:

After adding the access control device, you can set the uploading mode, and set the network center and wireless communication center.

Select the device in the device list, and click **Modify** to pop up the modifying device information window.

Click **Network Settings** tab to enter the network settings interface.

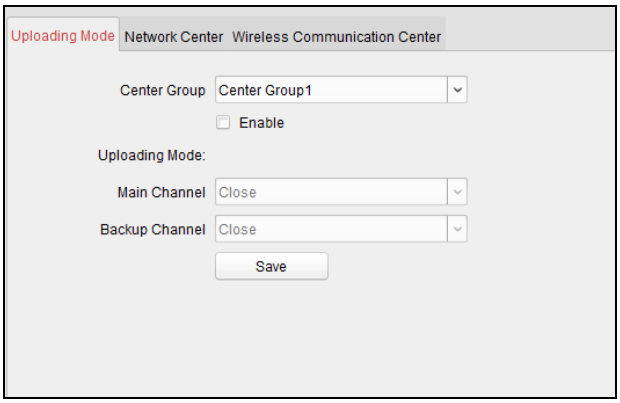
Uploading Mode Settings

Purpose：

You can set the center group for uploading the log via the EHome protocol.

Steps:

1. Click the **Uploading Mode** tab.



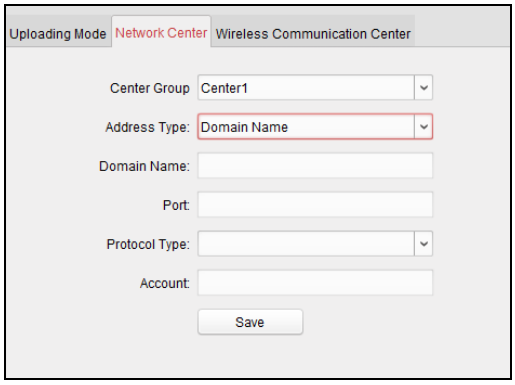
2. Select the center group in the dropdown list.
3. Check the **Enable** checkbox to enable the selected center group.
4. Select the uploading mode in the dropdown list. You can enable **N1/G1** for the main channel and the backup channel, or select **Close** to disable the main channel or the backup channel.
   Note: The main channel and the backup channel cannot enable N1 or G1 at the same time.
5. Click **Save** button to save parameters.

Network Center Settings

You can set the account for EHome protocol in Network Settings page. Then you can add devices via EHome protocol.

Steps:

1. Click the **Network Center** tab.



2. Select the center group in the dropdown list.
3. Select the address type.
4. Set the IP address/domain name.
5. Set the port No. for EHome protocol. By default, the port No. is 7660.
6. Select the protocol type as EHome.
7. Set an account name for the network center.
8. Click **Save** button to save parameters.

Notes:

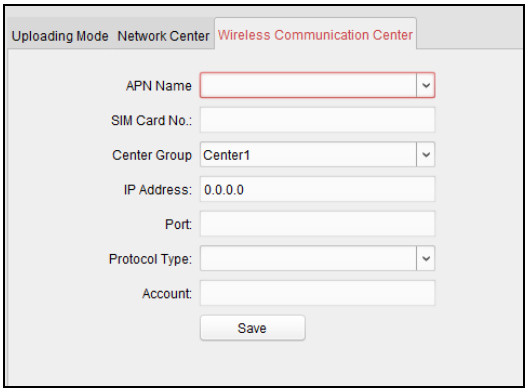
- The account should contain 1 to 32 characters and only letters and numbers are allowed.
- The port No. of the wireless network and wired network should be consistent with the port No. of EHome.
- You can set the domain name in Enable NTP area *Time* section in Remote Configuration. For

details, refer to *Time* in *4.4.5 Remote Configuration*.

Wireless Communication Center Settings

Steps:

1. Click the **Wireless Communication Center** tab.



2. Select the APN name as CMNET or UNINET.
3. Input the SIM Card No.
4. Select the center group in the dropdown list.
5. Input the IP address and port No.
6. Select the protocol type as EHome. By default, the port No. for EHome is 7660.
7. Set an account name for the network center. A consistent account should be used in one platform.
8. Click **Save** button to save parameters.

Note: The port No. of the wireless network and wired network should be consistent with the port No. of EHome.

4.4.5 Remote Configuration

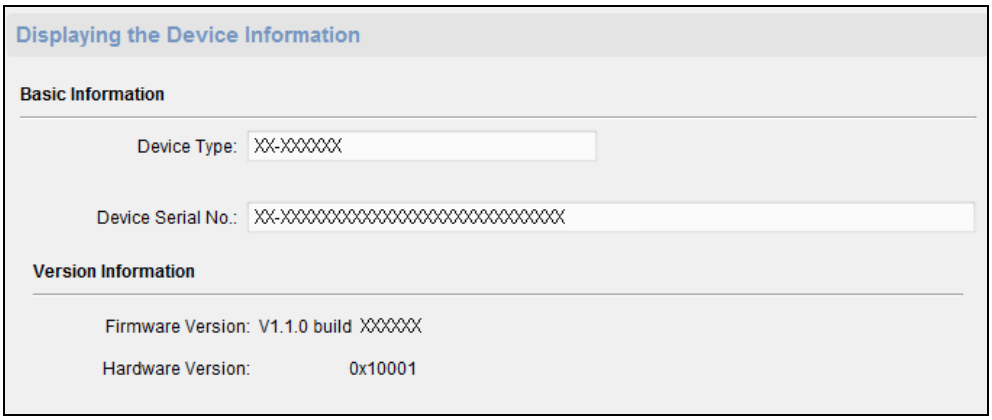
Purpose:

In the device list, select the device and click **Remote Configuration** button to enter the remote configuration interface. You can set the detailed parameters of the selected device.

Checking Device Information

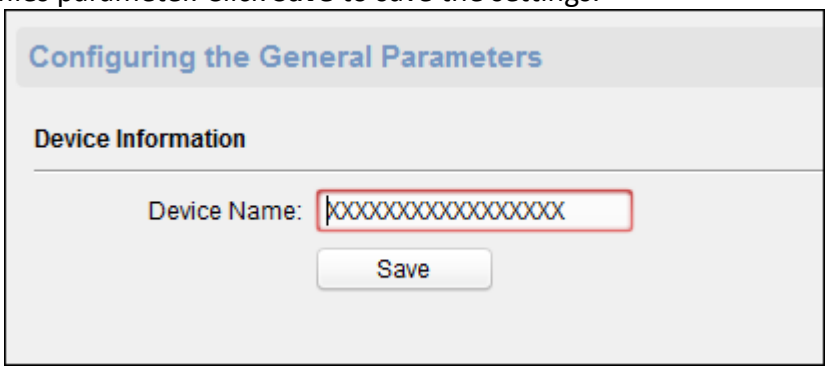
Steps:

1. In the device list, you can click **Remote Configuration** to enter the remote configuration interface.
2. Click **System** -> **Device Information** to check the device basic information and the device version information.



Editing Device Name

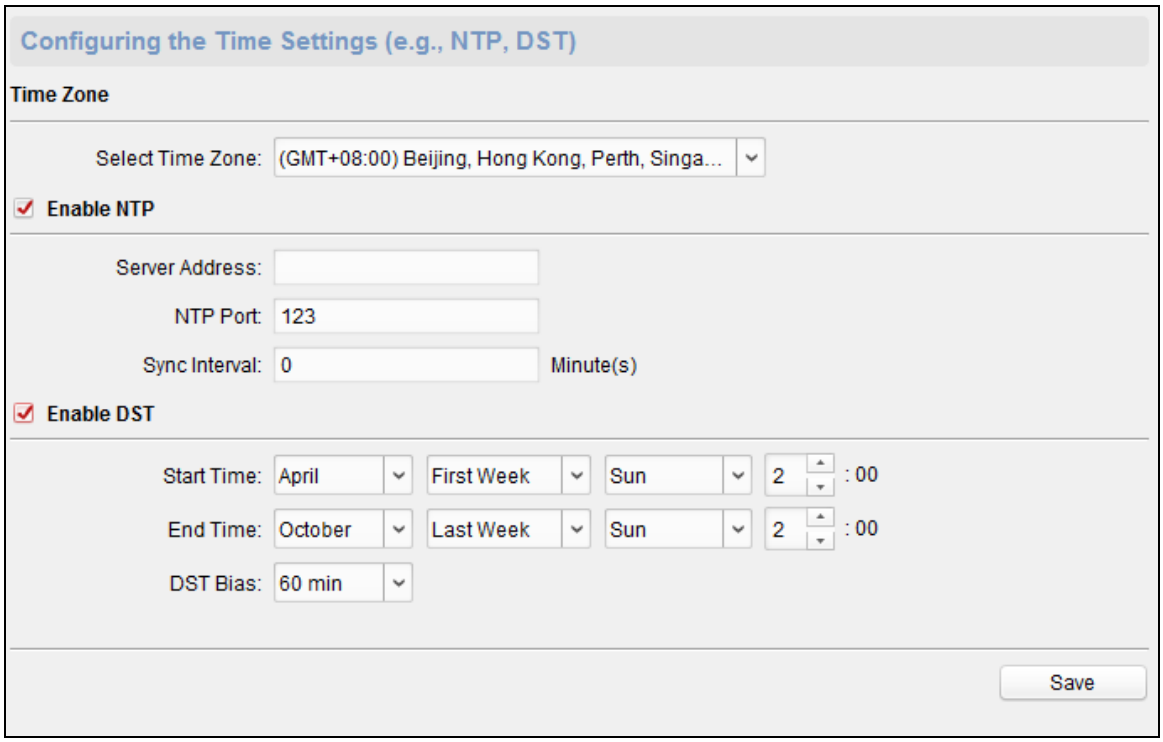
In the Remote Configuration interface, click **System** -> **General** to configure the device name and overwrite record files parameter. Click **Save** to save the settings.



Editing Time

Steps:

1. In the Remote Configuration interface, click **System** -> **Time** to configure the time zone.
2. (Optional) Check **Enable NTP** checkbox and configure the NTP server address, port No., and synchronization interval.
3. (Optional) Check **Enable DST** checkbox and configure the DST star time, end time and the bias.
4. Click **Save** to save the settings.



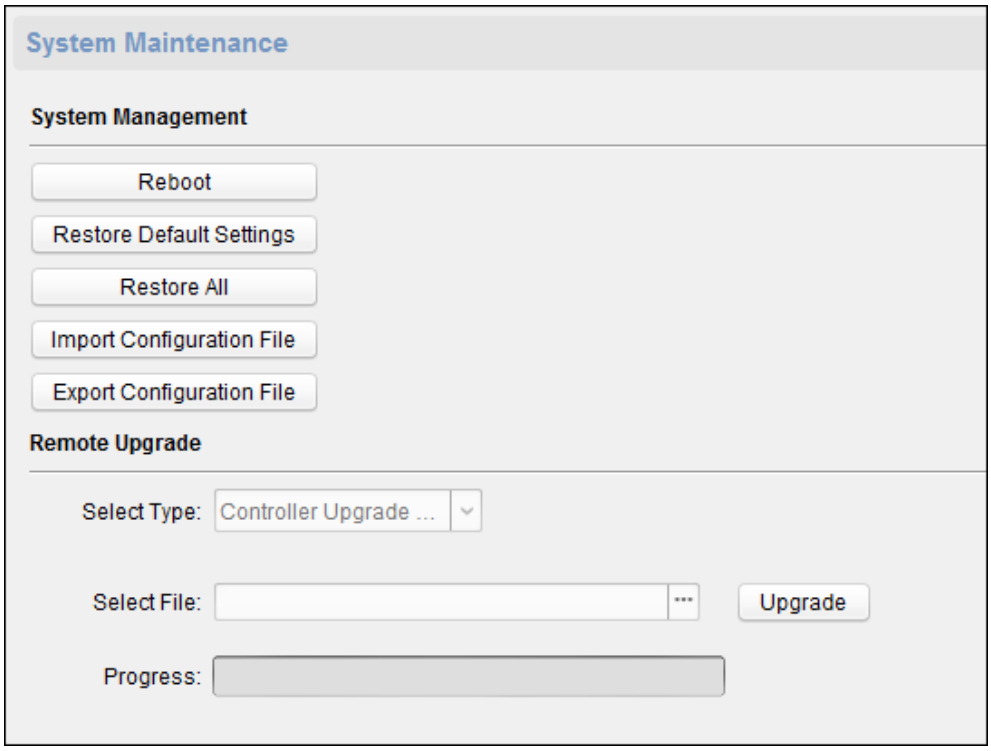
Setting System Maintenance

Purpose:

You can reboot the device remotely, restore the device to default settings, import configuration file, upgrade the device, etc.

Steps:

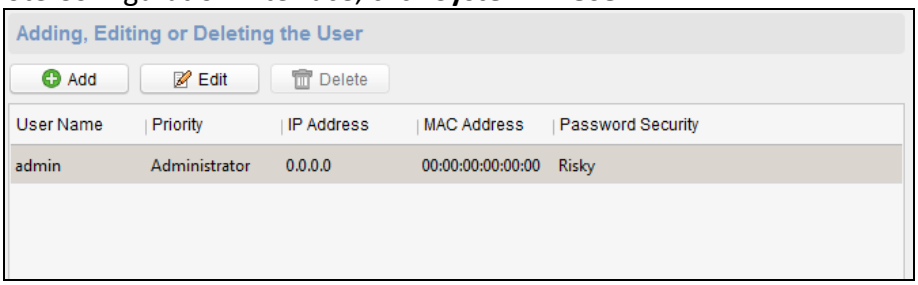
1. In the Remote Configuration interface, click **System** -> **System Maintenance**.
2. Click **Reboot** to reboot the device.
   Or click **Restore Default Settings** to restore the device settings to the default ones, excluding the IP address.
   Or click **Restore All** to restore the device parameters to the default ones. The device should be activated after restoring.
   Note: The configuration file contains the device parameters.
   Or click **Import Configuration File** to import the configuration file from the local PC to the device.
   Or click **Export Configuration File** to export the configuration file from the device to the local PC
   Note: The configuration file contains the device parameters.
3. You can also remote upgrade the device.
   1) In the Remote Upgrade part, click ··· to select the upgrade file.
   2) Click **Upgrade** to start upgrading.
      Note: Only the device connected via RS-485 supports card reader upgrading.



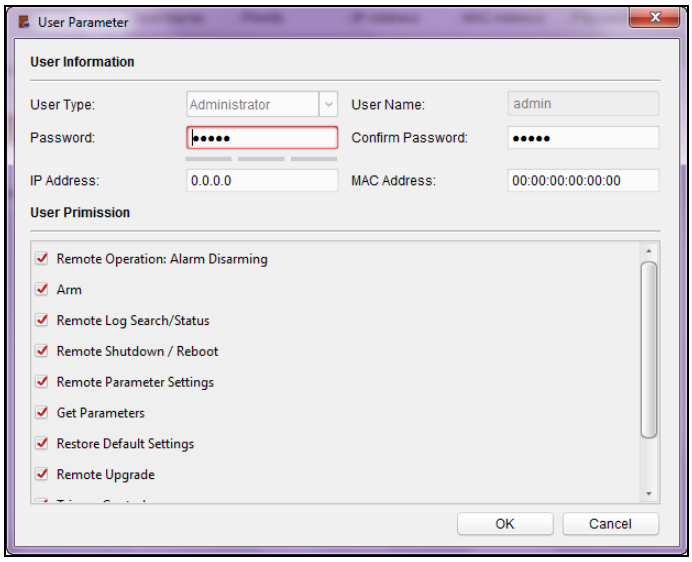
Managing User

Steps:

1. In the Remote Configuration interface, click **System** -> **User**.



2. Click **Add** to add the user (Do not support by the elevator controller.).
   Or select a user in the user list and click **Edit** to edit the user. You are able to edit the user password, the IP address, the MAC address and the user permission. Cilck **OK** to confirm editing.



Setting Security

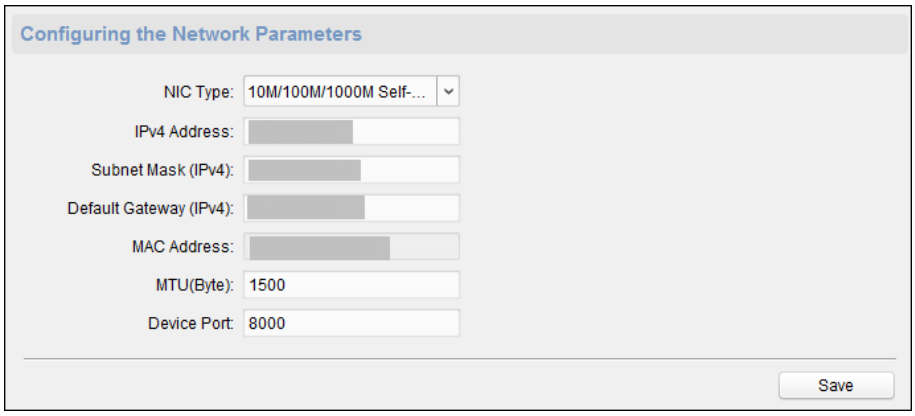
Steps:

1. Click **System** -> **Security**.

2. Select the encryption mode level in the dropdown list.
3. (Optional) Check **Enable SSH** checkbox and **Enable Illegal Login Lock** checkbox for the device security.
4. Click **Save** to save the settings.

Configuring Network Parameters

Click **Network** -> **General**. You can configure the NIC type, the IPv4 address, the subnet mask (IPv4), the default gateway (IPv4), MTU address, MTU, and the device port. Click **Save** to save the settings.



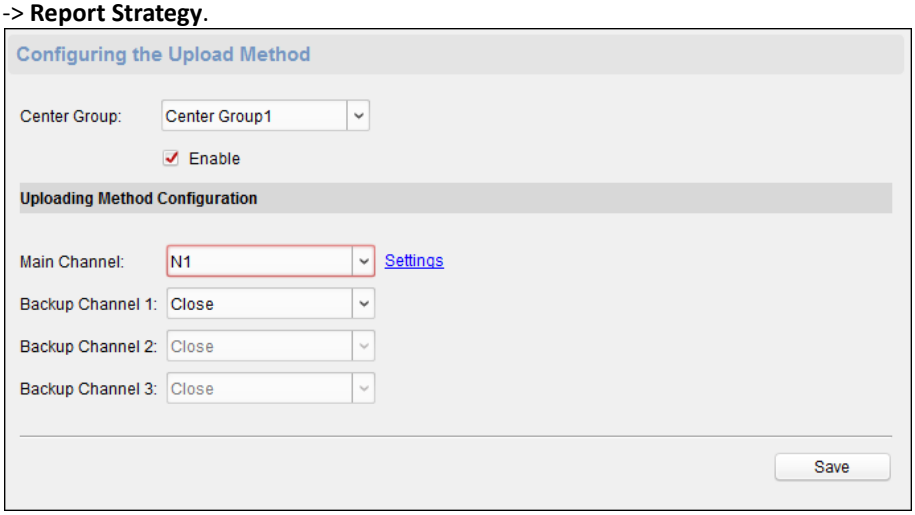
Configuring Upload Method

Purpose:

You can set the center group for uploading the log via the EHome protocol.

Steps:

1. Click **Network** -> **Report Strategy**.



2. Select a Center Group from the drop-down list.
3. Check the **Enable** check box.
4. Set the uploading method.
   You can set the main channel and the backup channel.
5. Click **Settings** on the right of the channel field to set the detailed information.
6. Click **Save** to save the settings.

Configuring Network Center Parameters

Purpose:

You can set the center network parameters when adding the device by EHome account.

Note: For details about adding device by EHome account, refer to *Chapter 4.4.1 Adding Access Control Device*.

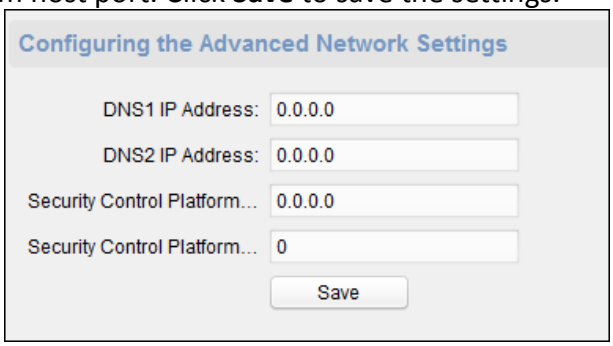
Steps:

1. Click **Network** –> **Network Center Configuration**.
2. Select Notify Surveillance Center in the dropdown list.
3. Set the center IP address, port No., protocol type, and user name.

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

Configuring Advanced Network

Click **Network** -> **Advanced Settings**. You can configure the DNS address 1, the DNS address 2, the alarm host IP and the alarm host port. Click **Save** to save the settings.



Configuring Wi-Fi

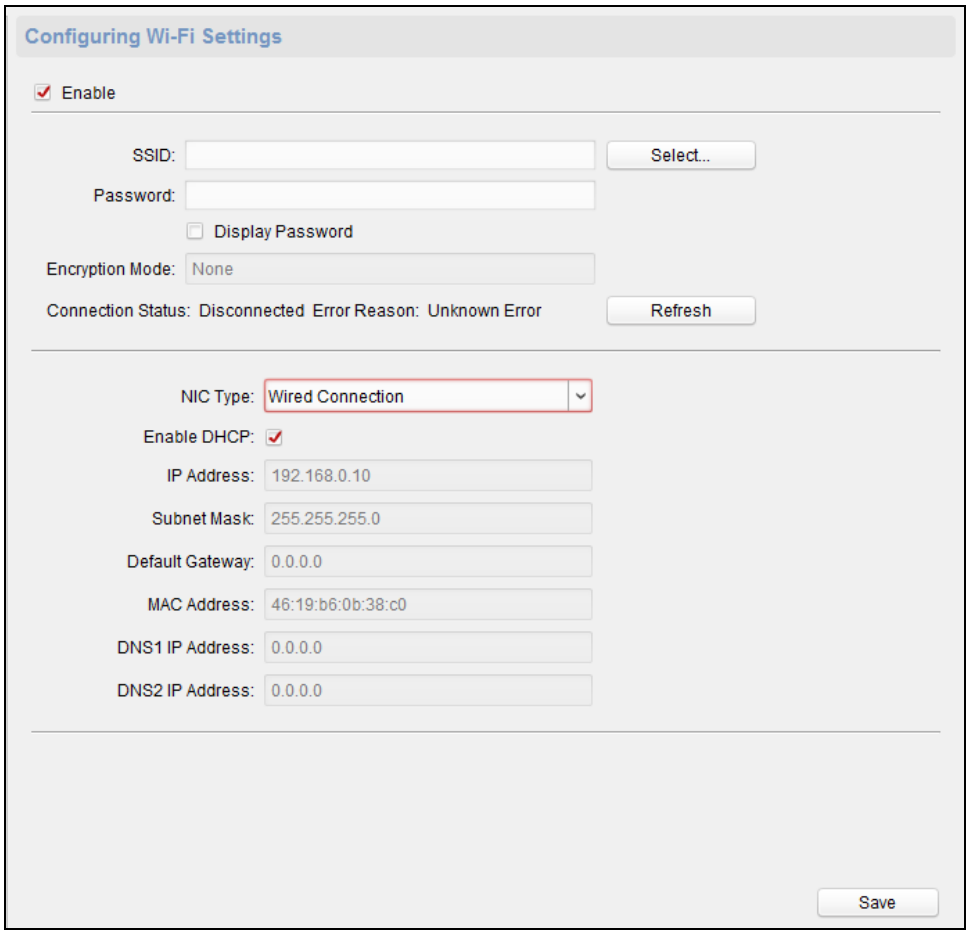
Purpose:

You can set the device Wi-Fi parameters for device to connect the Wi-Fi.

Note: The device model with -1 does not support the function.

Steps:

1. Click **Network -> Wi-Fi**.



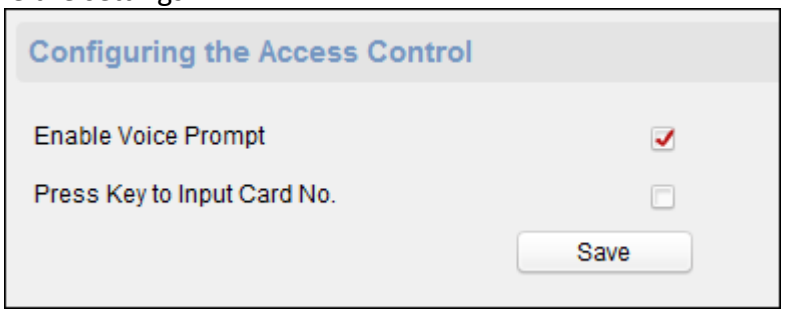
2. Check **Enable** checkbox.

3. Set the Wi-Fi SSID (Network Name).
   Or you can click **Select…** to select the Wi-Fi.
4. Input the Wi-Fi password.
5. (Optional) Click **Refresh** to refresh the Wi-Fi status.
6. (Optional) Select the NIC type.
   You can select either Wired Connection or Auto Switch.
7. (Optional) You can disable DHCP and set the network IP address, subnet mask, default gateway, MAC address, DNS1 IP Address, and DNS2 IP Address manually.
8. Click **Save** to save the settings.

Configuring Access Control Parameters

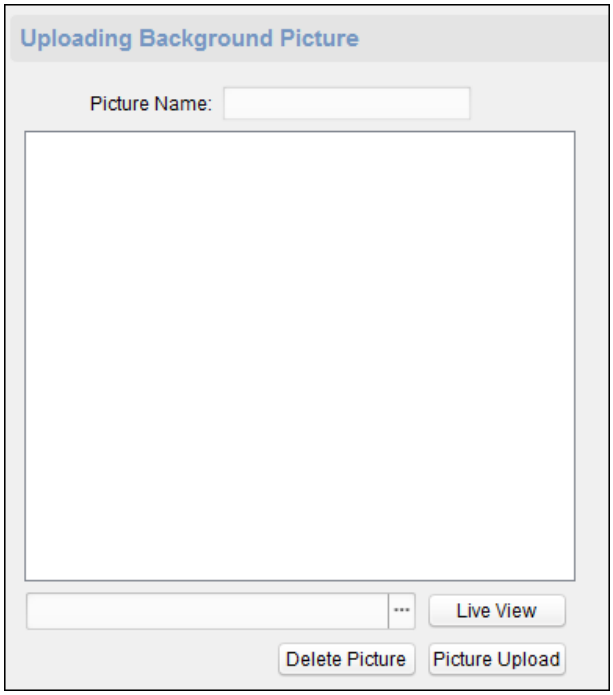
Steps:

1. In the Remote Configuration interface, click **Other** -> **Access Control Parameters**.
2. Select and check the item as you desired.
   Enable Voice Prompt: If check the checkbox, the voicce pormpt is enabled in the device. You can hear the voice prompt when operating in the device.
   Press Key to Input Card No.: If you check the checkbox, you can input the card No. by pressing the key.
3. Click **Save** to save the settings.



Uploading Background Picture

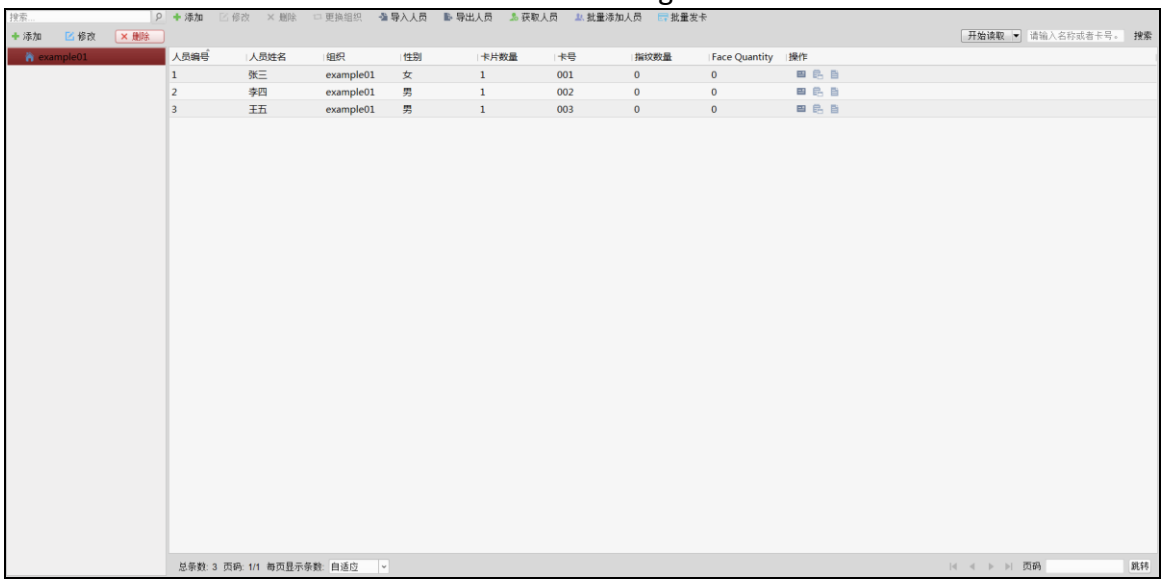
Click **Other** -> **Picture Upload**. Click ··· to select the picture from the local. You can also click **Live View** to preview the picture. Click **Picture Upload** to upload the picture.



4.5 Organization Management

You can add, edit, and delete the organization as desired.

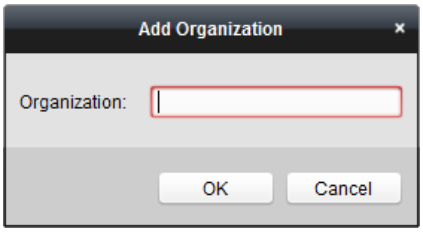
Click  tab to enter the Person and Card Management interface.



4.5.1 Adding Organization

Steps:

1. In the organization list on the left, you should add a top organization as the parent organization of all organizations.
   Click **Add** button to pop up the adding organization interface.



2. Input the Organization Name as desired.
3. Click **OK** to save the adding.
4. You can add multiple levels of organizations according to the actual needs.
   To add sub organizations, select the parent organization and click **Add**.
   Repeat *Step 2* and *3* to add the sub organization.
   Then the added organization will be the sub-organization of the upper-level organization.

Note: Up to 10 levels of organizations can be created.

4.5.2 Modifying and Deleting Organization

You can select the added organization and click **Modify** to modify its name.
You can select an organization, and click **Delete** button to delete it.

Notes:

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

4.6 Person Management

After adding the organization, you can add person to the organization and manage the added person such as issuing cards in batch, importing and exporting persons information in batch, etc.

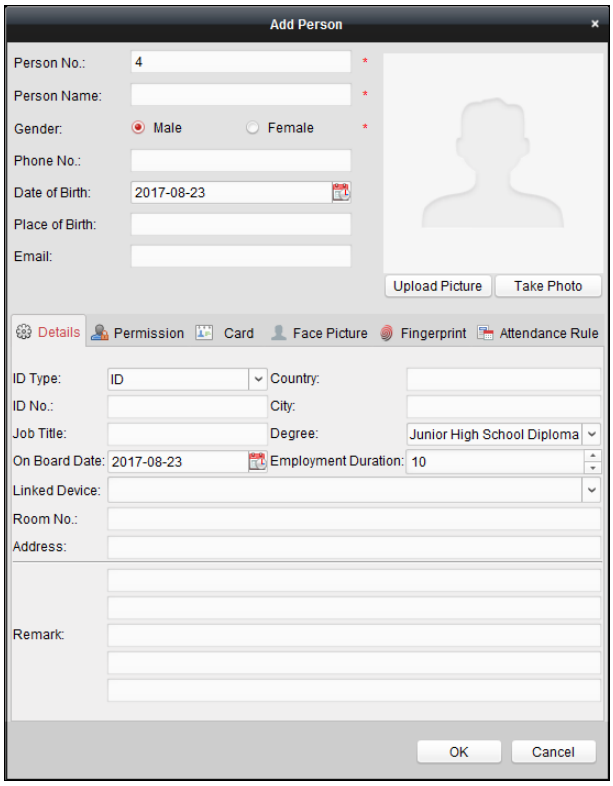
Note: Up to 10,000 persons or cards can be added.

4.6.1 Adding Person

Adding Person (Basic Information)

Steps:

1. Select an organization in the organization list and click **Add** button on the Person panel to pop up the adding person dialog.

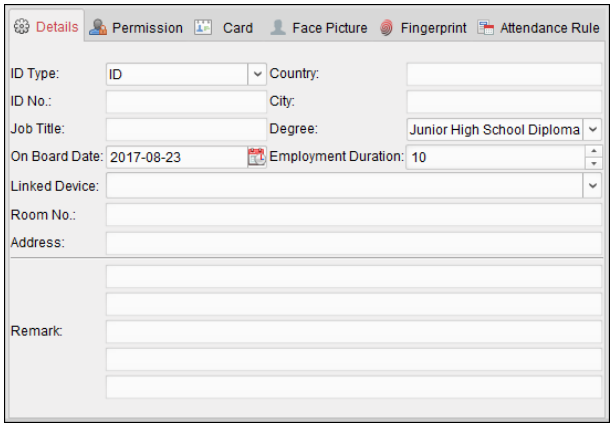


2. The Person No. will be generated automatically and is not editable.
3. Input the basic information including person name, gender, phone No., birthday details, and email address.
4. Click **Upload Picture** to select the person picture from the local PC to upload it to the client.
   Note: The picture should be in *.jpg format.
5. (Optional) You can also click **Take Phone** to take the person's photo with the PC camera.
6. Click **OK** to finish adding.

Adding Person (Detailed Information)

Steps:

1. In the Add Person interface, click **Details** tab.



2. Input the detailed information of the person, including person's ID type, ID No., country, etc., according to actual needs.
   - **Linked Device:** You can bind the indoor station to the person.

Note: If you select **Analog Indoor Station** in the Linked Device, the **Door Station** field will display and you are required to select the door station to communicate with the analog indoor station.

- **Room No.:** You can input the room No. of the person.

3. Click **OK** to save the settings.

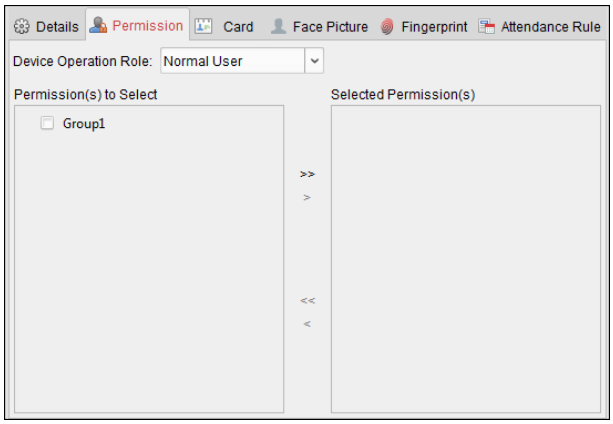
Adding Person (Permission)

You can assign the permissions (including operation permissions of access control device and access control permissions) to the person when adding person.

Note: For setting the access control permission, refer to *Chapter 4.8 Permission Configuration.*

Steps:

1. In the Add Person interface, click **Permission** tab.



2. In the Device Operation Role field, select the role of operating the access control device.
   Normal User: The person has the permission to check-in/out on the device, pass the access control point, etc.
   Administrator: The person has the normal user permission, as well as permission to configure the device, including adding normal user, etc.
3. In the Permission(s) to Select list, all the configured permissions display.
   Check the permission(s) checkbox(es) and click **>** to add to the Selected Permission(s) list.
   (Optional) You can click **>>** to add all the displayed permissions to the Selected Permission(s) list.
   (Optional) In the Selected Permission(s) list, select the selected permission and click **<** to remove it. You can also click **<<** to remove all the selected permissions.
4. Click **OK** to save the settings.

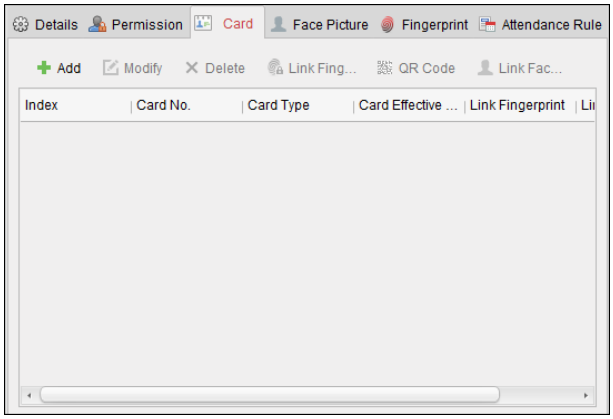
Adding Person (Card)

You can add card and issue the card to the person.

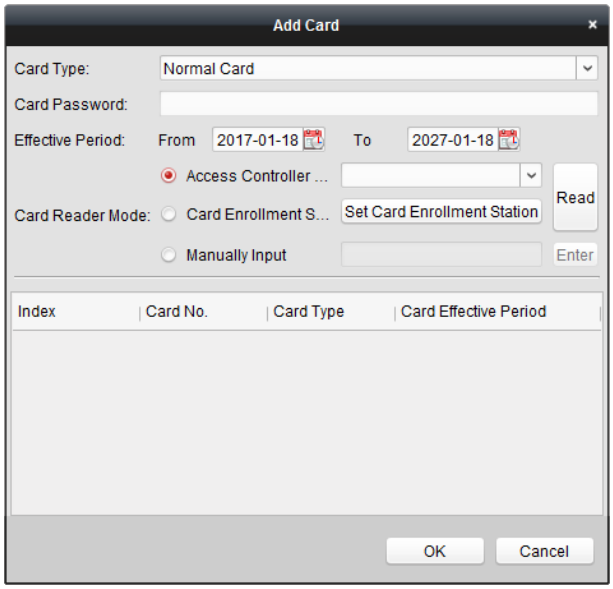
Note: Up to 5 cards can be added to each person.

Steps:

1. In the Add Person interface, click **Card** tab.



2. Click **Add** to pop up the Add Card dialog.



3. Select the card type according to actual needs.
   - **Normal Card**
   - **Card for Disabled Person**: The door will remain open for the configured time period for the card holder.
   - **Card in Blacklist**: The card swiping action will be uploaded and the door cannot be opened.
   - **Patrol Card**: The card swiping action can used for checking the working status of the inspection staff. The access permission of the inspection staff is configurable.
   - **Duress Card**: The door can open by swiping the duress card when there is duress. At the same time, the client can report the duress event.
   - **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. For the Visitor Card, you can set the **Max. Swipe Times**.

     Notes:
     - The Max. Swipe Times should be between 0 and 255. When your swiping card times is more than the configured times, card swiping will be invalid.
     - When set the times as 0, it means the card swiping is unlimited.

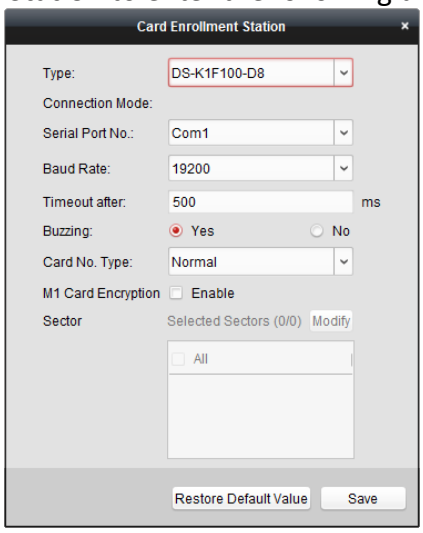
- **Dismiss Card:** The alarm will be dismissed after swiping the dismiss card.

4. Input the password of the card itself in the Card Password field. The card password should contain 4 to 8 digits.

   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 reader authentication mode as **Card and Password**, **Password and Fingerprint**, and **Card, Password, and Fingerprint**. For details, refer to *Chapter 4.9.2 Card Reader Authentication.*

5. Click  to set the effective time and expiry time of the card.
6. Select the Card Reader Mode for reading the card No.
   - **Access Controller Reader:** Place the card on the reader of the Access Controller and click **Read** to get the card No.
   - **Card Enrollment Station:** Place the card on the Card Enrollment Station and click **Read** to get the card No.

     Note: The Card Enrollment Station should connect with the PC running the client. You can click **Set Card Enrollment Station** to enter the following dialog.



     2) Select the Card Enrollment Station type.

        Note: Currently, the supported card reader types include DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E, and DS-K1F180-D8E.

     3) Set the serial port No., the baud rate, the timeout value, the buzzing, or the card No. type.

        Note: The fingerprint time attendance terminal does not support the M1 encryption function.

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

     You can click **Restore Default Value** button to restore the defaults.

   - **Manually Input:** Input the card No. and click **Enter** to input the card No.

7. Click **OK** and the card(s) will be issued to the person.
8. (Optional) You can select the added card and click **Modify**, **Delete** or **QR Code** to edit or delete the card or generate the QR code for the card.
9. (Optional) You can generate and save the card QR code for QR code authentication.
   1) Select an added card and click **QR Code** to generate the card QR code.

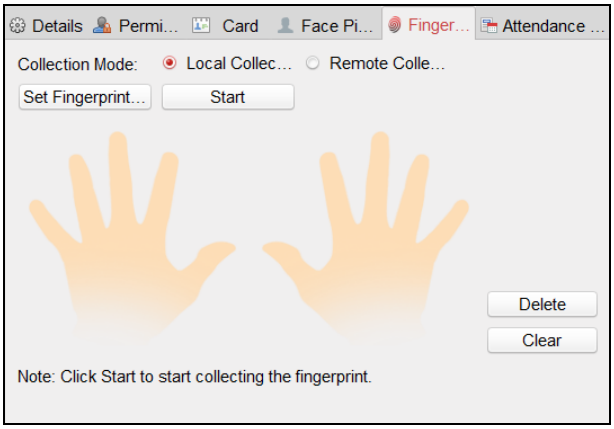
2) In the QR code pop-up window, click **Download** to save the QR code to the local PC.
You can print the QR code for authentication on the specified device.
Note: The device should support the QR code authentication function. For details about setting the QR code authentication function, see the specified device user manual.

10. Click **OK** to save the settings.

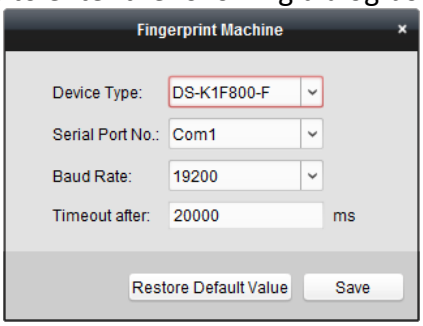
Adding Person (Fingerprint)

Steps:

1. In the Add Person interface, click **Fingerprint** tab.



2. Select **Local Collection** as the collection mode.
3. Before inputting the fingerprint, you should connect the fingerprint machine to the PC and set its parameters first.
Click **Set Fingerprint Machine** to enter the following dialog box.



1) Select the device type.
Currently, the supported fingerprint machine types include DS-K1F800-F, DS-K1F300-F, DS-K1F810-F, and DS-K1F820-F, and DS-K1F181-F.
2) For fingerprint machine type DS-K1F800-F, you can set the serial port number, baud rate, and overtime parameters of the fingerprint machine.
3) Click **Save** button to save the settings.
You can click **Restore Default Value** button to restore the default settings.

Notes:

- The serial port number should correspond to the serial port number of PC. You can check the serial port number in Device Manager in your PC.
- The baud rate should be set according to the external fingerprint card reader. The default value is 19200.

- **Timeout after** field 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.

4. Click **Start** button, click to select the fingerprint to start collecting.
5. Lift and rest the corresponding fingerprint on the fingerprint scanner twice to collect the fingerprint to the client.
6. (Optional) You can also click **Remote Collection** to collect fingerprint from the device.
   Note: The function should be supported by the device.
7. (Optional) You can select the registered fingerprint and click **Delete** to delete it.
   You can click **Clear** to clear all fingerprints.
8. Click **OK** to save the fingerprints.

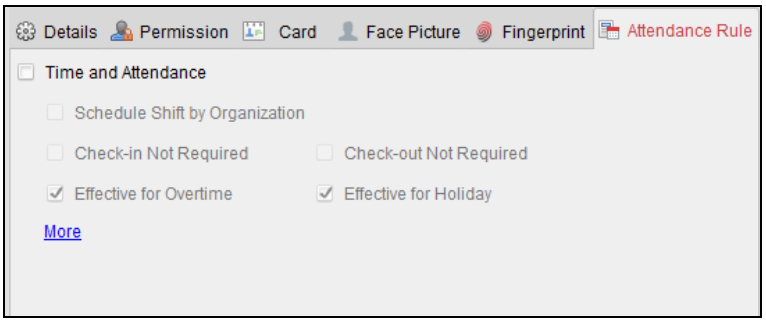
Adding Person (Attendance Rule)

You can set the attendance rule for the person.

Note: This tab page will display when you select **Non-Residence** mode in the application scene when running the software for the first time.

Steps:

1. In the Add Person interface, click **Attendance Rule** tab.



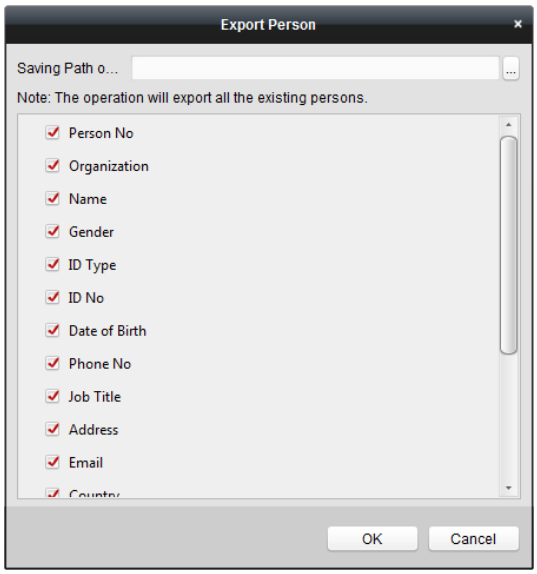
2. If the person joins in the time and attendance, check the **Time and Attendance** checkbox to enable this function for the person. Then the person's card swiping records will be recorded and analyzed for time and attendance.
   For details about Time and Attendance, click **More** to go to the Time and Attendance module.
3. Click **OK** to save the settings.

Importing and Exporting Person Information

The person information can be imported and exported in batch.

Steps:

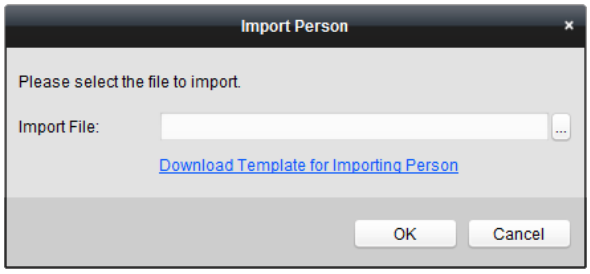
1. **Exporting Person:** You can export the added persons' information in Excel format to the local PC.
   1) After adding the person, you can click **Export Person** button in the Person and Card tab to pop up the following dialog.
   2) Click ... to select the path of saving the exported Excel file.
   3) Check the checkboxes to select the person information to export.



4) Click **OK** to start exporting.

2. **Importing Person:** You can import the Excel file with persons information in batch from the local PC

1) click **Import Person** button in the Person and Card tab.



2) You can click **Download Template for Importing Person** to download the template first.
3) Input the person information to the downloaded template.
4) Click ... to select the Excel file with person information.
5) Click **OK** to start importing.

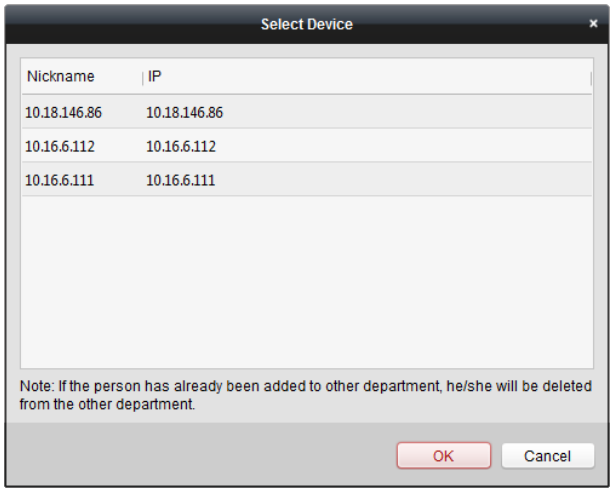
Getting Person Information from Access Control Device

If the added access control device has been configured with person information (including person details, fingerprint, issued card information), you can get the person information from the device and import to the client for further operation.

Note: This function is only supported by the device the connection mothod of which is TCP/IP when adding the device.

Steps:

1. In the organization list on the left, click to select an organization to import the persons.
2. Click **Get Person** button to pop up the following dialog box.



3. The added access control device will be displayed.
4. Click to select the device and then click **OK** to start getting the person information from the device.
   You can also double click the device name to start getting the person information.

Notes:

- The person information, including person details, person's fingerprint information (if configured), and the linked card (if configured), will be imported to the selected organization.
- If the person name stored in the device is empty, the person name will be filled with the issued card No. after importing to the client.
- The gender of the persons will be **Male** by default.
- Up to 10000 persons with up to 5 cards each can be imported.

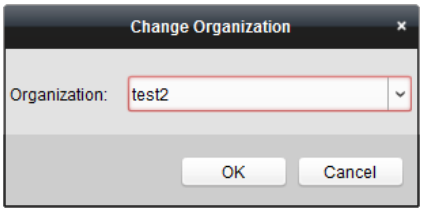
Modifying and Deleting Person

To modify the person information and attendance rule, click or in the Operation column, or select the person and click **Modify** to open the editing person dialog.
You can click to view the person's card swiping records.
To delete the person, select a person and click **Delete** to delete it.
Note: If a card is issued to the current person, the linkage will be invalid after the person is deleted.

Changing Person to Other Organization

You can move the person to another organization if needed.
Steps:

1. Select the person in the list and click **Change Organization** button.



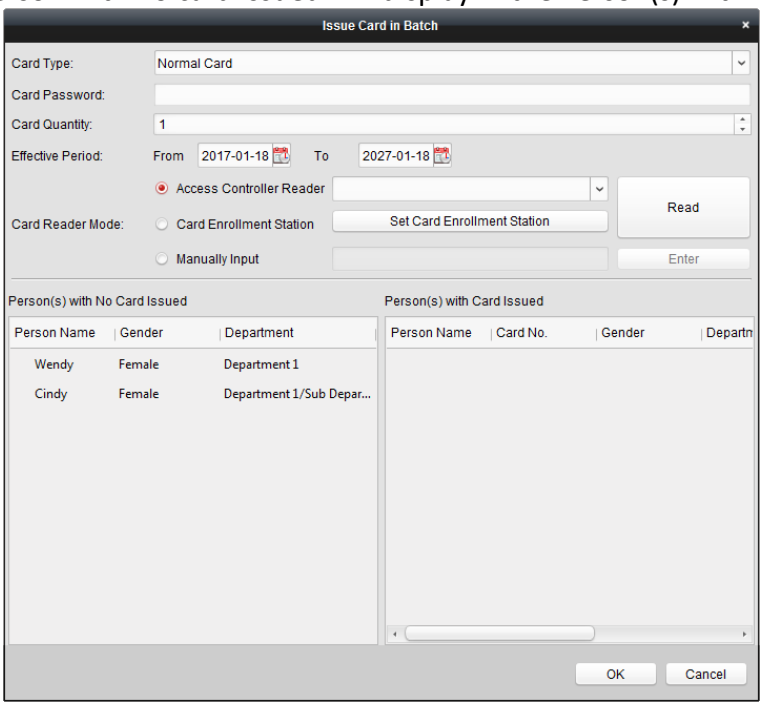
2. Select the organization to move the person to.
3. Click **OK** to save the settings.

Issuing Card in Batch

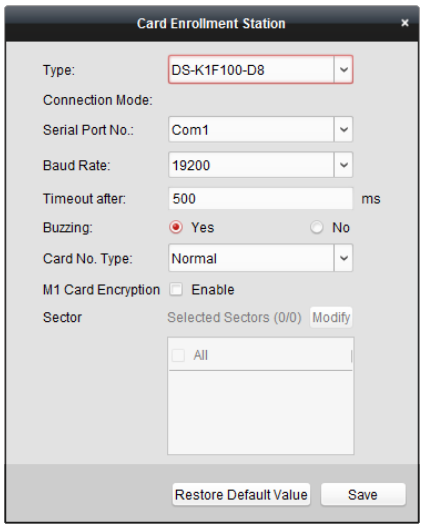
You can issue multiple cards for the person with no card issued in batch.

Steps:

1. Click **Issue Card in Batch** button to enter the following dialog.
   All the added person with no card issued will display in the Person(s) with No Card Issued list.



2. Select the card type according to actual needs.
   Note: For details about the card type, refer to *Adding Person.*
3. Input the password of the card itself in the Card Password field. The card password should contain 4 to 8 digits.
   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 reader authentication mode as **Card and Password**, **Password and Fingerprint**, and **Card, Password, and Fingerprint**. For details, refer to *Chapter 4.9.2 Card Reader Authentication.*
4. Input the card quantity issued for each person.
   For example, if the Card Quantity is 3, you can read or enter three card No. for each person.
5. Click to set the effective time and expiry time of the card.
6. Select the Card Reader Mode for reading the card No.
   - **Access Controller Reader:** Place the card on the reader of the Access Controller and click **Read** to get the card No.
   - **Card Enrollment Station:** Place the card on the Card Enrollment Station and click **Read** to get the card No.
     Note: The Card Enrollment Station should connect with the PC running the client. You can click **Set Card Enrollment Station** to enter the following dialog.



1) Select the Card Enrollment Station type.

   Note: Currently, the supported card reader types include DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E, and DS-K1F180-D8E.

2) Set the serial port No., the baud rate, the timeout value, the buzzing, or the card No. type.

   Note: The fingerprint time attendance terminal does not support the M1 encryption function.

3) Click **Save** button to save the settings.

You can click **Restore Default Value** button to restore the defaults.

- **Manually Input:** Input the card No. and click **Enter** to input the card No.

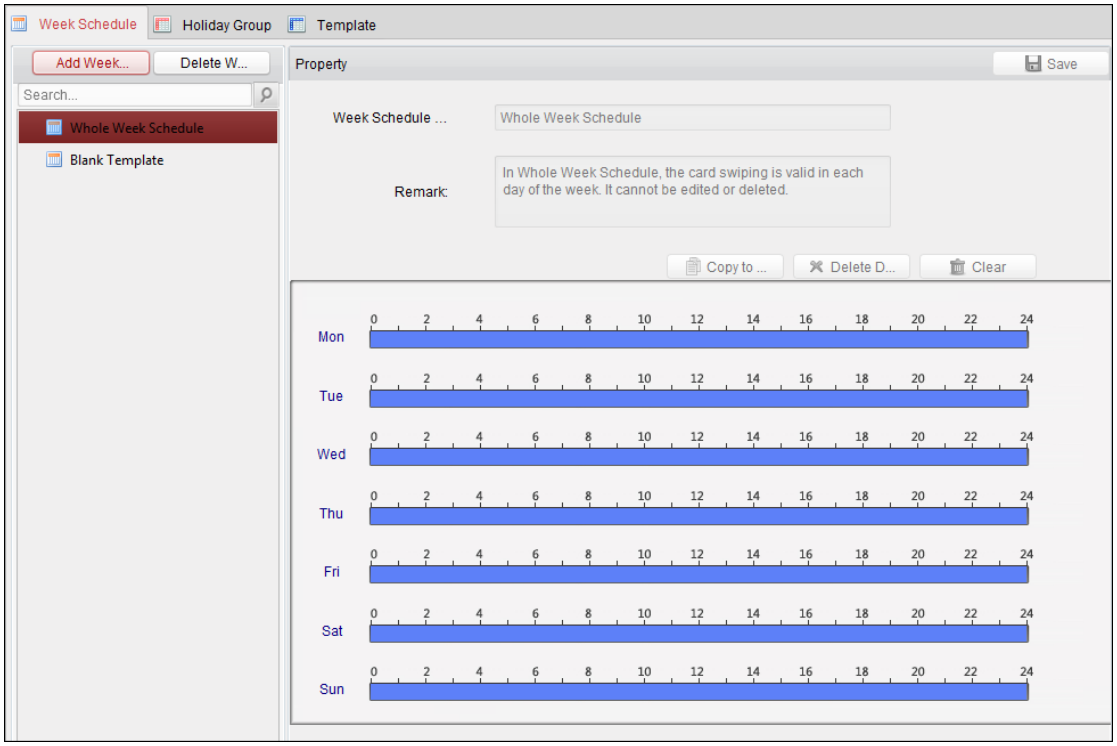
7. After issuing the card to the person, the person and card information will display in the Person(s) with Card Issued list.
8. Click **OK** to save the settings.

4.7 Schedule and Template

Purpose:

You can configure the template including week schedule and holiday schedule. After setting the templates, you can adopt the configured templates to access control permissions when setting the permission, so that the access control permission will take effect in the time durations of the template.

Click  to enter the schedule and template interface.



You can manage the schedule of access control permission including Week Schedule, Holiday Schedule, and Template. For permission settings, please refer to *Chapter 4.8 Permission Configuration.*

4.7.1 Week Schedule

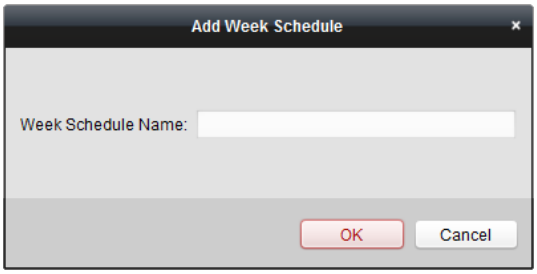
Click **Week Schedule** tab to enter the Week Schedule Management interface.
The client defines two kinds of week plan by default: **Whole Week Schedule** and **Blank Schedule**, which cannot be deleted and edited.

- **Whole Week Schedule:** Card swiping is valid on each day of the week.
- **Blank Schedule:** Card swiping is invalid on each day of the week.

You can perform the following steps to define custom schedules on your demand.

Steps:

1. Click **Add Week Schedule** button to pop up the adding schedule interface.



2. Input the name of week schedule and click **OK** button to add the week schedule.
3. Select the added week schedule in the schedule list and you can view its property on the right. You can edit the week schedule name and input the remark information.
4. On the week schedule, click and drag on a day to draw on the schedule, which means in that

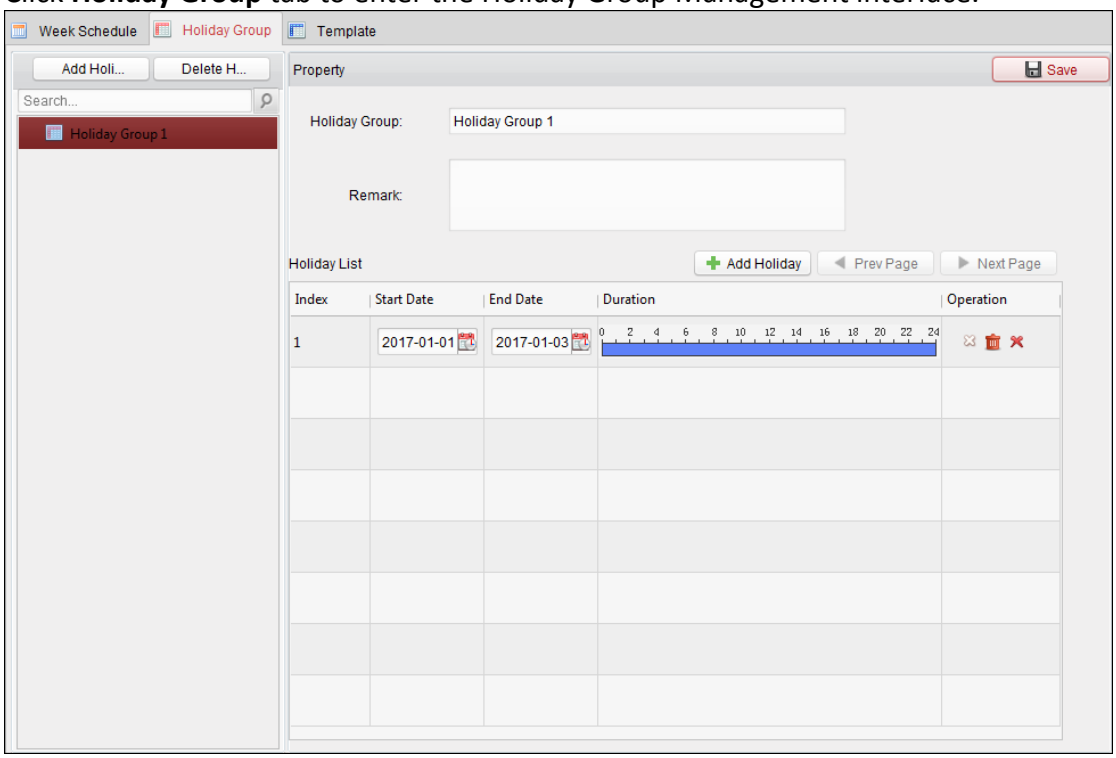
period of time, the configured permission is activated.

Note: Up to 8 time periods can be set for each day in the schedule.

5. When the cursor turns to , you can move the selected time bar you just edited. You can also edit the displayed time point to set the accurate time period.
   When the cursor turns to , you can lengthen or shorten the selected time bar.
6. Optionally, you can select the schedule time bar,
   and then click **Delete Duration** to delete the selected time bar,
   or click **Clear** to delete all the time bars,
   or click **Copy to Week** to copy the time bar settings to the whole week.
7. Click **Save** to save the settings.

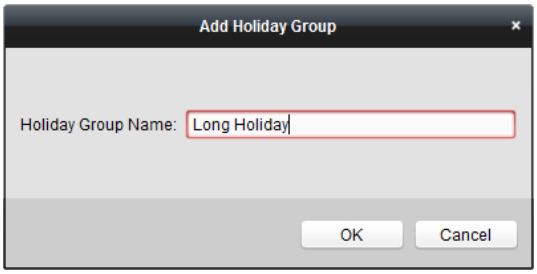
4.7.2 Holiday Group

Click **Holiday Group** tab to enter the Holiday Group Management interface.



Steps:

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

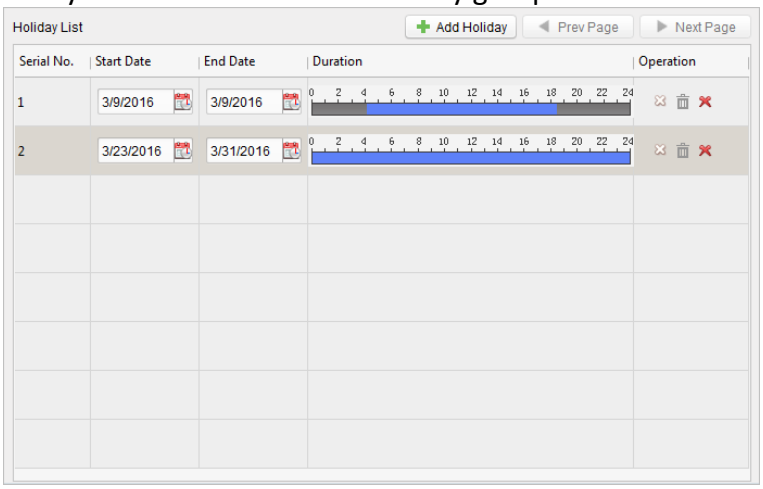


2. Input the name of holiday group in the text filed and click **OK** button to add the holiday group.
3. Select the added holiday group and you can edit the holiday group name and input the remark

information.

4. Click **Add Holiday** icon on the right to add a holiday period to the holiday list and configure the duration of the holiday.

   Note: Up to 16 holidays can be added to one holiday group.



   1) On the period schedule, click and drag to draw the period, which means in that period of time, the configured permission is activated.

      Note: Up to 8 time durations can be set for each period in the schedule.

   2) When the cursor turns to , you can move the selected time bar you just edited. You can also edit the displayed time point to set the accurate time period.

   3) When the cursor turns to , you can lengthen or shorten the selected time bar.

   4) Optionally, you can select the schedule time bar,
      and then click to delete the selected time bar,
      or click to delete all the time bars of the holiday,
      or click to delete the holiday directly.

5. Click **Save** to save the settings.

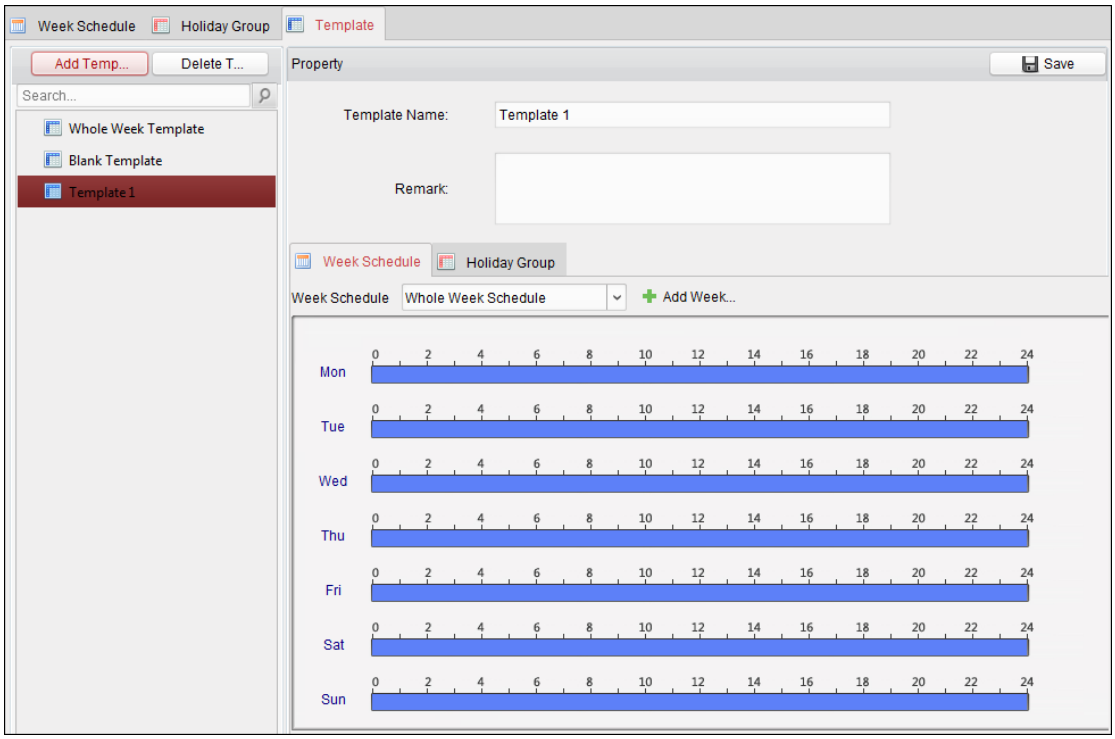
Note: The holidays cannot be overlapped with each other.

4.7.3 Template

After setting the week schedule and holiday group, you can configure the template which contains week schedule and holiday group schedule.

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

Click **Template** tab to enter the Template Management interface.



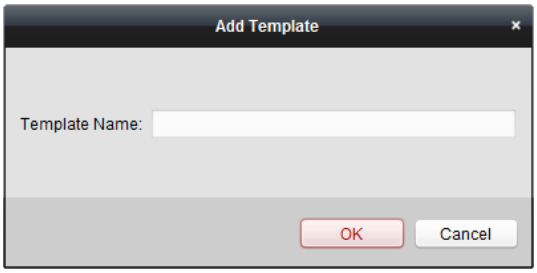
There are two pre-defined templates by default: **Whole Week Template** and **Blank Template**, which cannot be deleted and edited.

- **Whole Week Template:** The card swiping is valid on each day of the week and it has no holiday group schedule.
- **Blank Template:** The card swiping is invalid on each day of the week and it has no holiday group schedule.

You can define custom templates on your demand.

Steps:

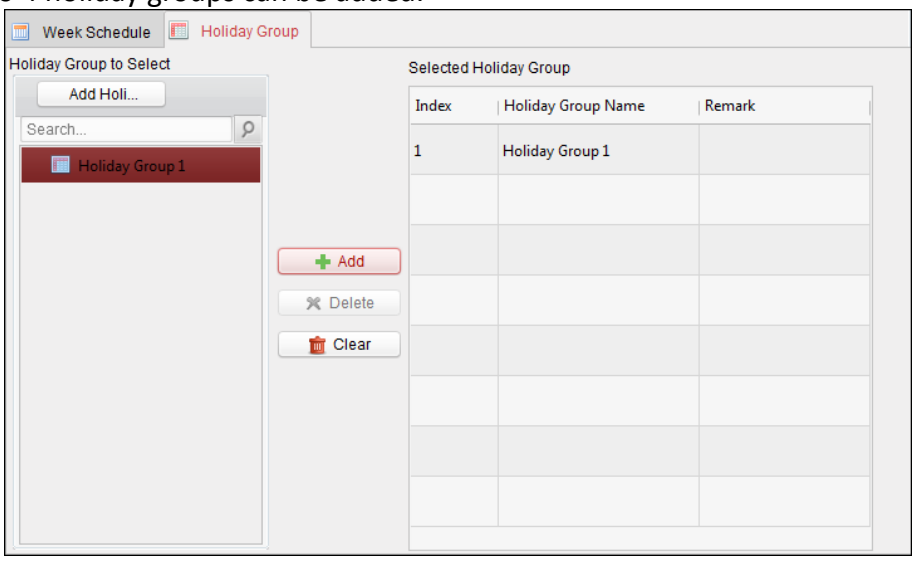
1. Click **Add Template** to pop up the adding template interface.



2. Input the template name in the text filed and click **OK** button to add the template.
3. Select the added template and you can edit its property on the right. You can edit the template name and input the remark information.
4. Select a week schedule to apply to the schedule.
   Click **Week Schedule** tab and select a schedule in the dropdown list.
   You can also click **Add Week Schedule** to add a new week schedule. For details, refer to *Chapter 4.7.1 Week Schedule.*

5. Select holiday groups to apply to the schedule.

   Note: Up to 4 holiday groups can be added.



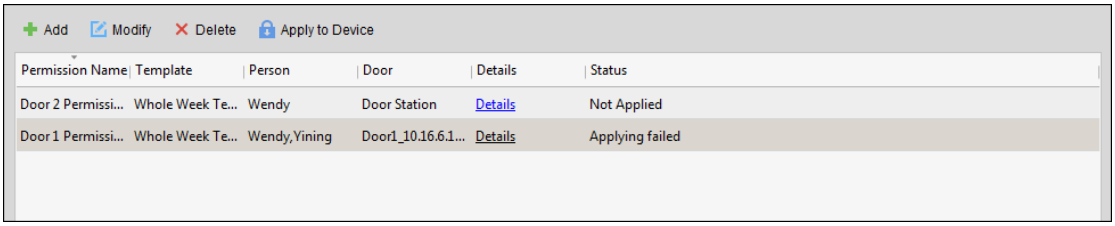
   Click to select a holiday group in the list and click **Add** to add it to the template. You can also click **Add Holiday Group** to add a new one. For details, refer to *Chapter 4.7.2 Holiday Group.*
   You can click to select an added holiday group in the right-side list and click **Delete** to delete it.
   You can click **Clear** to delete all the added holiday groups.

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

4.8 Permission Configuration

In Permission Configuration module, you can add, edit, and delete the access control permission, and then apply the permission settings to the device to take effect.

Click  icon to enter the Access Control Permission interface.



4.8.1 Adding Permission

Purpose:

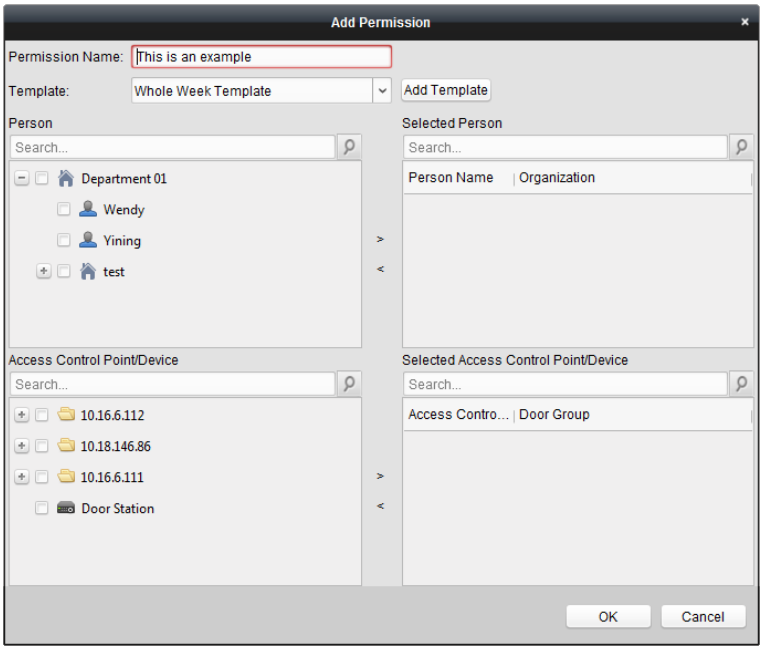
You can assign permission for persons to enter/exist the access control points (doors) in this section.

Notes:

- You can add up to 4 permissions to one access control point of one device.
- You can add up to 128 permissions in total.

Steps:

1. Click **Add** icon to enter following interface.



2. In the Permission Name field, input the name for the permission as desired.
3. Click on the dropdown menu to select a template for the permission.
   Note: You should configure the template before permission settings. You can click **Add Template** button to add the template. Refer to *Chapter 4.7 Schedule and Template* for details.
4. In the Person list, all the added persons display.
   Check the checkbox(es) to select person(s) and click **>** to add to the Selected Person list.
   (Optional) You can select the person in Selected Person list and click **<** to cancel the selection.
5. In the Access Control Point/Device list, all the added access control points (doors) and door stations will display.
   Check the checkbox(es) to select door(s) or door station(s) and click **>** to add to the selected

list.

(Optional) You can select the door or door station in the selected list and click **<** to cancel the selection.

6. Click **OK** button to complete the permission adding. The selected person will have the permission to enter/exit the selected door/door station with their linked card(s) or fingerprints.
7. (Optional) after adding the permission, you can click **Details** to modify it. Or you can select the permission and click **Modify** to modify.
   You can select the added permission in the list and click **Delete** to delete it.

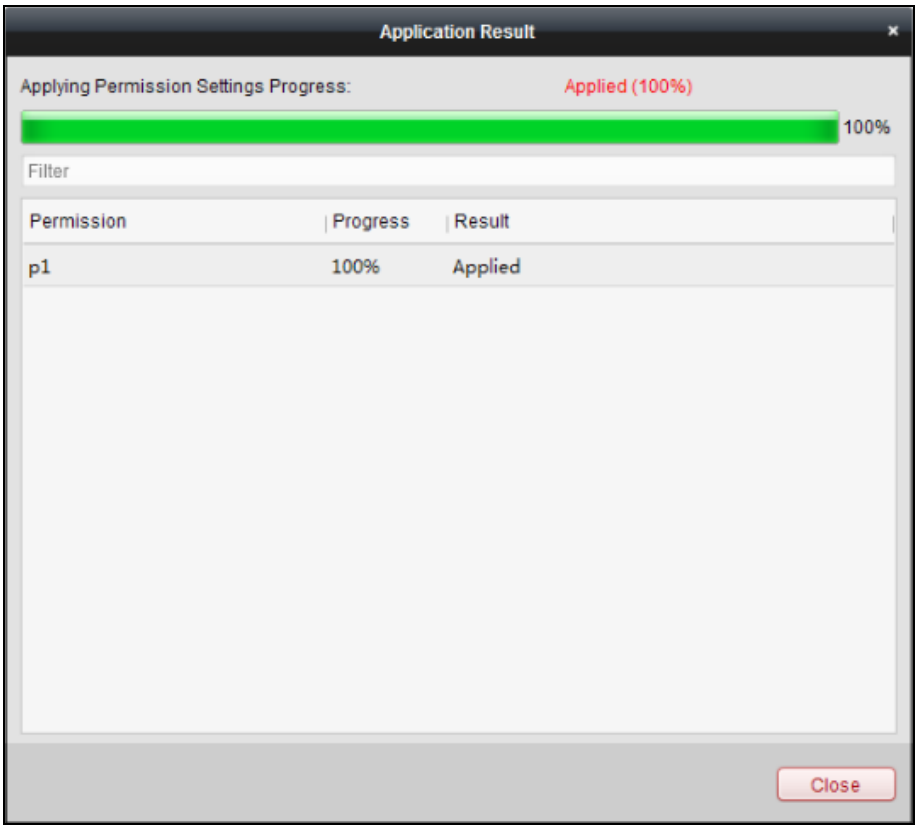
4.8.2 Applying Permission

Purpose:

After configuring the permissions, you should apply the added permission to the access control device to take effect.

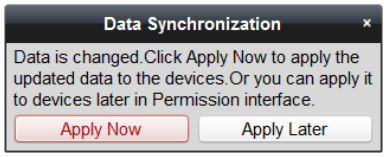
Steps:

1. Select the permission(s) to apply to the access control device. To select multiple permissions, you can hold the *Ctrl* or *Shift* key and select permissions.
2. Click **Apply to Device** to start applying the selected permission(s) to the access control device or door station.
3. The following window will pop up, indicating the applying permission result.



Notes:

- When the permission settings are changed, the following hint box will pop up.



You can click **Apply Now** to apply the changed permissions to the device.
Or you can click **Apply Later** to apply the changes later in the Permission interface.

- The permission changes include changes of schedule and template, permission settings, person's permission settings, and related person settings (including card No., fingerprint, face picture, linkage between card No. and fingerprint, linkage between card No. and fingerprint, card password, card effective period, etc.).

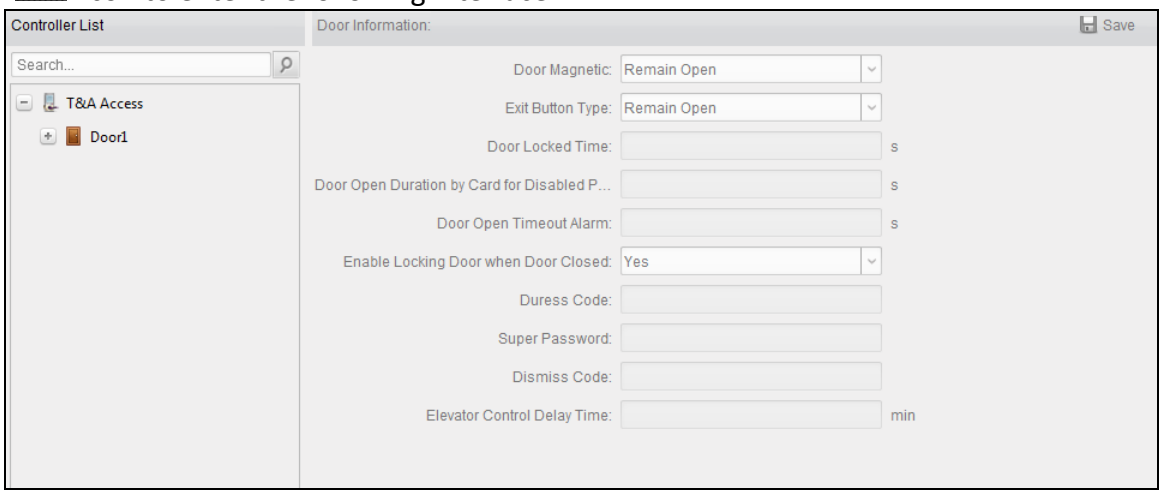
4.9 Advanced Functions

Purpose:

After configuring the person, template, and access control permission, you can configure the advanced functions of access control application, such as access control parameters, authentication password, and opening door with first card, anti-passing back, etc.

Note: The advanced functions should be supported by the device.

Click  icon to enter the following interface.



4.9.1 Access Control Parameters

Purpose:

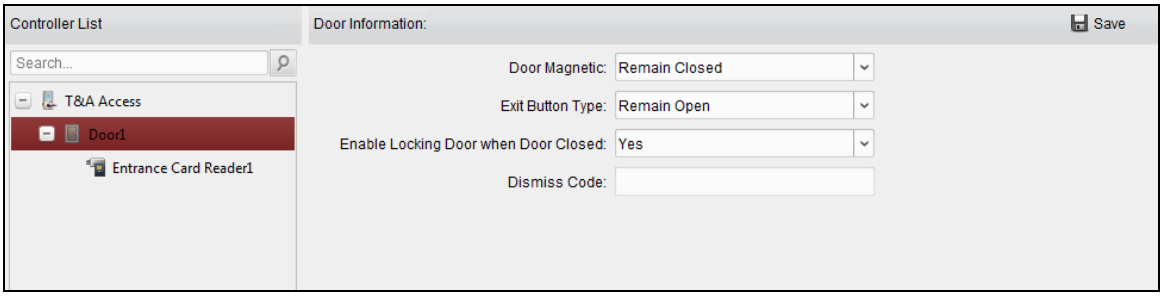
After adding the access control device, you can configure its access control point (door)'s parameters, and its card readers' parameters.

Click **Access Control Parameters** tab to enter the parameters settings interface.

Door Parameters

Steps:

1. In the controller list on the left, click  to expand the access control device, select the door (access control point) and you can edit the information of the selected door on the right.

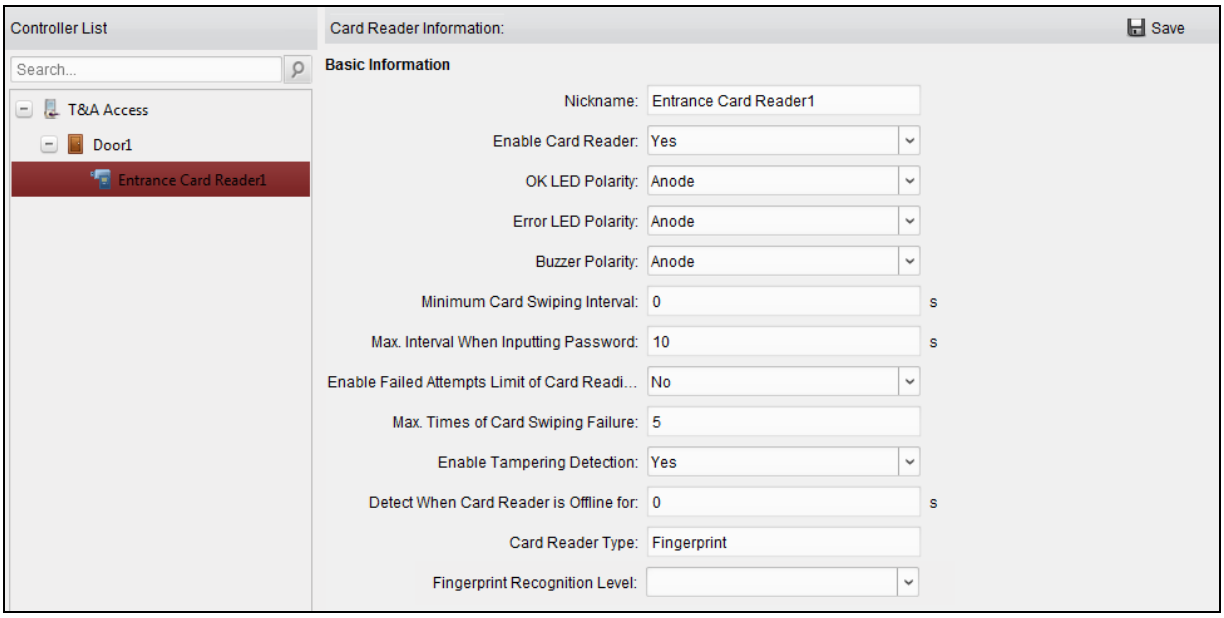


2. You can editing the following parameters:
   Door Magnetic: The Door Magnetic is in the status of **Remain Closed** (excluding special conditions).
   Exit Button Type: The Exit Button Type is in the status of **Remain Open** (excluding special conditions).
   Enable Locking Door when Door Closed: The door can be locked once it is closed even if the Door Locked Time is not reached.
   Dismiss Code: Input the dismiss code to stop the buzzer of the card reader.
3. Click **Save** button to save parameters.

Card Reader Parameters

Steps:

1. In the device list on the left, click ⊞ to expand the door, select the card reader name and you can edit the card reader parameters on the right.



2. You can editing the following parameters:

   - **Nickname:** Edit the card reader name as desired.
   - **Enable Card Reader:** Select **Yes** to enable the card reader.
   - **OK LED Polarity:** Select the OK LED Polarity of the card reader mainboard.
   - **Error LED Polarity:** Select the Error LED Polarity of the card reader mainboard.

- **Buzzer Polarity:** Select the Buzzer LED Polarity of the card reader mainboard.
- **Minimum Card Swiping Interval:** If the interval between card swiping of the same card is less than the set value, the card swiping is invalid. You can set it as 0 to 255.
- **Max. Interval When Inputting Password:** When you inputting the password on the card reader, if the interval between pressing two digits is larger than the set value, the digits you pressed before will be cleared automatically.
- **Enable Failed Attempts Limit of Card Reading:** Enable to report alarm when the card reading attempts reach the set value.
- **Max. Times of Card Swiping Failure:** Set the max. failure attempts of reading card.
- **Enable Tampering Detection:** Enable the anti-tamper detection for the card reader.
- **Detect When Card Reader is Offline for:** When the access control device cannot connect with the card reader for longer than the set time, the card reader will turn offline automatically.
- **Card Reader Type:** Get the card reader's type.
- **Fingerprint Recognition Level:** Select the fingerprint recognition level in the dropdown list. By default, the level is Low.

Note: Only DS-K1A802 series support setting the Fingerprint Recognition Level parameter.

3. Click the **Save** button to save parameters.

4.9.2 Card Reader Authentication

Purpose:

You can set the passing rules for the card reader of the access control device.

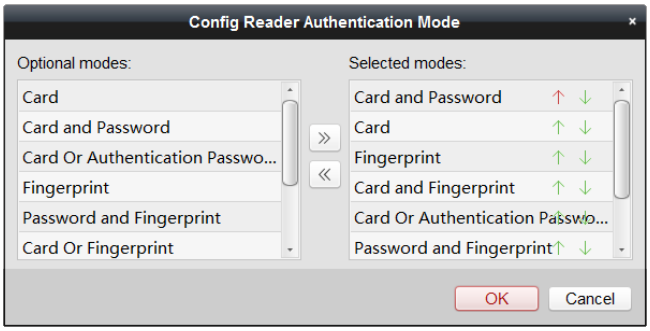
Steps:

1. Click **Card Reader Authentication** tab and select a card reader on the left.
2. Click **Configuration** button to select the card reader authentication modes for setting the schedule.

   Notes:

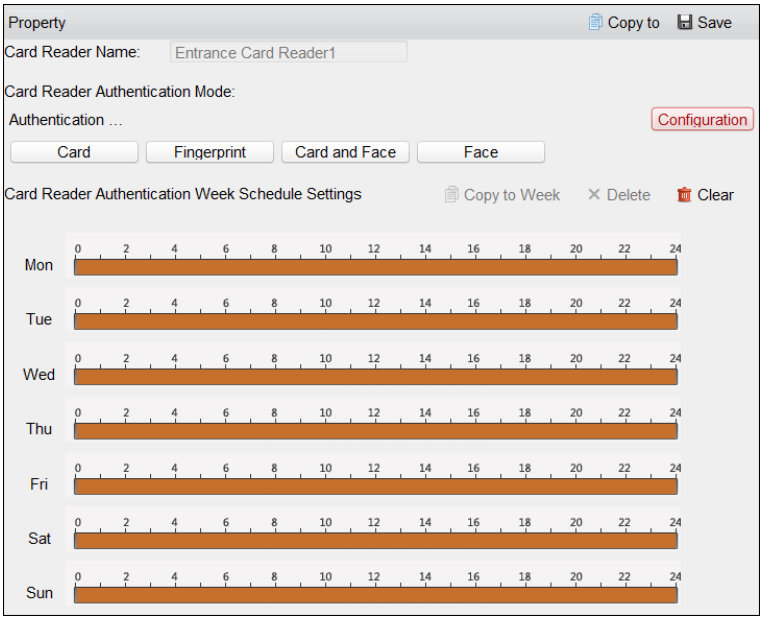
   - The available authentication modes depend on the device type.
   - Password refers to the card password set when issuing the card to the person. *Chapter 4.6 Person Management.*

   1) Select the modes and click » to add to the selected modes list.
      You can click ↑ or ↓ to adjust the display order.

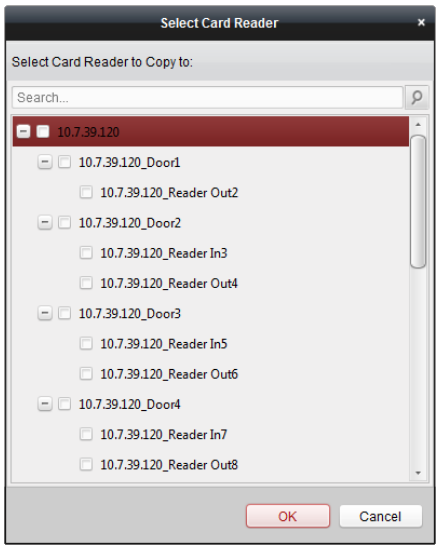


2) Click **OK** to confirm the selection.

3. After selecting the modes, the selected modes will display as icons.
   Click the icon to select a card reader authentication mode.
4. Click and drag your mouse on a day to draw a color bar on the schedule, which means in that period of time, the card reader authentication is valid.



5. Repeat the above step to set other time periods.
   Or you can select a configured day and click **Copy to Week** button to copy the same settings to the whole week.
   (Optional) You can click **Delete** button to delete the selected time period or click **Clear** button to delete all the configured time periods.
6. (Optional) Click **Copy to** button to copy the settings to other card readers.



7. Click **Save** button to save parameters.

4.10 Searching Access Control Event

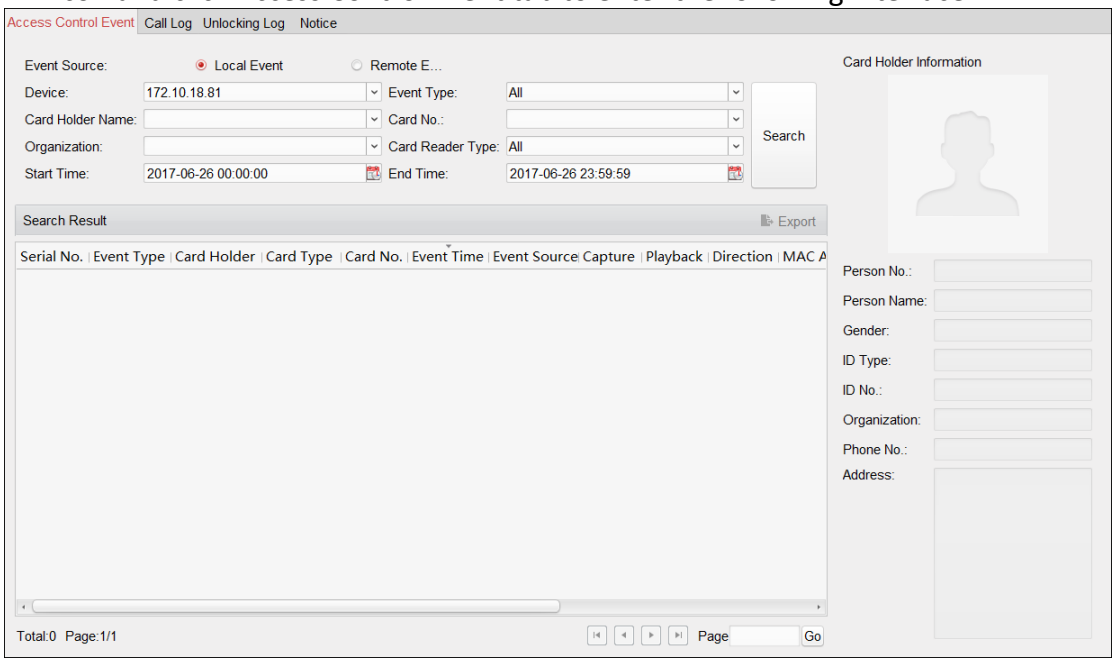
Purpose:

You can search the access control history events including device exception event, door event, alarm input, and card reader event.

Local Event: Search the access control event from the database of the control client.

Remote Event: Search the access control event from the device.

Click  icon and click Access Control Event tab to enter the following interface.



4.10.1 Searching Local Access Control Event

Steps:

1. Select the Event Source as **Local Event**.
2. Input the search condition according to actual needs.
3. Click **Search**. The results will be listed below.
4. For the access control event which is triggered by the card holder, you can click the event to view the card holder details, including person No., person name, organization, phone number, contact address and photo.
5. (Optional) If the event contains linked pictures, you can click in the **Capture** column to view the captured picture of the triggered camera when the alarm is trigged.
6. (Optional) If the event contains linked video, you can click in the **Playback** column to view the recorded video file of the triggered camera when the alarm is trigged.
   Note: For setting the triggered camera, refer to *Chapter 4.11.1* Access Control Event Linkage.
7. You can click **Export** to export the search result to the local PC in *.csv file.

4.10.2 Searching Remote Access Control Event

Steps:

1. Select the Event Source as **Remote Event**.
2. Input the search condition according to actual needs.
3. (Optional) You can check **With Alarm Picture** checkbox to search the events with alarm pictures.
4. Click **Search**. The results will be listed below.
5. You can click **Export** to export the search result to the local PC in *.csv file.

4.11 Access Control Event Configuration

Purpose:

For the added access control device, you can configure its access control linkage including access control event linkage, access control alarm input linkage, event card linkage, and cross-device linkage.

Click the  icon on the control panel,
Or click **Tool**->**Event Management** to open the Event Management page.

4.11.1 Access Control Event Linkage

Purpose:

You can assign linkage actions to the access control event by setting up a rule. For example, when the access control event is detected, an audible warning appears or other linkage actions happen.
Note: The linkage here refers to the linkage of the client software's own actions.

Steps:

1. Click the **Access Control Event** tab.
2. The added access control devices will display in the Access Control Device panel on the left. Select the access control device, or alarm input, or access control point (door), or card reader to configure the event linkage.
3. Select the event type to set the linkage.
4. Select the triggered camera. The image or video from the triggered camera will pop up when the selected event occurs.
   To capture the picture of the triggered camera when the selected event occurs, you can also set the capture schedule and the storage in Storage Schedule.
5. Check the checkboxes to activate the linkage actions. For details, refer to *Table 14.1 Linkage Actions for Access Control Event*.
6. Click **Save** to save the settings.
7. You can click Copy to button to copy the access control event to other access control device, alarm input, access control point, or card reader.
   Select the parameters for copy, select the target to copy to, and click **OK** to confirm.

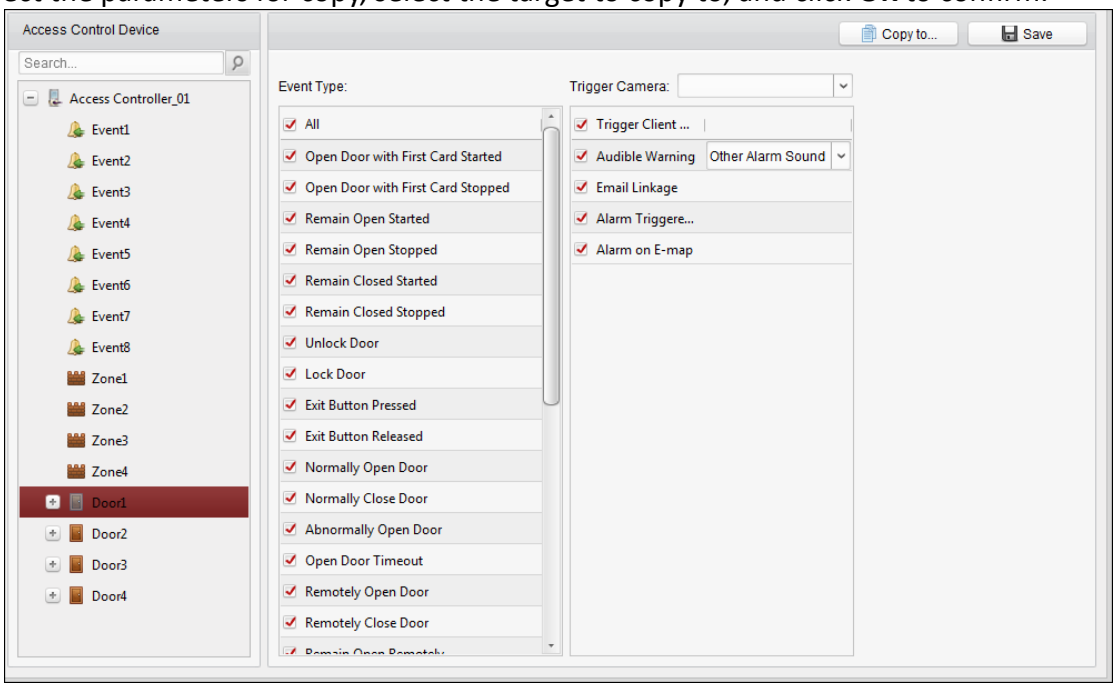


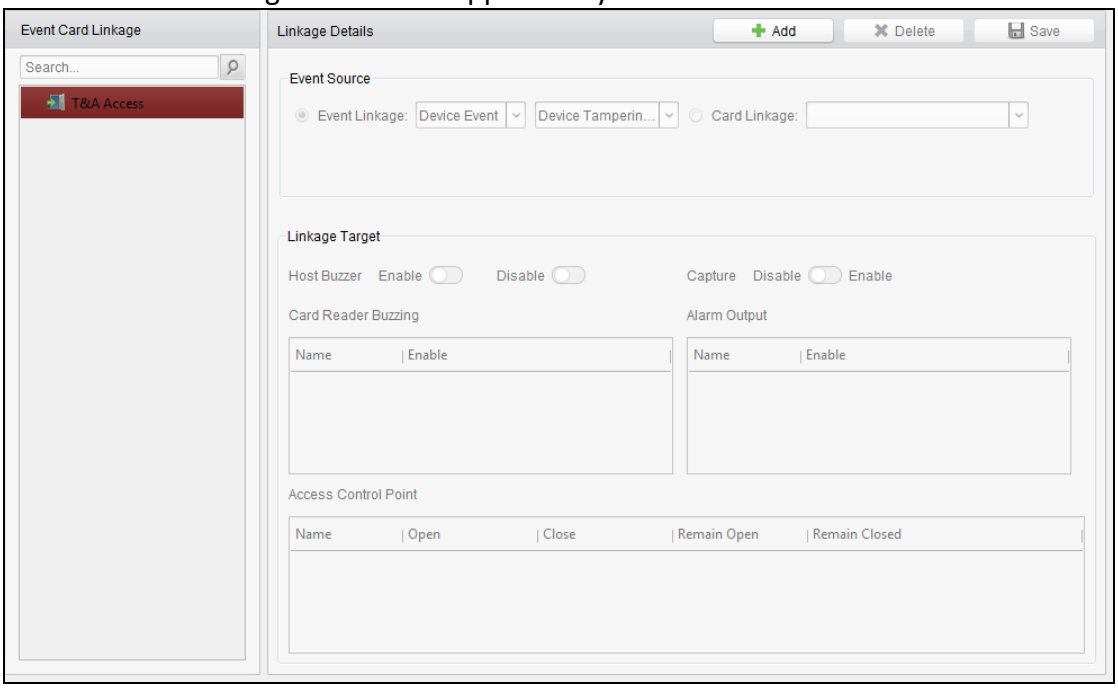
Table 1. 1 Linkage Actions for Access Control Event

Linkage Actions	Descriptions
Audible Warning	The client software gives an audible warning when alarm is triggered. You can select the alarm sound for audible warning.
Email Linkage	Send an email notification of the alarm information to one or more receivers.
Alarm on E-map	Display the alarm information on the E-map. ***Note:*** This linkage is only available to access control point and alarm input.

Alarm Triggered Pop-up Image	The image with alarm information pops up when alarm is triggered. ***Note:*** You should set the triggered camera first.

4.11.2 Event Card Linkage

Click **Event Card Linkage** tab to enter the following interface.
Note: The Event Card Linkage should be supported by the device.



Select the access control device from the list on the left.
Click **Add** button to add a new linkage. You can select the event source as **Event Linkage** or **Card Linkage**.

Event Linkage

For the event linkage, the alarm event can be divided into four types: device event, alarm input, door event, and card reader event.
Steps:

1. Click to select the linkage type as **Event Linkage**, and select the event type from the dropdown list.
   - For Device Event, select the detailed event type from the dropdown list.
   - For Alarm Input, select the type as alarm or alarm recovery and select the alarm input name from the table.
   - For Door Event, select the detailed event type and select the source door from the table.
   - For Card Reader Event, select the detailed event type and select the card reader from the table.
2. Set the linkage target, and switch the property from to  to enable this function.

- **Host Buzzer:** The audible warning of controller will be enabled/disabled.
- **Capture:** The real-time capture will be enabled.
- **Card Reader Buzzer:** The audible warning of card reader will be enabled/disabled.
- **Alarm Output:** The alarm output will be enabled/disabled for notification.
- **Access Control Point:** The door status of open, close, remain open, and remain closed will be enabled.

  Notes:
  - The door status of open, close, remain open, and remain close cannot be triggered at the same time.
  - The target door and the source door cannot be the same one.

3. Click **Save** button to save and take effect of the parameters.

Card Linkage

Steps:

1. Click to select the linkage type as **Card Linkage**.
2. Input the card No. or select the card from the dropdown list.
3. Select the card reader from the table for triggering.
4. Set the linkage target, and switch the property from to  to enable this function.
   - **Host Buzzer:** The audible warning of controller will be enabled/disabled.
   - **Capture:** The real-time capture will be enabled.
   - **Card Reader Buzzer:** The audible warning of card reader will be enabled/disabled.
   - **Alarm Output:** The alarm output will be enabled/disabled for notification.
   - **Access Control Point:** The door status of open, close, remain open, and remain closed will be enabled.
5. Click **Save** button to save and take effect of the parameters.

4.12 Door Status Management

Purpose:

The door status of the added access control device will be displayed in real time. You can check the door status and the linked event(s) of the selected door. You can control the status of the door and set the status duration of the doors as well.

4.12.1 Access Control Group Management

Purpose:

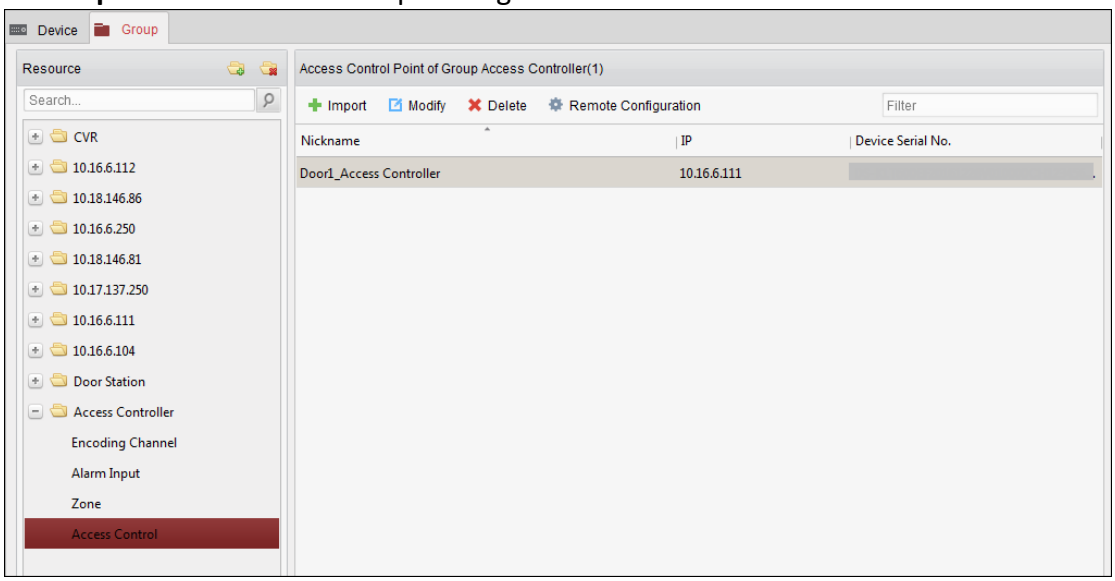
Before controlling the door status and setting the status duration, you are required to organize it into group for convenient management.

Perform the following steps to create the group for the access control device:

Steps:

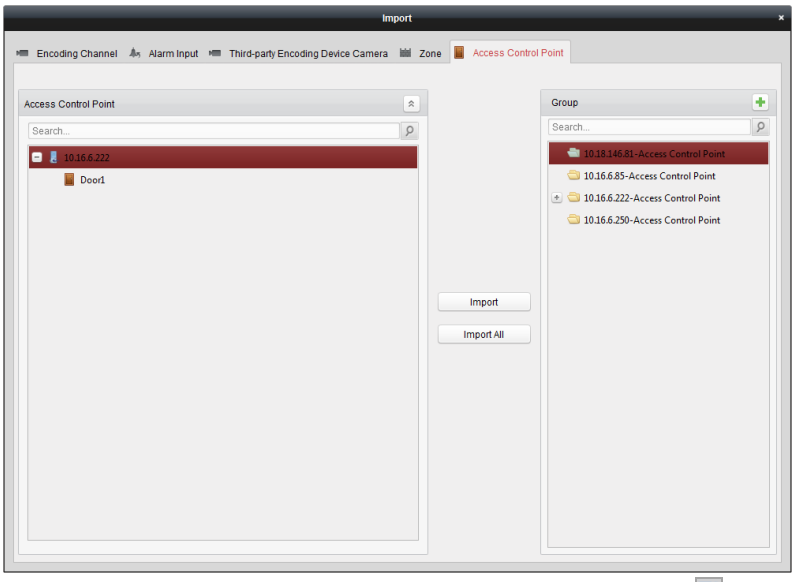
1. Click  on the control panel to open the Device Management page.

2. Click **Group** tab to enter the Group Management interface.



3. Perform the following steps to add the group.
   1) Click  to open the Add Group dialog box.
   2) Input a group name as you want.
   3) Click **OK** to add the new group to the group list.
      You can also check the checkbox **Create Group by Device Name** to create the new group by the name of the selected device.

4. Perform the following steps to import the access control points to the group:
   1) Click **Import** on Group Management interface, and then click the **Access Control** tab to open the Import Access Control page.
      Notes:
      - You can also select **Alarm Input** tab and import the alarm inputs to group.
      - For the Video Access Control Terminal, you can add the cameras as encoding channel to the group.
   2) Select the names of the access control points in the list.
   3) Select a group from the group list.
   4) Click **Import** to import the selected access control points to the group.
      You can also click **Import All** to import all the access control points to a selected group.



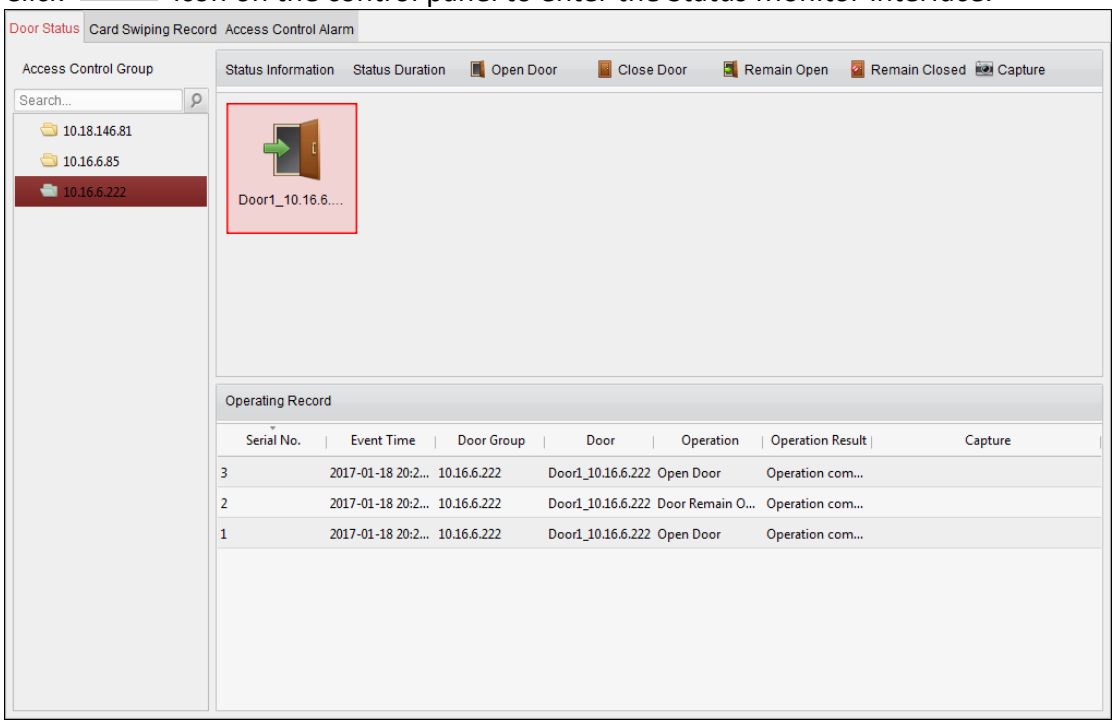
5. After importing the access control points to the group, you can click , or double-click the group/access control point name to modify it.

4.12.2 Controlling Door Status

Purpose:

You can control the status for a single access control point (a door), including opening door, closing door, remaining open, and remaining closed.

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



Steps:

1. Select an access control group on the left. For managing the access control group, refer to *Chapter 4.12.1 Access Control Group Management.*
2. The access control points of the selected access control group will be displayed on the right.

   Click icon  on the Status Information panel to select a door.
3. Click the following button listed on the **Status Information** panel to control the door.
   - **Open Door**: Click to open the door once.
   - **Close Door**: Click to close the door once.
   - **Remain Open**: Click to keep the door open.
   - **Remain Closed**: Click to keep the door closed.
   - **Capture**: Click to capture the picture manually.
4. You can view the anti-control operation result in the Operation Log panel.

Notes:

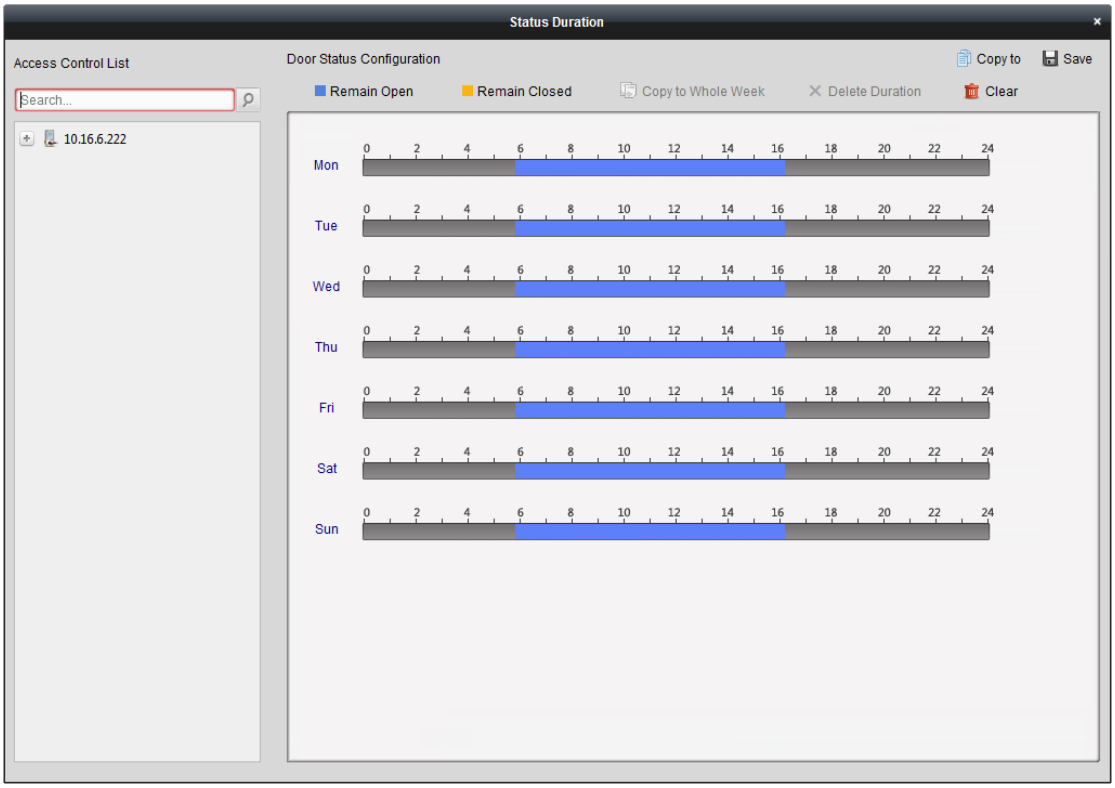
- If you select the status as **Remain Open/Remain Closed**, the door will keep open/closed until a new anti-control command being made.
- The **Capture** button is available when the device supports capture function. And it cannot be realized until the storage server is configured.
- If the door is in remain closed status, only super card can open the door or open door via the client software.

4.12.3 Configuring Status Duration

Purpose:

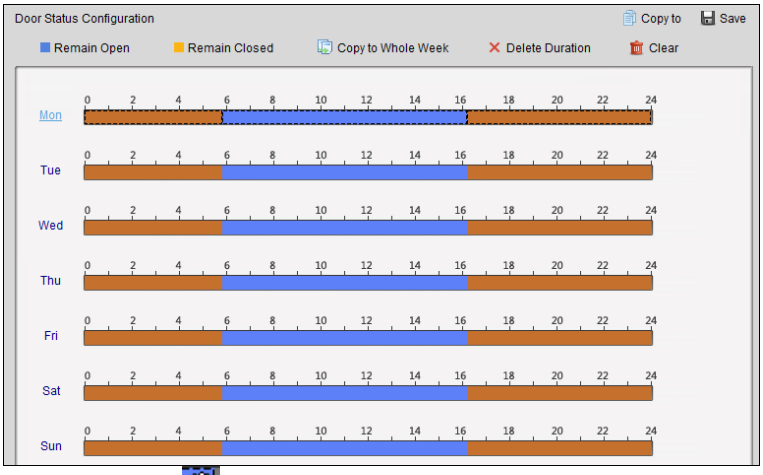
You can schedule weekly time periods for an access control point (door) to remain open or remain closed.

In the Door Status module, click **Status Duration** button to enter the Status Duration interface.



Steps:

1. Click to select a door from the access control device list on the left.
2. On the Door Status Configuration panel on the right, draw a schedule for the selected door.
   1) Select a door status brush as **Remain Open** or **Remain Closed**.
      Remain Open: The door will keep open during the configured time period. The brush is marked as .
      Remain Closed: The door will keep closed during the configured duration. The brush is marked as .
   2) Click and drag on the timeline to draw a color bar on the schedule to set the duration.



   3) When the cursor turns to , you can move the selected time bar you just edited. You can also edit the displayed time point to set the accurate time period.
      When the cursor turns to , you can lengthen or shorten the selected time bar.
   4) Optionally, you can select the schedule time bar and click **Copy to Whole Week** to copy the

time bar settings to the other days in the week.

5) You can select the time bar and click **Delete Duration** to delete the time period.

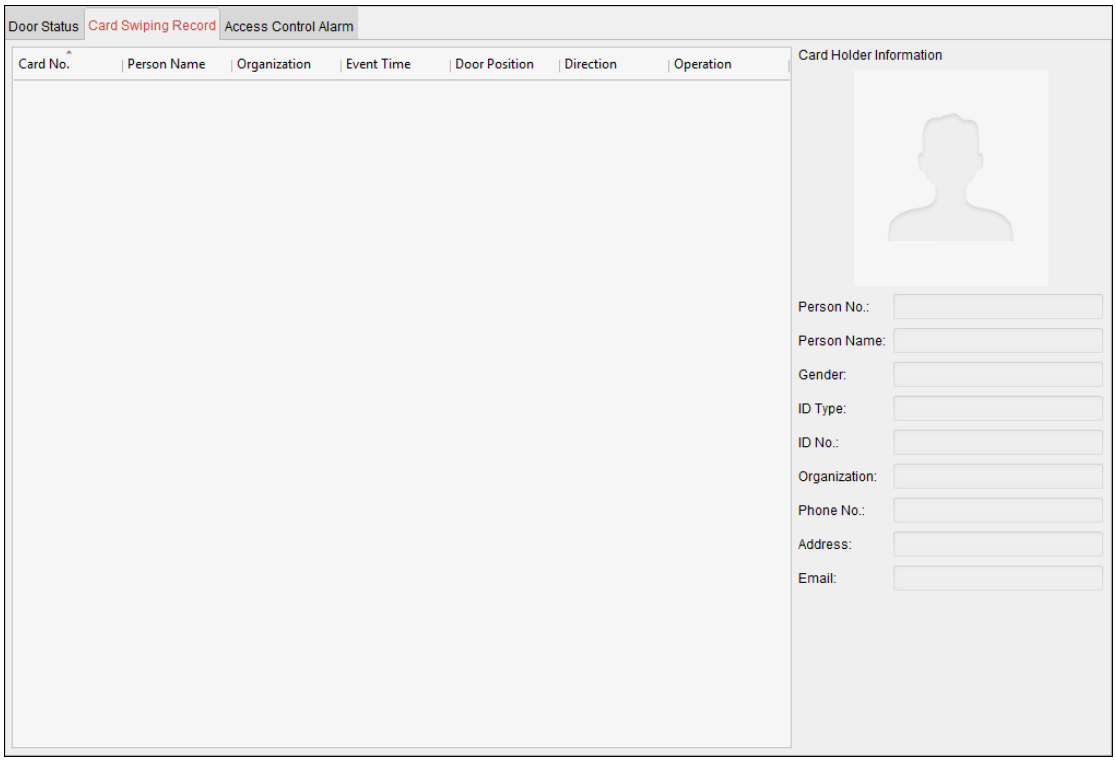
Or you can click **Clear** to clear all configured durations on the schedule.

6) Click **Save** to save the settings.

7) You can click **Copy to** button to copy the schedule to other doors.

4.12.4 Real-time Card Swiping Record

Click **Card Swiping Record** tab to enter the following interface.



The logs of card swiping records of all access control devices will display in real time. You can view the details of the card swiping event, including card No., person name, organization, event time, etc.

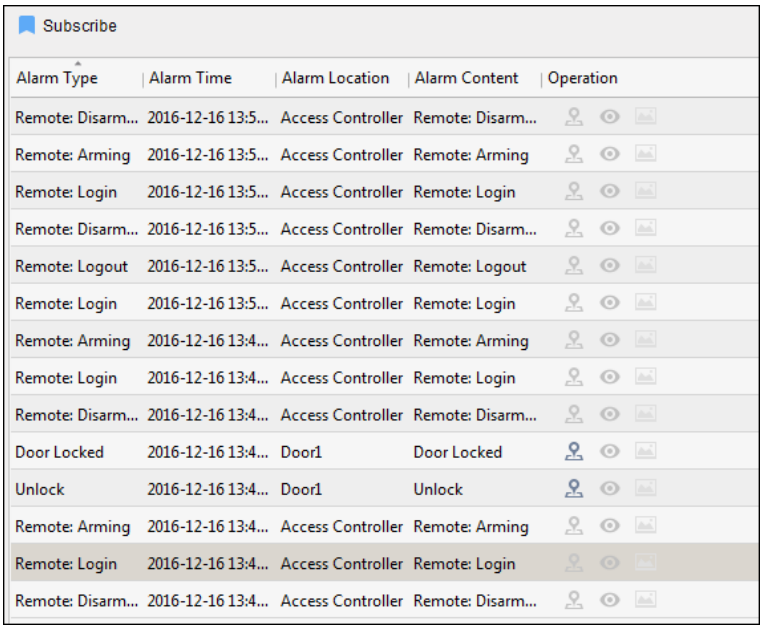
You can also click the event to view the card holder details, including person No., person name, organization, phone, contact address, etc.

4.12.5 Real-time Access Control Alarm

Purpose:

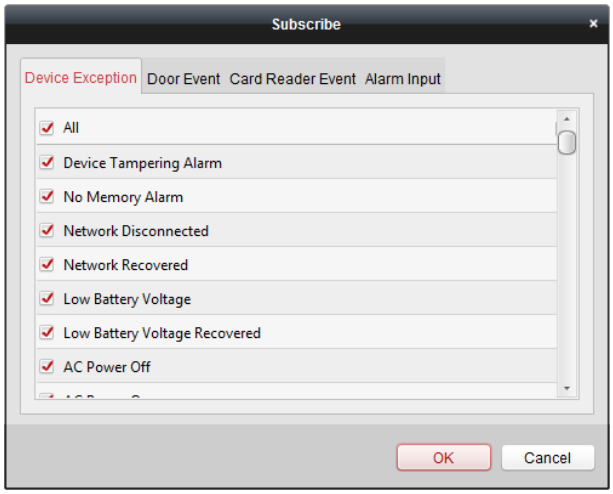
The logs of access control events will be displayed in real time, including device exception, door event, card reader event, and alarm input.

Click **Access Control Alarm** tab to enter the following interface.



Steps:

1. All access control alarms will display in the list in real time.
   You can view the alarm type, alarm time, location, etc.
2. Click to view the alarm on E-map.
3. You can click or to view the live view or the captured picture of the triggered camera when the alarm is trigged.
   Note: For setting the triggered camera, refer to *Chapter 4.11.1 Access Control Event Linkage.*
4. Click **Subscribe** to select the alarm that the client can receive when the alarm is triggered.



   1) Check the checkbox(es) to select the alarm(s), including device exception alarm, door event alarm, card reader alarm, and alarm input.
   2) Click **OK** to save the settings.

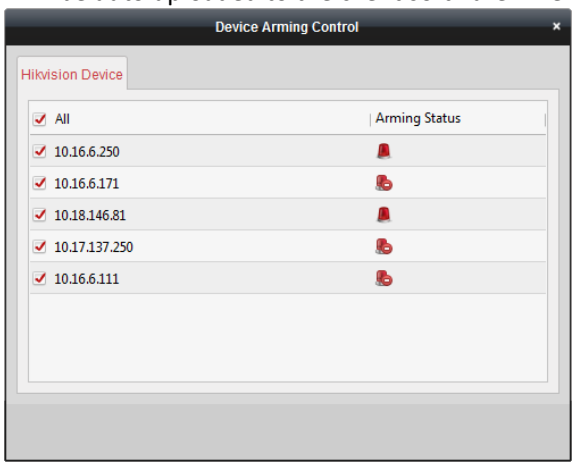
4.13 Arming Control

Purpose:

You can arm or disarm the device. After arming the device , the client can receive the alarm information from the device.

Steps:

1. Click **Tool->Device Arming Control** to pop up the Device Arming Control window.
2. Arm the device by checking the corresponding checkbox.
   Then the alarm information will be auto uploaded to the client software when alarm occurs.



4.14 Time and Attendance

Purpose:

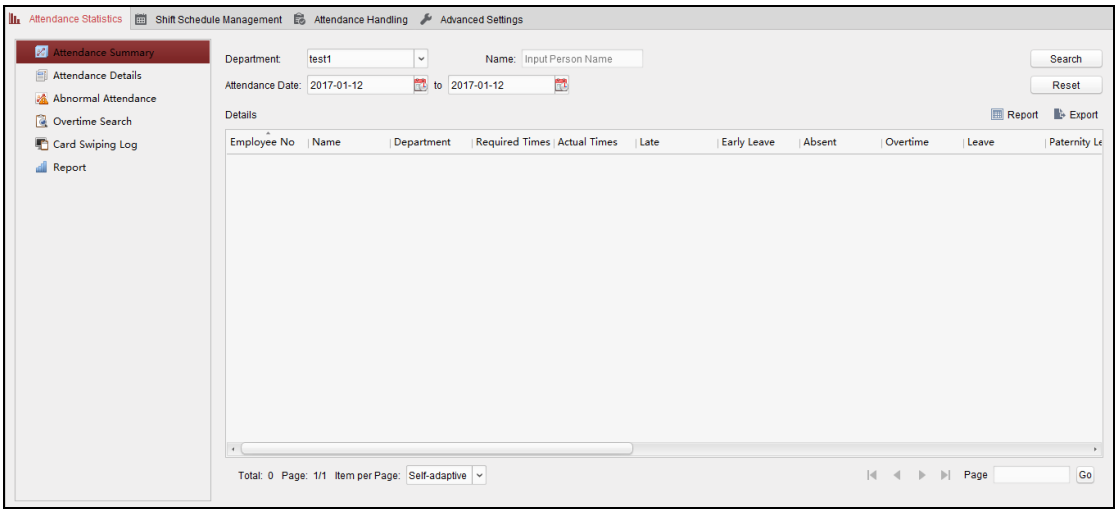
The Time and Attendance module provides multiple functionalities, including shift schedule management, attendance handling, attendance statistics and other advanced functions.

Before you start:

You should add organization and person in Access Control module. For details, refer to 4.5 Organization Management.

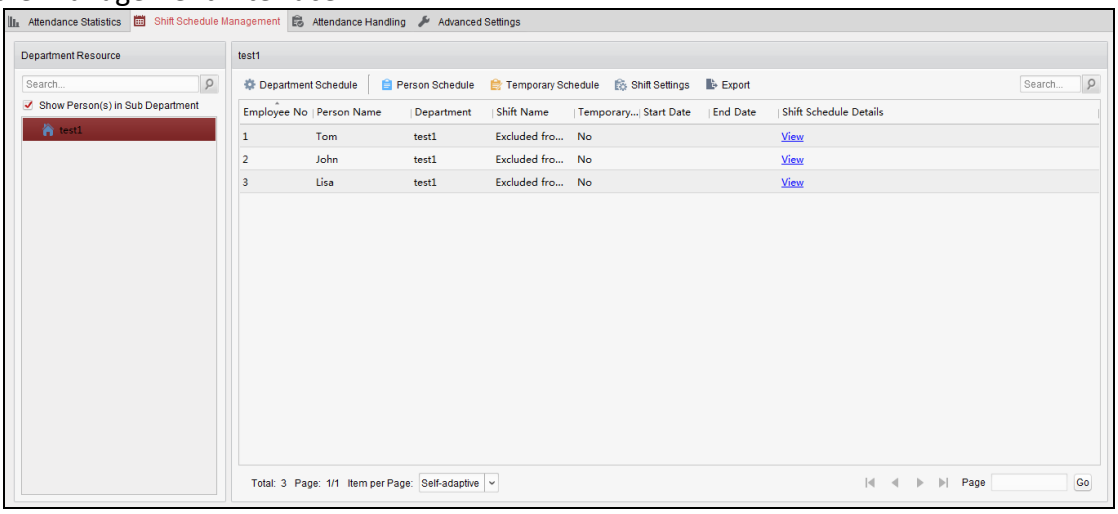
Perform the following steps to access the Time and Attendance module.

Click  to enter the Time and Attendance module as follows:



4.14.1 Shift Schedule Management

Open Time and Attendance module and click **Shift Schedule Management** to enter the Shift Schedule Management interface.



Shift Settings

Purpose:

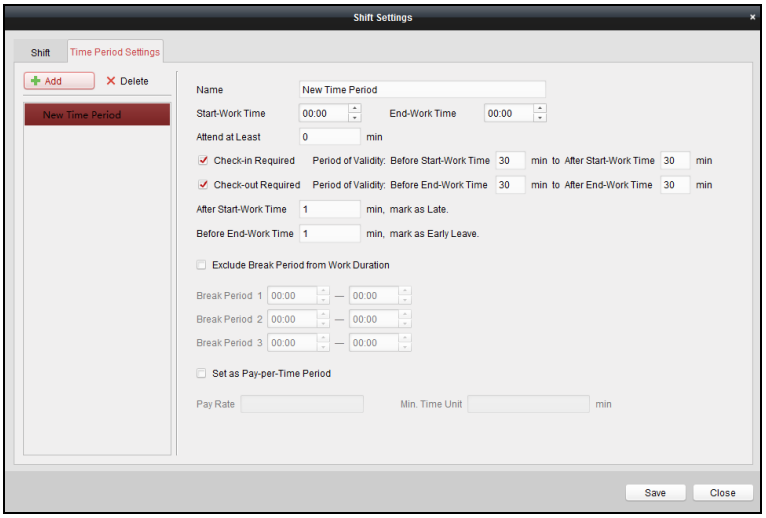
You can add time period and shift for the shift schedule.

Click **Shift Settings** to pop up Shift Settings dialog.

➢ **Adding Time Period**

Steps:

1. Click **Time Period** tab.
2. Click **Add**.



3. Set the related parameters.

   Name: Set the name for time period.

   Start-Work / End-Work Time: Set the start-work time and end-work time.

   Attend at Least: Set the minimum attendance time.

Check-in / Check-out Required: Check the checkboxes and set the valid period for check-in or check-out.

Mark as Late/Mark as Early Leave: Set the time period for late or early leave.

Exclude Break Period from Work Duration: Check the checkbox and set the break period excluded.

Note: Up to 3 break periods can be set.

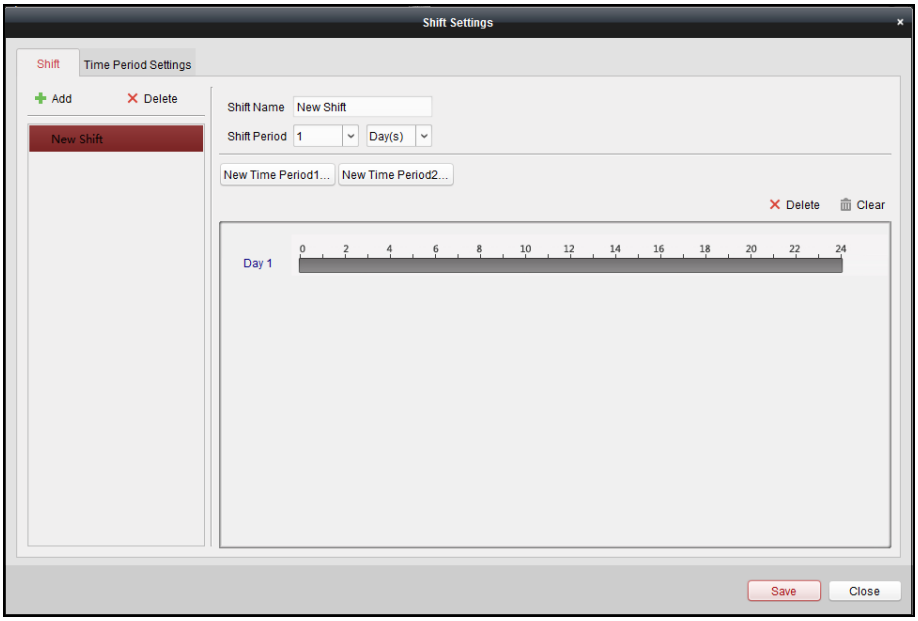
Set as Pay-per-Time Period: Check the checkbox and set the pay rate and minimum time unit.

4. Click **Save** to save the settings.
   The added time period will display on the left panel of the dialog.
   You can also click **Delete** to delete the time period.

➢ **Adding Shift**

Steps:

1. Click **Shift** Tab.
2. Click **Add**.



3. Set the name for shift.
4. Select the shift period from the drop-down list.
5. Configure the shift period with the added time period.
   1) Select the time period.
   2) Click the time bar to apply the time period for the select day.
   You can click the time period on the bar and click or **Delete** to delete the period.
   You can also click **Clear** to delete all days' time period.
6. Click **Save** to save the settings.
   The added shift will display on the left panel of the dialog.
   You can also click **Delete** on the left panel to delete the shift.

Shift Schedule Settings

Purpose:

After setting the shift, you can set department schedule, person schedule and temporary schedule.

Note: The temporary schedule has higher priority than department schedule and person schedule.

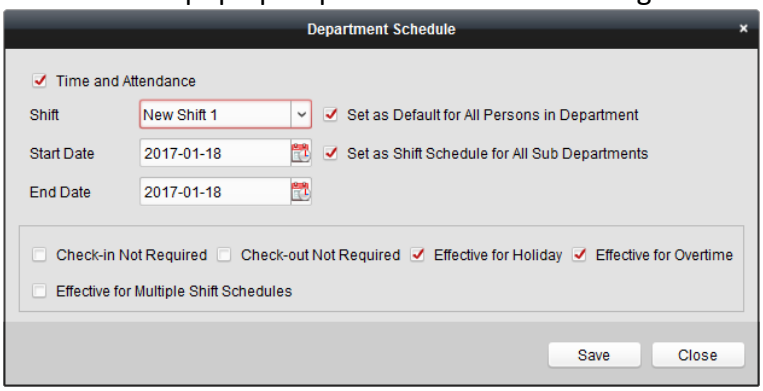
➢ **Department Schedule**

You can set the shift schedule for one department, and all the persons in the department will be assigned with the shift schedule.

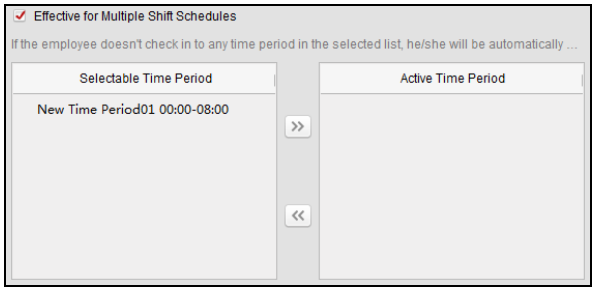
Note: In Time and Attendance module, the department list is the same with the **organization** in Access Control. For setting the organization in Access Control, refer to *Chapter 4.5 Organization Management*.

Steps:

1. Open the Shift Schedule Management interface and select the department on the left panel.
2. Click **Department Schedule** to pop up Department Schedule dialog.



3. Check **Time and Attendance** checkbox.
   All persons in the department expect those excluded from attendance will apply the attendance schedule.
4. Select the shift from the drop-down list.
5. Set the start date and end date.
6. (Optional) Set other parameters for the schedule.
   You can select Check-in Not Required, Check-out Not Required, Effective for Holiday, Effective for Overtime, Effective for Multiple Shift Schedules.
   Notes:
   - Multiple Shift Schedules contains more than one time periods. The person can check in/out in any of the time periods and the attendance will be effective.
     Example: If the multiple shift schedules contains three time periods: 00:00 to 07:00, 08:00 to 15:00 and 16:00 to 23:00. The attendance of the person adopting this multiple shift schedules will be effective in any of the three time periods. If the person checks in at 07:50, it will apply the nearest time period 08:00 to 15:00 to the person's attendance.
   - After checking the **Effective for Multiple Shift Schedules** checkbox, you can select the effective time period(s) from the added time periods for the persons in the department.



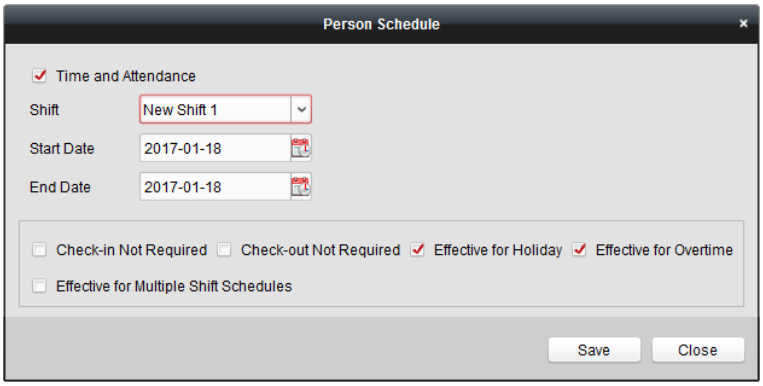
1) In the Selectable Time Period list on the left, click the added time period and click » to add it to the right.
2) (Optional) To remove the selected time period, select it and click «.

7. (Optional) Check **Set as Default for All Persons in Department** checkbox.
   All persons in the department will use this shift schedule by default.
8. (Optional) If the selected department contains sub department(s), the Set as **Shift Schedule for All Sub Departments** checkbox will display. You can check it to apply the department schedule to its sub departments.
9. Click **Save** to save the settings.

➢ **Person Schedule**

Steps:

1. Open the Shift Schedule Management interface and select the department on the left panel.
2. Select the person(s) on the right panel.
3. Click **Person Schedule** to pop up Person Schedule dialog.

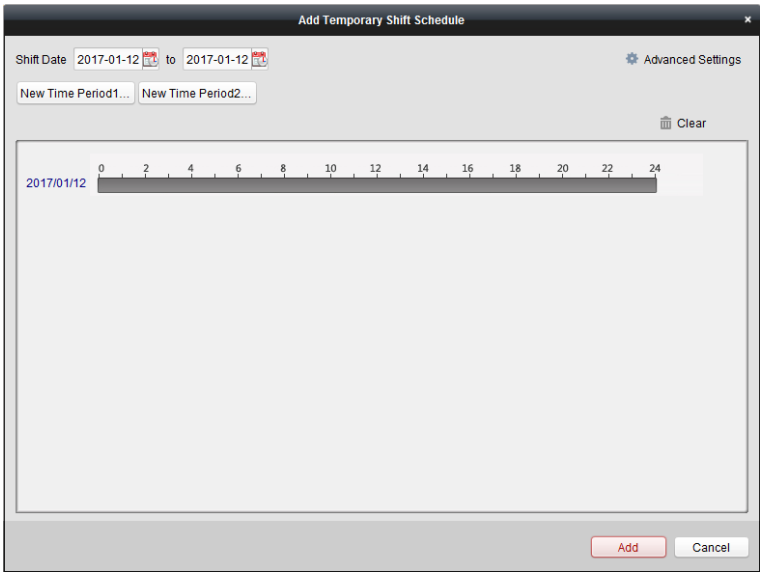


4. Check **Time and Attendance** checkbox.
   The configured person will apply the attendance schedule.
5. Select the shift from the drop-down list.
6. Set the start date and end date.
7. (Optional) Set other parameters for the schedule.
   You can select Check-in Not Required, Check-out Not Required, Effective for Holiday, Effective for Overtime, Effective for Multiple Shift Schedules.
8. Click **Save** to save the settings.

➢ **Temporary Schedule**

Steps:

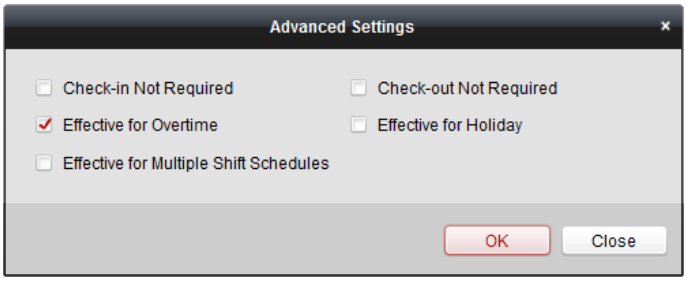
1. Open the Shift Schedule Management interface and select the department on the left panel.
2. Select the person(s) on the right panel.
3. Click **Temporary Schedule** to pop up Temporary Schedule dialog.



4. Click to set the shift date.
5. Configure the shift date with the added time period.
   1) Select the time period.
   2) Click the time bar to apply the time period for the select date.

   You can click the time period on the bar and click to delete the period.

   You can also click **Clear** to delete all days' time period.
6. You can click **Advanced Settings** to advanced attendance rules for the temporary schedule.



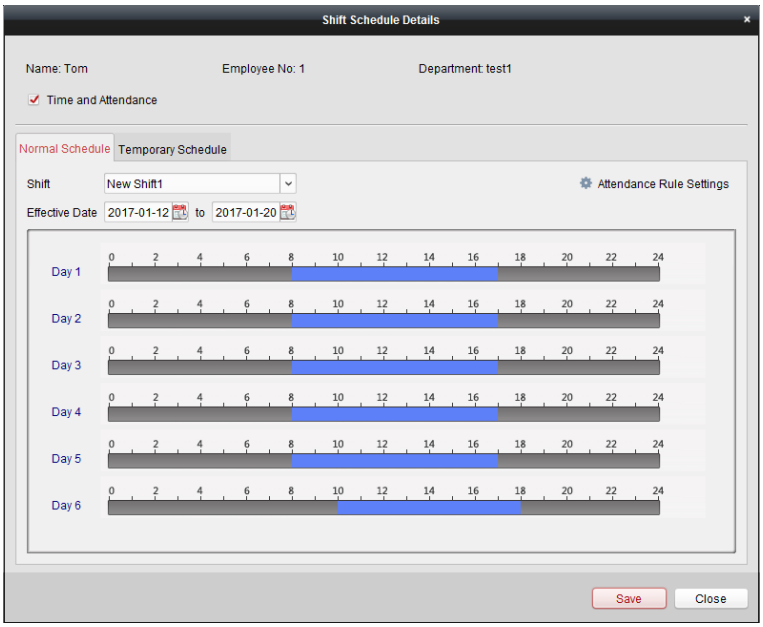
7. Click **Add** to save the settings.

➢ **Checking Shift Schedule Details**

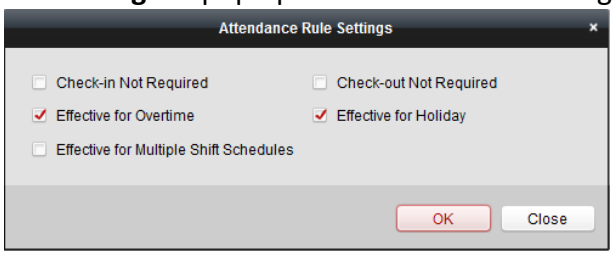
Steps:

1. On the Shift Schedule Management interface, select the department on the left panel.
2. Select the person(s) on the right panel.
3. Click **View** to pop up Shift Schedule Details dialog.

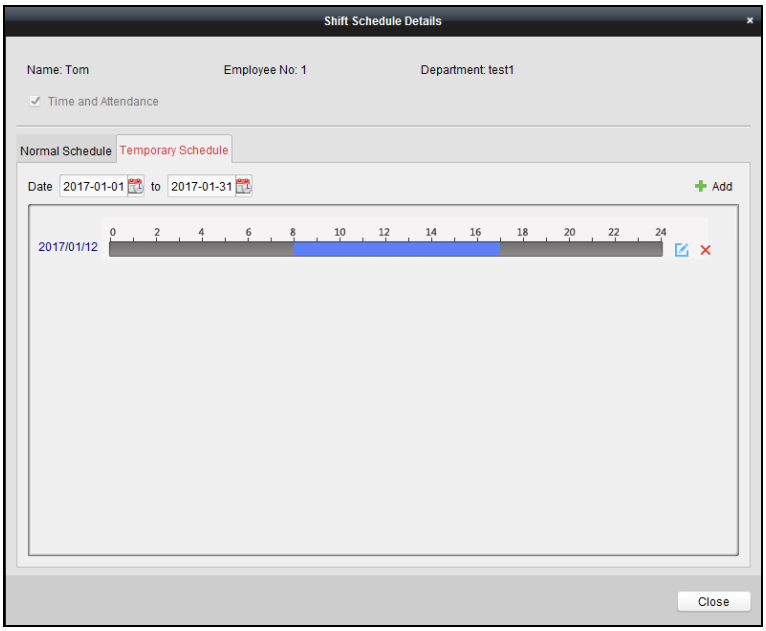
   You can check the shift schedule details.



4. Click **Normal Schedule** tab.
   You can check and edit the normal schedule details.
   1) Select the shift from the drop-down list.
   2) Click **Attendance Rule Settings** to pop up Attendance Rule Settings dialog.



   You can check the attendance rules as desired and click **OK** to save the settings.
   3) Click  to set the effective date.
   4) Click **Save** to save the settings.
5. (Optional) Click **Temporary Schedule** tab.



You can check and edit the temporary schedule details.

(Optional) Click **Add** to add temporary schedule for the selected person.

(Optional) Click to edit the time period.

(Optional) Click to delete the temporary schedule.

➢ **Exporting Shift Schedule Details**

On the Shift Schedule Management interface, select the department on the left panel and click **Export** to export all persons' shift schedule details to local PC.

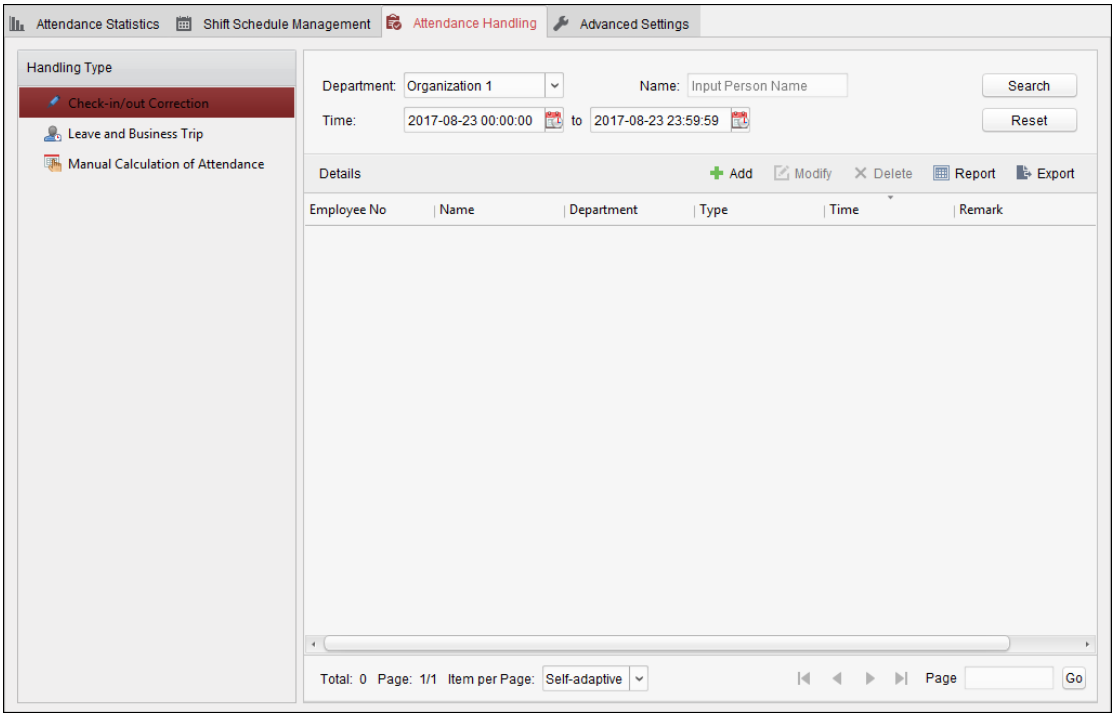
Note: The exported details are saved in *.csv format.

4.14.2 Attendance Handling

Purpose:

You can handle the attendance, including check-in correction, check-out correction, leave and business trip, and manual calculation of attendance data.

Open Time and Attendance module and click **Attendance Handling** to enter the Attendance Handling interface.



Check-in/out Correction

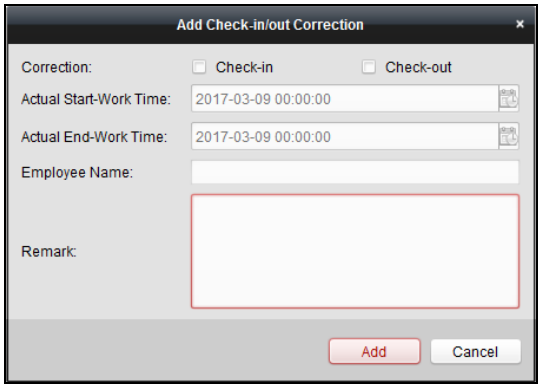
Purpose:

You can add, edit, delete, search the check-in/out correction and generate the related report. You can also export the check-in/out correction details to local PC.

➢ **Add Check-in/out Correction**

Steps:

1. Click **Check-in/out Correction** tab.
2. Click **Add** to pop up Add Check-in/out Correction dialog.



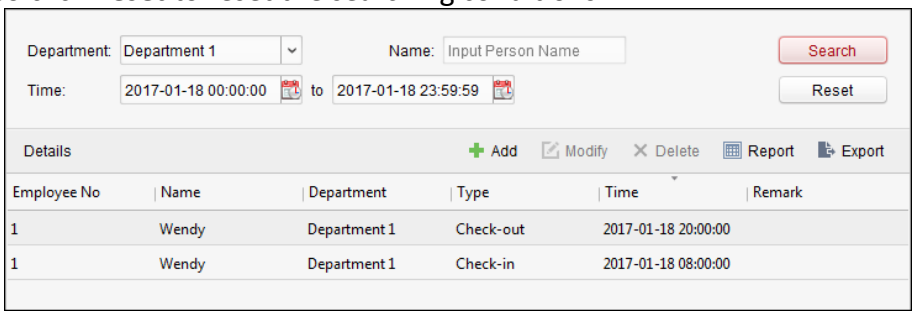
3. Set the check-in/out correction parameters.
   For Check-in Correction: Check **Check-in** checkbox and set the actual start-work time.
   For Check-out Correction: Check **Check-out** checkbox and set the actual end-work time.
4. Click **Employee Name** field and select the person.
   You can also input the keyword and click to search the person you want.
5. (Optional) Input the remark information as desired.
6. Click **Add** to add the check-in/out correction.

The added check-in/out correction will display on the Attendance Handling interface.
(Optional) Select the check-in/out correction and click **Modify** to edit the correction.
(Optional) Select the check-in/out correction and click **Delete** to delete the correction.
(Optional) Click **Report** to generate the check-in/out correction report.
(Optional) Click **Export** to export the check-in/out correction details to local PC.
Note: The exported details are saved in *.csv format.

➢ **Search Check-in/out Correction**

Steps:

1. Click **Check-in/out Correction** tab.
2. Set the searching conditions.
   Department: Select the department from the drop-down list.
   Name: Input the person name.
   Time: Click to set the specified time as time range.
3. Click **Search** to search the check-in/out corrections.
   The check-in/out correction details will display on the list.
   You can also click **Reset** to reset the searching conditions.



Leave and Business Trip

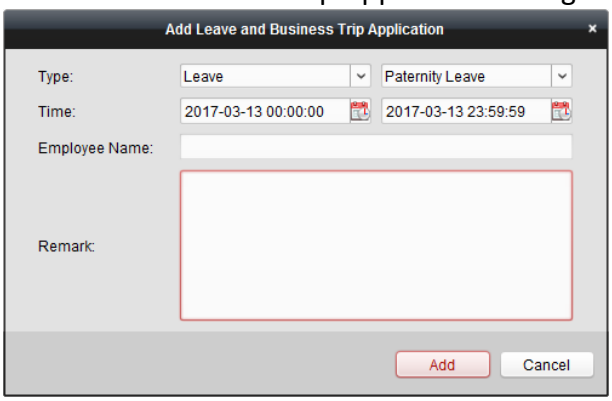
Purpose:

You can add, edit, delete, search the leave and business trip and generate the related report. You can also export the leave and business trip details to local PC.

➢ **Add Leave and Business Trip**

Steps:

1. Click **Leave and Business Trip** tab.
2. Click **Add** to pop up Add Leave and Business Trip Application dialog.



3. Select the leave and business trip type from the Type drop-down list.
   You can configure the leave type in Advanced Settings. For details, refer to *Chapter 0 Leave Type Settings*.
4. Click to set the specified time as time range.
5. Click **Employee Name** field and select the person for this application.
   You can also input the keyword and click to search the person you want.
6. (Optional) Input the remark information as desired.
7. Click **Add** to add the leave and business trip.
   The added leave and business trip will display on the Attendance Handling interface.
   (Optional) Select the leave and business trip and click **Modify** to edit the leave or business trip.
   (Optional) Select the leave and business trip and click **Delete** to delete the leave or business trip.
   (Optional) Click **Report** to generate the leave or business trip report.
   (Optional) Click **Export** to export the leave or business trip details to local PC.
   Note: The exported details are saved in *.csv format.

➢ **Search Leave and Business Trip**

Steps:

1. Click **Leave and Business Trip** tab.
2. Set the searching conditions.
   Department: Select the department from the drop-down list.
   Name: Input the person name.
   Time: Click to set the specified time as time range.
3. Click **Search** to search the leave and business trips.
   The leave and business trip details will display on the list.
   You can also click **Reset** to reset the searching conditions.

Manual Calculation of Attendance

Purpose:

You can calculate the attendance result manually if needed by specifying the start time and end time.

Steps:

1. Click **Manual Calculation of Attendance** tab.
2. Set the start time and end time for calculation.
3. Click **Calculate** to start.

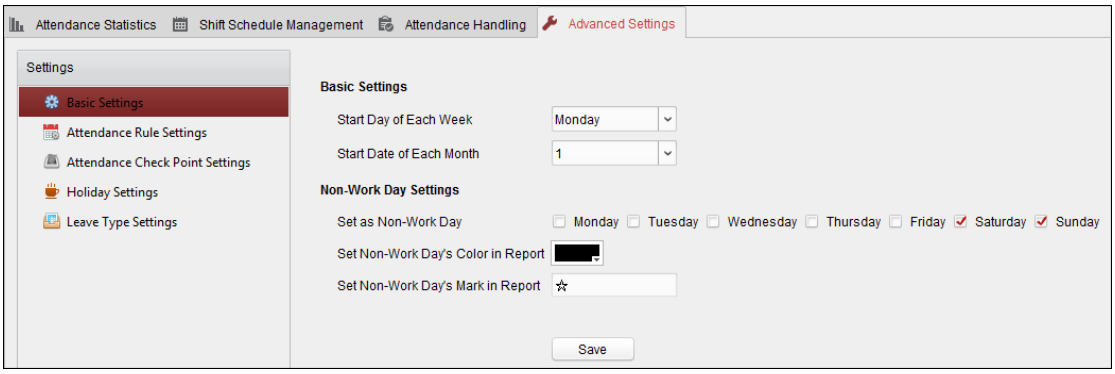
Note: It can only calculate the attendance data within three months.

4.14.3 Advanced Settings

Purpose:

You can configure the basic settings, attendance rule, attendance check point, holiday settings and leave type for attendance.

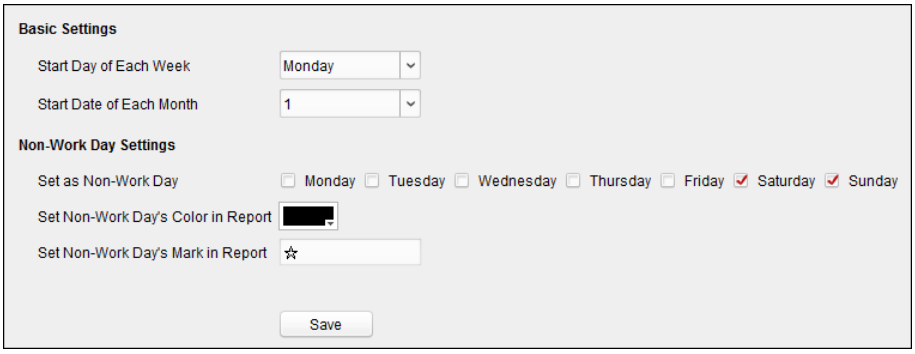
Open Time and Attendance module and click **Advanced Settings** to enter the Advanced Settings interface.



Basic Settings

Steps:

1. Click **Basic Settings** tab to enter the Basic Settings interface.



2. Set the basic settings.

   Start Day of Each Week: You can select one day as the start day of each week.

   Start Date of Each Month: You can select one day as the start date of each month.

3. Set the non-work day settings.

   Set as Non-Work Day: Check the checkbox(es) to set the selected day(s) as non-work day.

   Set Non-Work Day's Color in Report: Click the color filed and select the color to mark the non-work day in report.

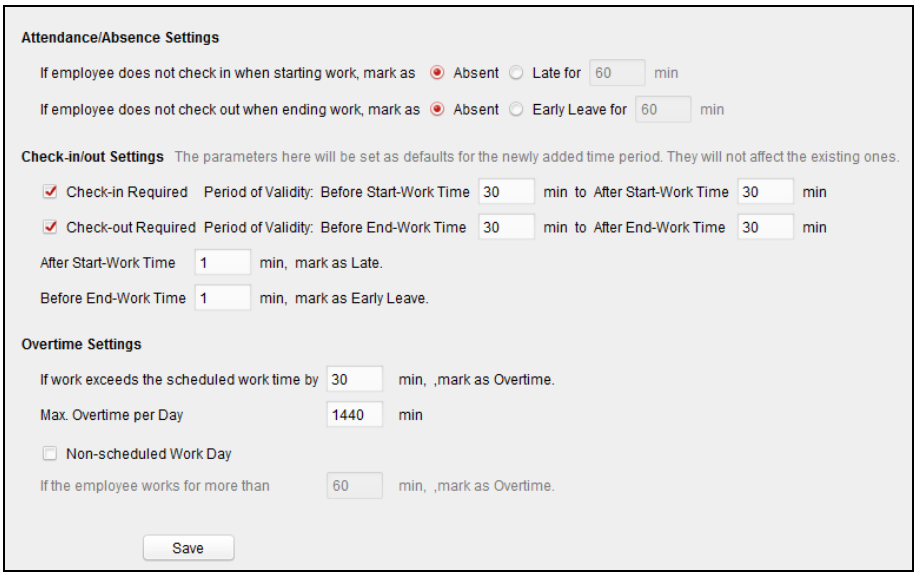
   Set Non-Work Day's Mark in Report: Input the mark as non-work day in report.

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

Attendance Rule Settings

Steps:

1. Click **Attendance Rule Settings** tab to enter the Attendance Rule Settings interface.



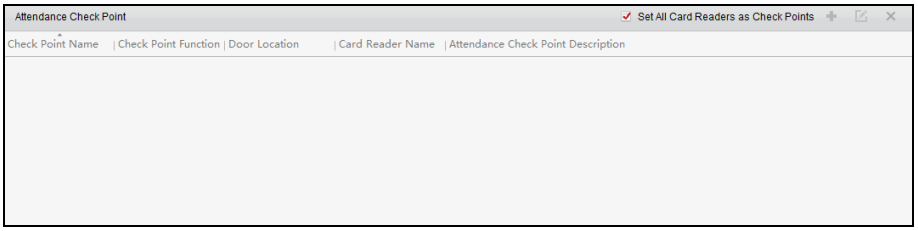
2. Set the attendance or absence settings.
   If employee does not check in when starting work, you can mark as **Absent** or **Late** and set the late time.
   If employee does not check out when ending work, you can mark as **Absent** or **Early Leave** and set the early leave duration.
3. Set the Check-in/out Settings.
   You can check the checkbox of **Check-in Required** or **Check-out Required** and set the valid period.
   You can also set the late rule or early leave rule.
   Note: The parameters here will be set as default for the newly added time period. It will not affect the existed one(s).
4. Set the overtime settings.
   You can set the overtime rule and set the maximum overtime for each day.
   (Optional) You can check **Non-scheduled Work Day** checkbox and set the overtime rule for non-work day.
5. Click **Save** to save the settings.

Attendance Check Point Settings

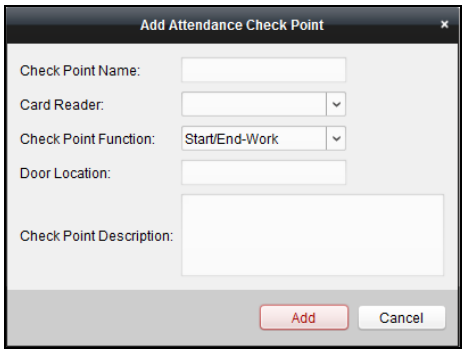
You can set the card reader(s) of the access control point as the attendance check point, so that the card swiping on the card reader(s) will be valid for attendance.

Steps:

1. Click **Attendance Check Point Settings** tab to enter the Attendance Check Point Settings interface.



2. Click + to pop up Add Attendance Check Point dialog.



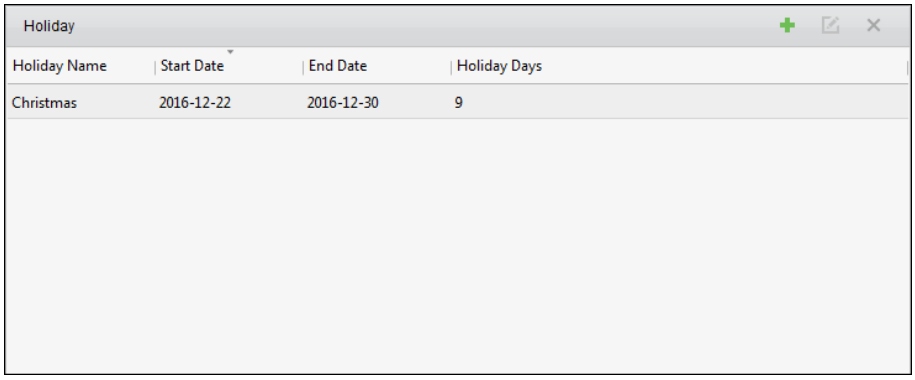
3. Set the related information.
   Check Point Name: Input a name for check point.
   Card Reader: Select the card reader from the drop-down list.
   Check Point Function: Select the function for check point.
   Door Location: Input the door location.
   Check Point Description: Set the description information for check point.
4. Click **Add** to add the attendance check point.
   The added attendance check point will display on the list.
5. (Optional) Check **Set All Card Readers as Check Points** checkbox.
   You can use all the card readers as check points.
   Note: If this checkbox is unchecked, only the card readers in the list will be added as attendance check points.

You can also edit or delete the card readers.
Click to edit the card reader.
Click to delete the card reader.

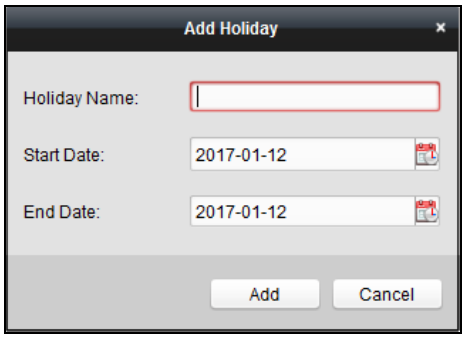
Holiday Settings

Steps:

1. Click **Holiday Settings** tab to enter the Holiday Settings interface.



2. Click to pop up Add Holiday dialog.



3. Set the related parameters.
   Holiday Name: Input the name for the holiday.
   Start Date / End Date: Click to specify the holiday date.
4. Click **Add** to add the holiday.
   The added holiday will display on the list.

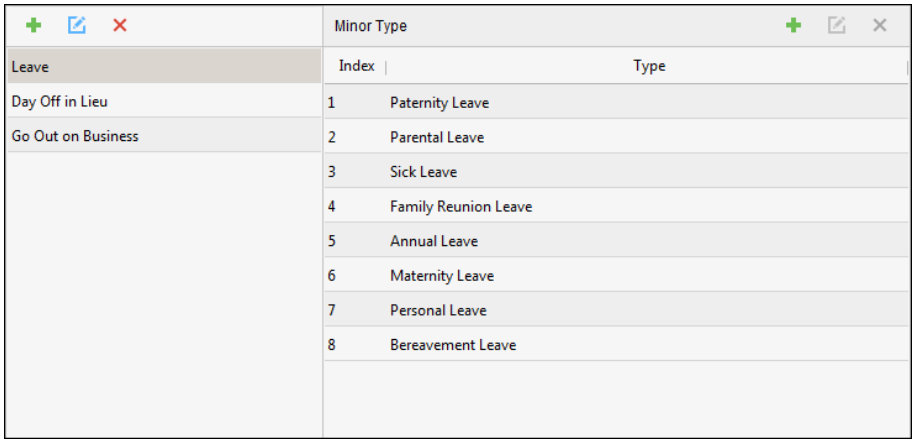
You can also edit or delete the holiday.
Click to edit the holiday.
Click to delete the holiday.

Leave Type Settings

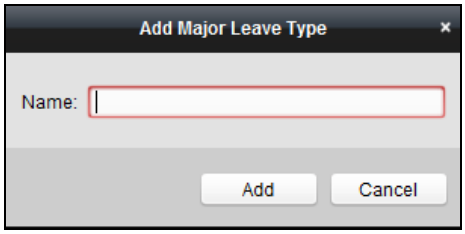
Purpose

Steps:

1. Click **Leave Type Settings** tab to enter the Leave Type Settings interface.



2. Add the major leave type.
   1) Click on the left panel to pop up the Add Major Leave Type dialog.

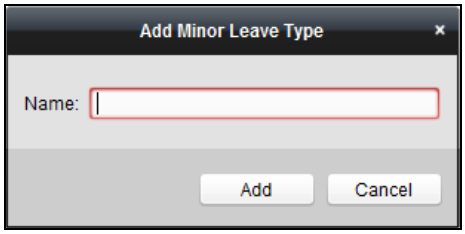


   2) Input the name for major leave type.
   3) Click **Add** to add the major leave type.

   You can also edit or delete the major leave type.
   Click to edit the major leave type.

Click ✕ to delete the major leave type.

3. Add the minor leave type.
   1) Select the major leave type.
      The minor leave type belonging to this major leave type will display on the right panel.
   2) Click ✚ on the right panel to pop up the Add Minor Leave Type dialog.



   3) Input the name for minor leave type.
   4) Click **Add** to add the minor leave type.

   You can also edit or delete the major leave type.
   Click ✎ to edit the minor leave type.
   Click ✕ to delete the minor leave type.

4.14.4 Attendance Statistics

Purpose:

After calculating attendance data, you can check the attendance summary, attendance details, abnormal attendance, overtime, card swiping logs and reports based on the calculated attendance data.

Notes:

- The client automatically calculates the previous day's attendance data at 1:00 am on the next day.
- Keep the client running at 1:00 am or it cannot calculate the previous day's attendance data automatically. If not calculated automatically, you can calculate the attendance data manually. For details, refer to *Manual Calculation of Attendance* in *Chapter 4.14.2 Attendance Handling*.

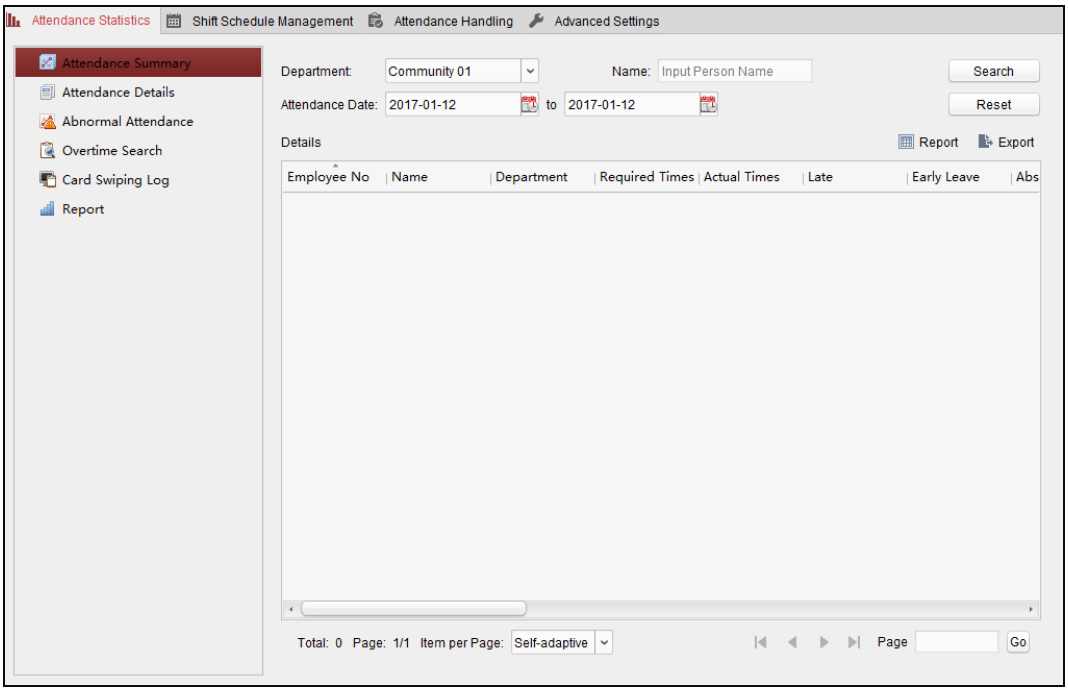
Attendance Summary

Purpose:

You can get all the attendance information statistics of the employees in the specified time period.

Steps:

1. In the Time and Attendance module, click **Attendance Statistics** tab to enter the Attendance Statistics page.
2. Click **Attendance Summary** item on the left panel to enter the Attendance Summary interface.

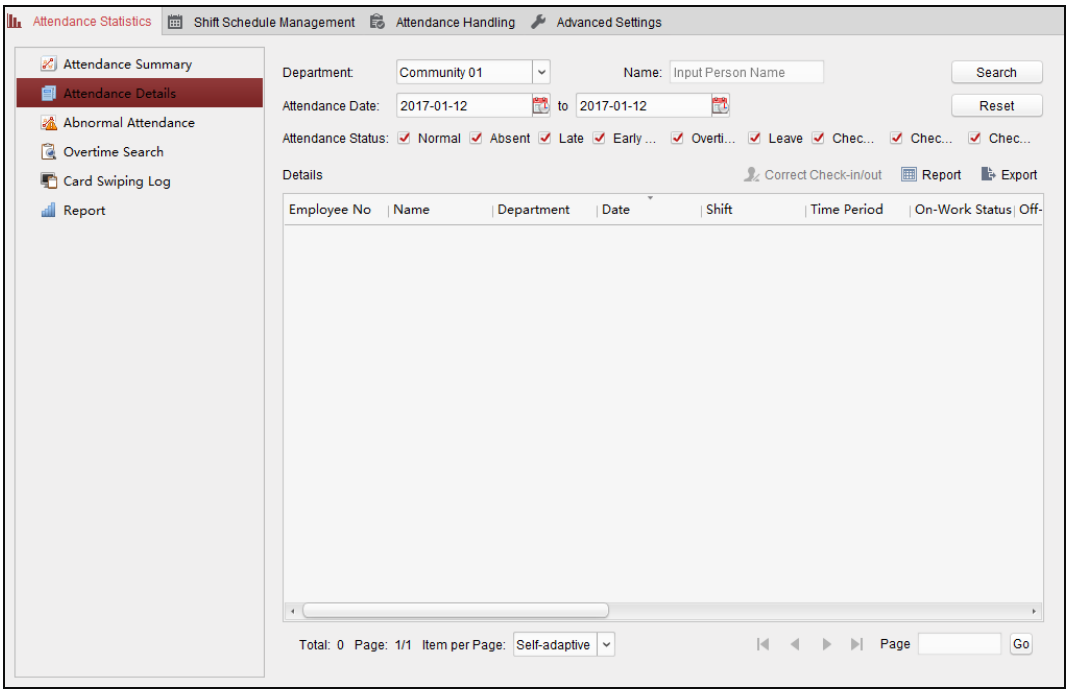


3. Set the search conditions, including department, employee name and attendance date.
   (Optional) You can click **Reset** to reset all the configured search conditions.
4. Click **Search** to start searching and the matched results will list on this page.
   (Optional) Click **Report** to generate the attendance report.
   (Optional) Click **Export** to export the results to the local PC.

Attendance Details

Steps:

1. In the Attendance Statistics page, click **Attendance Details** item on the left panel to enter the Attendance Details interface.



2. Set the search conditions, including department, employee name, attendance date and status.
   (Optional) You can click **Reset** to reset all the configured search conditions.
3. Click **Search** to start searching and the matched results will list on this page.
   (Optional) You can select a result item in the list and click **Correct Check-in/out** to correct the check-in or check-out status.
   (Optional) Click **Report** to generate the attendance report.
   (Optional) Click **Export** to export the results to the local PC.

Abnormal Attendance

You can search and get the statistics of the abnormal attendance data, including No., name and department of the employees, abnormal type, start/end time and date of attendance. For detailed operations, refer to *Chapter 0 Attendance Summary*.

Overtime Search

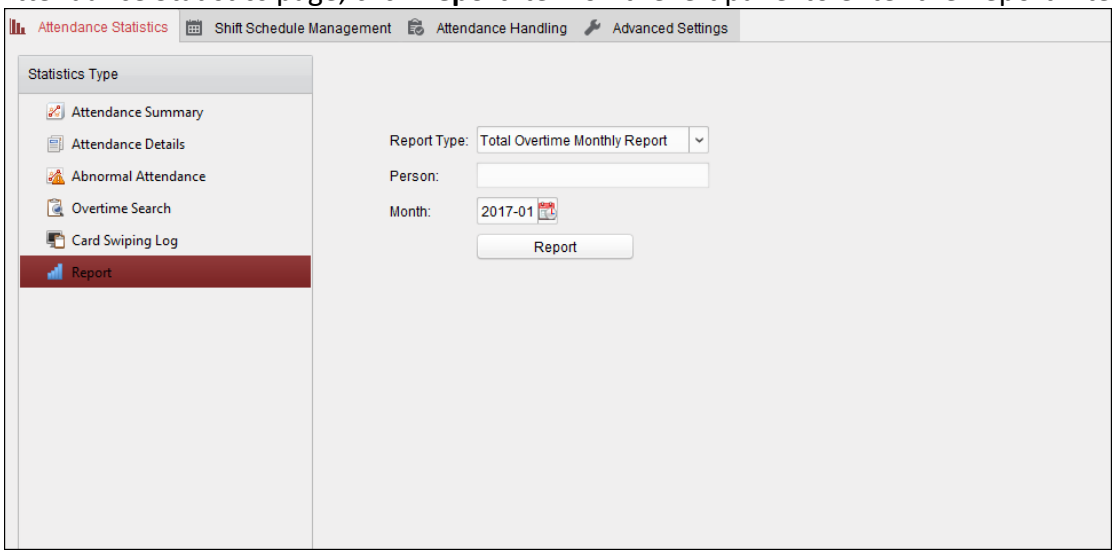
You can search and get the overtime status statistics of the selected employee in the specified time period. And you can check the detailed overtime information, including No., name and department of the employees, attendance date, overtime duration and overtime type. For detailed operations, refer to *Chapter 0 Attendance Summary*.

Card Swiping Log

You can search the card swiping logs used for the attendance statistics. After searching the logs, you can check the card swiping details, including name and department of the employees, card swiping time, card reader authentication mode and card No.. For detailed operations, refer to *Chapter 0 Attendance Summary*.

Report

In the Attendance Statistics page, click **Report** item on the left panel to enter the Report interface.

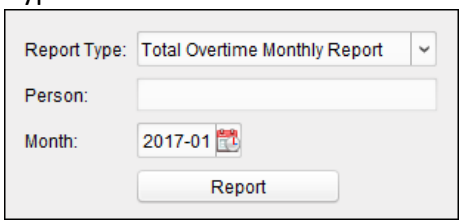


➢ **Generating Total Overtime Monthly Report**

Steps:

1. Click in the Report Type field to unfold the drop-down list and select **Total Overtime**

Monthly Report as the report type.



2. Click **Person** field to select the person.
3. Click to specify a month.
4. Click **Report** to start generating the matched total overtime monthly report.

➢ **Generating Overtime Details Monthly Report**

Select **Overtime Details Monthly Report** as the report type. You can generate overtime details monthly report. For detailed operations, refer to *Generating Total Overtime Monthly Report.*

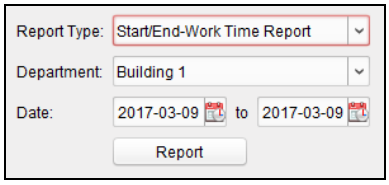
➢ **Generating Attendance Monthly Report**

Select **Attendance Monthly Report** as the report type. You can generate attendance monthly report. For detailed operations, refer to *Generating Total Overtime Monthly Report.*

➢ **Generating Start/End-Work Time Report**

Steps:

1. Click in the report type field to unfold the drop-down list and select **Start/End-Work Time Report** as the report type.



2. Click **Department** field to select the department.
3. Click to specify the start date and end date of a date period.
4. Click **Report** to start generating the matched total overtime monthly report.

➢ **Generating Department Attendance Report**

Set the report type as **Department Attendance Report** and you can generate department attendance report. For detailed operations, refer to *Generating Start/End-Work Time Report* above.

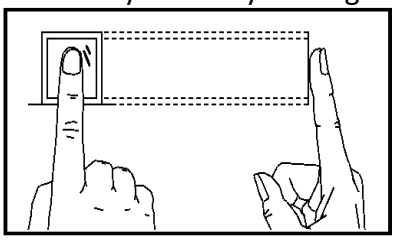
Appendix A Tips for Scanning Fingerprint

Recommended Finger

Forefinger, middle finger or the third finger.

Correct Scanning

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

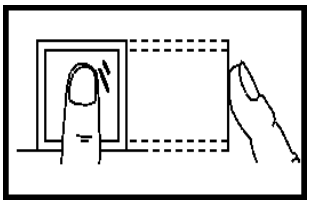


You should press your finger on the scanner horizontally. The center of your scanned finger should align with the scanner center.

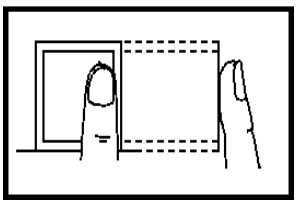
Incorrect Scanning

The figures of scanning fingerprint displayed below are wrong:

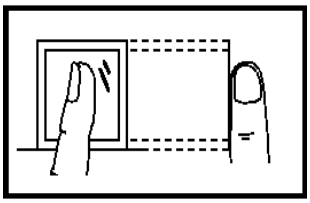
Vertical



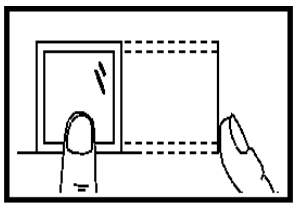
Edge I



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

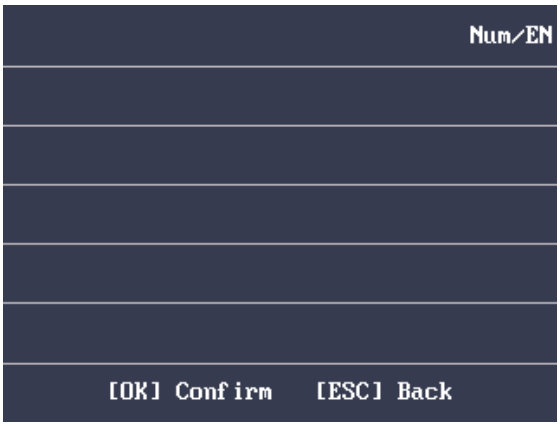
If your fingerprint is shallow, or it is hard to scan your fingerprint, we recommend you to use other authentication methods.

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

Appendix B Input Method Operation

Steps:

1. Press EN or key to enter the editing interface.
2. Press EN or key to shift input mode.
3. Input the text.
4. Press the OK key to confirm and exit the interface.



Note: Digits, uppercase letters, lowercase letters, Chinese characters and symbols are supported.

Appendix C Attendance Record Delete Rule

C.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.

C.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.

Appendix D 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

Appendix E Attendance Report Table

E.1 Description of Attendance Report File Name

File Name Rule

Device No. + Report Type.xls

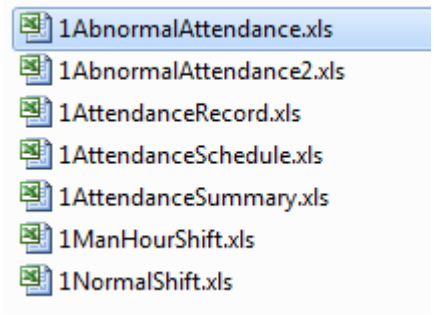
Device No.

A serial of numbers from 0 to 8.

Report Type

AbnormalAttendancel: The Attendance Abnormal table
AbnormalAttendance2: When the row of the Abnormal Attendance table is more than 60000, the record will be export in two tables. Here AbnormalAttendance2 refers to the second abnormal attendance table.
AttendanceSummary: The Attendance Summary table
AttendanceRecord: The Attendance Record table
AttendanceSchedule: The attendance schedule table
NormalShift: The Normal Shift table
ManHourShift: The Man-Hour Shift table

Example



E.2 Attendance Report Table Description

Attendance Schedule Create Time: 2017-04-26 10:12:20											
Employee ID	Card No.	Name	Department	2017/01/01 (Sun.)		2017/01/02 (Mon.)		2017/01/03 (Tue.)		2017/01/04 (Wed.)	
				Shift No.	Shift Type	Shift No.	Shift Type	Shift No.	Shift Type	Shift No.	Shift Type

Attendance Schedule 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.

Normal Shift Create Time: 2017-04-26 11:12:20									
Shift No.	Shift Name	Period 1		Period 2		Period 3		Period 4	
		Start	End	Start	Stop	Start	Stop	Start	Stop

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 (Start) and 17:00 (End), 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 Create Time: 2017-04-26 11:12:20					
Shift No.	Shift Name	Work Duration (min)	Latest Start-Work Time	Period 1	
				Start	End

Man-Hour Shift Table: Set the Man-Hour Shift working duration. If set the Latest Start-Work Time to 0, all users are attendant. If set the Latest Start-Work Time to more than 0, the user will be absent by taking attendance after the configured time.

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

Abnormal Attendance Create Time: 2017-04-26 11:12:20 SW: Start-Work EW: End-Work								
Employee ID	Card No.	Name	Department	Date	SW-EW	Late Duration (min)	Early Leave Duration (min)	Total (min)

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. Card No.: The user's card No.
3. Name: The user's name.
4. Department: The department of the user.
5. Date: The date of the data generated.
6. SW-EW: Up to 4 periods can be configured. It records the attendance time of each user every day.
7. Late Duration (min): The start-work attendance time is later than the normal start-work time.
8. Early Leave Duration (min): The end-work attendance time is earlier than the normal end-work time.
9. Total: The absence time duration of the day.

Attendance Record Create Time: 2017-04-24 19:17:25 SW: Start-Work EW: End-Work									
Employee ID	Card No.	Name	Department	2017/01/01	2017/01/02	2017/01/03	2017/01/04	2017/01/05	2017/01/06
				SW-EW	SW-EW	SW-EW	SW-EW	SW-EW	SW-EW

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

1. Employee ID: The user's ID No.
2. Card No.: The user's card No.
3. Name: The user's name.
4. Department: The department of the user.

Attendance Summary Create Time: 2017-04-24 19:17:25										
Empl-oyee ID	Card No.	Name	Depart-ment	Late Times	Late Duration (min)	Early Leave Times	Early Leave Duration (min)	Absence Times	Absence Time Duration (min)	Attendance/Total Work Days

Attendance Summary 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. Card No.: The user's card No.
3. The user's name.
4. Department: The user's department.
5. Late Times: The start-work attendance time is later than the normal start-work time. Late arriving for no more than once every day.
6. Late Duration (min): Total time duration for late.
7. Early Leave Times: The end-work attendance time is earlier than the normal end-work time. Early leave for no more than once every day.
8. Early Leave Duration (min): Total time duration for early leave.
9. Absence Times: Total absence times.
10. Absence Time Duration (min): Total absence duration.
11. Attendance/Total Work Days: Total attendance days.

0101001070823

First Choice for Security Professionals