



HIKVISION

Access Control Terminal

User Manual

V1.1.0

UD01651B

User Manual

©2016 Hangzhou Hikvision Digital Technology Co., Ltd.

This User Manual is intended for users of the models below:

Series	Model
Standalone Access Control Terminal	DS-K1T105E/M
	DS-K1T105E/M-C (with Camera)
Optical IP-Based Fingerprint Access Control Terminal	DS-K1T200EF/MF
	DS-K1T200EF/MF-C (with Camera)

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

About this Manual

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

Trademarks

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

Legal Disclaimer

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

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

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

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

Support

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

Regulatory Information

FCC Information

FCC compliance: This equipment has been tested and found to comply with the limits for a digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

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 Low Voltage Directive 2006/95/EC, the EMC Directive 2004/108/EC, 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 (A)/NMB-3(A) standards requirements.

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

1 Overview	3
1.1 Introduction	3
1.2 Main Features	3
1.2.1 Main Features of DS-K1T105 Series Model	3
1.2.2 Main Features of DS-K1T200 Series Model	4
2 Appearance	5
2.1 Appearance of DS-K1T105 Series Model	5
2.2 Appearance of DS-K1T200 Series Model	5
2.2.1 Description of Components	5
2.3 Appearance of Keys	6
2.3.1 Description of Items	6
3 Terminal Connection	8
3.1 Terminal Description	8
4 Wiring Description	10
4.1 External Device Wiring Overview	10
4.2 The Wiring of External Card Reader	11
4.2.1 The Wiring of External RS-485 Card Reader	11
4.2.2 The Wiring of External Wiegand Card Reader	11
4.3 The Wiring of Electric Lock and Door Contact	12
4.3.1 The Wiring of Electric Lock	12
4.3.2 The Wiring of Door Contact	12
4.4 The Wiring of Exit Button	13
4.5 The Wiring of Alarm Input	13
4.6 The Wiring of External Alarm Device	14
4.7 Card Reader Connection	14
4.7.1 The Wiring of Wiegand	14
4.7.2 The Wiring of RS-485 Output	15
5 Activating the Access Control Terminal	16
5.1 Activating via SADP Software	16
5.2 Activating via Client Software	17
6 Basic Operation	19
6.1 User Management	20
6.1.1 Adding User	20
6.1.2 Managing User	21
6.2 Communication Settings	23
6.2.1 Network Settings	24
6.2.2 Serial Port Settings	24
6.2.3 Wiegand Settings	25
6.2.4 Wi-Fi Settings	26
6.3 System Settings	26
6.3.1 Setting System	27
6.3.2 Managing Data	28
6.3.3 Restoring Settings	28
6.3.4 Door Settings	29
6.3.5 Setting the Camera	29
6.4 Time Settings	30

6.5 Upload/Download Settings	30
6.6 Testing	31
6.7 Log Query Settings	31
6.8 System Information	32
7 Client Operation	33
7.1 Overview of Access Control System	33
7.1.1 Description.....	33
7.1.2 Configuration Flow	33
7.2 Device Management	34
7.2.1 Controller Management	34
7.2.2 Access Control Point Management.....	41
7.3 Permission Management	42
7.3.1 Person Management	42
7.3.2 Card Management	47
7.3.3 Schedule Template.....	50
7.3.4 Door Status Management.....	53
7.3.5 Interact Configuration.....	55
7.3.6 Access Permission Configuration	58
7.3.7 Attendance Management	61
7.3.8 Advanced Functions.....	78
7.4 Checking Status and Event	85
7.4.1 Status Monitor	85
7.4.2 Access Control Event.....	86
7.4.3 Event Search	87
7.5 System Maintenance	89
7.5.1 Log Management	89
7.5.2 System Configuration	91
Appendix: Tips for Scanning Fingerprint	94

1 Overview

1.1 Introduction

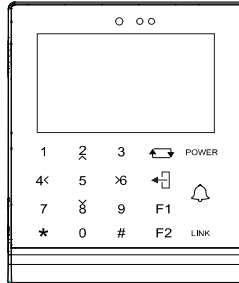


Figure 1-1 DS-K1T105 Series Standalone Access Control Terminal Front Panel

DS-K1T105 is a series of standalone access control terminal with picture capturing function. DS-K1T105 is designed with a 2.8-inch LCD display screen, and HD camera (2 MP optional). It supports two network communication methods (TCP/IP, and Wi-Fi), and supports offline operation.

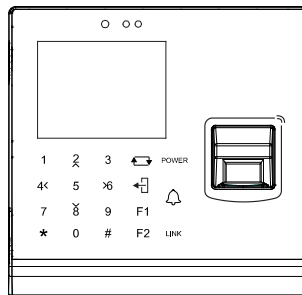


Figure 1-2 DS-K1T200 Series IP-Based Fingerprint Access Control Terminal Front Panel

DS-K1T200 is a series optical IP-based fingerprint access control terminal with multiple advanced technologies including fingerprint recognition, face detection, Wi-Fi, smart card recognition, LCD display screen, and picture capturing technology. It is designed with a 2.8-inch LCD display screen, and HD camera (2 MP optional). It is equipped with optical fingerprint recognition module (supporting 1:1 mode and 1:N mode), and supports offline operation.

1.2 Main Features

1.2.1 Main Features of DS-K1T105 Series Model

- Doorbell ringtone settings function
- Touch mode and blue light display technique for keypad
- Stand-alone settings for the terminal
- 2.8-inch LCD display screen
- Transmission modes of wired network (TCP/TP) and Wi-Fi
- Face detection and picture capturing function implemented by built-in camera (2 MP optional, only supports DS-K1T105E/M-C)
- Supports multiple door opening modes (card, card + password, exit button, etc.)
- Supports RS-485 communication for connecting to external card reader
- Supports working as a card reader, and supports Wiegand interface and RS-485 interface for accessing the controller
- Max. 100,000 valid card No., and Max. 300,000 access control events records storage
- Supports EM card reading (DS-K1T105E/E-C)
- Supports Mifare card reading, including card No. reading, & writing function (DS-K1T105M/M-C)
- Tampering detection, unlocking overtime alarm, invalid card swiping over times alarm, and duress card alarm
- Accurate data and time display provided by built-in electronic clock and watchdog program to ensure the basic function of the terminal

- Data can be permanently saved after power-off

1.2.2 Main Features of DS-K1T200 Series Model

- Doorbell ringtone settings function
- Touch mode and blue light display technique for keypad
- Stand-alone settings for the terminal
- 2.8-inch LCD display screen
- Transmission modes of wired network (TCP/IP) and Wi-Fi
- Face detection and picture capturing function implemented by built-in camera (2 MP optional, only supports DS-K1T200EF/MF-C)
- Supports RS-485 communication for connecting external card reader
- Supports working as a card reader, and supports Wiegand interface and RS-485 interface for accessing the controller
- Max. 100,000 card No., Max. 300,000 access control events records , and Max. 9500 fingerprints storage
- Adopts the optical fingerprint module, supporting 1:N mode (fingerprint, card + fingerprint) and 1:1 mode (card + fingerprint)
- Supports multiple authentication modes (card, fingerprint, card + fingerprint, card + password, fingerprint + password, card + fingerprint + password, and so on.)
- Supports EM card reading (DS-K1T200EF/EF-C)
- Supports Mifare card reading, including card No. reading, and sector reading & writing (DS-K1T200MF/MF-C)
- Tampering detection, unlocking overtime alarm, invalid card swiping over times alarm, duress card alarm, and so on
- Accurate data and time display provided by built-in electronic clock and watchdog program to ensure the basic function of the terminal
- Data can be permanently saved after power-off.

2 Appearance

2.1 Appearance of DS-K1T105 Series Model

Please refer to the following content for detailed information of the DS-K1T105 series model.

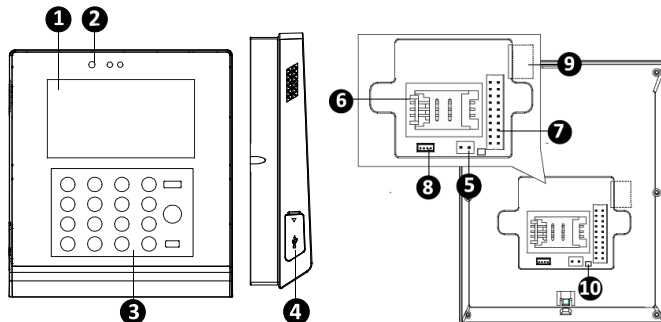


Figure 2-1 Appearance of DS-K1T105 Series Model

Table 2-1 Description of DS-K1T105 Series Model

No.	Description
1	2.8-Inch LCD Display Screen
2	HD Camera with 2 MP (only DS-K1T105E/M/ -C support)
3	Keypad
4	USB 2.0 Interface
5	Power Interface
6	PSAM Card Slot
7	External Wiring Terminals
8	Serial Port
9	Ethernet Port
10	Tampering Prevention Switch

2.2 Appearance of DS-K1T200Series Model

Please refer to the following content for detailed information of DS-K1T200 series model

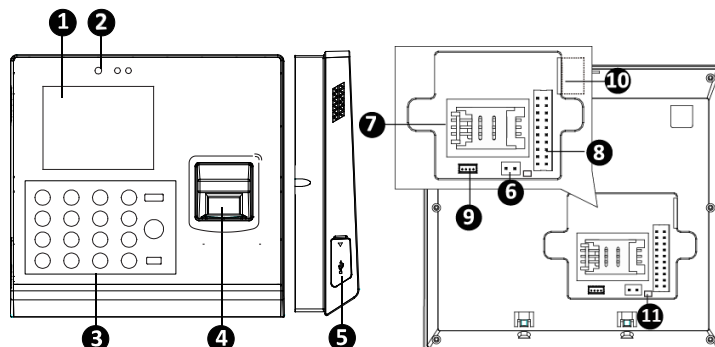


Figure 2-2 Appearance of DS-K1T200 IP-Based Fingerprint Access Control Terminal

2.2.1 Description of Components

Table 2-2 DS-K1T200 IP-Based Fingerprint Access Control Terminal Components

No.	Description
1	2.8-Inch LCD Display Screen

No.	Description
2	HD Camera with 2 MP (only DS-K1T200EF/MF -C support)
3	Keypad
4	Optical Fingerprint Reading Module
5	USB 2.0 Interface
6	Power Interface
7	PSAM Card Slot
8	External Wiring Terminals
9	Serial Port
10	Ethernet Port
11	Tampering Prevention Switch

2.3 Appearance of Keys

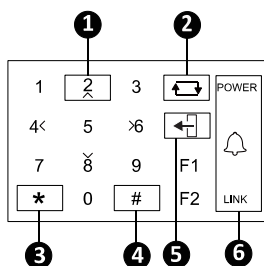


Figure 2-3 Appearance of Keys

2.3.1 Description of Items

Table 2-3 Description of Keys

No.	Description			
1	Numeric Keys: Enter number in the textbox. Direction Keys: Select icons in the menu.			
2	Editing Key: Click the key to enter/exit the editing status.			
3	Exiting Key: Click the key to exit the menu.			
4	Confirming Key: Click the key to confirm operations. Long-click the key to enter the login interface.			
5	Deleting Key: Click the key to delete contents in the textbox.			
6	Status Indicator: Indicator for power, ring, and connection status	POWER	Power Status Solid Blue: Normal Power. Off : Power Exception.	
			Doorbell Ring	
		LINK	Normal Card/ Illegal Card	Normal Card: Solid Blue Illegal Card: Solid Red
			Connection Status	Off: Network or Wi-Fi disconnected. Solid Blue: Network or Wi-Fi connected, but client unarmed. Flicker Blue: Network or Wi-Fi connected, but client armed.
			Flicker blue in the card reader mode.	

Note: In the Event Card Interact interface in the iVMS-4200 Client Software, choose the alarm output of Event Bell. You can connect a bell at the alarm output terminal. For details about configuring the Event Bell alarm output, see the *User Manual of iVMS-4200 Client Software*.

3 Terminal Connection

3.1 Terminal Description

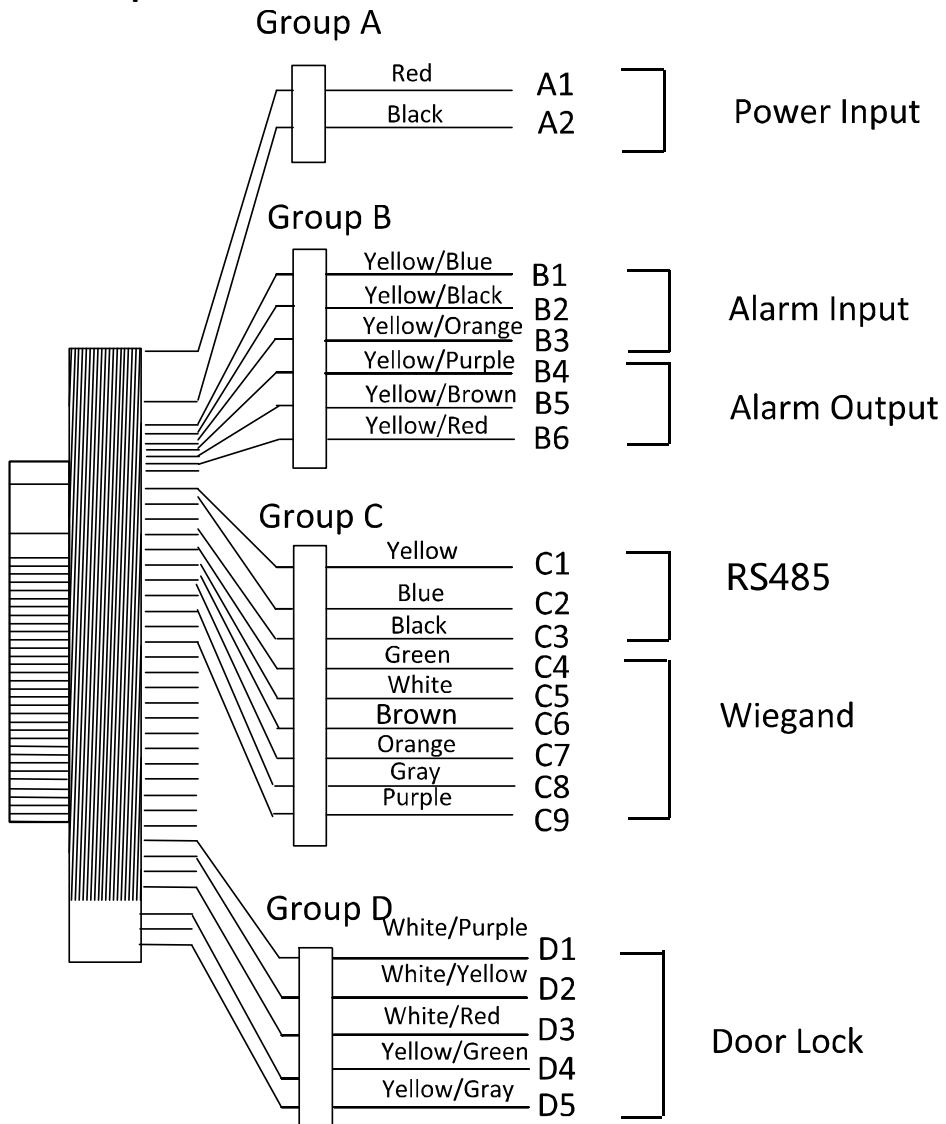


Figure 3-1 Terminal Diagram of Access Control Terminal

Table 3-1 Terminal Description

Line Group	No.	Function	Color	Terminal Name	Description
Line Group A	A1	Power Input	Red	+12V	12V DC Power Supply
	A2		Black	GND	GND
Line Group B	B1	Alarm Input	Yellow/Blue	IN1	Alarm Input 1
	B2		Yellow/Black	GND	GND
	B3		Yellow/Orange	IN2	Alarm Input 2
	B4	Alarm Output	Yellow/Purple	NC	Alarm Output Wiring
	B5		Yellow/Brown	COM	
	B6		Yellow/Red	NO	
Line Group C	C1	RS-485 Communication Port	Yellow	485 +	RS-485 Wiring
	C2		Blue	485 -	
	C3		Black	GND	
	C4	Wiegand	Green	W0	Wiegand Wiring 0
	C5		White	W1	Wiegand Wiring 1
	C6		Brown	WG_OK	Wiegand Authenticated
	C7		Orange	WG_ERR	Wiegand Authentication Failed
	C8		Grey	TAMPER	Tampering Alarm Wiring
	C9		Purple	BUZZER	Buzzer Wiring
Line Group D	D1	Lock	White/Purple	NC	Lock Wiring
	D2		White/Yellow	COM	
	D3		White/Red	NO	
	D4		Yellow/Green	SENSOR	Door Contact Signal Input
	D5		Yellow/Grey	BUTTON	Exit Door Wiring

4 Wiring Description

4.1 External Device Wiring Overview

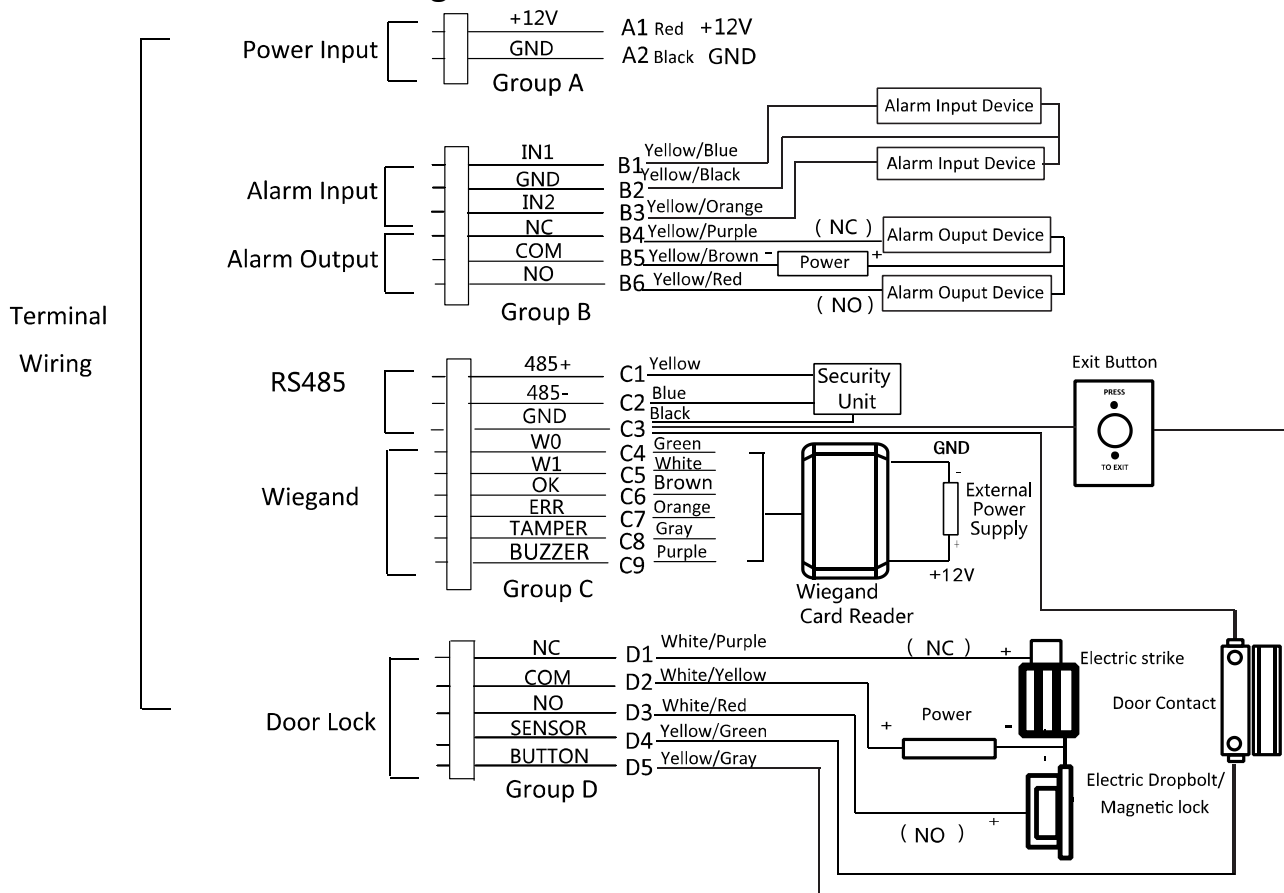


Figure 4-1 External Device Connection Diagram

4.2 The Wiring of External Card Reader

4.2.1 The Wiring of External RS-485 Card Reader

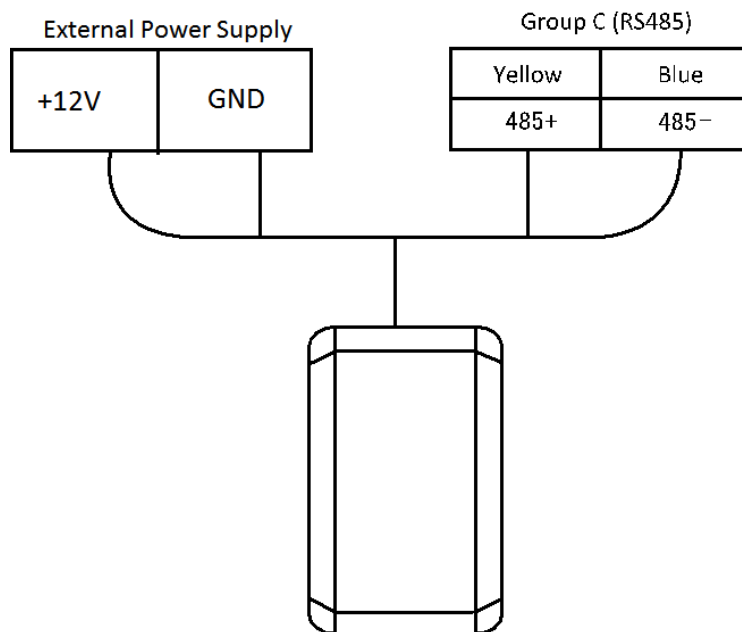


Figure 4-2 External RS-485 Card Reader Connection Diagram

4.2.2 The Wiring of External Wiegand Card Reader

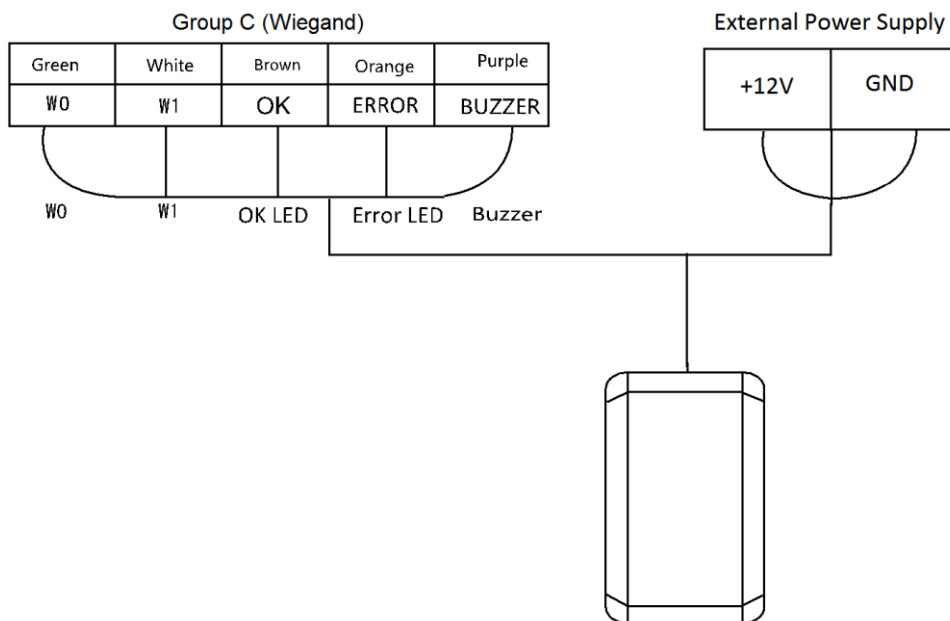


Figure 4-3 External Wiegand Card Reader Connection Diagram

Notes:

- Set the dial-up of the external card reader as 2 when connected to the access control terminal.
- The external power supply and the access control terminal should use the same GND cable.

4.4 The Wiring of Exit Button

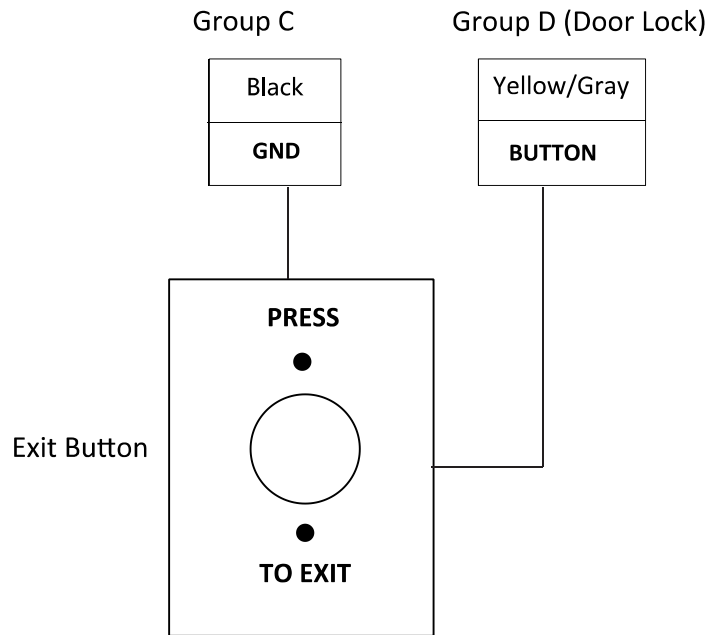


Figure 4-6 The Installation of Exit Button

4.5 The Wiring of Alarm Input

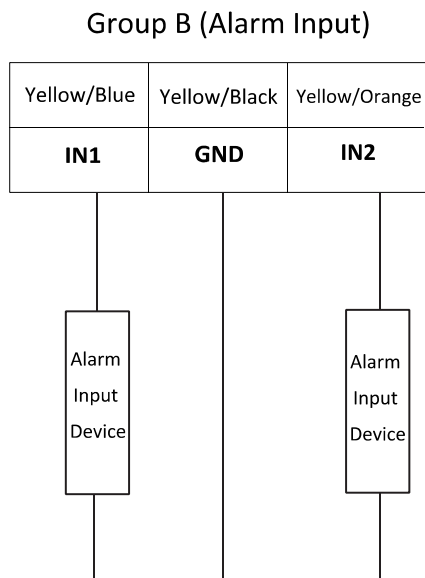


Figure 4-7 Alarm Input Connection

4.6 The Wiring of External Alarm Device

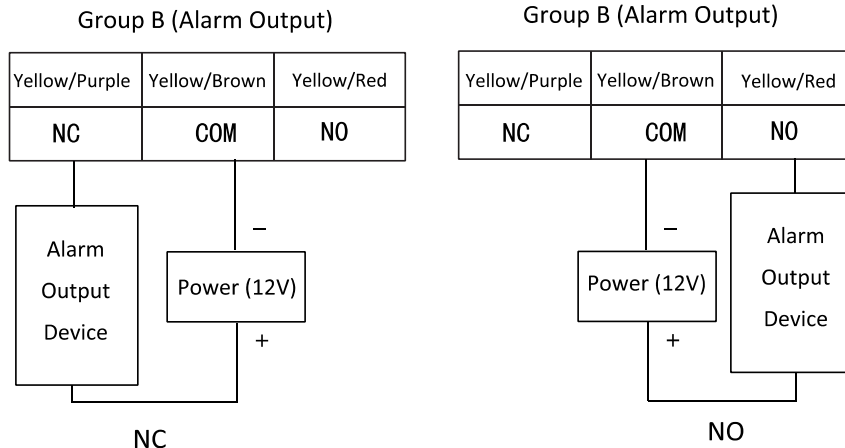


Figure 4-8 The Installation Diagram of External Alarm Device

4.7 Card Reader Connection

The access control terminal can be switched into the card reader mode. It can access to the access control as a card reader, and supports Wiegand communication port and RS-485 communication port.

Note: When the access control terminal works as a card reader, it only supports being connected to the controller, but does not support alarm input or output, or the connection of external devices.

4.7.1 The Wiring of Wiegand

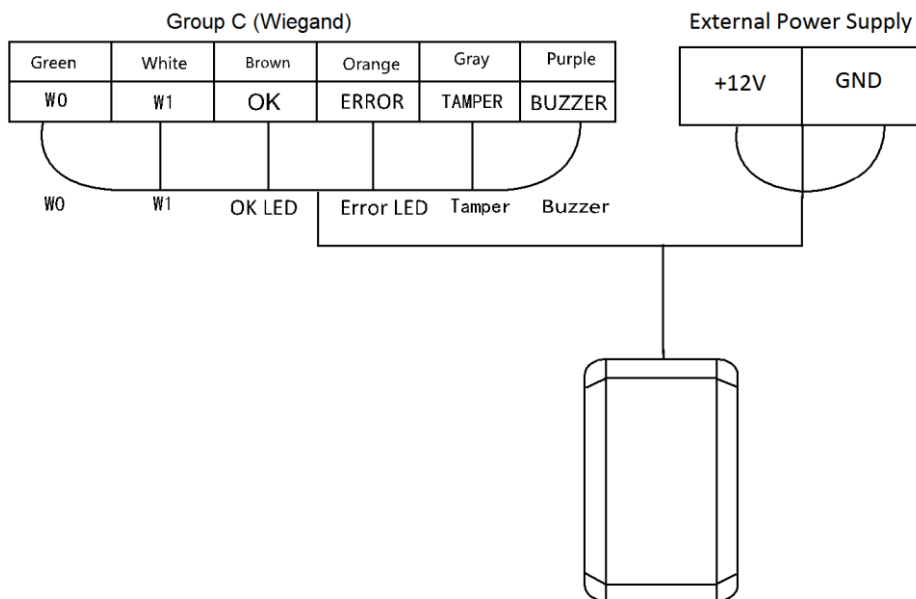


Figure 4-9 Wiegand Connection Diagram

Notes:

- When the access control terminal works as a card reader, you must connect the **WG_ERR**, **BUZZER** and **WG_OK** interfaces if you want to control the LED and buzzer of the Wiegand card reader.
- Set the working mode of the terminal as card reader, which can be configured in **System Parameter** → **Mode Switch**, if the terminal is required to work as a card reader. The card reader mode support to communicate by Wiegand or RS-485.
- The distance of Wiegand communication should be no longer than 80 m.
- The external power supply and the access control terminal should use the same GND cable.

4.7.2 The Wiring of RS-485 Output

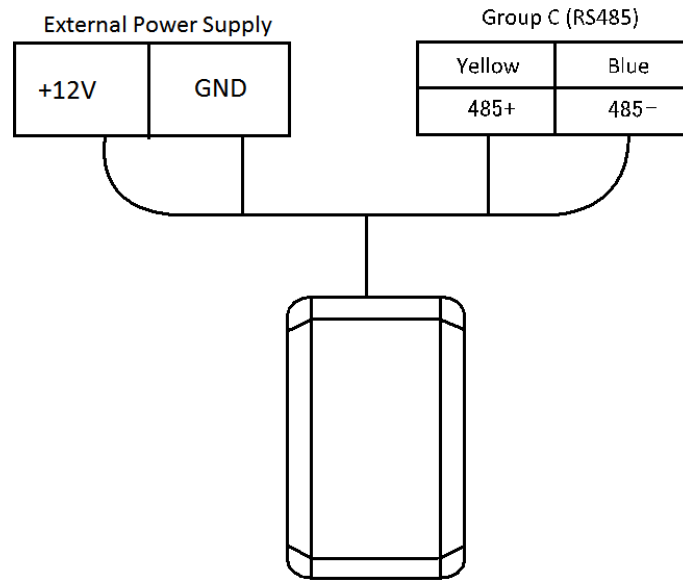


Figure 4-10 RS-485 Connection Diagram

Notes:

- Set the working mode of the terminal as card reader, which can be configured in **System Parameter** → **Mode Switch**, if the terminal requires working as a card reader.
- When the access control terminal works as a RS-485 card reader, the default RS-485 address is 1. RS-485 address can also be configured in **System Parameter** → **Serial Port Settings**.
- The external power supply and the access control terminal should use the same GND cable.

5 Activating the Access Control Terminal

Purpose:

You are required to activate the terminal first before using it.

Activation via SADP, and Activation via client software are supported.

The default values of the control terminal are as follows.

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

5.1 Activating via SADP Software

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.

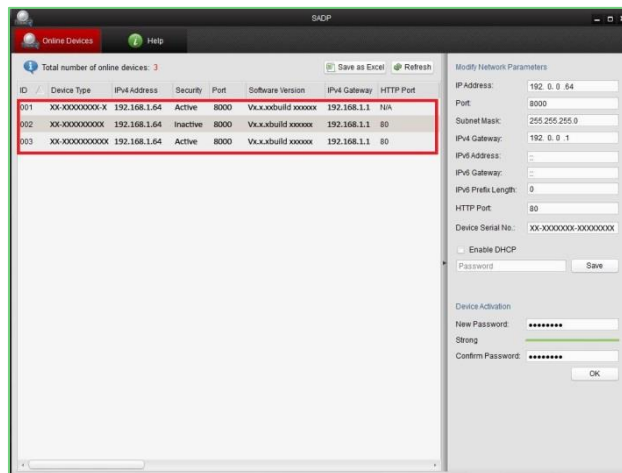


Figure 5-1 SADP Interface

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 **OK** to save the password.

You can check whether the activation is completed on the pop-up window.

If activation failed, please make sure that the password meets the requirement and then try again.

5. Change the device IP address to the same subnet with your computer by either modifying the IP address manually or checking the checkbox of Enable DHCP.

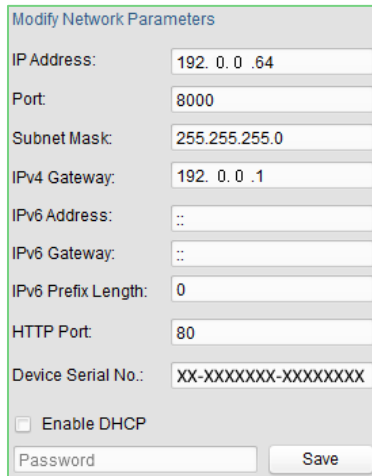


Figure 5-2 Modify Network Parameters Interface


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

5.2 Activating via Client Software

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 the  icon on the upper-left side of the page, select **Access Control** to enter the control panel.

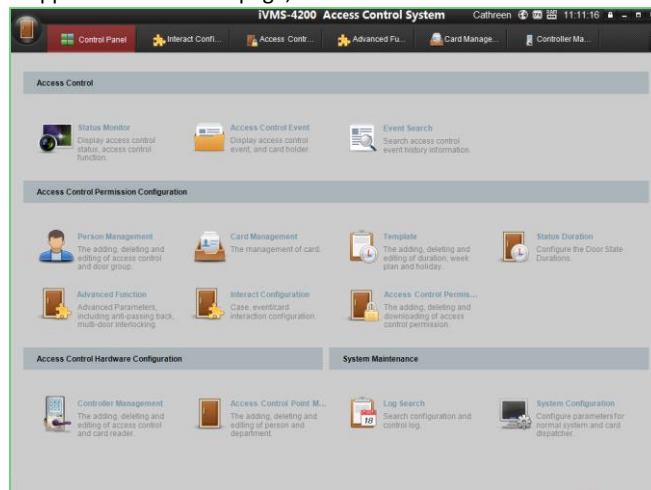


Figure 5-3 Control Panel Interface

3. Click the **Controller Management** icon to enter the Controller Management interface, as shown in the figure below.

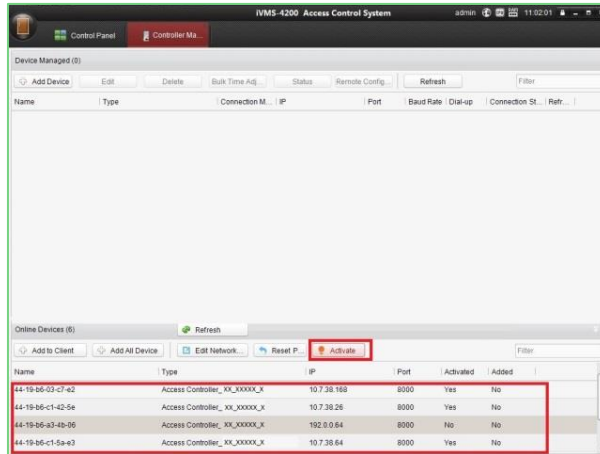


Figure 5-4 Device List

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.

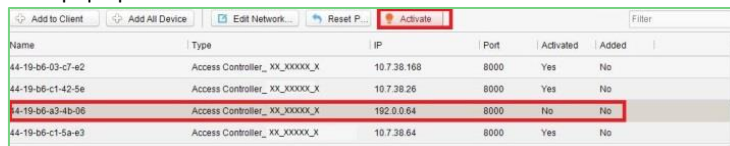


Figure 5-5 List Selecting Interface

6. 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.



7. Click **OK** button to start activation.
8. Click the **Edit Network...** button to pop up the Network Parameter Modification interface.
9. Change the device IP address to the same subnet with your computer by either modifying the IP address manually or checking the checkbox of Enable DHCP.
10. Input the password to activate your IP address modification.

6 Basic Operation

Before You Start:

- You should activate the device before the first login. Otherwise, after powered on, the system will switch into activate notifying interface. For detailed information about activation, see *Chapter 5 Activating the Access Control Terminal*.

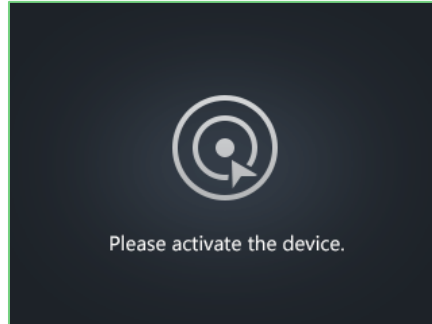
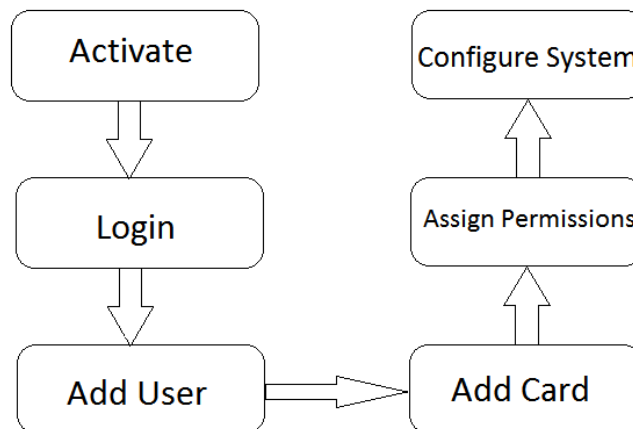


Figure 6-1 Activation Notifying Interface

- You should enter the default password for the first login.
Enter **System Settings** -> **System Parameter** -> **Login Password** to reset the login password.
The default password is 12345.

The working flow is as follows:



Steps:

- Power on the device to enter the initial interface.

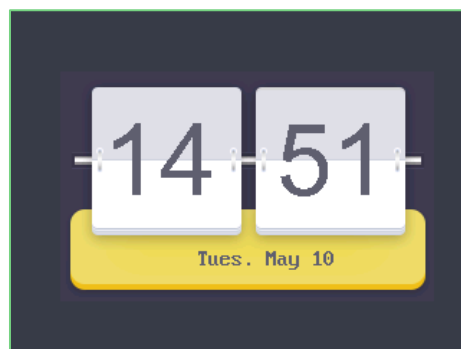


Figure 6-2 Initial Interface

- Long-click the # key to enter the password authentication interface.



Figure 6-3 Password Authentication Interface

3. Enter the default configuration password.
 - Tap the # key to confirm the settings. If the configuration password authentication failed, the system will return to the initial interface, and if the configuration password is successfully authenticated, the system will enter the menu operation interface

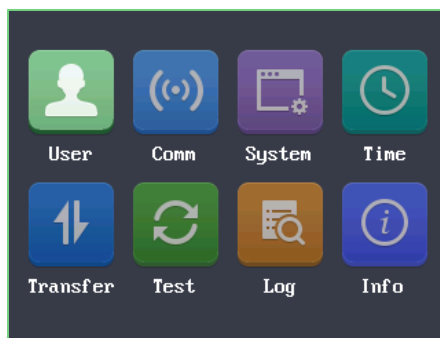


Figure 6-4 Menu Operation Interface

On the menu operation interface, you can manage users, set communication parameters, set system parameters, and so on.

6.1 User Management

Purpose:

On the user management interface, you can add and manage users.

Steps:

1. Move the cursor to **User** (user management) with the direction keys.
2. Tap the # key to enter the user management interface.

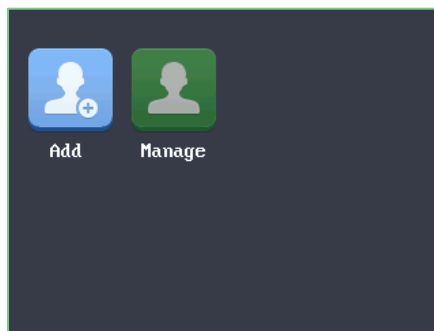


Figure 6-5 User Management Interface

6.1.2 Adding User

Purpose:

In the **Adding User** menu, you can add users, register card, and record fingerprints optionally for the corresponding person.

Steps:

1. Move the cursor to **Add** (add user) by using the direction keys.
2. Tap the # key to enter the card registration interface.



Figure 6-6 Card Registration Interface

3. Register the card.
 - Register the card by swiping the card.
 - 1) Place the card on the induction area.
 - 2) The system displays the card No. in the textbox automatically with a beep sound if the card No. has been recognized. .
 - Register the card by entering the card number into the **or enter the Card No.** textbox.
 - 1) Tap the $\leftarrow \rightarrow$ key to enter the editing mode.
 - 2) Enter the card number into the textbox.
 - 3) Tap the $\leftarrow \rightarrow$ key to exit the editing mode.
4. After registering the card, a dialog box about whether to register the fingerprint pops up.

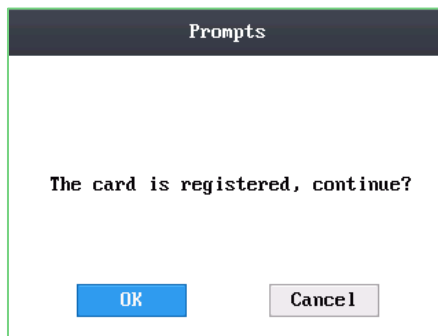


Figure 6-7 Card Registration PoP-Up Window

- 1) Move the cursor to the **OK** button, and tap the # key to enter the fingerprint registration interface.

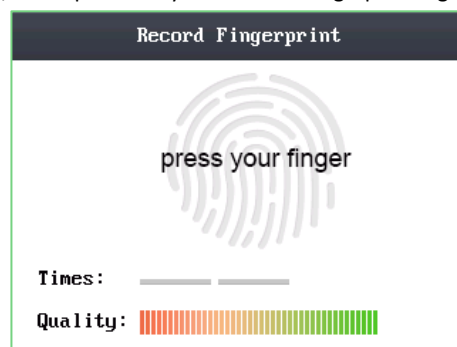


Figure 6-8 Fingerprint Registration Interface

- 2) Place the finger on the fingerprint scanner, rise and rest your finger by following the corresponding voice prompts.

Notes:

- The fingerprint registration function only supports device with fingerprint module.
- The same fingerprint cannot be repeatedly registered.
- For the optical access control terminal, you should place your finger twice to register the fingerprint. For details about scanning the fingerprint, see [Appendix](#).

6.1.2 Managing User

1. Move the cursor to **Manage** (edit user) by using direction keys on the user management interface.
2. Tap the # key to enter the managing user interface.

Searching User

Steps:

1. Move the cursor to a user by using direction keys.
2. Tap the # key to pop up an interface for selecting corresponding operations.

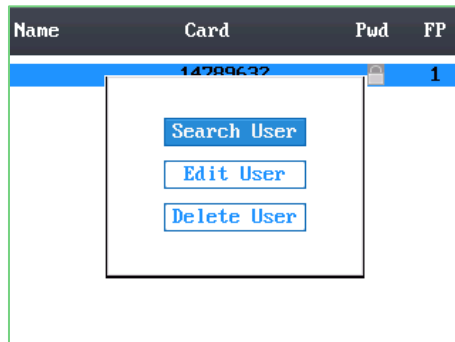


Figure 6-9 Managing User Interface

3. Move the cursor to **Search User**.
4. Tap the # key to enter the searching interface.

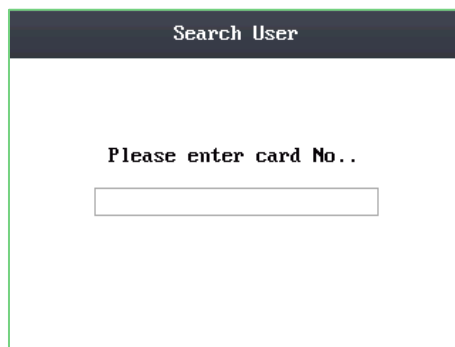


Figure 6-10 Searching Interface

5. Enter the card number into **Please enter card No.** textbox.
6. Tap the # key to view the basic information about the card holder.

Editing User

Steps:

1. Move the cursor to a user by using direction keys.
2. Click the # key to popup an interface for selecting corresponding operations. (Figure 6-9)
3. Move the cursor to **Editing User**.
4. Tap the # key to enter the editing interface.

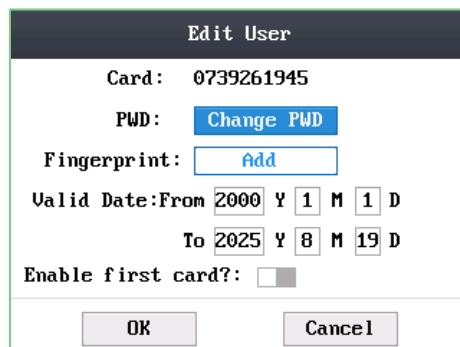


Figure 6-11 Editing Interface

5. Edit the user information.
 - Adding the Fingerprint

Move the cursor to **Add** to enter the fingerprint registration interface. See details in step 4 of adding user.

Note: DS-K1T105 series model does not support this function.

- Changing the Password
 - 1) Move the cursor to **Change PWD** to enter the password changing interface.
 - 2) Enter a new password.
 - 3) Confirm the new password.

Figure 6-12 Password Changing Interface

- Changing the valid date

You can set the start/end time of the user's permission.

Click the ↔ key to enter/exit the editing mode.
 - Enabling first card

Tap the # key to enable first card.

Note: After enabling first card, the door remains open during the pre-defined valid duration.
6. Move the cursor to the **OK** button, and click the # key to confirm the settings.

Deleting the User

Steps:

1. Move the cursor to the user by using direction keys.
2. Tap the # key to pop up an interface for selecting corresponding operations. (Figure 6-9)
3. Move the cursor to **Delete User**, and tap the # key to enter the deleting interface.
4. Move the cursor to **Delete User**, **Delete PWD only** or **Delete FP only**.

Delete User: Delete the user and the overall information.

Delete PWD only: Only delete the password set by the user.

Delete FP only: Only delete the fingerprint information of the user.

Note: DS-K1T105 series model does not support this function.

5. Tap the # key to finish the deleting operation.

Note: You can tap * key to return to the main menu.

6.2 Communication Settings

Purpose:

On the communication settings interface, you can set network parameters, the serial port, Wiegand parameters, and Wi-Fi.

Steps:

1. Move the cursor to **Comm** (communication settings) by using direction keys.
2. Tap the # key to enter the communication settings interface.

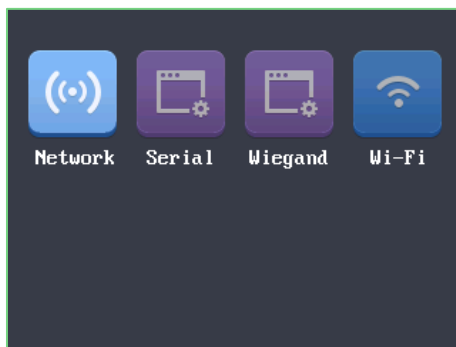


Figure 6-13 Communication Settings Interface

Network Settings: It refers to network parameters of the device, including IP address, subnet mask, and gateway address.

Serial Port Settings: When the access control terminal works as a RS-485 card reader, serial port parameters include working mode, Baud Rate, and RS-485 address.

Wiegand Settings: When the access control terminal works as a Wiegand card reader, Wiegand parameters involve the Wiegand direction, and the Wiegand mode.

Wi-Fi: You can enable the Wi-Fi function.

6.2.1 Network Settings

Purpose:

On the network settings interface, you can set network parameters of the device.

Steps:

1. Move the cursor to **Network** (network settings) by using direction keys.
2. Tap the # key to enter the network settings interface.

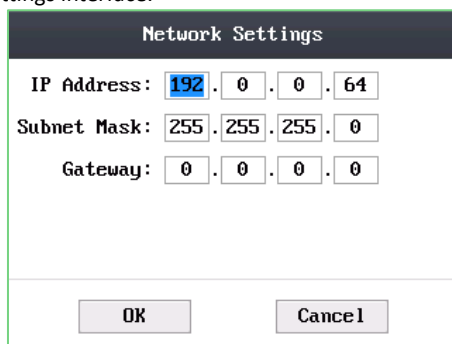


Figure 6-14 Network Settings Interface

3. Modify network parameters of the device, including IP address, subnet mask, and gateway address.

Note: Tap the ↵ key to enter/exit the editing mode.

4. Move the cursor to the **OK** button, and tap the # key.

6.2.2 Serial Port Settings

Purpose:

When the access control terminal works as the RS-485 card reader, you should set serial port parameters.

Steps:

1. Move the cursor to **Serial** (serial port settings) by using direction keys on the communication settings interface.
2. Tap the # key to enter the serial port settings interface.

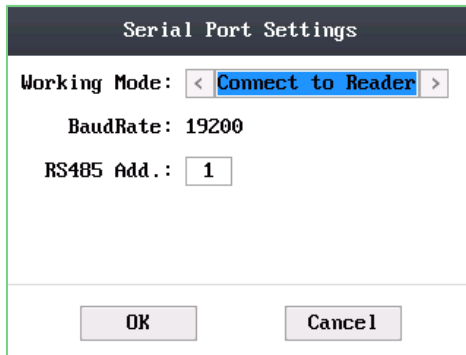


Figure 6-15 Serial Port Settings Interface

3. Modify parameters of the serial port, including working mode, Baud Rate, and RS-485 address.

Working Mode: When the access control terminal works as the terminal, you can connect it to Card Reader, Client Software and Control Unit.

Notes:

- Set the working mode of the serial port as **Connect to Card Reader** if the access control terminal is connected to the external card reader.
- If the terminal is worked as the card reader, Working Mode cannot be used.

Baud Rate: It will display the Baud Rate configured on the client software.

RS-485 Address: When the access control terminal works as a card reader, the RS-485 address should be configured.

Notes:

- Tap the $\leftarrow \rightarrow$ key to enter and exit the editing mode.
- Tap the Right/Left direction keys to choose contents.
- Tap the # key to switch the mode between “Yes” mode and “No” mode.

4. Move the cursor to the **OK** button, and tap the # key.

Note: Reboot the device after changing the working mode.

6.2.3 Wiegand Settings

Purpose:

When the access control terminal works as the Wiegand card reader, you should set Wiegand parameters.

Steps:

1. Move the cursor to **Wiegand** (Wiegand settings) by using direction keys on the communication settings interface.
2. Tap the # key to enter the Wiegand settings interface.



Figure 6-16 Wiegand Settings Interface

3. Edit parameters of the serial port, including the Wiegand direction, and the Wiegand mode.

Wiegand Direction:

- 1) In the terminal mode, select whether to **Receive** or to **Send**. In the **Receive** mode, the mode cannot be changed.
- 2) In the card reader mode, only **Send** is supported.

Wiegand Mode: The default Wiegand mode is Wigand 34.

Notes:

- Tap the $\leftarrow \rightarrow$ key to enter and exit the editing mode.
- Tap the Right/Left direction keys to choose contents.
- Tap the # key to switch the mode between “Yes” mode and “No” mode.

4. Move the cursor to the **OK** button, and tap the # key.
Note: Reboot the device after changing the Direction.

6.2.4 Wi-Fi Settings

Steps:

1. Move the cursor to **Wi-Fi** (Wi-Fi settings) by using direction keys on the communication settings interface.
2. Tap the # key to enter the Wi-Fi settings interface.



Figure 6-17 Wi-Fi Enabling

3. Move the cursor to and tap the # key to enable the WLAN.

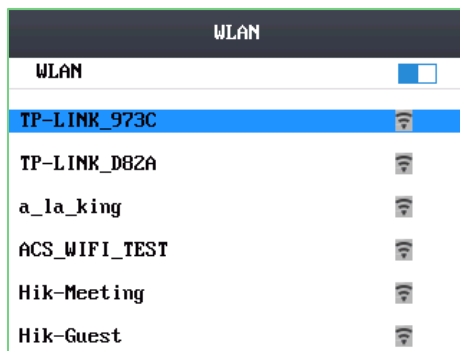


Figure 6-18 Wi-Fi Selection

4. Move the cursor to a network, and tap # key to enter the network connection interface.

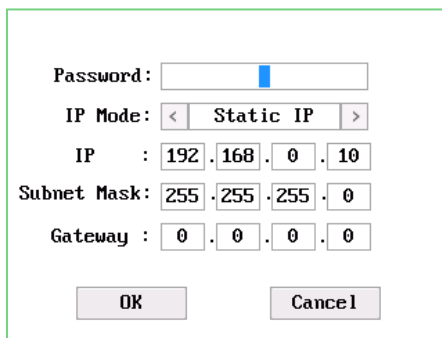


Figure 6-19 Wi-Fi Settings

5. Enter the password of the network. The password supports numbers, letters (uppercase and lowercase) and symbols.
6. Edit the IP mode, IP address, subnet mask, and gateway address.
7. Move the cursor to the **OK** button, and tap the # key.

Note: Tap the  key to enter and exit the editing mode.

6.3 System Settings

Purpose:

On the system settings interface, you can set system parameters, manage the data, restore default settings, set access control parameters, and set cameras.

Steps:

1. Move the cursor to **System** (system parameters) by using direction keys.
2. Tap the # key to enter the system parameters interface.

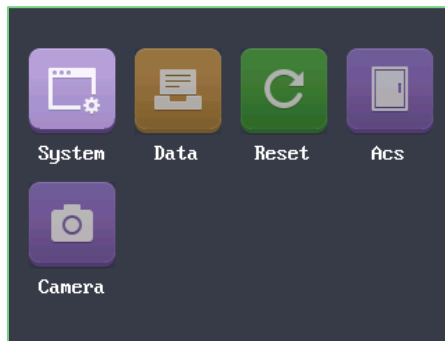


Figure 6-20 System Settings Interface

System Parameters: System parameters of the device include the device running mode, login password, and prompt sound.

Data Management: It is used to manage the storage data of the device, including Delete Card Parameters, Delete Event Only, and Delete Picture Only.

Restore Settings: The device can be restored into factory defaults or default settings.

Access Control Settings: You can set parameters of the access control terminal, including Controller Authentication, Card Reader Authentication, Door Action Time, Delayed Door Alarm, and Anti-passing Back.

Camera Settings: You can set the camera for the access control terminal (only supported by terminal with the model of -C).

Note: Camera Settings is will be displayed on the screen when the access control terminal has the function.

6.3.1 Setting System

Steps:

1. Move the cursor to **System** (system parameters) by using direction keys on the system settings interface.
2. Tap the # key to enter the system parameters interface.

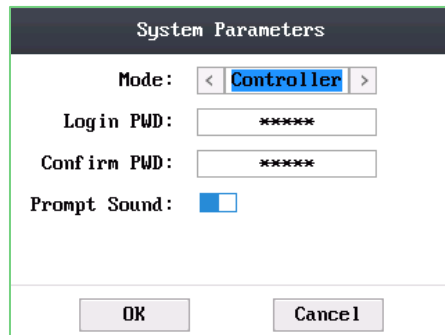


Figure 6-21 System Parameters Interface

3. Modify system parameters, including switching the mode, entering the login password, and enabling voice prompts.

Mode: The device mode can be switched between **Controller** and **Card Reader**. After switching the mode, the system can automatically reboot and enter into the interface of the new mode.

Notes:

- If the access control terminal works as a card reader, you should configure the serial port setting and the Wiegand setting. See details in *Chapter 6.2.2*.
- If the access control terminal is in the card reader mode, the terminal works as a card reader to access to the access controller or another access control terminal via RS-485 and Wiegand.
- If the access control terminal is in the card reader mode, the terminal will send the fingerprint via RS-485, the client software and the local.
- If the access control terminal is in the card reader mode, the terminal supports swiping card and scanning fingerprint. When scan the fingerprint, the bound card No. should contain 10 numbers. Or the fingerprint scanning will be failed.

Login Password: To reset the login password of the device, you should enter a new password, and confirm it.

Voice Prompts: After enabling voice prompts, you can hear the voice prompts to notify you the card status when you swipe the card. Otherwise, you will hear the beeper in place of the voice prompts.

- Beep three times: legal card.
- Beep four times: illegal card.

Notes:

- Tap the $\leftarrow \rightarrow$ key to enter and exit the editing mode.
 - Tap the Right/Left direction keys to choose contents.
 - Tap the # key to switch the mode between “Yes” mode and “No” mode.
4. Move the cursor to the **OK** button, and tap the # key.

6.3.2 Managing Data**Purpose:**

On the data management interface, you can delete the storage data of the device.

Steps:

1. Move the cursor to **Data** (data management) by using direction keys in the system settings Interface.
2. Tap the # key to enter the data management interface.

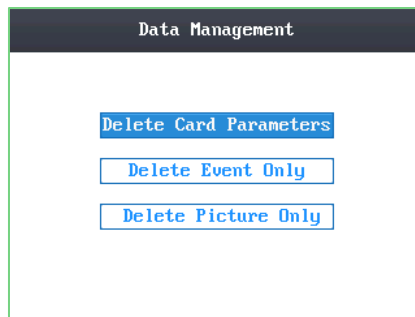


Figure 6-22 Data Management Interface

3. Move the cursor to Delete Card Parameters, Delete Event Only, or Delete Picture Only.
 - Delete Card Parameters:** Delete all cards parameters registered in the device.
 - Delete Event Only:** Delete all access events in the system.
 - Delete Picture Only:** Delete all captured pictures in the system.

Note: This function is only supported by terminal with the model of –C.

4. Tap the # key.

6.3.3 Restoring Settings**Purpose:**

On the restore settings interface, you can restore Factory Defaults or Default Settings.

Steps:

1. Move the cursor to **Reset** (restore settings) by using direction keys on the system settings interface.
2. Tap the # key to enter the restore settings interface.

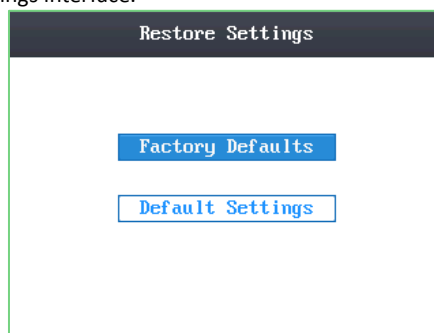


Figure 6-23 Restore Settings Interface

3. Move the cursor to Factory Defaults or Default Settings.
 - Factory Defaults:** After restoring factory defaults, all parameters of the device are returned to the factory defaults.
 - Default Settings:** After restoring default settings, parameters, excluding network parameters and event parameters, are returned to the factory defaults.
4. Tap the # key.
5. Move the cursor to the **OK** button, and tap the # key.

6.3.4 Door Settings

Purpose:

On the door settings interface, you can set door parameters, including Controller Authentication, Card Reader Authentication, Door Action Time, Delayed Door Alarm, and Anti-passing Back.

Steps:

1. Move the cursor to **ACS**(door settings) by using direction keys in the system settings interface.
2. Tap the # key to enter the door settings interface.

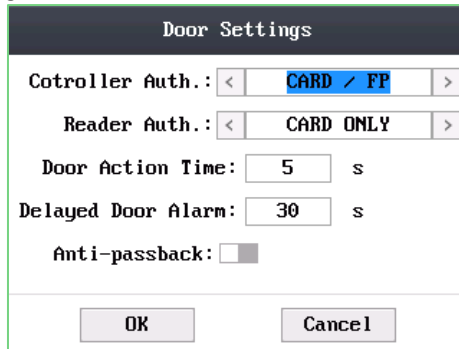


Figure 6-24 Door Settings Interface

3. Edit door parameters.

Controller Authentication: Set the controller authentication mode for opening the door, that is, Card Only, Fingerprint Only, Card/Fingerprint, Card & Fingerprint, Card & Password, Fingerprint & Password, Card & Fingerprint & Password.

Card Reader Authentication: Set the card reader authentication mode for opening the door, that is, Card Only, Fingerprint Only, Card/Fingerprint, Card & Fingerprint, Card & Password, Password & Fingerprint, Card & Password & Fingerprint.

Door Action Time: Set the door action time: 1 ~ 255 s.

Delayed Door Alarm: Set the delayed door alarm threshold: 1 ~ 255 s.

Anti-Passing Back: Set whether to enable the function of anti-passing back.

Notes:

- Tap the ↵ key to enter and exit the editing mode.
 - Tap the Right/Left direction keys to choose contents.
 - Tap the # key to switch the mode between “Yes” mode and “No” mode.
4. Move the cursor to the **OK** button, and tap the # key.

6.3.5 Setting the Camera

Purpose:

On the camera settings interface, you can set camera parameters.

Note: This function is only supported by terminal with the model of -C.

Steps:

1. Move the cursor to **Camera** (camera settings) by using direction keys in the system settings Interface.
2. Tap the # key to enter the camera settings interface.

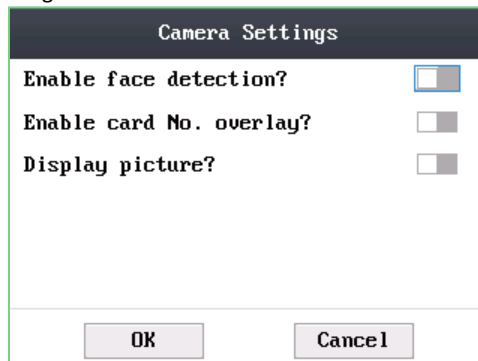


Figure 6-25 Camera Settings Interface

3. Edit camera parameters.

Enable Face Detection: When enabling face detection, the system can detect the face.

Enable Card No. Overlay: When enabling card No. overlay, captured pictures can be overlaid on the card information.

Display Picture: When enabling to display the picture, captured pictures can display on the screen.

Notes:

- Tap the $\leftarrow \rightarrow$ key to enter and exit the editing mode.
 - Tap the Right/Left direction keys to choose contents.
 - Tap the # key to switch the mode between “Yes” mode and “No” mode.
 - The captured pictures can be saved in the SD card.
4. Move the cursor to the **OK** button, and tap the # key.

6.4 Time Settings

Steps:

1. Move the cursor to **Time** (time settings) by using direction keys.
2. Tap the # key to enter the time settings interface.

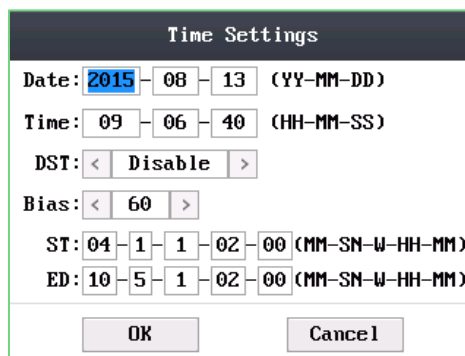


Figure 6-26 Time Settings Interface

3. Edit time parameters.

Date/Time: Edit the data and the time of the device.

DST (Daylight Saving Time): When enabling DST, you should set the bias time, the start time, and the end time of DST.

Notes:

- Tap the $\leftarrow \rightarrow$ key to enter and exit the editing mode.
 - Tap the Right/Left direction keys to choose contents.
 - Tap the # key to switch the mode between “Yes” mode and “No” mode.
4. Move the cursor to the **OK** button, and tap the # key.

6.5 Upload/Download Settings

Purpose:

On the upload/download interface, you can upgrade the device, upload the door parameters, download access parameters, download captured pictures, and download attendance record.

Steps:

1. Plug a USB disk into the access control terminal.
2. Move the cursor to **Transfer** (upload/download) by using direction keys.
3. Tap the # key to enter the upload/download interface.

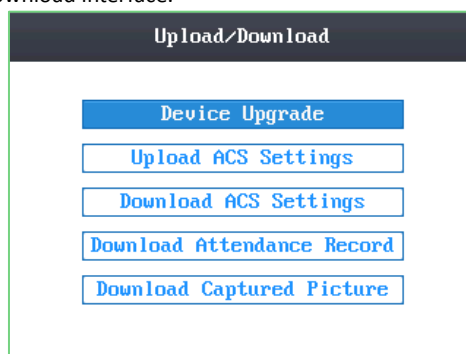


Figure 6-27 Upload/Download Interface

4. Move the cursor to Device Upgrade, Upload Access Settings, Download Access Settings, Download Attendance Record, or Download Captured Picture.
 - Device Upgrade:** The system can automatically read the upgrading information from the USB, and upgrade the device.
 - Note:** The upgrading file should be put in the root directory.
 - Upload Access Settings:** The system can automatically read the access parameters from the USB, and upload them to the device.
 - Download Access Settings:** The system can automatically download access parameters into the USB.
 - Download Attendance Record:** The system can automatically download attendance records into the USB.
 - Download Captured Picture:** The system can automatically download captured pictures into the USB. Click the # key.
 - Note:** The supported USB format is FAT32 and NTFS.

6.6 Testing

Purpose:

On the test interface, you can do voice test, keypad test, RTC test, and camera test.

Steps:

1. Move the cursor to **Test** by using direction keys.
2. Tap the # key to enter the test interface.

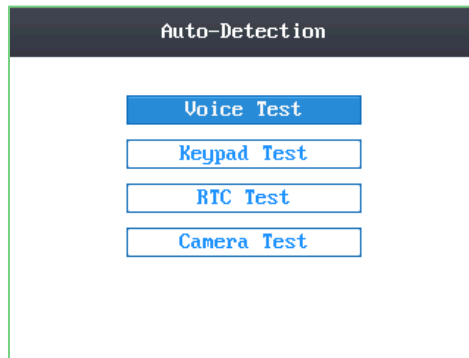


Figure 6-28 Test Interface

3. Move the cursor to select Voice Test, Keypad Test, RTC Test, or Camera Test to do corresponding test.
 - Voice Test:** You can hear a voice prompt “Voice prompt succeeds” after click the # key.
 - Keypad Test:** On the keypad test interface, if the keypad test succeeds, the screen will display corresponding numbers or functions of the keypad you click.
 - RTC Test:** On the RTC test interface, if the test succeeds, the screen will display the synchronization time.
 - Camera Test:** On the camera test, if the camera test succeeds, the screen will display the real-time picture the camera captures.
- Note:** This function is only supported by terminal with the model of –C.

6.7 Log Query Settings




Steps:

1. Move the cursor to **Log** (log query settings) by using direction keys.
2. Tap the # key to enter the log query interface.



Figure 6-29 Log Query Interface

3. Enter the card number.

- Enter the card number by swiping the card.
Place the card close to the screen.
 - Enter the card number manually.
- 1) Tap the  key to enter the text editing mode.
 - 2) Enter the card number in the textbox.
 - 3) Tap the  key to exit the text editing mode.
4. Set the start/end time.
Tap the  key to enter and exit the editing mode.
5. Move the cursor to the **OK** button, and tap the # key.

Note: On the log query display interface, you can view the card number, swiping time, and card reader ID.

6.8 System Information

Steps:

1. Move the cursor to **Info** (system information) by using direction keys.
2. Tap the # key to enter the system information interface.

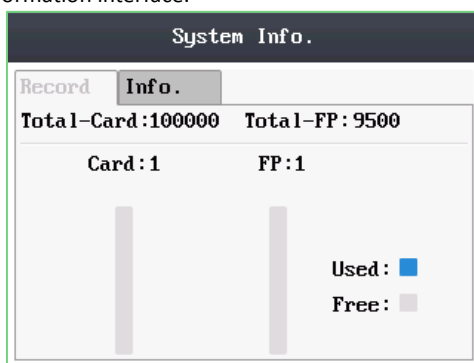


Figure 6-30 System Information Interface

3. Move the cursor to **Record Capacity** or **Information** by using Left/Right direction keys.

- **Record Capacity**

Card Capacity: It refers to the maximum amount of cards.

The default maximum card amount is 100,000.

Fingerprint Capacity: It refers to the maximum amount of fingerprints.

Note:

- Fingerprint capacity only supports devices with fingerprint registration function.
- The default maximum fingerprint amounts of devices with fingerprint registering function are as follows.
- Optical device: 9500
- DS-K1T105 series model does not support this function.

- **Device Information**

In the device information interface, you can view the device name, the serial No., Mac address, and so on.



Figure 6-31 Device Information Interface

7 Client Operation

7.1 Overview of Access Control System

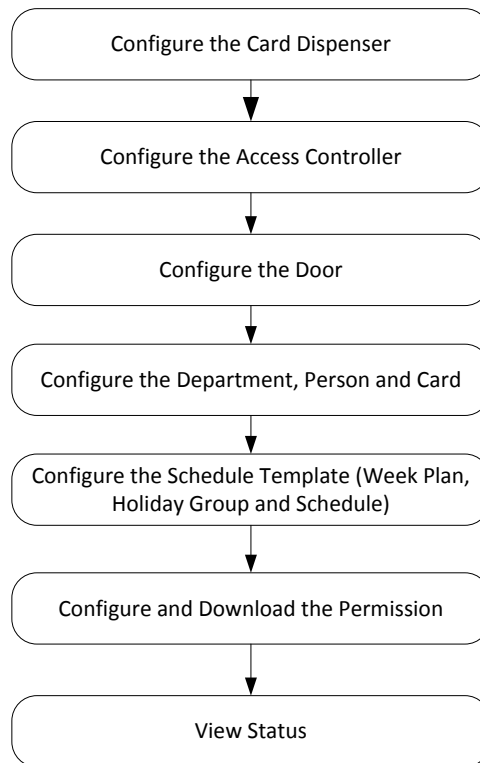
7.1.1 Description

The access control system is a system of configuring permission of door access. It provides multiple functionalities, including access controller management, people/card management, permission configuration, door status management, event search, etc.

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

7.1.2 Configuration Flow

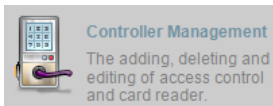
Refer to the following flow chart for the configuration order.



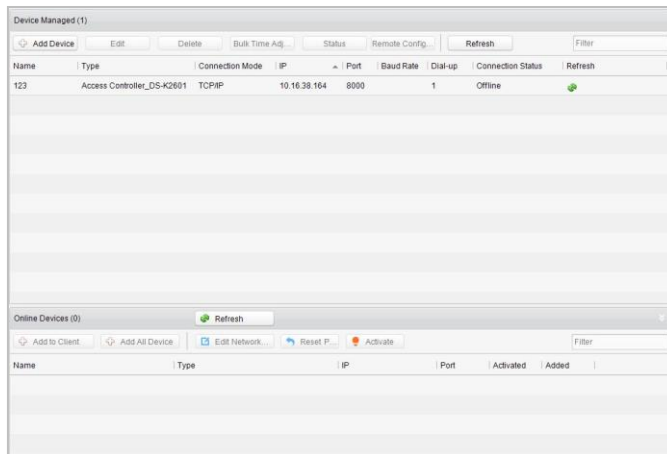
7.2 Device Management

7.2.1 Controller Management

Interface Introduction



Click the icon to enter the controller management interface.



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

Device Management:

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

Online Device Detection:

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

Note: The control client can manage 100 access controllers at most.

Device Management

Adding Controller

Steps:

1. Click the to enter the add access controller interface.

add the access controller ✕

Name:

Type:

Connection Method:

Address:

Port:


Baud Rate:

Dial-up:

Account:

User Name:

Password:

2. Input the device name.
3. Select the access controller type in the dropdown list.
4. Select the connection mode in the dropdown list: TCP/IP, or COM port, or Ehome.
 TCP/IP: Connect the device via the network.
 Ehome: Connect the device via the Ehome protocol.
5. Set the parameters of connecting the device.
 If you choose to connect the device via network, you should input the IP address and port No. of the device, and set the Dial-up value to 1.
 If you choose to connect the device via Ehome protocol, you should input an account.
 For the detailed information about the account, refer to 15.1.3.
6. Click the  button to finish adding.

You can click Status to check the detailed status of the controller, and click Remote Configuration to configure the settings of the controller.

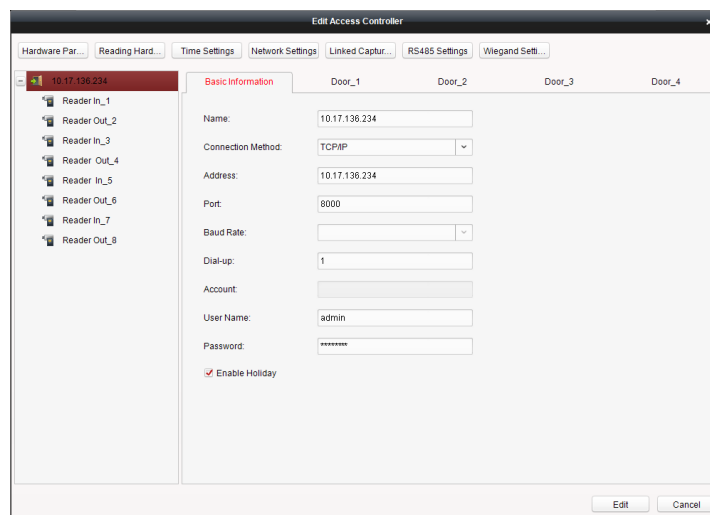
Editing Device (Basic Information)

Purpose:

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

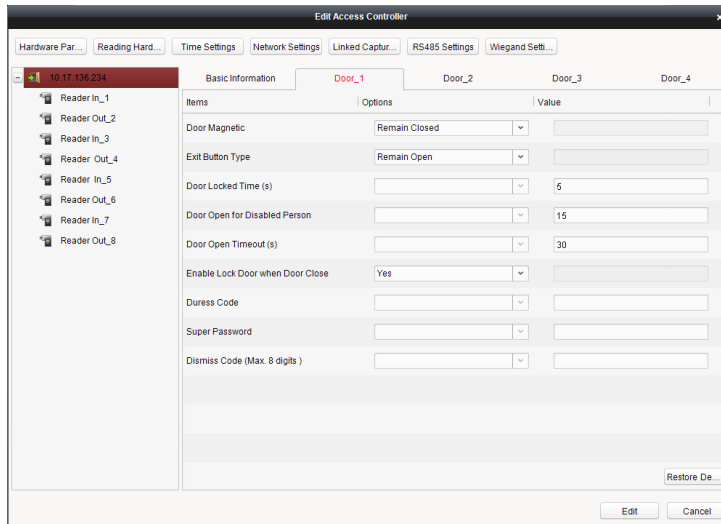
Steps:

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



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

Editing Device (Door Information)



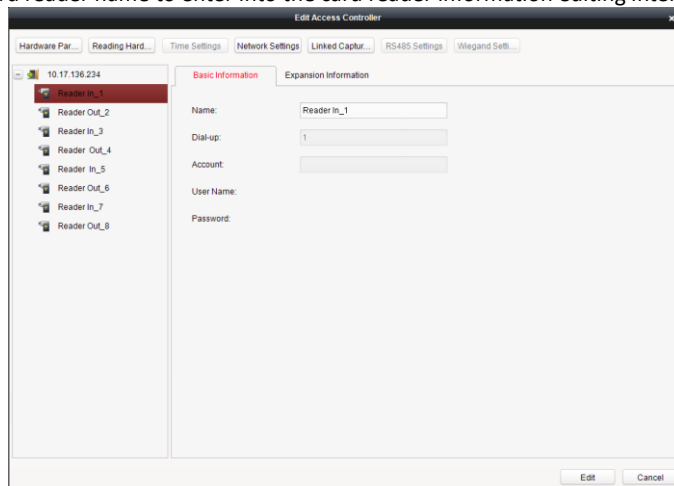
Steps:

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

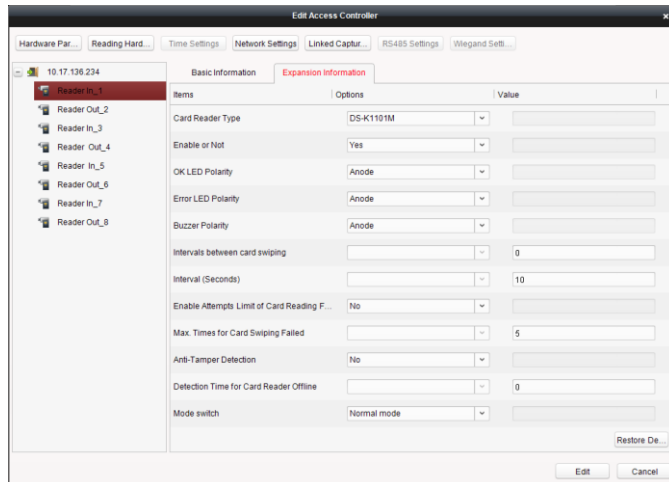
Editing Device (Card Reader Information)

Steps:

1. In the device list, select a card reader name to enter into the card reader information editing interface.




2. Click the Basic Information button to edit the basic information about the card reader.
3. Click the Expansion Information button to edit the expansion information about the card reader.

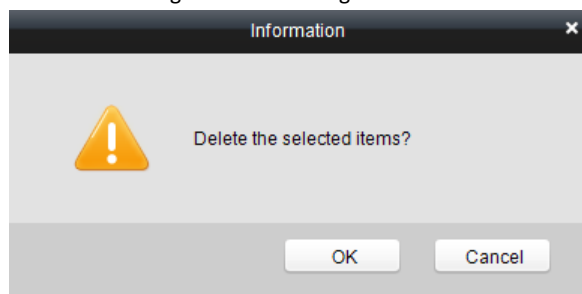


4. Click the Edit button to save parameters.
5. Click the Hardware Parameters Downloading button to download the updated parameters to the local memory of the device.

Deleting Device

Steps:

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



Bulk Time synchronization

Steps:

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

Status

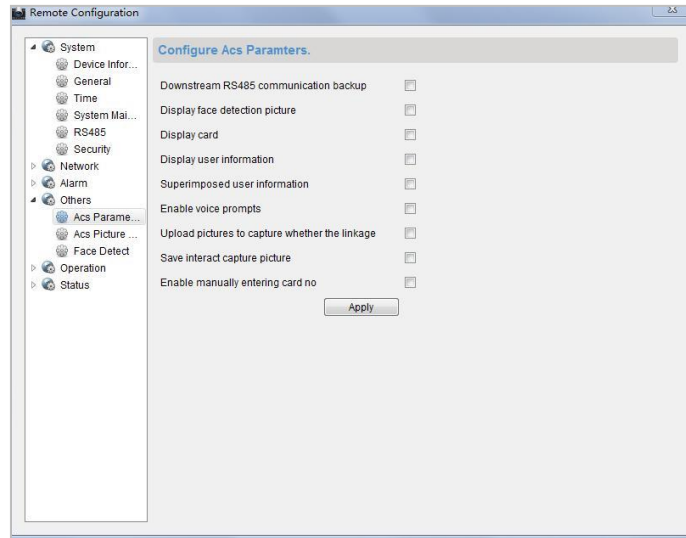
In the device list, you can click Status button to enter view the status.

Steps:

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

Remote Configuration

In the device list, you can click Remote Configuration button to enter the remote configuration interface. On this this interface, you can set the access parameters, enable the face detection function, and so on.

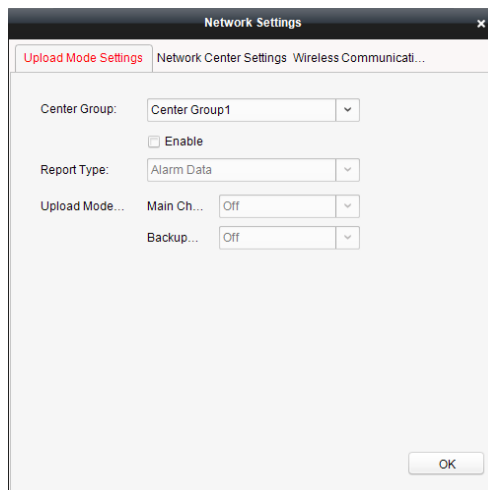


Network Settings

Purpose:

In the network settings interface, the network settings of the device can be uploaded and reported.

Uploading Mode Settings



Steps:

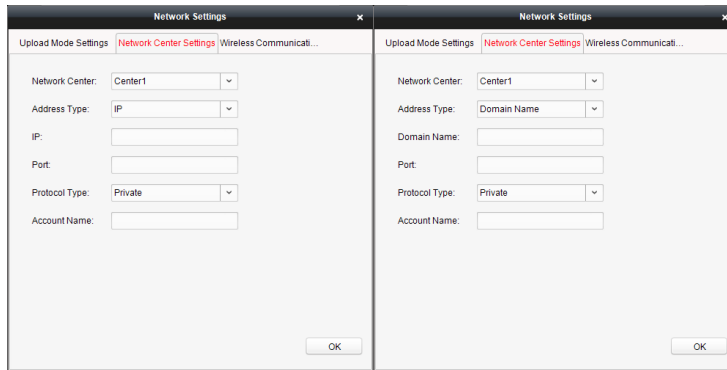
1. In the access controller editing interface, click Network Settings button to enter the network settings interface.
2. Click the Uploading Mode Settings button.
3. Select the center group in the dropdown list.
4. Tick the Enable to enable the selected center group.
5. Select the report type in the dropdown list.
6. Select the uploading mode in the dropdown list. You can enable N1/G1 for the main channel and the backup channel, or select off 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.

7. Click the OK button to save parameters.

Network Center Settings



Steps:

1. In the access controller editing interface, click Network Settings button to enter the network settings interface.
2. Click the Network Center Settings button.
3. Select the network center in the dropdown list.
4. Select the address type in the dropdown list: IP, or Domain Name.
IP: Input the IP address, and port No..
Domain Name: Input the domain name, and port No..
5. Select the protocol type: Ehome.
6. Set an account name for the network center. A consistent account should be used in one platform.
7. Click the OK button to save parameters.

Notes:

- In the Ehome protocol, the default port number is 7661, and the port type should be UDP port. Related settings files need modifying if the port type does not match.
- The port No. of the wireless network and wired network should be consistent with the port No. of Ehome.

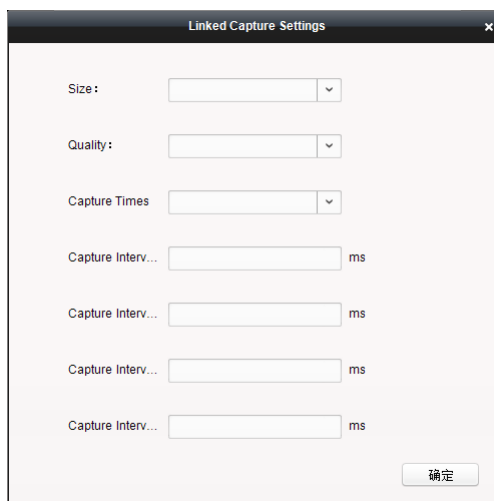
Setting Linked Capture

Purpose:

You can set the linked capture parameters including the picture size, quality, capture times and capture interval.

Steps:

1. In the Edit Access Controller interface, click the **Linked Capture Settings** button to enter the Linked Capture Settings interface.
2. Select the captured picture size, quality and times in the dropdown list.
3. Enter the captured interval.
4. Click **OK** to save the settings.



Note: It is available to get the linked capture parameters from the device.

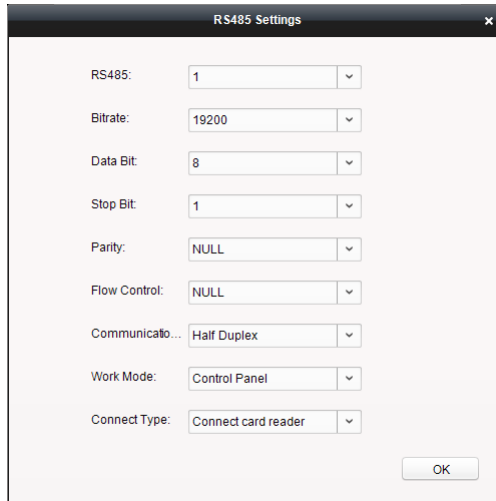
Setting RS-485

Purpose:

You can set the RS-485 parameters including the RS-485 channel, the bitrate, the data bit, the stop bit, the parity, the flow control, the communication mode, the work mode and the connect type.

Steps:

1. In the Edit Access Controller interface, click the **RS-485 Settings** button to enter the RS-485 Settings interface.
2. Select the RS-485 channel, the bitrate, the data bit, the stop bit, the parity, the flow control, the communication mode, the work mode and the connect type in the dropdown list.
3. Click **OK** to save the settings.



Note: The device need to reboot if the connect type has changed.

Setting Wiegand

Purpose:

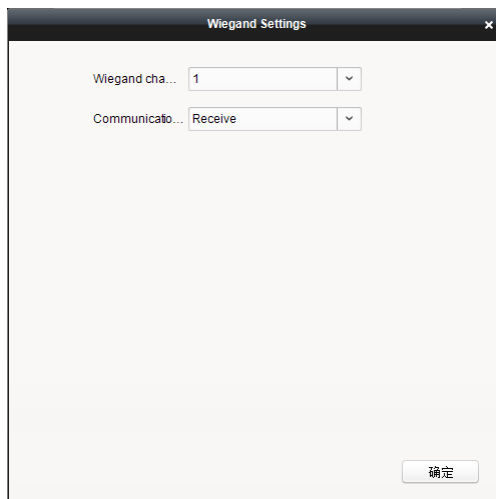
You can set the Wiegand channel and the communication mode.

Steps:

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

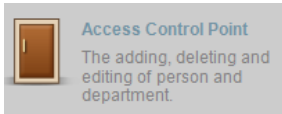
Note:

After changing the communication direction, the device will be rebooted. A prompt will be pop-up after changing the communication direction.

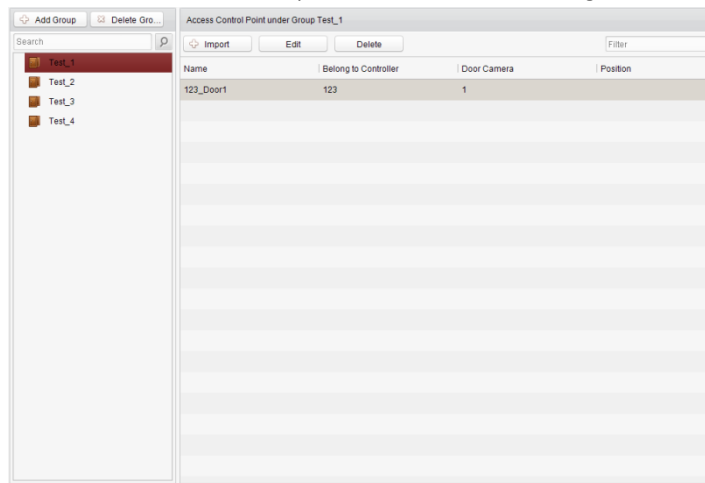


7.2.2 Access Control Point Management

Interface Introduction



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



Group Management

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

Door Management

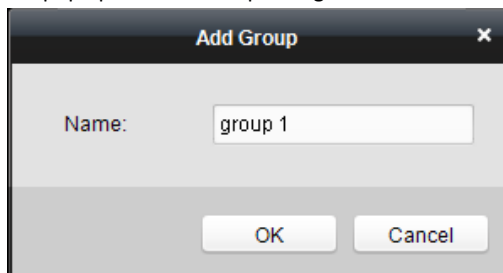
Manage the specific door under the door group, including importing, editing and deleting door.

Group Management

- Adding Group

Steps:

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



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

Note: Multi-level groups are not supported yet.

- Editing Group

Steps:

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

- Deleting Group

To delete a group, three ways are supported.

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

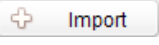


And then click the OK button in the popup window.

Access Control Point Management


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

- **Importing Access Control Point**

Steps:

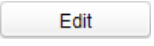
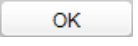
1. Click the  button to pop up the access control point importing interface.
2. Select an access control point to import by clicking it.
3. Click to select a group in the right side bar to import to.
4. Click  button to import the selected access control points or click  to import all the available access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

Notes:

- You can click  button on the upper-right corner of the window to create a new group.
- The control client can manage 100 access control points at most.

- **Editing Access Control Point**




Steps:

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

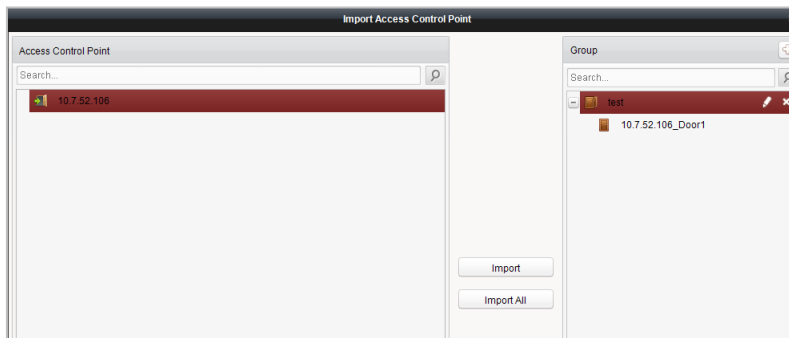
Note: You can also enter the Edit interface by double clicking the door from the list.

- **Deleting Access Control Point**

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

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

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



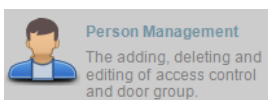
Steps:

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

7.3 Permission Management

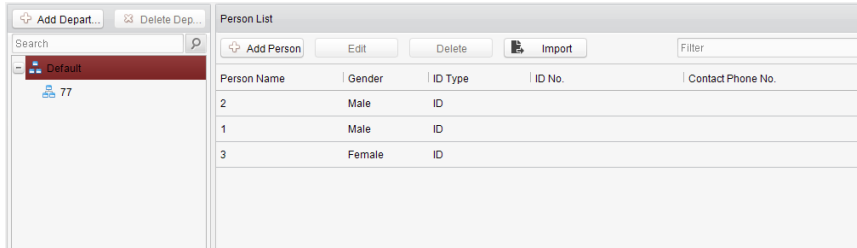
7.3.1 Person Management

Interface Introduction




Click the  icon on the control panel of the software.

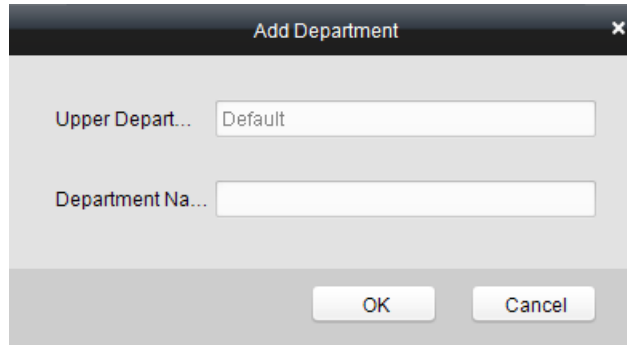
Adding, editing, deleting and filtering of the department and person are supported in this interface.



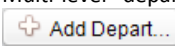
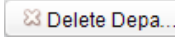
Department Management

Steps:

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



Notes:

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

Notes:

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



Person Management

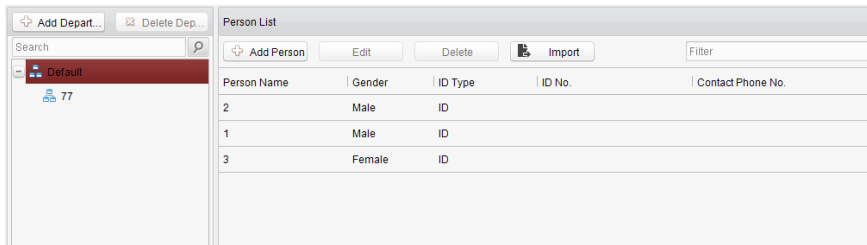
Purpose:

In the person management interface, you can add, delete, edit and import the person information.

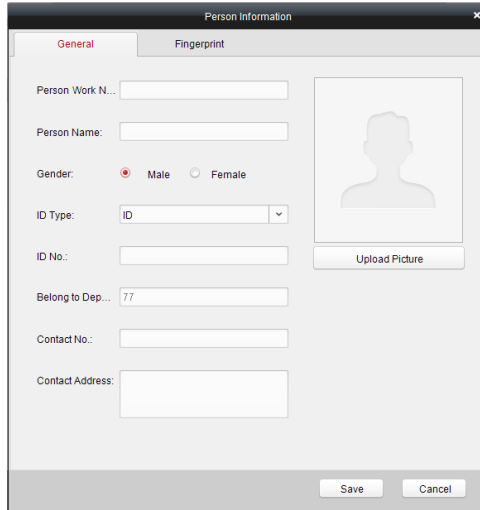
Adding Person

Steps:

1. Select a department in the list and click the  in the person information list to pop up the adding person interface.
2. Input the Person Name (required), Gender, ID Card, etc., upload the photo of the person and click the  icon to finish adding.

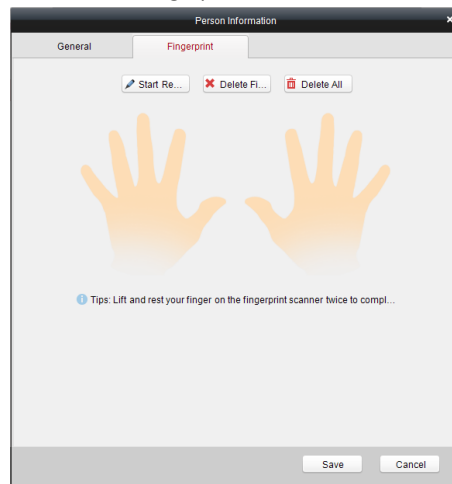


Note: The format of the photo should be .jpg, or .jpeg.



Optionally, you can

- 1) Click **Fingerprint** to enter the fingerprint adding interface.
 - 2) Click the **Start Register** button, and select the fingerprint to scan.
 - 3) Click the **Save** button to save the parameter.
- Or click the **Delete Fingerprint** button to delete the scanned fingerprint.
Or click the **Delete All** button to clear all scanned fingerprints.




Note:

Up to 2000 persons can be added.

Deleting Person

Steps:

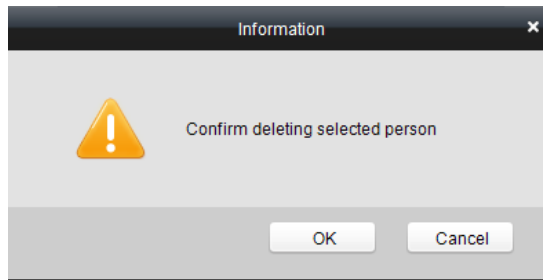
1. In the Person Management interface, select a person in the person list.
Or press the **Ctrl** key and select multiple persons.
2. Click the  **Delete** button to delete the select person(s).

Person Name	Gender	ID Type	ID No.	Contact Phone No.
2	Male	ID		
1	Male	ID		
3	Female	ID		
1110	Male	ID		
1111	Male	ID		
1112	Male	ID		

3. Click **OK** in the pop-up window to delete.

Note:

The card information associated with the person will also be deleted.

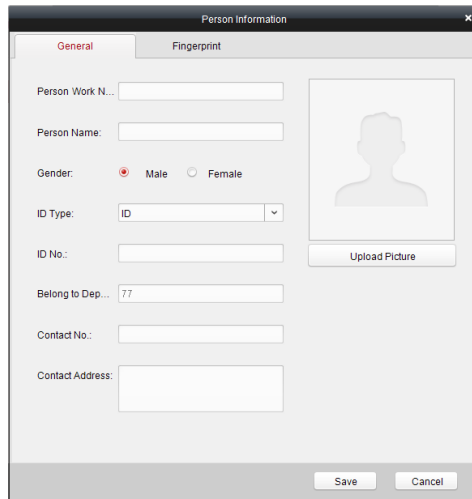


Editing Person

Steps:

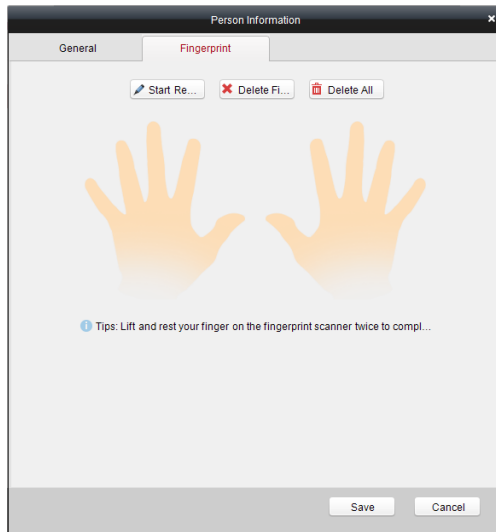
1. Double-click the person name in the person list.
Or select a person in the person list and click the **Edit** button to enter the edit interface.
3. Editing the Person Name (required), Gender, ID Card, etc., upload the photo of the person and click the **Save** icon to finish editing.

Note: The format of the photo should be .jpg, or .jpeg.



Or

- 4) Click **Fingerprint** to enter the fingerprint adding interface.
- 5) Click the **Start Register** button, and select the fingerprint to scan.
- 6) Click the **Save** button to save the parameter.
Or click the **Delete Fingerprint** button to delete the scanned fingerprint.
Or click the **Delete All** button to clear all scanned fingerprints.



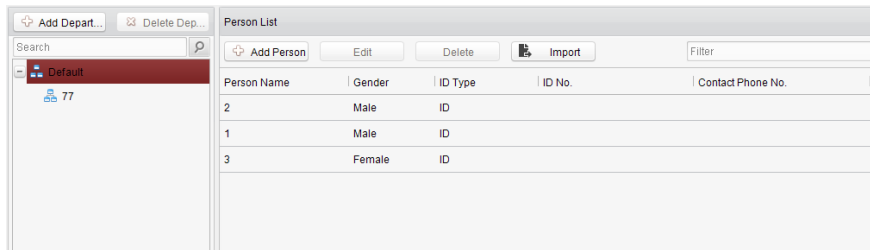
Importing Person

Purpose:

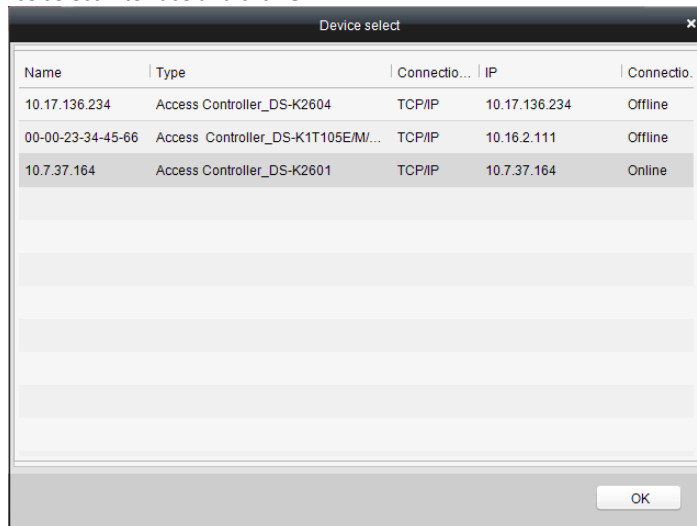
Import the person information in the device to the client software.


Steps:

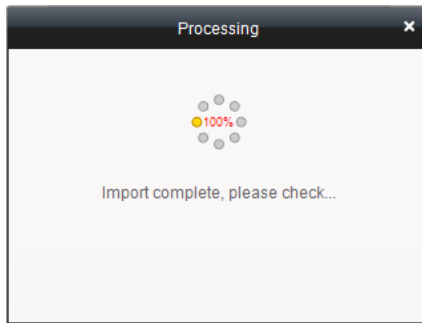
1. In the Person Management interface, select a department.
2. Click **Import**.



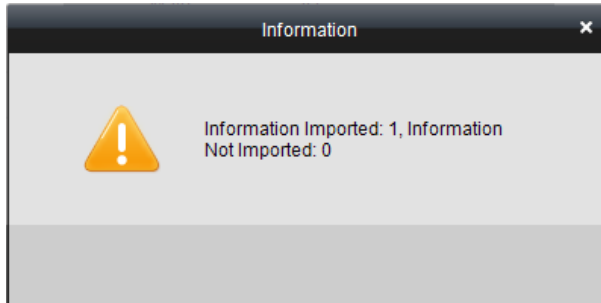
3. Select a device in the device select interface and click **OK**.



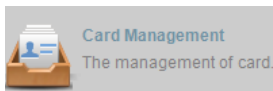
4. Click the  button when the import is completed.



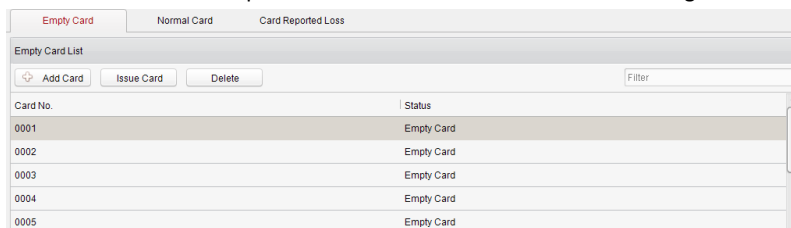
- Click the button again to complete importing. The person information will be added in the person list.



7.3.2 Card Management Interface Introduction



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



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

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

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

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

Blank Card

- Adding Card

Before you start:

Make sure a card dispenser is connected to the PC and is configured already. Refer to Section 0 Card Dispenser Configuration for details.

Steps:

- Click the **Add Card** button to add cards.
- Two modes of adding cards are supported.

Adding Single Card

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

Batch Adding Cards

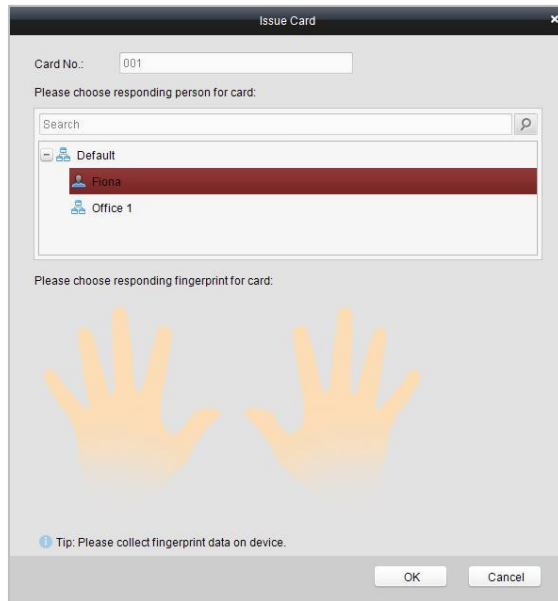
Choose the Bulking Adding as the adding mode by clicking the to and input the activation date, expiry date, start card No. and last card No. in the corresponding text fields.

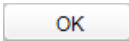
Note:

The start card No. and the last card No. should be in the same length. E.g., the last card No. is 234, then the start card No. should be like 028.

3. Click the button to finish adding.
4. Click an added blank card in the list and click button to issue the card with a person.

Note: You can double click the blank card in the card list to enter the Issue Card Page.



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

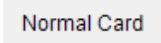
Notes:

- The issued card will disappear from the Blank Card list, you can check the card information in the Normal Card list.
- Up to 2000 cards can be added.
- The fingerprint associated functions are only supported by device with fingerprint recognition module.

Deleting Card

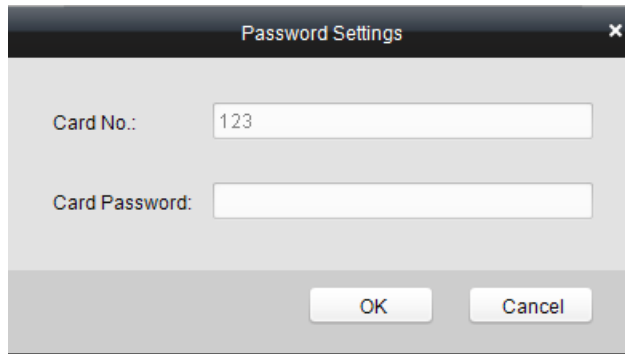
You can click an added blank card in the list and click  button to delete the selected card.

Normal Card

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

Card No.	Status	Card Holder Name	Department
0001	Normal Card	Lela	Market Department
0002	Normal Card	Olivia	Market Department
0003	Normal Card	Shanna	Market Department
0004	Normal Card	Sam	Market Department
0005	Normal Card	Lemon	Market Department

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



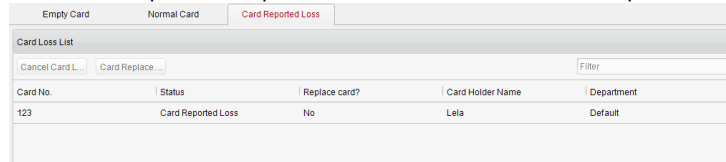
Note:

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

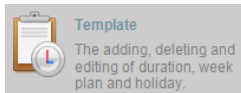
Lost Card

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

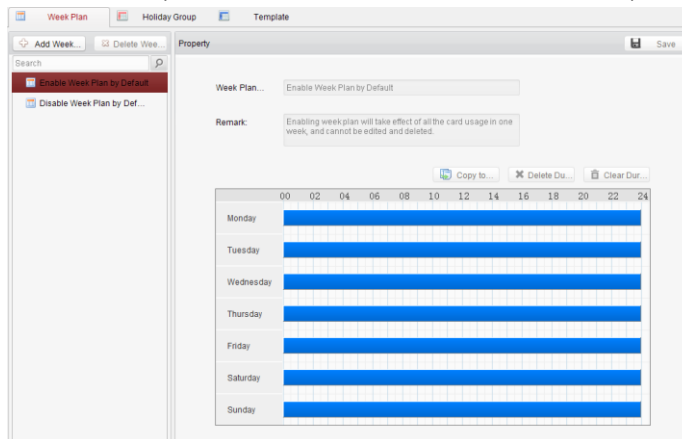
- Click the Cancel Card Loss button to resume the card to the normal card.
- Click the Card Replacement button to issue a new card to the card holder replacing for the lost card. Select another card in the popup window as the new card and the predefined permissions of the lost card will be copied to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



7.3.3 Schedule Template Interface Introduction



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



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

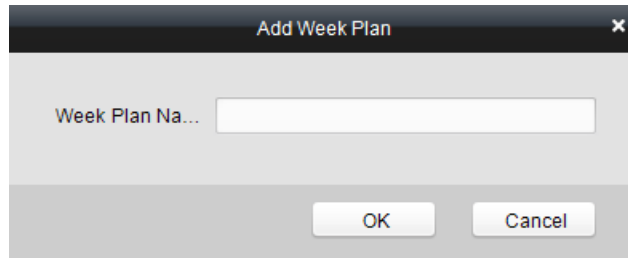
Setting Week Plan

● **Adding Week Plan**

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

Steps:

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



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

● **Deleting Week Plan**

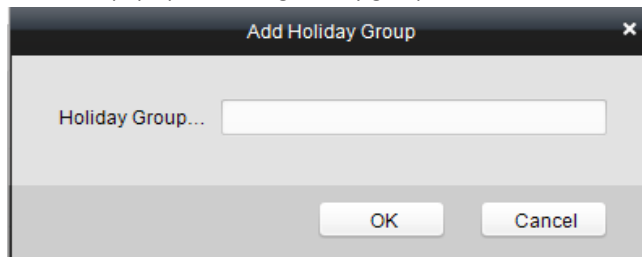
- ◆ Click to select a configured duration and click the Delete Duration button to delete it.
- ◆ Click the Clear Duration button to clear all the configured durations, while the week plan still exists.
- ◆ Click the Delete Week Plan button to delete the week plan directly.

Setting Holiday Group

- Adding Holiday Group

Steps:

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




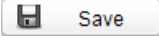


2. Input the name of holiday group in the text filed, and click the button to add the holiday group.
3. Click the icon to add a holiday in the holiday list and configure the duration of the holiday.

Note: At most 16 holiday periods can be added.

Holiday list					<input type="button" value="+ Add holiday"/>	<input type="button" value="Previous"/>	<input type="button" value="Next"/>
Serial...	Start Time	End Time	Duration	Opera...			
1	2014-10-28	2014-10-29	00 02 04 06 08 10 12 14 16 18 20 22 24 				
2	2014-10-30	2014-11-01	00 02 04 06 08 10 12 14 16 18 20 22 24 				
3	2014-11-05	2014-11-08	00 02 04 06 08 10 12 14 16 18 20 22 24 				
4	2014-11-10	2014-11-12	00 02 04 06 08 10 12 14 16 18 20 22 24 				

- 1) Click and drag your mouse on a day to draw a blue bar on the schedule, which means in that duration, the configured permission is activated.

- 2) Click to select a configured duration and click the  to delete it.
 - 3) Click the  to clear all the configured durations, while the holiday still exists.
 - 4) Click the  to delete the holiday directly.
4. Click the  button to save the settings.

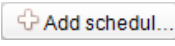
Note: The holidays cannot be overlapped with each other.

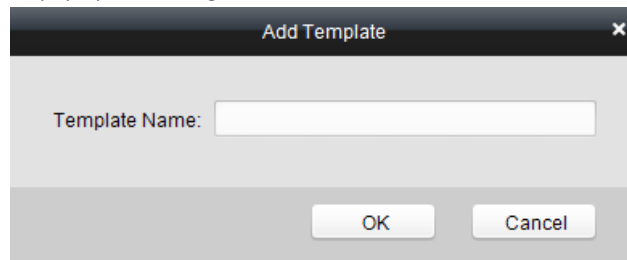
Setting Schedule Template

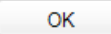
The schedule consists of week plan and holiday group; you can only choose which plan and group to enable in the schedule template configuration interface. Configure the week plan and holiday group before configuring the schedule template.

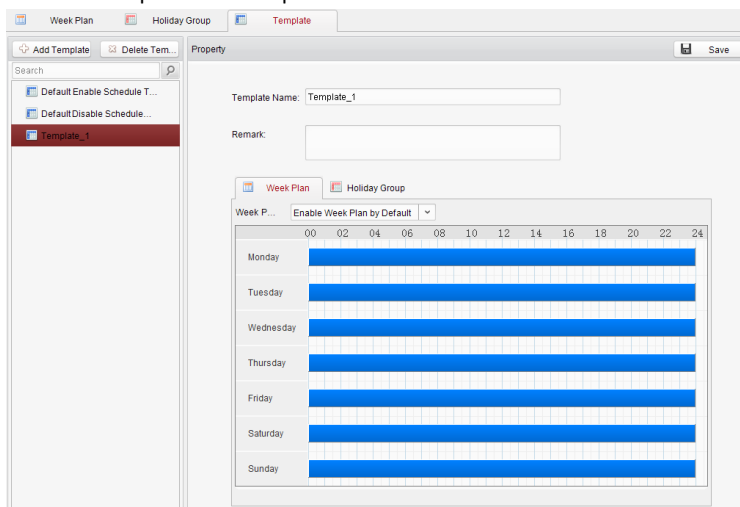
Note: The priority of holiday group schedule is higher than the week plan.

Steps:

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

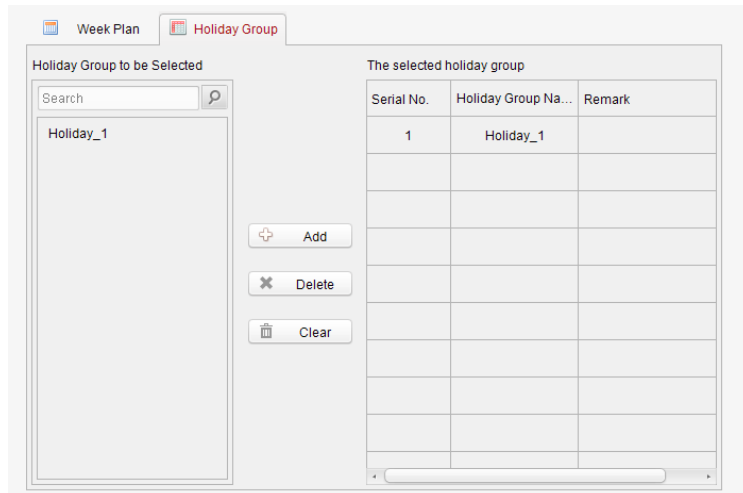


2. Input the name of schedule in the text field, and click the  button to add the schedule.
3. Select a week plan you want to apply to the schedule.
Click the Week Plan tab and select a plan in the dropdown list.



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

Note: At most 4 holiday groups can be added.

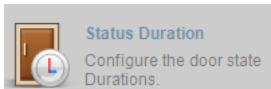


- Click to select a holiday group in the left-side list and click the **Add** to add it.
 - Click to select an added holiday group in the right-side list and click the **Delete** to delete it.
 - Click the **Clear** to delete all the added holiday groups.
5. Click the **Save** button to save the settings.

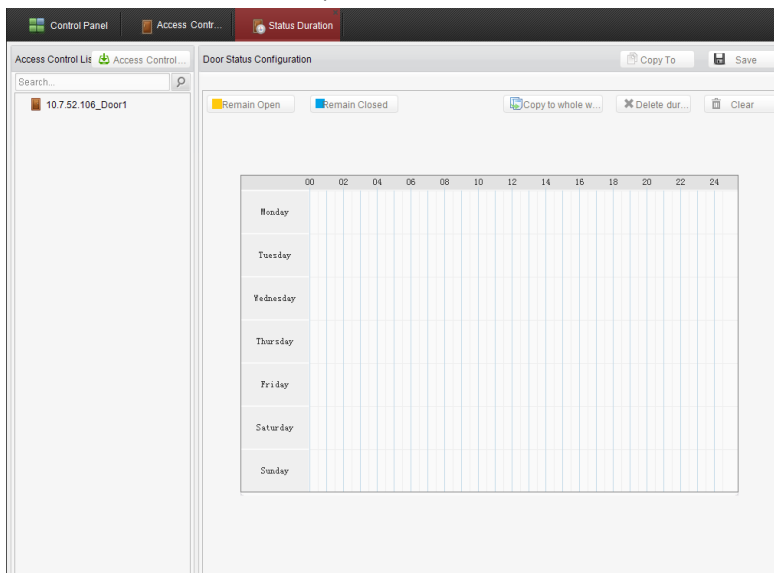
7.3.4 Door Status Management

Purpose:

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



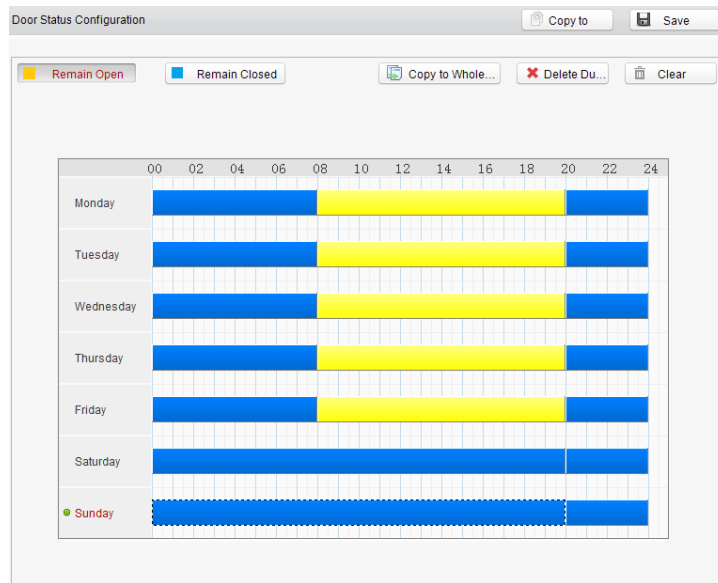
Click the icon on the control panel to enter the interface.



Steps:

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

- 2) Click and drag the mouse to draw a color bar on the schedule map to set the duration.



Notes:

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

Steps:

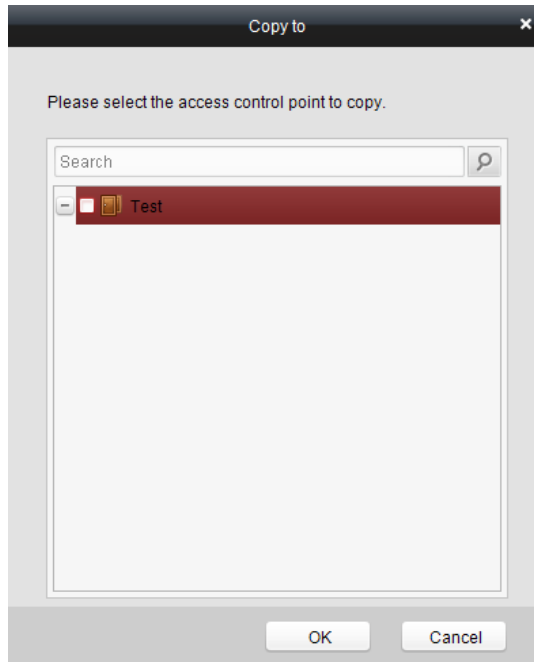
1. Select a day which has already been configured.
2. Click on to copy the time periods to the whole week.


4. Edit the schedule map.

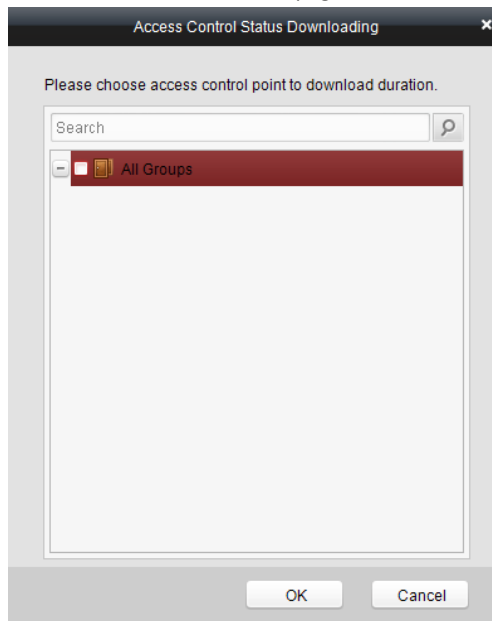
- Edit Duration:
Click and drag the color bar on the schedule map and you can move the bar on the time track.
Click and drag the mouse on the ends of the color bar and you can adjust the length of the bar.
- Delete a Duration:
Click and select a color bar and click to delete the time period.
- Clear All Durations:
Click to clear all configured durations on the schedule map.

5. Click on to save the settings.

6. You can copy the schedule to other doors by clicking on and select the required doors.

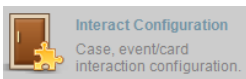



7. Click on  Access Control... to enter the Download Door State page.

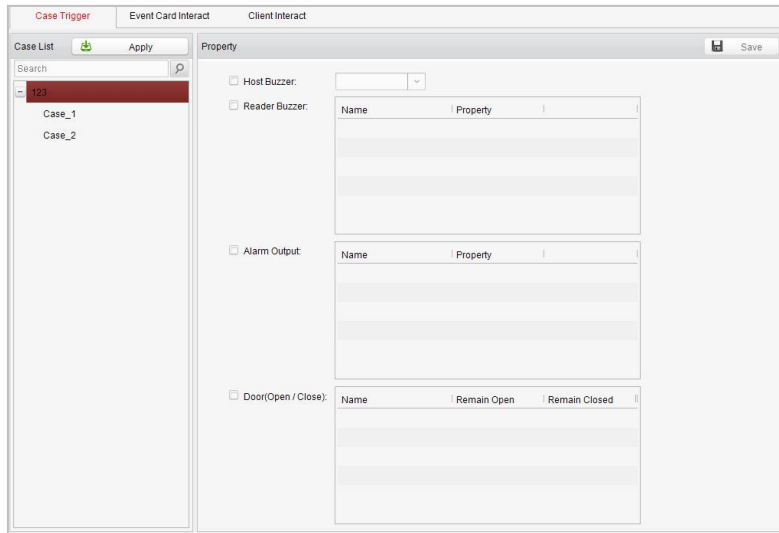


8. Select a control point and click OK to download the settings to the system.

7.3.5 Interact Configuration



Click  on the control panel of the software to enter the interact configuration interface.




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

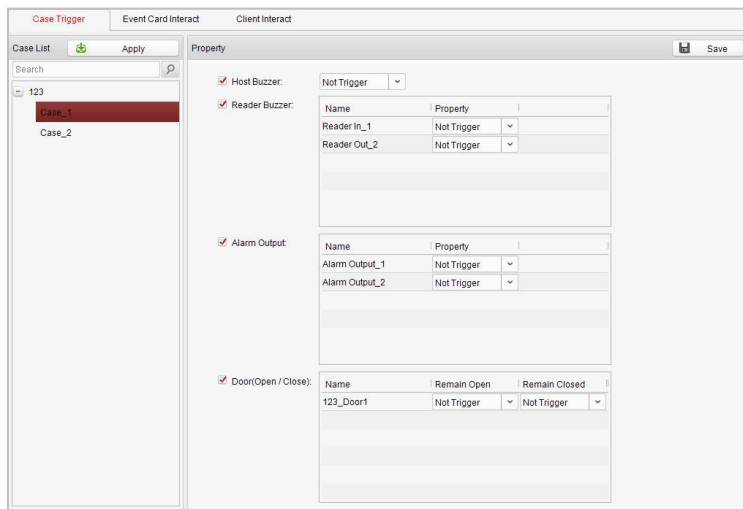
Case Trigger

Purpose:

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

Steps:

1. Click the  button to enter the case trigger interface, and select a case.



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

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

Event Card Interact

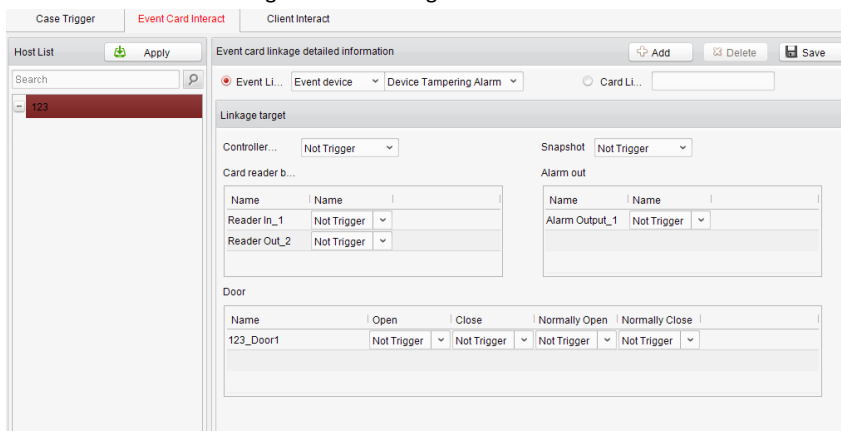
In the Interact Configuration interface, click the Event Card Interact button to enter the settings interface.

● **Event Linkage**

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

Steps:

1. Click the **Event Card Interact** button to enter the event card interface
2. Select the host to be set from the host list.
3. Click the **+ Add** button to start setting the event linkage.



4. Click the radio button of the event linkage, and select the event type from the dropdown list.
5. Set the linkage target, and set the property as Trigger to enable this function.
 Host Buzzer: The audible warning of controller will be triggered.
 Snapshot: The real-time capture will be triggered.
 Reader Buzzer: The audible warning of card reader will be triggered.
 Alarm Output: The alarm output will be triggered for notification.
 Door: The door status of open, close, normally open, and normally close will be triggered.
6. Click the **Save** button to save parameters.
7. Click the **Apply** button to download the updated parameters to the local memory of the device.

Note:

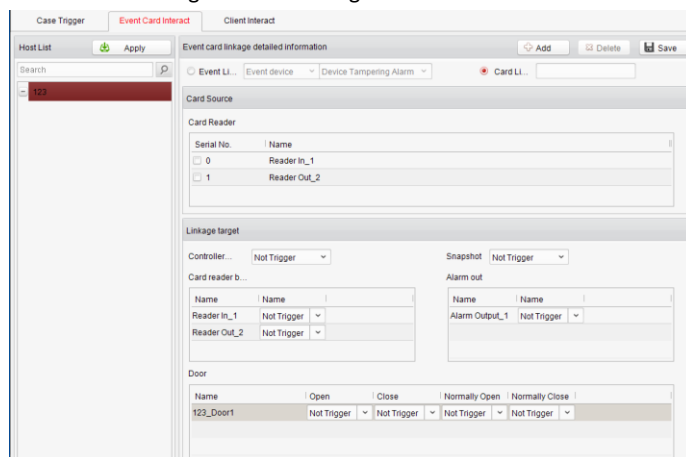
The door status of open, close, normally open, and normally close cannot be triggered at the same time.

● **Card Linkage**

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

Steps:

1. Click the **Event Card Interact** button to enter the event card interface
2. Select the host to be set from the host list.
3. Click the **+ Add** button to start setting the event linkage.

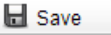


4. Click the radio button of card linkage, and input the card number.
5. Select the event source, and check the checkbox of the card reader's serial number.
6. Set the linkage target, and set the property as Trigger to enable this function.
 Controller Buzzer: The audible warning of controller will be triggered.
 Snapshot: The real-time capture will be triggered.

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

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

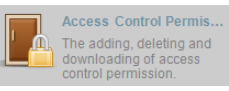
Door: The door status of open, close, normally open, and normally close will be triggered.

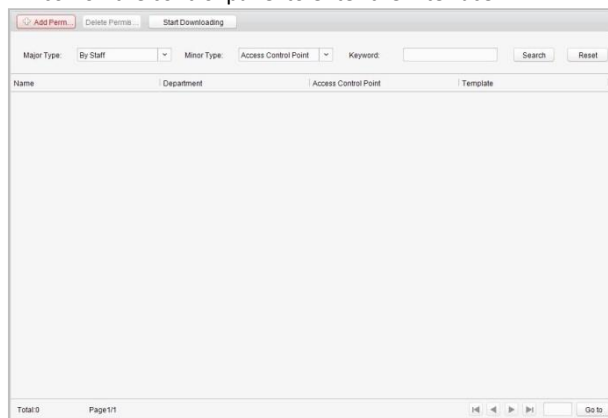
7. Click the  Save button to save parameters.
8. Click the Apply button to download the updated parameters to the local memory of the device.

Note:

The door status of open, close, normally open, and normally close cannot be triggered at the same time.

7.3.6 Access Permission Configuration

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

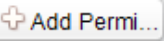


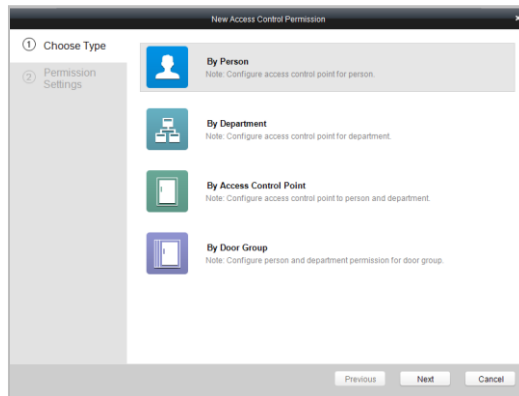
Access Permission Settings

Purpose:

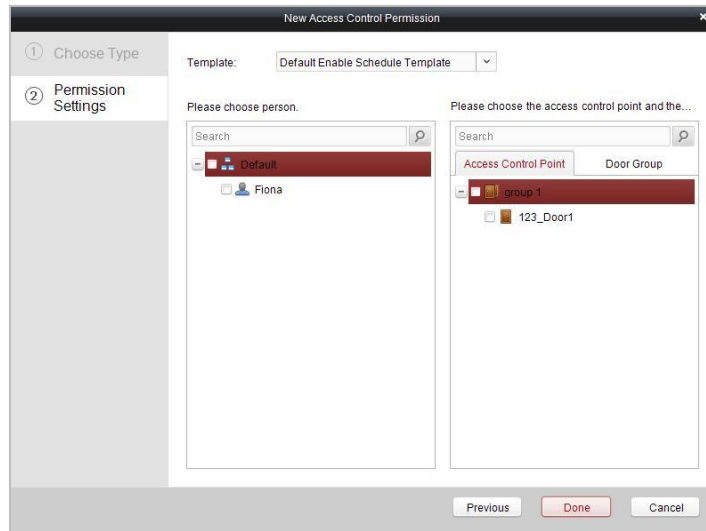
You can allocate permission for people/department to enter/exist the control points (doors) in this section.

Steps:

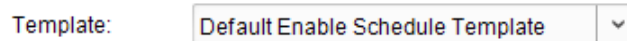
1. Enter the Permission page.
2. Click on  icon on the upper-left side of the page to enter the Add Permission page.



3. Select an adding type in the Select Type interface.
 - By Person: you can select people from the list to enter/exit the door.
 - By Department: You can select departments from the list to enter/exit the door. Once the permission is allocated, all the people in this department will have the permission to access the door.
 - By Access Control Point: You can select doors from the door list for people to enter/exit.
 - By Door Group: You can select groups from the door list for people to enter/exit. The permission will take effect on the door in this group.
4. Click Next to enter the Permission Settings interface.



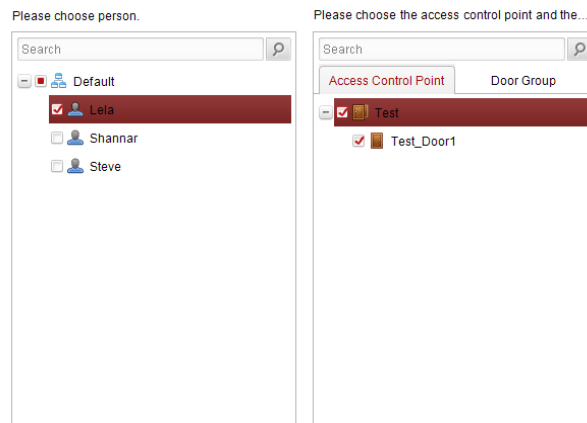
- Click on the dropdown menu to select a schedule template for the permission.



Note:

The schedule template must be configured before any permission settings. Refer to Section 7.3.3 Schedule Template for detailed configuration guide.

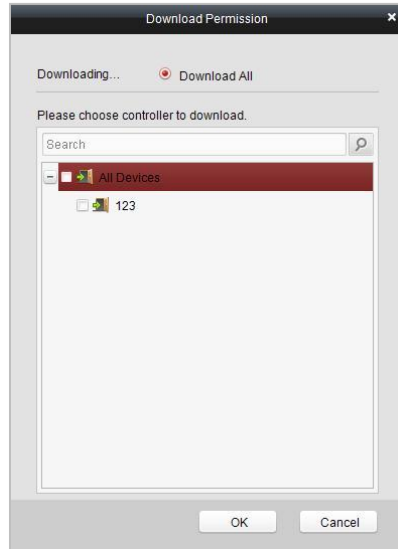
- Select people/ department and corresponding doors/door groups from the appropriate lists.



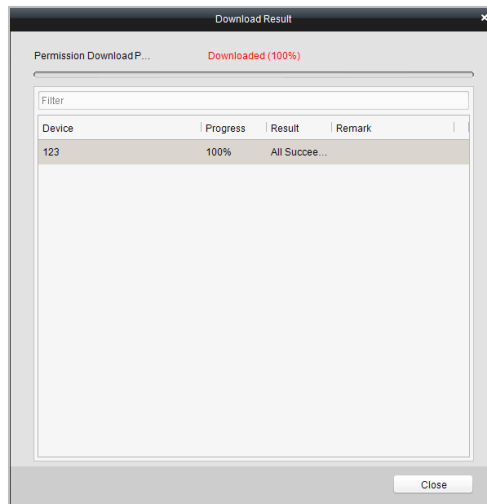
Note:

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

- Click the Done button to complete the permission adding.
- Click [Start Downloading](#) to enter the Download Permission page.



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



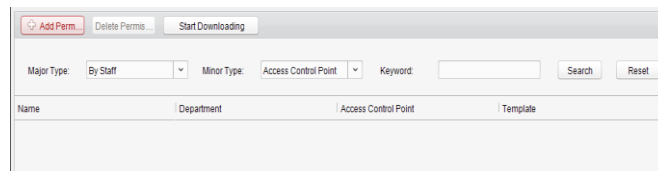
Access Permission Searching

Purpose:

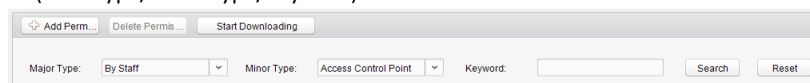
After the permission settings being completed, you can search and view permission assigning condition on the searching interface.

Steps:

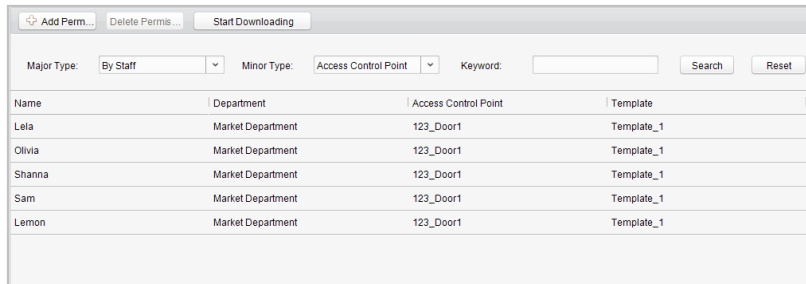
1. Enter the Permission page.



2. Enter the search criteria (main type/minor type/keyword).



3. Click Search to get the search results.



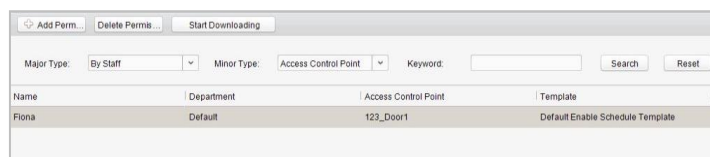
Note:

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

Permission Deleting

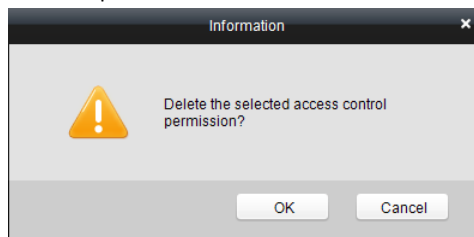
Steps:

1. Follow steps 1-3 in the Permission Searching section to search for the permission needs to be deleted.
2. Select the permission from the results list.

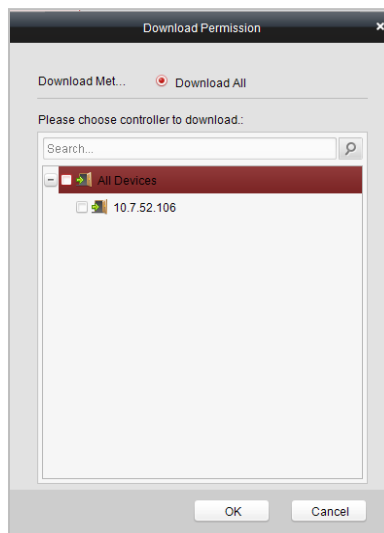


Note: You can press the Ctrl or Shift key on the keyboard,

3. Click the Delete Permission button to delete the permission.



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



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

7.3.7 Attendance Management

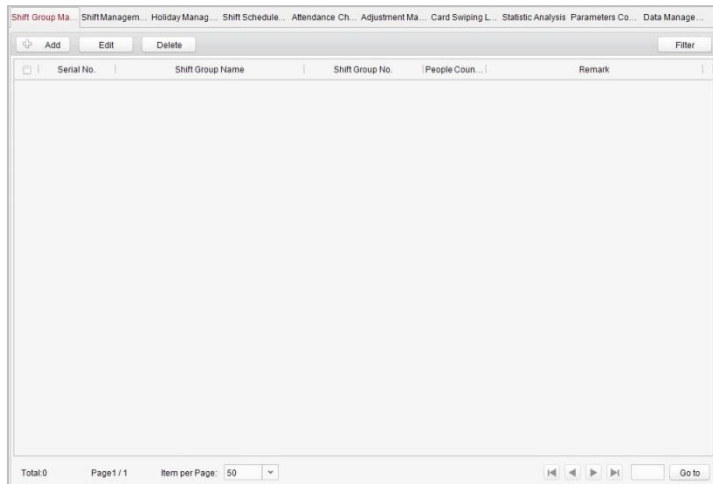
Purpose:

On the attendance management interface, various functions can be implemented such as shift group management, shift management, holiday management, shift schedule, and so on.



Click the

icon on the control panel to enter the interface.



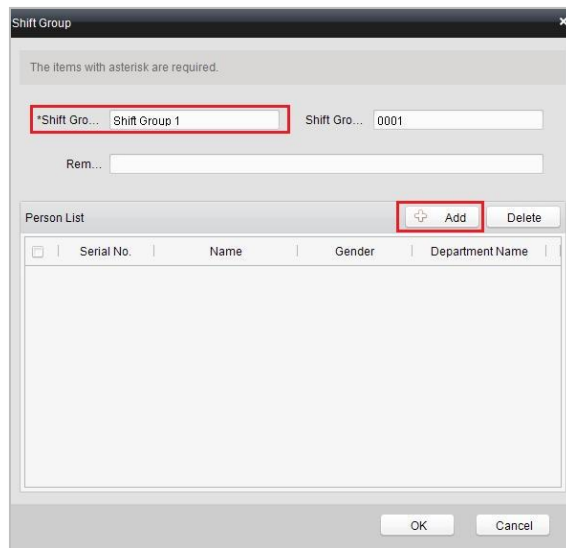
Shift Group Management

Purpose:

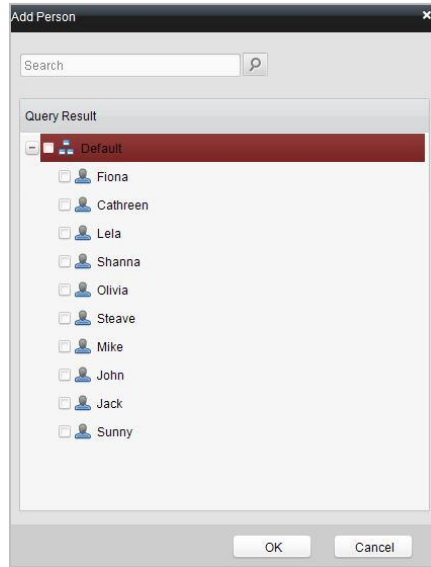
On the shift group management interface, you can add, edit, and delete shift groups for attendance management.

Steps:

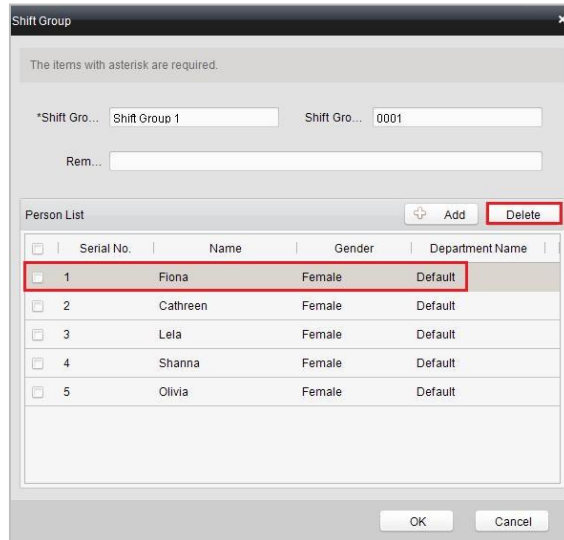
1. Click the  **Add** button to pop up the shift group formation window.



2. Enter the shift group name, and click the  **Add** button on the person list area to pop up the person adding window.



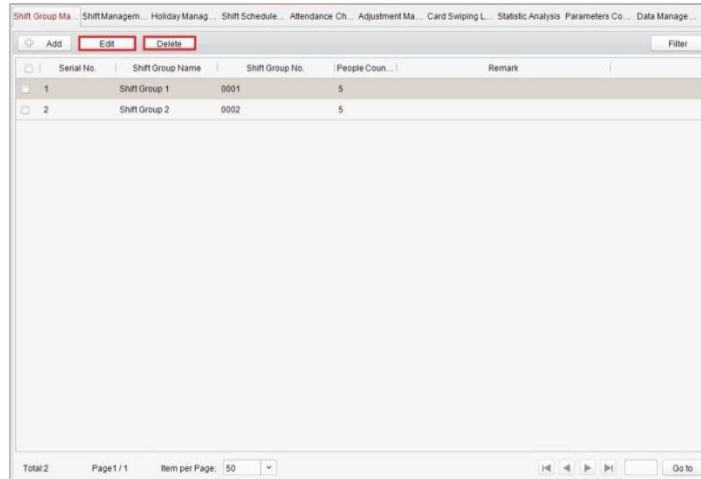
3. Check the checkbox(es) of persons to be added and click the button and return to the shift group settings interface.



Note:

To delete the added person, check the person from the person list, and click the button.

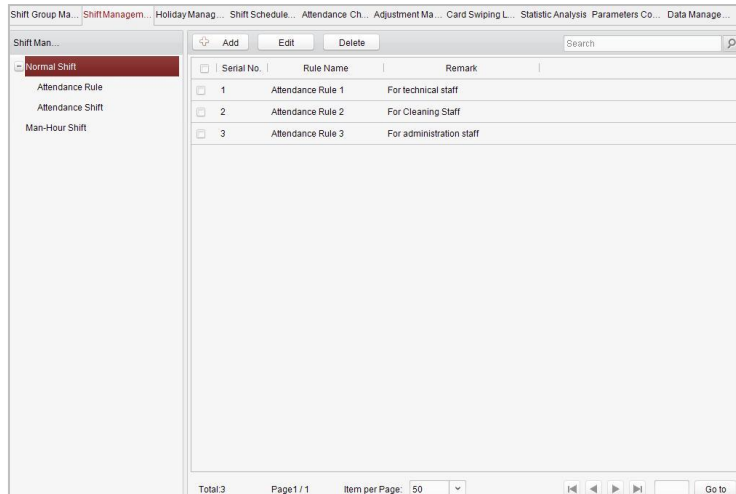
4. Click the button to complete the operation.



Note: You can edit and delete the added shift groups by clicking the **Edit** and **Delete** buttons.

Shift Management

Press the Shift Management tab to enter the shift management interface.



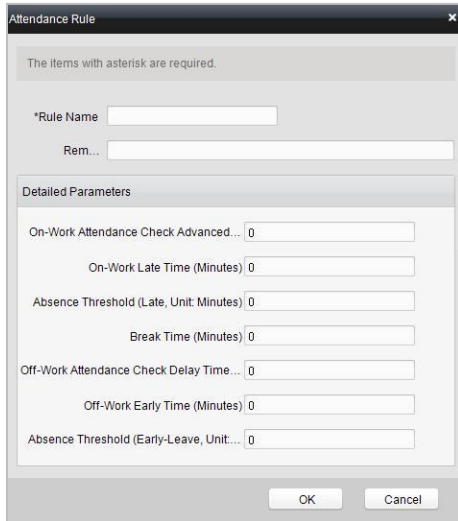
There are two kinds of shifts in this interface: Normal Shift, and Man-Hour Shift.

Normal Shift

- **Setting Attendance Rule**

Steps:

1. Click the **Add** button to pop up the attendance rule setting window.

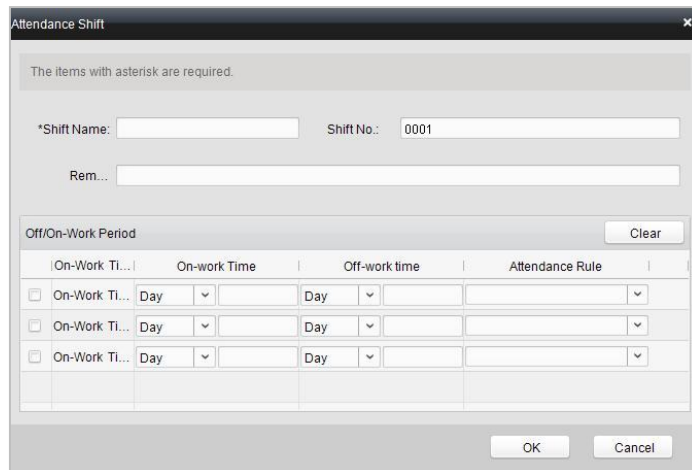


2. Set a rule name.
3. Set detailed parameters for the attendance rule: on-work attendance check advance time, on-work late time, absence threshold, break time, off-work attendance check delay time, off-work early time, and absence threshold (early leave).
4. Click the button to complete the operation.

● **Setting Attendance Shift**

Steps:

1. Click the button to pop up the attendance shift setting window.



2. Set a shift name.
3. Set on-work duration for the shift, and select the attendance rule.
4. Click the button to complete the operation.


Note:

The format of on-work time and off-work time should be 00:00 to 23:59.

● **Setting Man-Hour Shift**

Steps:


1. Click the button to pop up the man-hour shift setting window.

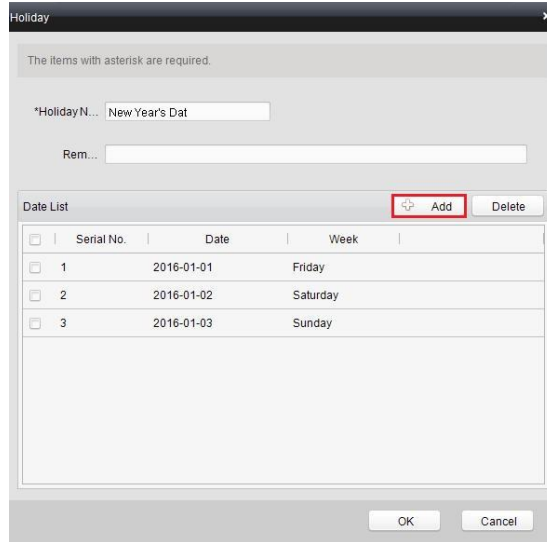
2. Set a shift name, and daily working duration.
3. (Optional) Check the checkbox of latest on-work time, and set the latest on-work time.
4. (Optional) Set the disregard man-hour period.
5. Click the  button to complete the operation.


Holiday Management

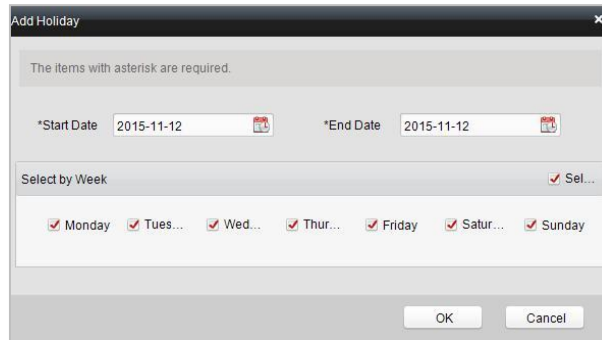
Press the Holiday Management tab to enter the holiday management interface.


Steps:

1. Click the  button to pop up the holiday setting window.



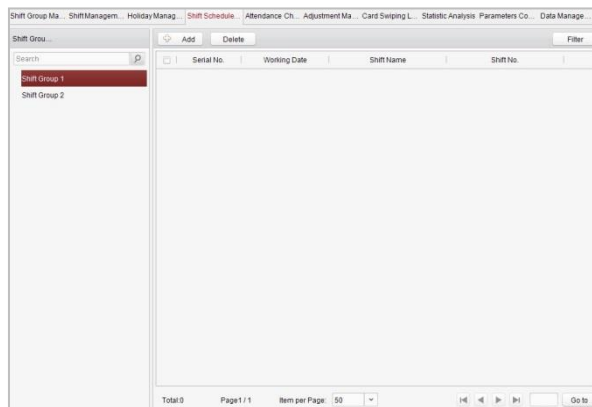
2. Click the  **Add** button to pop-up holiday adding window.




3. Set the start date and end date, select the date of week, and click the  **OK** button.

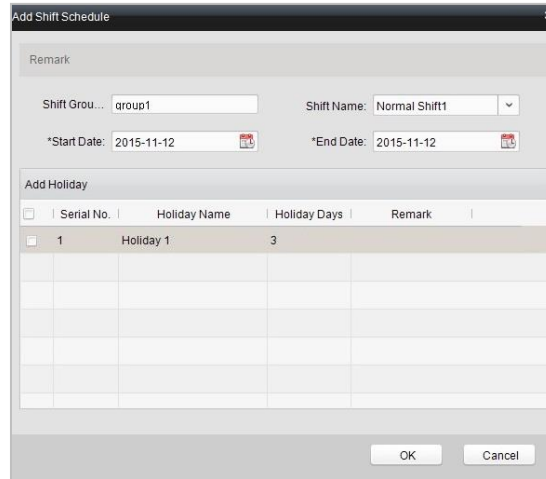
Shift Schedule Management

Press the Shift Schedule Management tab to enter the shift schedule management interface.



Steps:

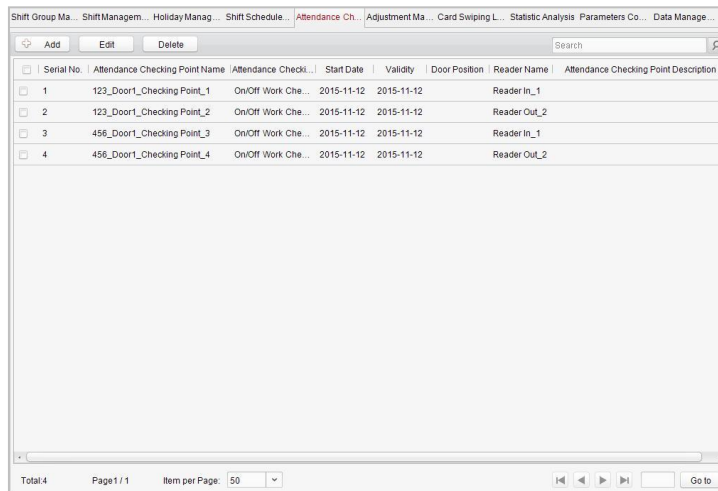
1. Press a tab of shift group on the shift group list.
2. Click the  **Add** button to pop up the shift schedule settings window.



3. Select the shift name from the drop-down list.
4. Set the start data and end data.
5. (Optional) Check the checkbox of holiday to add the holiday shift.
6. Click the button to complete the operation.

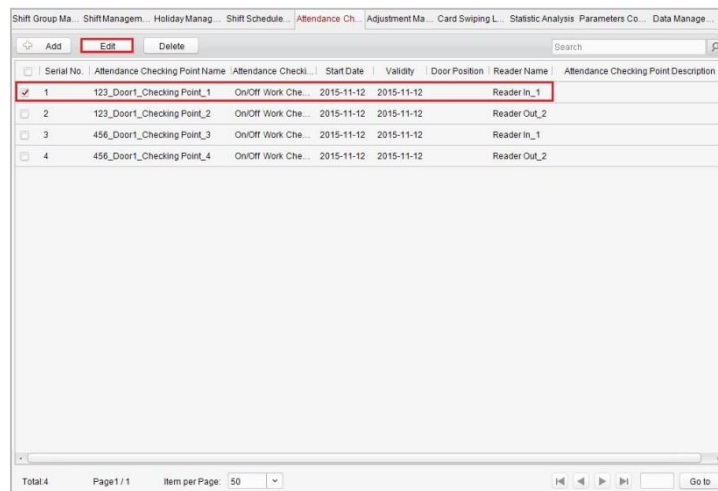
Attendance Check Point Management

Press the Attendance Check Point Management tab to enter the attendance check point management interface.



- **Adding Attendance Check Point**

Steps:



1. Check the checkbox of a checking point, and click the button to pop up the attendance checking point editing

window.

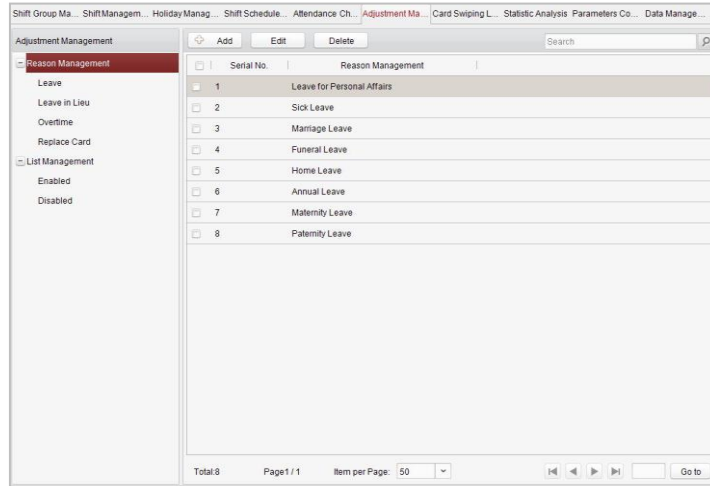
2. Edit the attendance checking point name, start date, validity, and attendance checking point type, controller name, door position, and reader name.
3. Click the button to complete the operation.

- **Adding Attendance Check Point**

Check the checkbox of a checking point and click the button to delete the added checking point.

Adjustment Management

Press the Adjustment Management tab to enter the adjustment management interface.



On this interface, Reason Management and List Management can be realized.

Reason Management

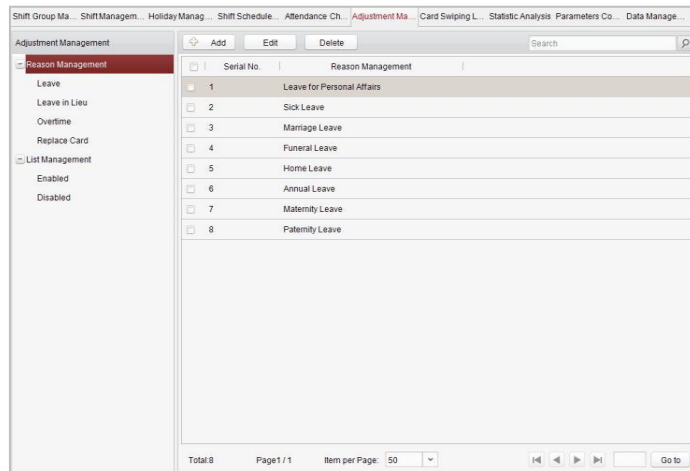
- **Leave**

Purpose:

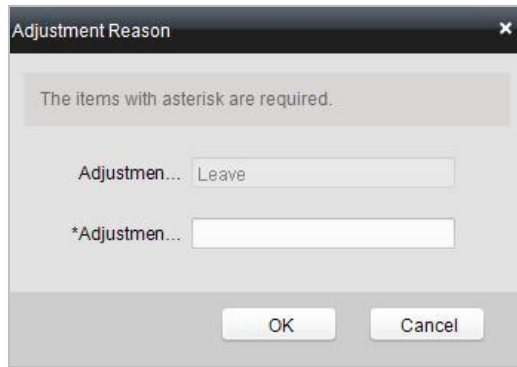
You can add, edit, and delete reasons for leave on the leave interface.

Steps:

1. Press the leave tab to enter the leave interface.



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



3. Enter the adjustment reason, and click the button.

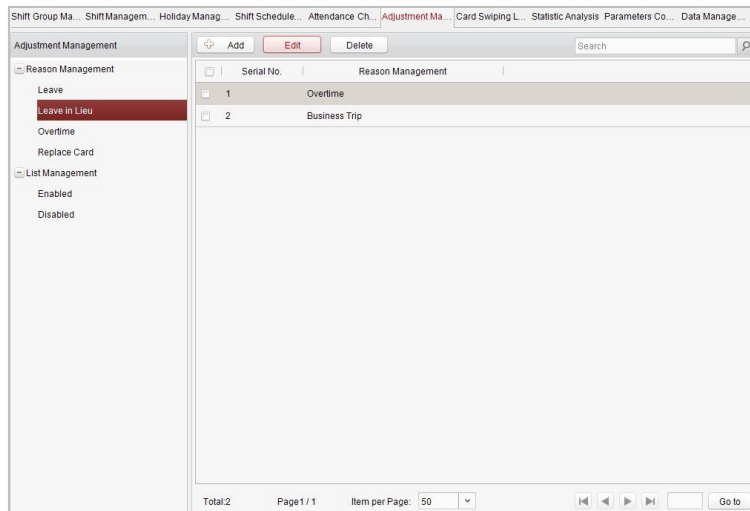
Notes:

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

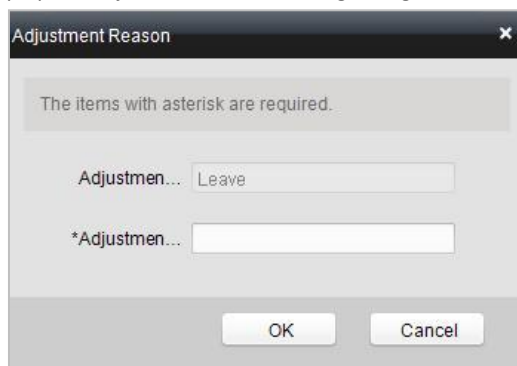
- **Leave in Lieu**

Steps:

1. Press the leave in lieu tab to enter the leave-in-lieu interface.



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



3. Enter the adjustment reason, and click the button.

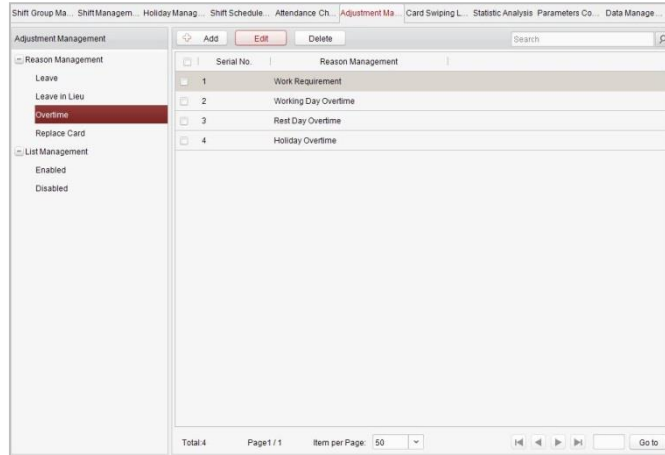
Notes:

- The default adjustment reasons for leave in lieu include overtime, and business trip.

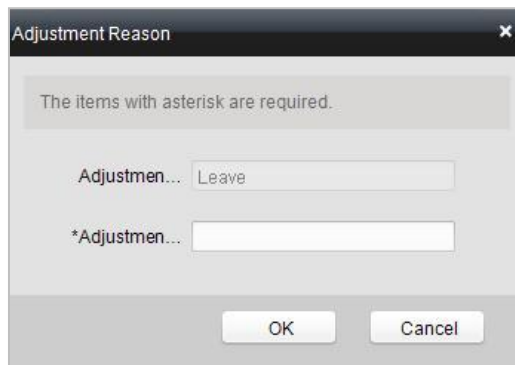
- You can check the checkbox of a reason and click the **Edit** button to edit the reason, and click the **Delete** button to delete the reason.
- Overtime**

Steps:

- Press the overtime tab to enter the overtime interface.



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



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

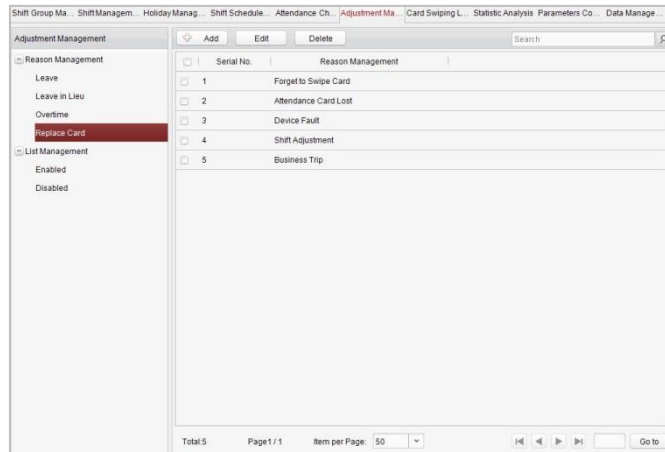
Notes:


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

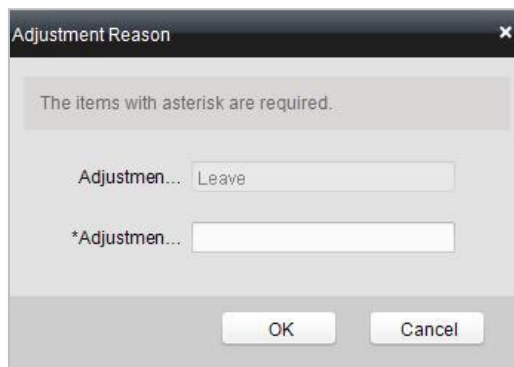
- Replace Card**


Steps:

- Press the replace card tab to enter.





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



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

Notes:

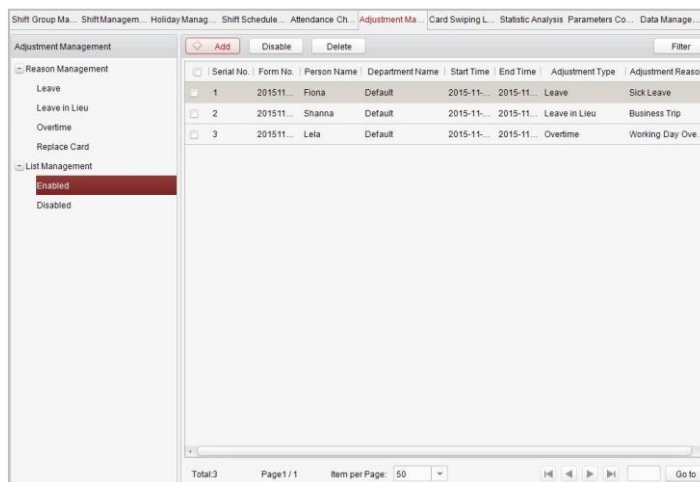
- The default adjustment reasons for card replacing include forget to swipe card, attendance card lost, device fault, shift adjustment, and business trip.
- You can check the checkbox of a reason and click the  **Edit** button to edit the reason, and click the  **Delete** button to delete the reason.

List Management

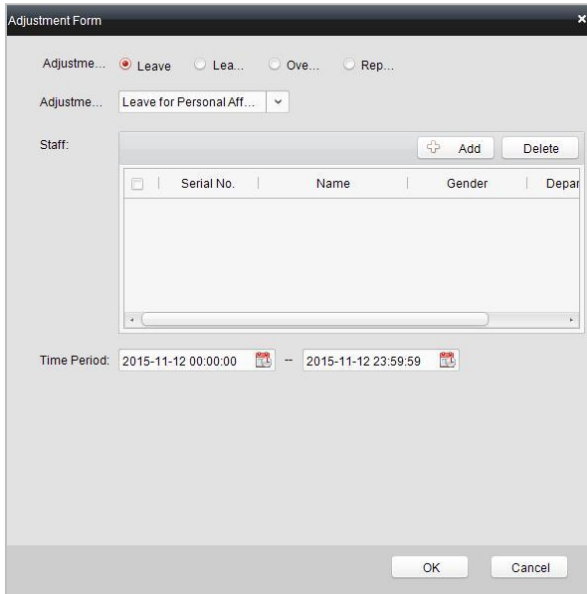
- Enabling**


Steps:

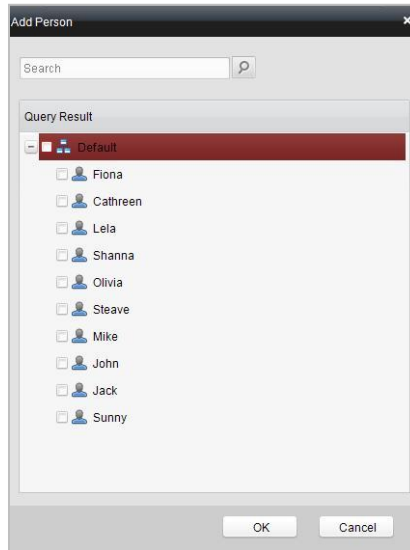
- Press the Enabled tab to enter the enabled list interface.




- Click the  button.



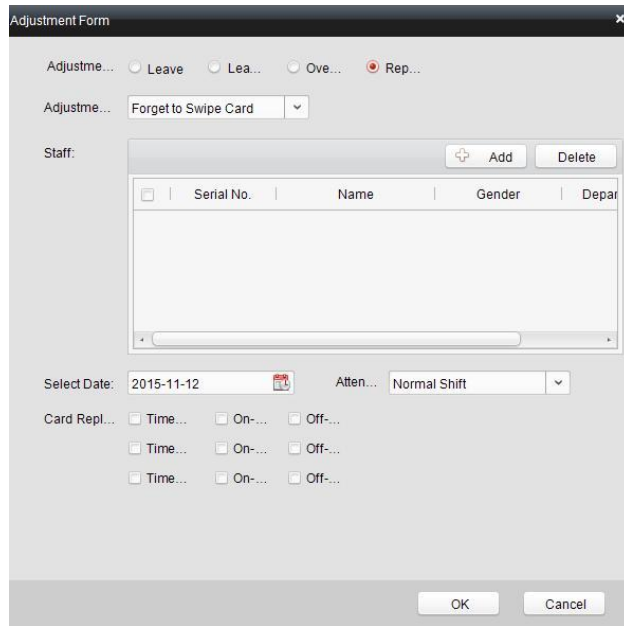
- Select the radio button of adjustment type: leave, leave in lieu, overtime, and replace card.
Leave, Leave in Lieu, and Overtime
 - Select the adjustment reason from the drop-down list.
 - Click the  button to pop up the person adding window.




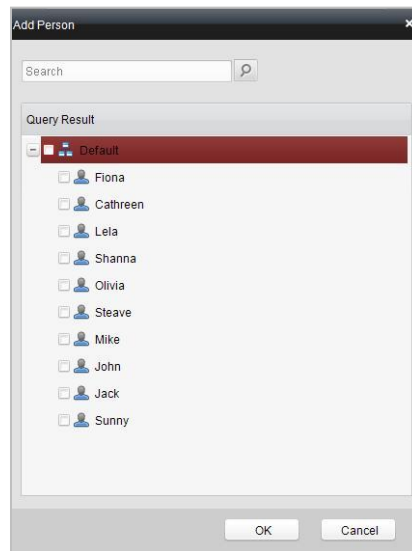
- Select the person and click the  button.
- Set the time period.



Replace Card

- Select the radio button of replace card.



- 2) Select the adjustment reason from the drop-down list.
- 3) Click the  **Add** button to pop up the person adding window.

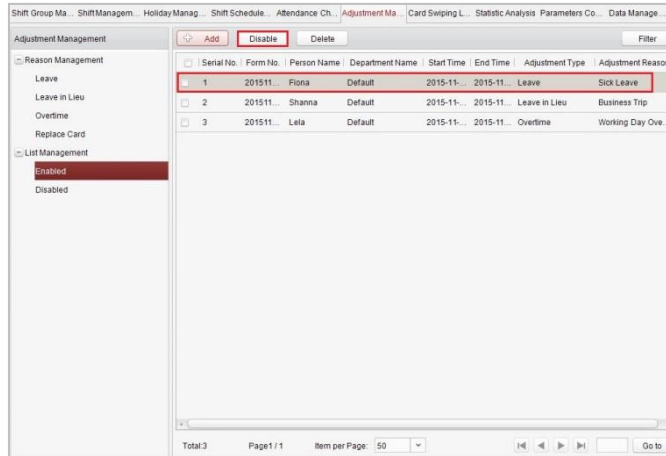


- 4) Select the person and click the  **OK** button.
 - 5) Set the date, attendance shift, and card replacing time.
4. Click the  **OK** button to complete the operation

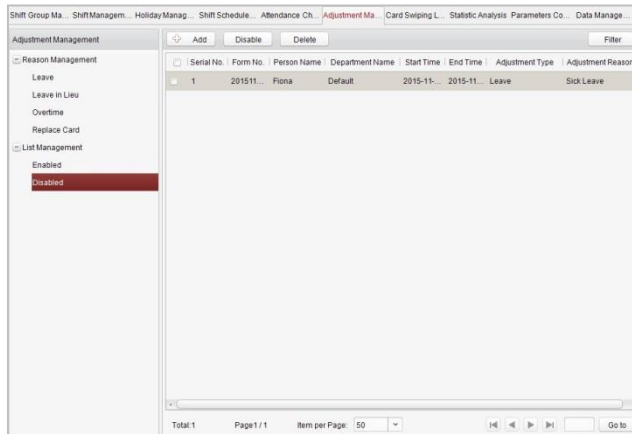
- **Disabling**

Steps:

1. Check the checkbox of a piece of enabled information.

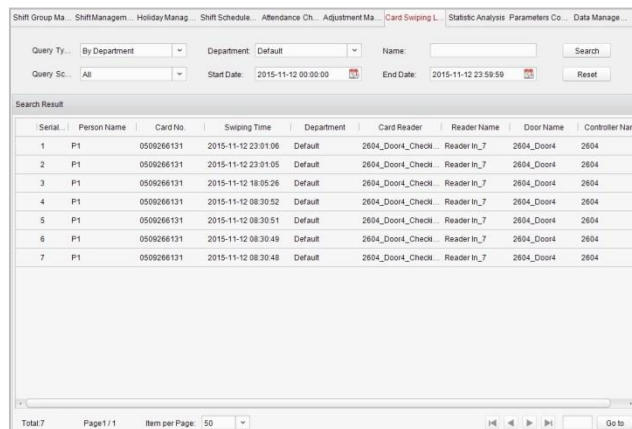


2. Click the **Disable** button to disable the information.
3. Press the Disabled tab and the disabled information will be listed on the disabled interface.



Card Swiping Log Query

Press the Card Swiping Log Query tab to enter the card swiping log searching and viewing interface.

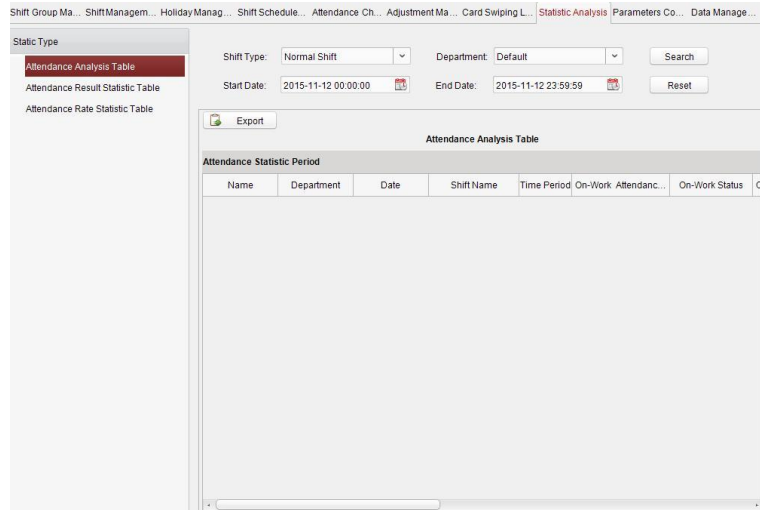


Notes:

- You can search the card swiping log by two query types: By Shift Group, and By Department.
- You can search the card swiping log by group name.
- You can search the card swiping log by start date and end date.
- You can restrict the query scope: All, First, or Last.

Statistic Analysis

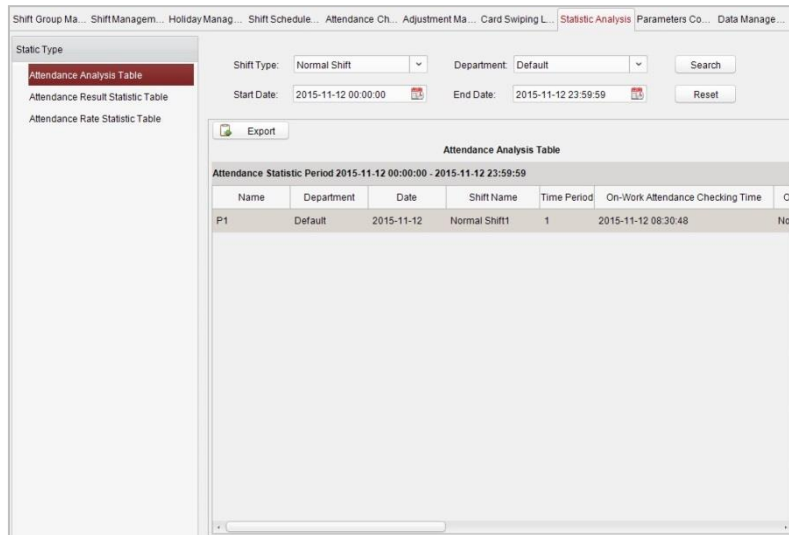
Press the Statistic Analysis tab to enter the statistic analysis interface.



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

Attendance Analysis Table

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

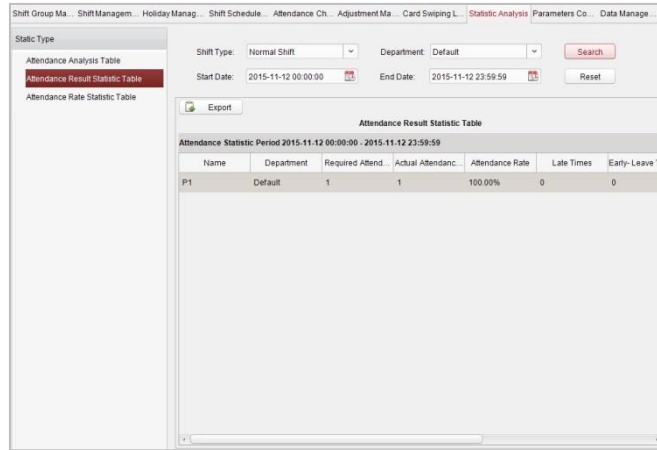


Notes:

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

Attendance Result Statistic Table

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

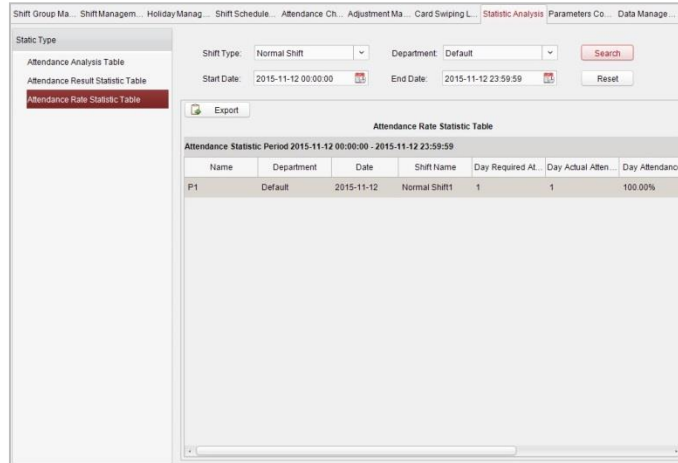


Notes:

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

Attendance Rate Statistic Table

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

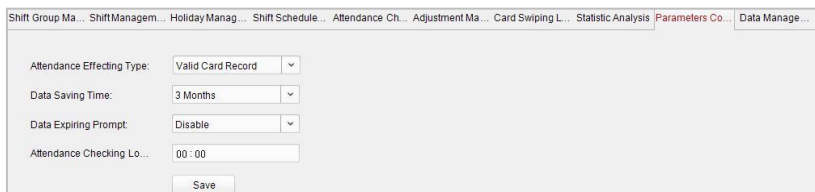


Notes:

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

Parameters Configuration

Press the Parameters Configuration tab to enter the parameters configuration interface.

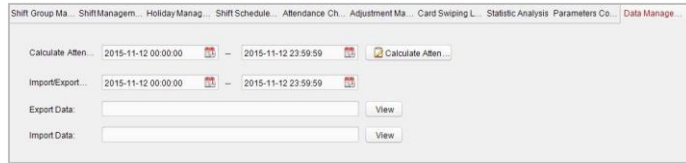



Steps:

1. Select the attendance effecting type (Valid Card Record, or Invalid Card Record), data saving time, data expiring prompt.
2. Set the attendance checking log clearing time.

Data Management

Press the Data Management tab to enter the data management interface.

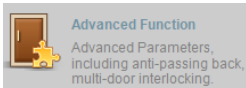



Click the  **Calculate Atten...** button to calculate the attendance date.
On this interface, you can export and import attendance data.

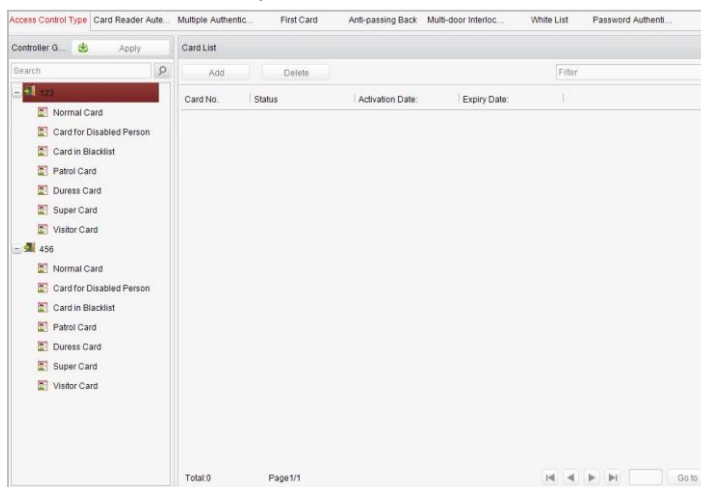
7.3.8 Advanced Functions

Purpose:

The advanced functions of the access control system can be configured, such as access control type, password authentication and first card.



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



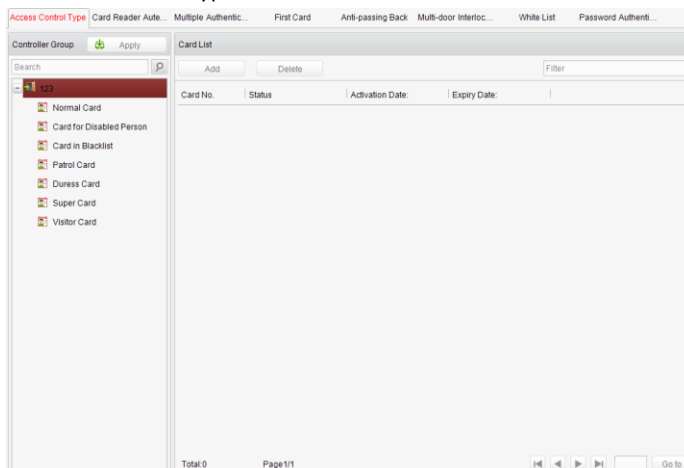
Access Control Type

Purpose:

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

Steps:

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



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

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

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

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

Duress Card: The card swiping action will be uploaded.

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

Visitor Card: The card is assigned for visitors.

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

Note: You can click Delete to remove the card from the card type and the card can be available for being re-assigned.

Card Reader Authentication

Purpose:

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

Notes:

- For this authentication mode, the card swiping operation cannot be replaced by entering the card No..
- For password settings, please refer to Section 16.2.3 Normal Card.

Steps:

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

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

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

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

Swipe Card/Password: The door can open by inputting the password or swiping the card.

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

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

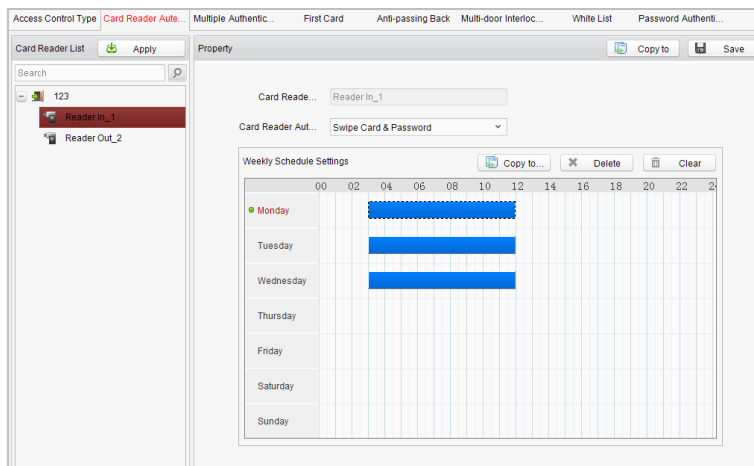
Fingerprint Swipe Card: The door can open by both inputting the fingerprint and swiping the card.

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

Note:

The fingerprint associated functions are only supported by device with fingerprint recognition module.

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



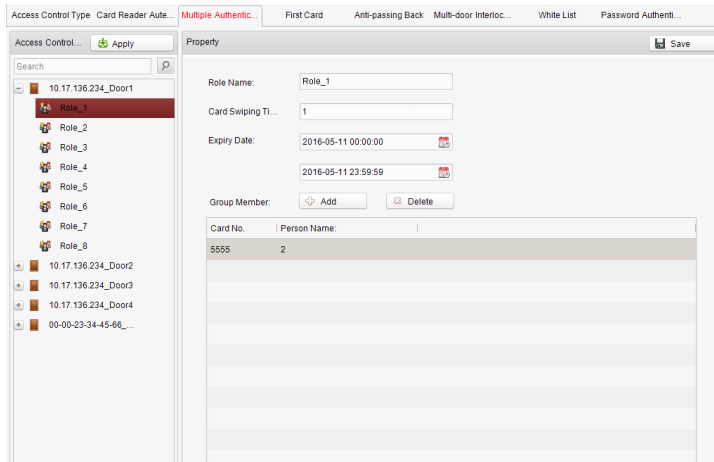
4. Repeat the above step to set other time periods.
Or you can select a configured day and click the Copy to Week button to copy the same settings to the whole week.
You can click the Delete button to delete the selected time period or click the Clear button to delete all the configured time periods.
5. (Optional) Click the Copy to button to copy the settings to other card readers.
6. Click the Save button to save parameters.
7. Click the Apply button to take effect of the new settings.

Multiple Authentication

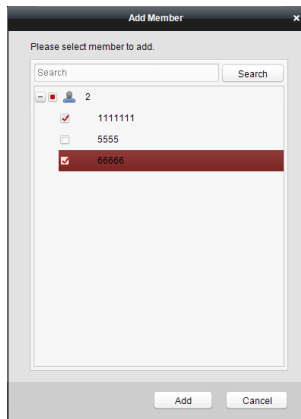
You can manage the cards by group and set the authentication for multiple cards for one access controller.

Steps:

1. Click **Multiple Authentication** tab and select a group in the access controller from the list on the left.
2. Edit the role name, the card swiping times and the expiry date. And click **Add** to add the group members.

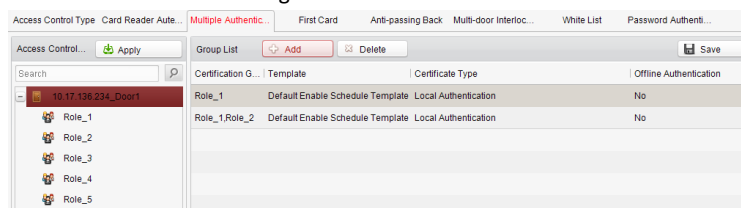


3. Check the target members and click **Add** to add the selected members. The added members will be displayed in the group member list.

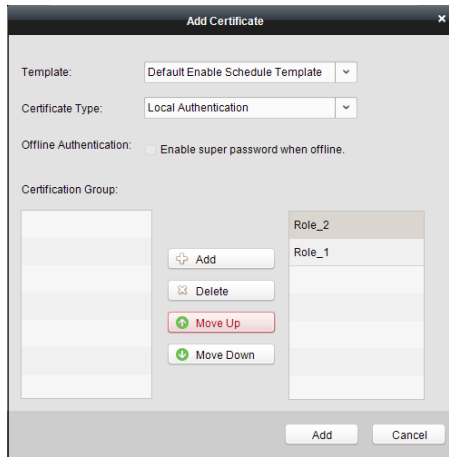


Or select the members and click **Delete** to delete the members.

4. Click **Save** to save the configuration.
5. Click the access controller which contains the configured role and click **Add**.



6. Configure the template, the certificate type, the offline authentication and the certification group. And click **Add** button in the middle to add the role from the left list to the right one.
Or select the target role in the right list and click **Delete** to delete the selected role.
Or select the target role and click **Move Up** or **Move Down** to change the role swiping card order.



7. Click **Add** at the bottom to add the configured the authentication group to the group list. And click **Save** to save the configuration.

Certification G...	Template	Certificate Type	Offline Authentication
Role_1	Default Enable Schedule Template	Local Authentication	No
Role_1,Role_2	Default Enable Schedule Template	Local Authentication	No

Note:

Click **Apply** on the upper-left to take effect of the new settings.

First Card

Purpose:

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



Steps:

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

Anti-Passing Back

Purpose:

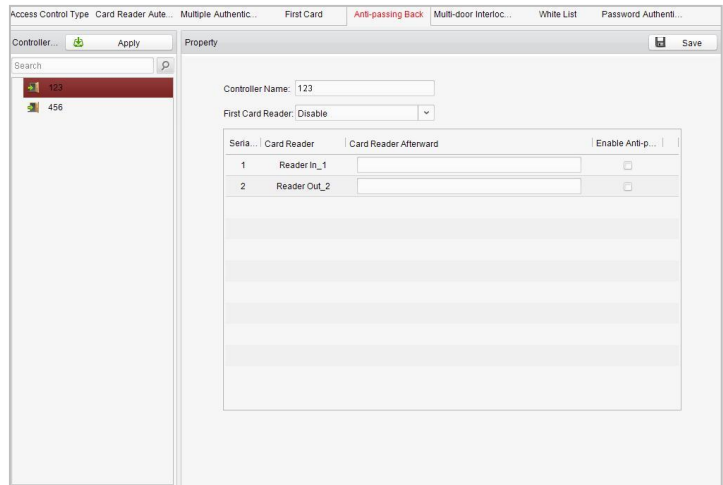
In this mode, you can only pass the access control system according to the specified path.

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

Setting the Path of Swiping Card (Card Reader Order)

Steps:

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



2. You can set the name for the controller and select the card reader as the beginning of the path.
3. In the list, click the text filed of Card Reader Afterward and select the linked card readers.
Example: If you select Reader In_01 as the beginning, and select Reader In_02, Reader Out_04 as the linked card readers. Then you can only get through the access control system by swiping the card in the order as Reader In_01, Reader In_02 and Reader Out_04.
4. Check the checkbox of Enable Anti-Passing back.
5. Click Save and then click the Apply button to take effect of the new settings.

Multi-door Interlocking

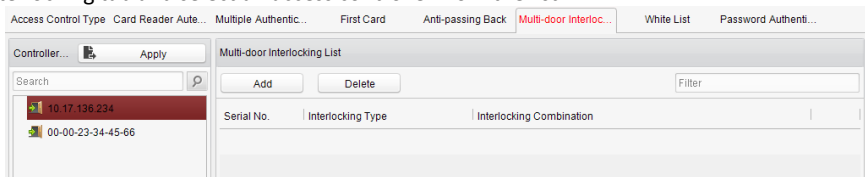
You can set the multi-door interlocking between multiple doors of the same access controller. To open one of the doors, other doors must keep closed. That means in the interlocking combined door group, up to one door can be opened at the same time.

Notes:

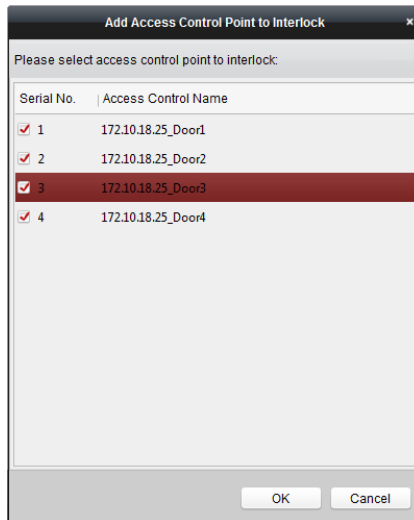
- The Multi-door Interlocking function is only supported by the access controller which has more than one access control points (doors).
- Either the anti-passing back or multi-door interlocking function can be configured for an access controller at the same time.

Steps:

1. Click Multi-door Interlocking tab and select an access controller from the list.



2. Click Add to pop up the Add Access Control Point to Interlock interface.

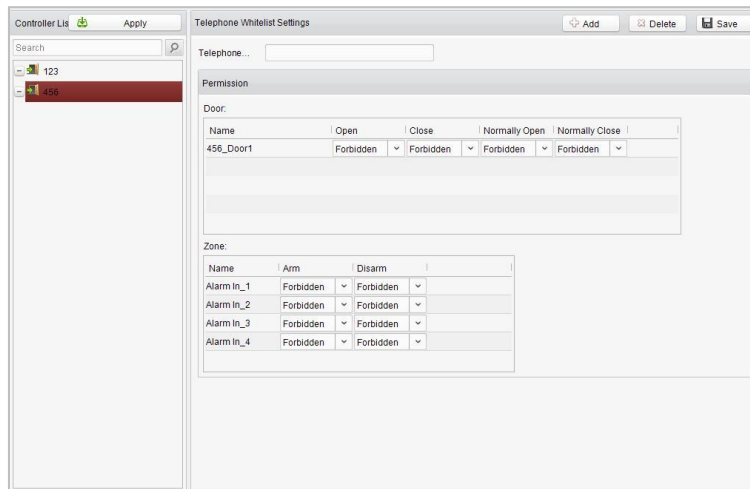


3. Select the access control point (door) from the list.
Note: Up to four doors can be added in one multi-door interlocking combination.
4. Click **OK** to save the adding.
5. (Optional) After adding the multi-door interlocking combination, you can select it from the list and click **Delete** to delete the combination.
Note: Click **Apply** button to take effect of the new settings.

White List

Steps:

1. Click the White List button to enter into the white list interface.



2. Select the access control point, and click the Add button. Multi-door Interlocking and select an access control point.
3. Select the access control points and click Add button.
4. Input the mobile number.
5. Select the settings of control permission, and set the property as Allow to enable this function.
Door: The mobile can control the door (open, closed, normally open, or normally closed).
Arming Region: The mobile can arm and disarm the arming channels
6. Click the Save button to save parameters.
7. Click the Apply button to take effect of the new settings.

Notes:

- The mobile can control the door and the arming region by sending SMS control instructions.
- The SMS control instruction is composed of Command, Operation Range, and Operation Object.

Instruction Content	Digit	Description	Format
Command	3	010-Open, 011-Closed, 020-Normally open, 021-Normally Closed, 120-Disarm, 121-Arm	
Operation Range	1	1-all objects with permission, 2-single operation	Command#1#
Operation Object	3	Starts from 1 (corresponding to different doors or arming regions according to commands)	Command#2#Operation Object#

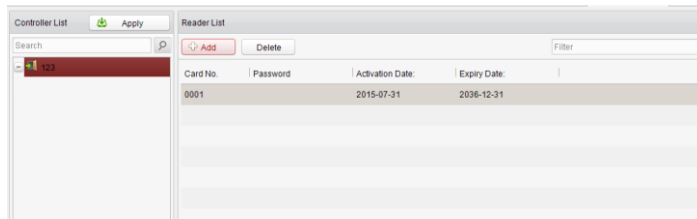
Password Authentication

Purpose:

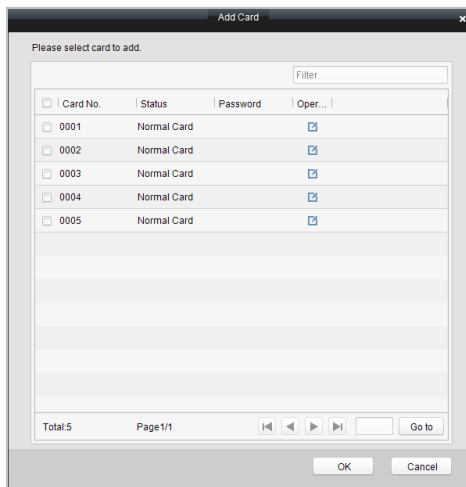
You can open the door by inputting the password only after finishing the operation of password authentication.


Steps:

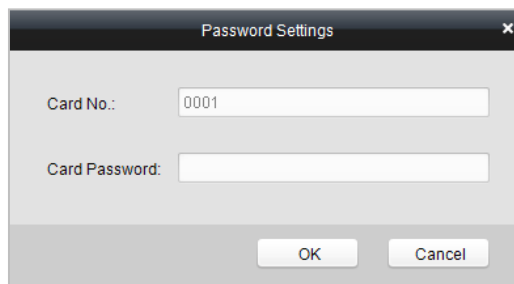
1. Click Password Authentication tab and select a host.



2. Click the Add button to enter card adding interface.



3. Check the checkbox of the corresponding card, and click the  button to pop up the password setting dialogue box.



4. Input the card password.

5. Click the Ok button to finish adding the card.

Notes:

- The card, having added the password, will display in the card list.
- You can select the card in the card list, and click the Delete button to delete the password authentication of the selected card.

7.4 Checking Status and Event

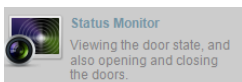
Purpose:

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

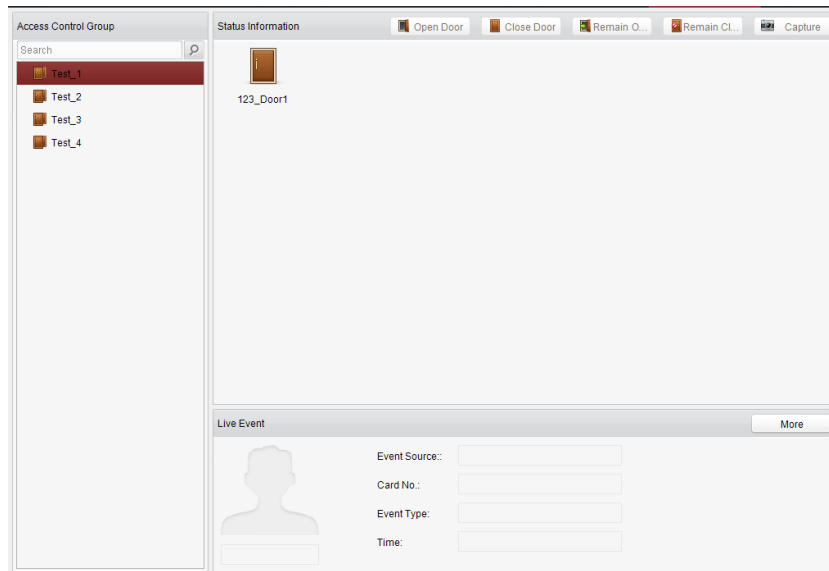
7.4.1 Status Monitor

Purpose:

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



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



Access Anti-control

Door Anti-control

Purpose:

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

Steps:

1. Enter the status monitor page.



2. Click on the icon on the Status Information panel to select a door.

3. Click on the button listed on the upper-left side of the Status Information panel to select a door status for the door.

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

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

Always Open : Click on the button to keep the door open.

Always Close : Click on the button to keep the door closed.

Capture : Click on the button to capture the picture.

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

Notes:

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

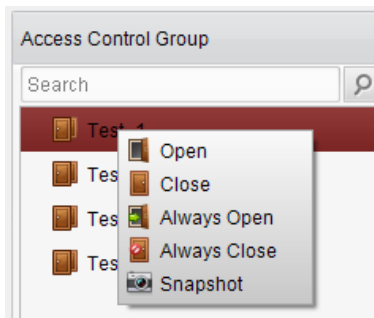
Group Anti-control

Purpose:

You can control the status for a group of control points (doors) in this section.

Steps:

1. Enter the status monitor page.
2. Right click on a group in the Group list and to select a door status for the group.

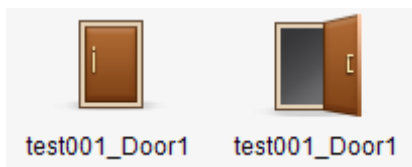


Notes:

- If the status is selected as Remain Open/Remain Closed, all the doors in the group will keep open/ closed until a new anti-control command being made.
- The function of picture capturing cannot be realized until the storage server is installed.

Access Status

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



Live Event

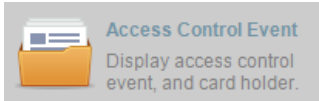
You can check the live information of the access event on this panel. Click **More** to enter the Access Event page to view more event information.



7.4.2 Access Control Event

Purpose:

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



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

Access Control Event Information						Card Holder Information
Serial No.	Event Type	Card Holder	Card No.	Event Time	Event Source	Direction
7	Remotely Arming			2015-07-31 16:50:24	123	
6	Remotely Disarm...			2015-07-31 16:50:24	123	
5	Remotely Logout			2015-07-31 16:48:42	123	
4	Remotely Login			2015-07-31 16:41:20	123	
3	Remotely Logout			2015-07-31 16:41:13	123	
2	Remotely Login			2015-07-31 16:39:43	123	
1	Remotely Clear...			2015-07-31 16:07:53	123	

Person No.:

Name:

Gender:

ID Type:

ID No.:

Belong to...:

Contact No.:

Contact Ad...:

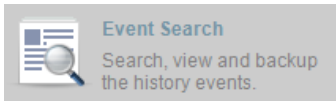
Steps:

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

7.4.3 Event Search

Purpose:

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



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

Event Type: Start Time:

Card Holder: End Time:

Card No.:

Search Result

Serial No.	Event Type	Card Holder	Card No.	Event Time	Event Source	Direction	Capture Images

Total: 0 Page 1/1

Card Holder Information

Person No.:

Name:

Gender:

ID Type:

ID No.:



Belong to...:

Contact No.:

Contact Ad...:

Steps:

1. Enter the event search page.
2. Enter the search criteria (event type/ person name/ card No/ start & end time).

Event Type:	<input type="text" value="All"/> ▾	Start Time:	<input type="text" value="2014-09-18 00:00:00"/> 	<input type="button" value="Search"/>
Card Holder:	<input type="text"/>	End Time:	<input type="text" value="2014-09-18 23:59:59"/> 	
Card No.:	<input type="text"/>			

3. Click Search to get the search results.
4. View the event information in the event list.
5. Click on an event to view the information of the card holder on the Person Information panel on the left side of the page.

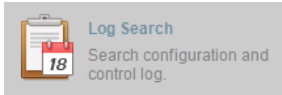
7.5 System Maintenance

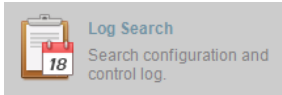
7.5.1 Log Management

Interface Introduction

Purpose:

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




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

Configuration Logs Searching

Purpose:

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

Steps:

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

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


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

Control Logs Searching

Purpose:

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

Steps:

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

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

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


Searching Configuration Log

Searching One-card Configuration Logs

Purpose:

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

Steps:

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

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


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

Searching Access Control Configuration Logs

Purpose:

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

Steps:

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

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


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

Searching Downloading Permission Logs

Purpose:

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

Steps:

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

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


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

Searching System Configuration Logs

Purpose:

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

Steps:

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

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

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

Searching Control Log


Searching Access Control Logs

Purpose:

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

Steps:

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

3. Select the operation type as Access Control Logs.
4. Click the icon  to specify the start time and end time.
5. Click Search. The matched log files will display on the list.

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


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

Log Search

Purpose:

The Log Search of the Access Control System includes information for configuration log files and control log files.

Steps:

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

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

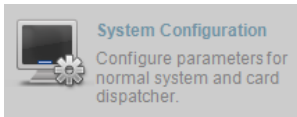
Note: Please narrow the search condition if there are too many log files.

7.5.2 System Configuration

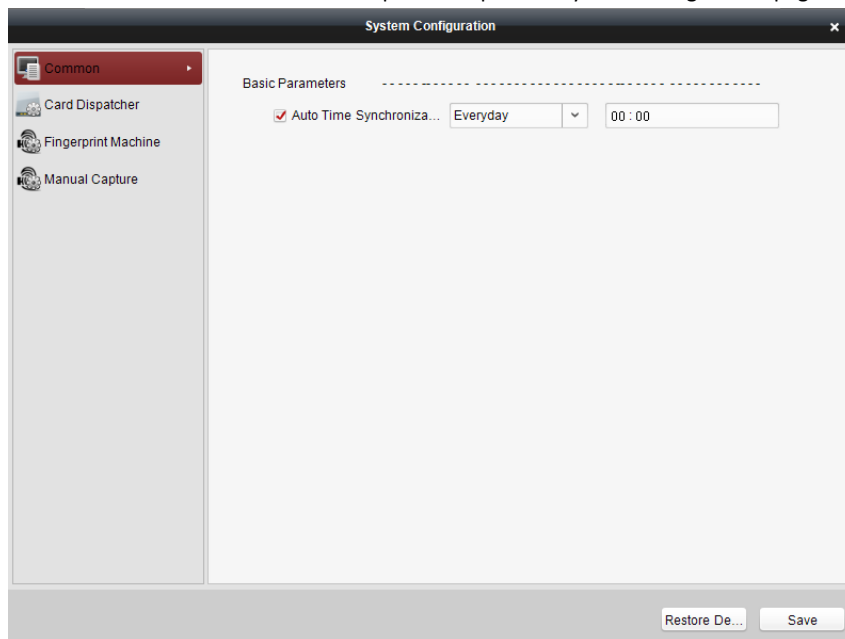
Interface Introduction

Purpose:

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



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



Auto Time Synchronization

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

Card Reader Configuration

The Card Reader Configuration is for Access Control System to read the card by setting Card Reader parameters.

Fingerprint Machine

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

Note:

The fingerprint associated functions are only supported by device with fingerprint recognition module

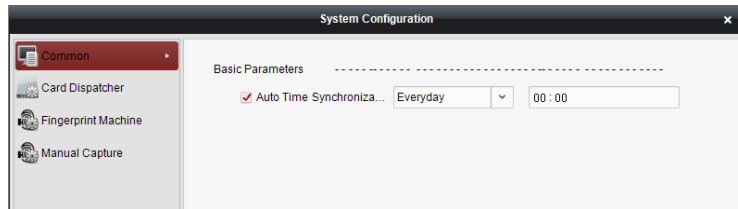
Manual Capture Configuration

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

Auto Time Synchronization

Steps:

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



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


Note: You can click the Restore Default Value button to restore the defaults of all the local configurations.

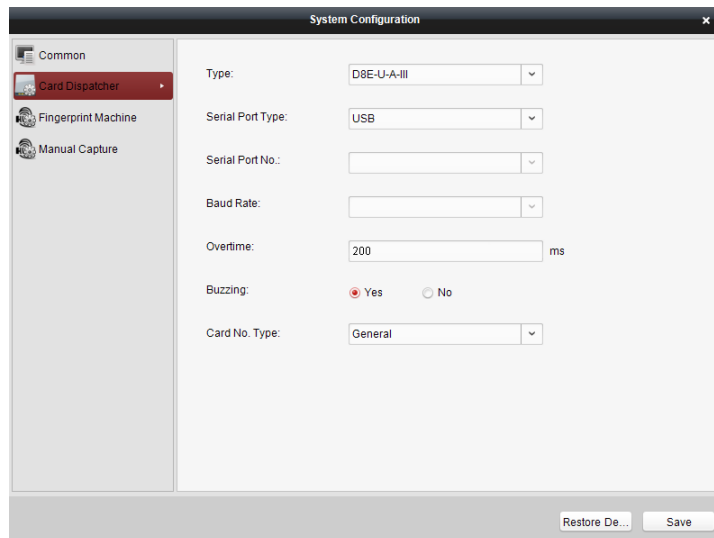
Card Dispenser Configuration

Purpose:

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

Steps:

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




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

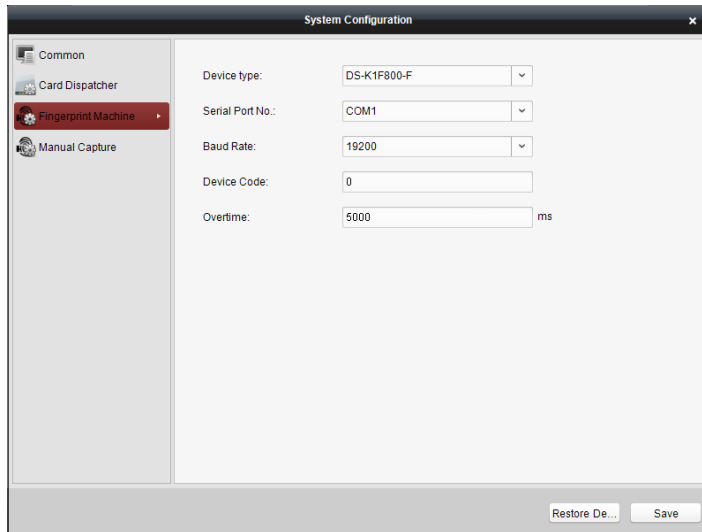
Notes:

- It is supported using card type as regular and Wiegand.
- When the BEEP is selected as “YES”, the audio will be off when you click the “SAVE” if the Card Reader Configuration is set wrong; the audio will be on when you click the “Save” and when you insert the card reader if the configuration is set correct.
- You can click the Restore Default Value button to restore the defaults of the entire local configuration.

Fingerprint Machine Configuration

Steps:

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



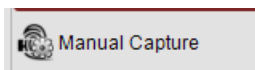
2. Select the device type, serial port number, baud rate, device code, and overtime parameters of the fingerprint machine.
3. Click the save button to save the settings.

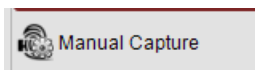
Notes:

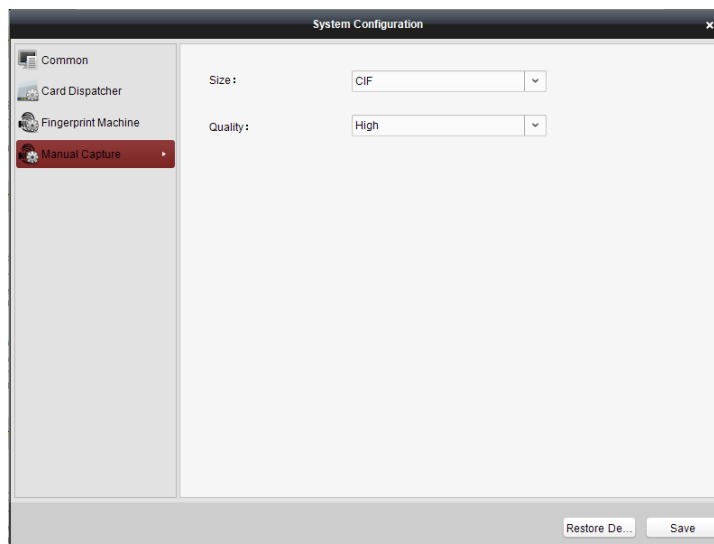
- It is supported using device type as DS-K1F800-F, DS-K1F810-FOptical Fingerprint Collecting Instrument and DS-K1300-F Capacitive Fingerprint Collecting Instrument.
- The serial port number should correspond to the serial port number of PC.
- The baud rate should be called according to the external fingerprint card dispatcher. The default value is 19200.
- Overtime refers to the valid fingerprint collecting time. If the user does not input a fingerprint or inputs a fingerprint unsuccessfully, the device will indicate that the fingerprint collecting is over.
- You can click the Restore Default Value button to restore the defaults of all local settings.

Manual Capture Configuration

Steps:



1. Click the  icon on the System Configuration interface to open the Manual Capture Configuration page.



2. Select the picture size from the dropdown list
3. Select the picture quality from the dropdown list.

Notes:

- It is supported using the picture size as CIF, QCIF, 4CIF/D1, SVGA, HD720P, VGA, WD1, and AUTO.
- It is supported using the picture quality as High, Medium, and Low.

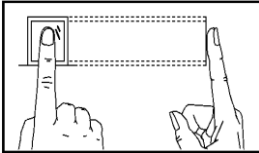
Appendix: Tips for Scanning Fingerprint

Recommended Finger

Forefinger, middle finger or the third finger.

Correct Scanning

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

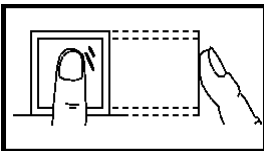


You should press your finger on the scanner horizontally. The center of your scanned finger should align with the scanner center.

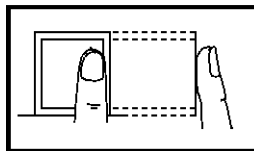
Incorrect Scanning

The figures of scanning fingerprint displayed below are wrong:

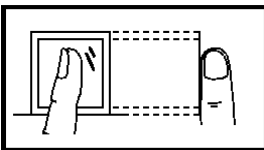
Vertical



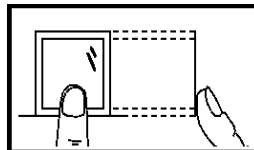
Edge I



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.

0101001060602

