Access Control Terminal

User Manual

UD.6L0206D1130A01

User Manual

©2015 Hangzhou Hikvision Digital Technology Co., Ltd.

This manual is applied for access control terminal.

Product Serials	Model	Product Name
DS-K1T802	DS-K1T802E	Access Control Terminal (EM Card)
	DS-K1T802M	Access Control Terminal (Mifare Card)

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.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, REGARDING THIS MANUAL. HIKVISION DOES NOT WARRANT, GUARANTEE, OR MAKE ANY REPRESENTATIONS REGARDING THE USE OF THE MANUAL, OR THE CORRECTNESS, ACCURACY, OR RELIABILITY OF INFORMATION CONTAINED HEREIN. YOUR USE OF THIS MANUAL AND ANY RELIANCE ON THIS MANUAL SHALL BE WHOLLY AT YOUR OWN RISK AND RESPONSIBILITY.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, 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, SECURITY BREACHES, OR LOSS OF DATA OR DOCUMENTATION, IN CONNECTION WITH THE USE OF OR RELIANCE ON THIS MANUAL, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY OR CERTAIN DAMAGES, SO SOME OR ALL OF THE ABOVE EXCLUSIONS OR LIMITATIONS MAY NOT APPLY TO YOU.

Support

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

0100001051101

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 1

1.1 Introduction 1
1.2 Main Features 1

2 Appearance 3

2.1 Appearance of the Termianl 3
2.2 Description of Keypad Items 4

3 Terminal Connection 5

3.1 Terminal Description 5
3.2 External Device Wiring 6

4 Installation 8

4.1 Mounting with Gang Box 8
4.2 Mounting without Gang Box 9

5 Activating the Access Control Terminal 11

5.1 Activating via SADP Software 11
5.2 Activating via Client Software 13

6 Basic Operation 17

6.1 User Management 18
6.1.2 Adding User 18
6.1.2 Editing User 20
6.1.3 Searching User 22
6.1.4 Deleting the User 23
6.2 Communication Settings 23
6.3 System Settings 24
6.3.1 Restoring Settings 25
6.3.2 Setting login Password 26
6.3.3 Door Settings 26
6.3.4 Settings Authentication Mode 27
6.3.5 Rebooting Device 28
6.4 Time Settings 28
6.5 Permission Settings 29
6.6 System Information 32

7 Client Operation 34

7.1 Overview of Access Control System 34
7.1.1 Description 34
7.1.2 Configuration Flow 34
7.2 Device Management 36

7.2.1 Controller Management 36
7.2.2 Access Control Point Management 45
7.3 Permission Management 48
7.3.1 Person Management 48
7.3.2 Card Management 53
7.3.3 Schedule Template 57
7.3.4 Door Status Management 62
7.3.5 Interact Configuration 66
7.3.6 Access Permission Configuration 71
7.3.7 Attendance Management 77
7.3.8 Advanced Functions 104
7.4 Checking Status and Event 113
7.4.1 Status Monitor 113
7.4.2 Access Control Event 115
7.4.3 Event Search 116
7.5 System Maintenance 118
7.5.1 Log Management 118
7.5.2 System Configuration 122

1 Overview

1.1 Introduction

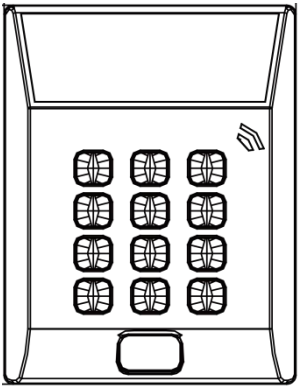


Figure 1-1 DS-K1T802 Series Standalone Access Control Terminal

DS-K1T802 is a series of standalone access control terminal designed with a LCD display screen. It supports TCP/IP network communication, offline records storage functions and so on.

1.2 Main Features

- Equipped with 32-bit high-speed processor
- Supports TCP/IP network communication, with self-adaptive network interface. The communication data is specially encrypted to relieve the concern of privacy leak
- Supports EM card and Mifare card reading
- Supports authentication methods of card, card and password
- Doorbell ring design
- Supports time synchronization via NTP, manual or automatic method

- Supports online upgrade, and remote operation and device rebooting control
- The access controller can store 3 thousand legal cards and 10 thousand card swiping records
- Unlocking overtime alarm, invalid card swiping over times alarm, blacklist alarm, and duress card/code alarm
- Supports various card types as normal/ disabled/ blacklist/ patrol/ guest/ duress/ super card, etc.
- Data can be permanently saved after power-off
- Accurate data and time display provided by built-in electronic clock and watchdog program to ensure the basic function of the terminal
- Remotely device rebooting control
- Supports alarm of offline event exceeding 90%

2 Appearance

2.1 Appearance of the Termianl

Please refer to the following content for detailed information of the terminal.

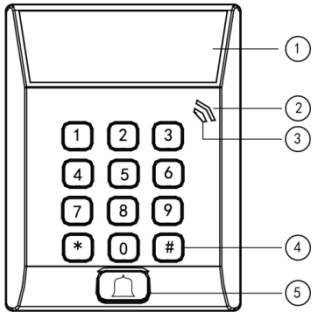


Figure 2-1 Appearance of Access Control Terminal

Table 2-1 Description of Access Control Terminal

No.	Name	Description	
1	LCD Display Screen	First Line: display date Second Line: display time Third Line: display authentication information or swiping status	
2	Power Indicator	Slow Flicking Green	Card reader is working properly.
		Solid Green for a period	The operation of pressing keys or swiping card is valid.

		Solid Red for a period	The operation of pressing keys or swiping card is invalid.
No.	**Name**	**Description**	
3	Link Indicator	Solid light	Normal
		Off	Network Exception
4	Keypad	Numeric key 0 to 9, Clearing key *, and Confirming key #	
5	Door Bell	Door Bell Ring	

2.2 Description of Keypad Items

Table 2-2 Description of Keys

No.	Description
0 to 9	Numeric Keys: Enter number in the textbox.
2 and 8	Direction Keys: Select icons in the menu.
*	Exiting Key: Click the key to exit the menu.
#	Confirming Key: Click the key to confirm operations.

3 Terminal Connection

3.1 Terminal Description

The following table shows the terminals description

Table 3-1 Terminal Description

Description		Color
Power Input	12V DC	Red
	GND	Black
Bell	Bell+	Orange
	Bell-	Yellow
Door Lock	BUTTON_IN	Purple
	DOOR_COM	Green
	DOOR_NO/NC	Blue
	SENSOR_IN	White
	GND	Black
	12V_LOCK	Brown

3.2 External Device Wiring

Power Supply Wiring

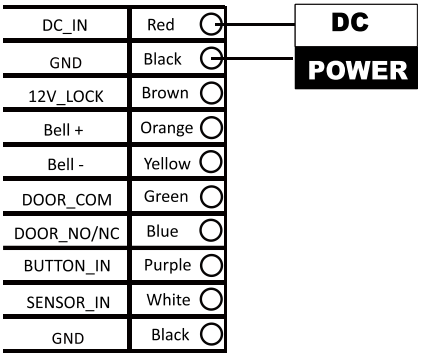


Figure 3-1 Power Supply Connection Diagram

Doorbell Wiring

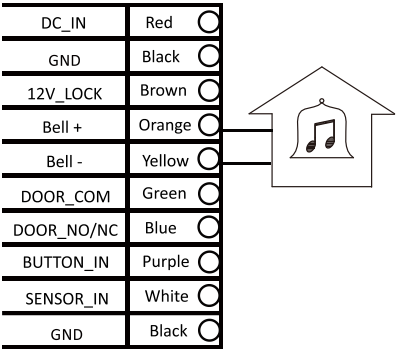


Figure 3-2 Doorbell Wiring Diagram

Door Button Wiring

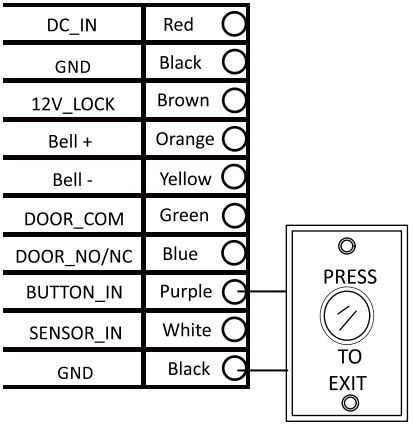


Figure 3-3 Door Button Wiring Diagram

Door Lock Wiring

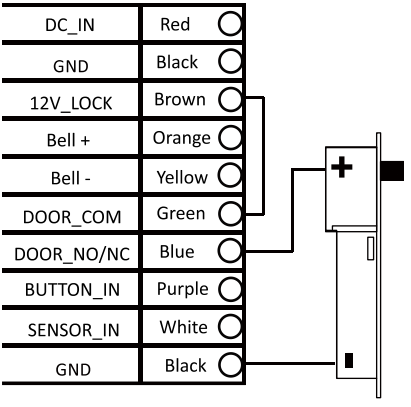


Figure 3-4 Door Lock Wiring Diagram

Door Magnetic Wiring

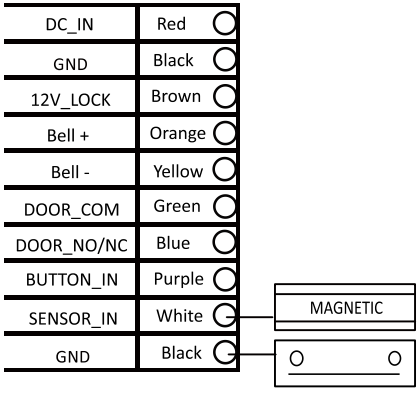


Figure 3-5 Door Magnetic Wiring Diagram

4 Installation

Before you start

- Please make sure that the device in the package is in good condition and all the assembly parts are included.
- Make sure that all the related equipment is power-off during the installation.
- Check the specification of the products for the installation environment.
- Check whether the power supply is matched with your AC outlet to avoid damage.
- If the product does not function properly, please contact your dealer or the nearest service center. Do not disassemble the camera for repair or maintenance by yourself.
- Please make sure the wall is strong enough to withstand three times the weight of the device and the mounting.

4.1 Mounting with Gang Box

Steps:

1. Route the cables through the cable hole of the mounting base.

2. Align the screw holes on mounting base with the screw holes on gang box.

3. Fix the mounting base on the gang box with inserting two KA4*22-SUS screws (supplied) into the two screw holes.

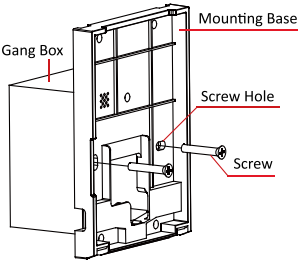


Figure 4-1 Install the Mounting

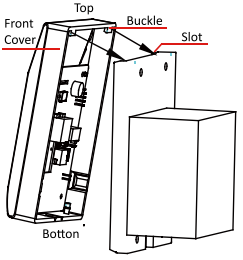


Figure 4-2 Attach the Front Cover

Base

4. Connect the corresponded cables.
5. Align the buckle of the front cover with the slot of the mounting base, and hang the front cover onto the mounting base. Make sure the buckle is embedded into the slot.
6. Secure the front cover with inserting and tightening two screws on the bottom of device.

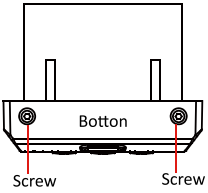


Figure 4-3 Secure the Front Cover

4.2 Mounting without Gang Box

Steps:

1. Drill 4 screw holes in the wall according to the holes of the mounting base, and then insert expansion screws sockets (not supplied) into the holes.

2. Route the cables through the cable hole of the mounting base.

3. Align the screw holes on the base with the screw sockets on the wall.

4. Attach the mounting base on the wall with Inserting 4 KA4*22-SUS screws (supplied) into the 4 screw sockets.

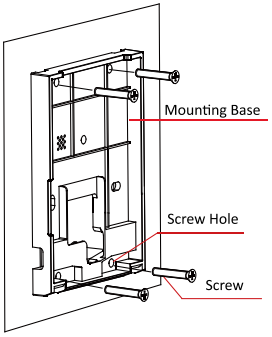


Figure 4-4 Install the Mounting Base

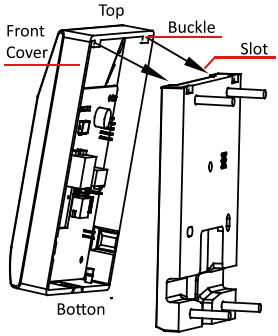


Figure 4-5 Attach the Front Cover

5. Connect the corresponded cables.
6. Align the buckle of the front cover with the slot of the mounting base, and hang the front cover onto the mounting base. Make sure the buckle is embedded into the slot.
7. Secure the front cover with inserting and tightening two screws on the bottom of device.

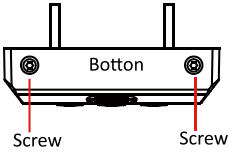


Figure 4-6 Secure the Front Cover

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.

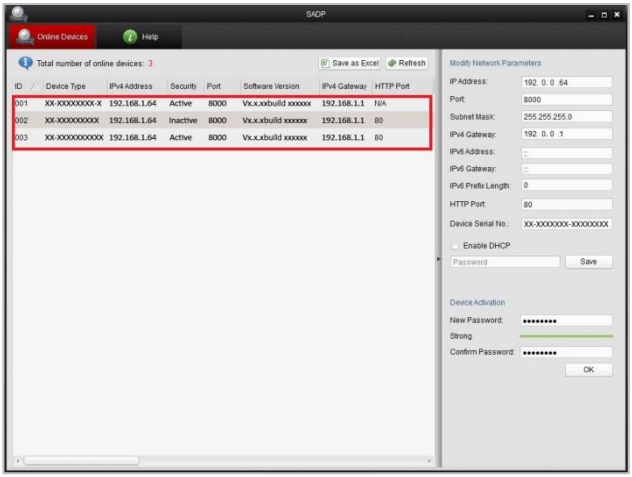


Figure 5-1 SADP Interface

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 modifying the IP address manually.

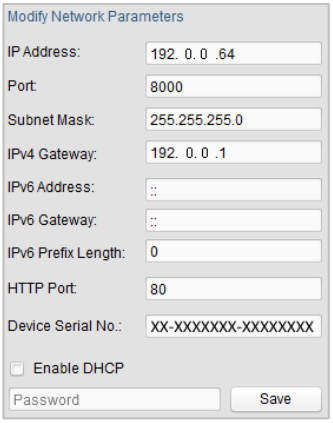


Figure 5-2 Modify Network Parameters Interface

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.

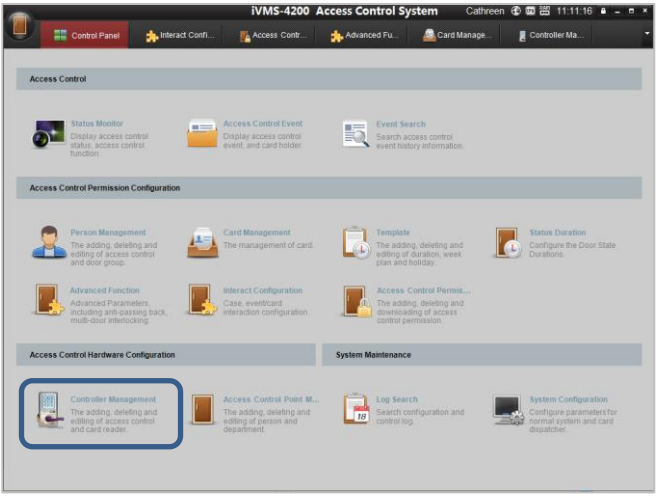


Figure 5-3 Control Panel Interface

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

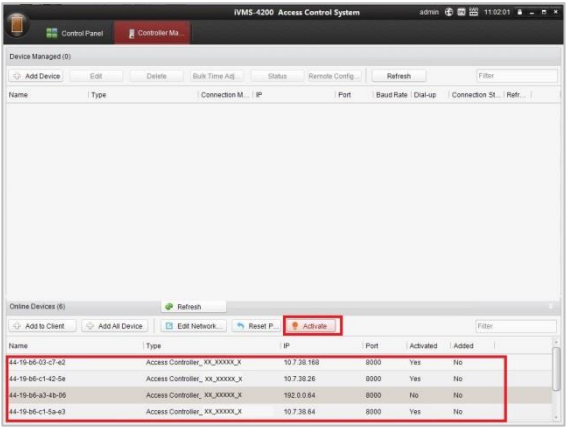


Figure 5-4 Device List

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 modifying the IP address manually.
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 activation notifying interface. For detailed information about activation, see Chapter 5.
- You should enter the default password for the first login.

  Enter **Sys Opt-Login Pwd** to reset the login password.

  The default password is 12345.

Steps:

1. The device enters the initial interface automatically after powered on.

Figure 6-1 Initial Interface

2. Enter [*] + [0] + [#] to enter the login interface

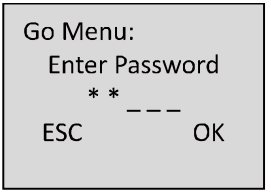


Figure 6-2 Login Interface

3. Enter the login password.

- Click 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

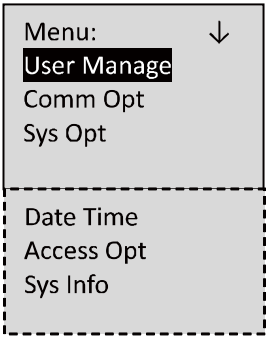


Figure 6-3 Menu Operation Interface

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 Manage** (user management) with the direction keys.
2. Click the **#** key to enter the adding user interface.

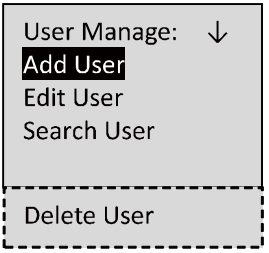


Figure 6-4 User Management Interface

6.1.2 Adding User

Purpose:

In the **Add User** menu, you can add users, and register card for the corresponding person.

Steps:

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

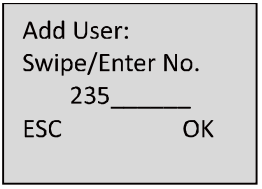


Figure 6-5 User Adding Interface

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.
4. After registering the card, select the permission template.

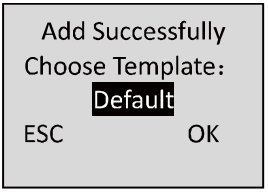


Figure 6-6 Template Selecting Interface

5. Click the **#** key to enter the password registration interface. If the password is registered, the card holder will be able to open the door with swiping card and entering password.

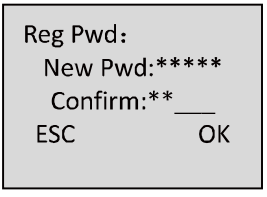


Figure 6-7 Password Configuring Interface

6. Register password.
   1) Enter a new password.
   2) Confirm the new password.
   3) Click the **#** key to confirm the settings.

NOTE The valid length of the password is 1 to 8 characters.

7. If the password registration is not required, click the # key to return to the Add User interface.

6.1.2 Editing User

Steps:

1. Move the cursor to **Edit User** by using direction keys on the user management interface.
2. Click the **#** key to enter the managing user interface.

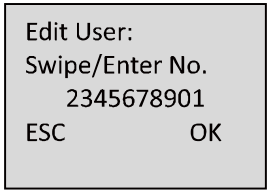


Figure 6-8 User Editing Interface

3. Swipe the card or enter the card No. .
4. Click the **#** key to enter the password settings interface.
    1) Move the cursor to **Change PWD** to enter the password changing interface.
    2) Enter a new password.
    3) Confirm the new password.
    4) Click the **#** key to confirm the settings.

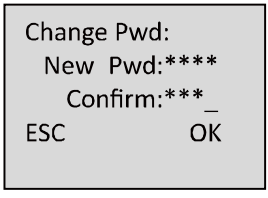


Figure 6-9 Password Changing Interface

5. If the password is not required, click the # key to clear the configured password.
6. Change the valid date

   You can set the valid date (start/end date) of the card.

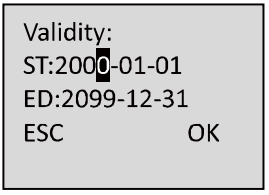


Figure 6-10 Validity Setting Interface

Click the **#** key to confirm the settings.

7. Enable the first card permission of the user.
   1) Click the **#** key to enter the editing mode.
   2) Press the direction key to select whether to enable the first card for the user.
   3) Click the **#** key to confirm the editing.

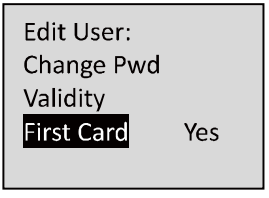


Figure 6-11 First Card Permission Setting Interface

NOTE

After enabling first card, the door remains open during the pre-defined valid duration.

8. Select the template for the user.
   1) Click the **#** key to enter the editing mode.
   2) Press the direction key to select the template No..

NOTE

Max.65 templates are selectable (including 64 schedule templates and 1 template disabling option) , the schedule template value is from **01** to **64**, and **Default** indicates the template 01. The template disabling option value is **00**.

   3) Click the **#** key to confirm the editing.

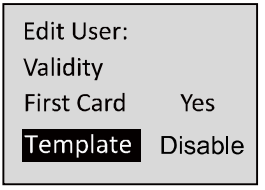


Figure 6-12 Template Settings Interface

6.1.3 Searching User

Steps:

1. Move the cursor to **Search User**.
2. Click the **#** key to enter the searching interface.

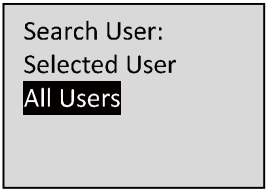


Figure 6-13 Searching User Interface

3. Select **All User** and the list of all user will be displayed.

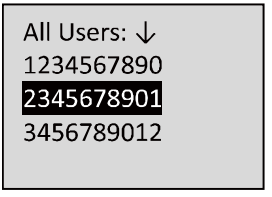


Figure 6-14 Searching for All User Interface

4. Select the **Selected User** to enter the query specified user interface.
5. Swipe card or enter the card No..

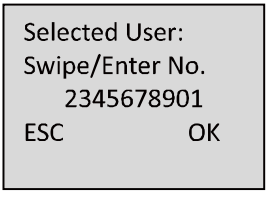


Figure 6-15 Searching for Selected User Interface

6. Click the **#** key to view the basic information about the card holder.

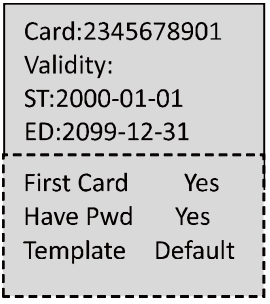


Figure 6-16 User Information Interface

6.1.4 Deleting the User

Steps:

1. Move the cursor to **Delete User**, and click the **#** key to enter the deleting interface.

Figure 6-17 User Deleting Interface

2. Swipe card or enter the card No..
3. Click the **#** key to enter the confirmation page.
4. Select whether to confirm the settings

NOTE

You can click * key to return to the main menu.

6.2 Communication Settings

Purpose:

On the communication settings interface, you can set network parameters,

Steps:

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

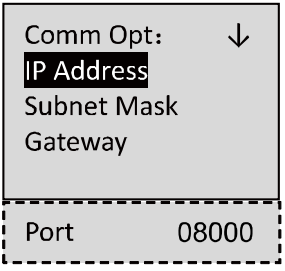


Figure 6-18 Network Settings Interface

NOTE The valid port No. range is from 2000 to 65535.

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

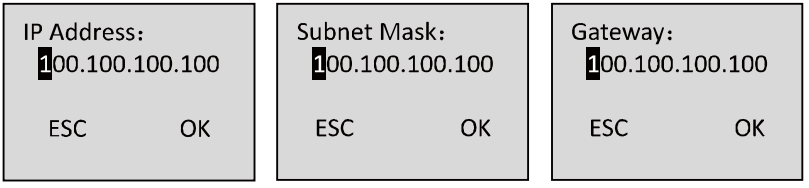


Figure 6-19 Network Settings Interface

4. Edit the port No. of the terminal.
5. Click the **#** key to complete the settings.

6.3 System Settings

Steps:

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

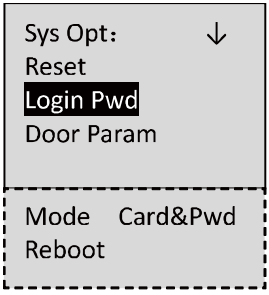


Figure 6-20 System Settings Interface

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

Login Pwd (Login Password): Change the login password.

Door Param (Door Parameters): Set parameters of the access control terminal, including Open Time (Door Action Time), Open Time-out(Delayed Door Alarm), Door Magnetic (Door Magnetic Status Settings), Button Type (Exit Button Status Settings), and First Card settings.

Mode (Authentication Mode): You can select the card authentication mode.

Reboot (Reboot Device): You can reboot the device

6.3.1 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. Click the **#** key to enter the restore settings interface.

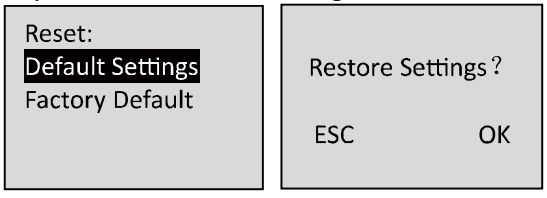


Figure 6-21 Restore Settings Interface

3. Select 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 defaults settings, parameters, excluding network parameters and event parameters, are returned to the factory defaults.

4. Click the **#** key to implement the settings.

6.3.2 Setting login Password

Steps:

1. Click the **#** key to enter the password settings interface.

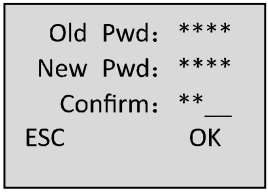


Figure 6-22 Password Changing Interface

1) Enter the old password.
2) Enter a new password.
3) Confirm the new password.

NOTE The valid password length should be 5 characters.

2. Click the **#** key to confirm the settings.

6.3.3 Door Settings

Purpose:

On the door settings interface, you can set door parameters, including Open Time (Door Action Time), Open Time-out (Delayed Door Alarm), Door Magnetic (Door Magnetic Status Settings), Button Type (Exit Button Status Settings), and First Card settings.

Steps:

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

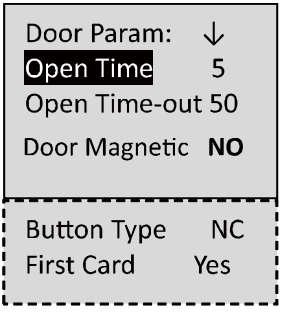


Figure 6-23 Door Settings Interface

3. Edit door parameters.

   Open Time: Door action time, set the door action time: 1 ~ 255 s.

   Open Time-out : Delayed door alarm, set the delayed door alarm threshold: 0 ~ 255s.

   Door Magnetic: Door magnetic status settings, Remain open and remain closed are selectable.

   Button Type: Exit button status settings, Remain open and remain closed are selectable.

   First Card: Set whether to enable the first card function, which is keeping the door open with the first card.

4. Click the **#** key to confirm the settings.

6.3.4 Settings Authentication Mode

In this section, you can set the controller authentication mode for opening the door, that is, **Card Only**, and **Card & Password**.

Steps:

1. Move the cursor to **Mode** (Authentication Settings) by using direction keys in the system settings interface.

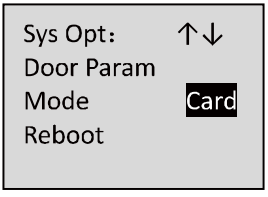


Figure 6-24 Authentication Settings Interface

2. Click the **#** key to select the authentication mode.

6.3.5 Rebooting Device

Steps:

1. Move the cursor to **Reboot** by using direction keys
2. Click the **#** key to start the rebooting operation of the device.

6.4 Time Settings

Steps:

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

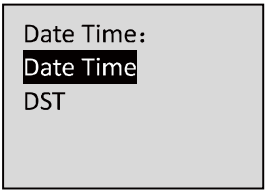


Figure 6-25 Time Settings Interface

3. Select to edit the Edit **Date Time** or **DST (Daylight Saving Time)** parameters of the device.
   - Edit **Date Time:**

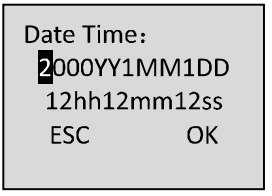


Figure 6-26 Date Time Settings Interface

   - Edit **DST (Daylight Saving Time)**

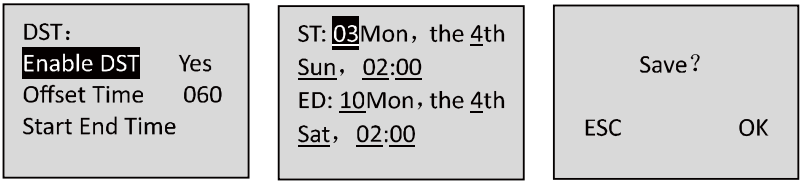


Figure 6-27 DST Settings Interface

When enabling DST, you should set the offset time, the start time, and the end time of DST.

NOTE

- Press * key to cancel the date/time settings, and return to the **Date Time** interface.
- Press # key to confirm the date/time settings, and return to the **Date Time** interface.

6.5 Permission Settings

Purpose:

On the permission settings section, you can set the weekly schedule, holiday schedule, Holiday group and template.

Steps:

1. Move the cursor to **Access Opt** (Access Operation) by using direction keys.
2. Click the **#** key to enter the interface.

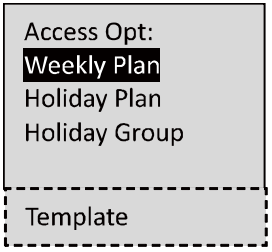


Figure 6-28 Permission Settings Interface

Weekly Schedule Settings

Steps:

1. Move the cursor to **Weekly Plan** by using direction keys.
2. Click the **#** key to enter the weekly schedule configuration interface.

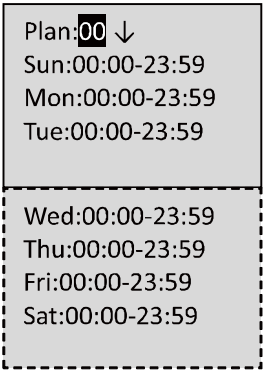


Figure 6-29 Weekly Schedule Settings Interface

3. Set the plan No., with entering the plan No. by the numeric keys.
   Max. 32 plans can be configured, and the plan No. range is from 1 to 32.
4. Set the detailed time periods from Sunday to Saturday with entering the start time and end time by the numeric keys.
5. Click the ***** key to return to the **Access Opt** interface.

Holiday Schedule Settings

Steps:

1. Move the cursor to **Holiday Plan** by using direction keys.
2. Click the **#** key to enter the holiday schedule configuration interface.

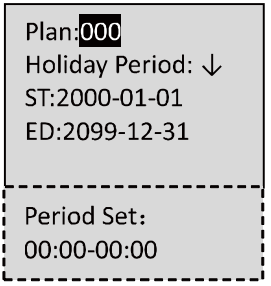


Figure 6-30 Holiday Schedule Settings Interface

3. Set the plan No., with entering the plan No. by the numeric keys.
   Max. 128 plans can be configured, and the plan No. range is from 1 to 128.
4. Set the detailed holiday information.
   Date: Enter the start date and end date by the numeric keys.

Period: Enter the start time and end time by the numeric keys.

5. Click the * key to return to the **Access Opt** interface.

Holiday Group Settings

Steps:

1. Move the cursor to **Holiday Group** by using direction keys.
2. Click the # key to enter the holiday group configuration interface.

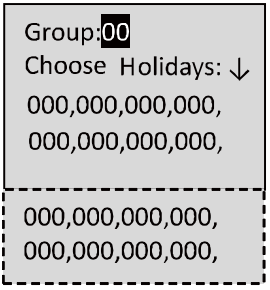


Figure 6-31 Holiday Group Settings Interface

3. Set the group No., with entering the group No. by the numeric keys.
   Max. 64 groups can be configured, and the group No. range is from 1 to 64.
4. Set the holiday group. Move the cursor to holiday No.(the default is 000), and
   Enter the holiday No. configured in **Holiday Schedule Settings** by the numeric keys.
   The holiday schedule No. is separated by a comma.
5. Click the * key to return to the **Access Opt** interface.

Template Settings

Steps:

1. Move the cursor to **Template** by using direction keys.
2. Click the # key to enter the template configuration interface.

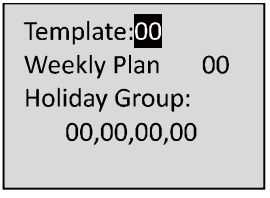


Figure 6-32 Template Settings Interface

3. Set the template No., with entering the template No. by the numeric keys.
   Max. 64 templates can be configured, and the template No. range is from 1 to 64.
4. Enter the Weekly Plan No. by the numeric keys.
5. Set the Holiday groups. Move the cursor to holiday group No.(the default is 000), and Enter the holiday group No. configured in **Holiday Group Settings** by the numeric keys.
   The holiday group No. is separated by a comma.
6. Click the ***** key to return to the **Access Opt** interface.

6.6 System Information

Steps:

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

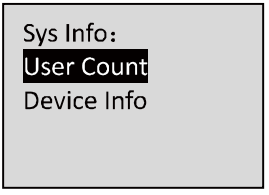


Figure 6-33 System Information Interface

3. Select **User Count** or Device **Information**.

- **User Capacity**

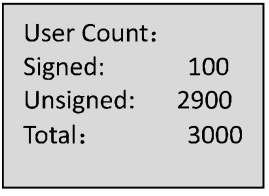


Figure 6-34 User Count Interface

Registered Amount: the count of user that is registered
Remainder Amount: the count of remainder registration amount
Total Amount: It refers to the maximum amount of cards

The default maximum card amount is 2000.

- **Device Information**

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

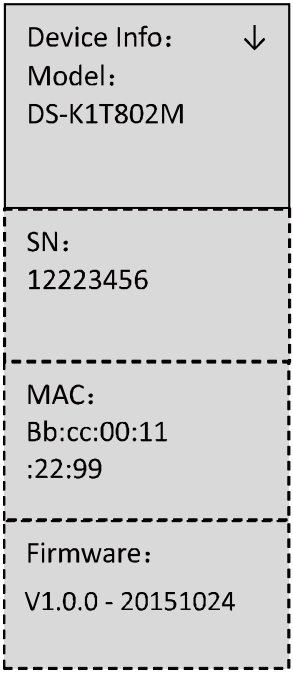


Figure 6-35 Device Information Interface

7 Client Operation

7.1 Overview of Access Control System

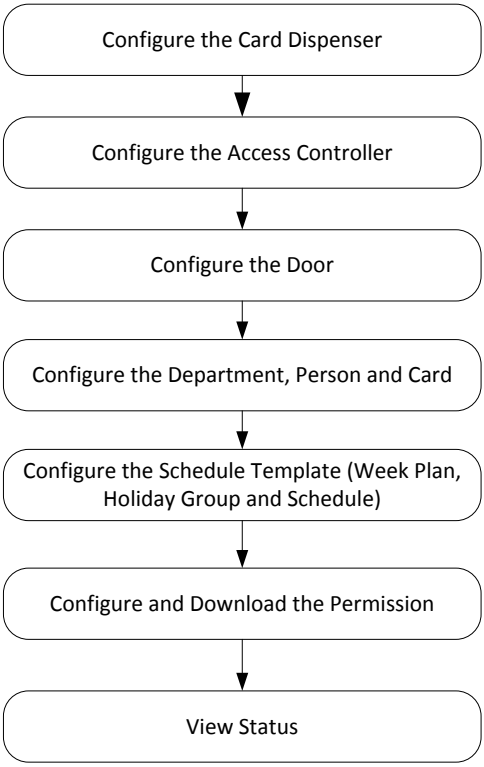
7.1.1 Description

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

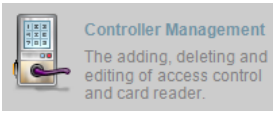
Refer to the following flow chart for the configuration order.


Configure the Card Dispenser
Configure the Access Controller
Configure the Door
Configure the Department, Person and Card
Configure the Schedule Template (Week Plan, Holiday Group and Schedule)
Configure and Download the Permission
View Status

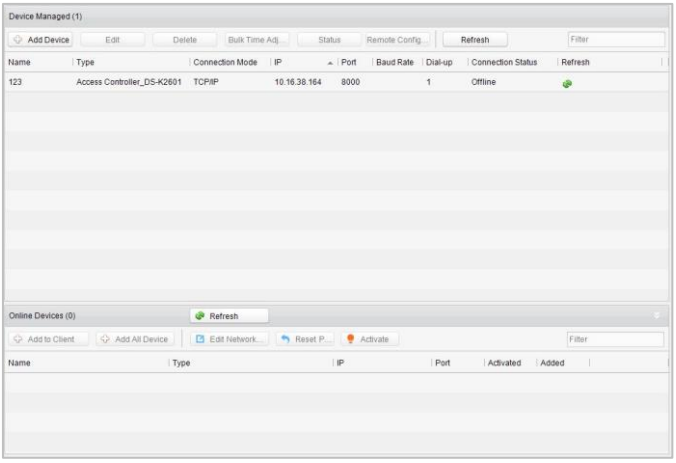
7.2 Device Management

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.

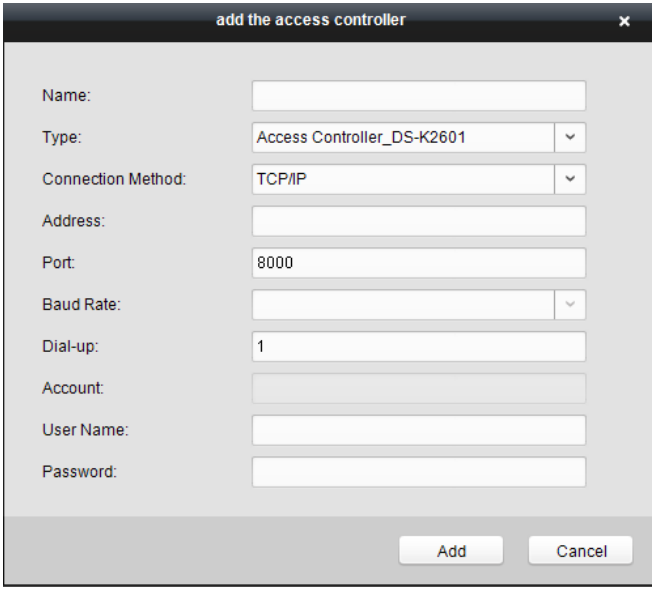
The control client can manage 100 access controllers at most.

Device Management

Adding Controller

Steps:

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



2. Input the device name.
3. Select the access controller type in the dropdown list.
4. Select the connection mode in the dropdown list: TCP/IP, or COM port, 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.

NOTE For the detailed information about the account, refer to 15.1.3.

6. Click the Add button to finish adding.

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

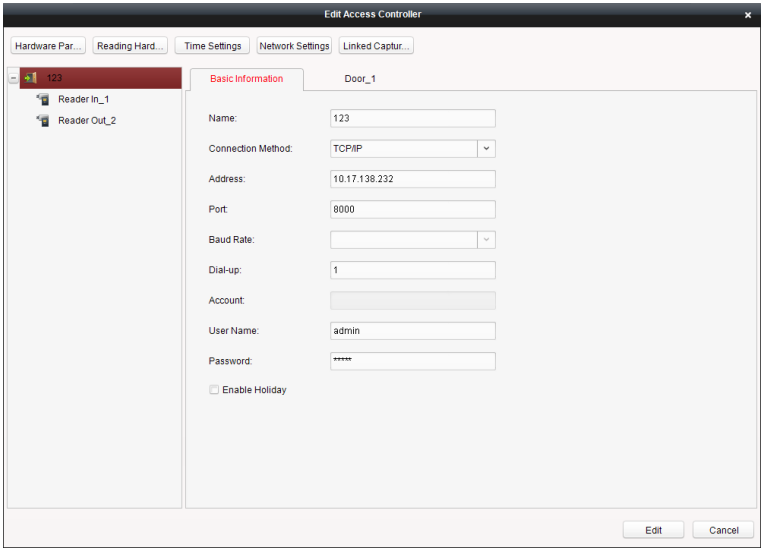
Editing Device (Basic Information)

Purpose:

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

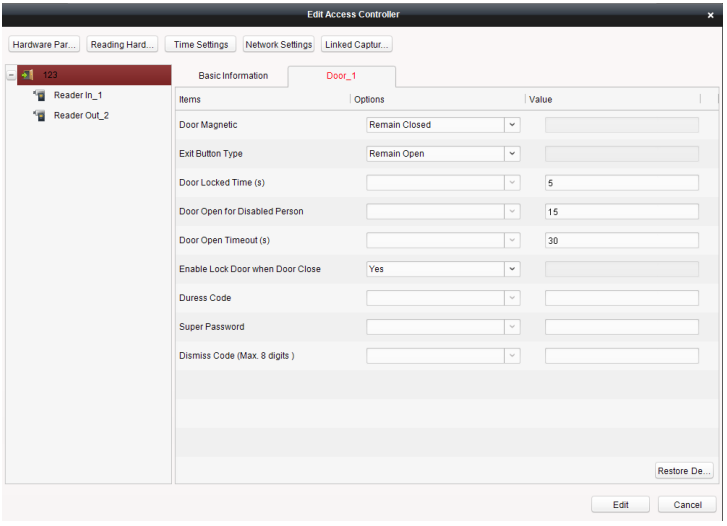
Steps:

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



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

Editing Device (Door Information)



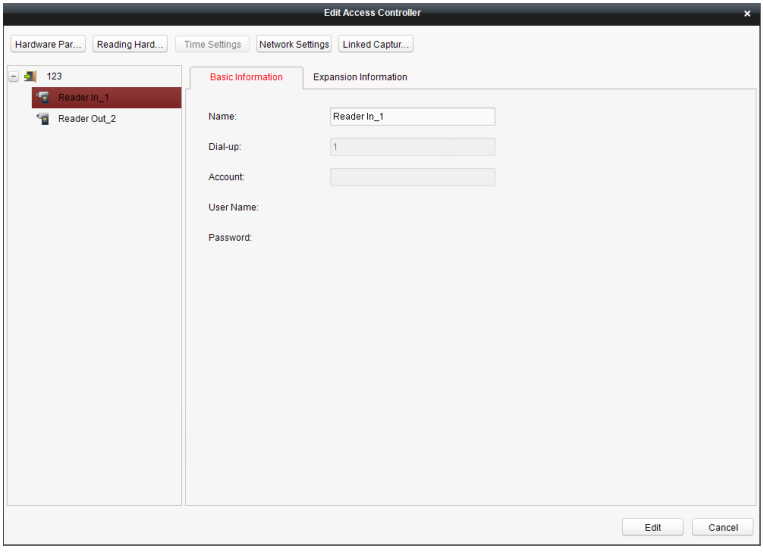
Steps:

1. In the editing interface, click the **Door_1** button to edit the information of the selected door.
   1) **Door Magnetic**: The Door Magnetic 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 magnetic 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:

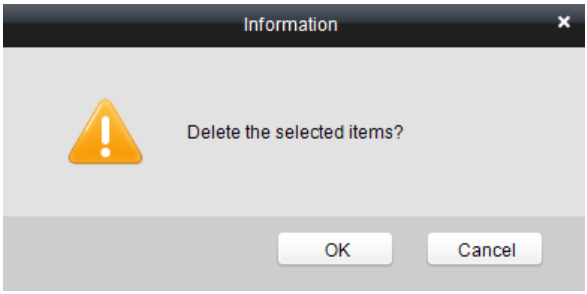
1. In the device list, select a card reader name to enter into the card reader information editing interface.
2. Click the **Basic Information** button to edit the basic information about the card reader.
3. Click the **Expansion Information** button to edit the expansion information about the card reader.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

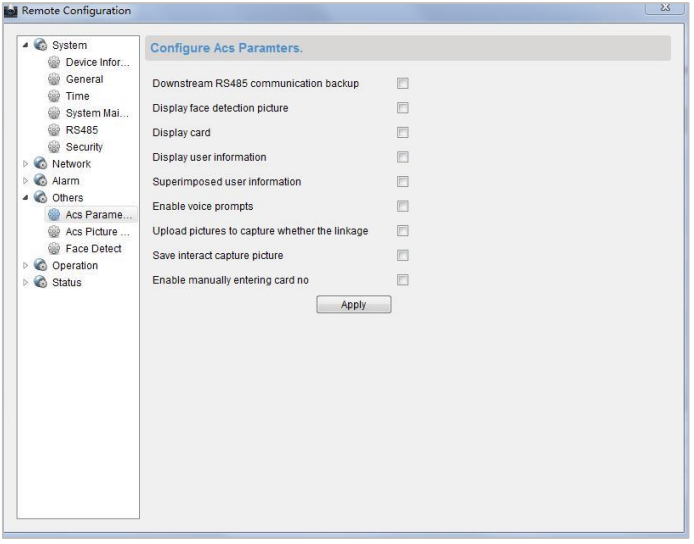
Status

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

1) **Door Status**: The status of the connected door.
2) **Host Status**: The status of the host, including Storage Battery Power Voltage, Device Power Supply Status, and 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.

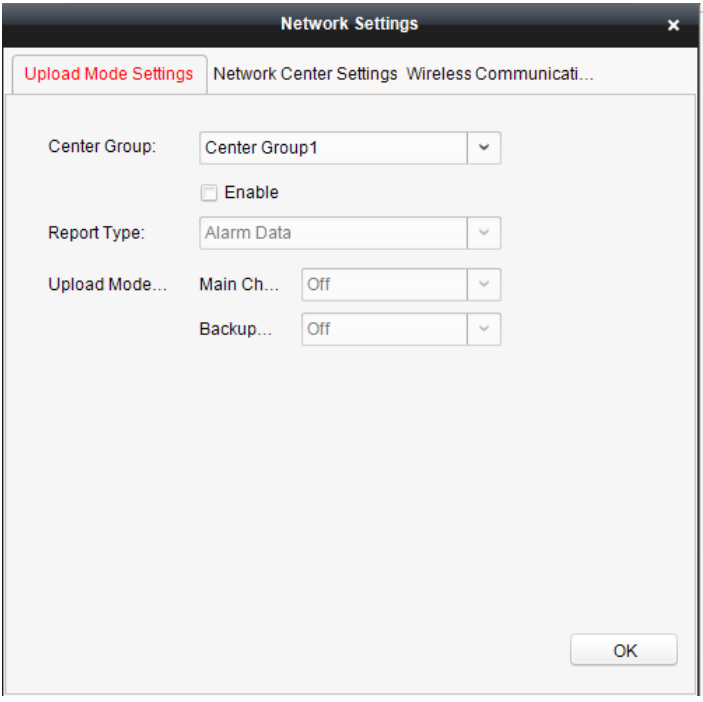


Network Settings

Purpose:

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

Uploading Mode Settings



Steps:

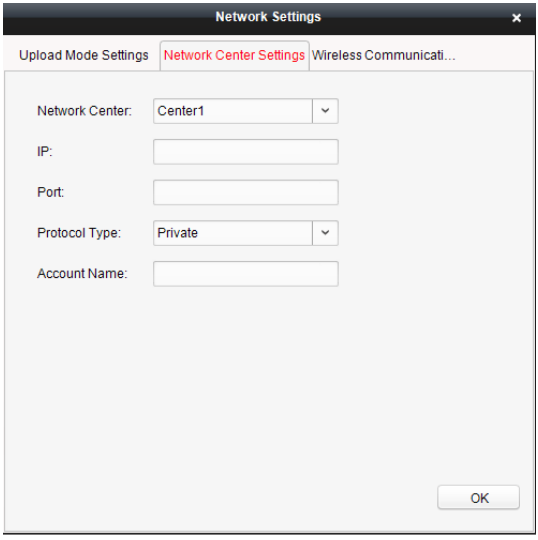
1. In the access controller editing interface, click **Network Settings** button to enter the network settings interface.
2. Click the **Uploading Mode Settings** button.
3. Select the center group in the dropdown list.
4. Tick the **Enable** to enable the selected center group.
5. Select the report 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:

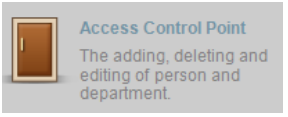
1. In the access controller editing interface, click **Network Settings** button to enter the network settings interface.
2. Click the **Network Center Settings** button.
3. Select the network center in the dropdown list.
4. Input IP address.
5. Input port number.
6. Select the protocol type.
7. Set an account name for the network center. A consistent account should be used in one platform.
8. Click the **OK** button to save parameters.

NOTE

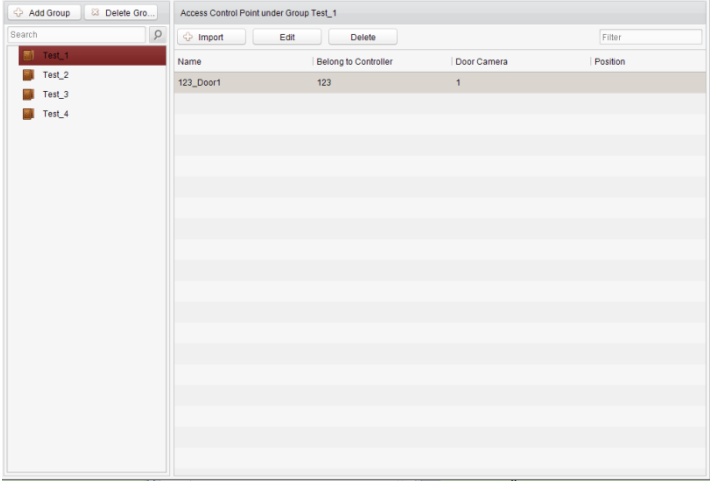
- In the Ehome protocol, the default port number is 7661, and the port type should be UDP port. Related settings files need modifying if the port type does not match.
- The port number of the wireless network and wired network should be consistent with the port number of Ehome.

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.

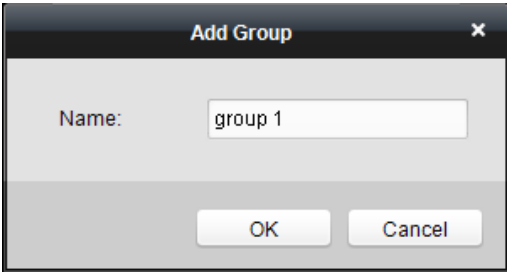
Group Management

- **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 OK 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 Delete Group 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 Import button to pop up the access control point importing interface.
2. Select a access control point to import by clicking it.
3. Click to select a group in the right side bar to import to.

4. Click Import button to import the selected access control points or click Import All to import all the available access control points.

NOTE

- 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 Edit button to edit the access control point.
2. Edit the Door Name and Position.
3. Click OK button to finish editing.

NOTE

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

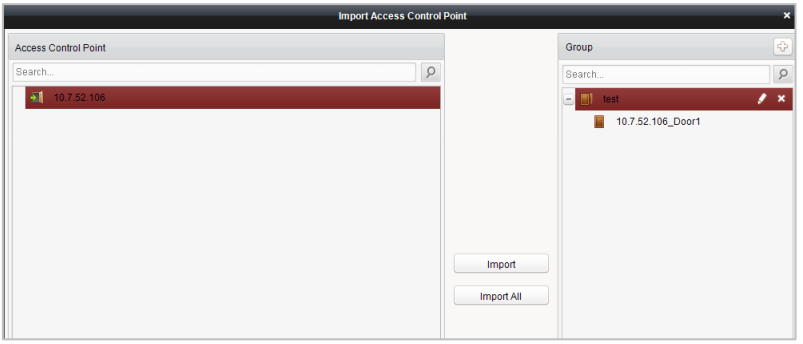
- **Deleting Access Control Point**

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 Delete button.
- Click to select a group in the group list, and click Delete 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

Uou can also edit/delete a door on the Import Access Control Point panel.



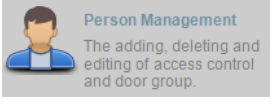
Steps:

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

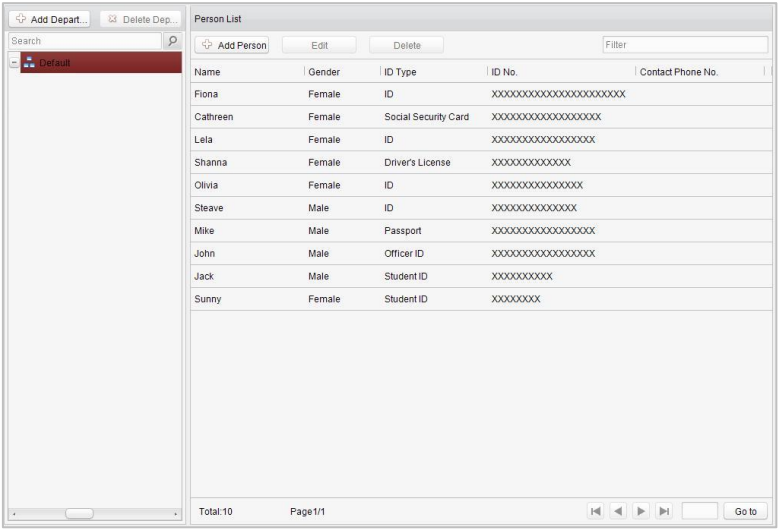
7.3.1 Person Management

Interface Introduction

Click the 

icon on the control panel of the software.

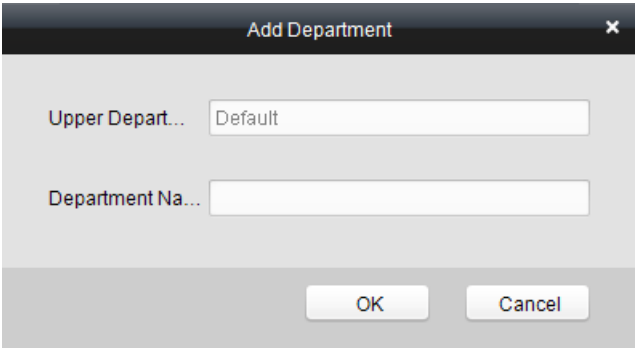
Adding, editing, deleting and filtering of the department and person are supported in this interface.



Department Management

Steps:

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



NOTE

- Multi-level department system can be created. Click a department as the upper-level deparment and click Add Depart... 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 Delete Depa... button to delete it.

NOTE

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

Person Management

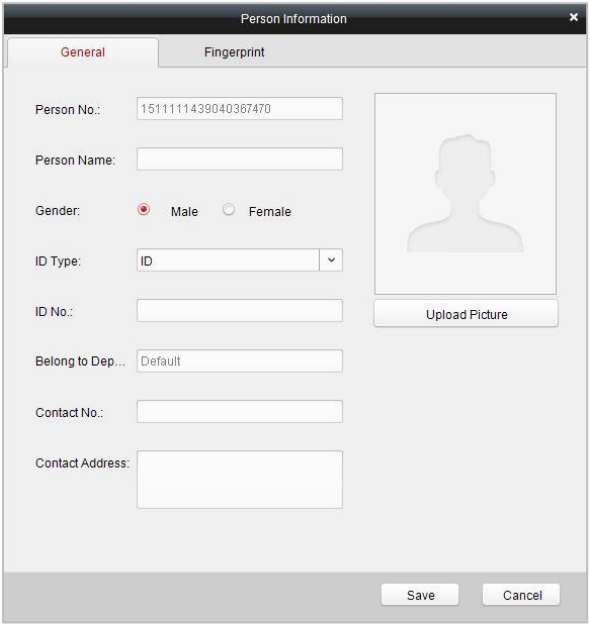
NOTE

- In the person management interface, double-click the person name or click the Edit button to edit the person informationt
- In the person management interface, click the **Delete** button to delete the person.
- Up to 2000 persons ban be added.

- **Inputting General Information**

Steps:

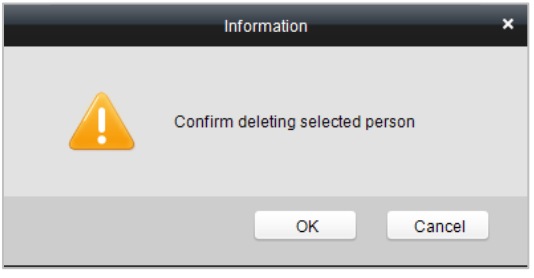
1. Select a department in the list and click the Add Person in the person information list to pop up the adding person interface.



2. Input the Person Name (required), Gender, ID Card, etc., upload the photo of the person and click the Save icon to finish adding.

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

3. You can double-click an added person to edit its information.
4. You can click to select a person, and click the Delete button to delete it.

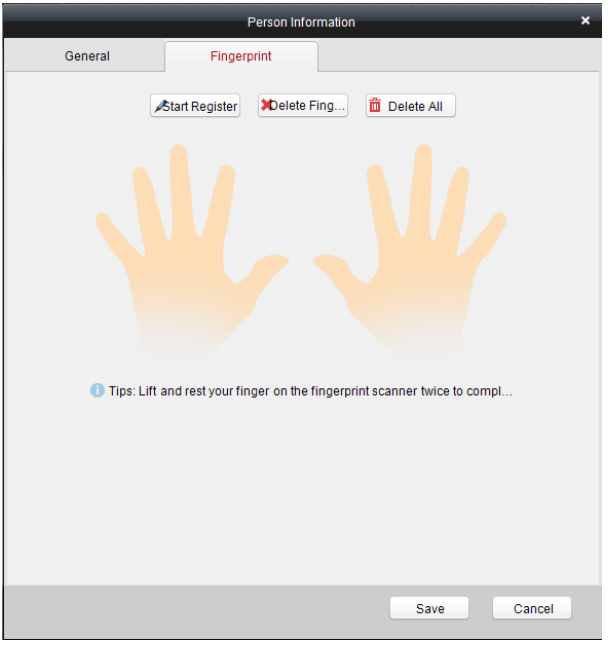


If a card is associated with the current person, the association will be invalid after the person is deleted.

- **Inputting Fingerprint**

Steps:

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



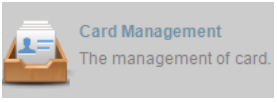
2. Click the **Start Register** button, and select the fingerprint to be input.
3. Click the **Save** button to save the parameter.

NOTE

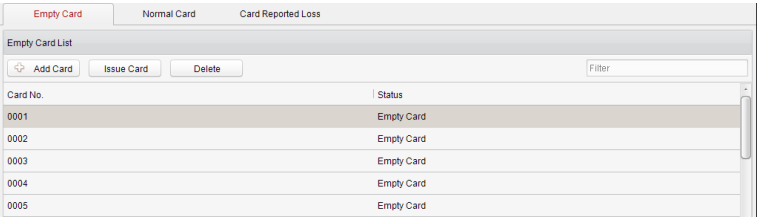
- Click the **Delete Fingerprint** button to delete the fingerprint.
- Click the **Delete All** button to clear all fingerprints input.
- Models DS-K1T802M and DS-K1T802E do not support fingerprint function.

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.

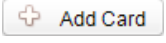
Blank Card

- **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.

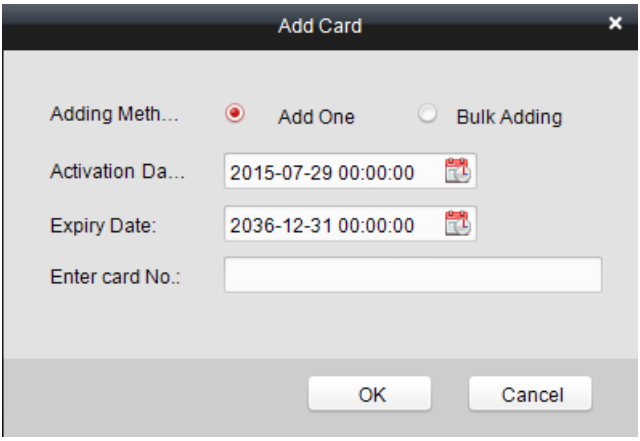
Steps:

1. Click the 

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

   Adding Single Card

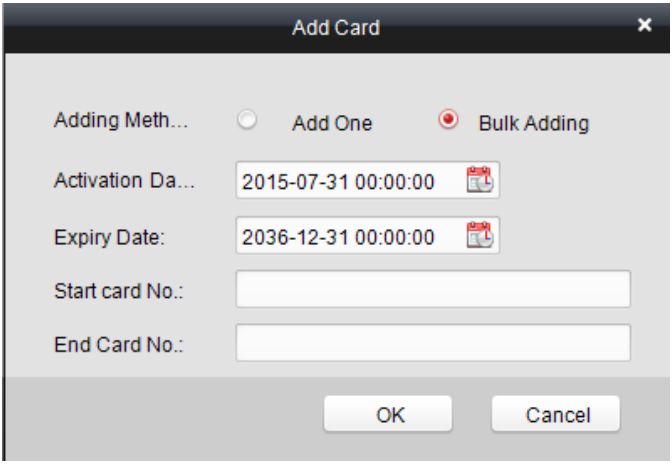
   Choose the Single Add as the adding mode by clicking the to and input the Start Date, Expiring Date and Card No. in the text field.



Batch Adding Cards

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

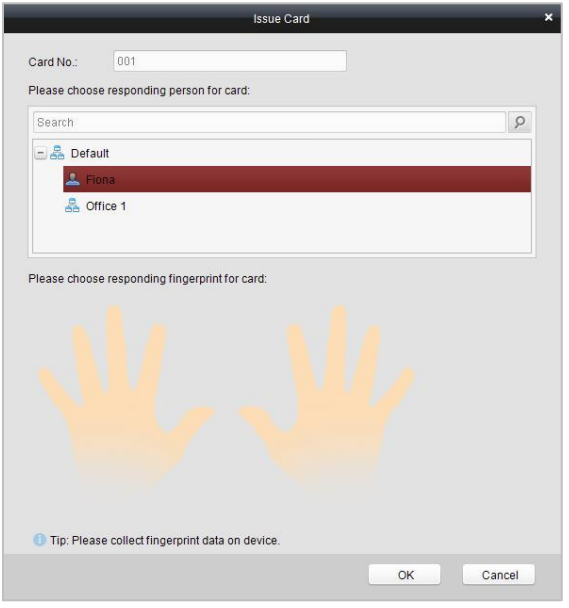
NOTE The start card No. and the last card No. should be the with same length. E.g., the last card No. is 234, then the start card No. should be like 028



3. Click the OK button to finish adding.
4. Click an added blank card in the list and click Issue Card 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 OK to finish.

NOTE

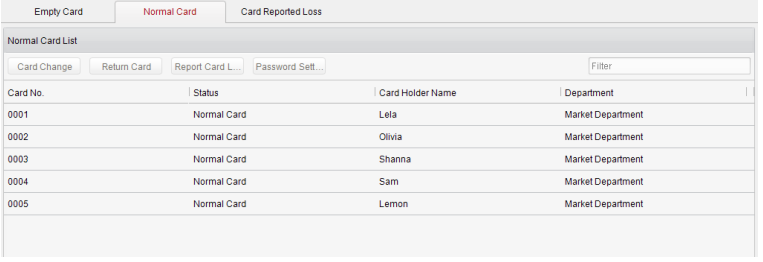
- The issued card will disappear from the Blank Card list, you can check the card information in the Normal Card list.
- Up to 2000 cards can be added.
- Models DS-K1T802M and DS-K1T802E do not support fingerprint function.
-

- **Deleting Card**

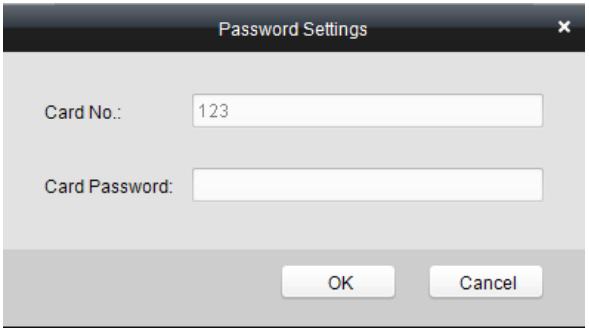
You can click an added blank card in the list and click Delete button to delete the selected card.

Normal Card

Click the Normal Card tab in the card managemet 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.



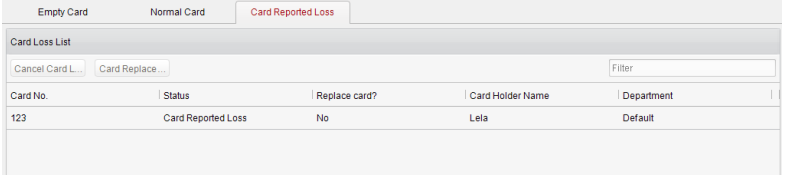
- Click to select a card and click the **Card Change** button to change the associated card for card holder. Select another card in the popup window to replace the current card.
- Click to select an issued card and click the **Return Card** button to cancel the assotiation of the card, then the card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



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

Lost Card

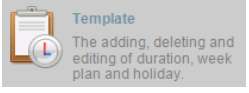
Click the Card Reported Loss tab in the card managemet interface to show the Lost Card list. You can view all the lost card information, including card No., card holder, and the department of the card holder.



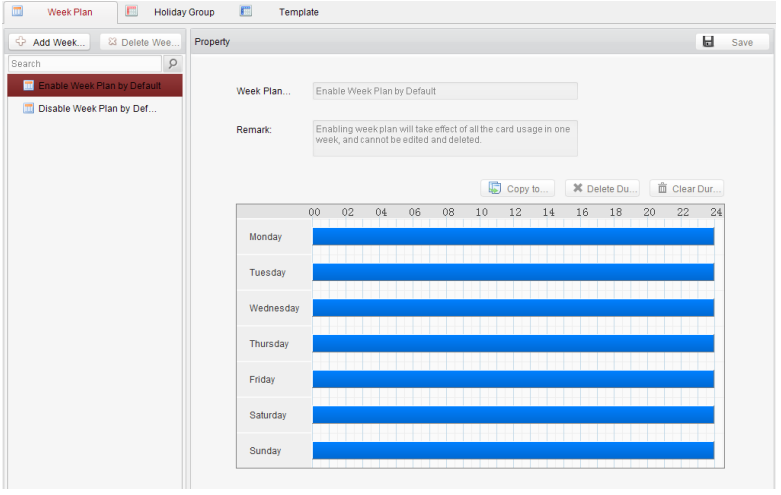
- Click the **Cancel Card Loss** button to resume the card to the normal card.
- Click the **Card Replacement** button to issue a new card to the card holder replacing for the lost card. Select another card in the popup window as the new card and the predefined permissions of the lost card will be copied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

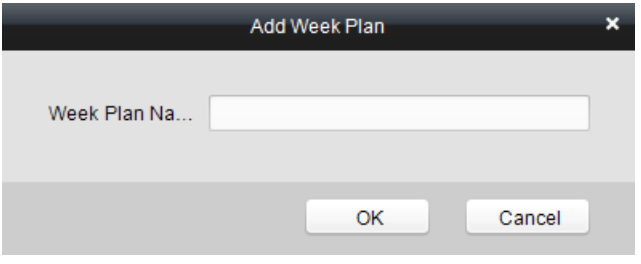
Setting Week Plan

- **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 cofigured 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.

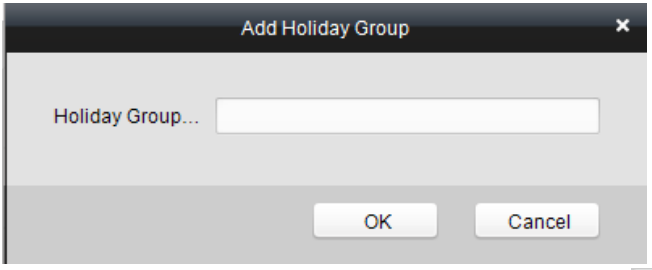
- **Deleting Week Plan**
  - Click to select a configured duration and click the **Delete Duration** button to delete it.
  - Click the **Clear Duration** button to clear all the configured durations, while the week plan still exists.
  - Click the **Delete Week Plan** button to delete the week plan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

Setting Holiday Group

- **Adding Holiday Group**

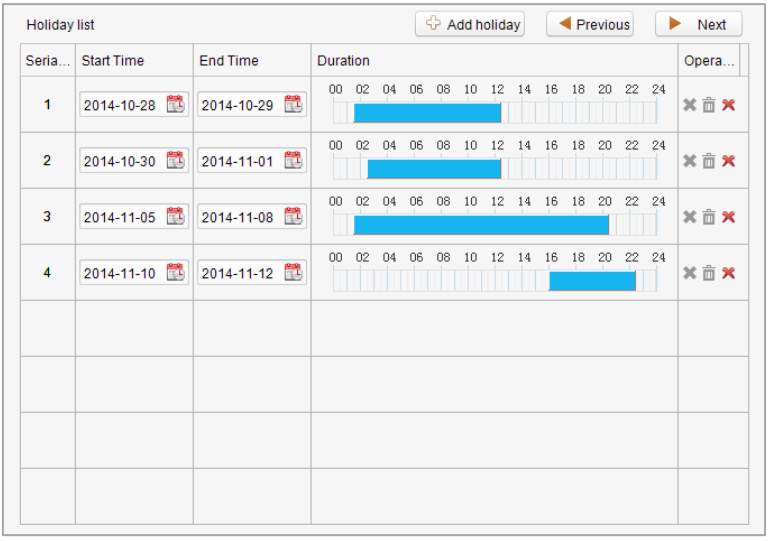
Steps:

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 field and click the OK button to add the holiday group.
3. Click the Add holiday icon to add a holiday in the holiday list and configure the duration of the holiday.

NOTE At most 16 holiday periods can be added.



1) Click and drag your mouse on a day to draw a blue bar on the schedule, which means in that duration, the cofigured 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 Save button to save the settings.

NOTE The holidays cannot be overlapped with each other.

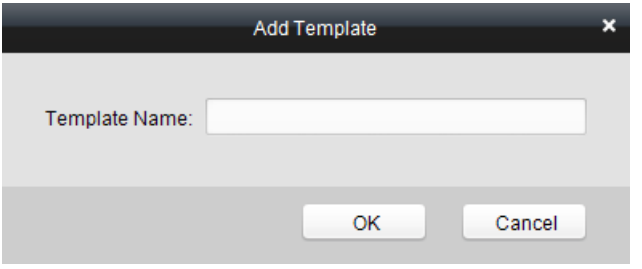
Setting Schedule Template

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.

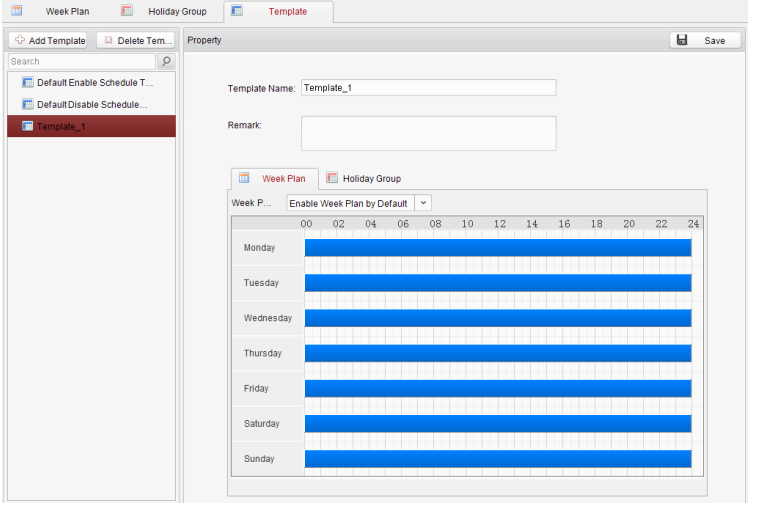
NOTE The priority of holiday group schedule is higher than the week plan.

Steps:

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

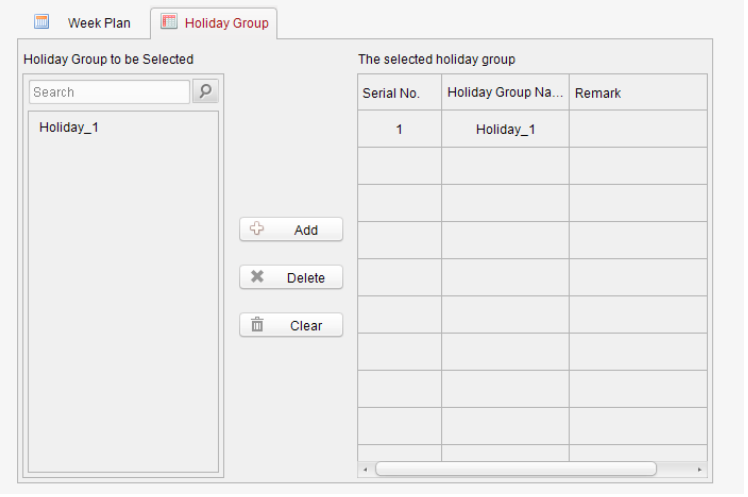


2. Input the name of schedule in the text field, and click the OK button to add the schedule.
3. Select a week plan you want to apply to the schedule.
   Click the Week Plan tab and select a plan in the dropdown list.



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

NOTE At most 4 holiday groups can be added.



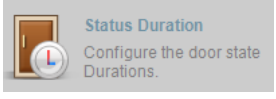
- Click to select a holiday group in the left-side list and click the Add to add it.
- Click to select an added holiday group in the right-side list and click the Delete to delete the it.
- Click the Clear to delete all the added holiday groups.

5. Click the Save button to save the settings.

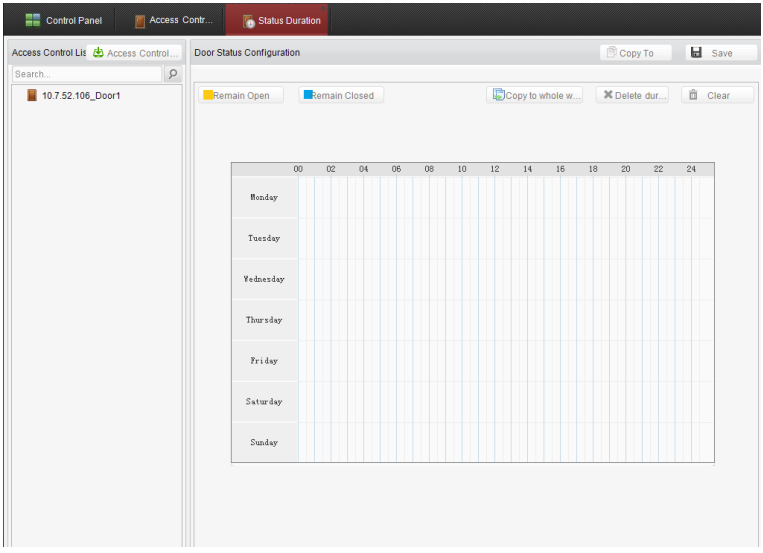
7.3.4 Door Status Management

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:

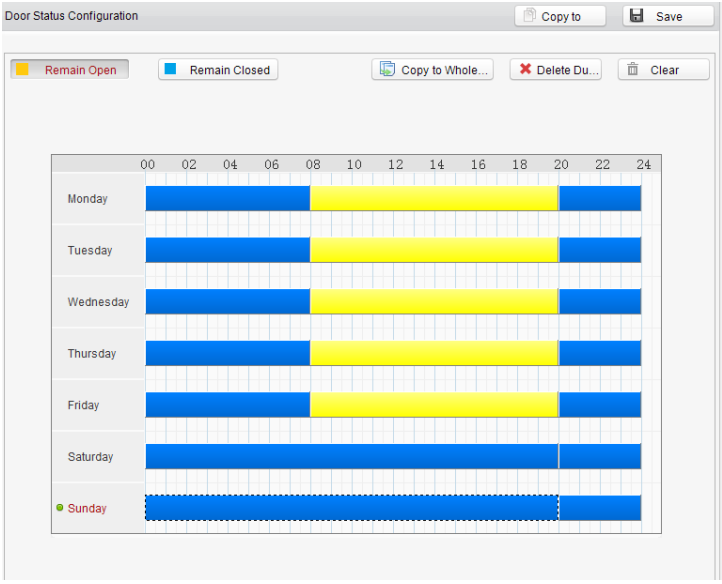
1. Enter the Door Status Management page.
2. Click and select a door from the door list on the left side of the page.
3. Draw a schedule map.
   1) Select a door status brush

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.

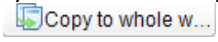
   2) Click and drag the mouse to draw a color bar on the schedule map to set the duration.



Notes

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

Steps:

1. Select a day which has already been configured.
2. Click on 

to copy the time periods to the whole week.

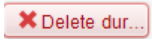
4. Edit the schedule map.

- **Edit Duration:**

  Click and drag the color bar on the schedule map and you can move the bar on the time track.

  Click and drag the mouse on the ends of the color bar and you can adjust the length of the bar.

- **Delete a Duration:**

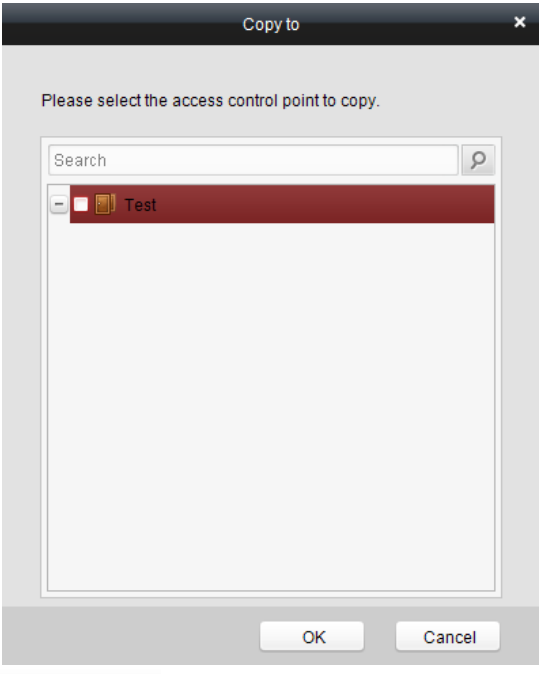
  Click and select a color bar and click 

to delete the time period.

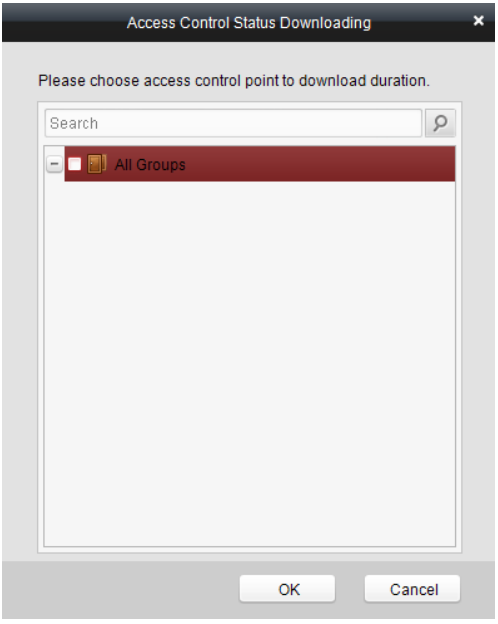
- **Clear All Durations:**

Click Clear to clear all configured durations on the schedule map.

5. Click on Save to save the settings.
6. You can copy the schedule to other doors by clicking on Copy To and select the required doors.

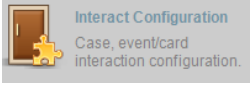


7. Click on Access Control... to enter the Download Door State page.

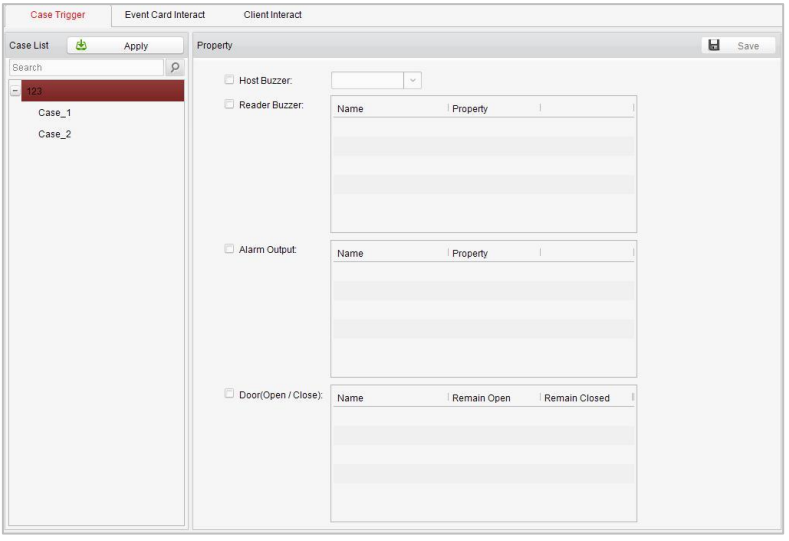


8. Select a control point and click **OK** to download the settings to the system.

7.3.5 Interact Configuration

Click 

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



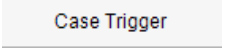
In this interface, you can set alarm linkage modes of the access host, including case trigger, event card interact, and client interact.

Case Trigger

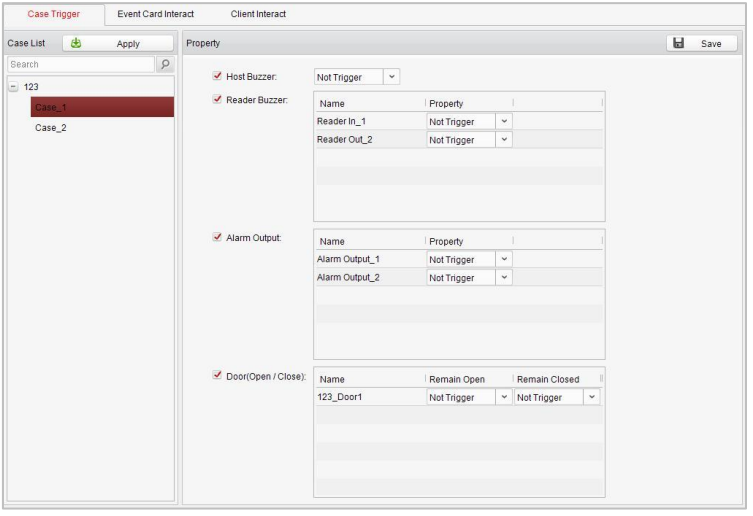
Purpose:

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.

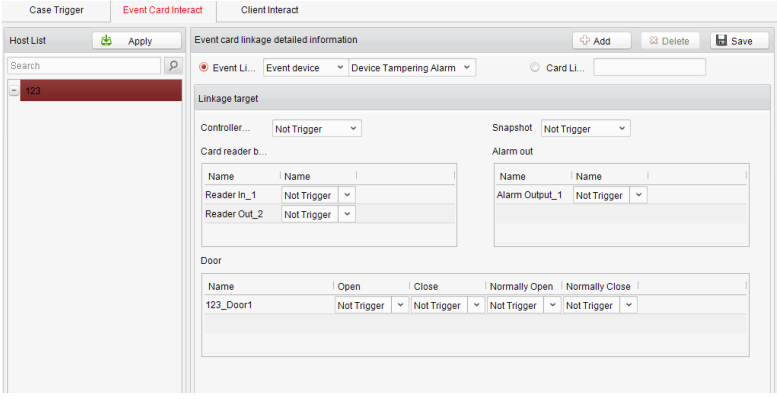
- **Event Linkage**

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

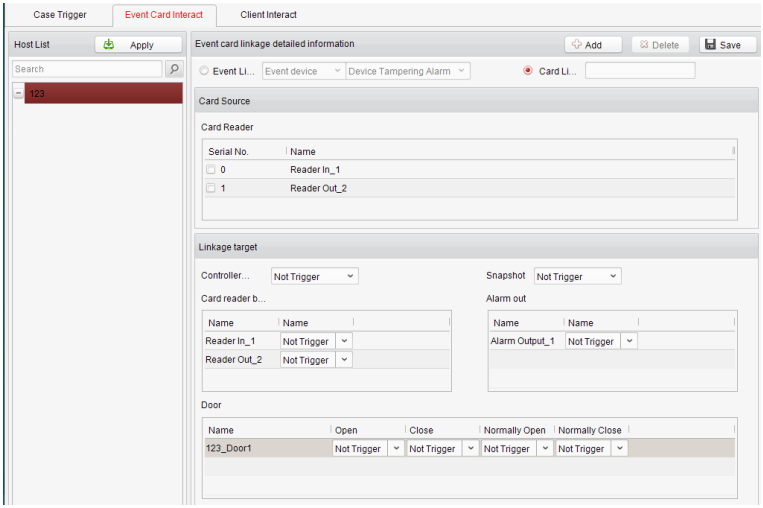
- The door status of open, close, normally open, and normally close cannot be triggered at the same time.
- Models DS-K1T802M and DS-K1T802E do not support the snapshot function.

- **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.

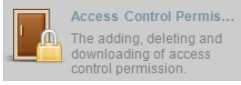
   Alarm Output: The alarm output will be triggered for notification.

   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.

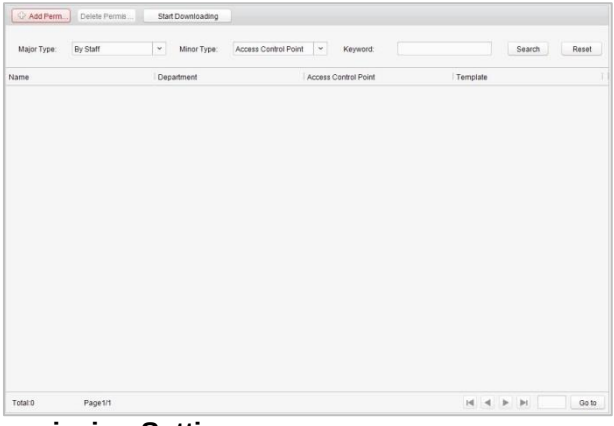
NOTE

- The door status of open, close, normally open, and normally close cannot be triggered at the same time.
- Models DS-K1T802M and DS-K1T802E do not support the snapshot function.

7.3.6 Access Permission Configuration

Click the 

icon on the control panel to enter the interface.

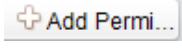


Access Permission Settings

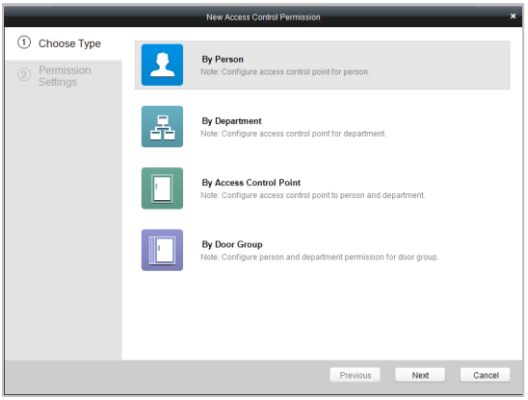
Purpose:

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

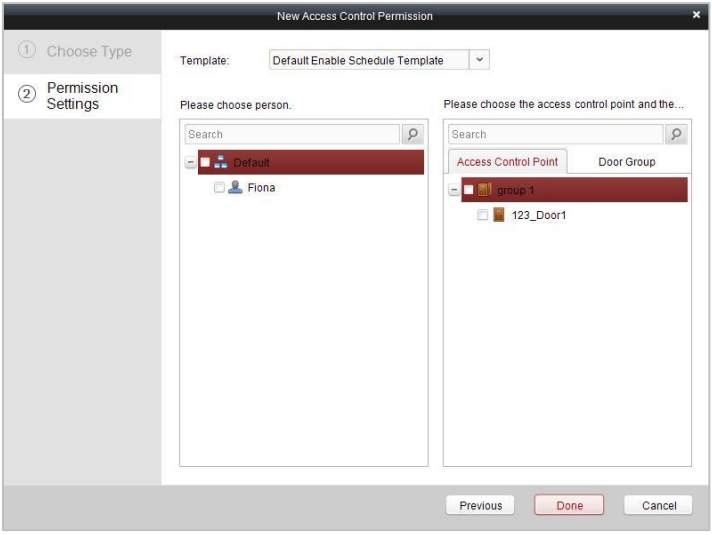
Steps:

1. Enter the **Permission** page.
2. Click on 

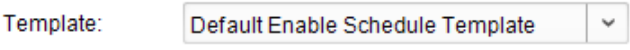
icon on the upper-left side of the page to enter the **Add Permission** page.



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.



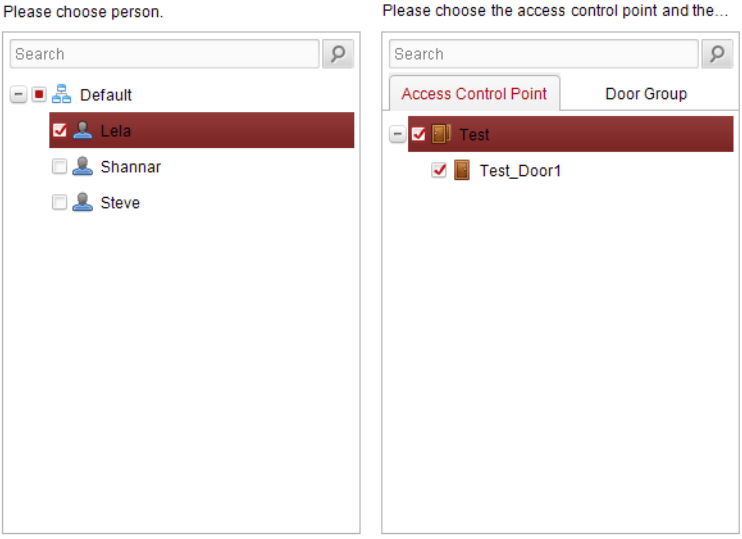
5. Click on the dropdown menu to select a schedule template for the permission.



NOTE

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

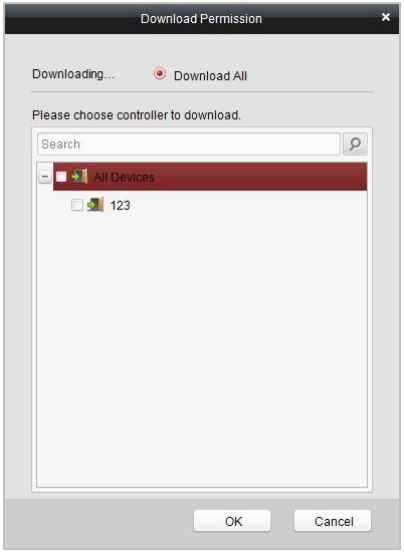
6. Select people/ department and corresponding doors/door groups from the appropriate lists.



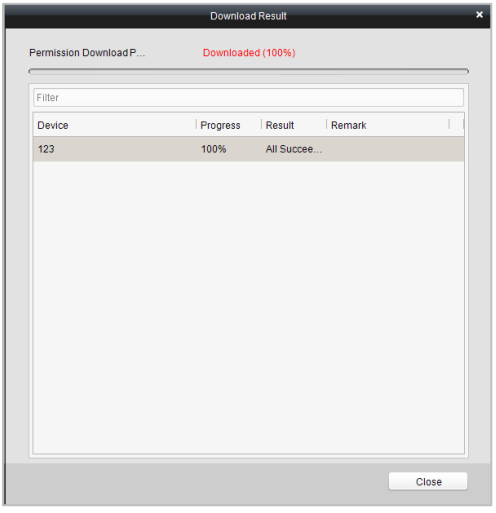
NOTE

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

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



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



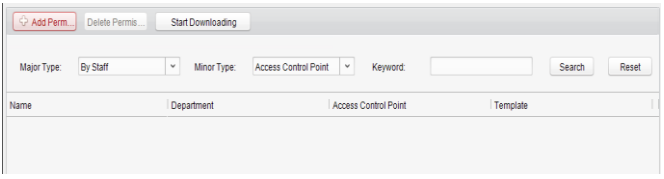
Access Permission Searching

Purpose:

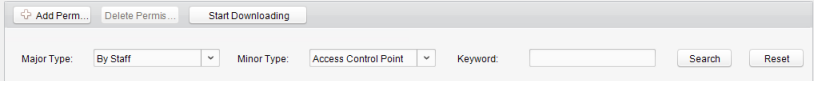
After the permission settings being completed, you can search and view permission assigning condition on the searching interface.

Steps:

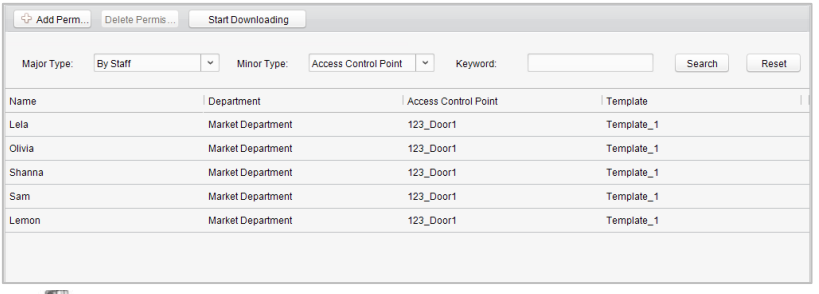
1. Enter the **Permission** page.



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



3. Click **Search** to get the search results.

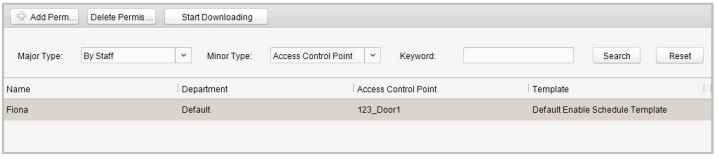


NOTE You can click **Reset** on the search criteria panel to clear all the displayed search results.

Permission Deleting

Steps:

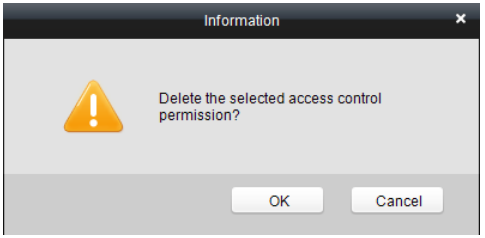
1. Follow steps 1-3 in the Permission Searching section to search for the permission needs to be deleted.
2. Select the permission from the results list.



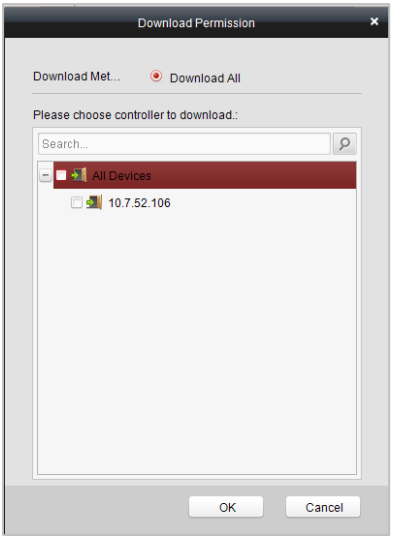
NOTE

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.

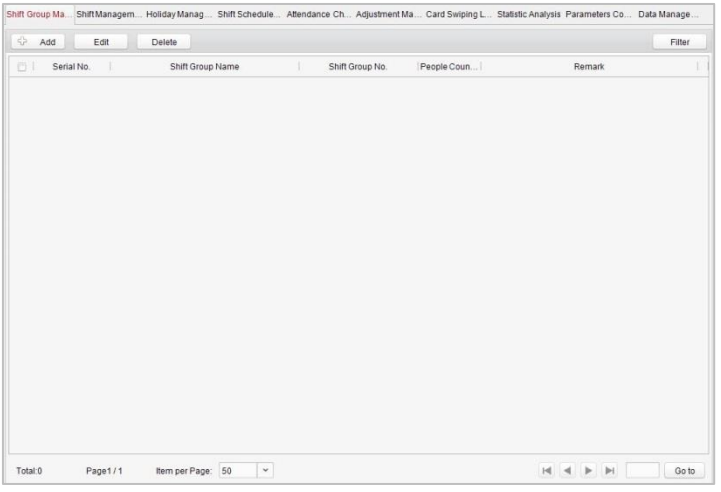
7.3.7 Attendance Management

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.

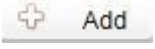


Shift Group Management

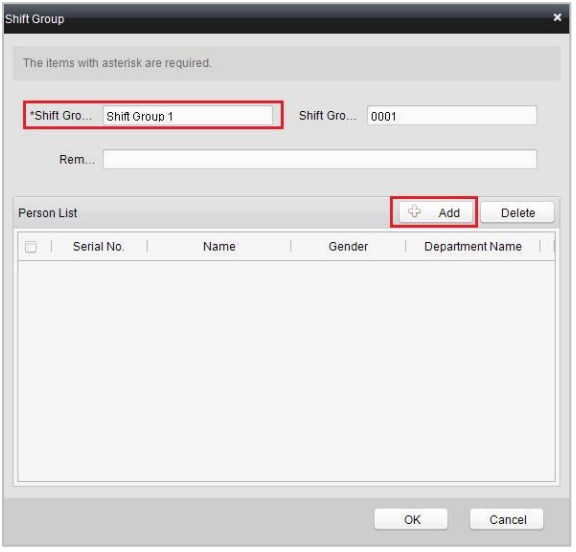
Purpose:

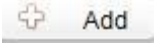
On the shift group management interface, you can add, edit, and delete shift groups for attendance management.

Steps:

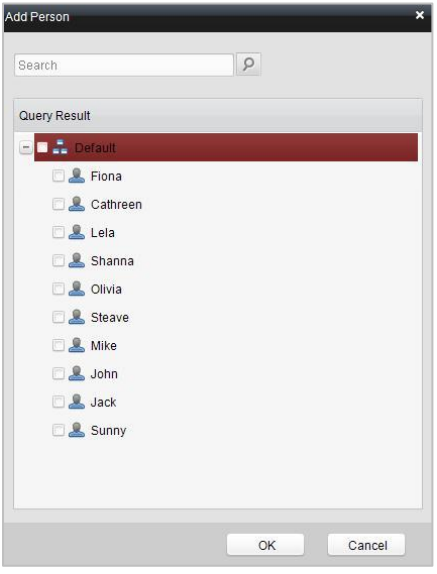
1. Click the 

button to pop up the shift group formation window.

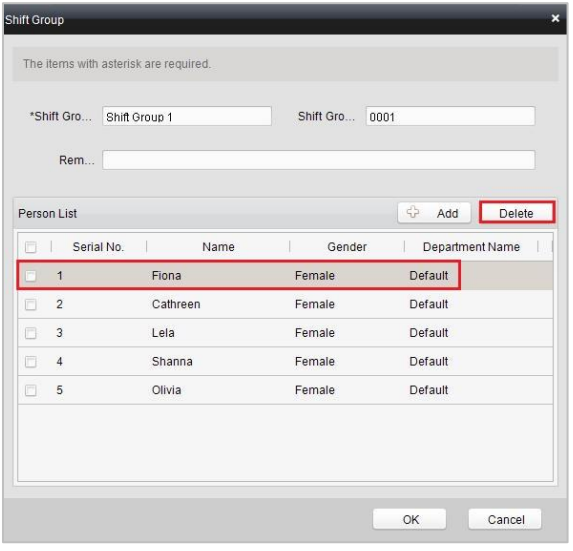


2. Enter the shift group name, and add the 

button on the person list area to add pop up the person adding window.

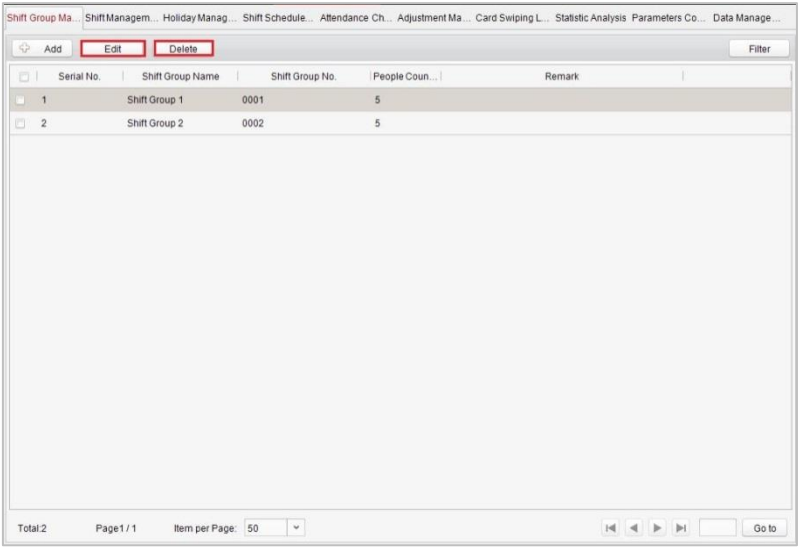


3. Check the checkbox(es) of persons to be added and click the OK button and return to the shift group settings interface.



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

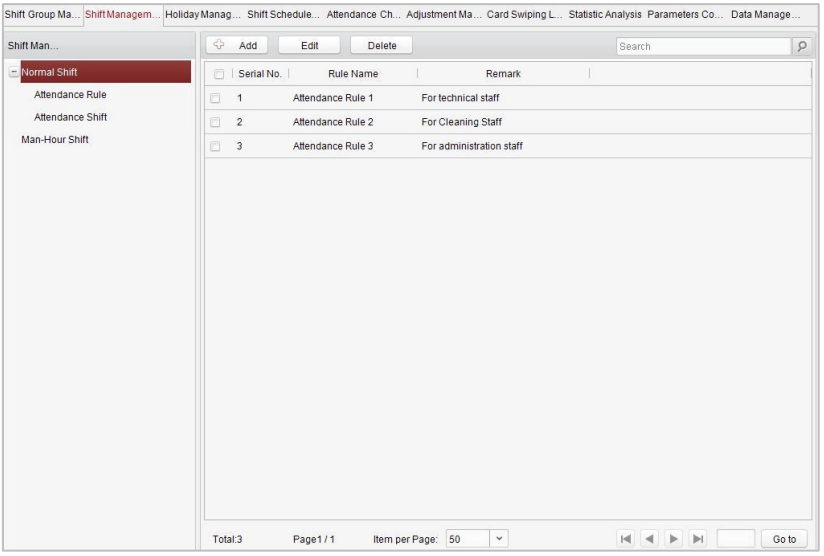
4. Click the OK button to complete the operation.



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.

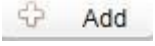


There are two kinds of shifts in this interface: **Normal Shift**, and **Man-Hour Shift**.

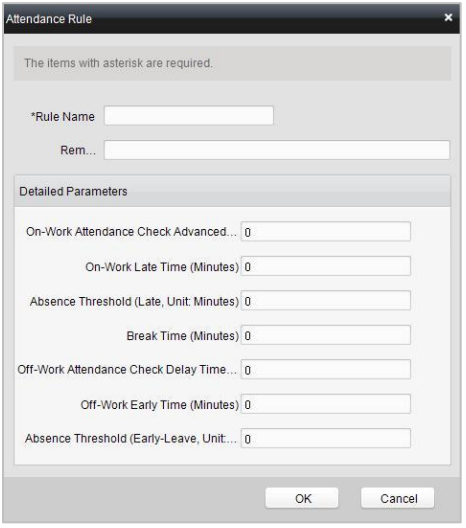
Normal Shift

- **Setting Attendance Rule**

Steps:

1. Click the 

button to pop up the attendance rule setting window.

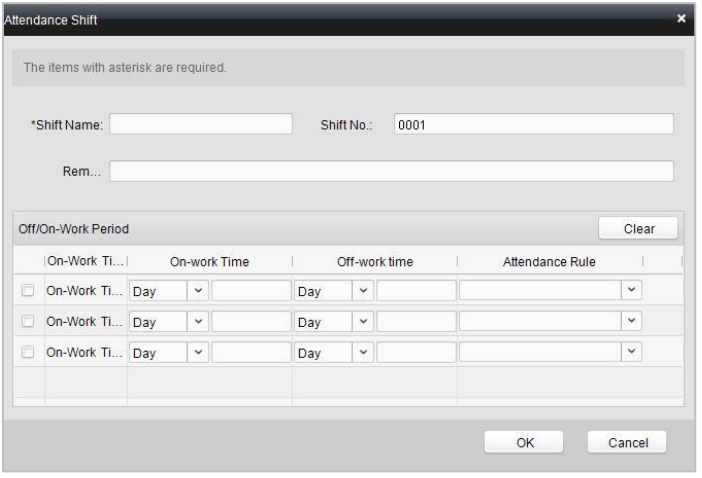


2. Set a rule name.
3. Set detailed parameters for the attendance rule: on-work attendance check advance time, on-work late time, absence threshold, break time, off-work attendance check delay time, off-work early time, and absence threshold (early leave).
4. Click the OK button to complete the operation.

- **Setting Attendance Shift**

Steps:

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



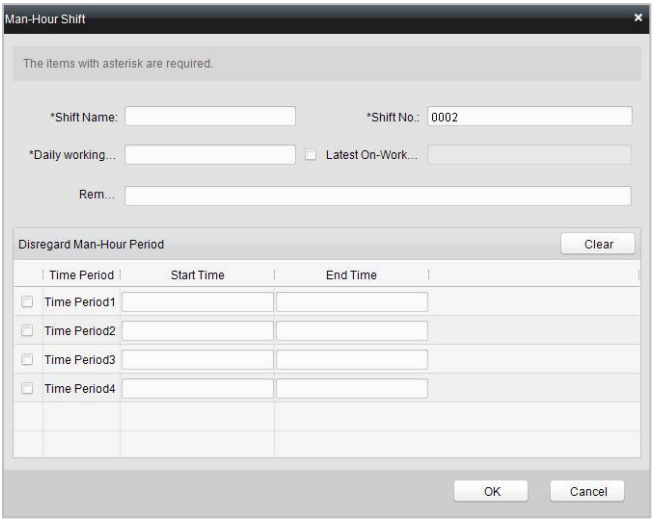
2. Set a shift name.
3. Set on-work duration for the shift, and select the attendance rule.
4. Click the OK button to complete the operation.

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

Man-Hour Shift

Steps:

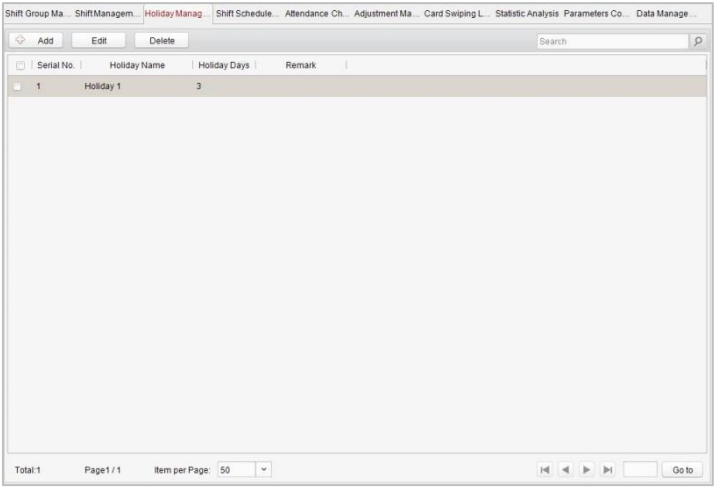
1. Click the Add button to pop up the man-hour shift setting window.



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 OK button to complete the operation.

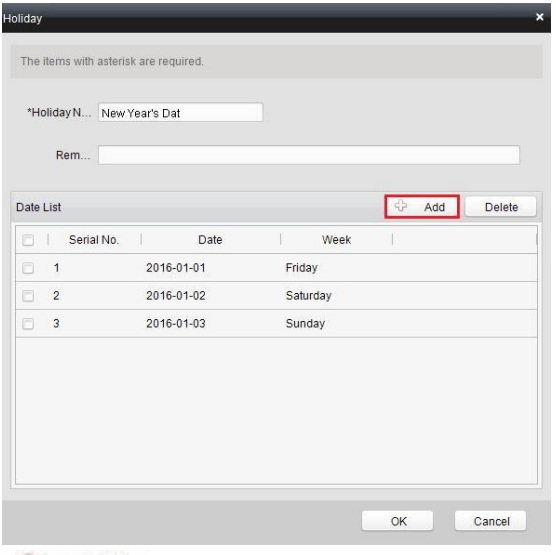
Holiday Management

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

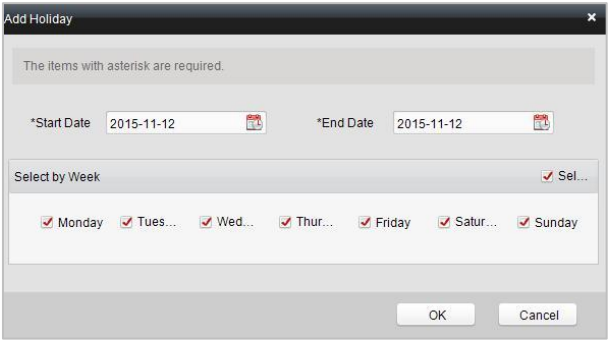


Steps:

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



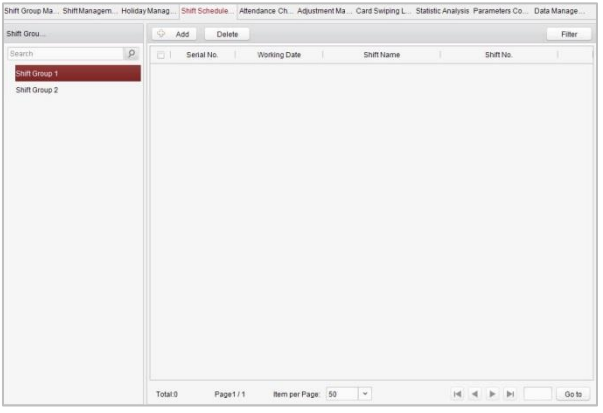
2. Click the Add button to pop-up holiday adding window.



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

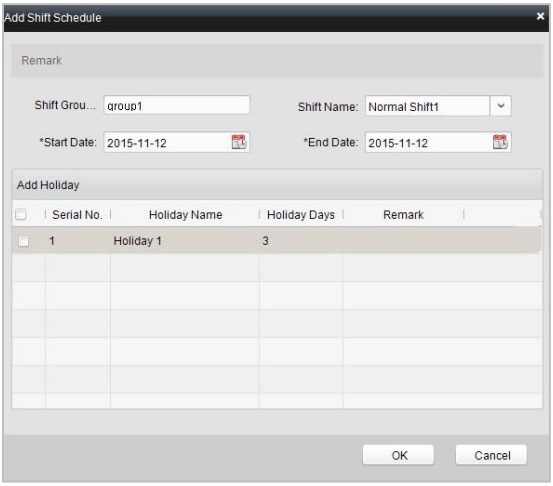
Shift Schedule Management

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



Steps:

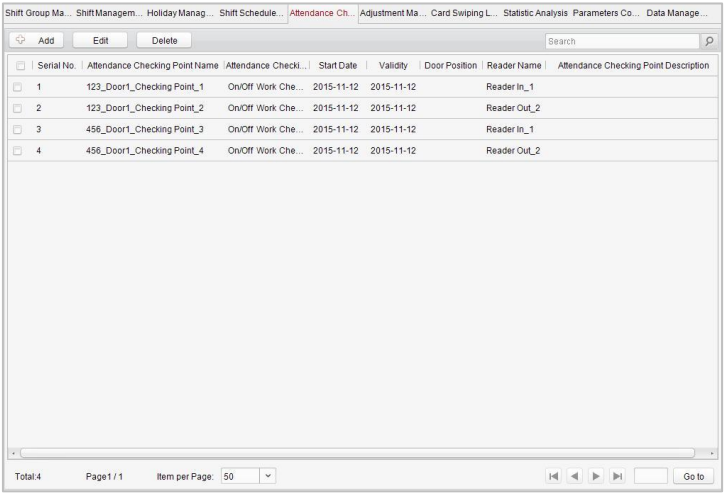
1. Press a tab of shift group on the shift group list.
2. Click the Add button to pop up the shift schedule settings window.



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 OK button to complete the operation.

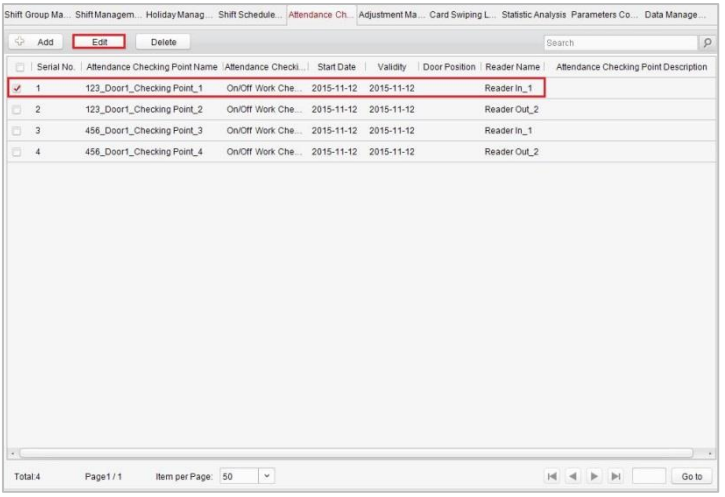
Attendance Check Point Management

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



- **Adding Attendance Check Point**

Steps:



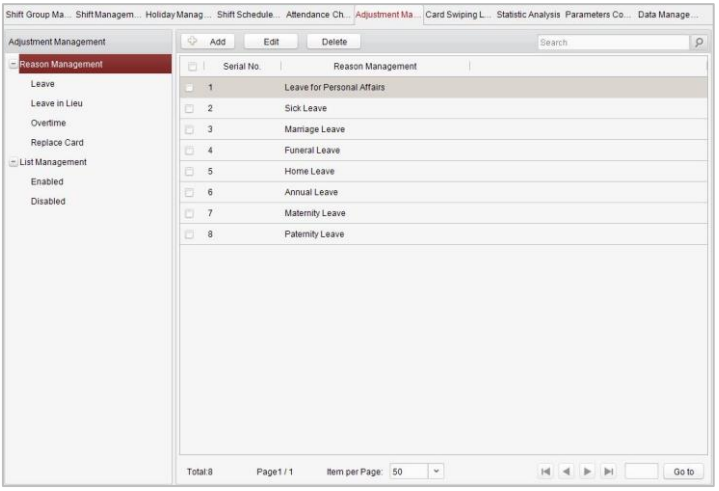
1. Check the checkbox of a checking point, and click the Edit button to pop up the attendance checking point editing window.
2. Edit the attendance checking point name, start date, validity, and attendance checking point type, controller name, door position, and reader name.
3. Click the OK button to complete the operation.

- **Adding Attendance Check Point**

Check the checkbox of a checking point and click the Delete 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

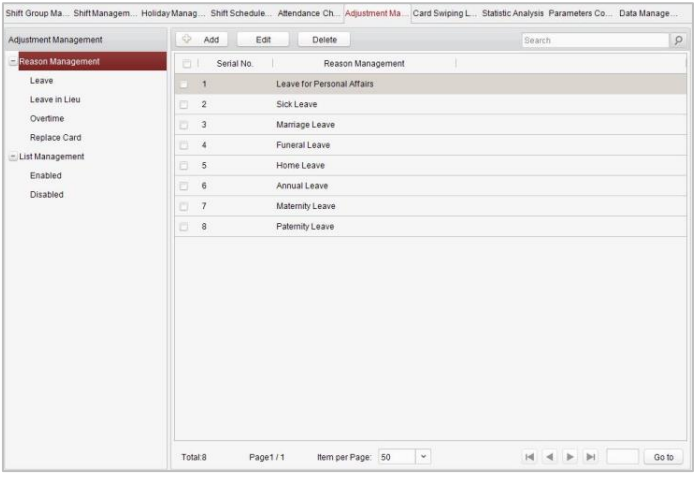
- **Leave**

Purpose:

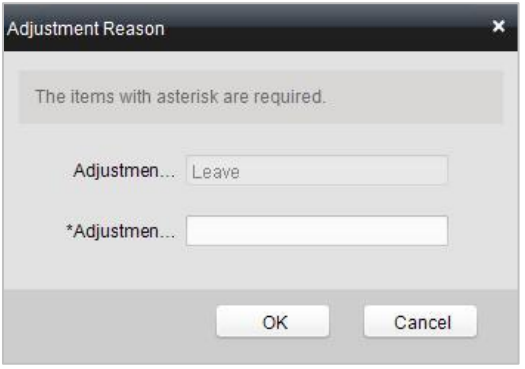
You can add, edit, and delete reasons for leave on the leave interface.

Steps:

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



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



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

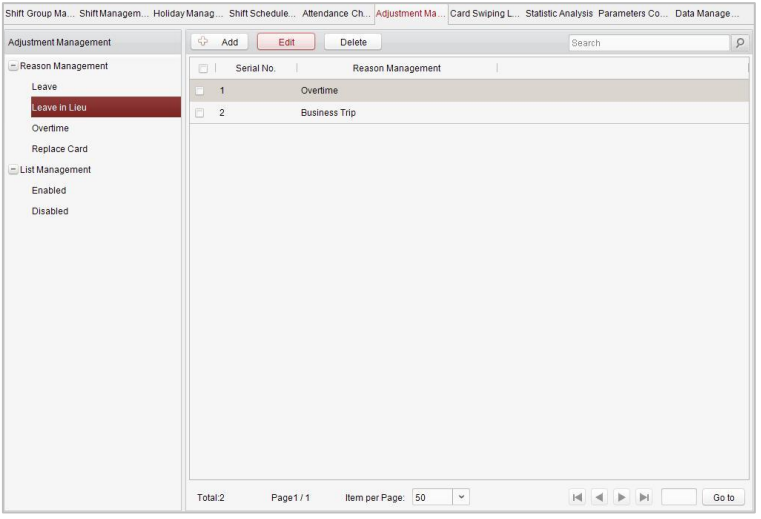
NOTE

- 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 Edit button to edit the reason, and click the Delete button to delete the reason.

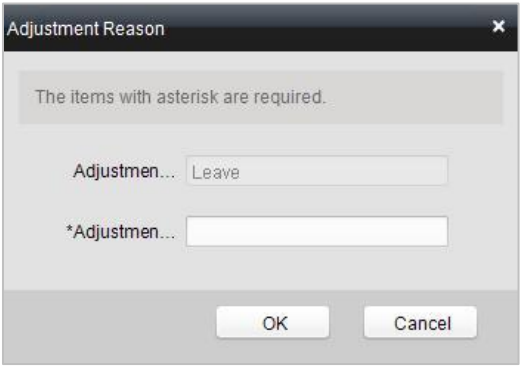
- **Leave in Lieu**

Steps:

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



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



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

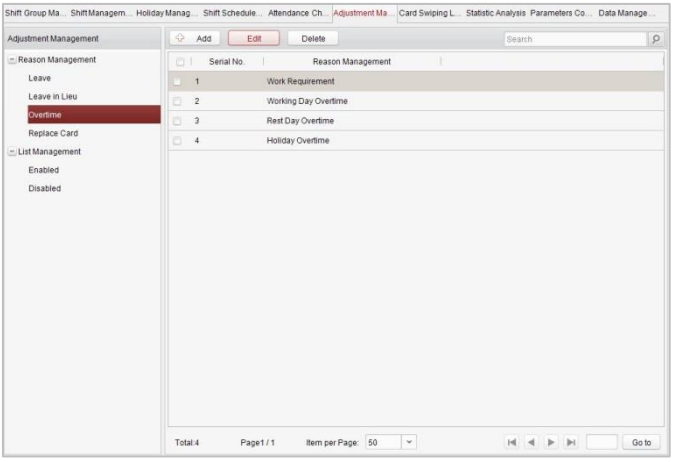
NOTE

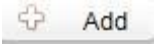
- The default adjustment reasons for leave in lieu include overtime, and business trip.
- You can check the checkbox of a reason and click the Edit button to edit the reason, and click the Delete button to delete the reason.

- **Overtime**

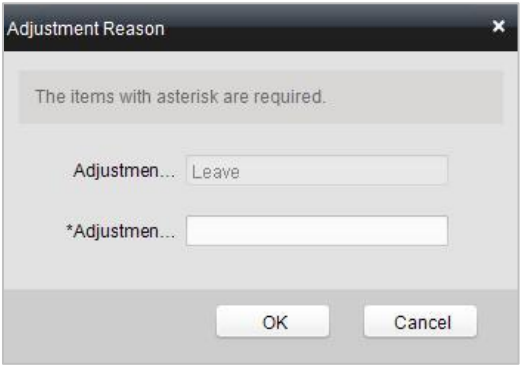
Steps:

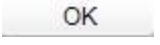
1. Press the overtime tab to enter the overtime interface.



2. Click the 

button to pop up the adjustment reason adding dialog box.



3. Enter the adjustment reason, and click the 

button.

NOTE

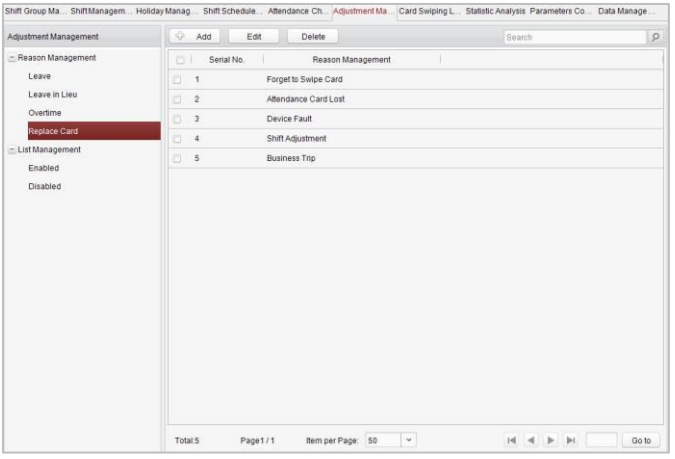
- The default adjustment reasons for overtime include work requirement, working day overtime, rest day overtime, and holiday overtime.

- 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.

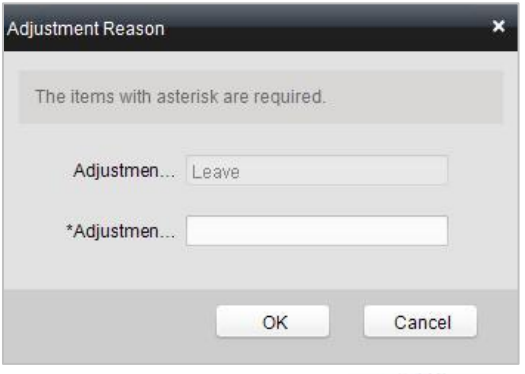
- **Replace Card**

Steps:

1. Press the replace card tab to enter.



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



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

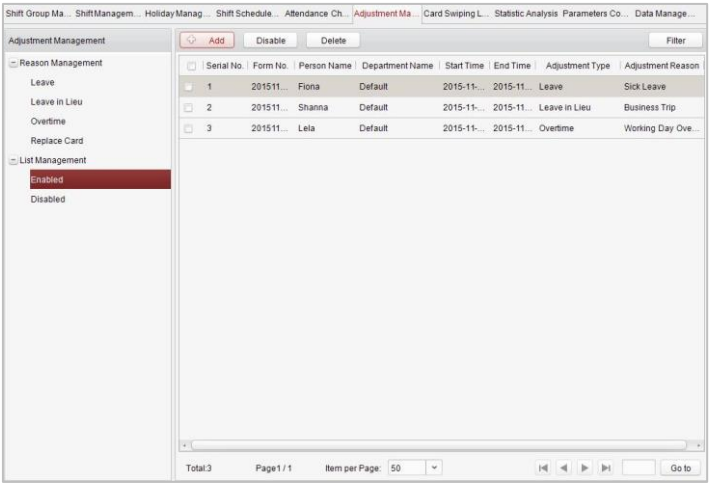
- The default adjustment reasons for card replacing include forget to swipe card, attendance card lost, device fault, shift adjustment, and business trip.
- You can check the checkbox of a reason and click the Edit button to edit the reason, and click the Delete button to delete the reason.

List Management

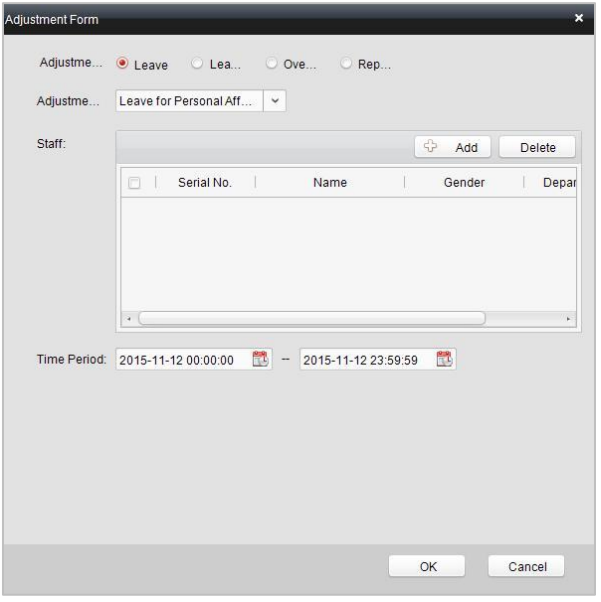
- **Enabling**

Steps:

1. Press the **Enabled** tab to enter the enabled list interface.

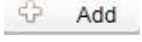


2. Click the Add button.

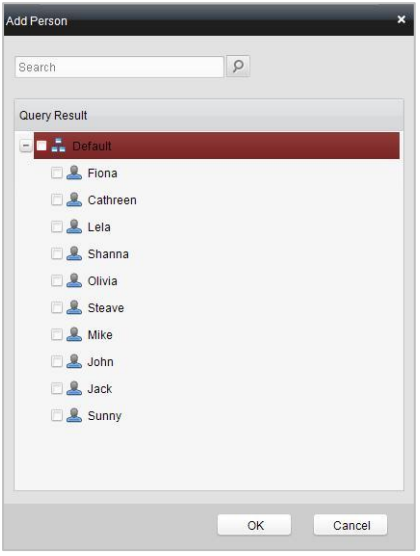


3. Select the radio button of adjustment type: leave, leave in lieu, overtime, and replace card.

   Leave, Leave in Lieu, and Overtime

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

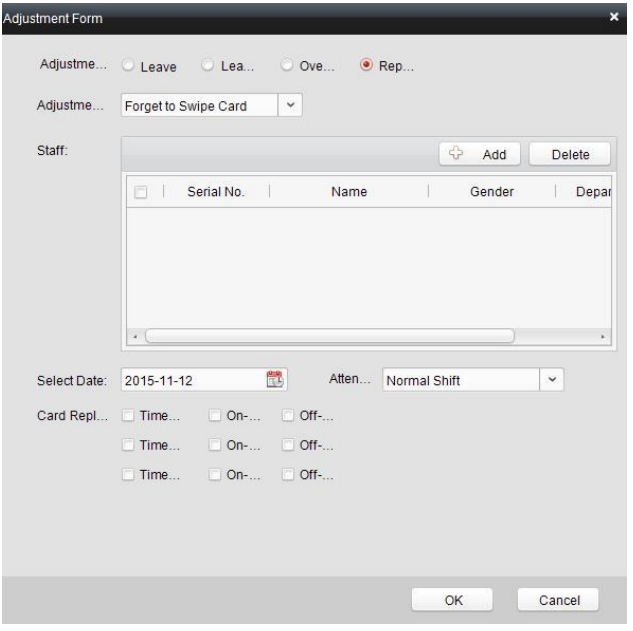
button to pop up the person adding window.



3) Select the person and click the OK button.
4) Set the time period.

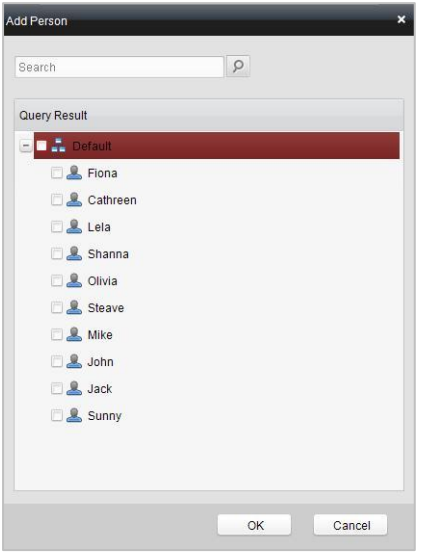
Replace Card

1) 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.



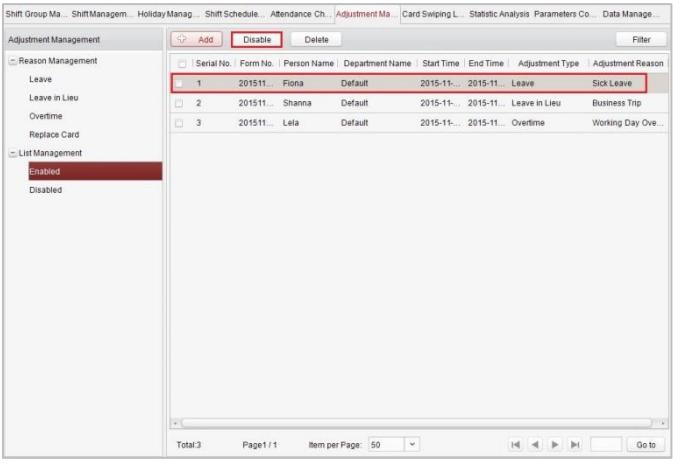
4) Select the person and click the OK button.
5) Set the date, attendance shift, and card replacing time.

4. Click the OK button to complete the operation

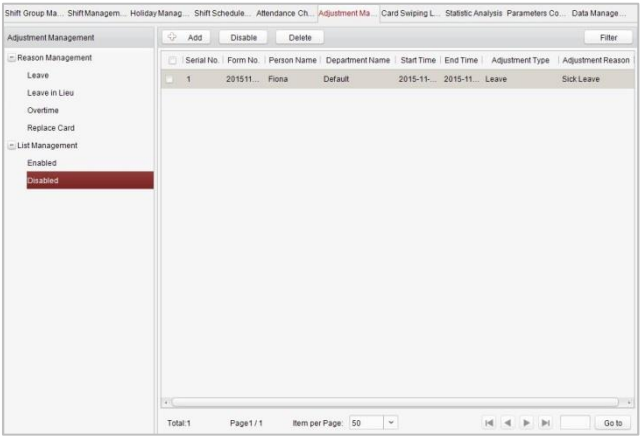
- **Disabling**

Steps:

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

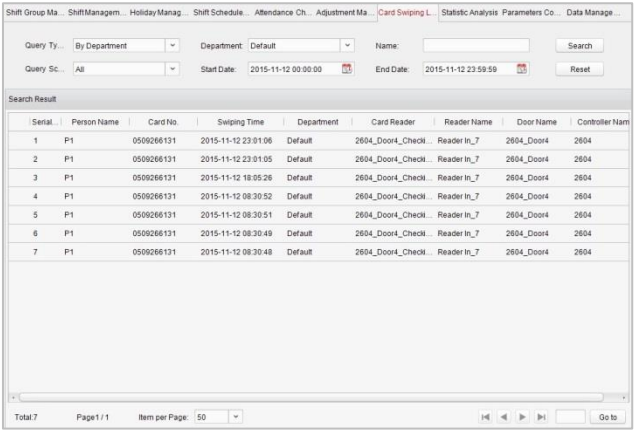


2. Click the Disable button to disable the information.
3. Press the **Disabled** tab and the disabled information will be listed on the disabled interface.



Card Swiping Log Query

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



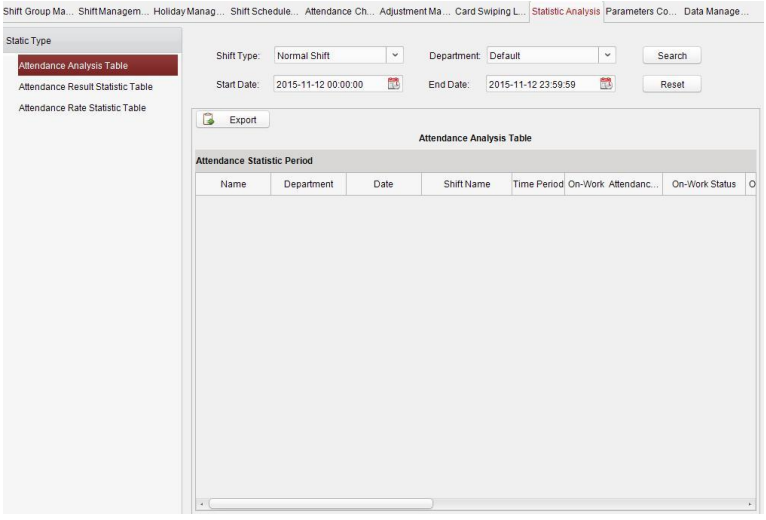
NOTE

- 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

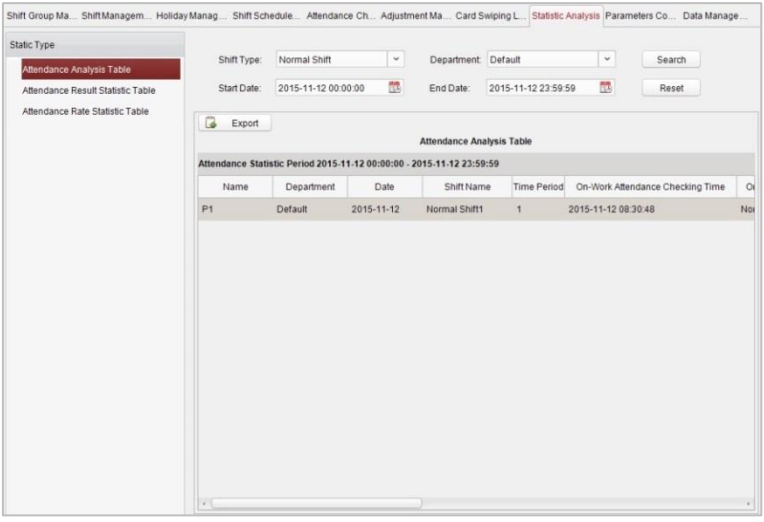
Press the **Statistic Analysis** tab to enter the statistic analysis interface.



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.

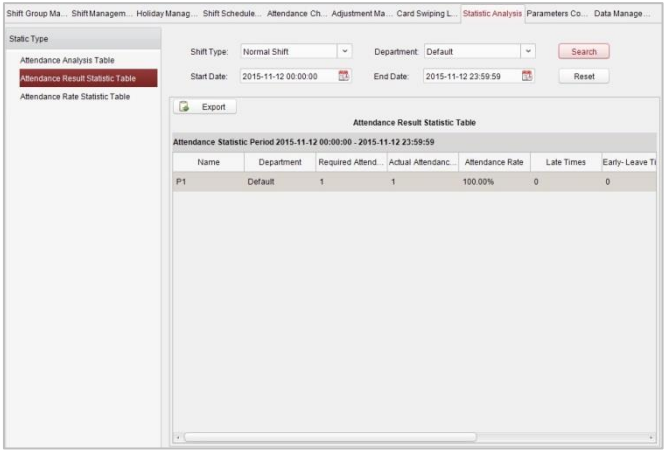


NOTE

- 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.

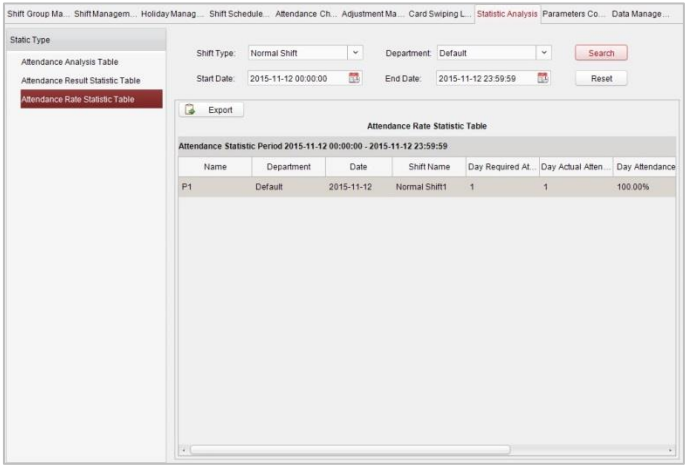


NOTE

- 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.

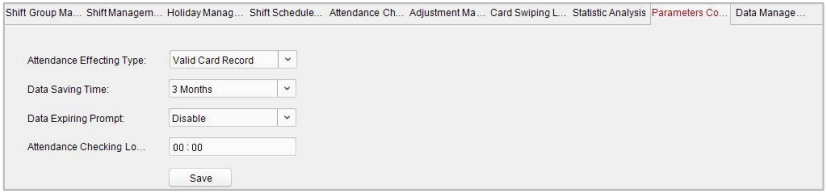


NOTE

- 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.

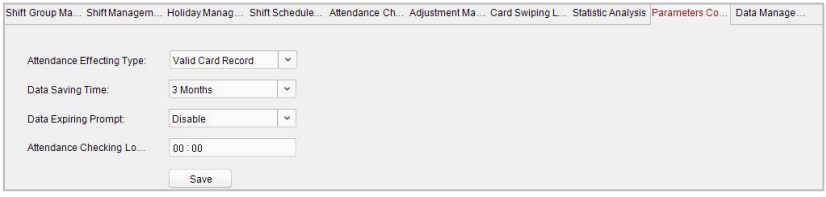


Steps:

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

button to calculate the attendance date.

On this interface, you can export and import attendance data.

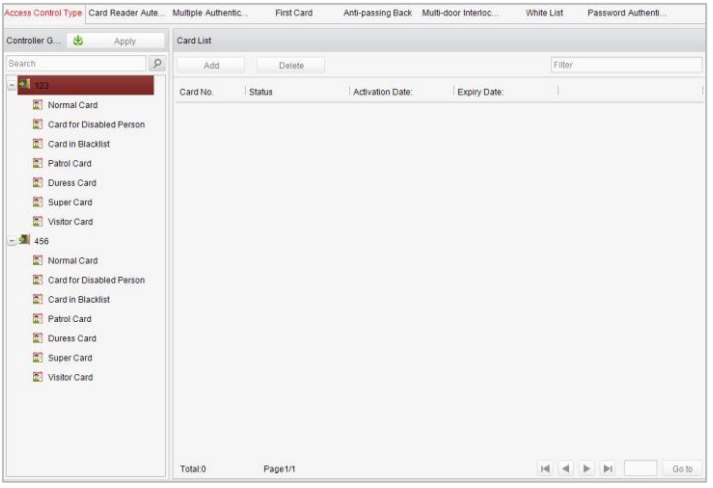
7.3.8 Advanced Functions

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.



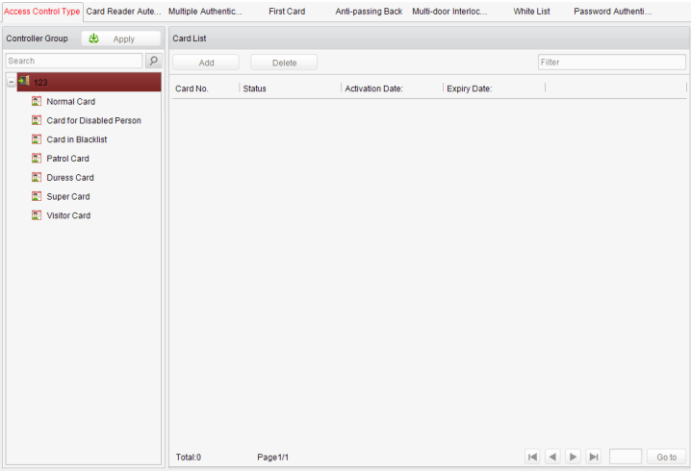
Access Control Type

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 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.

- 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*.
- For models DS-1T802M and DS-1T802E, only two kinds of card reader authentication are supported: **Swipe Card**, and **Swipe Card Password**.

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.

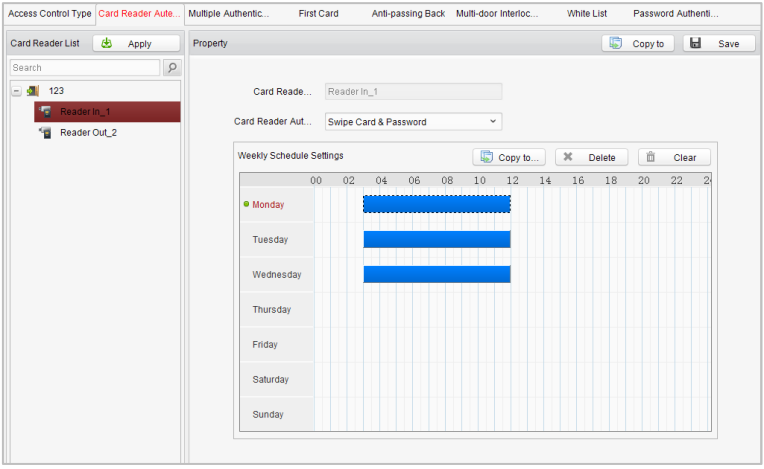
   Swipe Card/Password: The door can open by inputting the password or swiping the card.

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



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

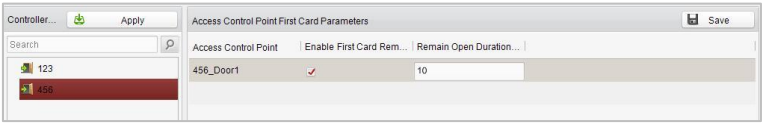
   Or you can select a configured day and click the **Copy to Week** button to copy the same settings to the whole week.

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

First Card

Purpose:

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



Steps:

1. Click **First Card** and select an access control point.
2. Check the checkbox of **Enable First Card Remain Open** to enable this function.
3. In the **Remain Open Duration** (min), input the time duration for remaining open the door.

4. Click **Add** and select the cards to add as first card for the door and click the **OK** button.
5. Click **Save** and then click the **Apply** button to take effect of the new settings.

Anti-Passing Back

Purpose:

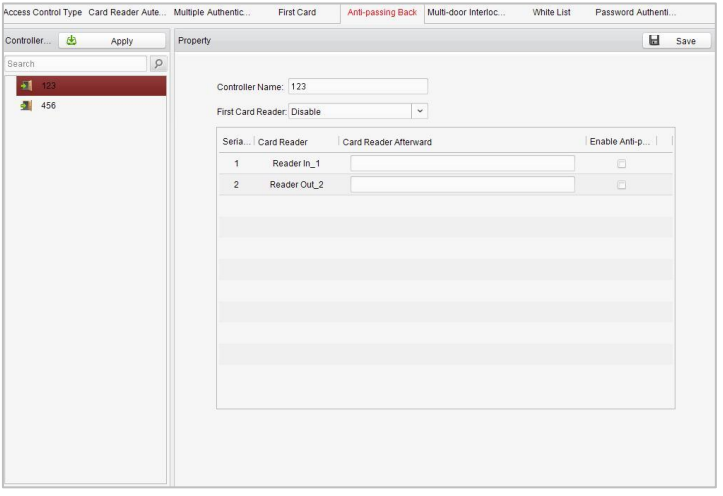
In this mode, you can only pass the access control system according to the specified path.

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.

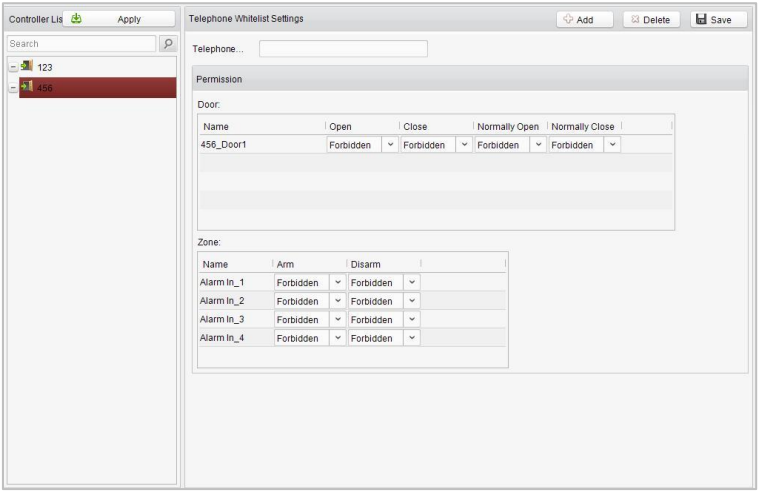
NOTE

Models DS-1T802M and DS-1T802E do not support the anti-passing back function.

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.

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#

Models DS-1T802M and DS-1T802E do not support the white list function.

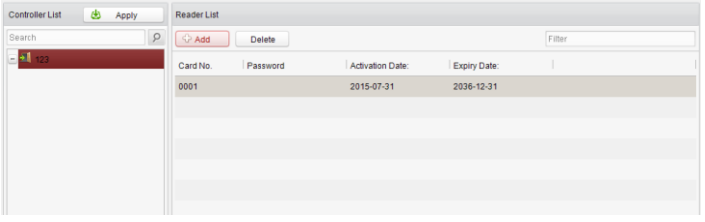
Password Authentication

Purpose:

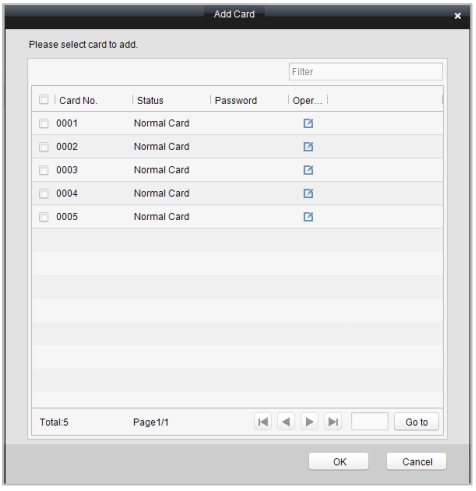
You can open the door by inputting the password only after finishing the operation of password authentication.

Steps:

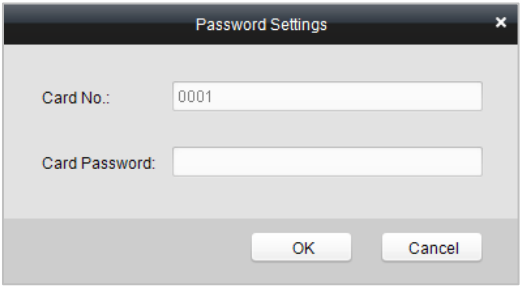
1. Click **Password Authentication** tab and select a host.



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.

NOTE

- 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.
- Models DS-1T802M and DS-1T802E do not support the password authentication function.

7.4 Checking Status and Event

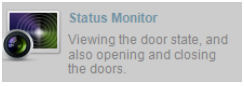
Purpose:

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

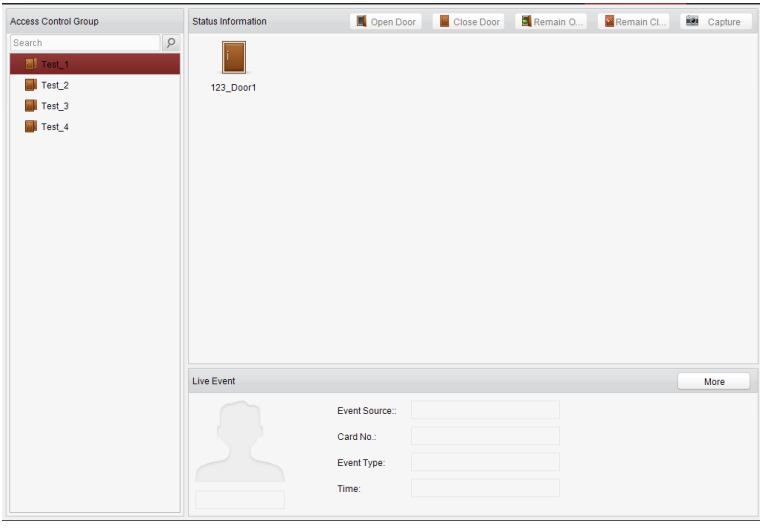
7.4.1 Status Monitor

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

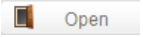
Purpose:

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

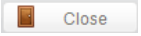
Steps:

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.

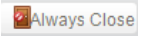


: Click on the button to open the door once.

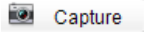


: Click on the button to close the door once.

: Click on the button to keep the door open.



: Click on the button to keep the door closed.



: Click on the button to capture the picture.

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

- 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.
- Models DS-K1T802M and DS-K1T802E do not support the picture capturing function.

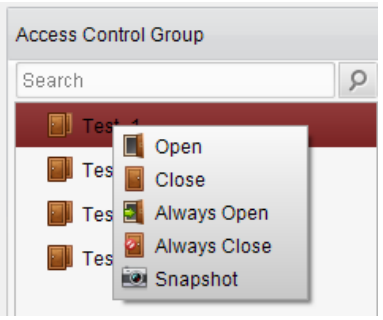
Group Anti-control

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.

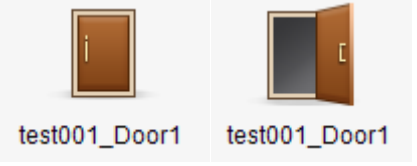


NOTE If the status is selected as **Remain Open/Remain Closed**, all the doors in the group will keep open/ closed until a new anti-control command being made.

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.



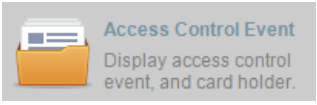
Live Event

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.

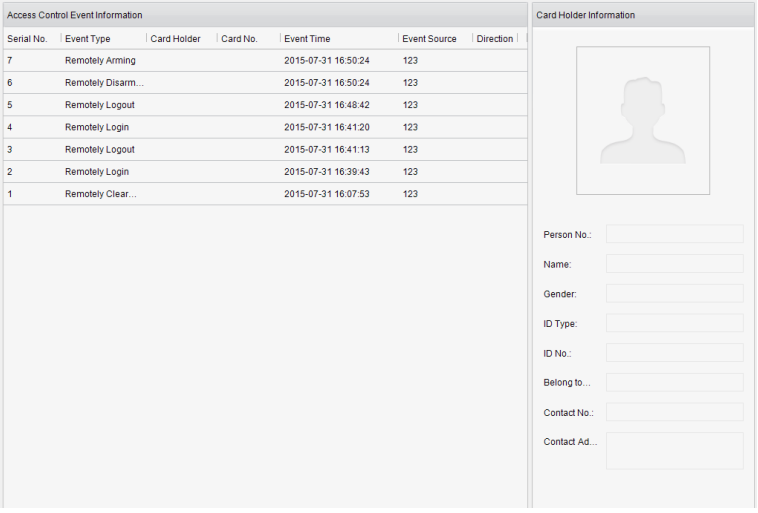
7.4.2 Access Control Event

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.



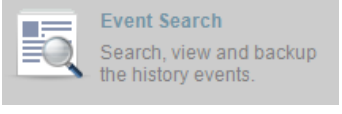
Steps:

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.

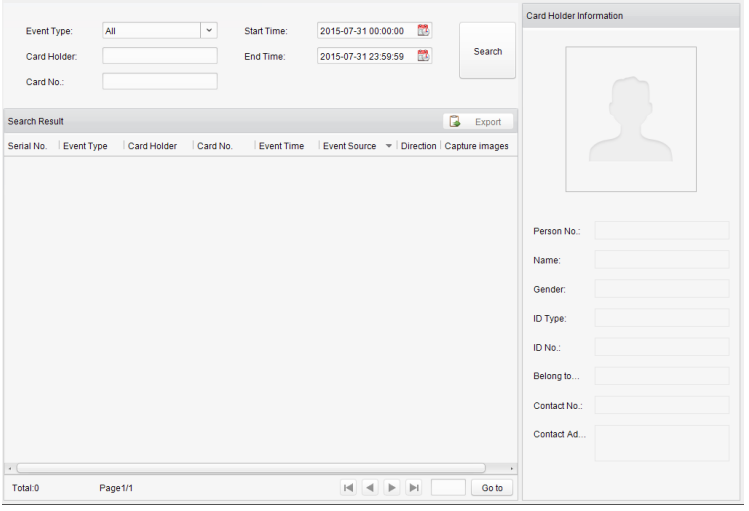
7.4.3 Event Search

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.

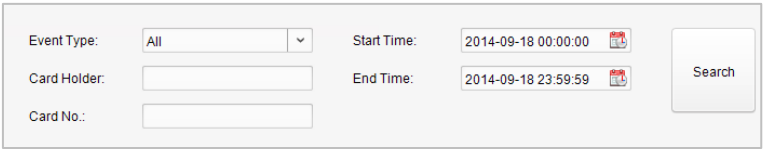
Click the 

icon on the control panel to enter the interface.



Steps:

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



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

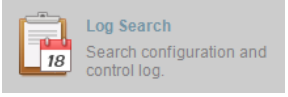
7.5 System Maintenance

7.5.1 Log Management

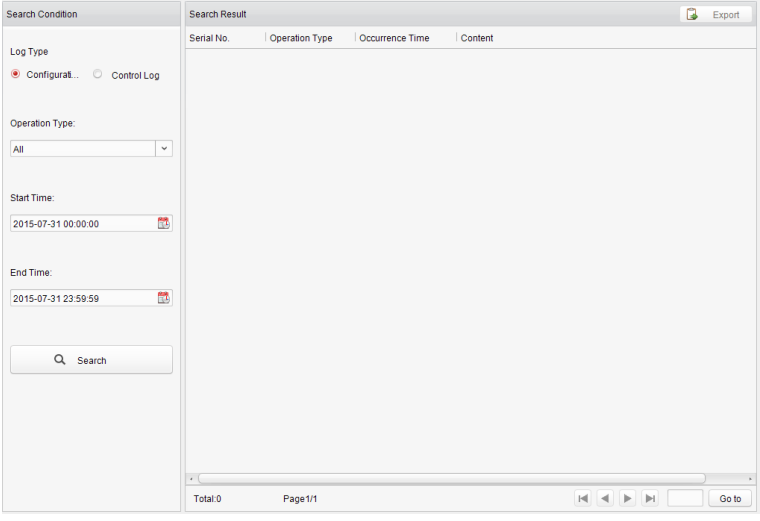
Interface Introduction

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.

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.

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.

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.

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.

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

Log Search

Purpose:

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

Steps:

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

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

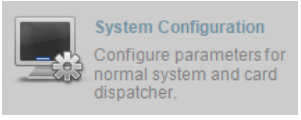
Please narrow the search condition if there are too many log files.

7.5.2 System Configuration

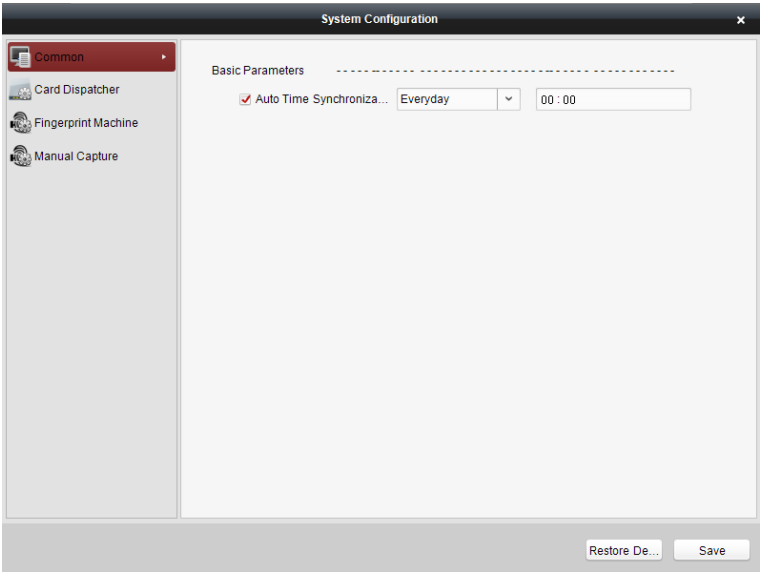
Interface Introduction

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

Models DS-K1T802M and DS-K1T802E do not support the fingerprint machine funciton.

Manual Capture Configuration

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

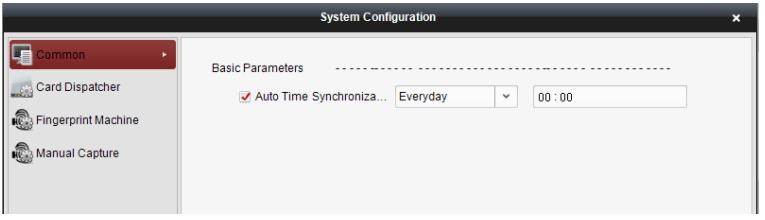
NOTE

Models DS-K1T802M and DS-K1T802E do not support the manual capture configuration.

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.

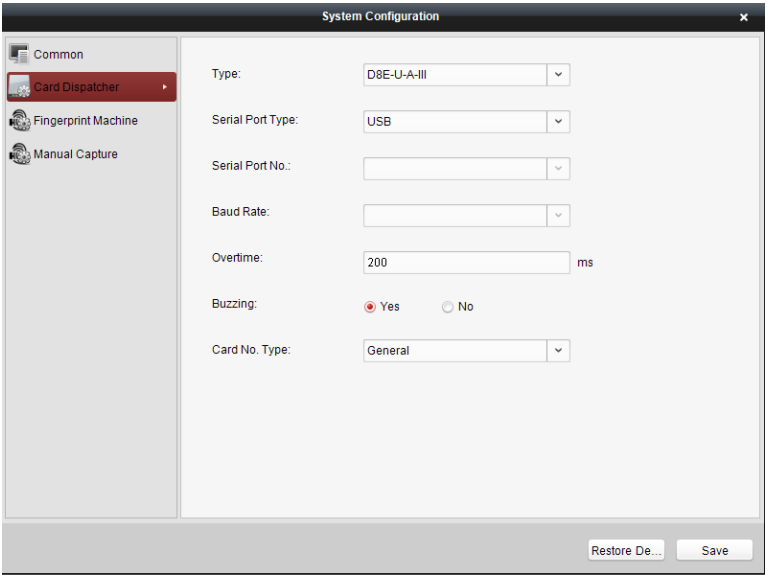
Card Dispenser Configuration

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.



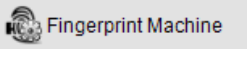
2. Select the device type, serial port type, serial port, baud rate, and other parameters of the Card Dispatcher.
3. Click the save button to save the settings.

NOTE

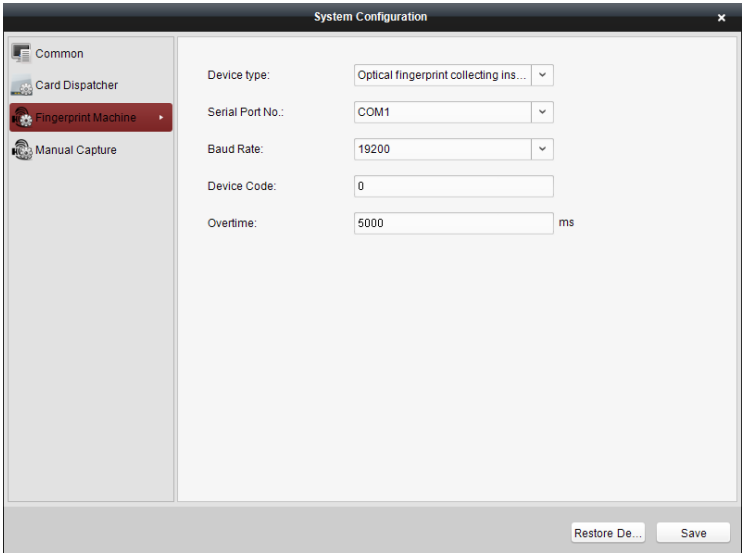
- It is supported using card type as regular and Wiegand.
- When the BEEP is selected as "YES", the audio will be off when you click the "SAVE" if the Card Reader Configuration is set wrong; the audio will be on when you click the "Save" and when you insert the card reader if the configuration is set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

Fingerprint Machine Configuration

Steps:

1. Click the 

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



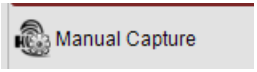
2. Select the device type, serial port number, baud rate, device code, and overtime parameters of the fingerprint machine.
3. Click the **Save** button to save the settings.

NOTE

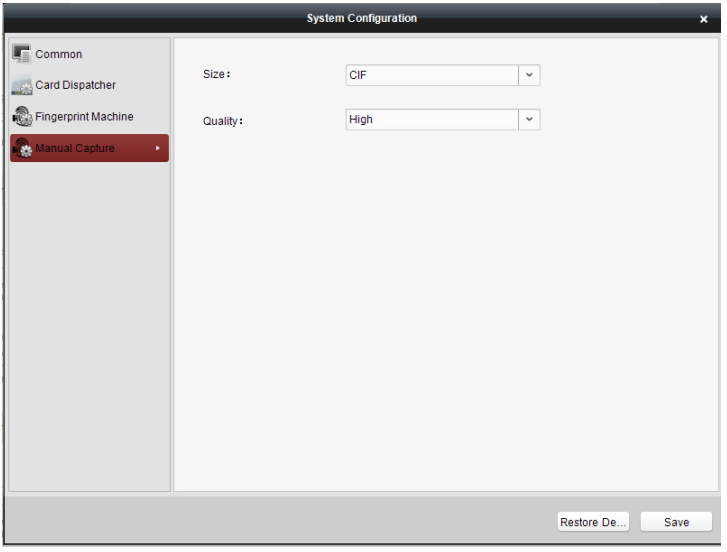
- Models DS-K1T802M and DS-K1T802E do not support the fingerprint machine funciton.
- It is supported using device type as Optical Fingerprint Collecting Instrument and Capacitive Fingerprint Collecting Instrument.
- The serial port number should correspond to the serial port number of PC.
- The baud 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.

NOTE

- Models DS-K1T802M and DS-K1T802E do not support the manual capture configuration.
- 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.

First Choice for Security Professionals