



Face Recognition Terminal

User Manual

User Manual

©2018 Hangzhou Hikvision Digital Technology Co., Ltd.

This manual is applied for face recognition terminal.

Name	Model
Face Recognition Terminal	DS-K5603-Z
	DS-K5603-Z (32 G)

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.

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

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

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

Support

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

Regulatory Information

FCC Information

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

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

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

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

FCC Conditions

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

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

EU Conformity Statement



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

Directive 2011/65/EU



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

www.recyclethis.info



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

Use only power supplies listed in the user instructions:

Model	Manufacturer
KPL-040F-VI	Channel Well Technology Co Ltd.



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 electromagnetic radiation. Avoid the equipment installation on vibrations surface or places subject to shock (ignorance can cause equipment damage).
- Do not place the device in extremely hot (refer to the specification of the device for the detailed operating temperature), cold, dusty or damp locations, and do not expose it to high electromagnetic radiation.
- The device cover for indoor use shall be kept from rain and moisture.
- Exposing the equipment to direct sun light, low ventilation or heat source such as heater or radiator is forbidden (ignorance can cause fire danger).
- Do not aim the device at the sun or extra bright places. A blooming or smear may occur otherwise (which is not a malfunction however), and affecting the endurance of sensor at the same time.
- Please use the provided glove when open up the device cover, avoid direct contact with the device cover, because the acidic sweat of the fingers may erode the surface coating of the device cover.
- Please use a soft and dry cloth when clean inside and outside surfaces of the device cover, do not use alkaline detergents.
- Please keep all wrappers after unpack them for future use. In case of any failure occurred, you need to return the device to the factory with the original wrapper. Transportation without the original wrapper may result in damage on the device and lead to additional costs.
- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.

Table of Contents

Chapter 1 Overview	1
1.1 Introduction	1
1.2 Main Features	1
Chapter 2 Appearance	3
Chapter 3 Installation	4
Chapter 4 Wiring	7
4.1 Wiring Access Control Terminal	7
4.2 Wiring the Third-Party Turnstile	7
Chapter 5 Device Activation	9
5.1 Activating via Device	9
5.2 Activating via SADP Software	9
5.3 Activating via Client Software	11
Chapter 6 Basic Operation	14
6.1 Application Mode Settings	14
6.2 Enter Administrative Backend	14
6.3 Communication Settings	14
6.3.1 Setting Network Parameters	14
6.3.2 Setting COM Parameters	15
6.4 System Settings	16
6.5 User Management	18
6.5.3 Adding User	18
6.5.4 Searching User	19
6.5.5 Editing User	19
6.6 Setting Face Picture Parameters	20
6.7 Changing Password	22
6.8 Managing Data	23
6.9 Maintaining System	23
6.9.6 Restoring Device Parameters	24
6.9.7 Upgrading Firmware	24
6.10 Viewing System Information	25
6.11 Viewing Device Information	25
6.12 Authenticating Identity	25
6.12.8 Authenticating via 1:1 Matching	25
6.12.9 Authenticating via 1:N Matching	26

6.13	Linking Access Control Device	26
Chapter 7	Client Operation	27
7.1	User Registration and Login	27
7.2	System Configuration	28
7.3	Access Control Management	28
7.3.1	Adding Access Control Device	29
7.3.2	Viewing Device Status	44
7.3.3	Editing Basic Information	45
7.3.4	Network Settings	46
7.3.5	Capture Settings	48
7.3.6	RS-485 Settings	49
7.3.7	Wiegand Settings	50
7.3.8	Setting Multiple NICs	51
7.3.9	Setting Face Recognition Terminal	51
7.3.10	Remote Configuration	52
7.4	Organization Management	63
7.4.1	Adding Organization	63
7.4.2	Modifying and Deleting Organization	63
7.5	Person Management	64
7.5.1	Adding Person	64
7.5.2	Managing Person	75
7.5.3	Issuing Card in Batch	75
7.5.4	Detecting Face Modeling Failed Records	77
7.6	Schedule and Template	78
7.6.1	Week Schedule	79
7.6.2	Holiday Group	80
7.6.3	Template	81
7.7	Permission Configuration	83
7.7.1	Adding Permission	84
7.7.2	Applying Permission	85
7.8	Advanced Functions	86
7.8.1	Access Control Parameters	87
7.8.2	Card Reader Authentication	90
7.8.3	Multiple Authentication	91
7.8.4	Open Door with First Card	94
7.8.5	Anti-Passing Back	96

7.8.6	Person in Blacklist.....	97
7.9	Searching Access Control Event	98
7.9.1	Searching Local Access Control Event	99
7.9.2	Searching Remote Access Control Event.....	99
7.10	Access Control Event Configuration	100
7.10.1	Access Control Event Linkage	100
7.10.2	Event Card Linkage	101
7.10.3	Cross-Device Linkage.....	103
7.11	Door Status Management	105
7.11.4	Access Control Group Management	105
7.11.5	Anti-control the Access Control Point (Door).....	106
7.11.6	Status Duration Configuration	108
7.11.7	Real-time Card Swiping Record	109
7.11.8	Real-time Access Control Alarm	110
7.12	Arming Control.....	112
7.13	Time and Attendance.....	112
7.13.1	Shift Schedule Management	113
7.13.2	Attendance Handling.....	119
7.13.3	Advanced Settings	123
7.13.4	Attendance Statistics.....	127
Appendix A Tips When Collecting/Comparing Face Picture		131
A.1 Positions (Recommended Distance:0.5m)		131
A.2 Expression.....		131
A.3 Posture		132
A.4 Size		132

Chapter 1 Overview

1.1 Introduction

DS-K5603-Z and DS-K5603-Z (32 G) face recognition terminal, designed with TX1 system, can be applied in the scenarios of examination hall, railway station, bank, building, hotel, etc., which needs identity verification.



1.2 Main Features

- 10.1-inch and 1280 × 800 resolution capacitive touch screen
 - 2 MP wide-angle dual-lens
 - Max. 10,000 face pictures, Max. 10,000 face pictures in blacklist, and Max. 50,000 comparing events for DS-K5603-Z face recognition terminal
 - Max. 50,000 face pictures, Max. 10,000 face pictures in blacklist, and Max. 100,000 comparing events for DS-K5603-Z (32 G) face recognition terminal
 - Multiple authentication modes: authentication by card + face picture, by auto mode (card + face picture or face picture)
 - Identity authentication by QR code instead of card
- Note:** The device should connect an external card reader or the card swiping function cannot be used.
- Two network interfaces
Each network interface can auto visit the EHome server separately.
 - Applies persons in blacklist via iVMS-4200 client software.
 - Applies face pictures from the system to the device via EHome protocol
 - Uploads blacklist authentication and blacklist event, and displays them on the main screen
 - Imports face pictures to the device via the USB interface

- Exports face pictures and events from the device via the USB interface
- Communication with access controller via RS-232 communication mode and communication with the third party devices via RS-485 communication mode
- Uploads offline events
- Audio prompt

Chapter 2 Appearance

The device appearance, dimensions and descriptions are as follows.

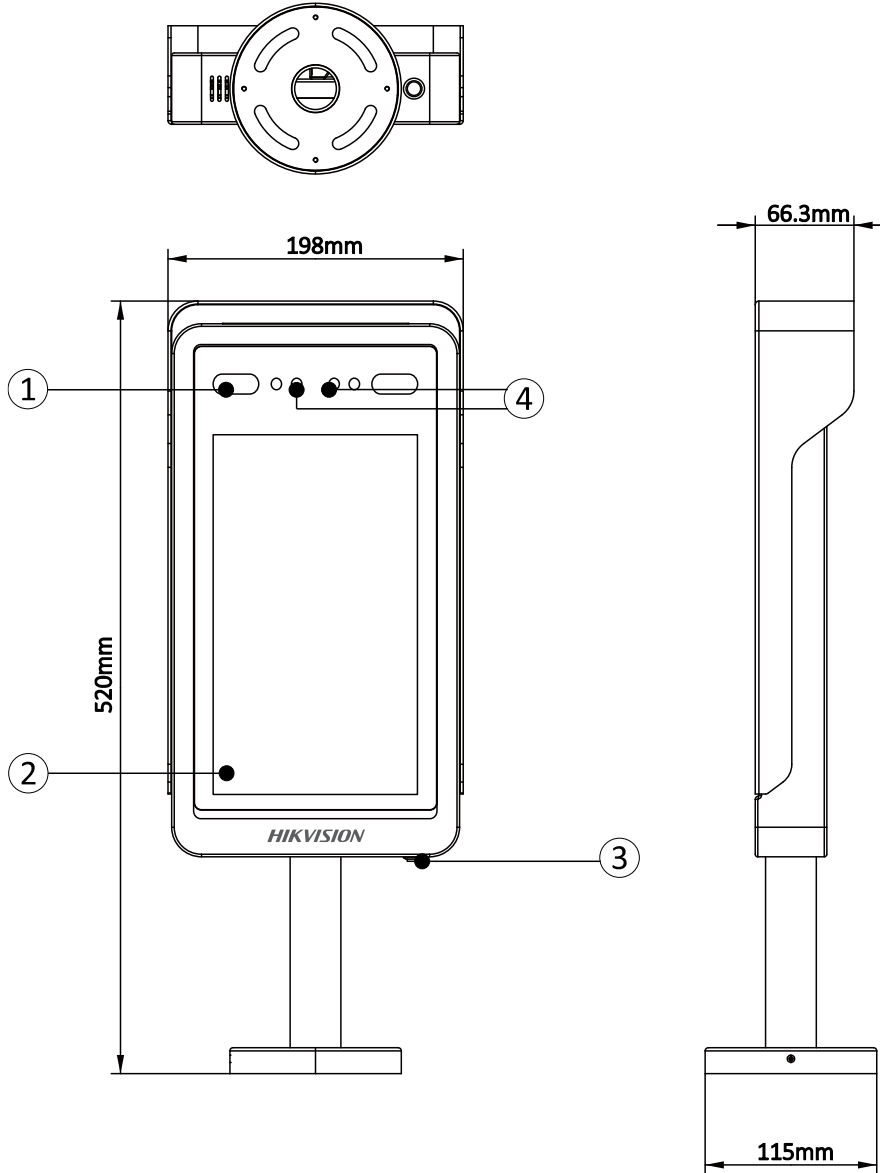


Table 2-1 Description of Face Recognition Terminal

No.	Description
1	Supplement Light
2	Display Screen
3	Power Button
4	Cameras

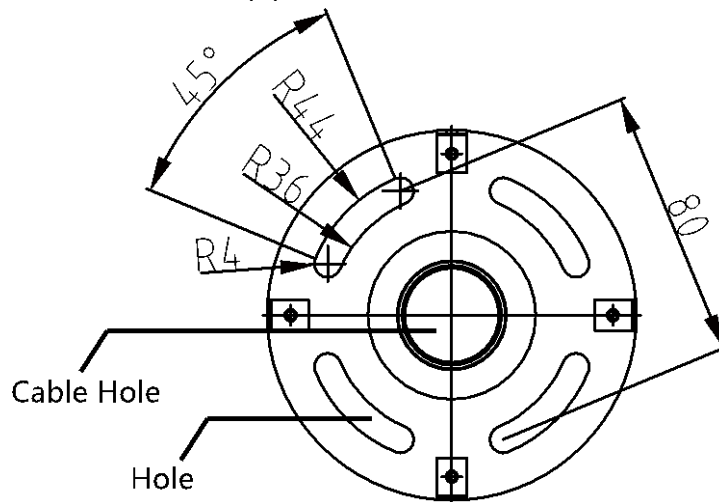
Chapter 3 Installation

Installation Environment:

- Avoid backlight and direct sunlight.
- If installing outdoors, install a sun shield over the device.
- The device should be installed on the pedestals of the barriers.

Before you start:

- Drill holes on the barrier pedestal's top panel according to the picture displayed below
- Riveted waterproof nut under the top panel.

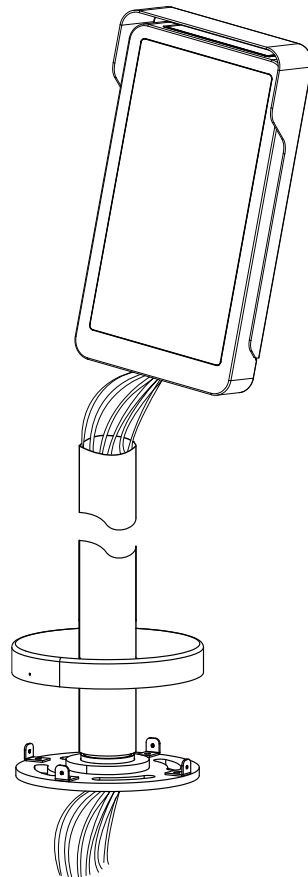


Notes:

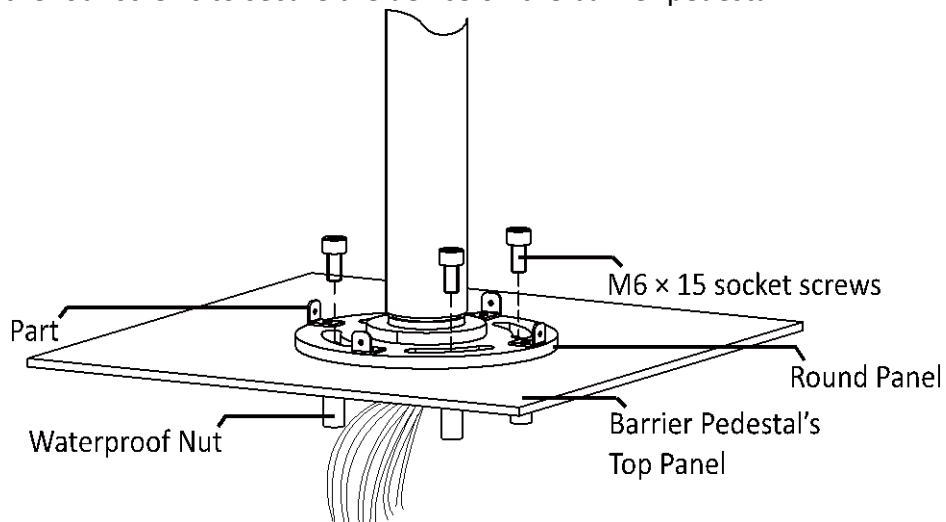
- SUITABLE FOR MOUNTING ON CONCRETE OR OTHER NON-COMBUSTIBLE SURFACE ONLY.
- The waterproof nut model is BS-M6-1.

Steps:

1. Route the cables through the pipe from top to bottom and thread them through the cable holes on the barrier pedestal's top panel.

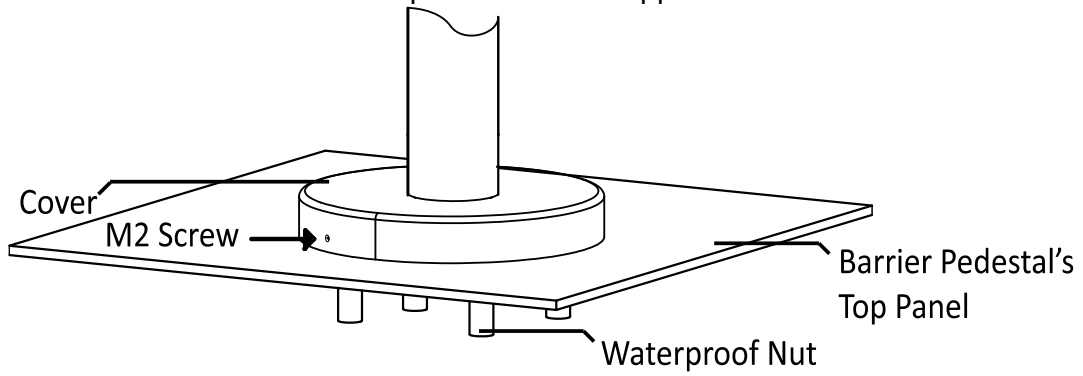


2. Wire the cable with the terminals in the barrier pedestal.
3. Raise the pipe and make sure the pipe and the pedestal top panel are vertical.
4. Secure hex socket screws.
 - 1) Rotate the pipe and align the four holes on the round panel with the holes on the pedestal top panel.
 - 2) Thread the supplied four M6 × 15 socket screws from up to down through the four holes respectively. (Do not tight up.)
 - 3) Rotate the pipe and make sure the device display screen is in the correct direction.
 - 4) Tight the four screws to secure the device on the barrier pedestal.



5. Install the cover on the round panel.

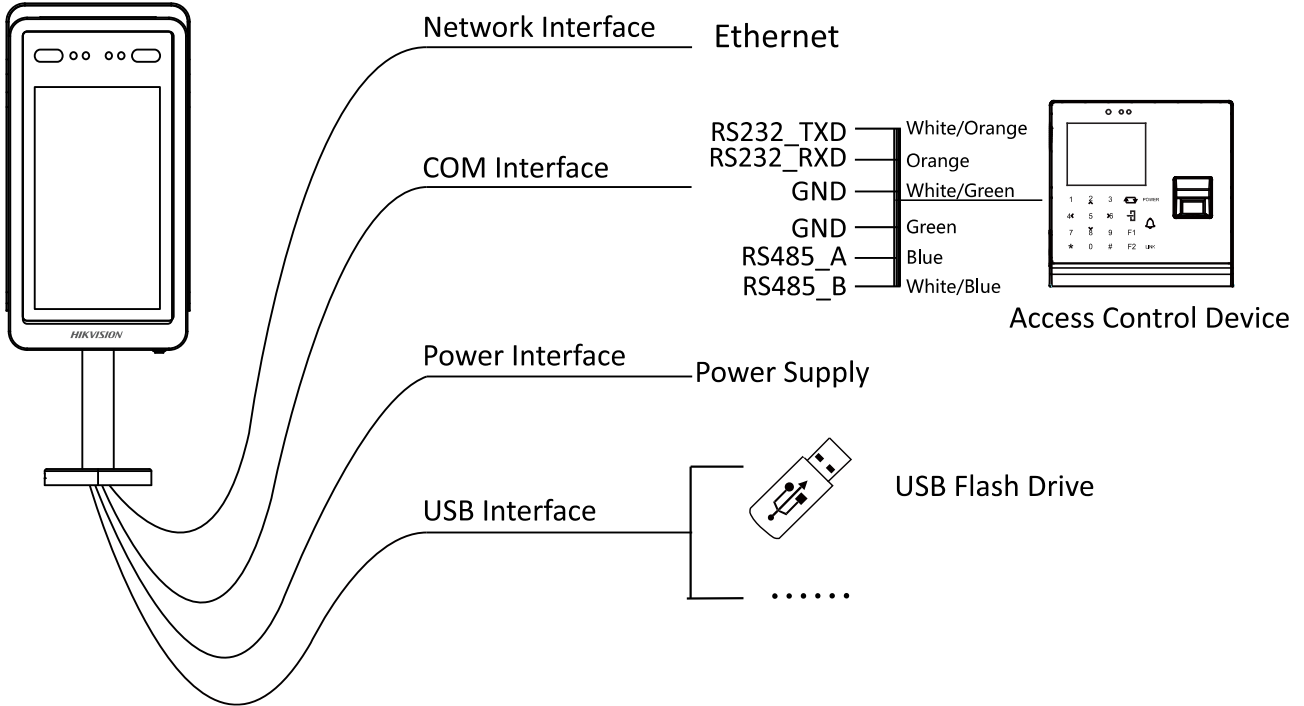
- 1) Move the cover on the round panel.
- 2) Rotate the cover and hide the hole on the cover and align the hole with one of the four small parts on the round panel.
- 3) Secure the cover and the round panel with one supplied M2 screw.



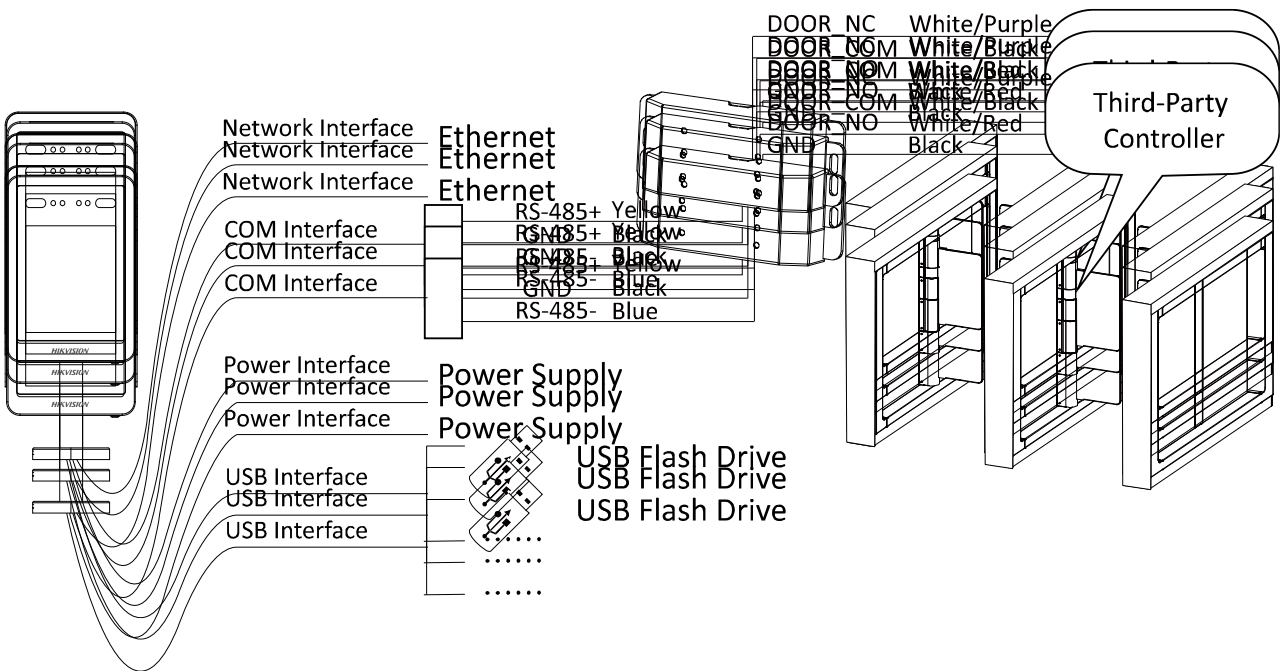
Chapter 4 Wiring

4.1 Wiring Access Control Terminal

The picture displayed below describes the access control terminal's wiring.



4.2 Wiring the Third-Party Turnstile



Notes:

- For details about I/O output module, see *User Manual of I/O Output Module* or scan the QR code below to view the manual via your mobile device.



- The device can also access to the third-party turnstile via RS-485 to Wiegand module. For details, see *User Manual of RS-485 to Wiegand Module* or scan the QR Code below to view the manual via your mobile device.



Chapter 5 Device Activation

Purpose:

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

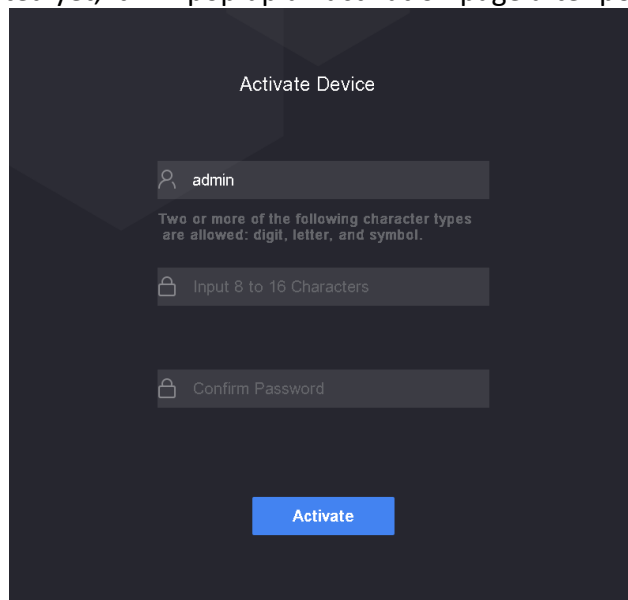
Activation via device, activation via SADP, and activation via client software are supported.

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 Device

If the device is not activated yet, it will pop up an activation page after powering on.



Steps:

1. Create a password for the Admin user.
2. Confirm the password.
3. Tap **Activate**.



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

5.2 Activating via SADP Software

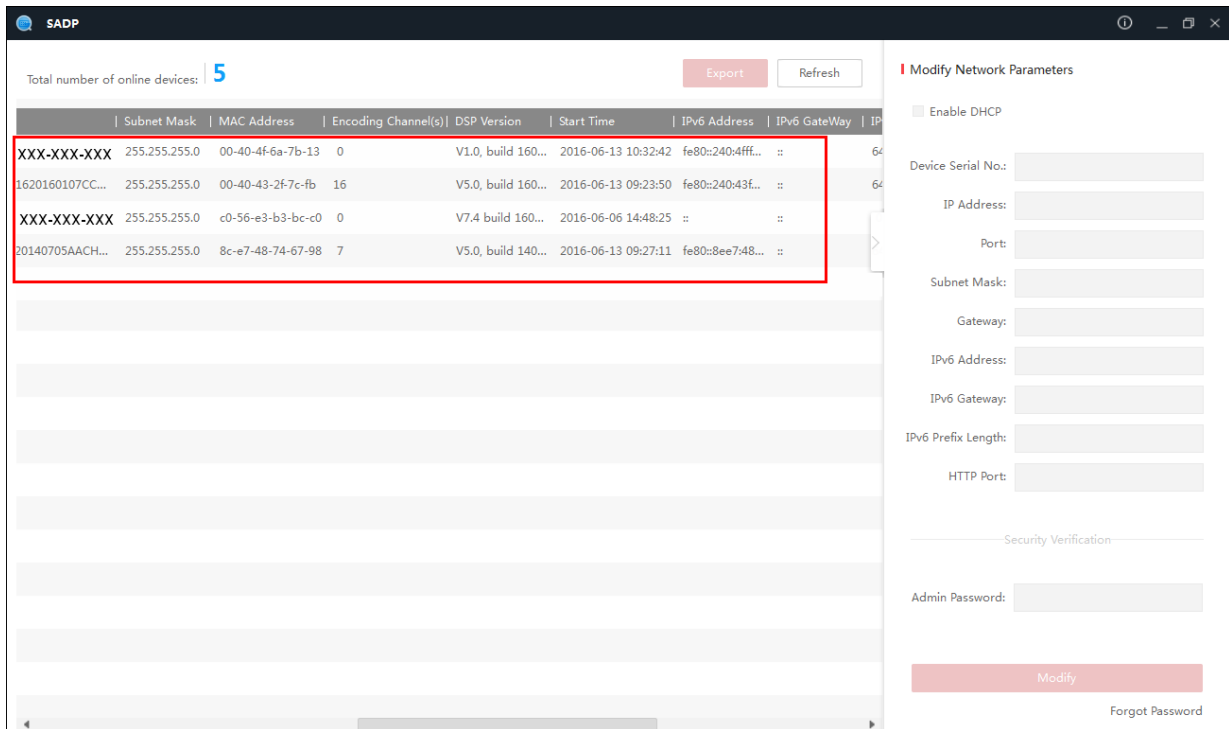
Purpose:

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

Get the SADP software from the supplied disc, and install the SADP according to the prompts. Follow the steps to activate the device.

Steps:

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



3. Create a password in the password field, and confirm the password.



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

4. Click **Activate** to activate the device.
5. Check the activated device. You can change the device IP address to the same network segment with your computer by either editing the IP address manually or checking the Enable DHCP checkbox.

Modify Network Parameters

Enable DHCP

Device Serial No.:

IP Address:

Port:

Subnet Mask:

Gateway:

IPv6 Address:

IPv6 Gateway:

IPv6 Prefix Length:

HTTP Port:

Security Verification

Admin Password:

[Modify](#)

[Forgot Password](#)

6. Input the password and click **Modify** to save the IP address.

5.3 Activating via Client Software

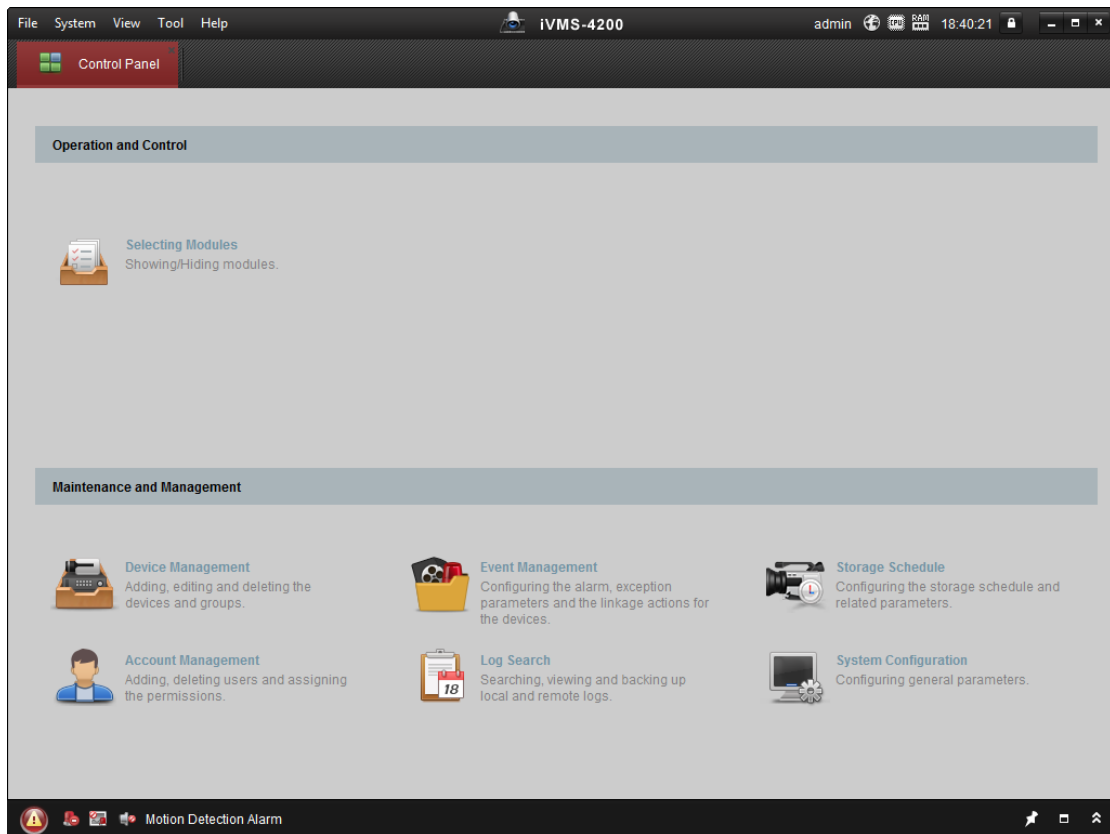
Purpose:

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

Get the client software from the supplied disc, and install the software according to the prompts. Follow the steps to activate the control panel.

Steps:

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



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

IP	Device Type	Firmware Version	Security	Server Port	Device Serial No.	Start Time
192.0.0.64			Active	8000		2017-01
192.168.1.64			Inactive	8000		2017-01

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



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



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

After activation, you will enter the initial page.

Chapter 6 Basic Operation

Purpose:

After entering the administrative backend, you can manage users, set communication parameters, change device password, manage and maintain data, and view device information.

6.1 Application Mode Settings

Purpose:

After activating the device, you should select an application mode for better device application.

Steps:

1. In the Welcome page, select **Indoor** or **Others** from the drop-down list.
2. Tap **OK** to save the settings.

Note: You can also change the settings in *Section 6.4 System Settings*.

6.2 Enter Administrative Backend

Purpose:

You should enter the de administrative backend before setting other parameters.

Steps:

1. On the initial page, long tap the screen for 3s to enter the input password page.
2. Input the password in the text box. The password here refers to the activation password.
3. Tap **OK** to enter the backend.
4. (Optional) Tap **Exit** at the lower left corner to exit the backend.

6.3 Communication Settings

Purpose:


You can set the device network parameters and COM parameters.

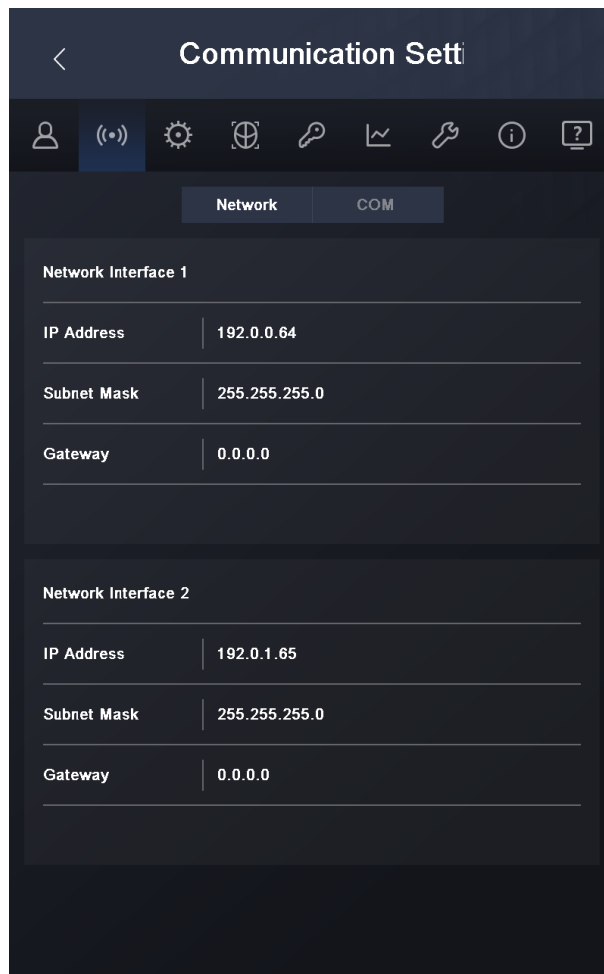
6.3.1 Setting Network Parameters

Purpose:

The device contains two network interfaces. You can select to enable one of them or both of them, and set the network parameters, including IP address, gateway, and subnet mask. The device can use the network interface to communicate with iVMS-4200 control client.

Steps:

1. In the backend, tap  to enter the Communication Settings page.
2. Tap **Network** to enter the Network tab.



3. Set the network interface parameters, including IP address, subnet mask, and gateway.

Notes:

- The device IP address and the PC's IP address should be in the same LAN.
- If using both of the network interfaces at the same time, the IP addresses of network interface 1 and 2 should be different to avoid IP address confliction.

4. Tap **Logout** to exit the page and save the parameters.

6.3.2 Setting COM Parameters

Purpose:

The device can be connected to other access control device via the COM interface. After selecting the baud rate, you can connect the device to other access control devices via RS-232 protocol or RS-485 protocol. For details about device linkage, see 6.13 Linking Access Control Device.

Steps:


1. Tap **COM** in the Communication Settings page to enter the COM tab.
2. Select a baud rate for RS-232 protocol and RS-485 protocol.
The parameters will be effective as soon as you have selected.

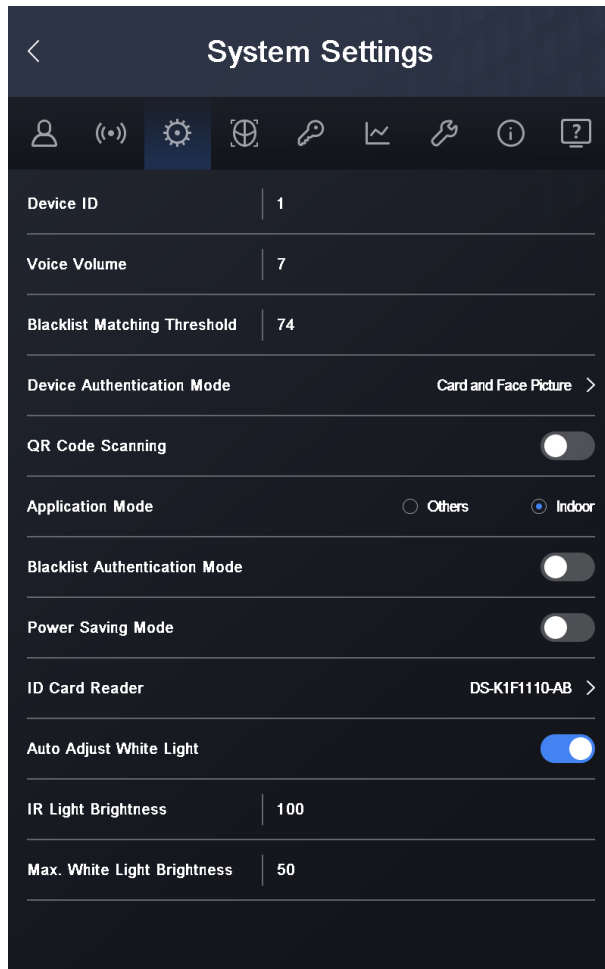
6.4 System Settings

Purpose:

In the System Settings page, you can set the parameters of device ID, live view in IR mode, voice volume, blacklist matching threshold, device authentication mode, QR code scanning, application mode, blacklist authentication mode, power saving mode, ID card reader, auto adjust white light brightness, IR light brightness, white light brightness, and Max. white light brightness.

Steps:

1. In the backend, tap  to enter the System Settings page.




2. Set the parameters.

The parameters descriptions are as follows:

Parameter Item	Description
Device ID	Set the device ID for device management. When the device is connected to a peripheral (access controller) via the RS-485 protocol, the device ID is the RS-485 protocol's DIP switch address. Note: The device ID should be numbers between 1 and 255.

Parameter Item	Description
Live View in IR Mode	The live view on the device screen will enter the IR mode.
Voice Volume	Adjust the voice prompt volume.
Blacklist Matching Threshold	Set the blacklist matching threshold when comparing user with the users in the blacklist.
Device Authentication Mode	<p>You can select the authentication mode.</p> <p>Auto: Authenticate via face picture, or face picture and card. When authenticating, if no card swiped, the device only starts 1:N authentication. If swiping card, the device will starts 1:1 authentication according to the face picture on the card.</p> <p>Face Picture: Authenticate via face picture only.</p> <p>Card + Face Picture: Authenticate via face picture and card</p> <p>Note: If you require a higher security level, do not use single authentication mode.</p>
QR Code Scanning	<p>Enable or disable the QR code scanning function. If enabling, the device camera can scan the QR code to authenticate instead of swiping card.</p> <p>Notes:</p> <ul style="list-style-type: none"> ● By default, the function is disabled. ● You can get the QR code from iVMS-4200 control client. For details about the operation, see the user manual of iVMS-4200 control client.
Application Mode	You can select the device application mode. You can select either others or indoor according to actual environment.
Blacklist Authentication Mode	<p>Enable or disable the function. If enabling, you should apply blacklist via iVMS-4200 control client before operation. After authentication completed, the system will judge whether the user is in the blacklist or not.</p> <p>Notes:</p> <ul style="list-style-type: none"> ● By default, the function is disabled. ● For details about applying users in blacklist, see the user manual of iVMS-4200 control client.
Power Saving Mode	<p>Enable or disable the function. If enabling, the device power will be saved.</p>
ID Card Reader	<p>If the device has connected to an external ID card reader, you should select an ID card reader model. If not, select None.</p> <p>Notes:</p> <ul style="list-style-type: none"> ● You should wire the ID card reader to the device USB

Parameter Item	Description
	interface if you want to connect an external ID card reader. <ul style="list-style-type: none"> The available ID card reader model are DS-K1F1110-A and DS-K1F1110-AB.
Auto Adjust White Light Brightness	If enabling the function, the device will adjust the white light brightness automatically according to the actual illumination. And you can set the max. brightness value. If disabling the function, the device supplement white light brightness will not be changed.
IR Light Brightness	Set the IR light's brightness. 0 represents the IR light is turned off.
White Light Brightness	Set the white light's brightness. 100 represents the most brightness, and 1 represents the darkest. 0 represents off.
Max. White Light Brightness	When the auto adjust white light brightness is enabled, you can set the brightness value. 100 represents the most brightness, and 1 represents the darkest. 0 represents off.

3. Click  to save the settings.

6.5 User Management

Purpose:


Manually add user information for authentication. You can add user name, card No., and face picture for the user. You can also view, search, and edit the added user.

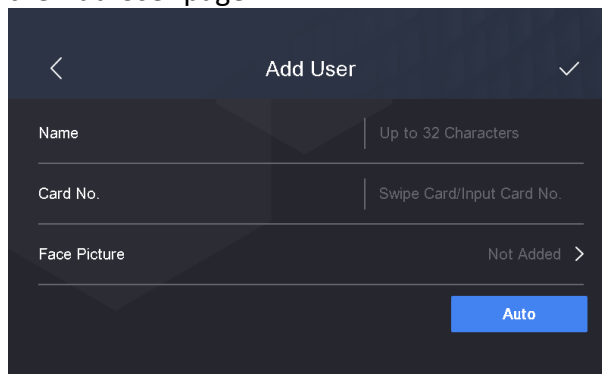
6.5.3 Adding User

Purpose:

You can swipe ID card to add the user automatically, or manually input the user information to add the user.

Steps:

1. In the backend, tap  to enter the User Management page.
2. Tap **Add User** to enter the Add User page.



3. Tap the Name text box and input the user name.

Input the user name via the popped up soft keyboard.

4. Tap the Card No. text box and input your card No.

Or you can swipe card on the device to gain the card No.

Note: Up to 20 digits or letters are allowed in the card No.

5. Add face picture.

- 1) Tap **Not Added** on the right of the Face Picture item to enter the face picture adding page.

- 2) Position the face looking at the device camera.

Make sure the face picture is in the blue square on this page and wait for the device recognition.

After adding the face picture completely, the prompt "Saved" will pop up.

- 3) Tap **Save** to save the parameters and go back to the Add User page.

Or wait for 3s and the system will go back to the Add User page automatically.

- 4) (Optional) Tap **Try Again** to delete the saved face picture and start adding face picture again.

Note: For details about the instructions of adding face pictures, see *Appendix A Tips When Collecting/Comparing Face Picture*.

6. Tap ✓ to save the parameters.

The added user will display in the user list.

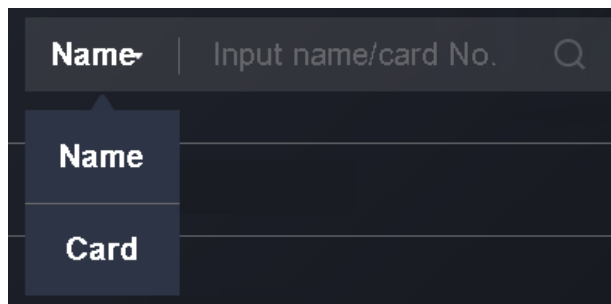
6.5.4 Searching User

Purpose:


When there are too many users in the user list, you can search for the required one via user name or card No.

Steps:

1. On the User Management page, tap **Name** or **Card No.** at the upper right corner of the page to select the search type.



2. Input the user name or card No. for search.

3. Tap  to start search.

The result will display in the user list.

6.5.5 Editing User

Purpose:

You can change the added user information by follow the steps below.

Steps:


1. On the User Management page, tap the user that you want to edit to enter the Edit User page. Refer to 6.5.3 Adding User to edit the user information.
2. Tap **Save** to save the parameters and go back to the User Management page.

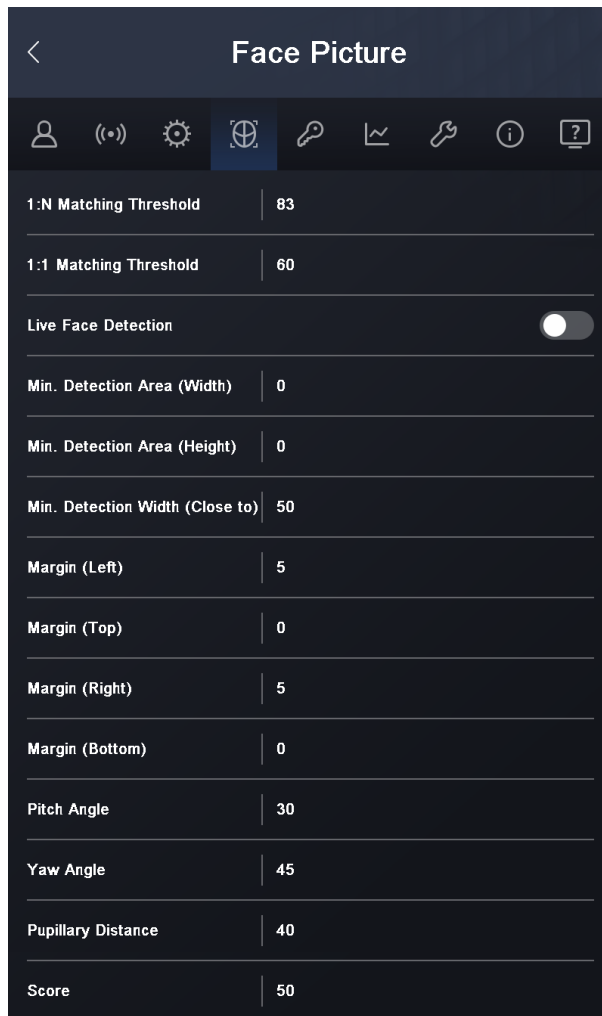
6.6 Setting Face Picture Parameters

Purpose:

You can set the face picture’s parameters for recognizing the face. The parameters includes 1:N matching threshold, 1:1 matching threshold, min. detection area (width), min. detection area (height), min. detection width (close to), margin (left), margin (top), margin (right), margin (bottom), pitch angle, yaw angle, pupillary distance, and score.

Steps:

1. In the backend, tap  to enter the Face Picture page.



2. Set the face picture parameters.
The description of each parameter item is as follows:

Parameter Item	Description
1:N Matching Threshold	Set the face picture matching threshold when authenticating via 1:N matching mode. Default Value: 83
1:1 Matching Threshold	Set the face picture matching threshold when authenticating via 1:1 matching mode. Default Value: 60
Min. Detection Area (Width)	When the distance between the camera and the user is long, the parameter represents the minimum percentage of the facial width in the total width of the recognition area. The actual percentage should be larger than the configured value when face picture authentication. Other percentages, distances and angles in this table should also meet their conditions. Recommended Value: 14
Min. Detection Area (Height)	When the distance between the camera and the user is long, the parameter represents the minimum percentage of the facial height in the total height of the recognition area. The actual percentage should be larger than the configured value when face picture authentication. Other percentages, distances and angles in this table should also meet their conditions. Recommended Value: 12
Min. Detection Width (Close to)	When the distance between the camera and the user is short, the parameter represents the minimum percentage of the facial width in the total width of the recognition area. The actual percentage should be larger than the configured value when face picture authentication. In this condition, the device will not detect other parameters.
Margin (Left)	The distance from the face left side to the left margin in the recognition area. The actual distance should be larger than the configured value when face picture authentication. Other percentages, distances, and angles should also meet their conditions.
Margin (Top)	The distance from the face top side to the top margin in the recognition area. The actual distance should be larger than the configured value when face picture authentication. Other percentages, distances, and angles should also meet their conditions.
Margin (Right)	The distance from the face right side to the right margin in the recognition area. The actual distance should be larger than the configured value when face picture authentication. Other percentages, distances, and angles should also meet their conditions.
Margin (Bottom)	The distance from the face bottom side to the bottom margin in the recognition area.

Parameter Item	Description
	The actual distance should be larger than the configured value when face picture authentication. Other percentages, distances, and angles should also meet their conditions.
Pitch Angle	The maximum pitch angle when face authentication. By default, the angle is 30°.
Yaw Angle	The maximum yaw angle when face authentication. By default, the angle is 20°.
Pupillary Distance	The minimum resolution between two pupils when face recognition. The actual resolution should be larger than the configured value. By default, the resolution is 40.
Score	Set the face picture's score when recognition. The device will score the captured picture according to the yaw angle, pitch angle, and pupillary distance. If the score is larger than the configured value, face recognition is failed.


3. Tap  to save the settings and leave the page.

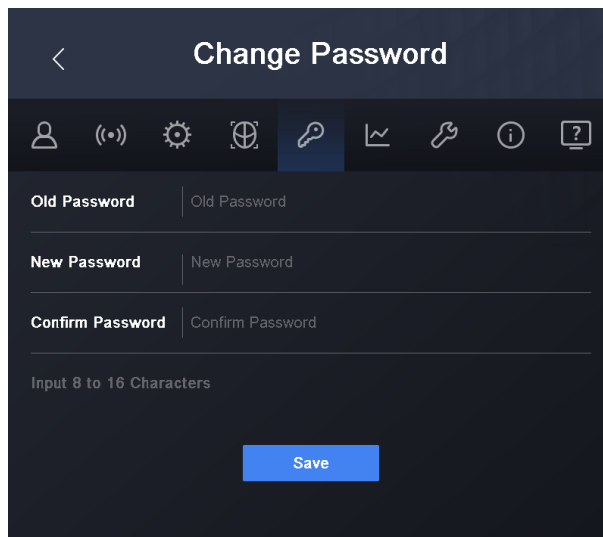
6.7 Changing Password

Purpose:


You can change the device password (activation password).

Steps:

1. In the backend, tap  to enter the Change Password page.



2. Input the old password, new password, and confirm the new password.
3. Tap **Save** to save the settings.

 **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.

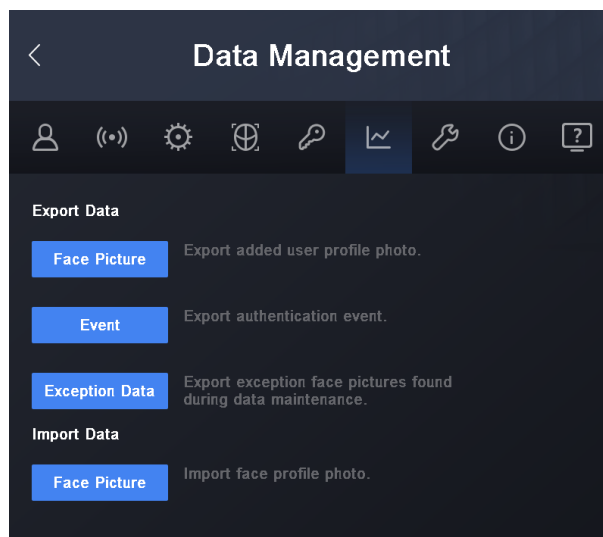
6.8 Managing Data

Purpose:

You can export added face pictures, and the authentication events and exception data from the system. You can also import the face information in batch to the system.

Steps:

1. Plug an USB flash drive in the device.
2. On the backend page, tap  to enter the Data Management page.



3. Tap **Face Picture**, **Event**, **Exception Data**, or **Face Picture** to export the face pictures, events, or exception data to the USB flash drive, and import the face picture from the USB flash drive respectively.

Notes:

- The name format of the imported face picture: Card No._Name_Department_Employee ID_Gender
- The imported face picture should contain the user's frontal face with the format of JPEG or JPG. The face picture's resolution should be 640 × 480 or more. The picture size should be between 60 KB and 200 KB. The pupillary distance of the picture should to more than 60p.
- The importing and exporting file should be Excel file.

6.9 Maintaining System

Purpose:


You can restore to default settings or factory settings. You can also upgrade the system.

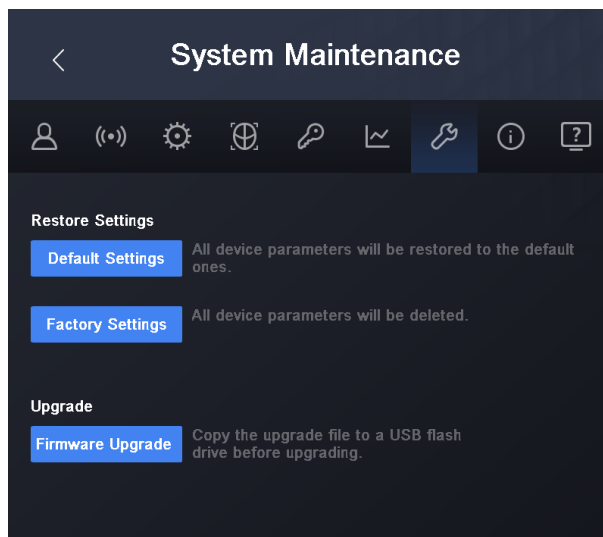
6.9.6 Restoring Device Parameters

Purpose:

You can restoring the device parameters to the default or to the factory.

Steps:

1. In the backend page, tap  to enter the System Maintenance page.



2. Tap **Default Settings** or **Factory Settings**.

Default Settings: All parameters will be restored to the default except for the device IP address.

Factory Settings: All parameters will be deleted. Activation is required the next time you start the device.

6.9.7 Upgrading Firmware


Purpose:

If there is new version available or the current firmware version is too low, you can upgrade the device firmware via the USB interface.

Steps:

1. Plug an USB flash drive in the device USB interface.


Note: Make sure there are upgrading file in the USB flash drive. The upgrading file's name should be digicap.dav

2. In the backend page, tap  to enter the System Maintenance page.
3. Tap **Firmware Upgrade**.


The device will read the upgrading file in the USB flash drive automatically and start upgrading.

Note: the upgrading file should be in the root directory.

6.10 Viewing System Information

In the backend page, tap  and you can view the total capacity and the capacity usage of the face pictures, card, event, and fingerprint.

6.11 Viewing Device Information

In the backend page, tap  and you can view the device name, the software version, the firmware version, and the open source code license.

6.12 Authenticating Identity

Purpose:

After setting network, system parameters and adding user, you can go back to the initial page for identity authentication.

The system will authenticate person according to the configured authentication mode.

You can authenticate identity via 1:1 matching or 1:N matching.

Note: If you require a higher security level, do not use single authentication mode.

1:N Matching: Compare the captured face picture or the collected fingerprint with all face pictures or all fingerprint pictures stored in the terminal.

1: 1 Matching: When swiping card or ID card, compare the captured face picture or the collected fingerprint with the information stored in the card (or ID card).

Before you start:

You should configure the terminal authentication mode. For details, see *6.4 System Settings*.

6.12.8 Authenticating via 1:1 Matching

Steps:

1. If the authentication mode is Card + Face Picture, or Auto, swipe card in the card swiping area.

Note: The card can be normal IC card, encrypted card, or ID card.

If the QR Code Scanning function is enabled, you can put the QR code in front of the device camera to authenticate via QR code.

2. (Optional) If the Blacklist Authentication Mode function is enabled, the device will compare the authentication information with the blacklist.

If the user is in the blacklist, a prompt of identity exception will pop up on the auxiliary screen and the device will send a blacklist alarm to the control center.

Notes:

- For details about enabling the Blacklist Authentication Mode function, see *6.4 System Settings*.

- You can connect an external HDMI screen as an auxiliary screen.
3. If the authentication mode is Card + Face Picture or Auto, position the face looking at the camera to authenticate face.

If authentication succeeded, the prompt “Authenticated” will pop up.

Notes:

- For better face picture authentication, the user height should be between 140 cm and 190 cm and the distance between the user and the device should be between 30 cm and 100 cm.
- For detailed information about authenticating face picture, see *Appendix A Tips When Collecting/Comparing Face Picture*.

6.12.9 Authenticating via 1:N Matching

If the authentication mode is Face Picture or Auto, position the face looking at the camera to start face picture authentication.

If authentication completed, a prompt “Authenticated” will pop up.

6.13 Linking Access Control Device

Purpose:

The face recognition terminal can connect to an access control device via RS-232 protocol and transmit authentication information to the access control device at the same time.

The access control device can control the door status according to authentication result and the access control device authentication mode, and transmit the door events to the control client or other systems.

Before you start:

- Make sure the access control device has connected to the face recognition terminal via RS-232 protocol.
- Make sure the face recognition terminal and the access control device are powered on.

Steps:

1. Set the baud rate of the RS-232 protocol in the COM tab.

Note: The face recognition terminal’s baud rate of RS-232 protocol should be the same as the access control device’s. For details about setting the baud rate of the RS-232 protocol, see *6.3.2 Setting COM Parameters*.

2. Authenticate via the face recognition terminal.

The face recognition terminal will send the authentication result and the card No. to the access control device. The access control device will control the door status according to the result. And it will also send the related events to the client or other systems.

Note: For details about access control device’s authentication mode, see the user manual of the related access control device.

Chapter 7 Client Operation

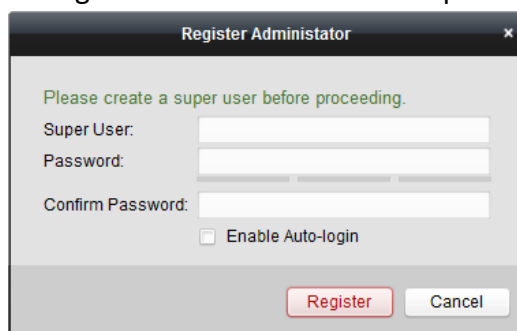
You can set and operate the access control devices via the client software. This chapter will introduce the access control device related operations in the client software. For integrated operations, refer to *User Manual of iVMS-4200 Client Software*.

7.1 User Registration and Login

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

Steps:

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

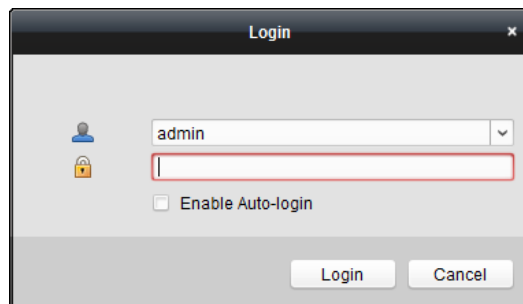


- ◆ A user name cannot contain any of the following characters: / \ : * ? " < > |. And the length of the password cannot be less than 6 characters.
- ◆ For your privacy, we strongly recommend changing the password to something of your own choosing (using a minimum of 8 characters, including upper case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

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

Steps:

1. Input the user name and password you registered.
2. Optionally, check the checkbox **Enable Auto-login** to log into the software automatically.
3. Click **Login**.



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

7.2 System Configuration

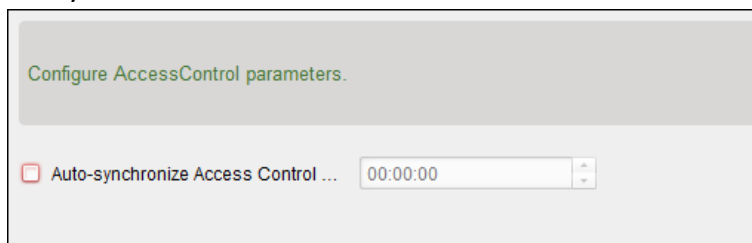
Purpose:

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

Steps:

1. Click **Tool – System Configuration**.
2. In the System Configuration window, check the **Auto-synchronize Access Control Event** checkbox.
3. Set the synchronization time.

The client will auto-synchronize the missed access control event to the client at the set time.



7.3 Access Control Management

Purpose:


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

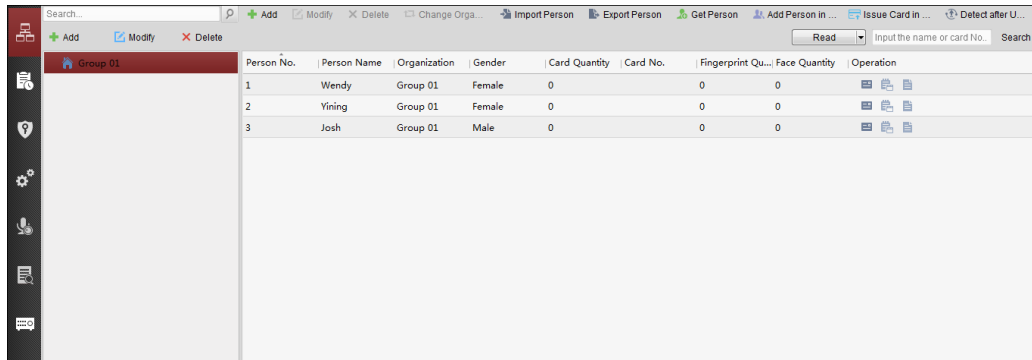
You can also set the event configuration for access control and display access control points and zones on E-map.

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



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

Click  to enter the Access Control module.

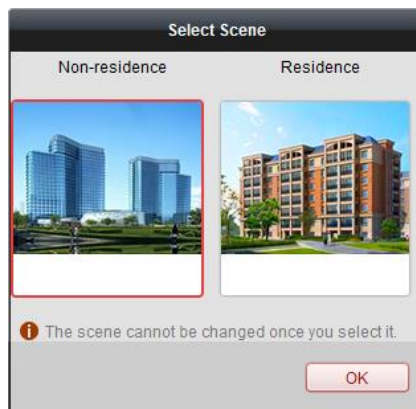


Before you start:

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


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

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



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

7.3.1 Adding Access Control Device

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

Device Type	Nickname	Connection ...	Network Parameters	Device Serial No.
Access Controller	Access Controller	TCP/IP	10.18.146.86:8000	DS- [REDACTED] 6
Encoding Device	10.33.3.159	TCP/IP	10.33.3.159:8000	DS- [REDACTED] 3
Encoding Device	10.16.6.250	TCP/IP	10.16.6.250:8000	2014- [REDACTED]
Encoding Device	10.20.132.215	TCP/IP	10.20.132.215:8000	DS- [REDACTED] 7
Encoding Device	10.66.76.193	TCP/IP	10.66.76.193:8005	DS- [REDACTED] J
Indoor Station	Indoor Station	TCP/IP	10.16.6.104:8000	DS- [REDACTED] J
Security Control Panel	Security Control Pa...	TCP/IP	10.18.146.81:8000	DS- [REDACTED] U
Security Control Panel	10.16.6.92	TCP/IP	10.16.6.92:8000	DS- [REDACTED] 7

Note: After adding the device, you should check the device arming status in **Tool – Device Arming Control**. If the device is not armed, you should arm it, or you will not receive the real-time events via the client software. For details about device arming control, see *7.12 Arming Control*.

Creating Password

Purpose:

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

Note: This function should be supported by the device.

Steps:

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

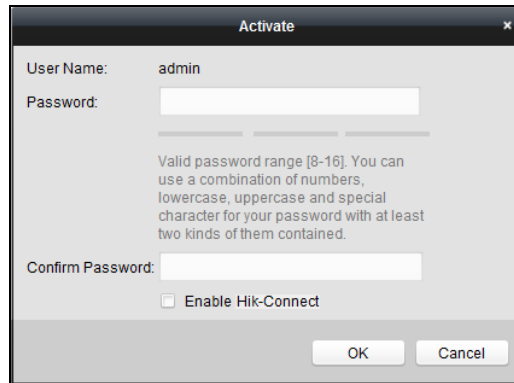
IP	Device Type	Firmware Version	Security	Server Port	Device Serial No.	Start Time
192.0.0.64	[REDACTED]	[REDACTED]	Active	8000	[REDACTED]	2017-01
192.168.1.64	[REDACTED]	[REDACTED]	Inactive	8000	[REDACTED]	2017-01

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

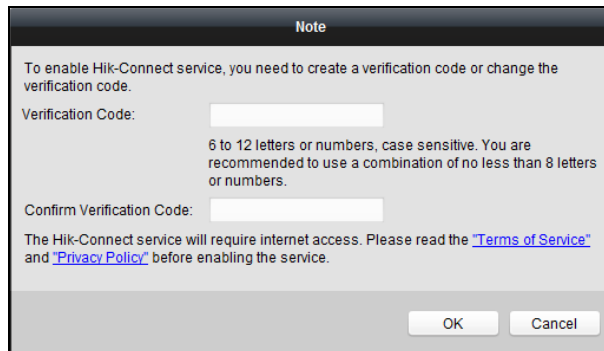


STRONG PASSWORD RECOMMENDED– We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product.

And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.



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



- 2) Create a verification code.
 - 3) Confirm the verification code.
 - 4) Click **Terms of Service** and **Privacy Policy** to read the requirements.
 - 5) Click **OK** to enable the Hik-Connect service.
6. Click **OK** to activate the device.

A "The device is activated." window pops up when the password is set successfully.
7. Click **Modify Netinfo** to pop up the Modify Network Parameter interface.

Note: This function is only available on the **Online Device** area. You can change the device IP address to the same subnet with your computer if you need to add the device to the software.
8. Change the device IP address to the same subnet with your computer by either modifying the IP address manually or checking the checkbox of DHCP.
9. Input the password set in step 4 and click **OK** to complete the network settings.

The screenshot shows a dialog box titled "Modify Network Parameter". It is divided into two main sections: "Device Information" and "Network Information".


- Device Information:**
 - MAC Address: [Text Field] [Copy]
 - Software Version: [Text Field] [Copy]
 - Device Serial No.: [Text Field] [Copy]
- Network Information:**
 - DHCP
 - Port: [Text Field] 8000
 - IPv4(Don't Save)
 - IP Address: [Text Field] 10.16.1.233
 - Subnet Mask: [Text Field] 255.255.255.0
 - Gateway: [Text Field] 10.16.1.254
 - IPv6(Don't Save)
 - Password: [Text Field] [Masked]

At the bottom right, there are "OK" and "Cancel" buttons.

Adding Online Device

Purpose:

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

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

The screenshot shows a window titled "Online Device (19)" with a "Refresh Every 60s" button. Below the title bar are several action buttons: "Add to Client", "Add All", "Modify Netinfo", "Reset Password", and "Activate". A "Filter" input field is also present. The main area contains a table with the following data:

IP	Device Type	Firmware Version	Security	Server Port	Device Serial No.	Start Time
10.16.6.236	D	[Masked]	Active	8000	[Masked]	2017-01
10.16.6.92	D	[Masked]	Active	8000	[Masked]	2017-01
192.0.0.64	D	[Masked]	Active	8000	[Masked]	2017-01

Steps:

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

Note: For the inactive device, you need to create the password for it before you can add the device properly.

2. Click **Add to Client** to open the device adding dialog box.
3. Input the required information.

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

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

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

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

Password: Input the device password.



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. Optionally, check the **Export to Group** checkbox to create a group by the device name. You can import all the channels of the device to the corresponding group by default.

Note: iVMS-4200 also provides a method to add the offline devices.

- 1) Check the **Add Offline Device** checkbox.
- 2) Input the required information, including the device channel number and alarm input number.
- 3) Click **Add**.

When the offline device comes online, the software will connect it automatically.

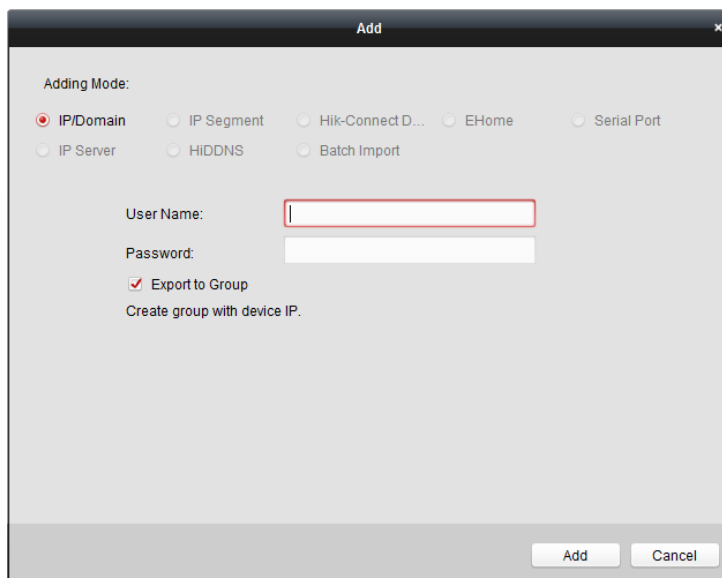
5. Click **Add** to add the device.

➤ Adding Multiple Online Device

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

➤ Adding All Online Devices

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



Adding Devices by IP or Domain Name

Steps:

1. Click **Add** to open the device adding dialog box.
2. Select **IP/Domain** as the adding mode.
3. Input the required information.

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

Address: Input the device's IP address or domain name.

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

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

Password: Input the device password.



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. Optionally, check the **Export to Group** checkbox to create a group by the device name. You can import all the channels of the device to the corresponding group by default.

Note: iVMS-4200 also provides a method to add the offline devices.

- 1) Check the **Add Offline Device** checkbox.
- 2) Input the required information, including the device channel number and alarm input number.
- 3) Click **Add**.

When the offline device comes online, the software will connect it automatically.

5. Click **Add** to add the device.

Adding Devices by IP Segment

Steps:

1. Click **Add** to open the device adding dialog box.
2. Select **IP Segment** as the adding mode.
3. Input the required information.

Start IP: Input a start IP address.

End IP: Input an end IP address in the same network segment with the start IP.

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

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

Password: Input the device password.



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. Optionally, check the **Export to Group** checkbox to create a group by the device name. You can import all the channels of the device to the corresponding group by default.

Note: iVMS-4200 also provides a method to add the offline devices.

- 1) Check the **Add Offline Device** checkbox.
- 2) Input the required information, including the device channel number and alarm input number.
- 3) Click **Add**.

When the offline device comes online, the software will connect it automatically.

5. Click **Add**.

You can add the device which the IP address is between the start IP and end IP to the device list.

Adding Devices by Hik-Connect Domain

Purpose:

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

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

➤ Add Single Device

Steps:

1. Click **Add** to open the device adding dialog.
2. Select **Hik-Connect Domain** as the adding mode.
3. Select **Single Adding**.
4. Input the required information.

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

Device Serial No.: Input the device serial No.

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

Password: Input the device 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.

Hik-Connect Account: Input the Hik-Connect account.

Hik-Connect Password: Input the Hik-Connect password.

- Optionally, check the **Export to Group** checkbox to create a group by the device name. You can import all the channels of the device to the corresponding group by default.
- Click **Add** to add the device.

The screenshot shows a dialog box titled "Add" with a close button (X) in the top right corner. The "Adding Mode:" section contains several radio button options: IP/Domain, IP Segment, Hik-Connect D... (selected), EHome, Serial Port, IP Server, HIDDNS, and Batch Import. Below this, the "Adding Mode:" section has two radio buttons: Batch Adding and Single Adding (selected). There are input fields for Nickname, Device Serial No., User Name, Password, Hik-Connect Account, and Hik-Connect Password. A checkbox labeled "Export to Group" is checked. Below the checkbox, there is a note: "Set the device name as the group name and add all the channels connected to the device to the group." At the bottom right, there are "Add" and "Cancel" buttons.

Add Devices in Batch

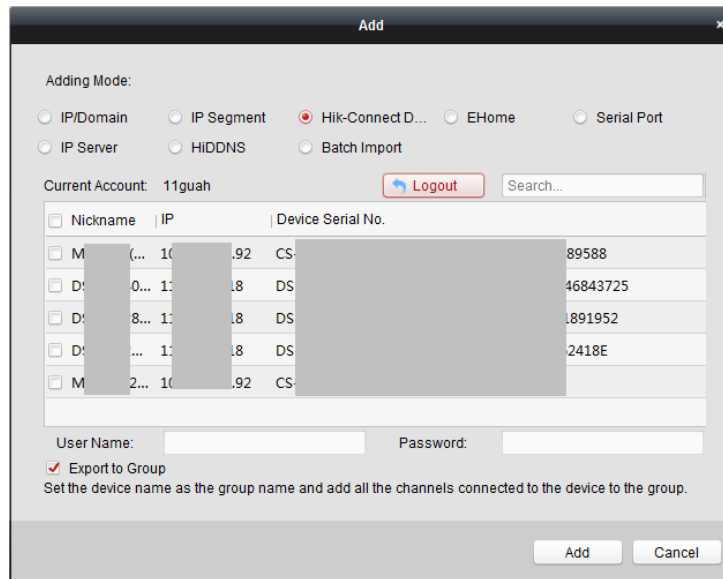
Steps:

- Click **Add** to open the device adding dialog.

The screenshot shows the same "Add" dialog box. In this view, the "Adding Mode:" section has "Batch Adding" selected. The "Hik-Connect Account:" and "Hik-Connect Password:" fields are visible, along with a "Get Device List" button. The "Export to Group" checkbox is not visible in this view. At the bottom right, there are "Add" and "Cancel" buttons.

- Select **Hik-Connect Domain** as the adding mode.
- Select **Batch Adding**.
- Input the required information.
Hik-Connect Account: Input the Hik-Connect account.
Hik-Connect Password: Input the Hik-Connect password.

- Click **Get Device List** to show the devices added to Hik-Connect account.



- Check the checkbox(es) to select the device as desired.
- Input the user name and password for the devices to be added.
- Optionally, check the **Export to Group** checkbox to create a group by the device name. You can import all the channels of the device to the corresponding group by default.
- Click **Add** to add the devices.

Adding Devices by EHome Account

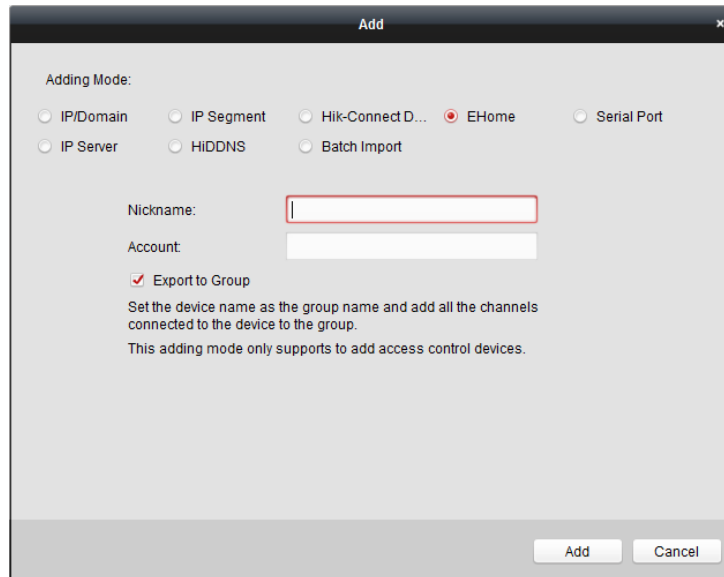
Purpose:

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

Before you start: Set the network center parameter first. For details, refer to *Chapter 7.3.4 Network Settings*.

Steps:

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



3. Input the required information.

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

Account: Input the account name registered on EHome protocol.

4. Optionally, check the **Export to Group** checkbox to create a group by the device name. You can import all the channels of the device to the corresponding group by default.

Note: iVMS-4200 also provides a method to add the offline devices.

1) Check the **Add Offline Device** checkbox.

2) Input the required information, including the device channel number and alarm input number.

3) Click **Add**.

When the offline device comes online, the software will connect it automatically.

5. Click **Add** to add the device.

Adding Devices by Serial Port

Purpose:

You can add access control device connected via serial port.

Steps:

1. Click **Add** to open the device adding dialog box.

2. Select **Serial Port** as the adding mode.

Adding Mode:

IP/Domain IP Segment Hiik-Connect D... EHome Serial Port

IP Server HiDDNS Batch Import

Nickname:

Serial Port No.

Baud Rate

DIP:

Export to Group

Set the device name as the group name and add all the channels connected to the device to the group.
This adding mode only supports to add access control devices.

Add Cancel

3. Input the required information.
 - Nickname:** Edit a name for the device as you want.
 - Serial Port No.:** Select the device's connected serial port No.
 - Baud Rate:** Input the baud rate of the access control device.
 - DIP:** Input the DIP address of the device.
4. Optionally, check the **Export to Group** checkbox to create a group by the device name. You can import all the channels of the device to the corresponding group by default.

Note: iVMS-4200 also provides a method to add the offline devices.

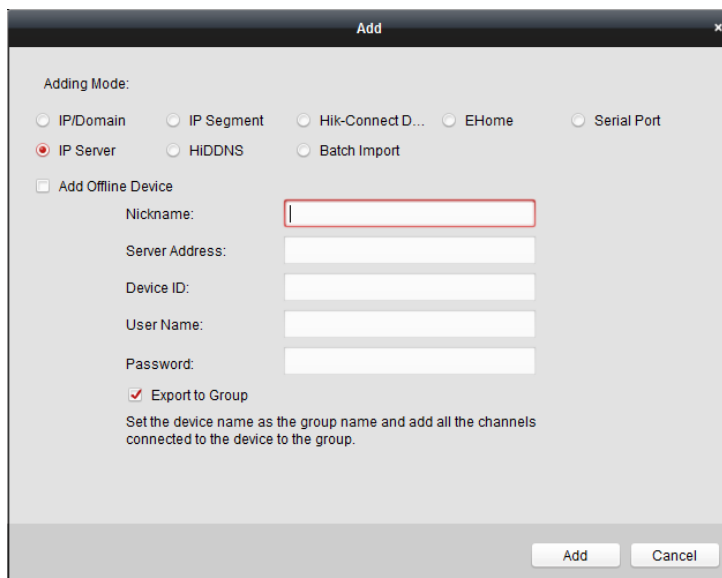
 - 1) Check the **Add Offline Device** checkbox.
 - 2) Input the required information, including the device channel number and alarm input number.
 - 3) Click **Add**.

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

Adding Devices by IP Server

Steps:

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



3. Input the required information.

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

Server Address: Input the IP address of the PC that installs the IP Server.

Device ID: Input the device ID registered on the IP Server.

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

Password: Input the device 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. Optionally, check the **Export to Group** checkbox to create a group by the device name. You can import all the channels of the device to the corresponding group by default.

Note: iVMS-4200 also provides a method to add the offline devices.

1) Check the **Add Offline Device** checkbox.

2) Input the required information, including the device channel number and alarm input number.

3) Click **Add**.

When the offline device comes online, the software will connect it automatically.

5. Click **Add** to add the device.

Adding Devices by HiDDNS

Steps:

1. Click **Add** to open the device adding dialog box.

2. Select **HiDDNS** as the adding mode.

3. Input the required information.

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

Server Address: www.hik-online.com.

Device Domain Name: Input the device domain name registered on HiDDNS server.

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

Password: Input the device 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. Optionally, check the **Export to Group** checkbox to create a group by the device name. You can import all the channels of the device to the corresponding group by default.

Note: iVMS-4200 also provides a method to add the offline devices.

1) Check the **Add Offline Device** checkbox.

2) Input the required information, including the device channel number and alarm input number.

3) Click **Add**.

When the offline device comes online, the software will connect it automatically.

5. Click **Add** to add the device.

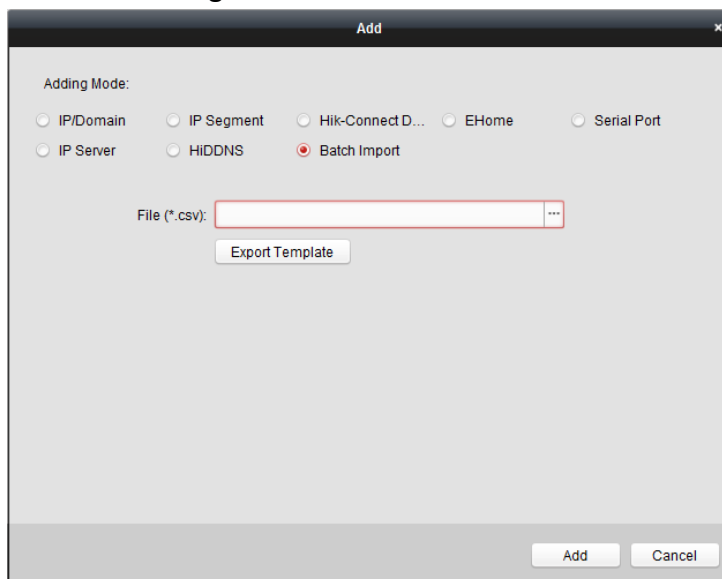
Importing Devices in Batch

Purpose:

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

Steps:

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




3. Click **Export Template** and save the pre-defined template (CSV file) on your PC.
4. Open the exported template file and input the required information of the devices to be added on the corresponding column.
 - **Nickname:** Edit a name for the device as you want.
 - **Adding Mode:** You can input 0, 2, 3, 4, 5, or 6 which indicated different adding modes. 0 indicates that the device is added by IP address or domain name; 2 indicates that the device is added via IP server; 3 indicates that the device is added via HiDDNS; 4 indicates that the device is added via EHome protocol; 5 indicates that the device is added by serial port; 6 indicates that the device is added via Hik-Connect Domain.
 - **Address:** Edit the address of the device. If you set 0 as the adding mode, you should input the IP address or domain name of the device; if you set 2 as the adding mode, you should input the IP address of the PC that installs the IP Server; if you set 3 as the adding mode, you should input *www.hik-online.com*.
 - **Port:** Input the device port No.. The default value is *8000*.
 - **Device Information:** If you set 0 as the adding mode, this field is not required; if you set 2 as the adding mode, input the device ID registered on the IP Server; if you set 3 as the adding mode, input the device domain name registered on HiDDNS server; if you set 4 as the adding mode, input the EHome account; if you set 6 as the adding mode, input the device serial No.
 - **User Name:** Input the device user name. By default, the user name is *admin*.
 - **Password:** Input the device password.



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.

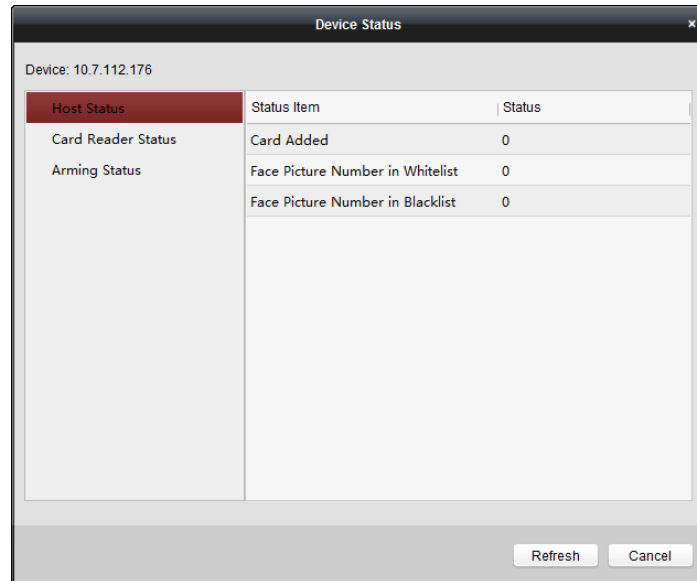
- **Add Offline Device:** You can input 1 to enable adding the offline device, and then the software will automatically connect it when the offline device comes online. 0 indicates disabling this function.
 - **Export to Group:** You can input 1 to create a group by the device name (nickname). All the channels of the device will be imported to the corresponding group by default. 0 indicates disabling this function.
 - **Channel Number:** If you set 1 for Add Offline Device, input the channel number of the device. If you set 0 for Add Offline Device, this field is not required.
 - **Alarm Input Number:** If you set 1 for Add Offline Device, input the alarm input number of the device. If you set 0 for Add Offline Device, this field is not required.
 - **Serial Port No.:** If you set 5 as the adding mode, input the serial port No. for the access control device.
 - **Baud Rate:** If you set 5 as the adding mode, input the baud rate of the access control device.
 - **DIP:** If you set 5 as the adding mode, input the DIP address of the access control device.
 - **Hik-Connect Account:** If you set 6 as the adding mode, input the Hik-Connect account.
 - **Hik-Connect Password:** If you set 6 as the adding mode, input the Hik-Connect password.
5. Click  and select the template file.
 6. Click **Add** to import the devices.

The devices will be displayed on the device list for management after added successfully. You can check the resource usage, HDD status, recording status, and other information of the added devices on the list.

Click **Refresh All** to refresh the information of all added devices. You can also input the device name in the filter field for search.

7.3.2 Viewing Device Status

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



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

- **Host Status:** The status of the host, including Added Card Number, Face Picture Number in Whitelist, and Face Picture Number in Blacklist.
- **Card Reader Status:** The status of card reader, including the card reader serial No., card reader online status, and current authentication method for card reader.
- **Arming Status:** The arming type and armed IP address of the device.

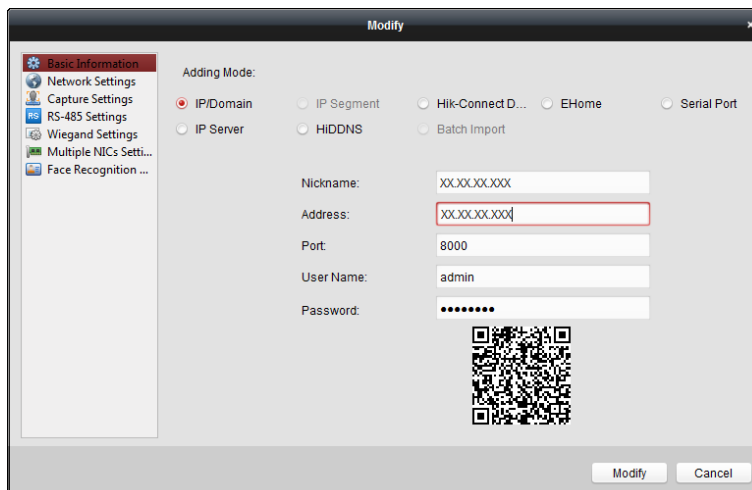
7.3.3 Editing Basic Information

Purpose:

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

Steps:

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



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

7.3.4 Network Settings

Purpose:

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

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

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

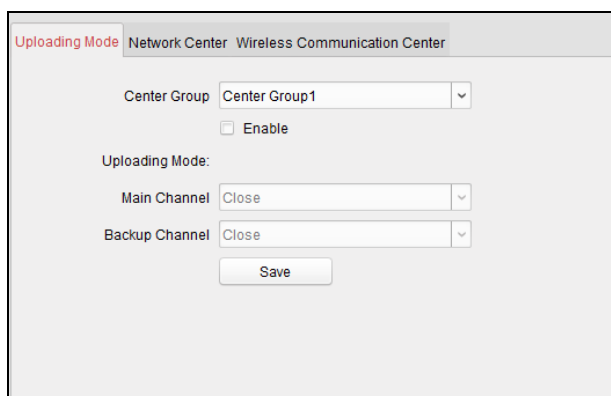
Uploading Mode Settings

Purpose :

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

Steps:

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



2. Select the center group in the dropdown list.
3. Check the **Enable** checkbox to enable the selected center group.
4. Select the uploading mode in the dropdown list. You can enable **N1/G1** for the main channel

and the backup channel, or select **Close** to disable the main channel or the backup channel.

Note: The main channel and the backup channel cannot enable N1 or G1 at the same time.

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

Network Center Settings

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

Steps:

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

2. Select the center group in the dropdown list.
3. Select the Address Type as **IP Address** or **Domain Name**.
4. Input IP address or domain name according to the address type.
5. Input the port No. for the protocol. By default, the port No. is 7660.
6. Select the protocol type as EHome.
7. Set an account name for the network center.

Note: The account should contain 1 to 32 characters and only letters and numbers are allowed.

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

Notes:

- The port No. of the wireless network and wired network should be consistent with the port No. of EHome.
- You can set the domain name in Enable NTP area *Editing Time* section in Remote Configuration. For details, refer to *Time* in Remote Configuration.

Wireless Communication Center Settings

Steps:

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

The screenshot shows a configuration window for a Network Center. At the top, there are tabs for 'Uploading Mode', 'Network Center', and 'Wireless Communication Center'. The 'Wireless Communication Center' tab is active. Below the tabs, there are several input fields: 'APN Name' is a dropdown menu; 'SIM Card No.' is a text input field; 'Center Group' is a dropdown menu with 'Center1' selected; 'IP Address' is a text input field containing '0.0.0.0'; 'Port' is a text input field; 'Protocol Type' is a dropdown menu; and 'Account' is a text input field. A 'Save' button is located at the bottom center of the form.

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

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

7.3.5 Capture Settings

You can set the parameters of capture linkage and manual capture.

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

Click **Capture Settings** tab to enter the capture settings interface.

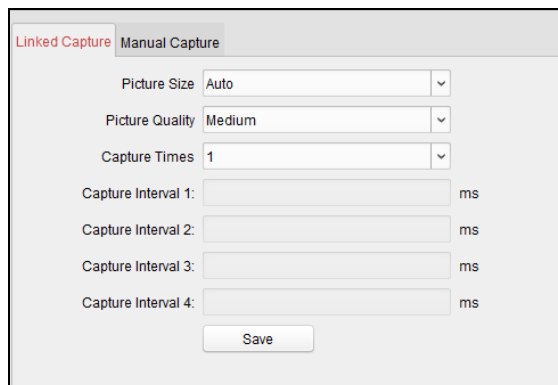
Notes:

- The **Capture Settings** should be supported by the device.
- Before setting the capture setting, you should configure the storage server for picture storage.

Linked Capture

Steps:

1. Select the **Linked Capture** tab.

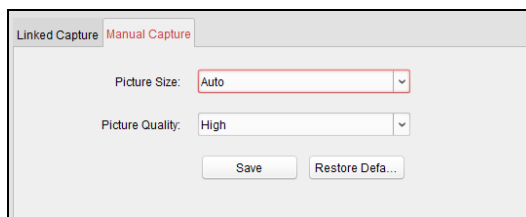


2. Set the picture size and quality.
3. Set the linked capture times once triggered.
4. Set the capture interval according to the capture times.
5. Click **Save** to save the settings.

Manual Capture

Steps:

1. Select the **Manual Capture** tab.



2. Select the resolution of the captured pictures from the dropdown list.
3. Select the picture quality as High, Medium, or Low.
4. Click **Save** to save the settings.
5. You can click **Restore Default Value** to restore the parameters to default settings.

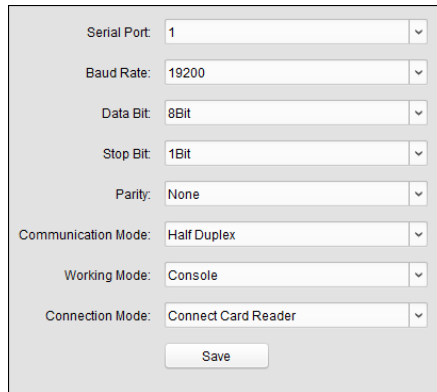
7.3.6 RS-485 Settings

Purpose:

You can set the RS-485 parameters including the baud rate, data bit, the stop bit, parity type, communication mode, work mode, and connection mode.

Steps:

1. Select the device in the device list, and click **Modify** to pop up the modifying device information window.
2. Click **RS-485 Settings** tab to enter the RS-485 settings interface.



Serial Port: 1

Baud Rate: 19200

Data Bit: 8Bit

Stop Bit: 1Bit

Parity: None

Communication Mode: Half Duplex

Working Mode: Console

Connection Mode: Connect Card Reader

Save

2. Select the serial No. of the port from the dropdown list to set the RS-485 parameters.
3. Set the baud rate, data bit, the stop bit, parity, communication mode, working mode, and the connection mode from the dropdown list.
4. Click **Save** to save the settings and the configured parameters will be applied to the device automatically.

Note: After changing the working mode, the device will be rebooted. A prompt will be popped up after changing the working mode.

7.3.7 Wiegand Settings

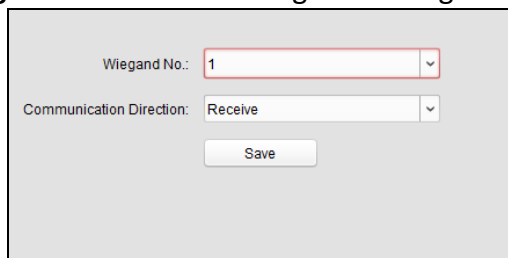
Purpose:

You can set the Wiegand channel and the communication mode.

Note: The Wiegand Settings should be supported by the device.

Steps:

1. Select the device in the device list, and click **Modify** to pop up the modifying device information window.
2. Click the **Wiegand Settings** tab to enter the Wiegand Settings interface.



Wiegand No.: 1

Communication Direction: Receive

Save

3. Select the Wiegand channel No. and the communication mode in the dropdown list.
If you set the **Communication Direction** as **Send**, you are required to set the Wiegand Mode as Wiegand 26 or Wiegand 34.
4. Click **Save** to save the settings and the configured parameters will be applied to the device automatically.

Note: After changing the communication direction, the device will be rebooted. A prompt will be popped up after changing the communication direction.

7.3.8 Setting Multiple NICs

Purpose:

You can set the parameters of NIC, NIC type, IPv4 address, Subnet Mask, Default Gateway, MAC, MTU, and device port.

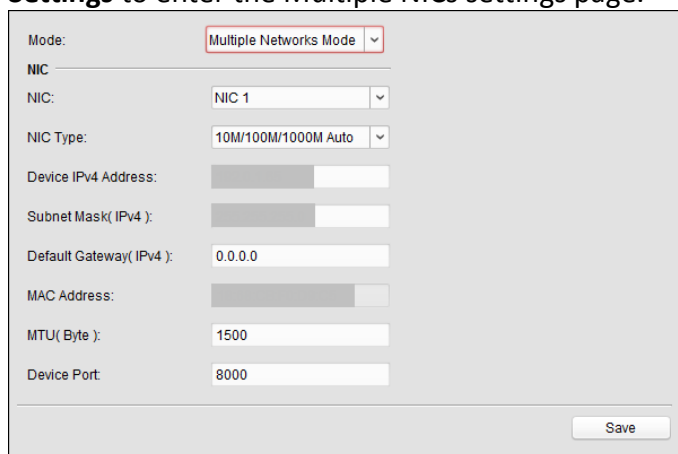
Note: The function should be supported by the device.

Before you start:

Adding devices by EHome account.

Steps:

1. Click **Multiple NICs Settings** to enter the Multiple NICs settings page.



Mode:	Multiple Networks Mode
NIC	
NIC:	NIC 1
NIC Type:	10M/100M/1000M Auto
Device IPv4 Address:	
Subnet Mask(IPv4):	
Default Gateway(IPv4):	0.0.0.0
MAC Address:	
MTU(Byte):	1500
Device Port:	8000
<input type="button" value="Save"/>	

2. Set the parameters as you desired.
3. Click **Save** to save the settings.

7.3.9 Setting Face Recognition Terminal

Purpose:

You can set the face recognition terminal's mode, including the face recognition database, authenticate by QR code, save authenticating face, etc.

Note: The function should be supported by the device.

Steps:

1. Click **Face Recognition Terminal Settings** to enter the Face Recognition Terminal Settings page.

The screenshot shows a configuration window titled "Device Mode". It contains the following elements:

- COM: A dropdown menu with "COM1" selected.
- Face Picture Database: A dropdown menu with "Deep Learning" selected.
- Authenticate by QR Code: A checkbox that is unchecked.
- Blacklist Authentication: A checkbox that is unchecked.
- Save Authenticating Face Picture: A checkbox that is checked.
- MCU Version: A text field containing "build 20180517".
- A "Save" button at the bottom center.

2. Set the face recognition terminal's parameters.

The parameters descriptions are as follows:

Parameter	Description
COM	Select a COM port for configuration. COM1 refers to the RS-485 interface and COM2 refers to the RS-232 interface.
Face Picture Database	You can select Deep Learning as the face picture database.
Authenticate by QR Code	If enabling the function, the device camera can scan the QR code to authenticate. By default, the function is disabled.
Blacklist Authentication	If enable the function, the device will authenticate the person to with the persons in the blacklist. Note: For details about importing persons in blacklist, see <i>7.8.6 Person in Blacklist</i> .
Save Authenticating Face Picture	If enabling the function, the captured face picture when authenticating will be saved to the device.
MCU Version	View the device MCU version.

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

You can also set the parameters in the Remote Configuration. For details, see *Configuring Face Recognition Terminal Parameters* in Section 7.3.10 Remote Configuration.

7.3.10 Remote Configuration

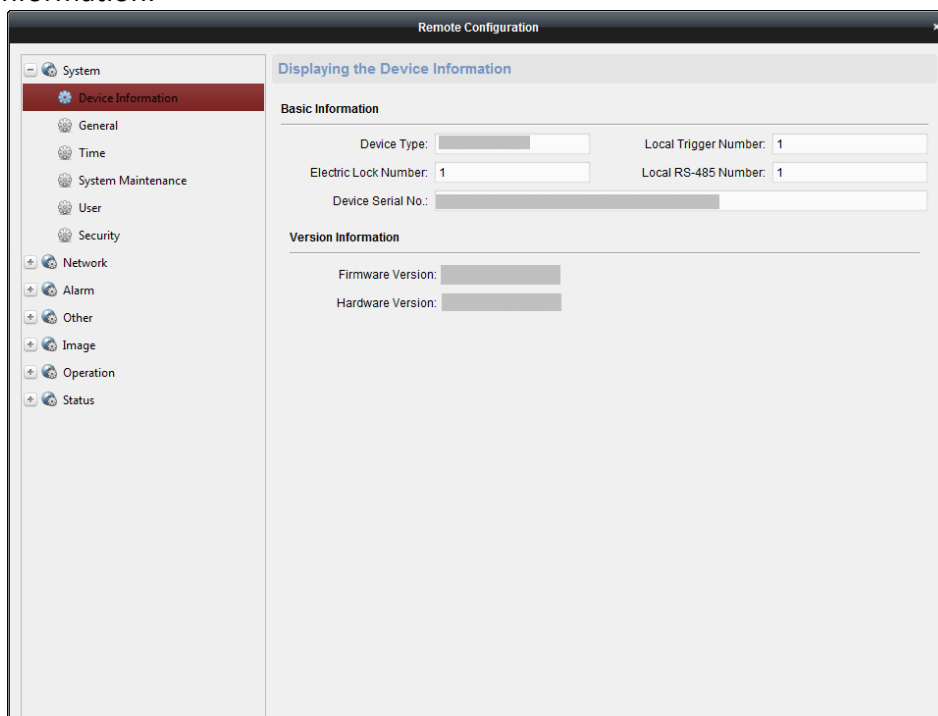
Purpose:

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

Checking Device Information

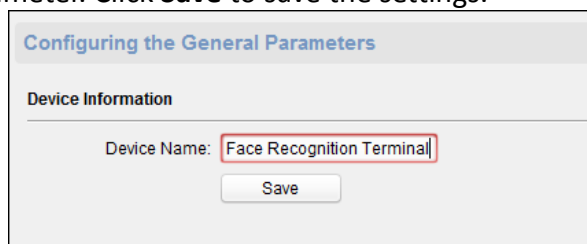
Steps:

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



Editing Device Name

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



Editing Time

Steps:

1. In the Remote Configuration interface, click **System** -> **Time** to configure the time zone.
2. (Optional) Check **Enable NTP** and configure the NTP server address, the NTP port, and the synchronization interval.
3. (Optional) Check **Enable DST** and configure the DST star time, end time and the bias.
4. Click **Save** to save the settings.

Setting System Maintenance

Purpose:

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

Steps:

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

2. Click **Reboot** to reboot the device.

Or click **Restore Default Settings** to restore the device settings to the default ones, excluding the IP address.

Or click **Restore All** to restore the device parameters to the default ones. The device should be activated after restoring.

Note: The configuration file contains the device parameters.

Or click **Import Configuration File** to import the configuration file from the local PC to the device.

Or click **Export Configuration File** to export the configuration file from the device to the local PC

Note: The configuration file contains the device parameters.

3. You can also remote upgrade the device.

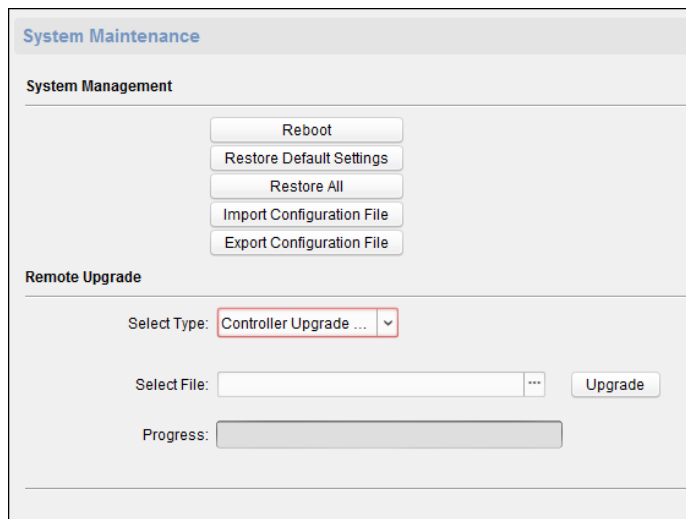
1) In the Remote Upgrade part, select an upgrade type from the drop-down list.

Notes:

- You need to set the device ID before upgrading if you select Controller Upgrade File as the remote upgrade type.
- Only the card reader that connected via RS-485 protocol supports upgrading.
- If you need to upgrade the device system, make sure the controller version and the extension module's version are the same. Here the controller refers to the TX1 system while the extension module refers to the MCU system.

2) Click to select the upgrade file.

3) Click **Upgrade** to start upgrading.



Configuring RS-485 Parameters

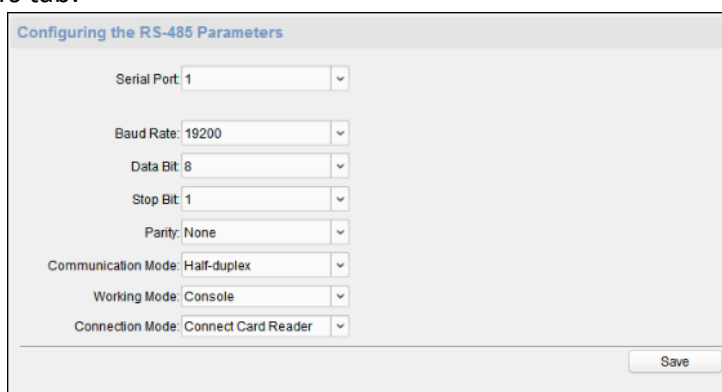
Purpose:

You can set the RS-485 parameters including the baud rate, data bit, stop bit, parity type, communication mode, work mode, and connection mode.

Note: The RS-485 Settings should be supported by the device.

Steps:

1. In the Remote Configuration page, click **System** -> **RS-485 Settings** to enter the Configuring the RS-485 Parameters tab.



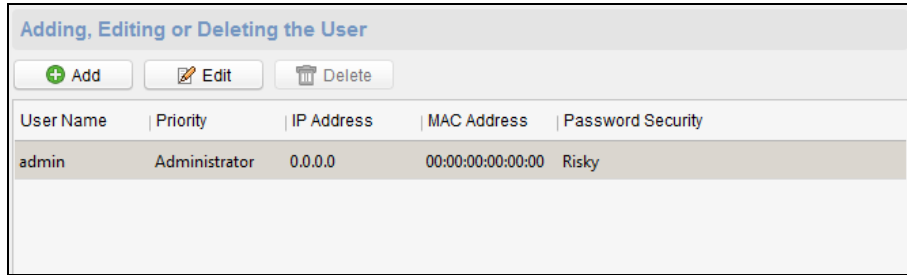
2. Select the serial No. of the port from the dropdown list to set the RS-485 parameters.
3. Set the baud rate, data bit, the stop bit, parity, flow control, communication mode, working mode, and the connection mode from the dropdown list.
4. Click **Save** to save the settings and the configured parameters will be applied to the device automatically.

Note: After changing the working mode, the device will be rebooted. A prompt will be popped up after changing the working mode.

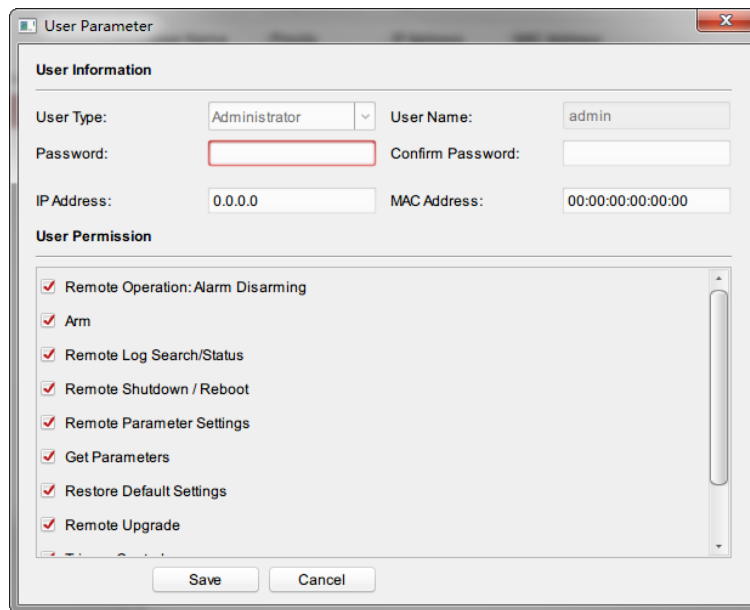
Managing User

Steps:

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



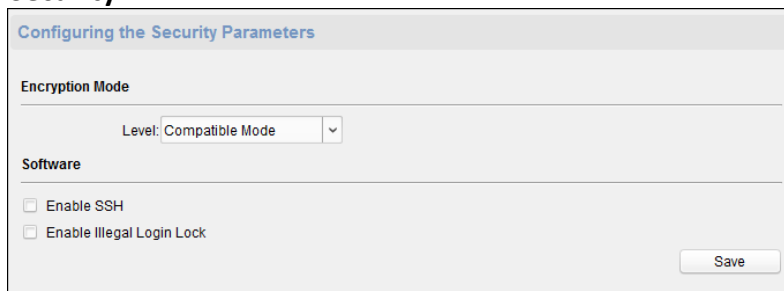
- Click **Add** to add the user (Do not support by the elevator controller.).
Or select a user in the user list and click **Edit** to edit the user. You are able to edit the user password, the IP address, the MAC address and the user permission. Cilck **OK** to confirm editing.



Setting Security

Steps:

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



- Select the encryption mode in the dropdown list.
You can select Compatible Mode or Encryption Mode.
- Click **Save** to save the settings.

Configuring Network Parameters

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

Configuring Upload Method

Purpose :

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

Steps:

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

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

Configuring Network Center

You can set the notify surveillance center, center's IP address, the port No., the Protocol (EHome), and the EHome account user name to transmit data via EHome protocol. For details about EHome

protocol's transmission, refer to *Network Center Settings* in *Chapter 7.3.4 Network Settings*. Click **Save** to save the settings or click

Configuring Advanced Network

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

Configuring Relay Parameters

Steps:

1. Click **Alarm** -> **Relay**.

You can view the relay parameters.

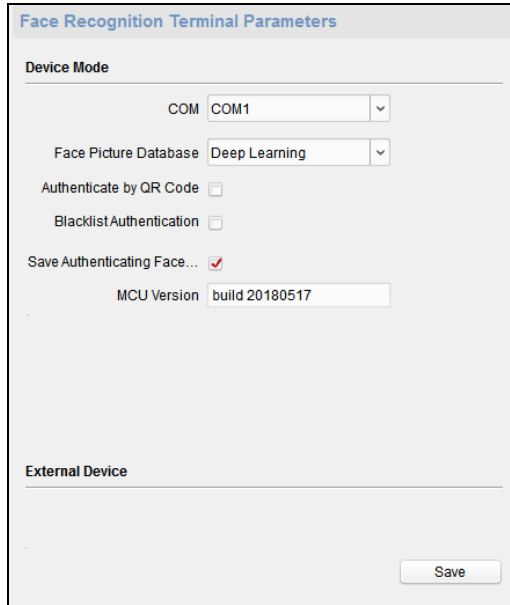
Relay	Name	Output Delay(s)	Zone Linkage	Settings
1		3	None	

2. Click the to pop up the Relay Parameters Settings window.
3. Set the relay name and the output delay.
4. Click **Save** to save the parameters.
Or click **Copy to...** to copy the relay information to other relays.

Configuring Face Recognition Terminal Parameters

Steps:

1. Click **Other** – **Face Recognition Terminal Parameters** to enter the Configuring Face Recognition Terminal Parameters page.



2. Set the parameters.

The parameters descriptions are as follows:

Parameter	Description
COM	Select a COM port for configuration. COM1 refers to RS-485 interface, and COM2 refers to RS-232 interface.
Face Picture Database	You can select Deep Learning as the face picture database.
Authenticate by QR Code	If enabling the function, the device camera can scan the QR code to authenticate. By default, the function is disabled.
Blacklist Authentication	If enable the function, the device will authenticate the person to with the persons in the blacklist. Note: For details about importing persons in blacklist, see <i>7.8.6 Person in Blacklist</i> .
Save Authenticating Face Picture	If enabling the function, the captured face picture when authenticating will be saved to the device.
MCU Version	View the device MCU version.

Configuring Face Picture Parameters

Click **Other – Face Picture Parameters** to enter the Configuring Face Picture Parameters page. You can set the face picture parameters when authenticating. Click **Save** to save the settings.

The parameters descriptions are as follows:

Parameter	Description
Min. Detection Width (Close to)	When the distance between the camera and the user is short, the parameter represents the minimum percentage of the facial width in the total width of the recognition area. The actual percentage should be larger than the

Parameter	Description
	configured value when face picture authentication. In this condition, the device will not detect other parameters.
Pitch Angle	The maximum pitch angle when face authentication. By default, the angle is 30°.
Yaw Angle	The maximum yaw angle when face authentication. By default, the angle is 45°.
Min. Detection Area (Width)	When the distance between the camera and the user is long, the parameter represents the minimum percentage of the facial width in the total width of the recognition area. The actual percentage should be larger than the configured value when face picture authentication. Other percentages, distances and angles in this table should also meet their conditions. Recommended Value: 14
Min. Detection Area (Height)	When the distance between the camera and the user is long, the parameter represents the minimum percentage of the facial height in the total height of the recognition area. The actual percentage should be larger than the configured value when face picture authentication. Other percentages, distances and angles in this table should also meet their conditions. Recommended Value: 12
Margin (Left)	The distance from the face left side to the left margin in the recognition area. The actual distance should be larger than the configured value when face picture authentication. Other percentages, distances, and angles should also meet their conditions.
Margin (Right)	The distance from the face right side to the right margin in the recognition area. The actual distance should be larger than the configured value when face picture authentication. Other percentages, distances, and angles should also meet their conditions.
Margin (Top)	The distance from the face top side to the top margin in the recognition area. The actual distance should be larger than the configured value when face picture authentication. Other percentages, distances, and angles should also meet their conditions.

Parameter	Description
Margin (Bottom)	The distance from the face bottom side to the bottom margin in the recognition area. The actual distance should be larger than the configured value when face picture authentication. Other percentages, distances, and angles should also meet their conditions.
Pupillary Distance	The minimum resolution between two pupils when face recognition. The actual resolution should be larger than the configured value. By default, the resolution is 40.
Score	Set the face picture's score when recognition. The device will score the captured picture according to the yaw angle, pitch angle, and pupillary distance. If the score is larger than the configured value, face recognition is failed.

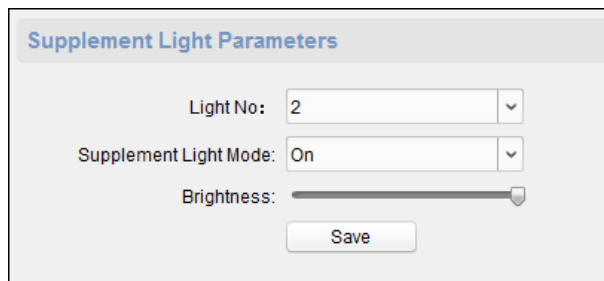
Configuring Supplement Light Parameters

Purpose:

You can turn on or off the supplement light. If the supplement light is in auto mode, you can also adjust the supplement light brightness.

Steps:

1. Click **Other – Supplement Light Parameters** to enter the Configuring Supplement Light Parameters page.



2. Select a supplement light No. from the drop-down list.
Note: Light 1 refers to white light and Light 2 refers to IR light.
3. Select a supplement light mode from the drop-down list.
4. (Optional) If the supplement light mode is **Auto**, you can set the supplement light brightness.
5. Click **Save** to save the settings.

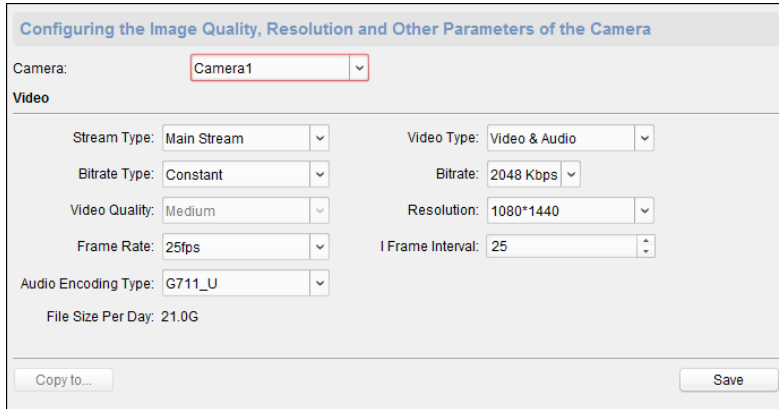
Configuring Video and Audio Parameters

Purpose:

You can set the device camera's image quality, resolution and other parameters.

Steps:

1. Click **Image – Video & Audio** to enter the settings page.

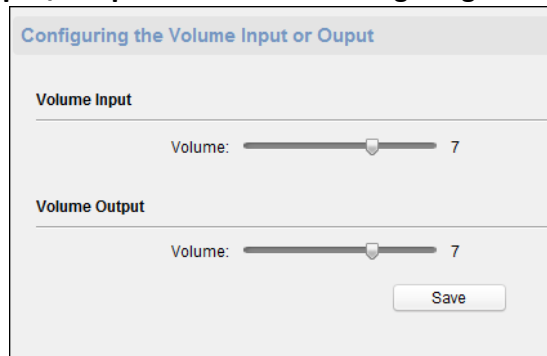


2. Set the device camera's parameters, including the stream type, the bitrate type, the video quality, the frame rate, the audio encoding type, the video type, the bitrate, the resolution, and the I frame interval.
3. Click **Save** to save the settings.

Configuring Volume Input or Output

Steps:

1. Click **Image – Volume Input/Output** to enter the Configuring the Volume Input or Output page.



2. Set the device input volume or output volume.
3. Click **Save** to save the parameters.

Operating Relay

1. Click **Operation -> Relay**.
You can view the relay status.
2. Check the relay checkbox
3. Click **Open** or **Close** to open/close the relay.
4. (Optional) Click **Refresh** to refresh the relay status.




Viewing Relay Status

Click **Status -> Relay** to view the relay status.

Relay Status	
Relay	Status
Relay1	Close

7.4 Organization Management

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

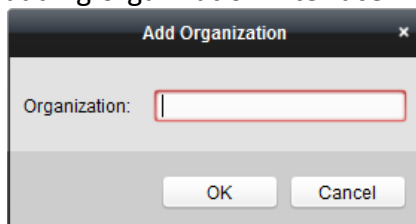
Click  tab to enter the Person and Card Management interface.

7.4.1 Adding Organization

Steps:

1. In the organization list on the left, you should add a top organization as the parent organization of all organizations.

Click **Add** button to pop up the adding organization interface.



The image shows a dialog box titled "Add Organization" with a close button (X) in the top right corner. Inside the dialog, there is a label "Organization:" followed by a text input field. At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

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

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

7.4.2 Modifying and Deleting Organization

You can select the added organization and click **Modify** to modify its name.

You can select an organization, and click **Delete** button to delete it.

Notes:

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

7.5 Person Management

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

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

7.5.1 Adding Person

Adding Person (Basic Information)

Steps:

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

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

Adding Person (Detailed Information)

Steps:

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

2. Input the detailed information of the person, including person's ID type, ID No., country, etc., according to actual needs.
 - **Linked Device:** You can bind the indoor station to the person.
 - Note:** If you select **Analog Indoor Station** in the Linked Device, the **Door Station** field will display and you are required to select the door station to communicate with the analog indoor station.
 - **Room No.:** You can input the room No. of the person.
3. Click **OK** to save the settings.

Adding Person (Permission)

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

Note: For setting the access control permission, refer to *Chapter 7.7 Permission Configuration*.

Steps:

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

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

list.

(Optional) In the Selected Permission(s) list, select the selected permission and click < to remove it. You can also click << to remove all the selected permissions.

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

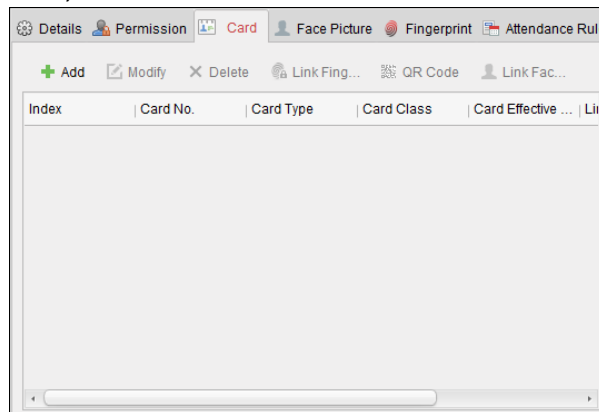
Adding Person (Card)

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

➤ Adding General Card

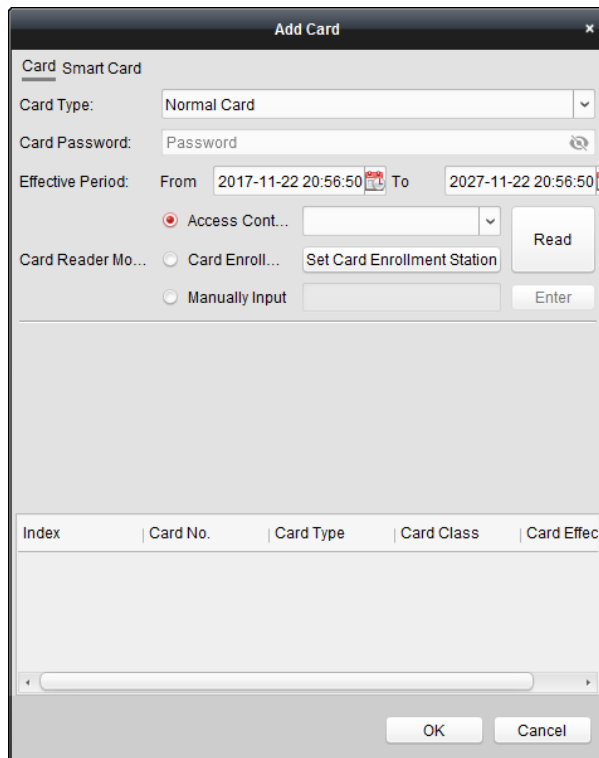
Steps:

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



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

3. Click **Card** to enter the Card tab.



4. Select the card type according to actual needs.


- **Normal Card**

- **Card for Disabled Person:** The door will remain open for the configured time period for the card holder.
- **Card in Blacklist:** The card swiping action will be uploaded and the door cannot be opened.
- **Patrol Card:** The card swiping action can be used for checking the working status of the inspection staff. The access permission of the inspection staff is configurable.
- **Duress Card:** The door can open by swiping the duress card when there is duress. At the same time, the client can report the duress event.
- **Super Card:** The card is valid for all the doors of the controller during the configured schedule.
- **Visitor Card:** The card is assigned for visitors. For the Visitor Card, you can set the **Max. Swipe Times**.

Note: The Max. Swipe Times should be between 0 and 255. When setting as 0, it means the card swiping is unlimited.

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

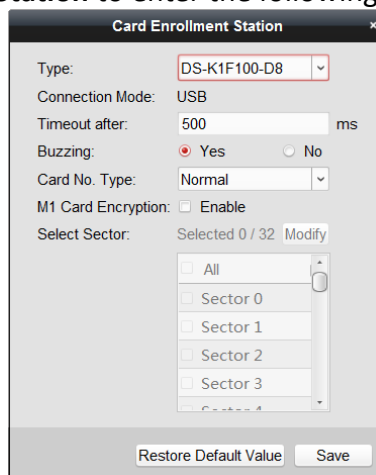
Note: The password will be required when the card holder swiping the card to get enter to or exit from the door if you enable the card reader authentication mode as **Card and Password**, **Password and Fingerprint**, and **Card, Password, and Fingerprint**.

6. Click  to set the effective time and expiry time of the card.

7. Select the Card Reader Mode for reading the card No.

- **Access Controller Reader:** Place the card on the reader of the Access Controller and click **Read** to get the card No.
- **Card Enrollment Station:** Place the card on the Card Enrollment Station and click **Read** to get the card No.

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



1) Select the Card Enrollment Station type.

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

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

If the card is M1 card, and if you need to enable the M1 Card Encryption function, you should check **Enable** checkbox of M1 Card Encryption and click **Modify** to select the sector.

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

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

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

8. Click **OK** and the card(s) will be issued to the person.

9. (Optional) You can select the added card and click **Modify** or **Delete** to edit or delete the card.

10. (Optional) You can generate and save the card QR code for QR code authentication.

1) Select an added card and click **QR Code** to generate the card QR code.

2) In the QR code pop-up window, click **Download** to save the QR code to the local PC.

You can print the QR code for authentication on the specified device.

Note: The device should support the QR code authentication function. For details about setting the QR code authentication function, see the specified device user manual.

11. (Optional) You can click **Link Fingerprint** to link the card with the person's fingerprint, so that the person can place the finger on the scanner instead of swiping card when passing the door.

12. (Optional) You can click **Link Face Picture** to link the card with the face picture, so that the person can pass the door by scanning the face via the device instead of swiping card when passing the door.

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

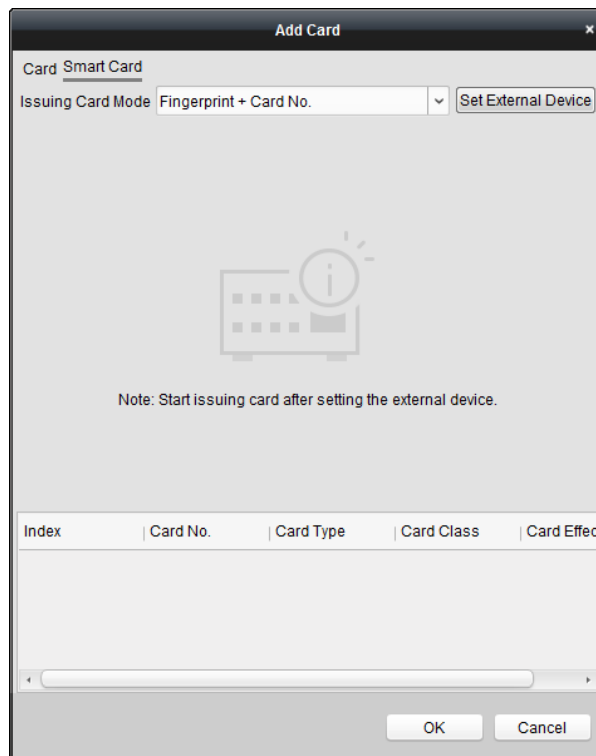
➤ **Adding Smart Card**

Purpose:

You can store fingerprints and ID card information in the smart card. When authenticating, after swiping the smart card on the device, you can scan your fingerprint or swipe your ID card on the device. The device will compare the fingerprint or ID card information in the smart card with the ones collected. If you use the smart card for authentication, there is no need to store the fingerprints or ID card information in the device in advance.

Steps:

1. In the Add Person page, set the person basic information.
2. Click **Card** to enter the card tab.
3. Click **Add** to pop up the Add Card dialog.
4. Click **Smart Card** to enter the Smart Card tab.



5. Select an issuing card mode from the dropdown list.
6. Set the external device.
 - 1) Click **Set External Device** to enter the Set External Device page.
 - 2) (Optional) Select the issuing card mode again.
 - 3) Set a card enrollment station.
 - 4) If you select “Fingerprint + Card No.” as the issuing mode, set the fingerprint recorder model.
 If you select “ID Card No. + Card No.” as the issuing mode, set the ID card reader model.
 If you select “Fingerprint + ID Card No. + Card No.” as the issuing mode, set the fingerprint recorder model and the ID card reader model.
 - 5) Click **OK** save the settings.
7. Select a card type for the smart card.
 - **Normal Card**
 - **Card for Disabled Person:** The door will remain open for the configured time period for the card holder.
 - **Card in Blacklist:** The card swiping action will be uploaded and the door cannot be opened.
 - **Patrol Card:** The card swiping action can be used for checking the working status of the inspection staff. The access permission of the inspection staff is configurable.
 - **Duress Card:** The door can be opened by swiping the duress card when there is duress. At the same time, the client can report the duress event.
 - **Super Card:** The card is valid for all the doors of the controller during the configured schedule.
 - **Visitor Card:** The card is assigned for visitors. For the Visitor Card, you can set the Max. Swipe Times.

Note: The Max. Swipe Times should be between 0 and 255. When setting as 0, it means the card swiping is unlimited.

- **Dismiss Card:** Swipe the card to dismiss alarm.

8. Set other parameters of the card.

- 1) Set the card password.
- 2) Set the card effective date.
- 3) Scan your fingerprint and swipe your ID card according to the prompt.
- 4) Swipe the smart card.

The added card information will display in the list below.

9. Click **OK** and the card(s) will be issued to the person.

10. (Optional) Select the added card and click **Modify** or **Delete** to edit or delete the card.

11. (Optional) Generate and save the card QR code for QR code authentication.

- 1) Select an added card and click **QR Code** to generate the card QR code.
- 2) In the QR code pop-up window, click **Download** to save the QR code to the local PC.

You can print the QR code for authentication on the specified device.

Note: The device should support the QR code authentication function. For details about setting the QR code authentication function, see the specified device user manual.

12. (Optional) Click **Link Fingerprint** to link the card with the person's fingerprint, so that the person can place the finger on the scanner instead of swiping card when passing the door.

13. (Optional) Click **Link Face Picture** to link the card with the face picture, so that the person can pass the door by scanning the face via the device instead of swiping card when passing the door.

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

Adding Person (Face Picture)

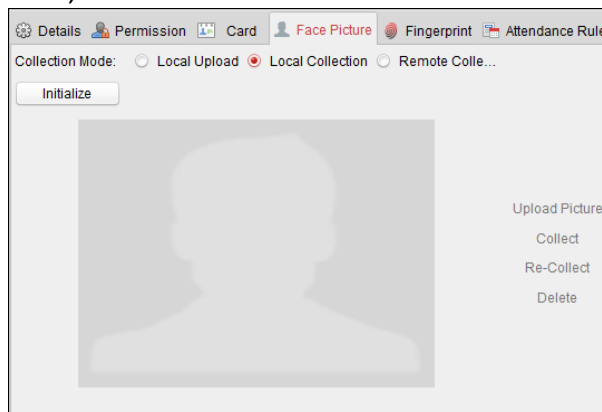
You can collect the face picture in two ways: Local Collection and Remote Collection.

- **Local Upload:** Upload local the face pictures from the local PC.
- **Local Collection:** Collect the face picture via face picture scanner.
- **Remote Collection:** Collect the face picture via the access control terminal.

Note: The access control terminal should support face recognition function.

Steps:

1. In the Add Person interface, click **Face Picture** tab.



2. To upload the face picture from the local PC:

- 1) Select **Local Upload**.

- 2) Click **Upload Picture** and select a face picture from the local PC.
Note: The uploaded picture should be in JPG format and the size should be less than 200K.
- 3) (Optional) By default, the uploaded face picture should be verified by the device.
You can select a device from the drop-down list to verify the uploaded face picture. Only after the face picture is verified, the face picture is adding completely.
3. To get the face picture via face picture scanner:
 - 1) Select **Local Collection**.
 - 2) Connect the face picture scanner to the PC.
 - 3) Select a device type.
Note: Currently, the face picture scanner of DS2CS5432B-S is supported.
 - 4) (Optional) You can click **Initialize** to initialize the face picture scanner.
4. To get the face picture via access control terminal:
 - 1) Select **Remote Collection**.
 - 2) Click **Select Device** to select the access control terminal which supports face recognition function.
5. Click **Collect** to capture the face picture.
You can click **Re-Collect** the captured picture again.
You can click **Delete** to delete the captured picture.
6. Click **OK** to save the settings.

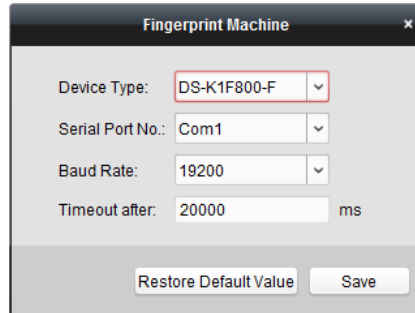
Adding Person (Fingerprint)

Steps:

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



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



- 1) Select the device type.

Currently, the supported fingerprint machine types include DS-K1F800-F, DS-K1F810-F, DS-K1F820-F, and DS-K1F181-F.

- 2) For fingerprint machine type DS-K1F800-F, you can set the serial port number, baud rate, and overtime parameters of the fingerprint machine.
- 3) Click **Save** button to save the settings.

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

Notes:

- The serial port number should correspond to the serial port number of PC. You can check the serial port number in Device Manager in your PC.
- The baud rate should be set according to the external fingerprint card reader. The default value is 19200.
- **Timeout after** field refers to the valid fingerprint collecting time. If the user does not input a fingerprint or inputs a fingerprint unsuccessfully, the device will indicate that the fingerprint collecting is over.

4. Click **Start** button, click to select the fingerprint to start collecting.
5. Lift and rest the corresponding fingerprint on the fingerprint scanner twice to collect the fingerprint to the client.

6. (Optional) You can also click **Remote Collection** to collect fingerprint from the device.

Note: The function should be supported by the device.

7. (Optional) You can select the registered fingerprint and click **Delete** to delete it.

You can click **Clear** to clear all fingerprints.

8. Click **OK** to save the fingerprints.

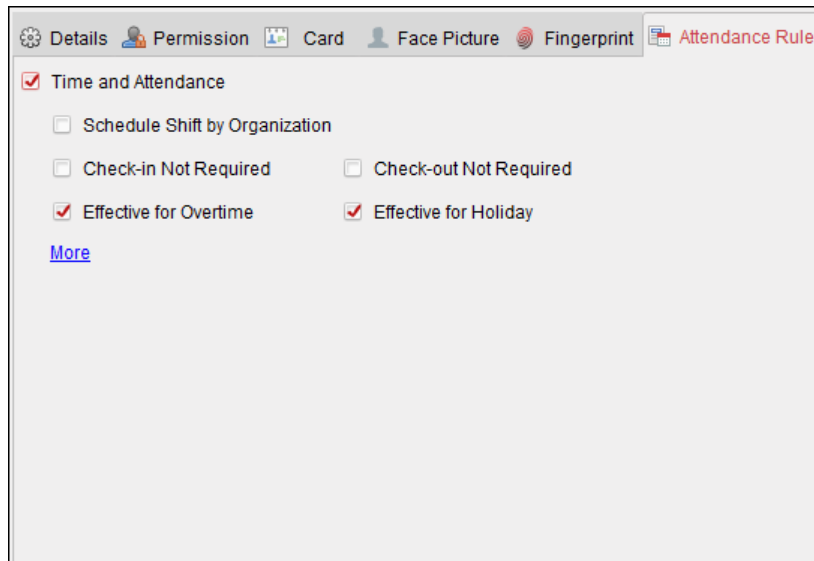
Adding Person (Attendance Rule)

You can set the attendance rule for the person.

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

Steps:

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



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

Importing Person Information

Purpose:

You can import the information of multiple persons (including identity information, fingerprint data, and fingerprint linked card number) to the client software in a batch by importing an Excel file from the local PC.

Steps:

1. Click **Import Person** and click **Person Information** as the content to import.
2. In the pop-up window, click **Download Template for Importing Person** to download the template first.
3. Input the person information in the downloaded template.
Note: If the person has multiple cards, separate the card No. with semicolon.
4. Select the Excel file with the person information.
5. Click **OK** to start importing.
Note: If the person No. already exists in the client software's database, it will replace the person information automatically after importing.

Importing Person Pictures

Purpose:

After adding the persons, you can import multiple person pictures in a batch by importing a ZIP file with pictures to the client software.

Steps:

1. Name the person picture after the person name.
Note: The picture should be in JPG format and smaller than 200 KB.

2. Compress the file which contains the person pictures to ZIP format.
3. In the Person and Card module, click **Import Person** and click **Person Pictures** as the content to import.
4. In the pop-up window, select the ZIP file.
5. Click **OK** to start importing.

Note: By default, the imported person picture is linked with the person's first card.

Exporting Person Information

You can export the added persons's information to the local PC in Excel format.

Steps:

1. After adding the person, you can click **Export Person** button to pop up the Export Person window.
2. Select the path of saving the exported Excel file.
3. Select the items of person information to export.
4. Click **OK** to start exporting.

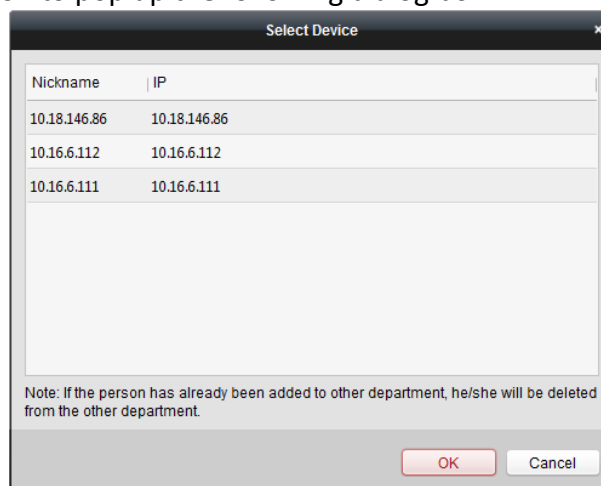
Getting Person Information from Access Control Device

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

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

Steps:

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



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

You can also double click the device name to start getting the person information.

Notes:



- The person information, including person details, person's fingerprint information (if


configured), and the linked card (if configured), will be imported to the selected organization.

- If the person name stored in the device is empty, the person name will be filled with the issued card No. after importing to the client.
- The gender of the persons will be **Male** by default.
- Up to 10000 persons can be imported.

7.5.2 Managing Person

Modifying and Deleting Person

To modify the person information and attendance rule, click  or  in the Operation column, or select the person and click **Modify** to open the editing person dialog.

You can click  to view the person's card swiping records.

To delete the person, select a person and click **Delete** to delete it.

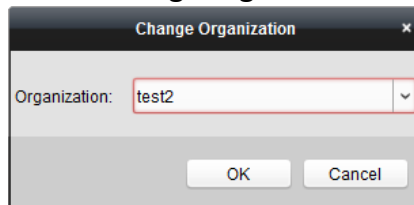
Note: If a card is issued to the current person, the linkage will be invalid after the person is deleted.

Changing Person to Other Organization

You can move the person to another organization if needed.

Steps:

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



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

Searching Person

You can input the keyword of card No. or person name in the search field, and click **Search** to search the person.

You can input the card No. by clicking **Read** to get the card No. via the connected card enrollment station.

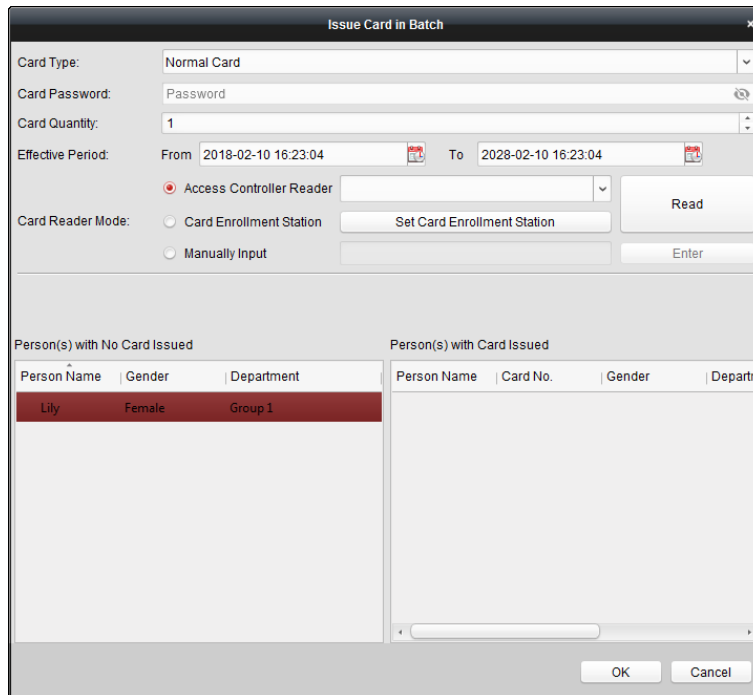
You can click **Set Card Enrollment Station** in the dropdown list to set the parameters.


7.5.3 Issuing Card in Batch

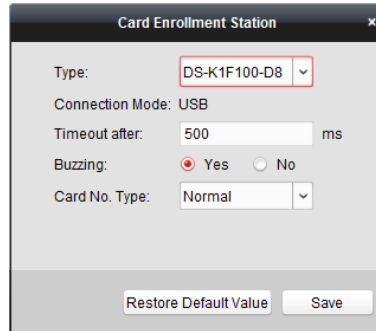
You can issue multiple cards for the person with no card issued in batch.

Steps:

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



2. Select the card type according to actual needs.
Note: For details about the card type, refer to *Adding Person*.
3. Input the password of the card itself in the Card Password field. The card password should contain 4 to 8 digits.
Note: The password will be required when the card holder swiping the card to get enter to or exit from the door if you enable the card reader authentication mode as **Card and Password**, **Password and Fingerprint**, and **Card, Password, and Fingerprint**.
4. Input the card quantity issued for each person.
 For example, if the Card Quantity is 3, you can read or enter three card No. for each person.
5. Click  to set the effective time and expiry time of the card.
6. In the Person(s) with No Card Issued list on the left, select the person to issue card.
Note: You can click on the Person Name, Gender, and Department column to sort the persons according to actual needs.
7. Select the Card Reader Mode for reading the card No.
 - **Access Controller Reader:** Place the card on the reader of the Access Controller and click **Read** to get the card No.
 - **Card Enrollment Station:** Place the card on the Card Enrollment Station and click **Read** to get the card No.
Note: The Card Enrollment Station should connect with the PC running the client. You can click **Set Card Enrollment Station** to enter the following dialog.



- 1) Select the Card Enrollment Station type.

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

- 2) Set the parameters about the connected card enrollment station.

If the card is M1 card, and if you need to enable the M1 Card Encryption function, you should check **Enable** checkbox of M1 Card Encryption and click **Modify** to select the sector.

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

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

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

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

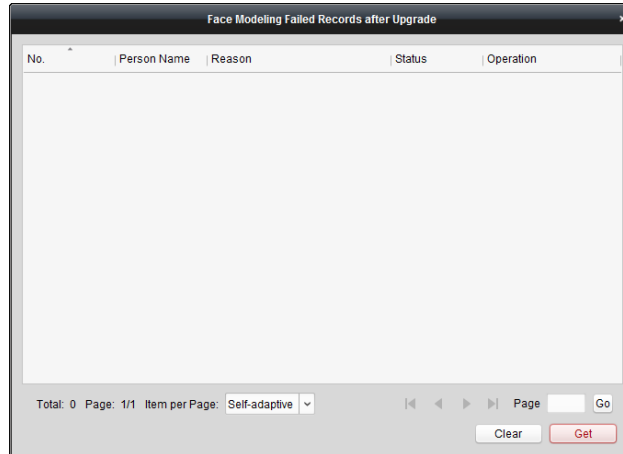
7.5.4 Detecting Face Modeling Failed Records

Purpose:

When the device is upgrading via the client software, the existing face pictures in the system will be re-modelled. Some face pictures' format will not be available because of the stricter face picture algorithm and re-modeling will be failed. This function can help to search the failed face modeling records and re-upload the face pictures.

Steps:

1. In the **Access Control** module, click **Person and Card** to enter the Person and Card page.
2. Click **Detect after Upgrade** at the upper right corner of the page to enter the Face modeling Failed Records after Upgrade window.




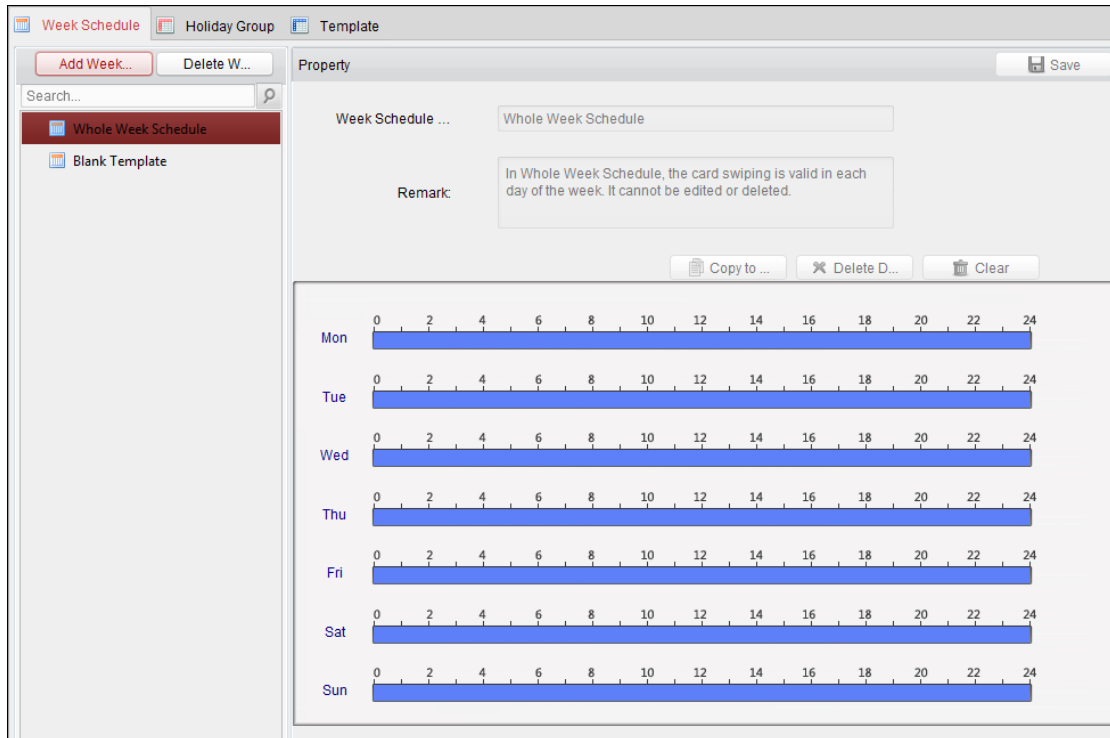
3. Click **Get** and select a device.
The failed records will be displayed in the list.
4. Click **Handle** and you will enter the Add Person page. You can re-upload the person's face picture.
The handled records will be displayed as Handled in the Status column.
5. (Optional) Click **Clear** to clear all failed records in the system.
Note: After clearing all records, you cannot get the failed records of the device.

7.6 Schedule and Template

Purpose:

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

Click  to enter the schedule and template interface.



You can manage the schedule of access control permission including Week Schedule, Holiday Schedule, and Template. For permission settings, please refer to *Chapter 7.7 Permission Configuration*.

7.6.1 Week Schedule

Click **Week Schedule** tab to enter the Week Schedule Management interface.

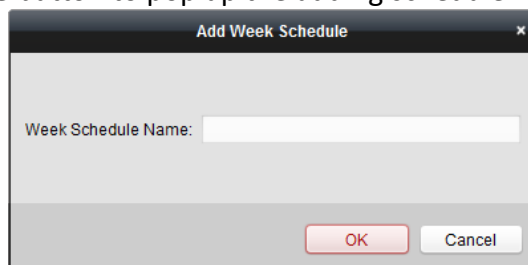
The client defines two kinds of week plan by default: **Whole Week Schedule** and **Blank Schedule**, which cannot be deleted and edited.

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

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

Steps:



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



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

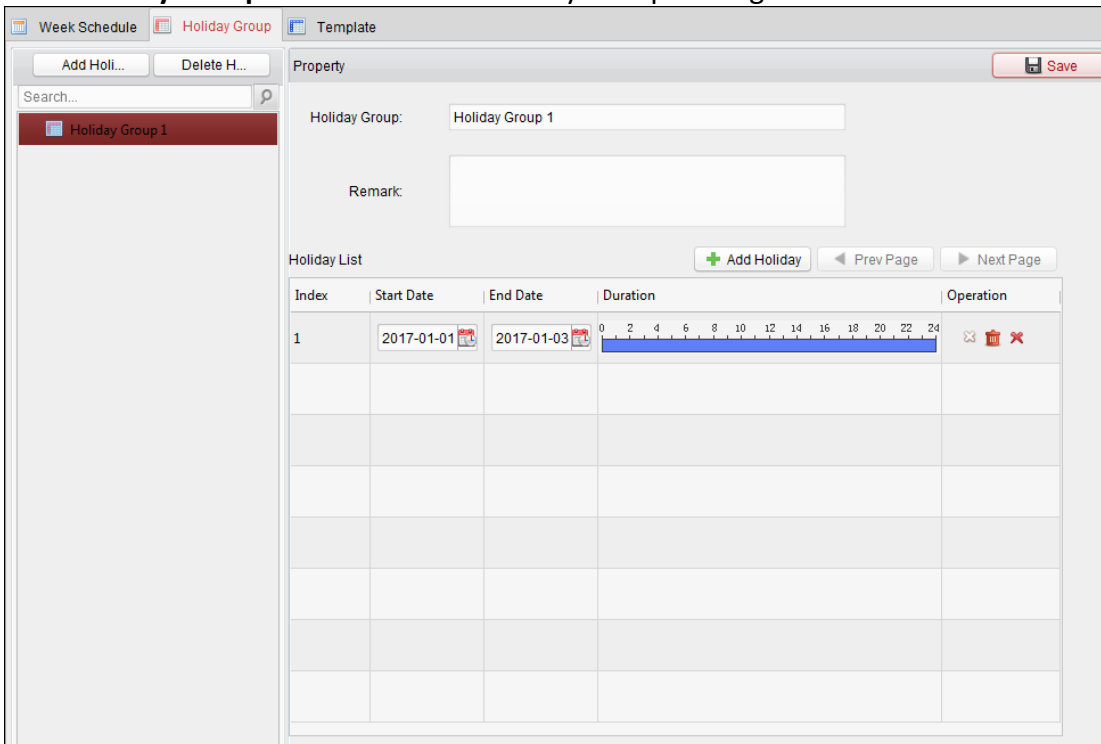
period of time, the configured permission is activated.

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

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

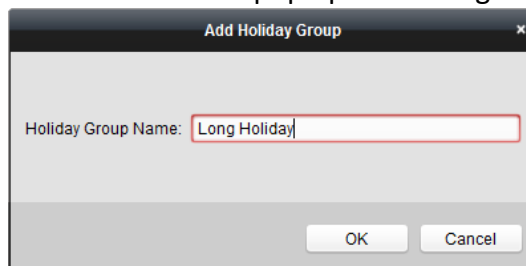
7.6.2 Holiday Group

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



Steps:

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

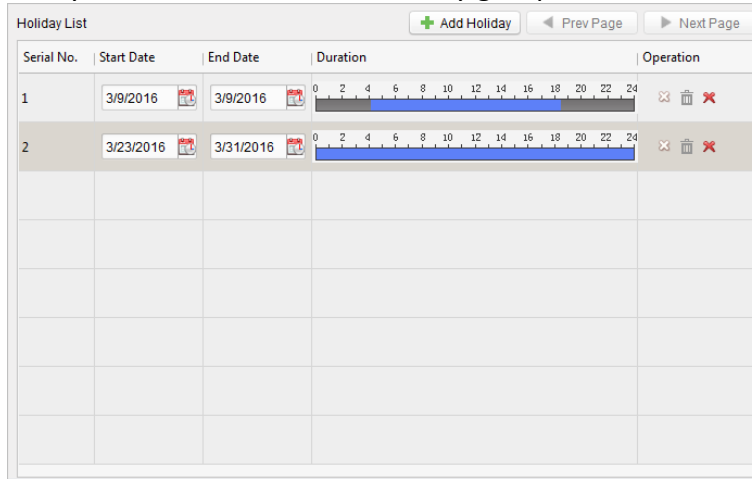


2. Input the name of holiday group in the text filed and click **OK** button to add the holiday group.
3. Select the added holiday group and you can edit the holiday group name and input the remark

information.






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

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



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

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

- When the cursor turns to , you can move the selected time bar you just edited. You can also edit the displayed time point to set the accurate time period.
- When the cursor turns to , you can lengthen or shorten the selected time bar.
- Optionally, you can select the schedule time bar, and then click  to delete the selected time bar, or click  to delete all the time bars of the holiday, or click  to delete the holiday directly.

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

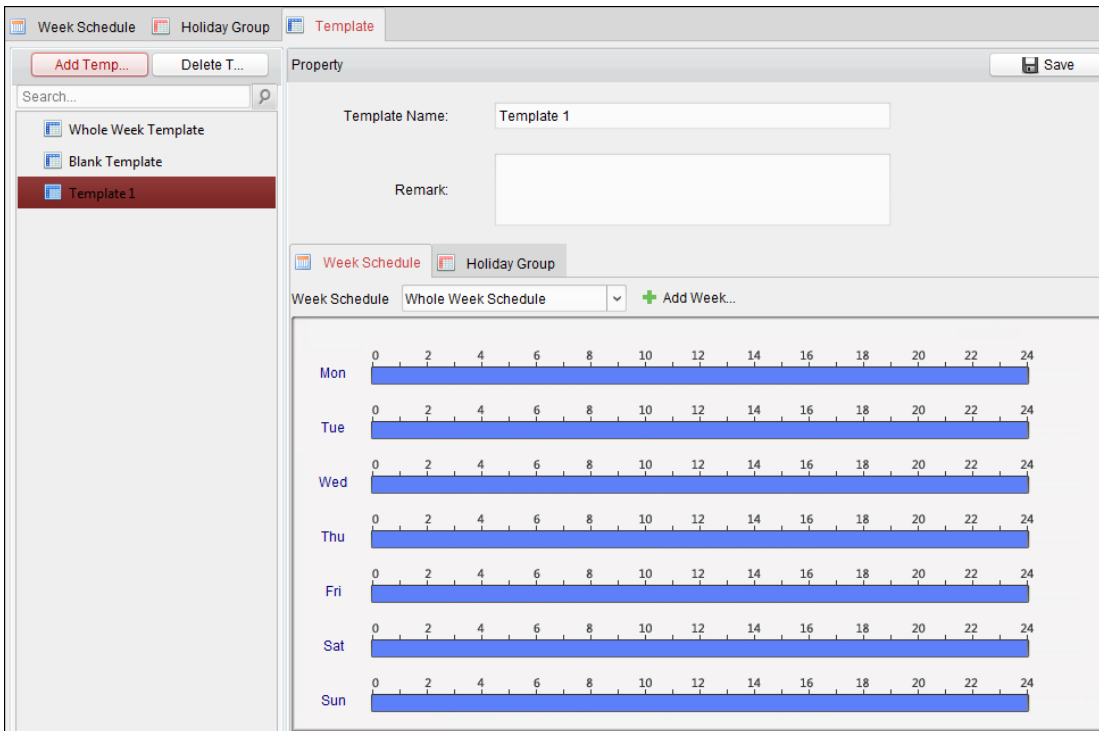
Note: The holidays cannot be overlapped with each other.

7.6.3 Template

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

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

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



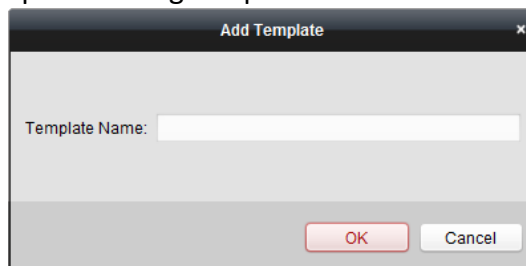
There are two pre-defined templates by default: **Whole Week Template** and **Blank Template**, which cannot be deleted and edited.

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

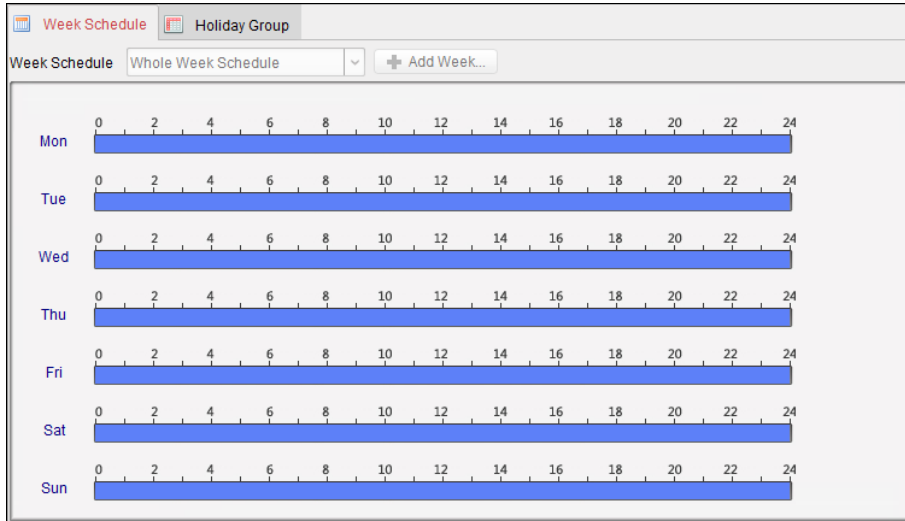
You can define custom templates on your demand.

Steps:

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

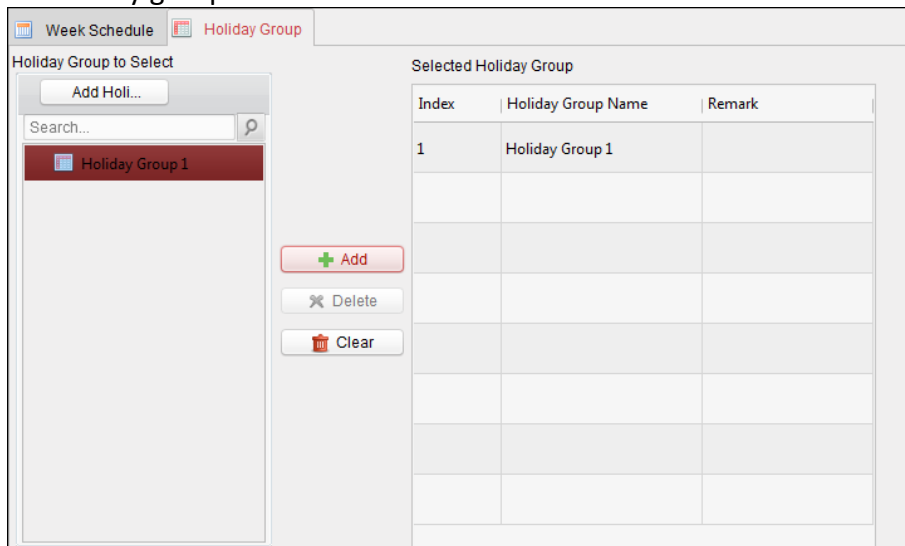


2. Input the template name in the text field and click **OK** button to add the template.
3. Select the added template and you can edit its property on the right. You can edit the template name and input the remark information.
4. Select a week schedule to apply to the schedule.
Click **Week Schedule** tab and select a schedule in the dropdown list.
You can also click **Add Week Schedule** to add a new week schedule. For details, refer to *Chapter 7.6.1 Week Schedule*.



5. Select holiday groups to apply to the schedule.

Note: Up to 4 holiday groups can be added.




Click to select a holiday group in the list and click **Add** to add it to the template. You can also click **Add Holiday Group** to add a new one. For details, refer to *Chapter 7.6.2 Holiday Group*. You can click to select an added holiday group in the right-side list and click **Delete** to delete it. You can click **Clear** to delete all the added holiday groups.

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

7.7 Permission Configuration

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

Click  icon to enter the Access Control Permission interface.

Permission Na...	Template	Person	Door	Details	Status
Permission 1	Whole Week T...	Wendy	Floor1_10.17....	Details	Not Applied

7.7.1 Adding Permission

Purpose:

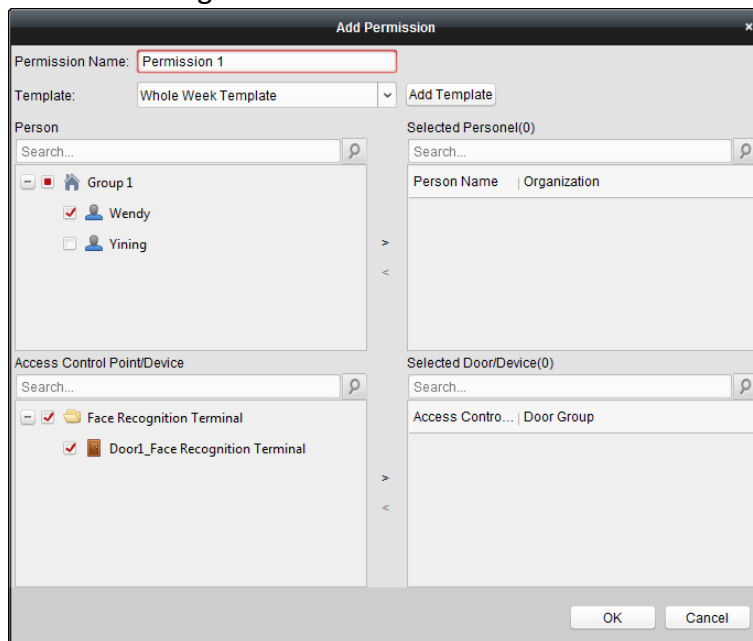
You can assign permission for persons to enter/exist the access control points (doors) in this section.

Notes:

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

Steps:

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



2. In the Permission Name field, input the name for the permission as desired.
3. Click on the dropdown menu to select a template for the permission.

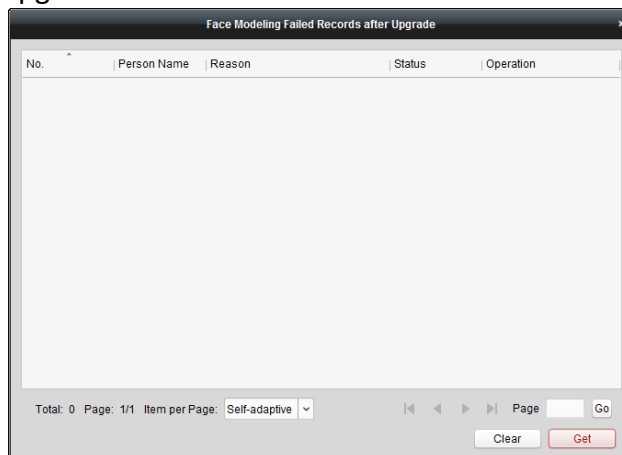
Note: You should configure the template before permission settings. You can click **Add Template** button to add the template. Refer to *Chapter 7.5.4 Detecting Face Modeling Failed Records*

Purpose:

When the device is upgrading via the client software, the existing face pictures in the system will be re-modelled. Some face pictures' format will not be available because of the stricter face picture algorithm and re-modeling will be failed. This function can help to search the failed face modeling records and re-upload the face pictures.

Steps:

6. In the **Access Control** module, click **Person and Card** to enter the Person and Card page.
7. Click **Detect after Upgrade** at the upper right corner of the page to enter the Face modeling Failed Records after Upgrade window.



8. Click **Get** and select a device.
The failed records will be displayed in the list.
9. Click **Handle** and you will enter the Add Person page. You can re-upload the person's face picture.
The handled records will be displayed as Handled in the Status column.
10. (Optional) Click **Clear** to clear all failed records in the system.
Note: After clearing all records, you cannot get the failed records of the device. Schedule and Template for details.
4. In the Person list, all the added persons display.
Check the checkbox(es) to select person(s) and click > to add to the Selected Person list.
(Optional) You can select the person in Selected Person list and click < to cancel the selection.
5. In the Access Control Point/Device list, all the added access control points (doors) and door stations will display.
Check the checkbox(es) to select door(s) or door station(s) and click > to add to the selected list.
(Optional) You can select the door or door station in the selected list and click < to cancel the selection.
6. Click **OK** button to complete the permission adding. The selected person will have the permission to enter/exit the selected door/door station with their linked card(s) or fingerprints.
7. (Optional) after adding the permission, you can click **Details** to modify it. Or you can select the permission and click **Modify** to modify.
You can select the added permission in the list and click **Delete** to delete it.

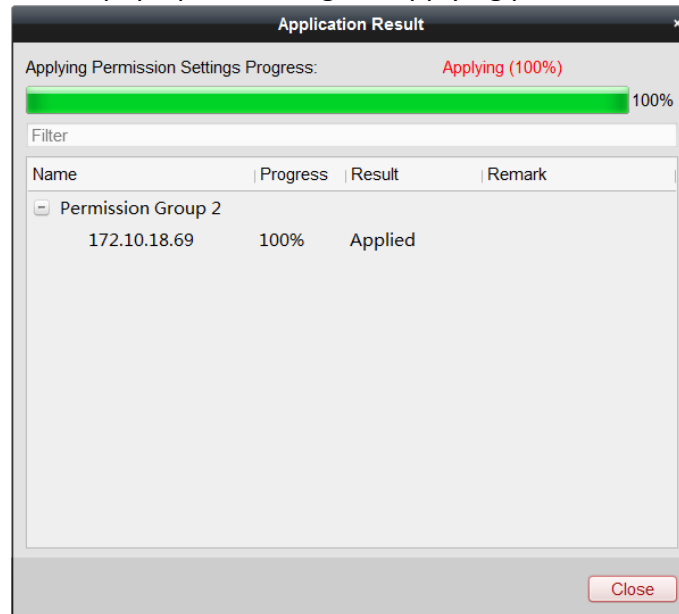
7.7.2 Applying Permission

Purpose:

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

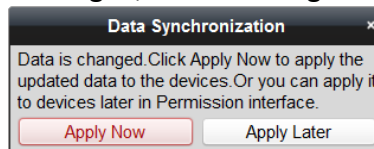
Steps:

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



Notes:

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



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


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

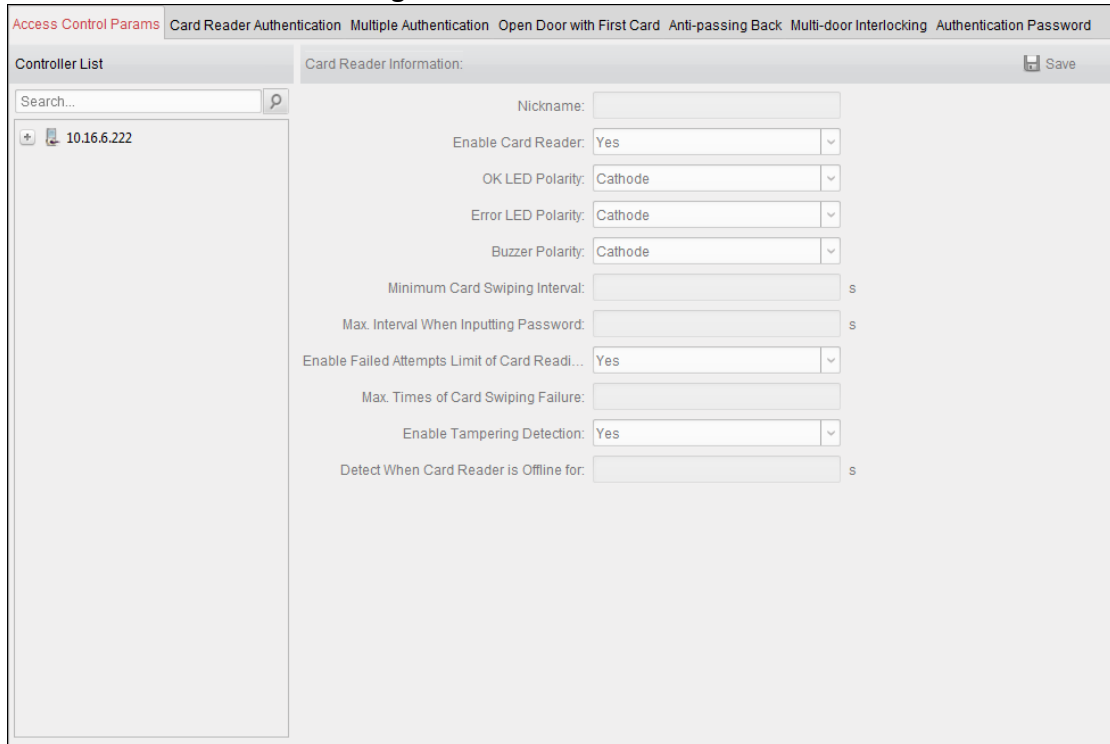
7.8 Advanced Functions

Purpose:

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

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

Click  icon to enter the following interface.



7.8.1 Access Control Parameters


Purpose:

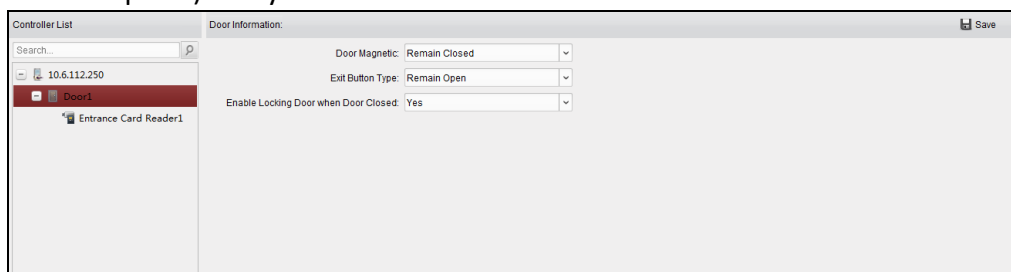
After adding the access control device, you can configure its access control point (door)'s parameters, and its card readers' parameters.

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

Door Parameters

Steps:

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



2. You can edit the following parameters:
 - **Door Magnetic:** The Door Magnetic is in the status of **Remain Closed** (excluding special conditions).
 - **Exit Button Type:** The Exit Button Type is in the status of **Remain Open** (excluding special

conditions).

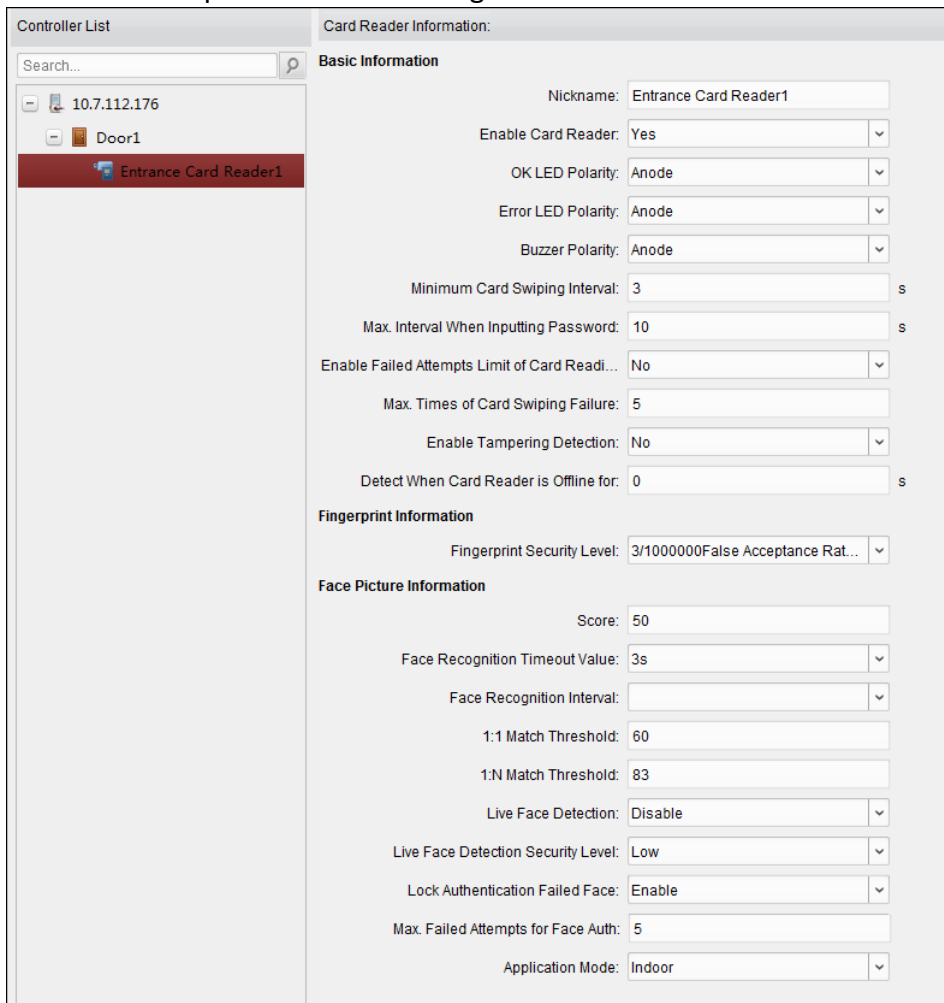
- **Enable Locking Door when Door Closed:** The door can be locked once it is closed even if the Door Locked Time is not reached.

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

Card Reader Parameters

Steps:

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



The screenshot displays the configuration interface for a card reader. On the left, the 'Controller List' shows a search bar and a tree view where 'Door1' is expanded to reveal 'Entrance Card Reader1'. The main area is titled 'Card Reader Information' and is divided into sections: 'Basic Information' and 'Face Picture Information'. The 'Basic Information' section includes fields for Nickname (Entrance Card Reader1), Enable Card Reader (Yes), OK LED Polarity (Anode), Error LED Polarity (Anode), Buzzer Polarity (Anode), Minimum Card Swiping Interval (3 s), Max. Interval When Inputting Password (10 s), Enable Failed Attempts Limit of Card Reading (No), Max. Times of Card Swiping Failure (5), Enable Tampering Detection (No), and Detect When Card Reader is Offline for (0 s). The 'Face Picture Information' section includes Fingerprint Security Level (3/1000000False Acceptance Rat...), Score (50), Face Recognition Timeout Value (3s), Face Recognition Interval, 1:1 Match Threshold (60), 1:N Match Threshold (83), Live Face Detection (Disable), Live Face Detection Security Level (Low), Lock Authentication Failed Face (Enable), Max. Failed Attempts for Face Auth (5), and Application Mode (Indoor).

2. You can edit the following parameters:

- **Nickname:** Edit the card reader name as desired.
- **Enable Card Reader:** Select **Yes** to enable the card reader.
- **OK LED Polarity:** Select the OK LED Polarity of the card reader mainboard.
- **Error LED Polarity:** Select the Error LED Polarity of the card reader mainboard.
- **Buzzer Polarity:** Select the Buzzer LED Polarity of the card reader mainboard.
- **Minimum Card Swiping Interval:** If the interval between card swiping of the same card is less than the set value, the card swiping is invalid. You can set it as 0 to 255.
- **Max. Interval When Inputting Password:** When you inputting the password on the card

reader, if the interval between pressing two digits is larger than the set value, the digits you pressed before will be cleared automatically.

- **Enable Failed Attempts Limit of Card Reading:** Enable to report alarm when the card reading attempts reach the set value.
- **Max. Times of Card Swiping Failure:** Set the max. failure attempts of reading card.
- **Enable Tampering Detection:** Enable the anti-tamper detection for the card reader.
- **Detect When Card Reader is Offline for:** When the access control device cannot connect with the card reader for longer than the set time, the card reader will turn offline automatically.
- **Fingerprint Security Level:** Select the fingerprint recognition level from the drop-down list.
- **Score:** The device will score the captured picture according to the yaw angle, pitch angle, and pupillary distance. If the score is less than the configured value, face recognition is failed.
- **Face Recognition Timeout Value:** If the recognition time is more than the configured time, the device will remind you.
- **Face Recognition Interval:** The time interval between two continuous face recognitions when authenticating.
- **1:1 Match Threshold:** Set the matching security level when authenticating via 1:1 matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate when authentication. By default, the value is 60.
- **1:N Match Threshold:** Set the matching security level when authenticating via 1:N matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate when authentication. By default, the value is 83.
- **Live Face Detection:** Enable or disable the live face detection function. If enabling the function, the device can recognize whether the person is a live one or not.
- **Live Face Detection Security Level:** After enabling Live Face Detection function, you can set the matching security level when performing live face authentication.
- **Lock Authentication Failed Face:** After enabling the Live Face Detection function, the system will lock the user's face for 5 minutes if the live face detection is failed for more than the configured attempts. The same user cannot authenticate via the fake face within 5 minutes. Within the 5 minutes, the user can authenticate via the real face twice continuously to unlock.
- **Max. Failed Attempts for Face Auth:** Set the maximum live face detection failed attempts. The system will lock the user's face for 5 minutes if the live face detection is failed for more than the configured attempts. The same user cannot authenticate via the fake face within 5 minutes. Within the 5 minutes, the user can authenticate via the real face twice continuously to unlock.
- **Application Mode:** You can select either others or indoor according to actual environment.

7.8.2 Card Reader Authentication

Purpose:




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

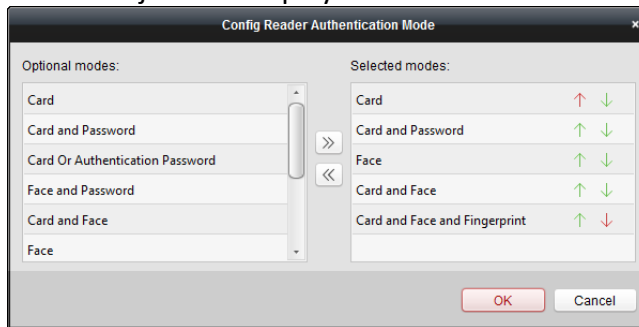
Steps:

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

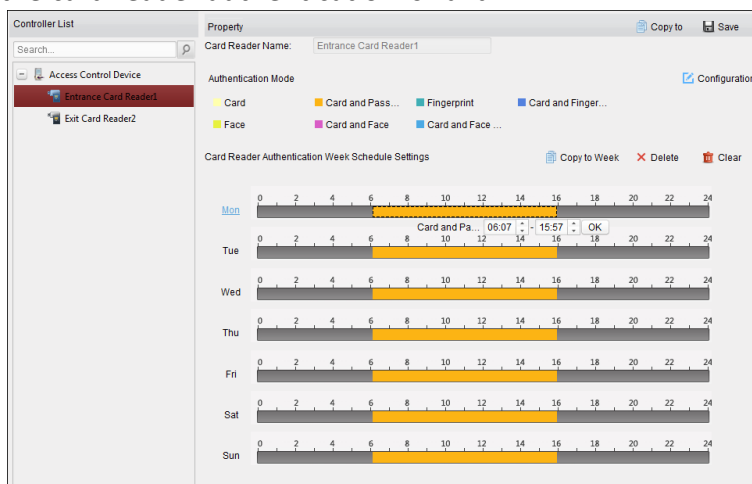
Notes:

- The available authentication modes depend on the device type.
- Password refers to the card password set when issuing the card to the person in *Chapter 7.5 Person Management*.

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



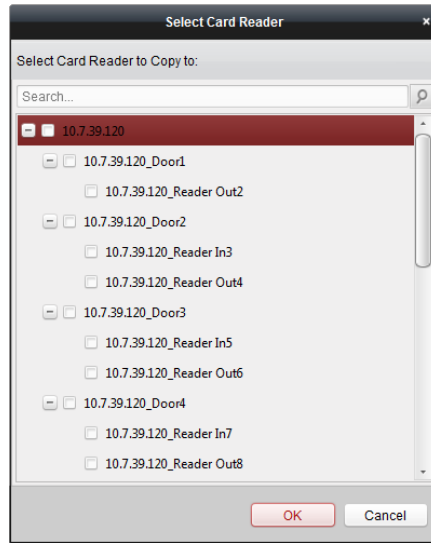
- 2) Click **OK** to confirm the selection.
3. After selecting the modes, the selected modes will display as icons. Click the icon to select a card reader authentication mode.
4. Click and drag your mouse on a day to draw a color bar on the schedule, which means in that period of time, the card reader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



5. Repeat the above step to set other time periods.
Or you can select a configured day and click **Copy to Week** button to copy the same settings to the whole week.

(Optional) You can click **Delete** button to delete the selected time period or click **Clear** button to delete all the configured time periods.

- (Optional) Click **Copy to** button to copy the settings to other card readers.



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

7.8.3 Multiple Authentication

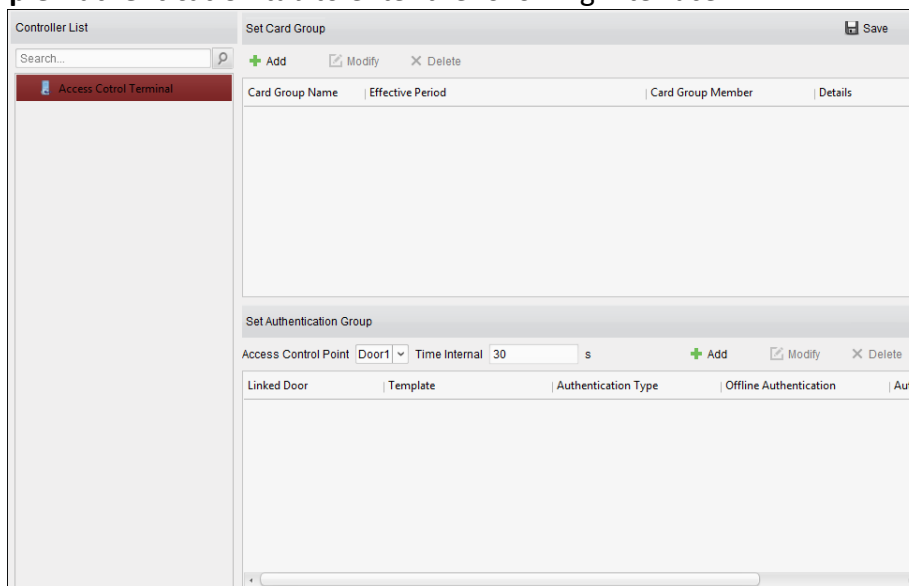
Purpose:

You can manage the cards by group and set the authentication for multiple cards for one access control point (door).

Note: Please set the card permission and apply the permission setting to the access control device first. For details, refer to *Chapter 7.7 Permission Configuration*.

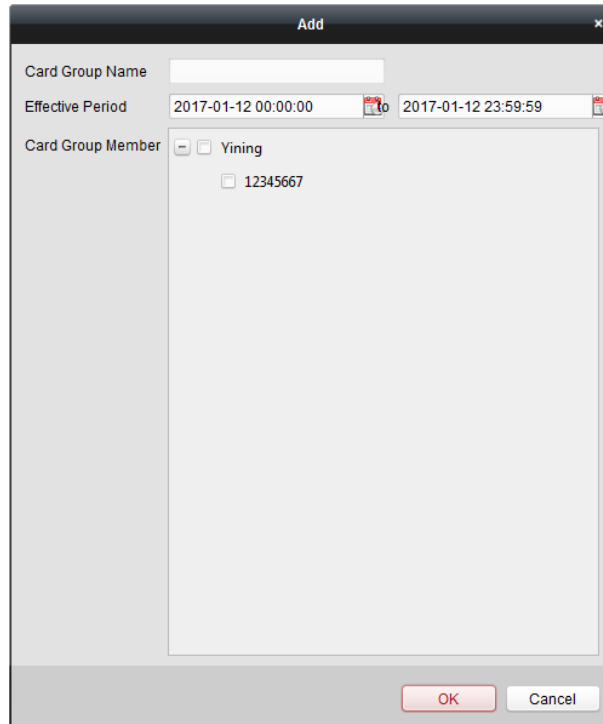
Steps:


- Click **Multiple Authentication** tab to enter the following interface.

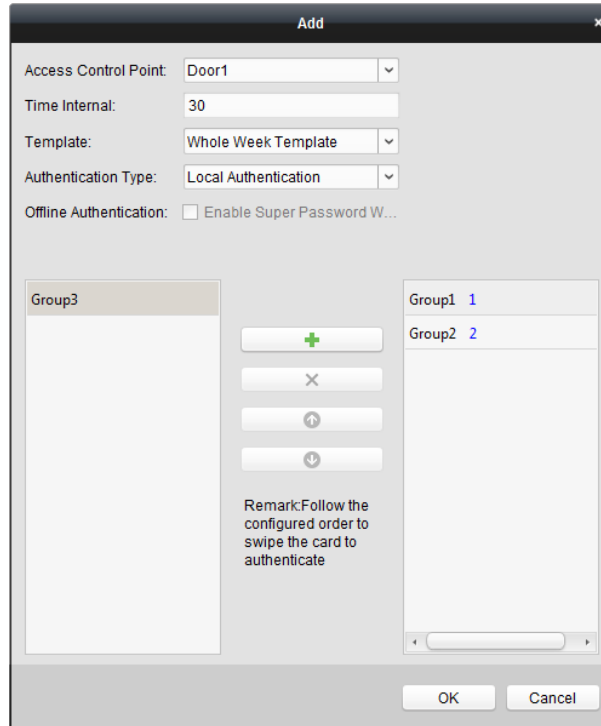


- Select access control device from the list on the left.

3. In the Set Card Group panel on the right, click **Add** button to pop up the following dialog:



- 1) In the Card Group Name field, input the name for the group as desired.
 - 2) Click  to set the effective time and expiry time of the card group.
 - 3) Check the checkbox(es) to select the card(s) to add the card group.
 - 4) Click **OK** to save the card group.
4. In the Set Authentication Group panel, select the access control point (door) of the device for multiple authentications.
 5. Input the time interval for card swiping.
 6. Click **Add** to pop up the following dialog.



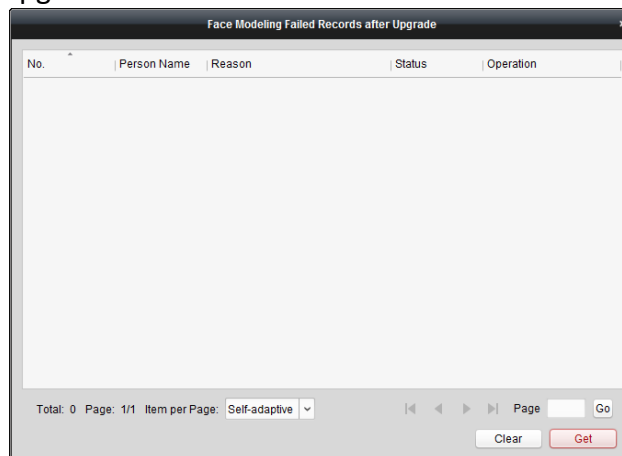
1) Select the template of the authentication group from the dropdown list. For details about setting the template, refer to *Chapter 7.5.4 Detecting Face Modeling Failed Records*

Purpose:

When the device is upgrading via the client software, the existing face pictures in the system will be re-modelled. Some face pictures' format will not be available because of the stricter face picture algorithm and re-modeling will be failed. This function can help to search the failed face modeling records and re-upload the face pictures.

Steps:

11. In the **Access Control** module, click **Person and Card** to enter the Person and Card page.
12. Click **Detect after Upgrade** at the upper right corner of the page to enter the Face modeling Failed Records after Upgrade window.



13. Click **Get** and select a device.
The failed records will be displayed in the list.
14. Click **Handle** and you will enter the Add Person page. You can re-upload the person's face

picture.

The handled records will be displayed as Handled in the Status column.

15. (Optional) Click **Clear** to clear all failed records in the system.

Note: After clearing all records, you cannot get the failed records of the device.


- 2) Schedule and Template.


- 3) Select the authentication type of the authentication group from the dropdown list.

- **Local Authentication:** Authentication by the access control device.
- **Local Authentication and Remotely Open Door:** Authentication by the access control device and by the client.

For Local Authentication and Remotely Open Door type, you can check the checkbox to enable the super password authentication when the access control device is disconnected with the client.

- **Local Authentication and Super Password:** Authentication by the access control device and by the super password.

- 4) In the list on the left, the added card group will display. You can click the card group and click  to add the group to the authentication group.

You can click the added card group and click  to remove it from the authentication group.

You can also click  or  to set the card swiping order.

- 5) Input the **Card Swiping Times** for the selected card group.

Notes:

- The Card Swiping Times should be larger than 0 and smaller than the added card quantity in the card group.
- The upper limit of Card Swiping Times is 16.

- 6) Click **OK** to save the settings.

7. Click **Save** to save and take effect of the new settings.

Notes:

- For each access control point (door), up to 20 authentication groups can be added.
- For the authentication group which certificate type is **Local Authentication**, up to 8 card groups can be added to the authentication group.
- For the authentication group which certificate type is **Local Authentication and Super Password** or **Local Authentication and Remotely Open Door**, up to 7 card groups can be added to the authentication group.

7.8.4 Open Door with First Card

Purpose:

You can set multiple first cards for one access control point. After the first card swiping, it allows multiple persons access the door or other authentication actions. The first card mode contains Remain Open with First Card and Disable Remain Open with First Card.

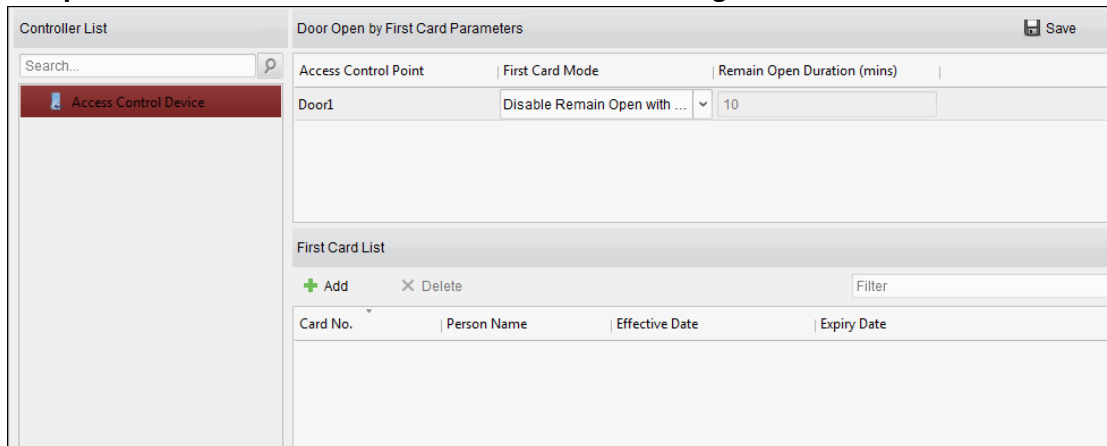
- **Remain Open with First Card:** The door remains open for the configured time duration after the first card swiping until the remain open duration ends.
- **Disable Remain Open with First Card:** Disable the function.

Notes:

- The first card authorization is effective only on the current day. The authorization will be expired after 24:00 on the current day.
- You can swipe the first card again to disable the first card mode.

Steps:

1. Click **Open Door with First Card** tab to enter the following interface.

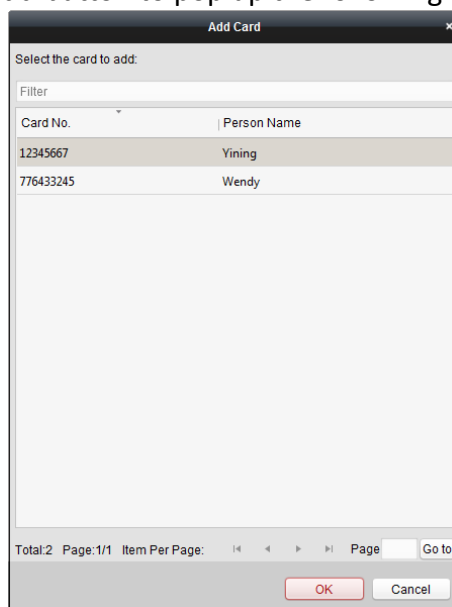


2. Select an access control device from the list on the left.
3. Select the first card mode in the drop-down list for the access control point and set the remain open duration.

Notes:

- The Remain Open Duration should be between 0 and 1440 minutes. By default, it is 10 minutes.
- You can swipe the first card again to disable the first card mode.

4. In the First Card list, Click **Add** button to pop up the following dialog box.



- 1) Select the cards to add as first card for the door
Note: Set the card permission and apply the permission setting to the access control device first. For details, refer to *Chapter 7.7 Permission Configuration*.
- 2) Click **OK** button to save adding the card.
5. You can click **Delete** button to remove the card from the first card list.
6. Click **Save** to save and take effect of the new settings.

7.8.5 Anti-Passing Back

Purpose:

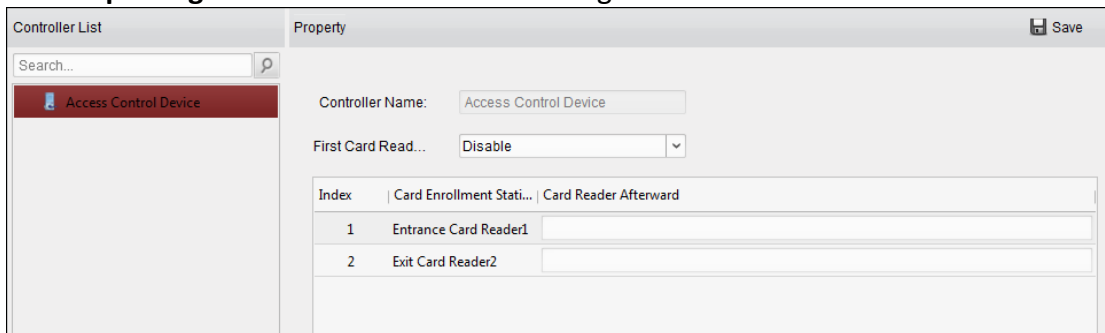
You can set to only pass the access control point according to the specified path and only one person could pass the access control point after swiping the card.

Notes:

- Either the anti-passing back or multi-door interlocking function can be configured for an access control device at the same time.
- You should enable the anti-passing back function on the access control device first.

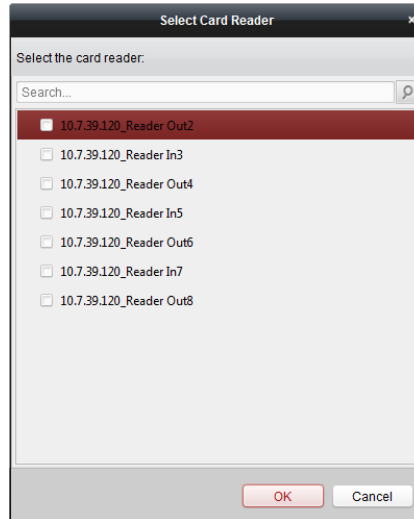
Steps:

1. Click **Anti-passing Back** tab to enter the following interface.



2. Select an access control device from the device list on the left.
3. In the First Card Reader field, select the card reader as the beginning of the path.
4. 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 point by swiping the card in the order as Reader In_01, Reader In_02 and Reader Out_04.



Note: Up to four afterward card readers can be added for one card reader.

- (Optional) You can enter the Select Card Reader dialog box again to edit its afterward card readers.
- Click **Save** to save and take effect of the new settings.

7.8.6 Person in Blacklist

Purpose:

You can configure the person information in the blacklist and apply to the device.

Adding Person to Blacklist

Purpose:

You can add persons to the blacklist, and configure the person's face pictures, gender, and ID number.

Note: The function should be supported by the device.

Steps:

- Click **Access Control > Advanced Function > Blacklist** to enter the person in blacklist management page.
- Click **Person** to enter the person management page.
- Click **Add**.
- Click **Select Picture** to select a face picture for the person from local PC.

Note: The picture should be in JPG format and it should be smaller than 200K.

- Set the person details including name, gender, and ID number.
- Click **Save**.
- (Optional) Select the added person and click **Delete** to remove it from the blacklist.
- Apply the person in blacklist to the device to take effect.
 - Select the person(s) to apply to the device.
 - Click **Apply**.
 - Click **Apply All** to start applying all the selected permission(s) to the access control device

or door station.

You can also click **Apply Changes** to apply the changed part of the selected permission(s) to the device(s).

- 4) Click **OK** to start applying.

Managing Blacklist Application Result

Purpose:

After applying the configured person information in blacklist, you can view the application results and manage the applied person.

Steps:

1. Click **Access Control > Advanced Function > Blacklist** to enter the person in blacklist management page.
2. Click **Application Result** to enter the application result management page.
You can check the person in blacklist applying record and view the application results.
3. (Optional) Remove the applied person in blacklist from device.
 - 1) Click **Delete Person**.
All the devices which support person in blacklist will display.
 - 2) Select the device that you want to remove person(s) from.
 - 3) Click **Next**.
All the persons in blacklist applied to the device will display.
 - 4) Select the person(s) you want to remove from the device.
 - 5) Click **OK** to remove the selected person from the blacklist of the device.
4. (Optional) Click **Clear Persons** and select the device to clear all the persons in the blacklist of the device.

7.9 Searching Access Control Event

Purpose:


You can search the access control history events including remote event and local event via the client.

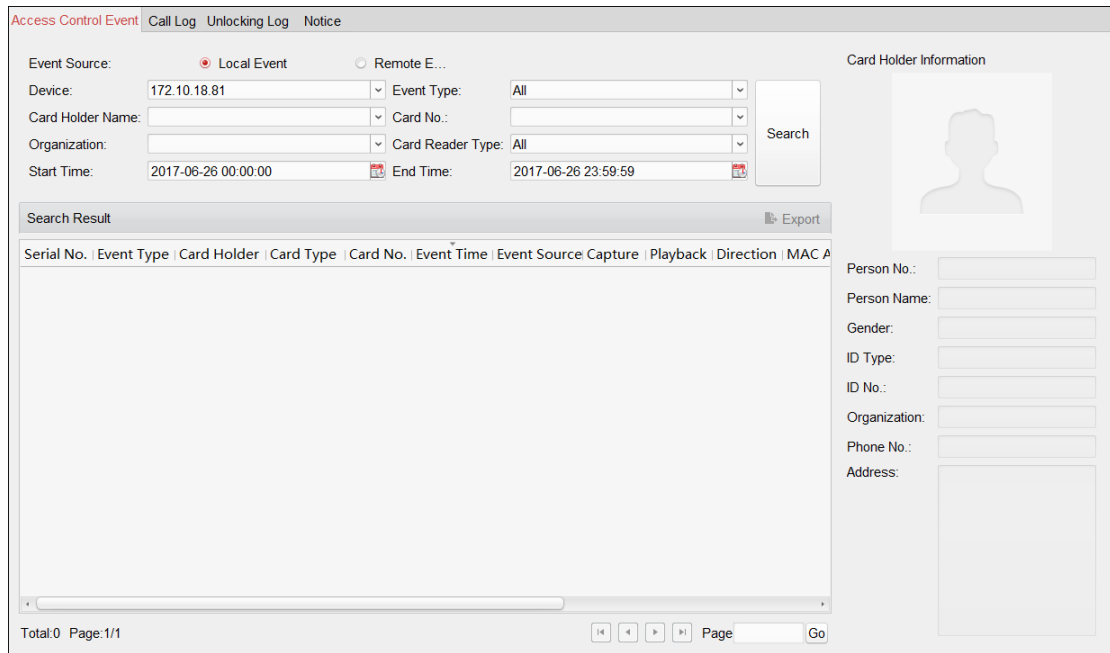
Before you start:

You should set the remote storage to view the captured face picture before searching the access control event. For details about setting remote storage, refers to *Chapter 5.1 Remote Storage* in *User Manual of iVMS-4200*.

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

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

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



7.9.1 Searching Local Access Control Event

Steps:

1. Select the Event Source as **Local Event**.
 2. Input the search condition according to actual needs.
 3. Click **Search**. The results will be listed below.
 4. For the access control event which is triggered by the card holder, you can click the event to view the card holder details, including person No., person name, organization, phone number, contact address and photo.
 5. (Optional) If the event contains linked pictures, you can click in the **Capture** column to view the captured picture of the triggered camera when the alarm is triggered.
 6. (Optional) If the event contains linked video, you can click in the **Playback** column to view the recorded video file of the triggered camera when the alarm is triggered.
- Note:** For setting the triggered camera, refer to *Chapter 7.10.1 Access Control Event Linkage*.
7. You can click **Export** to export the search result to the local PC in *.csv file.

7.9.2 Searching Remote Access Control Event

Steps:


1. Select the Event Source as **Remote Event**.
2. Input the search condition according to actual needs.

3. (Optional) You can check **With Alarm Picture** checkbox to search the events with alarm pictures.
4. Click **Search**. The results will be listed below.
5. You can click **Export** to export the search result to the local PC in *.csv file.

7.10 Access Control Event Configuration

Purpose:

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

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

7.10.1 Access Control Event Linkage

Purpose:

You can assign linkage actions to the access control event by setting up a rule. For example, when the access control event is detected, an audible warning appears or other linkage actions happen.

Note: The linkage here refers to the linkage of the client software's own actions.

Steps:

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

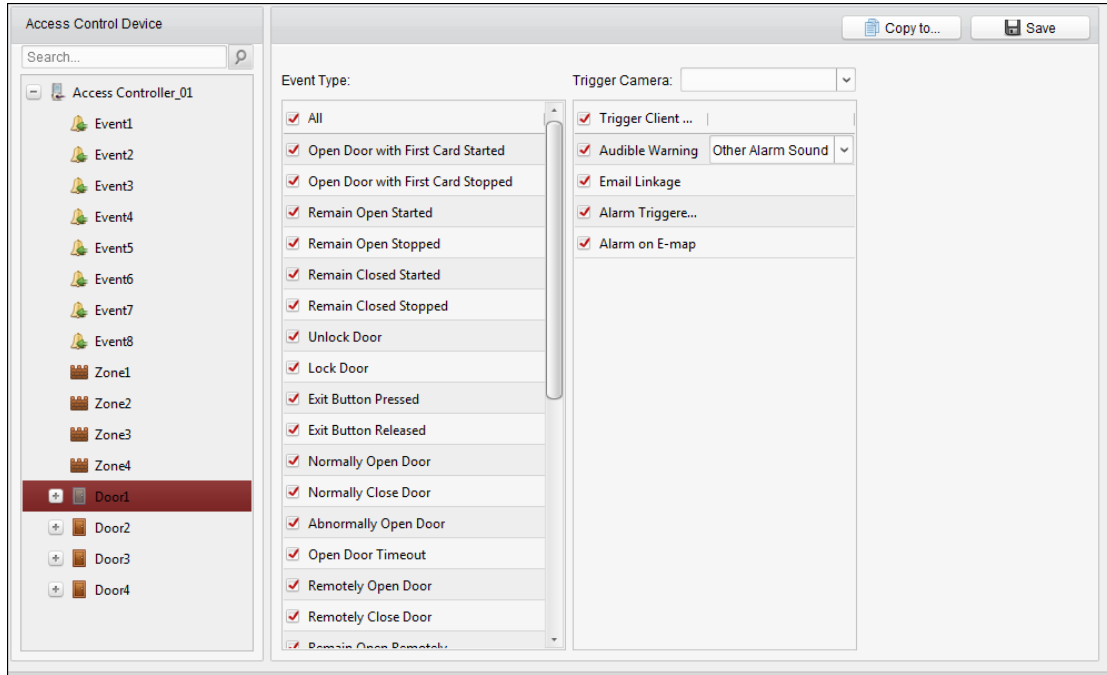


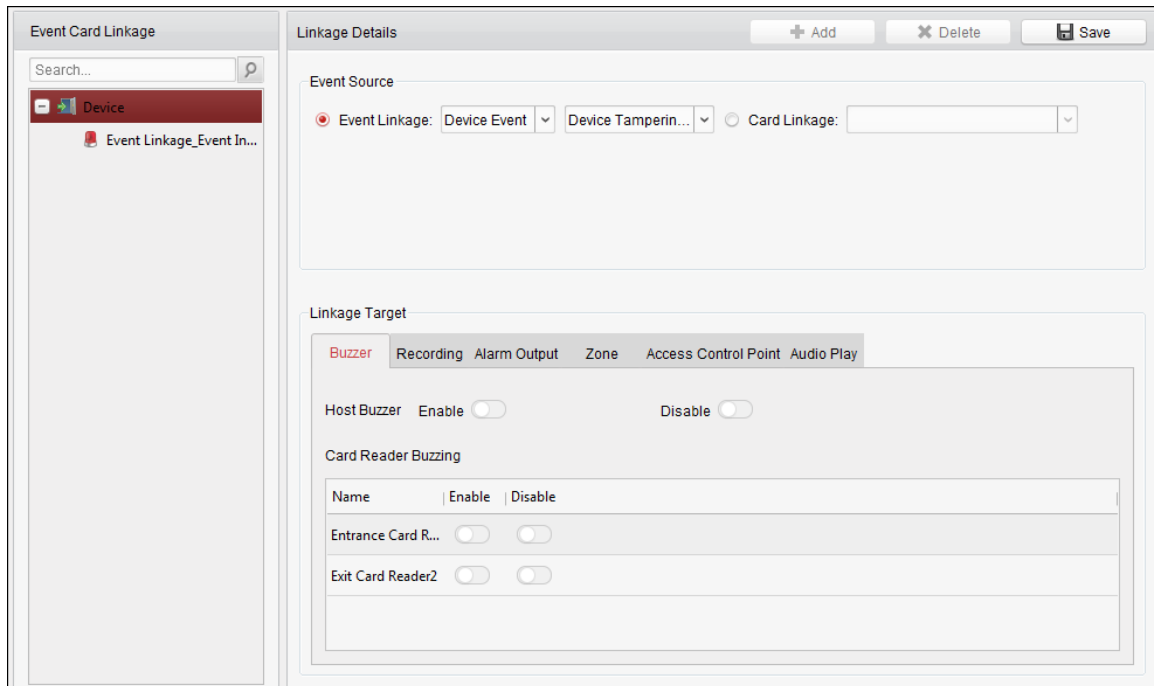
Table 1. 1 Linkage Actions for Access Control Event

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

7.10.2 Event Card Linkage

Click **Event Card Linkage** tab to enter the following interface.

Note: The Event Card Linkage should be supported by the device.



Select the access control device from the list on the left.

Click **Add** button to add a new linkage. You can select the event source as **Event Linkage** or **Card Linkage**.

Event Linkage

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

Steps:

1. Select a device on the left and click **Add**.
2. Click to select the linkage type as **Event Linkage**, and select the event type from the dropdown list.
 - For Device Event, select the detailed event type from the dropdown list.
 - For Alarm Input, select the type as alarm or alarm recovery and select the alarm input name from the panel.
 - For Door Event, select the detailed event type and select the source door from the panel.
 - For Card Reader Event, select the detailed event type and select the card reader from the panel.
3. Click different tabs to set different parameters. Switch the property from to to enable this function.

You can set the parameters of buzzer, recording, alarm output, and access control point.



Linkage Type	Linkage Target	Descriptions
Buzzer	Host Buzzer	The audible warning of controller will be triggered.
	Card Reader Buzing	The audible warning of card reader will be triggered.
Recording	Capture Status	The real-time capture will be triggered.
Alarm Output	Alarm Output	The alarm output will be triggered for notification.

Access Control Point	Access Control Point	<p>The door status of open, close, remain open, and remain closed will be triggered.</p> <p>Notes:</p> <ul style="list-style-type: none"> ● The door status of open, close, remain open, and remain close cannot be triggered at the same time. ● The target door and the source door cannot be the same one.
----------------------	----------------------	--

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

Card Linkage

Steps:

1. Click to select the linkage type as **Card Linkage**.
2. Input the card No. or select the card from the dropdown list.
3. Select the card reader from the panel for triggering.
5. Click different tabs to set different parameters. Switch the property from  to  to enable this function.

You can set the parameters of buzzer, recording, alarm output, and access control point.

Linkage Type	Linkage Target	Descriptions
Buzzer	Host Buzzer	The audible warning of controller will be triggered.
	Card Reader Buzzing	The audible warning of card reader will be triggered.
Recording	Capture Status	The real-time capture will be triggered.
Alarm Output	Alarm Output	The alarm output will be triggered for notification.
Access Control Point	Access Control Point	<p>The door status of open, close, remain open, and remain closed will be triggered.</p> <p>Notes:</p> <ul style="list-style-type: none"> ● The door status of open, close, remain open, and remain close cannot be triggered at the same time. ● The target door and the source door cannot be the same one.

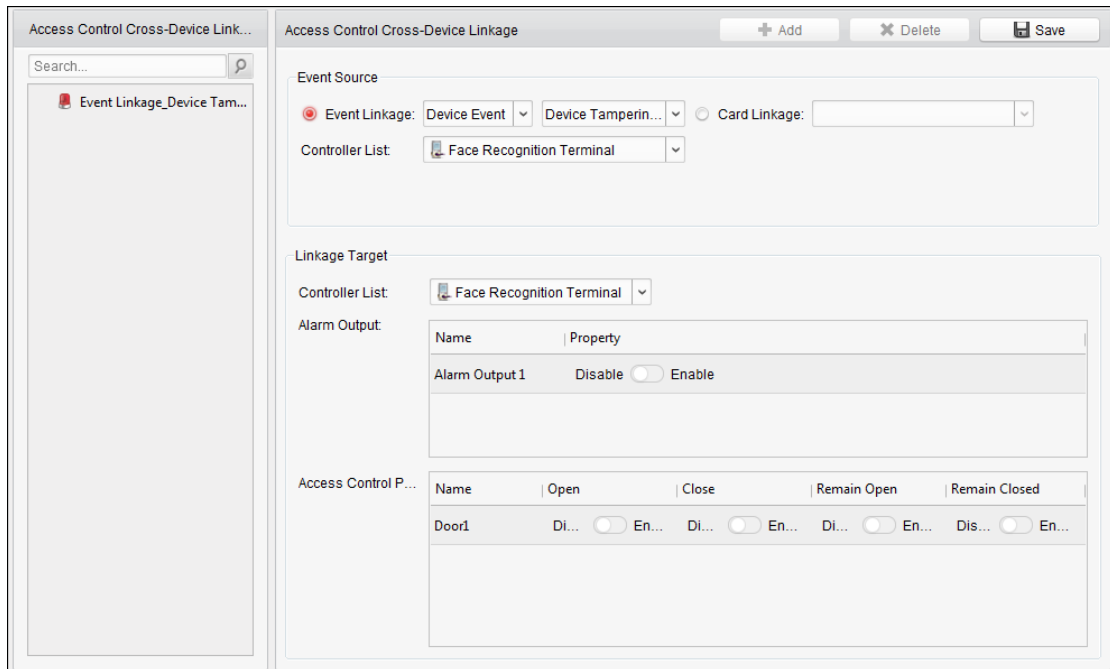
4. Click **Save** to save and take effect of the parameters.

7.10.3 Cross-Device Linkage

Purpose:

You can assign to trigger other access control device’s action by setting up a rule when the access control event is triggered.

Click **Cross-Device Linkage** tab to enter the following interface.



Click **Add** button to add a new client linkage. You can select the event source as **Event Linkage** or **Card Linkage**.

Event Linkage

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



Steps:

- Click to select the linkage type as **Event Linkage**, select the access control device as event source, and select the event type from the dropdown list.
 - For Device Event, select the detailed event type from the dropdown list.
 - For Alarm Input, select the type as alarm or alarm recovery and select the alarm input name from the table.
 - For Door Event, select the detailed event type and select the door from the table.
 - For Card Reader Event, select the detailed event type and select the card reader from the table.
- Set the linkage target, select the access control device from the dropdown list as the linkage target, and switch the property from to to enable this function.
 - Alarm Output:** The alarm output will be triggered for notification.
 - Access Control Point:** The door status of open, close, remain open, and remain close will be triggered.

Note: The door status of open, close, remain open, and remain close cannot be triggered at the same time.
- Click **Save** button to save parameters.

Card Linkage

Steps:

1. Click to select the linkage type as **Card Linkage**.
2. Select the card from the dropdown list and select the access control device as event source.
3. Select the card reader from the table for triggering.
4. Set the linkage target, select the access control device from the dropdown list as the linkage target, and switch the property from  to  to enable this function.
Alarm Output: The alarm output will be triggered for notification.
5. Click **Save** button to save parameters.

7.11 Door Status Management

Purpose:

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


7.11.4 Access Control Group Management

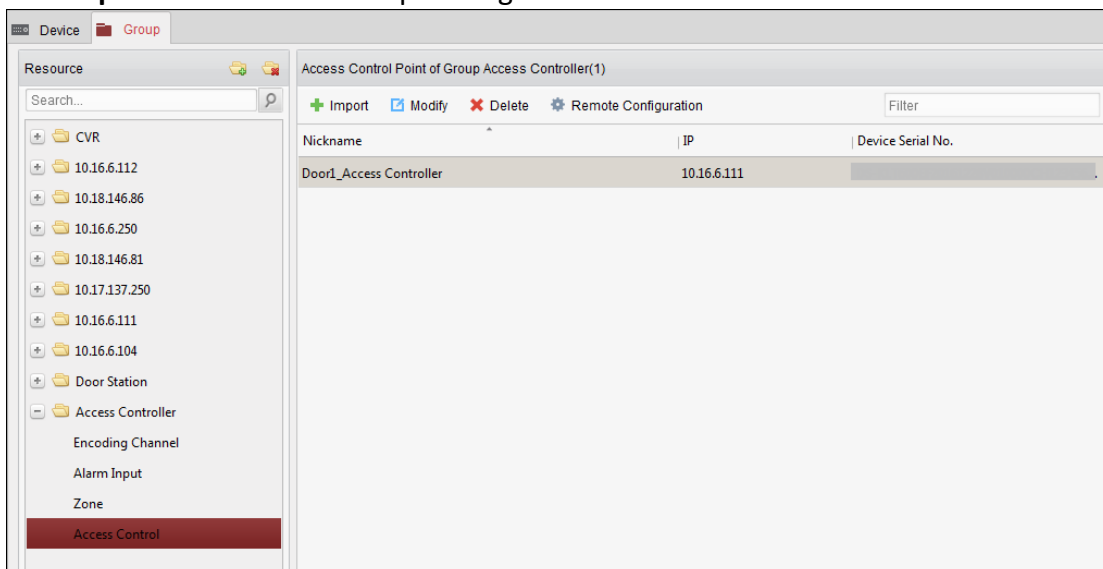
Purpose:


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

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

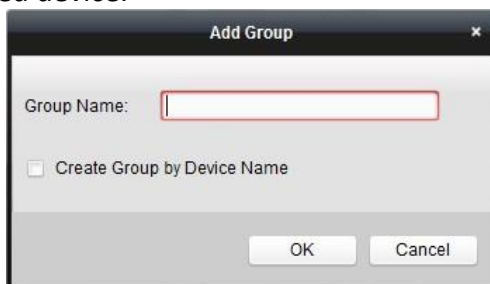
Steps:

1. Click  on the control panel to open the Device Management page.
2. Click **Group** tab to enter the Group Management interface.



3. Perform the following steps to add the group.
 - 1) Click  to open the Add Group dialog box.
 - 2) Input a group name as you want.
 - 3) Click **OK** to add the new group to the group list.

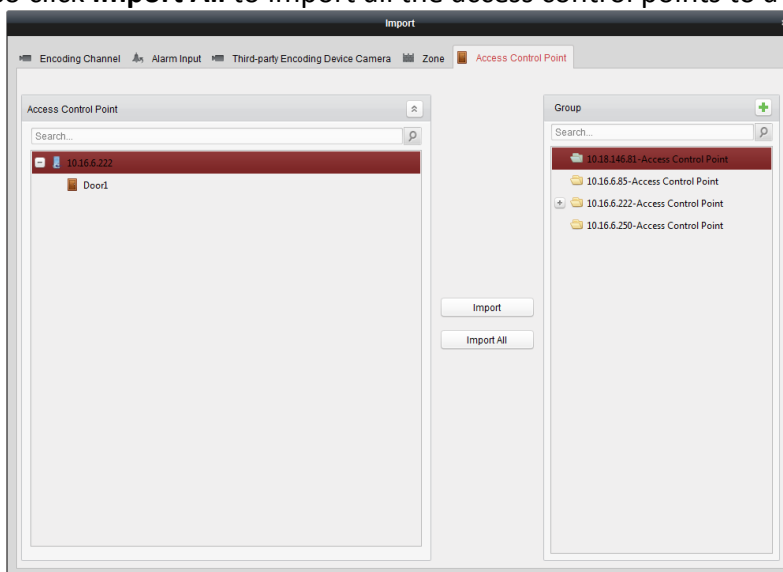
You can also check the checkbox **Create Group by Device Name** to create the new group by the name of the selected device.




4. Perform the following steps to import the access control points to the group:
 - 1) Click **Import** on Group Management interface, and then click the **Access Control** tab to open the Import Access Control page.

Notes:

- You can also select **Alarm Input** tab and import the alarm inputs to group.
 - For the Video Access Control Terminal, you can add the cameras as encoding channel to the group.
- 2) Select the names of the access control points in the list.
 - 3) Select a group from the group list.
 - 4) Click **Import** to import the selected access control points to the group.
You can also click **Import All** to import all the access control points to a selected group.



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

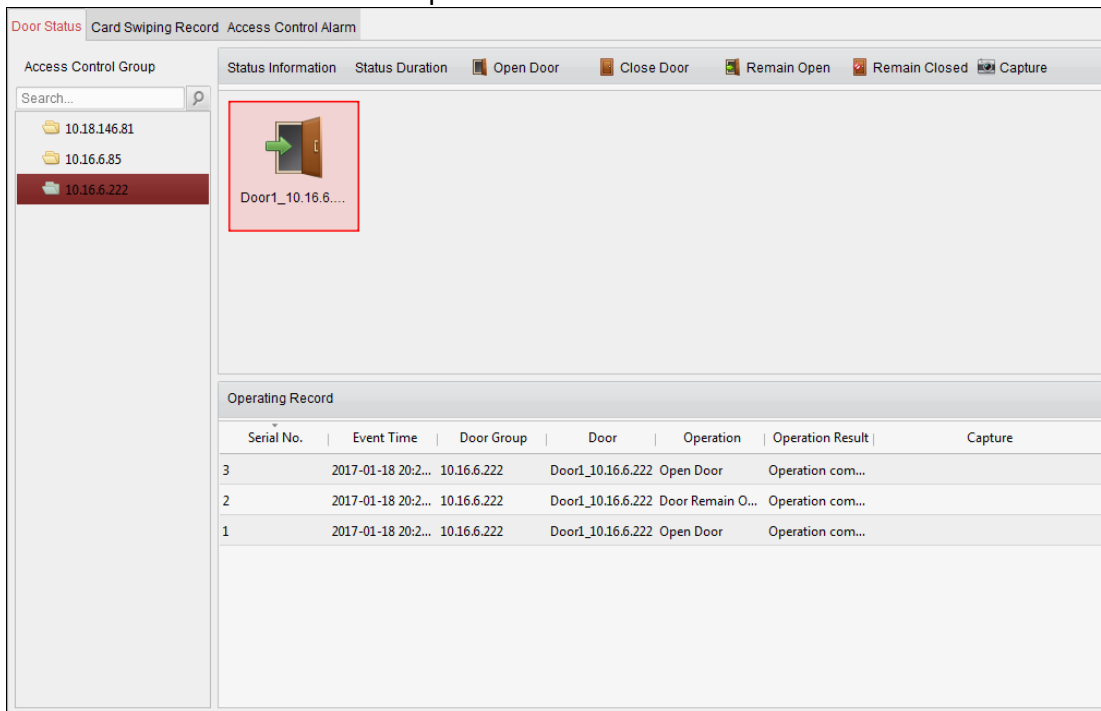
7.11.5 Anti-control the Access Control Point (Door)

Purpose:

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



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



Steps:

1. Select an access control group on the left. For managing the access control group, refer to *Chapter 7.11.4 Access Control Group Management*.
2. The access control points of the selected access control group will be displayed on the right.



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

3. Click the following button listed on the **Status Information** panel to control the door.

- Open Door**: Click to open the door once.
- Close Door**: Click to close the door once.
- Remain Open**: Click to keep the door open.
- Remain Closed**: Click to keep the door closed.
- Capture**: Click to capture the picture manually.

4. You can view the anti-control operation result in the Operation Log panel.

Notes:

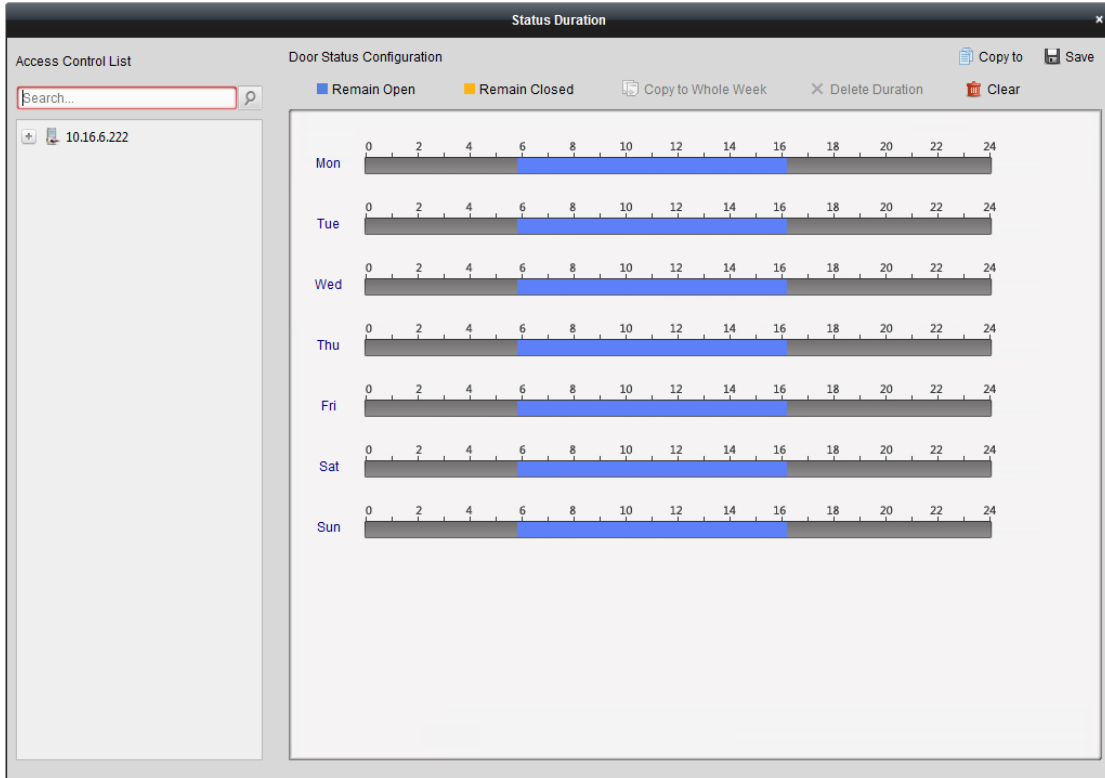
- If you select the status as **Remain Open/Remain Closed**, the door will keep open/closed until a new anti-control command being made.
- The **Capture** button is available when the device supports capture function. And it cannot be realized until the storage server is configured.
- If the door is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

7.11.6 Status Duration Configuration

Purpose:

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

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




Steps:


1. Click to select a door from the access control device list on the left.
2. On the Door Status Configuration panel on the right, draw a schedule for the selected door.
 - 1) Select a door status brush as Remain Open or Remain Closed.

Remain Open: The door will keep open during the configured time period. The brush is marked as ■.

Remain Closed: The door will keep closed during the configured duration. The brush is marked as ■.
 - 2) Click and drag on the timeline to draw a color bar on the schedule to set the duration.



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

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

3. Optionally, you can select the schedule time bar and click **Copy to Whole Week** to copy the time bar settings to the other days in the week.
4. You can select the time bar and click **Delete Duration** to delete the time period.
Or you can click **Clear** to clear all configured durations on the schedule.
5. Click **Save** to save the settings.
6. You can click **Copy to** button to copy the schedule to other doors.

7.11.7 Real-time Card Swiping Record

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

The screenshot displays a software interface with three tabs: 'Door Status', 'Card Swiping Record', and 'Access Control Alarm'. The 'Access Control Alarm' tab is active. Below the tabs is a table with columns: 'Card No.', 'Person Name', 'Organization', 'Event Time', 'Door Position', 'Direction', and 'Operation'. The table area is currently empty. To the right of the table is a sidebar titled 'Card Holder Information'. It features a placeholder image of a person's head and shoulders. Below the image are several input fields with labels: 'Person No.', 'Person Name', 'Gender', 'ID Type', 'ID No.', 'Organization', 'Phone No.', 'Address', and 'Email'.

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

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

7.11.8 Real-time Access Control Alarm

Purpose:

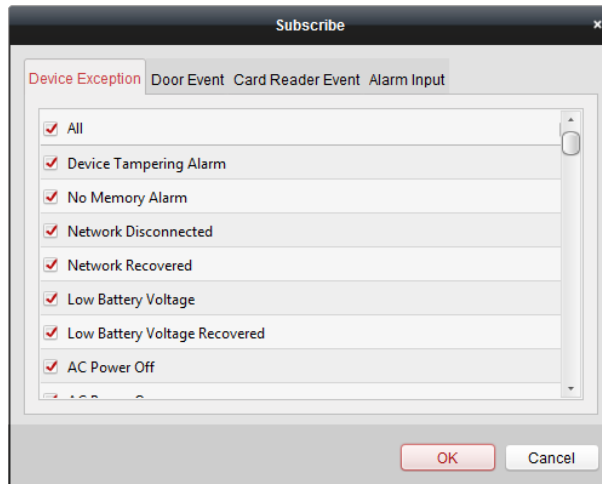
The logs of access control events will be displayed in real time, including device exception, door event, card reader event, and alarm input.

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

Alarm Type	Alarm Time	Alarm Location	Alarm Content	Operation
Remote: Disarm...	2016-12-16 13:5...	Access Controller	Remote: Disarm...	
Remote: Arming	2016-12-16 13:5...	Access Controller	Remote: Arming	
Remote: Login	2016-12-16 13:5...	Access Controller	Remote: Login	
Remote: Disarm...	2016-12-16 13:5...	Access Controller	Remote: Disarm...	
Remote: Logout	2016-12-16 13:5...	Access Controller	Remote: Logout	
Remote: Login	2016-12-16 13:5...	Access Controller	Remote: Login	
Remote: Arming	2016-12-16 13:4...	Access Controller	Remote: Arming	
Remote: Login	2016-12-16 13:4...	Access Controller	Remote: Login	
Remote: Disarm...	2016-12-16 13:4...	Access Controller	Remote: Disarm...	
Door Locked	2016-12-16 13:4...	Door1	Door Locked	
Unlock	2016-12-16 13:4...	Door1	Unlock	
Remote: Arming	2016-12-16 13:4...	Access Controller	Remote: Arming	
Remote: Login	2016-12-16 13:4...	Access Controller	Remote: Login	
Remote: Disarm...	2016-12-16 13:4...	Access Controller	Remote: Disarm...	

Steps:

1. All access control alarms will display in the list in real time.
You can view the alarm type, alarm time, location, etc.
 2. Click to view the alarm on E-map.
 3. You can click or to view the live view or the captured picture of the triggered camera when the alarm is triggered.
- Note:** For setting the triggered camera, refer to *Chapter 7.10.1 Access Control Event Linkage*.
4. Click **Subscribe** to select the alarm that the client can receive when the alarm is triggered.



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

7.12 Arming Control

Purpose:

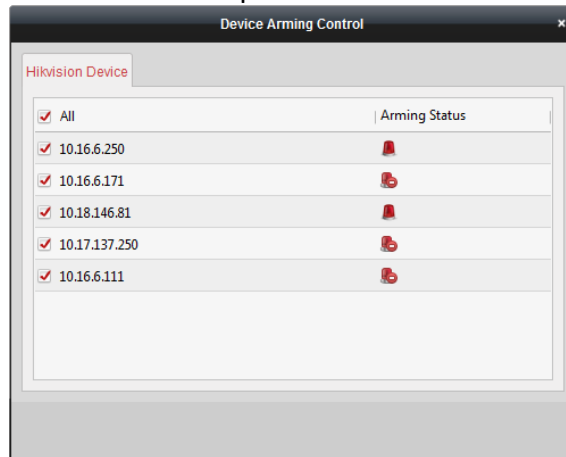
You can arm or disarm the device. After arming the device , the client can receive the alarm information from the device.

Steps:

9. Click **Tool->Device Arming Control** to pop up the Device Arming Control window.

10. Arm the device by checking the corresponding checkbox.

Then the alarm information will be auto uploaded to the client software when alarm occurs.



7.13 Time and Attendance

Purpose:


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

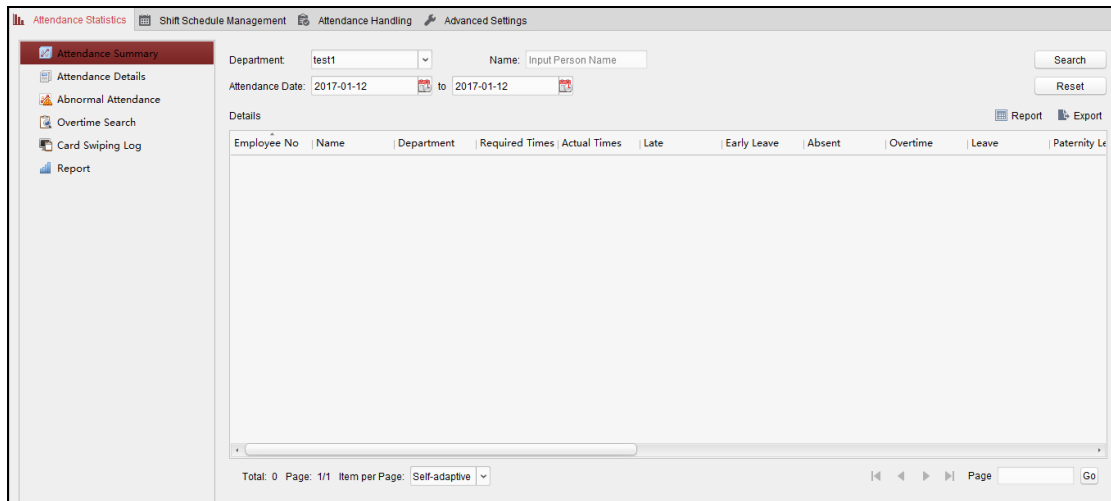
Before you start:

You should add organization and person in Access Control module. For details, refer to *Chapter 7.4.1 Adding Organization* and *Chapter 7.5.1 Adding Person*.

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

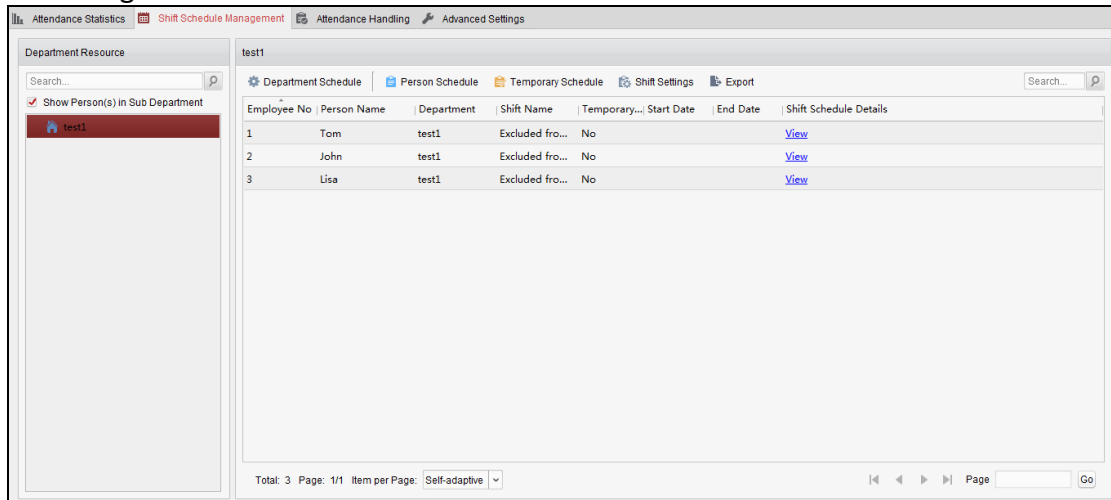


Click  to enter the Time and Attendance module as follows:



7.13.1 Shift Schedule Management

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



Shift Settings

Purpose:

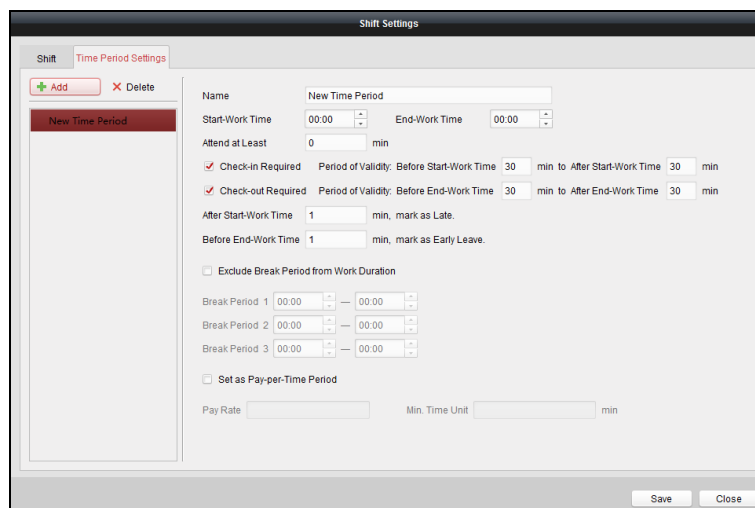
You can add time period and shift for the shift schedule.

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

➤ Adding Time Period

Steps:

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



3. Set the related parameters.

Name: Set the name for time period.

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

Attend at Least: Set the minimum attendance time.

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

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

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

Note: Up to 3 break periods can be set.

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

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

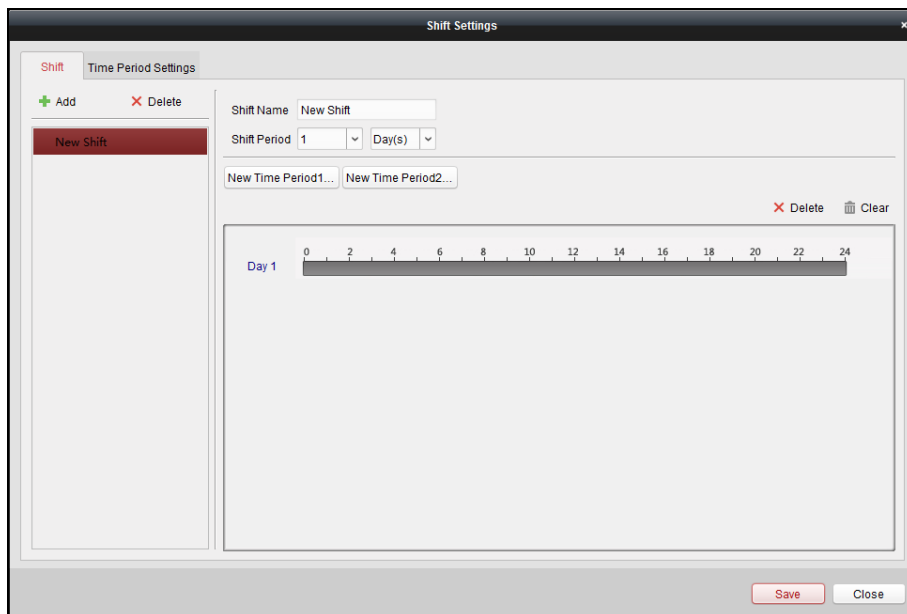
The added time period will display on the left panel of the dialog.

You can also click **Delete** to delete the time period.

➤ **Adding Shift**

Steps:

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



3. Set the name for shift.

4. Select the shift period from the drop-down list.

5. Configure the shift period with the added time period.

1) Select the time period.

2) Click the time bar to apply the time period for the select day.

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

You can also click **Clear** to delete all days' time period.

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

The added shift will display on the left panel of the dialog.

You can also click **Delete** on the left panel to delete the shift.

Shift Schedule Settings

Purpose:

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

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

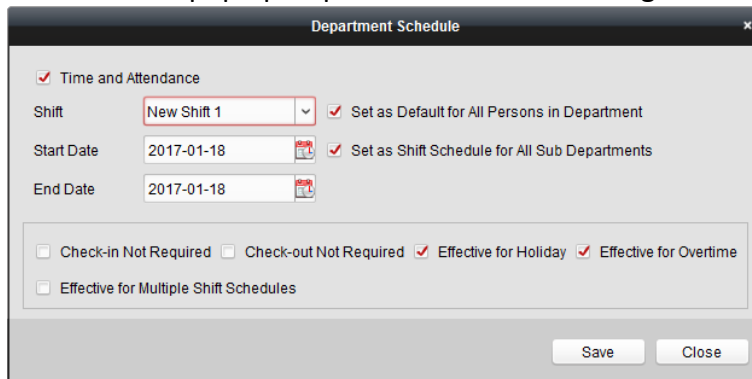
➤ **Department Schedule**

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

Note: In Time and Attendance module, the department list is the same with the **organization** in Access Control. For setting the organization in Access Control, refer to *Chapter 7.4 Organization Management*.

Steps:

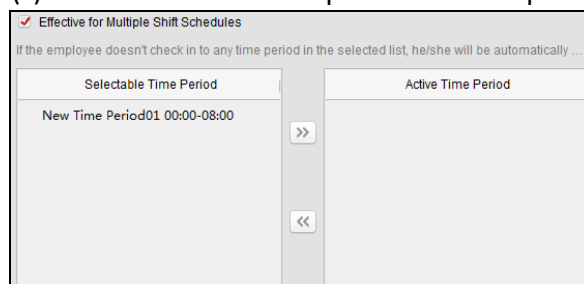
1. Open the Shift Schedule Management interface and select the department on the left panel.
2. Click **Department Schedule** to pop up Department Schedule dialog.





3. Check **Time and Attendance** checkbox.
All persons in the department except those excluded from attendance will apply the attendance schedule.
4. Select the shift from the drop-down list.
5. Set the start date and end date.
6. (Optional) Set other parameters for the schedule.
You can select Check-in Not Required, Check-out Not Required, Effective for Holiday, Effective for Overtime, Effective for Multiple Shift Schedules.

Notes:

- Multiple Shift Schedules contains more than one time periods. The person can check in/out in any of the time periods and the attendance will be effective.
Example: If the multiple shift schedules contains three time periods: 00:00 to 07:00, 08:00 to 15:00 and 16:00 to 23:00. The attendance of the person adopting this multiple shift schedules will be effective in any of the three time periods. If the person checks in at 07:50, it will apply the nearest time period 08:00 to 15:00 to the person’s attendance.
- After checking the **Effective for Multiple Shift Schedules** checkbox, you can select the effective time period(s) from the added time periods for the persons in the department.

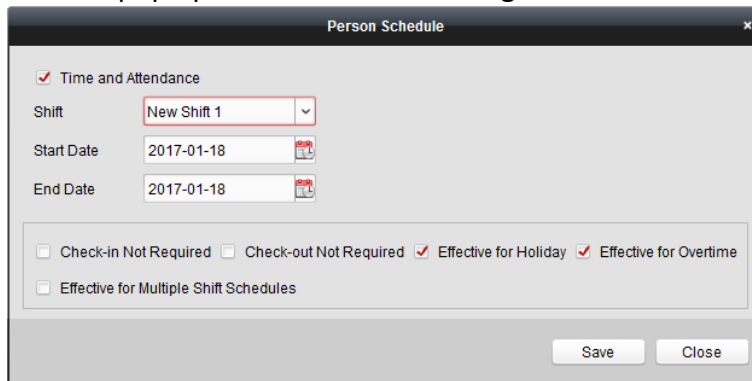


- 1) In the Selectable Time Period list on the left, click the added time period and click  to add it to the right.
- 2) (Optional) To remove the selected time period, select it and click .
7. (Optional) Check **Set as Default for All Persons in Department** checkbox. All persons in the department will use this shift schedule by default.
8. (Optional) If the selected department contains sub department(s), the Set as **Shift Schedule for All Sub Departments** checkbox will display. You can check it to apply the department schedule to its sub departments.
9. Click **Save** to save the settings.

➤ **Person Schedule**

Steps:

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

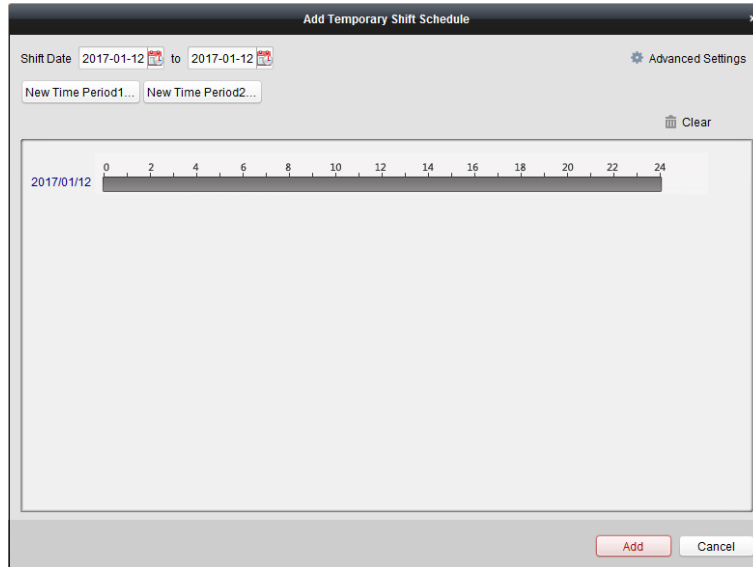




4. Check **Time and Attendance** checkbox. The configured person will apply the attendance schedule.
5. Select the shift from the drop-down list.
6. Set the start date and end date.
7. (Optional) Set other parameters for the schedule. You can select Check-in Not Required, Check-out Not Required, Effective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

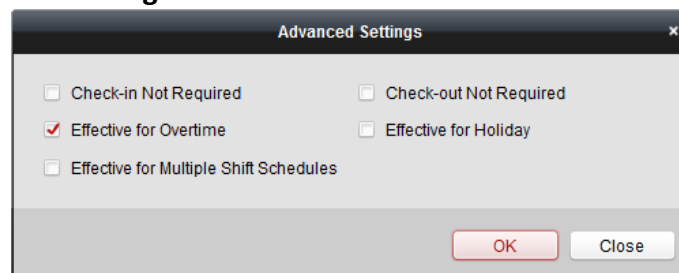
➤ **Temporary Schedule**

Steps:

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



4. Click  to set the shift date.
5. Configure the shift date with the added time period.
 - 1) Select the time period.
 - 2) Click the time bar to apply the time period for the select date.
You can click the time period on the bar and click  to delete the period.
You can also click **Clear** to delete all days' time period.
6. You can click **Advanced Settings** to advanced attendance rules for the temporary schedule.

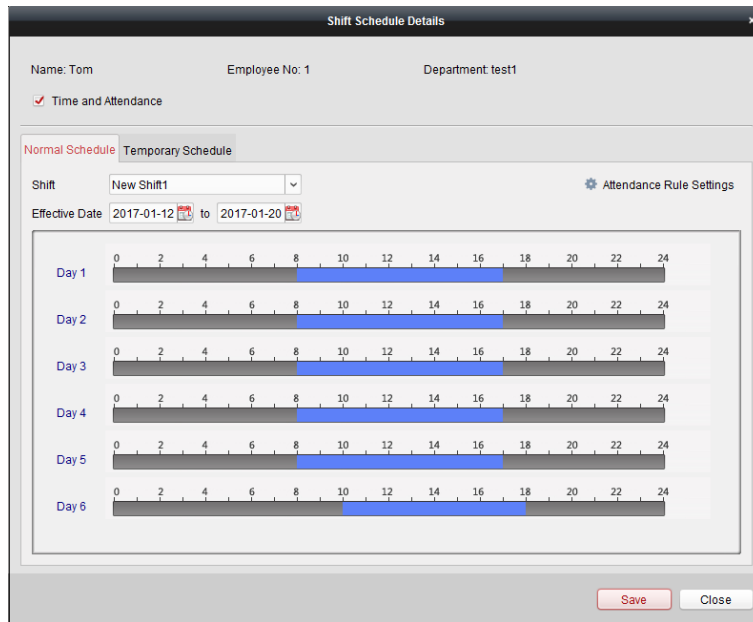


7. Click **Add** to save the settings.

➤ Checking Shift Schedule Details

Steps:

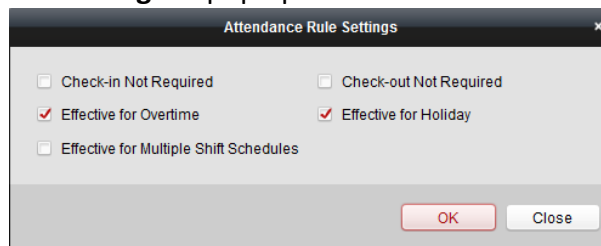
1. On the Shift Schedule Management interface, select the department on the left panel.
2. Select the person(s) on the right panel.
3. Click **View** to pop up Shift Schedule Details dialog.
You can check the shift schedule details.




4. Click **Normal Schedule** tab.

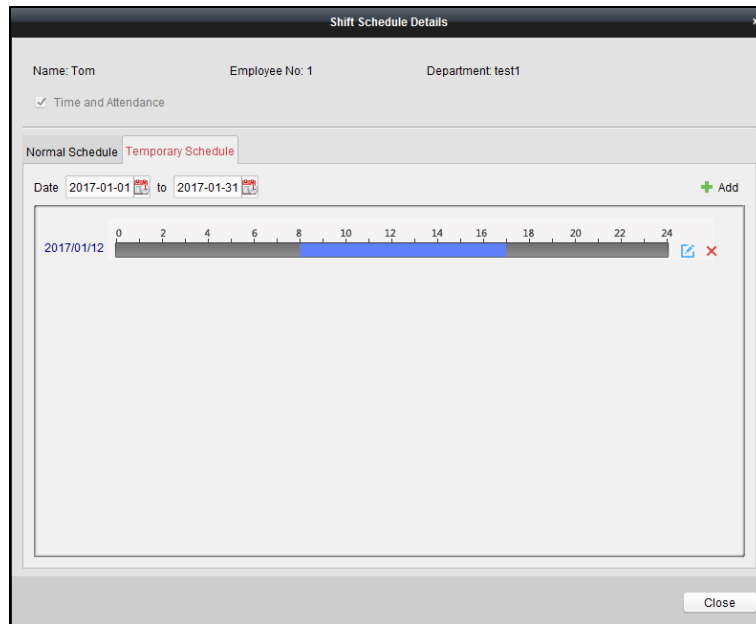
You can check and edit the normal schedule details.

- 1) Select the shift from the drop-down list.
- 2) Click **Attendance Rule Settings** to pop up Attendance Rule Settings dialog.




You can check the attendance rules as desired and click **OK** to save the settings.

- 3) Click  to set the effective date.
 - 4) Click **Save** to save the settings.
5. (Optional) Click **Temporary Schedule** tab.



You can check and edit the temporary schedule details.

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

(Optional) Click  to edit the time period.

(Optional) Click  to delete the temporary schedule.

➤ Exporting Shift Schedule Details

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

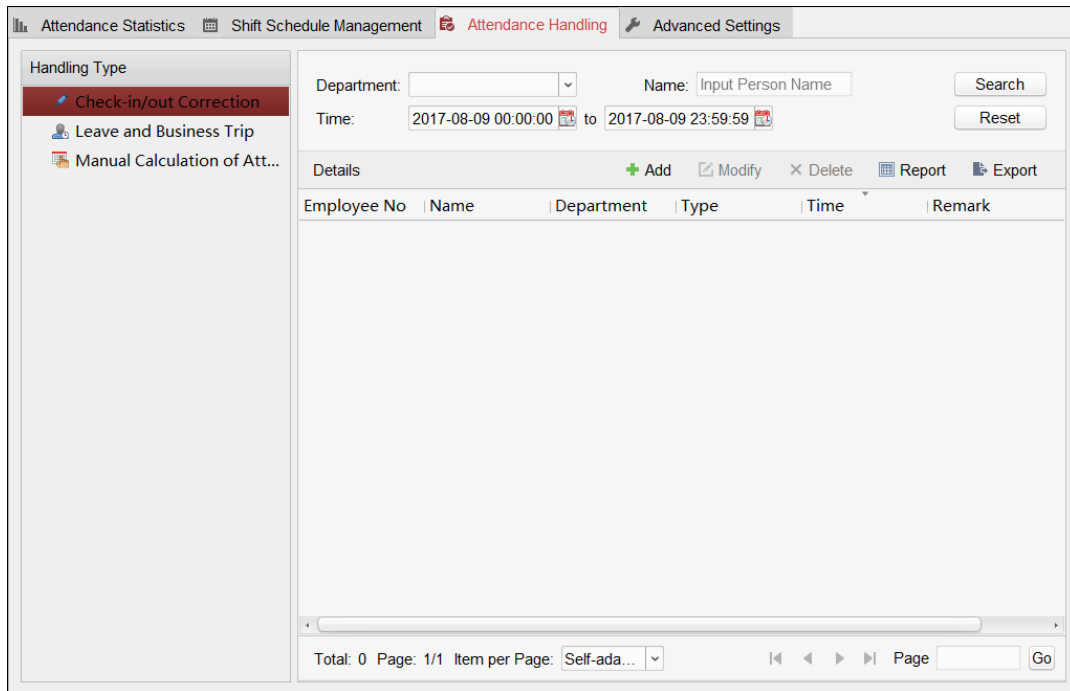
Note: The exported details are saved in *.csv format.

7.13.2 Attendance Handling

Purpose:

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

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



Check-in/out Correction


Purpose:

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

➤ **Add Check-in/out Correction**

Steps:

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


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

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

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

➤ **Search Check-in/out Correction**

Steps:

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

Leave and Business Trip



Purpose:

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

➤ **Add Leave and Business Trip**


Steps:

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

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

➤ **Search Leave and Business Trip**

Steps:

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

Department:	Department 1	Name:	Input Person Name	<input type="button" value="Search"/>			
Time:	2017-01-18 00:00:00	to	2017-01-18 23:59:59	<input type="button" value="Reset"/>			
Details <input type="button" value="+ Add"/> <input type="button" value="Modify"/> <input type="button" value="X Delete"/> <input type="button" value="Report"/> <input type="button" value="Export"/> 							
Employee No	Name	Department	Type	Reason	Start Time	End Time	Ren
1	Wendy	Department 1	Leave	Paternity Leave	2017-01-18 00:00:00	2017-01-18 23:59:59	
1	Wendy	Department 1	Day Off in Lieu	Overtime Exchange Holiday	2017-01-17 00:00:00	2017-01-17 23:59:59	

Manual Calculation of Attendance

Purpose:

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

Steps:

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

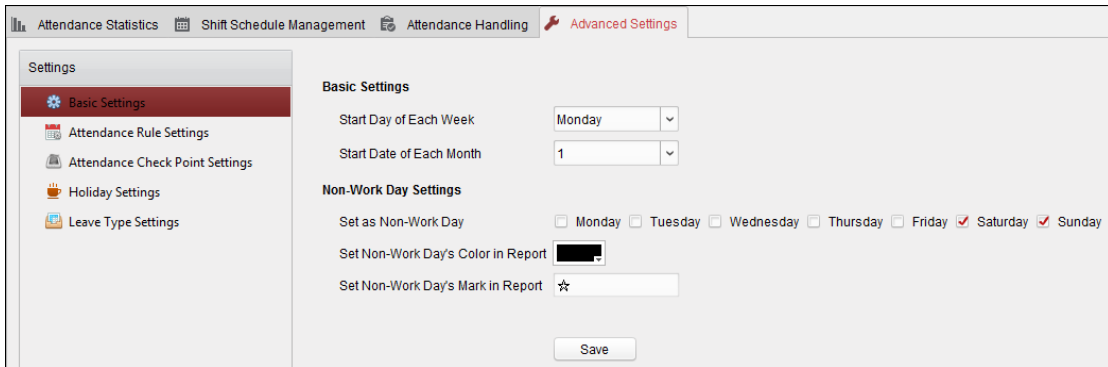
Note: It can only calculate the attendance data within three months.

7.13.3 Advanced Settings

Purpose:

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

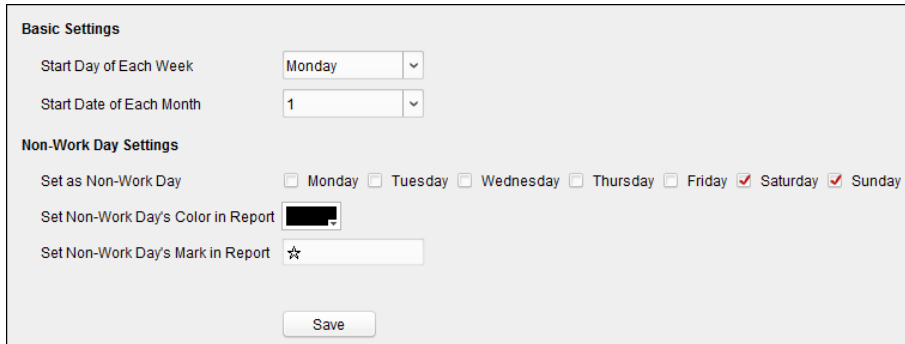
Open Time and Attendance module and click **Advanced Settings** to enter the Advanced Settings interface.



Basic Settings

Steps:

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



2. Set the basic settings.
 - Start Day of Each Week:** You can select one day as the start day of each week.
 - Start Date of Each Month:** You can select one day as the start date of each month.
3. Set the non-work day settings.
 - Set as Non-Work Day:** Check the checkbox(es) to set the selected day(s) as non-work day.
 - Set Non-Work Day's Color in Report:** Click the color filed and select the color to mark the non-work day in report.
 - Set Non-Work Day's Mark in Report:** Input the mark as non-work day in report.
4. Click **Save** to save the settings.

Attendance Rule Settings

Steps:

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


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

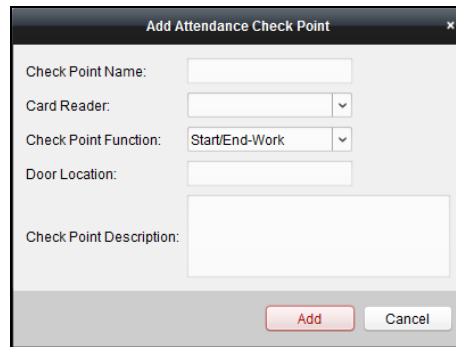
Attendance Check Point Settings

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

Steps:

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

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



3. Set the related information.

Check Point Name: Input a name for check point.

Card Reader: Select the card reader from the drop-down list.

Check Point Function: Select the function for check point.

Door Location: Input the door location.

Check Point Description: Set the description information for check point.

4. Click **Add** to add the attendance check point.


The added attendance check point will display on the list.

5. (Optional) Check **Set All Card Readers as Check Points** checkbox.

You can use all the card readers as check points.

Note: If this checkbox is unchecked, only the card readers in the list will be added as attendance check points.

You can also edit or delete the card readers.

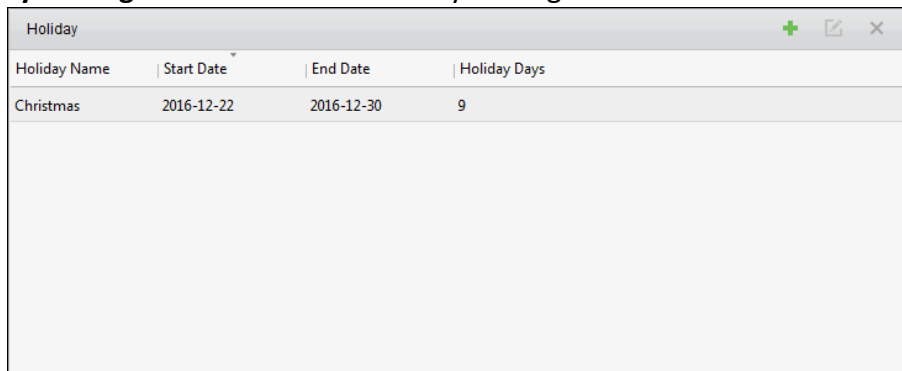
Click  to edit the card reader.

Click  to delete the card reader.


Holiday Settings

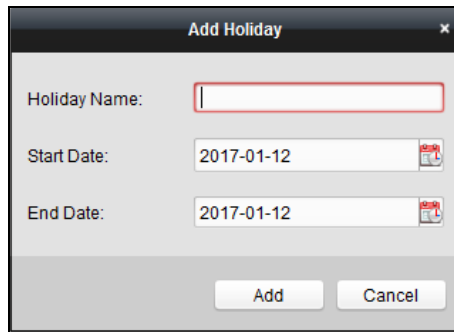
Steps:




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



Holiday Name	Start Date	End Date	Holiday Days
Christmas	2016-12-22	2016-12-30	9

2. Click  to pop up Add Holiday dialog.



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


Leave Type Settings

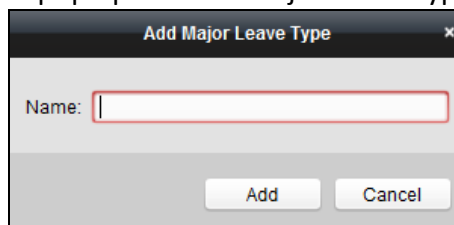
Purpose


Steps:

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

Leave		Minor Type	
	Index	Type	
Day Off in Lieu	1	Paternity Leave	
Go Out on Business	2	Parental Leave	
	3	Sick Leave	
	4	Family Reunion Leave	
	5	Annual Leave	
	6	Maternity Leave	
	7	Personal Leave	
	8	Bereavement Leave	

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



- 2) Input the name for major leave type.
- 3) Click **Add** to add the major leave type.
 You can also edit or delete the major leave type.
 Click  to edit the major leave type.

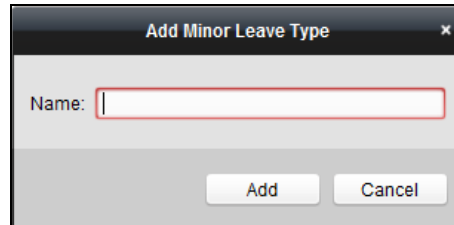
Click **X** to delete the major leave type.

3. Add the minor leave type.

1) Select the major leave type.

The minor leave type belonging to this major leave type will display on the right panel.

2) Click **+** on the right panel to pop up the Add Minor Leave Type dialog.



3) Input the name for minor leave type.

4) Click **Add** to add the minor leave type.

You can also edit or delete the major leave type.

Click **E** to edit the minor leave type.

Click **X** to delete the minor leave type.

7.13.4 Attendance Statistics

Purpose:

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

Notes:

- The client automatically calculates the previous day's attendance data at 1:00 am on the next day.
- Keep the client running at 1:00 am or it cannot calculate the previous day's attendance data automatically. If not calculated automatically, you can calculate the attendance data manually. For details, refer to *Manual Calculation of Attendance* in Chapter 7.13.2 Attendance Handling.

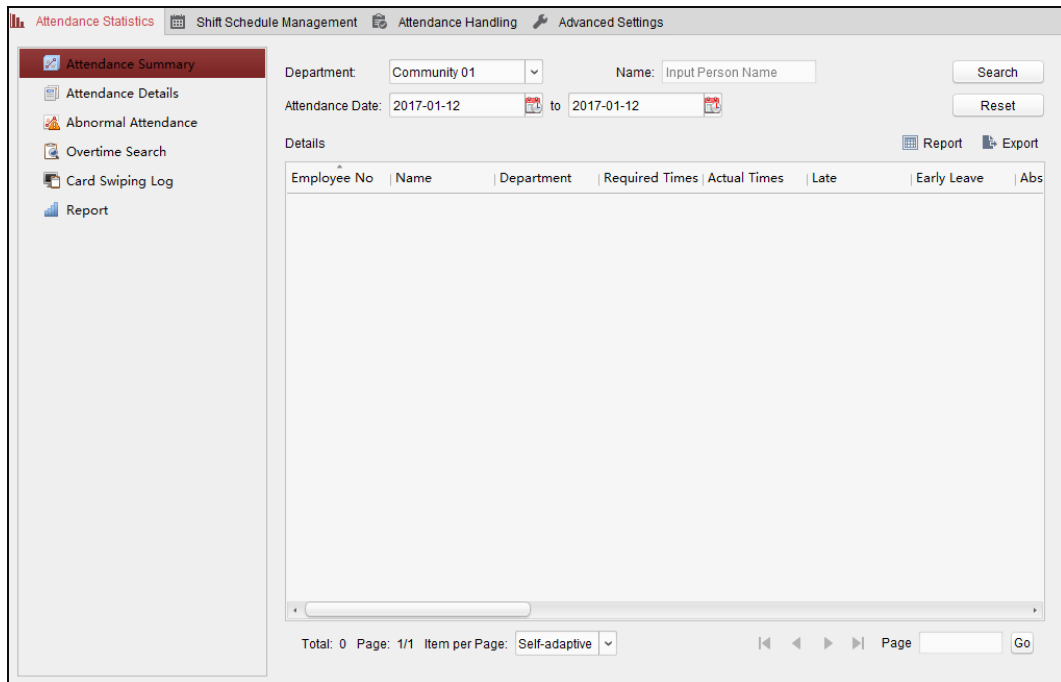
Attendance Summary

Purpose:

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

Steps:

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

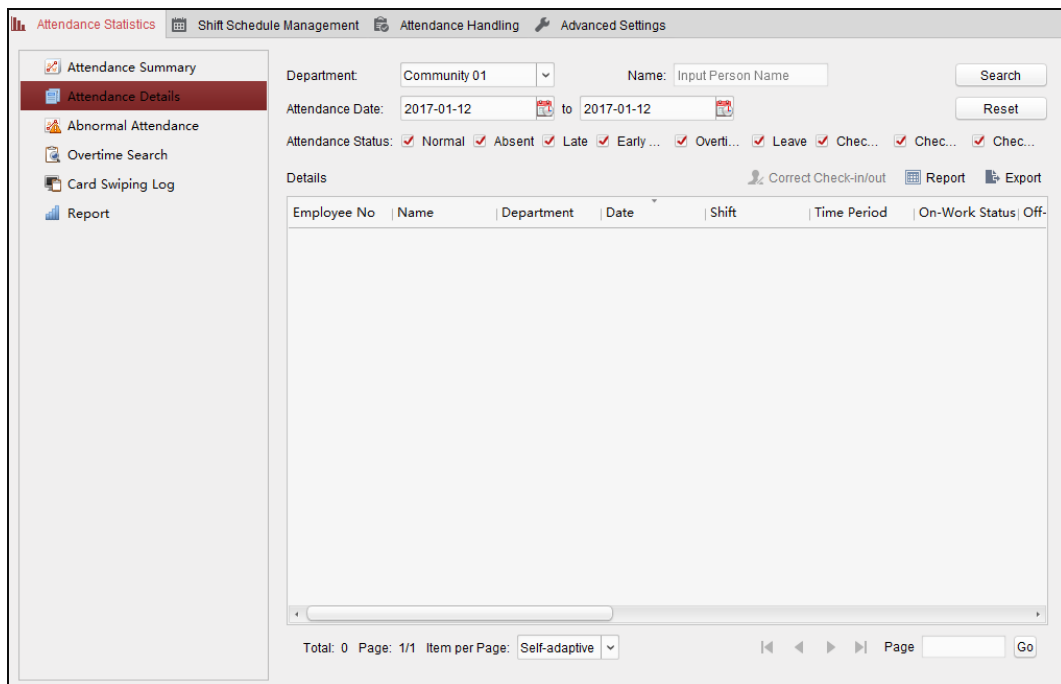


3. Set the search conditions, including department, employee name and attendance date.
(Optional) You can click **Reset** to reset all the configured search conditions.
4. Click **Search** to start searching and the matched results will list on this page.
(Optional) Click **Report** to generate the attendance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

Attendance Details

Steps:

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



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

Abnormal Attendance

You can search and get the statistics of the abnormal attendance data, including No., name and department of the employees, abnormal type, start/end time and date of attendance. For detailed operations, refer to *7.13.4 Attendance Statistics*.

Overtime Search

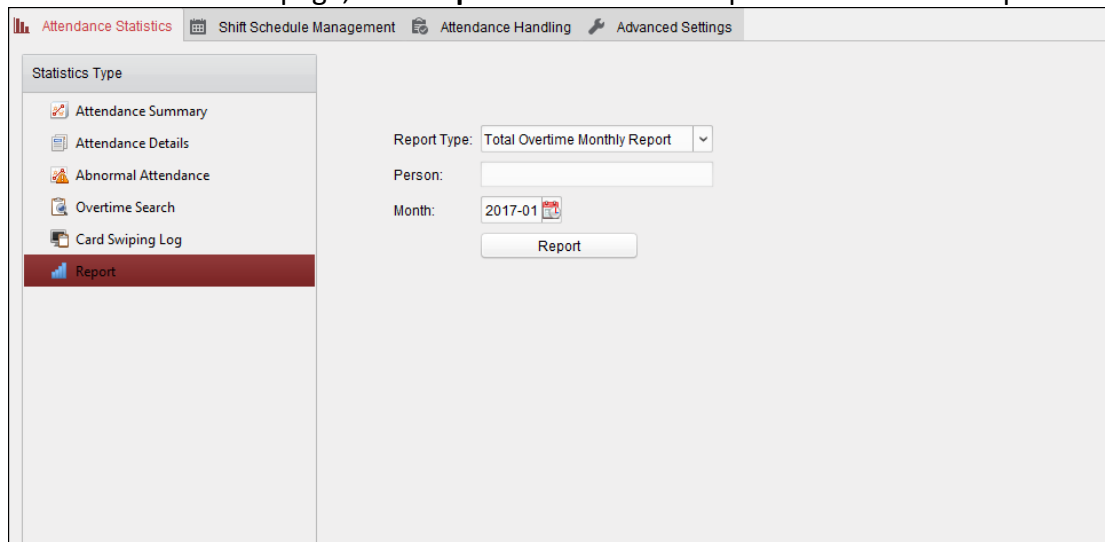
You can search and get the overtime status statistics of the selected employee in the specified time period. And you can check the detailed overtime information, including No., name and department of the employees, attendance date, overtime duration and overtime type. For detailed operations, refer to *7.13.4 Attendance Statistics*.

Card Swiping Log

You can search the card swiping logs used for the attendance statistics. After searching the logs, you can check the card swiping details, including name and department of the employees, card swiping time, card reader authentication mode and card No.. For detailed operations, refer to *7.13.4 Attendance Statistics*.

Report

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




➤ Generating Total Overtime Monthly Report

Steps:

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

Monthly Report as the report type.

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

➤ **Generating Overtime Details Monthly Report**


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


➤ **Generating Attendance Monthly Report**

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

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

Steps:

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

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

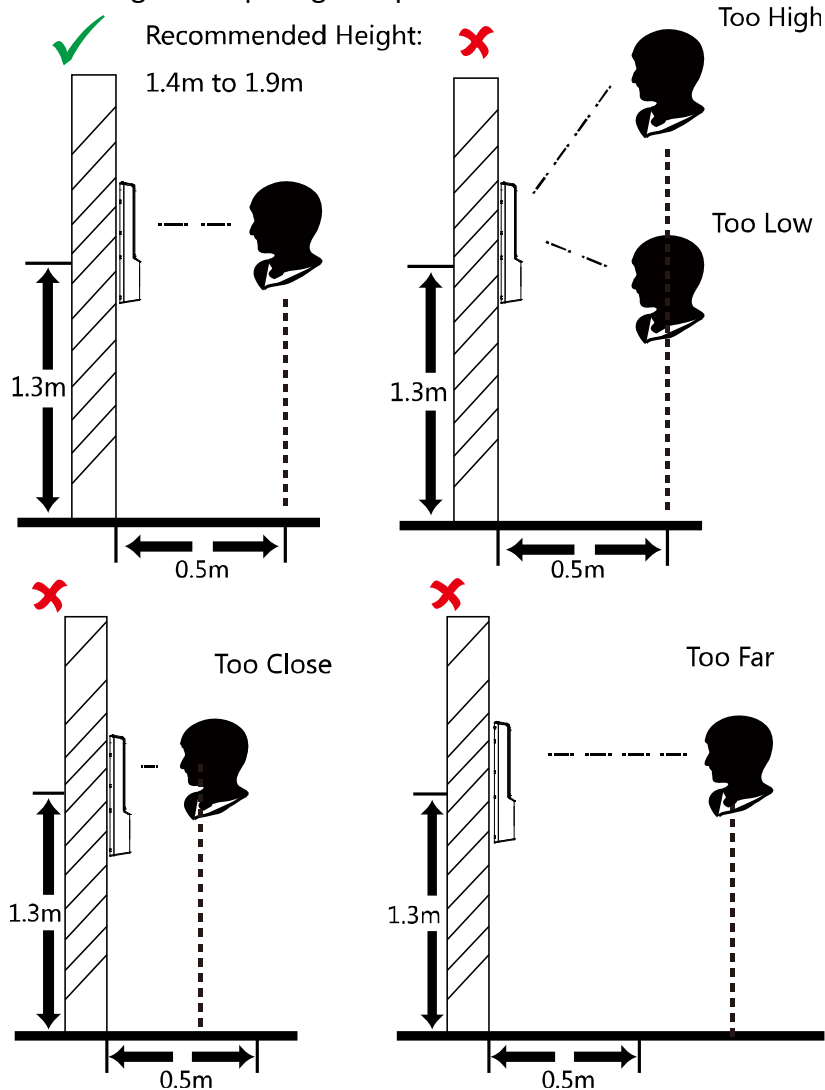
➤ **Generating Department Attendance Report**

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

Appendix A Tips When Collecting/Comparing Face Picture

A.1 Positions (Recommended Distance: 0.5m)

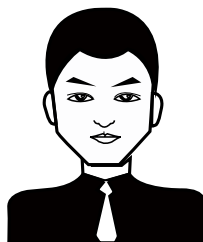
The position when collecting or comparing face picture is as below:



Note: For details about the relationship among person height, device height, and the distance between the person and the device, see Appendix C.

A.2 Expression

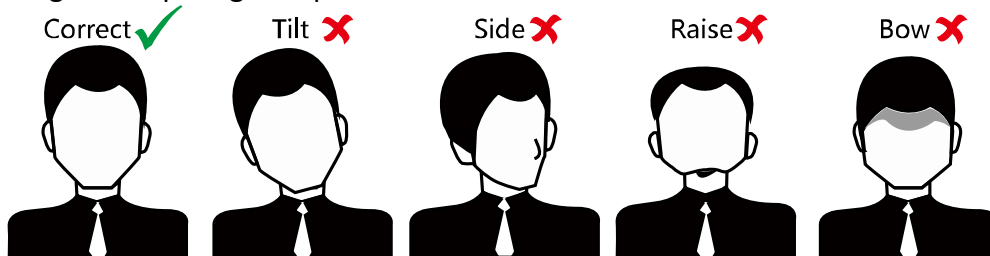
- Keep your expression naturally when collecting or comparing face pictures, just like the expression in the picture below.



- Do not wear hat, sunglasses, or other accessories that can affect the facial recognition function.
- Do not make your hair cover your eyes, ears, etc. and heavy makeup is not allowed.

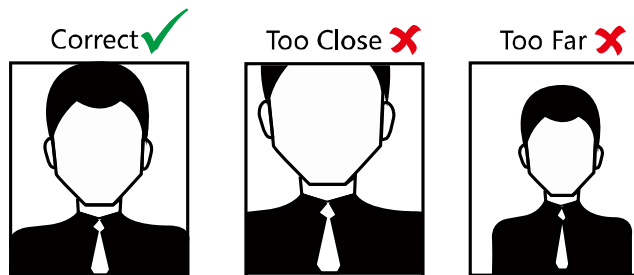
A.3 Posture

In order to get a good quality and accurate face picture, position your face looking at the camera when collecting or comparing face pictures.



A.4 Size

Make sure your face is in the middle of the collecting window.



010100001080711



See Far, Go Further