



## Face Recognition Terminal



# Legal Information

## User Manual

©2019 Hangzhou Hikvision Digital Technology Co., Ltd.

## 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.

Please use this user manual under the guidance of professionals.

## 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. HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

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

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

## Data Protection




During the use of device, personal data will be collected, stored and processed. To protect data, the development of Hikvision

devices incorporates privacy by design principles. For example, for device with facial recognition features, biometrics data is stored in your device with encryption method; for fingerprint device, only fingerprint template will be saved, which is impossible to reconstruct a fingerprint image.

As data controller, you are advised to collect, store, process and transfer data in accordance with the applicable data protection laws and regulations, including without limitation, conducting security controls to safeguard personal data, such as, implementing reasonable administrative and physical security controls, conduct periodic reviews and assessments of the effectiveness of your security controls.

# Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 <b>Danger</b>	Indicates a hazardous situation which, if not avoided, will or could result in death or serious injury.
 <b>Caution</b>	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
 <b>Note</b>	Provides additional information to emphasize or supplement important points of the main text.



# Contents

<b>1 Regulatory Information .....</b>	<b>1</b>
<b>2 Safety Instruction .....</b>	<b>2</b>
<b>3 Overview .....</b>	<b>3</b>
3.1 Overview .....	3
3.2 Features .....	4
<b>4 Appearance .....</b>	<b>4</b>
<b>5 Installation .....</b>	<b>6</b>
5.1 Installation Environment .....	6
5.2 Install with Gang Box .....	6
5.3 Install without Gang Box .....	8
<b>6 Wiring .....</b>	<b>10</b>
6.1 Terminal Description .....	10
6.2 Wire Device .....	12
6.3 Wire Secure Door Control Unit .....	13
<b>7 Activation .....</b>	<b>13</b>
7.1 Activate via Device .....	14
7.2 Activate via SADP .....	14
7.3 Activate Device via Client Software .....	15
<b>8 Basic Operation .....</b>	<b>16</b>
8.1 Login .....	16
8.2 Communication Settings .....	16
8.2.1 Set Network Parameters .....	16
8.2.2 Set Wi-Fi Parameters .....	17
8.2.3 Set RS-485 Parameters .....	17
8.2.4 Set Wiegand Parameters .....	18
8.3 User Management .....	18
8.3.1 Add Face Picture .....	18
8.3.2 Add Fingerprint .....	21

8.3.3 Add Card .....	22
8.3.4 Add Password .....	23
8.3.5 Set Authentication Mode .....	23
8.3.6 Search and Edit User .....	24
8.4 Import and Export Data .....	24
8.4.1 Export Data .....	24
8.4.2 Import Data .....	25
8.5 Time and Attendance Status Settings .....	26
8.5.1 Set Manual Attendance .....	26
8.5.2 Set Auto Attendance .....	26
8.5.3 Set Manual and Auto Attendance .....	27
8.5.4 Disable Attendance Mode .....	28
8.6 Identity Authentication .....	28
8.6.1 Authenticate via 1:1 Matching .....	29
8.6.2 Authenticate via Other Types .....	29
8.7 System Settings .....	29
8.7.1 Set Basic Parameters .....	29
8.7.2 Set Face Picture Parameters .....	31
8.7.3 Set Fingerprint Parameters .....	33
8.7.4 Set Time .....	33
8.8 Set Access Control Parameters .....	34
8.9 Maintenance .....	35
8.9.1 Reboot Device .....	35
8.9.2 Upgrade Firmware .....	35
8.9.3 Data Management .....	36
8.9.4 Log Query .....	38
8.9.5 Test .....	38
8.10 View System Information .....	39
<b>9 Client Software Configuration .....</b>	<b>41</b>
9.1 Person Management .....	41

9.1.1 Add Organization .....	41
9.1.2 Configure Basic Information .....	41
9.1.3 Issue a Card to One Person .....	42
9.1.4 Upload a Face Photo from Local PC .....	43
9.1.5 Take a Photo via Client .....	43
9.1.6 Collect Face via Access Control Device .....	44
9.1.7 Collect Fingerprint via Client .....	45
9.1.8 Collect Fingerprint via Access Control Device .....	45
9.1.9 Configure Access Control Information .....	46
9.1.10 Customize Person Information .....	47
9.1.11 Configure Resident Information .....	47
9.1.12 Configure Additional Information .....	48
9.1.13 Import and Export Person Identify Information .....	48
9.1.14 Import Person Information .....	48
9.1.15 Import Person Pictures .....	49
9.1.16 Export Person Information .....	50
9.1.17 Export Person Pictures .....	50
9.1.18 Get Person Information from Access Control Device .....	51
9.1.19 Move Persons to Another Organization .....	51
9.1.20 Issue Cards to Persons in Batch .....	51
9.1.21 Report Card Loss .....	52
9.1.22 Set Card Issuing Parameters .....	52
9.2 Configure Schedule and Template .....	53
9.2.1 Add Holiday .....	53
9.2.2 Add Template .....	54
9.3 Set Access Group to Assign Access Authorization to Persons .....	56
9.4 Configure Advanced Functions .....	57

9.4.1 Configure Device Parameters .....	57
9.4.2 Configure Remaining Open/Closed .....	63
9.4.3 Configure Multi-Factor Authentication .....	65
9.4.4 Configure Custom Wiegand Rule .....	67
9.4.5 Configure Card Reader Authentication Mode and Schedule .....	68
9.4.6 Configure First Person In .....	69
9.4.7 Configure Anti-Passback .....	70
9.4.8 Configure Multi-door Interlocking .....	70
9.4.9 Configure Other Parameters .....	71
9.5 Configure Linkage Actions for Access Control .....	77
9.5.1 Configure Client Actions for Access Event .....	77
9.5.2 Configure Device Actions for Access Event .....	78
9.5.3 Configure Device Actions for Card Swiping .....	79
9.5.4 Configure Device Linkage for Mobile Terminal's MAC Address .....	80
9.5.5 Configure Device Actions for Person ID .....	81
9.6 Door/Elevator Control .....	82
9.6.1 Control Door Status .....	83
9.6.2 Control Elevator Status .....	83
9.6.3 Check Real-Time Access Records .....	84
9.7 Time and Attendance .....	85
9.7.1 Configure Attendance Parameters .....	85
9.7.2 Add Timetable .....	90
9.7.3 Add Shift .....	91
9.7.4 Manage Shift Schedule .....	91
9.7.5 Manually Correct Check-in/out Record .....	94
9.7.6 Add Leave and Business Trip .....	95
9.7.7 Calculate Attendance Data .....	96

9.7.8 Attendance Statistics .....	97
<b>A. Tips for Scanning Fingerprint .....</b>	<b>100</b>
<b>B. Tips When Collecting/Comparing Face Picture .....</b>	<b>101</b>
<b>C. Tips for Installation Environment .....</b>	<b>103</b>
<b>D. Dimension .....</b>	<b>104</b>

# 1 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 EMC Directive 2014/30/EU, RE Directive 2014/53/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](http://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](http://www.recyclethis.info)

(1) 이 기기는 가정용으로 전자파적합등록을 한 기기로서 주거 지역에서는 물론 모든 지역에서 사용할 수 있습니다.

(2) 당해 무선설비는 전파혼신 가능성이 있으므로 인명안전과 관련된 서비스는 할 수 없음.

Model	Manufacturer	Standard
C2000IC12.0-24P-DE	MOSO Power Supply Technology Co., Ltd.	CEE
ADS-24S-12 1224GPG	Shenzhen Honor Electronic Co., Ltd.	CEE
C2000IC12.0-24P-GB	MOSO Power Supply Technology Co., Ltd.	BS

## 2 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 Dangers and Cautions:

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

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

⚠	⚠
<b>Dangers:</b> Follow these safeguards to prevent serious injury or death.	<b>Cautions:</b> Follow these precautions to prevent potential injury or material damage.

### ⚠ Danger:

- All the electronic operation should be strictly compliance with the electrical safety regulations, fire prevention regulations and other related regulations in your local region.
- Please use the power adapter, which is provided by normal company. The power consumption cannot be less than the required value.
- Do not connect several devices to one power adapter as adapter overload may cause over-heat or fire hazard.
- Please make sure that the power has been disconnected before you wire, install or dismantle the device.

- When the product is installed on wall or ceiling, the device shall be firmly fixed.
- If smoke, odors or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the device yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)

#### **⚠ Cautions:**

- Do not drop the device or subject it to physical shock, and do not expose it to high electromagnetism radiation. Avoid the equipment installation on vibrations surface or places subject to shock (ignorance can cause equipment damage).
- Do not place the device in extremely hot (refer to the specification of the device for the detailed operating temperature), cold, dusty or damp locations, and do not expose it to high electromagnetic radiation.
- The device cover for indoor use shall be kept from rain and moisture.
- Exposing the equipment to direct sun light, low ventilation or heat source such as heater or radiator is forbidden (ignorance can cause fire danger).
- Do not aim the device at the sun or extra bright places. A blooming or smear may occur otherwise (which is not a malfunction however), and affecting the endurance of sensor at the same time.
- Please use the provided glove when open up the device cover, avoid direct contact with the device cover, because the acidic sweat of the fingers may erode the surface coating of the device cover.
- Please use a soft and dry cloth when clean inside and outside surfaces of the device cover, do not use alkaline detergents.
- Please keep all wrappers after unpack them for future use. In case of any failure occurred, you need to return the device to the factory with the original wrapper. Transportation without the original wrapper may result in damage on the device and lead to additional costs.
- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.
- Biometric recognition products are not 100% applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.

## **3 Overview**

### **3.1 Overview**

Face recognition terminal is a kind of access control device for face recognition, which is mainly applied in security access



control systems, such as logistic centers, airports, university campuses, alarm centrals, dwellings and so on.

## 3.2 Features

- 5-inch LCD touch screen to display operation interface, etc.
- 2 MP wide-angle lens
- Face recognition distance: between 0.3 m and 1 m
- Deep learning algorithm
- Face capacity: 3200
- Max. 5,000 fingerprints storage



### Note

Some device models do not support fingerprint related functions.

---

- Multiple authentication modes



### Note

Some device models do support authenticating by fingerprint.

---

- Face recognition duration  $\leq 1$  s/User; face recognition accuracy rate  $> 99\%$
- Device parameters management, search, and settings
- Imports card and user data to the device via TCP/IP communication or USB flash drive
- Transmits data to the client software via TCP/IP communication
- Imports data to the device and exports the data from the device via USB flash drive
- Stand-alone operation
- Multiple languages supported: English, Thai, Spanish, and Arabic
- Supported attendance status: check in, check out, break out, break in, overtime in, and overtime out
- Connects to one external card reader via RS-485 protocol
- Connects to secure door control unit to avoid the door opening when the terminal is destroyed
- Connects to external access controller via RS-485 protocol and Wiegand protocol
- Voice prompt
- Watchdog design for protecting the device and ensuring device running properly

## 4 Appearance

You can view the device appearance introduction and their descriptions.

Refer to the following contents for detailed information of the face recognition terminal.

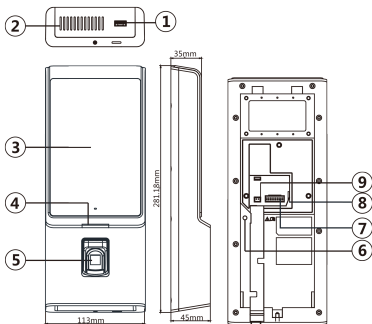




Figure 4-1 Appearance of Face Recognition Terminal

Table 4-1 Face Picture Parameters

No.	Name	Description
1	USB Interface	Plug in the USB flash drive and you can import or export the data.
2	Loudspeaker	The part that the sound comes from.
3	Display Screen	5-inch LCD touch screen with the resolution of 800 × 480 pixel.
4	Indicator	Solid Red: Standby.
		Flashing Red: Authentication failed.
		Solid Green: Authentication completed.
		Flashing Green: Authenticating (combined).
5	Fingerprint Module + Card Swiping Area	Scan fingerprint or swipe card.  <b>Note</b> Only the device without the fingerprint scanning function contains this part.

No.	Name	Description
	Card Swiping Area	Swipe card within this area.  <b>Note</b> Only the device with the fingerprint scanning function contains this part.
6	TAMPER	Tamper button
7	Wiring Terminals	Connect to other external devices, including RS-485 card reader, Wiegand card reader, door lock, alarm input, alarm output, etc.
8	Network Interface	Connect to Ethernet.
9	Power Interface	Connect to power supply.

## 5 Installation

### 5.1 Installation Environment

- Install the device at least 2 meters away from the light, and at least 3 meters away from the window or the door.
- Make sure the environment illumination is more than 100 Lux.

---

#### **Note**

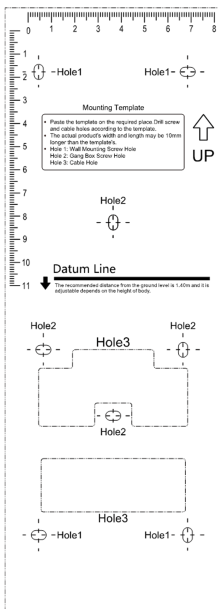
For details about installation environment, see *Tips for Installation Environment*.

---

### 5.2 Install with Gang Box

#### Steps

1. According to the datum line on the mounting template, stick the mounting template on the wall or other surface, 1.4 meters higher than the ground.



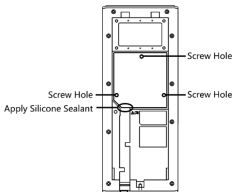
**Figure 5-1 Mounting Template**

2. Drill holes on the wall or other surface according to the mounting template and install the gang box (80 mm×80 mm).
3. Use two supplied screws to secure the mounting plate on the gang box.
4. Use another four supplied screws to secure the mounting plate on the wall.
5. Route the cables through the cable hole of the mounting plate, and connect to the corresponding external devices' cables.
6. Cover the interfaces with the supplied back sheet and secure the sheet with three screws.



**Note**

Apply Silicone sealant among the wiring hole to keep the raindrop from entering.



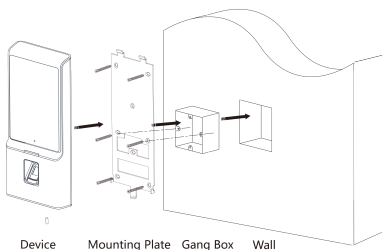
**Figure 5-2 Device Back Sheet**

7. Remove the screw at the bottom of the device.
8. Align the device with the mounting plate and buckle them together.

9. Use a hex wrench to fasten the screw at the bottom.

**Note**

- The installation height here is the recommended height. You can change it according to your actual needs.
- You can also install the device on the wall or other places without the gang box. For details, see *Installing without Gang Box*.
- For easy installation, drill holes on mounting surface according to the supplied mounting template.

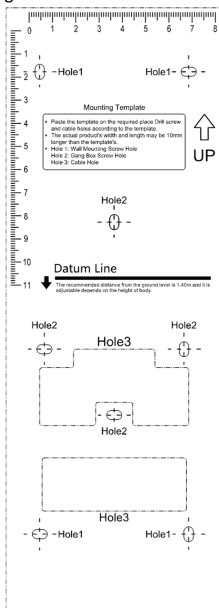


**Figure 5-3 Install with Gang Box**

## 5.3 Install without Gang Box

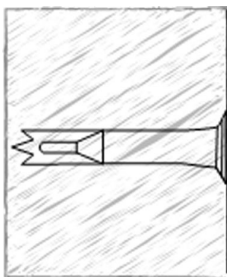
### Steps

1. According to the baseline on the mounting template, stick the mounting template on the wall or other surface, 1.4 meters higher than the ground.



**Figure 5-4 Mounting Template**

2. Drill 4 holes on the wall or other surface according to Hole 1 in the mounting template.
3. Insert the screw sockets of the setscrews in the drilled holes.



**Figure 5-5 Insert Screw Socket**

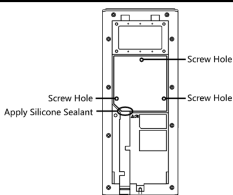
4. Align the 4 holes to the mounting plate with the drilled holes.
5. Route the cables through the cable hole of the mounting plate, and connect to the corresponding external devices' cables.
6. Cover the interfaces with the supplied back sheet and secure the sheet with three screws.



**Note**

Apply Silicone sealant among the wiring hole to keep the raindrop from entering.

---



**Figure 5-6 Device Back Sheet**

7. Fix and fasten the screws in the sockets on the wall or other surface.
8. Remove the screw at the bottom of the device.
9. Align the device with the mounting plate and buckle them together.
10. Use a hex wrench to fasten the screw at the bottom.



**Note**

- The installation height here is the recommended height. You can change it according to your actual needs.
  - You can also install the device on the wall or other places without the gang box. For details, see *Installing without Gang Box*.
  - For easy installation, drill holes on mounting surface according to the supplied mounting template.
-

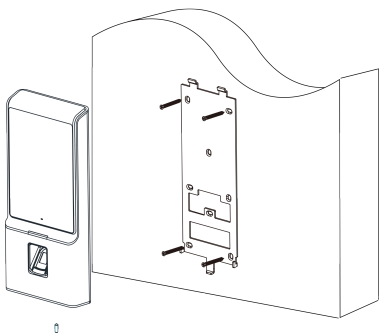


Figure 5-7 Install without Gang Box

## 6 Wiring

You can connect the RS-485 terminal with the RS-485 card reader, connect the DOOR terminal with the door lock, connect the BUT/GND terminal with the exit button, connect the ALARM OUT/ALRM IN terminal with the alarm output/input devices, and connect the WIEGAND terminal with the Wiegand card reader or the access controller. You can also connect the DS\_IN can with the power supply.

If connect the WIEGAND terminal with the access controller, the face recognition terminal can transmit the authentication information to the access controller and the access controller can judge whether to open the door or not.

---

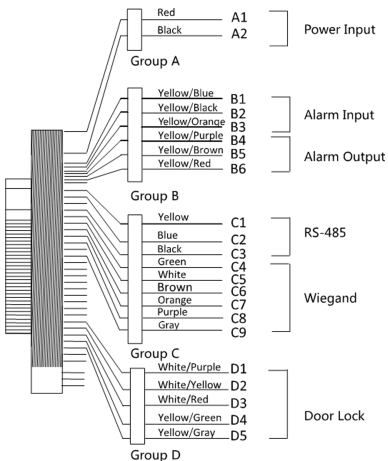
### Note

- If you use 1.0 mm cables, you should use a 12V switched-mode power supply. And the distance between the power supply and the device should be no more than 20 m.
  - If you use 1.5 mm cables, you should use a 12V switched-mode power supply. And the distance between the power supply and the device should be no more than 30 m.
  - If you use 2.0 mm cables, you should use a 12V switched-mode power supply. And the distance between the power supply and the device should be no more than 40 m.
- 

### 6.1 Terminal Description

The terminals contains power input, alarm input, alarm output, RS-485, Wiegand output, and door lock.

The terminal's diagram is as follows:



**Figure 6-1 Terminal Diagram**

The descriptions of the terminals are as follows:

**Table 6-1 Terminal Descriptions**

Group	No.	Function	Color	Name	Description
Group A	A1	Power Input	Red	+12 V	12 VDC Power Supply
	A2		Black	GND	Ground
Group B	B1	Alarm Input	Yellow/Blue	IN1	Alarm Input 1
	B2		Yellow/Black	GND	Ground
	B3		Yellow/Orange	IN2	Alarm Input 2
	B4	Alarm Output	Yellow/Purple	NC	Alarm Output Wiring
	B5		Yellow/Brown	COM	
	B6		Yellow/Red	NO	
Group C	C1	RS-485	Yellow	485+	RS-485 Wiring
	C2		Blue	485-	
	C3		Black	GND	Ground

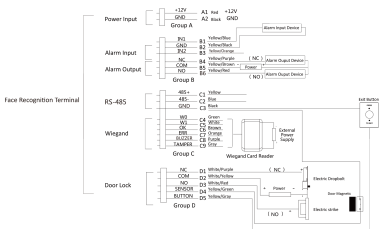


Group	No.	Function	Color	Name	Description
	C4	Wiegand	Green	W0	Wiegand Wiring 0
	C5		White	W1	Wiegand Wiring 1
	C6		Brown	WG_OK	Wiegand Authenticated
	C7		Orange	WG_ERR	Wiegand Authentication Failed
	C8		Purple	BUZZER	Buzzer Wiring
	C9		Gray	TAMPER	Tampering Alarm Wiring
Group D	D1	Door Lock	White/Purple	NC	Lock Wiring (NC)
	D2		White/Yellow	COM	Ground
	D3		White/Red	NO	Lock Wiring (NO)
	D4		Yellow/Green	SENSOR	Door Magnetic Sensor
	D5		Yellow/Gray	BUTTON	Exit Door Wiring

## 6.2 Wire Device

You can connect the terminal with peripherals.

The wiring diagram without secure door control unit is as follows.



**Figure 6-2 Device Wiring**

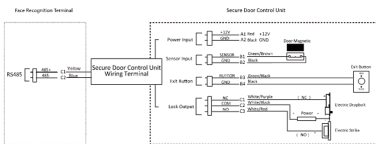


**Note**

- You should set the face recognition terminal's Wiegand direction to "Input" to connect to a Wiegand card reader. If connects to an access controller, you should set the Wiegand direction to "Output" to transmit authentication information to the access controller.
- For details about Wiegand direction settings, see *Setting Wiegand Parameters in Communication Settings*.
- The Min. power cable's diameter: 18 AWG.
- The power cable's rated current is 3 A, while other cable's rated current is 1 A.

### 6.3 Wire Secure Door Control Unit

You can connect the terminal with the secure door control unit. The wiring diagram is as follows.



**Figure 6-3 Secure Door Control Unit Wiring**



**Note**

The secure door control unit should connect to an external power supply separately.

## 7 Activation

You should activate the device before the first login. After powering on the device, the system will switch to Device Activation page.

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

The default values of the device are as follows:

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

## 7.1 Activate via Device

If the device is not activated, you can activate the device after it is powered on.

On the Activate Device page, create a password and confirm the password. Tap Next and the device will be activated.

---



### Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: 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.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

---

## 7.2 Activate via SADP

SADP is a tool to detect, activate and modify the IP address of the device over the LAN.

### Before You Start

- Get the SADP software from the supplied disk or the official website <http://www.hikvision.com/en/>, and install the SADP according to the prompts.
- The device and the PC that runs the SADP tool should be within the same subnet.

The following steps show how to activate a device and modify its IP address. For batch activation and IP addresses modification, refer to *User Manual of SADP* for details.

### Steps

1. Run the SADP software and search the online devices.
  2. Find and select your device in online device list.
  3. Input new password (admin password) and confirm the password.
- 

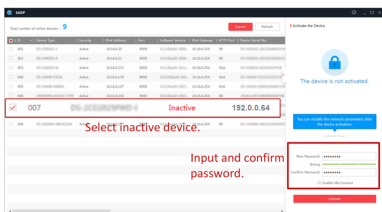


### Caution

**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 start activation.



Status of the device becomes Active after successful activation.

## 5. Modify IP address of the device.

- 1) Select the device.
- 2) Change the device IP address to the same subnet as your computer by either modifying the IP address manually or checking Enable DHCP.
- 3) Input the admin password and click Modify to activate your IP address modification.


## 7.3 Activate Device via Client Software

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

### Steps

#### Note

This function should be supported by the device.

1. Enter the Device Management page.
2. Click  on the right of **Device Management** and select Device.
3. Click Online Device to show the online device area.  
The searched online devices are displayed in the list.
4. Check the device status (shown on Security Level column) and select an inactive device.
5. Click Activate to open the Activation dialog.
6. Create a password in the password field, and confirm the password.

#### Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: 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.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

7. Click OK to activate the device.

# 8 Basic Operation

## 8.1 Login

You should enter the system backend first before setting the device parameters.

### First Login

If it is the first time to login, follow the descriptions below to login.

Tap the settings icon at the lower right corner of the initial page and enter the device activation password on the Input Password page. Tap OK to enter the home page.

### Administrator Login

If you have set the administrator on the User Management page, follow the steps below to login.

Tap the settings icon at the lower right corner of the initial page. Select a login type. Follow the instructions and authenticate the permissions to enter the home page.

---

#### Note

- The device will be locked for 30 minutes after 5 failed password attempts.
  - For details about setting the administrator authentication mode, see *Adding User*.
- 

## 8.2 Communication Settings

You can set the network parameters, the Wi-Fi parameter, the RS-485 parameters, and the Wiegand parameters on the communication settings page.

### 8.2.1 Set Network Parameters

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

#### Steps

1. Tap Comm. (Communication Settings) on the Home page to enter the Communication Settings page.
2. On the Communication Settings page, tap Network to enter the Network tab.

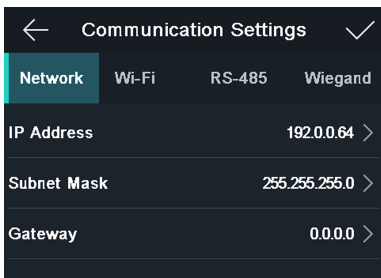


Figure 8-1 Network Settings

3. Tap IP Address, Subnet Mask, or Gateway and input the parameters.
4. Tap OK to save the settings.



#### Note

The device's IP address and the computer IP address should be in the same IP segment.

---

5. Tap  to save the network parameters.

## 8.2.2 Set Wi-Fi Parameters

You can enable the Wi-Fi function and set the Wi-Fi related parameters.

### Steps

1. Tap Comm. (Communication Settings) on the Home page to enter the Communication Settings page.
2. On the Communication Settings page, tap Wi-Fi to enter the Wi-Fi tab.

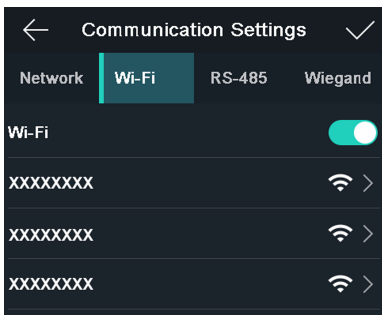


Figure 8-2 Wi-Fi Settings

3. Enable the Wi-Fi function.
4. Select a Wi-Fi in the list to enter the Wi-Fi parameters settings page.
5. Select an IP mode.
  - If selecting Static, you should input the Wi-Fi password, IP address, subnet mask and gateway.
  - If selecting Dynamic, you should input the Wi-Fi password.



#### Note

Numbers, upper case letters, lower case letters, and special characters are allowed in the Wi-Fi password.

---

6. Tap OK to save the settings and go back to the Wi-Fi tab.
7. Tap  to save the network parameters.

## 8.2.3 Set RS-485 Parameters

The face recognition terminal can connect external device, including access controller, secure door control unit or card reader via the RS-485 terminal.

### Steps

1. Tap Comm. (Communication Settings) on the Home page to enter the Communication Settings page.


2. On the Communication Settings page, tap RS-485 to enter the RS-485 tab.
3. Select an external device according to your actual needs.

---

 **Note**

Unit represents the secure door control unit and Reader represents the card reader.

---

4. Tap  to save the network parameters.

---

 **Note**

If you change the external device, and after you save the device parameters, the device will reboot automatically.

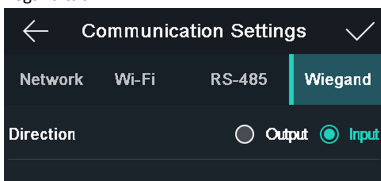
---

## 8.2.4 Set Wiegand Parameters


You can set the Wiegand transmission direction and the Wiegand mode.

### Steps

1. Tap Comm. (Communication Settings) on the Home page to enter the Communication Settings page.
2. On the Communication Settings page, tap Wiegand to enter the Wiegand tab.



**Figure 8-3 Wiegand Settings**

3. Select the transmission direction and its mode.
  - Output: A face recognition terminal can connect an external access controller. And the two devices will transmit the card No. via Wiegand 26 or Wiegand 34 mode.
  - Input: A face recognition terminal can connect a Wiegand card reader. And there is no need to set the Wiegand mode.
4. Tap  to save the network parameters.

---

 **Note**

If you change the external device, and after you save the device parameters, the device will reboot automatically.

---

## 8.3 User Management

On the user management interface, you can add, edit, delete and search the user.

---

 **Note**

Up to 5000 users can be added.

---

### 8.3.1 Add Face Picture

Add user's face picture to the device. And the user can use the face picture to authenticate.

## Steps

1. Tap User + to enter the Add User page.
2. Edit the employee ID.



### Note

- The employee ID should be between 1 and 999999999.
  - The employee ID should not start with 0 and should not be duplicated.
- 

3. Tap the Name field and input the user name on the soft keyboard.

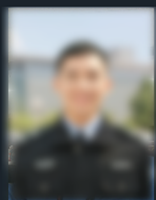


### Note

- Numbers, upper case letters, lower case letters, and special characters are allowed in the user name.
  - Up to 32 characters are allowed in the user name.
- 

4. Tap the Face Picture field to enter the face picture adding page.





Saved

Save

Try Again

Time



4

Figure 8-4 Add Face Picture

5. Position your face looking at the camera.



**Note**

- Make sure your face picture is in the face picture outline when adding the face picture.
- Make sure the captured face picture is in good quality and is accurate.
- For details about the instructions of adding face pictures, see *Tips When Collecting/Comparing Face Picture*.

After completely adding the face picture, a captured face picture will be displayed at the upper right corner of the page.

6. Tap Save to save the face picture.
7. **Optional:** Tap Try Again and adjust your face position to add the face picture again.

---

 **Note**

The maximum duration for adding a face picture is 15s. You can check the remaining time for adding a face picture on the left of the page.

---

8. Enable or disable the Administrator Permission function.

**Enable Administrator Permission**

The user is the administrator. Except for the normal attendance function, the user can also enter the Home page to operate after authenticating the permission.

**Disable Administrator Permission**

The User is the normal user. The user can only authenticate or take attendance on the initial page.

9. **Optional:** Tap the Schedule Template field, select a schedule template and save the settings.

10. Tap  to save the settings.

### 8.3.2 Add Fingerprint

Add a fingerprint for the user and the user can authenticate via the added fingerprint.

**Steps**

1. Tap User + to enter the Add User page.
2. Tap the Employee ID. field and edit the employee ID.

---

 **Note**

- The employee ID should be between 1 and 99999999.
  - The employee ID should not start with 0 and should not be duplicated.
- 

3. Tap the Name field and input the user name on the soft keyboard.

---

 **Note**

- Numbers, upper case letters, lower case letters, and special characters are allowed in the user name.
  - Up to 32 characters are allowed in the user name.
- 

4. Tap the Fingerprint field to enter the Add Fingerprint page.
5. Place your finger on the fingerprint module. And follow the instructions on the screen to record the fingerprint.
6. After adding the fingerprint completely, tap Yes on the pop-up dialog to save the fingerprint and continue to add another fingerprint.
7. **Optional:** Tap No to save the fingerprint and go back to the Add User page.

---

 **Note**

- The same fingerprint cannot be repeatedly added.
- Up to 10 fingerprints can be added for one user.
- You can also use the client software or the fingerprint recorder to record fingerprints.

For details about the instructions of scanning fingerprints, see *Tips for Scanning Fingerprint*.

---

8. Enable or disable the Administrator Permission function.

#### **Enable Administrator Permission**

The user is the administrator. Except for the normal attendance function, the user can also enter the Home page to operate after authenticating the permission.

#### **Disable Administrator Permission**

The User is the normal user. The user can only authenticate or take attendance on the initial page.

9. **Optional:** Tap the Schedule Template field, select a schedule template and save the settings.
10. Tap  to save the settings.

### **8.3.3 Add Card**

Add a card for the user and the user can authenticate via the added card.

#### **Steps**

1. Tap User + to enter the Add User page.
2. Tap the Employee ID. field and edit the employee ID.



#### **Note**

- The employee ID should be between 1 and 999999999.
  - The employee ID should not start with 0 and should not be duplicated.
- 

3. Tap the Name field and input the user name on the soft keyboard.



#### **Note**

- Numbers, upper case letters, lower case letters, and special characters are allowed in the user name.
  - Up to 32 characters are allowed in the user name.
- 

4. Tap the Card field and input the card No.
5. Configure the card No.
  - Enter the card No. manually.
  - Swipe the card over the card swiping area to get the card No.



#### **Note**

- The card No. cannot be empty.
  - Up to 20 characters are allowed in the card No.
  - By default, the card No. contains 10 characters. The system will use 0 to supplement the 10-character-card No. For example, 5 and 0000000005 are two different card No.
  - The card No. cannot be duplicated.
- 

6. **Optional:** Enable the Duress Card function. The added card  
When the user authenticates by swiping this duress card, the device will upload an duress card event to the client software.
7. Enable or disable the Administrator Permission function.

### Enable Administrator Permission

The user is the administrator. Except for the normal attendance function, the user can also enter the Home page to operate after authenticating the permission.

### Disable Administrator Permission

The User is the normal user. The user can only authenticate or take attendance on the initial page.

**8. Optional:** Tap the Schedule Template field, select a schedule template and save the settings.

9. Tap  to save the settings.

## 8.3.4 Add Password

Add a password for the user and the user can authenticate via the password.

### Steps

1. Tap User + to enter the Add User page.

2. Tap the Employee ID. field and edit the employee ID.

---

#### Note

- The employee ID should be between 1 and 99999999.
  - The employee ID should not start with 0 and should not be duplicated.
- 

3. Tap the Name field and input the user name on the soft keyboard.

---

#### Note

- Numbers, upper case letters, lower case letters, and special characters are allowed in the user name.
  - Up to 32 characters are allowed in the user name.
- 

4. Tap the Password field and create a password and confirm the password.

---

#### Note

- Only numbers are allowed in the password.
  - Up to 8 characters are allowed in the password.
- 

5. Enable or disable the Administrator Permission function.

### Enable Administrator Permission

The user is the administrator. Except for the normal attendance function, the user can also enter the Home page to operate after authenticating the permission.

### Disable Administrator Permission

The User is the normal user. The user can only authenticate or take attendance on the initial page.

**6. Optional:** Tap the Schedule Template field, select a schedule template and save the settings.

7. Tap  to save the settings.

## 8.3.5 Set Authentication Mode

After adding the user's fingerprint, face picture, password, or other credentials, you should set the authentication mode and

the user can authenticate his/her identity via the configured authentication mode.

#### Steps

1. On the Add User or Edit User page, tap Authentication Mode to enter the Authentication Mode page.
2. Select Device or Custom as the authentication mode.

##### Device

If you want to select device mode, you should set the terminal authentication mode in Access Control Settings page first. For details see *Setting Access Control Parameters*.

##### Custom



You can combine different authentication modes together according to your actual needs.

3. Tap  to save the settings.


### 8.3.6 Search and Edit User

After adding the user, you can search the user and edit it.

#### Search User

On the User Management page, Tap  to enter the Search User page. Tap Card on the left of the page and select a search type from the drop-down list. Enter the employee ID, card No., or the user name for search. Tap  to search.

#### Edit User

On the User Management page, select a user from the user list to enter the Edit User page. Follow the steps in *Add User* to edit the user parameters. Tap  to save the settings.

---

#### Note

The employee ID cannot be edited.

---

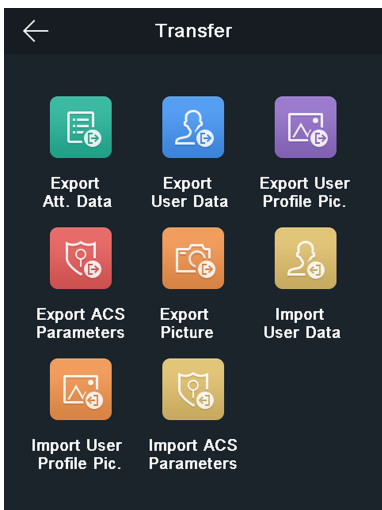
### 8.4 Import and Export Data

On the Transfer page, you can export the attendance data, the user data, the user picture, the access control parameter, and the captured picture to the USB flash drive. You can also import the user data, the user picture, and the access control parameter from the USB flash drive.

#### 8.4.1 Export Data

##### Steps

1. Tap Transfer on the Home page to enter the Transfer page.



**Figure 8-5 Transfer Page**

2. On the Transfer page, tap Export Att. Data, Export User Data, Export User Profile Pic., Export ACS Parameters, or Export Picture (Export Captured Picture).
3. Tap Yes on the pop-up page and the data will be exported from the device to the USB flash drive.



**Note**

- The supported USB flash drive format is FAT 32.
- The system supports the USB flash drive with the storage of 1G to 32G. Make sure the free space of the USB flash drive is more than 512M.
- The exported user data is a BIN file, which cannot be edited.

## 8.4.2 Import Data

### Steps

1. Plug a USB flash drive in the device.
2. On the Transfer page, tap Import User Data, Import User Profile Pic., or Import ACS Parameters.
3. Tap Yes on the pop-up window and the data will be imported from the USB flash drive to the device.
  - If you want to transfer all user information from one device (Device A) to another (Device B), you should export the information from Device A to the USB flash drive and then import from the USB flash drive to Device B. In this case, you should import the user data before importing the profile photo.
  - The supported USB flash drive format is FAT 32.
  - The imported picture should be saved in the root directory (enroll\_pic) and the picture file's name should be follow the rule below:  
Card No.\_Name\_Department\_Employee ID\_Gender.jpg

- The employee ID should be between 1 and 999999999, should not be duplicated, and should not start with 0.
- Requirements of face picture: It should be taken in full-face view, directly facing the camera. Do not wear a hat or head covering when taking the face picture. The format should be JPEG or JPG. The resolution should be more than 640 × 480 pixel and less than 2160 × 3840 pixel. The picture size should be between 40 KB and 200 KB.

## 8.5 Time and Attendance Status Settings

Set time and attendance status. You can set the attendance mode as check in, check out, break out, break in, overtime in, and over according to your actual situation.

### Note

The function should be used cooperatively with time and attendance function on the client software.

### 8.5.1 Set Manual Attendance

Set the attendance mode as manual, and you can select a status manually when you take attendance.

#### Before You Start

Add at least one user, and set the user's authentication mode. For details, see *User Management*.

#### Steps

1. Tap T&A Status to enter the T&A Status page.
2. Set the **Attendance Mode** as Manual.

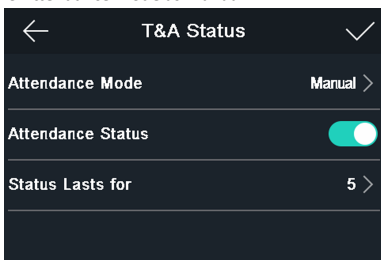


Figure 8-6 Manual Mode

3. Enable the **Attendance Status** function.

#### Result

When you authenticate on the initial page, you will enter the Select Status page. Select a status to take attendance.

### Note

If you do not select a status, the authentication will be failed and it will not be marked as a valid attendance.

### 8.5.2 Set Auto Attendance

Set the attendance mode as auto, and you can set the attendance status and its available schedule. The system will auto change the attendance status according to the configured parameters.

## Before You Start

Add at least one user, and set the user's authentication mode. For details, see *User Management*.

## Steps

1. Tap T&A Status to enter the T&A Status page.
2. Set the **Attendance Mode** as Auto.

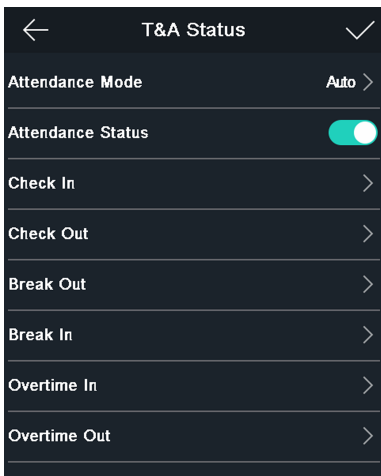


Figure 8-7 Auto Mode

3. Select an attendance status and set its schedule.



### Note

The attendance status will be valid within the configured schedule. For example, if set the break out's schedule as Monday 11:00, and break in's schedule as Monday 12:00, the valid user's authentication from Monday 11:00 to 12:00 will be marked as break.

---

## Result

When you authenticate on the initial page, the authentication will be marked as the configured attendance status according to the configured schedule.

## 8.5.3 Set Manual and Auto Attendance

Set the attendance mode as manual and auto and the system will auto change the attendance status according to the configured parameters. At the same time you can manually change the attendance status after the authentication.

## Before You Start

Add at least one user, and set the user's authentication mode. For details, see *User Management*.

## Steps

1. Tap T&A Status to enter the T&A Status page.
2. Set the **Attendance Mode** as Manual and Auto.



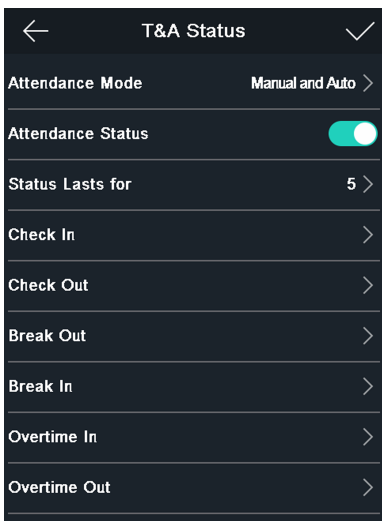


Figure 8-8 Manual and Auto Mode

3. Select an attendance status and set its schedule.



**Note**

The attendance status will be valid within the configured schedule. For example, if set the break out's schedule as Monday 11:00, and break in's schedule as Monday 12:00, the valid user's authentication from Monday 11:00 to 12:00 will be marked as break.

**Result**

Enter the initial page and authenticate. If you do not select a status, the authentication will be marked as the configured attendance status according to the schedule. If you tap Select Status and select a status to take attendance, the authentication will be marked as the selected attendance status.

### 8.5.4 Disable Attendance Mode

Disable the attendance mode and the system will not display the attendance status on the initial page.

Tap T&A Status to enter the T&A Status page.

Set the **Attendance Mode** as Disable.

You will not view or configure the attendance status on the initial page. And the system will follow the attendance rule that configured on the platform.

## 8.6 Identity Authentication

After network configuration, system parameters configuration and user configuration, 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.

### 1:N Matching

Compare the captured face picture or the collected fingerprint picture with all face pictures or all fingerprint pictures stored in the device.

### 1: 1 Matching


When swiping card, compare the captured face picture or the collected fingerprint with the information stored in the card.

## 8.6.1 Authenticate via 1:1 Matching

### Steps

1. On the Initial page, tap 1:1 at the lower right corner of the page to enter the 1:1 matching page.
2. Input the employee ID.
3. Select an authentication type to authenticate via face picture, fingerprint, or password.



Tap  to switch to the password entering page. You can enter the super password or duress code to authenticate.

---

## 8.6.2 Authenticate via Other Types

### Steps

1. According to the configured authentication mode, authenticate by comparing face pictures, fingerprints or by swiping card.

#### Face Picture Authentication

Stand in front of the device. Position your face looking at the camera and the device will enter the face picture authentication mode.



For detailed information about authenticating face picture, see *Tips When Collecting/Comparing Face Picture*.

---

#### Fingerprint Picture Authentication

Scan your fingerprint on the fingerprint module of the device. For detailed information about scanning fingerprint, see *Tips for Scanning Fingerprint*.

#### Authentication by Swiping Card

Swipe card above the card swiping area.

2. If the user has no other authentication modes, the authentication is completed. If the user has other authentication modes after the first authentication, follow the instructions to continue authenticating until the authentication is completed.

## 8.7 System Settings

On the System Settings page, you can set the system basic parameters, set the fingerprint parameters, set the face picture parameters, and upgrade the firmware.

### 8.7.1 Set Basic Parameters

You can set the device ID, time format, keyboard sound, voice prompt, voice volume, application mode, power saving mode, auto enable supplement light, brightness, and language.

On the Home page, tap System (System Settings) to enter the System Settings page.

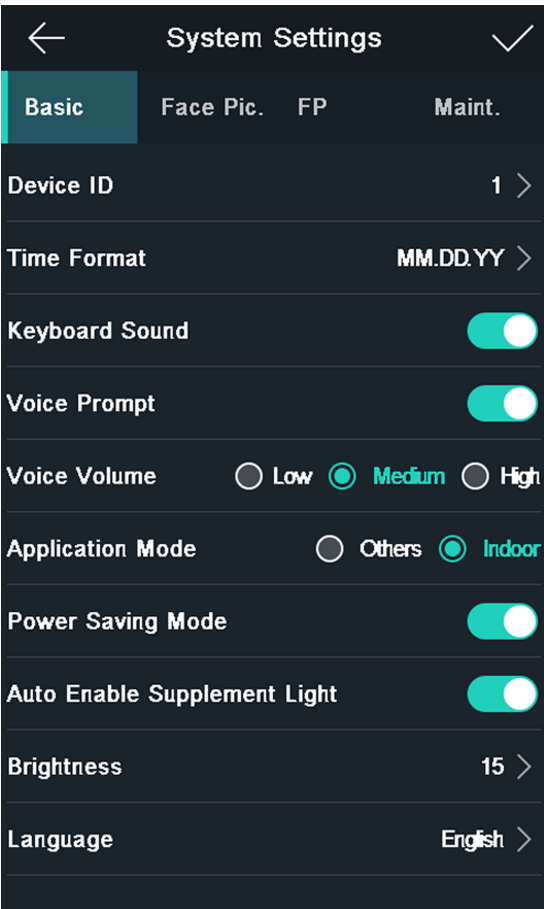





Figure 8-9 Basic Parameters

Table 8-1 Face Picture Parameters

Parameter	Description
Device ID	Set the face recognition terminal's device ID No. The device ID is the DIP address for the communication between the device and the access controller if the device should connect to an access controller via RS-485 protocol.

Parameter	Description
	 <b>Note</b> The device ID should be numbers and should range from 0 to 255.
Time Format	You can select one of the following formats: MM/DD/YYYY, MM.DD.YYYY, DD-MM-YYYY, DD/MM/YYYY, DD.MM.YYYY, YYYYMMDD, YY-MM-DD, YY/MM/DD, and MM-DD-YYYY.
Keyboard Sound	Tap <input type="checkbox"/> or <input checked="" type="checkbox"/> to disable or enable the keyboard sound.
Voice Prompt	Tap <input type="checkbox"/> or <input checked="" type="checkbox"/> to disable or enable the voice prompt.
Voice Volume	Adjust the voice volume. The larger the value, the louder the volume.
Application Mode	You can select either others or indoor according to actual environment.
Power Saving Mode	You can enable the power saving mode to save the power consumptions.
Auto Enable Supplement Light	<p>If enabling the function, when the device detects persons in the front, the supplement light will be automatically turned on. If not, the supplement light will be turned off automatically.</p>  <b>Note</b> The distance between the person and the device should be less than 1.3 m, or the supplement light will not turned on automatically.
Brightness	<p>You can set the supplement light's brightness. The brightness ranges from 0 to 100.</p> <p>0 refers to the supplement light is turned off. 1 refers to the darkest light, and 100 refers to the brightest light.</p>
Language	<p>Change the system language. English, Thai, Spanish, and Arabic are available.</p>  <b>Note</b> The system will auto reboot after you change the language.

## 8.7.2 Set Face Picture Parameters

You can set the face picture 1:N security level, 1:1 security level, liveness security level, face recognition interval, duplicated person, live face detection.

On the Home page, tap System (System Settings) to enter the System Settings page.

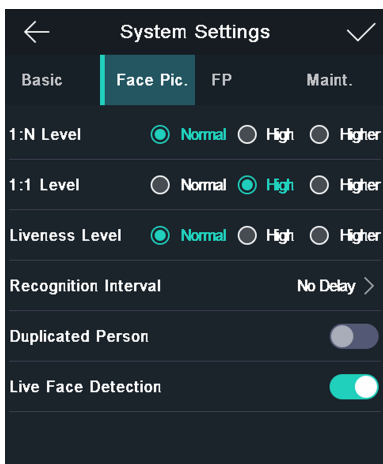



Figure 8-10 Face Picture Parameters

Table 8-2 Face Picture Parameters

Parameter	Description
1:N Level	Set the matching security level when authenticating via 1:N matching mode.
1:1 Level	Set the matching security level when authenticating via 1:1 matching mode.
Liveness Level	After enabling Live Face Detection function, you can set the matching security level when performing live face authentication.
Recognition Interval	<p>The time interval between two continuous face recognitions when authenticating. By default, it is 2s.</p> <p> <b>Note</b></p> <p>You can input the number from 1 to 10 or 255. 255 refers to infinite.</p>
Duplicated Person	If enabling the function, the system will compare the adding face picture with all pictures in the database when adding a

Parameter	Description
	user. If the person already exists in the database, the system will remind you.
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.

### 8.7.3 Set Fingerprint Parameters

You can set the fingerprint security level in this section.

#### Note

Some device models do not support the fingerprint related functions.

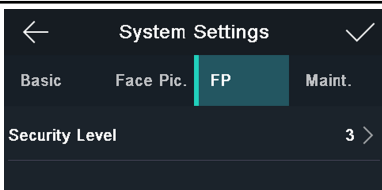


Figure 8-11 Fingerprint Parameters

#### Security Level

You can select the fingerprint security level.

The higher is the security level, the lower is the false acceptance rate (FAR).

The higher is the security level, the higher is the false rejection rate (FRR).

### 8.7.4 Set Time

You can set the device time and the DST in this section.

Tap Time (Time Settings) on the Home page to enter the Time Settings page. Edit the time parameters and tap  to save the settings.

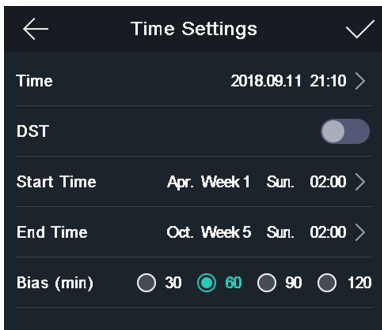



Figure 8-12 Time Parameters

## 8.8 Set Access Control Parameters

You can set the access control permissions, including the functions of authentication mode, door magnetic sensor, anti-passback, lock locked time, door open timeout alarm, etc.

On the Home page, tap ACS (Access Control Settings) to enter the Access Control Settings page. Edit the access control parameters on this page and tap  to save the settings.

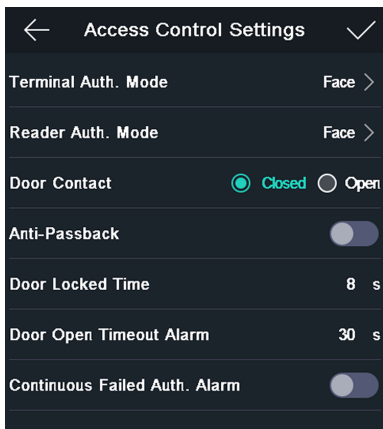



Figure 8-13 Access Control Parameters

The available parameters descriptions are as follows:

Table 8-3 Access Control Parameters Descriptions

Parameter	Description
Terminal Auth. Mode (Terminal Authentication Mode)	<p>Select the face recognition terminal's authentication mode. You can also customize the authentication mode.</p> <p> <b>Note</b></p> <ul style="list-style-type: none"><li>• Only the device with the fingerprint module supports the fingerprint related function.</li><li>• Biometric recognition products are not 100% applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.</li><li>• If you adopt multiple authentication modes, you should authenticate other</li></ul>

Parameter	Description
	methods before authenticating face.
Reader Auth. Mode (Card Reader Authentication Mode)	Select the card reader's authentication mode.
Door Contact	You can select "Open" or "Closed" according to your actual needs. By default, it is Closed.
Anti-Passback	When enabling the anti-passback function, you should set the anti-password path in the client software. The person should authenticate according to the configured path. Or the authentication will be failed.
Door Locked Time	Set the door unlocking duration. If the door is not opened for the set time, the door will be locked. Available door locked time range: 1 to 255s.
Door Open Timeout Alarm	The alarm can be triggered if the door has not been closed. Available range: 0 to 255s.
Continuous Failed Auth. Alarm	When you enable the function, you can set the maximum authentication times. If you failed to authenticate for the set times, the alarm will be triggered. Available range: 1 to 10.

## 8.9 Maintenance

### 8.9.1 Reboot Device

On the System Settings page, tap Maint. (Maintenance) to enter the Maintenance page and tap Reboot. The device starts rebooting.

### 8.9.2 Upgrade Firmware

Plug in the USB flash drive. Tap Maint. (Maintenance) on the System Settings page and tap Upgrade. The device will automatically read the upgrading file in the USB flash drive and upgrade the firmware.





## Note

- Do not power off during the device upgrade.
- The upgrading file should be in the root directory.
- The upgrading file name should be digicap.dav.

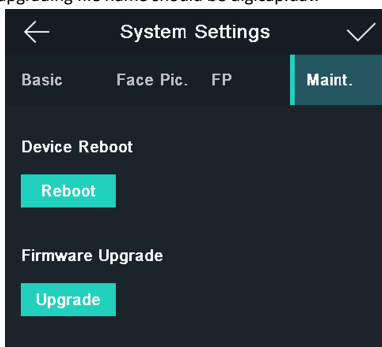


Figure 8-14 Upgrade

---

### 8.9.3 Data Management

On the Data Management page, you can delete all events, delete user data, delete all data, clear permission, delete captured pictures, restore to factory settings, or restore to default settings.

Tap Data (Data Management) to enter the Data Management page. Tap the button on the page to manage the data. Tap Yes on the pop-up window to complete the settings.

The available button descriptions are as follows:



## Data Management



**Delete  
All Events**



**Delete  
User Data**



**Delete  
All Data**



**Clear  
Permission**



**Delete  
Captured Pic.**



**Restore to  
Factory**



**Restore to  
Default**

**Figure 8-15 Data Management**

**Table 8-4 Data Descriptions**

<b>Parameters</b>	<b>Description</b>
Delete All Events	Delete all events stored in the device.
Clear Permission	Clear the administrator's permission but the administrator and the related logs will not be deleted.
Delete User Data	Delete all user data in the device.
Delete Captured Pic.	Delete the device captured pictured.

Parameters	Description
Restore to Factory	Restore the system to the factory settings. The device will reboot after the setting.
Restore to Default	Restore the system to the default settings. The system will save the communication settings and the remote user settings. Other parameters will be restored to default.

### 8.9.4 Log Query

You can search the authentication logs within a period of time by inputting employee ID, card No., or user name.

#### Steps

1. On the Home page, tap Log (Log) to enter the Log page.

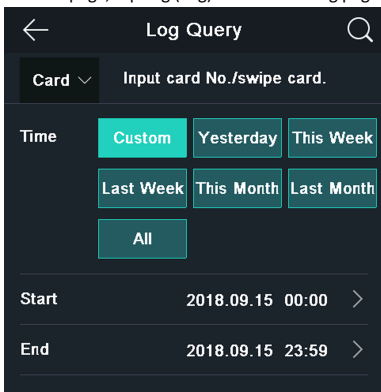


Figure 8-16 Log Query

2. Tap Card on the left of the page and select a search type from the drop-down list.
3. Tap the input box and input the employee ID, the card No., or the user name for search.
4. Select a time.



#### Note

You can select from Custom, Yesterday, This Week, Last Week, This Month, Last Month, or All. If you select Custom, you can customize the start time and the end time for search.

5. Tap to start search.

The result will be displayed on the page.

### 8.9.5 Test

You can test the capability of the device's face detection function, voice prompt function, fingerprint authentication function, time, and button.

Tap Test on the Home page to enter the Automatic Test page.

**Note**

Some device models do not support fingerprint authentication function.

---

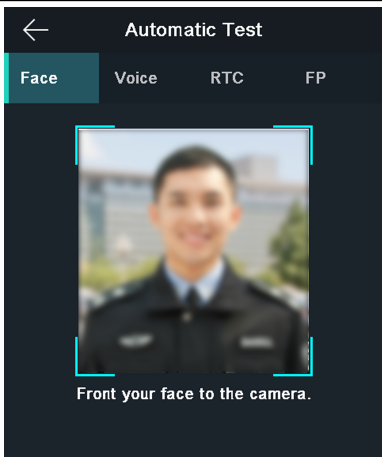


Figure 8-17 Test

## 8.10 View System Information

View device capacity, device information, and the open source software license.

### View Capacity

You can view the added user's number, the face picture's number, the card's number, the password's number, and the fingerprint's number.

**Note**

Some device models do not support displaying the fingerprint capacity.

---

Tap Info. (System Information) Capacity on the Home page to enter the Capacity page.





## System Information

### Capacity

### Device

### License

Admin:	0		Used	
User:	1		Total	
Used:	0	1	0	3
Total:	3200	5000	5000	100000

Face

Card

PWD

Event

FP

Figure 8-18 Capacity

### View Device Information

You can view the device information.

Tap Info. (System Information) Device to enter the Device page.



#### Note

Some device models do not support displaying the fingerprint information.

### Open Source License

View the Open Source License information.

Tap Info. (System Information) License to enter the Open Source Software Licenses page.

# 9 Client Software Configuration

## 9.1 Person Management

You can add person information to the system for further operations such as access control, video intercom, time and attendance, etc. You can manage the added persons such as issuing cards to them in a batch, importing and exporting person information in a batch, etc.

### 9.1.1 Add Organization

You can add an organization and import person information to the organization for effective management of the persons. You can also add a subordinate organization for the added one.

#### Steps

1. Enter Person module.
2. Select a parent organization in the left column and click Add in the upper-left corner to add an organization.
3. Create a name for the added organization.





#### Note

Up to 10 levels of organizations can be added.

---

4. **Optional:** Perform the following operation(s).

<b>Edit Organization</b>	Hover the mouse on an added organization and click  to edit its name.
--------------------------	--

<b>Delete Organization</b>	Hover the mouse on an added organization and click  to delete it.
----------------------------	--

---



#### Note

- 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.
- 

<b>Show Persons in Sub Organization</b>	Check Show Persons in Sub Organization and select an organization to show persons in its sub organizations.
---	---

### 9.1.2 Configure Basic Information

You can add person to the client software one by one and configure the person's basic information such as name, gender, phone number, etc.

#### Steps

1. Enter Person module.
2. Select an organization in the organization list to add the person.
3. Click Add to open the adding person window.

The Person ID will be generated automatically.

4. Enter the basic information including person name, gender, tel, email address, etc.
5. **Optional:** Set the effective period of the person. Once expired, the credentials and access control settings of the person will be invalid and the person will have no authorization to access the doors\floors.

#### Example

For example, if the person is a visitor, his/her effective period may be short and temporary.

6. Confirm to add the person.
  - Click Add to add the person and close the Add Person window.
  - Click Add and New to add the person and continue to add other persons.

### 9.1.3 Issue a Card to One Person

When adding person, you can issue a card with a unique card number to the person as a credential. After issued, the person can access the doors which he/she is authorized to access by swiping the card on the card reader.

#### Steps

---

#### Note

Up to five cards can be issued to one person.

---

1. Enter Person module.
  2. Select an organization in the organization list to add the person and click Add.
- 

#### Note

Enter the person's basic information first. For details about configuring person's basic information, refer to **Configure Basic Information**.

---

3. In the Credential Card panel, click +.
  4. Enter the card number.
    - Enter the card number manually.
    - Place the card on the card enrollment station or card reader and click Read to get the card number. The card number will display in the Card No. field automatically.
- 

#### Note

You need to click Settings to set the card issuing mode and related parameters first. For details, refer to **Set Card Issuing Parameters**.

---

5. Select the card type according to actual needs.

#### Normal Card

The card is used for opening doors for normal usage.

#### Duress Card

When the person is under duress, he/she can swipe the duress card to open the door. The door will be unlocked and the client will receive a duress event to notify the security personnel.

#### Patrol Card

This card is used for the inspection staff to check the their attendance of inspection. By swiping the card on the specified card reader, the person is marked as on duty of inspection at that time.

### Dismiss Card

By swiping the card on the card reader, it can stop the buzzing of the card reader.

#### 6. Click Add.

The card will be issued to the person.

#### 7. Confirm to add the person.

- Click Add to add the person and close the Add Person window.
- Click Add and New to add the person and continue to add other persons.

## 9.1.4 Upload a Face Photo from Local PC

When adding person, you can upload a face photo stored in local PC to the client as the person's profile.

### Steps

#### 1. Enter Person module.

#### 2. Select an organization in the organization list to add the person and click Add.



#### Note

Enter the person's basic information first. For details about configuring person's basic information, refer to **Configure Basic Information**.

---

#### 3. Click Add Face in the Basic Information panel.

#### 4. Select Upload.

#### 5. Select a picture from the PC running the client.



#### Note

The picture should be in JPG or JPEG format and smaller than 200 KB.

---

#### 6. **Optional:** Enable Verify by Device to check whether the facial recognition device managed in the client can recognize the face in the photo.

#### 7. Confirm to add the person.

- Click Add to add the person and close the Add Person window.
- Click Add and New to add the person and continue to add other persons .

## 9.1.5 Take a Photo via Client

When adding person, you can take a photo of the person by the webcam of the PC running the client and set this photo as the person's profile.

### Steps

#### 1. Enter Person module.

#### 2. Select an organization in the organization list to add the person and click Add.







## Note

Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information***.

---

3. Click Add Face in the Basic Information panel.
4. Select Take Photo.
5. Connect the face scanner to the PC running the client.
6. **Optional:** Enable Verify by Device to check whether the facial recognition device managed in the client can recognize the face in the photo.
7. Take a photo.
  - 1) Face to the webcam of the PC and make sure your face is in the middle of the collecting window.
  - 2) Click  to capture a face photo.
  - 3) **Optional:** Click  to capture again.
  - 4) Click OK to save the captured photo.
8. Confirm to add the person.
  - Click Add to add the person and close the Add Person window.
  - Click Add and New to add the person and continue to add other persons.

### 9.1.6 Collect Face via Access Control Device

When adding person, you can collect the person's face via access control device added to the client which supports facial recognition function.

#### Steps


1. Enter Person module.
2. Select an organization in the organization list to add the person and click Add.



## Note

Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information***.

---

3. Click Add Face in the Basic Information panel.
4. Select Remote Collection.
5. Select an access control device which supports face recognition function from the drop-down list.
6. Collect face.
  - 1) Face to the camera of the selected access control device and make sure your face is in the middle of the collecting window.
  - 2) Click  to capture a photo.
  - 3) Click OK to save the captured photo.
7. Confirm to add the person.
  - Click Add to add the person and close the Add Person window.
  - Click Add and New to add the person and continue to add other persons .

## 9.1.7 Collect Fingerprint via Client

Collecting fingerprints locally means you can collect the fingerprint via the fingerprint recorder connected directly to the PC running the client. The fingerprints recorded can be used as credentials of the persons to access the authorized doors.

### Before You Start

Connect the fingerprint recorder to the PC running the client.

### Steps

1. Enter Person module.
2. Select an organization in the organization list to add the person and click Add.



#### Note

Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information***.

---

3. In the Credential Fingerprint panel, click +.
4. In the pop-up window, select the collection mode as Local.
5. Select the model of the connected fingerprint recorder.



#### Note

If the fingerprint recorder is DS-K1F800-F, you can click Settings to select the COM the fingerprint recorder connects to.

---

6. Collect the fingerprint.
  - 1) Click Start.
  - 2) Place and lift your fingerprint on the fingerprint recorder to collect the fingerprint.
  - 3) Click Add to save the recorded fingerprint.
7. Confirm to add the person.
  - Click Add to add the person and close the Add Person window.
  - Click Add and New to add the person and continue to add other persons.

## 9.1.8 Collect Fingerprint via Access Control Device

When adding person, you can collect fingerprint information via the access control device's fingerprint module. The fingerprints recorded can be used as credentials of the persons to access the authorized doors.

### Before You Start

Make sure fingerprint collection is supported by the access control device.

### Steps

1. Enter Person module.
2. Select an organization in the organization list to add the person and click Add.



#### Note

Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information***.

---

3. In the Credential Fingerprint panel, click +.
4. In the pop-up window, select the collection mode as Remote.
5. Select an access control device which supports fingerprint recognition function from the drop-down list.
6. Collect the fingerprint.
  - 1) Click Start.
  - 2) Place and lift your fingerprint on the fingerprint scanner of the selected access control device to collect the fingerprint.
  - 3) Click Add to save the recorded fingerprint.
7. Confirm to add the person.
  - Click Add to add the person and close the Add Person window.
  - Click Add and New to add the person and continue to add other persons .

### 9.1.9 Configure Access Control Information

When adding a person, you can set her/his access control properties, such as setting the person as visitor or as blacklist person, or as super user who has super authorization.

#### Steps

1. Enter Person module.
2. Select an organization in the organization list to add the person and click Add.



#### Note

Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information***.

---

3. In the Access Control panel, set the person's access control properties.

#### PIN Code

The PIN code must be used after card or fingerprint when accessing. It cannot be used independently. It should contain 4 to 8 digits.

#### Super User

If the person is set as a super user, he/she will have authorization to access all the doors/floors and will be exempted from remaining closed restrictions, all anti-passback rules, and first person authorization.

#### Extended Door Open Time

When the person accessing door, grant this person more time to pass through doors which have been configured with extended open duration. Use this function for the persons with reduced mobility.

For details about setting the door's open duration, refer to ***Configure Parameters for Door/Elevator***.

#### Add to Blacklist

Add the person to the blacklist and when the person tries to access doors/floors, an event will be triggered and send to the client to notify the security personnel.

#### Mark as Visitor

If the person is a visitor, set the maximum times of authentications, including access by card and fingerprint to limit the visitor's access times.

---

 **Note**

The maximum times of authentications should be between 1 and 100.

---

### Device Operator

For person with device operator role, he/she is authorized to operate on the access control devices.

---

 **Note**

The Super User, Extended Door Open Time, Add to Blacklist, and Mark as Visitor functions cannot be enabled concurrently. For example, if one person is set as super user, you cannot enable extended door open time for her/him, add her/him to the blacklist, or set her/him as visitor.

---

#### 4. Confirm to add the person.

- Click Add to add the person and close the Add Person window.
- Click Add and New to add the person and continue to add other persons.

### 9.1.10 Customize Person Information

You can customize the person properties which are not pre-defined in the client according to actual needs, e.g., place of birth. After customizing, when add a person, you can enter the custom information to make the person information complete.

#### Steps

1. Enter Person module.

2. Set the fields of custom information.

- 1) Click Custom Property.
- 2) Click Add to add a new property.
- 3) Enter the property name.
- 4) Click OK.

3. Set the custom information when adding a person.

- 1) Select an organization in the organization list to add the person and click Add.
- 

 **Note**

Enter the person's basic information first. For details about configuring person's basic information, refer to **Configure Basic Information**.

---

- 2) In the Custom Information panel, enter the person information.
- 3) Click Add to add the person and close the Add Person window, or click Add and New to add the person and continue to add other persons.

### 9.1.11 Configure Resident Information

If the person is resident, for video intercom purpose, you need to set the room number for her/him and bind an indoor station.

After bound, you can call this person by calling the indoor station and perform video intercom with her/him.

#### Steps

1. Enter Person module.
2. Select an organization in the organization list to add the person and click Add.



#### Note

Enter the person's basic information first. For details about configuring person's basic information, refer to **Configure Basic Information**.

---

3. In the Resident Information panel, select the indoor station to link it to the person.



#### Note

If you select Analog Indoor Station, the Door Station field will display and you are required to select the door station to communicate with the analog indoor station.

---

4. Enter the floor No. and room No. of the person.
5. Confirm to add the person.
  - Click Add to add the person and close the Add Person window.
  - Click Add and New to add the person and continue to add other persons.

### 9.1.12 Configure Additional Information

When adding person, you can configure the additional information for the person, such as person's identity type, identity No., country, etc., according to actual needs.

#### Steps

1. Enter Person module.
2. Select an organization in the organization list to add the person and click Add.



#### Note

Enter the person's basic information first. For details about configuring person's basic information, refer to **Configure Basic Information**.

---

3. In the Additional Information panel, enter the additional information of the person, including person's ID type, ID No., job title, etc., according to actual needs.
4. Confirm to add the person.
  - Click Add to add the person and close the Add Person window.
  - Click Add and New to add the person and continue to add other persons.

### 9.1.13 Import and Export Person Identify Information

You can import the information and pictures of multiple persons to the client software in a batch. Meanwhile, you can also export the person information and pictures and save them in your PC.

### 9.1.14 Import Person Information

You can enter the information of multiple persons in a predefined template (a CSV file) to import the information to the client in a batch.


### Steps

1. Enter the Person module.
2. Select an added organization in the list, or click Add in the upper-left corner to add an organization and then select it.
3. Click Import to open the Import panel.
4. Select Person Information as the importing mode.
5. Click Download Template for Importing Person to download the template.
6. Enter the person information in the downloaded template.



#### Note

- If the person has multiple cards, separate the card No. with semicolon.
- Items with asterisk are required.
- By default, the Hire Date is the current date.

- 
7. Click  to select the CSV file with person information.
  8. Click Import to start importing.



#### Note

- If a person No. already exists in the client's database, delete the existing information before importing.
  - You can import information of no more than 10,000 persons.
- 


## 9.1.15 Import Person Pictures

After importing face pictures for the added persons to the client, the persons in the pictures can be identified by an added face recognition terminal. You can either import person pictures one by one, or import multiple pictures at a time according to your need.

### Before You Start

Be sure to have imported person information to the client beforehand.

### Steps

1. Enter the Person module.
2. Select an added organization in the list, or click Add in the upper-left corner to add an organization and then select it.
3. Click Import to open the Import panel and check Face.
4. **Optional:** Enable Verify by Device to check whether face recognition device managed in the client can recognize the face in the photo.
5. Click  to select a face picture file.

---

 **Note**

- The (folder of) face pictures should be in ZIP format.
  - Each picture file should be in JPG format and should be no larger than 200 KB.
  - Each picture file should be named as "Person ID\_Name". The Person ID should be the same with that of the imported person information.
- 

6. Click Import to start importing.

The importing progress and result will be displayed.

### 9.1.16 Export Person Information

You can export the added persons' information to local PC as a CSV file.

#### Before You Start

Make sure you have added persons to an organization.

#### Steps

1. Enter the Person module.
  2. **Optional:** Select an organization in the list.
- 

 **Note**

All persons' information will be exported if you do not select any organization.

---

3. Click Export to open the Export panel and check Person Information as the content to export.
4. Check desired items to export.
5. Click Export to save the exported CSV file in your PC.

### 9.1.17 Export Person Pictures

You can export face picture file of the added persons and save in your PC.

#### Before You Start

Make sure you have added persons and their face pictures to an organization.

#### Steps

1. Enter the Person module.
  2. **Optional:** Select an organization in the list.
- 

 **Note**

All persons' face pictures will be exported if you do not select any organization.

---

3. Click Export to open the Export panel and check Face as the content to export.
  4. Click Export to start exporting.
- 

 **Note**

- The exported file is in ZIP format.
  - The exported face picture is named as "Person ID\_Name\_0" ("0" is for a full-frontal face).
-

## 9.1.18 Get Person Information from Access Control Device

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

### Steps

---



#### Note

- 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.
  - If the card number or person ID (employee ID) stored on the device already exists in the client database, the person with this card number or person ID will not be imported to the client.
- 

1. Enter Person module.
2. Select an organization to import the persons.
3. Click Get from Device.
4. Select the access control device from the drop-down list.
5. Click Get to start importing the person information to the client.

The person information, including person details, person's fingerprint information (if configured), and the linked cards (if configured), will be imported to the selected organization.

## 9.1.19 Move Persons to Another Organization

You can move the added persons to another organization if you need.

### Before You Start

- Make sure you have added at least two organizations.
- Make sure you have imported person information.

### Steps

1. Enter Person module.
2. Select an organization in the left panel.  
The persons under the organization will be displayed in the right panel.
3. Select the person to move.
4. Click Change Organization.
5. Select the organization to move persons to.
6. Click OK.

## 9.1.20 Issue Cards to Persons in Batch

The client provides a convenient way to issue cards to multiple persons in a batch.

### Steps

1. Enter Person module.
2. Click Batch Issue Cards.



All the added persons with no card issued will display.

3. Set the card issuing parameters. For details, refer to **Set Card Issuing Parameters**.
4. Click Initialize to initialize the card enrollment station or card reader to make it ready for issuing cards.
5. Click the card number column and enter the card number.
  - Place the card on the card enrollment station.
  - Swipe the card on the card reader.
  - Enter the card number manually and press Enter key on your keyboard.


The card number will be read automatically and the card will be issued to the person in the list.

6. Repeat the above step to issue the cards to the persons in the list in sequence.


### 9.1.21 Report Card Loss

If the person lost his/her card, you can report the card loss so that the card's related access authorization will be inactive.

#### Steps

1. Enter Person module.
2. Select the person you want to report card loss for and click Edit to open the Edit Person window.
3. In the Credential Card panel, click  on the added card to set this card as lost card.

After reporting card loss, the access authorization of this card will be invalid and inactive. Other person who gets this card cannot access the doors by swiping this lost card.

4. **Optional:** If the lost card is found, you can click  to cancel the loss.

After cancelling card loss, the access authorization of the person will be valid and active.

5. If the lost card is added in one access group and the access group is applied to the device already, after reporting card loss or cancelling card loss, a window will pop up to notify you to apply the changes to the device. After applying to device, these changes can take effect on the device.

### 9.1.22 Set Card Issuing Parameters

The client provides two modes for reading a card's number: via card enrollment station or via the card reader of the access control device. If a card enrollment station is available, connect it to the PC running the client by USB interface or COM, and place the card on the card enrollment to read the card number. If not, you can also swipe the card on the card reader of the added access control device to get the card number. As a result, before issuing a card to one person, you need to set the card issuing parameters including the issuing mode and related parameters.

When adding a card to one person, click Settings to open the Card Issuing Settings window.

#### Local Mode: Issue Card by Card Enrollment Station

Connect a card enrollment station to the PC running the client. You can place the card on the card enrollment station to get the card number.

## Card Enrollment Station

Select the model of the connected card enrollment station

---

### Note

Currently, the supported card enrollment station models include DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E, and DS-K1F180-D8E.

---

## Card Type

This field is only available when the model is DS-K1F100-D8E or DS-K1F180-D8E.

Select the card type as EM card or IC card according to the actual card type.

## Serial Port

It is only available when the model is DS-K1F100-M.

Select the COM the card enrollment station connects to.

## Buzzing

Enable or disable the buzzing when the card number is read successfully.

## Card No. Type

Select the type of the card number according to actual needs.

## M1 Card Encryption

This field is only available when the model is DS-K1F100-D8, DS-K1F100-D8E, or DS-K1F180-D8E.

If the card is M1 card, and if you need to enable the M1 Card Encryption function, you should enable this function and select the sector of the card to encrypt.

## Remote Mode: Issue Card by Card Reader

Select an access control device added in the client and swipe the card on its card reader to read the card number.

## 9.2 Configure Schedule and Template

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

---

### Note

For access group settings, refer to *Set Access Group to Assign Access Authorization to Persons*.

---

### 9.2.1 Add Holiday

You can create holidays and set the days in the holidays, including start date, end date, and holiday duration in one day.

Perform this task when you need to add a holiday to pre-define the holidays.

#### Steps

---

### Note

You can add up to 64 holidays in the software system.

---

1. Click Access Control Template Holiday to enter the Holiday page.
2. Click Add on the left panel.
3. Create a name for the holiday.
4. **Optional:** Enter the descriptions or some notifications of this holiday in the Remark box.
5. Add a holiday period to the holiday list and configure the holiday duration.



#### Note

Up to 16 holiday periods can be added to one holiday.

---

- 1) Click Add in the Holiday List field.
- 2) Drag the cursor to draw the time duration, which means in that duration of time, the configured access group is activated.




#### Note


Up to 8 time durations can be set to one holiday period.




---

- 3) **Optional:** Perform the following operations to edit the time durations.

Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to .

Click the time duration and directly edit the start/end time in the appeared dialog.

Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to .

- 4) **Optional:** Select the time duration(s) that need to be deleted, and then click  in the Operation column to delete the selected time duration(s).
- 5) **Optional:** Click  in the Operation column to clear all the time duration(s) in the time bar.
- 6) **Optional:** Click  in the Operation column to delete this added holiday period from the holiday list.

6. Click Save.

## 9.2.2 Add Template

Template includes week schedule and holiday. You can set week schedule and assign the time duration of access authorization for different person or group. You can also select the added holiday(s) for the template.

Perform this task if you want to add and configure template.

### Steps

---



#### Note

You can add up to 255 templates in the software system.

---

1. Click Access Control Template Template to enter the Template page.

---

 **Note**

There are two default templates: All-Day Authorized and All-Day Denied, and they cannot be edited or deleted.

**All-Day Authorized**

The access authorization is valid in each day of the week and it has no holiday.

**All-Day Denied**

The access authorization is invalid in each day of the week and it has no holiday.

---


2. Click Add on the left panel to create a new template.
  3. Create a name for the template.
  4. Enter the descriptions or some notification of this template in the Remark box.
  5. Edit the week schedule to apply it to the template.
    - 1) Click Week Schedule tab on the lower panel.
    - 2) Select a day of the week and draw time duration(s) on the timeline bar.
- 

 **Note**


Up to 8 time duration(s) can be set for each day in the week schedule.

---

- 3) **Optional:** Perform the following operations to edit the time durations.

**Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to .**

**Click the time duration and directly edit the start/end time in the appeared dialog.**

**Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to .**
  - 4) Repeat the two steps above to draw more time durations on the other days of the week.
6. Add a holiday to apply it to the template.
- 

 **Note**

Up to 4 holidays can be added to one template.


---

- 1) Click Holiday tab.
  - 2) Select a holiday in the left list and it will be added to the selected list on the right panel.
  - 3) **Optional:** Click Add to add a new holiday.
- 

 **Note**

For details about adding a holiday, refer to **Add Holiday**.

---

- 4) **Optional:** Select a selected holiday in the right list and click  to remove the selected one, or click Clear to clear all the selected holiday(s) in the right list.
7. Click Save to save the settings and finish adding the template.

## 9.3 Set Access Group to Assign Access Authorization to Persons

After adding the person and configuring the person's credentials, you can create the access groups to define which person(s) can get access to which door(s) and then apply the access group to the access control device to take effect.

Perform this task if you need to assign access group to persons.

### Steps

- For one person, you can add up to 4 access groups to one access control point of one device.
  - You can add up to 128 access groups in total.
  - When the access group settings are changed, you need to apply the access groups to the devices again to take effect. The access group changes include changes of template, access group settings, person's access group settings, and related person details (including card number, fingerprint, face picture, linkage between card number and fingerprint, linkage between card number and fingerprint, card password, card effective period, etc).
1. Click Access Control Access Group to enter the Access Group interface.
  2. Click Add to open the Add window.
  3. In the Name text field, create a name for the access group as you want.
  4. Select a template for the access group.



#### Note

You should configure the template before access group settings. Refer to ***Configure Schedule and Template*** for details.

---

5. In the left list of the Select Person field, select person(s) and the person(s) will be added to the selected list .
6. In the left list of the Select Door field, select door(s) or door station(s) for the selected persons to access, and the selected door(s) or door station(s) will be added to the selected list.
7. Click OK.
8. After adding the access groups, you need to apply them to the access control device to take effect.
  - 1) Select the access group(s) to apply to the access control device.

To select multiple access groups, you can hold the Ctrl or Shift key and select access groups.
  - 2) Click Apply All to start applying all the selected access group(s) to the access control device or door station.




#### Caution

- Be careful to click Apply All, since this operation will clear all the access groups of the selected devices and then apply the new access group, which may brings risk to the devices.
  - You can click Apply Changes to only apply the changed part of the selected access group(s) to the device(s).
-

3) View the apply status in the Status column or click Applying Statusto view all the applied access group(s).

The selected persons in the applied access groups will have the authorization to enter/exit the selected doors/door stations with their linked card(s) or fingerprints.


**9. Optional:** Click  to edit the access group if necessary.

## 9.4 Configure Advanced Functions

You can configure the advanced functions of access control to meet some special requirements in different scene, such as multi-factor authentication, anti-passback, etc.

---

### Note

- For the card related functions(the type of access control card/ multi-factor authentication), only the card(s) with access group applied will be listed when adding cards.
  - The advanced functions should be supported by the device.
  - Hover the cursor on the Advanced Function, and then Click  to customize the advanced function(s) to be displayed.
- 

### 9.4.1 Configure Device Parameters

After adding the access control device, you can configure the parameters of access control device (access controller), access control points (door or floor), alarm inputs, alarm outputs, card readers and lane controller.


#### Configure Parameters for Access Control Device

After adding the access control device, you can configure its parameters, including overlaying user information on picture, uploading pictures after capturing, saving captured pictures, etc.

#### Steps

1. Click Access Control Advanced Function Device Parameter .
- 

### Note

If you can find Device Parameter in the Advanced Function list, Hover the cursor on the Advanced Function, and then Click  to select the Device Parameter to be displayed.

---

2. Select an access device to show its parameters on the right page.
  3. Turn the switch to ON to enable the corresponding functions.
- 

### Note

- The displayed parameters may vary for different access control devices.
  - Some of the following parameters are not listed in the Basic Information page, click More to edit the parameters.
- 

#### RS-485 Comm. Redundancy

You should enable this function if you wire the RS-485 card reader to the access control device redundantly.

#### Display Detected Face

Display face picture when authenticating.

#### Display Card Number

Display the card information when authenticating.

### **Display Person Information**

Display the person information when authenticating.

### **Overlay Person Info. on Picture**

Display the person information on the captured picture.

### **Voice Prompt**

If you enable this function, the voice prompt is enabled in the device. You can hear the voice prompt when operating in the device.

### **Upload Pic. After Linked Capture**

Upload the pictures captured by linked camera to the system automatically.

### **Save Pic. After Linked Capture**

If you enable this function, you can save the picture captured by linked camera to the device.

### **Press Key to Enter Card Number**

If you enable this function, you can input the card No. by pressing the key.

### **Wi-Fi Probe**

If you enable this function, the device can probe the surrounding communication devices' MAC address and upload the MAC address to the system. If the MAC address match the specified MAC address, the system can trigger some linkage actions.

### **3G/4G**


If you enable this function, the device can communicate in 3G/4G network.

4. Click OK.
5. **Optional:** Click Copy to, and then select the access control device(s) to copy the parameters in the page to the selected device(s).

## **Configure Parameters for Door/Elevator**

After adding the access control device, you can configure its access point (door or floor) parameters.

### **Steps**

1. Click Access Control Advanced Function Device Parameter .
2. Select an access control device on the left panel, and then click  to show the doors or floors of the selected device.
3. Select a door or floor to show its parameters on the right page.
4. Edit the door or floor parameters.



### **Note**

- The displayed parameters may vary for different access control devices.
- Some of the following parameters are not listed in the Basic Information page, click More to edit the parameters.

---

### **Name**

Edit the card reader name as desired.

## Door Contact

You can set the door sensor as remaining closed or remaining open. Usually, it is remaining closed.

## Exit Button Type

You can set the exit button as remaining closed or remaining open. Usually, it is remaining open.

## Door Locked Time

After swiping the normal card and relay action, the timer for locking the door starts working.

## Extended Open Duration

The door contact can be enabled with appropriate delay after person with extended access needs swipes her/his card.

## Door Open Timeout Alarm

The alarm can be triggered if the door has not been closed in a configured time period. If it is set as 0, no alarm will be triggered.

## Lock Door when Door Closed

The door can be locked once it is closed even if the **Door Locked Time** is not reached.

## Duress Code

The door can open by inputting the duress code when there is duress. At the same time, the client can report the duress event.

## Super Password

The specific person can open the door by inputting the super password.

## Dismiss Code

Create a dismiss code which can be used to stop the buzzer of the card reader (by entering the dismiss code on the keypad).

---

### Note

- The duress code, super code, and dismiss code should be different.
- The duress code, super password, and the dismiss code should be different from the authentication password.
- The length of duress code, super password, and the dismiss code is according the device, usually it should contains 4 to 8 digits.

5. Click OK.

6. **Optional:** Click Copy to , and then select the door/floor(s) to copy the parameters in the page to the selected doors/floor(s).

---

### Note

The door or floor's status duration settings will be copied to the selected door/floor(s) as well.


---

## Configure Parameters for Card Reader

After adding the access control device, you can configure its card reader parameters.



## Steps

1. Click Access Control Advanced Function Device Parameter .
2. In the device list on the left, click  to expand the door, select a card reader and you can edit the card reader's parameters on the right.
3. Edit the card reader basic parameters in the Basic Information page.



### Note

- The displayed parameters may vary for different access control devices. There are part of parameters listed as follows. Refer to the user manual of the device for more details.
- Some of the following parameters are not listed in the Basic Information page, click More to edit the parameters.

---

### Name

Edit the card reader name as desired.

### OK LED Polarity/Error LED Polarity/Buzzer Polarity

Set OK LED Polarity/Error LED Polarity/Buzzer LED Polarity of main board according to the card reader parameters. Generally, adopts the default settings.

### 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 Entering PWD

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.

### Alarm of Max. Failed Attempts

Enable to report alarm when the card reading attempts reach the set value.

### Max. Times of Card Failure

Set the max. failure attempts of reading card.

### Tampering Detection

Enable the anti-tamper detection for the card reader.

### Communicate with Controller Every

When the access control device cannot connect with the card reader for longer than the set time, the card reader will turn offline automatically.

### Buzzing Time

Set the card reader buzzing time. The available time ranges from 0 to 5,999s. 0 represents continuous buzzing.

### Card Reader Type/Card Reader Description

Get card reader type and description. They are read-only.

### Fingerprint Recognition Level

Select the fingerprint recognition level in the drop-down list.

### Default Card Reader Authentication Mode

View the default card reader authentication mode.

### **Fingerprint Capacity**

View the maximum number of available fingerprints.

### **Existing Fingerprint Number**

View the number of existed fingerprints in the device.

### **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 will be 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. By default, it is 2s.

### **Face 1:1 Matching Threshold**

Set the matching threshold 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.

### **1:N Security Level**

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.

### **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.

### **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.

### **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.

### **Application Mode**

You can select indoor or others application modes according to actual environment.

4. Click OK.

5. **Optional:** Click Copy to, and then select the card reader(s) to copy the parameters in the page to the selected card reader(s).

### Configure Parameters for Alarm Input

After adding the access control device, you can configure the parameters for its alarm inputs.

#### Steps


---



#### Note

If the alarm input is armed, you cannot edit its parameters. Disarm it first.

---

1. Click Access Control Advanced Function Device Parameter .
2. In the device list on the left, click  to expand the door, select an alarm input and you can edit the alarm input's parameters on the right.
3. Set the alarm input parameters.

#### Name

Edit the alarm input name as desired.

#### Detector Type

The detector type of the alarm input.

#### Zone Type

Set the zone type for the alarm input.

#### Sensitivity

Only when the duration of signal detected by the detector reaches the setting time, the alarm input is triggered. For example, you have set the sensitivity as 10ms, only when the duration of signal detected by the detector reach 10ms, this alarm input is triggered.

#### Trigger Alarm Output

Select the alarm output(s) to be triggered.


4. Click OK.

5. **Optional:** Click the switch on the upper-right corner to arm or disarm the alarm input.

### Configure Parameters for Alarm Output

After adding the access control device, if the device links to alarm outputs, you can configure the parameters.

#### Steps

1. Click Access Control Advanced Function Device Parameter to enter access control parameter configuration page.
2. In the device list on the left, click  to expand the door, select an alarm input and you can edit the alarm input's parameters on the right.
3. Set the alarm output parameters.

#### Name

Edit the card reader name as desired.

#### Alarm Output Active Time

How long the alarm output will last after triggered.

4. Click OK.

5. **Optional:** Set the switch on the upper right corner to ON to trigger the alarm output.

## Configure Parameters for Lane Controller

After adding the lane controller to the client, you can configure its parameters for passing through the lane.

### Steps

1. Click Access Control Advanced Function Device Parameter to enter Parameter Settings page.
2. In the device list on the left, select a lane controller and you can edit the lane controller's parameters on the right.
3. Edit the parameters.

#### Passing Mode

Select the controller which will control the barrier status of the device.

If you select **According to Lane Controller's DIP Settings**, the device will follow the lane controller's DIP settings to control the barrier. The settings on the software will be invalid.

If you select **According to Main Controller's Settings**, the device will follow the settings of the software to control the barrier. The DIP settings of the lane controller will be invalid.

#### Free Passing Authentication

If you enable this function, when both entrance and exit's barrier mode is Remain Open, the pedestrians should authenticate each time passing through the lane. Or an alarm will be triggered.

#### Opening/Closing Door Speed

Set the barrier's opening and closing speed. You can select from 1 to 10. The greater the value, the faster the speed.

---

#### Note

The recommended value is 6.

---

#### Audible Prompt Duration

Set how long the audio will last, which is played when an alarm is triggered .

---

#### Note

0 refers to the alarm audio will be played until the alarm is ended.

---

#### Temperature Unit

Select the temperature unit that displayed in the device status.

4. Click OK.

## 9.4.2 Configure Remaining Open/Closed

You can set the status of the door as open or closed and set the elevator controller as free and controlled. For example, you can set the door remaining closed in the holiday, and set the door remaining open in the specified period of the work day.

### Before You Start

Add the access control devices to the system.

## Steps

1. Click Access Control Advanced Function Remain Open/Closed to enter the Remain Open/Closed page.
2. Select the door or elevator controller that need to be configured on the left panel.
3. To set the door or elevator controller status during the work day, click the Week Schedule and perform the following operations.
  - 1) For door, click Remain Open or Remain Closed.
  - 2) For elevator controller, click Free or Controlled.
  - 3) Drag the cursor to draw the time duration, which means in that duration of time, the configured access group is activated.




### Note


Up to 8 time durations can be set to each day in the week schedule.

---

- 4) **Optional:** Perform the following operations to edit the time durations.

Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to .

Click the time duration and directly edit the start/end time in the appeared dialog.

Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to .

- 5) Click Save.

### Related Operations

<b>Copy to Whole Week</b>	Select one duration on the time bar, click Copy to Whole Week to copy all the duration settings on this time bar to other week days.
<b>Delete Selected</b>	Select one duration on the time bar, click Delete Selected to delete this duration.
<b>Clear</b>	Click Clear to clear all the duration settings in the week schedule.

4. To set the door status during the holiday, click the Holiday and perform the following operations.
  - 1) Click Remain Open or Remain Closed.
  - 2) Click Add.
  - 3) Enter the start date and end date.
  - 4) Drag the cursor to draw the time duration, which means in that duration of time, the configured access group is activated.




### Note


Up to 8 time durations can be set to one holiday period.




---

- 5) Perform the following operations to edit the time durations.

Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to .

Click the time duration and directly edit the start/end time in the appeared dialog.

Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to .

- 6) **Optional:** Select the time duration(s) that need to be deleted, and then click  in the Operation column to delete the selected time duration(s).
  - 7) **Optional:** Click  in the Operation column to clear all the time duration(s) in the time bar.
  - 8) **Optional:** Click  in the Operation column to delete this added holiday period from the holiday list.
  - 9) Click Save.
5. **Optional:** Click Copy to to copy the door status settings of this door to other door(s).

### 9.4.3 Configure Multi-Factor Authentication

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

#### Before You Start

Set access group and apply the access group to the access control device. For details, refer to ***Set Access Group to Assign Access Authorization to Persons***.

Perform this task when you want to set authentications for multiple cards of one access control point (door).

#### Steps

1. Click Access Control Advanced Function Multi-Factor Auth .
2. Select an access control device in device list on the left panel.
3. Add a person/card group for the access control device.
  - 1) Click Add on the right panel.
  - 2) Create a name for the group as desired.
  - 3) Specify the start time and end time of the effective period for the person/card group.
  - 4) Select members(s) and card(s) in the Available list, and the selected member(s) and card(s) will be added to the Selected list.

---

#### Note

Make sure you have issue card to the person.

Make sure you have set access group and apply the access group to the access control device successfully.

---

- 5) Click Save.
  - 6) **Optional:** Select the person/card group(s), and then click Delete to delete it(them).
  - 7) **Optional:** Select the person/card group(s), and then click Apply to re-apply access group that failed to be applied previously to the access control device.
4. Select an access control point (door) of selected device on the left panel.

5. Enter the maximum interval when entering password.
6. Add an authentication group for the selected access control point.
  - 1) Click Add on the Authentication Groups panel.
  - 2) Select a configured template as the authentication template from the drop-down list.

---

 **Note**

For setting the template, refer to *Configure Schedule and Template*.

---

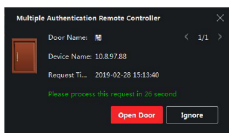
- 3) Select the authentication type as **Local Authentication**, **Local Authentication and Remotely Open Door**, or **Local Authentication and Super Password** from the drop-down list.

#### **Local Authentication**

Authentication by the access control device.

#### **Local Authentication and Remotely Open Door**

Authentication by the access control device and by the client. When the person swipes the card on the device, a window will pop up. You can unlock the door via the client.



**Figure 9-1 Remotely Open Door**

---

 **Note**

You can check Offline Authentication 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) Select the added person/card group in the left list below and it will be added to the Selected list on the right as the authentication group.
- 5) Click the added authentication group in the right list to set authentication times in the Auth Times column.

---

 **Note**

- The authentication times should be larger than 0 and smaller than the added personnel quantity in the personnel group.
  - The maximum value of authentication times is 16.
- 

- 6) Click Save.

---

 **Note**

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

7. Click Save.

### 9.4.4 Configure Custom Wiegand Rule

Based on the knowledge of uploading rule for the third party Wiegand, you can set multiple customized Wiegand rules to communicate between the device and the third party card readers.

#### Before You Start

Wire the third party card readers to the device.

Perform this task to configure the custom Wiegand rule for the third party card readers.

#### Steps

---

 **Note**

- By default, the device disables the custom wiegand function. If the device enables the custom Wiegand function, all wiegand interfaces in the device will use the customized wiegand protocol.
  - Up to 5 custom Wiegands can be set.
  - For details about the custom Wiegand, see .
- 

1. Click Access Control Advanced Function Custom Wiegand to enter the Custom Wiegand page.
  2. Select a custom Wiegand on the left.
  3. Create a Wiegand name.
- 

 **Note**

Up to 32 characters are allowed in the custom Wiegand name.

---

4. Click Select Device to select the access control device for setting the custom wiegand.
  5. Set the parity mode according to the property of the third party card reader.
- 

 **Note**

- Up to 80 bits are allowed in the total length.
  - The odd parity start bit, the odd parity length, the even parity start bit and the even parity length range from 1 to 80 bit.
  - The start bit of the card ID, the manufacturer code, the site code, and the OEM should range from 1 to 80 bit.
- 
6. Set output transformation rule.



- 1) Click Set Rule to open the Set Output Transformation Rules window.

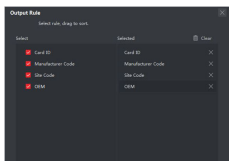


Figure 9-2 Set Output Transformation Rule

- 2) Select rules on the left list.  
The selected rules will be added to the right list.
  - 3) **Optional:** Drag the rules to change the rule order.
  - 4) Click OK.
  - 5) In the Custom Wiegand tab, set the rule's start bit, length, and the decimal digit.
7. Click Save.

## 9.4.5 Configure Card Reader Authentication Mode and Schedule

You can set the passing rules for the card reader of the access control device according to your actual needs.

Perform this task if you need to configure the card reader's authentication mode and schedule.

### Steps

1. Click Access Control Advanced Function Authentication to enter the authentication mode configuration page.
2. Select a card reader on the left to configure.
3. Set card reader authentication mode.
  - 1) Click Configuration.

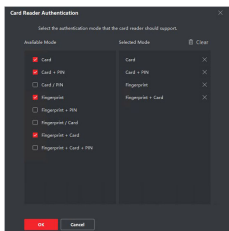


Figure 9-3 Select Card Reader Authentication Mode

---

### Note

PIN refers to the PIN code set to open the door. Refer to ***Configure Access Control Information***.

---

- 2) Check the modes in the Available Mode list and they will be added to the selected modes list.
- 3) Click OK.  
After selecting the modes, the selected modes will display as icons with different color.

4. Click the icon to select a card reader authentication mode, and drag the cursor 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.
6. **Optional:** Select a configured day and click Copy to Week to copy the same settings to the whole week.
7. **Optional:** Click Copy to to copy the settings to other card readers.
8. Click Save.

## 9.4.6 Configure First Person In

You can set multiple first persons for one access control point. After the first person is authorized, it allows multiple persons access the door or other authentication actions.

### Before You Start

Set the access group and apply the access group to the access control device. For details, refer to **Set Access Group to Assign Access Authorization to Persons**.

Perform this task when you want to configure opening door with first person.

### Steps

1. Click Access Control Advanced Function First Person In to enter the First Person In page.
2. Select an access control device in the list on the left panel.
3. Select the current mode as **Enable Remaining Open after First Person, Disable Remaining Open after First Person, or Authorization by First Person** from the drop-down list for each access control point of the selected device.

#### Enable Remaining Open after First Person

The door remains open for the configured time duration after the first person is authorized until the remain open duration ends. If you select this mode, you should set the remain open duration.



#### Note

The remain open duration should be between 0 and 1440 minutes. By default, the remain open duration is 10 minutes.

---

#### Disable Remaining Open after First Person

Disable the function of first person in, namely normal authentication.

#### Authorization by First Person

All authentications (except for the authentications of super card, super password, duress card, and duress code) are allowed only after the first person authorization.

---



#### Note

You can authenticate by the first person again to disable the first person mode.

---

4. Click Add on the First Person List panel.
5. Select person(s) in the left list and the person(s) will be add to the selected persons as the first person(s) of the doors.

The added first person(s) will list in the First Person List

6. **Optional:** Select a first person from the list and click Delete to remove the person from the first person list.

7. Click Save.

### 9.4.7 Configure Anti-Passback

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.

#### Before You Start

Enable the anti-passing back function of the access control device.

Perform this task when you want to configure the anti-passing back for the access control device.


#### Steps

---

##### Note

Either the anti-passing back or multi-door interlocking function can be configured for an access control device at the same time. For the configuration of multi-door interlocking, refer to ***Configure Multi-door Interlocking***.

---

1. Click Access Control Advanced Function Anti-Passback to enter the Anti-Passpack Settings page.
  2. Select an access control device on the left panel.
  3. Select a card reader as the beginning of the path in the First Card Reader field.
  4. Click  of the selected first card reader in the Card Reader Afterward column to open the select card reader dialog.
  5. Select the afterward card readers for the first card reader.
- 

##### Note

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

---

6. Click OK in the dialog to save the selections.
7. Click Save in the Anti-Passback Settings page to save the settings and take effect.

#### Example

##### Set Card Swiping Path

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.

### 9.4.8 Configure Multi-door Interlocking

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

Perform this task when you want to realize interlocking between multiple doors.

## Steps

---



### Note

- Multi-door Interlocking function is only supported by the access control device which has more than one access control points (doors).
  - Either the anti-passing back or multi-door interlocking function can be configured for an access control device at the same time. For the configuration of anti-passing back function, refer to **Configure Anti-Passback**.
- 

1. Click Access Control Advanced Function Multi-door Interlocking .
  2. Select an access control device on the left panel.
  3. Click Add on the Multi-door Interlocking List panel to open Add Access Control Point to open the Add window.
  4. Select at least two access control points(doors) from the list.
- 



### Note

Up to four doors can be added in one multi-door interlocking combination.

---

5. Click OK to add the selected access control point(s) for interlocking.  
The configured multi-door interlocking combination will list on the Multi-door Interlocking List panel.
6. **Optional:** Select an added multi-door interlocking combination from the list and click Delete to delete the combination.
7. Click Apply to apply the settings to the access control device.

## 9.4.9 Configure Other Parameters

After adding the access control device, you can set its parameters such as network parameters, capture parameters, RS-485 parameters, Wiegand parameters, etc.

### Set Multiple NIC Parameters

If the device supports multiple network interfaces, you can set the network parameters of these NICs via the client, such as IP address, MAC address, port number, etc.

## Steps

---



### Note

This function should be supported by the device.

---

1. Enter the Access Control module.
2. On the navigation bar on the left, enter Advanced Function More Parameters .
3. Select an access control device in the device list and click NIC to enter Multiple NIC Settings page.
4. Select an NIC you want to configure from the drop-down list.
5. Set its network parameters such as IP address, default gateway, subnet mask, etc.

### MAC Address

A media access control address (MAC address) is a unique identifier assigned to the network interface for communications on the physical network segment.

## MTU

The maximum transmission unit (MTU) of the network interface.

6. Click Save.

## Set Network Parameters

After adding the access control device, you can set the device log uploading mode, and create EHome account via wired or wireless network.

### Set Log Uploading Mode

You can set the mode for the device to upload logs via EHome protocol.

#### Steps

1. Enter the Access Control module.
2. On the navigation bar on the left, enter Advanced Function More Parameters .
3. Select an access control device in the device list and enter Network Uploading Mode .
4. Select the center group from the drop-down list.
5. Check Enable to enable to set the uploading mode.
6. Select the uploading mode from the drop-down list.
  - Enable N1 or G1 for the main channel and the backup channel.
  - 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.

---

7. Click Save.

## Create EHome Account in Wired Communication Mode

You can set the account for EHome protocol in wired communication mode. Then you can add devices via EHome protocol.

#### Steps



#### Note

This function should be supported by the device

---

1. Enter the Access Control module.
2. On the navigation bar on the left, enter Advanced Function More Parameters .
3. Select an access control device in the device list and enter Network Network Center .
4. Select the center group from the drop-down list.
5. Select the **Address Type** as IP Address or Domain Name.
6. Enter IP address or domain name according to the address type.

7. Enter the port number for the protocol.



#### Note

The port number of the wireless network and wired network should be consistent with the port number of EHome.

---

8. Select the **Protocol Type** as EHome.

9. Set an account name for the network center.

10. Click Save.

### Create EHome Account in Wireless Communication Mode

You can set the account for EHome protocol in wireless communication mode. Then you can add devices via EHome protocol.

#### Steps

---



#### Note

This function should be supported by the device

---

1. Enter the Access Control module.

2. On the navigation bar on the left, enter Advanced Function More Parameters .

3. Select an access control device in the device list and enter Network Wireless Communication Center .

4. Select the **APN Name** as CMNET or UNINET.

5. Enter the SIM Card No.

6. Select the center group from the drop-down list.

7. Enter the IP address and port number.



#### Note

- By default, the port number for EHome is 7660.
  - The port number of the wireless network and wired network should be consistent with the port number of EHome.
- 

8. Select the **Protocol Type** as EHome.

9. Set an account name for the network center.

10. Click Save.

### Set Device Capture Parameters

You can configure the capture parameters of the access control device, including manual capture and event triggered capture.

---



#### Note

- The capture function should be supported by the device.
  - Before setting the capture parameters, you should set the picture storage first to define where the event triggered pictures are saved. For details, refer to .
- 

### Set Triggered Capture Parameters

When an event occurs, the camera of the access control device can be triggered to capture picture(s) to record what happens when the event occurs. You can view the captured pictures when checking the event details in Event Center. Before that, you need to set the parameters for the capture such as number of pictures captured for one time.

### Before You Start

Before setting the capture parameters, you should set the picture storage first to define where the captured pictures are saved. For details, refer to .

### Steps

---

#### Note

This function should be supported by the device

---

1. Enter the Access Control module.
2. On the navigation bar on the left, enter Advanced Function More Parameters Capture .
3. Select an access control device in the device list and select Linked Capture.
4. Set the picture size and quality.
5. Set the capture times once triggered which defines how many pictures will be captures for one time.
6. If the capture times is more than 1, set the interval for each capture.
7. Click Save.

### Set Manual Capture Parameters

In Status Monitoring module, you can capture a picture manually the access control device's camera by clicking a button. Before that, you need to set the parameters for the capture such as picture quality.

### Before You Start

Before setting the capture parameters, you should set the saving path first to define where the captured pictures are saved. For details, refer to .

### Steps

---

#### Note

This function should be supported by the device

---

1. Enter the Access Control module.
2. On the navigation bar on the left, enter Advanced Function More Parameters Capture .
3. Select an access control device in the device list and select Manual Capture.
4. Select the resolution of the captured pictures from the drop-down list.
5. Select the picture quality as High, Medium, or Low. The higher the picture quality is, the larger size the picture will be.
6. Click Save.

### Set Parameters for Face Recognition Terminal

For face recognition terminal, you can set its parameters including face picture database, QR code authentication, etc.

### Steps

---

#### Note

This function should be supported by the device.

---

1. Enter the Access Control module.

2. On the navigation bar on the left, enter Advanced Function More Parameters .
3. Select an access control device in the device list and click Face Recognition Terminal.
4. Set the parameters.

---

 **Note**

These parameters displayed vary according to different device models.

---

**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**

select Deep Learning as the face picture database.

**Authenticate by QR Code**

If enabled, the device camera can scan the QR code to authenticate. By default, the function is disabled.

**Blacklist Authentication**

If enabled, the device will compare the person who want to access with the persons in the blacklist.

If matched (the person is in the blacklist), the access will be denied and the device will upload an alarm to the client.

If mismatched (the person is not in the blacklist), the access will be granted.

**Save Authenticating Face Picture**

If enabled, the captured face picture when authenticating will be saved on the device.

**MCU Version**

View the device MCU version.

5. Click Save.

**Set RS-485 Parameters**

You can set the access control device's RS-485 parameters including the baud rate, data bit, the stop bit, parity type, flow control type, communication mode, work mode, and connection mode.

**Steps**

---

 **Note**

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

---

1. Enter the Access Control module.
2. On the navigation bar on the left, enter Advanced Function More Parameters .
3. Select an access control device in the device list and click RS-485 to enter the RS-485 Settings page.
4. Select the serial port number from the drop-down list to set the RS-485 parameters.
5. Set the baud rate, data bit, the stop bit, parity type, communication mode, working mode, and connection mode in the drop-down list.



## 6. Click Save.

- The configured parameters will be applied to the device automatically.
- After changing the working mode or connection mode, the device will reboot automatically.

### Set Wiegand Parameters

You can set the access control device's Wiegand channel and the communication mode. After setting the Wiegand parameters, the device can connect to Wiegand card reader via Wiegand communication.

#### Steps

---

##### Note

This function should be supported by the device.

---

1. Enter the Access Control module.
  2. On the navigation bar on the left, enter Advanced Function More Parameters .
  3. Select an access control device in the device list and click Wiegand to enter the Wiegand Settings page.
  4. Set the switch to on to enable the Wiegand function for the device.
  5. Select the Wiegand channel No. and the communication mode from the drop-down list.
- 

##### Note

If you set **Communication Direction** as Sending, you are required to set the **Wiegand Mode** as Wiegand 26 or Wiegand 34.

---

## 6. Click Save.

- The configured parameters will be applied to the device automatically.
- After changing the communication direction, the device will reboot automatically.

### Enable M1 Card Encryption

M1 card encryption can improve the security level of authentication.

#### Steps

---

##### Note

The function should be supported by the access control device and the card reader.

---

1. Enter the Access Control module.
2. On the navigation bar on the left, enter Advanced Function More Parameters .
3. Select an access control device in the device list and click M1 Card Encryption to enter the M1 Card Encryption page.
4. Set the switch to on to enable the M1 card encryption function.
5. Set the sector ID.  
The sector ID ranges from 1 to 100.

6. Click Save to save the settings.

## 9.5 Configure Linkage Actions for Access Control

The events triggered by the access control devices, doors, card readers, and alarm inputs, as well as the card swiping of persons, mobile terminal's MAC address detected, and employee No. detected, can trigger a series of linkage actions to notify the security personnel and record the events.

Two types of linkage actions are supported: client actions and device actions.

- **Client Actions:** When the event is detected, it will trigger the actions on the client, such as the client playing alarm sound and sending an email to notify the security personnel.
- **Device Actions:** When the event is detected, it will trigger the actions of this device, such as buzzing, door open/closed, audio play, etc., to notify the security personnel and allow/forbid access.

### 9.5.1 Configure Client Actions for Access Event

You can assign client linkage actions to the event by setting up a rule. For example, when the event is detected, an audible warning appears to notify the security personnel.

#### Steps

---

#### Note

The linkage actions here refer to the linkage of the client software's own actions such as audible warning, email linkage, etc.

---

1. Click Event Management Access Control Event .

The added access control devices will display in the device list.

2. Select a resource (including device, alarm input, door/elevator, and card reader) from the device list.

The event types which the selected resource supports will display.

3. Select the event(s) and click Edit Priority to define the priority for the event(s), which can be used to filter events in the Event Center.

4. Set the linkage actions of the event.

- 1) Select the event(s) and click Edit Linkage to set the client actions when the events triggered.

#### **Audible Warning**

The client software gives an audible warning when alarm is triggered. You can select the alarm sound for audible warning.

---

#### Note

For setting the alarm sound, please refer to .

---

#### **Email Linkage**

Send an email notification of the alarm information to one or more receivers.

- 2) Click OK.

5. Enable the event so that when the event is detected, an event will be sent to the client and the linkage actions will be triggered.
6. **Optional:** Click Copy to... to copy the event settings to other access control device, alarm input, door/elevator, or card reader.

## 9.5.2 Configure Device Actions for Access Event

You can set the access control device's linkage actions for the access control device's triggered event. When the event is triggered, it can trigger the alarm output, host buzzer, and other actions on the same device.

### Steps

---

#### Note

It should be supported by the device.

---

1. Click Access Control Linkage Configuration .
2. Select the access control device from the list on the left.
3. Click Add button to add a new linkage.
4. Select the event source as Event Linkage.
5. select the event type and detailed event to set the linkage.
6. In the Linkage Target area, set the property target to enable this action.

#### **Buzzer on Controller**

The audible warning of access control device will be triggered.

#### **Capture**

The real-time capture will be triggered.

#### **Recording**

The recording will be triggered.

---

#### Note

The device should support recording.

---

#### **Buzzer on Reader**

The audible warning of card reader will be triggered.

#### **Alarm Output**

The alarm output will be triggered for notification.

#### **Alarm Input**

Arm or disarm the alarm input.

---

#### Note

The device should support alarm input function.

---

#### **Access Point**

The door status of open, close, remain open, and remain close will be triggered.

---

#### Note

The target door and the source door cannot be the same one.

---

#### **Audio Play**

The audio prompt will be triggered. And the select audio index related audio content will be played according to the configured play mode.

7. Click Save.

8. **Optional:** After adding the device linkage, you can do one or more of the following:

**Edit Linkage Settings** Select the configured linkage settings in the device list and you can edit its event source parameters, including event source and linkage target.

**Delete Linkage Settings** Select the configured linkage settings in the device list and click Delete to delete it.

### 9.5.3 Configure Device Actions for Card Swiping

You can set the access control device's linkage actions for the specified card swiping. When you swipe the specified card, it can trigger the alarm output, host buzzer, and other actions on the same device.

#### Steps

---

#### Note

It should be supported by the device.

---

1. Click Access Control Linkage Configuration .
2. Select the access control device from the list on the left.
3. Click Add button to add a new linkage.
4. Select the event source as Card Linkage.
5. Enter the card number or select the card from the dropdown list.
6. Select the card reader where the card swipes to trigger the linked actions.
7. In the Linkage Target area, set the property target to enable this action.

#### **Buzzer on Controller**

The audible warning of access control device will be triggered.

#### **Buzzer on Reader**

The audible warning of card reader will be triggered.

#### **Capture**

The real-time capture will be triggered.

#### **Recording**

The recording will be triggered.

---

#### Note

The device should support recording.

---

#### **Alarm Output**

The alarm output will be triggered for notification.

#### **Alarm Input**

Arm or disarm the alarm input.

---

 **Note**

The device should support alarm input function.

---

**Access Point**

The door status of open, close, remain open, or remain closed will be triggered.

**Audio Play**

The audio prompt will be triggered. And the select audio index related audio content will be played according to the configured play mode.

**8. Click Save.**

When the card (configured in Step 5) swipes on the card reader (configured in Step 6), it can trigger the linked actions (configured in step 7).

**9. Optional:** After adding the device linkage, you can do one or more of the following:

- |                                |  |
|--------------------------------|--|
| <b>Delete Linkage Settings</b> | Select the configured linkage settings in the device list and click Delete to delete it.   |
| <b>Edit Linkage Settings</b>   | Select the configured linkage settings in the device list and you can edit its event source parameters, including event source and linkage target. |

## 9.5.4 Configure Device Linkage for Mobile Terminal's MAC Address

You can set the access control device's linkage actions for the specified MAC address of mobile terminal. When access control device detects the specified MAC address, it can trigger the alarm output, host buzzer, and other actions on the same device.

**Steps**

---

 **Note**

It should be supported by the device.

---

1. Click Access Control Linkage Configuration .
2. Select the access control device from the list on the left.
3. Click Add button to add a new linkage.
4. Select the event source as Mac Linkage.
5. Enter the MAC address to be triggered.

---

 **Note**

MAC Address Format: AA:BB:CC:DD:EE:FF.

---

6. In the Linkage Target area, set the property target to enable this action.

**Buzzer on Controller**

The audible warning of access control device will be triggered.

**Buzzer on Reader**

The audible warning of card reader will be triggered.

**Capture**

The real-time capture will be triggered.

### Recording

The recording will be triggered.

---

 **Note**

The device should support recording.

---

### Alarm Output

The alarm output will be triggered for notification.

### Alarm Input

Arm or disarm the alarm input.

---

 **Note**

The device should support alarm input function.

---

### Access Point

The door status of open, close, remain open, or remain closed will be triggered.

### Audio Play

The audio prompt will be triggered. And the select audio index related audio content will be played according to the configured play mode.

7. Click Save to save the settings.

8. **Optional:** After adding the device linkage, you can do one or more of the following:

- |                                |  |
|--------------------------------|--|
| <b>Edit Linkage Settings</b>   | Select the configured linkage settings in the device list and you can edit its event source parameters, including event source and linkage target. |
| <b>Delete Linkage Settings</b> | Select the configured linkage settings in the device list and click Delete to delete it.   |

## 9.5.5 Configure Device Actions for Person ID

You can set the access control device's linkage actions for the specified person ID. When access control device detects the specified person ID, it can trigger the alarm output, host buzzer, and other actions on the same device.

### Steps

---

 **Note**

It should be supported by the device.

---

1. Click Access Control Linkage Configuration .
2. Select the access control device from the list on the left.
3. Click Add button to add a new linkage.
4. Select the event source as Person Linkage.
5. Enter the employee number or select the person from the dropdown list.
6. Select the card reader where the card swipes to trigger the linked actions.

7. In the Linkage Target area, set the property target to enable this action.

#### **Buzzer on Controller**

The audible warning of access control device will be triggered.

#### **Buzzer on Reader**

The audible warning of card reader will be triggered.

#### **Capture**

The real-time capture will be triggered.

#### **Recording**

The recording will be triggered.



#### **Note**

The device should support recording.

---

#### **Alarm Output**

The alarm output will be triggered for notification.

#### **Alarm Input**

Arm or disarm the alarm input.



#### **Note**

The device should support zone function.

---

#### **Access Point**

The door status of open, close, remain open, or remain closed will be triggered.

#### **Audio Play**

The audio prompt will be triggered. And the select audio index related audio content will be played according to the configured play mode.

8. Click Save.

9. **Optional:** After adding the device linkage, you can do one or more of the following:

**Delete Linkage Settings**      Select the configured linkage settings in the device list and click Delete to delete it.

**Edit Linkage Settings**      Select the configured linkage settings in the device list and you can edit its event source parameters, including event source and linkage target.

## **9.6 Door/Elevator Control**

In Monitoring module, you can view the real-time status of the doors or elevators managed by the added access control device. You can also control the doors and elevators such as open/close the door, or remain the door open/closed via the client remotely. The real-time access event are displayed in this module. You can view the access details and person details.



#### **Note**

For the user with door/elevator control permission, the user can enter the Monitoring module and control the door/elevator. Or

the icons used for control will not show. For setting the user permission, refer to .

---

## 9.6.1 Control Door Status

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

### Steps

1. Click Monitoring to enter the status monitoring page.
2. Select an access point group on the upper-right corner.



#### Note

For managing the access point group, refer to .

---

The doors in the selected access control group will display.

3. Click a door icon to select a door, or press Ctrl and select multiple doors.
4. Click the following buttons to control the door.

#### Open Door

When the door is locked, unlock it and it will be open for once. After the open duration, the door will be closed and locked again automatically.

#### Close Door

When the door is unlocked, lock it and it will be closed. The person who has the access authorization can access the door with credentials.

#### Remain Open

The door will be unlocked (no matter closed or open). All the persons can access the door with no credentials required.

#### Remain Closed

The door will be closed and locked. No person can access the door even if he/she has the authorized credentials, except the super users.

#### Capture

Capture a picture manually.

---



#### Note

The Capture button is available when the device supports capture function. The picture is saved in the PC running the client. For setting the saving path, refer to .

---

### Result

The icon of the doors will change in real-time according to the operation if the operation is succeeded.

## 9.6.2 Control Elevator Status

You can control the elevator status of the added elevator controller, including opening elevator's door, controlled, free, calling elevator, etc.



## Steps

---



### Note

- You can control the elevator via the current client if it is not armed by other client. The elevator cannot be controlled by other client software if the elevator status changes.
  - Only one client software can control the elevator at one time.
  - The client which has controlled the elevator can receive the alarm information and view the elevator real-time status.
- 

1. Click Monitoring to enter the status monitoring page.
  2. Select an access point group on the upper-right corner.
- 



### Note

For managing the access point group, refer to .

---

The elevators in the selected access point group will display.

3. Click a door icon to select an elevator.
4. Click the following buttons to control the elevator.

#### Open Door

When the elevator's door is closed, open it. After the open duration, the door will be closed again automatically.

#### Controlled

You should swipe the card before pressing the target floor button. And the elevator can go to the target floor.

#### Free

The selected floor's button in the elevator will be valid all the time.

#### Disabled

The selected floor's button in the elevator will be invalid and you cannot go to the target floor.

## Result

The icon of the doors will change in real-time according to the operation if the operation is succeeded.

## 9.6.3 Check Real-Time Access Records

The access records will display in real time, including card swiping records, face recognitions records, fingerprint comparison records, etc. You can view the person information and view the picture captured during access.

## Steps

1. Click Monitoring and select a group from the drop-down list on the upper-right corner.

The access records triggered at the doors in the selected group will display in real time. You can view the details of the records, including card No., person name, organization, event time, etc.

2. **Optional:** Check the event type and event status so that these events will show in the list if the events are detected. The events of unchecked type or status will not be displayed in the list.
3. **Optional:** Check Show Latest Event and the latest access record will be selected and displayed at the top of the record list.

- 4. Optional:** Click the event to view the accessed person details, including person pictures (captured picture and profile), person No., person name, organization, phone, contact address, etc.
- 

 **Note**

You can double click the captured picture to enlarge it to view the details.

---

- 5. Optional:** Right click on the column name of the access event table to show or hide the column according to actual needs.

## 9.7 Time and Attendance

The Time and Attendance module provides multiple functionalities to track and monitor when employees start and stop work, and full control of employees working hours such as late arrivals, early departures, time taken on breaks and absenteeism.

---

 **Note**

In this section, we introduce the configurations before you can getting the attendance reports. The access records recorded after these configurations will be calculated in the statistics.

---

### 9.7.1 Configure Attendance Parameters

You can configure the attendance parameters, including the general rule, overtime parameters, attendance check point, holiday, leave type, etc.

#### Configure General Rule

You can configure the general rule for attendance calculation, such as the week beginning, month beginning, weekend, absence, etc.

#### Steps

---

 **Note**

The parameters configured here will be set as default for the newly added time period. It will not affect the existed one(s).

---

1. Enter Time & Attendance module.
2. Click Attendance Settings General Rule .
3. Set the day as week beginning and the date as month beginning.
4. Select the day(s) as weekend.
5. Set absence parameters.
6. Click Save.

#### Configure Overtime Parameters

You can configure the overtime parameters for workday and non-workday, including overtime level, pay rate, attendance status for overtime, etc.

#### Steps

1. Enter Time & Attendance module.
2. Click Attendance Settings Overtime .
3. Set required information.

##### Overtime Level for Workday

When you work for certain period after end-work time on workday, you will reach different overtime level: overtime level 1, overtime level 2 and overtime level 3 . You can set different pay rate for three overtime levels, respectively.

### Pay Rate

Set corresponding pay rates for three overtime levels, which can be generally used to calculate total work hours.

### Overtime Rule for Non-Workday

You can enable overtime rule for non-workday and set calculation mode.

#### 4. Click Save.

### Configure Attendance Check Point

You can set the card reader(s) of the access point as the attendance check point, so that the authentication on the card readers will be recorded for attendance .

#### Before You Start

You should add access control device before configuring attendance check point. For details, refer to .

### Steps

---

#### Note

By default, all card readers of the added access control devices are set as attendance checkpoint.

---

1. Enter the Time & Attendance module.
2. Click Attendance Settings Attendance Check Point to enter the Attendance Check Point Settings page.
3. **Optional:** Set Set All Card Readers as Check Points switch to off.  
Only the card readers in the list will be set as the attendance check points.
4. Check the desired card reader(s) in the device list as attendance check point(s).
5. Set check point function as **Start/End-Work, Start-Work** or **End-Work**.
6. Click Set as Check Point.  
The configured attendance check point displays on the right list.

### Configure Holiday

You can add the holiday during which the check-in or check-out will not be recorded.

#### Add Regular Holiday

You can configure a holiday which will take effect annually on regular days during the effective period, such as New Year's Day, Independence Day, Christmas Day, etc.


### Steps

1. Enter the Time & Attendance module.
2. Click Attendance Settings Holiday to enter the Holiday Settings page.
3. Check Regular Holiday as holiday type.
4. Custom a name for the holiday.

5. Set the first day of the holiday.
6. Enter the number of the holiday days.
7. Set the attendance status if the employee works on holiday.
8. **Optional:** Check **Repeat Annually** to make this holiday setting effective every year.
9. Click OK.

The added holiday will display in the holiday list and calendar. If the date is selected as different holidays, it will be recorded as the first-added holiday.

10. **Optional:** After adding the holiday, perform one of the following operations.

**Edit Holiday**      Click  to edit the holiday information.

**Delete Holiday**      Select one or more added holidays, and click Delete to delete the holiday(s) from the holiday list.

### Add Irregular Holiday

You can configure a holiday which will take effect annually on irregular days during the effective period, such as Bank Holiday.

#### Steps

1. Enter the Time & Attendance module.
2. Click Attendance Settings Holiday to enter the Holiday Settings page.
3. Click Add to open the Add Holiday page.
4. Check Irregular Holiday as holiday type.
5. Custom a name for the holiday.
6. Set the start date of the holiday.


#### Example

If you want to set the forth Thursday in November, 2019 as the Thanksgiving Day holiday, you should select 2019, November, 4th, and Thursday from the four drop-down lists.

7. Enter the number of the holiday days.
8. Set the attendance status if the employee works on holiday.
9. **Optional:** Check **Repeat Annually** to make this holiday setting effective every year
10. Click OK.

The added holiday will display in the holiday list and calendar. If the date is selected as different holidays, it will be recorded as the first-added holiday.

11. **Optional:** After adding the holiday, perform one of the following operations.

**Edit Holiday**      Click  to edit the holiday information.


**Delete Holiday**      Select one or more added holidays, and click Delete to delete the holiday(s) from the holiday list.

### Configure Leave Type

You can customize the leave type (major leave type and minor leave type) according to actual needs. You can also edit or delete the leave type.

### Steps


1. Enter the Time & Attendance module.
2. Click Attendance Settings Leave Type to enter the Leave Type Settings page.
3. Click Add on the left to add a major leave type.
4. **Optional:** Perform one of the following operations for major leave type.

**Edit** Move the cursor over the major leave type and click  to edit the major leave type.

**Delete** Select one major leave type and click Delete on the left to delete the major leave type.

5. Click Add on the right to add a minor leave type.

6. **Optional:** Perform one of the following operations for minor leave type.

**Edit** Move the cursor over the minor leave type and click  to edit the minor leave type.

**Delete** Select one or multiple major leave types and click Delete on the right to delete the selected minor leave type(s).

### Synchronize Authentication Record to Third-Party Database

The attendance data recorded in client software can be used by other system for calculation or some other operations. You can enable synchronization function to apply the authentication record from client software to the third-party database automatically.

### Steps

1. Enter Time & Attendance module.
2. Click Attendance Settings Third-Party Database .
3. Set **Apply to Database** switch to on to enable synchronization function.
4. Set the required parameters of the third-party database, including database type, server IP address, database name, user name and password.
5. Set table parameters of database according to the actual configurations.
  - 1) Enter the table name of the third-party database.
  - 2) Set the mapped table fields between the client software and the third-party database.
6. Click Connection Test to test whether database can be connected.
7. Click Save to save the settings.

The attendance data will be written to the third-party database.

### Configure Break Time

You can add break time and set start time, end time, duration, calculation mode and other parameters for the break. The added break time can also be edited or deleted.

### Steps

1. Click Time & Attendance Timetable .

The added timetables are displayed in the list.

2. Select an added timetable or click Add to enter setting timetable page.
3. Click Settings in the break time area to enter break time management page.
4. Add break time.
  - 1) Click Add.
  - 2) Enter a name for the break time.
  - 3) Set related parameters for the break time.

#### **Start Time / End Time**

Set the time when the break starts and ends.

#### **No Earlier Than / No Later Than**

Set the earliest swiping time for starting break and the latest swiping time for ending break.

#### **Break Duration**

The duration from start time to end time of the break.

#### **Calculation**

##### **Auto Deduct**

The fixed break duration will be excluded from work hours.

##### **Must Check**

The break duration will be calculated and excluded from work hours according to actual check-in and check-out time.



#### **Note**

If you select **Must Check** as calculation method, you need to set attendance status for late or early returning from break.

---

5. Click Save to save the settings.
6. **Optional:** Click Add to continue adding break time.

### **Configure Report Display**

You can configure display contents displayed in the attendance report, such as the company name, logo, date format, time format, and mark.

### Steps

1. Enter Time & Attendance module.
2. Click Attendance Statistics Report Display .
3. Set the display settings for attendance report.

#### **Company Name**

Enter a company name to display the name in the report.

#### **Date Format / Time Format**

Set the date format and time format according to the actual needs.

#### **Attendance Status Mark in Report**

Enter the mark and select the color. The related fields of attendance status in the report will display with the mark and color.

#### **Weekend Mark in Report**

Enter the mark and select the color. The weekend fields in the report will display with the mark and color.

4. Click Save.

### **9.7.2 Add Timetable**

You can add the timetable for the shift schedule.

#### **Steps**

1. Click Time & Attendance Timetable to enter timetable settings window.
2. Click Add to enter Add Timetable page.
3. Create a name for the timetable.
4. Select calculation method.

#### **First Check-In & Last Check-Out**

The first check-in time is recorded as start work time and the last check-out time is recorded as the end-work time.

#### **Each Check-In/Out**

Each check-in time and check-out time is valid and the sum of all periods between adjacent check-in and check-out time will be recorded as the valid working duration.

You need to set **Valid Auth. Interval** for this calculation method. For example, if the interval between card swiping of the same card is less than the set value, the card swiping is invalid.

5. **Optional:** Set **Get Device Status** switch to on to get attendance status from the device.
6. Set the related attendance time.

#### **Work Time from**

Set the start-work time and end-work-time.

#### **Late/Early Leave**

Set the time period for late or early leave.

#### **Valid Check-in/out Time**

Set the time period during which the check-in or check-out is valid.

7. **Optional:** Select break time to exclude the duration from work hours.



#### **Note**

You can click Settings to manage break time. For more details about configuring break time, refer to **Configure Break Time**.

---

8. Click Save to add the timetable.
9. **Optional:** Perform one or more following operations after adding timetable.

**Edit Timetable** Select a timetable from the list to edit related information.

**Delete Timetable** Select a timetable from the list and click Delete to delete it.

### 9.7.3 Add Shift

You can add the shift for the shift schedule.

#### Before You Start

Add a timetable first. See **Add Timetable** for details.

#### Steps

1. Click Time & Attendance Shift to enter shift settings page.
2. Click Add to enter Add Shift page.
3. Enter the name for shift.
4. Select the shift period from the drop-down list.
5. Select the added timetable and click on the time bar to apply the timetable.

The screenshot displays the 'Add Shift' configuration page. At the top, the 'Shift Name' is 'New Shift 1'. Below it, 'Shift Period' is set to '1' and 'Week(s)' is a dropdown menu. There are two radio buttons: 'Default Time...' (which is selected) and 'Normal Workd...'. Below these are 'Delete' and 'Clear' buttons. A time bar shows 'Normal Workday : 09:00 - 18:00' with blue bars on Monday through Friday from 09:00 to 18:00. The time bar has columns for 00:00, 02:00, 04:00, 06:00, 08:00, 10:00, 12:00, 14:00, 16:00, 18:00, 20:00, 22:00, and 24:00. At the bottom are 'Save' and 'Assign' buttons.

Figure 9-4 Add Shift

6. Click Save.

The added shift lists on the left panel of the page. At most 64 shifts can be added.

7. **Optional:** Assign the shift to organization or person for a quick shift schedule.

- 1) Click Assign.

- 2) Select **Organization** or **Person** tab and check the desired organization(s) or person(s) box.

The selected organizations or persons will list on the right page.

- 3) Set the effective period for the shift schedule.

- 4) Set other parameters for the shift schedule, including Check-in Not Required, Check-out Not Required, Effective for Holiday, and Effective for Overtime.

- 5) Click Save to save the quick shift schedule.

### 9.7.4 Manage Shift Schedule

Shift work is an employment practice designed to make use of all 24 hours of the clock each day of the week. The practice typically sees the day divided into shifts, set periods of time during which different shifts perform their duties.



You can set department schedule, person schedule, and temporary schedule.

## Set 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.

### Before You Start

In Time & Attendance module, the department list is the same with the organization. You should add organization and persons in Person module first. See **Person Management** for details.

### Steps

1. Click Time & Attendance Shift Schedule to enter the Shift Schedule Management page.
2. Click Department Schedule to enter Department Schedule page.
3. Select the department from the organization list on the left.



#### Note

If **Include Sub Organization** is checked, when selecting the organization, its sub organizations are selected at the same time.

---

4. Select the shift from the drop-down list.
5. Check the checkbox to enable **Multiple Shift Schedules**.



#### Note

After checking Multiple Shift Schedules, you can select the effective time period(s) from the added time periods for the persons in the department.

### Multiple Shift Schedules

It contains more than one time periods. The person can check in/out in any of the time periods and the attendance will be effective.

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.

---

6. Set the start date and end date.
7. Set other parameters for the schedule, including Check-in Not Required, Check-out Not Required, Effective for Holiday, and Effective for Overtime.
8. Click Save.

## Set Person Schedule

You can assign the shift schedule to one or more persons. You can also view and edit the person schedule details.

### Before You Start

Add department and person in Person module. See **Person Management** for details.

## Steps

---

### Note

The person schedule has the higher priority than department schedule.

---

1. Click Time & Attendance Shift Schedule to enter the Shift Schedule Management page.
  2. Click Person Schedule to enter Person Schedule page.
  3. Select the organization and select the person(s).
  4. Select the shift from the drop-down list.
  5. Check the checkbox to enable **Multiple Shift Schedules**.
- 

### Note

After checking the Multiple Shift Schedules, you can select the effective timetable(s) from the added timetables for the persons.

#### **Multiple Shift Schedules**

It contains more than one timetables. The person can check in/out in any of the timetables and the attendance will be effective.

If the multiple shift schedules contains three timetables: 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 timetables. If the person checks in at 07:50, it will apply the nearest timetable 08:00 to 15:00 to the person's attendance.

---

6. Set the start date and end date.
7. Set other parameters for the schedule, including Check-in Not Required, Check-out Not Required, Effective for Holiday, and Effective for Overtime.
8. Click Save.

#### **Set Temporary Schedule**

You can add a temporary schedule for the person and the person will be assigned with the shift schedule temporarily. You can also view and edit the temporary schedule details.

#### **Before You Start**

Add department and person in Person module. See **Person Management** for details.

## Steps

---

### Note

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

---

1. Click Time & Attendance Shift Schedule to enter the Shift Schedule Management page.
2. Click Temporary Schedule to enter Temporary Schedule page.
3. Select the organization and select the person(s).
4. Click one date or click and drag to select multiple dates for the temporary schedule.
5. Select **Workday** or **Non-Workday** from drop-down list.

If **Non-Workday** is selected, you need to set the following parameters.

#### **Calculated as**

Select normal or overtime level to mark the attendance status for temporary schedule.

#### **Timetable**

Select a timetable from drop-down list.

#### **Multiple Shift Schedule**

It contains more than one timetables. The person can check in/out in any of the timetables and the attendance will be effective.

If the multiple shift schedules contains three timetables: 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 timetables. If the person checks in at 07:50, it will apply the nearest timetable 08:00 to 15:00 to the person's attendance.

#### **Rule**



Set other rule for the schedule, such as **Check-in Not Required**, and **Check-out Not Required**.

6. Click Save.

### **Check Shift Schedule**

You can check the shift schedule in calendar or list mode. You can also edit or delete the shift schedule.

#### **Steps**

1. Click Time & Attendance Shift Schedule to enter the Shift Schedule Management page.
2. Select the organization and corresponding person(s).
3. Click  or  to view the shift schedule in calendar or list mode.

#### **Calendar**

In calendar mode, you can view the shift schedule for each day in one month. You can click the temporary schedule for one day to edit or delete it.

#### **List**

In list mode, you can view the shift schedule details about one person or organization, such as shift name, type, effective period and so on. Check the shift schedule(s), and click Delete to delete the selected shift schedule(s).

## **9.7.5 Manually Correct Check-in/out Record**

If the attendance status is not correct, you can manually correct the check-in or check out record. You can also edit, delete, search, or export the check-in or check-out record.

#### **Before You Start**

- You should add organizations and persons in Person module. For details, refer to **Person Management**.
- The person's attendance status is incorrect.


#### **Steps**

1. Click Time & Attendance Attendance Handling to enter attendance handling page.

2. Click Correct Check-In/Out to enter adding the check-in/out correction page.
3. Select person from left list for correction.
4. Select the correction date.
5. Set the check-in/out correction parameters.
  - Select Check-in and set the actual start-work time.
  - Select Check-out and set the actual end-work time.



---

 **Note**

You can click  to add multiple check in/out items. At most 8 check-in/out items can be supported.

---

6. **Optional:** Enter the remark information as desired.
7. Click Save.
8. **Optional:** After adding the check-in/out correction, perform one of the following operations.

**View** Click  or  to view the added attendance handling information in calendar or list mode.

---

 **Note**

In calendar mode, you need to click Calculate to get the attendance status of the person in one month.

---

- Edit**
- In calendar mode, click the related label on date to edit the details.
  - In list mode, double-click the related field in Date, Handling Type, Time, or Remark column to edit the information.

**Delete** Delete the selected items.

**Export** Export the attendance handling details to local PC.

---

 **Note**

The exported details are saved in CSV format.

---

## 9.7.6 Add Leave and Business Trip

You can add leave and business trip when the employee want to ask for leave or go on a business trip.

### Before You Start

You should add organizations and persons in the Person module. For details, refer to **Person Management**.

### Steps

1. Click Time & Attendance Attendance Handling to enter attendance handling page.
2. Click Apply for Leave/Business Trip to enter adding the leave/business trip page.
3. Select person from left list.
4. Set the date(s) for your leave or business trip.
5. Select the major leave type and minor leave type from the drop-down list.

---

 **Note**

You can set the leave type in Attendance Settings. For details, refer to ***Configure Leave Type***.



---

6. Set the time for leave.

7. **Optional:** Enter the remark information as desired.

8. Click Save.

9. **Optional:** After adding the leave and business trip, perform one of the following operations.

**View** Click  or  to view the added attendance handling information in calendar or list mode.

---

 **Note**

In calendar mode, you need to click Calculate to get the attendance status of the person in one month.

---

**Edit**

- In calendar mode, click the related label on date to edit the details.
- In list mode, double-click the field in Date, Handling Type, Time, or Remark column to edit the related information.

**Delete** Delete the selected items.

**Export** Export the attendance handling details to local PC.

---

 **Note**

The exported details are saved in CSV format.

---

### 9.7.7 Calculate Attendance Data

You need to calculate the attendance data before searching and viewing the overview of the attendance data, employees' detailed attendance data, employees' abnormal attendance data, the employees' overtime working data, and card swiping log.

#### Automatically Calculate Attendance Data

You can set a schedule so that the client can calculate the attendance data automatically at the time you configured every day.

#### Steps

---

 **Note**

It will calculate the attendance data till the previous day.

---

1. Enter the Time & Attendance module.
2. Click Attendance Settings General Rule .
3. In the Auto-Calculate Attendance area, set the time that you want the client to calculate the data every day.
4. Click Save.

#### Manually Calculate Attendance Data

You can calculate the attendance data manually by setting the data range.

#### Steps

1. Enter the Time & Attendance module.

2. Click Attendance Statistics Calculate Attendance .
3. Set the start time and end time to define the attendance data range.
4. Set other conditions, including department, person name, employee No. and attendance status.
5. Click Calculate.

---

 **Note**

It can only calculate the attendance data within three months.

---

6. Perform one of the following operations.

**Correct Check-in/out** Click Correct Check-in/out to add check-in/out correction.

**Report** Click Report to generate the attendance report.

**Export** Click Export to export attendance data to local PC.

---

 **Note**

The exported details are saved in CSV format.

---

## 9.7.8 Attendance Statistics

You can check the original attendance record, generate and export the attendance report based on the calculated attendance data.

### Get Original Attendance Record

You can search the employee's attendance time, attendance status, check point, etc. in a time period to get an original record of the employees.

#### Before You Start

- You should add organizations and persons in Person module and the persons has swiped card. For details, refer to **Person Management**.
- Calculate the attendance data.

---

 **Note**

- The client will automatically calculate 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 **Manually Calculate Attendance Data**.
- 

#### Steps

1. Enter the Time & Attendance module.
2. Click Attendance Statistics Original Records .
3. Set the attendance start time and end time that you want to search from.
4. Set other search conditions, such as department, person name, and employee No.

- 5. Optional:** Click Get from Device to get the attendance data from the device.
- 6. Optional:** Click Reset to reset all search conditions and edit the search conditions again.
7. Click Search.  
The result displays on the page. You can view the employee's required attendance status and check point.
- 8. Optional:** After searching the result, perform one of the following operations.

<b>Generate Report</b>	Click Report to generate the attendance report.
<b>Export Report</b>	Click Export to export the results to the local PC.

### Generate Instant Report

It supports to generate the a series of attendance reports manually to view the employees' attendance results.

#### Before You Start

Calculate the attendance data.

---

#### Note

You can calculate the attendance data manually, or set the schedule so that the client can calculate the data automatically every day. For details, refer to **Calculate Attendance Data**.

---

#### Steps

1. Enter the Time & Attendance module.
2. Click Attendance Statistics Report .
3. Select a report type.
4. Select the department or person to view the attendance report.
5. Set the start time and end time during which the attendance data will be displayed in the report.
6. Click Report to generate the statistics report and open it.

### Custom Attendance Report

The client supports multiple report types and you can pre-define the report content and it can send the report automatically to the email address you configured.

#### Steps

---

#### Note

Set the email parameters before you want to enable auto-sending email functions. For details, refer to .

---

1. Enter the Time & Attendance module.
2. Click Attendance Statistics Custom Report .
3. Click Add to pre-define a report.
4. Set the report content.

#### Report Name

Enter a name for the report.

#### Report Type

Select one report type and this report will be generated.

### Report Time

The time to be selected may vary for different report type.

### Person

Select the added person(s) whose attendance records will be generated for the report.

**5. Optional:** Set the schedule to send the report to the email address(es) automatically.

- 1) Check the **Auto-Sending Email** to enable this function.
- 2) Set the effective period during which the client will send the report on the selected sending date(s).
- 3) Select the date(s) on which the client will send the report.
- 4) Set the time at which the client will send the report.

### Example

If you set the effective period as 2018/3/10 to 2018/4/10, select Friday as the sending date, and set the sending time as 20:00:00, the client will send the report at 8 p.m. on Fridays during 2018/3/10 to 2018/4/10.

---

### Note

Make sure the attendance records are calculated before the sending time. You can calculate the attendance data manually, or set the schedule so that the client can calculate the data automatically every day. For details, refer to **Calculate Attendance Data**.

---

5) Enter the receiver email address(es).

---

### Note

You can click + to add a new email address. Up to 5 email addresses are allowed.

---

6) **Optional:** Click Preview to view the email details.

6. Click OK.

**7. Optional:** After adding the custom report, you can do one or more of the followings:

- |                        |  |
|------------------------|--|
| <b>Edit Report</b>     | Select one added report and click Edit to edit its settings.   |
| <b>Delete Report</b>   | Select one added report and click Delete to delete it.   |
| <b>Generate Report</b> | Select one added report and click Report to generate the report instantly and you can view the report details. |



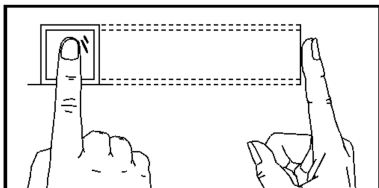
## A. Tips for Scanning Fingerprint

### Recommended Finger

Forefinger, middle finger or the third finger.

### Correct Scanning

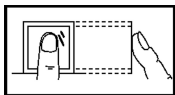
The figure displayed below is the correct way to scan your finger:



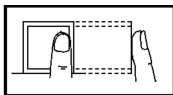
You should press your finger on the scanner horizontally. The center of your scanned finger should align with the scanner center.

### Incorrect Scanning

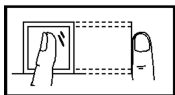
The figures of scanning fingerprint displayed below are incorrect:



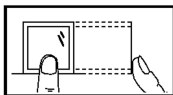
Vertical



Edge I



Side



Edge II

### Environment

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

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

### Others

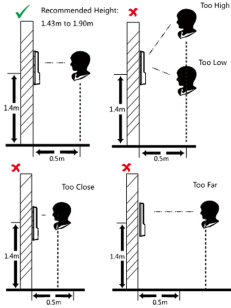
If your fingerprint is shallow, or it is hard to scan your fingerprint, we recommend you to use other authentication methods.

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

## B. Tips When Collecting/Comparing Face Picture

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

### Positions (Recommended Distance: 0.5 m)



### 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.

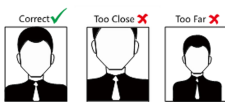
### Posture

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



### Size

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



## C. Tips for Installation Environment

### 1. Light Source Illumination Reference Value



Candle: 10Lux



Bulb: 100~850Lux



Sunlight: More than 1200Lux

2. Install the device at least 2 meters away from the light, and at least 3 meters away from the window or door.



3. Avoid backlight, direct and indirect sunlight



## D. Dimension

