



# Face Recognition Terminal

User Manual

## Legal Information

©2021 Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

### About this Manual

The Manual includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the Hikvision website ( <https://www.hikvision.com/> ).

Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

### Trademarks

**HIKVISION** and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.

Other trademarks and logos mentioned are the properties of their respective owners.

### Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE

DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.

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

## 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)

## 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. This equipment is intended to be supplied from the Class 2 surge protected power source rated DC 12V, 3A.
- 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.
- Do not ingest battery, Chemical Burn Hazard.  
This product contains a coin/button cell battery. If the coin/button cell battery is swallowed, it can cause severe internal burns in just 2 hours and can lead to death.  
Keep new and used batteries away from children. If the battery compartment does not close securely, stop using the product and keep it away from children. If you think batteries might have been swallowed or placed inside any part of the body, seek immediate medical attention.
- 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 completely applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.
- Working temperature: -30 °C to +60 °C
- Indoor and outdoor use. If installing the device indoors, the device should be at least 2 meters away from the light, and at least 3 meters away from the window or the door. If installing the device outdoors, you should apply Silicone sealant among the cable wiring area to keep the raindrop from entering.
- Protection level: IP65

## Available Models

Product Name	Model
Face Recognition Terminal	DS-K1T607M
	DS-K1T607MF
	DS-K1T607E
	DS-K1T607EF
	DS-K1T607MW
	DS-K1T607MFW
	DS-K1T607PE
	DS-K1T607PEF
	DS-K1T607PMW
	DS-K1T607PMFW
	DS-K1T607TM
	DS-K1T607TMF
	DS-K1T607TE
	DS-K1T607TEF
	DS-K1T607TMW
DS-K1T607TMFWW	

Use only power supplies listed in the user instructions:

Model	Manufacturer	Standard
C2000IC12.0-24P-DE	MOSO Power Supply Technology Co., Ltd.	CEE
C2000IC12.0-24P-GB	MOSO Power Supply Technology Co., Ltd.	BS
KPL-040F-VI	Channel Well Technology Co Ltd.	CEE

# Contents

<b>Chapter 1 Overview .....</b>	<b>1</b>
1.1 Overview .....	1
1.2 Features .....	1
1.2.1 Features (Normal Series) .....	1
1.2.2 Features (P Series) .....	2
1.2.3 Features (T Series) .....	2
<b>Chapter 2 Appearance .....</b>	<b>4</b>
<b>Chapter 3 Installation .....</b>	<b>6</b>
3.1 Installation Environment .....	6
3.2 Install with Gang Box .....	6
3.3 Install without Gang Box .....	12
<b>Chapter 4 Wiring .....</b>	<b>18</b>
4.1 Terminal Description .....	18
4.2 Wire Normal Device .....	21
4.3 Wire Secure Door Control Unit .....	22
<b>Chapter 5 Activation .....</b>	<b>23</b>
5.1 Activate via Device .....	23
5.2 Activate via SADP .....	24
5.3 Activate Device via Client Software .....	25
<b>Chapter 6 Basic Operation .....</b>	<b>27</b>
6.1 Set Application Mode .....	27
6.2 Login .....	29
6.2.1 Login For First Time .....	29
6.2.2 Login by Administrator .....	30
6.3 Communication Settings .....	33
6.3.1 Set Network Parameters .....	33

# Face Recognition Terminal User Manual

---

6.3.2 Set Wi-Fi Parameters .....	33
6.3.3 Set RS-485 Parameters .....	34
6.3.4 Set Wiegand Parameters .....	35
6.4 User Management .....	37
6.4.1 Add Administrator .....	37
6.4.2 Add Face Picture .....	38
6.4.3 Add Fingerprint .....	40
6.4.4 Add Card .....	41
6.4.5 Add Password .....	42
6.4.6 Set Authentication Mode .....	43
6.4.7 Search and Edit User .....	43
6.5 Import and Export Data .....	44
6.5.1 Export Data .....	44
6.5.2 Import Data .....	46
6.6 Identity Authentication .....	47
6.6.1 Authenticate via 1:1 Matching .....	47
6.6.2 Authenticate via 1:N Matching .....	48
6.6.3 Authenticate via 1:1 Matching and 1:N Matching .....	48
6.7 System Settings .....	48
6.7.1 Set Basic Parameters .....	48
6.7.2 Set Face Picture Parameters .....	50
6.7.3 Set Fingerprint Parameters .....	53
6.7.4 Set Time .....	54
6.8 Time and Attendance Status Settings .....	54
6.8.1 Disable Attendance Mode via Device .....	54
6.8.2 Set Manual Attendance via Device .....	55
6.8.3 Set Auto Attendance via Device .....	56
6.8.4 Set Manual and Auto Attendance via Device .....	57

6.9 Set Access Control Parameters .....	59
6.10 Maintenance .....	60
6.10.1 Upgrade Firmware .....	60
6.10.2 Data Management .....	61
6.10.3 Log Query .....	62
6.11 View System Information .....	63
6.12 Two-Way Audio .....	65
6.12.1 Call Client Software from Device .....	65
6.12.2 Call Main Station from Device .....	65
6.12.3 Call Device from Client Software .....	66
6.12.4 Call Indoor Station from Device .....	66
<b>Chapter 7 Client Software Configuration .....</b>	<b>68</b>
7.1 Configuration Flow of Client Software .....	68
7.2 Device Management .....	68
7.2.1 Add Device .....	69
7.2.2 Reset Device Password .....	76
7.3 Group Management .....	77
7.3.1 Add Group .....	77
7.3.2 Import Resources to Group .....	77
7.3.3 Edit Resource Parameters .....	78
7.3.4 Remove Resources from Group .....	78
7.4 Person Management .....	79
7.4.1 Add Organization .....	79
7.4.2 Configure Basic Information .....	79
7.4.3 Issue a Card to One Person .....	80
7.4.4 Upload a Face Photo from Local PC .....	81
7.4.5 Take a Photo via Client .....	82
7.4.6 Collect Face via Access Control Device .....	82

7.4.7 Collect Fingerprint via Client .....	83
7.4.8 Collect Fingerprint via Access Control Device .....	84
7.4.9 Configure Access Control Information .....	84
7.4.10 Customize Person Information .....	86
7.4.11 Configure Resident Information .....	86
7.4.12 Configure Additional Information .....	87
7.4.13 Import and Export Person Identify Information .....	87
7.4.14 Import Person Information .....	87
7.4.15 Import Person Pictures .....	88
7.4.16 Export Person Information .....	88
7.4.17 Export Person Pictures .....	89
7.4.18 Delete Registered Pictures .....	89
7.4.19 Get Person Information from Access Control Device .....	90
7.4.20 Move Persons to Another Organization .....	90
7.4.21 Issue Cards to Persons in Batch .....	90
7.4.22 Report Card Loss .....	91
7.4.23 Set Card Issuing Parameters .....	91
7.5 Configure Schedule and Template .....	92
7.5.1 Add Holiday .....	93
7.5.2 Add Template .....	93
7.6 Set Access Group to Assign Access Authorization to Persons .....	95
7.7 Configure Advanced Functions .....	96
7.7.1 Configure Device Parameters .....	96
7.7.2 Configure Remaining Open/Closed .....	102
7.7.3 Configure Multi-Factor Authentication .....	103
7.7.4 Configure Card Reader Authentication Mode and Schedule .....	105
7.7.5 Configure First Person In .....	107
7.7.6 Configure Anti-Passback .....	108

7.7.7 Configure Other Parameters .....	109
7.8 Configure Linkage Actions for Access Control .....	115
7.8.1 Configure Client Actions for Access Event .....	115
7.8.2 Configure Device Actions for Access Event .....	116
7.8.3 Configure Device Actions for Card Swiping .....	117
7.8.4 Configure Device Actions for Person ID .....	119
7.9 Door Control .....	120
7.9.1 Control Door Status .....	120
7.9.2 Check Real-Time Access Records .....	121
7.10 Event Center .....	122
7.10.1 Enable Receiving Event Notification from Devices .....	122
7.10.2 View Real-Time Events .....	122
7.10.3 Search Historical Events .....	123
7.11 Time and Attendance .....	127
7.11.1 Configure Attendance Parameters .....	127
7.11.2 Add Timetable .....	132
7.11.3 Add Shift .....	135
7.11.4 Manage Shift Schedule .....	137
7.11.5 Manually Correct Check-in/out Record .....	140
7.11.6 Add Leave and Business Trip .....	141
7.11.7 Calculate Attendance Data .....	142
7.11.8 Attendance Statistics .....	143
7.12 Remote Configuration (Web) .....	145
7.12.1 Check Device Information .....	145
7.12.2 Edit Device Name .....	146
7.12.3 Edit Time .....	146
7.12.4 Set System Maintenance .....	146
7.12.5 Configure RS-485 Parameters .....	147

7.12.6 Manage User .....	148
7.12.7 Set Security .....	148
7.12.8 Configure Network Parameters .....	148
7.12.9 Configure Advanced Network .....	149
7.12.10 Configure Wi-Fi .....	149
7.12.11 Configure SIP Parameters .....	149
7.12.12 Configure Face Picture Parameters .....	150
7.12.13 Configure Supplement Light Parameters .....	151
7.12.14 Set Room No. ....	151
7.12.15 Configure Video and Audio Parameters .....	152
7.12.16 Configure Volume Input or Output .....	152
7.12.17 View Relay Status .....	152
<b>Appendix A. Tips for Scanning Fingerprint .....</b>	<b>153</b>
<b>Appendix B. Tips When Collecting/Comparing Face Picture .....</b>	<b>155</b>
<b>Appendix C. Tips for Installation Environment .....</b>	<b>157</b>
<b>Appendix D. Relationship between Wake-up Distance and Environment .....</b>	<b>158</b>
<b>Appendix E. Dimension .....</b>	<b>159</b>

# Chapter 1 Overview

## 1.1 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, etc.

## 1.2 Features

### 1.2.1 Features (Normal Series)

- 7-inch LCD touch screen
- 2 MP wide-angle dual-lens
- Adjusts supplement light brightness manually
- Face recognition distance: 0.3 m to 1.5 m
- Suggested height for face recognition: between 1.4 m and 1.9 m
- Deep learning algorithm
- 6,000 face capacity, 5,000 fingerprint capacity, and 10,000 event capacity
- Multiple authentication modes
- Face recognition duration  $\leq 0.5$  s/User; face recognition accuracy rate  $\geq 99\%$
- Device parameters management, search, and settings
- Imports card and user data to the device via TCP/IP communication or USB flash drive
- Stand-alone operation
- Transmits data to the client software via TCP/IP communication and saves the data on the client software
- Capture linkage and captured pictures saving
- Imports data to the device from the client software
- Manage, search and set device data after logging in the device locally
- Connects to one external card reader or access controller via RS-485 protocol
- Connects to external access controller or Wiegand card reader via Wiegand protocol
- Connects to secure door control unit via RS-485 protocol to avoid the door opening when the terminal is destroyed
- Two-way audio with client software, door station, indoor station, and main station
- Automatic network replenishment (ANR)
- Remote live view via RTSP protocol; encoding mode: H.264
- NTP, manually time synchronization, and auto synchronization
- Audio prompt
- Watchdog design and tamper function
- NFC tag anti-cloning

## 1.2.2 Features (P Series)

- 7-inch LCD touch screen
- 2 MP wide-angle dual-lens
- Adjusts supplement light brightness manually
- Face recognition in dark environment
- Face recognition distance: 0.3 m to 1.5 m
- Suggested height for face recognition: between 1.4 m and 1.9 m
- Deep learning algorithm
- 10,000 face capacity, 5,000 fingerprint capacity, and 50,000 event capacity
- Multiple authentication modes
- Face recognition duration  $\leq 0.5$  s/User; face recognition accuracy rate  $\geq 99\%$
- Device parameters management, search, and settings
- Stand-alone operation
- Transmits data to the client software via TCP/IP communication and saves the data on the client software
- Capture linkage and captured pictures saving
- Imports data to the device from the client software
- Manage, search and set device data after logging in the device locally
- Connects to one external card reader or access controller via RS-485 protocol
- Connects to external access controller or Wiegand card reader via Wiegand protocol
- Connects to secure door control unit via RS-485 protocol to avoid the door opening when the terminal is destroyed
- Two-way audio with client software, door station, indoor station, and main station
- Automatic network replenishment (ANR)
- Remote live view via RTSP protocol; encoding mode: H.264
- NTP, manually time synchronization, and auto synchronization
- Audio prompt
- Watchdog design and tamper function
- NFC tag anti-cloning

## 1.2.3 Features (T Series)

- 7-inch LCD touch screen
- 2 MP wide-angle dual-lens
- Adjusts supplement light brightness manually
- Face recognition in dark environment
- Face recognition distance: 0.3 m to 1.5 m
- Suggested height for face recognition: between 1.4 m and 1.9 m
- Deep learning algorithm
- 50,000 face capacity, 5,000 fingerprint capacity, and 50,000 event capacity
- Multiple authentication modes

## Face Recognition Terminal User Manual

---

- Face recognition duration  $\leq 0.5$  s/User; face recognition accuracy rate  $\geq 99\%$
- Device parameters management, search, and settings
- Imports card and user data to the device via TCP/IP communication or USB flash drive
- Stand-alone operation
- Transmits data to the client software via TCP/IP communication and saves the data on the client software
- Capture linkage and captured pictures saving
- Imports data to the device from the client software
- Manage, search and set device data after logging in the device locally
- Connects to one external card reader or access controller via RS-485 protocol
- Connects to external access controller or Wiegand card reader via Wiegand protocol
- Connects to secure door control unit via RS-485 protocol to avoid the door opening when the terminal is destroyed
- Two-way audio with client software, door station, indoor station, and main station
- Automatic network replenishment (ANR)
- Remote live view via RTSP protocol; encoding mode: H.264
- NTP, manually time synchronization, and auto synchronization
- Audio prompt
- Watchdog design and tamper function
- NFC tag anti-cloning

## Chapter 2 Appearance

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

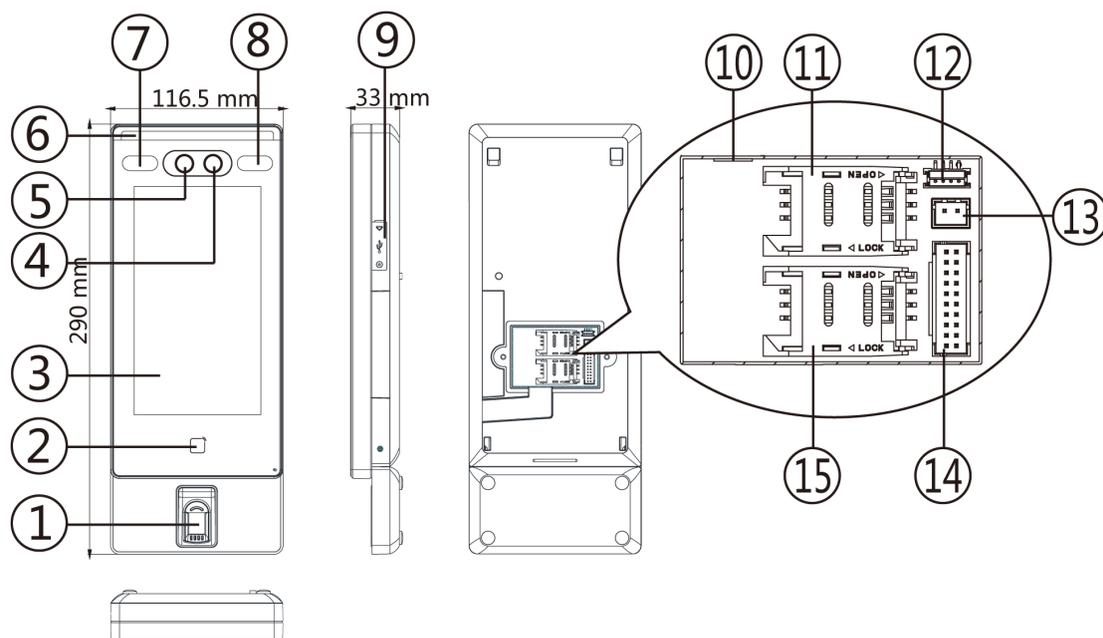


Figure 2-1 Face Recognition Terminal Diagram

Table 2-1 Description of Face Recognition Terminal

No.	Name	Description
1	Fingerprint Module	For fingerprint recognition.  <b>Note</b> Only parts of models support fingerprint recognition function.
2	Card Swiping Area	Swipe card within this area.
3	Display Screen	7-inch LCD touch screen.
4	Camera (IR Light)	IR light camera for recording or capturing videos or pictures in IR light.
5	Camera (White Light)	White light camera for recording or capturing white light videos or pictures.
6	Supplement Light (White Light)	Supplement light for white light camera.

## Face Recognition Terminal User Manual

---

No.	Name	Description
7	Supplement Light (IR Light)	Supplement light for IR camera.
8	Supplement Light (IR Light)	Supplement light for IR camera.
9	USB Interface	Connect to USB flash drive.
10	Network Interface	Connect to Ethernet.
11	SIM Card Slot	Reserved
12	Debugging Port	The debug terminal is used for debugging only.
13	Power Interface	Connect to power supply.
14	Wiring Terminals	Connect to other external devices, including RS-485 card reader, Wiegand card reader, door lock, alarm input, alarm output, etc.
15	PSAM Card Slot	Reserved

## Chapter 3 Installation

### 3.1 Installation Environment

- If installing the device indoors, the device should be at least 2 meters away from the light, and at least 3 meters away from the window or the door.
- If installing the device outdoors, you should apply Silicone sealant among the cable wiring area to keep the raindrop from entering.
- Make sure the environment illumination is more than 100 Lux.

---

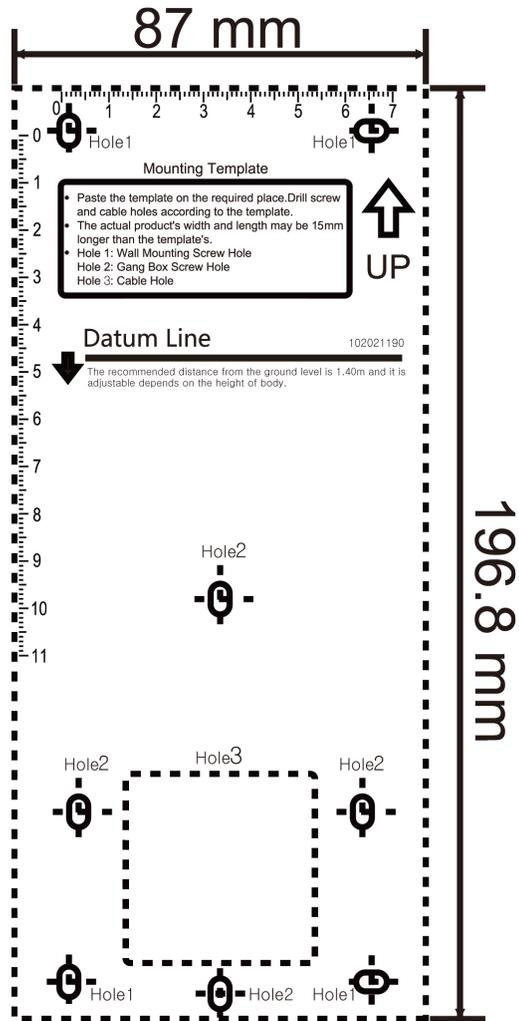
 **Note**

- For details about installation environment, see *Tips for Installation Environment*.
  - Make sure the output of external power supply fulfils LPS.
- 

### 3.2 Install with Gang Box

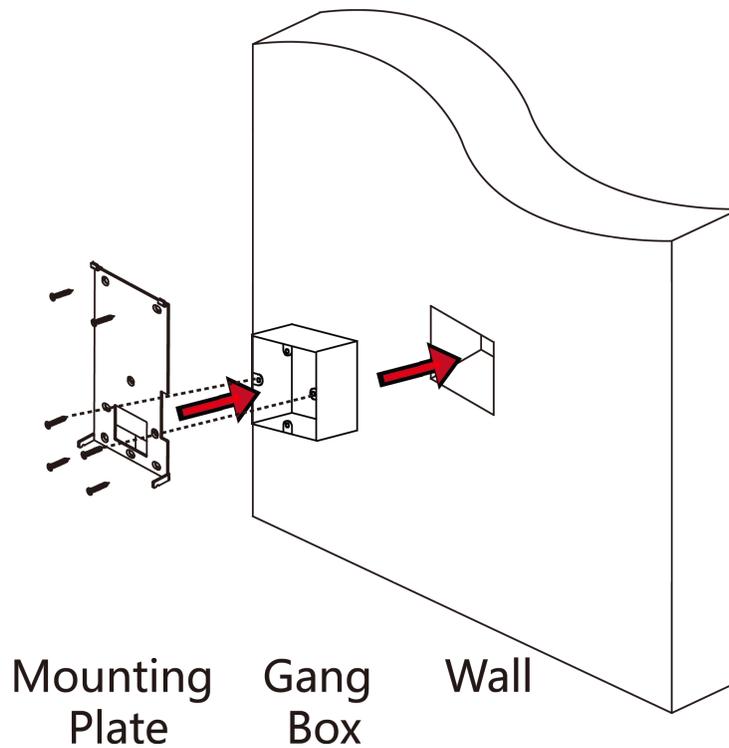
#### Steps

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.



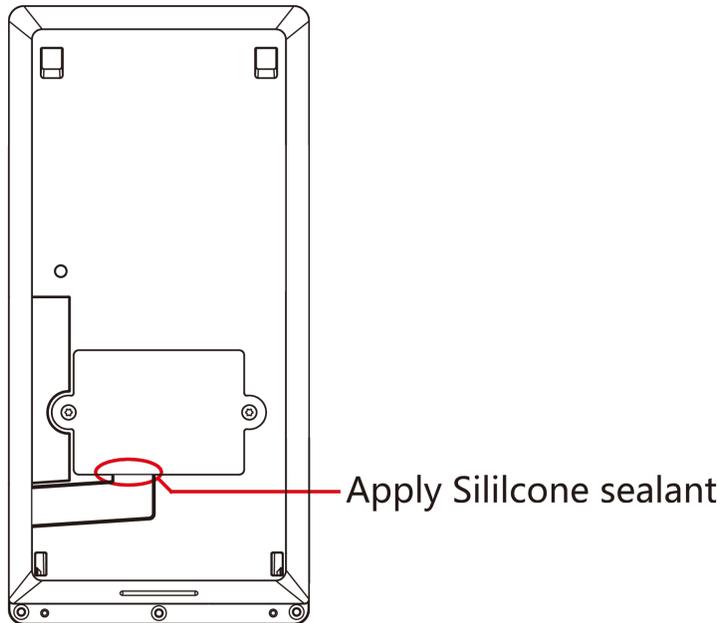
**Figure 3-1 Mounting Template**

2. Drill holes on the wall or other surface according to the mounting template and install the gang box.
3. Use two supplied screws (4\_KA4 × 22-SUS) to secure the mounting plate on the gang box.
4. Use another four supplied screws to secure the mounting plate on the wall.



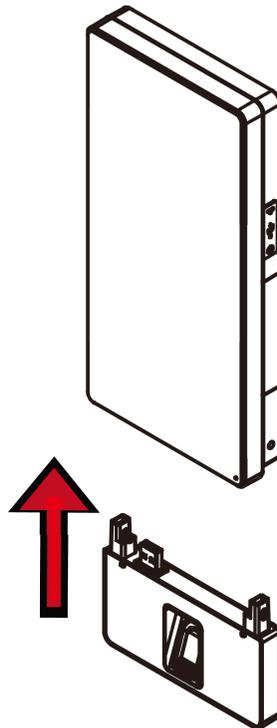
**Figure 3-2 Install Mounting Plate**

5. Remove the two screws on the rear panel and remove the sheet to display the wiring terminals.
6. Route the cable through the cable hole of the mounting plate, and connect to corresponding external devices' cables.
7. Install the sheet back to the device with the two screws.
8. Apply Silicone sealant among the cable wiring area to keep the raindrop from entering.



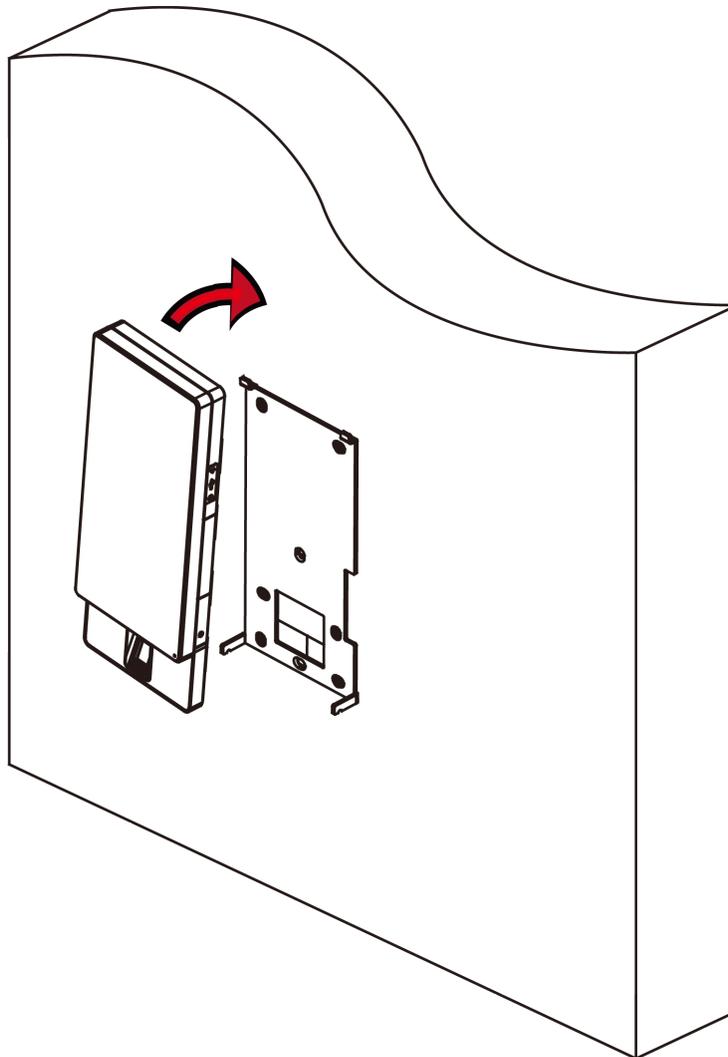
**Figure 3-3 Apply Silicone Sealant**

**9. Optional:** Insert the fingerprint module to the holes at the bottom of the main part.



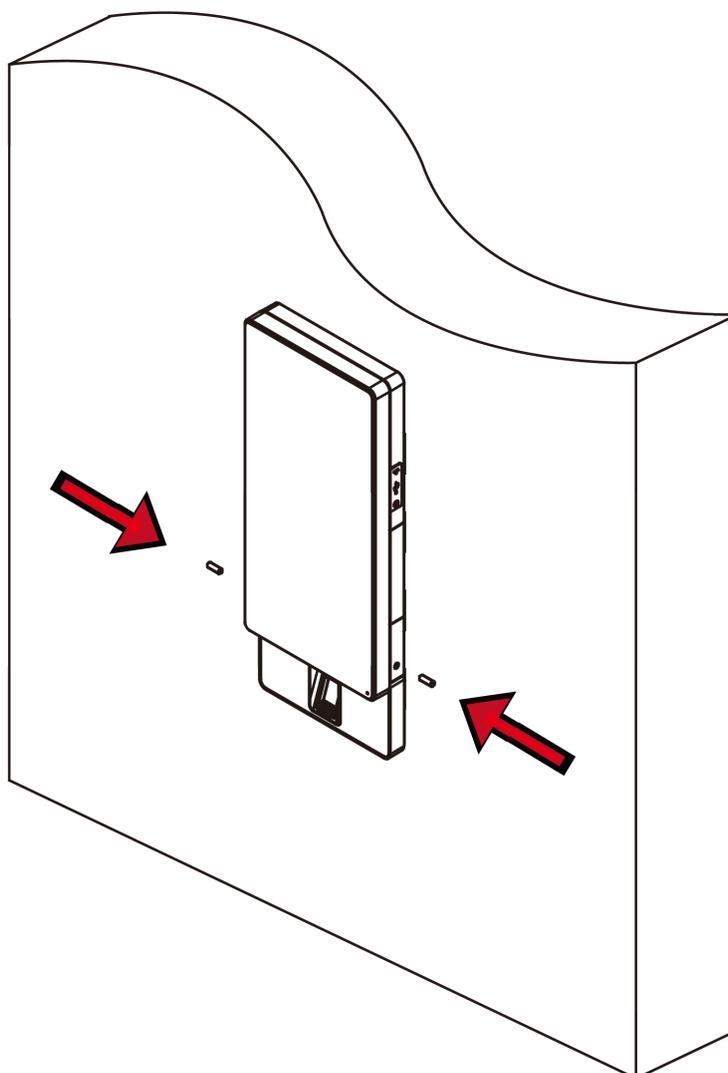
**Figure 3-4 Insert Fingerprint Module**

**10.** Align the device with the mounting plate and hang the device on the mounting plate.



**Figure 3-5 Install Device**

- 11.** Use two supplied screws (SC-M4 × 12TP10-SUS) to secure the device and the mounting plate.



**Figure 3-6 Secure Device**

---

**Note**

- The installation height here is the recommended height. You can change it according to your actual needs.
  - For easy installation, drill holes on mounting surface according to the supplied mounting template.
-

## 3.3 Install without 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.

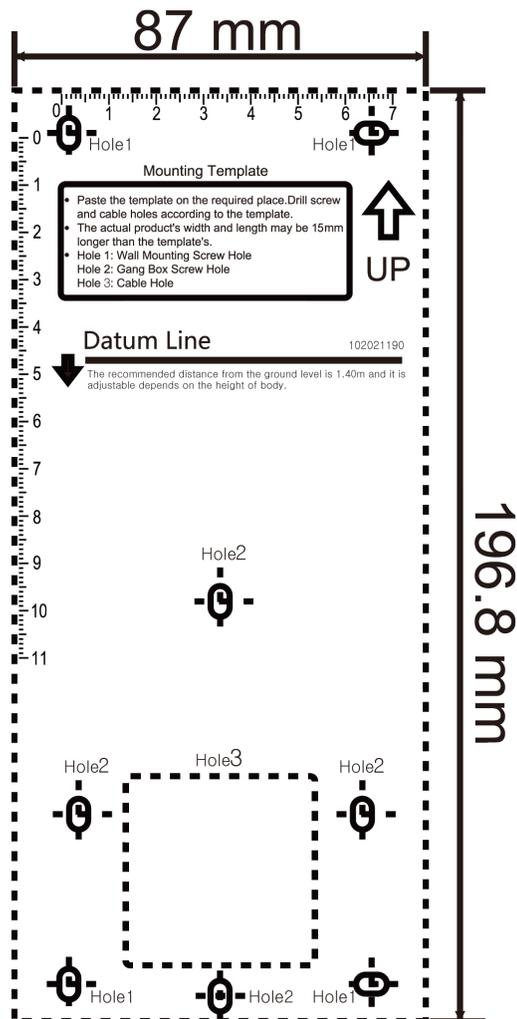
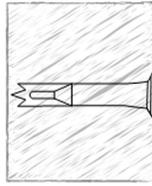


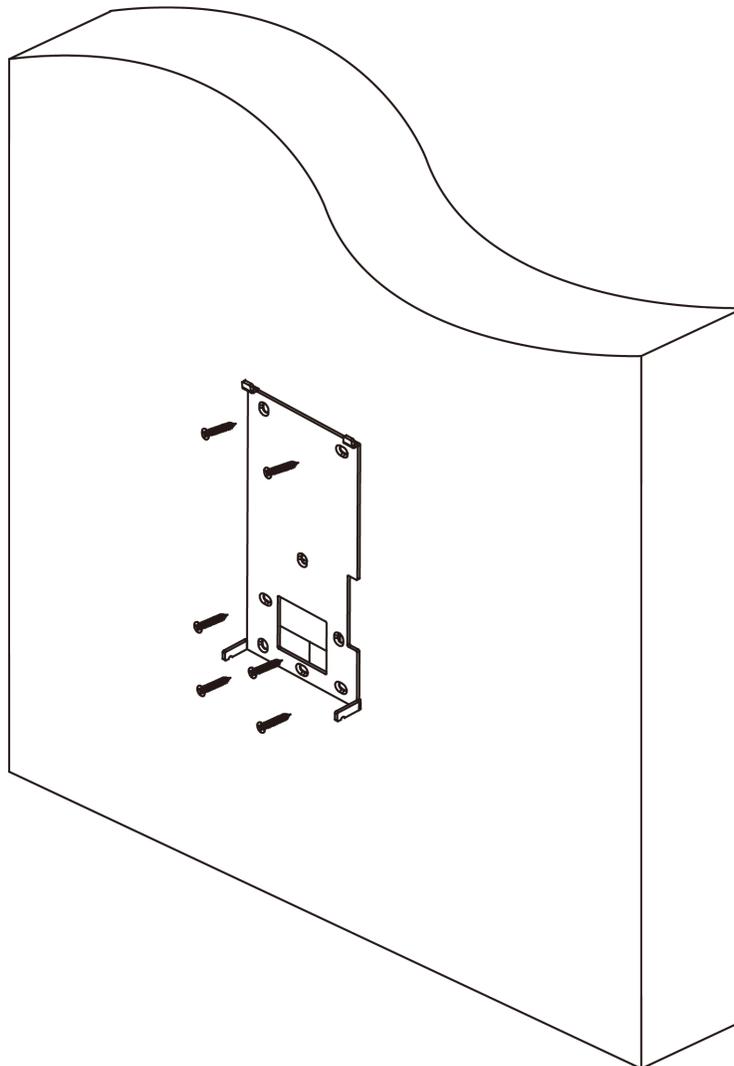
Figure 3-7 Mounting Template

2. Drill 6 holes on the wall or other surface according to Hole 1 and Hole 2 in the mounting template.
3. Insert the screw sockets of the setscrews in the drilled holes.



**Figure 3-8 Insert Screw Socket**

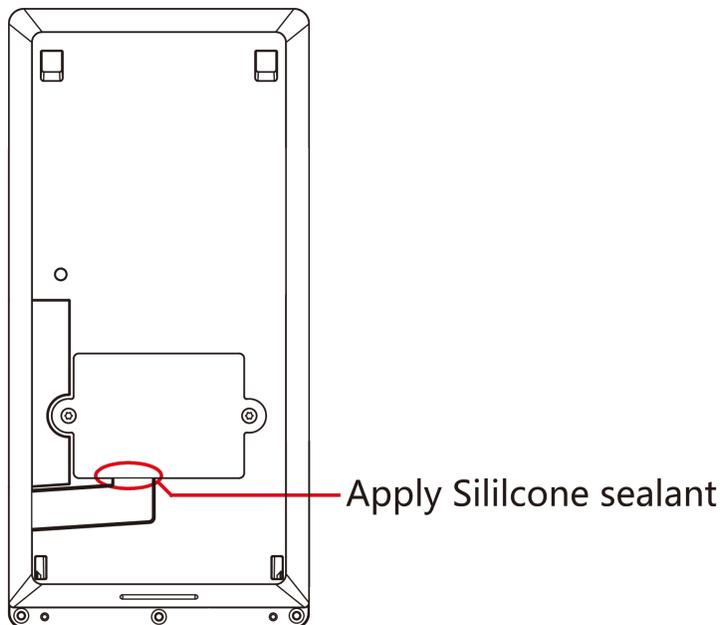
4. Align the 6 holes to the mounting plate with the drilled holes.



**Figure 3-9 Install Mounting Plate**

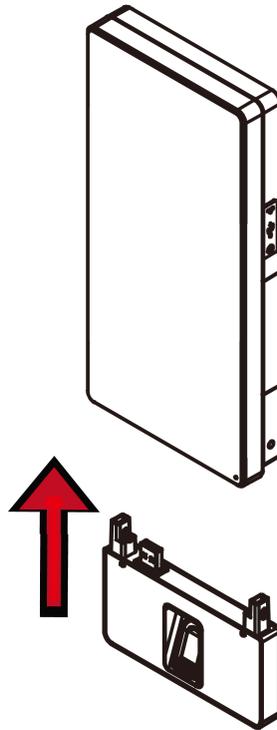
5. Remove the two screws on the rear panel and remove the sheet to display the wiring terminals.
6. Route the cable through the cable hole of the mounting plate, and connect to corresponding external devices' cables.

7. Install the sheet back to the device with the two screws.
8. Apply Silicone sealant among the cable wiring area to keep the raindrop from entering.



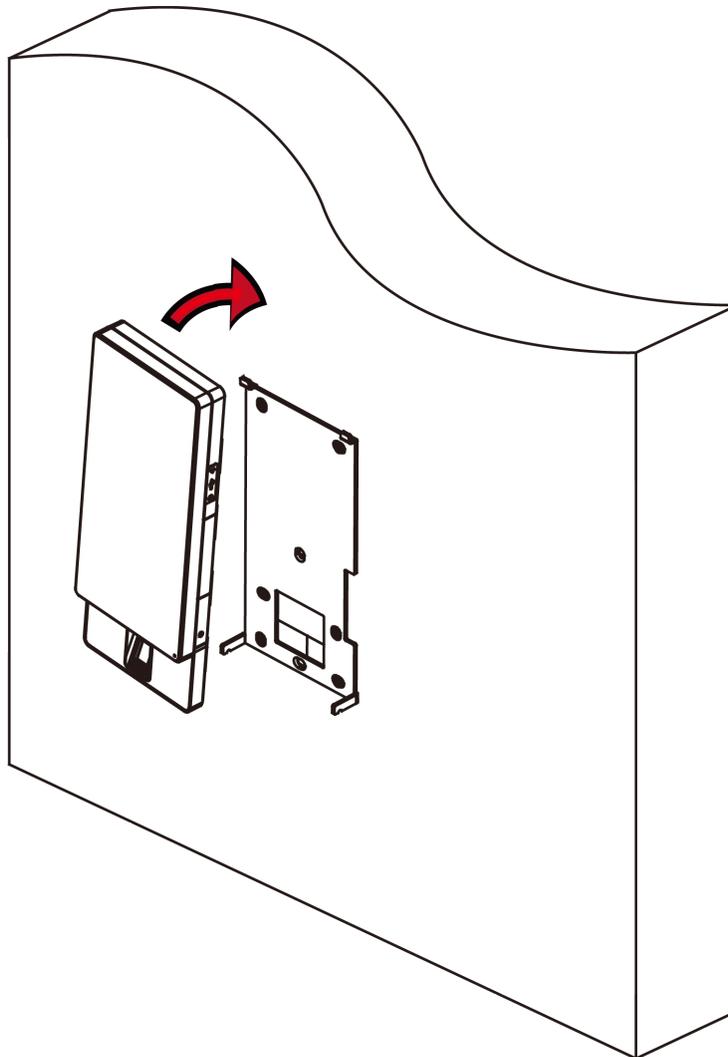
**Figure 3-10 Apply Silicone Sealant**

9. Insert the fingerprint module to the holes at the bottom of the main part.



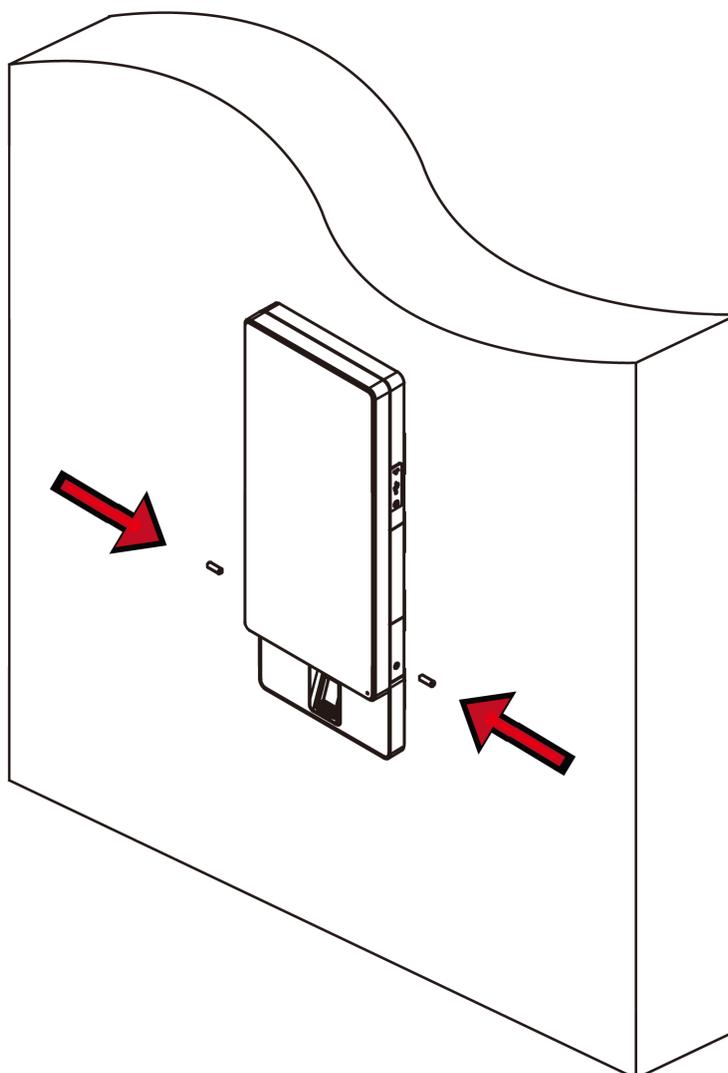
**Figure 3-11 Install Fingerprint Module**

- 10.** Align the device with the mounting plate and hang the device on the mounting plate.



**Figure 3-12 Install Device**

- 11.** Use two supplied screws (SC-M4 × 12TP10-SUS) to secure the device and the mounting plate.



**Figure 3-13 Secure Device**

---

**Note**

- The installation height here is the recommended height. You can change it according to your actual needs.
  - For easy installation, drill holes on mounting surface according to the supplied mounting template.
-

## Chapter 4 Wiring

You can connect the RS-485 terminal with the RS-485 card reader, connect the NC and COM terminal with the door lock, connect the SENSOR terminal with the door contact, the BTN/GND terminal with the exit button, connect the alarm output and input terminal with the alarm output/input devices, and connect the Wiegand terminal with the Wiegand card reader or the access controller.

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 cable size is 18 AWG, you should use a 12 V power supply. And the distance between the power supply and the device should be no more than 20 m.
  - If the cable size is 15 AWG, you should use a 12 V power supply. And the distance between the power supply and the device should be no more than 30 m.
  - If the cable size is 12 AWG, you should use a 12 V power supply. And the distance between the power supply and the device should be no more than 40 m.
- 

### 4.1 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:

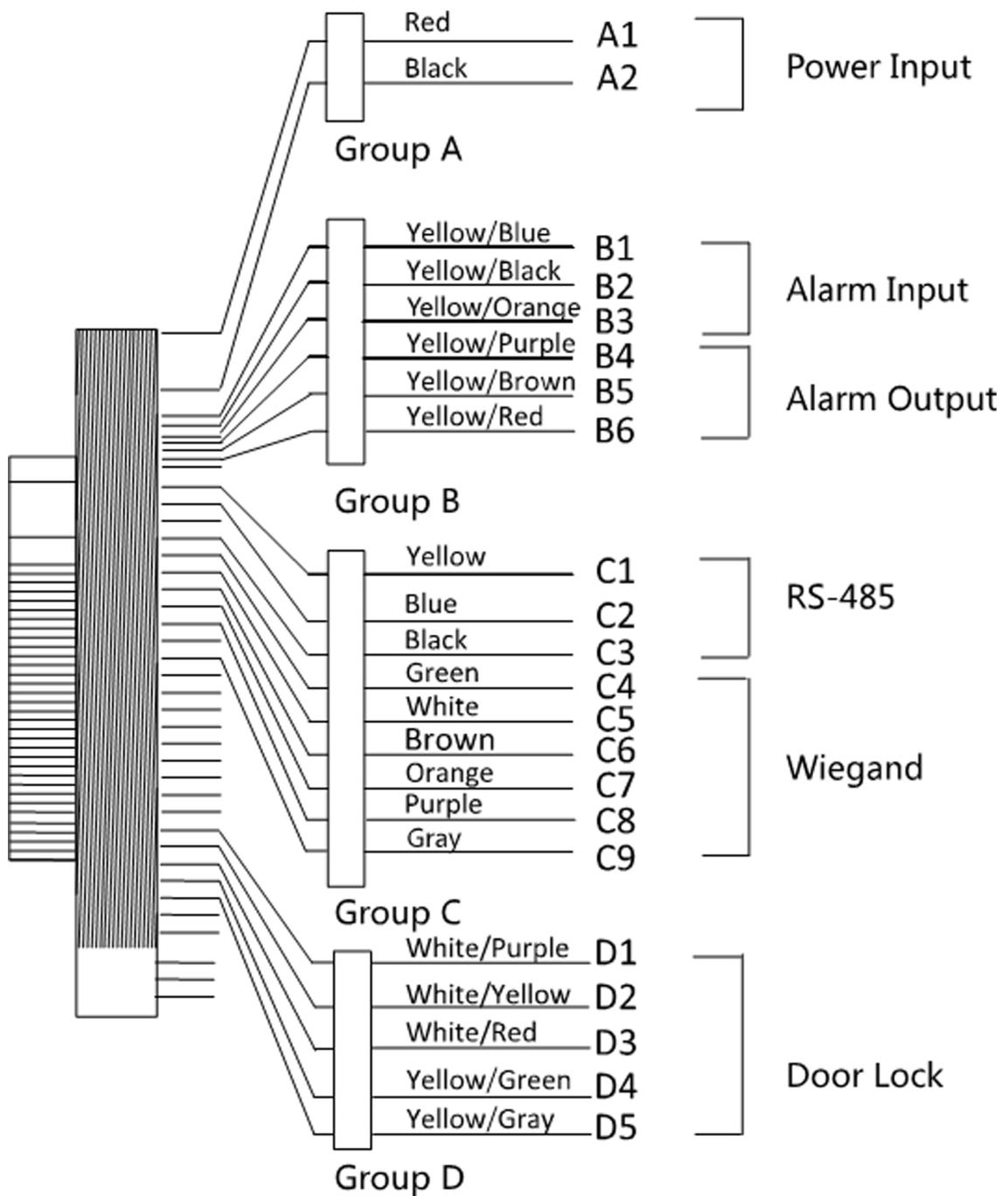


Figure 4-1 Terminal Diagram

The descriptions of the terminals are as follows:

**Table 4-1 Terminal Descriptions**

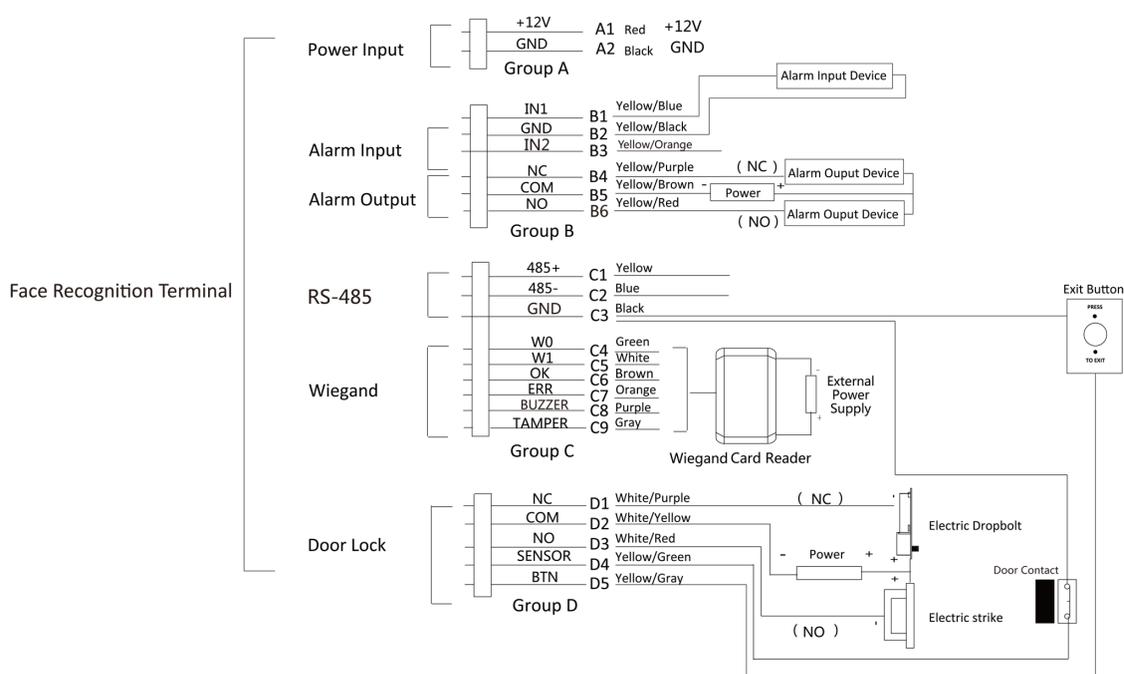
Group	No.	Function	Color	Name	Description
Group A	A1	Power Input	Red	+12 V	12 VDC Power Supply
	A2		Black	GND	Ground
Group B	B1	Alarm Input	Yellow/Blue	IN1	Alarm Input 1
	B2		Yellow/Black	GND	Ground
	B3		Yellow/Orange	IN2	Alarm Input 2
	B4	Alarm Output	Yellow/Purple	NC	Alarm Output Wiring
	B5		Yellow/Brown	COM	
	B6		Yellow/Red	NO	
Group C	C1	RS-485	Yellow	485+	RS-485 Wiring
	C2		Blue	485-	
	C3		Black	GND	
	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	Common
	D3		White/Red	NO	Lock Wiring (NO)

Group	No.	Function	Color	Name	Description
	D4		Yellow/Green	SENSOR	Door Contact
	D5		Yellow/Gray	BTN	Exit Door Wiring

## 4.2 Wire Normal Device

You can connect the terminal with normal peripherals.

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



**Figure 4-2 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 suggested external power supply for door lock is 12 V, 1 A. The suggested external power supply for the Wiegand card reader is 12 V, 1A.

- The suggested power cable's diameter: 22 AWG. The suggested other cable's diameter: 26 AWG.
- Do not wire the device to the electric supply directly.

## Warning

The face recognition terminal shall adapt an external listed Class 2 power supply with surge protected function.

## 4.3 Wire Secure Door Control Unit

You can connect the terminal with the secure door control unit.

The wiring diagram is as follows.

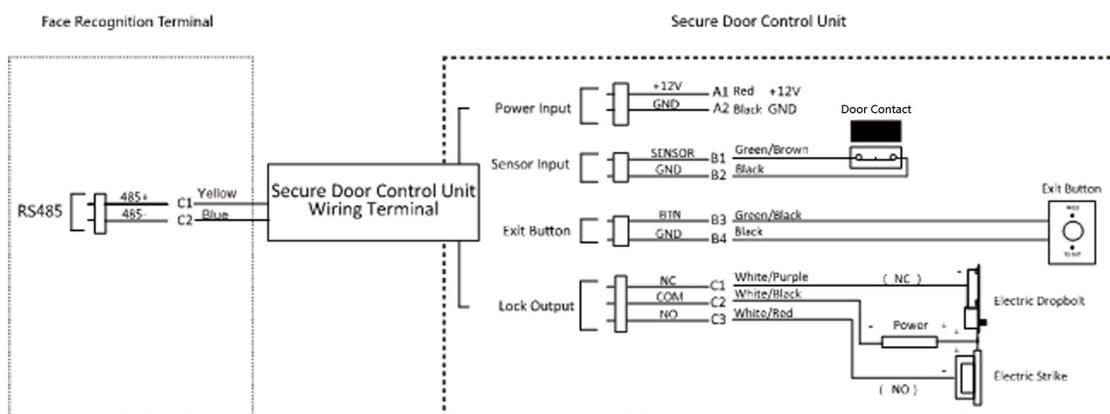


Figure 4-3 Secure Door Control Unit Wiring

## Note

The secure door control unit should connect to an external power supply separately. The suggested external power supply is 12V, 0.5A.

## Chapter 5 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

### 5.1 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 **Activate** and the device will activated.

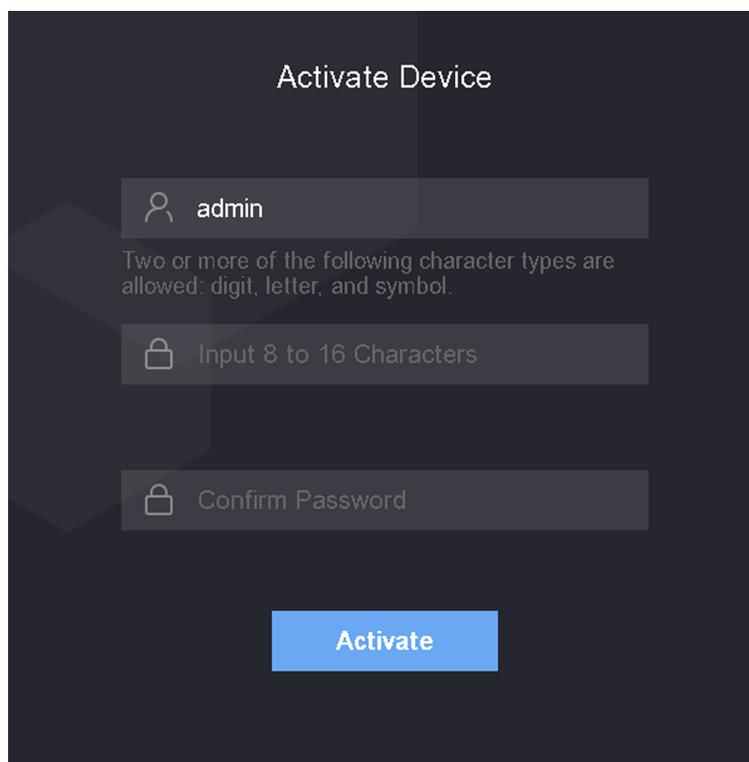


Figure 5-1 Activation Page

---

## **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.

---

- After activation, you should select an application mode. For details, see ***Set Application Mode***
- After activation, if you need to add the device to the client software or other platforms, you should edit the device IP address. For details, see *Communication Settings*.

## 5.2 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.

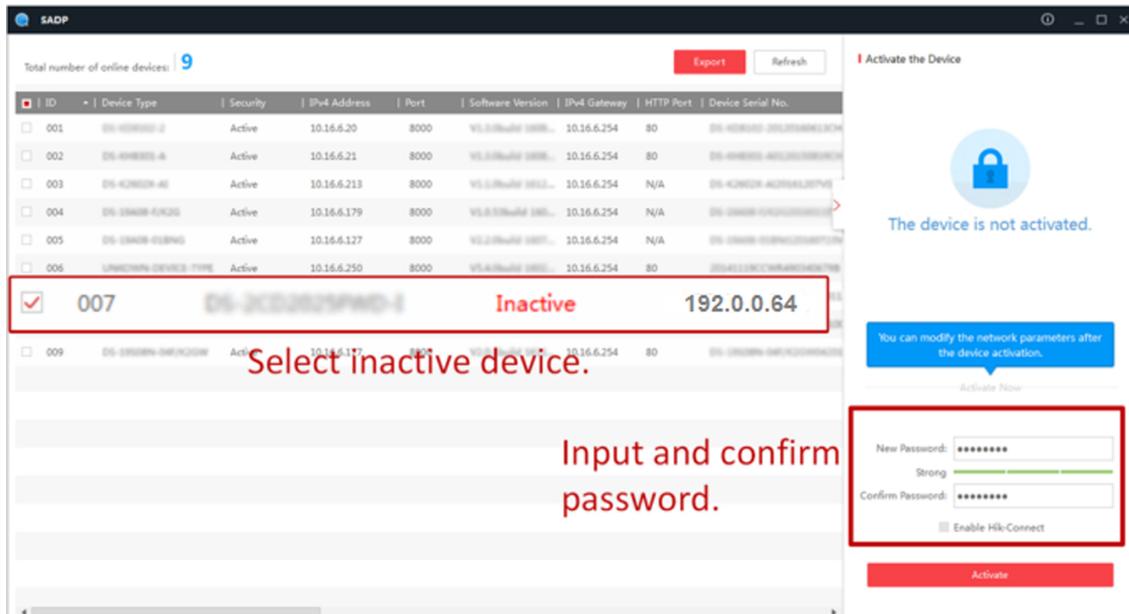
---

## **Note**

Characters containing admin and nimda are not supported to be set as activation password.

---

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.

## 5.3 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.

---



### Note

Characters containing admin and nimda are not supported to be set as activation password.

---

7. Click **OK** to activate the device.

## Chapter 6 Basic Operation

### 6.1 Set Application Mode

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

#### Steps

1. On the Welcome page, select **Indoor** or **Others** from the drop-down list.

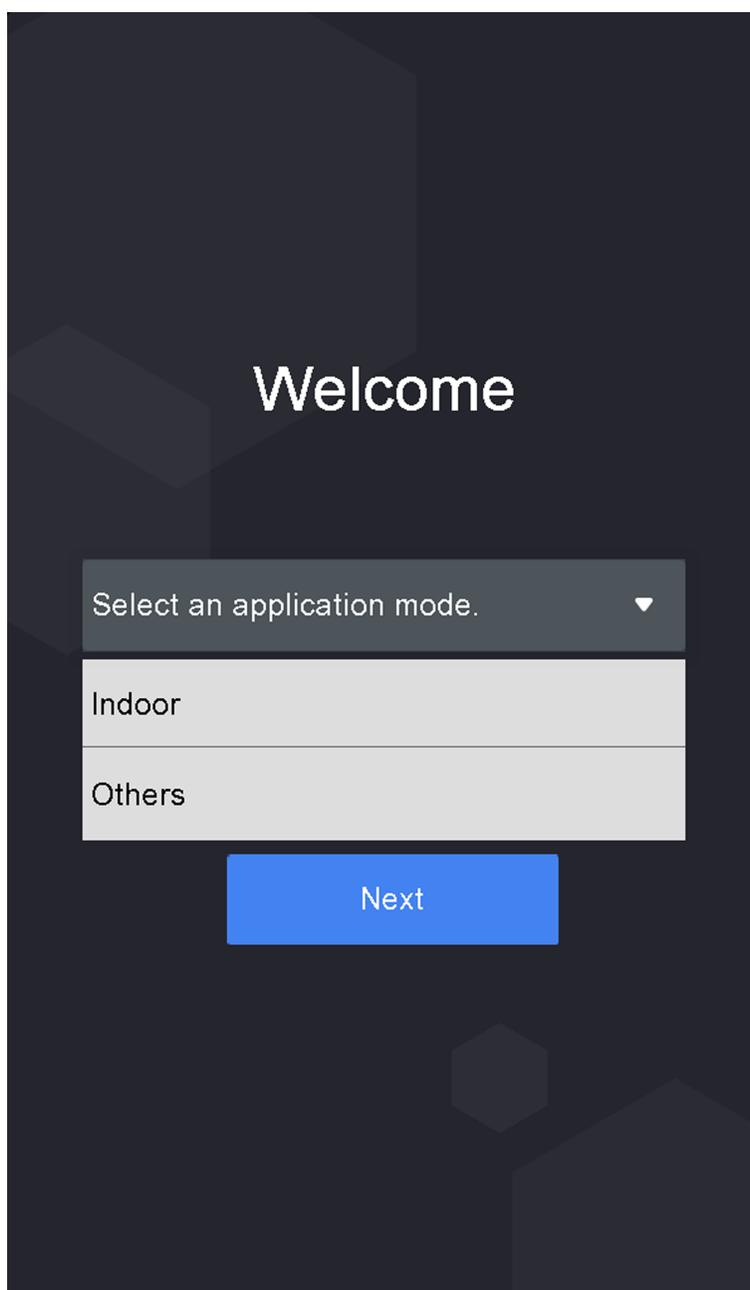


Figure 6-1 Welcome Page

2. Tap **OK** to save.

---

 **Note**

- You can also change the settings in *System Settings*.
- If you install the device indoors near the window or the face recognition function is not working well, select **Others**.

- If you do not configure the application mode and tap **Next**, the system will select **Indoor** by default.
  - If you activate the device via other tools remotely, the system will select **Indoor** as the application mode by default.
- 

## 6.2 Login

Login the device to set the device basic parameters. You should enter the device activation password for the first login. Or if you have add the administrator's credential, you can login via the configured credential.

### 6.2.1 Login For First Time

You should login the system before other device operations.

#### Steps

1. Long tap on the initial page for 3 s to enter password entering page.
2. Tap the Password field and enter the device activation password.
3. Tap **OK** 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*.
-

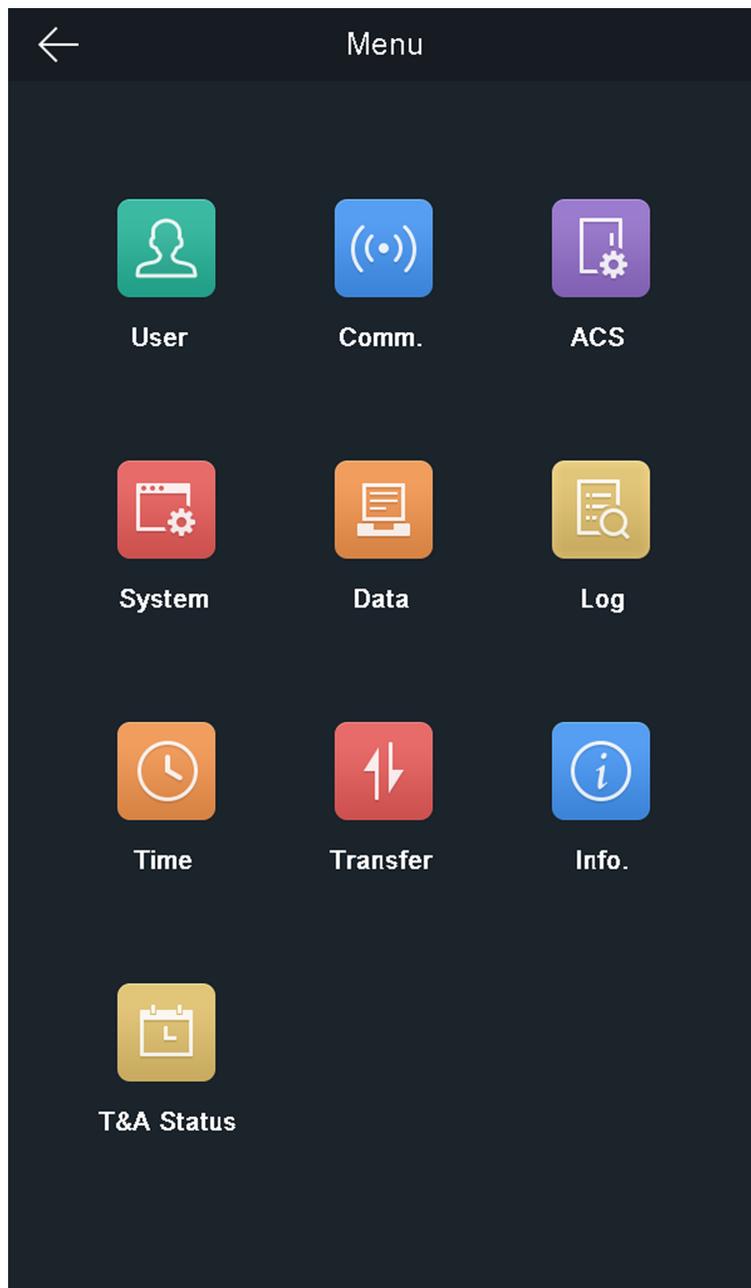


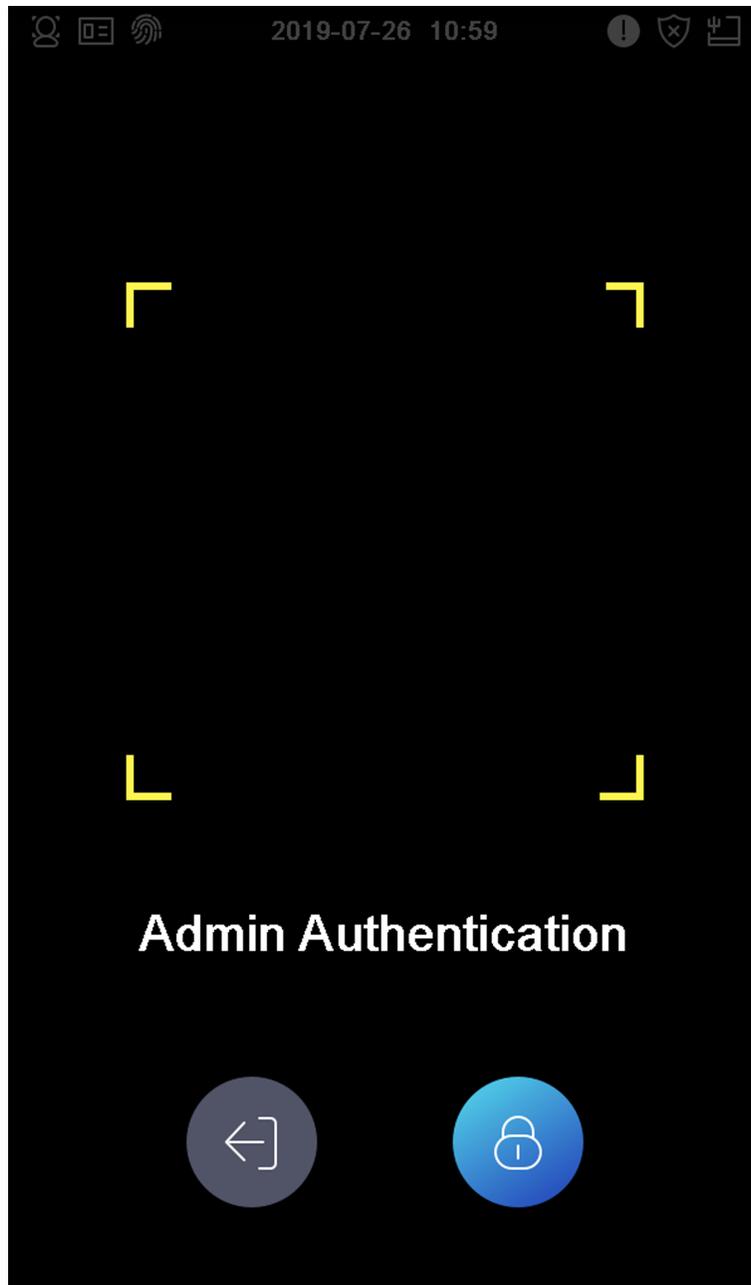
Figure 6-2 Home Page

### 6.2.2 Login by Administrator

After you add the administrator for the device, only the administrator can login the device for device operation.

## Steps

1. Long tap on the initial page for 3 s to enter the admin login page.



**Figure 6-3 Admin Login**

2. Authenticate the administrator's face, fingerprint, or card to enter the home page.

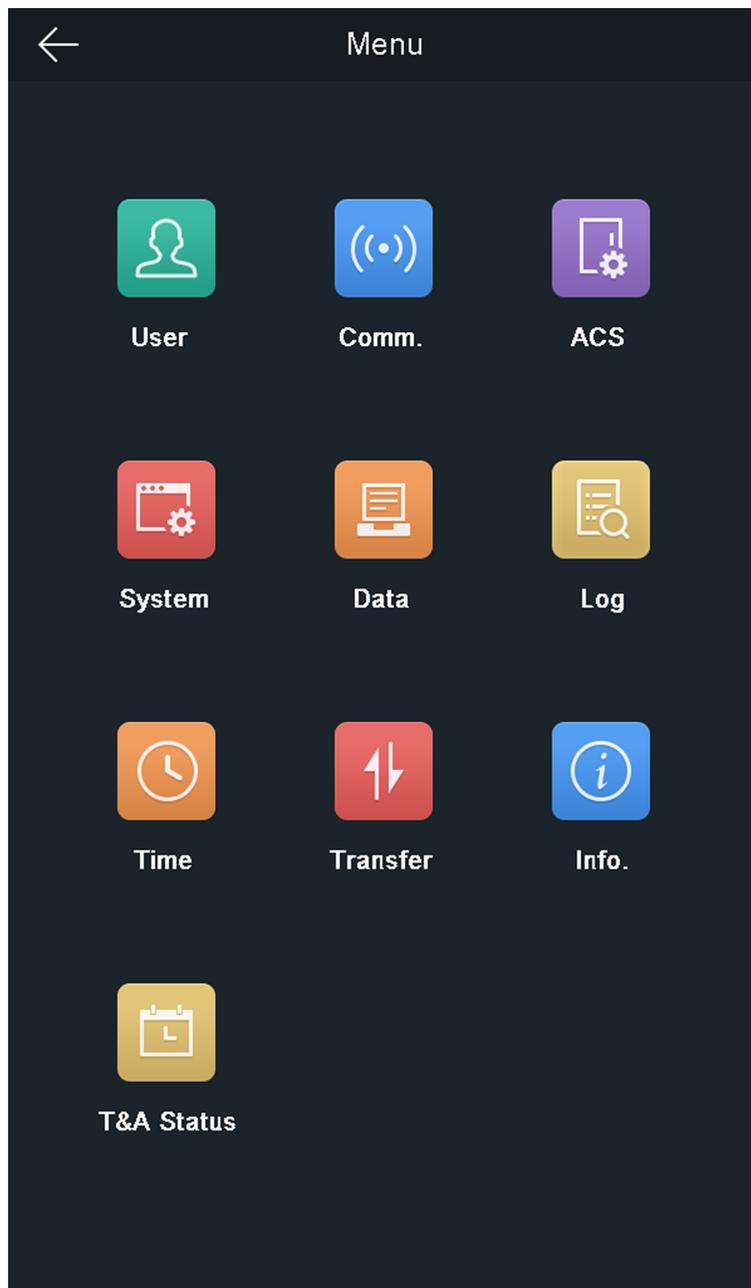


Figure 6-4 Home Page

---

 **Note**

The device will be locked for 30 minutes after 5 failed fingerprint or card attempts.

- 3. Optional:** Tap  and you can enter the device activation password for login.
- 4. Optional:** Tap  and you can exit the admin login page.

## 6.3 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.

### 6.3.1 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.

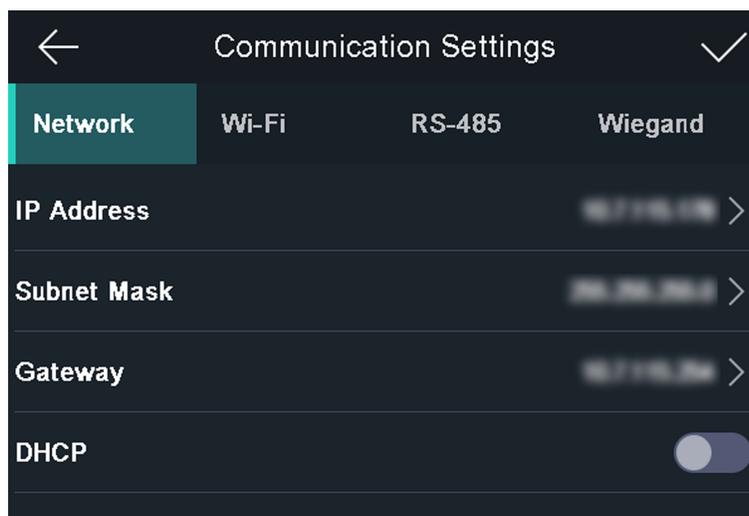


Figure 6-5 Network Settings

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.

### 6.3.2 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.

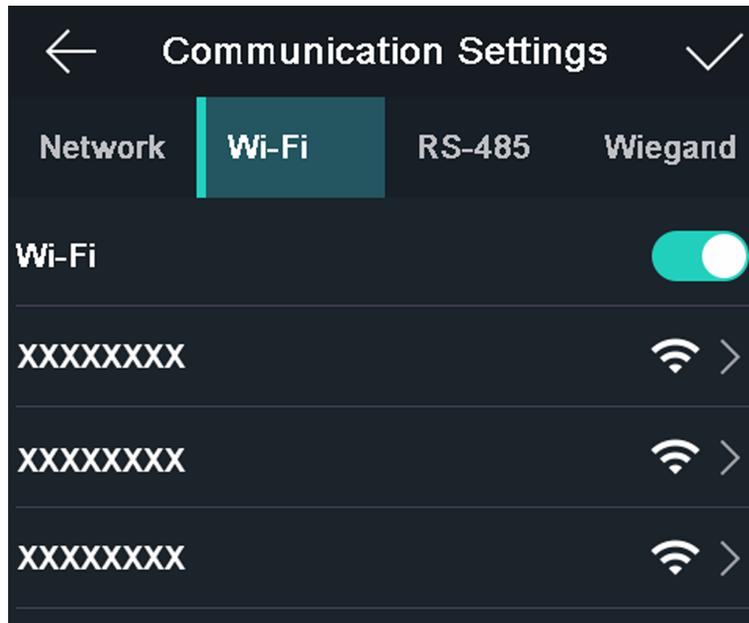


Figure 6-6 Wi-Fi Settings

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.

## 6.3.3 Set RS-485 Parameters

The face recognition terminal can connect external 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**

- Controller represents the access controller, Unit represents the secure door control unit and Reader represents the card reader.
- Set the RS-485 address as 2 if you need to connect an access controller or 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.

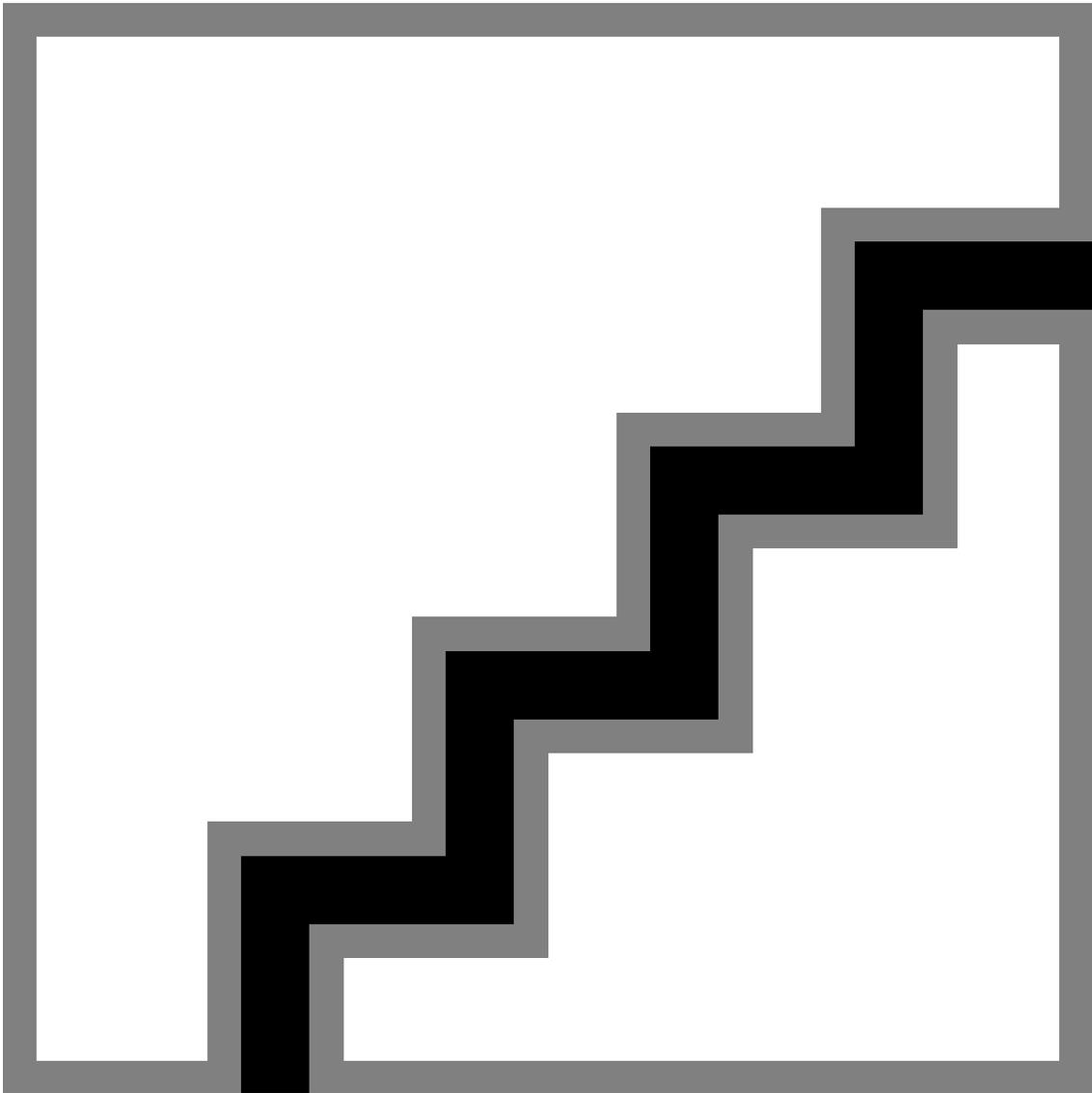
---

### 6.3.4 Set Wiegand Parameters

You can set the Wiegand transmission direction.

#### 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 6-7 Wiegand Settings**

3. Enable the Wiegand function.
4. Select a transmission direction.
  - 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.
  - Input: A face recognition terminal can connect a Wiegand card reader.
5. 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.

---

## 6.4 User Management

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

### 6.4.1 Add Administrator

The administrator can login the device backend and configure the device parameters.

#### Steps

1. Long tap on the initial page and log in the backend.
2. Tap **User** → **+** to enter the Add User page.
3. Edit the employee ID.

---

#### Note

- The employee ID should be less than 32 characters. And it can be a combination of lower letters, upper letters, and numbers.
- The employee ID should not be duplicated.

- 
4. 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.

- 
5. **Optional:** Add a face picture, fingerprints, cards, or password for the administrator.

---

#### Note

- For details about adding a face picture, see ***Add Face Picture*** .

-  Note

For details about adding a fingerprint, see ***Add Fingerprint*** .

- For details about adding a card, see ***Add Card*** .
- For details about adding a password, see ***Add Password*** .

- 
6. **Optional:** Set the administrator's authentication type.

---

#### Note

For details about setting the authentication type, see ***Set Authentication Mode*** .

- 
7. Enable 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.

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

9. Tap  to save the settings.

## 6.4.2 Add Face Picture

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

### Steps

---

#### Note

Up to 3000 face pictures can be added.

---

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

#### Note

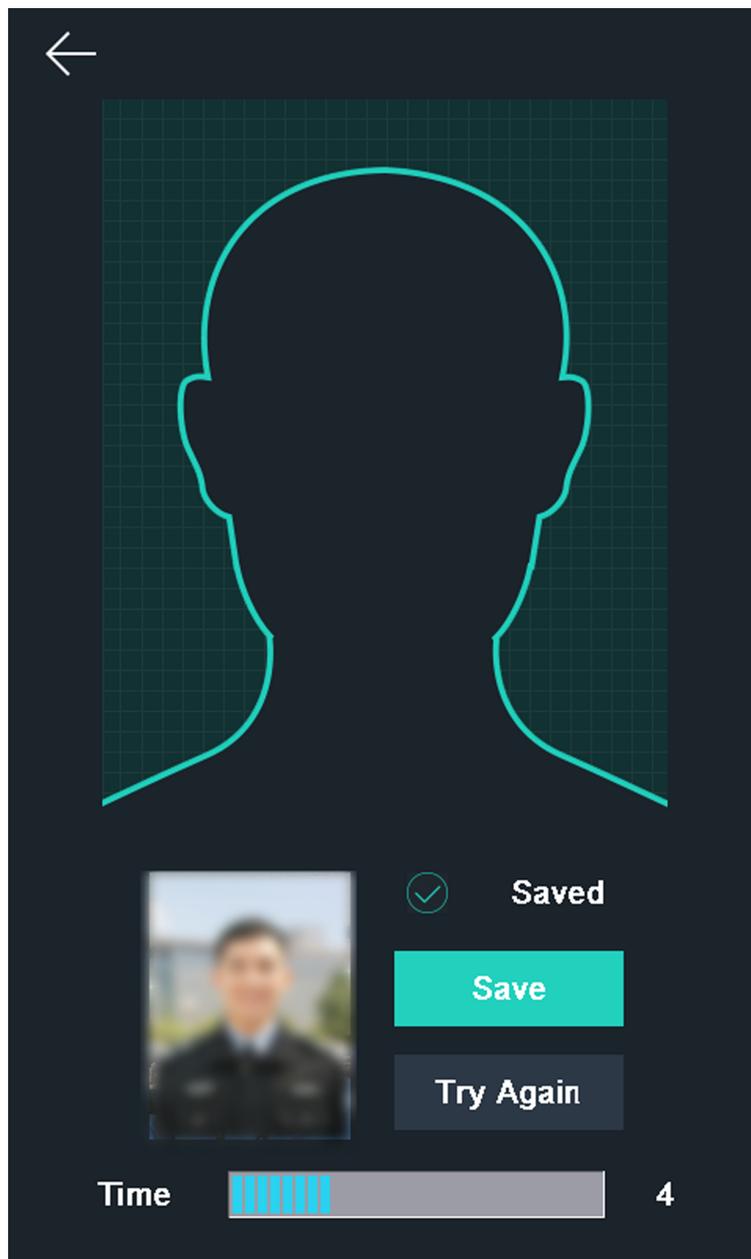
- The employee ID should be less than 32 characters. And it can be a combination of lower letters, upper letters, and numbers.
  - The employee ID should not start with 0 and should not be duplicated.
- 

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.



**Figure 6-8 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.

### 6.4.3 Add Fingerprint

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

#### Steps

---

### **Note**

- The function should be supported by the device.
  - Up to 5000 fingerprints can be added.
- 

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 less than 32 characters. And it can be a combination of lower letters, upper letters, and numbers.
  - 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.

### **6.4.4 Add Card**

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

#### **Steps**

### **Note**

Up to 5000 cards can be added.

---

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 less than 32 characters. And it can be a combination of lower letters, upper letters, and numbers.
  - 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.
- 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.

## **6.4.5 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 less than 32 characters. And it can be a combination of lower letters, upper letters, and numbers.
- 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.

## **6.4.6 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. Long tap on the initial page and login.
2. Tap **User → Add User/Edit User → Authentication Mode** .
3. 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.

4. Tap  to save the settings.

## **6.4.7 Search and Edit User**

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

## Search User

On the User Management page, Tap the search area 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 ***User Management*** to edit the user parameters. Tap  to save the settings.



The employee ID cannot be edited.

---

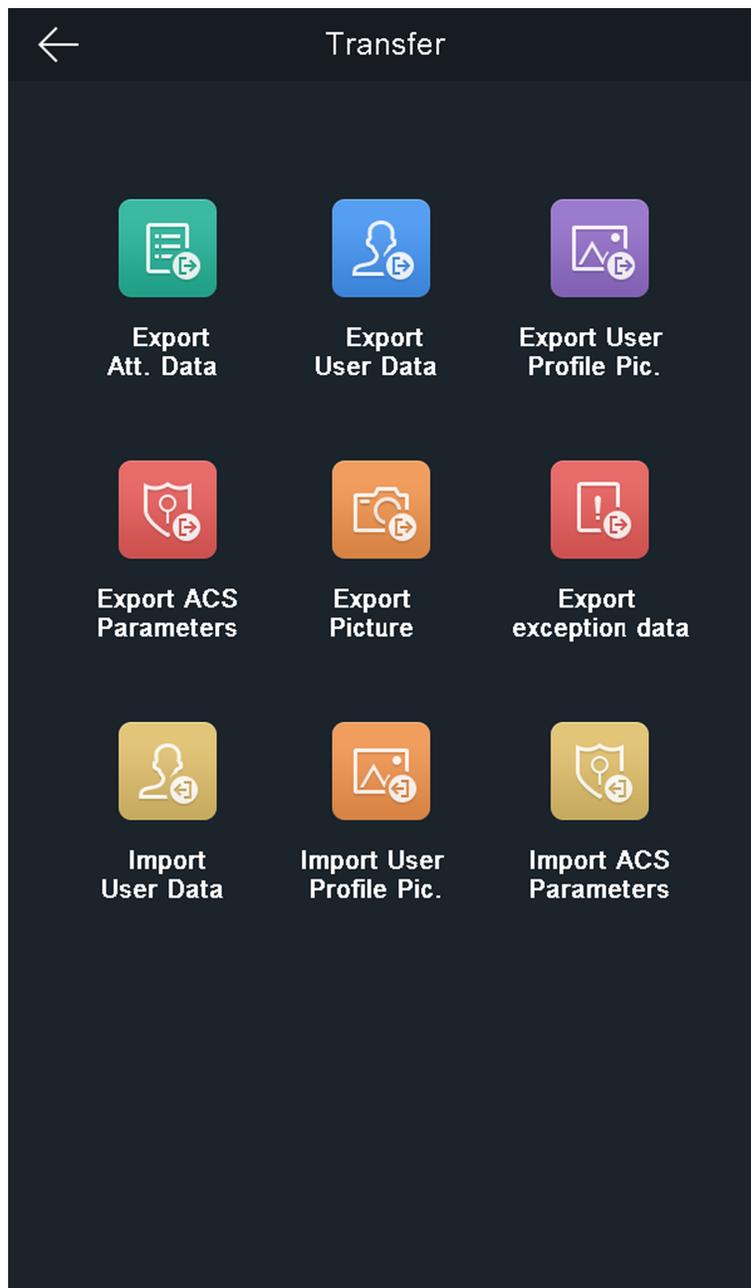
## 6.5 Import and Export Data

On the Transfer page, you can export the attendance data, the user data, the user picture, the access control parameter, the captured picture, and the exception data 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.

### 6.5.1 Export Data

#### Steps

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



**Figure 6-9 Transfer Page**

2. On the Transfer page, tap Export Att. Data, Export User Data, Export Face Pic., Export Access Control Param., or Export Captured Pic.
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 DB.
  - 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 DB file, which cannot be edited.
- 

## 6.5.2 Import Data

### Steps

1. Plug a USB flash drive in the device.
  2. On the Transfer page, tap Import User Data, Import Face Pic., or Import Access Control Param.
  3. Tap **Yes** on the pop-up window and the data will be imported from the USB flash drive to the device.
- 

 **Note**

- 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 data of model with T and without T cannot be transferred with each other.
  - The supported USB flash drive format is FAT32.
  - Under the normal mode (face recognition mode), the imported pictures should be saved in the folder (named enroll\_pic) of the root directory and the picture's name should be follow the rule below:  
Card No.\_Name\_Department\_Employee ID\_Gender.jpg
  - Under the normal mode (face recognition mode), if the folder enroll\_pic cannot save all imported pictures, you can create another folders, named enroll\_pic1, enroll\_pic2, enroll\_pic3, enroll\_pic4, under the root directory.
  - Under the deep mode (face recognition mode), the imported pictures should be exported pictures of another device.
  - The employee ID should be less than 32 characters. It can be a combination of lower letters, upper letters, and numbers. It should not be duplicated, and should not start with 0.
  - Requirements of face picture should follow the rules below: 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 640 × 480 pixel or more than of 640 × 480 pixel. The picture size should be between 60 KB and 200 KB.
-

## 6.6 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

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

### 6.6.1 Authenticate via 1:1 Matching

#### Steps

1. If the authentication mode is Card and Face, Card and Face and Fingerprint, swipe card in the card swiping area.

---

#### Note

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

2. Continue authentication.
  - If the authentication mode is Card and Face, position the face looking at the camera to authenticate face.
  - If the authentication mode is Card and Face and Fingerprint, after authenticating face completely, authenticate the fingerprint on the fingerprint module when the prompt "Continue to authenticate" pops up.

---

#### Note

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

---

If authentication succeeded, the prompt "Authenticated" will pop up.

## 6.6.2 Authenticate via 1:N Matching

If the authentication mode is Face, position the face looking at the camera to start face authentication.

If authentication completed, a prompt "Authenticated" will pop up.

## 6.6.3 Authenticate via 1:1 Matching and 1:N Matching

### Steps

1. If the authentication mode is Fingerprint and Face, authenticate fingerprint first according to the prompt on the device screen.

The device will compare the fingerprint with the fingerprint information in the device database (1:N Matching).

When authentication is completed, a prompt "Continue to authenticate" will pop up.

2. Front the face looking at the camera to start face authentication.



### Note

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

---

The device will compare the captured face picture with the user information gained from the last step (1:1 Matching).

When authentication completed, a prompt "Authenticated" will pop up.

## 6.7 System Settings

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

### 6.7.1 Set Basic Parameters

You can set the community No., building No., the unit No., voice prompt, voice volume, application mode, wake-up distance, IR light brightness, and white light brightness.

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

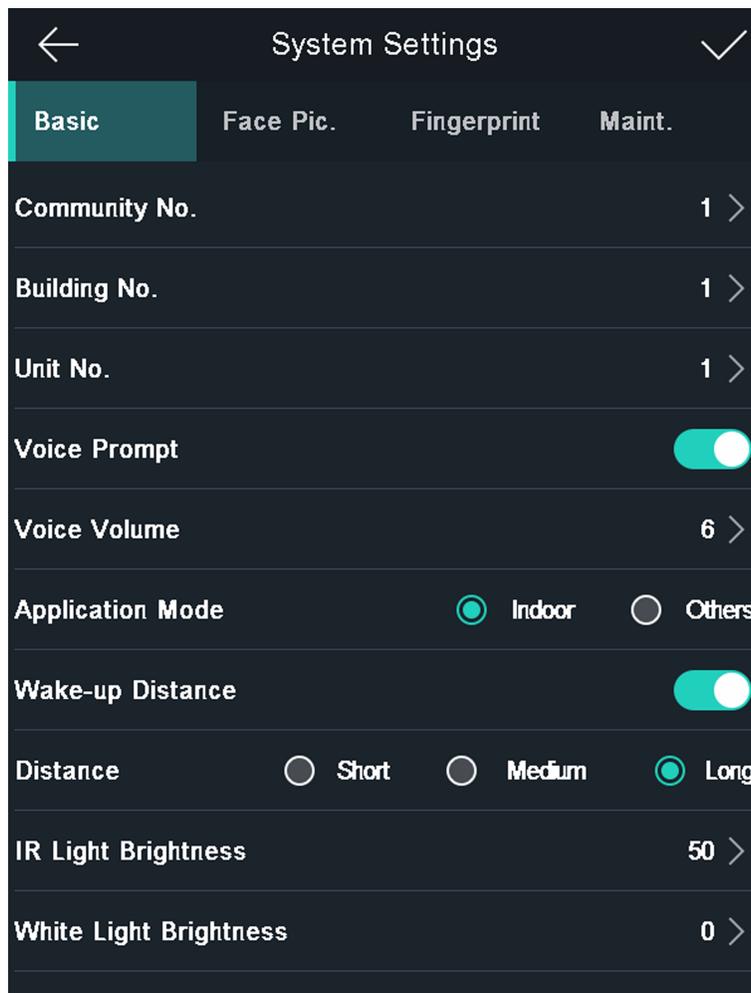


Figure 6-10 Basic Parameters

Table 6-1 Basic Parameters

Parameter	Description
Community No.	Set the device installed community No.
Building No.	Set the device installed building No.
Unit No.	Set the device installed Unit No.
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.
Wake-up Distance	The live view on the device screen will enter the IR mode.

Parameter	Description
IR Light Brightness	Set the IR light brightness when the IR light is enabled.
White Light Brightness	Set the supplement white light's brightness. The brightness ranges from 0 to 100. 0 refers to turning off the light. 1 refers to the darkest, and 100 refers to the brightest

### 6.7.2 Set Face Picture Parameters

You can set the face 1:N security level, 1:1 security level, recognition interval, liveness security level, pupillary distance, WDR level, and ECO mode.

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



Figure 6-11 Face Picture Parameters

**Table 6-2 Face Picture Parameters**

Parameter	Description
1:N Security Level	Set the matching threshold when authenticating via 1:N matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate.
1:1 Security Level	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.
Recognition Interval	Set the time interval between two continuous face recognitions when authenticating.   <b>Note</b> You can input the number from 1 to 10.
Liveness Security Level	After enabling Live Face Detection function, you can set the matching security level when performing live face authentication.
WDR Level	The device can auto enable the WDR function. The higher the level, the device can enter the WDR mode easier. 0 represents WDR is disabled.   <b>Note</b> When there are both very bright and very dark areas simultaneously in the view, WDR balances the brightness level of the whole image and provide clear images with details.
Pupillary Distance	The minimum resolution between two pupils when starting face recognition. The actual resolution should be larger than the configured value.  By default, the resolution is 40.
ECO Mode	After enabling the ECO mode, the device can authenticate faces in the low light or dark environment. And you can set the ECO mode threshold, ECO mode (1:N), and ECO mode (1:1).
ECO Mode Threshold	When enabling the ECO mode, you can set the ECO mode's threshold. The larger the value, the easier the device entering the ECO mode. Available range: 0 to 7.

Parameter	Description
ECO Mode (1:N)	Set the matching threshold when authenticating via ECO mode 1:N matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate.
ECO Mode (1:1)	Set the matching threshold when authenticating via ECO mode 1:1 matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate.

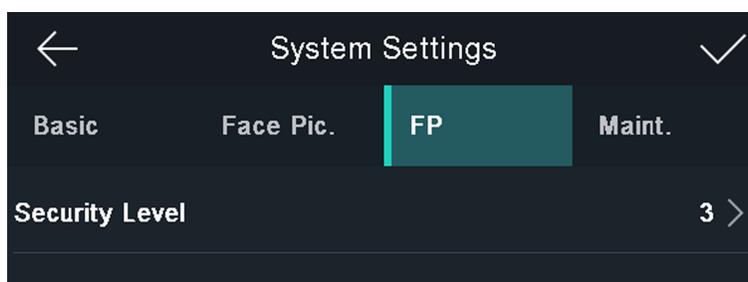
### 6.7.3 Set Fingerprint Parameters

You can set the fingerprint security level in this section.

 **Note**

Some device models do not support the fingerprint related functions.

---



**Figure 6-12 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).

The security level related false acceptance rate is shown as below:

Fingerprint Security Level	FAR
1	0.1%
2	0.003%
3	0.001%
4	0.0003%
5	0.0001%

## 6.7.4 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.

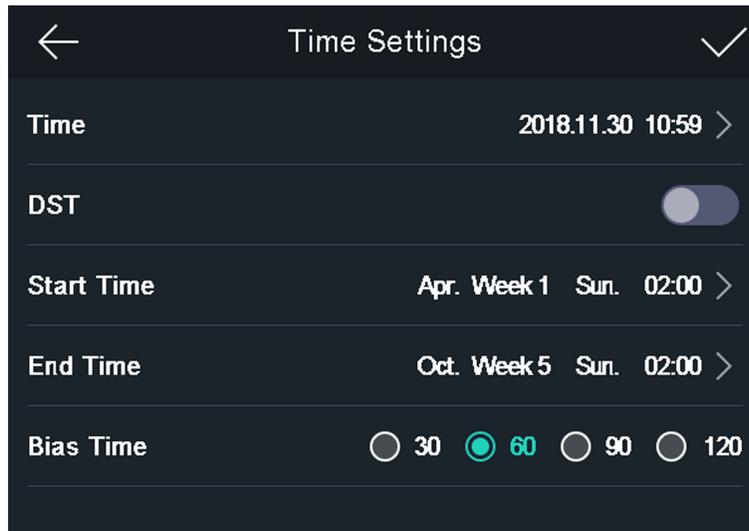


Figure 6-13 Time Parameters

## 6.8 Time and Attendance Status Settings

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

---

### Note

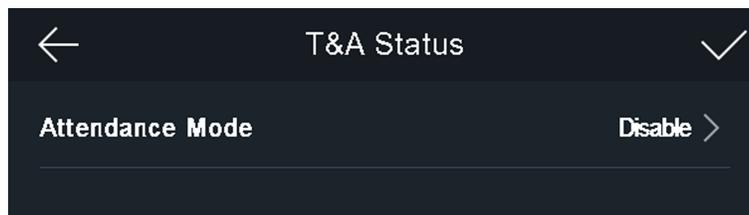
The function should be used cooperatively with time and attendance function on the client software.

---

### 6.8.1 Disable Attendance Mode via Device

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.



**Figure 6-14 Disable Attendance Mode**

Set the **Attendance Mode** as **Disable**. And tap .

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.

## 6.8.2 Set Manual Attendance via Device

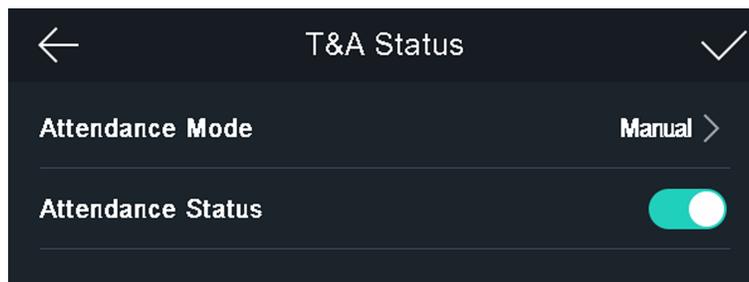
Set the attendance mode as manual, and you can select a status manually when you take attendance.

### 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 6-15 Manual Attendance Mode**

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

### Result

You should select the attendance status manually after authentication.

---

### Note

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

---

## 6.8.3 Set Auto Attendance via Device

Set the attendance mode as auto, and you can set the attendance status and its available schedule. The system will automatically 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**.

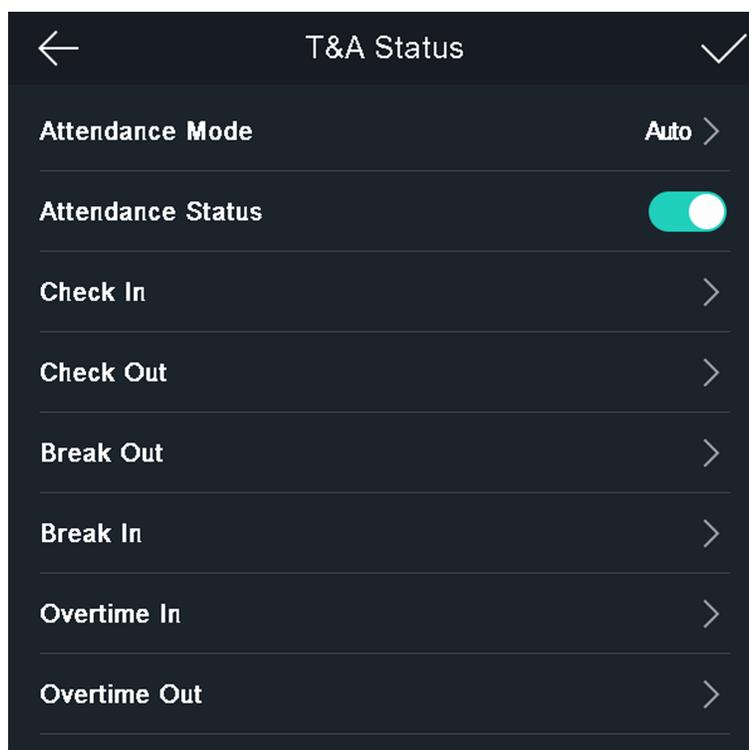


Figure 6-16 Auto Attendance Mode

3. Select an attendance status and set its schedule.
  - 1) Select **Check In**, **Check Out**, **Break Out**, **Break In**, **Overtime In**, or **Overtime Out** as the attendance status.
  - 2) Tap **Schedule**.
  - 3) Select **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday**, or **Sunday**.
  - 4) Tap the select date and set the selected attendance status's start time.
  - 5) Tap **Confirm**.
  - 6) Repeat step 1 to 5 according to your actual needs.



The attendance status will be valid within the configured schedule.

---

4. Tap  .

## Result

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

## Example

If set the **Break Out Schedule** as Monday 11:00, and **Break In Schedule** as Monday 12:00, the valid user's authentication from Monday 11:00 to 12:00 will be marked as break.

## 6.8.4 Set Manual and Auto Attendance via Device

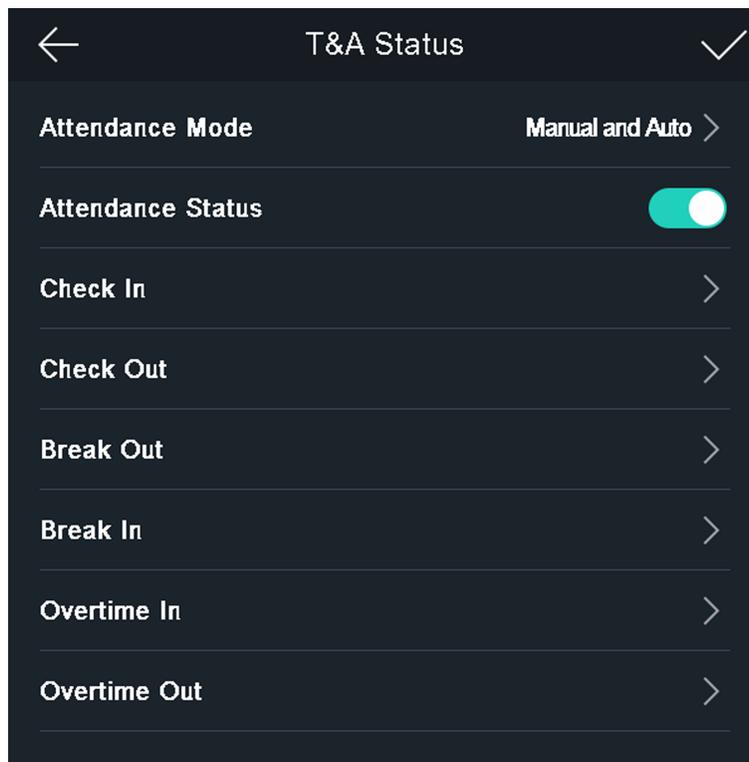
Set the attendance mode as **Manual and Auto**, and the system will automatically change the attendance status according to the configured parameters. At the same time you can manually change the attendance status after the authentication.

### 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 6-17 Manual and Auto Mode**

3. Select an attendance status and set its schedule.
  - 1) Select **Check In**, **Check Out**, **Break Out**, **Break In**, **Overtime In**, or **Overtime Out** as the attendance status.
  - 2) Tap **Schedule**.
  - 3) Select **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday**, or **Sunday**.
  - 4) Tap the select date and set the selected attendance status's start time.
  - 5) Tap **Confirm**.
  - 6) Repeat step 1 to 5 according to your actual needs.

---

 **Note**

The attendance status will be valid within the configured schedule.

---

4. Tap .

### **Result**

On 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.

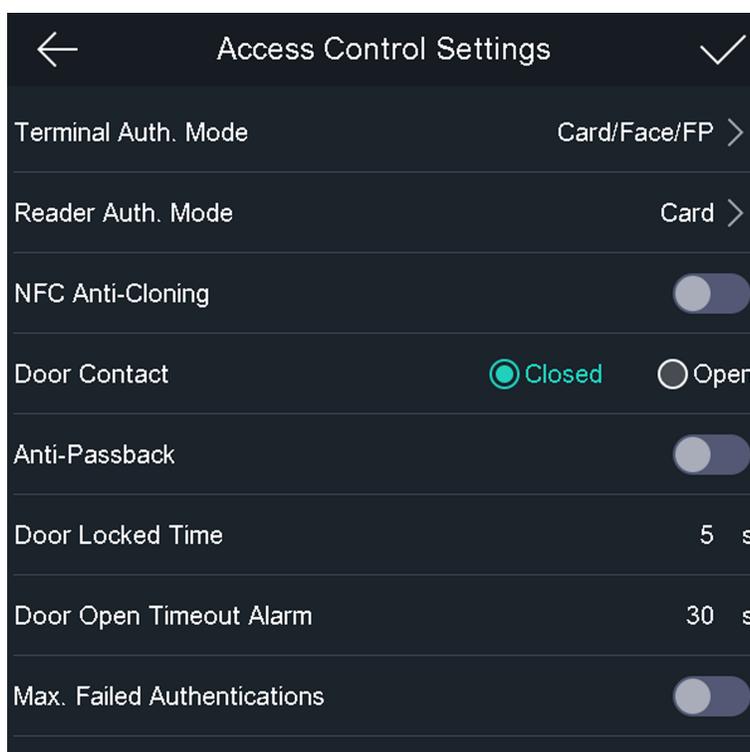
**Example**

If set the **Break Out Schedule** as Monday 11:00, and **Break In Schedule** as Monday 12:00, the valid user's authentication from Monday 11:00 to 12:00 will be marked as break.

## 6.9 Set Access Control Parameters

You can set the access control permissions, including the functions of authentication mode, door contact, and door locked time.

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 6-18 Access Control Parameters**

The available parameters descriptions are as follows:

**Table 6-3 Access Control Parameters Descriptions**

Parameter	Description
Terminal Auth. Mode (Terminal Authentication Mode)	Select the face recognition terminal's authentication mode. You can also customize the authentication mode.

Parameter	Description
	 <b>Note</b> <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 completely applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.</li></ul>
Reader Auth. Mode (Card Reader Authentication Mode)	Select the card reader's authentication mode.
Door Contact	You can select "Open (Remain Open)" or "Close (Remian Closed)" according to your actual needs. By default, it is Close (Remian Closed).
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.

## 6.10 Maintenance

### 6.10.1 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.

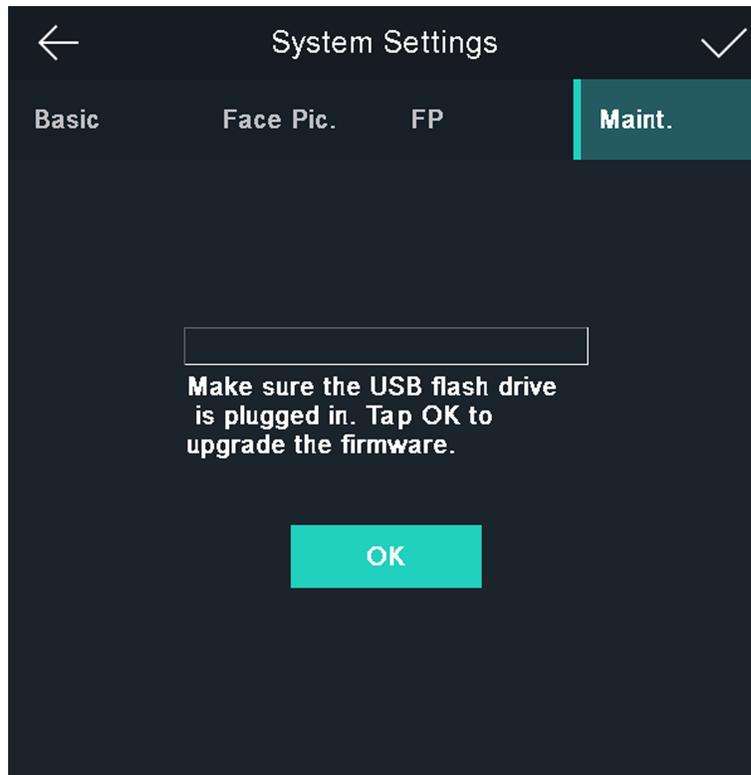


Figure 6-19 Upgrade

---

### 6.10.2 Data Management

On the Data Management page, you can delete all events, delete user data, delete all data, 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:

Table 6-4 Data Descriptions

Parameters	Description
Delete All Events	Delete all events stored in the device.
Delete User Data	Delete all user data in the device.
Delete Captured Pic.	Delete the device captured pictured.

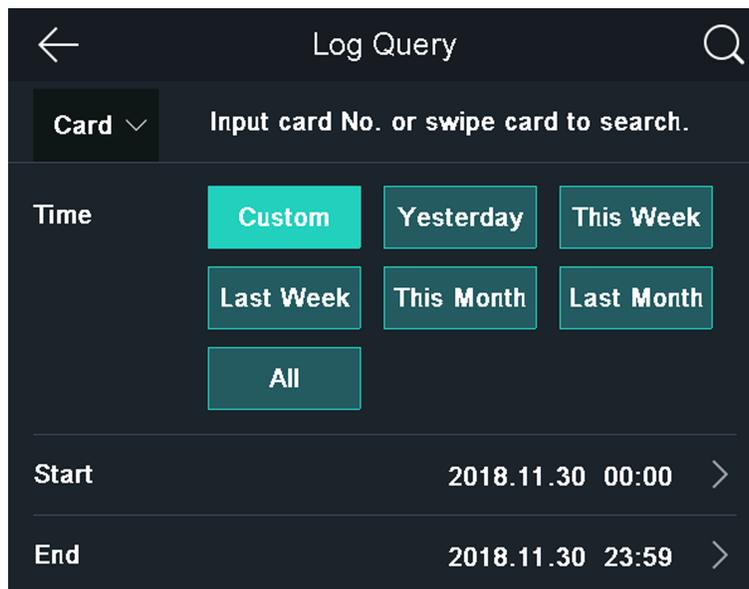
Parameters	Description
Restore to Factory	Restore the system to the factory settings. The device will reboot after the setting.
Restore to Default	Restore the system to the default settings. The system will save the communication settings and the remote user settings. Other parameters will be restored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

### 6.10.3 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 6-20 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.

## 6.11 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.



Some device models do not support displaying the fingerprint capacity.

---

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

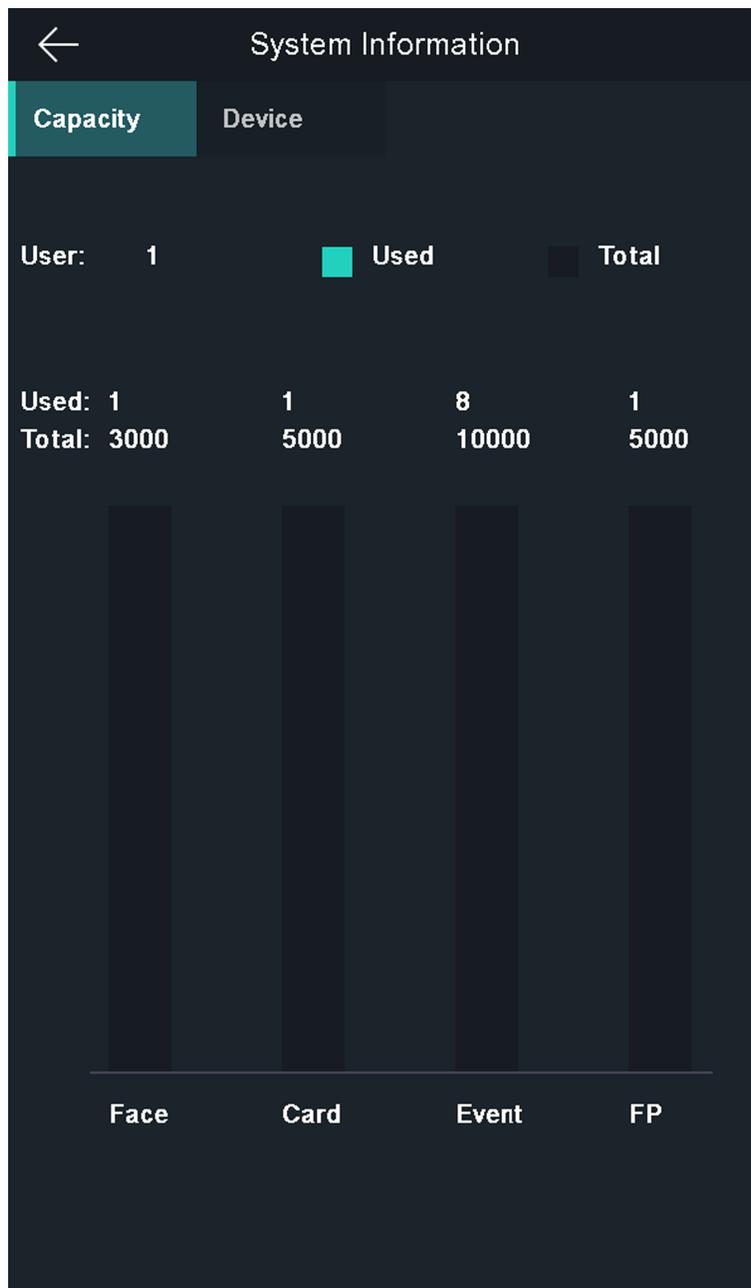


Figure 6-21 Capacity

### 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.

## 6.12 Two-Way Audio

After adding the device to the client software, you can call the device from the client software, call the main station from the device, call the client software from the device, or call the indoor station from the device.

### 6.12.1 Call Client Software from Device

#### Steps

1. Get the client software from the supplied disk or the official website, and install the software according to the prompts.
2. Run the client software and the control panel of the software pops up.
3. Click **Device Management** to enter the Device Management interface.
4. Add the device to the client software.

---

#### Note

For details about adding device, see *Add Device*.

---

5. Call the client software.
  - 1) Tap **Call** on the device initial page.
  - 2) Input **0** in the pop-up window.
  - 3) Tap **Call** to call the client software.
6. Tap **Answer** on the pop-up page of the client software and you can start two-way audio between the device and the client software.

---

#### Note

If the device is added to multiple client softwares and when the device is calling the client software, only the first client software added the device will pop up the call receiving window.

---

### 6.12.2 Call Main Station from Device

#### Steps

1. Get the client software from the supplied disk or the official website, and install the software according to the prompts.
2. Run the client software and the control panel of the software pops up.
3. Click **Device Management** to enter the Device Management interface.
4. Add the main station and the device to the client software.

---

 **Note**

For details about adding device, see *Add Device*.

- 
5. Set the main station's IP address and SIP address in the remote configuration page.

---

 **Note**

For details about the operation, see the user manual of the main station.

- 
6. Answers the call via the main station and starts two-way audio.

---

 **Note**

The device will call the main station in priority when tap  .

---

## 6.12.3 Call Device from Client Software

### Steps

1. Get the client software from the supplied disk or the official website, and install the software according to the prompts.
2. Run the client software and the control panel of the software pops up.
3. Click **Device Management** to enter the Device Management page.
4. Add the device to the client software.

---

 **Note**

For details about adding device, see *Add Device*.

- 
5. Enter the **Live View** page and double-click the added device to start live view.

---

 **Note**

For details about operations in the **Live View** page, see *Live View* in the user manual of the client software.

- 
6. Right click the live view image to open the right-click menu.  
7. Click **Start Two-Way Audio** to start two-way audio between the device and the client software.

## 6.12.4 Call Indoor Station from Device

### Steps

1. Get the client software from the supplied disk or the official website, and install the software according to the prompts.
2. Run the client software and the control panel of the software pops up.
3. Click **Device Management** to enter the Device Management interface.
4. Add the indoor station and the device to the client software.



### Note

For details about adding device, see *Add Device*.

---

5. Link a user to an indoor station and set a room No. for the indoor station.
6. Tap  on the authentication page of the device.
7. Input the room No. on the dial page and tap  to call the indoor station.
8. After the indoor station answers the call, you can start two-way audio with the indoor station.

## Chapter 7 Client Software Configuration

### 7.1 Configuration Flow of Client Software

Follow the flow diagram below to configure on the client software.

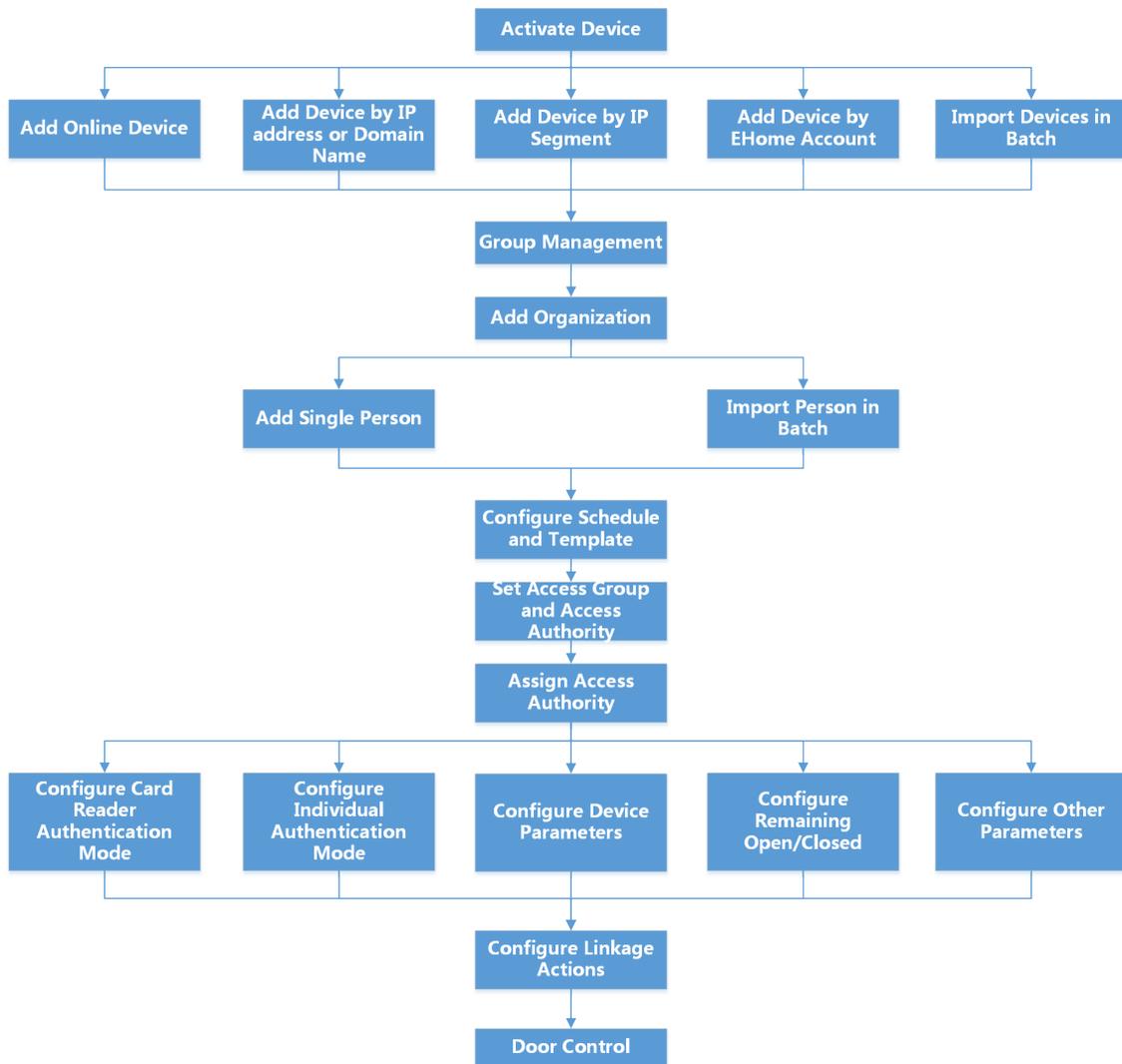


Figure 7-1 Flow Diagram of Configuration on Client Software

### 7.2 Device Management

You can manage devices on the client, including adding, editing, and deleting the devices. You can also perform operations such as checking device status.

## 7.2.1 Add Device

After running the client, devices including access control devices, video intercom devices, etc., should be added to the client for the remote configuration and management, such as controlling door status, attendance management, event settings, etc.

### Add Online Device

The active online devices in the same local subnet with the client software will be displayed on the **Online Device** area.



- You can click **Refresh per 60s** to refresh the information of the online devices.
  - SADP log function can be enabled or disabled by right-clicking **Online Device**.
- 

### Add an Online Device

You can add an online device to the client.

#### Steps

1. Enter the Device Management module.
2. Click **Device** tab on the top of the right panel.
3. Click **Online Device** to show the online device area.

The searched online devices are displayed in the list.

4. Select an online device in the **Online Device** area, and click **Add** to open the device adding window.



For the inactive device, you need to create the password for it before you can add the device properly. For detailed steps, refer to .

5. Enter the required information.
- 

#### Name

Enter a descriptive name for the device.

#### IP Address

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

#### Port

You can customize the port number. The port number of the device is obtained automatically in this adding mode.

#### User Name

By default, the user name is **admin**.

## Password

Enter the device 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.

---

6. Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.
7. **Optional:** Check **Import to Group** to create a group by the device name.
8. Click **Add**.
9. **Optional:** Perform the following operation(s).

### **Remote Configuration**

Click  on Operation column to set remote configuration of the corresponding device.

---

### **Note**

See the user manual of the device for details.

---

### **Device Status**

Click  on Operation column to view device status, including cameras, recording status, signal status, hardware status, etc.

### **Edit Device Information**

Click  on Operation column to edit the device information, such as IP address, user name, and password.

### **Check Online User**

Click  on Operation column to check the online users who access the device, such as user name, user type, user's IP address, and login time.

### **Refresh**

Click  on Operation column to get the latest device information.

### **Delete Device**

Select one or multiple devices and click **Delete** to delete the selected device(s) from the client.

## Add Multiple Online Devices

You can add multiple online devices to the client in a batch.

### Before You Start

Make sure the to-be-added devices are online.

## Steps

1. Enter the Device Management module.
2. Click **Device** tab on the top of the right panel.
3. Click **Online Device** to show the online device area at the bottom of the page.

The searched online devices are displayed in the list.

4. Select multiple devices.



### Note

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

5. Click **Add** to open the device adding window.
6. Enter the required information.

### User Name

By default, the user name is *admin*.

### Password

Enter the device 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. **Optional:** Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.
8. **Optional:** Check **Import to Group** to create a group by the device name .
9. Click **Add** to add the devices.
10. **Optional:** Perform the following operation(s).

### Remote Configuration

Click  on Operation column to set remote configuration of the corresponding device.



### Note

See the user manual of the device for details.

### Device Status

Click  on Operation column to view device status, including cameras, recording status, signal status, hardware status, etc.

### Edit Device Information

Click  on Operation column to edit the device information, such as IP address, user name, and password.

<b>Check Online User</b>	Click  on Operation column to check the online users who access the device, such as user name, user type, user's IP address, and login time.
<b>Refresh</b>	Click  on Operation column to get the latest device information.
<b>Delete Device</b>	Select one or multiple devices and click <b>Delete</b> to delete the selected device(s) from the client.

### Add Device by IP Address or Domain Name

When you know the IP address or domain name of the device to add, you can add devices to the client by specifying the IP address (or domain name), user name, password, and other related parameters.

#### Steps

1. Enter Device Management module.
2. **Optional:** Click  on the right of **Device Management** and select **Device**.  
The added devices are displayed in the list.
3. Click **Add** to open the Add window.
4. Select **IP/Domain** as the adding mode.
5. Enter the required information, including name, address, port number, user name, and password.

#### Name

Create a descriptive name for the device. For example, you can use a name that can show the location or feature of the device.

#### Address

The IP address or domain name of the device.

#### Port

The devices to add have the same port No. The default value is 8000.

#### User Name

Enter the device user name. By default, the user name is admin.

#### Password

Enter the device 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.

- 
- Optional:** Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.
  - Optional:** Check **Import to Group** to create a group by the device name.
- 

### **Note**

You can import all the channels of the device to the corresponding group by default.

---

- Finish adding the device.
  - Click **Add** to add the device and back to the device list page.
  - Click **Add and New** to save the settings and continue to add other device.
- Perform the following operations after adding the devices.

### **Remote Configuration**

Click  on Operation column to set remote configuration of the corresponding device.

---

### **Note**

- For some models of devices, you can open its web window. To open the original remote configuration window, press **Ctrl** and click .
  - For detail operation steps for the remote configuration, see the user manual of the device.
- 

### **Device Status**

Click  on Operation column to view device status.

## Add Devices by IP Segment

If you want to add devices of which the IP addresses are within an IP segment, you can specify the start IP address and end IP address, user name, password, and other parameters to add them.

### Steps

- Enter the Device Management module.
- Optional:** Click  on the right of **Device Management** and select **Device**.

The added devices are displayed in the list.

- Click **Add** to open the Add window.
- Select **IP Segment** as the adding mode.
- Enter the required information.

### **Start IP**

Enter a start IP address.

### **End IP**

Enter an end IP address in the same network segment with the start IP.

## Port

Enter the device port No. The default value is 8000.

## User Name

By default, the user name is admin.

## Password

Enter the device 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.

---

- 6. Optional:** Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.
  - 7. Optional:** Check **Import to Group** to create a group by the device name.
- 



### Note

You can import all the channels of the device to the corresponding group by default.

---

8. Finish adding the device.
  - Click **Add** to add the device and back to the device list page.
  - Click **Add and New** to save the settings and continue to add other device.
- 9. Optional:** Click  on Operation column to view device status.

## Add Device by EHome Account

For areas where devices using dynamic IP addresses instead of static ones, you can add access control device connected via EHome protocol by specifying the EHome account.

### Before You Start

Set the network center parameter first. For details, refer to [\*\*\*Set Network Parameters\*\*\*](#) .

### Steps

---



### Note

For the devices added by EHome don't support uploading events with captured pictures to the client.

---

1. Enter Device Management module.

- 2. Optional:** Click  on the right of **Device Management** and select **Device**.

The added devices are displayed in the list.

- 3.** Click **Add** to open the Add window.
- 4.** Select **EHome** as the adding mode.
- 5.** Enter the required information.

### Device Account

Enter the account name registered on EHome protocol.

### EHome Key

Enter the EHome key if you have set it when configuring network center parameter for the device.



### Note

This function should be supported by the device.

- 6. Optional:** Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.
- 7. Optional:** Check **Import to Group** to create a group by the device name.
- 8.** Finish adding the device.
  - Click **Add** to add the device and back to the device list page.
  - Click **Add and New** to save the settings and continue to add other device.
- 9. Optional:** Click  on Operation column to view device status.

## Import Devices in a Batch

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

### Steps

1. Enter the Device Management page
2. Click **Add** to open the adding device window.
3. Select **Batch Import** as the adding mode.
4. Click **Export Template** and then save the pre-defined template (CSV file) on your PC.
5. Open the exported template file and enter the required information of the devices to be added on the corresponding column.

### Adding Mode

You can enter **0** or **1** which indicated different adding modes. **0** indicates that the device is added by IP address or domain name; **1** indicates that the device is added via EHome.

### Address

Edit the address of the device. If you set **0** as the adding mode, you should enter the IP address or domain name of the device; if you set **1** as the adding mode, this field is not required.

## Port

Enter the device port No. The default value is 8000.

## Device Information

If you set **0** as the adding mode, this field is not required. If you set **1** as the adding mode, enter the EHome account.

## User Name

Enter the device user name. By default, the user name is admin.

## Password

If you set **0** as the adding mode, enter the password. If you set **1** as the adding mode, enter the EHome key.



### 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.

---

## Import to Group

You can enter **1** to create a group by the device name. All the channels of the device will be imported to the corresponding group by default. **0** indicates disabling this function.

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

## 7.2.2 Reset Device Password

If you forgot the password of the detected online devices, you can reset the device password through the client.

### Steps

1. Enter Device Management page.
2. Click **Online Device** to show the online device area.  
All the online devices in the same subnet will display in the list.
3. Select the device from the list and click  on the Operation column.
4. Click **Export** to save the device file on your PC and then send the file to our technical support.



### Note

For the following operations for resetting the password, contact our technical support.

---



## 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.

---

## 7.3 Group Management

The client provides groups to manage the added resources in different groups. You can group the resources into different groups according to the resources' locations.

### Example

For example, on the 1st floor, there mounted 64 alarm inputs, and 16 alarm outputs. You can organize these resources into one group (named 1st Floor) for convenient management. You can and do some other operations of the devices after managing the resources by groups.

### 7.3.1 Add Group

You can add group to organize the added device for convenient management.

#### Steps

1. Enter the Device Management module.
2. Click **Device Management** → **Group** to enter the group management page.
3. Create a group.
  - Click **Add Group** and enter a group name as you want.
  - Click **Create Group by Device Name** and select an added device to create a new group by the name of the selected device.



#### Note

The resources (such as alarm inputs/outputs, etc.) of this device will be imported to the group by default.

---

### 7.3.2 Import Resources to Group

You can import the device resources (such as alarm inputs/outputs, etc.) to the added group in a batch.

## Before You Start

Add a group for managing devices. Refer to **Add Group** .

## Steps

1. Enter the Device Management module.
2. Click **Device Management** → **Group** to enter the group management page.
3. Click **Import**.
4. Select the thumbnails/names of the resources in the thumbnail/list view.



## Note

You can click  or  to switch the resource display mode to thumbnail view or to list view.

5. Click **Import** to import the selected resources to the group.

## 7.3.3 Edit Resource Parameters

After importing the resources to the group, you can edit the resource parameters. For alarm input, you can edit the alarm input name. Here we take as an example.

## Before You Start

Import the resources to group.

## Steps

1. Enter the Device Management module.
2. Click **Device Management** → **Group** to enter the group management page.  
All the added groups are displayed on the left.
3. Select a group on the group list and click .  
The imported to the group will display.
4. Click  in the Operation column to open the Edit Resource window.
5. Click **OK** to save the new settings.

## 7.3.4 Remove Resources from Group

You can remove the added resources from the group.

## Steps

1. Enter the Device Management module.
2. Click **Device Management** → **Group** to enter the group management page.  
All the added groups are displayed on the left.
3. Click a group to show the resources added to this group.
4. Select the resource(s) and click **Delete** to remove the resource(s) from the group.

## 7.4 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.

### 7.4.1 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.



Up to 10 levels of organizations can be added.

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

**Edit Organization**      Hover the mouse on an added organization and click  to edit its name.

**Delete Organization**      Hover the mouse on an added organization and click  to delete it.



- 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.

---

**Show Persons in Sub Organization**      Check **Show Persons in Sub Organization** and select an organization to show persons in its sub organizations.

### 7.4.2 Configure Basic Information

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

### 7.4.3 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

---



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**.
- 



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.
- 



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 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.

### 7.4.4 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 .

### 7.4.5 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.

#### Before You Start

Add at least one access control device checking whether the face in the photo can be recognized by the facial recognition device managed by the client.

#### Steps

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



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.

### 7.4.6 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**.



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 .

### 7.4.7 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.

### 7.4.8 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**.



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 .

### 7.4.9 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 blocklist 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**.



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.

---

#### Note

Once a person has been configured as a super user, all his/her fingerprints or cards turn to super fingerprints or super cards.

---

### 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 Blocklist

Add the person to the blocklist 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 Blocklist, 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 blocklist, 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.

### 7.4.10 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.

### 7.4.11 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 bind 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.

### 7.4.12 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 .

### 7.4.13 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.

### 7.4.14 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.
- 

### 7.4.15 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.

### 7.4.16 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.



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.

## 7.4.17 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.



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.



- 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).
- 

## 7.4.18 Delete Registered Pictures

You can delete face picture file of the added persons automatically.

## Before You Start

Make sure you have saved the structure data.

## Steps

1. Enter the Person module.
2. **Optional:** Select a person item in the list.
3. Click **Delete Registered Picture** to delete the registered picture.

### 7.4.19 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



- 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.
- 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.

### 7.4.20 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**.

### 7.4.21 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.

### 7.4.22 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.

### 7.4.23 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



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.

## 7.5 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.



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

---

## 7.5.1 Add Holiday

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

### Steps

---



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

---

1. Click **Access Control** → **Schedule** → **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.
- 



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.
- 



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**.

## 7.5.2 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.

## Steps

---

### Note

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

---

1. Click **Access Control** → **Schedule** → **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.

### 7.6 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.

#### 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 Devices** to start applying all the selected access group(s) to the access control device or door station.



## Caution

- Be careful to click **Apply All to Devices**, since this operation will clear all the access groups of the selected devices and then apply the new access group, which may bring risk to the devices.
- You can click **Apply Changes to Devices** 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 Status** to 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.

## 7.7 Configure Advanced Functions

You can configure the advanced functions of access control to meet some special requirements in different scene.



## Note

- For the card related functions (the type of access control card), 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.

### 7.7.1 Configure Device Parameters

After adding the access control device, you can configure the parameters of access control device, access control points.

## Configure Parameters for Access Control Device

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

### Steps

1. Click **Access Control** → **Advanced Function** → **Device Parameter** .



## Note

If you cannot 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.
- 

### 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.

### Face Recognition Mode

Normal Mode: Recognize face via the camera normally.

### Enable NFC Card

If enable the function, the device can recognize the NFC card. You can present NFC card on the device.

### Enable M1 Card

If enable the function, the device can recognize the M1 card. You can present M1 card on the device.

### Enable EM Card

If enable the function, the device can recognize the EM card. You can present EM card on the device.

### Enable CPU Card

If enable the function, the device can recognize the CPU card. You can present CPU card on the device.

### Enable ID Card

If enable the function, the device can recognize the ID card. You can present ID card on the device.

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.

## Before You Start

Add access control device to the client.

## 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 Left 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.

### **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.

### **Fingerprint Recognition Level**

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

### **Face Recognition Timeout Value**

If the recognition time is more than the configured time, the device will remind you.

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

Set the matching threshold 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.

### **Face Recognition Interval**

The time interval between two continuous face recognitions when authenticating.

### **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.

### **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.

## Application Mode

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

## 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.

## 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.

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 Output

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

### Before You Start

Add access control device to the client, and make sure the device supports alarm output.

### 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.

## 7.7.2 Configure Remaining Open/Closed

You can set the status of the door as open or closed. 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 that need to be configured on the left panel.
3. To set the door status during the work day, click the **Week Schedule** and perform the following operations.
  - 1) Click **Remain Open** or **Remain Closed**.
  - 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 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) Click **Save**.

### Related Operations

**Copy to Whole Week** 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.

**Delete Selected** Select one duration on the time bar, click **Delete Selected** to delete this duration.

**Clear** 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).

## 7.7.3 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.

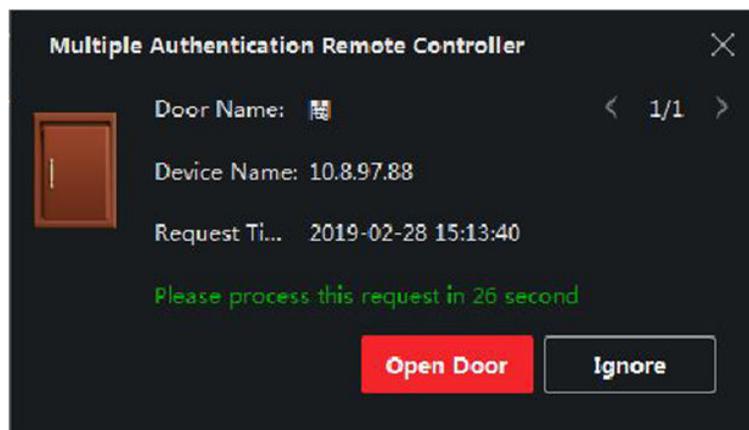


Figure 7-2 Remotely Open Door

---

### 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.

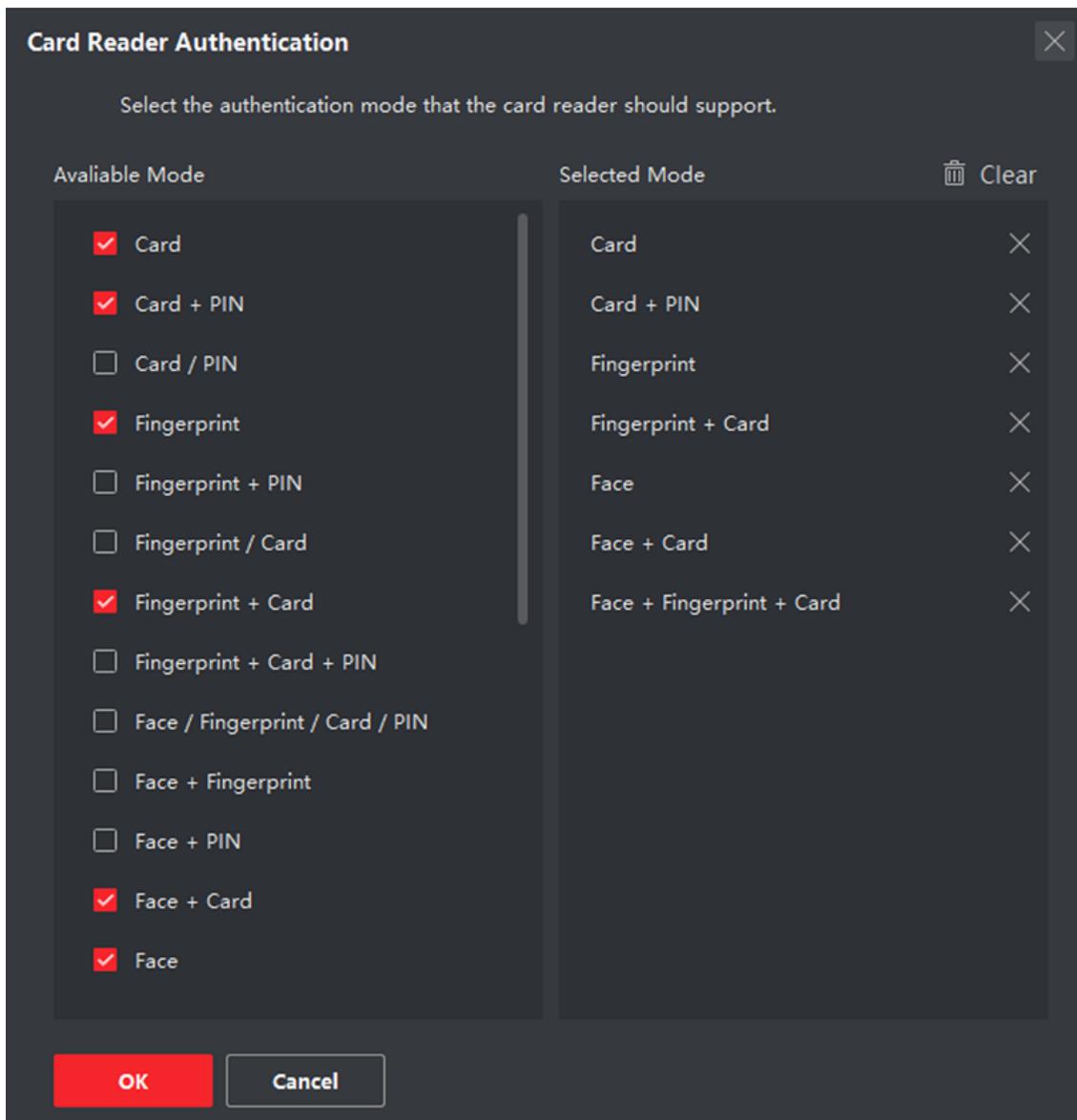
- 
7. Click **Save**.

### 7.7.4 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.

#### 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 7-3 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.

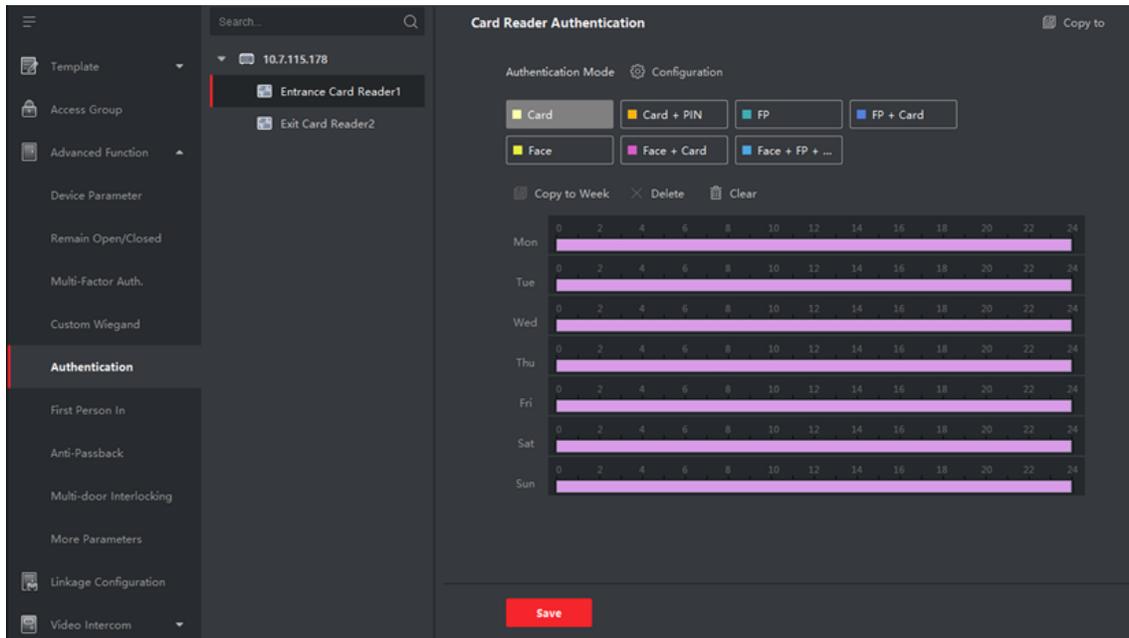


Figure 7-4 Set Authentication Modes for Card Readers

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**.

## 7.7.5 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

- Add access control device to the client, and make sure the device supports the first person in function.
- Add person and assign access authorization to designed person. For details, refer to [Person Management](#) and [Set Access Group to Assign Access Authorization to Persons](#) .

### 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**.

## **7.7.6 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 .

---

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.

## **7.7.7 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.

#### **Before You Start**

Add access control device to the client, and make sure the device supports multiple NICs.

#### **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 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 network.

### Set Log Uploading Mode

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

#### Steps

---



#### Note

Make sure the device is not added by EHome.

---

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.
  - Make sure the device is not added by EHome.
- 

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**.

## 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 Picture Storage* in the user manual of the client software. .

## 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 *Set Picture Storage* in the user manual of the client software.

### 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 *Set Picture Storage* in the user manual of the client software.

#### 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.

### Blocklist Authentication

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

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

If mismatched (the person is not in the blocklist), 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**.

## 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.

## 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

---



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

---



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.
- 



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

---

6. Check **Enable Wiegand** to enable the Wiegand function.
-

### 7. Click **Save**.

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

## 7.8 Configure Linkage Actions for Access Control

You can configure different linkage actions for the event detected by the access control device. After that, linkage actions will be triggered once the event happens. This mechanism is used for notifying the security personnel the event, or triggering automatic access control in real time.

Two types of linkage actions are supported:

- **Client Actions:** When the event is detected, it will trigger the actions on the client, such as the client making an audible warning..
- **Device Actions:** When the event is detected, it will trigger the actions of a specific device, such as buzzing of a card reader and, opening/closing of a door, ..

### 7.8.1 Configure Client Actions for Access Event

Even if you are far away from an access point, you can still know what happens and how urgent the event is by configuring linked actions of access event on the client. You will be notified on the client once an event is triggered, so that you can response to the event instantly. You can also configure client actions of access points in a batch at a time.

#### Steps

---



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 *Set Alarm Sound* in the user manual of client software..

---

### Send Email

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

For details about setting email parameters, refer to *Set Email Parameters* in the user manual of client software..

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, or card reader.

## 7.8.2 Configure Device Actions for Access Event

You can set the access control device's linkage actions for the access control device's triggered event. After that, when an event is triggered, it can trigger the alarm output, buzzer on access controller, and other actions.

### Steps

---

## Note

The linkage actions 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** to add a new linkage.
4. Select **Event Linkage** as the event source.
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

An event-related picture will be captured when the selected event happens.

### Recording

An event-related picture will be captured when the selected event happens.

---

## 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 when the selected event happens

## 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 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 followings:

<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 <b>Delete</b> to delete it.

## 7.8.3 Configure Device Actions for Card Swiping

You enable access control device's linkage actions (such as disarming a zone and triggering audio prompt) for the swiping of a specific card, In this way, you can monitor the card holder's behaviors and whereabouts.

### 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** to add a new linkage.
4. Select **Card Linkage** as the event source.
5. Enter the card number or select the card from the drop-down list.

6. Select the card reader where the card swipes.
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**

An event-related picture will be captured when the selected event happens.

### **Recording**

An event-related picture will be captured when the selected event happens.



### **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 followings:

<b>Delete Linkage Settings</b>	Select the configured linkage settings in the device list and click <b>Delete</b> 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.

## 7.8.4 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, buzzer on card reader, and other actions, so as to implement special monitoring on the specified person.

### Steps



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** to add a new linkage.
4. Select **Person Linkage** as the event source.
5. Enter the employee number or select the person from the drop-down list.
6. Select the card reader where the card swipes.
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**

An event-related picture will be captured when the selected event happens.

#### **Recording**

An event-related picture will be captured when the selected event happens.

---



The device should support recording.

---

#### **Alarm Output**

The alarm output will be triggered for notification.

#### **Alarm Input**

Arm or disarm the alarm input.

---



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 followings:

<b>Delete Linkage Settings</b>	Select the configured linkage settings in the device list and click <b>Delete</b> 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.

## 7.9 Door Control

In Monitoring module, you can view the real-time status of the doors managed by the added access control device. You can also control the doors 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.



For the user with door control permission, the user can enter the Monitoring module and control the door. Or the icons used for control will not show. For setting the user permission, refer to ***Person Management***.

---

### 7.9.1 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.



For managing the access point group, refer to *Group Management* in the user manual of the client software.

---

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 *Set File Saving Path* in the user manual of the client software.

---

### Result

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

## 7.9.2 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.

## 7.10 Event Center

In the Event Center, you can view the real-time events, search the historical events and view the pop-up alarm information.

Before the client can receive the event information from the device, you need to arm the device first. For details, refer to [\*\*\*Enable Receiving Event Notification from Devices\*\*\*](#).

Before the you can view the pop-up alarm information, you need to enable alarm triggered pop-up image in the event center. For details, refer to .

### 7.10.1 Enable Receiving Event Notification from Devices

Before the client software can receive event notifications from the device, you need to arm the device first.

#### Steps

1. Click  → **Tool** → **Device Arming Control** to open Device Arming Control page.

All the added devices appear on this page.

2. In the Auto-Arming column, turn on the switch to enable auto-arming.

After turned on, the device(s) will be armed. And notifications about the events triggered by the armed device(s) will be automatically sent to the client software in real-time..

### 7.10.2 View Real-Time Events

In the Real-time Event module of the event center page, you can view the real-time event information, including event source, event time, priority, event key words, etc.

#### Before You Start

Enable receiving events from devices before the client can receive event information from the device, see [\*\*\*Enable Receiving Event Notification from Devices\*\*\*](#) for details.

#### Steps

1. Click **Event Center** → **Real-time Event** to enter the real-time event page and you can view the real-time events received by the client.

#### Event Time

For video device, event time is the client time when it receives the event. For none-video device, event time is the time when the event is triggered.

#### Priority

The urgent degree of the event.

2. Filter the events.

**Filter by Device Type and (or) Priority**

Select device type(s) and (or) priorities to filter events.

## Filter by Keywords

Enter the keywords to filter the events.

3. **Optional:** Right-click the table header of the event list to customize the event related items to be displayed in the event list.
4. View the event details.
  - 1) Select an event in the event list.
  - 2) Click **Expand** in the right-lower corner of the page.
  - 3) View the related picture, detail description and handing records of the event.
  - 4) **Optional:** Hover the cursor on the related picture, and then click the download icon on the upper-right corner of the picture to download it to the local PC. You can set the saving path manually.
5. **Optional:** Perform the following operations if necessary.

### Handle Single Event

Click **Handle** to enter the processing suggestion, and then click **Commit**.



After an event is handled, the **Handle** button will become **Add Remark**, click **Add Remark** to add more remarks for this handled event.

---

### Handle Events in a Batch

Select events that need to be processed, and then click **Handle in Batch**. Enter the processing suggestion, and then click **Commit**.

### Enable/Disable Alarm Audio

Click **Enable Audio/Disable Audio** to enable/disable the audio of the event.

### Select the Latest Event Automatically

Check **Auto-Select Latest Event** to select the latest event automatically and the event information details is displayed.

### Clear Events

Click **Clear** to clear the all the events in the event list.

### Send Email

Select an event and then click **Send Email**, and the information details of this event will be sent by email.

---



You should configure the email parameters first, see for details.

---

## 7.10.3 Search Historical Events

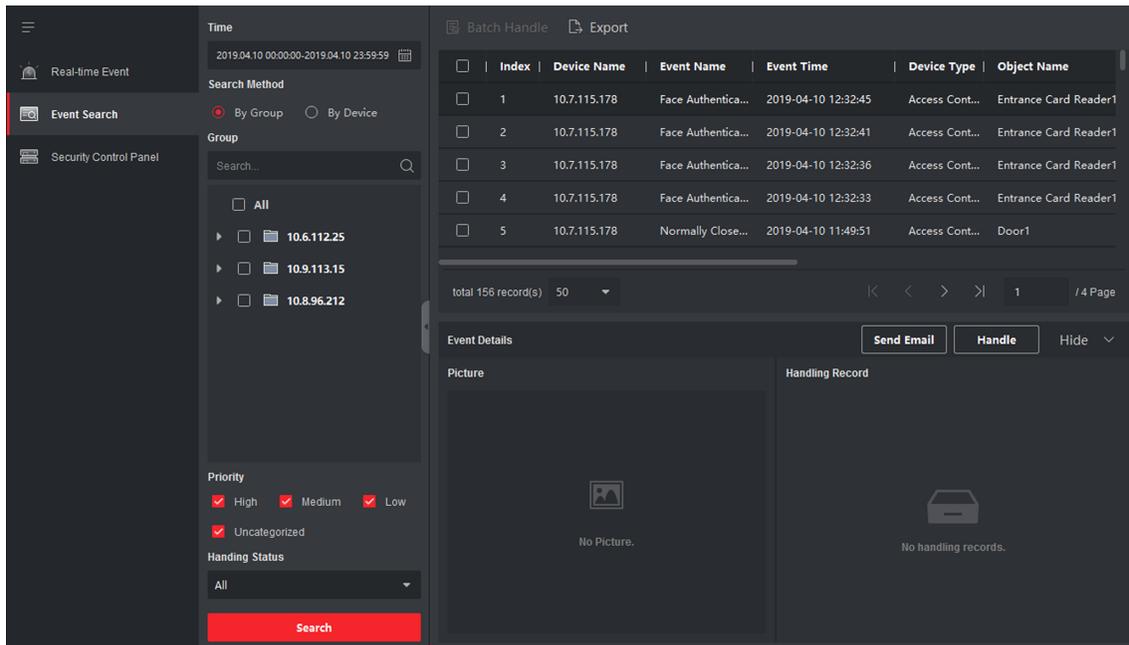
In the Event Search module of the event center page, you can search the historical events via time, device type, and other conditions according to the specified device type, and then process the events.

## Before You Start

Enable receiving events from devices before the client can receive event information from the device, see [Enable Receiving Event Notification from Devices](#) for details.

## Steps

1. Click **Event Center** → **Event Search** to enter the event search page.



**Figure 7-5 Search History Event**

2. Set the filter conditions to display the required events only.

### Time

The client time when the event starts.

### Search by

**Group:** Search the events occurred on the resources in the selected group.

**Device:** Search the events occurred on the selected device.

### Device Type

The type of device that occurred the event.

### All

All the device types, and you can set the following filter conditions: group, priority, and status.

### Video Intercom

For the events of video intercom, you need to select searching scope: All Record and Only Unlocking.

- **All Records:** You can filter the events from all the video intercom events, and you need to set the following filter conditions: device, priority, status.
- **Only Unlocking:** You can filter the events from all the video intercom unlocking events, and you need to set the following filter conditions: device, unlocking type.

### Access Control

For the events of access control, you can set the following filter conditions: device, priority, status, event type, card reader type, person name, card no., organization.



Click **Show More** to set the event type, card reader type, person name, card no., organization.

---

### Group

The group of the device that occurred the event. You should set the group as condition only when you select the Device Type as **All**.

### Device

The device that occurred the event.

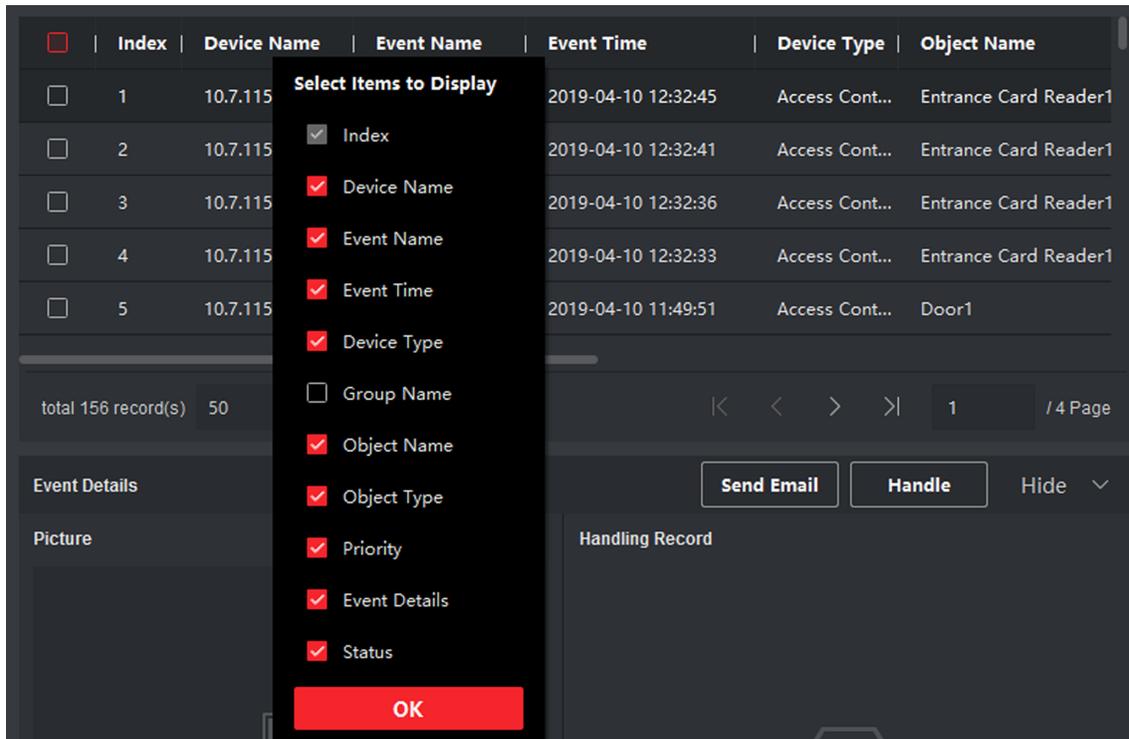
### Priority

The priority including low, medium, high and uncategorized which indicates the urgent degree of the event.

### Status

The handling status of the event.

3. Click **Search** to search the events according the conditions you set.
4. **Optional:** Right-click the table header of the event list to customize the event related items to be displayed in the event list.



**Figure 7-6 Customize Event Related Items to be Displayed**

**5. Optional:** Perform one of the following operations.

**Handle a Single Event**      Handle single event: Select one event that need to be processed, and then click **Handle** in the event information details page, and enter the processing suggestion.

---

**Note**

After an event is handled, the **Handle** button will become **Add Remark**, click **Add Remark** to add more remarks for this handled event.

---

**Batch Handle Events**      Handle events in a batch: Select the events which need to be processed, and then click **Handle in Batch**, and enter the processing suggestion.

---

**Note**

After an event is handled, the **Handle** button will become **Add Remark**, click **Add Remark** to add more remarks for this handled event.

---

**Send Email**      Select an event and then click **Send Email**, and the information details of this event will be sent by email.



You should configure the email parameters first, see for details.

---

<b>Export Event Information</b>	Click <b>Export</b> to export the event log or event pictures to the local PC in CSV format. You can set the saving path manually.
<b>Download Event Related Picture</b>	Hover the cursor on the related picture, and then click the download icon on the upper-right corner of the picture to download it to the local PC. You can set the saving path manually.

## 7.11 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.



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.

---

### 7.11.1 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



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 weekend, including overtime level, work hour 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 work hour rate for three overtime levels, respectively.

#### Work Hour Rate

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

#### Overtime Rule for Weekend

You can enable overtime rule for weekend 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 ***Add Device*** .

### Steps



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 fourth 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 test whether database can be connected and save the settings for the successful connection.

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.



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.

#### Attendance Status Mark

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

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

4. Click **Save**.

### 7.11.2 Add Timetable

On the timetable page, you can set the start-work time, end-work time and set attendance rules for being late and leaving early, etc.

#### Steps

1. Click **Time and Attendance → Timetable** to enter the timetable settings page.
2. Click **Add** to enter Basic Settings page.

The screenshot shows a configuration window with two main sections: 'Basic Settings' and 'Attendance Time'. In 'Basic Settings', the 'Name' field is 'New Period1' with a blue square icon to its right. 'Timetable Type' is set to 'General' and 'Calculated By' is 'First Check-in and Last Check-...'. A toggle for 'Get Check-in/out Status f...' is turned off. The 'Attendance Time' section includes 'Start/End-Work Time' (9:00 to 18:00), 'Calculated As' (540 min), 'Late Allowable' (10 min), and 'Early Leave Allowable' (10 min). At the bottom, a 24-hour time bar shows a blue bar from 09:00 to 18:00 and yellow bars at the start and end. 'Valid Check-in Time' and 'Valid Check-out Time' fields are present below the bar. 'Save' and 'Cancel' buttons are at the bottom.

**Figure 7-7 Add Timetable**

3. Create a name for the timetable.

---

**Note**

You can click the color icon beside the name to customize the color for the valid timetable on the time bar on the bottom of the page.

4. Select the timetable type.

**General**

Suitable for general attendance scene, which requires the fixed start-work time and end-work time, and you can set valid check-in/out time, allowable timetable for being late and leaving early.

**Flexible**

Suitable for man-hour shift, which does not requires the check-in/out time and only requires the staffs' working time (from the start time you set) is equal or greater than the predefined work hours.

5. 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.

6. **Optional:** Set **Get Check-in/out Status from Device** switch to on to calculate according to attendance status of the device.



Make sure the device support this function if you need to enable this

7. If you select **General** as the timetable type, set the related attendance time parameters as the following:

### Start/End-Work Time

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

### Valid Check-in/out Time

On the time bar, adjust the yellow bar to set the timetable during which the check-in or check-out is valid.

### Calculated as

Set the duration calculated as the actual work duration.

### Late/Early Leave Allowable

Set the timetable for late or early leave.

8. If you select **Flexible** as the timetable type, set the related attendance time parameters as the following:

### Working Hours

The staffs' working hours should be equal or greater than the set value.

### Start Time of Timetable

Calculate the working hours of each day from the set value.

For example, if you have set the working hours as 8 hours, and the start time of timetable as 9:00 am, and the staff A checked-in at 8:00 am and checked-out at 5:00 pm (effective working hours are 9:00 am to 5:00 pm, totally 8 hours), the attendance result for staff A will be calculated as normal.

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



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

10. Click **Save** to add the timetable.

**11. 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.

### 7.11.3 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.

**Basic Settings**

Shift Name: Default Shift

Shift Period: 1 Weekday

Default Timetable

✕ Delete Clear

Time	00:00	02:00	04:00	06:00	08:00	10:00	12:00	14:00	16:00	18:00	20:00	22:00	24:00
Monday						█	█	█	█	█			
Tuesday						█	█	█	█	█			
Wednesday						█	█	█	█	█			
Thursday						█	█	█	█	█			
Friday						█	█	█	█	█			
Saturday													
Sunday													

**Save** **Assign**

**Figure 7-8 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.

## 7.11.4 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.



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**.



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

---



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**.
- 



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).

### 7.11.5 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.

---

## 7.11.6 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 filed 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.

---

## 7.11.7 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 automatically calculate attendance data of the previous day at the time you configured every day.

#### Steps



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.
4. Click **Save**.

The client will calculate the attendance data of the previous day from the time you have configured.

### 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**.



It can only calculate the attendance data within three months.

6. Perform one of the following operations.

<b>Correct Check-in/out</b>	Click <b>Correct Check-in/out</b> to add check-in/out correction.
<b>Report</b>	Click <b>Report</b> to generate the attendance report.
<b>Export</b>	Click <b>Export</b> to export attendance data to local PC.



The exported details are saved in CSV format.

---

## 7.11.8 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.



- 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.

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

**Export Report**      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.

---



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

---



Set the email parameters before you want to enable auto-sending email functions. For details, refer to *Set Email Parameters* in the user manual of the client software.

---

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 <b>Edit</b> to edit its settings.   |
| <b>Delete Report</b>   | Select one added report and click <b>Delete</b> to delete it.   |
| <b>Generate Report</b> | Select one added report and click <b>Report</b> to generate the report instantly and you can view the report details. |

## 7.12 Remote Configuration (Web)

Configure device parameters remotely.

### 7.12.1 Check Device Information

#### Steps

1. Click **Maintenance and Management** → **Device** to enter the device list.
2. Press **CTRL** and click  to enter the remote configuration page.
3. Click **System** → **Device Information** and view the device basic information and the device version information.

## 7.12.2 Edit Device Name

Click **Maintenance and Management** → **Device** to enter the device list.

Press **CTRL** and click  to enter the remote configuration page.

Click **System** → **General** to configure the device name and overwrite record files parameter.

Click **Save**.

## 7.12.3 Edit Time

### Steps

1. Click **Maintenance and Management** → **Device** to enter the device list.
2. Press **CTRL** and click  to enter the remote configuration page.
3. Click **System** → **Time** to configure the time zone.
4. **Optional:** Check **Enable NTP** and set the NTP server address, the NTP port, and the synchronization interval.
5. **Optional:** Check **Enable DST** and set the DST start time, end time and the bias.
6. Click **Save**.

## 7.12.4 Set System Maintenance

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

### Steps

1. Click **Maintenance and Management** → **Device** to enter the device list.
2. Press **CTRL** and click  to enter the remote configuration page.
3. Click **System** → **System Maintenance** .
4. Maintain the device.

#### Reboot

The device starts rebooting.

#### Restore Default Settings

Restore the device settings to the default ones, excluding the IP address.

#### Restore All

Restore the device parameters to the default ones. The device should be activated after restoring.

#### Restore Part of Settings

Restore all settings except communication settings and the remote user settings to default ones.

#### Import Configuration File

Import the configuration file from the local PC to the device.

 **Note**

The configuration file contains the device parameters.

---

### Export Configuration File

Export the configuration file from the device to the local PC.

---

 **Note**

The configuration file contains the device parameters.

---

### 5. Remotely upgrade the device.

1) In the Remote Upgrade part, select an upgrade type.

---

 **Note**

- You need to set the device ID before upgrading if you select Controller Upgrade File as the remote upgrade type.
  - Only the card reader that connected via RS-485 protocol supports upgrading.
- 

2) Click ... to select an upgrade file.

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

---

 **Note**

Do not power off during the upgrading.

---

## 7.12.5 Configure RS-485 Parameters

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

### Steps

1. Click **Maintenance and Management** → **Device** to enter the device list.
  2. Press **CTRL** and click  to enter the remote configuration page.
  3. Click **System** → **RS-485 Settings** to enter the Configuring the RS-485 Parameters tab.
  4. Select the serial No. of the port from the dropdown list to set the RS-485 parameters.
  5. Set the baud rate, data bit, the stop bit, parity, flow control, communication mode, working mode, and the connection mode from the dropdown list.
  6. Click **Save** and the configured parameters will be applied to the device automatically.
- 

 **Note**

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

---

## 7.12.6 Manage User

### Steps

1. Click **Maintenance and Management → Device** to enter the device list.
2. Press **CTRL** and click  to enter the remote configuration page.
3. Click **System → User** .
4. Click **Add** to add the user (Do not support by the elevator controller).
5. **Optional:** Select a user in the user list and click **Edit** to edit the user.  
You are able to edit the user password, the IP address, the MAC address and the user permission.
6. Click **OK**.

## 7.12.7 Set Security

### Steps

1. Click **Maintenance and Management → Device** to enter the device list.
2. Press **CTRL** and click  to enter the remote configuration page.
3. Click **System → Security** .
4. Select the encryption mode in the dropdown list.
5. You can select **Compatible Mode** or **Encryption Mode**.

#### Compatible Mode

The user information verification is compatible with the old client software version when logging in.

#### Encryption Mode

High security level during the user information verification when logging in.

6. **Optional:** Check **Enable SSH**.
7. Click **Save**.

## 7.12.8 Configure Network Parameters

### Steps

1. Click **Maintenance and Management → Device** to enter the device list.
2. Press **CTRL** and click  to enter the remote configuration page.
3. Click **Network → General** .  
You can configure the NIC type, the IPv4 address, the subnet mask (IPv4), the default gateway (IPv4), MTU, and the device port.
4. Click **Save**.

### 7.12.9 Configure Advanced Network

Click **Maintenance and Management** → **Device** to enter the device list.

Press **CTRL** and click  to enter the remote configuration page.

Click **Network** → **Advanced Settings** and you can configure the DNS IP address 1 and the DNS IP address.

Click **Save** to save the settings.

### 7.12.10 Configure Wi-Fi

#### Steps

1. Click **Maintenance and Management** → **Device** to enter the device list.

2. Press **CTRL** and click  to enter the remote configuration page.

3. Click **Network** → **Wi-Fi**.

4. Check **Enable** to enable the Wi-Fi function.

5. Input the hot spot name or you can click **Select...** to select a network.

6. Input the Wi-Fi password.

7. **Optional:** Click **Refresh** to refresh the network status

8. **Optional:** Select the NIC Type.

9. **Optional:** Select to uncheck **Enable DHCP** and set the IP address, the subnet mask, the default gateway, the MAC address, the DNS1 IP Address, and the DNS2 IP address.

10. Click **Save**.

### 7.12.11 Configure SIP Parameters

Set the main station's IP address and the SIP server's IP address. After setting the parameters, you can communicate among the access control device, door station, indoor station, main station, and the platform.

---

#### **Note**

Only the access control device and other devices or systems (such as door station, indoor station, main station, platform) are in the same IP segment, the two-way audio can be performed.

---

Click **Maintenance and Management** → **Device** to enter the device list.

Press **CTRL** and click  to enter the remote configuration page.

Click **Network** → **Linked Network Configuration** and set the main station's IP address and SIP server's IP address.

Click **Save**.

## 7.12.12 Configure Face Picture Parameters

### Steps

1. Click **Maintenance and Management** → **Device** to enter the device list.
2. Press **CTRL** and click  to enter the remote configuration page.
3. Click **Other** → **Face Picture Parameters** to enter the Configuring Face Picture Parameters page.

### Min. Detection Width (Close to)

When the distance between the camera and the user is short, the parameter represents the minimum percentage of the facial width in the total width of the recognition area.

The actual percentage should be larger than the configured value when face picture authentication. In this condition, the device will not detect other parameters.

### Pitch Angle

The maximum pitch angle when face authentication. By default, the angle is 30°.

### Yaw Angle

The maximum yaw angle when face authentication. By default, the angle is 45°.

### Min. Detection Area (Width)

When the distance between the camera and the user is long, the parameter represents the minimum percentage of the facial width in the total width of the recognition area.

The actual percentage should be larger than the configured value when face picture authentication. Other percentages, distances and angles in this table should also meet their conditions.

Recommended Value: 14

### Min. Detection Area (Height)

When the distance between the camera and the user is long, the parameter represents the minimum percentage of the facial height in the total height of the recognition area.

The actual percentage should be larger than the configured value when face picture authentication. Other percentages, distances and angles in this table should also meet their conditions.

Recommended Value: 12

### Margin (Left)

The distance percentage from the face left side to the left margin in the recognition area.

The actual distance percentage should be larger than the configured value when face picture authentication. Other percentages, distances, and angles should also meet their conditions.

### Margin (Right)

The distance percentage from the face right side to the right margin in the recognition area.

The actual distance percentage should be larger than the configured value when face picture authentication. Other percentages, distances, and angles should also meet their conditions.

### Margin (Top)

The distance percentage from the face top side to the top margin in the recognition area.

The actual distance percentage should be larger than the configured value when face picture authentication. Other percentages, distances, and angles should also meet their conditions.

### Margin (Bottom)

The distance percentage from the face bottom side to the bottom margin in the recognition area.

The actual distance percentage should be larger than the configured value when face picture authentication. Other percentages, distances, and angles should also meet their conditions.

### Pupillary Distance

The minimum resolution between two pupils when face recognition.

The actual resolution should be larger than the configured value.

By default, the resolution is 40.

You can set the face picture parameters when authenticating.

4. Click **Save**.

## 7.12.13 Configure Supplement Light Parameters

You can turn on or off the supplement light. You can also adjust the supplement light brightness.

### Steps

1. Click **Maintenance and Management** → **Device** to enter the device list.
2. Press **CTRL** and click  to enter the remote configuration page.
3. Click **Other** → **Supplement Light Parameters** to enter the Configuring Supplement Light Parameters page.
4. Select a supplement light No. from the drop-down list.



### Note

Light 1 refers to white light and Light 2 refers to IR light.

5. Select a supplement light mode from the drop-down list.
6. **Optional:** If the supplement light mode is **Auto**, you can set the supplement light brightness.
7. Click **Save** to save the settings.

## 7.12.14 Set Room No.

Set the device type, community No., building No., floor No., and unit No., and room No.

Click **Maintenance and Management** → **Device** to enter the device list.

Press **CTRL** and click  to enter the remote configuration page.

Click **Other** → **Device Room No.** and Set the device type, community No., building No., floor No., and unit No., and room No.

### 7.12.15 Configure Video and Audio Parameters

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

#### Steps

1. Click **Maintenance and Management** → **Device** to enter the device list.
2. Press **CTRL** and click  to enter the remote configuration page.
3. Click **Image** → **Video & Audio** to enter the settings page.
4. Set the device camera's parameters, including the stream type, the bitrate type, the video quality, the frame rate, the audio encoding type, the video type, the bitrate, the resolution, and the I frame interval.
5. Click **Save**.

### 7.12.16 Configure Volume Input or Output

#### Steps

1. Click **Maintenance and Management** → **Device** to enter the device list.
2. Press **CTRL** and click  to enter the remote configuration page.
3. Click **Image** → **Volume Input/Output** to enter the Configuring the Volume Input or Output page.
4. Set the device input volume or output volume.
5. Click **Save**.

### 7.12.17 View Relay Status

Click **Maintenance and Management** → **Device** to enter the device list.

Press **CTRL** and click  to enter the remote configuration page.

Click **Status** → **Relay** and you can view the relay status.

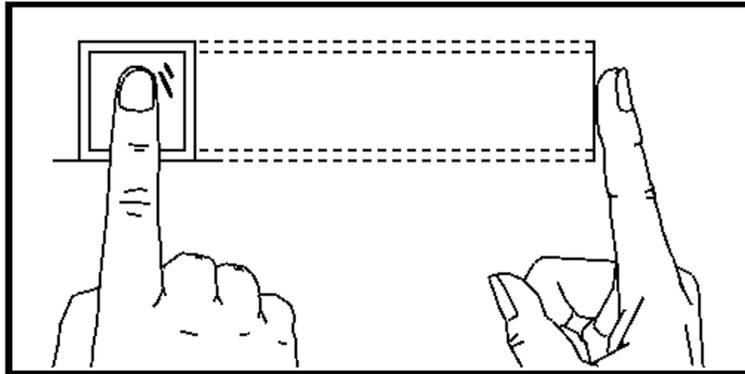
## Appendix A. Tips for Scanning Fingerprint

### Recommended Finger

Forefinger, middle finger or the third finger.

### Correct Scanning

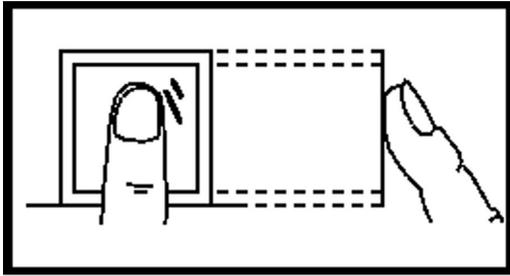
The figure displayed below is the correct way to scan your finger:



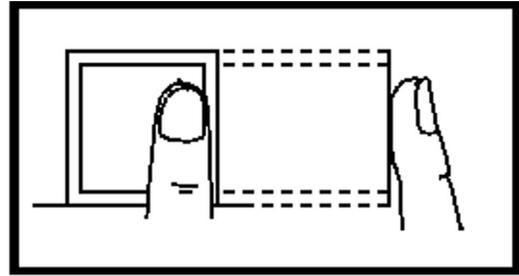
You should press your finger on the scanner horizontally. The center of your scanned finger should align with the scanner center.

### Incorrect Scanning

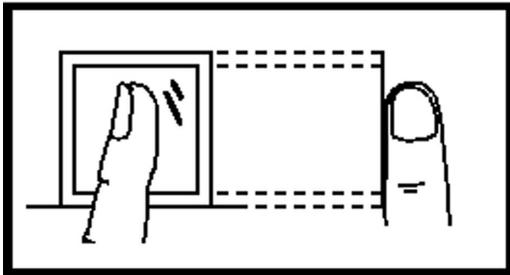
The figures of scanning fingerprint displayed below are incorrect:



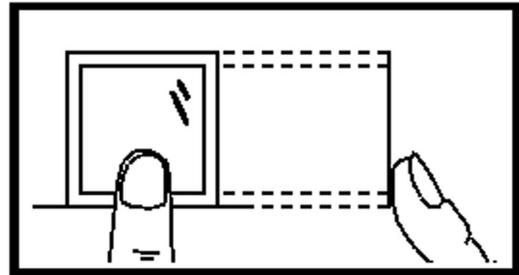
Vertical



Edge I



Side



Edge II

### Environment

The scanner should avoid direct sun 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.

### Others

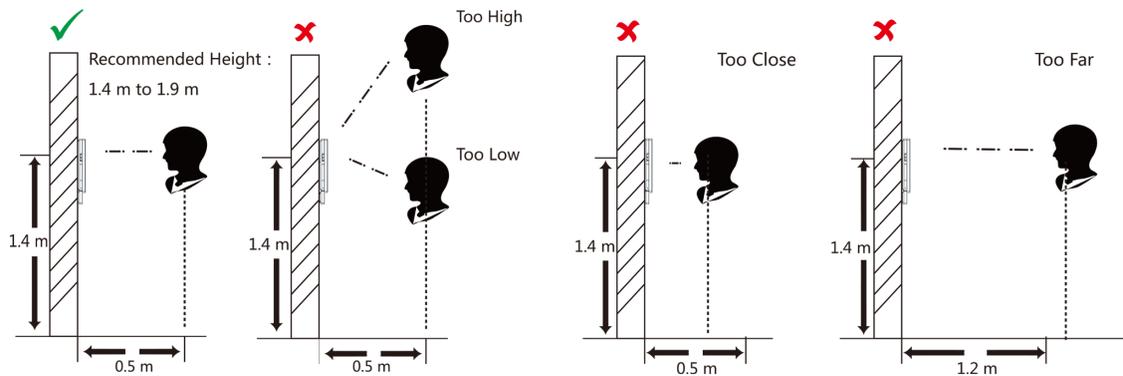
If your fingerprint is shallow, or it is hard to scan your fingerprint, we recommend you to use other authentication methods.

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

## Appendix B. 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.

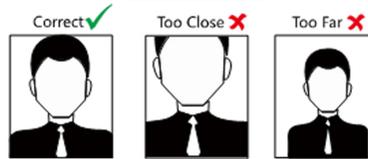
### Posture

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.



## Appendix C. Tips for Installation Environment

### 1. Light Source Illumination Reference Value



Candle: 10Lux

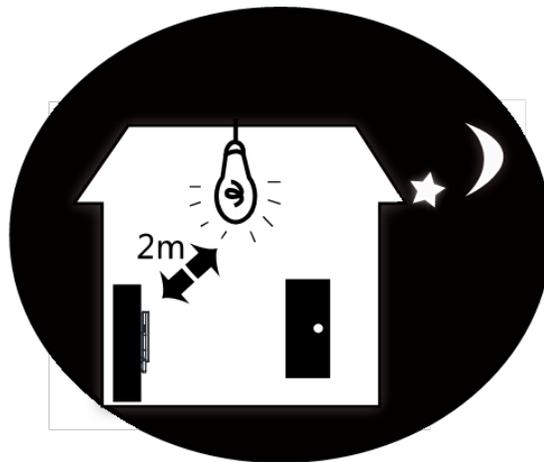
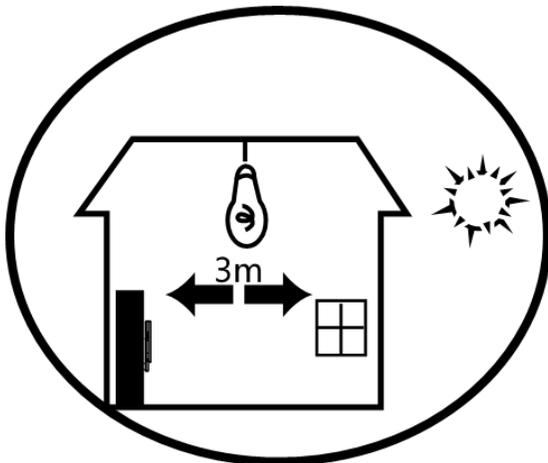


Bulb: 100~850Lux

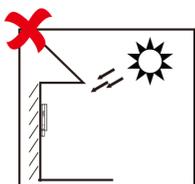


Sunlight: More than 1200Lux

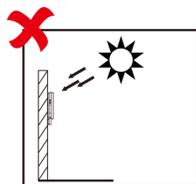
2. Install the device at least 2 meters away from the light, and at least 3 meters away from the window or door.



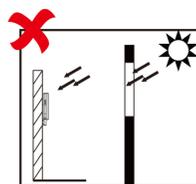
### 3. Avoid backlight, direct and indirect sunlight



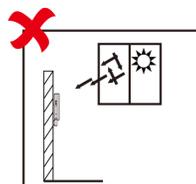
Backlight



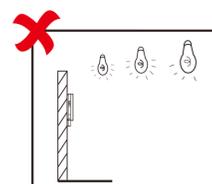
Direct Sunlight



Direct Sunlight



Indirect Sunlight  
through Window



Close to Light

## Appendix D. Relationship between Wake-up Distance and Environment

	Environment	Short	Medium	Long
At Dusk (Low Illumination)	Normal White Wall	1.06 m	1.67 m	3.62 m
	Acrylic Wall in Laboratory	0.85/0.73 m	1.30/1.21 m	4.16 m
	Human Body	0.74 m	0.94 m	1.50/1.45 m
	Window Glass	/	/	/
At Night (Turn Light Off)	Normal White Wall	0.97 m	1.61 m	3.91 m
	Acrylic Wall in Laboratory	0.79 m	1.32 m	3.67 m
	Human Body	0.47 m	1.03 m	1.65 m
	Window Glass	1.18/1.65 m (Turn on Light at Night)	1.53/2.66 m (Turn on Light at Night)	3.35 m
Daytime (Turn Fluorescent Lamp on)	Normal White Wall	1.1 m	1.8 m	> 4 m
	Acrylic Wall in Laboratory	0.8 m	1.5 m	3.1 m
	Human Body	0.7/0.6 m	1.2/1.14 m	1.5/1.42 m
	Window Glass	1.1 m	1.8 m	> 4 m
Daytime (Turn Camera to Sunlight)	Human Body	0.3/0.26 m	0.56/0.5 m	1.03/1.06 m
Daytime (Turn device's back to Sunlight)	Human Body	0.36 m	0.6 m	1.25 m
At Night (Turn Light on)	Acrylic Black Wall	0.56 m	0.83 m	1.25 m

## Appendix E. Dimension

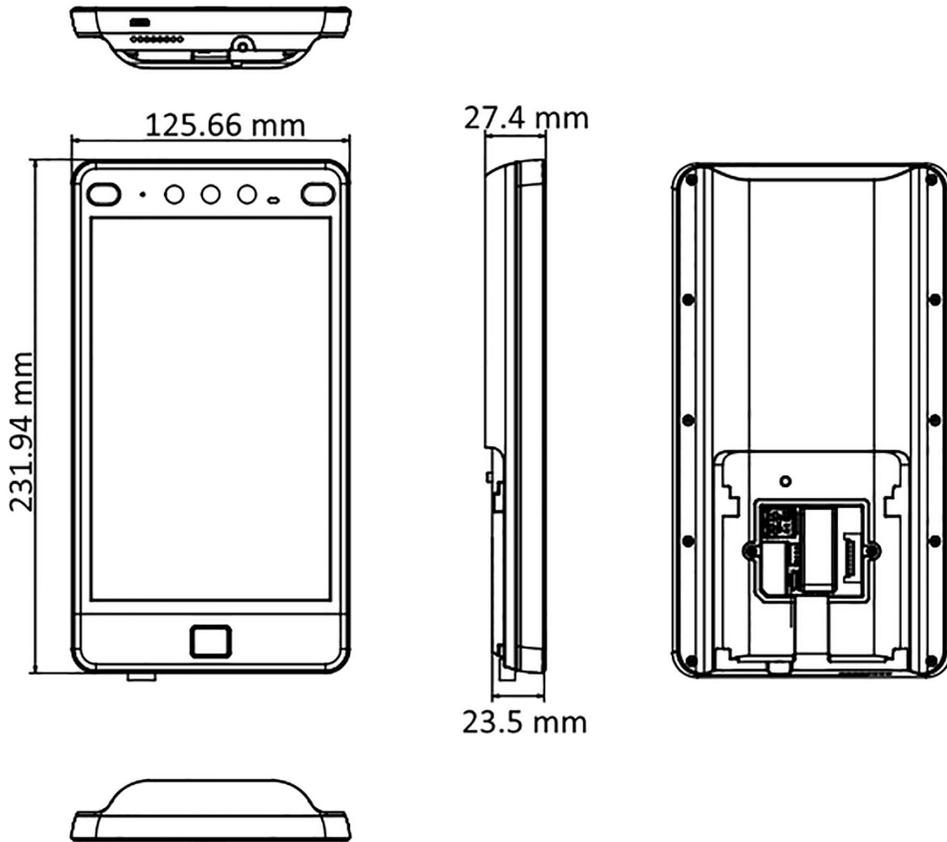


Figure E-1 Dimension



See Far, Go Further