DS-K5671-3XF Series Face Recognition Terminal

User Manual

Legal Information

©2020 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 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 INSPECTION, 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 LATER PREVAILS.

Data Protection

During the use of device, personal data will be collected, stored and processed. To protect data, the development of Hikvision devices incorporates privacy by design principles. For example, for device with facial recognition features, biometrics data is stored in your device with encryption method; for fingerprint device, only fingerprint template will be saved, which is impossible to reconstruct a fingerprint image.
As data controller, you are advised to collect, store, process and transfer data in accordance with the applicable data protection laws and regulations, including without limitation, conducting security controls to safeguard personal data, such as, implementing reasonable administrative and physical security controls, conduct periodic reviews and assessments of the effectiveness of your security controls.

Symbol Conventions

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

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

Regulatory Information

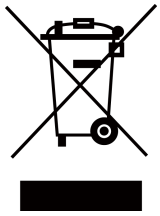
FCC Information

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

CE 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

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

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.

⚠	⚠
Dangers: Follow these safeguards to prevent serious injury or death.	**Cautions:** 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 12 VDC, 2 A.
- 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 100% applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.
- Working temperature: 0 °C to 50 °C; Working humidity: 10% to 90% (no condensing)
- Indoor use. The device should be at least 2 meters away from the light, and at least 3 meters away from the window.
- Version: 1.0, Issue Date: 20200519

Available Models

Product Name	Model
Face Recognition Terminal	DS-K5671-3XF/ZU

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

Chapter 1 Overview 1
1.1 Overview 1
1.2 Features 1
Chapter 2 Appearance 2
Chapter 3 Installation 3
3.1 Installation Environment 3
3.2 Mount With Bracket 3
3.2.1 Preparation before Mounting with Bracket 3
3.2.2 Mount with Bracket 5
Chapter 4 Wiring 7
4.1 Terminal Description 7
4.2 Wire Normal Device 9
4.3 Wire Secure Door Control Unit 10
Chapter 5 Activation 12
5.1 Activate via Device 12
5.2 Activate via SADP 13
5.3 Activate Device via Client Software 14
Chapter 6 Basic Operation 16
6.1 Set Application Mode 16
6.2 Login 17
6.2.1 Login For First Time 17
6.2.2 Login by Administrator 18
6.3 Communication Settings 20
6.3.1 Set Network Parameters 21
6.3.2 Set Wi-Fi Parameters 21
6.3.3 Set RS-485 Parameters 22

6.3.4 Set Wiegand Parameters 23
6.4 User Management 24
6.4.1 Add Administrator 24
6.4.2 Add Face Picture 25
6.4.3 Add Card 27
6.4.4 Add Password 28
6.4.5 Set Authentication Mode 29
6.4.6 Search and Edit User 29
6.5 Temperature Measurement 30
6.5.1 Temperature Measurement Settings 30
6.5.2 Black Body Settings 32
6.6 Import and Export Data 34
6.6.1 Export Data 34
6.6.2 Import Data 34
6.7 Identity Authentication 35
6.7.1 Authenticate via Multiple Credential 35
6.7.2 Authenticate via Single Credential 36
6.8 System Settings 36
6.8.1 Set Basic Parameters 36
6.8.2 Set Face Picture Parameters 37
6.8.3 Set Time 40
6.9 Set Access Control Parameters 40
6.10 Maintenance 42
6.10.1 Upgrade Firmware 42
6.10.2 Data Management 42
6.10.3 Log Query 43
6.11 Time and Attendance Status Settings 44
6.11.1 Disable Attendance Mode via Device 44

6.11.2 Set Auto Attendance via Device 44
6.11.3 Set Manual Attendance via Device 45
6.11.4 Set Manual and Auto Attendance via Device 46
6.12 View System Information 48
6.13 Video Intercom 49
6.13.1 Call Client Software from Device 49
6.13.2 Call Main Station from Device 50
6.13.3 Call Device from Client Software 50
6.13.4 Call Indoor Station from Device 51
Chapter 7 Client Software Configuration 52
7.1 Configuration Flow of Client Software 52
7.2 Device Management 52
7.2.1 Add Device 53
7.2.2 Reset Device Password 60
7.3 Group Management 61
7.3.1 Add Group 61
7.3.2 Import Resources to Group 62
7.3.3 Edit Resource Parameters 62
7.3.4 Remove Resources from Group 63
7.4 Person Management 63
7.4.1 Add Organization 63
7.4.2 Configure Basic Information 64
7.4.3 Issue a Card by Local Mode 64
7.4.4 Upload a Face Photo from Local PC 66
7.4.5 Take a Photo via Client 66
7.4.6 Collect Face via Access Control Device 68
7.4.7 Configure Access Control Information 68
7.4.8 Customize Person Information 70

7.4.9 Configure Resident Information 71
7.4.10 Configure Additional Information 71
7.4.11 Import and Export Person Identify Information 72
7.4.12 Import Person Information 72
7.4.13 Import Person Pictures 72
7.4.14 Export Person Information 73
7.4.15 Export Person Pictures 73
7.4.16 Get Person Information from Access Control Device 74
7.4.17 Move Persons to Another Organization 75
7.4.18 Issue Cards to Persons in Batch 75
7.4.19 Report Card Loss 75
7.4.20 Set Card Issuing Parameters 76
7.5 Configure Schedule and Template 77
7.5.1 Add Holiday 77
7.5.2 Add Template 78
7.6 Set Access Group to Assign Access Authorization to Persons 79
7.7 Configure Advanced Functions 81
7.7.1 Configure Device Parameters 81
7.7.2 Configure Remaining Open/Closed 87
7.7.3 Configure Multi-Factor Authentication 88
7.7.4 Configure Card Reader Authentication Mode and Schedule 90
7.7.5 Configure First Person In 92
7.7.6 Configure Anti-Passback 93
7.7.7 Configure Device Parameters 94
7.8 Configure Linkage Actions for Access Control 100
7.8.1 Configure Client Actions for Access Event 100
7.8.2 Configure Device Actions for Access Event 101
7.8.3 Configure Device Actions for Card Swiping 102

7.8.4 Configure Device Actions for Person ID 103
7.9 Door Control 104
7.9.1 Control Door Status 104
7.9.2 Check Real-Time Access Records 105
7.10 Event Center 105
7.10.1 Enable Receiving Event from Devices 106
7.10.2 View Real-Time Events 106
7.10.3 Search Historical Events 108
7.11 Time and Attendance 110
7.11.1 Configure Attendance Parameters 110
7.11.2 Add General Timetable 116
7.11.3 Add Shift 118
7.11.4 Manage Shift Schedule 120
7.11.5 Manually Correct Check-in/out Record 123
7.11.6 Add Leave and Business Trip 124
7.11.7 Calculate Attendance Data 125
7.11.8 Attendance Statistics 126
7.12 Remote Configuration (Web) 129
7.12.1 View Device Information 129
7.12.2 Change Device Password 130
7.12.3 Time Management 131
7.12.4 System Maintenance 132
7.12.5 Configure RS-485 Parameters 133
7.12.6 Security Mode Settings 133
7.12.7 Network Parameters Settings 134
7.12.8 Report Strategy Settings 134
7.12.9 Network Center Parameters Settings 134
7.12.10 Configure Wi-Fi 135

7.12.11 Configure SIP Parameters 135
7.12.12 Set Relay Parameters 135
7.12.13 Set Access Control Parameters 136
7.12.14 Set Face Recognition Terminal Parameters 136
7.12.15 Configure Face Picture Parameters 137
7.12.16 Configure Supplement Light Parameters 138
7.12.17 Set Device No. 139
7.12.18 Configure Video and Audio Parameters 139
7.12.19 Configure Volume Input or Output 139
7.12.20 Operate Relay 139
7.12.21 View Relay Status 139
Appendix A. Tips When Collecting/Comparing Face Picture 141
Appendix B. Tips for Installation Environment 142
Appendix C. Dimension 143

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

- Compatible with Hikvision turnstile
- Communicates with the third-party turnstile via IO output or Wiegand
- Supports Vanadium Oxide uncooled sensor to measure target's temperature
- Temperature measuring range: 30 °C to 45 °C (86 °F to 113 °F), accuracy: 0.1 °C, deviation: ± 0.5 °C without black body calibration
- Recognition distance: 0.3 to 2 m
- Fast temperature measurement mode: Detects face and takes skin-surface temperature without identity authentication.
- Multiple authentication modes with temperature measure are available
- Face mask wearing alert
  If the recognizing face does not wear a mask, the device will prompt a voice reminder. At the same time, the authentication or attendance is valid.
- Forced mask wearing alert
  If the recognizing face does not wear a mask, the device will prompt a voice reminder. At the same time, the authentication or attendance will be failed.
- Displays temperature measurement results on the authentication page
- Triggers voice prompt when detecting abnormal temperature
- Configurable door status (open/close) when detecting abnormal temperature
- Transmits online and offline temperature information to the client software via TCP/IP communication and saves the data on the client software
- Adjustable supplement light brightness
- High performance processor with deep learning algorithm
- 50,000 face capacity and 100,000 event capacity
- Face recognition duration ≤ 0.2 s/User; face recognition accuracy rate ≥ 99%
- Transmits and saves the comparison results and the captured pictures to the client software or others
- NTP, manually time synchronization, and auto synchronization
- Watchdog design for protecting the device and ensuring device running properly
- Supports 6 attendance status, including check in, check out, break in, break out, overtime in, overtime out
- Audio prompt for authentication result

Chapter 2 Appearance

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

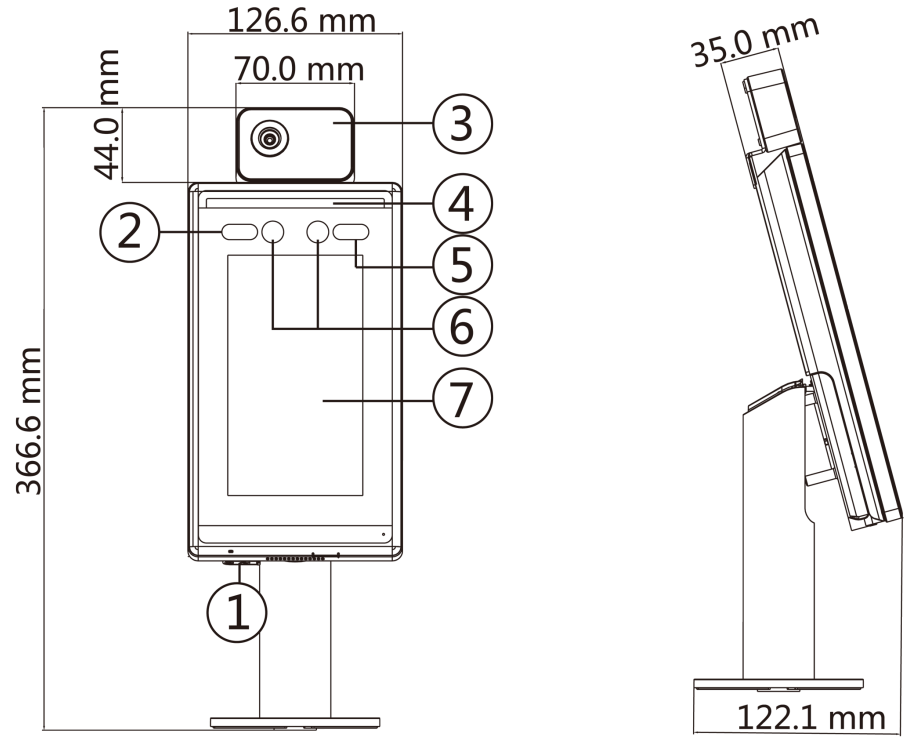


Figure 2-1 Face Recognition Terminal Diagram

Table 2-1 Description of Face Recognition Terminal

No.	Name
1	USB Interface
2	IR Light
3	Thermographic Module
4	White Light
5	IR Light
6	Camera
7	Touch Screen

Chapter 3 Installation

3.1 Installation Environment

- Avoid backlight, direct sunlight, and indirect sunlight.
- For better face recognition, there should be light source in or near the installation environment.
- Sunlight, wind, hot/cool air from air conditioner and other external factors, which may affect surface temperature, will create the deviation of the temperature measurement. In order to get an accurate result, make sure the device is applied indoors and windlessly (where is relatively isolated from the outdoors). The working temperature should keep between 10 °C and 35 °C. If there are no suitable environments for temperature measurement (the area faces the indoor and connects the outdoor, the area at the door of the indoor environment, etc.), building a temporary temperature measurement environment is suggested.
- Influence Factors of Temperature Measurement:
  Wind: The wind will take the heat away, which may affect the measurement result.
  Sweat: The sweat will take the heat away, which may affect the measurement result.
  Air Conditioner (Cool Air): If the indoor temperature is low, the surface temperature may also lower than the actual temperature, which may affect the measurement result.
  Air Conditioner (Heat) or Heating: If the indoor temperature is high, the surface temperature may also higher than the actual temperature, which may affect the measurement result.
- In order to make the device work properly, you should wait for 90 min after the device is powered on.
- For details about installation environment, see ***Tips for Installation Environment*** .

3.2 Mount With Bracket

3.2.1 Preparation before Mounting with Bracket

Make sure you have drilled holes on the turnstile. If not, follow the steps below to drill holes.

Steps

1. Use 4 screws (M3 or M4), secured by flange nuts, to install the reinforcing board on the inner surface of the turnstile.

   Note

   The distance between the turnstile and the edge should be no longer than 10 mm.

2. Drill holes on the turnstile's inner surface according to the figure displayed below. And install water-proof nut.

Note

Solder after pressing rivets to avoid water from entering.

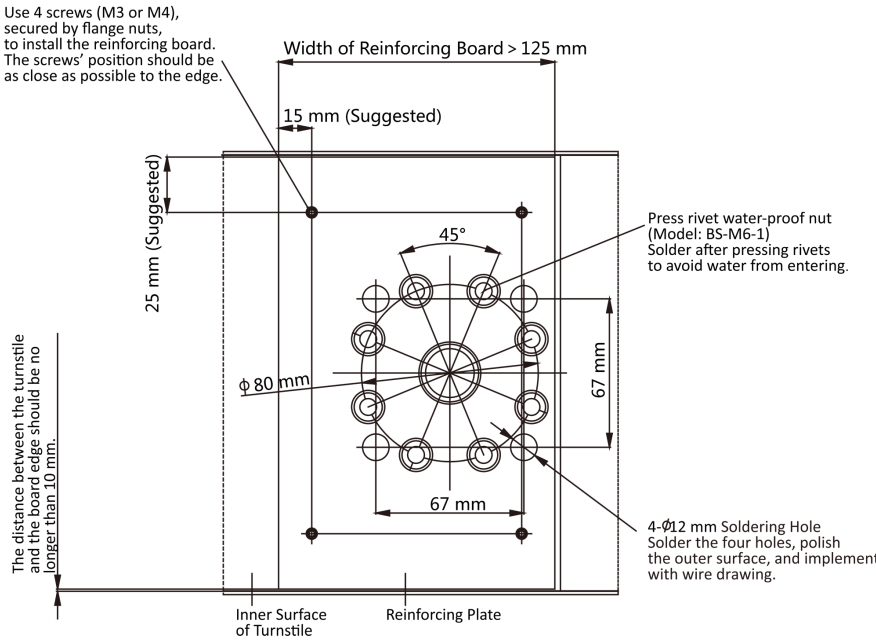


Figure 3-1 Drill Holes on Turnstile

3. Solder the other four holes, polish the surface, and implement wire drawing.
4. Solder circular tubes on the turnstile's inner surface to avoid water from entering.

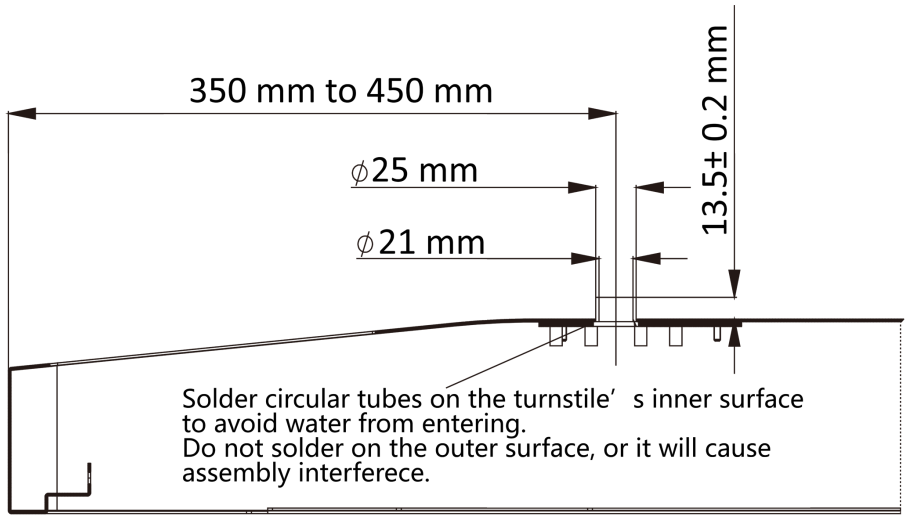


Figure 3-2 Solder Tubes

3.2.2 Mount with Bracket

Steps

1. Rotate to open the lower cover.
2. Route the cables through the cable hole on the turnstile.
3. Align the holes on the base with those on the turnstile and place the device with bracket on the turnstile.
4. Use 4 screws to secure the bracket and the turnstile.

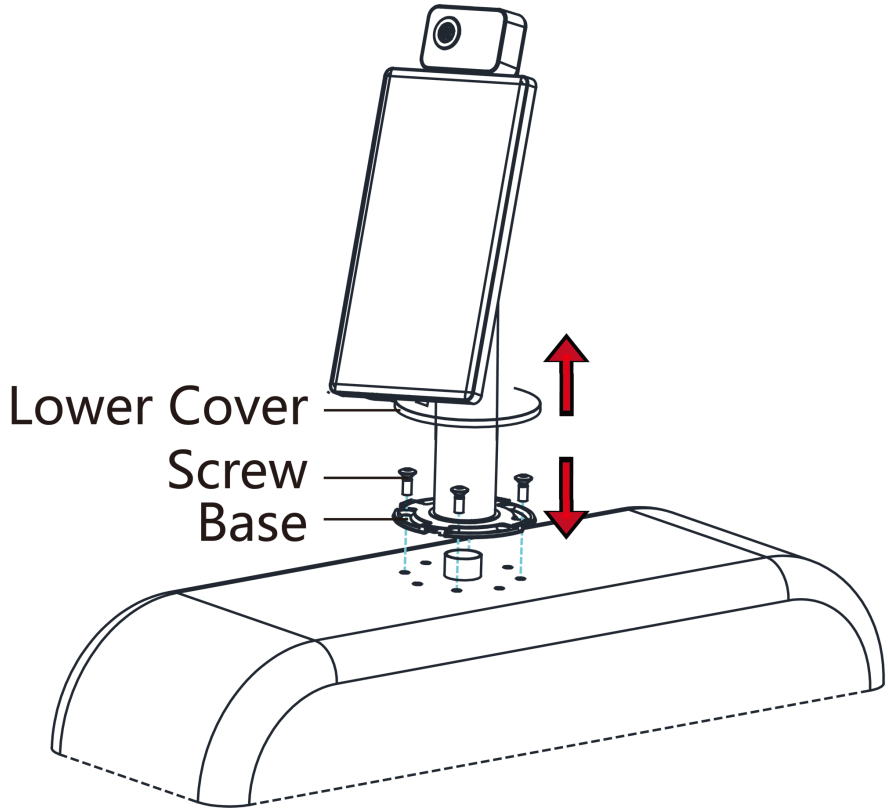


Figure 3-3 Secure Bracket and Turnstile

5. Install the lower cover back on the base and rotate to secure.
6. Adjust the device elevation.
   1) Loosen the screws inside.
   2) Adjust the device elevation.
   3) After adjustment, secure the screws and install the upper cover.

Note

The default elevation angle is 15°. The adjustable elevation angle is from 0° to 15°.

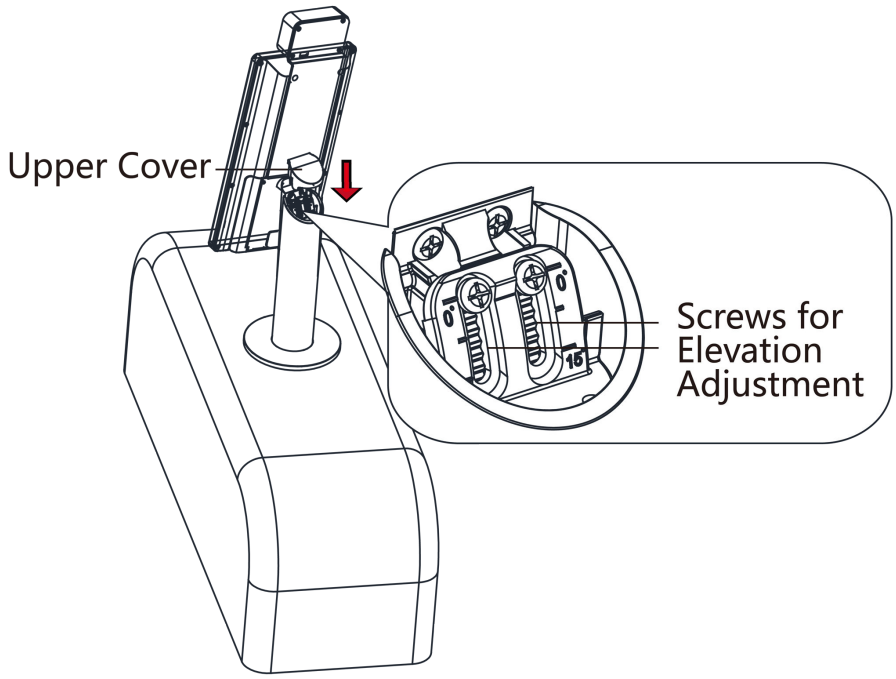


Figure 3-5 Adjust Elevation

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:

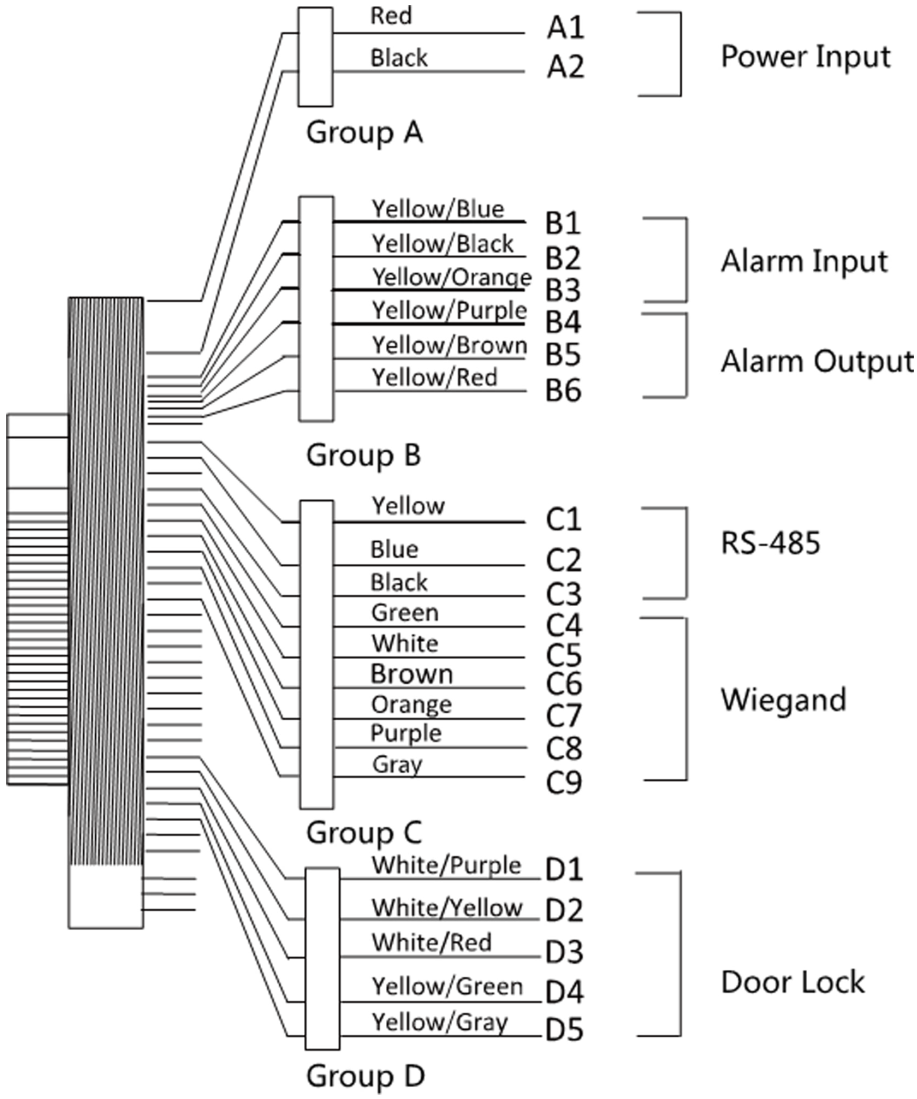


Figure 4-1 Terminal Diagram

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

Group	No.	Function	Color	Name	Description
	B4	Alarm Output	Yellow/Purple	NC	Alarm Output Wiring
	B5		Yellow/Brown	COM	
	B6		Yellow/Red	NO	
Group C	C1	RS-485	Yellow	485+	RS-485 Wiring
	C2		Blue	485-	
	C3		Black	GND	Ground
	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)
	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.

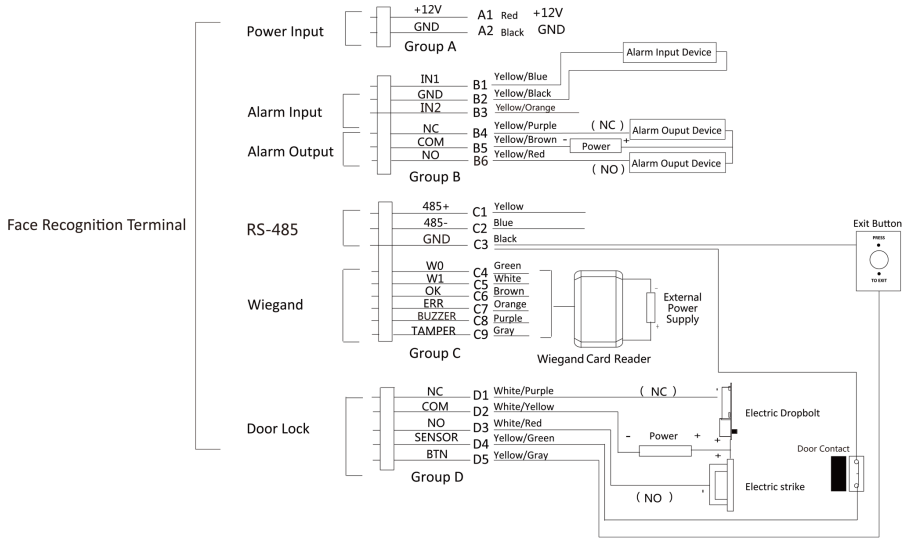


Figure 4-2 Device Wiring

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 power supply for the device should be 12 VDC/2 A. 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.

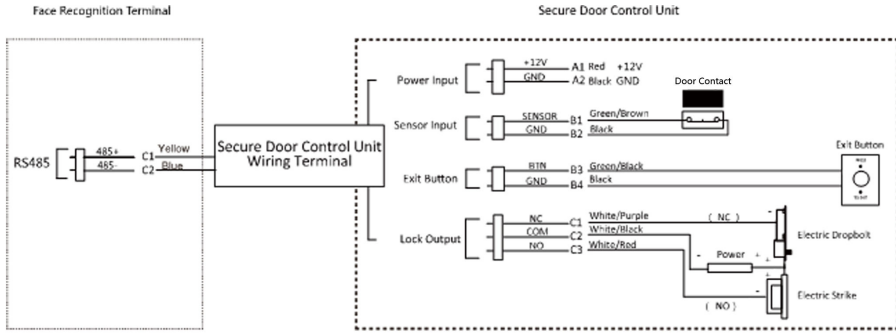


Figure 4-3 Secure Door Control Unit Wiring

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.

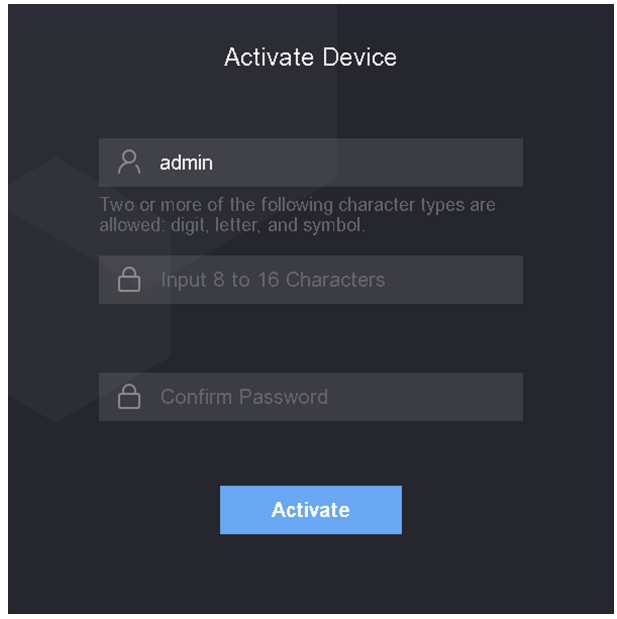


Figure 5-1 Activation Page

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 change your password regularly, especially in the high security system, changing 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.

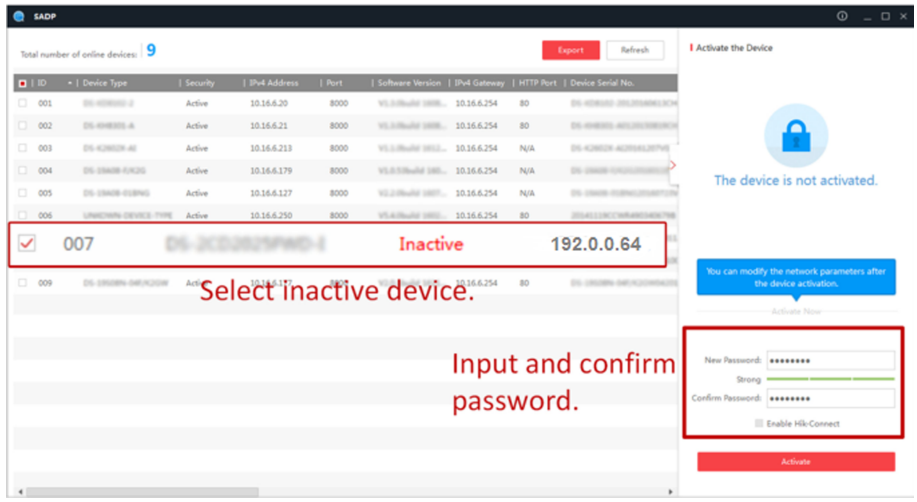
Steps

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.

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 change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.
Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

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

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.

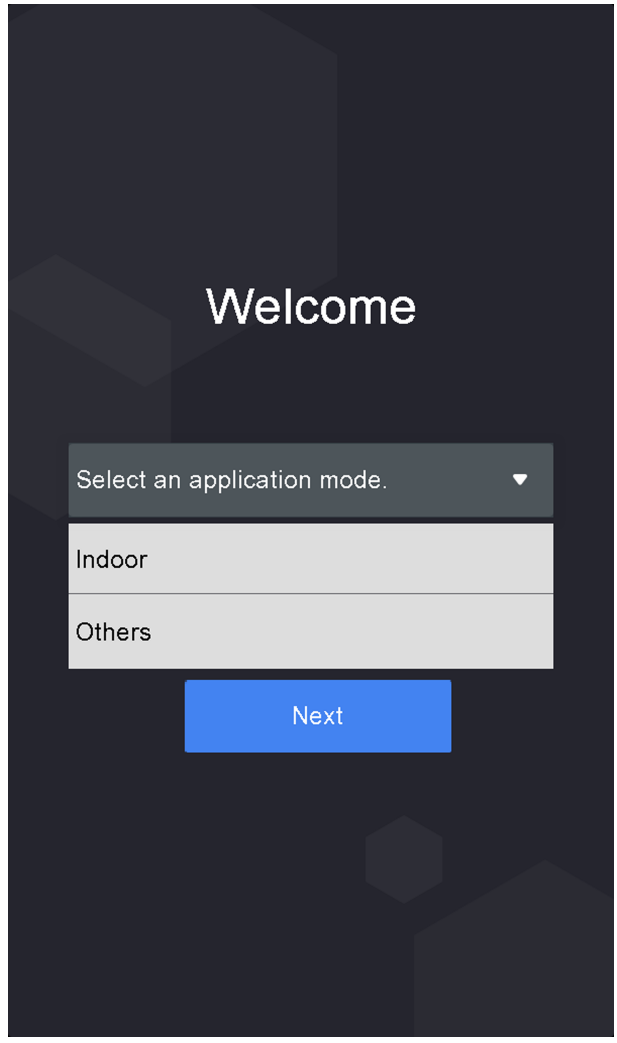


Figure 6-1 Welcome Page

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*.

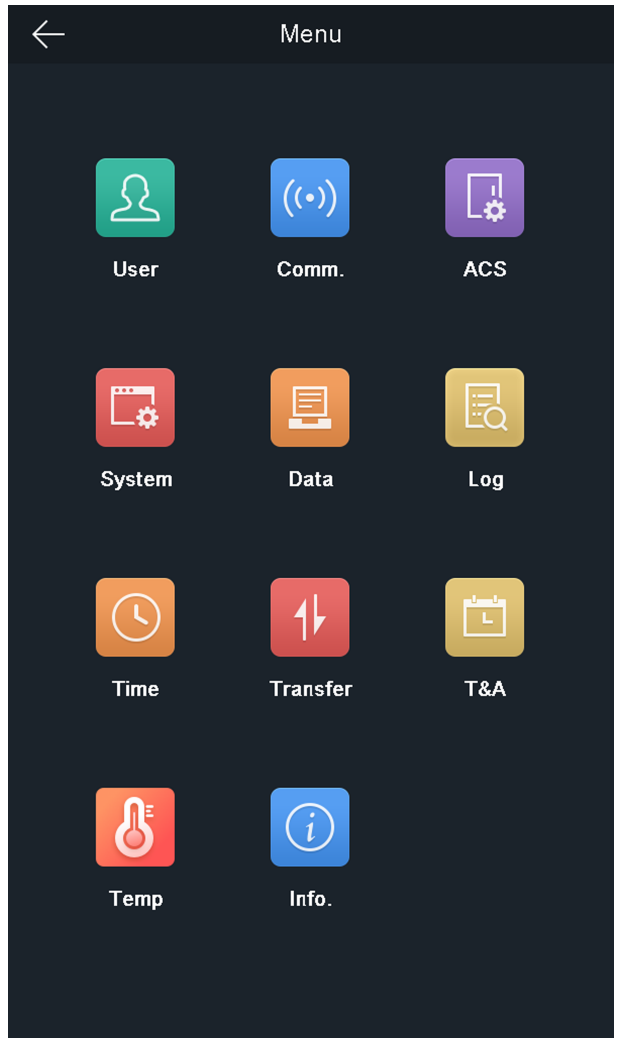


Figure 6-2 Home Page

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.

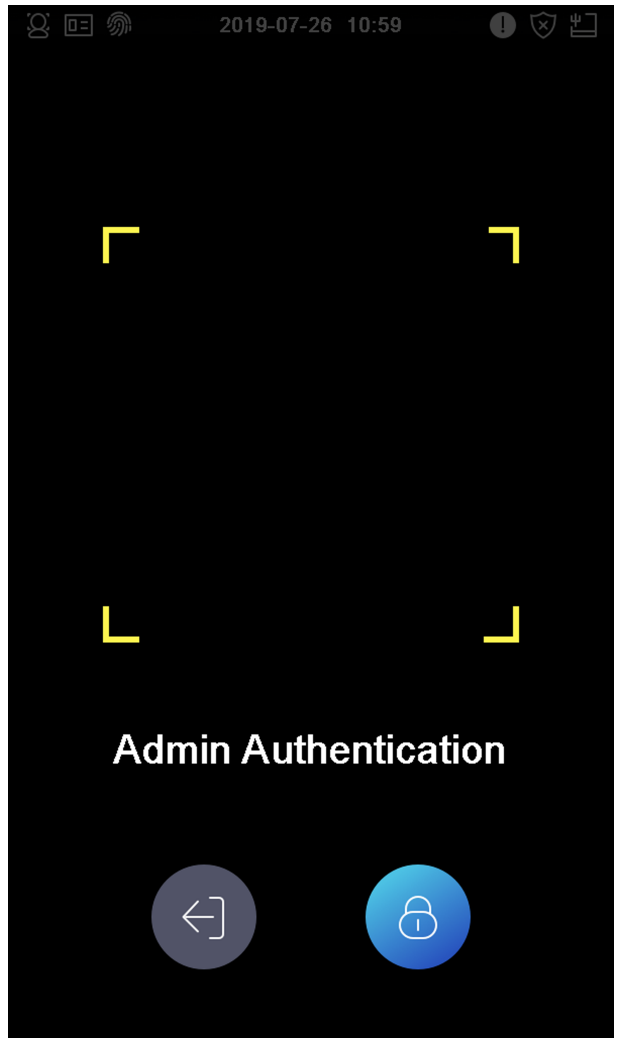


Figure 6-3 Admin Login

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

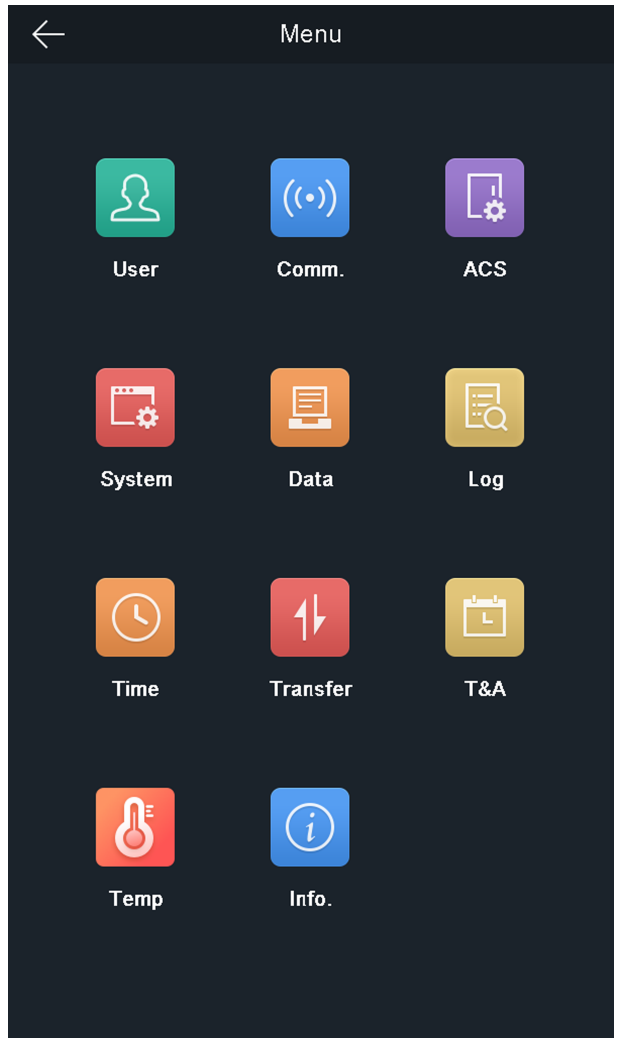


Figure 6-4 Home Page

Note

The device will be locked for 30 minutes after 5 failed face 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, the Wiegand parameters, and enable 3G/4G 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.

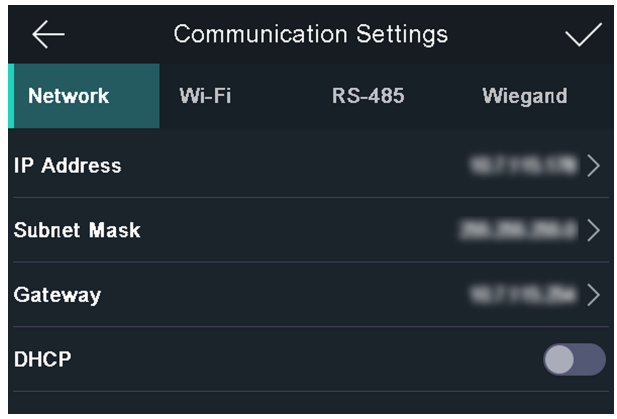


Figure 6-5 Network Settings

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

Note

The function should be supported by the device, or it will not displayed on the configuration page and cannot be used.

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.

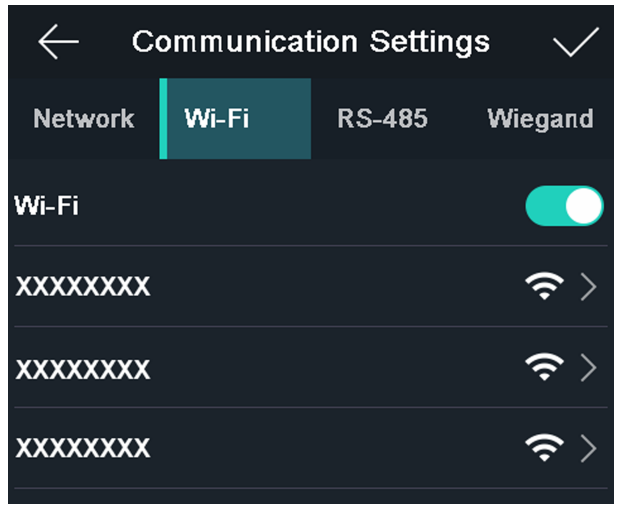


Figure 6-6 Wi-Fi Settings

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 **DHCP**, you should input the Wi-Fi password.
   - If selecting **Static**, you should input the Wi-Fi password, IP address, subnet mask and gateway.

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.

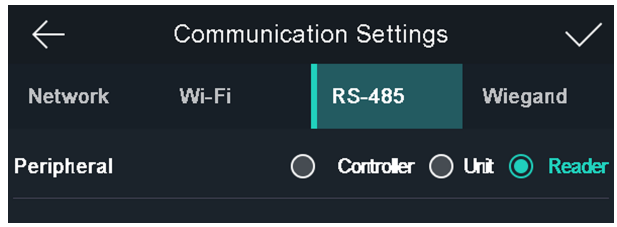


Figure 6-7 Set RS-485 Parameters

3. Select an peripheral type according to your actual needs.

Note

- Controller represents the access controller, Unit represents the secure door control unit and Reader represents the card reader.
- If you select **Controller**: If connect the device to a terminal via the RS-485 interface, set the RS-485 address as 2. If you connect the device to a controller, set the RS-485 address according to the door No.

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.

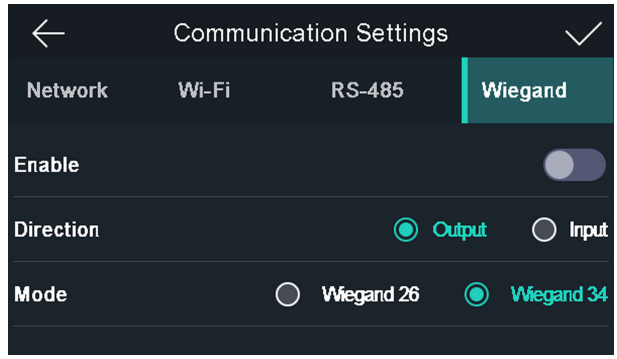


Figure 6-8 Wiegand Settings

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, cards, or password for the administrator.

Note

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

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

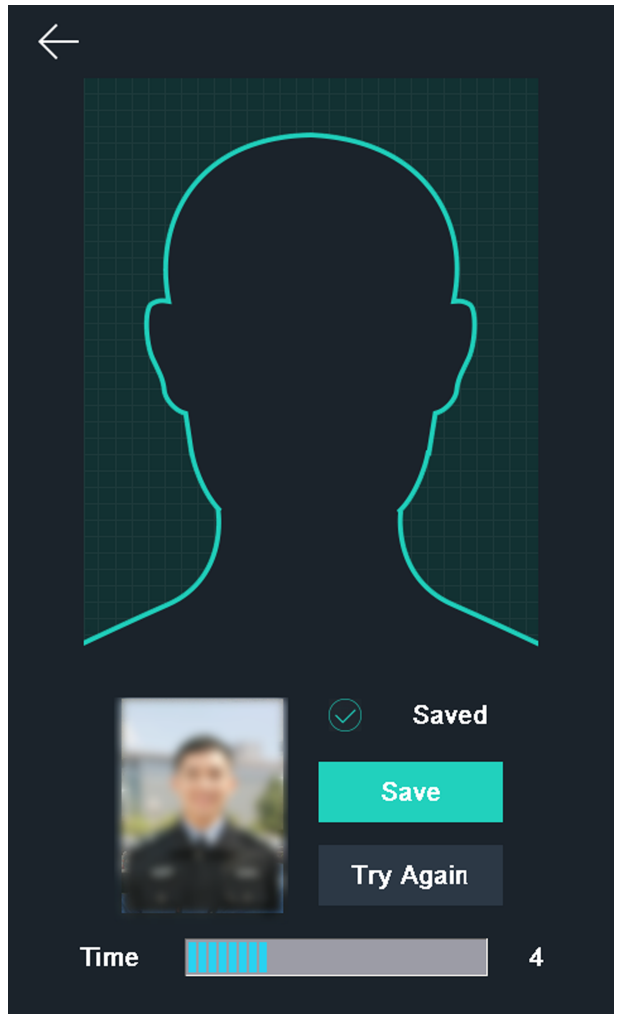


Figure 6-9 Add Face Picture

6. 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.

7. Tap **Save** to save the face picture.
8. **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.

9. 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.

10. Tap ✓ to save the settings.

6.4.3 Add Card

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

Steps

1. Long tap on the initial page and log in the backend.
2. Tap **User → +** to enter the Add User page.
3. 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 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. Tap the Card field and input the card No.
6. 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.

7. **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.

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. Tap ✓ to save the settings.

6.4.4 Add Password

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

Steps

1. Long tap on the initial page and login.
2. Tap **User → +** to enter the Add User page.
3. 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 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. 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.

6. 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.

7. Tap ✓ to save the settings.

6.4.5 Set Authentication Mode

After adding the user's 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.

6.4.6 Search and Edit User

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

Search User

On the User Management page, Tap 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.

Note

The employee ID cannot be edited.

6.5 Temperature Measurement

6.5.1 Temperature Measurement Settings

You can set the temperature measurement parameters, including temperature detection, over-temperature alarm threshold, temperature compensation, door not open when temperature is abnormal, temperature measurement mode, temperature unit, measurement area calibration, measurement area, black body, etc.

On the Home page, tap **Temp** (Temperature) to enter the Temperature Settings page. Edit the temperature measurement parameters on this page and tap ✓ to save the settings.

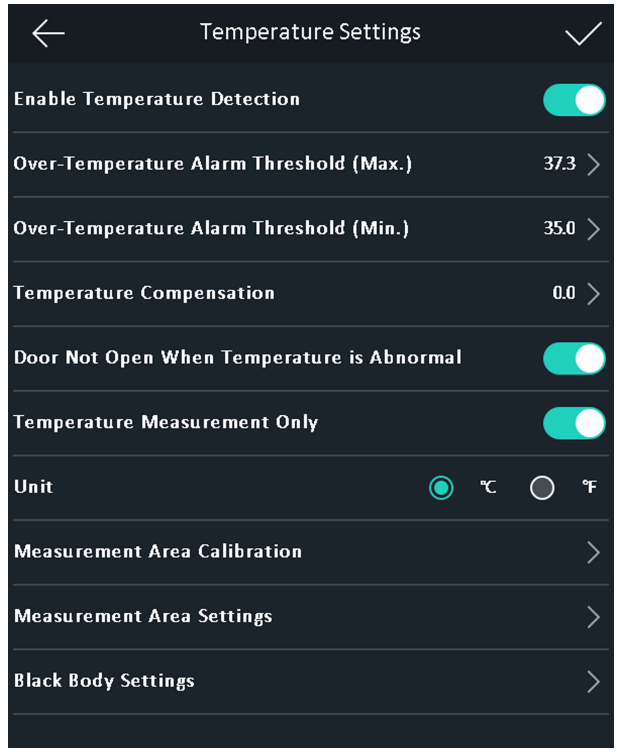


Figure 6-10 Temperature Measurement Parameters

The available parameters descriptions are as follows:

Table 6-1 Temperature Measurement Parameters Descriptions

Parameter	Description
Enable Temperature Detection	When enabling the function, the device will authenticate the permissions and at the same time take the temperature. When disabling the device, the device will authenticate the permissions only.
Over-Temperature Alarm Threshold(Max./Min.)	Edit the threshold according to actual situation. If the detected temperature is higher or lower than the configured parameters, an alarm will be triggered. By default, the value is 37.3°.
Temperature Compensation	If the measured temperature is higher/lower than the actual object's temperature, you can set the compensation temperature here. Available range: -99 °C to 99 °C
Door Not Open When Temperature is Abnormal	When enabling the function, the door will not open when the detected temperature is higher or lower than the configured temperature threshold. By default, the function is enabled.
Temperature Measurement Only	When enabling the function, the device will not authenticate the permissions, but only take the temperature. When disabling the function, the device will authenticate the permissions and at the same time take the temperature.
Unit	Select a temperature unit according to your preference.
Measurement Area Calibration/Measure Area Settings	Configure the temperature measurement area and the correction parameters.
Black Body Settings	When enabling the function, you can configure the black body's parameters, including the distance, temperature, and emissivity. **Note** When measuring the black body, make sure the device's camera faces the black body, and there should be no other objects between the black body and the camera. Once the sample black body is calibrated, make sure the measurement area of the measuring black body should be the same as the calibrated one, or the temperature measurement may be failed.

6.5.2 Black Body Settings

The black body can correct the measuring temperature. You should set the black body parameters if the black body temperature measurement scene is required. If no black bad is required, do not set the black body parameters, or the temperature may not correct.

Steps

Note

When measuring the black body, make sure the device's camera faces the black body, and there should be no other objects between the black body and the camera. Once the sample black body is calibrated, make sure the measurement area of the measuring black body should be the same as the calibrated one, or the temperature measurement may be failed.

1. On the Home page, tap **Temp (Temperature) → Black Body Settings** to enter the Black Body Settings page.

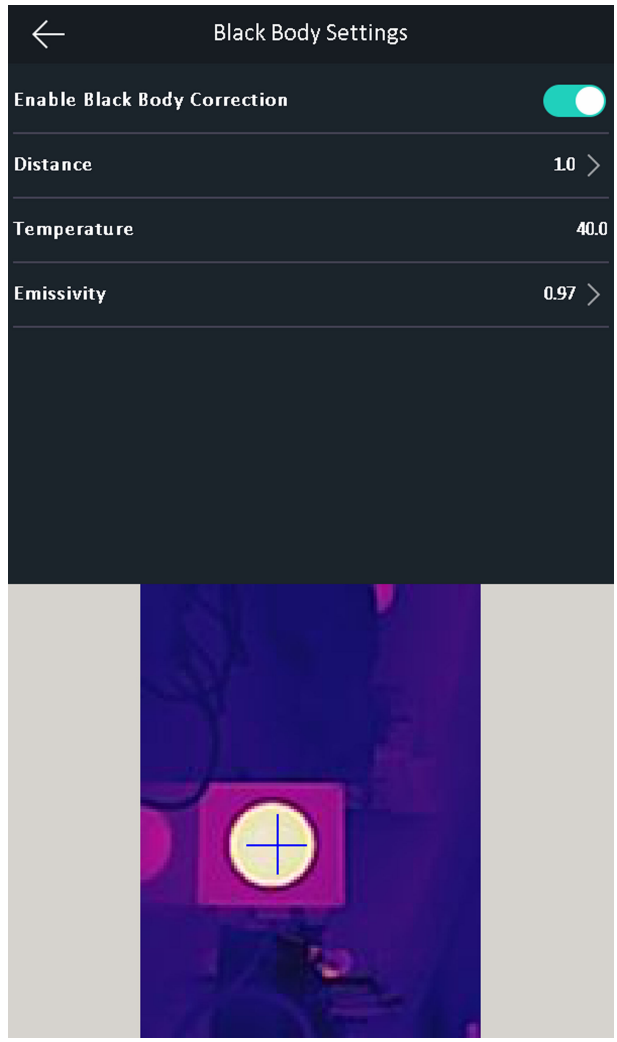


Figure 6-11 Black Body Settings Page

2. Enable black body correction function.
3. Put a black body in front of the camera. Make sure there are no other objects between the camera and the black body.
4. Set the distance between the black body and the camera (straight line), and the emissivity of the black body.

Note

The black body's temperature is fixed.

5. Tap the black body's position on the lower side of the page. When **+** is displayed on the black body on the screen, the black body is calibrated.

6.6 Import and Export Data

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

6.6.1 Export Data

Steps

1. Tap **Transfer** on the Home page to enter the Transfer page.
2. On the Transfer page, tap Export Event, Export User Data, Export Profile Photo, and export captured picture.
3. Tap **Yes** on the pop-up page and the data will be exported from the device to the USB flash drive.

Note

- The supported USB flash drive format is 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.

6.6.2 Import Data

Steps

1. Plug a USB flash drive in the device.
2. On the Transfer page, tap Import User Data, and Import Profile Photo.
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 supported USB flash drive format is FAT32.
- The imported pictures should be saved in the enroll_pic folder of the root directory and the picture's name should be follow the rule below:
  Card No._Name_Department_Employee ID_Gender.jpg

- 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.

6.7 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 with all face pictures stored in the device.

1: 1 Matching

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

6.7.1 Authenticate via Multiple Credential

Before You Start

Set the user authentication type before authentication. For details, see ***Set Authentication Mode*** .

Steps

1. If the authentication mode is Card and Face, Password and Face, Card and Password, authenticate any credential according to the instructions on the live view page.

   Note

   - The card can be normal IC card, or encrypted card.
   - If the QR Code Scanning function is enabled, you can put the QR code in front of the device camera to authenticate via QR code.

2. After the previous credential is authenticated, continue authenticate other credentials.

   Note

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

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

6.7.2 Authenticate via Single Credential

Set the user authentication type before authentication. For details, see ***Set Authentication Mode*** .

Authenticate face, card or QR code.

Face

Face forward at the camera and start authentication via face.

Card

Present the card on the card presenting area and start authentication via card.

Note

The card can be normal IC card, or encrypted card.

QR Code

Put the QR code in front of the device camera to authenticate via QR code.

Note

Authentication via QR code should be supported by the device.

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

6.8 System Settings

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

6.8.1 Set Basic Parameters

You can set the community No., building No., the unit No., voice prompt, voice volume, application mode, and white light brightness.

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

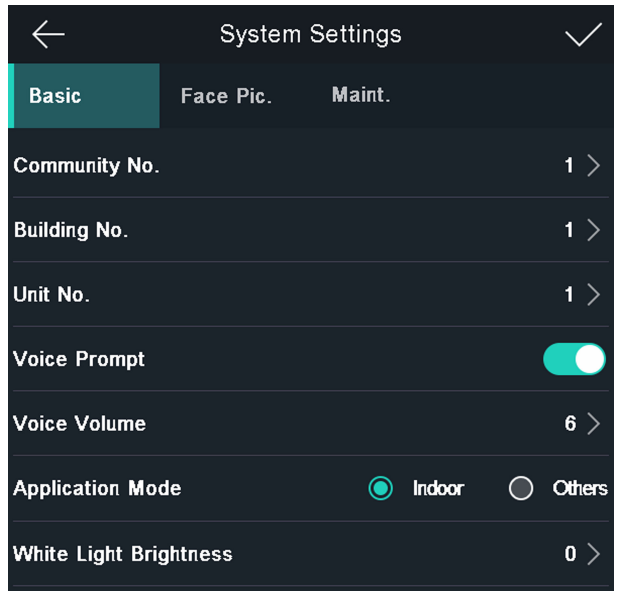


Figure 6-12 Basic Parameters

Table 6-2 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 or 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.
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

6.8.2 Set Face Picture Parameters

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

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

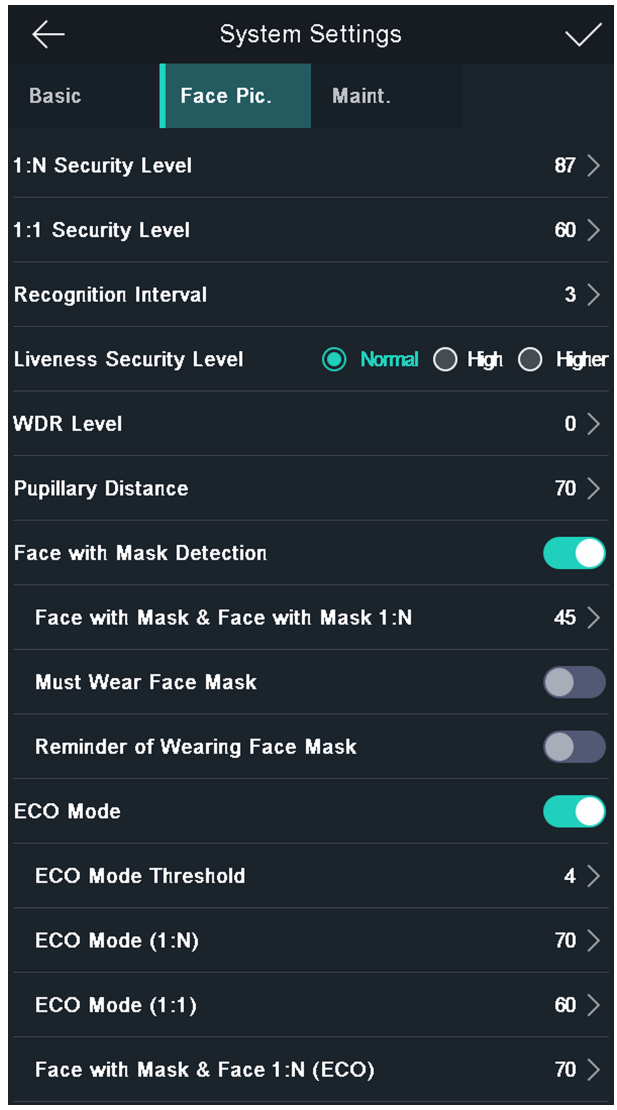


Figure 6-13 Face Picture Parameters

Table 6-3 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. By default, the value is 84.
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. By default, the value is 75.
Recognition Interval	Set the time interval between two continuous face recognitions when authenticating one person's permission.

Parameter	Description
	Note You can enter the number from 1 to 10.
Liveness Level (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.
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.
Face with Mask Detection	After the function is eanbled, when a person authenticates the permissions on the authentication page, the device can recognize the face whether wearing a mask or not, and prompts to wear a mask according to the configuration.
Face with Mask & Face with Mask (1:N)	Matching threshold for face with mask 1 : N. The larger the value, the smaller the false accept rate and the larger the false rejection rate. The Max. value is 100.
Must Wear Face Mask	After the function is enabled, the authenticated person must wear a face mask, otherwise the authentication will be failed.
Reminder of Wearing Face Mask	After the function is enabled, if the authenticating person does not wear a face mask, a prompt will be pop up to remind to wear a face mask.
ECO Mode	After enabling the ECO mode, the device will use the IR camera to authenticate faces in the low light or dark environment. And you can set he 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 8.
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. By default, the value is 84.

Parameter	Description
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. By default, the value is 75.
Face with Mask&Face (1:N) (ECO)	Matching threshold for face with mask 1: N in ECO mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate. The Max. value is 100.

6.8.3 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.

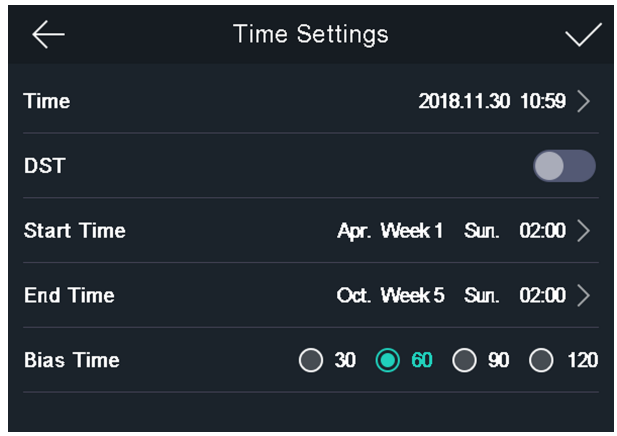


Figure 6-14 Time Parameters

6.9 Set Access Control Parameters

You can set the access control permissions, including the functions of terminal auth. mode, reader auth. mode, QR code, remote authentication, door contact, and door locked time, etc.

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

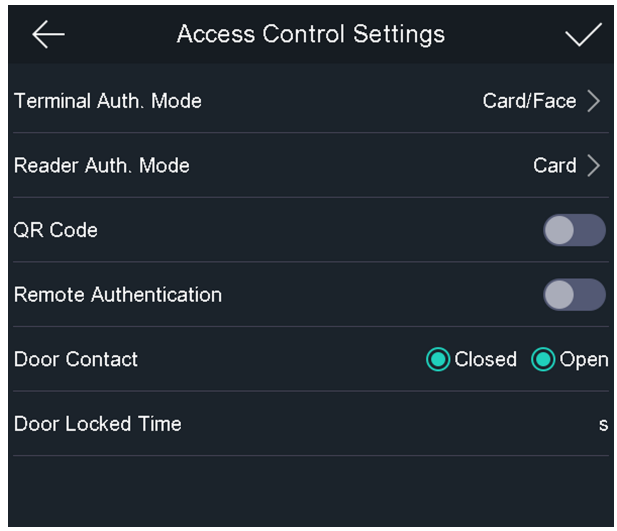


Figure 6-15 Access Control Parameters

The available parameters descriptions are as follows:

Table 6-4 Access Control Parameters Descriptions

Parameter	Description
Terminal Auth. Mode	Select the face recognition terminal's authentication mode. You can also customize the authentication mode. **Note** • Biometric recognition products are not 100% applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes. • If you adopt multiple authentication modes, you should authenticate other methods before authenticating face.
Reader Auth. Mode	Select the card reader's authentication mode.
QR code	You can use the QR code scanning function on the authentication interface. The device will upload the information associated with the obtained QR code to the platform.
Remote Authentication	When you authenticate the permission, the platform will control whether to grant the access or not remotely.
Door Contact	You can select **Open** or **Closed** according to your actual needs. By default, it is **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 255 s.

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.

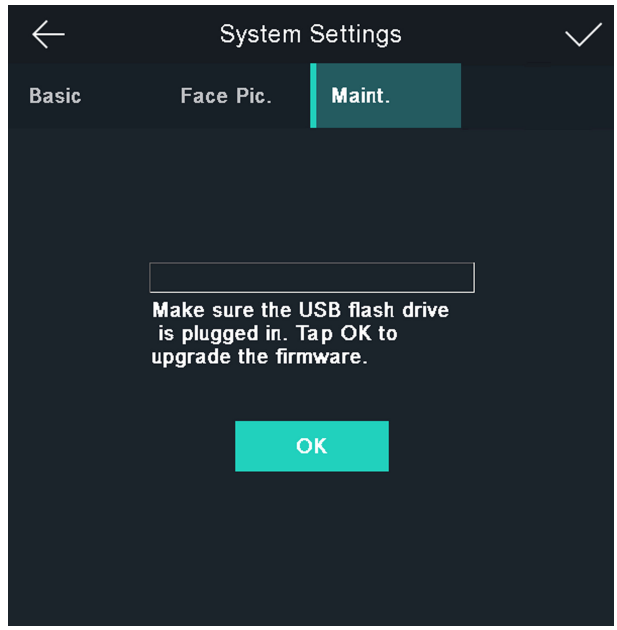


Figure 6-16 Upgrade

6.10.2 Data Management

On the Data Management page, you can delete user data, 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 6-5 Data Descriptions

Parameters	Description
Delete User Data	Delete all user data in the device.
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.

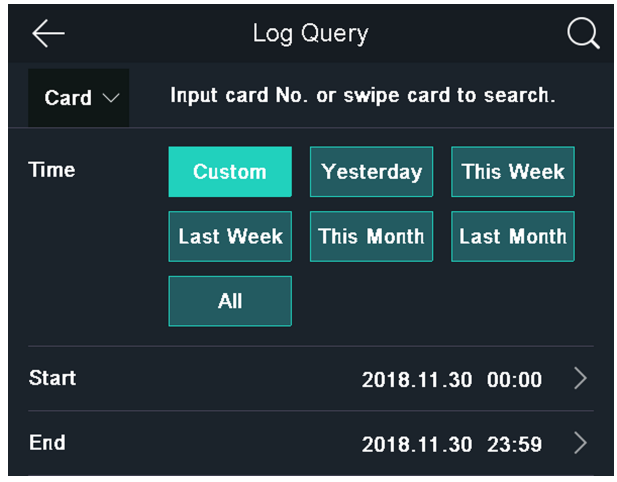


Figure 6-17 Log Query

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 Time and Attendance Status Settings

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

Note

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

6.11.1 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.

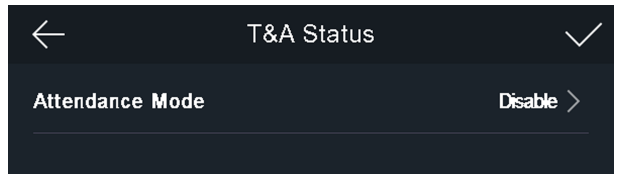


Figure 6-18 Disable Attendance Mode

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.

6.11.2 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**.

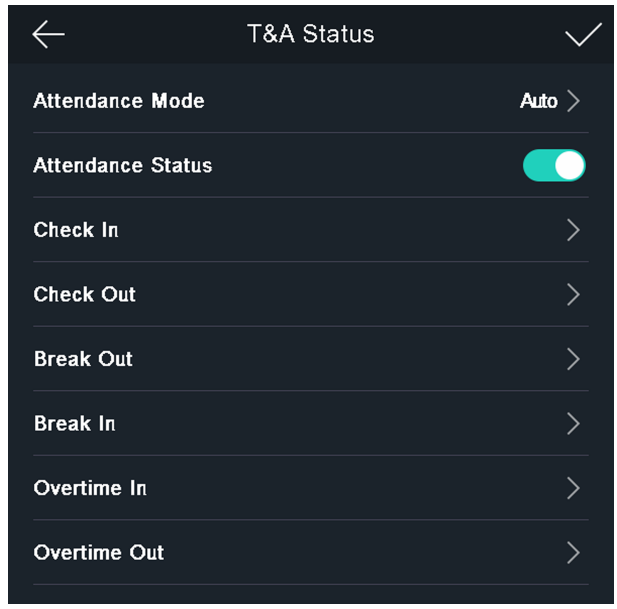


Figure 6-19 Auto Attendance Mode

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.

Note

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.

6.11.3 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**.

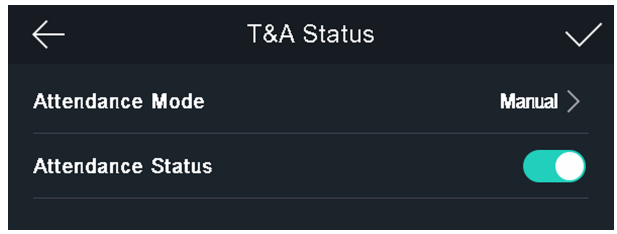


Figure 6-20 Manual Attendance Mode

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.

6.11.4 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**.

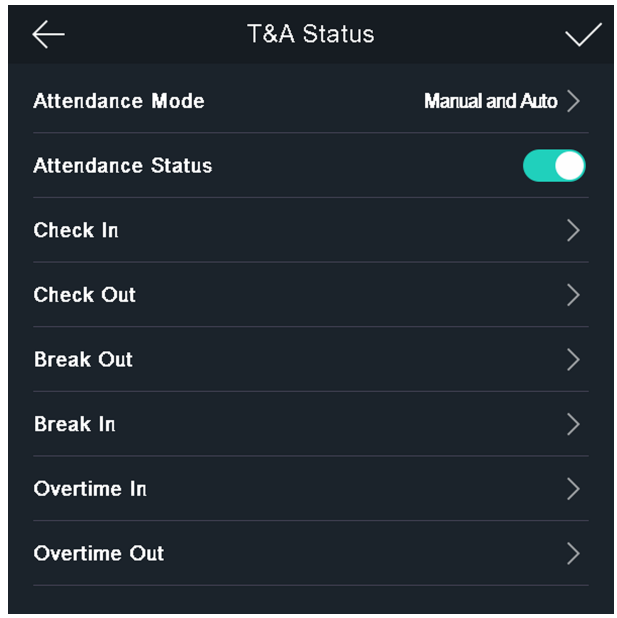


Figure 6-21 Manual and Auto Mode

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.

6.12 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 face with mask's number, the card's number, and the event's number.

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

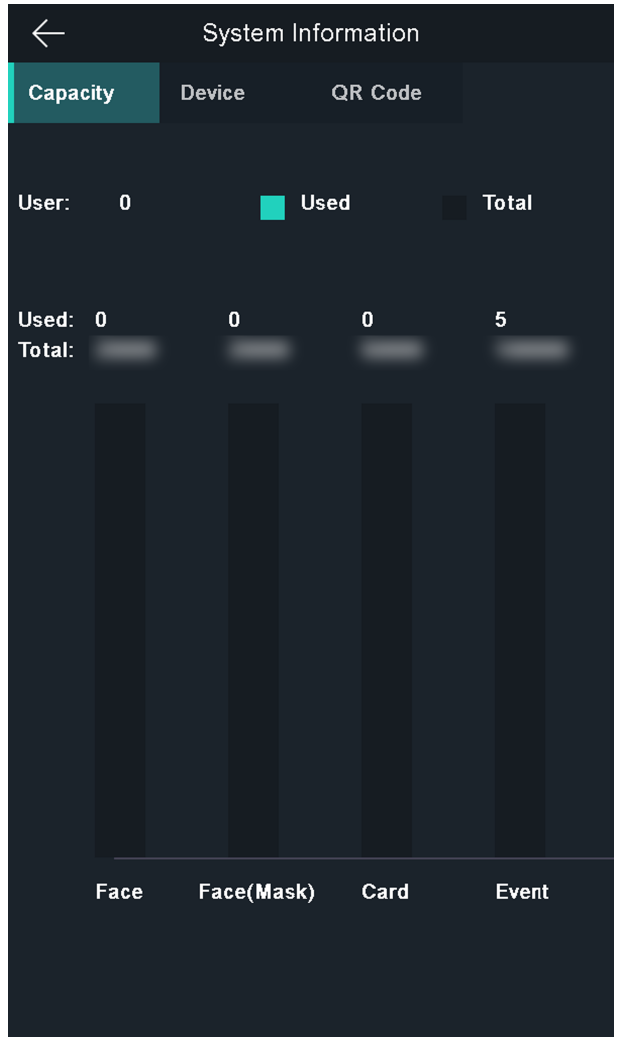


Figure 6-22 Capacity

View Device Information

You can view the device information.

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

Open Source License

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

View Device QR Code

You can add the device to the mobile client by scanning the device QR code.
Tap **Info. (System Information) → QR Code** to view the device QR code.

6.13 Video Intercom

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.

6.13.1 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.

6.13.2 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 .

6.13.3 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.

6.13.4 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.

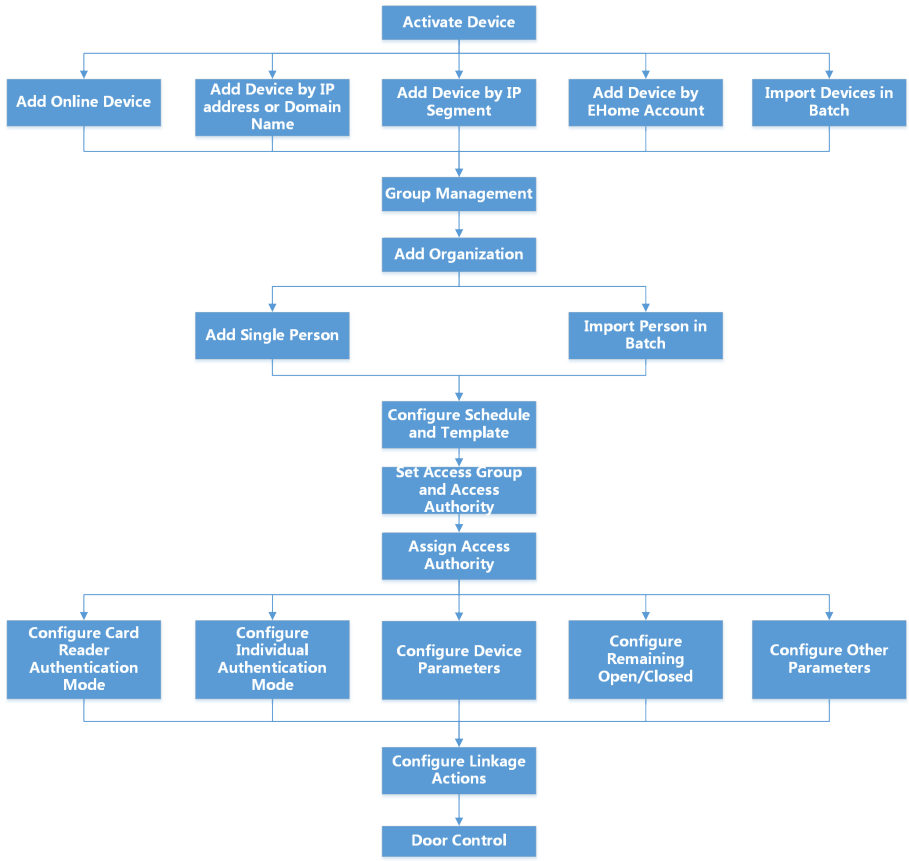


Figure 7-1 Flow Diagram of Configuration on Client Software

7.2 Device Management

The client supports managing access control devices and video intercom devices.

Example

You can control entrance & exit and manage attendance after adding access control devices to the client; you can perform video intercom with the indoor stations and door stations.

7.2.1 Add Device

The client provides three device adding modes including by IP/domain, IP segment, and ISUP protocol. The client also supports importing multiple devices in a batch when there are large amount of devices to be added.

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 Every 60s** to refresh the information of the online devices.

Add a Detected Online Device

You can select a detected online device displayed in the online device list and add it 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.

   Note

   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 change your password regularly, especially in the high security system, changing 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 **Transmission Encryption (TLS)** to enable transmission encryption using TLS (Transport Layer Security) protocol for security purpose.

Note

- This function should be supported by the device.
- If you have enabled Certificate Verification, you should click **Open Certificate Directory** to open the default folder, and copy the certificate file exported from the device to this default directory to strengthen the security. See for details about enabling certificate verification.
- You can log into the device to get the certificate file by web browser.

7. 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, and import all the channels of the device to this group.

   Example

   For access control device, its access points, alarm inputs/outputs, and encoding channels (if exist) will be imported to this group.
9. Click **Add**.

Add Multiple Detected Online Devices

For detected online devices sharing the same user name and password, you can add them 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 change your password regularly, especially in the high security system, changing 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, and import all the channels of the device to this group.

Example

For access control device, its access points, alarm inputs/outputs, and encoding channels (if exist) will be imported to this group.

9. Click **Add** to add the devices.

Add Device by IP Address or Domain Name

If 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, etc.

Steps

1. Enter Device Management module.
2. Click **Device** tab on the top of the right panel.

The added devices are displayed on the right panel.

3. Click **Add** to open the Add window, and then select **IP/Domain** as the adding mode.
4. Enter the required information.

   Name

   Create a descriptive name for the device. For example, you can use a nickname 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 share the same port number. 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 change your password regularly, especially in the high security system, changing 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.

5. **Optional:** Check **Transmission Encryption (TLS)** to enable transmission encryption using TLS (Transport Layer Security) protocol for security purpose.

   Note

   - This function should be supported by the device.
   - If you have enabled Certificate Verification, you should click **Open Certificate Directory** to open the default folder, and copy the certificate file exported from the device to this default directory to strengthen the security. See for details about enabling certificate verification.
   - You can log into the device to get the certificate file by web browser.

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, and import all the channels of the device to this group.

Example

For access control device, its access points, alarm inputs/outputs, and encoding channels (if exist) will be imported to this group.

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.

Add Devices by IP Segment

If the devices share the same port No., user name and password, and their IP addresses ranges in the same IP segment, you can add them to the client by specifying the start IP address and the end IP address, port No., user name, password, etc of the devices.

Steps

1. Enter the Device Management module.
2. Click **Device** tab on the top of the right panel.

   The added devices are displayed on the right panel.
3. Click **Add** to open the Add window.
4. Select **IP Segment** as the adding mode.
5. 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 change your password regularly, especially in the high security system, changing 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 **Transmission Encryption (TLS)** to enable transmission encryption using TLS (Transport Layer Security) protocol for security purpose .

Note

- This function should be supported by the device.
- If you have enabled Certificate Verification, you should click **Open Certificate Folder** to open the default folder, and copy the certificate file exported from the device to this default directory to strengthen the security. See for details about enabling certificate verification.
- You can log into the device to get the certificate file by web browser.

7. 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, and import all the channels of the device to the group.
9. 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.

Add Device by ISUP Account

For access control devices supports ISUP 5.0 protocol, you can add them to the client by ISUP protocol after entering device ID and key, if you have configured their server addresses, port No., and device IDs.

Before You Start

Make sure the devices have connected to the network properly.

Steps

1. Enter Device Management module.

   The added devices are displayed on the right panel.
2. Click **Add** to open the Add window.
3. Select **ISUP** as the adding mode.
4. Enter the required information.

   Device Account

   Enter the account name registered on ISUP protocol.

   ISUP Key

   For ISUP 5.0 devices, enter the ISUP key if you have set it when configuring network center parameter for the device.

Note

This function should be supported by the device.

5. **Optional:** Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.
6. **Optional:** Check **Import to Group** to create a group by the device name, and import all the channels of the device to the group.
7. Finish adding the device.
   - Click **Add** to add the device and go back to the device list.
   - Click **Add and New** to save the settings and continue to add other device.

Note

Face pictures cannot be applied to devices added by ISUP account except DS-K1T671 series and DS-K1T331 series.

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

Device Status	Click on Operation column to view device status.
Edit Device Information	Click on Operation column to edit the device information, such as device name, device account, and ISUP key.
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.

Import Devices in a Batch

You can add multiple devices to the client in a batch by entering the device parameters in a pre-defined CSV file.

Steps

1. Enter the Device Management module.
2. Click **Device** tab on the top of the right panel.
3. Click **Add** to open the Add window, and then 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.

Note

For detailed description of the required fields, refer to the introductions in the template.

Adding Mode

Enter ***0*** or ***1*** or ***2***.

Address

Edit the address of the device.

Port

Enter the device port number. The default port number 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 change your password regularly, especially in the high security system, changing 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

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. Enter ***0*** to disable 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 via the client.

Steps

1. Enter Device Management page.
2. Click **Online Device** to show the online device area.

   All the online devices sharing the same subnet will be displayed in the list.
3. Select the device from the list and click on the Operation column.
4. Reset the device password.

- Click **Generate** to pop up the QR Code window and click **Download** to save the QR code to your PC. You can also take a photo of the QR code to save it to your phone. Send the picture 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 change your password regularly, especially in the high security system, changing 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 16 doors, 64 alarm inputs, and 16 alarm outputs. You can organize these resources into one group (named 1st Floor) for convenient management. You can control door status, 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, access points, 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, access points, 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. Select a group from the group list and select the resource type as **Access Point**, **Alarm Input**, **Alarm Output**, etc.
4. Click **Import**.
5. 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.
6. 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 access point, you can edit the access point name. For alarm input, you can edit the alarm input name. Here we take access point 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 **Access Point**.

   The access points imported to the group will display.
4. Click in the Operation column to open the Edit Resource window.
5. Edit the resource name.
6. 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 surbodinate organization for the added one.

Steps

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

   Note

   Up to 10 levels of organizations can be added.

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

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

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, gender, phone number, etc.

Steps

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

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

   Example

   For example, if the person is a visitor, his/her effective period may be short and temporary.
6. Confirm to add the person.
   - Click **Add** to add the person and close the Add Person window.
   - Click **Add and New** to add the person and continue to add other persons.

7.4.3 Issue a Card by Local Mode

If a card enrollment station is available, you can issue a card by local mode. To read the card number, you should connect the card enrollment station to the PC running the client by USB interface or COM, and place the card on the card enrollment station.

Steps

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

   Note

   Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .
3. In the **Credential → Card** area, click **+**.
4. Click **Settings** to enter the Settings page.
5. Select **Local** as the card issuing mode.

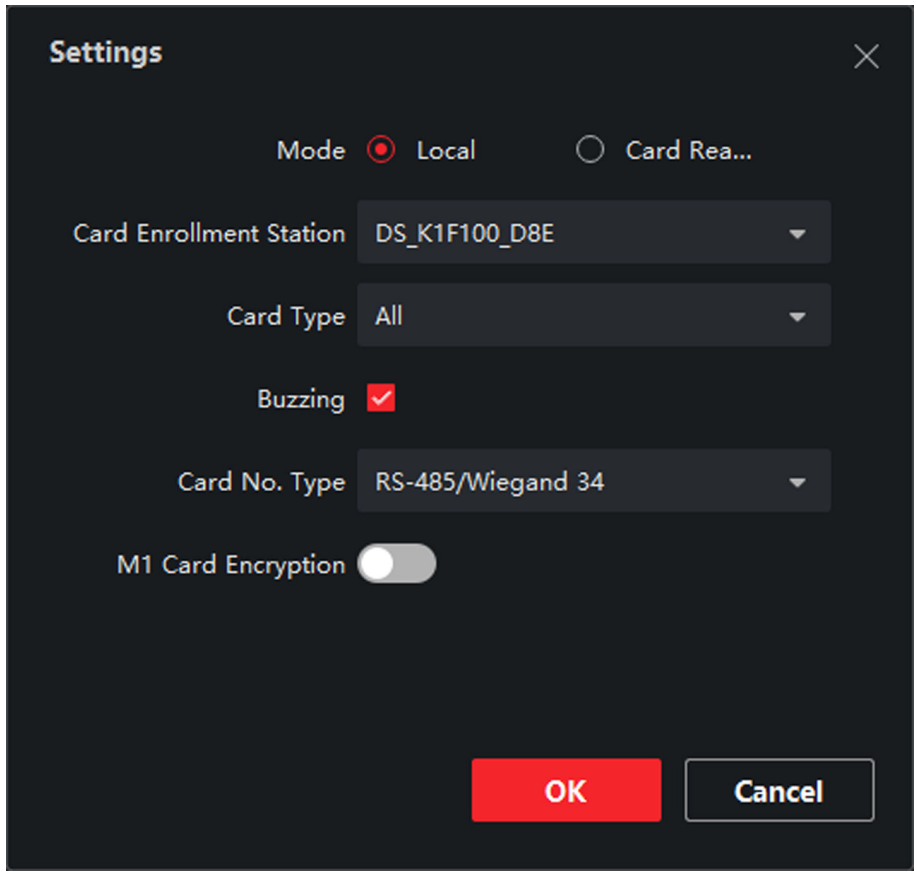


Figure 7-2 Issue a Card by Local Mode

6. Set other related parameters.

Card Enrollment Station

Select the model of the connected card enrollment station.

Note

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

Card Type

This field is only available when the model is DS-K1F100-D8E or DS-K1F180-D8E. Select the card type as EM card or Mifare card according to the actual card type.

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, then you can enable the M1 Card Encryption function and select the sector of the card to encrypt.

7. Click **OK** to confirm the operation.
8. Place the card on the card enrollment station, and click **Read** to get the card number.

   The card number will display in the Card No. field automatically.
9. Click **Add**.

   The card will be issued to the person.

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 a person, you can take a photo of the her/him via the client and set this photo as the person's profile.

Before You Start

Make sure PC running the client has a camera or you have connected other USB camera to the PC.

Steps

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

Note

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

3. Click **Add Face** in the Basic Information area.
4. Select **Take Photo** to enter Take Photo window.
5. **Optional:** Enable **Verify by Device** to check whether the captured face photo can meet the uploading requirements.
6. Take a photo.
   1) Face to the camera 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.

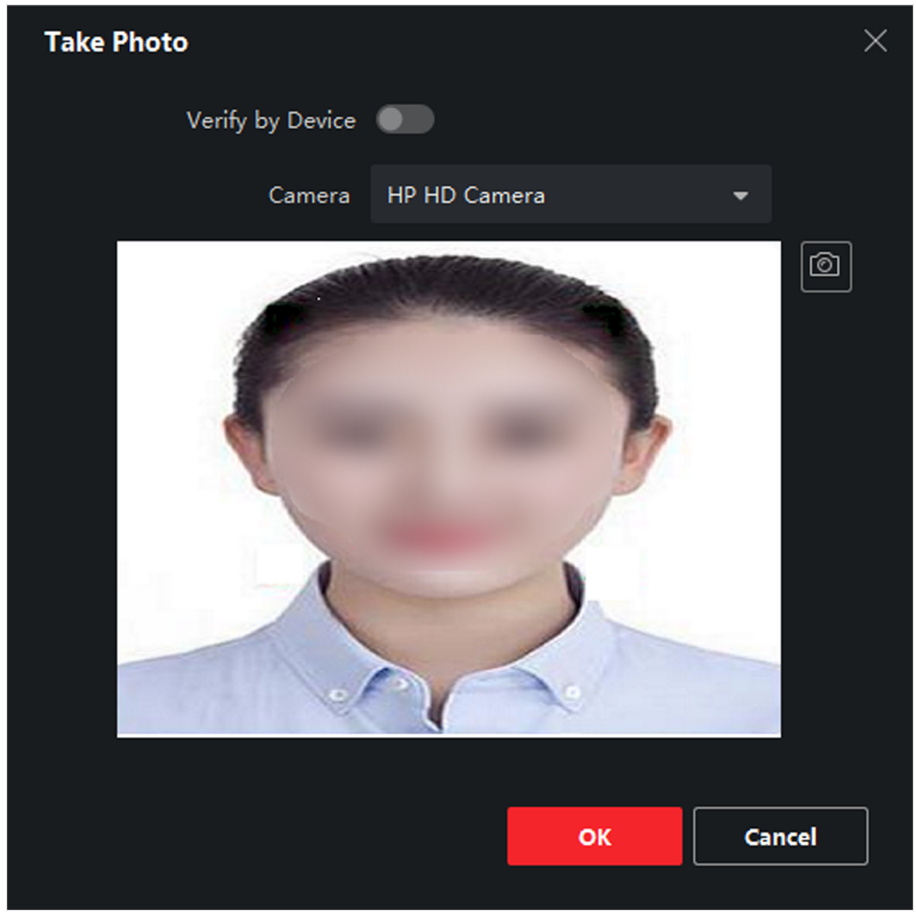


Figure 7-3 Take a Photo via Client

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.

7.4.6 Collect Face via Access Control Device

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

Steps

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

   Note

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

3. Click **Add Face** in the Basic Information panel.
4. Select **Remote Collection**.
5. Select an added access control device or the enrollment station from the drop-down list.

   Note

   If you select the enrollment station, you should click **Login** to set related parameters of the device including IP address, port No., user name, and password. Also, you can check **Face Anti-Spoofing** and select the liveness level as Low, Medium, or High.

   Face Anti-Spoofing

   If you check this function, then the device can detect whether the face to be collected is an authentic one.

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 Configure Access Control Information

When adding a person, you can set her/his access control information, such as binding an access control group with the person, configuring PIN code, setting the person as a visitor, a blocklist person, or a super user, etc.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.
3. In the **Access Control** area, click to select access group(s) for the person.

Note

For details, refer to ***Set Access Group to Assign Access Authorization to Persons*** .

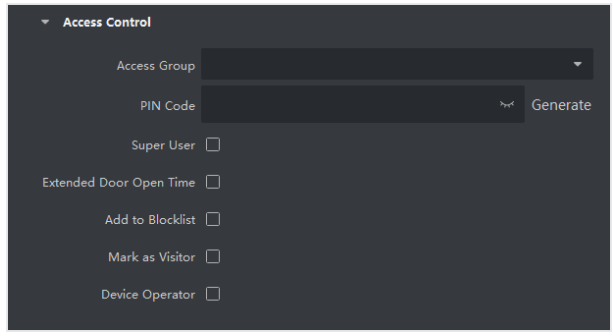


Figure 7-4 Configure Access Control Information

4. Set a unique PIN code for the person which can be used for access authentication.
   - Manually enter a PIN code containing 4 to 8 digits.

     Note

     Persons' PIN codes cannot be repeated.
   - Click **Generate** to randomly generate an unrepeated PIN code of 6 digits.

     Note

     If there are repeated PIN codes, a prompt will pop up on the client. The admin can generate a new PIN code to replace the repeated PIN code and notify related persons.
5. Check the person's operation permissions.

   Super User

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

   Extended Door Open Time

   Use this function for persons with reduced mobility. When accessing the door, the person will have more time than others to pass through doors.

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

   Add to Blocklist

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

   Mark as Visitor

If the person is a visitor, you should set the her/his valid times for visit.

Note

The valid times for visit is between 1 and 100. You can also check **No Limit**, then there are no limited times for the visitor to access doors/floors.

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.

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.

7.4.8 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.

7.4.9 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.

7.4.10 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 .

7.4.11 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.

7.4.12 Import Person Information

You can enter the information of multiple persons in a predefined template (CSV/Excel 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/Excel file with person information from local PC.
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 2,000 persons.

7.4.13 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.

7.4.14 Export Person Information

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

Before You Start

Make sure you have added persons to an organization.

Steps

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

Note

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

3. Click **Export** to open the Export panel.
4. Check **Person Information** as the content to export.
5. Check desired items to export.
6. Click **Export** to save the exported file in CSV/Excel file on your PC.

7.4.15 Export Person Pictures

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

Before You Start

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

Steps

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

Note

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

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

Note

- The exported file is in ZIP format.
- The exported face picture is named as "Person ID_Name_0" ("0" is for a full-frontal face).

7.4.16 Get Person Information from Access Control Device

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

Steps

Note

- If the person name stored in the device is empty, the person name will be filled with the issued card No. after importing to the client.
- The gender of the persons will be **Male** by default.
- If the card number or person ID (employee ID) stored on the device already exists in the client database, the person with this card number or person ID will not be imported to the client.

1. Enter **Person** module.
2. Select an organization to import the persons.
3. Click **Get from Device**.
4. Select an added access control device or the enrollment station from the drop-down list.

Note

If you select the enrollment station, you should click **Login**, and set IP address, port No., user name and password of the device.

5. Click **Import** to start importing the person information to the client.

Note

Up to 2,000 persons and 5,000 cards can be imported.

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

7.4.17 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**.

7.4.18 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 be displayed in the right panel.
3. **Optional:** Enter key words (name or person ID) in the input box to filter the person(s) that need issuing cards.
4. **Optional:** Click **Settings** to set the card issuing parameters. For details, refer to .
5. Click **Initialize** to initialize the card enrollment station or card reader to make it ready for issuing cards.
6. Click the **Card No.** column and enter the card number.
   - Place the card on the card enrollment station.
   - Swipe the card on the card reader.
   - Manually enter the card number and press the **Enter** key.

   The person(s) in the list will be issued with card(s).

7.4.19 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.

7.4.20 Set Card Issuing Parameters

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

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

Local Mode: Issue Card by Card Enrollment Station

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

Card Enrollment Station

Select the model of the connected card enrollment station

Note

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

Card Type

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

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

Serial Port

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

Select the COM the card enrollment station connects to.

Buzzing

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

Card No. Type

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

M1 Card Encryption

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

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

Remote Mode: Issue Card by Card Reader

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

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.

Note

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

Note

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.

   Note

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

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

Note

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

3) **Optional:** Perform the following operations to edit the time durations.
   - Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to .
   - Click the time duration and directly edit the start/end time in the appeared dialog.
   - Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to .
4) **Optional:** Select the time duration(s) that need to be deleted, and then click in the Operation column to delete the selected time duration(s).
5) **Optional:** Click in the Operation column to clear all the time duration(s) in the time bar.
6) **Optional:** Click in the Operation column to delete this added holiday period from the holiday list.

6. Click **Save**.

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

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, face picture, linkage between card number and linkage between card number and card password, card effective period, etc).

1. Click **Access Control → Authorization → 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) to assign access authority.
6. In the left list of the Select Access Point field, select door(s), door station(s) or floor(s) for the selected persons to access.
7. Click **Save**.

   You can view the selected person(s) and the selected access point(s) on the right side of the interface.

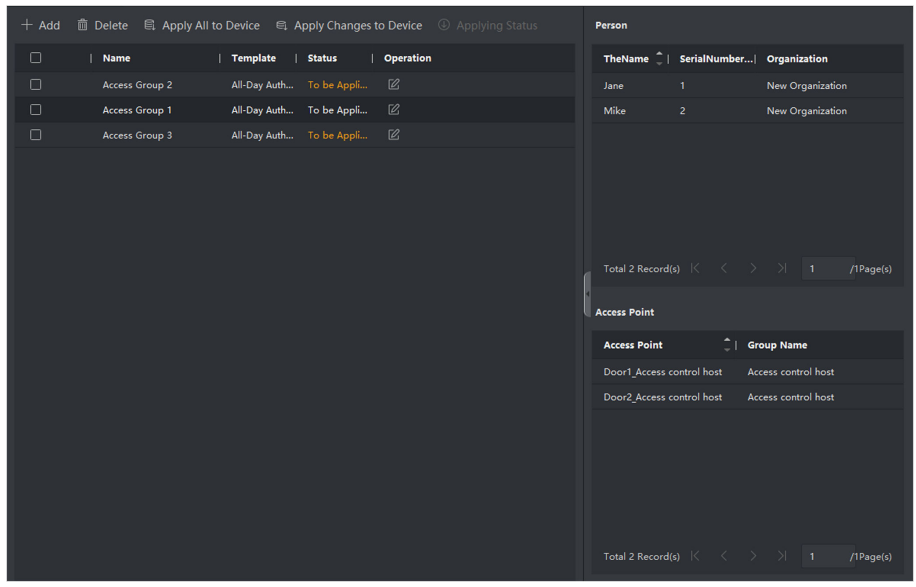


Figure 7-5 Display the Selected Person(s) and Access Point(s)

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.
   2) Click **Apply All to Devices** start applying all the selected access group(s) to the access control device or door station.
   3) Click **Apply All to Devices** or **Apply Changes to Devices**.

      Apply All to Devices

      This operation will clear all the existed access groups of the selected devices and then apply the new access group to the device.

      Apply Changes to Devices

      This operation will not clear the existed access groups of the selected devices and only apply the changed part of the selected access group(s) to the device(s).
   4) View the applying status in the Status column or click **Applying Status** to view all the applied access group(s).

Note

You can check **Display Failure Only** to filter the applying results.

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).

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

Note

If you change the persons' access information or other related information, you will view the prompt**Access Group to Be Applied** on the right corner of the client.
You can click the prompt to apply the changed data to the device. You can select either **Apply Now** or **Apply Later**.

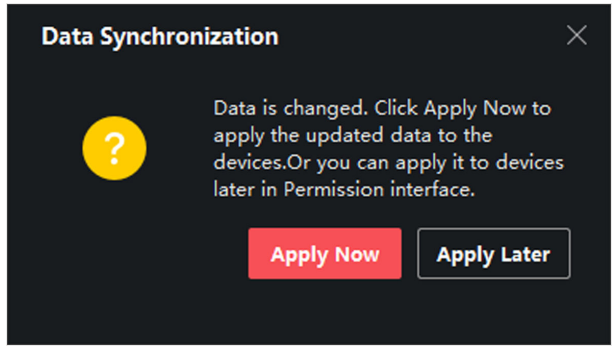


Figure 7-7 Data Synchronization

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, including overlaying user information on picture, uploading pictures after capturing, saving captured pictures, etc.

Steps

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

Note

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

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

Note

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

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.

Deep Mode

The device can recognize a much wider people range than the normal mode. This mode is applicable to a more complicated environment.

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

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

Enable ID Card

Reserved. 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

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

Steps

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

Note

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

Name

Edit the card reader name as desired.

Door Contact

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

Exit Button Type

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

Door Locked Time

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

Extended Open Duration

The door contact can be enabled with appropriate delay after person with extended accesss 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.

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.

Note

- The duress code and super password should be different.
- The duress code and super password should be different from the authentication password.
- The length of duress code and super password 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 to copy the parameters in the page to the selected doors.

Note

The door or floor's status duration settings will be copied to the selected door 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 **Advanced** to edit the parameters.

Basic Information

Name

Edit the card reader name as desired.

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.

Alarm of Max. Failed Attempts

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

Card Reader Type/Card Reader Description

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

Advanced

Enable Card Reader

Enable the function and e device can be used as an card reader.

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.

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.

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.

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. By default, it is 2s.

Face Anti-spoofing

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.

Liveness Detection Security Level

After enabling Live Face Detection function, you can set the matching security level when performing live face authentication.

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.

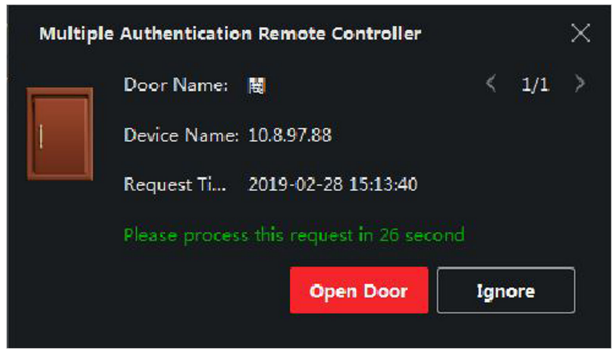


Figure 7-8 Remotely Open Door

      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**.

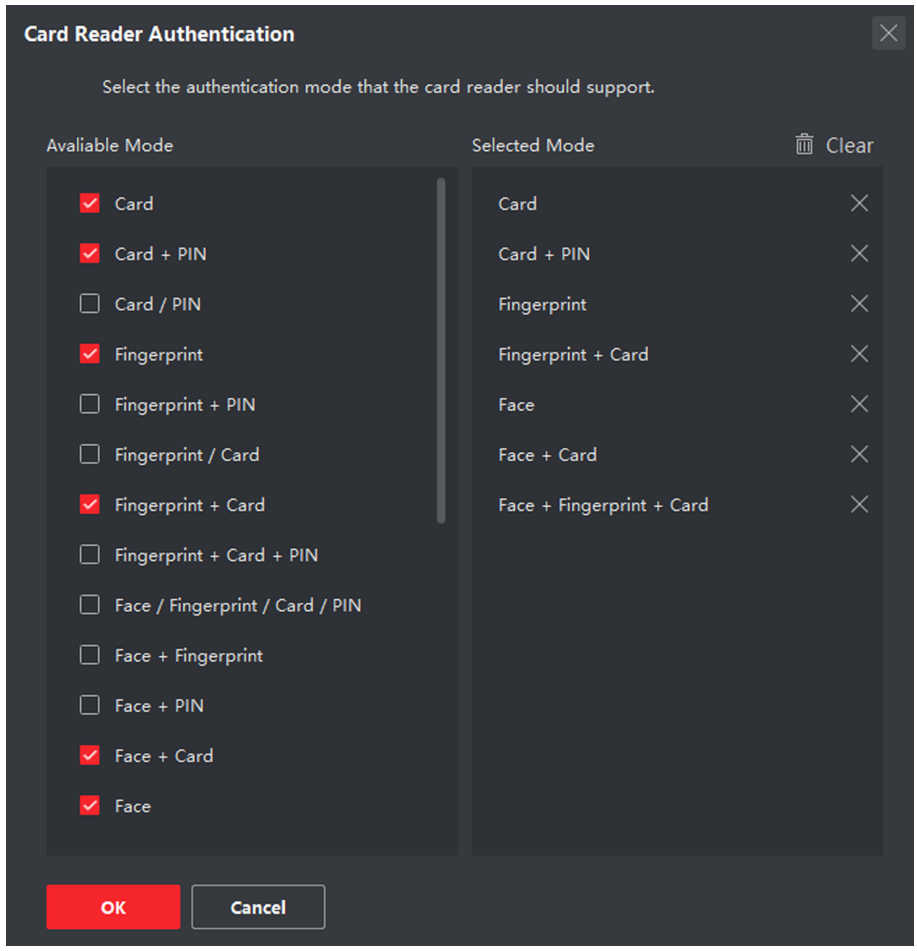


Figure 7-9 Select Card Reader Authentication Mode

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.

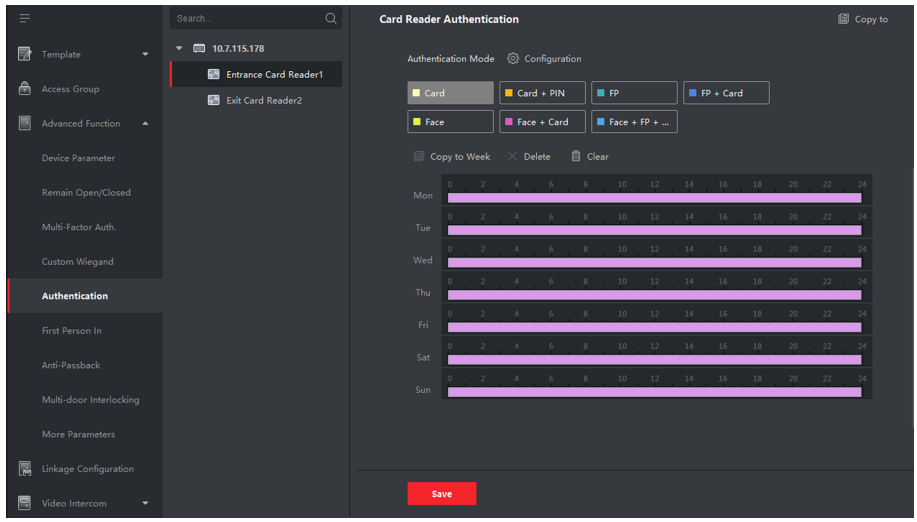


Figure 7-10 Set Authentication Modes for Card Readers

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

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

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

Steps

1. Click **Access Control → Advanced Function → First Person In** to enter the First Person In page.
2. Select an access control device in the list on the left panel.
3. Select the current mode as **Enable Remaining Open after First Person** or **Disable Remaining Open after 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.

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 Device Parameters

After adding the access control device, you can set its parameters such as network parameters.

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 ISUP account via wired network.

Set Log Uploading Mode

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

Steps

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

   Note

   The main channel and the backup channel cannot enable N1 or G1 at the same time.
7. Click **Save**.

Create ISUP Account in Wired Communication Mode

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

Steps

Note

This function should be supported by the device.

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

   Note

   The port number of the wireless network and wired network should be consistent with the port number of ISUP.
8. Select the **Protocol Type** as **ISUP**.
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, 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.

   Algorithm

   Select **Deep Learning** as the face picture database.

   Save Authenticating Face Picture

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

   ECO Mode

   After enabling the ECO mode, the device can authenticate faces in the low light or dark environment. And you can set he ECO mode threshold, ECO mode (1:N), and ECO mode (1:1).

   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.

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 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 8.

Work Mode

Set the device work mode as Access Control Mode. The access control mode is the device normal mode. You should authenticate your credential for accessing.

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 Verification** to enter the M1 Card Encryption Verification page.
4. Set the switch to on to enable the M1 card encryption function.
5. Set the sector ID.

Note

- The sector ID ranges from 1 to 100.
- By default, Sector 13 is encrypted. It is recommended to encrypt sector 13.

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.

Before You Start

Add access control device to the client, and make sure the device supports RS-485 interface.

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 **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.

   Note

   When the connection mode is **Connect Access Control Device**, you can select **Card No.** or **Person ID** as the output type.

6. Click **Save**.
   - The configured parameters will be applied to the device automatically.
   - When you change the working mode or connection mode, the device will reboot automatically.

Set Wiegand Parameters

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

Steps

Note

This function should be supported by the device.

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

   Note

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

6. 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

Note

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

1. Click **Event Management → Access Control Event** .

   The added access control devices will display in the device list.
2. Select a resource (including device, alarm input, door/elevator, and card reader) from the device list.

   The event types which the selected resource supports will display.
3. Select the event(s) and click **Edit Priority** to define the priority for the event(s), which can be used to filter events in the Event Center.
4. Set the linkage actions of the event.
   1) Select the event(s) and click **Edit Linkage** to set the client actions when the events triggered.

      Audible Warning

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

      Note

      For setting the alarm sound, please refer to *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, en 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. When the event is triggered, it can trigger the alarm output, host buzzer, and other actions on the same device.

Steps

Note

It should be supported by the device.

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

Buzzer on Controller

The audible warning of access control device will be triggered.

Capture

The real-time capture will be triggered.

Access Point

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

Note

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

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

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

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

7.8.3 Configure Device Actions for Card Swiping

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

Steps

Note

It should be supported by the device.

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

   Buzzer on Controller

   The audible warning of access control device will be triggered.

   Capture

   The real-time capture will be triggered.

   Access Point

   The door status of open, close, remain open, or remain closed will be triggered.
8. Click **Save**.

   When the card (configured in Step 5) swipes on the card reader (configured in Step 6), it can trigger the linked actions (configured in step 7).
9. **Optional:** After adding the device linkage, you can do one or more of the following:

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

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 buzzer on card reader, and other actions.

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 **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.

   Note

   The device should support recording.

   Access Point

   The door status of open, close, remain open, or remain closed will be triggered.
8. Click **Save**.
9. **Optional:** After adding the device linkage, you can do one or more of the followings:

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

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.

Note

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.

   Note

   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, 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

The event information (for example, device offline) received by the client displays. In the Event Center, you can check the detailed information of the real-time and historical events, view the event linked video, handle the events, and so on.

Before the client can receive the event information from the device, you need to enable the events of the resource and arm the device first. For details, refer to and ***Enable Receiving Event from Devices*** .

7.10.1 Enable Receiving Event 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.

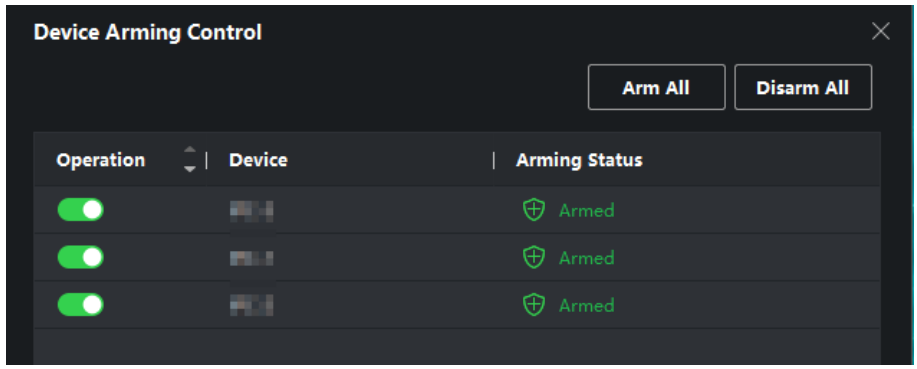


Figure 7-11 Arm Device

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

The real-time event information received by the client of the connected resources are displayed. You can check the real-time event information, including event source, event time, priority, etc.

Before You Start

Enable receiving events from devices before the client can receive event from the device, see ***Enable Receiving Event 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 encoding device, event time is the client time when it receives the event. For other device types, event time is the time when the event is triggered.

Priority

Priority represents the emergency 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 detail description and handing records of the event.
5. **Optional:** Perform the following operations if necessary.

Handle Single Event	Click **Handle** to enter the processing suggestion, and then click **Commit**. **Note** 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. **Note** 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 from Devices*** for details.

Steps

1. Click **Event Center → Event Search** to enter the event search page.
2. Set the filter conditions to display the required events only.

   Time

   The time when the event starts.

   Search by

   Device

   Search the events by device or the device's resource channels. If searched by device, you need to set the followings:

   - **Include Sub-Node**: Search the events of the device and all resource channels.
   - **Device Type**: Select the device from which you want to search events.

   Group

   Search the events by resource channels in the group.

   Note

   - For video intercom device, you need to select search scope: All and Locking Log.
   - For access control device, you can click **Show More** to set more conditions: status, event type, card reader type, person name, card No., and organization.

   Priority

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

   Status

   The handling status of the event.
3. Click **Search** to search the events according the conditions you set.

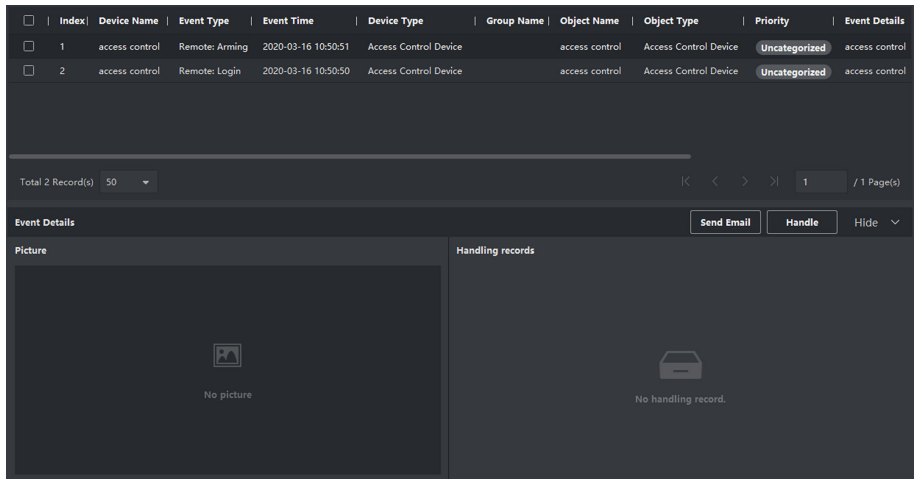


Figure 7-12 Search Historical Events

4. **Optional:** Right click the table header of the event list to customize the event related items to be displayed in the event list.
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.

Note

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

Export Event Information

Click **Export** to export the event log or event pictures to the local PC in CSV/Excel file. You can set the saving path manually.

Download Event Related Picture	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.

Note

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

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.

Set Weekend

The days of weekends may vary in different countries and regions. The client provides weekends definition function. You can select one or more days as the weekends according to actual requirements, and set different attendance rules for weekends from workdays.

Steps

Note

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

1. Enter Time & Attendance module.
2. Click **Attendance Settings → General Rule** .
3. Select the day(s) as weekend, such as Saturday and Sunday.
4. 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. Click **Time & Attendance → Attendance Settings → Overtime** .
2. Set required information.

   Overtime Level for Workday

   When you work for a 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

   Work Hour Rate is used to calculate work hours by multiplying it by overtime. When you work for a certain period after end-work time on workday, you will reach different overtime level. You can set different work hour rates (1-10, can be a decimal) for three overtime levels. For example, your valid overtime is one hour (in overtime level 1), and the work hour rate of overtime level 1 is set as 2, then the work hours in the period will be calculated as 2 hours.

   Overtime Rule for Weekend

   You can enable overtime rule for weekend and set calculation mode.
3. 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

Note

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

1. Enter the Time & Attendance module.
2. Click **Attendance Settings → Attendance Check Point** to enter the Attendance Check Point Settings page.
3. **Optional:** Set **Set All Card Readers as Check Points** switch to off.

   Only the card readers in the list will be set as the attendance check points.
4. Check the desired card reader(s) in the device list as attendance check point(s).
5. Set check point function as **Start/End-Work**, **Start-Work** or **End-Work**.
6. Click **Set as Check Point**.

   The configured attendance check point displays on the right list.

Configure Holiday

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

Add Regular Holiday

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

Steps

1. Enter the Time & Attendance module.
2. Click **Attendance Settings → Holiday** to enter the Holiday Settings page.
3. Check **Regular Holiday** as holiday type.
4. Custom a name for the holiday.
5. Set the first day of the holiday.
6. Enter the number of the holiday days.
7. Set the attendance status if the employee works on holiday.
8. **Optional:** Check **Repeat Annually** to make this holiday setting effective every year.
9. Click **OK**.

   The added holiday will display in the holiday list and calendar.

   If the date is selected as different holidays, it will be recorded as the first-added holiday.
10. **Optional:** After adding the holiday, perform one of the following operations.

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

Add Irregular Holiday

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

Steps

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

Example

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

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

    The added holiday will display in the holiday list and calendar.

    If the date is selected as different holidays, it will be recorded as the first-added holiday.
11. **Optional:** After adding the holiday, perform one of the following operations.

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

Configure Leave Type

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

Steps

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

Edit	Move the cursor over the major leave type and click to edit the major leave type.
Delete	Select one major leave type and click **Delete** on the left to delete the major leave type.

5. Click **Add** on the right to add a minor leave type.
6. **Optional:** Perform one of the following operations for minor leave type.

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

Synchronize Authentication Record to Third-Party Database

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

Steps

1. Enter Time & Attendance module.
2. Click **Attendance Settings → Third-Party Database** .
3. Set **Apply to Database** switch to on to enable synchronization function.
4. Select database Type as **SQLServer** or **MySql**.

   Note

   If you select **MySql**, you should import the configuration file (libmysql.dll) from local PC.

5. Set the other required parameters of the third-party database, including server IP address, database name, user name and password.
6. Set table parameters of database according to the actual configuration.
   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.
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.
   - During synchronization, if the client disconnects with the third-party database, the client will start reconnection every 30 mins. After being reconnected, the client will synchronize the data recorded during the disconnected time period 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 **Break Time** to enter Break Time page.
4. Click **Break Time Settings**.
5. Add break time.
   1) Click **Add**.
   2) Enter a name for the break time.
   3) Set related parameters for the break time.

      Start Time / End Time

Set the time when the break starts and ends.

No Earlier Than / No Later Than

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

Break Duration

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

Calculation

Auto Deduct

The fixed break duration will be excluded from work hours.

Must Check

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

Note

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

6. Click **Save** to save the settings.
7. **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 General Timetable

On the timetable page, you can add general timetable for employees, which requires the fixed start-work time and end-work time. Also, you can set valid check-in/out time, allowable timetable for being late and leaving early.

Steps

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

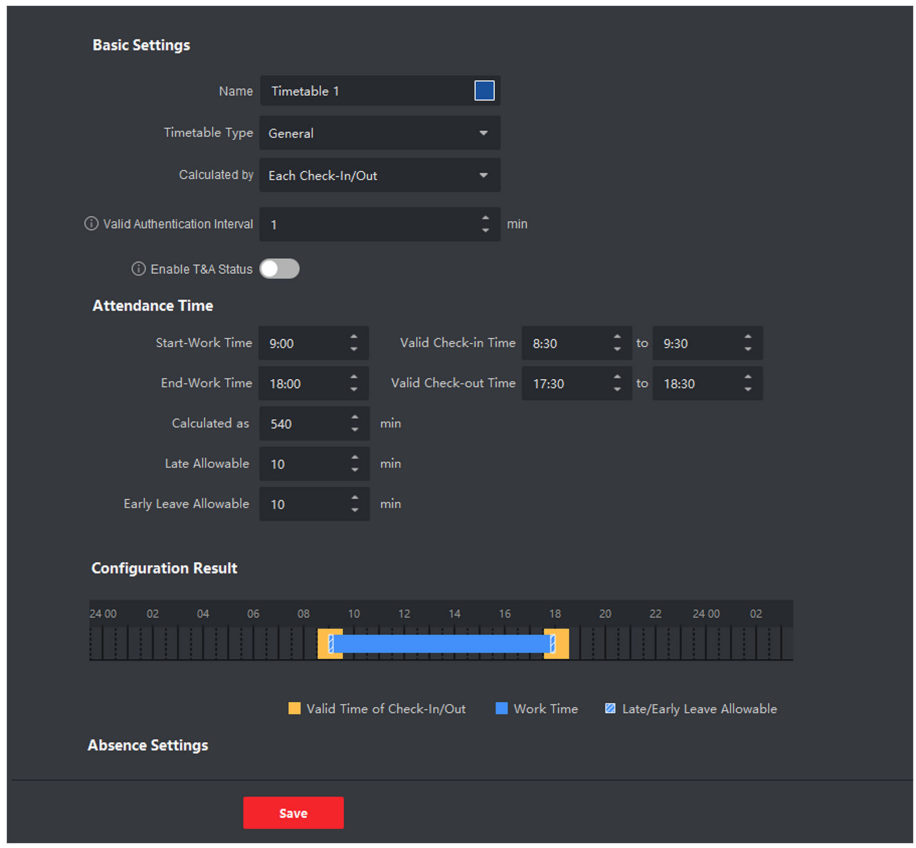


Figure 7-13 Add Timetable

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 in the Configuration Result area.

4. Select the timetable type as general.
5. Select calculation method.

First In & Last 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 Authentication 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 **Enable T&A Status** switch to on to calculate according to attendance status of the device.

Note

This function should be supported by the device.

7. 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. Set absence related parameters.

Check-In, Late for

You can set the late time duration for the employee who has checked in but is late for work. If the employee exceeds the required time period, his/her attendance data will be marked as absent.

Check-Out, Early Leave for

You can set the early leave time duration for the employee who checks out earlier than the normal leave time, and his/her attendance data will be marked as absent.

No Check-in

If the employee does not check in, his/her attendance data may be marked as absent or late.

No Check-Out

If the employee does not check out, his/her attendance data may be marked as absent or early leave.

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

10. 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 shift for employees including setting shift period (day, week, month) and the effective attendance time. According to the actual requirements, you can adding multiple timetables in one shift for employees, which requires them to check in and check out for each timetable.

Before You Start

Add a timetable first. See ***Add General 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.

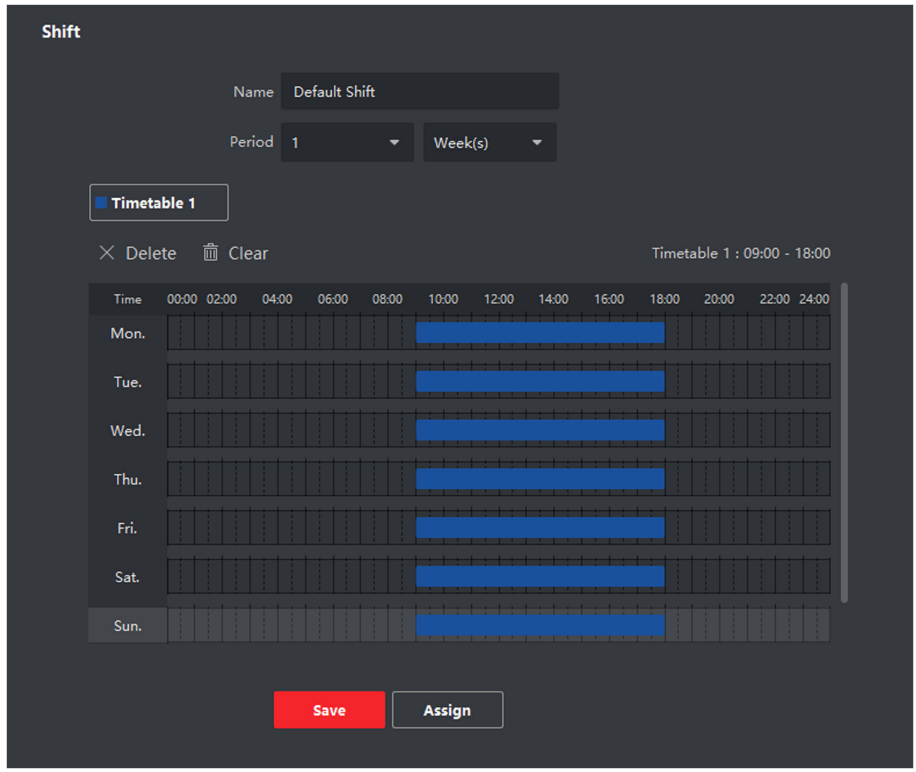


Figure 7-14 Add Shift

Note

You can select more than one timetables. The start and end work time and the valid check-in and out time in different time tables can not be overlapped.

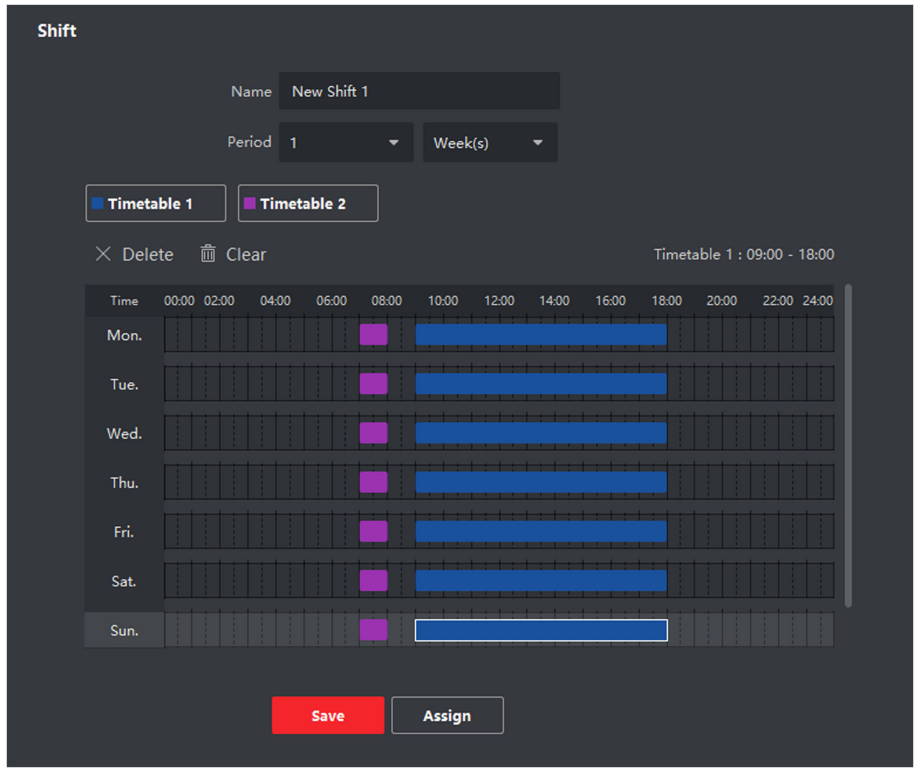


Figure 7-15 Add Multiple Timetables

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 Expire Date for the shift schedule.
   4) Set other parameters for the schedule.

      Check-in Not Required

      Persons in this schedule do not need to check-in when they come to work.

      Check-out Not Required

      Persons in this schedule do not need to check-out when they end work.

      Scheduled on Holidays

      On the holidays, this schedule is still effective and the persons needs to go to work according to the schedule.

Effective for Overtime

The persons' overtime will be recorded for this schedule.

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.

Note

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

4. Select the shift from the drop-down list.
5. **Optional:** Enable **Multiple Shift Schedules** and select the effective time period(s) from the added timetables for the persons.

Note

This is only available for shift with only one timetable.

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.

   Check-in Not Required

   Persons in this schedule do not need to check-in when they come to work.

   Check-out Not Required

   Persons in this schedule do not need to check-out when they end work.

   Scheduled on Holidays

   On the holidays, this schedule is still effective and the persons needs to go to work according to the schedule.

   Effective for Overtime

   The persons' overtime will be recorded for this schedule.
8. Click **Save**.

Set Person Schedule

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

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

Steps

Note

The person schedule has the higher priority than department schedule.

1. Click **Time & Attendance → Shift Schedule** to enter the Shift Schedule 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. **Optional:** Enable **Multiple Shift Schedules** and select the effective time period(s) from the added timetables for the persons.

   Note

   This is only available for shift with only one timetable.

   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.

Check-in Not Required

Persons in this schedule do not need to check-in when they come to work.

Check-out Not Required

Persons in this schedule do not need to check-out when they end work.

Scheduled on Holidays

On the holidays, this schedule is still effective and the persons needs to go to work according to the schedule.

Effective for Overtime

The persons' overtime will be recorded for this schedule.

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 ca 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 filed 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

Note

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 → Calculation** .
3. Set the start time and end time to define the attendance data range.
4. Set other conditions, including department, name, person ID and attendance status.
5. Click **Calculate**.

   Note

   It can only calculate the attendance data within three months.

6. Perform one of the following operations.

Correct Check-in/out	Click **Correct Check-in/out** to add check-in/out correction.
Select Items to Display	Click , or right-click the titles of different items to select items to be displayed in the report.
Generate Report	Click **Report** to generate the attendance report.
Export Report	Click **Export** to export attendance data to local PC. **Note** 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 an Overview of Employees' Attendance Data

You can search and view the employee's attendance records on the client, including attendance time, attendance status, check point, etc.

Before You Start

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

Note

- The client will automatically calculate the previous day's attendance data at 1:00 am on the next day.
- Keep the client running at 1:00 am or it cannot calculate the previous day's attendance data automatically. If not calculated automatically, you can calculate the attendance data manually. For details, refer to ***Manually Calculate Attendance Data*** .

Steps

1. Enter the Time & Attendance module.
2. Click **Attendance Statistics → Attendance Record** .
3. Set the attendance start time and end time that you want to search.
4. Set other search conditions, including department, name, and person ID.
5. Select data source as **Original Records on Device** or **Manual Handling Records**.
6. **Optional:** Click **Get Events from Device** to get the attendance data from the device.
7. **Optional:** Click **Reset** to reset all the search conditions and edit the search conditions again.
8. Click **Search**.

   The result displays on the page. You can view the employee's required attendance status and check point.
9. **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.
Custom Export	For details, refer to .

Generate Instant Report

It supports to generate the a series of attendance reports manually to view the employees' attendance results.

Before You Start

Calculate the attendance data.

Note

You can calculate the attendance data manually, or set the schedule so that the client can calculate the data automatically every day. For details, refer to ***Calculate Attendance Data*** .

Steps

1. Enter the Time & Attendance module.

2. Click **Attendance Statistics → Report** .
3. Select a report type.
4. Select the department or person to view the attendance report.
5. Set the start time and end time during which the attendance data will be displayed in the report.
6. Click **Report** to generate the statistics report and open it.

Custom Attendance Report

The client supports multiple report types and you can pre-define the report content and it can send the report automatically to the email address you configured.

Steps

Note

Set the email parameters before you want to enable auto-sending email functions. For details, refer to *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:

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

7.12 Remote Configuration (Web)

Configure device parameters remotely.

7.12.1 View Device Information

View and set device name, view device type, serial No., version, relay number, and lock number.

Select a device from the Device for Management tab and click → **System** → **Device Information** to enter the Device Information page.

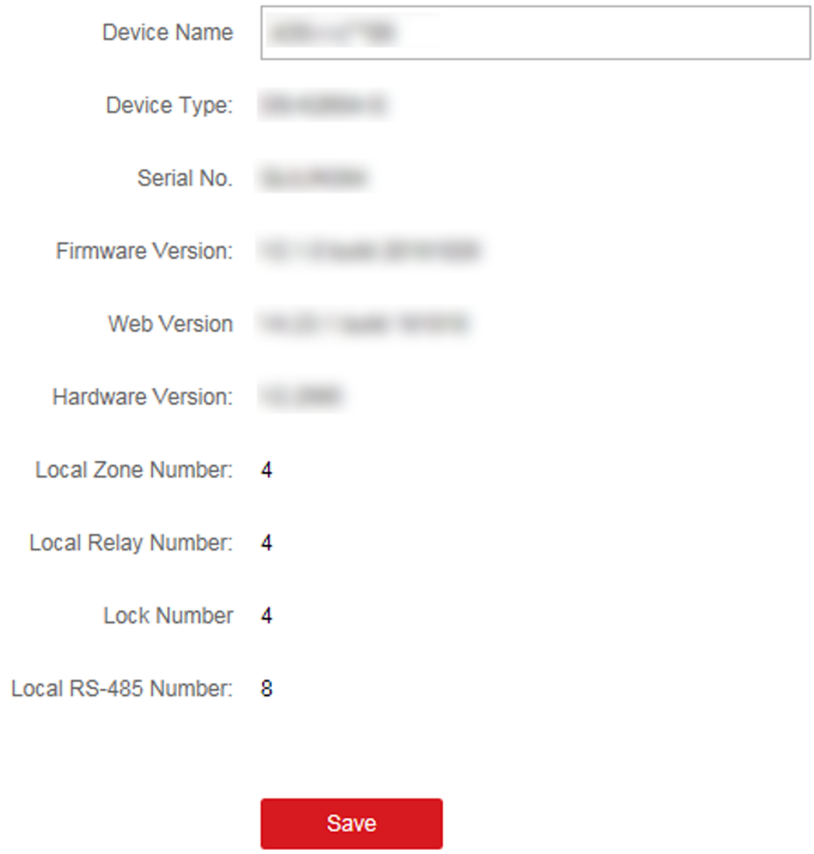


Figure 7-16 View Device Information

You can set the device name, view the device type, serial No., version, relay number, and lock number. Click **Save** to save the settings.

7.12.2 Change Device Password

You can change the device password.

Before You Start

Make sure the device is activated. For details, see *Activation*.

Steps

1. On the Device for Management page, click → **System** → **User** to enter the User tab.
2. Select a user and click **Edit** to enter the Edit page.
3. Input the old password, create a new password, and confirm the new 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 change your password regularly, especially in the high security system, changing 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.

4. Click **OK**.

Result

The device password is changed. You should enter the new password on the Device for Management page to reconnect the device.

7.12.3 Time Management

Manage device's time zone, time synchronization, and DST parameters.

Time Zone and Time Synchronization

On the Device for Management page, select a device and click → **System** → **Time** to enter the Time tab.
You can select a time zone, set NTP parameters, or manually synchronize time.

Time Zone

Select a time zone from the drop-down list.

NTP

The device will synchronize time with NTP automatically. After you enable **NTP**, you should set the NTP server address, NTP port, and synchronization interval.

Manual Time Synchronization

After you enable **Manual Time Synchronization**, you can manually set the device time.

If you check **Synchronize with Computer Time**, the **Set Time** will display the current computer's time. At this time, uncheck **Synchronize with Computer Time**, and click , you can edit the device time manually.

Click **Save** to save the settings.

DST

On the Device for Management page, click **Remote Configuration** → **System** → **Time** → **DST** to enter the DST tab.
Enable DST and you can edit the DST bias time, the DST start time, and end time.
Click **Save**.

7.12.4 System Maintenance

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

Reboot

On the Device for Management page, click → **System** → **System Maintenance** to enter the System Maintenance tab.
Click **Reboot** and the device starts rebooting.

Restore Settings

On the Device for Management page, click **Remote Configuration** → **System** → **System Maintenance** to enter the System Maintenance tab.

Restore Default

The parameters will be restored the default ones, excluding the IP address.

Restore Part of Settings

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

Restore All

All device parameters will be restored to the default ones. The device should be activated after restoring.

Import and Export

On the Device for Management page, click **Remote Configuration** → **System** → **System Maintenance** to enter the System Maintenance tab.
Import or export configuration file.

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.

Upgrade

On the Device for Management page, click **Remote Configuration** → **System** → **System Maintenance** to enter the System Maintenance tab.

Select a device type from the drop-down list, click **Browse** and select an upgrade file from the local computer, and click **Upgrade**.

Note

- If you select Card reader as the device type, you should also select a card reader No. from the drop-down list.
- The upgrade will lasts for about 2 min. Do not power off during the upgrading. After upgrading, the device will reboot automatically.

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. 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 drop-down 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 drop-down 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 Security Mode Settings

Set the security mode for logging in the client software.

On the Device for Management page, click → **System → Security** to enter the Security Mode tab.

Select a security mode from the drop-down list, and click **Save**.

You can also enable **SSH** to get a more secure network.

Security Mode

High security level for user information verification when logging in the client software.

Compatible Mode

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

7.12.7 Network Parameters Settings

Set device network parameters, including the NIC type, DHCP, and HTTP.

On the Device for Management page, click → **Network** → **Network Parameters** to enter the Network Parameters Settings tab.

NIC Type

Select a NIC type from the drop-down list. You can select either Self-adaptive, 10M, or 100M.

DHCP

If you disable the function, you should manually set the device's IPv4 address, IPv4 subnet mask, IPv4 default gateway, MTU, and port.

If you enable the function, the system will automatically assign IPv4 address, IPv4 subnet mask, IPv4 default gateway for the device.

HTTP

Set the HTTP port, DNS1 server address, and DNS2 server address.

7.12.8 Report Strategy Settings

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

On the Device for Management page, click → **Network** → **Report Strategy** to enter the Report Strategy Settings tab.

You can set the center group and the system will transfer logs via EHome protocol. Click **Save** to save the settings.

Center Group

Select a center group from the drop-down list.

Main Channel

The device will communicate with the center via the main channel.

Note

N1 refers to wired network.

7.12.9 Network Center Parameters Settings

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

On the Device for Management page, click → **Network** → **Network Center Parameters** to enter the Network Center Parameters Settings tab.

Select a center from the drop-down list.

After enabling the function, you can set the center's address type, IP address/domain name, port No., EHome user name, etc.

Click **Save**.

7.12.10 Configure Wi-Fi

Steps

1. On the Device for Management page, click → **Network** → **Wi-Fi** to enter the **Wi-Fi Settings** tab.
2. Check **Enable** to enable the Wi-Fi function.
3. Enter the SSID name and password or you can select a network from the Wi-Fi list.
4. Set the Wi-Fi **Security Mode** from the drop-down list.
5. **Optional:** Click **Refresh** to refresh the network status.
6. **Optional:** Set WLAN parameters.
   1) On the **Wi-Fi Settings** page, click **WLAN** to enter the **WLAN** page.
   2) Uncheck **DHCP** and set the IP address, the subnet mask, the default gateway, the MAC address, the DNS1 IP Address, and the DNS2 IP address.
7. 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.

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 Set Relay Parameters

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

Click to enter the remote configuration page.

Click **Alarm** → **Relay** . Select a relay and click and set the relay name and output delay time.
Click **OK** to save the settings.

7.12.13 Set Access Control Parameters

Steps

1. On the Device for Management page, click → **Others** → **Access Control Parameters** to enter the **Access Control Parameters** tab.
2. Check the checkbox to enable the function.

   Audio Prompt (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 Pictures after Capturing

   If you enable this function, the captured pictures will be sent to the client software.

   Save Captured Pictures

   If you enable this function, the captured pictures will be saved.

   Temperature Measurement Only

   When enabling the function, the device will not authenticate the permissions, but only take the temperature. When disabling the function, the device will authenticate the permissions and at the same time take the temperature.

   Capture White Light Picture

   When enabling the function, the pictures captured by the white light camera will be uploaded to the platform. If disabling the function, the device will only upload pictures captured by thermographic camera to the platform.

   Door Not Open When Detecting Abnormal Temperature

   When enabling the function, the door will not open when the detected temperature is higher or lower than the configured temperature threshold. By default, the temperature is enabled.

   Must Wear Face Mask

   After enabling this function, the authenticated person must wear a face mask, otherwise the authentication will be failed.

   Over-Temperature Alarm

   Edit the threshold according to actual situation. If the detected temperature is higher than the configured parameters, an alarm will be triggered. The value should be between 35.1 ℃ and 44.9 ℃.
3. Click **Save**.

7.12.14 Set Face Recognition Terminal Parameters

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

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

Click **Other → Face Recognition Terminal Parameters** and you can configure the device parameters.

Face Picture Database

Select **Deep Learning** as the face picture database.

Save Authenticating Face Picture

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

CPU Card Reading

Select to read card No. or file.

Work Mode

Set the device work mode as **Normal Mode**. You should authenticate your credential for accessing.

ECO Mode

After enabling the ECO mode, the device will use the IR camera to authenticate faces in the low light or dark environment. And you can set he ECO mode threshold, ECO mode (1:N), and ECO mode (1:1).

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.

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 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 8.

Click **Save** to save the settings.

7.12.15 Configure Face Picture Parameters

Steps

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

   Pitch Angle

   The maximum pitch angle when face authentication.

   Yaw Angle

   The maximum yaw angle when face authentication.

   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.

Score

The device will score the captured picture according to the yaw angle, pitch angle, and pupillary distance. If the score is less than the configured value, face recognition will be failed.

You can set the face picture parameters when authenticating.

4. Click **Save**.

7.12.16 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. 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 type from the drop-down list.
5. Select a supplement light mode from the drop-down list.
6. **Optional:** Set the supplement light brightness.
7. Click **Save** to save the settings.

7.12.17 Set Device 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.

Click to enter the remote configuration page.

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

7.12.18 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. 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**.

7.12.19 Configure Volume Input or Output

Steps

1. On the Device for Management page, click **→ Image → Audio Input or Output** to enter **Audio Input or Output** tab.
2. Move the block to adjust the device input and output volume.
3. Click **Save**.

7.12.20 Operate Relay

Steps

1. Click **Maintenance and Management → Device** to enter the device list.
2. Click to enter the remote configuration page.
3. Click **Operation → Relay** .
4. Enable or disable the relay.

7.12.21 View Relay Status

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

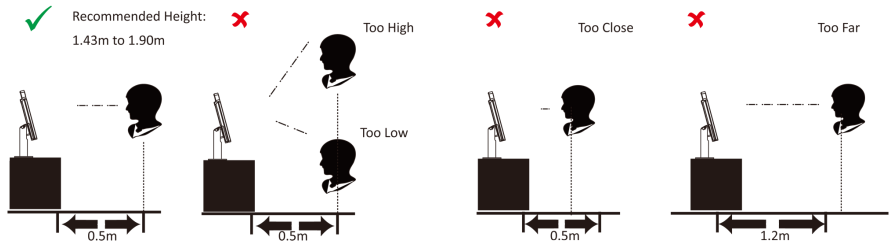
Click to enter the remote configuration page.

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

Appendix A. Tips When Collecting/Comparing Face Picture

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

Positions (Recommended Distance: 0.5 m)



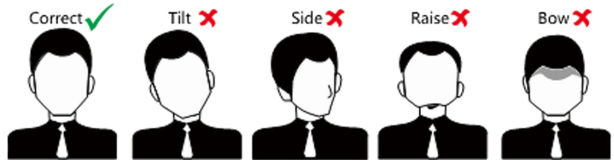
Expression

- 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.

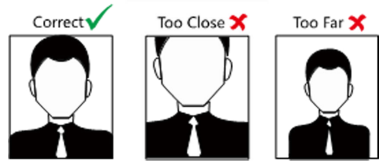
Posture

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 B. Tips for Installation Environment

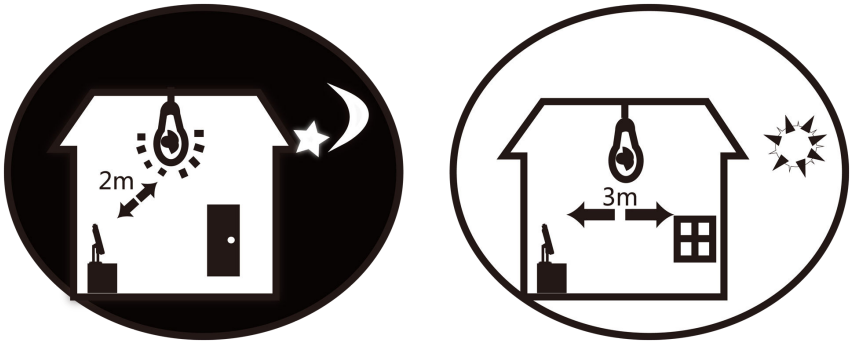
1. Light Source Illumination Reference Value

Candle: 10Lux

Bulb: 100~850Lux

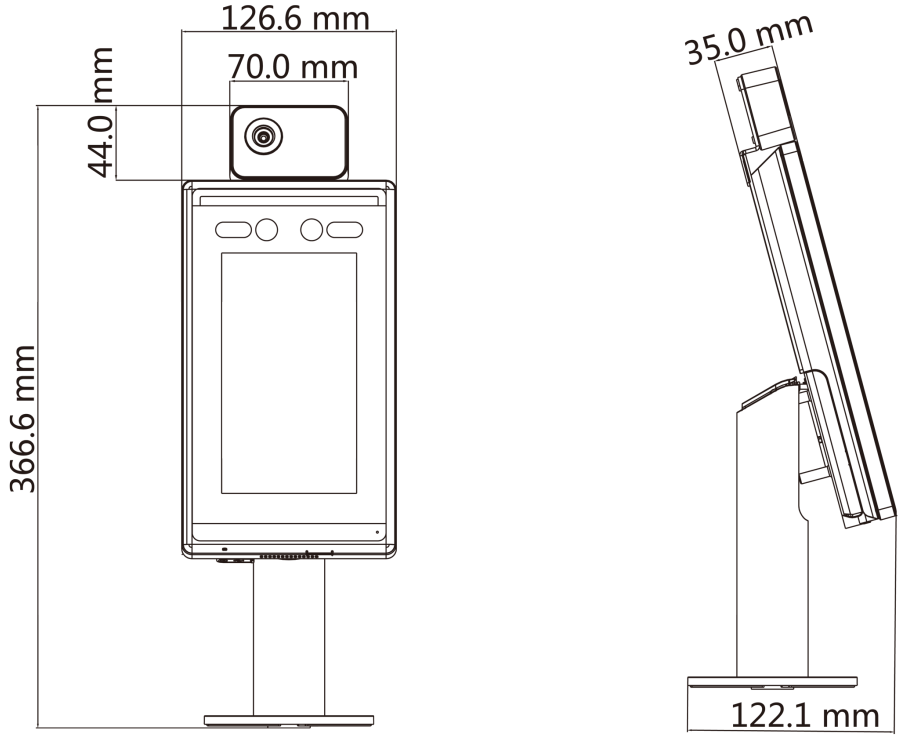
Sunlight: More than 1200Lux

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

Appendix C. Dimension



See Far, Go Further