Face Recognition Terminal

User Manual

Legal Information

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

About this Manual

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

Trademarks

HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
Other trademarks and logos mentioned are the properties of their respective owners.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.
YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE

DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Data Protection

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

Symbol Conventions

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

Symbol	Description
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

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

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:
(1) this device may not cause interference, and
(2) this device must accept any interference, including interference that may cause undesired operation of the device.
Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radioexempts de licence. L'exploitation est autorisée aux deux conditions suivantes :
(1) l'appareil ne doit pas produire de brouillage, et
(2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

COMPLIANCE NOTICE

The thermal series products might be subject to export controls in various countries or regions, including without limitation, the United States, European Union, United Kingdom and/or other member countries of the Wassenaar Arrangement. Please consult your professional legal or compliance expert or local government authorities for any necessary export license requirements if you intend to transfer, export, re-export the thermal series products between different countries.

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 completely 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
- Outdoor use or use in environment exceeding the device temperature measurement will affect the temperature measurement accuracy.

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 3
Chapter 3 Installation 5
3.1 Installation Environment 5
3.2 Mount With Bracket 5
3.2.1 Preparation before Mounting with Bracket 5
3.2.2 Mount with Bracket 7
Chapter 4 Wiring 10
4.1 Terminal Description 10
4.2 Wire Normal Device 13
4.3 Wire Secure Door Control Unit 14
Chapter 5 Activation 15
5.1 Activate via Device 15
5.2 Activate via SADP 17
5.3 Activate Device via Client Software 18
5.4 Activate via Web Browser 19
Chapter 6 Quick Operation 20
6.1 Select Language 20
6.2 Set Application Mode 21
6.3 Set Network Parameters 23
6.4 Set Administrator 25
Chapter 7 Basic Operation 28
7.1 Login 28
7.1.1 Login by Administrator 28

7.1.2 Login by Activation Password 31
7.2 Communication Settings 32
7.2.1 Set Wired Network Parameters 33
7.2.2 Set Wi-Fi Parameters 34
7.2.3 Set RS-485 Parameters 36
7.2.4 Set Wiegand Parameters 37
7.3 User Management 38
7.3.1 Add Administrator 38
7.3.2 Add Face Picture 39
7.3.3 Add Card 41
7.3.4 View Password 42
7.3.5 Set Authentication Mode 43
7.3.6 Search and Edit User 43
7.4 Temperature Measurement Settings 44
7.5 Data Management 46
7.5.1 Delete Data 46
7.5.2 Import Data 46
7.5.3 Export Data 47
7.6 Identity Authentication 48
7.6.1 Authenticate via Single Credential 48
7.6.2 Authenticate via Multiple Credential 48
7.7 Basic Settings 49
7.8 Set Biometric Parameters 52
7.9 Set Access Control Parameters 53
7.10 Time and Attendance Status Settings 55
7.10.1 Disable Attendance Mode via Device 55
7.10.2 Set Manual Attendance via Device 56
7.10.3 Set Auto Attendance via Device 58

7.10.4 Set Manual and Auto Attendance via Device 59
7.11 System Maintenance 61
7.12 Video Intercom 63
7.12.1 Call Client Software from Device 63
7.12.2 Call Center from Device 64
7.12.3 Call Device from Client Software 64
7.12.4 Call Room from Device 65
7.12.5 Call Mobile Client from Device 65
Chapter 8 Operation via Web Browser 67
8.1 Login 67
8.2 Live View 67
8.3 Person Management 69
8.4 Search Event 70
8.5 Configuration 70
8.5.1 Set Local Parameters 70
8.5.2 View Device Information 71
8.5.3 Set Time 71
8.5.4 Set DST 72
8.5.5 View Open Source Software License 73
8.5.6 Upgrade and Maintenance 73
8.5.7 Log Query 74
8.5.8 Security Mode Settings 74
8.5.9 Certificate Management 75
8.5.10 Change Administrator's Password 76
8.5.11 View Device Arming/Disarming Information 77
8.5.12 Network Settings 77
8.5.13 Set Video and Audio Parameters 81
8.5.14 Customize Audio Content 83

8.5.15 Set Image Parameters 84
8.5.16 Set Supplement Light Brightness 85
8.5.17 Time and Attendance Settings 86
8.5.18 Set Video Intercom Parameters 89
8.5.19 Configure SIP Parameters 90
8.5.20 Access Control Settings 91
8.5.21 Set Biometric Parameters 98
8.5.22 Set Notice Publication 101
8.5.23 Temperature Measurement Settings 102
Chapter 9 Client Software Configuration 106
9.1 Configuration Flow of Client Software 106
9.2 Device Management 106
9.2.1 Add Device 107
9.2.2 Reset Device Password 109
9.2.3 Manage Added Devices 110
9.3 Group Management 111
9.3.1 Add Group 111
9.3.2 Import Resources to Group 111
9.4 Person Management 112
9.4.1 Add Organization 112
9.4.2 Import and Export Person Identify Information 113
9.4.3 Get Person Information from Access Control Device 115
9.4.4 Issue Cards to Persons in Batch 116
9.4.5 Report Card Loss 116
9.4.6 Set Card Issuing Parameters 116
9.5 Configure Schedule and Template 118
9.5.1 Add Holiday 118
9.5.2 Add Template 119

9.6 Set Access Group to Assign Access Authorization to Persons 120
9.7 Configure Advanced Functions 122
9.7.1 Configure Device Parameters 122
9.7.2 Configure Device Parameters 129
9.8 Door Control 132
9.8.1 Control Door Status 132
9.8.2 Check Real-Time Access Records 133
Appendix A. Tips When Collecting/Comparing Face Picture 136
Appendix B. Tips for Installation Environment 138
Appendix C. Dimension 139
Appendix D. Communication Matrix and Device Command 140

Chapter 1 Overview

1.1 Overview

The face recognition terminal is a kind of access control device integrated with temperature screening function. It can fast taking skin-surface temperature and upload abnormal temperature event to the center, which can be widely applied in multiple scenarios, such as enterprises, stations, dwellings, factories, schools, campus and so on.

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:

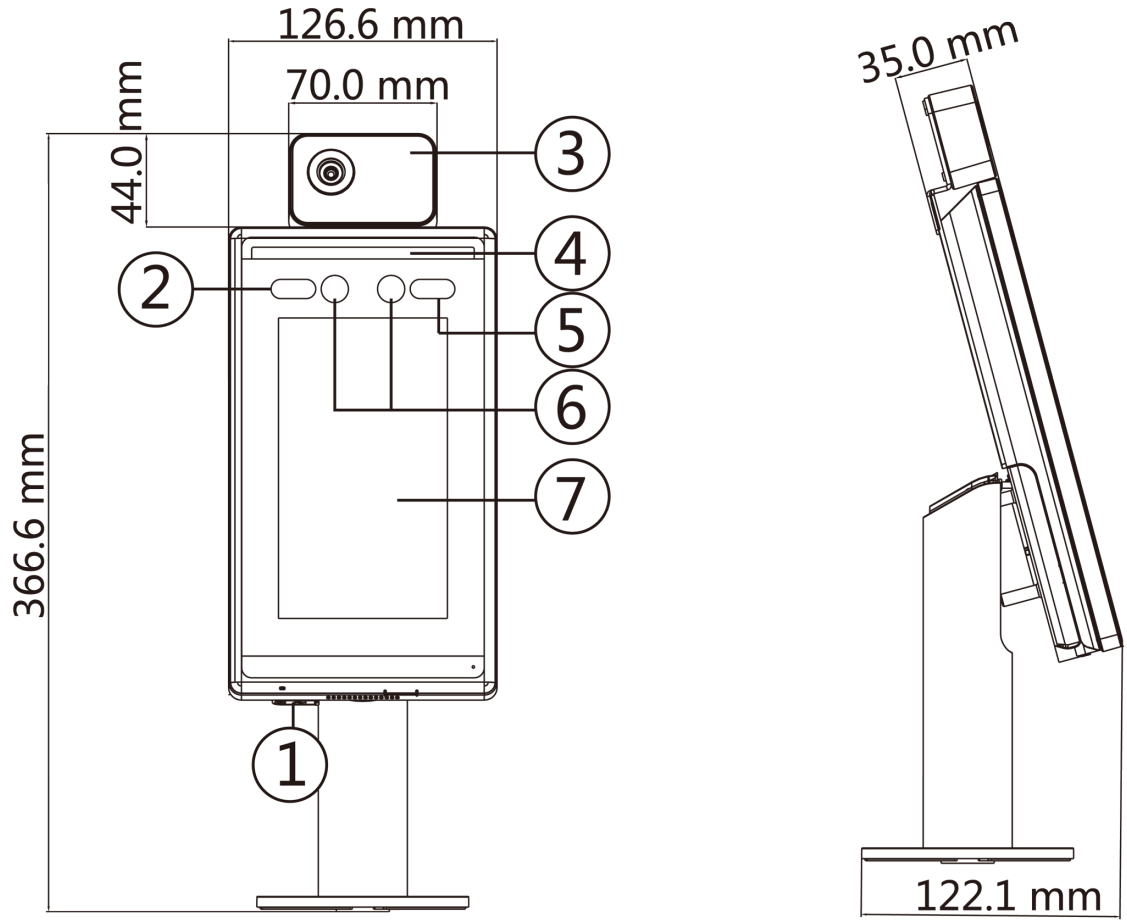


Figure 2-1 Face Recognition Terminal Diagram

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

No.	Name
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.

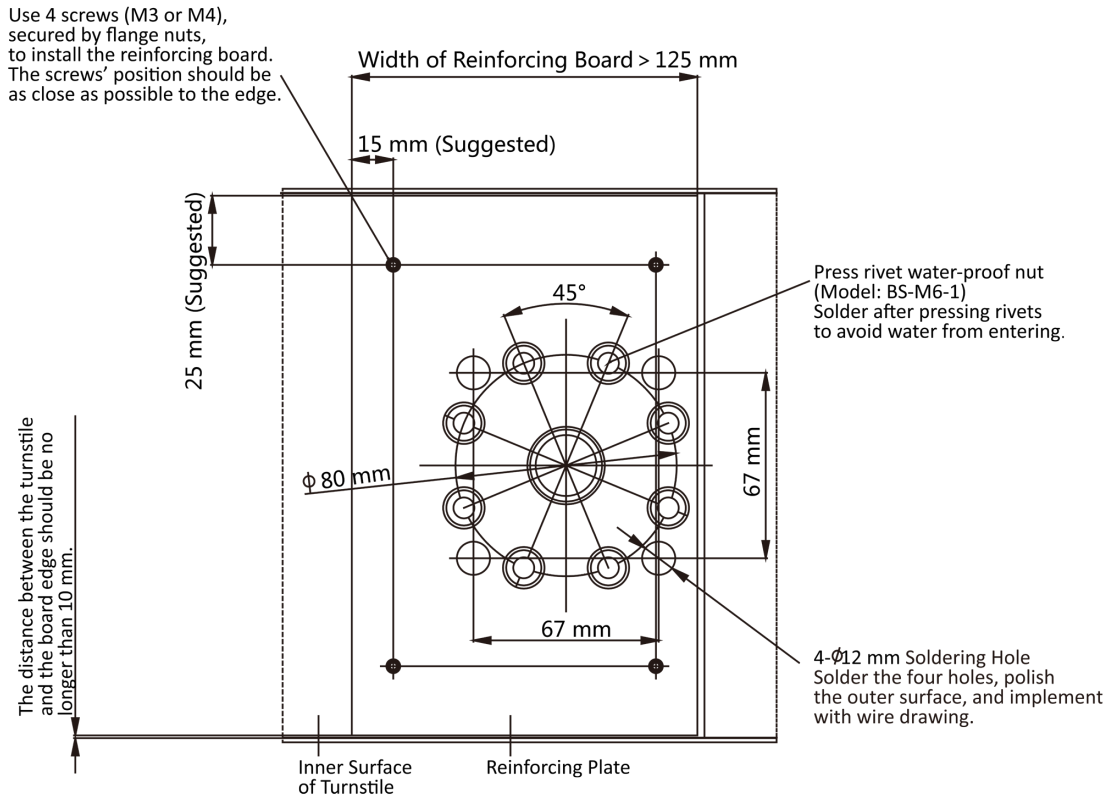


Figure 3-1 Drill Holes on Turnstile

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.

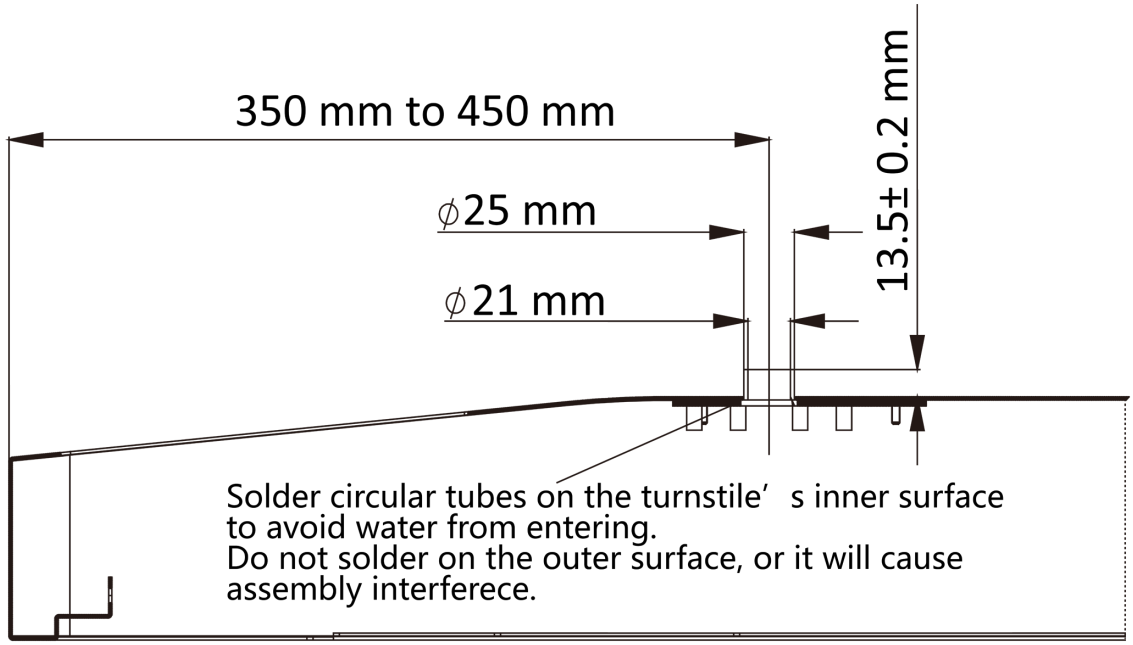


Figure 3-2 Solder Tubes

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.

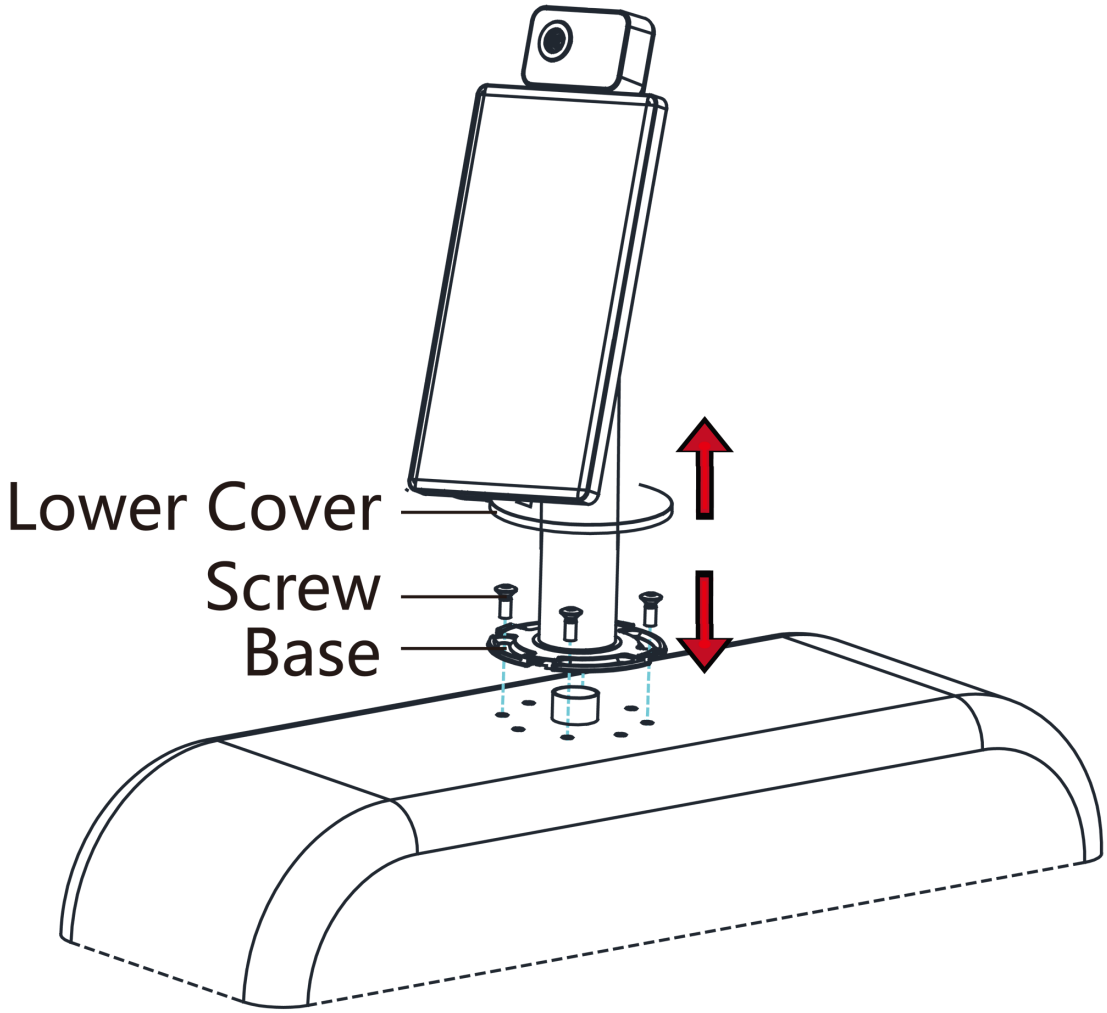


Figure 3-3 Secure Bracket and Turnstile

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°.

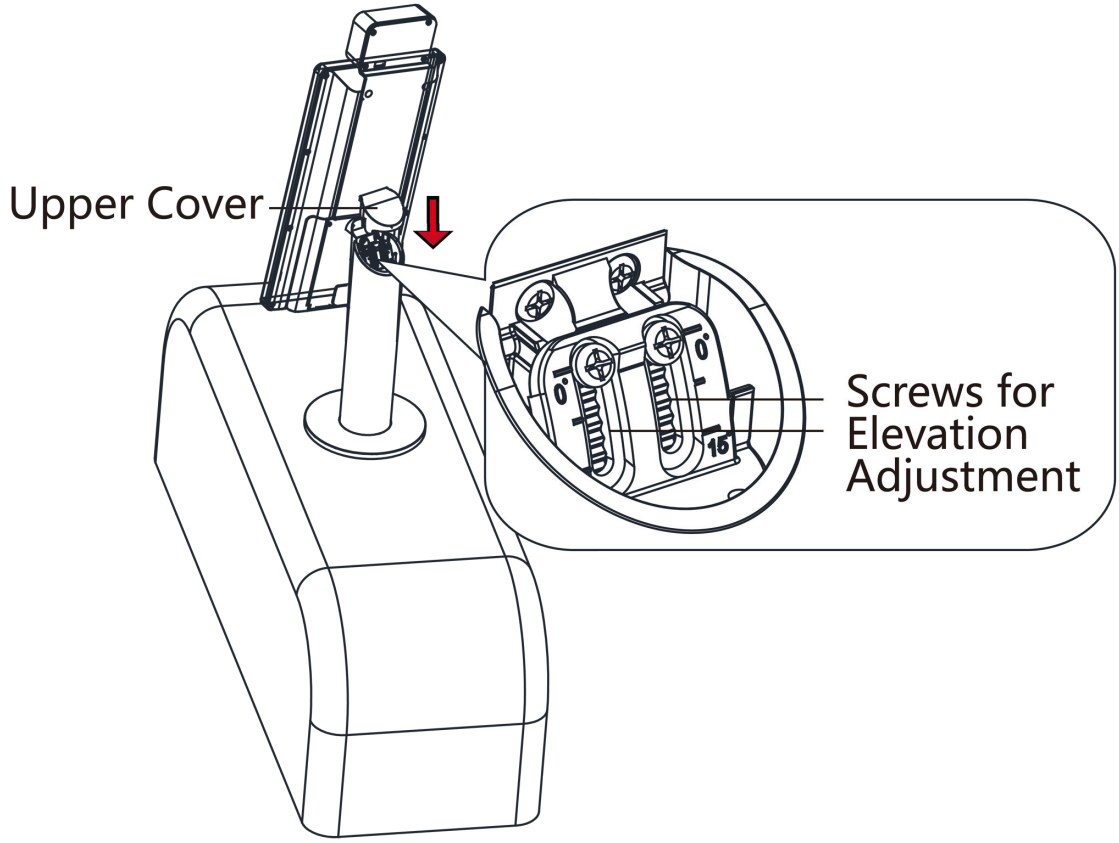


Figure 3-5 Adjust Elevation

7. After installation, for the proper use of the device (outdoor use), stick the protection film (parts of models supplied) on the screen.

Chapter 4 Wiring

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

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

Note

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

4.1 Terminal Description

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

The terminal's diagram is as follows:

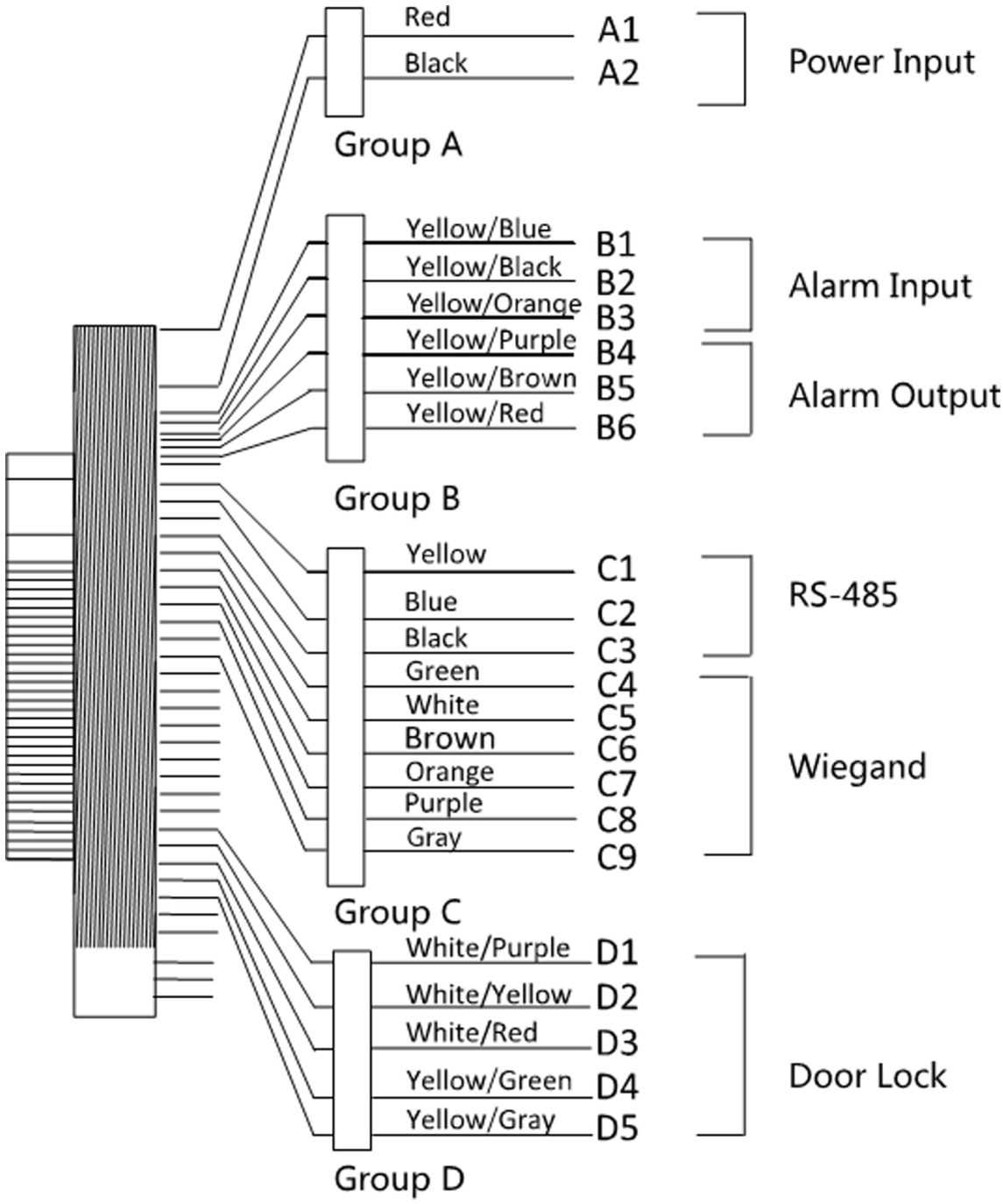


Figure 4-1 Terminal Diagram

The descriptions of the terminals are as follows:

Table 4-1 Terminal Descriptions

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

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

4.2 Wire Normal Device

You can connect the terminal with normal peripherals.

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

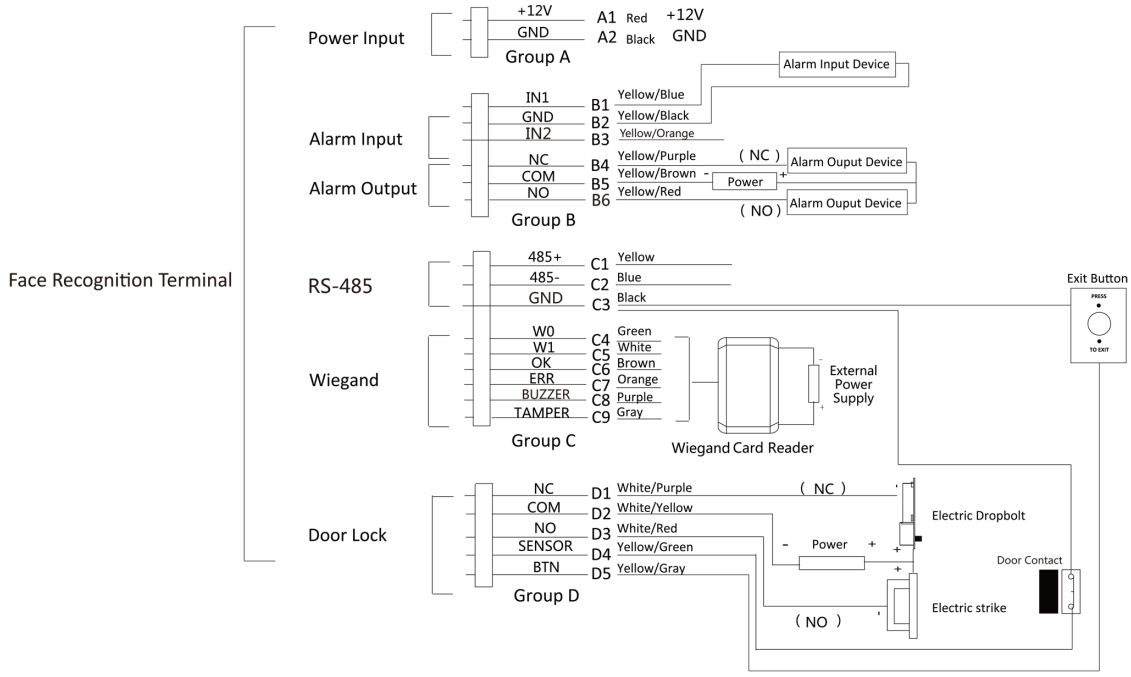


Figure 4-2 Device Wiring

Note

- You should set the face recognition terminal's Wiegand direction to "Input" to connect to a Wiegand card reader. If connects to an access controller, you should set the Wiegand direction to "Output" to transmit authentication information to the access controller.
- For details about Wiegand direction settings, see *Setting Wiegand Parameters* in *Communication Settings*.
- The 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.

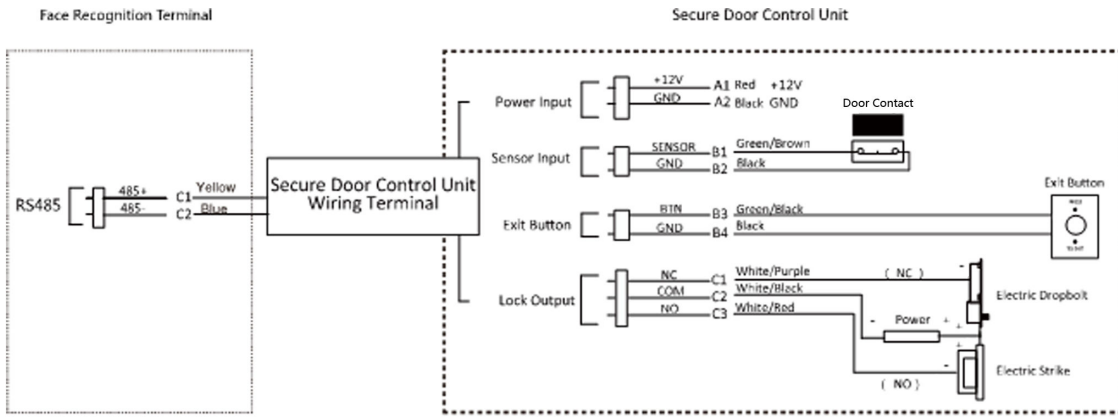


Figure 4-3 Secure Door Control Unit Wiring

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.

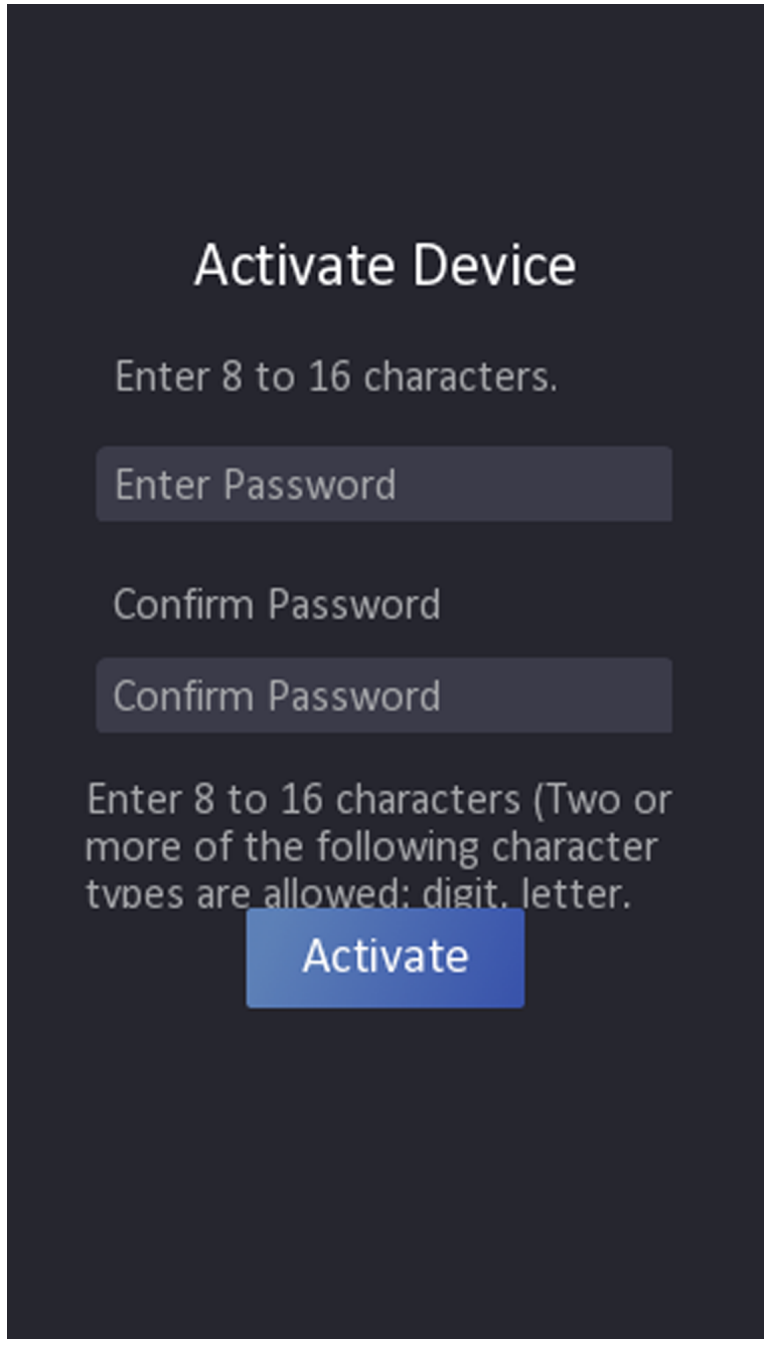


Figure 5-1 Activation Page

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.

Note

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

- After activation, you should select a language according to your actual needs.
- 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 ***Set Network Parameters*** .
- After activation, if you need to operate the device remotely via APP, you should scan the QR code to link to the APP. For details, see .
- After activation, if you need to add administrator to manage the device parameters, you should set administrator. For details, see ***Add Administrator*** .

5.2 Activate via SADP

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

Before You Start

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

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

Steps

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

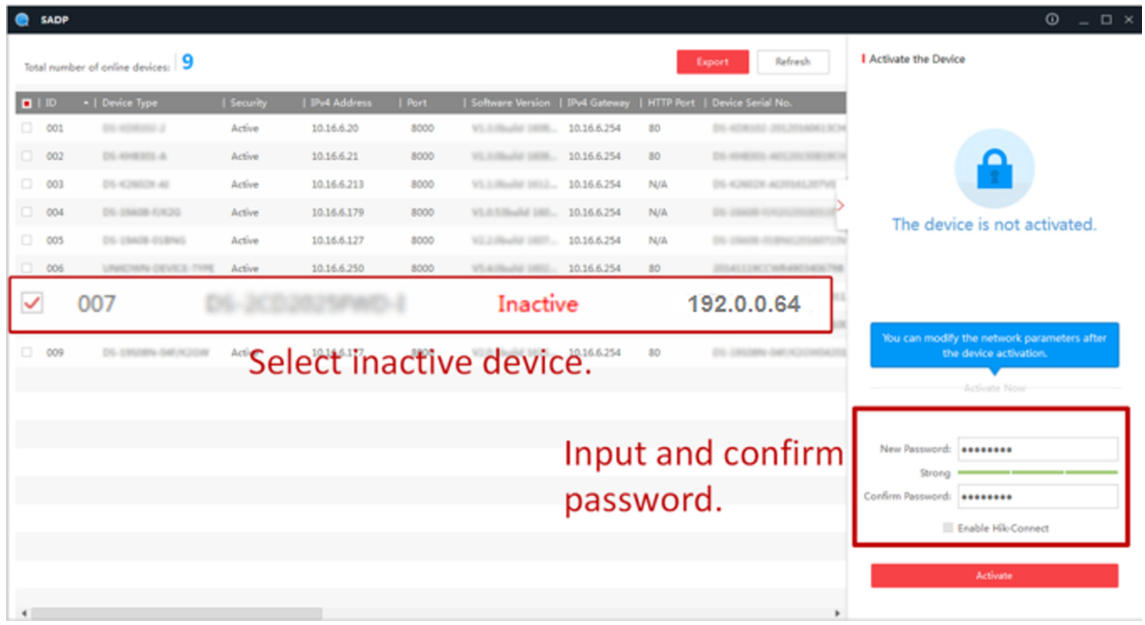
Caution

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

Note

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

4. Click **Activate** to start activation.



Status of the device becomes **Active** after successful activation.

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

5.3 Activate Device via Client Software

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

Steps

Note

This function should be supported by the device.

1. Enter the Device Management page.
2. Click on the right of **Device Management** and select **Device**.
3. Click **Online Device** to show the online device area.

   The searched online devices are displayed in the list.
4. Check the device status (shown on **Security Level** column) and select an inactive device.

5. Click **Activate** to open the Activation dialog.
6. Create a password in the password field, and confirm the password.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you 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.

Note

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

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

5.4 Activate via Web Browser

You can activate the device via the web browser.

Steps

1. Enter the device default IP address (192.0.0.64) in the address bar of the web browser, and press **Enter**.

Note

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

2. Create a new password (admin password) and confirm the password.

Caution

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

Note

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

3. Click **Activate**.
4. Edit the device IP address. You can edit the IP address via the SADP tool, the device, and the client software.

Chapter 6 Quick Operation

6.1 Select Language

You can select a language for the device system.

After the device activation, you can select a language for the device system.

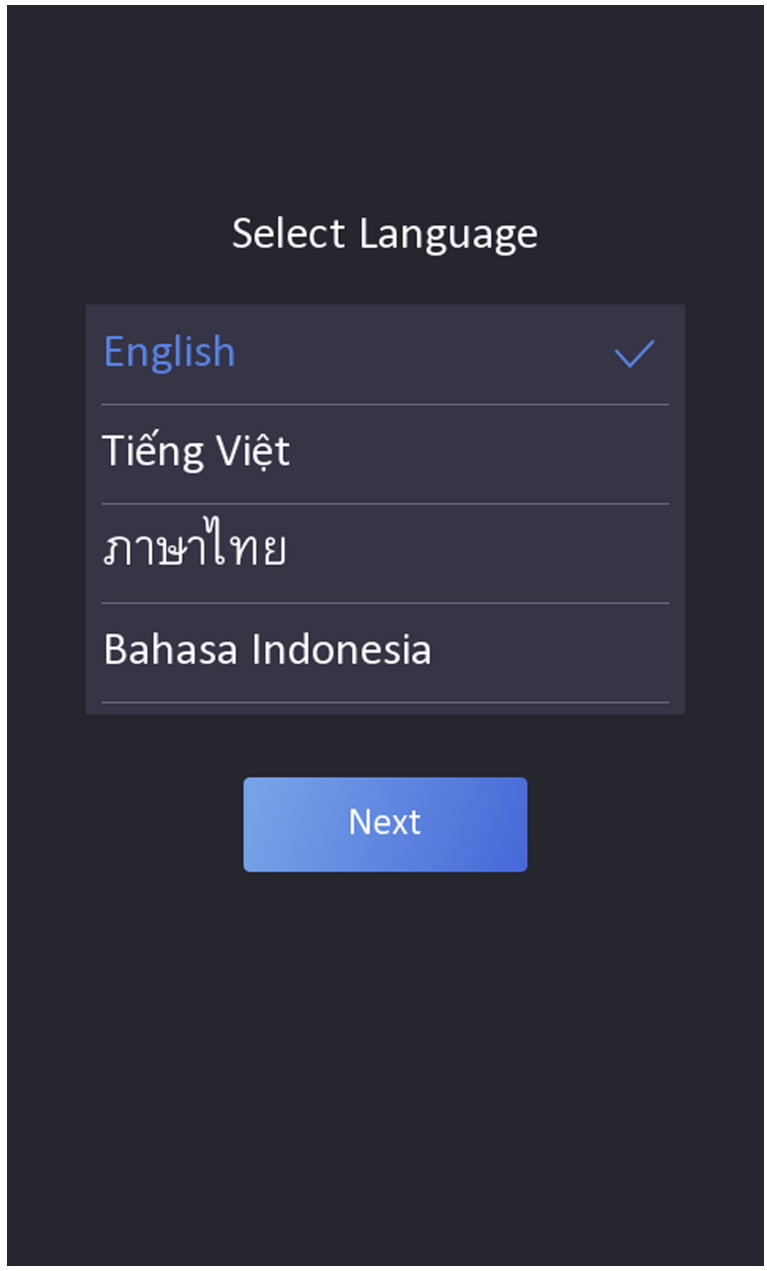


Figure 6-1 Select System Language

By default, the system language is English.

6.2 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.

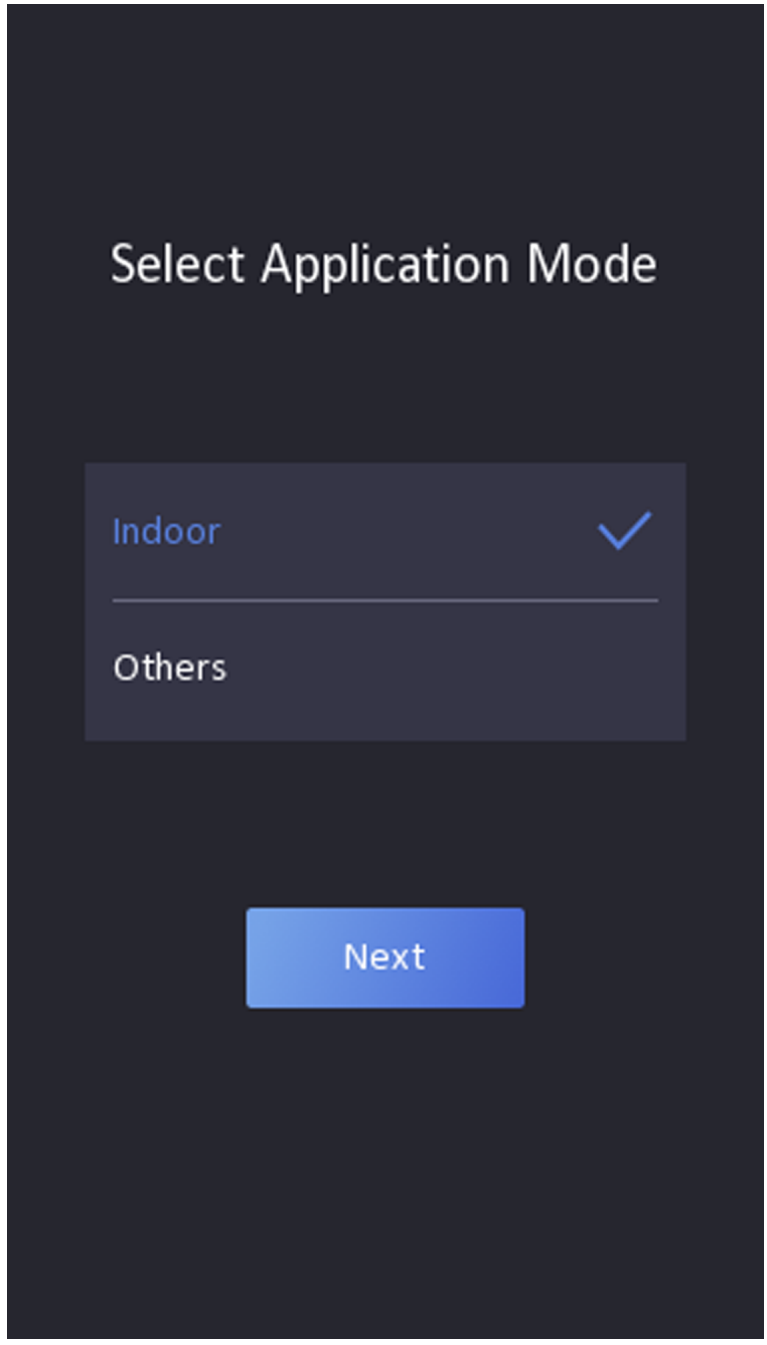


Figure 6-2 Welcome Page

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.

6.3 Set Network Parameters

After activation and select application mode, you can set the network for the device

Steps

1. When you enter the Select Network page, tap **Wired Network** or **Wi-Fi** for your actual needs.

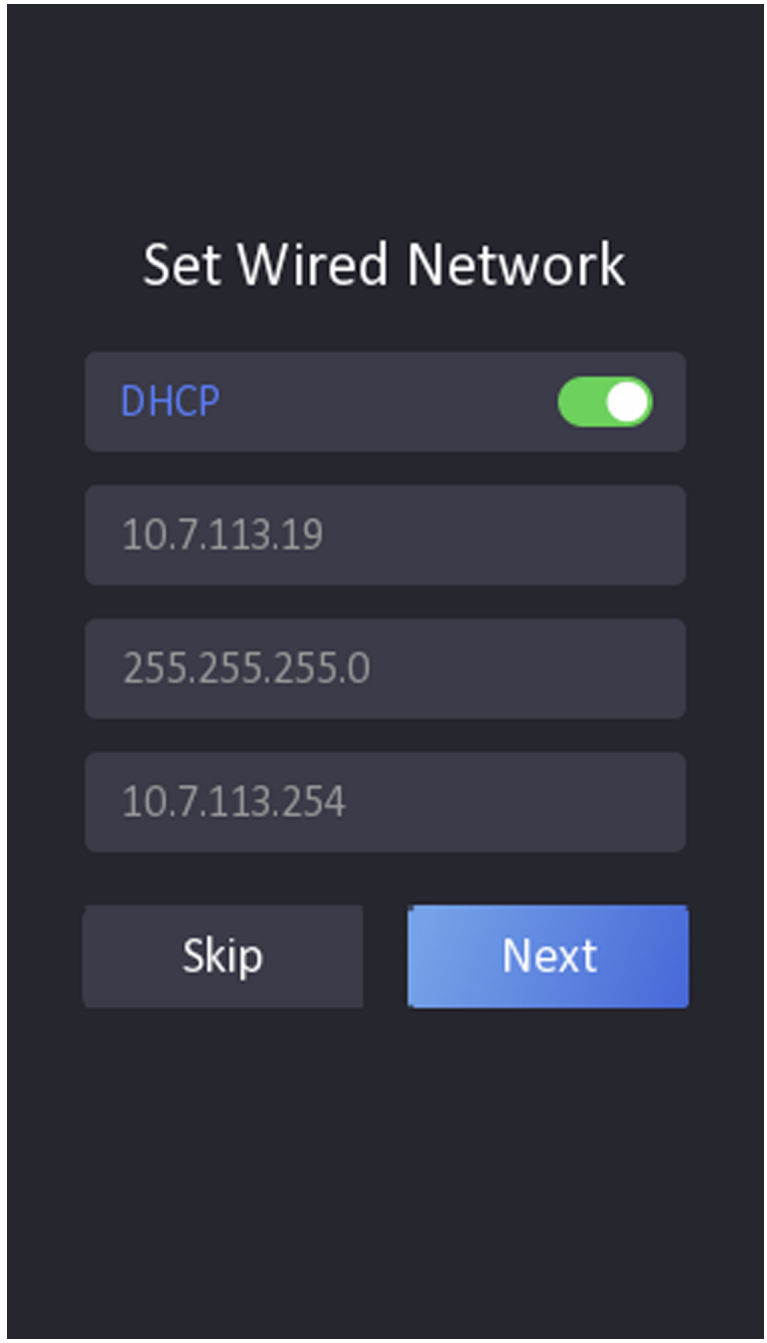


Figure 6-3 Select Network

Note

Disconnect the wired network before connecting a Wi-Fi.

2. Tap **Next**.

Wired Network

Note

Make sure the device has connected to a network.

If enable **DHCP**, the system will assign the IP address and other parameters automatically.

If disable **DHCP**, you should set the IP address, the subnet mask, and the gateway.

Wi-Fi

Select a Wi-Fi and enter the Wi-Fi's password to get connected.

Or tap **Add Wi-Fi** and enter the Wi-Fi's name and the password to get connected.

3. **Optional:** Tap **Skip** to skip network settings.

6.4 Set Administrator

After device activation, you can add an administrator to manage the device parameters.

Before You Start

Activate the device and select an application mode.

Steps

1. **Optional:** Tap **Skip** to skip adding administrator if required.
2. Enter the administrator's name (optional) and tap **Next**.

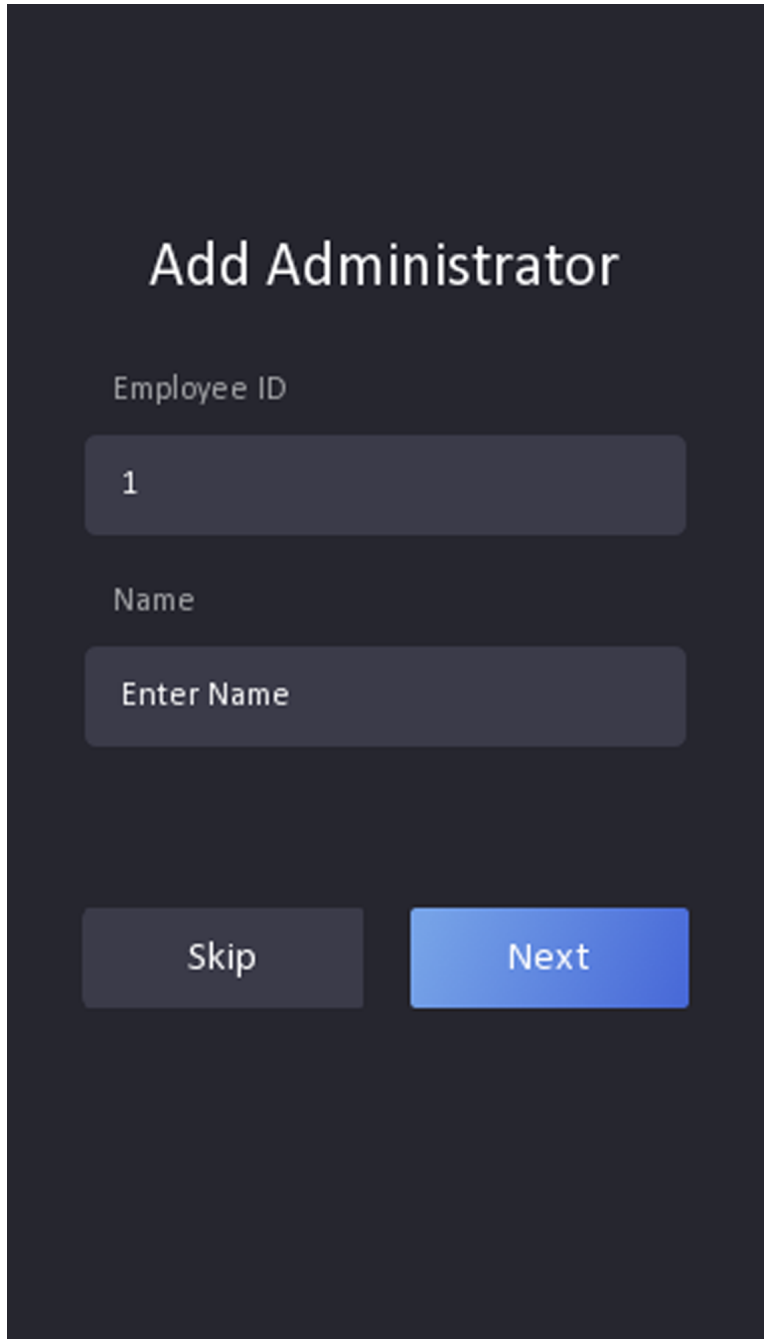


Figure 6-4 Add Administrator Page

3. Select a credential to add.

Note

Up to one credential should be added.

- : Face forward at the camera. Make sure the face is in the face recognition area. Click to capture and click to confirm.
- : Enter the card No. or present card on the card presenting area. Click **OK**.

4. Click **OK**.

You will enter the authentication page.

Status Icon Description

/

Device is armed/not armed.

/

Hik-Connect is enabled/disabled.

/ /

The device wired network is connected/not connected/connecting failed.

/ /

The device' Wi-Fi is enabled and connected/not connected/enabled but not connected.

Shortcut Keys Description

Note

You can configure those shortcut keys displayed on the screen. For details, see ***Basic Settings*** .

- Enter the device room No. and tap **OK** to call.
- Tap to call the center.

Note

The device should be added to the center, or the calling operation will be failed.

Enter password to authenticate.

Chapter 7 Basic Operation

7.1 Login

Login the device to set the device basic parameters.

7.1.1 Login by Administrator

If you have added an 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 and slide to the left/right by following the gesture to enter the admin login page.

Figure 7-1 Admin Login

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

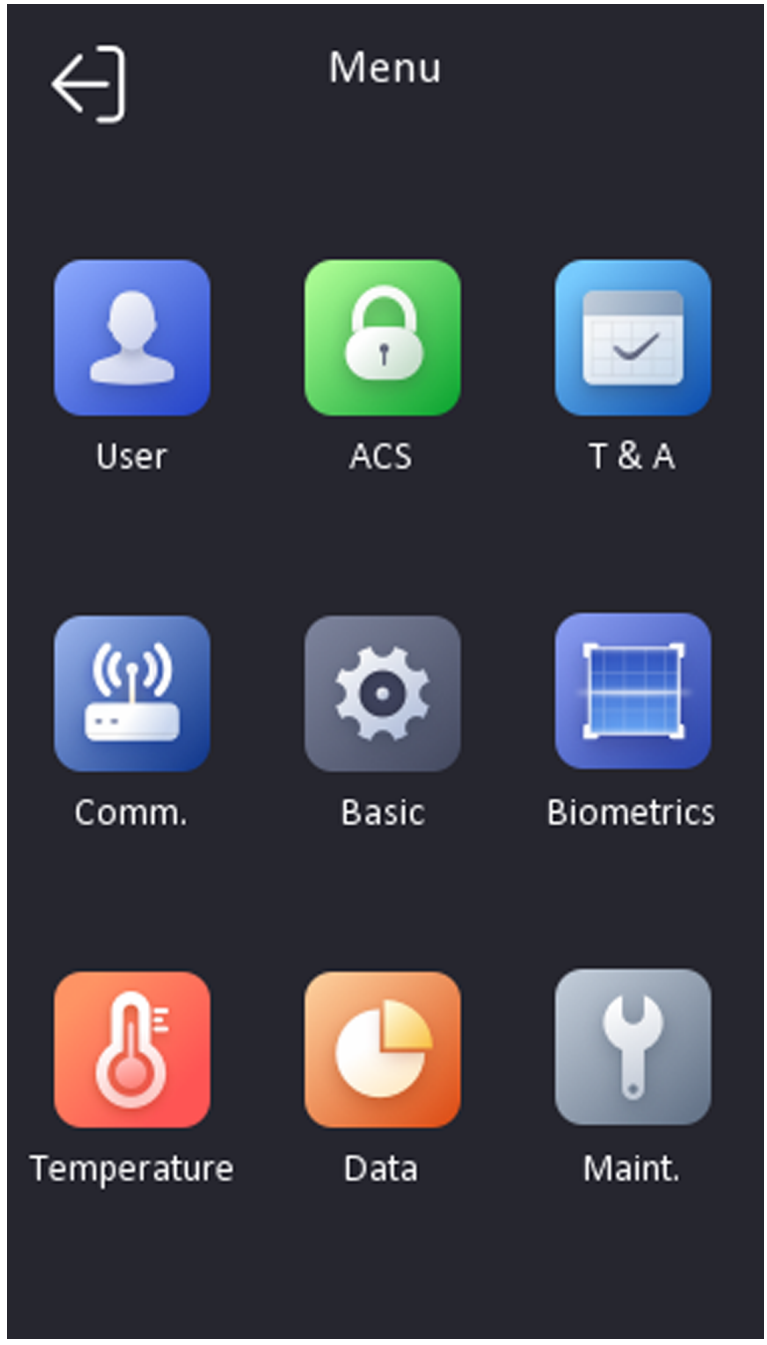


Figure 7-2 Home Page

Note

The device will be locked for 30 minutes after 5 failed 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.

7.1.2 Login by Activation Password

You should login the system before other device operations. If you do not configure an administrator, you should follow the instructions below to login.

Steps

1. Long tap on the initial page for 3 s and slide to the left/right by following the gesture 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.

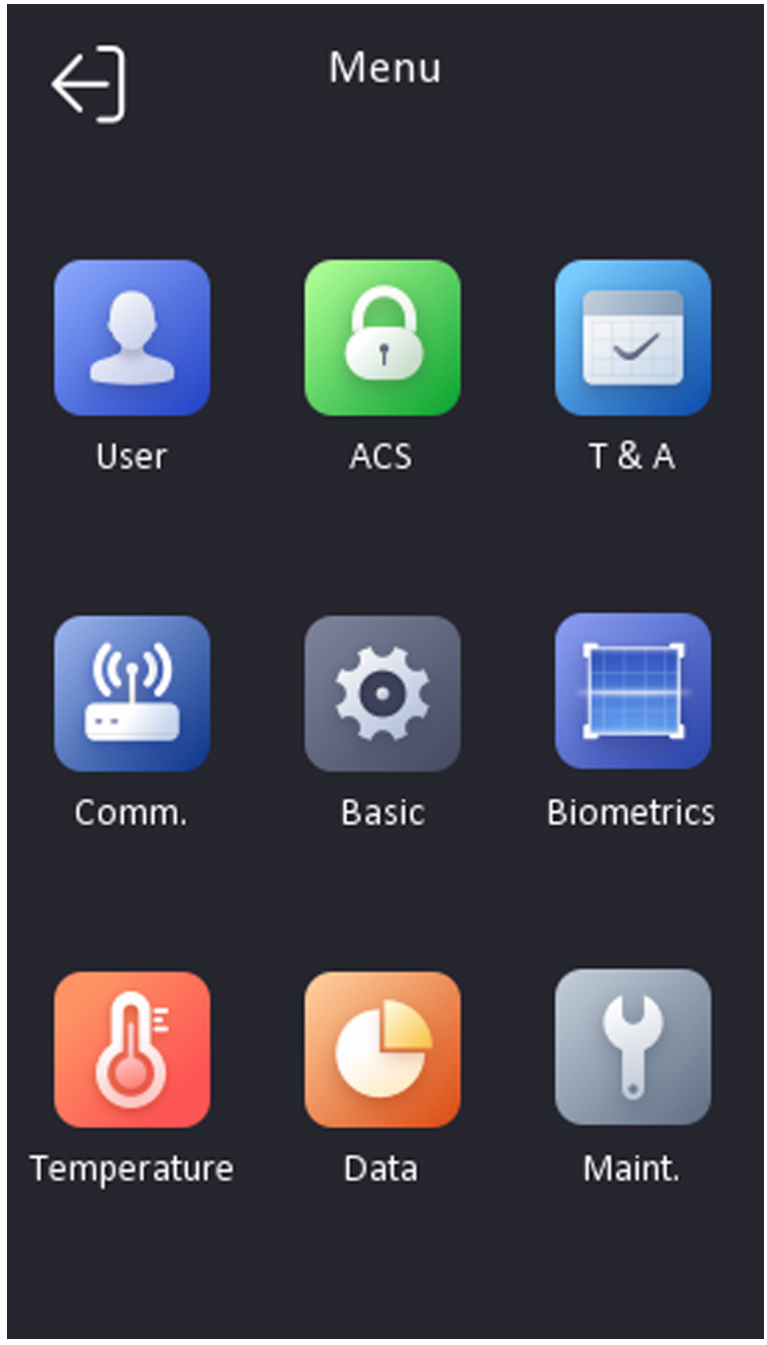


Figure 7-3 Home Page

7.2 Communication Settings

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

7.2.1 Set Wired Network Parameters

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

Steps

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

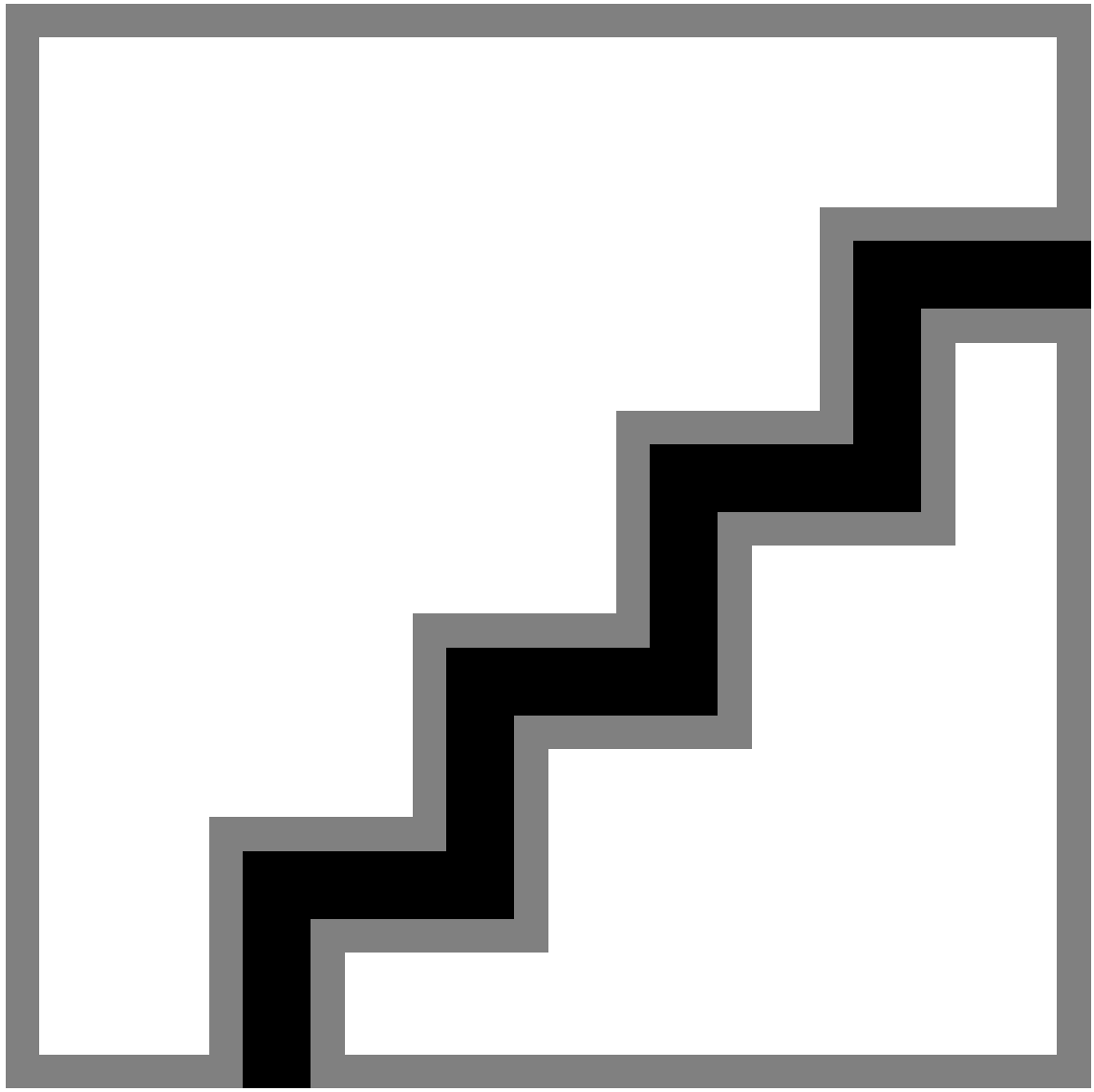


Figure 7-4 Wired Network Settings

3. Set IP Address, Subnet Mask, and Gateway.
   - Enable **DHCP**, and the system will assign IP address, subnet mask, and gateway automatically.

- Disable **DHCP**, and you should set the IP address, subnet mask, and gateway manually.

  Note

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

4. Set the DNS parameters. You can enable **Auto Obtain DNS**, set the preferred DNS server and the alternate DNS server.

7.2.2 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.

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

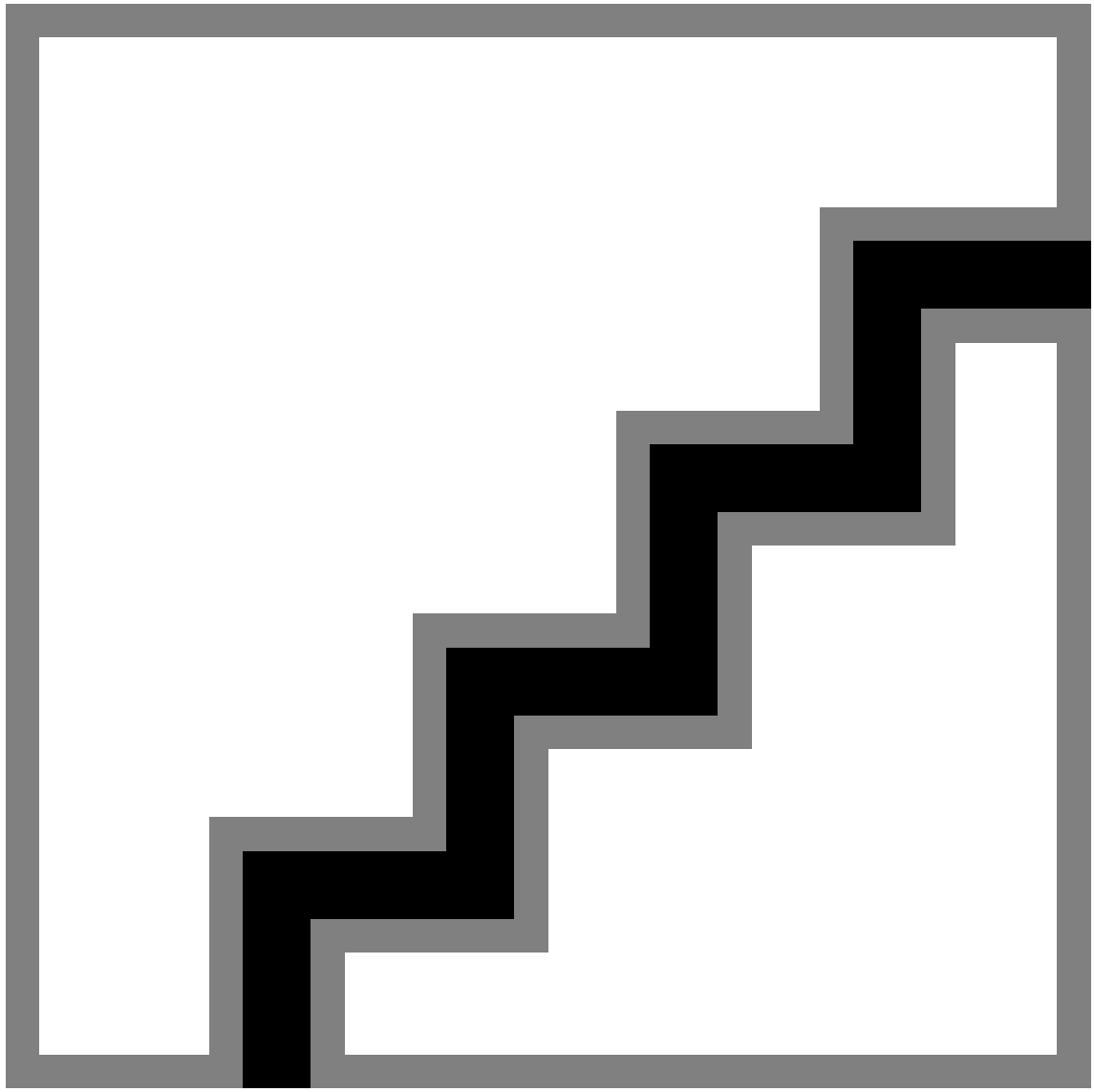


Figure 7-5 Wi-Fi Settings

3. Enable the Wi-Fi function.
4. Configure the Wi-Fi parameters.
   - Select a Wi-Fi from the list, and enter the Wi-Fi's password. Tap **OK**.
   - If the target Wi-Fi is not in the list,tap **Add Wi-Fi**. Enter the Wi-Fi's name and password. And tap **OK**.

Note

Only digits, letters, and special characters are allowed in the password.

5. Set the Wi-Fi's parameters.
   - By default, DHCP is enable. The system will allocate the IP address, the subnet mask, and the gateway automatically.

- If disable DHCP, you should enter the IP address, the subnet mask, and the gateway manually.

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

7.2.3 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.

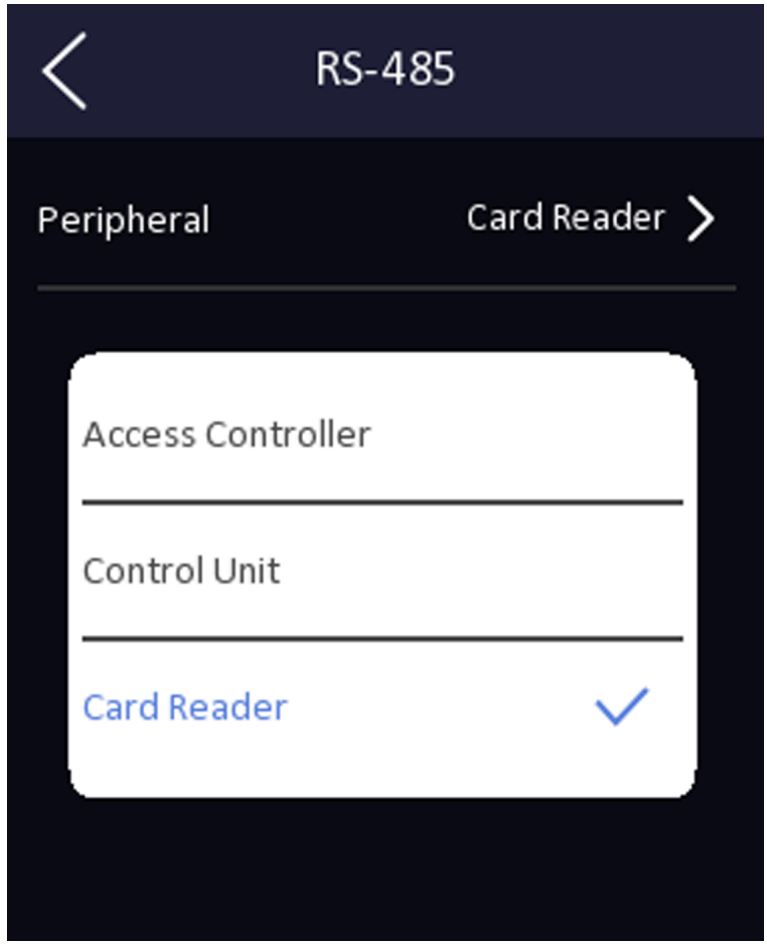


Figure 7-6 Set RS-485 Parameters

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

Note

If you select **Access 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 the back icon at the upper left corner and you should reboot the device if you change the parameters.

7.2.4 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.

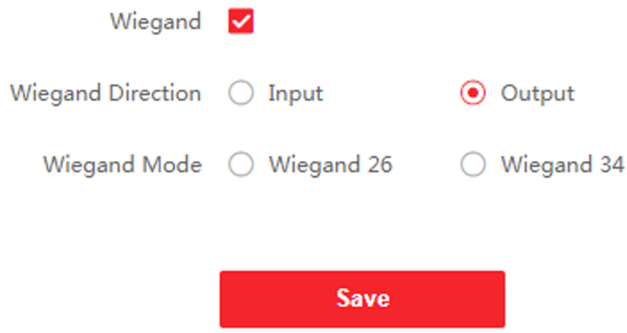


Figure 7-7 Wiegand Settings

3. Enable the Wiegand function.
4. Select a transmission direction.
   - Output: A face recognition terminal can connect an external access controller. And the two devices will transmit the card No. via Wiegand 26 or Wiegand 34.
   - Input: A face recognition terminal can connect a Wiegand card reader.
5. Tap ✓ to save the network parameters.

Note

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

7.3 User Management

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

7.3.1 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, or cards for the administrator.

   Note

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

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.

7.3.2 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 for 3 s and slide to the left/right by following the gesture 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.
   - The suggested user name should be within 32 characters.

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

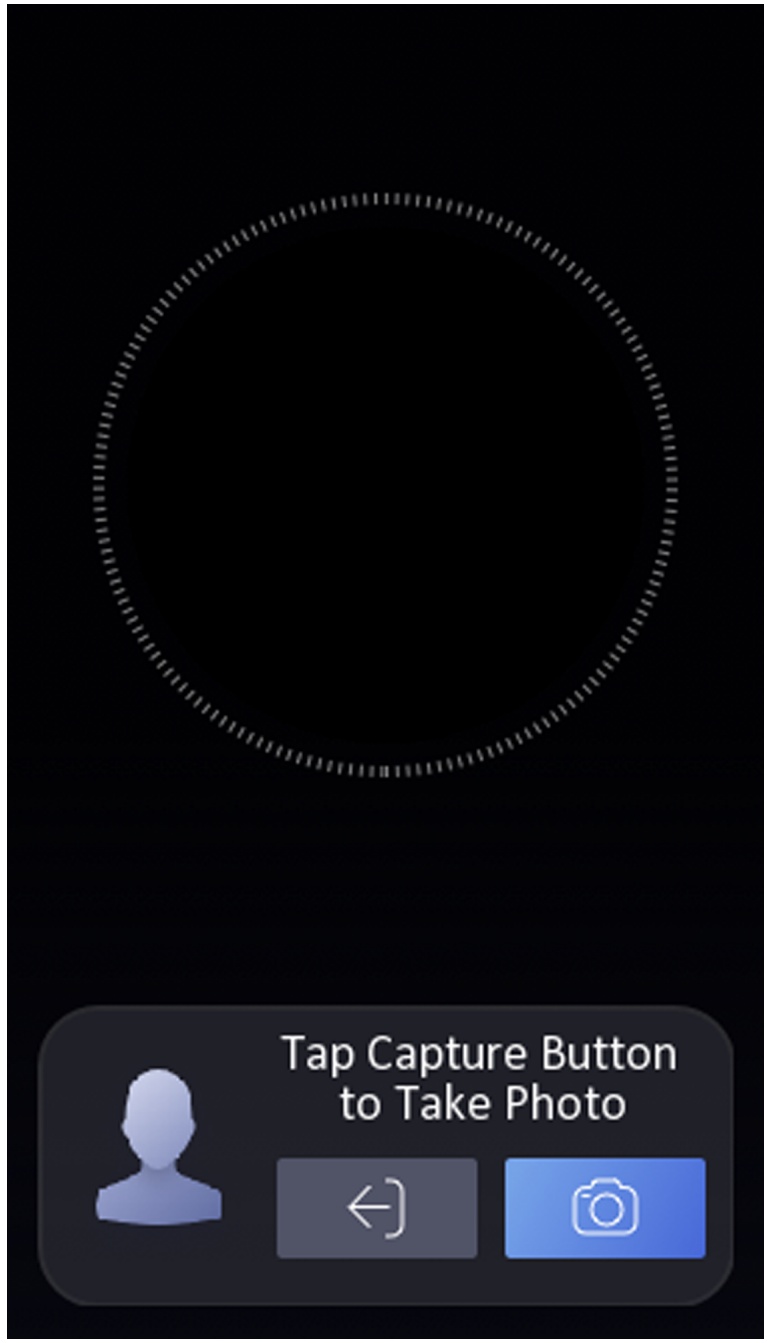


Figure 7-8 Add Face Picture

6. Look 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.
9. Set the user role.

   Administrator

   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.

   Normal User

   The User is the normal user. The user can only authenticate or take attendance on the initial page.
10. Tap ✓ to save the settings.

7.3.3 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 for 3 s and slide to the left/right by following the gesture and log in the backend.
2. Tap **User → +** to enter the Add User page.
3. Connect an external card reader according to the wiring diagram.
4. 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.
5. 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.
   - The suggested user name should be within 32 characters.
6. Tap the Card field and tap **+**.

7. Configure the card No.
   - Enter the card No. manually.
   - Present the card over the card presenting 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.

8. Configure the card type.
9. Set the user role.

   Administrator

   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.

   Normal User

   The User is the normal user. The user can only authenticate or take attendance on the initial page.
10. Tap ✓ to save the settings.

7.3.4 View Password

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

Steps

1. Long tap on the initial page for 3 s and slide to the left/right by following the gesture 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.
- The suggested user name should be within 32 characters.

5. Tap the Password to view the password.

Note

The password cannot be edited. It can only be applied by the platform.

6. Set the user role.

   Administrator

   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.

   Normal User

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

7. Tap ✓ to save the settings.

7.3.5 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 for 3 s and slide to the left/right by following the gesture and log in the backend.
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.

7.3.6 Search and Edit User

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

Search User

On the User Management page, Tap 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.

7.4 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, etc.

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

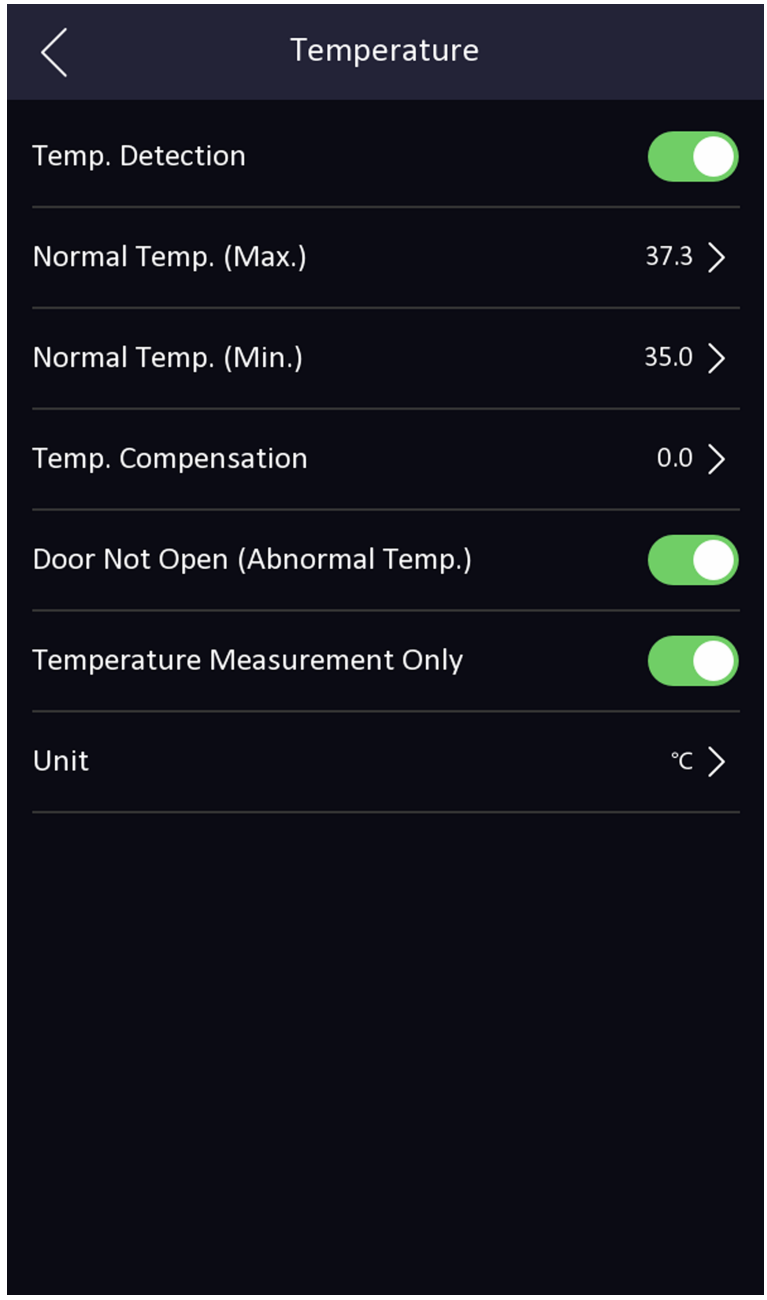


Figure 7-9 Temperature Measurement Parameters

The available parameters descriptions are as follows:

Table 7-1 Temperature Measurement Parameters Descriptions

Parameter	Description
Temp. 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.
Norm Temp. (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°.
Temp. 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 (Abnormal Temp.)	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	Configure the temperature measurement area.

7.5 Data Management

You can delete data, import data, and export data.

7.5.1 Delete Data

Delete user data.

On the Home page, tap **Data → Delete Data → User Data** . All user data added in the device will be deleted.

7.5.2 Import Data

Steps

1. Plug a USB flash drive in the device.

2. On the Home page, tap **Data → Import Data** .
3. Tap **User Data** or **Face Data**.
4. Enter the created password when you exported the data. If you do not create a password when you exported the data, leave a blank in the input box and tap **OK** immediately.

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 folder (named enroll_pic) of the root directory and the picture's name should be follow the rule below:
  Card No._Name_Department_Employee ID_Gender.jpg
- If the folder enroll_pic cannot save all imported pictures, you can create another folders, named enroll_pic1, enroll_pic2, enroll_pic3, enroll_pic4, under the root directory.
- 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.

7.5.3 Export Data

Steps

1. Plug a USB flash drive in the device.
2. On the Home page, tap **Data → Export Data** .
3. Tap **Event Data**, **User Data**, or **Face Data**.
4. **Optional:** Create a password for exporting. When you import those data to another device, you should enter the password.

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.

7.6 Identity Authentication

After network configuration, system parameters configuration and user configuration, you can go back to the initial page for identity authentication. The system will authenticate person according to the configured authentication mode.

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

1:N Matching

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

1: 1 Matching

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

7.6.1 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.
- The dimension of the recognized QR code picture should be larger than 6 cm × 6 cm.

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

7.6.2 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. The dimension of the recognized QR code picture should be larger than 6 cm × 6 cm.

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.

7.7 Basic Settings

You can set the shortcut key, voice, time, language, supplement light, community No., building No., Unit No., beauty, and advertisement.

Long tap on the initial page for 3 s and slide to the left/right by following the gesture and login the device home page. Tap **Basic**.

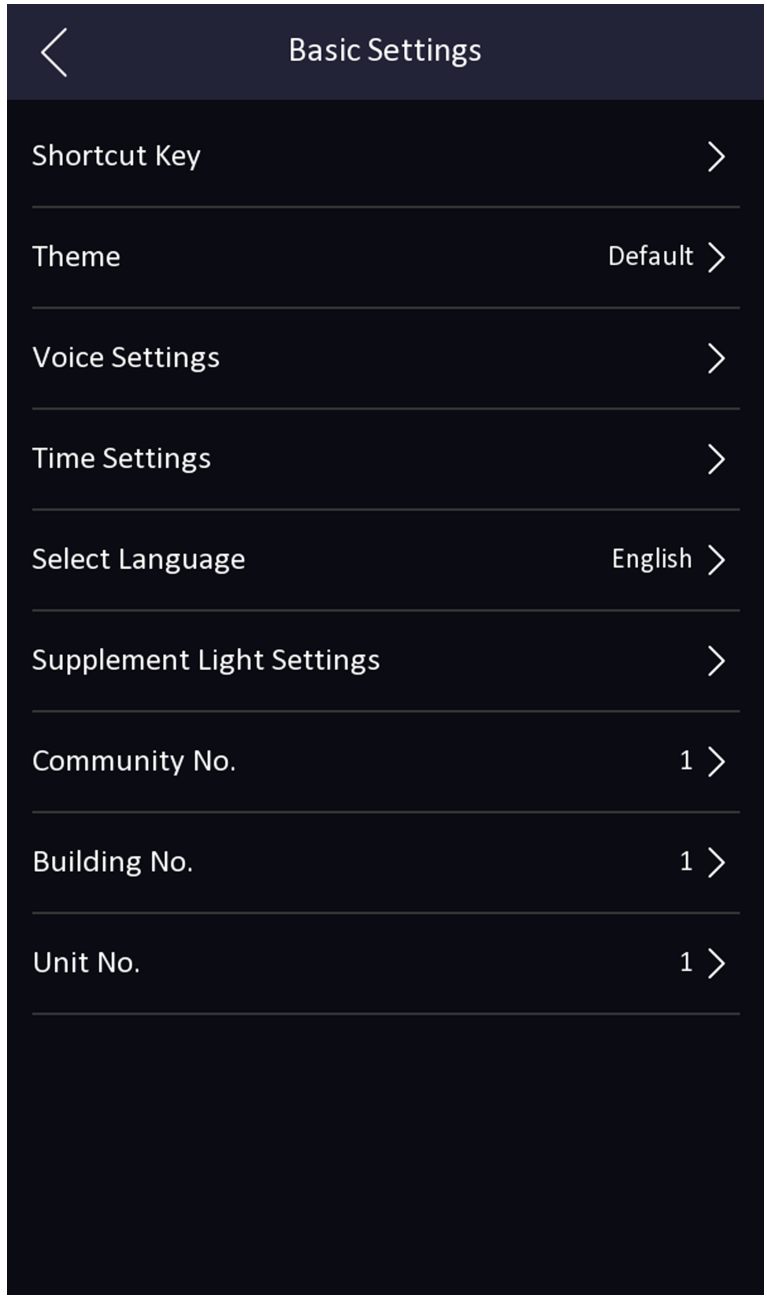


Figure 7-10 Basic Settings Page

shortcut key, voice, time, language, supplement light, community No., building No., and Unit No.

Shortcut Key

Choose the shortcut key that displayed on the authentication page, including the QR code function, the call function, call type, and the password entering function.

Note

- If the combination authentication of face and QR code is supported, and the QR code shortcut key is disabled (there is no QR code shortcut key icon in the authentication page), you can scan the QR code in the middle of the authentication page to authenticate.
- You can select call type from **Call Room**, **Call Center**, and **Call Specified Room No.**

  Call Room

  When you tap the call button on the authentication page, you should dial a room No. to call.

  Call Center

  When you tap the call button on the authentication page, you can call the center directly.

  Call Specified Room No.

  You should set a room No. When you tap the call button on the authentication page, you can call the configured room directly without dialing.

Theme

You can set the theme of the prompt window on the authentication page. You can select **Theme** as **Default**/**Simple**. If select **Simple**, the live view of the authentication page will be disabled, and in the meanwhile, the person's name, employee ID, face pictures will all be hidden.

Voice Settings

You can enable/disable the voice prompt function and adjust the voice volume.

Note

You can set the voice volume between 0 and 10.

Time Settings

Set the time zone, the device time and the DST.

Select Language

Select the language according to actual needs.

Supplement Light Settings

Tap **White Light** and you can set the supplement light mode. You can select to enable or disable the supplement light, or customize the supplement light's brightness, start time, and end time.

Community No.

Set the device installed community No.

Building No.

Set the device installed building No.

Unit No.

Set the device installed unit No.

7.8 Set Biometric Parameters

You can customize the face parameters to improve the face recognition performance. The configurable parameters includes application mode, face liveness level, face recognition distance, face recognition interval, wide dynamic, face 1:N security level, face 1:1 security level, ECO settings, and face with mask detection.

Long tap on the initial page for 3 s and login the home page. Tap **Biometric**.

Table 7-2 Face Picture Parameters

Parameter	Description
Application Mode	Select either others or indoor according to actual environment.
Face Liveness Level	After enabling face anti-spoofing function, you can set the matching security level when performing live face authentication.
Face Recognition Distance	Set the valid distance between the user and the camera when authenticating.
Face Recognition Interval	The time interval between two continuous face recognitions when authenticating. **Note** You can input the number from 1 to 10.
Wide Dynamic	It is suggested to enable the WDR function if installing the device outdoors. When there are both very bright and very dark areas simultaneously in the view, you can enable the WDR function to balance the brightness of the whole image and provide clear images with details.
Face 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.
Face 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.
ECO Settings	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 the ECO mode threshold, ECO mode (1:N), and ECO mode (1:1). **ECO Threshold**

Parameter	Description
	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. **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
Face with Mask Detection	After enabling the face with mask detection, the system will recognize the captured face with mask picture. You can set face with mask & face 1:N level and the strategy. **Reminder of Wearing** If the person do not wear a face mask when authenticating, the device prompts a notification and the door will open. **Must Wear** If the person do not wear a face mask when authenticating, the device prompts a notification and the door keeps closed.

7.9 Set Access Control Parameters

You can set the access control permissions, including the functions of authentication mode, enable NFC card, door contact, and door open time.

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

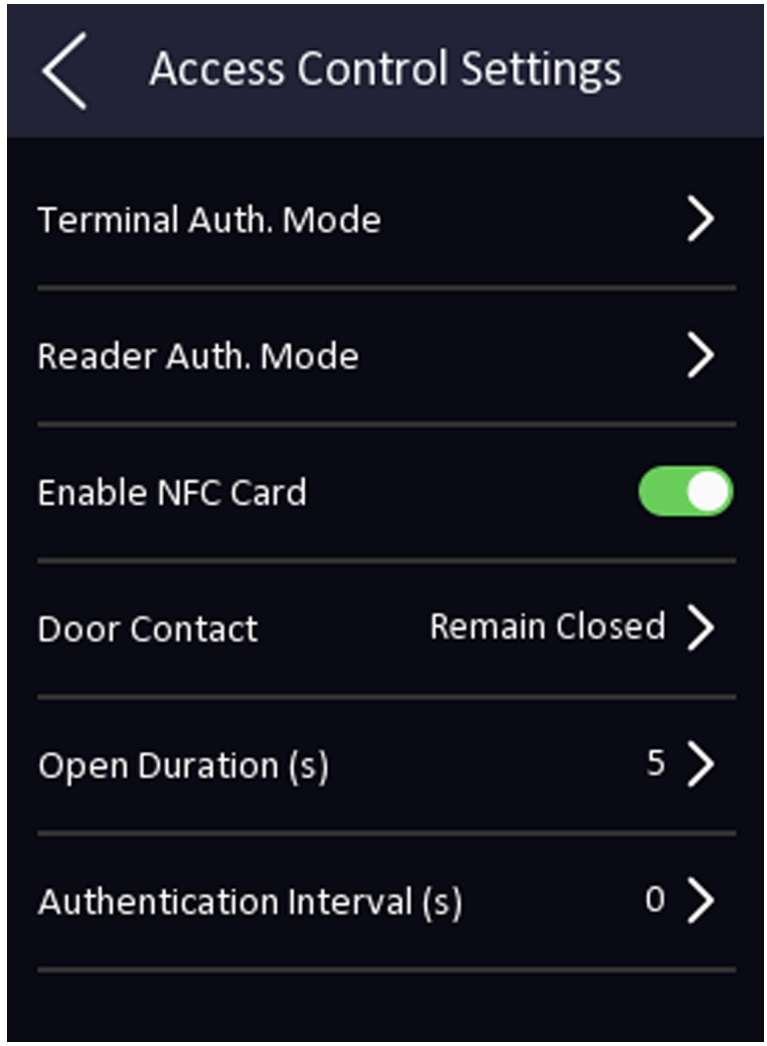


Figure 7-12 Access Control Parameters

The available parameters descriptions are as follows:

Table 7-3 Access Control Parameters Descriptions

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

Parameter	Description
	Note • Biometric recognition products are not completely 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 (Card Reader Authentication Mode)	Select the card reader's authentication mode.
Enable NFC Card	Enable the function and you can present the NFC card to authenticate.
Door Contact	You can select "Open (Remain Open)" or "Close (Remian Closed)" according to your actual needs. By default, it is Close (Remian Closed).
Open Duration	Set the door unlocking duration. If the door is not opened for the set time, the door will be locked. Available door locked time range: 1 to 255s.
Authentication Interval	Set the device authenticating interval. Available authentication interval range: 0 to 65535.

7.10 Time and Attendance Status Settings

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

Note

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

7.10.1 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.

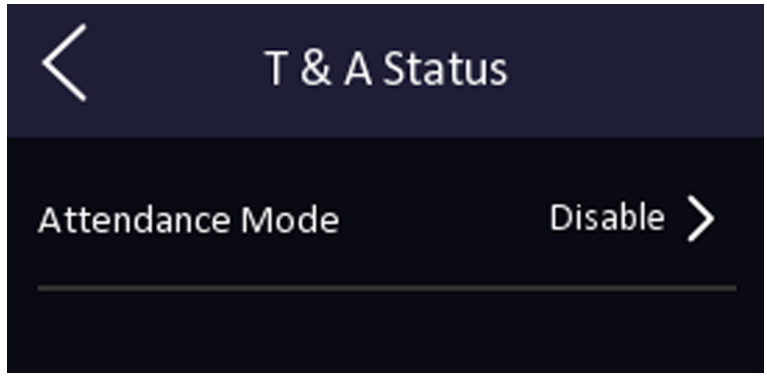


Figure 7-13 Disable Attendance Mode

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

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

7.10.2 Set Manual Attendance via Device

Set the attendance mode as manual, and you should 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**.

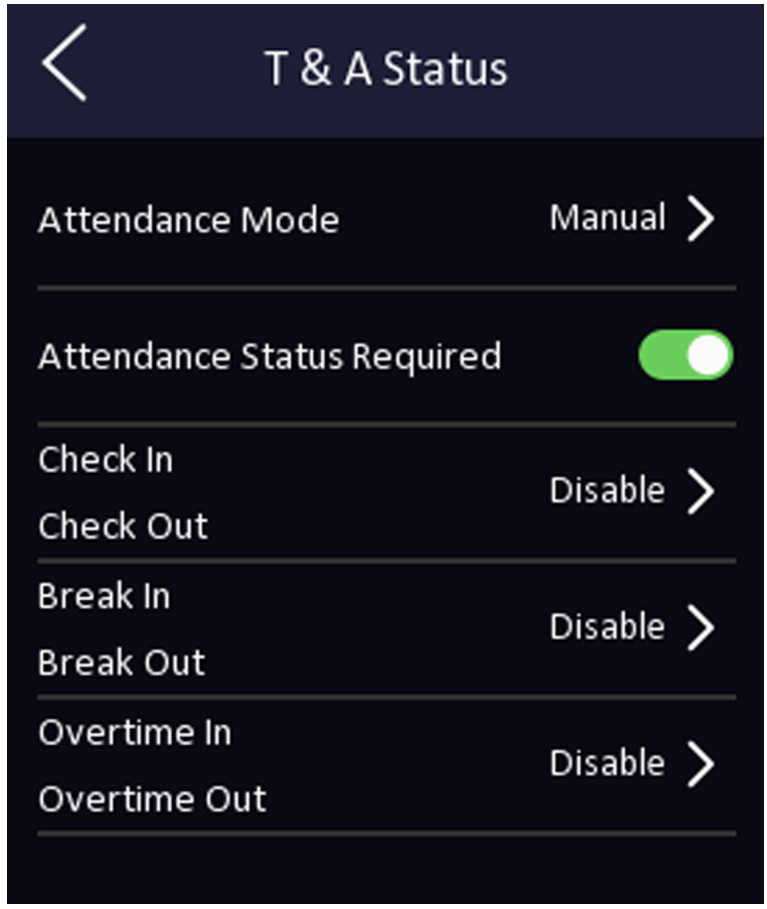


Figure 7-14 Manual Attendance Mode

3. Enable the **Attendance Status Required**.
4. Enable a group of attendance status.

Note

The Attendance Property will not be changed.

5. **Optional:** Select an status and change its name if required.

   The name will be displayed on the T & A Status page and the authentication result page.

Result

You should select an 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.

7.10.3 Set Auto Attendance via Device

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

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**.

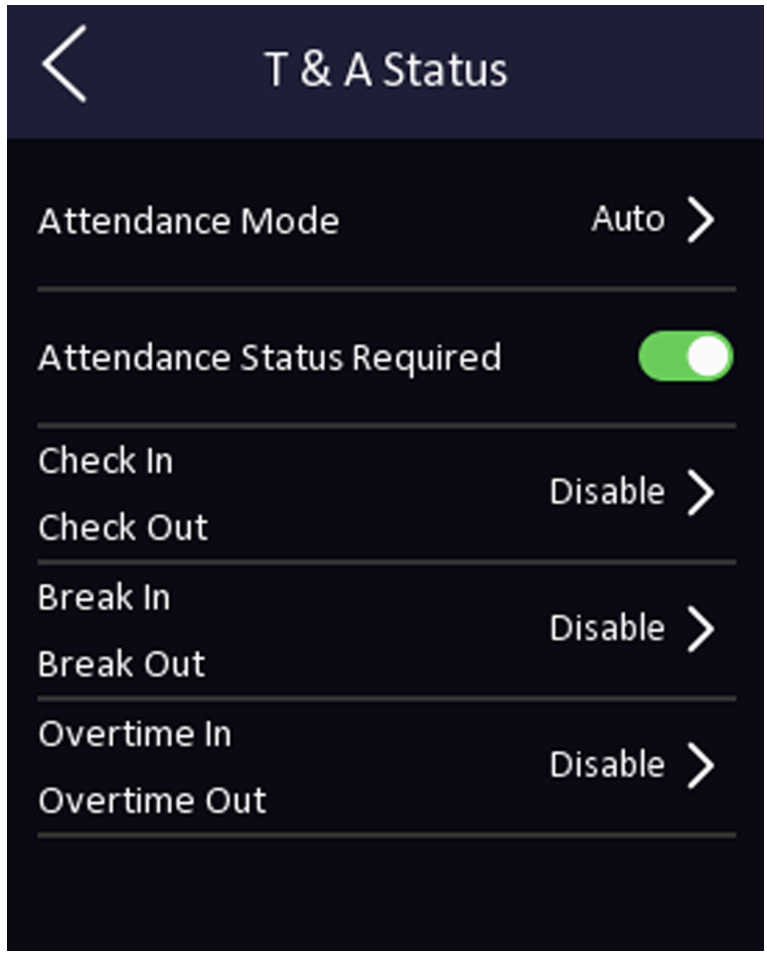


Figure 7-15 Auto Attendance Mode

3. Enable the **Attendance Status** function.
4. Enable a group of attendance status.

Note

The Attendance Property will not be changed.

5. **Optional:** Select an status and change its name if required.

   The name will be displayed on the T & A Status page and the authentication result page.
6. Set the status' schedule.
   1) Tap **Attendance Schedule**.
   2) Select **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday**, or **Sunday**.
   3) Set the selected attendance status's start time of the day.
   4) Tap **Confirm**.
   5) Repeat step 1 to 4 according to your actual needs.

Note

The attendance status will be valid within the configured schedule.

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

7.10.4 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 schedule. 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**.

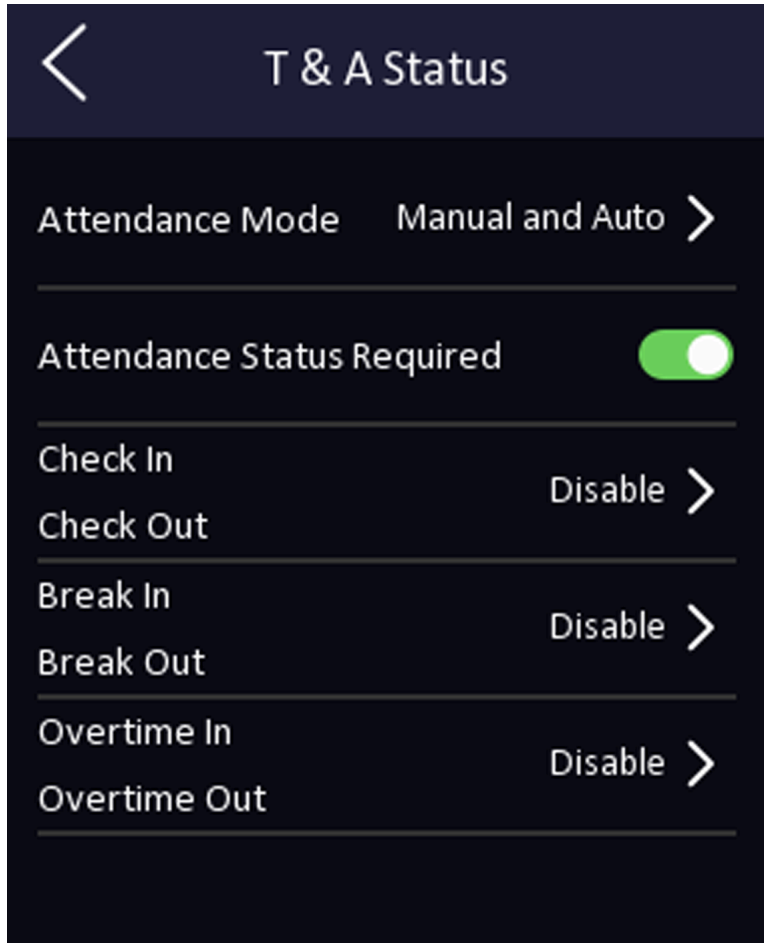


Figure 7-16 Manual and Auto Mode

3. Enable the **Attendance Status** function.
4. Enable a group of attendance status.

Note

The Attendance Property will not be changed.

5. **Optional:** Select an status and change its name if required.

   The name will be displayed on the T & A Status page and the authentication result page.
6. Set the status' schedule.
   1) Tap **Attendance Schedule**.
   2) Select **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday**, or **Sunday**.
   3) Set the selected attendance status's start time of the day.
   4) Tap **OK**.
   5) Repeat step 1 to 4 according to your actual needs.

Note

The attendance status will be valid within the configured schedule.

Result

On the initial page and authenticate. The authentication will be marked as the configured attendance status according to the schedule. If you tap the edit icon on the result tab, you can select a status to take attendance manually, the authentication will be marked as the edited attendance status.

Example

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

7.11 System Maintenance

You can view the system information and the capacity. You can also upgrade the device, restore to factory settings, restore to default settings, and reboot the device.

Long tap on the initial page for 3 s and slide to the left/right by following the gesture and login the home page. Tap **Maint.**.

Hold the **?** on the upper-right corner of the page and enter the password to view the version of the device.

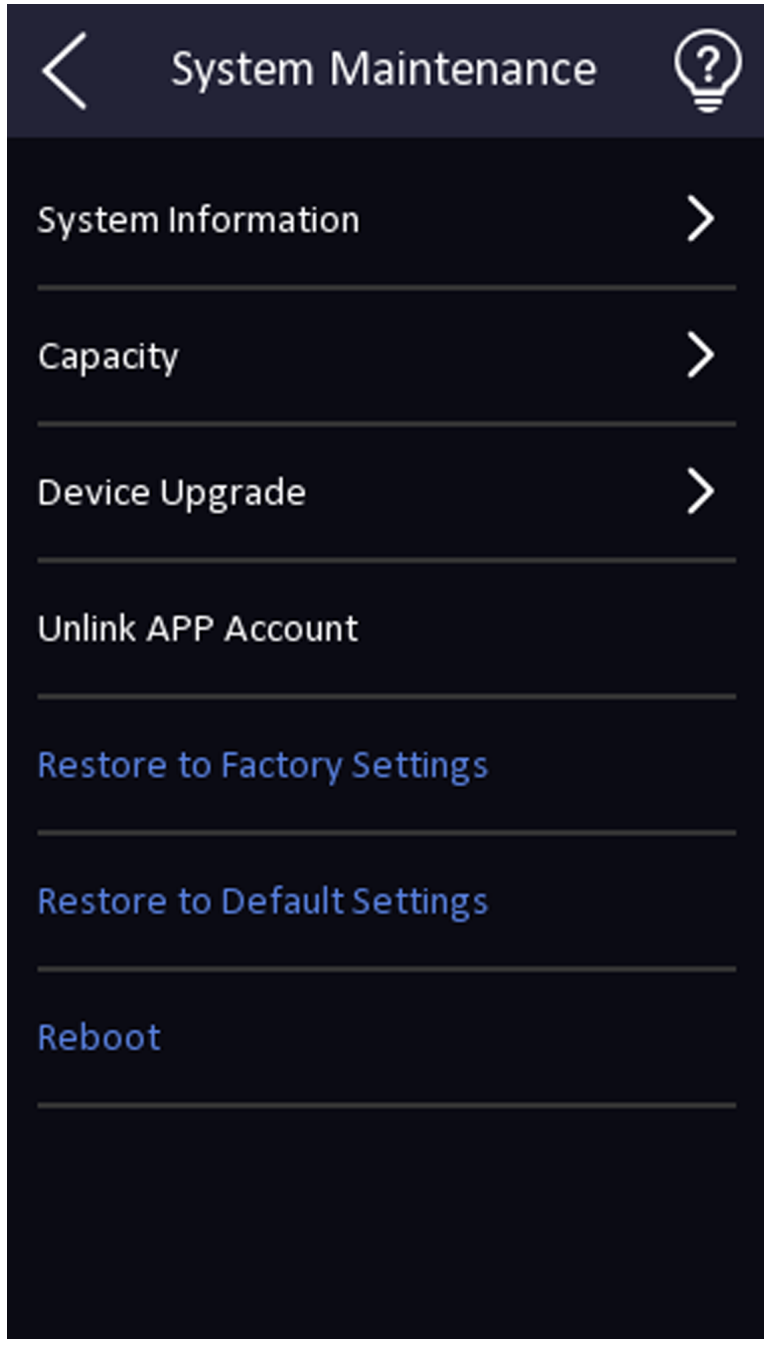


Figure 7-17 Maintenance Page

System Information

You can view the device model, serial No., versions, address, production data, QR code, and open source code license.

Note

The page may vary according to different device models. Refers to the actual page for details.

Capacity

You can view the number of, user, face picture, card, and event.

Device Upgrade

Plug the USB flash drive in the device USB interface. Tap **Upgrade**, and the device will read the *digicap.dav* file in the USB flash drive to start upgrading.

Unlink APP Account

After unlinking APP account, you cannot operate via APP.

Restore to Default Settings

All parameters, except for the communication settings, remotely imported user information, will be restored to the default settings. The system will reboot to take effect.

Restore to Factory Settings

All parameters will be restored to the factory settings. The system will reboot to take effect.

Reboot

Reboot the device.

7.12 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.

7.12.1 Call Client Software from Device

Steps

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

   Note

   For details about adding device, see *Add Device*.
5. Call the client software.
   1) Tap on the device initial page.
   2) Enter ***0*** in the pop-up window.
   3) Tap 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.

7.12.2 Call Center 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. Call the center.
   - If you have configured to call center in the ***Basic Settings*** , you can tap to call the center.
   - If you have not configured to call center in the ***Basic Settings*** , you should tap → to call the center
7. Answers the call via the main station and starts two-way audio.

Note

The device will call the main station in priority.

7.12.3 Call Device from Client Software

Steps

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

Note

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

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

Note

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

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

7.12.4 Call Room 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. Call the room.
   - If you have configured a specified room No. in the ***Basic Settings*** , you can tap to call the room.
   - If you have not configured a specified room No. in the ***Basic Settings*** , you should tap on the authentication page of the device. Enter the room No. on the dial page and tap to call the room.
7. After the indoor station answers the call, you can start two-way audio with the indoor station.

7.12.5 Call Mobile Client from Device

Steps

1. Get the mobile mobile client from the supplied disk or the official website, and install the software according to the prompts.
2. Run the mobile client and add the device to the mobile client.

Note

For details, see the user manual of the mobile client.

3. Enter **Basic Settings → Shortcut Key** and enable **Call APP**.
4. Go back to the initial page and call the mobile client.

1) Tap on the device initial page.
2) Tap to call the mobile client.

Chapter 8 Operation via Web Browser

8.1 Login

You can login via the web browser or the remote configuration of the client software.

Note

Make sure the device is activated. For detailed information about activation, see ***Activation*** .

Login via Web Browser

Enter the device IP address in the address bar of the web browser and press **Enter** to enter the login page.

Note

Make sure that the IP address starts with "Https:".

Enter the device user name and the password. Click **Login**.

Login via Remote Configuration of Client Software

Download and open the client software. After adding the device, click to enter the Configuration page.

8.2 Live View

You can view the live video of the device.

After logging in, you will enter the live view page. You can perform the live view, capture, video recording, and other operations.

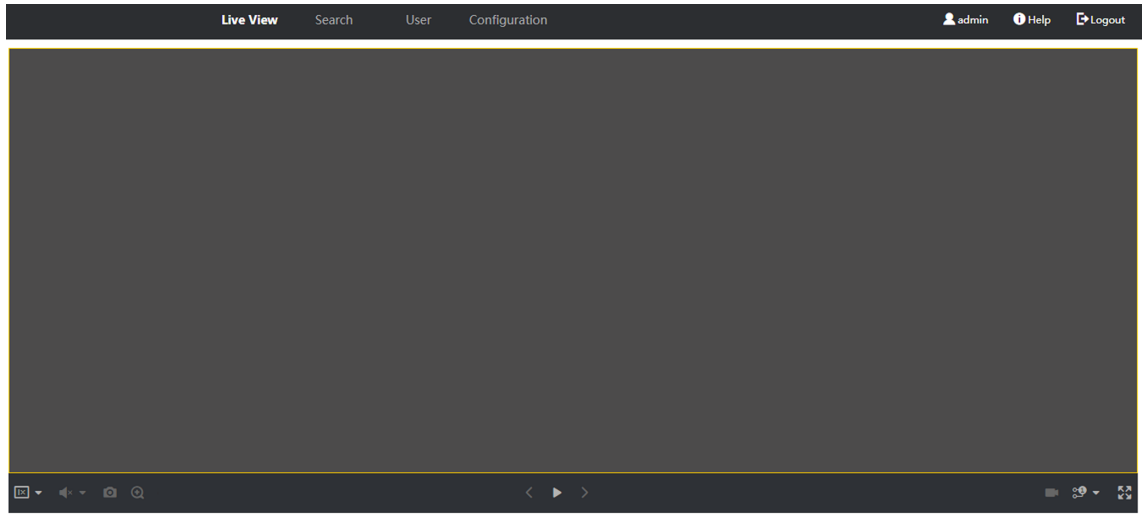


Figure 8-1 Live View Page

Function Descriptions:

Select the image size when starting live view.

Set the volume when starting live view.

Note

If you adjust the volume when starting two-way audio, you may hear a repeated sounds.

You can capture image when starting live view.

Reserved function. You can zoom in the live view image.

Start or stop live view.

Start or stop video recording.

Select the streaming type when starting live view. You can select from the main stream and the sub stream.

Full screen view.

8.3 Person Management

Click and add the person's information, including the basic information, card, authentication mode, and the picture.

Click **OK** to save the person.

Add Basic Information

Click **User → Add** to enter the Add Person page.
Add the person's basic information, including the employee ID, the person's name, user level, floor No., and room No.
Click **OK** to save the settings.

Add Card

Click **User → Add** to enter the Add Person page.
Click **Add Card** and enter a card number.
Click **OK** to save the settings.

Add Face Picture

Click **User → Add** to enter the Add Person page.
Click **+** on the right to upload a face picture from the local PC.

Note

The picture format should be JPG, JPEG or PNG. The size should be less than 200K.

Click **OK** to save the settings.

Set Permission Time

Click **User → Add** to enter the Add Person page.
Set **Start Time** and **End Time**.
Click **OK** to save the settings.

Set Access Control

Click **User → Add** to enter the Add Person page.
After check **Adminstrator** in **Access Control**, the added person can log in by authenticating face.
Click **OK** to save the settings.

Add Authentication Mode

Click **User → Add** to enter the Add Person page.
Set the authentication type.
Click **OK** to save the settings.

8.4 Search Event

Click **Search** to enter the Search page.

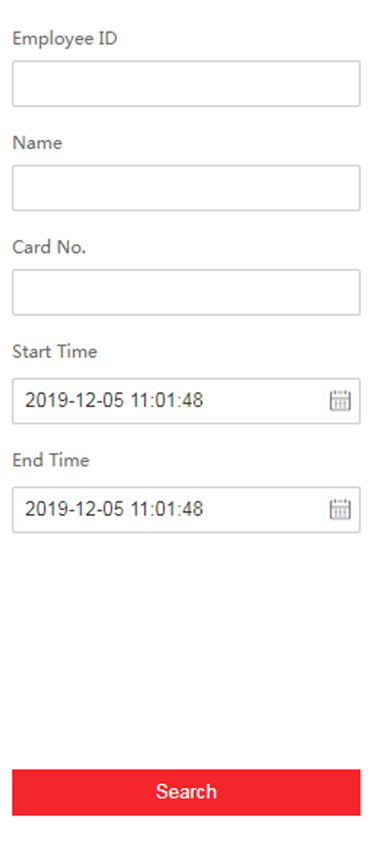


Figure 8-2 Search Page

Enter the search conditions, including the employee ID, the name, the card No., the start time, and the end time, and click **Search**.

The results will be displayed on the right panel.

8.5 Configuration

8.5.1 Set Local Parameters

Set the live view parameters, record file saving path, and captured pictures saving path.

Set Live View Parameters

Click **Configuration → Local** to enter the Local page. Configure the stream type, the play performance, auto start live view, and the image format and click **Save**.

Set Record File Saving Path

Click **Configuration → Local** to enter the Local page. Select a record file size and select a saving path from your local computer and click **Save**.
You can also click **Open** to open the file folder to view details.

Set Captured Pictures Saving Path

Click **Configuration → Local** to enter the Local page. Select a saving path from your local computer and click **Save**.
You can also click **Open** to open the file folder to view details.

8.5.2 View Device Information

View the device name, language, model, serial No., QR code, version, number of channels, alarm input, alarm output, lock and RS-485, device capacity, etc.

Click **Configuration → System → System Settings → Basic Information** to enter the configuration page.

You can view the device name, language, model, serial No., QR code, version, number of channels, alarm input, alarm output, lock and RS-485, device capacity, etc.

8.5.3 Set Time

Set the device's time zone, synchronization mode, and the device time.

Click **Configuration → System → System Settings → Time Settings** .

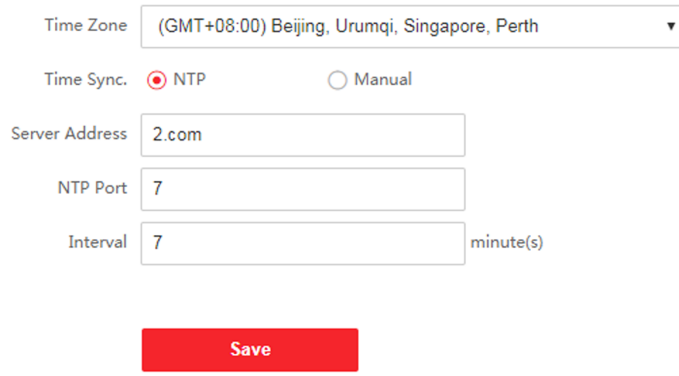


Figure 8-3 Time Settings

Click **Save** to save the settings after the configuration.

Time Zone

Select the device located time zone from the drop-down list.

Time Sync.

NTP

You should set the NTP server's IP address, port No., and interval.

Manual

By default, the device time should be synchronized manually. You can set the device time manually or check **Sync. with Computer Time** to synchronize the device time with the computer's time.

8.5.4 Set DST

Steps

1. Click **Configuration → System → System Settings → DST** .

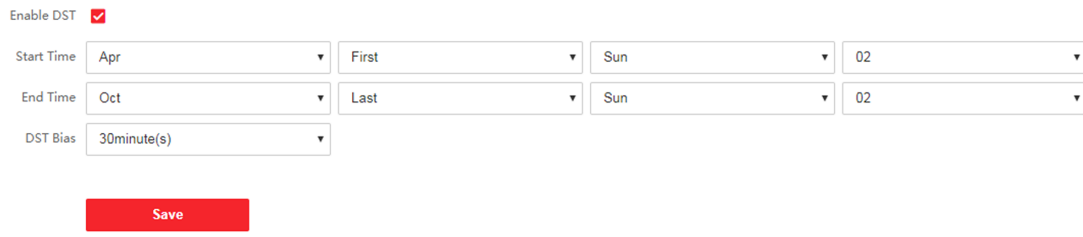


Figure 8-4 DST Page

2. Check **Enable DST**.
3. Set the DST start time, end time and bias time.

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

8.5.5 View Open Source Software License

Go to **Configuration → System → System Settings → About Device** , and click **View Licenses** to view the device license.

8.5.6 Upgrade and Maintenance

Reboot device, restore device parameters, and upgrade device version.

Reboot Device

Click **Configuration → System → Maintenance → Upgrade & Maintenance** .

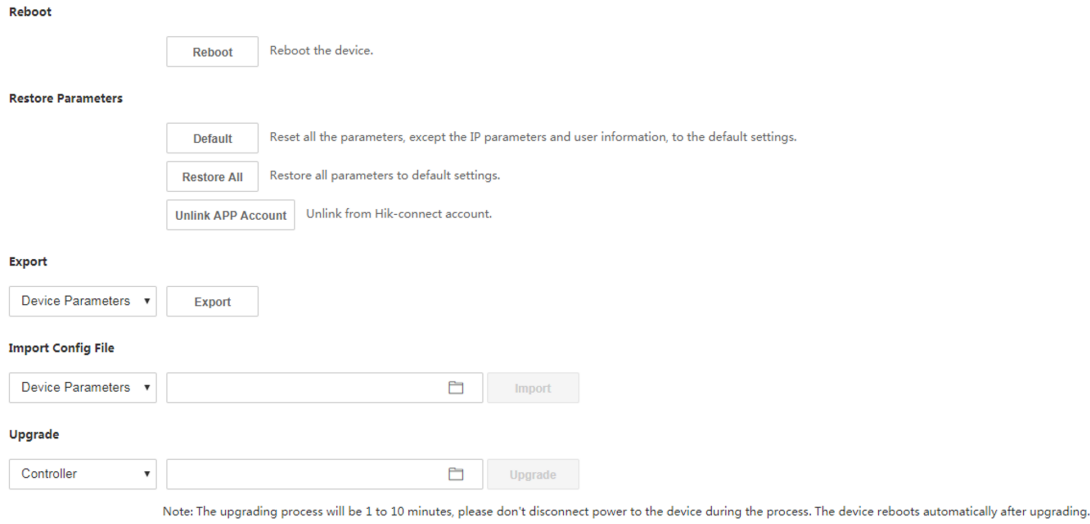


Figure 8-5 Upgrade and Maintenance Page

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

Restore Parameters

Click **Configuration → System → Maintenance → Upgrade & Maintenance** .

Restore All

All parameters will be restored to the factory settings. You should activate the device before usage.

Default

The device will restore to the default settings, except for the device IP address and the user information.

Unlink APP Account

Unlink the Hik-Connect account from the platform.

Import and Export Parameters

Click **Configuration → System → Maintenance → Upgrade & Maintenance** .

Export

Click **Export** to export the logs or device parameters.

Note

You can import the exported device parameters to another device.

Import

Click and select the file to import. Click **Import** to start import configuration file.

Upgrade

Click **Configuration → System → Maintenance → Upgrade & Maintenance** .
Select an upgrade type from the drop-down list. Click and select the upgrade file from your local PC. Click **Upgrade** to start upgrading.

Note

Do not power off during the upgrading.

8.5.7 Log Query

You can search and view the device logs.

Go to **Configuration → System → Maintenance → Log Query** .

Set the major and minor type of the log type. Set the start time and end time for searching, and click **Search**.

The results will be displayed below, which including the No., time, the major type the minor type, the channel No., the local/remote user information, the remote host IP, etc.

8.5.8 Security Mode Settings

Set the security mode for logging in the client software.

On the Device for Management page, click **Configuration → System → Security → Security Service** .

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

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.

Enable SSH

To raise network security, disable SSH service. The configuration is only used to debug the device for the professionals.

Enable HTTP

In order to increase the network security level when visiting websites, you can enable HTTP to acquire a more secure and encrypted network communication environment. The communication should authenticated by identity and encryption password after enabling HTTP, which is save.

8.5.9 Certificate Management

It helps to manage the server/client certificates and CA certificate.

Note

The function is only supported by certain device models.

Create and Install Self-signed Certificate

Steps

1. Go to **Configuration → System → Security → Certificate Management** .
2. In the **Certificate Files** area, select a **Certificate Type** from the drop-down list.
3. Click **Create**.
4. Input certificate information.
5. Click **OK** to save and install the certificate.

   The created certificate is displayed in the **Certificate Details** area.

   The certificate will be saved automatically.
6. Download the certificate and save it to an asking file in the local computer.
7. Send the asking file to a certification authority for signature.
8. Import the signed certificate.
   1) Select a certificate type in the **Import Passwords** area, and select a certificate from the local, and click **Install**.
   2) Select a certificate type in the **Import Communication Certificate** area, and select a certificate from the local, and click **Install**.

Install Other Authorized Certificate

If you already has an authorized certificate (not created by the device), you can import it to the device directly.

Steps

1. Go to **Configuration → System → Security → Certificate Management** .
2. In the **Import Passwords** and **Import Communication Certificate** areas, select certificate type and upload certificate.
3. Click **Install**.

Install CA Certificate

Before You Start

Prepare a CA certificate in advance.

Steps

1. Go to **Configuration → System → Security → Certificate Management** .
2. Create an ID in the **Inport CA Certificate** area.

   Note

   The input certificate ID cannot be the same as the existing ones.

3. Upload a certificate file from the local.
4. Click **Install**.

8.5.10 Change Administrator's Password

Steps

1. Click **Configuration → User Management** .
2. Click .
3. Enter the old password and create a new password.
4. Confirm the new password.
5. Click **OK**.

   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.

8.5.11 View Device Arming/Disarming Information

View device arming type and arming IP address.

Go to **Configuration → Arming/Disarming Information** .

You can view the device arming/disarming information. Click **Refresh** to refresh the page.

8.5.12 Network Settings

Set TCP/IP, port, Wi-Fi, report strategy, platform access and HTTP listening.

Set Basic Network Parameters

Click **Configuration → Network → Basic Settings → TCP/IP** .

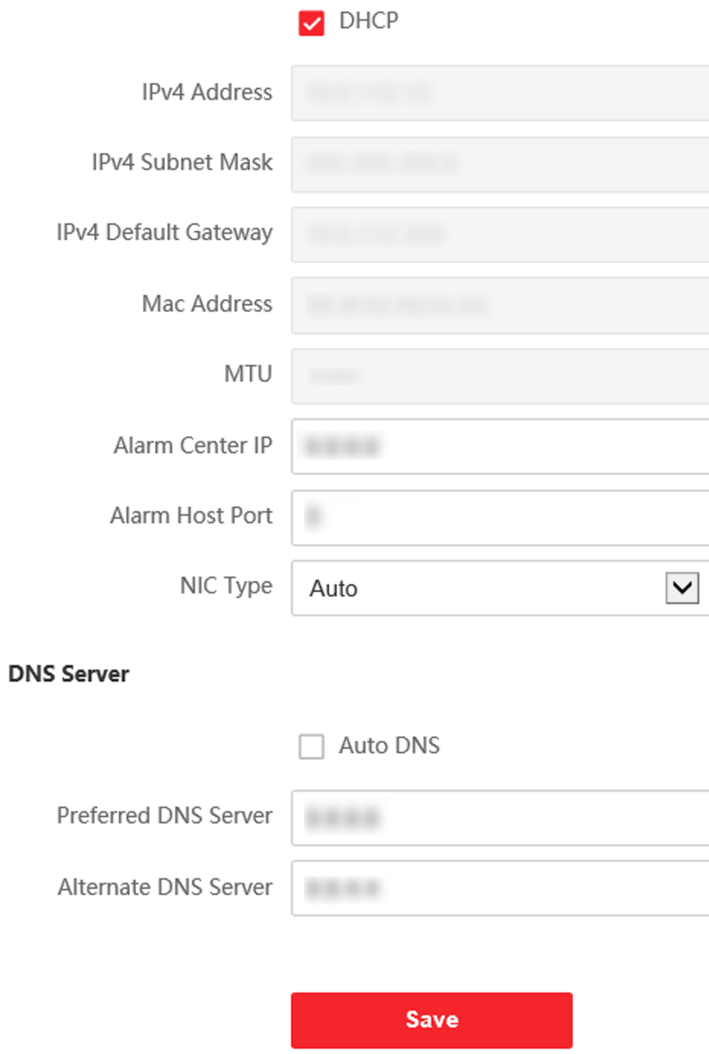


Figure 8-6 TCP/IP Settings Page

Set the parameters and click **Save** to save the settings.

DHCP

If uncheck the function, you should set the IPv4 address, IPv4 subnet mask, IPv4 default gateway, MTU, and the device port.

If you check the function, the system will allocate the IPv4 address, IPv4 subnet mask, and the IPv4 default gateway automatically.

NIC Type

Select a NIC type from the drop-down list. By default, it is **Auto**.

DNS Server

Set the preferred DNS server and the Alternate DNS server according to your actual need.

Set Port Parameters

Set the HTTP, RTSP, HTTPS and Server port parmaeters.

Click **Configuration → Network → Basic Settings → Port** .

HTTP

It refers to the port through which the browser accesses the device. For example, when the HTTP Port is modified to 81, you need to enter ***http://192.0.0.65:81*** in the browser for login.

RTSP

It refers to the port of real-time streaming protocol.

HTTPS

Set the HTTPS for accessing the browser. Certificate is required when accessing.

Server

It refers to the port through which the client adds the device.

Set Wi-Fi Parameters

Set the Wi-Fi parameters for device wireless connection.

Steps

Note

The function should be supported by the device.

1. Click **Configuration → Network → Basic Settings → Wi-Fi** .

Figure 8-7 Wi-Fi Settings Page

2. Check **Wi-Fi**.

3. Select a Wi-Fi
   - Click 🔗 of a Wi-Fi in the list and enter the Wi-Fi password.
   - Click **Add** and enter a Wi-Fi's name, password, and encryption type. Click **Connect**. When the Wi-Fi is connected, click **OK**.
4. **Optional:** Set the WLAN parameters.
   1) Click **TCP/IP Settings**.
   2) Set the IP address, subnet mask, and default gateway. Or check **Enable DHCP** and the system will allocate the IP address, subnet mask, and default gateway automatically.
5. Click **Save**.

Report Strategy Settings

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

Go to **Configuration → Network → Basic Settings → Report Strategy** .

You can set the center group and the system will transfer logs via ISUP 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.

Platform Access

Platform access provides you an option to manage the devices via platform.

Steps

1. Click **Configuration → Network → Advanced → Platform Access** to enter the settings page.
2. Check the checkbox of **Enable** to enable the function.
3. Select the **Platform Access Mode**.

   Note

   Hik-Connect is an application for mobile devices. With the App, you can view live image of the device, receive alarm notification and so on.
4. Create a **Stream Encryption/Encryption Key** for the device.

   Note

   6 to 12 letters (a to z, A to Z) or numbers (0 to 9), case sensitive. You are recommended to use a combination of no less than 8 letters or numbers.

5. Click **Save** to enable the settings.

Set ISUP Parameters

Set the ISUP parameters for accessing device via ISUP protocol.

Steps

Note

The function should be supported by the device.

1. Click **Configuration → Network → Advanced Settings → Platform** .
2. Select **ISUP** from the platform access mode drop-down list.
3. Check **Enable**.
4. Set the ISUP version, server address, device ID, and the ISUP status.

   Note

   If you select 5.0 as the version, you should set the ISUP key as well.
5. Click **Save**.

Configure HTTP Listening

The device can send alarm information to the destination IP or host via HTTP protocol/HTTPS protocol.

Before You Start

The destination IP or host name should support the HTTP protocol/HTTPS protocol to receive the alarm information.

Note

The function should be supported by the device.

Steps

1. Click **Configuration → Network → Advanced → HTTP Listening** .
2. Edit the destination IP or host name, URL and port.
3. **Optional:** Click **Test** to test whether the entered IP address or host name are valid.
4. **Optional:** Click **Default** to reset the destination IP or host name.
5. Click **Save**.

8.5.13 Set Video and Audio Parameters

Set the image quality, resolution, and the device volume.

Set Video Parameters

Click **Configuration → Video/Audio → Video** .

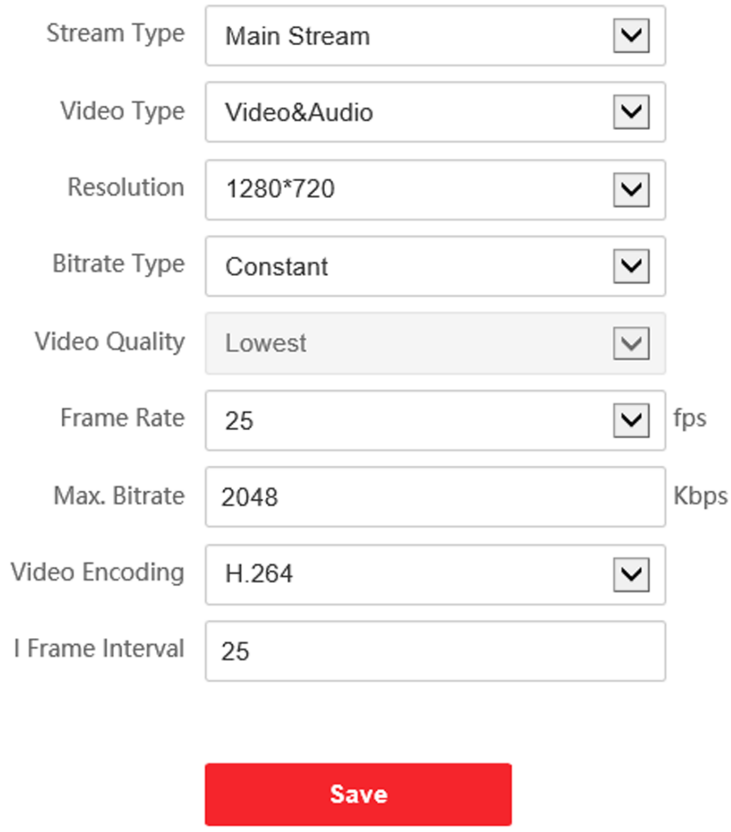


Figure 8-8 Video Settings Page

Set the stream type, the video type, the bitrate type, the frame rate, the Max. bitrate, and the video encoding.
Click **Save** to save the settings after the configuration.

Set Audio Parameters

Click **Configuration → Video/Audio → Audio** .
Set the audio stream type and audio encoding.
Drag the slider to adjust the device input and output volume.
You can also enable voice prompt.
Click **Save** to save the settings after the configuration.

Note

The functions vary according to different models. Refers to the actual device for details.

8.5.14 Customize Audio Content

Customize the output audio content when authentication succeeded and failed.

Steps

1. Click **Configuration → Video/Audio → Audio Prompt** .

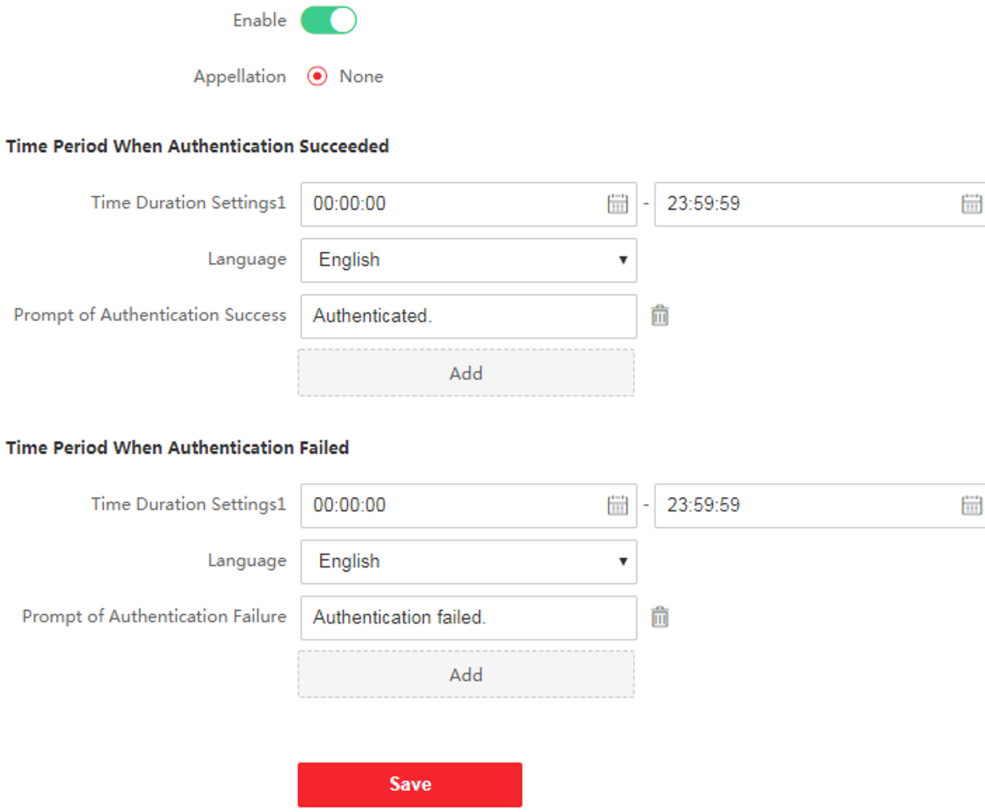


Figure 8-9 Customize Audio Content

2. set the appellation.
3. Enable the function.
4. Set the time duration when authentication succeeded.
   1) Click **Add**.
   2) Set the time duration and the language.

   Note

   If authentication is succeeded in the configured time duration, the device will broadcast the configured content.

   3) Enter the audio content.
   4) **Optional:** Repeat substep 1 to 3.
   5) **Optional:** Click 🗑 to delete the configured time duration.
5. Set the time duration when authentication failed.

1) Click **Add**.
2) Set the time duration and the language.

Note

If authentication is failed in the configured time duration, the device will broadcast the configured content.

3) Enter the audio content.
4) **Optional:** Repeat substep 1 to 3.
5) **Optional:** Click to delete the configured time duration.

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

8.5.15 Set Image Parameters

Set the video standard, WDR, brightness, contrast, saturation, and sharpness.

Steps

1. Click **Configuration → Image Adjustment** .

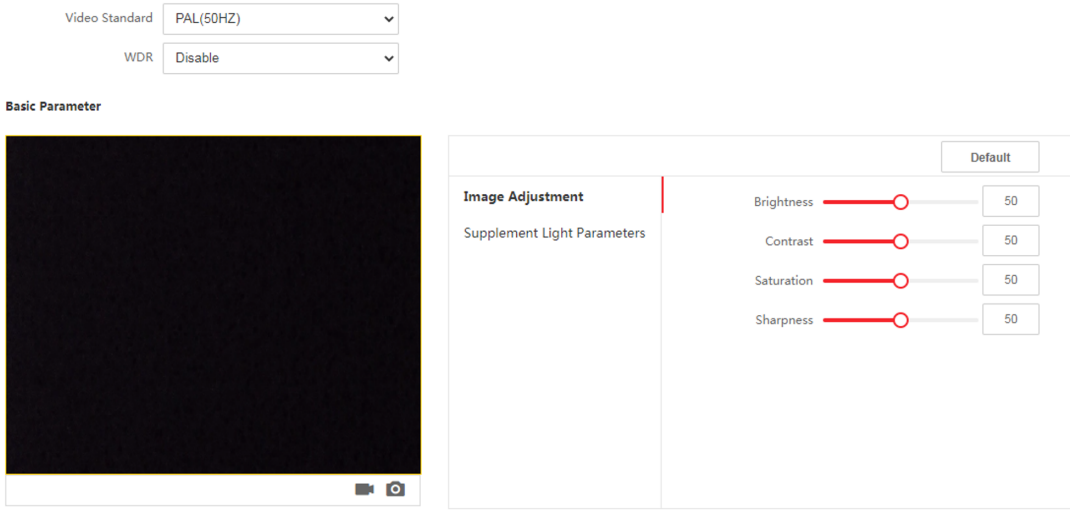


Figure 8-10 Image Settings Page

2. Configure the parameters to adjust the image.

Video Standard

Set the video frame rate when performing live view remotely. After changing the standard, you should reboot the device to take effect.

PAL

25 frames per second. Suitable for mainland China, Hong Kong (China), the Middle East countries, Europe countries, etc.

NTSC

30 frames per second. Suitable for the USA, Canada, Japan, Taiwan (China), Korea, the Philippines, etc.

WDR

Enable or disable the WDR function.

When there are both very bright and very dark areas simultaneously in the view, WDR balances the brightness level of the whole image and provide clear images with details.

Brightness/Contrast/Saturation/Sharpness

Drag the block or enter the value to adjust the live video's brightness, contrast, saturation, and sharpness.

Start/end recording video.

Capture the image.

3. Click **Default** to restore the parameters to the default settings.

8.5.16 Set Supplement Light Brightness

Set the device supplement light brightness.

Steps

1. Click **Configuration → Image → Supplement Light Parameters** .

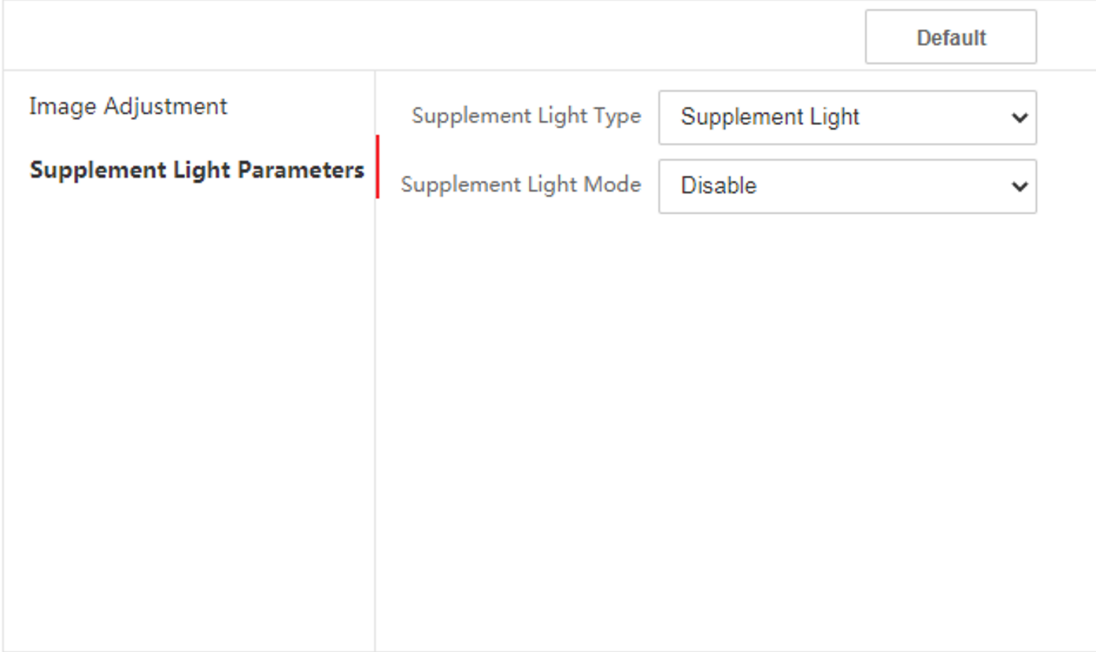


Figure 8-11 Supplement Light Settings Page

2. Select a supplement light type and mode from the drop-down list. If you select the mode as **ON**, you should set the brightness.

8.5.17 Time and Attendance Settings

If you want to track and monitor when the persons start/stop work and monitor their working hours and late arrivals, early departures, time taken on breaks, and absenteeism, you can add the person to the shift group and assign a shift schedule (a rule for the attendance defining how the schedule repeats, the shift type, break settings, and the card swiping rule.) to the shift group to define the attendance parameters for the persons in the shift group.

Disable Attendance Mode via Web

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

Steps

1. Click **Configuration → Attendance** to enter the settings page.
2. Set the **Attendance Mode** as **Disable**.

Result

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.

Time Settings

Steps

1. Click **Configuration → Time Settings** to enter the settings page.
2. Select **Status Type**.
3. **Optional:** Edit **Schedule Name** according to the actual needs.
4. Drag mouse to set the schedule.

   Note

   Set the schedule from Monday to Sunday according to the actual needs.

5. **Optional:** Select a timeline and click **Delete**. Or click **Delete All** to clear the settings.
6. Click **Save**.

Set Manual Attendance via Web

Set the attendance mode as manual, and you should 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. Click **Configuration → Attendance** to enter the settings page.
2. Set the **Attendance Mode** as **Manual**.
3. Enable the **Attendance Status Required** and set the attendace status lasts duration.
4. Enable a group of attendance status.

   Note

   The Attendance Property will not be changed.

5. **Optional:** Select an status and change its name if required.

Result

You should select an 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.

Set Auto Attendance via Web

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 schedule.

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

Steps
1. Click **Configuration → Attendance** to enter the settings page.
2. Set the **Attendance Mode** as **Auto**.
3. Enable the **Attendance Status** function.
4. Enable a group of attendance status.

   Note
   The Attendance Property will not be changed.
5. **Optional:** Select an status and change its name if required.
6. Set the status' schedule. Refers to ***Time Settings*** for details.

Set Manual and Auto Attendance via Web

Set the attendance mode as **Manual and Auto**, and the system will automatically change the attendance status according to the configured schedule. 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. Click **Configuration → Attendance** to enter the settings page.
2. Set the **Attendance Mode** as **Manual and Auto**.
3. Enable the **Attendance Status** function.
4. Enable a group of attendance status.

   Note
   The Attendance Property will not be changed.
5. **Optional:** Select an status and change its name if required.
6. Set the status' schedule. Refers to ***Time Settings*** for details.

Result

On the initial page and authenticate. The authentication will be marked as the configured attendance status according to the schedule. If you tap the edit icon on the result tab, you can select a status to take attendance manually, the authentication will be marked as the edited attendance status.

Example

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

8.5.18 Set Video Intercom Parameters

The device can be used as a door station, outer door station, or access control device. You should set the device No. before usage.

Click **Configuration → Video Intercom → Device No.** .

If set the device type as **Door Station**, **Outer Door Station**, **Access Control Device**, you can set the period No., building No., unit No., floor No., door station No., and community No.

Click **Save** to save the settings after the configuration.

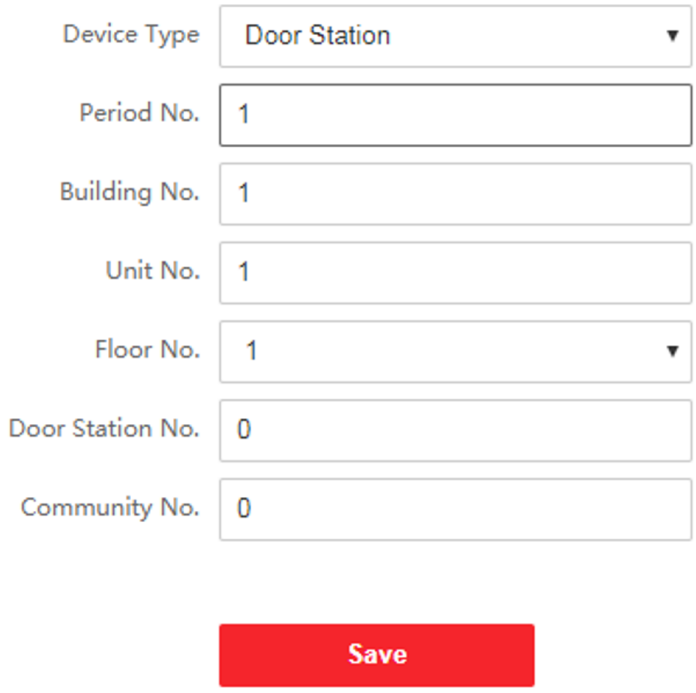


Figure 8-12 Device No. Settings

Device Type

The device can be used as a door station, outer door station, or access control device. Select a device type from the drop-down list.

Note

If you change the device type, you should reboot the device.

Period No.

Set the device installed period No.

Building No.

Set the device installed building No.

Unit No.

Set the device installed unit No.

Floor No.

Set the device installed floor No.

Door Station No.

Set the device installed floor No.

Note

If you change the No., you should reboot the device.

Community No.

Set the device installed community No.

If set the device type as **Outer Door Station**, you can set the period No., outer door station No., and community No.

Period No.

Set the device installed period No.

Outer Door Station No.

If you select outer door station as the device type, you should enter a number between **1** and **99**.

Note

If you change the No., you should reboot the device.

Community No.

Set the device installed community No.

8.5.19 Configure SIP Parameters

Set the device'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.

Go to **Configuration → Access Control → Linked Network Settings** .

Set the main station's IP address and SIP server's IP address.

Click **Save**.

8.5.20 Access Control Settings

Set Authentication Parameters

Click **Configuration → Access Control → Authentication Settings** .

Note

The functions vary according to different models. Refers to the actual device for details.

Click **Save** to save the settings after the configuration.

Device Type

Select **Main Card Reader** or **Sub Card Reader** from the drop-down list.

Main Card Reader

You can configure the device card reader's parameters.

Sub Card Reader

You can configure the connected peripheral card reader's parameters.

If select **Main Card Reader**:

Card Reader Type/Card Reader Description

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

Enable Card Reader

Enable the card reader's function.

Authentication

Select an authentication mode according to your actual needs from the drop-down list.

Recognition Interval

You can set the interval between 2 continuous recognition of a same person during the authentication. In the configured interval, Person A can only recognized once. If another person (Person B) has recognized during the interval, Person A can recognized again.

Authentication Interval

You can set the authentication interval of the same person when authenticating. The same person can only authenticate once in the configured interval. A second authentication will be failed.

Alarm of Max. Failed Attempts

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

Enable Tampering Detection

Enable the anti-tamper detection for the card reader.

Enable Card No. Reversing

The read card No. will be in reverse sequence after enabling the function.

If select **Sub Card Reader**:

Card Reader Type/Card Reader Description

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

Enable Card Reader

Enable the card reader's function.

Authentication

Select an authentication mode according to your actual needs from the drop-down list.

Recognition Interval

If the interval between card presenting of the same card is less than the configured value, the card presenting is invalid.

Authentication Interval

You can set the authentication interval of the same person when authenticating. The same person can only authenticate once in the configured interval. A second authentication will be failed.

Alarm of Max. Failed Attempts

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

Communication 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.

Max. Interval When Entering Password

When you entering the password on the card reader, if the interval between pressing two digits is longer than the set value, the digits you pressed before will be cleared automatically.

OK LED Polarity/Error LED Polarity

Set OK LED Polarity/Error LED Polarity of the access control device according to the card reader parameters. Generally, adopts the default settings.

Enable Tampering Detection

Enable the anti-tamper detection for the card reader.

Set Door Parameters

Click **Configuration → Access Control → Door Parameters** .

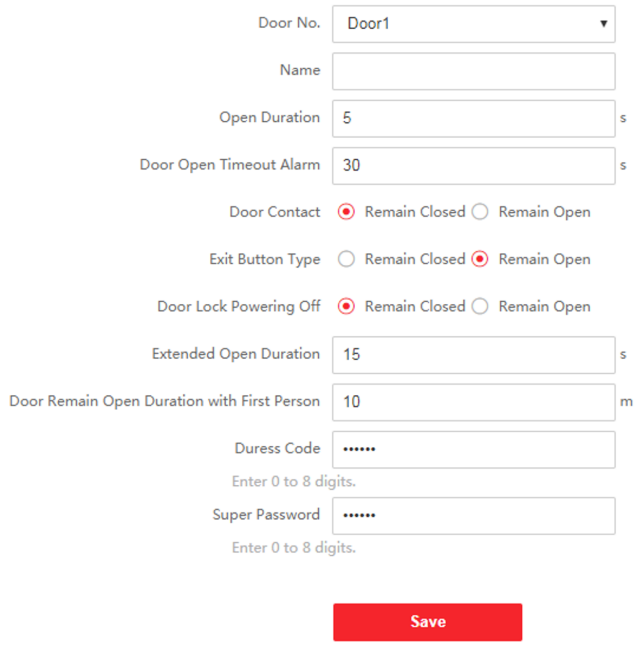


Figure 8-13 Door Parameters Settings Page

Click **Save** to save the settings after the configuration.

Door No.

Select the device corresponded door No.

Name

You can create a name for the door.

Open Duration

Set the door unlocking duration. If the door is not opened for the set time, the door will be locked.

Door Open Timeout Alarm

An alarm will be triggered if the door has not been closed within the configured time duration.

Door Contact

You can set the door contact as **Remain Open** or **Remain Closed** according to your actual needs. By default, it is **Remain Closed**.

Exit Button Type

You can set the exit button as **Remain Open** or **Remain Closed** according to your actual needs. By default, it is **Remain Open**.

Door Lock Powering Off Status

You can set the door lock status when the door lock is powering off. By default, it is **Remain Closed**.

Extended Open Duration

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

Door Remain Open Duration with First Person

Set the door open duration when first person is in. After the first person is authorized, it allows multiple persons access the door or other authentication actions.

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 the super code should be different.

Set Card Security

Click **Configuration → Access Control → Card Security** to enter the settings page.

Set the parameters and click **Save**.

Enable NFC Card

In order to prevent the mobile phone from getting the data of the access control, you can enable NFC card to increase the security level of the data.

Enable M1 Card

Enable M1 card and authenticating by presenting M1 card is available.

M1 Card Encryption
Sector

M1 card encryption can improve the security level of authentication.

Enable the function and set the encryption sector. By default, Sector 13 is encrypted. It is recommended to encrypt sector 13.

Enable EM Card

Enable EM card and authenticating by presenting EM card is available.

Note

If the peripheral card reader supports presenting EM card, the function is also supported to enable/disable the EM card function.

Set RS-485 Parameters

You can set the RS-485 parameters including the peripheral, address, baud rate, etc.

Click **Configuration → Access Control → RS-485 Settings** .

Click **Save** to save the settings after the configuration.

No.

Set the RS-485 No.

Peripheral Type

Select a peripheral from the drop-down list according the actual situation. You can select from **Card Reader**, **Extension Module**, **Access Controller**, or **Disable**.

Note

After the peripheral is changed and saved, the device will reboot automatically.

RS-485 Address

Set the RS-485 Address according to your actual needs.

Note

If you select **Access 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.

Baud Rate

The baud rate when the devices are communicating via the RS-485 protocol.

Set Wiegand Parameters

You can set the Wiegand transmission direction.

Steps

Note

Some device models do not support this function. Refer to the actual products when configuration.

1. Click **Configuration → Access Control → Wiegand Settings** .

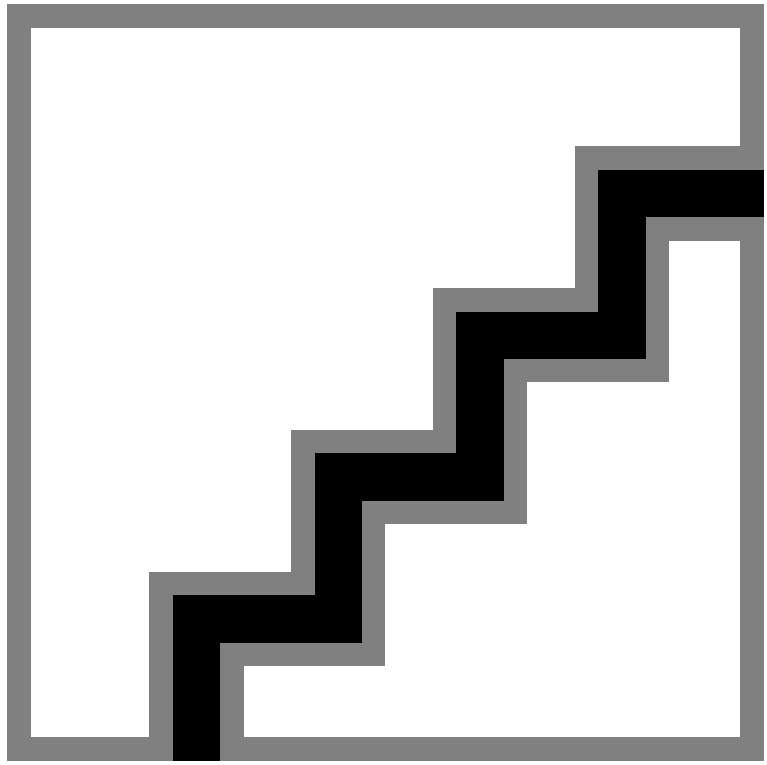


Figure 8-14 Wiegand Page

2. Check **Wiegand** to enable the Wiegand function.
3. Set a transmission direction.

   Input

   The device can connect a Wiegand card reader.

   Output

   The can connect an external access controller. And the two devices will transmit the card No. via Wiegand 26 or 34.
4. Click **Save** to save the settings.

Note

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

Set Face Recognition Parameters

You can set face recognition parameters for accessing.

Click **Configuration → Access Control → Face Recognition Parameters** .

You can set **Working Mode** as **Access Control Mode**. The access control mode is the device normal mode. You should authenticate your credential for accessing.

Set Privacy Parameters

Set the event storage type, picture upload and storage parameters, and the picture clearing parameters.

Go to **Configuration → Access Control → Privacy**

Event Storage Settings

Select a method to delete the event. You can select from **Delete Old Events Periodically**, **Delete Old Events by Specified Time**, or **Overwriting**.

Delete Old Events Periodically

Drag the block or enter number to set the period for event deleting. All events will be deleted according to the configured time duration.

Delete Old Events by Specified Time

Set a time and all events will be deleted on the configured time.

Overwriting

The earliest 5% events will be deleted when the system detects the stored events has been over 95% of the full space.

Authentication Settings

Display Authentication Result

You can check **Face Picture**, **Name**, **Employee ID** and **Temperature**, to display the authentication result.

Picture Uploading and Storage

Upload Captured Picture When Authenticating

Upload the pictures captured when authenticating to the platform automatically.

Save Captured Picture When Authenticating

If you enable this function, you can save the picture when authenticating to the device.

Save Registered Picture

The registered face picture will be saved to the system if you enable the function.

Upload Picture After Linked Capture

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

Save Pictures After Linked Capture

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

Upload Thermographic Picture

Upload thermographic picture captured to the platform automatically.

Save Thermographic Picture

If you enable this function, you can save the thermographic picture captured to the device.

Clear All Pictures in Device

Note

All pictures cannot be restored once they are deleted.

Clear Registered Face Pictures

All registered pictures in the device will be deleted.

Clear Captured Pictures

All captured pictures in the device will be deleted.

Set Card Authentication Parameters

Set the card reading content when authenticate via card on the device.

Go to **Configuration → Access Control → Card Authentication Settings** .

Select a card authentication mode and click **Save**.

Full Card No.

All card No. will be read.

Wiegand 26 (3 bytes)

The device will read card via Wiegand 26 protocol (read 3 bytes).

Wiegand 34 (4 bytes)

The device will read card via Wiegand 34 protocol (read 4 bytes).

8.5.21 Set Biometric Parameters

Set Basic Parameters

Click **Configuration → Smart → Smart** .

Note

The functions vary according to different models. Refers to the actual device for details.

Figure 8-15 Smart Settings Page

Click **Save** to save the settings after the configuration.

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.

Note

Biometric recognition products are not completely applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.

Live Face Detection Security Level

After enabling the face anti-spoofing function, you can set the matching security level when performing live face authentication.

Recognition Distance

Select the distance between the authenticating user and the device camera.

Application Mode

Select either others or indoor according to actual environment.

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.

Continuous Face Recognition Interval

Set the time interval between two continuous face recognitions when authenticating.

Pitch Angle

The maximum pitch angle when starting face authentication.

Yaw Angle

The maximum yaw angle when starting face authentication.

Face Grading

Set the face grading according to your needs.

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.

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.

Face Recognition Timeout Value

Set the timeout value when face recognizing. If the face recognition time is longer than the configured value, the system will pop up a prompt.

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 the 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

Face with Mask Detection

After enabling the face with mask detection, the system will recognize the captured face with mask picture. You can set face with mask1:N matching threshold, it's ECO mode, and the strategy.

None

The device will detect the face with mask without prompt.

Prompt and Open

If the person do not wear a face mask when authenticating, the device prompts a notification and the door will open.

Prompt and Not Open Door

If the person do not wear a face mask when authenticating, the device prompts a notification and the door keeps closed.

Set Recognition Area

Click **Configuration → Smart → Area Configuration** .
Drag the yellow frame in the live video to adjust the recognition area. Only the face within the area can be recognized by the system.
Click **Save** to save the settings.
Click or to record videos or capture pictures.

8.5.22 Set Notice Publication

You can set the theme for the device.

Click **Configuration → Theme** .

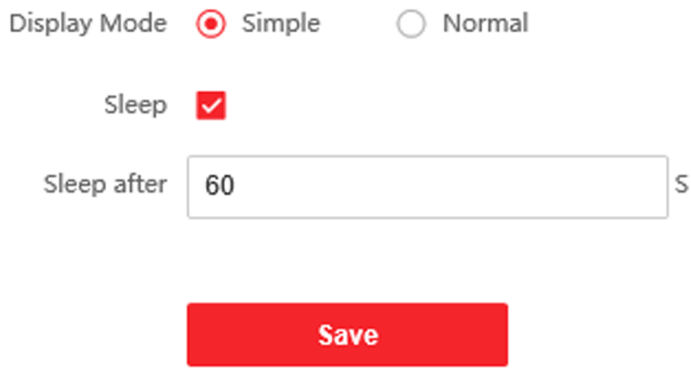


Figure 8-16 Theme Page

Display Mode

You can select display theme for device authentication. You can select **Display Mode** as **Simple** or **Normal**. When you select **Simple**, the information of name, ID, face picture will be not displayed.

Sleep

Enable **Sleep** and the device will enter the sleep mode when no operation within the configured sleep time. After enabling **Sleep**, you need set the start time of display.

8.5.23 Temperature Measurement Settings

Temperature Measurement Settings

You can set the temperature measurement parameters, including temperature measurement only, temperature unit, over-temperature threshold, temperature compensation, door not open when temperature is abnormal, etc.

Steps

1. Click **Configuration → Temperature → Temperature Settings** .

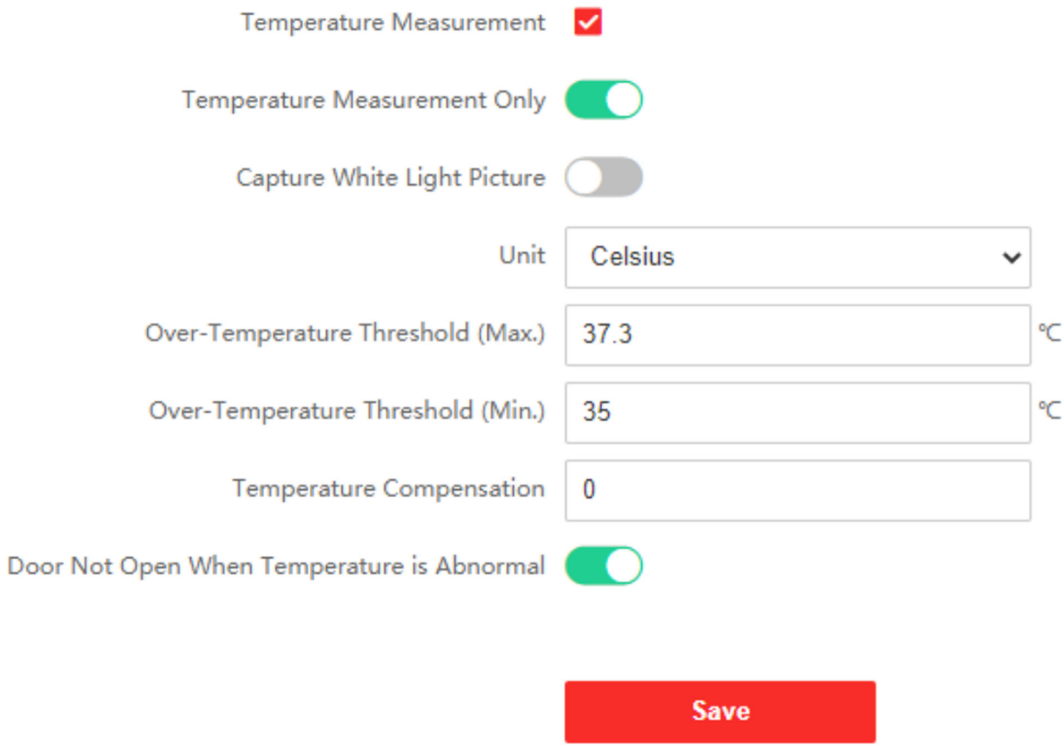


Figure 8-17 Temperature Measurement Settings

2. Enable **Temperature Measurement**.
3. Configure the temperature measurement parameters.

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.

Capture White Light Picture

After enabling **Temperature Measurement Only**, you can enable **Capture White Light Picture**. After enabling this function, the device will capture white light picture.

Measure Area Settings

Configure the temperature measurement area.

Unit

Select a temperature unit according to your preference.

4. Click **Save**.

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 body is required, do not set the black body parameters, or the temperature may not correct.

Steps

1. Click **Configuration → Temperature → Black Body Settings** .

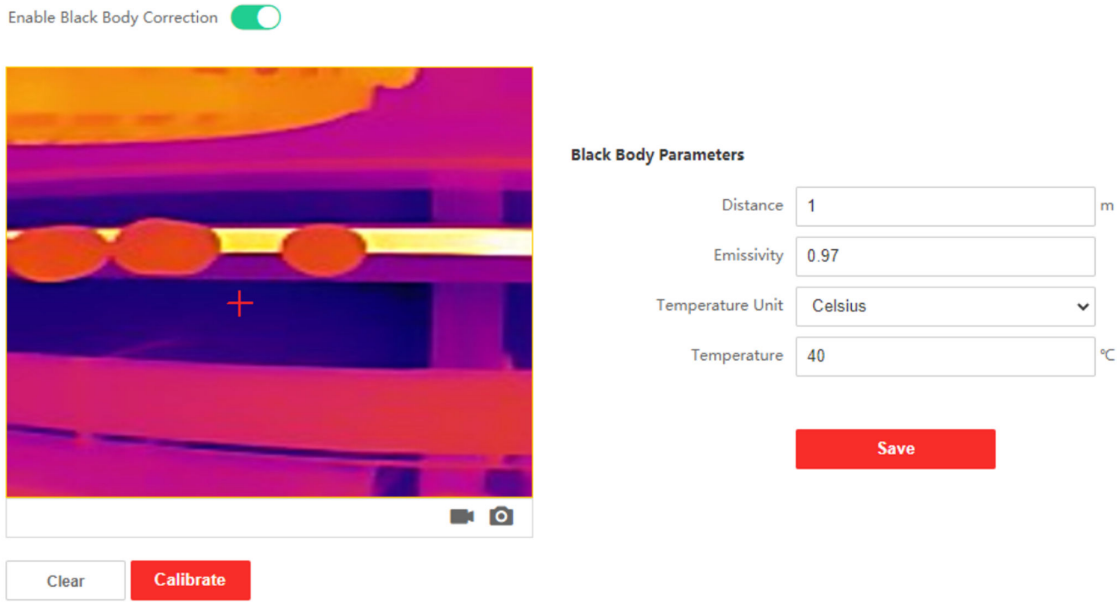


Figure 8-18 Black Body Settings

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), the emissivity of the black body, and the temperature unit.

Note

The black body's temperature is fixed.

5. Click **Calibrate**, and draw the black body's position on the page. When **+** is displayed on the black body on the screen, the black body is calibrated.
6. Click **Save**.

Chapter 9 Client Software Configuration

9.1 Configuration Flow of Client Software

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

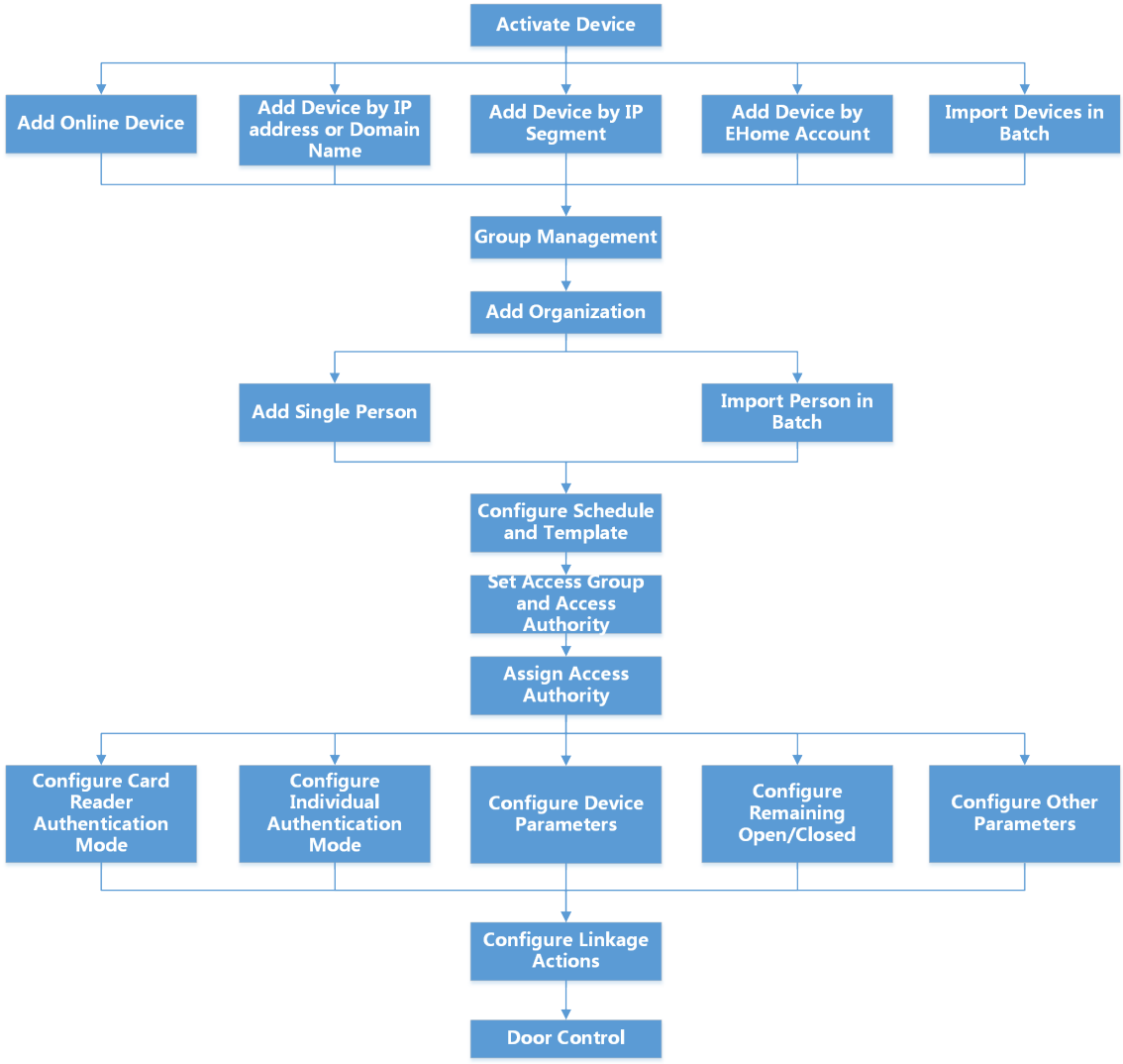


Figure 9-1 Flow Diagram of Configuration on Client Software

9.2 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.

9.2.1 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 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.

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.

9.2.2 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.

9.2.3 Manage Added Devices

After adding devices to device list, you can manage the added devices including editing device parameters, remote configuration, viewing device status, etc.

Table 9-1 Manage Added Devices

Edit Device	Click to edit device information including device name, address, user name, password, etc.
Delete Device	Check one or more devices, and click **Delete** to delete the selected devices.
Remote Configuration	Click to set remote configuration of the corresponding device. For details, refer to the user manual of device.
View Device Status	Click to view device status, including door No., door status, etc. **Note** For different devices, you will view different information about device status.
View Online User	Click to view the details of online user who access the device, including user name, user type, IP address and login time.
Refresh Device Information	Click to refresh and get the latest device information.

Upgrade Device	View device status on Firmware Upgrade column, check one or more upgradable devices, and click **Upgrade Device Firmware** to upgrade the selected devices. For details, refer to .
Get Events from Device	Check one device, and click **Get Events from Device** to synchronize events. For details, refer to .

9.3 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.

9.3.1 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.

9.3.2 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.

9.4 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.

9.4.1 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.

9.4.2 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.

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.

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.

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.

Export Person Pictures

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

Before You Start

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

Steps

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

   Note

   All persons' face pictures will be exported if you do not select any organization.
3. Click **Export** to open the Export panel and check **Face** as the content to export.
4. Click **Export** to start exporting.

   Note

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

9.4.3 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.
- 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.

9.4.4 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 *Issue a Card by Local Mode*.
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).

9.4.5 Report Card Loss

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

Steps

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

   After reporting card loss, the access authorization of this card will be invalid and inactive. Other person who gets this card cannot access the doors by swiping this lost card.
4. **Optional:** If the lost card is found, you can click to cancel the loss.

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

9.4.6 Set Card Issuing Parameters

The client provides two modes for reading a card's number: via card enrollment station or via the card reader of the access control device. If a card enrollment station is available, connect it to the

PC running the client by USB interface or COM, and place the card on the card enrollment to read the card number. If not, you can also swipe the card on the card reader of the added access control device to get the card number. As a result, before issuing a card to one person, you need to set the card issuing parameters including the issuing mode and related parameters.

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

Local Mode: Issue Card by Card Enrollment Station

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

Card Enrollment Station

Select the model of the connected card enrollment station

Note

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

Card Type

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

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

Serial Port

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

Select the COM the card enrollment station connects to.

Buzzing

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

Card No. Type

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

M1 Card Encryption

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

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

Remote Mode: Issue Card by Card Reader

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

9.5 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*** .

9.5.1 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**.

9.5.2 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.

9.6 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.

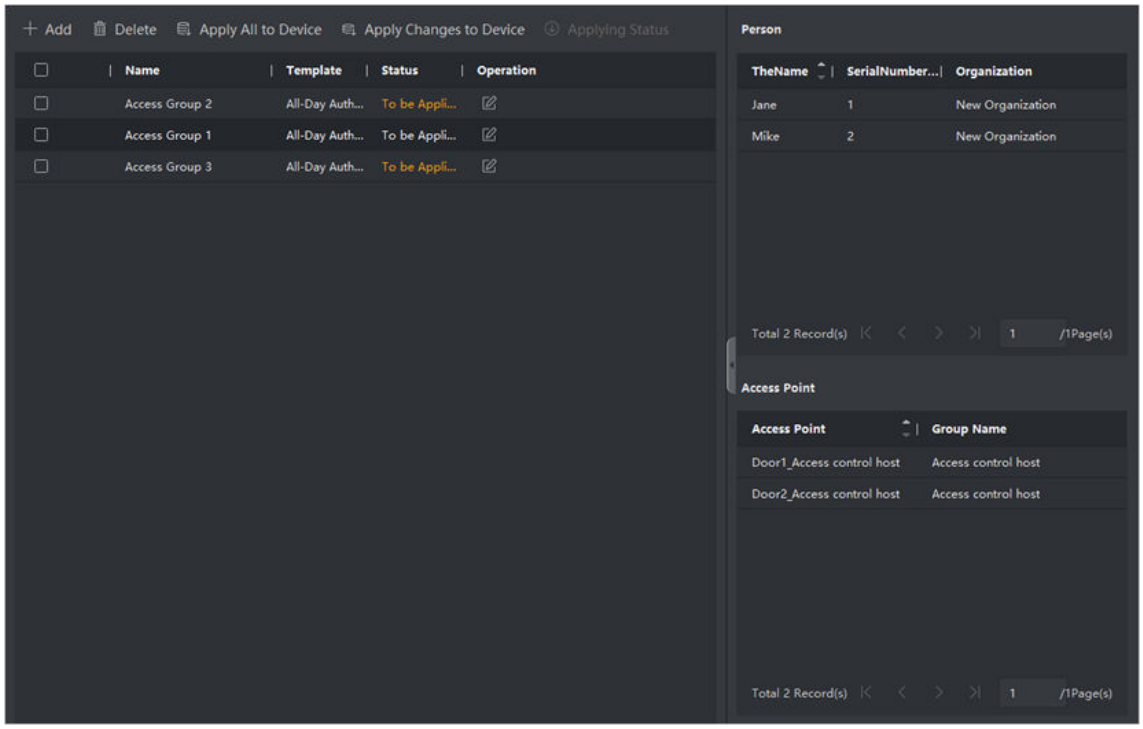


Figure 9-2 Display the Selected Person(s) and Access Point(s)

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**.

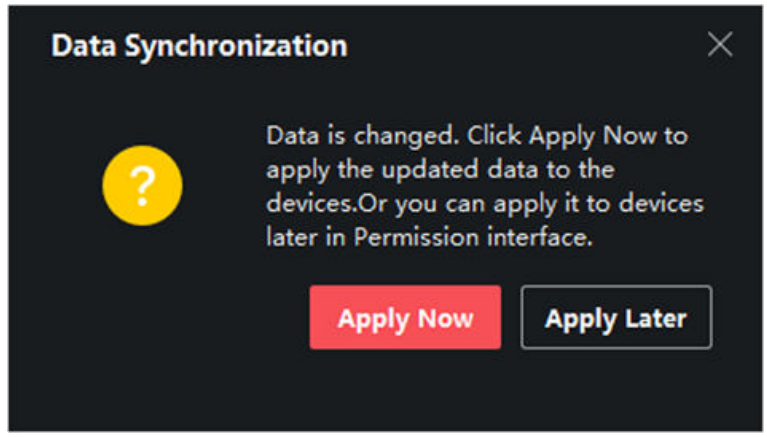


Figure 9-4 Data Synchronization

9.7 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.

9.7.1 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.

Before You Start
Add access control device to the client.

Steps

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

   Note

   If you can not find Device Parameter in the Advanced Function list, hover the cursor on the Advanced Function, and then Click to select the Device Parameter to be displayed.

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

   Note

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

   RS-485 Comm. Redundancy

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

   Display Detected Face

   Display face picture when authenticating.

   Display Card Number

   Display the card information when authenticating.

   Display Person Information

   Display the person information when authenticating.

   Overlay Person Info. on Picture

   Display the person information on the captured picture.

   Voice Prompt

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

   Upload Pic. After Linked Capture

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

   Save Pic. After Linked Capture

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

Press Key to Enter Card Number

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

Wi-Fi Probe

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

3G/4G

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

NFC Anti-Cloning

If you enable this function, you cannot use the cloned card for authentication and further enhance security.

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

Configure Parameters for Door/Elevator

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

Before You Start

Add access control device to the client.

Steps

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

Note

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

Name

Edit the card reader name as desired.

Door Contact

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

Exit Button Type

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

Door Locked Time

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

Extended Open Duration

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

Lock Door when Door Closed

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

Duress Code

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

Super Password

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

Dismiss Code

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

Note

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

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

Note

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

Configure Parameters for Card Reader

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

Before You Start

Add access control device to the client.

Steps

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

Note

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

Name

Edit the card reader name as desired.

OK LED Polarity/Error LED Polarity/Buzzer Polarity

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

Minimum Card Swiping Interval

If the interval between card swiping of the same card is less than the set value, the card swiping is invalid. You can set it as 0 to 255.

Max. Interval When Entering PWD

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

Alarm of Max. Failed Attempts

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

Max. Times of Card Failure

Set the max. failure attempts of reading card.

Tampering Detection

Enable the anti-tamper detection for the card reader.

Communicate with Controller Every

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

Buzzing Time

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

Card Reader Type/Card Reader Description

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

Fingerprint Recognition Level

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

Default Card Reader Authentication Mode

View the default card reader authentication mode.

Fingerprint Capacity

View the maximum number of available fingerprints.

Existing Fingerprint Number

View the number of existed fingerprints in the device.

Score

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

Face Recognition Timeout Value

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

Face Recognition Interval

The time interval between two continuous face recognitions when authenticating. By default, it is 2s.

Face 1:1 Matching Threshold

Set the matching threshold when authenticating via 1:1 matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate when authentication.

1:N Security Level

Set the matching security level when authenticating via 1:N matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate when authentication.

Live Face Detection

Enable or disable the live face detection function. If enabling the function, the device can recognize whether the person is a live one or not.

Live Face Detection Security Level

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

Max. Failed Attempts for Face Auth.

Set the maximum live face detection failed attempts. The system will lock the user's face for 5 minutes if the live face detection is failed for more than the configured attempts. The same user cannot authenticate via the fake face within 5 minutes. Within the 5 minutes, the user can authenticate via the real face twice continuously to unlock.

Lock Authentication Failed Face

After enabling the Live Face Detection function, the system will lock the user's face for 5 minutes if the live face detection is failed for more than the configured attempts. The same

user cannot authenticate via the fake face within 5 minutes. Within the 5 minutes, the user can authenticate via the real face twice continuously to unlock.

Application Mode

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

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

Configure Parameters for Alarm 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.

Configure Parameters for Lane Controller

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

Before You Start

Add access control device to the client.

Steps

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

Passing Mode

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

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

Free Passing Authentication

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

Opening/Closing Barrier Speed

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

Note

The recommended value is 6.

Audible Prompt Duration

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

Note

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

Temperature Unit

Select the temperature unit that displayed in the device status.

4. Click **OK**.

9.7.2 Configure Device Parameters

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

Set Parameters for Face Recognition Terminal

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

Steps

Note

This function should be supported by the device.

1. Enter the Access Control module.

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

Note

These parameters displayed vary according to different device models.

COM

Select a COM port for configuration. COM1 refers to the RS-485 interface and COM2 refers to the RS-232 interface.

Face Picture Database

select Deep Learning as the face picture database.

Authenticate by QR Code

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

Blocklist Authentication

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

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

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

Save Authenticating Face Picture

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

MCU Version

View the device MCU version.

5. Click **Save**.

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.

Before You Start

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

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 **Wiegand** to enter the Wiegand Settings page.
4. Set the switch to on to enable the Wiegand function for the device.
5. Select the Wiegand channel No. and the communication mode from the drop-down list.

Note

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

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

Enable M1 Card Encryption

M1 card encryption can improve the security level of authentication.

Steps

Note

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

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

   The sector ID ranges from 1 to 100.
6. Click **Save** to save the settings.

9.8 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*** .

9.8.1 Control Door Status

You can control the status for the door(s), including unlock door, locking door, remaining the door unlock, remaining the door locked, remain all unlocked, etc.

Before You Start

- Add person and assign access authorization to designed person, and person will have the access authorization to the access points (doors). For details, refer to ***Person Management*** and ***Set Access Group to Assign Access Authorization to Persons*** .
- Make sure the operation user has the permission of the access points (doors). For details, refer to .

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*** .

   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.

Note

For **Remain All Unlocked** and **Remain All Locked**, ignore this step.

4. Click the following buttons to control the door.

Unlock

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.

Lock

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 Unlocked

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

Remain Locked

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.

Remain All Unlocked

All doors in the group will be unlocked (no matter closed or open). All the persons can access the doors with no credentials required.

Remain All Locked

All doors in the group will be closed and locked. No person can access the doors 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.

9.8.2 Check Real-Time Access Records

The real-time access records can be displayed in the client, including card swiping records, face recognition records, skin-surface temperature information, etc. Also, you can view the person information and view the picture captured during access.

Before You Start

You have added person(s) and access control device(s) to the client. For details, refer to ***Person Management*** and ***Add Device*** .

Steps

1. Click **Monitoring** to enter monitoring module.

   Real-time access records are displayed on the bottom of the page. You can view record details, including card No., person name, event time, door location, temperature, authentication type etc.

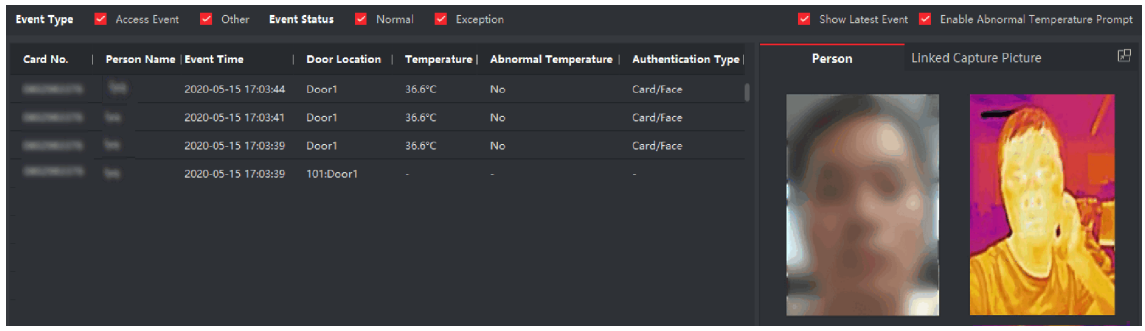


Figure 9-5 Real-time Access Records

Note

You can right click the column name of access event table to show or hide the column according to actual needs.

2. **Optional:** Select an access point group from the drop-down list in the upper-right corner to show the real time access records of the selected group.
3. **Optional:** Check the event type and event status.

   The detected events of checked type and status will be displayed in the list below.
4. **Optional:** Check **Show Latest Event** to view the latest access record.

   The record list will be listed reverse chronologically.
5. **Optional:** Check **Enable Abnormal Temperature Prompt** to enable abnormal skin-surface temperature prompt.

Note

When enabled, if there is abnormal temperature information, an Abnormal Temperature window pops up when you enter Monitoring module, displaying person's picture, skin-surface temperature, card No., person name, etc.

6. **Optional:** Click an event to view person pictures (including captured picture and profile).

Note

In **Linked Capture Picture** field, you can double click the captured picture to view an enlarged picture.

7. **Optional:** Click to view details (including person's detailed information and the captured picture).

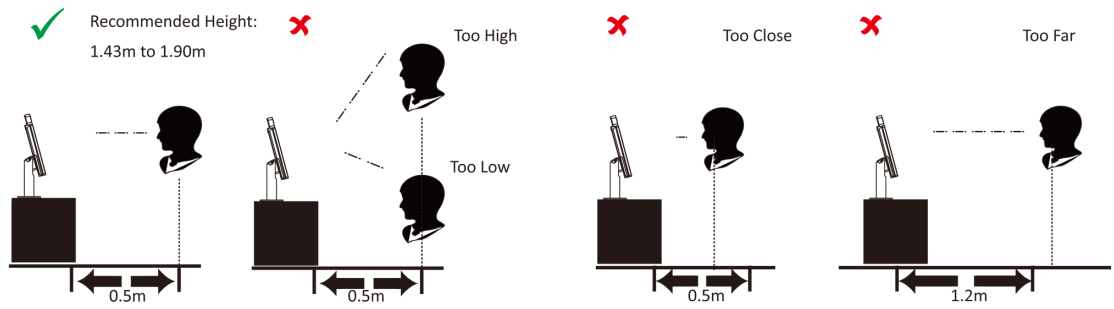
Note

In the pop-up window, you can click to view details in full screen.

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)



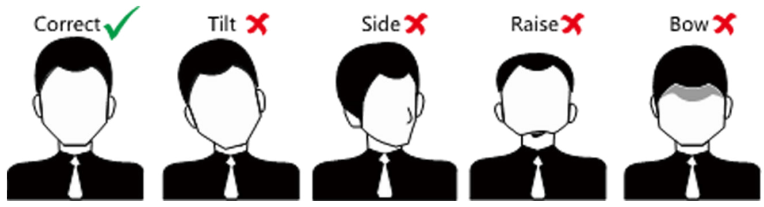
Expression

- 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.

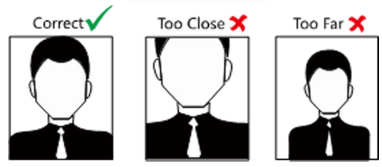
Posture

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.


Correct
Too Close
Too Far

Appendix B. Tips for Installation Environment

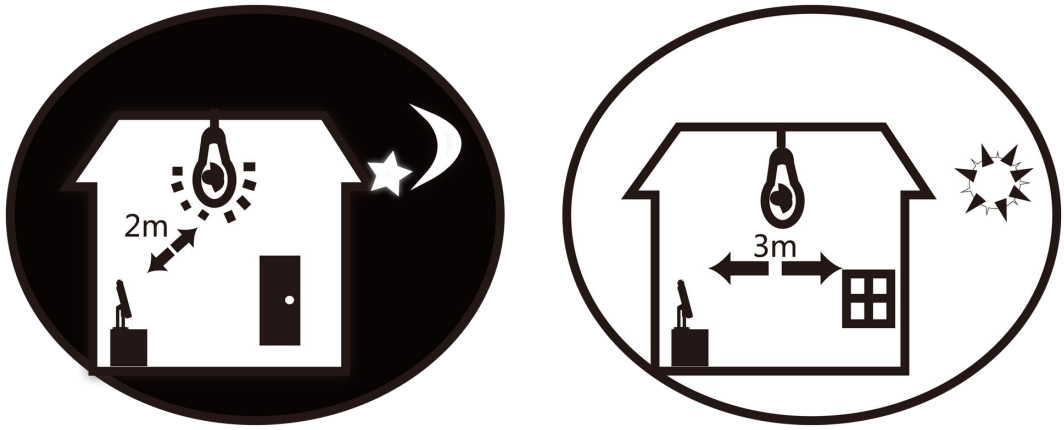
1. Light Source Illumination Reference Value

Candle: 10Lux

Bulb: 100~850Lux

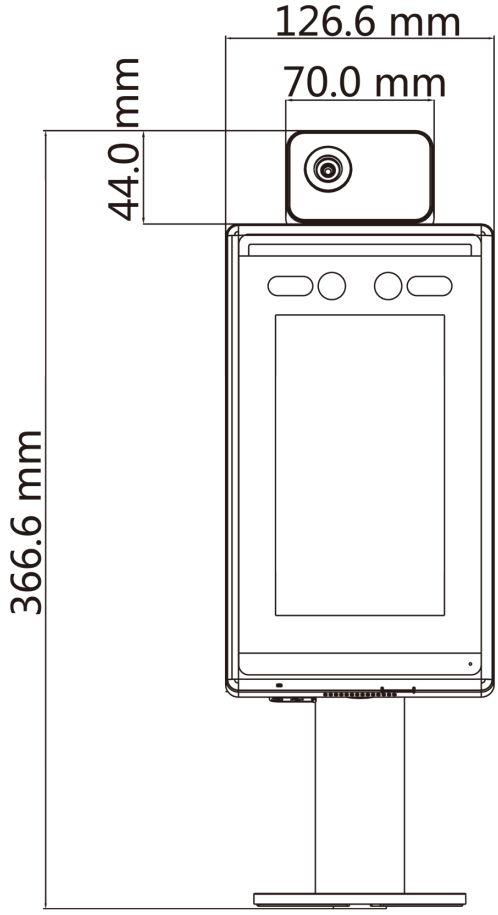
Sunlight: More than 1200Lux

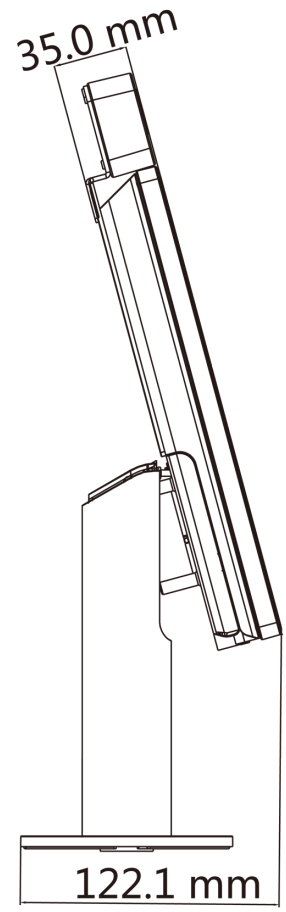
2. Install the device at least 2 meters away from the light, and at least 3 meters away from the window or door.



3.Avoid backlight, direct and indirect sunlight

Appendix C. Dimension





Appendix D. Communication Matrix and Device Command

Communication Matrix

Scan the following QR code to get the device communication matrix.
Note that the matrix contains all communication ports of Hikvision access control and video intercom devices.

Figure D-1 QR Code of Communication Matrix

Device Command

Scan the following QR code to get the device common serial port commands.
Note that the command list contains all commonly used serial ports commands for all Hikvision access control and video intercom devices.

Figure D-2 Device Command

See Far, Go Further