DS-K6300 Series Payment Terminal

User Manual

Legal Information

©2022 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.
This equipment complies with FCC/IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator & your body.
ce matériel est conforme aux limites de dose d'exposition aux rayonnements, FCC / CNR-102 énoncée dans un autre environnement.cette eqipment devrait être installé et exploité avec distance minimale de 20 entre le radiateur et votre corps.

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:

- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region.
- Please use the power adapter, which is provided by normal company. The power consumption cannot be less than the required value.
- Do not connect several devices to one power adapter as adapter overload may cause over-heat or fire hazard.
- Please make sure that the power has been disconnected before you wire, install or dismantle the device.
- When the product is installed on wall or ceiling, the device shall be firmly fixed.
- If smoke, odors or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the device yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)
- The socket-outlet shall be installed near the equipment and shall be easily accessible.
- An all-pole mains switch shall be incorporated in the electrical installation of the building.
- The equipment has been designed, when required, modified for connection to an IT power distribution system.
- 1. Do not ingest battery. Chemical burn hazard!
  2. 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.
  3. Keep new and used batteries away from children.
  4. If the battery compartment does not close securely, stop using the product and keep it away from children.
  5. If you think batteries might have been swallowed or placed inside any part of the body, seek immediate medical attention.
  6. CAUTION: Risk of explosion if the battery is replaced by an incorrect type.

7. Improper replacement of the battery with an incorrect type may defeat a safeguard (for example, in the case of some lithium battery types).
8. Do not dispose of the battery into fire or a hot oven, or mechanically crush or cut the battery, which may result in an explosion.
9. Do not leave the battery in an extremely high temperature surrounding environment, which may result in an explosion or the leakage of flammable liquid or gas.
10. Do not subject the battery to extremely low air pressure, which may result in an explosion or the leakage of flammable liquid or gas.
11. Dispose of used batteries according to the instructions

- This equipment is not suitable for use in locations where children are likely to be present.
- This equipment is for use only with DS-K1T341 mounting plate, bracket. Use with other (carts, stands, or carriers) may result in instability causing injury.
- To prevent possible hearing damage, do not listen at high volume levels for long periods.

⚠ Cautions:

- No naked flame sources, such as lighted candles, should be placed on the equipment The USB port of the equipment is used for connecting to a mouse, a keyboard, or a USB flash drive only.
- The serial port of the equipment is used for debugging only.
- Burned fingers when handling the back panel. Wait one-half hour after switching off before handling the parts.
- 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).
- Install the equipment according to the instructions in this manual. To prevent injury, this equipment must be securely attached to the floor/wall in accordance with the installation instructions.
- Do not place the device in extremely hot (refer to the specification of the device for the detailed operating temperature), cold, dusty or damp locations, and do not expose it to high electromagnetic radiation.
- The device cover for indoor use shall be kept from rain and moisture.
- Exposing the equipment to direct sun light, low ventilation or heat source such as heater or radiator is forbidden (ignorance can cause fire danger).
- Do not aim the device at the sun or extra bright places. A blooming or smear may occur otherwise (which is not a malfunction however), and affecting the endurance of sensor at the same time.
- Please use the provided glove when open up the device cover, avoid direct contact with the device cover, because the acidic sweat of the fingers may erode the surface coating of the device cover.
- Please use a soft and dry cloth when clean inside and outside surfaces of the device cover, do not use alkaline detergents.
- Please keep all wrappers after unpack them for future use. In case of any failure occurred, you need to return the device to the factory with the original wrapper. Transportation without the original wrapper may result in damage on the device and lead to additional costs.

- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.
- Biometric recognition products are not 100% applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.
- Indoor and outdoor use. If installing the device indoors, the device should be at least 2 meters away from the light, and at least 3 meters away from the window or the door. If installing the device outdoors, you should apply Silicone sealant among the cable wiring area to keep the raindrop from entering.
- Input voltage should meet both the SELV (Safety Extra Low Voltage) and the Limited Power Source with 100~240 VAC or 12 VDC according to the IEC60950-1 standard. Please refer to technical specifications for detailed information.

Available Models

Product Name	Model	
Payment Terminal	DS-K6300X-MFG	13.56 MHz Card Presenting Frequency, Wi-Fi, 2.4G
	DS-K6300X-T-MFG	13.56 MHz Card Presenting Frequency, Wi-Fi, 2.4G
	DS-K6300X-Z-MFG	13.56 MHz Card Presenting Frequency, Wi-Fi, 2.4G

Contents

Chapter 1 Overview 1
1.1 Overview 1
1.2 Features 1
1.3 Appearance 1
1.3.1 Keypad 2
Chapter 2 Installation 3
2.1 Installation Environment 3
2.2 Install with Gang Box 3
2.3 Mount With Cylinder Bracket 9
2.3.1 Preparation before Mounting with Bracket 9
2.3.2 Cylinder Bracket Mounting 11
2.4 Base Mounting 13
Chapter 3 Device Wiring 14
Chapter 4 Activation 15
4.1 Activate via Device 15
4.2 Activate via Web Browser 16
4.3 Activate via SADP 17
4.4 Activate Device via Client Software 18
Chapter 5 Quick Operation 20
5.1 Select Language 20
5.2 Set Password Change Type 22
5.3 Set Application Mode 24
5.4 Set Network Parameters 26
5.5 Access to Platform 28
5.6 Privacy Settings 30
5.7 Set Administrator 32

Chapter 6 Administrator Mode 35
6.1 Login by Administrator 35
6.2 Add Administrator 38
6.3 View Consumer Information 39
6.4 Communication Settings 39
6.4.1 Set Wired Network Parameters 40
6.4.2 Set Wi-Fi Parameters 42
6.4.3 Platform Access 44
6.5 Payment Settings 44
6.6 Basic Settings 44
6.6.1 Voice Settings 46
6.6.2 Time Settings 47
6.6.3 IR Light Brightness Settings 47
6.6.4 Card Security Parameter Settings 47
6.7 Set Biometric Parameters 47
6.8 Data Management 49
6.8.1 Delete Data 49
6.8.2 Import Data 49
6.8.3 Export Data 50
6.9 System Maintenance 50
6.10 Payment Statistics (For Administrator) 52
Chapter 7 Operator Mode 53
7.1 Login by Activation Password 53
7.2 Payment Administrator (For Operator) 54
7.3 Payment Settings (For Operator) 55
7.4 Check Balance 55
Chapter 8 Transaction 57
Chapter 9 Operation via Web Browser 58

9.1 Login 58
9.2 Live View 58
9.3 Search Event 59
9.4 Check Transaction 59
9.5 Configuration 60
9.5.1 Set Local Parameters 60
9.5.2 View Device Information 60
9.5.3 Set Time 60
9.5.4 View Open Source Software License 61
9.5.5 Upgrade and Maintenance 61
9.5.6 Log Query 63
9.5.7 Security Mode Settings 63
9.5.8 Change Administrator's Password 64
9.5.9 Online Users 64
9.5.10 View Device Arming/Disarming Information 64
9.5.11 Network Settings 64
9.5.12 Set Video and Audio Parameters 67
9.5.13 Set Payment Prompt 68
9.5.14 Set Image Parameters 68
9.5.15 General Settings 69
9.5.16 Set Biometric Parameters 71
9.5.17 Set Payment 74
Chapter 10 Client Software Configuration 75
10.1 Configuration Flow of Client Software 75
10.2 Device Management 75
10.2.1 Add Device 76
10.2.2 Reset Device Password 84
10.3 Group Management 84

10.3.1 Add Group 84
10.3.2 Import Resources to Group 85
10.3.3 Edit Resource Parameters 85
10.3.4 Remove Resources from Group 85
10.4 Person Management 86
10.4.1 Add Organization 86
10.4.2 Configure Basic Information 86
10.4.3 Issue a Card by Local Mode 88
10.4.4 Upload a Face Photo from Local PC 90
10.4.5 Take a Photo via Client 91
10.4.6 Collect Face via Access Control Device 92
10.4.7 Collect Fingerprint via Client 93
10.4.8 Collect Fingerprint via Access Control Device 94
10.4.9 Configure Access Control Information 95
10.4.10 Customize Person Information 96
10.4.11 Configure Resident Information 97
10.4.12 Configure Additional Information 97
10.4.13 Import and Export Person Identify Information 98
10.4.14 Import Person Information 98
10.4.15 Import Person Pictures 99
10.4.16 Export Person Information 99
10.4.17 Export Person Pictures 100
10.4.18 Delete Registered Pictures 100
10.4.19 Get Person Information from Access Control Device 100
10.4.20 Move Persons to Another Organization 101
10.4.21 Issue Cards to Persons in Batch 102
10.4.22 Report Card Loss 102
10.4.23 Set Card Issuing Parameters 102

10.5 Configure Schedule and Template 103
10.5.1 Add Holiday 104
10.5.2 Add Template 104
10.6 Set Access Group to Assign Access Authorization to Persons 106
10.7 Configure Advanced Functions 108
10.7.1 Configure Device Parameters 108
10.7.2 Configure Remaining Open/Closed 113
10.7.3 Configure Multi-Factor Authentication 114
10.7.4 Configure Custom Wiegand Rule 117
10.7.5 Configure Person Authentication Mode 118
10.7.6 Configure Card Reader Authentication Mode and Schedule 119
10.7.7 Configure First Person In 121
10.7.8 Configure Anti-Passback 122
10.7.9 Configure Device Parameters 123
10.8 Configure Linkage Actions for Access Control 129
10.8.1 Configure Client Actions for Access Event 129
10.8.2 Configure Device Actions for Access Event 130
10.8.3 Configure Device Actions for Card Swiping 131
10.8.4 Configure Device Actions for Person ID 132
10.9 Control Door Status 133
10.10 Event Center 134
10.10.1 Enable Receiving Event from Devices 134
10.10.2 View Real-Time Events 135
10.10.3 Search Historical Events 137
10.11 System Configuration 140
10.11.1 Set General Parameters 140
10.11.2 Set Picture Storage 142
10.11.3 Set Alarm Sound 142

10.11.4 Set Access Control and Video Intercom Parameters 142
10.11.5 Set File Saving Path 143
10.11.6 Set Email Parameters 143
10.12 Operation and Maintenance 144
Appendix A. Tips for Scanning Fingerprint 146
Appendix B. Tips When Collecting/Comparing Face Picture 148
Appendix C. Tips for Installation Environment 150
Appendix D. Communication Matrix and Device Command 151

Chapter 1 Overview

1.1 Overview

Payment terminal is a kind of face recognition terminal for payment, which supports payment via face, card, etc., and is applicable to department stores, canteens, companies, schools, and other situations.

1.2 Features

- Supports payment via card, face, and QR Code.
- Supports custom payment prompt.
- Supports various payment modes, including fixed amount mode, unfixed amount mode, time count mode, and set meal mode.
- Supports amount correction, refundment and offline-recording.
- Supports checking for IP conflict.
- Supports max. 50,000 payment records and 80,000 user information.
- Supports circulated storage of payment records.
- Supports configuration via local device, client and Web.
- Supports communication via ISAPI.
- Supports time correction via NTP.

1.3 Appearance

Refer to the following contents for detailed information of the payment terminal:

Table 1-1 Description of Payment Terminal

No.	Description
1	Camera
2	Camera
3	IR Light
4	Touch Screen
5	Card Presenting Area
6	IR Light
7	Network Interface
8	Tamper

No.	Description
9	Debugging Port
10	Micro USB Interface **Note** Use micro USB cable to connect with USB interface. Do not insert or plug USB disk during data transfer.
11	SPK Interface
12	PSAM Card Slot (Reserved)
13	Wiring Terminal
14	Loudspeaker
15	USB Interface
16	QR Code Scanner
17	Audio Plug

1.3.1 Keypad

CL: Cancel the payment.

RE: Enter an amount, and press RE to refund.

CE: Clear one digit each press.

OK: Enter an amount, and press OK to collect.

Note

Keypad needs to be purchased separately.

Chapter 2 Installation

2.1 Installation Environment

- Avoid backlight, direct sunlight, and indirect sunlight.
- For better recognition, there should be light source in or near the installation environment.
- The minimum bearing weight of the wall or other places should be 3 times heavier than the device weight.
- There shall be no strong reflective objects (such as glass doors/walls, stainless steel objects, acrylic and other glossy plastics, lacquer, ceramic tiles, etc.) within 1 m of the field of view of the device.
- Avoid device reflection.
- Face recognition distance shall be greater than 30 cm.
- Keep the camera clean.

Note

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

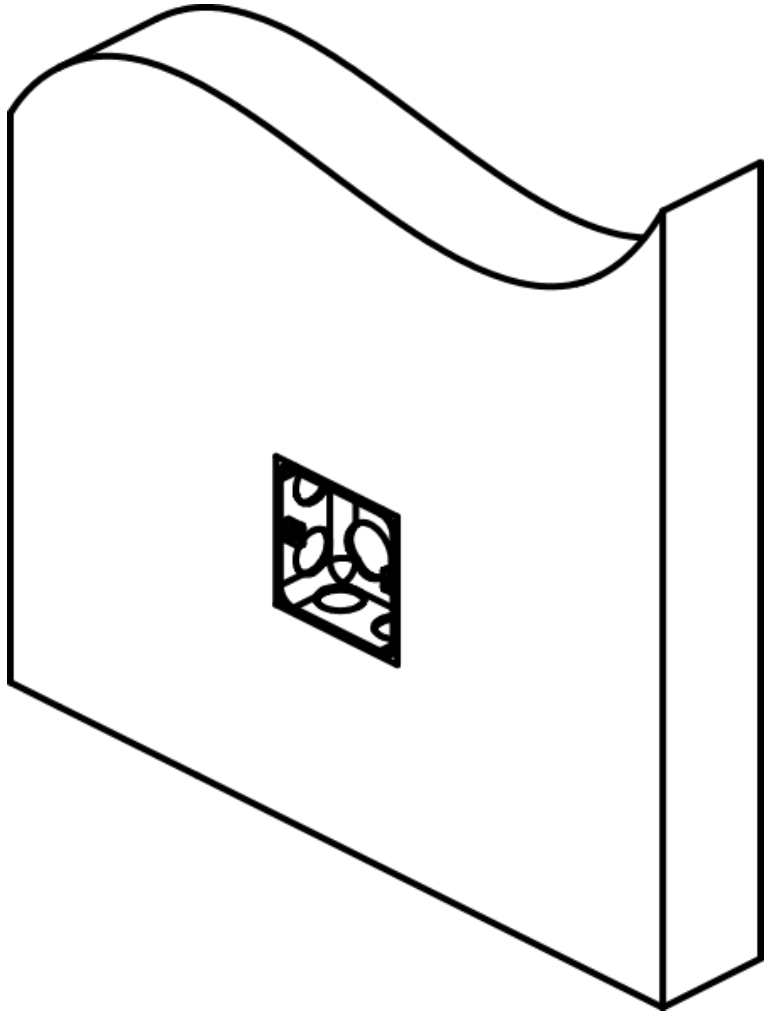
2.2 Install with Gang Box

Steps

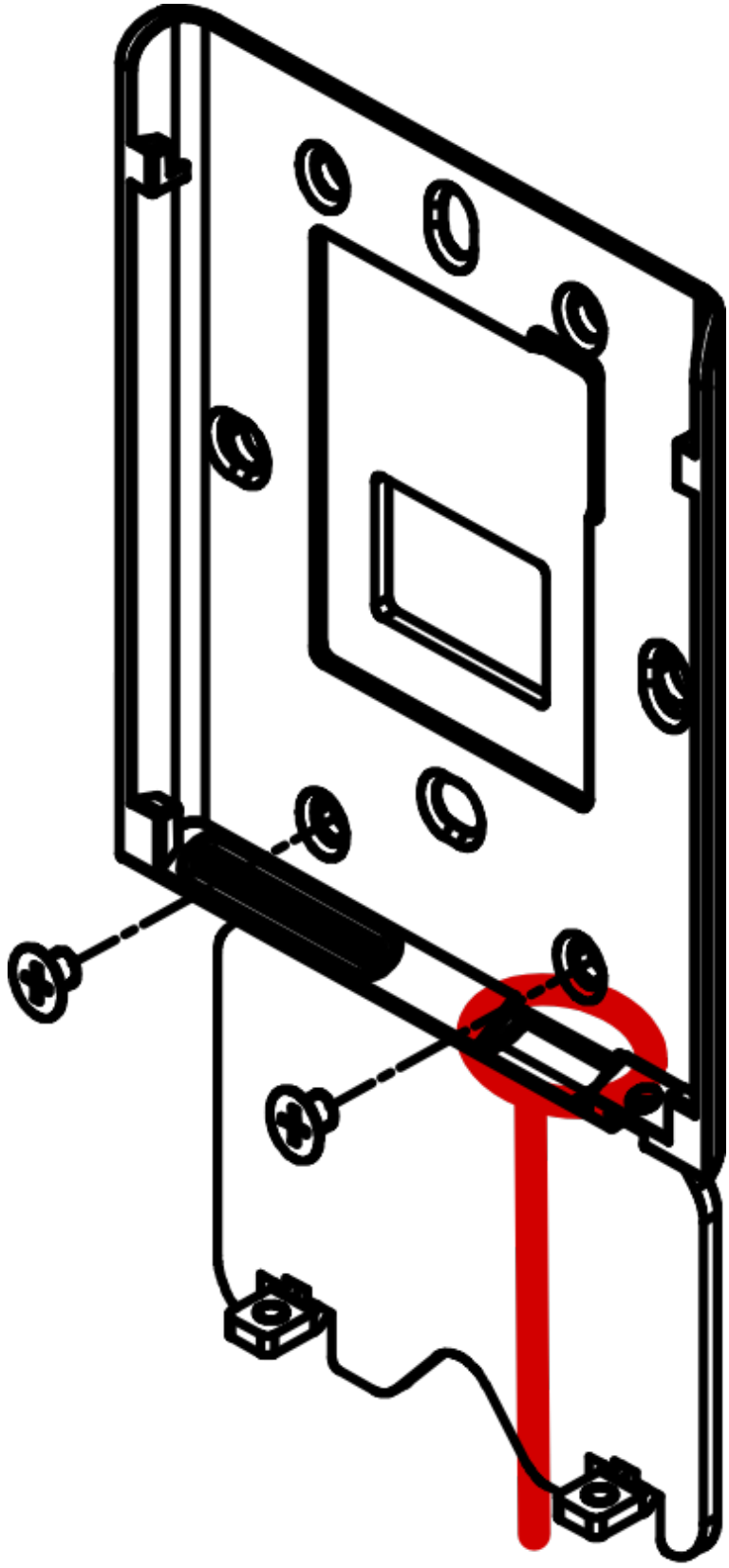
1. Make sure the gang box is installed on the wall.

   Note

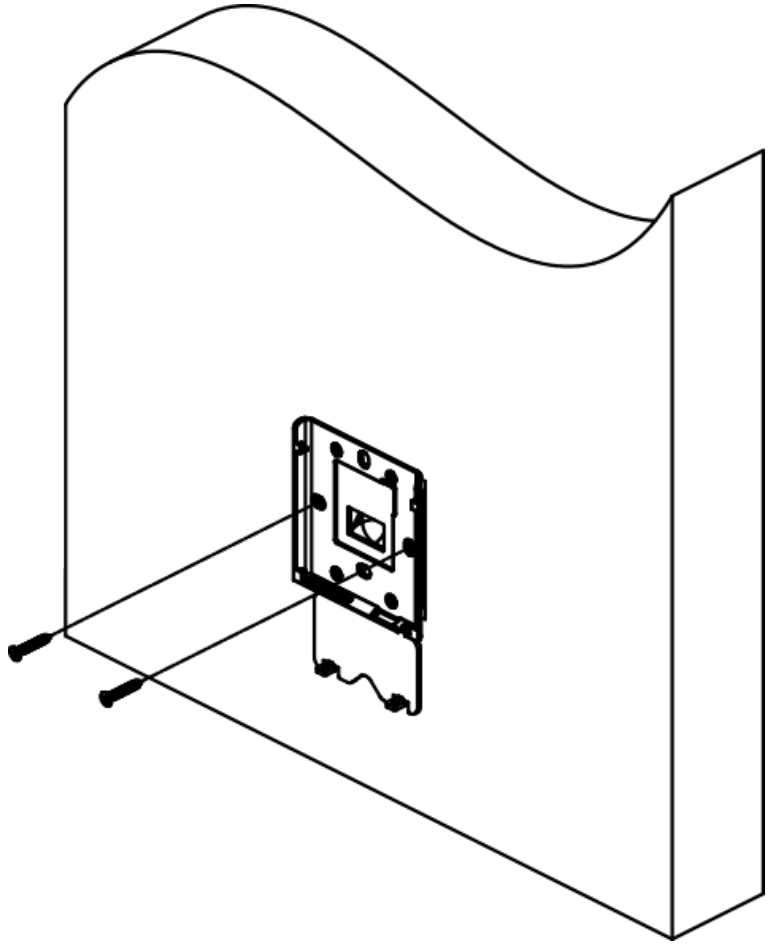
   Gang box is not supplied.



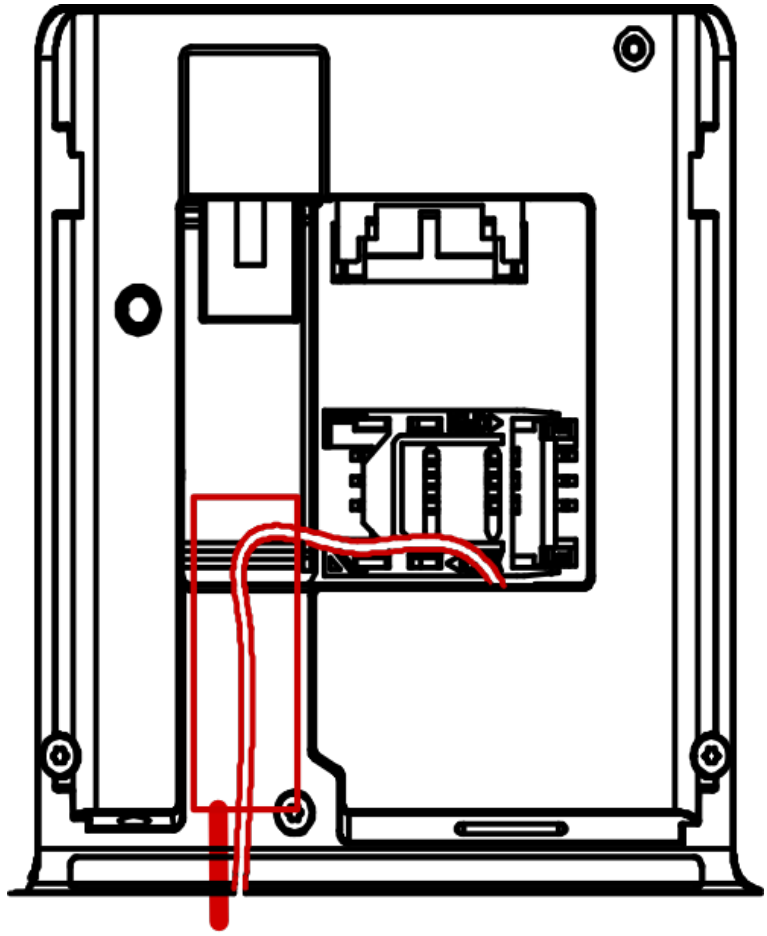
2. Remove the notch on the mounting plate to leave the cable hole. Secure the mounting plate on the switching plate with two supplied screws (SC-K1M4×4-BNI-SUS316).


Notch

3. Align the plate hole with the gang box hole. Secure the mounting plate on the wall with two supplied screws (SC-KA4×22-SUS).



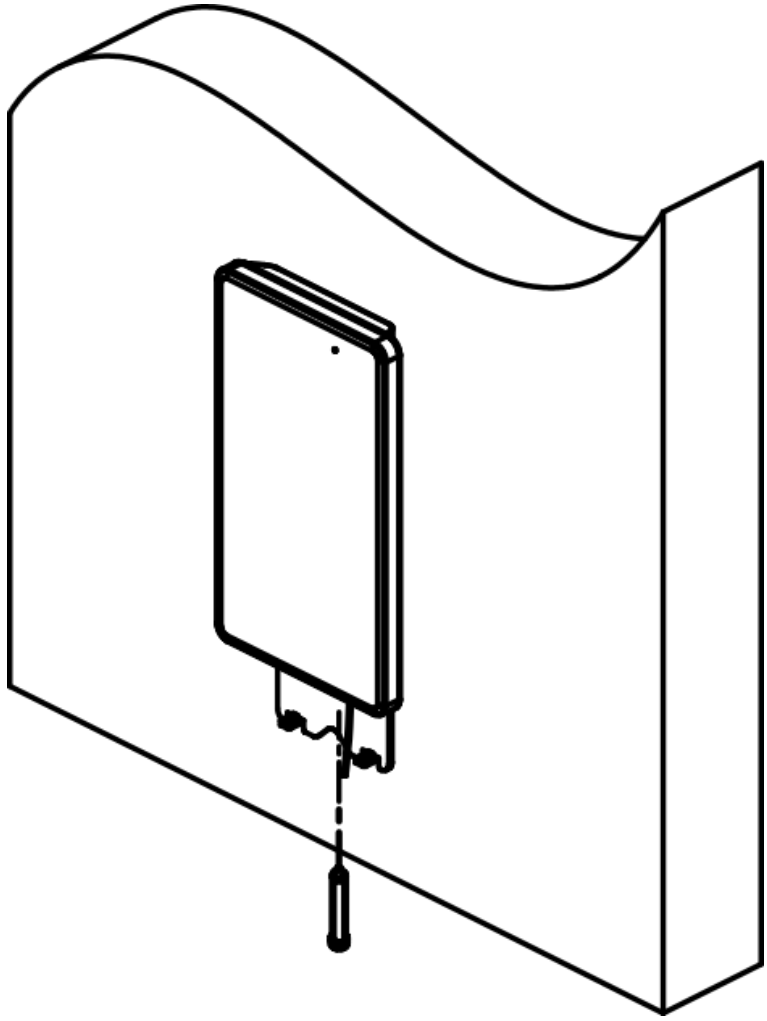
4. Wire the audio cable, and route the cable through the cable hole.



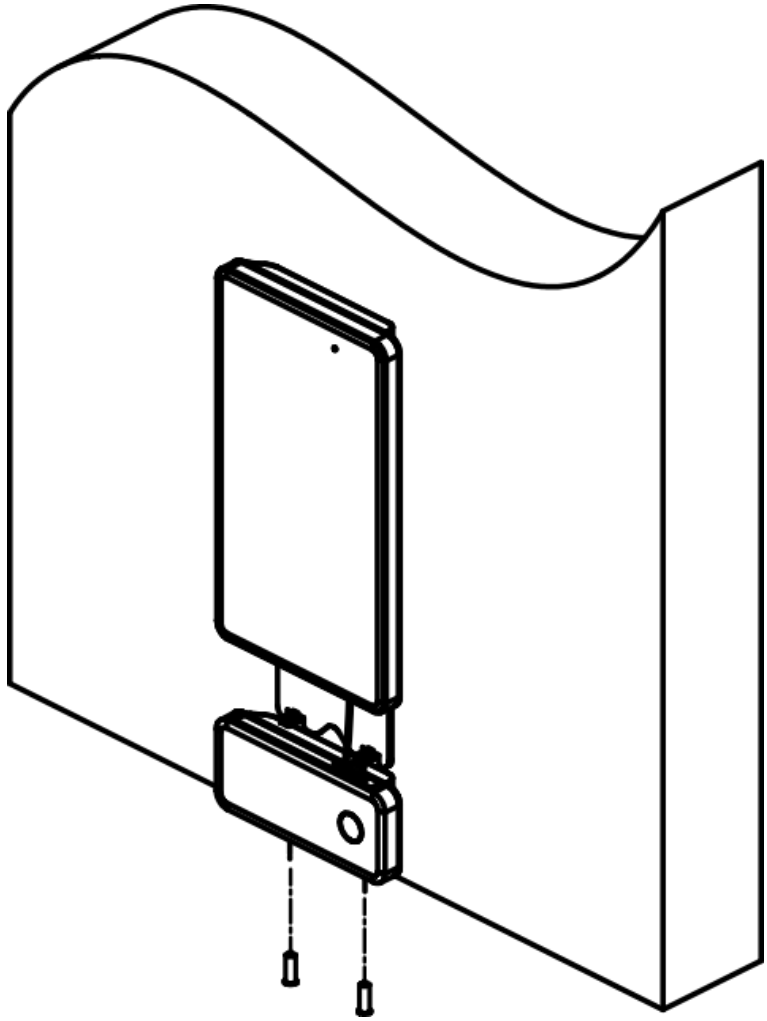
5. Hang the device on the mounting plate from top to bottom in a vertical direction, and secure the device on the mounting plate with 1 supplied screw (SC-KM3X6-H2-SUS).

Note

Audio cable should be routed from the cable hole to avoid being pressed by the mounting plate.



6. Insert the audio cable into the peripheral module, and insert the module into device from top to bottom in a vertical direction. Secure the peripheral module on the mounting plate with 2 supplied screws (SC-KM3X6-H2-SUS).



2.3 Mount With Cylinder Bracket

2.3.1 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.

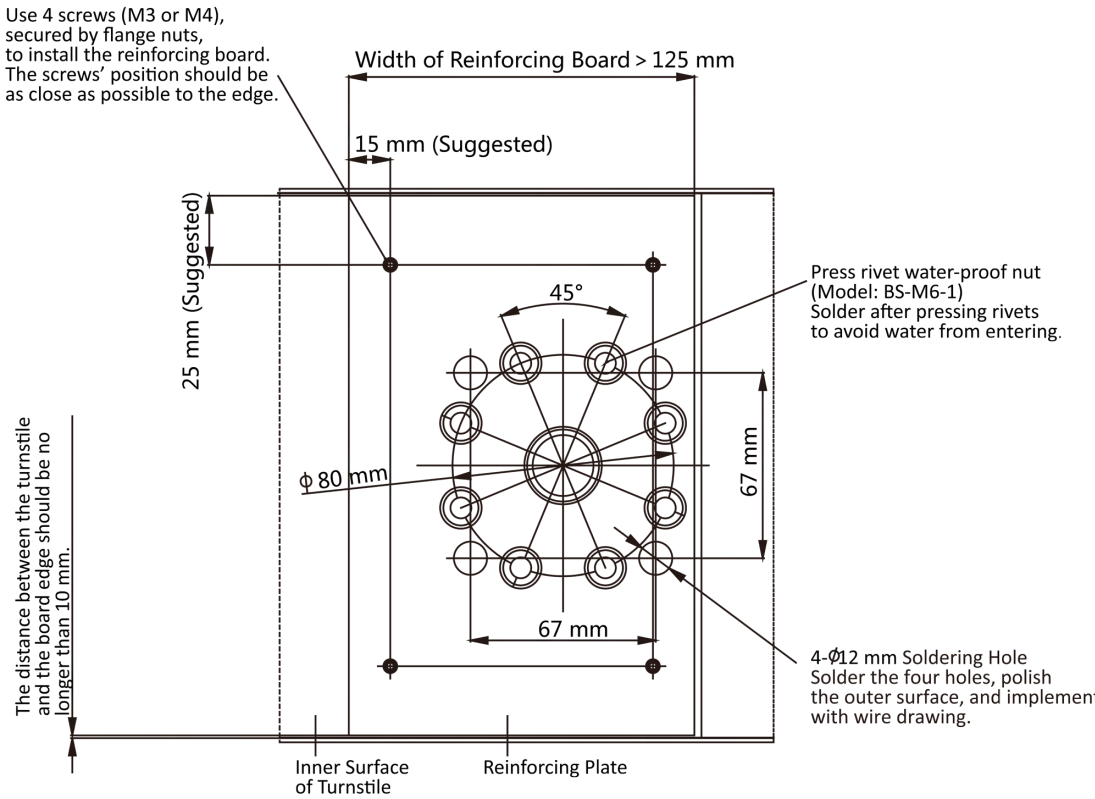


Figure 2-1 Drill Holes on Turnstile

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.

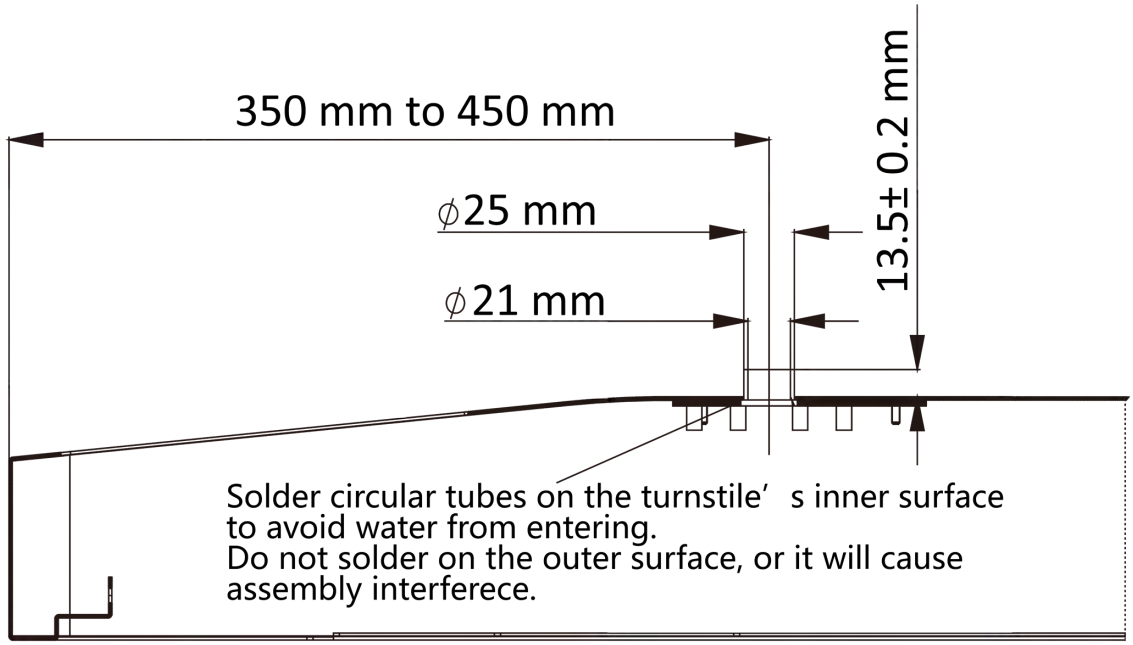
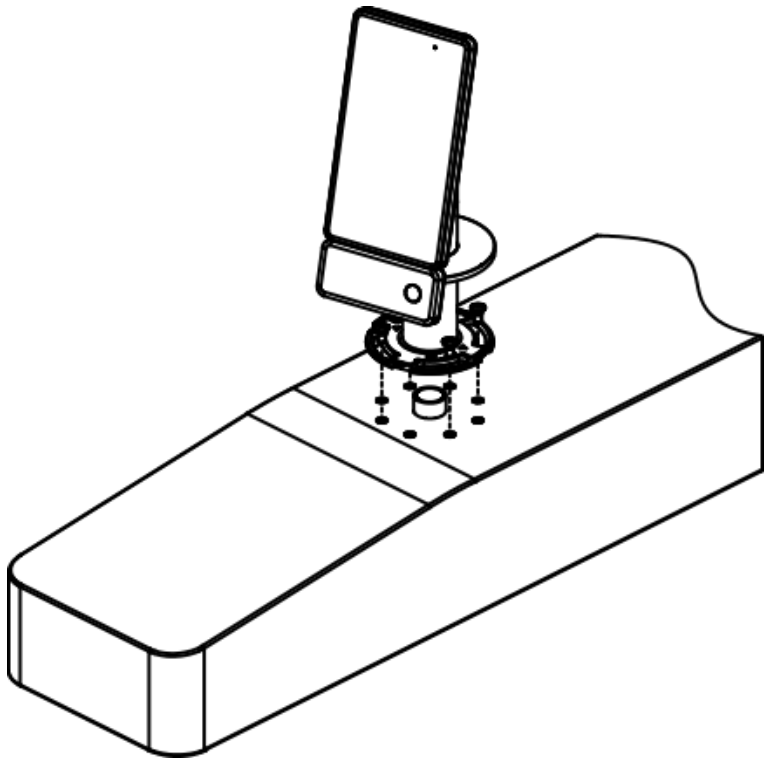


Figure 2-2 Solder Tubes

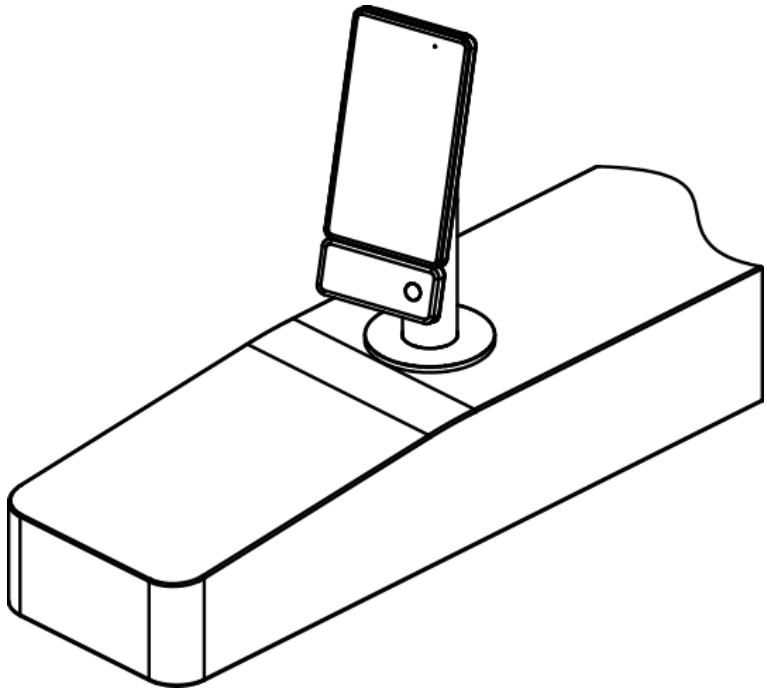
2.3.2 Cylinder Bracket Mounting

Steps

1. Rotate to open the lower cover.
2. Route all cables through the cable hole on the turnstile. Align the holes with those on the turnstile. Secure the rack on the turnstile with 4 supplied screws (SC-OM6×12-H-SUS).



3. Cover the lower cover on the base and rotate to secure.



4. Loosen the screws inside and adjust the device elevaon. Aer adjustment, secure the screws and install the upper cover.

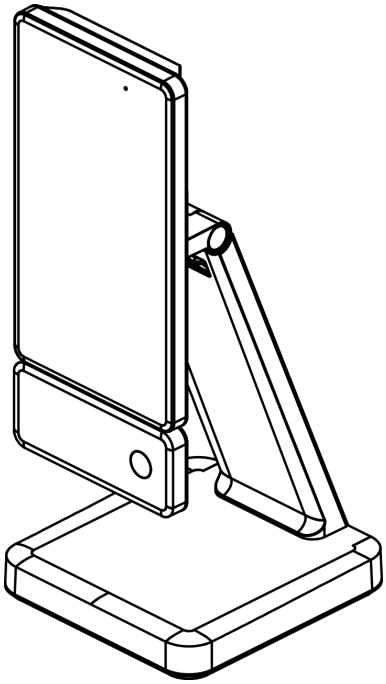
Note

The elevation can be 0° or 15° (default).

2.4 Base Mounting

Steps

1. Set the device flat in a proper place.



2. (Optional) Connect to external keypad.
3. Plug the power cable into the power input interface. After powering on, the device will enter the main interface.

Chapter 3 Device Wiring

Connect the device to the power supply with the supplied power cable.

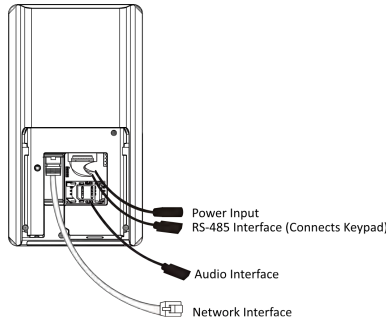


Figure 3-1 Device Wiring

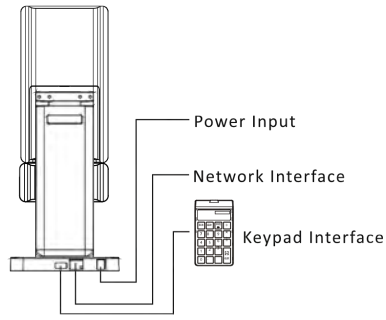


Figure 3-2 Base Mounting Wiring

Chapter 4 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

4.1 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 4-1 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.

4.2 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.

4.3 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.

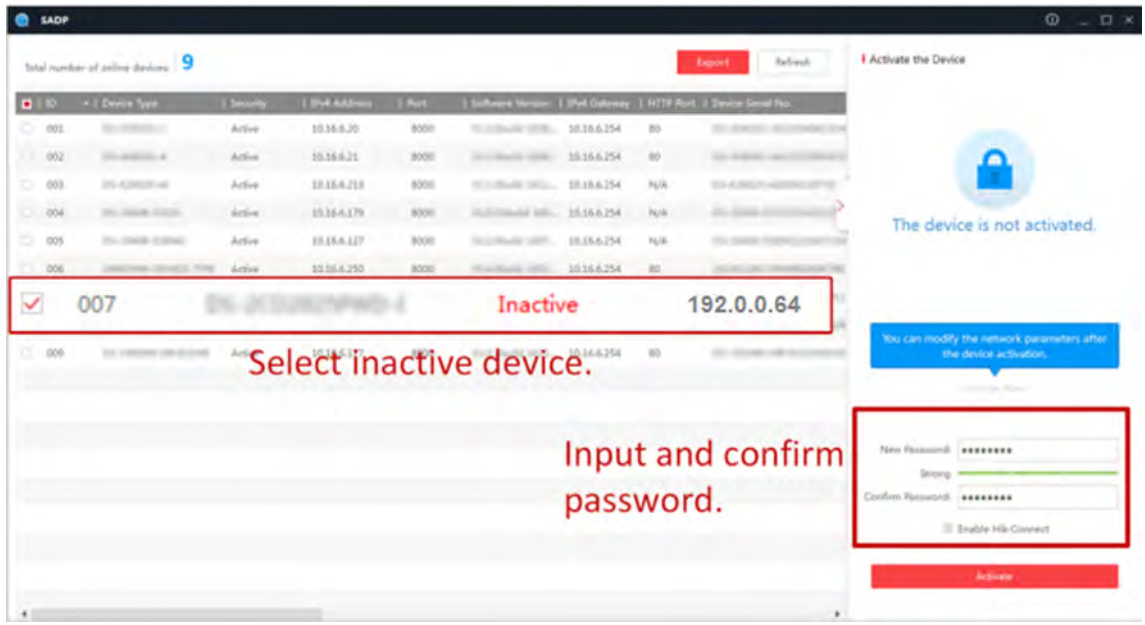
Caution

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.

4.4 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.

Chapter 5 Quick Operation

5.1 Select Language

You can select a language for the device system.

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

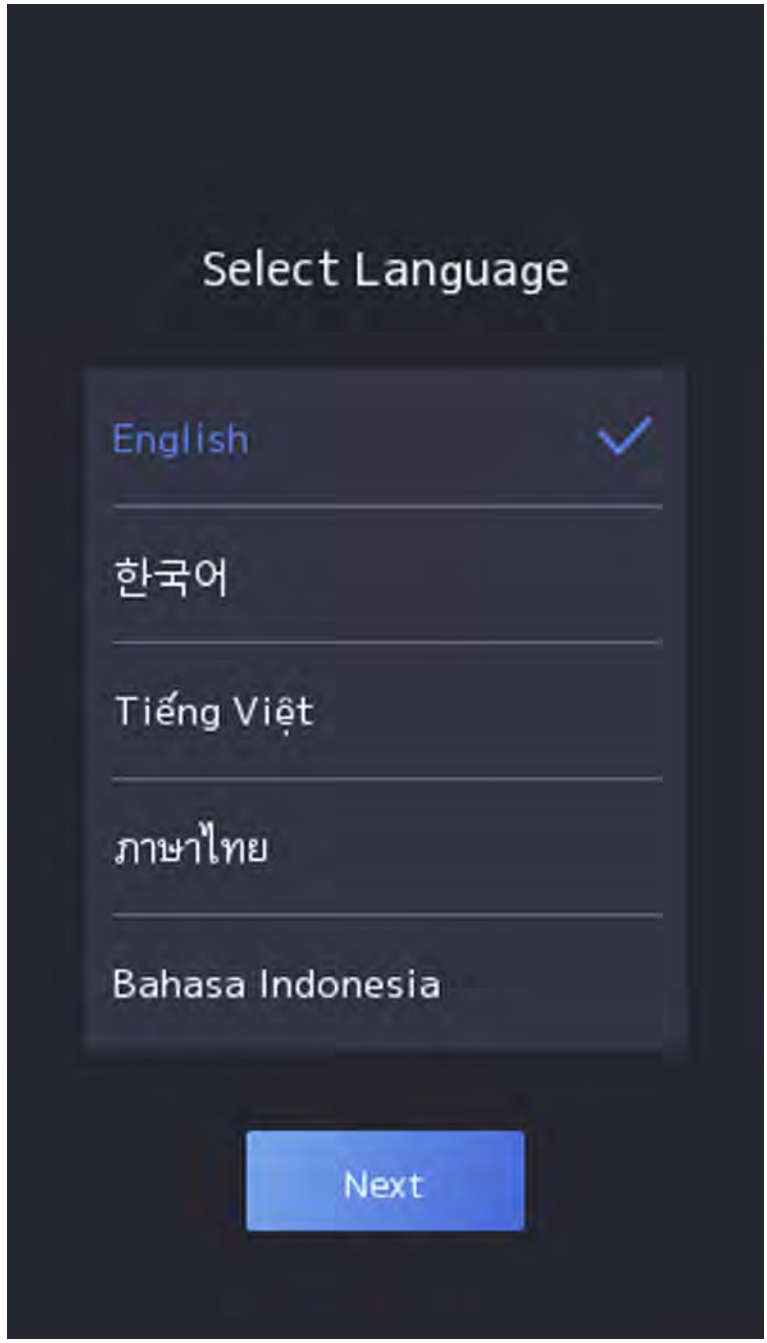


Figure 5-1 Select System Language

By default, the system language is English.

Note

After you change the system language, the device will reboot automatically.

5.2 Set Password Change Type

After activating the device, you can set the password change type as reserved email address or security questions. Once you forgot the device password, you can change the password via the selected change type.

Change Password via Email Address

If you need to change password via reserved email, you can enter an email address, and tap **Next**.

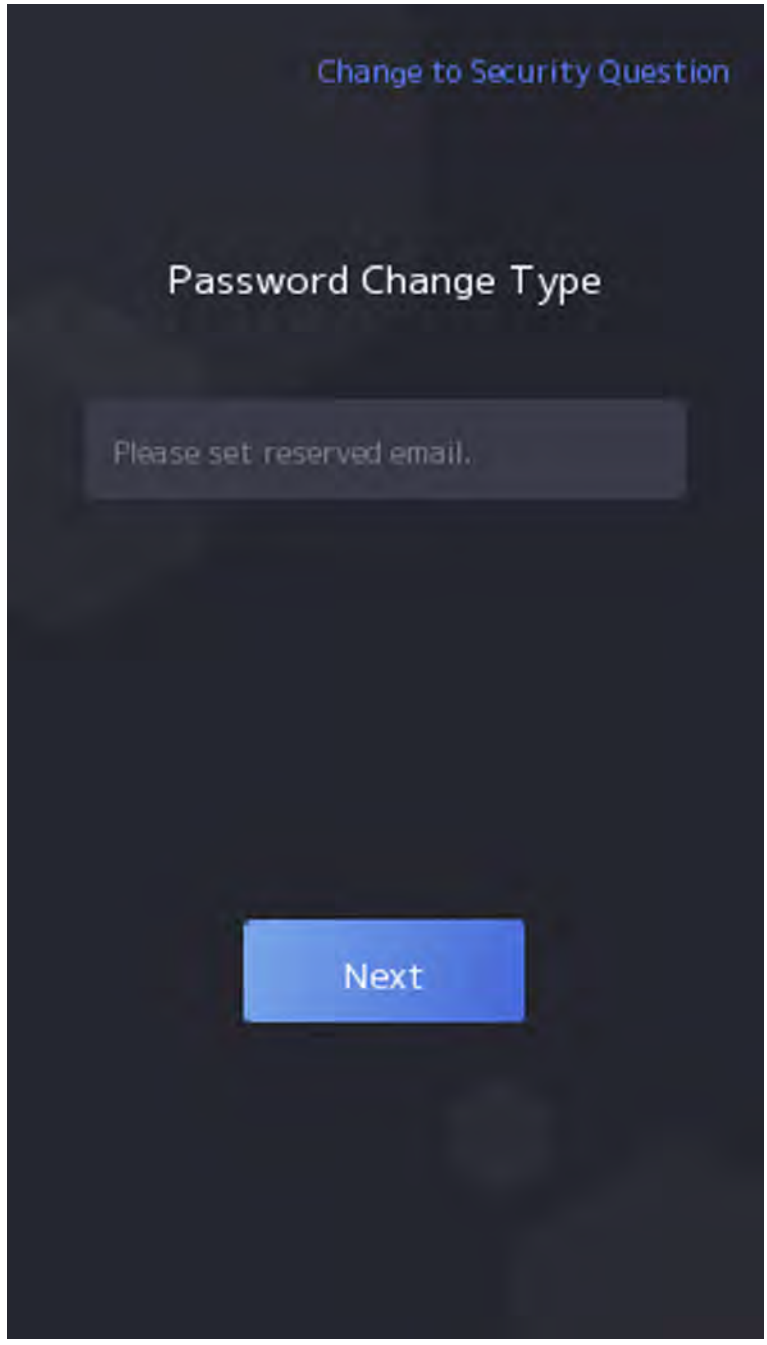


Figure 5-2 Password Change Page

Change via Security Questions

If you need to change password via security questions, you can tap **Change to Security Questions** on the right corner. Select the security questions and enter the answers. Click **Next**.

Note

You can only select one type to change password. If you need, you can enter the web page to set both of the changing types.

5.3 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.

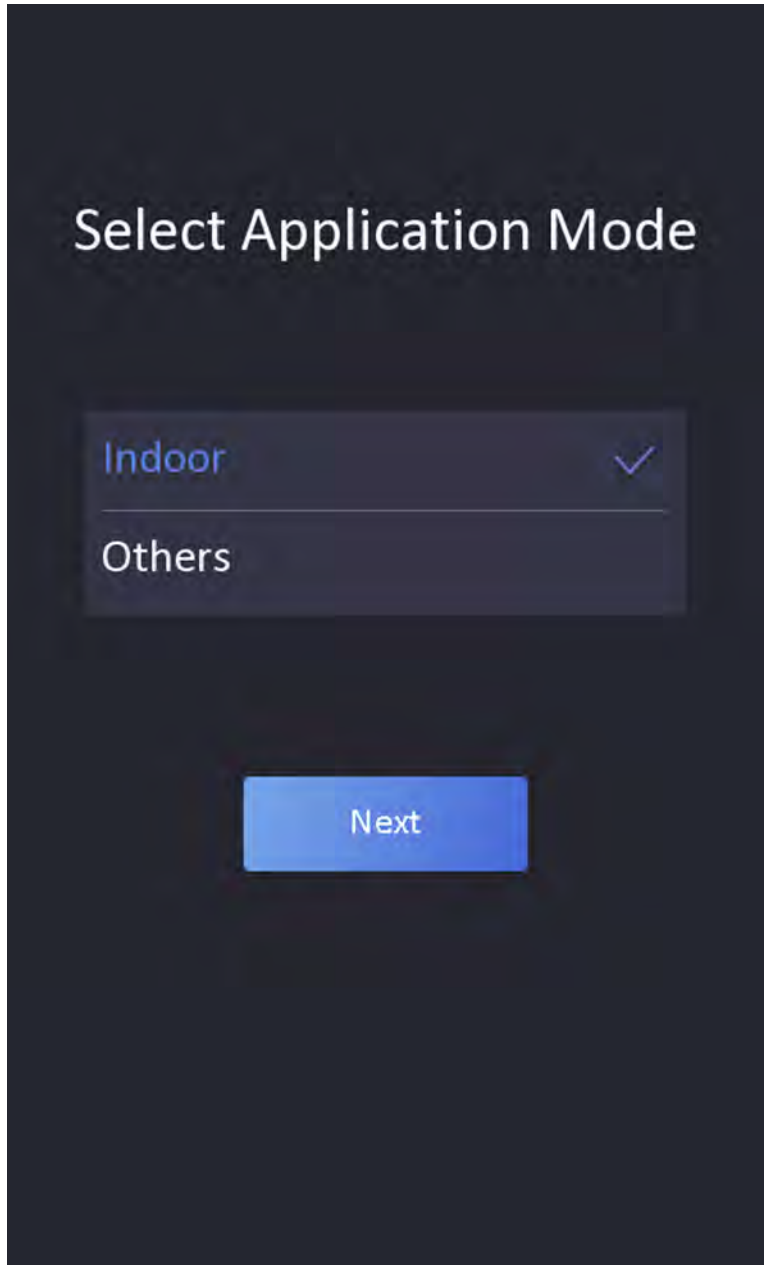


Figure 5-3 Welcome Page

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.

5.4 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.

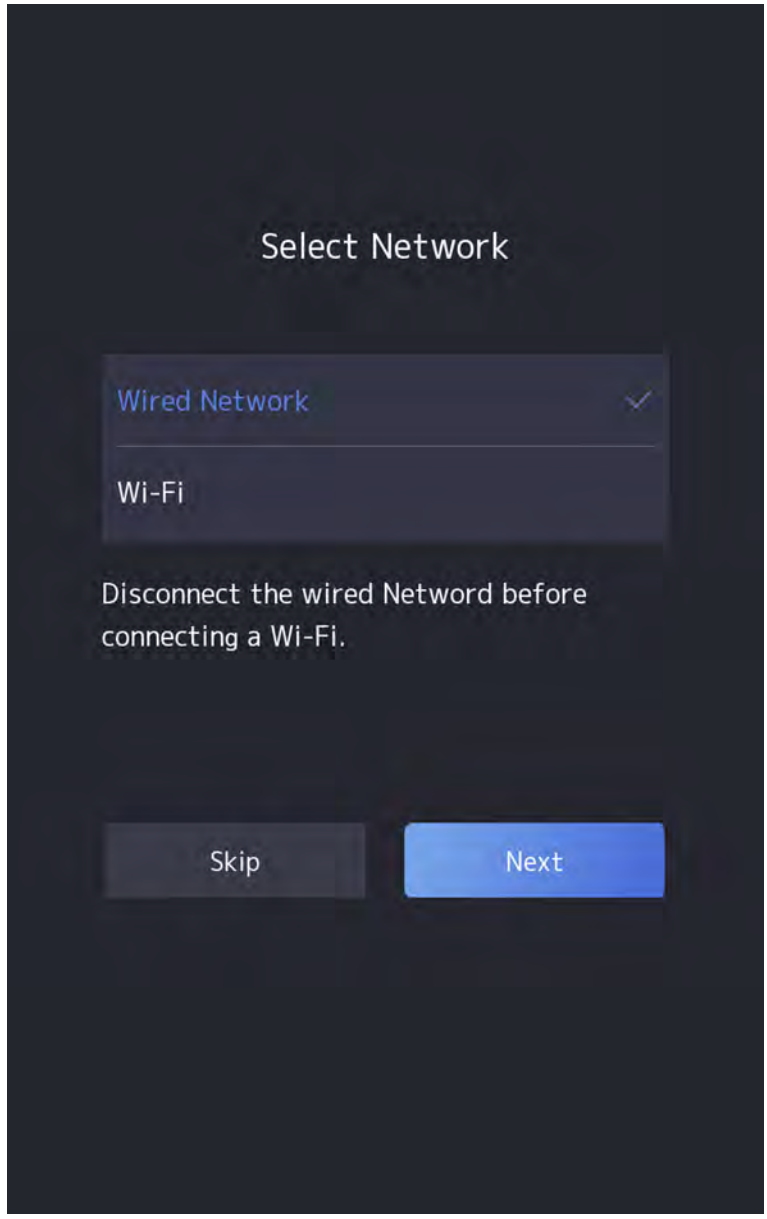


Figure 5-4 Select Network

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.

5.5 Access to Platform

Enable the function and the device can communicate via Hik-Connect. You can add the device to Hik-Connect modile client and so on.

Steps

1. Enable **Access to Hik-Connect**, and set the server IP and verification code.

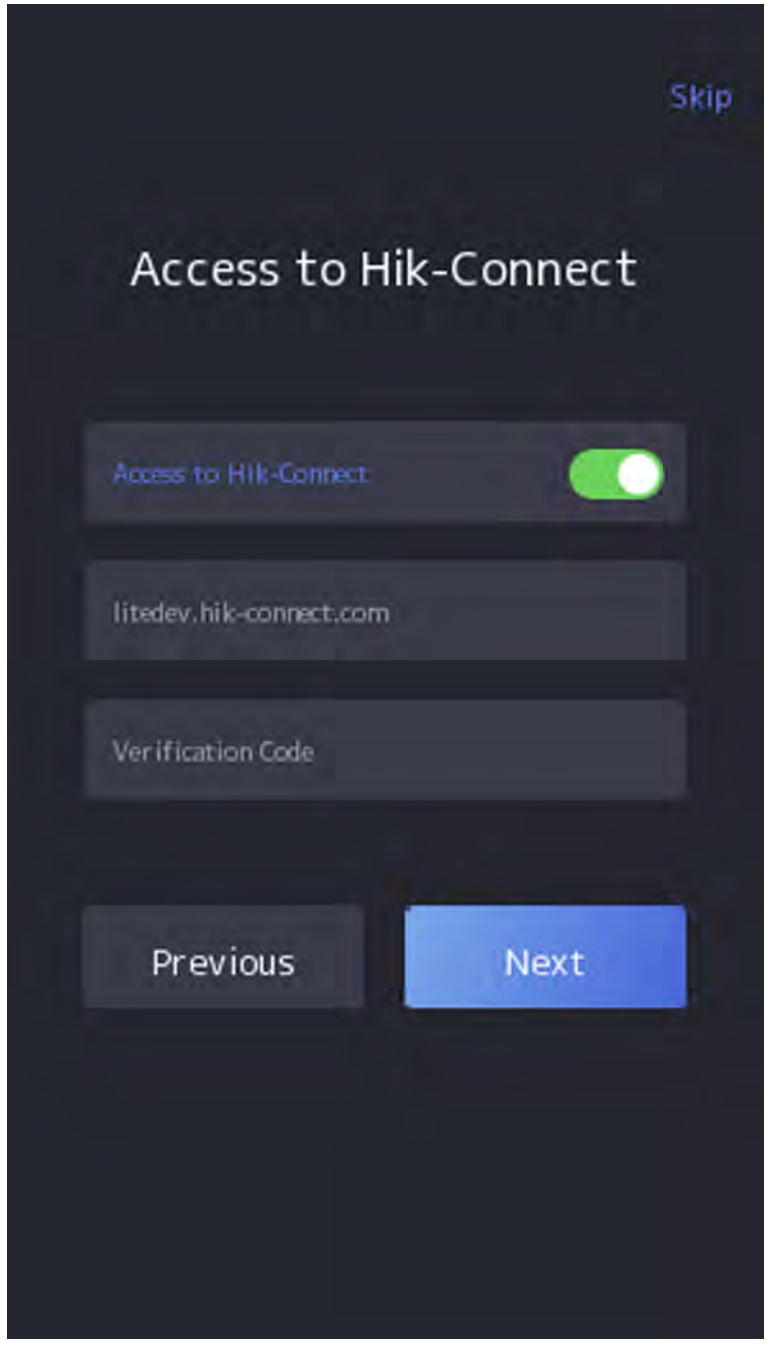


Figure 5-5 Access to Hik-Connect

2. Tap **Next**.
3. **Optional:** Tap **Skip** to skip the step.
4. **Optional:** Tap **Previous** to go to the previous page.

Note

If you tap **Previous** to return to the Wi-Fi configuration page, you need to tap the connected Wi-Fi or connect another Wi-Fi to enter the platform page again.

5.6 Privacy Settings

After activation, selecting application mode, and selecting network, you should set the privacy parameters, including the picture uploading and storage.

Select parameters according to your actual needs.

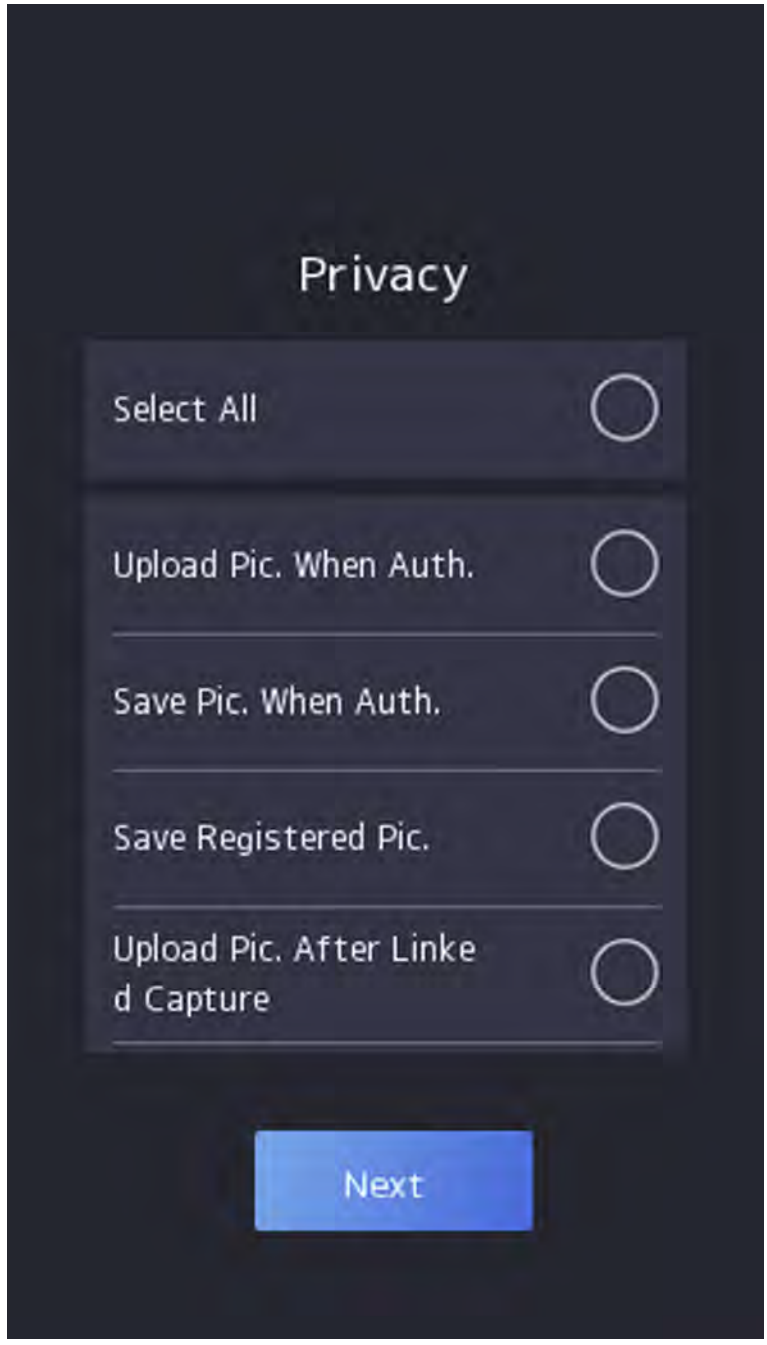


Figure 5-6 Privacy

Upload Captured Pic. When Auth. (Upload Captured Picture When Authenticating)

Upload the pictures captured when authenticating to the platform automatically.

Save Captured Pic. When Auth. (Save Captured Picture When Authenticating)

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

Save Registered Pic. (Save Registered Picture)

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

Upload Pic. After Linked Capture (Upload Picture After Linked Capture)

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

Save Pic. After Linked Capture (Save Pictures After Linked Capture)

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

Tap **Next** to complete the settings.

5.7 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**.

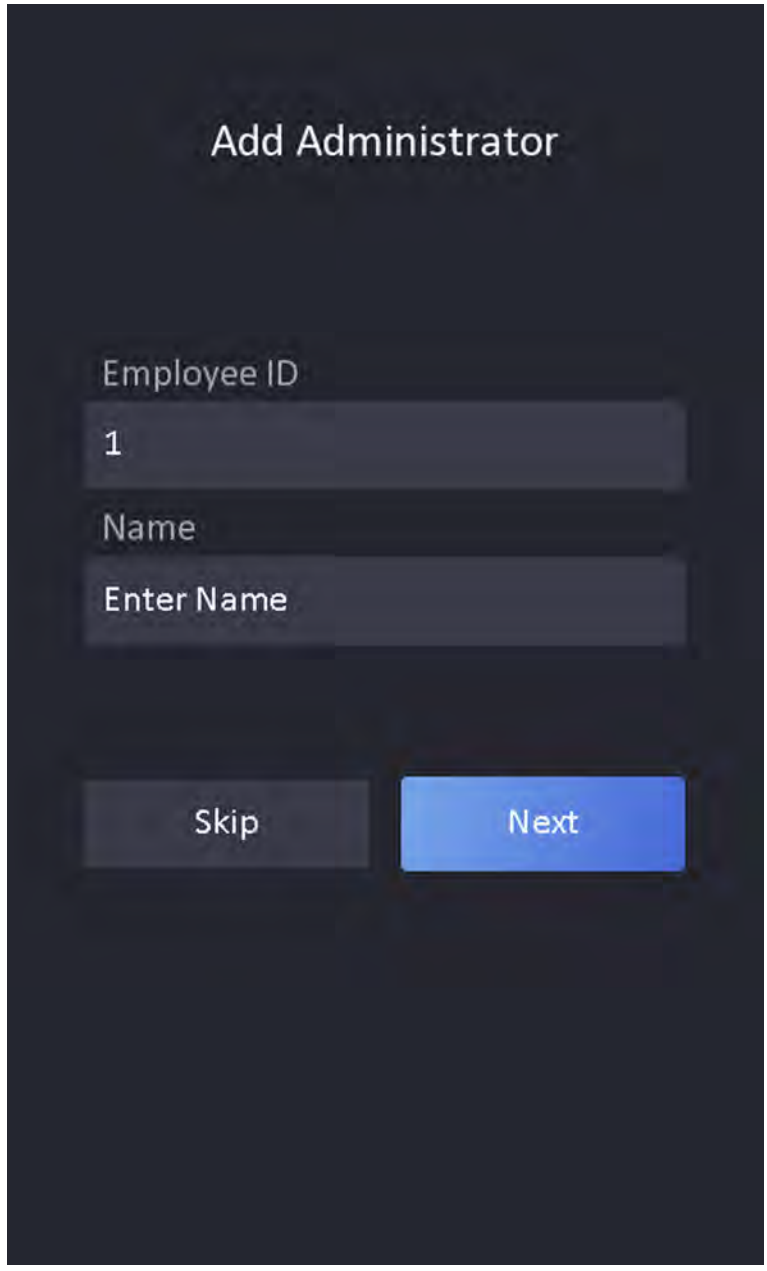


Figure 5-7 Add Administrator Page

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.
- : Press your finger according to the instructions on the device screen. 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*** .

Scan QR code to authenticate.

Note

The QR code can be obtained from the visitor terminal.

- 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 6 Administrator Mode

6.1 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.

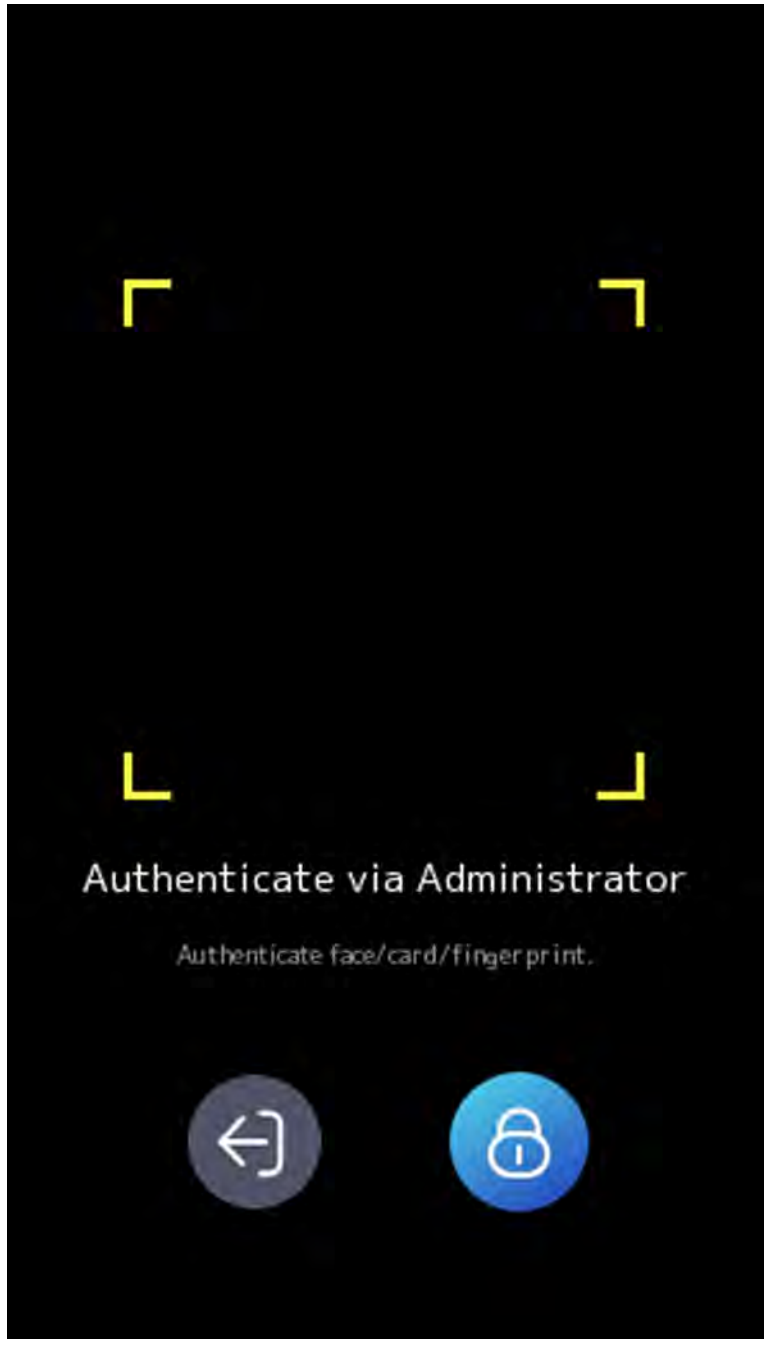


Figure 6-1 Admin Login

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

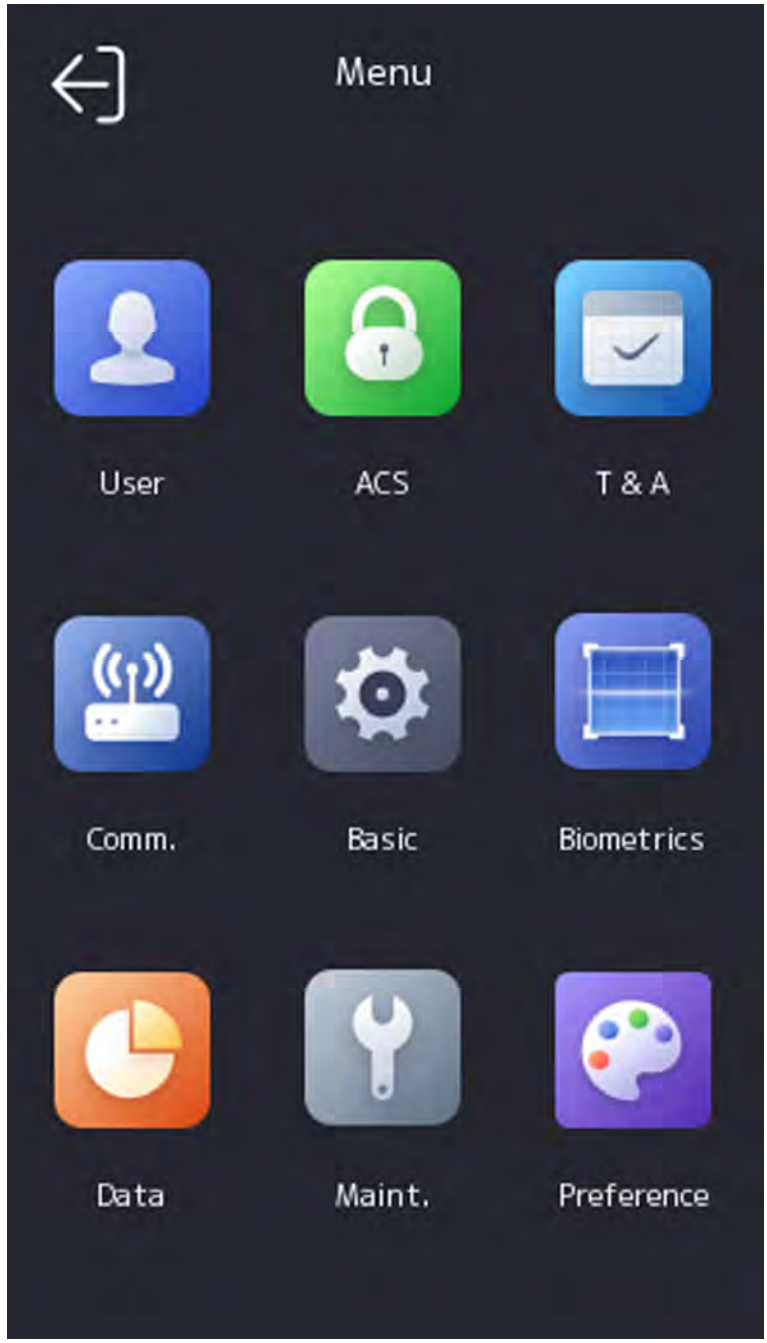


Figure 6-2 Home Page

Note

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

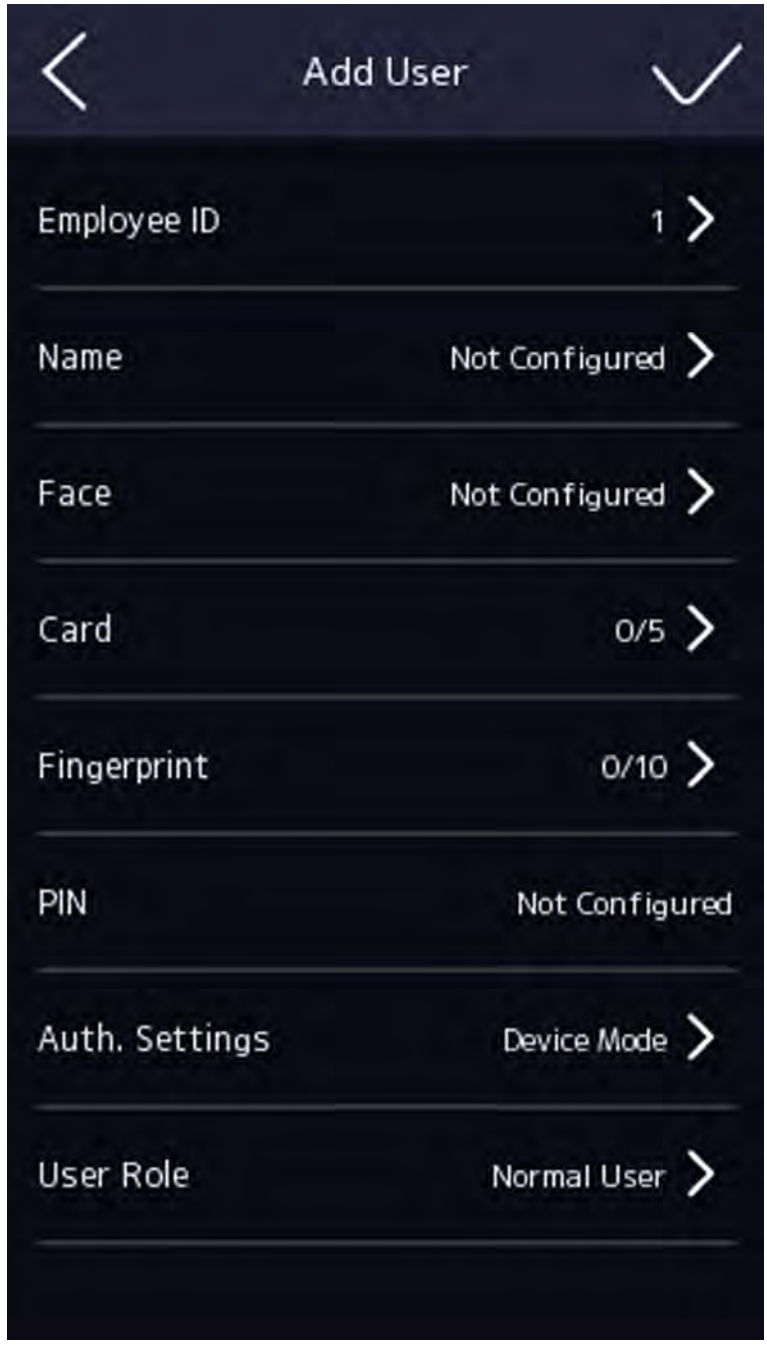
3. **Optional:** Tap and you can enter the device activation password for login.
4. **Optional:** Tap and you can exit the admin login page.

6.2 Add Administrator

The administrator can log in the device backend and configure the device parameters.

Steps

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



3. Edit the employee ID.

Note

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

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

Note

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

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

Note

- For details about adding a face picture, see .
- **Note**

  For details about adding a fingerprint, see .
- For details about adding a card, see .
- For details about adding a password, see .

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

Note

For details about setting the authentication type, see .

7. Enable the Administrator Permission function.

   Enable Administrator Permission

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

8. Tap ✓ to save the settings.

6.3 View Consumer Information

Enter a short description of your concept here (optional).

This is the start of your concept.

6.4 Communication Settings

You can set the wired network, the Wi-Fi parameter, and access to Hik-Connect on the communication settings page.

6.4.1 Set Wired Network Parameters

You can set the device wired network parameters, including the IPv4/IPv6 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**.

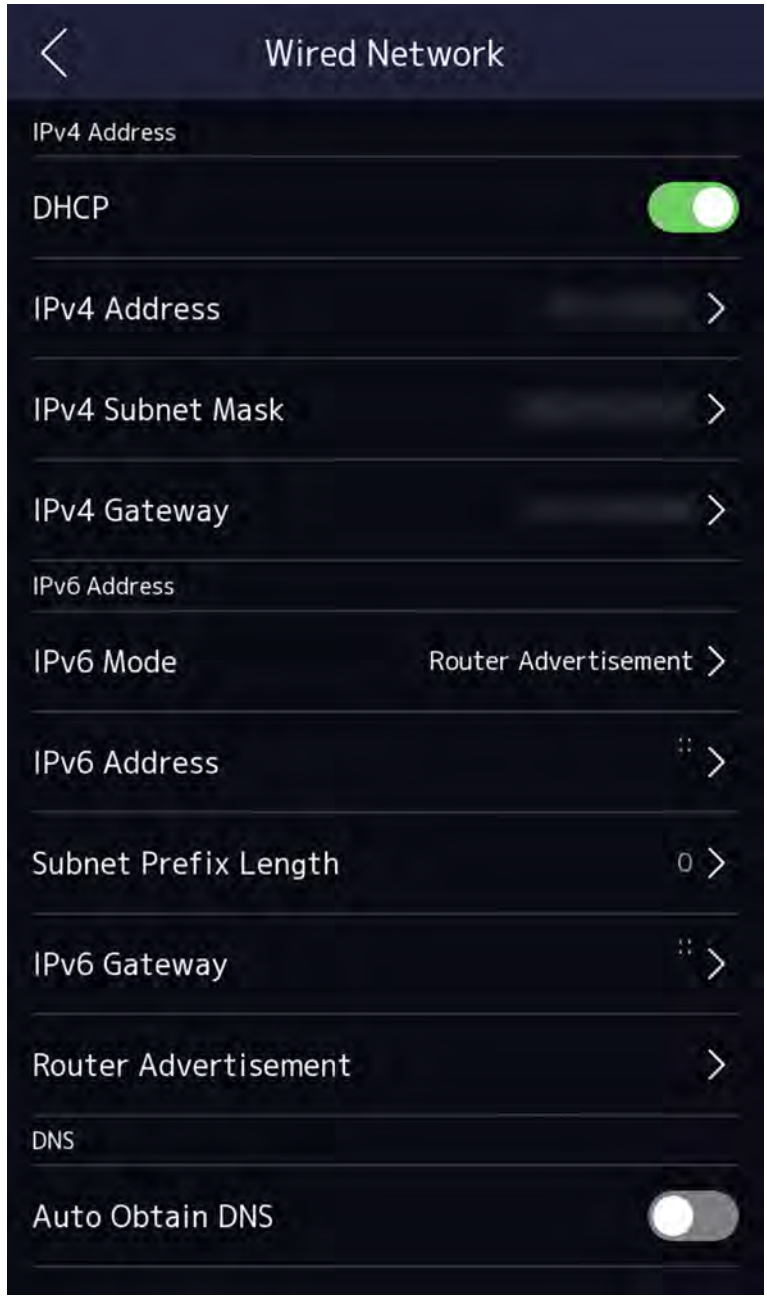


Figure 6-3 Wired Network Settings

3. Set IPv4/IPv6 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.

6.4.2 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 **Communication** on the Home page to enter the Communication Settings page.
2. On the Communication Settings page, tap.

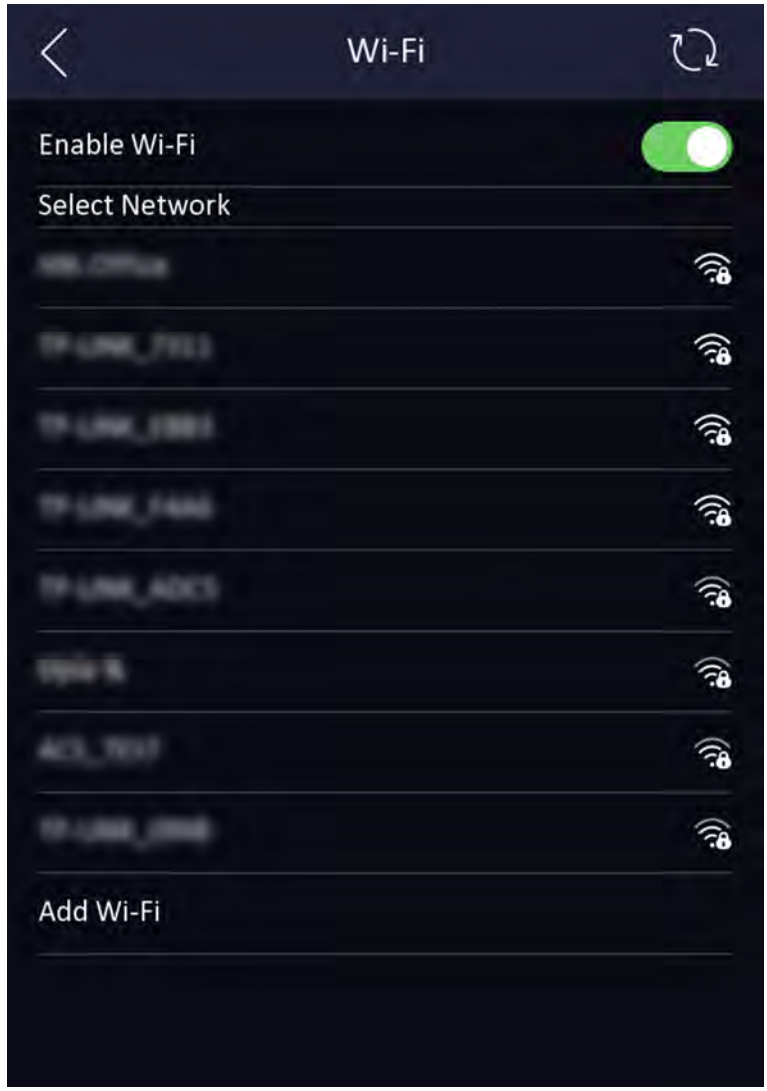


Figure 6-4 Wi-Fi Settings

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.

6.4.3 Platform Access

You can change the device verification code before you add the device to the Hik-Connect mobile client.

Before You Start
Make sure your device has connected to a network.

Steps
1. Tap **Communication** on the Home page to enter the Communication Settings page.
2. On the Communication Settings page, tap **Hik-Connect**.
3. Enable **Hik-Connect**
4. Create the **Verification Code**, and you need to enter the verification code when you manage the devices via **Hik-Connect**.

6.5 Payment Settings

Enter a short description of your task here (optional).

Before You Start
Enter the prerequisites here (optional).
Enter the context of your task here (optional).

Steps
1. Enter your first step here.
   Enter the result of your step here (optional).

Example
Enter an example that illustrates the current task (optional).

What to do next
Enter the tasks the user should do after finishing this task (optional).

6.6 Basic Settings

You can set the shortcut key, theme, voice settings, time settings, sleeping (s), community No., building No., Unit No., and beauty.

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**.

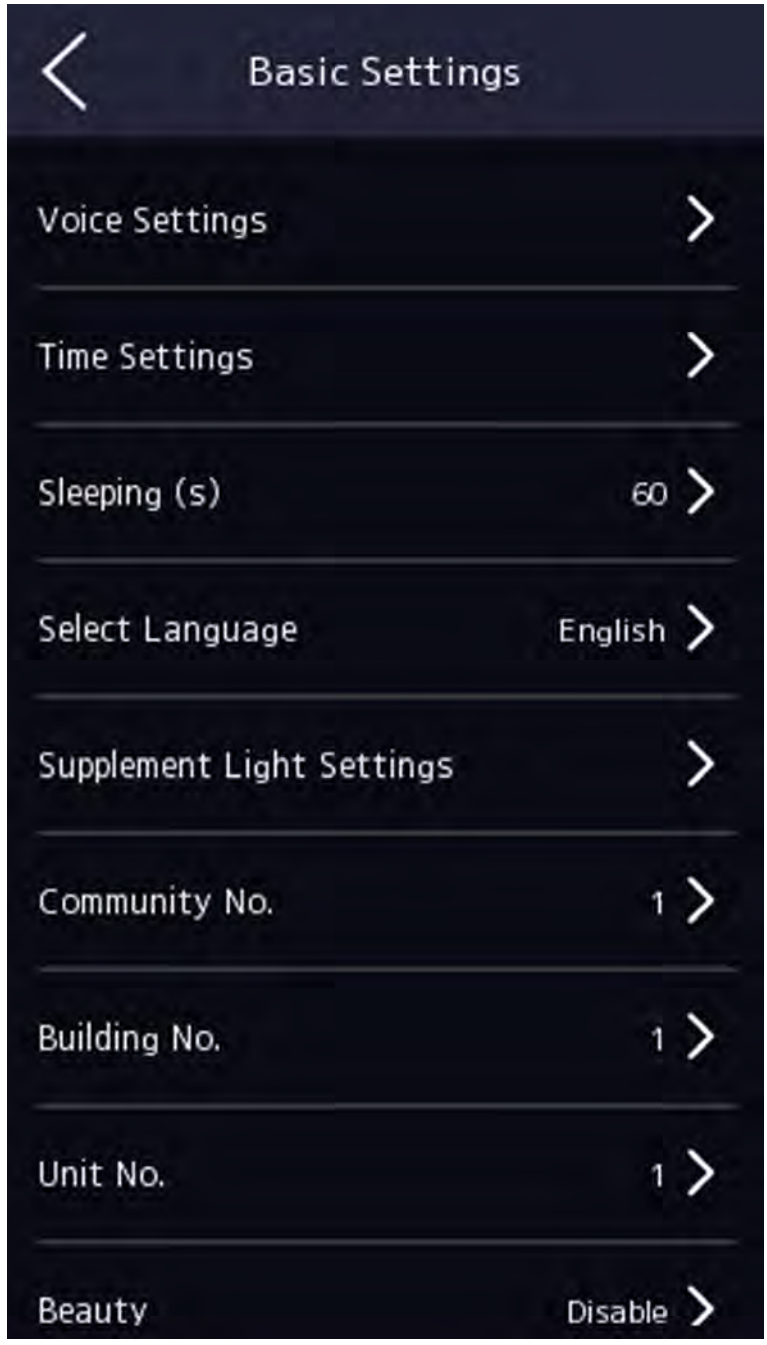


Figure 6-5 Basic Settings Page

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.

Sleeping (s)

Set the device sleeping waiting time (minute). When you are on the initial page and if you set the sleeping time to 30 min, the device will sleep after 30 min without any operation.

Note

If you set the sleeping time to 0, the device will not enter sleeping mode.

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.

Beauty

You can enable the beauty function and set the smooth and the whiten parameter. Tap **+** or **-** to control the effect strength.

Note

By default, the function is disabled.

6.6.1 Voice Settings

Enter a short description of your task here (optional).

Before You Start

Enter the prerequisites here (optional).
Enter the context of your task here (optional).

Steps

1. Enter your first step here.
   Enter the result of your step here (optional).

Example

Enter an example that illustrates the current task (optional).

What to do next
Enter the tasks the user should do after finishing this task (optional).

6.6.2 Time Settings

Enter a short description of your task here (optional).

Before You Start
Enter the prerequisites here (optional).
Enter the context of your task here (optional).

Steps
1. Enter your first step here.
   Enter the result of your step here (optional).

Example
Enter an example that illustrates the current task (optional).

What to do next
Enter the tasks the user should do after finishing this task (optional).

6.6.3 IR Light Brightness Settings

Enter a short description of your concept here (optional).

This is the start of your concept.

6.6.4 Card Security Parameter Settings

Enter a short description of your concept here (optional).

This is the start of your concept.

6.7 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, face with mask detection and multiple faces authentication.

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

Table 6-1 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** 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)**

Parameter	Description
	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.
Multiple Faces Authentication	After multiple faces authentication is enabled, multiple faces authentication is supported.

6.8 Data Management

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

6.8.1 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.

6.8.2 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**, **Face Data** or **Access Control Parameters** .

   Note

   The imported access control parameters are configuration files of the device.
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.

6.8.3 Export Data

Steps

1. Plug a USB flash drive in the device.
2. On the Home page, tap **Data → Export Data** .
3. Tap **Face Data**, **Event Data**, **User Data**, or **Access Control Parameters**.

   Note

   The exported access control parameters are configuration files of the device.
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.

6.9 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.

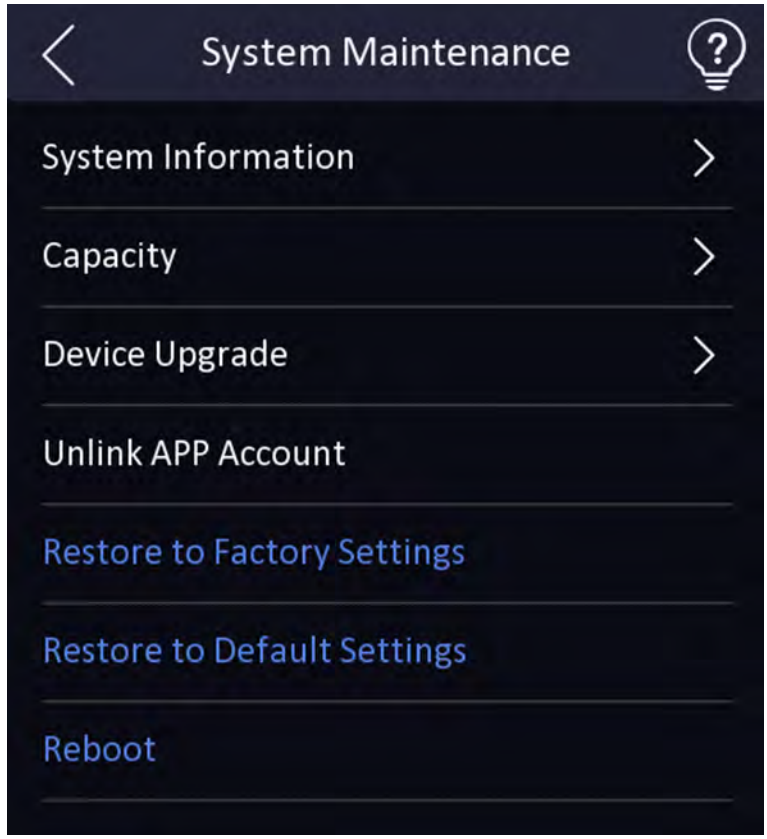


Figure 6-7 Maintenance Page

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, event and fingerprint.

Note

Parts of the device models support displaying the fingerprint number. Refers to the actual page for details.

Device Upgrade

Online Update

If the device has been connected to Hik-Connect and network, when there is a new installation package in Hik-Connect, you can tap **Device Upgrade → Online Update** to upgrade the device system.

Update via USB

Plug the USB flash drive in the device USB interface. Tap **Device Upgrade → Update via USB** , 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.

6.10 Payment Statistics (For Administrator)

Enter a short description of your task here (optional).

Before You Start

Enter the prerequisites here (optional).
Enter the context of your task here (optional).

Steps

1. Enter your first step here.
   Enter the result of your step here (optional).

Example

Enter an example that illustrates the current task (optional).

What to do next

Enter the tasks the user should do after finishing this task (optional).

Chapter 7 Operator Mode

7.1 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.

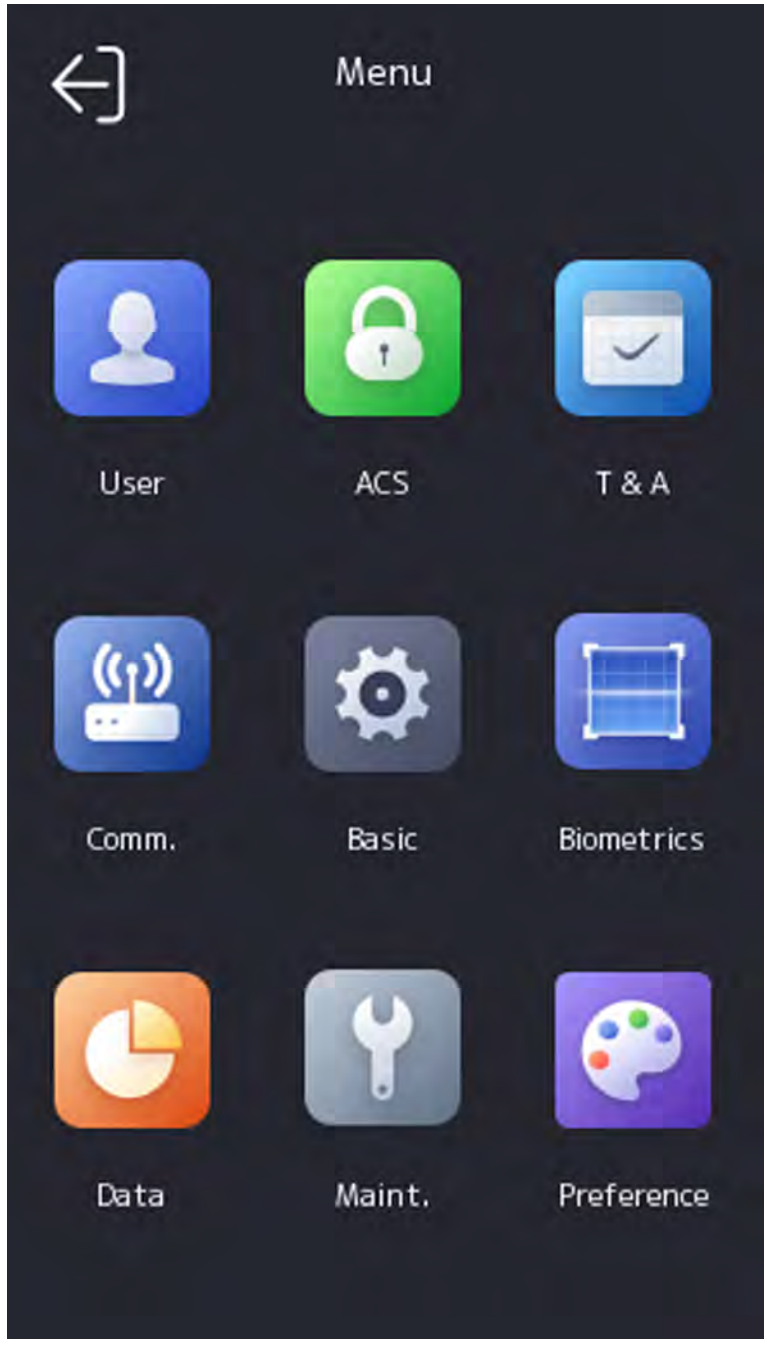


Figure 7-1 Home Page

7.2 Payment Administrator (For Operator)

Enter a short description of your task here (optional).

Before You Start
Enter the prerequisites here (optional).
Enter the context of your task here (optional).

Steps
1. Enter your first step here.
   Enter the result of your step here (optional).

Example
Enter an example that illustrates the current task (optional).

What to do next
Enter the tasks the user should do after finishing this task (optional).

7.3 Payment Settings (For Operator)

Enter a short description of your task here (optional).

Before You Start
Enter the prerequisites here (optional).
Enter the context of your task here (optional).

Steps
1. Enter your first step here.
   Enter the result of your step here (optional).

Example
Enter an example that illustrates the current task (optional).

What to do next
Enter the tasks the user should do after finishing this task (optional).

7.4 Check Balance

Enter a short description of your task here (optional).

Before You Start
Enter the prerequisites here (optional).
Enter the context of your task here (optional).

Steps
1. Enter your first step here.
   Enter the result of your step here (optional).

Example
Enter an example that illustrates the current task (optional).

What to do next

Enter the tasks the user should do after finishing this task (optional).

Chapter 8 Transaction

Enter a short description of your concept here (optional).

This is the start of your concept.

Chapter 9 Operation via Web Browser

9.1 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.

9.2 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.

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.

9.3 Search Event

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

Enter the search conditions, including the event type, 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.

9.4 Check Transaction

Search and view transaction records, including transaction type, payment mode, transaction amount, balance after payment, payment/remaining attempts, transaction center and capture.

Click **Check Transaction**to enter the interface.

Enter **Employee ID**, **Card No.**, **Select Type**, **Start Time**, **End Time** according to actual needs, and click **Search**. All the qualifying transaction record information will be listed in the interface, including transaction type, payment mode, transaction amount, balance after payment, payment/remaining attempts, transaction center and capture.

Note

Due to the existence of offline transaction records, payment statistics are subject to the server (client or web) data.

9.5 Configuration

9.5.1 Set Local Parameters

Set the live view parameters, record file size and saving path, and captured pictures and clip 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 Size and 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 and Clips 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.

9.5.2 View Device Information

View the device name, language, model, serial No., QR code, version, number of channels, and 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, and device capacity, etc.

9.5.3 Set Time

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

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

Figure 9-1 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 alarm receiver type, 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.

9.5.4 View Open Source Software License

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

9.5.5 Upgrade and Maintenance

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

Reboot Device

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

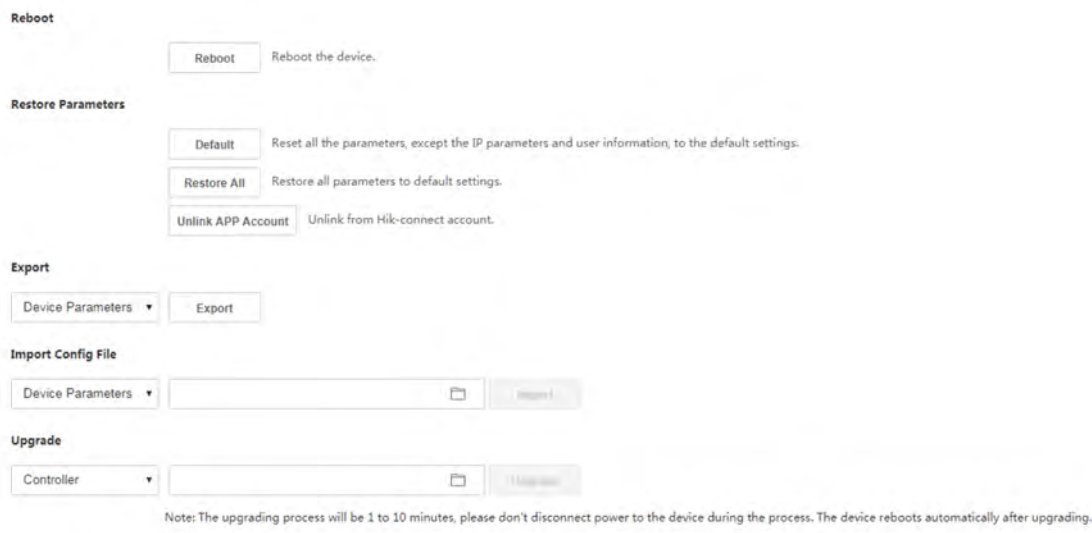


Figure 9-2 Upgrade and Maintenance Page

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.
If the device has been connected to Hik-Connect and network, when there is a new installation package in Hik-Connect, you can click **Upgrade** after Online Update to upgrade the device system.

Note

Do not power off during the upgrading.

9.5.6 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.

9.5.7 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.

9.5.8 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.

9.5.9 Online Users

The information of users logging into the device is shown.

Go to **Configuration → System → User Management → Online Users** to view the list of online users.

9.5.10 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.

9.5.11 Network Settings

Set TCP/IP, port, Wi-Fi parameters, and platform access.

Note

Some device models do not support Wi-Fi settings. Refer to the actual products during configuration.

Set Basic Network Parameters

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

Figure 9-3 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 and HTTPS 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.

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 9-4 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**.

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. 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.

3. Check the checkbox of **Enable** to enable the function.
4. **Optional:** Check the checkbox of **Custom**, and you can set the server address by yourself.
5. 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.

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

Configure HTTP Listening

The device can send alarm information to the event alarm IP address or domain name via HTTP protocol/HTTPS protocol.

Before You Start

The event alarm IP address or domain 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 event alarm IP address or domain name, URL, port, and protocol.
3. **Optional:** Click **Default** to reset the event alarm IP address or domain name.
4. Click **Save**.

9.5.12 Set Video and Audio Parameters

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

Set Video Parameters

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

Set the video channel, camera name, stream type, the video type, the bitrate type, the frame rate, the Max. bitrate, the video encoding, and I Frame Interval.

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

Set Audio Parameters

Click **Configuration → Video/Audio → Audio** .
Select the audio channel.
You can also drag the block to adjust the device input and output volume.
Click to 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.

9.5.13 Set Payment Prompt

Choose to enable payment amount prompt and payment result prompt. Customize prompt for successful payment and failed payment.

Steps

1. Click **Configuration → Video/Audio → Payment Prompt** .
2. Choose to enable **Payment Amount Prompt** and **Payment Result Prompt** according to actual needs.
3. Enter prompt in the textboxes to customize prompt for successful payment and failed payment.
4. Click **Save** to save the settings after the configuration.

9.5.14 Set Image Parameters

Set the video standard, WDR, image adjustment, supplement light, beauty, and image fusion.

Steps

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

Supplement Light Parameters

Set the supplement light type from the drop down list and select to enable or disable it.

If you select **On**, you can set the light brightness.

If you select **Schedule**, you can set the light brightness and its schedule.

Start/end recording video.

Capture the image.

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

9.5.15 General Settings

Set Authentication Parameters

Click **Configuration → General → 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.

Card Reader

Main Card Reader

You can configure the device card reader's parameters.

Enable Card Reader

After enabling this function, the card reader can be used via card; Aftering disabling this function, the entrance card reader cannot be used via card.

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.

Set Privacy Parameters

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

Go to **Configuration → General → 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**, and **Employee ID**, 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.

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 Face Recognition Parameters

You can set face recognition parameters for accessing.

Click **Configuration → General → 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.

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

Set Card Security

Click **Configuration → General → 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 CPU Card

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

CPU Card Read Content

Enable the device to read CPU card content.

Enable ID Card

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

9.5.16 Set Biometric Parameters

Set Biometric Parameters

Click **Configuration → Smart → Smart** .

Note

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

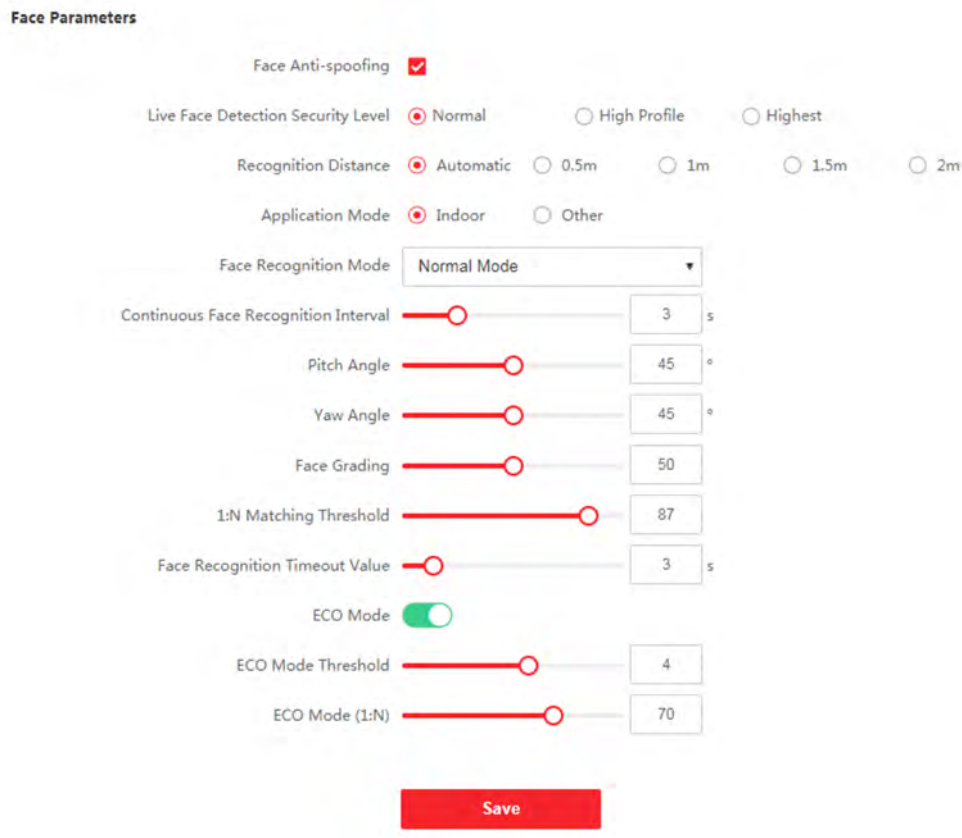


Figure 9-5 Smart Settings Page

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 100% 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 indoor.

Continuous Face Recognition Interval

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

Rating

Set the face rating 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 without Mask Detection

After enabling the face without mask detection, the system will recognize the captured face with mask picture or not. You can set face with mask1:N matching threshold, it's ECO mode, and the strategy.

No Prompt

The function is disabled. The device will not detect whether a person is wearing a face mask or not.

Must Wear

If the person do not wear the face mask when authenticating, the device will pop up a prompt and the door will keep closed.

Face with Mask 1:N Matching Threshold (ECO Mode)

Set the matching threshold when authenticating with face mask via ECO mode 1:N matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate.

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.

9.5.17 Set Payment

Set payment parameters, including meal picking settings, payment verification mode, offline bookkeeping, fixed amount display, insufficient account balance prompt, default payment mode and payment amount limit.

Steps

1. Click **Configuration → Payment Configuration** to enter the Payment Parameters setting page.
2. Click to enable or disable meal picking.
   After enabling meal picking,

Chapter 10 Client Software Configuration

10.1 Configuration Flow of Client Software

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

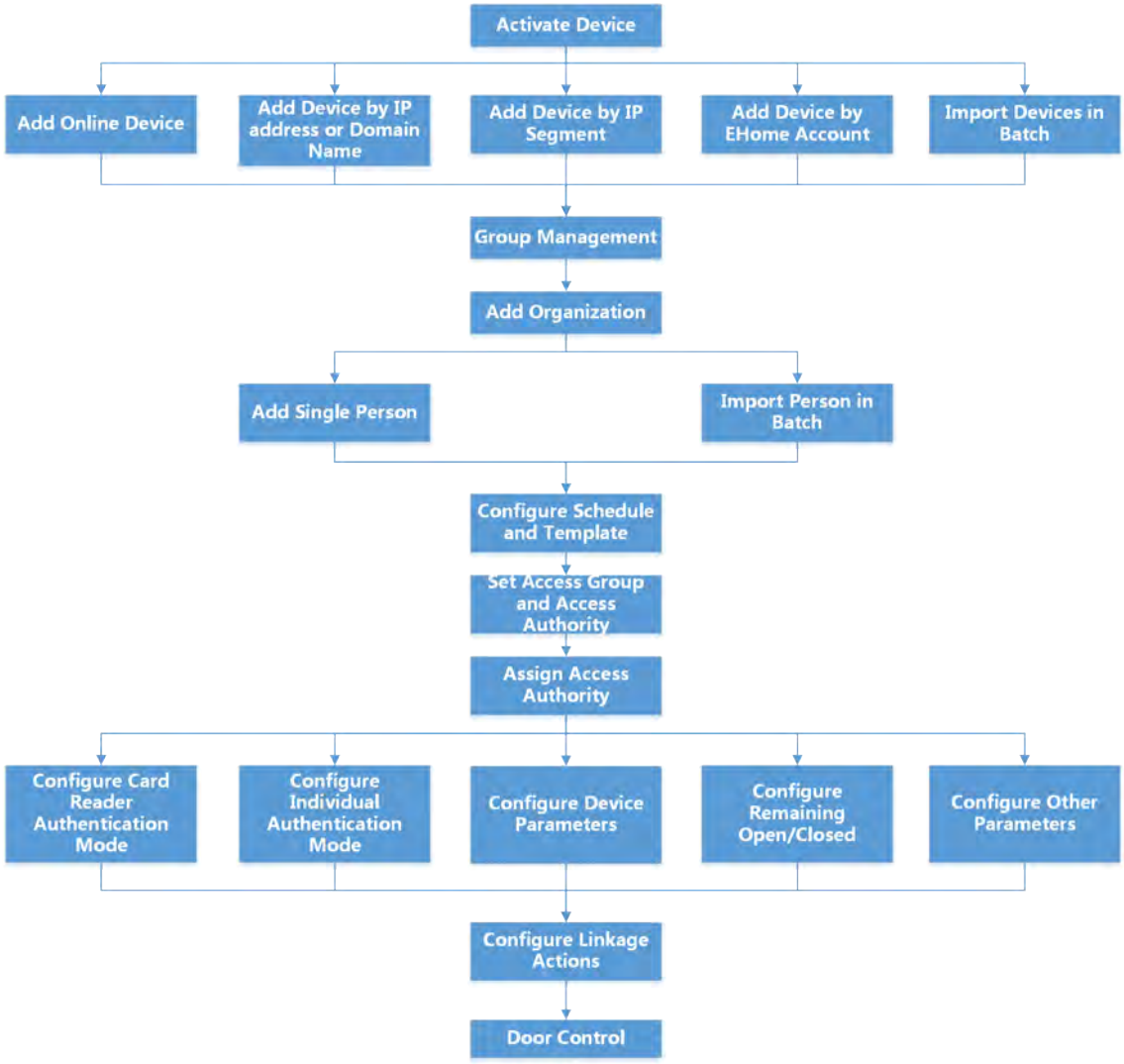


Figure 10-1 Flow Diagram of Configuration on Client Software

10.2 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.

10.2.1 Add Device

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

Add Online Device

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

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

Add Single Online Device

You can add single online device to the client software.

Steps
1. Enter the Device Management module.
2. **Optional:** 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. Select an online device from the **Online Device** area.

   Note
   For the inactive device, you need to create the password for it before you can add the device properly. For detailed steps, refer to ***Activation*** .
5. Click **Add** to open the device adding window.
6. Enter the required information.

   Name
   Enter a descriptive name for the device.

   Address
   The IP address of the device is obtained automatically in this adding mode.

   Port

The port number is obtained automatically.

User Name

By default, the user name is admin.

Password

Enter the device password.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.
Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

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

Note

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

9. Click **OK** to add the device.

Add Multiple Online Devices

You can add multiple online devices to the client software.

Steps

1. Enter the Device Management module.
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. Select multiple devices.

Note

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

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

User Name

By default, the user name is admin.

Password

Enter the device password.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.
Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

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

Note

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

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

Add Device by IP Address or Domain Name

When you know the IP address or domain name of the device to add, you can add devices to the client by specifying the IP address (or domain name), user name, password, 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.
- 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.
8. Finish adding the device.
   - Click **Add** to add the device and back to the device list page.
   - Click **Add and New** to save the settings and continue to add other device.
9. **Optional:** Perform the following operation(s).

Remote Configuration	Click on Operation column to set remote configuration of the corresponding device. **Note** For detail operation steps for the remote configuration, see the user manual of the device.
Device Status	Click on Operation column to view device status, including cameras, recording status, signal status, hardware status, etc.
Edit Device Information	Click on Operation column to edit the device information, such as IP address, user name, and password.
Check Online User	Click on Operation column to check the online users who access the device, such as user name, user type, user's IP address, and login time.
Refresh	Click on Operation column to get the latest device information.

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

Add Devices by IP Segment

If the devices share the same port No., user name and password, and their IP addresses are sharing an IP segment. You can specify the start IP address and the end IP address, port No., user name, password, etc of the devices to add them to the client.

Steps

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

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

   Start IP

   Enter a start IP address.

   End IP

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

   Port

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

   User Name

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

   Password

   Enter the device password.

   Caution

   The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.
   Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.
6. **Optional:** Check **Transmission Encryption (TLS)** to enable transmission encryption using TLS (Transport Layer Security) protocol for security purpose .

Note

- This function should be supported by the device.
- You can log into the device to get the certificate file by web browser.

7. Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.
8. **Optional:** Check **Import to Group** to create a group by the device name.
9. Finish adding the device.
   - Click **Add** to add the device and back to the device list page.
   - Click **Add and New** to save the settings and continue to add other device.
10. **Optional:** Perform the following operation(s).

Remote Configuration	Click on Operation column to set remote configuration of the corresponding device. **Note** For detail operation steps for the remote configuration, see the user manual of the device.
Device Status	Click on Operation column to view device status, including cameras, recording status, signal status, hardware status, etc.
Edit Device Information	Click on Operation column to edit the device information, such as IP address, user name, and password.
Check Online User	Click on Operation column to check the online users who access the device, such as user name, user type, user's IP address, and login time.
Refresh	Click on Operation column to get the latest device information.
Delete Device	Select one or multiple devices and click **Delete** to delete the selected device(s) from the client.

Add Device by EHome Account

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

Before You Start

Make sure the devices have connected to the network properly.

Steps

1. Enter Device Management module.

   The added devices are displayed on the right panel.
2. Click **Add** to open the Add window.

3. Select **EHome** as the adding mode.
4. Enter the required information.

   Device Account

   Enter the account name registered on EHome protocol.

   EHome Key

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

   Note

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

   Note

   Face pictures cannot be applied to devices added by EHome account.
8. **Optional:** Perform the following operation(s).

Device Status	Click on Operation column to view device status.
Edit Device Information	Click on Operation column to edit the device information, such as device name, device account, and EHome key.
Check Online User	Click on Operation column to check the online users who access the device, such as user name, user type, user's IP address, and login time.
Refresh	Click on Operation column to get the latest device information.
Delete Device	Select one or multiple devices and click **Delete** to delete the selected device(s) from the client.

Import Devices in a Batch

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

Steps

1. Enter the Device Management page
2. Click **Add** to open the adding device window.
3. Select **Batch Import** as the adding mode.
4. Click **Export Template** and then save the pre-defined template (CSV file) on your PC.

5. Open the exported template file and enter the required information of the devices to be added on the corresponding column.

Adding Mode

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

Address

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

Port

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

Device Information

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

User Name

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

Password

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

Caution

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

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

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

10.2.2 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.

10.3 Group Management

The resources added should be organized into groups for convenient management, such as access points. You can do some further operations of the device through the groups.

10.3.1 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.

10.3.2 Import Resources to Group

You can import the device resources 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 such as **Access Control Point**.
4. Click **Import**.
5. Select the channel names from the To Be Imported area.
6. Click **Import** to import the selected resources to the group.

10.3.3 Edit Resource Parameters

After importing the resources to the group, you can edit the resource parameters. For access points, you can edit the resource name.

Before You Start
Import the resources to group. Refer to ***Import Resources to Group*** .

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

10.3.4 Remove Resources from Group

You can remove the added resources from the group.

Steps
1. Enter the Device Management module.
2. Click **Device Management → Group** to enter the group management page.

All the added groups are displayed on the left.

3. Click a group to show the resources added to this group.
4. Select the resource(s) and click **Delete** to remove the resource(s) from the group.

10.4 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.

10.4.1 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.

10.4.2 Configure Basic Information

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

Steps

1. Enter **Person** module.

Note

For the first time you enter **Person** module, a window pops up, and you can set the rules to generate person ID (letters and numbers supported) when adding person. When getting person information from device, if there are no person IDs, the person IDs will be generated according to the rule.

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

   The Person ID will be generated automatically.
4. Enter the basic information including person name, gender, telephone number, email address, validity period, etc.

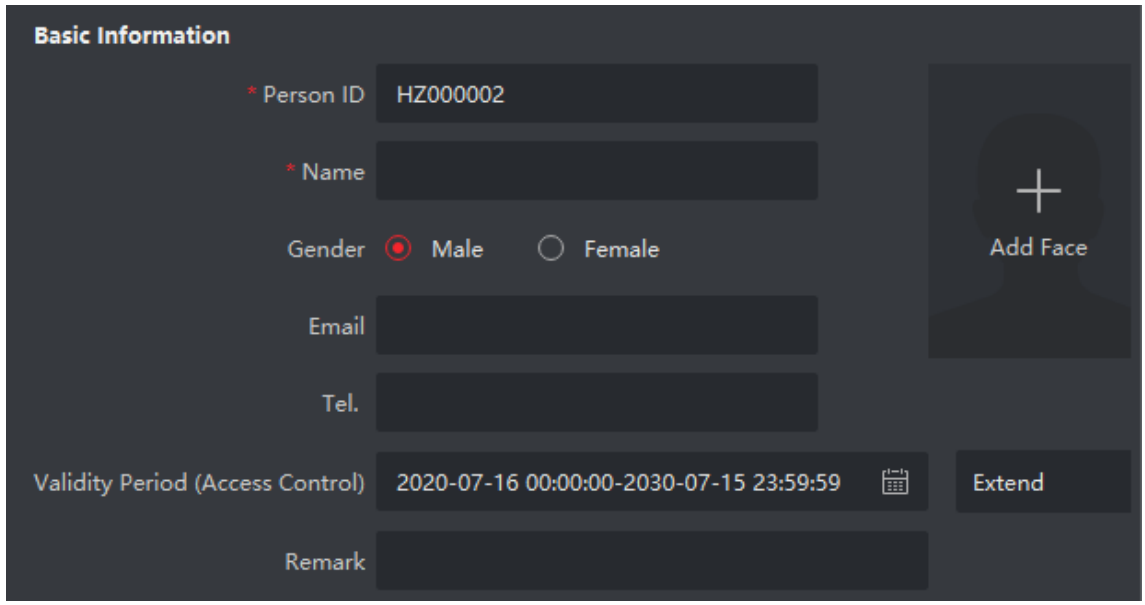


Figure 10-2 Configure Basic Information

Note

Once validity period expired, the credentials and access control settings of the person will be invalid and the person will have no authorization to access the doors\floors. You can click **Extend** to extend the person's validity period for 1 month, 3 months, 6 months, or 1 year.

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

10.4.3 Issue a Card by Local Mode

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

Steps

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

   Note

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

3. In the **Credential → Card** area, click **+**.
4. Click **Settings** to enter the Settings page.
5. Select **Local** as the card issuing mode.

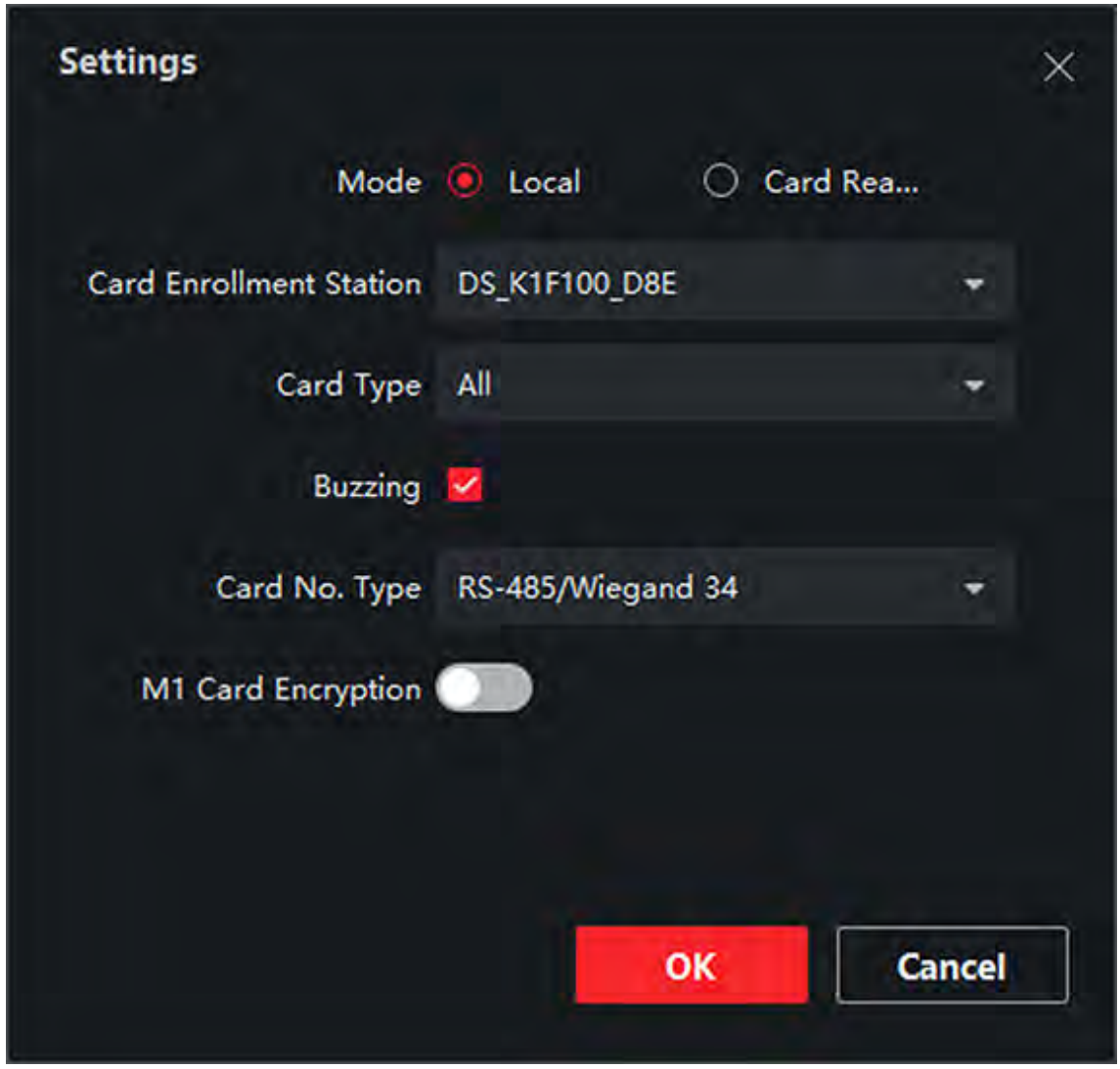


Figure 10-3 Issue a Card by Local Mode

6. Set other related parameters.

Card Enrollment Station

Select the model of the connected card enrollment station.

Note

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

Card Type

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

Buzzing

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

Card No. Type

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

M1 Card Encryption

This field is only available when the model is DS-K1F100-D8, DS-K1F100-D8E, or DS-K1F180-D8E. If the card is M1 card, then you can enable the M1 Card Encryption function and select the sector of the card to encrypt.

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

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

   The card will be issued to the person.

10.4.4 Upload a Face Photo from Local PC

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

Steps

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

   Note

   Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .
3. Click **Add Face** in the Basic Information panel.
4. Select **Upload**.
5. Select a picture from the PC running the client.

   Note

   The picture should be in JPG or JPEG format and smaller than 200 KB.
6. **Optional:** Enable **Verify by Device** to check whether the facial recognition device managed in the client can recognize the face in the photo.

   Note

   This function is hidden or shown according to the device capacity.
7. Confirm to add the person.
   - Click **Add** to add the person and close the Add Person window.
   - Click **Add and New** to add the person and continue to add other persons .

10.4.5 Take a Photo via Client

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

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

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

   Note
   Enter the person's basic information first. For details, refer to ***Configure Basic Information*** .
3. Click **Add Face** in the Basic Information area.
4. Select **Take Photo** to enter Take Photo window.
5. **Optional:** Enable **Verify by Device** to check whether the captured face photo can meet the uploading requirements.

   Note
   This function is hidden or shown according to the device capacity.
6. Take a photo.
   1) Face to the camera and make sure your face is in the middle of the collecting window.
   2) Click to capture a face photo.
   3) **Optional:** Click to capture again.
   4) Click **OK** to save the captured photo.

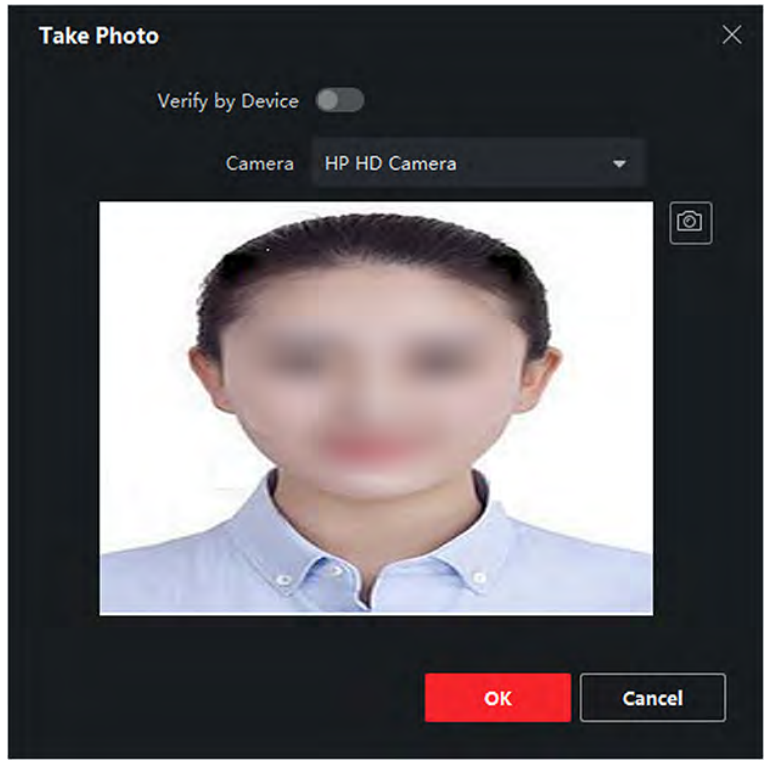


Figure 10-4 Take a Photo via Client

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

10.4.6 Collect Face via Access Control Device

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

Steps

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

   Note

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

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

Note

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

Face Anti-Spoofing

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

6. Collect face.
   1) Face to the camera of the selected access control device and make sure your face is in the middle of the collecting window.
   2) Click to capture a photo.
   3) Click **OK** to save the captured photo.
7. Confirm to add the person.
   - Click **Add** to add the person and close the Add Person window.
   - Click **Add and New** to add the person and continue to add other persons .

10.4.7 Collect Fingerprint via Client

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

Before You Start

Connect the fingerprint recorder to the PC running the client.

Steps

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

   Note

   Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .
3. In the **Credential → Fingerprint** panel, click **+**.
4. In the pop-up window, select the collection mode as **Local**.
5. Select the model of the connected fingerprint recorder.

   Note

   If the fingerprint recorder is DS-K1F800-F, you can click **Settings** to select the COM the fingerprint recorder connects to.
6. Collect the fingerprint.
   1) Click **Start**.
   2) Place and lift your fingerprint on the fingerprint recorder to collect the fingerprint.

3) Click **Add** to save the recorded fingerprint.

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

Note

Once the fingerprint is added, the fingerprint type cannot be changed.

10.4.8 Collect Fingerprint via Access Control Device

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

Before You Start

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

Steps

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

Note

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

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

Note

Once the fingerprint is added, the fingerprint type cannot be changed.

10.4.9 Configure Access Control Information

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

Steps

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

Note

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

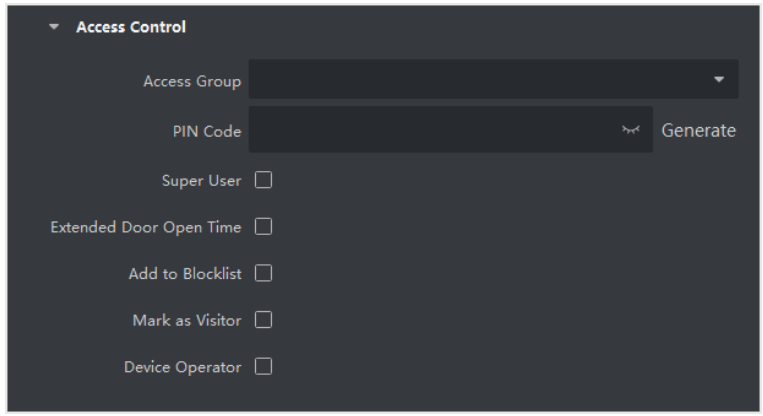


Figure 10-5 Configure Access Control Information

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

     Note

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

     Note

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

   Super User

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

Extended Door Open Time

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

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

Add to Blocklist

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

Mark as Visitor

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

Note

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

Device Operator

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

Note

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

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

10.4.10 Customize Person Information

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

Steps

1. Enter **Person** module.
2. Set the fields of custom information.
   1) Click **Custom Property**.
   2) Click **Add** to add a new property.
   3) Enter the property name.
   4) Click **OK**.
3. Set the custom information when adding a person.

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

Note

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

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

10.4.11 Configure Resident Information

If the person is resident, for video intercom purpose, you need to set the room number for her/him and bind an indoor station. After bound, you can call this person by calling the indoor station and perform video intercom with her/him.

Steps

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

Note

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

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

Note

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

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

10.4.12 Configure Additional Information

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

Steps

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

Note

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

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

10.4.13 Import and Export Person Identify Information

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

10.4.14 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.

10.4.15 Import Person Pictures

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

Before You Start
Be sure to have imported person information to the client beforehand.

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

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

6. Click **Import** to start importing.
   The importing progress and result will be displayed.

10.4.16 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.

10.4.17 Export Person Pictures

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

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

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

   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).

10.4.18 Delete Registered Pictures

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

Before You Start
Make sure you have saved the structure data.

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

10.4.19 Get Person Information from Access Control Device

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

Steps

Note

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

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

   Note

   If you select the enrollment station, you should click **Login**, and set IP address, port No., user name and password of the device.
5. Click **Import** to start importing the person information to the client.

   Note

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

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

10.4.20 Move Persons to Another Organization

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

Before You Start

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

Steps

1. Enter **Person** module.
2. Select an organization in the left panel.

   The persons under the organization will be displayed in the right panel.
3. Select the person to move.
4. Click **Change Organization**.
5. Select the organization to move persons to.
6. Click **OK**.

10.4.21 Issue Cards to Persons in Batch

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

Steps

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

   All the added persons with no card issued will 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).

10.4.22 Report Card Loss

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

Steps

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

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

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

10.4.23 Set Card Issuing Parameters

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

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

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

Local Mode: Issue Card by Card Enrollment Station

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

Card Enrollment Station

Select the model of the connected card enrollment station

Note

Currently, the supported card enrollment station model is DS-K1F180-D8E.

Card Type

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

Buzzing

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

Card No. Type

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

M1 Card Encryption

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.

10.5 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*** .

10.5.1 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**.

10.5.2 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.

10.6 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.

Before You Start

- Add person to the client.
- Add access control device to the client and group access points. For details, refer to ***Group Management*** .
- Add template.

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

1. Click **Access Control → 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.

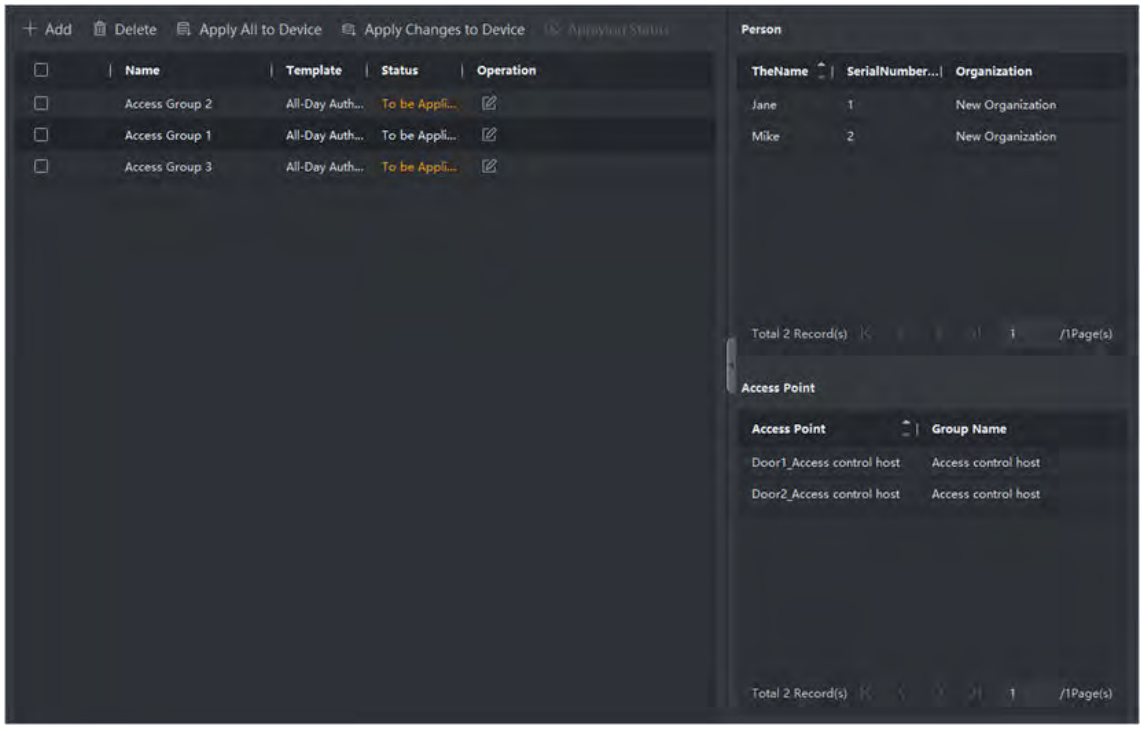


Figure 10-6 Display the Selected Person(s) and Access Point(s)

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) or fingerprints.

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**.

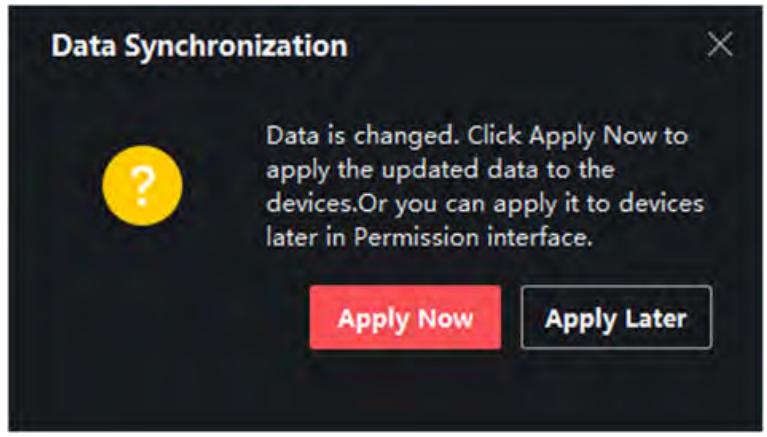


Figure 10-7 Data Synchronization

10.7 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.

10.7.1 Configure Device Parameters

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

Configure Parameters for Access Control Device

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

Steps

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

   Note

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

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

   Note

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

   Voice Prompt

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

   Upload Pic. After Linked Capture

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

   Save Pic. After Linked Capture

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

   Face Recognition Mode

   Normal Mode

   Recognize face via the camera normally.

   Deep Mode

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

   Enable NFC Card

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

   Enable M1 Card

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

   Enable EM Card

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

Note

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

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) parameters.

Steps

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

Note

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

Open Duration

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

Extended Open Duration

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

Door Left Open Timeout Alarm

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

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

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

Note

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

Configure Parameters for Card Reader

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

Steps

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

Note

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

Basic Information

Name

Edit the card reader name as desired.

Minimum Card Swiping Interval

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

Alarm of Max. Failed Attempts

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

Card Reader Type/Card Reader Description

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

Fingerprint Capacity

View the maximum number of available fingerprints.

Existing Fingerprint Number

View the number of existed fingerprints in the device.

Advanced

Enable Card Reader

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

OK LED Polarity/Error LED Polarity/Buzzer Polarity

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

Max. Interval When Entering PWD

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

Tampering Detection

Enable the anti-tamper detection for the card reader.

Max. Times of Card Failure

Set the max. failure attempts of reading card.

Fingerprint Recognition Level

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

Face 1:N Mathcing Threshold

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

Face Recognition Interval

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

Face Anti-spoofing

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

Face 1:1 Matching Threshold

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

Application Mode

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

Lock Authentication Failed Face

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

Liveness Detection Security Level

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

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

10.7.2 Configure Remaining Open/Closed

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

Before You Start

Add the access control devices to the system.

Steps

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

   Note

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

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

- Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to .
- Click the time duration and directly edit the start/end time in the appeared dialog.
- Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to .

4) Click **Save**.

Related Operations

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

4. To set the door status during the holiday, click the **Holiday** and perform the following operations.

1) Click **Remain Open** or **Remain Closed**.
2) Click **Add**.
3) Enter the start date and end date.
4) Drag the cursor to draw the time duration, which means in that duration of time, the configured access group is activated.

Note

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

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

5. Optional: Click **Copy to** to copy the door status settings of this door to other door(s).

10.7.3 Configure Multi-Factor Authentication

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

Before You Start

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

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

Steps

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

   Note

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

   5) Click **Save**.
   6) **Optional:** Select the person/card group(s), and then click **Delete** to delete it(them).
   7) **Optional:** Select the person/card group(s), and then click **Apply** to re-apply access group that failed to be applied previously to the access control device.
4. Select an access control point (door) of selected device on the left panel.
5. Enter the maximum interval when entering password.
6. Add an authentication group for the selected access control point.
   1) Click **Add** on the Authentication Groups panel.
   2) Select a configured template as the authentication template from the drop-down list.

   Note

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

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

   Local Authentication

   Authentication by the access control device.

   Local Authentication and Remotely Open Door

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

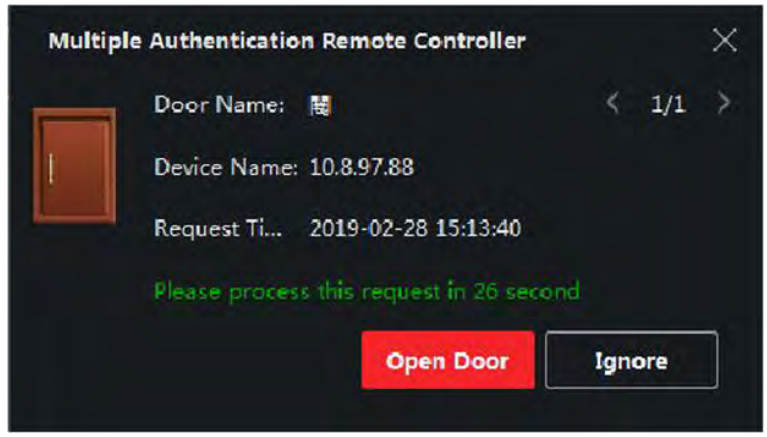


Figure 10-8 Remotely Open Door

Note

You can check **Offline Authentication** to enable the super password authentication when the access control device is disconnected with the client.

Local Authentication and Super Password

Authentication by the access control device and by the super password.

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

Note

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

6) Click **Save**.

Note

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

7. Click **Save**.

10.7.4 Configure Custom Wiegand Rule

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

Before You Start

Wire the third party card readers to the device.

Steps

Note

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

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

   Note

   Up to 32 characters are allowed in the custom Wiegand name.
4. Click **Select Device** to select the access control device for setting the custom wiegand.
5. Set the parity mode according to the property of the third party card reader.

   Note

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

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

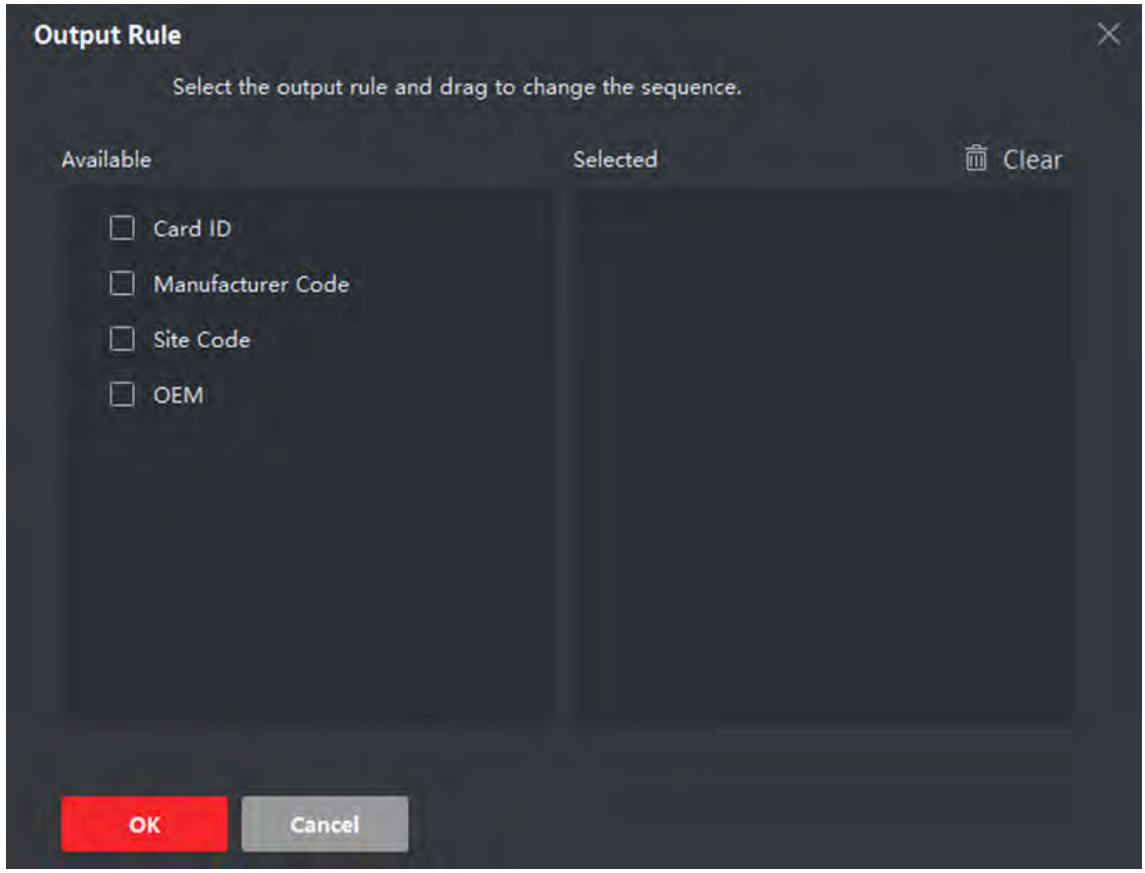


Figure 10-9 Set Output Transformation Rule

2) Select rules on the left list.

   The selected rules will be added to the right list.

3) **Optional:** Drag the rules to change the rule order.
4) Click **OK**.
5) In the Custom Wiegand tab, set the rule's start bit, length, and the decimal digit.

7. Click **Save**.

10.7.5 Configure Person Authentication Mode

You can set the passing rules for person to the specified the access control device according to your actual needs.

Before You Start

- Add access control device to the client, and make sure the access control device support the function of person authentication.
- Add person and assign access authorization to designed person. For details, refer to ***Person Management*** and ***Set Access Group to Assign Access Authorization to Persons*** .

Steps

1. Click **Access Control → Advanced Function → Authentication** .
2. Select an access control device (support the function of person authentication) on the left panel to enter the person Authentication Mode page.
3. Click **Add** to enter the Add window.
4. Select the person(s) need to be configured on the left panel.

   The selected person(s) will be added to the right panel.
5. Select the authentication mode on the drop-down list of **Authentication Mode**.
6. Click **OK**.

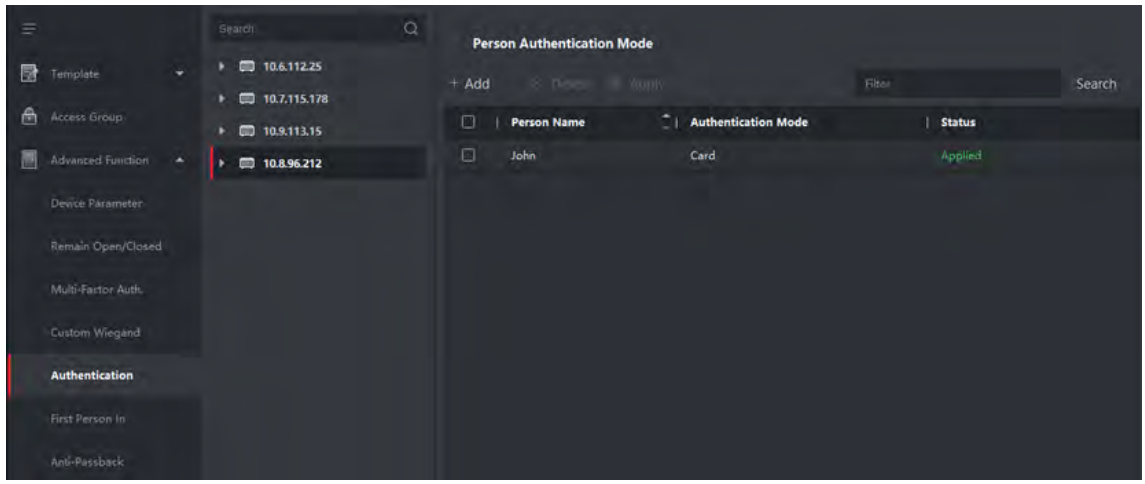


Figure 10-10 Set Authentication Modes for Persons

7. **Optional:** Select person(s) on the Person Authentication mode page, and then click **Apply** to apply the person authentication mode to the device.

Note

Person authentication has higher priority than other authentication mode. When the access control device has been configured person authentication mode, the person should authenticate on this device via person authentication mode.

10.7.6 Configure Card Reader Authentication Mode and Schedule

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

Steps

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

   1) Click **Configuration**.

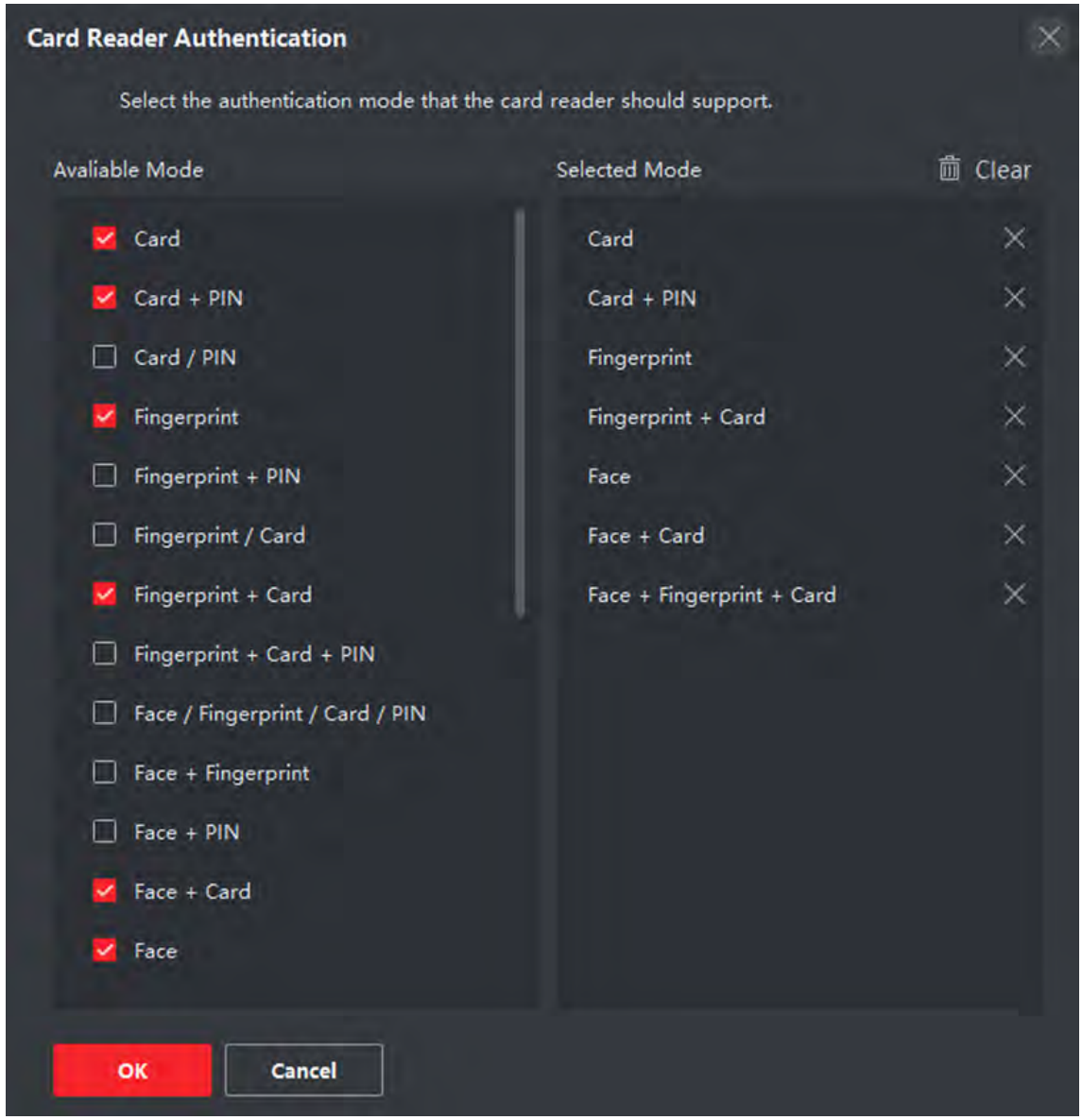


Figure 10-11 Select Card Reader Authentication Mode

Note

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

2) Check the modes in the Available Mode list and they will be added to the selected modes list.
3) Click **OK**.

After selecting the modes, the selected modes will display as icons with different color.

4. Click the icon to select a card reader authentication mode, and drag the cursor to draw a color bar on the schedule, which means in that period of time, the card reader authentication is valid.

5. Repeat the above step to set other time periods.

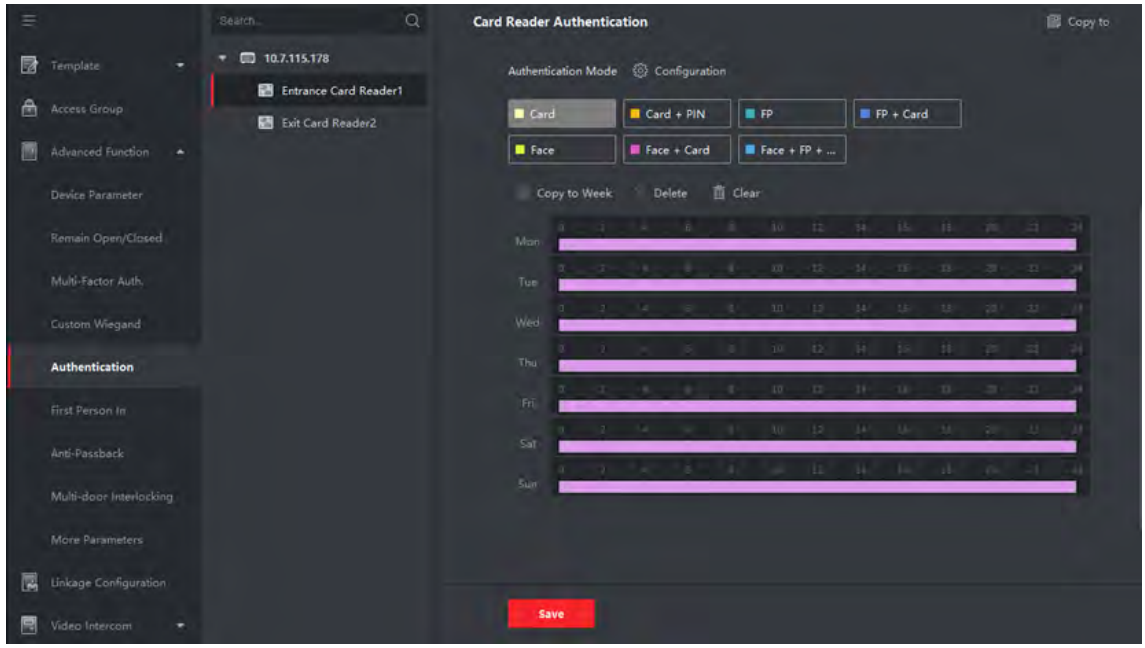


Figure 10-12 Set Authentication Modes for Card Readers

6. **Optional:** Select a configured day and click **Copy to Week** to copy the same settings to the whole week.
7. **Optional:** Click **Copy to** to copy the settings to other card readers.
8. Click **Save**.

10.7.7 Configure First Person In

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

Before You Start

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

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

Steps

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

   Enable Remaining Open after First Person

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

Note

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

Disable Remaining Open after First Person

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

Note

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

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

   The added first person(s) will list in the First Person List
6. **Optional:** Select a first person from the list and click **Delete** to remove the person from the first person list.
7. Click **Save**.

10.7.8 Configure Anti-Passback

The anti-passback feature is designed to minimizes the misuse or fraudulent use of access credentials such as passing back card to an unauthorized person, or tailed access. The anti-passback function establishes a specific sequence in which access credentials must be used in order to grant access. You can set the sequence according to the actual path via the client and if the person uses the credential in wrong sequence, you can also reset the anti-password records.

Before You Start

Add access control device to the client, and enable the anti-passing back function of the access control device.

Steps

Note

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

1. Click **Access Control → Advanced Function → Anti-Passback** to enter the Anti-Passpack Settings page.
2. Select an access control device on the left panel.
3. Select a card reader as the beginning of the path in the **First Card Reader** field.

4. Click of the selected first card reader in the **Card Reader Afterward** column to open the select card reader dialog.
5. Select the afterward card readers for the first card reader.

Note

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

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

Example

Set Card Swiping Path: If you select Reader In_01 as the beginning, and select Reader In_02, Reader Out_04 as the linked card readers. Then you can only get through the access control point by swiping the card in the order as Reader In_01, Reader In_02 and Reader Out_04.

8. Click **Reset Anti-Passback** and select the person(s) to delete the related anti-passback records about the person(s) on the device.

Note

This function should be supported by the device.

10.7.9 Configure Device Parameters

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

Set Multiple NIC Parameters

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

Before You Start

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

Steps

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

MAC Address

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

MTU

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

6. Click **Save**.

Set Network Parameters

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

Set Log Uploading Mode

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

Steps

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

Create ISUP Account in Wired Communication Mode

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

Steps

Note

This function should be supported by the device.

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

Note

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

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

Note

If set the ISUP version as **5.0**, you should create an ISUP key for the ISUP account.

9. Set an account name for the network center.
10. Click **Save**.

Set Device Capture Parameters

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

Note

- The capture function should be supported by the device.
- Before setting the capture parameters, you should set the picture storage first to define where the event triggered pictures are saved. For details, refer to *Set Picture Storage* in the user manual of the client software. .

Set Triggered Capture Parameters

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

Before You Start

Before setting the capture parameters, you should set the picture storage first to define where the captured pictures are saved. For details, refer to *Set Picture Storage* in the user manual of the client software.

Steps

Note

This function should be supported by the device

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function → More Parameters → Capture** .
3. Select an access control device in the device list and select **Linked Capture**.
4. Set the picture size and quality.

5. Set the capture times once triggered which defines how many pictures will be captures for one time.
6. If the capture times is more than 1, set the interval for each capture.
7. Click **Save**.

Set Manual Capture Parameters

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

Before You Start

Before setting the capture parameters, you should set the saving path first to define where the captured pictures are saved. For details, refer to *Set Picture Storage* in the user manual of the client software.

Steps

Note

This function should be supported by the device

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

Set Parameters for Face Recognition Terminal

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

Steps

Note

This function should be supported by the device.

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

Note

These parameters displayed vary according to different device models.

COM

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

Face Picture Database

select Deep Learning as the face picture database.

Authenticate by QR Code

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

Blocklist Authentication

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

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

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

Save Authenticating Face Picture

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

MCU Version

View the device MCU version.

5. Click **Save**.

Set RS-485 Parameters

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

Steps

Note

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

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

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

Set Wiegand Parameters

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

Steps

Note

This function should be supported by the device.

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

   Note

   If you set **Communication Direction** as **Sending**, you are required to set the **Wiegand Mode** as **Wiegand 26**, **Wiegand 34**, **Wiegand 27**, or **Wiegand 35**.
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 Verification** to enter the M1 Card Encryption Verification page.
4. Set the switch to on to enable the M1 card encryption function.

5. Set the sector ID.

Note

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

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

10.8 Configure Linkage Actions for Access Control

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

Two types of linkage actions are supported:

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

10.8.1 Configure Client Actions for Access Event

Even if you are far away from an access point, you can still know what happens and how urgent the event is via the client by configuring client actions for the access event. Client actions here refer to the actions automatically executed by the client itself, such as making an audible warning and sending an email. Once an event is triggered, the client will notify the security personnel, so that he/she can handle the event in time.

Before You Start

Add access control device to the client.

Steps

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

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

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

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

      Audible Warning

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

Note

For details about setting the alarm sound, refer to *Set Alarm Sound* in the user manual of the client software.

Send Email

Send an email notification about the event to one or more receivers.

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

2) Click **OK**.

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

10.8.2 Configure Device Actions for Access Event

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

Steps

Note

It should be supported by the device.

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

Buzzer on Controller

The audible warning of access control device will be triggered.

Capture

The real-time capture will be triggered.

Access Point

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

Note

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

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

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

10.8.3 Configure Device Actions for Card Swiping

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

Steps

Note

It should be supported by the device.

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

   Buzzer on Controller

   The audible warning of access control device will be triggered.

   Capture

   The real-time capture will be triggered.

   Access Point

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

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

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

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

10.8.4 Configure Device Actions for Person ID

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

Steps

Note

It should be supported by the device.

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

   Buzzer on Controller

   The audible warning of access control device will be triggered.

   Buzzer on Reader

   The audible warning of card reader will be triggered.

   Capture

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

   Recording

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

   Note

   The device should support recording.

   Access Point

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

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

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

10.9 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.

10.10 Event Center

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

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

10.10.1 Enable Receiving Event from Devices

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

Steps

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

   All the added devices appear on this page.
2. **Optional:** If there are to many devices, enter the key words in Filter filed to filter the device(s) you want.

   Note

   For the filtered devices, you can click **Arm All** or **Disarm All** to enable receiving event of these devices.
3. In the Auto-Arming column, turn on the switch to enable auto-arming.

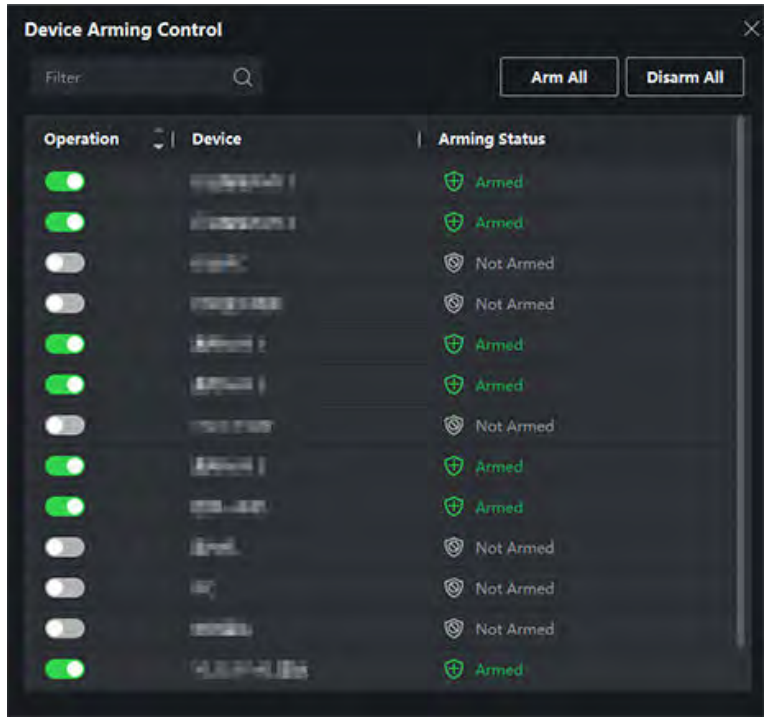


Figure 10-13 Arm Device

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

10.10.2 View Real-Time Events

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

Before You Start

Enable receiving events from devices before the client can receive event from the device, see ***Enable Receiving Event from Devices*** for details.

Steps

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

   Event Time

   For encoding device, event time is the client time when it receives the event. For other device types, event time is the time when the event is triggered.

   Priority

   Priority represents the emergency degree of the event.

2. Filter the events.

Filter by Device Type and (or) Priority	Select device type(s) and (or) priorities to filter events.
Filter by Keywords	Enter the keywords to filter the events.

3. **Optional:** Right-click the table header of the event list to customize the event related items to be displayed in the event list.
4. Select an event in the event list to view the event details.
5. **Optional:** Perform the following operations if necessary.

Handle Single Event	Click **Handle** to enter the processing suggestion, and then click **OK**. **Note** After an event is handled, the **Handle** button will become **Add Remark**. Click **Add Remark** to add more remarks for this handled event.
Handle Events in a Batch	Select events that need to be processed, and then click **Handle in Batch**. Enter the processing suggestion, and then click **OK**.
Enable/Disable Alarm Audio	Click **Audio On/Mute** to enable/disable the audio of the event.
Select the Latest Event Automatically	Check **Auto-Select Latest Event** to select the latest event automatically and the event information details is displayed.
Clear Events	Click **Clear** to clear the all the events in the event list.
Send Email	Select an event and then click **Send Email**, and the information details of this event will be sent by email. **Note** You should configure the email parameters first, see *Set Email Parameters* in the user manual of the client software for details.
Auto-Play Video	Check **Auto-Play Video** to automatically play video when displaying event details.
Enlarge Video or Picture	• Double click the video image to view video in a larger window. • Put the cursor on the picture, and click to view picture in a larger window.
Download Captured Picture	Hover the cursor on the captured picture, and click the download icon on the lower right corner of the picture to download it to the local PC.
Download Event Triggered Video	Hover the cursor on the recorded video, click to download the video (30s before the event happens) triggered by the event.

10.10.3 Search Historical Events

You can search and view historical events by setting search conditions such as time, device type, and priority in the client. For the searched events, you can handle and export them.

Before You Start

Enable receiving events from devices before the client can receive event information from the device,see ***Enable Receiving Event from Devices*** for details.

Steps

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

Time

The time when the event starts.

Search by

Device

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

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

Group

Search the events by resource channels in the group.

Note

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

Priority

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

Event Type

Select one or more event types to be searched from the drop-down list.

Note

You can enter a key word (supports fuzzy search) in the search box to search the target event type(s).

Status

The handling status of the event.

Search by Keyword

Enter a key word (supports fuzzy search) to quickly search the target historical event(s). For example, you can enter a person's name to search the events related with this person.

3. Click **Search** to search the events according the conditions you set.

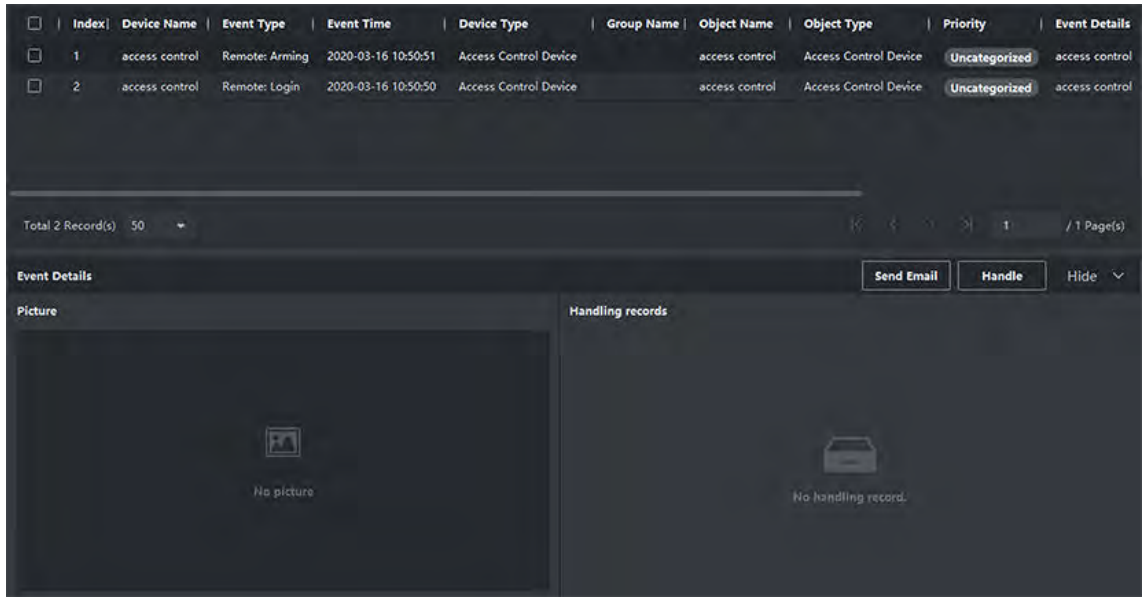


Figure 10-14 Search Historical Events

Note

If you have selected **Access Control** as device type in Step 2, you can view extra information such as card No., skin-surface temperature, and abnormal temperature (if device supports) in the searched events.

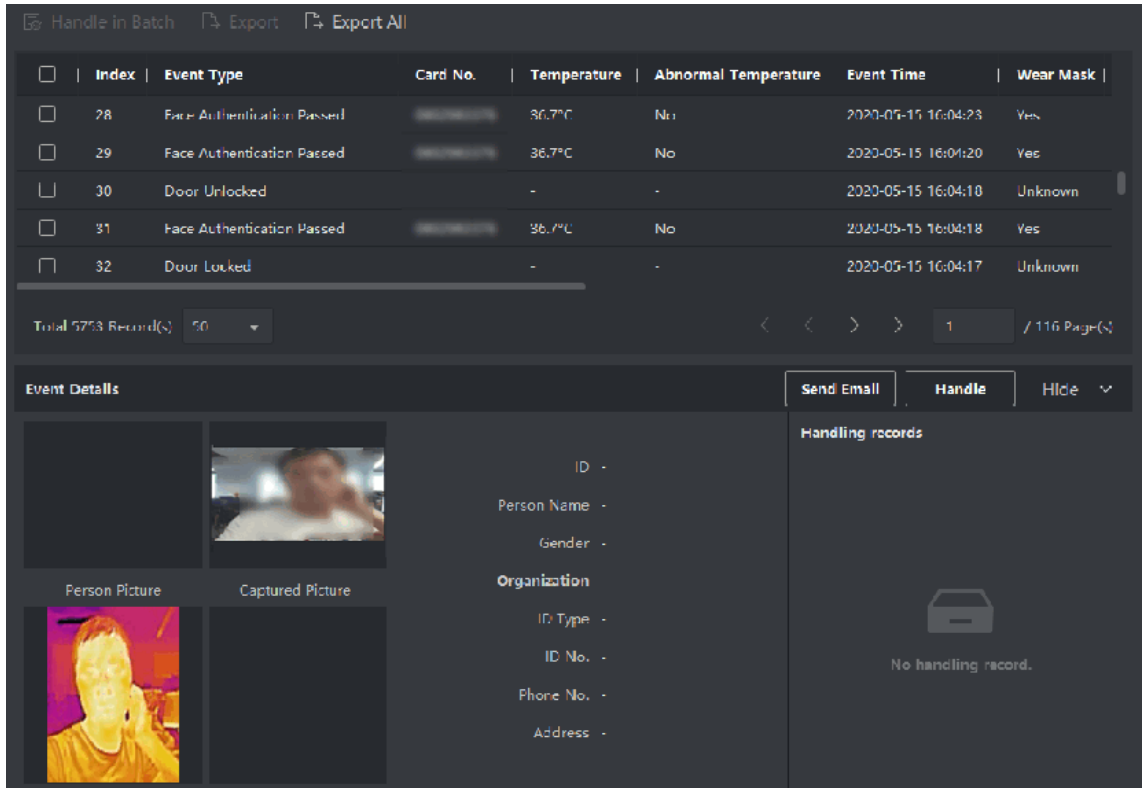


Figure 10-15 Search Historical Event

4. **Optional:** Right click the table header of the event list to customize the event related items to be displayed in the event list.
5. Select an event in the event list to view the event details.
6. **Optional:** Perform one of the following operations.

Handle Single Event	Handle single event: Select one event that needs to be handled, and then click **Handle** in the event information details page, and enter the handling suggestion.

Note

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

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

Note

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

Auto-Play Video	Check **Auto-Play Video** to automatically play video when displaying event details.
Enlarge Video or Picture	• Double click the video image to view video in a larger window. • Put the cursor on the picture, and click to view picture in a larger window.
Send Email	Select an event and then click **Send Email**, and the information details of this event will be sent by email. **Note** You should configure the email parameters first, see *Set Email Parameters* in the user manual of the client software for details.
Export Event Information	Click **Export** to export the event log or event pictures to the local PC in CSV/Excel file. You can set the saving path manually.
Download Captured Picture	Hover the cursor on the captured picture, and click the download icon on the lower right corner of the picture to download it to the local PC.
Download Event Triggered Video	Hover the cursor on the recorded video, click to download the video (30s before the event happens) triggered by the event.

10.11 System Configuration

10.11.1 Set General Parameters

You can configure the frequently-used parameters, including log expired time, network performance, etc.

Steps

1. Enter the System Configuration module.
2. Click **General** tab to enter the General Settings page.
3. Configure the general parameters.

Date Format / Time Format

The display style of date and time on related pages.

Log Expiry Date

The time for keeping the log files. Once exceeded, the files will be deleted.

Maximum Mode

Select **Maximize** or **Full Screen** as the maximum mode. **Maximize** mode can maximize the display and show the taskbar. **Full Screen** mode can display the client in full-screen mode.

Calendar Type

Select **Gregorian Calendar** or **Nepali Calendar** as the calendar type. If you select **Nepali Calendar**, the calender will switch to Nepali language and calculated time by Nepali calendar. You need to restart the client after switching the calendar.

Network Performance

Set the network conditions to **Normal**, **Better** or **Best**.

Save Pictures in Structure Data Format

You can enable **Save Pictures in Structure Data Format** to save structure data and delete registered picture.

Save Event for

Set the event deleting cycle to delete the old event.

Detect New Software Version

After enabled, the client can automatically detect the new software version and remind the user to upgrade the software.

Automatic Time Synchronization

Automatically synchronize the time of the added devices with the time of the PC running the client at a specified time point.

Auto-Upgrade Device

Set the upgrading mode after the new version of device are detected.

Disable

After enabled, the client will not download the firmware package and upgrade even if the client detects a new version of the client.

Prompt Me If Download and Upgrade

After the client detects a new version of the device, it will prompt the user whether to download the firmware package and upgrade.

Download and Prompt Me If Upgrade

After the client detects the new version of the device, it will download the firmware package automatically, and prompt the user whether to upgrade.

Download and Prompt Automatically

After the client detects the new version of the devices, it will download the firmware package and upgrade the new version automatically.

You need to set a schedule in the **Upgrade Time** field, during which the client upgrades the new version automatically.

4. Click **Save**.

10.11.2 Set Picture Storage

The pictures, captured by the camera of video access control terminal, triggered by events, can be saved in the PC running the iVMS-4200 Service. You can set the picture storage location here manually.

Steps

1. Enter the System Configuration module.
2. Click **Event Picture Storage**.
3. Set the **Store Pictures in Server** switch to on.
   All the disks of the PC running the iVMS-4200 service will show.
4. Select the disk to save the pictures.

   Note
   The default saving path is: Disk/iVMS-4200alarmPicture
5. Click **Save**.

10.11.3 Set Alarm Sound

When the event is triggered, the client can give an audible warning to notify the security personnel. You can set the sound of the audible warning in this section.

Steps

1. Open the System Configuration page.
2. Click **Alarm Sound** tab to enter the Alarm Sound Settings page.
3. **Optional:** Click ··· and select the audio files from the local path for different events.
4. **Optional:** Add customized alarm sound.
   1) Click **Add** to add customized alarm sound.
   2) Double click the **Type** field to customize the alarm sound name as desired.
   3) Click ··· and select the audio files from the local path for different alarms.
5. **Optional:** Click for a testing of the audio file.
6. **Optional:** Click in the Operation column to delete the custom sound.
7. Click **Save**.

   Note
   The format of the audio file can only be WAV.

10.11.4 Set Access Control and Video Intercom Parameters

You can configure the access control and video intercom parameters according to actual needs.

Steps

1. Open the System Configuration page.
2. Click the **Access Control & Video Intercom** tab.
3. Input the required information.

   Ringtone

   Click ... and select the audio file from the local path for the ringtone of indoor station. Optionally, you can click for a testing of the audio file.

   Max. Ring Duration

   Specify the seconds that the ring will last for at most. The maximum ring duration can be set from 15s to 60s.

   Max. Speaking Duration with Indoor Station

   Specify the seconds that the call with indoor station will last for at most. The maximum speaking duration between indoor station and the client can be set from 120s to 600s.

   Max. Speaking Duration with Door Station

   Specify the seconds that the call with door station will last for at most. The maximum speaking duration between door station and the client can be set from 90s to 120s.

   Max. Speaking Duration with Access Control Device

   Specify the seconds that the call with access control device will last for at most. The maximum speaking duration between access control device and the client can be set from 90s to 120s.
4. Click **Save**.

10.11.5 Set File Saving Path

The pictures captured in Status Monitoring module are stored on the local PC. The saving path of these files can be set.

Steps

1. Open the System Configuration page.
2. Click **File** tab to enter the File Saving Path Settings page.
3. Click ... and select a local path for the files.
4. Click **Save**.

10.11.6 Set Email Parameters

When an event is triggered, if you can set **Send Email** as linkage action for this event, the client will an email to the recipients for notification. You need to set the email settings and specify target recipients in this section.

Steps

1. Enter the System Configuration module.

2. Click **Email** tab to enter the Email Settings interface.
3. Enter the required information.

STMP Server

The STMP server IP address of host name (e.g., smtp.263xmail.com)

Encryption Type

You can check the radio to select **Non-Encrypted**, **SSL**, or **STARTTLS** .

Port

Enter the communication port used for SMTP. The port is 25 by default.

Sender Address

The email address of the sender.

Security Certificate (Optional)

If your email server requires authentication, check this checkbox to use authentication to log into the server and enter the login user name and password of your email account.

User Name

Enter the user name of the sender email address if **Server Authentication** is checked.

Password

Enter the password of the sender Email address if **Server Authentication** is checked.

Receiver 1 to 3

Enter the email address of the receiver. Up to 3 receivers can be set.

4. **Optional:** Click **Send Test Email** to send an email to the receiver for test.
5. Click **Save**.

10.12 Operation and Maintenance

You can perform maintaining operations in the menu to ensure a smooth and convenient usage of the client.

In the upper-right corner of the client, click → **File** → **System** → **Tool** , and perform the following operations.

Open Log File

You can open a log file saved in your local PC or log files of the client.

Import/Export Configuration File

You can import configuration files from local PC to the client if needed, and vice versa.

Auto Backup

Select day and time to backup configuration files and data in database, or restore the backed up data.

Skin

Change the skin of the client, including bright-color series and black-color series.

Batch Time Sync

Synchronize selected devices' time with your PC time.

Message Queue

After configuring email linkage, the triggered event(s) will be displayed here. Select an event and cancel sending the an email to the receiver.

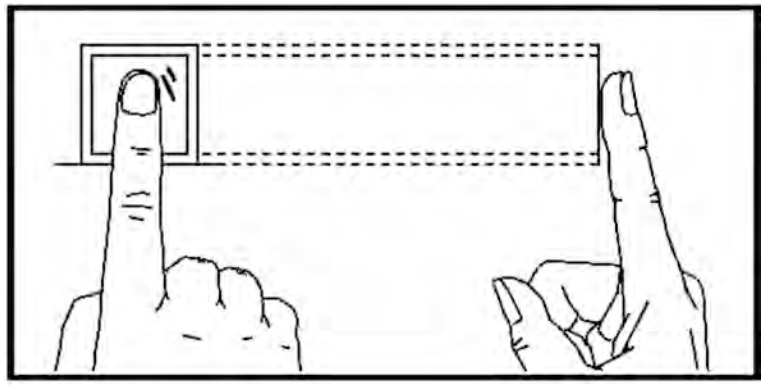
Appendix A. Tips for Scanning Fingerprint

Recommended Finger

Forefinger, middle finger or the third finger.

Correct Scanning

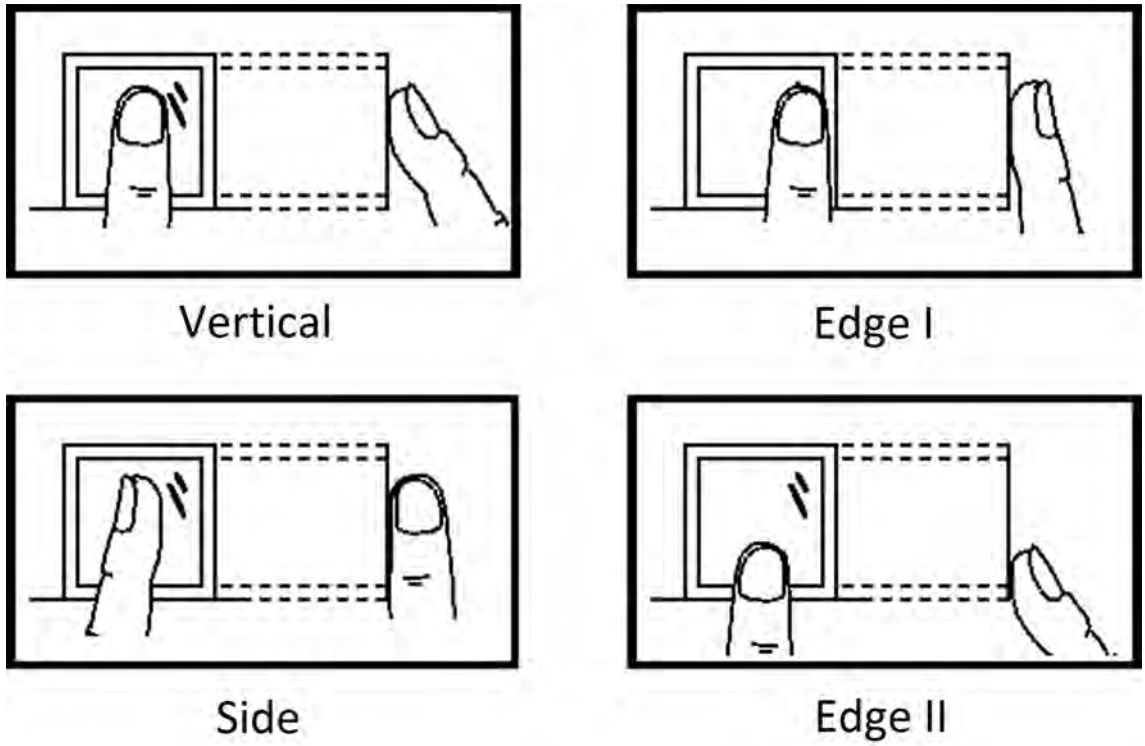
The figure displayed below is the correct way to scan your finger:



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

Incorrect Scanning

The figures of scanning fingerprint displayed below are incorrect:



Environment

The scanner should avoid direct sun light, high temperature, humid conditions and rain.
When it is dry, the scanner may not recognize your fingerprint successfully. You can blow your finger and scan again.

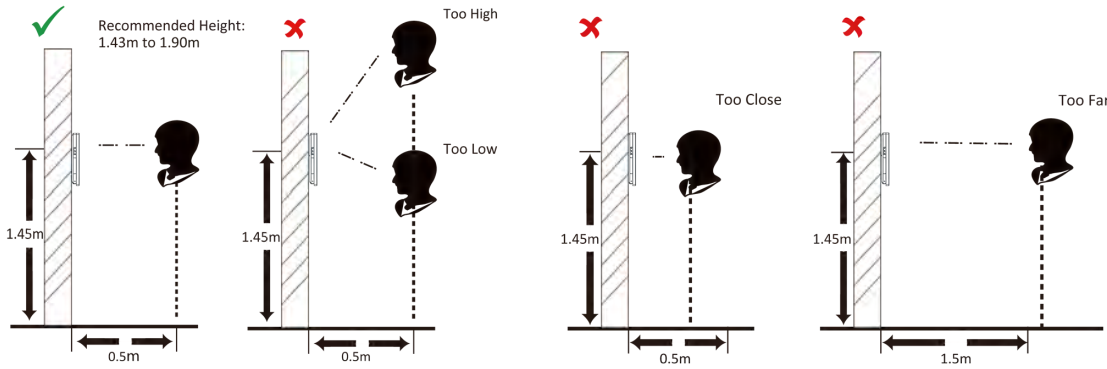
Others

If your fingerprint is shallow, or it is hard to scan your fingerprint, we recommend you to use other authentication methods.
If you have injuries on the scanned finger, the scanner may not recognize. You can change another finger and try again.

Appendix B. Tips When Collecting/Comparing Face Picture

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

Positions (Recommended Distance: 0.5 m)



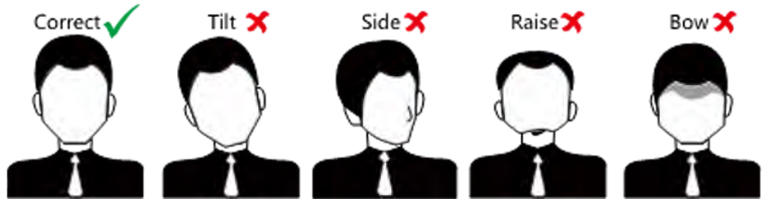
Expression

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

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

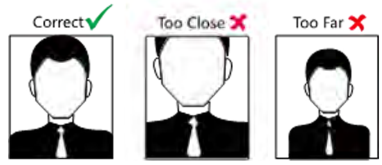
Posture

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



Size

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



Appendix C. Tips for Installation Environment

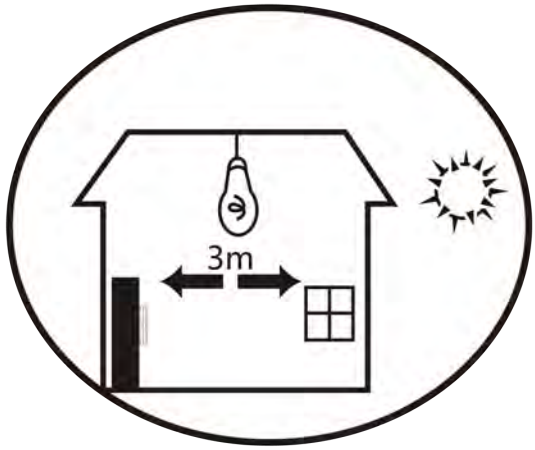
1. Light Source Illumination Reference Value

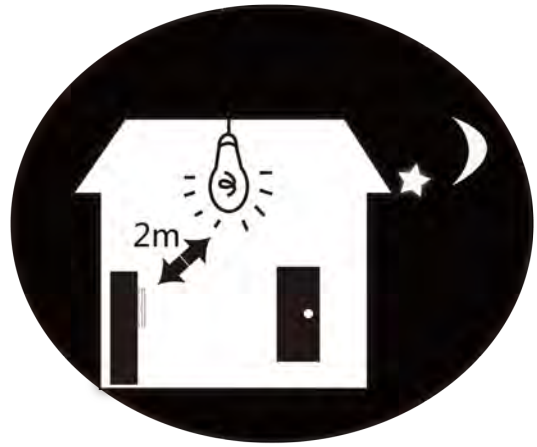
Candle: 10Lux

Bulb: 100~850Lux

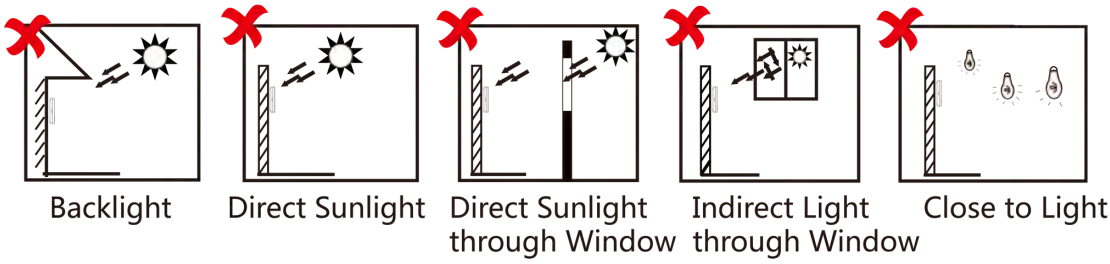
Sunlight: More than 1200Lux

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





3.Avoid backlight, direct and indirect sunlight



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

UD29338B