Face Recognition Terminal

User Manual

Legal Information

©2020 Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

About this Manual

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

Trademarks

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

Disclaimer

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

Data Protection

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

Symbol Conventions

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

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

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
FCC compliance: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
—Reorient or relocate the receiving antenna.
—Increase the separation between the equipment and receiver.
—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
—Consult the dealer or an experienced radio/TV technician for help
This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.
FCC Conditions
This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:
1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement

CE

This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed

under the EMC Directive 2014/30/EU, RE Directive 2014/53/EU,the RoHS Directive 2011/65/EU

2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info

2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see:www.recyclethis.info

Safety Instruction

These instructions are intended to ensure that user can use the product correctly to avoid danger or property loss.

The precaution measure is divided into Dangers and Cautions:

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

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

⚠	⚠
Dangers: Follow these safeguards to prevent serious injury or death.	**Cautions:** Follow these precautions to prevent potential injury or material damage.

⚠ Danger:

- All the electronic operation should be strictly compliance with the electrical safety regulations, fire prevention regulations and other related regulations in your local region.
- Please use the power adapter, which is provided by normal company. 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.
- 1. Risk of explosion if the battery is replaced by an incorrect type
  2. Improper replacement of the battery with an incorrect type may defeat a safeguard (for example, in the case of some lithium battery types).
  3. This equipment is not suitable for use in locations where children are likely to be present.
  4. 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.
  5. 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.
  6. Do not subject the battery to extremely low air pressure, which may result in an explosion or the leakage of flammable liquid or gas.
  7. Dispose of used batteries according to the instructions
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the device yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)

⚠ Cautions:

- Do not drop the device or subject it to physical shock, and do not expose it to high electromagnetism radiation. Avoid the equipment installation on vibrations surface or places subject to shock (ignorance can cause equipment damage).
- Do not place the device in extremely hot (refer to the specification of the device for the detailed operating temperature), cold, dusty or damp locations, and do not expose it to high electromagnetic radiation.
- The device cover for indoor use shall be kept from rain and moisture.
- Exposing the equipment to direct sun light, low ventilation or heat source such as heater or radiator is forbidden (ignorance can cause fire danger).
- Do not aim the device at the sun or extra bright places. A blooming or smear may occur otherwise (which is not a malfunction however), and affecting the endurance of sensor at the same time.
- Please use the provided glove when open up the device cover, avoid direct contact with the device cover, because the acidic sweat of the fingers may erode the surface coating of the device cover.
- Please use a soft and dry cloth when clean inside and outside surfaces of the device cover, do not use alkaline detergents.
- Please keep all wrappers after unpack them for future use. In case of any failure occurred, you need to return the device to the factory with the original wrapper. Transportation without the original wrapper may result in damage on the device and lead to additional costs.
- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.
- Biometric recognition products are not completely applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.
- 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
Face Recognition Terminal	DS-K1T672M
	DS-K1T672MW
	DS-K1T672E

Use only power supplies listed in the user instructions:

Model	Manufacturer	Standard
ADS-26FSG-12 12024EPG	Shenzhen Honor Electronic Co.,Ltd	PG
MSA-C2000IC12.0-24P-DE	MOSO Technology Co.,Ltd	PDE
ADS-26FSG-12 12024EPB	Shenzhen Honor Electronic Co.,Ltd	PB
ADS-26FSG-12 12024EPCU/EPC	Shenzhen Honor Electronic Co.,Ltd	PCU
ADS-26FSG-12 12024EPI-01	Shenzhen Honor Electronic Co.,Ltd	PI
ADS-26FSG-12 12024EPBR	Shenzhen Honor Electronic Co.,Ltd	PBR

Contents

Chapter 1 Overview

1.1 Overview

Face recognition terminal is a kind of access control device for face recognition, which is mainly applied in security access control systems, such as logistic centers, airports, university campuses, alarm centrals, dwellings, etc.

1.2 Features

- 7-inch touch screen with bezel-less design
- Presents card on the screen to authenticate card permission.
- 2 MP wide-angle dual-lens
- Face anti-spoofing
- Face recognition distance: 0.3 m to 3 m
- Deep learning algorithm
- 50,000 face capacity, 50,000 card capacity, and 50,000 event capacity
- Face recognition duration ＜ 0.2 s/User; face recognition accuracy rate ≥ 99%
- Capture linkage and captured pictures storage
- Transmits card and user data from or to the client software via TCP/IP protocol and saves the data on the client software
- Imports pictures from the USB flash drive to the device or export pictures, events, from the device to the USB flash drive
- Stand-alone operation
- Manage, search and set device data after logging in the device locally
- Connects to one external card reader via RS-485 protocol
- Connects to secure door control unit via RS-485 protocol to avoid the door opening when the terminal is destroyed
- Connects to external access controller or Wiegand card reader via Wiegand protocol
- Two-way audio with indoor station and main station
- Supports 6 attendance status, including check in, check out, break in, break out, overtime in, overtime out
- Configuration via the web client
- Remotely opens door and starts live view via Hik-Connect
- Supports ISAPI and ISUP5.0 protocol
- Self-defined voice prompt of authentication result
- Support English, Spanish (South America), Arabic, Thai, Indonesian, Russian, Vietnamese, Portuguese (Brazil)

spec-tip

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

Chapter 2 Appearance

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

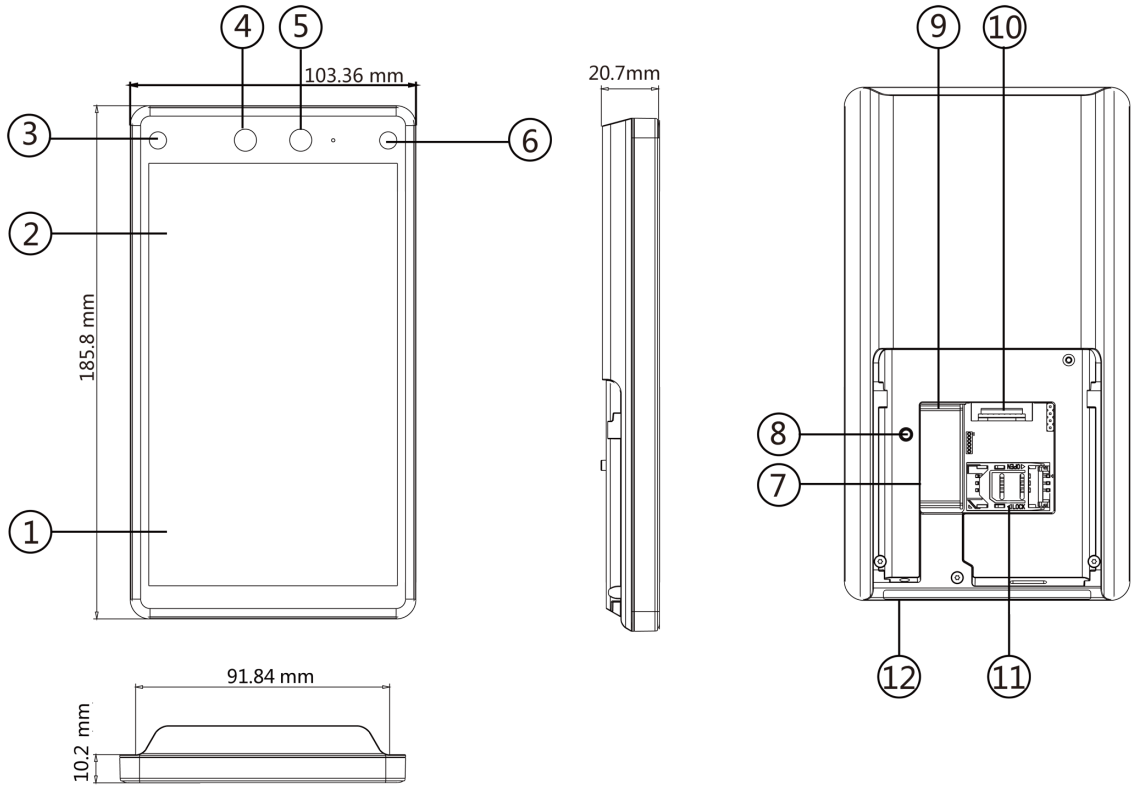


Figure 2-1 Face Recognition Terminal Diagram

Table 2-1 Description of Face Recognition Terminal

No.	Description
1	Card Presenting Area
2	Display Screen
3	IR Light
4	Camera
5	Camera
6	IR Light
7	Debugging Port

No.	Description
8	Tamper
9	Network Interface
10	Wiring Terminals
11	PSAM Card Slot (Reserved)
12	microUSB Interface Included **Note** USB to micro USB cable is included in the package.

Chapter 3 Installation

3.1 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*.

3.2 Flush Mounting with Gang Box (Type I)

Steps

Note

- The hole distance of the gang box is 83.3 mm to 83.5 mm.
- The additional force shall be equal to three times the weight of the equipment. The equipment ad its associated mounting means shall remain secure during the installation. After the installation, the equipment, including any associated mounting plate, shall not be damaged.

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

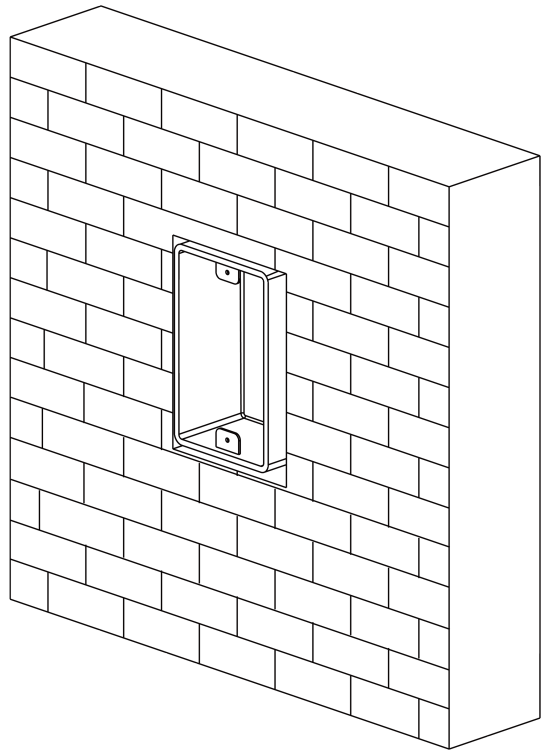


Figure 3-1 Install Gang Box

2. Use 1 supplied screws (Pa4×25) to secure the base plate on the gang box.

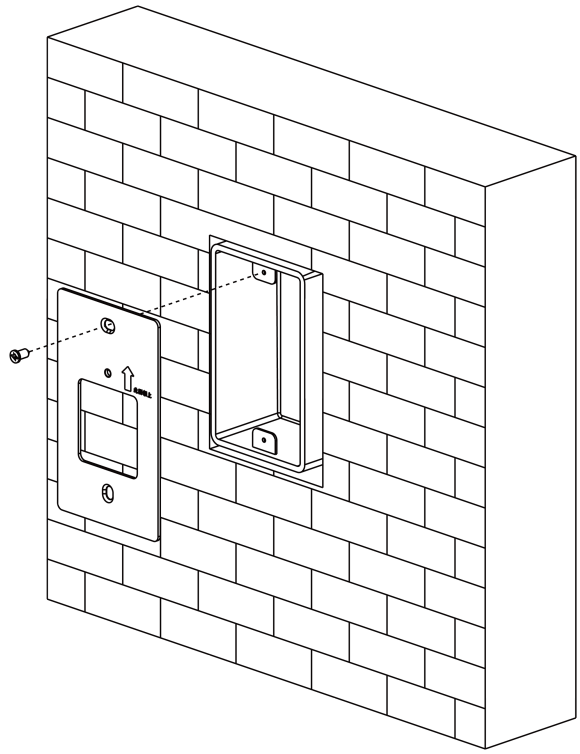


Figure 3-2 Secure Base Plate

3. Use another 2 supplied screws (K1M4×8) to secure the mounting plate on the base plate.

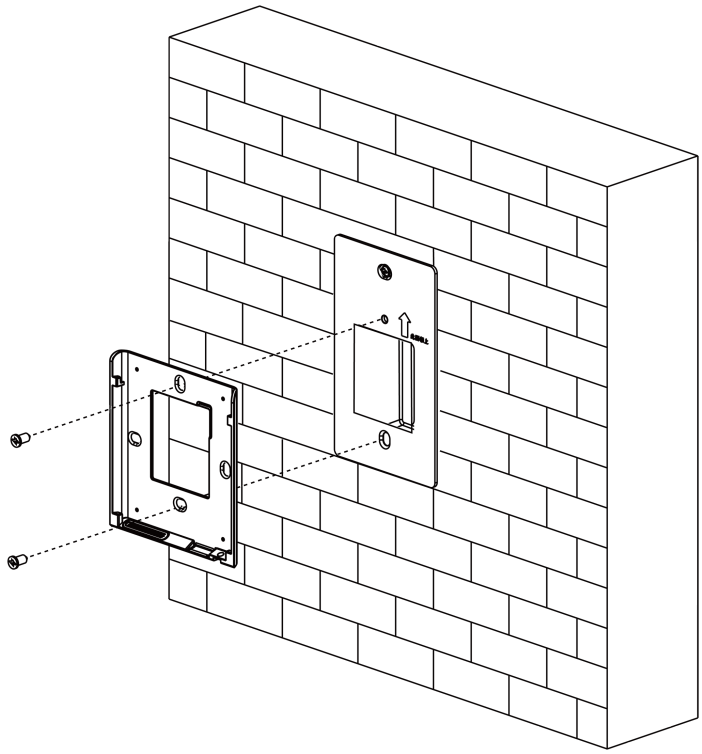


Figure 3-3 Install Mounting Plate

4. Route the cable through the cable hole of the mounting plate, and connect to corresponding external devices' cables.
5. Align the device with the mounting plate and hang the device on the mounting plate.

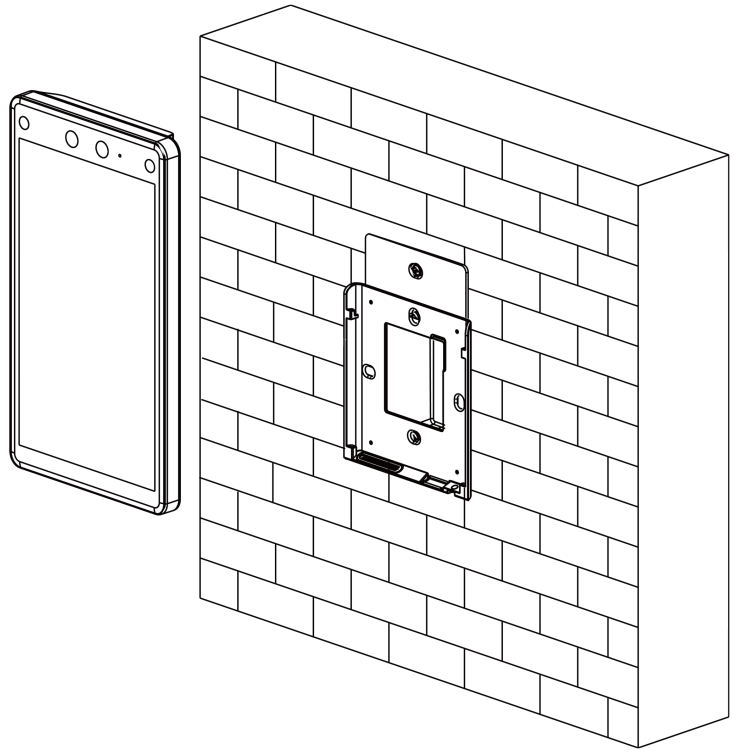


Figure 3-4 Hang Device

6. Use 1 supplied screw (KM3×6) to secure the device and the mounting plate.

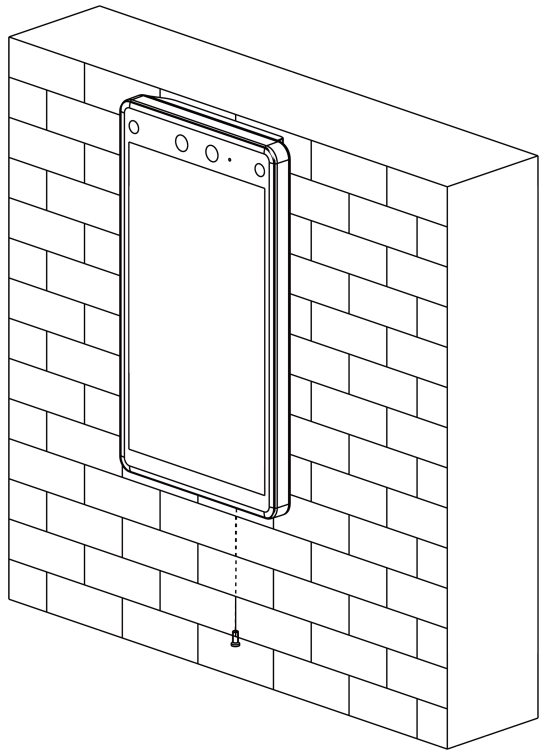


Figure 3-5 Secure Device

3.3 Flush Mounting with Gang Box (Type II)

Steps

Note

- The hole distance of the gang box is 60 mm.
- The additional force shall be equal to three times the weight of the equipment. The equipment ad its associated mounting means shall remain secure during the installation. After the installation, the equipment, including any associated mounting plate, shall not be damaged.

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

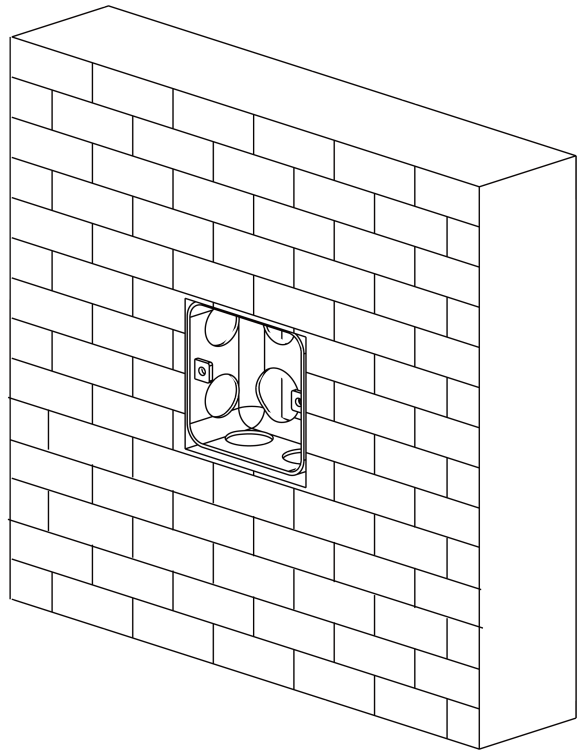


Figure 3-6 Install Gang Box

2. Remove the cable hole with tool and use two supplied screws (Pa4×25) to secure the mounting plate on the gang box.

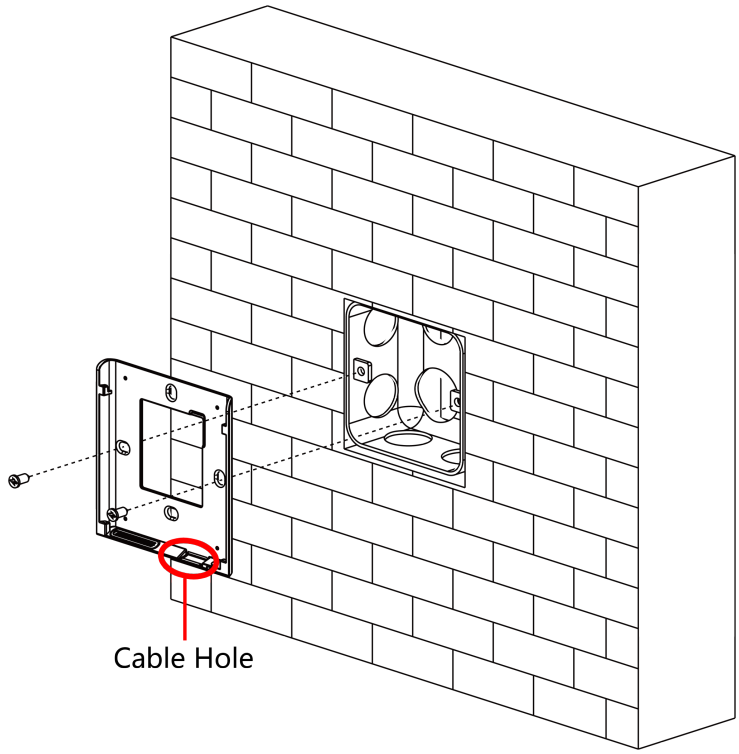


Figure 3-7 Install Mounting Plate

3. Route the cable through the cable hole of the mounting plate, and connect to corresponding external devices' cables.
4. Align the device with the mounting plate and hang the device on the mounting plate.

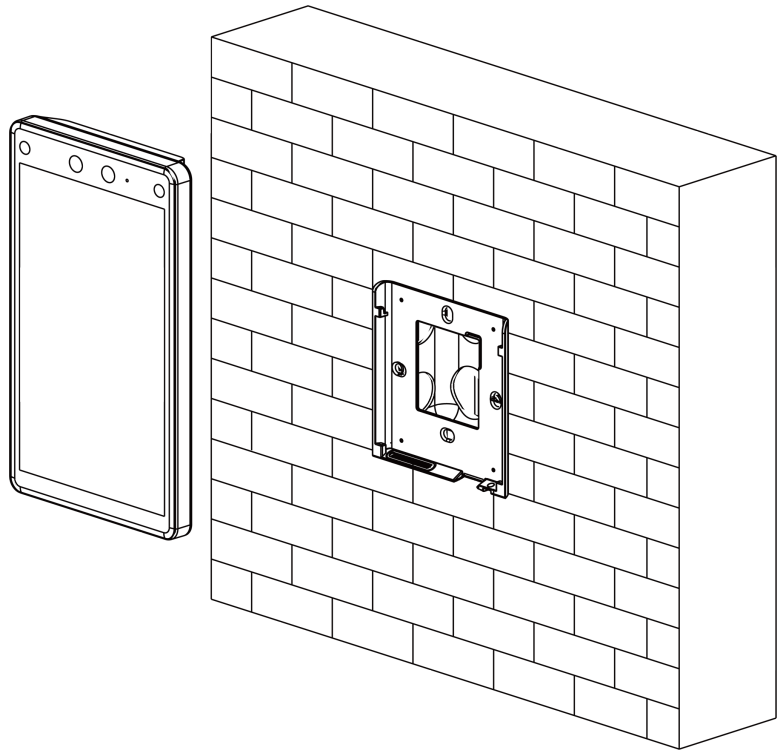


Figure 3-8 Hang Device

5. Use 1 supplied screws (KM3×6) to secure the device and the mounting plate.

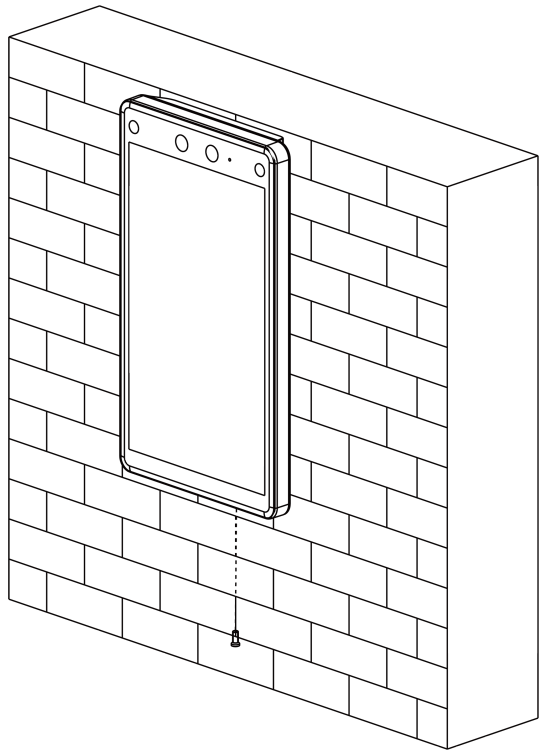


Figure 3-9 Secure Device

3.4 Surface Mounting

Steps

Note

The additional force shall be equal to three times the weight of the equipment. The equipment ad its associated mounting means shall remain secure during the installation. After the installation, the equipment, including any associated mounting plate, shall not be damaged.

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

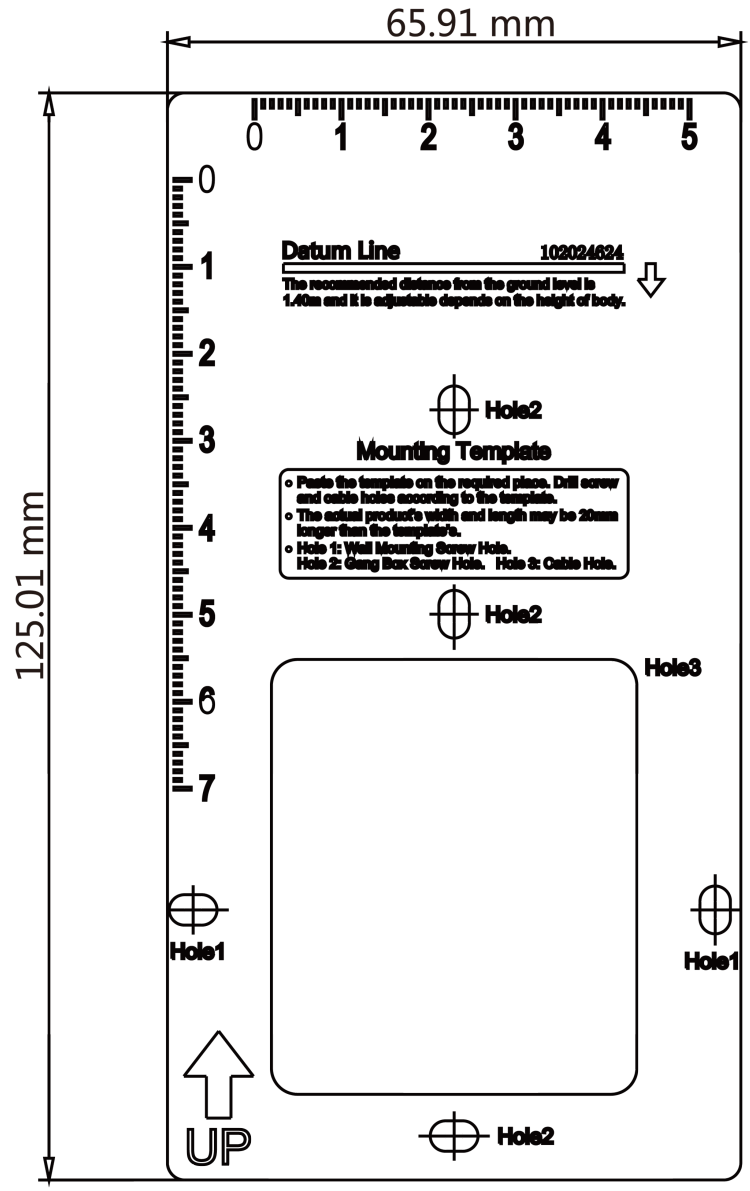


Figure 3-10 Mounting Template

2. Drill holes on the wall or other surface according to the Hole 1 on the mounting template.
3. Remove the cable hole on the mounting plate with tools.
4. Align the holes to the mounting plate and secure the mounting plate on the wall with the 2 supplied screws (Pa4×25).

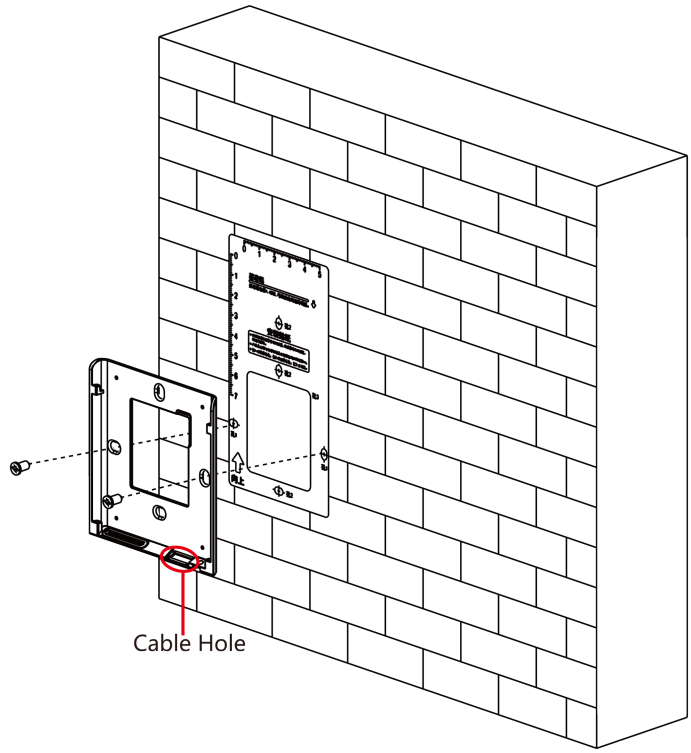


Figure 3-11 Install Mounting Plate

5. Route the cable through the cable hole of the mounting plate, and connect to corresponding external devices' cables.
6. Align the device with the mounting plate and hang the device on the mounting plate.

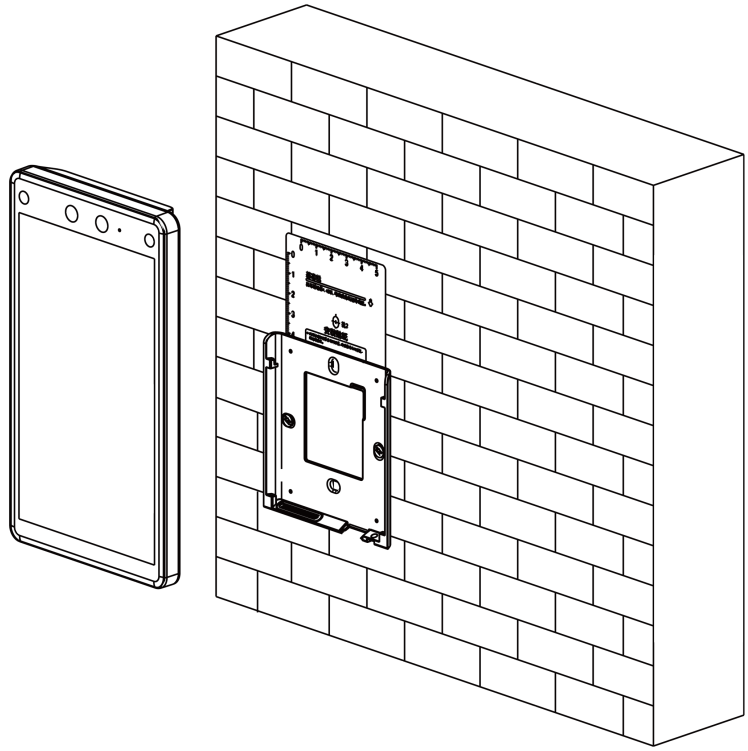


Figure 3-12 Hang Device

7. Use 1 supplied screw (KM3×6) to secure the device and the mounting plate.

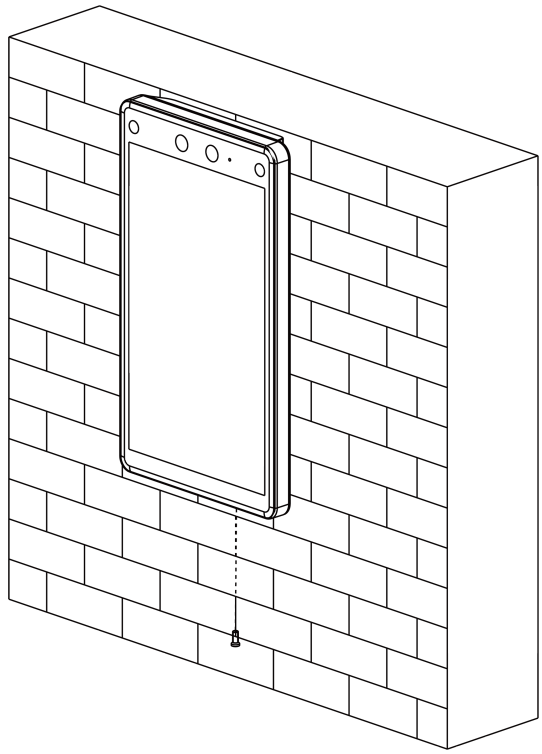


Figure 3-13 Secure Device

Chapter 4 Wiring

The device supports connecting to the RS-485 terminal, the door lock, the exit button, the alarm output/input devices, the Wiegand card reader, the access controller, and the power supply. You can wire the peripherals according to the descriptions below.

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

Note

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

4.1 Terminal Description

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

The terminal's diagram is as follows:

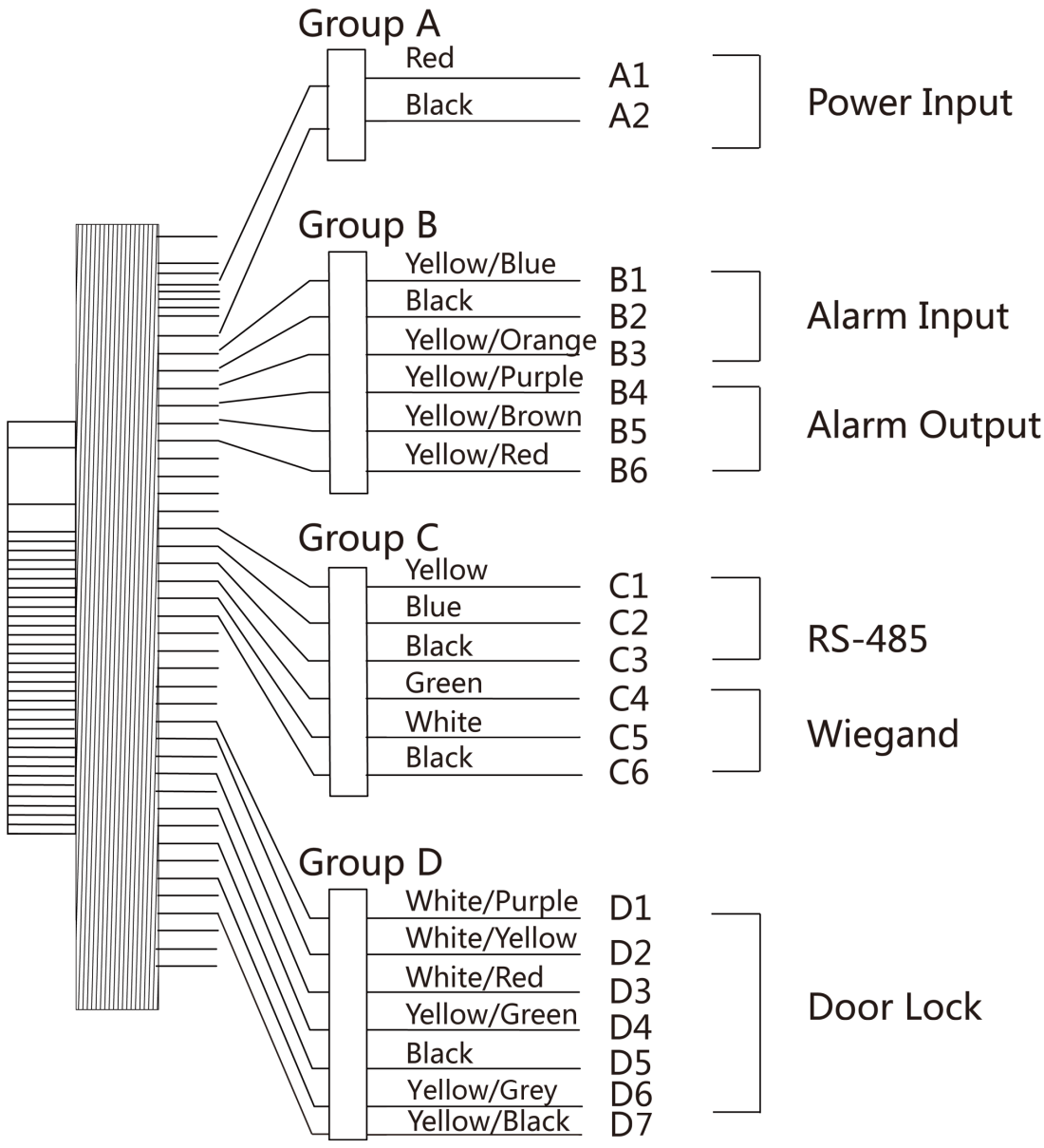


Figure 4-1 Terminal Diagram

The descriptions of the terminals are as follows:

Table 4-1 Terminal Descriptions

Group	No.	Function	Color	Name	Description
Group A	A1	Power Input	Red	+12 V	12 VDC Power Supply
	A2		Black	GND	Ground

Group	No.	Function	Color	Name	Description
Group B	B1	Alarm Input	Yellow/Blue	IN1	Alarm Input 1
	B2		Black	GND	Ground
	B3		Yellow/Orange	IN2	Alarm Input 2
	B4	Alarm Output	Yellow/Purple	NC	Alarm Output Wiring
	B5		Yellow/Brown	COM	
	B6		Yellow/Red	NO	
Group C	C1	RS-485	Yellow	485+	RS-485 Wiring
	C2		Blue	485-	
	C3		Black	GND	Ground
	C4	Wiegand	Green	W0	Wiegand Wiring 0
	C5		White	W1	Wiegand Wiring 1
	C6		Black	GND	Ground
Group D	D1	Door Lock	White/Purple	NC	Lock Wiring (NC)
	D2		White/Yellow	COM	Common
	D3		White/Red	NO	Lock Wiring (NO)
	D4		Yellow/Green	SENSOR	Door Contact
	D5		Black	GND	Ground
	D6		Yellow/Gray	BTN	Exit Door Wiring
	D7		Yellow/Black	GND	Ground

4.2 Wire Normal Device

You can connect the terminal with normal peripherals.

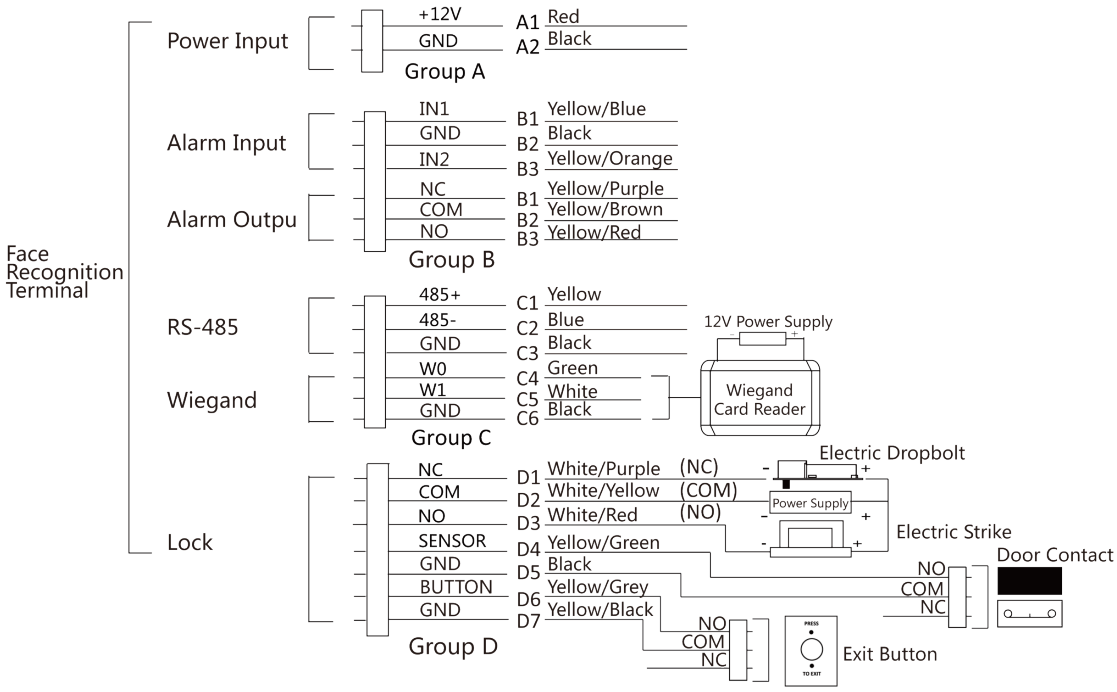


Figure 4-2 Device Wiring

Note

- You should set the face recognition terminal's Wiegand direction as **Input** to connect to a Wiegand card reader. If connects to an access controller, you should set the Wiegand direction as **Output** to transmit authentication information to the access controller.
- For details about Wiegand direction settings, see ***Set Wiegand Parameters*** .
- Do not wire the device to the electric supply directly.

4.3 Wire Secure Door Control Unit

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

The wiring diagram is as follows.

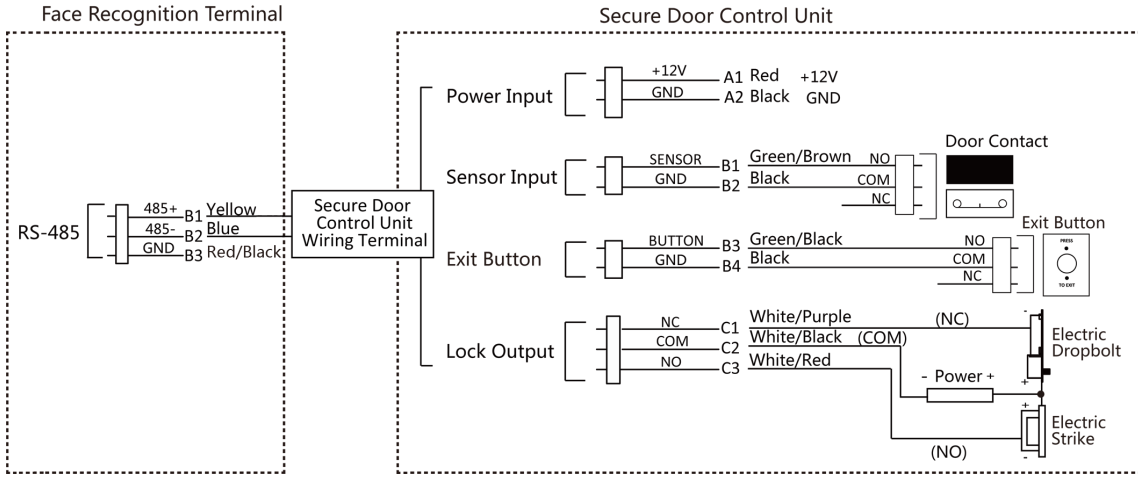


Figure 4-3 Secure Door Control Unit Wiring

Note

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

4.4 Wire Fire Module

4.4.1 Wiring Diagram of Door Open When Powering Off

Lock Type: Anode Lock, Magnetic Lock, and Electric Bolt (NO)

Security Type: Door Open When Powering Off

Scenario: Installed in Fire Engine Access

Type 1

Note

The fire system controls the power supply of the access control system.

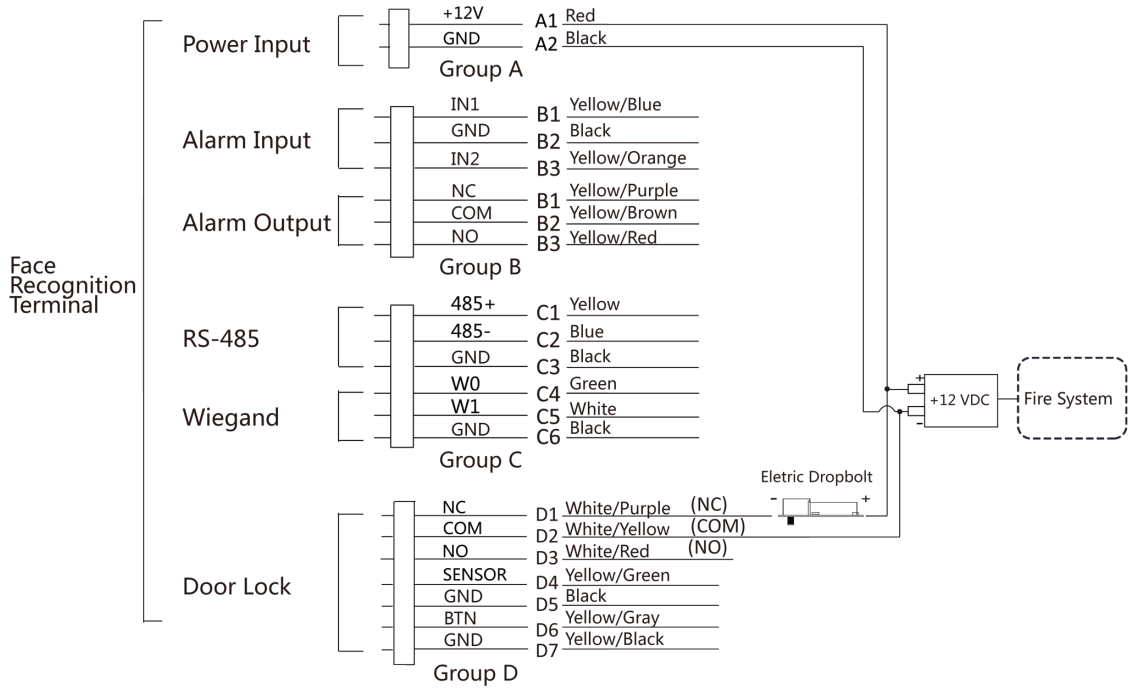


Figure 4-4 Wire Device

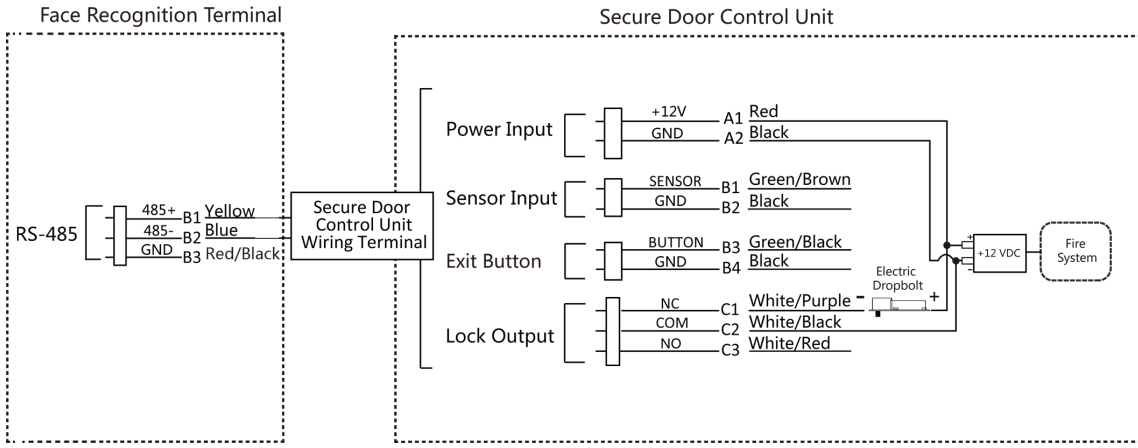


Figure 4-5 Wire Secure Door Control Unit

Type 2

Note

The fire system (NO and COM, normally open when powering off) is connected with the lock and the power supply in series. When an fire alarm is triggered, the door remains open. In normal times, NO and COM are closed.

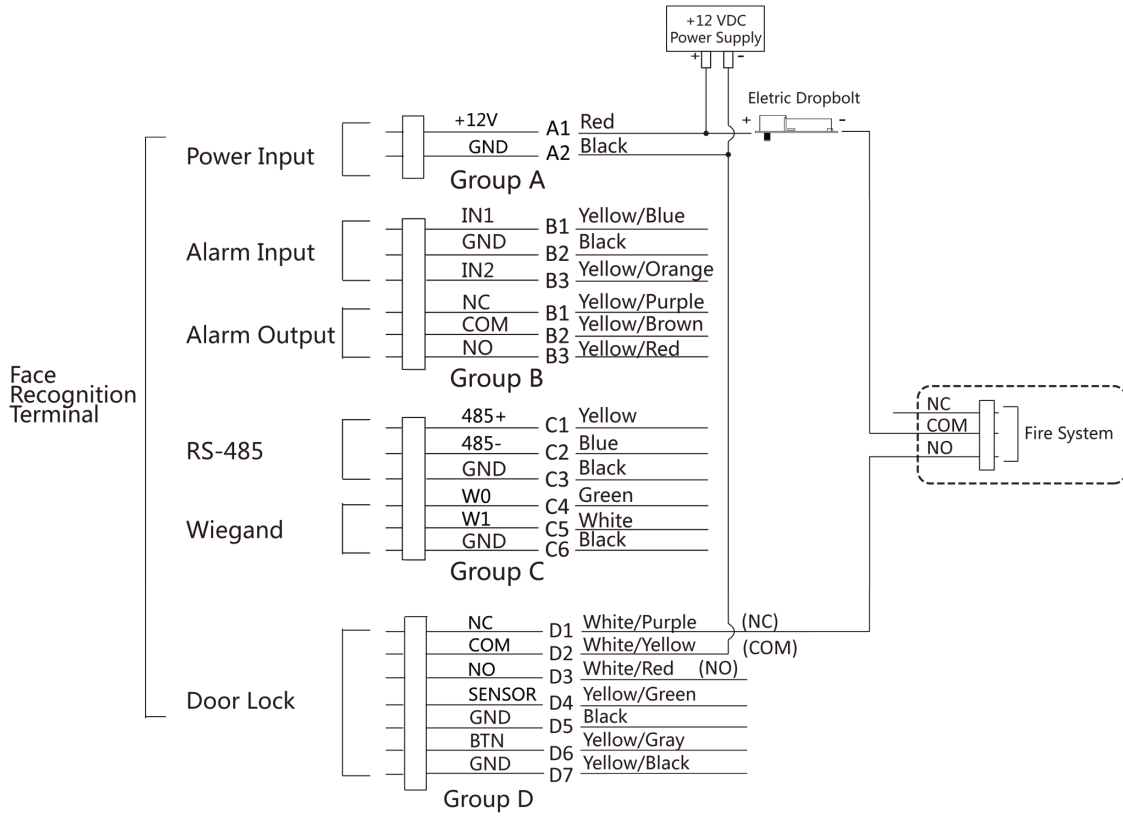


Figure 4-6 Wiring Device

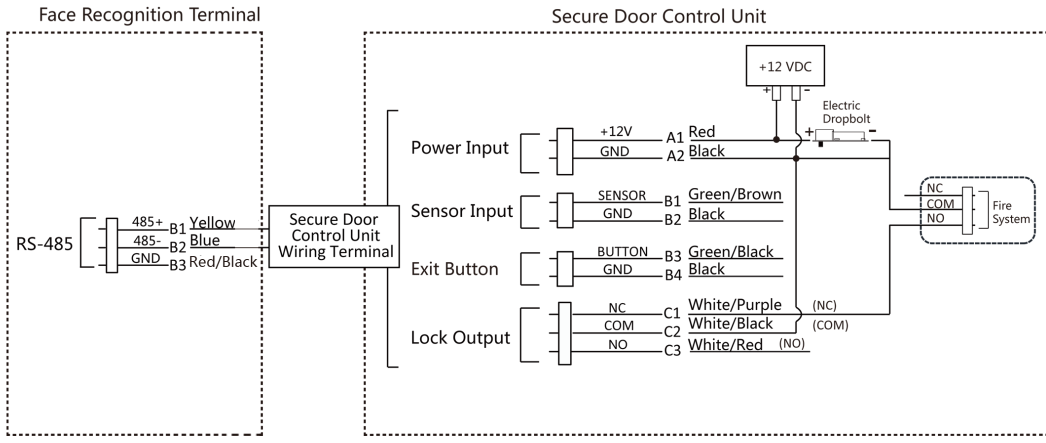


Figure 4-7 Wiring Secure Door Control Unit

4.4.2 Wiring Diagram of Door Locked When Powering Off

Lock Type: Cathode Lock, Electric Lock, and Electric Bolt (NC)

Security Type: Door Locked When Powering Off

Scenario: Installed in Entrance/Exit with Fire Linkage

Note

- The Uninterpretable Power Supply (UPS) is required.
- The fire system (NC and COM, normally closed when powering off) is connected with the lock and the power supply in series. When an fire alarm is triggered, the door remains open. In normal times, NC and COM are open.

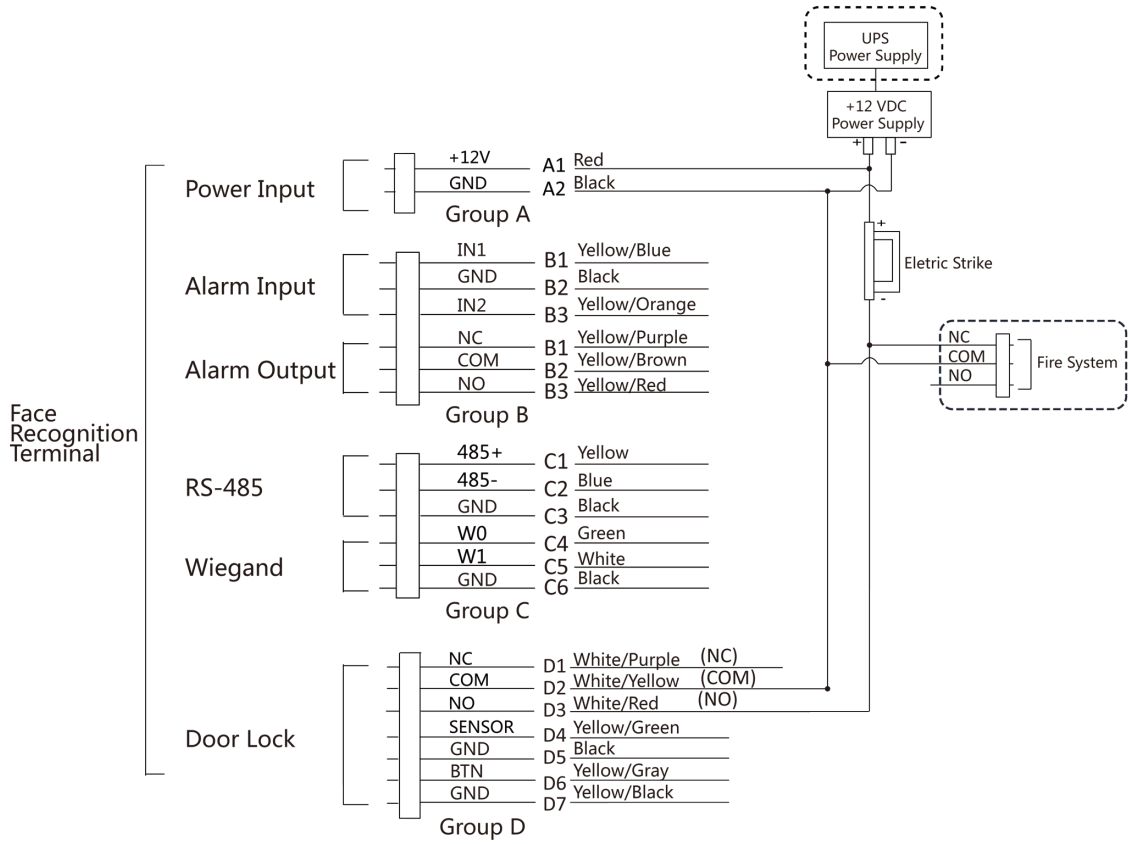


Figure 4-8 Device Wiring

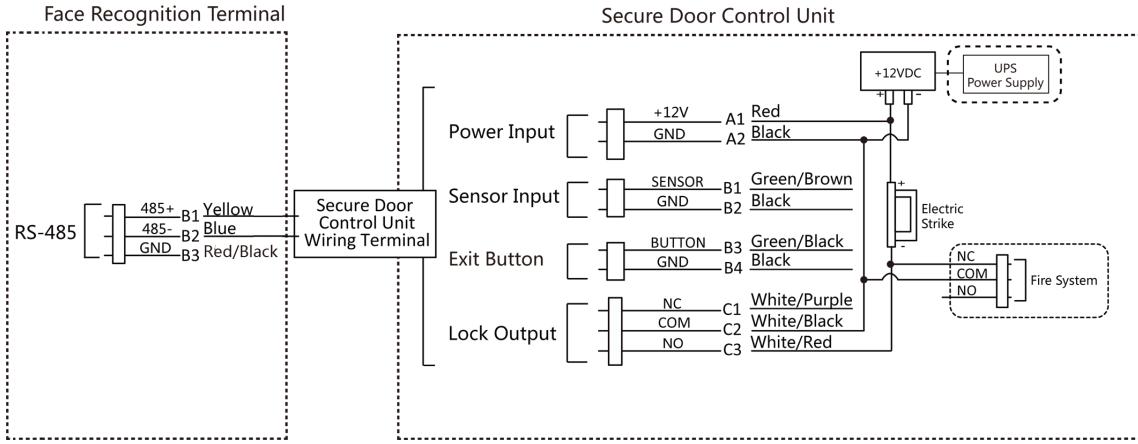


Figure 4-9 Wiring Diagram

Chapter 5 Activation

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

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

The default values of the device are as follows:

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

5.1 Activate via Device

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

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

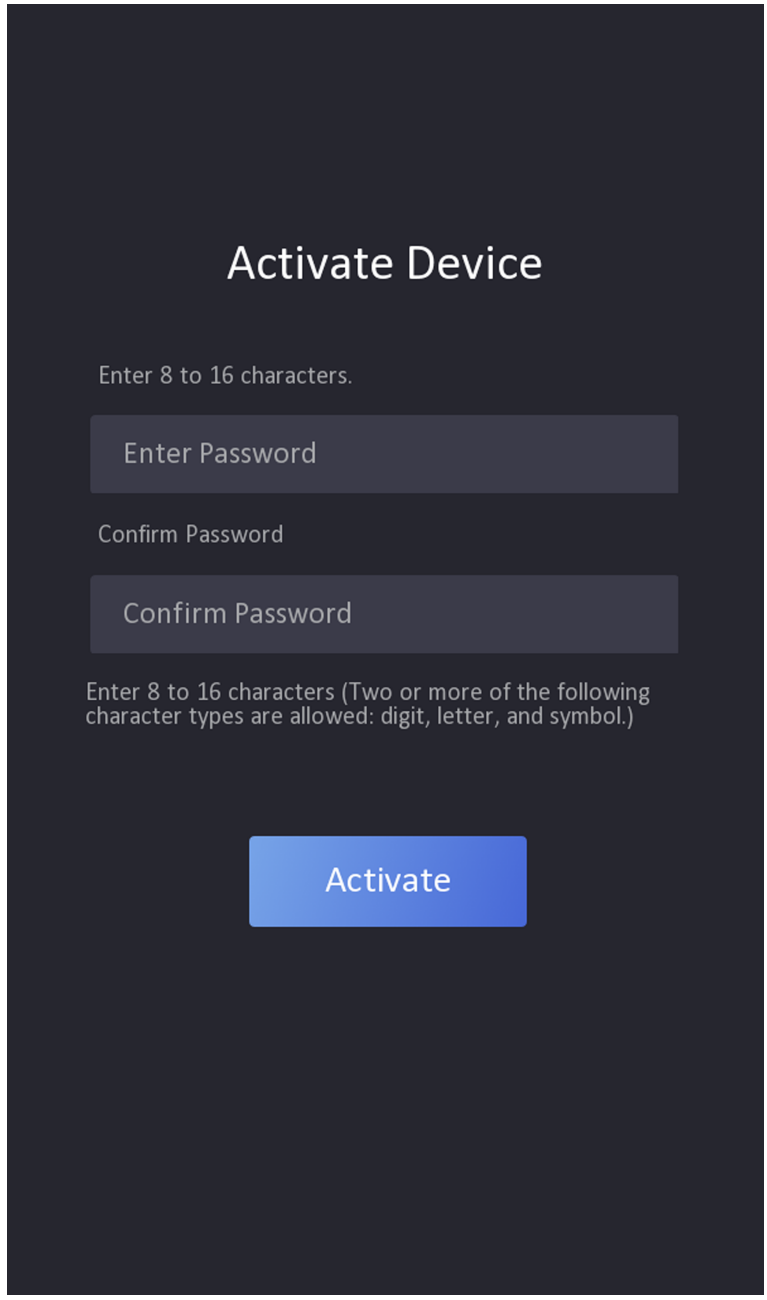


Figure 5-1 Activation Page

Caution

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

characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.
Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

Note

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

- After activation, you should select a language according to your actual needs.
- After activation, you should select an application mode. For details, see ***Set Application Mode*** .
- After activation, if you need to add the device to the client software or other platforms, you should edit the device IP address. For details, see ***Set Network Parameters*** .
- After activation, if you need to operate the device remotely via APP, you should scan the QR code to link to the APP. For details, see .
- After activation, if you need to add administrator to manage the device parameters, you should set administrator. For details, see ***Add Administrator*** .

5.2 Activate via 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.

5.3 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.

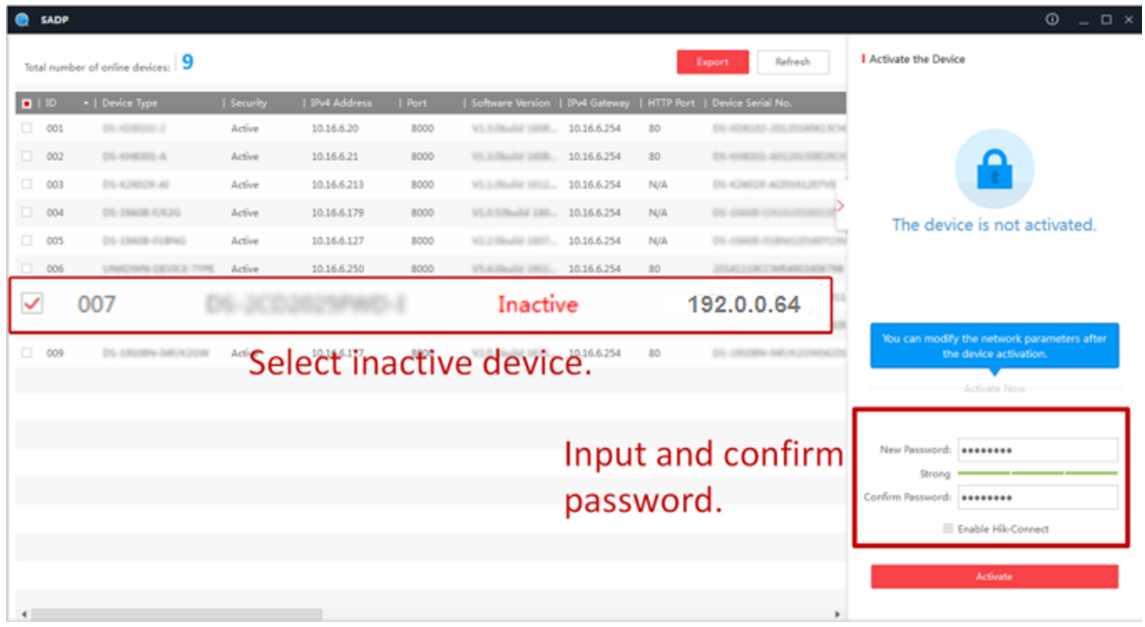
Caution

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.

5.4 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 6 Quick Operation

6.1 Select Language

You can select a language for the device system.

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

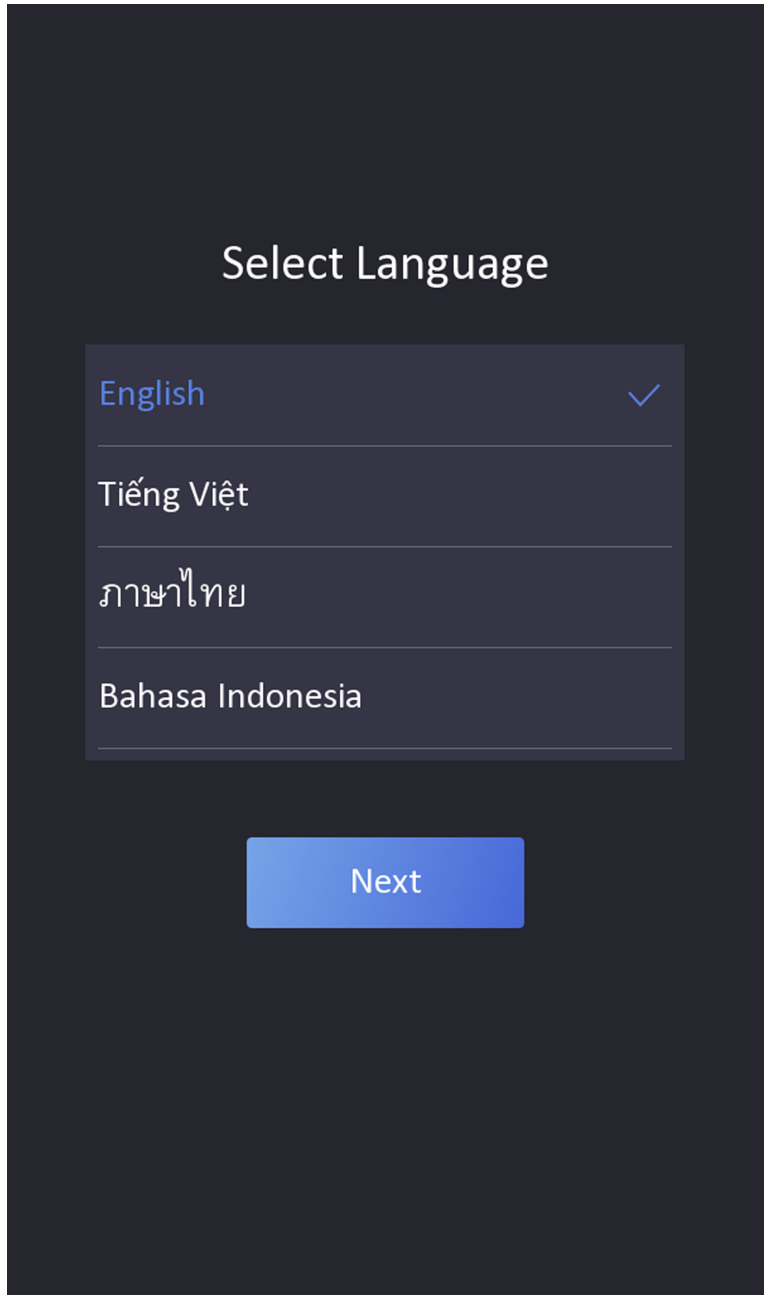


Figure 6-1 Select System Language

By default, the system language is English.

Note

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

6.2 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**.

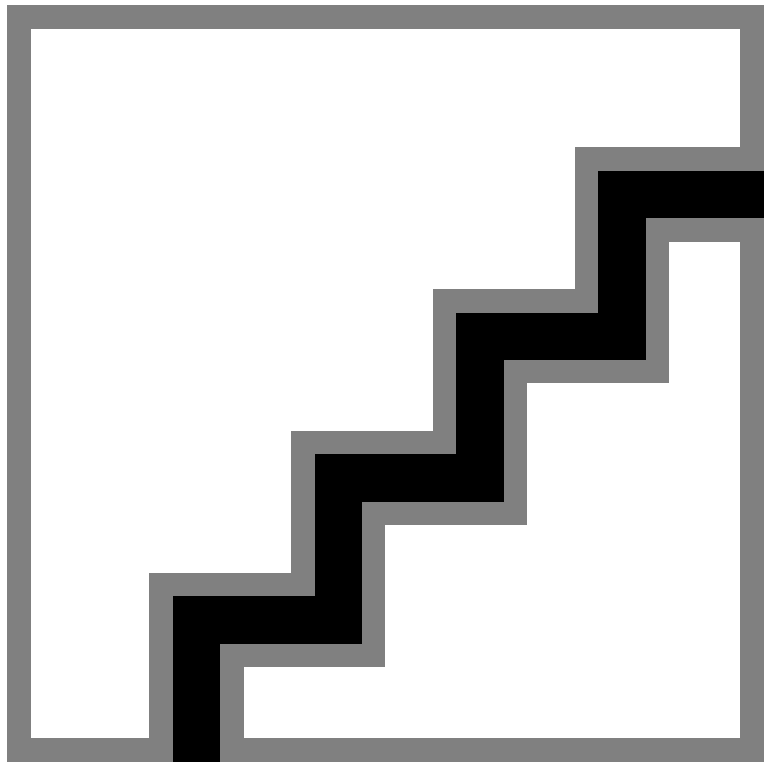


Figure 6-2 Password Change Page

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.

6.3 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.

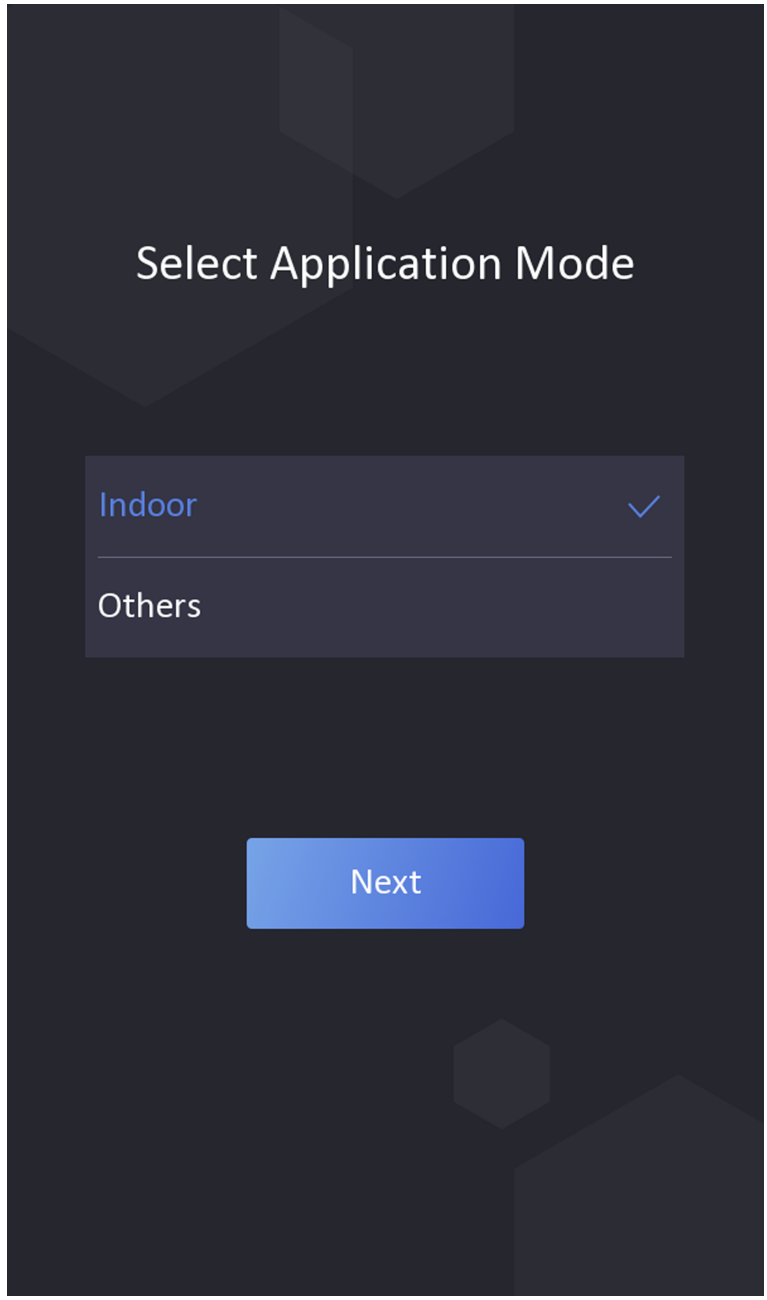


Figure 6-3 Welcome Page

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.

6.4 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.

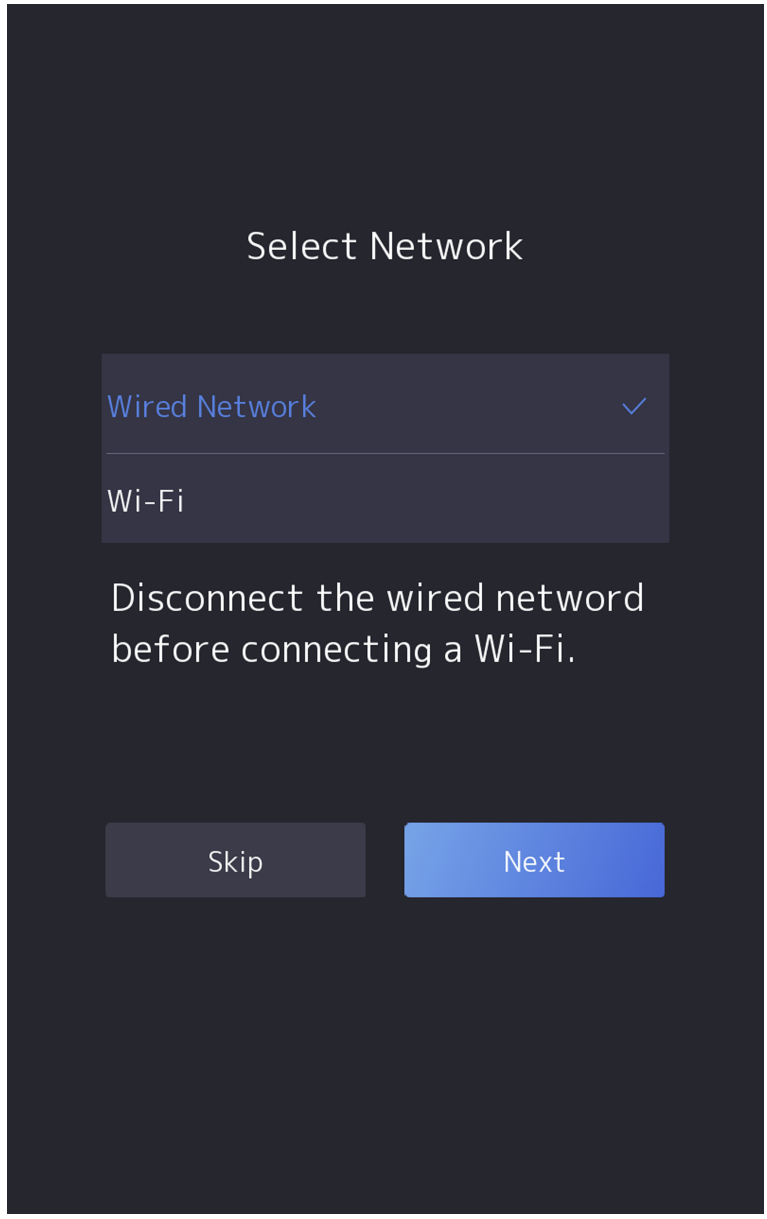


Figure 6-4 Select Network

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.

6.5 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.

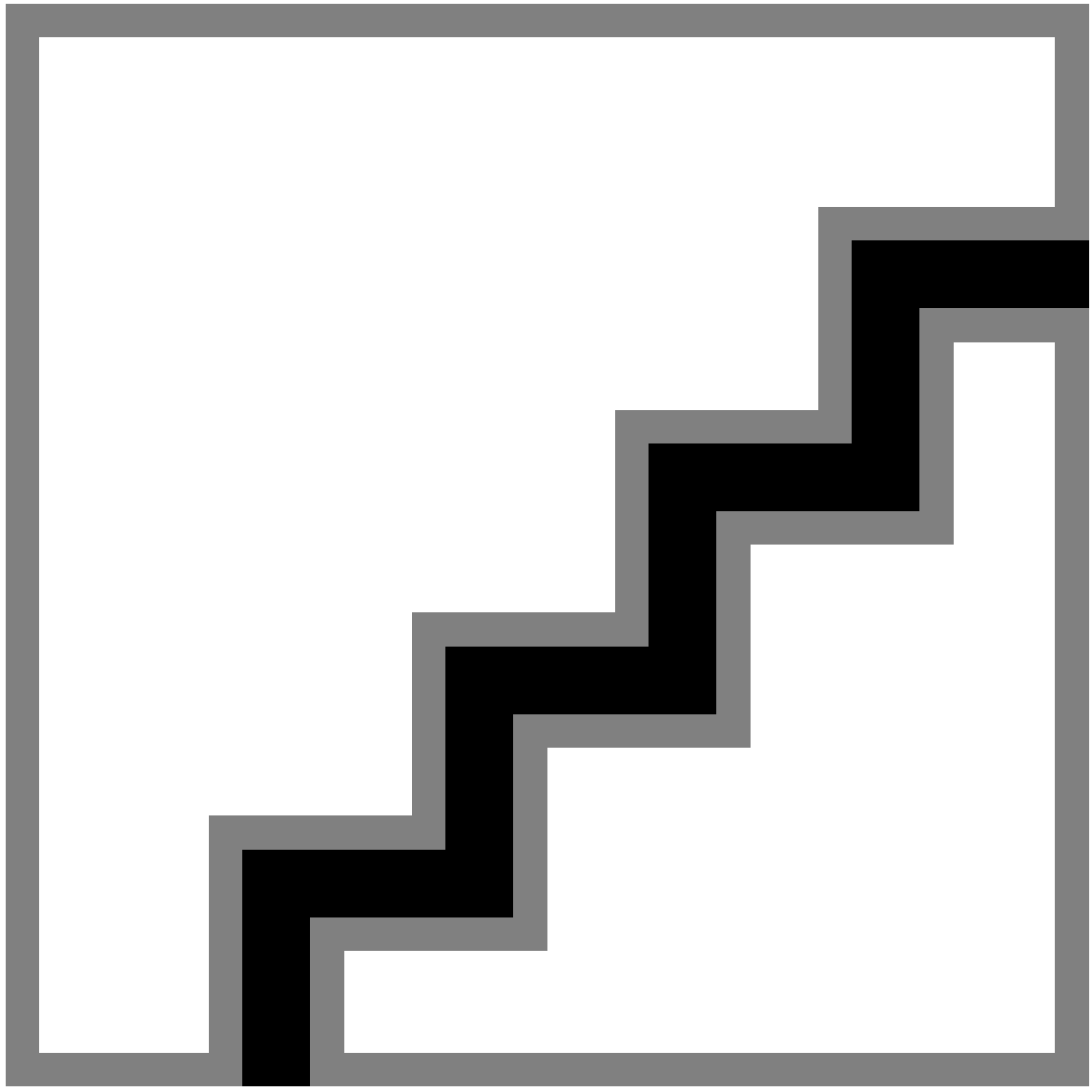


Figure 6-5 Access to Hik-Connect

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.

6.6 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.

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.

6.7 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**.

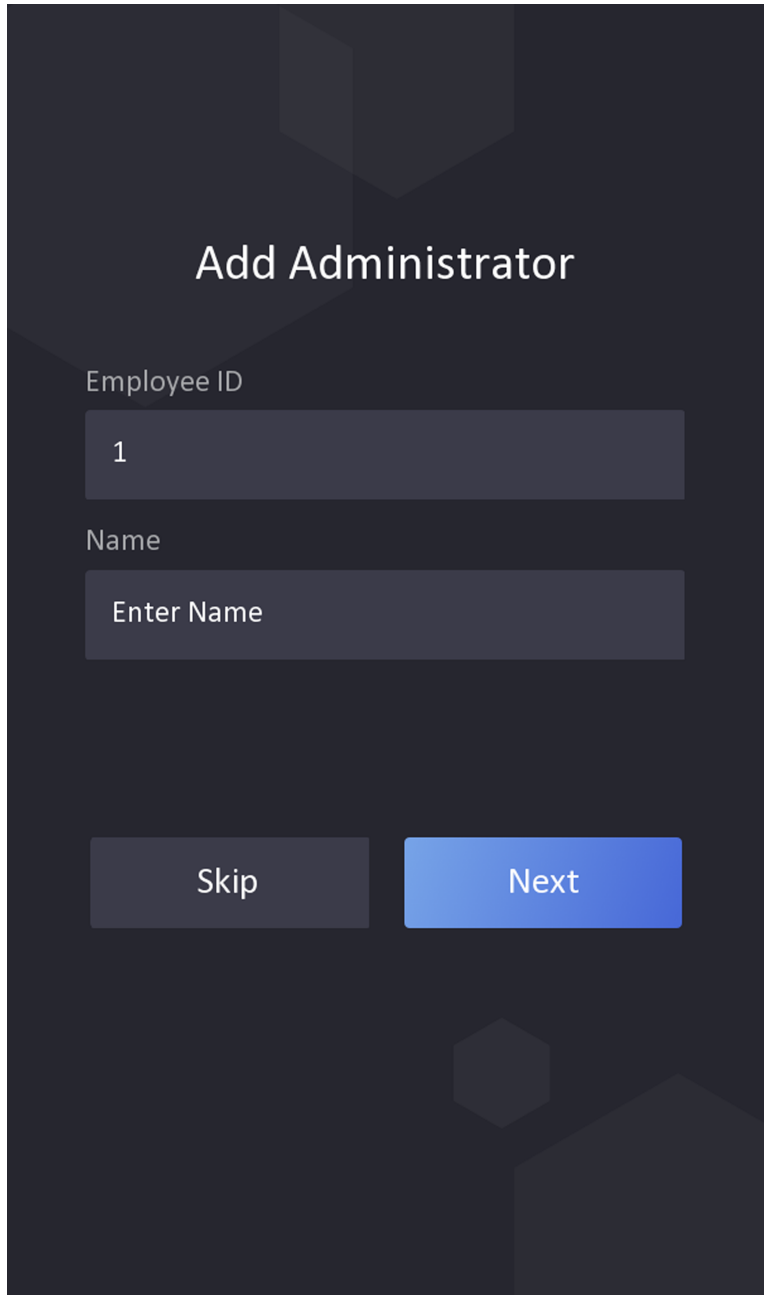


Figure 6-6 Add Administrator Page

3. Select a credential to add.

Note

Up to one credential should be added.

- : Face forward at the camera. Make sure the face is in the face recognition area. Click to capture and click to confirm.

- : Enter the card No. or present card on the card presenting area. Click **OK**.

4. Click **OK**.

You will enter the authentication page.

Status Icon Description

/

Device is armed/not armed.

/

Hik-Connect is enabled/disabled.

/ /

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

/ /

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

Shortcut Keys Description

Note

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

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 7 Basic Operation

7.1 Login

Login the device to set the device basic parameters.

7.1.1 Login by Administrator

If you have added an administrator for the device, only the administrator can login the device for device operation.

Steps

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

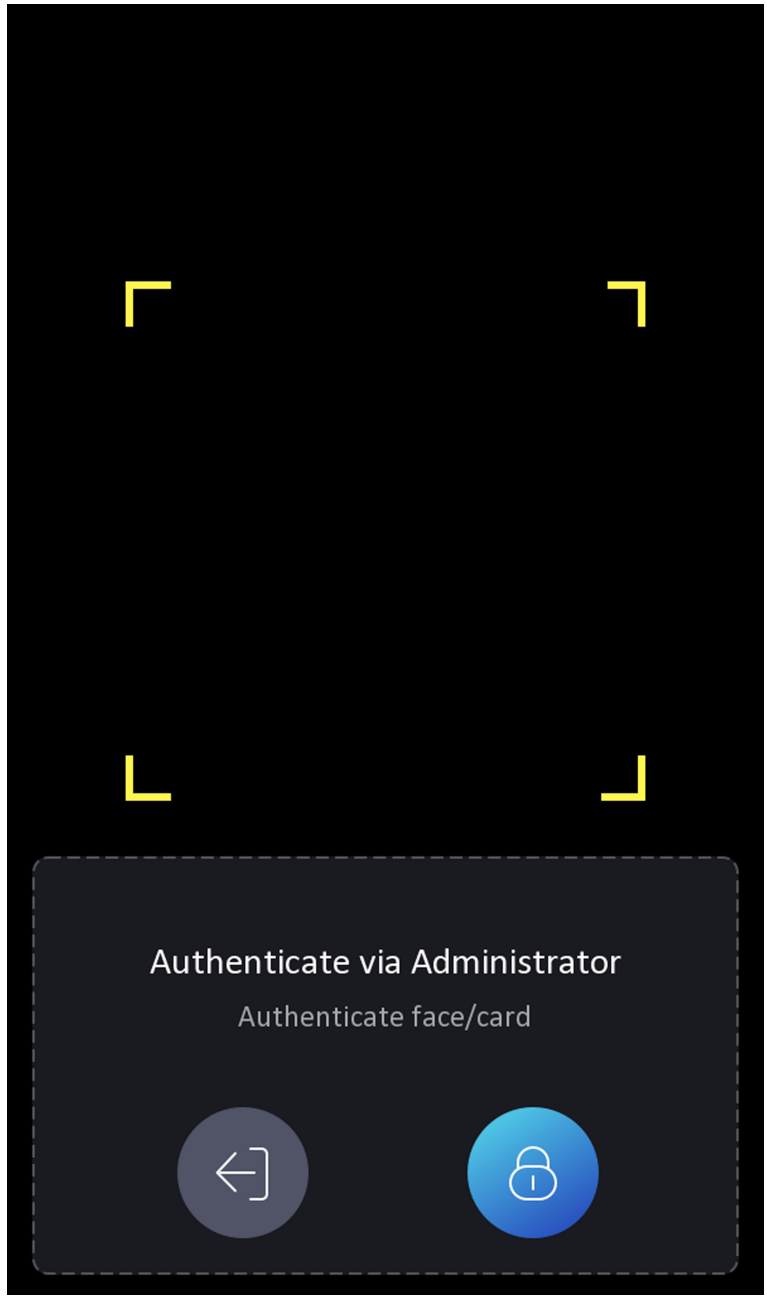


Figure 7-1 Admin Login

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

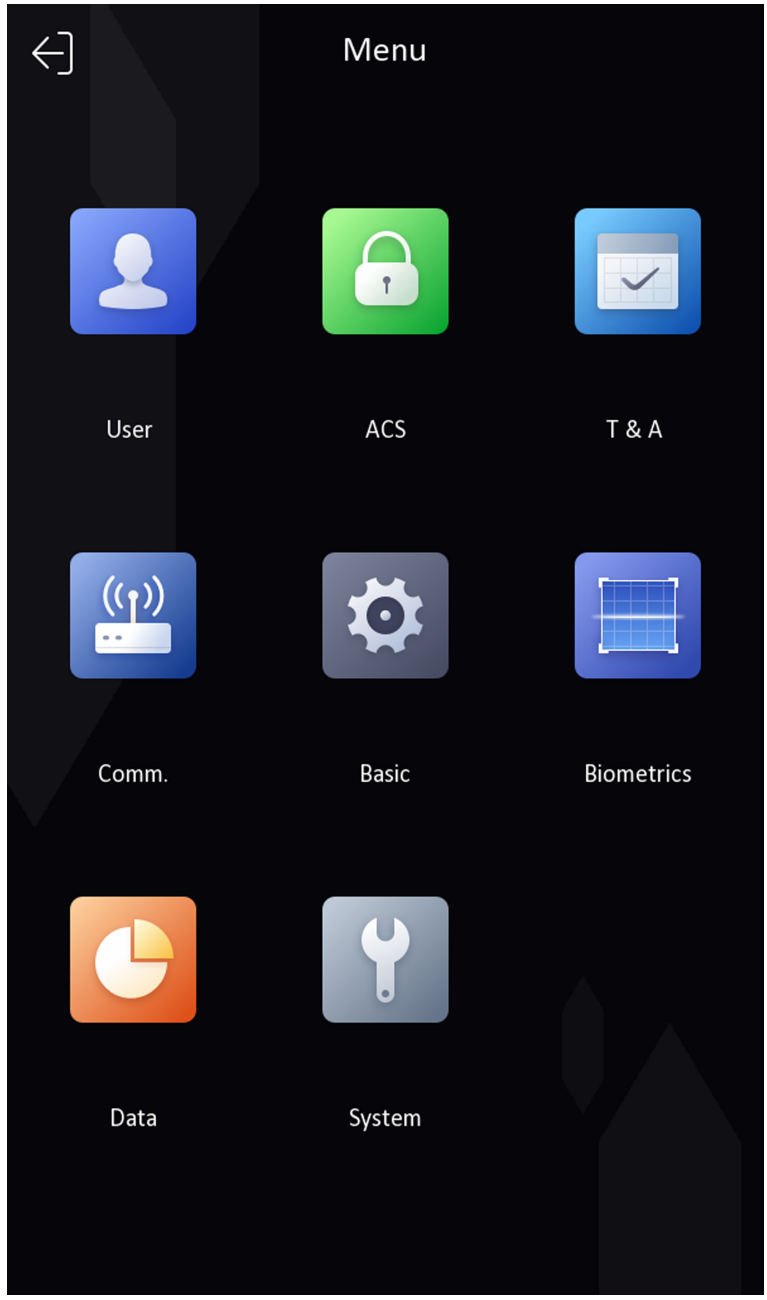


Figure 7-2 Home Page

Note

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

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

7.1.2 Login by Activation Password

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

Steps

1. Long tap on the initial page for 3 s and slide to the left/right by following the gesture to enter password entering page.
2. Tap the Password field and enter the device activation password.
3. Tap **OK** to enter the home page.

Note

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

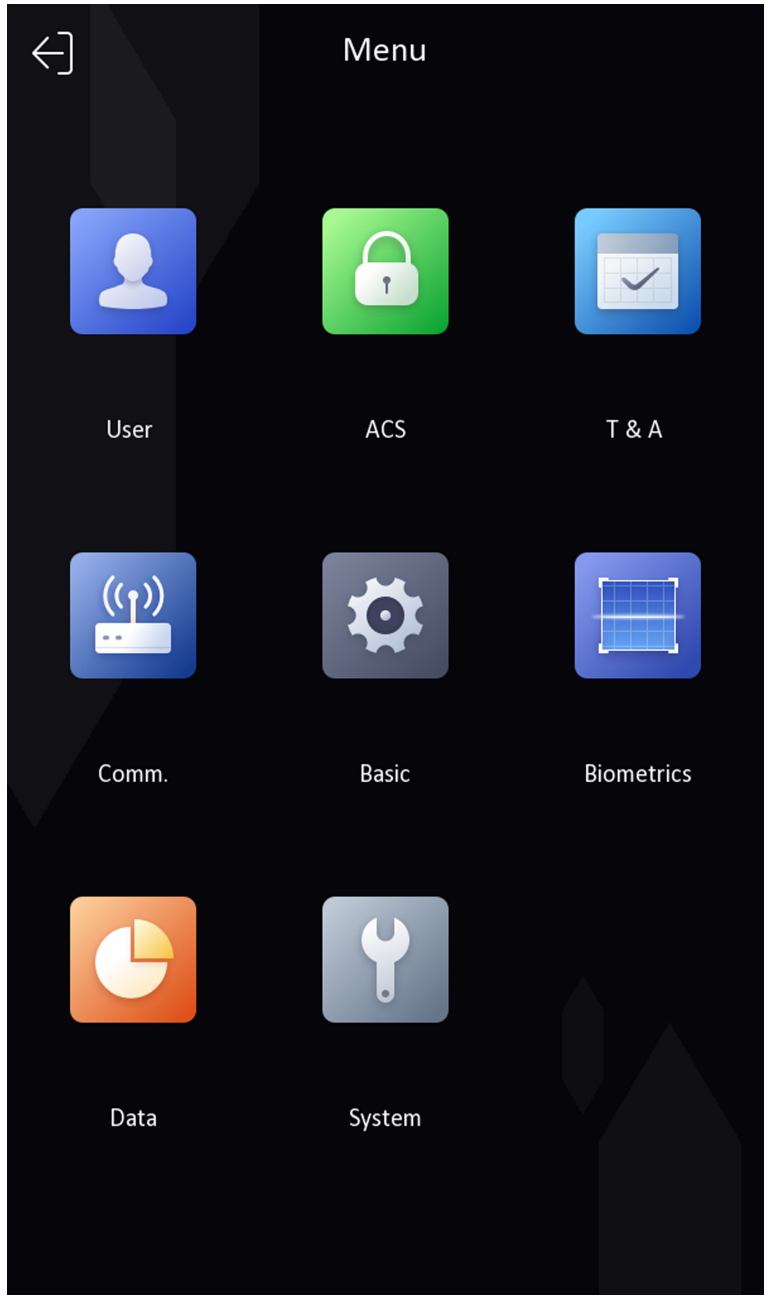


Figure 7-3 Home Page

7.1.3 Forgot Password

If you forget the password during authentication, you can change the password.

Steps

1. Hold the initial page for 3 s and slide to the left/right by following the gesture and log in the page.
2. **Optional:** If you have set an administrator, tap in the pop-up admin authentication page.

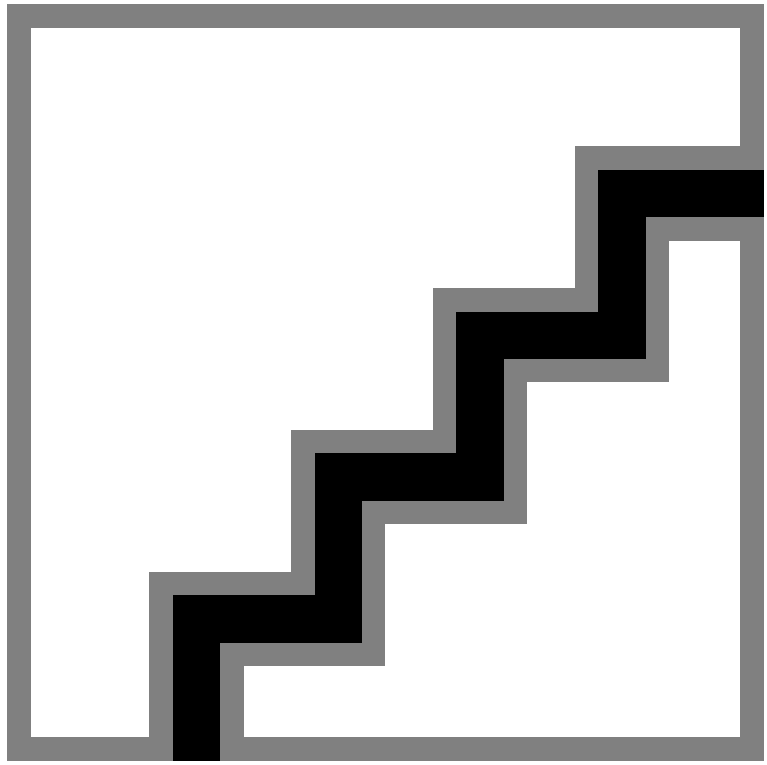


Figure 7-4 Password Authentication Page

3. Tap **Forgot Password**.
4. Select a password change type from the list.

Note

If you have only set 1 password change type, you will go to the corresponded password change page for further settings.

5. Answer the security questions or change the password according to email address.
   - Security Questions: Answer the security questions that configured when activation.
   - Email Address

   Note

   Make sure the device has added to the Hik-Connect account.

   a. Download Hik-Connect app.
   b. Go to **More → Reset Device Password** .
   c. Scan the QR code on the device and a verification code will be popped up.

Note

Tap the QR code to get a larger picture.

d. Enter the verification code on the device page.

6. Create a new password and confirm it.
7. Tap **OK**.

7.2 Communication Settings

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

7.2.1 Set Wired Network Parameters

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

Steps

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

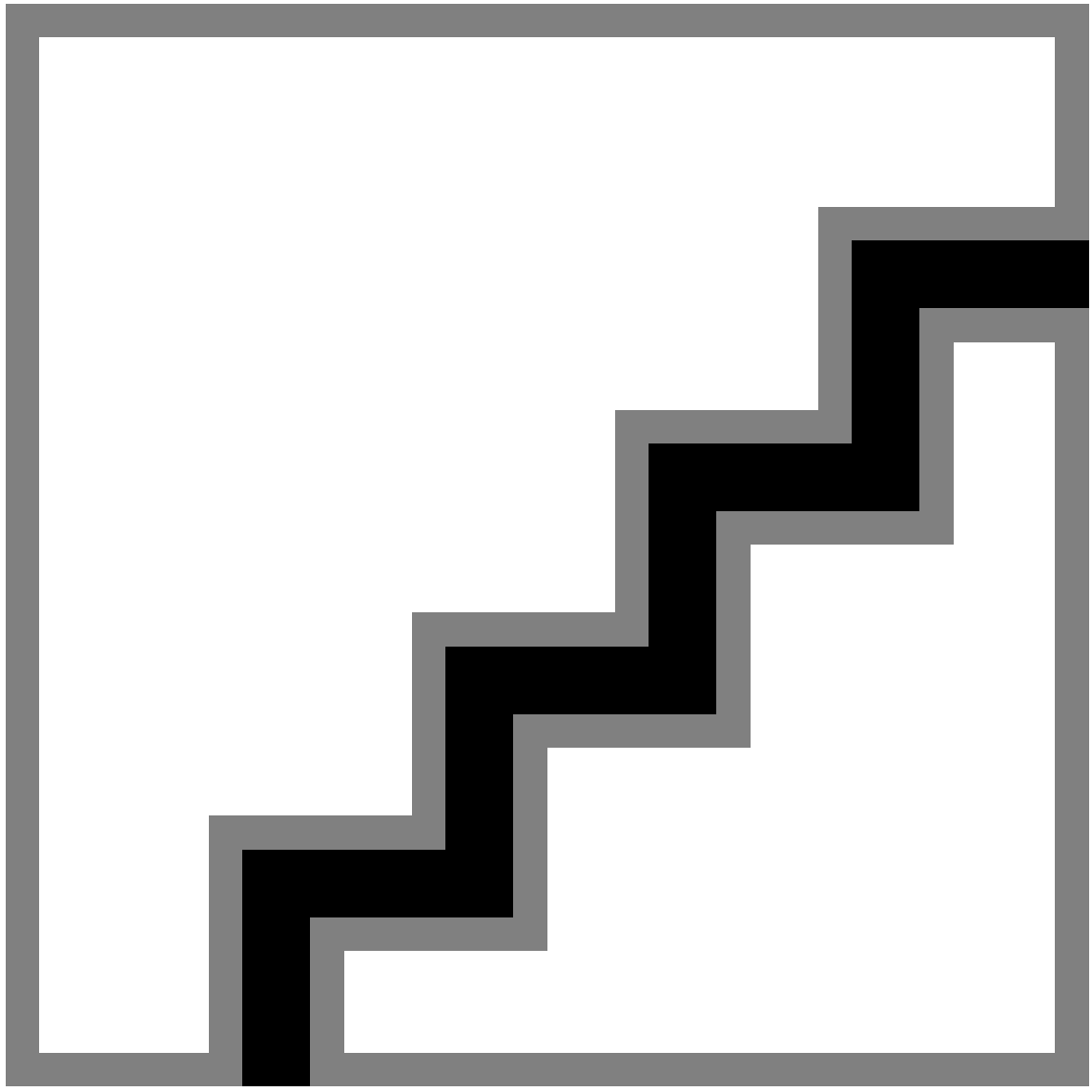


Figure 7-5 Wired Network Settings

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

   Note

   The device's IP address and the computer IP address should be in the same IP segment.
4. Set the DNS parameters. You can enable **Auto Obtain DNS**, set the preferred DNS server and the alternate DNS server.

7.2.2 Set Wi-Fi Parameters

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

Steps

Note

The function should be supported by the device.

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

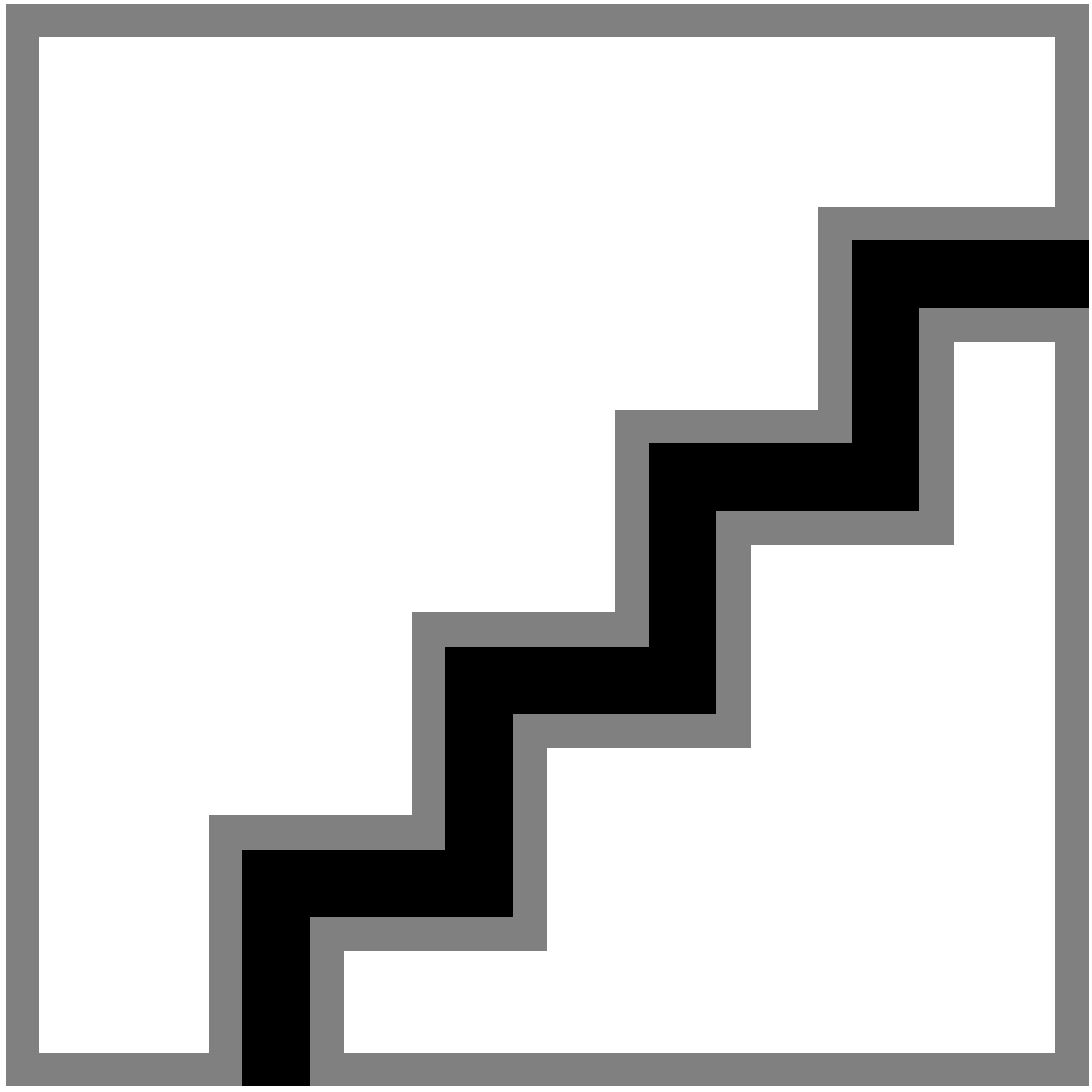


Figure 7-6 Wi-Fi Settings

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

Note

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

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

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

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

7.2.3 Set RS-485 Parameters

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

Steps

1. Tap **Comm.** (Communication Settings) on the Home page to enter the Communication Settings page.
2. On the Communication Settings page, tap **RS-485** to enter the RS-485 tab.

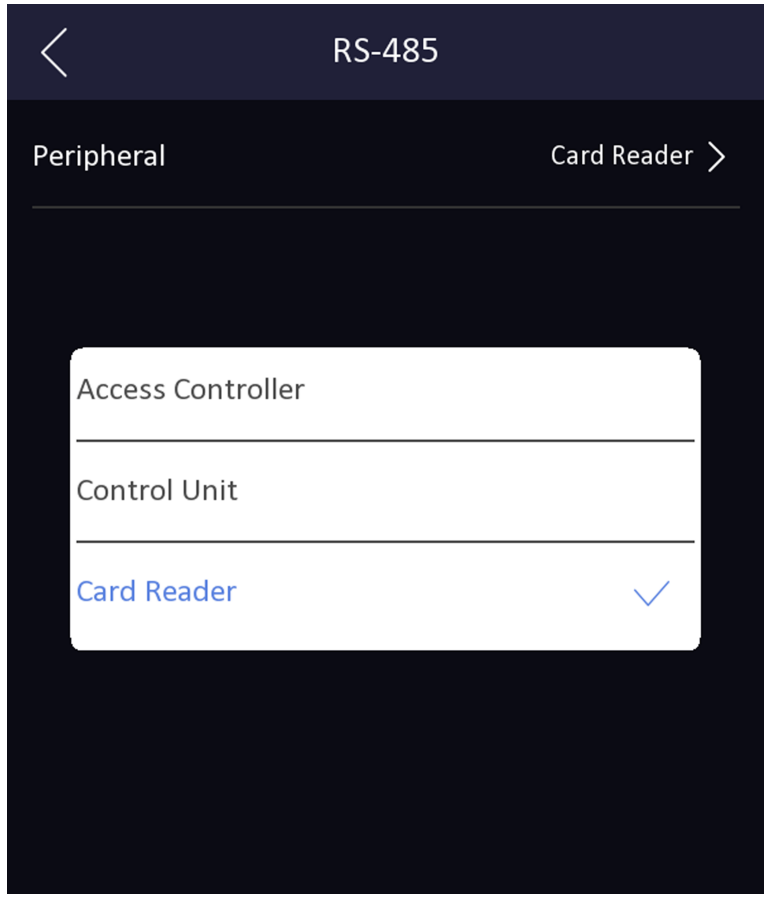


Figure 7-7 Set RS-485 Parameters

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

Note

If you select **Access Controller**: If connect the device to a terminal via the RS-485 interface, set the RS-485 address as 2. If you connect the device to a controller, set the RS-485 address according to the door No.

4. Tap the back icon at the upper left corner and you should reboot the device if you change the parameters.

7.2.4 Set Wiegand Parameters

You can set the Wiegand transmission direction.

Steps

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

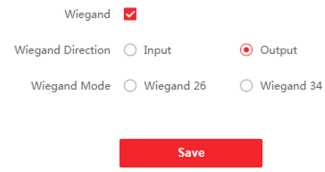


Figure 7-8 Wiegand Settings

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

Note

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

7.2.5 Set EHome Parameters

Set EHome parameters and the device can upload data via EHome protocol.

Before You Start

Make sure your device has connect to a network.

Steps

1. Move the cursor and select **Comm.** → **EHome** .

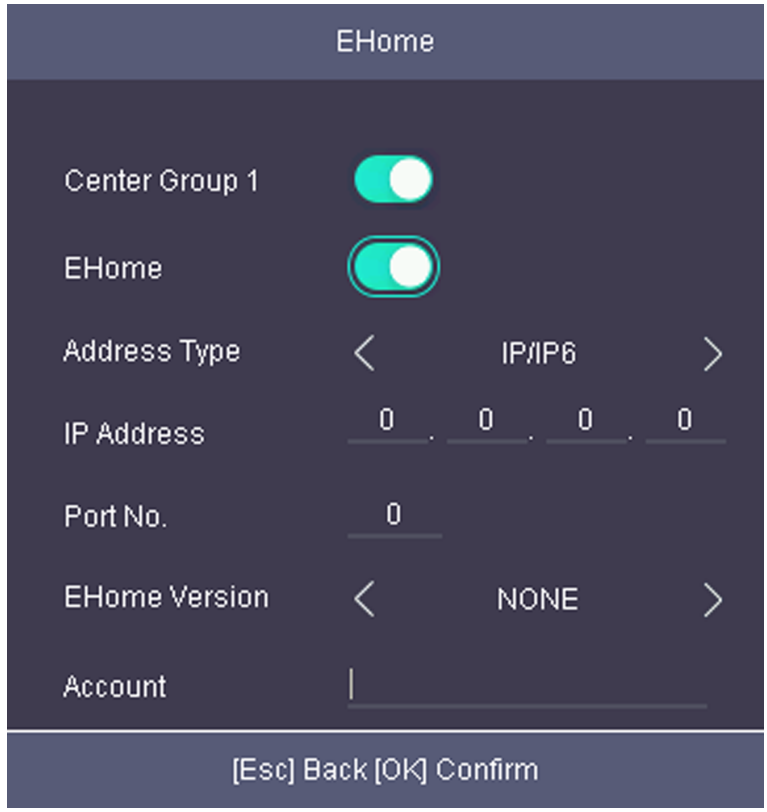


Figure 7-9 EHome Settings

2. Enable the EHome function and set the EHome server parameters.

Center Group 1

Enable center group 1 and the data will be uploaded to the center group.

EHome

Enable EHome function and the data will be uploaded via EHome protocol.

Address Type

Select an address type according to your actual needs.

IP Address

Set the EHome server's IP address.

Port No.

Set the EHome server's port No.

EHome Version

Set the EHome version according to your actual needs. If you choose V5.0, you should create an account and EHome key. If you choose other version, you should create an EHome account only.

Note

- Remember the EHome account and EHome key. You should enter the account name or the key when the device should communicate with other platforms via EHome protocol.
- EHome key range: 8 to 32 characters.

7.2.6 Platform Access

You can change the device verification code and set the server address 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 **Comm.** (Communication Settings) on the Home page to enter the Communication Settings page.
2. On the Communication Settings page, tap **Access to Hik-Connect**.
3. Enable **Access to Hik-Connect**
4. Enter **Server IP**.
5. Create the **Verification Code**, and you need to enter the verification code when you manage the devices via **Hik-Connect**.

7.3 User Management

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

7.3.1 Add Administrator

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

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

Note

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

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

Note

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

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

Note

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

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

Note

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

7. Enable the Administrator Permission function.

Enable Administrator Permission

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

8. Tap ✓ to save the settings.

7.3.2 Add Face Picture

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

Steps

Note

Up to 50,000 face pictures can be added.

1. Long tap on the initial page for 3 s and slide to the left/right by following the gesture and log in the backend.
2. Tap **User → +** to enter the Add User page.
3. Edit the employee ID.

Note

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

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

Note

- Numbers, upper case letters, lower case letters, and special characters are allowed in the user name.
- The suggested user name should be within 32 characters.

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

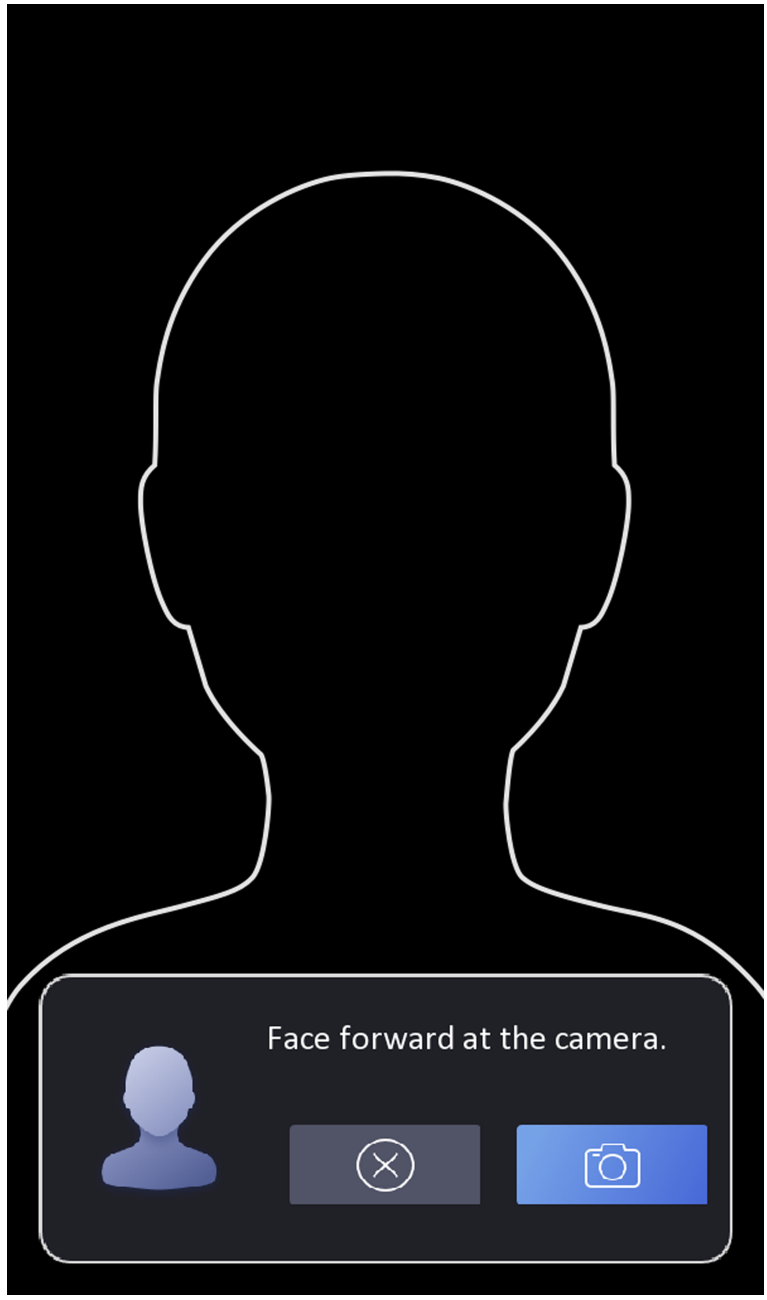


Figure 7-10 Add Face Picture

6. Look at the camera.

Note

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

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

7. Tap **Save** to save the face picture.
8. **Optional:** Tap **Try Again** and adjust your face position to add the face picture again.
9. Set the user role.

Administrator

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

Normal User

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

10. Tap ✓ to save the settings.

7.3.3 Add Card

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

Steps

Note

Up to 50,000 cards can be added.

1. Long tap on the initial page for 3 s and slide to the left/right by following the gesture and log in the backend.
2. Tap **User → +** to enter the Add User page.
3. Connect an external card reader according to the wiring diagram.
4. Tap the Employee ID. field and edit the employee ID.

Note

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

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

Note

- Numbers, upper case letters, lower case letters, and special characters are allowed in the user name.
- The suggested user name should be within 32 characters.

6. Tap the Card field and tap **+**.
7. Configure the card No.
   - Enter the card No. manually.
   - Present the card over the card presenting area to get the card No.

Note

- The card No. cannot be empty.
- Up to 20 characters are allowed in the card No.
- The card No. cannot be duplicated.

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

   Administrator

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

   Normal User

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

7.3.4 View Password

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

Steps

1. Long tap on the initial page for 3 s and slide to the left/right by following the gesture and log in the backend.
2. Tap **User → +** to enter the Add User page.
3. Tap the Employee ID. field and edit the employee ID.

Note

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

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

Note

- Numbers, upper case letters, lower case letters, and special characters are allowed in the user name.
- The suggested user name should be within 32 characters.

5. Tap the Password to view the password.

Note

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

6. Set the user role.

Administrator

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

Normal User

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

7. Tap ✓ to save the settings.

7.3.5 Set Authentication Mode

After adding the user's face picture, password, or other credentials, you should set the authentication mode and the user can authenticate his/her identity via the configured authentication mode.

Steps

1. Long tap on the initial page for 3 s and slide to the left/right by following the gesture and log in the backend.
2. Tap **User → Add User/Edit User → Authentication Mode** .
3. Select Device or Custom as the authentication mode.

Device

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

Custom

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

4. Tap ✓ to save the settings.

7.3.6 Search and Edit User

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

Search User

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

Edit User

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

Note

The employee ID cannot be edited.

7.4 Data Management

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

7.4.1 Delete Data

Delete user data.

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

7.4.2 Import Data

Steps

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

Note

- If you want to transfer all user information from one device (Device A) to another (Device B), you should export the information from Device A to the USB flash drive and then import from the USB flash drive to Device B. In this case, you should import the user data before importing the profile photo.
- The supported USB flash drive format is FAT32.
- The imported pictures should be saved in the folder (named enroll_pic) of the root directory and the picture's name should be follow the rule below:
  Card No._Name_Department_Employee ID_Gender.jpg

- If the folder enroll_pic cannot save all imported pictures, you can create another folders, named enroll_pic1, enroll_pic2, enroll_pic3, enroll_pic4, under the root directory.
- The employee ID should be less than 32 characters. It can be a combination of lower letters, upper letters, and numbers. It should not be duplicated, and should not start with 0.
- Requirements of face picture should follow the rules below: It should be taken in full-face view, directly facing the camera. Do not wear a hat or head covering when taking the face picture. The format should be JPEG or JPG. The resolution should be 640 × 480 pixel or more than of 640 × 480 pixel. The picture size should be between 60 KB and 200 KB.

7.4.3 Export Data

Steps

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

Note

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

7.5 Identity Authentication

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

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

1:N Matching

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

1: 1 Matching

Compare the captured face picture with card linked face pictures.

7.5.1 Authenticate via Single Credential

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

Authenticate face, card or QR code.

Face

Face forward at the camera and start authentication via face.

Card

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

Note

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

QR Code

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

Note

- Authentication via QR code should be supported by the device.
- The dimension of the recognized QR code picture should be larger than 6 cm × 6 cm.

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

7.5.2 Authenticate via Multiple Credential

Before You Start

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

Steps

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

   Note

   - The card can be normal IC card, or encrypted card.
   - If the QR Code Scanning function is enabled, you can put the QR code in front of the device camera to authenticate via QR code.
   - The dimension of the recognized QR code picture should be larger than 6 cm × 6 cm.

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

   Note

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

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

7.6 Basic Settings

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

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

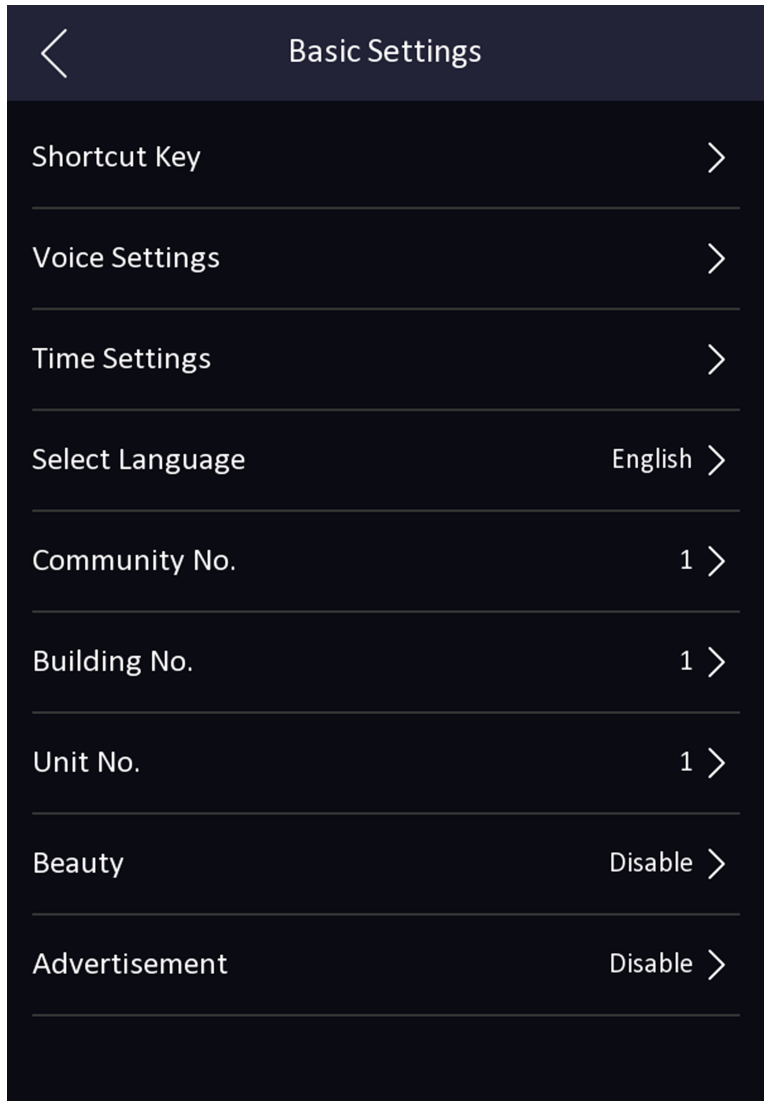


Figure 7-11 Basic Settings Page

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

Shortcut Key

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

Note

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

  Call Room

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

  Call Center

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

  Call Specified Room No.

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

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.

Language

Select the language according to actual needs.

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.

Advertisement

You can enable the advertisement function, and the advertisement will be displayed on the authentication page. The advertisement can be added in web browser. For details, see ***Set Notice Publication*** .

7.7 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, hard hat detection level, and face with mask detection.

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

Table 7-1 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.

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

7.8 Set Access Control Parameters

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

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

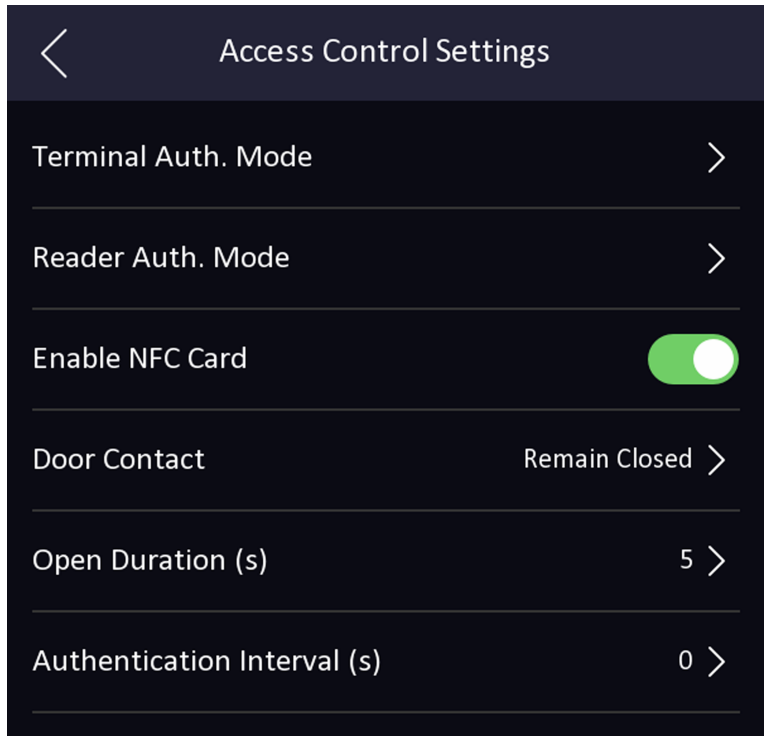


Figure 7-13 Access Control Parameters

The available parameters descriptions are as follows:

Table 7-2 Access Control Parameters Descriptions

Parameter	Description
Terminal Auth. Mode (Terminal Authentication Mode)	Select the face recognition terminal's authentication mode. You can also customize the authentication mode. **Note** • Biometric recognition products are not completely applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes. • If you adopt multiple authentication modes, you should authenticate other methods before authenticating face.
Reader Auth. Mode (Card Reader Authentication Mode)	Select the card reader's authentication mode.
Enable NFC Card	Enable the function and you can present the NFC card to authenticate.

Parameter	Description
Door Contact	You can select "Remain Open" or "Remian Closed" according to your actual needs. By default, it is Remian Closed.
Open Duration	Set the door unlocking duration. If the door is not opened for the set time, the door will be locked. Available door locked time range: 1 to 255s.
Authentication Interval	Set the device authenticating interval. Available authentication interval range: 0 to 65535.

7.9 Time and Attendance Status Settings

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

Note

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

7.9.1 Disable Attendance Mode via Device

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

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

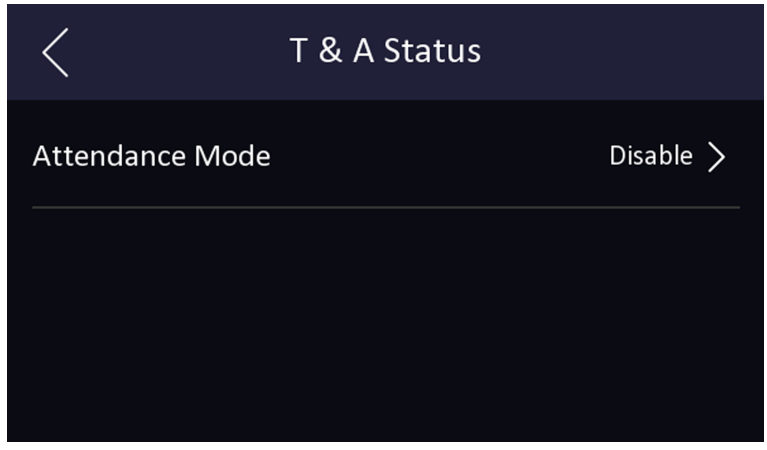


Figure 7-14 Disable Attendance Mode

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

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

7.9.2 Set Manual Attendance via Device

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

Before You Start

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

Steps

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

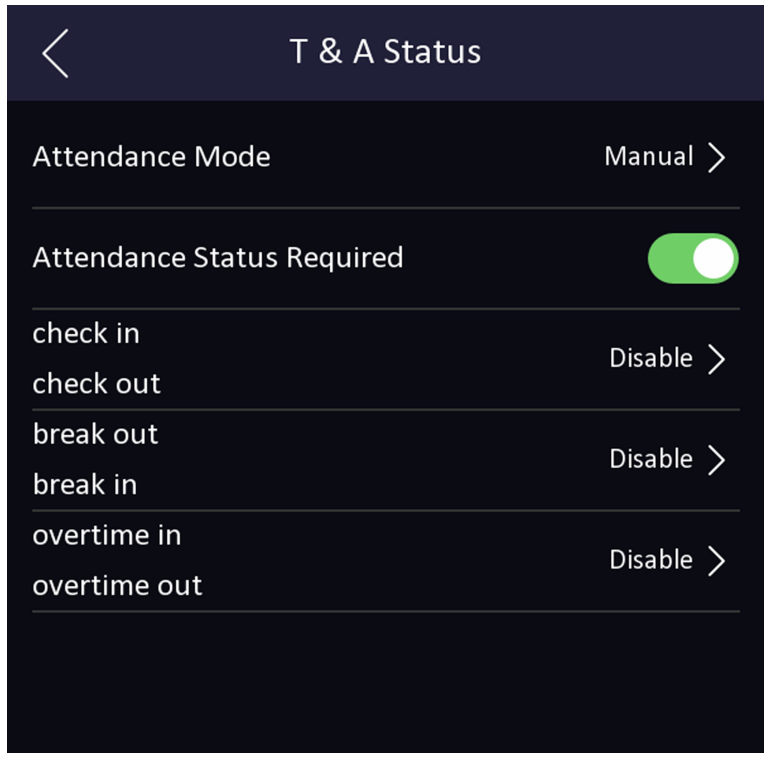


Figure 7-15 Manual Attendance Mode

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

Note

The Attendance Property will not be changed.

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

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

Result

You should select an attendance status manually after authentication.

Note

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

7.9.3 Set Auto Attendance via Device

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

Before You Start

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

Steps

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

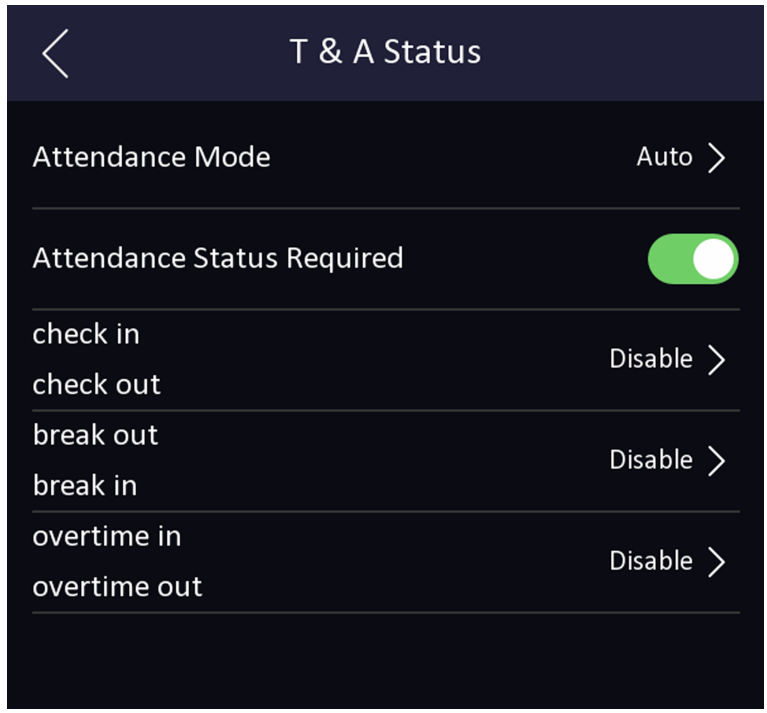


Figure 7-16 Auto Attendance Mode

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

Note

The Attendance Property will not be changed.

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

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

6. Set the status' schedule.

   1) Tap **Attendance Schedule**.

   2) Select **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday**, or **Sunday**.

   3) Set the selected attendance status's start time of the day.

   4) Tap **Confirm**.

   5) Repeat step 1 to 4 according to your actual needs.

Note

The attendance status will be valid within the configured schedule.

Result

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

Example

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

7.9.4 Set Manual and Auto Attendance via Device

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

Before You Start

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

Steps

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

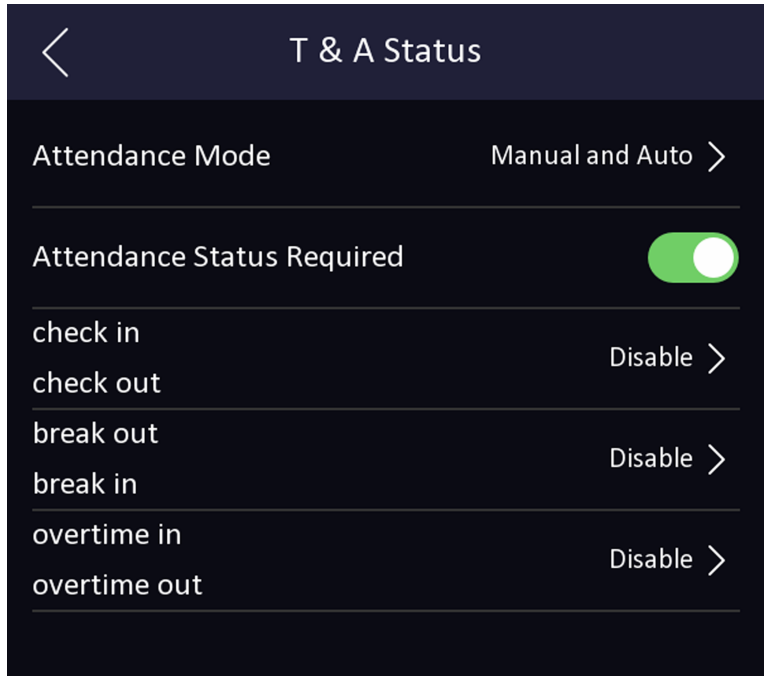


Figure 7-17 Manual and Auto Mode

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

Note

The Attendance Property will not be changed.

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

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

Note

The attendance status will be valid within the configured schedule.

Result

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

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

7.10 System Maintenance

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

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

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

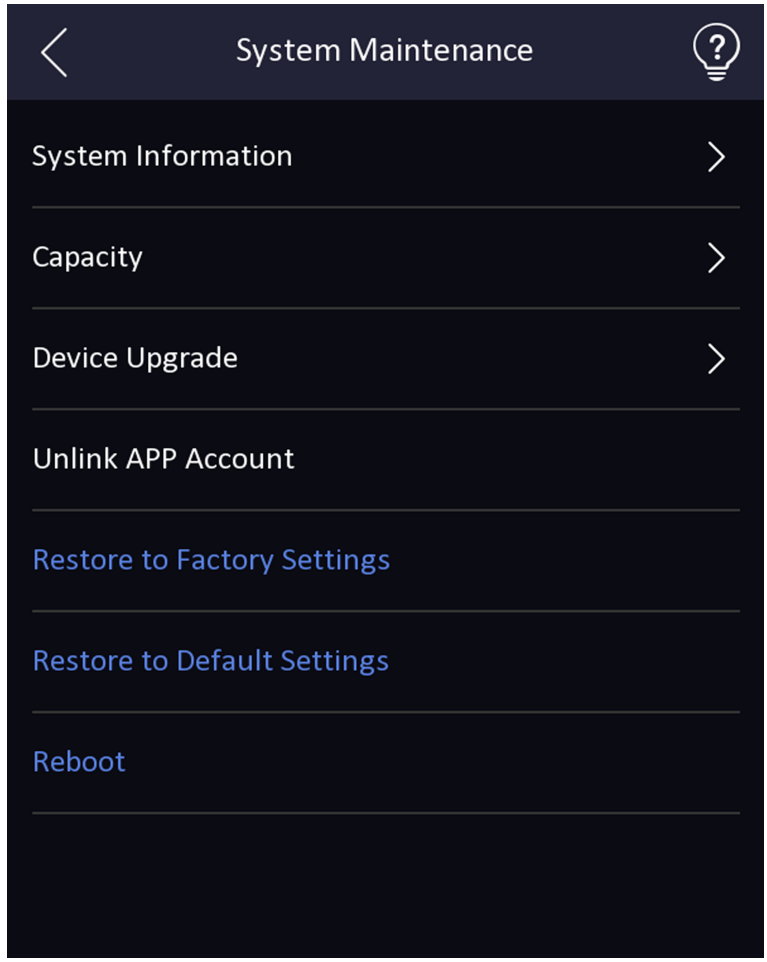


Figure 7-18 Maintenance Page

System Information

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

Note

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

Capacity

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

Device Upgrade

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

Unlink APP Account

After unlinking APP account, you cannot operate via APP.

Restore to Default Settings

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

Restore to Factory Settings

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

Reboot

Reboot the device.

7.11 Preference Settings

You can configure preference settings parameters.

Steps

1. Tap **Basic Settings → Preference Settings** to enter the preference settings page.

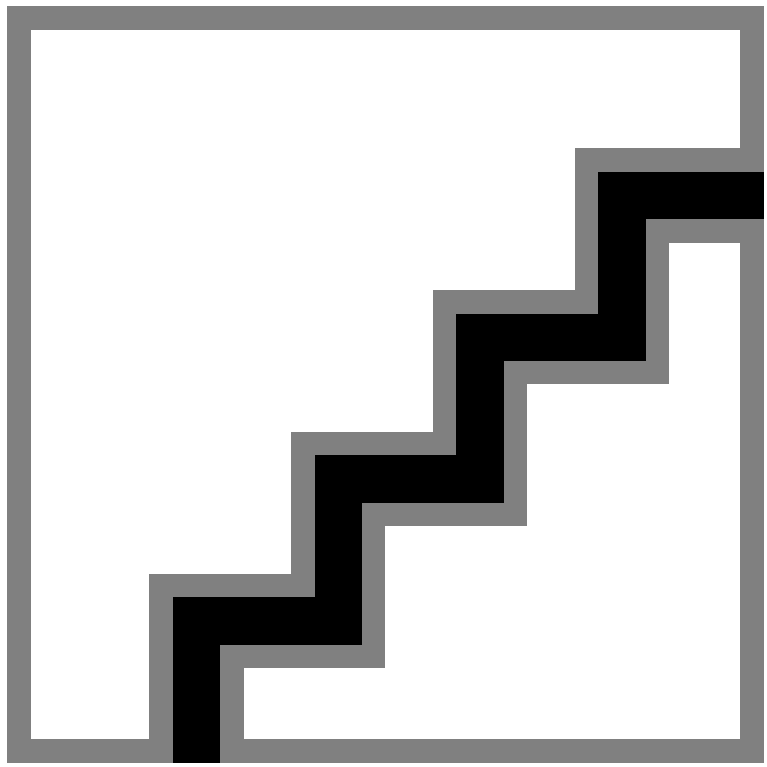


Figure 7-19 Preference Settings

Theme

You can set the theme of the prompt window on the authentication page. You can select **Theme** as **Iris Recognition Mode**/**Advertisement**/**Meeting**/**Simple**.

Advertisement

After selecting this mode, the advertising area and identification authentication area of the device will be displayed on separate screens. Video and advertising information playback, welcome speech display are supported.

Meeting

After selecting this mode, the device supports editing and displaying meeting room name, displaying scheduled meeting information and the status of the meeting room, and signing in on the device.

Simple

After selecting this mode, the live view of the authentication page will be disabled, and in the meanwhile, the person's name, employee ID, face pictures will all be hidden.

Shortcut Key

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

Note

You can select call type from **Call Room**, **Call Center**, **Call Specified Room No.** and **Call APP**.

Call Room

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

Call Center

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

Call Specified Room No.

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

Call APP

When you tap the call button on the authentication page, you will call the mobile client where the device is added.

Password

Enable this function amd you can enter the password to authenticate via password.

QR Code

You can use the QR code scanning function on the authentication interface. The device will upload the information associated with the obtained QR code to the platform.

7.12 Video Intercom

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

7.12.1 Call Client Software from Device

Steps

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

Note

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

5. Call the client software.
   1) Tap on the device initial page.

2) Enter ***0*** in the pop-up window.
3) Tap to call the client software.

6. Tap **Answer** on the pop-up page of the client software and you can start two-way audio between the device and the client software.

Note

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

7.12.2 Call Center from Device

Steps

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

Note

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

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

Note

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

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

Note

The device will call the main station in priority.

7.12.3 Call Device from Client Software

Steps

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

Note

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

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

Note

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

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

7.12.4 Call Room from Device

Steps

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

Note

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

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

7.12.5 Call Mobile Client from Device

Steps

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

Note

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

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

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

Chapter 8 Operation via Web Browser

8.1 Login

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

Note

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

Login via Web Browser

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

Note

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

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

Login via Remote Configuration of Client Software

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

8.2 Live View

You can view the live video of the device.

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

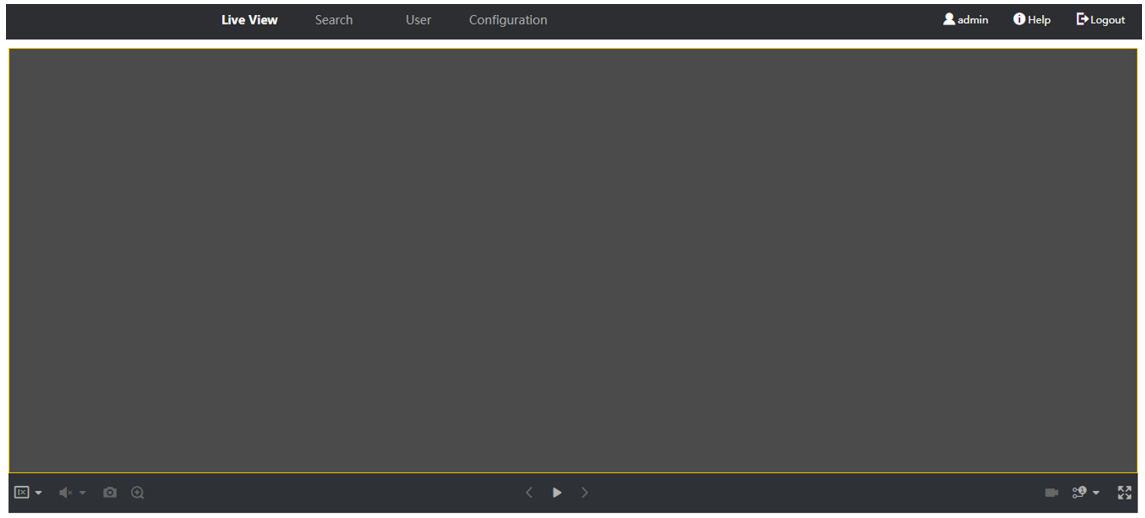


Figure 8-1 Live View Page

Function Descriptions:

Select the image size when starting live view.

Set the volume when starting live view.

Note

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

You can capture image when starting live view.

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

Start or stop live view.

Start or stop video recording.

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

Full screen view.

8.3 Person Management

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

Click **OK** to save the person.

Add Basic Information

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

Add Card

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

Add Face Picture

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

Note

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

Click **OK** to save the settings.

Set Permission Time

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

Set Access Control

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

Add Authentication Mode

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

8.4 Search Event

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

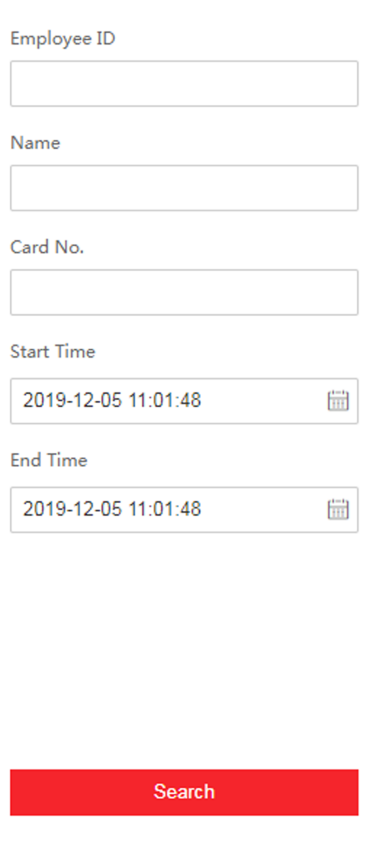


Figure 8-2 Search Page

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

The results will be displayed on the right panel.

8.5 Configuration

8.5.1 Set Local Parameters

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

Set Live View Parameters

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

Set Record File Saving Path

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

Set Captured Pictures Saving Path

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

8.5.2 View Device Information

View the device name, language, model, serial No., QR code, version, 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, device capacity, etc.

8.5.3 Set Time

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

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

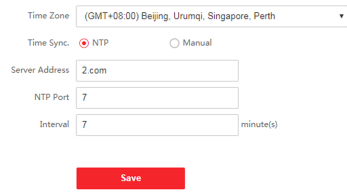


Figure 8-3 Time Settings

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

Time Zone

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

Time Sync.

NTP

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

Manual

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

8.5.4 Set DST

Steps

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

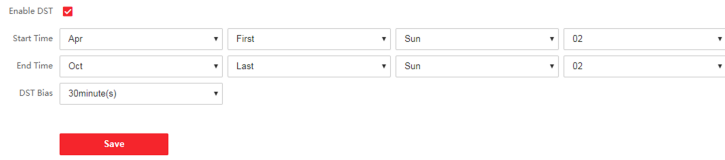


Figure 8-4 DST Page

2. Check **Enable DST**.
3. Set the DST start time, end time and bias time.
4. Click **Save** to save the settings.

8.5.5 View Open Source Software License

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

8.5.6 Upgrade and Maintenance

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

Reboot Device

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

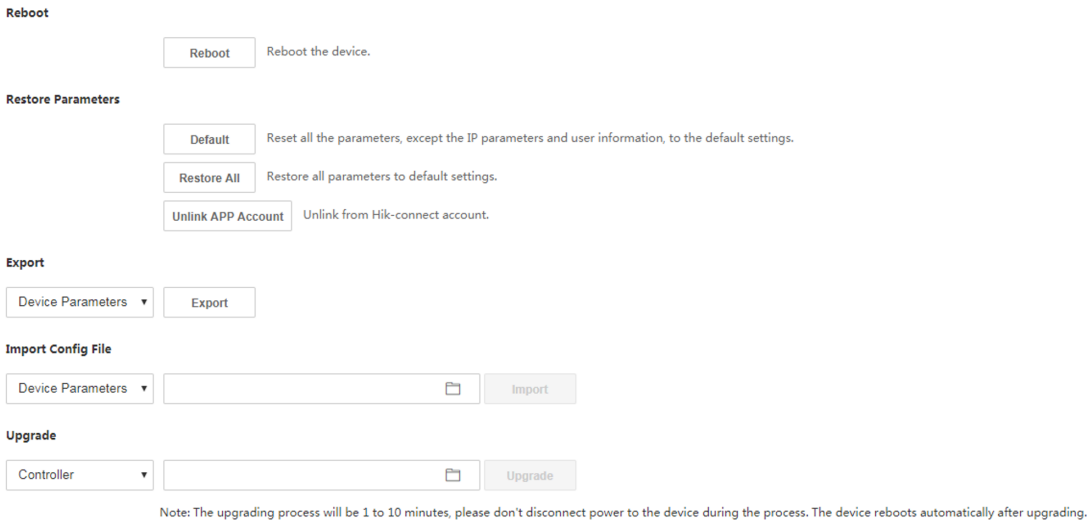


Figure 8-5 Upgrade and Maintenance Page

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

Restore Parameters

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

Restore All

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

Default

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

Unlink APP Account

Unlink the Hik-Connect account from the platform.

Import and Export Parameters

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

Export

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

Note

You can import the exported device parameters to another device.

Import

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

Upgrade

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

Note

Do not power off during the upgrading.

8.5.7 Log Query

You can search and view the device logs.

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

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

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

8.5.8 Security Mode Settings

Set the security mode for logging in the client software.

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

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

Security Mode

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

Compatible Mode

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

Enable SSH

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

Enable HTTP

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

8.5.9 Certificate Management

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

Note

The function is only supported by certain device models.

Create and Install Self-signed Certificate

Steps

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

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

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

Install Other Authorized Certificate

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

Steps

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

Install CA Certificate

Before You Start

Prepare a CA certificate in advance.

Steps

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

   Note

   The input certificate ID cannot be the same as the existing ones.
3. Upload a certificate file from the local.
4. Click **Install**.

8.5.10 Change Administrator's Password

Steps

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

   Caution

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

8.5.11 View Device Arming/Disarming Information

View device arming type and arming IP address.

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

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

8.5.12 Network Settings

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

Note

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

Set Basic Network Parameters

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

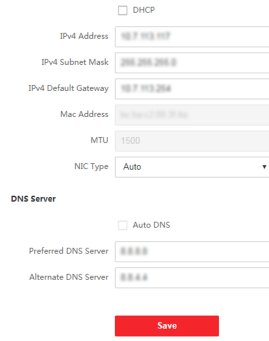


Figure 8-6 TCP/IP Settings Page

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

DHCP

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

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

NIC Type

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

DNS Server

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

Set Port Parameters

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

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

HTTP

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

RTSP

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

HTTPS

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

Server

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

Set Wi-Fi Parameters

Set the Wi-Fi parameters for device wireless connection.

Steps

Note

The function should be supported by the device.

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

Figure 8-7 Wi-Fi Settings Page

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

Report Strategy Settings

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

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

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

Center Group

Select a center group from the drop-down list.

Main Channel

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

Note

N1 refers to wired network.

Platform Access

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

Steps

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

Note

Hik-Connect is an application for mobile devices. With the App, you can view live image of the device, receive alarm notification and so on.

4. Create a **Stream Encryption/Encryption Key** for the device.

Note

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

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

Set ISUP Parameters

Set the ISUP parameters for accessing device via ISUP protocol.

Steps

Note

The function should be supported by the device.

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

   Note

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

Configure HTTP Listening

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

Before You Start

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

Note

The function should be supported by the device.

Steps

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

8.5.13 Set Video and Audio Parameters

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

Set Video Parameters

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

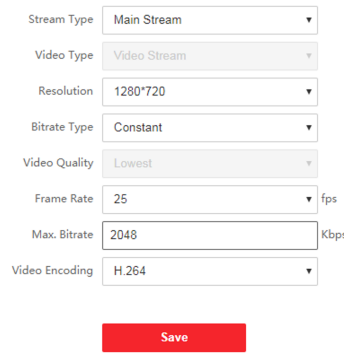


Figure 8-8 Video Settings Page

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

Set Audio Parameters

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

Note

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

8.5.14 Customize Audio Content

Customize the output audio content when authentication succeeded and failed.

Steps

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

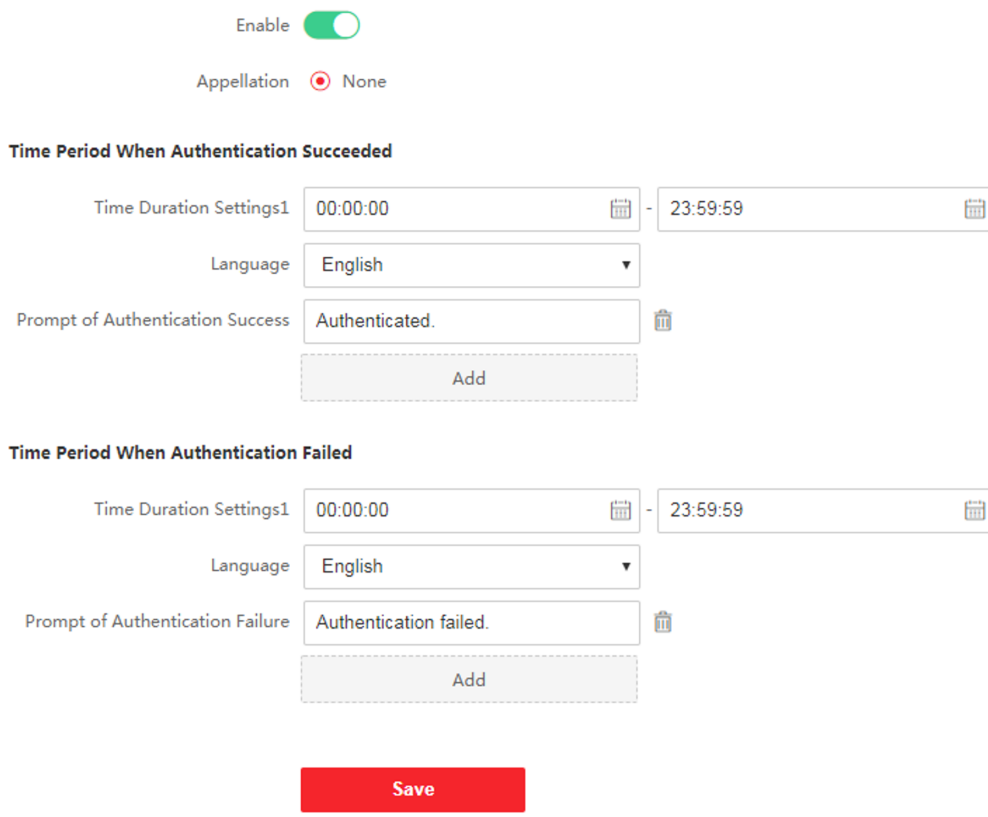


Figure 8-9 Customize Audio Content

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

   Note

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

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

   Note

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

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

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

8.5.15 Set Image Parameters

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

Steps

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

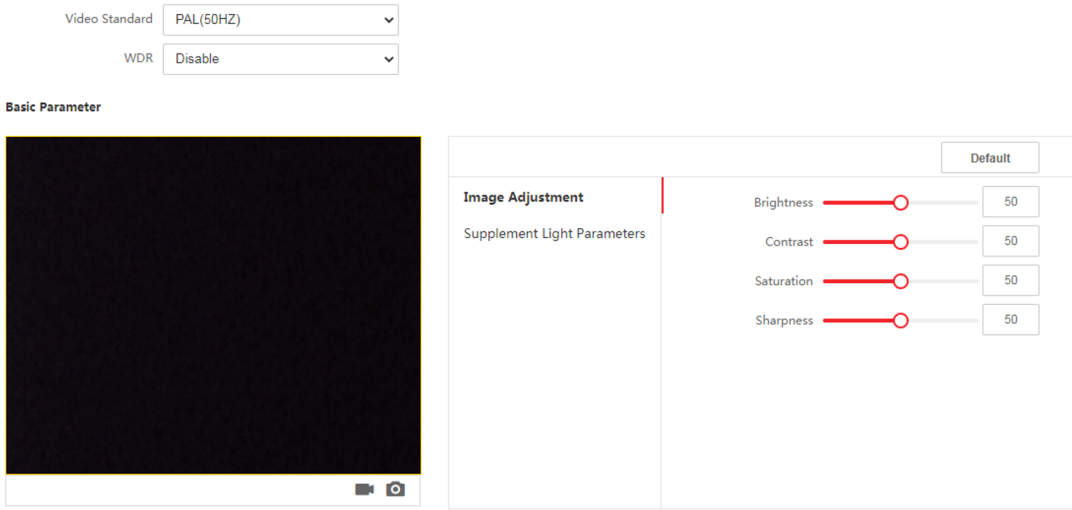


Figure 8-10 Image Settings Page

2. Configure the parameters to adjust the image.

Video Standard

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

PAL

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

NTSC

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

WDR

Enable or disable the WDR function.

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

Brightness/Contrast/Saturation/Sharpness

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

Start/end recording video.

Capture the image.

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

8.5.16 Set Supplement Light Brightness

Set the device supplement light brightness.

Steps

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

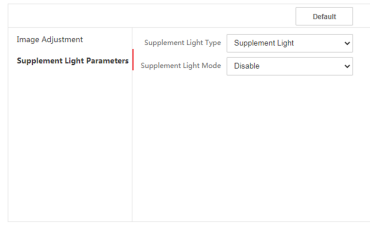


Figure 8-11 Supplement Light Settings Page

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

8.5.17 Time and Attendance Settings

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

Disable Attendance Mode via Web

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

Steps

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

Result

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

Time Settings

Steps

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

   Note

   Set the schedule from Monday to Sunday according to the actual needs.
5. **Optional:** Select a timeline and click **Delete**. Or click **Delete All** to clear the settings.
6. Click **Save**.

Set Manual Attendance via Web

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

Before You Start

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

Steps

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

   Note

   The Attendance Property will not be changed.
5. **Optional:** Select an status and change its name if required.

Result

You should select an attendance status manually after authentication.

Note

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

Set Auto Attendance via Web

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

Before You Start

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

Steps

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

   Note

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

Set Manual and Auto Attendance via Web

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

Before You Start

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

Steps

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

   Note

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

Result

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

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

8.5.18 Set Video Intercom Parameters

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

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

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

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

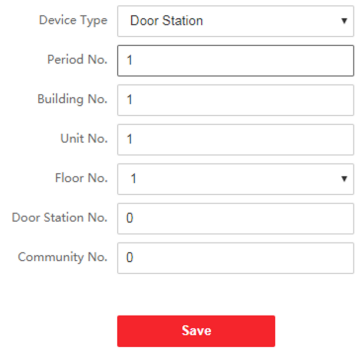


Figure 8-12 Device No. Settings

Device Type

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

Note

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

Period No.

Set the device installed period No.

Building No.

Set the device installed building No.

Unit No.

Set the device installed unit No.

Floor No.

Set the device installed floor No.

Door Station No.

Set the device installed floor No.

Note

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

Community No.

Set the device installed community No.

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

Period No.

Set the device installed period No.

Outer Door Station No.

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

Note

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

Community No.

Set the device installed community No.

8.5.19 Access Control Settings

Set Authentication Parameters

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

Note

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

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

Device Type

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

Main Card Reader

You can configure the device card reader's parameters.

Sub Card Reader

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

If select **Main Card Reader**:

Card Reader Type/Card Reader Description

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

Enable Card Reader

Enable the card reader's function.

Authentication

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

Display Authentication Result

Check **Face Picture**, **Name**, or **Employee ID**. When authentication is completed, the system will display the selected contents in the result.

Recognition Interval

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

Authentication Interval

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

Alarm of Max. Failed Attempts

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

Enable Tampering Detection

Enable the anti-tamper detection for the card reader.

Enable Card No. Reversing

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

If select **Sub Card Reader**:

Card Reader Type/Card Reader Description

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

Enable Card Reader

Enable the card reader's function.

Authentication

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

Recognition Interval

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

Authentication Interval

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

Alarm of Max. Failed Attempts

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

Communication with Controller Every

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

Max. Interval When Entering Password

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

OK LED Polarity/Error LED Polarity

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

Enable Tampering Detection

Enable the anti-tamper detection for the card reader.

Set Door Parameters

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

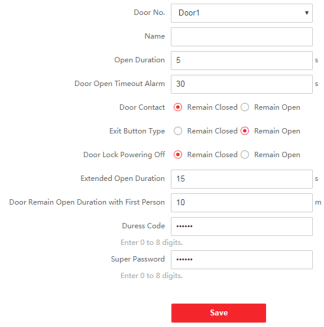


Figure 8-13 Door Parameters Settings Page

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

Door No.

Select the device corresponded door No.

Name

You can create a name for the door.

Open Duration

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

Door Open Timeout Alarm

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

Door Contact

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

Exit Button Type

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

Door Lock Powering Off Status

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

Extended Open Duration

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

Door Remain Open Duration with First Person

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

Duress Code

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

Super Password

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

Note

The duress code and the super code should be different.

Set Card Security

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

Set the parameters and click **Save**.

Enable NFC Card

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

Enable M1 Card

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

M1 Card Encryption

Sector

M1 card encryption can improve the security level of authentication.

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

Enable EM Card

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

Note

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

Configure SIP Parameters

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

Note

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

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

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

Click **Save**.

Set RS-485 Parameters

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

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

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

No.

Set the RS-485 No.

Peripheral Type

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

Note

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

RS-485 Address

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

Note

If you select **Access Controller**: If connect the device to a terminal via the RS-485 interface, set the RS-485 address as 2. If you connect the device to a controller, set the RS-485 address according to the door No.

Baud Rate

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

Set Wiegand Parameters

You can set the Wiegand transmission direction.

Steps

Note

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

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

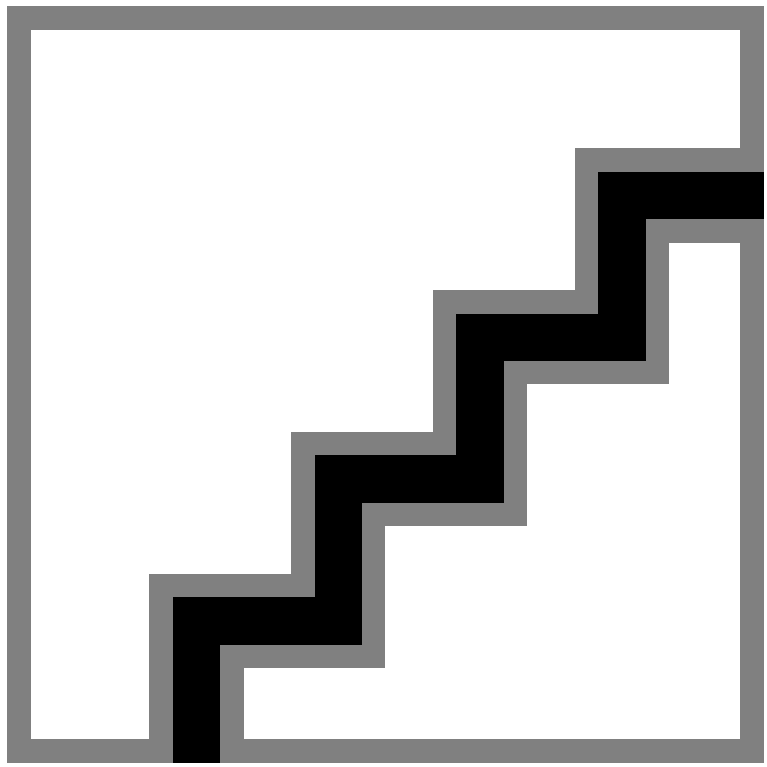


Figure 8-14 Wiegand Page

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

   Input

   The device can connect a Wiegand card reader.

   Output

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

Note

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

Set Privacy Parameters

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

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

Event Storage Settings

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

Delete Old Events Periodically

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

Delete Old Events by Specified Time

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

Overwriting

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

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 Card Authentication Parameters

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

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

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

Full Card No.

All card No. will be read.

Wiegand 26 (3 bytes)

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

Wiegand 34 (4 bytes)

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

8.5.20 Set Biometric Parameters

Set Basic Parameters

Click **Configuration → Smart → Smart** .

Figure 8-15 Smart Settings Page

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

Face Anti-spoofing

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

Note

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

Live Face Detection Security Level

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

Recognition Distance

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

Application Mode

Select either others or indoor according to actual environment.

Face Recognition Mode

Normal Mode

Recognize face via the camera normally.

Deep Mode

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

Continuous Face Recognition Interval

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

Pitch Angle

The maximum pitch angle when starting face authentication.

Yaw Angle

The maximum yaw angle when starting face authentication.

Face Grading

Set the face grading according to your needs.

1:1 Matching Threshold

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

1:N Matching Threshold

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

Face Recognition Timeout Value

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

ECO Mode

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

ECO Mode (1:1)

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

ECO Mode (1:N)

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

Enable Hard Hat Detection

After enabling the hard hat detection, you can set the reminder strategy.

None

The function is disabled. The device will not detect whether a person is wearing a hard hat or not.

Reminder of Wearing Hard Hat

If the person do not wear the hard hat when authenticating, the device will pop up a prompt and the door will open.

Must Wear Hard Hat

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

Face with Mask Detection

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

None

The device will detect the face with mask without prompt.

Prompt and Open

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

Prompt and Not Open Door

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

Set Recognition Area

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

Click or to record videos or capture pictures.

8.5.21 Set Notice Publication

You can set the screen saver and the sleep time for the device.

Click **Configuration → Notice Publication** .

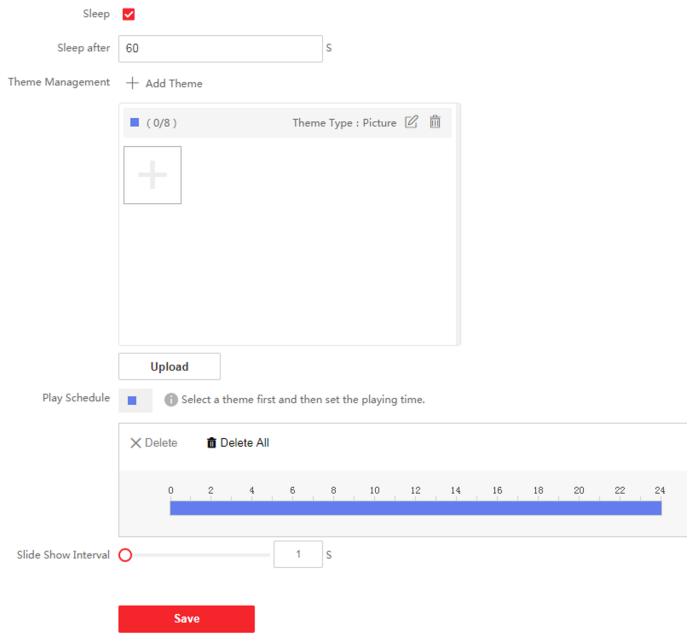


Figure 8-16 Notice Page

Sleep

Enable **Sleep** and the device will enter the sleep mode when no operation within the configured sleep time.

Theme Management

You can click **+** in the frame and upload the screen saver pictures from the local PC.

Note

By now, there is only one theme can be added.

Play Schedule

After you have created a theme, you can select the theme and draw a schedule on the time line.

Select the drawn schedule and you can edit the exact start and end time.

Select the drawn schedule and you can click **Delete** or **Delete All** to delete the schedule.

Slide Show Interval

Drag the block or enter the number to set the slide show interval. The picture will be changed according to the interval.

Chapter 9 Client Software Configuration

9.1 Configuration Flow of Client Software

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

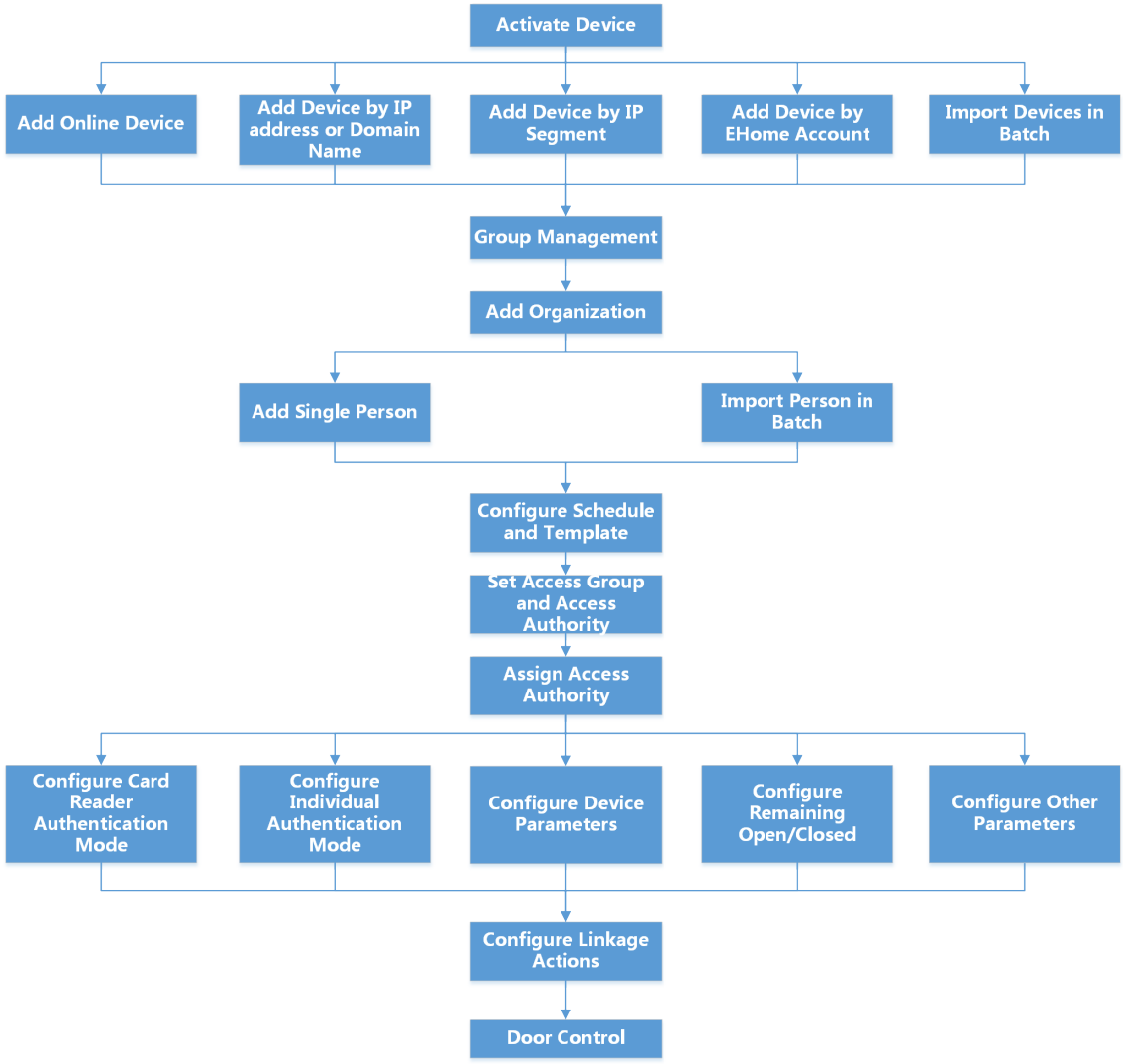


Figure 9-1 Flow Diagram of Configuration on Client Software

9.2 Device Management

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

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

9.2.1 Add Device

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

Add Online Device

The active online devices in the same local subnet with the client software will be displayed on the **Online Device** area. You can click **Refresh Every 60s** to refresh the information of the online devices.

Add Single or Multiple Online Devices

The client can detect online devices which are in the same network as the PC running the client. You can select a detected online device displayed in the online device list and add it to the client. For detected online devices sharing the same user name and password, you can add them to the client in a batch.

Before You Start
- The device(s) to be added are in the same network as the PC running the client.
- The device(s) to be added have been activated.

Steps
1. Click **Device Management → Device** 。
2. Click **Online Device** to show the online device area.
   The searched online devices are displayed in the list.

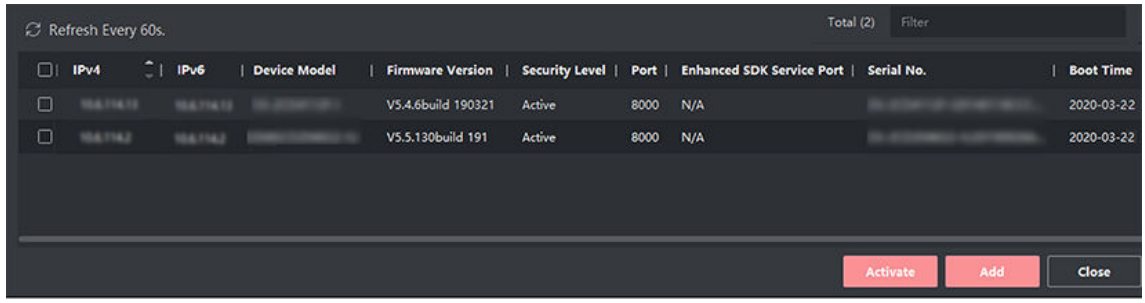


Figure 9-2 Online Device

3. In the **Online Device** area, check one or more online device(s), and click **Add** to open the device adding window.

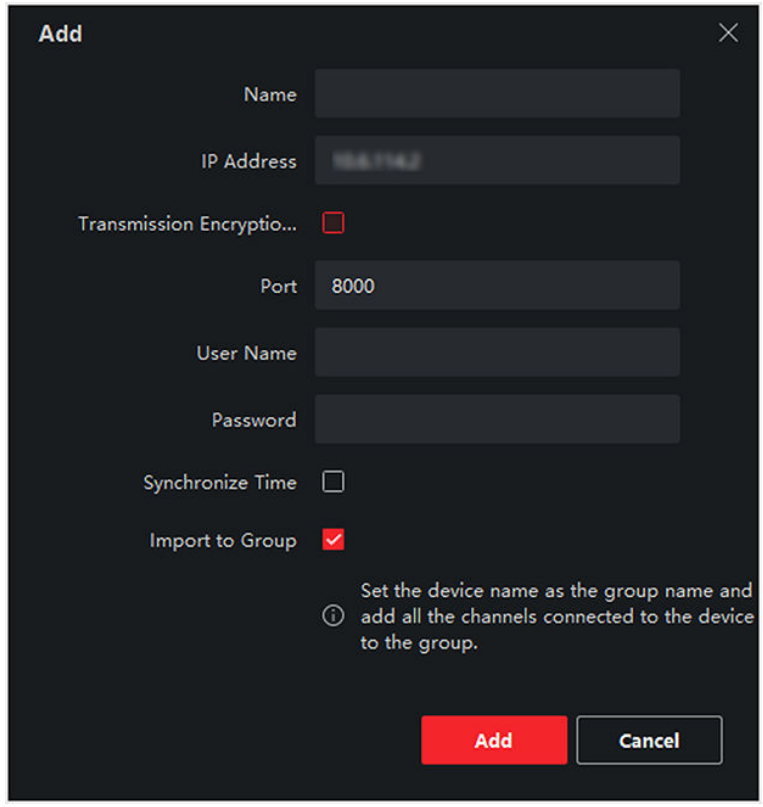


Figure 9-3 Add Single Online Device

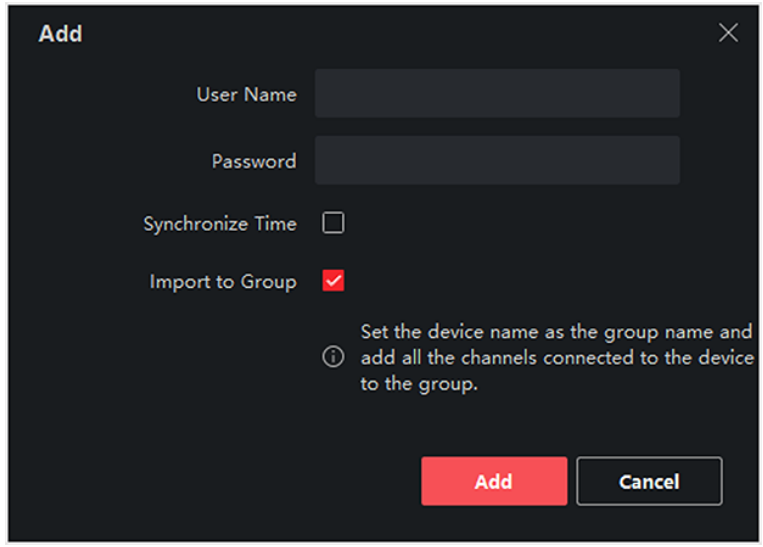


Figure 9-4 Add Multiple Online Devices

4. Enter the required information.

Name

Enter a descriptive name for the device.

IP Address

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

Port

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

User Name

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

Password

Enter the device password.

Caution

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

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

Note

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

6. Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.
7. **Optional:** Check **Import to Group** to create a group by the device name, and import all the channels of the device to this group.

Example

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

8. Click **Add**.

Add Multiple Detected Online Devices

For detected online devices sharing the same user name and password, you can add them to the client in a batch.

Before You Start
Make sure the to-be-added devices are online.

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

   The searched online devices are displayed in the list.
4. Select multiple devices.

   Note

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

   User Name

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

   Password

   Enter the device password.

   Caution

   The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.
   Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.
7. **Optional:** Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.
8. **Optional:** Check **Import to Group** to create a group by the device name, and import all the channels of the device to this group.

   Example

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

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

Add Device by IP Address or Domain Name

If you know the IP address or domain name of the device to add, you can add devices to the client by specifying the IP address (or domain name), user name, password, etc.

Steps

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

   The added devices are displayed on the right panel.
3. Click **Add** to open the Add window, and then select **IP/Domain** as the adding mode.
4. Enter the required information.

   Name

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

   Address

   The IP address or domain name of the device.

   Port

   The devices to add share the same port number. The default value is ***8000***.

   User Name

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

   Password

   Enter the device password.

   Caution

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

Note

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

6. Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.
7. **Optional:** Check **Import to Group** to create a group by the device name, and import all the channels of the device to this group.

   Example

   For access control device, its access points, alarm inputs/outputs, and encoding channels (if exist) will be imported to this group.
8. Finish adding the device.
   - Click **Add** to add the device and back to the device list page.
   - Click **Add and New** to save the settings and continue to add other device.

Add Devices by IP Segment

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

Steps

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

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

   Start IP

   Enter a start IP address.

   End IP

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

   Port

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

   User Name

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

   Password

Enter the device password.

Caution

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

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

Note

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

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

Add Device by ISUP Account

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

Before You Start

Make sure the devices have connected to the network properly.

Steps

1. Enter Device Management module.

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

Device Account

Enter the account name registered on ISUP protocol.

ISUP Key

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

Note

This function should be supported by the device.

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

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

Import Devices in a Batch

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

Steps

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

Note

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

Adding Mode

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

Address

Edit the address of the device.

Port

Enter the device port number. The default port number is ***8000***.

User Name

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

Password

Enter the device password.

Caution

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

Import to Group

Enter ***1*** to create a group by the device name. All the channels of the device will be imported to the corresponding group by default. Enter ***0*** to disable this function.

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

9.2.2 Reset Device Password

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

Steps

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

   All the online devices sharing the same subnet will be displayed in the list.
3. Select the device from the list and click on the Operation column.
4. Reset the device password.
   - Click **Generate** to pop up the QR Code window and click **Download** to save the QR code to your PC. You can also take a photo of the QR code to save it to your phone. Send the picture to our technical support.

Note

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

Caution

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

9.3 Group Management

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

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

9.3.1 Add Group

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

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

     Note

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

9.3.2 Import Resources to Group

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

Before You Start
Add a group for managing devices. Refer to ***Add Group*** .

Steps
1. Enter the Device Management module.
2. Click **Device Management → Group** to enter the group management page.
3. Select a group from the group list and select the resource type as **Access Point**, **Alarm Input**, **Alarm Output**, etc.
4. Click **Import**.
5. Select the thumbnails/names of the resources in the thumbnail/list view.

   Note

   You can click or to switch the resource display mode to thumbnail view or to list view.
6. Click **Import** to import the selected resources to the group.

9.3.3 Edit Resource Parameters

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

Before You Start
Import the resources to group.

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

   All the added groups are displayed on the left.
3. Select a group on the group list and click **Access Point**.

   The access points imported to the group will display.
4. Click in the Operation column to open the Edit Resource window.
5. Edit the resource name.
6. Click **OK** to save the new settings.

9.3.4 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.

9.4 Person Management

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

9.4.1 Add Organization

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

Steps

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

   Note

   Up to 10 levels of organizations can be added.
4. **Optional:** Perform the following operation(s).

Edit Organization	Hover the mouse on an added organization and click to edit its name.
Delete Organization	Hover the mouse on an added organization and click to delete it. **Note** • The lower-level organizations will be deleted as well if you delete an organization. • Make sure there is no person added under the organization, or the organization cannot be deleted.
Show Persons in Sub Organization	Check **Show Persons in Sub Organization** and select an organization to show persons in its sub organizations.

9.4.2 Configure Basic Information

You can add person to the client one by one and configure the person's basic information such as name, 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, telephone number, email address, validity period, etc.
5. Confirm to add the person.
   - Click **Add** to add the person and close the Add Person window.
   - Click **Add and New** to add the person and continue to add other persons.

9.4.3 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.

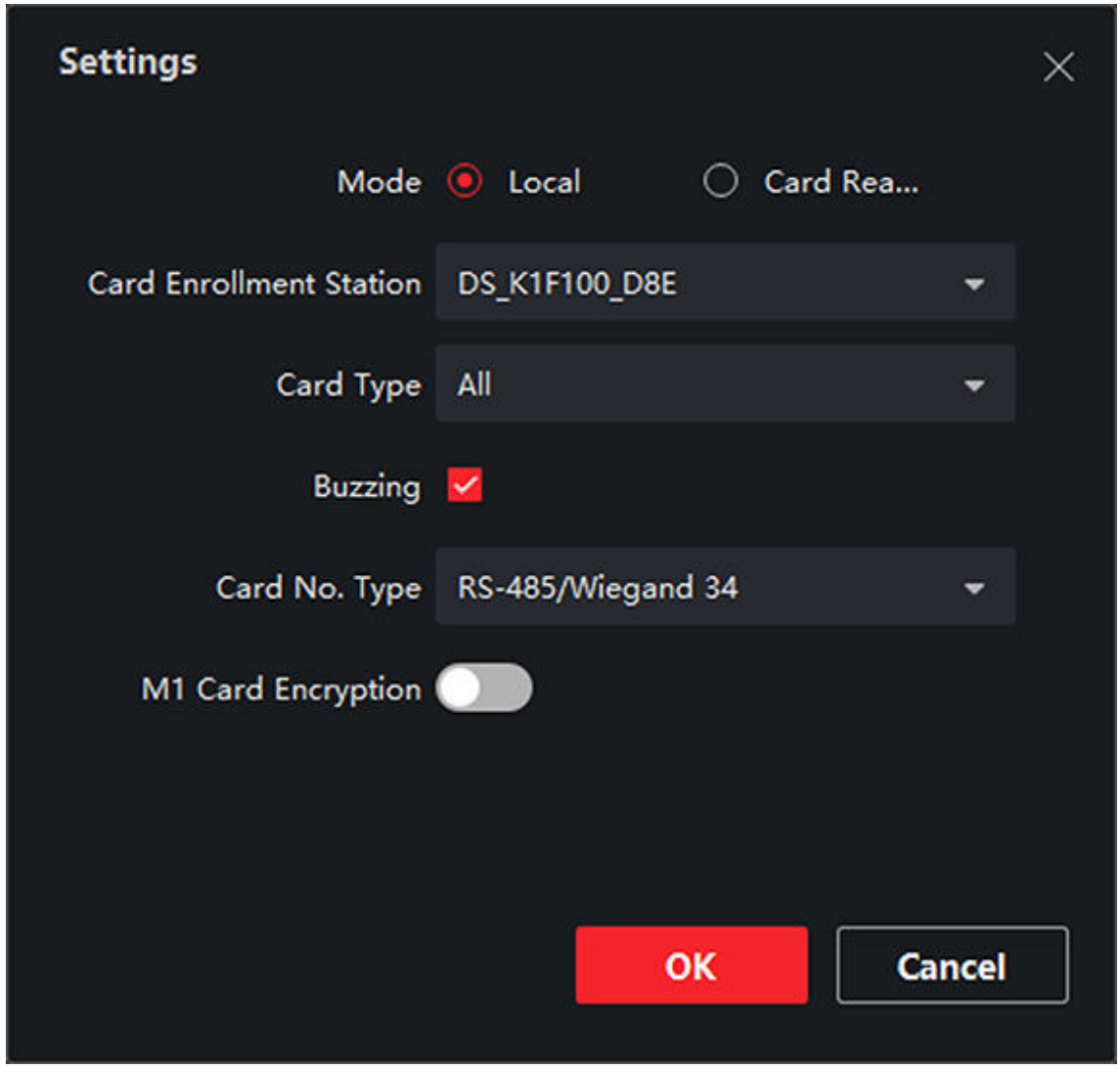


Figure 9-5 Issue a Card by Local Mode

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.

9.4.4 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 .

9.4.5 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.

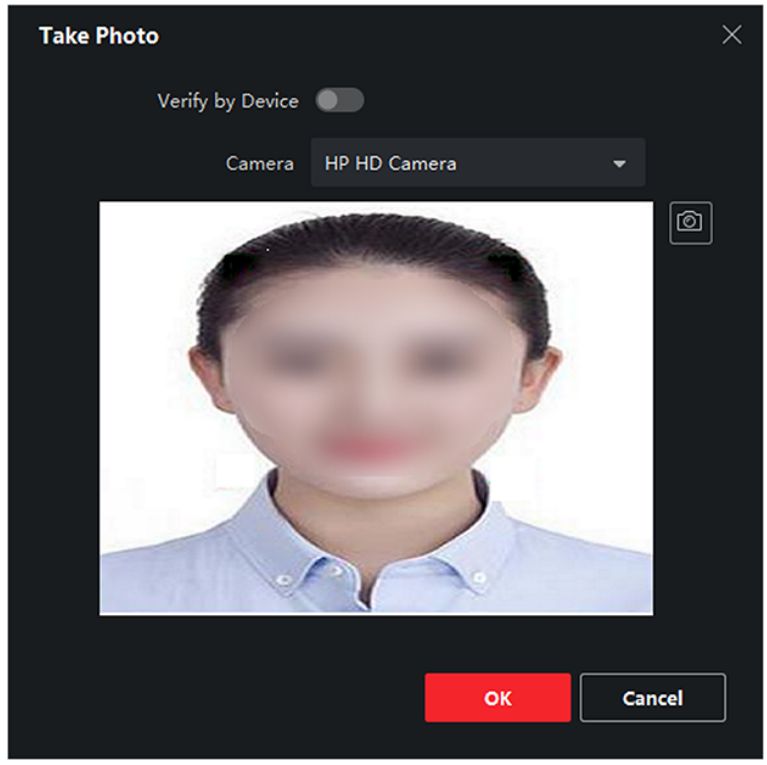


Figure 9-6 Take a Photo via Client

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.

9.4.6 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 .

9.4.7 Configure Access Control Information

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

Steps

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

Note

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

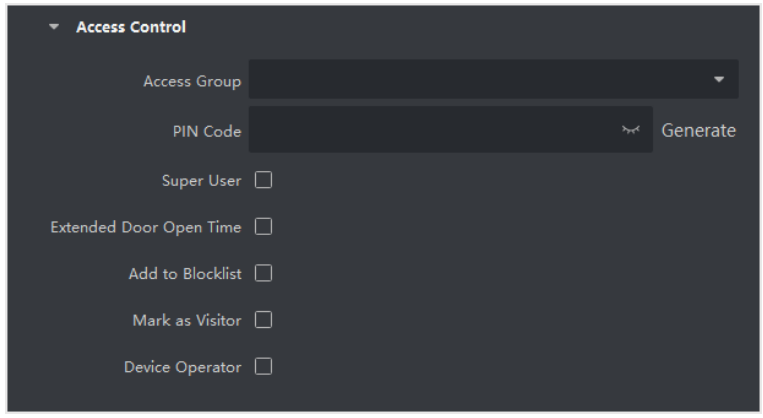


Figure 9-7 Configure Access Control Information

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

     Note

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

     Note

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

   Super User

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

   Extended Door Open Time

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

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

   Add to Blocklist

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

   Mark as Visitor

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

Note

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

Device Operator

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

Note

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

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

9.4.8 Customize Person Information

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

Steps

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

      Note

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

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

9.4.9 Configure Resident Information

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

Steps

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

   Note

   Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .
3. In the **Resident Information** panel, select the indoor station to bind it to the person.

   Note

   If you select **Analog Indoor Station**, the **Door Station** field will display and you are required to select the door station to communicate with the analog indoor station.
4. Enter the floor No. and room No. of the person.
5. Confirm to add the person.
   - Click **Add** to add the person and close the Add Person window.
   - Click **Add and New** to add the person and continue to add other persons.

9.4.10 Configure Additional Information

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

Steps

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

   Note

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

9.4.11 Import and Export Person Identify Information

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

9.4.12 Import Person Information

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

Steps

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

Note

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

7. Click ... to select the CSV/Excel file with person information from local PC.
8. Click **Import** to start importing.

Note

- If a person No. already exists in the client's database, delete the existing information before importing.
- You can import information of no more than 2,000 persons.

9.4.13 Import Person Pictures

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

Before You Start

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

Steps

1. Enter the Person module.

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

Note

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

6. Click **Import** to start importing.

   The importing progress and result will be displayed.

9.4.14 Export Person Information

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

Before You Start

Make sure you have added persons to an organization.

Steps

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

Note

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

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

9.4.15 Export Person Pictures

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

Before You Start

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

Steps

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

Note

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

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

Note

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

9.4.16 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.

9.4.17 Get Person Information from Access Control Device

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

Steps

Note

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

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

Note

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

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

Note

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

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

9.4.18 Move Persons to Another Organization

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

Before You Start

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

Steps

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

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

9.4.19 Issue Cards to Persons in Batch

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

Steps

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

   All the added persons with no card issued will be displayed in the right panel.
3. **Optional:** Enter key words (name or person ID) in the input box to filter the person(s) that need issuing cards.
4. **Optional:** Click **Settings** to set the card issuing parameters. For details, refer to *Issue a Card by Local Mode*.
5. Click **Initialize** to initialize the card enrollment station or card reader to make it ready for issuing cards.
6. Click the **Card No.** column and enter the card number.

- Place the card on the card enrollment station.
- Swipe the card on the card reader.
- Manually enter the card number and press the **Enter** key.

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

9.4.20 Report Card Loss

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

Steps

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

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

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

9.4.21 Set Card Issuing Parameters

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

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

Local Mode: Issue Card by Card Enrollment Station

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

Card Enrollment Station

Select the model of the connected card enrollment station

Note

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

Card Type

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

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

Serial Port

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

Select the COM the card enrollment station connects to.

Buzzing

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

Card No. Type

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

M1 Card Encryption

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

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

Remote Mode: Issue Card by Card Reader

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

9.5 Configure Schedule and Template

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

Note

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

9.5.1 Add Holiday

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

Steps

Note

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

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

   Note

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

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

      Note

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

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

9.5.2 Add Template

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

Steps

Note

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

1. Click **Access Control → Schedule → Template** to enter the Template page.

Note

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

All-Day Authorized

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

All-Day Denied

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

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

   Note

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

   3) **Optional:** Perform the following operations to edit the time durations.
      - Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to .
      - Click the time duration and directly edit the start/end time in the appeared dialog.
      - Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to .
   4) Repeat the two steps above to draw more time durations on the other days of the week.
6. Add a holiday to apply it to the template.

Note

Up to 4 holidays can be added to one template.

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

   Note

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

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

9.6 Set Access Group to Assign Access Authorization to Persons

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

Steps

When the access group settings are changed, you need to apply the access groups to the devices again to take effect. The access group changes include changes of template, access group settings, person's access group settings, and related person details (including card number, face picture, linkage between card number and linkage between card number and card password, card effective period, etc).

1. Click **Access Control → Authorization → Access Group** to enter the Access Group interface.
2. Click **Add** to open the Add window.
3. In the **Name** text field, create a name for the access group as you want.
4. Select a template for the access group.

   Note

   You should configure the template before access group settings. Refer to ***Configure Schedule and Template*** for details.
5. In the left list of the Select Person field, select person(s) to assign access authority.
6. In the left list of the Select Access Point field, select door(s), door station(s) or floor(s) for the selected persons to access.
7. Click **Save**.

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

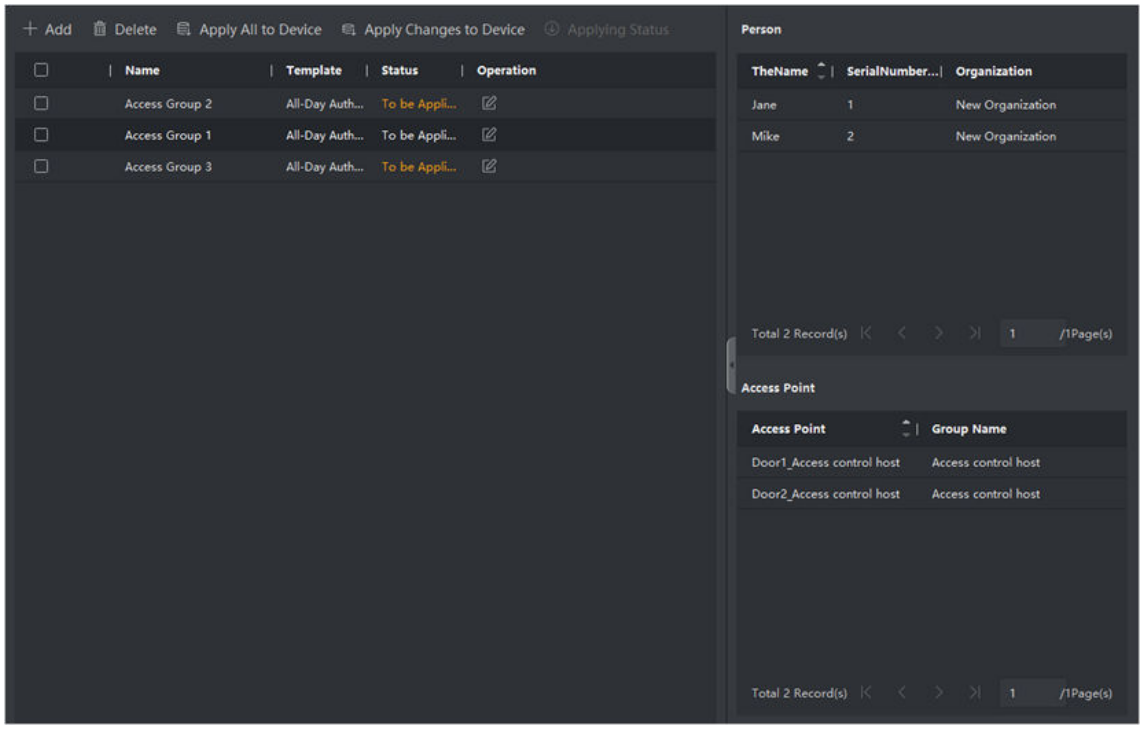


Figure 9-8 Display the Selected Person(s) and Access Point(s)

8. After adding the access groups, you need to apply them to the access control device to take effect.
   1) Select the access group(s) to apply to the access control device.
   2) Click **Apply All to Devices** start applying all the selected access group(s) to the access control device or door station.
   3) Click **Apply All to Devices** or **Apply Changes to Devices**.

      Apply All to Devices

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

      Apply Changes to Devices

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

   Note

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

   The selected persons in the applied access groups will have the authorization to enter/exit the selected doors/door stations with their linked card(s).
9. **Optional:** Click to edit the access group if necessary.

Note

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

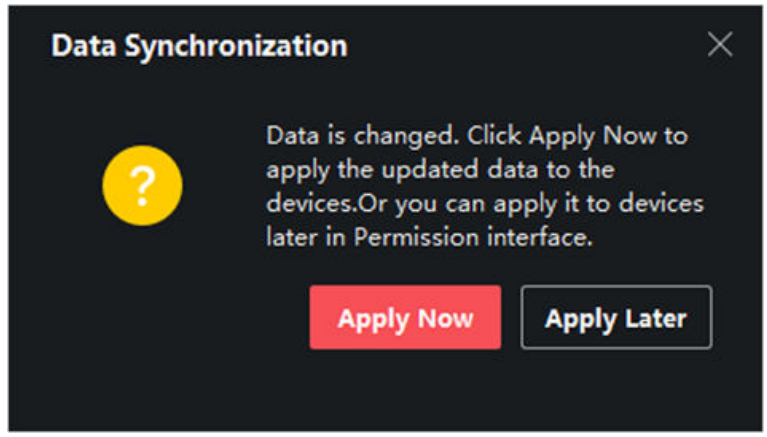


Figure 9-10 Data Synchronization

9.7 Configure Advanced Functions

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

Note

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

9.7.1 Configure Device Parameters

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

Configure Parameters for Access Control Device

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

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

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 of the selected device.
3. Select a door to show its parameters on the right page.
4. Edit the door 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.

Super Password

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

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.

Click **Advanced** to configure more parameters.

Extended Open Duration

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

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.

Note

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

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

Note

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

Configure Parameters for Card Reader

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

Steps

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

Note

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

Basic Information

Name

Edit the card reader name as desired.

Minimum Card Swiping Interval

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

Alarm of Max. Failed Attempts

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

Card Reader Type/Card Reader Description

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

Advanced

Enable Card Reader

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

OK LED Polarity/Error LED Polarity/Buzzer Polarity

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

Max. Interval When Entering PWD

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

Tampering Detection

Enable the anti-tamper detection for the card reader.

Communication with Controller Every

Set the max. failure attempts of reading card.

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 Level

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

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

Configure Parameters for Alarm Output

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

Before You Start

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

Steps

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

Name

Edit the card reader name as desired.

Alarm Output Active Time

How long the alarm output will last after triggered.

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

9.7.2 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).

9.7.3 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.

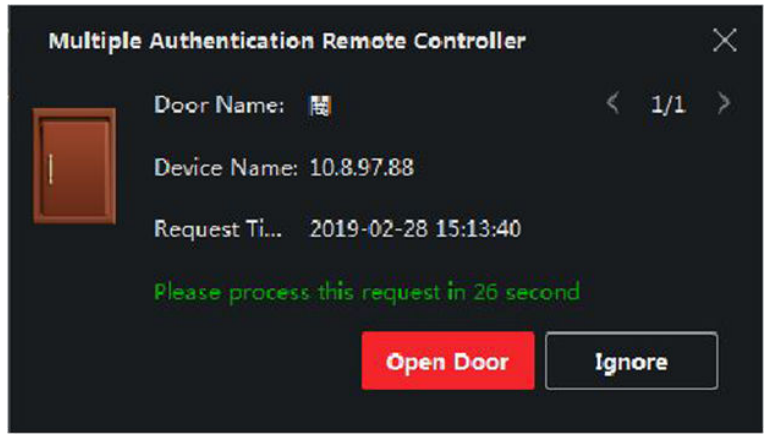


Figure 9-11 Remotely Open Door

Note

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

Local Authentication and Super Password

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

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

Note

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

6) Click **Save**.

Note

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

7. Click **Save**.

9.7.4 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.

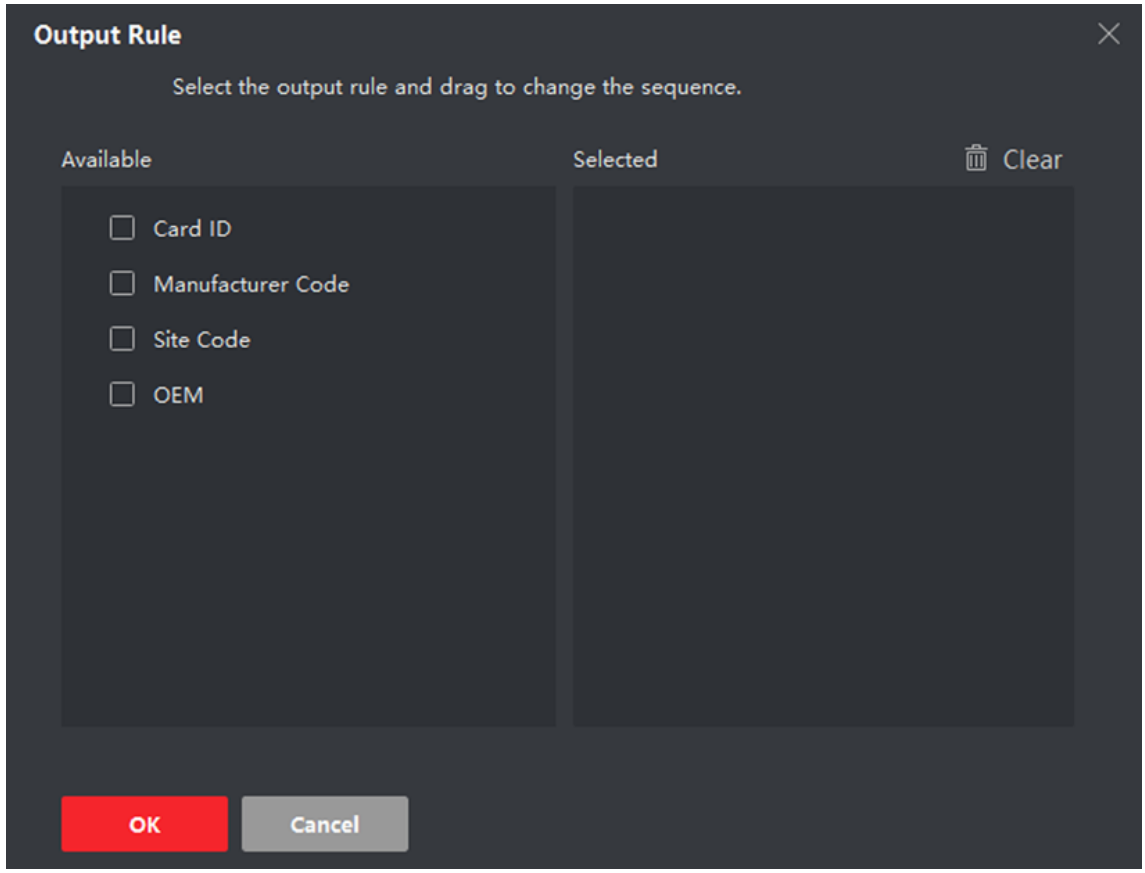


Figure 9-12 Set Output Transformation Rule

2) Select rules on the left list.

The selected rules will be added to the right list.

3) **Optional:** Drag the rules to change the rule order.

4) Click **OK**.

5) In the Custom Wiegand tab, set the rule's start bit, length, and the decimal digit.

7. Click **Save**.

9.7.5 Configure Card Reader Authentication Mode and Schedule

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

Steps

1. Click **Access Control → Advanced Function → Authentication** to enter the authentication mode configuration page.

2. Select a card reader on the left to configure.

3. Set card reader authentication mode.

1) Click **Configuration**.

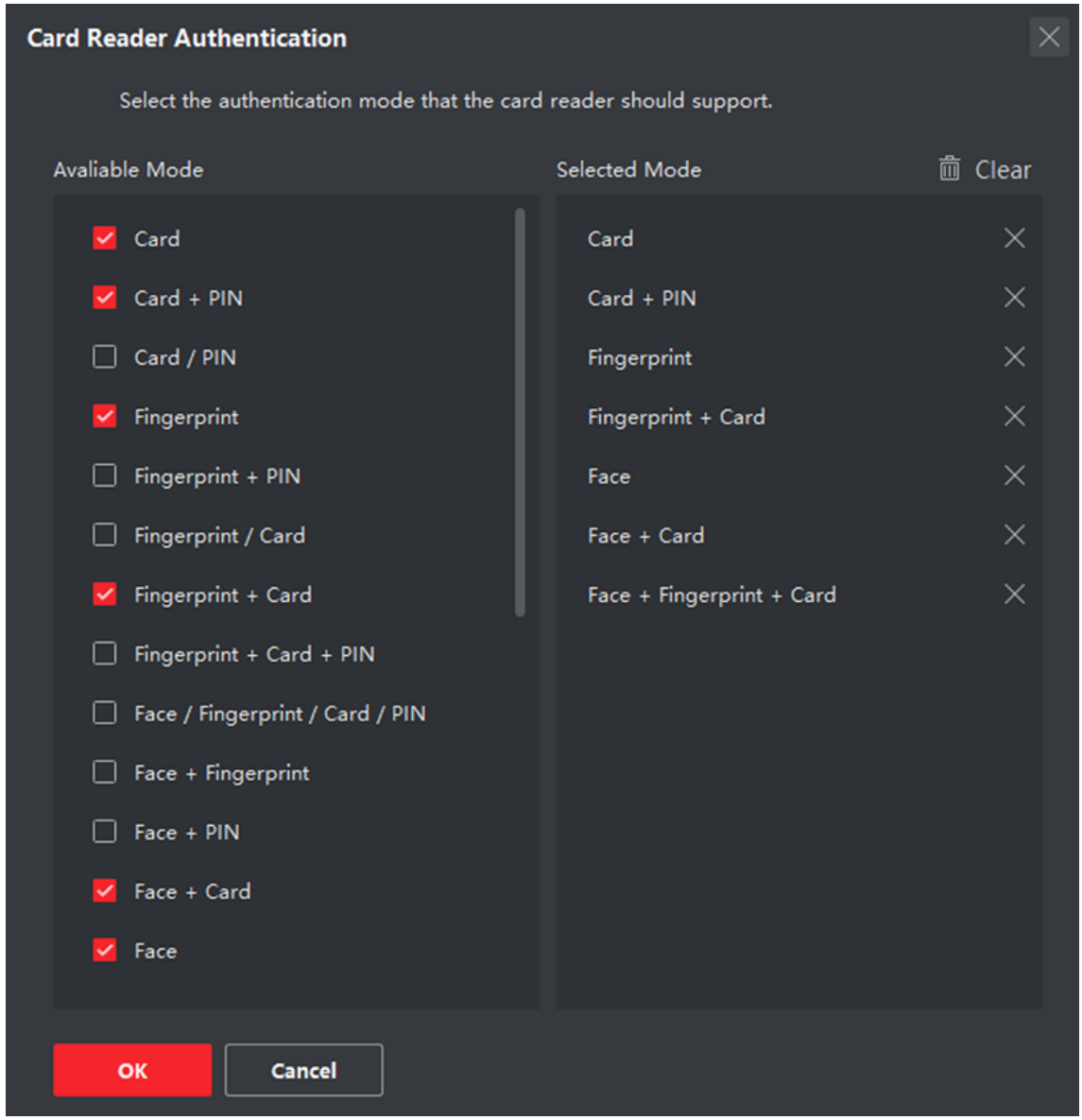


Figure 9-13 Select Card Reader Authentication Mode

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.

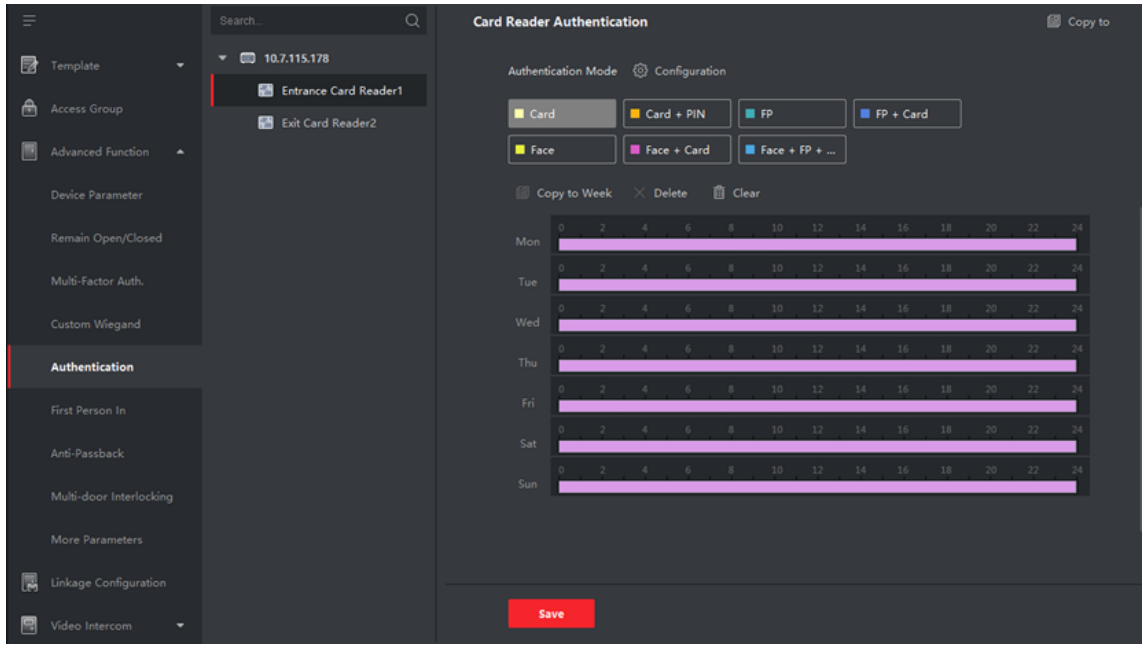


Figure 9-14 Set Authentication Modes for Card Readers

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**.

9.7.6 Configure First Person In

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

Before You Start

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

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

Steps

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

9.7.7 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.

9.7.8 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 EHome account via wired network.

Set Log Uploading Mode

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

Steps

Note

Make sure the device is not added by ISUP.

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

   Note

   - The main channel and the backup channel cannot enable N1 or G1 at the same time.
   - N1 refers to wired network and G1 refers to GPRS.
7. Click **Save**.

Create EHome Account in Wired Communication Mode

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

Steps

Note

- This function should be supported by the device.
- Make sure the device is not added by EHome.

1. Enter the Access Control module.

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

Note

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

8. Select the **Protocol Type** as **EHome** and select EHome version.

Note

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

Steps

Note

This function should be supported by the device.

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

   Note

   These parameters displayed vary according to different device models.

   Algorithm

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

   Save Authenticating Face Picture

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

   ECO Mode

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

   Note

   Only device in the normal mode supports configuring ECO mode parameters.

   Work Mode

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

Enable M1 Card Encryption

M1 card encryption can improve the security level of authentication.

Steps

Note

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

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

5. Set the sector ID.

Note

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

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

Set RS-485 Parameters

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

Steps

Note

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

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function → More Parameters** .
3. Select an access control device in the device list and click **RS-485** to enter the RS-485 Settings page.
4. Select the serial port number from the drop-down list to set the RS-485 parameters.
5. Set the baud rate, data bit, the stop bit, parity type, communication mode, working mode, and connection mode in the drop-down list.
6. Click **Save**.
   - The configured parameters will be applied to the device automatically.
   - After changing the working mode or connection mode, the device will reboot automatically.

Set Wiegand Parameters

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

Steps

Note

This function should be supported by the device.

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function → More Parameters** .
3. Select an access control device in the device list and click **Wiegand** to enter the Wiegand Settings page.

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

Note

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

6. Check **Enable Wiegand** to enable the Wiegand function.
7. Click **Save**.
   - The configured parameters will be applied to the device automatically.
   - After changing the communication direction, the device will reboot automatically.

9.8 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, ..

9.8.1 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.

9.8.2 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.

9.8.3 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.

9.8.4 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.

9.9 Door Control

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

Note

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

9.9.1 Control Door Status

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

Before You Start

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

Steps

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

   Note

   For managing the access point group, refer to ***Group Management*** .

   The doors in the selected access control group will display.
3. Click a door icon to select a door, or press **Ctrl** and select multiple doors.

   Note

   For **Remain All Unlocked** and **Remain All Locked**, ignore this step.
4. Click the following buttons to control the door.

   Unlock

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

Lock

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

Remain Unlocked

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

Remain Locked

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

Remain All Unlocked

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

Remain All Locked

All doors in the group will be closed and locked. No person can access the doors even if he/she has the authorized credentials, except the super users.

Capture

Capture a picture manually.

Note

The **Capture** button is available when the device supports capture function. The picture is saved in the PC running the client. For setting the saving path, refer to *Set File Saving Path* in the user manual of the client software.

Result

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

9.9.2 Check Real-Time Access Records

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

Before You Start

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

Steps

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

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

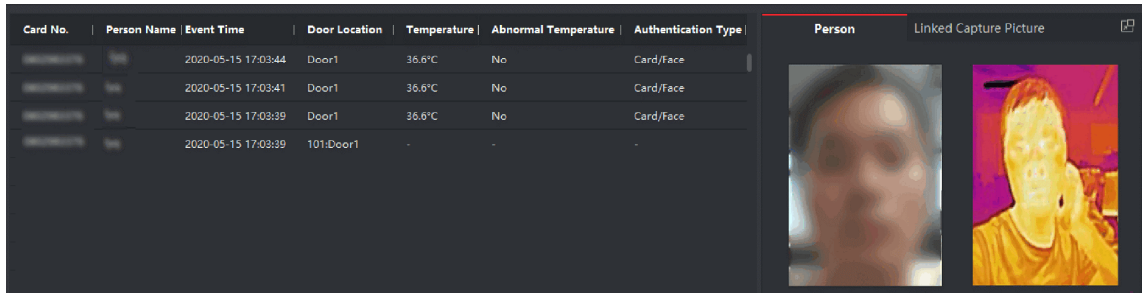


Figure 9-15 Real-time Access Records

Note

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

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

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

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

Note

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

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

Note

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

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

Note

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

9.10 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*** .

9.10.1 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.

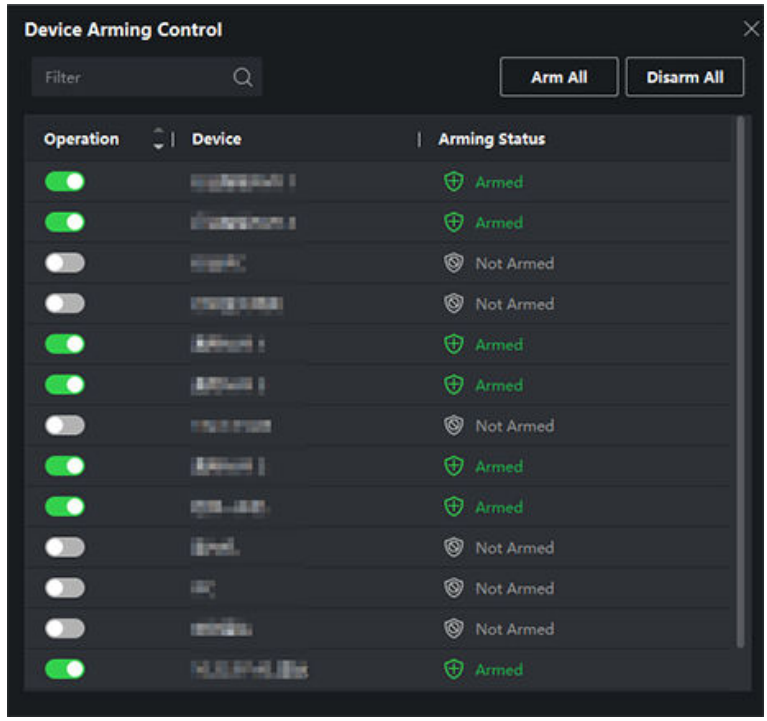


Figure 9-16 Arm Device

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.

9.10.2 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.

9.10.3 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.

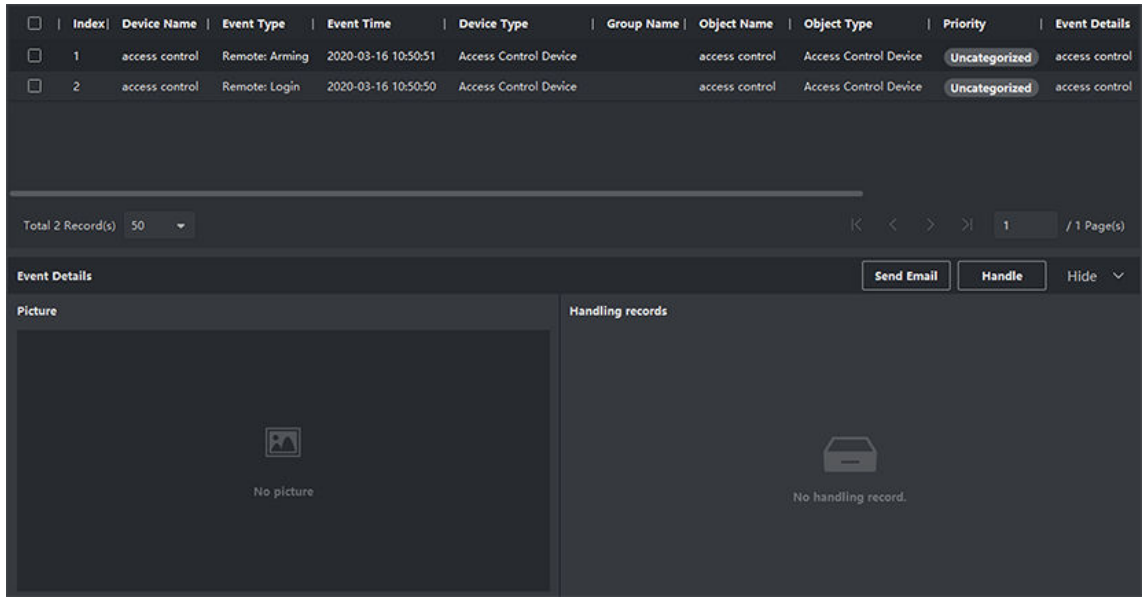


Figure 9-17 Search Historical Events

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.

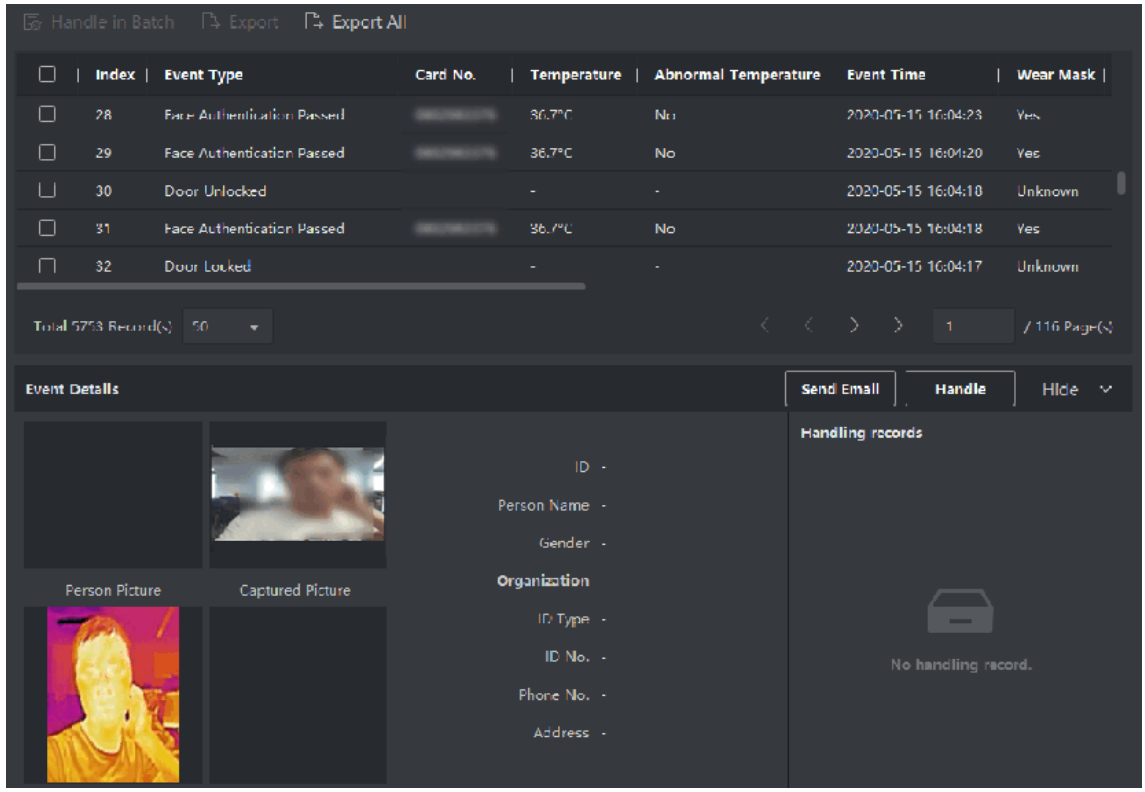


Figure 9-18 Search Historical Event

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.

9.11 Time and Attendance

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

Note

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

9.11.1 Configure Attendance Parameters

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

Set Weekend

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

Steps

Note

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

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

Configure Overtime Parameters

You can configure the overtime parameters for workday and weekend, including overtime level, work hour rate, attendance status for overtime, etc.

Steps

1. Click **Time & Attendance → Attendance Settings → Overtime** .
2. Set required information.

   Overtime Level for Workday

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

   Work Hour Rate

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

   Overtime Rule for Weekend

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

Configure Attendance Check Point

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

Before You Start

- You have added access control device(s). For details, refer to ***Add Device*** .
- You have enabled T&A Status. For details, refer to ***Add General Timetable*** .

By default, all card readers of the added access control devices are set as start/end-work check points. If you need to edit check point function of card reader(s), you can perform the following operations.

Steps

1. Enter the Time & Attendance module.
2. Click **Attendance Settings → Attendance Check Point** to enter the attendance check point settings page.
3. Set **Set All Card Readers as Check Points** switch to off.
4. Check the desired card reader(s) as attendance check point(s) in the list below.
5. Set check point function as **Start/End-Work**, **Start-Work** or **End-Work**.

Note

When selecting **Start-Work** or **End-Work**, the attendance status uploaded from the device will be decided by the check point function you set here.

Start-Work

Attendance status uploaded from the device will all be calculated as Check-in.

End-Work

Attendance status uploaded from the device will all be calculated as Check-out.

Start/End-Work

Attendance status will be calculated as Check in/out according to the actual attendance status on the device.

6. Click **Set as Check Point**.

The configured attendance check point(s) are displayed on the right list.

7. **Optional:** After setting attendance check points, and perform the following operations.

Edit Check Point	Check one attendance check point, click **Edit** to edit its information including name, check point function, etc. Check two or more attendance check points, click **Edit** to batch edit check point function, enter remark, etc.
Delete Check Point	Check one or more check points, and click **Delete** to delete it/them.

Configure Holiday

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

Add Regular Holiday

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

Steps

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

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

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

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

Add Irregular Holiday

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

Steps

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

   Example

   If you want to set the forth Thursday in November, 2019 as the Thanksgiving Day holiday, you should select 2019, November, 4th, and Thursday from the four drop-down lists.
7. Enter the number of the holiday days.
8. Set the attendance status if the employee works on holiday.
9. **Optional:** Check **Repeat Annually** to make this holiday setting effective every year

10. Click **OK**.

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

    If the date is selected as different holidays, it will be recorded as the first-added holiday.

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

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

Configure Leave Type

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

Steps

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

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

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

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

Synchronize Authentication Record to Third-Party Database

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

Steps

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

Note

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

5. Set the other required parameters of the third-party database, including server IP address, port No., database name, user name and password.

Note

The default port No. of the selected database type is displayed automatically. You can enter a number ranging from 1 to 65535 to customize the port No if needed.

6. Set table parameters of database according to the actual configuration.
   1) Enter the table name of the third-party database.
   2) Set the mapped table fields between the client and the third-party database.
7. Click **Save** to test whether database can be connected and save the settings for the successful connection.
   - The attendance data will be written to the third-party database.
   - During synchronization, if the client disconnects with the third-party database, the client will start reconnection every 30 mins. After being reconnected, the client will synchronize the data recorded during the disconnected time period to the third-party database.

Configure Break Time

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

Steps

1. Click **Time & Attendance → Timetable → Break Time** .
   The added break time is displayed in the list.
2. Click **Break Time Settings** to enter Break Time Settings window.
3. Click **Add**.
4. Enter a name for the break time.
5. Set related parameters for the break time.

Start Time / End Time

Set the time when the break starts and ends.

No Earlier Than / No Later Than

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

Break Duration

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

Calculation

Auto Deduct

The break duration will be calculated according to the time you set.

Must Check

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

Return from Break Early for

The actual check-in and check-out time does not exceed the break time, and can be marked as normal work or work overtime.

Return from Break Late for

The actual check-in and check-out time exceeds the break time, and can be marked as late, absent or early leave.

Calculated by

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

First In & Last Out: The first check-in time is recorded as start break time and the last check-out time is recorded as the end break time.

Enable T&A Status

Set **Enable T&A Status** switch to on to calculate the actual break time according to attendance status on the device.

Note

This function should be supported by the device.

Valid Authentication Interval

During the valid authentication interval, person swiping card for several times will only be calculated as once when calculating attendance data.

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

Configure Report Display

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

Steps

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

Company Name

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

Attendance Status Mark

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

Weekend Mark

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

4. Click **Save**.

9.11.2 Add General Timetable

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

Steps

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

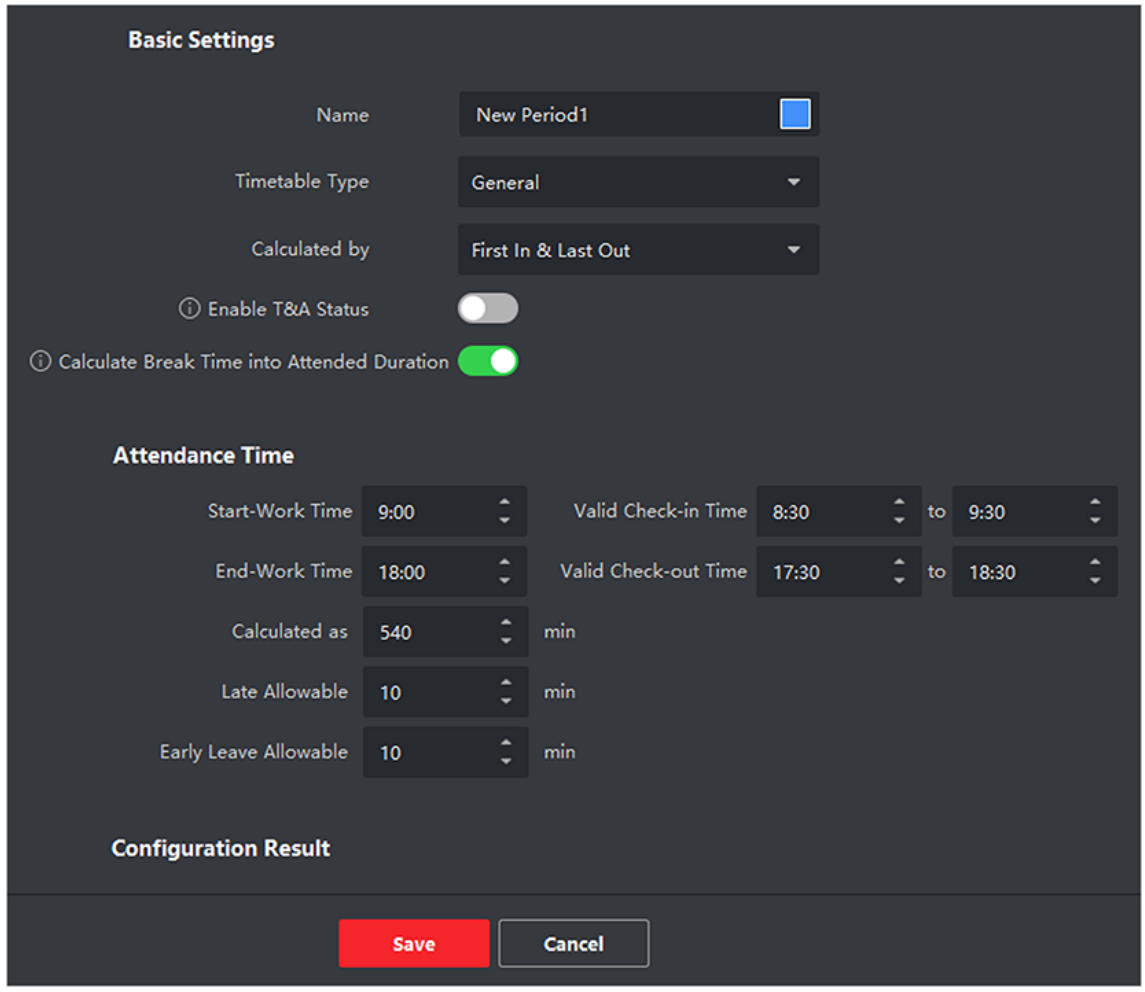


Figure 9-19 Add Timetable

3. Create a name for the timetable.

Note

You can click the color icon beside the name to customize the color for the valid timetable on the time bar in the Configuration Result area.

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

First In & Last Out

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

Each Check-In/Out

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

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

6. **Optional:** Set **Enable T&A Status** switch to on to calculate according to attendance status of the device.

Note

This function should be supported by the device.

7. **Optional:** Enable **Calculate Break Time into Attended Duration**.

Note

When enabled, break time will be calculated into the overall attendance duration. That is, the actual attendance duration equals to the overall attendance duration (includes break time).

8. Set the related attendance time parameters as the following:

Start/End-Work Time

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

Valid Check-in/out Time

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

Calculated as

Set the duration calculated as the actual work duration.

Late/Early Leave Allowable

Set the timetable for late or early leave.

9. Set absence related parameters.

Check-In, Late for

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

Check-Out, Early Leave for

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

No Check-in

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

No Check-Out

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

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

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

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

9.11.3 Add Shift

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

Before You Start
Add a timetable first. See ***Add General Timetable*** for details.

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

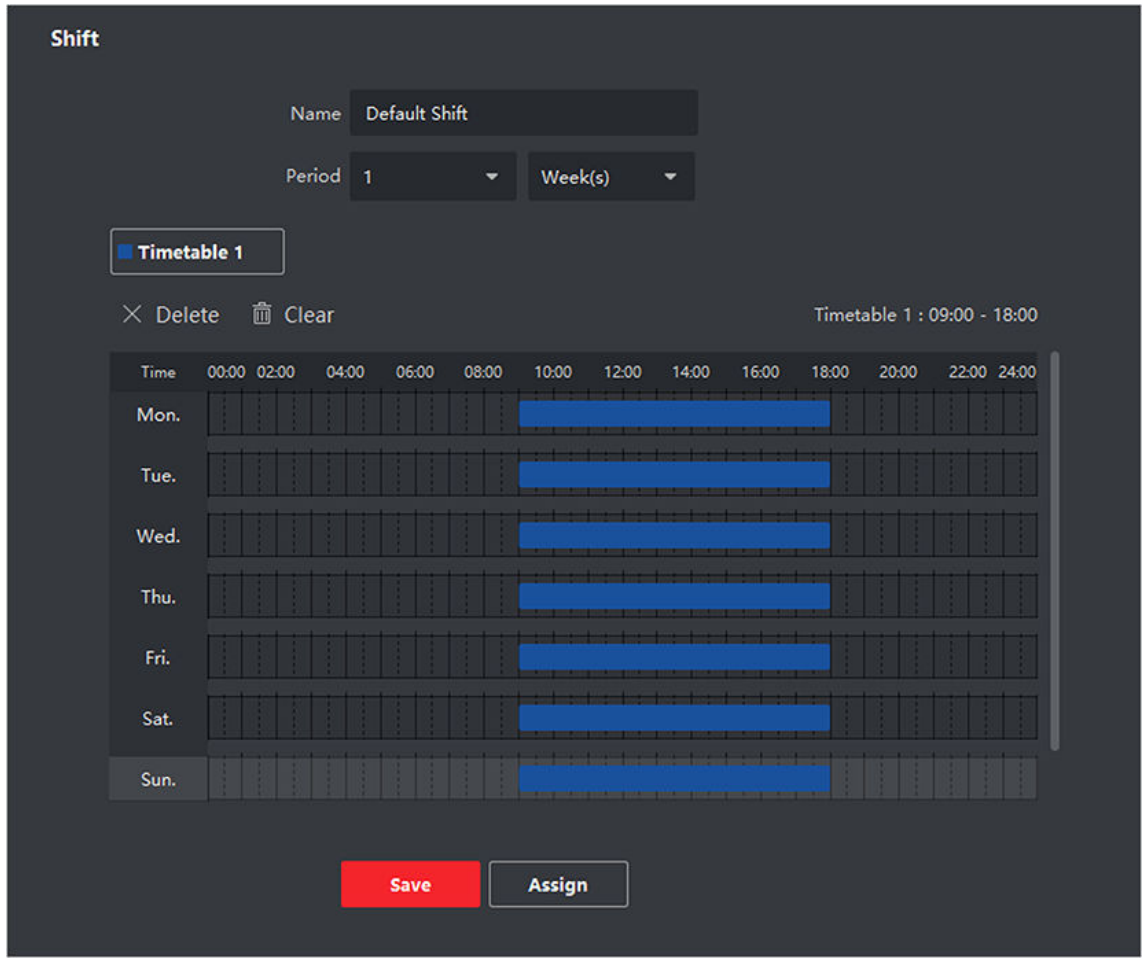


Figure 9-20 Add Shift

Note

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

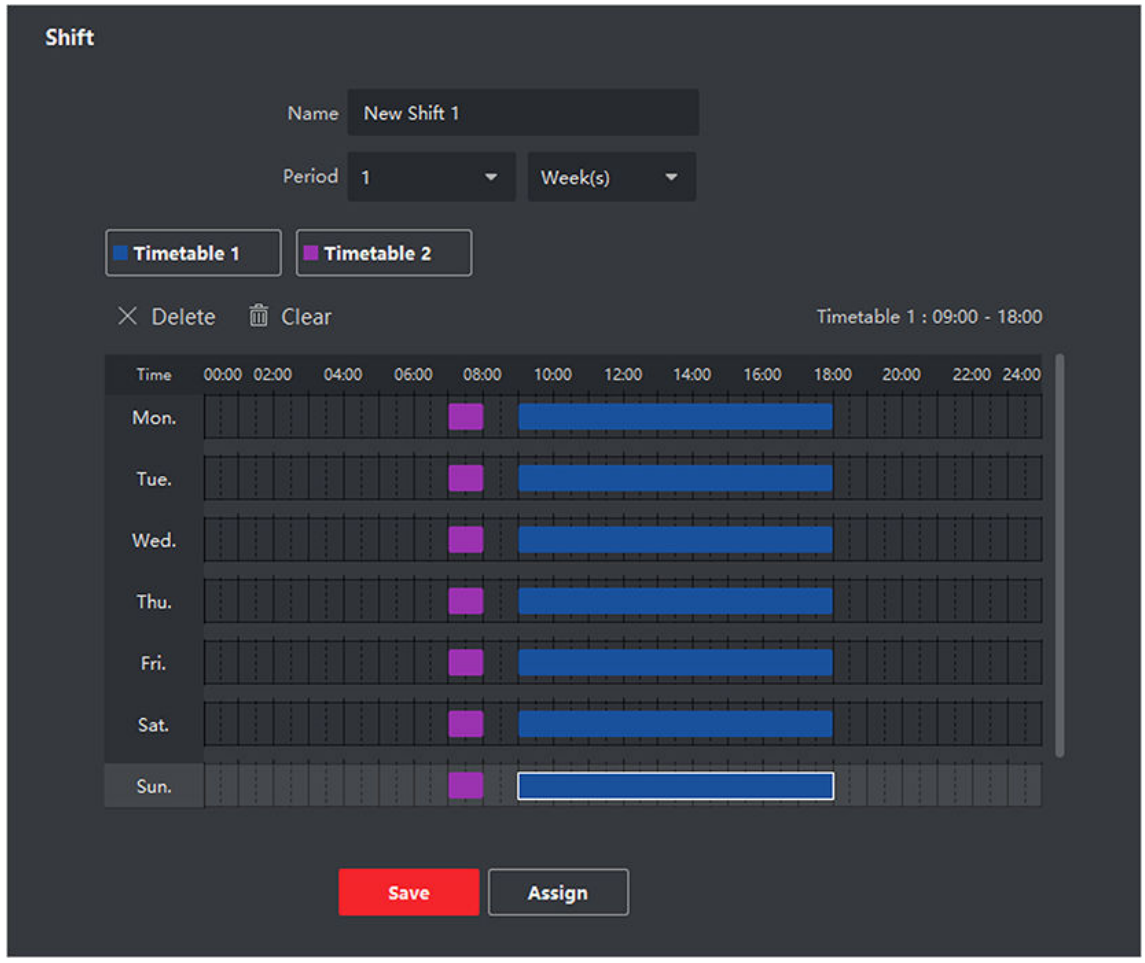


Figure 9-21 Add Multiple Timetables

6. Click **Save**.

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

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

   1) Click **Assign**.

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

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

   3) Set the Expire Date for the shift schedule.

   4) Set other parameters for the schedule.

      Check-in Not Required

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

      Check-out Not Required

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

      Scheduled on Holidays

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

Effective for Overtime

The persons' overtime will be recorded for this schedule.

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

9.11.4 Manage Shift Schedule

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

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

Set Department Schedule

You can set the shift schedule for one department, and all the persons in the department will be assigned with the shift schedule.

Before You Start

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

Steps

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

Note

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

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

Note

This is only available for shift with only one timetable.

Multiple Shift Schedules

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

If the multiple shift schedules contains three timetables: 00:00 to 07:00, 08:00 to 15:00 and 16:00 to 23:00. The attendance of the person adopting this multiple shift schedules will be effective in any of the three timetables. If the person checks in at 07:50, it will apply the nearest timetable 08:00 to 15:00 to the person's attendance.

6. Set the start date and end date.
7. Set other parameters for the schedule.

Check-in Not Required

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

Check-out Not Required

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

Scheduled on Holidays

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

Effective for Overtime

The persons' overtime will be recorded for this schedule.

Flexible Shift Schedule on Weekend

The person's attendance on the weekend will be recorded as overtime.

8. Click **Save**.

Set Person Schedule

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

Before You Start

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

Steps

Note

The person schedule has the higher priority than department schedule.

1. Click **Time & Attendance → Shift Schedule** to enter the Shift Schedule page.
2. Click **Person Schedule** to enter Person Schedule page.
3. Select the organization and select the person(s).
4. Select the shift from the drop-down list.
5. **Optional:** Enable **Multiple Shift Schedules** and select the effective time period(s) from the added timetables for the persons.

Note

This is only available for shift with only one timetable.

Multiple Shift Schedules

It contains more than one timetables. The person can check in/out in any of the timetables and the attendance will be effective.
If the multiple shift schedules contains three timetables: 00:00 to 07:00, 08:00 to 15:00 and 16:00 to 23:00. The attendance of the person adopting this multiple shift schedules will be effective in any of the three timetables. If the person checks in at 07:50, it will apply the nearest timetable 08:00 to 15:00 to the person's attendance.

6. Set the start date and end date.
7. Set other parameters for the schedule.

Check-in Not Required

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

Check-out Not Required

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

Scheduled on Holidays

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

Effective for Overtime

The persons' overtime will be recorded for this schedule.

Flexible Shift Schedule on Weekend

The person's attendance on the weekend will be recorded as overtime.

8. Click **Save**.

Set Temporary Schedule

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

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

Steps

Note

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

1. Click **Time & Attendance → Shift Schedule** to enter the Shift Schedule Management page.
2. Click **Temporary Schedule** to enter Temporary Schedule page.
3. Select the organization and select the person(s).

4. Click one date or click and drag to select multiple dates for the temporary schedule.
5. Select **Workday** or **Non-Workday** from drop-down list.

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

   Calculated as

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

   Timetable

   Select a timetable from drop-down list.

   Multiple Shift Schedule

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

   If the multiple shift schedules contains three timetables: 00:00 to 07:00, 08:00 to 15:00 and 16:00 to 23:00. The attendance of the person adopting this multiple shift schedules will be effective in any of the three timetables. If the person checks in at 07:50, it will apply the nearest timetable 08:00 to 15:00 to the person's attendance.

   Rule

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

Check Shift Schedule

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

Steps

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

   Calendar

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

   List

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

9.11.5 Manually Correct Check-in/out Record

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

Before You Start

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

Steps

1. Click **Time & Attendance → Attendance Handling** to enter attendance handling page.
2. Click **Correct Check-in/out** to enter adding check-in/out correction page.
3. Select one or more persons from left list for correction.
4. Select the correction date.
5. Select the correction type as **Check-in**, **Check-out**, **Break-in**, **Break-out**, etc,. and set the correct time.

   Note

   You can click ⊕ to add multiple correction items. At most 8 check-in/out items can be added.
6. **Optional:** Enter the remark information as desired.
7. Click **Save** to save the above settings.
8. **Optional:** After adding the check-in/out correction, perform one of the following operations.

View	Click ▦ or ☰ to view the added attendance handling information in calendar or list mode.
Edit	• In calendar mode, click ✎ → **Edit** to edit the details. • In list mode, double-click the related field in Date, Handling Type, Time, or Remark column to edit the details. **Note** The edited check-in/out correction will take affect.
Delete	• In calendar mode, select one check-in/out correction, and click **Delete** to delete the selected item. • In list mode, check one or more check-in/out corrections, and click **Delete** to delete the selected items. **Note** The deleted check-in/out correction will no longer take affect.
Export	In list mode, check one or more check-in/out corrections to export the attendance handling details (CSV file) to local PC.

9.11.6 Add Leave and Business Trip

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

Before You Start

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

Steps

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

   Note

   You can set the leave type in Attendance Settings. For details, refer to ***Configure Leave Type*** .
6. Set the time for leave.
7. **Optional:** Enter the remark information as desired.
8. Click **Save**.
9. **Optional:** After adding the leave and business trip, perform one of the following operations.

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

   Note

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

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

   Delete Delete the selected items.

   Export Export the attendance handling details to local PC.

   Note

   The exported details are saved in CSV format.

9.11.7 Calculate Attendance Data

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

Automatically Calculate Attendance Data

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

Steps

Note

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

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

Manually Calculate Attendance Data

You can manually calculate attendance data by setting conditions including attendance time, department, attendance status, etc.

Steps

1. Enter the Time & Attendance module.
2. Click **Attendance Statistics → Calculation** .
3. Set the start time and end time to define the attendance data range.
4. Select the department from the drop-down list.
5. **Optional:** Set other conditions, including name and person ID.
6. Check attendance status (supports multi-selection).
7. Click **Calculate**.

   Note

   Only the attendance data within three months can be calculated.
8. **Optional:** Perform one of the following operations.

Correct Check-in/out	Select one person, click **Correct Check-in/out** to add check-in/out correction.
Select Items to Display	Click on the upper right corner, or right click the table header of the attendance data list to customize the items to be displayed in the list.
Adjust Items Sequence	Click one item (except Person ID) and move the mouse to customize the sequence of different items.
Generate Report	Click **Report** to generate the attendance report.

Note

The report items will be displayed in the sequence you have set.

Export Report Click **Export** to export attendance data (CSV file) to local PC.

Note

The report items will be displayed in the sequence you have set.

9.11.8 Attendance Statistics

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

Get an Overview of Employees' Attendance Data

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

Before You Start

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

Note

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

Steps

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

Note

There are two methods for getting attendance events from the device, including **Online** and **Import File**. For more details about operations, refer to *Get Events from Device* in the user manual of the client software.

7. **Optional:** Click **Reset** to reset all the search conditions and edit the search conditions again.
8. Click **Search**.
9. **Optional:** For the displayed search results, perform one of the following operations.

Edit Attendance Status	Select one incorrect record, double click the field of **Attendance Status** column and select from the drop-down list to edit single piece of attendance status. Check two or more incorrect records, click **Edit Attendance Status** on the upper left corner and select from the drop-down list to batch edit multiple pieces of attendance status.
Generate Report	Click **Report** to generate the attendance report.
Export Report	Click **Export** and select saving path to export the attendance report (CVS file) to the local PC.
Custom Export	Click **Custom Report** and set conditions to export attendance records according to actual needs. For details, refer to *Custom Export Attendance Records* in the user manual of the client software.

Generate Instant Report

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

Before You Start

Calculate the attendance data.

Note

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

Steps

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

Send Report Regularly

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

Steps

1. Enter the Time & Attendance module.
2. Click **Attendance Statistics → Regularly Send Report** .
3. Click **Add** to enter the add custom report page.
4. Set the report content.

   Report Name

   Enter a name for the report.

   Report Type

   Select one report type and this report will be generated.

   Report Time

   The time to be selected may vary for different report type.

   Person

   Select the added person(s) whose attendance records will be generated for the report.

   Note

   You can view the selected person(s) in the right side of the Person area.

5. Set the schedule to send the report to the email address(es) automatically.

   Note

   The **Auto-Send Email** function is enabled by default.

   1) Set the Effective Period during which the client will send the report on the selected sending date(s).
   2) Select the Sending Date(s) on which the client will send the report.
   3) Set the Sending Time at which the client will send the report.

      Example

      If you set the effective period as ***2018/3/10 to 2018/4/10***, select ***Friday*** as the sending date, and set the sending time as ***20:00:00***, the client will send the report at 8 p.m. on Fridays during 2018/3/10 to 2018/4/10.

      Note

      Make sure the attendance records are calculated before the sending time. You can calculate the attendance data manually, or set the schedule so that the client can calculate the data automatically every day. For details, refer to ***Calculate Attendance Data*** .

   4) Enter the receiver email address(es).

Note

Up to 5 email addresses can be added. You can click **+** to add a new email address.

5) **Optional:** Click **Preview** to view the email details.

6. Click **OK**.

7. **Optional:** After adding the custom report, you can do one or more of the followings:

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

9.12 System Configuration

9.12.1 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**.

9.12.2 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**.

9.12.3 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.

9.12.4 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**.

9.12.5 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**.

9.12.6 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**.

9.13 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.

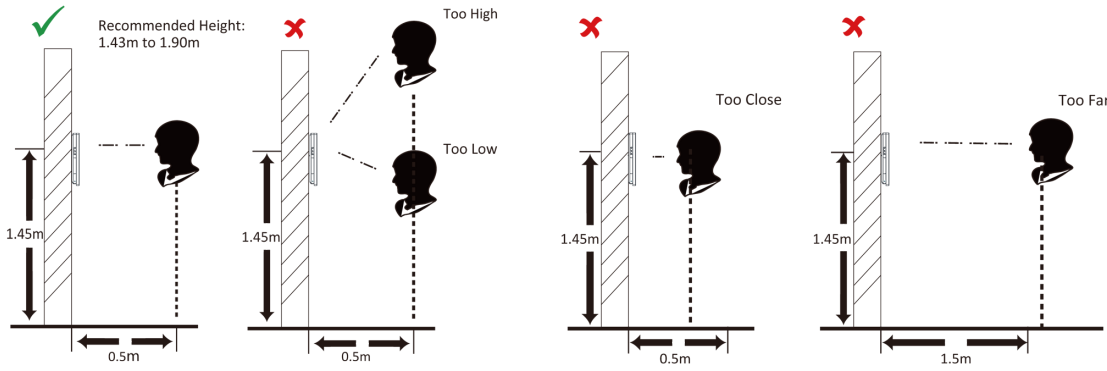
Message Queue

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 When Collecting/Comparing Face Picture

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

Positions (Recommended Distance: 0.5 m)



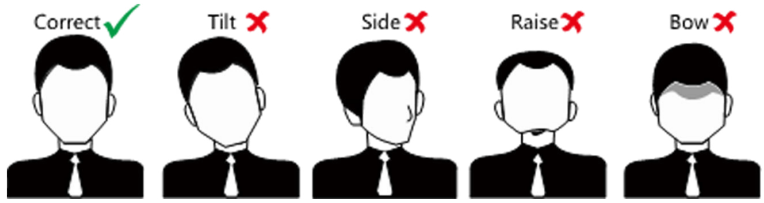
Expression

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

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

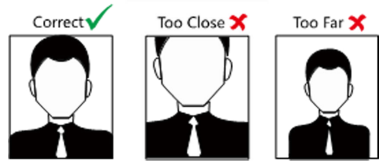
Posture

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



Size

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



Appendix B. Tips for Installation Environment

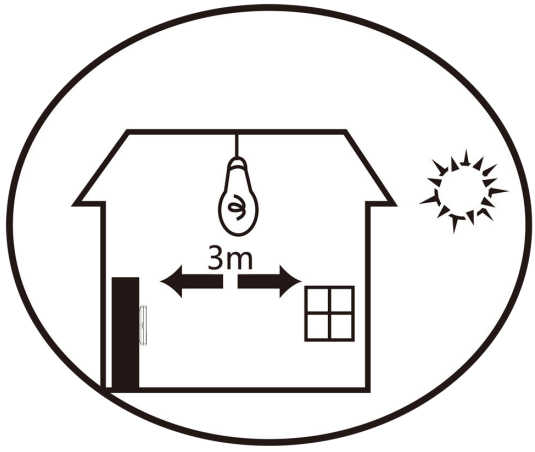
1. Light Source Illumination Reference Value

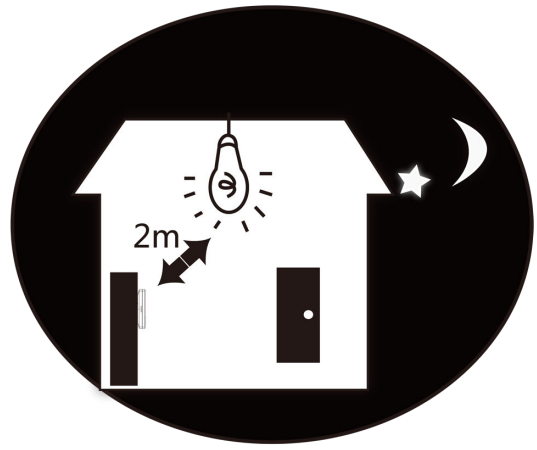
Candle: 10Lux

Bulb: 100~850Lux

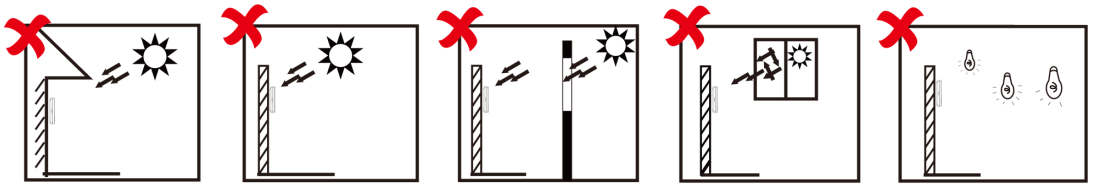
Sunlight: More than 1200Lux

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



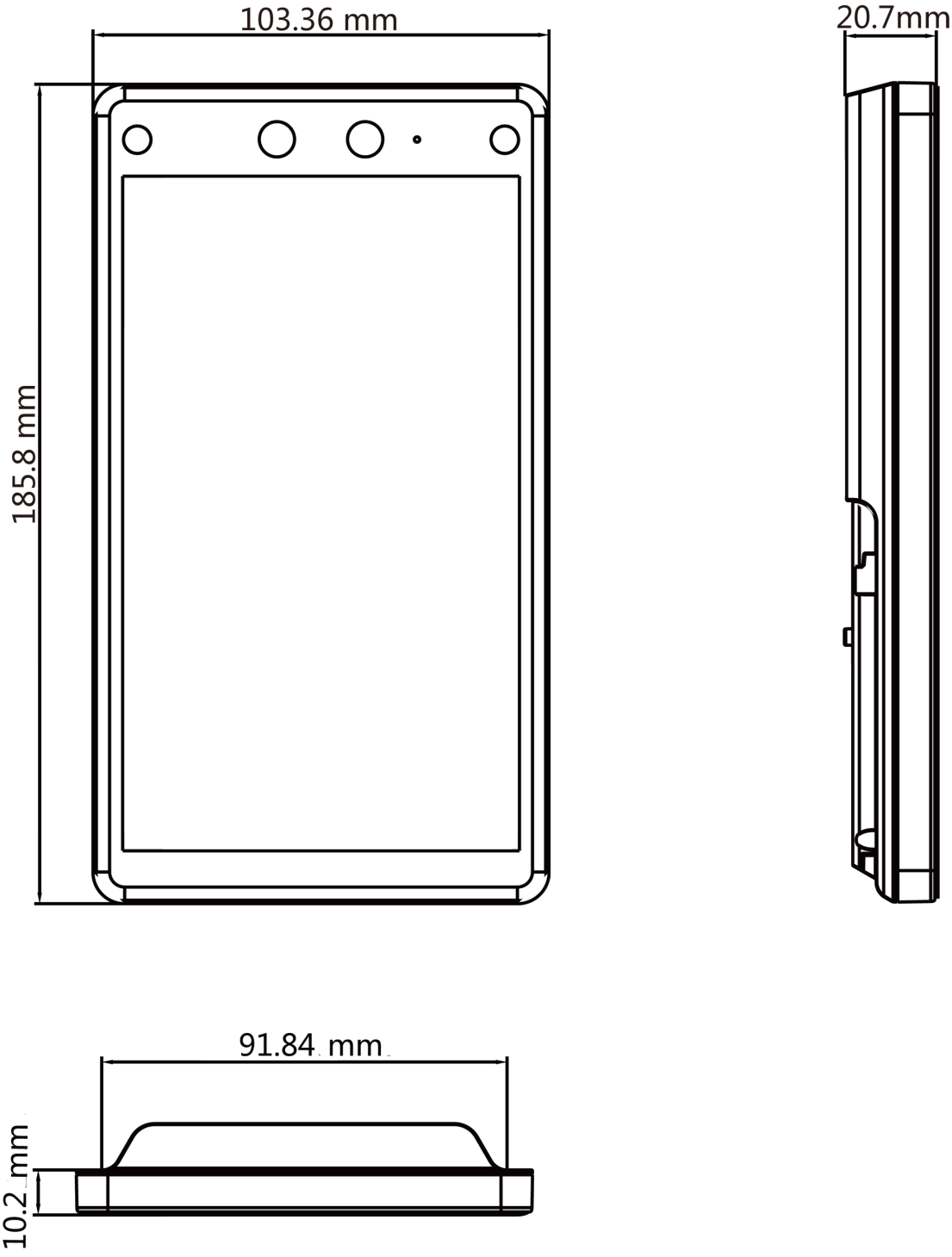


3.Avoid backlight, direct and indirect sunlight



Backlight | Direct Sunlight | Direct Sunlight through Window | Indirect Light through Window | Close to Light

Appendix C. Dimension



Appendix D. Communication Matrix and Device Command

Communication Matrix

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

Figure D-1 QR Code of Communication Matrix

Device Command

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

Figure D-2 Device Command


See Far, Go Further