DS-K1T981 Series Access Control Terminal

User Manual

Regulatory Information

FCC Information

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

EU Conformity Statement

CE

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

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



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



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

Safety Instruction

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

The precaution measure is divided into Dangers and Cautions:

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

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

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

⚠ Danger:

- All the electronic operation should be strictly compliance with the electrical safety regulations, fire prevention regulations and other related regulations in your local region.
- Please use the power adapter, which is provided by normal company. This equipment is intended to be supplied from the Class 2 surge protected power source rated DC 12V, 3A.
- Do not connect several devices to one power adapter as adapter overload may cause over-heat or fire hazard.
- Please make sure that the power has been disconnected before you wire, install or dismantle the device.
- When the product is installed on wall or ceiling, the device shall be firmly fixed.
- If smoke, odors or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.
- Do not ingest battery, Chemical Burn Hazard.
  This product contains a coin/button cell battery. If the coin/button cell battery is swallowed, it can cause severe internal burns in just 2 hours and can lead to death.
  Keep new and used batteries away from children. If the battery compartment does not close securely, stop using the product and keep it away from children. If you think batteries might have been swallowed or placed inside any part of the body, seek immediate medical attention.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the device yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)

⚠ Cautions:

- Do not drop the device or subject it to physical shock, and do not expose it to high electromagnetism radiation. Avoid the equipment installation on vibrations surface or places subject to shock (ignorance can cause equipment damage).
- Do not place the device in extremely hot (refer to the specification of the device for the detailed operating temperature), cold, dusty or damp locations, and do not expose it to high electromagnetic radiation.
- The device cover for indoor use shall be kept from rain and moisture.
- Exposing the equipment to direct sun light, low ventilation or heat source such as heater or radiator is forbidden (ignorance can cause fire danger).
- Do not aim the device at the sun or extra bright places. A blooming or smear may occur otherwise (which is not a malfunction however), and affecting the endurance of sensor at the same time.
- Please use the provided glove when open up the device cover, avoid direct contact with the device cover, because the acidic sweat of the fingers may erode the surface coating of the device cover.
- Please use a soft and dry cloth when clean inside and outside surfaces of the device cover, do not use alkaline detergents.
- Please keep all wrappers after unpack them for future use. In case of any failure occurred, you need to return the device to the factory with the original wrapper. Transportation without the original wrapper may result in damage on the device and lead to additional costs.
- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.
- Biometric recognition products are not completely applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.
- Working temperature: -30 °C to +60 °C
- Indoor and outdoor use. If installing the device indoors, the device should be at least 2 meters away from the light, and at least 3 meters away from the window or the door. If installing the device outdoors, you should apply Sililcone sealant among the cable wiring area to keep the raindrop from entering.
- Protection level: IP65

Available Models

Product Name	Model
Access Control Terminal	DS-K1T981M
	DS-K1T981MF

Use only power supplies listed in the user instructions:

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

Contents

Chapter 1 Appearance 1

Chapter 2 Installation 3

2.1 Installation Environment 3

2.2 Flush Mounting with Gang Box 3

2.3 Surface Mounting 7

2.4 Mount With Bracket 12

2.4.1 Preparation before Mounting with Bracket 12

2.4.2 Bracket Mounting 14

2.5 Mount With Cylinder Bracket 15

2.5.1 Preparation before Mounting with Bracket 15

Chapter 3 Wiring 20

3.1 Terminal Description 20

3.2 Wire Normal Device 22

3.3 Wire Secure Door Control Unit 23

3.4 Wire Fire Module 24

3.4.1 Wiring Diagram of Door Open When Powering Off 24

3.4.2 Wiring Diagram of Door Locked When Powering Off 26

Chapter 4 Activation 28

4.1 Activate via Device 28

4.2 Activate via Web Browser 30

4.3 Activate via SADP 31

4.4 Activate Device via iVMS-4200 Client Software 32

Chapter 5 Quick Operation 34

5.1 Select Language 34

5.2 Set Password Change Type 36

5.3 Set Application Mode 36

5.4 Installation Angle 38
5.5 Set Network Parameters 38
5.6 Access to Platform 40
5.7 Privacy Settings 42
5.8 Set Administrator 42
5.9 Authentication Page Instructions 43
Chapter 6 Basic Operation 45
6.1 Login 45
6.1.1 Login by Administrator 45
6.1.2 Login by Activation Password 48
6.1.3 Forgot Password 49
6.2 Communication Settings 50
6.2.1 Set Wired Network Parameters 50
6.2.2 Set Wi-Fi Parameters 51
6.2.3 Set RS-485 Parameters 53
6.2.4 Set Wiegand Parameters 54
6.2.5 Set ISUP Parameters 54
6.2.6 Platform Access 56
6.3 Person Management 56
6.3.1 Add Administrator 57
6.3.2 Import and Export Face and Person Data in Batch via Device 58
6.3.3 Add Face Picture 60
6.3.4 Add Card 63
6.3.5 Add Fingerprint 64
6.3.6 View PIN code 65
6.3.7 Add Iris 65
6.3.8 Set Person Type via Device 68
6.3.9 Set Authentication Mode 70

6.3.10 Search and Edit Person 70
6.4 Data Management 71
6.4.1 Delete Data 71
6.4.2 Import Data 71
6.4.3 Export Data 72
6.5 Person Authentication 72
6.5.1 Authenticate via Single Credential 72
6.5.2 Authenticate via Multiple Credential 73
6.6 Basic Settings 74
6.6.1 Enable/Disable Voice Prompt via Device 75
6.6.2 Set Device Time via Device 75
6.6.3 Set Sleep Duration via Device 75
6.6.4 Select Language 75
6.6.5 Set Installation Angle 75
6.6.6 Set Device Number via Device 76
6.6.7 Set Privacy Parameters via Device 76
6.6.8 Set Video Standard 77
6.7 Set Face Parameters 77
6.7.1 Set Application Mode 77
6.7.2 Set Face Liveness Level via Device 77
6.7.3 Set Recognition Distance via Device 78
6.7.4 Set Face Recognition Interval via Device 78
6.7.5 Set Wide Dynamic 78
6.7.6 Set Face 1:N Security Level via Device 78
6.7.7 Set Face 1:1 Security Level via Device 79
6.7.8 Enable/Disable ECO Mode via Device 79
6.7.9 Enable/Disable Hard Hat Detection via Device 79
6.7.10 Enable/Disable Mask Detection via Device 80

6.7.11 Iris Settings 81
6.8 Access Control Settings 82
6.8.1 Set Terminal Authentication Mode via Device 83
6.8.2 Set Reader Authentication Mode via Device 84
6.8.3 Enable/Disable NFC Card 84
6.8.4 Enable/Disable M1 Card 85
6.8.5 Remote Authentication 85
6.8.6 Set Authentication Interval via Device 85
6.8.7 Door Parameter Configuration 85
6.9 Platform Attendance 86
6.9.1 Disable Attendance Mode via Device 86
6.9.2 Set Manual Attendance via Device 87
6.9.3 Set Auto Attendance via Device 88
6.9.4 Set Manual and Auto Attendance via Device 89
6.10 Preference Settings 91
6.10.1 Set Shortcut Key via Device 92
6.10.2 Theme 93
6.11 System Maintenance 93
6.11.1 View System Information 94
6.11.2 View Device Capacity via Device 94
6.11.3 Upgrade 95
6.11.4 Restore Settings 95
6.12 Video Intercom 96
6.12.1 Call Client Software from Device 96
6.12.2 Call Center from Device 97
6.12.3 Call Device from Client Software 97
6.12.4 Call Room from Device 98
6.12.5 Call Mobile Client from Device 98

Chapter 7 Operation via Web Browser 99
7.1 Login 99
7.2 Forget Password 99
7.3 Download Web Plug-In 99
7.4 Help 100
7.4.1 Open Source Software Licenses 100
7.4.2 View Online Help Document 100
7.5 Logout 100
7.6 Quick Operation via Web Browser 100
7.6.1 Change Password 100
7.6.2 Select Language 101
7.6.3 Time Settings 101
7.6.4 Environment Settings 102
7.6.5 Privacy Settings 102
7.6.6 Administrator Settings 103
7.6.7 No. and System Network 104
7.7 Person Management 105
7.8 Access Control Management 107
7.8.1 Overview 107
7.8.2 Search Event 108
7.8.3 Door Parameter Configuration 108
7.8.4 Authentication Settings 111
7.8.5 Set Face Parameters 115
7.8.6 Card Settings 121
7.8.7 Set Working Mode via PC Web 123
7.8.8 Privacy Settings 123
7.8.9 Call Settings 125
7.9 System Configuration 127

7.9.1 Set Local Parameters 127
7.9.2 View Device Information via PC Web 128
7.9.3 Set Time 128
7.9.4 Change Administrator's Password 129
7.9.5 Account Security Settings via PC Web 130
7.9.6 View Device Arming/Disarming Information via PC Web 130
7.9.7 Network Settings 130
7.9.8 Set Video and Audio Parameters via PC Web 134
7.9.9 Image Parameter Settings 134
7.9.10 Alarm Settings via PC Web 135
7.9.11 Access Configuration 136
7.9.12 Time and Attendance Settings 138
7.10 Preference Settings 140
7.10.1 Set Sleep Time via PC Web 140
7.10.2 Customize Authentication Desk via PC Web 141
7.10.3 Set Notice Publication via PC Web 141
7.10.4 Set Prompt Schedule via PC Web 142
7.10.5 Customize Prompt Voice via PC Web 143
7.10.6 Set Authentication Result Text via PC Web 144
7.11 System and Maintenance 144
7.11.1 Reboot 144
7.11.2 Upgrade 144
7.11.3 Restoration 145
7.11.4 Export Device Parameters via PC Web 145
7.11.5 Import Device Parameters via PC Web 146
7.11.6 Device Debugging 146
7.11.7 View Log via PC Web 147
7.11.8 Security Management 147

7.11.9 Certificate Management 148
Chapter 8 Other Platforms to Configure 150
Appendix A. Legal Information 151
Appendix B. Symbol Conventions 153
Appendix C. Tips for Scanning Fingerprint 154
Appendix D. Tips When Collecting/Comparing Face Picture 156
Appendix E. Tips for Installation Environment 159
Appendix F. Dimension 160

Chapter 1 Appearance

Refer to the following contents for detailed information of the access control terminal:

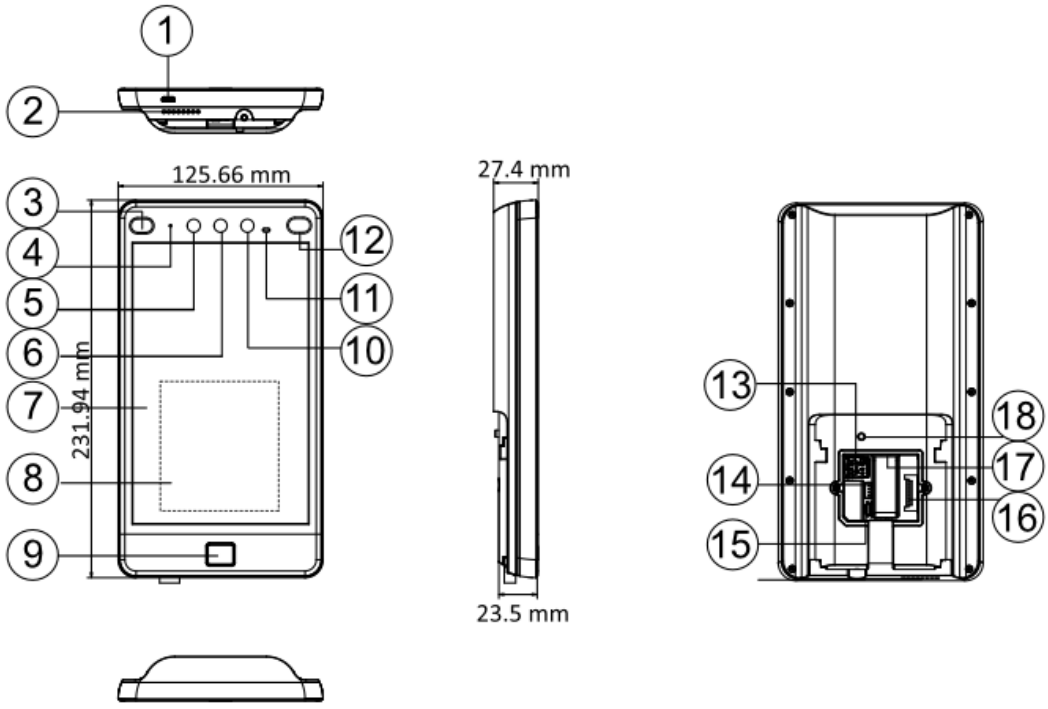


Figure 1-1 Access Control Terminal Diagram

Table 1-1 Description of Access Control Terminal

No.	Name
1	USB Interface
2	Loudspeaker
3	IR Light
4	MIC
5	Camera
6	Iris Camera
7	Touchscreen

No.	Name
8	Card Presenting Area
9	Fingerprint Recognition Area
10	Camera
11	TOF
12	IR Light
13	SIM Card Slot (Reserved)
14	USB Interface (Reserved)
15	Debugging Port (For debugging only)
16	Wiring Terminal
17	Network Interface
18	Tamper

Chapter 2 Installation

2.1 Installation Environment

- Install the device at least 2 meters away from the light, and at least 3 meters away from the window or the door.
- Make sure the environment illumination is more than 100 Lux.
- Indoor use.
- Avoid backlight, direct sunlight, and indirect sunlight.

Note

- The device doesn't support outdoor use.
- For details about installation environment, see *Tips for Installation Environment*.

2.2 Flush Mounting with Gang Box

Before You Start

Remove the back sheet of the device.

Steps

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

   Note

   Gang box is not supplied.

2. Secure the mounting plate on the gang box with 2 supplied screws (SC-KA4X22-SUS).

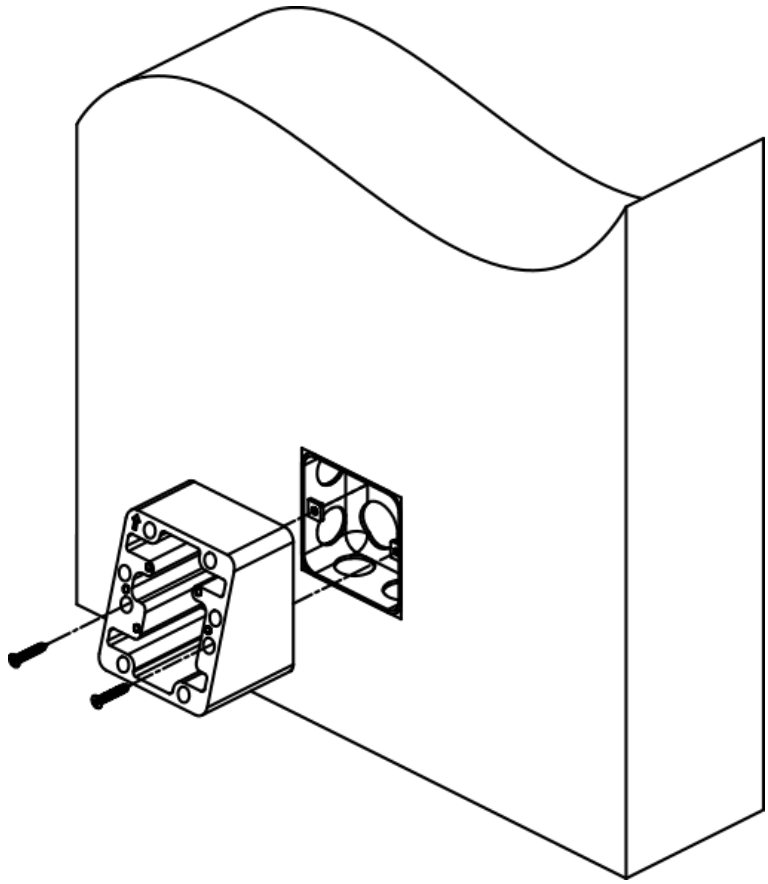


Figure 2-1 Install Gang Box

3. Secure the mounting plate on the bracket with 2 supplied screws (SC-K1M4X6-SUS).

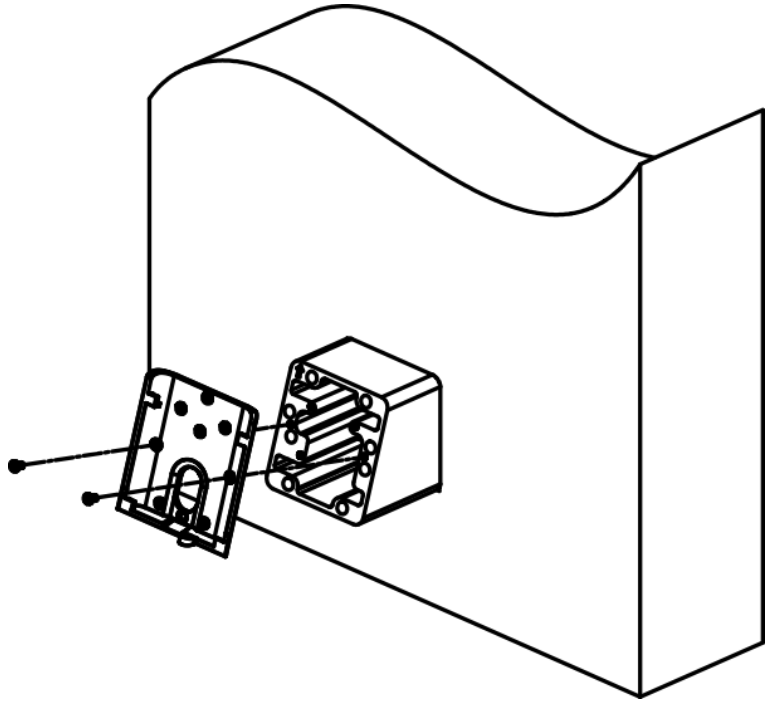


Figure 2-2 Install Mounting Plate

4. Route the cable through the cable hole, wire the cables and insert the cables in the gang box.

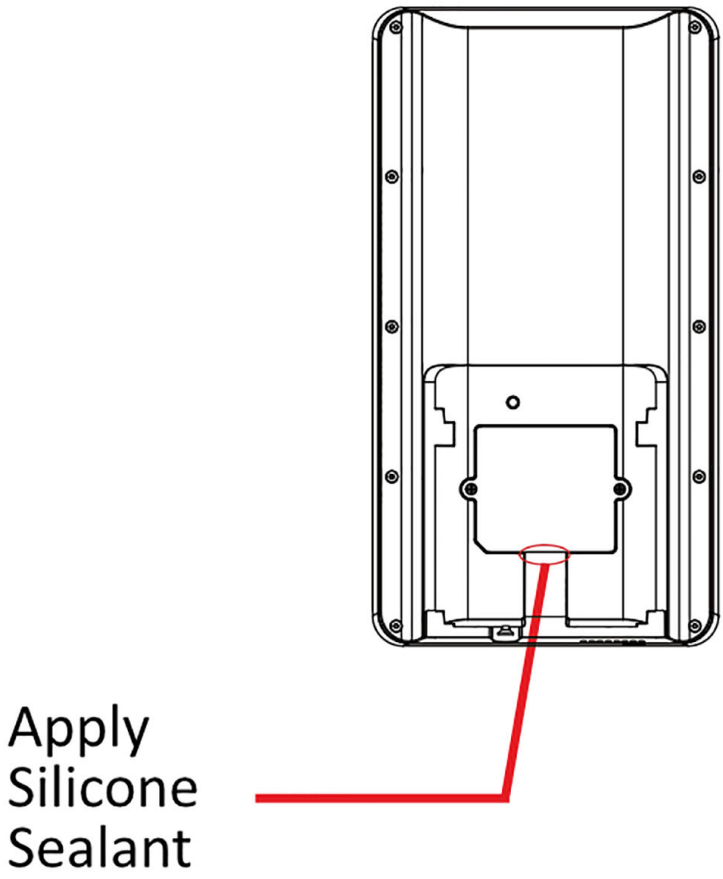


Figure 2-3 Apply Silicone Sealant

Note

Apply Silicone sealant among the cable wiring area to keep the raindrop from entering.

5. Align the device with the mounting plate, and secure the device on the mounting plate with 1 supplied screw (SC-KM3X6-T10-SUS).

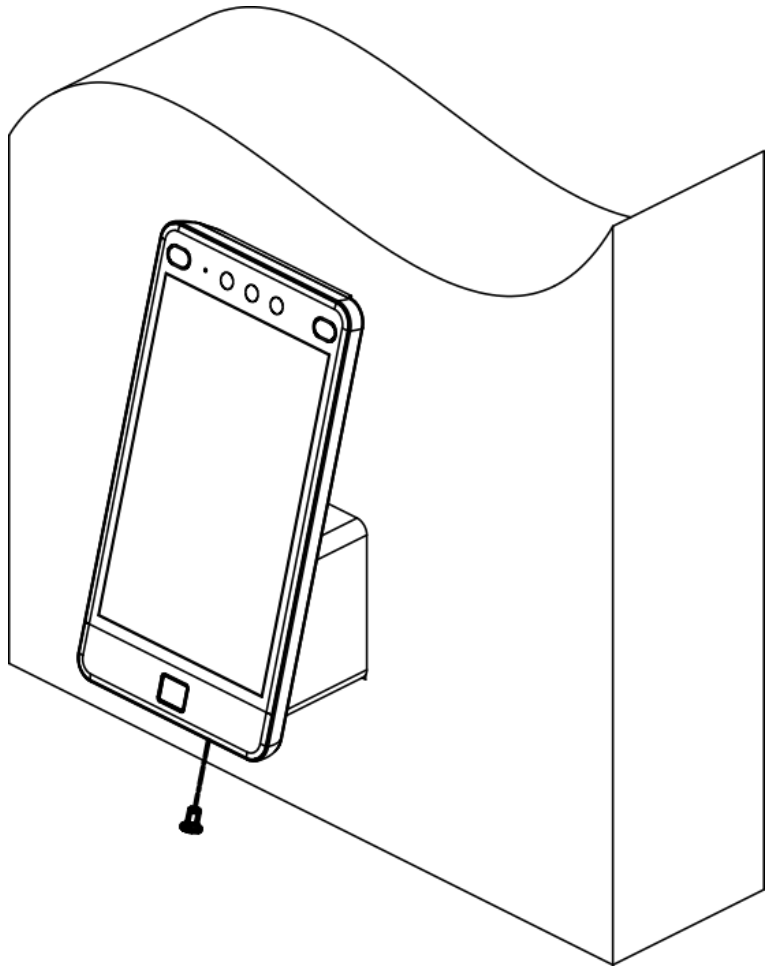


Figure 2-4 Secure Device

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

2.3 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.

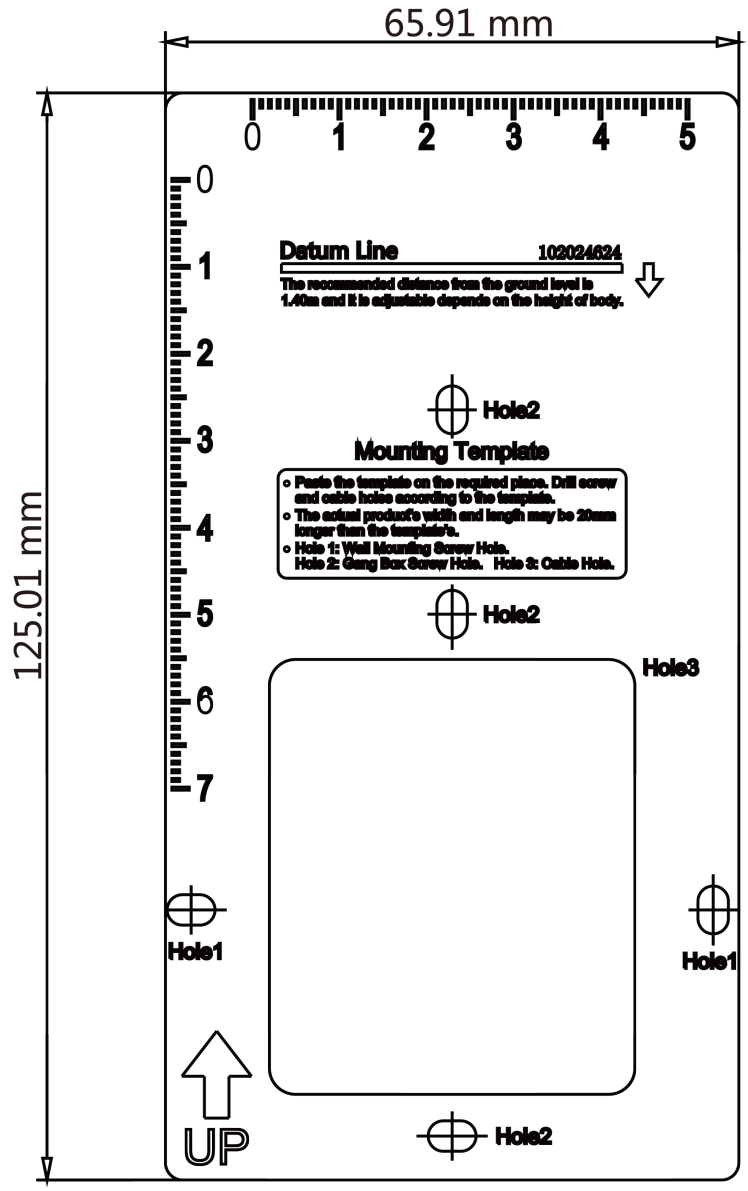


Figure 2-5 Mounting Template

2. Drill 2 holes on the wall or other surface according to the Hole 1 on the mounting template.

3. Insert the plastic sleeve of the provided expansion screw into the punched hole.

4. Install the mounting plate on the wall with the 2 supplied screws (SC-KA4×22-SUS).

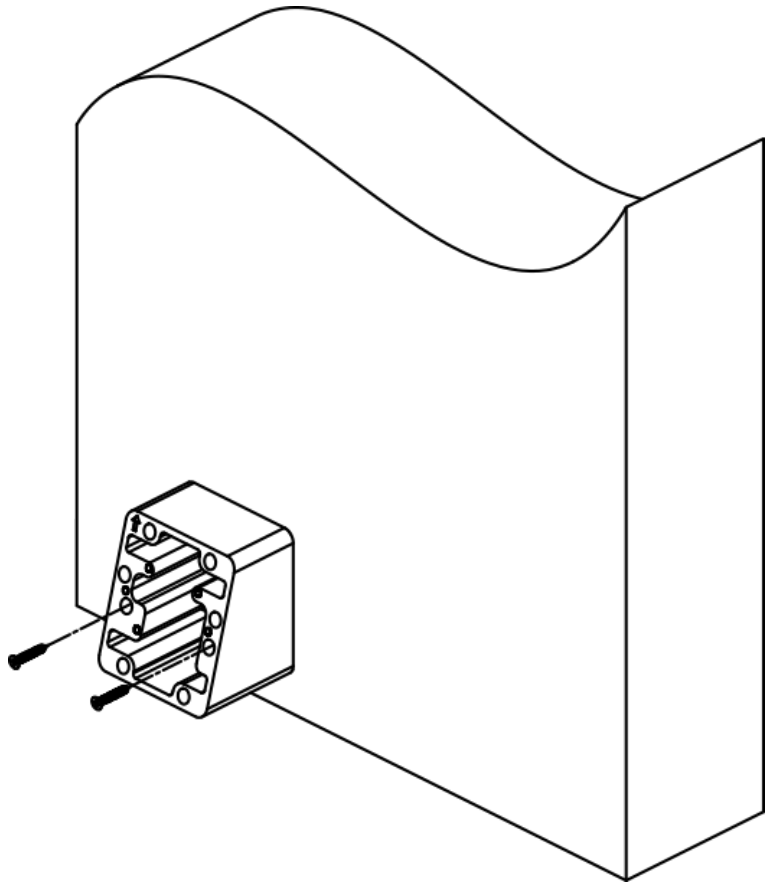


Figure 2-6 Install Bracket

5. Align the holes to the mounting plate and secure the mounting plate on the bracket with the 2 supplied screws (SC-K1M4×6-SUS).

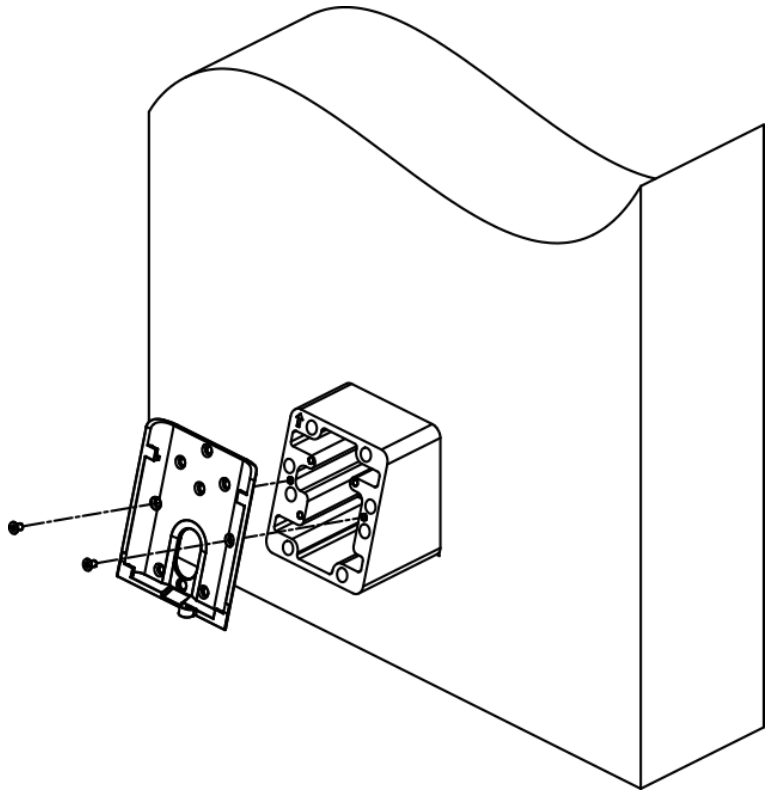


Figure 2-7 Install Mounting Plate

6. Route the cable through the cable hole, wire the cables and insert the cables.

Note

If the device is installed outdoor, you should apply silicone sealant to the wiring exit to avoid water from entering.

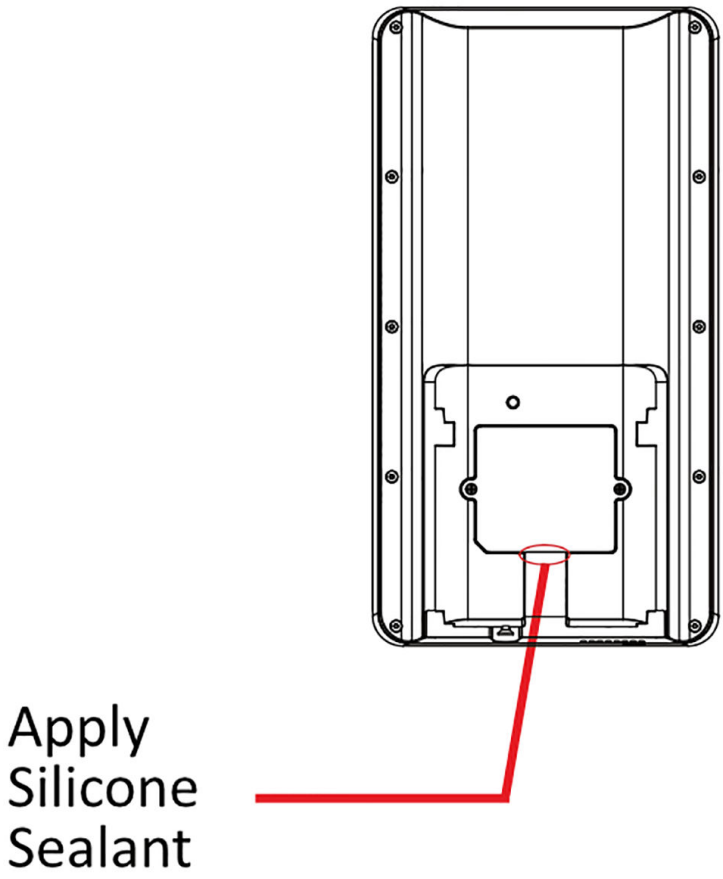


Figure 2-8 Apply Silicone Sealant

7. Align the device with the mounting plate and hang the device on the mounting plate.

8. Use 1 supplied screw (SC-KM3×6-T10-SUS) to secure the device and the mounting plate.

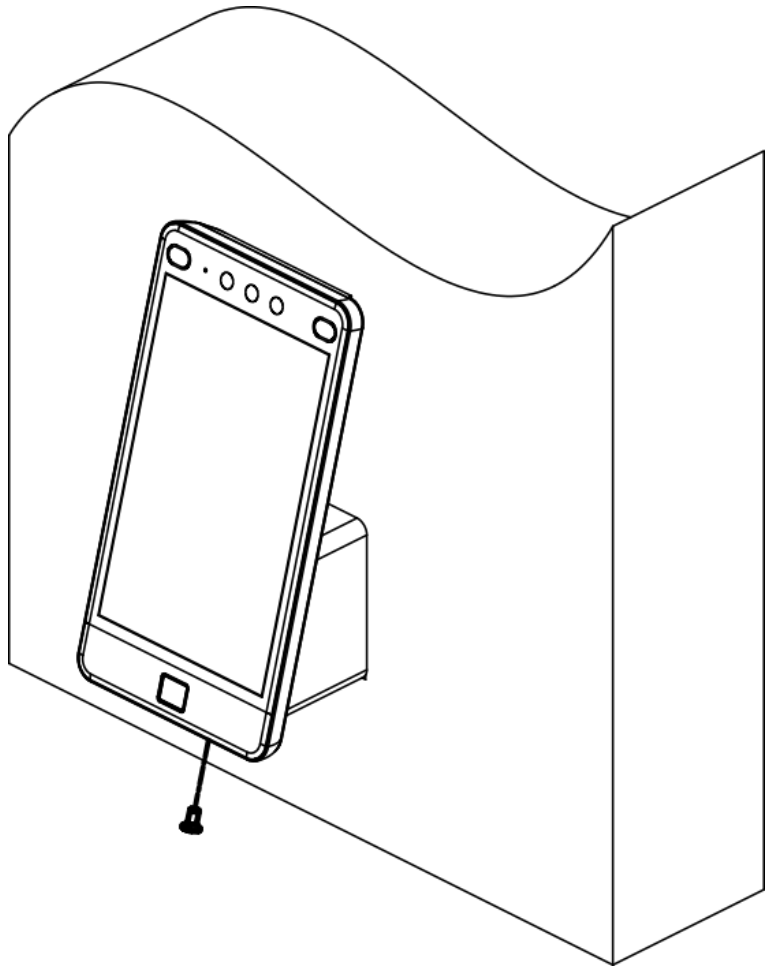


Figure 2-9 Secure Device

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

2.4 Mount With Bracket

2.4.1 Preparation before Mounting with Bracket

Steps

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

Note

Solder after pressing rivets to avoid water from entering.

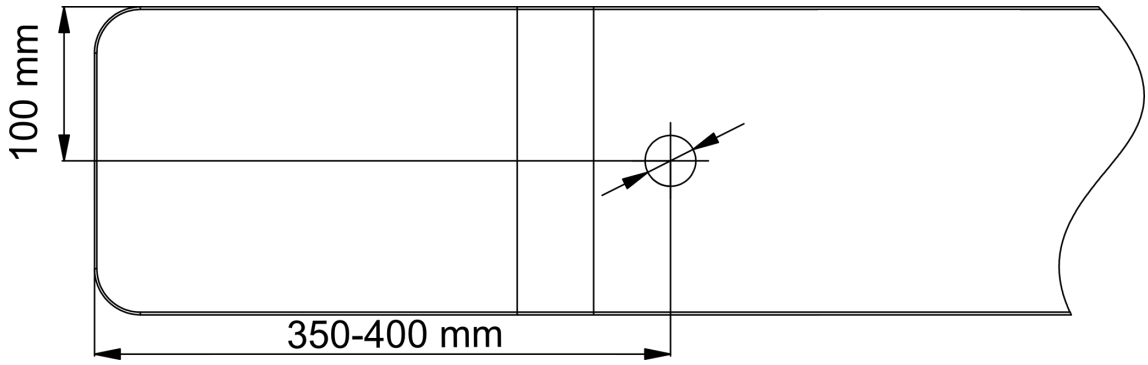


Figure 2-10 Drill Holes on Turnstile

2. If the installation angle needs to be 180° perpendicular to the body of the turnstile, the following operations are required.

1) Take off the 3 screws shown in the following figure.

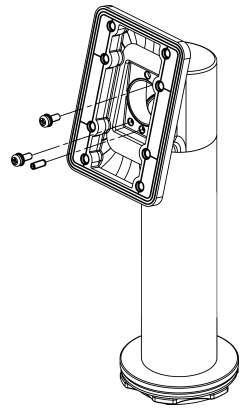


Figure 2-11 Take off Screws

2) Rotate the fixed part by 180°, and install the 3 screws back.

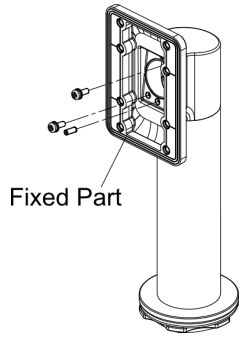


Figure 2-12 Rotate Fixed Part

2.4.2 Bracket Mounting

Steps

1. Install the mounting template on the bracket with 4 supplied screws (SC-K1M4×8-SUS).

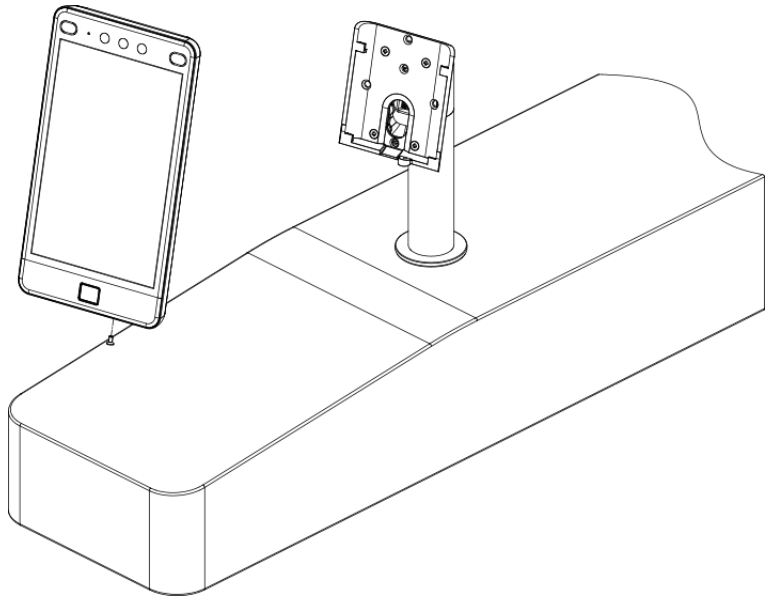


Figure 2-13 Install Mounting Template

2. Remove the back cover plate, route the cables through the cable hole, and connect them to the corresponding external devices' cables.
3. Install the back cover plate back, and install the device on the bracket with 1 supplied screw (SC-KM3×6-T10-SUS).

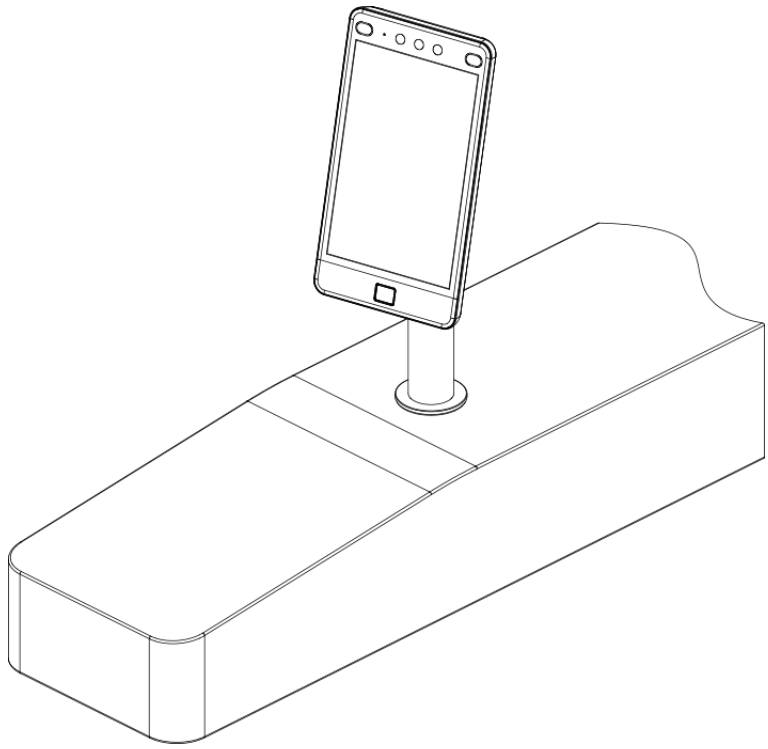


Figure 2-14 Install Device

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

2.5 Mount With Cylinder Bracket

2.5.1 Preparation before Mounting with Bracket

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

Steps

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

Note

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

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

Note

Solder after pressing rivets to avoid water from entering.

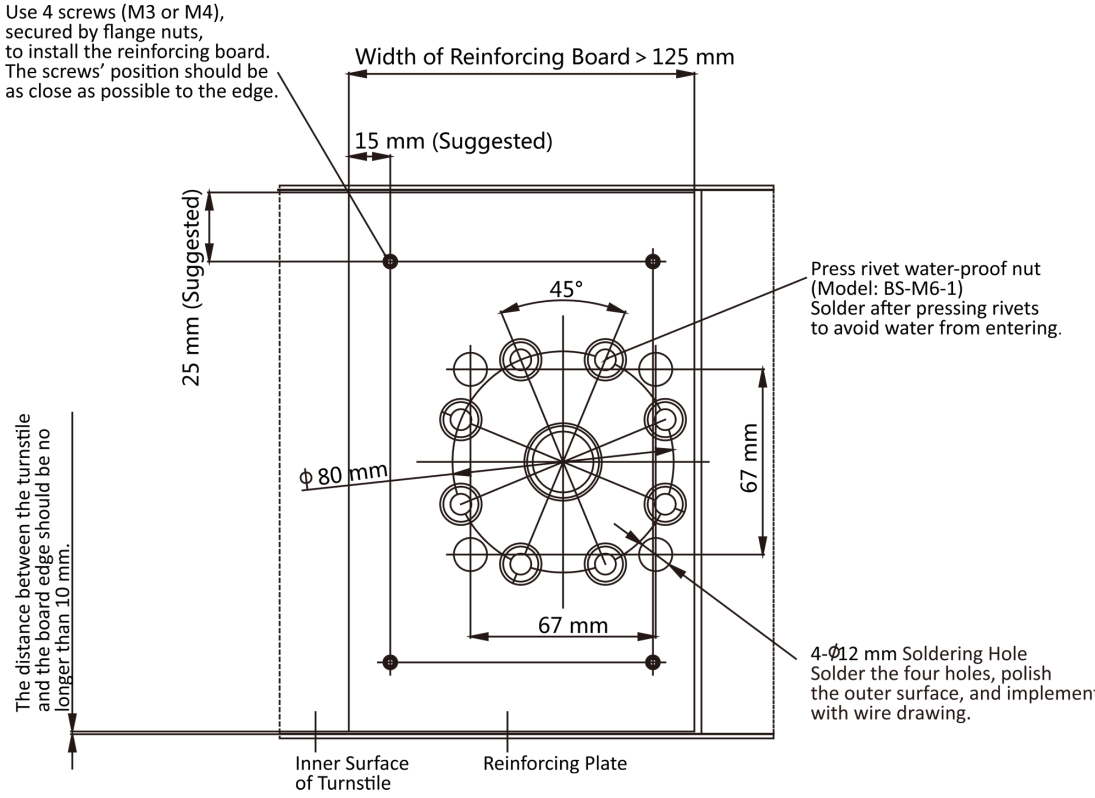


Figure 2-15 Drill Holes on Turnstile

3. Solder the other four holes, polish the surface, and implement wire drawing.

4. Solder circular tubes on the turnstile's inner surface to avoid water from entering.

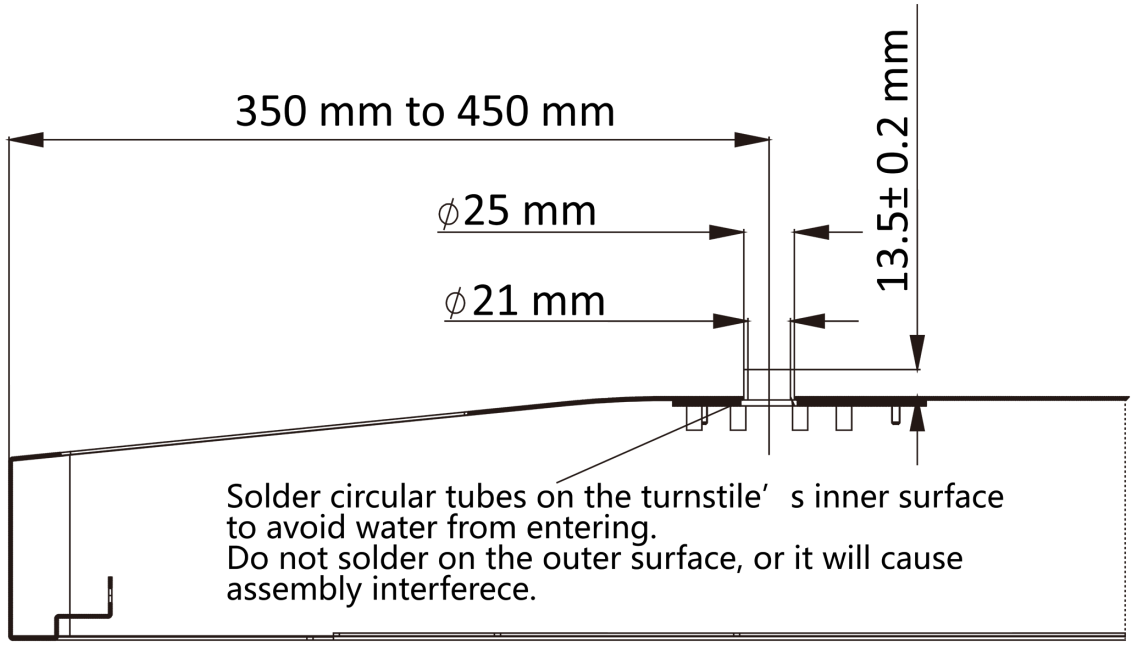


Figure 2-16 Solder Tubes

Cylinder Bracket Mounting

Steps

1. Install the base on the turnstile.
   1) Align the hole on the turnstile and place the base on the turnstile.
   2) Rotate the base to the acquired place and make sure the device will face a correct direction.
   3) Secure the base with 4 SC-OM6×12-H-SUS screws.

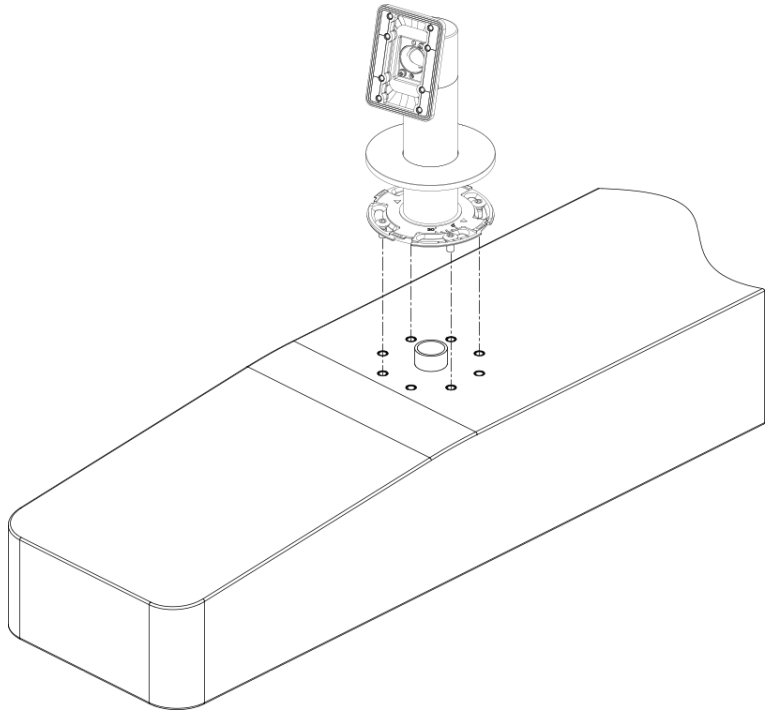


Figure 2-17 Install Base

2. Fix the mounting plate into the bracket by 4 SC-K1M4×8-SUS screws.

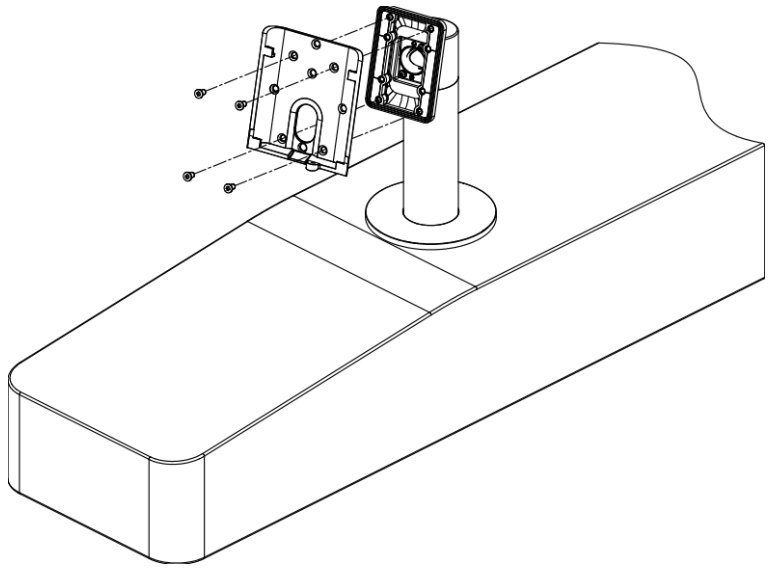


Figure 2-18 Fix Mounting Plate

3. Route the cables through the cable hole on the turnstile.

4. Fix the face recognition terminal into the mounting plate with 1 SC-KM3×6-T10-SUS screw.

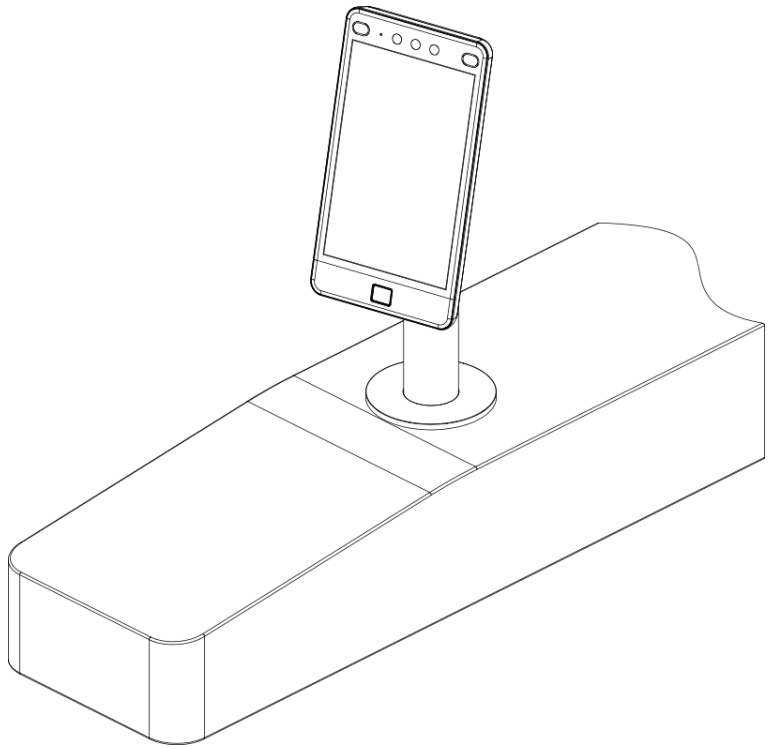


Figure 2-19 Fix Mounting Plate

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

Chapter 3 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 access control 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.

3.1 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:

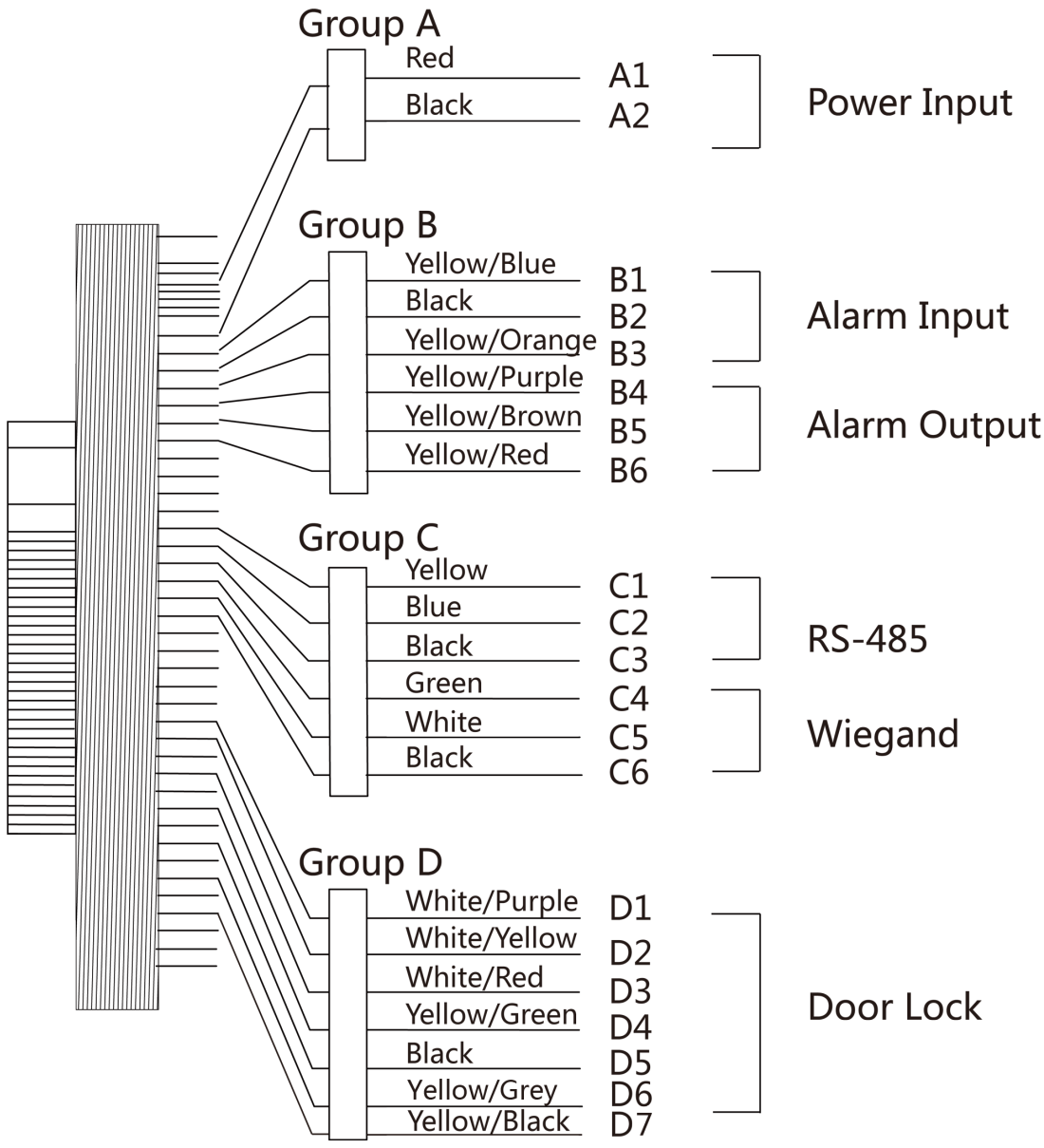


Figure 3-1 Terminal Diagram

The descriptions of the terminals are as follows:

Table 3-1 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

3.2 Wire Normal Device

You can connect the terminal with normal peripherals.

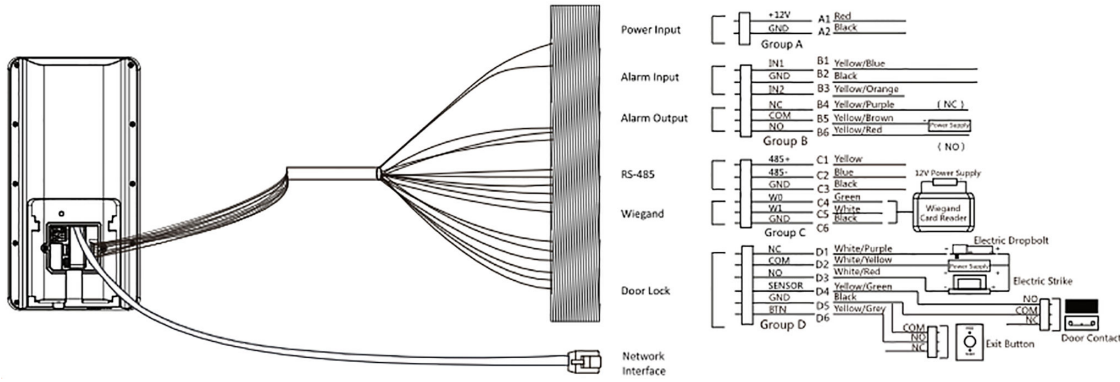


Figure 3-2 Device Wiring

Note

- 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.

3.3 Wire Secure Door Control Unit

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

The wiring diagram is as follows.

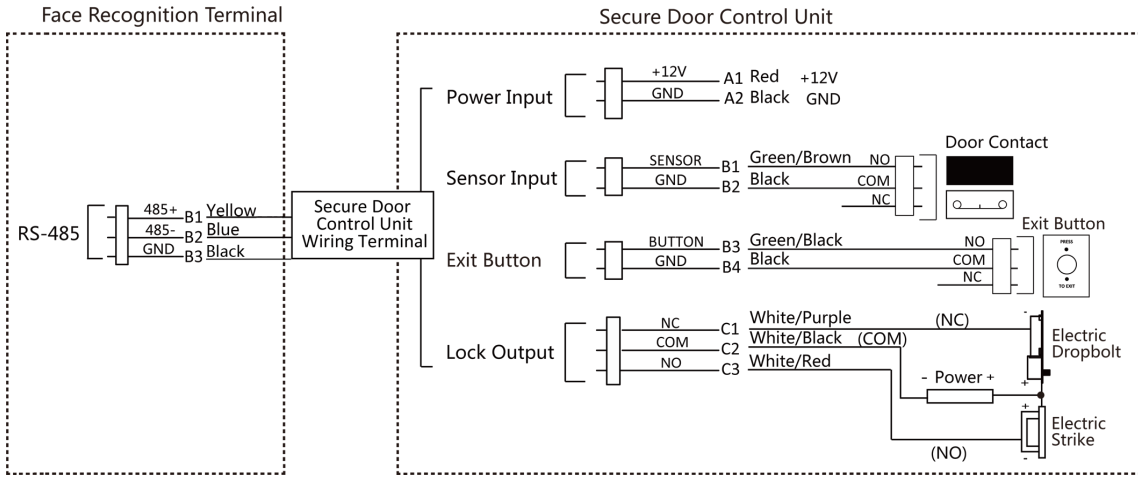


Figure 3-3 Secure Door Control Unit Wiring

Note

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

3.4 Wire Fire Module

3.4.1 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.

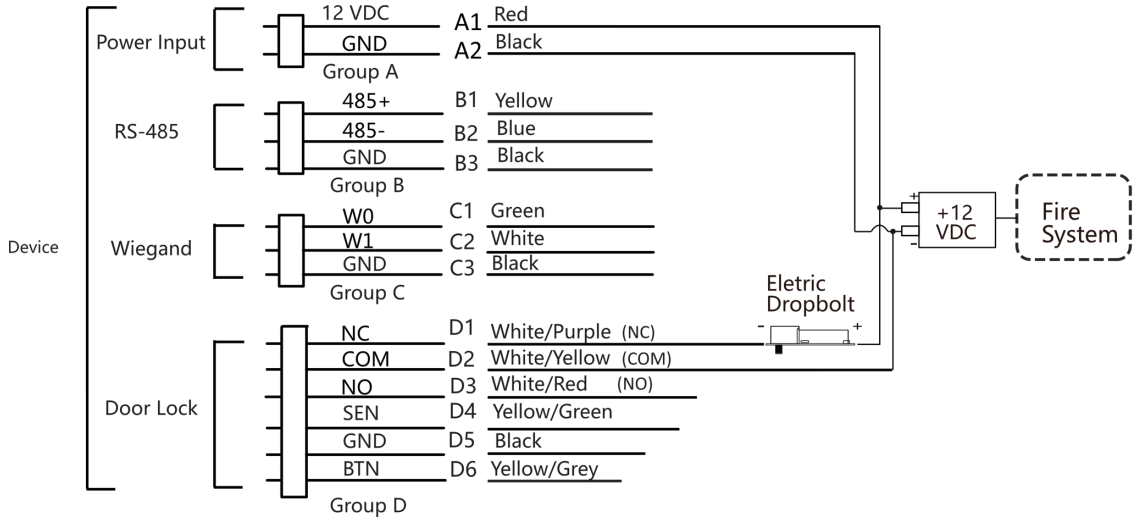


Figure 3-4 Wire Device

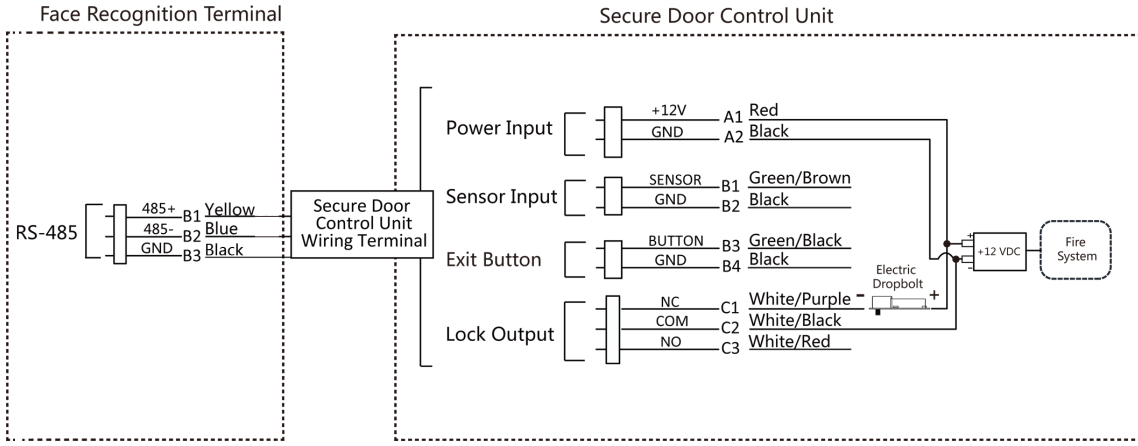


Figure 3-5 Wire Secure Door Control Unit

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.

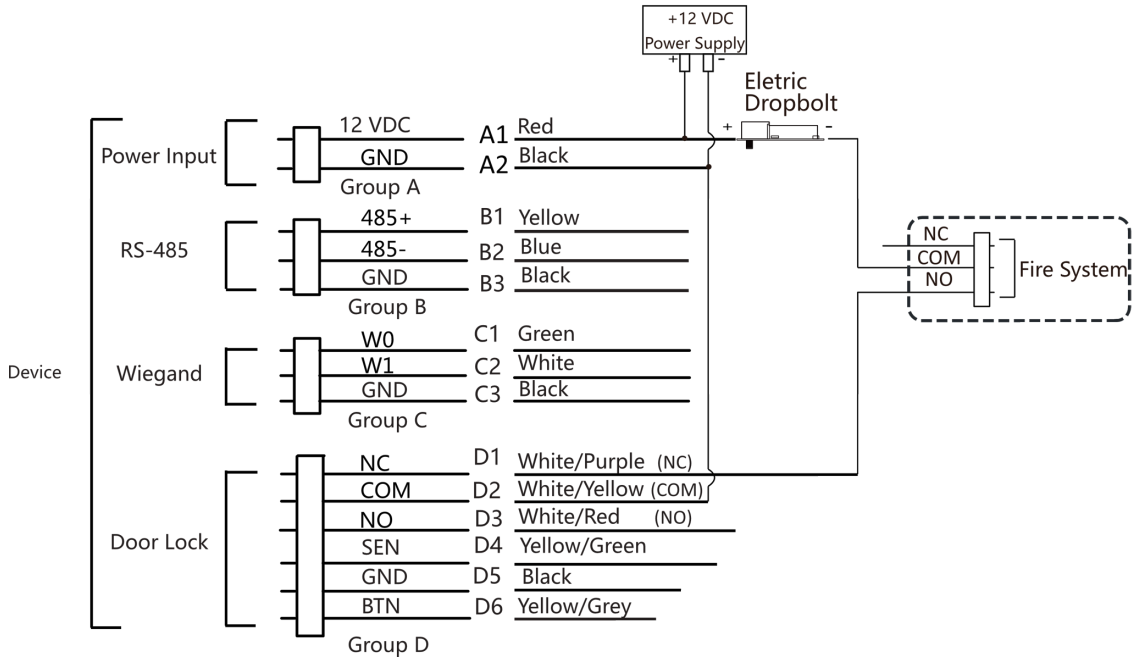


Figure 3-6 Wiring Device

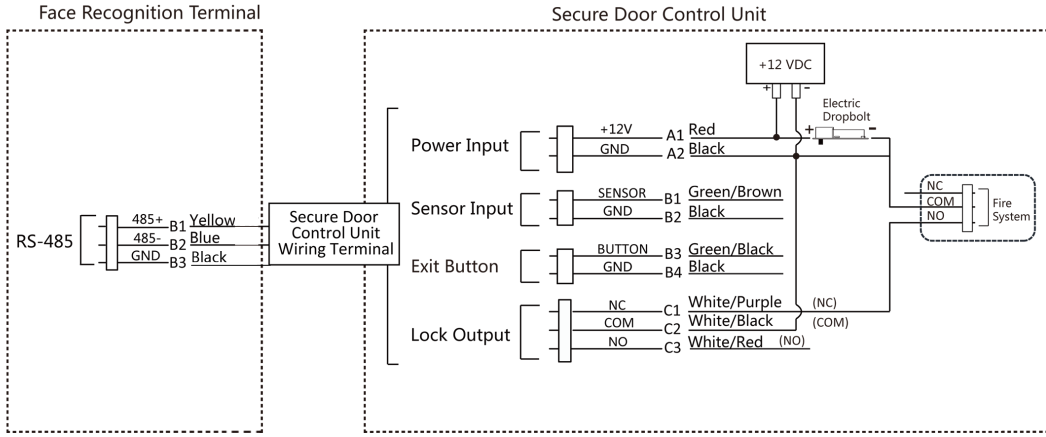


Figure 3-7 Wiring Secure Door Control Unit

3.4.2 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.

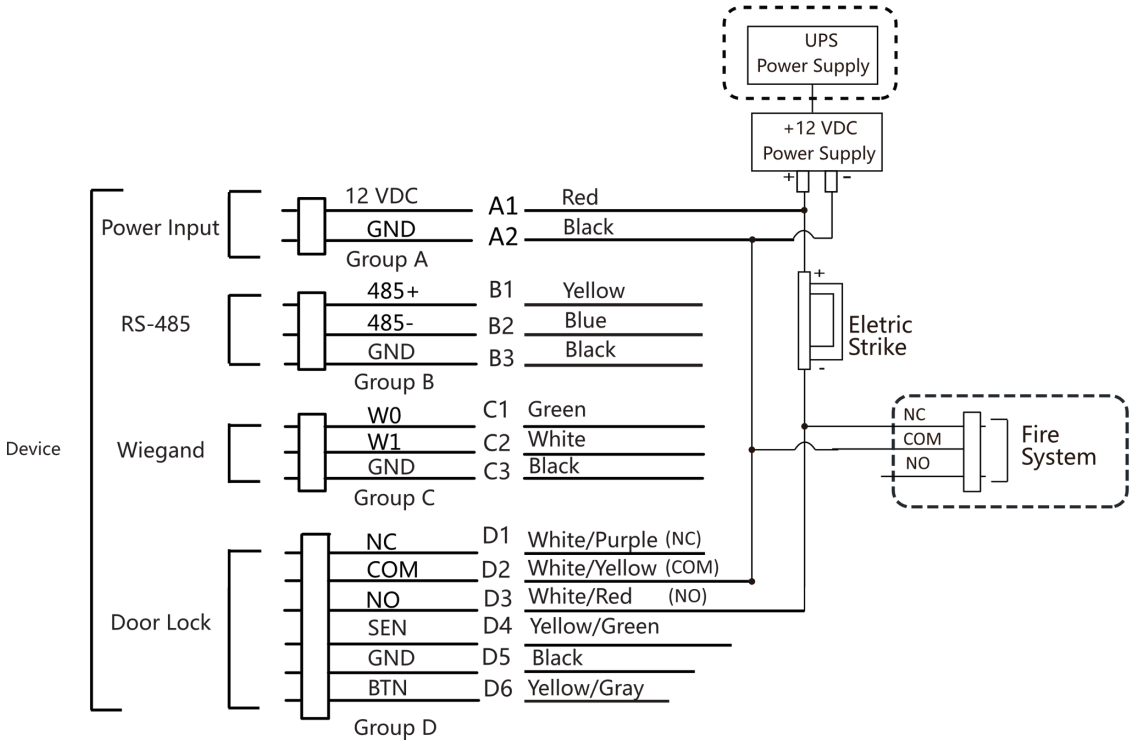


Figure 3-8 Device Wiring

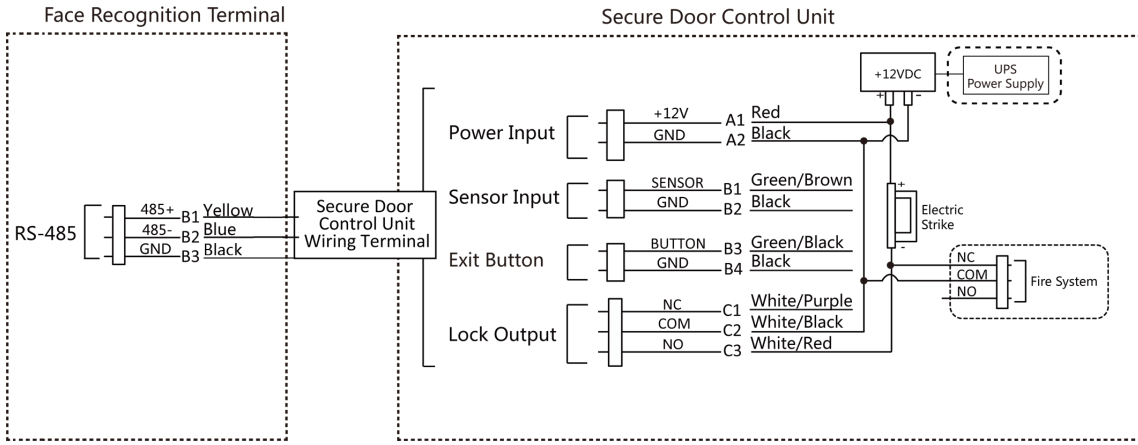


Figure 3-9 Wiring Diagram

Chapter 4 Activation

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

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

The default values of the device are as follows:

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

4.1 Activate via Device

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

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

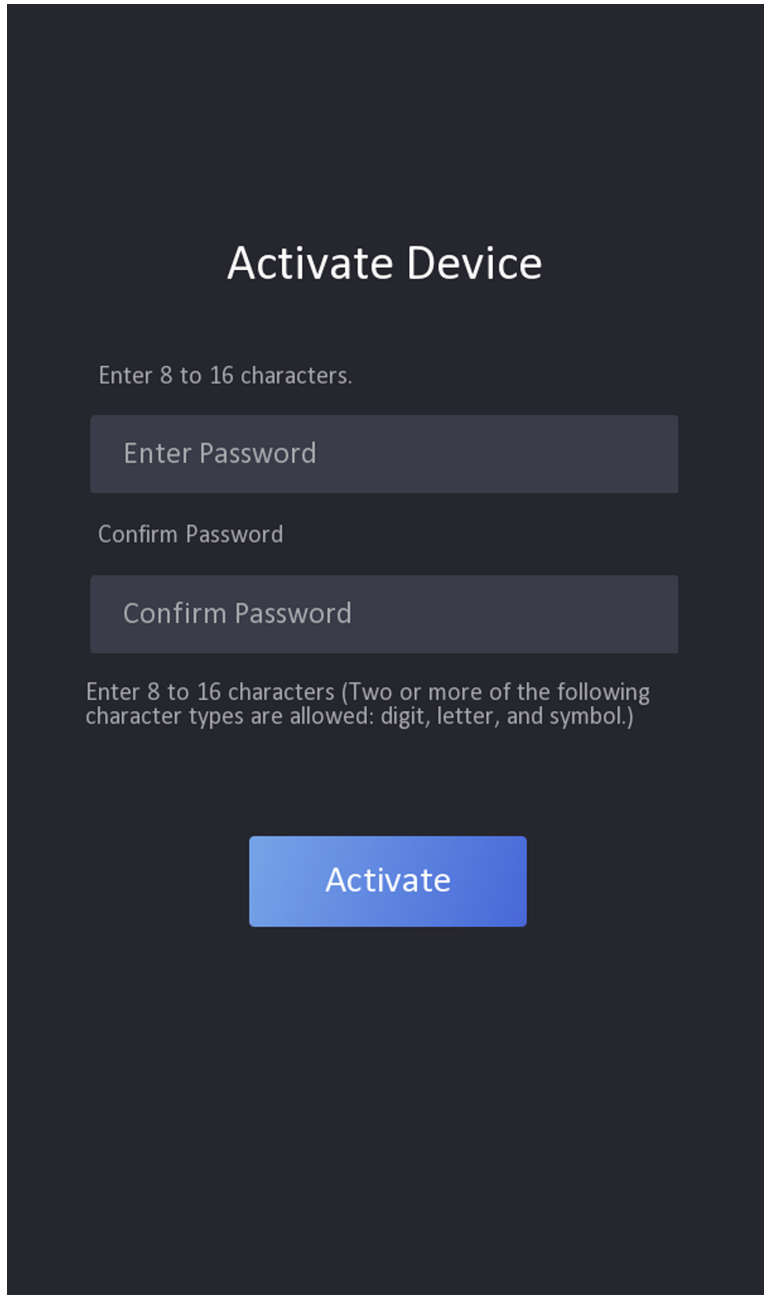


Figure 4-1 Activation Page

Caution

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

characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.
- Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.
- Do not contain following characters in the password: the user name, 123, admin (case-insensitive), 4 or more continuously increasing or decreasing digits, or 4 or more consecutively repeated characters.
- Password cannot contain words such as hik, hkws, and hikvision (case insensitive).

4.2 Activate via Web Browser

You can activate the device via the web browser.

Steps

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

   Note

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

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

   Caution

   - 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 service provider and/or end-user.
   - Do not contain following characters in the password: the user name, 123, admin (case-insensitive), 4 or more continuously increasing or decreasing digits, or 4 or more consecutively repeated characters.
   - Password cannot contain words such as hik, hkws, and hikvision (case insensitive).

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

4.3 Activate via SADP

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

Before You Start

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

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

Steps

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

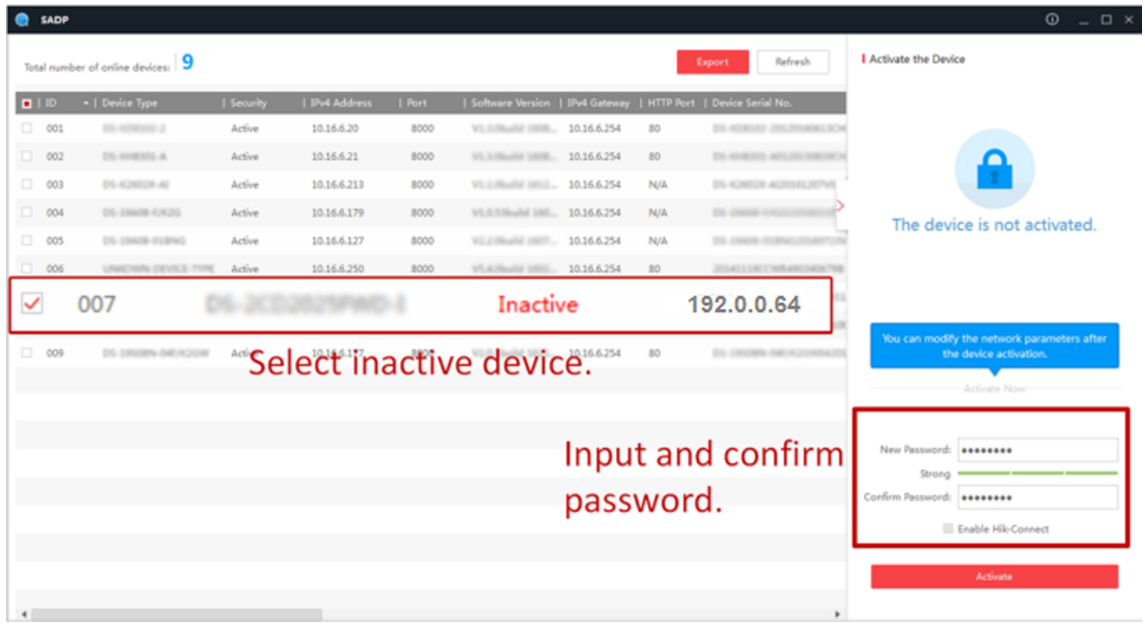
Caution

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

Note

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

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



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

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

4.4 Activate Device via iVMS-4200 Client Software

For some devices, you are required to create the password to activate them before they can be added to the iVMS-4200 software and work properly.

Steps

Note

This function should be supported by the device.

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

   The searched online devices are displayed in the list.
4. Check the device status (shown on **Security Level** column) and select an inactive device.
5. Click **Activate** to open the Activation dialog.
6. Create a password in the password field, and confirm the password.

Caution

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

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

Note

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

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

Chapter 5 Quick Operation

5.1 Select Language

You can select a language for the device system.

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

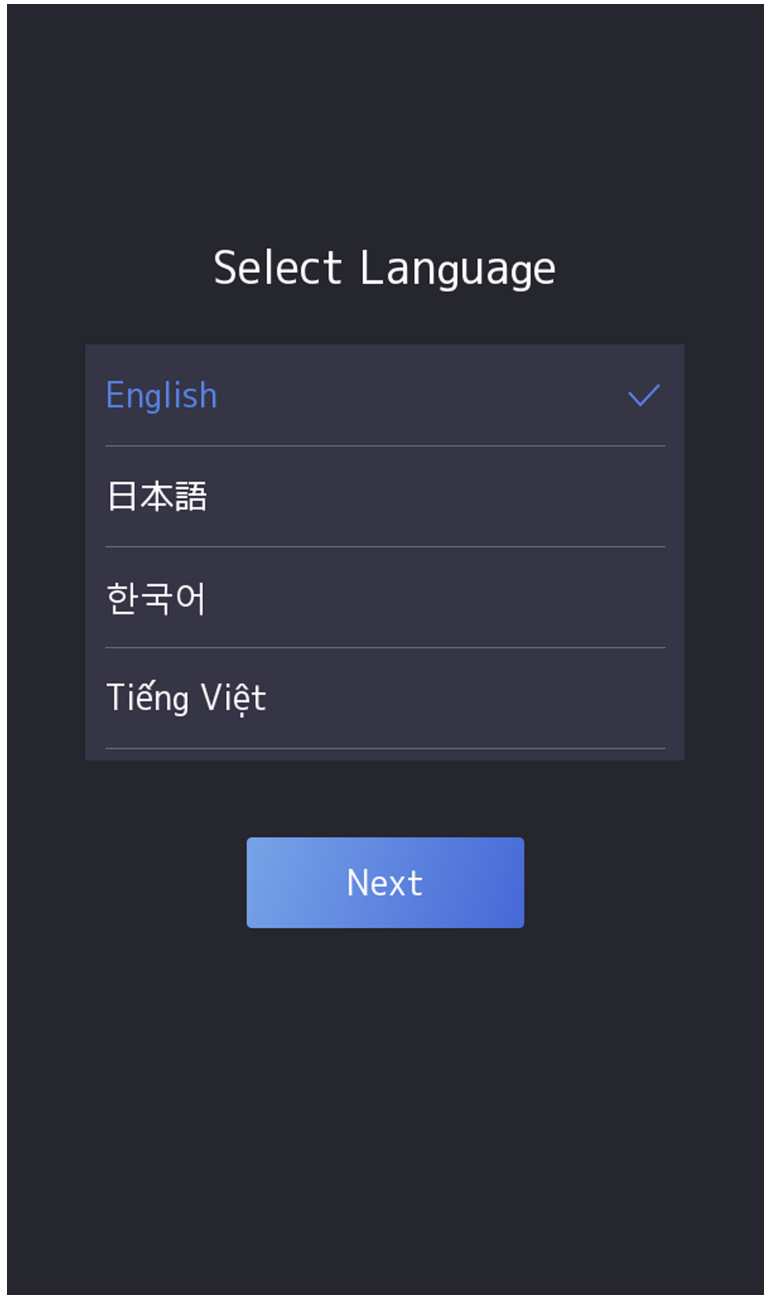


Figure 5-1 Select System Language

By default, the system language is English.

Note

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

5.2 Set Password Change Type

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**.

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. Tap **Next**.

Note

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

5.3 Set Application Mode

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

Steps

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

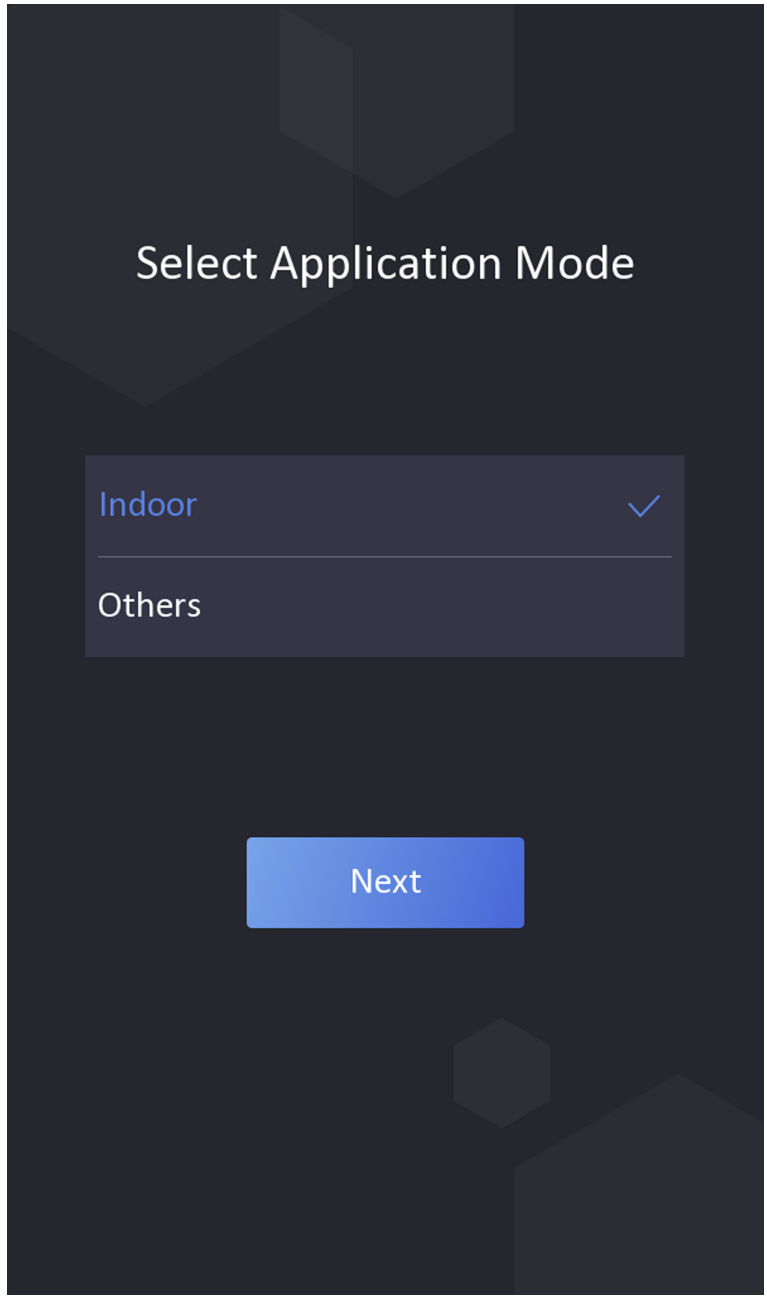


Figure 5-2 Welcome Page

2. Tap **OK** to save.

Note

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

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

5.4 Installation Angle

Select the installation angle according to your actual needs.

5.5 Set Network Parameters

You can set the network for the device.

Steps

Note

Parts of the device models supports wi-fi function. Refers to the actual device for details.

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

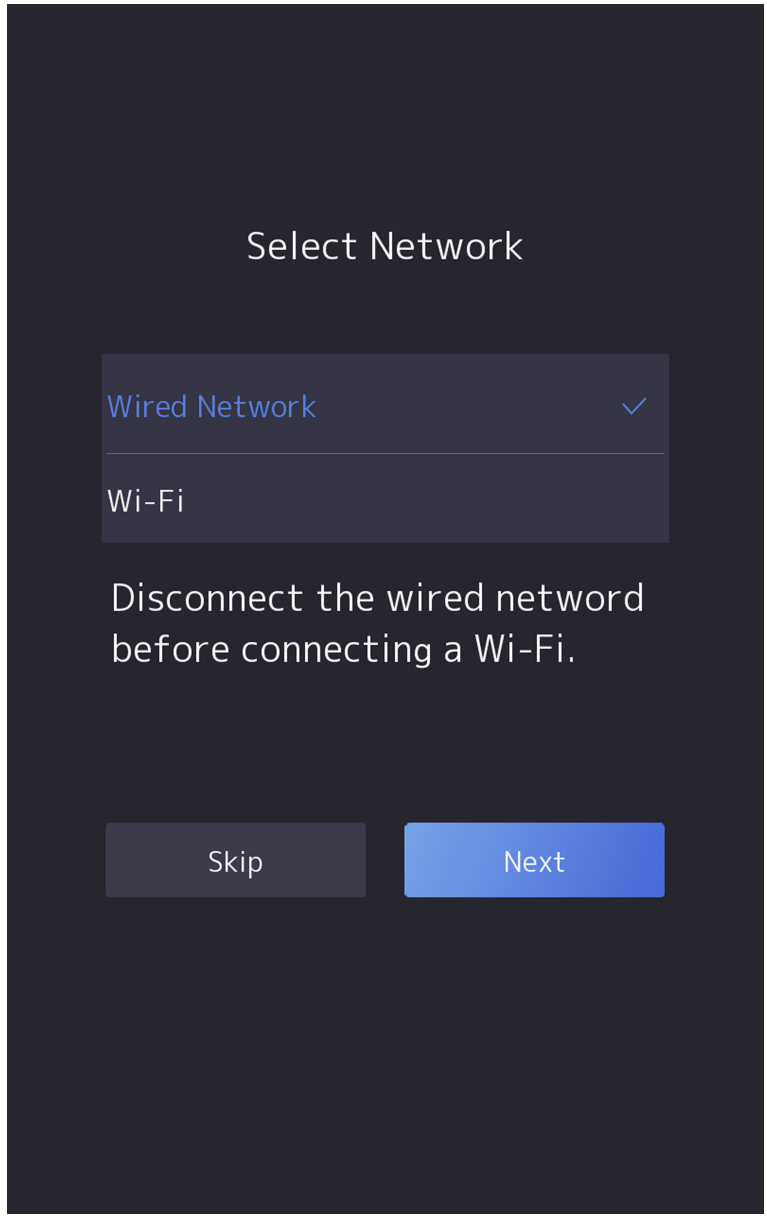


Figure 5-3 Select Network

Note

Disconnect the wired network before connecting a Wi-Fi.

2. Tap **Next**.

Wired Network

Note

Make sure the device has connected to a network.

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

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

Wi-Fi

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

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

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

5.6 Access to Platform

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

Steps

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

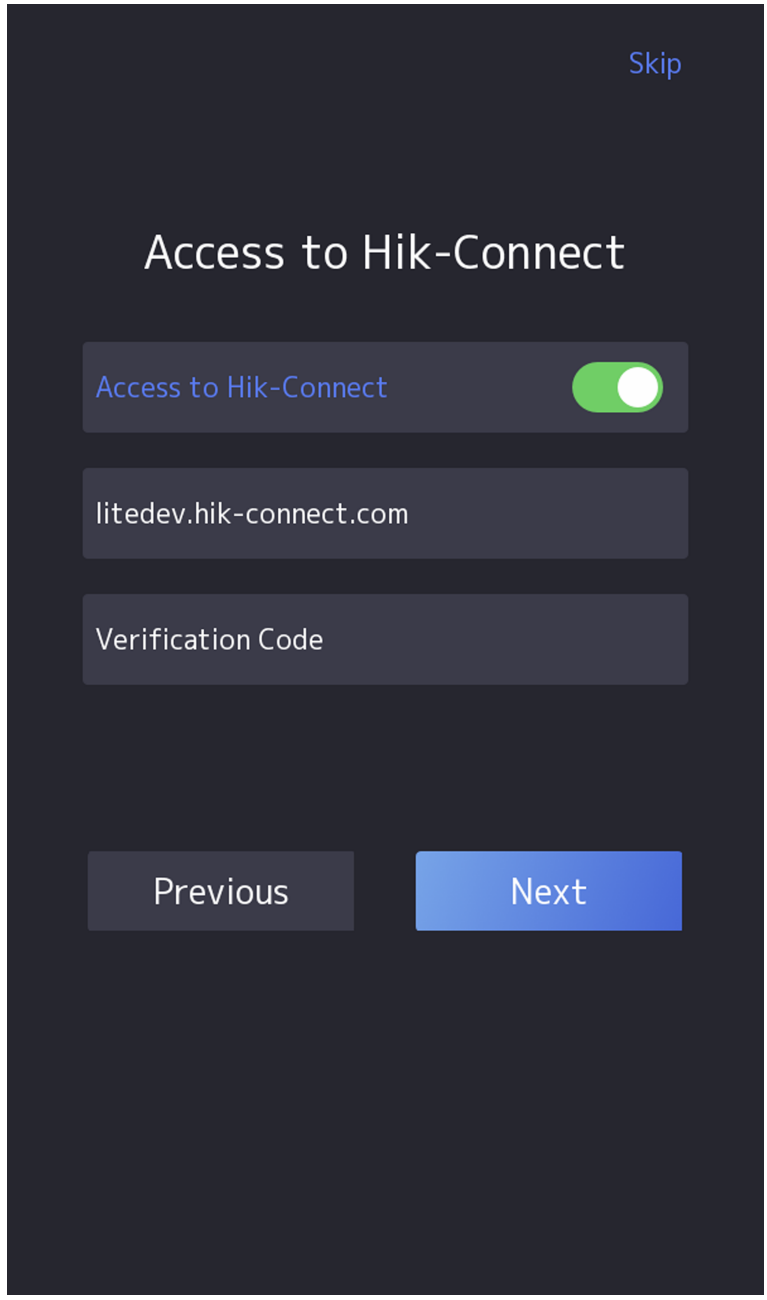


Figure 5-4 Access to Hik-Connect

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

Note

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

5.7 Privacy Settings

Select parameters according to your actual needs.

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

Upload the pictures captured when authenticating to the platform automatically.

Save Pic. When Auth. (Save 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.

Save Registered Iris Picture

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

Tap **Next**.

5.8 Set Administrator

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

Before You Start

Activate the device and select an application mode.

Steps

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

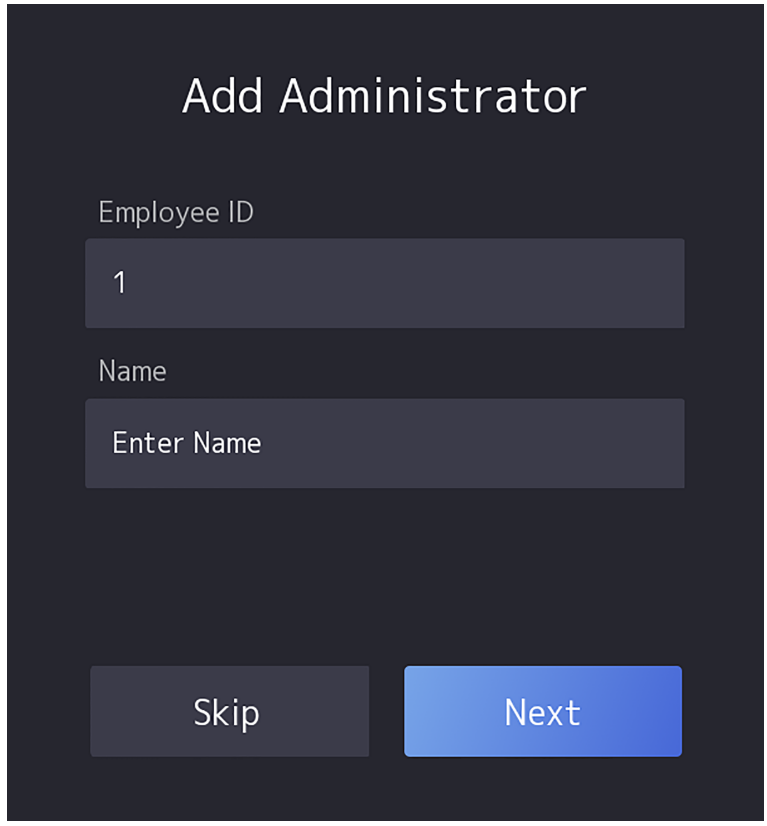


Figure 5-5 Add Administrator Page

3. Select a credential to add.

Note

Up to one credential should be added.

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

Note

Only devices connected to the external fingerprint module support fingerprint function.

4. Click **OK**.

You will enter the authentication page.

5.9 Authentication Page Instructions

Introduce the authentication page.

Status Bar Instructions

/

Device is armed/not armed.

/ /

The device' Wi-Fi is enabled and signal is strong/Wi-Fi is enabled but not connected/Wi-Fi's IP address is conflict.

/ /

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

Authentication Page Icon

Note

The displayed icon on the authentication page can be controlled. For details, see shortcut key settings in ***Set Shortcut Key via Device*** .

Show QR code to the camera and you can authenticate via the QR code.

- Enter the 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 PIN to authenticate.

Chapter 6 Basic Operation

6.1 Login

Login the device to set the device basic parameters.

6.1.1 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.

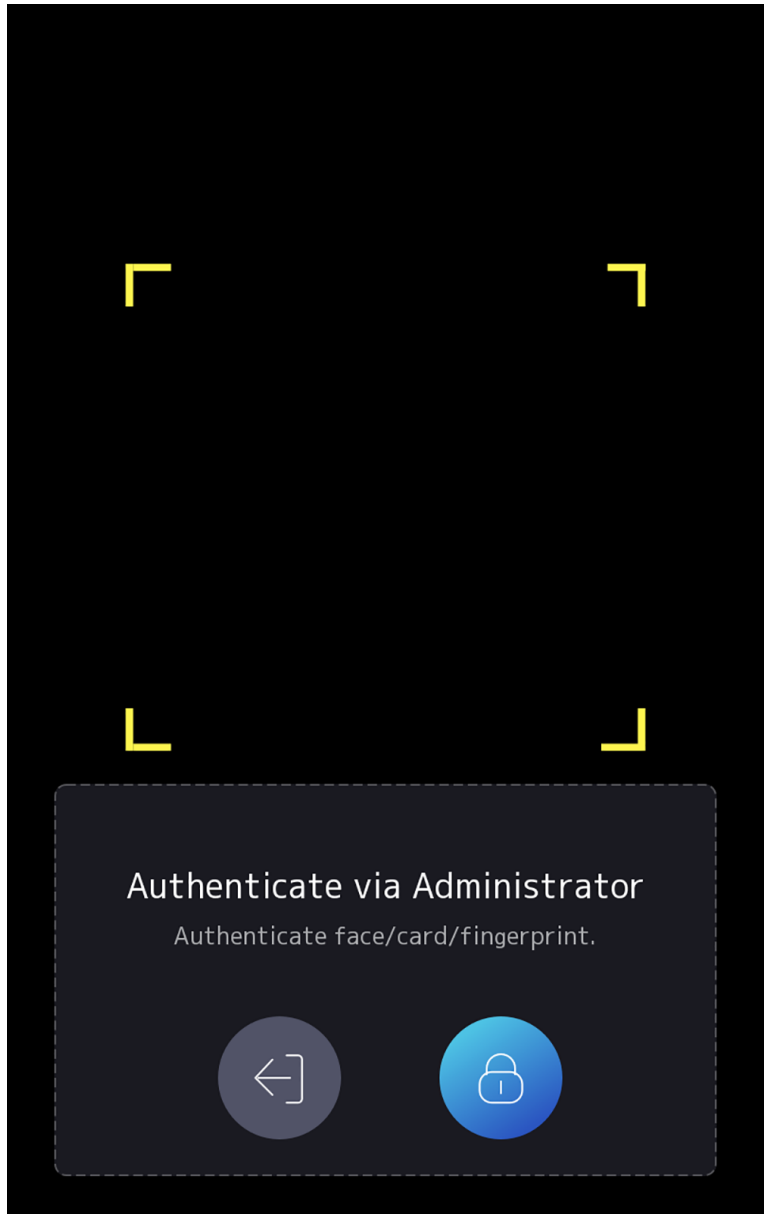


Figure 6-1 Admin Login

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

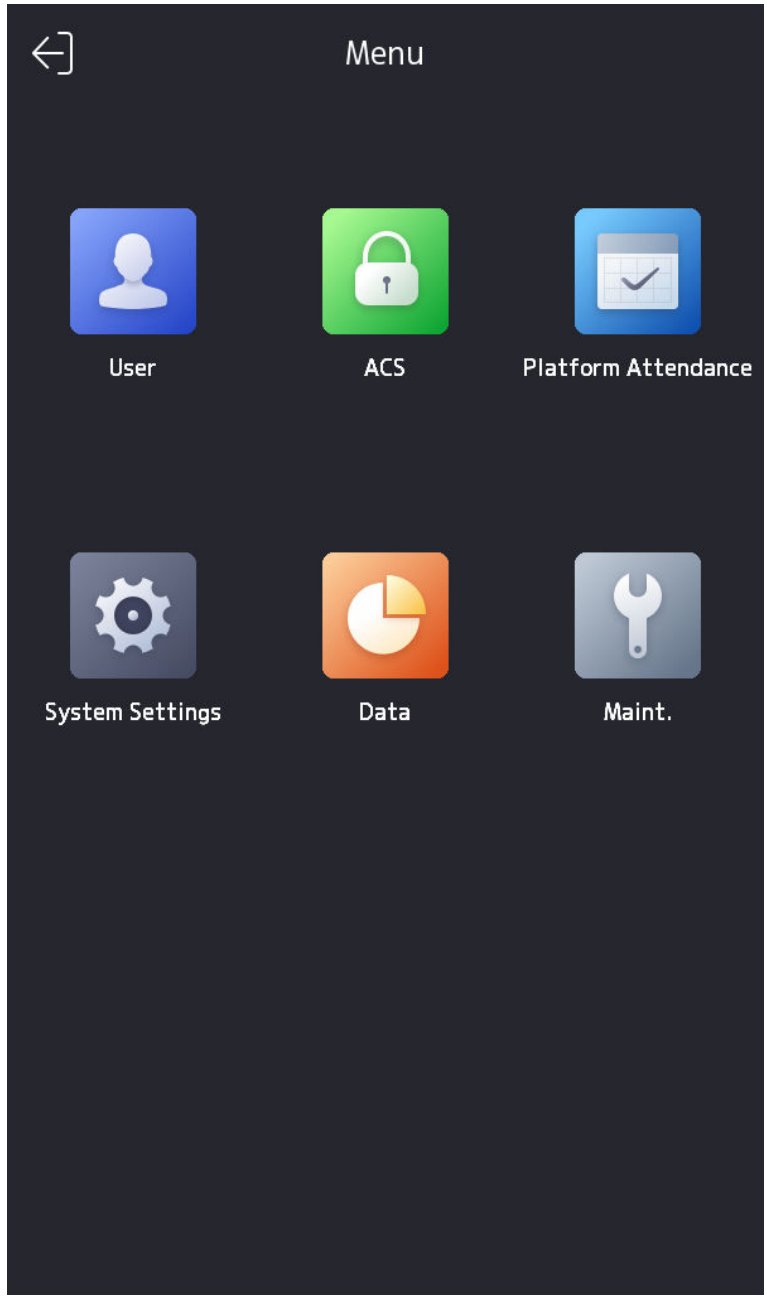


Figure 6-2 Home Page

Note

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

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

6.1.2 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. Enter the password.
   - If you have added an administrator for the device, tap  and enter the password.
   - If you haven't added an administrator for the device, enter the password.
3. Tap **OK** to enter the home page.

Note

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

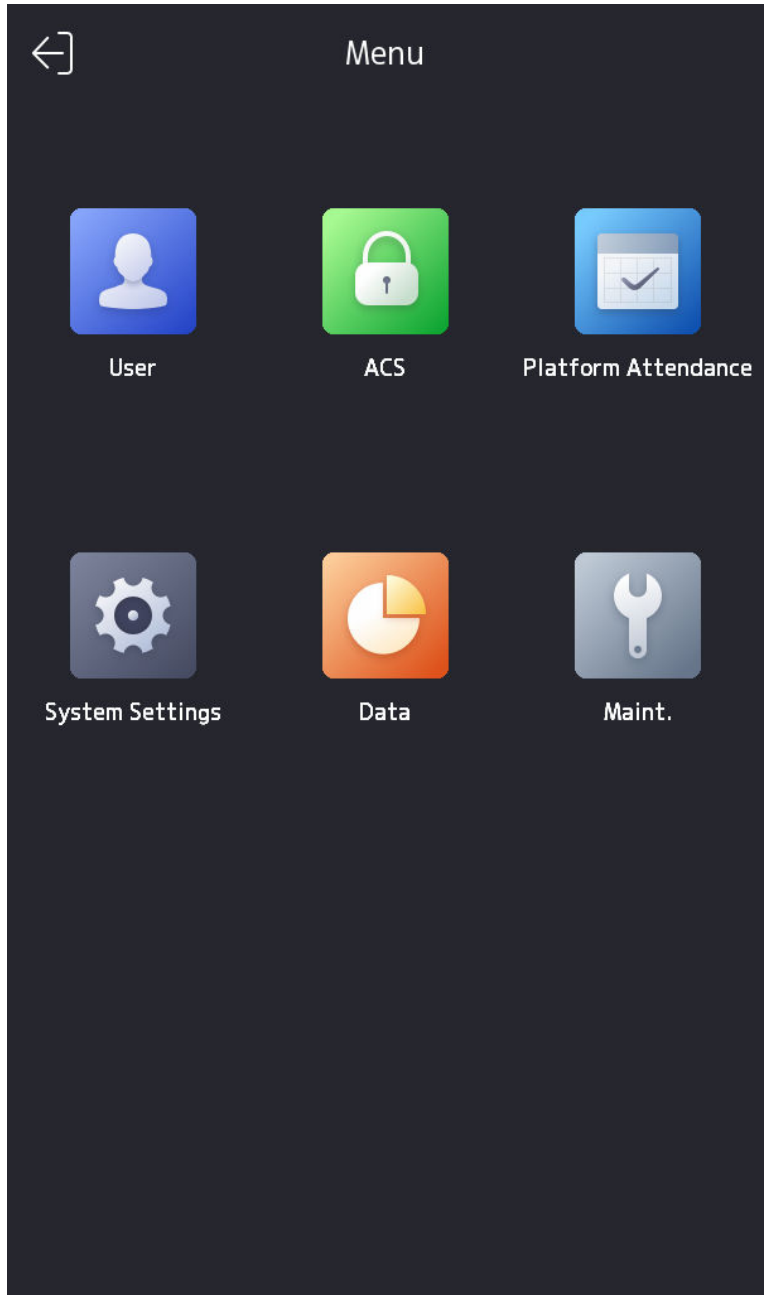


Figure 6-3 Home Page

6.1.3 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.
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**.

6.2 Communication Settings

You can set the wired network, the Wi-Fi parameter, the RS-485 parameters, the Wiegand parameters, ISUP and access to Hik-Connect on the communication settings page.

6.2.1 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 **System Settings → Comm.** (Communication Settings) on the Home page to enter the Communication Settings page.
2. On the Communication Settings page, tap **Wired Network**.

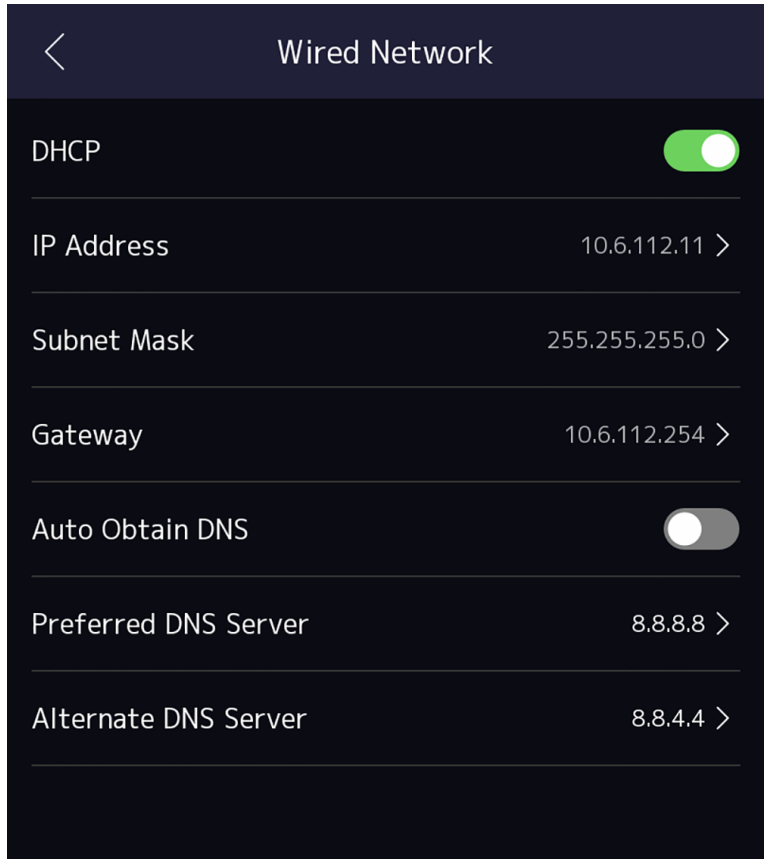


Figure 6-4 Wired Network Settings

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

   Note

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

6.2.2 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 **System → Comm.** (Communication Settings) on the Home page to enter the Communication Settings page.
2. On the Communication Settings page, tap.

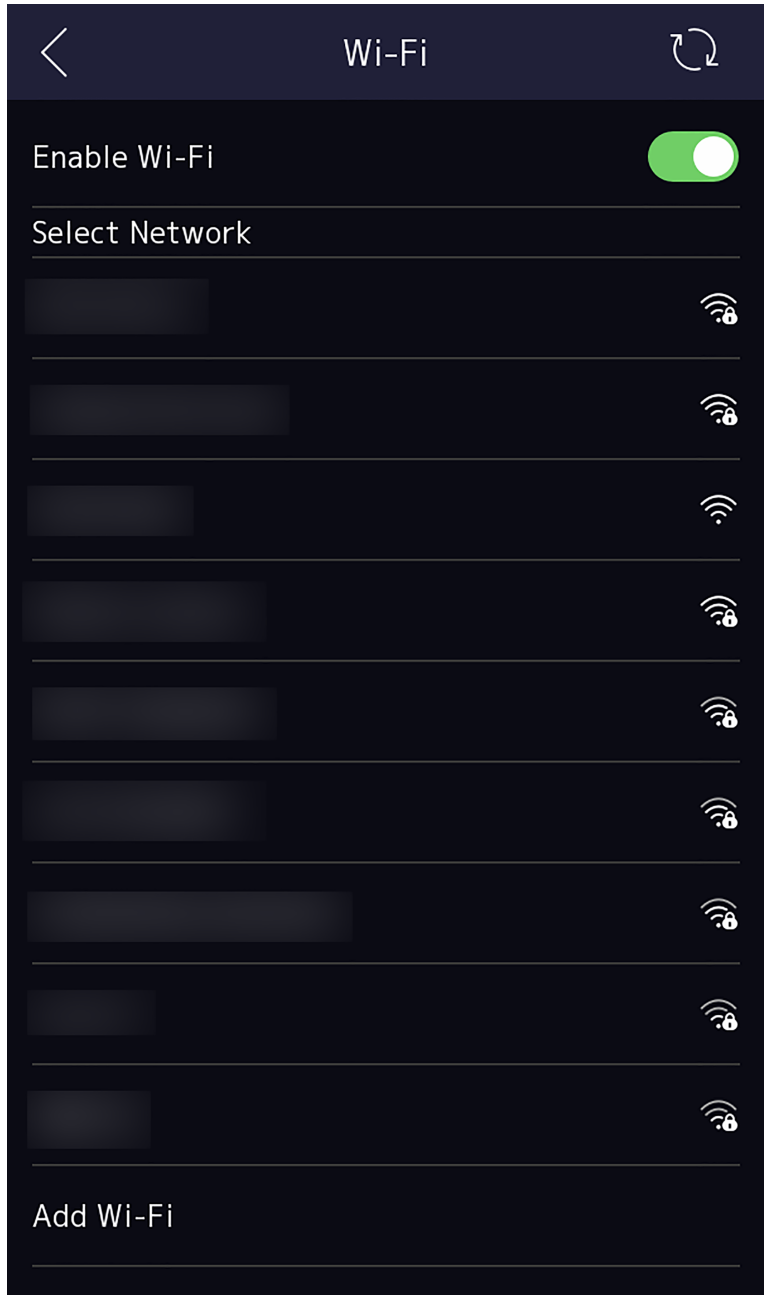


Figure 6-5 Wi-Fi Settings

3. Enable the Wi-Fi function.
4. Configure the Wi-Fi parameters.
   - Select a Wi-Fi from the list, and enter the Wi-Fi's password. Tap **OK**.

- If the target Wi-Fi is not in the list,tap **Add Wi-Fi**. Enter the Wi-Fi's name and password. And tap **OK**.

Note

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

5. Set the Wi-Fi's parameters.
   - By default, DHCP is enable. The system will allocate the IP address, the subnet mask, and the gateway automatically.
   - If disable DHCP, you should enter the IP address, the subnet mask, and the gateway manually.
6. Tap **OK** to save the settings and go back to the Wi-Fi tab.
7. Tap ✓ to save the network parameters.

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

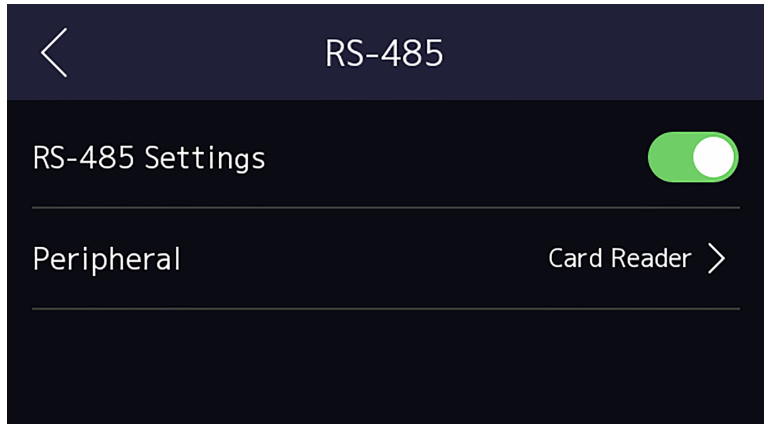


Figure 6-6 Set RS-485 Parameters

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

Note

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

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

6.2.4 Set Wiegand Parameters

You can set the Wiegand transmission direction.

Steps

1. Tap **System → 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.
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 34.
   - Input: A face recognition terminal can connect a Wiegand card reader.
5. Tap ✓ to save the network parameters.

Note

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

6.2.5 Set ISUP Parameters

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

Before You Start

Make sure your device has connect to a network.

Steps

1. Tap **System → Comm. → ISUP** (Communication Settings) on the Home page to enter the settings page.

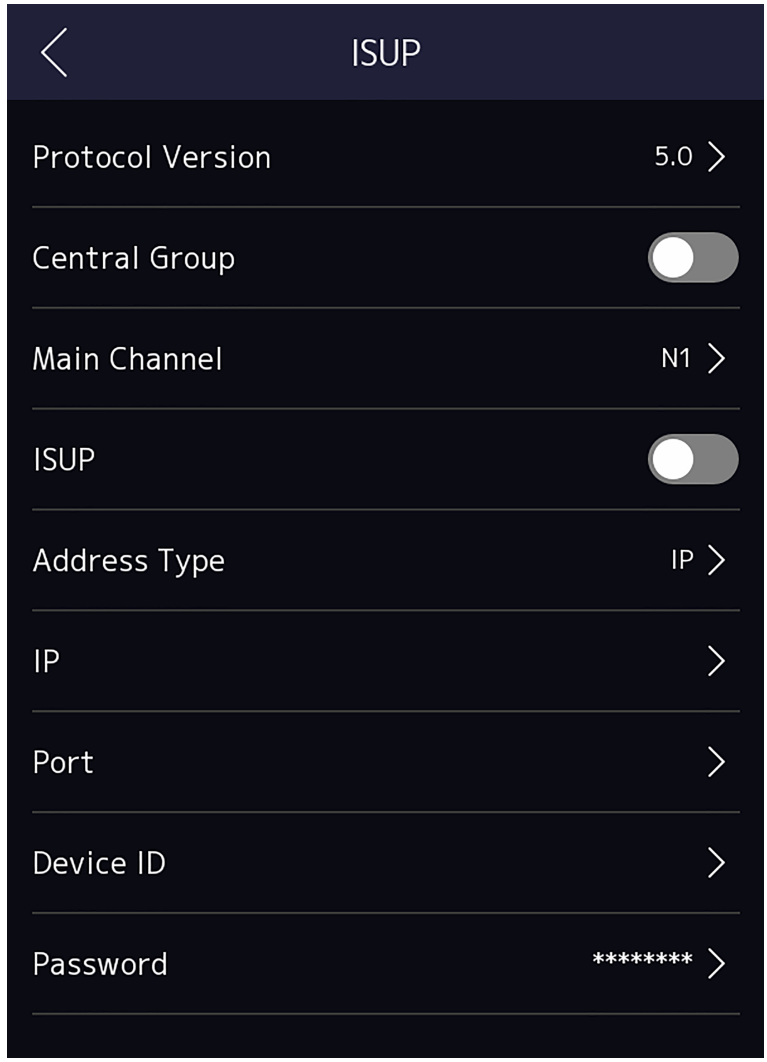


Figure 6-7 ISUP Settings

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

ISUP Version

Set the ISUP version according to your actual needs.

Central Group

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

Main Channel

Support N1 or None.

ISUP

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

Address Type

Select an address type according to your actual needs.

IP Address

Set the ISUP server's IP address.

Port No.

Set the ISUP server's port No.

Note

Port No. Range: 0 to 65535.

Device ID

Set device serial no.

Password

If you choose V5.0, you should create an account and ISUP key. If you choose other version, you should create an ISUP account only.

Note

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

6.2.6 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 **System → 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**.

6.3 Person Management

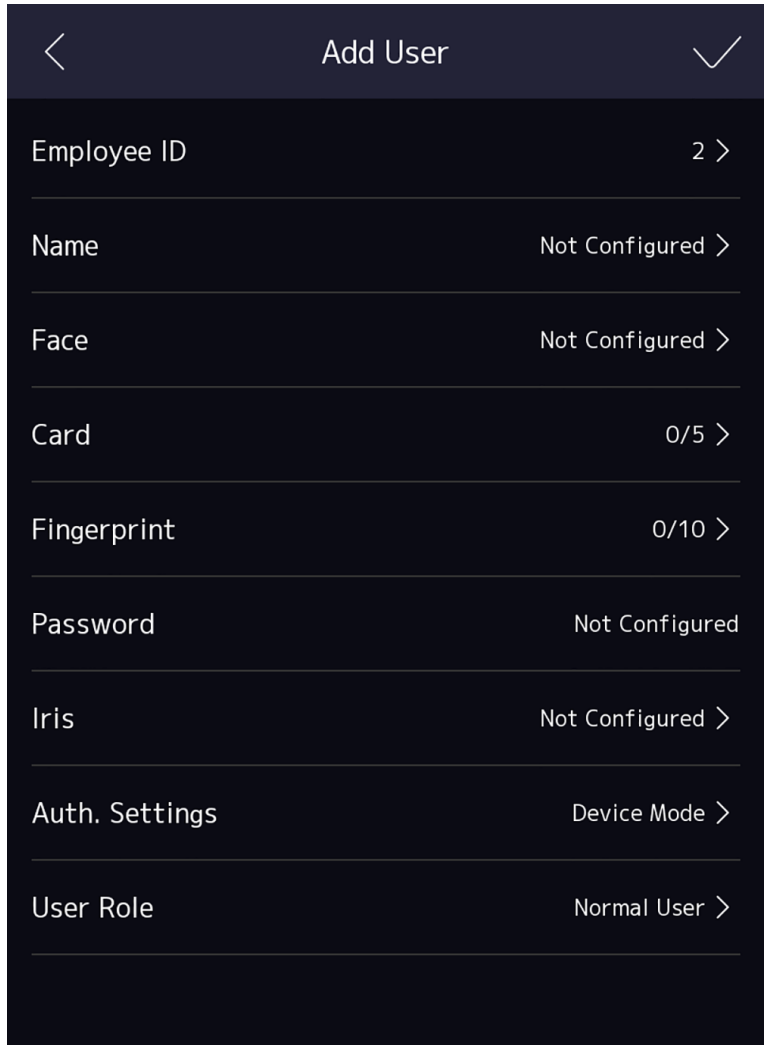
On the person management interface, you can add, edit, delete and search the person.

6.3.1 Add Administrator

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

Steps

1. Long tap on the initial page for 3 s and slide to the left/right by following the gesture and enter the device backend.
2. Tap **Person → +** to enter the Add Person 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 person name on the soft keyboard.

Note

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

5. **Optional:** Add a face picture, fingerprints, cards, PIN, iris for the administrator.

Note

- For details about adding a face picture, see ***Add Face Picture*** .
- For details about adding a fingerprint, see ***Add Fingerprint*** .
- For details about adding a card, see ***Add Card*** .
- For details about adding a password, see ***View PIN code*** .
- For details about adding a iris, see ***Add Iris*** .

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

8. Tap ✓ to save the settings.

6.3.2 Import and Export Face and Person Data in Batch via Device

You can use the import and export function to import the data from device A to device B by USB flash drive.

Before You Start

- Login Device A (The device that you need to export data). For details, see ***Login*** .
- Insert an USB flash drive to Device A.

Note

- The supported USB flash drive format is FAT32 or exFAT.
- The system supports the USB flash drive with the storage of 1 G to 256 G. Make sure the free space of the USB flash drive is more than 512 M.

Steps

1. On Device A menu, tap **Data** and enter the **Data** page.

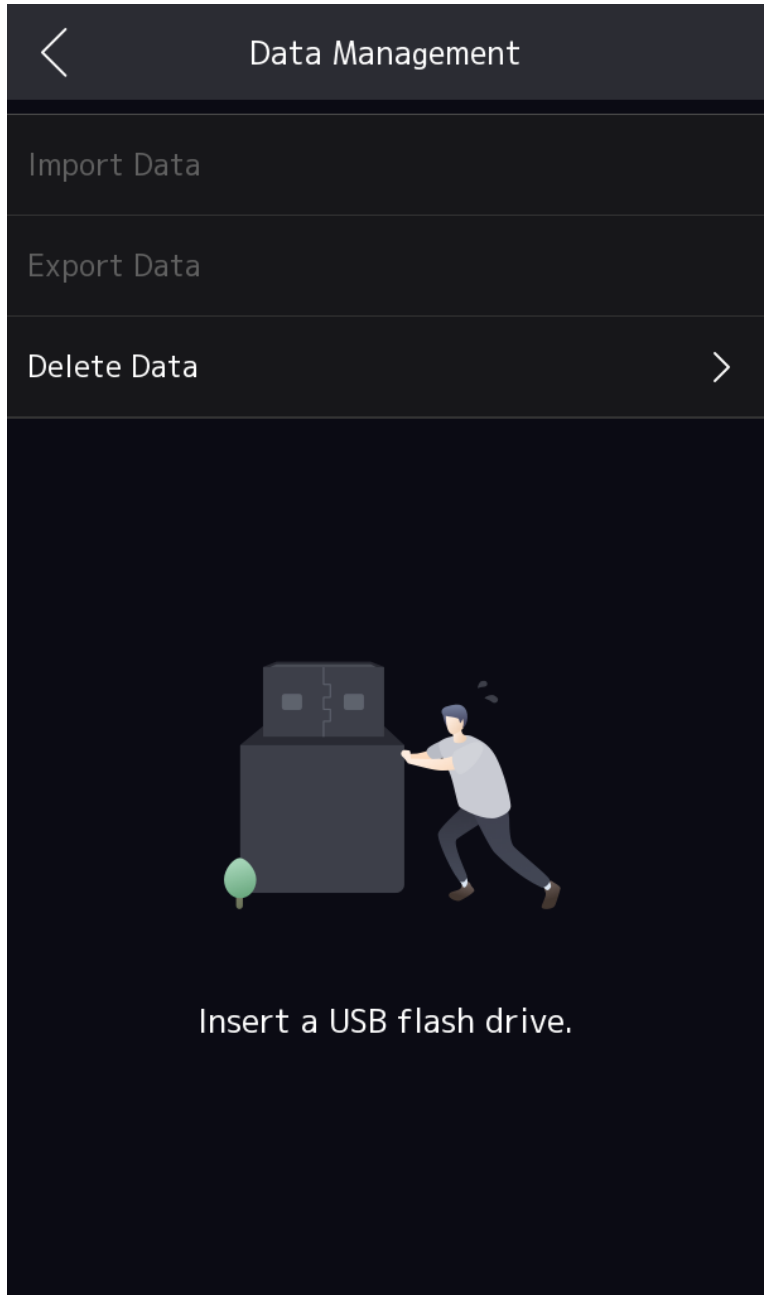


Figure 6-8 Data Management Page

2. Tap **Export Data** in the Data Management page.
3. Select **Person 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 password cannot be empty. If you do not set a password, you can view the exported data in your PC.
- If you set a password, you cannot view the exported data in your PC.
- The exported person data is a DB file, which cannot be edited.

5. Insert the USB flash drive to Device B that need to import face and person data.

Note

Make sure the two device are of the same device type.

6. On Device B menu, tap **Data**and enter the **Data** page.
7. Tap **Import Data**.
8. Select **Person Data** or **Face Data**.
9. 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**. The data will be imported from USB flash drive.

Note

- If you need to import pictures manually, you should save the pictures in the root directory (enroll_pic) of the USB flash drive. The picture's name should be follow the rule below: Card No._Name_Department_Employee ID_Gender.jpg For gender, 3 refers to male, 6 refers to female, and 0 refers to none. The employee ID should be less than 32 characters. The name should be less than 20 characters, and the card No. should be less than 20 characters.
- Up to 10,000 pictures can be saved in the Enroll_pic folder. 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. Up to 10 folders can be added. The picture name should follow the picture naming rule.
- Requirements of face picture should follow the rules below: It should be taken in full-face view, directly facing the camera. Do not wear a hat or head covering when taking the face picture. The format should be JPEG or JPG. The resolution should be 640 × 480 pixel or more than of 640 × 480 pixel. The picture size should be between 60 KB and 200 KB.

6.3.3 Add Face Picture

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

Steps

1. Long tap on the initial page for 3 s and slide to the left/right by following the gesture and log in the backend.
2. Tap **Person → +** to enter the Add Person 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 person name on the soft keyboard.

Note

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

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

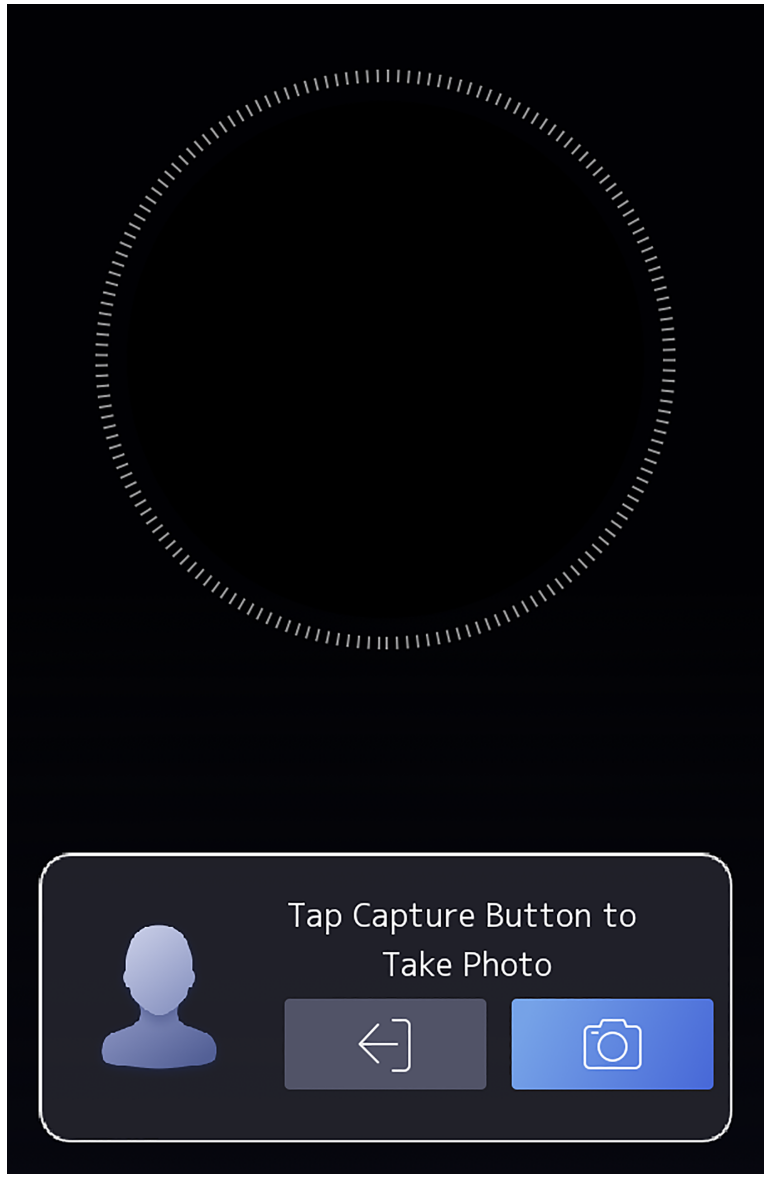


Figure 6-9 Add Face Picture

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 person type.

   Basic Person

   The person is the normal person. The person can only authenticate or take attendance on the initial page. You can also set the basic person as an **Administrator** by enable the administrator function.
10. Tap ✓ to save the settings.

6.3.4 Add Card

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

Steps

Note

Each person can add up to 5 cards.

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 **person → +** to enter the Add Person 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 person name on the soft keyboard.

   Note

   - Numbers, upper case letters, lower case letters, and special characters are allowed in the person name.
   - The suggested person 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. Tap ✓ to save the settings.

6.3.5 Add Fingerprint

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

Steps

Note

The function should be supported by the device.

1. Long tap on the initial page for 3 s and slide to the left/right by following the gesture and enter the device backend.
2. Tap **Person → +** to enter the Add Person 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 start with 0 and should not be duplicated.

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

Note

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

5. Tap the Fingerprint field to enter the Add Fingerprint page.
6. Follow the instructions to add a fingerprint.

Note

- The same fingerprint cannot be repeatedly added.
- Up to 10 fingerprints can be added for one person.
- You can also use the client software or the fingerprint recorder to record fingerprints. For details about the instructions of scanning fingerprints, see ***Tips for Scanning Fingerprint*** .

7. Tap ✓ to save the settings.

6.3.6 View PIN code

Add a PIN code for the person and the person can authenticate via the PIN code.

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 **Person → +** to enter the Add Person 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 person name on the soft keyboard.

Note

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

5. Tap the PIN code to view the PIN code.

Note

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

6. Tap ✓ to save the settings.

6.3.7 Add Iris

Add user's iris information to the device. And the user can use the iris information to authenticate.

Steps

Note

Up to 5000 iris 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 Iris field to enter the iris picture adding page.

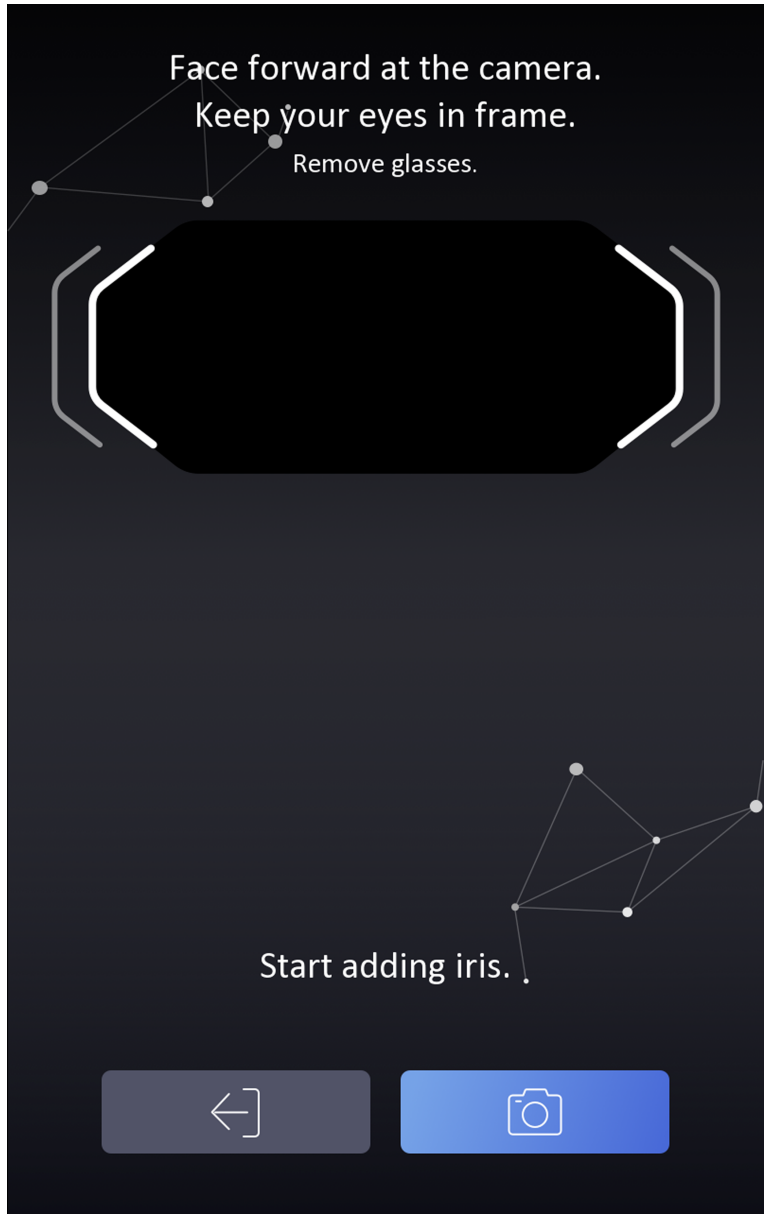


Figure 6-10 Add Iris

6. Look at the camera.

Note

- Make sure your eyes in frame when adding the iris.
- Make sure the captured iris is in good quality and is accurate.
- Remove your glasses when adding the iris.
- Keep your position when adding the iris.

7. Tap ✓ to save the iris information.
8. **Optional:** Tap and adjust your eyes position to add the iris 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.

6.3.8 Set Person Type via Device

Set the person type.

Before You Start

Login the device. For details, see ***Login*** .

Steps

1. Tap **Person → +**.

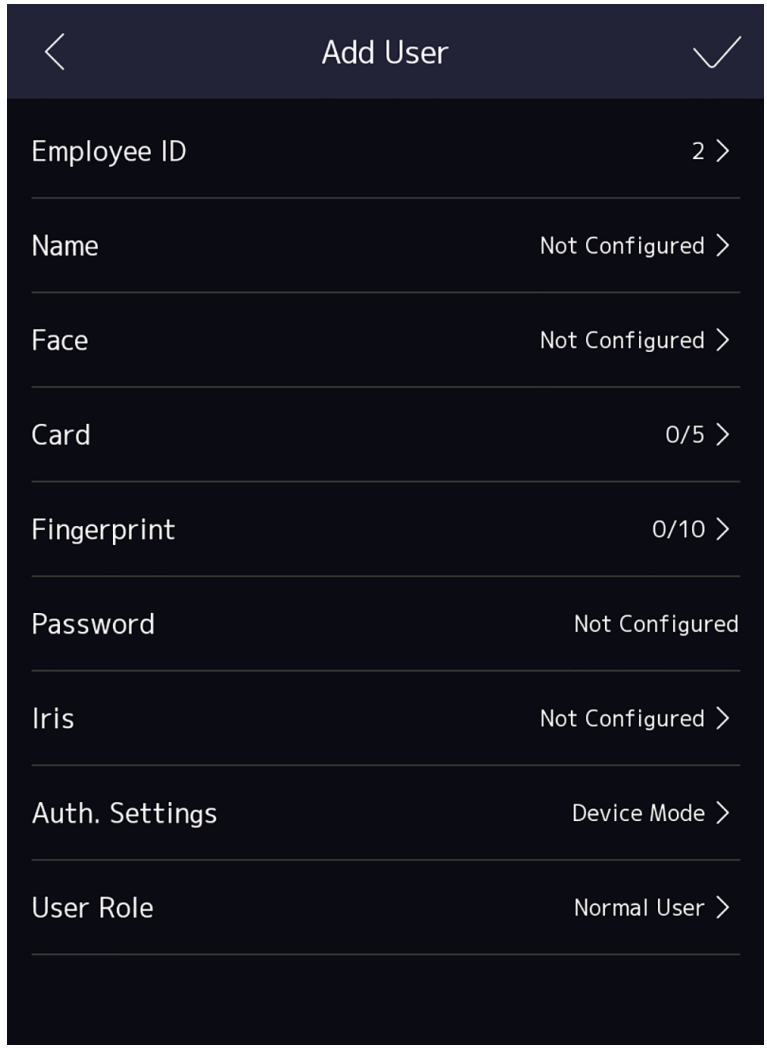


Figure 6-11 Add Person

2. Tap **Employee ID** and you can edit the Employee ID.

Note

The employee ID cannot be more than 32 characters. It can be a combination of upper case letters, lower case letters, and digits.

3. Tap **Name** and create a name. Enter the person's name according to the pop-up keyboard.

Note

- The name supports digits, upper case letters, lower case letters, and special characters.
- The name should be within 128 characters.

4. Set the face, card, fingerprint, and iris.

Note

- Refers to ***Add Face Picture*** , ***Add Card*** , ***Add Fingerprint*** , and ***Add Iris*** to add face, card, fingerprint and iris.
- Only device with fingerprint modules supports the fingerprint functions.

5. Tap **Person Type**.
6. Tap ✓ to save the settings.

6.3.9 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 **Person → Add Person/Edit Person → Authentication Mode** .
3. Select Device or Custom as the authentication mode.

   Device

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

   Custom

   You can combine different authentication modes together according to your actual needs.
4. Tap ✓ to save the settings.

6.3.10 Search and Edit Person

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

Search Person

On the Person Management page, Tap the search area to enter the Search Person 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 person name for search. Tap 🔍 to search.

Edit Person

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

Note

The employee ID cannot be edited.

6.4 Data Management

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

6.4.1 Delete Data

Delete person data.

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

6.4.2 Import Data

Steps

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

   Note

   The imported access control parameters are configuration files of the device.
4. Enter the created password when you exported the data. If you do not create a password when you exported the data, leave a blank in the input box and tap **OK** immediately.

   Note

   - If you want to transfer all person 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 person data before importing the profile photo.
   - The supported USB flash drive format is FAT32.
   - The imported pictures should be saved in the folder (named enroll_pic) of the root directory and the picture's name should be follow the rule below:
     Card No._Name_Department_Employee ID_Gender.jpg
   - If the folder enroll_pic cannot save all imported pictures, you can create another folders, named enroll_pic1, enroll_pic2, enroll_pic3, enroll_pic4, under the root directory.
   - The employee ID should be less than 32 characters. It can be a combination of lower letters, upper letters, and numbers. It should not be duplicated, and should not start with 0.
   - Requirements of face picture should follow the rules below: It should be taken in full-face view, directly facing the camera. Do not wear a hat or head covering when taking the face

picture. The format should be JPEG or JPG. The resolution should be 640 × 480 pixel or more than of 640 × 480 pixel. The picture size should be between 60 KB and 200 KB.

6.4.3 Export Data

Steps

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

Note

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

4. **Optional:** Create a password for exporting. When you import those data to another device, you should enter the password.

Note

- The supported USB flash drive format is DB.
- The system supports the USB flash drive with the storage of 1 G to 256 G. Make sure the free space of the USB flash drive is more than 512M.
- The exported person data is a DB file, which cannot be edited.

6.5 Person Authentication

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

6.5.1 Authenticate via Single Credential

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

Authentication combination groups related to iris are as follows.

Face or Fingerprint or Card or Password or Iris

Face or QR Code or Password or Iris

Face or Fingerprint or QR Code or Iris

Face or Fingerprint or Password or Iris

Fingerprint or QR Code or Password or Iris

QR Code or Password or Iris

Authenticate face, fingerprint, card or QR code.

Face

Face forward at the camera and start authentication via face.

Iris

Look at the camera and make your eyes in frame and start authentication via iris.

Fingerprint

Place the enrolled fingerprint on the fingerprint module and start authentication via fingerprint.

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.

Password

Enter the password to authenticate via password.

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

6.5.2 Authenticate via Multiple Credential

Before You Start

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

Steps

1. Authenticate any credential according to the instructions on the live view page.

   Note

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

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

   Note

   - For detailed information about scanning fingerprint, see *Tips for Scanning Fingerprint*.
   - For detailed information about authenticating face, see *Tips When Collecting/Comparing Face Picture*.

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

6.6 Basic Settings

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 **System → Basic** .

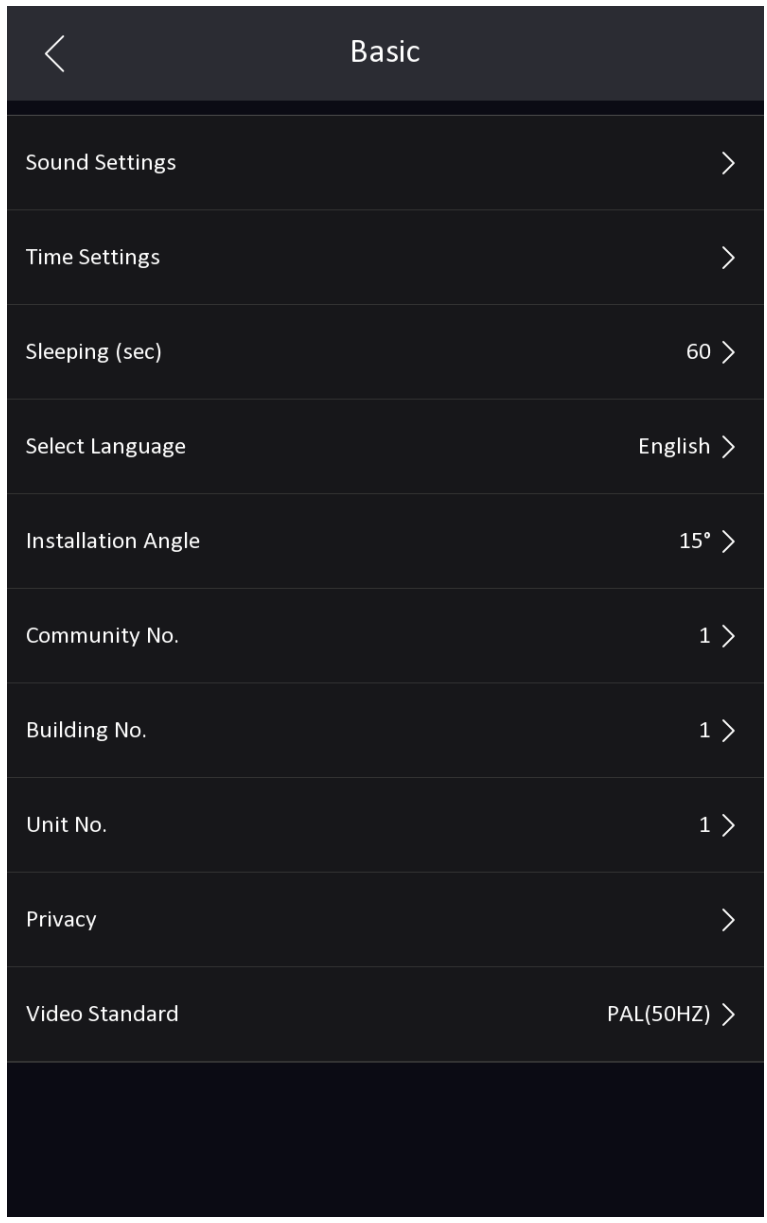


Figure 6-12 Basic Settings Page

6.6.1 Enable/Disable Voice Prompt via Device

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

Login the device. For details, see ***Login*** .

Tap **System Settings → Basic → Sound Settings**.

You can enable **Voice Prompt** function and adjust the voice volume. Enable the voice prompt function and you can set the voice volume.

6.6.2 Set Device Time via Device

Set the device time.

Login the device. For details, see ***Login*** .

Tap **System Settings → Basic → Time Settings**.

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

6.6.3 Set Sleep Duration via Device

Set the device sleeping waiting time.

Login the device. For details, see ***Login*** .

Tap **System Settings → Basic**. And Set **Sleep Duration**.

When you are on the initial page and if you set the sleeping time to 30 s, the device will sleep after 30 s without any operation.

Note

If you set the sleeping time to 0, the device will not enter sleeping mode. The configurable sleep time is between 20 and 999s.

6.6.4 Select Language

Login the device. For details, see ***Login*** .

Tap **System Settings → Basic** . And tap **Select Language** to change the device language.

The device will reboot after changing the language.

6.6.5 Set Installation Angle

You can set installation angle.

Login the device. For details, see ***Login*** .

Tap **System Settings → Basic → Privacy** .

Set the installation angle.

6.6.6 Set Device Number via Device

The device can be used as access control device, door station, or outer door station. You can set the device number for video intercom.

Login the device. For details, see ***Login*** .

Tap **System Settings → Basic**. And set **Community No.**, **Building No.**, and **Unit No.**

6.6.7 Set Privacy Parameters via Device

Set the picture uploading parameters.

Note

Different device models support different functions. Refers to actual model.

Login the device. For details, see ***Login*** .

Tap **System Settings → Basic → Privacy**.

Authentication Settings

Name / Employee ID / Face Picture

You can choose to display/not display/desensitize name and Employ ID when authenticating.

Picture Uploading and Storage

Set picture uploading and storage parameters.

Save Registered Pic.

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

Save Pic. After Linked Capture

If you enable this function, you can save the picture after linked capture.

Upload Pic. After Linked Capture

Upload the pictures captured after linked capture.

Save Pic When Auth.

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

Upload Pic. When Auth.

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

Save Iris Picture

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

6.6.8 Set Video Standard

Set video standard for the live view.

Login the device. For details, see ***Login*** .

Go to **System → Basic → 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 (50HZ)

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

NTSC (60HZ)

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

6.7 Set Face Parameters

You can customize the face parameters to improve the face recognition performance.

Long tap on the initial page for 3 s and login the home page. Tap **System Settings → Biometrics → Face** .

6.7.1 Set Application Mode

Set application mode.

Login the device. For details, see ***Login*** .

Tap **System Settings → Biometrics → Application Mode** .

Select **Application Mode**.

6.7.2 Set Face Liveness Level via Device

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

Login the device. For details, see ***Login*** .

Tap **System Settings → Biometrics → Face** .

Select a face liveness level.

You can select from general, advanced, and professional. The higher the level, the fault acceptance rate will be lower and the false rejection rate will be higher.

6.7.3 Set Recognition Distance via Device

Set the valid distance between the user and the camera when authenticating.

Login the device. For details, see ***Login*** .

Tap **System Settings → Biometrics → Face → Recognition Distance** .

Set the recognition distance.

6.7.4 Set Face Recognition Interval via Device

The time interval between two continuous face recognitions when authenticating.

Login the device. For details, see ***Login*** .

Tap **System Settings → Biometrics → Face → Face Recognition Interval (sec)** .

Set the face recognition interval.

Note

Please enter a number between 1 and 10.

6.7.5 Set Wide Dynamic

When there are both very bright and very dark areas simultaneously in the view, you can enable the Wide Dynamic function.

Long tap on the initial page for 3 s and slide to the left/right by following the gesture. Login and tap **System → Biometrics → Face** .

Note

It is suggested to enable the Wide Dynamic function if installing the device outdoors.

Enable **Wide Dynamic**.

When there are both very bright and very dark areas simultaneously in the view, you can enable the Wide Dynamic function to balance the brightness of the whole image and provide clear images with details.

6.7.6 Set Face 1:N Security Level via Device

Set the matching threshold when authenticating via 1:N matching mode.

Login the device. For details, see ***Login*** .

Tap **System Settings → Biometrics → Face → Face 1:N Security Level** .

Set the matching threshold when authenticating via 1:N matching mode.

The larger the value of the threshold, the fault acceptance rate will be lower and the false rejection rate will be higher when authenticating via face. The maximum value is 100.

6.7.7 Set Face 1:1 Security Level via Device

Set the matching threshold when authenticating via 1:1 matching mode.

Login the device. For details, see ***Login*** .

Tap **System Settings → Biometrics → Face → Face 1: 1 Security Level** .

Set the matching threshold when authenticating via 1:1 matching mode.

The larger the value of the threshold, the fault acceptance rate will be lower and the false rejection rate will be higher when authenticating via face. The maximum value is 100.

6.7.8 Enable/Disable ECO Mode via Device

If the ECO mode is enabled, you can authenticate faces in the low light or dark environment with IR camera.

Login the device. For details, see ***Login*** .

Tap **System Settings → Biometrics → Face → ECO Mode Settings** .

If the ECO mode is enabled, you can authenticate faces in the low light or dark environment with IR camera. You can set the ECO mode threshold, ECO mode (1:N), and ECO mode (1:1).

ECO Mode Threshold

When enabling the ECO mode, you can set the ECO mode's threshold. The larger the value, the easier the device entering the ECO mode. The threshold has relationship with the illumination.

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. The maximum value is 100.

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. The maximum value is 100.

6.7.9 Enable/Disable Hard Hat Detection via Device

After enabling the hard hat detection, when the device starts face authentication, the system will detection whether the person wearing a hard hat or not.

Login the device. For details, see ***Login*** .

Tap **System Settings → Biometrics → Face → Hard Hat Detection** .

Hard Hat Detection

After enabling the hard hat detection function, you can set the strategy of door opening.

None

If the person do not wear a face mask when authenticating, the device will not prompt a notification.

Reminder of Wearing

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

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

6.7.10 Enable/Disable Mask Detection via Device

After enabling the face with mask detection, the system will recognize the captured face with mask picture.

Login the device. For details, see ***Login*** .

Tap **System Settings → Biometrics → Face → Mask Settings**.

After enabling the face with mask detection, the system will recognize the captured face with mask picture. You can set **Face with Mask & Face (1:1)**、**Face with Mask & Face (1:N)**、**ECO Mode (1:1) Threshold**、**ECO Mode (1:N) Threshold**, and **Prompt Method**.

Face with Mask & Face (1:1)

Set face with mask 1:1 matching threshold. The larger the value, the smaller the false accept rate and the larger the false rejection rate. The maximum value is 100.

Face with Mask & Face (1:N)

Set face with mask 1:N matching threshold. The larger the value, the smaller the false accept rate and the larger the false rejection rate. The maximum value is 100.

ECO Mode (1:1) Threshold

After enabling the ECO mode, you can set the face with mask function. You can set the threshold.

Set the matching threshold when authenticating via ECO mode 1:1 matching mode. The larger the value of the threshold, the fault acceptance rate will be lower and the false rejection rate will be higher when authenticating via face. The maximum value is 100.

ECO Mode (1:N) Threshold

After enabling the ECO mode, you can set the face with mask function. You can set the threshold.

Set the matching threshold when authenticating via ECO mode 1:N matching mode. The larger the value of the threshold, the fault acceptance rate will be lower and the false rejection rate will be higher when authenticating via face. The maximum value is 100.

Strategy

Set **None**、 **Reminder of Wearing**, and **Must Wear**.

None

If the person do not wear a face mask when authenticating, the device will not prompt a notification.

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.

6.7.11 Iris Settings

Long tap on the initial page for 3 s and login the home page. Tap **System → Biometric → Iris** to enter the page.

Table 6-1 Iris Parameters

Parameter	Description
Face Anti-Spoofing Detection	Enable or disable the iris detection function. If enabling the function, the device can recognize whether the iris is a true one or not. **Note** Biometric recognition products are not 100% applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.
Iris Recognition Interval	The time interval between two continuous iris recognitions when authenticating.
Iris Recognition Mode	Iris recognition mode consists of single-eye mode and dual-eye mode.
Iris Detection Level	After enabling the iris anti-spoofing function, you can set the matching security level when performing live iris authentication.
Single-Eye Iris 1:1 Security Level	Set the single-eye 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
Single-Eye Iris 1:N Security Level	Set the single-eye 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.
Dual-Eye Iris 1:1 Security Level	Set the dual-eye 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.
Dual-Eye Iris 1:N Security Level	Set the dual-eye 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.
Lock Iris for Anti-spoofing Protection	Enable or disable the lock iris for anti-spoofing protection function. If enabling the function, the device can recognize whether the iris is a live one or not. **Note** Biometric recognition products are not 100% applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.
Iris Recognition Timeout	Set the timeout value when iris recognizing. If the iris recognition time is longer than the configured value, the system will pop up a prompt.

6.8 Access Control Settings

You can set the access control permissions.

On the Home page, tap **ACS** to enter the Settings page.

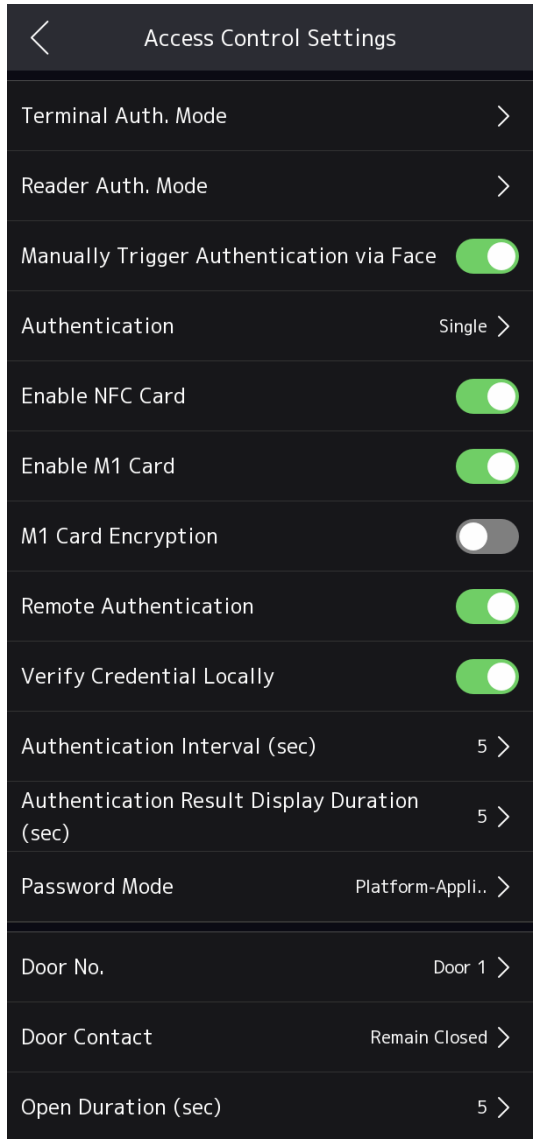


Figure 6-13 Access Control Settings

6.8.1 Set Terminal Authentication Mode via Device

Select the face recognition terminal's authentication mode. You can select different combination to authenticate.

Login the device. For details, see ***Login*** .

Tap **ACS → Terminal Auth. Mode** .

Select person authentication type and method and save the settings.

If all persons on the device's authentication mode is **Device Mode**, all persons on the device will use the device authentication mode. For detail about person authentication mode settings, see ***Set Authentication Mode*** .

Note

Device with fingerprint module supports fingerprint function.

Caution

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

6.8.2 Set Reader Authentication Mode via Device

Set the person authentication type on the wired external reader. You can select different combination to authenticate.

Login the device. For details, see ***Login*** .

Tap **ACS → Reader Auth. Mode** .

Select person authentication type and save the settings.

Select person authentication type and method and save the settings.

If all persons on the device's authentication mode is **Device Mode**, all persons on the device will use the device authentication mode. For detail about person authentication mode settings, see ***Set Authentication Mode*** .

Note

Device with fingerprint module supports fingerprint function.

Caution

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

6.8.3 Enable/Disable NFC Card

Enable/disable NFC card function.

After login, tap **ACS**.

Tap **Enable NFC**. After enabling, the device can read NFC card.

6.8.4 Enable/Disable M1 Card

Enable or disable M1 card function.

Login the device. For details, see ***Login*** .

After login, tap **ACS**.

Tap **Enable M1 Card**, and the device can read M1 card.

Enable M1 Card

After enabling, the device can read M1 card.

M1 Card Encryption

After enabling M1 Card Encryption, the device will verify the M1 card sector. Go to the platform to set the M1 card's encryption sector.

6.8.5 Remote Authentication

Judge the authentication passes or not by remote platforms.

Login the device. For details, see ***Login*** .

Tap **ACS**.

Enable **Remote Authentication**. When there's a person is authenticating, the remote platform will judge to pass or not.

Authenticate the credential on the device and verify by the platform.

You can also enable **Verify Credential Locally** and the verification will be produced on the device.

6.8.6 Set Authentication Interval via Device

Login the device. For details, see ***Login*** .

Tap **ACS**, and set **Authentication Interval** and save.

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. Available authentication interval range: 0 to 65535.

6.8.7 Door Parameter Configuration

Configure parameters for unlocking doors.

Set Door Contact via Device

Select door contact status according to the door contact's wiring method.

Login the device. For details, see ***Login*** .

Tap **ACS**.

You can select Remain Open or Remain Closed according to your actual needs. By default, it is Remain Closed.

Set Open Duration via Device

Set the door unlocking duration.

Login the device. For details, see ***Login*** .

Tap **ACS**.

Set the door unlocking duration. If the door is not opened for the set time, the door will be locked. Available door locked time range: 1 to 255s.

6.9 Platform Attendance

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

Note

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

6.9.1 Disable Attendance Mode via Device

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

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

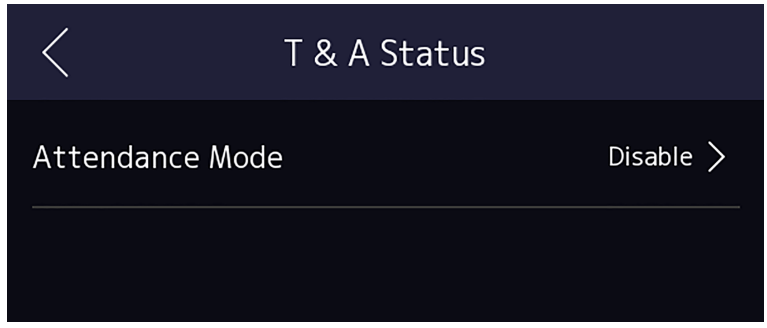


Figure 6-14 Disable Attendance Mode

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.

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

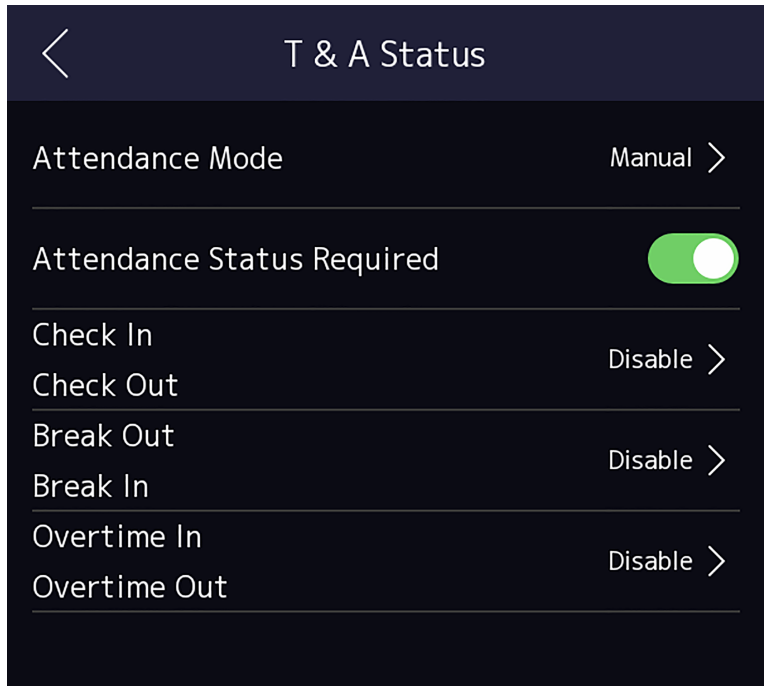


Figure 6-15 Manual Attendance Mode

3. Enable the **Attendance Status 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.

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

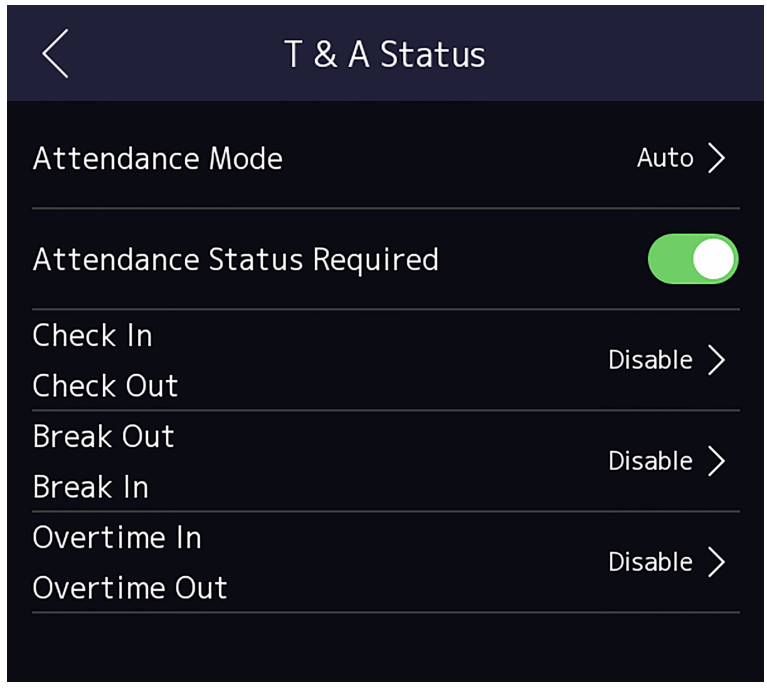


Figure 6-16 Auto Attendance Mode

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.

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

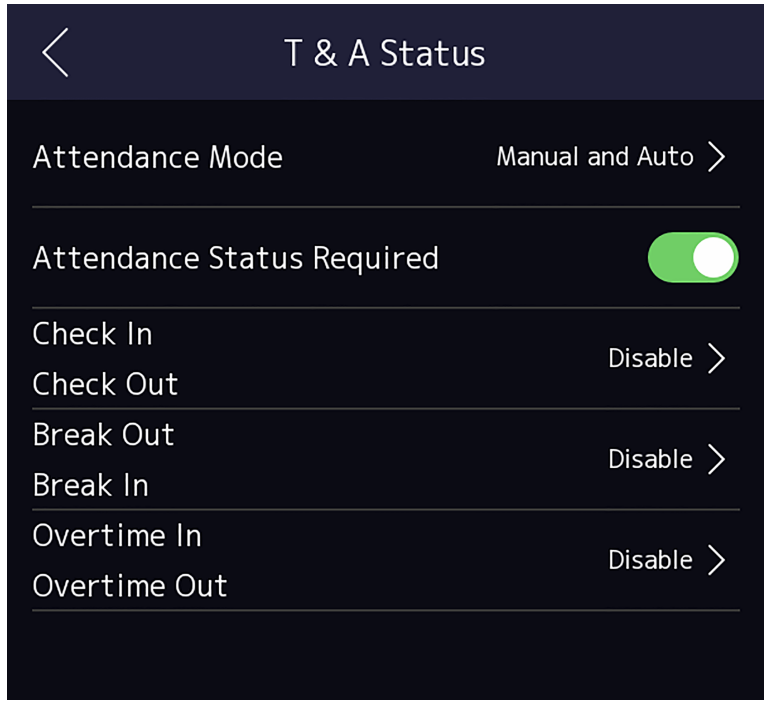


Figure 6-17 Manual and Auto Mode

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.

6.10 Preference Settings

You can configure preference settings parameters.

Steps
1. Tap **System → Preference** to enter the preference settings page.

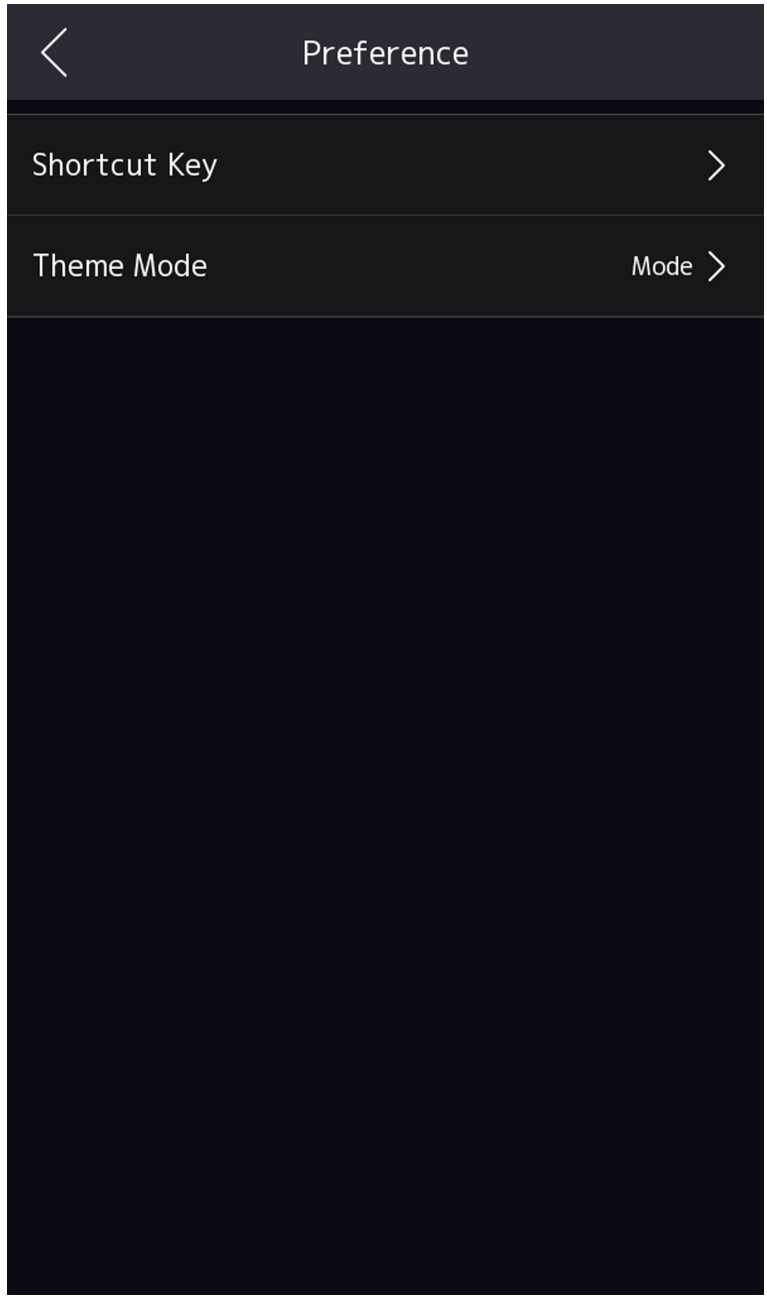


Figure 6-18 Preference Settings

6.10.1 Set Shortcut Key via Device

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.

Login the device. For details, see ***Login*** .

Tap **System Settings → Preference**.

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.

Password

Enable this function and you can enter the password to authenticate via password. Tap on the authentication page to verify.

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. Tap on the authentication page to verify.

Call

You can select call types from Call Room, Call Center, Call Specified Room, or Call APP. If you select **Call Specified Room**, you should enter the room No.

Tap on the authentication page to call.

6.10.2 Theme

Select different theme and the authentication page will show different contents.

Login the device. For details, see ***Login*** .

System Settings → Preference.

Select a theme mode.

Authentication

The live view will be displayed in authentication, and in the meanwhile, the person's name, employee ID, face pictures will all displayed as well.

Advertisement

The advertising area and identification authentication area of the device will be displayed on separate screens. Video, text, welcome words will be displayed in the advertizement area.

Simple Mode

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

6.11 System Maintenance

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.**

6.11.1 View System Information

View the device system information.

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. → System Info.** .

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.

Long tap on the right corner to enter the advanced settings page. You can set biometrics parameters and view the device version information.

Biometric Parameter

Custom Anti-Spoofing Detection

Face Liveness Level

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

Anti-Spoofing Detection Threshold

The larger the value, the smaller the false accept rate and the larger the false rejection rate. The smaller the value, the larger the false accept rate and the smaller the false rejection rate.

Lock Face for Anti-Spoofing Protection

After enabling this function, the device will lock automatically when anti-spoofing detection failed.

Lock Duration

The lock duration after enabling **Lock Face for Anti-Spoofing Protection** when anti-spoofing detection failed.

Version Information

You can view the device information.

6.11.2 View Device Capacity via Device

You can view the device capacity.

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. → Capacity**.

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

Note

Only device installed with fingerprint module supports display fingerprint capacity.

6.11.3 Upgrade

Online Upgrade

You can online upgrade 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. → Device Upgrade**.

If the device is connected to the network and added to Hik-Connect App, you can tap **Device Upgrade → Online Upgrade**on device for upgrading when there is an updated version in Hik-Connect App.

Local Upgrade

You can upgrade the device locally.

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. → Device Upgrade**.

Insert an USB flash drive. Tap **Device Upgrade → Update vi USB**, and the device will read the digicap.dav file in the USB flash drive to start upgrading.

6.11.4 Restore Settings

Restore to Factory Settings via Device

All parameters will be restored to the factory settings.

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. → Restore to Factory Settings**. The system will reboot to take effect.

Restore to Default Settings via Device

All parameters, except for the communication settings, remotely imported user information, will be restored to the default settings.

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. → Restore to Default Settings**. The system will reboot to take effect.

All parameters, except for the communication settings, remotely imported user information, will be restored System default settings. System will reboot after restoring the default settings.

Device Reboot

You can reboot the device manually.

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. → Reboot**.

6.12 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, call the indoor station from the device, or call the specific room from the device.

6.12.1 Call Client Software from Device

Steps

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

   Note

   For details about adding device, see *Add Device*.
5. Call the client software.
   1) Tap 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.

6.12.2 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.

6.12.3 Call Device from Client Software

Steps

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

Note

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

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

Note

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

6. Right click the live view image to open the right-click menu.

7. Click **Start Two-Way Audio** to start two-way audio between the device and the client software.

6.12.4 Call 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.

6.12.5 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 7 Operation via Web Browser

7.1 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.
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.

7.2 Forget Password

If you forget the password when logging in, you can change the password by email address or security questions.

On the login page, click **Forget Password**.

Select **Verification Mode**.

Security Question Verification

Answer the security questions.

E-mail Verification

1. Export the QR code and send it to ***pw_recovery@hikvision.com*** as attachment.
2. You will receive a verification code within 5 minutes in your reserved email.
3. Enter the verification code into the verification code field to verify your identification.

Click **Next**, create a new password and confirm it.

7.3 Download Web Plug-In

Both non-Plug-in live view and live view after downing plug-in are available. For better live view, downloading plug-in for live view is recommended.

Click → **Download Web Pug-In** to download the pulg-in to the local.

7.4 Help

7.4.1 Open Source Software Licenses

You can view open source software licenses.

Click → **Open Source Software Statement** on the upper-right corner to view the licenses.

7.4.2 View Online Help Document

You can view the help document for Web configuration.

Click → **Online Document** on the upper right of the Web page to view the document.

7.5 Logout

Log out the account.

Click **admin → Logout → OK** to logout.

7.6 Quick Operation via Web Browser

7.6.1 Change Password

You can change the device password.

Click on the top right of the web page to enter the **Change Password** page. You can set security questions from the drop-down list and fill in the answers.

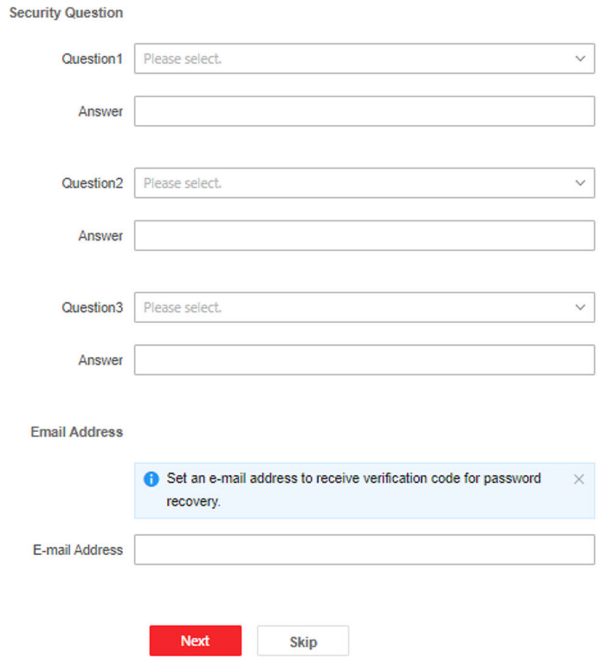


Figure 7-1 Change Password

Click **Next** to complete the settings. Or click **Skip** to skip the step.

7.6.2 Select Language

You can select a language for the device system.

Click in the top right of the web page to enter the **Device Language Settings** page. You can select a language for the device system from the drop-down list.

By default, the system language is English.

Note

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

7.6.3 Time Settings

Click in the top right of the web page to enter the wizard page. After setting device language, you can click **Next** to enter the **Time Settings** page.

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.

Server Address/NTP Port/Interval

You can set the server address, NTP port, and interval.

DST

You can view the DST start time, end time and bias time.

Click **Next** to save the settings and go to the next parameter. Or click **Skip** to skip time settings.

7.6.4 Environment Settings

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

Steps

1. Click in the top right of the web page to enter the wizard page. After setting device language and time, you can click **Next** to enter the **Environment Settings** page.
2. Select **Indoor** or **Other**.

Note

- 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.

Click **Next** to save the settings and go to the next paramater. Or click **Skip** to skip environment settings.

7.6.5 Privacy Settings

Set the picture uploading and storage parameters.

Click in the top right of the web page to enter the wizard page.

Picture Uploading and Storage

Save Picture When Authenticating

Save picture when authenticating automatically.

Upload Picture When Authenticating

Upload the pictures when authenticating to the platform automatically.

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.

Save Iris Picture

If enabled, the Iris pictures when registered will be saved to the device.

Click **Next** to save the settings and go to the next parameter. Or click **Skip** to skip privacy settings.

7.6.6 Administrator Settings

Steps

1. Click in the top right of the web page to enter the wizard page.
2. Enter the employee ID and name of the administrator.
3. Select a credential to add.

Note

You should select at least one credential.

1) Click **Add Face** to upload a face picture from local storage.

Note

The uploaded picture should be within 200 K, in JPG、JPEG、PNG format.

2) Click **Add Card** to enter the Card No. and select the property of the card.

Note

Up to 5 cards can be supported.

3) Click **Add Fingerprint** to add fingerprints.

Note

Up to 10 fingerprints are allowed.

4) Click **Add Iris**, add iris or select the picture from files.

7.6.7 No. and System Network

Steps

1. Click in the top right of the web page to enter the wizard page. After previous settings, you can click **Next** to enter the **No. and Network System Network** settings page.
2. Set the device type.

Note

- If set the device type as **Door Station**, you can set the **Floor No.**, **Door Station No.**, **Community No.**, **Building No.**, **Unit No.**, **Floor No.**, and **Door Station No.**.
- If set the device type as **Outer Door Station**, you can set **Outer Door Station No.**, and **Community No.**

Device Type

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

Community No.

Set the device community No.

Building No.

Set the device building No.

Unit No.

Set the device unit No.

Floor No.

Set the device installed floor No.

Door Station No.

Set the device installed door station No.

Note

The main door station No. is 0, and the sub door station No. ranges from 1 to 16.

Outer Door Station No.

Set the device installed outer door station No.

Note

The No. ranges from 1 to 99.

3. Set the video intercom network parameters.

Registration Password

Set the registration password of the main station for communication. Set the registration password of the main station for communication.

Main Station IP

Enter the main station's IP address that used for communication.

Private Server IP

Refers to the SIP server IP. Enter the main station's IP address that used for communication. At this time the main station is used as a SIP server. Other intercom devices should registered to this server address to realize communication.

Enable Protocol 1.0

If enabled, the door station can be registered to the main station by old protocol version. If disabled, the door station can be registered to the main station by new protocol version.

4. Click **Complete** to save the settings after the configuration.

7.7 Person Management

Click **Add** to add the person's information, including the basic information, certificate, authentication and settings.

Add Basic Information

Click **Person Management → Add** to enter the Add Person page.
Add the person's basic information, including the employee ID, the person's name, gender, and person type.
Click **Save** to save the settings.

Set Permission Time

Click **Person Management → Add** to enter the Add Person page.
Enable **Long-Term Effective User**, or set **Long-Term Effective User**, and the person can only has the permission within the configured time period according to your actual needs.
Set the door permission.
Click **Save** to save the settings.

Set Device No.

Click **Person Management → Add Person → Add** to enter the Add Person page.
Click the textbox of **Floor No.** and **Room No.** and enter a numeric between 1 and 999 to set the floor No. and room No.
Click **Save** to save the settings.

Authentication Settings

Click **Person Management → Add** to enter the Add Person page.
Set the authentication type.
Click **Save** to save the settings.

Add Card

Click **Person Management → Add** to enter the Add Person page.

Click **Add Card**, enter the **Card No.** and select the **Property**, and click **OK** to add the card.
Click **Save** to save the settings.

Add Face Picture

Click **Person Management → Add** to enter the Add Person page.
Click **+ Upload** to upload a face picture from the local PC.

Note

The picture format should be JPG or JPEG or PNG, and the size should be less than 200 kb.

Click **Save** to save the settings.

Add Fingerprint

Note

Only devices supporting the fingerprint function can add the fingerprint.

Click **Person Management → Add** to enter the Add Person page.
Click **Add Fingerprint**, and press your finger on the fingerprint module of the device to add your fingerprint.
Click **Save** to save the settings.

Add Iris

Click **Person Management → Add** to enter the Add Person page.
Click to add the iris or click **Upload** to upload from the file.
Click **OK** to save the settings.

Device No. Settings

Click **Person Management → Add** to enter the Add Person page.
Add the person's basic information. Go to the Device No. module. Click **Add** and enter the person belonged room No. and floor No. Click **Add** or **Save and Continue**.

Delete Person

On the person management page, check the person need to delete and click **Delete**.
Click **Clear All** to clear all person.

Edit Person

On the person management page, check the person need to edit. Click to edit the person information.

Filter

On the person management page, enter **Employee ID / Name / Card No.**. Select **Credential Status**, and click **Filter** to filter the person. Click **Reset** to clear all conditions.

7.8 Access Control Management

7.8.1 Overview

You can view the live video of the device, linked device, person information, network status, basic information, and device capacity.

Function Descriptions:

Door Status

Click on the video to view the device live video.

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.

/ / /

The door status is open/closed/remaining open/remaining closed.

You can record when starting live view.

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

Full screen view.

Controlled Status

You can control the door to be opened, closed, remaining open or remaining closed according to your actual needs.

Real-Time Event

You can view the event Employee ID, Name, Card No., Event Type, Time, and Operation. You can also click **View More** to enter the page of Event Search. You can select event types, enter 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.

Link Device

You can view the quantity and status of linked devices.

Note

You can click **View More** to go to .

Person Information

You can view the added and not added information of person credentials.

Network Status

You can view the connected and registered status of wired network, wireless network, Hik-Connect, ISUP, OTAP, and VoIP.

Basic Information

You can view the model, serial No. and firmware version.

Device Capacity

You can view the person, face, fingerprint, card, iris and event capacity.

Note

Only device installed fingerprint module can display the fingerprint capacity.

7.8.2 Search Event

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

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

The results will be displayed on the right panel.

7.8.3 Door Parameter Configuration

Configure parameters for unlocking doors.

Select Door No.

Select a door to configure relative parameters.

Click **Access Control → Parameter Settings → Door Parameters** to enter the settings page.

Select **Door No.**. Usually, Door 1 is the door linked with the device and door 2 is the door linked with the secure door control unit.

Set other door parameters and click **Save**.

View Device Online Status

View and refresh the device status.

Click **Access Control → Parameter Settings → Door Parameters** to enter the settings page.

You can view the online status of the device. Click **Refresh** to refresh the status of the device.

Set Door Name

Create door name.

Click **Access Control → Parameter Settings → Door Parameters** to enter the settings page.

Set **Door Name** and click **Save**.

Set Open Duration via PC Web

You can set the time for the door lock to open after swiping the card.

Click **Access Control → Parameter Settings → Door Parameters** to enter the settings page.

Set the open duration, that is the action time after the door is unlocked. If the door is not opened within the set time, the door will automatically lock. Configurable time: 1 to 255 seconds.

Click **Save**.

Set Door Open Timeout Alarm via PC Web

If the door is not closed after reaching the lock action time, the access control point will sound an alarm.

Click **Access Control → Parameter Settings → Door Parameters** to enter the settings page.

Set **Door Open Timeout Alarm**. If the door is not closed after reaching the lock action time, the access control point will sound an alarm. When set as 0, alarm will not be enabled.

Click **Save**.

Set Door Magnetic Sensor Type via PC Web

You can select door contact type according to the wiring method.

Click **Access Control → Parameter Settings → Door Parameters** to enter the settings page.

Select magnetic sensor type as remain closed or remain open. By default, it is **Remain Closed** (excluding special needs).

Click **Save**.

Set Exit Button via PC Web

Set the exit button as remain open or remain closed according to the actual wiring method.

Click **Access Control → Parameter Settings → Door Parameters** to enter the settings page.

Set **Exit Button Type**. By default, it is Remain Open (excluding special needs).

Click **Save**.

Set Door Lock Powering Off Status via PC Web

You can set the door lock status when the door lock is powering off.

Click **Access Control → Parameter Settings → Door Parameters** to enter the settings page.

Set **Door Lock Powering Off Status**. By default, it is remain closed.

Click **Save**.

Set Extended Open Duration via PC Web

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

Click **Access Control → Parameter Settings → Door Parameters** to enter the settings page.

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

Click **Save**.

Set Door Remain Open Duration with First Person via PC Web

After the first person is authorized, it allows multiple persons access the door or other authentication actions.

Click **Access Control → Parameter Settings → Door Parameters** to enter the settings page.

Set the door open duration when first person is in and click **Save**.

Set Duress Code via PC Web

After configuring duress code, when encountering duress, enter the code to open the door. At the same time, the access control system will report duress events.

Click **Access Control → Parameter Settings → Door Parameters** to enter the settings page.

Set duress code, and click **Save**.

Note

Duress code and super password can’t be duplicated, usually consisting of 4 to 8 digits.

Set Super Password via PC Web

Administrator or designated person can enter the super password to open the door.

Click **Access Control → Parameter Settings → Door Parameters** to enter the settings page.

Set **Super Password**, the designated person can enter the super password to open the door.

Click **Save**.

Note

Duress code and super password can't be duplicated, usually consisting of 4 to 8 digits.

7.8.4 Authentication Settings

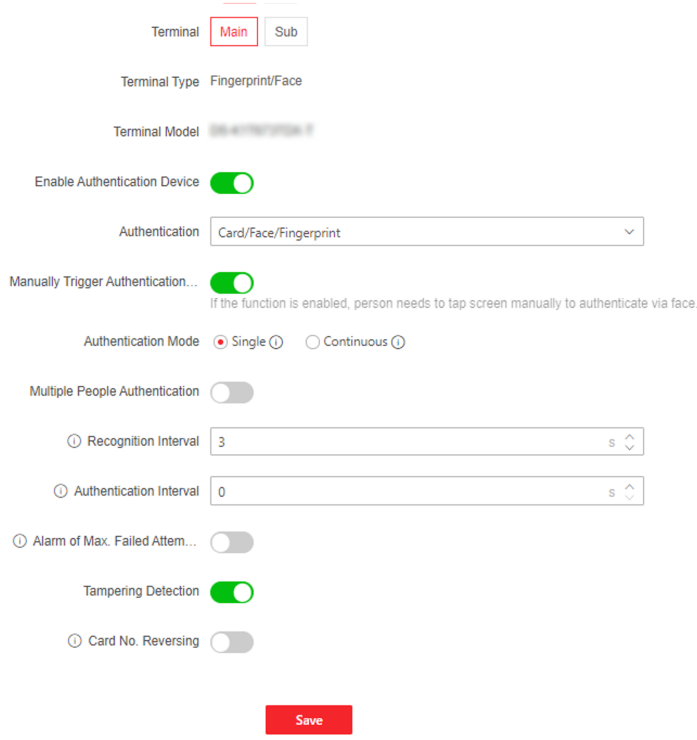


Figure 7-2 Authentication Settings

Select Main or Sub Card Reader via PC Web

Set the terminal for person authentication.

Click **Access Control → Parameter Settings → Authentication Settings** to enter the settings page.

Select the terminal as main or sub card reader.

Set other parameters and click **Save**.

View Terminal Type and Model via PC Web

You can view terminal type and model.

Click **Access Control → Parameter Settings → Authentication Settings** to enter the settings page.

View **Terminal Type** and **Terminal Model**.

Enable Authentication Device via PC Web

After enabling, the authentication terminal can be used for card swiping.

Steps

1. Click **Access Control → Parameter Settings → Authentication Settings** to enter the settings page.
2. Enable **Authentication Device**. After enabling, the terminal can be used for card swiping normally.
3. Click **Save**.

Set Recognition Interval via PC Web

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

Click **Access Control → Parameter Settings → Authentication Settings** to enter the settings page.

When you select the terminal as main or sub card reader, set recognition interval, and click **Save**.

Note

Please enter a number between 1 and 10.

Set Authentication Interval via PC Web

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. If other person authenticate in the configured interval, the person can authenticate again.

Click **Access Control → Parameter Settings → Authentication Settings** to enter the settings page.

When you select the terminal as main card reader, set **Authentication Interval**, and click **Save**.

Enable Alarm of Max. Failed Attempts via PC Web

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

Click **Access Control → Parameter Settings → Authentication Settings** to enter the settings page.

When you select the terminal as main or sub card reader, slide to enable **Alarm of Max. Failed Attempts**, and set **Max. Authentication Failed Attempts**.

Click **Save**.

Enable/Disable Tampering Detection via PC Web

You can enable tampering detection, the device will automatically generate tampering events when the card reader is removed or taken away.

Click **Access Control → Parameter Settings → Authentication Settings** to enter the settings page.

Enable or disable **Tampering Detection** according to your actual needs. After enabling the function, the device will automatically generate tampering events when the card reader is removed or taken away. If the function is disabled, no alarm events will be generated.

Click **Save**.

Set Sub Card Reader Position

You can choose the position for the sub card reader.

Click **Access Control → Parameter Settings → Authentication Settings** to enter the settings page.

When Sub Card Reader is selected as the Terminal, you can select the position of sub card reader as **Different Side from Main Card Reader**or**Same Side as Main Card Reader**. Click**Save**.

Set Communication with Controller Every via PC Web

You can set communication with controller every of sub card reader. If the card reader can't connect with the access controller in the set time, the card reader is offline.

Click **Access Control → Parameter Settings → Authentication Settings** to enter the settings page.

When you select the terminal as sub card reader, set **Communication with Controller Every**, and click **Save**.

Set Timeout Duration of Entering Password via Web Client

Set the maximum interval of entering two characters of the password. After entering one character, if the next character is not entered within the set interval, the entered characters will all be automatically cleared.

Click **Access Control → Parameter Settings → Authentication Settings** to enter the settings page.

When selecting the sub card reader as the Terminal, you can set **Max. Interval When Entering Password** and click**Save**.

Set OK LED Polarity and Error LED Polarity via PC Web

Select the polarity of the diodes for OK and ERR interfaces according to actual wiring, with a default positive polarity.

Click **Access Control → Parameter Settings → Authentication Settings** to enter the settings page.

When you select the terminal as sub card reader, set **OK LED Polarity** and **Error LED Polarity**, and click **Save**.

Set Authentication Plan

You can set authentication plan.

Click **Access Control → Parameter Settings → Authentication Settings** to enter the settings page.

Select the authentication type and drag the time period in the time bar.

Click **Save**.

7.8.5 Set Face Parameters

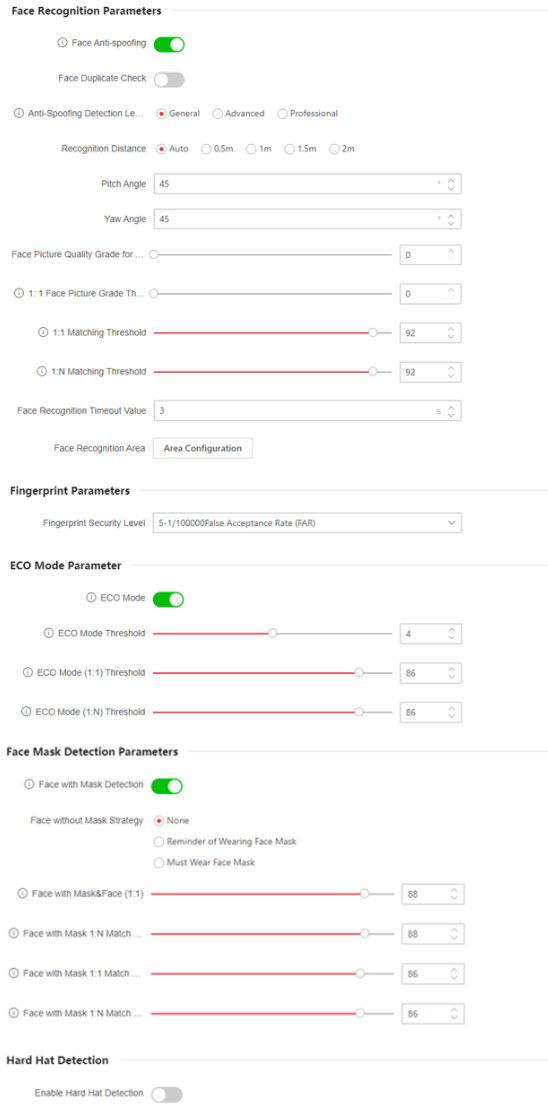


Figure 7-3 Set Face Parameters

Enable/Disable Face Anti-spoofing via Web Browser

When enabled, the device can recognize whether the person is a live one or not.

Click **Access Control → Parameter Settings → Smart** to enter the settings page.

Enable **Face Anti-spoofing** and click **Save**.

Enable or disable the live face detection function. When enabled, the device can recognize whether the person is a live one or not. If the face is not a live one, authentication will fail.

Set Anti-Spoofing Detection Level via PC Web

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

Click **Access Control → Parameter Settings → Smart** to enter the settings page.

Select the anti-spoofing detection level and click **Save**.

You can choose from general, advanced and professional. The higher the level, the lower the fake recognition rate and the higher the rejection rate.

Set Recognition Distance via PC Web

You can set the distance between the authenticating user and the device camera.

Click **Access Control → Parameter Settings → Smart** to enter the settings page.

Select the recognition distance, and click **Save**.

Set Application Mode and Installation Angle

You can set the application mode and installation angle.

Click **Access Control → Parameter Settings → Smart** to enter the settings page.

Select the **Application Mode** and **Installation Angle**, and click **Save**.

Set Pitch Angle via PC Web

You can set the pitch angle of the lens during face recognition and authentication.

Click **Access Control → Parameter Settings → Smart** to enter the settings page.

Note

Different models may support different parameters, please refer to the actual page.

Set **Pitch Angle** and click **Save**.

Set Yaw Angle via PC Web

You can set the yaw angle of the lens during face recognition and authentication.

Click **Access Control → Parameter Settings → Smart** to enter the settings page.

Note

Different models may support different parameters, please refer to the actual page.

Set yaw angle, and click **Save**.

Set Face Picture Quality Grade for Applying via PC Web

The grade for face authentication needs to be higher than the threshold to be successful.

Click **Access Control → Parameter Settings → Smart** to enter the settings page.

Note

Different models may support different parameters, please refer to the actual page.

Set **Face Picture Quality Grade for Applying** , the grade for face authentication needs to be higher than the threshold to be successful.

Click **Save**.

Set 1:1 Face Grade Threshold via PC Web

Set 1:1 face grade threshold.

Go to **Access Control → Parameters Settings → Smart** .

Set **1:1 Face Picture Grade Threshold**, and click **Save**.

The higher the threshold, the higher the requirements for the quality of the captured images of the front camera, and the easier to prompt authentication failure.

Set Face 1:1 Matching Threshold via PC Web

Set face 1:1 matching threshold.

Click **Access Control → Parameter Settings → Smart** to enter the settings page.

Set face 1:1 matching threshold and click **Save**.

The larger the value of the threshold, the fault acceptance rate will be lower and the false rejection rate will be higher when authenticating via face. The maxium value is 100.

Set 1:N Matching Threshold via PC Web

You can set the matching threshold for face 1:N matching.

Click **Access Control → Parameter Settings → Smart** to enter the settings page.

Set the 1:N matching threshold and click **Save**.

The larger the value, the smaller the false accept rate and the larger the false rejection rate. The maximum value is 100.

Set Face Recognition Area via Web Browser

You can set the recognition area of the lens during face recognition and authentication.

Click **Access Control → Parameter Settings → Area Configuration** to enter the settings page.

Drag the yellow box in the preview screen to adjust the effective area for face recognition on the left, right, up, and down sides.

Or drag the block or enter the number to set the effective area.

Click **Save**.

Click , , or to capture, record, or go to full screen view.

Set Fingerprint Parameters via PC Web

You can set the fingerprint parameters of the device.

Click **Access Control → Parameter Settings → Smart** to enter the settings page.

Select **Fingerprint Security Level**. The higher the level, the lower the fake recognition rate and the higher the rejection rate.

Click **Save**.

Iris Settings

Steps

1. Click **Access Control → Parameter Settings → Smart** to enter the settings page.
2. Set the following parameters.

Iris Anti-Spoofing Detection

Enable or disable the iris detection function. If enabling the function, the device can recognize whether the iris is a true one or not.

Note

Biometric recognition products are not 100% applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.

Iris Liveness Security Level

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

Iris Recognition Interval

The time interval between two continuous iris recognitions when authenticating.

Iris 1:N Security Level (Single-Eye)

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

Iris 1:N Security Level (Dual-Eye)

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

3. Set the single-eye or dual-eye or auto recognition mode.

Single-eye Recognition Mode

Single-eye recognition mode allows you to authenticate via single eye.

Dual-eye Recognition Mode

Dual-eye recognition mode allows you to authenticate via dual eyes.

Auto Recognition Mode

Auto recognition mode allows you to authenticate automatically.

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

Enable/Disable ECO Mode via PC Web

If the ECO mode is enabled, you can authenticate faces in the low light or dark environment with IR camera.

Click **Access Control → Parameter Settings → Smart** to enter the settings page.

If the ECO mode is enabled, you can authenticate faces in the low light or dark environment with IR camera. You can set the ECO mode (1:N) and ECO mode (1:1).

If the face with mask detection is enabled, you can set face mask detection parameters also.

ECO Mode (1:1) Threshold

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. The maximum value is 100.

ECO Mode (1:N) Threshold

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. The maximum value is 100.

Face with Mask 1:1 Match Threshold (ECO)

Set the matching threshold when authenticating with face mask via ECO mode 1:1 matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate. The maximum value is 100.

Face with Mask 1:N Match Threshold (ECO)

Set the matching threshold when authenticating with face mask via ECO mode 1:N matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate. The maximum value is 100.

Click **Save**.

Enable/Disable Face with Mask Detection via PC Web

After enabling the face with mask detection, the system will recognize the captured face with mask picture or not.

Click **Access Control → Parameter Settings → Smart** to enter the settings page.

After enabling the face with mask detection, you can set **Face without Mask Strategy**, **Face with Mask&Face (1:1)**, **Face with Mask 1:N Match Threshold (ECO)**, **Face with Mask 1:1 Match Threshold** and **Face with Mask 1:N Match Threshold (ECO)**.

Face without Mask Strategy

You can select **None**, **Reminder of Wearing Face Mask** and **Must Wear Face Mask**.

Reminder of Wearing Face Mask

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

Must Wear Face Mask

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

Face with Mask&Face (1:1)

Set the matching value when authenticating with face mask via 1:1 matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate. The maximum value is 100.

Face with Mask&Face (1:N)

Set the matching threshold when authenticating with face mask via 1:N matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate. The maximum value is 100.

Face with Mask 1:1 Match Threshold (ECO)

Set the matching value when authenticating with face mask via ECO mode 1:1 matching mode. The larger the threshold, the lower the recognition error rate and the higher the rejection rate when authenticating faces. The maximum value is 100.

Face with Mask 1:N Match Threshold (ECO)

Set the matching value when authenticating with face mask via ECO mode 1:N matching mode. The larger the threshold, the lower the recognition error rate and the higher the rejection rate when authenticating faces. The maximum value is 100.

Click **Save**.

Enable/Disable Hard Hat Detection via PC Web

After enabling the hard hat detection, the system will recognize whether the safety helmet is worn when authenticating faces.

Click **Access Control → Parameter Settings → Smart** to enter the settings page.

Enable **Hard Hat Detection** and click **Save**.

Enable Hard Hat Detection

You can set the reminder strategy.

Reminder of Wearing

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

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

7.8.6 Card Settings

Enable/Disable NFC Protection via PC Web

After enabling, the device can read NFC card.

Click **Access Control → Parameter Settings → Card Settings** to enter the settings page.

Click to **Enable NFC Card** and click **Save**. After enabling, the device can read NFC card. If the data of access control devices is obtained by mobile devices, the situation of unauthenticated access may occur. To prevent this situation, you can disable NFC function.

Enable/Disable M1 Card via Web Client

After enabling, the device can recognize M1 card and users can swipe M1 card via the device.

Click **Access Control → Parameter Settings → Card Settings** to enter the settings page.

Click to **Enable M1 Card**.

M1 Card Encryption

Enable M1 Card Encryption can improve the security level of the entrance card. Therefore, the entrance card will be harder to be copied.

Sector

After enabling M1 Card Encryption, you will need to set the encrypted sector.

Note

You are advised to encrypt sector 13.

Click **Save**.

Enable/Disable EM Card via Web Client

After enabling, the device can recognize EM card and users can swipe EM card via the device.

Click **Access Control → Parameter Settings → Card Settings** to enter the settings page.

Click to **Enable EM Card** and click **Save**.

Note

If the peripheral card reader which can read EM card is connected, after enabling this function, you can also swipe EM card via this card reader.

Enable/Disable CPU Card via Web Client

After enabling, the device can recognize CPU card and users can swipe CPU card via the device.

Click **Access Control → Parameter Settings → Card Settings** to enter the settings page.

Click to **Enable CPU Card**.

Click to **Enable CPU Card Read Content**. After enabling, the device can read content from CPU card.

Click **Save**.

Set DESFire Card

You can enable DESFire card and DESFire card read content.

Click **Parameter Settings → Card Settings** to enter the settings page.

Select **Enable DESFire Card** and **DESFire Card Read Content**and click **Save**.

Set FeliCa Card

You can enable FeliCa card.

Click **Parameter Settings → Card Settings** to enter the settings page.

Select **Enable FeliCa Card**.

Set Card No. Authentication Parameters via Web

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

Go to **Access Control → Parameter Settings → Card Settings** .

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

Full Card No.

All card No. will be read.

3 bytes

The device will read card via read 3 bytes.

4 bytes

The device will read card via 4 bytes.

7.8.7 Set Working Mode via PC Web

You can set the terminal parameters of the device.

Note

Only some models support this function, please refer to the specific device.

Click **Access Control → Parameter Settings → Terminal Parameters** to enter the settings page.

Working Mode

You can set the working mode as access control mode or permission free mode.

Access Control Mode

The access control mode is the device normal mode. You should authenticate your credential for accessing.

7.8.8 Privacy Settings

Set Event Storage Type via PC Web Browser

You can configure the event storage type.

Click **Access Control → Parameter Settings → Privacy Settings** to enter the settings page.

You can select **Event Storage Type** as **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.

Click **Save**.

Set Authentication Result via PC Web

Set authentication result contents, such as picture, name, employee ID, and temperature.

Click **Access Control → Access Control → Parameter Settings → Privacy Settings** .

Check the displayed contents in the authentication result, such as picture, name, employee ID.

Check **Name De-identification** and **ID De-identification** according to actual needs. After de-identification, the name and the ID will display parts of contents.

Set **Authentication Result Display Duration** and the authentication result will display the configured time duration.

Click **Save**.

Configure Picture Uploading and Storage via PC Web

You can set picture uploading and storage parameters.

Click **Access Control → Parameter Settings → Privacy Settings** to enter the settings page.

Save Picture When Auth.

Save picture when authenticating automatically.

Upload Picture When Auth.

Upload the pictures when authenticating to the platform automatically.

Save Registered Picture

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

Save Pictures After Linked Capture

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

Upload Picture After Linked Capture

Upload the pictures captured by linked camera to the platform automatically

Save Iris Picture

If enabled, the Iris pictures when registered will be saved to the device.

Click **Save**.

Clear Device Pictures via PC Web

You can clear all registered, authenticated or captured face or pictures.

Click **Access Control → Parameter Settings → Privacy Settings** to enter the settings page.

Click **Clear** to clear all registered, captured face pictures or registered iris pictures.

7.8.9 Call Settings

Set Device No. via Web

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

Click **Access Control → Call Settings → Device No.** .

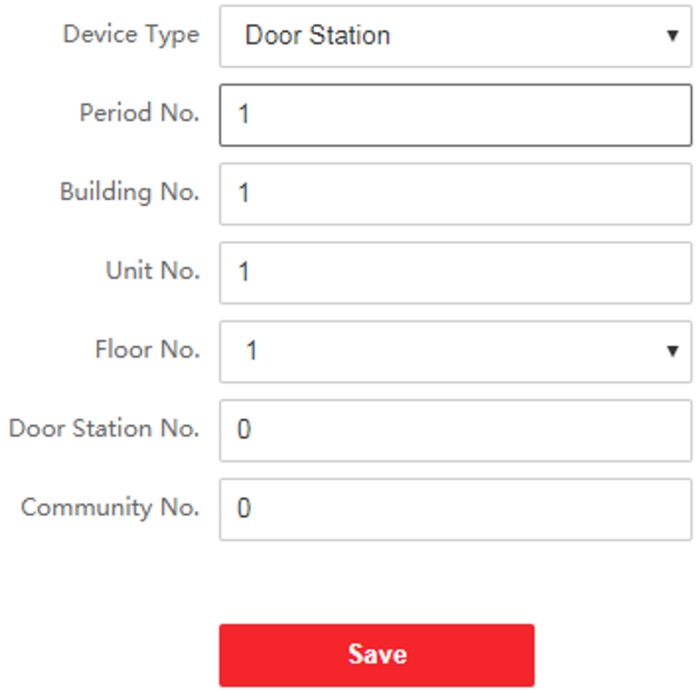


Figure 7-4 Device No. Settings

If set the device type as **Door Station**, you can set the **Floor No.**, **Door Station No.**, **Community No.**, **Building No.**, and **Unit No.**

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.

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.
- The main door station No. is 0, and the sub door station No. ranges from 1 to 16.

Community No.

Set the device community No.

Building No.

Set the device building No.

Unit No.

Set the device unit No.

Note

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

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

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

Configure Video Intercom Network Parameters via Web Browser

You can set the registration password, main station IP and private server IP.

Click **Call Settings → Video Intercom Network** to enter the settings page.

Main Station IP

Enter the main station's IP address that used for communication.

SIP Server IP Address

Refers to the SIP server IP. Enter the main station's IP address that used for communication. At this time the main station is used as a SIP server. Other intercom devices should registered to this server address to realize communication.

After configuration, you can achieve communication between access control devices and video intercom door station, indoor station, main station, platforms, etc.

Click **Save**.

Press Button to Call via PC Web

Steps

1. Click **Access Control → Call Settings → Press Button to Call** to enter the settings page.

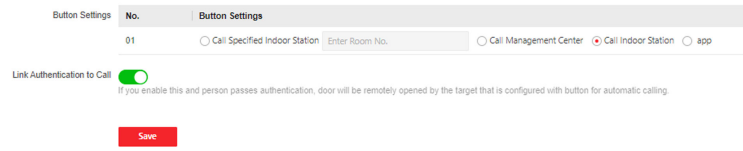


Figure 7-5 Press Button to Call

2. Select **Call Specified Indoor Station**, **Call Management Center**, **Call Indoor Station** or **APP** at your needs.

Note

If you select **Call Specified Indoor Station**, you need to enter the **Room No.** of the indoor station.

3. Enable **Link Authentication to Call** according to your needs. After enabled, when person passes authentication, the door will be remotely opened by the target that is configured with button for automatic calling.
4. Click **Save**.

7.9 System Configuration

7.9.1 Set Local Parameters

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

Set Live View Parameters

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

Set Record File Size and Saving Path

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

Set Captured Pictures and Clips Saving Path

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

7.9.2 View Device Information via PC Web

View the device name, device No., language, model, serial No., version, number of channels, IO input, IO output, lock, alarm input, alarm output, and device capacity, etc.

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

You can view the device name, device No., language, model, serial No., version, number of channels, IO input, IO output, lock, alarm input, alarm output, and device capacity, etc.

Click **Upgrade** in the Firmware Version, you can go to the upgrade page to upgrade the device.

7.9.3 Set Time

Set the device's time zone, synchronization mode, server address, NTP port, and interval.

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

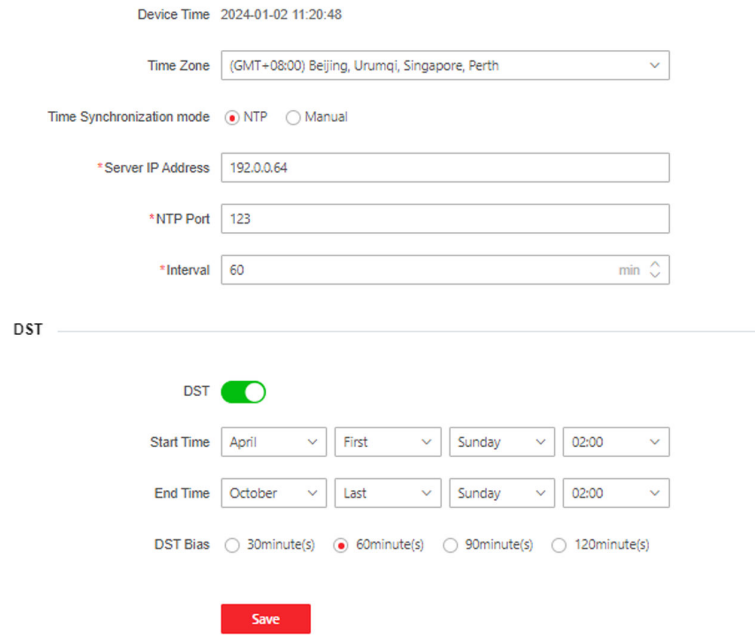


Figure 7-6 Time Settings

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.

Server Address Type/Server Address/NTP Port/Interval

You can set the server address type, server address, NTP port, and interval.

7.9.4 Change Administrator's Password

Steps

1. Click **System and Maintenance → System Configuration → System → User Management → User Management** .
2. Click ✎ .

3. Enter the old password and create a new password.
4. Confirm the new password.
5. Click **Save**.

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.

7.9.5 Account Security Settings via PC Web

You can change the security questions and answers, or the email address for the device. After change the settings, once you forgot the device password, you should answer the new questions or use the new email address to reset the device password.

Steps

1. Click **System and Maintenance → System Configuration → System → User Management → User Management → Account Security Settings** .
2. Change the security questions or email address according your actual needs.
3. Enter the device password and click **OK** to confirm changing.

7.9.6 View Device Arming/Disarming Information via PC Web

View device arming type and arming IP address.

Go to **System and Maintenance → System Configuration → System → User Management → Arming/Disarming Information** .

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

7.9.7 Network Settings

Set Basic Network Parameters via PC Web

Click **System and Maintenance → System Configuration → Network → Network Settings → TCP/IP** .

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

NIC Type

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

DHCP

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

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

DNS Server

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

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 **System and Maintenance → System Configuration → Network → Network Settings → Wi-Fi** .

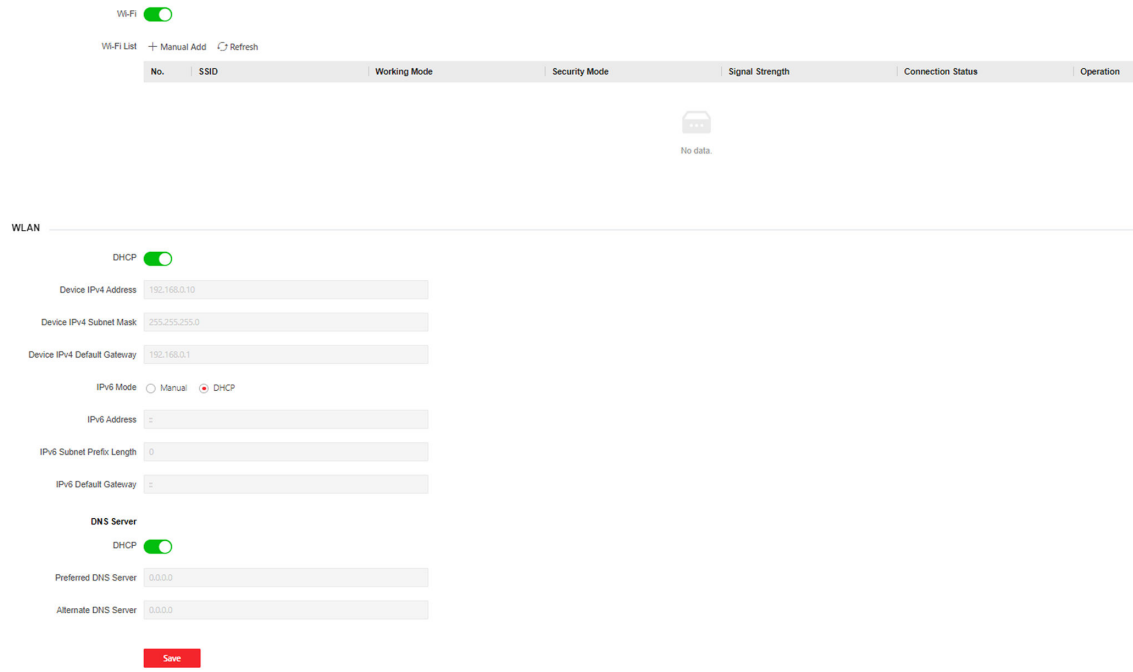


Figure 7-7 Wi-Fi Settings Page

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) Set the IP address, subnet mask, and default gateway. Or enable **DHCP** and the system will allocate the IP address, subnet mask, and default gateway automatically.
5. Click **Save**.

Set Port via PC Web

Go to **System and Maintenance → System Configuration → Network → Network Service** .

Enable/Disable HTTP

Enable the HTTP function to improve the broswer's visiting security.

Go to **System and Maintenance → System Configuration → Network → Network Service → HTTP(S)** .

Click**Save** after parameters are configured.

HTTP Port

When you log in with a browser, you need to add the modified port number after the address. For example, when the HTTP port number is changed to 81, you need to enter http://192.0.0.65：81 when you log in with a browser.

HTTPS Port

Set the HTTPS port for visiting browser. But certification is required.

HTTP Listening

The device will send the alarm information to the destination IP or domain name by HTTP protocol. The destination IP or domain name should support HTTP protocol. Enter the destination IP or domain name, URL and port. And select the protocol type.

View RTSP Port via PC Web

The RTSP port is the port of real-time streaming protocol.

Go to **System and Maintenance → System Configuration → Network → Network Service → RTSP** .

View the Port.

Enable SDK Service

After enabling SDK service, the device can be connected to the SDK server.

Click **System and Maintenance → System Configuration → Network → Device Access → SDK Server** to enter the settings page.

Enter **Server Port**.

Click **Save** to enable the settings.

Set ISUP Parameters via PC Web

Set the ISUP parameters for accessing device via ISUP protocol.

Steps

Note

The function should be supported by the device.

1. Click **System and Maintenance → System Configuration → Network → Device Access → ISUP** .
2. Check **Enable**.
3. 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 encryption key as well.
4. Set the ISUP listening parameters, including ISUP alarm center IP address/domain name, ISUP alarm center URL, and ISUP alarm center port.
5. Click **Save**.

Platform Access via PC Web

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

Steps

1. Click **System and Maintenance → System Configuration → Network → Device Access → Hik-Connect** to enter the settings page.

   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.
2. Check **Enable** to enable the function.
3. **Optional:** Check the checkbox of **Custom**, and you can set the server address by yourself.
4. Enter the verification code.
5. Click **View** to view device QR code. Scan the QR code to bind the account.

Note

8 to 32 letters (a to z, A to Z) or numbers (0 to 9), case sensitive. You are recommended to use a combination of no less than 8 letters or numbers.

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

7.9.8 Set Video and Audio Parameters via PC Web

Configure Video Parameters via Web Browser

You can set quality, resolution and other parameters of device camera.

Click **System and Maintenance → System Configuration → Video/Audio → Video** to enter the settings page.

Set camera name, stream type, video type, resolution, bit rate type, video quality, frame rate, Max. bitrate, video encoding and I frame interval.

Click **Save**.

Configure Audio Parameters via PC Web

You can set device volume.

Go to **System and Maintenance → System Configuration → Video/Audio → Audio**.

Set stream type and audio encoding according to your actual needs. Slide to set input and output volume.

Slide to enable **Voice Prompt**.

Tap **Save**.

7.9.9 Image Parameter Settings

Set Brightness/Contrast/Saturation/Sharpness via PC Web

You can set picture information such as brightness, contrast, saturation and sharpness of live view page.

Click **System and Maintenance → System Configuration → Image → Display Settings** to enter the settings page.

Image Adjustment

Drag the block or enter numbers to set brightness, contrast, saturation and sharpness.

Click **Restore Default Settings** to restore the to the default.

Set LED Light via PC Web

You can adjust the brightness of the supplement light.

Steps

1. Click **System and Maintenance → System Configuration → Image → Display Settings** to enter the settings page.
2. Set the type, mode and brightness of the supplement light.
3. **Optional:** Click **Restore Default Settings** to restore the to the default.

Set WDR via PC Web

Click **System and Maintenance → System Configuration → Image → Display Settings** to enter the settings page.

Enable or disable wide dynamic range. After enabling, both bright and dark parts of the scene can be seen more clearly at the same time.

Click **Restore Default Settings** to restore the to the default.

Set Video Standard via PC Web

You can set the video standard of live view page.

Click **System and Maintenance → System Configuration → Image → Display Settings** to enter the settings page.

Video Adjustment

Set the video frame rate during remote preview. You need to reboot the device to make the new settings effective.

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.

Click **Restore Default Settings** to restore the to the default.

7.9.10 Alarm Settings via PC Web

Set the alarm output parameters.

Steps

1. Click **System and Maintenance → System Configuration → Event → Alarm Settings → Alarm Output** .
2. Set **Alarm Name** and mode of **Alarm Duration**.

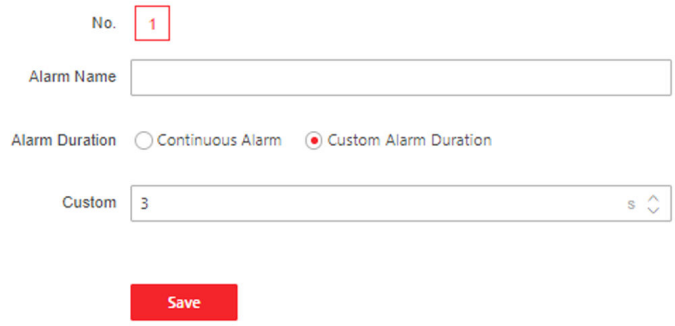


Figure 7-8 Alarm Settings

Continuous Alarm

When the alarm is triggered, it will alarm continuously.

Custom Alarm Duration

You can set **Alarm Duration** for the device when the alarm is triggered.

7.9.11 Access Configuration

Set RS-485 Parameters via PC Web

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

Click **System and Maintenance → System Configuration → Access Configuration → RS-485** .

Check **Enable RS-485**, and set the parameters.

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 via PC Web

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 **System and Maintenance → System Configuration → Access Configuration → Wiegand Settings** .

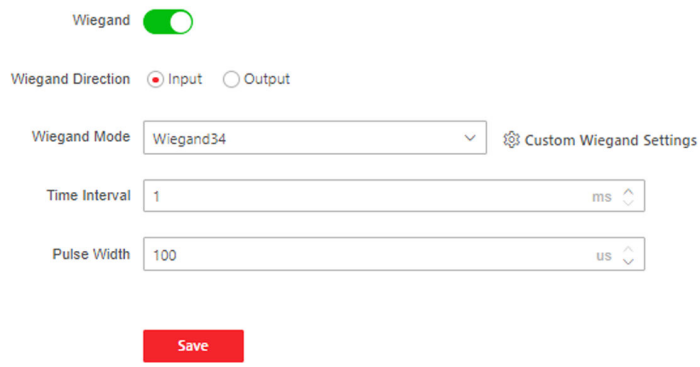


Figure 7-9 Wiegand Page

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.

7.9.12 Time and Attendance Settings

If you want to record the person's working hour, late arrivals, early departures, breaks, absenteeism, etc., 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.

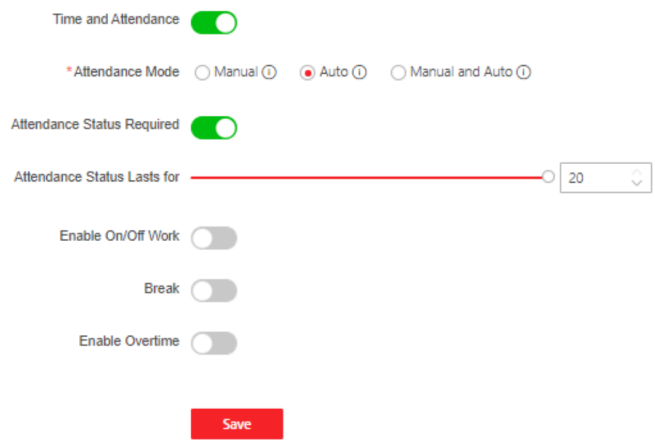


Figure 7-10 Time and Attendance

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 **System and Maintenance → System Configuration → Platform Attendance** to enter the settings page.
2. Disable the **Time and Attendance**.

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.

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 **System and Maintenance → System Configuration → Platform Attendance** to enter the settings page.
2. Set the **Attendance Mode** as **Manual**.
3. Enable the **Attendance Status Required** and set the attendance 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 **System and Maintenance → System Configuration → Platform Attendance** to enter the settings page.
2. Set the **Attendance Mode** as **Auto**.
3. Enable the **Attendance Status Required** 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 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 **System and Maintenance → System Configuration → Platform Attendance** to enter the settings page.
2. Set the **Attendance Mode** as **Manual and Auto**.
3. Enable the **Attendance Status Required** 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 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.

7.10 Preference Settings

7.10.1 Set Sleep Time via PC Web

The device will in sleep mode after the configured time duration. The function can reduce power consumption.

Go to **System and Maintenance → Preference → Screen Display** .



Figure 7-11 Sleep Settings

Slide **Sleep** and set the sleep time.

Click **Save**.

7.10.2 Customize Authentication Desk via PC Web

Customize the modules on the authentication page/desk.

Steps

1. Go to **System and Maintenance → Preference → Custom Home Page** .
2. Select **Application Mode**.

   Authentication Mode

   The device authentication page will display the live view page. And the person's name, employee ID, face pictures will all be displayed after authentication.

   Ad in Full Screen

   The ad takes up the full screen of authentication page. Screensaver, Welcome Message can be played in ad.

   Simple Mode

   After selecting this mode, the live view of the authentication page will be disabled. The person's name, employee ID, face pictures will all be hidden after authentication.
3. Click **Apply**.

7.10.3 Set Notice Publication via PC Web

You can set the notice publication for the device.

Go to **System and Maintenance → Preference → Notice Publication** .

Material Management

You can click **+ Add Theme**, and set **Theme Name** and **Theme Type**.

Click **Upload**, and click **+** to upload the picture or video from the local PC.

Note

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

Add Program

You can set the program name and select program type.

Picture

If you select picture, you can click **+** to add picture.

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 and video will be changed according to the interval.

7.10.4 Set Prompt Schedule via PC Web

Customize the output audio content when authentication succeeded and failed.

Steps

1. Go to **System and Maintenance → Preference → Prompt Schedule** .

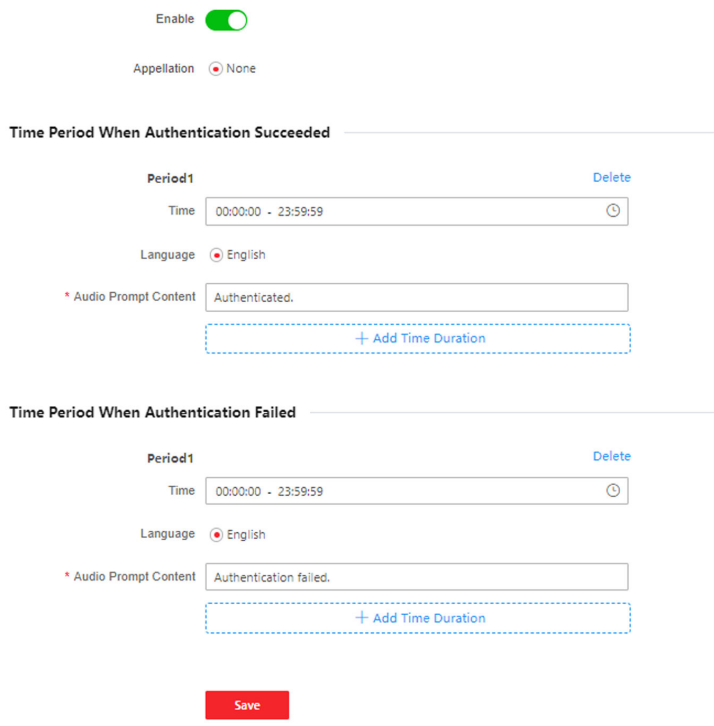


Figure 7-12 Prompt Schedule

2. Enable the function.
3. Set the appellation.
4. Select time schedule.
5. Set the time period when authentication succeeded.
   1) Click **Add Time Duration**.
   2) Set the time duration.

   Note

   If authentication is succeeded in the configured time duration, the device will broadcast the configured content.
   3) Set the audio prompt content.
   4) **Optional:** Repeat substep 1 to 3.
   5) **Optional:** Click to delete the configured time duration.
6. Set the time duration when authentication failed.
   1) Click **Add Time Duration**.
   2) Set the time duration.

   Note

   If authentication is failed in the configured time duration, the device will broadcast the configured content.
   3) Set the audio content.
   4) **Optional:** Repeat substep 1 to 3.
   5) **Optional:** Click to delete the configured time duration.
7. Click **Save** to save the settings.

7.10.5 Customize Prompt Voice via PC Web

You can customize prompt voices for the device.

Steps

1. Go to **System and Maintenance → Preference → Custom Prompt** .



Figure 7-13 Custom Prompt

2. Click → and import audio file from local PC according to your actual needs.

Note

The uploaded audio file should be less than 512 kb, in WAV format.

7.10.6 Set Authentication Result Text via PC Web

Steps

1. Go to **System and Maintenance → Preference → Authentication Result Text** .

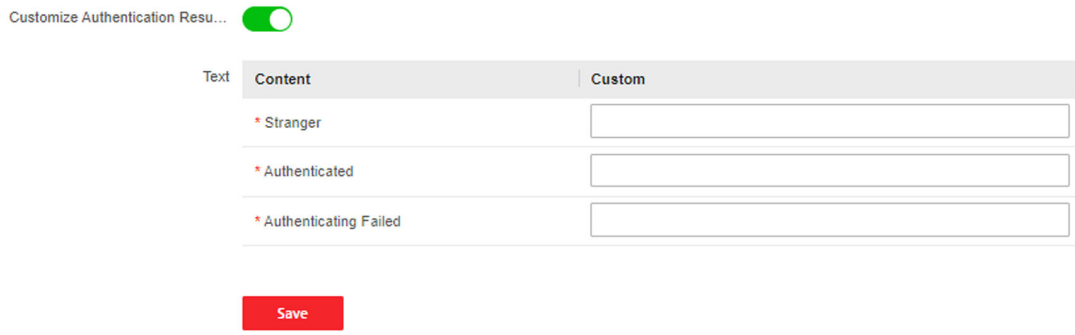


Figure 7-14 Authentication Result Text

2. Enable **Customize Authentication Result Text**.
3. Enter custom texts.
4. Click **Save**.

7.11 System and Maintenance

7.11.1 Reboot

You can reboot the device.

Click **System and Maintenance → Maintenance → Restart** to enter the settings page.

Click **Restart** to reboot the device.

7.11.2 Upgrade

Upgrade Locally via PC Web

You can upgrade the device locally.

Click **System and Maintenance → Maintenance → Upgrade** to enter the settings page.

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

Online Upgrading via PC Web

You can upgrade the device online.

Click **System and Maintenance → Maintenance → Upgarde** to enter the settings page.

Click**Check for Updates**to check whether there is updated versions.

If the device is connected to the network and added to Hik-Connect App, you can tap **Device Upgrade → Online Upgrade** on device for upgrading when there is an updated version in Hik-Connect App.

7.11.3 Restoration

Restore to Factory Settings via Web Browser

You can restore device to factory settings.

Click **System and Maintenance → Maintenance → Backup and Reset** to enter the settings page.

Click **Restore All**, all parameters will be restored to the factory settings. You should activate the device before usage.

Restore to Default Settings via PC Web

You can restore device to default settings.

Click **System and Maintenance → Maintenance → Backup and Reset** to enter the settings page.

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

7.11.4 Export Device Parameters via PC Web

Export device parameters.

Go to **System and Maintenance → Maintenance → Backup and Reset** .

Backup

Click **Export** to export device parameters.

Note

Export device parameters and import those parameters to other devices.

7.11.5 Import Device Parameters via PC Web

Import the configuration parameters.

Go to **System and Maintenance → Maintenance → Backup and Reset** .

Import Config File

Click and select a file from local PC. Click **Import**.

7.11.6 Device Debugging

You can set device debugging parameters.

Enable/Disable SSH via Web Browser

You can enable SSH to perform remote debugging.

Click **System and Maintenance → Maintenance → Device Debugging → Log for Debugging**.

Enable SSH

SSH is used for remote debugging. When you don't need to use this service, it's recommended to disable SSH to improve security.

Print Device Log via PC Web

You can print out the device log.

Click **System and Maintenance → Maintenance → Log** to enter the settings page.

Click**Export** to print out the device log.

Capture Network Packet via PC Web

Set the capture packet duration and size and start caputre. You can view the log and debug according to the capture result.

Go to **System and Maintenance → Maintenance → Device Debugging → Log for Debugging** .

Set **Capture Packet Duration**,**Capture Packet Size**, and click **Start Capture**.

Test Protocol via PC Web

Select a protocol address, and enter the protocol to test. You can debug the device according to the response header and returned value.

Go to **System and Maintenance → Maintenance → Device Debugging → Protocol Testing** .

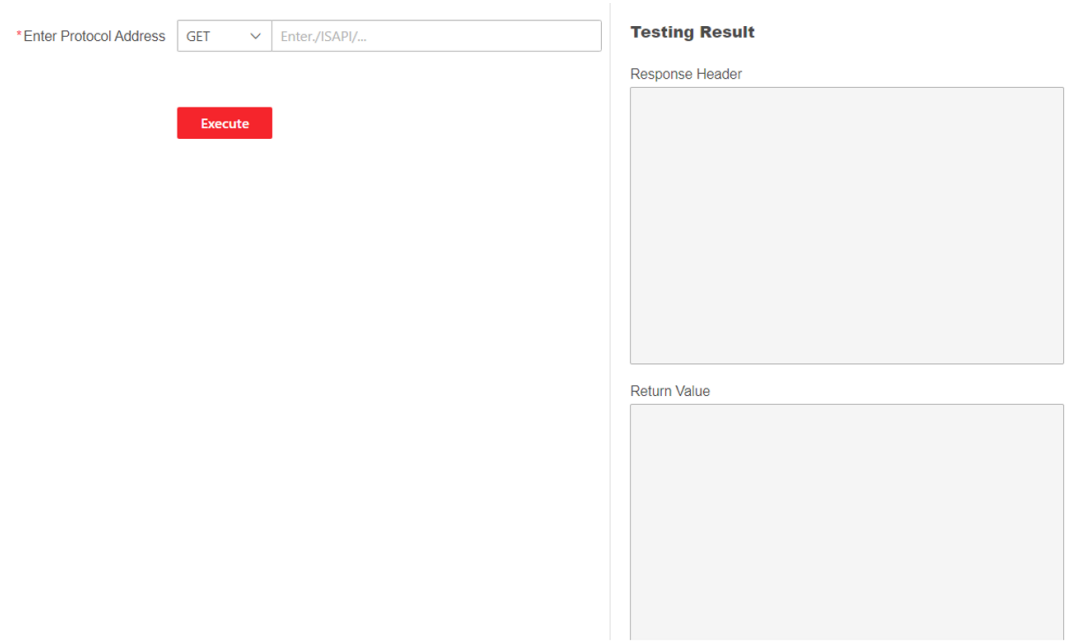


Figure 7-15 Protocol Testing

Select a protocol address, and enter the protocol. Click **Execute**.

Debug the device according to the response header and returned value.

7.11.7 View Log via PC Web

You can search and view the device logs.

Go to **System and Maintenance → Maintenance → Log** .

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.

7.11.8 Security Management

Set security level when login the PC web.

Go to **System and Maintenance → Safe → Security Service** .

Security Mode

High security level when logging in and verify user information.

Compatible Mode

Compatible with old user verification method.

Click **Save**.

7.11.9 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 Import Self-signed Certificate

Steps

1. Go to **System and Maintenance → Safe → 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 Key** area, and select a certificate from the local, and click **Import**.
   2) Select a certificate type in the **Import Communication Certificate** area, and select a certificate from the local, and click **Import**.

Import 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 **System and Maintenance → Safe → Certificate Management** .
2. In the **Import Key** and **Import Communication Certificate** areas, select certificate type and upload certificate.
3. Click **Import**.

Import CA Certificate

Before You Start

Prepare a CA certificate in advance.

Steps

1. Go to **System and Maintenance → Safe → Certificate Management** .
2. Create an ID in the **Import 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 **Import**.

Chapter 8 Other Platforms to Configure

You can also configure the device via iVMS-4200 Client Software or HikCentral Access Control. For details, see the platforms' user manual.

iVMS-4200 Client Software

Click/tap the link to view the client software's user manual.

http://enpinfodata.hikvision.com/analysisQR/showQR/ca930247

HikCentral Access Control (HCAC)

Click/tap the link to view the HCAC's user manual.

http://enpinfodata.hikvision.com/analysisQR/showQR/f2f6cf42

Appendix A. Legal Information

About this Document

- This Document 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 Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (***https://www.hikvision.com***). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

- This product can only enjoy the after-sales service support in the country or region where the purchase is made.
- If the product you choose is a video product, please scan the following QR code to obtain the "Initiatives on the Use of Video Products", and read it carefully.

Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- 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.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT 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 DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Data Protection

- To protect data, the development of Hikvision Products incorporates privacy by design principles. For example, for Products with facial recognition features, biometrics data is stored in your Products with encryption method; for fingerprint Products, only fingerprint template will be saved, which is impossible to reconstruct a fingerprint image.
- As a data controller/processor, you may process personal data, including collection, storage, use, processing, disclosure, deletion, etc. You are advised to pay attention to and comply with applicable laws and regulations related to the protection of personal data, including without limitation, conducting security controls to safeguard personal data, such as, implementing reasonable administrative and physical security controls, conduct periodic reviews and the assessments of the effectiveness of your security controls.

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

Appendix B. 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.

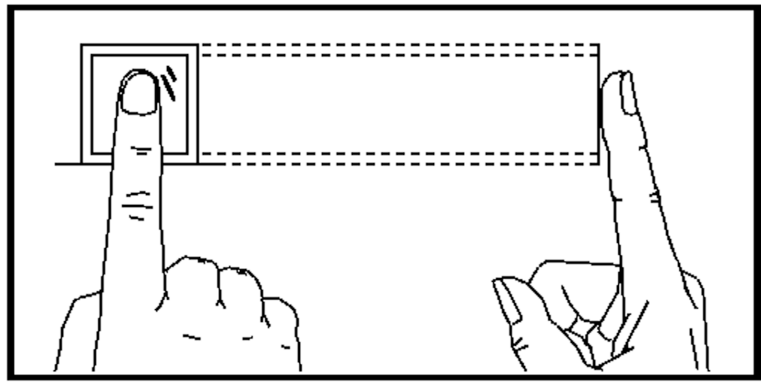
Appendix C. Tips for Scanning Fingerprint

Recommended Finger

Forefinger, middle finger or the third finger.

Correct Scanning

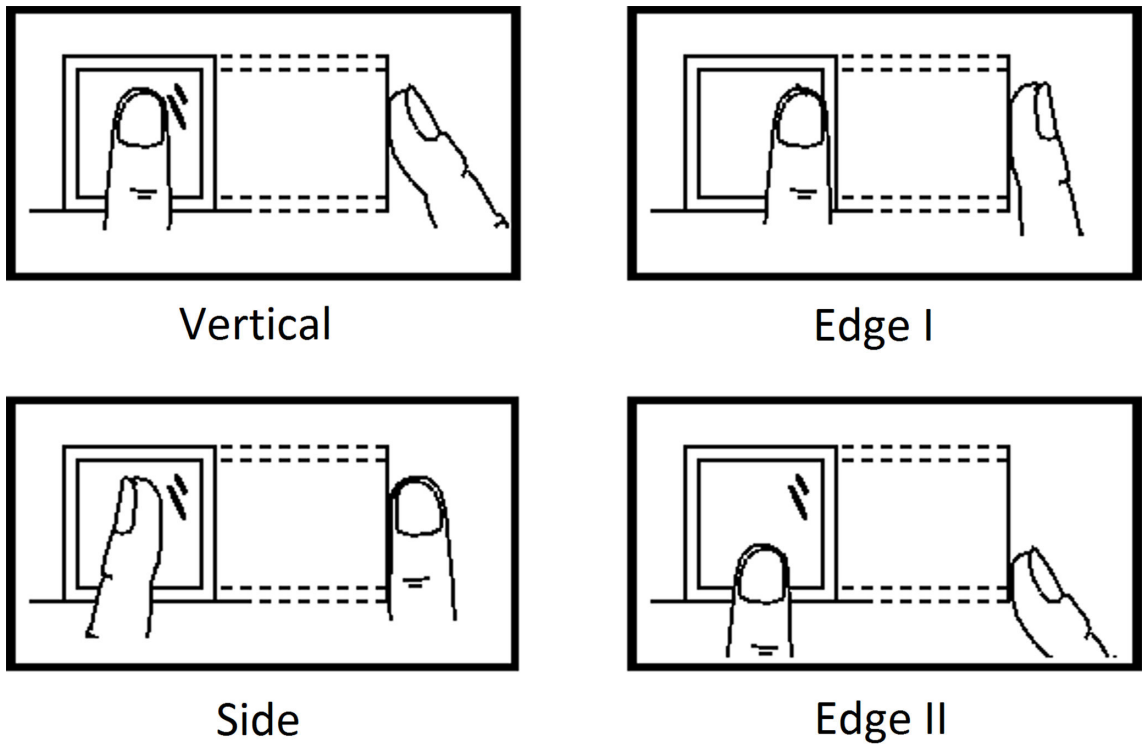
The figure displayed below is the correct way to scan your finger:



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

Incorrect Scanning

The figures of scanning fingerprint displayed below are incorrect:



Environment

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

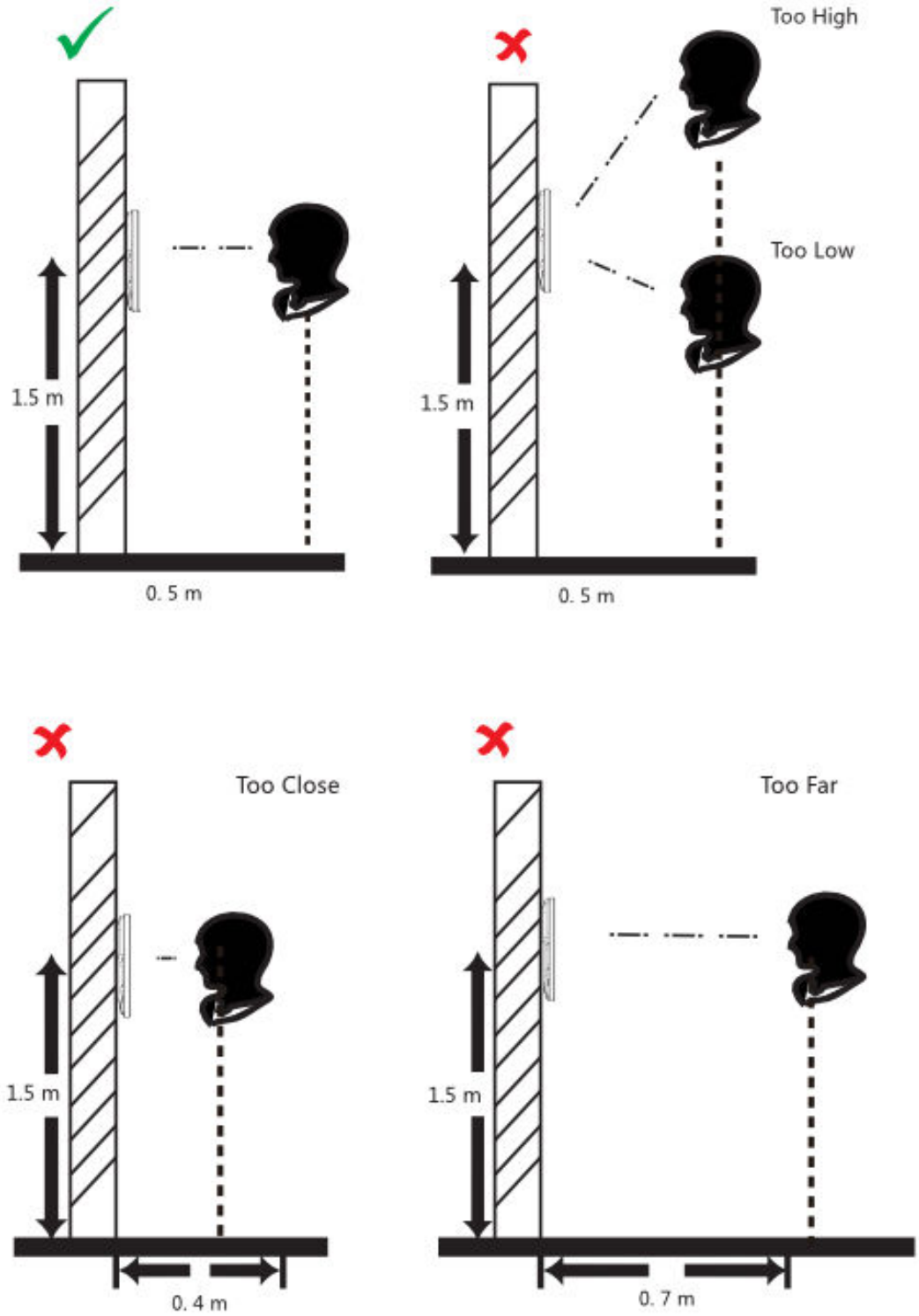
Others

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

Appendix D. Tips When Collecting/Comparing Face Picture

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

Positions (Recommended Distance: 0.3 m)



Expression

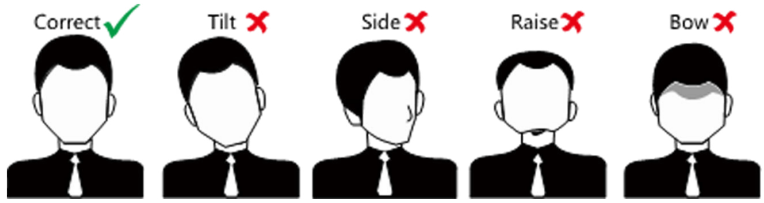
- Keep your expression naturally when collecting or comparing face pictures, just like the expression in the picture below.



- 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.

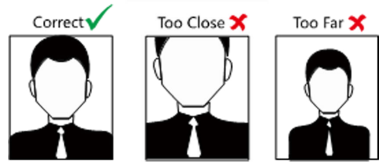
Posture

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 E. Tips for Installation Environment

1. Light Source Illumination Reference Value



Candle: 10Lux

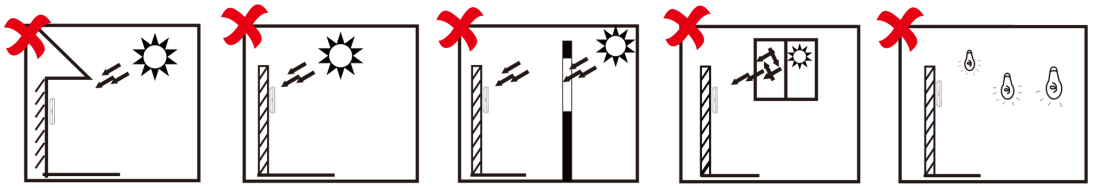


Bulb: 100~850Lux



Sunlight: More than 1200Lux

2. Avoid backlight, direct and indirect sunlight



Appendix F. Dimension

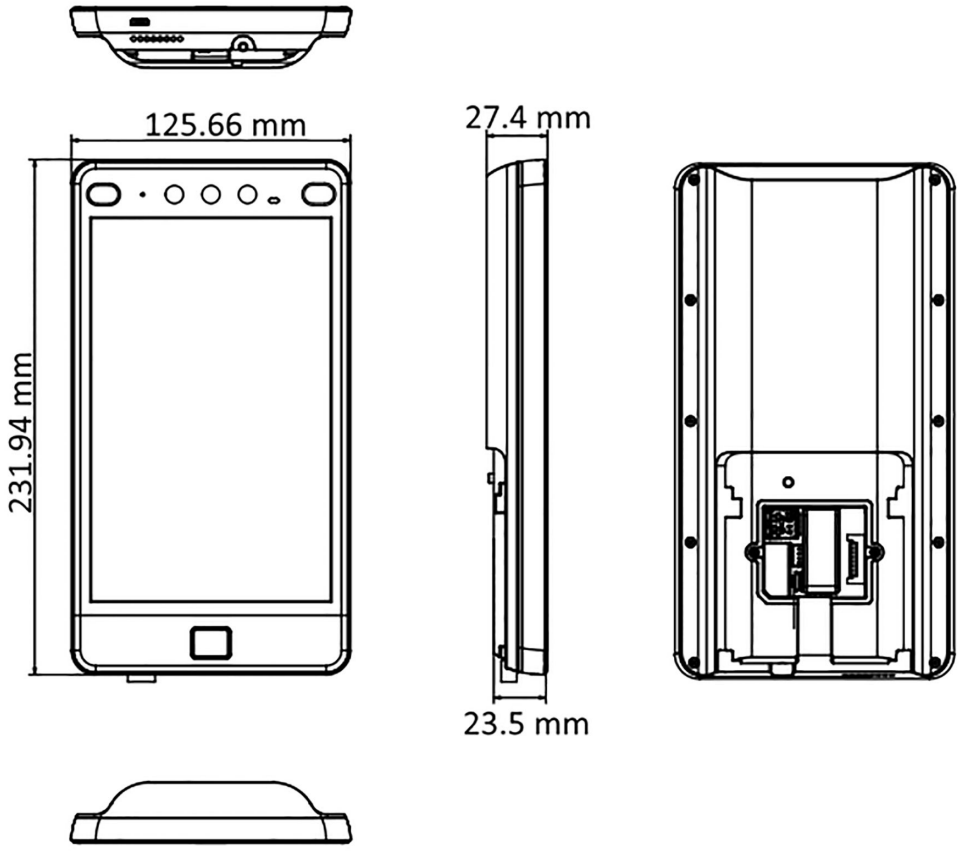


Figure F-1 Dimension


See Far, Go Further