DS-K1T344 Series Face Recognition 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

This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2014/30/EU, RE Directive 2014/53/EU,the RoHS Directive 2011/65/EU

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

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

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

COMPLIANCE NOTICE

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

Safety Instruction

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

The precaution measure is divided into Dangers and Cautions:

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

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

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

⚠ Danger:

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

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

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

⚠ Cautions:

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

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

Available Models

Product Name	Model
Face Recognition Terminal	DS-K1T344MBFWX-E1
	DS-K1T344MFX-E1
	DS-K1T344MBWX-E1
	DS-K1T344MBWX-QRE1
	DS-K1T344MX-E1
	DS-K1T344EBFWX-E1
	DS-K1T344EBWX-E1
	DS-K1T344EBWX-QRE1
	DS-K1T344EX-E1

Contents

Chapter 1 Appearance 1

Chapter 2 Installation Description 3

2.1 Installing Environment 3

2.2 Flush Mounting with Gang Box 3

Chapter 3 Terminal and Wiring Description 9

3.1 Wire Normal Device 9

3.2 Wire Secure Door Control Unit 11

3.3 Typical Application 12

Chapter 4 Activation 13

4.1 Activate via Mobile Web 13

4.2 Activate via Device 14

4.3 Activate via Web Browser 16

4.4 Activate via SADP 17

4.5 Activate Device via iVMS-4200 Client Software 18

Chapter 5 Quick Operation 20

5.1 Set Password Change Type 20

5.2 Set Network Parameters 20

5.3 Access to Platform 22

5.4 Remote Operation via APP 24

5.5 Privacy Settings 25

5.6 Set Administrator 26

5.7 Authentication Page Instructions 28

Chapter 6 Basic Operation 31

6.1 Login 31

6.1.1 Login by Activation Password 31

6.1.2 Login by Administrator 32

6.1.3 Forgot Password 35
6.1.4 Change Device Password 35
6.2 Communication Settings 36
6.2.1 Set Wired Network Parameters 36
6.2.2 Set Wi-Fi Parameters 38
6.2.3 Set RS-485 Parameters 40
6.2.4 Set Wiegand Parameters 41
6.2.5 Set ISUP Parameters 42
6.2.6 Platform Access 43
6.2.7 Set AP Mode 44
6.3 Person Management 44
6.3.1 Add Administrator 44
6.3.2 Import and Export Face and Person Data in Batch via Device 46
6.3.3 Add Face Picture 48
6.3.4 Add Card 51
6.3.5 Add Fingerprint 52
6.3.6 Add PIN 53
6.3.7 Set Person Type via Device 54
6.3.8 Set Authentication Mode 56
6.3.9 Search and Edit Person 57
6.4 Data Management 57
6.4.1 Delete Data 57
6.4.2 Import Data 57
6.4.3 Export Data 58
6.5 Person Authentication 58
6.5.1 Authenticate via Single Credential 59
6.5.2 Authenticate via Multiple Credential 59
6.6 Basic Settings 60

6.6.1 Enable/Disable Voice Prompt via Device 62
6.6.2 Set Device Time via Device 62
6.6.3 Set Sleep Duration via Device 62
6.6.4 Select Language 62
6.6.5 Set Device Number via Device 62
6.6.6 Set Privacy Parameters via Device 63
6.6.7 Set Video Standard 63
6.6.8 Set Secure Door Control Unit Parameters 64
6.7 Set Face Parameters 64
6.7.1 Set Face Liveness Level via Device 65
6.7.2 Set Recognition Distance via Device 66
6.7.3 Set Face Recognition Interval via Device 66
6.7.4 Set Face 1:N Security Level via Device 66
6.7.5 Set Face 1:1 Security Level via Device 66
6.7.6 Enable/Disable ECO Mode via Device 67
6.7.7 Enable/Disable Face Mask Detection via Device 67
6.8 Access Control Settings 68
6.8.1 Set Terminal Authentication Mode via Device 69
6.8.2 Set Reader Authentication Mode via Device 70
6.8.3 Enable/Disable NFC Card 70
6.8.4 Enable/Disable M1 Card 71
6.8.5 Set Authentication Interval via Device 71
6.8.6 Set Authentication Result Display Duration via Device 71
6.8.7 Set Password Mode 71
6.8.8 Set Door Contact via Device 72
6.8.9 Set Open Duration via Device 72
6.9 Preference Settings 72
6.9.1 Set Shortcut Key via Device 73

6.9.2 Theme 74

6.10 System Maintenance 75

6.10.1 View System Information 75

6.10.2 View Device Capacity via Device 76

6.10.3 Upgrade 76

6.10.4 View User Manual 77

6.10.5 Restore Settings 77

6.11 Video Intercom 77

6.11.1 Call Client Software from Device 78

6.11.2 Call Center from Device 78

6.11.3 Call Device from Client Software 79

6.11.4 Call Room from Device 79

6.11.5 Call Mobile Client from Device 80

Chapter 7 Configure Device via Mobile Web 81

7.1 Login 81

7.2 Forget Password 81

7.3 Account Security Settings 81

7.4 Home 82

7.5 Configuration 82

7.5.1 View Device Information 82

7.5.2 Set Device Time 83

7.5.3 User Management 83

7.5.4 Network Settings 84

7.5.5 Add Person 88

7.5.6 Event Search 90

7.5.7 Audio Settings 90

7.5.8 Access Control Settings 90

7.5.9 Video Intercom Settings 96

7.5.10 Set Face Parameters 98
7.5.11 Enable/Disable Masl Detection via Device 99
7.5.12 Set Privacy Parameters 100
7.5.13 Set PIN Mode 101
7.5.14 System Upgrade & Maintenance 101
7.5.15 View User Document 102
7.5.16 Open Source Software Licenses 102
7.5.17 Log Out of Mobile Web 102
Chapter 8 Operation via Web Browser 103
8.1 Login 103
8.2 Forget Password 103
8.3 Help 103
8.3.1 Open Source Software Licenses 103
8.3.2 View Online Help Document 104
8.4 Logout 104
8.5 Quick Operation via Web Browser 104
8.5.1 Change Password 104
8.5.2 Select Language 105
8.5.3 Time Settings 105
8.5.4 Privacy Settings 105
8.5.5 Administrator Settings 106
8.5.6 No. and System Network 107
8.6 Person Management 108
8.7 Access Control Management 110
8.7.1 Overview 110
8.7.2 Search Event 112
8.7.3 Door Parameter Configuration 113
8.7.4 Authentication Settings 116

8.7.5 Set Face Parameters 120

8.7.6 Card Settings 125

8.7.7 Linkage Settings 126

8.7.8 Set Working Mode via PC Web 127

8.7.9 Privacy Settings 128

8.8 Call Settings 131

8.8.1 Device Management 131

8.8.2 Set Device No. via Web 131

8.8.3 Configure Video Intercom Network Parameters via Web Browser 133

8.8.4 Set Communication Time via PC Web 134

8.8.5 Press Button to Call via PC Web 134

8.8.6 Number Settings via PC Web 135

8.9 System and Maintenance 135

8.9.1 View Device Information via PC Web 135

8.9.2 Set Time 135

8.9.3 Change Administrator's Password 137

8.9.4 Account Security Settings via PC Web 137

8.9.5 View Device Arming/Disarming Information via PC Web 137

8.9.6 Network Settings 138

8.9.7 Set Video and Audio Parameters via PC Web 144

8.9.8 Image Parameter Settings 145

8.9.9 Alarm Settings via PC Web 147

8.9.10 Access Configuration 147

8.10 Preference Settings 149

8.10.1 Set Standby Image via PC Web 149

8.10.2 Set Sleep Time via PC Web 149

8.10.3 Customize Authentication Desk via PC Web 150

8.10.4 Set Notice Publication via PC Web 150

8.10.5 Set Prompt Schedule via PC Web 151
8.10.6 Customize Prompt Voice via PC Web 153
8.10.7 Set Authentication Result Text via PC Web 153
8.11 System and Maintenance 154
8.11.1 Reboot 154
8.11.2 Upgrade 154
8.11.3 Restoration 155
8.11.4 Export Device Parameters via PC Web 155
8.11.5 Import Device Parameters via PC Web 155
8.11.6 Device Debugging 156
8.11.7 View Log via PC Web 157
8.11.8 Advanced Settings via PC Web 157
8.11.9 Security Management 158
8.11.10 Certificate Management 158
Appendix A. Tips for Scanning Fingerprint 160
Appendix B. Tips When Collecting/Comparing Face Picture 162
Appendix C. Tips for Installation Environment 164
Appendix D. Dimension 165
Appendix E. Legal Information 166
Appendix F. Symbol Conventions 168

Chapter 1 Appearance

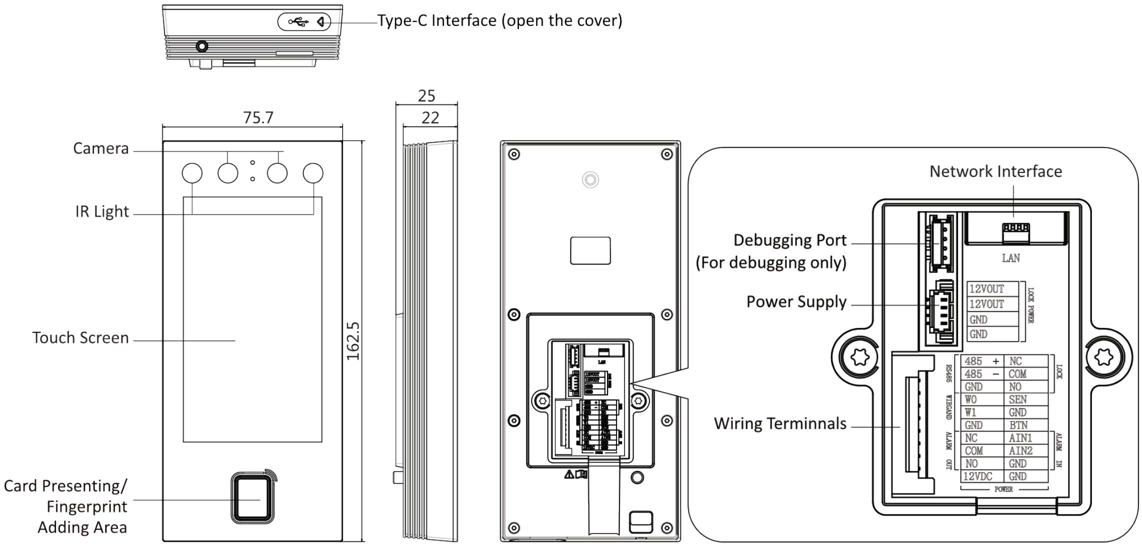
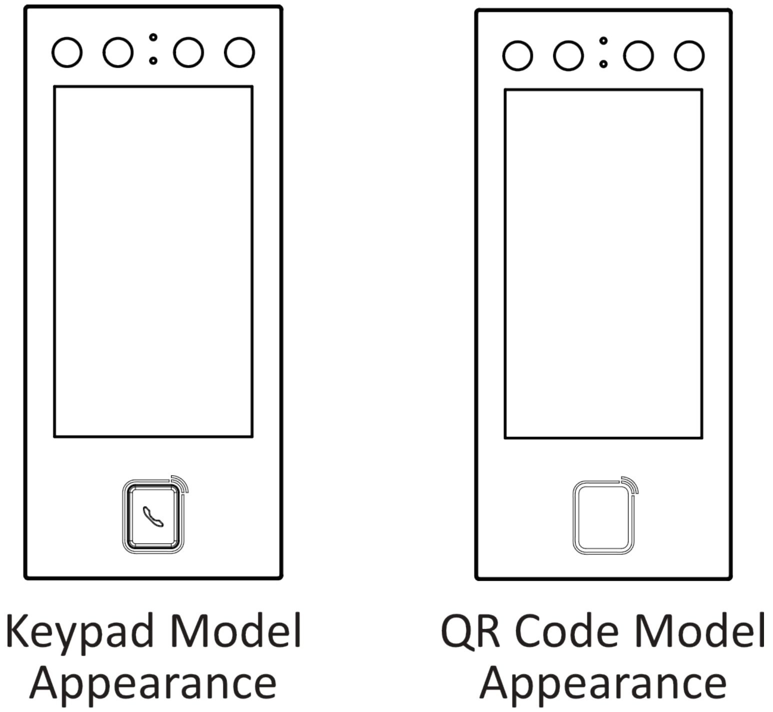


Figure 1-1 Appearance Description (Unit: mm)

Note

Parts of models support fingerprint function, refers to the actual product.



Keypad Model Appearance

QR Code Model Appearance

Figure 1-2 Other Types

Note

For different device models, the device will support fingerprint, QR code, and keypad. Refers to actual products for details.

Chapter 2 Installation Description

2.1 Installing Environment

Avoid backlight, direct sunlight, and indirect sunlight. For better recognition, there should be light source in or near the installation environment.

If you have to install the device outdoors, you should install a protective shield (optional) for the device.

Note

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

2.2 Flush Mounting with Gang Box

Steps

Note

The gang box is optional. You should purchase it separately.

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

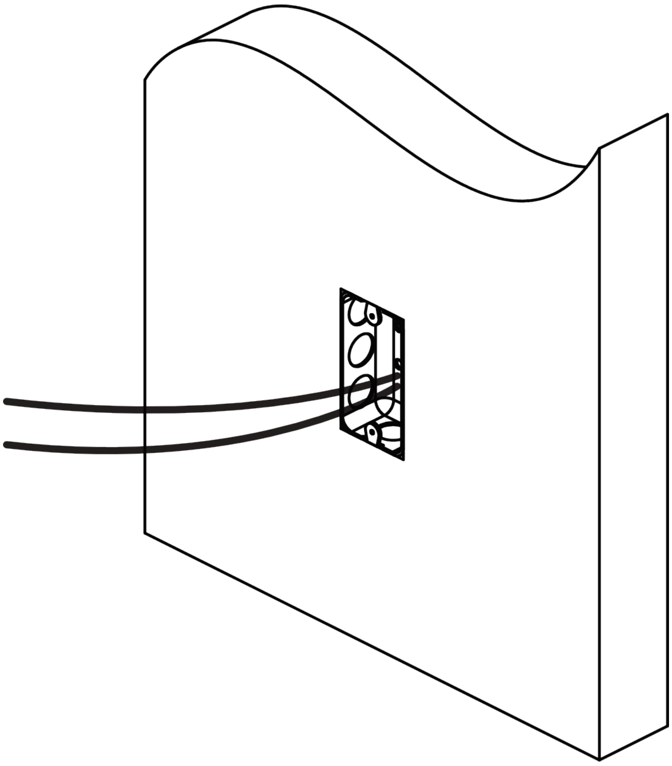


Figure 2-1 Gang Box is on Wall

2. Align the mounting plate holes with gang box holes, using 2 screws (KA4×25) to secure the mounting plate on the gang box.

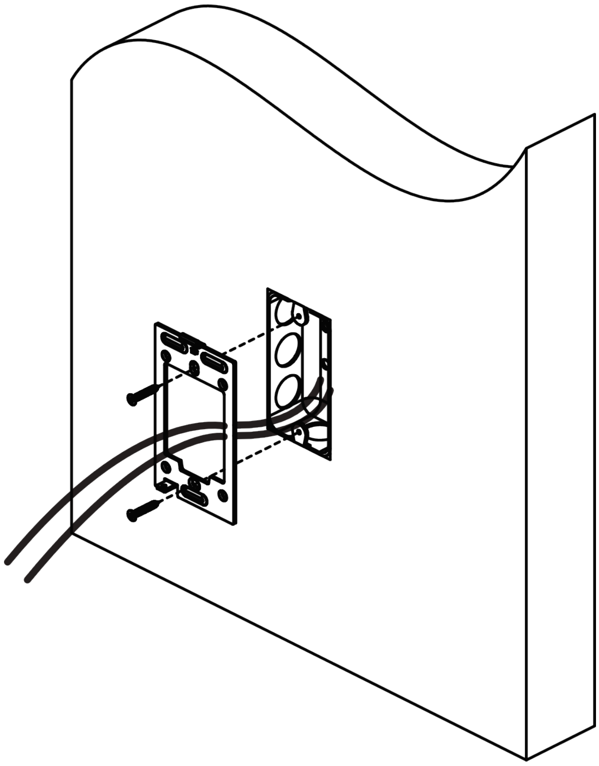


Figure 2-2 Secure Mounting Template

3. Complete wiring. For details, see the wiring diagram.

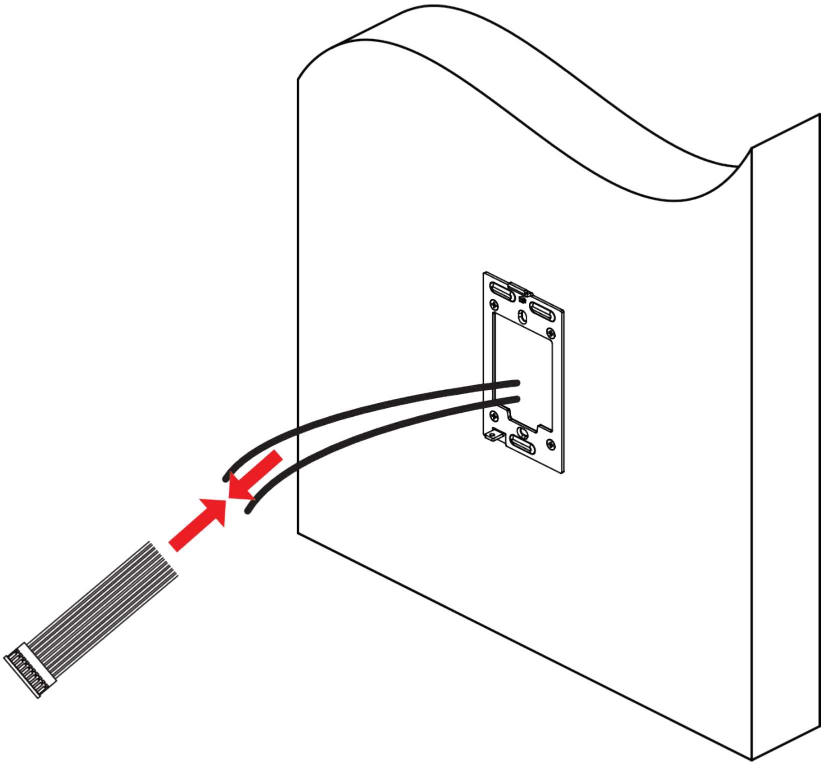


Figure 2-3 Wiring

4. Remove screws on the back sheet, and remove the back sheet.

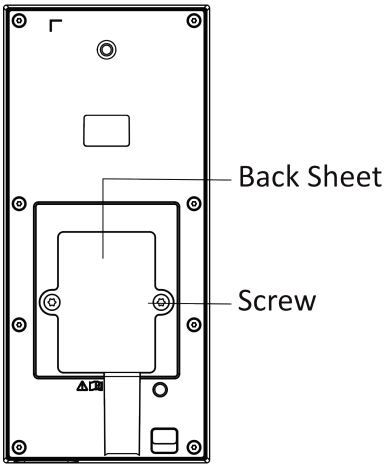


Figure 2-4 Remove Back Sheet

5. Insert the terminals in the device. For details, see wiring diagram. Use 1 screw (KM3×8) to secure the device on the mounting plate.

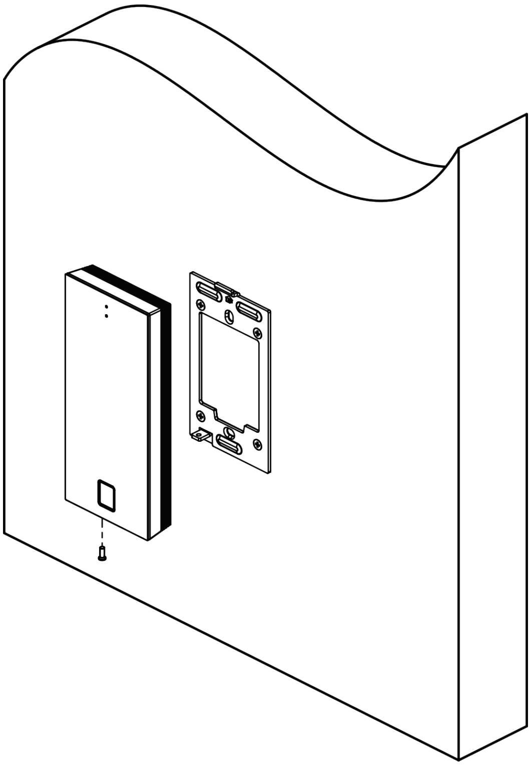
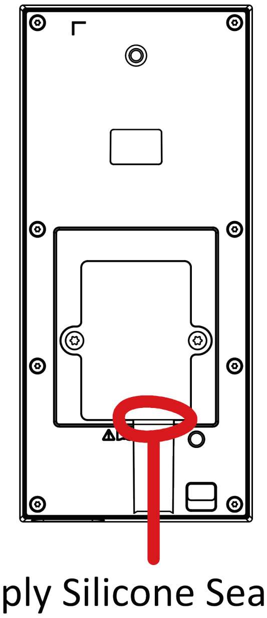


Figure 2-5 Install Device

6. Arrange the cables and install the back sheet back. Apply silicone sealant among the cable wiring area to keep the raindrop from entering.



Apply Silicone Sealant

Figure 2-6 Apply Silicone Sealant

7. Complete installation.

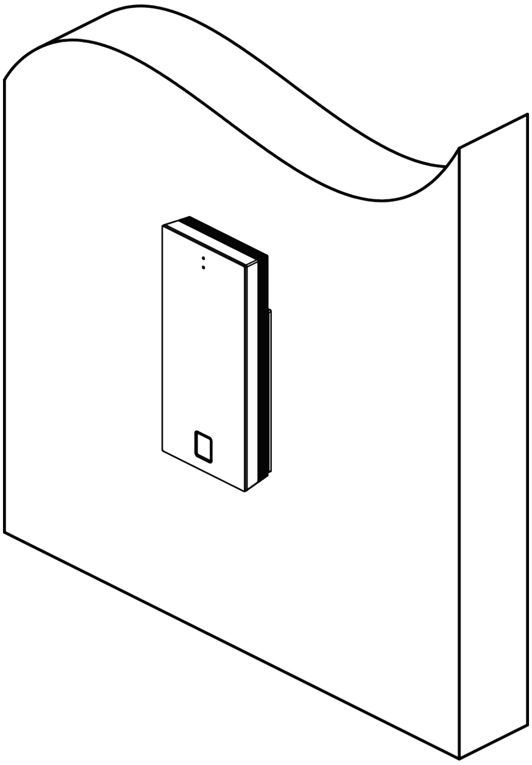


Figure 2-7 Complete Installation

Chapter 3 Terminal and Wiring Description

You can connect to RS-485 card reader, door lock, exit button, door contact, alarm device, etc. via the terminals.

You can connect the RS-485 terminal with the RS-485 card reader, connect the LOCK terminal with the door lock, connect the SEN and GND terminal with the door contact, the BTN/GND terminal with the exit button, and connect the Wiegand terminal with the access controller.

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

Pay attentions when wiring:

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

Note

The external card reader, door lock, exit button, and door contact need individual power supply.

3.1 Wire Normal Device

The wiring diagram is as follows:

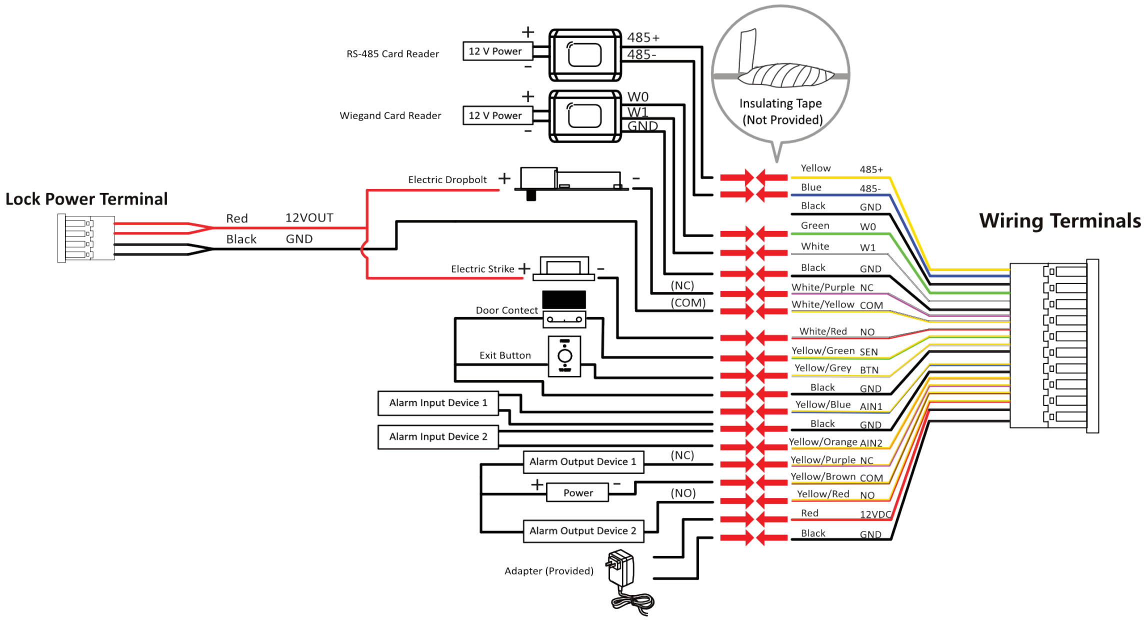


Figure 3-1 Terminal and Wiring Description

Note

- The wiegand interface shown in the figure is wiegand input interface, which can be connected to the wiegand card reader, and you need to set the wiegand transmission direction as “input”. If the device connects to the access controller, the wiegand interface is wiegand output interface, and you need to set the transmission direction as “output”. For more information about setting transmission direction, refer to Set Wiegand Parameters in Communication Settings section.
- Alarm input devices are usually sensors, and alarm output devices are usually alarms and lights.
- Connect the wires according to the actual needs, and power cable must be connected.
- There is no need to connect external power supply when using PoE power supply.
- Use 12 VDC power supply with 12 W power.
- Do not directly connect the device to 220 V electric supply.
- When using the PoE power supply, the lock power supply (equipped) can be used to power the lock. The lock power interface will contain power when connect PoE power supply.
- If the device do not support PoE, do not connect the lock power terminal. And instead, you should wire an external power for the door lock.

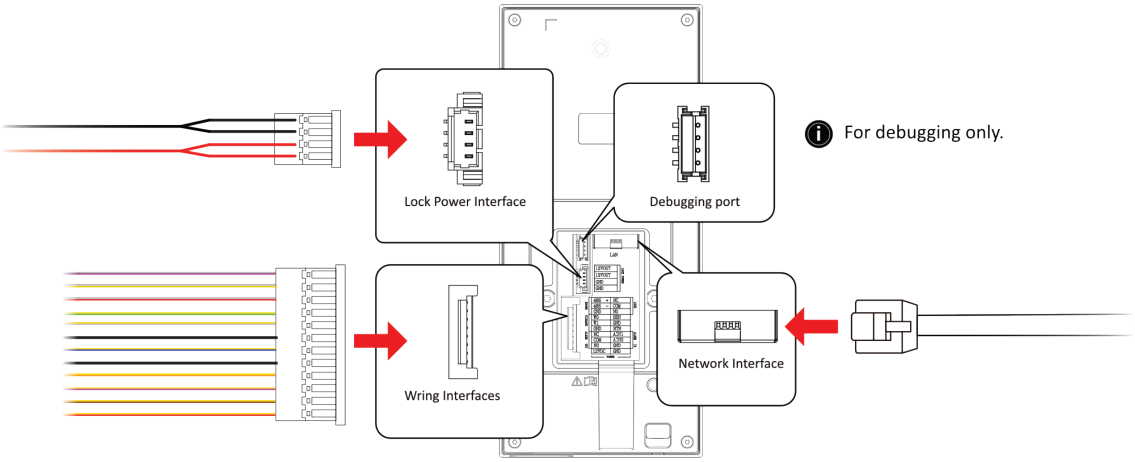


Figure 3-2 Connect the Terminals to the Interfaces

Note

- Connect the cables according to the actual needs, and power cable must be connected.
- Supports PoE network interface, and it can be powered by PoE power supply.
- There is no need to connect external power supply when using PoE power supply.
- The debugging port is for debugging only.

3.2 Wire Secure Door Control Unit

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

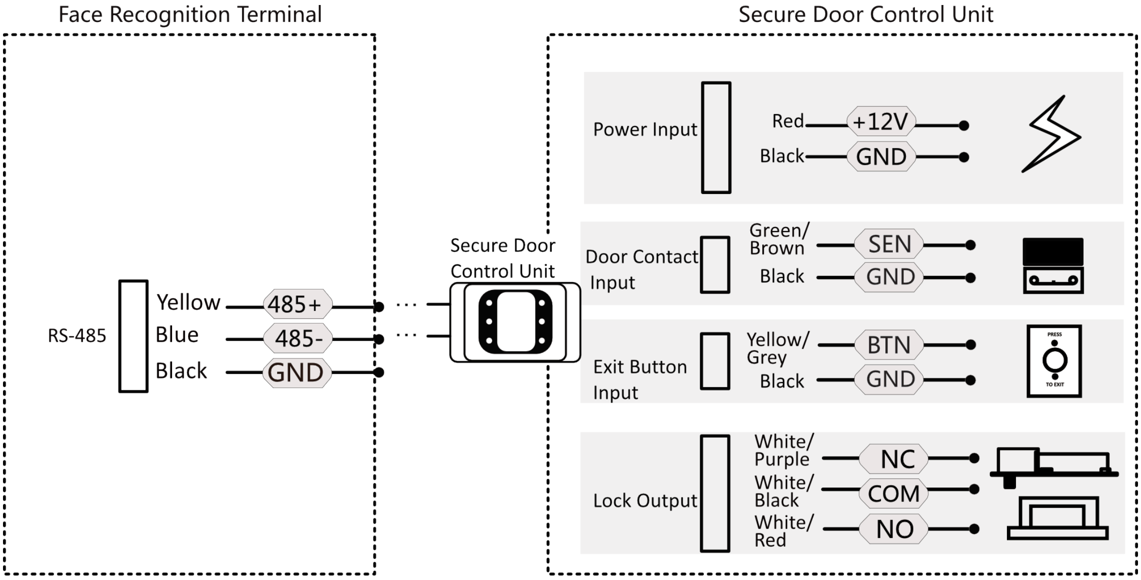


Figure 3-3 Secure Door Control Unit Wiring

Note

- The secure door control unit should connect to an external power supply separately. The suggested external power supply is 12 V, 0.5 A.
- For scenarios with high safety requirement, use the secure door control unit wiring first. You can ask the technical support to purchase for the secure door control unit separately.
- The picture here are parts of the wiring. For details, see the secure door control unit’s user manual.

3.3 Typical Application

Typical Application 1

Scene: After installation and wiring, you can add face and other information for the person. And the person can authenticate on the device.

1. Finish installation and wiring. For details, refers to ***Installation Description*** and ***Terminal and Wiring Description*** .
2. Finish device activation. For details, see ***Activation*** .
3. Finish quick operation on the device. For details, see ***Quick Operation*** .
4. Add face and permission. For details, see ***Add Face Picture*** and ***Set Authentication Mode*** .
5. Person authentication. For details, see ***Person Authentication*** .

Typical Application 2

Scene: Call door station via the device.

1. Finish installation and wiring. For details, refers to ***Installation Description*** and ***Terminal and Wiring Description*** .
2. Set the device No. For details, refers to ***Set Device Number via Device*** and ***Configure Video Intercom Network Parameters via Web Browser*** .
3. Add indoor station or sub door station. For details, see ***Device Management*** .
4. Set private intercom server IP address (SIP server IP). The IP address would be the main station’s IP. For details, see ***Configure Video Intercom Network Parameters via Web Browser*** .
5. Set the indoor station No. or sub door station No. and set the SIP server IP address (the same as the device). For details, see the indoor station and the door station's user manual.
6. Call indoor station from the device. For details, see ***Call Room from Device*** .

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 Mobile Web

You can activate the device via mobile web.

Steps

1. Connect to the device hotspot with your mobile phone by entering the hotspot password.

   Note

   - For inactive devices, hotspot is enabled by default.
   - The hotspot name and the default hotspot password is the device serial number.
   - After the device is activated, the hotspot password will change to the activation password (admin password).

   The login page will pop up.
2. Create a new password (admin password) and confirm the password.

   Caution

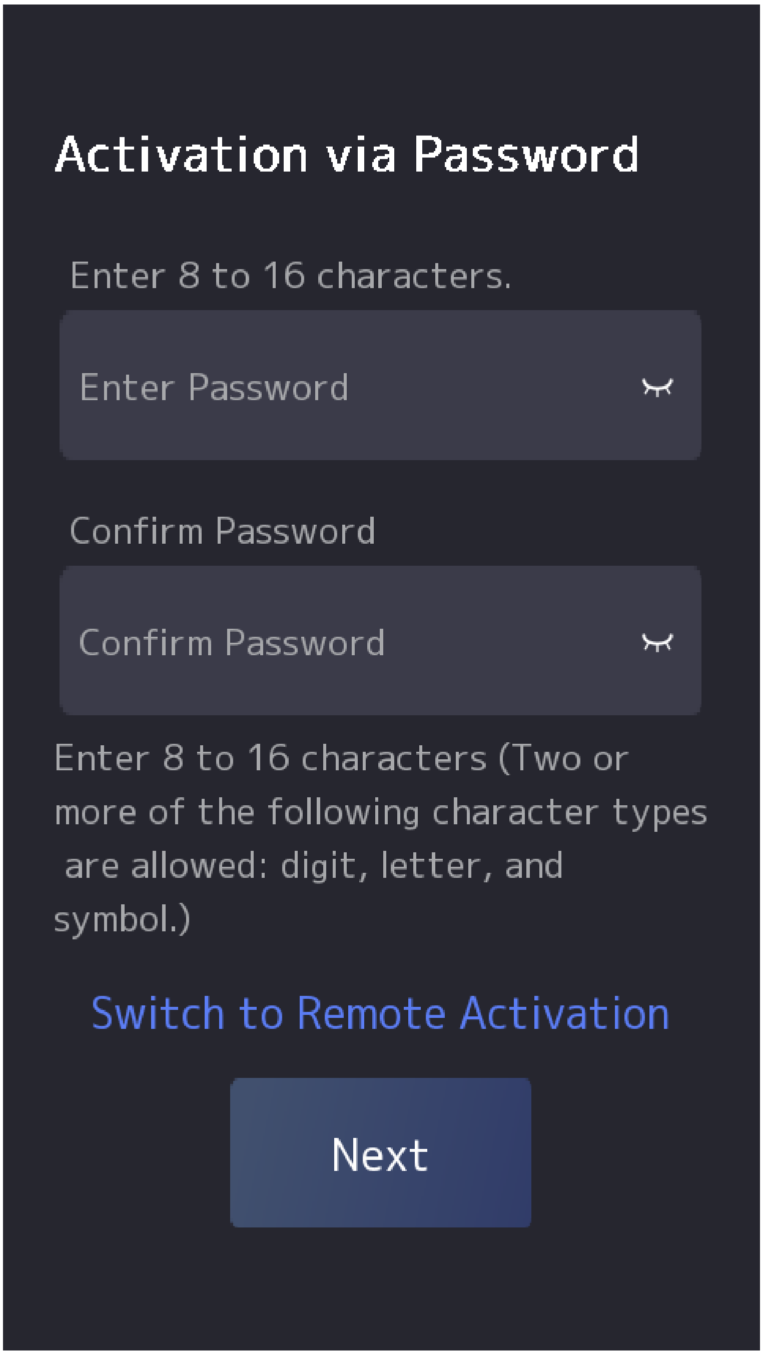
   - The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order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

4.2 Activate via Device

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

On the Remote Config. page, tap **Switch to Local Activation** create a password and confirm the password. Tap **Next** and the device will activated.



Activation via Password

Enter 8 to 16 characters.

Enter Password

Confirm Password

Confirm Password

Enter 8 to 16 characters (Two or more of the following character types are allowed: digit, letter, and symbol.)

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).

4.3 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.

4.4 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

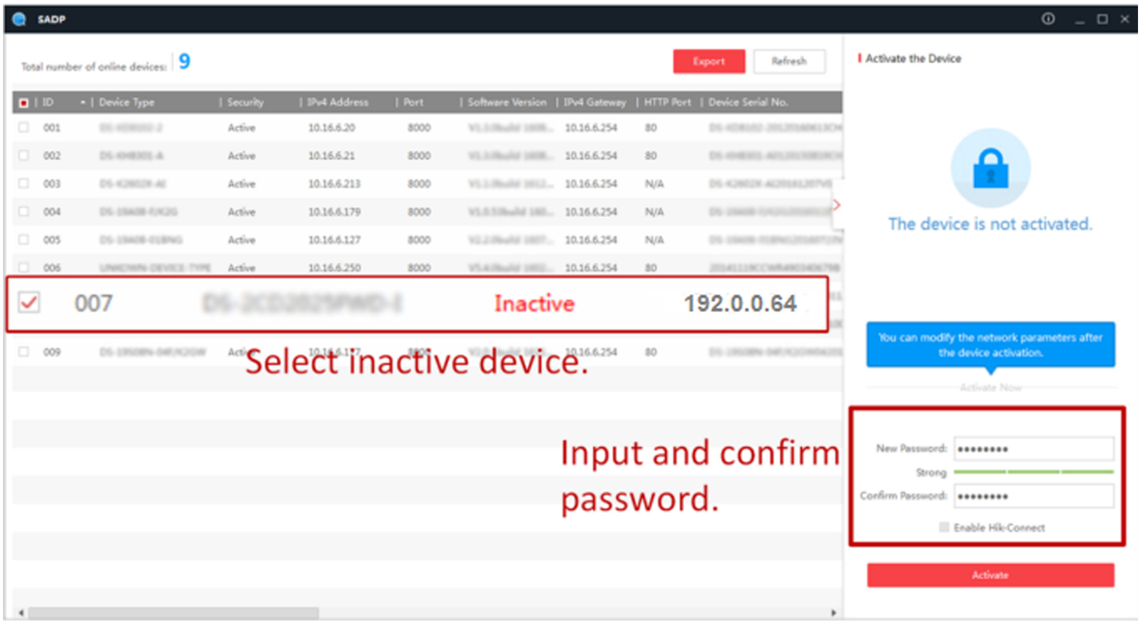
1. Run the SADP software and search the online devices.
2. Find and select your device in online device list.
3. Input new password (admin password) and confirm the password.

   ⚠ **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.

   ℹ **Note**

   Characters containing admin and nimda are not supported to be set as activation password.
4. Click **Activate** to start activation.



Total number of online devices: 9

☐ ID	Device Type	Security	IPv4 Address	Port	Software Version	IPv4 Gateway	HTTP Port	Device Serial No.
☐ 001	[illegible]	Active	10.16.6.20	8000	[illegible]	10.16.6.254	80	[illegible]
☐ 002	[illegible]	Active	10.16.6.21	8000	[illegible]	10.16.6.254	80	[illegible]
☐ 003	[illegible]	Active	10.16.6.213	8000	[illegible]	10.16.6.254	N/A	[illegible]
☐ 004	[illegible]	Active	10.16.6.179	8000	[illegible]	10.16.6.254	N/A	[illegible]
☐ 005	[illegible]	Active	10.16.6.127	8000	[illegible]	10.16.6.254	N/A	[illegible]
☐ 006	[illegible]	Active	10.16.6.250	8000	[illegible]	10.16.6.254	80	[illegible]
☑ 007	[illegible]	Inactive	192.0.0.64					
☐ 009	[illegible]	Acti[illegible]	10.16.6.1[illegible]	[illegible]	[illegible]	10.16.6.254	80	[illegible]

Select inactive device.

Input and confirm password.

You can modify the network parameters after the device activation.

New Password: ••••••••

Strong

Confirm Password: ••••••••

☐ Enable Hik-Connect

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.

4.5 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 service provider and/or end-user.

ℹ **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 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.

5.2 Set Network Parameters

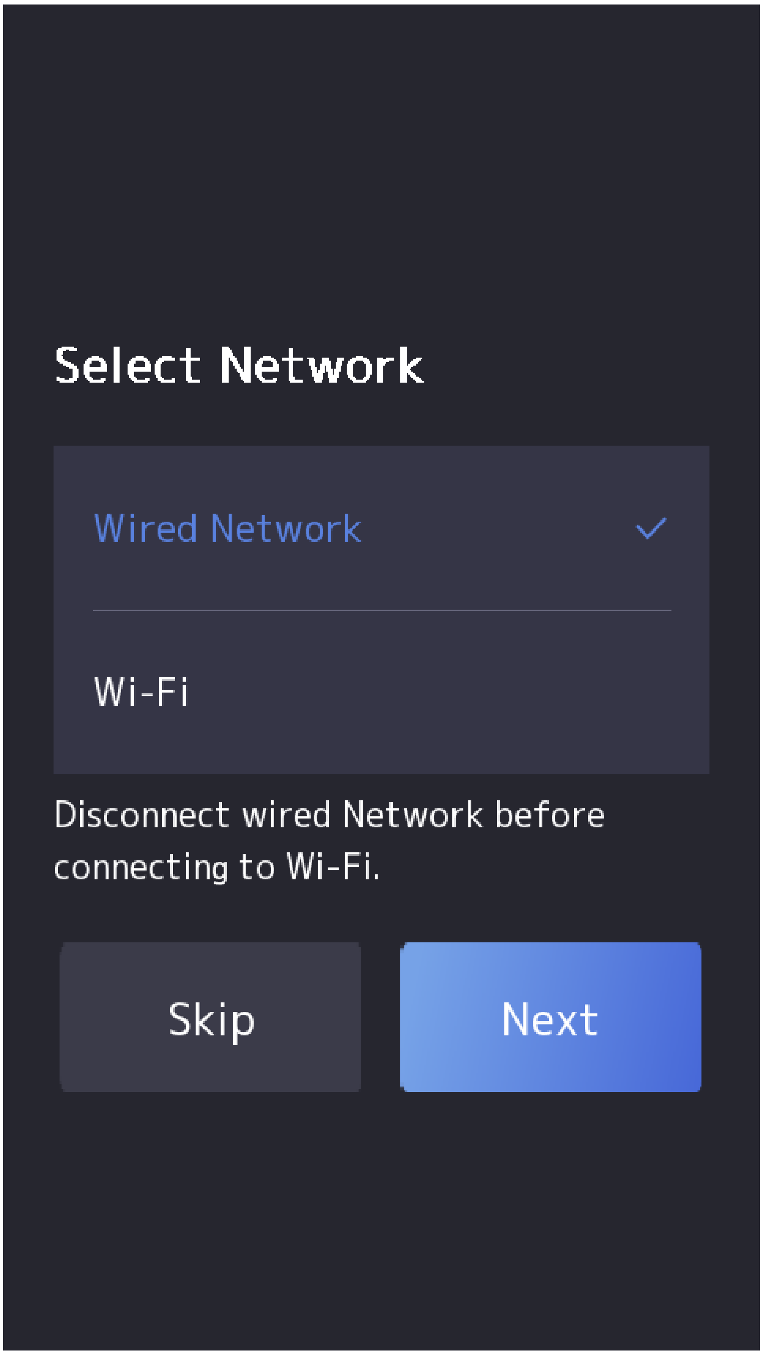
You can set the network for the device.

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.



Select Network

Wired Network ✓

Wi-Fi

Disconnect wired Network before connecting to Wi-Fi.

Figure 5-1 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.

5.3 Access to Platform

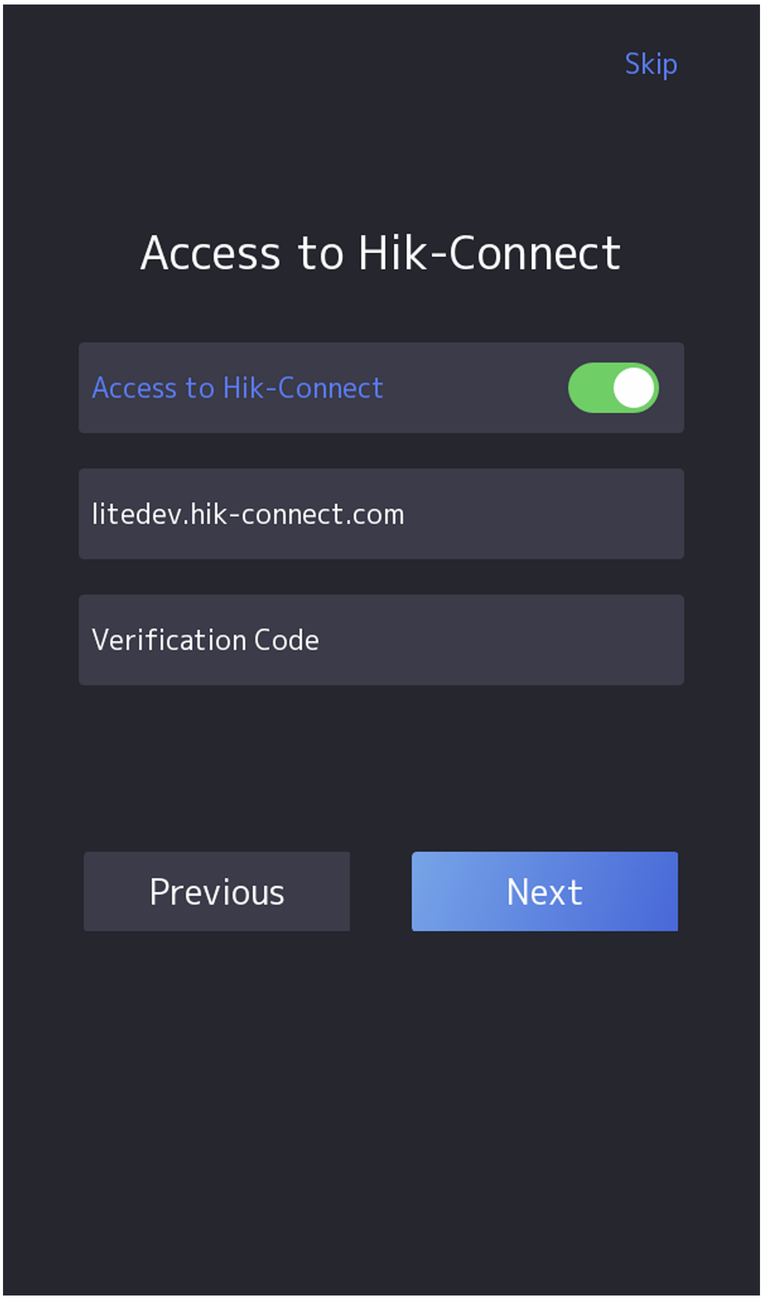
Enable the function and the device can communicate via Hik-Connect. You can add the device to Hik-Connect mobile client and so on.

Steps

Note

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

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



Skip

Access to Hik-Connect

Access to Hik-Connect

litedev.hik-connect.com

Verification Code

Previous

Next

Figure 5-2 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.

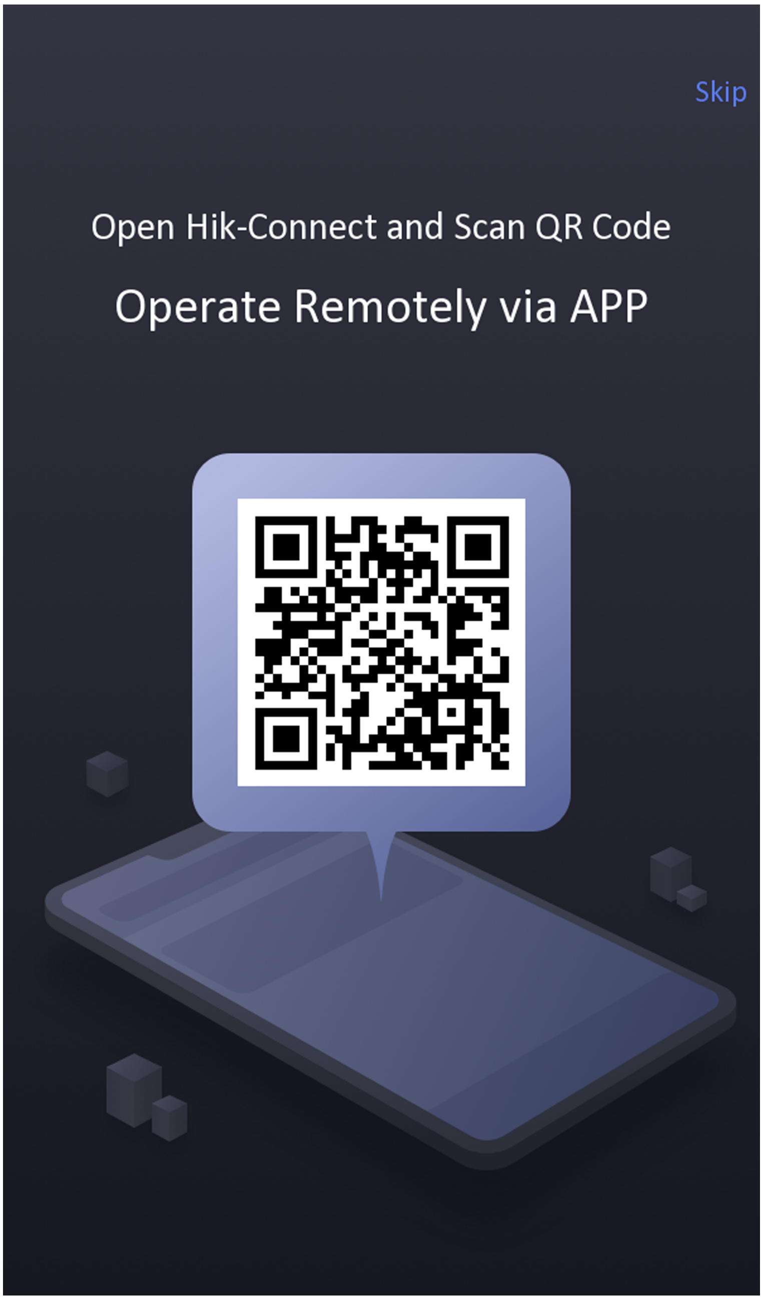
Note

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.

5.4 Remote Operation via APP

You can add the device to your mobile client for remote operation.

Download Hik-Connect to your mobile client and run the APP. Scan the QR Code in the following picture to add the device to your mobile client for remote operation.
Following the instruction in your mobile client to add the device.



Skip

Open Hik-Connect and Scan QR Code

Operate Remotely via APP

Figure 5-3 Operate Remotely via APP

5.5 Privacy Settings

You should set the privacy parameters, including the picture uploading and storage.

Select parameters according to your actual needs.

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

Upload the pictures captured when authenticating to the platform automatically.

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

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

Save Registered Pic. (Save Registered Picture)

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

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

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

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

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

Tap **Next** to complete the settings.

5.6 Set Administrator

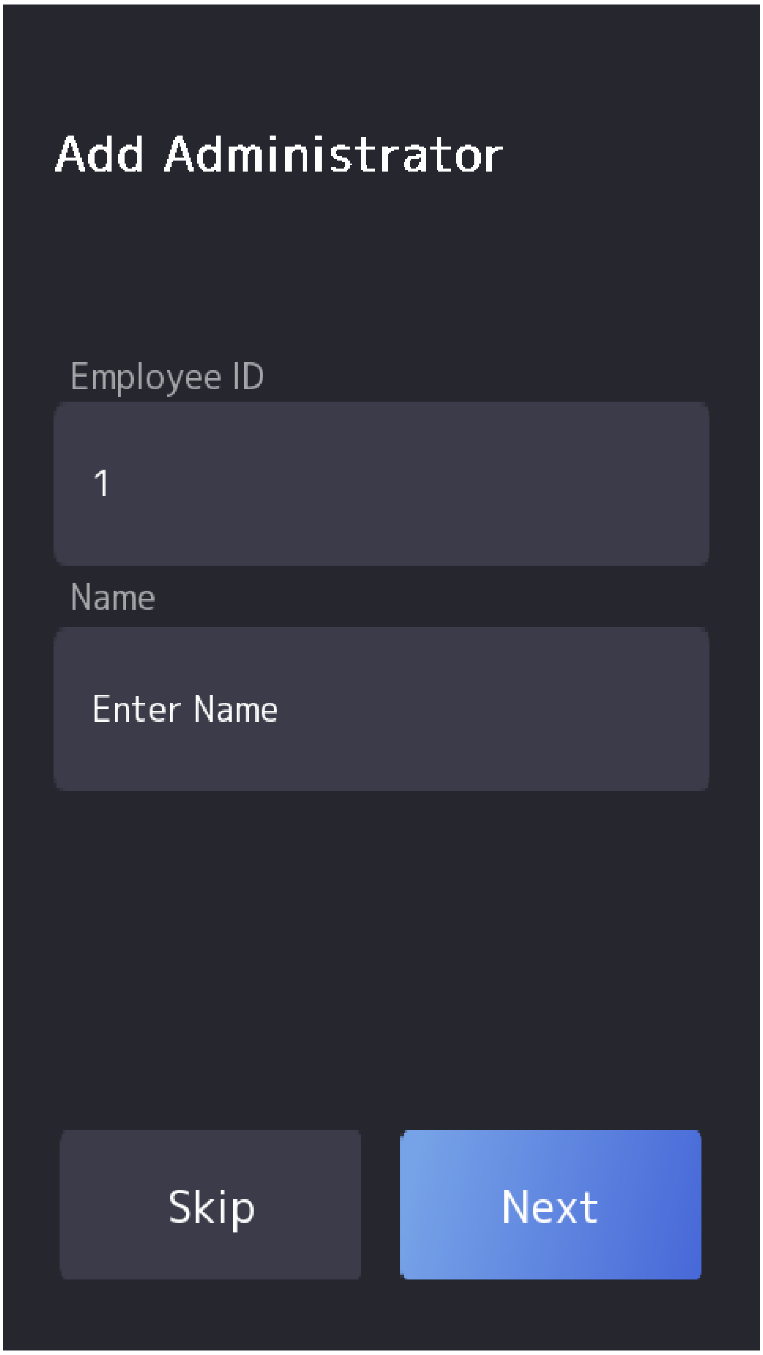
After device activation, you can add an administrator to manage the device parameters.

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**.



Add Administrator

Employee ID

1

Name

Enter Name

Figure 5-4 Add Administrator Page

3. Select a credential to add.

Note

Up to one credential should be added.

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

5.7 Authentication Page Instructions

Introduce the authentication page.

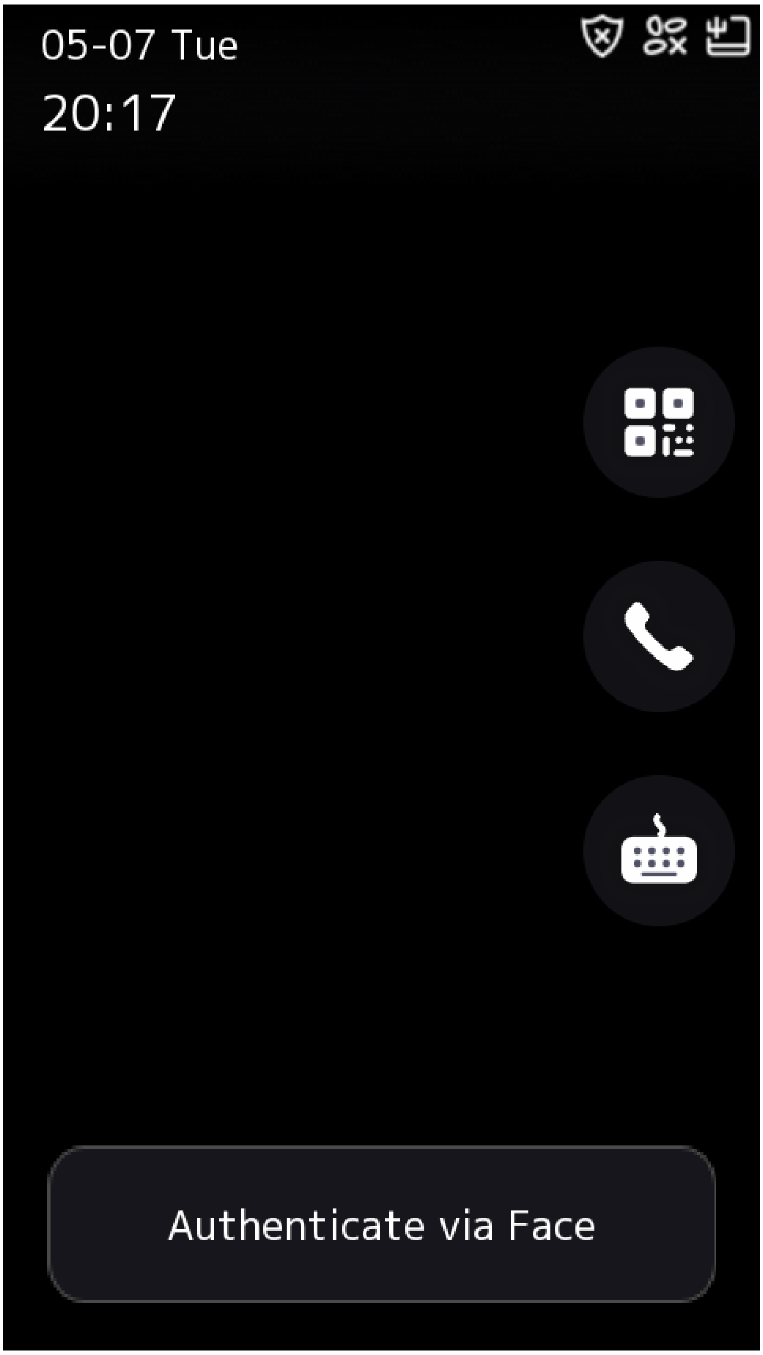


Figure 5-5 Authentication Page

Status Bar Instructions

🛡 / 🛡

The device is armed/not armed.

📶 / 📶 / 📶

Wi-Fi is connected and signal is strong/Wi-Fi is enabled but not connected/Wi-Fi IP conflicts.

□ / ☒ / ⚠

Network is connected/not connected/connection error.

SIP / SIP / SIP

SIP server is registered/registering failed/registered to door station but not to main station.

Authentication Page Icon

Note

The displayed icon on the authentication page can be controlled. For details, see shortcut key settings in .

Object Missing This object is not available in the repository.

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

Note

The QR code is generated and applied from platform for visitors or is converted from card No.

Object Missing This object is not available in the repository.

- Enter the room No., and tap **OK** to call.
- Tap Object Missing This object is not available in the repository. to call the center.

Note

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

Object Missing This object is not available in the repository.

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

Chapter 6 Basic Operation

6.1 Login

Login the device to set the device basic parameters.

6.1.1 Login by Activation Password

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

Steps

1. Long tap on the initial page for 3 s and slide to the left/right by following the gesture to enter password entering page.
2. 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.

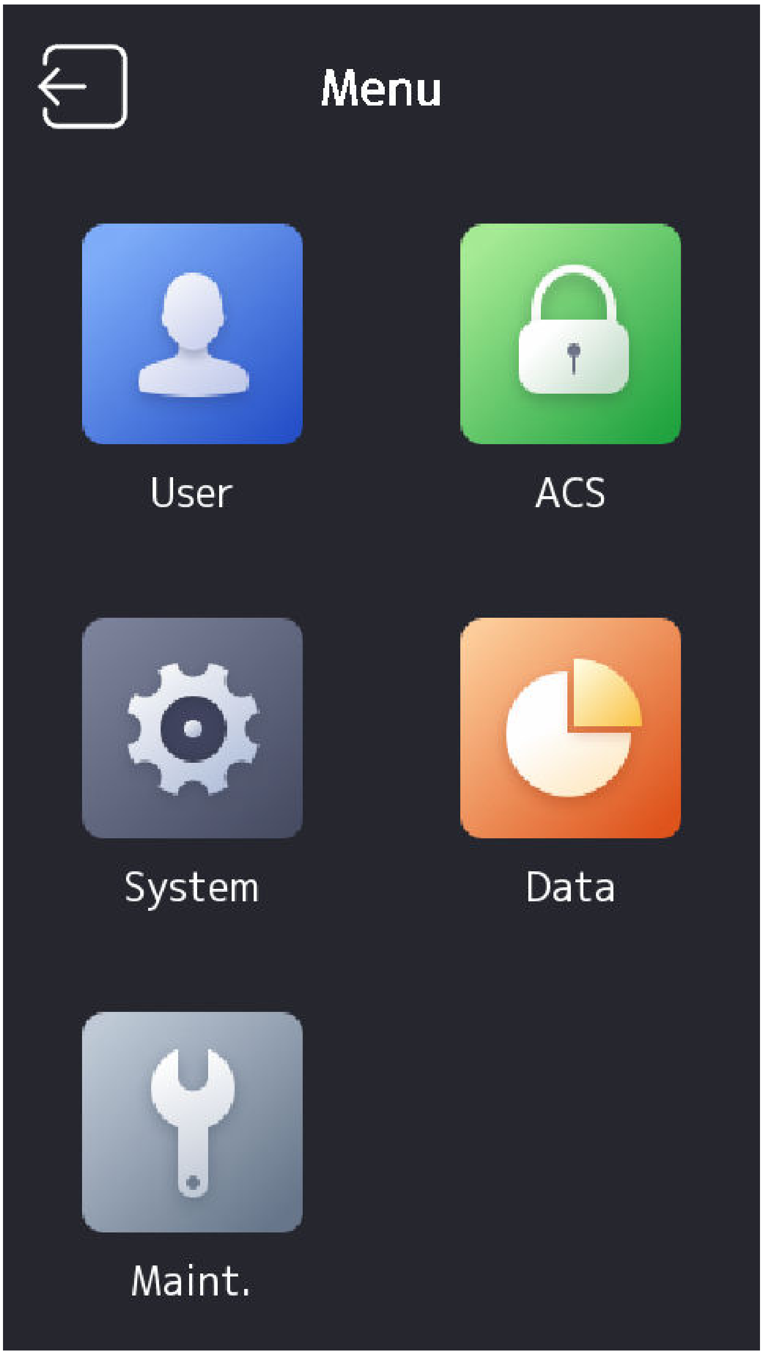


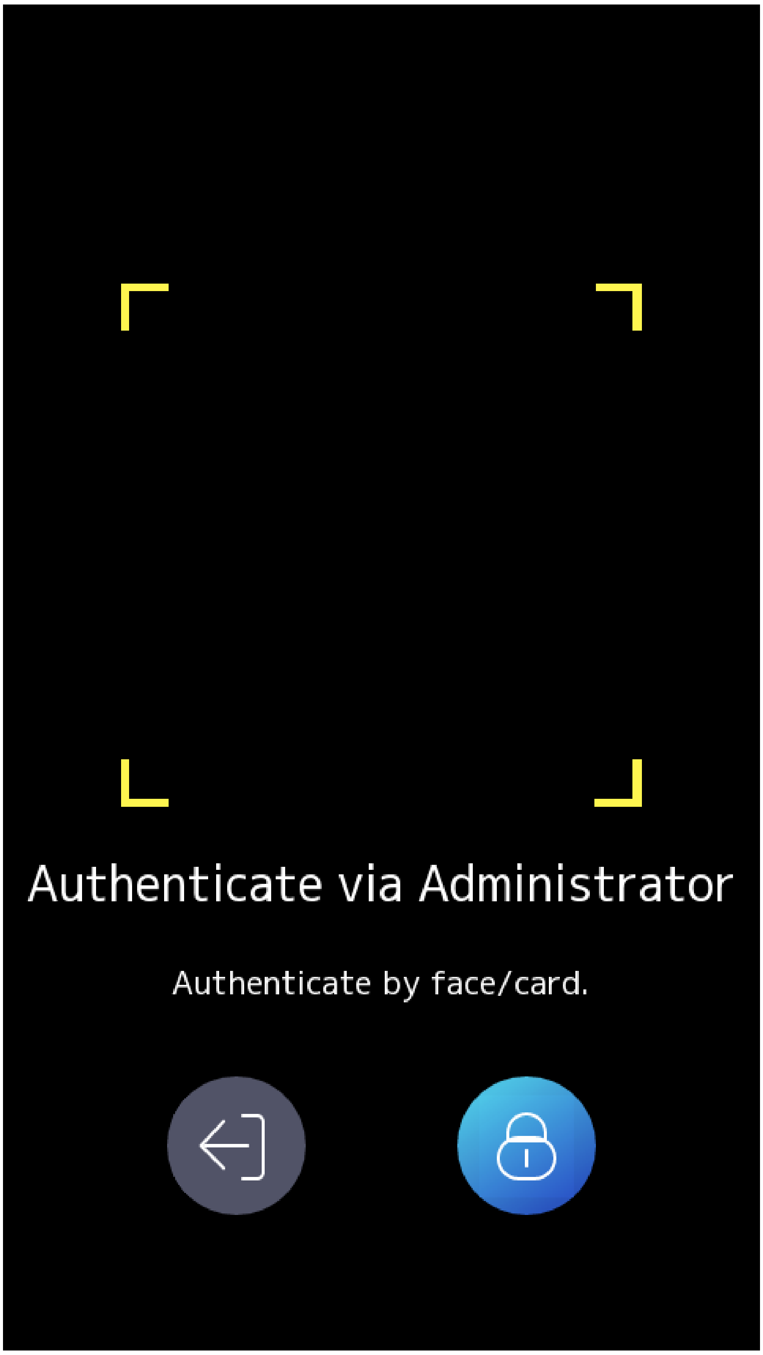
Figure 6-1 Home Page

6.1.2 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.



Authenticate via Administrator

Authenticate by face/card.

Figure 6-2 Admin Login

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

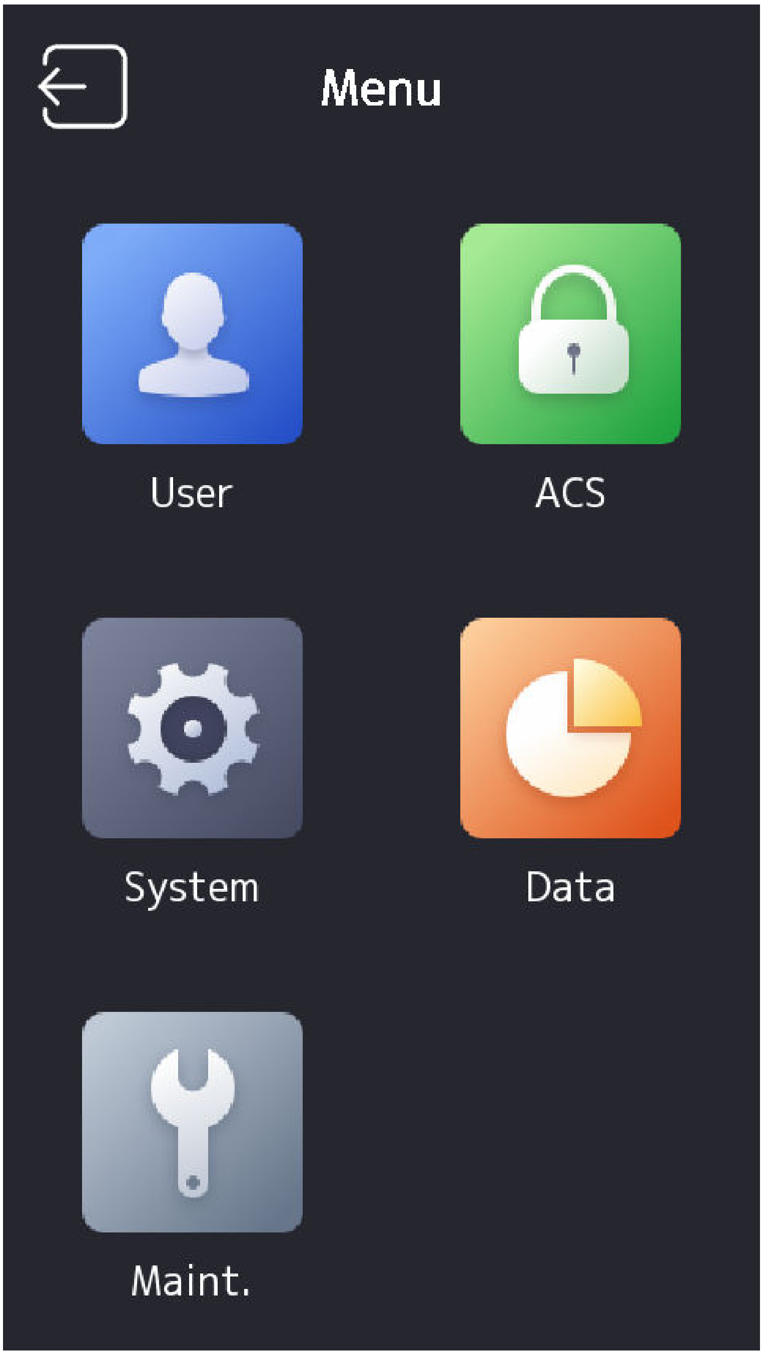


Figure 6-3 Home Page

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.

6.1.3 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**.

6.1.4 Change Device Password

You can change the device password by entering the old password.

Steps

1. Long tap on the initial page for 3 s and login the home page. Tap **System → Password** .
2. Tap **Change Device Password**.
3. Enter the device old password.

   Note

   If you forget your password, you can tap **Forgot Password** and change the password. For details, see ***Forgot Password*** .

4. Enter new 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).

5. Tap **OK**.

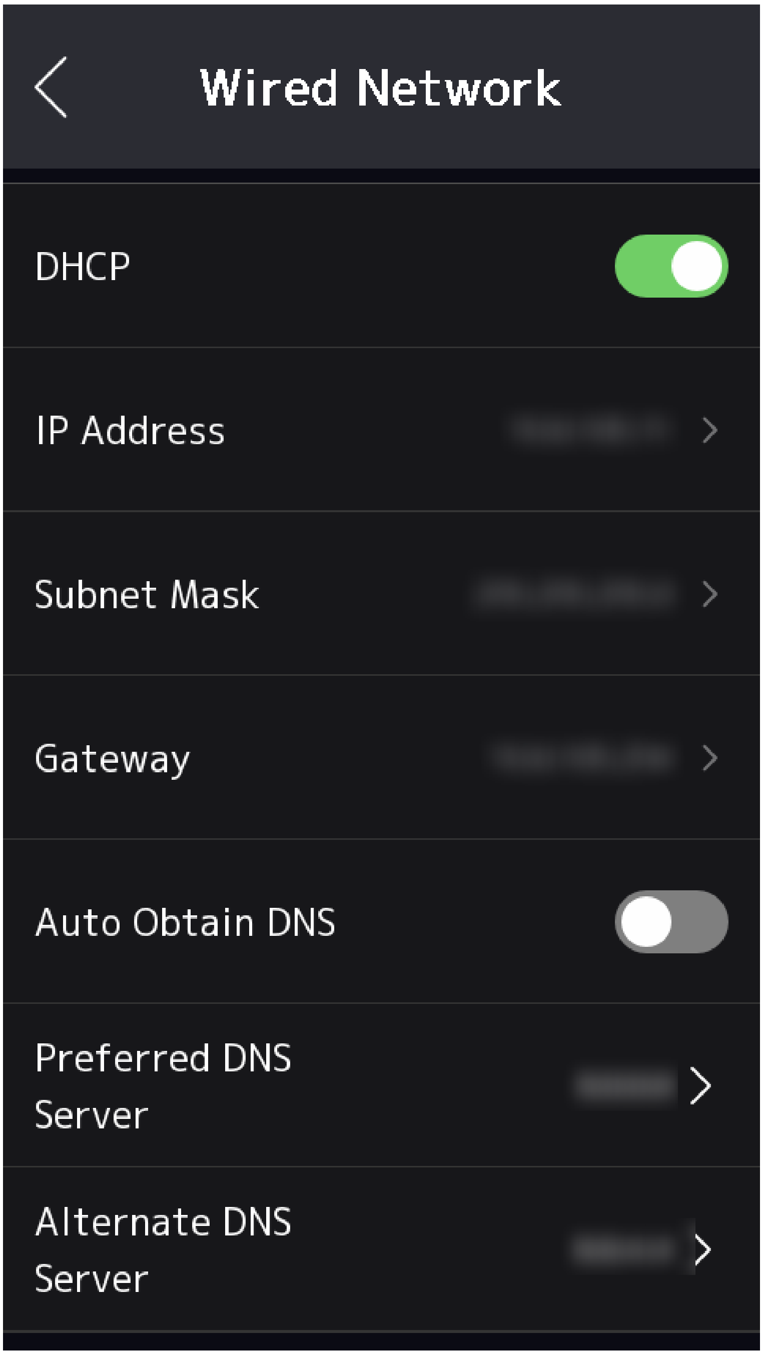
6.2 Communication Settings

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**.



Wired Network

DHCP ●

IP Address >

Subnet Mask >

Gateway >

Auto Obtain DNS ○

Preferred DNS Server >

Alternate DNS Server >

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

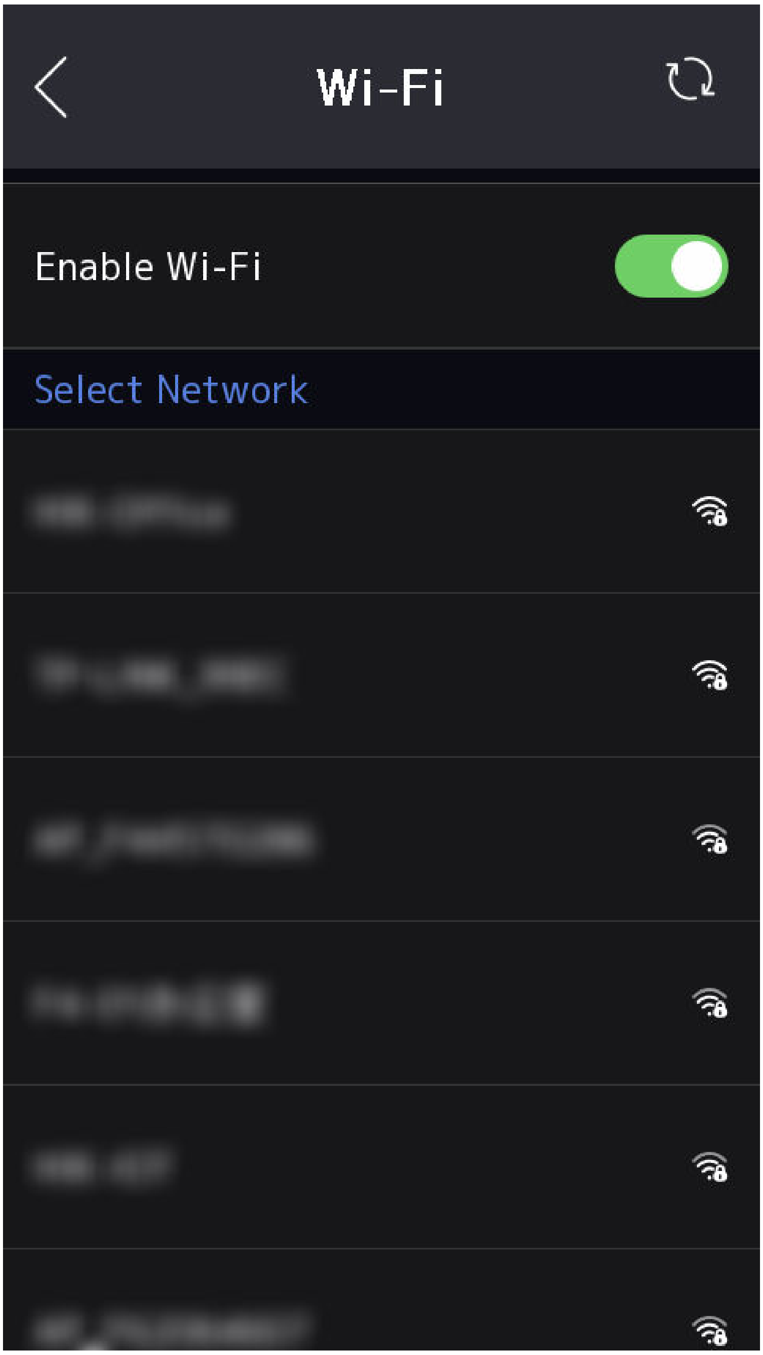
You can enable the Wi-Fi function and set the Wi-Fi related parameters.

Steps

Note

The function should be supported by the device.

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



Wi-Fi

Enable Wi-Fi

Select Network

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.

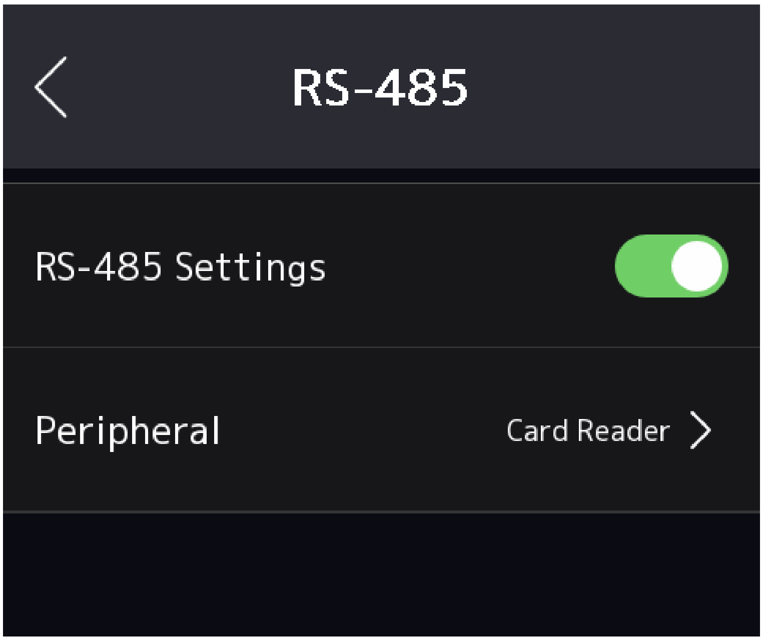
5. Set the Wi-Fi's parameters.
   - By default, DHCP is enable. The system will allocate the IP address, the subnet mask, and the gateway automatically.
   - If disable DHCP, you should enter the IP address, the subnet mask, and the gateway manually.
6. Tap **OK** to save the settings and go back to 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, card reader, or QR code scanner via the RS-485 terminal.

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 **RS-485** to enter the RS-485 tab.



RS-485

RS-485 Settings

Peripheral Card Reader

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.

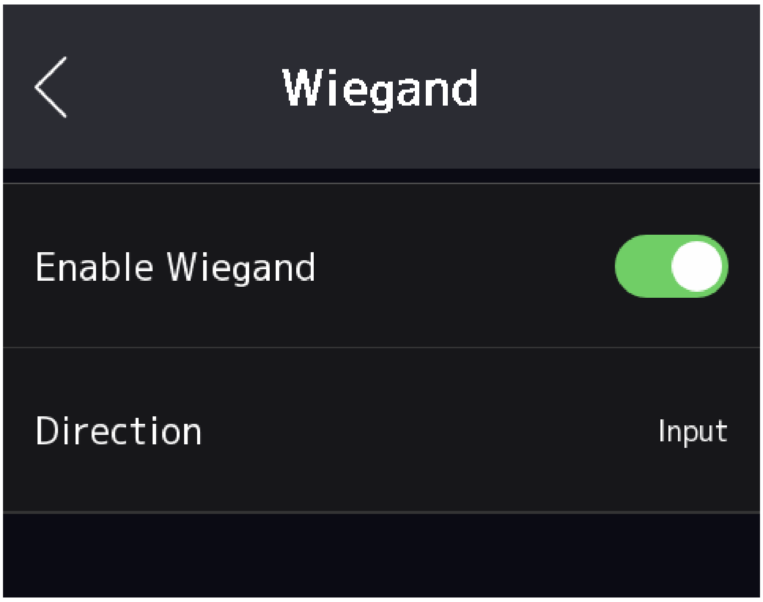
4. Tap the back icon at the upper left corner and you should reboot the device if you change the parameters.

6.2.4 Set Wiegand Parameters

You can set the Wiegand transmission direction.

Steps

1. Tap **System Settings → 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.



Wiegand

Enable Wiegand

Direction Input

Figure 6-7 Wiegand Settings

3. Enable the Wiegand function.
4. Select a Wiegand mode.
   - Output: A face recognition terminal can connect an external access controller. And the two devices will transmit the card No. via Wiegand 26 or Wiegand 34.
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

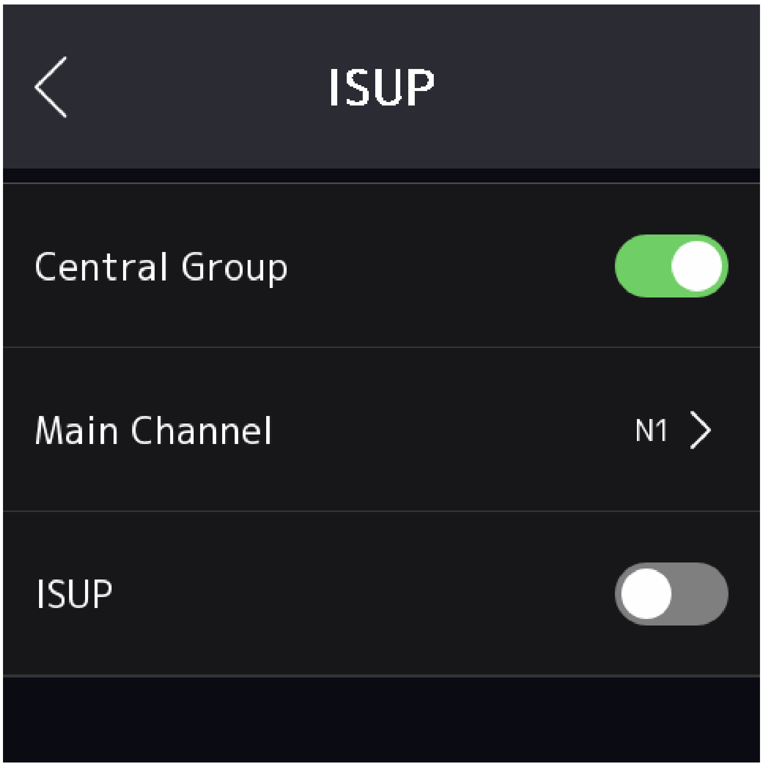
Set ISUP parameters and the device can upload data via ISUP protocol.

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.



ISUP

Central Group

Main Channel N1

ISUP

Figure 6-8 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

Note

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

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

6.2.7 Set AP Mode

You can enable AP mode, and add the device to Hik-Connect to set network.

Steps

1. Tap **System Settings → Comm.** (Communication Settings) on the Home page to enter the Communication Settings page.
2. Tap **AP Mode** to enter the settings page.
3. Enable AP mode. and use the phone's Wi-Fi function to connect the device hotspot.

Note

- Hotspot Name: Device serial No.
- Hotspot Password: Admin password.
- The device Wi-Fi will be disabled when the AP mode is enabled.

4. **Optional:** If the Wi-Fi adding page is not go to the web browser automatically after you connect to the device hotspot, you can enter ***www.acsvis.com*** manually in the phone's browser address bar to enter the mobile web login page.

6.3 Person Management

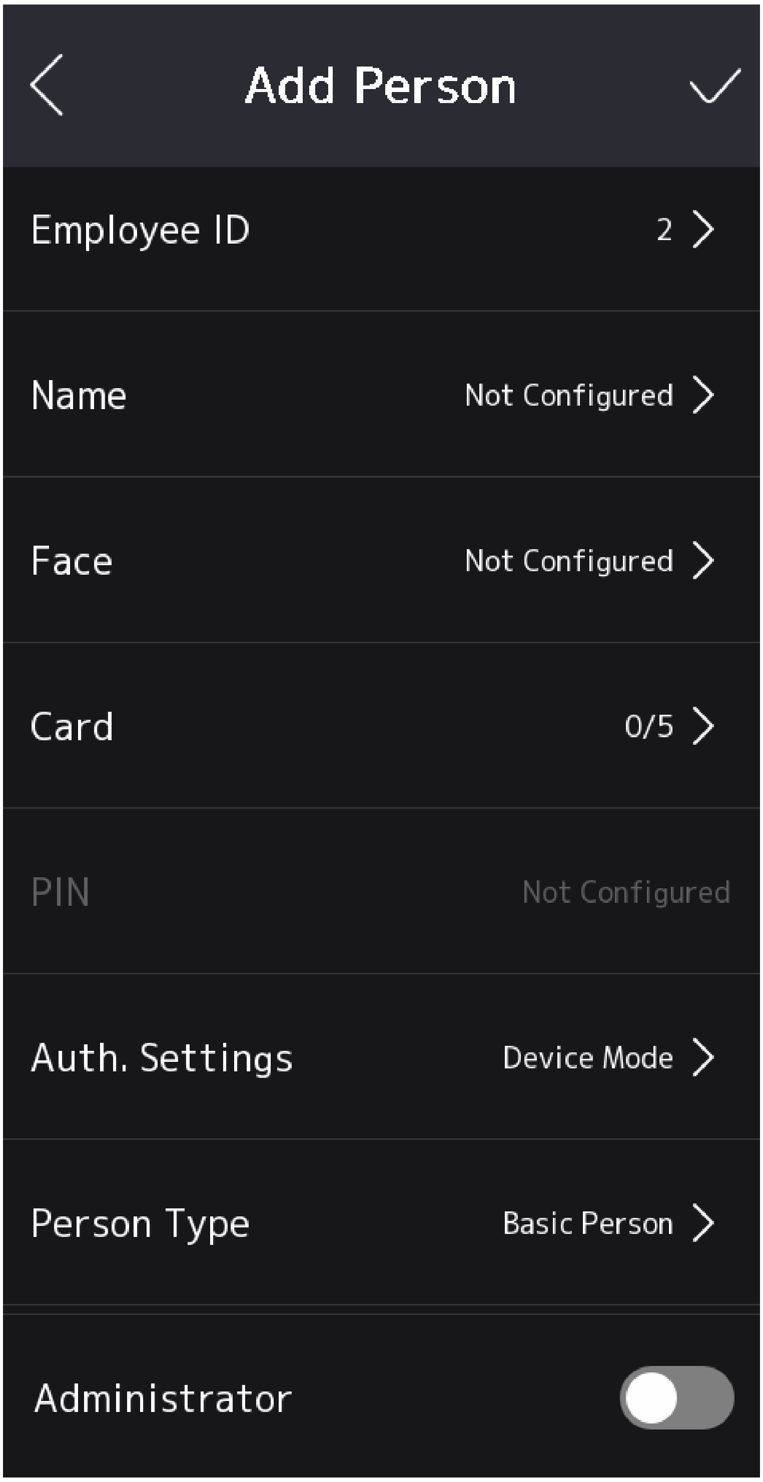
On the person management interface, you can add, edit, delete and search the person.

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.



Add Person

Employee ID 2

Name Not Configured

Face Not Configured

Card 0/5

PIN Not Configured

Auth. Settings Device Mode

Person Type Basic Person

Administrator

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 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 ***Add PIN*** .

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. Set **Door Permission**.
9. 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

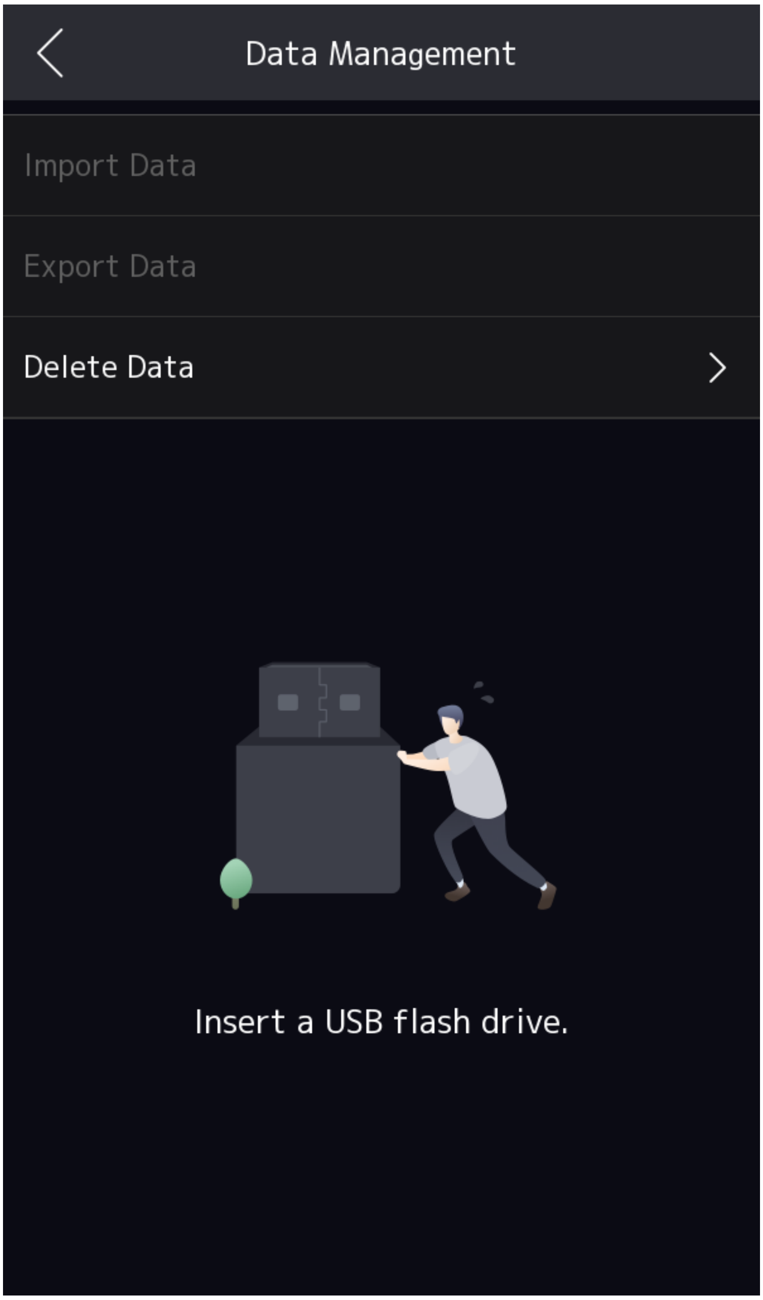
- Login Device A (The device that you need to export data). For details, see ***Login*** .
- Insert an USB flash drive to Device A.

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.



Data Management

Insert a USB flash drive.

Figure 6-9 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.

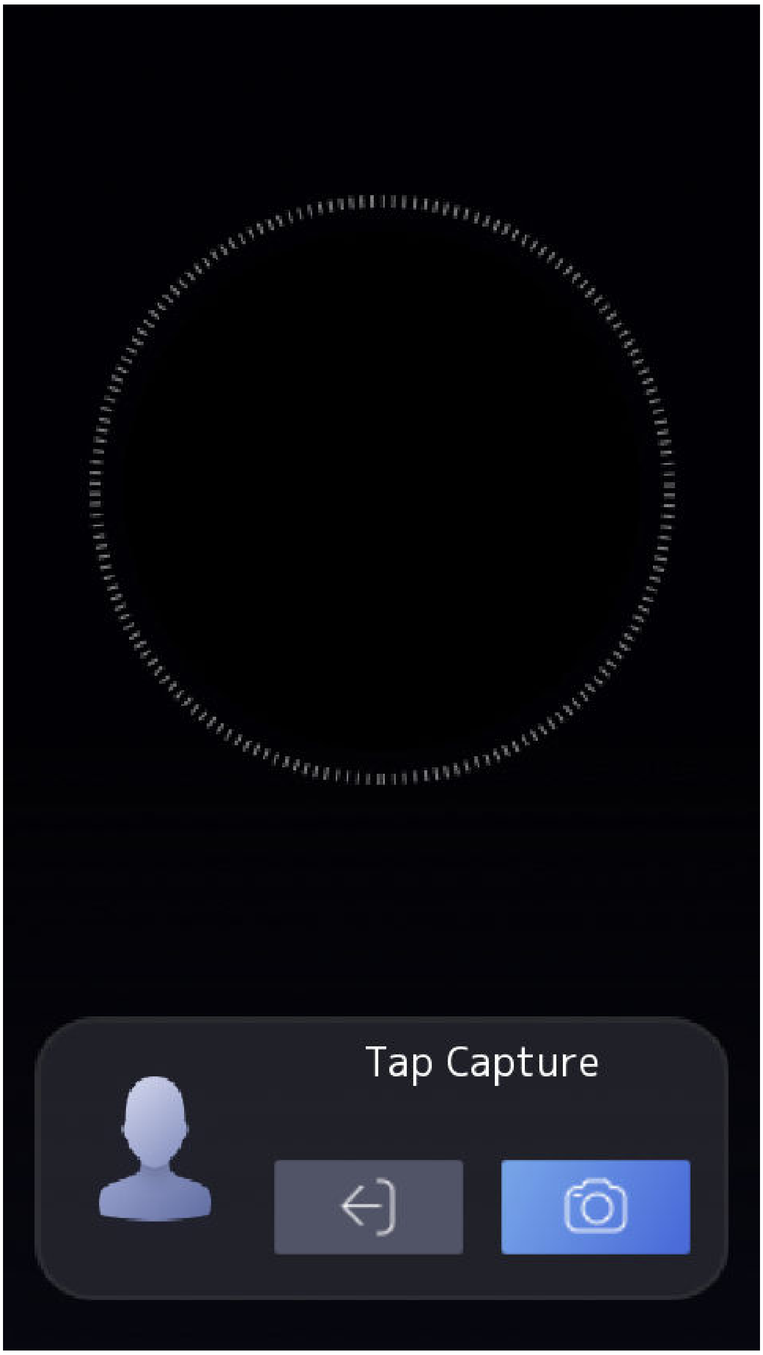


Figure 6-10 Add Face Picture

6. Look at the camera.

Note

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

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

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

Visitor

The person is a visitor.

Person in Blocklist

The person is in the blocklist. When the person starts authentication, an event will be upload.

Custom Type

Set the custom person type.

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 50 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 Add PIN

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

Before You Start

Note

Make sure the password mode is **Device-Set Personal PIN** or **Platform-Applied Personal PIN**. If you select **Device-Set Personal PIN**, you can add PIN on the device or Web. If you select **Platform-Applied Personal PIN**, you cannot add PIN on the device or Web, instead, you should add PIN on the platform. For details about setting the password mode, see ***Set Password Mode*** .

Steps

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

Note

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

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

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 PIN code and create a PIN for the user.

Note

Make sure the password mode is **Device-Set Personal PIN**, or the PIN area cannot be edtied.

6. Set the user role.

   Administrator

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

   Normal User

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

7. Tap ✓ to save the settings.

6.3.7 Set Person Type via Device

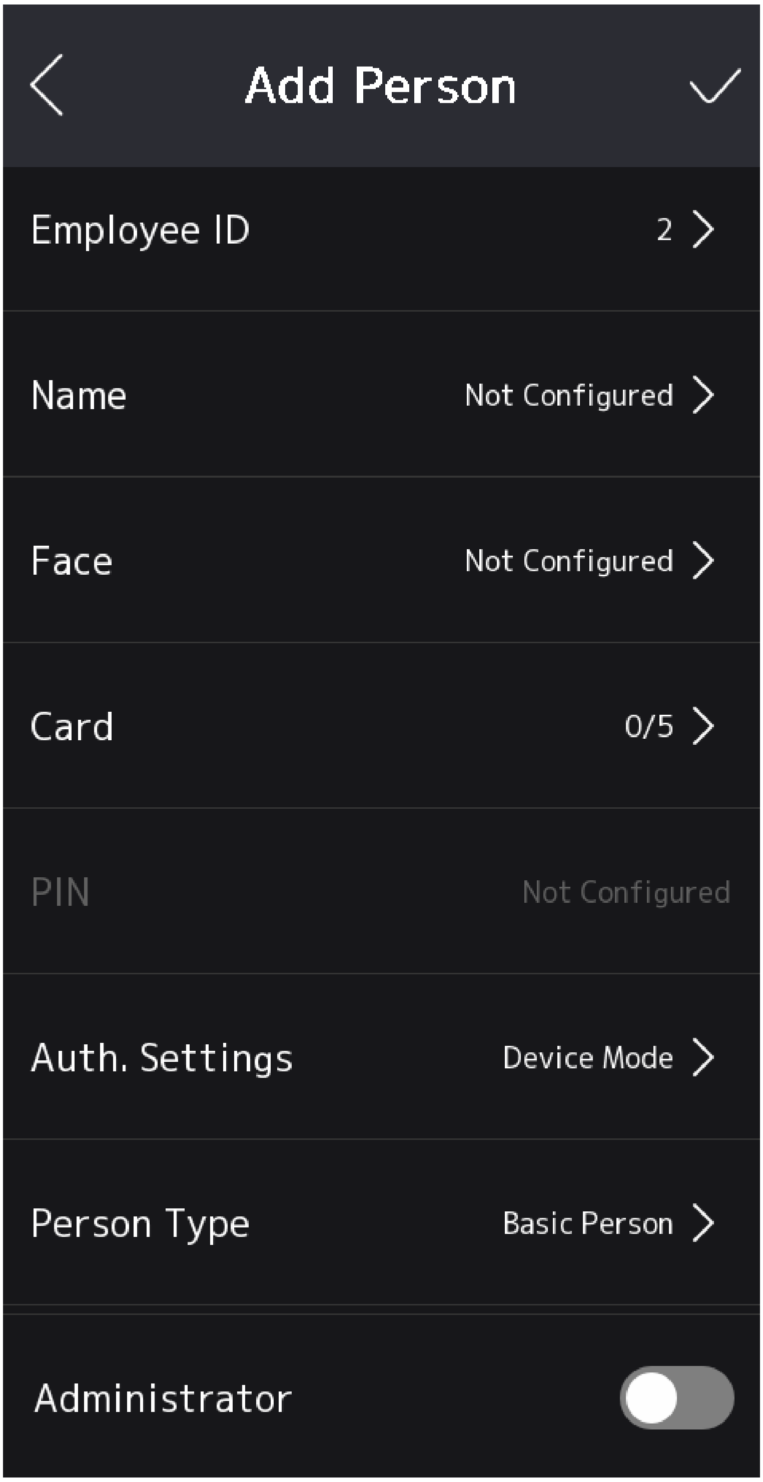
Set the person type as basic person, visitor, person in blocklist, or custom type.

Before You Start

Login the device. For details, see .

Steps

1. Tap **Person → +**.



Add Person

Employee ID	2
Name	Not Configured
Face	Not Configured
Card	0/5
PIN	Not Configured
Auth. Settings	Device Mode
Person Type	Basic Person
Administrator	○

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 or fingerprint.

Note

- Refers to , , and to add face, card, and fingerprint.
- Only device with fingerprint module supports the fingerprint functions.

5. Tap **Person Type** and set the type as **Basic Person**, **Visitor**, **Person in Blocklist** or **Custom Type**.

Note

- When setting the person to visitor, administrator cannot be set. If set the person as person in blocklist, you cannot configure the door permission for the person.
- Set the custom type’s name in PC web. After settings, the custom type will change to the configured name. For web settings, see .

6. Tap ✓ to save the settings.

6.3.8 Set Authentication Mode

After adding the person's face picture, password, or other credentials, you should set the authentication mode and the person 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.

6.3.9 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*** .

Note

The function are different according to different device models, refers to actual products.

Face

Face forward at the camera and start authentication via face.

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.
- You should enable QR code function in ***Preference Settings*** .

PIN

Enter the PIN to authenticate via PIN.

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. If the authentication mode is Card and Face, Password and Face, Card and Password, Card and Face and Fingerprint, 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.

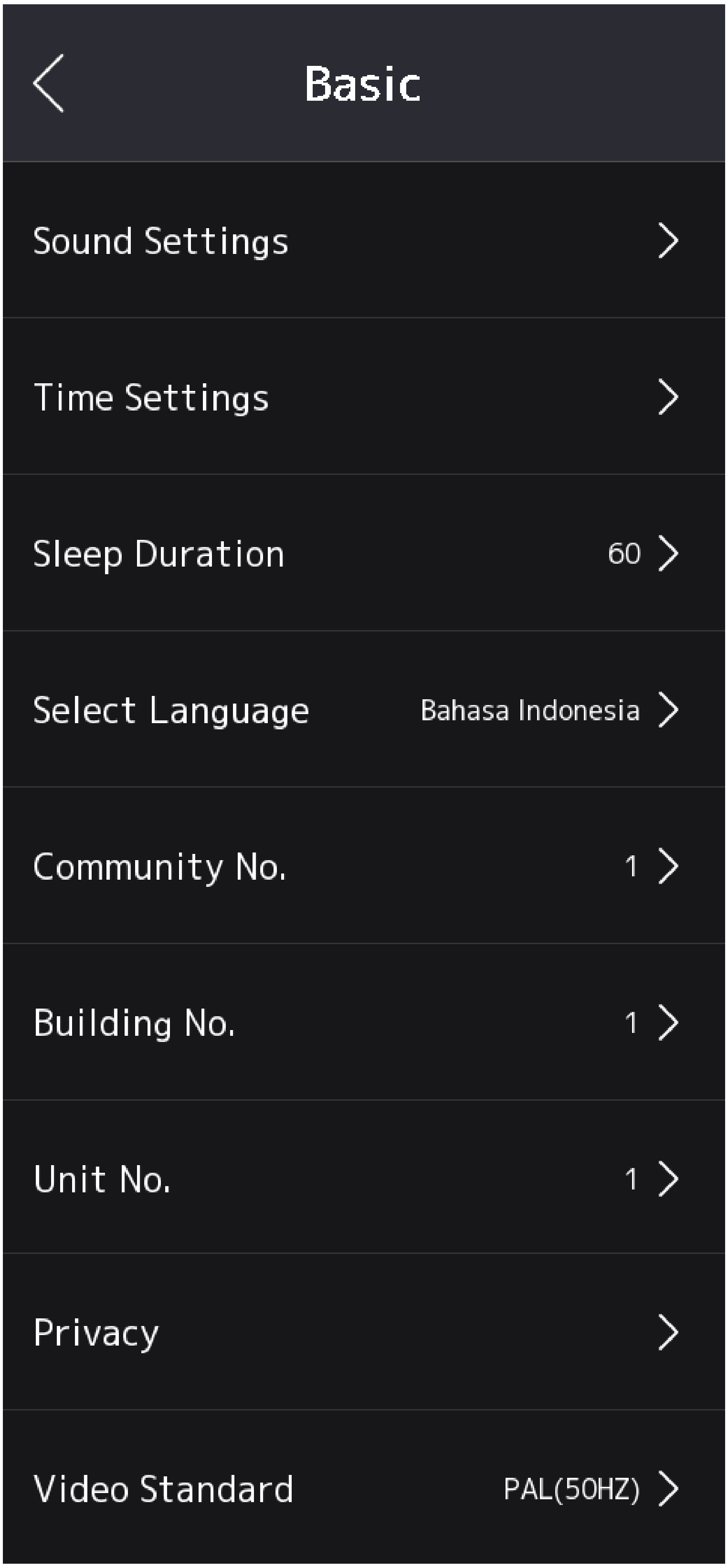
Note

- 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** .



Basic

Sound Settings

Time Settings

Sleep Duration 60

Select Language Bahasa Indonesia

Community No. 1

Building No. 1

Unit No. 1

Privacy

Video Standard PAL(50HZ)

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 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.**

6.6.6 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 .

Tap **System → Basic → Privacy**.

Authentication Settings

Name / Employee ID / Face Picture

You can choose to display/not display name, employ ID, or face picture when authenticating. You can choose to 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, the captured pictures will be saved to the device automatically.

Upload Picture 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.

6.6.7 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.

6.6.8 Set Secure Door Control Unit Parameters

You can wire peripherals according to the secure door control unit. You can set to use door 1 or door 2 to control the secure door control unit.

Before You Start

Device is wiring the secure door control unit by RS-485. For detailed wiring method, see .

Steps

1. Login the device. For details, see ***Login*** .
2. Go to **System → Basic → Secure Door Control Unit**.
3. Select **Door 1** or **Door 2** as door No.

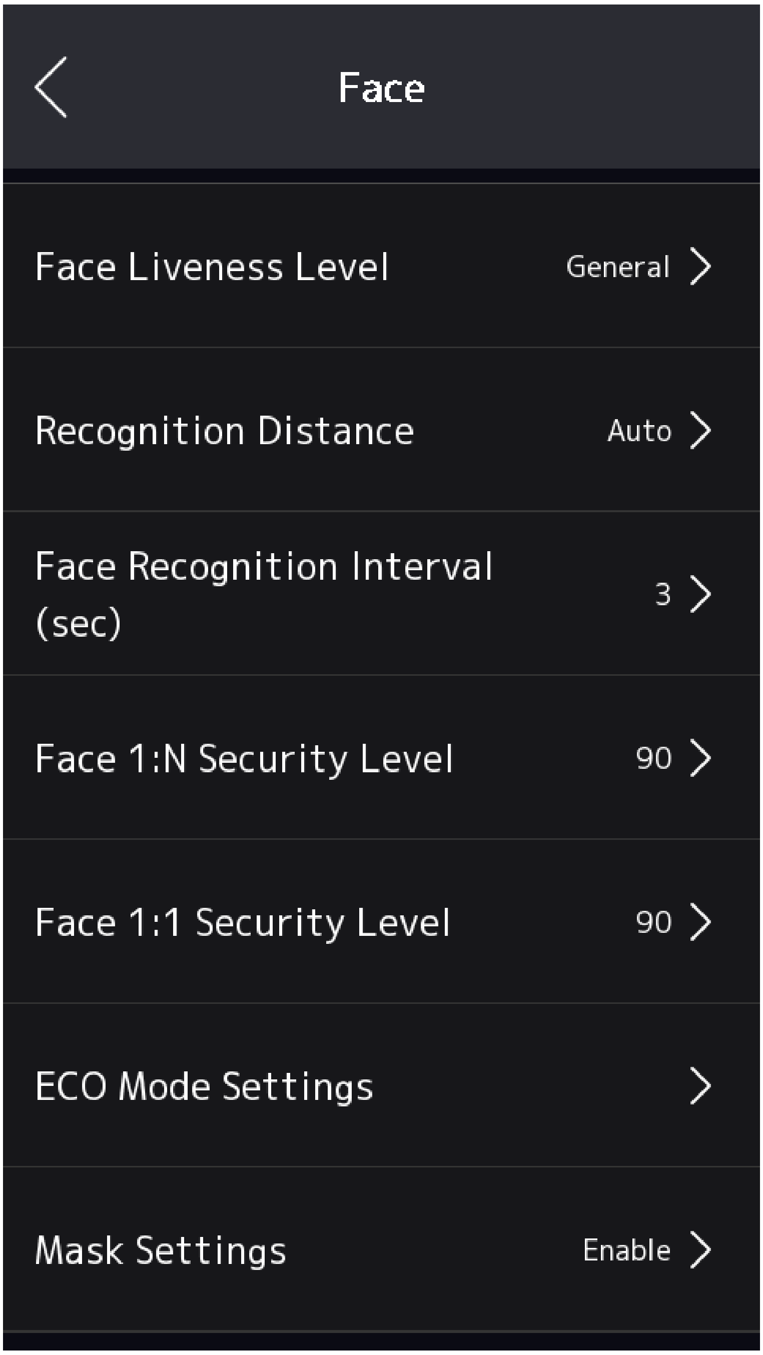
Note

Door 1 means that the door will be controlled by secure door control unit. The same goes to the selection of door 2.

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

Face Liveness Level General

Recognition Distance Auto

Face Recognition Interval (sec) 3

Face 1:N Security Level 90

Face 1:1 Security Level 90

ECO Mode Settings

Mask Settings Enable

Figure 6-13 Face Settings

6.7.1 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 .

Tap **System → Biometrics**.

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.

6.7.2 Set Recognition Distance via Device

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

Login the device. For details, see .

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

Set the recognition distance.

6.7.3 Set Face Recognition Interval via Device

The time interval between two continuous face recognitions when authenticating.

Login the device. For details, see .

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

Set the face recognition interval.

Note

Please enter a number between 1 and 10.

6.7.4 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 .

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

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

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

6.7.5 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 .

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

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

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

6.7.6 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 .

Tap **System → Biometrics → 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.

6.7.7 Enable/Disable Face 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 .

Tap **System → Biometrics → 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, the smaller the false accept rate and the larger the false rejection rate. 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, the smaller the false accept rate and the larger the false rejection rate. The maximum value is 100.

Prompt Method

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 Face Mask

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

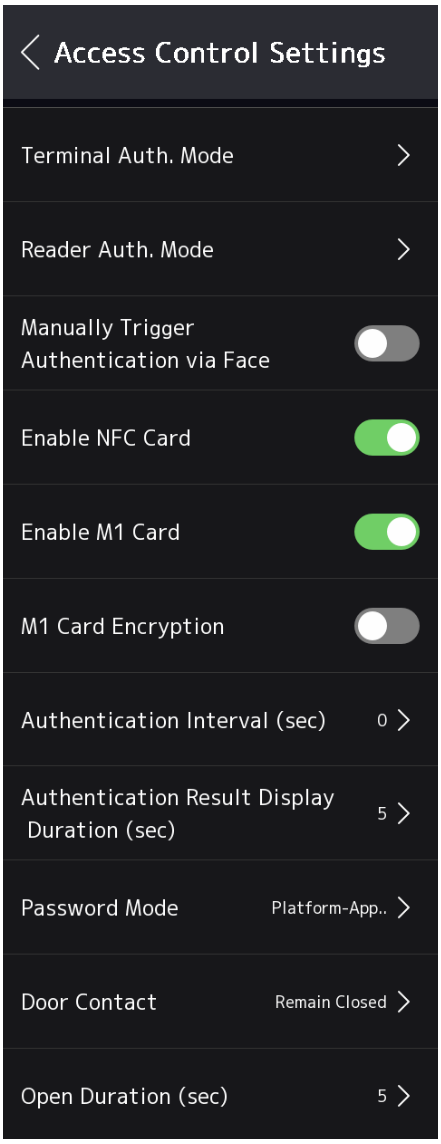
Must Wear

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

6.8 Access Control Settings

You can set the access control permissions.

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



Access Control Settings

Terminal Auth. Mode

Reader Auth. Mode

Manually Trigger Authentication via Face: Off

Enable NFC Card: On

Enable M1 Card: On

M1 Card Encryption: Off

Authentication Interval (sec): 0

Authentication Result Display Duration (sec): 5

Password Mode: Platform-App..

Door Contact: Remain Closed

Open Duration (sec): 5

Figure 6-14 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 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.

6.8.6 Set Authentication Result Display Duration via Device

Set the authentication result display duration when authenticating.

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

Tap **ACS**, and set **Authentication Result Display Duration** and save.

6.8.7 Set Password Mode

You can set the password mode and choose whether to edit password on device / PC web, or platform.

Steps

1. Login the device. For details, see ***Login*** .
2. Tap **ACS**.
3. Tap **Password Mode** and set the mode.

   Platform-Applied Personal PIN

   The PIN is managed and distributed by the platform after the device accesses the platform.

   Device-Set Personal PIN

The PIN is set on the device or PC Web.

4. Go back to the previous page to save the settings.

6.8.8 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.

6.8.9 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 Preference Settings

You can configure preference settings parameters.

Steps

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

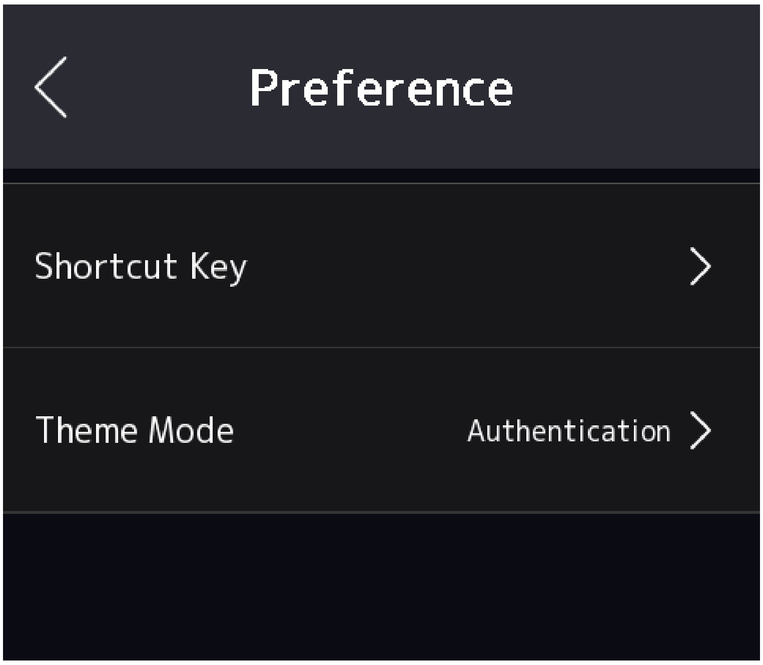


Figure 6-15 Preference Settings

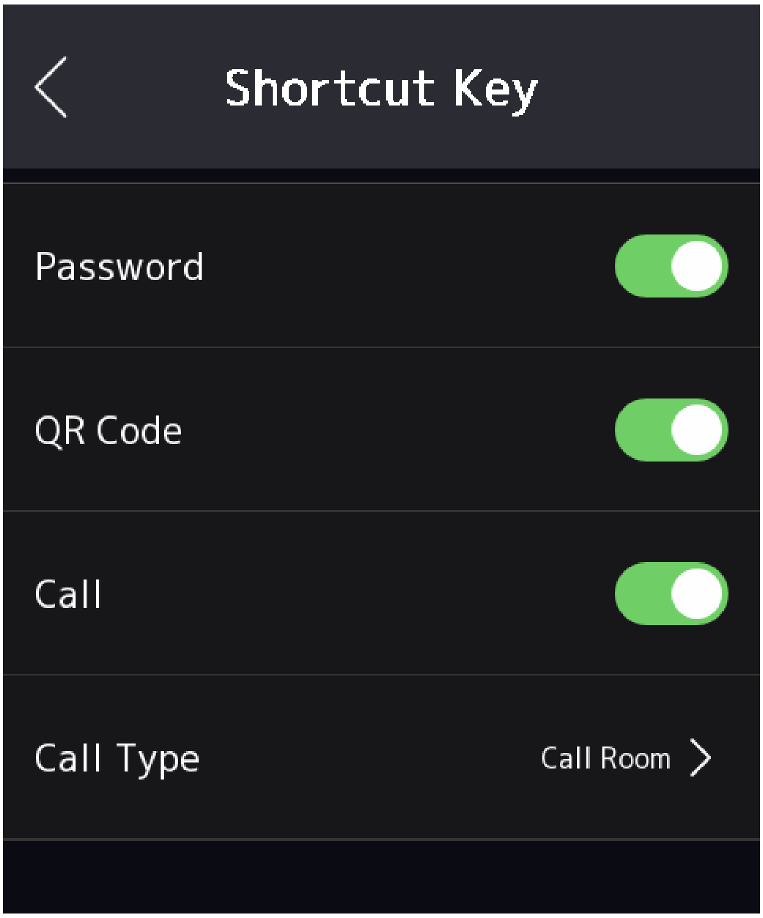
6.9.1 Set Shortcut Key via Device

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 .

Tap **System → Preference → Shortcut Key**.

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



Shortcut Key

Password

QR Code

Call

Call Type: Call Room

Figure 6-16 Shortcut Key Settings

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.

6.9.2 Theme

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

Login the device. For details, see .

Tap **System → Preference → Theme Mode**.

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.

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.

6.10 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.**

6.10.1 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 **Face** parameters and view the device **Version Information**.

Face

Custom Anti-Spoofing Detection

You can set **Face Liveness Level**, **Anti-Spoofing Detection Threshold**, and **Anti-Spoofing Detection Threshold of Face with Mask**.

Note

You can set the value between 1 and 100. The smaller the value, the larger the false accept rate and the smaller the false rejection rate. The larger the value, the smaller the false accept rate and the larger the false rejection rate.

Lock Face for Anti-Spoofing Protection

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

Locking Duration

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

Version Information

You can view the device version.

6.10.2 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 capacity of person, face picture, card, fingerprint and event.

Note

Only device installed with fingerprint module supports display fingerprint capacity.

6.10.3 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.

6.10.4 View User Manual

You can view the QR code of the user manual.

Tap **System Maintenance → User Manual** , scan the QR code to view the user manual.

6.10.5 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**.

6.11 Video Intercom

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

6.11.1 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.

6.11.2 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.

6.11.3 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.

6.11.4 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.

6.11.5 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 Configure Device via Mobile Web

7.1 Login

You can login via mobile browser.

Note

- Make sure the device is activated. For details, see .
- Enable the device Wi-Fi function and set an IP for the device. Make sure the device and the mobile phone are in the same Wi-Fi. For details, see .

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

Or after enabling the device hotspot, you can search the device hotspot in the phone Wi-Fi settings page, enter the device activation password to enter the login page. For details, see ***Set Device Hotspot*** .

Enter user name and device password, and tap **Login**.

7.2 Forget Password

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

Steps

1. On the login page, tap **Forget Password**.
2. Select Verification Mode.

   Security Question Verification

   If you have set security questions on the device or mobile web, you can enter the answers to reset the password. Tap **Security Question Verification**, and tap **Next**.
3. Enter the answer of the security question, and tap **Next**.
4. Enter the new password and confirm it.
5. Tap **Next**.

7.3 Account Security Settings

Change the reserved phone No. and when you forgot the password, you can use the phone No. to change the login password.

Steps

Note

Only the device and the phone are in the same LAN, can you see the settings.

1. Tap ≡ → **User Management →** ··· **→ Account Security Settings**.
2. Select a password reset method and start to edit.
   - Security Question: Edit the answer of the questions. When you forget your password, you can use the answers to change the password.
   - E-mail Address: Download mobile app and go to More -> Reset Device Password. Scan the QR code on the device and a verification code will be popped up. When you forget your login password, you can enter the phone No. to change the password.
3. Tap **Save**.

7.4 Home

You can view the door status, enter the configuration page via shortcut entry, view the network status, and view basic information.

Door Status

You can view the door status. And control the door status.

Shortcut Entry

Tap the configuration function name and enter the page.

Network Status

You can view the network connection status.

Basic Information

You can view the device model, serial No., and version, or enter the basic information page.

7.5 Configuration

7.5.1 View Device Information

View the device name, language, model, serial No., version, number of channels, IO input number, local RS-485 number, register No., Mac address, factory information and device capacity, etc.

On the home page, tap ≡ **→ System Settings → Basic Information**.

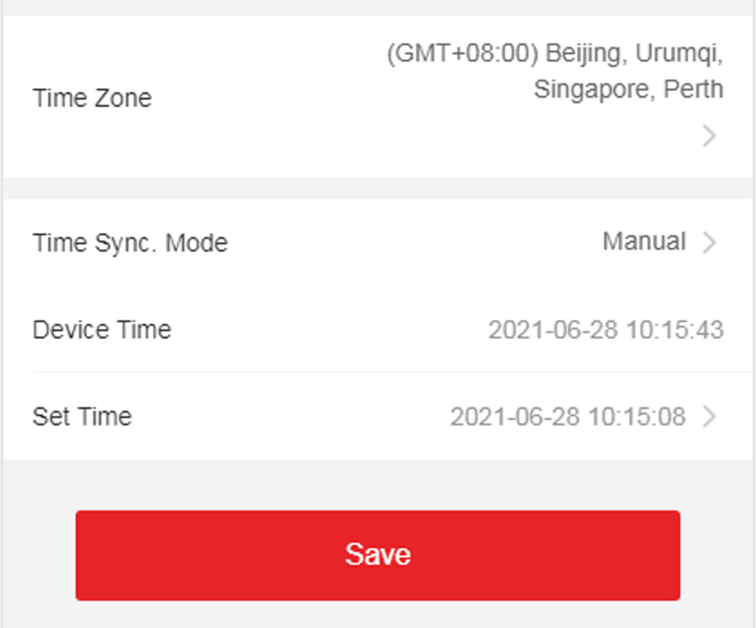
View the device name, language, model, serial No., version, number of channels, IO input number, local RS-485 number, register No., Mac address, factory information and device capacity, etc.

Tap **Save**.

7.5.2 Set Device Time

Set the time zone of the device and the device current time.

Tap ☰ → **System Settings** → **Time Settings**.



Time Zone (GMT+08:00) Beijing, Urumqi, Singapore, Perth

Time Sync. Mode Manual

Device Time 2021-06-28 10:15:43

Set Time 2021-06-28 10:15:08

Figure 7-1 Time Settings

Time Zone

Tap to select a time zone for the device.

Time Sync. Mode

Manual

By default, manually synchronization is checked, you can set the device time manually.

NTP

You should Set the NTP server’s IP address, NTP port, and interval.

Tap **Save**.

7.5.3 User Management

Changed the user’s password.

On the home page, tap ☰ → **User Management**.

Tap the user, enter the old password, create a new password and confirm the password. Tap **Save**.

7.5.4 Network Settings

Set Wired Network Parameters

Set wired network parameters of the device.

Before You Start

The device is connected to a wired network.

Steps

1. On the home page, tap ☰ → **Communication Settings → TCP/IP** .
2. Set the wired network parameters.

   NIC Type

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

   DHCP

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

   If enabled the function, the system wil allocate IPv4 address, IPv4 subnet mask, IPv4 default gateway, and MTU.

   Preferred DNS Server and Alternate DNS Server

   Set the DNS server IP.
3. Tap **Save**.

Set Wi-Fi Settings

Set the Wi-Fi parameters of the device.

Before You Start

After the device is added to the App, you can enabled the device Wi-Fi function. And then you can set eh Wi-Fi parameters in the mobile web.

Steps

1. On the home page, tap ☰ → **Communication Settings → Wi-Fi**.
2. Enable **Wi-Fi**.
3. Select a Wi-Fi in the list and enter the password to connect.
4. **Optional:** Add a Wi-Fi.
   1) Slide the page to the end and tap **Add Network**.
   2) Enter **Wi-Fi Name**, and select the Wi-Fi’s **Encryption Type**.
   3) Tap **OK**.
5. **Optional:** Set WLAN.
   1) Set the connected Wi-Fi’s name, and view the network details.

2) Tap **WLAN Settings**.
3) Set the WLAN parameters.

Enable DHCP

Enable **DHCP** to **Auto DNS**, the device will allocate the IP and DNS automatically.

Disable DHCP

Manually set the IP and DNS server.

4) Tap **Save**.

Result

After Wi-Fi and WLAN settings, you can enter the WLAN IP address in the mobile browser to login the device.

Device Hotspot

After enabling the device hotspot, you can use the mobile phone to connect the hotspot and set.

Note

You can set the parameters only when you connect the device by hotspot. If you login the device by IP address, the function is not supported.

On the home page, tap ≡ → **Network Settings** → **Device Hotspot**.

Enable **Device Hotspot** and tap **Save**.

The device will in hotspot mode. The indicator will flash green.

If disable the function, the indicator will remain green.

Set Port

You can set HTTP Port, RTSP Port, HTTPS Port, and Server Port. When accessing the device through the network, you can set the corresponding port according to your needs.

On the home page, tap ≡ → **Network Service** → **HTTP(S)**.

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.

Cloud Service Accessing

The device can communicate via cloud service. You can add the device to mobile client and operate.

Steps

1. Tap ≡ → **Device Access** → **Hik-Connect** → **Guarding Vision** .
2. Check **Enable**.
3. **Optional:** You can enable **Custom** and edit the server IP address.
4. **Optional:** View the network connection status.
5. **Optional:** You can select to enable video encryption, and set the video encryption password.

   Note

   After the device adding to the mobile App, if you need to start live view, you should enter the video encryption password.
6. **Optional:** Tap **Link with Account** and view the device QR code. Use the App to scan the QR code to add the device.
7. Tap **Save**.

Set ISUP Parameters

Set the ISUP parameters for transmitting logs via ISUP protocol.

Tap ≡ → **Device Access** → **ISUP**.

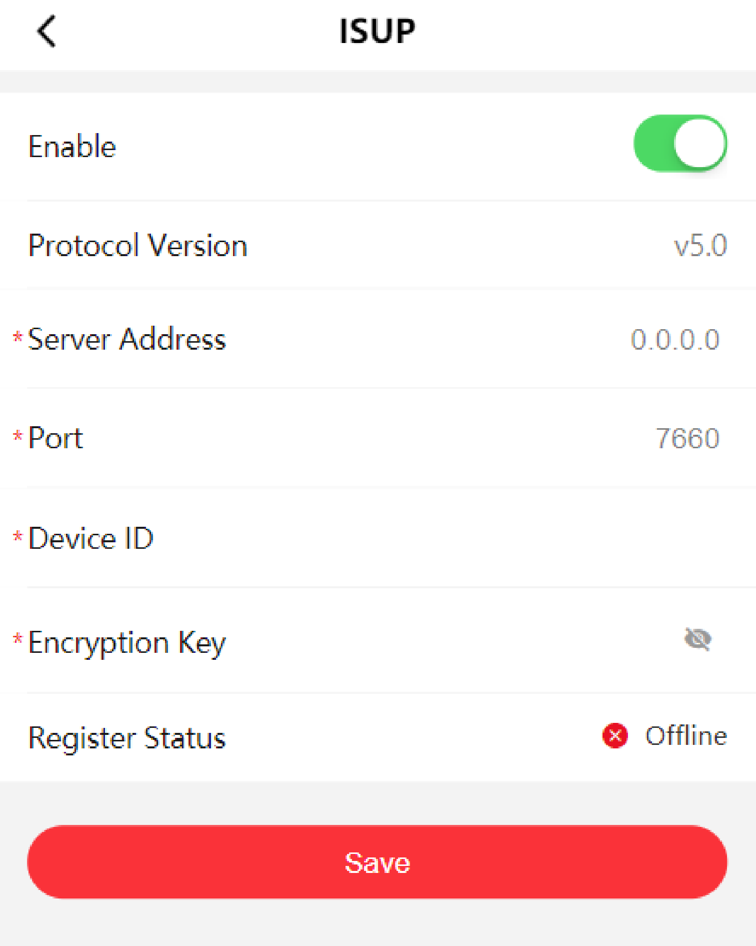
Slide **Enable** to enable ISUP.

Set the server address and port.

Note

The protocol version is 5.0, you should set the encryption key.

Tap **Save**.



Enable

Protocol Version v5.0

*Server Address 0.0.0.0

*Port 7660

*Device ID

*Encryption Key

Register Status Offline

Figure 7-2 ISUP Settings Page

Set OTAP Protocol

You can access the device to the maintenance platform by OTAP protocol to realize searching and gaining device information, uploading device running status and exceptions, rebooting and upgrading.

Steps

1. Tap ≡ → **Device Access** → **OTAP** .

Object Missing

This object is not available in the repository.

Figure 7-3 OTAP

2. Slide **Enable**.
3. Set server address, port, device ID and encryption key.
4. Tap **Test**, and make sure the device can connect to the server and registration completed.
5. Tap **Save**.

Result

Refresh the web page or reboot the device to make sure the OTAP’s **Register Status** turns to online.

VoIP Settings

Devices in different network segments can communicate with each other via the server. If not registered to the VoIP, the terminals can only communicate with each other in the same network segment. After registering to the VoIP server completed, terminals can call each other via by entering VoIP ID.

Steps

1. Tap ☰ → **Device Access** → **VoIP** .
2. Enable **VOIP**.
3. Enter **Registered User Name** and **Registration Password** of the VoIP server.
4. Set VoIP server’s **Server IP Address** and **Server Port**.
5. **Optional:** Set **Expiry Time** and view the **Register Status**.
6. Create a **Number** and **Display User Name**.
7. Tap **Save**.

7.5.5 Add Person

Add Person Basic Information

Tap ☰ → **Person Management** → **+**.

Create person employee ID, name, floor No., and room No.
Tap **Save**.

Set Person Permission

Tap ☰ → **Person Management** → **+**.
Enable **Long-Term Effective User** and set the start time and end time of the person.
Tap **Save**.

Set Administrator

Tap ☰ → **Person Management**.
Enable **Administrator** and the person can use the credential to login the device.
Tap **Save**.

Select User Role.

Tap ☰ → **Person Management** → **+**.
Tap **User Role** and set the type as **Normal User**, **Visitor**, **Person in Blocklist** or **Custom Type**.

Note

- When setting the person to visitor, administrator cannot be set. If set the person as person in blocklist, you cannot configure the door permission for the person.
- Set the custom type's name in PC web. After settings, the custom type will change to the configured name. For web settings, see .

Add Face Picture

Tap ☰ → **Person Management** → **+** → **Face**.
Tap **Camera** to add a face picture. Or tap **Choose from Album** to select a face picture from the phone photo library.
Tap **Add**.

Add Fingerprint

Tap ☰ → **Person Management** → **+** → **Fingerprint**.
Tap **+** and put your finger on finger recognition module.

Add Card

Tap ☰ → **Person Management** → **+** → **Card**.
Tap **+**, enter the card No. and select a card property (type).
Tap **Save**.

Add PIN

Note

Before configuring passwords, it is necessary to clarify whether the password is a device-set personal PIN or a platform-applied personal PIN. If it is a device-set personal PIN, it can be created or edited on the device or on the web, and cannot be set on other platforms; If it is a platform-applied personal PIN, it can be created or edited on the platform, and issued to the device before it can be used. It cannot be set on the device or on the web.

Tap ≡ → **Person Management** → **+**.
Enter PIN in the PIN entering area.

7.5.6 Event Search

Tap ≡ → **Event Search**.

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

Note

Support searching for names within 32 digits.

The result will display in the list.

7.5.7 Audio Settings

You can enable or adjust the audio.

Tap ≡ → **Audio**.

Enable **Enable Voice Prompt** according to actual needs. The device will prompt voice instructions. You can also adjust the audio volume.

7.5.8 Access Control Settings

Set Authentication Parameters

Set authentication parameters.

Steps

1. Tap ≡ → **Access Control** → **Authentication Settings**.
2. After settings, tap **Save**.

   If select **Terminal** as **Main Card Reader**.

   Terminal

   Select terminal for settings.

   Terminal Type

   Display the terminal's type. Read only.

   Terminal Model

When the terminal is online, it will display the terminal's model, or it will display offline. (Read-only)

Enable Authentication Device

If enable the function, you can authenticate credential on the terminal; or you cannot use credential to authenticate.

Authentication Mode

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

Continuous Face Recognition Interval

Set the interval between 2 continuous recognition of a same person during the authentication. In the configured interval, the same person can only recognized once.

Authentication Interval

You can set the authentication interval of the same person when authenticating. The same person can only authenticate once in the configured interval. A second authentication will be failed. If there is another person authenticate in the configured interval, the person can authenticate again.

Alarm of Max. Failed Attempts/Max. Authentication Failed Attempts

Enable **Alarm of Max. Failed Attempts** and you can set the max. authentication failed attempts. When the authentication attempts reach the set value, the authentication will be failed and report to center.

Home Page Mode

You can set the device home page as **Authentication Mode** or **Simple**.

Authentication Mode

If select **Authentication Mode**, the authentication page will display the live view page only.

Simple

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.

Enable Tampering Detection

After enabling the function, when the card reader is removed, an alarm will be triggered. If the function is disabled, the alarm will not be triggered.

Enable Card No. Reversing

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

If select **Terminal** as **Sub Card Reader**.

Terminal

Select terminal for settings.

Terminal Type

Display the terminal’s type. Read only.

Terminal Model

When the terminal is online, it will display the terminal's model, or it will display offline. (Read-only)

Enable Authentication Device

If enable the function, you can authenticate credential on the terminal; or you cannot use credential to authenticate.

Authentication Mode

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

Continuous Face Recognition Interval

Set the interval between 2 continuous recognition of a same person during the authentication. In the configured interval, the same person can only recognized once.

Alarm of Max. Failed Attempts/Max. Authentication Failed Attempts

Enable **Alarm of Max. Failed Attempts** and you can set the max. authentication failed attempts. When the authentication attempts reach the set value, the authentication will be failed and report to center.

Home Page Mode

You can set the device home page as **Authentication Mode** or **Simple**.

Authentication Mode

If select **Authentication Mode**, the authentication page will display the live view page only.

Simple

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.

Communication with Controller Every

If the card reader cannot communicate with the controller within the configured time duration, the card reader will be regarded as offline.

Max. Interval When Entering Password

Set the maximum interval of entering 2 characters of the PIN. After entering one character, if the next character is not entered within the set interval, the entered characters will all be automatically cleared.

OK LED Polarity/Error LED Polarity

Select anode or cathode of the main board.

Enable Tampering Detection

After enabling the function, when the card reader is removed, an alarm will be triggered. If the function is disabled, the alarm will not be triggered.

Set Door Parameters

Set door parameters, including door name, open duration, exit button type, door remain open duration with first person, door open timeout alarm, door contact, extended open duration, duress code, super password.

Tap ≡ → **Access Control** → **Door Parameters**.

After settings, tap **Save**.

Name

Create a name for the door.

Open Duration

Set the door unlocking duration after swiping the card.

Exit Button Type

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

Door Remain Open Duration with First Person

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

Door Opening Timeout Alarm Threshold

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.

Door Contact

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

Door Lock Powering Off

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

Extended Open Duration

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

Duress Code

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

Super Password

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

Note

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

Set Terminal Parameters

You can set terminal parameters for accessing.

Tap ≡ → **Access Control** → **Terminal Parameters**.

Working Mode

You can set Working Mode as Access Control Mode.

Access Control Mode

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

Tap **Save**.

Set RS-485 Parameters

You can connect to access controller ,extension module, or card reader via RS-485. Set the RS-485 parameters and connect to other devices.

Tap ≡ → **Access Control** → **RS-485** .

After settings, tap **Save**.

Peripheral Type

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

Note

After changing the device type, when you save the parameters, the device will reboot.

RS-485 Address

Set the RS-485 address.

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.

Data Bit

The data bit when the devices are communicating via the RS-485 protocol.

Parity/Flow Ctrl/Communication Mode

Enabled by default.

Output Type

Set the output type according to your actual needs.

Set Card Security

Set the device card parameters.

在手机网⍰端主⍰点⍰ ≡ → **⍰禁配置** → 卡片安全。

配置卡片相关参数，点⍰**保存**。

Enable NFC Card

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. 通⍰启用 NFC 功能，使⍰禁⍰⍰⍰⍰受保⍰。

启用 **M1** 卡

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

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. Set the sector No.

Sector

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

Note

You are advised to encrypt sector 13.

Enable EM Card

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

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 CPU Card

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

CPU Card Read Content

After enabling, the device can read content from CPU card.

Enable ID Card

启用身份⍰后，⍰⍰可⍰⍰身份⍰，用⍰可在⍰⍰上刷身份⍰。

7.5.9 Video Intercom Settings

Set Device No. via Mobile Web

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

Tap ☰ → **Intercom** → **Device ID Settings**.

Tap **Save**.

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

Device Type

The device can used as door station. You can select other device type from the drop-down list.

Community No.

Enter the device community No. (period No.)

Building No.

Enter the device building No.

No.

Customize device No.

Note

- If the device type is **Door Station** or **Access Control Device**, the No. should be between 0 and 99.
- After changing the device type or No., you should reboot the device to take effect.

Unit No.

Enter the device unit No.

Floor No.

Enter the device floor No.

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

Device Type

The device can used as out door station. You can select other device type from the drop-down list.

Community No.

Enter the device community No. (period No.)

No.

Customize device No.

Note

- If the device type is **Outer Door Station**, the No. should be between 1 and 99.
- After changing the device type or No., you should reboot the device to take effect.

Note

After changing the device type or No., you should reboot the device to take effect.

Session Settings

You can set the registration password, main station IP and private server IP, and you can enable protocol 1.0 according to your actual needs.

Tap ≡ → **Intercom** → **Session Settings**.

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.

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

Tap **Save**.

Call Settings

you can set Max. communication duration between the main station and other devices.

Tap ≡ → **Intercom** → **Call Settings**.

Max. Communication Time

The Maximum communication time when the main station and the other devices are in the call. When the communication time exceeds the configured time, the communication will stop. The Max. communication time range is 90 s to 120 s.

Number Settings

Set SIP number for the room. The rooms can communicate with each other via SIP number.

Steps

1. Tap ≡ → **Intercom → Number Settings**.
2. Enter **Room No.** and **SIP Number1**.
3. Tap **Save**.
4. **Optional:** Tap the configured room No., edit or tap **+Add** to add another SIP number.
5. **Optional:** Tap **Delete** to delete room number.

Press Button to Call via Mobile Web

You can press the button to call.

Steps

1. Tap ≡ → **Intercom → Press Button to Call**.
2. Tap **1** to enter the page.

   Note

   - When you check Call Specified Indoor Station, you should set the linked room's No.
   - By default, you can press the button to call indoor station, and hold the button to call center.

3. Select the item that the button linked to. When select **Call Specified Indoor Station**, you should set the room's No.
4. Tap **Save**.

7.5.10 Set Face Parameters

Set face recognition parameters.

Tap ≡ → **Smart → Access Control Parameters**.

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

Face Anti-spoofing

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

Face 1:1 Security Level

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

Face 1:N Security Level

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

Face Recognition Timeout Value

Configure the timeout period for face recognition. If the face recognition time exceeds the configured value, the device will prompt the face recognition timeout.

Tap **Save**.

7.5.11 Enable/Disable Masl Detection via Device

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

Tap ≡ **→ Smart → Face Mask Detection Parameters**.

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 1:N Matching Threshold**, **Face with Mask&Face (1:1 ECO)**, **Face with Mask 1:N Matching Threshold (ECO Mode)**, and **Face without Mask Strategy**.

Tap **Save**.

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 1:N Matching Threshold

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.

Face with Mask 1:1 Match Threshold (ECO)

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, 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)

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

Face without Mask 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 Face Mask

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

Must Wear Face Mask

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

7.5.12 Set Privacy Parameters

Set the display parameters, picture upload and storage parameters.

Tap ≡ → **Security** → **Privacy Settings**.

Authentication Settings

Picture Display/Name Display/Employee ID Display

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

Name/ID De-identification

You can choose to desensitize the name and Employee ID when authenticating. After de-identification, the name and the ID will display parts of contents.

Picture Uploading and Storage

Set picture uploading and storage parameters.

Save Registered Picture

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

Save Picture When Auth.

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

Upload Captured Picture When Authenticating

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

Save Pictures After Linked Capture

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

Upload Picture After Linked Capture

Upload the pictures captured after linked capture.

7.5.13 Set PIN Mode

Make sure the PIN is platform-applied personal PIN or device-set personal PIN before settings. If it is a device-set personal PIN, it can be created or edited on the device or on the web, and cannot be set on other platforms; If it is a platform-applied personal PIN, it can be created or edited on the platform, and issued to the device before it can be used. It cannot be set on the device or on the web.

Tap ≡ → **Security** → **PIN Mode**.

Platform-Applied Personal PIN

You can create the person PIN on the platform. You should apply the PIN to the device. You cannot create or edit the PIN on the device or PC Web.

Device-Set Personal PIN

You can create or edit the PIN on the device or PC Web. You cannot set the PIN on the platform.

Tap **Save**.

7.5.14 System Upgrade & Maintenance

Restart device, restore device and upgrade device.

Restart Device

Tap ≡ .
Tap **Restart** to restart the device.

Restore Parameters

Tap ≡ → **Default** to enter the settings page.

Restore to Default Settings

All data will be cleared except the network parameters and user account.

Restore to Factory Settings

All functions and parameters will be restored to factory settings. You should activate the device again to use.

Upgrade Device

On home page, tap ≡ → **Upgrade**.
Click **Upgrade** to upgrade the device.

Note

The upgrading process will take 1 to 10 minutes. Do not power off. The device will restart automatically after upgrading.

7.5.15 View User Document

View the user document.

Note

Only when you enter the mobile web by IP address, can you view the user document. Login by hot spot does not support the function.

Tap ≡ to enter the page.

Tap **View Online Document** to view the user manual.

7.5.16 Open Source Software Licenses

You can view the open source software licenses.

Tap ≡ to enter the page.

Tap **Open Source Software Licenses**.

7.5.17 Log Out of Mobile Web

Log out of the configuration page on the mobile web.

On the home page, tap ≡ → **Log Out** , and tap **OK** to log out of the web.

If you need to go to the configuration page, please enter user name and password again.

Chapter 8 Operation via Web Browser

8.1 Login

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

Note

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

Note

5 failed password enterings will lock the device. You should try again after 30 min.

8.2 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.

8.3 Help

8.3.1 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.

8.3.2 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.

8.4 Logout

Log out the account.

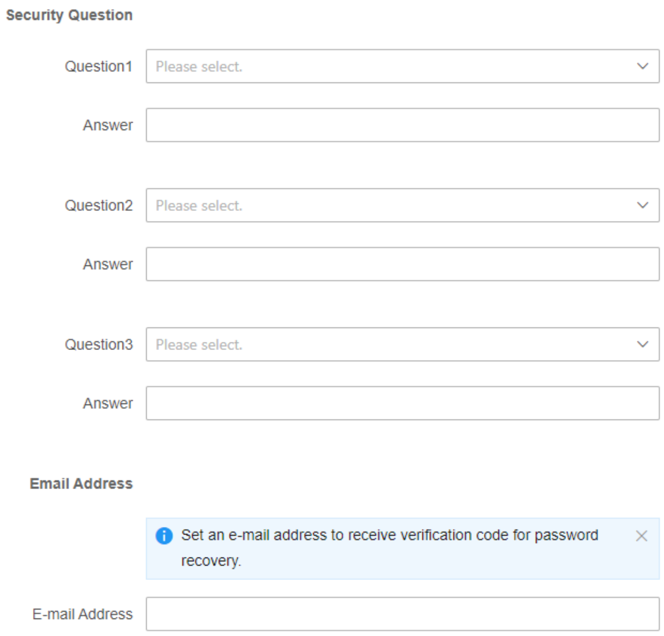
Click **admin** → **Logout** → **OK** to logout.

8.5 Quick Operation via Web Browser

8.5.1 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.



Security Question

Question1: Please select.

Answer:

Question2: Please select.

Answer:

Question3: Please select.

Answer:

Email Address

Set an e-mail address to receive verification code for password recovery.

E-mail Address:

Figure 8-1 Change Password

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

8.5.2 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.

8.5.3 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

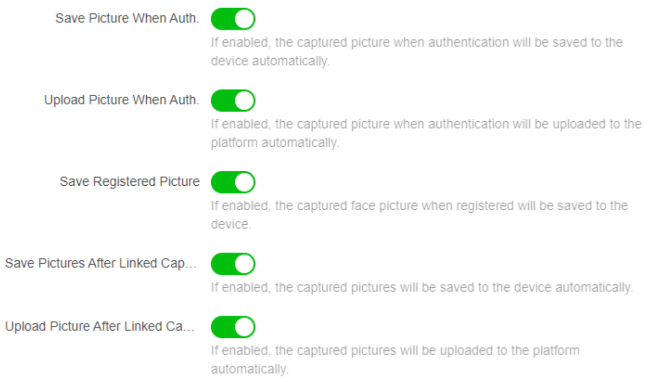
You can view the DST start time, end time and bias time.

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

8.5.4 Privacy Settings

Set the picture uploading and storage parameters.

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



Save Picture When Auth. ●

If enabled, the captured picture when authentication will be saved to the device automatically.

Upload Picture When Auth. ●

If enabled, the captured picture when authentication will be uploaded to the platform automatically.

Save Registered Picture ●

If enabled, the captured face picture when registered will be saved to the device.

Save Pictures After Linked Cap... ●

If enabled, the captured pictures will be saved to the device automatically.

Upload Picture After Linked Ca... ●

If enabled, the captured pictures will be uploaded to the platform automatically.

Figure 8-2 Privacy Settings

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.

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

8.5.5 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.

Click **Complete** to complete the settings.

8.5.6 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.

8.6 Person Management

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.
If you select **Visitor** as the person type, you can set the visit times.
If you select **Person in Blocklist**, when the person starts authenticate, the system will report an event.
If you select **Custom Type**, you can edit the name. The changed name will be applied to the device.
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.

Add Face Picture

Click **Person Management → Add** to enter the Add Person page.
Click **Add from Device** and you can take a face picture via the device.
Or 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 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 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 PIN

Before configuring PIN, it is necessary to clarify whether the PIN is a device-set personal PIN or a platform-applied personal PIN. If it is a device-set personal PIN, it can be created or edited on the device or on the web, and cannot be set on other platforms; If it is a platform-applied personal PIN, it can be created or edited on the platform, and issued to the device before it can be used. It cannot be set on the device or on the web.
Make sure you have already set the PIN mode as **Device-Set Personal PIN** in . Click **PIN Mode** on the page to go to configure.
Click **Person Management → Add** to enter the Add Person page.
Set the PIN. Or click **Auto Generate** to generate a PIN automatically.
Click **Add** to save the settings.
Click **Save and Configure** to save the settings and continue to add next person.

Authentication Settings

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

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.

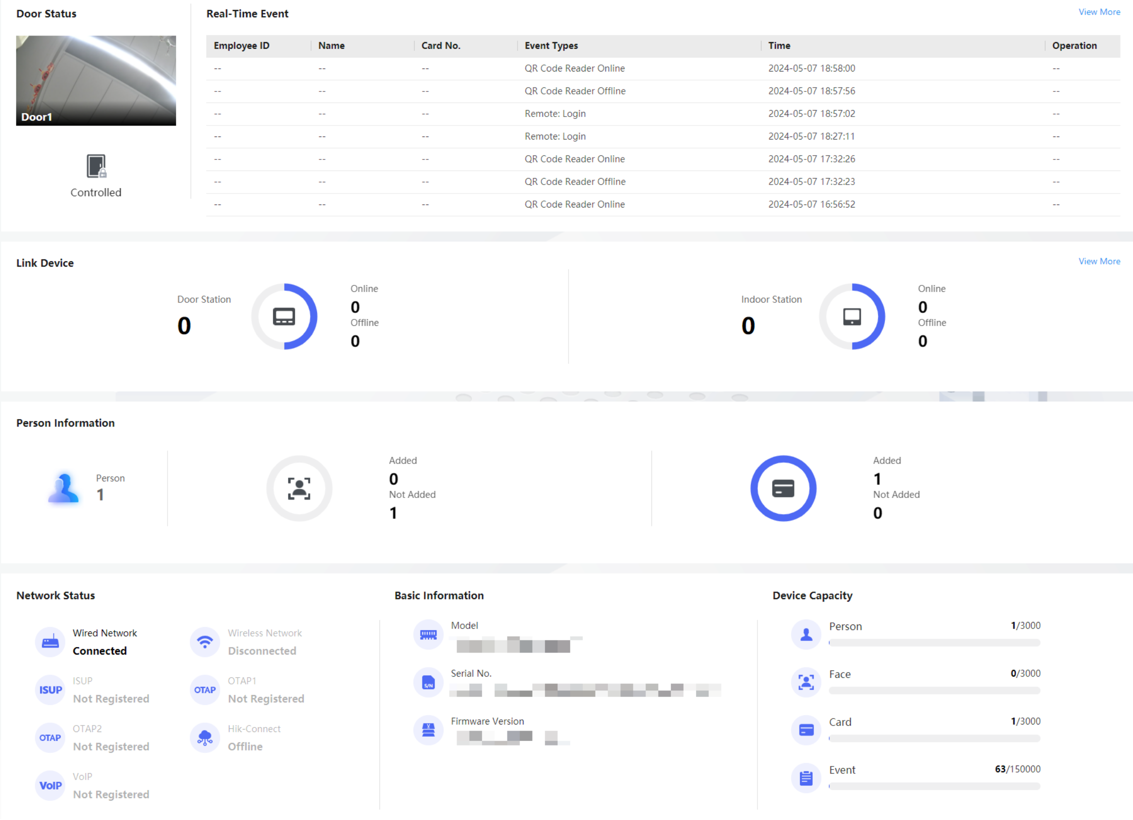
Filter

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.

8.7 Access Control Management

8.7.1 Overview

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



Door Status

Door1

Controlled

Real-Time Event

View More

Employee ID	Name	Card No.	Event Types	Time	Operation
--	--	--	QR Code Reader Online	2024-05-07 18:58:00	--
--	--	--	QR Code Reader Offline	2024-05-07 18:57:56	--
--	--	--	Remote: Login	2024-05-07 18:57:02	--
--	--	--	Remote: Login	2024-05-07 18:27:11	--
--	--	--	QR Code Reader Online	2024-05-07 17:32:26	--
--	--	--	QR Code Reader Offline	2024-05-07 17:32:23	--
--	--	--	QR Code Reader Online	2024-05-07 16:56:52	--

Link Device

View More

Door Station 0 — Online 0, Offline 0

Indoor Station 0 — Online 0, Offline 0

Person Information

Person 1

Added 0, Not Added 1

Added 1, Not Added 0

Network Status

Wired Network: Connected

Wireless Network: Disconnected

ISUP: Not Registered

OTAP1: Not Registered

OTAP2: Not Registered

Hik-Connect: Offline

VoIP: Not Registered

Basic Information

Model: [redacted]

Serial No.: [redacted]

Firmware Version: [redacted]

Device Capacity

Person	1/3000
Face	0/3000
Card	1/3000
Event	63/150000

Figure 8-3 Live View Page

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

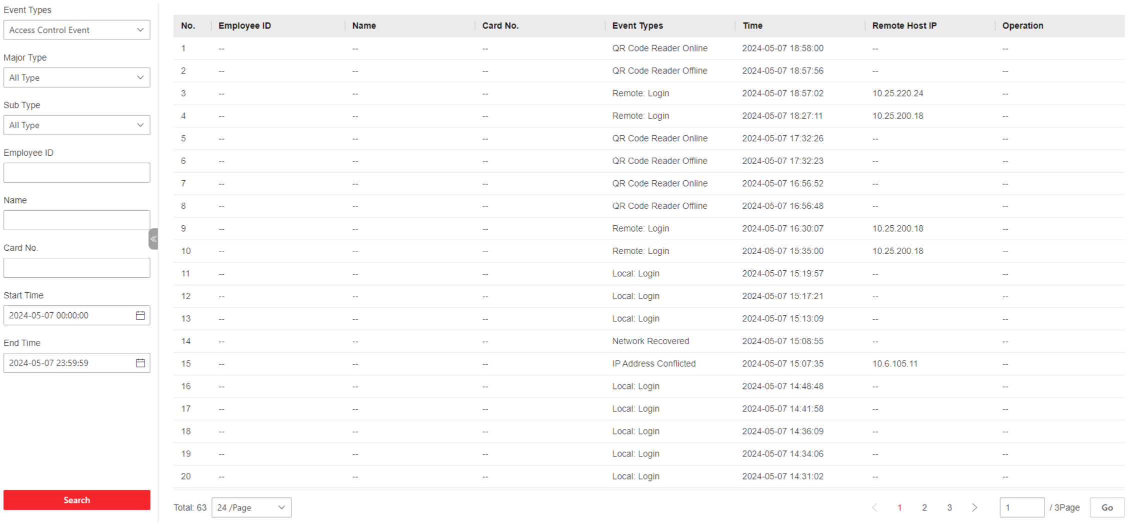
You can view the person, face, fingerprint, card, and event capacity.

Note

Only device installed fingerprint module can display the fingerprint capacity.

8.7.2 Search Event

Click **Access Control → Event Search** to enter the page.



Event Types: Access Control Event

Major Type: All Type

Sub Type: All Type

Employee ID:

Name:

Card No.:

Start Time: 2024-05-07 00:00:00

End Time: 2024-05-07 23:59:59

No.	Employee ID	Name	Card No.	Event Types	Time	Remote Host IP	Operation
1	--	--	--	QR Code Reader Online	2024-05-07 18:58:00	--	--
2	--	--	--	QR Code Reader Offline	2024-05-07 18:57:56	--	--
3	--	--	--	Remote: Login	2024-05-07 18:57:02	10.25.220.24	--
4	--	--	--	Remote: Login	2024-05-07 18:27:11	10.25.200.18	--
5	--	--	--	QR Code Reader Online	2024-05-07 17:32:26	--	--
6	--	--	--	QR Code Reader Offline	2024-05-07 17:32:23	--	--
7	--	--	--	QR Code Reader Online	2024-05-07 16:56:52	--	--
8	--	--	--	QR Code Reader Offline	2024-05-07 16:56:48	--	--
9	--	--	--	Remote: Login	2024-05-07 16:30:07	10.25.200.18	--
10	--	--	--	Remote: Login	2024-05-07 15:35:00	10.25.200.18	--
11	--	--	--	Local: Login	2024-05-07 15:19:57	--	--
12	--	--	--	Local: Login	2024-05-07 15:17:21	--	--
13	--	--	--	Local: Login	2024-05-07 15:13:09	--	--
14	--	--	--	Network Recovered	2024-05-07 15:08:55	--	--
15	--	--	--	IP Address Conflicted	2024-05-07 15:07:35	10.6.105.11	--
16	--	--	--	Local: Login	2024-05-07 14:48:48	--	--
17	--	--	--	Local: Login	2024-05-07 14:41:58	--	--
18	--	--	--	Local: Login	2024-05-07 14:36:09	--	--
19	--	--	--	Local: Login	2024-05-07 14:34:06	--	--
20	--	--	--	Local: Login	2024-05-07 14:31:02	--	--

Total: 63 24 /Page

Figure 8-4 Search Event

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.

8.7.3 Door Parameter Configuration

Configure parameters for unlocking doors.

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 Lock Status via Web Page

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

Click **Access Control → Parameter Settings → Door Parameters**.

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

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.

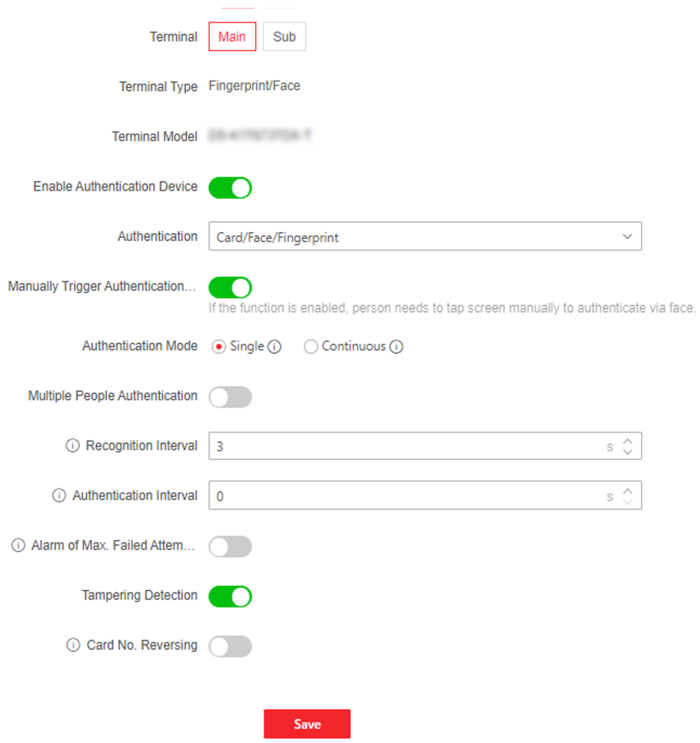
Set **Super Password**, the designated person can enter the super password to open the door.

Click **Save**.

Note

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

8.7.4 Authentication Settings



Terminal: Main | Sub

Terminal Type: Fingerprint/Face

Terminal Model: [redacted]

Enable Authentication Device: on

Authentication: Card/Face/Fingerprint

Manually Trigger Authentication...: on

If the function is enabled, person needs to tap screen manually to authenticate via face.

Authentication Mode: ● Single ⓘ ○ Continuous ⓘ

Multiple People Authentication: off

ⓘ Recognition Interval: 3 s

ⓘ Authentication Interval: 0 s

ⓘ Alarm of Max. Failed Attem...: off

Tampering Detection: on

ⓘ Card No. Reversing: off

Figure 8-5 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 Authentication Mode via PC Web

Set authentication credential for device authentication .

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

If select the terminal as Main or Sub, you can select an authentication mode from the drop-down list.

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**.

Enable/Disable Card No. Reversing via PC Web

You can enable or disable the card No. reversing function.

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

Enable **Card No. Reversing**, the read card No. will be in reverse sequence.

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**.

Enable/Disable Bluetooth via PC Web

You can enable device bluetooth to connect a bluetooth sound.

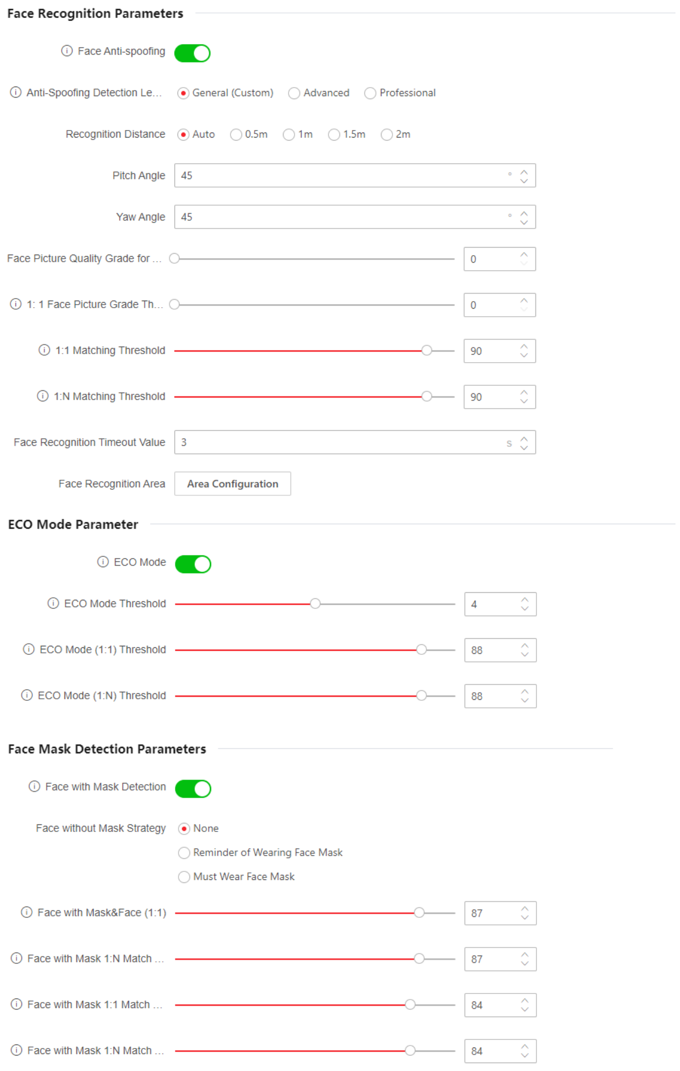
Steps

1. Click **Access Control → Parameter Settings → Authentication Settings** to enter the settings page.
2. In the bluetooth parameter configuration section, enable **Enable Bluetooth**.
3. Enter the external sound in the **Device Name**. After the bluetooth is connected, click **Save**.
4. Enable **Open Door via Bluetooth**, you can control the door remotely.

Note

You should add the device to mobile App before operation.

8.7.5 Set Face Parameters



Face Recognition Parameters

Face Anti-spoofing: On

Anti-Spoofing Detection Le...: ● General (Custom) ○ Advanced ○ Professional

Recognition Distance: ● Auto ○ 0.5m ○ 1m ○ 1.5m ○ 2m

Pitch Angle: 45 °

Yaw Angle: 45 °

Face Picture Quality Grade for ...: 0

1: 1 Face Picture Grade Th...: 0

1:1 Matching Threshold: 90

1:N Matching Threshold: 90

Face Recognition Timeout Value: 3 s

Face Recognition Area: Area Configuration

ECO Mode Parameter

ECO Mode: On

ECO Mode Threshold: 4

ECO Mode (1:1) Threshold: 88

ECO Mode (1:N) Threshold: 88

Face Mask Detection Parameters

Face with Mask Detection: On

Face without Mask Strategy: ● None ○ Reminder of Wearing Face Mask ○ Must Wear Face Mask

Face with Mask&Face (1:1): 87

Face with Mask 1:N Match ...: 87

Face with Mask 1:1 Match ...: 84

Face with Mask 1:N Match ...: 84

Figure 8-6 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 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 Timeout Value

Configure the timeout period for face recognition. If the face recognition time exceeds the configured value, the device will prompt the face recognition timeout.

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

Configure the timeout duration for face recognition.

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 border of 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**.

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) threshold and ECO mode (1:1) threshold .

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.

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**.

8.7.6 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 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

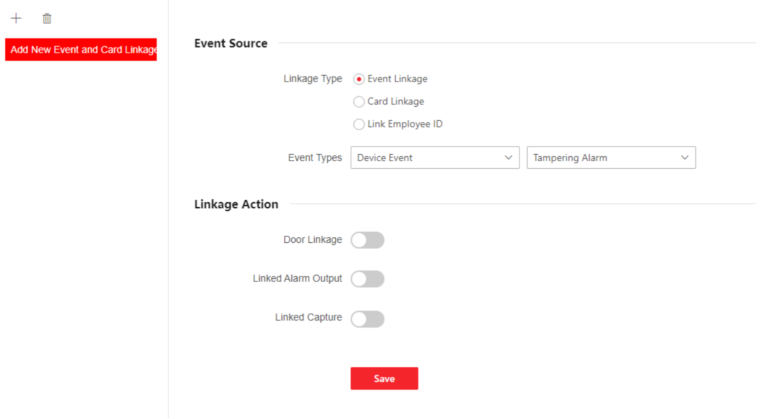
The device will read card via 4 bytes.

8.7.7 Linkage Settings

When the configured event is triggered, upload the event information to the central platform according to the configured method.

Steps

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



Linkage Type ● Event Linkage ○ Card Linkage ○ Link Employee ID

Event Types: Device Event; Tampering Alarm

Door Linkage ○

Linked Alarm Output ○

Linked Capture ○

Figure 8-7 Linkage Settings

2. Click **+** .
3. Set event source. Select the linkage type as **Event Linkage**, **Card Linkage** or **Link Employee ID**.
   - Select **Linkage Type** as **Event Linkage**, you can select event types according to your actual needs.
   - Select **Linkage Type** as **Card Linkage**, enter **Card No.** and select **Card reader**.
   - Select **Linkage Type** as **Link Employee ID**, enter **Employee ID** and select **Card reader**.
4. Set linkage action.
   1) Enable **Door Linkage**, check and select door action.
   2) Enable **Linked Alarm Output**, check and select alarm output action.
   3) Enable **Linked Capture**.
   4) Enable **Link Recording**, click **General Linkage Settings** to set pre-record time and recording delay, and enable record audio when recording video. Click **Save**.

   Note

   To use the recording function, you need to prepare the SD card. After recording, you can click **Event Search** to view recordings. For details, see ***Search Event***
5. Click**Save** to enable the settings.

8.7.8 Set Working Mode via PC Web

You can set terminal parameters for accessing.

Note

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

Go to **Access Control → Parameter Settings → Terminal Parameters**.

Click**Save** after parameters are configured.

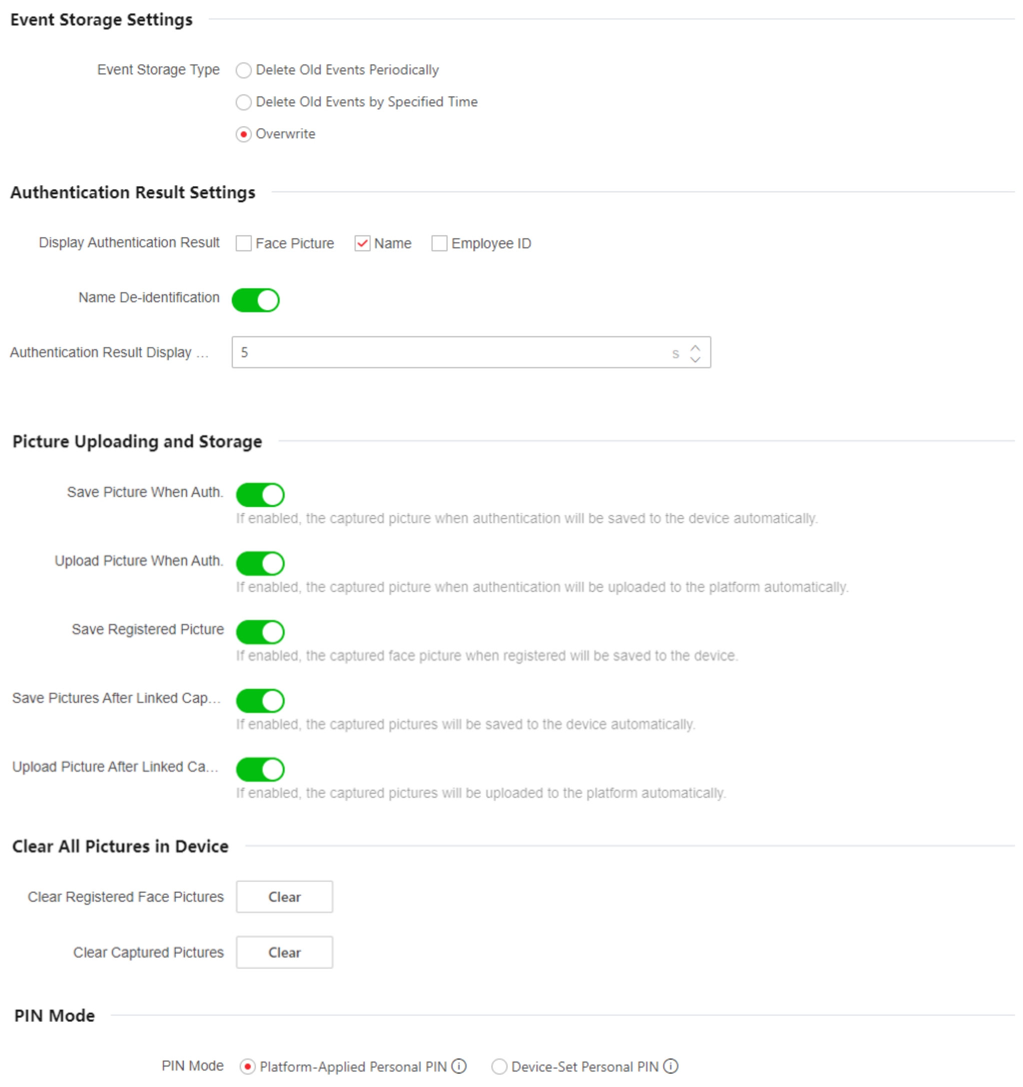
Working Mode

You can set the working mode as access control mode.

Access Control Mode

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

8.7.9 Privacy Settings



Event Storage Settings

Event Storage Type ○ Delete Old Events Periodically

○ Delete Old Events by Specified Time

● Overwrite

Authentication Result Settings

Display Authentication Result □ Face Picture ☑ Name □ Employee ID

Name De-identification

Authentication Result Display ... 5 s

Picture Uploading and Storage

Save Picture When Auth.

If enabled, the captured picture when authentication will be saved to the device automatically.

Upload Picture When Auth.

If enabled, the captured picture when authentication will be uploaded to the platform automatically.

Save Registered Picture

If enabled, the captured face picture when registered will be saved to the device.

Save Pictures After Linked Cap...

If enabled, the captured pictures will be saved to the device automatically.

Upload Picture After Linked Ca...

If enabled, the captured pictures will be uploaded to the platform automatically.

Clear All Pictures in Device

Clear Registered Face Pictures Clear

Clear Captured Pictures Clear

PIN Mode

PIN Mode ● Platform-Applied Personal PIN ⓘ ○ Device-Set Personal PIN ⓘ

Figure 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**.

Set Picture Uploading and Storage Parameters

Set picture uploading and storage parameters.

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

Enable the function as you need.

Save Picture When Auth.

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

Upload Picture When Auth.

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

Save Registered Picture

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

Save Pic. After Linked Capture

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

Upload Picture After Linked Capture

Upload the pictures captured after linked capture.

Tap **Save**.

Clear Device Pictures via PC Web

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

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

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

Set PIN Mode via PC Web

Make sure the PIN is platform-applied personal PIN or device-set personal PIN before settings. If the PIN is device-set personal PIN, you can edit the PIN on the device or PC Web, but not set it on the platform. If the PIN is platform-applied personal PIN, you should set the PIN on the platform, but not on the device or PC Web.

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

In the PIN Mode module, you can set the following parameters. Click **Save** after parameters settings.

Platform-Applied Personal PIN

You can create the person PIN on the platform. You should apply the PIN to the device. You cannot create or edit the PIN on the device or PC Web.

Device-Set Personal PIN

You can create or edit the PIN on the device or PC Web. You cannot set the PIN on the platform.

Click **Save**.

8.8 Call Settings

8.8.1 Device Management

You can view the device No., type, IP, serial No., model, version, floor No., room No., No., arming status, user name, network status and operation. You can also add indoor station and sub door station on the device management page, and manage, upgrade or delete devices.

Steps

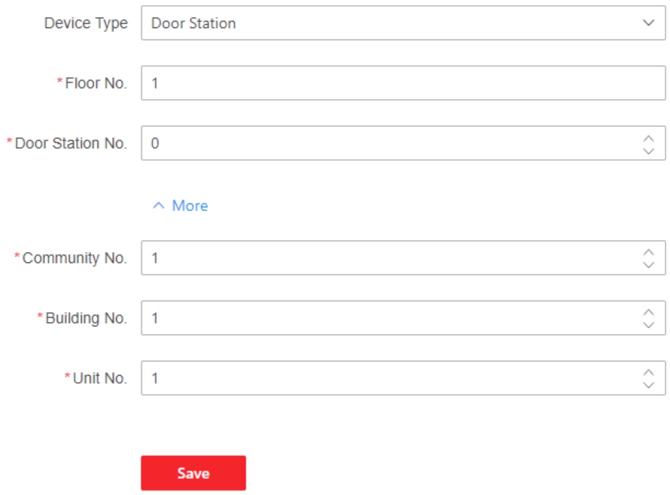
1. Click **Device Management**.
2. Click **Add**.
3. Select **Device Type**, enter **Device Password**, **Registration Password**, **Serial No.**, **IP Address**, **IPv4 Subnet Mask**, **IPv4 Default Gateway**, **Port**, **Floor No.** (not needed to enter **Floor No.**, and **No.** for indoor station.
4. Click **Save**.
5. **Optional:** You can also perform the following operations.

Delete Device	Check devices need to delete, and click **Delete**.
Import Device	Plug the USB flash drive (containing device information) to the device, click **Import** to import the device information.
Export Device	Click **Export** to export the device information files to the USB flash drive.

8.8.2 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.** .



Device Type: Door Station

*Floor No.: 1

*Door Station No.: 0

*Community No.: 1

*Building No.: 1

*Unit No.: 1

Figure 8-9 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.

8.8.3 Configure Video Intercom Network Parameters via Web Browser

You can set the registration password, main station IP and private server IP, and you can enable protocol 1.0 according to your actual needs.

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

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

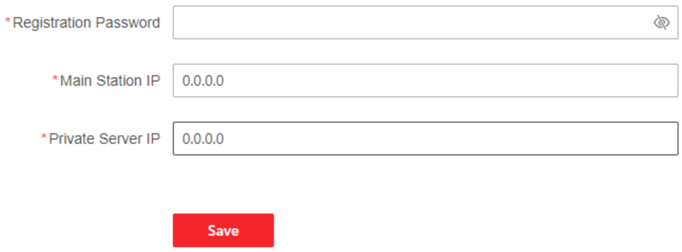
Enter the main station's IP address that used for communication.

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.



*Registration Password

*Main Station IP: 0.0.0.0

*Private Server IP: 0.0.0.0

Figure 8-10 Video Intercom Network

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

Click **Save**.

8.8.4 Set Communication Time via PC Web

Set the max. communication time.

Go to **Access Control → Call Settings → Call Settings** .

Enter the **Max. Communication Time**. Click **Save**.

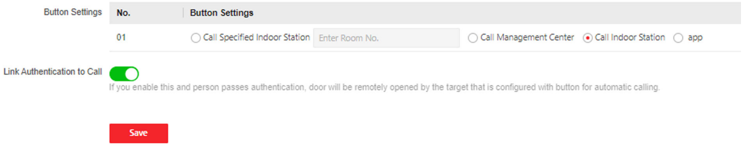
Note

The Max. Communication time range is 90 s to 120 s.

8.8.5 Press Button to Call via PC Web

Steps

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



Button Settings

No.	Button Settings
01	○ Call Specified Indoor Station (Enter Room No.) ○ Call Management Center ● Call Indoor Station ○ app

Link Authentication to Call: on

If you enable this and person passes authentication, door will be remotely opened by the target that is configured with button for automatic calling.

Figure 8-11 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.

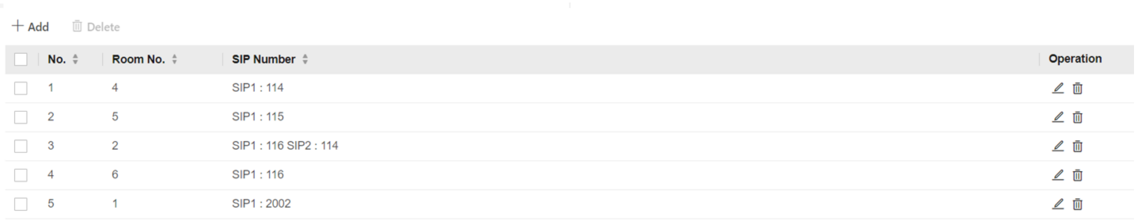
3. Enable **Link Authentication to Call** according to your needs. After enabled, when person passes authentication, the door will be remotely opened by the target that is configured with button for automatic calling.
4. Click **Save**.

8.8.6 Number Settings via PC Web

Set SIP number for the room. The rooms can communicate with each other via SIP number.

Steps

1. Go to **Access Control → Call Settings → Number Settings**.



□	No.	Room No.	SIP Number	Operation
□	1	4	SIP1 : 114	✎ 🗑
□	2	5	SIP1 : 115	✎ 🗑
□	3	2	SIP1 : 116 SIP2 : 114	✎ 🗑
□	4	6	SIP1 : 116	✎ 🗑
□	5	1	SIP1 : 2002	✎ 🗑

Figure 8-12 Number Settings

2. Click **Add**, and enter **Room No.** and **SIP1** phone number.
3. **Optional:** Click **Add** to add the SIP number or click 🗑 to delete the number.
4. Click**Save**.
5. **Optional:** You can click **Delete** to delete room number and its SIP number.

8.9 System and Maintenance

8.9.1 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.

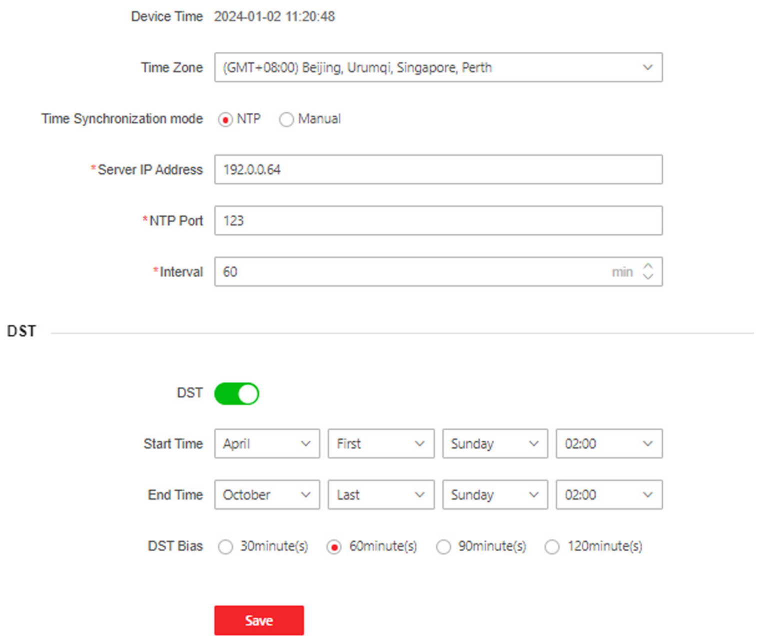
You can view the device name, device No., language, model, serial No., version, number of channels, IO input, IO output, lock, alarm input, alarm output, and device capacity, etc.

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

8.9.2 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** .



Device Time 2024-01-02 11:20:48

Time Zone (GMT+08:00) Beijing, Urumqi, Singapore, Perth

Time Synchronization mode ● NTP ○ Manual

*Server IP Address 192.0.0.64

*NTP Port 123

*Interval 60 min

DST

DST ●

Start Time April First Sunday 02:00

End Time October Last Sunday 02:00

DST Bias ○ 30minute(s) ● 60minute(s) ○ 90minute(s) ○ 120minute(s)

Figure 8-13 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.

8.9.3 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 service provider and/or end-user.

8.9.4 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.

8.9.5 View Device Arming/Disarming Information via PC Web

View device arming type and arming IP address.

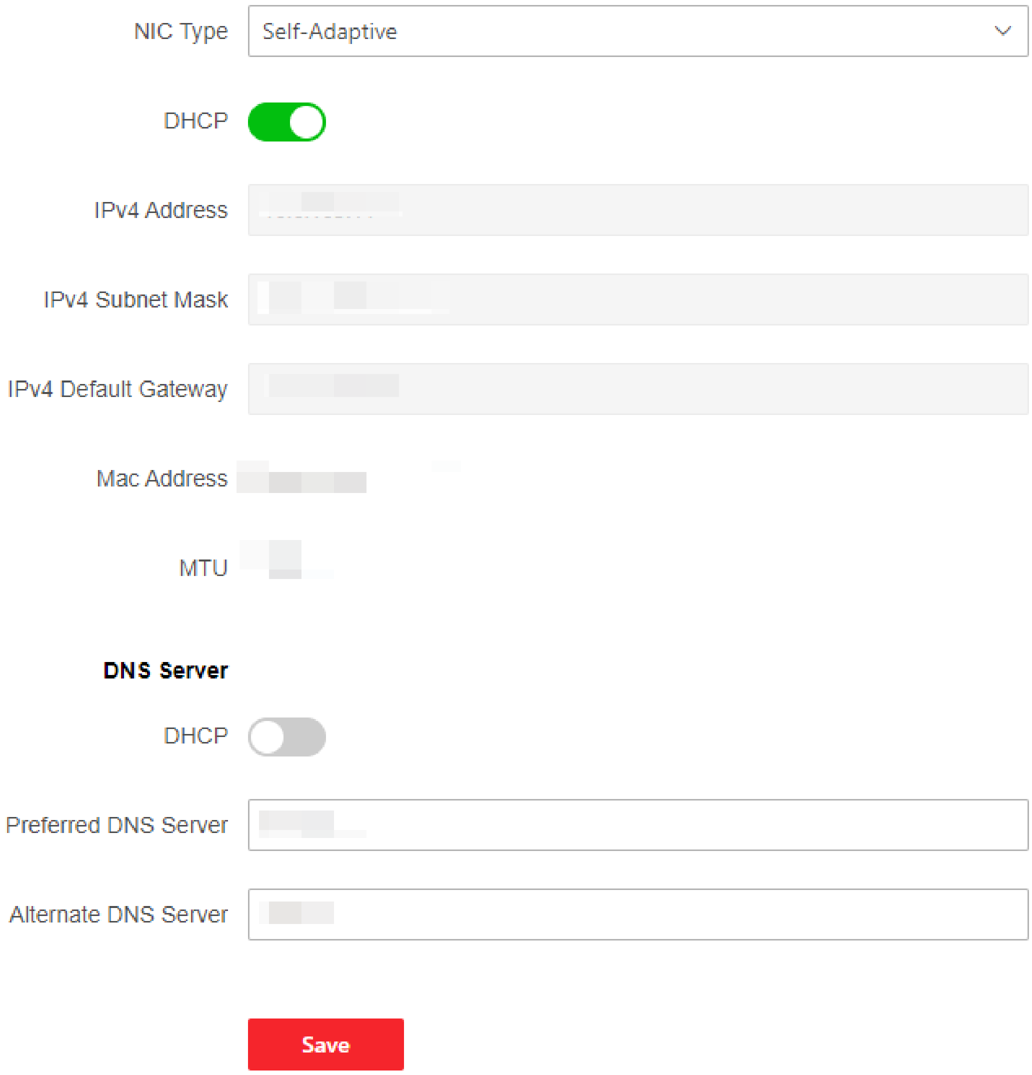
Go to **System and Maintenance → System Configuration → System → User Management → Arming/Disarming Information** .

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

8.9.6 Network Settings

Set Basic Network Parameters via PC Web

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



NIC Type: Self-Adaptive

DHCP: on

IPv4 Address: [redacted]

IPv4 Subnet Mask: [redacted]

IPv4 Default Gateway: [redacted]

Mac Address: [redacted]

MTU: [redacted]

DNS Server

DHCP: off

Preferred DNS Server: [redacted]

Alternate DNS Server: [redacted]

Figure 8-14 TCP/IP Settings Page

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

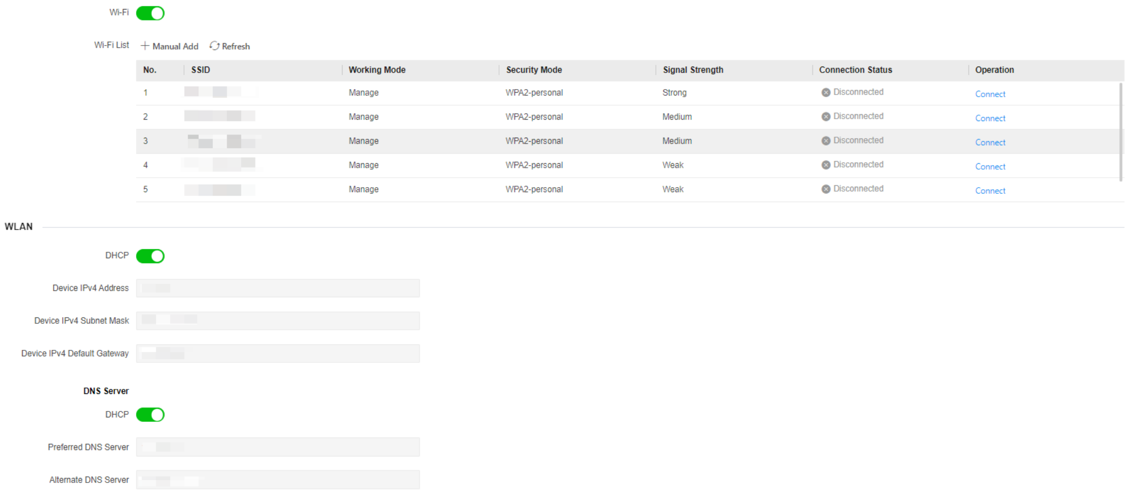
Set the Wi-Fi parameters for device wireless connection.

Steps

Note

The function should be supported by the device.

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



Wi-Fi ●

Wi-Fi List + Manual Add ⟳ Refresh

No.	SSID	Working Mode	Security Mode	Signal Strength	Connection Status	Operation
1	[redacted]	Manage	WPA2-personal	Strong	⊗ Disconnected	Connect
2	[redacted]	Manage	WPA2-personal	Medium	⊗ Disconnected	Connect
3	[redacted]	Manage	WPA2-personal	Medium	⊗ Disconnected	Connect
4	[redacted]	Manage	WPA2-personal	Weak	⊗ Disconnected	Connect
5	[redacted]	Manage	WPA2-personal	Weak	⊗ Disconnected	Connect

WLAN

DHCP ●

Device IPv4 Address [redacted]

Device IPv4 Subnet Mask [redacted]

Device IPv4 Default Gateway [redacted]

DNS Server

DHCP ●

Preferred DNS Server [redacted]

Alternate DNS Server [redacted]

Figure 8-15 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 Device Hotspot

After enabling the device hotspot, you can use the mobile phone to connect the hotspot and set.

Go to **System and Maintenance → System Configuration → Network → Network Settings → Device Hotspot**.

Slide **Enable Device Hotspot** and you can use the mobile phone to connect the hotspot and set. Click **Save**.

Note

Hotspot and Wi-Fi cannot be enabled at the same time.

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.

Set WebSocket(s) via PC Web

View WebSocket and WebSockets port.

Go to **System and Maintenance → System Configuration → Network → Network Service → WebSocket(s)** .
View WebSocket and WebSockets port.

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

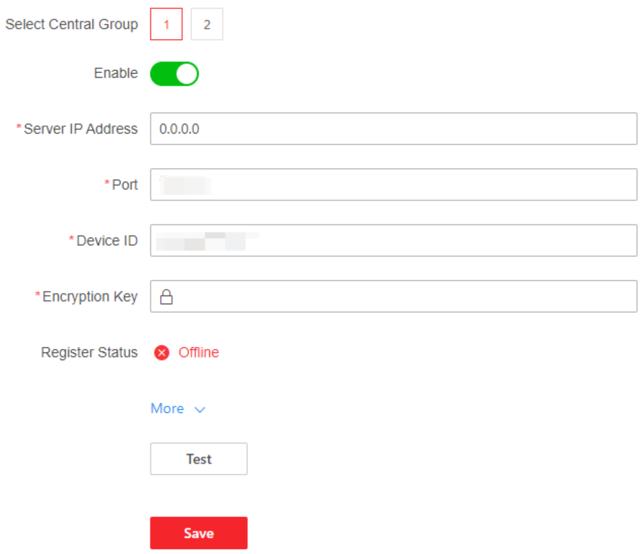
   If you select 5.0 as the version, you should set the encryption key as well.
4. Set the ISUP listening parameters, including ISUP alarm center IP address/domain name, ISUP alarm center URL, and ISUP alarm center port.
5. Click **Save**.

Set OTAP via PC Web

Connect the device to the platform through the OTAP protocol to obtain device information, upload operation status and alarm information, restart and upgrade the device.

Steps

1. Click **System and Maintenance → System Configuration → Network → Device Access → OTAP** .



Select Central Group 1 2

Enable

*Server IP Address 0.0.0.0

*Port [redacted]

*Device ID [redacted]

*Encryption Key

Register Status Offline

Figure 8-16 Set OTAP

2. Click to **Enable** OTAP.
3. Set **Server IP Address**, **Port**, **Device ID** and **Encryption Key**.
4. Click **Test** to ensure the device can connect to the server and register successfully. Refresh the page or restart the device to see the **Register Status**.
5. Click **More** to view the network type and access priority. Drag the operation icon upward or downward to adjust the network priority.
6. 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.

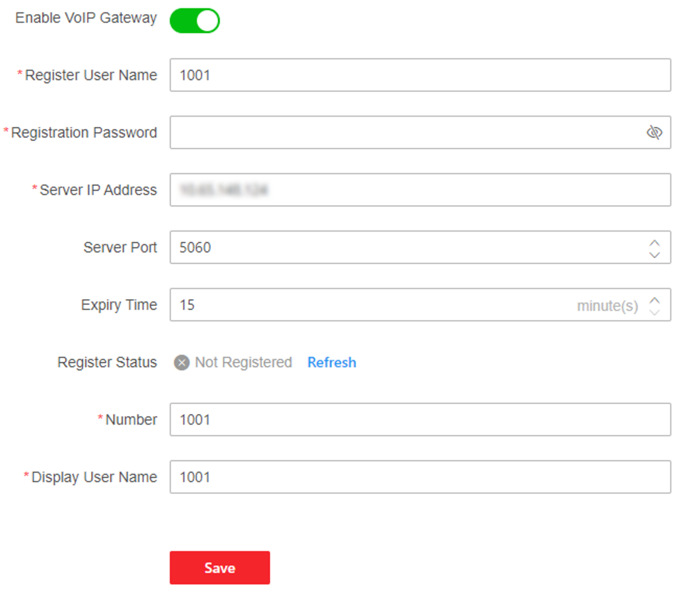
6. Click **Save** to enable the settings.

VoIP Account Settings

You can realize voice call by network.

Steps

1. Go to **System and Maintenance → System Configuration → Network → Device Access → VoIP**.
2. Enable **VoIP Gateway**.
3. Set **Register User Name**、 **Registration Password**、 **Server IP Address**、 **Server Port**、 **Expiry Time**、 **Register Status**、 **Number**、 **Display User Name.**



Enable VoIP Gateway	●
*Register User Name	1001
*Registration Password	
*Server IP Address	[redacted]
Server Port	5060
Expiry Time	15 minute(s)
Register Status	Not Registered Refresh
*Number	1001
*Display User Name	1001

Figure 8-17 VoIP Account Settings

Registration Password

Enter the registration password for communication via SIP server. The registration password for the SIP server is configured usually in the main station's SIP settings.

Server IP Address

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

Number / Display User Name

The device displayed call number and user name.

4. Click **Save**.

8.9.7 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.

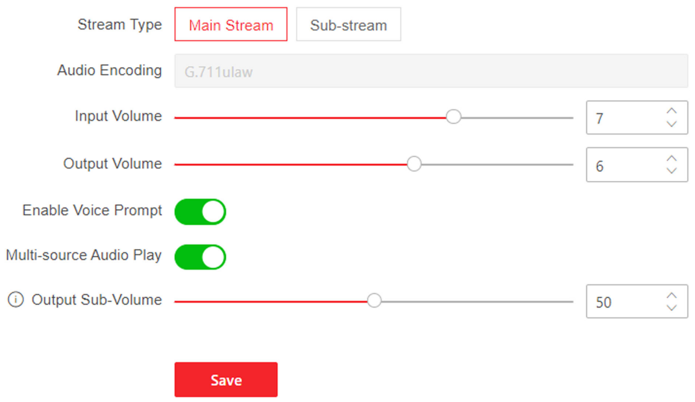
Set camera name, stream type, video type, resolution, bit rate type, video quality, frame rate, Max. bitrate, video encoding and I frame interval.

Click **Save**.

Configure Audio Parameters via PC Web

You can set device volume.

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



Stream Type: Main Stream | Sub-stream

Audio Encoding: G.711ulaw

Input Volume: 7

Output Volume: 6

Enable Voice Prompt

Multi-source Audio Play

Output Sub-Volume: 50

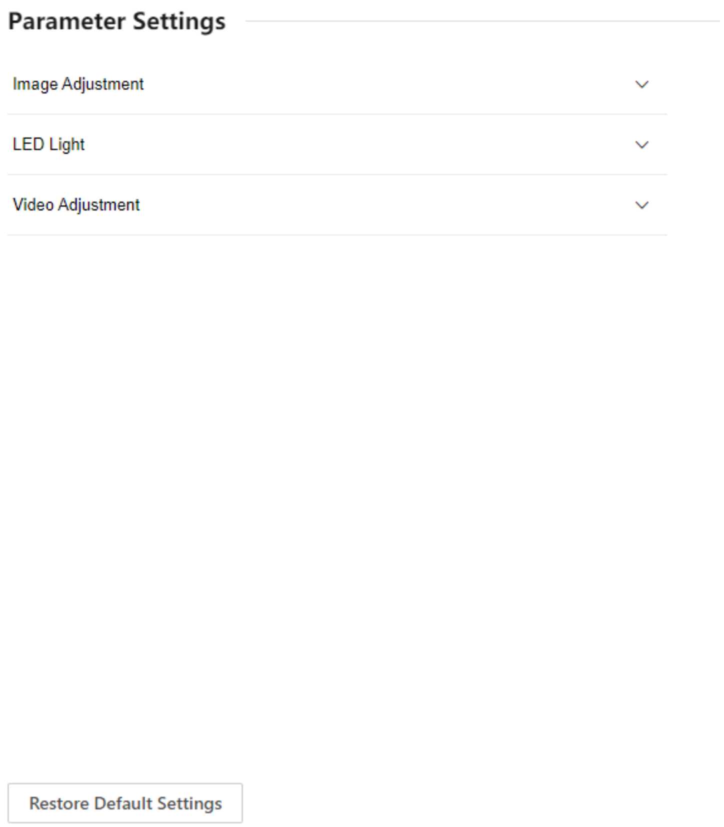
Figure 8-18 Audio

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**.

8.9.8 Image Parameter Settings



Parameter Settings

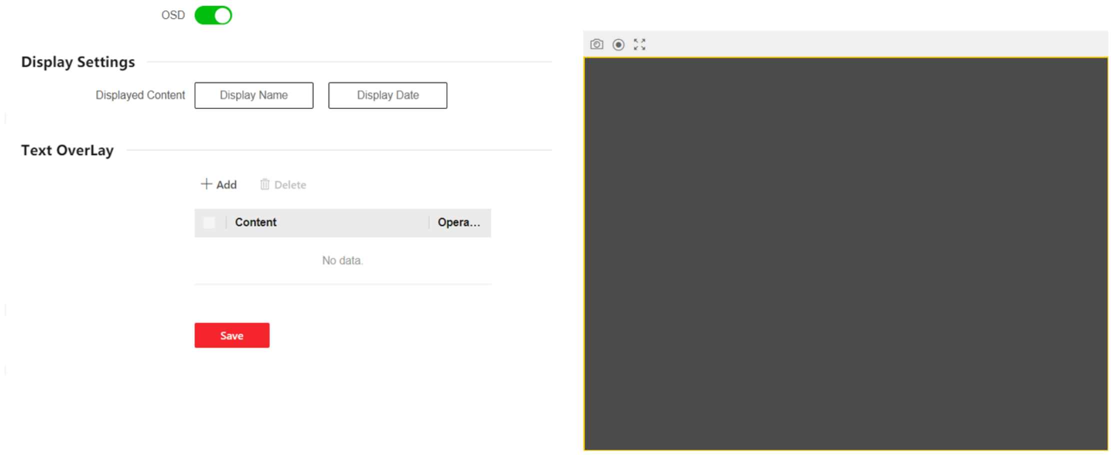
Image Adjustment

LED Light

Video Adjustment

Restore Default Settings

Figure 8-19 Display Settings



OSD

Display Settings

Displayed Content: Display Name, Display Date

Text OverLay

+ Add | Delete

	Content	Opera...

No data

Save

Figure 8-20 OSD 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 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.

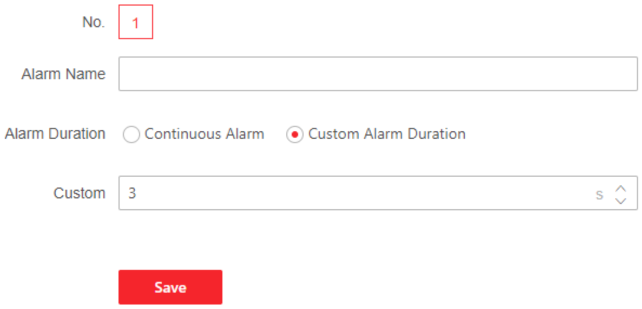
Click **Restore Default Settings** to restore the to the default.

8.9.9 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**.



No. 1

Alarm Name

Alarm Duration ○ Continuous Alarm ● Custom Alarm Duration

Custom 3 s

Figure 8-21 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.

8.9.10 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

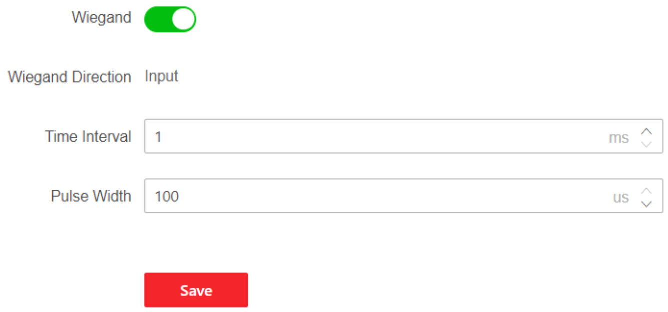
You can set the Wiegand transmission direction.

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** .



Wiegand: On

Wiegand Direction: Input

Time Interval: 1 ms

Pulse Width: 100 us

Figure 8-22 Wiegand Page

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

   Input

   The device can connect a Wiegand card reader.
4. Set the time interval and pulse width if you need.
5. Click **Save** to save the settings.

Note

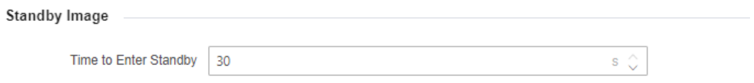
If you change the peripheral, and after you save the device parameters, the device will reboot automatically.

8.10 Preference Settings

8.10.1 Set Standby Image via PC Web

Set the standby image parameters, including the time to enter standby, and sleep time.

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



Standby Image

Time to Enter Standby: 30 s

Figure 8-23 Standby Time Settings

Click **Save** after parameters are configured.

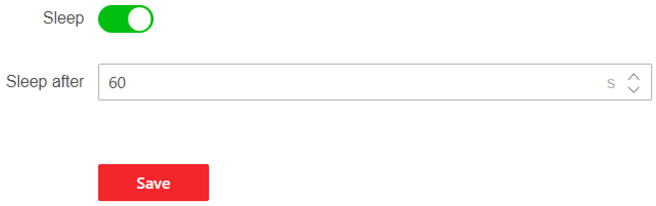
Time to Enter Standby

The device will show the standby image after the configured time duration.

8.10.2 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** .



Sleep: ●

Sleep after: 60 s

Figure 8-24 Sleep Settings

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

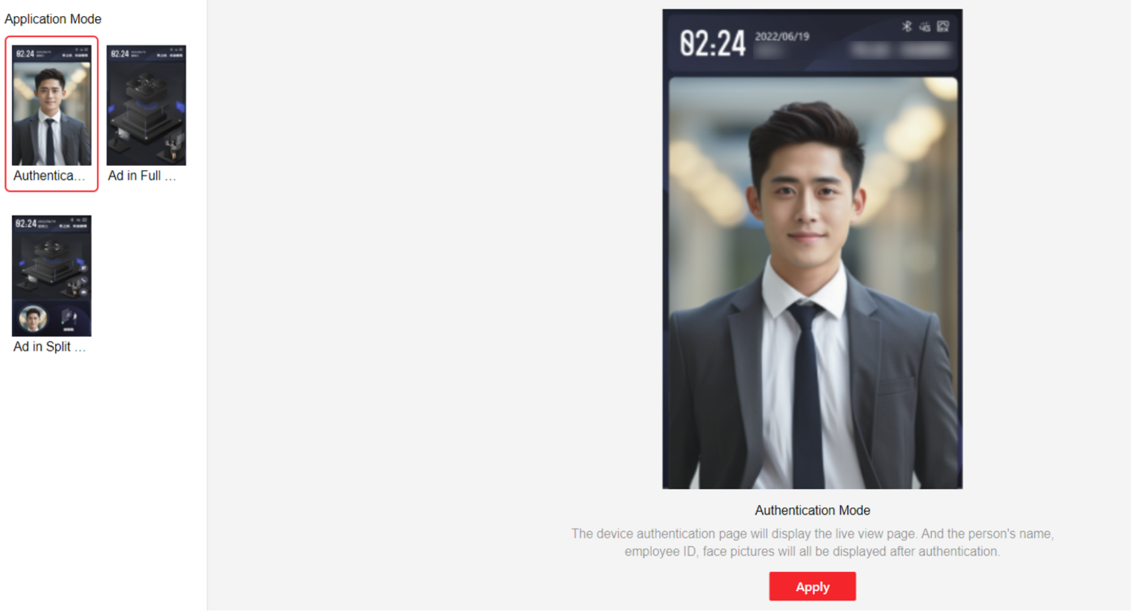
Click **Save**.

8.10.3 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**.



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.

Figure 8-25 Select Application Mode

Authentication Mode

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.

Simple Mode

After selecting this mode, the authentication page will not display the live view image. The person's name, employee ID, face pictures will all be hidden after authentication.

3. Click **Apply**.

8.10.4 Set Notice Publication via PC Web

You can set the notice publication for the device.

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

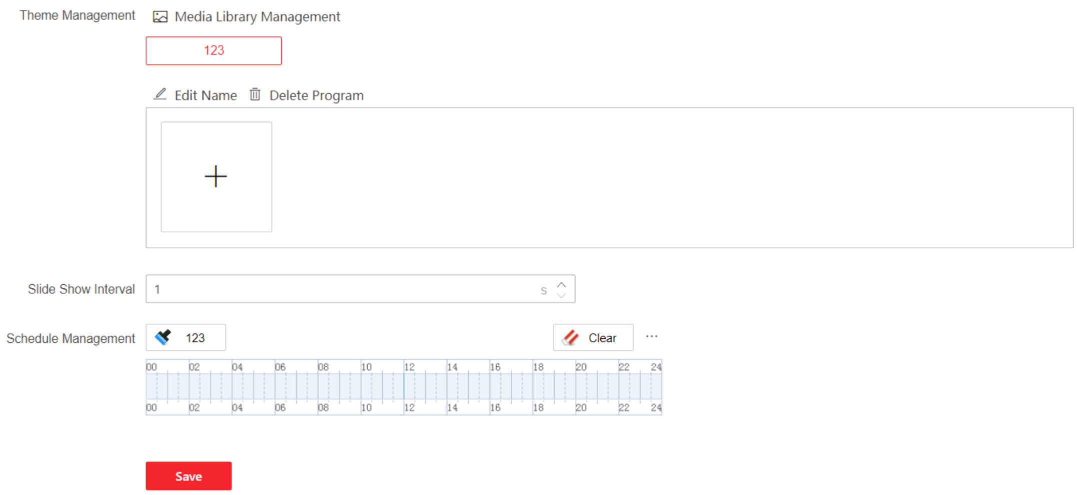


Figure 8-26 Notice Publication

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

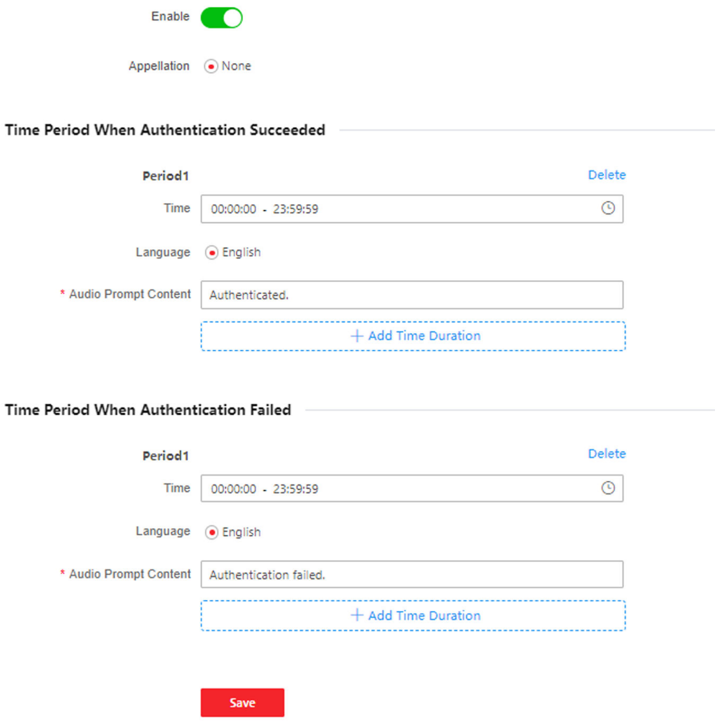
Drag the block or enter the number to set the slide show interval. The picture and video will be changed according to the interval.

8.10.5 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** .



Enable

Appellation ● None

Time Period When Authentication Succeeded

Period1 Delete

Time 00:00:00 - 23:59:59

Language ● English

* Audio Prompt Content Authenticated.

+ Add Time Duration

Time Period When Authentication Failed

Period1 Delete

Time 00:00:00 - 23:59:59

Language ● English

* Audio Prompt Content Authentication failed.

+ Add Time Duration

Save

Figure 8-27 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.

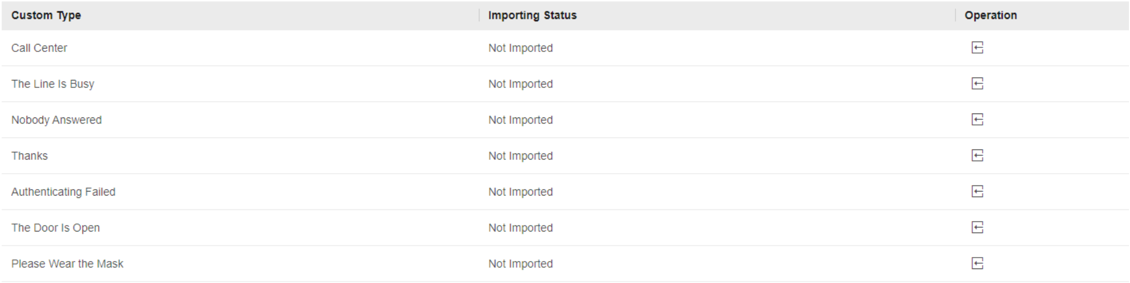
7. Click **Save** to save the settings.

8.10.6 Customize Prompt Voice via PC Web

You can customize prompt voices for the device.

Steps

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



Custom Type	Importing Status	Operation
Call Center	Not Imported	⇤
The Line Is Busy	Not Imported	⇤
Nobody Answered	Not Imported	⇤
Thanks	Not Imported	⇤
Authenticating Failed	Not Imported	⇤
The Door Is Open	Not Imported	⇤
Please Wear the Mask	Not Imported	⇤

Figure 8-28 Custom Prompt

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

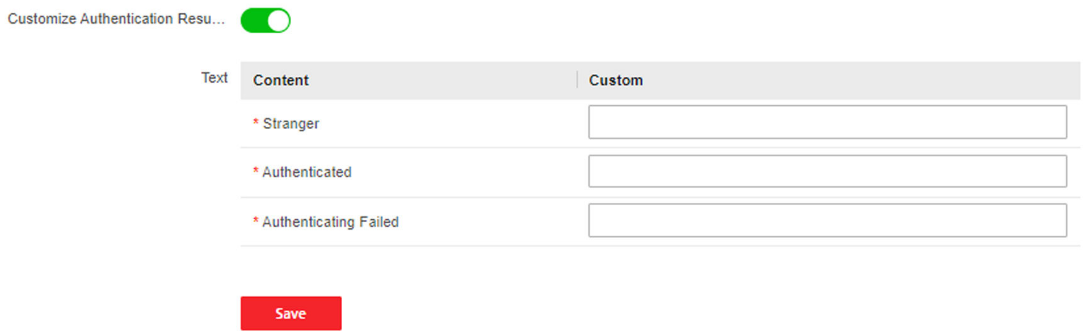
Note

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

8.10.7 Set Authentication Result Text via PC Web

Steps

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



Customize Authentication Resu...

Text

Content	Custom
* Stranger	
* Authenticated	
* Authenticating Failed	

Figure 8-29 Authentication Result Text

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

8.11 System and Maintenance

8.11.1 Reboot

You can reboot the device.

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

8.11.2 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.

8.11.3 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.

8.11.4 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.

8.11.5 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**.

8.11.6 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** .

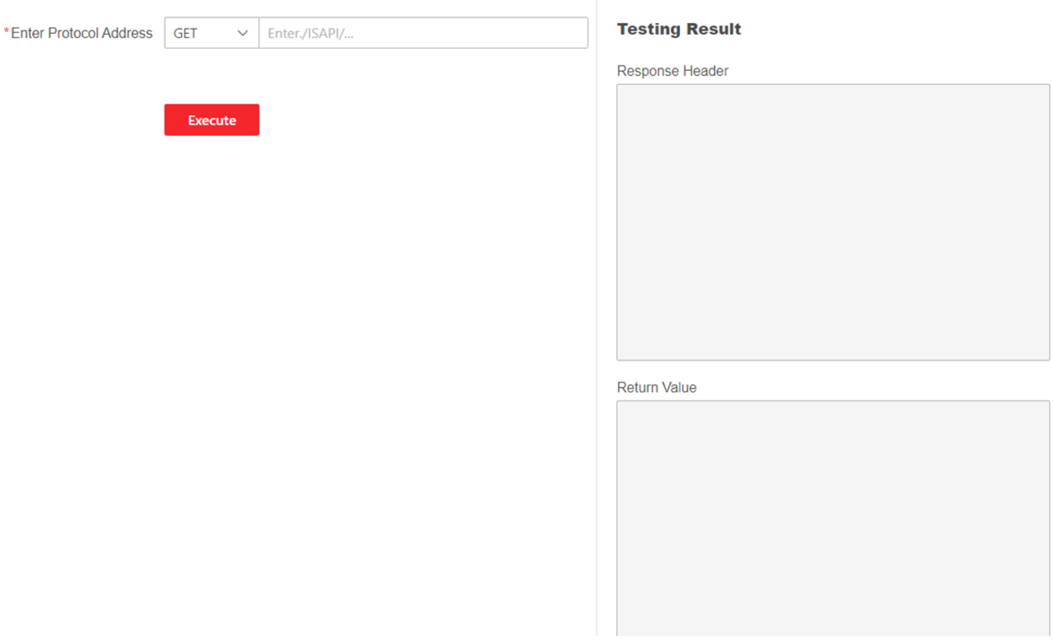


Figure 8-30 Protocol Testing

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

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

8.11.7 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.

8.11.8 Advanced Settings via PC Web

You can configure face parameters and view version information.

Go to **System and Maintenance → Maintenance → Advanced Settings** .

Enter the device activation password and click **Enter**.

Face Parameter

Enable **Custom Anti-Spoofing Detection** and you can set the **Anti-Spoofing Detection Threshold 1:1**, **Anti-Spoofing Detection Threshold 1:N**.

Enable **Lock Face for Authentication**, and set **Lock Duration**. The face will be locked for the set lock duration after the failed attempt limit of anti-spoofing detection has been reached.
Click **Save**.

Version Information

You can view the different version information here.

8.11.9 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**.

8.11.10 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**.

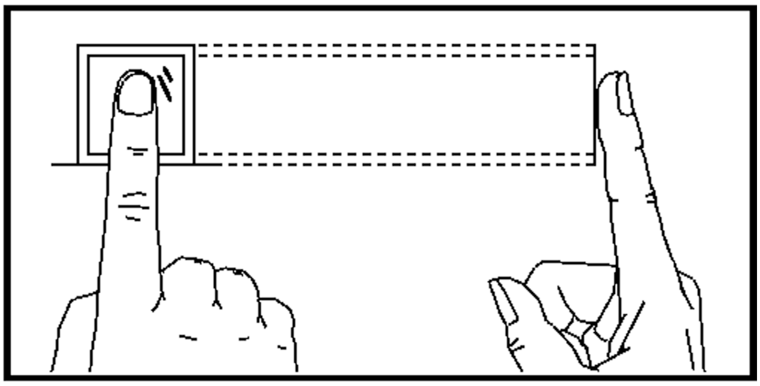
Appendix A. Tips for Scanning Fingerprint

Recommended Finger

Forefinger, middle finger or the third finger.

Correct Scanning

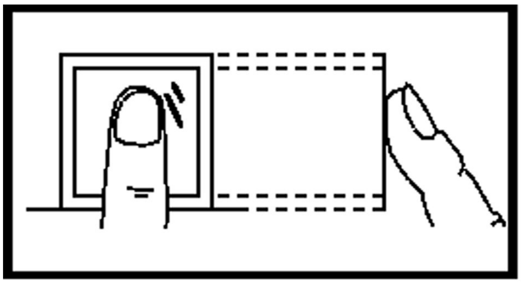
The figure displayed below is the correct way to scan your finger:



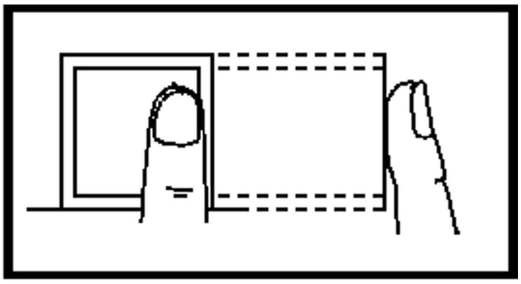
You should press your finger on the scanner horizontally. The center of your scanned finger should align with the scanner center.

Incorrect Scanning

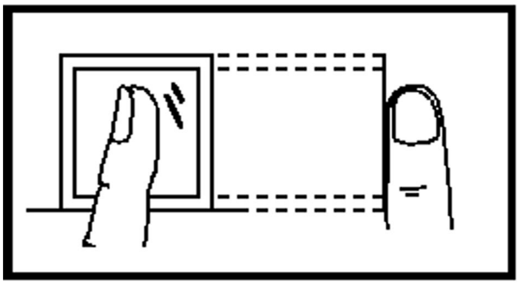
The figures of scanning fingerprint displayed below are incorrect:



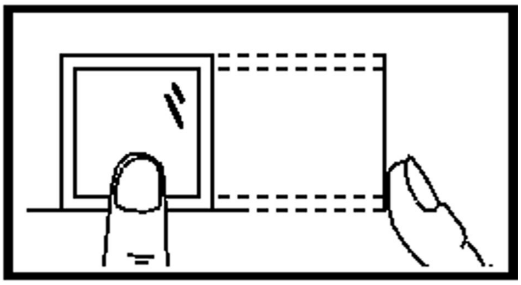
Vertical



Edge I



Side



Edge II

Environment

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

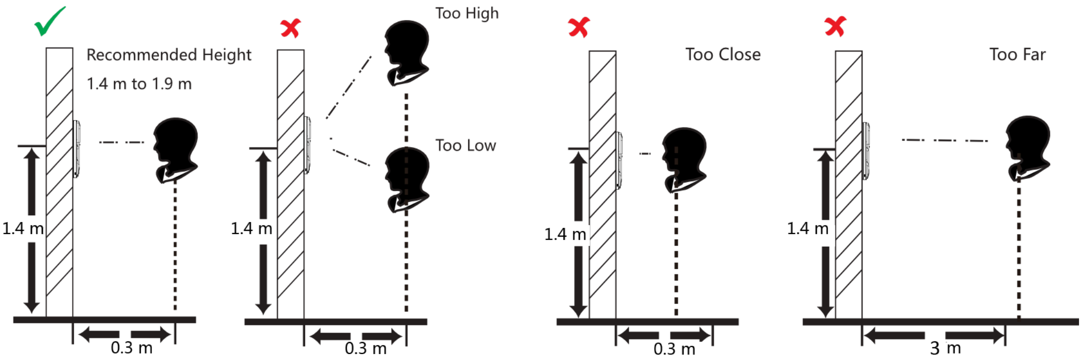
Others

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

Appendix B. Tips When Collecting/Comparing Face Picture

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

Positions (Recommended Distance: 0.5 m)



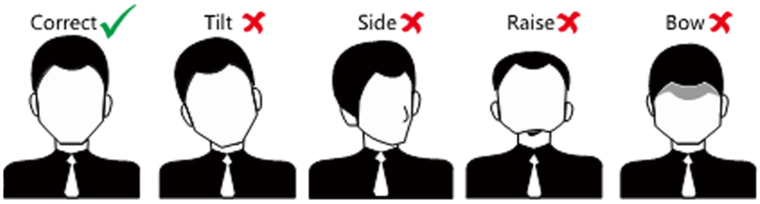
Expression

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

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

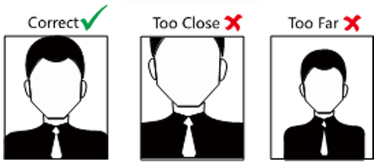
Posture

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



Size

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



Appendix C. Tips for Installation Environment

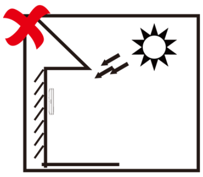
1. Light Source Illumination Reference Value

Candle: 10Lux

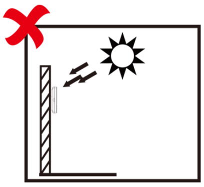
Bulb: 100~850Lux

Sunlight: More than 1200Lux

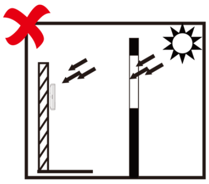
2. Avoid backlight, direct and indirect sunlight



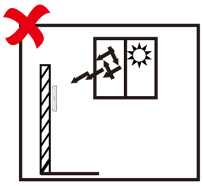
Backlight



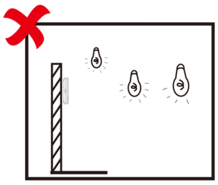
Direct Sunlight



Direct Sunlight through Window



Indirect Light through Window



Close to Light

Appendix D. Dimension

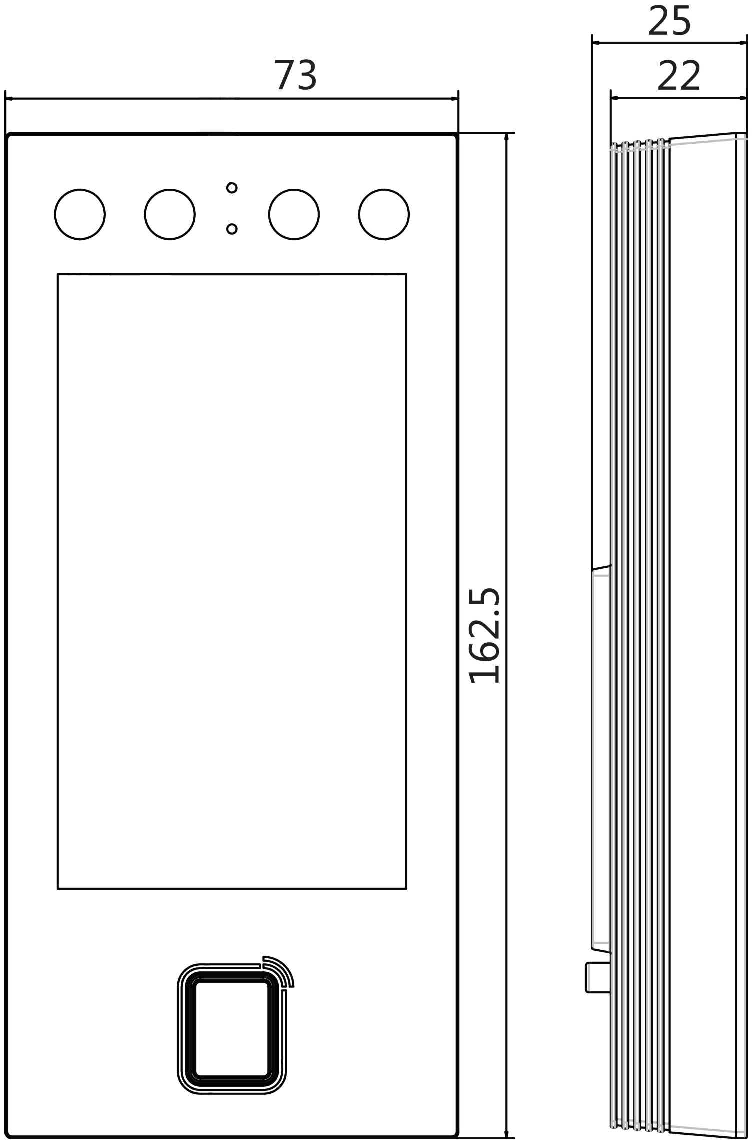


Figure D-1 Dimension (Unit: mm)

Appendix E. 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 F. 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.
ℹ **Note**	Provides additional information to emphasize or supplement important points of the main text.

See Far, Go Further