



DS-K1T681 Series Face Recognition Terminal

User Manual

Legal Information

©2023 Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

About this Manual

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

Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.

Other trademarks and logos mentioned are the properties of their respective owners.

Disclaimer

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

YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE

DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATTER PREVAILS.




Data Protection

During the use of device, personal data will be collected, stored and processed. To protect data, the development of Hikvision devices incorporates privacy by design principles. For example, for device with facial recognition features, biometrics data is stored in your device with encryption method; for fingerprint device, only fingerprint template will be saved, which is impossible to reconstruct a fingerprint image.

As data controller, you are advised to collect, store, process and transfer data in accordance with the applicable data protection laws and regulations, including without limitation, conducting security controls to safeguard personal data, such as, implementing reasonable administrative and physical security controls, conduct periodic reviews and assessments of the effectiveness of your security controls.

Symbol Conventions

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

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

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC compliance: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help

This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.

FCC Conditions

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement



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

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



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



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



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.
- CAUTION: To reduce the risk of fire, replace only with the same type and rating of fuse.
- CAUTION: This equipment is for use only with Hikvision's 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.
- 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.)

Cautions:

- + identifies the positive terminal(s) of equipment which is used with, or generates direct current.
- + identifies the negative terminal(s) of equipment which is used with, or generates direct current.
- 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 USB flash drive only.
- The serial port of the equipment is used for debugging only.

- Burned fingers when handling the fingerprint sensor metal. Wait one-half hour after switching off before handling the parts.
- 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 drop the device or subject it to physical shock, and do not expose it to high electromagnetism radiation. Avoid the equipment installation on vibrations surface or places subject to shock (ignorance can cause equipment damage).
- Do not place the device in extremely hot (refer to the specification of the device for the detailed operating temperature), cold, dusty or damp locations, and do not expose it to high electromagnetic radiation.
- 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.
- Please make sure that the biometric recognition accuracy will be affected by the collected pictures' quality and the light in the environment, which cannot be completely correct.

Available Models

Product Name	Model
Face Recognition Terminal	DS-K1T681DBX
	DS-K1T681DBWX

Use only power supplies listed in the user instructions:

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

Contents

Chapter 1 How to Customize My Manual	1
Chapter 2 Overview	4
2.1 Overview	4
2.2 Features	4
Chapter 3 Appearance	6
Chapter 4 Installation	8
4.1 Installation Environment	8
4.2 Flush Mounting with Gang Box	8
4.3 Mount With Cylinder Bracket	11
4.3.1 Preparation before Mounting with Bracket	11
4.3.2 Cylinder Bracket Mounting	13
Chapter 5 Wiring	19
5.1 Terminal Description	19
5.2 Wire Normal Device	21
5.3 Wire Secure Door Control Unit	22
5.4 Wire Fire Module	23
5.4.1 Wiring Diagram of Door Open When Powering Off	23
5.4.2 Wiring Diagram of Door Locked When Powering Off	24
Chapter 6 Activation	25
6.1 Activate via Device	25
6.2 Activate via Web Browser	27
6.3 Activate via SADP	27
6.4 Activate Device via iVMS-4200 Client Software	29
Chapter 7 Quick Operation	30
7.1 Select Language	30
7.2 Set Password Change Type	30

7.3 Set Network Parameters	32
7.4 Access to Platform	33
7.5 Set Administrator	35
7.6 Status Description and Control Center	37
Chapter 8 Basic Operation	38
8.1 Login	38
8.1.1 Login by Administrator	38
8.1.2 Login by Activation Password	41
8.1.3 Forgot Password	42
8.2 Communication Settings	44
8.2.1 Set Wired Network Parameters	44
8.2.2 Set Wi-Fi Parameters	46
8.2.3 Set RS-485 Parameters	48
8.2.4 Set Wiegand Parameters	50
8.2.5 Set ISUP Parameters	50
8.2.6 Platform Access	52
8.2.7 Enable Mobile Network	53
8.3 User Management	53
8.3.1 Add Administrator	53
8.3.2 Add Face Picture	55
8.3.3 Add Fingerprint	57
8.3.4 Add Card	58
8.3.5 View PIN code	59
8.3.6 Set Authentication Mode	60
8.3.7 Search and Edit User	60
8.4 Data Management	61
8.4.1 Delete Data	61
8.4.2 Import Data	61

8.4.3 Export Data	62
8.5 Identity Authentication	62
8.5.1 Authenticate via Single Credential	63
8.5.2 Authenticate via Multiple Credential	63
8.6 Basic Settings	64
8.7 Password Management	66
8.8 Set Biometric Parameters	66
8.8.1 Set Face Liveness Level	66
8.8.2 Set Face Recognition Distance	67
8.8.3 Set Face Recognition Interval	67
8.8.4 Set Wide Dynamic Range	67
8.8.5 Set Face 1:1/1:N Security Level	67
8.8.6 Set ECO Mode	68
8.8.7 Set Face with Mask Detection	68
8.8.8 Set Multiple Faces Authentication	69
8.9 Set Access Control Parameters	69
8.9.1 Set Terminal Authentication Mode	69
8.9.2 Set Card Reader Authentication Mode	70
8.9.3 Enable NFC Card	71
8.9.4 Enable M1 Card and M1 Card Encryption	72
8.9.5 Set Door Contact Parameters	74
8.9.6 Set Door Open Duration	75
8.9.7 Set Authentication Interval	76
8.10 Time and Attendance Status Settings	77
8.10.1 Disable Attendance Mode via Device	78
8.10.2 Set Manual Attendance via Device	79
8.10.3 Set Auto Attendance via Device	81
8.10.4 Set Manual and Auto Attendance via Device	83

8.11 Preference Settings	85
8.11.1 Set Interface Style	85
8.11.2 Set Theme Mode	86
8.11.3 Set Authentication Page Shortcut	88
8.11.4 Set Control Center Displayed Items	90
8.12 System Maintenance	90
8.12.1 View System Information	90
8.12.2 View Device Capacity	90
8.12.3 Upgrade	91
8.12.4 View User Manual	91
8.12.5 Restore Parameters	91
8.12.6 Reboot	91
8.12.7 Advanced Settings	92
8.13 Video Intercom	92
8.13.1 Call Client Software from Device	93
8.13.2 Call Center from Device	93
8.13.3 Call Device from Client Software	94
8.13.4 Call Room from Device	94
8.13.5 Call Mobile Client from Device	95
8.13.6 Doorbell Call	95
Chapter 9 Quick Operation via Web Browser	96
9.1 Select Language	96
9.2 Time Settings	96
9.3 Privacy Settings	96
9.4 Administrator Settings	97
9.5 No. and System Network	98
Chapter 10 Operation via Web Browser	99
10.1 Login	99

10.2	Forgot Password	99
10.3	Live View	99
10.4	Person Management	101
10.4.1	Add Person Basic Information	101
10.4.2	Set Permission Duration	103
10.4.3	Add Face Picture	105
10.4.4	Add Card	107
10.4.5	Add Fingerprint	109
10.4.6	Add Room No.	111
10.4.7	Set Authentication Type	113
10.5	Search Event	115
10.6	Device Management	115
10.7	Configuration	116
10.7.1	View Device Information	116
10.7.2	Set Time	116
10.7.3	Change Administrator's Password	117
10.7.4	Account Security Settings	117
10.7.5	View Device Arming/Disarming Information	117
10.7.6	Network Settings	117
10.7.7	Set Video and Audio Parameters	122
10.7.8	Set Image Parameters	123
10.7.9	Alarm Settings	124
10.7.10	Access Control Settings	125
10.7.11	Video Intercom Settings	139
10.7.12	Card Settings	142
10.7.13	Platform Attendance	143
10.7.14	Set Privacy Parameters	145
10.7.15	Set Biometric Parameters	146

10.7.16 Set Open Platform	151
10.7.17 Preference Settings	153
10.7.18 Upgrade and Maintenance	155
10.7.19 Device Debugging	156
10.7.20 Log Query	157
10.7.21 Security Mode Settings	157
10.7.22 Certificate Management	157
Chapter 11 Other Platforms to Configure	159
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. Function Differences	166

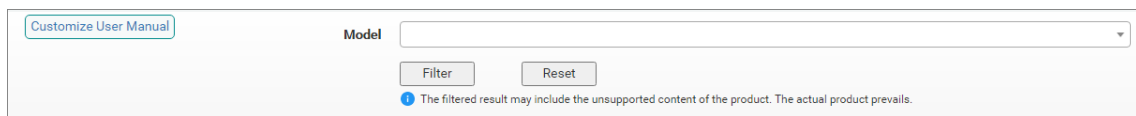
Chapter 1 How to Customize My Manual

This document provides the content customization function to help you quickly get the information that you need. On the Customize User Manual pane, you can select or check option(s) to filter contents and customize your own manual by different categories, including the product model, function, application, and scene.

Note

- This function is only available when you view the online documentation. If you have downloaded the PDF documentation for viewing, please ignore this chapter.
 - Options and contents in videos and pictures below are for examples only, please subject to the actual information.
-

Customize Manual by Product Model



The screenshot shows a user interface for customizing a manual. On the left, there is a button labeled "Customize User Manual". To its right, the word "Model" is displayed above a drop-down menu. Below the drop-down menu are two buttons: "Filter" and "Reset". At the bottom of the pane, there is a small blue circular icon followed by the text: "The filtered result may include the unsupported content of the product. The actual product prevails."

Figure 1-1 Customize User Manual Pane (by Product Model)

On the Customize User Manual pane, click the input field of the Model category to unfold the drop-down list, select a model from the list, and then click **Filter**. The result is shown below.

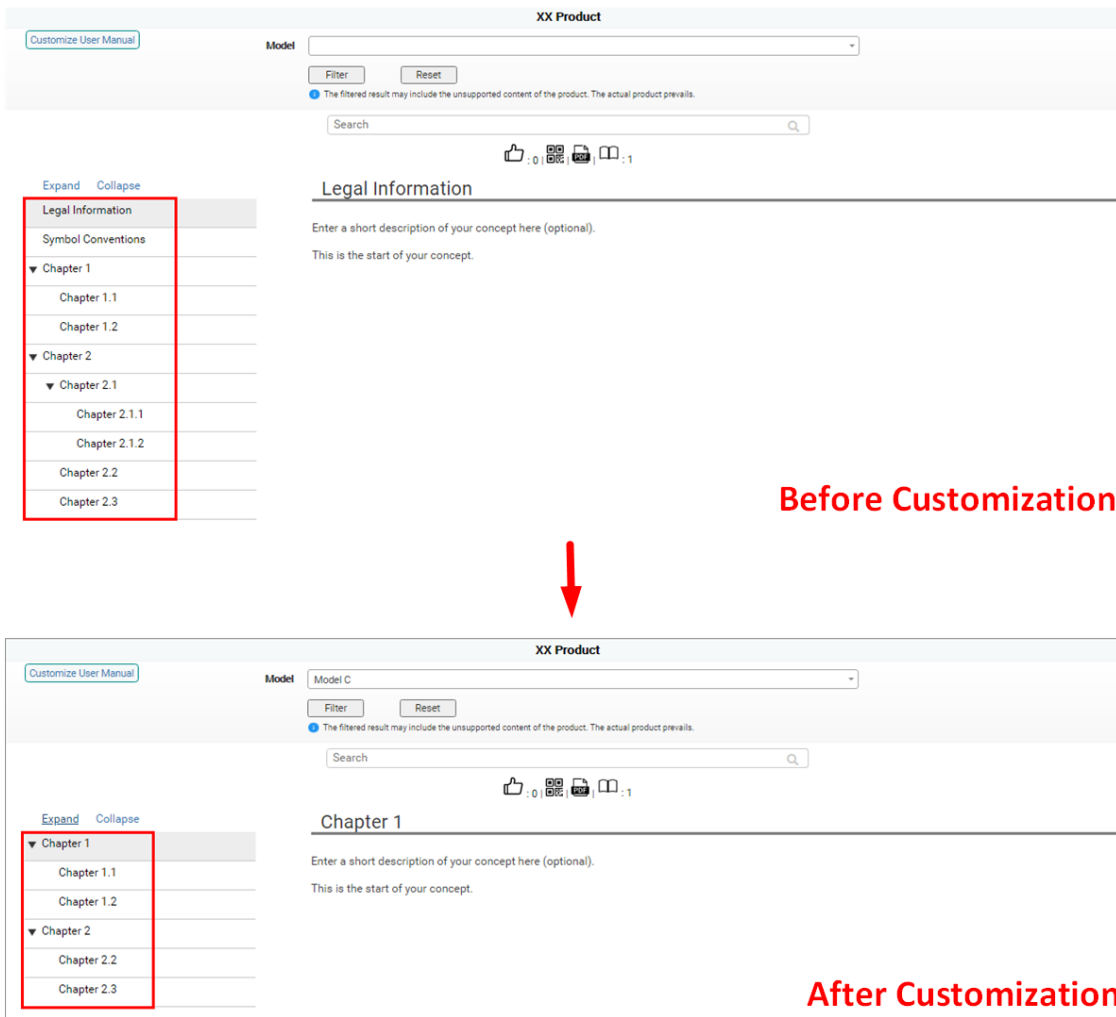


Figure 1-2 Result of Customizing Manual by Product Model

You can view the video below to get more details about the customization process.

Customize Manual by Application

Note

Due to the similarity among processes of customizing by Function, Application, and Scene categories, here we only take the process of customizing by application as an example.

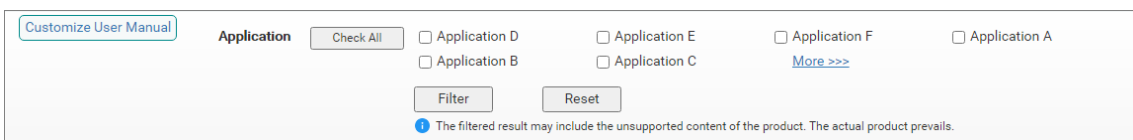


Figure 1-3 Customize User Manual Pane (by Application)

DS-K1T681 Series Face Recognition Terminal User Manual

On the Customize User Manual pane, check one or multiple options under the Application category, and then click **Filter**. The result is shown below.

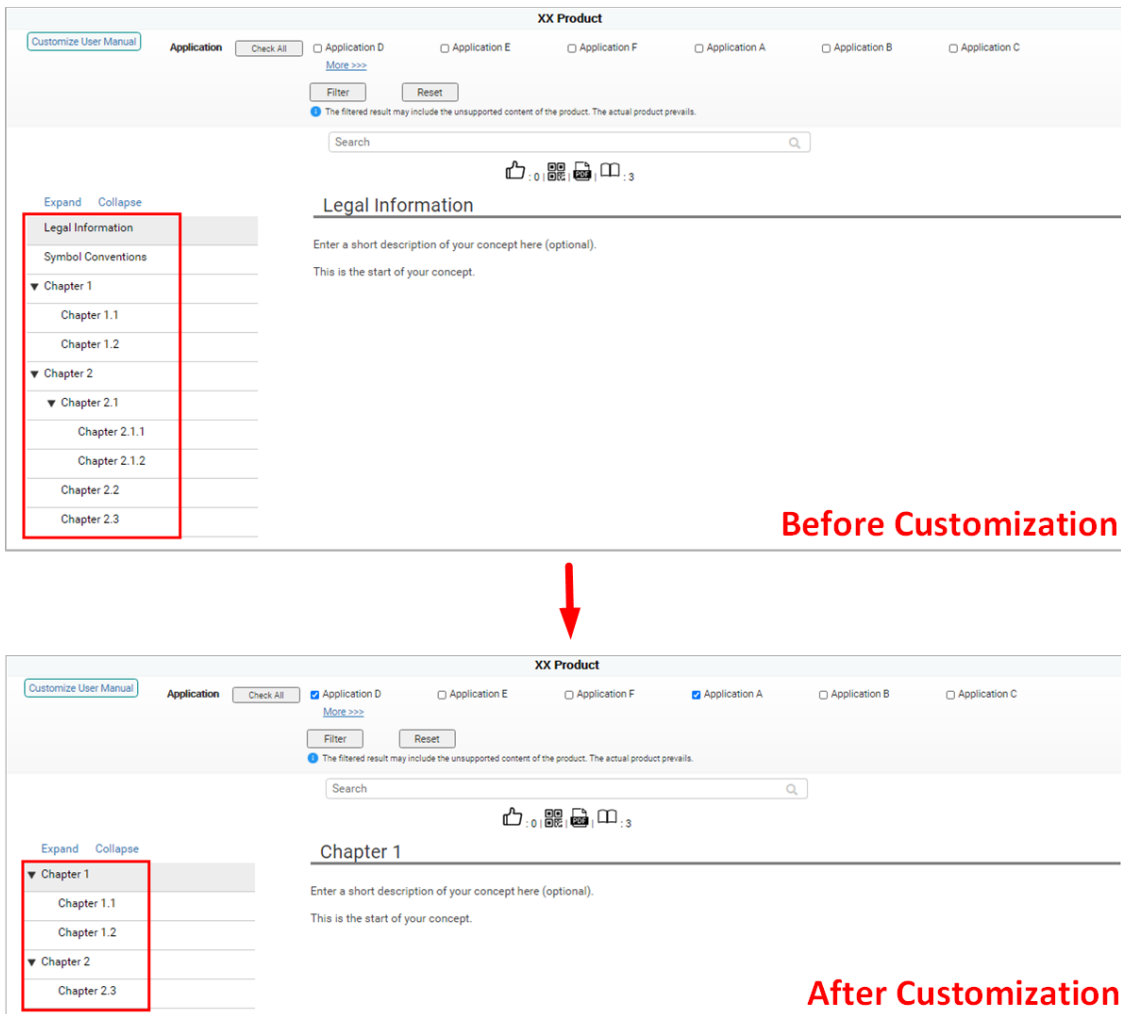


Figure 1-4 Result of Customizing Manual by Application

You can view the video below to get more details about the customization process.

Chapter 2 Overview

2.1 Overview

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

2.2 Features

- 8-inch touch screen with bezel-less design
- Presents card on the screen to authenticate card permission.
- 2 MP wide-angle dual-lens
- Face anti-spoofing
- Face recognition distance: 0.3 m to 3 m
- Deep learning algorithm
- Up to 100,000 face capacity, 500,000 card capacity, and 500,000 event capacity
- Face recognition duration < 0.2 s/User; face recognition accuracy rate $\geq 99\%$
- Capture linkage and captured pictures storage
- Transmits card and user data from or to the client software via TCP/IP protocol and saves the data on the client software
- Imports pictures from the USB flash drive to the device or export pictures, events, from the device to the USB flash drive
- Stand-alone operation
- Supports Wi-Fi in the 2.4G frequency band.

 **Note**

Only devices that support Wi-Fi support this function.

- Manage, search and set device data after logging in the device locally
- Connects to one external card reader via RS-485 protocol
- Connects to secure door control unit via RS-485 protocol to avoid the door opening when the terminal is destroyed
- Connects to external access controller or Wiegand card reader via Wiegand protocol
- Two-way audio with indoor station and main station
- Supports 6 attendance status, including check in, check out, break in, break out, overtime in, overtime out
- Configuration via the web client
- Remotely opens door and starts live view via Hik-Connect
- Supports ISAPI and ISUP 5.0 protocol

- Supports multiple languages: English, Thai, Portuguese, Russian, Spanish, Arabic, Japanese, Ukrainian, and Indonesian
- Self-defined voice prompt of authentication result

Chapter 3 Appearance

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

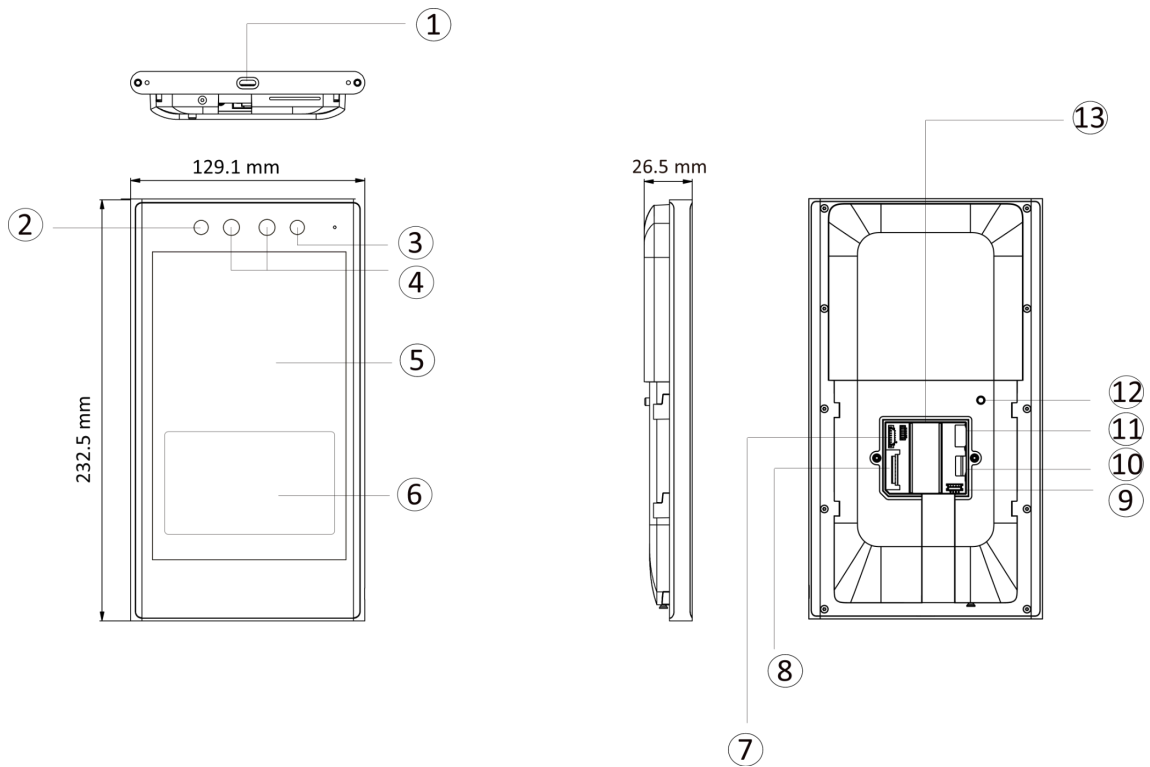


Figure 3-1 Face Recognition Terminal Diagram

Table 3-1 Description of Face Recognition Terminal

No.	Description
1	USB Type C Interface
2	IR Light
3	IR Light
4	Camera
5	Touch Screen
6	Card Presenting Area
7	USB Interface
8	Wiring Terminals

No.	Description
9	Debugging Port
10	SD Card Slot (Reserved)
11	SIM Card Slot (Reserved)
12	TAMPER
13	Network Interface

Chapter 4 Installation

4.1 Installation 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.



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

4.2 Flush Mounting with Gang Box

Steps



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

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

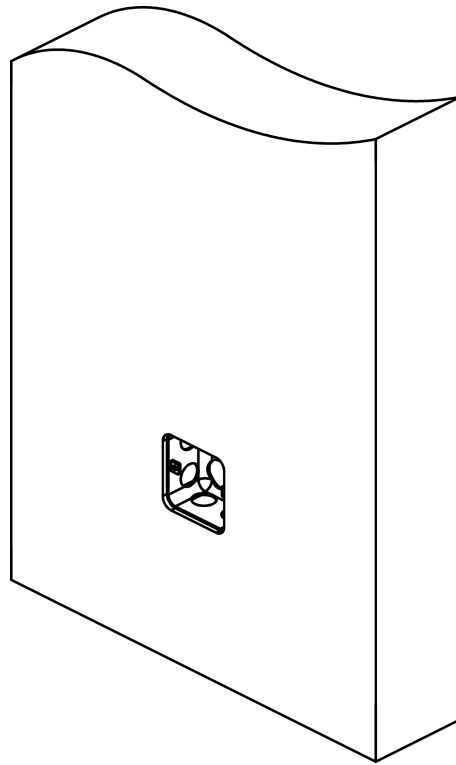


Figure 4-1 The Gang Box on the Wall

2. Secure the mounting plate on the gang box with the four supplied screws (SC-KA4X22). Remove the back cover and route the cable through the cable hole, wire the cables and insert the cables in the gang box.

 **Note**

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

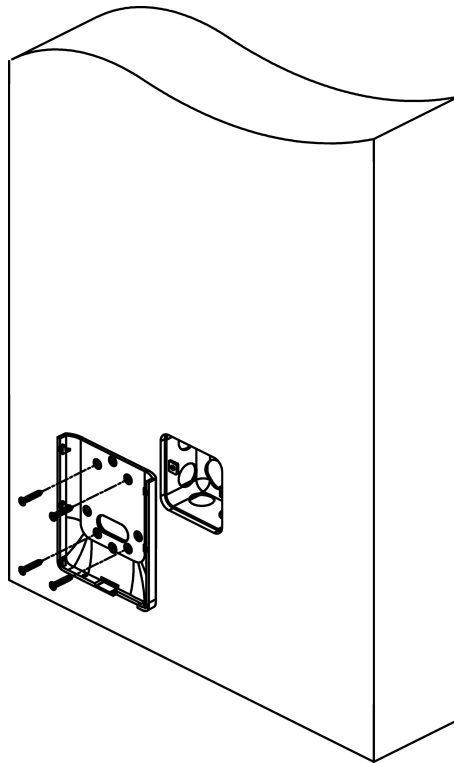


Figure 4-2 Secure the Mounting Plate and Wire the Cable

3. Align the device with the mounting plate, and secure the device on the mounting plate with 2 supplied screw (SC-KM3X8T10-SUS-NL).

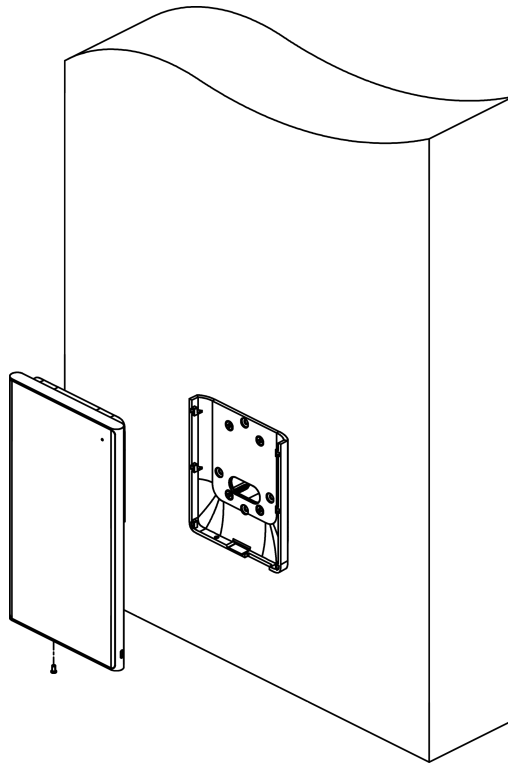


Figure 4-3 Align the Device

4.3 Mount With Cylinder Bracket

4.3.1 Preparation before Mounting with Bracket

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

Steps

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

 **Note**

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

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

 **Note**

Solder after pressing rivets to avoid water from entering.

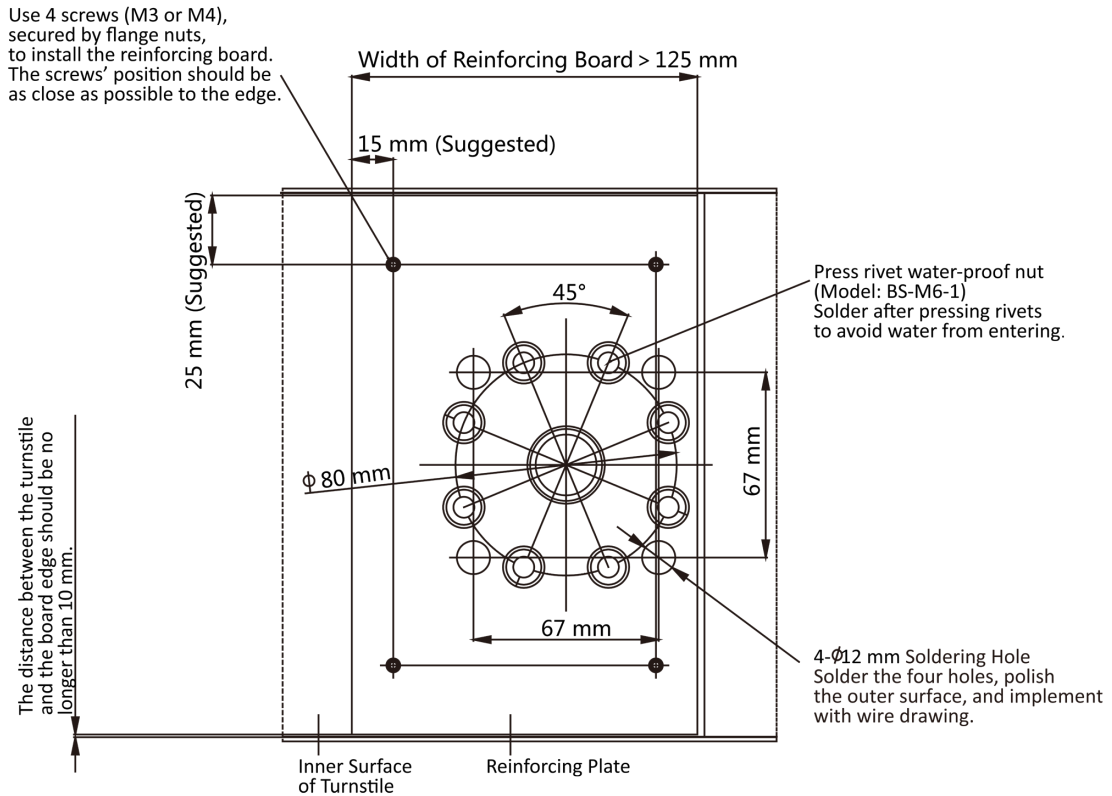


Figure 4-4 Drill Holes on Turnstile

3. Solder the other four holes, polish the surface, and implement wire drawing.
4. Solder circular tubes on the turnstile's inner surface to avoid water from entering.

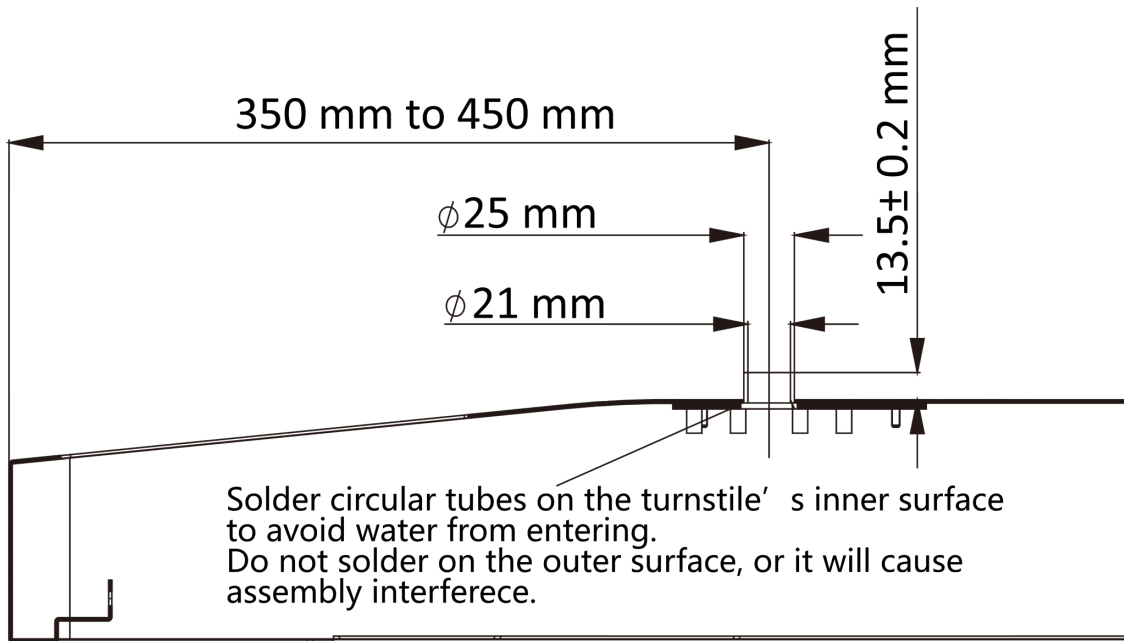


Figure 4-5 Solder Tubes

4.3.2 Cylinder Bracket Mounting

Steps

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

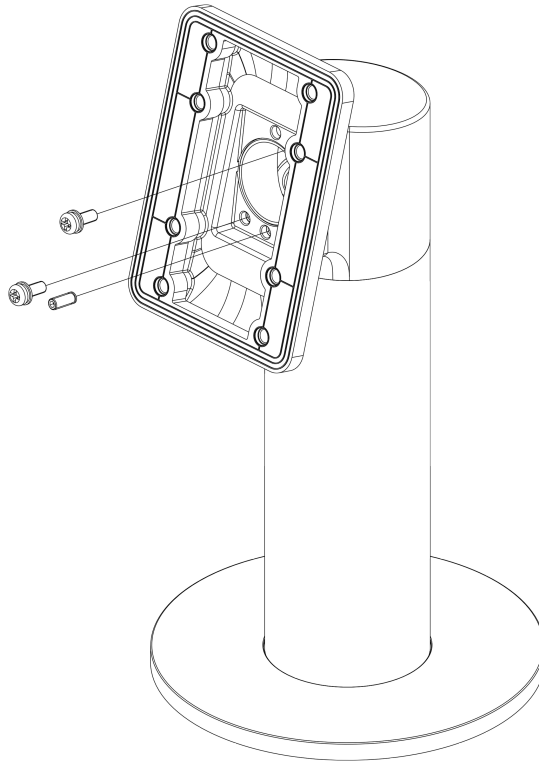


Figure 4-6 Adjust Bracket Angle

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

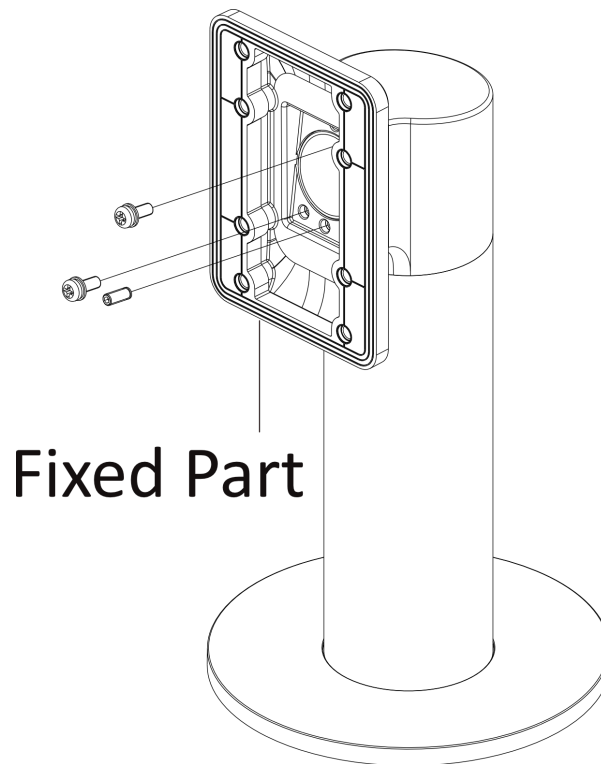


Figure 4-7 Adjust Bracket Angle

3. Pass face recognition terminal cables through the cable hole, and insert them into the inner turnstile. Pass the bracket bottom through the turnstile and fix it into the turnstile with self-contained nut. Adjust the bracket to the suitable angle, and fix the nut tightly by the wrench.

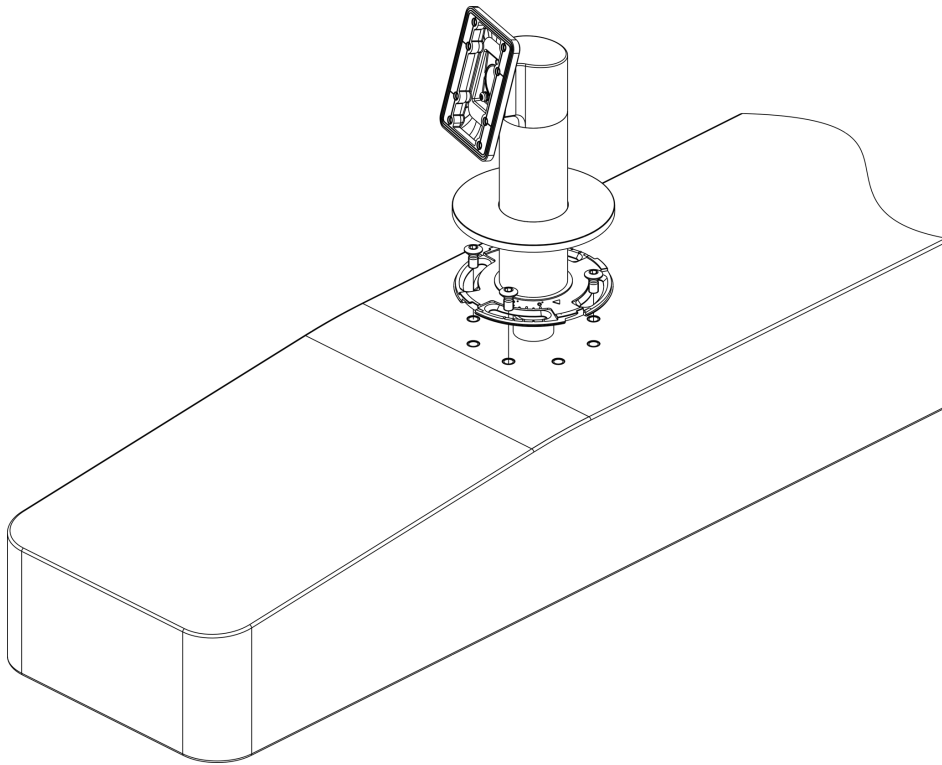


Figure 4-8 Fix the Bracket

4. Fix the mounting plate into the bracket by 4 SC-K1M4X6-SUS screws.

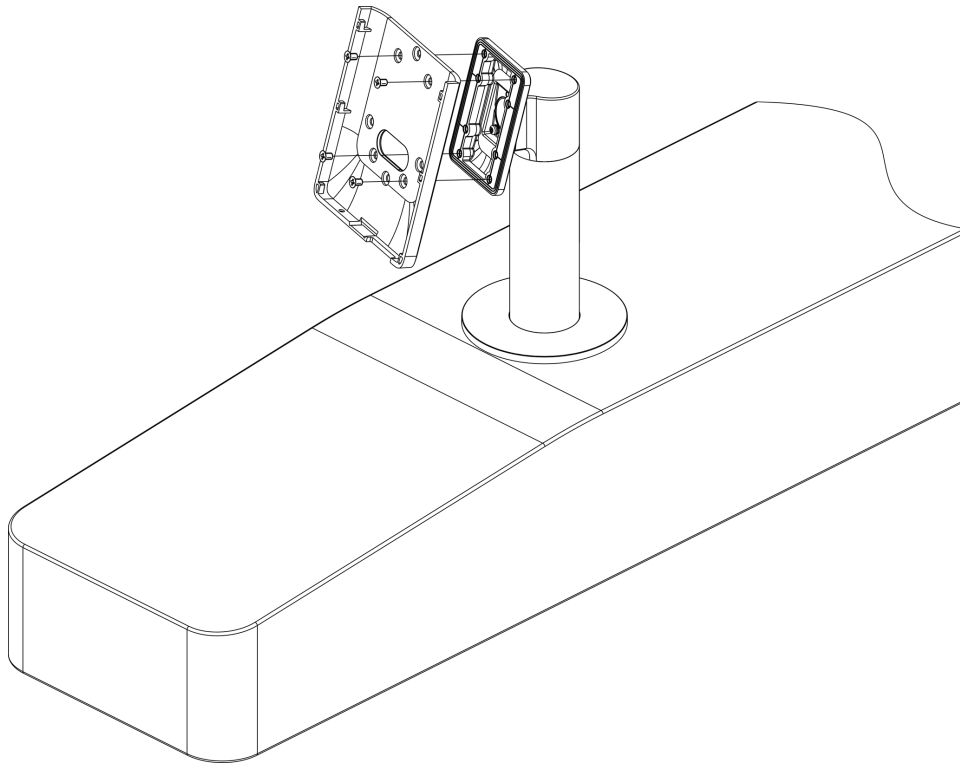


Figure 4-9 Fix the Mounting Plate

5. Fix the face recognition terminal into the mounting plate with 1 SC-KM3X8-T10-SUS-NL screws.

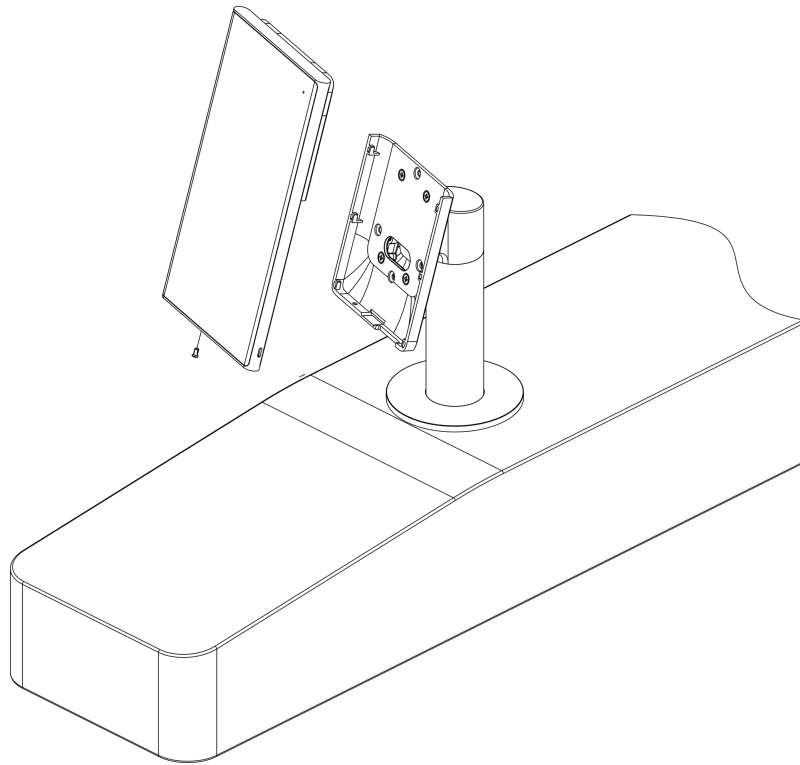


Figure 4-10 Fix the Device

Chapter 5 Wiring

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

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

Note

- If the cable size is 19 AWG, you should use a 12 V or 24 V switched-mode power supply. If you use a 12 V switched-mode power supply, the distance between the power supply and the device should be no more than 5 m. If you use a 24 V switched-mode power supply, the distance between the power supply and the device should be no more than 40 m.
If the cable size is 18 AWG, you should use a 12 V switched-mode power supply. And the distance between the power supply and the device should be no more than 10 m.
 - If the cable size is 16 AWG, you should use a 12 V switched-mode power supply. And the distance between the power supply and the device should be no more than 15 m.
-

5.1 Terminal Description

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

The terminal's diagram is as follows:

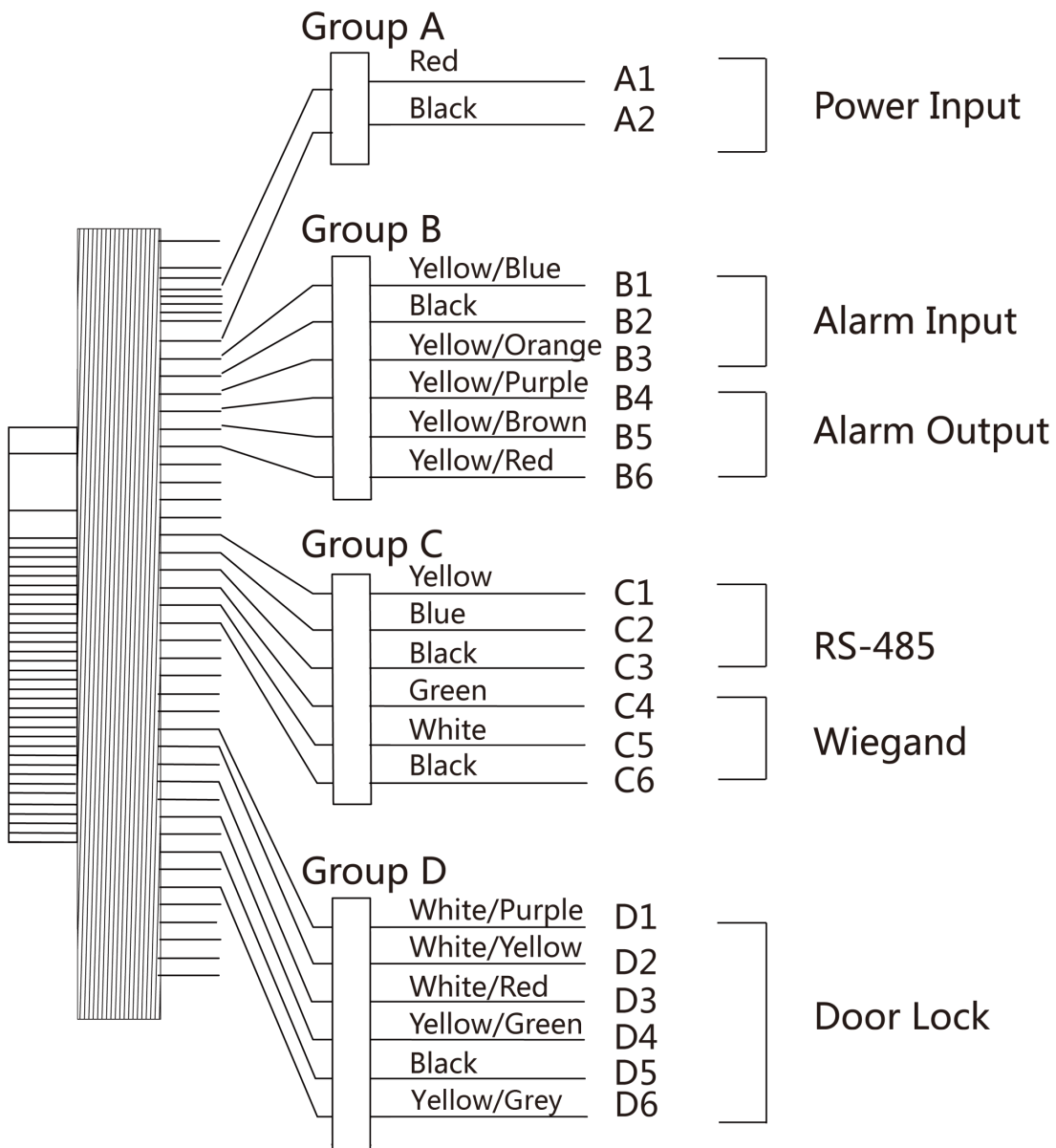


Figure 5-1 Terminal Diagram

The descriptions of the terminals are as follows:

Table 5-1 Terminal Descriptions

Group	No.	Function	Color	Name	Description
Group A	A1	Power Input	Red	+12 ~ 24 VDC, 3~1.5 A	Power Supply
	A2		Black	GND	Ground

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

5.2 Wire Normal Device

You can connect the terminal with normal peripherals.

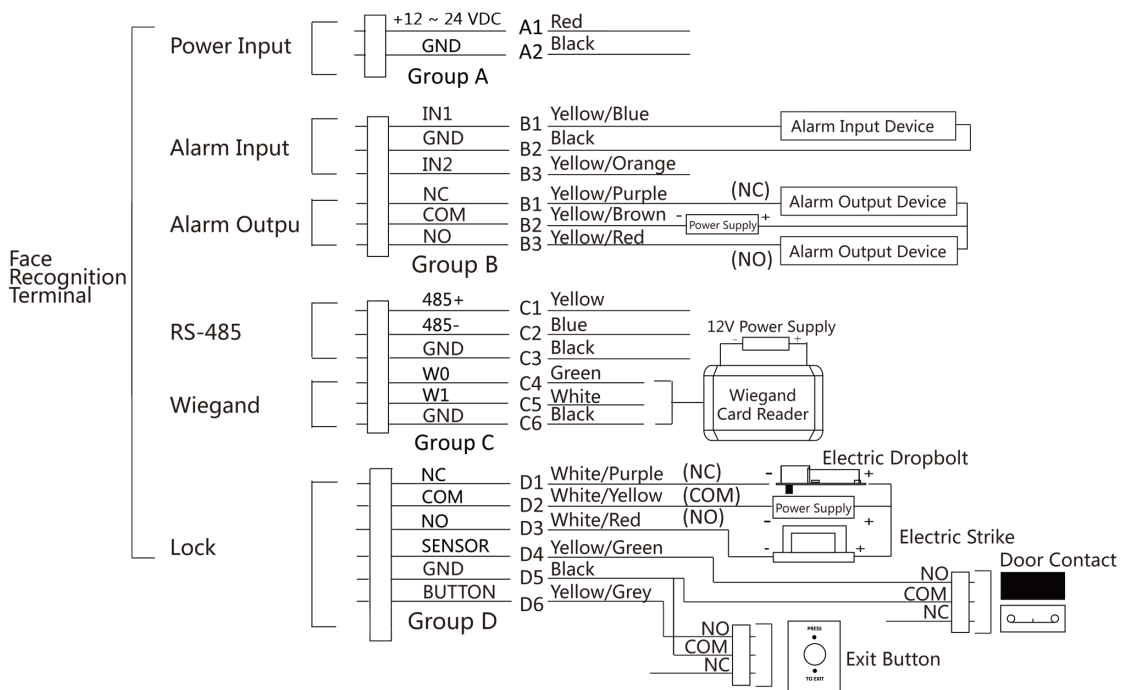


Figure 5-2 Device Wiring

Note

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

5.3 Wire Secure Door Control Unit

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

The wiring diagram is as follows.

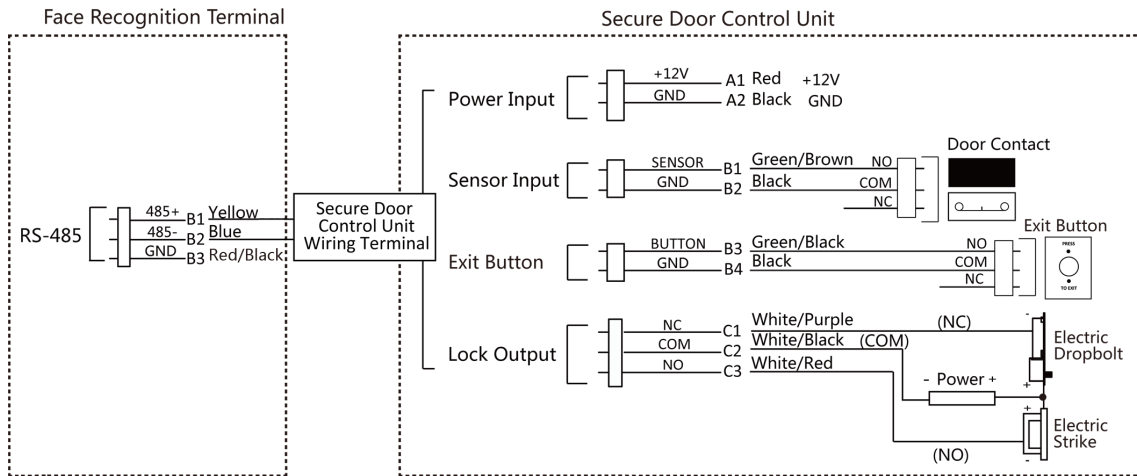


Figure 5-3 Secure Door Control Unit Wiring

Note

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

5.4 Wire Fire Module

5.4.1 Wiring Diagram of Door Open When Powering Off

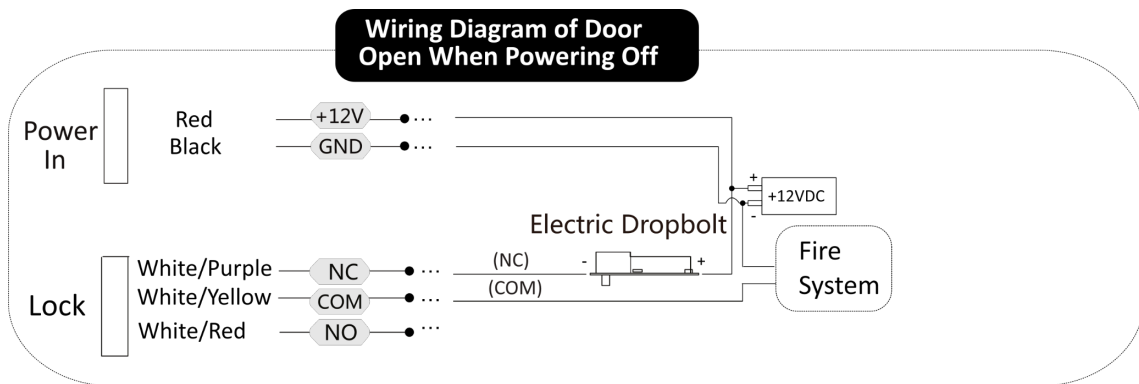
Lock Type: Anode Lock, Magnetic Lock, and Electric Bolt (NO)

Security Type: Door Open When Powering Off

Scenario: Installed in Fire Engine Access

Note

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



5.4.2 Wiring Diagram of Door Locked When Powering Off

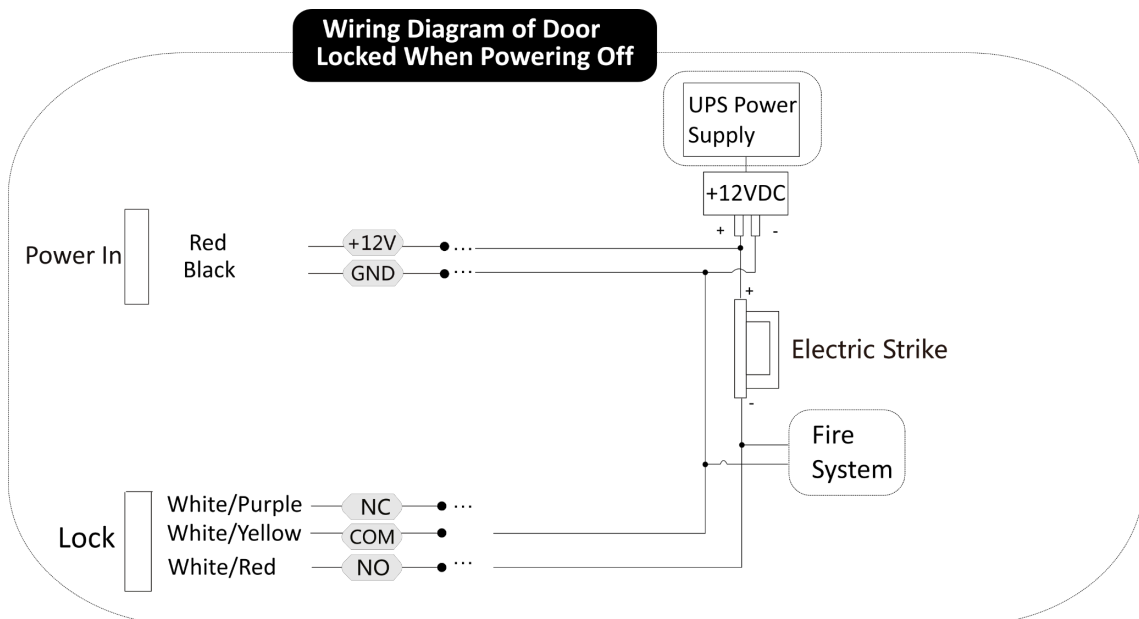
Lock Type: Cathode Lock, Electric Lock, and Electric Bolt (NC)

Security Type: Door Locked When Powering Off

Scenario: Installed in Entrance/Exit with Fire Linkage

Note

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



Chapter 6 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

6.1 Activate via Device

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

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

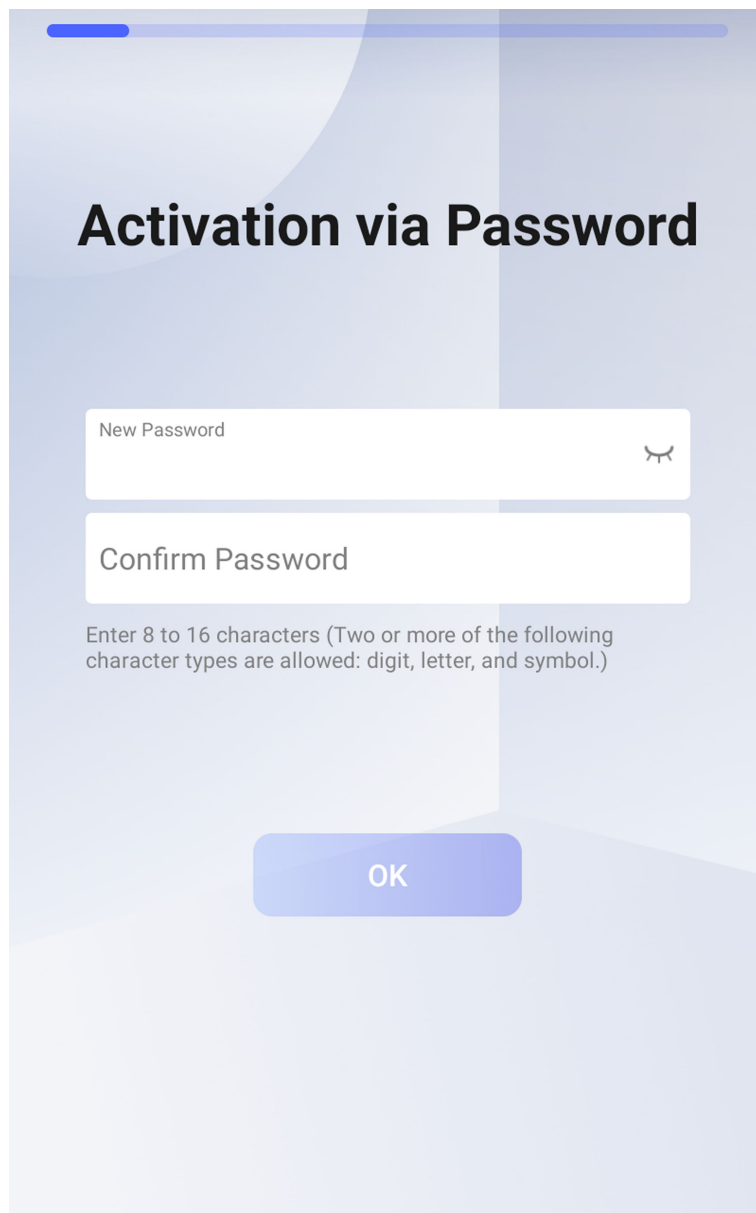


Figure 6-1 Activation Page

 **Caution**

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

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

Note

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

After activation, you should select language, set password change type, set application mode, set network, set platform parameters, set privacy parameters, and set administrator.

6.2 Activate via Web Browser

You can activate the device via the web browser.

Steps

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

Note

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

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

Caution

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

Note

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

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

6.3 Activate via SADP

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

Before You Start

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

DS-K1T681 Series Face Recognition Terminal User Manual

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

Steps

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

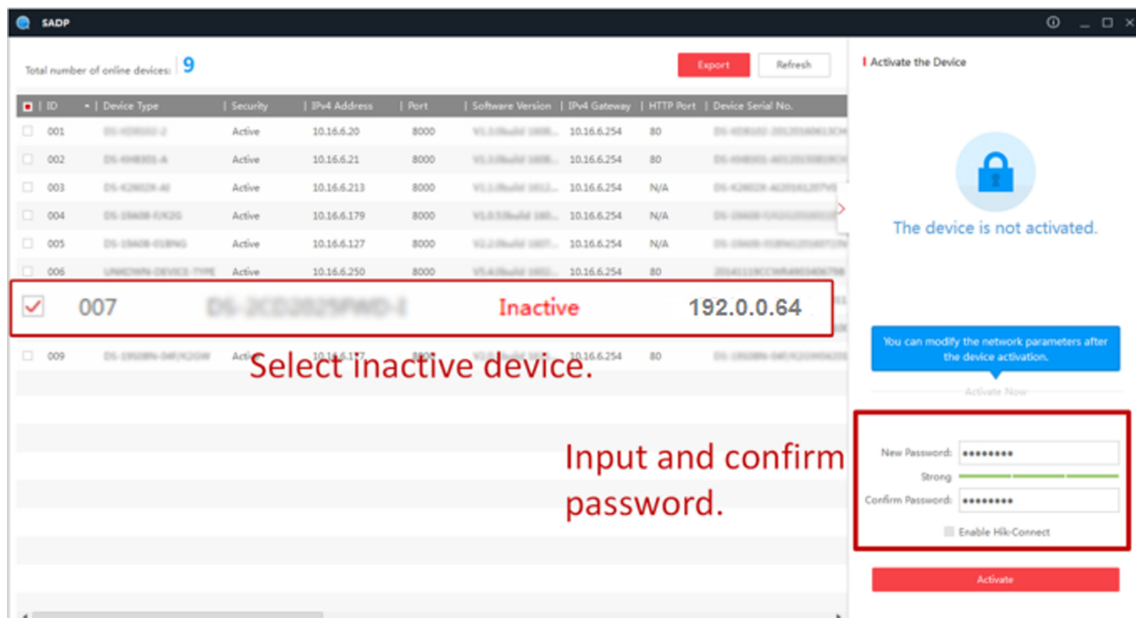
Caution

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

Note

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

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



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

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


6.4 Activate Device via iVMS-4200 Client Software

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

Steps

Note

This function should be supported by the device.

1. Enter the Device Management page.
 2. Click  on the right of **Device Management** and select **Device**.
 3. Click **Online Device** to show the online device area.
The searched online devices are displayed in the list.
 4. Check the device status (shown on **Security Level** column) and select an inactive device.
 5. Click **Activate** to open the Activation dialog.
 6. Create a password in the password field, and confirm the password.
-

Caution

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

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

Note

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

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

Chapter 7 Quick Operation

7.1 Select Language

After activation, you should select a language.

Steps

1. Select a language according to the actual needs.
2. Click **Next**.

7.2 Set Password Change Type

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

Change Password via Email Address

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

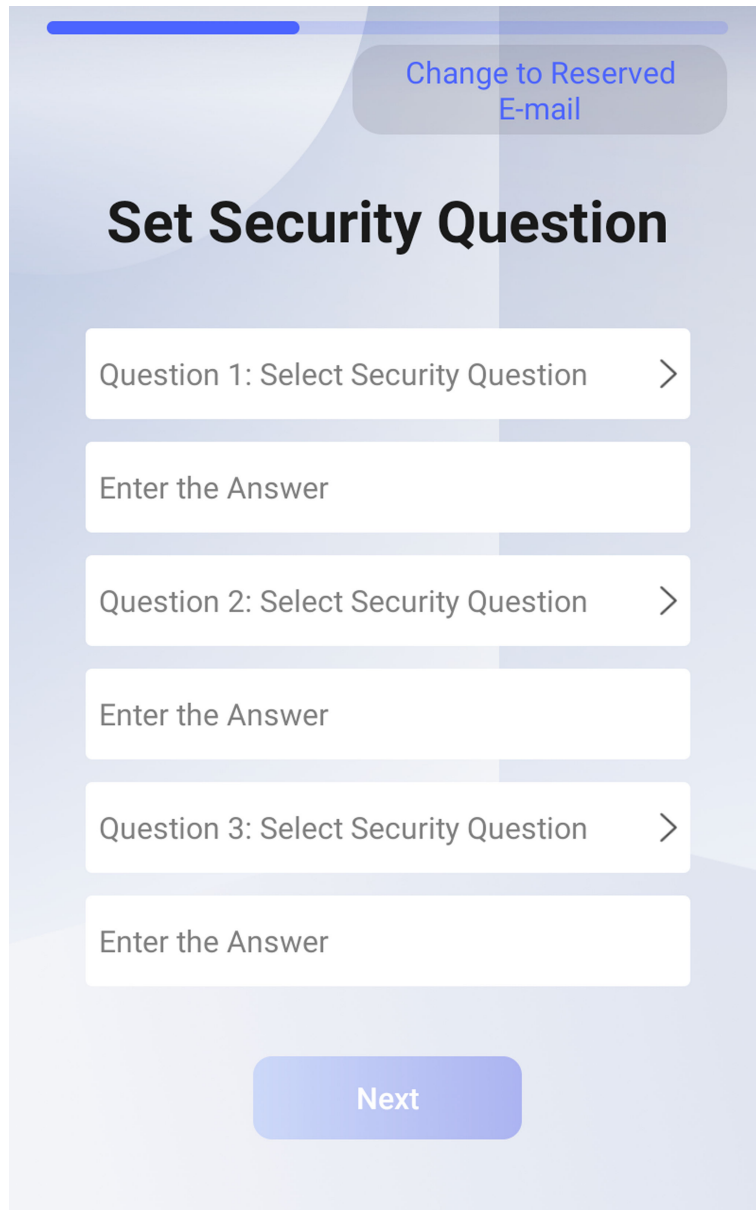


Figure 7-1 Password Change Page

Change via Security Questions

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

 **Note**

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

7.3 Set Network Parameters

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

Steps

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

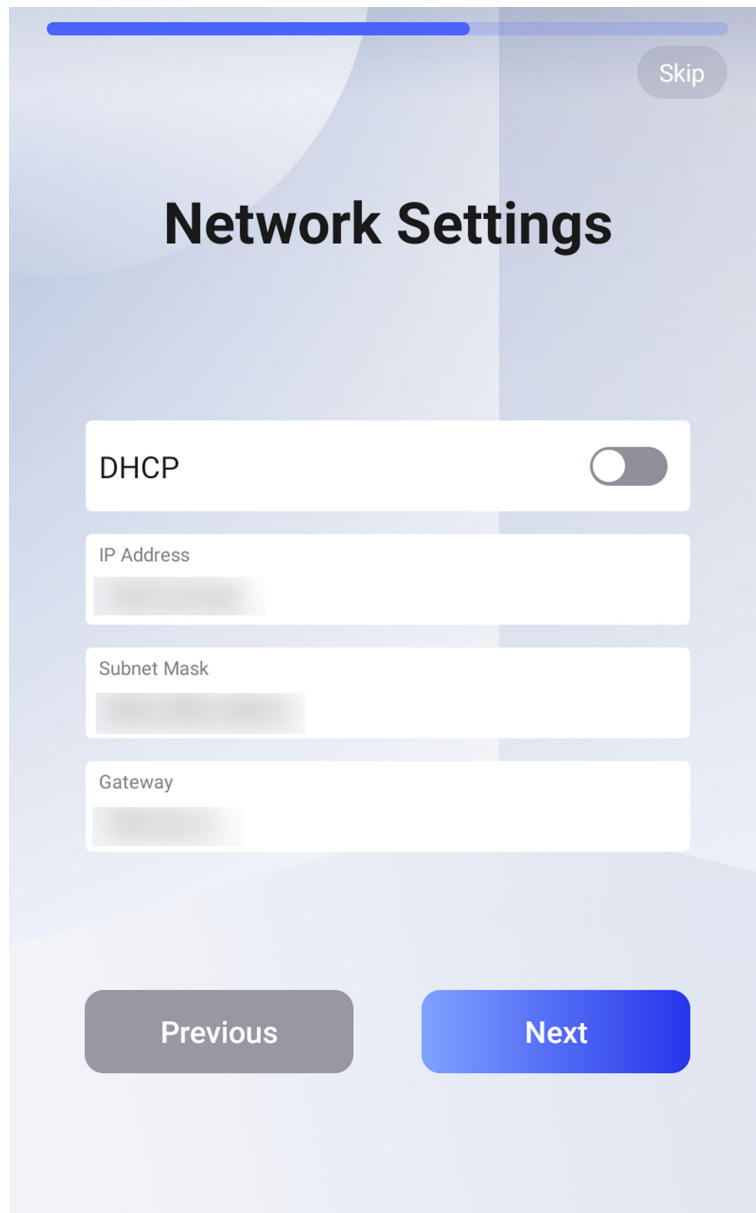


Figure 7-2 Select Network

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.

Note

IP address of 192.168.1.64, and 192.168.1.7 are not suggested to use.

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.

7.4 Access to Platform

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

Steps

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

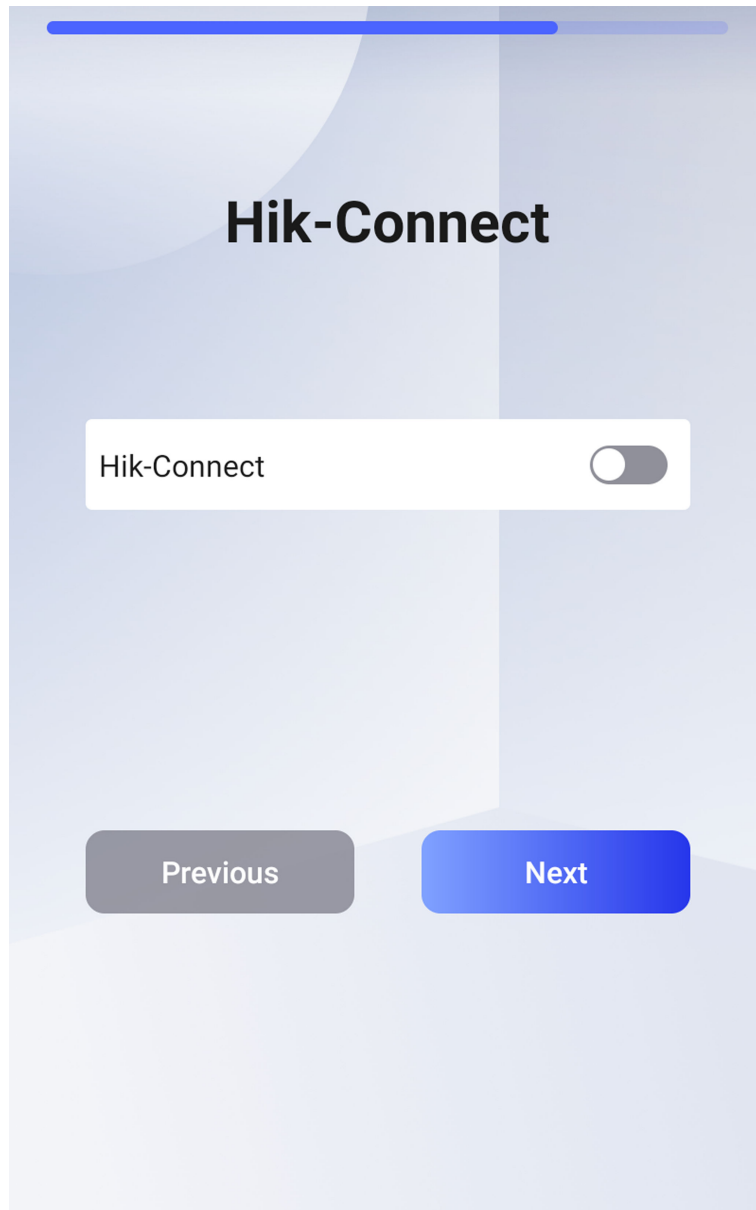


Figure 7-3 Access to Hik-Connect

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.

7.5 Set Administrator

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

Before You Start

Activate the device and select an application mode.

Steps

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

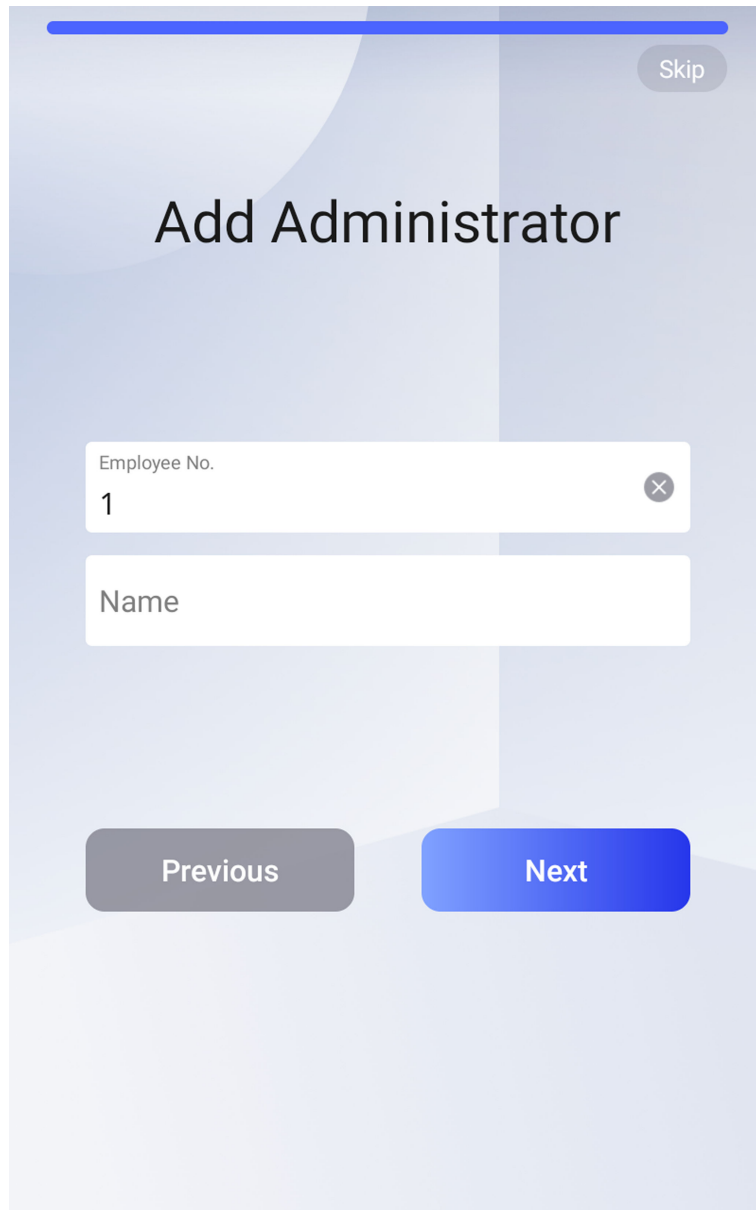








Figure 7-4 Add Administrator Page

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**.

4. Click OK.

You will enter the authentication page.

7.6 Status Description and Control Center

On the authentication page, you can view the device status at the upper right corner of the device interface. You can also use finger to pull down the authentication page to enter the control center.

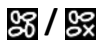
Control Center

Use finger to pull down the authentication page to enter the control center.

Status Icon Description



Device is armed/not armed.



Hik-Connect is enabled/disabled.



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



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



3G/4G is enabled.

Shortcut Keys Description



You can configure those shortcut keys displayed on the screen. For details, see [Basic Settings](#).




Scan QR code to authenticate.



The QR code can be obtained from the visitor terminal.



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



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



Enter password to authenticate.

Chapter 8 Basic Operation

8.1 Login

Login the device to set the device basic parameters.

8.1.1 Login by Administrator

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

Steps

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

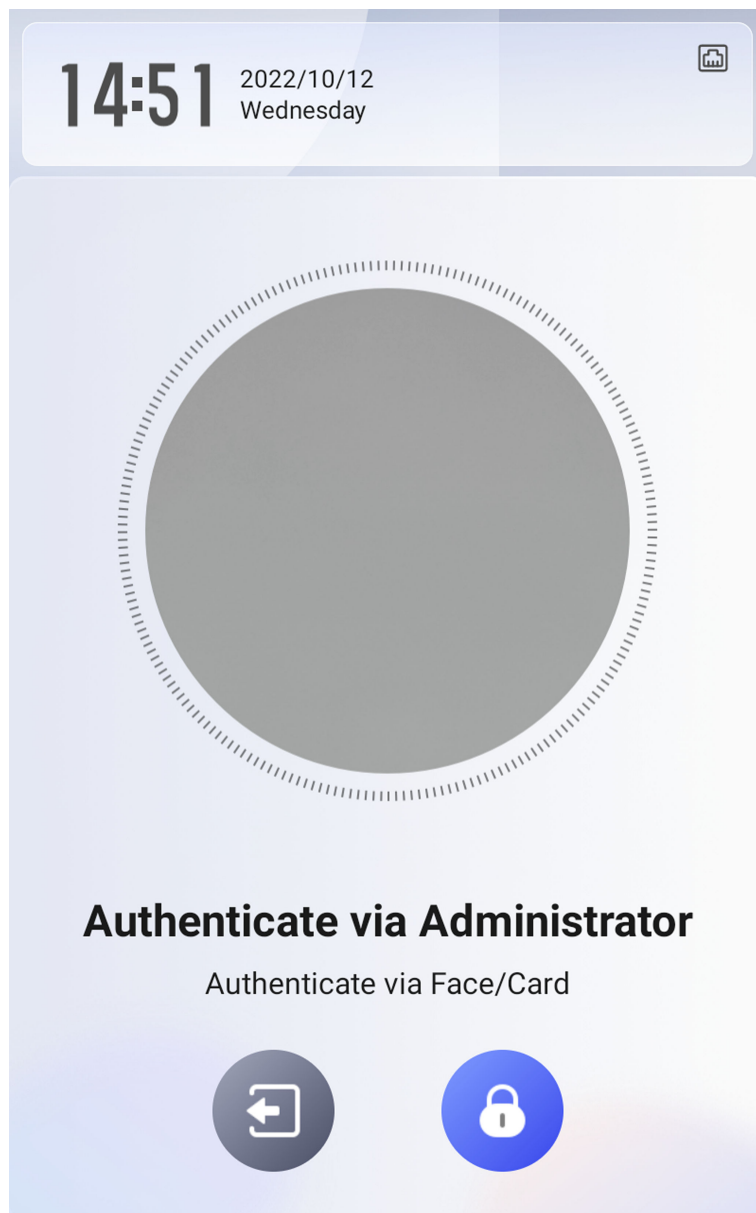


Figure 8-1 Admin Login

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

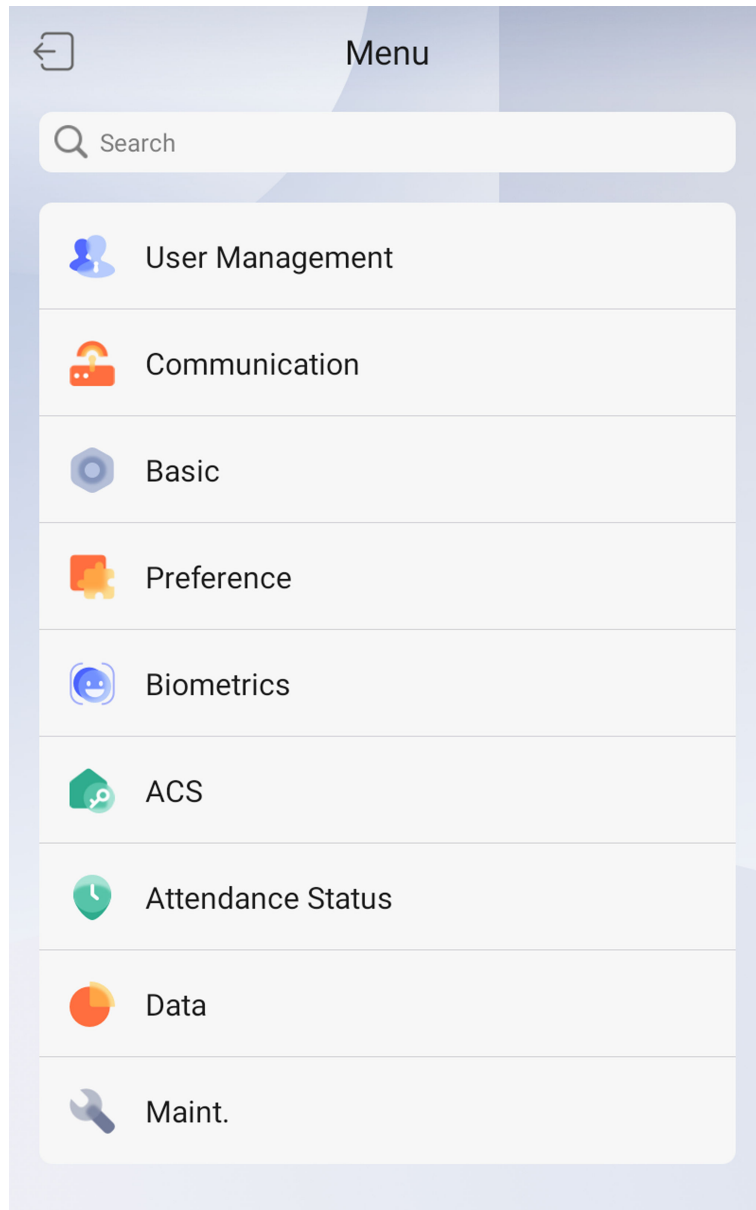




Figure 8-2 Home Page

 **Note**

- The device will be locked for 30 minutes after 5 failed fingerprint or card attempts.
- After login to the main page, you can search function in the searching bar which locates on the top of the main page.


3. Optional: Tap  and you can enter the device activation password for login.

4. Optional: Tap  and you can exit the admin login page.

8.1.2 Login by Activation Password

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

Steps

1. Long tap on the initial page for 3 s and slide to the left/right by following the gesture to enter password entering page.
2. Enter the password.
 - If you have added an administrator for the device, tap  and enter the password.
 - If you haven't added an administrator for the device, enter the password.
3. Tap **OK** to enter the home page.



Note

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

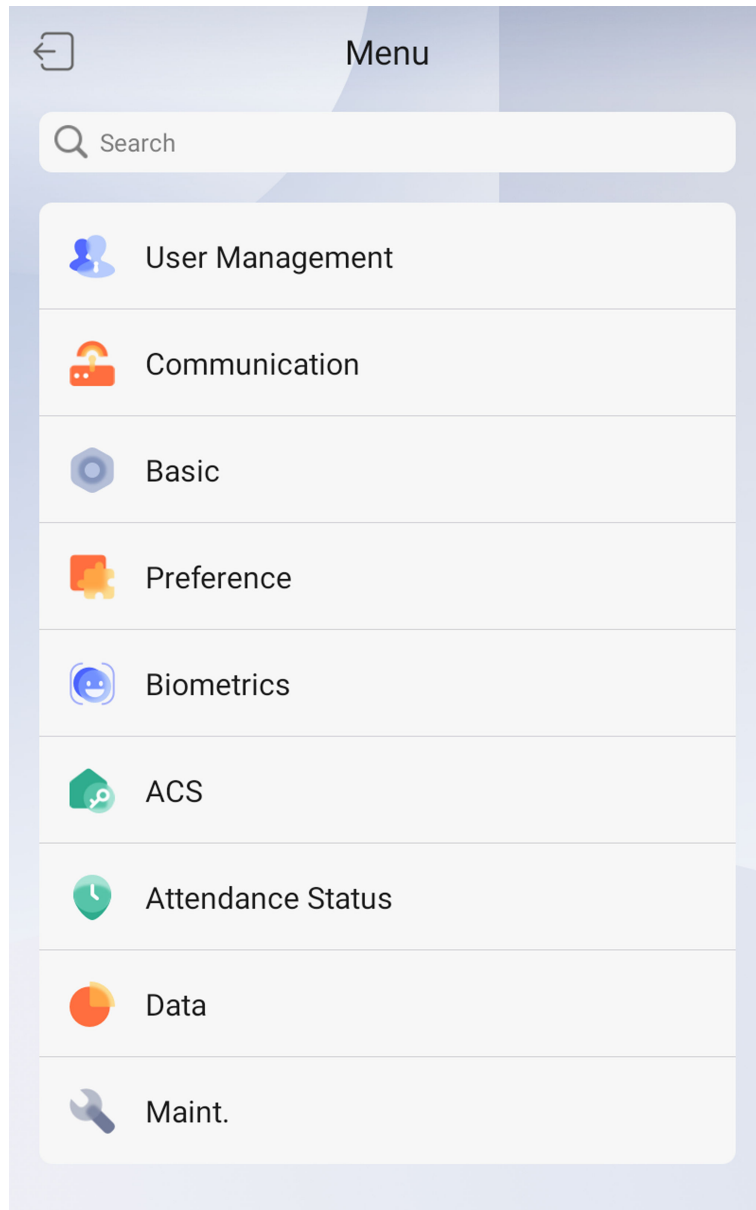



Figure 8-3 Home Page

8.1.3 Forgot Password

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

Steps

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

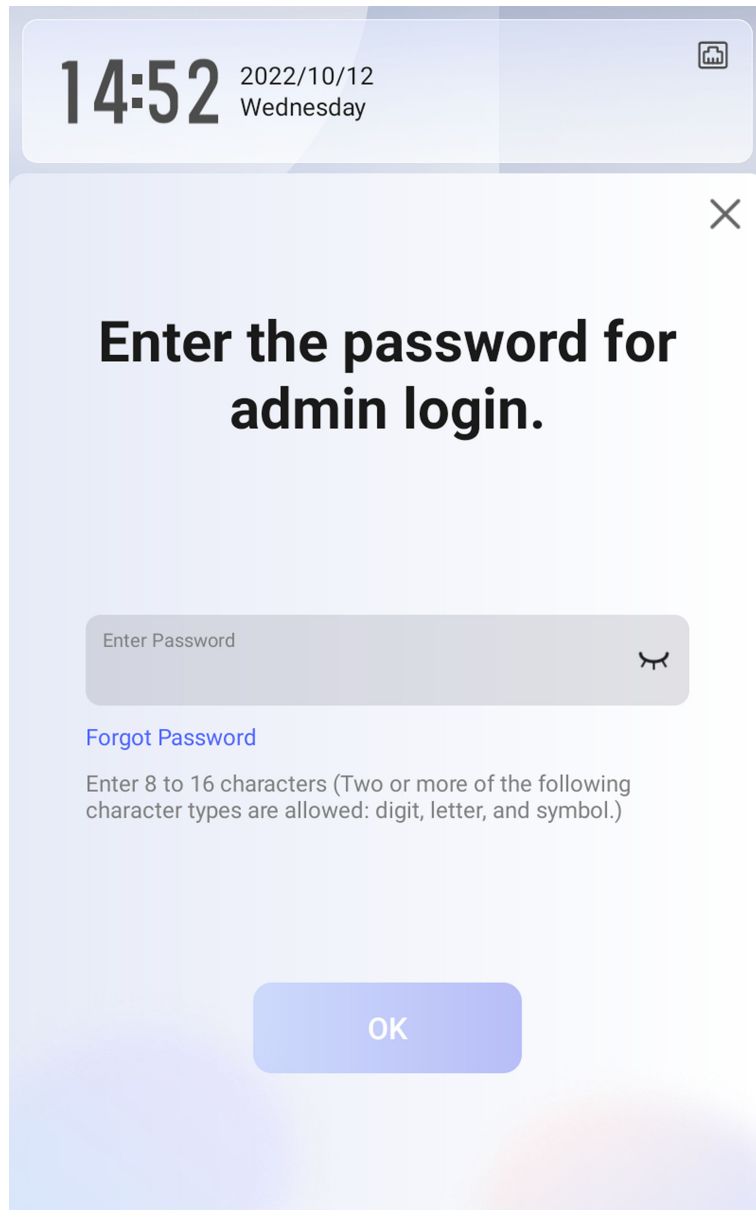


Figure 8-4 Password Authentication Page

- 3. Tap **Forgot Password**.**
- 4. Answer the security questions that configured when activation.**
- 5. Create a new password and confirm it.**
- 6. Tap **OK**.**

8.2 Communication Settings

You can set the network parameters, the Wi-Fi parameter, the RS-485 parameters, the Wiegand parameters, and enable 3G/4G on the communication settings page.

8.2.1 Set Wired Network Parameters

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

Steps

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

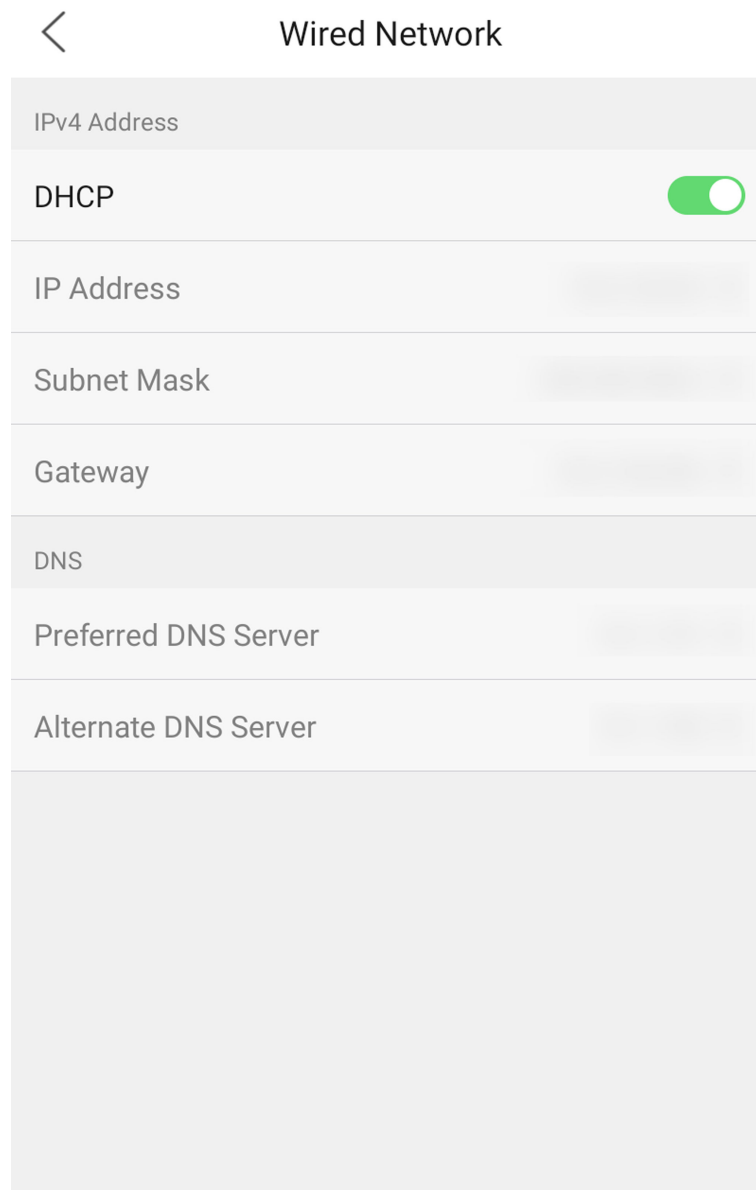


Figure 8-5 Wired Network Settings

3. Set IP Address, Subnet Mask, and Gateway.

- Enable **DHCP**, and the system will assign IP address, subnet mask, and gateway automatically.
- Disable **DHCP**, and you should set the IP address, subnet mask, and gateway manually.

 **Note**

- The device's IP address and the computer IP address should be in the same IP segment.
- IP address of 192.168.1.64, and 192.168.1.7 are not suggested to use.

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

8.2.2 Set Wi-Fi Parameters

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

Steps



The function should be supported by the device.

1. Tap **Communication** on the Home page to enter the Communication Settings page.
2. On the Communication Settings page, tap **Wi-Fi** to enter the page of Wi-Fi.

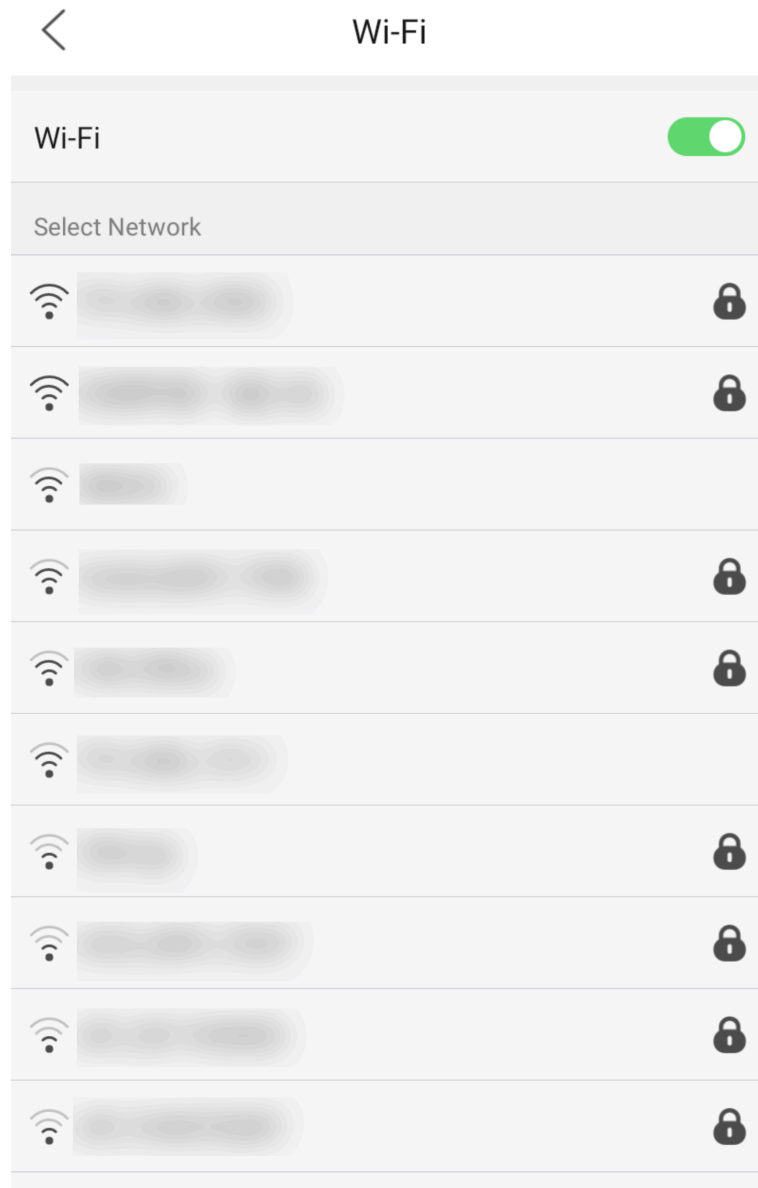


Figure 8-6 Wi-Fi Settings

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

 **Note**

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

5. Set the Wi-Fi's parameters.

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

8.2.3 Set RS-485 Parameters

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

Steps

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

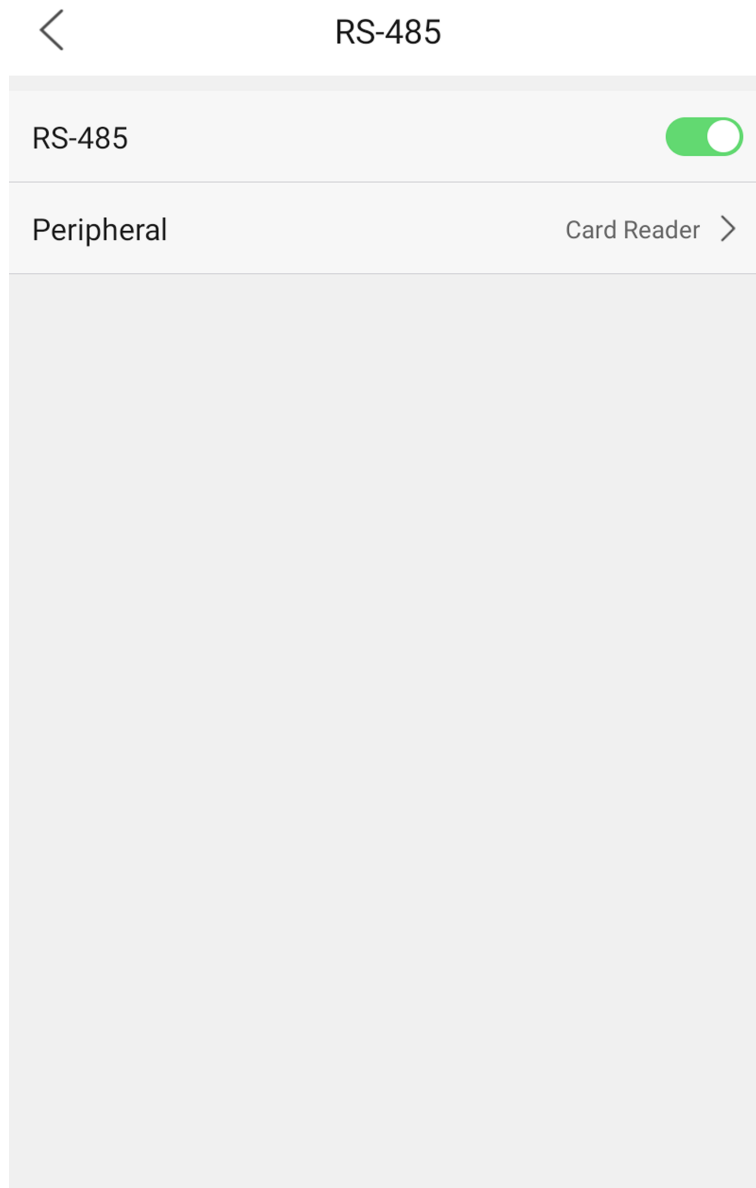


Figure 8-7 Set RS-485 Parameters

3. Enable **RS-485 Settings**.
4. 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.

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

8.2.4 Set Wiegand Parameters

You can set the Wiegand transmission direction.

Steps

1. Tap **Communication** on the Home page to enter the Communication Settings page.
2. On the Communication Settings page, tap **Wiegand** to enter the Wiegand tab.
3. Enable the Wiegand function.
4. Select a transmission direction.
 - Output: A face recognition terminal can connect an external access controller. And the two devices will transmit the card No. via Wiegand 34.
 - Input: A face recognition terminal can connect a Wiegand card reader.
5. Tap to save the network parameters.



Note

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

8.2.5 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 **Comm.** → **ISUP** .

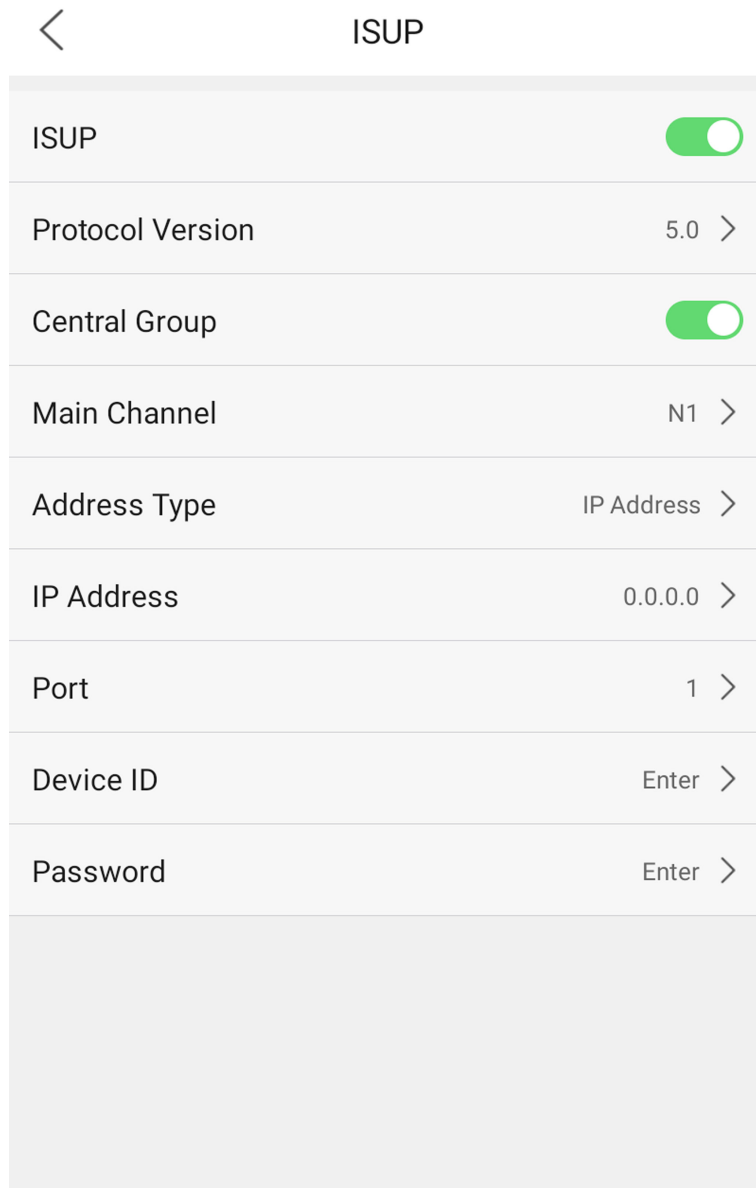


Figure 8-8 ISUP Settings

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.

ISUP Key

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.
-

8.2.6 Platform Access

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

Before You Start

Make sure your device has connected to a network.

Steps

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

8.2.7 Enable Mobile Network

You can enable **Mobile Network** function to connect the mobile network .



You can set mobile network when the device supports this function.

Tap **Communication Settings** on the main page to enter the Communication Settings page, and enable **Mobile Network**.

8.3 User Management

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

8.3.1 Add Administrator

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

Steps

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

< Add User >

Employee No.	2 >
Name	Enter >
User Role	Normal User >
Face	Add >
Card	0/50 >
Password	Not Configured
Authentication Settings	>

[Large grey rectangular area at the bottom of the screen]

3. Edit the employee ID.

 **Note**

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

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

Note

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

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

Note

- For details about adding a face picture, see [***Add Face Picture***](#) .

-  Note

For details about adding a fingerprint, see [***Add Fingerprint***](#) .

- For details about adding a card, see [***Add Card***](#) .

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

Note

For details about setting the authentication type, see [***Set Authentication Mode***](#) .

7. Enable the Administrator Permission function.

Enable Administrator Permission

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

8. Tap to save the settings.

8.3.2 Add Face Picture

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

Steps

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

Note

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

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

 **Note**

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

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



Figure 8-9 Add Face Picture

6. Look at the camera.

Note

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

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

7. Tap **Save** to save the face picture.

8. **Optional:** Tap **Try Again** and adjust your face position to add the face picture again.

9. Set the user role.

Administrator

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

Normal User

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

10. Tap  to save the settings.

8.3.3 Add Fingerprint

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

Steps

Note

- Devices with fingerprint module support fingerprint function.
 - Up to 10,000 fingerprints can be added.
-

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 **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 start with 0 and should not be duplicated.
-

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

 **Note**

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

-
5. Tap the 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 user.
- 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. 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.

8. Tap to save the settings.

8.3.4 Add Card

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

Steps

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

 **Note**

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

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

Note

- Numbers, upper case letters, lower case letters, and special characters are allowed in the user name.
- The suggested user name should be within 128 characters.

6. Tap the Card field and tap +.

7. Configure the card No.

- Enter the card No. manually.
- Present the card over the card presenting area to get the card No.

Note

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

8. Configure the card type.


9. Set the user role.

Administrator

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

Normal User

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

10. Tap  to save the settings.

8.3.5 View PIN code

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

Steps

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

Note

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

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

Note

- Numbers, upper case letters, lower case letters, and special characters are allowed in the user name.
- The suggested user name should be within 128 characters.

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

Note

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

6. 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.

8.3.6 Set Authentication Mode

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

Steps

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

Device

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

Custom


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

4. Tap  to save the settings.


8.3.7 Search and Edit User

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

Search User

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

Edit User

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

Note

The employee ID cannot be edited.

8.4 Data Management

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

8.4.1 Delete Data

Delete user data.

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

8.4.2 Import Data

Steps

1. Plug a USB flash drive in the device.
2. On the Home page, tap **Data → Import Data** .

Note

After insert the USB flash driver, you can tap **Import Data** on the **Data** page.

3. Tap **User Data, Face Data** or **Access Control Parameters** .

Note

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

4. Enter the created password when you exported the data. If you do not create a password when you exported the data, leave a blank in the input box and tap **OK** immediately.

Note

- If you want to transfer all user information from one device (Device A) to another (Device B), you should export the information from Device A to the USB flash drive and then import from

the USB flash drive to Device B. In this case, you should import the user data before importing the profile photo.

- The supported USB flash drive format is FAT32.
 - The imported pictures should be saved in the folder (named enroll_pic) of the root directory and the picture's name should be follow the rule below:
Card No. _Name _Department _Employee ID _Gender.jpg
 - If the folder enroll_pic cannot save all imported pictures, you can create another folders, named enroll_pic1, enroll_pic2, enroll_pic3, enroll_pic4, under the root directory.
 - The employee ID should be less than 32 characters. It can be a combination of lower letters, upper letters, and numbers. It should not be duplicated, and should not start with 0.
 - Requirements of face picture should follow the rules below: It should be taken in full-face view, directly facing the camera. Do not wear a hat or head covering when taking the face picture. The format should be JPEG or JPG. The resolution should be 640 × 480 pixel or more than of 640 × 480 pixel. The picture size should be between 60 KB and 200 KB.
-

8.4.3 Export Data

Steps

1. Plug a USB flash drive in the device.
2. On the Home page, tap **Data** → **Export Data** .



After insert the USB flash driver, you can tap **Export Data** on the **Data** page.

3. Tap **Face Data**, **Event Data**, **User Data**, or **Access Control Parameters**.



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.



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

8.5 Identity Authentication

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

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

1:N Matching

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

1:1 Matching

Compare the captured face picture with the linked face picture.

8.5.1 Authenticate via Single Credential

Set the user authentication type before authentication. For details, see [***Set Authentication Mode***](#) .
Authenticate face, fingerprint, card or QR code.

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.



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.



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

Password

Enter the password to authenticate via password.

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

8.5.2 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**

- After enabling **Control Initial Authentication Type** on the web client, the initial authentication type will be fixed.
 - The card can be normal IC card, or encrypted card.
 - The card can be normal IC card, or encrypted card.
 - If the QR Code Scanning function is enabled, you can put the QR code in front of the device camera to authenticate via QR code.
 - The dimension of the recognized QR code picture should be larger than 6 cm × 6 cm.
 - The dimension of the recognized QR code picture should be larger than 6 cm × 6 cm.
-
2. After the previous credential is authenticated, continue authenticate other credentials.
If authentication succeeded, the prompt "Authenticated" will pop up.

8.6 Basic Settings

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

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

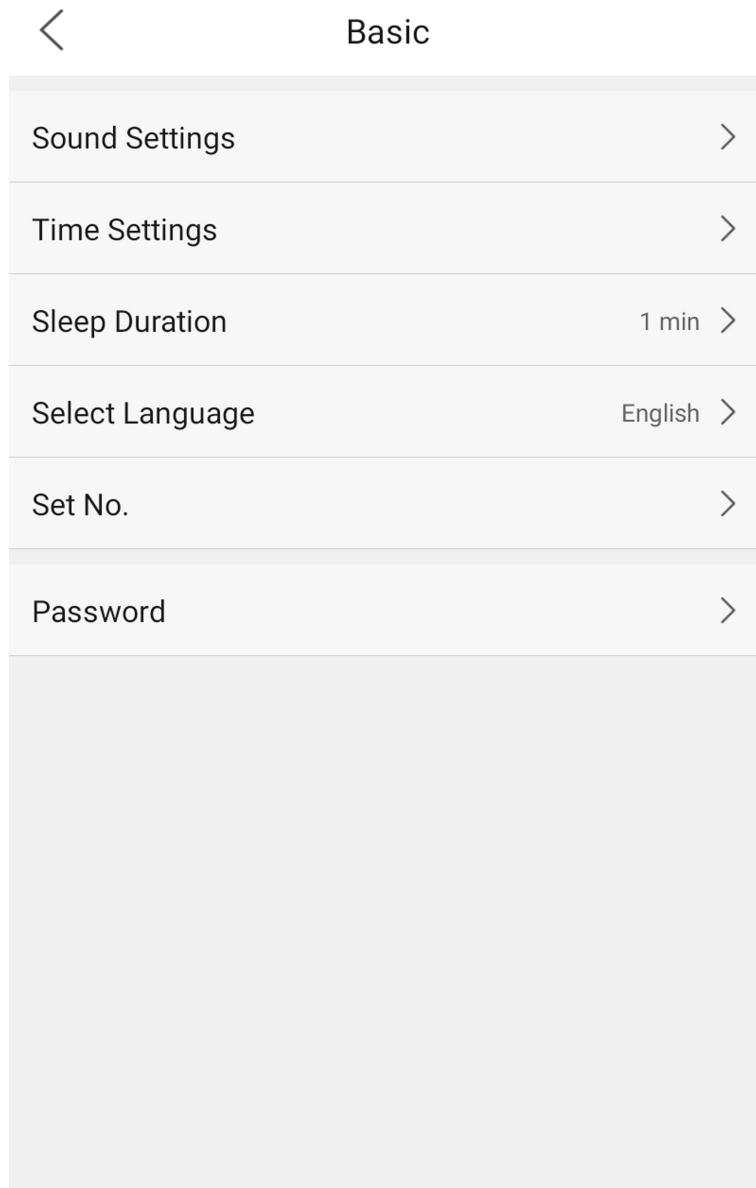


Figure 8-10 Basic Settings Page

Sound Settings

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

 **Note**

You can set the voice volume between 0 and 10.

Time Settings

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

Sleeping Duration

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

Select Language

Select the language according to actual needs.

Set No.

Set the Community No., Building No. and Unit No.

8.7 Password Management

You can change device password.

Steps

1. Long tap on the initial page for 3 s and slide to the left/right by following the gesture and login the device home page. Tap **Basic** → **Password** .
2. Tap **Change Password**. Enter the old password.
3. Enter the new password and confirm it.
4. Tap **OK**.



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 two 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.

8.8 Set Biometric Parameters

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

8.8.1 Set Face Liveness Level

Set the matching security level when performing face anti-spoofing authentication

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

After enabling face anti-spoofing function, you can set the matching security level when performing face anti-spoofing authentication. The higher the level, the more strict of the recognition.

8.8.2 Set Face Recognition Distance

Set the valid distance between the person and the device camera.

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

Set the valid distance between the person and the device camera when authenticating.

8.8.3 Set Face Recognition Interval

You can set the time interval between 2 continuous face recognitions when authenticating.

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

Set the time interval between 2 continuous face recognitions when authenticating.



Note

You can input the number from 1 to 10.

8.8.4 Set Wide Dynamic Range

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

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



Note

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

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

8.8.5 Set Face 1:1/1:N Security Level

Set the face recognition threshold.

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

Set the parameters.

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.

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.

8.8.6 Set ECO Mode

After enabling the ECO mode, the device will use the IR camera to authenticate faces in the low light or dark environment.

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

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

ECO Threshold

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

ECO Mode (1:1)

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

ECO Mode (1:N)

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

8.8.7 Set Face with Mask Detection

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

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

After enabling the face with mask detection, the system will recognize the captured face with mask picture. You can set face with mask & face 1:N level and the strategy.

Reminder of Wearing

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

Must Wear

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

8.8.8 Set Multiple Faces Authentication

You can authenticate multiple faces at the same time.

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

After multiple faces authentication is enabled, multiple faces authentication is supported.

8.9 Set Access Control Parameters

You can set the access control permissions, including the functions of authentication mode, enable NFC card, enable M1 card, door contact, open duration(s) and authentication interval(s).

8.9.1 Set Terminal Authentication Mode

Set the device's authentication mode. You can also customize the authentication mode. if authenticating on the device, you should follow the device's authentication mode.

On the Home page, tap **ACS** (Access Control Settings) to enter the Access Control Settings page.

Select the face recognition terminal's authentication mode. You can also customize the authentication mode.



Note

- Only the device with the fingerprint module supports the fingerprint related function.
 - Biometric recognition products are not completely applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.
 - If you adopt multiple authentication modes, you should authenticate other methods before authenticating face.
-

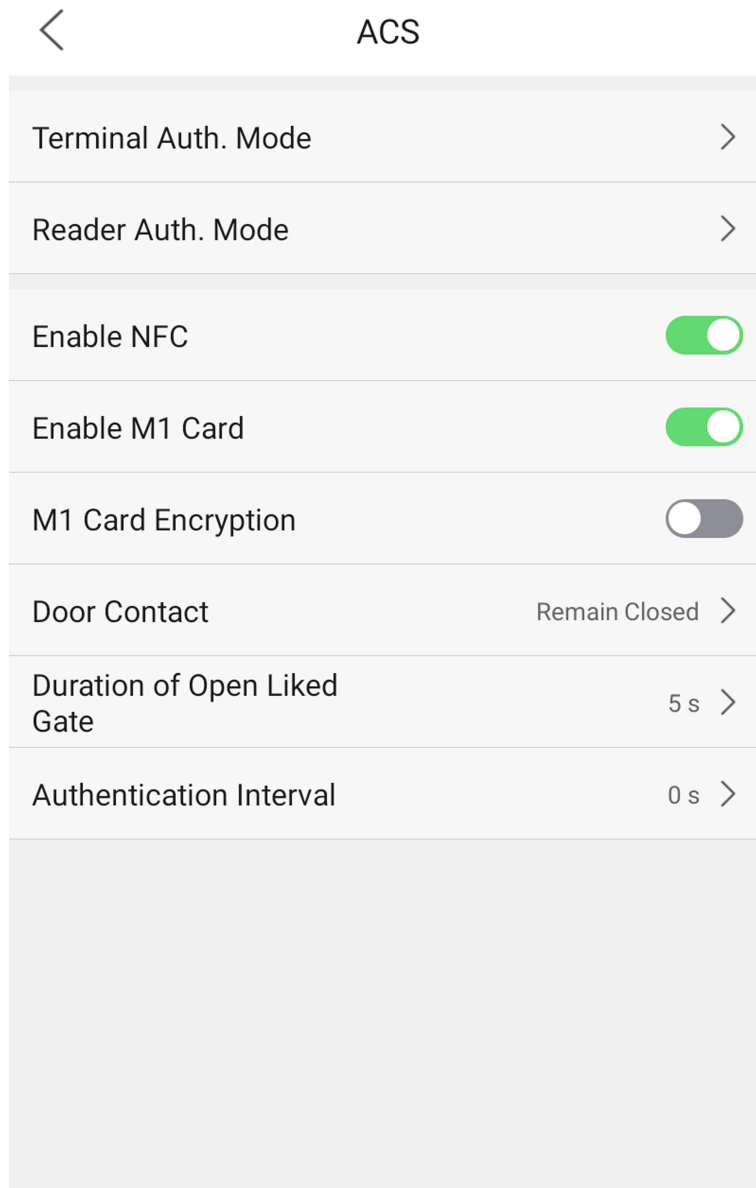


Figure 8-11 Access Control Parameters

8.9.2 Set Card Reader Authentication Mode

Set the card reader's authentication mode and if authenticating on the card reader, you should follow the card reader's authentication mode.

On the Home page, tap **ACS** (Access Control Settings) to enter the Access Control Settings page. Select **Reader's Auth. Mode** (card reader's authentication mode). If authenticating on the card reader, you should follow the card reader's authentication mode.

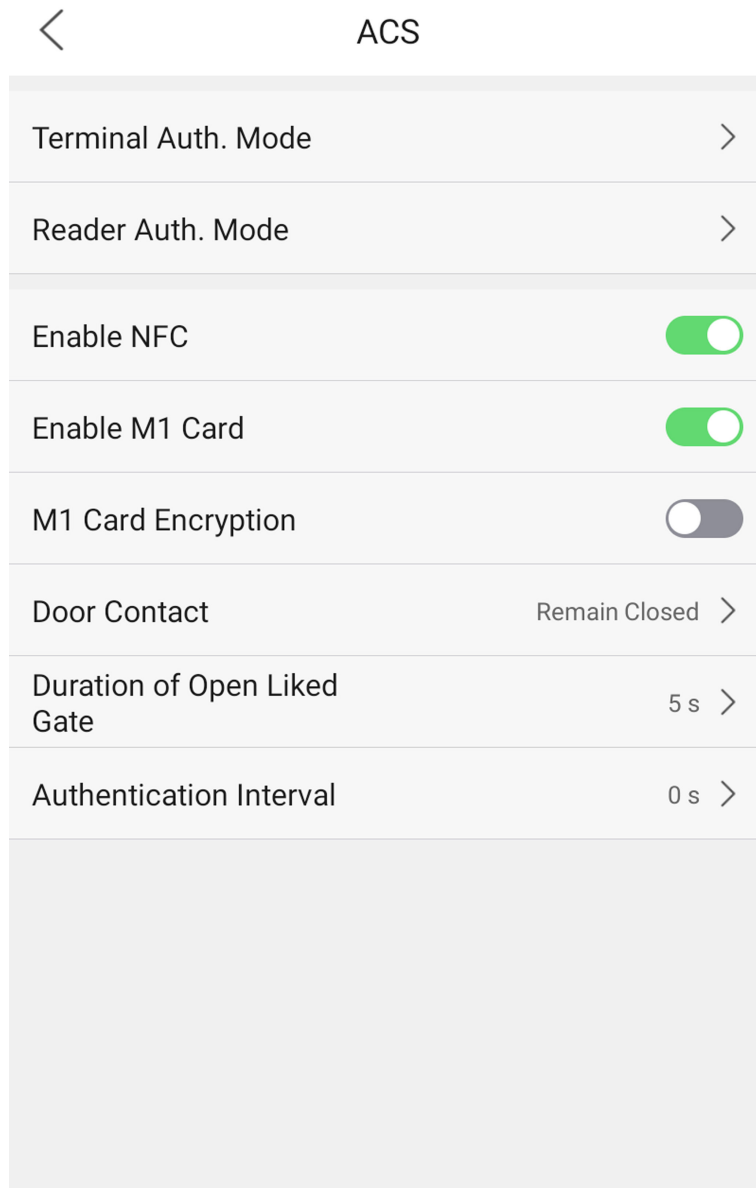


Figure 8-12 Access Control Parameters

8.9.3 Enable NFC Card

Enable NFC card function and you can present NFC card on the device to authenticate.

Steps

1. On the Home page, tap **ACS** (Access Control Settings) to enter the Access Control Settings page.

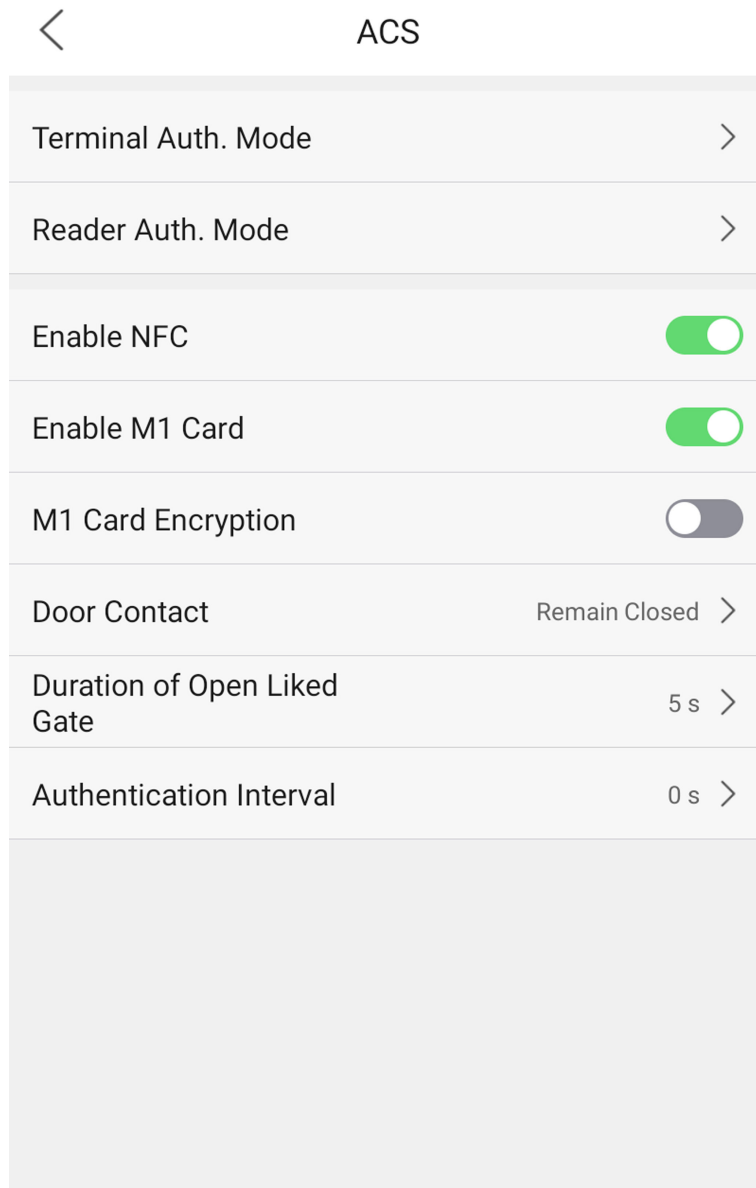


Figure 8-13 Access Control Parameters

2. Enable the function and you can present the NFC card to authenticate.

8.9.4 Enable M1 Card and M1 Card Encryption

Enable M1 card function and you can present M1 card on the device to authenticate. M1 card encryption can improve the security level of authentication.

Steps

1. On the Home page, tap **ACS** (Access Control Settings) to enter the Access Control Settings page.

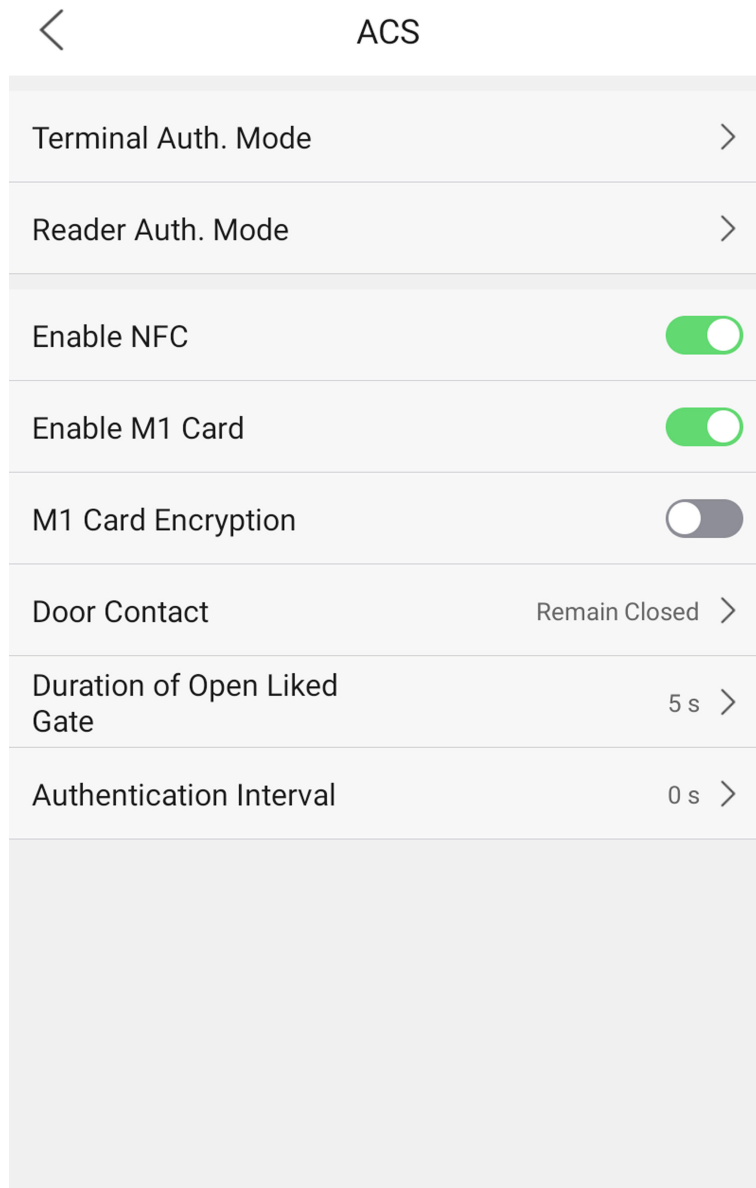


Figure 8-14 Access Control Parameters

2. Set the M1 card function.

Enable M1 Card

Enable the function and you can present the M1 card to authenticate.

M1 Card Encryption

Enable the function and set the sector ID.

 **Note**

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

8.9.5 Set Door Contact Parameters

If connecting a door contact, you should confirm the NO or NC connection method. Select remain open or remain closed according to actual NO/NC connection method.

On the Home page, tap **ACS** (Access Control Settings) to enter the Access Control Settings page. You can select "Remain Open" or "Remian Closed" according to your actual needs. By default, it is Remian Closed.

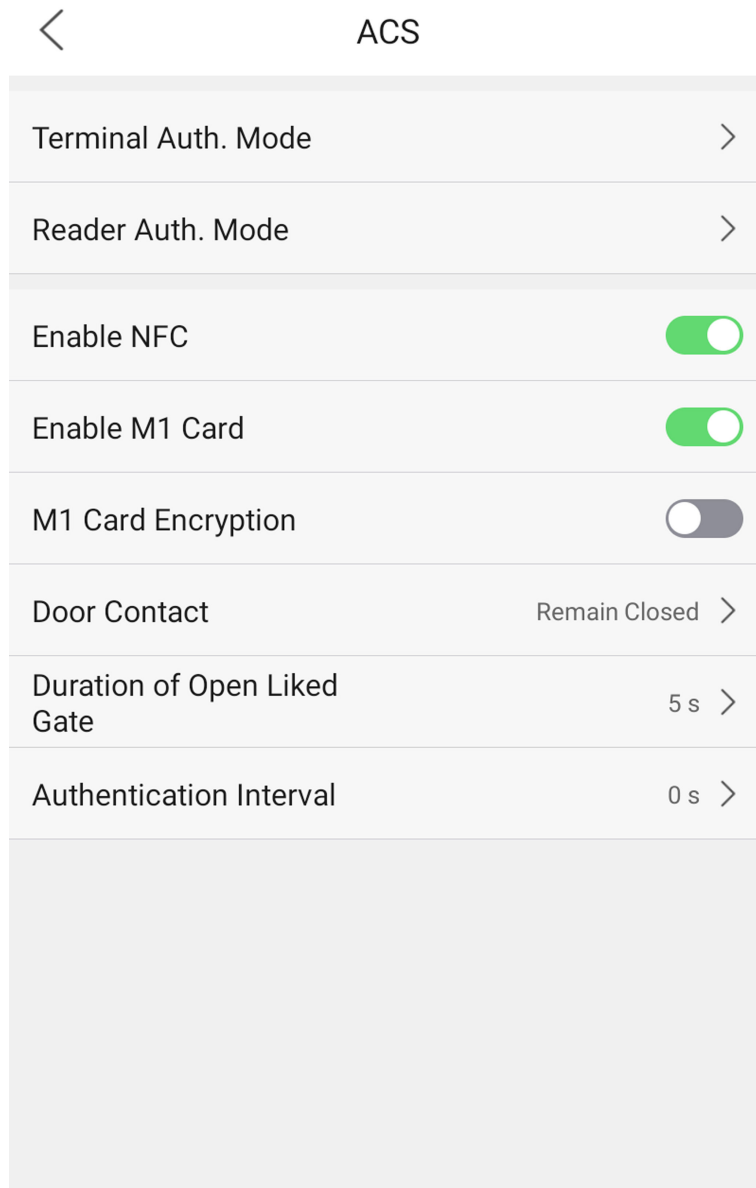


Figure 8-15 Access Control Parameters

8.9.6 Set Door Open Duration

Set the door unlocking duration.

On the Home page, tap **ACS** (Access Control Settings) to enter the Access Control Settings page. 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.

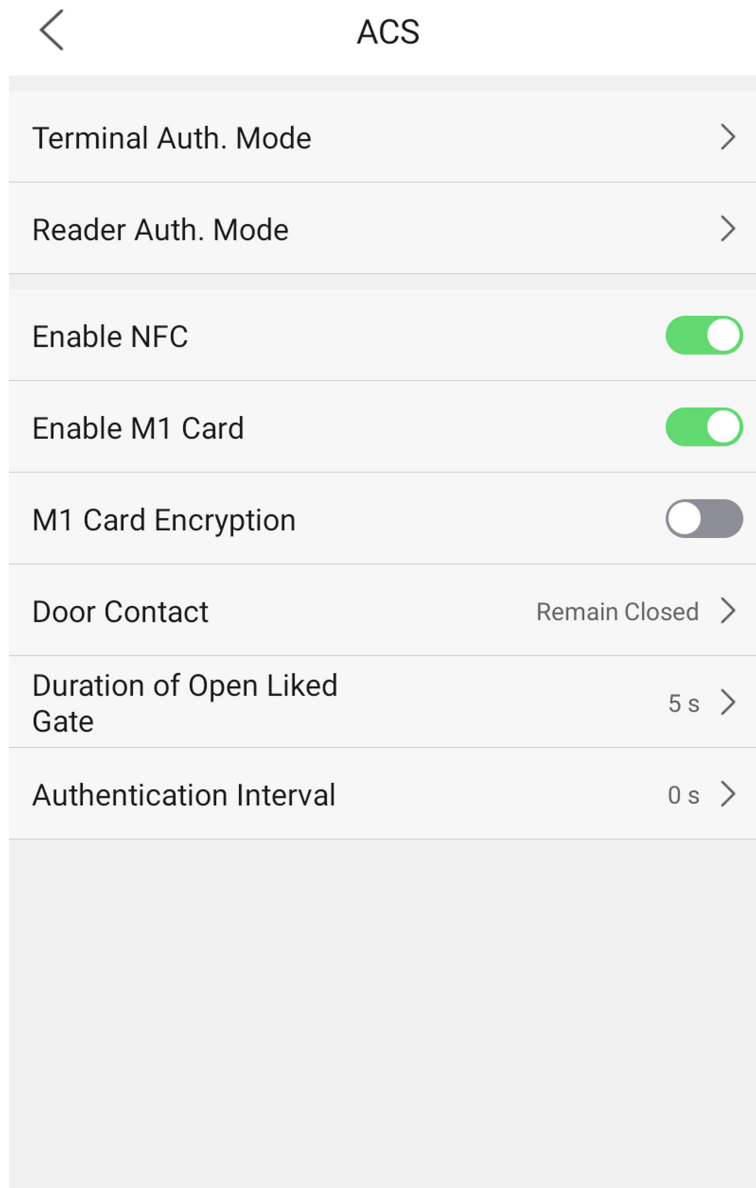


Figure 8-16 Access Control Parameters

8.9.7 Set Authentication Interval

Set the authentication interval between 2 authentications. Within the interval, the same person can authenticate only once.

On the Home page, tap **ACS** (Access Control Settings) to enter the Access Control Settings page. Set the authentication interval between 2 authentications. Within the interval, the same person can authenticate only once. Available authentication interval range: 0 to 65535.

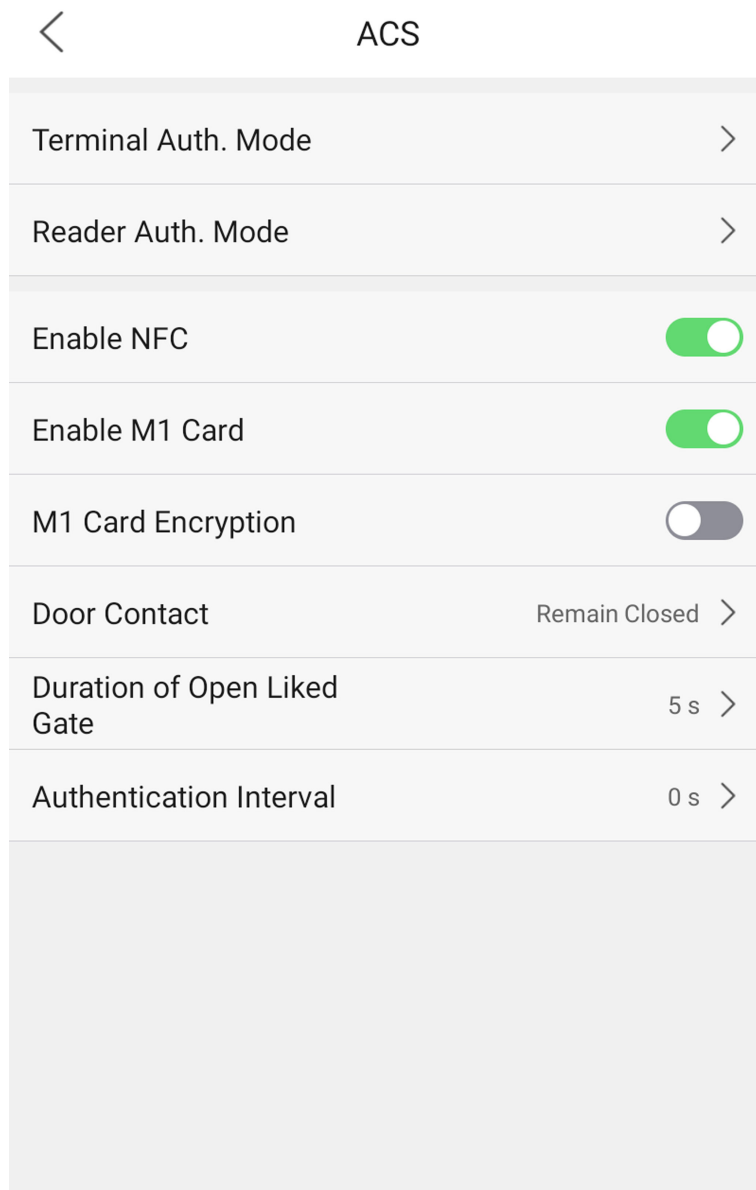


Figure 8-17 Access Control Parameters

8.10 Time and Attendance Status Settings

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

 **Note**

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

8.10.1 Disable Attendance Mode via Device

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

Tap **Attendance Status** to enter the Attendance Status page.

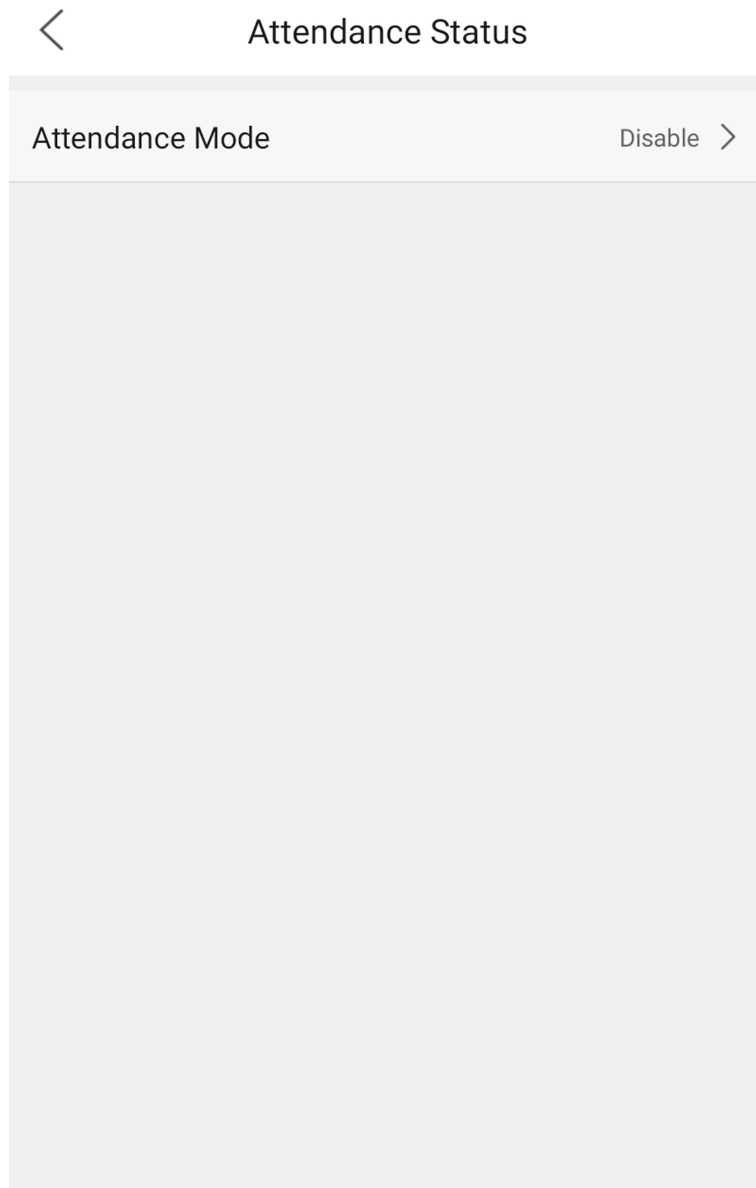


Figure 8-18 Disable Attendance Mode

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

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

8.10.2 Set Manual Attendance via Device

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

Before You Start

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

Steps

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

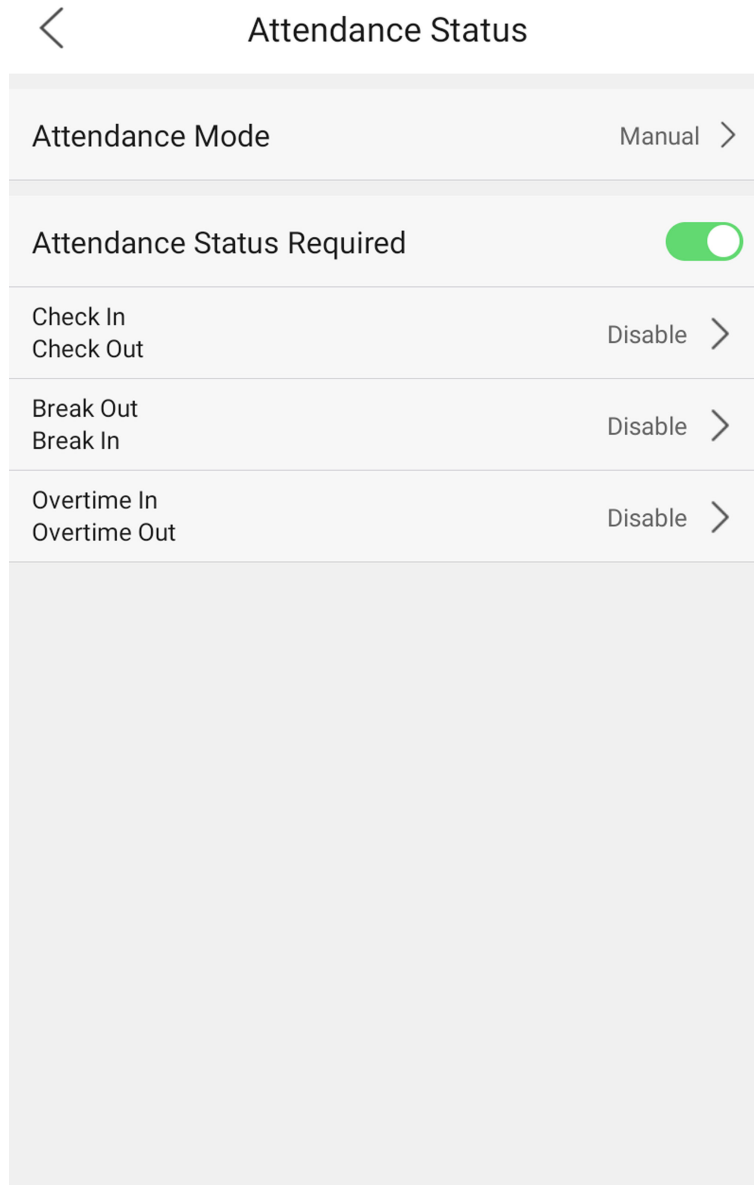


Figure 8-19 Manual Attendance Mode

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



The Attendance Property will not be changed.

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

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

Result

You should select an attendance status manually after authentication.



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

8.10.3 Set Auto Attendance via Device

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

Before You Start

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

Steps

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

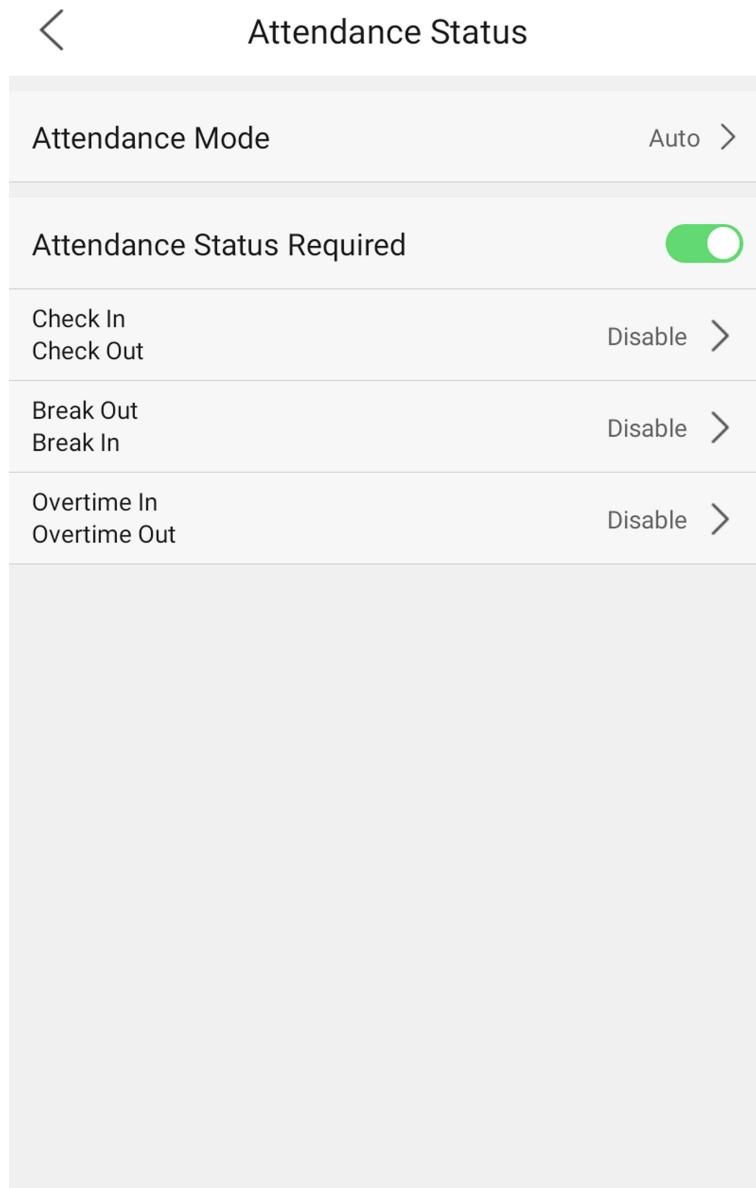


Figure 8-20 Auto Attendance Mode

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

 **Note**

The Attendance Property will not be changed.

5. **Optional:** Select an status and change its name if required.
The name will be displayed on the T & A Status page and the authentication result page.
6. Set the status' schedule.
 - 1) Tap **Attendance Schedule**.

- 2) Select **Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, or Sunday**.
- 3) Set the selected attendance status's start time of the day.
- 4) Tap **Confirm**.
- 5) Repeat step 1 to 4 according to your actual needs.



The attendance status will be valid within the configured schedule.

Result

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

Example

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

8.10.4 Set Manual and Auto Attendance via Device

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

Before You Start

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

Steps

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

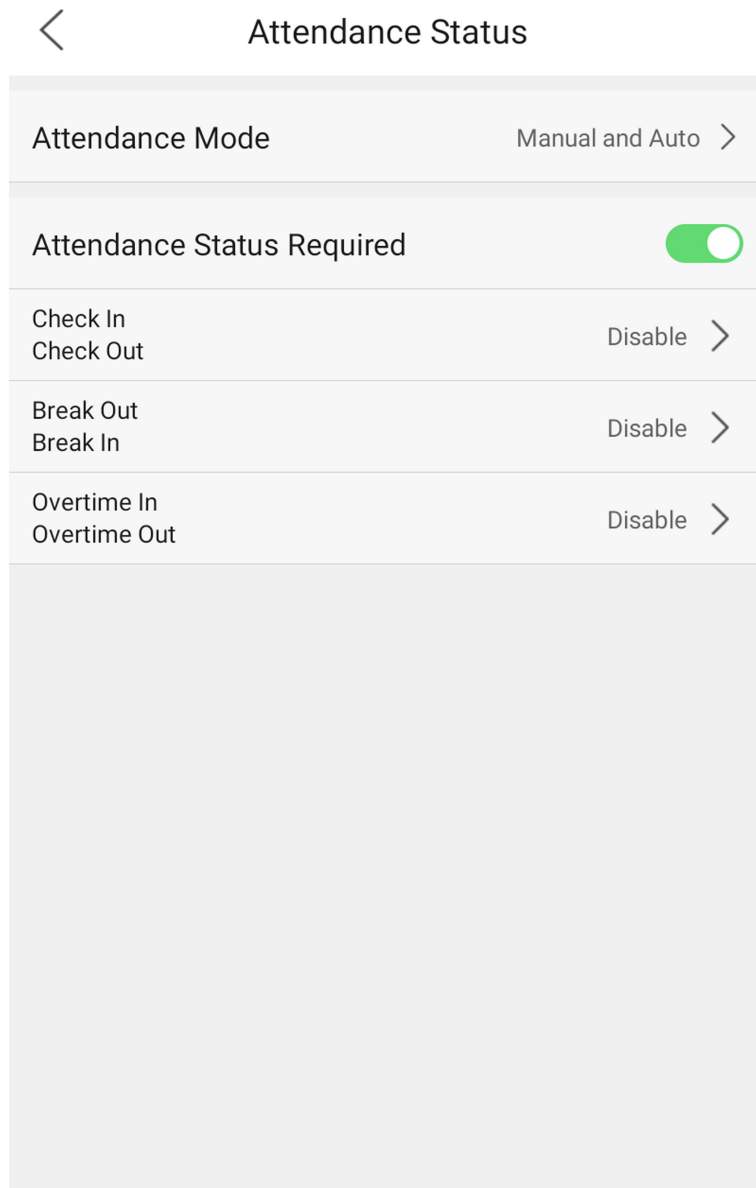


Figure 8-21 Manual and Auto Mode

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

 **Note**

The Attendance Property will not be changed.

5. **Optional:** Select an status and change its name if required.
The name will be displayed on the T & A Status page and the authentication result page.
6. Set the status' schedule.
 - 1) Tap **Attendance Schedule**.

- 2) Select **Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, or Sunday**.
- 3) Set the selected attendance status's start time of the day.
- 4) Tap **OK**.
- 5) Repeat step 1 to 4 according to your actual needs.



The attendance status will be valid within the configured schedule.

Result

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

Example

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

8.11 Preference Settings

Set interface style, theme, shortcut and control center.

8.11.1 Set Interface Style

You can configure the device interface to light or dark mode.

Steps

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

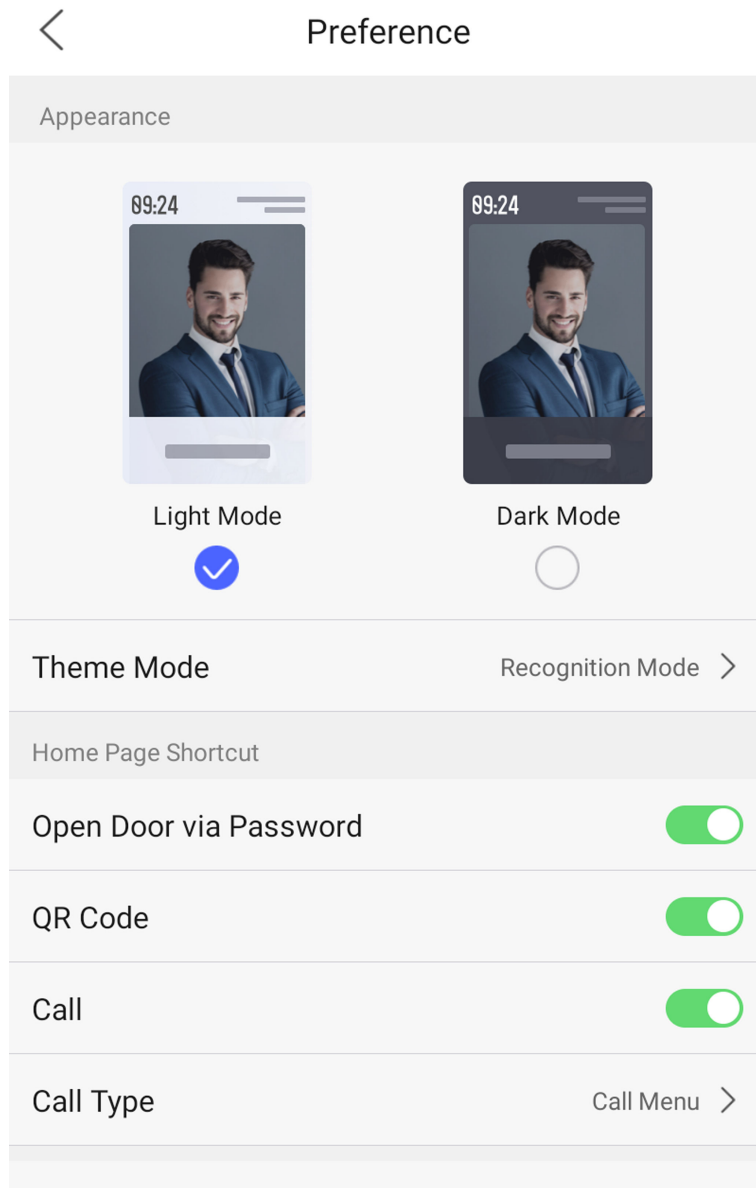


Figure 8-22 Preference Settings

2. You can set the interface style of the device as **Light Mode** or **Dark Mode**.

8.11.2 Set Theme Mode

You can set the theme mode to recognition or advertisement mode.

Steps

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

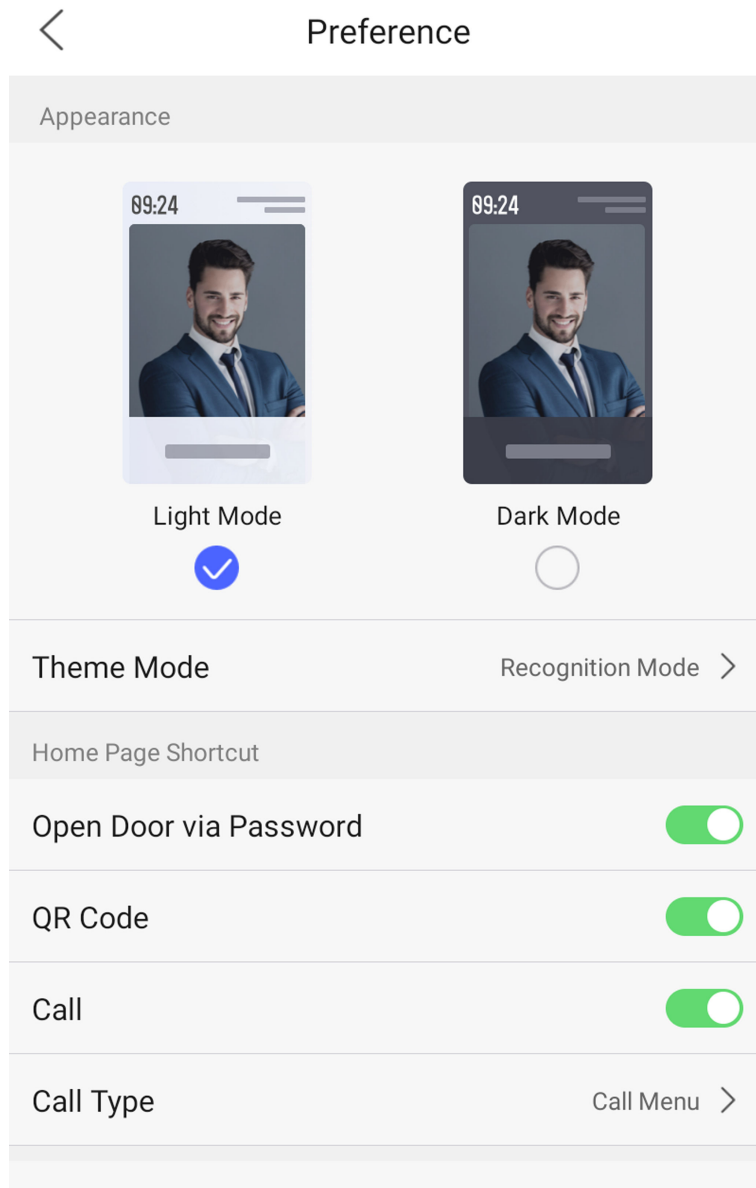


Figure 8-23 Preference Settings

2. You can set the theme of the prompt window on the authentication page. You can select **Theme Mode** as **Recognition Mode**, or **Advertisement Mode**.

Recognition 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.

Advertisement Mode

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

8.11.3 Set Authentication Page Shortcut

You can set the displayed shortcuts on authentication mode.

Steps

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

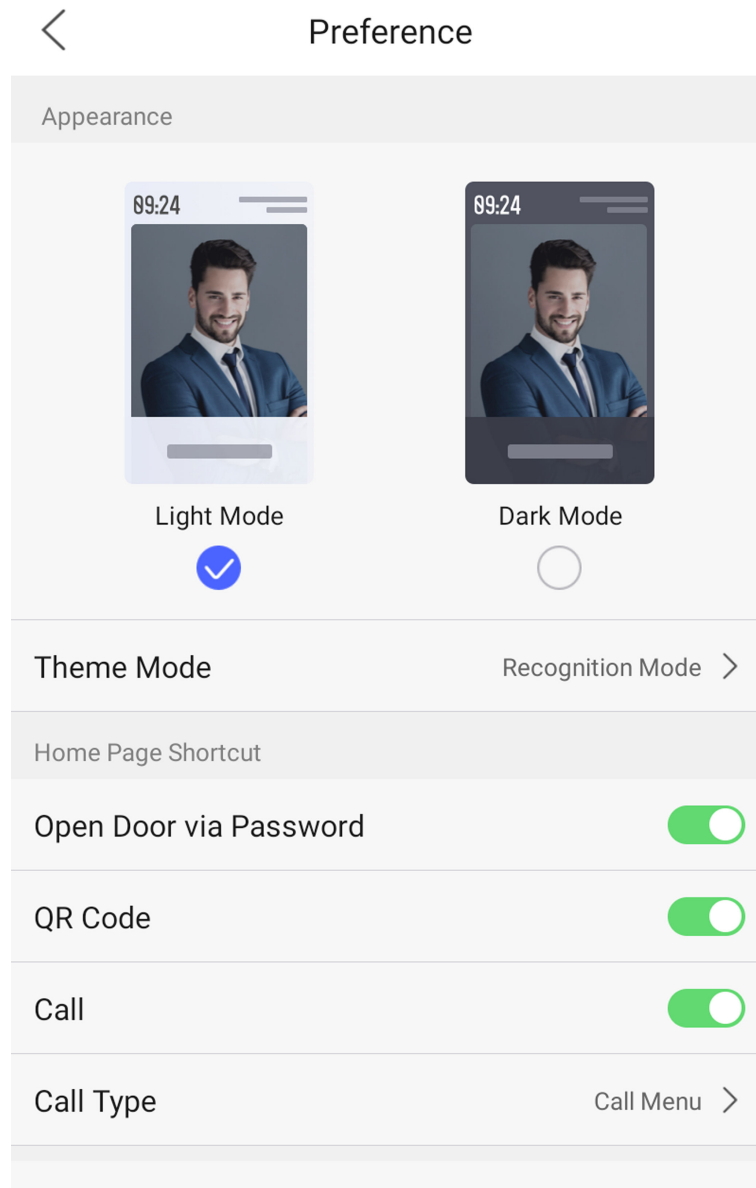


Figure 8-24 Preference Settings

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

Call

After enabling this function, you can select **Call Type** from the list of Call Menu, Call Center and Call Specific Room according to your needs.

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.

Open Door via Password

Enable this function and you can enter the PIN code to open the door.

8.11.4 Set Control Center Displayed Items

You can set the items that displayed in the control center.

Steps

1. Tap **Preference** to enter the preference settings page.
2. Set the control items displayed in the control center.

On the authentication page, use finger to pull down to enter the control center page to view the control items.

8.12 System Maintenance

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

8.12.1 View System Information

You can view the device system information.

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

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



Note

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

8.12.2 View Device Capacity

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

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

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



Note

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

8.12.3 Upgrade

Choose online upgrading or upgrading via the USB flash drive.

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

Choose one of the following upgrade methods to upgrade.

Online Update

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

Update via USB

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

8.12.4 View User Manual

View the device user manual.

Long tap on the initial page for 3 s and slide to the left/right by following the gesture. Login and tap **Maint. → User Manual** .

Scan the QR code to obtain and view the user manual.

8.12.5 Restore Parameters

Restore to default settings or restore to factory settings.

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

Restore to default settings or restore to factory settings.

Restore to Default Settings

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

Restore to Factory Settings

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

8.12.6 Reboot

Reboot device if needed.

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

Reboot the device.

8.12.7 Advanced Settings

You can set face parameters and view device version.

Steps

1. Long tap on the initial page for 3 s and slide to the left/right by following the gesture. Login and tap **Maint.** → **System Information** . Long tap ? on the right upper corner.
2. Enter the admin password.
3. Tap **Face Parameters**.

Face Parameter

Custom Anti-Spoofing Detection

Face Liveness Level

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

Anti-Spoofing Detection Threshold

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

Lock Face for Anti-Spoofing Protection

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

Lock Duration

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

4. Tap **Version Information** to view device version.

8.13 Video Intercom

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



8.13.1 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.



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.



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.

8.13.2 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.






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

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



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.

8.13.3 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.




8.13.4 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.
-

8.13.5 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.

8.13.6 Doorbell Call



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. Tap doorbell button to call.
 - 1) Tap  on the device initial page.
 - 2) Tap  to call.

Chapter 9 Quick Operation via Web Browser

9.1 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.



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

Click **Next** to complete the settings.

9.2 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.

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

9.3 Privacy Settings

Set the picture uploading and storage parameters.

Click  in the top right of the web page to enter the wizard page. After previous settings, you can click **Next** to enter the **Privacy Settings** page.

Picture Uploading and Storage

Save Picture When Authenticating

Save picture when authenticating automatically.

Upload Picture When Authenticating

Upload the pictures when authenticating to the platform automatically.

Save Registered Picture

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

Upload Picture After Linked Capture

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


Save Pictures After Linked Capture

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

Click **Next** to complete the settings.

9.4 Administrator Settings

Steps

1. Click  in the top right of the web page to enter the wizard page. After setting device language, time, environment and privacy, you can click **Next** to enter the **Administrator Settings** 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.

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

9.5 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 System Network** settings page.

2. Set the device type.

If set the device type as **Door Station** or **Outer Door Station**, you can set the **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.

3. Set **Registration Password**, **Main Station IP** and **Private Server IP**.

4. **Optional:** Click to **Enable Protocol 1.0**.

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

Chapter 10 Operation via Web Browser

10.1 Login

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




Make sure the device is activated. For detailed information about activation, see [Activation](#) .

Login via Web Browser

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

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

Login via Remote Configuration of Client Software

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

10.2 Forgot Password

If you forget the device password, you can change the device password via security questions.

Steps



You can change the device password via PC web.

1. Click **Forgot Password** on the login page.
 2. Select the verification method.
 3. Answer the reserved security questions.
-



The answers are configured when you first activate the device.

4. Create a new password and confirm the password.
5. Click **Next** to save the settings.

10.3 Live View

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

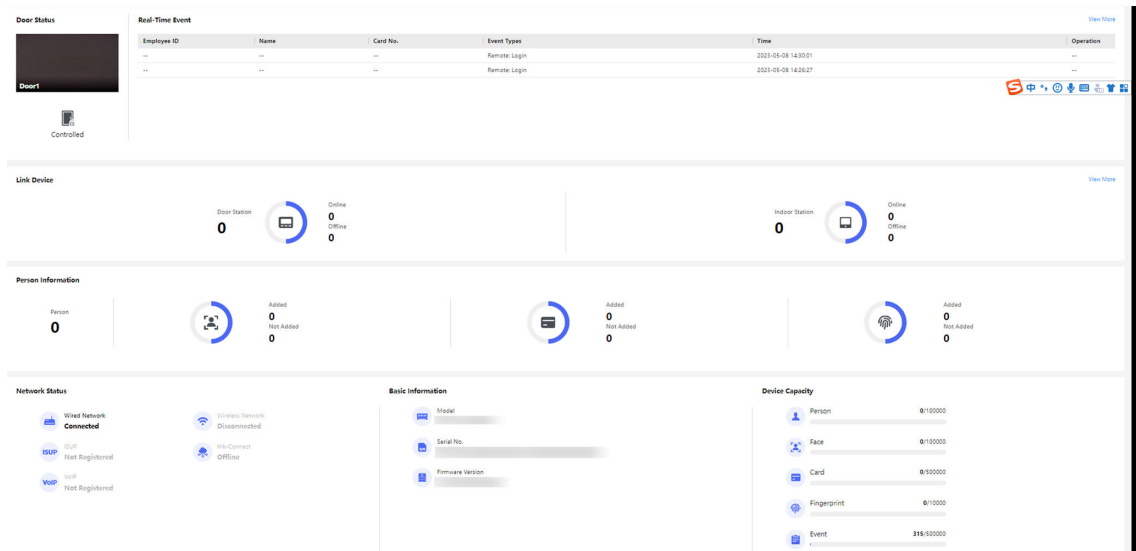


Figure 10-1 Live View Page

Function Descriptions:

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.

Door Status

Click  to view the device live view.



Set the volume when starting live view.



Note

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



You can capture image when starting live view.



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



Full screen view.



You can record when starting live view.



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

Controlled Status

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

Link Device

You can view the quantity and status of linked devices.



Note

You can click **View More** to [*Device Management*](#) .

Person Information

You can view the added and not added information of person face and card.

Network Status

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

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.

10.4 Person Management

Add person's basic information, permission, credentials, room No., and authentication type.

10.4.1 Add Person Basic Information

Add the person's basic information, including the employee ID, the person's name, the gender, person type and the person's organization.

Steps

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

Basic Information

*Employee ID

Name

Gender Male Female Unknown

Person Type Normal User Visitor Person in Blocklist

Long-Term Effective User

Validity Period -

Administrator

Certificate Configuration

Face ⓘ 200 allowed. No larger than JPG, JPEG, PNG KB.

+ Add from Device

+ Upload

Card ⓘ Up to 50 cards can be supported.

+ Add Card

Authentication Settings

Authentication Type Same as Device Custom

Figure 10-2 Add Person

2. Add the person's basic information, including the employee ID, the person's name, person type, the person's organization, etc.
3. **Optional:** If you select **Visitor** as the person type, you can set the visit times.
4. Click **Save**.

10.4.2 Set Permission Duration

Set the person's permission duration.

Steps

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

Basic Information

*Employee ID

Name

Gender Male Female Unknown

Person Type Normal User Visitor Person in Blocklist

Long-Term Effective User

Validity Period -

Administrator

Certificate Configuration

Face ⓘ 200 allowed. No larger than JPG, JPEG, PNG KB.

+ Add from Device

+ Upload

Card ⓘ Up to 50 cards can be supported.

+ Add Card

Authentication Settings

Authentication Type Same as Device Custom

Figure 10-3 Add Person

2. Enable **Long-Term Effective User** and the person will have the configured permission permanently. Or set **Validity Period** and the person can only has the permission within the configured time period according to your actual needs.
3. Click **Save**.

10.4.3 Add Face Picture

Add face picture for a person.

Steps

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

Basic Information

*Employee ID

Name

Gender Male Female Unknown

Person Type Normal User Visitor Person in Blocklist

Long-Term Effective User

Validity Period -

Administrator

Certificate Configuration

Face ⓘ 200 allowed. No larger than JPG, JPEG, PNG KB.

+ Add from Device

+ Upload

Card ⓘ Up to 50 cards can be supported.

+ Add Card

Authentication Settings

Authentication Type Same as Device Custom

Figure 10-4 Add Person

2. Click + on the right 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 K.

3. Click **Save**.

10.4.4 Add Card

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

Steps

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

Basic Information

*Employee ID

Name

Gender Male Female Unknown

Person Type Normal User Visitor Person in Blocklist

Long-Term Effective User

Validity Period -

Administrator

Certificate Configuration

Face ⓘ 200 allowed. No larger than JPG, JPEG, PNG KB.

+ Add from Device

+ Upload

Card ⓘ Up to 50 cards can be supported.

+ Add Card

Authentication Settings

Authentication Type Same as Device Custom

Figure 10-5 Add Person

2. Click Add Card.

3. Enter **Card No.** and select a **Property**.
4. Click **OK** to add the card.



Note

Up to 5 cards can be added.

5. Click **Save**.

10.4.5 Add Fingerprint

Add fingerprint for a person.

Steps

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

Basic Information

*Employee ID

Name

Gender Male Female Unknown

Person Type Normal User Visitor Person in Blocklist

Long-Term Effective User

Validity Period -

Administrator

Certificate Configuration

Face ⓘ 200 allowed. No larger than JPG, JPEG, PNG KB.

+ Add from Device

+ Upload

Card ⓘ Up to 50 cards can be supported.

+ Add Card

Authentication Settings

Authentication Type Same as Device Custom

Figure 10-6 Add Person

2. Click **Add Fingerprint**, and press your finger on the fingerprint module of the device to add your fingerprint.



Note

Only devices supporting the fingerprint function can add the fingerprint.

3. Click **Save**.

10.4.6 Add Room No.

Add a room No. for the person.

Steps

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

Basic Information

*Employee ID

Name

Gender Male Female Unknown

Person Type Normal User Visitor Person in Blocklist

Long-Term Effective User

Validity Period -

Administrator

Certificate Configuration

Face ⓘ 200 allowed. No larger than JPG, JPEG, PNG KB.

+ Add from Device

+ Upload

Card ⓘ Up to 50 cards can be supported.

+ Add Card

Authentication Settings

Authentication Type Same as Device Custom

Figure 10-7 Add Person

2. Click **Add** to add a device. Enter the **Room No.** and **Floor No.** of the device.



Note

Take floor 1, room 1 as an example, the room No. should be 1-1-1-1 (Community-Building-Unit-Room).

3. Click **Save**.

10.4.7 Set Authentication Type

Set the person's authentication type as same as device or custom. If you set as **Same as Device**, the person will follow the device's authentication mode. If you set as **Custom**, the person will follow his/her own authentication mode.

Steps

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

Basic Information

*Employee ID

Name

Gender Male Female Unknown

Person Type Normal User Visitor Person in Blocklist

Long-Term Effective User

Validity Period -

Administrator

Certificate Configuration

Face ⓘ 200 allowed. No larger than JPG, JPEG, PNG KB.

+ Add from Device

+ Upload

Card ⓘ Up to 50 cards can be supported.

+ Add Card

Authentication Settings

Authentication Type Same as Device Custom

Figure 10-8 Add Person

2. Set Authentication Type as Same as Device or Custom.

Same as Device

If you want to select **Same as Device**, you should set the terminal authentication mode first. For details, see [Set Authentication Mode](#).

Custom

You can select an authentication mode according to your actual needs.

3. Click **Save**.

10.5 Search Event

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

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

The results will be displayed on the right panel.

10.6 Device Management


You can manage the linked device on the page.

Steps



1. Click **Device Management** to enter the settings page.



Figure 10-9 Device Management

2. Click **Add** to add the indoor station or sub door station. Enter the parameters and click **Save** to add.
3. Click **Import** to download the template. Enter the information of the device in the template and click  to import the template.
4. Click **Export** to export the information to the PC.
5. Select the device and click **Delete** to remove the selected device from the list.
6. Click **Refresh** to get the device information.

7. Optional: Set Device Information.

- Edit Device Information** Click  to edit device information.
- Delete Device Information** Click  to delete device information from the list.
- Search Devices** Select **Status** and **Device Type** to search devices.

10.7 Configuration

10.7.1 View Device Information

View the device name, language, model, serial No., version, IO input, IO OUTPUT, Lock, Local RS-485, register number, alarm input, alarm output, and device capacity, etc.

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

You can view device name, language, model, serial No., version, IO input, IO output, Lock, Local RS-485, register number, alarm input, alarm output, and device capacity, etc.

10.7.2 Set Time

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

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

10.7.3 Change Administrator's Password

Steps

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



Caution

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

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

10.7.4 Account Security Settings

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 **Configuration** → **System** → **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.

10.7.5 View Device Arming/Disarming Information

View device arming type and arming IP address.

Click **Configuration** → **System** → **User Management** → **Arming/Disarming Information** .

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

10.7.6 Network Settings

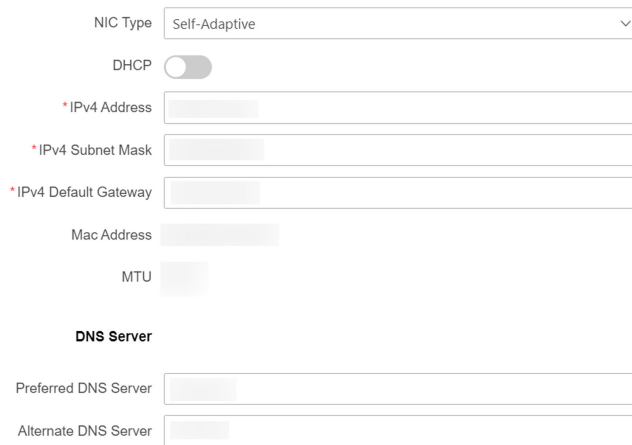
Set TCP/IP, port, Wi-Fi parameters, ISUP, and platform access.

Note

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

Set Basic Network Parameters

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



The screenshot shows the TCP/IP Settings page with the following fields and controls:

- NIC Type:** A drop-down menu currently set to "Self-Adaptive".
- DHCP:** A toggle switch that is currently turned off.
- *IPv4 Address:** A text input field.
- *IPv4 Subnet Mask:** A text input field.
- *IPv4 Default Gateway:** A text input field.
- Mac Address:** A text input field.
- MTU:** A text input field.
- DNS Server:** A section header for the following two fields:
 - Preferred DNS Server:** A text input field.
 - Alternate DNS Server:** A text input field.

Figure 10-10 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 **Self-Adaptive**.

DHCP

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

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 **Configuration** → **Network** → **Network Settings** → **Wi-Fi** .



Figure 10-11 Wi-Fi Settings Page

2. Check **Wi-Fi**.
3. Select a Wi-Fi
 - Click **Connect** of a Wi-Fi in the list and enter the Wi-Fi password.
 - Click **Manual Add** and enter a Wi-Fi's SSID, working mode, security mode, and password. Click **OK**.
4. 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. Set the DNS server. Set the preferred DNS server and alternate DNS server. Or enable **DHCP** and the system will allocate the preferred DNS server and alternate DNS server automatically.
6. Click **Save**.

Set Mobile Data

Set the mobile data parameters for the device .

Note

The function should be supported by the device models.

Click **Configuration** → **Network** → **Network Settings** → **Mobile Data** .

Enable Mobile Data

If the device supports mobile data function, you can enable it.

Dialing Mode/Dialing No.

Select the dialing mode as **Manual**. And set the dialing No.

User Name/Password/APN

If you need, you can set the user name, password and APN for mobile number.

Bluetooth Settings

You can enable bluetooth function.

Open

Enable **Open** to enable the bluetooth function.

Device Name

You can edit the device name connected to the bluetooth.

Open Door via Bluetooth

After enabling this function, you can open doors via Hik-Connect app.

Set Port Parameters

Set the HTTP, HTTPS, HTTP Listening, RTSP and Server port parameters.

Click **Configuration** → **Network** → **Network Service** → **HTTP(S)** .

HTTP

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

HTTPS

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

HTTP Listening

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



Note

The event alarm IP address or domain name should support the HTTP protocol/HTTPS protocol to receive the alarm information.

Click **Configuration** → **Network** → **Network Service** → **RTSP** .

RTSP

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

Click **Configuration** → **Network** → **Device Access** → **SDK Server** .

SDK Server

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

Platform Access

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

Steps

1. Click **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 server IP address, and verification code.

Note

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

5. Enable **Video Encryption**, and create the password and confirm it.

Note

After adding the device to APP, you need to enter the video encryption password to live view the device.

6. **Optional:** Click **View** to view the device QR code. Scan the QR code to account.

Note

Scan the QR code before it loses efficacy.

7. **Optional:** Click **More** to set the network connection priority.
 - 1) Enable **WLAN** or **Wired Network** according to your actual needs.
 - 1) Hold and drag ☰ to adjust the access priority.
8. Click **Save** to enable the settings.

Set ISUP Parameters

Set the ISUP parameters for accessing device via ISUP protocol.

Steps

Note

The function should be supported by the device.

1. Click **Configuration** → **Network** → **Device Access** → **ISUP** .
 2. Check **Enable**.
 3. Select the ISUP version and Server IP Address, Port, Device ID, and you can view the Register status.
-

Note

If you select 5.0 as the version, you should set the Encryption Key and Network Connection Priority as well. You can click **More** and check **WLAN** or **Wired Network** to adjust the network priority.

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**.

SIP Setting

Steps

1. Click **Configuration** → **Network** → **Device Access** → **SIP** to enter the settings page.
2. Check **Enable VOIP Gateway**.
3. Configure the SIP parameters.
4. Click **Save** to enable the settings.

10.7.7 Set Video and Audio Parameters

Set the image quality and resolution.

Set Video Parameters

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

Stream Type: **Main Stream** | Sub-stream | Third Stream

Video Type: Video Stream Video&Audio

Resolution: 1280*720P

Bit Rate Type: Variable Constant

Video Quality: Medium

Frame Rate: 25 fps

*Max. Bitrate: 2048 Kbps

Video Encoding: H.264

*I Frame Interval: 50

Save

Figure 10-12 Video Settings Page

Set the stream type, the video type, the resolution, the bitrate type, the Max. bitrate, and I Frame Interval.

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

Stream Type: **Main Stream** | Sub-stream | Third Stream

Audio Encoding: G.711uLaw

Input Volume: 7

Output Volume: 7

Save

Figure 10-13 Audio Settings

Set the stream type, input volume, output volume and enable voice prompt according to your actual needs.

Click **Save** to save the settings.

10.7.8 Set Image Parameters

You can adjust the image parameters, video parameters, supplement parameters, backlight, image fusion and capture interval.

Steps

1. Click **Configuration** → **Image** .
2. Configure the parameters to adjust the image.

Video Adjust(Video Standard)

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

PAL

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

NTSC

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

Image Adjustment

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

LED Light Parameters

Set the supplement light type, mode, start time and end time. You can also set the brightness.

Backlight

Enable or disable the WDR function.

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

Image Fusion

When the environment is dark, you can select **Automatic** to enable the image fusion function. The live view page will display the fusion image. And you can also set the sensitivity.

Select **Disable** to disable the function.

Capture Interval

You can select the capture interval according to your actual needs.

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

10.7.9 Alarm Settings

Set the alarm output parameters.

Steps

1. Click **Configuration** → **Event** → **Alarm Settings** → **Alarm Output** .
2. Set **Alarm Name** and **Output Delay**.

10.7.10 Access Control Settings

Set Authentication Parameters

Set authentication related parameters, such as enable authentication function, select authentication mode, etc.

View Device Information

View the device or the card reader's information.

Steps

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



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

2. Select **1** or **2** to view the terminal type and model. They are read-only.



1 refers to the device and 2 refers to the connected card reader.

Set Authentication Mode

Select an authentication mode for the device or the connected card reader according to your actual needs. People will authenticate follow the configuration.

Steps

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



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

2. Select Terminal **1** or Terminal **2**.



1 refers to the device and 2 refers to the connected card reader.

3. Enable **Enable Authentication Device** to enable the authentication function.
4. Select an authentication mode from the drop-down list. The device (terminal 1) or the card reader (terminal 2) will apply the configured authentication mode. People authentication should follow the configured authentication mode.
5. Click **Save**.

Set Multiple People Authentication

Multiple people can be authenticated at the same time.

Steps

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



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

2. Select Terminal **1**.
-



1 refers to the device and 2 refers to the connected card reader.

3. Enable **Enable Authentication Device** to enable the authentication function.
4. Enable **Multiple People Authentication**. Multiple people can be authenticated at the same time.
5. Click **Save**.

Set Authentication Interval

Set the device's authentication interval of the same person when authenticating.

Steps

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



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

2. Select Terminal **1**.
-



1 refers to the device and 2 refers to the connected card reader.

3. Enable **Enable Authentication Device** to enable the authentication function.
4. 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.
5. Click **Save**.

Set Alarm of Max. Failed Attempts

The device will report alarm when the authentication attempts reach the set value.

Steps

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



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

2. Select Terminal 1.
-



1 refers to the device and 2 refers to the connected card reader.

3. Enable **Enable Authentication Device** to enable the authentication function.
 4. Enable **Alarm of Max. Failed Attempts** and set the Max. value. The device will report alarm when the authentication attempts reach the set value.
 5. Click **Save**.
-

Enable Tampering Detection

Enable the anti-tamper detection for the device or the connected card reader. The device will report alarm if an tampering event is triggered.

Steps

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



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

2. Select Terminal 1 or Terminal 2.
-



1 refers to the device and 2 refers to the connected card reader.

3. Enable **Enable Authentication Device** to enable the authentication function.
 4. Enable **Tampering Detection**. The device will report alarm if an tampering event is triggered.
 5. Click **Save**.
-

Set Card No. Reversing

The device's or the connected card reader's reading sequence of card No. will be in reverse sequence after enabling the function.

Steps

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



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

2. Select Terminal 1 or Terminal 2.
-

Note

1 refers to the device and 2 refers to the connected card reader.

3. Enable **Enable Authentication Device** to enable the authentication function.
4. Set **Card No. Reversing**. The read card No. will be in reverse sequence after enabling the function.
5. Click **Save**.

Set Sub Card Reader Position

If the device has connected to a card reader, you can select sub card reader position as different or same side as the main device.

Steps

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

Note

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

2. Select Terminal **2**.

Note

1 refers to the device and 2 refers to the connected card reader.

3. Enable **Enable Authentication Device** to enable the authentication function.
4. Select sub card reader position as different or same side as the main card reader.
5. Click **Save**.

Set Face Recognition Interval

You can set the interval between 2 continuous recognition of a same person during the authentication.

Steps

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

Note

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

2. Select Terminal **1** or Terminal **2**.

Note

1 refers to the device and 2 refers to the connected card reader.

3. Enable **Enable Authentication Device** to enable the authentication function.
4. Set **Continuous Face Recognition Interval**. You can set the interval between 2 continuous recognition of a same person during the authentication. In the configured interval, Person A can

only recognized once. If another person (Person B) has recognized during the interval, Person A can recognized again.

5. Click **Save**.

Set Communication Duration between Device and Card Reader

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

Steps

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



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

2. Select Terminal **2**.
-



1 refers to the device and 2 refers to the connected card reader.

3. Enable **Enable Authentication Device** to enable the authentication function.
4. Set **Communication with Controller Every**. When the device cannot connect with the card reader for longer than the set time, the card reader will turn offline automatically.
5. Click **Save**.

Set Max. Interval When Entering Password

Set Max. interval when entering password. When you entering the password on the card reader, if the interval between pressing 2 digits is longer than the set value, the digits you pressed before will be cleared automatically.

Steps

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



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

2. Select Terminal **2**.
-



1 refers to the device and 2 refers to the connected card reader.

3. Enable **Enable Authentication Device** to enable the authentication function.
4. Set **Max. Interval When Entering Password**. When you entering the password on the card reader, if the interval between pressing 2 digits is longer than the set value, the digits you pressed before will be cleared automatically.
5. Click **Save**.

Set OK LED Polarity/Error LED Polarity

Set OK LED Polarity/Error LED Polarity of the connected card reader according to the actual card reader parameters. Generally, adopts the default settings.

Steps

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



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

2. Select Terminal **2**.
-



1 refers to the device and 2 refers to the connected card reader.

3. Enable **Enable Authentication Device** to enable the authentication function.
4. Set OK LED Polarity/Error LED Polarity of the access control device according to the actual card reader parameters. Generally, adopts the default settings.
5. Click **Save**.

Set Door Parameters

Set door related parameters.

Set Door No. and Name

If the device has connected to different door locks, you can select the door No. and set door name to distinguish.

Steps

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

Door No.

Door Name

Open Duration s

Door Open Timeout Alarm s

Door Magnetic Sensor Type Remain Closed Remain Open

Exit Button Type Remain Closed Remain Open

Door Lock Powering Off Status Remain Closed Remain Open

Extended Open Duration s

Door Remain Open Duration with ... min

Duress Code

Super Password

Figure 10-14 Door Parameters Settings Page

2. Select the device corresponded door No. and create a name for the door.
3. Click **Save**.

Set Door Open Duration

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

Steps

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

Door No.

Door Name

Open Duration s

Door Open Timeout Alarm s

Door Magnetic Sensor Type Remain Closed Remain Open

Exit Button Type Remain Closed Remain Open

Door Lock Powering Off Status Remain Closed Remain Open

Extended Open Duration s

Door Remain Open Duration with ... min

Duress Code

Super Password

Figure 10-15 Door Parameters Settings Page

2. Set the door unlocking duration. If the door is not opened for the set time, the door will be locked.
3. Click **Save**.

Set Door Open Timeout Alarm

Set door open timeout alarm and an alarm will be triggered if the door has not been closed within the configured time duration.

Steps

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

Door No. 1

Door Name

Open Duration 5 s

Door Open Timeout Alarm 30 s

Door Magnetic Sensor Type Remain Closed Remain Open

Exit Button Type Remain Closed Remain Open

Door Lock Powering Off Status Remain Closed Remain Open

Extended Open Duration 15 s

Door Remain Open Duration with ... 10 min

Duress Code

Super Password

Figure 10-16 Door Parameters Settings Page

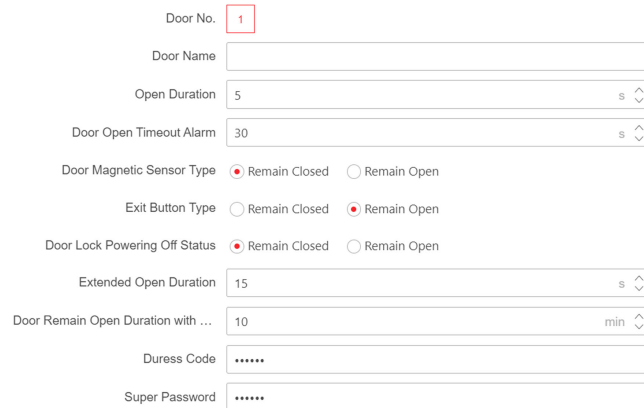
2. Set door open timeout alarm and an alarm will be triggered if the door has not been closed within the configured time duration.
3. Click **Save**.

Set Door Contact

If the device has connected with door contact, you can set the door contact to remain open or closed according to actual wiring.

Steps

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



Door No. 1

Door Name

Open Duration 5 s

Door Open Timeout Alarm 30 s

Door Magnetic Sensor Type Remain Closed Remain Open

Exit Button Type Remain Closed Remain Open

Door Lock Powering Off Status Remain Closed Remain Open

Extended Open Duration 15 s

Door Remain Open Duration with ... 10 min

Duress Code *****

Super Password *****

Figure 10-17 Door Parameters Settings Page

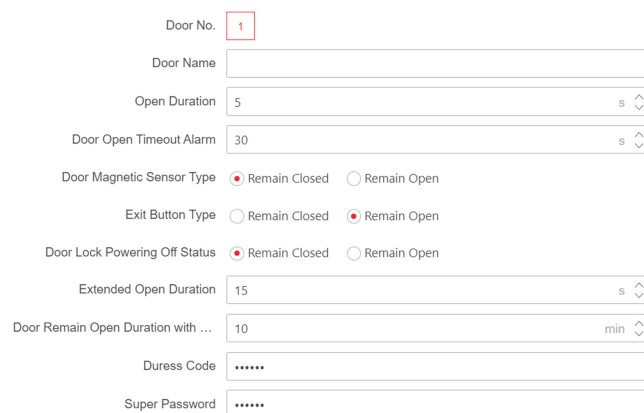
2. Set **Door Magnetic Sensor Type**. You can set the door contact as **Remain Open** or **Remain Closed** according to your actual needs. By default, it is **Remain Closed**.
3. Click **Save**.

Set Exit Button Type

If the device has connected to an exit button, you can set the exit button as remain open or closed according to actual wiring.

Steps

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



Door No. 1

Door Name

Open Duration 5 s

Door Open Timeout Alarm 30 s

Door Magnetic Sensor Type Remain Closed Remain Open

Exit Button Type Remain Closed Remain Open

Door Lock Powering Off Status Remain Closed Remain Open

Extended Open Duration 15 s

Door Remain Open Duration with ... 10 min

Duress Code *****

Super Password *****

Figure 10-18 Door Parameters Settings Page

2. Set **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**.
3. Click **Save**.

Set Door Lock Powering Off Status

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

Steps

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

Door No. 1

Door Name

Open Duration 5 s

Door Open Timeout Alarm 30 s

Door Magnetic Sensor Type Remain Closed Remain Open

Exit Button Type Remain Closed Remain Open

Door Lock Powering Off Status Remain Closed Remain Open

Extended Open Duration 15 s

Door Remain Open Duration with ... 10 min

Duress Code

Super Password

Figure 10-19 Door Parameters Settings Page

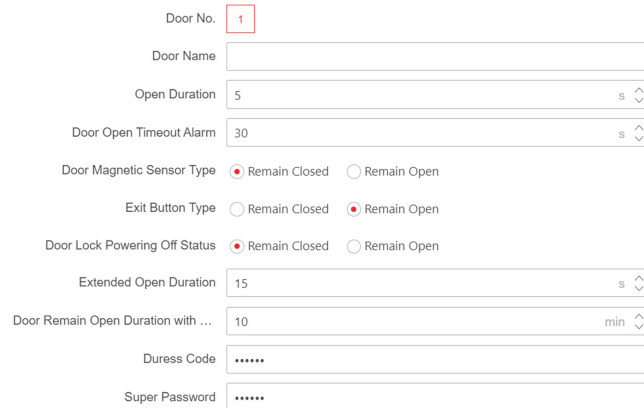
2. Set **Door Lock Powering Off Status**. You can set the door lock status when the door lock is powering off. By default, it is **Remain Closed**.
3. Click **Save**.

Set Extended Open Duration

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

Steps

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



Door No. 1

Door Name

Open Duration 5 s

Door Open Timeout Alarm 30 s

Door Magnetic Sensor Type Remain Closed Remain Open

Exit Button Type Remain Closed Remain Open

Door Lock Powering Off Status Remain Closed Remain Open

Extended Open Duration 15 s

Door Remain Open Duration with ... 10 min

Duress Code *****

Super Password *****

Figure 10-20 Door Parameters Settings Page

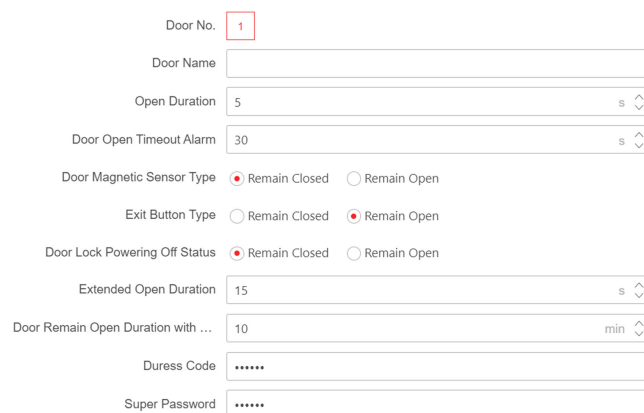
2. Set **Extended Open Duration**. The door contact can be enabled with appropriate delay after person with extended access needs authenticating her/his credentials.
3. Click **Save**.

Set 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.

Steps

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



Door No. 1

Door Name

Open Duration 5 s

Door Open Timeout Alarm 30 s

Door Magnetic Sensor Type Remain Closed Remain Open

Exit Button Type Remain Closed Remain Open

Door Lock Powering Off Status Remain Closed Remain Open

Extended Open Duration 15 s

Door Remain Open Duration with ... 10 min

Duress Code *****

Super Password *****

Figure 10-21 Door Parameters Settings Page

2. 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.
3. Click **Save**.

Set Duress Code/Super Password

The door can open by inputting the duress code when there is duress. And the specific person can open the door by inputting the super password.

Steps

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

Door No. 1

Door Name

Open Duration 5 s

Door Open Timeout Alarm 30 s

Door Magnetic Sensor Type Remain Closed Remain Open

Exit Button Type Remain Closed Remain Open

Door Lock Powering Off Status Remain Closed Remain Open

Extended Open Duration 15 s

Door Remain Open Duration with ... 10 min

Duress Code

Super Password

Figure 10-22 Door Parameters Settings Page

2. Set duress code or super password.

Duress Code

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

Super Password

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

3. Click **Save**.

Set RS-485 Parameters

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

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

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**.



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.



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/Stop Bit/Parity/Flow Control/Communication Mode

Set the paramters according to your actual needs.

Set Wiegand Parameters

You can set the Wiegand transmission direction.

Steps



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

1. Click **Configuration** → **Access Control** → **Wiegand Settings** .
2. Check **Wiegand** to enable the Wiegand function.
3. Set a transmission direction.

Input

The device can connect a Wiegand card reader.

Output

The can connect an external access controller. And the two devices will transmit the card No. via Wiegand 26 or 34.

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



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

Elevator Control

Steps

1. Click **Configuration** → **Access Control** → **Elevator Control Parameters** .

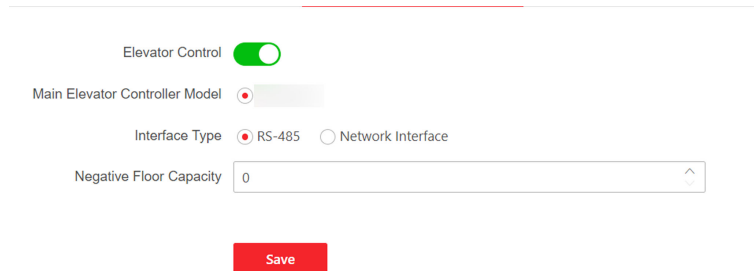


Figure 10-23 Access Control and Elevator Control

2. Click to enable **Elevator Control**.
3. Set the elevator parameters.

Elevator No.

Select an elevator No.

Main Elevator Controller Model

Select an elevator controller.

Interface Type

If you select **RS-485**, make sure you have connected the device to the elevator controller with RS-485 wire.

If you select **Network Interface**, enter the elevator controller's IP address, port No., user name, and password for communication.

Negative Floor Capacity

Set the negative floor number.



Note

- Up to 4 elevator controllers can be connected to 1 device.
 - Up to 10 negative floors can be added.
 - Make sure the interface types of elevator controllers, which are connected to the same device, are consistent.
-

Set Terminal Parameters

You can set terminal parameters for accessing.

- Click **Configuration** → **Access Control** → **Terminal Parameters** .

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

You can enable **Remote Verification** according to your actual needs. After enabling, you can verify remotely.

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

10.7.11 Video Intercom Settings

Set Video Intercom Parameters

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

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

If set the device type as **Door Station**, you can set the floor No., door station No., and click **More** to set **Community No.**, **Building No.**, and **Unit No.** You can press any digit button to enter the calling page, and enter the room No. and press call button to call the resident.

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

Device Type	Door Station ▼
Period No.	1
Building No.	1
Unit No.	1
Floor No.	1 ▼
Door Station No.	0
Community No.	0

Save

Figure 10-24 Device No. Settings

Device Type

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



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.



- 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.



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

If set the device type as **Outer Door Station**, you can set outer door station No., and community No. You can press call button to enter the calling page, and enter **【Community No. + Building No. + # + Unit No. + # + Room No.】** and press call button to call resident.

Outer Door Station No.

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



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

Community No.

Set the device community No.

Session Settings

Enable the communication between door station, main station, and video intercom server.

Steps

1. Click **Configuration** → **Intercom** → **Session Settings** to enter the settings page.
2. Set registration password, main station IP, private server IP and enable Protocol 1.0.

Registration Password

Create a registration password for communication via SIP

Main Station IP

IP address of the main station.

Private Server IP

Enter the IP address of the device that need to communicate via SIP. The device will be the SIP server. Other devices should register to the SIP server, or the video intercom between devices will be failed.

Enable Protocol 1.0

After enabling, the device is registered to the main station through the previous protocol. If disabled, the device is registered to the main station through the new protocol.

3. Click **Save**.

Time Duration Settings

Set the Max. call duration.

Go to **Configuration** → **Intercom** → **Call Settings** .

Drag the block to set the Max. call duration. Click **Save**.



The Max. call duration range is 90 s to 120 s.

Press Button to Call

Steps

1. Click **Intercom** → **Press Button to Call** to enter the settings page.
2. Set the parameters.
 - Check **Call Management Center**, **Specified Indoor Station**, **Indoor Station** or **APP** to set the button.



If you check **Call Specified Indoor Station**, you should enter the specified indoor station No.

Number Settings

You can call the room SIP to call the room.

Steps

1. Click **Configuration** → **Intercom** → **Number Settings** to enter the settings page.
2. Click **+ Add**, enter the **Room No.** and **SIP**.
3. Click **Save**.

10.7.12 Card Settings

Set Card Security

Click **Configuration** → **Card Settings** → **Card Type** to enter the settings page.

Set the parameters and click **Save**.

Enable NFC Card

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

Enable M1 Card

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

M1 Card Encryption

Sector

M1 card encryption can improve the security level of authentication.

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

Enable EM Card

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

Enable DESFire Card

The device can read the data from DESFire card when enabling the DESFire card function.

DESFire Card Read Content

The device can read the DESFire card content.

Enable FeliCa Card

The device can read the data from FeliCa card when enabling the FeliCa card function.

Set Card No. Authentication Parameters

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

Go to **Configuration** → **Card Settings** → **Card No. Authentication Settings** .

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

Full Card No.

All card No. will be read.

Wiegand 26 (3 bytes)

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

Wiegand 34 (4 bytes)

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

10.7.13 Platform Attendance

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

Set Manual Attendance via Web

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

Before You Start

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

Steps

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

Note

The Attendance Property will not be changed.

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

Result

You should select an attendance status manually after authentication.

Note

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

Set Auto Attendance via Web

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

Before You Start

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

Steps

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



The Attendance Property will not be changed.

5. **Optional:** Select an status and change its name if required.
6. Set the status' schedule. Refers to for details.

Set Manual and Auto Attendance via Web

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

Before You Start

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

Steps

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



The Attendance Property will not be changed.

5. **Optional:** Select an status and change its name if required.
6. Set the status' schedule. Refers to for details.

Result

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

Example

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

10.7.14 Set Privacy Parameters

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

Go to **Configuration → Security → Privacy Settings**

Event Storage Settings

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

Delete Old Events Periodically

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

Delete Old Events by Specified Time

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

Overwriting

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

Authentication Settings

Display Authentication Result

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

Name De-identification

You can check **Name De-identification**, and the whole name will not be displayed.

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.

Clear All Pictures in Device



All pictures cannot be restored once they are deleted.

Clear Registered Face Pictures

All registered pictures in the device will be deleted.

Clear Captured Pictures

All captured pictures in the device will be deleted.

10.7.15 Set Biometric Parameters

Set face parameters of the device, such as enable face anti-spoofing, set live face security level, recognition distance, etc.

Enable Face Anti-spoofing

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

Steps

1. Click **Configuration** → **Smart** → **Smart** .
-



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

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

Set Live Face Detection Security Level

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

Steps

1. Click **Configuration** → **Smart** → **Smart** .

Note

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

2. After enabling the face anti-spoofing function, you can set the matching security level when performing live face authentication. The higher the level, the more strict the authentication.
3. Click **Save**.

Face Duplicate Check

You can check face duplicate when you import face data.

Steps

1. Click **Configuration** → **Smart** → **Smart**
2. Enable **Face Duplicate Check**. After enabling this function, you can check face duplicate when you import face data.

Set Recognition Distance

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

Steps

1. Click **Configuration** → **Smart** → **Smart** .
-

Note

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

2. Select the distance between the authenticating user and the device camera.
3. Click **Save**.

Set Face Pitch Angle

Set the maximum pitch angle when starting face authentication.

Steps

1. Click **Configuration** → **Smart** → **Smart** .
-

Note

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

2. The maximum pitch angle when starting face authentication.
3. Click **Save**.

Set Yaw Angle

The maximum yaw angle when starting face authentication.

Steps

1. Click **Configuration** → **Smart** → **Smart** .
-



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

2. Set the maximum yaw angle when starting face authentication.
3. Click **Save**.

Set Face Picture Quality Grade for Applying

Set face picture quality grade for applying according to your needs.

Steps

1. Click **Configuration** → **Smart** → **Smart** .
-



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

2. Set face picture quality grade for applying according to your needs. The higher the threshold, the higher the requirement for image quality. If the image applying fails, the threshold or image quality can be adjusted according to actual needs.
3. Click **Save**.

Set 1: 1 Face Picture Grade Threshold

Set 1: 1 face picture grade threshold according to your needs.

Steps

1. Click **Configuration** → **Smart** → **Smart** .
-



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

2. Set 1: 1 face picture grade threshold according to your needs. The higher the threshold, the higher the quality requirement for the captured images of the front facing camera, and it is easy to prompt authentication failure.
-



The default threshold is 0, which can be used. Setting the threshold too high will intercept images and cause authentication failure.

3. Click **Save**.

Set Face 1:1/1:N Threshold

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

Steps

1. Click **Configuration** → **Smart** → **Smart** .
-



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

2. Set the face matching threshold when authenticating via 1:1 or 1:N matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate.
3. Click **Save**.

Set Face Recognition Timeout Value

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

Steps

1. Click **Configuration** → **Smart** → **Smart** .
-



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

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

Set ECO Mode

After enabling the ECO mode, the device will use the IR camera to authenticate faces in the low light or dark environment.

Steps

1. Click **Configuration** → **Smart** → **Smart** .
-



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

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

ECO Mode Threshold

The larger the value, the device enter the ECO Mode easier.

ECO Mode (1:1)

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

ECO Mode (1:N)

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

3. Click **Save**.

Set Face without Mask Detection

After enabling the face without mask detection, the system will recognize the face with mask or not.

Steps

1. Click **Configuration** → **Smart** → **Smart** .



Note

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

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

Face without Mask Detection

None

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

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.

Face with Mask 1:N Matching Threshold

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.

Face with Mask & Face (1:1 ECO)

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

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

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

3. Click **Save**.

Set Recognition Area

Set the recognition area on the device screen.

Steps

1. Click **Configuration → Smart → Area Configuration** .



Note

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

2. Drag the yellow frame in the live video or enter values for the left, right, top, and bottom margin to adjust the recognition area. Only the face within the area can be recognized by the system.
3. Click **Save**.

10.7.16 Set Open Platform

If the device supports HEOP protocol, you can upload the third-party application to the device from this page.

Before You Start

Make sure the device contains the HEOP program.

Steps

1. Click **Configuration → Open Platform** .


2. If it is the first time to use the function, you should read the Disclaimer and make sure that the application you want to install fit the following conditions.

- Each application has its own exclusive name.
- The FLASH memory space that the application takes up is less than the available FLASH memory space of the device.
- The memory and computing power of the application is less than that available memory and computing power of the device.

3. **Optional:** You can enable **Developer Mode**.

Note

After obtaining the license certificate, you can enable **Developer Mode** and import third-party applications for ADB debugging.

- Click  and select the imported application package from your local computer.
- Click **Import** to complete the installation.

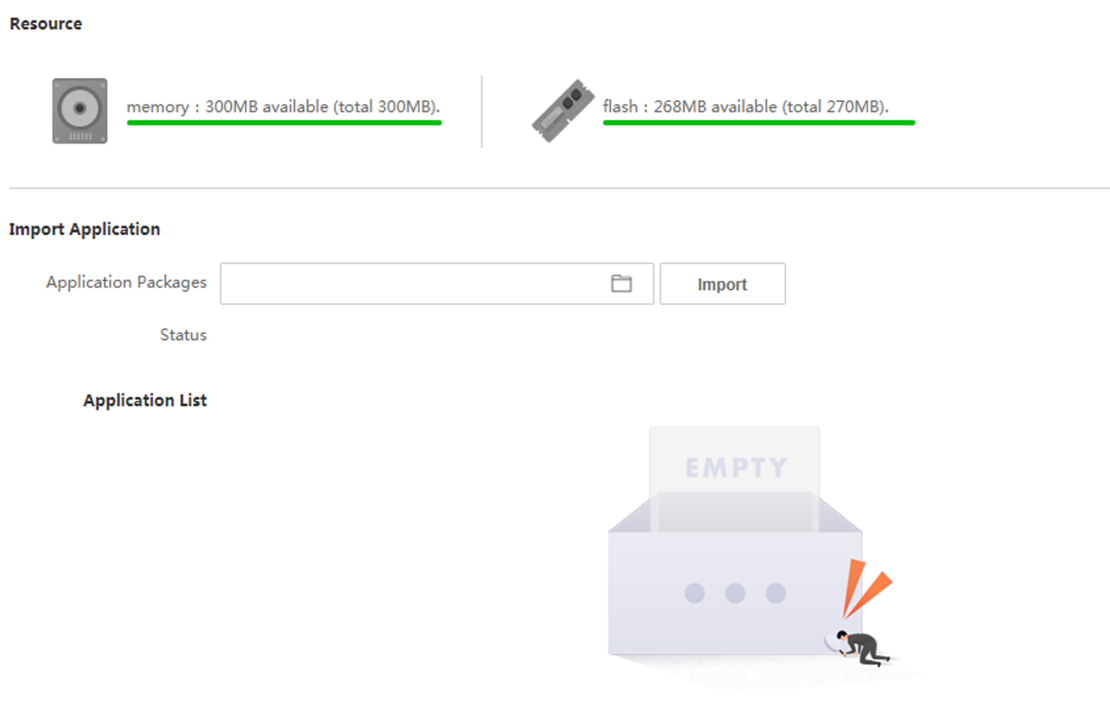







Figure 10-25 Open Platform

The installed applications and their related information are displayed in **Application List**, such as application name, operation, version, memory used, flash used, company, status and license.

- Import license.
 - If the application package has a license, click the application name on the navigation on the left. Click **Browse** and select the license file from your local computer. Click **Import**.
 - If the application package has a license, click  → **Browse** and select a license file from your local computer. Click **Import**.
 - If the application package does not have a license, enter <https://partner.hikvision.com/tpp> in the web browser to get a license.
- 7. Optional:** Set other functions.
 -  Enable or disable the application.
 -  Export log.
 - Set permission.

-  Delete the application.
-  View and upload license.

10.7.17 Preference Settings

Set the theme, notice publication, prompt schedule, custom prompt, and authentication result text.

Set Screen Display

You can set the display theme and the sleep time for the device.

Click **Configuration** → **Preference** → **Screen Display** .

Sleep

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

Display Theme

You can select display theme for device authentication. You can select **Theme Mode** as **Advertisement** or **Authenticate**.

Notice Publication

You can set the notice publication for the device.

Click **Configuration** → **Preference** → **Notice Publication** .

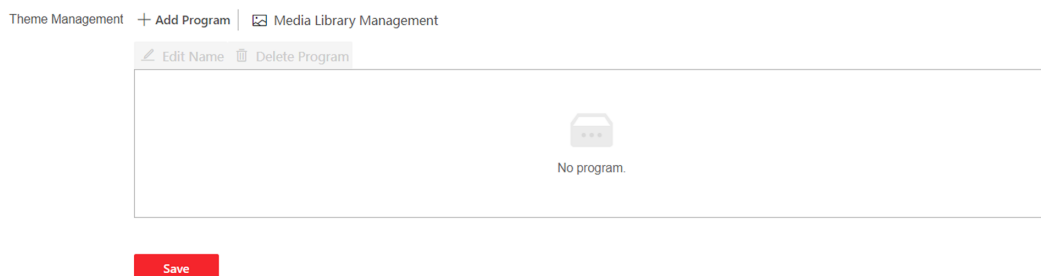


Figure 10-26 Notice Publication

Theme Management

Click **Media Library Management** → **+** to upload the picture from the local PC.

You can click **+**, and set **Name** and **Type** to create a theme. After creating the theme, click **+** in the **Theme Management** panel to select pictures in the media library. Click **OK** to add pictures to the theme.

Customize Audio Content


Customize the output audio content when authentication succeeded and failed.

Steps

1. Click **Configuration** → **Video/Audio** → **Prompt** .
2. Set the appellation.
3. Enable the function.
4. Set the time duration when authentication succeeded.
 - 1) Click **Add**.
 - 2) Set the time duration and the language.


Note

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

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

Note

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

- 3) Enter the audio content.
- 4) **Optional**: Repeat substep 1 to 3.
- 5) **Optional**: Click  to delete the configured time duration.
6. **Optional**: Import custom prompt.
 - 1) Select **Custom Type**.
 - 2) Select the importing path, and click **Import**.
7. Click **Save** to save the settings.

Customize Prompt Voice

You can customize prompt voices for the device.

Steps

1. Click **Configuration** → **Preference** → **Custom Prompt** .

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



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

Configure Authentication Result Text

Steps

1. Go to **Configuration** → **Preference** → **Authentication Result Text** .
2. Enable **Customize Authentication Result Text**.
3. Enter custom texts.
4. Click **Save**.

10.7.18 Upgrade and Maintenance

Reboot device, restore device parameters, upgrade device version, and set advanced face parameters.


Reboot Device

Click **Maintenance and Security** → **Maintenance** → **Restart** .

Click **Restart** to reboot the device.

Upgrade

Click **Maintenance and Security** → **Maintenance** → **Upgrade** .

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

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



Do not power off during the upgrading.

Restore Parameters

Click **Maintenance and Security** → **Maintenance** → **Backup and Reset** .

Restore All

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

Restore

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

Import and Export Parameters

Click **Maintenance and Security** → **Maintenance** → **Backup and Reset** .

Export

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



Note

You can import the exported device parameters to another device.

Import

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

Click **Advanced Settings**, and enter the admin password.

Face Parameter

Custom Anti-Spoofing Detection

Face Liveness Level

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

Anti-Spoofing Detection Threshold

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

Lock Face for Anti-Spoofing Protection

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

Lock Duration

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

Version Information

You can view the device information.

10.7.19 Device Debugging

You can set device debugging parameters.

Steps

1. Click **Maintenance and Security** → **Maintenance** → **Device Debugging** .
2. You can set the following parameters.

Enable SSH

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

Print Log

You can click **Export** to export log.

Capture Network Packet

You can set the **Capture Packet Duration**, **Capture Packet Size**, and click **Start Capture** to capture.

10.7.20 Log Query

You can search and view the device logs.

Go to **Maintenance and Security → 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.

10.7.21 Security Mode Settings

Set the security mode for logging in the client software.

On the Device for Management page, click **Maintenance and Security → Security → Security Service** .

Select a security mode, and click **Save**.

Security Mode

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

Compatible Mode

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

Illegal Login Lock

After enabling **Illegal Login Lock**, the device will be locked if it is logged in illegally.

10.7.22 Certificate Management

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



Note

The function is only supported by certain device models.

Create and Install Self-signed Certificate

Steps

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

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

The certificate will be saved automatically.

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

Install Other Authorized Certificate

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

Steps

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

Install CA Certificate

Before You Start

Prepare a CA certificate in advance.

Steps

1. Go to **Maintenance and Security → Security → Certificate Management** .
2. Create an ID in the **Import CA Certificate** area.



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

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

Chapter 11 Other Platforms to Configure

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

iVMS-4200 Client Software

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

https://pinfo.hikvision.com/hkwsen/unzip/20230109110406_14606_doc/UD31348B_iVMS-4200%20AC%20Client_User%20Manual_V1.9.0_PDF1-TEST_en-US_20221226.PDF

HikCentral Access Control (HCAC)

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

https://pinfo.hikvision.com/hkwsen/unzip/20230207191241_72415_doc/index.html

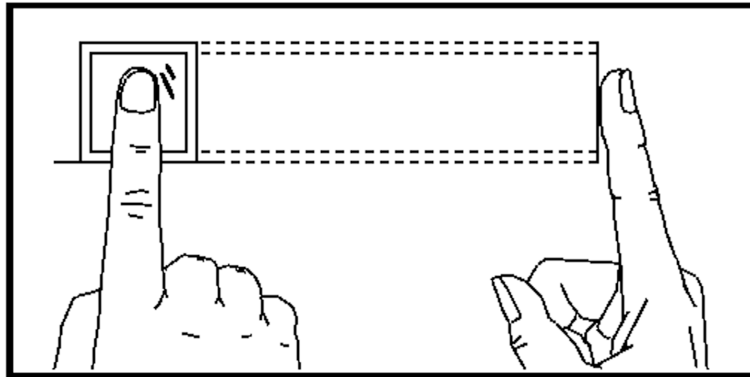
Appendix A. Tips for Scanning Fingerprint

Recommended Finger

Forefinger, middle finger or the third finger.

Correct Scanning

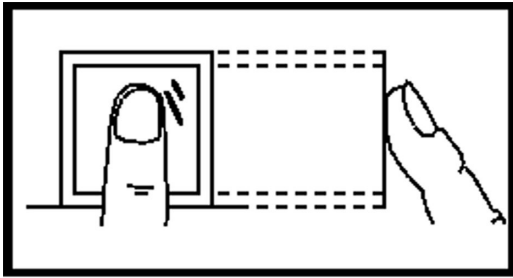
The figure displayed below is the correct way to scan your finger:



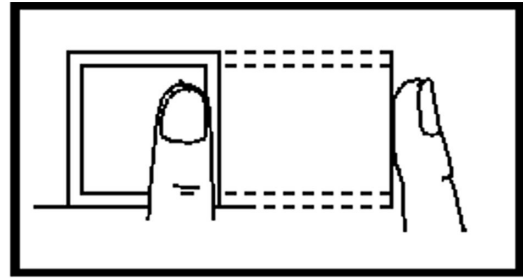
You should press your finger on the scanner horizontally. The center of your scanned finger should align with the scanner center.

Incorrect Scanning

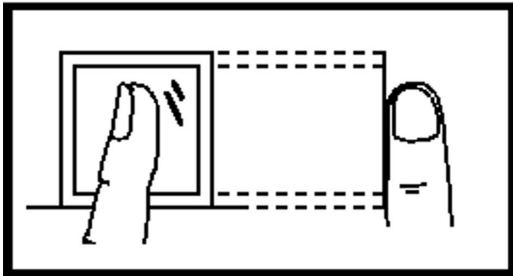
The figures of scanning fingerprint displayed below are incorrect:



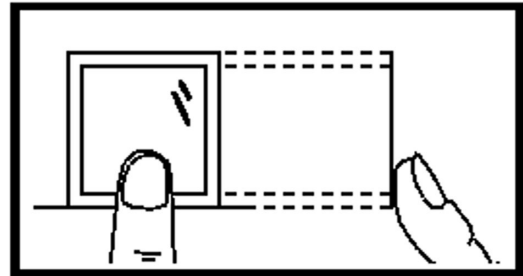
Vertical



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

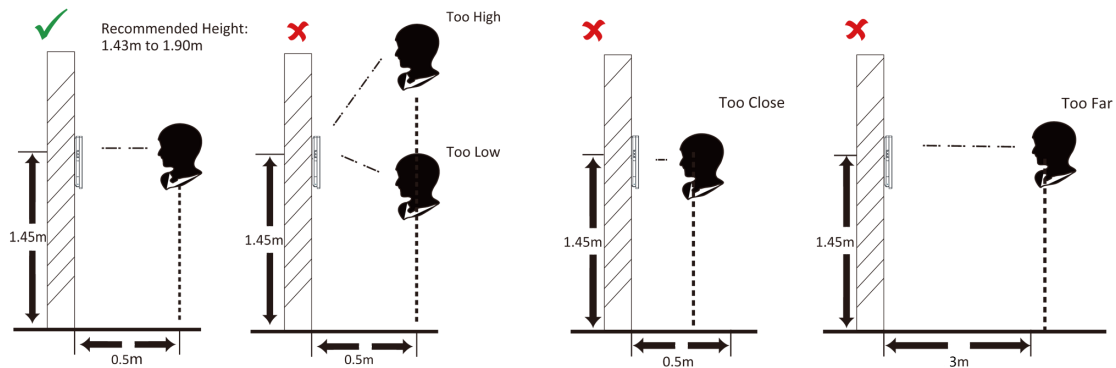
If your fingerprint is shallow, or it is hard to scan your fingerprint, we recommend you to use other authentication methods.

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.

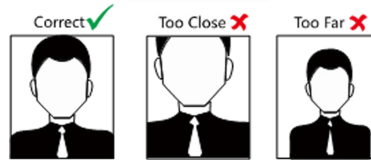
Posture

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

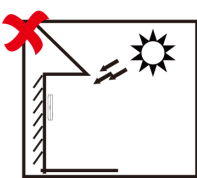


Bulb: 100~850Lux

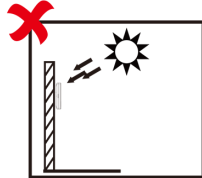


Sunlight: More than 1200Lux

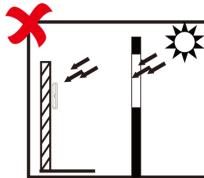
2. Avoid backlight, direct and indirect sunlight



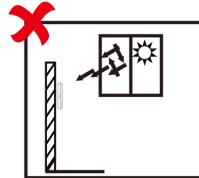
Backlight



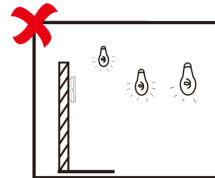
Direct Sunlight



Direct Sunlight
through Window



Indirect Light
through Window



Close to Light

Appendix D. Dimension

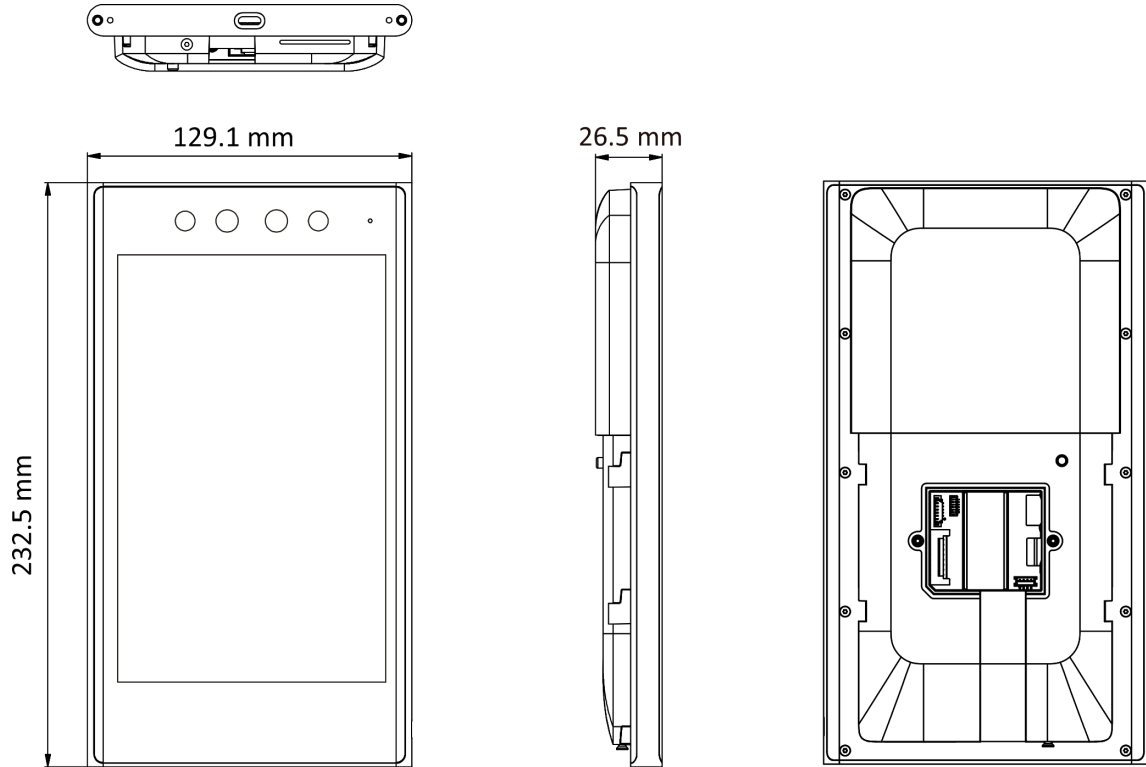
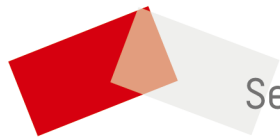


Figure D-1 Dimension

Appendix E. Function Differences

Model	DS-K1T681DBWX	DS-K1T681DBX
Wi-Fi	Support	Not Support
PoE	Not Support	Not Support
3G/4G	Not Support	Not Support



See Far, Go Further