



DS-K1T343 Series Face Recognition Terminal

User Manual

Legal Information

About this Document

- This Document includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only.
- The information contained in the Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (<https://www.hikvision.com>). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

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



Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- **HIKVISION** and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR

IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Data Protection

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

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

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.
- Do not connect several devices to one power adapter as adapter overload may cause over-heat or fire hazard.
- 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.
- The socket-outlet shall be installed near the equipment and shall be easily accessible.
- 1. Do not ingest battery. Chemical burn hazard!
- 2. This product contains a coin/button cell battery. If the coin/button cell battery is swallowed, it can cause severe internal burns in just 2 hours and can lead to death.
- 3. Keep new and used batteries away from children.
- 4. If the battery compartment does not close securely, stop using the product and keep it away from children.
- 5. If you think batteries might have been swallowed or placed inside any part of the body, seek immediate medical attention.
- 6. CAUTION: Risk of explosion if the battery is replaced by an incorrect type.
- 7. Improper replacement of the battery with an incorrect type may defeat a safeguard (for example, in the case of some lithium battery types).
- 8. Do not dispose of the battery into fire or a hot oven, or mechanically crush or cut the battery, which may result in an explosion.
- 9. Do not leave the battery in an extremely high temperature surrounding environment, which may result in an explosion or the leakage of flammable liquid or gas.
- 10. Do not subject the battery to extremely low air pressure, which may result in an explosion or the leakage of flammable liquid or gas.
- 11. Dispose of used batteries according to the instructions.

Cautions:

- Do not drop the device or subject it to physical shock, and do not expose it to high electromagnetism radiation. Avoid the equipment installation on vibrations surface or places subject to shock (ignorance can cause equipment damage).
- Do not place the device in extremely hot (refer to the specification of the device for the detailed operating temperature), cold, dusty or damp locations, and do not expose it to high electromagnetic radiation.
- Exposing the equipment to direct sun light, low ventilation or heat source such as heater or radiator is forbidden (ignorance can cause fire danger).
- The device cover for indoor use shall be kept from rain and moisture.
- Exposing the equipment to direct sun light, low ventilation or heat source such as heater or radiator is forbidden (ignorance can cause fire danger).
- Please use a soft and dry cloth when clean inside and outside surfaces of the device cover, do not use alkaline detergents.
- Biometric recognition products are not completely applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.
- The serial port of the equipment is used for debugging only.
- 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.
- 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.
- This bracket is intended for use only with equipped devices. Use with other equipment may result in instability causing injury.
- This equipment is for use only with equipped bracket. Use with other (carts, stands, or carriers) may result in instability causing injury.

Available Models

Product Name	Model	Wireless
Face Recognition Terminal	DS-K1T343MX	13.56 MHz Card Presenting Frequency
	DS-K1T343MWX	13.56 MHz Card Presenting Frequency, Wi-Fi
	DS-K1T343MFX	13.56 MHz Card Presenting Frequency
	DS-K1T343MFWX	13.56 MHz Card Presenting Frequency, Wi-Fi
	DS-K1T343EX	125 KHz Card Presenting Frequency
	DS-K1T343EWX	125 KHz Card Presenting Frequency, Wi-Fi
	DS-K1T343EFX	125 KHz Card Presenting Frequency
	DS-K1T343EFWX	125 KHz Card Presenting Frequency, Wi-Fi

Use only power supplies listed in the user instructions:

Model	Manufacturer	Standard
ADS-12FG-12N 12012EPG	Shenzhen Honor Electronic Co., Ltd	PG

Contents

Appendix A. Symbol Conventions	155
Chapter 1 Overview	1
1.1 Overview	1
1.2 Features	1
Chapter 2 Appearance	2
Chapter 3 Installation	4
3.1 Installation Environment	4
3.2 Install with Gang Box	4
3.3 Base Mounting	7
Chapter 4 Wiring	9
4.1 Terminal Description	9
4.2 Wire Normal Device	11
4.3 Wire Secure Door Control Unit	12
4.4 Wire Fire Module	13
4.4.1 Wiring Diagram of Door Open When Powering Off	13
4.4.2 Wiring Diagram of Door Locked When Powering Off	15
Chapter 5 Activation	17
5.1 Activate via Device	17
5.2 Activate via Web Browser	18
5.3 Activate via SADP	19
5.4 Activate Device via iVMS-4200 Client Software	20
Chapter 6 Quick Operation	22
6.1 Select Language	22
6.2 Set Password Change Type	22
6.3 Set Network Parameters	23
6.4 Access to Platform	23

6.5 Privacy Settings	24
6.6 Set Administrator	25
Chapter 7 Basic Operation	28
7.1 Login	28
7.1.1 Login by Administrator	28
7.1.2 Login by Activation Password	29
7.1.3 Forgot Password	30
7.2 Communication Settings	31
7.2.1 Set Wired Network Parameters	31
7.2.2 Set Wi-Fi Parameters	32
7.2.3 Set RS-485 Parameters	33
7.2.4 Set Wiegand Parameters	34
7.2.5 Set ISUP Parameters	35
7.2.6 Platform Access	37
7.2.7 SNMP Settings	38
7.2.8 ONVIF Settings	38
7.3 User Management	38
7.3.1 Add Administrator	38
7.3.2 Add Face Picture	40
7.3.3 Add Fingerprint	42
7.3.4 Add Card	43
7.3.5 Add PIN	44
7.3.6 Set Person Type via Device	45
7.3.7 Set Authentication Mode	46
7.3.8 Search and Edit User	46
7.3.9 Check Attendance Only	47
7.4 Platform Attendance	47
7.4.1 Disable Attendance Mode via Device	48

7.4.2 Set Manual Attendance via Device	48
7.4.3 Set Auto Attendance via Device	49
7.4.4 Set Manual and Auto Attendance via Device	51
7.5 Data Management	52
7.5.1 Delete Data	52
7.5.2 Import Data	52
7.5.3 Export Data	53
7.6 Identity Authentication	54
7.6.1 Authenticate via Single Credential	54
7.6.2 Authenticate via Multiple Credential	54
7.7 Basic Settings	55
7.7.1 Enable/Disable Voice Prompt via Device	58
7.7.2 Set Device Time via Device	58
7.7.3 Set Sleep Duration via Device	58
7.7.4 Select Language	58
7.7.5 Set Device Number via Device	58
7.7.6 Set Beauty via Device	59
7.7.7 Call Settings	59
7.7.8 Set Privacy Parameters via Device	59
7.7.9 Set Video Standard	60
7.7.10 Set Secure Door Control Unit Parameters	60
7.8 Set Biometric Parameters	61
7.9 Change Device Password	63
7.10 Authentication Settings	64
7.10.1 Set Terminal Authentication Mode via Device	66
7.10.2 Set Reader Authentication Mode via Device	66
7.10.3 Manually Trigger Face Authentication via PC Web	67
7.10.4 Enable/Disable NFC Card	67

7.10.5 Enable/Disable M1 Card	67
7.10.6 Remote Authentication	68
7.10.7 Set Authentication Interval via Device	68
7.10.8 Set Authentication Result Display Duration via Device	68
7.10.9 Set Password Mode	68
7.10.10 Door Parameter Configuration	69
7.11 Preference Settings	69
7.11.1 Set Shortcut Key via Device	70
7.11.2 Theme	71
7.12 System Maintenance	71
Chapter 8 Configure the Device via the Mobile Web	74
8.1 Login	74
8.2 Overview	74
8.3 Forget Password	75
8.4 Configuration	75
8.4.1 View Device Information	75
8.4.2 Time Settings	75
8.4.3 Set DST	76
8.4.4 User Management	77
8.4.5 Network Settings	77
8.4.6 Access Configuration	81
8.4.7 User Management	82
8.4.8 Device Management	84
8.4.9 Search Event	84
8.4.10 Access Control Settings	84
8.4.11 Call Settings	90
8.4.12 Audio Settings	92
8.4.13 Custom Home Page	93

8.4.14 Upgrade and Maintenance	93
8.4.15 View User Manual	94
8.4.16 View Open Source Software License	94
Chapter 9 Quick Operation via Web Browser	95
9.1 Change Password	95
9.2 Select Language	95
9.3 Time Settings	95
9.4 Privacy Settings	96
9.5 Administrator Settings	96
9.6 No. and System Network	97
Chapter 10 Operation via Web Browser	98
10.1 Login	98
10.2 Forget Password	98
10.3 Help	98
10.3.1 Open Source Software Licenses	98
10.3.2 View Online Help Document	99
10.4 Logout	99
10.5 Quick Operation via Web Browser	99
10.5.1 Change Password	99
10.5.2 Select Language	99
10.5.3 Time Settings	99
10.5.4 Privacy Settings	100
10.5.5 Administrator Settings	101
10.5.6 No. and System Network	101
10.6 Person Management	102
10.7 Live View	103
10.8 Access Control Application	104
10.8.1 Anti-Passback Settings	104

10.8.2 Multi-Door Interlocking Settings	104
10.9 Access Control Management	105
10.9.1 Search Event	105
10.9.2 Door Parameter Configuration	105
10.9.3 Authentication Settings	108
10.9.4 Authentication Linkage Settings	112
10.9.5 Set Authentication Plan	112
10.9.6 Set Face Parameters	113
10.9.7 Card Settings	117
10.9.8 Set Remote Verification	119
10.9.9 Privacy Settings	120
10.9.10 Video Intercom Settings	122
10.10 Device Management	125
10.11 System Configuration	126
10.11.1 View Device Information	126
10.11.2 Set Time	126
10.11.3 Change Administrator's Password	127
10.11.4 Account Security Settings	127
10.11.5 View Device Arming/Disarming Information	127
10.11.6 Set Working Mode via PC Web	128
10.11.7 Network Settings	128
10.11.8 Set Video and Audio Parameters	134
10.11.9 Access Configuration	136
10.11.10 Image Parameter Settings	138
10.11.11 Linkage Settings	139
10.11.12 Time and Attendance Settings	140
10.12 Preference Settings	142
10.12.1 Set Standby Image via PC Web	142

10.12.2 Set Sleep Time via PC Web	142
10.12.3 Customize Authentication Desk via PC Web	142
10.12.4 Notice Publication	143
10.12.5 Customize Audio Content	143
10.12.6 Customize Prompt Voice via PC Web	144
10.12.7 Configure Authentication Result Text	144
10.13 Upgrade and Maintenance	145
10.13.1 Reboot	146
10.13.2 Upgrade	147
10.13.3 Restoration	148
10.13.4 Export Device Parameters via PC Web	148
10.13.5 Import Device Parameters via PC Web	149
10.13.6 Device Debugging	149
10.13.7 Log Query	151
10.13.8 Advanced Settings via PC Web	151
10.13.9 Security Management	151
10.13.10 Certificate Management	152
Chapter 11 Other Platforms to Configure	154
Appendix B. Tips for Scanning Fingerprint	156
Appendix C. Tips When Collecting/Comparing Face Picture	158
Appendix D. Tips for Installation Environment	160

Chapter 1 Overview

1.1 Overview

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

1.2 Features

- 4.3-inch LCD touch screen
- 2 MP wide-angle dual-lens
- Face anti-spoofing
- Face recognition distance: 0.3 m to 1.5 m
- Suggested height for face recognition: between 1.4 m and 1.9 m
- Deep learning algorithm
- 1500 face capacity, 3,000 card capacity, and 150,000 events
- 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
- Manage, search and set device data after logging in the device locally
- Connects to one external card reader or access controller via RS-485 protocol
- Connects to secure door control unit via RS-485 protocol to avoid the door opening when the device is destroyed
- Two-way audio
- Arms by multiple client softwares
- Watchdog design and tamper function
- Support English, Spanish (South America), Arabic, Thai, Indonesian, Russian, Vietnamese, Portuguese (Brazil), Korean, and Japanese

Chapter 2 Appearance

The appearance of the device with fingerprint is as follows:

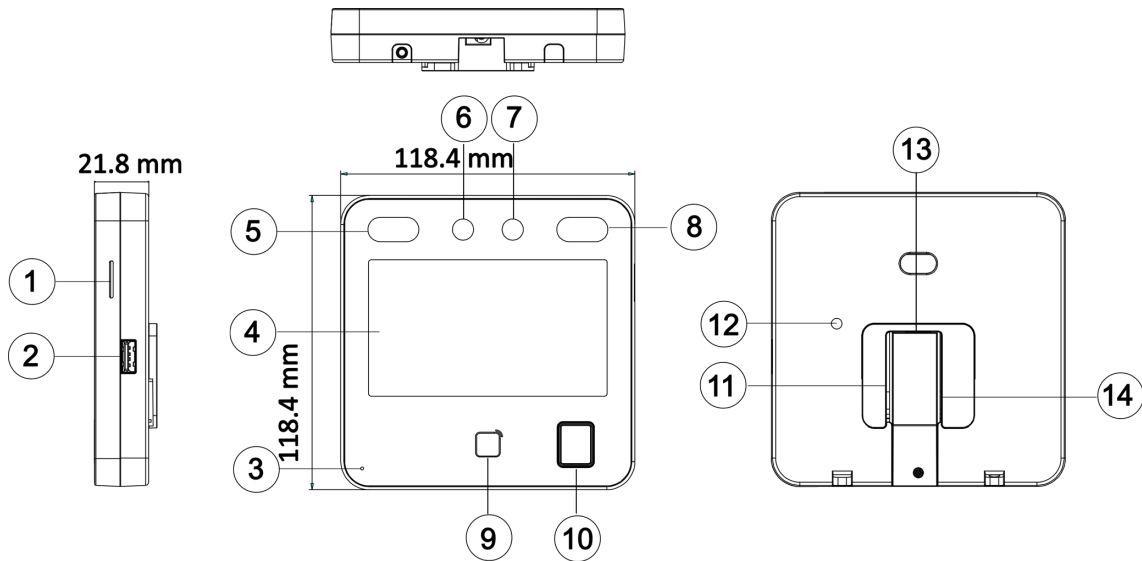


Figure 2-1 Appearance (With Fingerprint)

The appearance of the device without fingerprint is as follows:

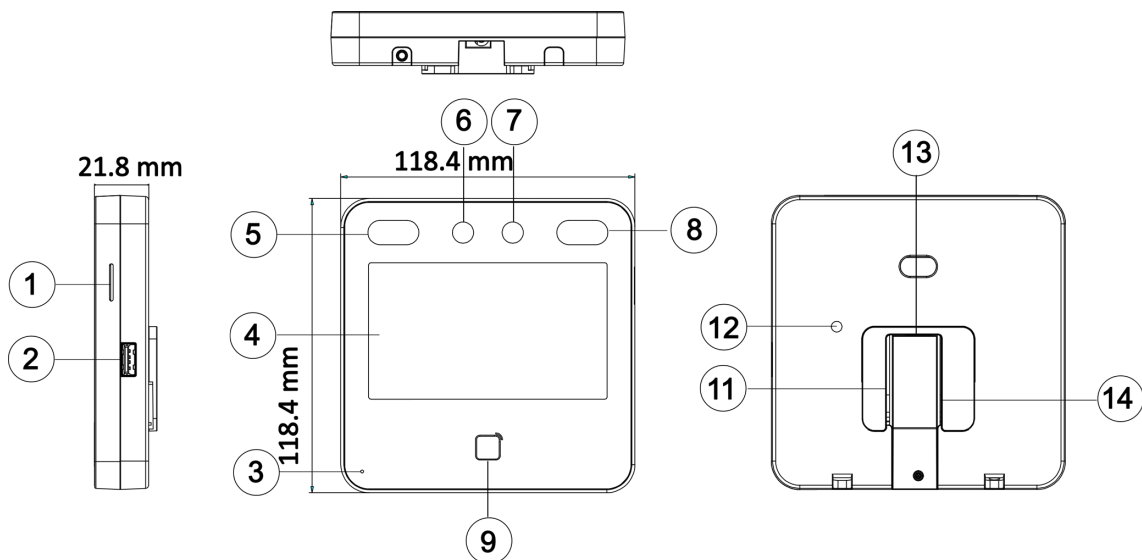


Figure 2-2 Appearance (Without Fingerprint)

Table 2-1 Appearance Description

No.	Name
1	Loudspeaker
2	USB Interface
3	MIC
4	Touch Screen
5	IR Light
6	Camera
7	Camera
8	IR Light
9	Card Presenting Area
10	Fingerprint Module  Note Only devices that support the fingerprint function contain a fingerprint module.
11	Wiring Terminal (Including Power Supply Interface)
12	TAMPER
13	Network Interface
14	Debugging Port (For Debugging Only)

Chapter 3 Installation

3.1 Installation Environment

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

3.2 Install with Gang Box

Steps

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



You should purchase the gang box separately.

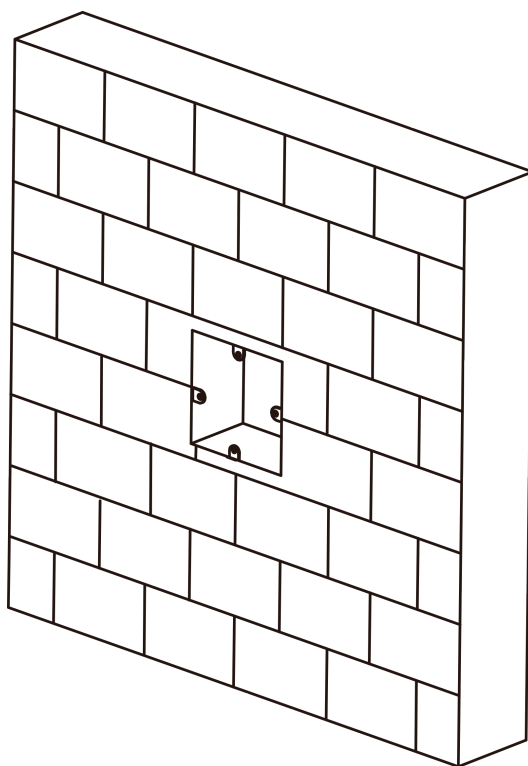


Figure 3-1 Install Gang Box

2. Use 4 supplied screws (M4) to secure the mounting plate on the gang box.

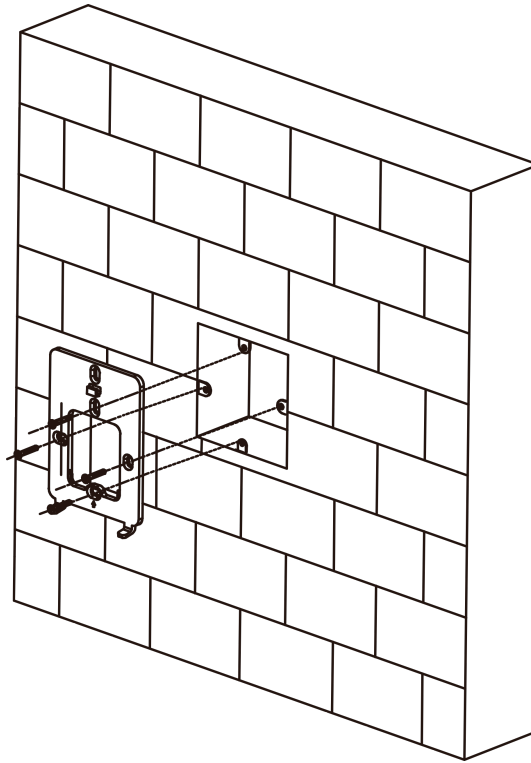


Figure 3-2 Install Mounting Plate

3. Route the cables through the cable hole of the mounting plate, and connect to the corresponding peripherals cables.
4. Buckle into the mounting plate after aligning the device with the mounting plate. Use 1 supplied screw (M3) to secure the device on the mounting plate.

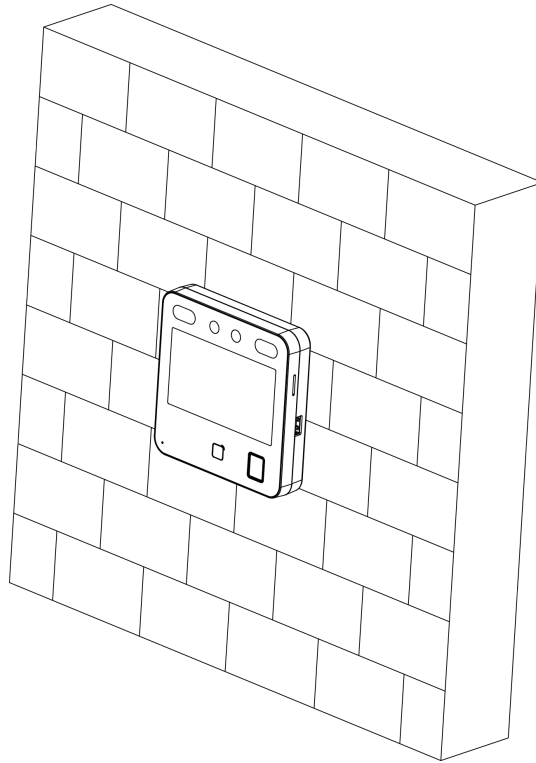


Figure 3-3 Secure Device

3.3 Base Mounting

Steps

1. Route the cables through the cable hole of the bracket, and connect the terminals with peripherals cables. Place the bracket close to the back side of the device.

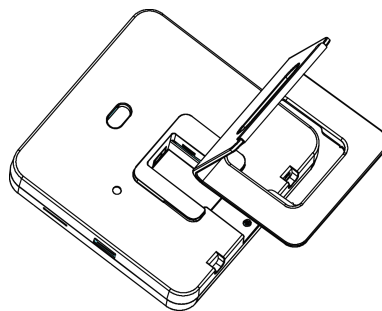


Figure 3-4 Place Bracket Close to Device Back Side

2. Press the bracket with both hands, and make sure that the buckle of the bracket fits with the back side of the device. Fasten the bracket in the direction of the arrow.

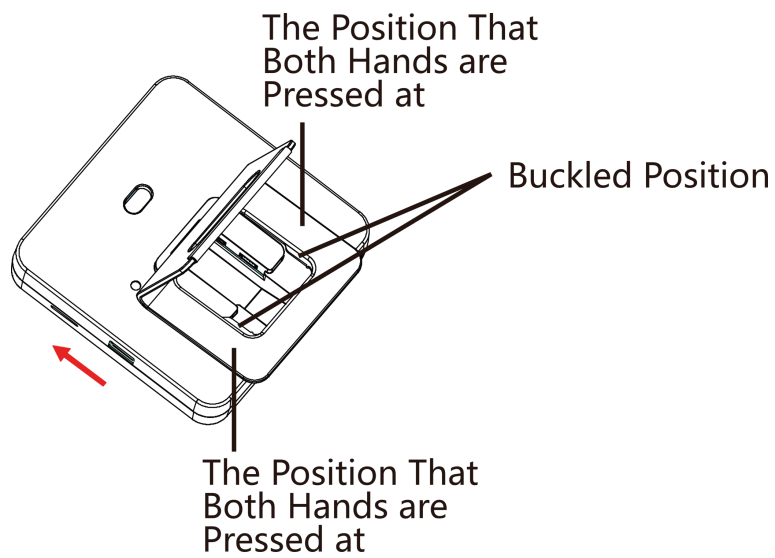


Figure 3-5 Fasten Bracket

3. Buckle into the bracket to the end to complete the installation.

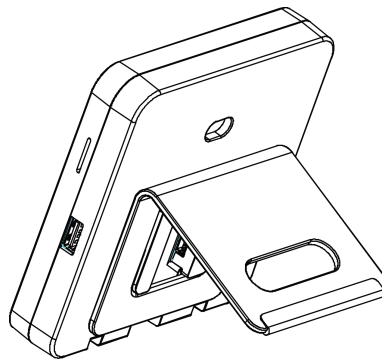


Figure 3-6 Complete Installation

Chapter 4 Wiring

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

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



Note

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

4.1 Terminal Description

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

The terminal's diagram is as follows:

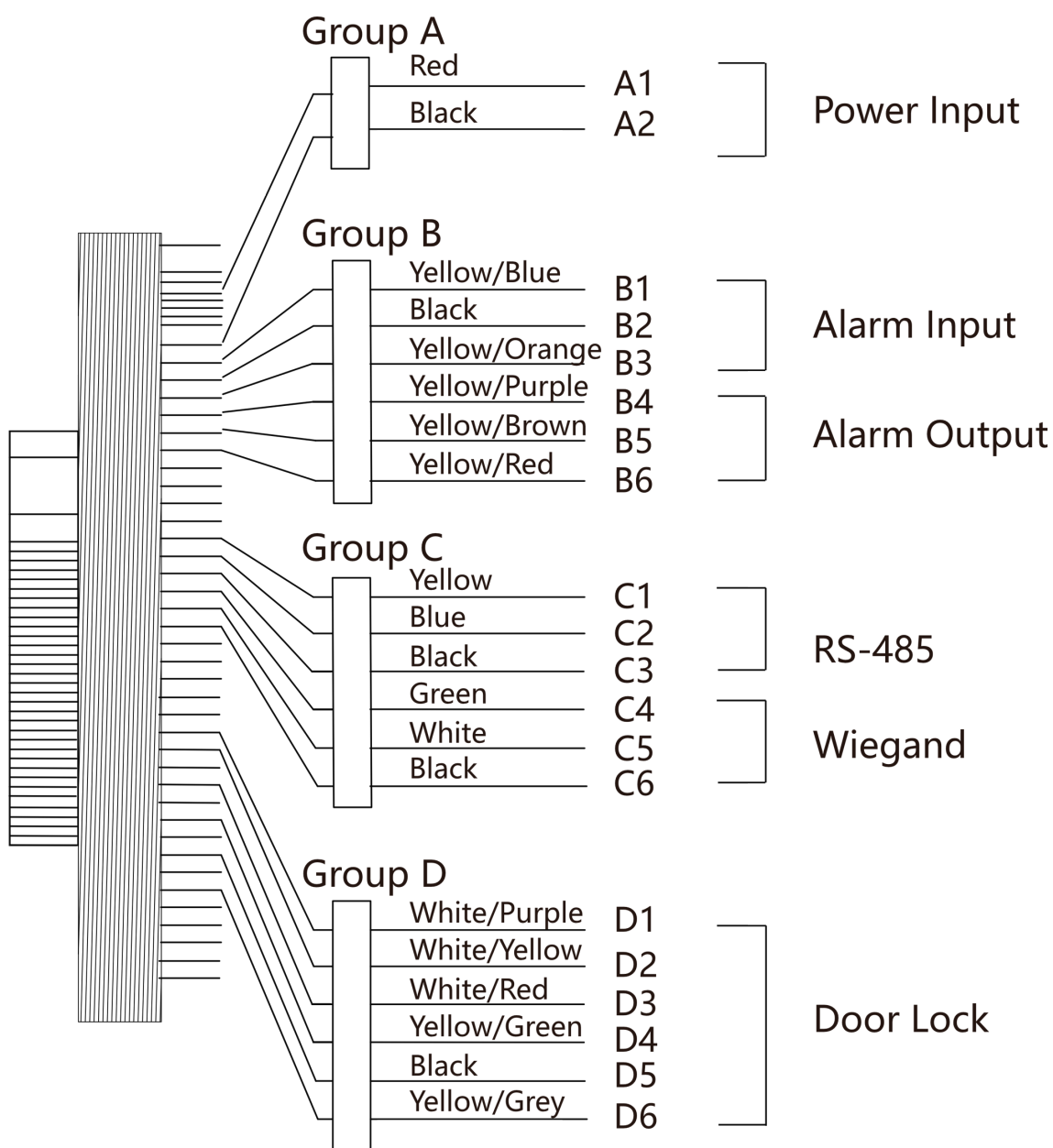


Figure 4-1 Terminal Diagram

The descriptions of the terminals are as follows:

Table 4-1 Terminal Descriptions

Group	No.	Function	Color	Name	Description
Group A	A1	Power Input	Red	+12 V	12 VDC Power Supply
	A2		Black	GND	Ground
Group 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/Grey	BTN	Exit Door Wiring

4.2 Wire Normal Device

You can connect the terminal with normal peripherals.

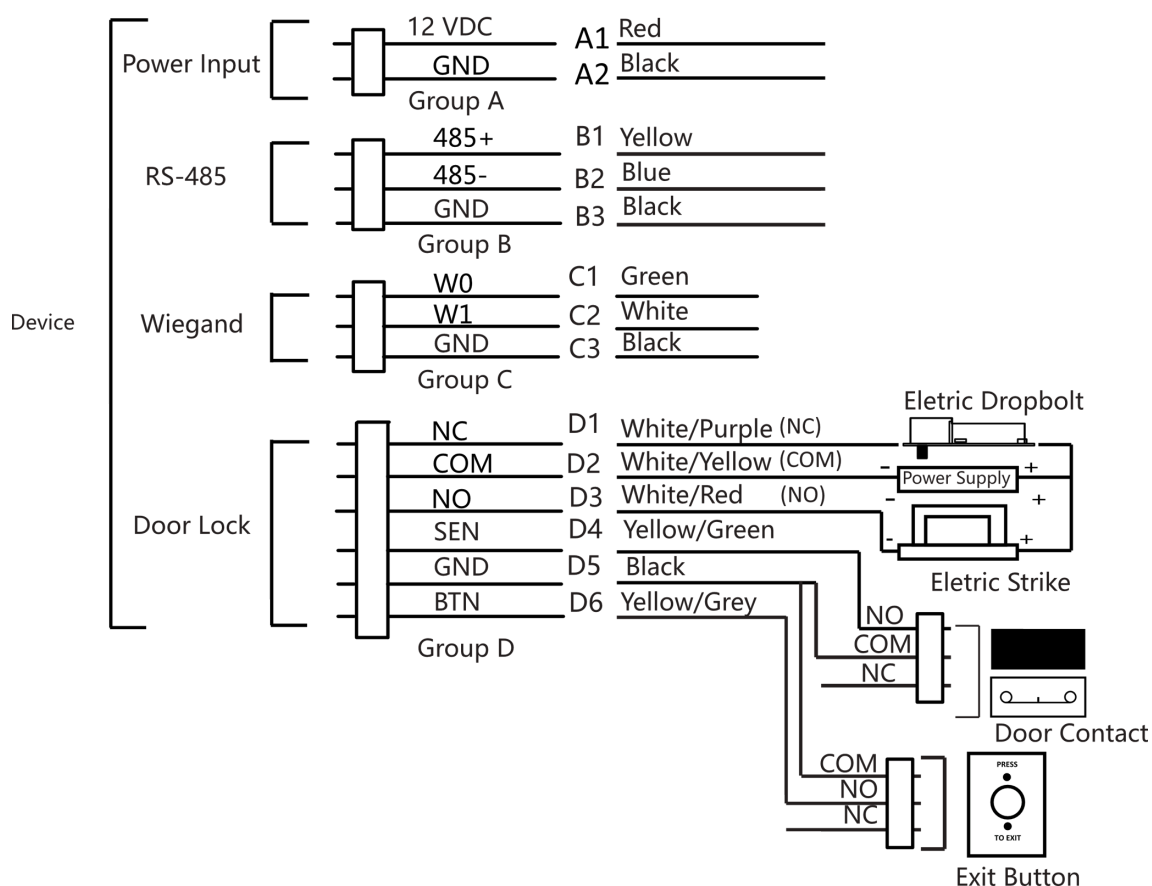


Figure 4-2 Device Wiring

Note

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

4.3 Wire Secure Door Control Unit

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

The wiring diagram is as follows.

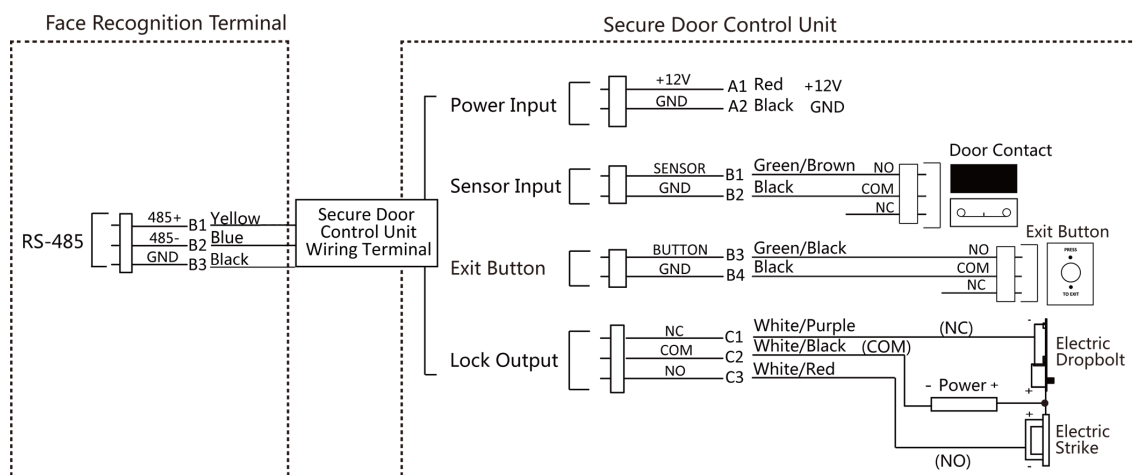


Figure 4-3 Secure Door Control Unit Wiring

Note

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

4.4 Wire Fire Module

4.4.1 Wiring Diagram of Door Open When Powering Off

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

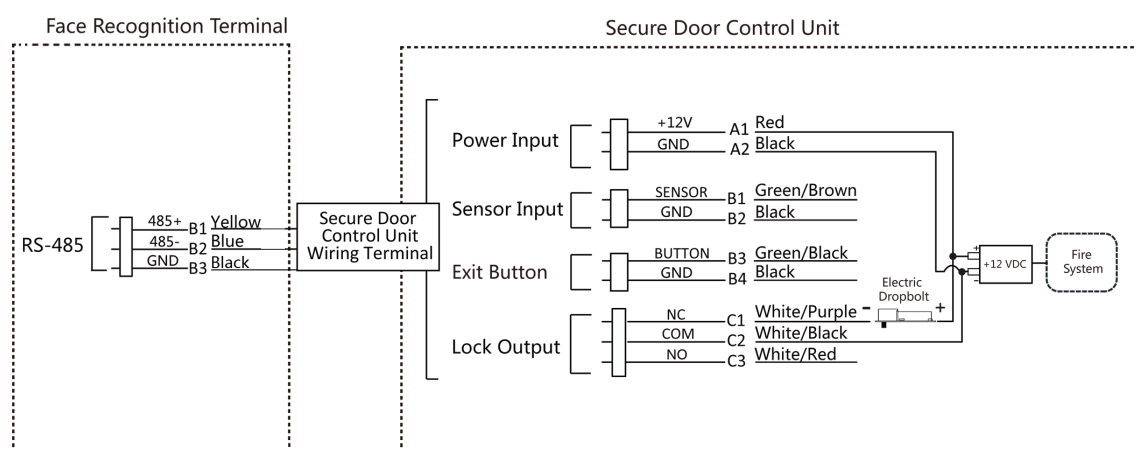
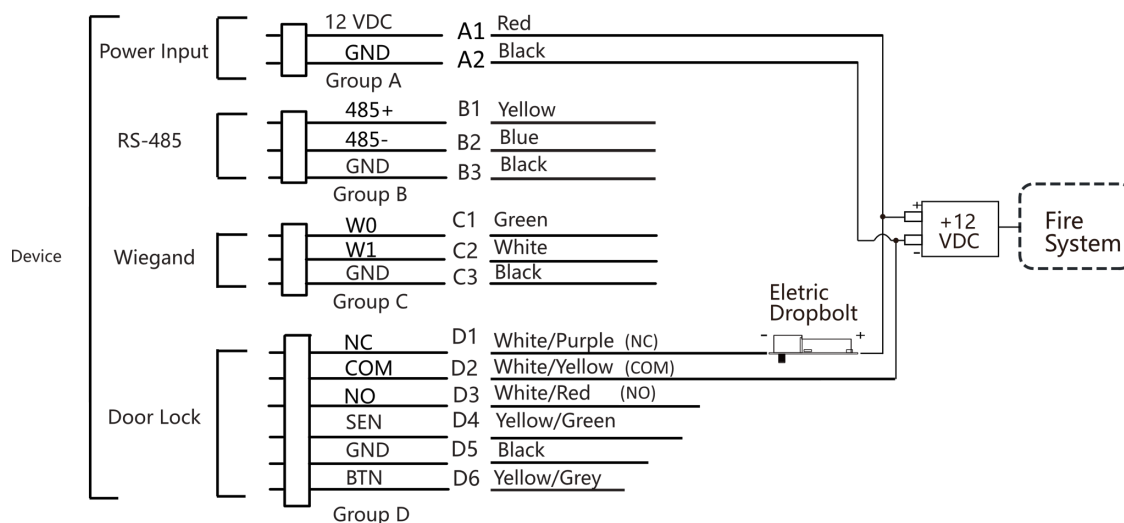
Security Type: Door Open When Powering Off

Scenario: Installed in Fire Engine Access

Type 1

Note

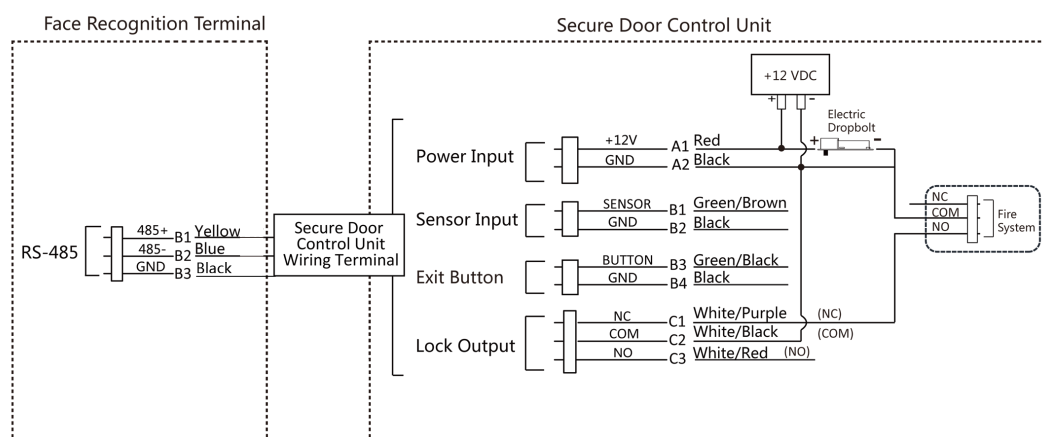
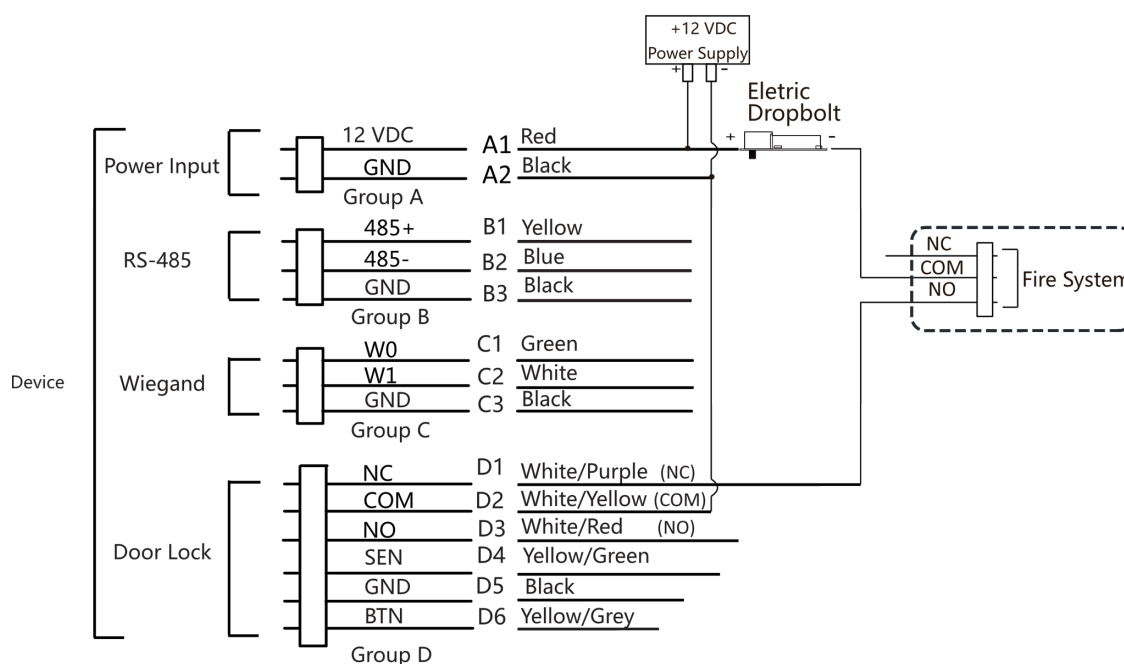
The fire system controls the power supply of the access control system.



Type 2

Note

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



4.4.2 Wiring Diagram of Door Locked When Powering Off

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

Security Type: Door Locked When Powering Off

Scenario: Installed in Entrance/Exit with Fire Linkage

Note

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

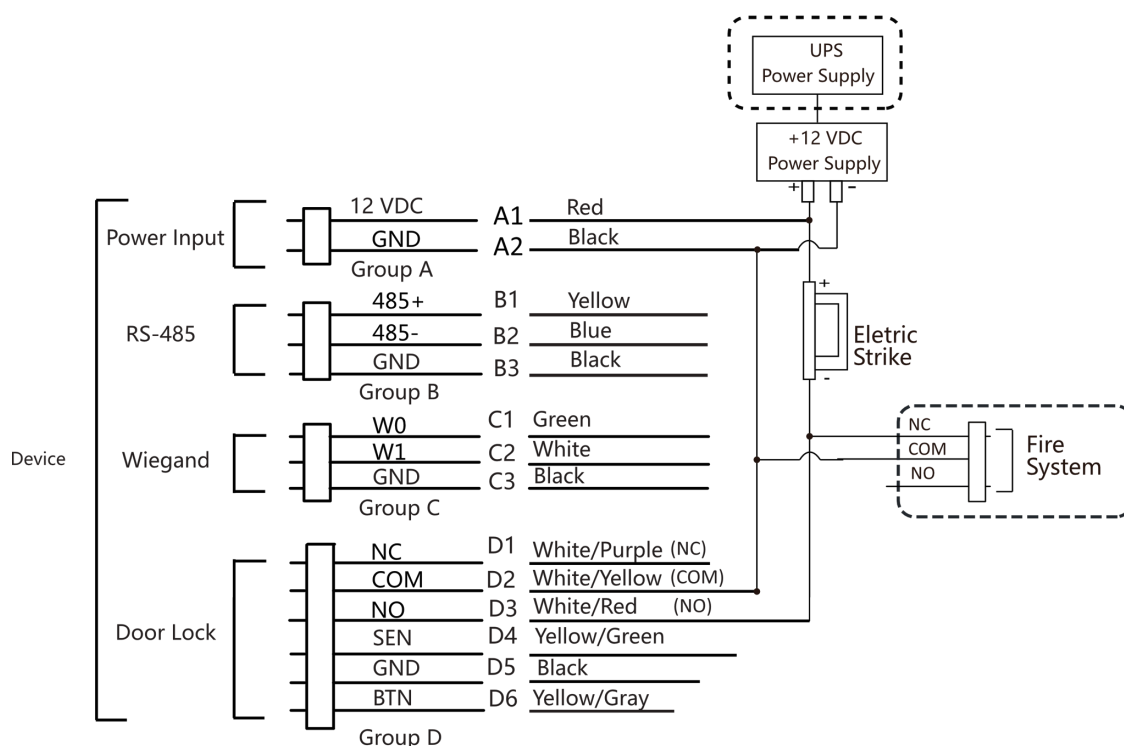


Figure 4-8 Device Wiring

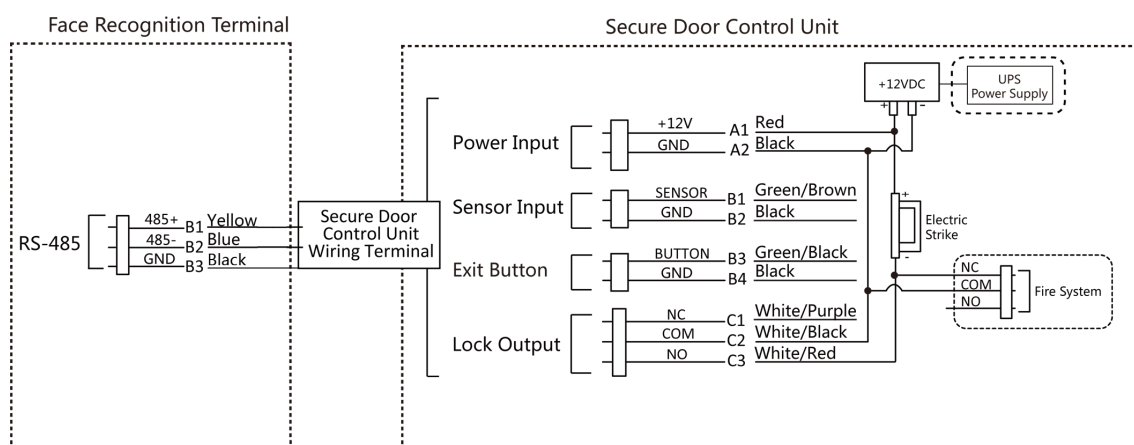


Figure 4-9 Wiring Diagram

Chapter 5 Activation

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

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

The default values of the device are as follows:

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

5.1 Activate via Device

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

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

Figure 5-1 Activation Page



Caution

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

characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

- Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.
 - Do not contain following characters in the password: the user name, 123, admin (case-insensitive), 4 or more continuously increasing or decreasing digits, or 4 or more consecutively repeated characters.
 - Password cannot contain words such as hik, hkws, and hikvision (case insensitive).
-
- After activation, you should select a language according to your actual needs.
 - After activation, if you need to set privacy, you should check the item. For details, see **Privacy Settings**.
 - After activation, if you need to add administrator to manage the device parameters, you should set administrator. For details, see **Add Administrator**.

5.2 Activate via Web Browser

You can activate the device via the web browser.

Steps

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



Note

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

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



Caution

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



Note

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

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

5.3 Activate via SADP

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

Before You Start

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

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

Steps

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



Caution

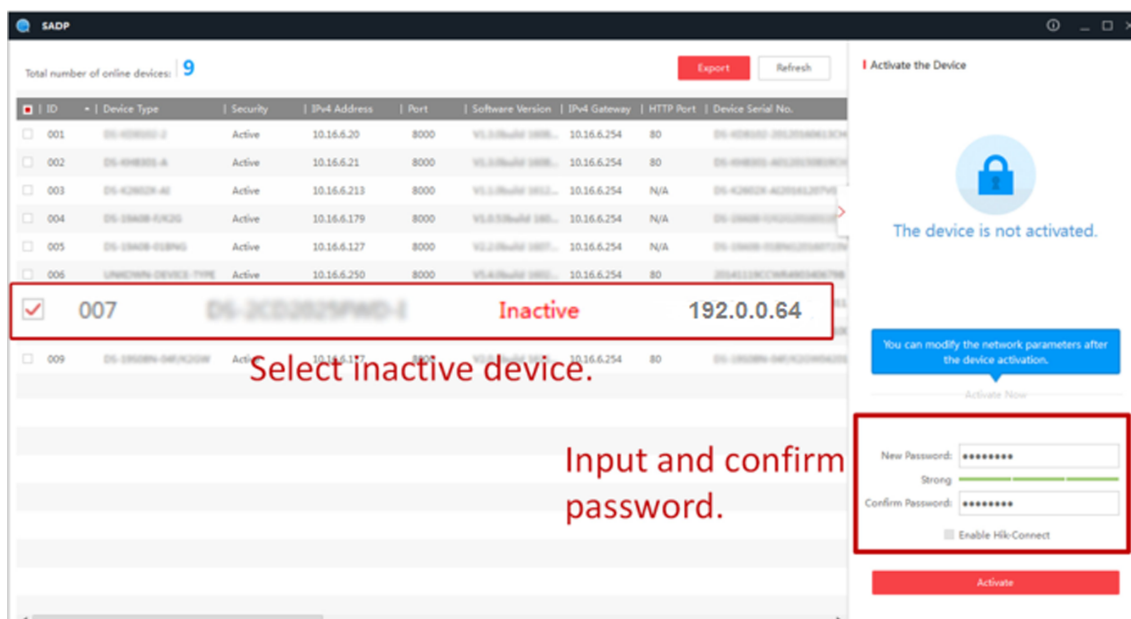
STRONG PASSWORD RECOMMENDED-We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password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



Note

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

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



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

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

5.4 Activate Device via 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 6 Quick Operation

6.1 Select Language

You can select a language for the device system.

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

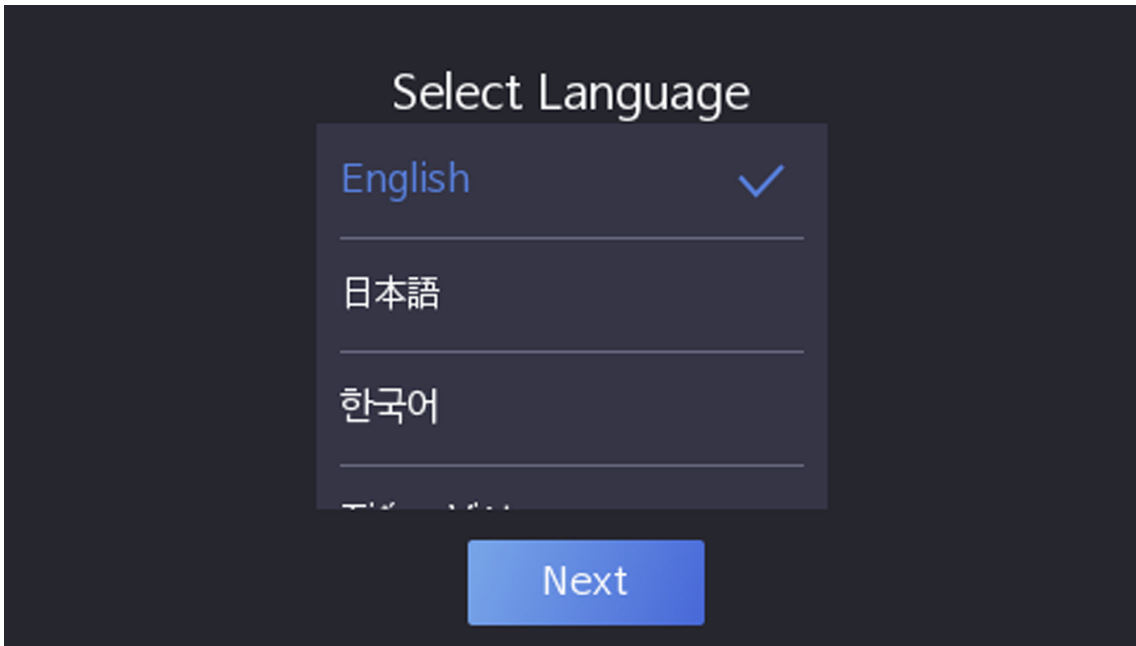


Figure 6-1 Select System Language

By default, the system language is English.



Note

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

6.2 Set Password Change Type

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

Change Password via Email Address

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

Change via Security Questions

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



Note

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

6.3 Set 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.
2. Tap **Next**.

Wired Network



Note

Make sure the device has connected to a network.

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

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

Wi-Fi

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

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

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

6.4 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.
2. Tap **Next**.
3. **Optional:** Tap **Skip** to skip the step.
4. **Optional:** Tap **Previous** to go to the previous page.

Note

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

6.5 Privacy Settings

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

Select parameters according to your actual needs.

The screenshot displays the 'Privacy Settings' page, which is organized into several sections:

- Event Storage Settings:** Includes 'Event Storage Type' with three radio button options: 'Delete Old Events Periodically', 'Delete Old Events by Specified Time', and 'Overwrite' (which is selected).
- Authentication Result Settings:** Includes 'Display Authentication Result' with four checkboxes: 'Face Picture', 'Name' (checked), 'Employee ID', and 'Temperature' (checked). It also features a 'Name De-identification' toggle switch (turned on) and an 'Authentication Result Display ...' field set to '5'.
- Picture Uploading and Storage:** This section contains multiple toggle switches and dropdown menus:
 - 'Save Picture When Auth.' (on) with a note: 'If enabled, the captured picture when authentication will be saved to the device automatically.'
 - 'Upload Picture When Auth.' (on) with a note: 'If enabled, the captured picture when authentication will be uploaded to the platform automatically.'
 - 'Captured Picture Mode' with radio buttons for 'Default' (selected) and 'Face Picture Matting'.
 - 'Max. Picture Size' dropdown menu set to 'All'.
 - 'Picture Resolution' dropdown menu set to 'Auto'.
 - 'Save Registered Picture' (on) with a note: 'If enabled, the captured face picture when registered will be saved to the device.'
 - 'Save Pictures After Linked Cap...' (on) with a note: 'If enabled, the captured pictures will be saved to the device automatically.'
 - 'Upload Picture After Linked Ca...' (on) with a note: 'If enabled, the captured pictures will be uploaded to the platform automatically.'
 - 'Save Thermographic Picture' (off).
- Clear All Pictures in Device:** Contains two buttons: 'Clear Registered Face Pictures' and 'Clear Captured Pictures'.
- PIN Mode:** Includes 'PIN Mode' with two radio button options: 'Platform-Applied Personal PIN' (selected) and 'Device-Set Personal PIN'.

A red 'Save' button is located at the bottom center of the page.

Figure 6-2 Privacy

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

Upload the pictures captured when authenticating to the platform automatically.

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

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

Save Registered Pic. (Save Registered Picture)

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

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

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

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

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

Tap **Next** to complete the settings.

6.6 Set Administrator

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

Before You Start

Activate the device.

Steps

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

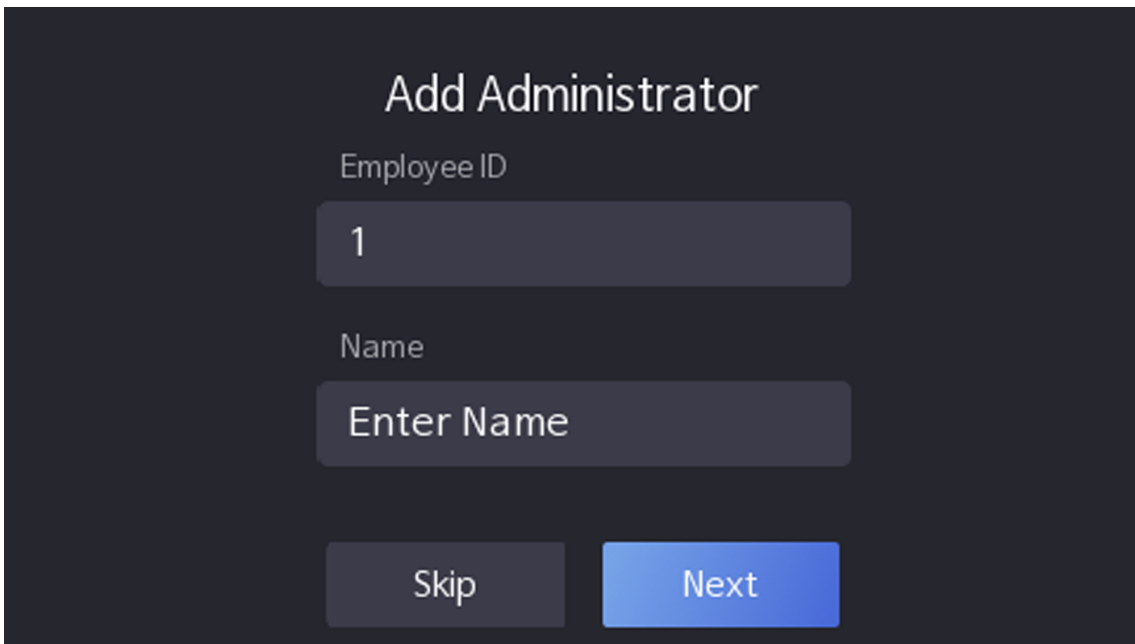


Figure 6-3 Add Administrator Page

3. Select a credential to add.



Note

Up to one credential should be added.

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

4. Click **OK**.

You will enter the authentication page.

Status Icon Description



Device is armed/not armed.



Hik-Connect is enabled/disabled/enabled but not connected/upgrading online.



SIP is enabled/disabled/enabled but not connected.



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



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

Shortcut Keys Description



Note

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



Scan QR code to authenticate.



Note

The QR code can be obtained from the visitor terminal.



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



Note

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



Enter password to authenticate.

Chapter 7 Basic Operation

7.1 Login

Login the device to set the device basic parameters.

7.1.1 Login by Administrator

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

Steps

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



Figure 7-1 Admin Login

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

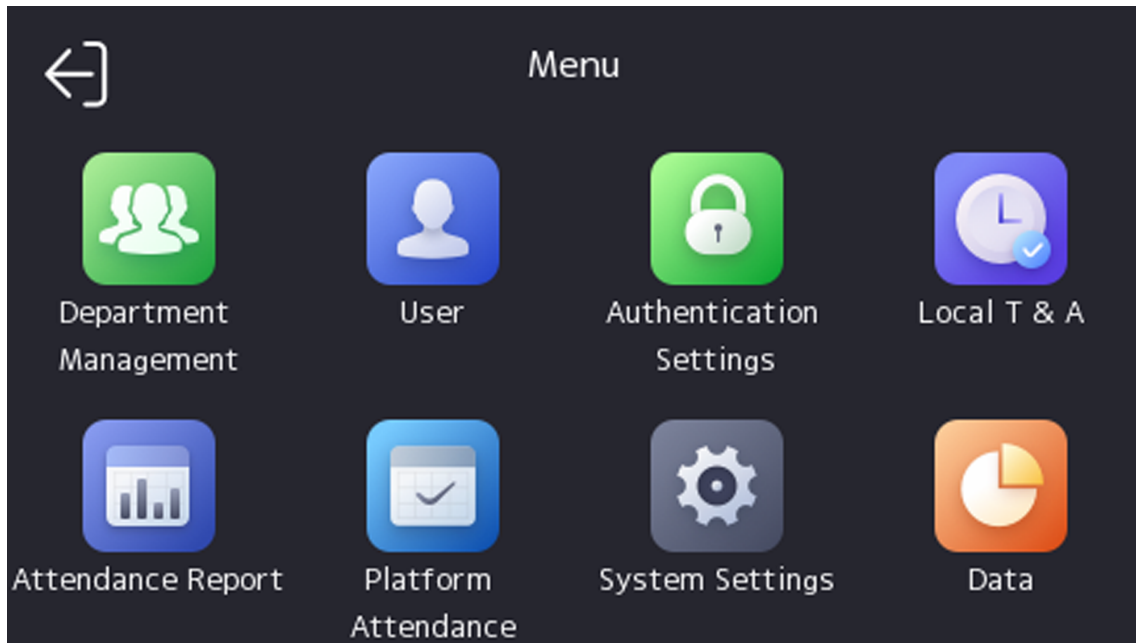


Figure 7-2 Home Page

 Note

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

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

7.1.2 Login by Activation Password

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

Steps

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

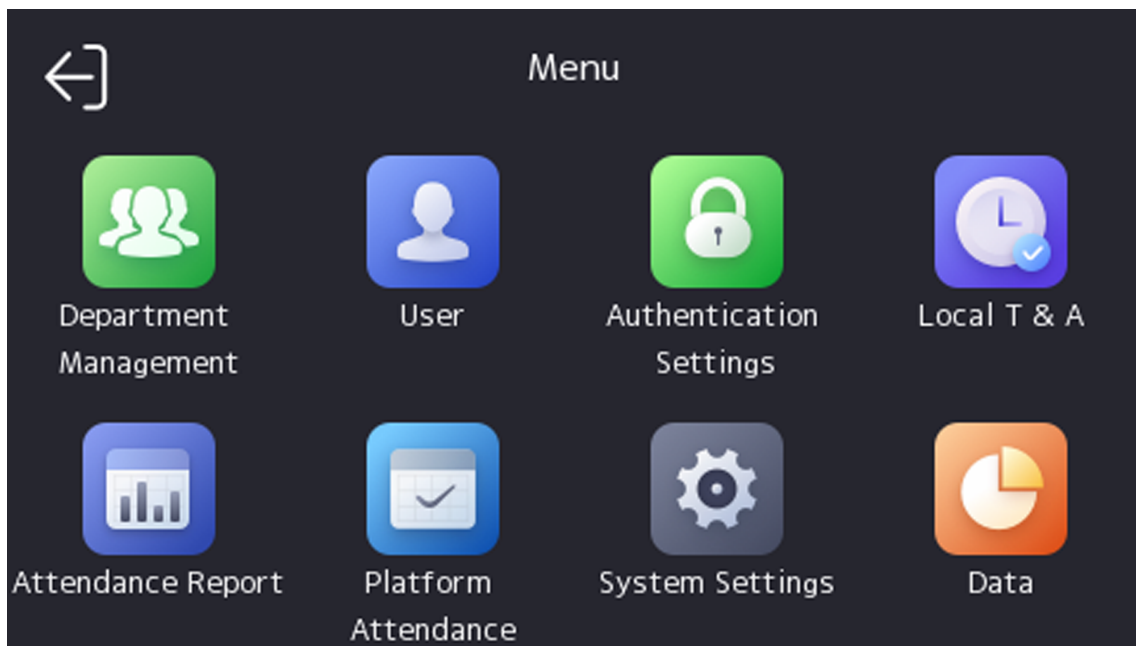


Figure 7-3 Home Page

7.1.3 Forgot Password

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

Steps

1. Hold the initial page for 3 s and slide to the left/right by following the gesture and log in the page.
2. **Optional:** If you have set an administrator, tap  in the pop-up admin authentication page.
3. Tap **Forgot Password**.
4. Select a password change type from the list.

Note

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

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

Note

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

- a. Download Hik-Connect app.
- b. Go to **More** → **Reset Device Password** .

- c. Scan the QR code on the device and a verification code will be popped up.

**Note**

Tap the QR code to get a larger picture.

- d. Enter the verification code on the device page.

6. Create a new password and confirm it.

7. Tap **OK**.

7.2 Communication Settings

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

7.2.1 Set Wired Network Parameters

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

Steps

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

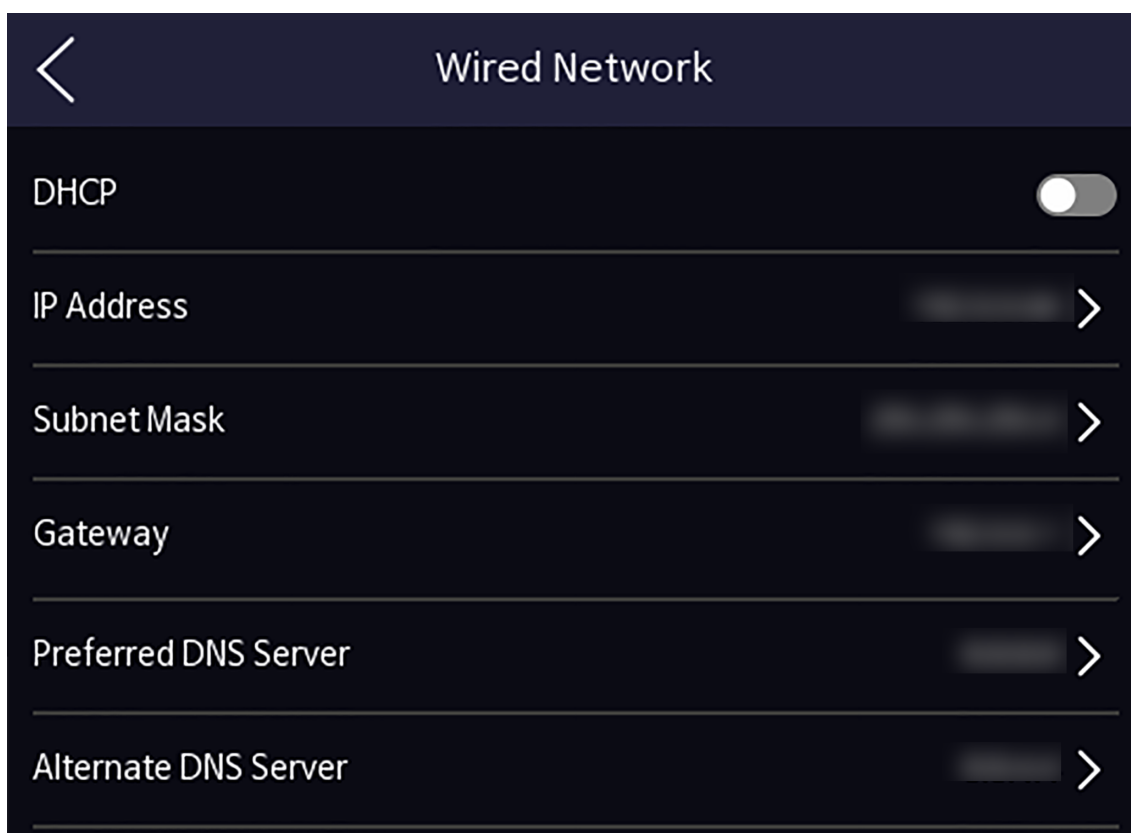


Figure 7-4 Wired Network Settings

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

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

 Note

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

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

7.2.2 Set Wi-Fi Parameters

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

Steps

 Note

The function should be supported by the device.

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

2. On the Communication Settings page, tap.

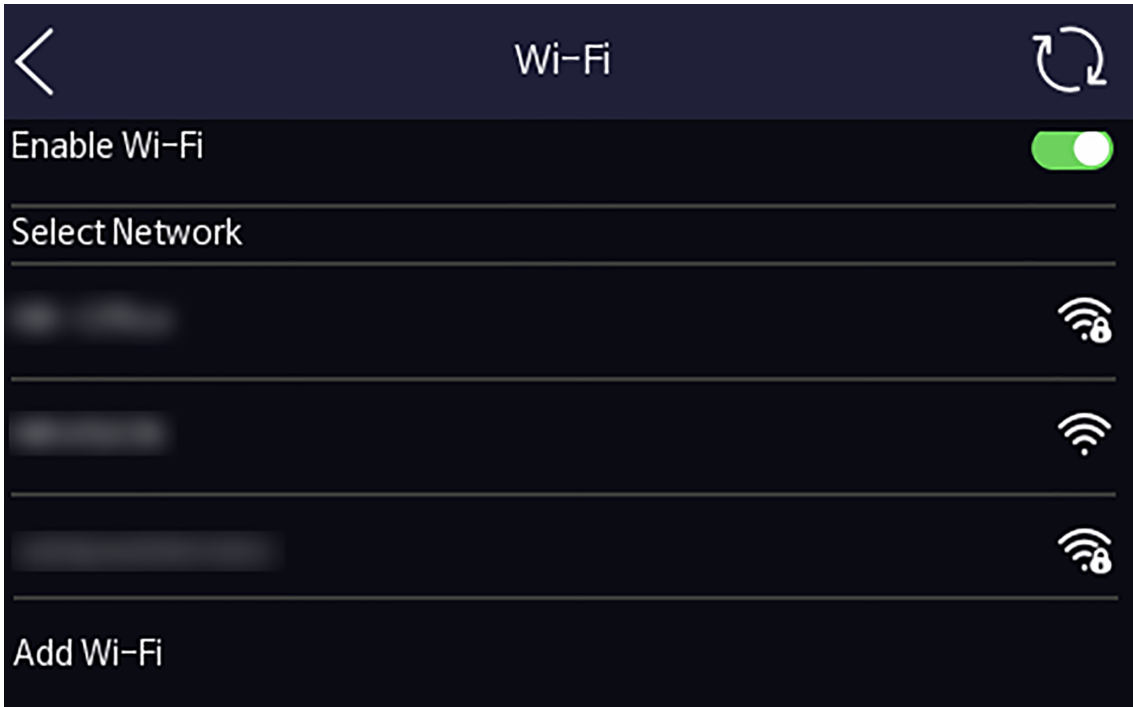


Figure 7-5 Wi-Fi Settings

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

 Note

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

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

7.2.3 Set RS-485 Parameters

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

Steps

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

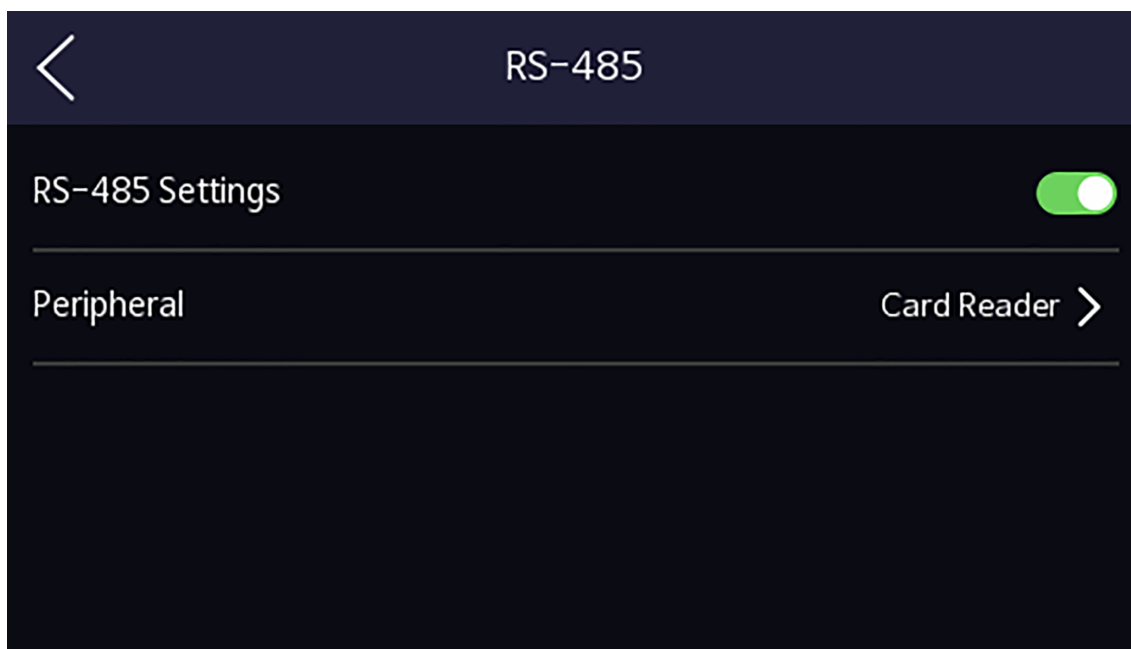


Figure 7-6 Set RS-485 Parameters

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



Note

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

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

7.2.4 Set Wiegand Parameters

You can set the Wiegand transmission direction.

Steps

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



Figure 7-7 Wiegand Settings

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

 Note

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

7.2.5 Set ISUP Parameters

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

Before You Start

Make sure your device has connect to a network.

Steps

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

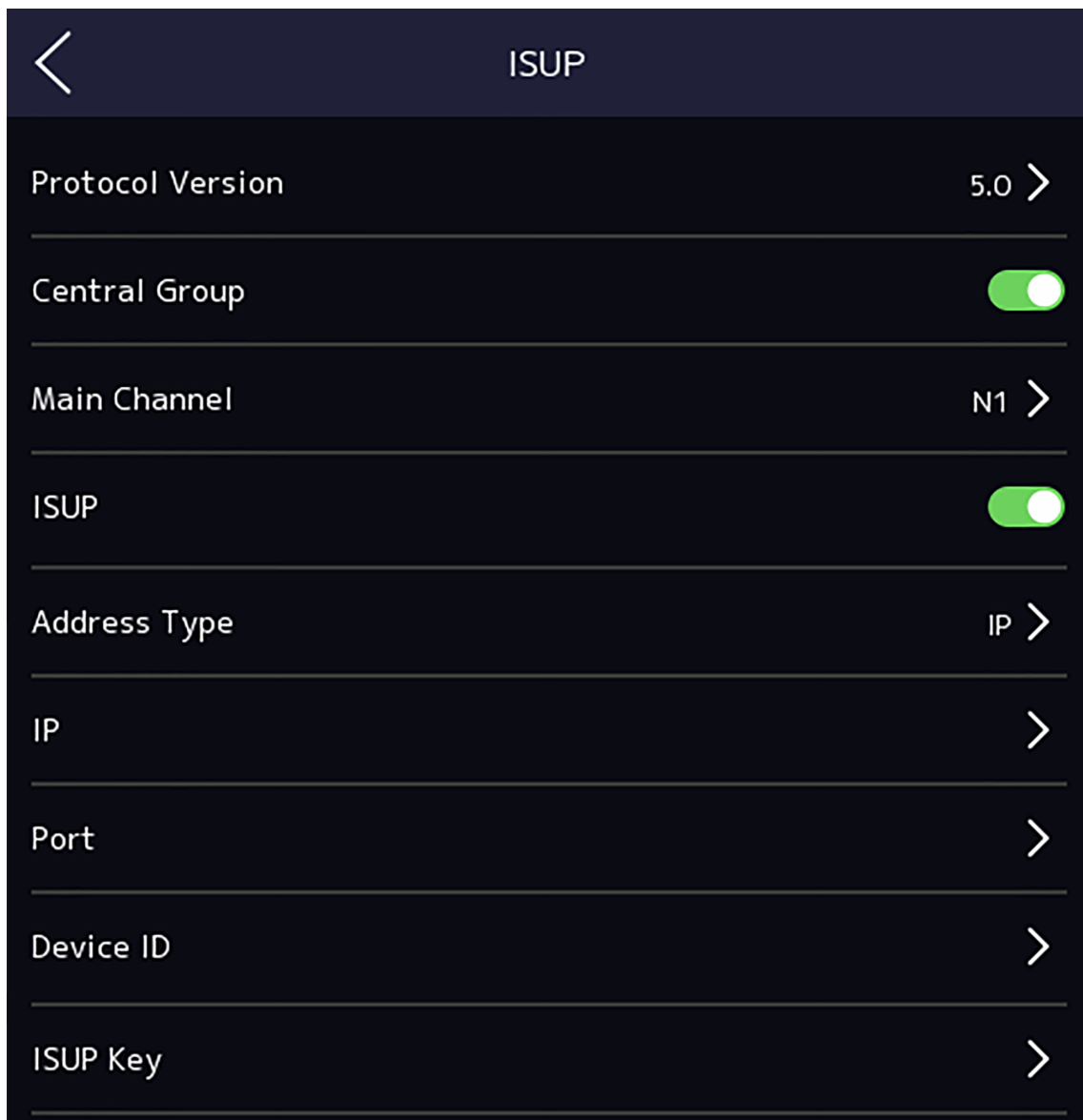


Figure 7-8 ISUP Settings

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 EHome protocol.

Address Type

Select an address type according to your actual needs.

IP Address

Set the ISUP server's IP address.

Port No.

Set the ISUP server's port No.



Note

Port No. Range: 0 to 65535.

Device ID

Set device serial no.

Password

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



Note

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

7.2.6 Platform Access

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

Before You Start

Make sure your device has connected to a network.

Steps

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

7.2.7 SNMP Settings

You can set SNMP parameters.

Steps

1. Tap **System Settings** → **Comm.** (Communication Settings) on the Home page to enter the Communication Settings page.
2. On the Communication Settings page, tap **SNMP**.
3. Enable **SNMP**.
4. Set **Trap Community String**.
5. Set **NMS IP Address** and **NMS Port**.



Note

Enabling SNMP increases network vulnerability. You can enable or disable according to your actual needs.

7.2.8 ONVIF Settings

ONVIF (Open Network Video Interface Forum) defines common protocols for information exchange between network video devices, including device discovery, real-time video, audio, meta data, and control information. The ONVIF protocol can be enabled to achieve interoperability between different network video products.

Steps

1. Tap **System Settings** → **Comm.** to enter the communication settings interface.
2. When returning to save, the device will prompt for a restart. Click **Confirm/Cancel** based on actual needs.

7.3 User Management

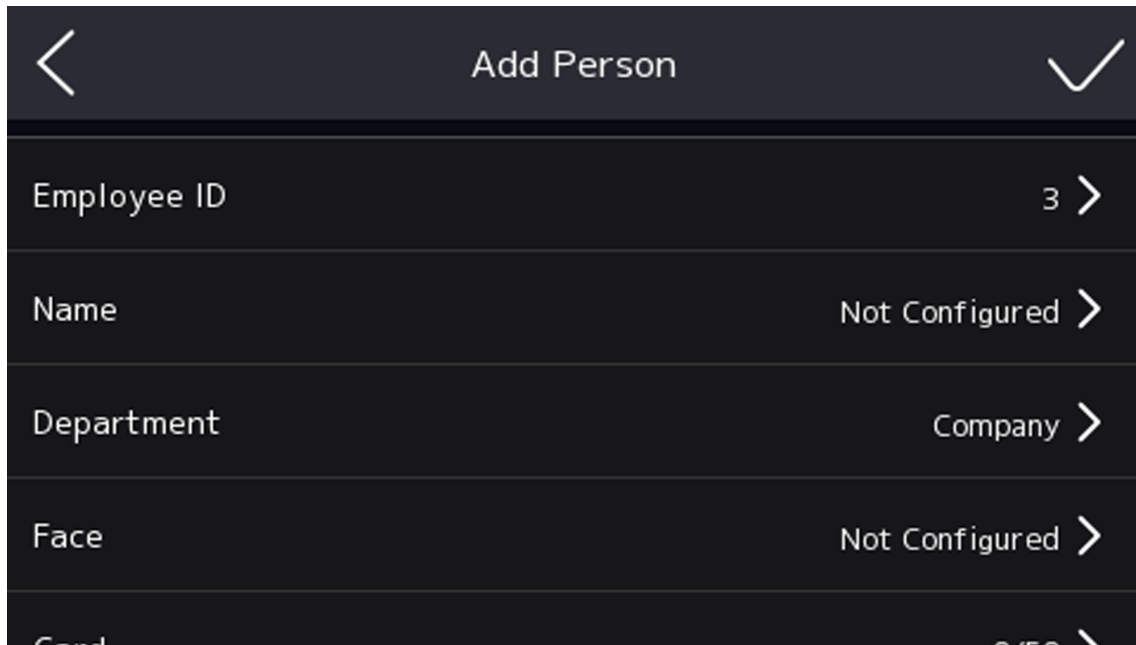
On the user management interface, you can add, edit, delete and search the user.

7.3.1 Add Administrator

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

Steps

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



3. Edit the employee ID.

 Note

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

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

 Note

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

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

 Note

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

- **Note**

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

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

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



Note

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

7. Enable the Administrator Permission function.

Enable Administrator Permission

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

8. Tap  to save the settings.

7.3.2 Add Face Picture

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

Steps



Note

Up to 1500 face pictures can be added.

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



Note

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

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



Note

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

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

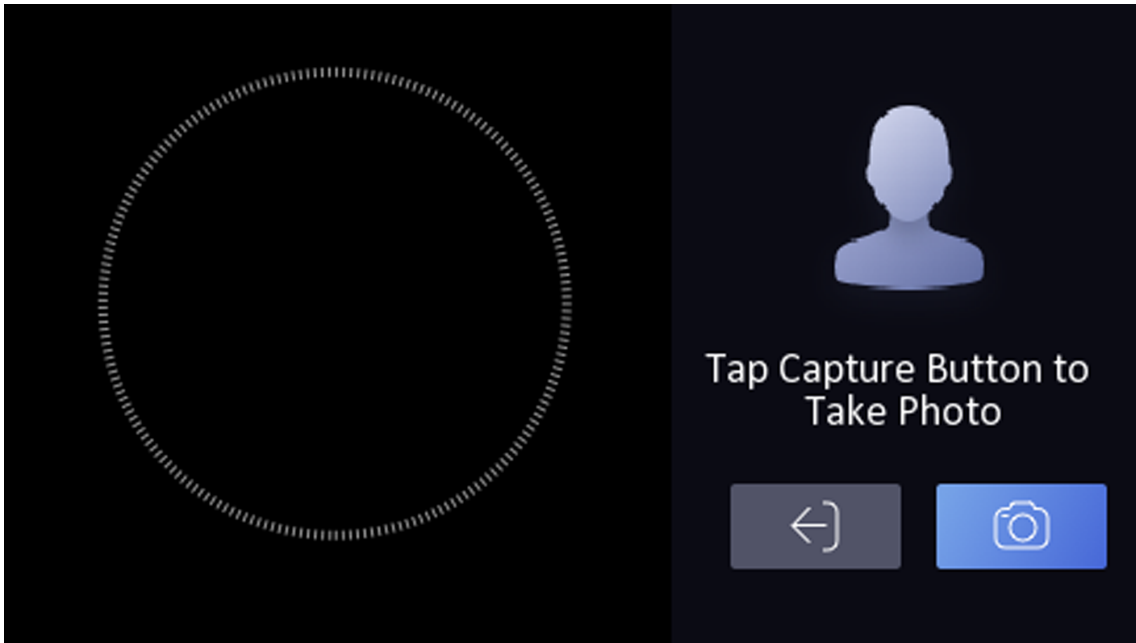


Figure 7-9 Add Face Picture

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.

7.3.3 Add Fingerprint

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

Steps

Note

- The function should be supported by the device.
 - Up to 3000 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 and select department.
-

Note

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

7.3.4 Add Card

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

Steps



Up to 3000 cards can be added.

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



- 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 and select department.
-



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

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



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

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

Administrator

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

Normal User

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

10. Tap  to save the settings.

7.3.5 Add PIN

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

Before You Start



Make sure the password mode is **Local Password** or **Platform Password**. If you select **Local Password**, you can add PIN on the device or Web. If you select **Platform Password**, you cannot add PIN on the device or Web, instead, you should add PIN on the platform. For details about setting the password mode, see [***Authentication Settings***](#).

Steps

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



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

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



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

5. Tap the PIN code and create a PIN for the user.
-



Make sure the password mode is **Local Password**, or the PIN area cannot be edited.

6. Set the user role.
-

Administrator

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

Normal User

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

7. Tap  to save the settings.

7.3.6 Set Person Type via Device

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

Before You Start

Login the device. For details, see [Login](#) .

Steps

1. Tap **Person** → +.

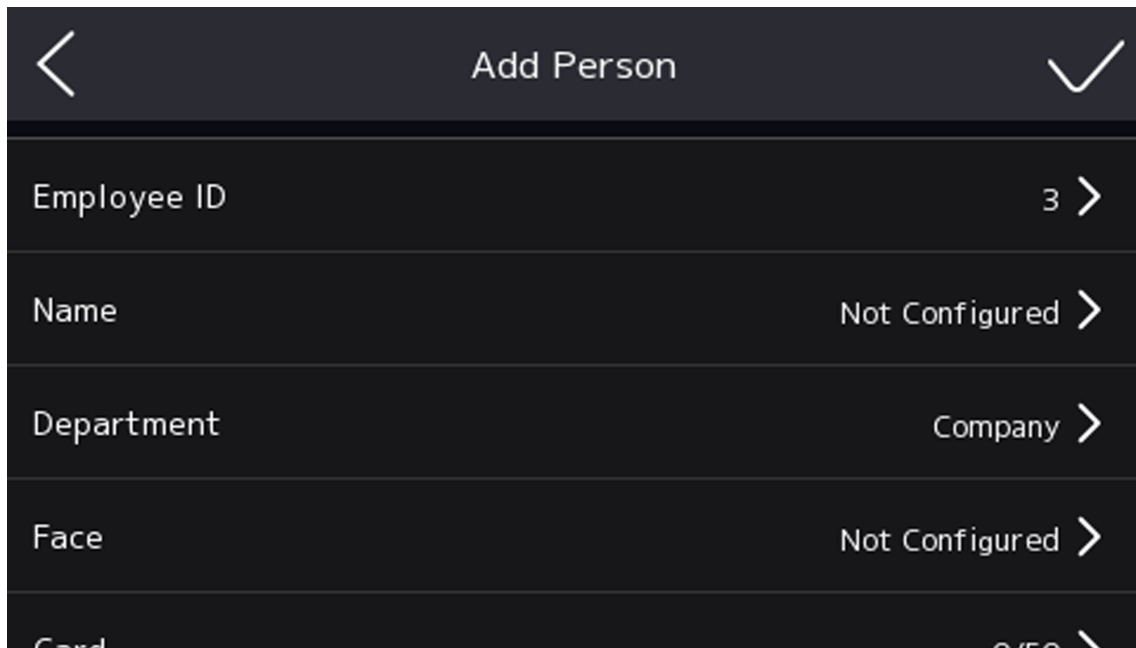


Figure 7-10 Add Person

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



Note

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

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



Note

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

4. Set the face, card, fingerprints.
-



Note

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

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



Note

- When setting the person to visitor, administrator cannot be set. When setting the person to person in blocklist, the door permission cannot be configured.
- You should set the name of the custom type on PC web. After naming the custom type, the custom type on the device will be change to the named one. For detailed settings, see **Person Management** .

-
6. Tap to save the settings.
-

7.3.7 Set Authentication Mode

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

Steps

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

Device

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

Custom

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

4. Tap to save the settings.

7.3.8 Search and Edit User

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

Search User

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

Edit User

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



Note

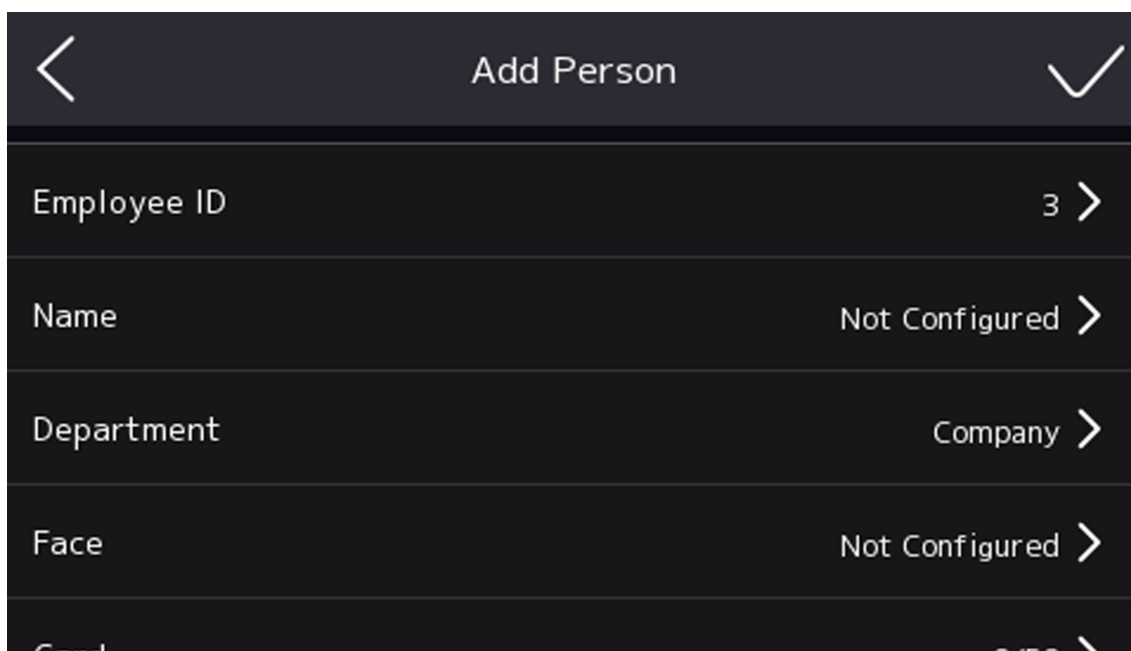
The employee ID cannot be edited.

7.3.9 Check Attendance Only

You can set person as **Check Attendance Only**. The person will have no authentication and door permission

Steps

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



Add Person	
Employee ID	3 >
Name	Not Configured >
Department	Company >
Face	Not Configured >
Card	0/50 >

3. Enable **Check Attendance Only**.

7.4 Platform Attendance

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

Note

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

7.4.1 Disable Attendance Mode via Device

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

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

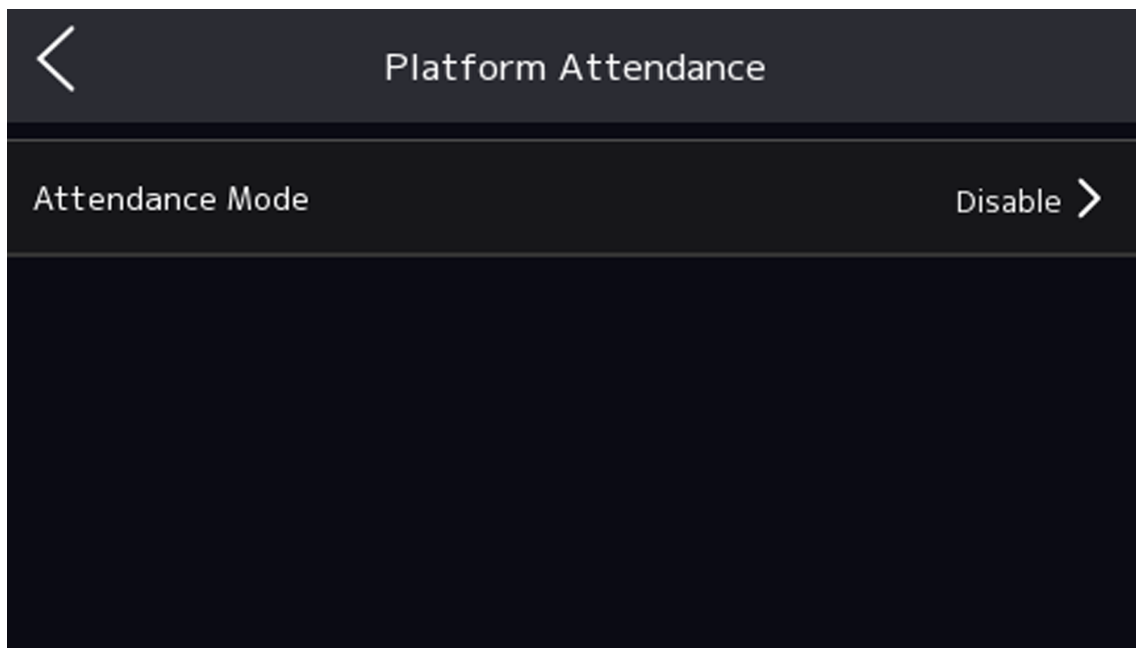


Figure 7-11 Disable Attendance Mode

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

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

7.4.2 Set Manual Attendance via Device

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

Before You Start

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

Steps

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

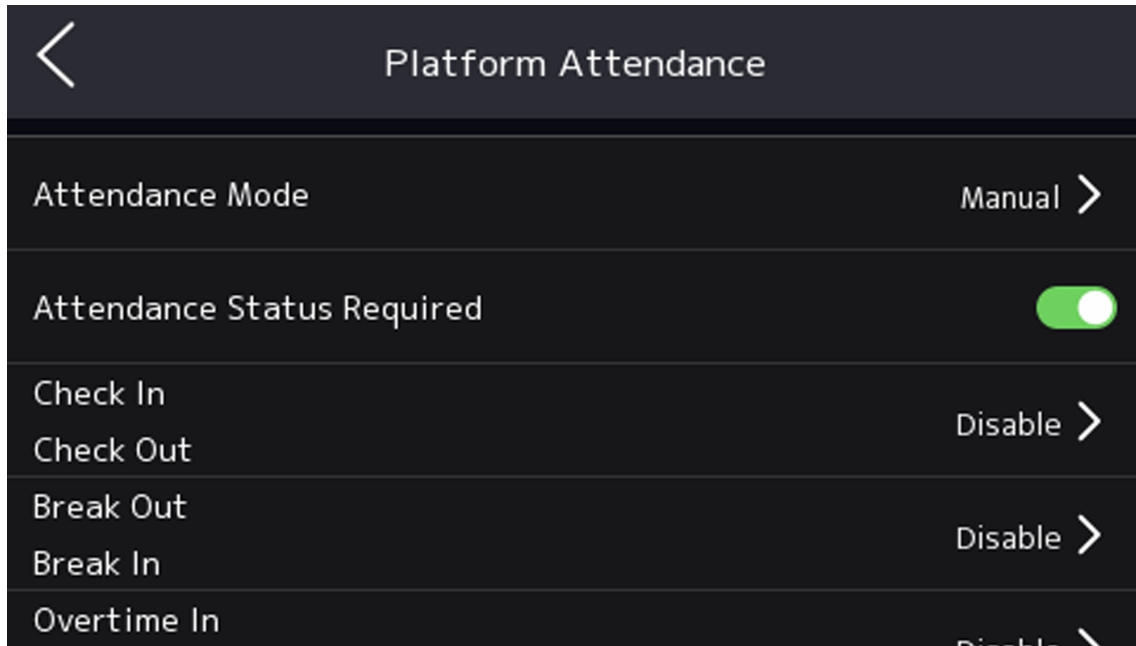


Figure 7-12 Manual Attendance Mode

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



Note

The Attendance Property will not be changed.

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

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

Result

You should select an attendance status manually after authentication.



Note

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

7.4.3 Set Auto Attendance via Device

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

Before You Start

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

Steps

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

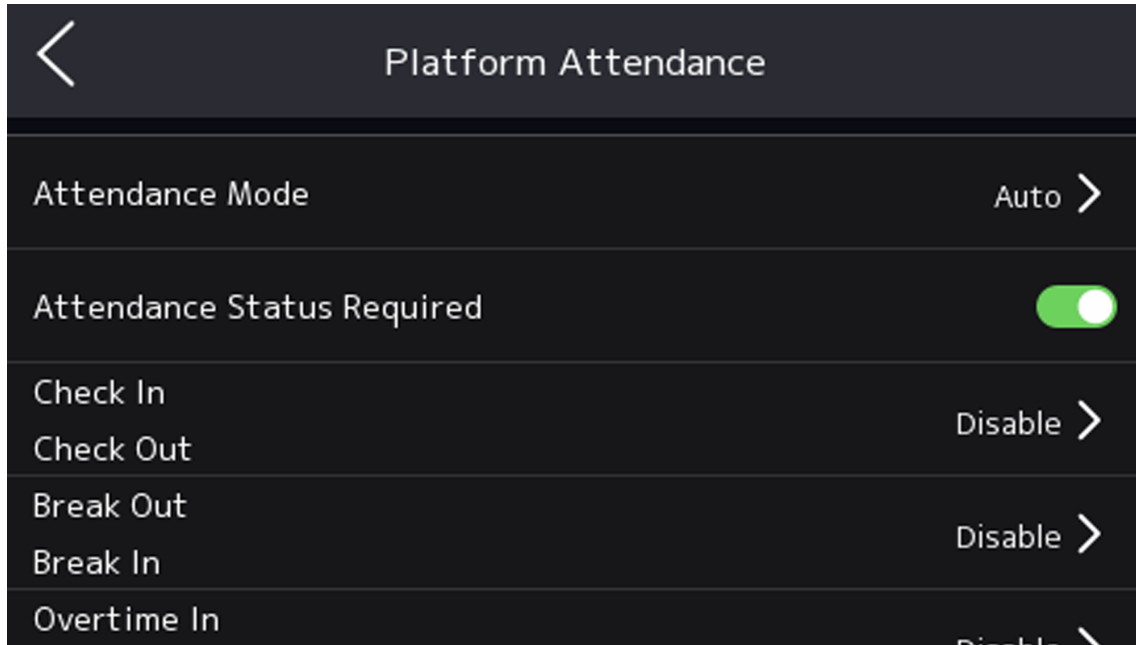


Figure 7-13 Auto Attendance Mode

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



Note

The Attendance Property will not be changed.

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

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

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



Note

The attendance status will be valid within the configured schedule.

Result

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

Example

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

7.4.4 Set Manual and Auto Attendance via Device

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

Before You Start

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

Steps

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

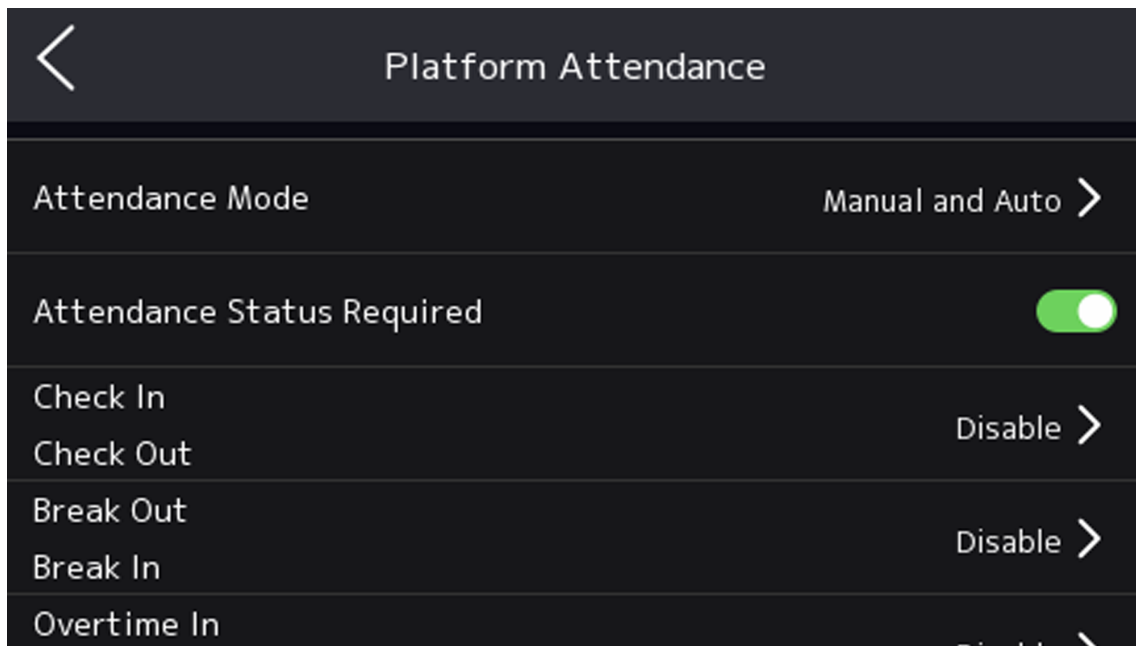


Figure 7-14 Manual and Auto Mode

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



Note

The Attendance Property will not be changed.

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

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

6. Set the status' schedule.

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



Note

The attendance status will be valid within the configured schedule.

Result

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

Example

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

7.5 Data Management

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

7.5.1 Delete Data

Delete user data.

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

7.5.2 Import Data

Steps

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



Note

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

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



Note

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

7.5.3 Export Data

Steps

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



Note

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

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



Note

- The supported USB flash drive format is DB.
- The system supports the USB flash drive with the storage of 1 G to 256 G. Make sure the free space of the USB flash drive is more than 512M.
- The exported file is in ZIP format and can be directly viewed on a computer.

7.6 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.

7.6.1 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.



Note

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

QR Code

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



Note

Authentication via QR code should be supported by the device.

Password

Enter the password to authenticate via password.

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

7.6.2 Authenticate via Multiple Credential

Before You Start

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

Steps

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



Note

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

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



Note

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

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

7.7 Basic Settings

You can set the sound, time, sleeping (s), language, community No., building No., Unit No., privacy and video standard.

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

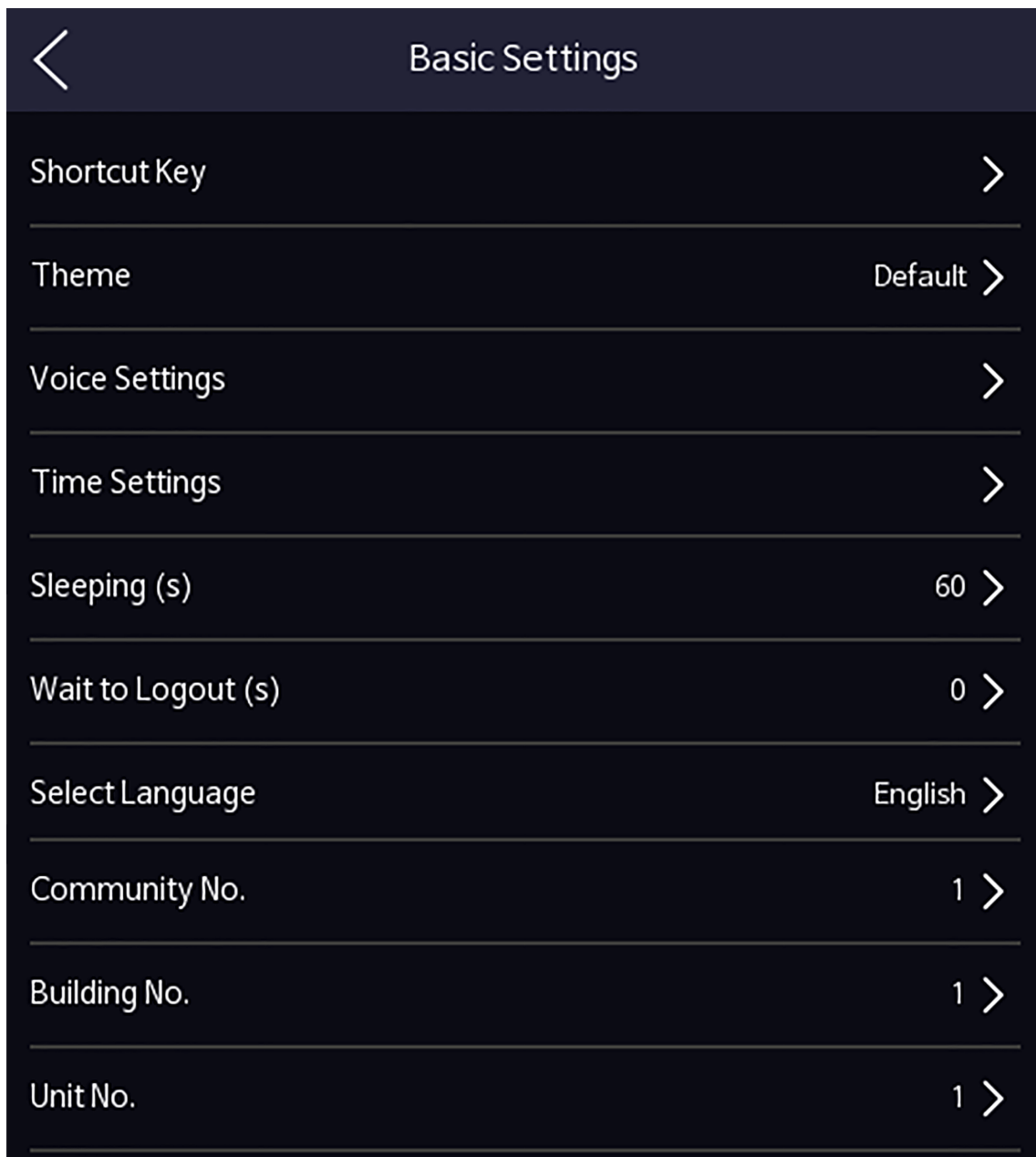


Figure 7-15 Basic Settings Page

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. 0 refers to silence.

Time Settings

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

Sleeping (s)

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



Note

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

Select Language

Select the language according to actual needs.

Community No.

Set the device installed community No.

Building No.

Set the device installed building No.

Unit No.

Set the device installed unit No.

Privacy

Name/Employ ID

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

Face Picture

You can choose to display/not display face picture when authenticating.

Save Registered Picture

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

Save Picture When Authenticating

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

Upload Picture When Authenticating

Upload the pictures captured when authenticating to the platform automatically.

Video Standard

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

PAL(50HZ)

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

NTSC(60HZ)

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

7.7.1 Enable/Disable Voice Prompt via Device

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

Login the device. For details, see [Login](#) .

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

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

7.7.2 Set Device Time via Device

Set the device time.

Login the device. For details, see [Login](#) .

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

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

7.7.3 Set Sleep Duration via Device

Set the device sleeping waiting time.

Login the device. For details, see [Login](#) .

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

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



Note

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

7.7.4 Select Language

Login the device. For details, see [Login](#) .

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

The device will reboot after changing the language.

7.7.5 Set Device Number via Device

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

Login the device. For details, see [Login](#) .

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

7.7.6 Set Beauty via Device

You can enable the beauty function and set the smooth and the whiten parameter.

Login the device. For details, see [Login](#) .

Tap **System Settings** → **Basic** → **Beauty**.

Enable the beauty function and set the smooth and the whiten parameter. Tap + or - to control the effect strength.

7.7.7 Call Settings

You can set call parameters.

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 **System Settings** → **Basic** .
2. Tap **Call Settings**.
3. Set call parameters.

Call Settings

Automatic Calling After Dialing

You can enable **Automatic Calling After Dialing**, and set timeout period.

Calling Target of Call Center Button

Select calling target.

VoIP Server

Select VoIP server.

7.7.8 Set Privacy Parameters via Device

Set the picture uploading paramters.



Note

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

Login the device. For details, see [Login](#) .

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

Authentication Settings

Name / Employee ID / Face Picture

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

Picture Uploading and Storage

Set picture uploading and storage parameters.

Save Registered Pic.

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

Save Pic. After Linked Capture

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

Upload Pic. After Linked Capture

Upload the pictures captured after linked capture.

Save Pic When Auth.

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

Upload Pic. When Auth.

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

7.7.9 Set Video Standard

Set video standard for the live view.

Login the device. For details, see [Login](#).

Go to **System** → **Basic** → **Video Standard**.

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

PAL (50HZ)

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

NTSC (60HZ)

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

7.7.10 Set Secure Door Control Unit Parameters

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

Before You Start

Device is wiring the secure door control unit by RS-485. For detailed wiring method, see [Wiring](#).

Steps

1. Login the device. For details, see [Login](#).

2. Go to **System → Basic → Secure Door Control Unit**.

3. Select **Door 1** or **Door 2** as door No.

**Note**

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

7.8 Set Biometric Parameters

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

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

Table 7-1 Face Picture Parameters

Parameter	Description
Face Liveness Level	After enabling face anti-spoofing function, you can set the matching security level when performing live face authentication.
Recognition Distance	Set the valid distance between the user and the camera when authenticating.
Face Recognition Interval(s)	The time interval between two continuous face recognitions when authenticating. Note You can input the number from 1 to 10.
Face 1:N Security Level	Set the matching threshold when authenticating via 1:N matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate.
Face 1:1 Security Level	Set the matching threshold when authenticating via 1:1 matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate.
ECO Mode Settings	After enabling the ECO mode, the device will use the IR camera to authenticate faces in the low light or dark environment. And you can set the ECO mode threshold, ECO mode (1:N), ECO mode (1:1). ECO Mode Threshold

Parameter	Description
	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
Mask Settings	After enabling the mask detection function, the system will recognize the captured face with mask picture. You can set Face with Mask & Face (1:1), Face with Mask & Face (1:N), ECO (1:1) Threshold, ECO Mode (1:N) Threshold, and Prompt Method. 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 & Face (1:N) Set the matching value 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. ECO Mode (1:1) Threshold 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. ECO Mode (1:N) Threshold Set the matching value 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. Prompt Method Set the None, Reminder of Wearing and Must Wear 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.

Parameter	Description
	Must Wear If the person do not wear a face mask when authenticating, the device prompts a notification and the door keeps closed. None If the person do not wear a face mask when authenticating, the device will not prompt a notification.
Multiple Faces Authentication	After multiple faces authentication is enabled, multiple faces authentication is supported.

7.9 Change Device Password

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

Steps

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



Note

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

4. Enter new password and confirm the password.



Caution

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

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

5. Tap **OK**.
-

7.10 Authentication Settings

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

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

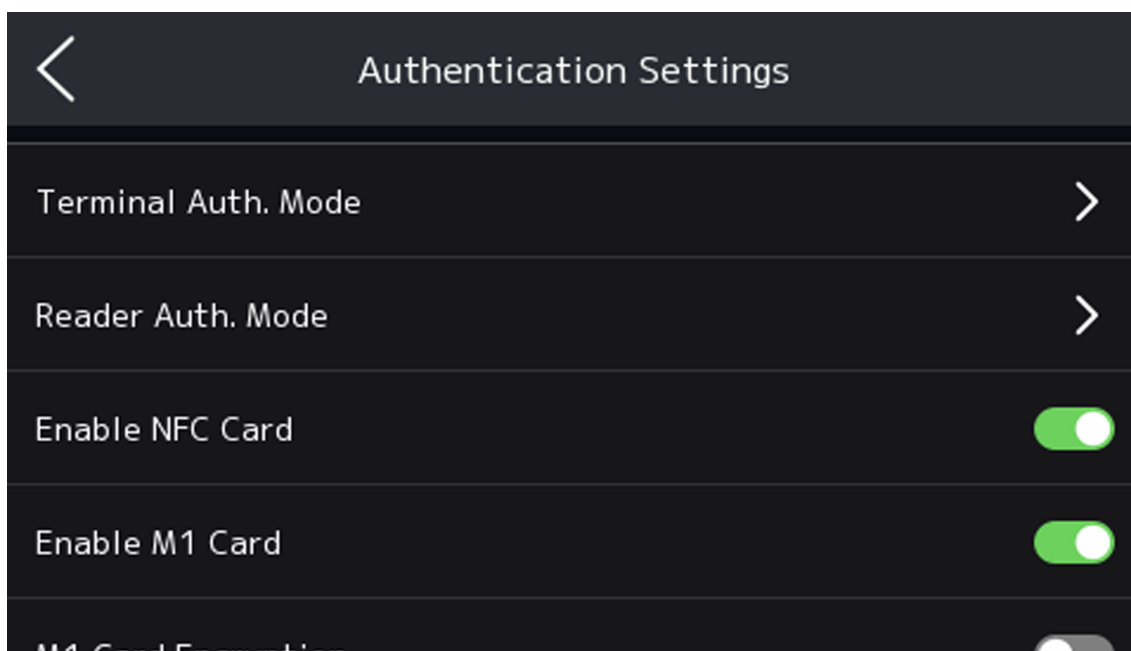


Figure 7-16 Authentication Settings

The available parameters descriptions are as follows:

Table 7-2 Access Control Parameters Descriptions

Parameter	Description
Terminal Auth. Mode (Terminal Authentication Mode)	Select the face recognition terminal's authentication mode. You can also customize the authentication mode.

Parameter	Description
	 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.
Reader Auth. Mode (Card Reader Authentication Mode)	Select the card reader's authentication mode.
Enable NFC Card	Enable the function and you can present the NFC card to authenticate.
Enable M1 Card	Enable the function and you can present the M1 card to authenticate.
M1 Card Encryption	Enabling the M1 card encryption function can improve the card security level. The card will not be copied easily.
Door Contact	You can select "Open (Remain Open)" or "Close (Remian Closed)" according to your actual needs. By default, it is Close (Remian Closed).
Open Duration	Set the door unlocking duration. If the door is not opened for the set time, the door will be locked. Available door locked time range: 1 to 255s.
Authentication Interval	Set the device authenticating interval. Available authentication interval range: 0 to 65535.
Authentication Result Display Duration (s)	Set the authentication result displaying time duration after authentication.
Password Mode	Platform-Applied Personal PIN The PIN is managed and distributed by the platform. You cannot set the PIN on the device or Web. Device-Set Personal PIN The PIN is set on the device or Web. You cannot set the PIN on other platform.

7.10.1 Set Terminal Authentication Mode via Device

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

Login the device. For details, see [Login](#) .

Tap **ACS → Terminal Auth. Mode** .

Select person authentication type and method and save the settings.

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



Note

Device with fingerprint module supports fingerprint function.



Caution

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

7.10.2 Set Reader Authentication Mode via Device

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

Login the device. For details, see [Login](#) .

Tap **ACS → Reader Auth. Mode** .

Select person authentication type and save the settings.

Select person authentication type and method and save the settings.

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



Note

Device with fingerprint module supports fingerprint function.



Caution

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

7.10.3 Manually Trigger Face Authentication via PC Web

After enabling Manually Trigger Authentication via Face, you need to touch the screen of the device manually for face recognition.

Login the device. For details, see [Login](#) .

Tap **ACS**.

Enable **Manually Trigger Authentication via Face**, and set **Authentication** as **Single** or **Continuous Single**

The person should tap **Authentication** on the authentication page manually to trigger recognition before each face recognition.

Continuous

After triggering the recognition, you can recognize via face until the device enter into the sleeping mode.

7.10.4 Enable/Disable NFC Card

Enable/disable NFC card function.

After login, tap **ACS**.

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



Note

When the dual-frequency card module access to the face recognition terminal, swiping the card on the device is invalid.

7.10.5 Enable/Disable M1 Card

Enable or disable M1 card function.

Login the device. For details, see [Login](#) .

After login, tap **ACS**.

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

Enable M1 Card

After enabling, the device can read M1 card.

M1 Card Encryption

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

Note

When the dual-frequency card module access to the face recognition terminal, swiping the card on the device is invalid.

7.10.6 Remote Authentication

Judge the authentication passes or not by remote platforms.

Login the device. For details, see [Login](#) .

Tap **ACS**.

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

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

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

7.10.7 Set Authentication Interval via Device

Login the device. For details, see [Login](#) .

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

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

Available authentication interval range: 0 to 65535.

7.10.8 Set Authentication Result Display Duration via Device

Set the authentication result display duration when authenticating.

Login the device. For details, see [Login](#) .

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

7.10.9 Set Password Mode

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

Steps

1. Login the device. For details, see [Login](#) .
2. Tap **ACS**.
3. Tap **Password Mode** and set the mode.

Platform-Applied Personal PIN

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

Device-Set Personal PIN

The PIN is set on the device or PC Web.

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

7.10.10 Door Parameter Configuration

Configure parameters for unlocking doors.

Set Door No. via Device

Select a door No. for the device.

Login the device. For details, see [Login](#) .

After login, tap **ACS**.

Tap **Door No.**. Select **Door 1** or **Door 2**.

The door 1 means the device installed at the entrance. Door 2 means the device installed at the exit.

Set Door Contact via Device

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

Login the device. For details, see [Login](#) .

Tap **ACS**.

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

Set Open Duration via Device

Set the door unlocking duration.

Login the device. For details, see [Login](#) .

Tap **ACS**.

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

7.11 Preference Settings

You can configure preference settings parameters.

Steps

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

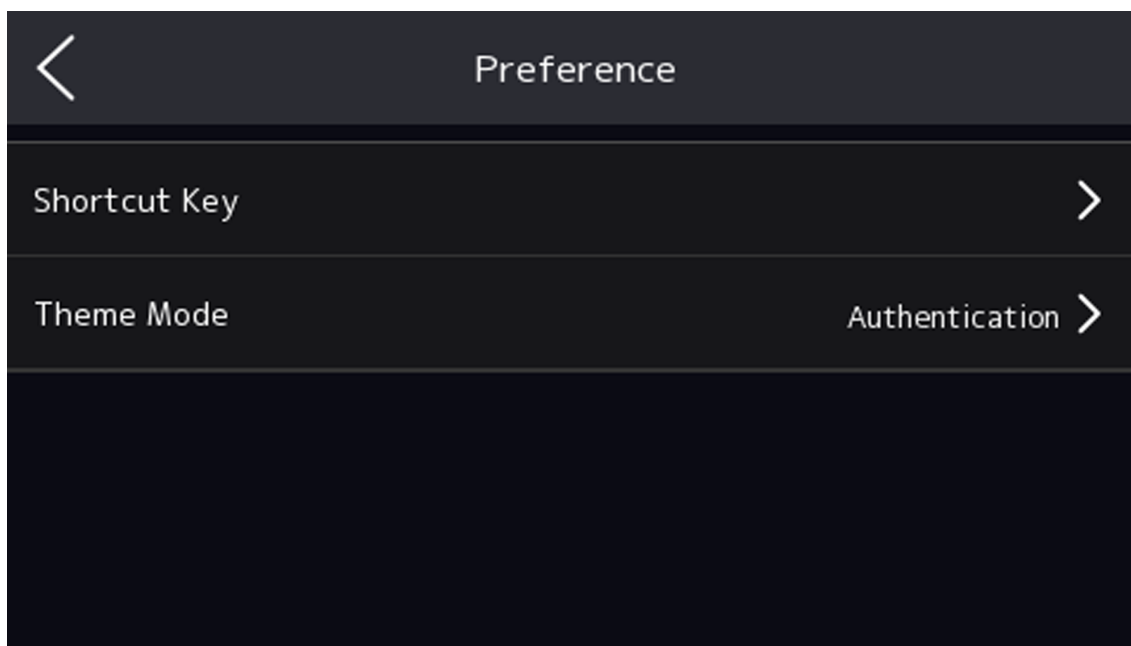


Figure 7-17 Preference Settings

7.11.1 Set Shortcut Key via Device

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

Login the device. For details, see [Login](#) .

Tap **System Settings** → **Preference**.

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

Password

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

QR Code

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

Call

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

Tap  on the authentication page to call.

Call Indoor Station No.

After enabling, the Indoor Station No. will be displayed on the authentication page.

Call Management Center/Call VoIP Center

After enabling, you can call Management Center or VoIP Center on the authentication page.

7.11.2 Theme

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

Login the device. For details, see [Login](#) .

System Settings → Preference.

Select a theme mode.

Authentication

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

Advertisement

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

Intercom Mode

After selecting this mode, the shortcut will be displayed on the bottom of the authenticating page.

7.12 System Maintenance

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

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

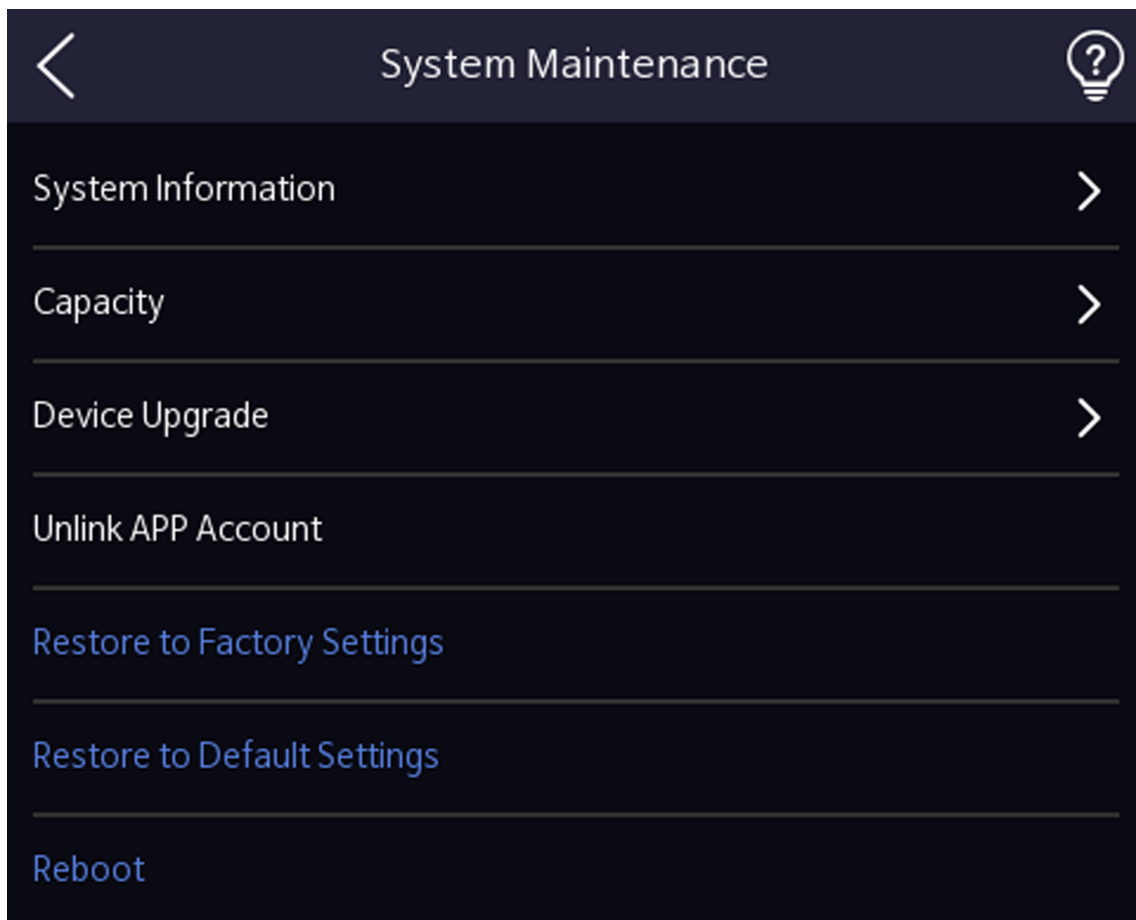


Figure 7-18 Maintenance Page

System Information

You can view the device information including device model, serial No., firmware version, MAC address, production data, and license.



Note

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

Long tap , and enter admin password to view device version information.

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.

Capacity

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



Note

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

Device Upgrade

Online Update

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

Update via USB

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

User Manual

Scan the QR code to view the device user manual.

Restore to Factory Settings

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

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.

Reboot

The device will reboot after the confirmation.

Chapter 8 Configure the Device via the Mobile Web

8.1 Login

You can login via mobile browser.



- Parts of the model supports Wi-Fi settings.
 - Make sure the device is activated.
 - Make sure the device and the mobile phone are in the same Wi-Fi.
-

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

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

8.2 Overview

You can view the door status, real-time event, network status, and basic information, and set person management, event search, and door parameters via shortcut entry.

Function Descriptions:

Door Status



The door status is open/closed/remaining open/remaining closed. You can tap to select open/closed/remaining open/remaining closed status according to your actual needs.

Shortcut Entry

You can set person management, smart settings, authentication settings, and door parameters via shortcut entry.

Network Status

You can view the connected and registered status of network.

Basic Information

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

Real-Time Event

You can view real-time event details.

8.3 Forget Password

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

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

Select **Verification Mode**.

Security Question Verification

Answer the security questions.

E-mail Verification

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

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

8.4 Configuration

8.4.1 View Device Information

View the device name, language, model, serial No., version, IO input number, IO output number, local RS-485 number, alarm input number, alarm output number, register number, factory information, device capacity, etc.

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

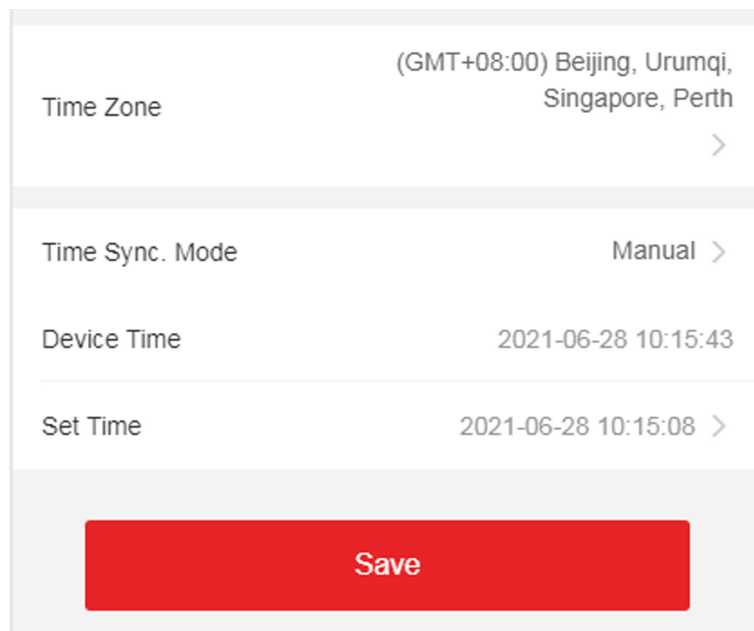
View the device name, language, model, serial No., version, IO input number, IO output number, local RS-485 number, alarm input number, alarm output number, register number, factory information, device capacity, etc.

Tap **Save**.

8.4.2 Time Settings

Set the time zone, time sync. mode, and displayed time.

Tap  → **System Settings** → **Time Settings** to enter the settings page.



Time Zone	(GMT+08:00) Beijing, Urumqi, Singapore, Perth >
Time Sync. Mode	Manual >
Device Time	2021-06-28 10:15:43
Set Time	2021-06-28 10:15:08 >
Save	

Figure 8-1 Time Settings

Tap **Save** to save the settings.

Time Zone

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

Time Sync. Mode

Manual

By default, the device time should be synchronized manually. You can set the device time manually.

NTP

Set the NTP server's IP address, port No., and interval.

8.4.3 Set DST

Steps

1. Tap  → **System Settings** → **Time Settings** , to enter the settings page.

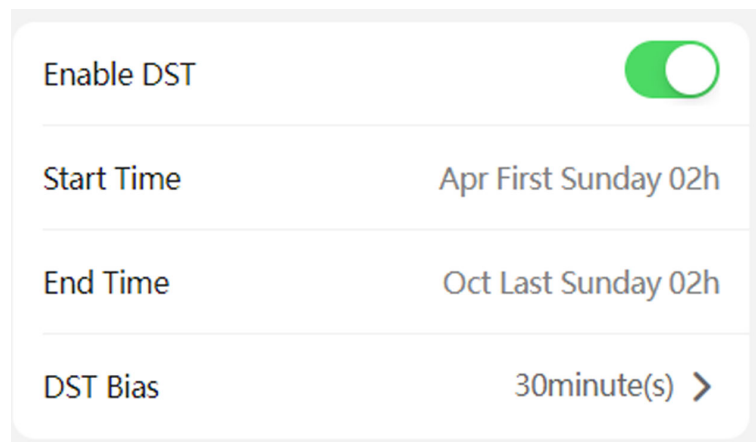


Figure 8-2 DST

2. Tap **Enable DST**.
3. Set the start time, end time, and DST bias.
4. Tap **Save**.

8.4.4 User Management

Steps

1. Tap  → **User Management** → **User Management** → **admin** to enter the setting page.
2. Enter the old password and create a new password.
3. Confirm the new password.
4. Tap **Save**.

Note

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using 8-16 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.

8.4.5 Network Settings

Wired Network

Set wired network.

Tap  → **Communication Settings** → **Wired Network** to enter the configuration page.

DHCP

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

If you enable 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. Tap  → **Communication Settings** → **Wi-Fi** to enter the settings page.
2. Enable **Wi-Fi**.

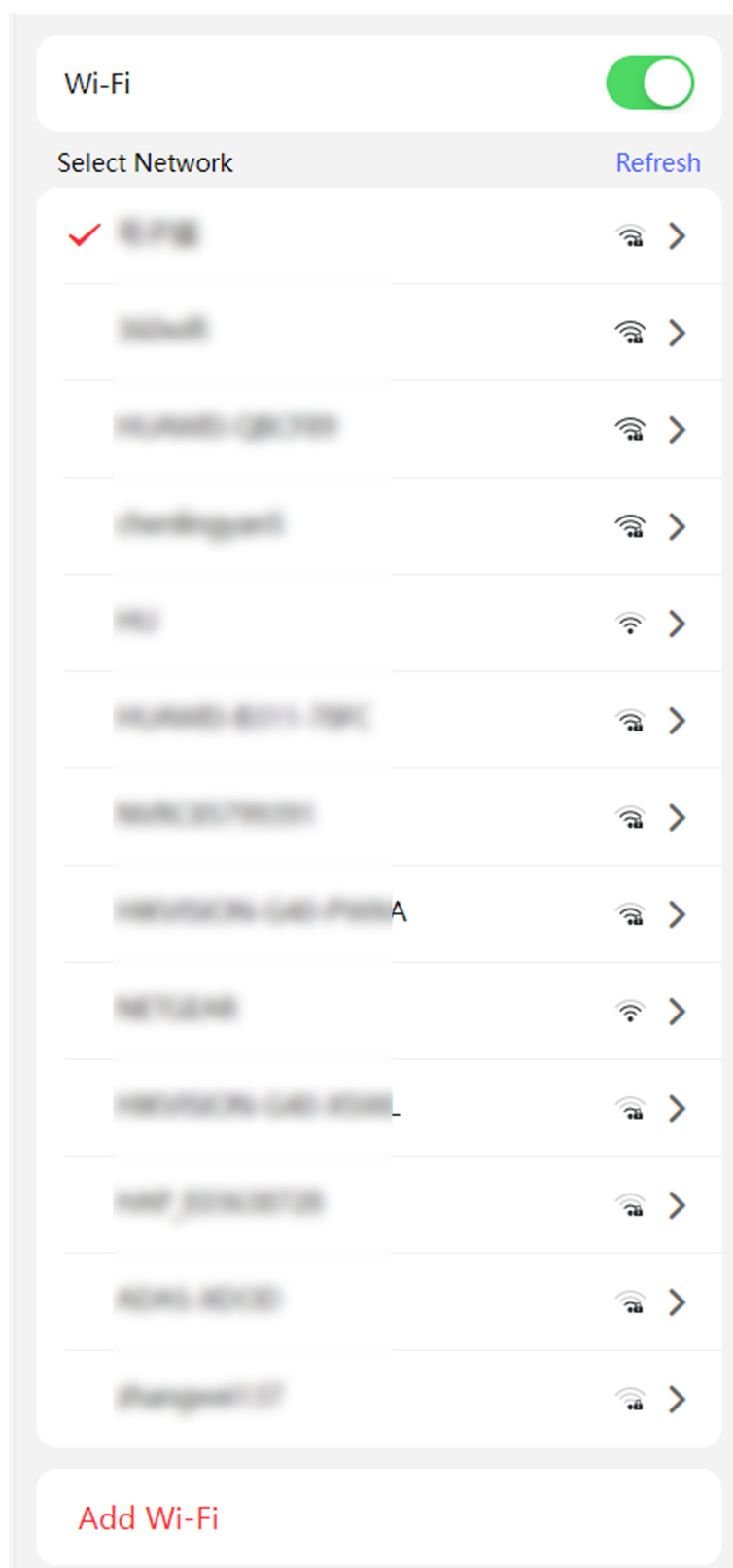


Figure 8-3 Wi-Fi

3. Add Wi-Fi.

- 1) Tap **Add Wi-Fi**.
- 2) Enter **Wi-Fi Name** and **Wi-Fi Password**, and select **Encryption Type**.
- 3) Tap **Save**.

4. Select the Wi-Fi name, and tap **Connect**.

5. Enter the password and tap **Save**.

Set Port Parameters

You can set the HTTP, HTTPS and Websocket(s) according to actual needs when accessing the device via network.

Tap  → **Network Service** → **HTTP(S)** , to enter the settings page.

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.

Tap  → **Network Service** → **Websocket(s)** , to enter the settings page.

You can view the Websocket(s) port No.

Platform Access

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

Steps

1. Tap  → **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. You can enable **Custom** to enter the server address.



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.
- The verification code cannot be **123456** or **abcdef** (case non-sensitive0).

4. You can view **Network Connection Status** and **Binding Status**.
5. You can set **Network Connection Priority**.
6. Tap **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. Tap  → **Device Access** → **ISUP** to enter the settings page.
2. Enable **ISUP**.
3. Set the ISUP version, server Address, port, device ID and encryption key.



Note

If you select 5.0 as the version, you should set the encryption key as well.

4. You can view **Registration Status**.
5. You can set **Network Connection Priority**.
6. Set the ISUP listening parameters, including ISUP alarm center IP address/domain name, ISUP alarm center URL, and ISUP alarm center port.
7. Tap **Save** to save the settings.

Set OTAP

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

Steps

1. Tap  → **Device Access** → **OTAP** to enter the settings page.
2. Tap **Enable OTAP**.
3. Set **Server Address**, **Port**, **Device ID** and **Encryption Key**.
4. Tap **Test** to ensure the device can connect to the server and register successfully. Refresh the page or restart the device to see the **Register Status**.
5. Tap **Save**.

8.4.6 Access Configuration

Set RS-485 Parameters

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

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

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

Peripheral Type

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



Note

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

RS-485 Protocol

Private

The device can connect with the third party device via RS-485.

OSDP

Standard RS-485 protocol.

RS-485 Address

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



Note

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

Baud Rate

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

Data Bit

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

Stop Bit

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

Parity/Flow Ctrl/Communication Mode

Enabled by default.

8.4.7 User Management

You can add, edit, delete, and search users via mobile Web browser.

Steps

1. Tap  → **Person Management** to enter the settings page.
2. Add user.
 - 1) Tap+.
 - 2) Set the following parameters.

Employee ID

Enter the employee ID. The Employee ID cannot be 0 or exceed 32 characters. It can be a combination of uppercase, lowercase letters and numbers.

Name

Enter your name. The name supports numbers, uppercase and lowercase English, and characters. The name is recommended to be within 32 characters.

Person Role

Select your person role.

Person Type

Select your person type.

Attendance Check Only

After enabling, this person won't be given access control permission.

Face

Add Face picture. Tap **Face**, then tap **Camera** to add face or tap **Choose from Album** to import the face.

Fingerprint

Add fingerprint. Tap **Fingerprint**, then tap **+**, and add fingerprint via the fingerprint module.

Card

Add card. Tap **Card**, then tap **+**, enter the card No. and select card type.

PIN

Edit or view PIN.



Note

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

Gender

Select gender.

Long-Term Effective User

Set the user permission as long-term effective.

Start Date/End Date

Set **Start Date** and **End Date** of user permission.

Authentication Type

Same as Device

If you want to select device mode, you should set the terminal authentication mode in Access Control Settings page first.

Custom

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

3) Tap **Save**.

3. Optional: Tap **Management** to manage person.

4. Optional: You can search the user by entering the employee ID or name in the search bar.

8.4.8 Device Management

Auto Search Device

The system can automatically search for online and offline devices that have been connected to the face recognition terminal.

Tap  → **Device Management** → **Add** → **Auto Search Device**. The searched online and offline devices that have been connected to the face recognition terminal will be displayed in the list of the page.

8.4.9 Search Event

Tap  → **Event Search** to enter the Search page.

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



Note

Support searching for names within 32 digits.

8.4.10 Access Control Settings

Set Authentication Parameters

Set Authentication Parameters.

Steps

1. Tap  → **Access Control** → **Authentication Settings**.

2. Tap **Save**.

Terminal

You can select the terminal as main or sub, and set corresponding parameters.

Terminal Name

Set the terminal name.

Terminal Model

Get terminal model. It is read-only.

Authentication

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

Continuous Face Recognition Interval (s)

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

Authentication Interval

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

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

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

Enable Tampering Detection

Enable the anti-tamper detection for the card reader.

Enable Card No. Reversing

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

Communication with Controller Every (s)

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

Max. Interval When Entering Password (s)

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

Set Door Parameters

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

Select the corresponding door and edit the door parameters. Tap **Save** to save the settings after the configuration. You can tap **Save and Sync. to All**.

Door Name

You can create a name for the door.

Area

Select the area.

Open Duration

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

Door Opening Timeout Alarm Threshold

Set the Door Opening Timeout Alarm Threshold, an alarm will be triggered if the door has not been closed within the configured time duration.

Exit Button Type

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

Door Remain Open Duration with First Person (min)

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.

Super Password

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



Note

The duress code and the super code should be different. And the digit ranges from 4 to 8.

Terminal Parameters

You can set terminal parameters for accessing.

Tap  → **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.

Remote Verification

After enabling the **Remote Verification**, when authenticating, the device will upload authentication information to the platform, and the platform will confirm whether to open the door.

Verify Credential Locally

After enabling the function, the device will check permission but not estimate the plan template.

Timeout Period

You can set remote authentication timeout period.

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

Face Parameters Settings

Set Face Parameters.

Face Parameters Settings

Tap  → Smart → Face Recognition Parameters .

Face Anti-spoofing

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

Live Face Detection Security Level

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

1:1 Matching Threshold

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

1:N Matching Threshold

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

Face Recognition Timeout Value (s)

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

Fingerprint Parameters

Tap  → Smart → Fingerprint Parameters .

Fingerprint Security Level

You can set the security level of fingerprint. The higher the security level you set, the lower the False Acceptance Rate (FAR) will be. The higher the security level you set, the lower the False Rejection Rate (FRR) will be.

Face Mask Detection Parameters

Face with Mask Detection

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

None

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

Reminder of Wearing

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

Must Wear

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

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.



Note

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

Tap **Save** to save the settings.

Set Card Security

Tap  → **Access Control** → **Card Security** to enter the configuration page.

Set the parameters and tap **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

M1 card encryption can improve the security level of authentication.

Sector

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

Enable EM Card

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



Note

EM card is supported when the device connects a peripheral card reader that supports presenting EM card.

Enable DESFire Card

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

Enable FeliCa Card

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

Set Privacy Parameters

Set the display settings, picture upload and storage parameters.

Tap  → **Access Control** → **Privacy Settings** .

Event Storage Settings

Delete Old Events Periodically

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

Picture Display/Name Display/Employee ID

You can tap to enable Picture, Name, or Employee ID to display. When authentication is completed, the system will display the selected contents in the result.

Name De-identification

The name information is desensitized with an asterisk.

Picture Uploading and Storage

You can upload and store pictures.

Save Registered Picture

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

Save Picture When Auth.

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

Upload Captured Picture When Auth.

Upload the pictures captured when authenticating 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.

Upload Picture After Linked Capture

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

PIN Mode

Device-Set Personal PIN

It can be created or edited on the device or on the web, and cannot be set on other platforms.

Platform-Applied Personal PIN

It can be created or edited on the platform, and issued to the device before it can be used. It cannot be set on the device or on the web.

Clear All Pictures in Device

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

Password Settings

Set public password.

Tap  → **Access Control** → **Password Settings** to enter the page.

Tap **Add** to add password.

Set password and remarks and click to enable electric lock.

Tap **Save** to save the settings.

8.4.11 Call Settings

Device ID Settings

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

Steps

1. Tap  → **Call Settings** → **No. Settings** .
2. Set the following parameters.

Device Type

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



Note

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

Period No.

Set the device period No.

Building No.

Set the device building No.

Unit No.

Set the device unit No.



Note

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

Floor No.

Set the device installed floor No.

Door Station No.

Set the device installed floor No.



Note

- If you change the No., you should reboot the device.
 - The main door station No. is 0, and the sub door station No. ranges from 1 to 16.
-

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

Outer Door Station No.

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



Note

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

Period No.

Set the device period No.

Session Settings

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

Steps

1. Tap  → **Call Settings** → **Session Settings** .
2. Set registration password, main station IP, private server IP and enable Protocol 1.0.

Registration Password

Activation password of the main station.

Main Station IP

IP address of the main station.

Private Server IP

IP address of the private server.

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. Tap **Save**.

Time Duration Settings

Set the Max. call duration.

Tap  → **Call Settings** → **Call Settings** .

Set the Max. communication time. Tap **Save**.



Note

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

Number Settings

You can call the room SIP to call the room.

Steps

1. Tap  → **Call Settings** → **Number Settings** .
2. Tap +, enter the **Room No.** and **SIP Number**.
3. Tap **Save**.

Press Button to Call

Steps

1. Tap  → **Call Settings** → **Press Button to Call** .
2. Tap **Call** or **Call Center** as your needs.

8.4.12 Audio Settings

Steps

1. Tap  → **Audio** .

2. Optional: Set input and output volume.

8.4.13 Custom Home Page

You can set home page mode.

Steps

1. Tap  → **Preference** → **Custom Home Page** .
2. Select **Home Page Mode**.

Access 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.

Intercom Mode

The authentication interface displays a quick operation area and an authentication area. The quick operation area supports customizable shortcut keys for functions.

Simple

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

3. Tap **Save**.

8.4.14 Upgrade and Maintenance

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

View Handling Advice

Tap  → **Maintenance** → **Restart** .

You can view item exception records, and view handling advice.

Restart Device

Tap  → **Maintenance** → **Restart** .

Tap **Restart** to restart the device.

Upgrade

Tap  → **Maintenance** → **Upgrade** .

Tap **Upgrade** to upgrade the device.



Note

Do not power off during the upgrading.

Restore Parameters

Tap  → **Maintenance** → **Default** .

Restore

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

Restore All

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

Device Debugging

Tap  → **Maintenance** → **Device Debugging** .
You can enable **SSH** for device debugging.

View Log

Tap  → **Maintenance** → **Log** .
Set log type and time, and tap **Search** to search logs.

8.4.15 View User Manual

Tap  → **View User Manual** . You can scan the QR code with your mobile phone for details.

8.4.16 View Open Source Software License

Tap  → **Open Source Software Statement** , you can view the Open Source Software Statement.

Chapter 9 Quick Operation via Web Browser

9.1 Change Password

You can change the device password.

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

You can also set the reserved E-mail address for password reset.

Click **Next** to complete the settings.

9.2 Select Language

You can select a language for the device system.

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

Click **Next** on the change password page. You can select a language for the device system from the drop-down list.

By default, the system language is English.



Note

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

Click **Next** to complete the settings.

9.3 Time Settings

Set Time and DST

Click  → **Time Settings** .

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.

DST Settings

Enable **DST**.

Set the DST start time, end time and bias time.

Click **Next** to complete the settings.

9.4 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.

9.5 Administrator Settings

Steps

1. Click  in the top right of the web page to enter the wizard page. After setting device language, time 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.
 - 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.

9.6 No. and System Network

Steps

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

If you set the device type as **Door Station** or **Access Control Device**, you can set the floor No., No., and click **More** to set **Community No.**, **Building No.**, and **Unit No.**

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

Device Type

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

Floor No.

Set the device installed floor No.

No.

Set the device No.



Note

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.

3. Click **Complete** to save the settings.

Chapter 10 Operation via Web Browser

10.1 Login

You can login via the web browser.



Note

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

Login via Web Browser

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

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

10.2 Forget Password

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

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

Select **Verification Mode**.

Security Question Verification

Answer the security questions.

E-mail Verification

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

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

10.3 Help

10.3.1 Open Source Software Licenses

You can view open source software licenses.

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

10.3.2 View Online Help Document

You can view the help document for Web configuration.

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

10.4 Logout

Log out the account.

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

10.5 Quick Operation via Web Browser

10.5.1 Change Password

You can change the device password.

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

You can also set the reserved E-mail address for password reset.

Click **Next** to complete the settings.

10.5.2 Select Language

You can select a language for the device system.

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

Click **Next** on the change password page. You can select a language for the device system from the drop-down list.

By default, the system language is English.



Note

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

Click **Next** to complete the settings.

10.5.3 Time Settings

Set Time and DST

Click  → **Time Settings** .

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.

DST Settings

Enable **DST**.

Set the DST start time, end time and bias time.

Click **Next** to complete the settings.

10.5.4 Privacy Settings

Set the picture uploading and storage parameters.

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

10.5.5 Administrator Settings

Steps

1. Click  in the top right of the web page to enter the wizard page. After setting device language, time 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.
 - 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.

10.5.6 No. and System Network

Steps

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

If you set the device type as **Door Station** or **Access Control Device**, you can set the floor No., No., and click **More** to set **Community No.**, **Building No.**, and **Unit No.**

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

Device Type

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

Floor No.

Set the device installed floor No.

No.

Set the device No.



Note

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.

3. Click **Complete** to save the settings.

10.6 Person Management

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

Add Basic Information

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

Add the person's basic information, including the employee ID, the person's name, person type, department, etc.

If you select **Visitor** as the person type, you can set the visit times.

Click **Save** to save the settings.

Set Permission Time

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

Enable **Long-Term Effective User**, or set **Start Time** and **End Time** and the person can only has the permission within the configured time period according to your actual needs.

Click **Save** to save the settings.

Authentication Settings

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

Set the authentication type.

Click **Save** to save the settings.

Add Card

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

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

Click **Save** to save the settings.

Add Face Picture

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

Click + **Upload** to upload a face picture from the local PC.



Note

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

Click **Save** to save the settings.

Add Password

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

Click **Configuration → Security → Password Mode**, select **Password Mode** as **Device-Set Personal PIN**.

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

Set the password.

Click **Save** to save the settings.

10.7 Live View

You can view the live video of the device, real-time event, person information, network status, basic information, and device capacity.

Function Descriptions:

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.



Full screen view.



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

Controlled Status

You can select open/closed/remaining open/remaining closed status according to your actual needs.

Real-Time Event

You can view the event Employee ID, Name, Card No., Event Type, Time, and Operation. You can also click **View More** to enter the search conditions, including the event type, 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.

Person Information

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

Network Status

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

Basic Information

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

Device Capacity

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

10.8 Access Control Application

10.8.1 Anti-Passback Settings

The anti-passback function between devices requires personnel to authenticate sequentially according to the configured route. Only sub device supports this function and only one-way passing with authentication is supported.

Steps

1. Click **Access Control** → **Access Control Application** → **Cross-Device Anti-Passback** .
2. Enable the function.
3. Set access controller parameters, including **Main Device IP Address**, **Main Device Port No.** and **Main Device Password**.
4. Set device registered code, and you can view **Registration Status**.
5. Check **Card Reader**. Unchecked card reader cannot be interconnected for anti-passback.

10.8.2 Multi-Door Interlocking Settings

Set the multi-door interlocking between multiple doors of the same access control device. To open one of the doors, other doors must keep closed.

Steps

1. Click **Access Control** → **Access Control Application** → **Cross-Device Multi-Door Interlocking** .
2. Enable the function.
3. Select **Device Type**

- If the device set as main device, you need to set **Port No.**, and click **Add** to add access point. Click **Sub Device Management**, you can view device status and delete the device.
- If the device set as sub device, you need to set access controller parameters, including **Main Device IP Address**, **Main Device Port No.** and **Main Device Password**. Set device registered code, and you can view **Registration Status**. Check **Card Reader**. Unchecked card reader cannot be interconnected for anti-passback.

4. Set **Anti-Passback Rule**.

By Authentication Status

Anti-Passback Routine judged by authentication via card.

By Actual Traffic Status

Anti-Passback Routine judged by actual card opening.

5. Click **OK**.

10.9 Access Control Management

10.9.1 Search Event

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

Event Types

Access Control Event

Employee ID

Name

Card No.

Start Time

2022-07-06 00:00:00

End Time

2022-07-06 23:59:59

No.	Employee ID	Name	Card No.	Event Types	Time	Operation
1	--	-	--	Device Powering On	2022-07-06 09:32:04 08:00	-
2	--	-	--	Door Locked	2022-07-06 09:32:04 08:00	-
3	--	-	--	Device Tampered	2022-07-06 09:32:07 08:00	-
4	--	-	--	Authentication via Fingerprint Failed	2022-07-06 09:32:21 08:00	-
5	--	-	--	The password mismatches.	2022-07-06 09:54:24 08:00	-
6	--	-	--	The password mismatches.	2022-07-06 10:04:54 08:00	-
7	--	-	--	Network Disconnected	2022-07-06 10:05:05 08:00	-
8	--	-	--	Network Recovered	2022-07-06 10:05:05 08:00	-
9	--	-	--	Local Login	2022-07-06 10:06:06 08:00	-
10	--	-	--	Remote Login	2022-07-06 10:07:21 08:00	-
11	--	-	--	Remote Login	2022-07-06 10:12:50 08:00	-
12	--	-	--	Remote Login	2022-07-06 10:14:59 08:00	-
13	--	-	--	Remote Login	2022-07-06 10:20:46 08:00	-
14	--	-	--	Remote Login	2022-07-06 10:25:30 08:00	-
15	--	-	--	Remote Login	2022-07-06 10:37:30 08:00	-
16	--	-	--	Local Login	2022-07-06 10:40:55 08:00	-
17	--	-	--	Remote Login	2022-07-06 10:47:01 08:00	-
18	--	-	--	Remote Login	2022-07-06 11:05:29 08:00	-

Figure 10-1 Search Event

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

The results will be displayed on the right panel.

10.9.2 Door Parameter Configuration

Configure parameters for unlocking doors.

Select Door No.

Select a door to configure relative parameters.

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

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

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

View Device Online Status

View and refresh the device status.

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

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

Set Door Name

Create door name.

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

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

Set Open Duration via PC Web

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

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

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

Click **Save**.

Set Door Open Timeout Alarm via PC Web

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

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

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

Click **Save**.

Set Lock Door when Door Closed

You can set lock door when door closed.

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

You can enable **Lock Door when Door Closed**.

Click **Save**.

Set Door Lock Status via Web Page

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

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

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

Click **Save**.

Set Exit Button via PC Web

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

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

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

Click **Save**.

Set Door Lock Powering Off Status via PC Web

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

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

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

Click **Save**.

Set Extended Open Duration via PC Web

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

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

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

Click **Save**.

Set Door Remain Open Duration with First Person via PC Web

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

Click **Access Control → Parameter Settings → Door Parameters** to enter the settings page.
Set the door open duration when first person is in and click **Save**.

Set Duress Code via PC Web

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

Click **Access Control → Parameter Settings → Door Parameters** to enter the settings page.
Set duress code, and click **Save**.



Note

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

Set Super Password via PC Web

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

Click **Access Control → Parameter Settings → Door Parameters** to enter the settings page.
Set **Super Password**, the designated person can enter the super password to open the door.
Click **Save**.



Note

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

10.9.3 Authentication Settings

Select Main or Sub Card Reader via PC Web

Set the terminal for person authentication.

Click **Access Control → Parameter Settings → Authentication Settings** to enter the settings page.
Select the terminal as main or sub card reader.
Set other parameters and click **Save**.

View Terminal Type and Model via PC Web

You can view terminal type and model.

Click **Access Control** → **Parameter Settings** → **Authentication Settings** to enter the settings page.
View **Terminal Type** and **Terminal Model**.

Enable Authentication Device via PC Web

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

Steps

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

Set Authentication via PC Web

Configure Certification.

Click **Access Control** → **Parameter Settings** → **Authentication Settings** to enter the settings page.
When selecting main card reader as the Terminal, you can select Authentication from the drop-down list. When there is more than one authentication, you should set **Single Credential Authenticating Timeout** and **Control Initial Authentication Type**.

Single Credential Authenticating Timeout

You can configure the duration for each certification.



Note

The password authenticating timeout is 20 s by default, which is not limited by above settings.

Control Initial Authentication Type

If enabled, all selected types can be used for first-time authentication.

When selecting sub card reader as the Terminal, you can select Authentication from the drop-down list.

Click **Save**.

Manually Trigger Authentication via Face on PC Web

After enabling **Manually Trigger Authentication via Face**, you need to touch the screen of the device manually for face recognition.

Click **Access Control** → **Parameter Settings** → **Authentication Settings** to enter the settings page. When the main card reader is selected as the Terminal, click to enable **Manually Trigger Authentication via Face** and choose authentication mode.

Single Recognition

After completing the previous facial recognition, no matter successful or failed, you need to tap the screen to trigger the next recognition.

Continuous

After triggering the recognition, you can recognize via face until the device enter into the sleeping mode.

Click **Save**.

Set Recognition Interval via PC Web

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

Click **Access Control** → **Parameter Settings** → **Authentication Settings** to enter the settings page. When you select the terminal as main or sub card reader, set recognition interval, and click **Save**.



Note

Please enter a number between 1 and 10.

Set Authentication Interval via PC Web

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

Click **Access Control** → **Parameter Settings** → **Authentication Settings** to enter the settings page. When you select the terminal as main card reader, set **Authentication Interval**, and click **Save**.

Enable Alarm of Max. Failed Attempts via PC Web

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

Click **Access Control** → **Parameter Settings** → **Authentication Settings** to enter the settings page. When you select the terminal as main or sub card reader, slide to enable **Alarm of Max. Failed Attempts**, and set **Max. Authentication Failed Attempts**.

Click **Save**.

Enable/Disable Tampering Detection via PC Web

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

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

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

Click **Save**.

Enable/Disable Card No. Reversing via PC Web

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

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

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

Click **Save**.

Set Sub Card Reader Position

You can choose the position for the sub card reader.

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

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

Set Communication with Controller Every via PC Web

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

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

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

Set Timeout Duration of Entering Password via Web Client

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

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

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

Set OK LED Polarity and Error LED Polarity via PC Web

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

Click **Access Control → Parameter Settings → Authentication Settings** to enter the settings page. When you select the terminal as sub card reader, set **OK LED Polarity** and **Error LED Polarity**, and click **Save**.

10.9.4 Authentication Linkage Settings

You can set authentication linkage settings.

Steps

1. Click **Access Control → Parameter Settings → Authentication Settings** to enter the settings page.
2. Set linkage functions.

Link to Call If Authenticated

If you enable this and person passes authentication, it will automatically call Button Settings's calling target to open door remotely.

Link to Call If Authentication Failed

After enabling, if authentication failed attempts reached the set number, it will automatically call Button Settings's calling target to open door remotely.

3. Click **Save**.

10.9.5 Set Authentication Plan

You can set authentication plan.

Click **Access Control → Parameter Settings → Authentication Settings** to enter the settings page. Select the authentication type and drag the time period in the time bar. Click **Save**.

10.9.6 Set Face Parameters

Enable/Disable Face Anti-spoofing via Web Browser

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

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

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

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

Enable/Disable Face Duplicate Check

After enabling face duplicate check and everytime adding person's face, the system will check the face's duplication. If a duplicated face is detected, a prompt will be on.



Note

The function is not supported when add face remotely or applying face in batch.

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

Enable **Face Duplicate Check**.

Click **Save**.

Set Anti-Spoofing Detection Level via PC Web

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

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

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

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

Set Recognition Distance via PC Web

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

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

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

Set Pitch Angle via PC Web

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

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



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

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

Set Yaw Angle via PC Web

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

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



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

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

Set Face Picture Quality Grade for Applying via PC Web

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

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



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

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

Click **Save**.

Set 1:1 Face Grade Threshold via PC Web

Set 1:1 face grade threshold.

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

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

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

Set Face 1:1 Matching Threshold via PC Web

Set face 1:1 matching threshold.

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

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

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

Set 1:N Matching Threshold via PC Web

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

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

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

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

Set Face Recognition Area via Web Browser

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

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

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

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

Click **Save**.

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

Set Fingerprint Parameters via PC Web

You can set the fingerprint parameters of the device.

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

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

Click **Save**.

Enable/Disable ECO Mode via PC Web

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

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

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

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

ECO Mode (1:1) Threshold

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

ECO Mode (1:N) Threshold

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

Face with Mask 1:1 Match Threshold (ECO)

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

Face with Mask 1:N Match Threshold (ECO)

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

Click **Save**.

Enable/Disable Face with Mask Detection via PC Web

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

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

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

Face without Mask Strategy

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

Reminder of Wearing Face Mask

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

Must Wear Face Mask

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

Face with Mask&Face (1:1)

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

Face with Mask&Face (1:N)

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

Face with Mask 1:1 Match Threshold (ECO)

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

Face with Mask 1:N Match Threshold (ECO)

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

Click **Save**.

10.9.7 Card Settings

Enable/Disable NFC Protection via PC Web

After enabling, the device can read NFC card.

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

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

Click **Enable NFC Security Encryption**. When enabled, the card reader can only recognize the NFC credential generated from Hik-Connect.

Enable/Disable M1 Card via Web Client

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

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

Click to **Enable M1 Card**.

M1 Card Encryption

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

Sector

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



Note

You are advised to encrypt sector 13.

Click **Save**.

Enable/Disable EM Card via Web Client

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

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

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



Note

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

Enable/Disable CPU Card via Web Client

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

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

Click to **Enable CPU Card**.

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

Click **Save**.

Set DESFire Card

You can enable DESFire card and DESFire card read content.

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

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

Set FeliCa Card

You can enable FeliCa card.

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

Select **Enable FeliCa Card**.

Set Card No. Authentication Parameters

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).

10.9.8 Set Remote Verification

The device will upload the person's authentication information to the platform. The platform will judge to open the door or not.

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

Click **Save** after parameters are configured.

Remote Verification

After enabling the remote verification, when authenticating, the device will upload authentication information to the platform, and the platform will confirm whether to open the door.

Verifying Person Type Remotely

Select **Verifying Person Type Remotely**.

Verify Credential Locally

After enabling the function, the device will check permission but not estimate the plan template.

Timeout Duration of Remote Verification

Set Timeout Duration of Remote Verification.

Offline Remote Verifying Unlocking

You can enable **Offline Remote Verifying Unlocking**.

Result Return Mode

Set **Result Return Mode**.

10.9.9 Privacy Settings

Set Event Storage Type via PC Web Browser

You can configure the event storage type.

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

You can select **Event Storage Type** as **Delete Old Events Periodically**, **Delete Old Events by Specified Time** or **Overwriting**.

Delete Old Events Periodically

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

Delete Old Events by Specified Time

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

Overwriting

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

Click **Save**.

Set Authentication Result via PC Web

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

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

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

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

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

Click **Save**.

Configure Picture Uploading and Storage via PC Web

You can set picture uploading and storage parameters.

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

Save Picture When Auth.

Save picture when authenticating automatically.

Upload Picture When Auth.

Upload the pictures when authenticating to the platform automatically.

Picture Mode

When selecting as default, the device will capture the panoramic view. You can set the Max. picture size and picture resolution.

When selecting as matting picture mode, the device will only capture face. You can set the Max. picture size.

Save Registered Picture

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

Save Pictures After Linked Capture

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

Upload Picture After Linked Capture

Upload the pictures captured by linked camera to the platform automatically

Click **Save**.

Clear Device Pictures via PC Web

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

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

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

Set PIN Mode via PC Web

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

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

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

Platform-Applied Personal PIN

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

Device-Set Personal PIN

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

10.9.10 Video Intercom Settings

Set Video Intercom Parameters

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

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

If set the device type as **Door Station** or **Access Control Device**, you can set the floor No. and No., and click **More** to set **Community No.**, **Building No.**, and **Unit No.**

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

Device Type

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



Note

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

Floor No.

Set the device installed floor No.

No.

Set the device No.



Note

- If you change the No., you should reboot the device.
 - The main door station No. is 0, and the sub door station No. ranges from 1 to 16.
-

Community No.

Set the device community No.

Building No.

Set the device building No.

Unit No.

Set the device unit No.



Note

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

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

Outer Door Station No.

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



Note

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

Community No.

Set the device community No.

Configure Video Intercom Network Parameters via Web Browser

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

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

Main Station IP

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

SIP Server IP Address

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

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

Click **Save**.

Set Communication Time via PC Web

Set the max. communication time.

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

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



Note

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

Press Button to Call via PC Web

Steps

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

Button Settings

No.	Button Settings
01	☒ Call Specified Indoor Station ☐ Enter Room No. ☐ Call Management Center ☒ Call Indoor Station ☐ app

Link Authentication to Call ☒

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

Save

Figure 10-2 Press Button to Call

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



Note

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

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

Call Priority

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

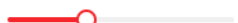
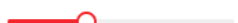
Before You Start

Enter the prerequisites here (optional).

Enter the context of your task here (optional).

Steps

1. Click **Intercom** → **Call Priority** to enter the settings page.

Call Priority	Call Type	Ring Duration
Priority1	☒ Indoor ☐ Telephone	 60 s
Priority2	☐ Indoor ☒ Telephone	 60 s
Priority3	☐ Indoor ☐ Telephone	 60 s

 The higher the level, the earlier the device to be called. After the call time is over, the next level of call is triggered.

Save

Figure 10-3 Call Priority

2. Check the **Call Type** and set the **Ring Duration** of each 3 priorities.
3. Click **Save** to enable the settings.



Note

The higher the level, the earlier the device to be called. After the call time is over, the next level of call is triggered.

Number Settings via PC Web

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

Steps

1. Go to **Access Control** → **Call Settings** → **Number Settings**.
2. Click **Add**, and enter **Room No.** and **SIP1** phone number.
3. **Optional:** Click **Add** to add the SIP number or click  to delete the number.
4. **Optional:** You can click **Import No.** to import SIP No. through Excel in batch. You can click **Download SIP No. Data Template**, and enter the data to import.



Note

Please refer to the downloaded EXCEL for detailed filling instructions.

5. **Optional:** You can click **Export No.** and click **Confirm** to export SIP No.
6. Click **Save**.
7. **Optional:** You can click **Delete** to delete room number and its SIP number.

10.10 Device Management

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

Steps

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

Delete Device Select devices to be deleted and click **Delete**.

Import Device Connect the USB flash drive with device information files, and click **Import**.

Export Device Click **Export** to export device information files to the connected USB flash drive.

10.11 System Configuration

10.11.1 View Device Information

View the device name, language, model, serial No., version, number of channels, IO input, IO output, lock, RS-485, alarm input, alarm output, and device capacity, etc.

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

You can view the device name, language, model, serial No., version, number of channels, IO input, IO output, lock, local RS-485, alarm input, alarm output, and device capacity, etc.

10.11.2 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.

10.11.3 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.

10.11.4 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.

10.11.5 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.

10.11.6 Set Working Mode via PC Web

You can set the terminal parameters of the device.



Note

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

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

Working Mode

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

Access Control Mode

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

10.11.7 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** → **Basic Settings** → **TCP/IP** .

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

- NIC Type:** A dropdown menu set to "Self-Adaptive".
- DHCP:** A toggle switch currently turned off.
- *IPv4 Address:** A text input field containing "10.6.122.245".
- *IPv4 Subnet Mask:** A text input field containing "255.255.255.0".
- *IPv4 Default Gateway:** A text input field containing "10.6.122.254".
- IPv6 Mode:** Three radio buttons: "Manual" (unselected), "DHCP" (selected), and "Route Advertisement" (unselected).
- IPv6 Address:** A text input field containing "6012:bbbbce2ca:3cff:fe9e0f2".
- IPv6 Subnet Prefix Length:** A text input field containing "64".
- IPv6 Default Gateway:** A text input field containing "fe80::8261:6cff:eda7:445".
- Mac Address:** A text input field containing "e0:ca:3c:f9:e0:f2".
- MTU:** A text input field containing "1500".
- DNS Server:** A section header.
- DHCP:** A toggle switch currently turned on.
- Preferred DNS Server:** A text input field containing "8.8.8.8".
- Alternate DNS Server:** A text input field containing "8.8.4.4".
- Save:** A red button at the bottom center.

Figure 10-4 TCP/IP Settings Page

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

Network Card

Select network card according to your actual needs.

DHCP

If uncheck the function, you should set the IPv4 address, IPv4 subnet mask, IPv4 default gateway, IPv6 mode, IPv6 address, IPv6 subnet prefix length, IPv6 default gateway, Mac address, and MTU.

If you check the function, the system will allocate the IPv4 address, IPv4 subnet mask, the IPv4 default gateway, IPv6 mode, IPv6 address, IPv6 subnet prefix length, and IPv6 default gateway automatically.

NIC Type

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

DNS Server

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

Set 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 10-5 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 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.

Enable/Disable HTTP

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

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

Click **Save** after parameters are configured.

HTTP Port

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

HTTPS Port

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

View RTSP Port via PC Web

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

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

Set WebSocket(s) via PC Web

View WebSocket and WebSockets port.

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

View WebSocket and WebSockets port.

Enable SDK Service

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

Click **Configuration** → **Network** → **Advanced** → **Network Service** to enter the settings page.

Check the checkbox of **Enable** to enable the function.

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. Set the ISUP version, server address, device ID, and the ISUP status.
-



Note

If you select 5.0 as the version, you should set the **Encryption Key**.

4. Set the **Network Connection Priority**. You can enable **Allow Access**, and click the network and drag it to adjust the network priority.
5. Set the ISUP listening parameters, including ISUP alarm center IP address/domain name, ISUP alarm center URL, and ISUP alarm center port.
6. Click **Save**.

Set OTAP via PC Web

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

Steps

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

Platform Access

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.

VoIP Account Settings

You can realize voice call by network.

Steps

1. Go to **System and Maintenance → System Configuration → Network → Device Access → VoIP**.
2. Select **Call Type**, and select VoIP.
3. Enable **VoIP Gateway**.
4. Set **Register User Name**、**Registration Password**、**Server IP Address**、**Server Port**、**Expiry Time**、**Register Status**、**Number**、**Display User Name**. and **Center No**.
5. Click **Save**.

PushSDK

Enable PushSDK, after saving the device can communicate with the platform via PushSDK.

Steps

1. Click **System Maintenance → System Management → Network → Device Access → PushSDK** .
2. Enable the PushSDK function.
3. Set **Protocol Version**, **Server IP Address**, **Port**, **Device ID**, and **Encryption Key**.
4. Click **Save**.

Result

After refreshing the Web or restarting the device, check the **Registration Status** of PushSDK, which should display as Online.

10.11.8 Set Video and Audio Parameters

Set the image quality and resolution.

Set Video Parameters

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

Camera Name

Stream Type ☒ Main Stream ☐ Sub-stream

Video Type ☐ Video Stream ☒ Video&Audio

Resolution

Bit Rate Type ☐ Constant ☒ Variable

Video Quality

Frame Rate

* Max. Bitrate Kbps

Video Encoding

* I Frame Interval

Save

Figure 10-6 Video Settings Page

Set the camera name, stream type, video type, resolution, bit rate type, Max. bit rate and I Frame Interval.

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



Note

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

Set Audio Parameters

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

Set the audio stream type, input volume, and output volume.

Check **Enable Voice Prompt** according to your needs.

Configure Video Parameters via Web Browser

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

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

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

Click **Save**.

Configure Audio Parameters via Web Browser

You can set device volume.

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

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

Slide to enable voice prompt function.

You can enable **Audio Mixing**, and set **Output Sub-Volume**.

Click **Save**.

10.11.9 Access Configuration

Set RS-485 Parameters

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

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

Check **Enable**, and set the parameters.

Peripheral Type

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



Note

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

RS-485 Address

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



Note

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

Baud Rate

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

Output Type

If you select **Access Controller** as the peripheral type, you should set the parameter. The device will output the card No. or the employee ID to the access controller.

Click **Save** to save the settings.

Set Wiegand Parameters

You can set the Wiegand transmission direction.

Steps



Note

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

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

Input

The device can connect a Wiegand card reader.

Output

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

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



Note

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

Elevator Control via Web

Steps

1. Click **System and Maintenance** → **Access Configuration** → **Elevator Control** .
2. Enable **Elevator Control**.
3. Set the elevator parameters.

Elevator No.

Select elevator No.

Main Elevator Controller Model

Select an elevator No. for configuration.

Interface Type

Select a communication type from the drop-down list for elevator communication.

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.

Access Protocol

Select protocol according to actual needs.

Main Elevator Controller Address/Port/User Name/Password

Enter the Main Elevator Controller IP address, port, login admin user name, and password.

Negative Floor Capacity

Set the negative floor number.

Installation Location

Select installation location as **Out of Elevator Cab** or **In Elevator Cab**.

Double-sided Elevator

You can enable double-sided elevator function. Please enable Double-sided Elevator function on the elevator controller side, otherwise this function will not take effect.

Call Elevator Mode

Select call elevator mode.

Call Elevator Only

After the person passes authentication, the device will call elevator to its floor.

Call Elevator + Authorize

After the person passes authentication, the device will call elevator to its floor and authorize the permission of the floor linked to the person's room. The person can get to the target floor by pressing corresponding floor No.



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.
-

10.11.10 Image Parameter Settings

Set Brightness/Contrast/Saturation/Sharpness via PC Web

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

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

Image Adjustment

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

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

Set LED Light via PC Web

You can adjust the brightness of the supplement light.

Steps

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

Set Video Standard via PC Web

You can set the video standard of live view page.

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

Video Adjustment

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

PAL

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

NTSC

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

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

10.11.11 Linkage Settings

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

Steps

1. Click **Access Control** → **Parameter Settings** → **Linkage Settings** to enter the settings page.
2. Click + .
3. Set event source. Select the linkage type as **Event Linkage**, **Card Linkage** or **Link Employee ID**.
 - Select **Linkage Type** as **Event Linkage**, you can select event types according to your actual needs.
 - Select **Linkage Type** as **Card Linkage**, enter **Card No.** and select **Card reader**.
 - Select **Linkage Type** as **Link Employee ID**, enter **Employee ID** and select **Card reader**.
4. Set linkage action.
 - 1) Enable **Door Linkage**, check and select door action.

2) Enable **Linked Capture**.

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

10.11.12 Time and Attendance Settings

If you want to record the person's working hour, late arrivals, early departures, breaks, absenteeism, etc., you can add the person to the shift group and assign a shift schedule (a rule for the attendance defining how the schedule repeats, the shift type, break settings, and the card swiping rule.) to the shift group to define the attendance parameters for the persons in the shift group.

Disable Attendance Mode via Web

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

Steps

1. Click **Configuration → Platform Attendance** to enter the settings page.
2. Disable the **Time and Attendance**.

Result

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

Set Manual Attendance via Web

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

Before You Start

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

Steps

1. Click **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.



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.

10.12 Preference Settings

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

10.12.1 Set Standby Image via PC Web

Set the standby image parameters, including the time to enter standby, screen saver picture, displayed effect, and slide show interval.

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

Time to Enter Standby

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

10.12.2 Set Sleep Time via PC Web

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

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

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

Click **Save**.

10.12.3 Customize Authentication Desk via PC Web

Customize the modules on the authentication page/desk.

Steps

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

Access 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.

Intercom Mode

The authentication interface displays a quick operation area and an authentication area. The quick operation area supports customizable shortcut keys for functions.

Simple

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

3. Click **Apply**.

10.12.4 Notice Publication

You can set the notice publication for the device.

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

Theme Management

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



Note

Only the format of JPG is supported. Each picture should be smaller than 1 MB with resolution up to 1920*1280. Up to 8 pictures are supported.

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.

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



Note

The slide show interval ranges from 1 s to 10 s.

Click **Edit Name** to change the them name. Click **Delete Program** to delete the theme.

Schedule Management

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

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

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

10.12.5 Customize Audio Content

Customize the output audio content when authentication succeeded and failed.

Steps

1. Click **Configuration → Preference → Prompt Schedule** .
2. Enable the function.
3. Set the appellation.
4. Set the time period when authentication succeeded.
 - 1) Click **Add Time Duration**.
 - 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 Time Duration**.
 - 2) Set the time duration and the language.



Note

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

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

10.12.6 Customize Prompt Voice via PC Web

You can customize prompt voices for the device.

Steps

1. Go to **System and Maintenance → Preference → Custom Prompt** .
2. Click  →  and import audio file from local PC according to your actual needs.



Note

Supports wav audio format at 8 kHz, 16 kHz, 32 kHz, 44.1 kHz, 48 kHz sampling rate with individual file size limit of 512 KB.

10.12.7 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**.

10.13 Upgrade and Maintenance

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

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.



Note

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.

Unlock

You can click **Unlock** according to your needs.

Version Information

You can view the device information.

10.13.1 Reboot

You can choose to reboot device manually or automatically.

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

Manually Reboot

Reboot Device

Reboot Automatically

Reboot Automatically ☒

Rebooting Time

Figure 10-7 Reboot

Click **Restart** to reboot the device manually.

Slide to enable **Reboot Automatically**. Set Rebooting Time and click **Save**.

10.13.2 Upgrade

Upgrade Locally via PC Web

You can upgrade the device locally.

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

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

Online Upgrading via PC Web

You can upgrade the device online.

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

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

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

Upgrade Keyfob



- Make sure that the peripheral module is online.
 - When upgrading the keyfob, keep only one face recognition terminal around and don't move the keyfob.
-

Click **System and Maintenance → Maintenance → Upgrade** . In the Upgrade Settings drop-down list, select **Keyfob**. Select the upgrade file from your local PC. Click **Upgrade → OK** . Press any button of the keyfob to upgrade.

10.13.3 Restoration

Restore to Factory Settings via Web Browser

You can restore device to factory settings.

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

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

Restore to Default Settings via PC Web

You can restore device to default settings.

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

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

10.13.4 Export Device Parameters via PC Web

Export device parameters.

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

Backup

Click **Export** to export device parameters.



Export device parameters and import those parameters to other devices.

10.13.5 Import Device Parameters via PC Web

Import the configuration parameters.

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

Import Config File

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

10.13.6 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** to capture.

Enable/Disable SSH via Web Browser

You can enable SSH to perform remote debugging.

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

Enable SSH

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

Print Device Log via PC Web

You can print out the device log.

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

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

Capture Network Packet via PC Web

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

Go to **System and Maintenance → Maintenance → Device Debugging → Log for Debugging** .
Set **Capture Packet Duration**, **Capture Packet Size**, and click **Start Capture**.

Set Protocol Testing

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

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

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

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

Set Network Diagnosis

Enter the device IP address or domain name, you can perform PING settings. Debug the network according to the PING result.

Go to **Maintenance and Security → Maintenance → Network Diagnosis** .

Enter the device IP for PING operation, select the network connection mode, PING duration, and Ping data package size (default parameter is recommended.) Click **Diagnose**. The result will displayed in **PING Result**.

Set Network Penetration Service via PC Web

When the device is deployed in the LAN, you can enable the penetration service to realize device remote management.

Steps

1. Go to **System and Maintenance → Maintenance → Device Debugging → Network Penetration Service**.
2. Slide **Enable Penetration Service**.
3. Set **Server IP Address** and **Server Port**. Create **User Name** and **Password**.
4. **Optional**: You can set **Heartbeat Timeout**. The value range is 1 to 6000.
5. **Optional**: You can view the status of the penetration service. Click **Refresh** to refresh the status.
6. Click **Save**.



Note

The penetration service will auto disabled after 48 h.

10.13.7 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.

10.13.8 Advanced Settings via PC Web

You can configure face parameters and view version information.

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

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

Face Parameter

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

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

Click **Save**.

Version Information

You can view the different version information here.

10.13.9 Security Management

Set security level when login the PC web.

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

Security Mode

High security level when logging in and verify user information.

Compatible Mode

Compatible with old user verification method.

Click **Save**.

10.13.10 Certificate Management

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



Note

The function is only supported by certain device models.

Create and Install Self-signed Certificate

Steps

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

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

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

Install Other Authorized Certificate

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

Steps

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

Install CA Certificate

Before You Start

Prepare a CA certificate in advance.

Steps

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



Note

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

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

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

HikCentral Access Control (HCAC)

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

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

Appendix A. Symbol Conventions

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

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

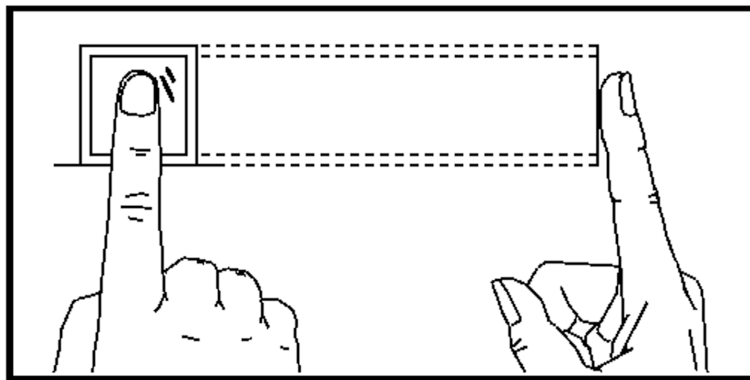
Appendix B. Tips for Scanning Fingerprint

Recommended Finger

Forefinger, middle finger or the third finger.

Correct Scanning

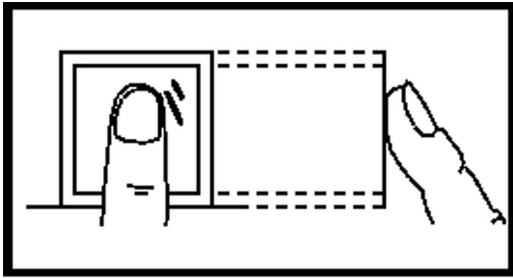
The figure displayed below is the correct way to scan your finger:



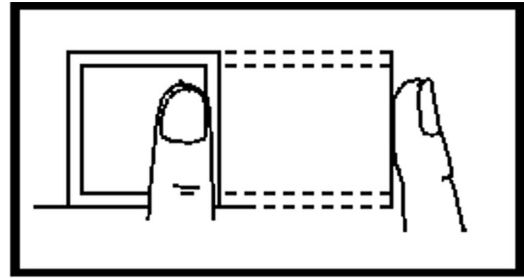
You should press your finger on the scanner horizontally. The center of your scanned finger should align with the scanner center.

Incorrect Scanning

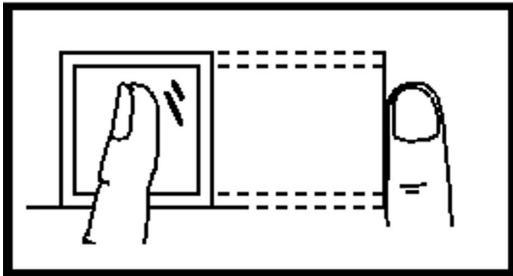
The figures of scanning fingerprint displayed below are incorrect:



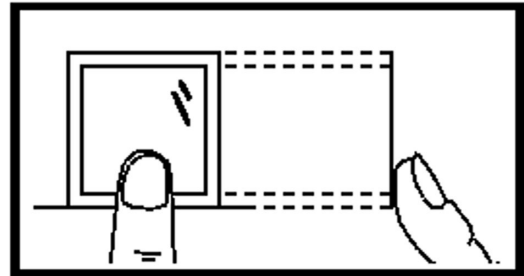
Vertical



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

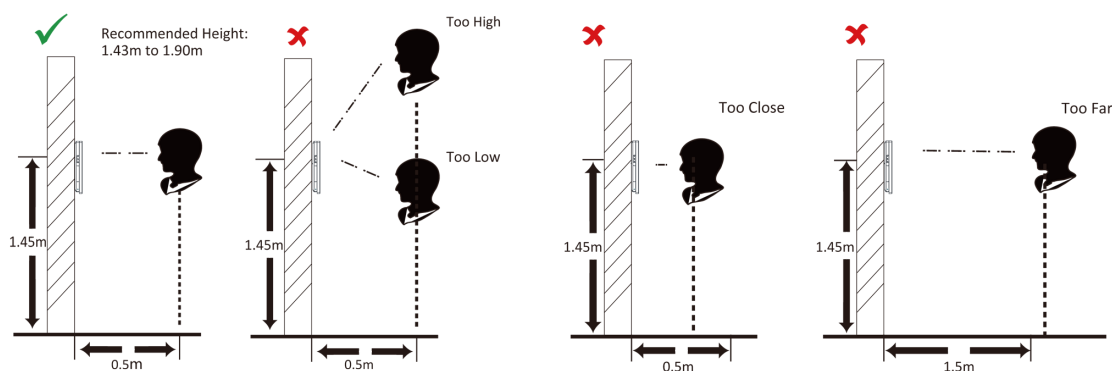
If your fingerprint is shallow, or it is hard to scan your fingerprint, we recommend you to use other authentication methods.

If you have injuries on the scanned finger, the scanner may not recognize. You can change another finger and try again.

Appendix C. Tips When Collecting/Comparing Face Picture

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

Positions (Recommended Distance: 0.3 m)



Expression

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



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

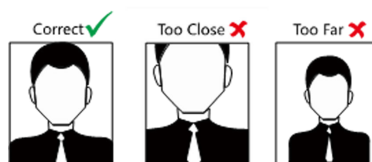
Posture

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



Size

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



Appendix D. Tips for Installation Environment

1. Light Source Illumination Reference Value



Candle: 10Lux

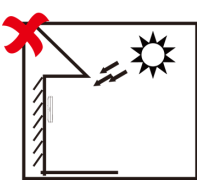


Bulb: 100~850Lux

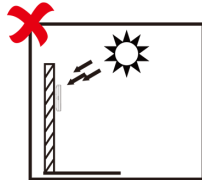


Sunlight: More than 1200Lux

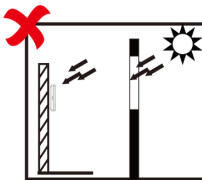
2. Avoid backlight, direct and indirect sunlight



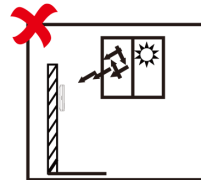
Backlight



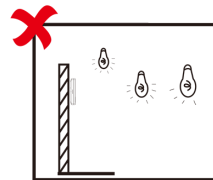
Direct Sunlight



Direct Sunlight
through Window



Indirect Light
through Window



Close to Light



See Far, Go Further