DS-K1T321 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.

Symbol Conventions

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

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

Regulatory Information

FCC Information

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

EU Conformity Statement

CE

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

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



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



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

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

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:

- At the time of final installation, the user needs to be informed in an obvious position that the device has a face collection function.
- 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-K1T321MFX	13.56 MHz Card Presenting Frequency
	DS-K1T321MWX	13.56 MHz Card Presenting Frequency, Wi-Fi, 2.4G
	DS-K1T321MFWX	13.56 MHz Card Presenting Frequency, Wi-Fi, 2.4G
	DS-K1T321EX	125 KHz Card Presenting Frequency
	DS-K1T321EFX	125 KHz Card Presenting Frequency
	DS-K1T321EWX	125 KHz Card Presenting Frequency, Wi-Fi, 2.4G
	DS-K1T321EFWX	125 KHz Card Presenting Frequency, Wi-Fi, 2.4G
	DS-K1T321MX	13.56 MHz Card Presenting Frequency

Use only power supplies listed in the user instructions:

Model	Manufacturer	Standard
TS-A012-120100E2 05K000C00	Shenzhen Transin Technologies Co., Ltd	CE

Contents

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 Install with Battery Plate 6

Chapter 4 Wiring 10

4.1 Wire Normal Device 10

4.2 Wire Secure Door Control Unit 12

Chapter 5 Activation 13

5.1 Activate via Device 13

5.2 Activate via Mobile Web 14

5.3 Activate via Web Browser 14

5.4 Activate via SADP 15

5.5 Activate Device via iVMS-4200 Client Software 16

Chapter 6 Quick Operation 18

6.1 Select Language 18

6.2 Set Password Change Type 18

6.3 Set Network Parameters 19

6.4 Access to Platform 20

6.5 Privacy Settings 20

6.6 Set Administrator 21

Chapter 7 Basic Operation 23

7.1 Login 23

7.1.1 Login by Activation Password 23
7.1.2 Login by Administrator 23
7.1.3 Forgot Password 24
7.2 Communication Settings 24
7.2.1 Set Wired Network Parameters 25
7.2.2 Set Wi-Fi Parameters 25
7.2.3 Set ISUP Parameters 26
7.2.4 Platform Access 28
7.2.5 Set RS-485 Parameters 28
7.2.6 Set AP Mode 29
7.3 User Management 29
7.3.1 Add Administrator 29
7.3.2 Add Face Picture 31
7.3.3 Add Fingerprint 32
7.3.4 Add Card 33
7.3.5 View PIN code 35
7.3.6 Set Authentication Mode 35
7.3.7 Edit User 36
7.4 Local Time and Attendance 36
7.4.1 Attendance Process Description 36
7.4.2 Department Management 37
7.4.3 Enable Local T&A 38
7.4.4 Shift Management 38
7.4.5 Shift Schedule 40
7.5 Platform Attendance 41
7.5.1 Disable Attendance Mode via Device 41
7.5.2 Set Manual Attendance via Device 42
7.5.3 Set Auto Attendance via Device 43

7.5.4 Set Manual and Auto Attendance via Device 45
7.6 Attendance Report 46
7.7 Data Management 46
7.7.1 Delete Data 46
7.7.2 Import Data 46
7.7.3 Export Data 47
7.8 Identity Authentication 48
7.8.1 Authenticate via Single Credential 48
7.8.2 Authenticate via Multiple Credential 48
7.9 Basic Settings 49
7.10 Set Privacy Parameters via Device 50
7.11 Password Management 51
7.12 Set Biometric Parameters 51
7.13 Set Authentication Parameters 52
7.14 Preference Settings 54
7.15 System Maintenance 54
Chapter 8 Configure the Device via the Mobile Browser 57
8.1 Login 57
8.2 Overview 57
8.3 Forget Password 58
8.4 Configuration 58
8.4.1 View Device Information 58
8.4.2 Time Settings 58
8.4.3 Set DST 59
8.4.4 User Management 60
8.4.5 Network Settings 60
8.4.6 Access Configuration 65
8.4.7 User Management 66

8.4.8 Device Management 67
8.4.9 Search Event 68
8.4.10 Access Control Settings 68
8.4.11 Set Time and Attendance via Mobile Web Browser 73
8.4.12 Audio Settings 77
8.4.13 Custom Home Page 77
8.4.14 Upgrade and Maintenance 77
8.4.15 View User Manual 78
8.4.16 View Open Source Software License 78
Chapter 9 Quick Operation via Web Browser 79
9.1 Change Password 79
9.2 Select Language 79
9.3 Time Settings 79
9.4 Privacy Settings 80
9.5 Administrator Settings 80
9.6 No. and System Network 81
Chapter 10 Operation via Web Browser 83
10.1 Login 83
10.2 Forget Password 83
10.3 Help 83
10.3.1 Open Source Software Licenses 83
10.3.2 View Online Help Document 84
10.4 Logout 84
10.5 Quick Operation via Web Browser 84
10.5.1 Change Password 84
10.5.2 Select Language 84
10.5.3 Time Settings 84
10.5.4 Privacy Settings 85

10.5.5 Administrator Settings 85
10.5.6 No. and System Network 86
10.6 Person Management 87
10.7 Overview 89
10.8 Access Control Management 90
10.8.1 Search Event 90
10.8.2 Door Parameter Configuration 91
10.8.3 Authentication Settings 94
10.8.4 Authentication Linkage Settings 97
10.8.5 Set Authentication Plan 97
10.8.6 Set Face Parameters 97
10.8.7 Card Settings 101
10.8.8 Set Remote Verification 103
10.8.9 Privacy Settings 103
10.9 Local Time and Attendance Settings 106
10.9.1 Manage Department via Web 106
10.9.2 Enable Local T&A 106
10.9.3 Set Attendance Rule for Shift 106
10.9.4 Manage Shift 107
10.9.5 Manage Schedule 108
10.9.6 View Attendance Report 109
10.10 System Configuration 109
10.10.1 View Device Information via PC Web 109
10.10.2 Set Time 109
10.10.3 Change Administrator's Password 110
10.10.4 Account Security Settings via PC Web 111
10.10.5 View Device Arming/Disarming Information via PC Web 111
10.10.6 Set Working Mode via PC Web 111

10.10.7 Network Settings 112
10.10.8 Set Video and Audio Parameters via PC Web 117
10.10.9 Access Configuration 117
10.10.10 Image Parameter Settings 119
10.10.11 Linkage Settings 120
10.10.12 Time and Attendance Settings 120
10.11 Preference Settings 123
10.11.1 Set Standby Image via PC Web 123
10.11.2 Set Sleep Time via PC Web 123
10.11.3 Customize Authentication Desk via PC Web 123
10.12 System and Maintenance 124
10.12.1 Reboot 124
10.12.2 Upgrade 124
10.12.3 Restoration 125
10.12.4 Export Device Parameters via PC Web 125
10.12.5 Import Device Parameters via PC Web 125
10.12.6 Device Debugging 125
10.12.7 View Log via PC Web 127
10.12.8 Advanced Settings via PC Web 127
10.12.9 Security Management 128
10.12.10 Certificate Management 128
Chapter 11 Other Platforms to Configure 130
Appendix A. Tips for Scanning Fingerprint 131
Appendix B. Tips When Collecting/Comparing Face Picture 133
Appendix C. Tips for Installation Environment 135
Appendix D. Dimension 136

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

- 2.4-inch LCD screen, 2 MP lens
- Multiple authentication methods, including face, fingerprint, card, and PIN, etc
- Supports M1 card or EM card according to different models
- Max. 500 faces, 3,000 cards, 3,000 fingerprints and 100,000 events
- Face recognition duration < 0.2 s/User
- Supports ISAPI and ISUP 5.0 protocols
- Configuration via the PC web browser and mobile web browser
- Supports AP mode

Chapter 2 Appearance

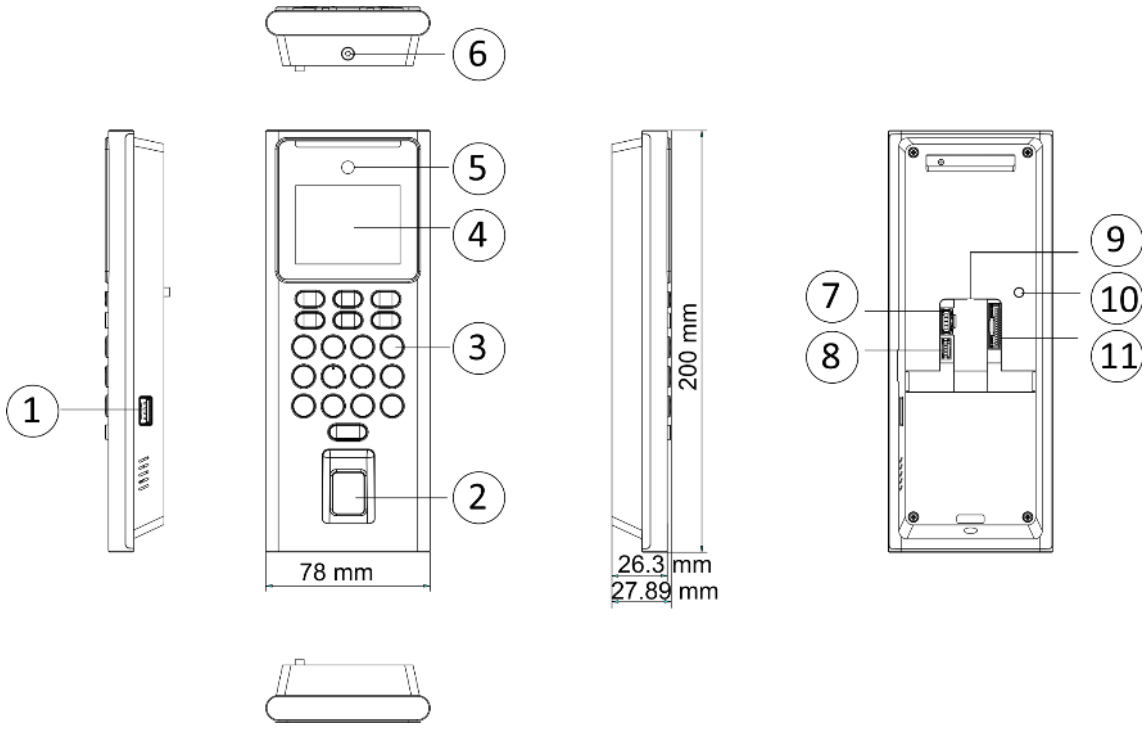


Figure 2-1 Appearance

Table 2-1 Appearance Description

No.	Name
1	USB Interface
2	Fingerprint Module **Note** Only devices that support the fingerprint function contain a fingerprint module.
3	Keypad
4	Screen
5	Camera
6	Screw Hole
7	Battery Interface

No.	Name
	Note You can access battery box to the interface. Battery box is not supplied. You can purchase it seperately.
8	Debugging Port (For Debugging Only)
9	Wiring Terminal (Including Power Supply Interface)
10	Tamper
11	Network Interface

Chapter 3 Installation

3.1 Installation Environment

- Indoor use only.
- Avoid backlight, direct sunlight, and indirect sunlight.
- For better recognition, there should be light source in or near the installation environment.
- The minimum bearing weight of the wall or other places should be 3 times heavier than the device weight.

3.2 Install with Gang Box

Steps

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

Note

You should purchase the gang box separately.

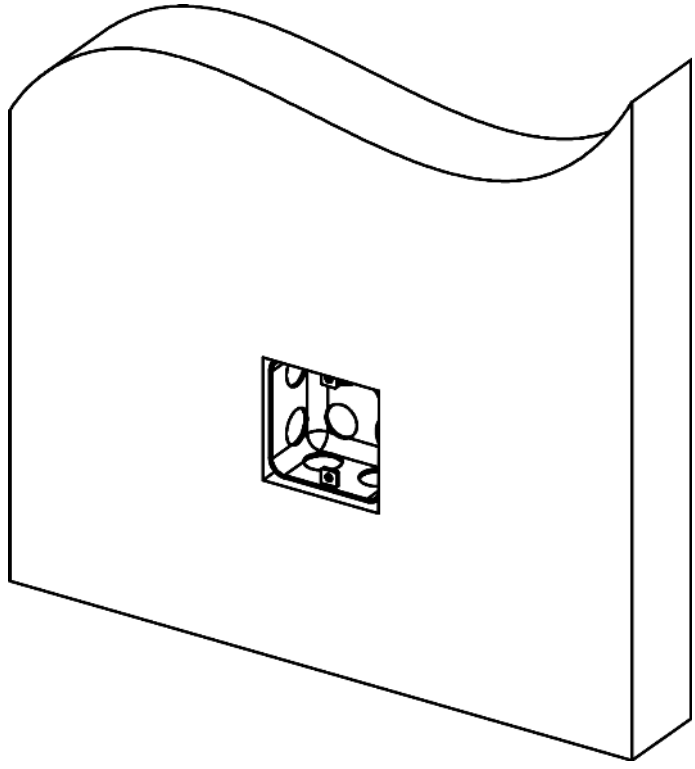


Figure 3-1 Install Gang Box

2. Secure the mounting plate on the gang box with two supplied screws (SC-KA4X25). Route the cable through the cable hole, wire the cables and insert the cables in the gang box.

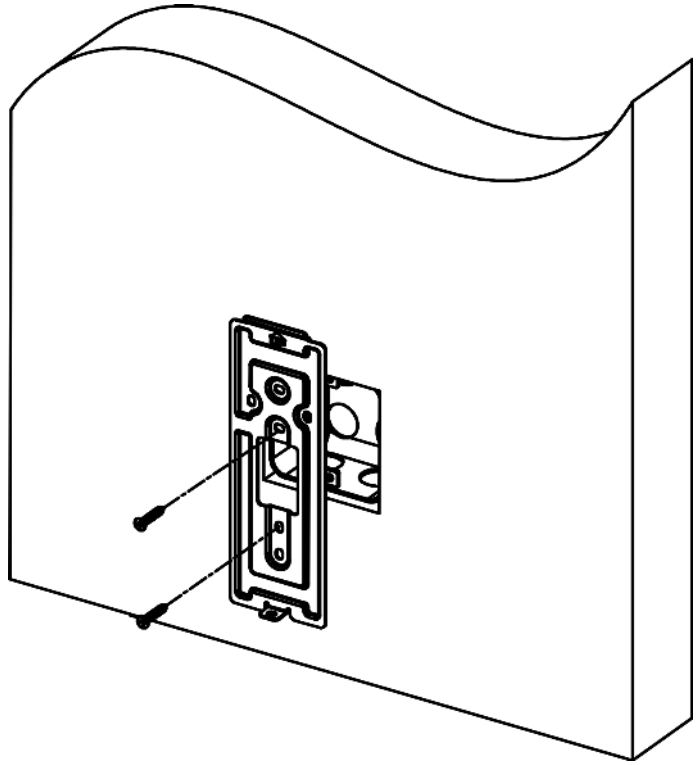


Figure 3-2 Install Mounting Plate

3. Align the device with the mounting plate, and secure the device on the mounting plate with 1 supplied screw (SC-CM3X8-B-T10-SUS).

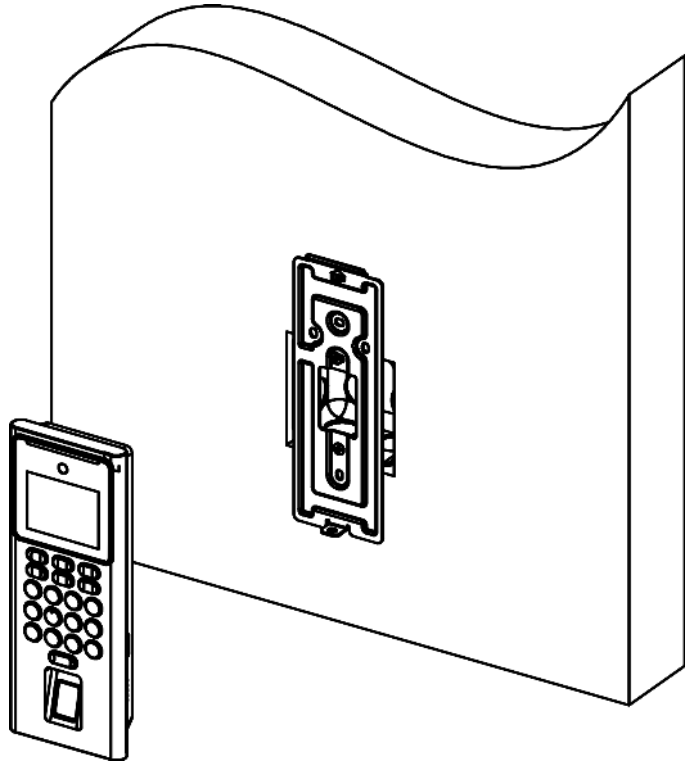


Figure 3-3 Secure Device

3.3 Install with Battery Plate

Steps

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

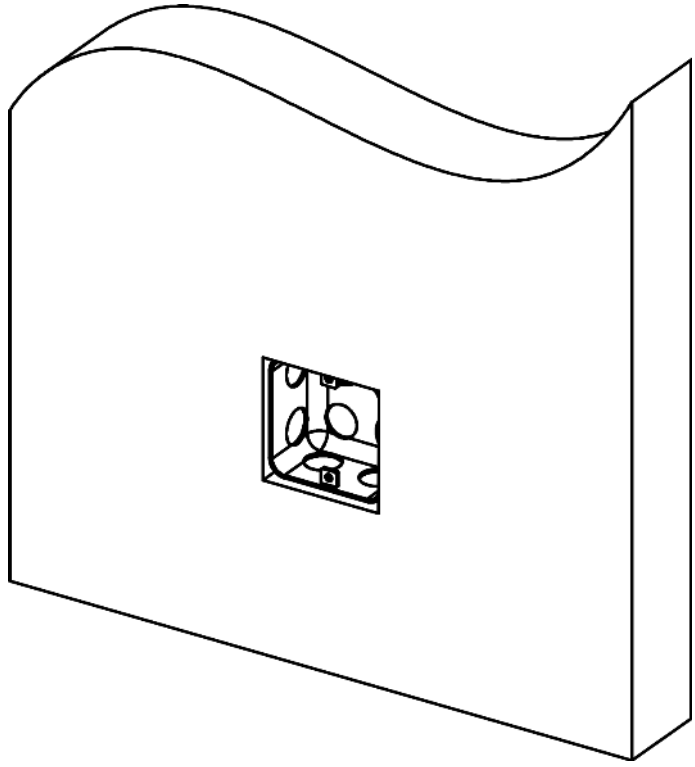


Figure 3-4 Install Gang Box

Note

Gang box and battery plate are not supplied. You can purchase separately.

2. Secure the battery plate on the gang box with two supplied screws (SC-KA4X25). Route the cable through the cable hole, wire the cables and insert the cables in the gang box.

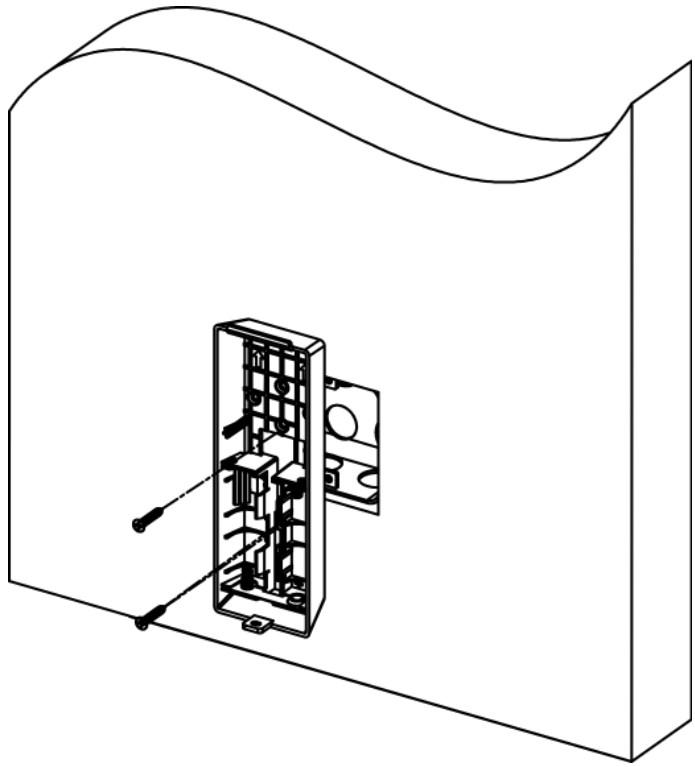


Figure 3-5 Install Mounting Plate

3. Align the device with the mounting plate, and secure the device on the battery plate with 1 supplied screw (SC-CM4X14-5T10-SUSS).

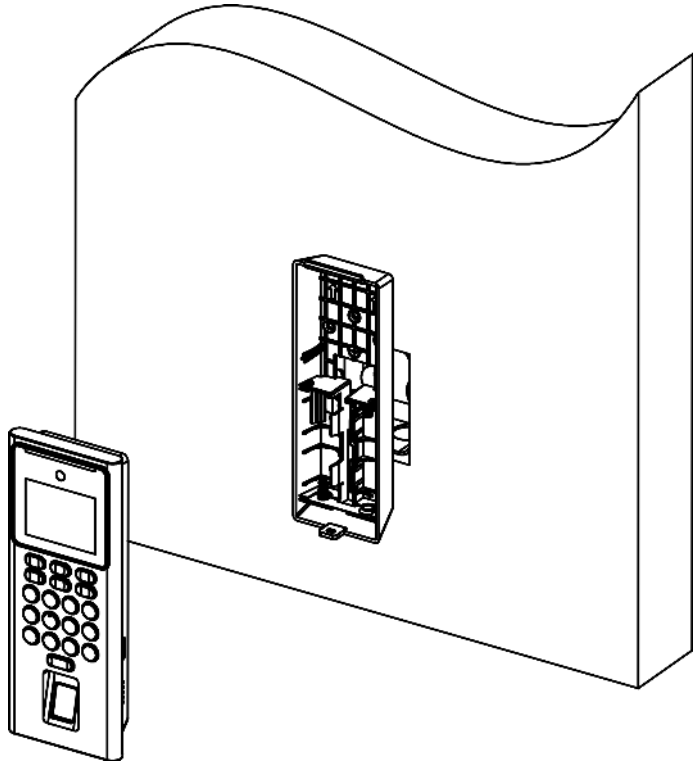


Figure 3-6 Hang Device

Chapter 4 Wiring

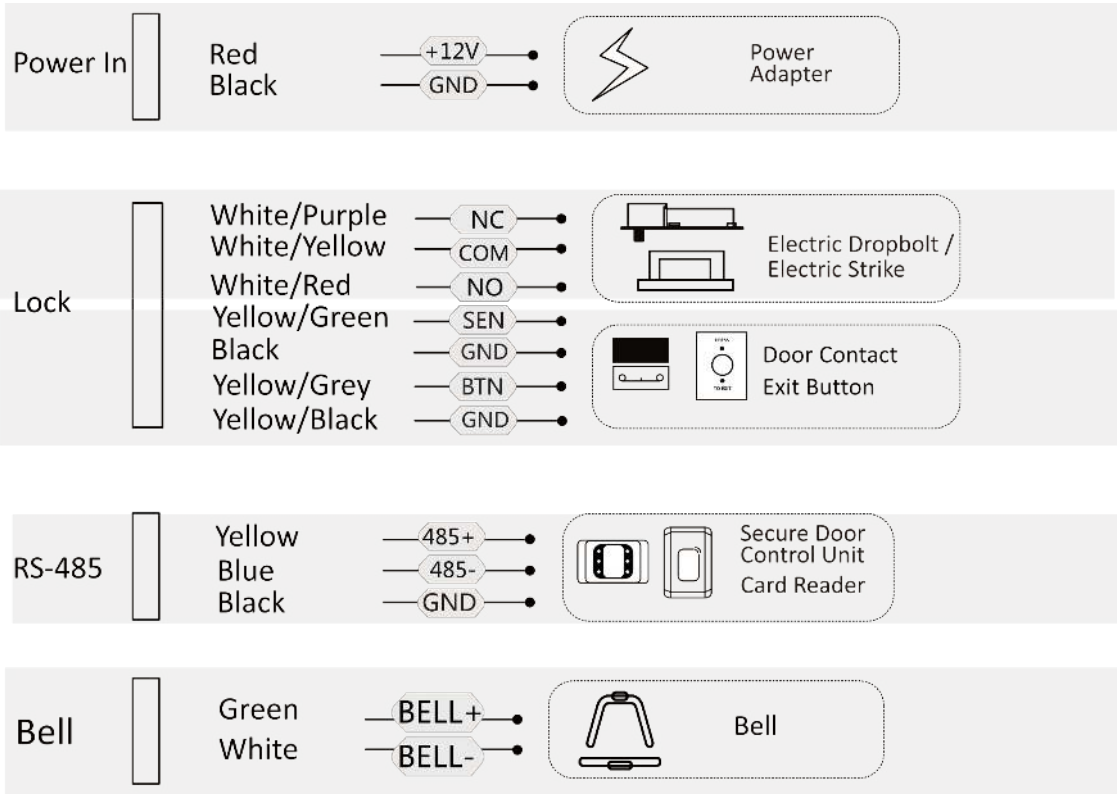
You can connect the NC/NO and COM terminal with the door lock, connect the SEN and GND terminal with the door contact and the BTN/GND terminal with the exit button.

Note

- If cable size is 18 AWG, you should use a 12 V power supply. And the distance between the power supply and the device should be no more than 20 m.
- If the cable size is 15 AWG, you should use a 12 V power supply. And the distance between the power supply and the device should be no more than 30 m.
- If the cable size is 12 AWG, you should use a 12 V power supply. And the distance between the power supply and the device should be no more than 40 m.
- The external card reader, door lock, exit button, and door magnetic need individual power supply.

4.1 Wire Normal Device

You can connect the terminal with normal peripherals.



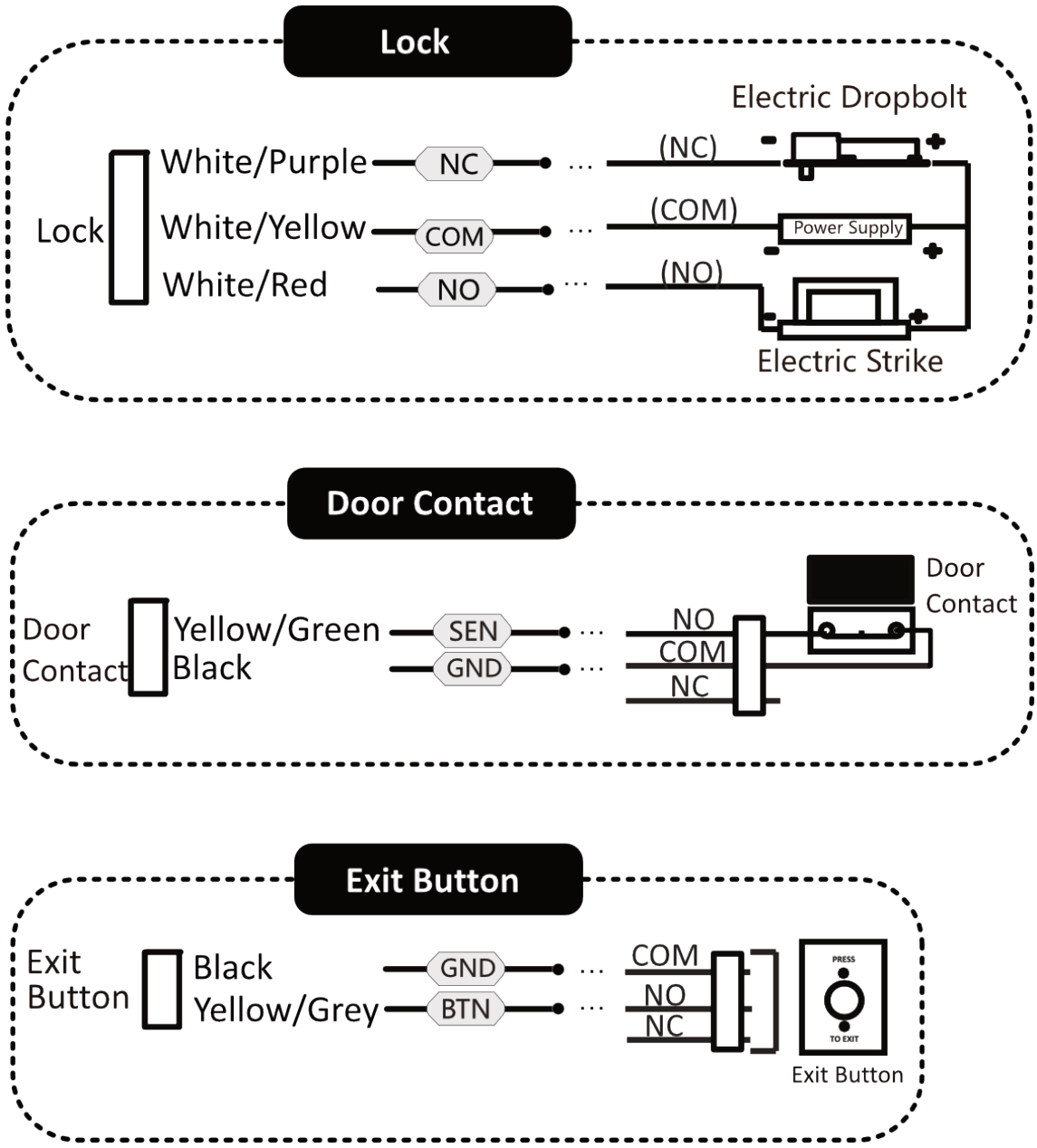


Figure 4-1 Wiring Terminal Description

Note

- Do not wire the device to the electric supply directly.
- When connecting door contact and exit button, the device should use the same common ground connection.
- The suggested external power supply for door lock is 12 V, 1 A

4.2 Wire Secure Door Control Unit

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

The wiring diagram is as follows.

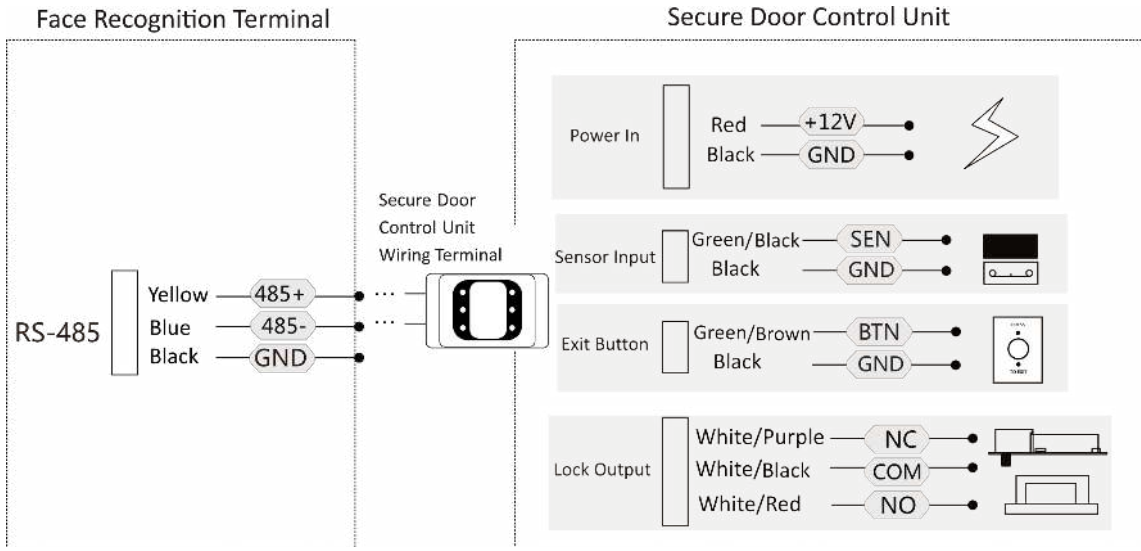


Figure 4-2 Secure Door Control Unit Wiring

Note

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

Chapter 5 Activation

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

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

The default values of the device are as follows:

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

5.1 Activate via Device

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

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



Figure 5-1 Activation Page

Caution

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

password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.
Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

Note

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

5.2 Activate via Mobile Web

You can activate the device via mobile web.

Steps

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

   Note

   - For inactive devices, hotspot is enabled by default.
   - The default hotspot password is the device serial number.

   The login page will pop up.
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 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.

5.4 Activate via SADP

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

Before You Start

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

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

Steps

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

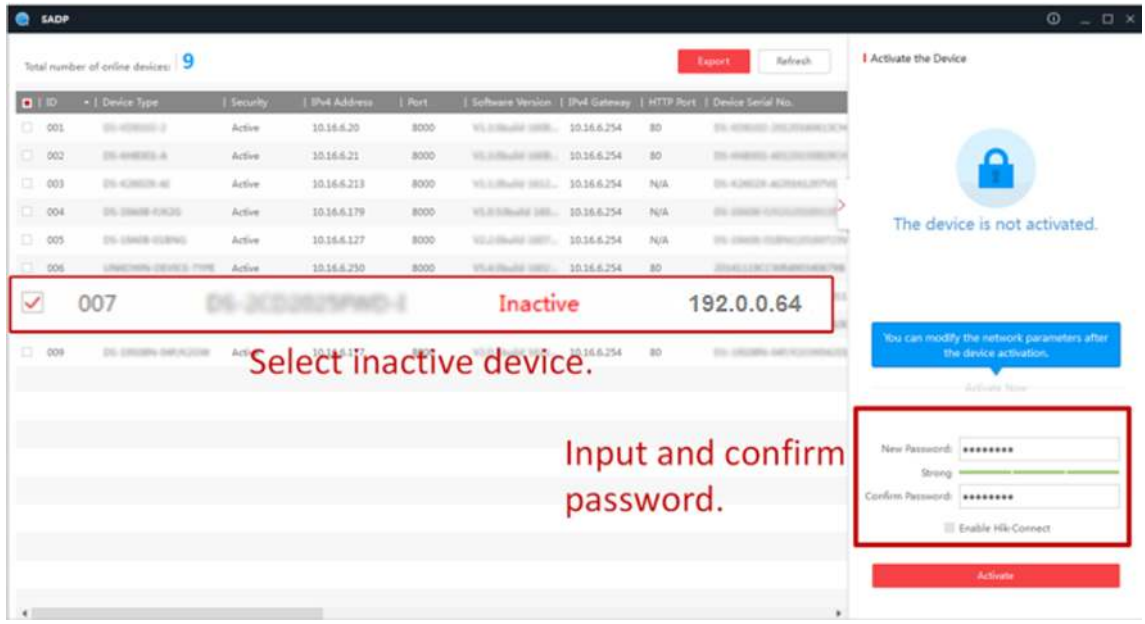
Caution

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

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.

5.5 Activate Device via iVMS-4200 Client Software

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

Steps

Note

This function should be supported by the device.

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

   The searched online devices are displayed in the list.
4. Check the device status (shown on **Security Level** column) and select an inactive device.

5. Click **Activate** to open the Activation dialog.
6. Create a password in the password field, and confirm the password.

Caution

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

Proper configuration of all passwords and other security settings is the responsibility of the 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.

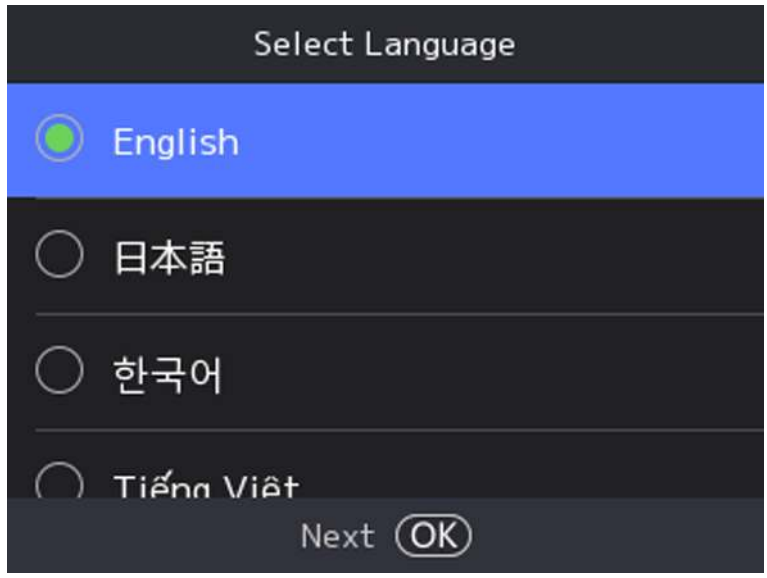


Figure 6-1 Select System Language

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 press **OK**.

Change via Security Questions

If you need to change password via security questions, you can set security questions on Web. Press **ESC**.

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, select **Wired Network** or **Wi-Fi** for your actual needs.



Figure 6-2 Select Network

Note

Disconnect the wired network before connecting a Wi-Fi.

2. Select **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 select **Add Wi-Fi** and enter the Wi-Fi's name and the password to get connected.

3. **Optional:** Select **Back** 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. Press **OK**.

6.5 Privacy Settings

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

Select parameters according to your actual needs.

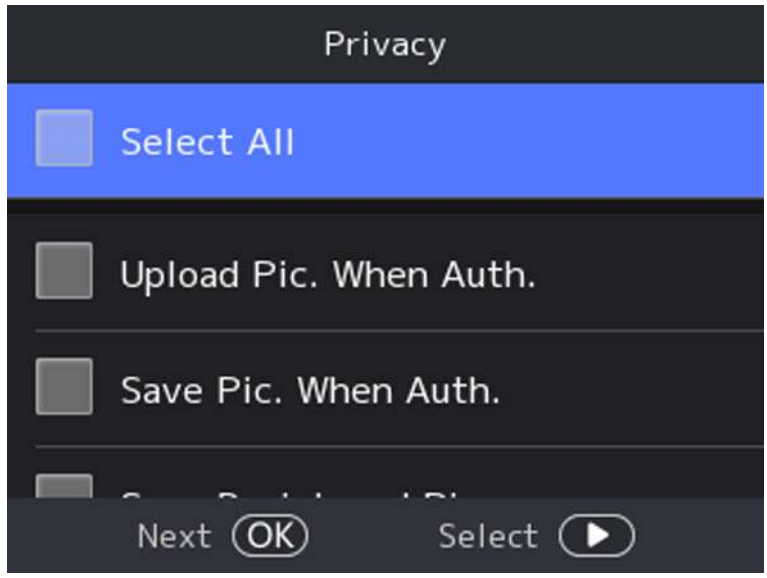


Figure 6-3 Privacy

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

Upload the pictures captured when authenticating to the platform automatically.

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

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

Save Registered Pic. (Save Registered Picture)

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

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

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

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

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

Select **OK** 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. Enter the employee ID, name and press **OK**.

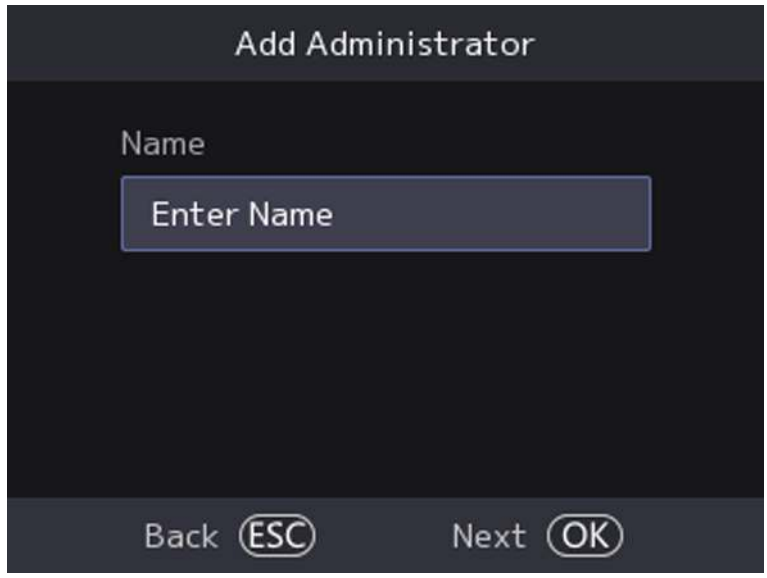


Figure 6-4 Add Administrator Page

2. 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. Press **OK** to capture and press **OK** to confirm.

-  : Press your finger according to the instructions on the device screen. Press **OK** to confirm.
-  : Enter the card No. or present card on the card presenting area. Press **OK** to confirm.

3. Press **OK**.

Chapter 7 Basic Operation

7.1 Login

Login the device to set the device basic parameters.

7.1.1 Login by Activation Password

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

Steps

1. Long press OK to enter Authenticate via Admin page.
2. Press to enter the password.
   - If you have added an administrator for the device, press OK and enter the password.
   - If you haven't added an administrator for the device, enter the password.
3. Press OK to enter the home page.

Note

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

7.1.2 Login by Administrator

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

Steps

1. Long press OK 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.

Note

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

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

7.1.3 Forgot Password

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

Steps

1. Long press OK to enter Authenticate via Administrator page.
2. Press to enter the password entering page, and then press ESC.
3. Select **Forgot Password**.
4. Answer the security questions that configured when activation.
5. Create a new password and confirm it.
6. Press **OK**.

7.2 Communication Settings

You can set the wired network, the Wi-Fi parameter, the RS-485 parameters, AP Mode, 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. Select **System Settings → Comm.** (Communication) to enter the Communication settings page.
2. On the Communication page, select **Wired Network**.

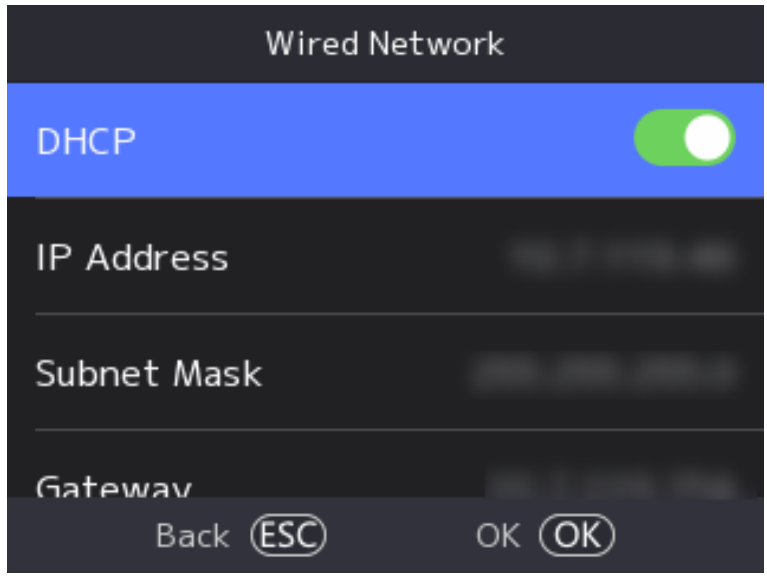


Figure 7-2 Wired Network Settings

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. Select **System Settings → Comm.** (Communication) to enter the Communication settings page.
2. On the Communication settings page, select **Wi-Fi**.



Figure 7-3 Wi-Fi Settings

3. Enable the Wi-Fi function.
4. Select a Wi-Fi from the list, and enter the Wi-Fi's password. 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. Press OK to save the settings and go back to the Wi-Fi tab.
7. Press ESC to save the network parameters.

7.2.3 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. Select **System Settings → Comm. → ISUP** .

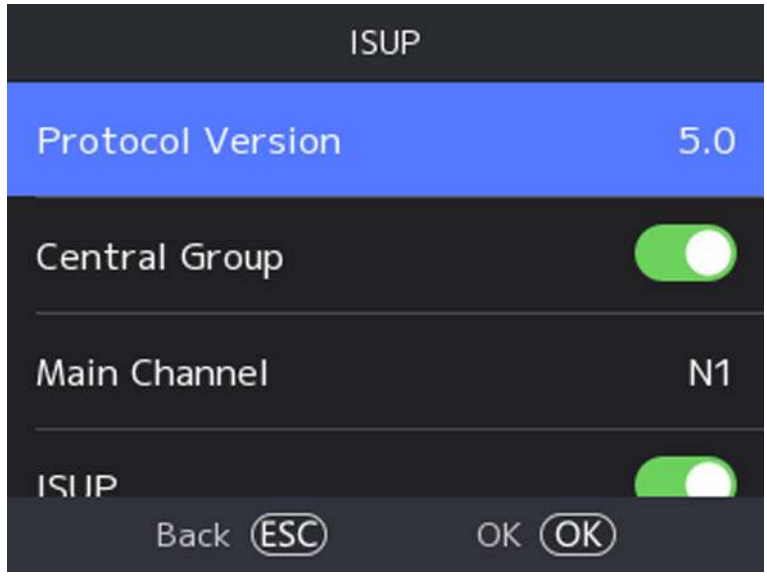


Figure 7-4 ISUP Settings

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

ISUP Version

Set the ISUP version according to your actual needs.

Central Group

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

Main Channel

Support N1 or None.

ISUP

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

Address Type

Select an address type according to your actual needs.

IP

Set the ISUP server's IP address.

Port

Set the ISUP server's port No.

Note

Port No. Range: 1 to 65535.

Device ID

Set device serial no.

ISUP Key

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

Note

- Remember the ISUP account and ISUP key. You should enter the account name or the key when the device should communicate with other platforms via ISUP protocol.
- ISUP key range: 8 to 16 characters.

7.2.4 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. Select **System Settings → Comm.** (Communication) on the Home page to enter the Communication settings page.
2. On the Communication settings page, select **Hik-Connect**.
3. Enable **Hik-Connect**
4. Enter **Server IP**.
5. Create the **Verification Code**, and you need to enter the verification code when you manage the devices via **Hik-Connect**.
6. Select **Device QR Code**, scan the QR code to bind the device.

7.2.5 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. Select **System Settings → Comm.** (Communication Settings) on the Home page to enter the Communication Settings page.
2. On the Communication Settings page, select **RS-485** to enter the RS-485 tab.
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. Select **ESC** and you should reboot the device if you change the parameters.

7.2.6 Set AP Mode

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

Steps

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

Note

- Hotspot Name: AP_Device serial No.
- Hotspot Password: Device serial No.
- The device Wi-Fi will be disabled when the AP mode is enabled.
- When the device is powered on for the first time, its hotspot is enabled by default and will automatically turn off after 30 minutes. Once successfully connected, your phone will automatically redirect to the Web interface, where you can perform activation and configuration operations.
- If your phone does not redirect automatically, please enter ***www.acsvis.com*** in your browser to access.

7.3 User Management

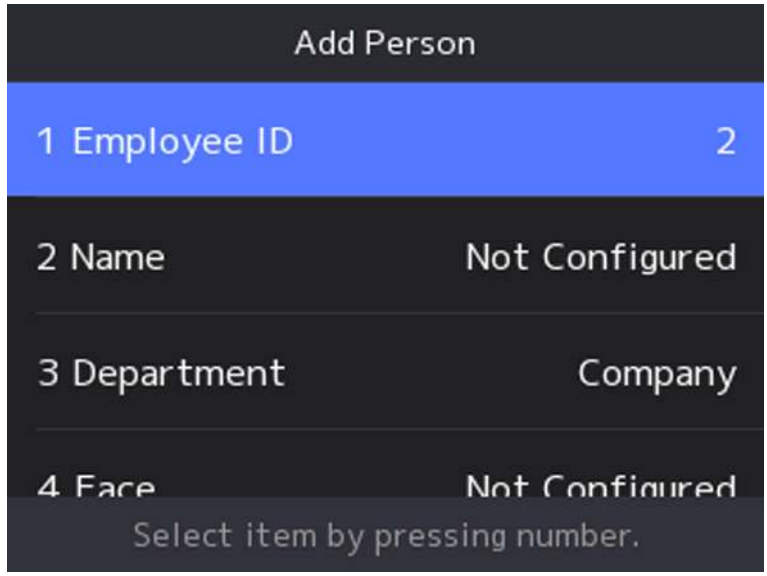
On the user management interface, you can add, edit, delete and search the user.

7.3.1 Add Administrator

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

Steps

1. Long press OK to enter the admin login page.
2. Select **User → Add 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. Select the Name field and input the user name on the keyboard.

Note

- Numbers, upper case letters, lower case letters, and special characters are allowed in the user name.
- Up to 128 characters are allowed in the user name.

5. Select the **Department**.
6. **Optional:** Add a face picture, fingerprints, cards, or PIN for the user.

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 ***View PIN code*** .

7. **Optional:** Set the user's authentication type.

Note

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

8. 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.

9. You can enable **Attendance Check Only**.
10. Press ESC and then press OK 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 500 face pictures can be added.

1. Long press OK and login the device.
2. Select **User → Add 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. Select the Name field and input the user name on the keyboard.

Note

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

5. Select the Face field to enter the face picture adding page.

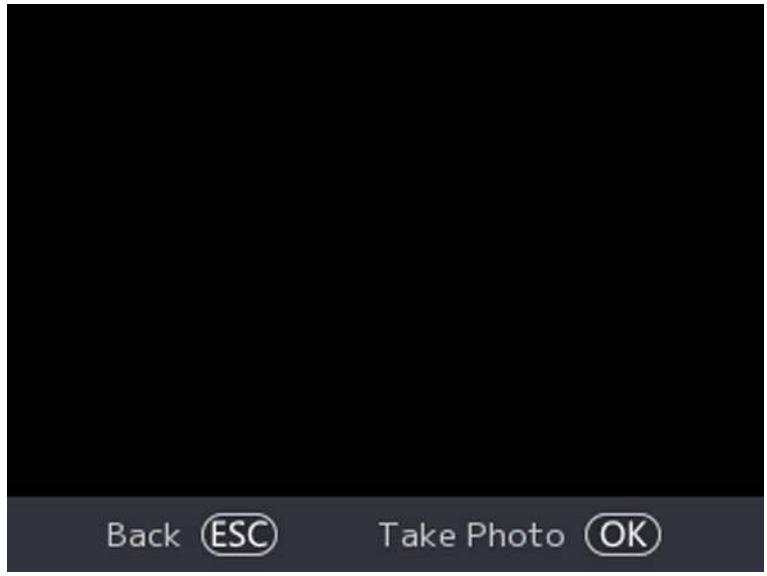


Figure 7-5 Add Face Picture

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 center of the page.

7. Press OK to save the face picture.
8. **Optional:** Press ESC to select **Retake** 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. Press ESC and then press OK 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 1000 fingerprints can be added.

1. Long press OK and login the device.
2. Press **User → Add User** to enter the Add User page.
3. Select 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. Select the Name field and input the user name on the keyboard.

   Note

   - Numbers, upper case letters, lower case letters, and special characters are allowed in the user name.
   - The suggested user name should be within 128 characters.
5. Select the Fingerprint field to enter the 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. Press ESC and then press OK 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

Note

The device supports EM card or M1 card. The supported card type varies between different models.

1. Long press OK and login the device.
2. Select **User → Add User** to enter the Add User page.
3. Select the Employee ID field and edit the employee ID.

   Note

   - The employee ID should be less than 32 characters. And it can be a combination of lower letters, upper letters, and numbers.
   - The employee ID should not be duplicated.
4. Select the Name field and input the user name on the keyboard.

   Note

   - Numbers, upper case letters, lower case letters, and special characters are allowed in the user name.
   - The suggested user name should be within 128 characters.
5. Select the Card field and press OK to enter the Add Card page.
6. Configure the card No.
   - Enter the card No. manually.
   - Present the card over the card swiping area to get the card No.

   Note

   - The card No. cannot be empty.
   - Up to 20 characters are allowed in the card No.
   - The card No. cannot be duplicated.
7. Configure the card type.
8. 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.
9. Press ESC and then press OK to save the settings.

7.3.5 View PIN code

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

Steps

1. Long press OK and login the device.
2. Select **User → Add 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. Select the Name field and input the user name on the keyboard.

Note

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

5. Select the PIN code and create a PIN for the user.

Note

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

6. Set the user role.

Administrator

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

Normal User

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

7. Press ESC and then press OK to save the settings.

7.3.6 Set Authentication Mode

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

Steps

1. Long press OK and login the device.
2. Select **User → Add User → Auth. Settings** .

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. Press ESC to save the settings.

7.3.7 Edit User

After adding the user, you can edit it.

Edit User

On the User Management page, select a user from the User List to enter the User Information page. Follow the steps in ***User Management*** to edit the user parameters. Press ESC to save the settings.

Note

The employee ID cannot be edited.

7.4 Local Time and Attendance

Manage department, shift, schedule, and report.

You can add, edit, delete department/shift/schedule. You can also export the attendance report.

7.4.1 Attendance Process Description

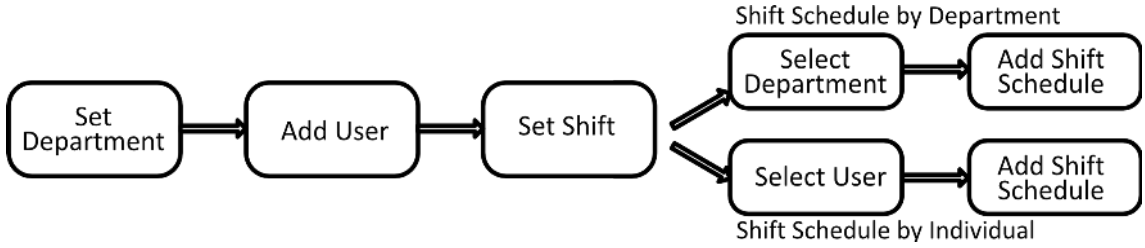


Figure 7-6 Attendance Process Description

7.4.2 Department Management

You can add, edit and delete the department.

Tap **Dept.** on the Home page to enter the settings page.

Add Department

Tap **+**, enter the department name, and tap **OK**.

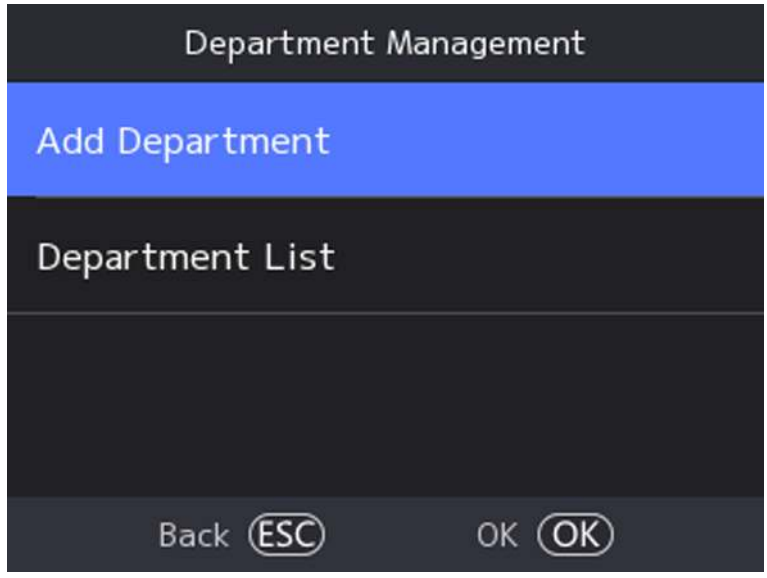


Figure 7-7 Add Department

Note

- The department name supports uppercase English, lowercase English, numbers and symbols.
- Up to 32 characters can be entered in department name.
- There are 7 departments in the department management by default.

Edit Department

Tap the department that needs to be edited, to edit the settings.
You can edit the department name, and view employee information according to your actual needs.

Delete Department

Tap the department that needs to be deleted.
Tap , and tap **OK** to delete the department.

7.4.3 Enable Local T&A

You can enable Local T&A, and set attendance rules, shift and schedule.

Steps

1. Long press **OK** to enter the admin login page.
2. Select **Local T&A**, and enable **Local T&A**.

7.4.4 Shift Management

Set Attendance Rule for Shift

Set attendance rule before setting shift.

Select **Local T&A → T&A → Shift Management → Attendance Rule** to enter the page.

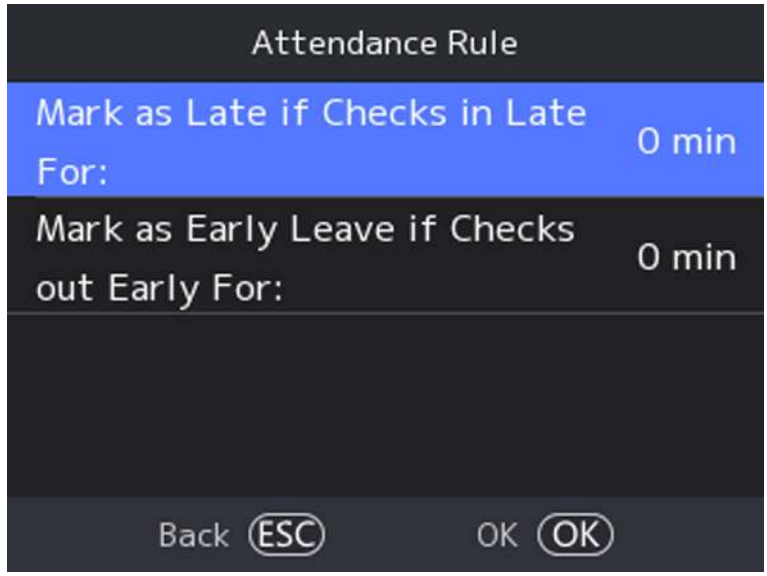


Figure 7-8 Attendance Rule

Set the attendance rule, including Mark as Later if Checks in Late For and Mark as Early Leave if Checks out Early For. After entering the duration, Select **OK** to save the settings.

Take the following picture as an example to describe the rules.

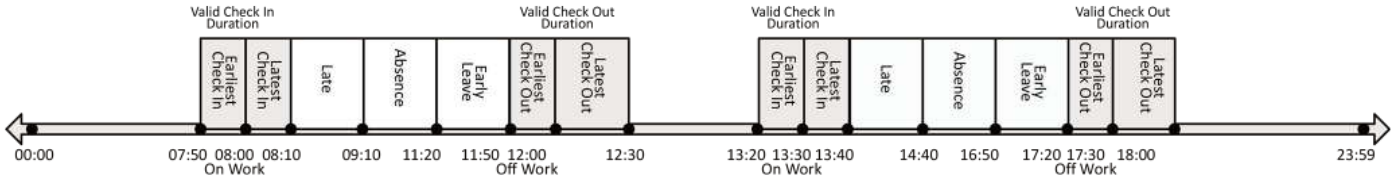


Figure 7-9 Attendance Rule Example

Mark as Early Leave if Checks out Early For

Set the Mark as Early Leave if Checks out Early For time. For example, set the off work time as 17:30 and set the parameter as 10 min, the earliest check out time will be 17:20. Checking out at or earlier than 17:19 will be marked as invalid.

Mark as Later if Checks in Late For

Set the Mark as Later if Checks in Late For time. For example, set the off work time as 17:30 and set the parameter as 30 min, the latest check out time will be 18:00. Checking out at or later than 18:01 will be marked as invalid.

Note

By default, if set as 0 min, the valid check out time ends at 23:59:59.

Note

- The unit is min.
- The available time is from 0 to 1440 min.

Set Shift

Edit or add the shift attendance information, including the shift name, the shift period, and the overtime shift period. You can also reset the normal shift after editing.

Before You Start

Set the attendance rule. For details, see ***Set Attendance Rule for Shift*** .

Steps

1. Select **Local T&A → T&A → Shift Management** to enter the page.

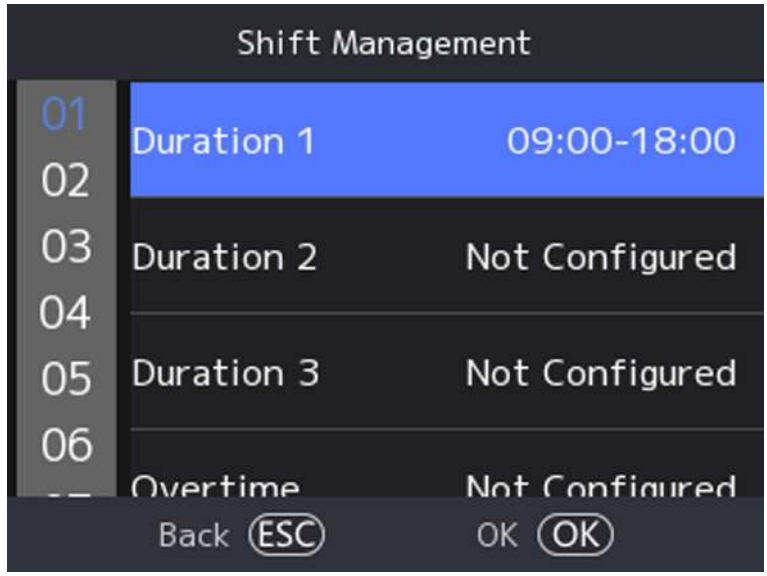


Figure 7-10 Shift Management

2. Set the shift name and period in order and set the overtime shift period according to your needs.

Note

- If the attendance rules conflict with the normal shift period, the device will prompt "Incorrect Time Duration". Delete all configured time durations and reset after exiting.
- The shift name supports numbers, uppercase letters, lowercase letters, Chinese characters and symbols.
- Up to 32 characters are allowed in the shift name.

3. Select **OK** to save the settings.

7.4.5 Shift Schedule

Combine shift and holiday according to your actual needs. Scheduling shift by department and scheduling shift by individual are supported.

Schedule Shift by Department: All persons in the department use the same shift schedule to take attendance.

Schedule Shift by Individual: Take attendance according to individual's conditions.

Shift Schedule by Department

All persons in the department use the same shift schedule to take attendance.

Before You Start

- Edit department. For details, see ***Department Management*** .
- Set shift. For details, see ***Set Shift*** .

Steps

1. Select **Local T&A → T&A → Schedule** to enter the Shift Schedule by Department page.
2. Select **Add Shift Schedule**.
3. Select the **Department/Person**, select a department. For details, see ***Department Management*** .
4. Set **Shift** according to your actual needs.
5. Select **OK**.
6. **Optional:** You can edit the schedule information in **Shift Schedule List**.

Shift Schedule by Person

Take attendance according to individual's conditions.

Before You Start

- Add user before setting shift schedule by individual. For details, see ***User Management*** .
- Set shift. For details, see ***Set Shift*** .

Steps

1. Select **Local T&A → T&A → Schedule** to enter the Shift Schedule by Department page.
2. Select **Add Shift Schedule**.
3. Select the **Department/Person**, select the person. For details, see ***User Management*** .
4. Set **Shift** according to your actual needs.
5. Select **OK**.
6. **Optional:** You can edit the schedule information in **Shift Schedule List**.

7.5 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.

7.5.1 Disable Attendance Mode via Device

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

Select **Platform Attendance** to enter the settings page.

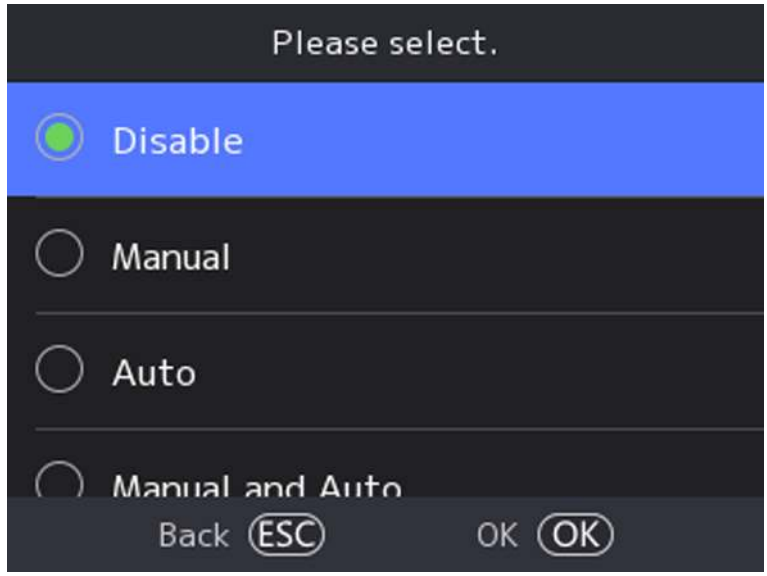


Figure 7-11 Disable Attendance Mode

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.

7.5.2 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. Select **Platform Attendance** to enter the settings page.
2. Set the **Attendance Mode** as **Manual**.

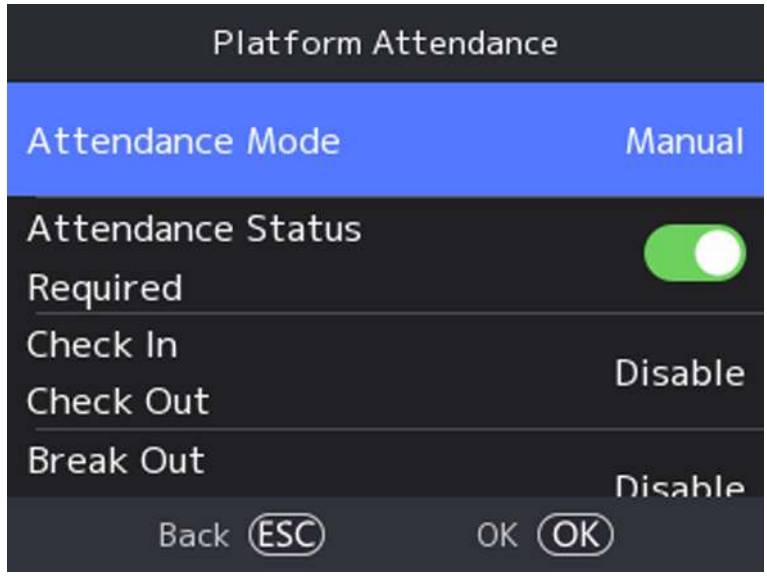


Figure 7-12 Manual Attendance Mode

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.

7.5.3 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. Select **Platform Attendance** to enter the settings page.
2. Set the **Attendance Mode** as **Auto**.

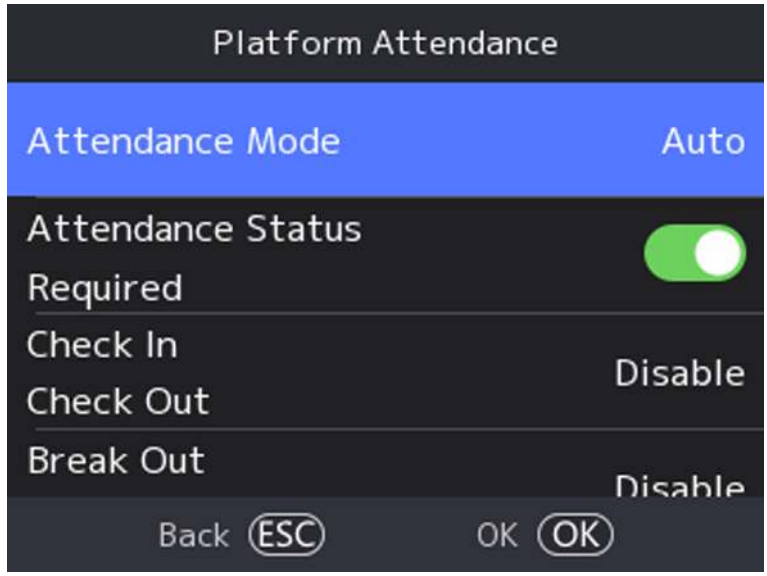


Figure 7-13 Auto Attendance Mode

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

Note

The Attendance Property will not be changed.

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

   The name will be displayed on the T & A Status page and the authentication result page.
6. Set the status' schedule.
   1) Select **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) Press OK.
   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.

7.5.4 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. Select **Platform Attendance** to enter the settings page.
2. Set the **Attendance Mode** as **Manual and Auto**.

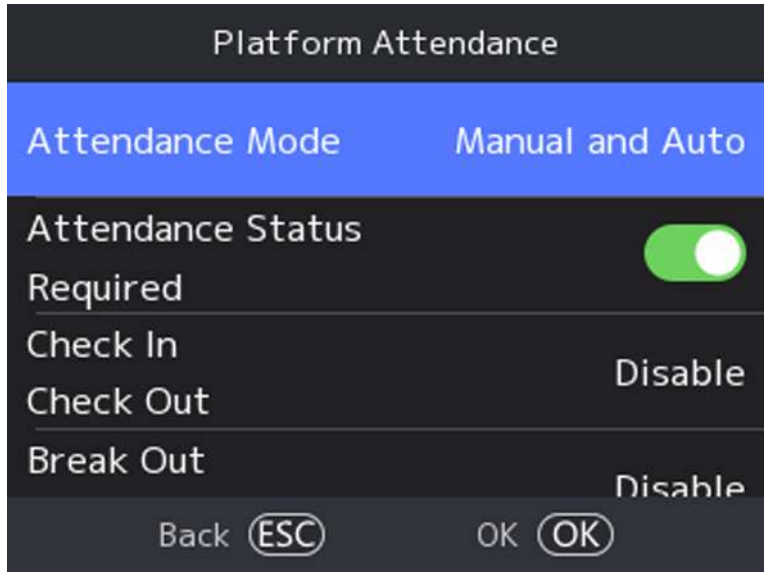


Figure 7-14 Manual and Auto Mode

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

Note

The Attendance Property will not be changed.

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

   The name will be displayed on the T & A Status page and the authentication result page.
6. Set the status' schedule.
   1) Select **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) Press 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.

7.6 Attendance Report

You can export Total Reports, Attendance Record, Summary Report, Abnormal Attendance, Shift Schedule and Attendance Card.

Select **Attendance Report**, plug a USB flash drive, and you can select to export Total Reports, Attendance Record, Summary Report, Abnormal Attendance, Shift Schedule and Attendance Card.

7.7 Data Management

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

7.7.1 Delete Data

Delete user data.

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

7.7.2 Import Data

Steps

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

7.7.3 Export Data

Steps

1. Plug a USB flash drive in the device.
2. On the Home page, select **Data → Export Data** .
3. Select **Face Data**, **Event Data**, **User 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 1G to 32G. 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.

7.8 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.

7.8.1 Authenticate via Single Credential

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

Authenticate face, fingerprint, card or PIN.

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 swiping area and start authentication via card.

Note

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

PIN Code

Enter the pin code to authenticate via PIN code.

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

7.8.2 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.

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.

7.9 Basic Settings

You can set the sound, time, screen off time, language, supplement light and video standard.

Long press OK and login the device. Select **System Settings → Basic** to enter Basic Settings page.

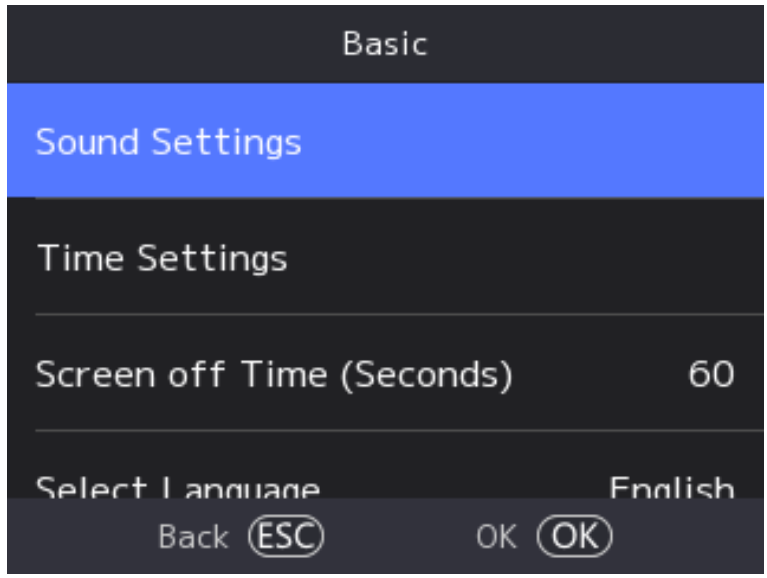


Figure 7-15 Basic Settings Page

Sound Settings

You can enable/disable the sound function.

Time Settings

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

Screen Off Time

Set the device sleeping waiting time (s). For example, 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

20 s to 999 s are available to configure.

Select Language

Select the language according to actual needs.

Supplement Light

Set the white light mode, brightness, start time and end time.

Video Standard

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.

7.10 Set Privacy Parameters via Device

Set the picture uploading parameters.

Note

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

Login the device. .

Select **System → Basic → Privacy** .

Authentication Settings

Name / Employee ID / Face Picture

You can choose to display/not display name, employ ID, or face picture when authenticating. You can choose to desensitize name and Employ ID when authenticating.

Picture Uploading and Storage

Set picture uploading and storage parameters.

Save Registered Pic.

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

Save Pic. After Linked Capture

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

Upload Picture After Linked Capture

Upload the pictures captured after linked capture.

Save Pic When Auth.

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

Upload Pic. When Auth.

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

7.11 Password Management

You can change device password.

Steps

1. Long press **OK** and login the device. Select **System Settings → Basic → Password** .
2. Select **Change Password**. Enter the old password.
3. Enter the new password and confirm it.
4. Select **OK**.

Note

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

7.12 Set Biometric Parameters

You can customize the face parameters to improve the face recognition performance. The configurable parameters includes face liveness level, face recognition distance, face recognition interval, face 1:N security level, face 1:1 security level.

Long press OK and login the device. Select **System Settings**to enter System Settings page. Then select **Biometrics** to enter Biometrics settings page.

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.
Face Recognition Distance	Set the valid distance between the user and the camera when authenticating.
Face Recognition Interval	The time interval between two continuous face recognitions when authenticating.

Parameter	Description
	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.
Face Duplicate Check	Enable **Face Duplicate Check**. After enabling the function, when adding person's face, the system will check the duplication. If there is duplicated face picture detected in the system, a prompt will be pop up.

7.13 Set Authentication Parameters

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

On the home page, select **Authentication Settings** (Access Control Settings) to enter the page. Edit the access control parameters on this page.

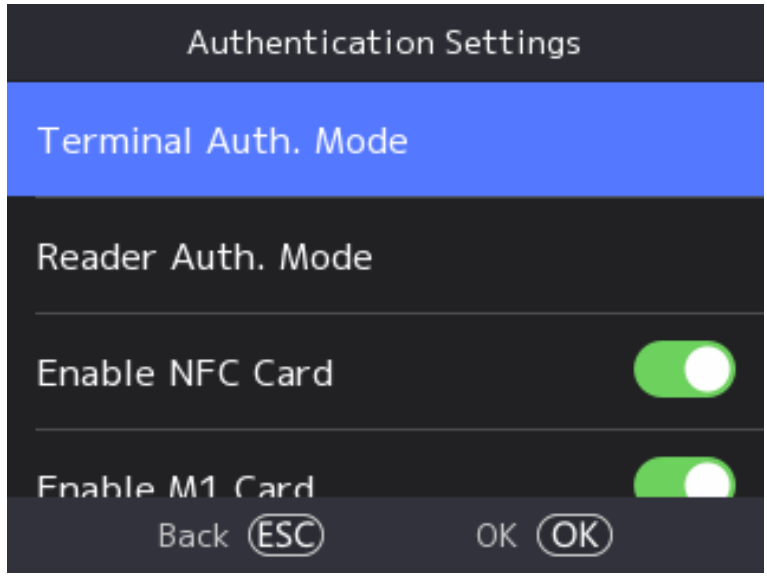


Figure 7-16 Authencation Parameters

The available parameters descriptions are as follows:

Table 7-2 Access Control Parameters Descriptions

Parameter	Description
Terminal Authentication Mode	Select the face recognition terminal's authentication mode. You can also customize the authentication mode. **Note** • Only the device with the fingerprint module supports the fingerprint related function. • Biometric recognition products are not completely applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes. • If you adopt multiple authentication modes, you should authenticate other methods before authenticating face.
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.
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.
Door Contact	You can select "Remain Open" or "Remain Closed" according to your actual needs. By default, it is "Remain 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**

Parameter	Description
	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.

7.14 Preference Settings

You can configure preference settings parameters.

Steps

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

   Theme

   You can set the theme of the prompt window on the authentication page. You can select **Theme** as **Authentication/Simple**.

   Authentication

   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.

   Simple

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

2. Select **OK** .

7.15 System Maintenance

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

Long press OK and login the device. Select **Maint.** to enter System Maintenance page.

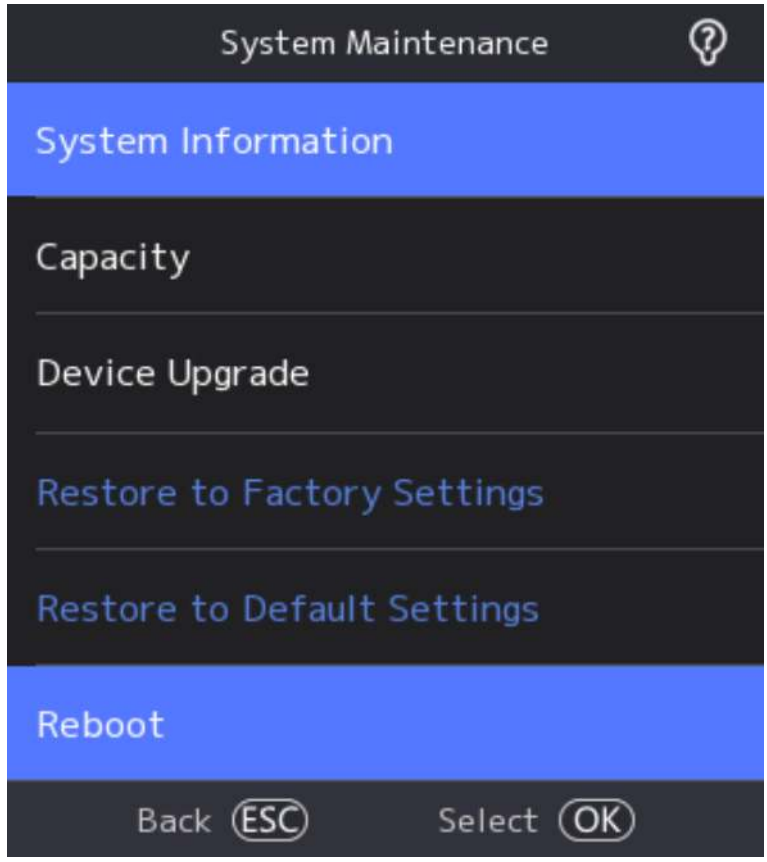


Figure 7-17 Maintenance Page

System Information

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

Note

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

Capacity

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

Note

Parts of the device models support displaying the fingerprint number. 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 select **Device Upgrade → Online Update** to upgrade the device system.

Update via USB

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

User Manual

You can scan the QR code to view the 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.



Select **System Information →** , long press **OK**, and enter admin password to set the face

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.

Chapter 8 Configure the Device via the Mobile Browser

When the device is powered on for the first time, its hotspot is enabled by default and will automatically turn off after 30 minutes. To reconnect, it must be manually enabled. Use your phone to turn on WLAN, search for the device's hotspot, and connect to it (the hotspot name is "AP_[Device Serial No.]", and the password is the device serial No.). Once successfully connected, your phone will automatically redirect to the Web interface, where you can perform activation and configuration operations.

If your phone does not redirect automatically, please enter ***www.acsvis.com*** in your browser to access.

8.1 Login

You can login via mobile browser.

Note

- 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, network status and basic information, and set person management, smart settings, authentication settings, 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.

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.

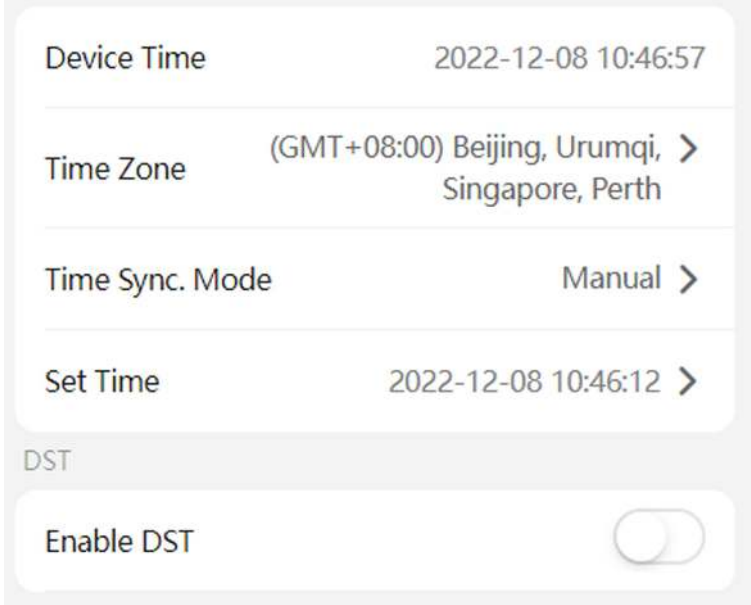


Figure 8-1 Time Settings

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.

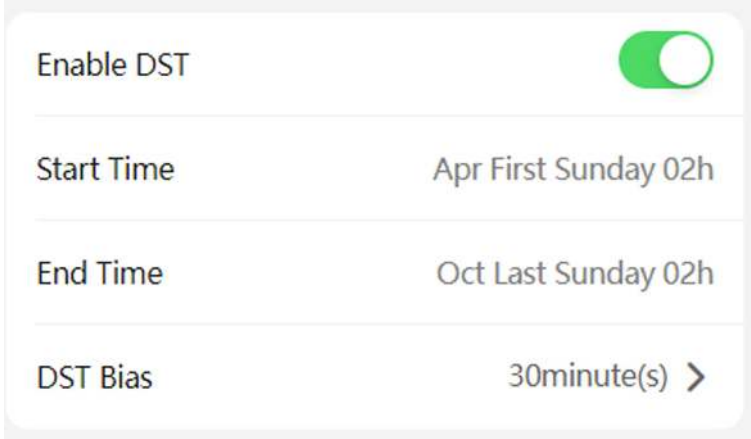


Figure 8-2 DST

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**.

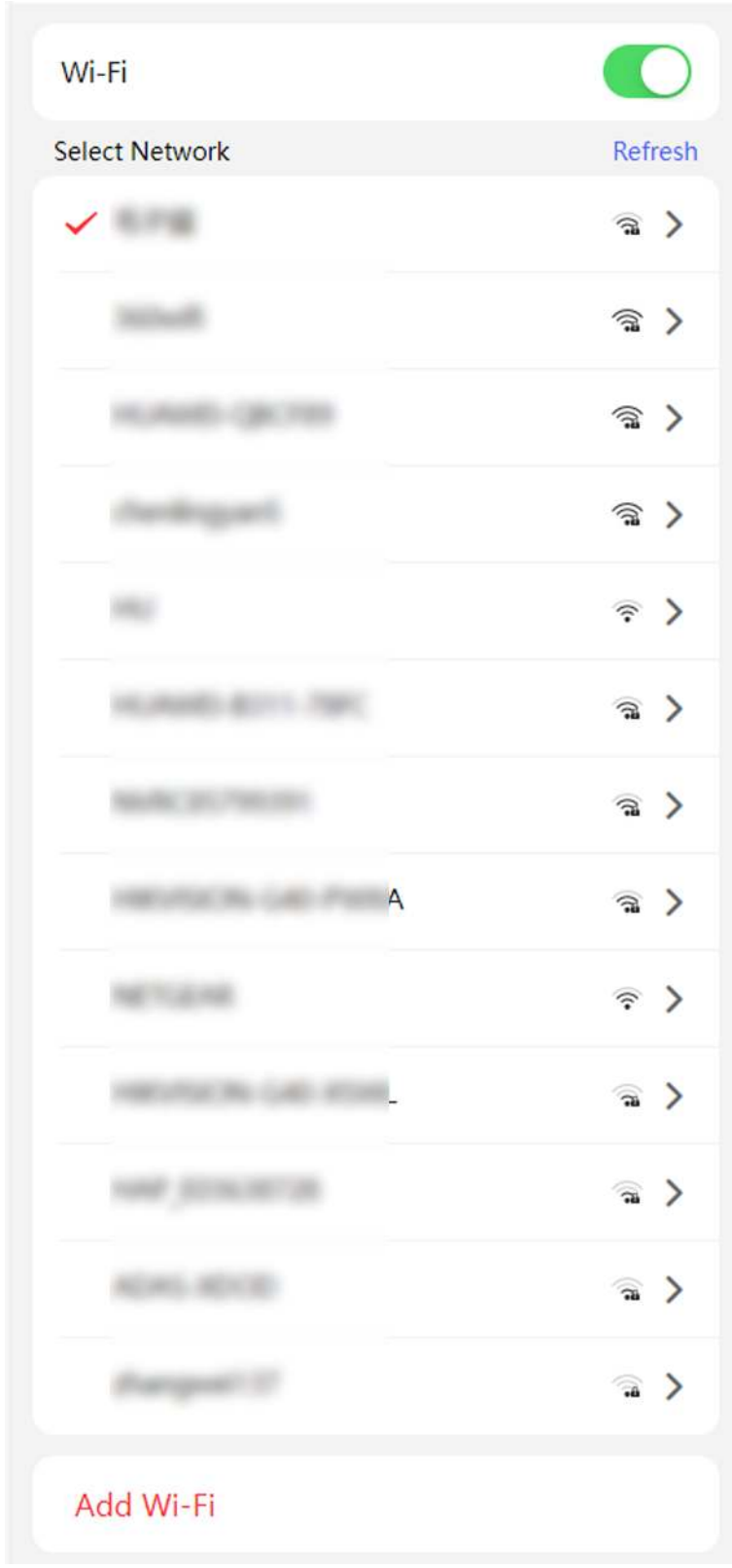


Figure 8-3 Wi-Fi

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 Device Hotspot

Set the device hotspot, and mobile phone can connect to the device to enter the mobile browser.

Steps

1. Tap → **Network Settings** → **Device Hotspot** .
2. You can enable device hotspot and view the hotspot name.

Note

- Hotspot Name: AP_Device serial No.
- Hotspot Password: Device serial No.
- The device Wi-Fi will be disabled when the AP mode is enabled.
- When the device is powered on for the first time, its hotspot is enabled by default and will automatically turn off after 30 minutes. Once successfully connected, your phone will automatically redirect to the Web interface, where you can perform activation and configuration operations.
- If your phone does not redirect automatically, please enter ***www.acsvis.com*** in your browser to access.

3. 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.

Web Authentication

You can select Digest Algorithm. Digest algorithm applies to both HTTP and HTTPS.

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.

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.

8.4.11 Set Time and Attendance via Mobile Web Browser

You can set time and attendance by managing department, user, shift, holiday, and shift schedule. You can add, edit, and delete attendance department, user, shift, holiday, and shift schedule.

Manage Department via Mobile Web Browser

You can add, edit and delete the department.

Steps

1. Tap → **Department Management** to enter the settings page.
2. Add the department.
   1) Tap **+**.
   2) Enter the department name, and tap **OK**.

Note

- The department name supports uppercase English, lowercase English, numbers and symbols.
- Up to 32 characters can be entered in department name.
- There are 7 departments in the department management by default.

3. **Optional:** You can view employee according to your actual needs.
4. Delete the department.
   1) Tap the department that needs to be deleted.
   2) Tap , and tap **OK** to delete the department.

Set Attendance Rule for Shift

Set attendance rule before setting shift.

Tap → **Time and Attendance** → **Attendance Rule** to enter the page.

Set the attendance rule, including Mark as Later if Checks in Late For and Mark as Early Leave if Checks out Early For. After entering the duration, tap **Save** to save the settings.

Take the following picture as an example to describe the rules.

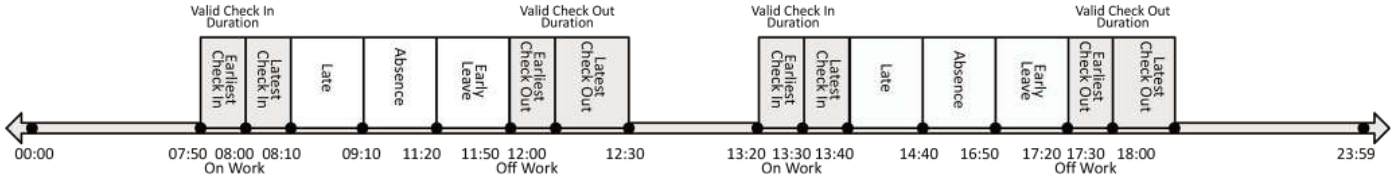


Figure 8-4 Attendance Rule Example

Mark as Early Leave if Checks out Early For

Set the Mark as Early Leave if Checks out Early For time. For example, set the off work time as 17:30 and set the parameter as 10 min, the earliest check out time will be 17:20. Checking out at or earlier than 17:19 will be marked as invalid.

Mark as Later if Checks in Late For

Set the Mark as Later if Checks in Late For time. For example, set the off work time as 17:30 and set the parameter as 30 min, the latest check out time will be 18:00. Checking out at or later than 18:01 will be marked as invalid.

Note

By default, if set as 0 min, the valid check out time ends at 23:59:59.

Note

- The unit is min.
- The available time is from 0 to 1440 min.

Manage Shift via Mobile Web Browser

You can set the normal shift and man-hour shift. Normal shift can be applied in attendance scenarios of regular attendance, and you can set the attendance rules and the attendance number. Man-hour shift can be applied in the attendance scenarios of flexible working system.

Manage Normal Shift via Mobile Web Browser

You can edit and add shift attendance information, including shift name and attendance duration.

Steps

1. Set attendance rules.
   1) Tap → **Time and Attendance** → **Shift Management** .
2. Set shift.
   1) Tap a normal shift to enter the settings page.
   2) Set the **Shift Name**, **On-Work Time**, and **Off-Work Time**.

Note

- If the attendance rules conflict with the normal shift durations, the device will prompt "Duration error". Please delete all durations and reconfigure the settings after exiting.
- The shift name supports Chinese, uppercase English, lowercase English, numbers and symbols.
- Up to 32 characters can be entered in shift name.

3) You can enable **Set Overtime**, and set the start time and end time.

3. Tap **Save**.

Manage Flexible Shift via Mobile Web Browser

You can edit and add shift attendance information, including shift name and work duration.

Steps

1. Set attendance rules.
   1) Tap → **Time and Attendance** → **Shift Management** .
2. Set shift.
   1) Tap **Add Shift** to enter the settings page.
   2) Set the **Shift Name**, **Work Duration**, and **Latest On-Work Time**.

Note

- If the attendance rules conflict with the normal shift durations, the device will prompt "Duration error". Please delete all durations and reconfigure the settings after exiting.
- The shift name supports Chinese, uppercase English, lowercase English, numbers and symbols.
- Up to 32 characters can be entered in shift name.

   3) You can enable break according your actual needs.
3. Tap **Save**.

Manage Shift Schedule via Mobile Web Browser

You can combine the shift and holiday according to your actual needs. Shift schedule by department and shift schedule by individual are supported.

Manage Shift Schedule by Department via Mobile Web Browser

All persons in the department use the same shift schedule to take attendance.

Before You Start

- Edit the department. You can refer to ***Manage Department via Mobile Web Browser*** for details.
- Set the shift. You can refer to ***Manage Normal Shift via Mobile Web Browser*** for details.

Steps

1. Tap → **Time and Attendance** → **Schedule** to enter the Shift Schedule page.
2. Tap **Add Schedule**.
3. Set **Schedule Name**.
4. Select the **Department**. For details, see ***User Management*** .
5. Select **Shift Type**.

Note

- If you select **Quick Schedule**, you need to set **Day of Week**, **On-duty Time** and **Off-duty Time**.
- If you select **Advanced Schedule**, you need to set **Day of Week**, **Shift** and choose to enable **Holiday Settings** or not.

6. Tap **Complete**.

Shift Schedule by Person

Take attendance according to individual's conditions.

Before You Start

- Edit person. For details, see ***User Management*** .
- Set the shift. You can refer to ***Manage Normal Shift via Mobile Web Browser*** for details.

Steps

1. Tap → **Time and Attendance** → **Schedule** to enter the Shift Schedule page.
2. Tap **Add Schedule**.
3. Set **Schedule Name**.
4. Select the **Person**. For details, see ***User Management*** .
5. Set **Schedule Name** and **Schedule Type** according to your actual needs.

Note

- If you select **Quick Schedule**, you need to set **Day of Week**, **On-duty Time** and **Off-duty Time**.
- If you select **Advanced Schedule**, you need to set **Day of Week**, **Shift** and choose to enable **Holiday Settings** or not.

6. Tap **Complete**.

View Attendance Statistics

You can view Attendance Statistics by day or month.

You can view attendance statistics by the following ways.

1. Tap **Attendance Statistics**.
2. Tap → **Attendance Statistics** .

You can tap **Day** or **Month** to view attendance statistics.

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.

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

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 **Device Language Settings** page. You can select a language for the device system from the drop-down list.

By default, the system language is English.

Note

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

9.3 Time Settings

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

Time Zone

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

Time Sync.

NTP

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

Manual

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

Server Address/NTP Port/Interval

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

DST

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

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

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.

Picture Uploading and Storage

Save Picture When Authenticating

Save picture when authenticating automatically.

Upload Picture When Authenticating

Upload the pictures when authenticating to the platform automatically.

Save Registered Picture

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

Upload Picture After Linked Capture

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

Save Pictures After Linked Capture

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

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

9.5 Administrator Settings

Steps

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

Note

You should select at least one credential.

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

Note

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

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

Note

Up to 50 cards can be supported.

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

Note

Up to 10 fingerprints are allowed.

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 Network System Network** settings page.
2. Set the device type.

Note

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

Device Type

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

Community No.

Set the device community No.

Building No.

Set the device building No.

Unit No.

Set the device unit No.

Floor No.

Set the device installed floor No.

Door Station No.

Set the device installed door station No.

Note

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

Outer Door Station No.

Set the device installed outer door station No.

Note

The No. ranges from 1 to 99.

3. Set the video intercom network parameters.

Registration Password

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

Main Station IP

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

Private Server IP

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

Enable Protocol 1.0

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

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

Chapter 10 Operation via Web Browser

10.1 Login

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

Note

Make sure the device is activated.

Login via Web Browser

Enter the device IP address in the address bar of the web browser and press **Enter** to enter the login page.
Enter the device user name and the password. Click **Login**.

Login via Remote Configuration of Client Software

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

10.2 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 → **User Manual** or scan the QR code 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.

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

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 **Device Language Settings** page. You can select a language for the device system from the drop-down list.

By default, the system language is English.

Note

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

10.5.3 Time Settings

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

Time Zone

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

Time Sync.

NTP

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

Manual

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

Server Address/NTP Port/Interval

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

DST

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

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

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.

Picture Uploading and Storage

Save Picture When Authenticating

Save picture when authenticating automatically.

Upload Picture When Authenticating

Upload the pictures when authenticating to the platform automatically.

Save Registered Picture

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

Upload Picture After Linked Capture

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

Save Pictures After Linked Capture

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

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

10.5.5 Administrator Settings

Steps

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

2. Enter the employee ID and name of the administrator.
3. Select a credential to add.

Note

You should select at least one credential.

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

Note

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

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

Note

Up to 50 cards can be supported.

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

Note

Up to 10 fingerprints are allowed.

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 Network System Network** settings page.
2. Set the device type.

Note

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

Device Type

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

Community No.

Set the device community No.

Building No.

Set the device building No.

Unit No.

Set the device unit No.

Floor No.

Set the device installed floor No.

Door Station No.

Set the device installed door station No.

Note

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

Outer Door Station No.

Set the device installed outer door station No.

Note

The No. ranges from 1 to 99.

3. Set the video intercom network parameters.

Registration Password

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

Main Station IP

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

Private Server IP

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

Enable Protocol 1.0

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

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

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, gender, and person type.
If you select **Visitor** as the person type, you can set the visit times.
If you select **Custom Type**, you can edit the name. The changed name will be applied to the device.
If you select **Blocklist User**, the user will be reported when recognizing.

Select **Person Role**.
Click **Save** to save the settings.

Set Permission Time

Click **Person Management → Add** to enter the Add Person page.
Enable **Long-Term Effective User**, or set **Long-Term Effective User**, and the person can only has the permission within the configured time period according to your actual needs.
You can set **Visit Times**.
You can enable **Attendance Check Only**. After enabling, this person won't be given access control permission.
Set the door permission. You can enable **Extend Door Opening**. After Extend Door Opening is enabled, the close time needs to be configured in
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 PIN

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

Click **Save and Continue** to save the settings and continue to add next person.

Device No. Settings

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

Delete Person

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

Edit Person

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

Filter

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

10.7 Overview

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

Click .

Function Descriptions:

Door Status

Click on the video to view the device live video.

Set the volume when starting live view.

Note

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

You can capture image when starting live view.

/ / / /

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

You can record when starting live view.

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



Full screen view.

Controlled Status

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

Real-Time Event

You can view the event Employee ID, Name, Card No., Event Type, Time, and Operation. You can also click **View More** to enter the page of Event Search. You can select event types, enter the employee ID, the name, the card No., the start time, and the end time, and click **Search**. The results will be displayed on the right panel.

Link Device

You can view the quantity and status of linked devices.

Note

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

Person Information

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

Network Status

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

Basic Information

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

Device Capacity

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

Note

Only device installed fingerprint module can display the fingerprint capacity.

10.8 Access Control Management

10.8.1 Search Event

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

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

The results will be displayed on the right panel.

10.8.2 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 Magnetic Sensor Type via PC Web

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

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

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

Click **Save**.

Set Exit Button via PC Web

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

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

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

Click **Save**.

Set Door Lock Powering Off Status via PC Web

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

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

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

Click **Save**.

Set Extended Open Duration via PC Web

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

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

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

Click **Save**.

Set Door Remain Open Duration with First Person via PC Web

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

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

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

Set Duress Code via PC Web

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

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

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

Note

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

Set Super Password via PC Web

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

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

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

Click **Save**.

Note

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

10.8.3 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**.

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**.

10.8.4 Authentication Linkage Settings

You can set authentication linkage settings.

Steps

1. Click **Access Control → Parameter Settings → Authentication Settings** to enter the settings page.
2. Select user type, and 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**.

10.8.5 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**.

10.8.6 Set Face Parameters

Enable/Disable Face Anti-spoofing via Web Browser

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

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

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

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

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.

Note

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

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

Set Yaw Angle via PC Web

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

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

Note

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

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

Set Face Picture Quality Grade for Applying via PC Web

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

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

Note

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

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

Click **Save**.

Set 1:1 Face Grade Threshold via PC Web

Set 1:1 face grade threshold.

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

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

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

Set Face 1:1 Matching Threshold via PC Web

Set face 1:1 matching threshold.

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

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

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

Set 1:N Matching Threshold via PC Web

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

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

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

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

Set Face Recognition Area via Web Browser

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

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

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

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

Click **Save**.

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

Set Fingerprint Parameters via PC Web

You can set the fingerprint parameters of the device.

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

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

Click **Save**.

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**.

10.8.7 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.

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.
- When a Dual-frequency Card Module is connected, you can swipe both the EM card and the DESfire card at the same time. However, swiping the card on the device is invalid.

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**.

Note

When a Dual-frequency Card Module is connected, you can swipe both the EM card and the DESfire card at the same time. However, swiping the card on the device is invalid.

Set FeliCa Card

You can enable FeliCa card.

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

Select **Enable FeliCa Card**.

Set Card No. Authentication Parameters via Web

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

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

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

Full Card No.

All card No. will be read.

3 bytes

The device will read card via read 3 bytes.

4 bytes

The device will read card via 4 bytes.

10.8.8 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**.

10.8.9 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 devicel 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

Upload Captured Picture During Call

If enabled, pictures will be captured automatically during calls and will be uploaded automatically.

Click **Save**.

Clear Device Pictures via PC Web

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

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

Click **Clear** to clear all registered, authenticated, captured face pictures or palm print 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 Local Time and Attendance Settings

10.9.1 Manage Department via Web

You can add, edit and delete department information via Web.

Steps

1. Click **Person**.
2. Click **Add Department** to add department.
   1) Enter **Department Name**.
   2) Click **OK** to save the settings.
3. **Optional:** Manage department information.

Edit Department Information	Click to edit department information.
Delete Department Information	Click to delete department information.

10.9.2 Enable Local T&A

You can enable Local T&A, and set attendance rules, shift and schedule.

Steps

1. Click **System and Maintenance → System Configuration → Attendance → Basic Information** .
2. Enable **Local T&A**.

10.9.3 Set Attendance Rule for Shift

Set attendance rule before setting shift.

Click **Attendance → Time and Attendance → Schedule → Attendance Rule** to enter the Shift Schedule page.

Set the attendance rule, including Mark as Later if Checks in Late For and Mark as Early Leave if Checks out Early For. After entering the duration, click **Save** to save the settings.

Take the following picture as an example to describe the rules.

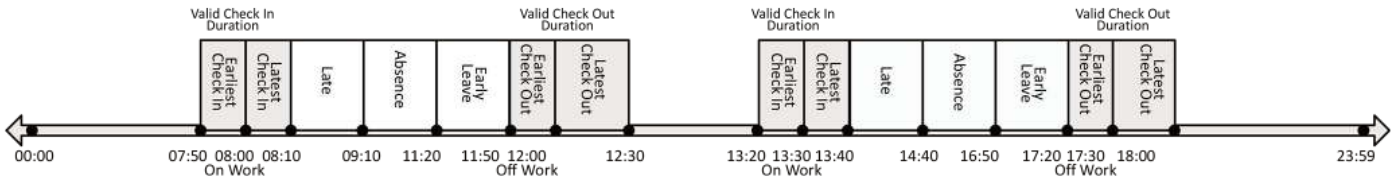


Figure 10-1 Attendance Rule Example

Mark as Early Leave if Checks out Early For

Set the Mark as Early Leave if Checks out Early For time. For example, set the off work time as 17:30 and set the parameter as 10 min, the earliest check out time will be 17:20. Checking out at or earlier than 17:19 will be marked as invalid.

Mark as Later if Checks in Late For

Set the Mark as Later if Checks in Late For time. For example, set the off work time as 17:30 and set the parameter as 30 min, the latest check out time will be 18:00. Checking out at or later than 18:01 will be marked as invalid.

Note

By default, if set as 0 min, the valid check out time ends at 23:59:59.

Note

- The unit is min.
- The available time is from 0 to 1440 min.

10.9.4 Manage Shift

Manage Normal Shift via Web

You can set fixed on-work and off-work time of person for attendance check.

Steps

1. Click **Attendance → Time and Attendance → Schedule → Shift Management** .
2. Click a shift to edit information.
   1) Enter the shift name.
   2) Select **Normal Shift**.
   3) Set the time and attendance duration.
   4) **Optional:** Enable **Overtime**, and set the start time and end time of overtime.
3. Click **Save**.

Manage Flexible Shift via Web

You can set fixed work duration and flexible on-work and off-work time of person for attendance check..

Steps

1. Click **Attendance → Time and Attendance → Schedule → Shift Management** .
2. Click a shift to edit information.
   1) Enter the shift name.
   2) Select **Flexible Shift**.
   3) Set the **Work Duration** and **Latest On-Work Time**.

4) You can enable Break, and set **Break Duration**.

3. Click **Save**.

10.9.5 Manage Schedule

Shift Schedule by Department

All persons in the department use the same shift schedule to take attendance.

Before You Start

- Edit department. For details, see ***Manage Department via Web*** .
- Set shift. For details, see ***Manage Normal Shift via Web*** and ***Manage Flexible Shift via Web*** .

Steps

1. Click **Attendance → Time and Attendance → Schedule** to enter the Shift Schedule by Department page.
2. Click **Add Schedule**.
3. Set **Schedule Name**.
4. Click **Add** to select the **Department/Person**, and select a department. For details, see ***Manage Department via Web*** .
5. Click **Next** select **Schedule Type** according to your actual needs. You can also click **Add Rule** to add new rules.
6. Click **Complete**.

Shift Schedule by Person

Take attendance according to individual's conditions.

Before You Start

- Edit person. For details, see ***Person Management*** .
- Set shift. For details, see ***Manage Normal Shift via Web*** and ***Manage Flexible Shift via Web*** .

Steps

1. Click **Attendance → Time and Attendance → Schedule** to enter the Shift Schedule page.
2. Click **Add Schedule**.
3. Set **Schedule Name**.
4. Click **Add** to select the **Department/Person**, and select the person. For details, see ***Person Management*** .
5. Click **Next** select **Schedule Type** according to your actual needs. You can also click **Add Rule** to add new rules.
6. Click **Complete**.

10.9.6 View Attendance Report

View Attendance Statistics Information

You can view attendance statistics information

Note

You need to enable Local T&A. For details, see ***Enable Local T&A*** .

Click **Attendance Report → Attendance Statistics** , and you can view attendance statistics information.

Export Attendance Report

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

Click **Attendance → Attendance Report → Attendance Report** , select the report, and you can view the Summary Report, Abnormal Attendance, Attendance Card, Attendance Record, Shift Schedule, Total Reports, and export it.

10.10 System Configuration

10.10.1 View Device Information via PC Web

View the device name, device No., language, model, serial No., version, number of channels, IO input, IO output, lock, local RS-485 number, register number, alarm input, alarm output, and device capacity, etc.

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

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

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

10.10.2 Set Time

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

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

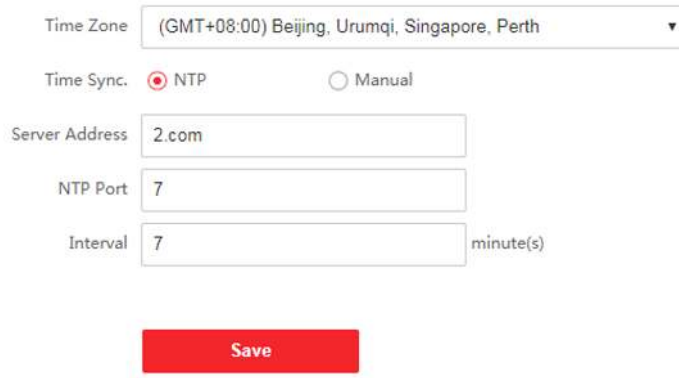


Figure 10-2 Time Settings

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.

10.10.3 Change Administrator's Password

Steps

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

Caution

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

10.10.4 Account Security Settings via PC Web

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

Steps

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

10.10.5 View Device Arming/Disarming Information via PC Web

View device arming type and arming IP address.

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

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

10.10.6 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.

10.10.7 Network Settings

Set Basic Network Parameters via PC Web

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

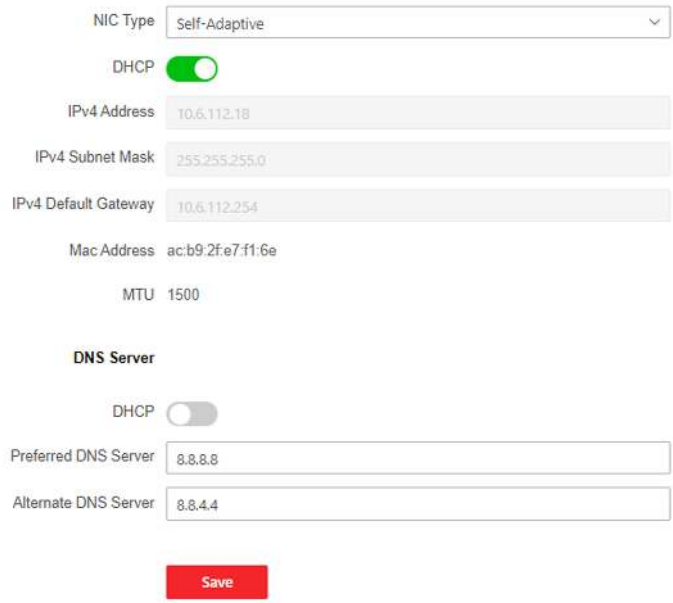


Figure 10-3 TCP/IP Settings Page

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

NIC Type

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

DHCP

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

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

DNS Server

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

Set Wi-Fi Parameters

Set the Wi-Fi parameters for device wireless connection.

Steps

Note

The function should be supported by the device.

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

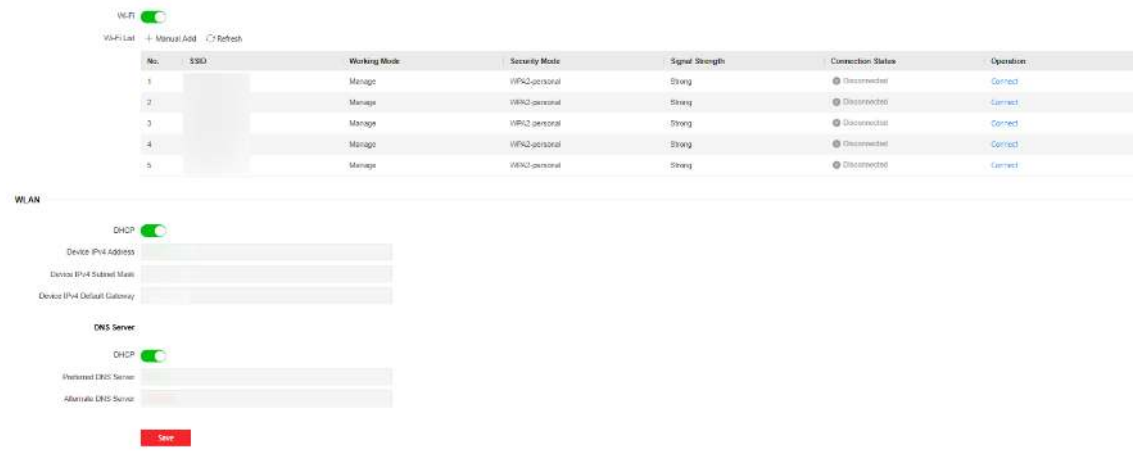


Figure 10-4 Wi-Fi Settings Page

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

Set Port via PC Web

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

Enable/Disable HTTP

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

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

Click**Save** after parameters are configured.

HTTP Port

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

HTTPS Port

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

Web Authentication

You can select **Digest Algorithm**. Digest algorithm applies to both HTTP and HTTPS.

HTTP Listening

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

View RTSP Port via PC Web

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

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

View the Port.

Set WebSocket(s) via PC Web

View WebSocket and WebSockets port.

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

View WebSocket and WebSockets port.

Enable SDK Service

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

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

Enter **Server Port**.

You can also enable **Enhanced SDK Service**, and enter the port.

Click **Save** to enable the settings.

Set ISUP Parameters via PC Web

Set the ISUP parameters for accessing device via ISUP protocol.

Steps

Note

The function should be supported by the device.

1. Click **System and Maintenance → System Configuration → Network → Device Access → ISUP** .
2. Check **Enable**.
3. Set the ISUP version, server address, device ID, and the ISUP status.

   Note

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

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 via PC Web

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

Steps

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

   Note

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

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

   Note

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

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

VoIP Account Settings

You can realize voice call by network.

Steps

1. Go to **System and Maintenance → System Configuration → Network → Device Access → VoIP**.
2. 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.

SADP

If SADP service is enabled, you can activate the device, change password, and modify IP address through the software. SADP service is enabled by default.

1. Go to **System Configuration → Network → Device Access → SADP** .
2. Enable **SADP**.

Note

If SADP service is disabled, some of the functions may become unavailable. It is recommended to enable this service.

10.10.8 Set Video and Audio Parameters via PC Web

Configure Video Parameters via Web Browser

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

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

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

Click **Save**.

10.10.9 Access Configuration

Set RS-485 Parameters via PC Web

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

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

Select **RS-485 Protocol**.

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

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

No.

Set the RS-485 No.

Peripheral Type

Select a peripheral from the drop-down list according the actual situation.

Note

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

RS-485 Address

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

Note

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

Baud Rate

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

Set Wiegand Parameters via PC Web

You can set the Wiegand transmission direction.

Steps

Note

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

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

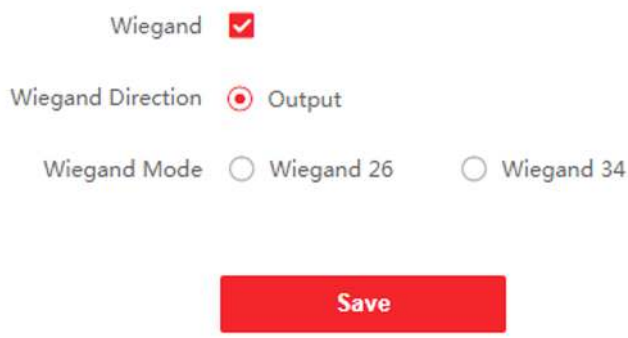


Figure 10-5 Wiegand Page

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

Input

The device can connect a Wiegand card reader.

4. Set the time interval and pulse width if you need.
5. Click **Save** to save the settings.

Note

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

10.10.10 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.

10.10.11 Linkage Settings

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

Steps

1. Click **System and Maintenance → System Configuration → Event → Linkage Settings** to enter the settings page.
2. Click **Add** .
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.

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

Result

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

Set Manual Attendance via Web

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

Before You Start

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

Steps

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

   Note

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

Result

You should select an attendance status manually after authentication.

Note

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

Set Auto Attendance via Web

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

Before You Start

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

Steps

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

Note

The Attendance Property will not be changed.

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

Set Manual and Auto Attendance via Web

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

Before You Start

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

Steps

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

Note

The Attendance Property will not be changed.

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

Result

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

Example

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

10.11 Preference Settings

10.11.1 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** .

Set the standby image parameters, and click **Save**.

Time to Enter Standby

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

10.11.2 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** .

Select **Entrance** or **Exit**. The screen will execute the configured settings.

Slide **Enable Screen-off** . Drag the block or enter the value to set **Screen-off Time**.

10.11.3 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 System and Maintenance

10.12.1 Reboot

You can reboot the device.

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

Click **Restart** to reboot the device.

10.12.2 Upgrade

Upgrade Locally via PC Web

You can upgrade the device locally.

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

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

Online Upgrading via PC Web

You can upgrade the device online.

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

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

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

Upgrade Keyfob

Note

- 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.

10.12.3 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.

10.12.4 Export Device Parameters via PC Web

Export device parameters.

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

Backup

Click **Export** to export device parameters.

Note

Export device parameters and import those parameters to other devices.

10.12.5 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**.

10.12.6 Device Debugging

You can set device debugging parameters.

Enable/Disable SSH via Web Browser

You can enable SSH to perform remote debugging.

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

Enable SSH

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

Print Device Log via PC Web

You can print out the device log.

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

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

Capture Network Packet via PC Web

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

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

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

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 → 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 **System and Maintenance → 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 devcie 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.

10.12.7 View Log via PC Web

You can search and view the device logs.

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

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

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

10.12.8 Advanced Settings via PC Web

You can configure face parameters, palm 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**.

Palm Print Parameter

Enable **Custom Anti-Spoofing Detection** and you can set the **Anti-Spoofing Detection Threshold**.

Click **Save**.

Version Information

You can view the different version information here.

10.12.9 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**.

10.12.10 Certificate Management

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

Note

The function is only supported by certain device models.

Create and Import Self-signed Certificate

Steps

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

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

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

Import Other Authorized Certificate

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

Steps

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

Import CA Certificate

Before You Start

Prepare a CA certificate in advance.

Steps

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

   Note

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

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

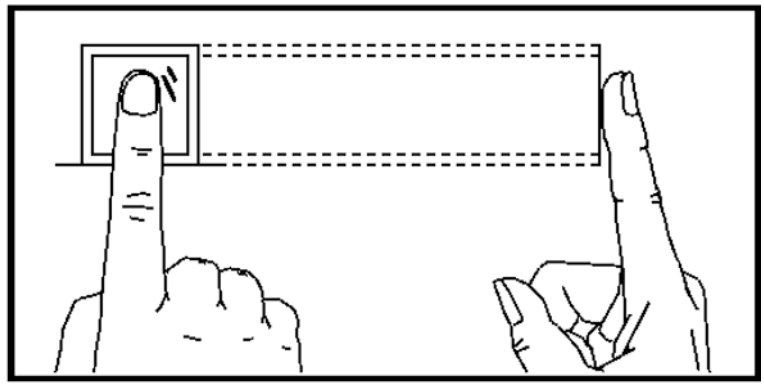
Appendix A. Tips for Scanning Fingerprint

Recommended Finger

Forefinger, middle finger or the third finger.

Correct Scanning

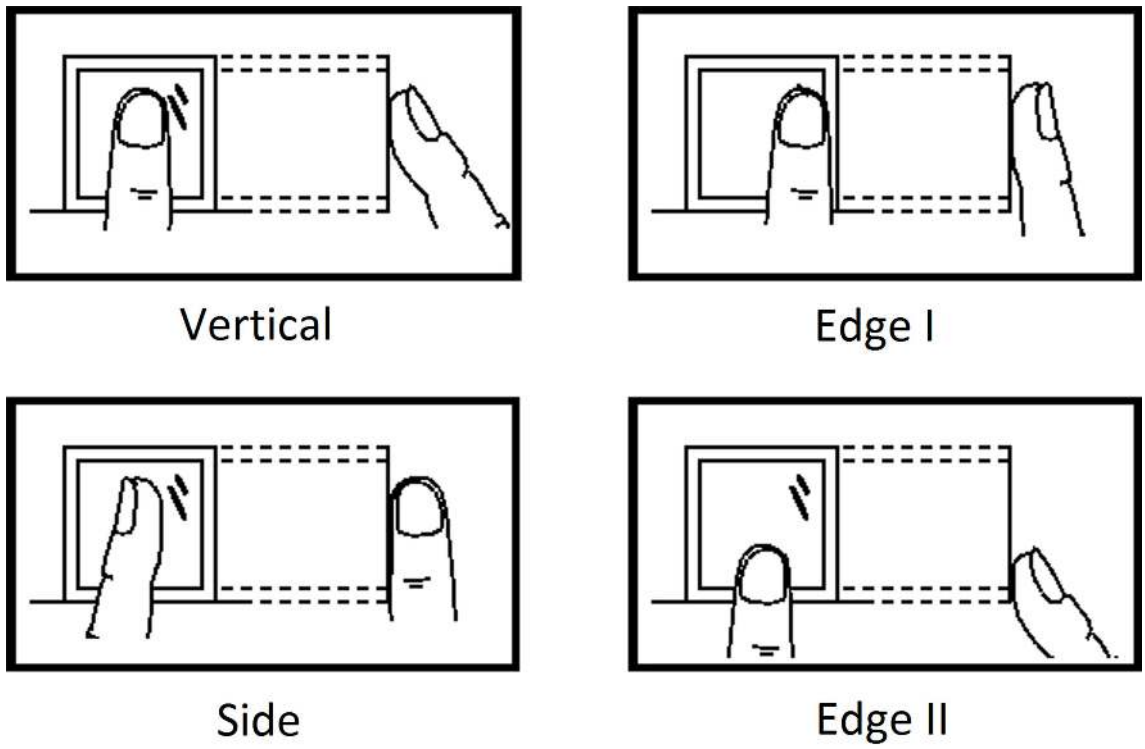
The figure displayed below is the correct way to scan your finger:



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

Incorrect Scanning

The figures of scanning fingerprint displayed below are incorrect:



Environment

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

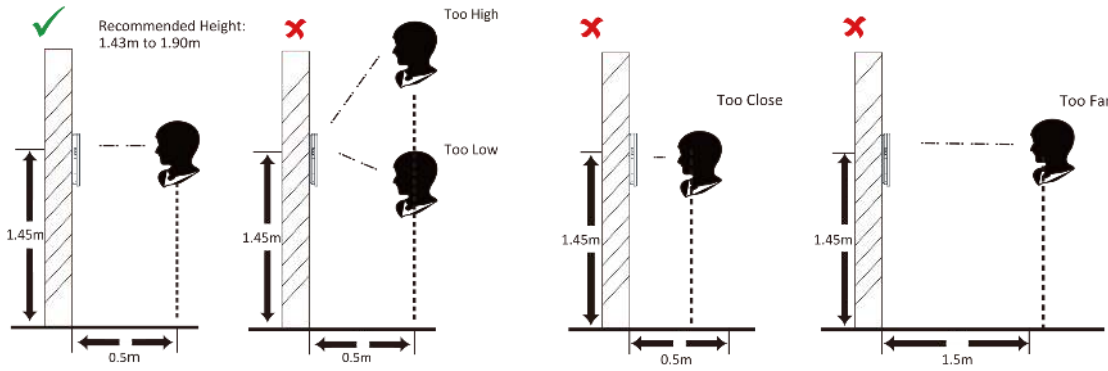
Others

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

Appendix B. Tips When Collecting/Comparing Face Picture

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

Positions (Recommended Distance: 0.5 m)



Expression

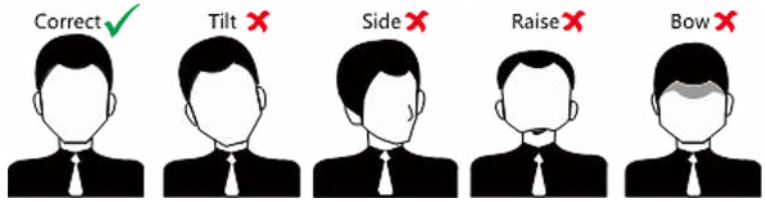
- Keep your expression naturally when collecting or comparing face pictures, just like the expression in the picture below.



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

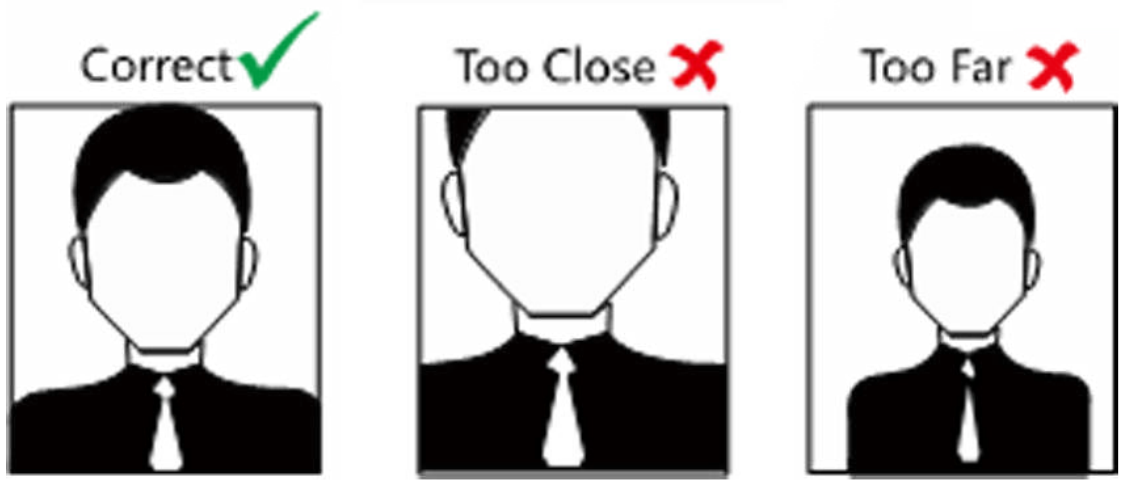
Posture

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



Size

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



Appendix C. Tips for Installation Environment

1. Light Source Illumination Reference Value



Candle: 10Lux

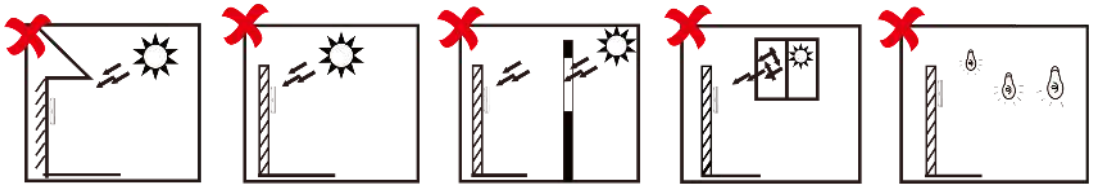


Bulb: 100~850Lux



Sunlight: More than 1200Lux

2. Avoid backlight, direct and indirect sunlight



Appendix D. Dimension

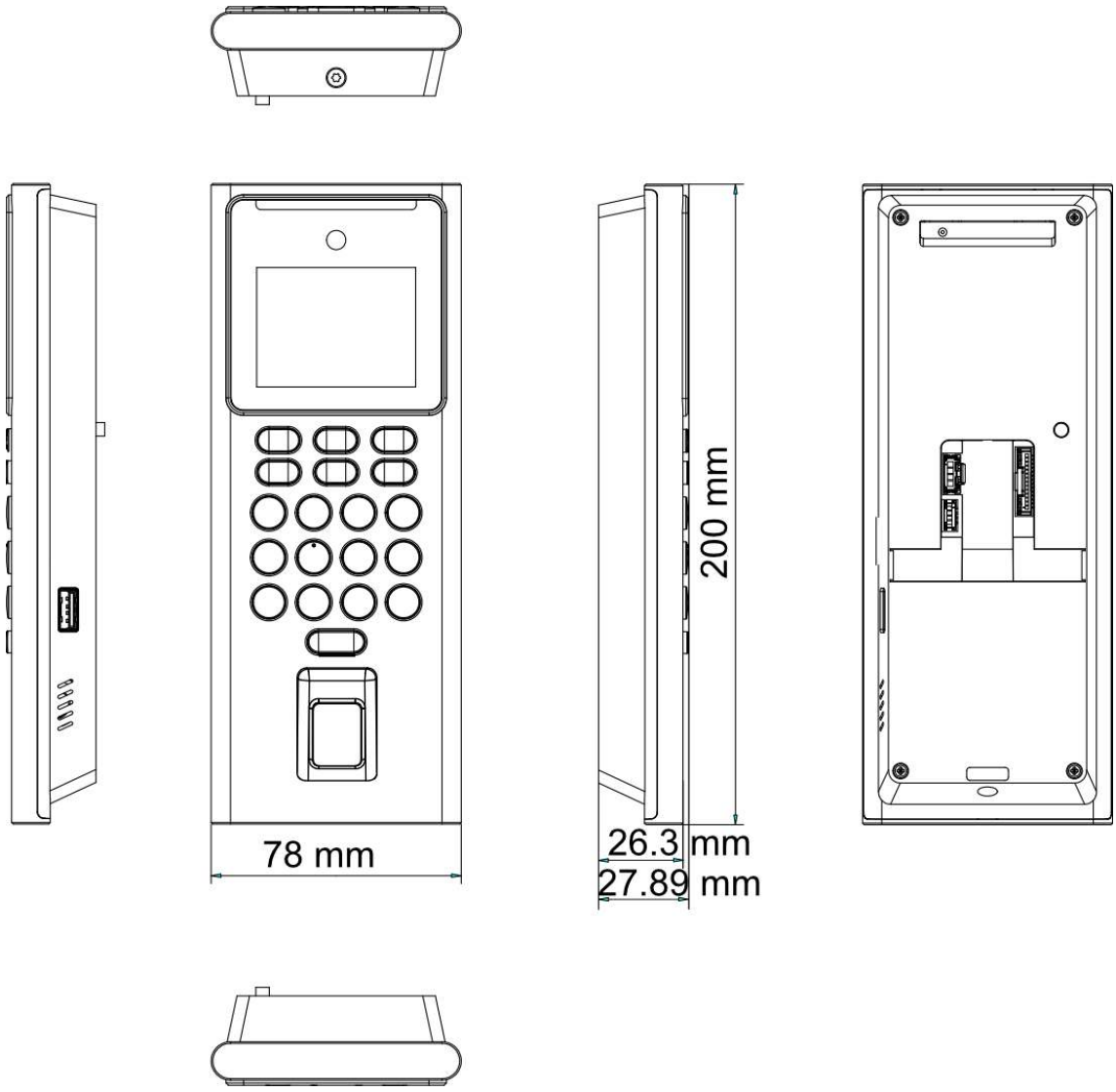


Figure D-1 Dimension


See Far, Go Further