DS-K1T8005 Series Access Control 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.

Symbol Conventions

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

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

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-K1T8005MFX	13.56 MHz Card Presenting Frequency
	DS-K1T8005MFWX	13.56 MHz Card Presenting Frequency, Wi-Fi, 2.4G
	DS-K1T8005MFWX-B	13.56 MHz Card Presenting Frequency, Wi-Fi, 2.4G
	DS-K1T8005EFX	125 KHz Card Presenting Frequency
	DS-K1T8005EFWX	125 KHz Card Presenting Frequency, Wi-Fi, 2.4G
	DS-K1T8005EFWX-B	125 KHz Card Presenting Frequency, Wi-Fi, 2.4G

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 Overview

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

1.2 Features

- 4.3-inch LCD touch screen
- 2 MP wide-angle dual-lens
- Face anti-spoofing
- Face recognition distance: 0.3 m to 1.5 m
- Suggested height for face recognition: between 1.4 m and 1.9 m
- Deep learning algorithm
- 1500 face capacity, 3,000 card capacity, and 150,000 events
- Face recognition duration ＜ 0.2 s/User; face recognition accuracy rate ≥ 99%
- Capture linkage and captured pictures storage
- Transmits card and user data from or to the client software via TCP/IP protocol and saves the data on the client software
- Imports pictures from the USB flash drive to the device or export pictures, events, from the device to the USB flash drive
- Stand-alone operation
- Manage, search and set device data after logging in the device locally
- Connects to one external card reader or access controller via RS-485 protocol
- Connects to secure door control unit via RS-485 protocol to avoid the door opening when the device is destroyed
- Two-way audio
- Arms by multiple client softwares
- Watchdog design and tamper function
- Support English, Spanish (South America), Arabic, Thai, Indonesian, Russian, Vietnamese, Portuguese (Brazil), Korean, and Japanese

Chapter 2 Appearance

The appearance of the device with fingerprint is as follows:

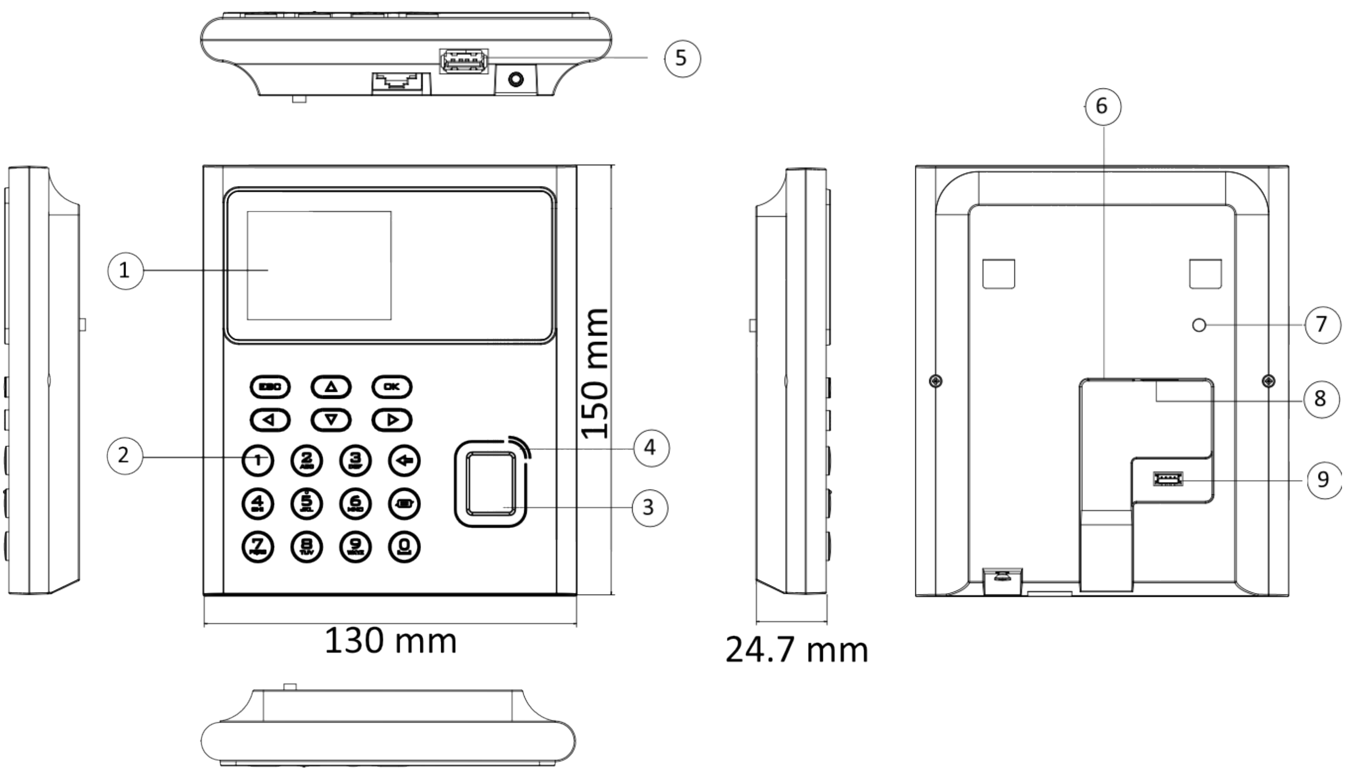


Figure 2-1 Appearance （With Fingerprint)

The appearance of the device without fingerprint is as follows:

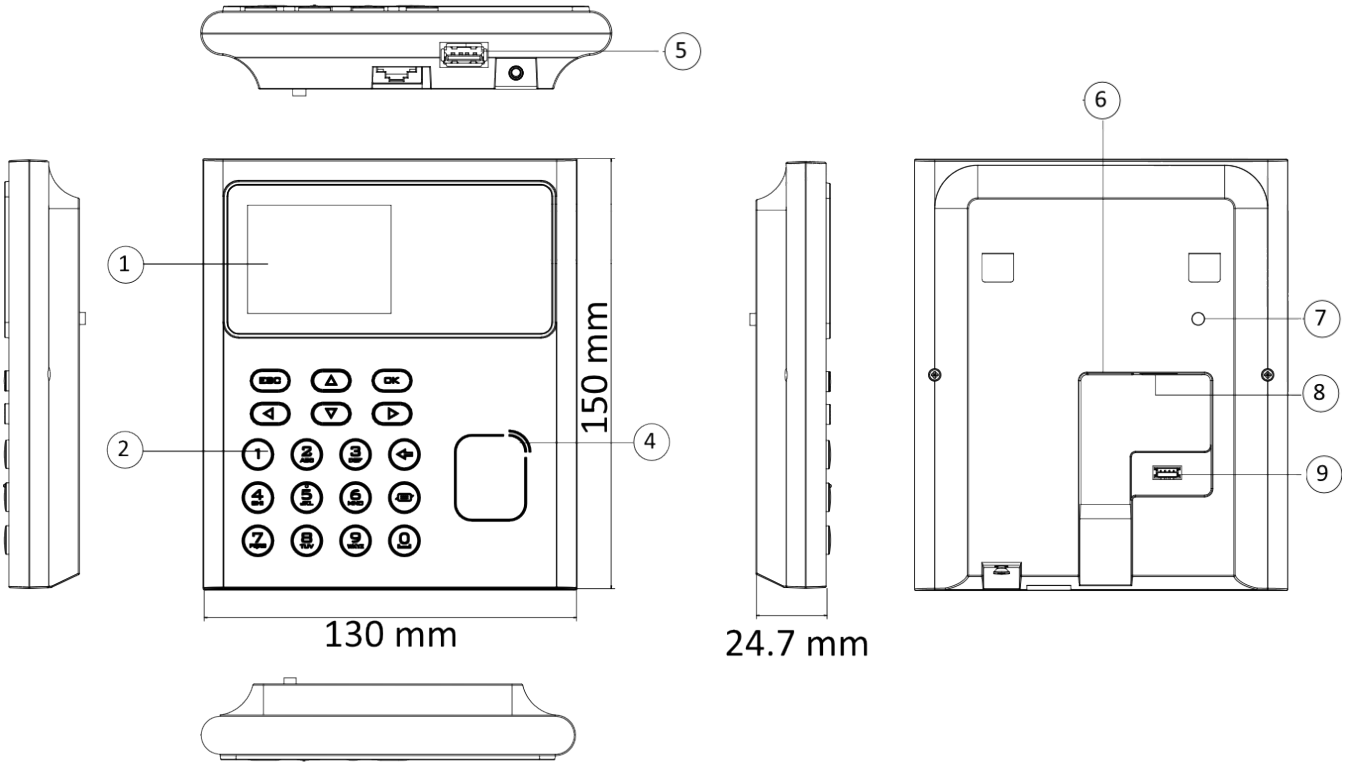


Figure 2-2 Appearance （Without Fingerprint)

Table 2-1 Appearance Description

No.	Name
1	Screen
2	Keypad
3	Fingerprint Module **Note** Only devices that support the fingerprint function contain a fingerprint module.
4	Card Swiping Area
5	USB Interface
6	Network Interface
7	Tamper
8	Wiring Terminal (Including Power Supply Interface)
9	Debugging Port (For Debugging Only)

Chapter 3 Installation

3.1 Installation Environment

- Indoor use only.
- 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.

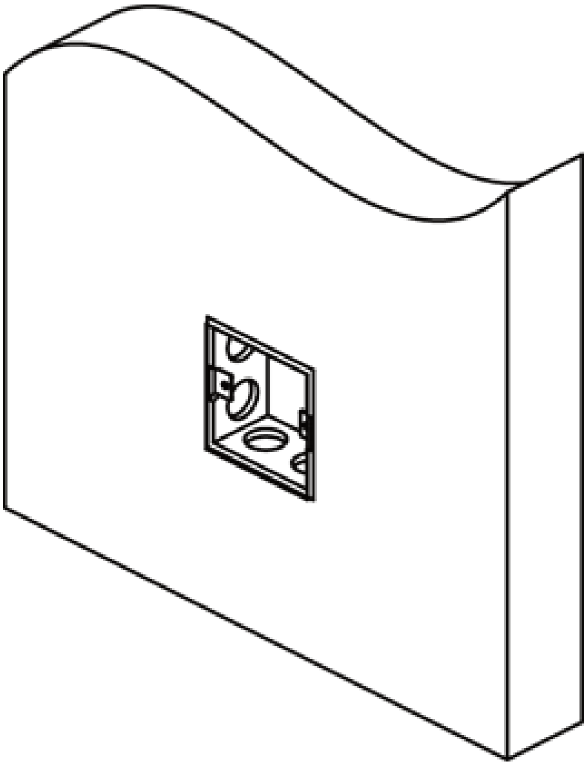


Figure 3-1 Install Gang Box

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

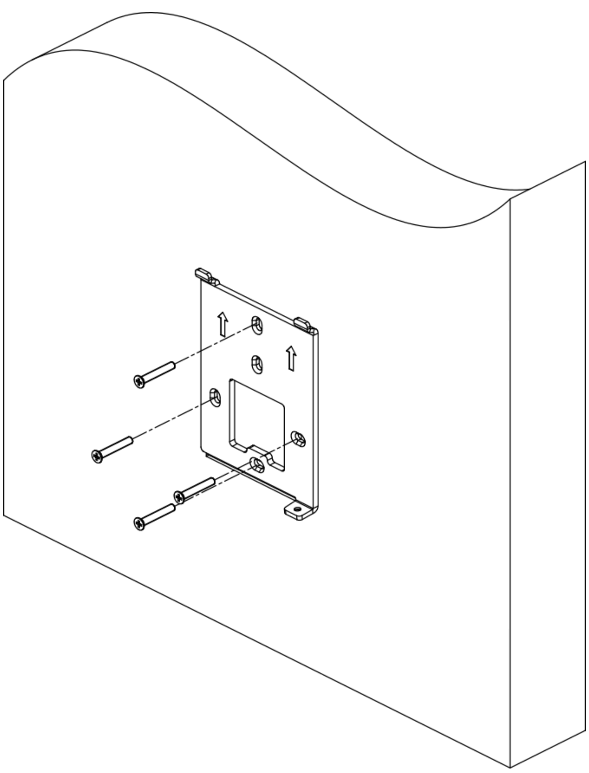


Figure 3-2 Install Mounting Plate

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

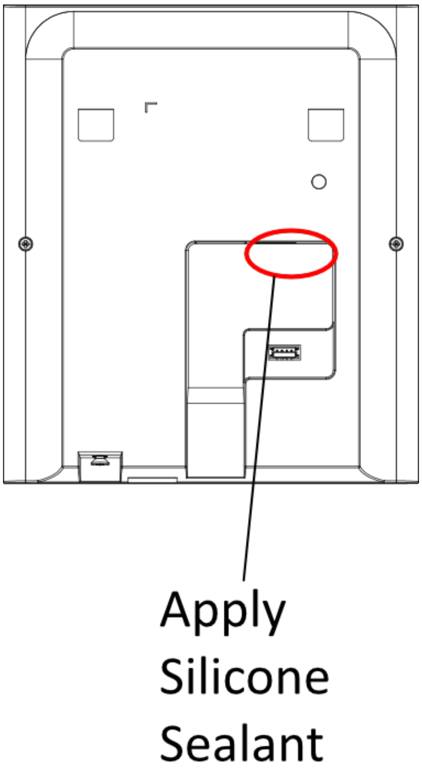


Figure 3-3 Apply Silicone Sealant

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

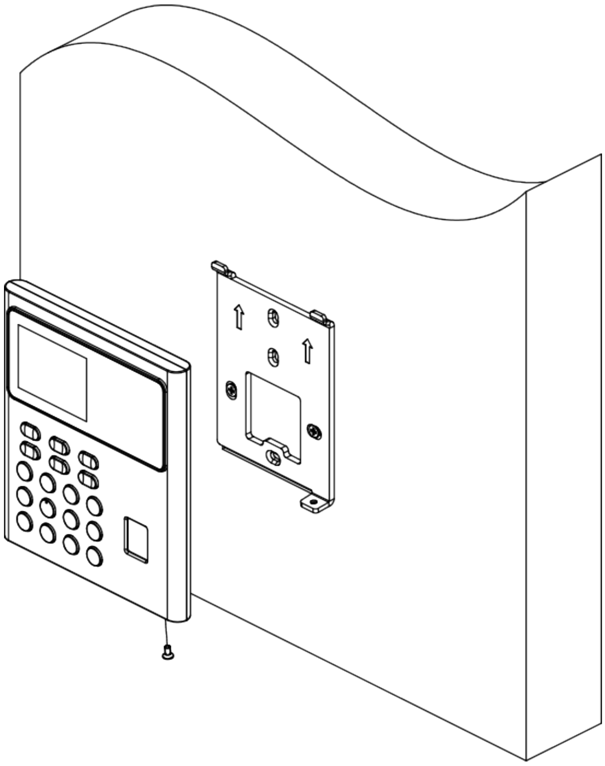


Figure 3-4 Secure Device

3.3 Surface Mounting

Steps

Note

The additional force shall be equal to three times the weight of the equipment. The equipment ad its associated mounting means shall remain secure during the installation. After the installation, the equipment, including any associated mounting plate, shall not be damaged.

1. Secure the mounting plate on the wall with the 4 supplied screws (SC-KA4X22).

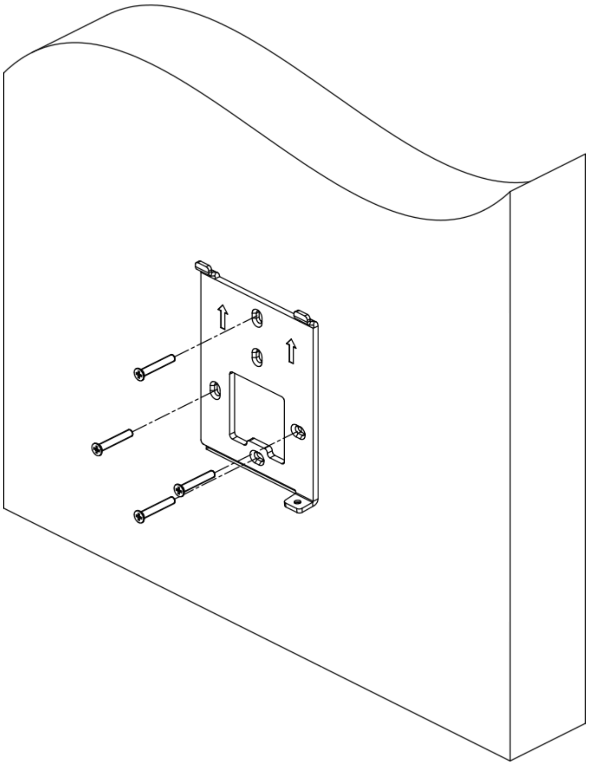


Figure 3-5 Install Mounting Plate

2. Route the cable through the cable hole of the mounting plate, and connect to corresponding peripherals cables.

Note

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

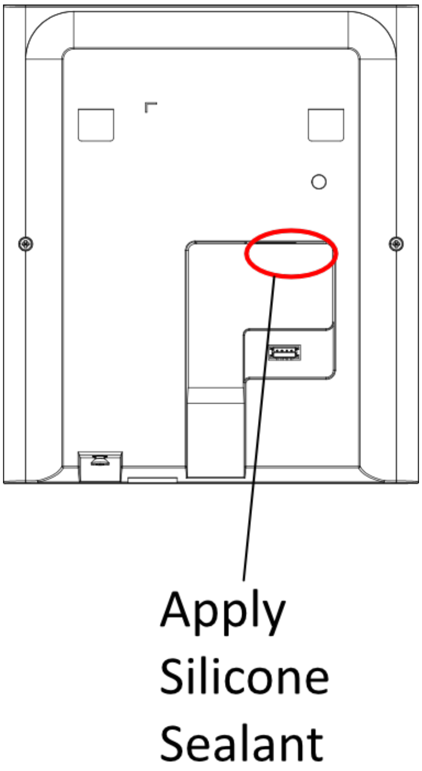


Figure 3-6 Apply Silicone Sealant

3. Align the device with the mounting plate and hang the device on the mounting plate. Use 1 supplied screw (SC-CM4X14_5T10-SUSS) to secure the device and the mounting plate.

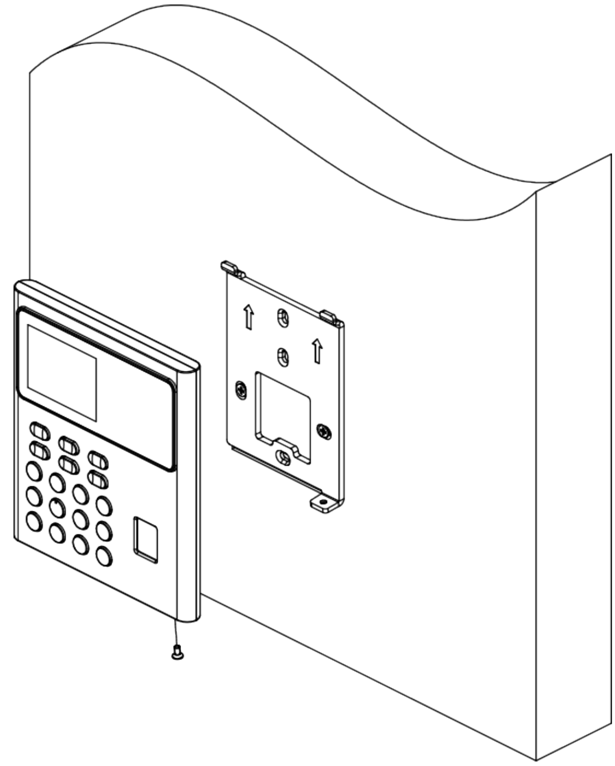


Figure 3-7 Hang Device

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

3.4 Base Mounting

Steps

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

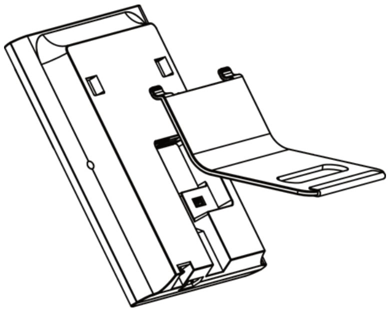


Figure 3-8 Place Bracket Close to Device Back Side

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

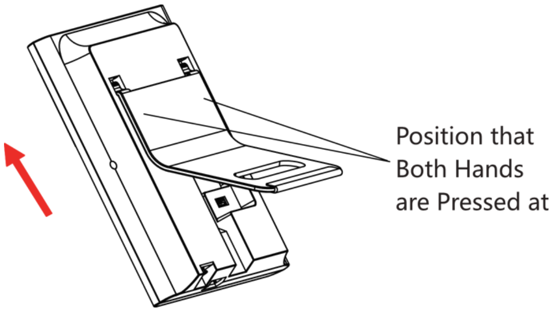


Figure 3-9 Fasten Bracket

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

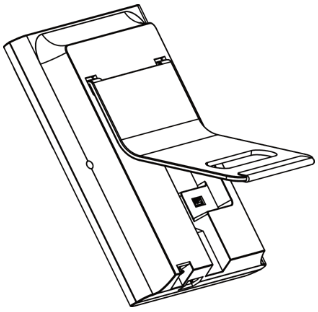


Figure 3-10 Complete Installation

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 Terminal Description

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

The terminal's diagram is as follows:

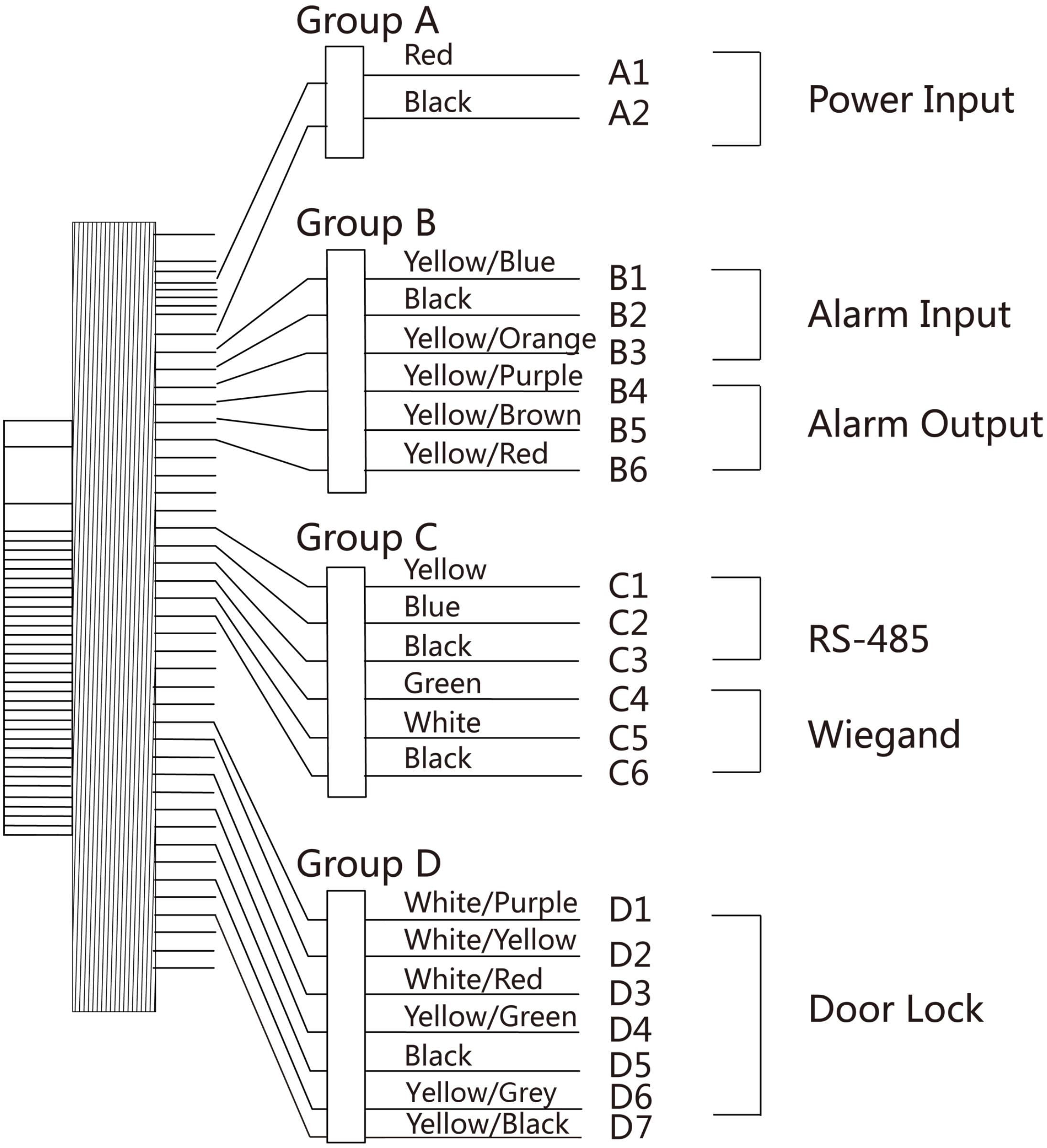


Figure 4-1 Terminal Diagram

The descriptions of the terminals are as follows:

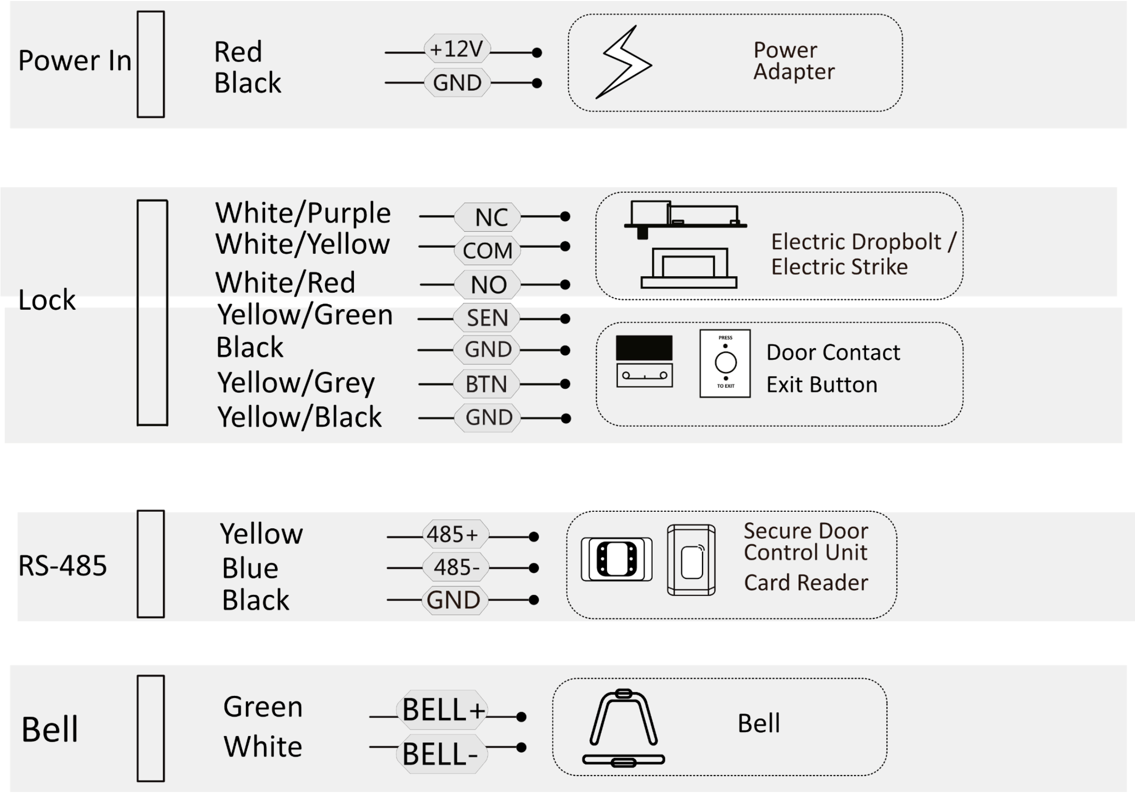
Table 4-1 Terminal Descriptions

Group	No.	Function	Color	Name	Description
Group A	A1	Power Input	Red	+12 V	12 VDC Power Supply
	A2		Black	GND	Ground

Group	No.	Function	Color	Name	Description
Group B	B1	Alarm Input	Yellow/Blue	IN1	Alarm Input 1
	B2		Black	GND	Ground
	B3		Yellow/Orange	IN2	Alarm Input 2
	B4	Alarm Output	Yellow/Purple	NC	Alarm Output Wiring
	B5		Yellow/Brown	COM	
	B6		Yellow/Red	NO	
Group C	C1	RS-485	Yellow	485+	RS-485 Wiring
	C2		Blue	485-	
	C3		Black	GND	Ground
	C4	Wiegand	Green	W0	Wiegand Wiring 0
	C5		White	W1	Wiegand Wiring 1
	C6		Black	GND	Ground
Group D	D1	Door Lock	White/Purple	NC	Lock Wiring (NC)
	D2		White/Yellow	COM	Common
	D3		White/Red	NO	Lock Wiring (NO)
	D4		Yellow/Green	SENSOR	Door Contact
	D5		Black	GND	Ground
	D6		Yellow/Gray	BTN	Exit Door Wiring
	D7		Yellow/Black	GND	Ground

4.2 Wire Normal Device

You can connect the terminal with normal peripherals.


Power In
Red
Black
+12V
GND
Power Adapter
Lock
White/Purple
White/Yellow
White/Red
Yellow/Green
Black
Yellow/Grey
Yellow/Black
NC
COM
NO
SEN
GND
BTN
GND
Electric Dropbolt / Electric Strike
PRESS
TO EXIT
Door Contact
Exit Button
RS-485
Yellow
Blue
Black
485+
485-
GND
Secure Door Control Unit
Card Reader
Bell
Green
White
BELL+
BELL-
Bell

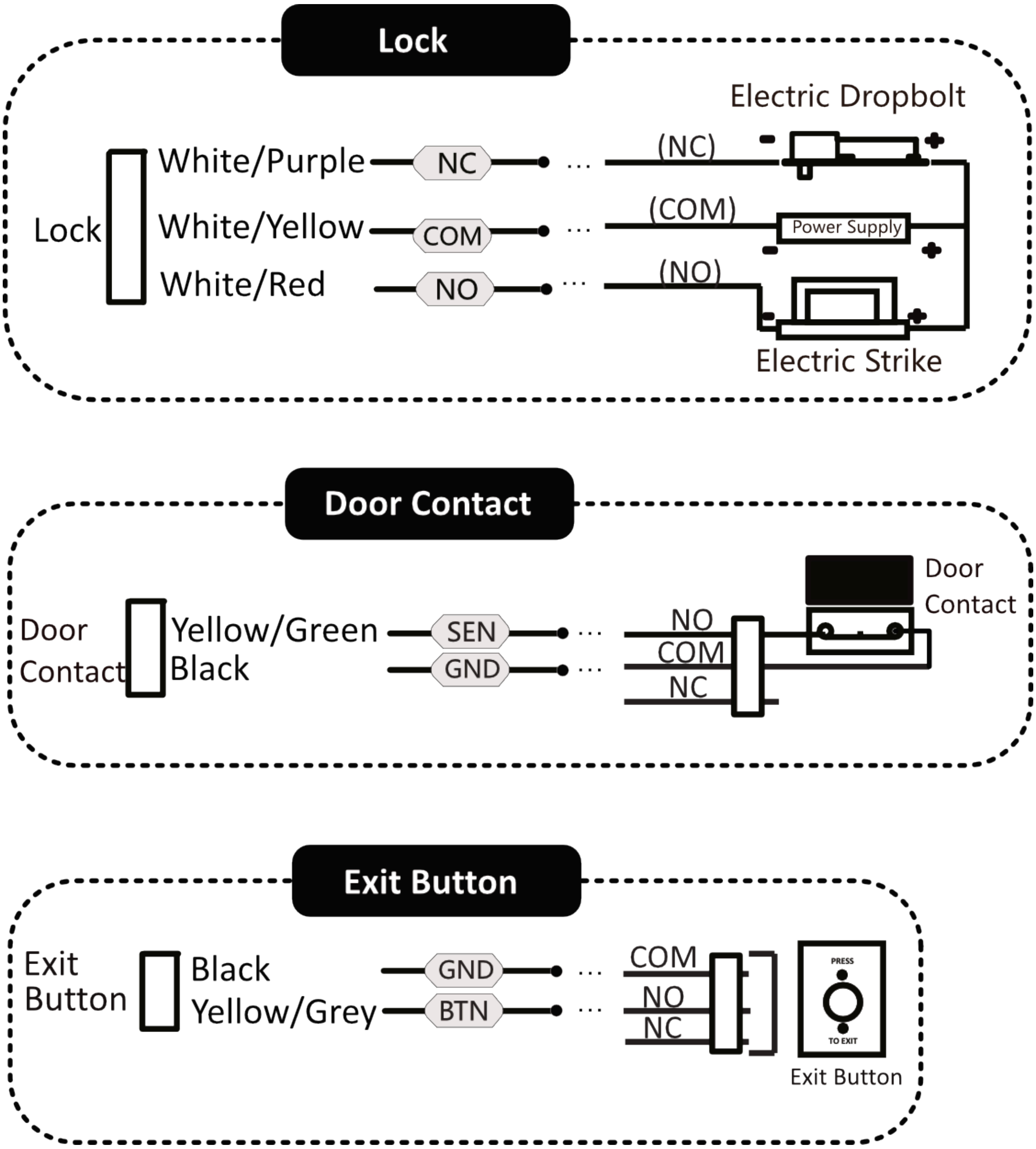


Figure 4-2 Wiring Terminal Description

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

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.

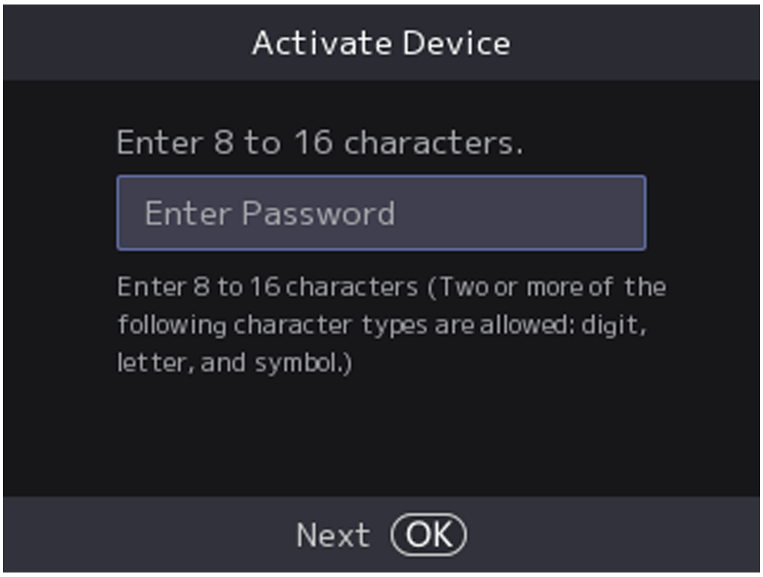
The default values of the device are as follows:

- 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.


Activate Device

Enter 8 to 16 characters.

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

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

Note

- After powering on the device for the first time, the hotspot function is enabled by default.
- Only the device with Wi-Fi function supports activation via AP mode.

1. Connect to the device hotspot with your mobile phone by entering the hotspot password. The activation page will pop up.

   Note

   - If automatic pop-up failed. Enter the device default IP or enter www.acsvis.com in the browser to enter the activation page.
   - For inactive devices, the device hotspot name is AP_Serial Number, and the hotspot password is the device serial number.
   - The device is in the AP mode by default. The AP mode will be disabled after 30 min. Hold key 3 for 5 s to enter the AP mode again.
   - After device activation, the hotspot password will be changed to the device activation password.

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

   Note

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

3. Tap **Activate**.

4. Select **Configuration → Communication Settings → Wi-Fi** and connect to a Wi-Fi. Or edit the IP address via the mobile web, PC web browser and the client software. Edit the device IP address. You can edit the IP address via the SADP tool, PC web browser and the client software.

What to do next

Login the mobile web to configure parameters. For details, see ***Login*** .

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.

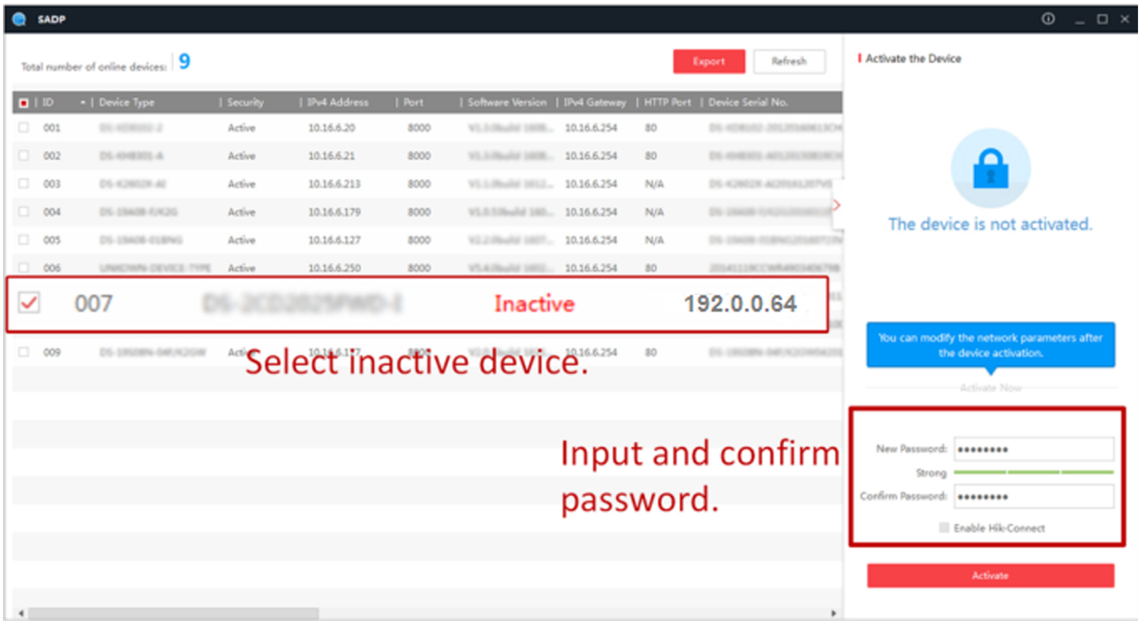
Caution

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.



SADP

Total number of online devices: 9

ID	Device Type	Security	IPv4 Address	Port	Software Version	IPv4 Gateway	HTTP Port	Device Serial No.
□ 001	[illegible]	Active	10.16.6.20	8000	[illegible]	10.16.6.254	80	[illegible]
□ 002	[illegible]	Active	10.16.6.21	8000	[illegible]	10.16.6.254	80	[illegible]
□ 003	[illegible]	Active	10.16.6.213	8000	[illegible]	10.16.6.254	N/A	[illegible]
□ 004	[illegible]	Active	10.16.6.179	8000	[illegible]	10.16.6.254	N/A	[illegible]
□ 005	[illegible]	Active	10.16.6.127	8000	[illegible]	10.16.6.254	N/A	[illegible]
□ 006	[illegible]	Active	10.16.6.250	8000	[illegible]	10.16.6.254	80	[illegible]
☑ 007	[illegible]	Inactive	192.0.0.64					
□ 009	[illegible]	Acti	10.16.6.17	80	[illegible]	10.16.6.254	80	[illegible]

Select inactive device.

Input and confirm password.

Activate the Device

The device is not activated.

You can modify the network parameters after the device activation.

Activate Now

New Password: ••••••••

Strong

Confirm Password: ••••••••

□ Enable Hik-Connect

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

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

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

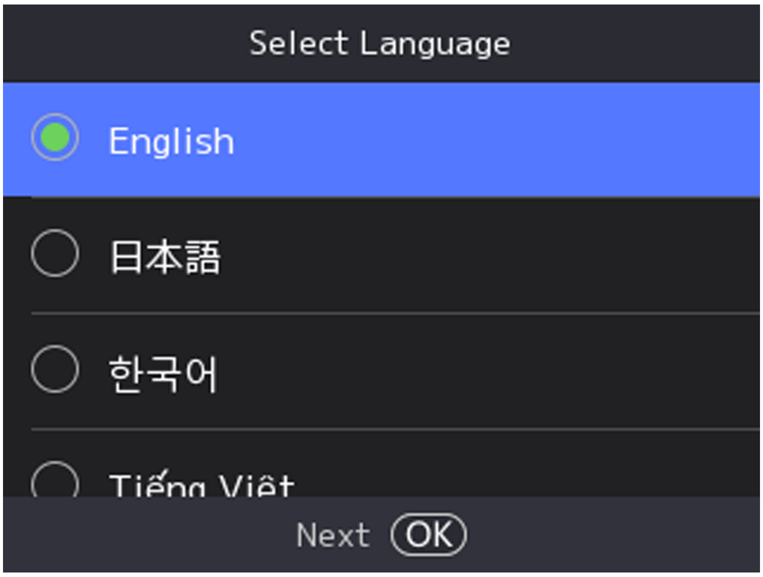
   Characters containing admin and nimda are not supported to be set as activation password.
7. Click **OK** to activate the device.

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.



Select Language

● English

○ 日本語

○ 한국어

○ Tiếng Việt

Next OK

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

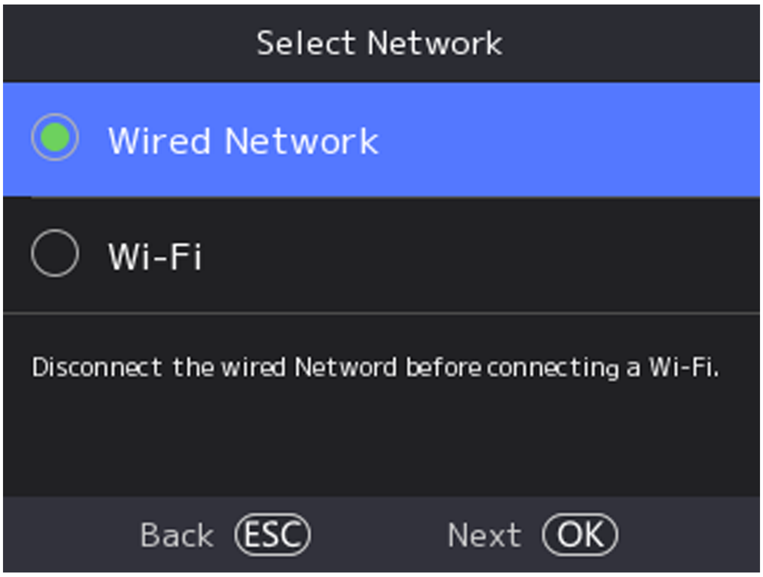
You can only select one type to change password. If you need, you can enter the web page to set both of the changing types.

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.



Select Network

● Wired Network

○ Wi-Fi

Disconnect the wired Netword before connecting a Wi-Fi.

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 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**.

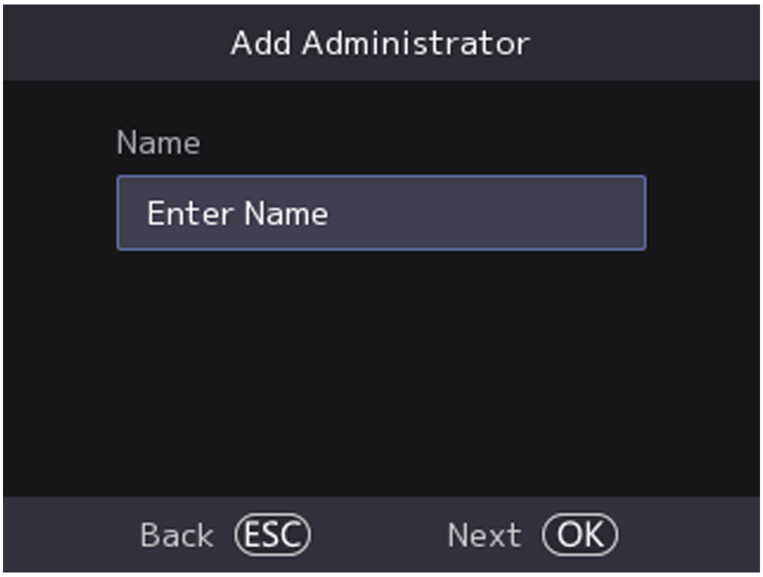


Figure 6-3 Add Administrator Page

2. Select a credential to add.

Note

Up to one credential should be added.

- : 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

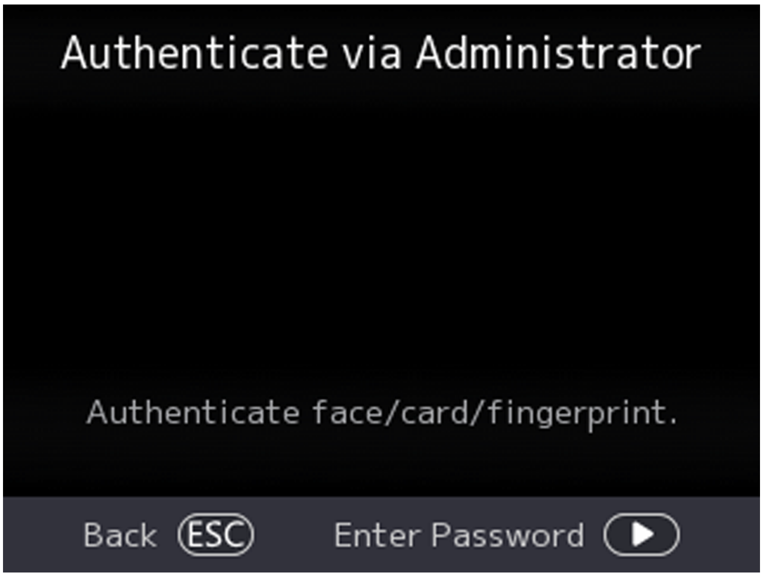
The device will be locked for 30 minutes after 5 failed password attempts.

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.



Authenticate via Administrator

Authenticate face/card/fingerprint.

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

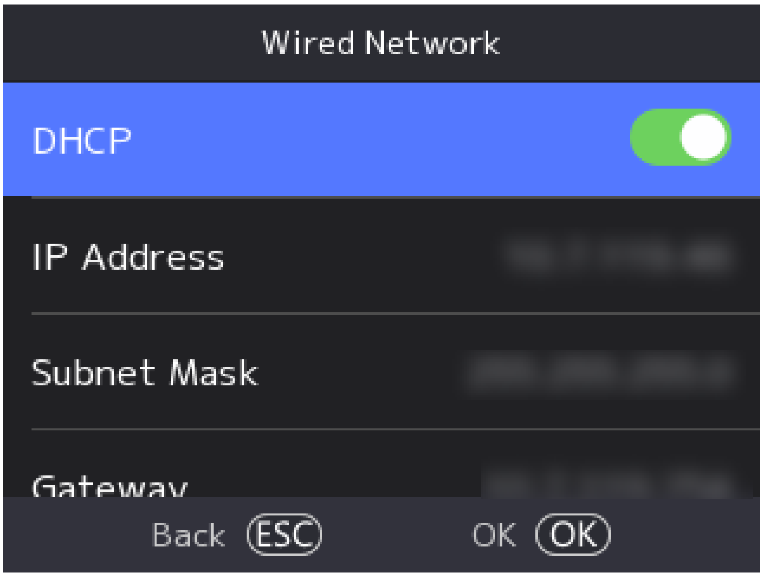
You can set the wired network, the Wi-Fi parameter, the RS-485 parameters, the Wiegand parameters, ISUP and access to Hik-Connect on the communication settings page.

7.2.1 Set Wired Network Parameters

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

Steps

1. Select **System Settings → Comm.** (Communication) to enter the Communication settings page.
2. On the Communication page, select **Wired Network**.



Wired Network

DHCP ●

IP Address [redacted]

Subnet Mask [redacted]

Gateway [redacted]

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

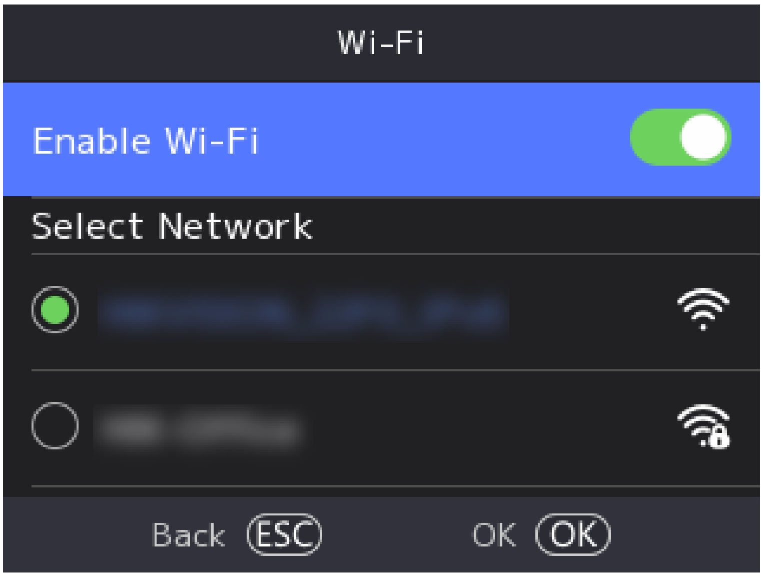
You can enable the Wi-Fi function and set the Wi-Fi related parameters.

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**.



Wi-Fi

Enable Wi-Fi

Select Network

● [redacted]

○ [redacted]

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

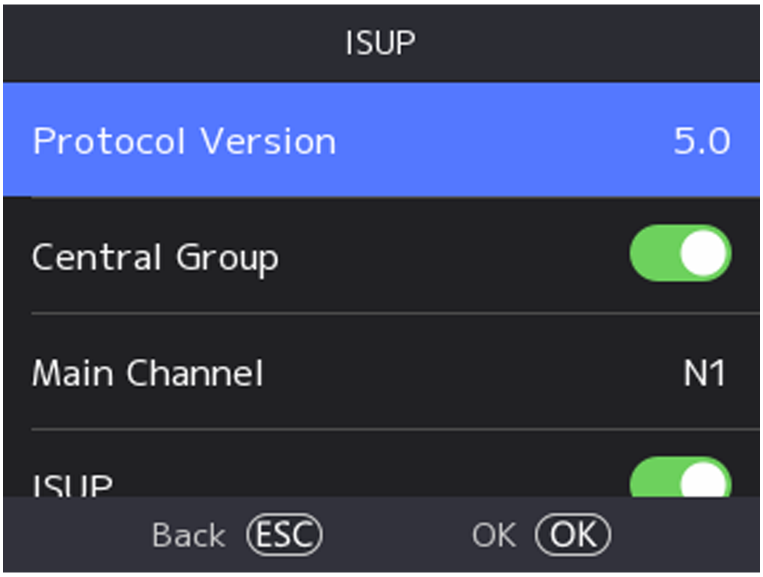
Set ISUP parameters and the device can upload data via ISUP protocol.

Before You Start

Make sure your device has connect to a network.

Steps

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



ISUP

Protocol Version 5.0

Central Group

Main Channel N1

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 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. On the Communication Settings page, select **AP Mode** to enter the settings page.
3. Enable AP mode.
4. Select **Device QR Code**, scan the QR code in Hik-Connect to add the device to set network.

7.3 User Management

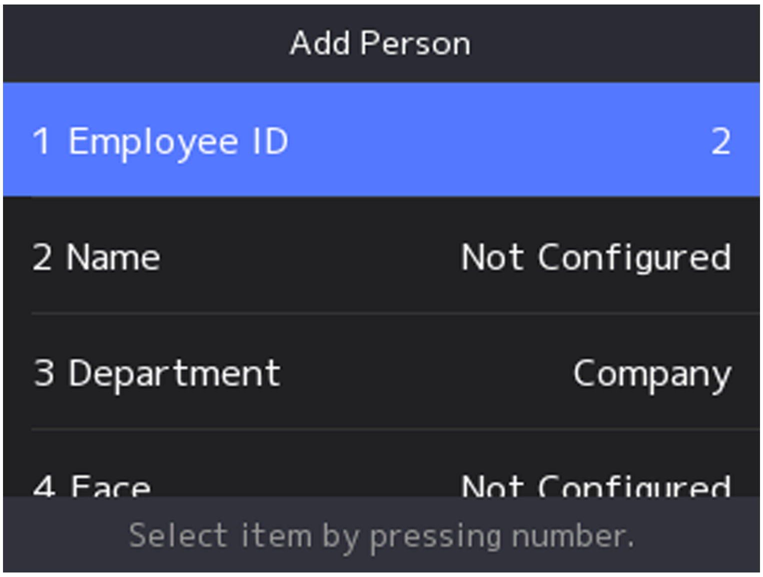
On the user management interface, you can add, edit, delete and search the user.

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.



Add Person

1 Employee ID 2

2 Name Not Configured

3 Department Company

4 Face Not Configured

Select item by pressing number.

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 .
- **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. Press ESC and then press OK to save the settings.

7.3.2 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.

7.3.3 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.

7.3.4 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.

7.3.5 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.

7.3.6 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

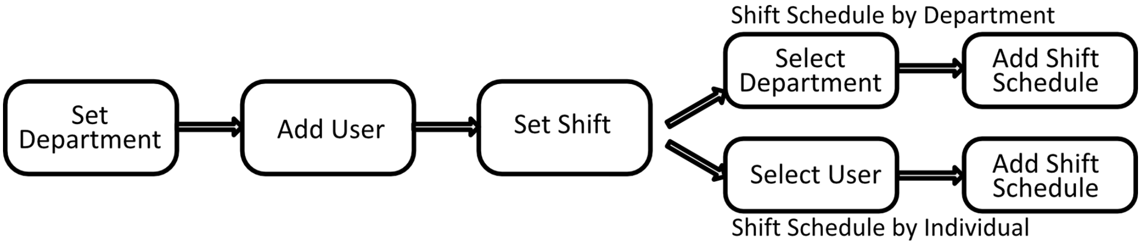


Figure 7-5 Attendance Process Description

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**.

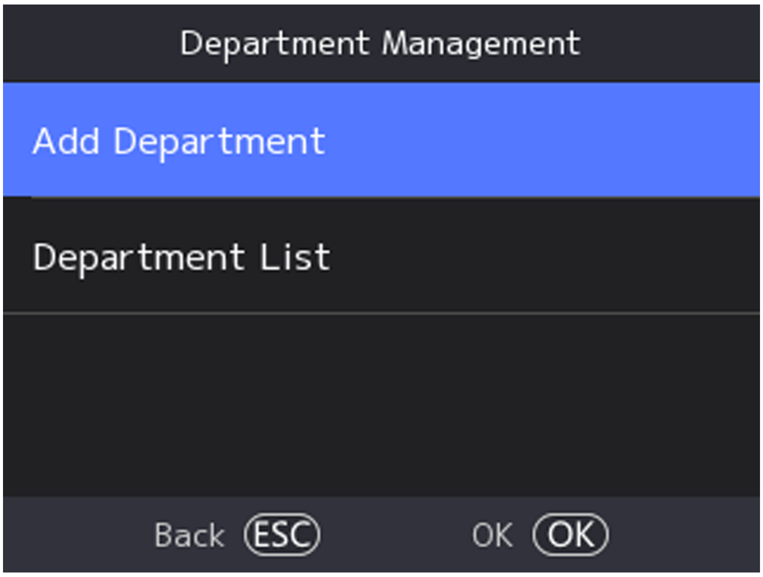


Figure 7-6 Add Department

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

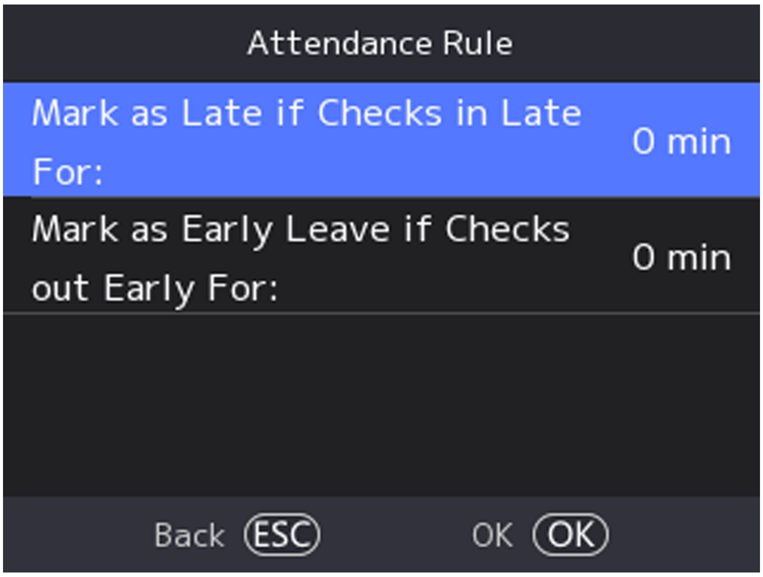
1. Long press **OK** to enter the admin login page.
2. Select **Local T&A**, and enable **Local T&A**.

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.



Attendance Rule

Mark as Late if Checks in Late For: 0 min

Mark as Early Leave if Checks out Early For: 0 min

Figure 7-7 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.

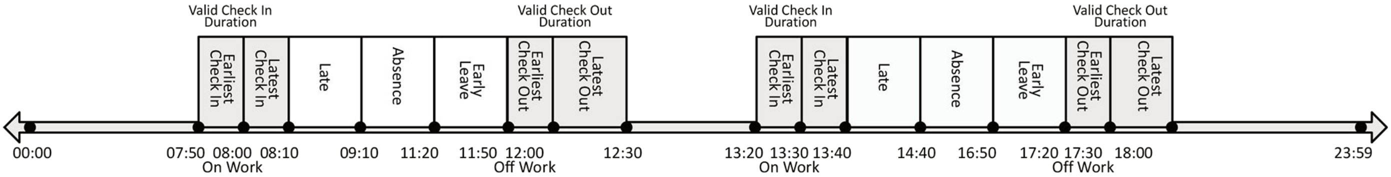


Figure 7-8 Attendance Rule Example

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

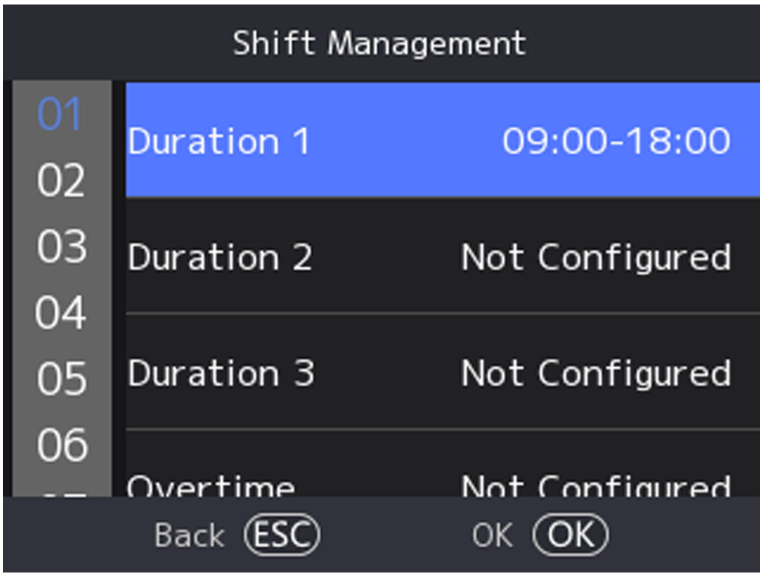
Edit or add the shift attendance information, including the shift name, the shift period, and the overtime shift period. You can also reset the normal shift after editing.

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.



Shift Management

01
02
03
04
05
06

Duration 1 09:00-18:00

Duration 2 Not Configured

Duration 3 Not Configured

Overtime Not Configured

Figure 7-9 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.

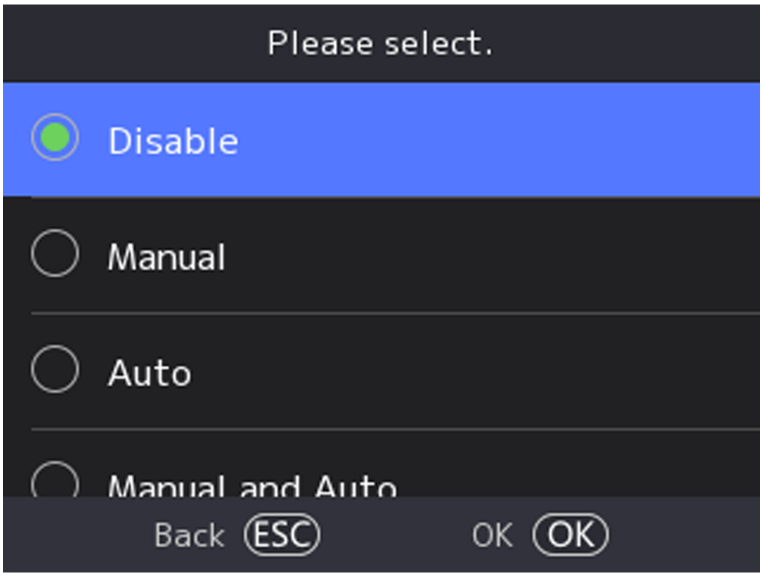
Note

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.



Please select.

● Disable

○ Manual

○ Auto

○ Manual and Auto

Figure 7-10 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

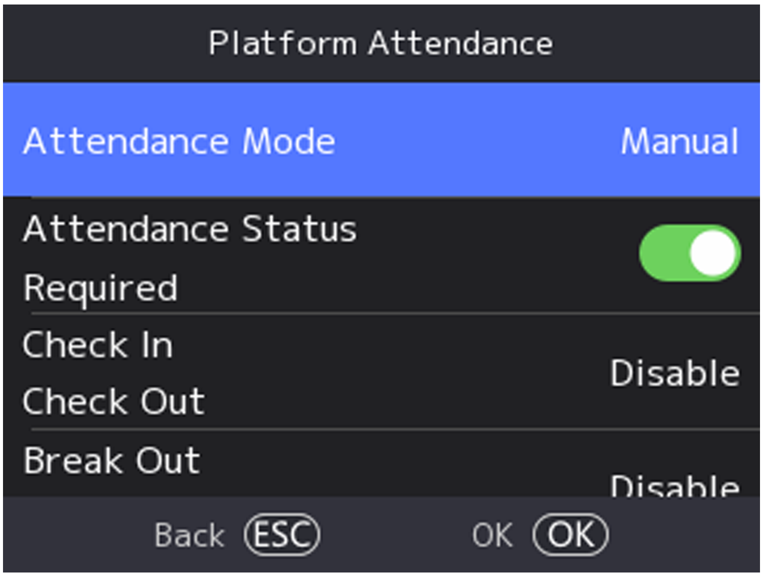
Set the attendance mode as manual, and you should select a status manually when you take attendance.

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**.



Platform Attendance

Attendance Mode Manual

Attendance Status Required

Check In
Check Out
Disable

Break Out
Disable

Figure 7-11 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

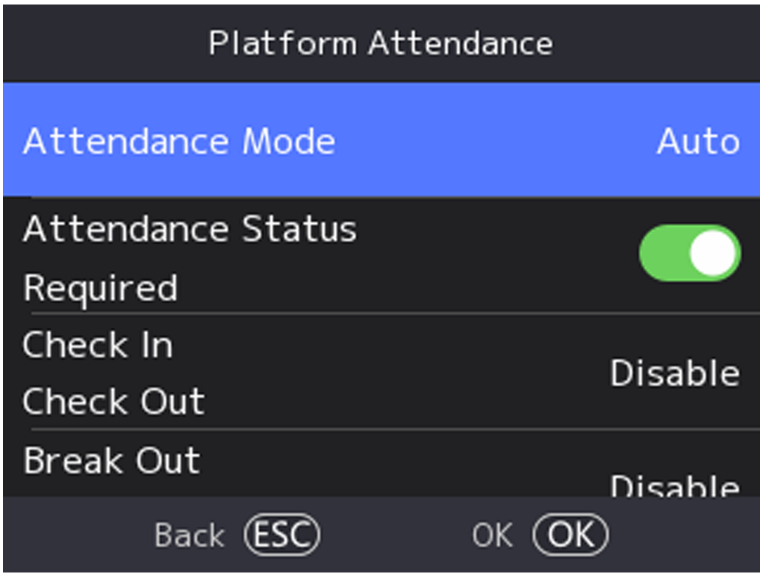
Set the attendance mode as auto, and you can set the attendance status and its available schedule. The system will automatically change the attendance status according to the configured schedule.

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**.



Platform Attendance

Attendance Mode: Auto

Attendance Status Required: ●

Check In / Check Out: Disable

Break Out: Disable

Figure 7-12 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

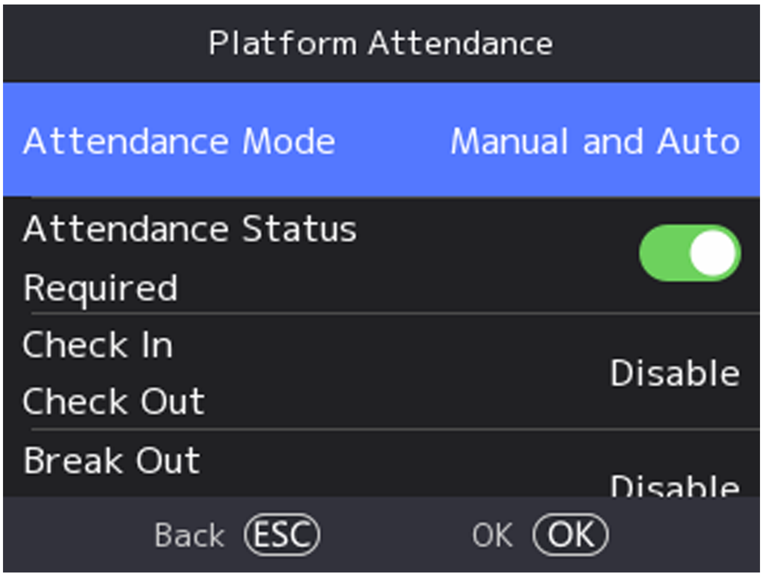
Set the attendance mode as **Manual and Auto**, and the system will automatically change the attendance status according to the configured schedule. At the same time you can manually change the attendance status after the authentication.

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**.



Platform Attendance

Attendance Mode Manual and Auto

Attendance Status Required ●

Check In Check Out Disable

Break Out Disable

Figure 7-13 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 user data is a DB file, which cannot be edited.

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 fingerprint, card or PIN.

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 Password, 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

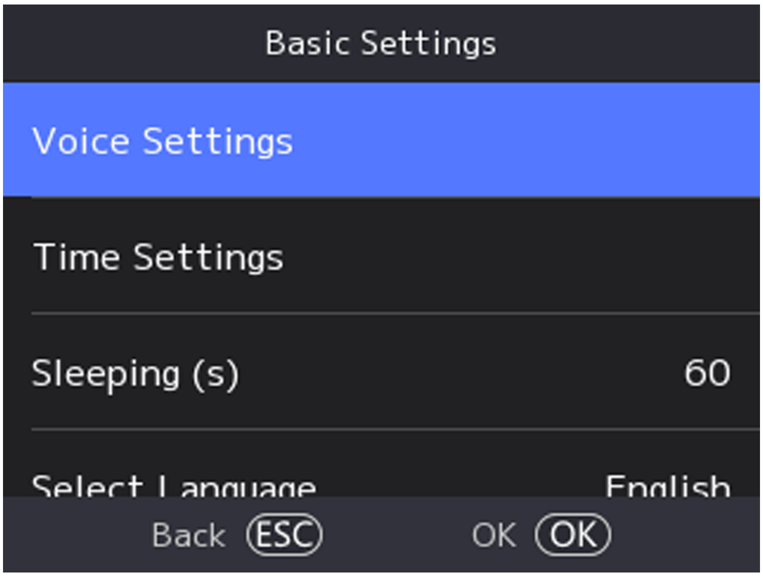
- For detailed information about scanning fingerprint, see *Tips for Scanning Fingerprint*.

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

7.9 Basic Settings

You can set the voice, time, sleeping (s), language, supplement light and video standard.

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


Basic Settings

Voice Settings

Time Settings

Sleeping (s) 60

Select Language English

Figure 7-14 Basic Settings Page

Voice Settings

You can enable/disable the voice function.

Time Settings

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

Sleeping (s)

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 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.

7.11 Set Access Control Parameters

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

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

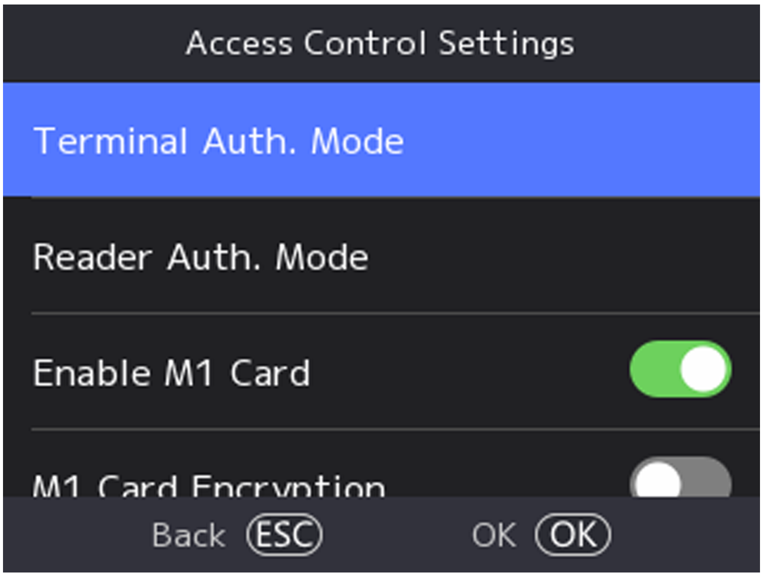


Figure 7-15 Access Control Parameters

The available parameters descriptions are as follows:

Table 7-1 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.

Parameter	Description
Enable M1 Card	Enable the function and you can present the M1 card to authenticate.
M1 Card Encryption	Enabling the M1 card encryption function can improve the card security level. The card will not be copied easily.
Door Contact	You can select "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** 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.

7.12 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.

Show Attendance Record During Check

You can enable **Show Attendance Record During Check**, after enabling, attendance record will display during check.

2. Select **OK** .

7.13 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.

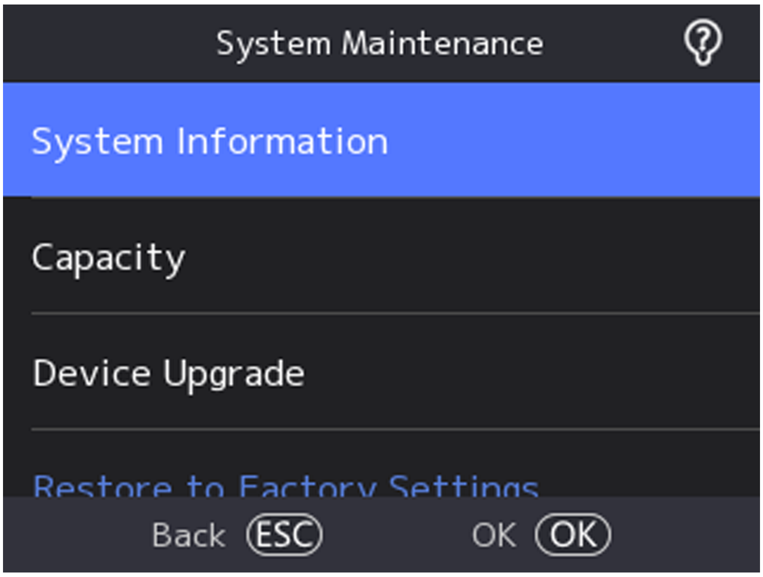


Figure 7-16 Maintenance Page

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

Version Information

You can view the device information.

Chapter 8 Configure the Device via the Mobile Browser

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 wired network, wireless network, bluetooth, ISUP and Hik-Connect.

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, number of channels, IO input number, local RS-485 number, number of alarm input and output, Mac address, factory information and device capacity, etc.

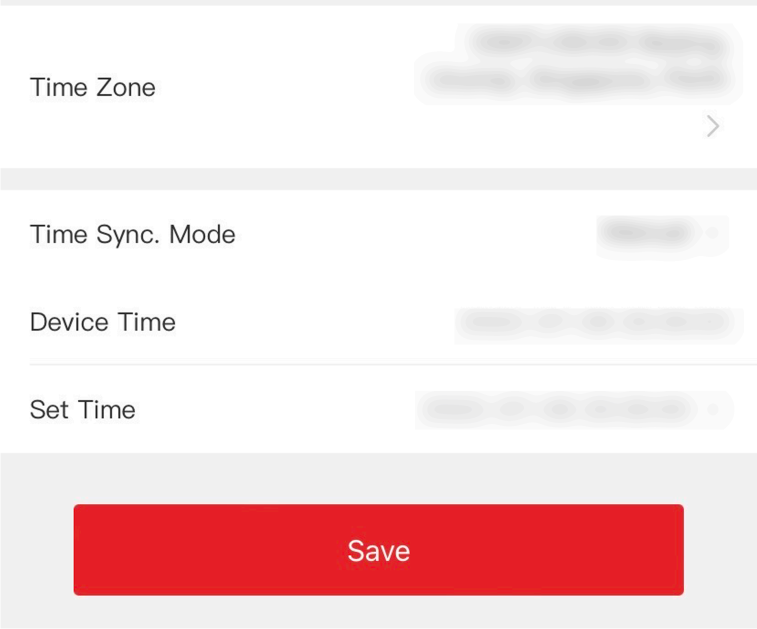
Tap ≡ → **System Settings** → **Basic Information** to enter the configuration page.

You can view the device name, language, model, serial No., version, number of channels, IO input number, local RS-485 number, number of alarm input and output, Mac address, factory information and device capacity, etc.

8.4.2 Time Settings

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

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



Time Zone

Time Sync. Mode

Device Time

Set Time

Save

Figure 8-1 Time Settings

Tap **Save** to save the settings.

Time Zone

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

Time Sync. Mode

Manual

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

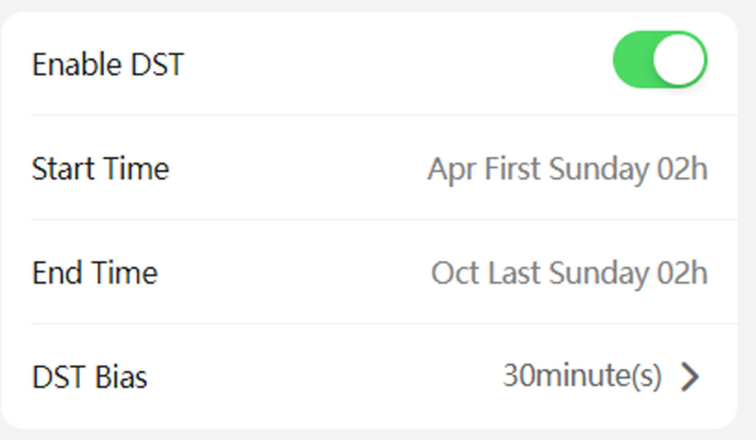
NTP

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

8.4.3 Set DST

Steps

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



Enable DST

Start Time Apr First Sunday 02h

End Time Oct Last Sunday 02h

DST Bias 30minute(s)

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

You can set the wired network, Wi-Fi parameters and device port.

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

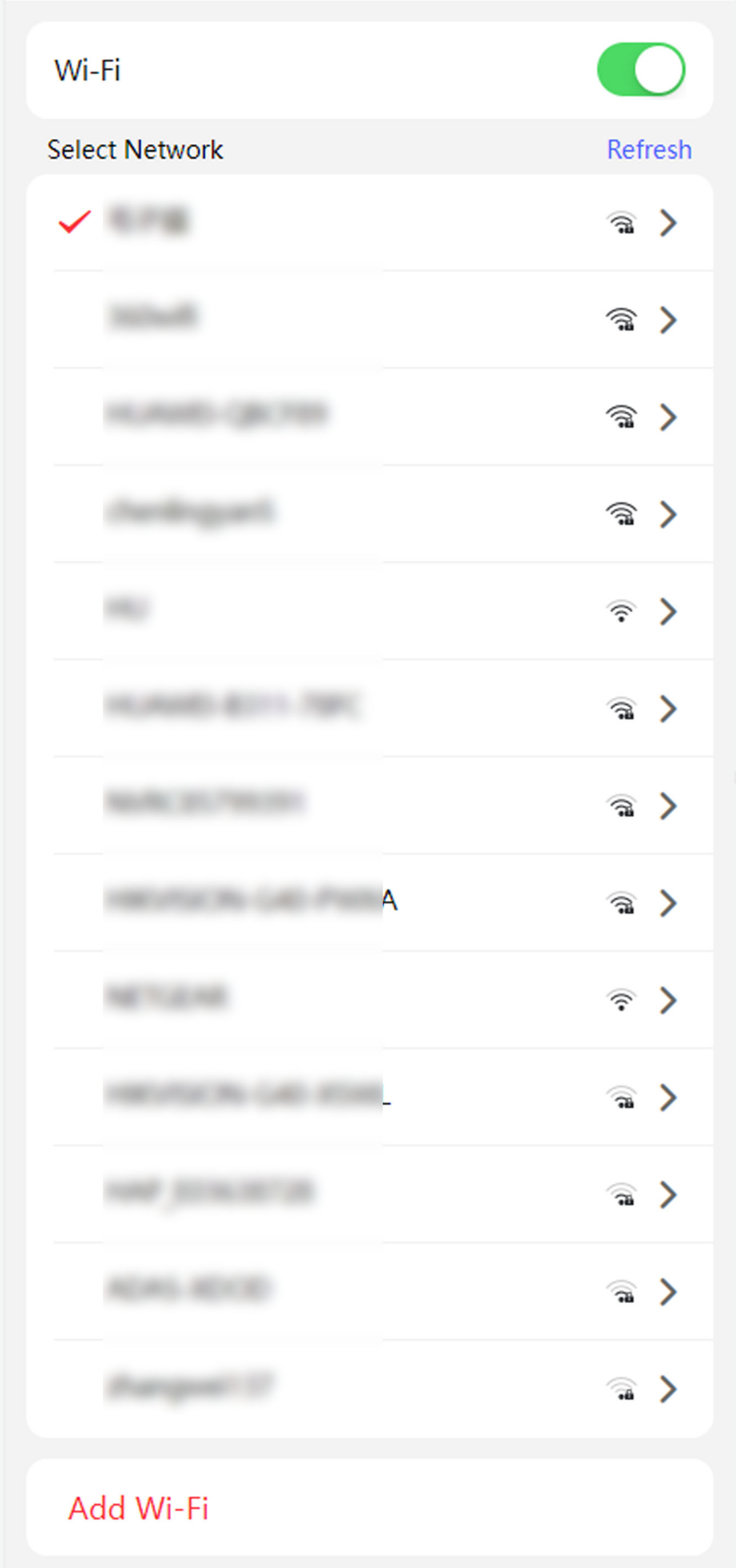
Set the Wi-Fi parameters for device wireless connection.

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**.



Wi-Fi

Select Network Refresh

✓ [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]A

[redacted]

[redacted]_

[redacted]

[redacted]

[redacted]

Add 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 ≡ → **Communication Settings** → **Device Hotspot** .
2. You can enable device hotspot and view the hotspot name.

   Note

   By default, the hotspot name is the AP_Device Serial No.
3. Tap **Save**.

Set Port Parameters

You can set the HTTP and HTTPS according to actual needs when accessing the device via network.

Tap ≡ → **Network Service** → **HTTP(S)** , to enter the setting 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.

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

Note

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

6. You can tap **Bind An Account → View QR Code** , scan the QR code to bind an acount.
7. 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. Tap **Save** to save the settings.

8.4.6 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.

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.

Administrator

If the user needs to be set as administrator, you can enable **Administrator**.

User Role

Select your user role.

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

Note

- Before configuring passwords, it is necessary to clarify whether the password is device-set personal PIN or a platform-applied personal PIN. If it is a device-set personal PIN, it can be created and edited on Web and cannot be created and edited on the platform; If it is a platform-applied personal PIN, it needs to be configured on the platform and cannot be edited on the Web.
- Make sure **Password Mode** is selected as **Device Password**.

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

Enter the password.

3) Tap **Save**.

3. Tap the user that needs to be edited in the user list to edit the information.
4. Tap the user that needs to be deleted in the user list, and tap 🗑 to delete the user.
5. You can search the user by entering the employee ID or name in the search bar.

8.4.7 Search Event

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

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

Note

Support searching for names within 32 digits.

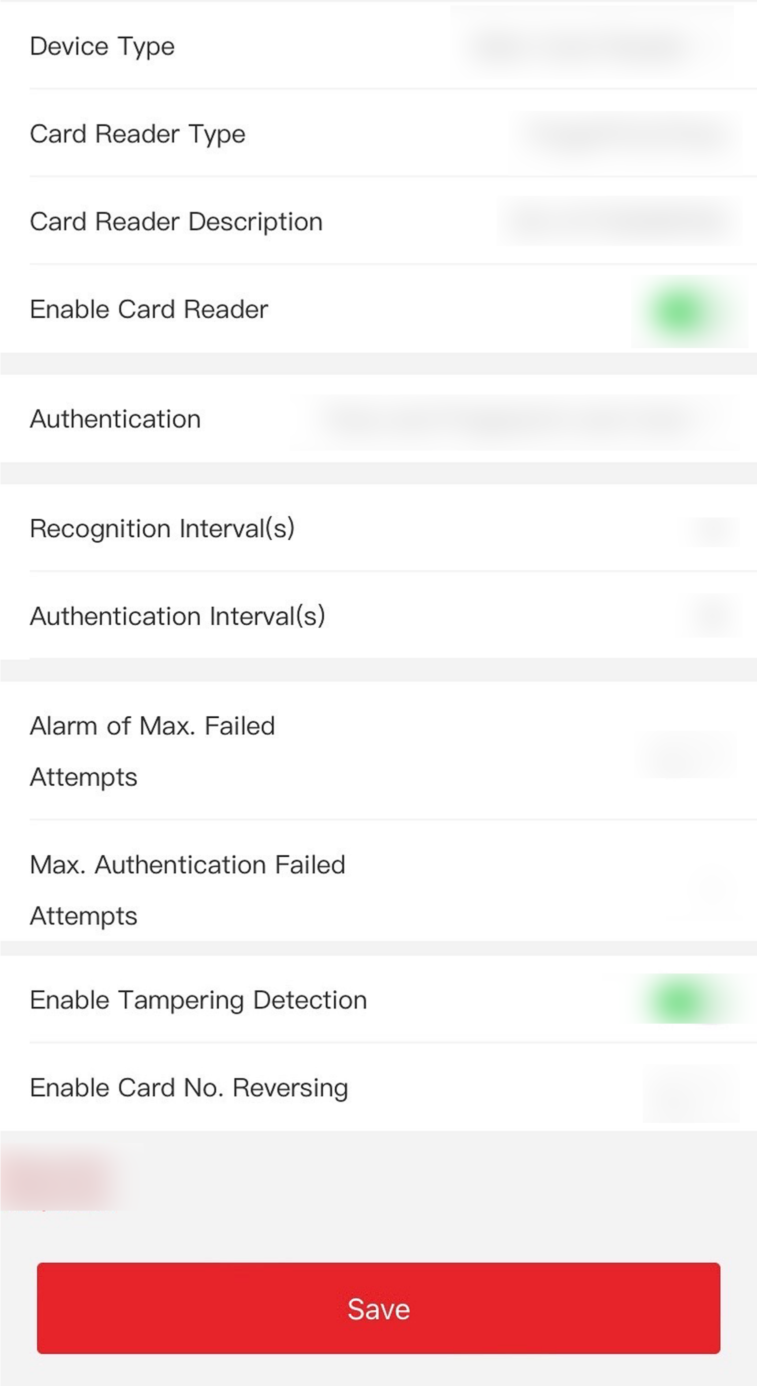
8.4.8 Access Control Settings

Set Authentication Parameters

Set Authentication Parameters.

Steps

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



Device Type

Card Reader Type

Card Reader Description

Enable Card Reader

Authentication

Recognition Interval(s)

Authentication Interval(s)

Alarm of Max. Failed Attempts

Max. Authentication Failed Attempts

Enable Tampering Detection

Enable Card No. Reversing

Figure 8-4 Authentication Settings

2. Tap **Save**.

Terminal

Select terminal for settings.

Terminal Type/Terminal Model

Get terminal description. They are read-only.

Enable Authentication Device

Enable the authentication function.

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.

Alarm of Max. Failed Attempts

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

Main Interface Mode

You can set the **Main Interface Mode** as **Authentication Mode** or **Simple**.

Communication with Controller Every

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

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.

OK LED Polarity/Error LED Polarity

Set OK LED Polarity/Error LED Polarity of the access control device according to the card reader parameters. Generally, adopts the default settings.

Enable Tampering Detection

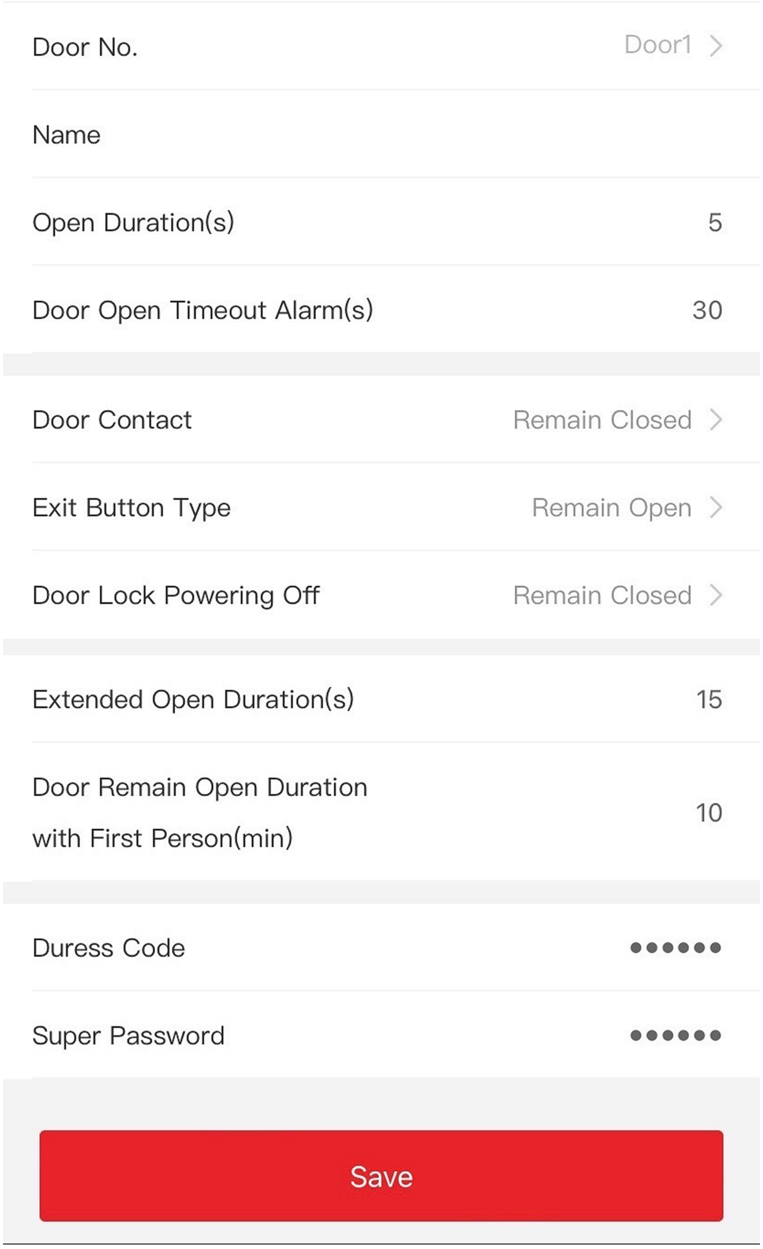
Enable the anti-tamper detection for the card reader.

Enable Card No. Reversing

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

Set Door Parameters

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



Door No.	Door1 >
Name	
Open Duration(s)	5
Door Open Timeout Alarm(s)	30
Door Contact	Remain Closed >
Exit Button Type	Remain Open >
Door Lock Powering Off	Remain Closed >
Extended Open Duration(s)	15
Door Remain Open Duration with First Person(min)	10
Duress Code	●●●●●●
Super Password	●●●●●●

Figure 8-5 Door Parameters Settings Page

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

Name

You can create a name for the door.

Open Duration

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

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.

Door Open Timeout Alarm

An alarm will be triggered if the door has not been closed within the configured time duration.

Door Contact

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

Extended Open Duration

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

Duress Code

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

Super Password

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

Unlock Password

The specific person can open the door by inputting the unlock 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.

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

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 CPU Card

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

8.4.9 Fingerprint Parameters Settings

Set fingerprint Parameters.

Note

The function should support by the device.

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.

8.4.10 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.

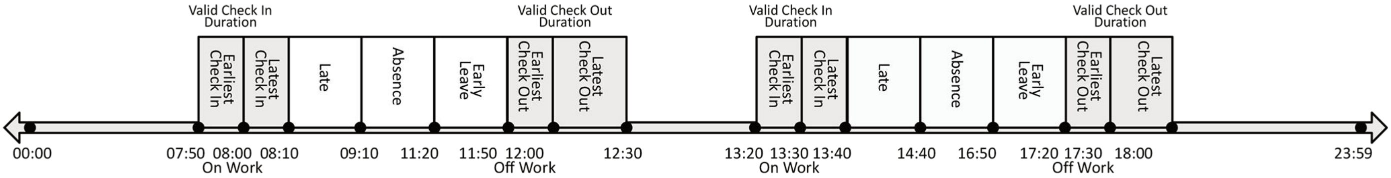


Figure 8-6 Attendance Rule Example

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 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 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 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. Tap **Next** to set **Week** and **Shift** according to your actual needs. You can also click **Add Rule** to add new rules.
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 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. Tap **Next** to set **Week** and **Shift** according to your actual needs. You can also click **Add Rule** to add new rules.
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.

8.4.11 Set Privacy Parameters

Set the display settings.

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

Authentication Settings

Name Display/Employee ID

You can tap to enable 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.

8.4.12 Password Mode

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

Steps

1. Tap ≡ → **Configuration** → **Security** → **Password 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.

2. Tap **Save**.

8.4.13 Upgrade and Maintenance

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

Restart Device

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

Upgrade

Tap ≡ → **Upgrade** .
Tap **Upgrade** to upgrade the device.

Note

Do not power off during the upgrading.

Restore Parameters

Tap ≡ → **Default** .

Restore to Default Settings

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

Restore to Factory Settings

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

8.4.14 View Online Document

Tap ≡ → **View Online Document** . Tap **View Online Document**, you can scan the QR code with your mobile phone for details.

8.4.15 View Open Source Software License

Tap ≡ → **Open Source Software License** , and tap **Open Source Software License** to view the device license.

Chapter 9 Quick Operation via Web Browser

9.1 Select Language

You can select a language for the device system.

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

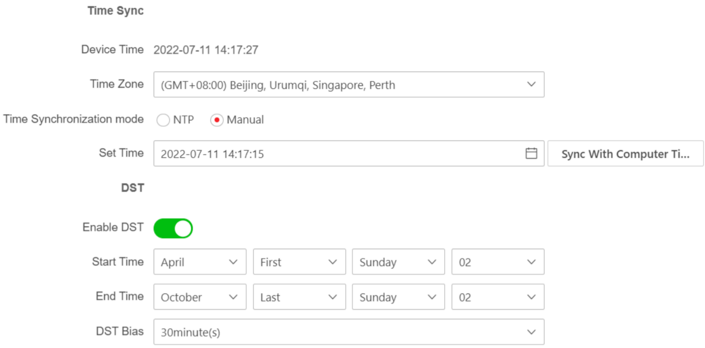
By default, the system language is English.

Note

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

9.2 Time Settings

Set Time and DST



Time Sync

Device Time 2022-07-11 14:17:27

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

Time Synchronization mode ○ NTP ● Manual

Set Time 2022-07-11 14:17:15 Sync With Computer Ti...

DST

Enable DST

Start Time April First Sunday 02

End Time October Last Sunday 02

DST Bias 30minute(s)

Figure 9-1 Time Settings

Click → **Time Settings** .

Time Zone

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

Time Sync.

NTP

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

Manual

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

Server Address Type/Server Address/NTP Port/Interval

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

DST Settings

Enable **DST**.

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

Click **Next** to complete the settings.

9.3 Administrator Settings

Steps

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

Note

You should select at least one credential.

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

Note

Up to 5 cards can be supported.

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

Note

Up to 10 fingerprints are allowed.

4. Click **Complete**.

Chapter 10 Operation via Web Browser

10.1 Login

You can login via the web browser.

Note

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

Login via Web Browser

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

10.2 Forget Password

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

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

Select **Verification Mode**.

Security Question Verification

Answer the security questions.

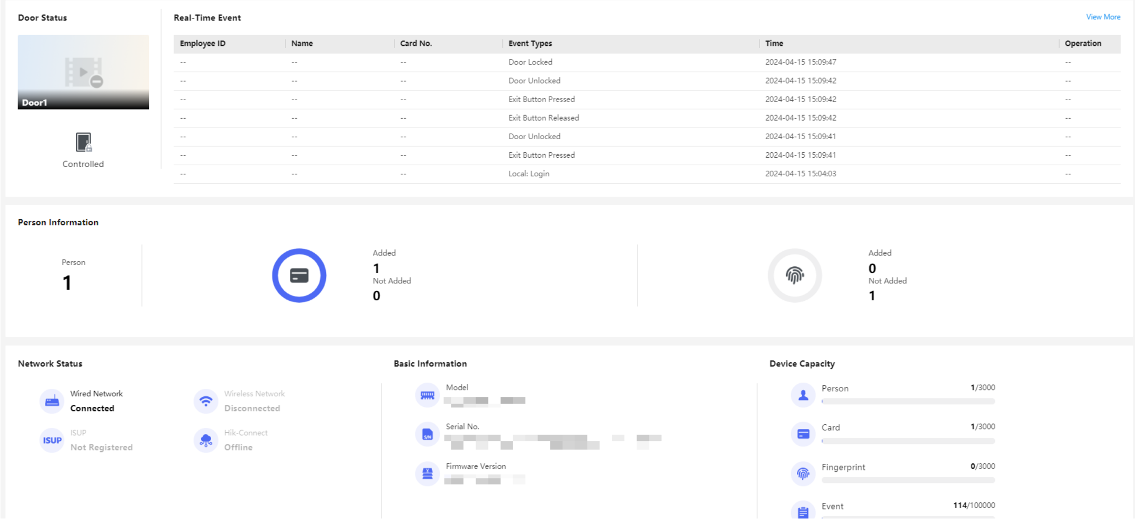
E-mail Verification

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

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

10.3 Overview

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



Employee ID	Name	Card No.	Event Types	Time	Operation
--	--	--	Door Locked	2024-04-15 15:09:47	--
--	--	--	Door Unlocked	2024-04-15 15:09:42	--
--	--	--	Exit Button Pressed	2024-04-15 15:09:42	--
--	--	--	Exit Button Released	2024-04-15 15:09:42	--
--	--	--	Door Unlocked	2024-04-15 15:09:41	--
--	--	--	Exit Button Pressed	2024-04-15 15:09:41	--
--	--	--	Local: Login	2024-04-15 15:04:03	--

Person Information

Person 1

Added 1 Not Added 0

Added 0 Not Added 1

Network Status

Wired Network: Connected

Wireless Network: Disconnected

ISUP: Not Registered

Hik-Connect: Offline

Basic Information

Model: [redacted]

Serial No.: [redacted]

Firmware Version: [redacted]

Device Capacity

Person 1/3000

Card 1/3000

Fingerprint 0/3000

Event 114/100000

Figure 10-1 Live View Page

Function Descriptions:

Door Status

🔓 / 🔒 / ▣ / ▣

Tap the door status icon and you can change the door status to open/closed/remaining open/remaining closed.

Real-Time Event

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

Person Information

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

Network Status

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

Basic Information

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

Device Capacity

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

10.4 Person Management

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

Add Basic Information

Click **Person Management → Add** to enter the Add Person page.
Add the person's basic information, including the employee ID, the person's name, person type, department, etc.
If you select **Visitor** as the person type, you can set the visit times.
Click **Save** to save the settings.

Set Permission Time

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

Add Card

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

Add Fingerprint

Note

Only devices supporting the fingerprint function can add the fingerprint.

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

Add PIN

Before configuring passwords, it is necessary to clarify whether the password is a device-set personal PIN or a platform-applied personal PIN. If it is a device-set personal PIN, it can be created or edited on the device or on the web, and cannot be set on other platforms; If it is a platform-applied personal PIN, it can be created or edited on the platform, and issued to the device before it can be used. It cannot be set on the device or on the web.
Click **Configuration → Security → Password Mode** , select **Password Mode** as **Device-Set Personal PIN**.
Click **Person Management → Add** to enter the Add Person page.
Set the password.

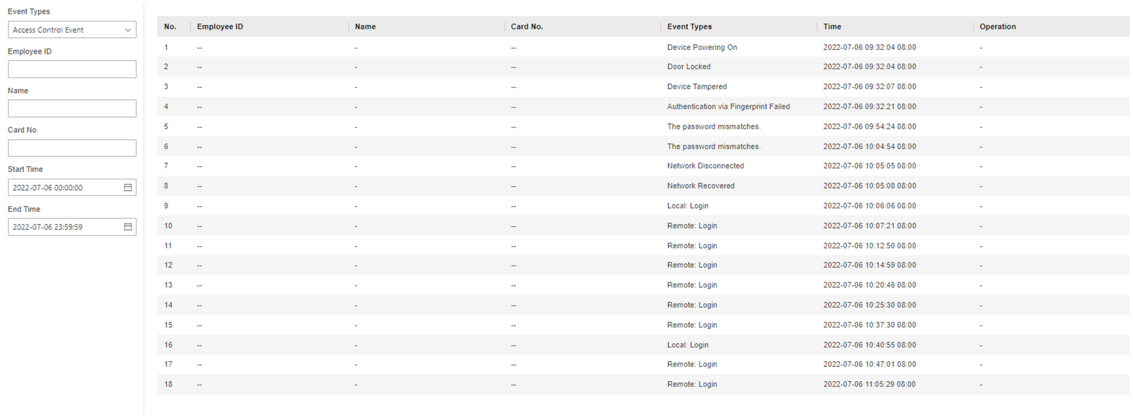
Click **Save** to save the settings.

Authentication Settings

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

10.5 Search Event

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



Event Types: Access Control Event
Employee ID:
Name:
Card No.:
Start Time: 2022-07-06 00:00:00
End Time: 2022-07-06 23:59:59

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

Figure 10-2 Search Event

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

The results will be displayed on the right panel.

10.6 Configuration

10.6.1 View Device Information

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

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

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

10.6.2 Set Time

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

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

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

Time Zone

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

Time Sync.

NTP

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

Manual

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

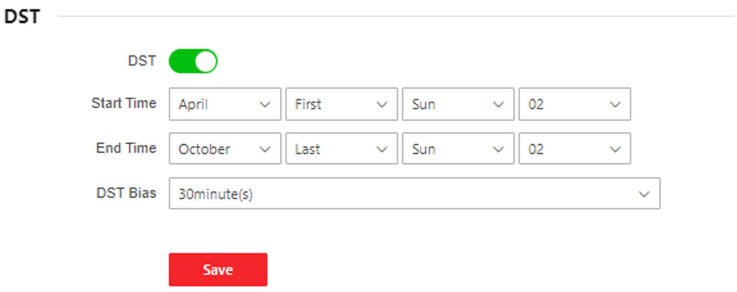
Server Address Type/Server Address/NTP Port/Interval

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

10.6.3 Set DST

Steps

1. Click **Configuration → System → System Settings → Time Settings** .



DST

DST: ●

Start Time: April | First | Sun | 02

End Time: October | Last | Sun | 02

DST Bias: 30minute(s)

Figure 10-3 DST Page

2. Enable **DST**.
3. Set the DST start time, end time and bias time.
4. Click **Save** to save the settings.

10.6.4 Change Administrator's Password

Steps

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

⚠**Caution**

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

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

10.6.5 Account Security Settings

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

Steps

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

10.6.6 View Device Arming/Disarming Information

View device arming type and arming IP address.

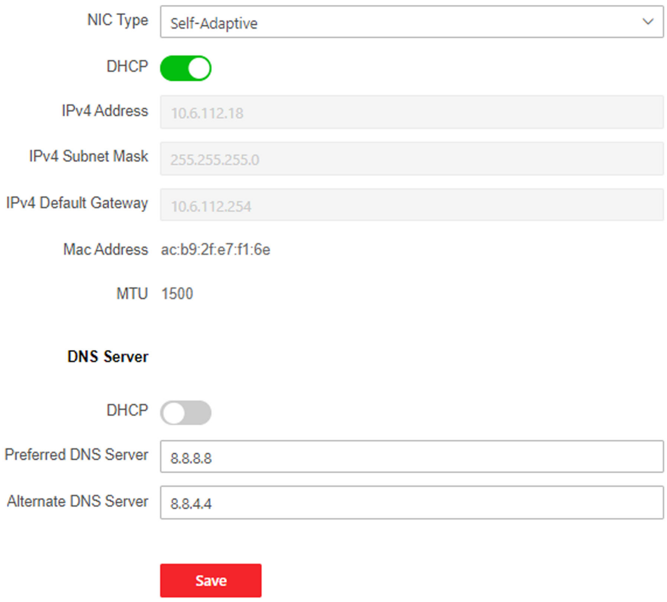
Click **Configuration → System → User Management → Arming/Disarming Information** .

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

10.6.7 Network Settings

Set Basic Network Parameters

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



NIC Type: Self-Adaptive

DHCP: ●

IPv4 Address: 10.6.112.18

IPv4 Subnet Mask: 255.255.255.0

IPv4 Default Gateway: 10.6.112.254

Mac Address: ac:b9:2f:e7:f1:6e

MTU: 1500

DNS Server

DHCP: ○

Preferred DNS Server: 8.8.8.8

Alternate DNS Server: 8.8.4.4

Figure 10-4 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

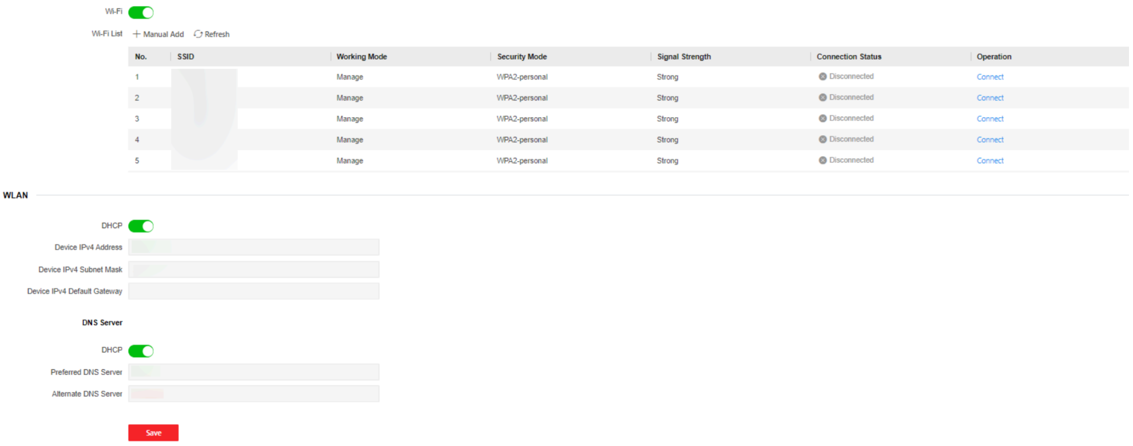
Set the Wi-Fi parameters for device wireless connection.

Steps

Note

The function should be supported by the device.

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



Wi-Fi ●

Wi-Fi List + Manual Add ↻ Refresh

No.	SSID	Working Mode	Security Mode	Signal Strength	Connection Status	Operation
1		Manage	WPA2-personal	Strong	Disconnected	Connect
2		Manage	WPA2-personal	Strong	Disconnected	Connect
3		Manage	WPA2-personal	Strong	Disconnected	Connect
4		Manage	WPA2-personal	Strong	Disconnected	Connect
5		Manage	WPA2-personal	Strong	Disconnected	Connect

WLAN

DHCP ●

Device IPv4 Address

Device IPv4 Subnet Mask

Device IPv4 Default Gateway

DNS Server

DHCP ●

Preferred DNS Server

Alternate DNS Server

Save

Figure 10-5 Wi-Fi Settings Page

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

Set Device Hotspot

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

Steps

1. Click **Configuration → Network → Network Settings → Device Hotspot** .
2. You can enable device hotspot, and click **Save**.

Set Port Parameters

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

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

HTTP

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

HTTPS

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

HTTP Listening

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

Note

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

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

SDK Server

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

Set ISUP Parameters

Set the ISUP parameters for accessing device via ISUP protocol.

Steps

Note

The function should be supported by the device.

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

   Note

   If you select 5.0 as the version, you should set the **Encryption Key**.
4. Set the **Network Connection Priority**. You can enable **Allow Access**, and click the network and drag it to adjust the network priority.
5. Set the ISUP listening parameters, including ISUP alarm center IP address/domain name, ISUP alarm center URL, and ISUP alarm center port.

6. Click **Save**.

Platform Access

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

Steps

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

   Note

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

2. Check **Enable** to enable the function.
3. **Optional:** Check the checkbox of **Custom**, and you can set the server address by yourself.
4. Enter the server IP address, and verification code.

   Note

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

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

   Note

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

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

   Note

   Scan the QR code before it loses efficacy.

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

10.6.8 Access Control Settings

Set Authentication Parameters

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

Note

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

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

If select **Terminal Main**:

Terminal/Terminal Type/Terminal Model

Select terminal and get the terminal description. They are read-only.

Enable Authentication Device

Enable the authentication function.

Authentication

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

Recognition Interval

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

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.

Alarm of Max. Failed Attempts

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

Tampering Detection

Enable the anti-tamper detection for the card reader.

Card No. Reversing

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

If select **Terminal Sub**:

Terminal/Terminal Type/Terminal Model

Select terminal and get the terminal description. They are read-only.

Enable Authentication Device

Enable the authentication function.

Sub Card Reader Position

You can select sub card reader position as different or same side as the main card reader.

Authentication

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

Recognition Interval

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

Alarm of Max. Failed Attempts

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

Communication with Controller Every

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

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.

OK LED Polarity/Error LED Polarity

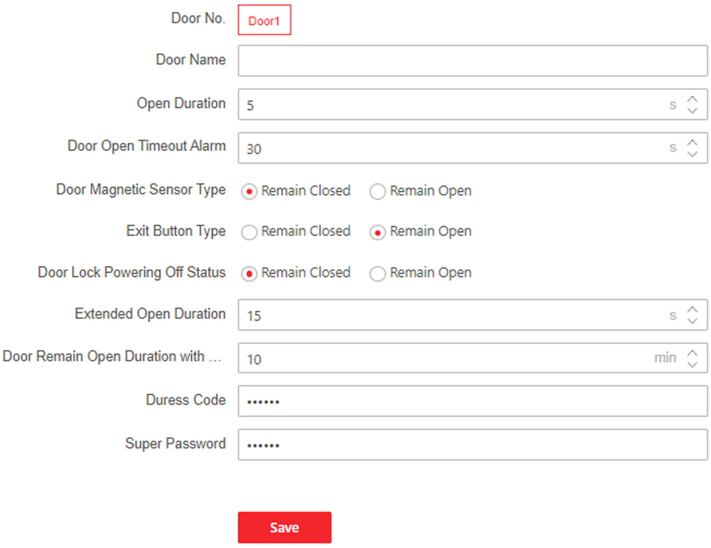
Set OK LED Polarity/Error LED Polarity of the access control device according to the card reader parameters. Generally, adopts the default settings.

Tampering Detection

Enable the anti-tamper detection for the card reader.

Set Door Parameters

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



Door No.	Door1
Door Name	
Open Duration	5 s
Door Open Timeout Alarm	30 s
Door Magnetic Sensor Type	● Remain Closed ○ Remain Open
Exit Button Type	○ Remain Closed ● Remain Open
Door Lock Powering Off Status	● Remain Closed ○ Remain Open
Extended Open Duration	15 s
Door Remain Open Duration with ...	10 min
Duress Code	••••••
Super Password	••••••

Figure 10-7 Door Parameters Settings Page

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

Door No.

Select the device corresponded door No.

Name

You can create a name for the door.

Open Duration

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

Door Open Timeout Alarm

An alarm will be triggered if the door has not been closed within the configured time duration.

Door Contact

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

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 Lock Powering Off Status

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

Extended Open Duration

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

Door Remain Open Duration with First Person

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

Duress Code

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

Super Password

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

Note

The duress code and the super code should be different.

Set Terminal Parameters

Set the working mode.

Steps

1. Set the device working mode.

   Access Control Mode

   The device works normally and will verify the person's permission to open the barrier.

2. Click **Save** to complete terminal parameter settings.

10.6.9 Card Settings

Set Card Security

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

Set the parameters and click **Save**.

Enable NFC Card

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

Enable M1 Card

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

M1 Card Encryption
Sector

M1 card encryption can improve the security level of authentication.

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

Enable CPU Card

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

Set Card No. Authentication Parameters

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

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

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

Full Card No.

All card No. will be read.

3 bytes

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

4 bytes

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

10.6.10 Time and Attendance Settings

If you want to record the person's working hour, late arrivals, early departures, breaks, absenteeism, etc., you can add the person to the shift group and assign a shift schedule (a rule for the attendance defining how the schedule repeats, the shift type, break settings, and the card swiping rule.) to the shift group to define the attendance parameters for the persons in the shift group.

Disable Attendance Mode via Web

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

Steps

1. Click **Configuration → Platform Attendance** to enter the settings page.
2. Disable the **Time and Attendance**.

Result

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

Time Settings

Steps

1. Click **Configuration → Platform Attendance** to enter the settings page.
2. Select **Schedule Template**.
3. Drag mouse to set the schedule.

   Note

   Set the schedule from Monday to Sunday according to the actual needs.
4. You can enable **On/off Work**, **Break**, **Overtime** according to your actual needs and set the custom name.
5. **Optional:** Select a timeline and click **Delete**. Or click **Delete All** to clear the settings.
6. Click **Save**.

Set Manual Attendance via Web

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

Before You Start

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

Steps

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

Note

The Attendance Property will not be changed.

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

Result

You should select an attendance status manually after authentication.

Note

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

Set Auto Attendance via Web

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

Before You Start

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

Steps

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

   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 ***Time Settings*** for details.

Set Manual and Auto Attendance via Web

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

Before You Start

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

Steps

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

4. Enable a group of attendance status.

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 ***Time Settings*** 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.

10.6.11 Local Time and Attendance Settings

Manage Department via Web

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

Steps

1. Click **Person Management**.
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.

Enable Local T&A

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

Steps

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

Set Attendance Rule for Shift

Set attendance rule before setting shift.

Click **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.

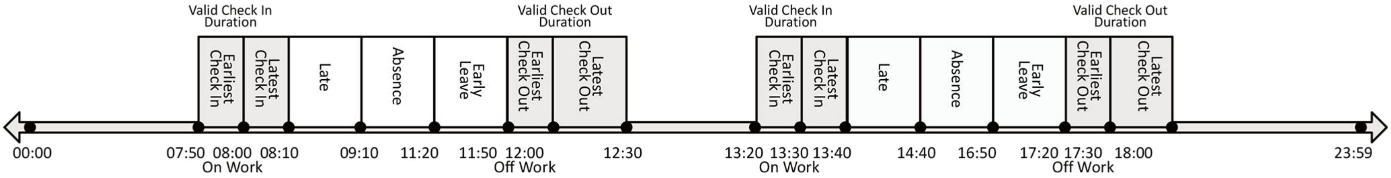


Figure 10-8 Attendance Rule Example

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

Manage Normal Shift via Web

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

Steps

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

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 **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** to set **Week** and **Shift** 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 **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** to set **Week** and **Shift** according to your actual needs. You can also click **Add Rule** to add new rules.
6. Click **Complete**.

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 Report → Attendance Report** , select the report, and you can view the Attendance Report and click **Export Excel** to export it.

10.6.12 Set Privacy Parameters

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

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

Event Storage Settings

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

Delete Old Events Periodically

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

Delete Old Events by Specified Time

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

Overwriting

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

Authentication Settings

Display Authentication Result

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

Name De-identification

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

10.6.13 Set Password Mode

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

Steps

1. Click **Configuration → Security → Password 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.

2. Click **Save**.

10.6.14 Set Fingerprint Security Level on PC Web

Click **Configuration → Smart → Smart** .

Fingerprint Security Level

Select the fingerprint security level.
The higher is the security level, the lower is the false acceptance rate (FAR).
The higher is the security level, the higher is the false rejection rate (FRR).

10.6.15 Set Preference

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

Set Theme

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

Sleep

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

Display Mode

You can select display theme for device authentication. You can select **Display Mode** as **Simple**. When you select **Simple**, the information of name, ID will be not displayed.

10.6.16 Upgrade and Maintenance

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

Reboot Device

Click **Maintenance and Security → Maintenance → Restart** .
Click **Restart** to reboot the device.

Upgrade

Click **Maintenance and Security → Maintenance → Upgrade** .
Select an upgrade type from the drop-down list. Click 🗀 and select the upgrade file from your local PC. Click **Upgrade** to start upgrading.
If the device has been connected to Hik-Connect and network, when there is a new installation package in Hik-Connect, you can click **Upgrade** after Online Update to upgrade the device system.

Note

Do not power off during the upgrading.

Restore Parameters

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

Restore All

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

Restore

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

Import and Export Parameters

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

Export

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

Note

You can import the exported device parameters to another device.

Import

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

10.6.17 Device Debugging

You can set device debugging parameters.

Steps

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

   Enable SSH

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

   Print Log

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

   Capture Network Packet

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

10.6.18 Log Query

You can search and view the device logs.

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

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

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

10.6.19 Security Mode Settings

Set the security mode for logging in the client software.

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

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

Security Mode

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

Compatible Mode

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

10.6.20 Certificate Management

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

Note

The function is only supported by certain device models.

Create and Install Self-signed Certificate

Steps

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

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

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

Install Other Authorized Certificate

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

Steps

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

Install CA Certificate

Before You Start

Prepare a CA certificate in advance.

Steps

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

   Note

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

Chapter 11 Other Platforms to Configure

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

iVMS-4200 Client Software

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

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

HikCentral Access Control (HCAC)

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

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

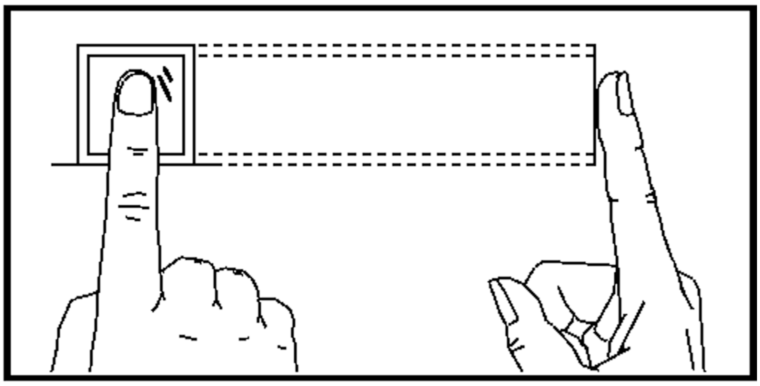
Appendix A. Tips for Scanning Fingerprint

Recommended Finger

Forefinger, middle finger or the third finger.

Correct Scanning

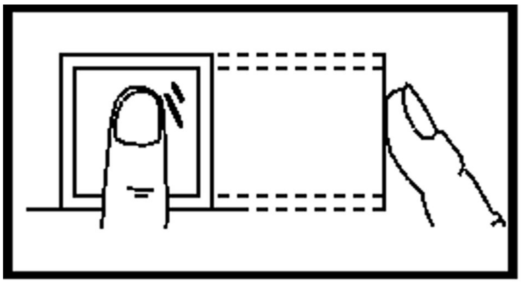
The figure displayed below is the correct way to scan your finger:



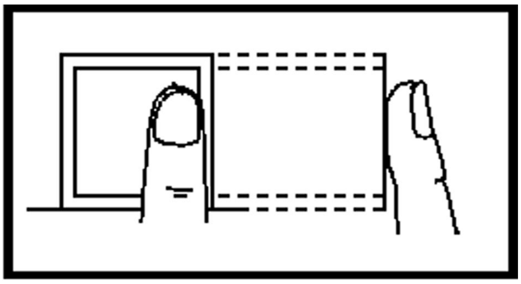
You should press your finger on the scanner horizontally. The center of your scanned finger should align with the scanner center.

Incorrect Scanning

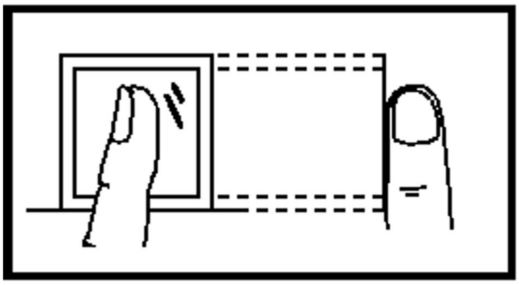
The figures of scanning fingerprint displayed below are incorrect:



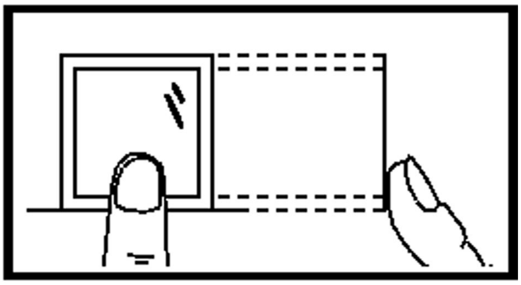
Vertical



Edge I



Side



Edge II

Environment

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

Others

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

Appendix B. Dimension

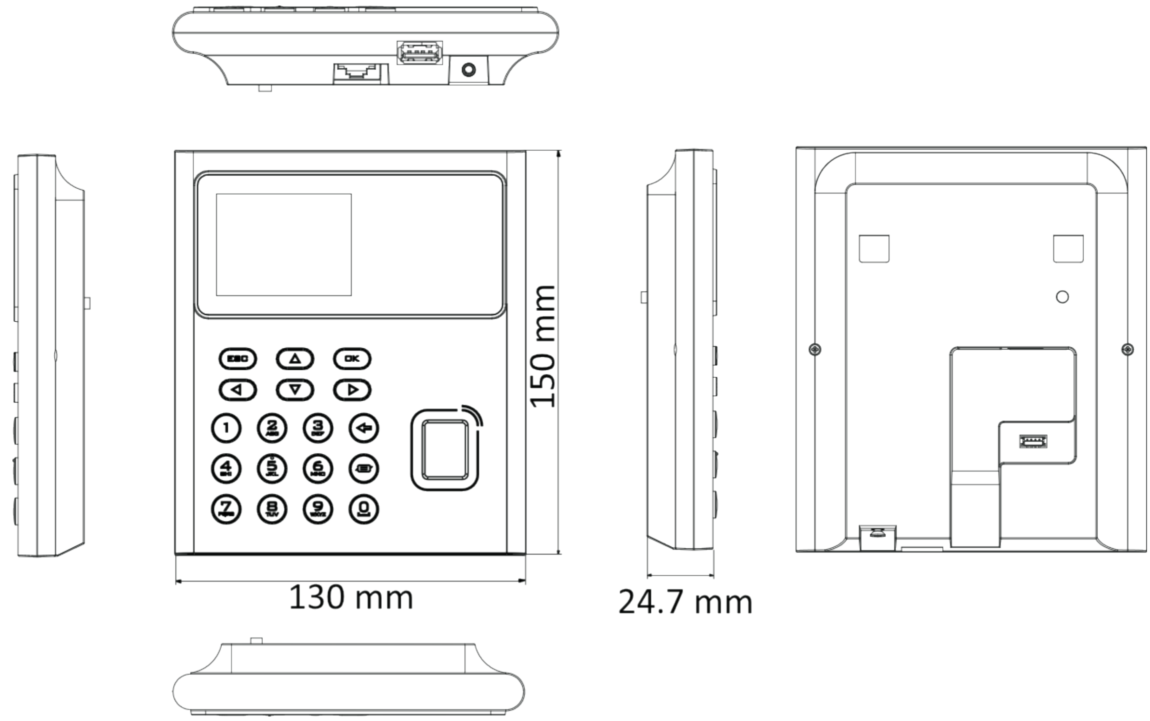


Figure B-1 Dimension

See Far, Go Further