DS-K1T321 Series Face Recognition Terminal

Legal Information

About this Manual

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

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

Trademarks

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

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

Disclaimer

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

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

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

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

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

Data Protection

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

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

Symbol Conventions

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

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

Regulatory Information

FCC Information

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

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

—Reorient or relocate the receiving antenna.

—Increase the separation between the equipment and receiver.

—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

—Consult the dealer or an experienced radio/TV technician for help

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

FCC Conditions

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

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

EU Conformity Statement

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

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

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

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

Safety Instruction

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

The precaution measure is divided into Dangers and Cautions:

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

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

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

⚠ Danger:

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

⚠ Cautions:

- 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 100% applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.
- The serial port of the equipment is used for debugging only.
- Install the equipment according to the instructions in this manual. To prevent injury, this equipment must be securely attached to the floor/wall in accordance with the installation instructions.
- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.
- This bracket is intended for use only with equipped devices. Use with other equipment may result in instability causing injury.
- This equipment is for use only with equipped bracket. Use with other (carts, stands, or carriers) may result in instability causing injury.

Available Models

Product Name	Model	Wireless
Face Recognition Terminal	DS-K1T321MFX	13.56 MHz Card Presenting Frequency
	DS-K1T321MWX	13.56 MHz Card Presenting Frequency, WiFi, 2.4G
	DS-K1T321MFW	13.56 MHz Card Presenting Frequency, WiFi, 2.4G
	DS-K1T321EX	125 KHz Card Presenting Frequency
	DS-K1T321EFX	125 KHz Card Presenting Frequency
	DS-K1T321EWX	125 KHz Card Presenting Frequency, WiFi, 2.4G
	DS-K1T321EFWX	125 KHz Card Presenting Frequency, WiFi, 2.4G
	DS-K1T321MX	13.56 MHz Card Presenting Frequency

Use only power supplies listed in the user instructions:

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

Contents

Chapter 1 Overview

1.1 Overview

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

1.2 Features

- 2.4-inch LCD screen, 2 MP lens
- Multiple authentication methods, including face, fingerprint, card, and PIN, etc
- Supports Mifare card or EM card according to different models
- Max. 500 faces, 1,000 cards, 1,000 fingerprints and 100,000 events
- Face recognition duration < 0.2 s/User
- Supports ISAPI and ISUP 5.0 protocols
- Configuration via the PC web browser and mobile web browser

Chapter 2 Appearance

The appearance of the device with fingerprint is as follows:

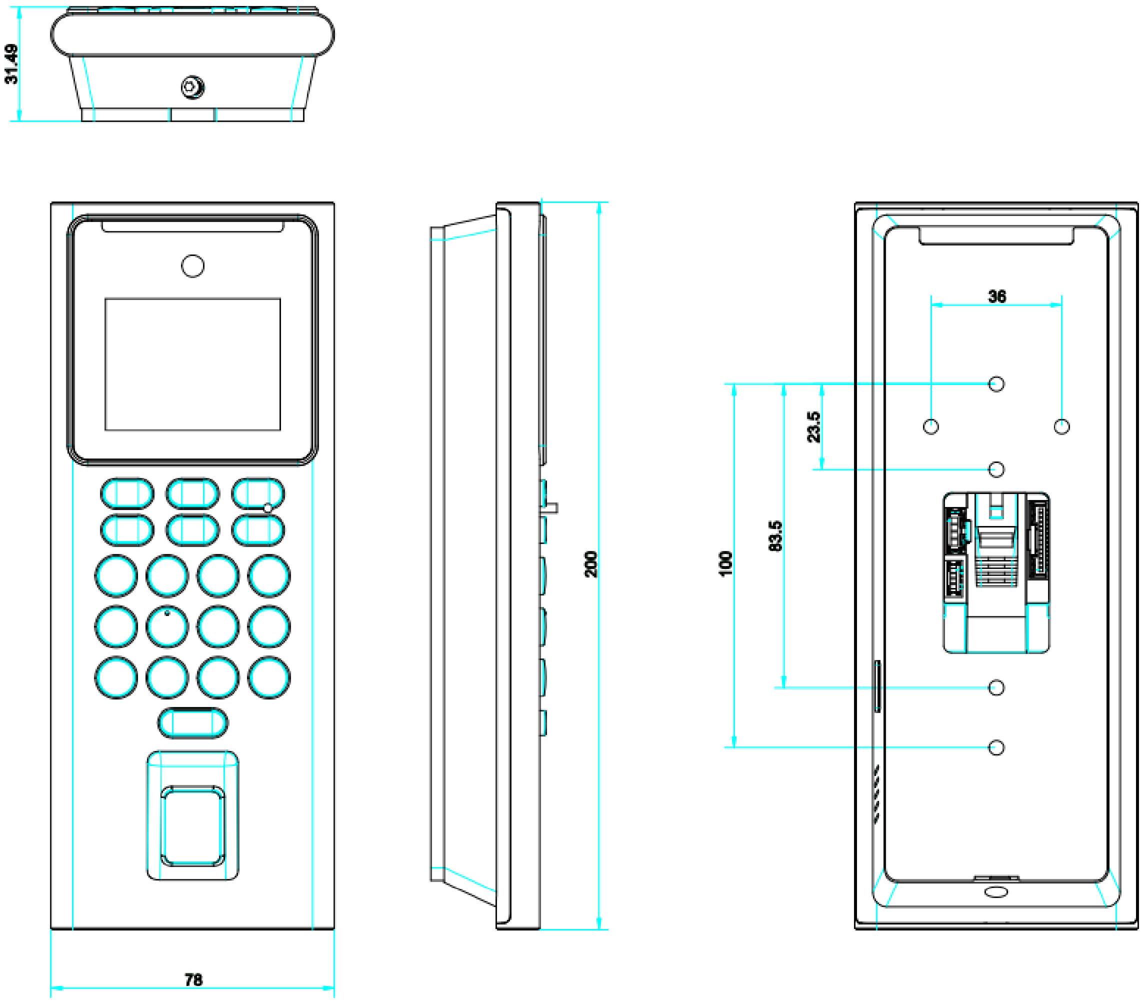


Figure 2-1 Appearance

The appearance of the device without fingerprint is as follows:

Table 2-1 Appearance Description

No.	Name
1	Screen
2	Keypad
3	Fingerprint Module

No.	Name
	Note Only devices that support the fingerprint function contain a fingerprint module.
4	Card Swiping Area
5	Camera
6	Supplement Light
7	USB Interface
8	Network Interface
9	Tamper
10	Wiring Terminal (Including Power Supply Interface)
11	Debugging Port (For Debugging Only)

Chapter 3 Installation

3.1 Installation Environment

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

3.2 Install with Gang Box

Steps

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

   Note

   You should purchase the gang box separately.

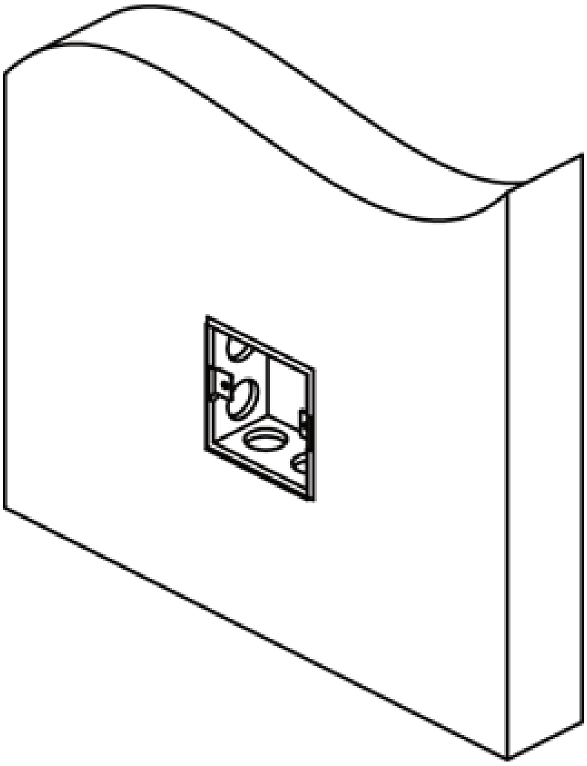


Figure 3-1 Install Gang Box

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

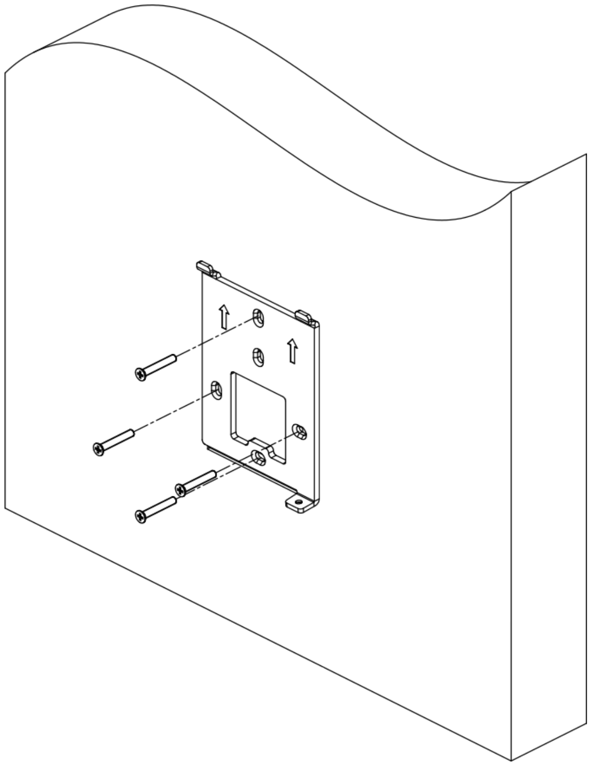


Figure 3-2 Install Mounting Plate

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

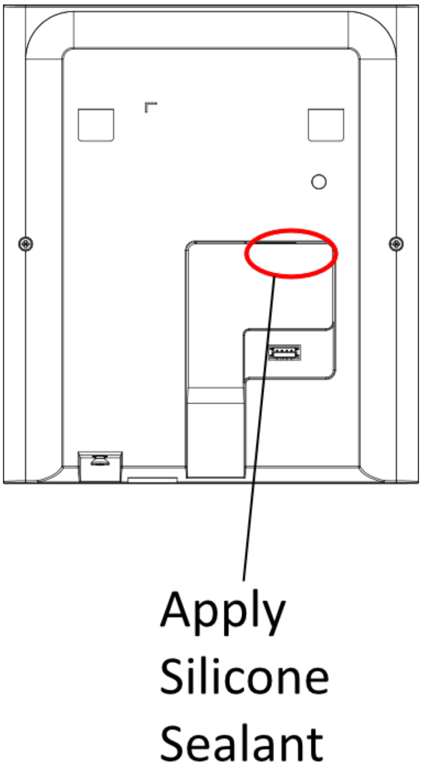


Figure 3-3 Apply Silicone Sealant

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

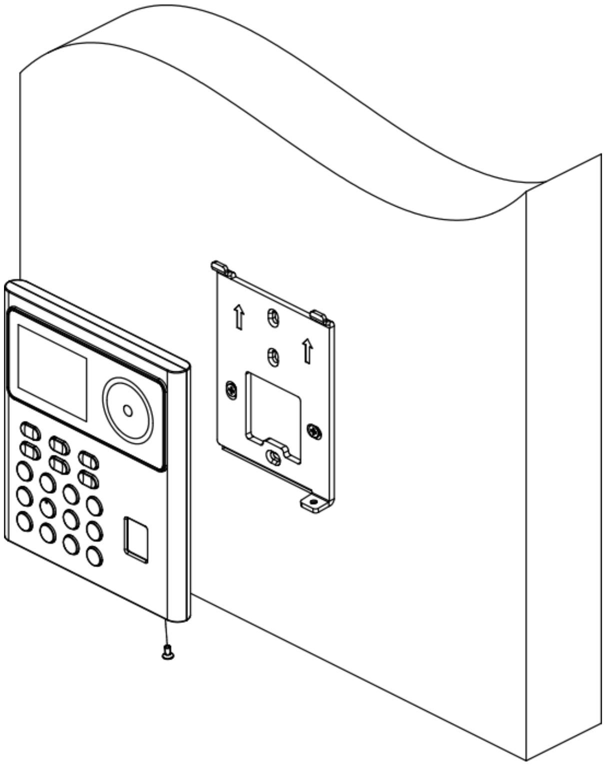


Figure 3-4 Secure Device

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).

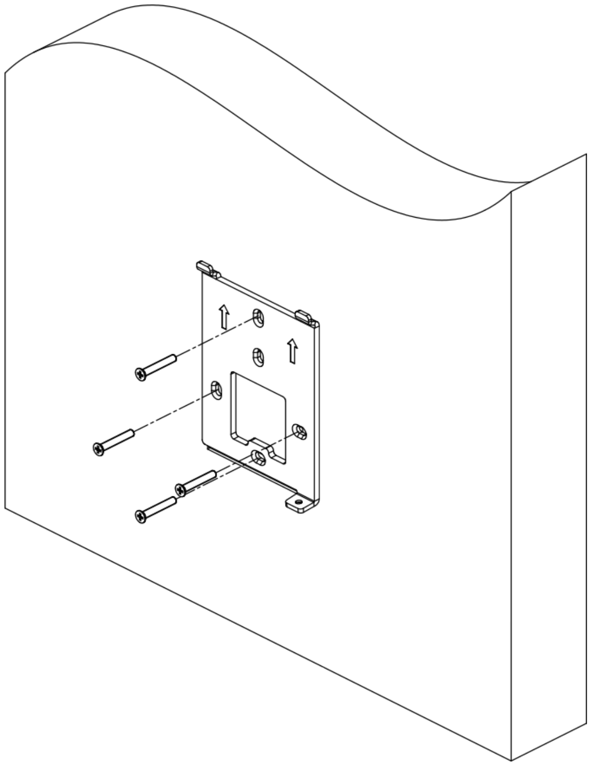


Figure 3-5 Install Mounting Plate

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.

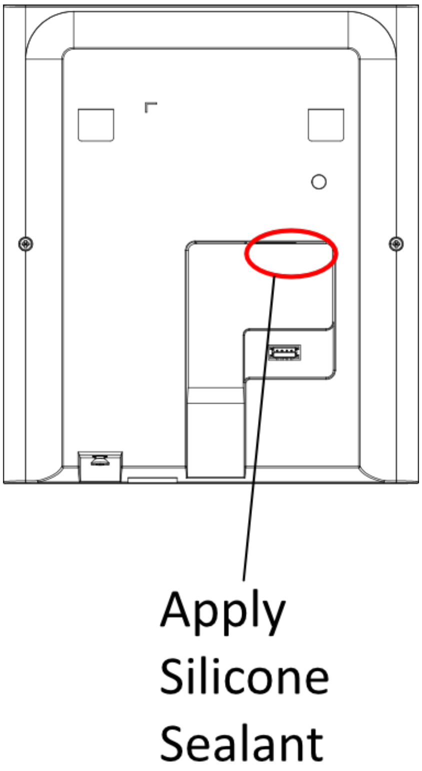


Figure 3-6 Apply Silicone Sealant

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.

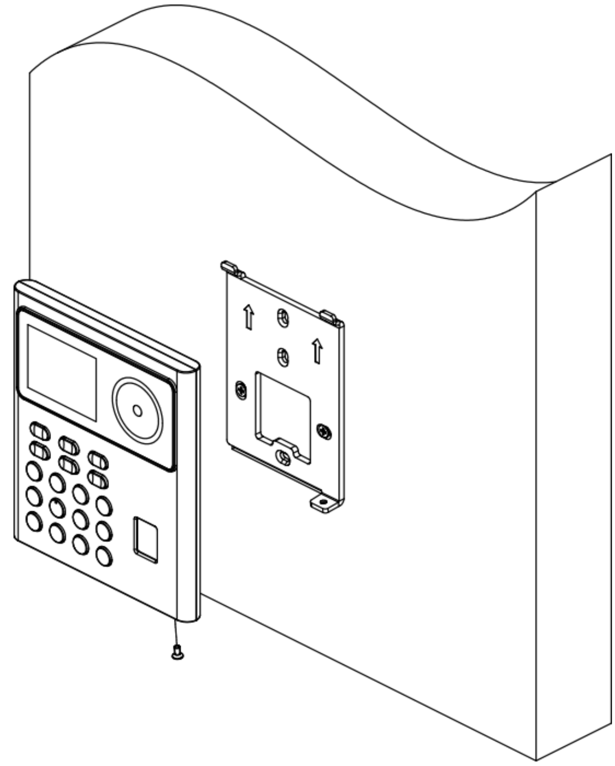


Figure 3-7 Hang Device

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.

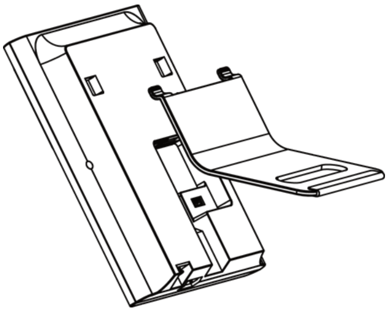


Figure 3-8 Place Bracket Close to Device Back Side

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.

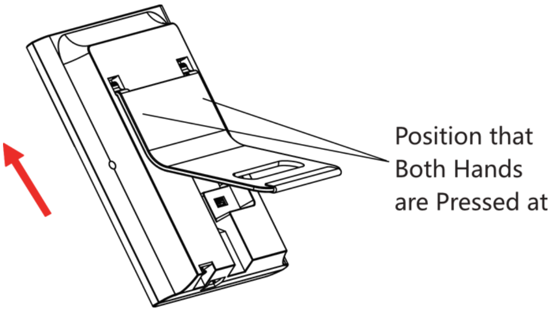


Figure 3-9 Fasten Bracket

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

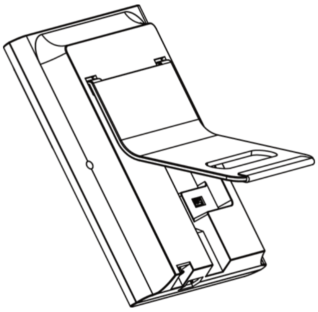


Figure 3-10 Complete Installation

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 and door lock.

The descriptions of the terminals are as follows:

Table 4-1 Terminal Descriptions

Group	No.	Function	Color	Name	Description
Group A	A1	Power Input	Red	+12 V	12 VDC Power Supply
	A2		Black	GND	Ground
Group B	B1	Door Lock	White/Purple	NC	Lock Wiring (NC)
	B2		White/Yellow	COM	Common
	B3		White/Red	NO	Lock Wiring (NO)
	B4		Yellow/Green	SENSOR	Door Contact
	B5		Black	GND	Ground
	B6		Yellow/Grey	BUTTON	Exit Door Wiring

4.2 Wire Normal Device

You can connect the terminal with normal peripherals.

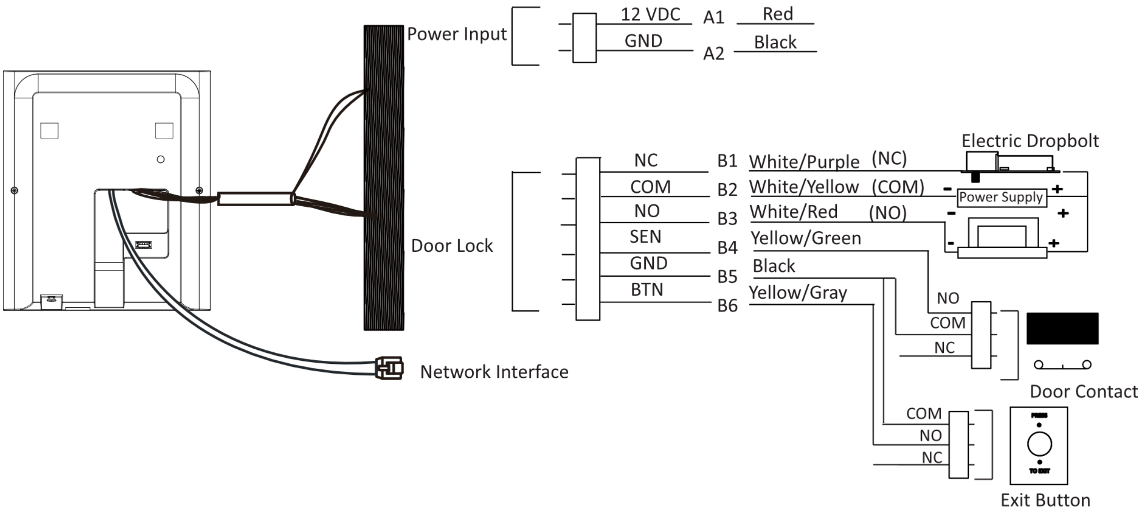


Figure 4-1 Device Wiring

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.

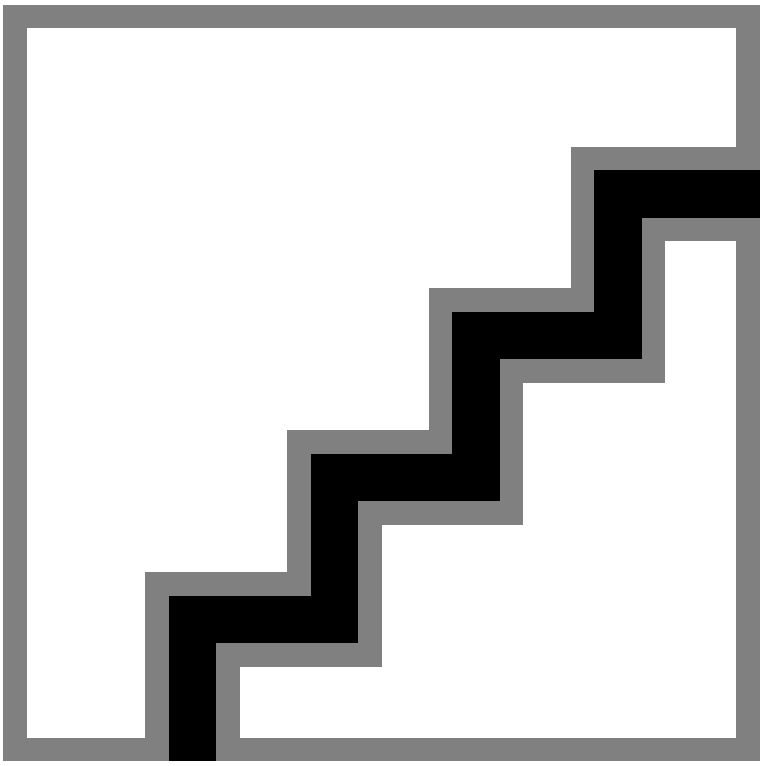


Figure 5-1 Activation Page

⚠ **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.

- After activation, you should select a language according to your actual needs.
- After activation, you should set the network. For details, see ***Set Network Parameters*** .
- After activation, you can add the device to the platform. For details, see ***Access to Platform*** .
- After activation, if you need to set privacy, you should check the item. For details, see ***Privacy Settings*** .
- After activation, if you need to add administrator to manage the device parameters, you should set administrator. For details, see ***Add Administrator*** .

5.2 Activate via Web Browser

You can activate the device via the web browser.

Steps

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

   Note

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

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

   ⚠ **Caution**

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

Note

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

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

5.3 Activate via SADP

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

Before You Start

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

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

Steps

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

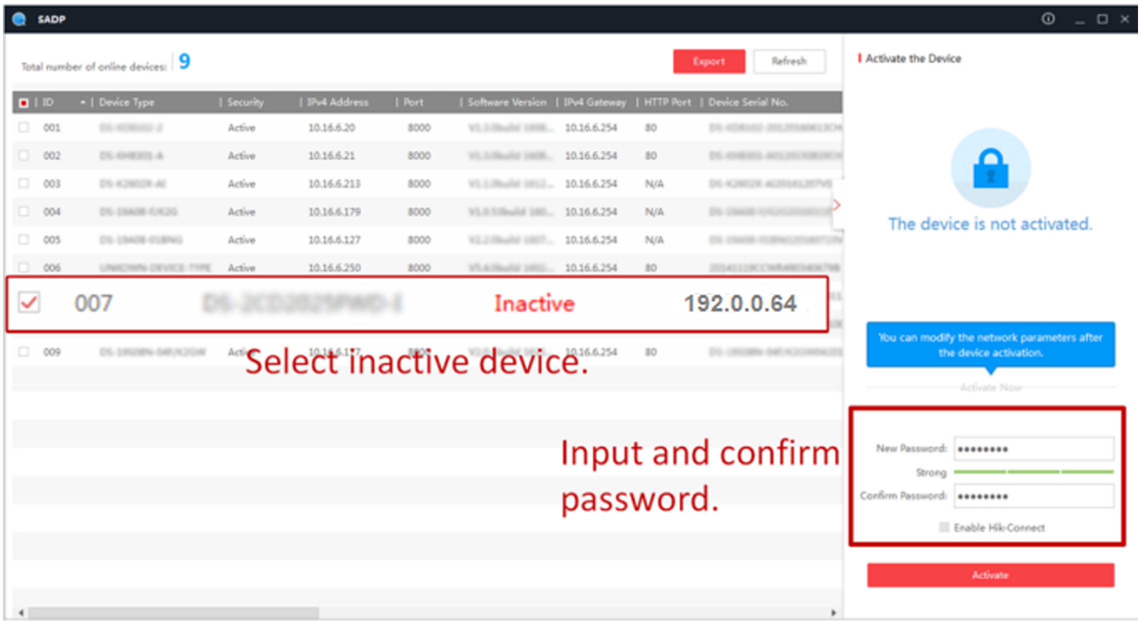
Caution

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

Note

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

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



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]	Active	10.16.6.177	8000	[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.

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.

5.4 Activate Device via iVMS-4200 Client Software

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

Steps

Note

This function should be supported by the device.

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

   The searched online devices are displayed in the list.
4. Check the device status (shown on **Security Level** column) and select an inactive device.
5. Click **Activate** to open the Activation dialog.
6. Create a password in the password field, and confirm the password.

⚠ **Caution**

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

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

Note

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

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

Chapter 6 Quick Operation

6.1 Select Language

You can select a language for the device system.

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

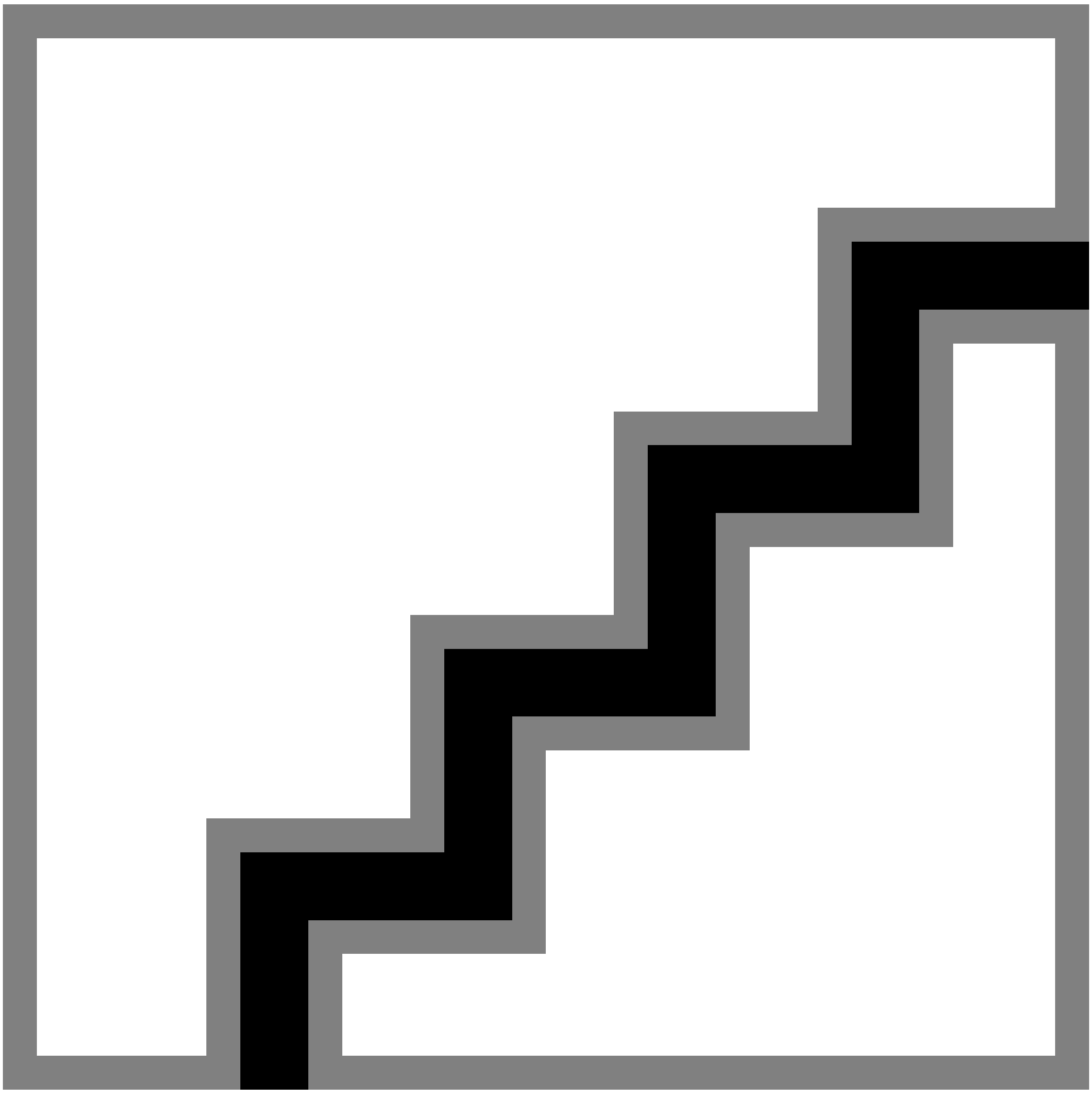


Figure 6-1 Select System Language

By default, the system language is English.

Note

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

6.2 Set Network Parameters

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

Steps

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

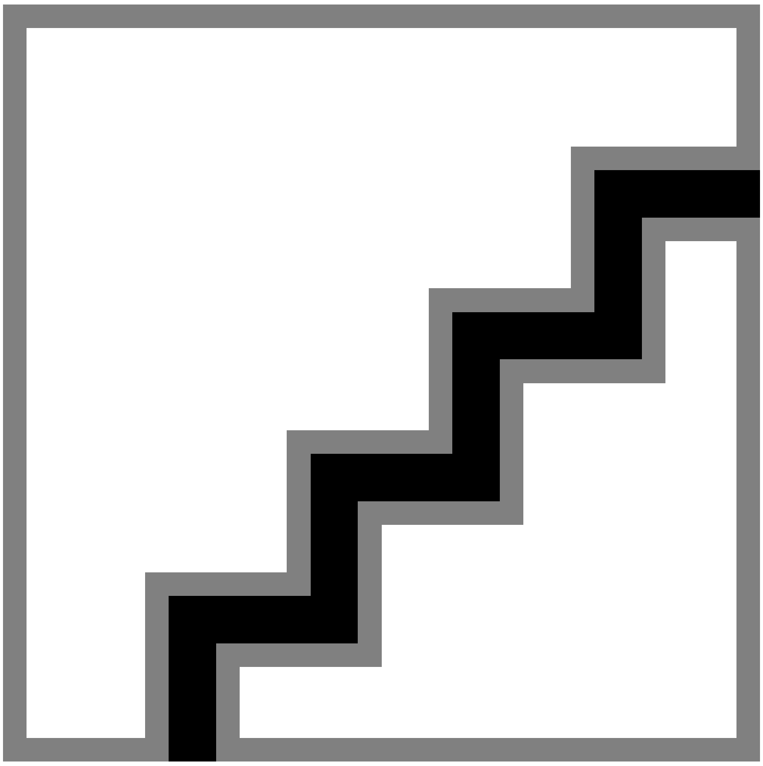


Figure 6-2 Select Network

Note

Disconnect the wired network before connecting a Wi-Fi.

2. Select **Next**.

Wired Network

Note

Make sure the device has connected to a network.

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

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

Wi-Fi

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

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

3. **Optional:** Select **Back** to skip network settings.

6.3 Access to Platform

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

Steps

1. Enable **Access to Hik-Connect**, and set the Server IP and Verification Code.
2. Tap **Next**.

6.4 Privacy Settings

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

Select parameters according to your actual needs.

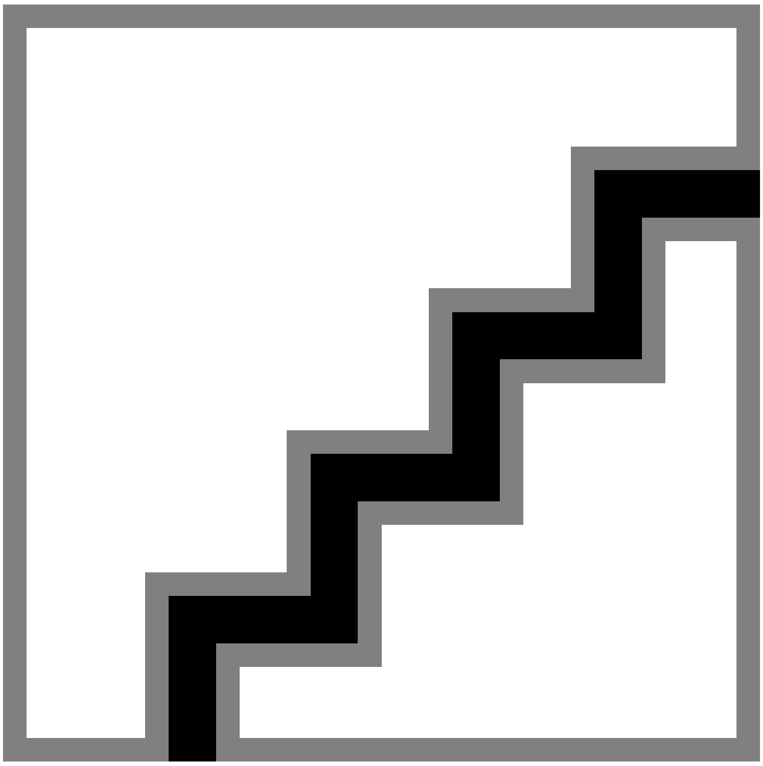


Figure 6-3 Privacy

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

Upload the pictures captured when authenticating to the platform automatically.

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

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

Save Registered Pic. (Save Registered Picture)

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

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

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

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

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

Select **Next** to complete the settings.

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 administrator's name (optional) and select **Next**.

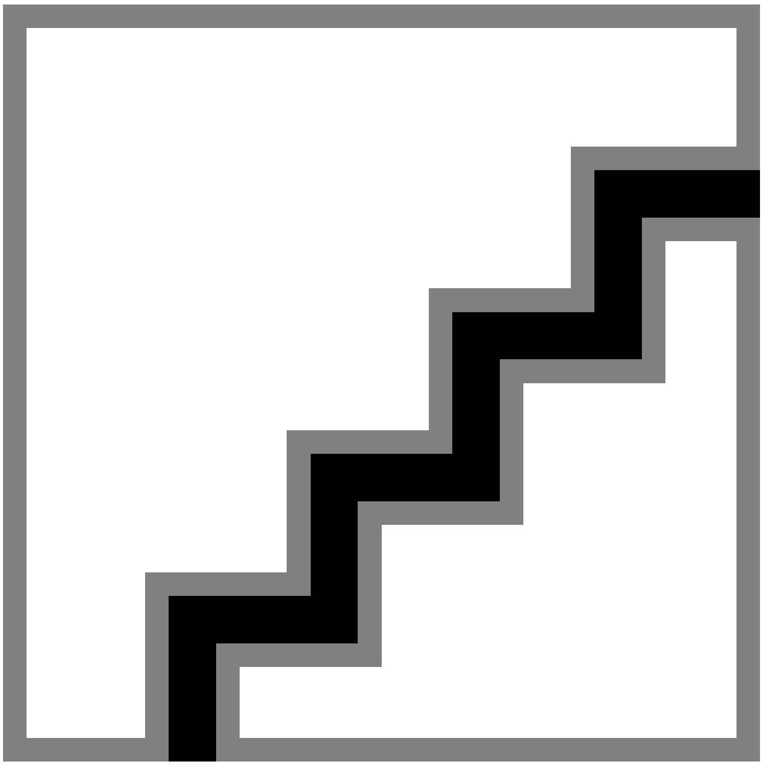


Figure 6-4 Add Administrator Page

2. Select a credential to add.

Note

Up to one credential should be added.

- : Face forward at the camera. Make sure the face is in the face recognition area. Press OK to capture and press OK to confirm.
- : Press your finger according to the instructions on the device screen. Press OK to confirm.
- : Enter the card No. or present card on the card presenting area. Press OK to confirm.

3. Press OK.

Chapter 7 Basic Operation

7.1 Login

Login the device to set the device basic parameters.

7.1.1 Login by Administrator

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

Steps

1. Long press OK to enter the admin login page.

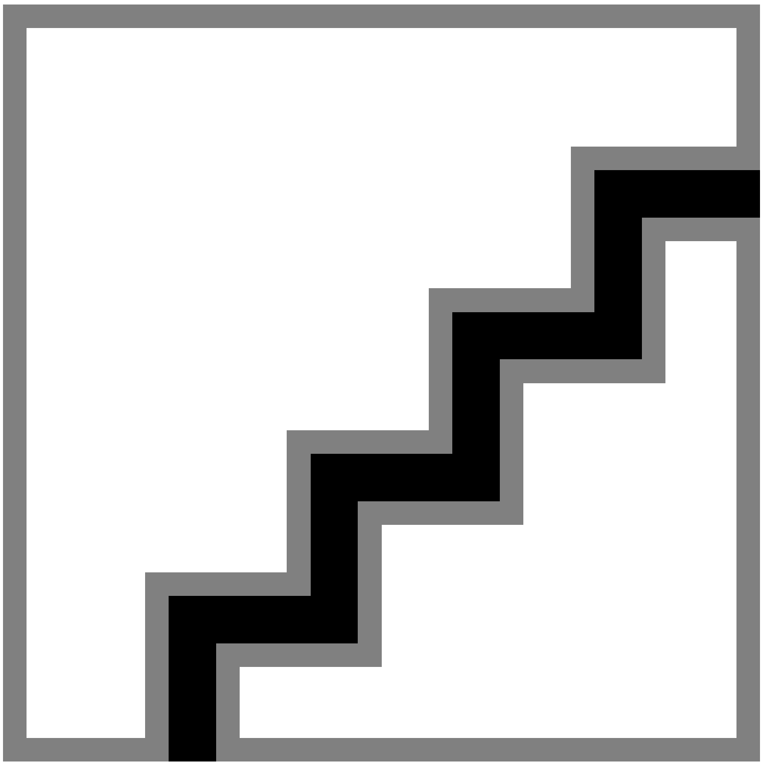


Figure 7-1 Admin Login

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

   Note

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

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

7.1.2 Login by Activation Password

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

Steps

1. Long 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.

7.1.3 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 **Basic → Comm.** (Communication) to enter the Communication settings page.
2. On the Communication page, select **Wired Network**.

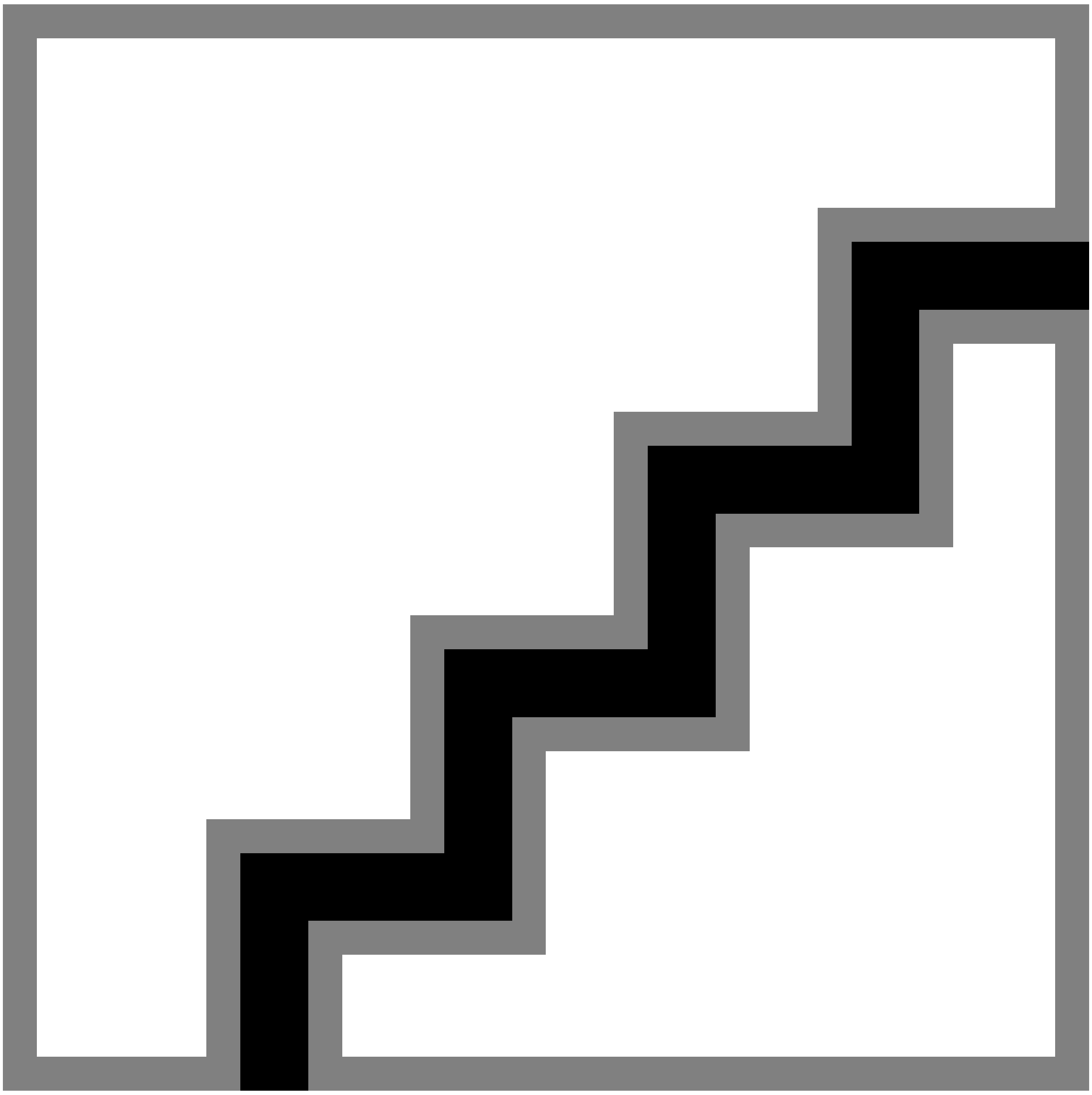


Figure 7-2 Wired Network Settings

3. Set IP Address, Subnet Mask, and Gateway.
   - Enable **DHCP**, and the system will assign IP address, subnet mask, and gateway automatically.
   - Disable **DHCP**, and you should set the IP address, subnet mask, and gateway manually.

   Note

   The device's IP address and the computer IP address should be in the same IP segment.
4. Set the DNS parameters. You can enable **Auto Obtain DNS**, set the preferred DNS server and the alternate DNS server.

7.2.2 Set Wi-Fi Parameters

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

Steps

Note

The function should be supported by the device.

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

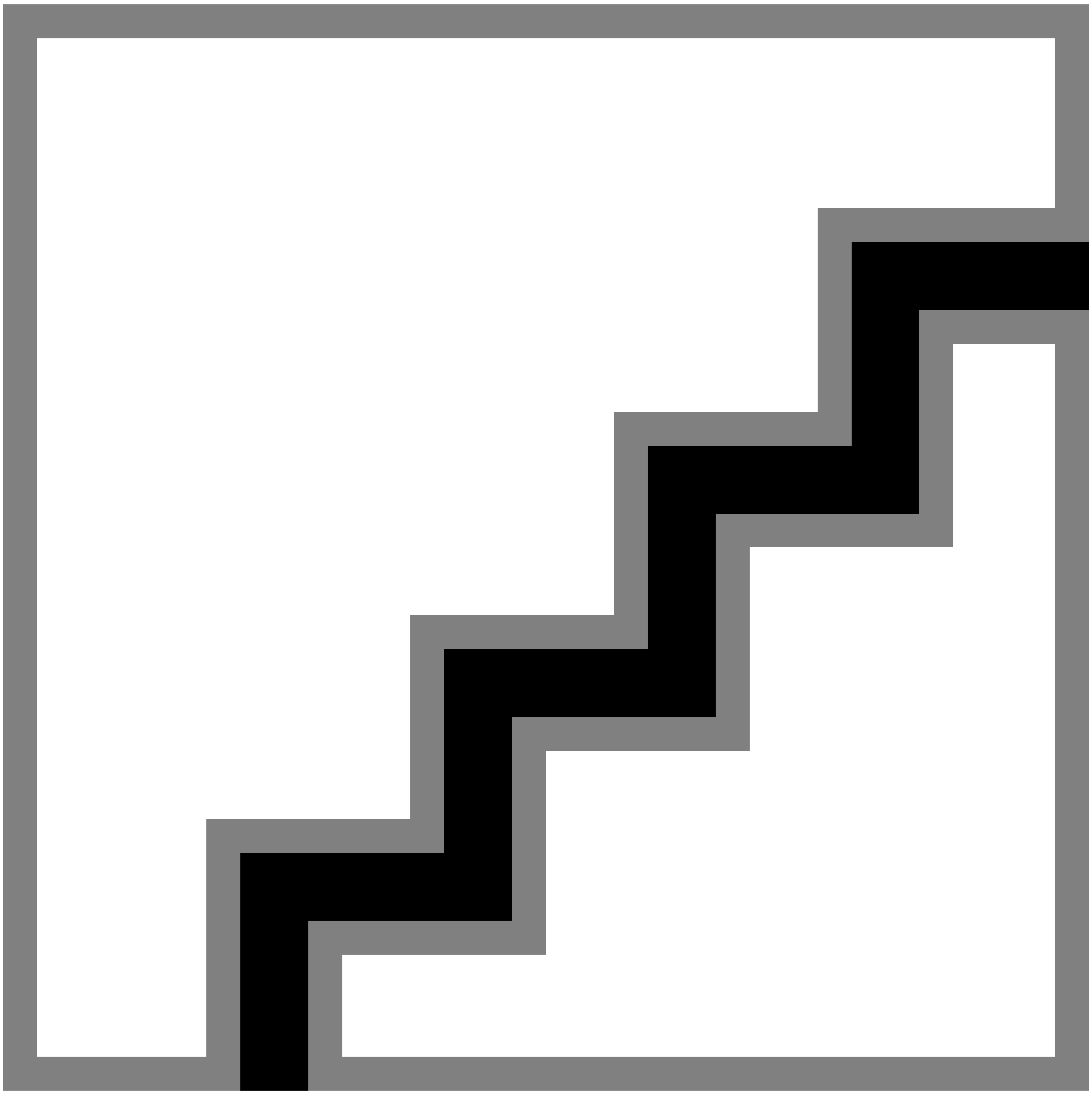


Figure 7-3 Wi-Fi Settings

3. Enable the Wi-Fi function.
4. Select a Wi-Fi from the list, and enter the Wi-Fi's password. Tap **OK**.

Note

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

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

7.2.3 Set ISUP Parameters

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

Before You Start

Make sure your device has connect to a network.

Steps

1. Select **Comm. → ISUP** .

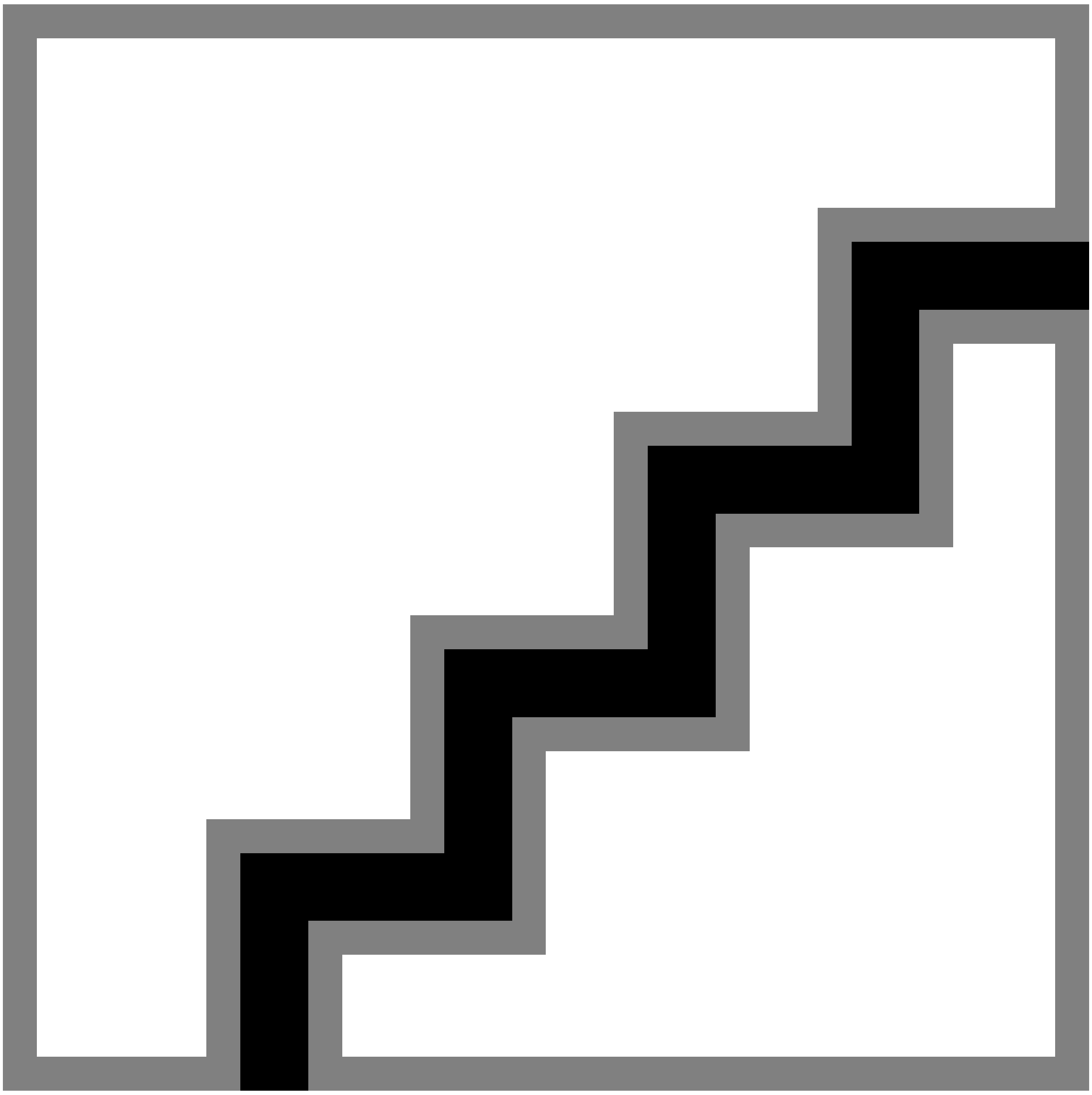


Figure 7-4 ISUP Settings

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

   ISUP Version

   Set the ISUP version according to your actual needs.

   Central Group

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

   Main Channel

   Support N1 or None.

   ISUP

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

Address Type

Select an address type according to your actual needs.

IP

Set the ISUP server's IP address.

Port

Set the ISUP server's port No.

Note

Port No. Range: 1 to 65535.

Device ID

Set device serial no.

ISUP Key

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

Note

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

7.2.4 Platform Access

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

Before You Start

Make sure your device has connected to a network.

Steps

1. Select **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**.

7.3 User Management

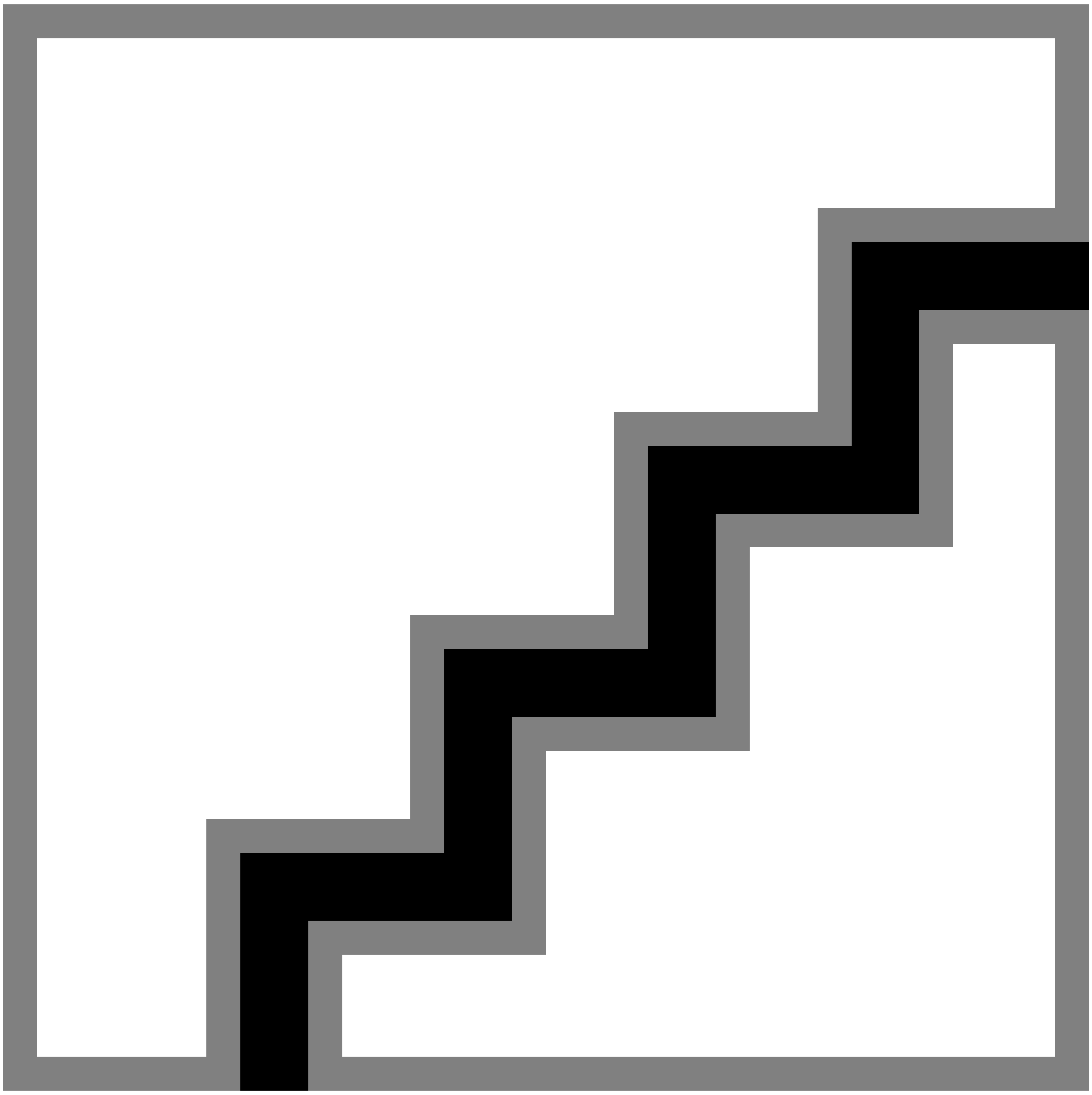
On the user management interface, you can add, edit, delete and search the user.

7.3.1 Add Administrator

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

Steps

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



3. Edit the employee ID.

Note

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

4. Select the Name field and input the user name on the keyboard.

   Note

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

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

   Note

   - For details about adding a face picture, see ***Add Face Picture*** .
   - **Note**

     For details about adding a fingerprint, see ***Add Fingerprint*** .
   - For details about adding a card, see ***Add Card*** .
   - For details about adding a password, see ***View PIN code*** .

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

   Note

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

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.

7.3.2 Add Face Picture

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

Steps

Note

Up to 500 face pictures can be added.

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

Note

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

4. Select the Name field and input the user name on the keyboard.

Note

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

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

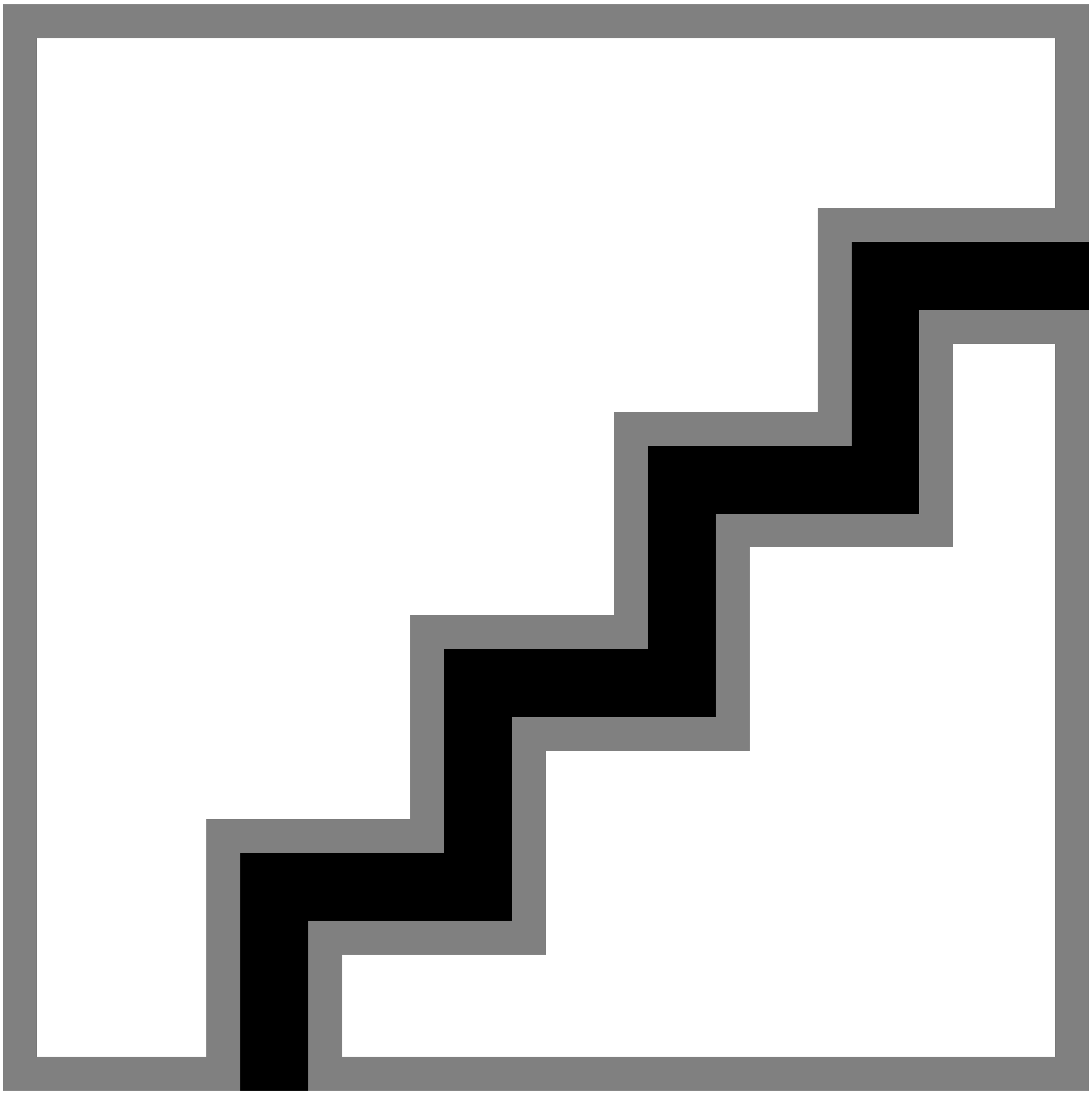


Figure 7-5 Add Face Picture

6. Look at the camera.

Note

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

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

7. Press OK to save the face picture.

8. **Optional:** Press ESC to select **Retake** and adjust your face position to add the face picture again.
9. Set the user role.

   Administrator

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

   Normal User

   The User is the normal user. The user can only authenticate or take attendance on the initial page.
10. Press ESC and then press OK to save the settings.

7.3.3 Add Fingerprint

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

Steps

Note

- The function should be supported by the device.
- Up to 1000 fingerprints can be added.

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

   Note

   - The employee ID should be less than 32 characters. And it can be a combination of lower letters, upper letters, and numbers.
   - The employee ID should not start with 0 and should not be duplicated.
4. Select the Name field and input the user name on the keyboard.

   Note

   - Numbers, upper case letters, lower case letters, and special characters are allowed in the user name.
   - The suggested user name should be within 128 characters.
5. Select the Fingerprint field to enter the Fingerprint page.
6. Follow the instructions to add a fingerprint.

   Note

   - The same fingerprint cannot be repeatedly added.
   - Up to 10 fingerprints can be added for one user.
   - You can also use the client software or the fingerprint recorder to record fingerprints.

For details about the instructions of scanning fingerprints, see ***Tips for Scanning Fingerprint*** .

7. Set the user role.

   Administrator

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

   Normal User

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

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

7.3.4 Add Card

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

Steps

Note

The device supports EM card or Mifare card. The supported card type varies between diffrerent models.

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

   Note

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

4. Select the Name field and input the user name on the keyboard.

   Note

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

5. Select the Card field and press OK to enter the Add Card page.
6. Configure the card No.
   - Enter the card No. manually.
   - Present the card over the card swiping area to get the card No.

Note

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

7. Configure the card type.
8. Set the user role.

   Administrator

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

   Normal User

   The User is the normal user. The user can only authenticate or take attendance on the initial page.
9. Press ESC and then press OK to save the settings.

7.3.5 View PIN code

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

Steps

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

   Note

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

   Note

   - Numbers, upper case letters, lower case letters, and special characters are allowed in the user name.
   - The suggested user name should be within 128 characters.
5. Select the PIN field to view the PIN code.

   Note

   The PIN code cannot be edited. It can only be applied by the platform.
6. Set the user role.

   Administrator

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

Normal User

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

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

7.3.6 Set Authentication Mode

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

Steps

1. Long press OK and login the device.
2. Select **User → Add User → Auth. Settings** .
3. Select Device or Custom as the authentication mode.

   Device

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

   Custom

   You can combine different authentication modes together according to your actual needs.
4. Press ESC to save the settings.

7.3.7 Edit User

After adding the user, you can edit it.

Edit User

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

Note

The employee ID cannot be edited.

7.4 Data Management

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

7.4.1 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.

7.4.2 Import Data

Steps

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

   Note

   The imported access control parameters are configuration files of the device.
4. Enter the created password when you exported the data. If you do not create a password when you exported the data, leave a blank in the input box and tap **OK** immediately.

   Note

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

7.4.3 Export Data

Steps

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

7.5 Identity Authentication

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

7.5.1 Authenticate via Single Credential

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

Authenticate face, fingerprint, card or PIN.

Face

Face forward at the camera and start authentication via face.

Fingerprint

Place the enrolled fingerprint on the fingerprint module and start authentication via fingerprint.

Card

Present the card on the card swiping area and start authentication via card.

Note

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

PIN Code

Enter the pin code to authenticate via PIN code.

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

7.5.2 Authenticate via Multiple Credential

Before You Start

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

Steps

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

   Note

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

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

   Note

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

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

7.6 Basic Settings

You can set the voice, time, sleeping (s), language, supplement light, community No., building No., and unit No.

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

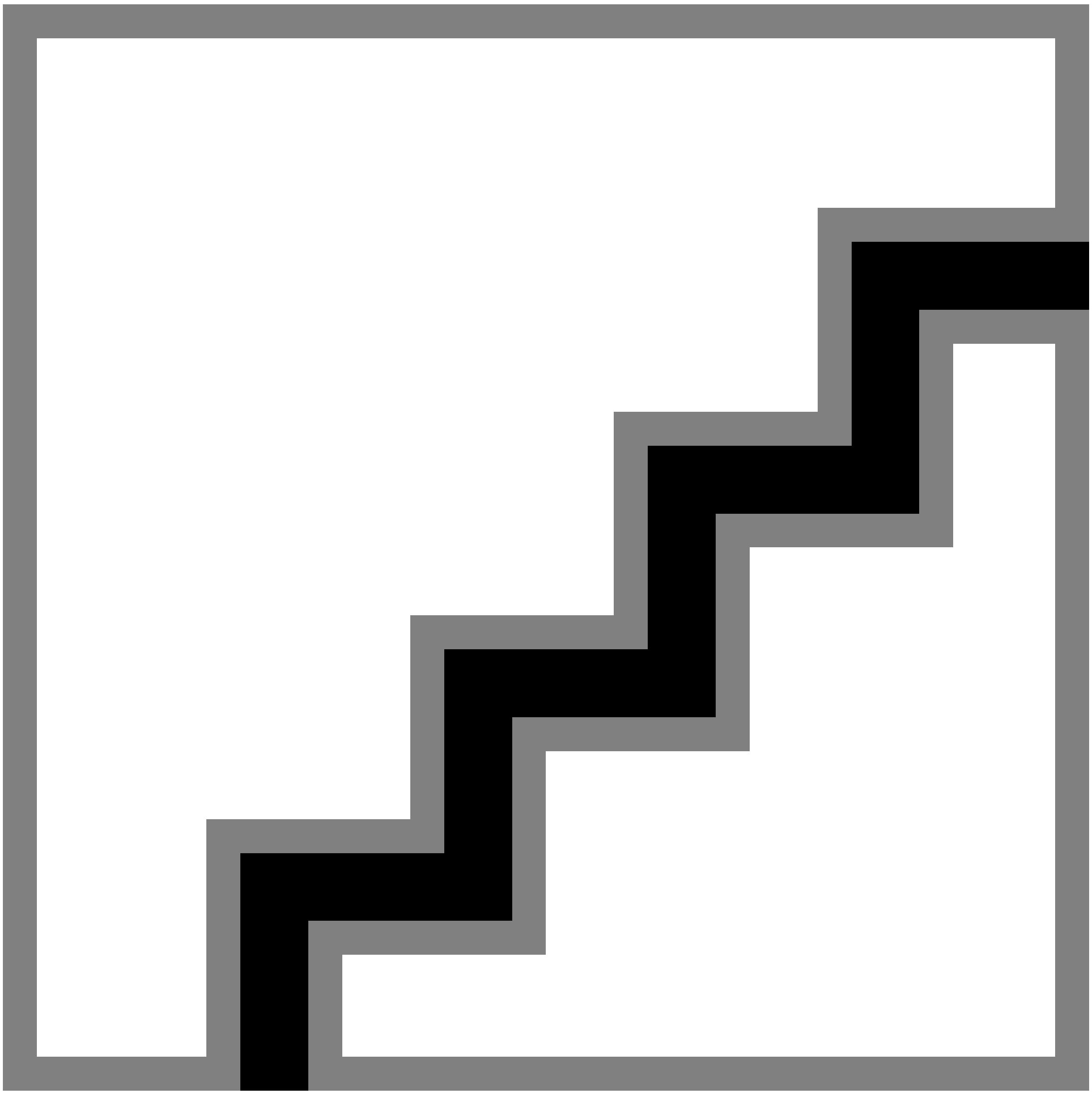


Figure 7-6 Basic Settings Page

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.

Community No.

Set the device installed community No.

Building No.

Set the device installed building No.

Unit No.

Set the device installed unit No.

7.7 Set Biometric Parameters

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

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

Table 7-1 Face Picture Parameters

Parameter	Description
Application Mode	Select either others or indoor according to actual environment.
Face Liveness Level	After enabling face anti-spoofing function, you can set the matching security level when performing live face authentication.
Face Recognition Distance	Set the valid distance between the user and the camera when authenticating.
Face Recognition Interval	The time interval between two continuous face recognitions when authenticating. **Note** You can input the number from 1 to 10.

Parameter	Description
Face 1:N Security Level	Set the matching threshold when authenticating via 1:N matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate.
Face 1:1 Security Level	Set the matching threshold when authenticating via 1:1 matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate.
Face with Mask Detection	After enabling the face with mask detection, the system will recognize the captured face with mask picture. You can set face with mask & face 1:1 level and 1:N level and the strategy. **Reminder of Wearing** If the person do not wear a face mask when authenticating, the device prompts a notification and the door will open. **Must Wear** If the person do not wear a face mask when authenticating, the device prompts a notification and the door keeps closed. **None** If the person do not wear a face mask when authenticating, the device will not prompt a notification.

7.8 Set Access Control Parameters

You can set the access control permissions, including the functions of authentication mode, enable NFC 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.

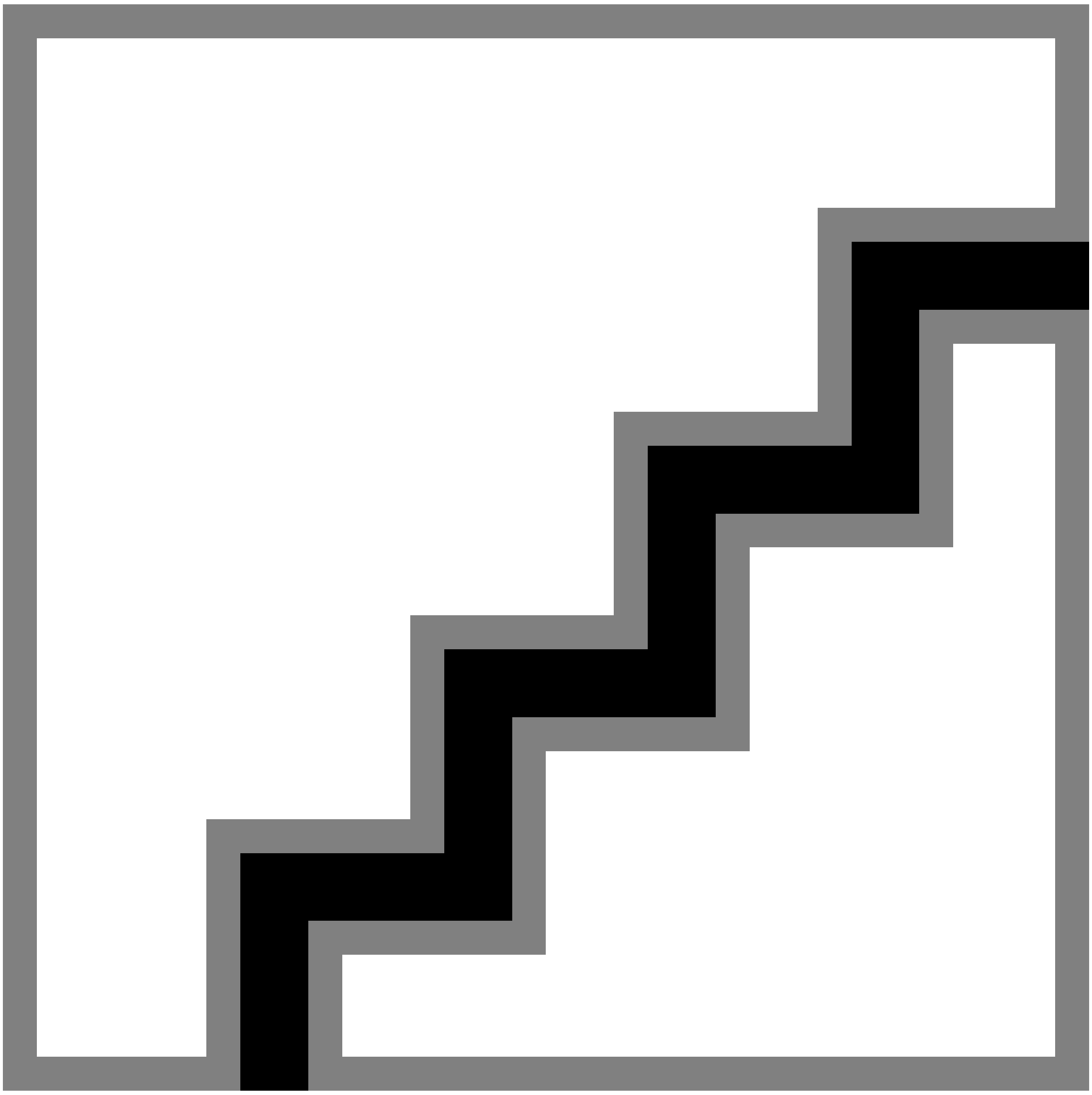


Figure 7-7 Access Control Parameters

The available parameters descriptions are as follows:

Table 7-2 Access Control Parameters Descriptions

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

Parameter	Description
	Note • Only the device with the fingerprint module supports the fingerprint related function. • Biometric recognition products are not 100% 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.
Enable NFC Card	Enable the function and you can present the NFC card to authenticate.
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.

7.9 Time and Attendance Status Settings

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

Note

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

7.9.1 Disable Attendance Mode via Device

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

Select **T&A** to enter the T&A Status page.

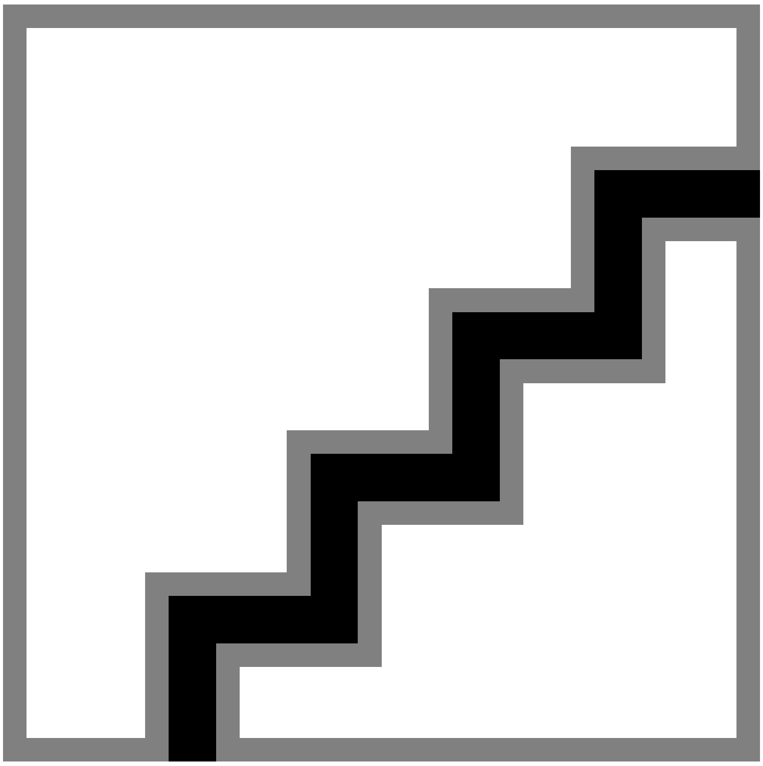


Figure 7-8 Disable Attendance Mode

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.

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

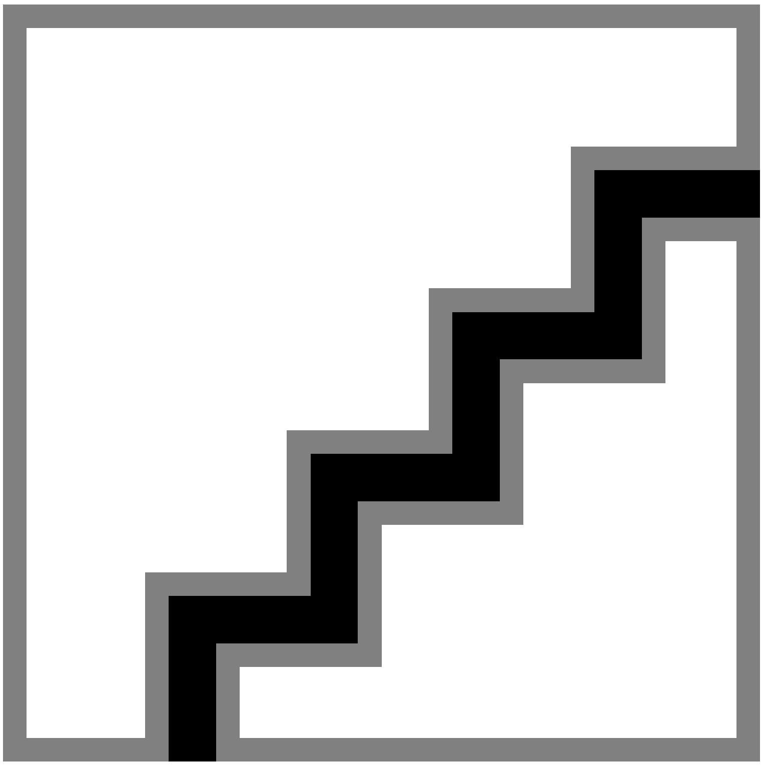


Figure 7-9 Manual Attendance Mode

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.

7.9.3 Set Auto Attendance via Device

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

Before You Start

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

Steps

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

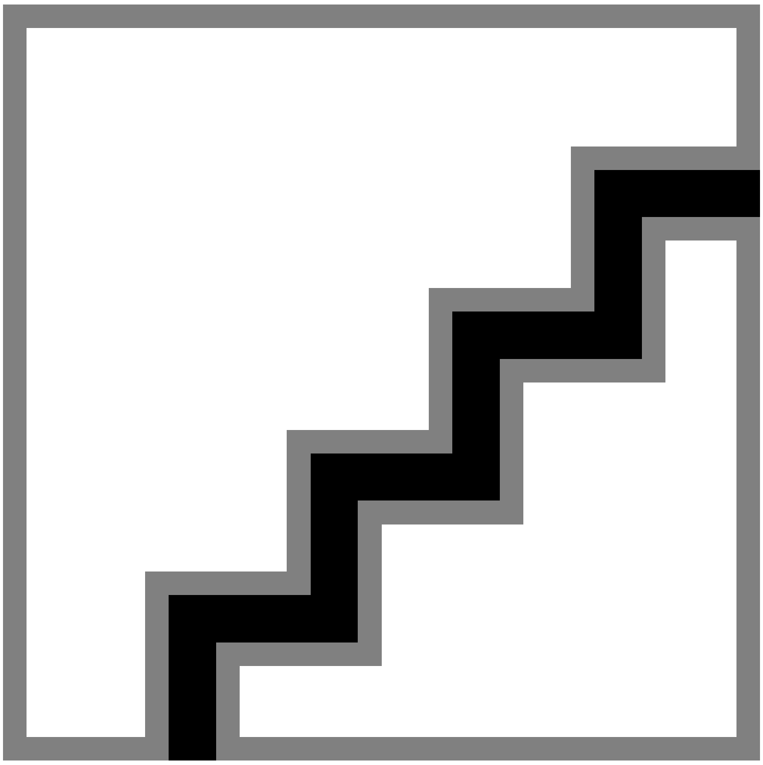


Figure 7-10 Auto Attendance Mode

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.

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

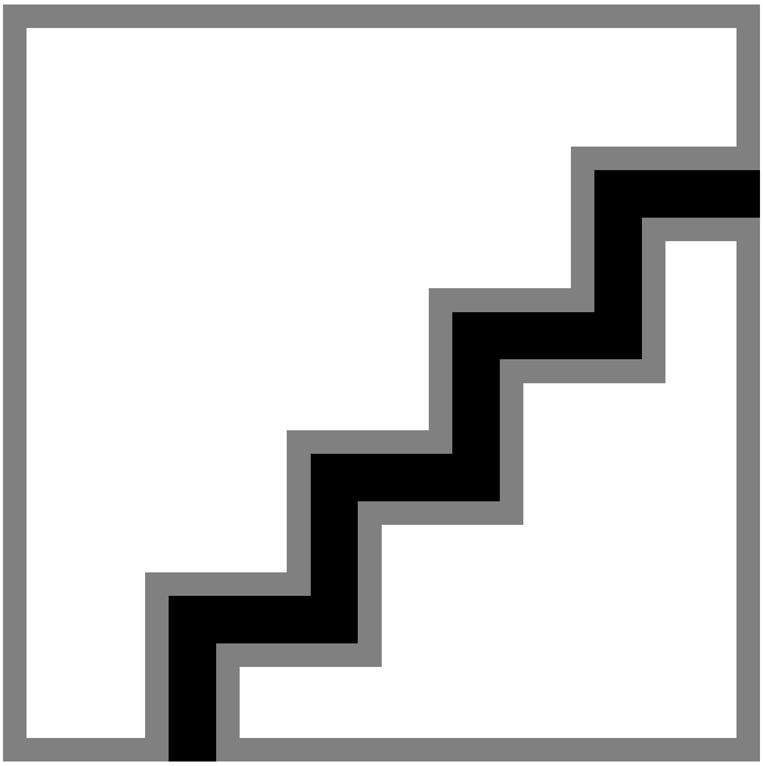


Figure 7-11 Manual and Auto Mode

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.

7.10 System Maintenance

You can view the device system information and capacity. You can also upgrade device, 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.

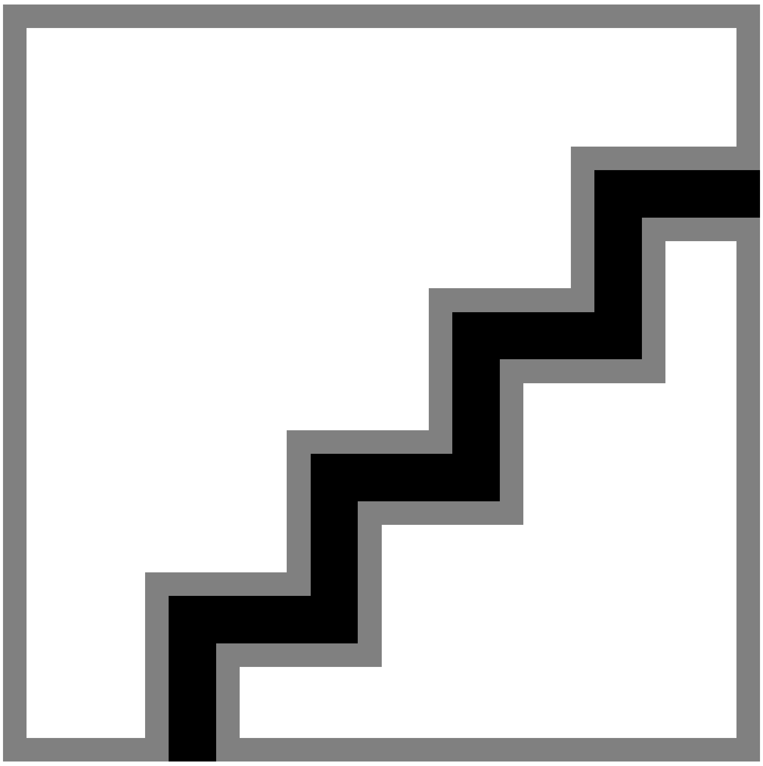


Figure 7-12 Maintenance Page

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, and event.

Note

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

Device Upgrade

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

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 💡 , long press OK, and enter admin password to view device version 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.

Obtain the IP address from the device after Wi-Fi is enabled. Make sure the IP segment of the device and the computer is the same. For details, refers to ***Set Wi-Fi Parameters*** .

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 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.

8.3 User Management

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

Steps

1. Tap **User** to enter the settings page.
2. Add user.
   1) Tap**+**.

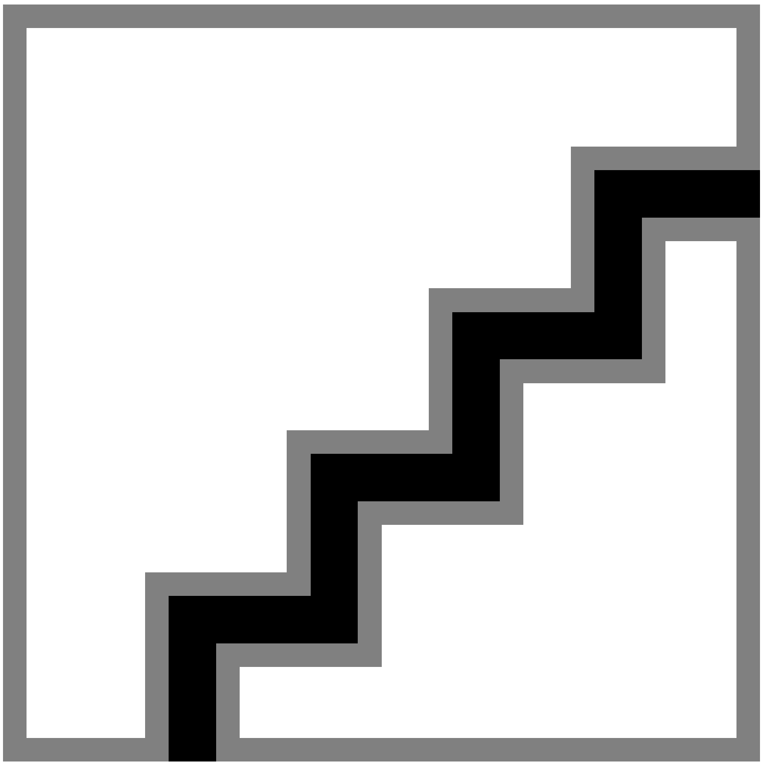


Figure 8-1 Add User

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

Gender

Select the gender.

User Role

Select your user role.

Floor No./Room No.

Enter the floor No./room No.

Face

Add Face picture. Tap **Face**, then tap **Import**, and select the mode to import the face.

Card No.

Enter the card No.

Fingerprint

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

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**.

Authentication Type

Set the authentication type.

3) Tap **Save**.

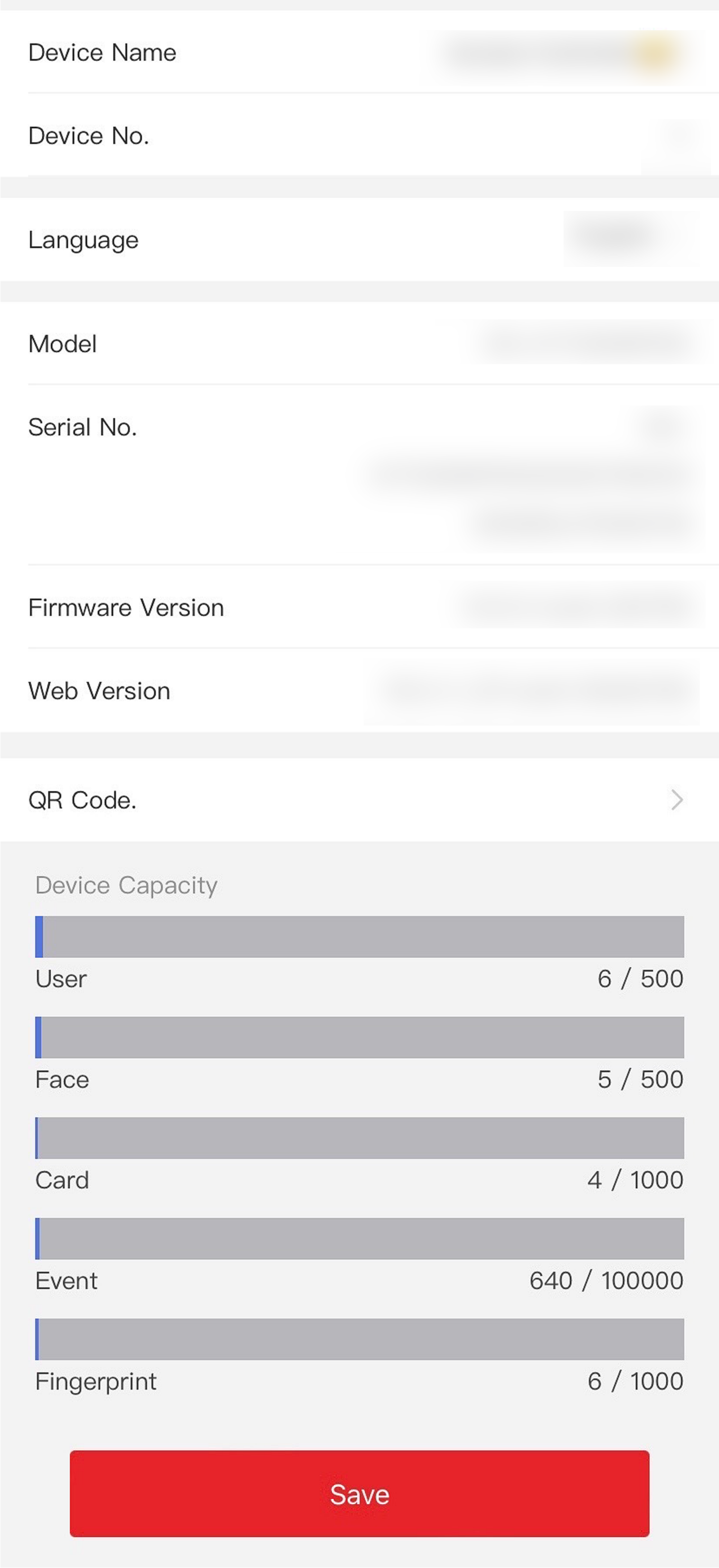
3. Tap the user that needs to be edited in the user list to edit the information.
4. Tap the user that needs to be deleted in the user list, and tap 🗑 to delete the user.
5. You can search the user by entering the employee ID or name in the search bar.

8.4 Configuration

8.4.1 View Device Information

You can view the device name, device No., language, model, serial No., version, device capacity, etc.

Tap **Configuration → System → System Settings → Basic Information** , to enter the settings page.



Device Name [redacted]

Device No. [redacted]

Language [redacted]

Model [redacted]

Serial No. [redacted]

Firmware Version [redacted]

Web Version [redacted]

QR Code.

Device Capacity

User	6 / 500
Face	5 / 500
Card	4 / 1000
Event	640 / 100000
Fingerprint	6 / 1000

Figure 8-2 Device Information

You can view the device name, device No., language, model, serial No., version, device capacity, etc.

8.4.2 Time Settings

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

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

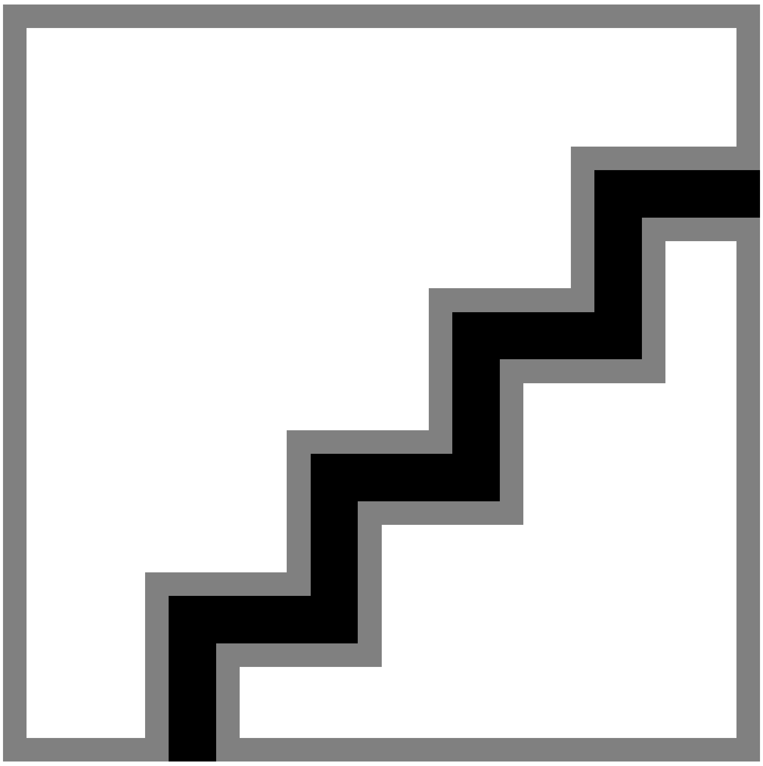


Figure 8-3 Time Settings

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.

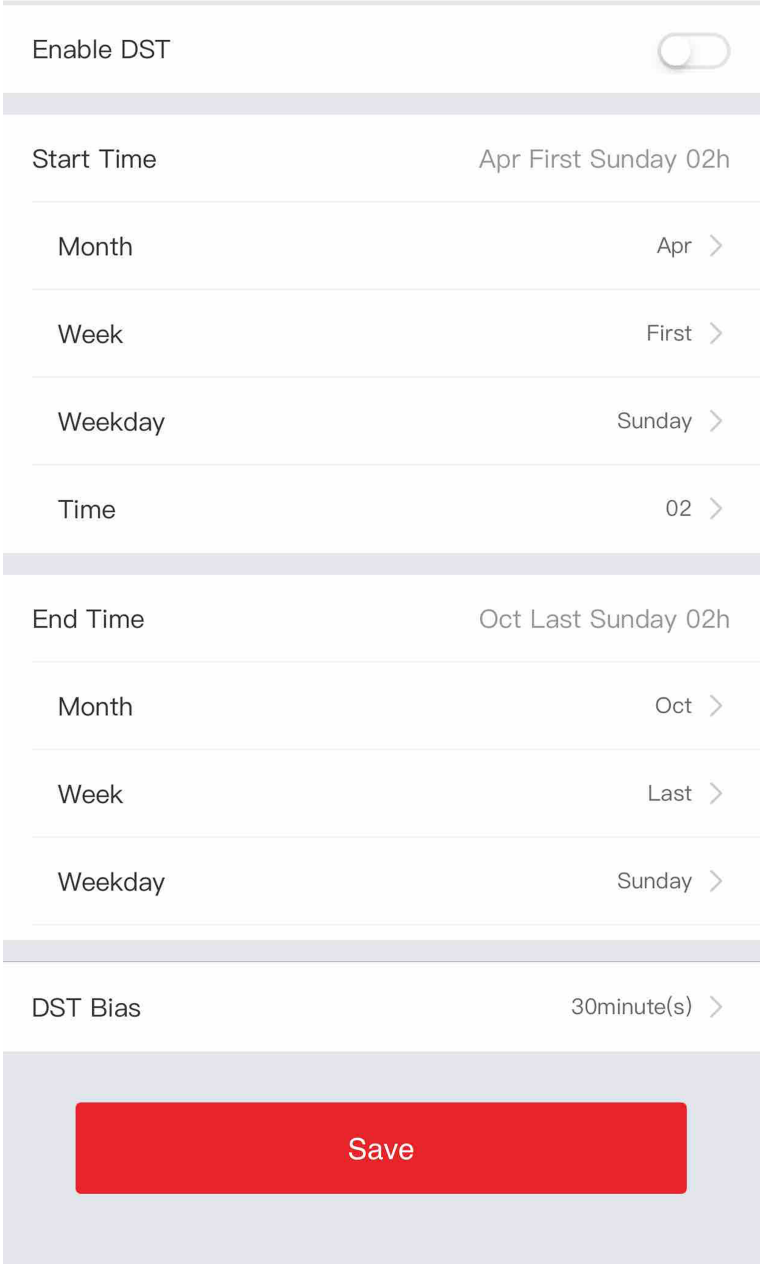
NTP

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

8.4.3 Set DST

Steps

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



Enable DST

Start Time Apr First Sunday 02h

Month Apr

Week First

Weekday Sunday

Time 02

End Time Oct Last Sunday 02h

Month Oct

Week Last

Weekday Sunday

DST Bias 30minute(s)

Figure 8-4 DST

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

8.4.4 View Open Source Software License

Tap **Configuration → System → System Settings → About** , and tap **View Licenses** to view the device license.

8.4.5 User Management

Steps

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

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.

8.4.6 Upgrade and Maintenance

Reboot device, restore device parameters, upgrade device version and unlink the app.

Reboot Device

Tap **Configuration → System → Maintenance** .
Tap **Reboot** to reboot the device.

Upgrade

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

Note

Do not power off during the upgrading.

Restore Parameters

Tap **Configuration → System → Maintenance** .

Default

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

Restore All

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

Unlink

Tap **Configuration → System → Maintenance** .
Tap **Unlink** to unlink the app.
After unlinking APP account, you cannot operate via APP.

8.4.7 Security Settings

You can set the SSH and HTTP according to actual needs.

Tap **Configuration → System → Security** , to enter the settings page.

Check **Enable** to enable SSH.

Check **Enable** to enable HTTP.

8.4.8 Network Settings

You can set the port and Wi-Fi parameters.

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 **Configuration → Network → Basic Settings → Wi-Fi** to enter the settings page.
2. Check **Enable Wi-Fi**.

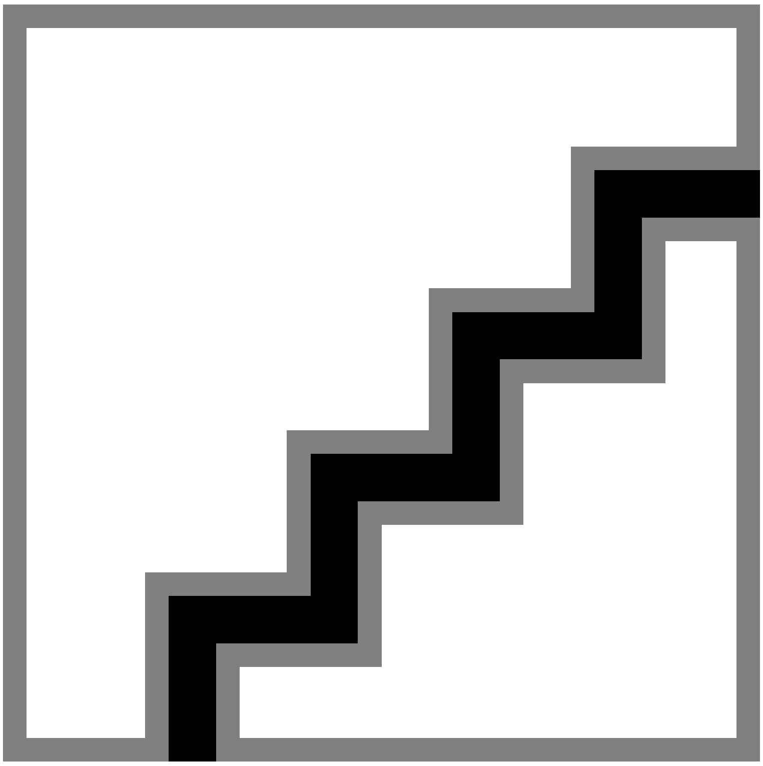
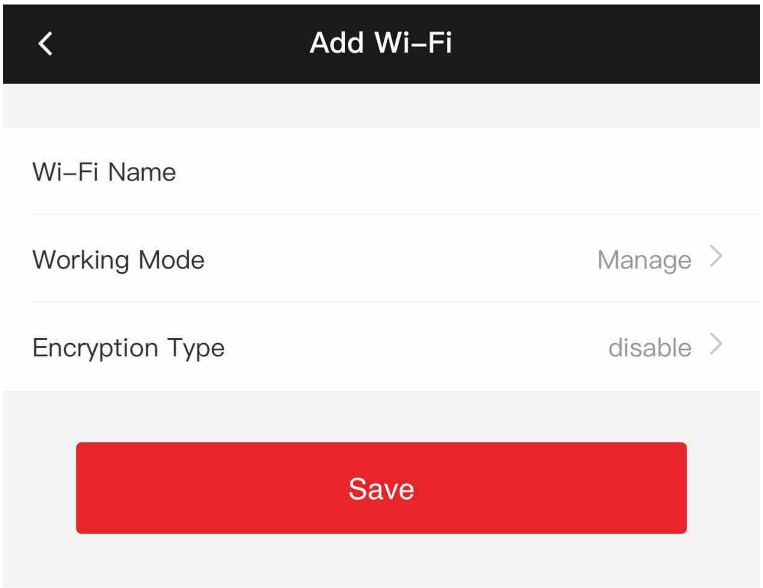


Figure 8-5 Wi-Fi

3. Add Wi-Fi.
    1) Tap **+**.



Add Wi–Fi

Wi–Fi Name

Working Mode Manage

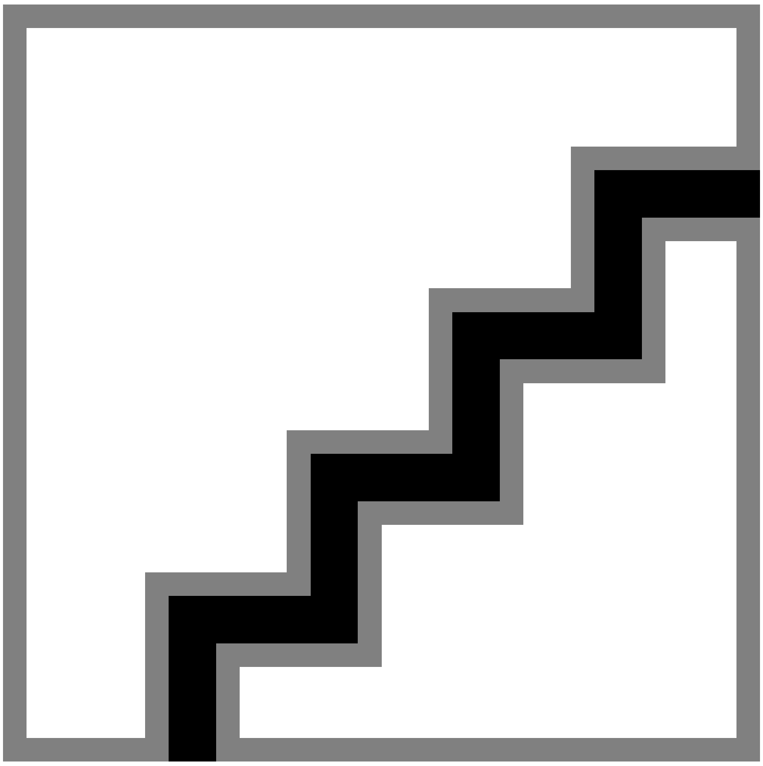
Encryption Type disable

Figure 8-6 Add Wi-Fi

2) Enter **Wi-Fi Name** and **Wi-Fi Password**, and select **Working Mode** and **Encryption Type**.

3) Tap **Save**.

4. Select the Wi-Fi name, and tap **Connect**.
5. Enter the password and tap **Save**.
6. Set WLAN parameters.



1) Set the IP address, subnet mask, and gateway. Or enable DHCP and the system will allocate the IP address, subnet mask, and gateway automatically.
2) Set the DNS parameters. You can enable Auto Obtain DNS, set the preferred DNS server and the alternate DNS server.
3) Tap **Save**.

Set Port Parameters

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

Tap **Configuration → Network → Basic Settings → Port** , to enter the setting page.

HTTP

It refers to the port through which the browser accesses the device.

RTSP

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

HTTPS

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

Server

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

Platform Access

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

Steps

1. Tap **Configuration → Network → Advanced → 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. Enter the server address and stream encryption.

   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.

4. You can view **Register Status** and **Device QR Code**.
5. 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 **Configuration → Network → Advanced → ISUP** .
2. Check **Enable**.
3. Set the ISUP version, IP Address, Port, and Account.

   Note

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

4. Set the Center Group.

   Center Group

   Select a center group from the drop-down list.

   Main Channel/Backup Channel

The device will communicate with the center via the main channel. When exception occurs in the main channel, the device and the center will communicate with each other via the backup channel.

5. Tap **Save** to save the settings.

HTTP Listening

You can set the HTTP listening parameters.

Steps

1. Tap **Configuration → Network → Advanced → HTTP Listening** .
2. Edit the destination IP or domain name, URL and port.
3. **Optional:** Tap **Default** to reset the destination IP or domain name.
4. Tap **Save**.

8.4.9 General Settings

Set Authentication Parameters

Set Authentication Parameters.

Steps

1. Tap **Configuration → General Settings → Authentication Settings** .

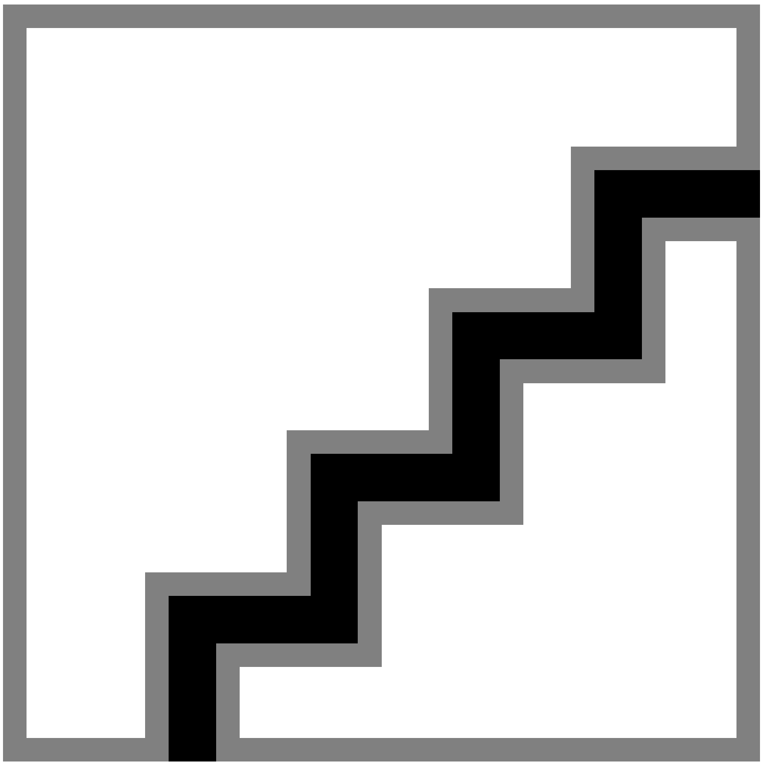


Figure 8-7 Authentication Settings

2. Tap **Save**.

   Device Type

   Main Card Reader

   You can configure the device card reader's parameters. If you select main card reader, you need to configure the following parameters: **Card Reader Type**, **Card Reader Description**, **Enable Card Reader**, **Authentication**, **Recognition Interval (s)**, **Minimum Card Swiping Interval (s)**, **Max. Authentication Failed Attempts Alarm/Alarm of Max. Failed Attempts**, **Enable Tampering Detection** and **Enable Card No. Reversing**.

   Card Reader Type

   Get card reader type.

   Card Reader Description

   Get card reader description. It is read-only.

   Enable Card Reader

   Enable the card reader's function.

   Authentication

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

   Recognition Interval

If the interval between card presenting of the same card is less than the configured value, the card presenting is invalid. The interval time range is from 0 to 255 seconds (When set to 0, it means that recognition interval is not enabled, and the same authentication can be used for unlimited times).

Authentication Interval

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

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

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

Enable Tampering Detection

Enable the anti-tamper detection for the card reader.

Enable Card No. Reversing

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

Set Privacy Parameters

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

Tap **Configuration → General Settings → Privacy** .

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

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

Check Face Picture, Name, or Employee ID. 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.

ID De-identification

The ID information is desensitized with an asterisk.

Picture Uploading and Storage

You can upload and store pictures.

Upload Captured Picture When Authenticating

Upload the pictures captured when authenticating to the platform automatically.

Save Captured Picture When Authenticating

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

Save Registered Picture

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

Upload Picture After Linked Capture

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

Save Pictures After Linked Capture

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

Clear All Pictures in Device

You can clear registered face pictures and captured pictures in device.

Clear Registered Face Pictures

Select **Face Picture**, and tap **Clear**. All registered pictures in the device will be deleted.

Clear Authentication/Captured Picture

Select **Authentication/Captured Picture**, and tap **Clear**. All authentication/captured pictures in the device will be deleted.

Set Card Security

Tap **Configuration → General Settings → Card Security** to enter the settings page.

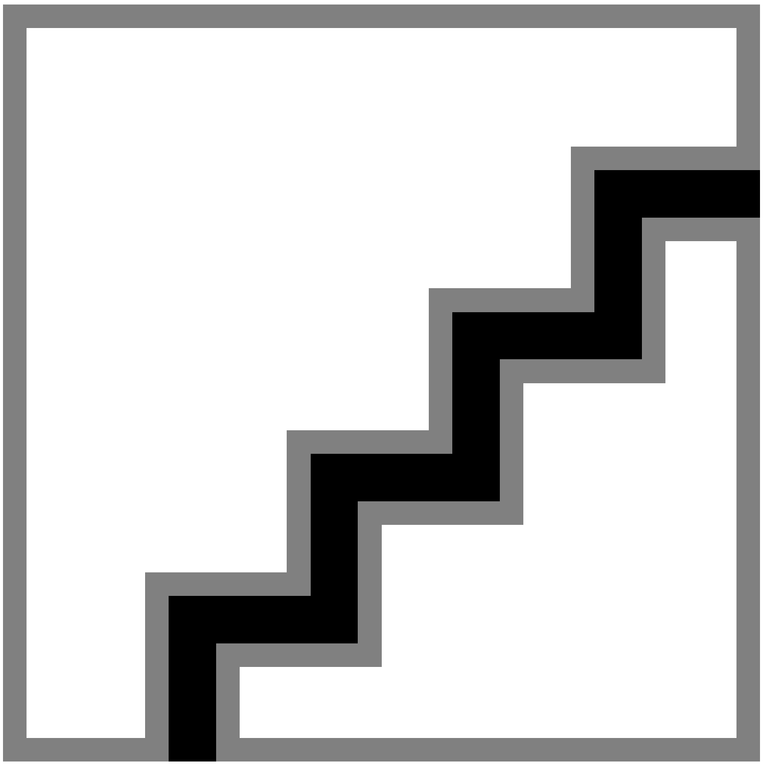


Figure 8-8 Card Security

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

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

Set Card Authentication Parameters

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

Tap **Configuration → General Settings → Card Authentication Settings** .

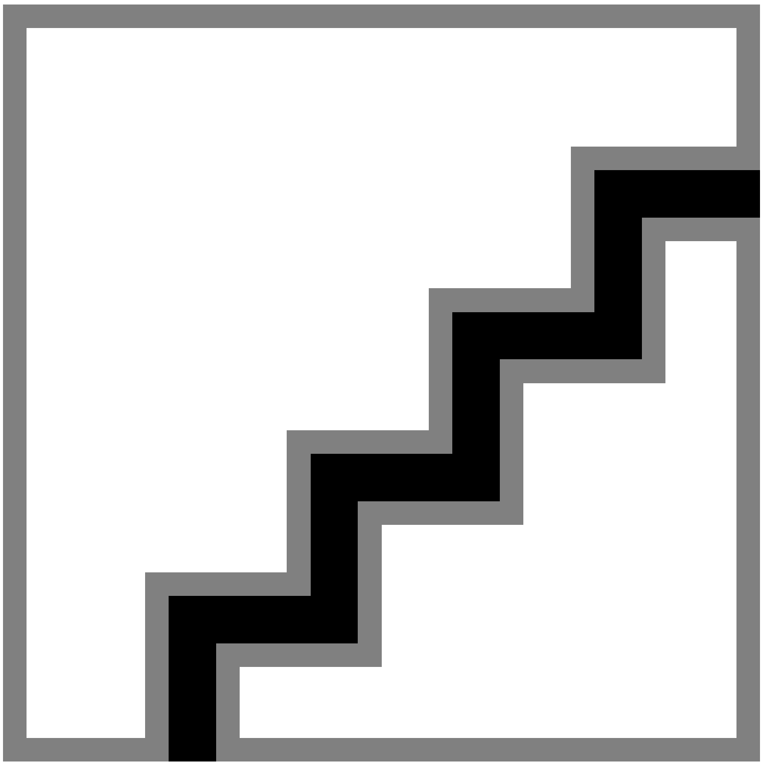


Figure 8-9 Card Authentication Page

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

Full Card No.

All card No. will be read.

Wiegand 26 (3 bytes)

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

Wiegand 34 (4 bytes)

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

8.4.10 Face Parameters Settings

Set face parameters.

Face Parameters Settings

Tap **Configuration → Smart → Intelligent Parameter** .

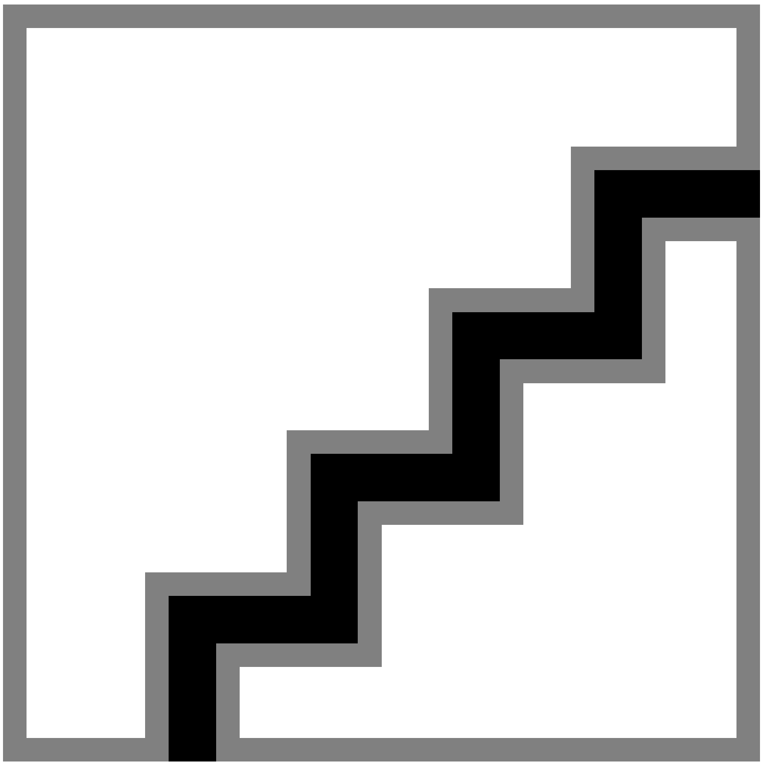


Figure 8-10 Face Parameters

Note

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

Set Face Parameters.

Face Anti-spoofing

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

Live Face Detection Security Level

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

Recognition Distance

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

Application Mode

Select **Indoor** or **Others** according to actual environment. In the outdoor scene, indoor scene near the window, or bad environment, you can choose **Others**.

Note

If the device is not activated by other tools, the device uses indoor as the environment mode by default.

Face Recognition Mode

Normal Mode

The device uses a camera to perform face recognition.

The device uses a camera to perform face recognition.

Continuous Face Recognition Interval (s)

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

Note

Value Range: 1 to 10.

1:1 Matching Threshold

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

1:N Matching Threshold

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

Face Recognition Timeout Value (s)

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

Face with Mask Detection

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

None

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

Reminder of Wearing

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

Must Wear

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

Face with Mask & Face (1:1)

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

Face with Mask 1:N Matching Threshold

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

Fingerprint Security Level

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

Set Recognition Area

Tap **Configuration → Smart → Area Configuration** to enter the page.
Drag the blue frame in the live video to adjust the recognition area. Only the face within the area can be recognized by the system.
Drag the slider to configure the effective area of face recognition.
Tap **Save** to save the settings.

8.4.11 Access Control Settings

Set Door Parameters

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

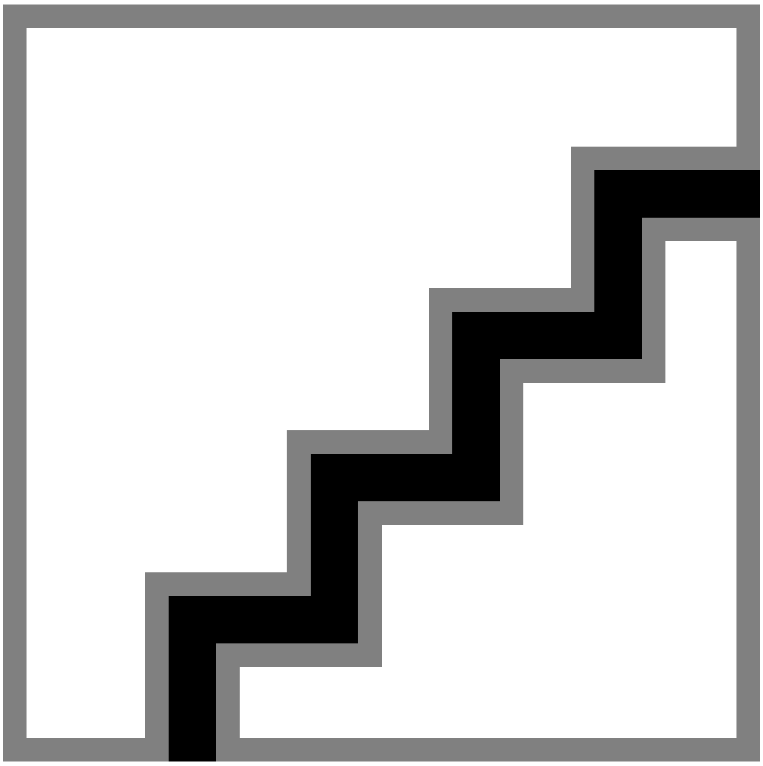


Figure 8-11 Door Parameters Settings Page

Tap **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. And the digit ranges from 4 to 8.

8.5 Door Operation

You can operate the door remotely via mobile web.

Tap **Door Operation** to enter the operation page.

Tap 🔓 to open the door.

Tap 🔒 to close the door.

Tap ▣ to set the door to remain open.

Tap ▣ to set the door to remain closed.

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.

Click **Next** to complete the settings.

9.2 Time Settings

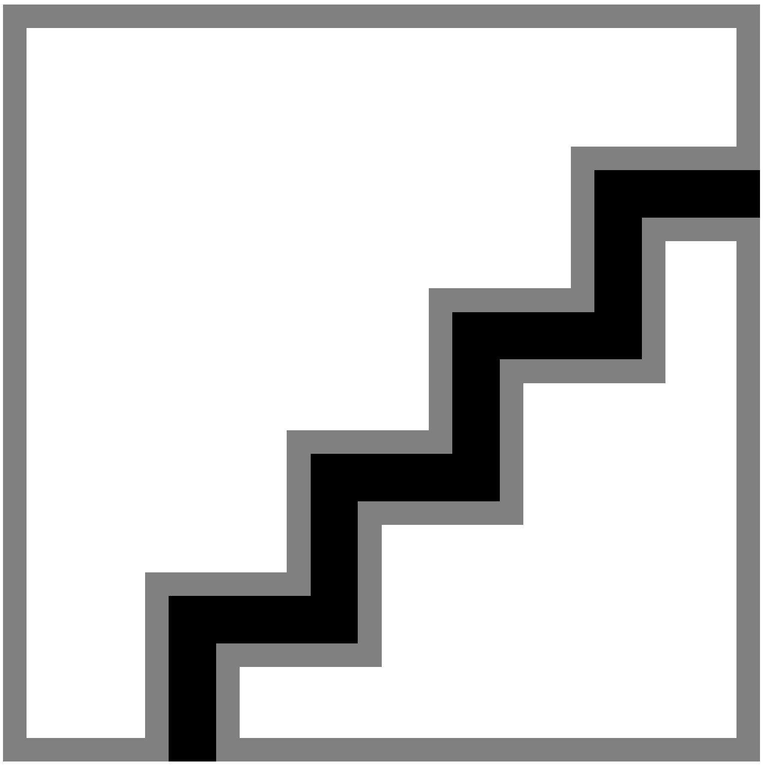


Figure 9-1 Set Time and DST

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

Time Zone

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

Time Sync.

NTP

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

Manual

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

Server Address/NTP Port/Interval

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

DST Settings

Check DST to enable DST settings.

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

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

9.3 Environment Settings

After activating the device, you should select an application mode for better device application.

Steps

1. Click ◁ in the top right of the web page to enter the wizard page. After setting device language and time, you can click **Next** to enter the **Environment Settings** page.
2. Select **Indoor** or **Other**.

Note

- If you install the device indoors near the window or the face recognition function is not working well, select **Others**.
- If you do not configure the application mode and tap **Next**, the system will select **Indoor** by default.
- If you activate the device via other tools remotely, the system will select **Indoor** as the application mode by default.

Click **Next** to save the settings and go to the next paramater. Or click **Skip** to skip environment settings.

9.4 Privacy Settings

Set the picture uploading and storage parameters.

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

Picture Uploading and Storage

Save Picture When Authenticating

Save picture when authenticating automatically.

Upload Picture When Authenticating

Upload the pictures when authenticating to the platform automatically.

Save Registered Picture

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

Upload Picture After Linked Capture

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

Save Pictures After Linked Capture

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

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

9.5 Administrator Settings

Steps

1. Click ◁ in the top right of the web page to enter the wizard page. After setting device language, time, environment and privacy, you can click **Next** to enter the **Administrator Settings** page.
2. Enter the employee ID and name of the administrator.
3. Select a credential to add.

   Note

   You should select at least one credential.

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

      Note

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

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

      Note

      Up to 5 cards can be supported.

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

      Note

      Up to 10 fingerprints are allowed.

   Click **Complete** to complete the settings.

Chapter 10 Operation via Web Browser

10.1 Login

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

Note

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

Login via Web Browser

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

Login via Remote Configuration of Client Software

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

10.2 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 Live View

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

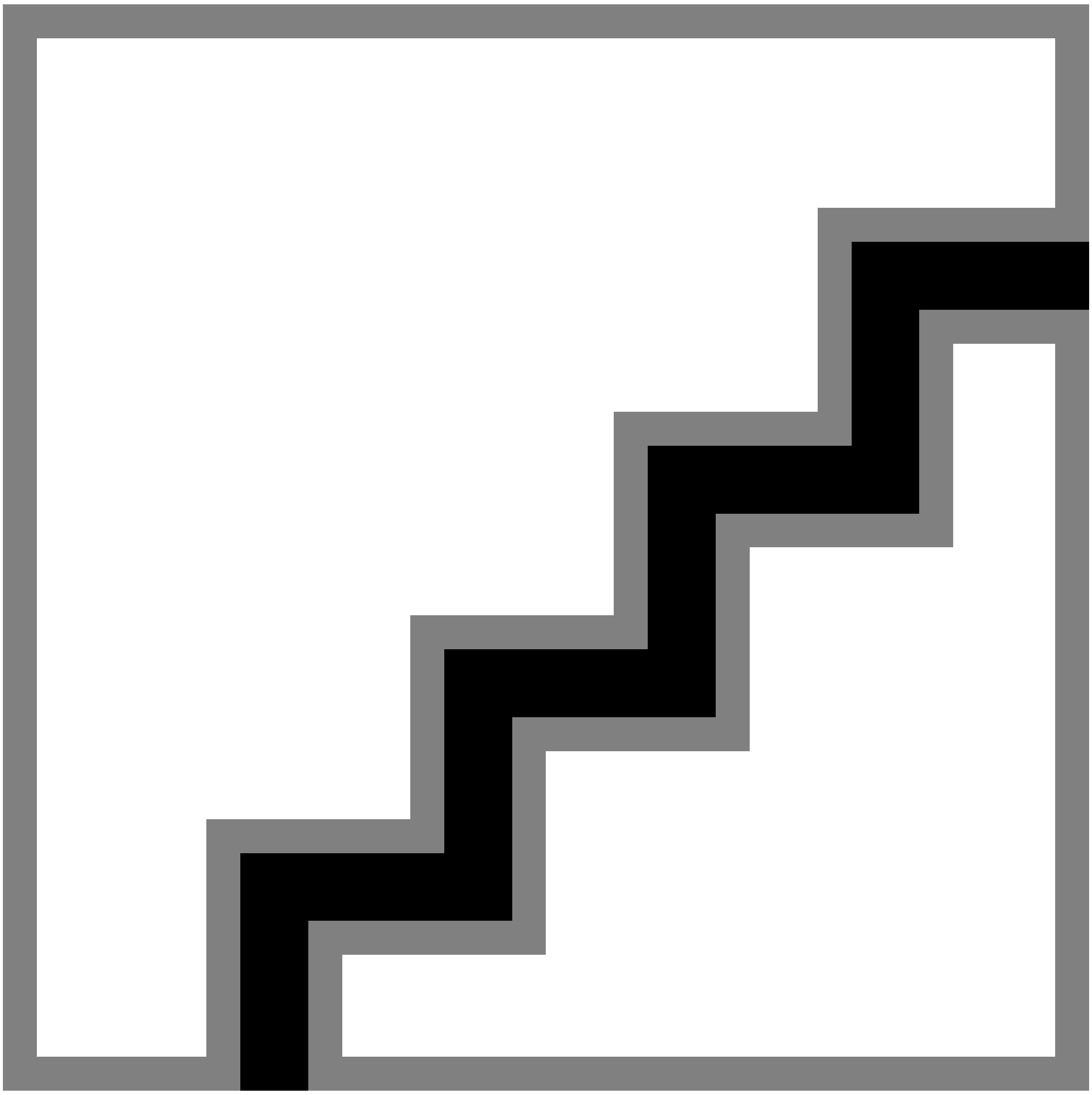


Figure 10-1 Live View Page

Function Descriptions:

Door Status

Click ▶ to view the device live view.

🔊

Set the volume when starting live view.

Note

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

📷

You can capture image when starting live view.

① ②

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

⛶

Full screen view.

🔓 / 🔒 / ▯ / ▯

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

Controlled Status

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

Real-Time Event

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

Person Information

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

Network Status

You can view the connected and registered status of wired network, wireless network, ISUP and cloud service.

Basic Information

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

Device Capacity

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

View More

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

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, the gender, and person type.
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.

Set Room No.

Click **Person Management → Add** to enter the Add Person page.
Click **Add** to add the **Floor No.** and **Room No.**.
Click 🗑 to delete it.
Click **Save** to save the settings.

Authentication Settings

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

Add Card

Click **Person Management → Add** to enter the Add Person page.
Click **Add Card**, enter the **Card No.** and select the **Property**, and click **Save** 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 Face Picture

Click **Person Management → Add** to enter the Add Person page.
Click **+** on the right to upload a face picture from the local PC.

Note

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

Click **Save** to save the settings.

10.5 Search Event

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

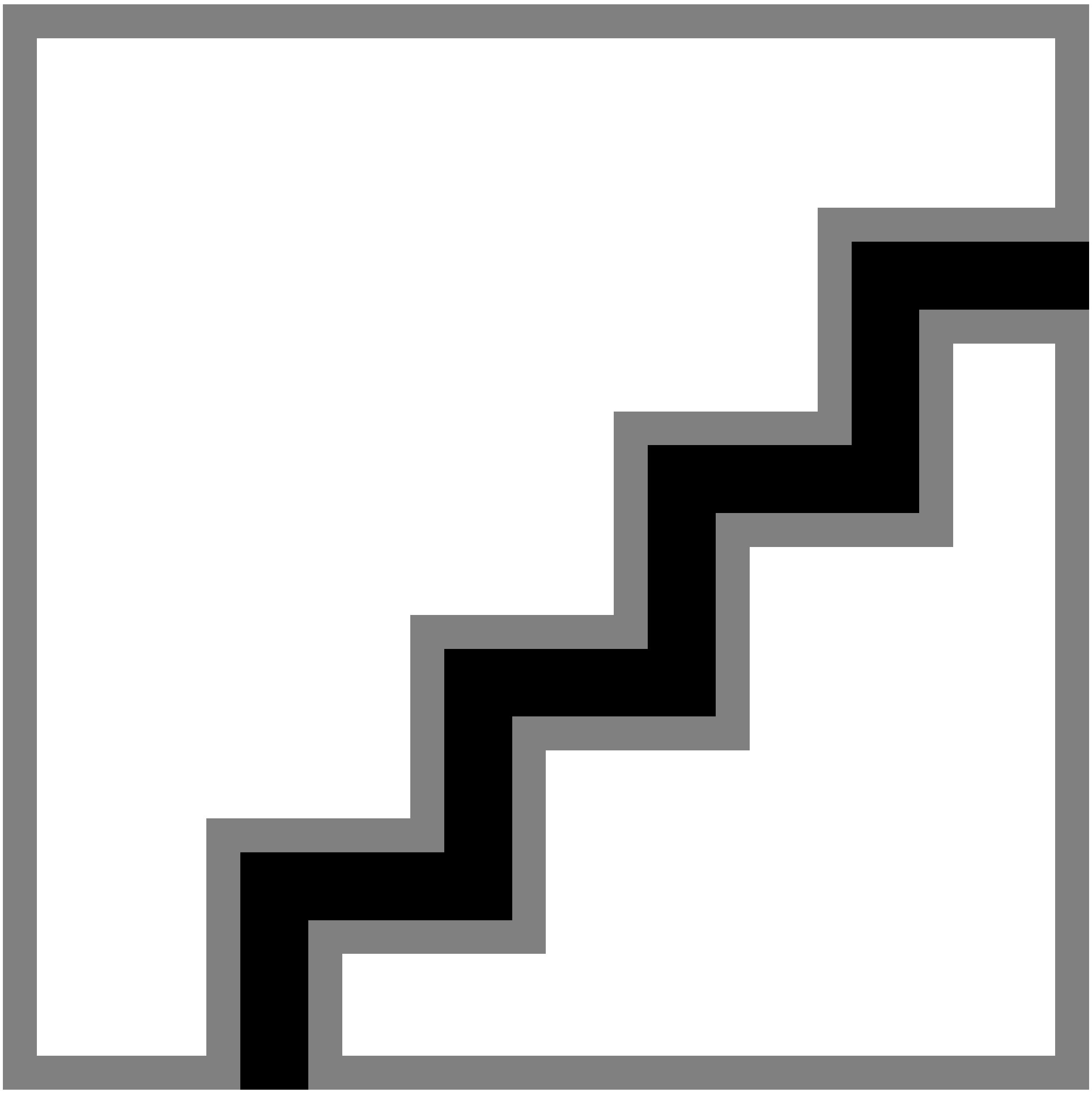


Figure 10-2 Search Event

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 Set Local Parameters

Set the live view parameters, picture and clip settings.

Set Live View Parameters

Click **Configuration → Local** to enter the Local page. Configure the stream type, the play performance and click **Save**.

Picture and Clip Settings

Click **Configuration → Local** to enter the Local page. Select image format, saving path and click **Save**.
You can also click **Open** to open the file folder to view details.

10.6.2 View Device Information

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

Click **Configuration → System → System Settings → Basic Information** to enter the configuration page.
You can view the device name, device No., language, model, serial No., version, number of channels, IO input, IO output, lock, alarm input, alarm output, and device capacity, etc.

10.6.3 Set Time

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

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

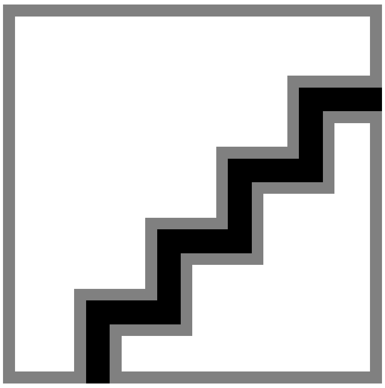


Figure 10-3 Time Settings

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.

10.6.4 Set DST

Steps

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

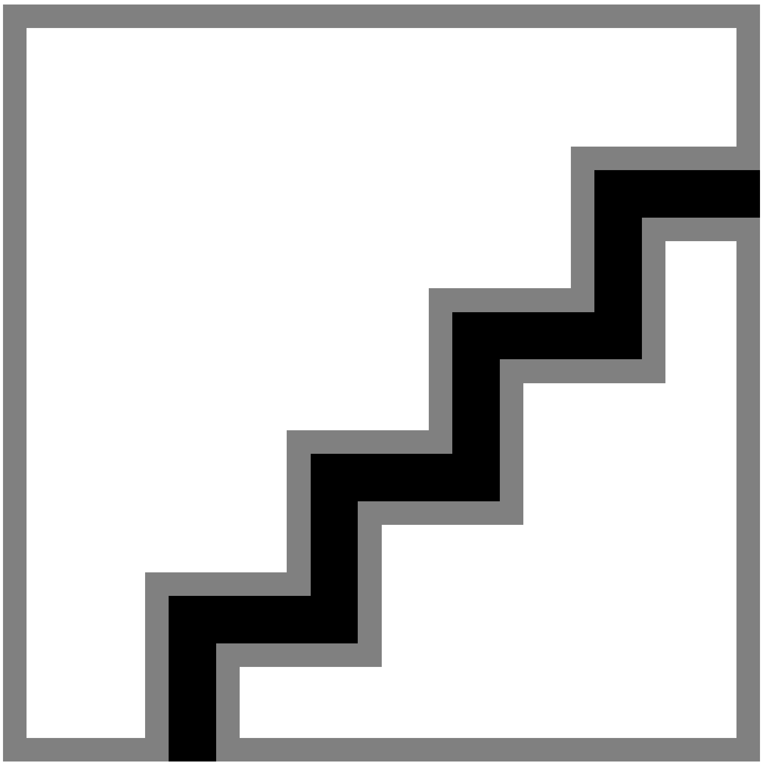


Figure 10-4 DST Page

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

10.6.5 Change Administrator's Password

Steps

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

⚠ **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.

10.6.6 View Device Arming/Disarming Information

View device arming type and arming IP address.

Go to **Configuration → Arming/Disarming Information** .

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

10.6.7 Network Settings

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

Note

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

Set Basic Network Parameters

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

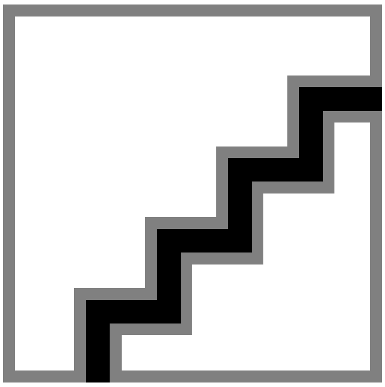


Figure 10-5 TCP/IP Settings Page

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** .

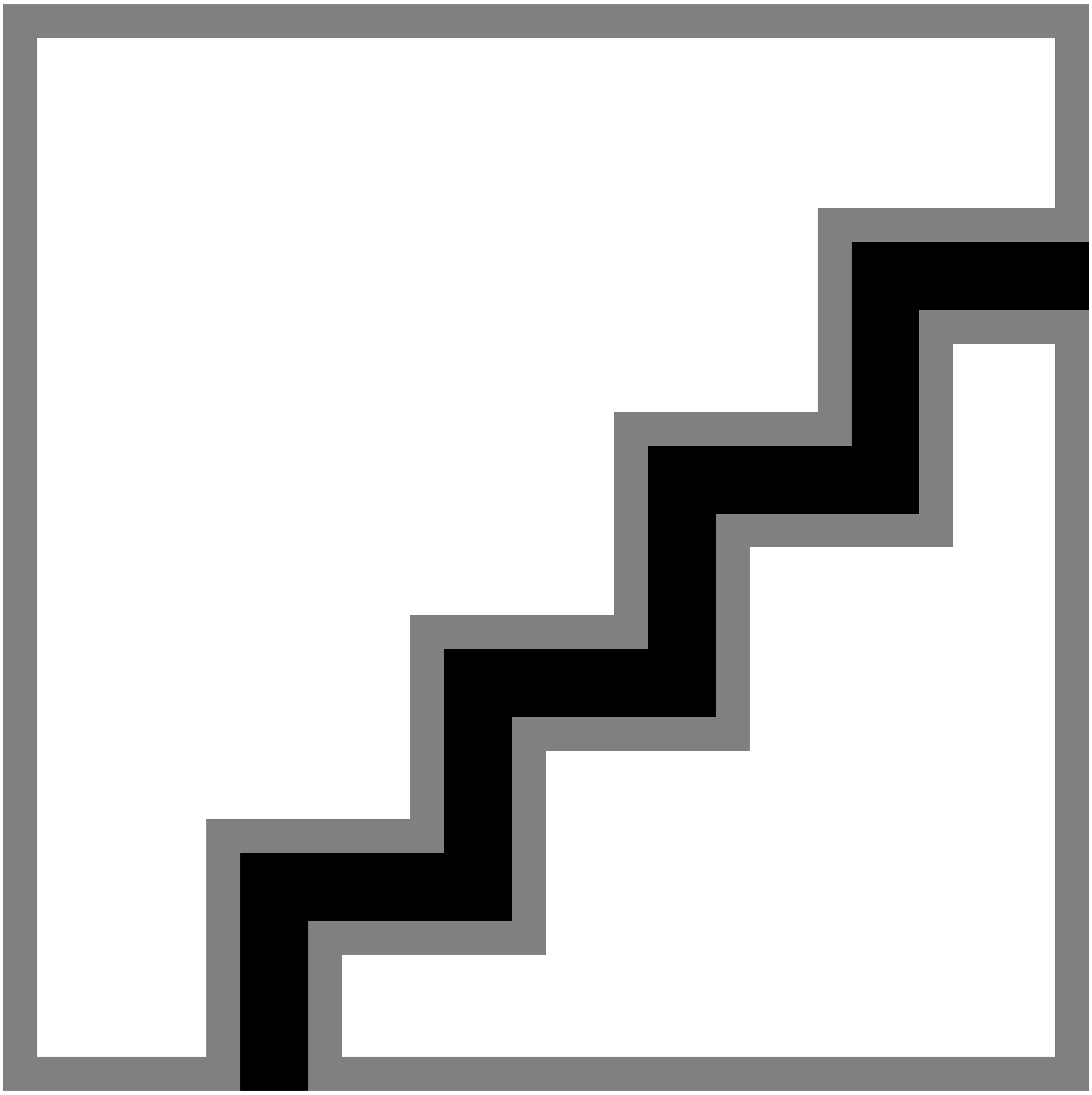


Figure 10-6 Wi-Fi Settings Page

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

Set Port Parameters

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

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

HTTP

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

HTTPS

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

HTTP Listening

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

Note

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

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

RTSP

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

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

SDK Server

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

Platform Access

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

Steps

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

   Note

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

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

Note

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

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

Set ISUP Parameters

Set the ISUP parameters for accessing device via ISUP protocol.

Steps

Note

The function should be supported by the device.

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

   Note

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

10.6.8 Set Video and Audio Parameters

Set the image quality and resolution.

Set Video Parameters

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

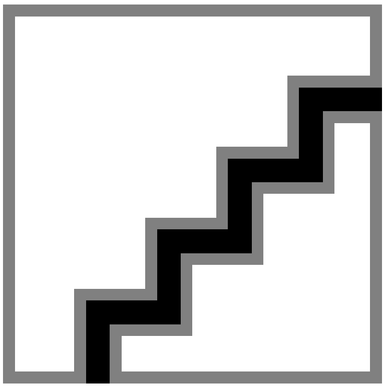


Figure 10-7 Video Settings Page

Set the stream type, the video type, the bitrate type, the frame rate, the Max. bitrate, the video encoding, and I Frame Interval.

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

Note

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

10.6.9 Set Image Parameters

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

Steps

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

Video Adjust(Video Standard)

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

PAL

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

NTSC

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

Image Adjustment

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

Supplement Light Parameters

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

Capture Interval

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

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

10.6.10 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.

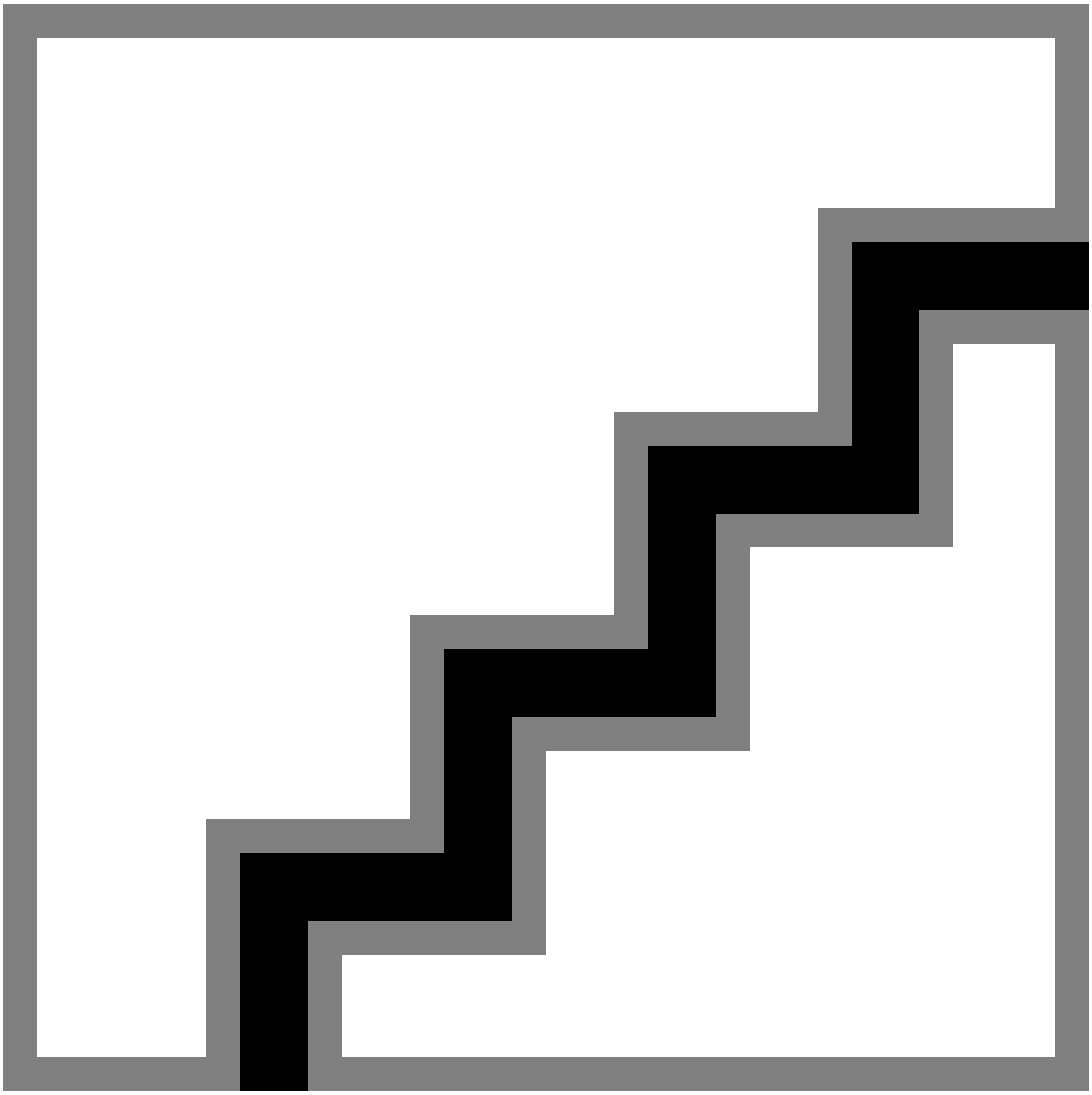


Figure 10-8 Set Authentication Parameters

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

Terminal/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

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.

Max. Authentication 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.

Set Door Parameters

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

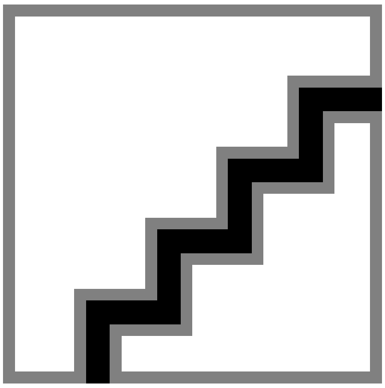


Figure 10-9 Door Parameters Settings Page

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

You can set terminal parameters for accessing.

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

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

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

10.6.11 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.

Wiegand 26 (3 bytes)

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

Wiegand 34 (4 bytes)

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

10.6.12 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 **Face Picture**, **Name**, and **Employee ID**, to display the authentication result.

Name De-identification

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

Picture Uploading and Storage

Save Picture When Authenticating

Save picture when authenticating automatically.

Upload Picture When Authenticating

Upload the pictures when authenticating to the platform automatically.

Save Registered Picture

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

Upload Picture After Linked Capture

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

Save Pictures After Linked Capture

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

Clear All Pictures in Device

Note

All pictures cannot be restored once they are deleted.

Clear Registered Face Pictures

All registered pictures in the device will be deleted.

Clear Captured Pictures

All captured pictures in the device will be deleted.

10.6.13 Time and Attendance Settings

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

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 → T&A Status** 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 → T&A Status** 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 → T&A Status** 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 → T&A Status** 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 → T&A Status** 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.

10.6.14 Set Biometric Parameters

Set Basic Parameters

Click **Configuration → Smart → Smart** .

Note

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

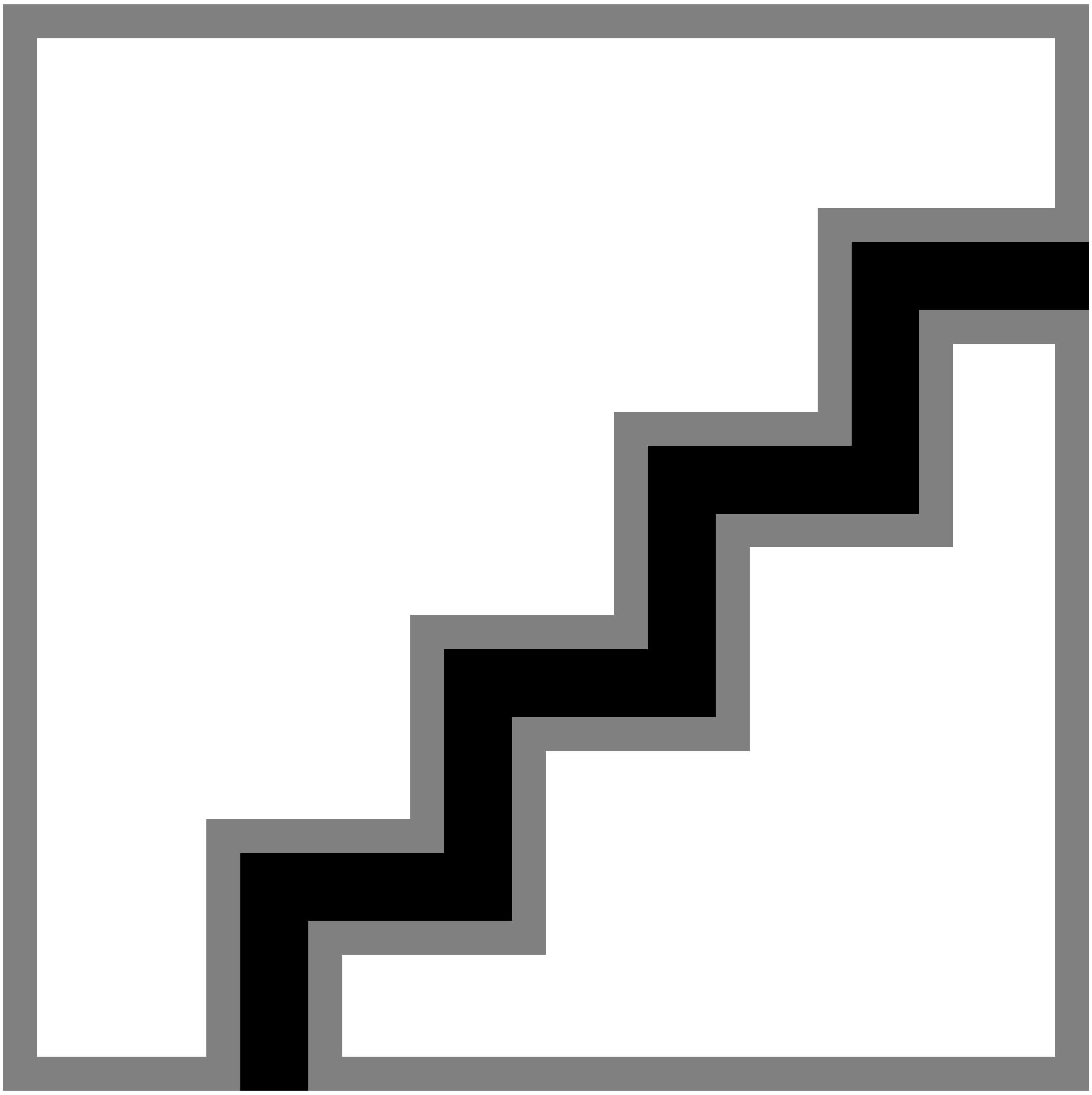


Figure 10-10 Smart Settings Page

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

Face Anti-spoofing

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

Note

Biometric recognition products are not 100% applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.

Live Face Detection Security Level

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

Recognition Distance

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

Application Mode

Select either others or indoor according to actual environment.

Face Recognition Mode

Normal Mode

Recognize face via the camera normally.

Pitch Angle

The maximum pitch angle when starting face authentication.

Yaw Angle

The maximum yaw angle when starting face authentication.

1:1 Matching Threshold

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

1:N Matching Threshold

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

Face Recognition Timeout Value

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

Face without Mask Detection

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

None

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

Reminder of Wearing Face Mask

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

Must Wear Face Mask

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

Face with Mask & Face (1:1)

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

Face with Mask 1:N Matching Threshold

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

Set Recognition Area

Click **Configuration → Smart → Area Configuration** .
Drag the yellow frame in the live video to adjust the recognition area. Only the face within the area can be recognized by the system.
Click **Save** to save the settings.
Click 🎥 or 📷 to record videos or capture pictures.

10.6.15 Set Preference

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

Set Theme

Click **Configuration → Preference** .

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 **Default** or **Simple**. When you select **Simple**, the information of name, ID, face picture 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 Client Software Configuration

11.1 Configuration Flow of Client Software

Follow the flow diagram below to configure on the client software.

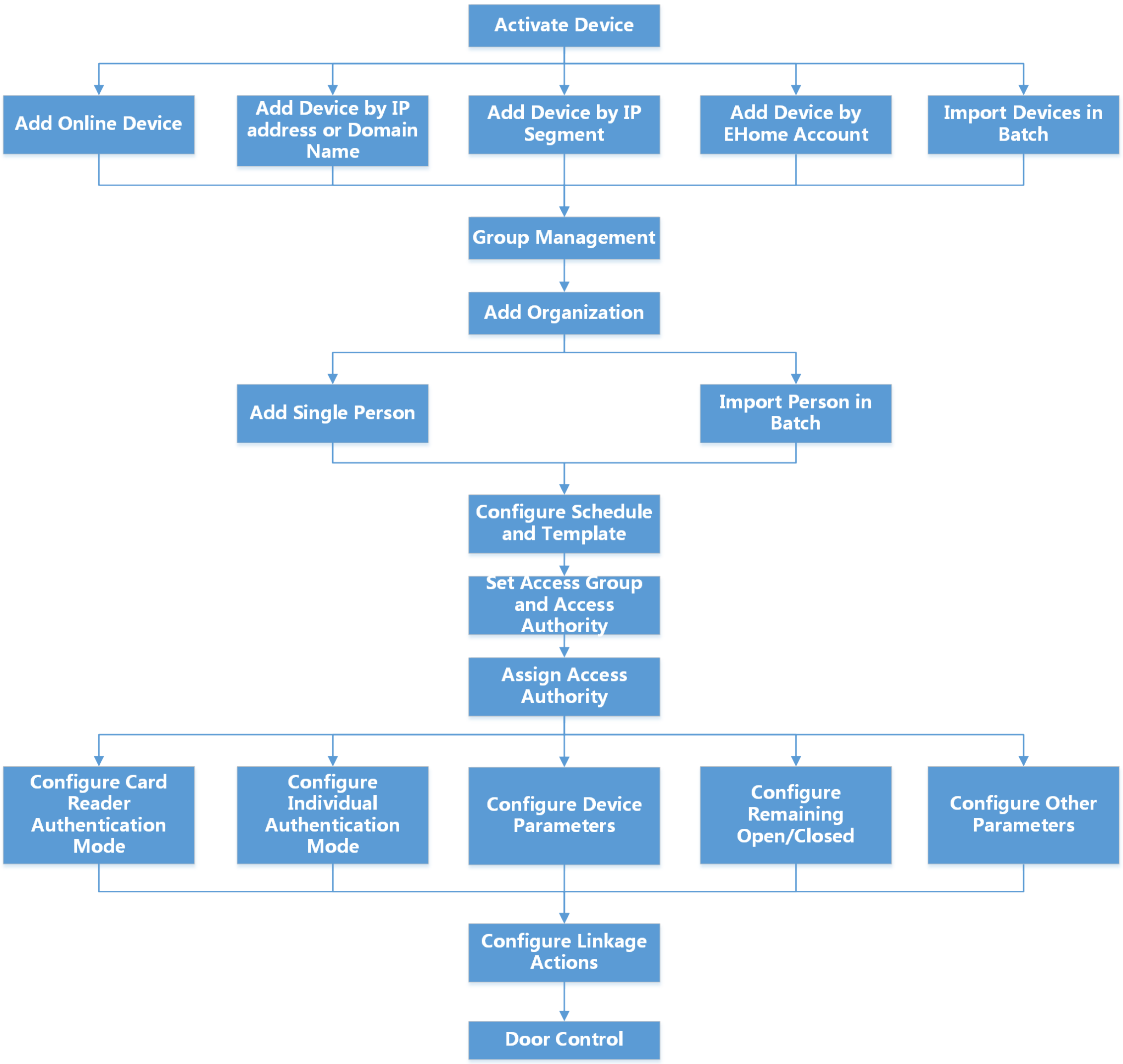

Activate Device
Add Online Device
Add Device by IP address or Domain Name
Add Device by IP Segment
Add Device by EHome Account
Import Devices in Batch
Group Management
Add Organization
Add Single Person
Import Person in Batch
Configure Schedule and Template
Set Access Group and Access Authority
Assign Access Authority
Configure Card Reader Authentication Mode
Configure Individual Authentication Mode
Configure Device Parameters
Configure Remaining Open/Closed
Configure Other Parameters
Configure Linkage Actions
Door Control

Figure 11-1 Flow Diagram of Configuration on Client Software

11.2 Device Management

The client supports managing access control devices and video intercom devices.

Example

You can control entrance & exit and manage attendance after adding access control devices to the client; you can perform video intercom with the indoor stations and door stations.

11.2.1 Add Device

The client provides three device adding modes including by IP/domain, IP segment, and EHome protocol. The client also supports importing multiple devices in a batch when there are large amount of devices to be added.

Add Device by IP Address or Domain Name

If you know the IP address or domain name of the device to add, you can add devices to the client by specifying the IP address (or domain name), user name, password, etc.

Steps

1. Enter Device Management module.
2. Click **Device** tab on the top of the right panel.

   The added devices are displayed on the right panel.
3. Click **Add** to open the Add window, and then select **IP/Domain** as the adding mode.
4. Enter the required information.

   Name

   Create a descriptive name for the device. For example, you can use a nickname that can show the location or feature of the device.

   Address

   The IP address or domain name of the device.

   Port

   The devices to add share the same port number. The default value is ***8000***.

   User Name

   Enter the device user name. By default, the user name is ***admin***.

   Password

   Enter the device password.

   ⚠ **Caution**

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

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

5. **Optional:** Check **Transmission Encryption (TLS)** to enable transmission encryption using TLS (Transport Layer Security) protocol for security purpose.

Note

- This function should be supported by the device.
- If you have enabled Certificate Verification, you should click **Open Certificate Directory** to open the default folder, and copy the certificate file exported from the device to this default directory to strengthen the security. See for details about enabling certificate verification.
- You can log into the device to get the certificate file by web browser.

6. Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.
7. **Optional:** Check **Import to Group** to create a group by the device name, and import all the channels of the device to this group.

Example

For access control device, its access points, alarm inputs/outputs, and encoding channels (if exist) will be imported to this group.

8. Finish adding the device.
   - Click **Add** to add the device and back to the device list page.
   - Click **Add and New** to save the settings and continue to add other device.

Import Devices in a Batch

You can add multiple devices to the client in a batch by entering the device parameters in a pre-defined CSV file.

Steps

1. Enter the Device Management module.
2. Click **Device** tab on the top of the right panel.
3. Click **Add** to open the Add window, and then select **Batch Import** as the adding mode.
4. Click **Export Template** and then save the pre-defined template (CSV file) on your PC.
5. Open the exported template file and enter the required information of the devices to be added on the corresponding column.

Note

For detailed description of the required fields, refer to the introductions in the template.

Adding Mode

Enter ***0*** or ***1*** or ***2***.

Address

Edit the address of the device.

Port

Enter the device port number. The default port number is ***8000***.

User Name

Enter the device user name. By default, the user name is ***admin***.

Password

Enter the device 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.

Import to Group

Enter ***1*** to create a group by the device name. All the channels of the device will be imported to the corresponding group by default. Enter ***0*** to disable this function.

6. Click ⋯ and select the template file.
7. Click **Add** to import the devices.

11.2.2 Reset Device Password

If you forgot the password of the detected online devices, you can reset the device password via the client.

Steps

1. Enter Device Management page.
2. Click **Online Device** to show the online device area.

   All the online devices sharing the same subnet will be displayed in the list.
3. Select the device from the list and click 🔑 on the Operation column.
4. Reset the device password.
   - Click **Generate** to pop up the QR Code window and click **Download** to save the QR code to your PC. You can also take a photo of the QR code to save it to your phone. Send the picture to our technical support.

Note

For the following operations for resetting the password, contact our technical support.

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.

11.2.3 Manage Added Devices

After adding devices to device list, you can manage the added devices including editing device parameters, remote configuration, viewing device status, etc.

Table 11-1 Manage Added Devices

Edit Device	Click to edit device information including device name, address, user name, password, etc.
Delete Device	Check one or more devices, and click **Delete** to delete the selected devices.
Remote Configuration	Click to set remote configuration of the corresponding device. For details, refer to the user manual of device.
View Device Status	Click to view device status, including door No., door status, etc. **Note** For different devices, you will view different information about device status.
View Online User	Click to view the details of online user who access the device, including user name, user type, IP address and login time.
Refresh Device Information	Click to refresh and get the latest device information.

11.3 Group Management

The client provides groups to manage the added resources in different groups. You can group the resources into different groups according to the resources' locations.

Example

For example, on the 1st floor, there mounted 16 doors, 64 alarm inputs, and 16 alarm outputs. You can organize these resources into one group (named 1st Floor) for convenient management. You can control door status, and do some other operations of the devices after managing the resources by groups.

11.3.1 Add Group

You can add group to organize the added device for convenient management.

Steps

1. Enter the Device Management module.
2. Click **Device Management → Group** to enter the group management page.
3. Create a group.
   - Click **Add Group** and enter a group name as you want.
   - Click **Create Group by Device Name** and select an added device to create a new group by the name of the selected device.

   Note

   The resources (such as alarm inputs/outputs, access points, etc.) of this device will be imported to the group by default.

11.3.2 Import Resources to Group

You can import the device resources (such as alarm inputs/outputs, access points, etc.) to the added group in a batch.

Before You Start

Add a group for managing devices. Refer to ***Add Group*** .

Steps

1. Enter the Device Management module.
2. Click **Device Management → Group** to enter the group management page.
3. Select a group from the group list and select the resource type as **Access Point**, **Alarm Input**, **Alarm Output**, etc.
4. Click **Import**.
5. Select the thumbnails/names of the resources in the thumbnail/list view.

Note

You can click ⊞ or ☰ to switch the resource display mode to thumbnail view or to list view.

6. Click **Import** to import the selected resources to the group.

11.4 Person Management

You can add person information to the system for further operations such as access control, video intercom, time and attendance, etc. You can manage the added persons such as issuing cards to them in a batch, importing and exporting person information in a batch, etc.

11.4.1 Add Organization

You can add an organization and import person information to the organization for effective management of the persons. You can also add a surbodinate organization for the added one.

Steps

1. Enter **Person** module.
2. Select a parent organization in the left column and click **Add** in the upper-left corner to add an organization.
3. Create a name for the added organization.

Note

Up to 10 levels of organizations can be added.

4. **Optional:** Perform the following operation(s).

Edit Organization

Hover the mouse on an added organization and click ✎ to edit its name.

Delete Organization

Hover the mouse on an added organization and click ✕ to delete it.

Note

- The lower-level organizations will be deleted as well if you delete an organization.
- Make sure there is no person added under the organization, or the organization cannot be deleted.

Show Persons in Sub Organization

Check **Show Persons in Sub Organization** and select an organization to show persons in its sub organizations.

11.4.2 Import and Export Person Identify Information

You can import the information and pictures of multiple persons to the client software in a batch. Meanwhile, you can also export the person information and pictures and save them in your PC.

Import Person Information

You can enter the information of multiple persons in a predefined template (CSV/Excel file) to import the information to the client in a batch.

Steps

1. Enter the Person module.
2. Select an added organization in the list, or click **Add** in the upper-left corner to add an organization and then select it.
3. Click **Import** to open the Import panel.
4. Select **Person Information** as the importing mode.
5. Click **Download Template for Importing Person** to download the template.
6. Enter the person information in the downloaded template.

   Note

   - If the person has multiple cards, separate the card No. with semicolon.
   - Items with asterisk are required.
   - By default, the Hire Date is the current date.
7. Click … to select the CSV/Excel file with person information from local PC.
8. Click **Import** to start importing.

   Note

   - If a person No. already exists in the client's database, delete the existing information before importing.
   - You can import information of no more than 2,000 persons.

Import Person Pictures

After importing face pictures for the added persons to the client, the persons in the pictures can be identified by an added face recognition terminal. You can either import person pictures one by one, or import multiple pictures at a time according to your need.

Before You Start

Be sure to have imported person information to the client beforehand.

Steps

1. Enter the Person module.
2. Select an added organization in the list, or click **Add** in the upper-left corner to add an organization and then select it.
3. Click **Import** to open the Import panel and check **Face**.
4. **Optional:** Enable **Verify by Device** to check whether face recognition device managed in the client can recognize the face in the photo.
5. Click … to select a face picture file.

Note

- The (folder of) face pictures should be in ZIP format.
- Each picture file should be in JPG format and should be no larger than 200 KB.
- Each picture file should be named as "Person ID_Name". The Person ID should be the same with that of the imported person information.

6. Click **Import** to start importing.

   The importing progress and result will be displayed.

Export Person Information

You can export the added persons' information to local PC as a CSV/Excel file.

Before You Start
Make sure you have added persons to an organization.

Steps

1. Enter the Person module.
2. **Optional:** Select an organization in the list.

   Note

   All persons' information will be exported if you do not select any organization.

3. Click **Export** to open the Export panel.
4. Check **Person Information** as the content to export.
5. Check desired items to export.
6. Click **Export** to save the exported file in CSV/Excel file on your PC.

Export Person Pictures

You can export face picture file of the added persons and save in your PC.

Before You Start
Make sure you have added persons and their face pictures to an organization.

Steps

1. Enter the Person module.
2. **Optional:** Select an organization in the list.

   Note

   All persons' face pictures will be exported if you do not select any organization.

3. Click **Export** to open the Export panel and check **Face** as the content to export.
4. Click **Export** to start exporting.

Note

- The exported file is in ZIP format.
- The exported face picture is named as "Person ID_Name_0" ("0" is for a full-frontal face).

11.4.3 Get Person Information from Access Control Device

If the added access control device has been configured with person information (including person details, fingerprint, and issued card information), you can get the person information from the device and import them to the client for further operations.

Steps

Note

- If the person name stored in the device is empty, the person name will be filled with the issued card No. after importing to the client.
- The gender of the persons will be **Male** by default.
- If the card number or person ID (employee ID) stored on the device already exists in the client database, the person with this card number or person ID will not be imported to the client.

1. Enter **Person** module.
2. Select an organization to import the persons.
3. Click **Get from Device**.
4. Select an added access control device or the enrollment station from the drop-down list.

   Note

   If you select the enrollment station, you should click **Login**, and set IP address, port No., user name and password of the device.
5. Click **Import** to start importing the person information to the client.

   Note

   Up to 2,000 persons and 5,000 cards can be imported.

   The person information, including person details, person's fingerprint information (if configured), and the linked cards (if configured), will be imported to the selected organization.

11.4.4 Issue Cards to Persons in Batch

The client provides a convenient way to issue cards to multiple persons in a batch.

Steps

1. Enter **Person** module.
2. Click **Batch Issue Cards**.

   All the added persons with no card issued will be displayed in the right panel.

3. **Optional:** Enter key words (name or person ID) in the input box to filter the person(s) that need issuing cards.
4. **Optional:** Click **Settings** to set the card issuing parameters. For details, refer to *Issue a Card by Local Mode*.
5. Click **Initialize** to initialize the card enrollment station or card reader to make it ready for issuing cards.
6. Click the **Card No.** column and enter the card number.
   - Place the card on the card enrollment station.
   - Swipe the card on the card reader.
   - Manually enter the card number and press the **Enter** key.

   The person(s) in the list will be issued with card(s).

11.4.5 Report Card Loss

If the person lost his/her card, you can report the card loss so that the card's related access authorization will be inactive.

Steps

1. Enter **Person** module.
2. Select the person you want to report card loss for and click **Edit** to open the Edit Person window.
3. In the **Credential → Card** panel, click on the added card to set this card as lost card.

   After reporting card loss, the access authorization of this card will be invalid and inactive. Other person who gets this card cannot access the doors by swiping this lost card.
4. **Optional:** If the lost card is found, you can click to cancel the loss.

   After cancelling card loss, the access authorization of the person will be valid and active.
5. If the lost card is added in one access group and the access group is applied to the device already, after reporting card loss or cancelling card loss, a window will pop up to notify you to apply the changes to the device. After applying to device, these changes can take effect on the device.

11.4.6 Set Card Issuing Parameters

The client provides two modes for reading a card's number: via card enrollment station or via the card reader of the access control device. If a card enrollment station is available, connect it to the PC running the client by USB interface or COM, and place the card on the card enrollment to read the card number. If not, you can also swipe the card on the card reader of the added access control device to get the card number. As a result, before issuing a card to one person, you need to set the card issuing parameters including the issuing mode and related parameters.

When adding a card to one person, click **Settings** to open the Card Issuing Settings window.

Local Mode: Issue Card by Card Enrollment Station

Connect a card enrollment station to the PC running the client. You can place the card on the card enrollment station to get the card number.

Card Enrollment Station

Select the model of the connected card enrollment station

Note

Currently, the supported card enrollment station models include DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E, and DS-K1F180-D8E.

Card Type

This field is only available when the model is DS-K1F100-D8E or DS-K1F180-D8E.

Select the card type as EM card or IC card according to the actual card type.

Serial Port

It is only available when the model is DS-K1F100-M.

Select the COM the card enrollment station connects to.

Buzzing

Enable or disable the buzzing when the card number is read successfully.

Card No. Type

Select the type of the card number according to actual needs.

M1 Card Encryption

This field is only available when the model is DS-K1F100-D8, DS-K1F100-D8E, or DS-K1F180-D8E.

If the card is M1 card, and if you need to enable the M1 Card Encryption function, you should enable this function and select the sector of the card to encrypt.

Remote Mode: Issue Card by Card Reader

Select an access control device added in the client and swipe the card on its card reader to read the card number.

11.5 Configure Schedule and Template

You can configure the template including holiday and week schedule. After setting the template, you can adopt the configured template to access groups when setting the access groups, so that the access group will take effect in the time durations of the template.

Note

For access group settings, refer to ***Set Access Group to Assign Access Authorization to Persons*** .

11.5.1 Add Holiday

You can create holidays and set the days in the holidays, including start date, end date, and holiday duration in one day.

Steps

Note

You can add up to 64 holidays in the software system.

1. Click **Access Control → Schedule → Holiday** to enter the Holiday page.
2. Click **Add** on the left panel.
3. Create a name for the holiday.
4. **Optional:** Enter the descriptions or some notifications of this holiday in the Remark box.
5. Add a holiday period to the holiday list and configure the holiday duration.

   Note

   Up to 16 holiday periods can be added to one holiday.

   1) Click **Add** in the Holiday List field.
   2) Drag the cursor to draw the time duration, which means in that duration of time, the configured access group is activated.

      Note

      Up to 8 time durations can be set to one holiday period.
   3) **Optional:** Perform the following operations to edit the time durations.
      - Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to ✋ .
      - Click the time duration and directly edit the start/end time in the appeared dialog.
      - Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to ⇔ .
   4) **Optional:** Select the time duration(s) that need to be deleted, and then click ⊗ in the Operation column to delete the selected time duration(s).
   5) **Optional:** Click 🗑 in the Operation column to clear all the time duration(s) in the time bar.
   6) **Optional:** Click ☒ in the Operation column to delete this added holiday period from the holiday list.
6. Click **Save**.

11.5.2 Add Template

Template includes week schedule and holiday. You can set week schedule and assign the time duration of access authorization for different person or group. You can also select the added holiday(s) for the template.

Steps

Note

You can add up to 255 templates in the software system.

1. Click **Access Control → Schedule → Template** to enter the Template page.

   Note

   There are two default templates: All-Day Authorized and All-Day Denied, and they cannot be edited or deleted.

   All-Day Authorized

   The access authorization is valid in each day of the week and it has no holiday.

   All-Day Denied

   The access authorization is invalid in each day of the week and it has no holiday.

2. Click **Add** on the left panel to create a new template.
3. Create a name for the template.
4. Enter the descriptions or some notification of this template in the Remark box.
5. Edit the week schedule to apply it to the template.

   1) Click **Week Schedule** tab on the lower panel.

   2) Select a day of the week and draw time duration(s) on the timeline bar.

   Note

   Up to 8 time duration(s) can be set for each day in the week schedule.

   3) **Optional:** Perform the following operations to edit the time durations.

   - Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to ✋ .
   - Click the time duration and directly edit the start/end time in the appeared dialog.
   - Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to ⇔ .

   4) Repeat the two steps above to draw more time durations on the other days of the week.

6. Add a holiday to apply it to the template.

   Note

   Up to 4 holidays can be added to one template.

   1) Click **Holiday** tab.

   2) Select a holiday in the left list and it will be added to the selected list on the right panel.

   3) **Optional:** Click **Add** to add a new holiday.

   Note

   For details about adding a holiday, refer to ***Add Holiday*** .

4) **Optional:** Select a selected holiday in the right list and click ☒ to remove the selected one, or click **Clear** to clear all the selected holiday(s) in the right list.

7. Click **Save** to save the settings and finish adding the template.

11.6 Set Access Group to Assign Access Authorization to Persons

After adding the person and configuring the person's credentials, you can create the access groups to define which person(s) can get access to which door(s) and then apply the access group to the access control device to take effect.

Before You Start

- Add person to the client.
- Add access control device to the client and group access points. For details, refer to ***Group Management*** .
- Add template.

Steps

When the access group settings are changed, you need to apply the access groups to the devices again to take effect. The access group changes include changes of template, access group settings, person's access group settings, and related person details (including card number, fingerprint, face picture, linkage between card number and fingerprint, linkage between card number and fingerprint, card password, card effective period, etc).

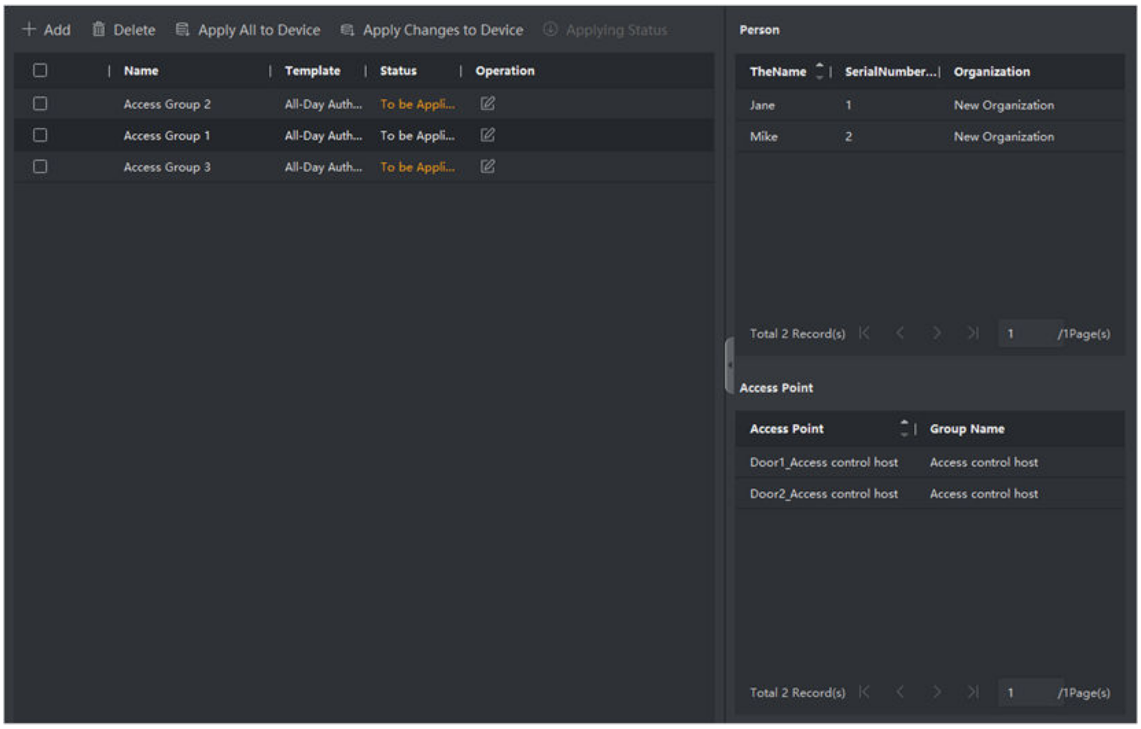
1. Click **Access Control → Authorization → Access Group** to enter the Access Group interface.
2. Click **Add** to open the Add window.
3. In the **Name** text field, create a name for the access group as you want.
4. Select a template for the access group.

   Note

   You should configure the template before access group settings. Refer to ***Configure Schedule and Template*** for details.

5. In the left list of the Select Person field, select person(s) to assign access authority.
6. In the left list of the Select Access Point field, select door(s), door station(s) or floor(s) for the selected persons to access.
7. Click **Save**.

   You can view the selected person(s) and the selected access point(s) on the right side of the interface.



□	Name	Template	Status	Operation
□	Access Group 2	All-Day Auth...	To be Appli...	✎
□	Access Group 1	All-Day Auth...	To be Appli...	✎
□	Access Group 3	All-Day Auth...	To be Appli...	✎

TheName	SerialNumber...	Organization
Jane	1	New Organization
Mike	2	New Organization

Total 2 Record(s) 1 /1Page(s)

Access Point	Group Name
Door1_Access control host	Access control host
Door2_Access control host	Access control host

Total 2 Record(s) 1 /1Page(s)

Figure 11-2 Display the Selected Person(s) and Access Point(s)

8. After adding the access groups, you need to apply them to the access control device to take effect.
   1) Select the access group(s) to apply to the access control device.
   2) Click **Apply All to Devices** start applying all the selected access group(s) to the access control device or door station.
   3) Click **Apply All to Devices** or **Apply Changes to Devices**.

      Apply All to Devices

      This operation will clear all the existed access groups of the selected devices and then apply the new access group to the device.

      Apply Changes to Devices

      This operation will not clear the existed access groups of the selected devices and only apply the changed part of the selected access group(s) to the device(s).
   4) View the applying status in the Status column or click **Applying Status** to view all the applied access group(s).

   Note

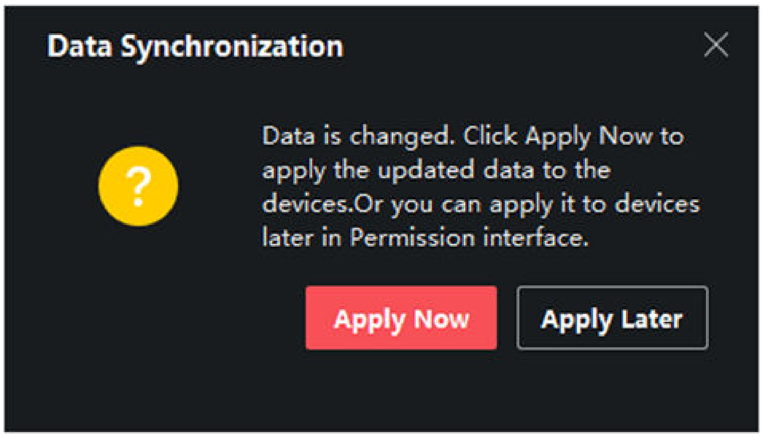
   You can check **Display Failure Only** to filter the applying results.

   The selected persons in the applied access groups will have the authorization to enter/exit the selected doors/door stations with their linked card(s) or fingerprints.
9. **Optional:** Click ✎ to edit the access group if necessary.

Note

If you change the persons' access information or other related information, you will view the promptAccess Group to Be Applied on the right corner of the client.

You can click the prompt to apply the changed data to the device. You can select either **Apply Now** or **Apply Later**.



Data Synchronization

Data is changed. Click Apply Now to apply the updated data to the devices.Or you can apply it to devices later in Permission interface.

Figure 11-3 Data Synchronization

11.7 Configure Advanced Functions

You can configure the advanced functions of access control to meet some special requirements in different scene.

Note

- For the card related functions(the type of access control card), only the card(s) with access group applied will be listed when adding cards.
- The advanced functions should be supported by the device.
- Hover the cursor on the Advanced Function, and then Click ⚙ to customize the advanced function(s) to be displayed.

11.7.1 Configure Device Parameters

After adding the access control device, you can configure the parameters of access control device, access control points.

Configure Parameters for Access Control Device

After adding the access control device, you can configure its parameters, including overlaying user information on picture, uploading pictures after capturing, saving captured pictures, etc.

Steps

1. Click **Access Control → Advanced Function → Device Parameter** .

   Note

   If you can find Device Parameter in the Advanced Function list, Hover the cursor on the Advanced Function, and then Click ⚙ to select the Device Parameter to be displayed.

2. Select an access device to show its parameters on the right page.
3. Turn the switch to ON to enable the corresponding functions.

   Note

   - The displayed parameters may vary for different access control devices.
   - Some of the following parameters are not listed in the Basic Information page, click **More** to edit the parameters.

Voice Prompt

If you enable this function, the voice prompt is enabled in the device. You can hear the voice prompt when operating in the device.

Upload Pic. After Linked Capture

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

Save Pic. After Linked Capture

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

Face Recognition Mode

Normal Mode

Recognize face via the camera normally.

Deep Mode

The device can recognize a much wider people range than the normal mode. This mode is applicable to a more complicated environment.

Enable NFC Card

If enable the function, the device can recognize the NFC card. You can present NFC card on the device.

Enable M1 Card

If enable the function, the device can recognize the M1 card. You can present M1 card on the device.

Enable EM Card

If enable the function, the device can recognize the EM card. You can present EM card on the device.

Note

If the peripheral card reader supports presenting EM card, the function is also supported to enable/disable the EM card function.

4. Click **OK**.
5. **Optional:** Click **Copy to**, and then select the access control device(s) to copy the parameters in the page to the selected device(s).

Configure Parameters for Door/Elevator

After adding the access control device, you can configure its access point (door or floor) parameters.

Before You Start
Add access control device to the client.

Steps

1. Click **Access Control → Advanced Function → Device Parameter** .
2. Select an access control device on the left panel, and then click ▸ to show the doors or floors of the selected device.
3. Select a door or floor to show its parameters on the right page.
4. Edit the door or floor parameters.

Note

- The displayed parameters may vary for different access control devices.
- Some of the following parameters are not listed in the Basic Information page, click **More** to edit the parameters.

Name

Edit the card reader name as desired.

Door Contact

You can set the door sensor as remaining closed or remaining open. Usually, it is remaining closed.

Exit Button Type

You can set the exit button as remaining closed or remaining open. Usually, it is remaining open.

Door Locked Time

After swiping the normal card and relay action, the timer for locking the door starts working.

Extended Open Duration

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

Door Left Open Timeout Alarm

The alarm can be triggered if the door has not been closed in a configured time period. If it is set as 0, no alarm will be triggered.

Lock Door when Door Closed

The door can be locked once it is closed even if the **Door Locked Time** is not reached.

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.

Dismiss Code

Create a dismiss code which can be used to stop the buzzer of the card reader (by entering the dismiss code on the keypad).

Note

- The duress code, super code, and dismiss code should be different.
- The duress code, super password, and the dismiss code should be different from the authentication password.
- The length of duress code, super password, and the dismiss code is according the device, usually it should contains 4 to 8 digits.

5. Click **OK**.
6. **Optional:** Click **Copy to** , and then select the door/floor(s) to copy the parameters in the page to the selected doors/floor(s).

Note

The door or floor's status duration settings will be copied to the selected door/floor(s) as well.

Configure Parameters for Card Reader

After adding the access control device, you can configure its card reader parameters.

Before You Start

Add access control device to the client.

Steps

1. Click **Access Control → Advanced Function → Device Parameter** .
2. In the device list on the left, click ▸ to expand the door, select a card reader and you can edit the card reader's parameters on the right.
3. Edit the card reader basic parameters in the Basic Information page.

Note

- The displayed parameters may vary for different access control devices. There are part of parameters listed as follows. Refer to the user manual of the device for more details.
- Some of the following parameters are not listed in the Basic Information page, click **More** to edit the parameters.

Name

Edit the card reader name as desired.

OK LED Polarity/Error LED Polarity/Buzzer Polarity

Set OK LED Polarity/Error LED Polarity/Buzzer LED Polarity of main board according to the card reader parameters. Generally, adopts the default settings.

Minimum Card Swiping Interval

If the interval between card swiping of the same card is less than the set value, the card swiping is invalid. You can set it as 0 to 255.

Max. Interval When Entering PWD

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

Alarm of Max. Failed Attempts

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

Max. Times of Card Failure

Set the max. failure attempts of reading card.

Tampering Detection

Enable the anti-tamper detection for the card reader.

Communicate 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.

Buzzing Time

Set the card reader buzzing time. The available time ranges from 0 to 5,999s. 0 represents continuous buzzing.

Card Reader Type/Card Reader Description

Get card reader type and description. They are read-only.

Fingerprint Recognition Level

Select the fingerprint recognition level in the drop-down list.

Default Card Reader Authentication Mode

View the default card reader authentication mode.

Fingerprint Capacity

View the maximum number of available fingerprints.

Existing Fingerprint Number

View the number of existed fingerprints in the device.

Score

The device will score the captured picture according to the yaw angle, pitch angle, and pupillary distance. If the score is less than the configured value, face recognition will be failed.

Face Recognition Timeout Value

If the recognition time is more than the configured time, the device will remind you.

Face Recognition Interval

The time interval between two continuous face recognitions when authenticating. By default, it is 2s.

Face 1:1 Matching Threshold

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

1:N Security Level

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

Live Face Detection

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

Live Face Detection Security Level

After enabling Live Face Detection function, you can set the matching security level when performing live face authentication.

Max. Failed Attempts for Face Auth.

Set the maximum live face detection failed attempts. The system will lock the user's face for 5 minutes if the live face detection is failed for more than the configured attempts. The same user cannot authenticate via the fake face within 5 minutes. Within the 5 minutes, the user can authenticate via the real face twice continuously to unlock.

Lock Authentication Failed Face

After enabling the Live Face Detection function, the system will lock the user's face for 5 minutes if the live face detection is failed for more than the configured attempts. The same user cannot authenticate via the fake face within 5 minutes. Within the 5 minutes, the user can authenticate via the real face twice continuously to unlock.

Application Mode

You can select indoor or others application modes according to actual environment.

4. Click **OK**.

5. **Optional:** Click **Copy to**, and then select the card reader(s) to copy the parameters in the page to the selected card reader(s).

Configure Parameters for Alarm Output

After adding the access control device, if the device links to alarm outputs, you can configure the parameters.

Before You Start

Add access control device to the client, and make sure the device supports alarm output.

Steps

1. Click **Access Control → Advanced Function → Device Parameter** to enter access control parameter configuration page.
2. In the device list on the left, click ▸ to expand the door, select an alarm input and you can edit the alarm input's parameters on the right.
3. Set the alarm output parameters.

   Name

   Edit the card reader name as desired.

   Alarm Output Active Time

   How long the alarm output will last after triggered.
4. Click **OK**.
5. **Optional:** Set the switch on the upper right corner to **ON** to trigger the alarm output.

11.7.2 Configure Device Parameters

After adding the access control device, you can set its parameters such as network parameters.

Set Parameters for Face Recognition Terminal

For face recognition terminal, you can set its parameters including face picture database, QR code authentication, etc.

Steps

Note

This function should be supported by the device.

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function → More Parameters** .
3. Select an access control device in the device list and click **Face Recognition Terminal**.
4. Set the parameters.

Note

These parameters displayed vary according to different device models.

COM

Select a COM port for configuration. COM1 refers to the RS-485 interface and COM2 refers to the RS-232 interface.

Face Picture Database

select Deep Learning as the face picture database.

Authenticate by QR Code

If enabled, the device camera can scan the QR code to authenticate. By default, the function is disabled.

Blocklist Authentication

If enabled, the device will compare the person who want to access with the persons in the blocklist.

If matched (the person is in the blocklist), the access will be denied and the device will upload an alarm to the client.

If mismatched (the person is not in the blocklist), the access will be granted.

Save Authenticating Face Picture

If enabled, the captured face picture when authenticating will be saved on the device.

MCU Version

View the device MCU version.

5. Click **Save**.

Set RS-485 Parameters

You can set the access control device's RS-485 parameters including the baud rate, data bit, the stop bit, parity type, flow control type, communication mode, work mode, and connection mode.

Steps

Note

The RS-485 Settings should be supported by the device.

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function → More Parameters** .
3. Select an access control device in the device list and click **RS-485** to enter the RS-485 Settings page.
4. Select the serial port number from the drop-down list to set the RS-485 parameters.
5. Set the serial number, external device, authentication center, baud rate, data bit, stop bit, parity type, flow control type, communication mode, and working mode in the drop-down list.

6. Click **Save**.
   - The configured parameters will be applied to the device automatically.
   - When you change the working mode or connection mode, the device will reboot automatically.

Set Wiegand Parameters

You can set the access control device's Wiegand channel and the communication mode.

Steps

Note

This function should be supported by the device.

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function → More Parameters** .
3. Select an access control device in the device list and click **Wiegand** to enter the Wiegand Settings page.
4. Set the switch to on to enable the Wiegand function for the device.
5. Select the Wiegand channel No. and the communication mode from the drop-down list.

   Note

   If you set **Communication Direction** as **Sending**, you are required to set the **Wiegand Mode** as **Wiegand 26** or **Wiegand 34**.
6. Check **Enable Wiegand** to enable the Wiegand function.
7. Click **Save**.
   - The configured parameters will be applied to the device automatically.
   - After changing the communication direction, the device will reboot automatically.

Enable M1 Card Encryption

M1 card encryption can improve the security level of authentication.

Steps

Note

The function should be supported by the access control device and the card reader.

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function → More Parameters** .
3. Select an access control device in the device list and click **M1 Card Encryption Verification** to enter the M1 Card Encryption Verification page.
4. Set the switch to on to enable the M1 card encryption function.

5. Set the sector ID.

   Note

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

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

11.8 Door Control

In Monitoring module, you can view the real-time status of the doors managed by the added access control device. You can also control the doors such as open/close the door, or remain the door open/closed via the client remotely. The real-time access event are displayed in this module. You can view the access details and person details.

Note

For the user with door control permission, the user can enter the Monitoring module and control the door. Or the icons used for control will not show. For setting the user permission, refer to ***Person Management*** .

11.8.1 Control Door Status

You can control the status for the door(s), including unlock door, locking door, remaining the door unlock, remaining the door locked, remain all unlocked, etc.

Before You Start

- Add person and assign access authorization to designed person, and person will have the access authorization to the access points (doors). For details, refer to ***Person Management*** and ***Set Access Group to Assign Access Authorization to Persons*** .
- Make sure the operation user has the permission of the access points (doors). For details, refer to .

Steps

1. Click **Monitoring** to enter the status monitoring page.
2. Select an access point group on the upper-right corner.

   Note

   For managing the access point group, refer to ***Group Management*** .

   The doors in the selected access control group will display.
3. Click a door icon to select a door, or press **Ctrl** and select multiple doors.

Note

For **Remain All Unlocked** and **Remain All Locked**, ignore this step.

4. Click the following buttons to control the door.

   Unlock

   When the door is locked, unlock it and it will be open for once. After the open duration, the door will be closed and locked again automatically.

   Lock

   When the door is unlocked, lock it and it will be closed. The person who has the access authorization can access the door with credentials.

   Remain Unlocked

   The door will be unlocked (no matter closed or open). All the persons can access the door with no credentials required.

   Remain Locked

   The door will be closed and locked. No person can access the door even if he/she has the authorized credentials, except the super users.

   Remain All Unlocked

   All doors in the group will be unlocked (no matter closed or open). All the persons can access the doors with no credentials required.

   Remain All Locked

   All doors in the group will be closed and locked. No person can access the doors even if he/she has the authorized credentials, except the super users.

   Capture

   Capture a picture manually.

   Note

   The **Capture** button is available when the device supports capture function. The picture is saved in the PC running the client. For setting the saving path, refer to *Set File Saving Path* in the user manual of the client software.

Result

The icon of the doors will change in real-time according to the operation if the operation is succeeded.

11.8.2 Check Real-Time Access Records

The access records will display in real time, including card swiping records, face recognitions records, fingerprint comparison records, etc. You can view the person information and view the picture captured during access.

Steps

1. Click **Monitoring** and select a group from the drop-down list on the upper-right corner.

   The access records triggered at the doors in the selected group will display in real time. You can view the details of the records, including card No., person name, organization, event time, etc.
2. **Optional:** Check the event type and event status so that these events will show in the list if the events are detected. The events of unchecked type or status will not be displayed in the list.
3. **Optional:** Check **Show Latest Event** and the latest access record will be selected and displayed at the top of the record list.
4. **Optional:** Click the event to view the accessed person details, including person pictures (captured picture and profile), person No., person name, organization, phone, contact address, etc.

   Note

   You can double click the captured picture to enlarge it to view the details.
5. **Optional:** Right click on the column name of the access event table to show or hide the column according to actual needs.

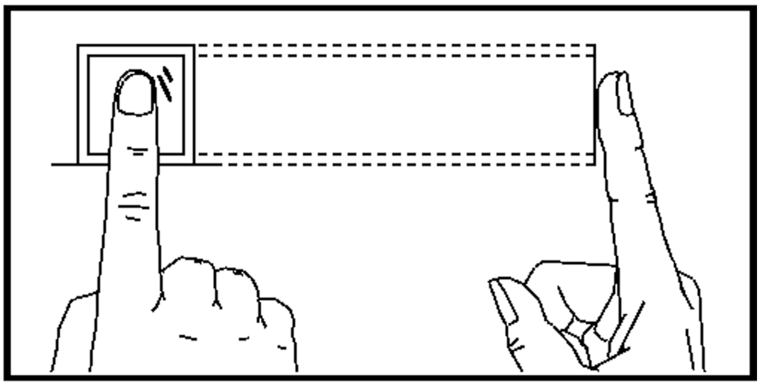
Appendix A. Tips for Scanning Fingerprint

Recommended Finger

Forefinger, middle finger or the third finger.

Correct Scanning

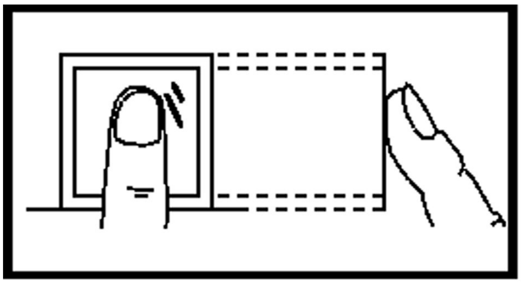
The figure displayed below is the correct way to scan your finger:



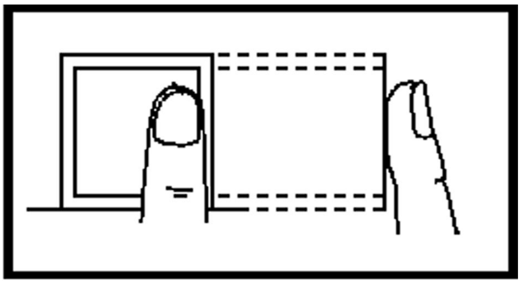
You should press your finger on the scanner horizontally. The center of your scanned finger should align with the scanner center.

Incorrect Scanning

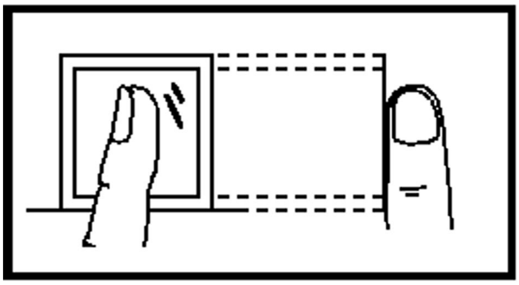
The figures of scanning fingerprint displayed below are incorrect:



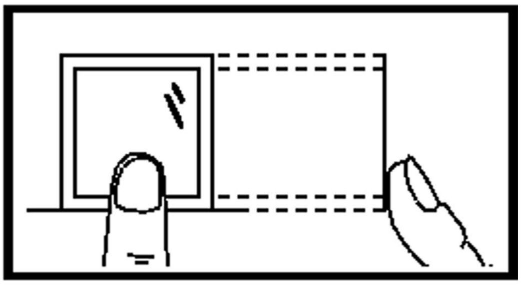
Vertical



Edge I



Side



Edge II

Environment

The scanner should avoid direct sun light, high temperature, humid conditions and rain.

When it is dry, the scanner may not recognize your fingerprint successfully. You can blow your finger and scan again.

Others

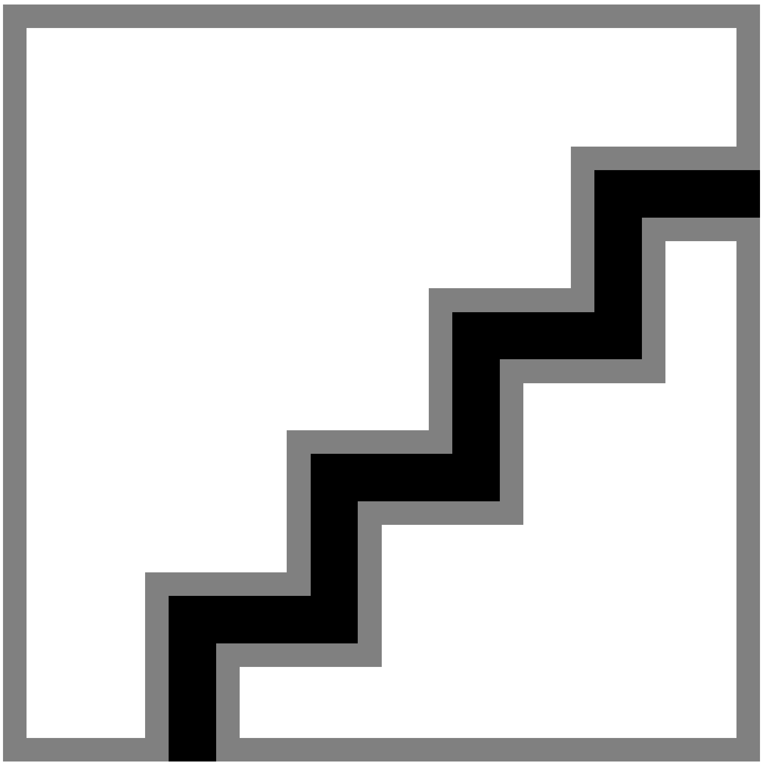
If your fingerprint is shallow, or it is hard to scan your fingerprint, we recommend you to use other authentication methods.

If you have injuries on the scanned finger, the scanner may not recognize. You can change another finger and try again.

Appendix B. Tips When Collecting/Comparing Face Picture

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

Positions (Recommended Distance: 0.5 m)



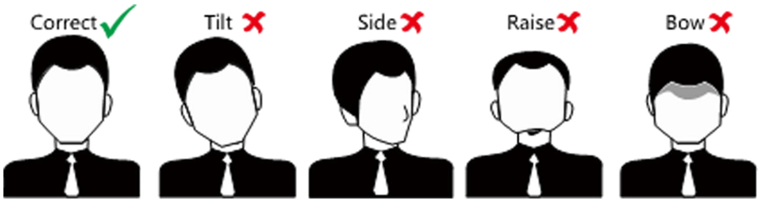
Expression

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

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

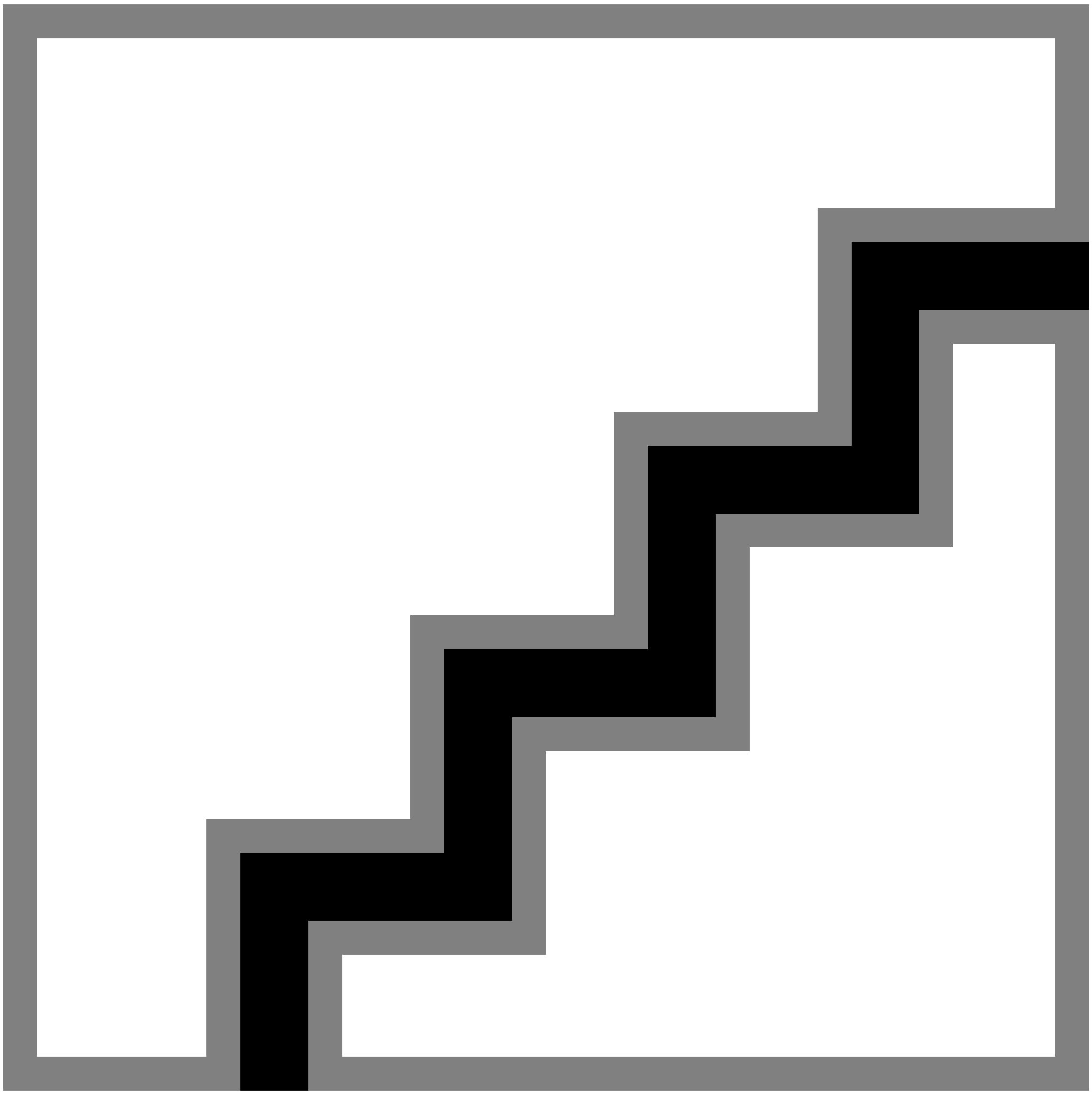
Posture

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



Size

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



Appendix C. Tips for Installation Environment

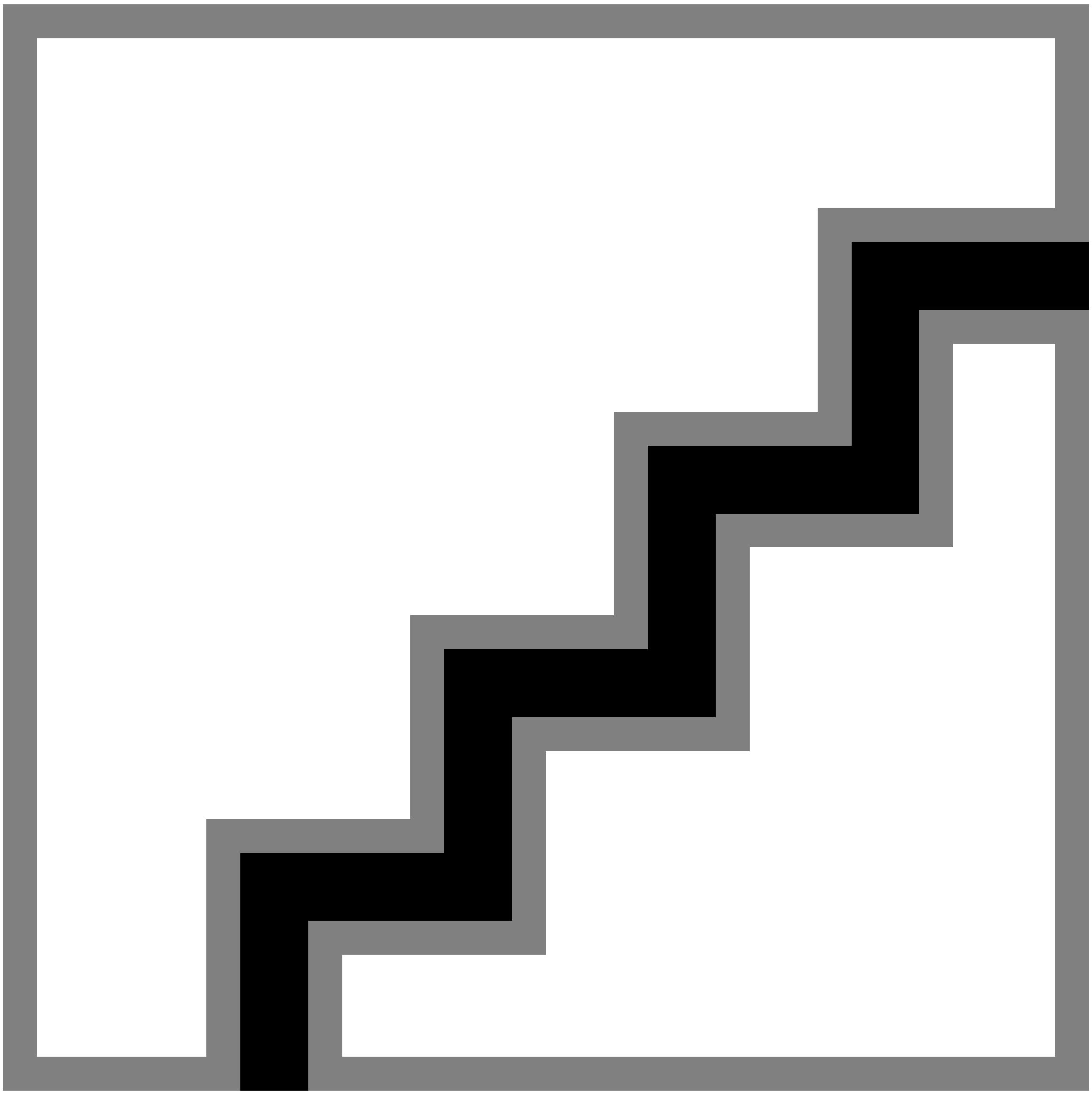
1. Light Source Illumination Reference Value

Candle: 10Lux

Bulb: 100~850Lux

Sunlight: More than 1200Lux

2. Avoid backlight, direct and indirect sunlight



Appendix D. Dimension

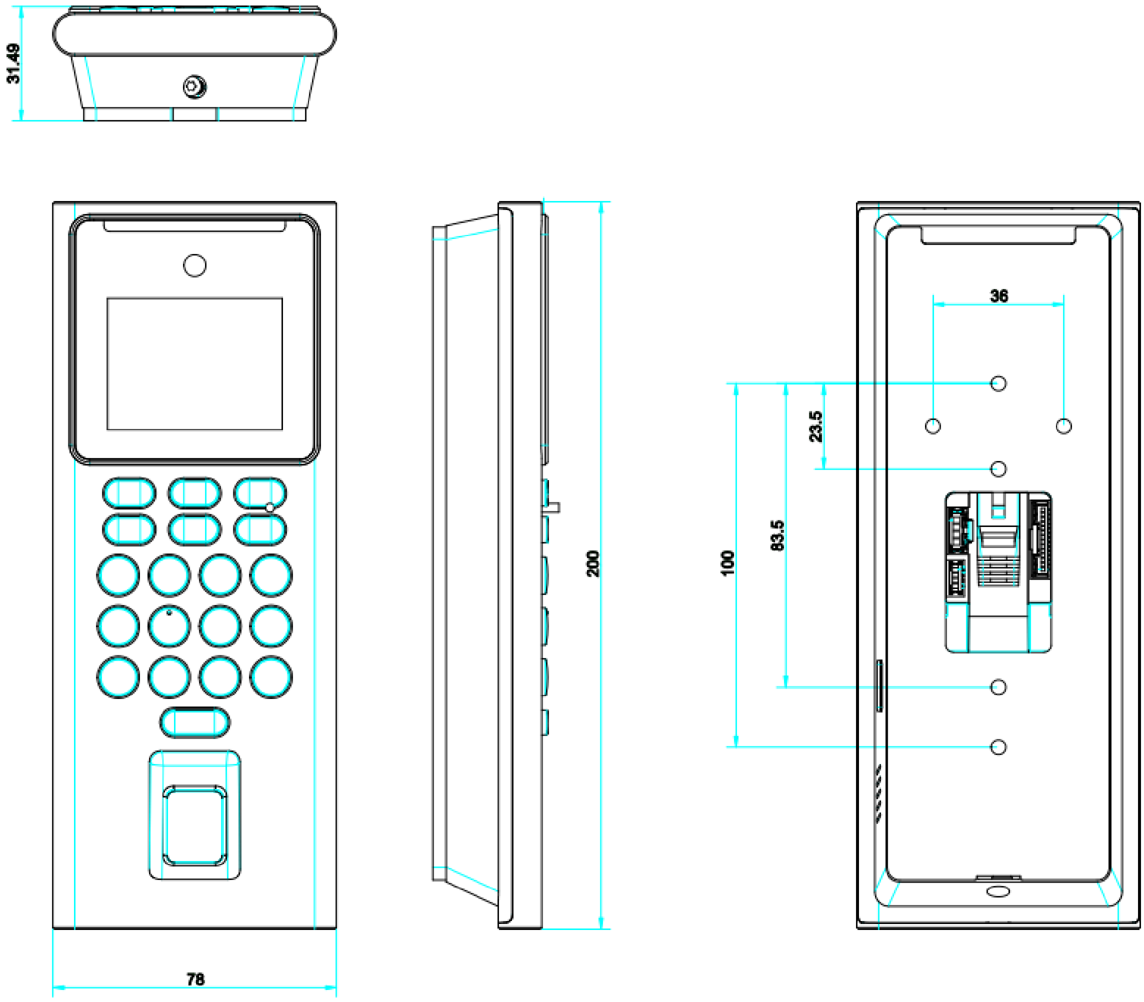


Figure D-1 Dimension

Appendix E. Communication Matrix and Device Command

Communication Matrix

Scan the following QR code to get the device communication matrix.

Note that the matrix contains all communication ports of Hikvision access control and video intercom devices.

Figure E-1 QR Code of Communication Matrix

Device Command

Scan the following QR code to get the device common serial port commands.

Note that the command list contains all commonly used serial ports commands for all Hikvision access control and video intercom devices.

Figure E-2 Device Command

See Far, Go Further