Face Recognition Terminal

Quick Start Guide

Quick Start Guide

This manual is applied for face recognition terminal.

Series	Models
Face Recognition Terminal	DS-K1T604M
	DS-K1T604MF

Note: In the model, F represents the product contains fingerprint module. M represents the product supports swiping Mifare card.

It includes instructions on how to use the Product. The software embodied in the Product is governed by the user license agreement covering that Product.

About this Manual

Trademarks

Disclaimer

Support

Should you have any questions, please do not hesitate to contact your local dealer.

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

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 RE Directive 2014/53/EU, the EMC Directive 2014/30/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 is intended for mainly home use (Class B) and may be used in all areas.
B 급 기기: 이 기기는 가정용(B 급) 전자파적합기기로써 주로 가정에서 사용하는 것을 목적으로 하며, 모든 지역에서 사용할 수 있습니다.

Use only power supplies listed in the user instructions:

Model	Manufacturer
KPL-040F-VI	Channel Well Technology Co Ltd.

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 **Warnings** and **Cautions**:

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

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

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

 **Warnings**

- All the electronic operation should be strictly compliance with the electrical safety regulations, fire prevention regulations and other related regulations in your local region.
- Please use the power adapter, which is provided by normal company. The power consumption cannot be less than the required value.
- Do not connect several devices to one power adapter as adapter overload may cause over-heat or fire hazard.
- Please make sure that the power has been disconnected before you wire, install or dismantle the device.
- When the product is installed on wall or ceiling, the device shall be firmly fixed.
- If smoke, odors or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.

- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the device yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)

Cautions

- 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.
- 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).
- Do not aim the device at the sun or extra bright places. A blooming or smear may occur otherwise (which is not a malfunction however), and affecting the endurance of sensor at the same time.
- Please use the provided glove when open up the device cover, avoid direct contact with the device cover, because the acidic sweat of the fingers may erode the surface coating of the device cover.
- Please use a soft and dry cloth when clean inside and outside surfaces of the device cover, do not use alkaline detergents.
- Please keep all wrappers after unpack them for future use. In case of any failure occurred, you need to return the device to the factory with the original wrapper. Transportation without the original wrapper may result in damage on the device and lead to additional costs.
- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.
- Biometric recognition products are not 100% applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.

Table of Contents

Chapter 1 Overview

1.1 Introduction

DS-K1T604 series 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 and so on.

1.2 Main Features

- 7-inch LCD touch screen with the screen ratio of 16:9 and the resolutions of 1024 × 600 pixel to display operation interface, view live video, etc.
- 2,000,000-pixel wide-angle dual-lens
- Adjusts supplement light brightness manually or automatically
- QR code authentication
- Face recognition distance: between 0.3 m and 1 m
- Suggested height for face recognition: between 1.4 m and 1.9 m
- Deep learning algorithm
- Max. 10,000 face storage
- Multiple authentication modes:

  Card, card and password, card or password, fingerprint, fingerprint and password, fingerprint or card, fingerprint and card, fingerprint and card and password, card or fingerprint or face or password, face and fingerprint, face and password, card and face, face, employee ID and password, fingerprint or password, employee ID and fingerprint, employee ID and fingerprint and password, card and fingerprint and face, face and fingerprint and password, employee ID and face, face and fingerprint and password, employee ID and face, face or fingerprint, card or face or password

  Note: Only products with fingerprint module support the fingerprint scanning function.
- Face recognition duration ≤ 0.5s/User; face recognition accuracy rate ≥ 99%
- Device parameters management, search, and settings
- Imports card and user data to the device via TCP/IP communication or USB flash drive
- Stand-alone operation
- Transmits data (authentication results and captured pictures) to the client software via TCP/IP communication and saves the data on the client software
- Capture linkage and captured pictures saving
- Imports data (face pictures and face templates) to the device via the USB flash drive or from the client software

- Exports data (face pictures, events, and captured pictures) from the device via the USB flash drive
- Manage, search and set device data after logging the system backend
- Connects to one external card reader or access controller via RS-485 protocol
- Connects to external access controller or Wiegand card reader via Wiegand protocol
- Connects to secure door control unit via RS-485 protocol to avoid the door opening when the terminal is destroyed
- Two-way audio

Chapter 2 Appearance

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

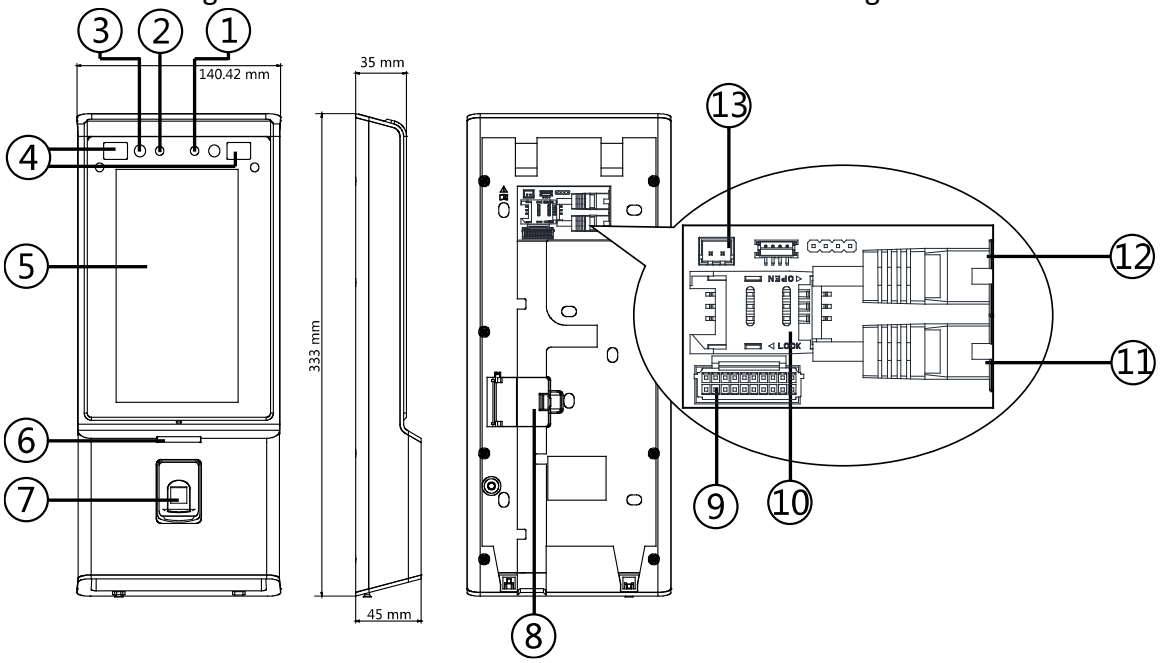


Table 2-1 Description of Face Recognition Terminal

No.	Name	Description
1	Camera (White Light)	White light camera for recording or capturing white light videos or pictures.
2	Camera (IR Light)	IR light camera for recording or capturing videos or pictures in IR light.
3	Supplement Light (IR Light)	Supplement light for IR camera.
4	Supplement Light (White Light)	Supplement light for white light camera.
5	Display Screen	7-inch LCD touch screen with the resolution of 1024 × 600.
6	Indicator	Solid Red: Standby.
		Flashing Red: Authentication failed.

		Solid Green: Authentication completed.
		Flashing Green: Authenticating (combined).
7	Fingerprint Module + Card Swiping Area	Scan fingerprint or swipe card. ***Note:*** Only the device with the fingerprint scanning function contains this part.
	Card Swiping Area	Swipe card within this area. ***Note:*** Only the device without the fingerprint scanning function contains this part.
8	PSAM Card Slot	Insert the PSAM card. The PSAM card is a card with Purchase Secure Access Module, which supports multiple secure accessing methods and permissions. It also supports communicating in a secure way.
9	Wiring Terminals	Connect to other external devices, including RS-485 card reader, Wiegand card reader, door lock, alarm input, alarm output, etc.
10	Micro SIM Card Slot	Insert SIM card.
11	Network Interface	Connect to Ethernet.
12	Network Interface	Connect to Ethernet.
13	Power Interface	Connect to power supply.

Chapter 3 Installation

Installation Environment:

- If installing the device indoors, the device should be at least 2 meters away from the light, and at least 3 meters away from the window or the door.
- Make sure the environment illumination is more than 100Lux.

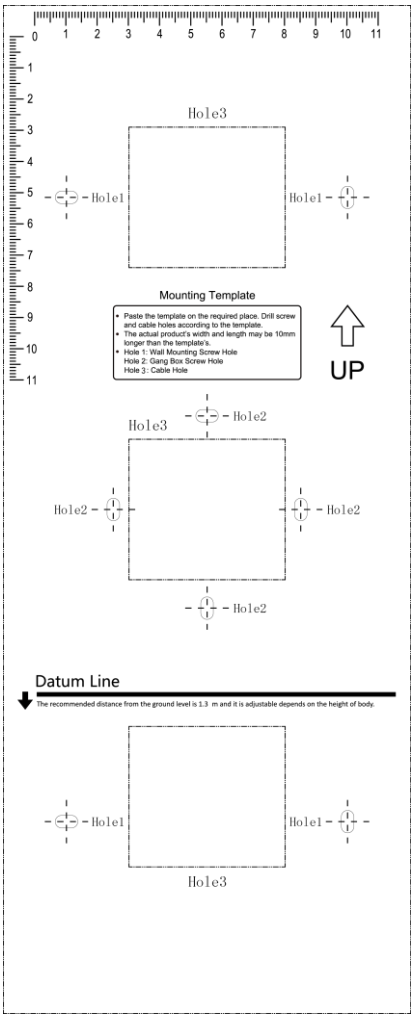
Note: For details about installation environment, see *Appendix D Tips for Installation Environment*.

Installation Types: Wall mounting with gang box and wall mounting without gang box.

3.1 Installing with Gang Box

Steps:

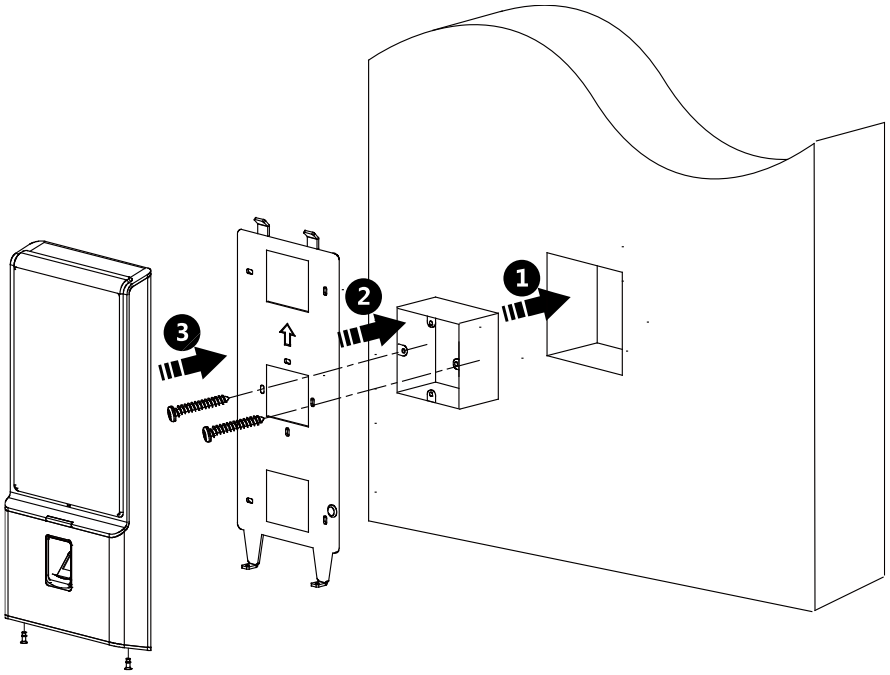
1. According to the datum line on the mounting template, stick the mounting template on the wall or other surface, 1.3 meters higher than the ground.



2. Drill holes on the wall or other surface according to the mounting template and install the gang box (80mm×80mm).
3. Use two supplied screws to secure the mounting plate on the gang box.
4. Use another four supplied screws to secure the mounting plate on the wall.
5. Remove the screw at the bottom of the device.
6. Align the terminal with the mounting plate and buckle them together.
7. Use a hex wrench to fasten the screw at the bottom.

Notes:

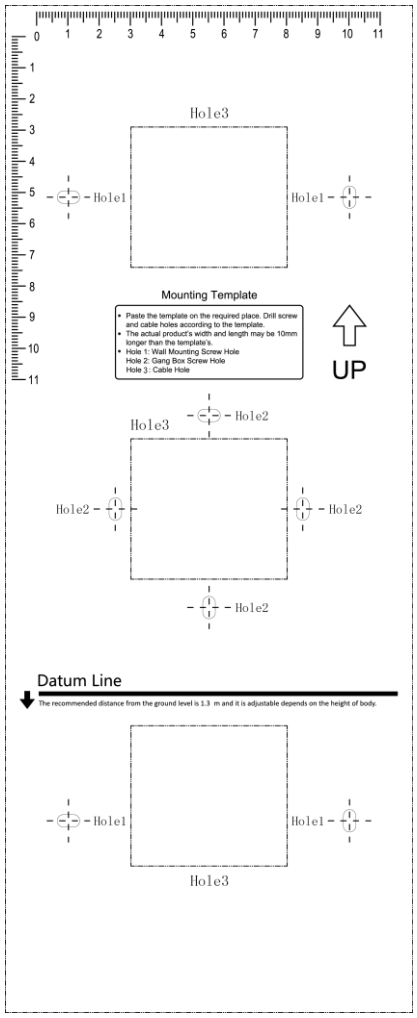
- The installation height here is the recommended height. You can change it according to your actual needs.
- For easy installation, drill holes on mounting surface according to the supplied mounting template.



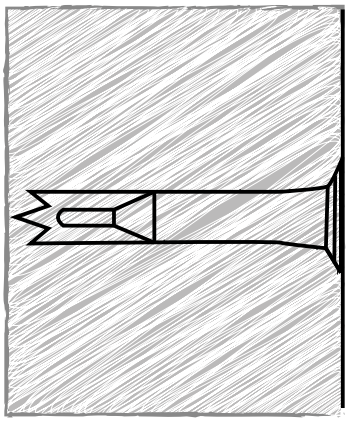
3.2 Installing without Gang Box

Steps:

1. According to the basline on the mounting template, stick the mounting template on the wall or other surface, 1.3 meters higher than the ground.

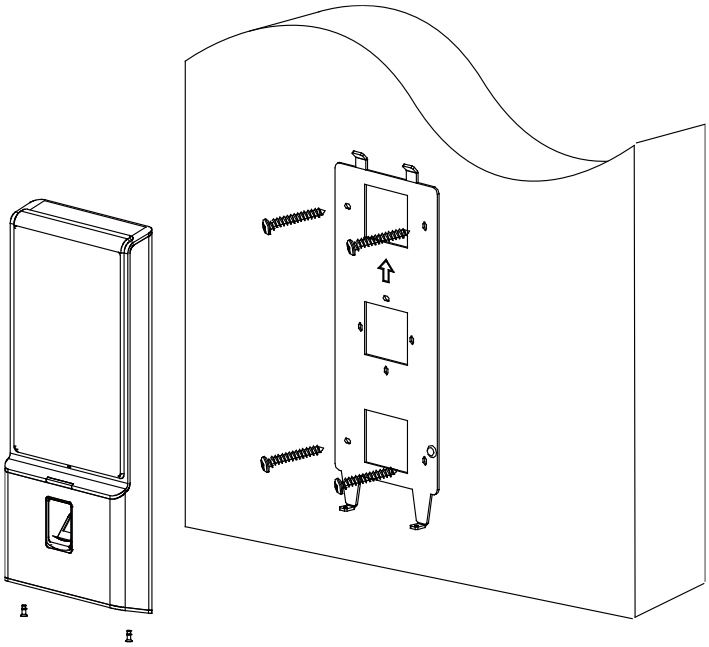


2. Drill 4 holes on the wall or other surface according to Hole 1 in the mounting template.
3. Insert the screw sockets of the setscrews in the drilled holes.



4. Align the 4 holes to the mounting plate with the drilled holes.
5. Fix and fasten the screws in the sockets on the wall or other surface.
6. Remove the two screws at the bottom of the device.
7. Align the terminal with the mounting plate and buckle them together.

8. Use a hex wrench to fasten the screw at the bottom.



Chapter 4 Terminal Connection

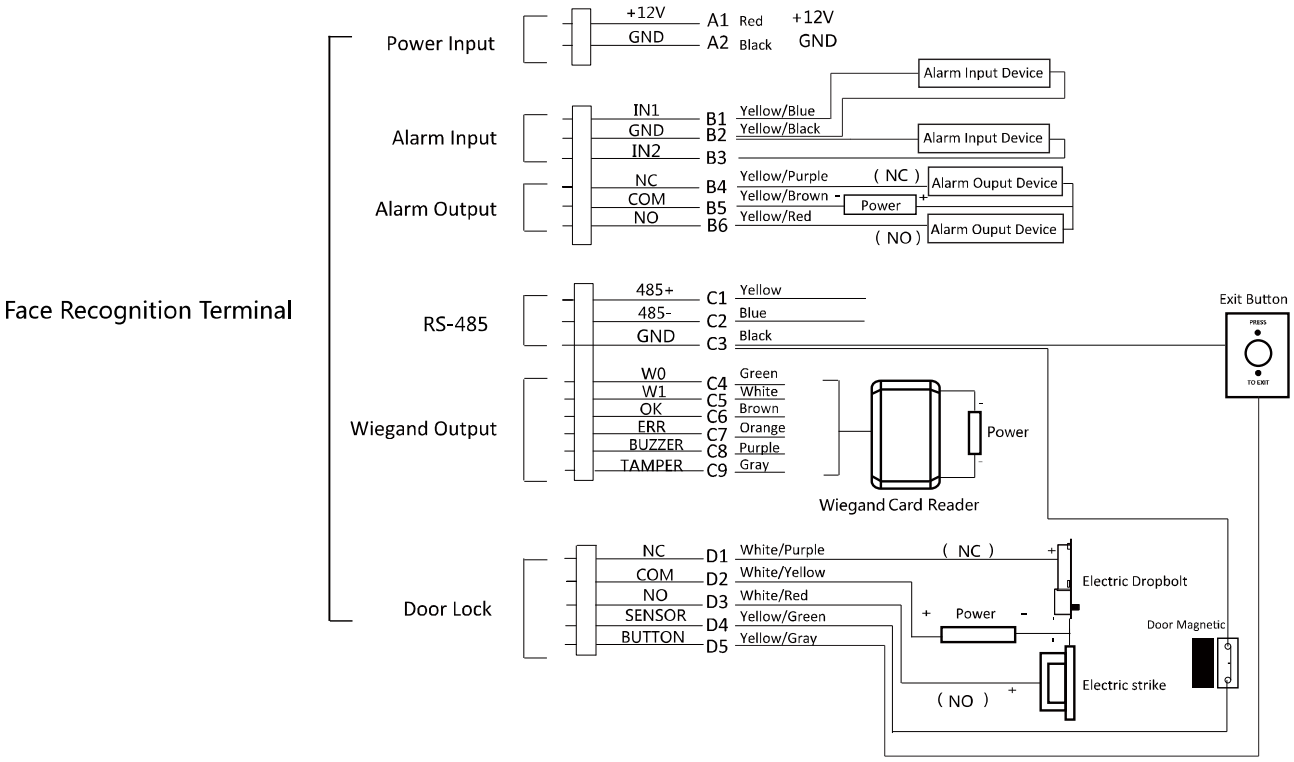
You can connect the RS-485 terminal with the RS-485 card reader, connect the NC and COM terminals with the door lock, connect the SENSOR terminal with the door magnetic sensor, connect the BUTTON/GND terminal with the exit button, connect the alarm output and input terminal with the alarm output/input devices, and connect the Wiegand terminal with the Wiegand card reader or the access controller.

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

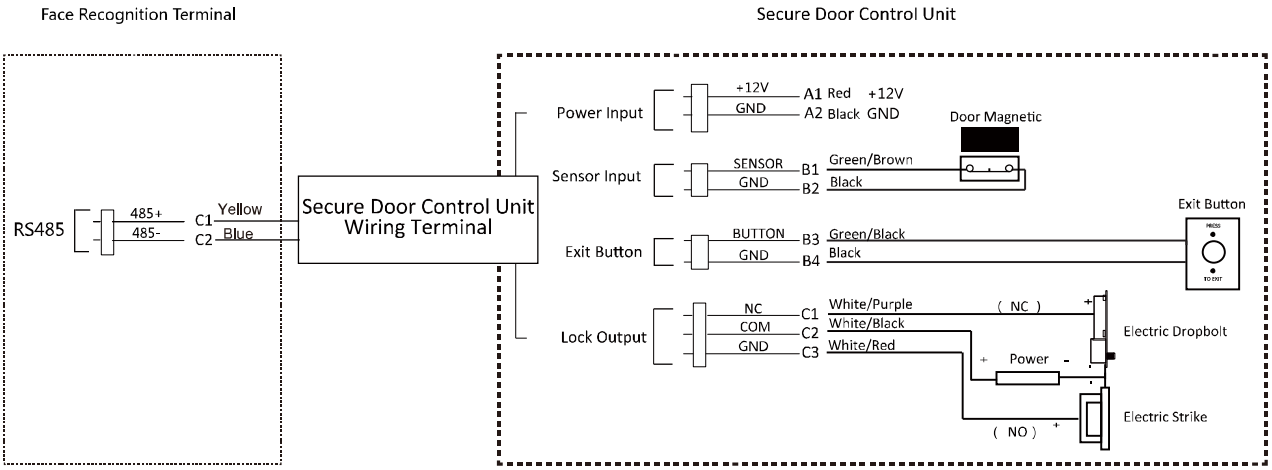
Notes:

- If you use 1.0 mm cables, you should use a 12V switched-mode power supply. And the distance between the power supply and the device should be no more than 20 m.
- If you use 1.5 mm cables, you should use a 12V switched-mode power supply. And the distance between the power supply and the device should be no more than 30 m.
- If you use 2.0 mm cables, you should use a 12V switched-mode power supply. And the distance between the power supply and the device should be no more than 40 m.

The wiring diagram is as follows:



You can also connect the terminal with the seucure door control unit. The wiring diagram is as follows:



Note: The secure door control unit should connect to an external power supply seperately.

Chapter 5 Basic Operation

5.1 Activate Device

Purpose:

You are required to activate the terminal first before using it.

Activation via device, activation via SADP, and activation via client software are supported.

The default values of the control terminal are as follows.

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

5.1.1 Activating via Device

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

Steps:

1. Tap the Password field and create a password.
2. Tap the Confirm field and input the password again.
3. Tap **Activate** and the device will be activated.

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.*

5.1.2 Activating via SADP Software

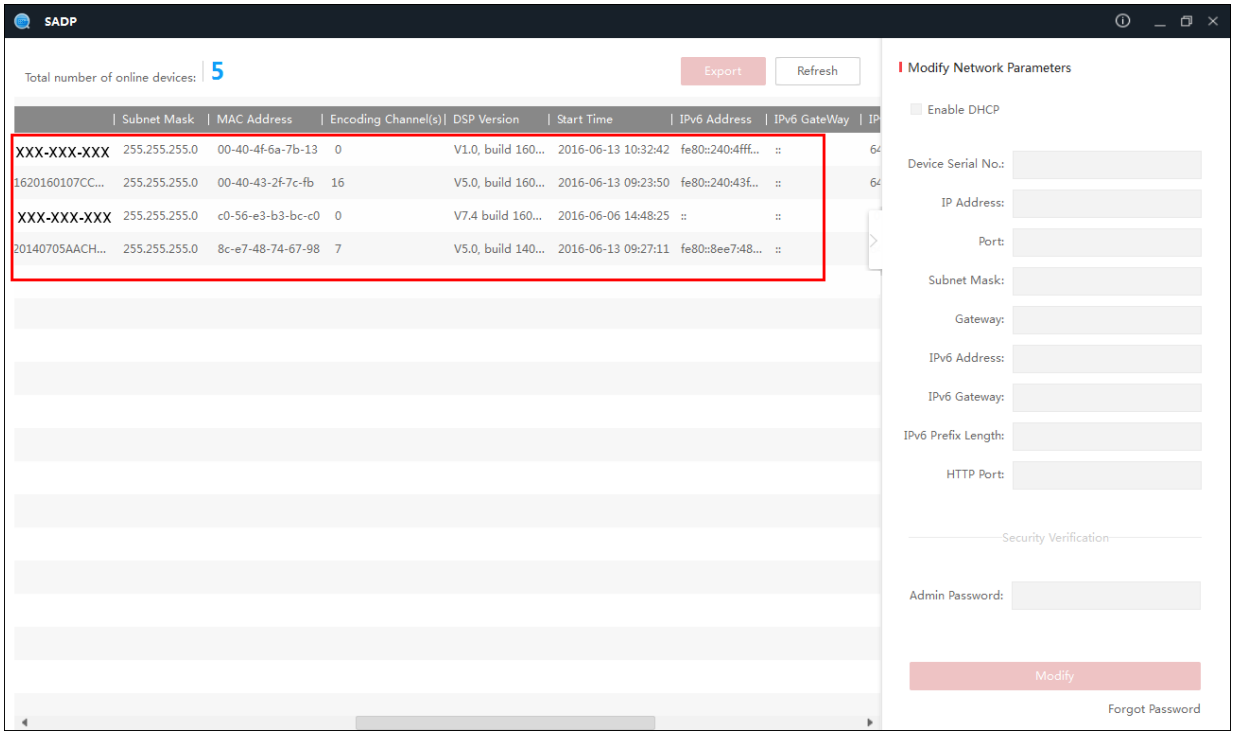
Purpose:

SADP software is used for detecting the online device, activating the device, and resetting the password.

Get the SADP software from the supplied disk or the official website, and install the SADP according to the prompts. Follow the steps to activate the device**.**

Steps:

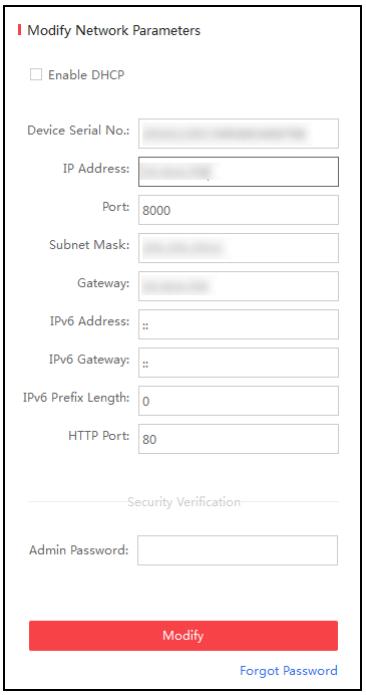
1. Run the SADP software to search the online devices.
2. Check the device status from the device list, and select an inactive device.



3. Create a password in the password field, and confirm the password.

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.*

4. Click **Activate** to activate the device.
5. Check the activated device. You can change the device IP address to the same network segment with your computer by either editing the IP address manually or checking the Enable DHCP checkbox.



6. Input the password and click **Modify** to save the IP address.

5.1.3 Activating via Client Software

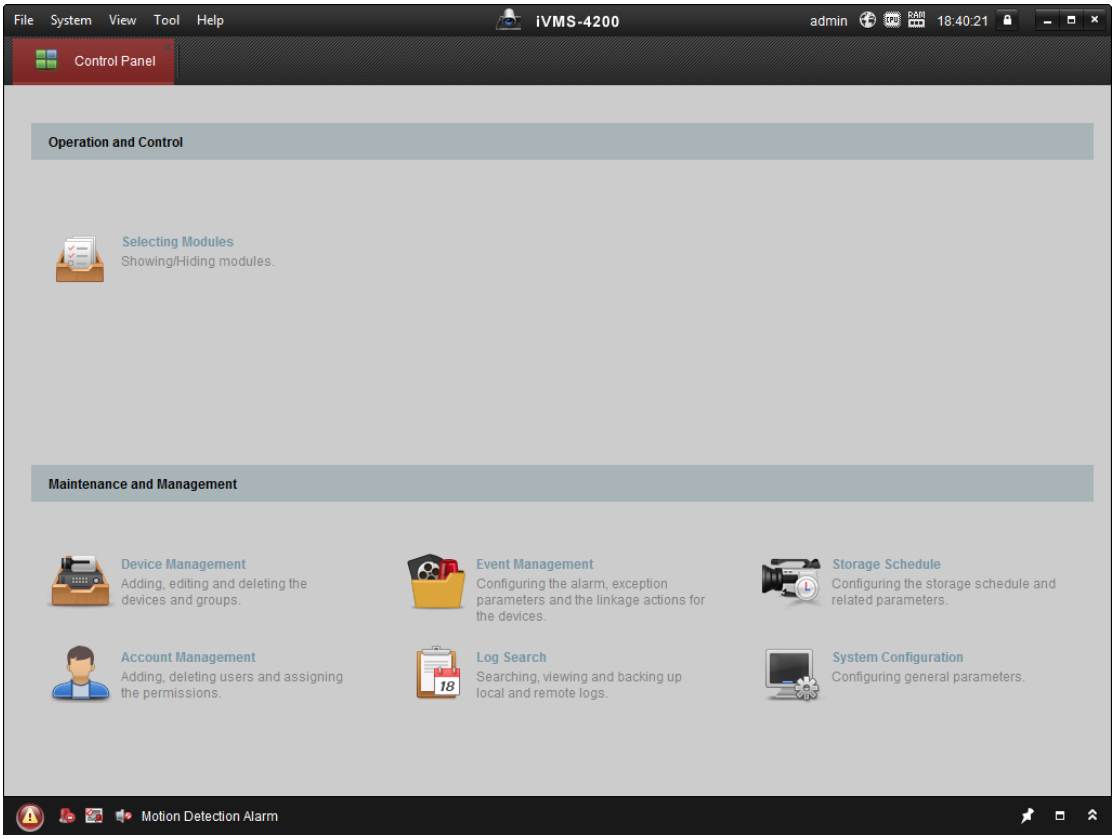
Purpose:

The client software is versatile video management software for multiple kinds of devices.

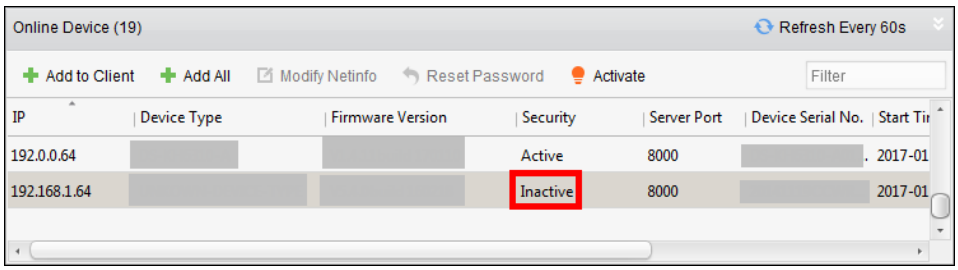
Get the client software from the supplied disk or the official website, and install the software according to the prompts. Follow the steps to activate the control panel.

Steps:

1. Run the client software and the control panel of the software pops up, as shown in the figure below.



2. Click **Device Management** to enter the Device Management interface.
3. Check the device status from the device list, and select an inactive device.



4. Check the device status from the device list, and select an inactive device.
5. Click **Activate** to pop up the Activation interface.
6. In the pop-up window, create a password in the password field, and confirm the password.

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.*

7. Click **OK** button to start activation.
8. Click the **Modify Netinfor** button to pop up the Network Parameter Modification interface.
9. Change the device IP address to the same network segment as your computer by modifying the IP address manually.
10. Input the password and click **OK** to save the settings.

After activation, you will enter the initial page.

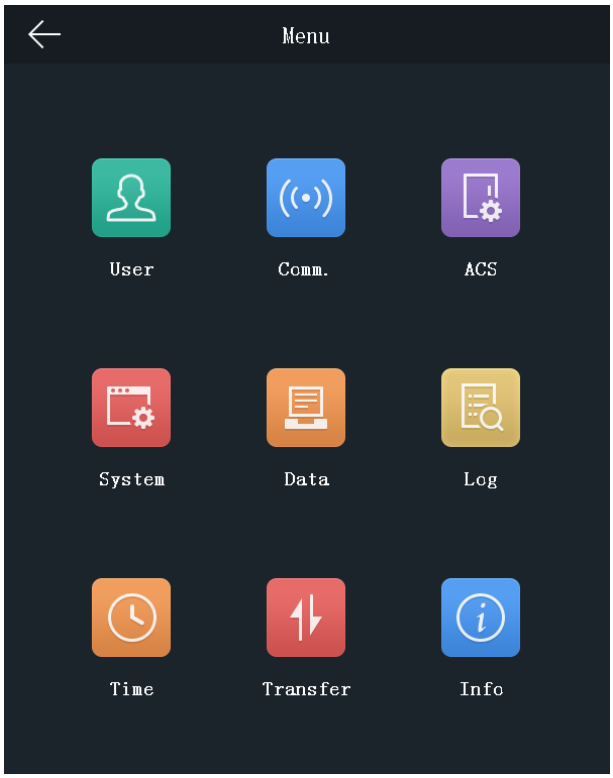
5.2 Login

You should enter the system backend first before setting the device parameters.

Steps:

1. Long tap the initial page for 3s to open the password inputting window.
2. Tap the Password field and input the device activation password.

   Note: The password here is the activation password.
3. Tap **OK** to enter the home page.



Notes:

- The device will be locked for 30 minutes after 5 failed password attempts.
- For details about setting the administrator authentication mode, see *5.4.1 Adding User*.

5.3 General Parameters Settings

5.3.1 Communication Settings

Purpose:

You can set the network parameters, the RS-485 parameters, and the Wiegand parameters on the communication settings page.

Tap **Comm.** (Communication Settings) on the Home page to enter the Communication Settings page.

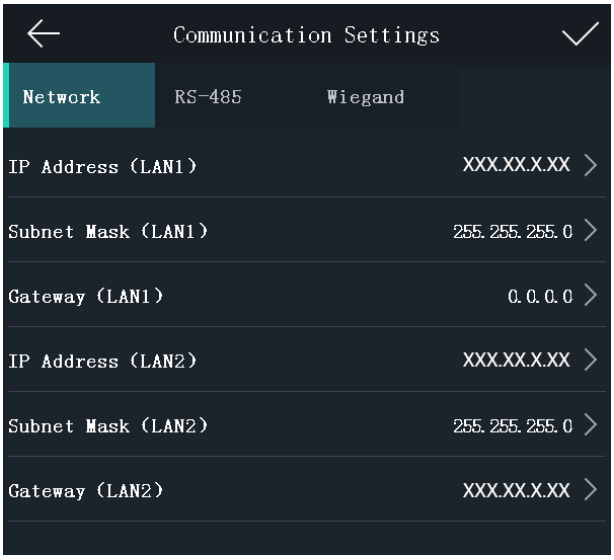
Setting Network Parameters

Purpose:

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

Steps:

1. On the Communication Settings page, tap **Network** to enter the Network tab.



2. Configure the network parameters, including IP Address, Subnet Mask, and Gateway.

   Notes:

   - The device's IP address and the computer IP address should be in the same LAN.
   - To avoid IP addresses confliction, the IP address of Network Interface 1 and 2 should be different if you want to apply both of them.

3. Tap ✓ to save the network parameters.

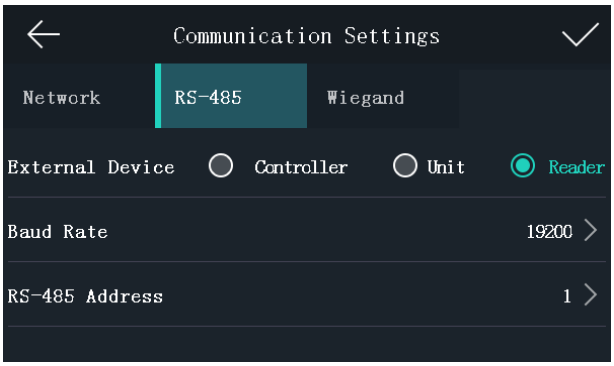
Setting RS-485 Parameters

Purpose:

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

Steps:

1. On the Communication Settings page, tap **RS-485** to enter the RS-485 tab.



2. Select an external device according to your actual needs.

   Note: Controller represents the access controller, Unit represents the secure door control unit and Reader represents the card reader.

3. Tap **Baud Rate** to enter the Baud Rate page.
4. Select a baud rate for connecting external device via RS-485 protocol.
5. In the Communication Settings page, select an RS-485 address.
6. Tap ✓ to save the RS-485 parameters and go back to the Home page.

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

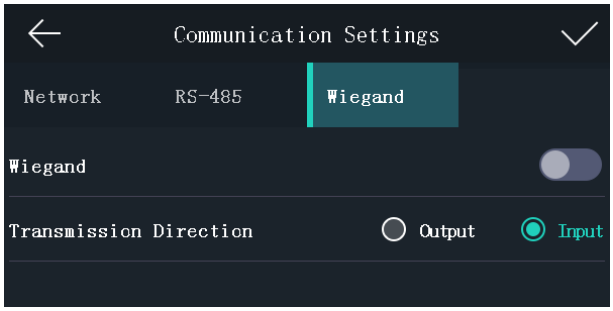
Setting Wiegand Parameters

Purpose:

You can set the Wiegand transmission direction.

Steps:

1. On the Communication Settings page, tap **Wiegand** to enter the Wiegand tab.



2. Tap the slider to enable the Wiegand function.
3. Select the transmission direction.

   Transmission Direction:

   - Output: A face recognition terminal can connect an external access controller. And the two devices will transmit the card No. via Wiegand 34.
   - Input: A face recognition terminal can connect a Wiegand card reader.
4. Tap ✓ to save the Wiegand parameters and go back to the Home page.

5.3.2 System Settings

Purpose:

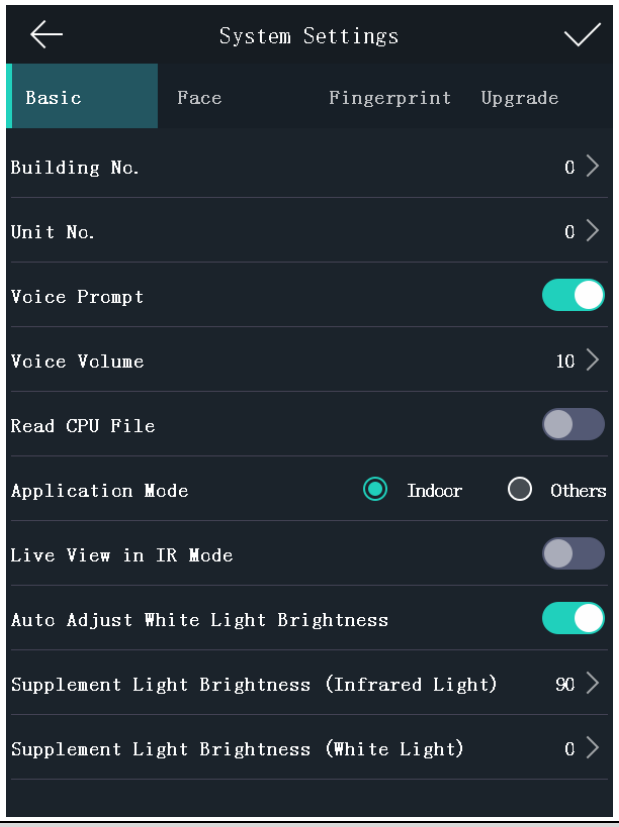
On the System Settings page, you can set the system basic parameters, the face parameters, the fingerprint parameters, and upgrade the firmware.

On the Home page, tap **System** (System Settings) to enter the System Settings page.

Setting Basic Parameters

Purpose:

You can set the building No. and the unit No., voice prompt, voice volume, read CPU file, application mode, live view in IR mode, auto adjust white light brightness, supplement light brightness (Infrared Light), and supplement light brightness (white light).



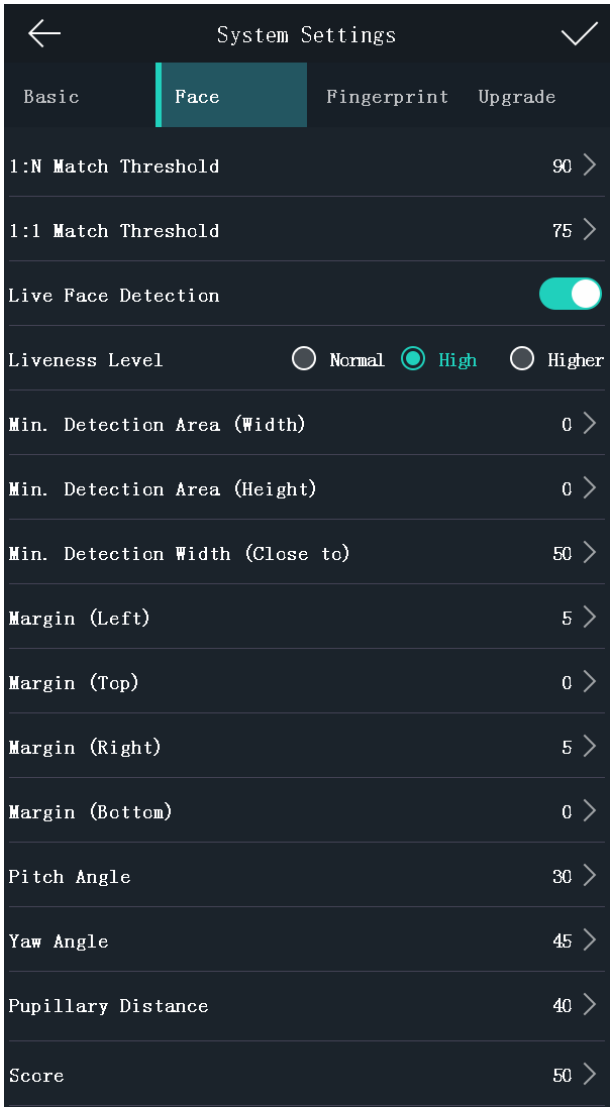
Parameter	Description
Building No.	Set the device installed building No.
Unit No.	Set the device installed Unit No.
Voice Prompt	Tap  or  to disable or enable the voice promt.
Voice Volume	Adjust the voice volume. The larger the value, the louder the volume.
Read CPU File	If the device supports swiping CPU card, you can enable the function and the device can read the CPU card information.
Application Mode	You can select either others or indoor according to actual environment.
Live View in IR Mode	The live view on the device screen will enter the IR mode.
Auto Adjust White Light Brightness	If enabling the function, the device will auto adjust the white light brightness according to the illumination. If disabling the function, the white light will turn on all the time and the brightness is the configured value of the supplement light brightness (white light).
Supplement Light Brightness (Infrared Light)	Set the IR light brightness when the IR light is enabled.
Supplement Light Brightness (White Light)	Set the supplement white light's brightness. The brightness ranges from 0 to 100. 0 refers to turning off the light. 1 refers to the darkest, and 100 refers to

	the brightest.

Setting Face Parameters

Purpose:

You can set the face 1:N match threshold, 1:1 match threshold, live face detection, liveness level, min. detection area (width), min. detection area (height), min. detection width (close to), margin (left), margin (top), margin (right), margin (bottom), pitch angle, yaw angle, pupillary distance, and score.



Parameter	Description
1:N Match 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 when authentication. By default, the value is 84.
1:1 Match 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

Parameter	Description
	authentication. By default, the value is 75.
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. ***Note:*** Biometric recognition products are not 100% applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.
Liveness Level (Liveness Security Level)	After enabling Live Face Detection function, you can set the matching security level when performing live face authentication.
Min. Detection Area (Width)	When the distance between the camera and the user is long, the parameter represents the minimum percentage of the facial width in the total width of the recognition area. The actual percentage should be larger than the configured value when starting face authentication. Other percentages, distances and angles in this table should also meet their conditions. Recommended Value: 14
Min. Detection Area (Height)	When the distance between the camera and the user is long, the parameter represents the minimum percentage of the facial height in the total height of the recognition area. The actual percentage should be larger than the configured value when starting face authentication. Other percentages, distances and angles in this table should also meet their conditions. Recommended Value: 12
Min. Detection Width (Close to)	When the distance between the camera and the user is short, the parameter represents the minimum percentage of the facial width in the total width of the recognition area. The actual percentage should be larger than the configured value when starting face authentication. In this condition, the device will not detect other parameters.
Margin (Left)	The distance from the face left side to the left margin in the recognition area. The actual distance should be larger than the configured value when starting face authentication. Other percentages, distances, and angles should also meet their conditions.
Margin (Top)	The distance from the face top side to the top margin in the recognition area. The actual distance should be larger than the configured value when starting face authentication. Other percentages, distances, and angles should also meet their conditions.
Margin (Right)	The distance from the face right side to the right margin in

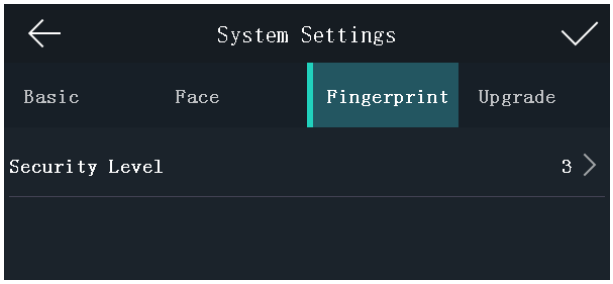
Parameter	Description
	the recognition area. The actual distance should be larger than the configured value when starting face authentication. Other percentages, distances, and angles should also meet their conditions.
Margin (Bottom)	The distance from the face bottom side to the bottom margin in the recognition area. The actual distance should be larger than the configured value when starting face authentication. Other percentages, distances, and angles should also meet their conditions.
Pitch Angle	The maximum pitch angle when starting face authentication. By default, the angle is 30°.
Yaw Angle	The maximum yaw angle when starting face authentication. By default, the angle is 45°.
Pupillary Distance	The minimum resolution between two pupils when starting face recognition. The actual resolution should be larger than the configured value. By default, the resolution is 40.
Score	Set the face's score when recognition. 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 is failed.

Setting Fingerprint Parameters

Purpose:

You can set the fingerprint security level in this section.

Note: Only the device with the fingerprint scanning function supports the fingerprint related function.



Parameter	Description
Security Level :	You can select the fingerprint security level. The higher is the security level, the lower is the false acceptance rate (FAR). The higher is the security level, the higher is the false rejection rate (FRR).

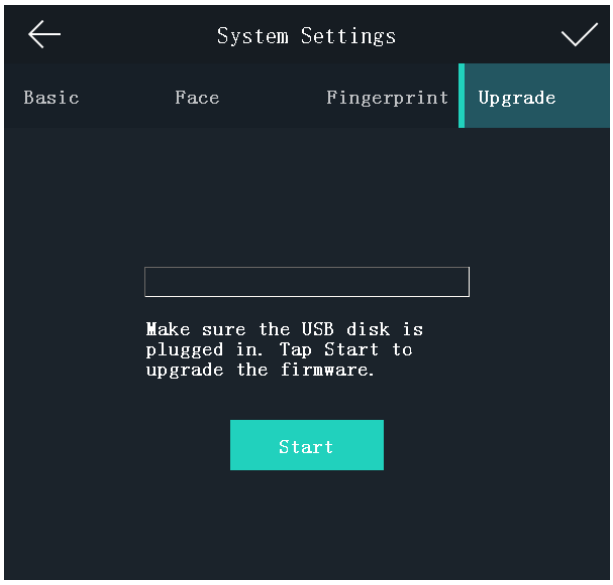
Upgrading Firmware

On the Upgrade page, plug in the USB flash drive and tap **Start**. The device will automatically read

the upgrading file in the USB flash drive and upgrade the firmware.

Note:

- The upgrading file should be in the root directory.
- The upgrading file name should be digicap.dav.



5.3.3 Setting Time

Purpose:

You can set the device time and the DST in this section.

Steps:

1. Tap **Time** (Time Settings) on the Home page to enter the Time Settings page.
2. Edit the time parameters.

Parameter	Description
Time	Set the time which will be displayed on the device screen.
DST	Enable or disable the DST function. If enabling the DST function, you can set the DST start time, end time, and the bias time. **Start Time:** Set the DST start time. **End Time:** Set the DST end time. **Bias Time:** Set the DST bias time when the DST starts.

3. Tap  to save the settings and go back to the Home page.

5.4 User Management

Purpose:

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

Tap **User** on the Home page to enter the User Management page.

5.4.1 Adding User

Purpose:

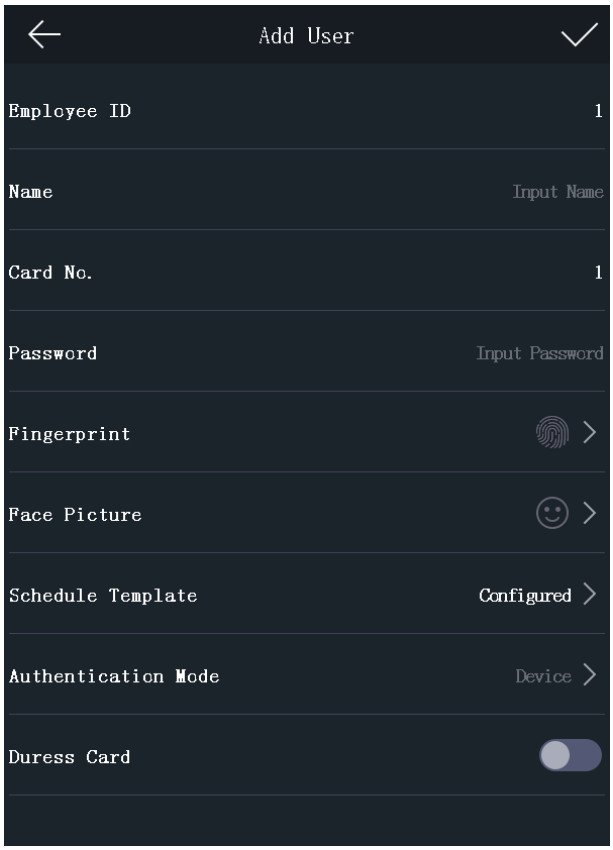
On the Add User page, you can add users, including the employee No., name, card No. You can also link the fingerprint, the face picture to the user, or set password, authentication mode, schedule template, administrator permission for the user.

Notes:

- Up to 50000 users can be added.
- The device with the model of DS-K1T604M does not support the fingerprint related function.

Steps:

1. On the User Management page, tap **+** to enter the Add User page.



2. Tap the **Employee ID.** field and edit the employee ID.

   Notes:

   The employee ID should be between 1 and 99999999. The employee ID should not start with 0 and should not be duplicated.

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

   Notes:

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

4. Tap the **Card** field and input the card No.

   Option 1: Input the card No. manually.

   Option2: Swipe the card over the card swiping area to get the card No.

   Notes:

   - The card No. cannot be empty.
   - Up to 20 characters are allowed in the card No.
   - By default, the card No. contains 10 characters. The system will use 0 to supplement the 10-character-card No. For example, 5 and 0000000005 are two different card No.
   - The card No. cannot be duplicated.

5. Tap the **Password** field and create a password and confirm the password.

   Note:

   - Only numbers are allowed in the password.
   - Up to 8 characters are allowed in the password.

6. Tap the **Fingerprint** field to enter the Add Fingerprint page.

   Follow the steps below to add fingerprint.

   1) Place your finger on the fingerprint module.
   2) Follow the instructions on the screen to record the fingerprint.
   3) After adding the fingerprint completely, tap **Yes** in the pop-up dialog to save the fingerprint and continue to add another fingerprint.

      Or tap **No** to save the fingerprint and go back to the Add User page.

      Notes:

      - 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 Appendix B Tips for Scanning Fingerprint.

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

   Follow the steps below to add the user's face picture.

   1) Position your face looking at the camera.

      Note: Make sure your face picture is in the face picture outline when adding the face picture.

      After completely adding the face picture, a captured face picture will display on the page.

      Notes:

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

2) Tap **Save** to save the face picture.

Or tap **Try Again** and adjust your face position to add the face picture again.

Note: The maximum duration for adding a face picture is 15s. You can check the remaining time for adding a face picture on the left of the page.

8. Tap the **Schedule Template** field to enter the Schedule Template page. Select a schedule template and tap ✓ to save the settings.

   Note: For details about setting the schedule template, see the *User Manual of Face Recognition Terminal*. After applying the schedule tem plate from the client software to the devce, you can select the corresponding schedule template

9. Tap **Authentication Mode** to enter the Authentication Mode page. Select **Device** or **Custom** as the authentication mode.

   Device: If you want to seelct device mode, you should set the terminal authentication mode in Acess Control Settings page first. For details see *5.5 Setting Access Control Parameters*.

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

10. Enable or disable the **Duress Card** function.

    When the function is enabled, the user's card will be the duress card. When the user authenticates by swiping this duress card, the device will upload an duress card event to the client software.

11. Tap ✓ to save the user parameters and go back to the Home page.

5.4.2 Managing User

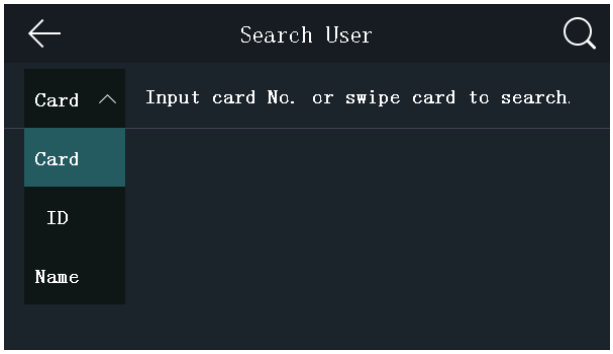
Searching User

Purpose:

You can search the user in the list according to the employee ID, the card No., or the user name.

Steps:

1. On the User Management page, Tap  to enter the Search User page.



2. Tap **Card** on the left of the page and select a search type from the drop-down list.
3. Tap the input box and input the employee ID, the card No., or the user name for search.
4. Tap  to start search.

   The searching result will be displayed in the list below.

Editing User

Purpose:

You can edit the added user information by following the steps in this section.

Steps:

1. In the User Management page, tap the user that needs to be edited to enter the Edit User page.
2. Refer to the parameters' instructions in *Section 5.4.1 Adding User* to edit the user information.
3. Tap √ to save the settings and go back to the User Management page.

   Note: The employee ID cannot be edited.

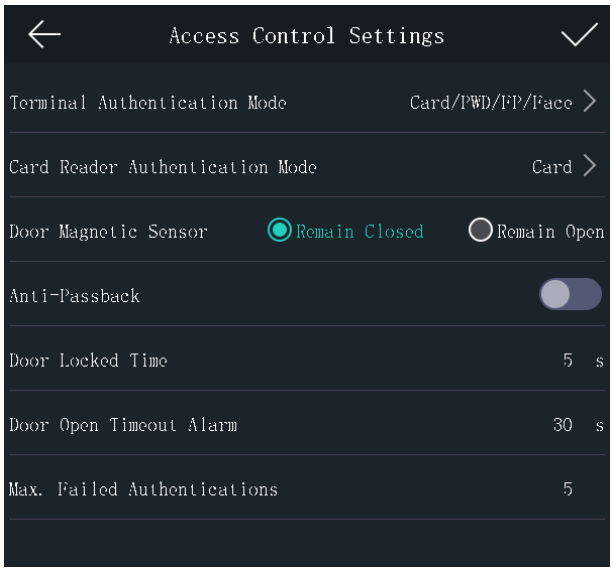
5.5 Setting Access Control Parameters

Purpose:

You can set the access control permissions, including the functions of authentication mode, door magnetic sensor, anti-passback, door locked time, door open timeout alarm, and max. failed authentications.

Steps:

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



2. Edit the access control parameters.

   The available parameters descriptions are as follows:

Parameter	Description
Terminal Authentication Mode	Select the face recognition terminal's authentication mode. You can also customize the authentication mode. ***Notes:*** ● Only the device with the fingerprint scanning function supports the fingerprint related function.

Parameter	Description
	● Biometric recognition products are not 100% applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.
Card Reader Authentication Mode	Select the card reader's authentication mode.
Door Magnetic Sensor	You can select **Remain Open** or **Remain Closed** according to your actual needs. By default, it is Remain Closed.
Anti-Passback	When enabling the anti-passback function, you should set the anti-password path in the iVMS-4200 Client Software. The person should authenticate according to the configured path. Or the authentication will be failed.
Door Locked Time	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.
Door Open Timeout Alarm	The alarm can be triggered if the door has not been closed. Available range: 0 to 255s.
Max. Failed Authentications	Set the maximum authentication times. If you failed to authenticate for the set times, the alarm will be triggered.

3. Tap ✓ to save the settings.

5.6 Other Management

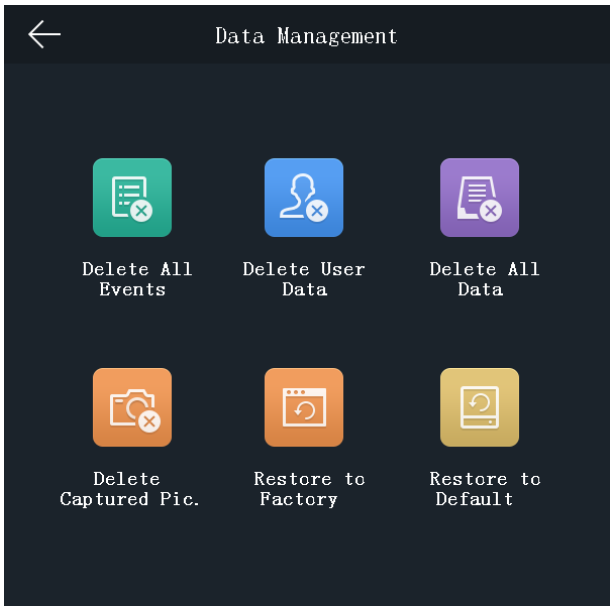
5.6.1 Managing Data

Purpose:

On the Data Management page, you can delete all events, delete user data, delete all data, clear permissions, delete captured pictures, restore to factory settings, or restore to default settings.

Steps:

1. Tap **Data** (Data Management) to enter the Data Management page.



2. Tap the button on the page to manage data.
   The available button descriptions are as follows:

Parameter	Description
Delete All Events	Delete all events stored in the device.
Delete User Data	Delete all user data in the device.
Delete All Data:	Delete all user data and events stored in the device.
Delete Captured Pic.	Delete the device captured pictured.
Restore to Factory	Restore the system to the factory settings. The device will reboot after the setting.
Restore to Default	Restore the system to the default settings. The system will save the communication settings and the remote user settings. Other parameters will be restored to default.

3. Tap **Yes** on the pop-up window to complete the settings.

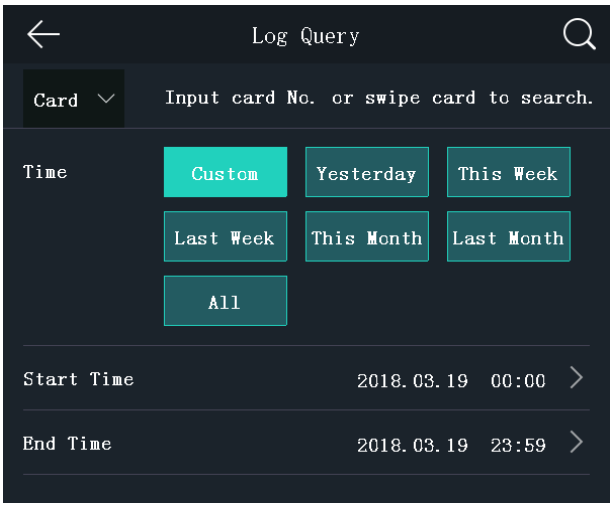
5.6.2 Managing Log Query

Purpose:

You can search the authentication logs within a period of time by inputting employee ID, card No., or user name.

Steps:

1. On the Home page, tap **Log** (Log Query) to enter the Log Query page.



2. Tap **Card** on the left of the page and select a search type from the drop-down list.
3. Tap the input box and input the employee ID, the card No., or the user name for search.
4. Select time.

   You can select from **Custom**, **Yesterday**, **This Week**, **Last Week**, **This Month**, **Last Month**, or **All**.

   If you select **Custom**, you can customize the start time and the end time for search.
5. Tap  to start search.

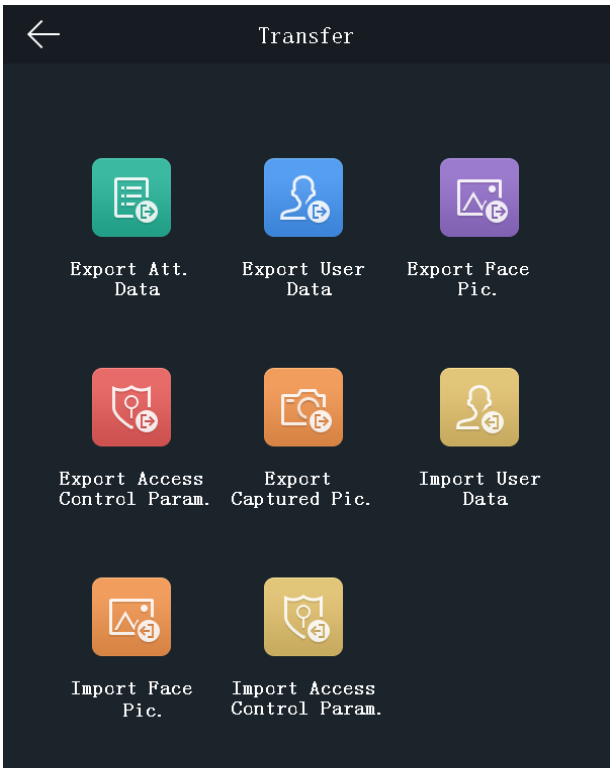
   The result will be displayed in the page.

5.6.3 Importing/Exporting Data

Purpose:

On the Transfer page, you can export the attendance data, the user data, the user picture, the access control parameter, and the captured picture to the USB flash drive. You can also import the user data, the user picture, and the access control parameter from the USB flash drive.

Tap **Transfer** on the Home page to enter the Transfer page.



Exporting Data

Steps:

1. Plug a USB flash drive in the device.
2. On the Transfer page, tap **Export Att. Data**, **Export User Data**, **Export Face Pic.**, **Export Access Control Param.**, or **Export Captured Pic**.
3. Tap **Yes** on the pop-up page and the data will be exported from the device to the USB flash drive.

   Notes:

   - The supported USB flash drive format is FAT 32.
   - 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 BIN file, which cannot be edited

Importing Data

Steps:

1. Plug a USB flash drive in the device.
2. On the Transfer page, tap **Import User Data**, **Import Face Pic.**, or **Import Access Control Param**.
3. Tap **Yes** on the pop-up window and the data will be imported from the USB flash drive to the device.

   Notes:

   - 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 FAT 32.
- The imported picture should be saved in the root directory (enroll_pic) and the picture file's name should be follow the rule below:

  Card No._Name_Department_Employee ID_Gender.jpg
- The employee ID should between 1 and 99999999, should not be duplicated, and should not start with 0.
- Requirements of face: It should be taken in full-face view directly facing the camera. Do not wear a hat or head covering when taking the face picture. The format should be JPEG or JPG. The resolution should be 640 × 480 pixel or more than of 640 × 480 pixel. The picture size should be between 60 KB and 200 KB.

5.6.4 Viewing System Information

Viewing Capacity

Purpose:

You can view the added user's number, the face picture's number, the card's number, the password's number, and the fingerprint's number.

Note: The device with the model of DS-K1T604M does not support displaying the fingerprint capacity.

Tap **Info.** (System Information) **-> Capacity** on the Home page to enter the Capacity page.

Viewing Device Information

Purpose:

You can view the device model, the serial No., the MAC address, the firmware version, the MCU version, and the production date.

Tap **Device** to enter the Device page.

Note: The device information page may vary according to different device models.

5.7 Authenticating Identity

Purpose:

After setting network, system parameters and adding user, you can go back to the initial page for identity authentication.

The system will authenticate person according to the configured authentication mode.

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

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

1:N Matching: Compare the captured face picture or the collected fingerprint picture with all face pictures or all fingerprint pictures stored in the device

1: 1 Matching: When swiping card, compare the captured face picture or the collected fingerprint with the information stored in the card.

5.7.1 Authenticating via 1:1 Matching

Steps:

1. If the authentication mode is Card and Face, Card and Face and Fingerprint, or Auto, swipe card in the card swiping area.

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

   If the QR Code Scanning function is enabled, you can put the QR code in front of the device camera to authenticate via QR code.
2. If the authentication mode is Card and Face, or Auto, position the face looking at the camera to authenticate face.

   If the authentication mode is Card and Face and Fingerprint, after authenticating face completely, authenticate the fingerprint on the fingerprint module when the prompt "Continue to authenticate" will pop up.

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

   Notes:

   - For better face authentication, the user height should between 140 cm and 190 cm and the distance between the user and the device should be between 30 cm and 100 cm.
   - For detailed information about scanning fingerprint, see *Appendix B Tips for Scanning Fingerprint*.
   - For detailed information about authenticating face, see *Appendix C Tips When Collecting/Comparing Face Picture*.

5.7.2 Authenticating via 1:N Matching

If the authentication mode is Face or Auto, position the face looking at the camera to start face authentication.

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

5.7.3 Authenticating via 1:1 Matching and 1:N Matching

Steps:

1. If the authentication mode is Fingerprint and Face, authenticate fingerprint first according to the prompt on the device screen.

   The device will compare the fingerprint with the fingerprint information in the device database (1:N Matching).

   If authentication completed, a prompt "Continue to authenticate" will pop up.
2. Front the face looking at the camera to start face authentication.

The device will compare the captured face picture with the user information gained from the last step (1:1 Matching).
If authentication completed, a prompt "Authenticated" will pop up.

Notes:

- For better face authentication, the user height should between 140 cm and 190 cm and the distance between the user and the device should be between 30 cm and 100 cm.
- For detailed information about scanning fingerprint, see *Appendix B Tips for Scanning Fingerprint*.
- For detailed information about authenticating face, see *Appendix C Tips When Collecting/Comparing Face Picture.*

5.8 Two-way Audio

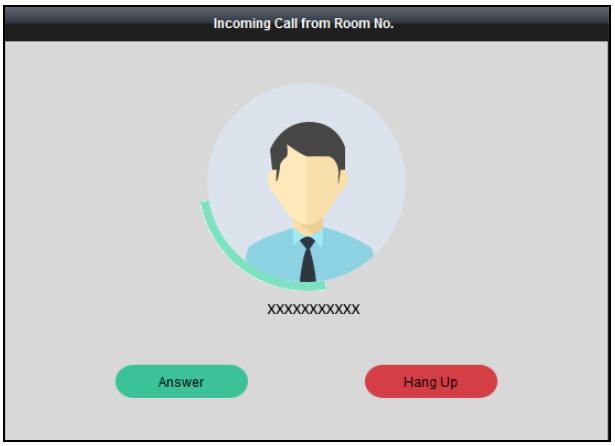
Purpose:

After adding the device to the iVMS-4200 client software, you can call the device from the client software or call the client software from the device.

5.8.1 Calling iVMS-4200 Client Software from Device

Steps:

1. Get the client software from the supplied disk or the official website, and install the software according to the prompts.
2. Run the client software and the control panel of the software pops up.
3. Click **Device Management** to enter the Device Management interface.
4. Add the device to the client software.
   Note: For details about adding device, see *Adding Access Control Device* in the user manual.
5. Call the client software.
   1) Tap **Call** on the device initial page.
   2) Input **0** in the pop-up window.
   3) Tap **Call** to call the client software.
6. Tap **Answer** on the pop-up page of the client software and you can start two-way audio between the device and the client software.
   Note: If the device is added by multiple client softwares and when the device is calling the client software, only the first client software added the device will pop up the call receiving window.



5.8.2 Calling Device from iVMS-4200 Client Software

Steps:

1. Get the client software from the supplied disk or the official website, and install the software according to the prompts.
2. Run the client software and the control panel of the software pops up.
3. Click **Device Management** to enter the Device Management interface.
4. Add the device to the client software.
   Note: For details about adding device, see *Adding Access Control Device* in the user manual.
5. Enter the Live View page and double-click the added device to start live view.
   Note: For details about operations in the Live View page, see *Live View* in the user manual.
6. Right click the live view image to open the right-click menu.
7. Click **Start Two-Way Audio** to start two-way audio between the device and the client software.

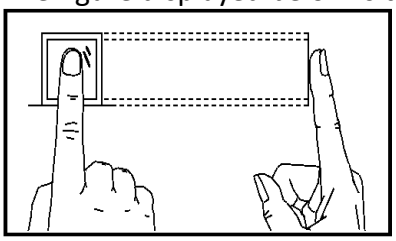
Appendix B Tips for Scanning Fingerprint

Recommended Finger

Forefinger, middle finger or the third finger.

Correct Scanning

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

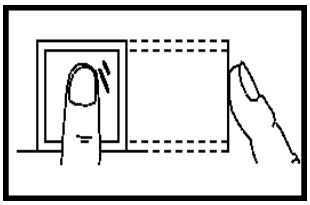


You should press your finger on the scanner horizontally. The center of your scanned finger should align with the scanner center.

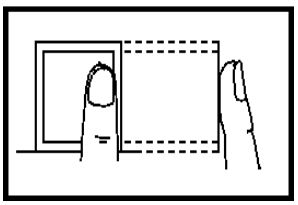
Incorrect Scanning

The figures of scanning fingerprint displayed below are wrong:

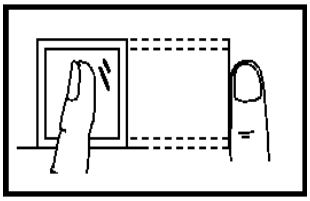
Vertical



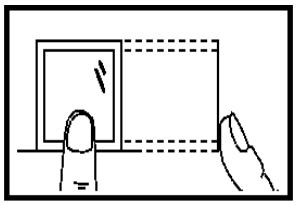
Edge I



Side



Edge II



Environment

The scanner should avoid direct high 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 after drying the finger.

Others

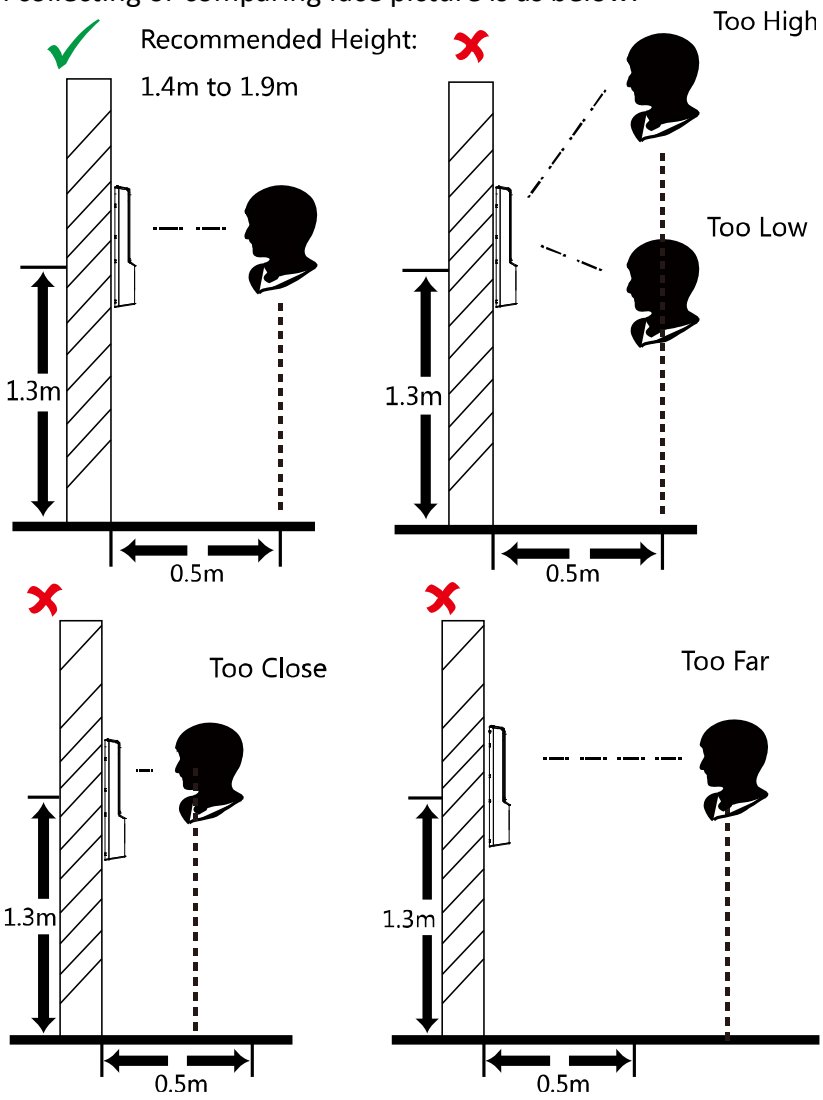
If your fingerprint is shallow, or it is hard to scan your fingerprint, we recommend you to use other authentication methods.

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

Appendix C Tips When Collecting/Comparing Face Picture

C.1 Positions (Recommended Distance:0.5m)

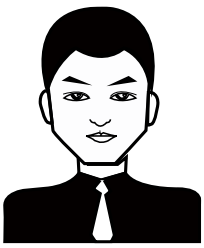
The position when collecting or comparing face picture is as below:



Note: For details about the relationship among person height, device height, and the distance between the person and the device, see Appendix C.

C.2 Expression

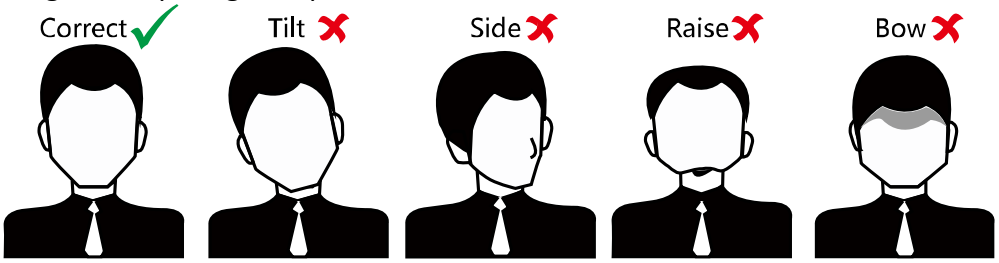
- Keep your expression naturally when collecting or comparing face pictures, just like the expression in the picture below.



- 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.

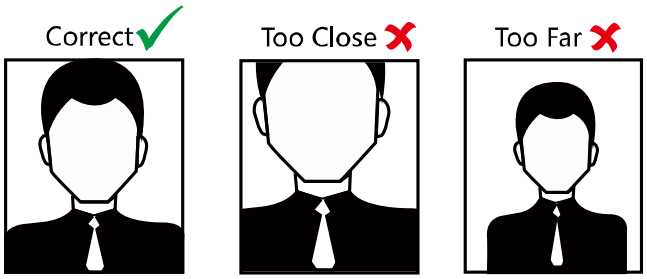
C.3 Posture

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



C.4 Size

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

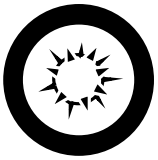


Appendix D Tips for Installation Environment

1. Light Source Illumination Reference Value

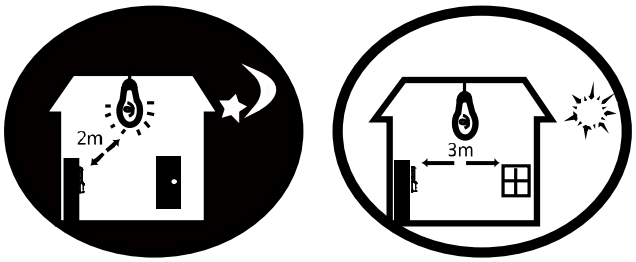
Candel: 10Lux

Bulb: 100~850Lux

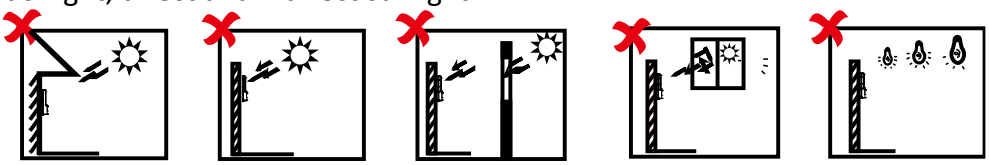


Sunlight: More than 1200Lux

2. If the light source is 0.5 m away from the device, the illumination should be no less than 100 Lux.
3. Install the device indoors, at least 2 meters away from the light, and at least 3 meters away from the window or door.

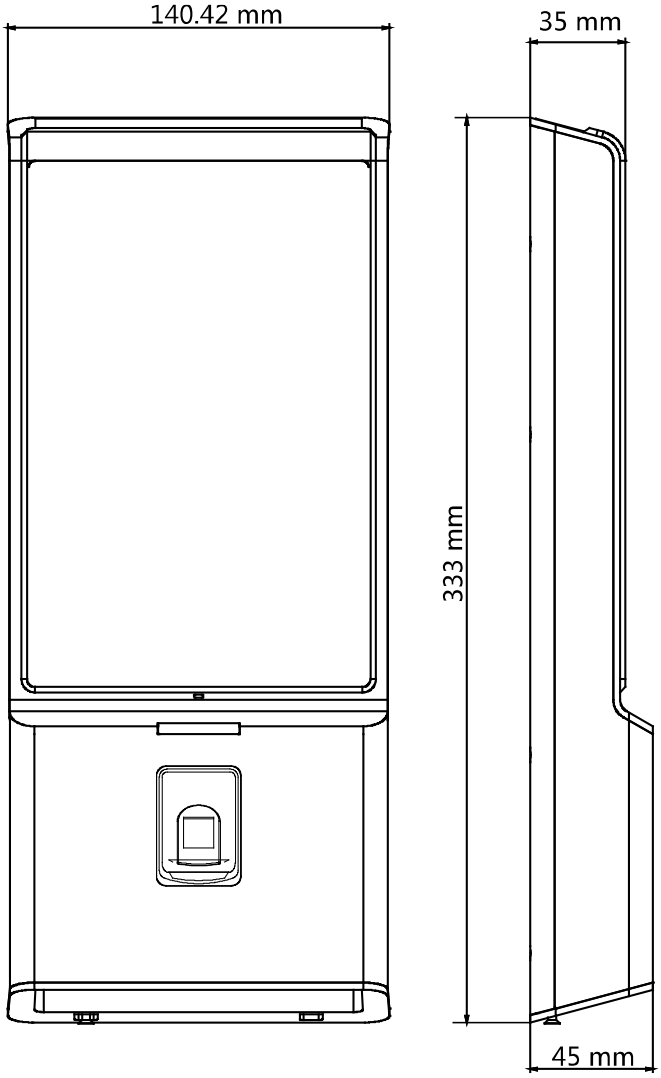


4. Avoid backlight, direct and indirect sunlight.



Backlight | Direct Sunlight | Direct Sunlight through Window | Indirect Sunlight through Window | Close to Light

Appendix E Dimension



010000001080830


See Far, Go Further