




CANTRONIC SYSTEMS 0235TKK2 Face Recognition Access Control Terminal User Guide

[Home](#) » [CANTRONIC SYSTEMS](#) » CANTRONIC SYSTEMS 0235TKK2 Face Recognition Access Control Terminal User Guide 

Contents

- [1 0235TKK2 Face Recognition Access Control Terminal](#)
- [2 1. Packing List](#)
- [3 2. Product Overview](#)
- [4 3. Device Installation](#)
- [5 4. Device Startup](#)
- [6 5. Web Login](#)
- [7 6. Personnel Management](#)
- [8 7 Appendix](#)
- [9 Disclaimer and Safety Warnings](#)
- [10 Regulatory Compliance](#)
- [11 Documents / Resources](#)
- [12 Related Posts](#)

0235TKK2 Face Recognition Access Control Terminal

Quick Guide

1. Packing List

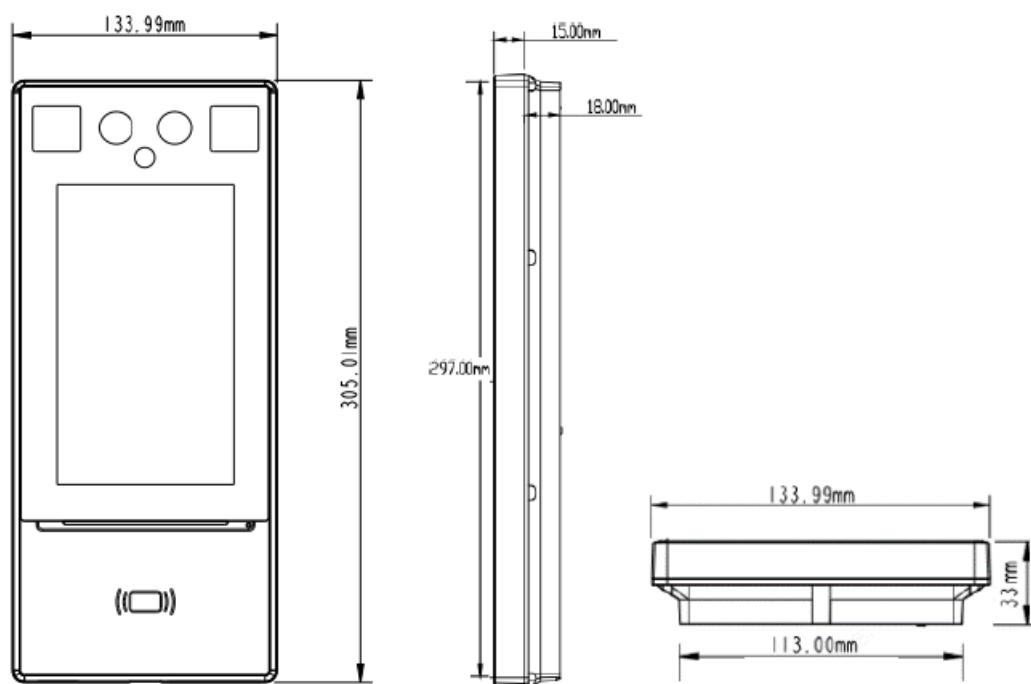
No.	Name	Qty	Unit
1	Face recognition access control terminal	1	PCS
2	Screw component	1	Set
3	Bracket	1	PCS
4	T10 box-end wrench with hole-L shape	1	PCS
5	Installation sticker	1	PCS
6	20-pin cable	1	PCS
7	2-pin power cable	1	PCS
8	User manual	1	PCS

2. Product Overview

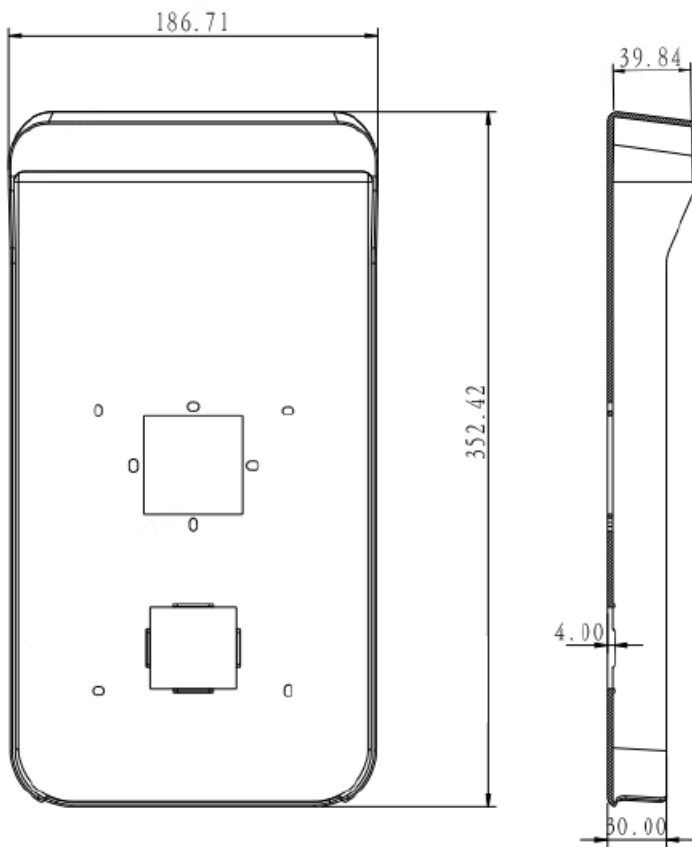
The face recognition access control terminal features high performance and high reliability. It perfectly integrates our company face recognition technology, and supports face scanning-based verification and door opening by relying on the deep learning algorithm, thereby implementing accurate control of personnel access. Visitors can call the indoor unit of a resident so that the resident opens the door remotely. The product is highlighted by high recognition rate, large storage capacity, and fast recognition. The access control terminal also supports attendance, and other functions. It can be widely applied in building systems in smart communities, public security, campuses, and other similar scenes.

2.1 Appearance and Dimension

The actual device appearance shall prevail. The figure below shows the dimension of the device.

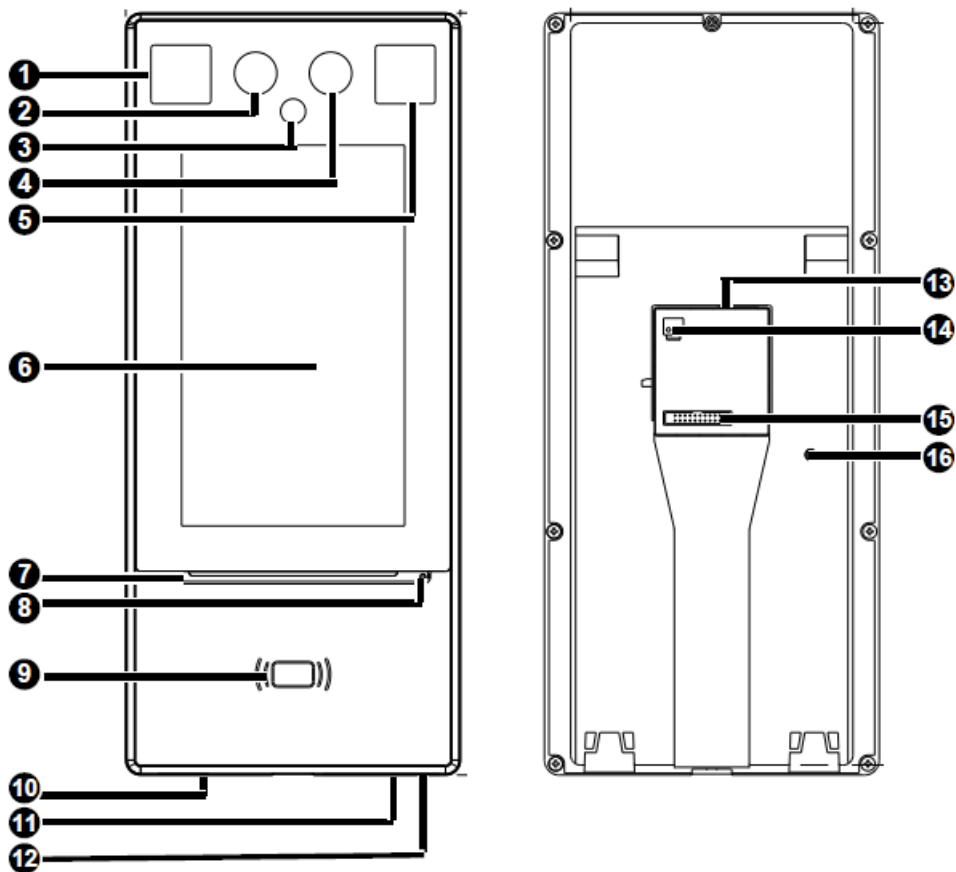


A waterproof hood is required in waterproof installation. The figure below shows the dimensions of the waterproof hood.



2.2 Structure Description

The figure below shows the structure of the device. The actual device shall prevail. Figure 2-1 Device Structure



1.Light supplement lamp 1	2.Infrared camera
3.Infrared light supplement lamp	4.Visible light camera
5.Light supplement lamp 2	6.Display screen
7.Pass-through indicator	8.Microphone
9.Card reading area	10.Loudspeaker
11.Reset button	12.USB2.0
13.Network interface	14.Power input (DC 12V±25%)
15.20-pin interface	16.Tamper proof button

3. Device Installation

3.1 Installation Environment

Try to avoid intense direct light and intense backlighting scenes when installing the device. Please keep the ambient light bright.

3.2 Device Wiring

1. Wiring Embedding

Before installing the face recognition access control terminal, plan the layout of cables, including the power cable (for the diameter selection for the extension power cable, see Table 3-1), network cable, door lock cable, Wiegand cable, alarm cable, and RS485 (RS232) cable. The number of cables depends on the actual networking conditions. For details, see Wiring Description.

Table 3-1 Diameter Selection Table for Extension Power Cables

DC 12V/2A for power supply; the lower limit for the operating voltage is DC 9V (12V-25%)				
Wire Diameter (mm)	0.8mm	1mm	1.25mm	1.63mm
	(20AWG)	(18AWG)	(16AWG)	(14AWG)
Transmission Distance (m)	18	37	58	99

2. Wiring Description

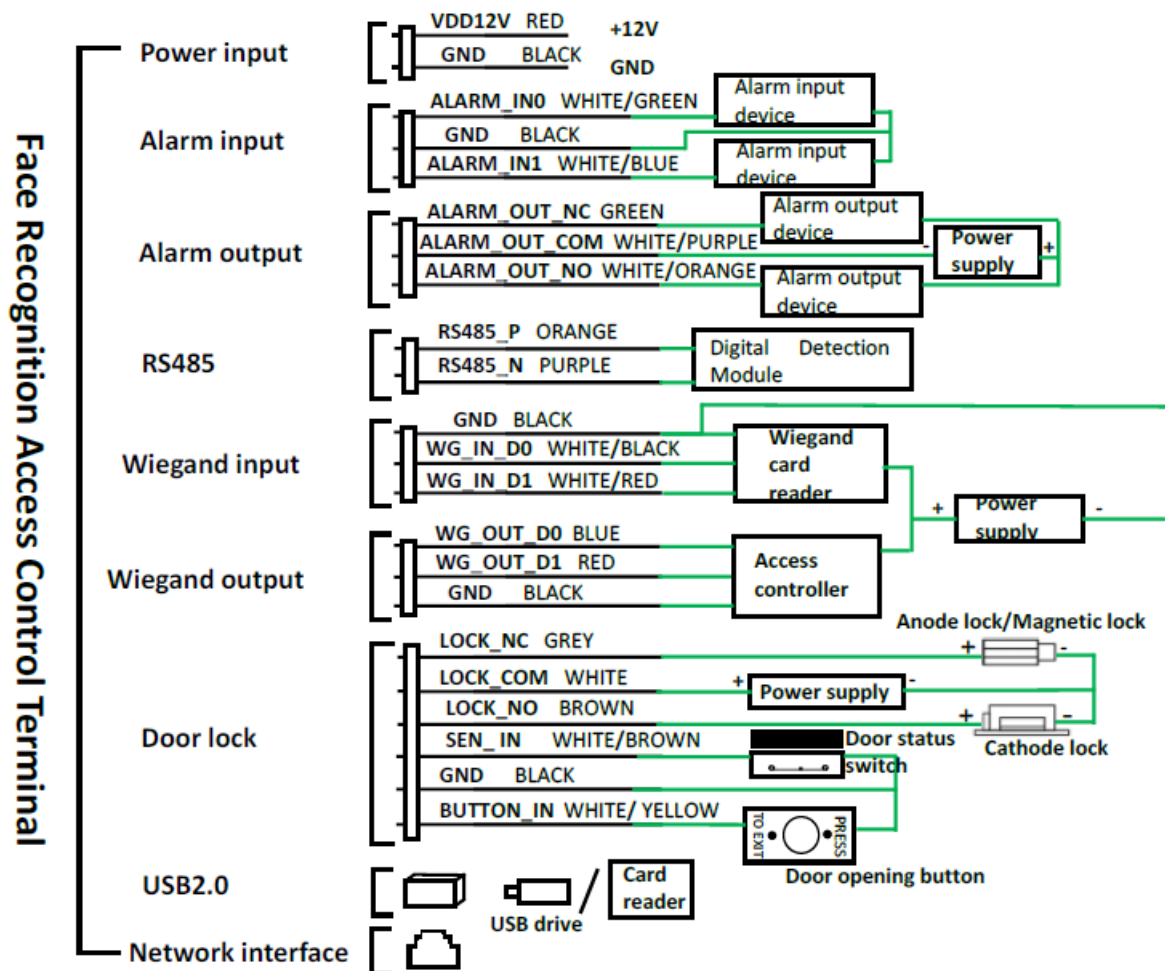
The figures below show the wiring between the access control terminal and different devices. For the wiring terminal of each device, see the operation manual of the device or consult related manufacturers.

NOTE!

In the wiring schematic diagrams, input devices and output devices are defined as follows:

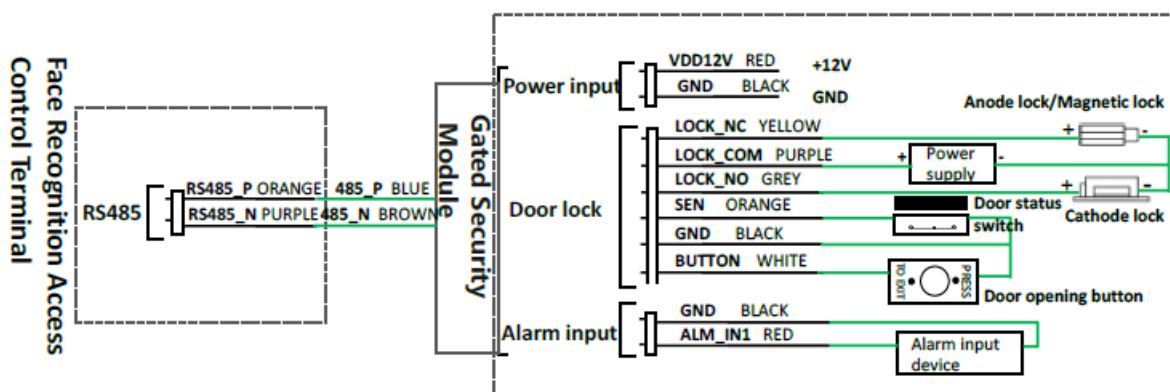
- Input devices refer to devices that send signals to the access control terminal.
- Output devices refer to devices that receive output signals from the access control terminal.

Figure 3-1 Wiring Schematic Diagrams (without Security Module)



The face recognition access control terminal can be also connected to a security module. The figure below shows the wiring of the security module.

Figure 3-2 Wiring Schematic Diagrams (with Security Module)



3.3 Tools Preparations

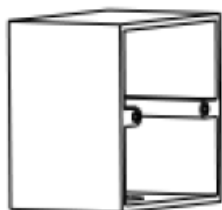
- Phillips screwdriver
- Antistatic wrist strap or antistatic gloves
- Drill
- Tape measure

- Marker
- Plenty of silicone rubber
- Silicone gun

3.4 Installation Steps

1. Determine the position of the 86*86mm wall-mounted junction box.

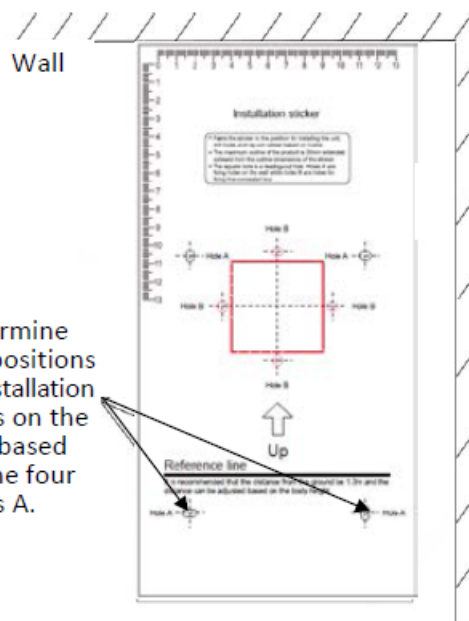
This installation mode embeds an 86*86mm junction box in the wall in advance or makes a hole on the wall to embed the box.



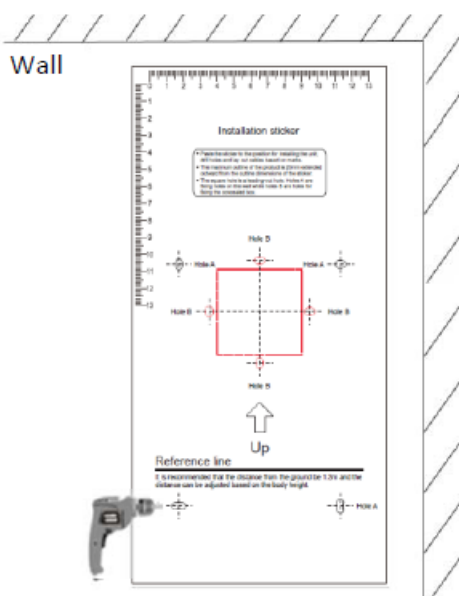
NOTE!

There are two installation holes on the 86*86mm wall-mounted junction box. They can be parallel to the ground or vertical to the ground. They need to map to intermediate holes on the bracket during actual installation.

2. Determine the positions of holes on the wall by referring to the positions of four holes A on the installation sticker.



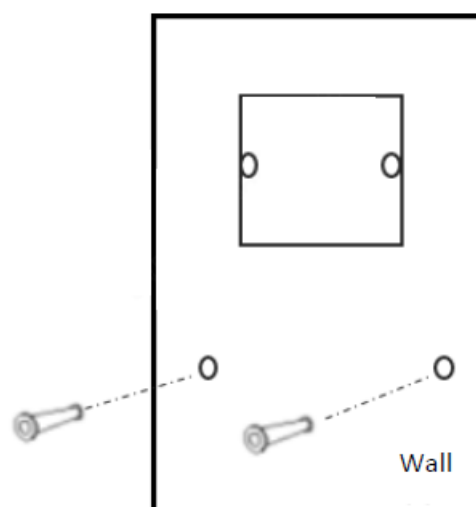
3. Use a drill to drill two holes with the depth of 30mm and diameter of 6mm to 6.5mm on the wall.



Note:

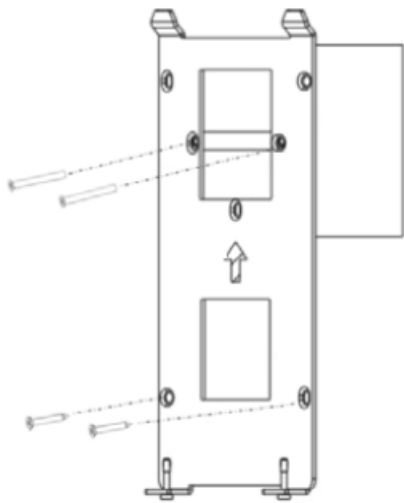
Avoid embedded wires in the wall during drilling!

4. Embed expansion bolts inside the two installation holes on the wall.

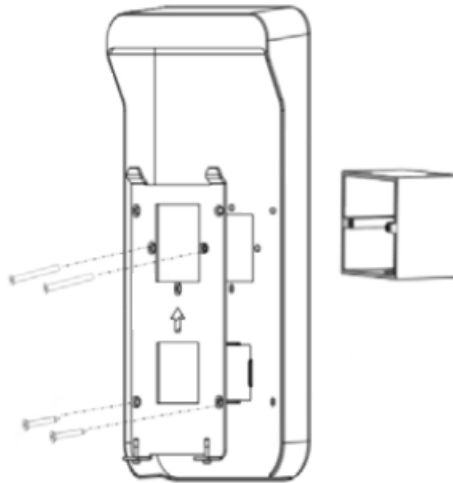


5. Bracket.

- **Normal Installation:** Align holes on the bracket with installation holes on the wall and the 86*86mm wall-mounted junction box and use the Phillips screwdriver to tighten the screws clockwise to fasten the bracket.
- **Waterproof Installation:** The waterproof installation process is basically the same as the normal installation process. You need to fasten the bracket and waterproof hood together, for detail, see figure below. After the waterproof installation is completed, apply enough silicone rubber along the gap between the edge of the waterproof hood and the wall(left, top and right). Silicone rubber must be continuous.

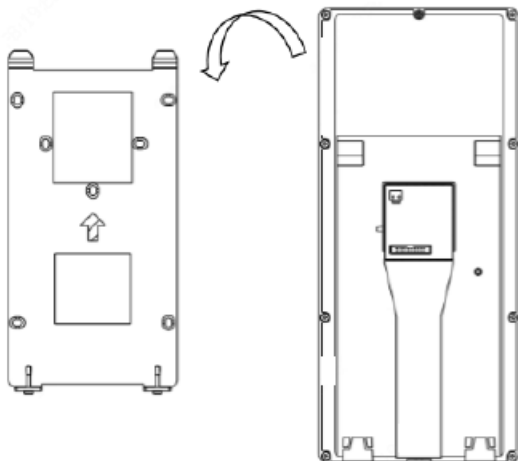


(without waterproof hood)

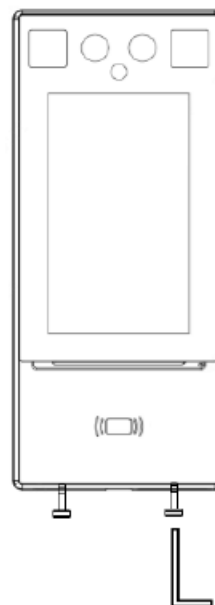


(with waterproof hood)

6. Fasten the access control terminal to the bracket hook.



7. At the bottom of the device (dotted box as shown in the figure below), use the L-shape wrench to tighten the two fastening screws clockwise.



4. Device Startup

After the device is installed correctly, connect one end of the power adapter (purchased or prepared) to the mains supply and the other end to the power interface of the face recognition access control terminal, and then start the device. The display screen of the outdoor monitor is energized and lights up, and the live view is displayed on the screen, indicating that the device is started successfully.

5. Web Login

You can log in to the Web page of the access control terminal to manage and maintain the device. For detailed operations, see the Visual Intercom Face Recognition Terminal User Manual.

1. On a client PC, open the Internet Explorer (IE9 or later), enter the IP address of the device 192.168.1.13 into the address bar, and press Enter.
2. In the login dialog box, enter the username (admin by default) and password (123456 by default), and click Login to access the Web page.

NOTE!

- DHCP is enabled by default. If a DHCP server is used in the network environment, an IP address may be dynamically assigned to the device. Log in with the actual IP address.
- At initial login, the system will prompt you to install a plugin. Close all browsers when installing the plugin. Follow instructions on the page to complete the plugin installation, and then restart the Internet Explorer to log in to the system.
- The default password of this product is used only for initial login. You are required to change the default password after initial login to ensure security. Set a strong password of at least nine characters including all three elements: digits, letters and special characters.
- If the password has been changed, use the new password to log in to the Web interface.

6. Personnel Management

The face recognition access control terminal supports personnel management on the Web interface and GUI interface.

Personnel management on the Web interface

On the Web interface, you can add persons (one by one or in batches), modify person information, or delete persons (one by one or together). The detailed operations are described as follows:

1. Log in to the Web interface.
2. Choose Setup > Intelligent > Face Library to go to the Face Library interface, on which you can manage personnel information. For detailed operations, see the Visual Intercom Face Recognition Terminal User Manual II.

Personnel management on the GUI

1. Tap and hold the main interface of the face recognition access control terminal (for more than 3s).
2. On the displayed password input interface, enter the correct activation password to go to the Activation Config interface.
3. On the Activation Config interface, click User Management. On the displayed User Management interface,

input personnel information. For detailed operations, see the Visual Intercom Face Recognition Terminal User Manual II.

7 Appendix

7.1 Face Recognition Precautions

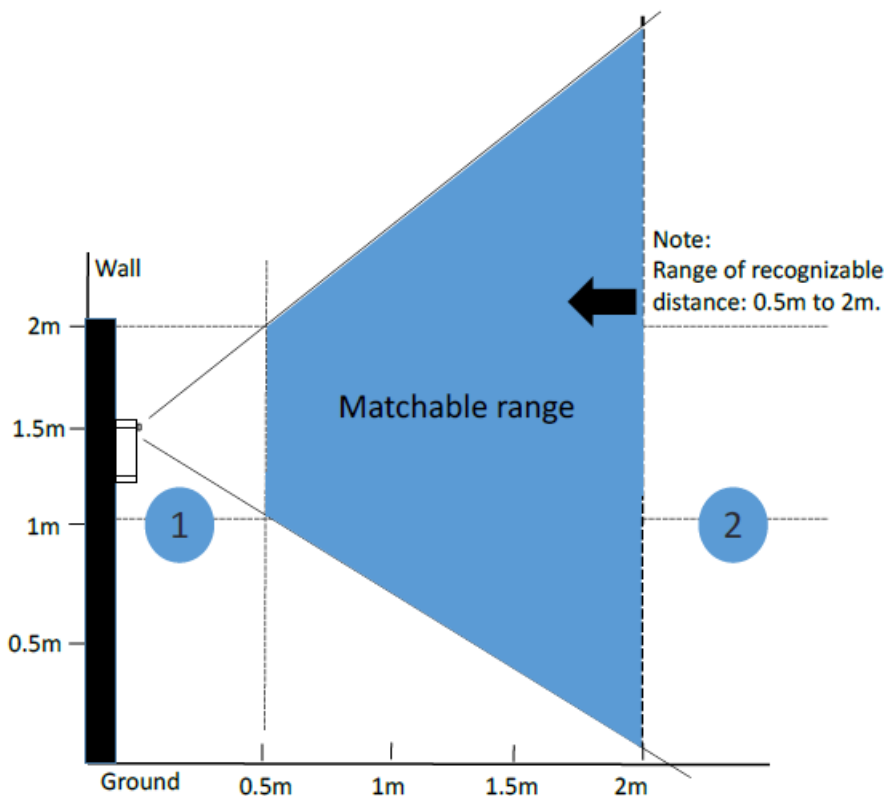
7.1.1 Face Photo Collection Requirements

- General requirement: bareheaded full face photo, with the front side facing the camera.
- Range requirement: The photo should show the outline of a person's both ears and cover the range from the top of the head (including all hair) to the bottom of the neck.
- Color requirement: true color photo.
- Makeup requirement: There should be no cosmetic color that affects the true appearance during collection, such as eyebrow makeup and eyelash makeup.
- Background requirement: The white, blue, or other pure color background is acceptable.
- Light requirement: Light with appropriate brightness is required during collection. Too dark photos, too bright photos, and light- and dark-colored face photos should be avoided.

7.1.2 Face Match Position

The figure below shows the correct face match position.

Figure 7-1 Face Match Position



NOTE!

The face match position should be within the recognizable range shown in the figure. If face match fails in area 1 shown in the figure, move backward. If face match fails in area 2 shown in the figure, move forward.

7.1.3 Face Match Posture

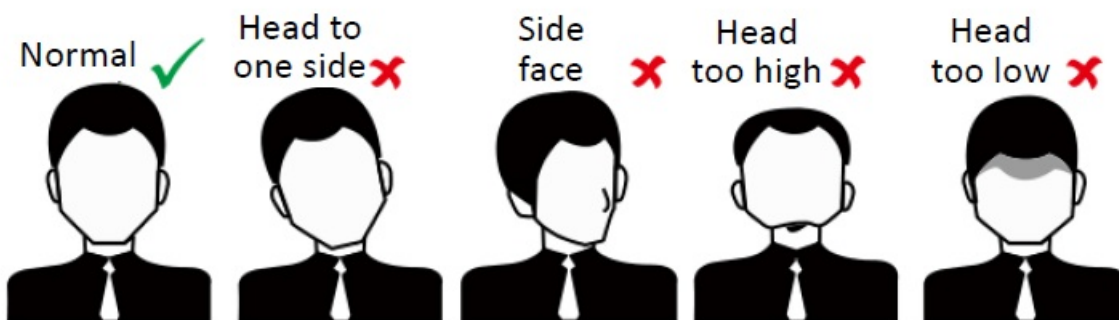
1. Facial Expression

To ensure the accuracy of face match, keep natural expression during the match (as shown in the figure below).



2. Facial Posture

To ensure the accuracy of face match, keep the face facing the recognition window during the match. Avoid the head to one side, side face, head too high, head too low, and other incorrect postures.



Disclaimer and Safety Warnings

Copyright Statement

No part of this manual may be copied, reproduced, translated or distributed in any form by any means without prior content in writing from our company (referred to as us hereafter).

The product described in this manual may contain proprietary software owned by our company and its possible licensors. Unless permitted, no one is allowed to copy, distribute, modify, abstract, decompile, disassemble, decrypt, reverse engineer, rent, transfer, or sublicense the software in any form by any means.

Export Compliance Statement

Our company complies with applicable export control laws and regulations worldwide, including that of the People's Republic of China and the United States, and abides by relevant regulations relating to the export, re-export and transfer of hardware, software and technology. Regarding the product described in this manual, our company asks you to fully understand and strictly abide by the applicable export laws and regulations worldwide.

Privacy Protection Reminder

Our company complies with appropriate privacy protection laws and is committed to protecting user privacy. You may want to read our full privacy policy at our website and get to know the ways we process your personal information. Please be aware, using the product described in this manual may involve the collection of personal information such as face, fingerprint, license plate number, email, phone number, GPS. Please abide by your local laws and regulations while using the product.

About This Manual

- This manual is intended for multiple product models, and the photos, illustrations, descriptions, etc, in this manual may be different from the actual appearances, functions, features, etc, of the product.
- This manual is intended for multiple software versions, and the illustrations and descriptions in this manual may be different from the actual GUI and functions of the software.
- Despite our best efforts, technical or typographical errors may exist in this manual. Our company cannot be held responsible for any such errors and reserves the right to change the manual without prior notice.
- Users are fully responsible for the damages and losses that arise due to improper operation.
- Our company reserves the right to change any information in this manual without any prior notice or indication. Due to such reasons as product version upgrade or regulatory requirement of relevant regions, this manual will be periodically updated.

Disclaimer of Liability

- To the extent allowed by applicable law, in no event will our company be liable for any special, incidental, indirect, consequential damages, nor for any loss of profits, data, and documents.
- The product described in this manual is provided on an “as is” basis. Unless required by applicable law, this manual is only for informational purpose, and all statements, information, and recommendations in this manual are presented without warranty of any kind, expressed or implied, including, but not limited to, merchantability, satisfaction with quality, fitness for a particular purpose, and noninfringement.
- Users must assume total responsibility and all risks for connecting the product to the Internet, including, but not limited to, network attack, hacking, and virus. We strongly recommends that users take all necessary measures to enhance the protection of network, device, data and personal information. Our company disclaims any liability related thereto but will readily provide necessary security related support.
- To the extent not prohibited by applicable law, in no event will our company and its employees, licensors, subsidiary, affiliates be liable for results arising out of using or inability to use the product or service, including, not limited to, loss of profits and any other commercial damages or losses, loss of data, procurement of substitute goods or services; property damage, personal injury, business interruption, loss of business information, or any special, direct, indirect, incidental, consequential, pecuniary, coverage, exemplary, subsidiary losses, however caused and on any theory of liability, whether in contract, strict liability or tort (including negligence or otherwise) in any way out of the use of the product, even if our company has been advised of the possibility of such damages (other than as may be required by applicable law in cases involving personal injury, incidental or subsidiary damage).
- To the extent allowed by applicable law, in no event shall our total liability to you for all damages for the product described in this manual (other than as may be required by applicable law in cases involving personal injury) exceed the amount of money that you have paid for the product.

Network Security

Please take all necessary measures to enhance network security for your device. The following are necessary measures for the network security of your device:

- Change default password and set strong password: You are strongly recommended to change the default password after your first login and set a strong password of at least nine characters including all three elements: digits, letters and special characters.
- Keep firmware up to date: It is recommended that your device is always upgraded to the latest version for the latest functions and better security. Visit our official website or contact your local dealer for the latest firmware.

The following are recommendations for enhancing network security of your device:

- Change password regularly: Change your device password on a regular basis and keep the password safe. Make sure only the authorized user can log in to the device.
- Enable HTTPS/SSL: Use SSL certificate to encrypt HTTP communications and ensure data security.
- Enable IP address filtering: Allow access only from the specified IP addresses.
- Minimum port mapping: Configure your router or firewall to open a minimum set of ports to the WAN and keep only the necessary port mappings. Never set the device as the DMZ host or configure a full cone NAT.
- Disable the automatic login and save password features: If multiple users have access to your computer, it is recommended that you disable these features to prevent unauthorized access.
- Choose username and password discretely: Avoid using the username and password of your social media, bank, email account, etc, as the username and password of your device, in case your social media, bank and email account information is leaked.
- Restrict user permissions: If more than one user needs access to your system, make sure each user is granted only the necessary permissions.
- Disable UPnP: When UPnP is enabled, the router will automatically map internal ports, and the system will automatically forward port data, which results in the risks of data leakage. Therefore, it is recommended to disable UPnP if HTTP and TCP port mapping have been enabled manually on your router.
- SNMP: Disable SNMP if you do not use it. If you do use it, then SNMPv3 is recommended.
- Multicast: Multicast is intended to transmit video to multiple devices. If you do not use this function, it is recommended you disable multicast on your network.
- Check logs: Check your device logs regularly to detect unauthorized access or abnormal operations.
- Physical protection: Keep the device in a locked room or cabinet to prevent unauthorized physical access.
- Isolate video surveillance network: Isolating your video surveillance network with other service networks helps prevent unauthorized access to devices in your security system from other service networks.

Safety Warnings

The device must be installed, serviced and maintained by a trained professional with necessary safety knowledge and skills. Before you start using the device, please read through this guide carefully and make sure all applicable requirements are met to avoid danger and loss of property.

Storage, Transportation, and Use

- Store or use the device in a proper environment that meets environmental requirements, including and not limited to, temperature, humidity, dust, corrosive gases, electromagnetic radiation, etc.
- Make sure the device is securely installed or placed on a flat surface to prevent falling.
- Unless otherwise specified, do not stack devices.
- Ensure good ventilation in the operating environment. Do not cover the vents on the device. Allow adequate space for ventilation.
- Protect the device from liquid of any kind.
- Make sure the power supply provides a stable voltage that meets the power requirements of the device. Make sure the power supply's output power exceeds the total maximum power of all the connected devices.
- Verify that the device is properly installed before connecting it to power.
- Do not remove the seal from the device body without consulting Uniview first. Do not attempt to service the product yourself. Contact a trained professional for maintenance.
- Always disconnect the device from power before attempting to move the device.
- Take proper waterproof measures in accordance with requirements before using the device outdoors.

Power Requirements

- Installation and use of the device must be in strict accordance with your local electrical safety regulations.
- Use a UL certified power supply that meets LPS requirements if an adapter is used.
- Use the recommended cordset (power cord) in accordance with the specified ratings.
- Only use the power adapter supplied with your device.
- Use a mains socket outlet with a protective earthing (grounding) connection.
- Ground your device properly if the device is intended to be grounded.

Battery Use Caution

- When battery is used, avoid:
 - High or low extreme temperatures during use, storage and transportation;
 - Extremely low air pressure, or low air pressure at high altitude.
- Battery replacement.
- Use the battery properly. Improper use of the battery such as the following may cause risks of fire, explosion or leakage of flammable liquid or gas.
- Replace battery with an incorrect type;
- Dispose of a battery into fire or a hot oven, or mechanically crushing or cutting of a battery;
- Dispose the used battery according to your local regulations or the battery manufacturer's instructions
- Personal safety warnings:
 - Chemical Burn Hazard. This product contains a coin cell battery. Do not ingest battery. If the coin cell battery is swallowed, it can cause severe internal burns in just 2 hours and can lead to death.
- Keep new and used batteries away from children.
- If the battery compartment does not close securely, stop using the product and keep it away from children.

If you think batteries might have been swallowed or placed inside any part of the body, seek immediate medical attention.

Regulatory Compliance

FCC Statements

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, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Caution: The user is cautioned that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

NOTE: 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..

RF Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.
Industry Canada ICES-003 Compliance

This device meets the CAN ICES-3 (B)/NMB-3(B) standards requirements.

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.

LVD/EMC Directive

This product complies with the European Low Voltage Directive 2014/35/EU and EMC Directive 2014/30/EU, 2014/53/EU.


WEEE Directive–2012/19/EU

The product this manual refers to is covered by the Waste Electrical & Electronic Equipment (WEEE) Directive and must be disposed of in a responsible manner.

Battery Directive-2013/56/EC

Battery in the product complies with the European Battery Directive 2013/56/EC. For proper recycling, return the battery to your supplier or to a designated collection point.

Documents / Resources

	<p>CANTRONIC SYSTEMS 0235TKK2 Face Recognition Access Control Terminal [pdf] User Guide</p> <p>0235TKK2, 2AX8Q-0235TKK2, 2AX8Q0235TKK2, 0235TKK2 Face Recognition Access Control Terminal, 0235TKK2, Face Recognition Access Control Terminal</p>
---	--