Zhejiang Uniview Technologies 0235C68X Face Recognition Access Control Terminal User Guide

Zhejiang Uniview Technologies 0235C68X Face Recognition Access Control Terminal

Packing List

Contact your local dealer if the package is damaged or incomplete. The package contents may vary with device model.

No.	Name	Qty	Unit
1	Face recognition access control terminal	1	PCS
2	Screw components	2	Set
3	Wall mount bracket	1	PCS
4	T10 star-head key	1	PCS
5	Drill template	1	PCS
6	Tail cable	1	PCS
7	Power cable	1	PCS
8	Wiring terminal block	1	PCS
9	Cover	1	PCS
10	User manual	1	PCS

Product Overview

The face recognition access control terminal perfectly integrates face recognition technology, audio playing and other functionalities. Based on deep learning algorithm, it supports face authentication to control door opening and people flow counting, thereby implementing access control.

Appearance and Dimension

The figures in the manual are for your reference only. The actual appearance may vary with the product model.

- For IC card

- For QR code

110mm
[4.3"]

23.5mm
[0.9"]

260mm
[10.2"]

9.6mm
[0.4"]

M3X10
2PCS

49mm
[1.9"]

60.5mm
[2.4"]
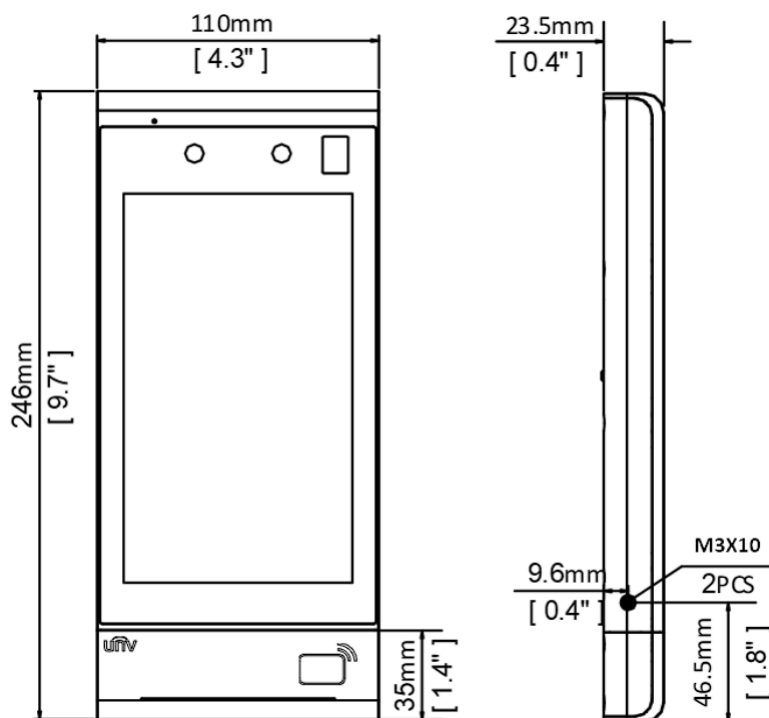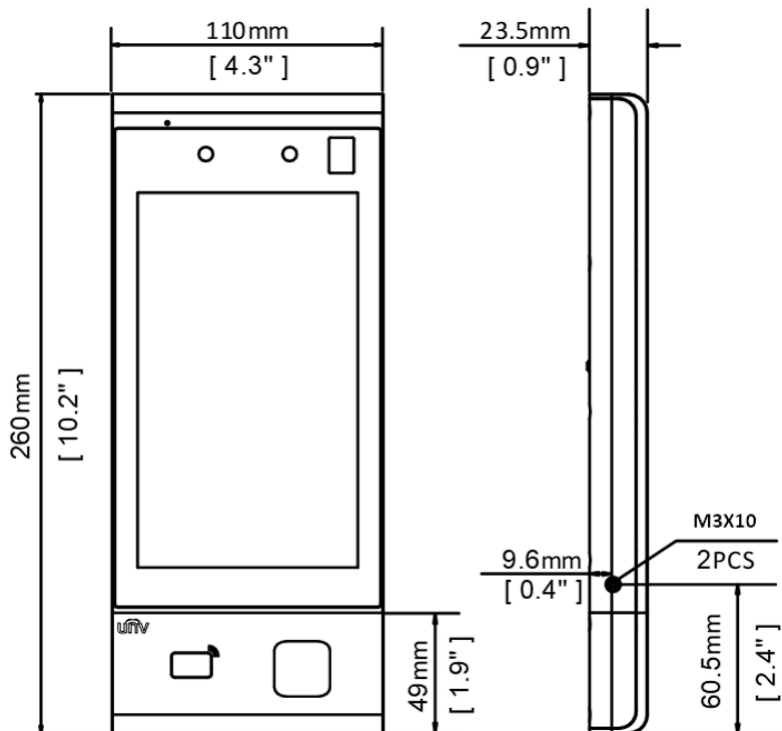
Structure Description

- For IC card
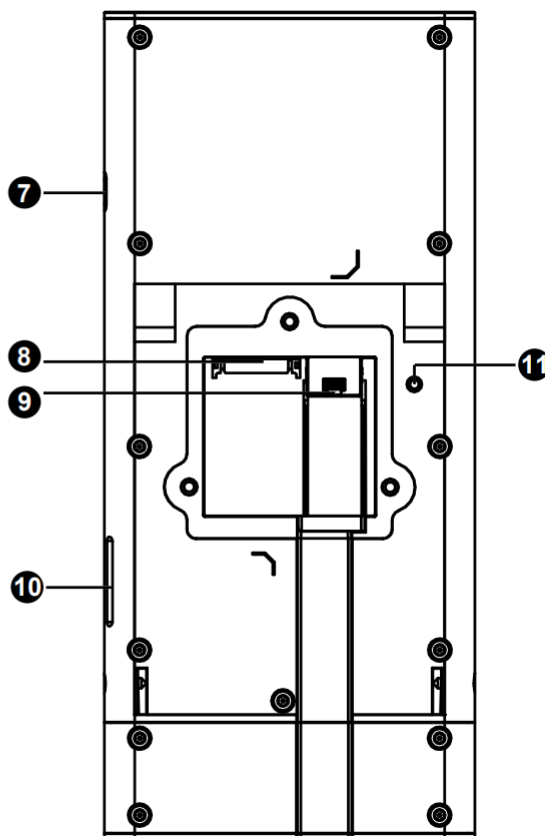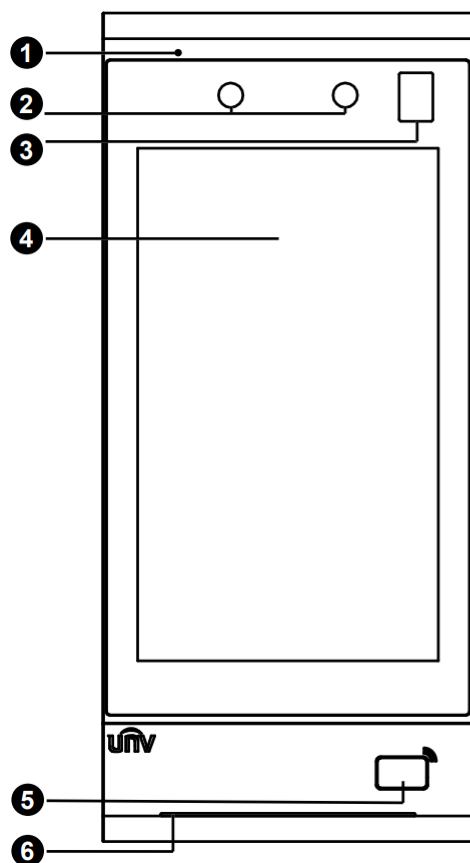
1.Microphone

2.Camera

3.Illuminator

4.Display screen

5.Card reading area

6.QR code reading area

7.Reboot button

8.Cable interface

9.Network interface

10.Loudspeaker

11.Tamper proof button

- For QR code
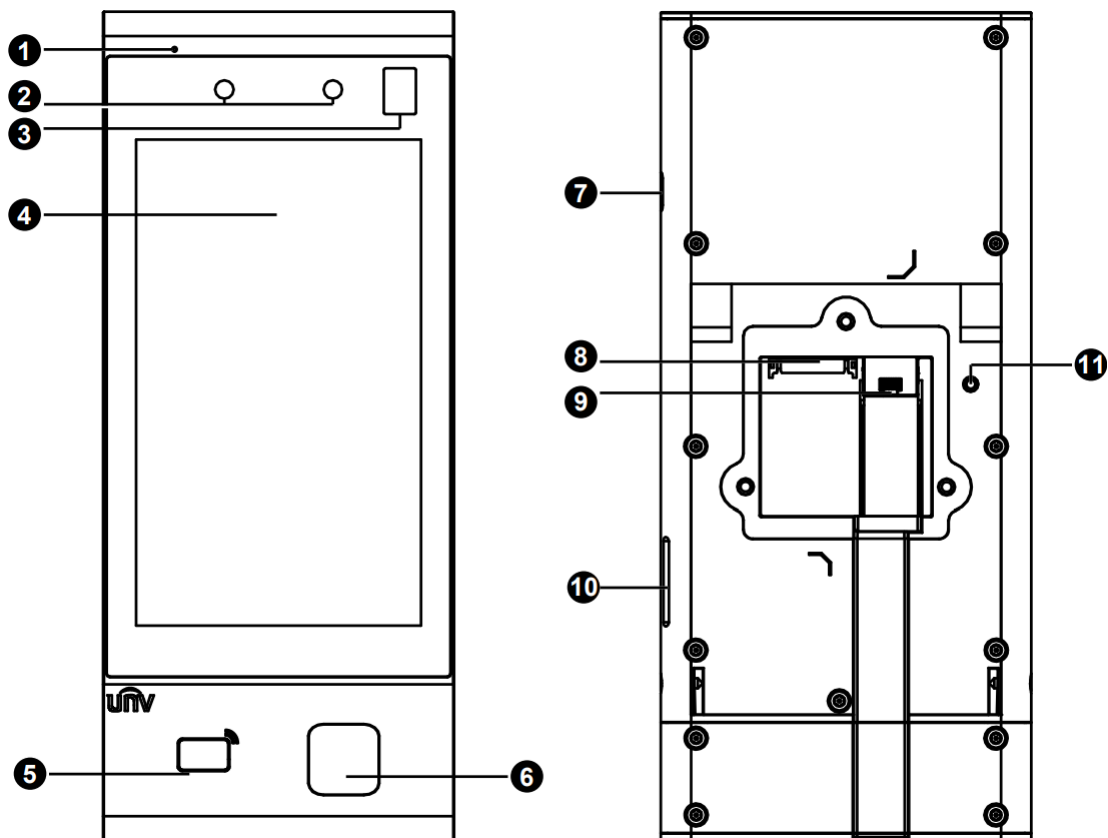
1.Microphone	2.Camera
3.Illuminator	4.Display screen
5.Card reading area	6.QR code reading area
7.Reboot button	8.Cable interface
9.Network interface	10.Loudspeaker
11.Tamper proof button	

Installation

Installation Environment

Ensure adequate lighting at the site. Avoid intense light. 3

Wiring

Before installation, plan wiring for power cable, network cable, door lock cable, wiegand cable, alarm cable, RS485 cable, etc. The number of cables depends on the actual networking conditions. See the figures below for wiring between the terminal and other devices.

 NOTE!

- Input devices in the diagrams below refer to devices that send signals to the access control terminal. Output devices refer to devices that receive signals from the terminal.
- For the wiring terminal of each device, see the operation manual of the device or consult related manufacturers.

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

Face Recognition Access Control Terminal

Power input
VDD12V Red — +12V
GND Black — GND

Alarm input
ALM_IN1 Purple → Alarm input device
GND Black
ALM_IN2 White/Purple → Alarm input device

Alarm output
ALM_OUT_NC Gray → Alarm output device
ALM_OUT_COM White/Orange → Power supply + −
ALM_OUT_NO White/Blue → Alarm output device

RS485
RS485_A Orange
RS485_B Yellow → Digital detection module

Wiegand input
GND Black
WIEGAND_IN0 Blue
WIEGAND_IN1 White → Wiegand card reader

Wiegand output
WIEGAND__OUT0 Brown
WIEGAND__OUT1 Green
GND Black → Access controller

Door lock
LOCK_NC Pink → Electric drop bolt lock /Magnetic lock + −
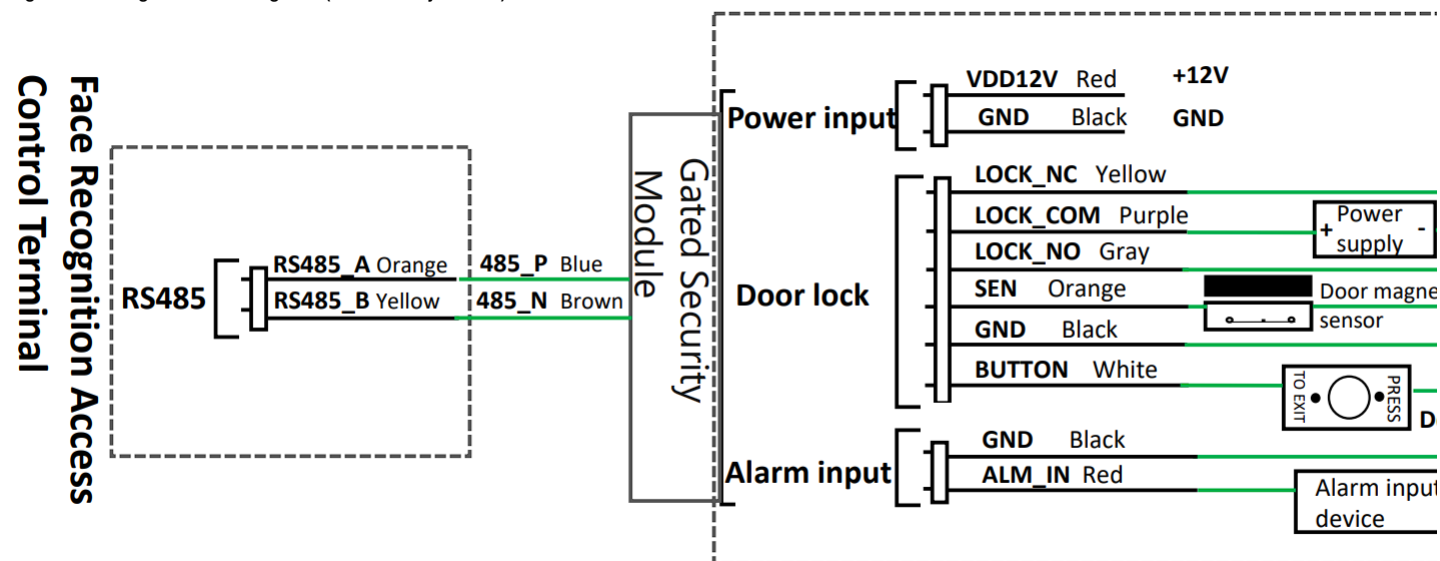LOCK_COM White/Yellow → +Power supply −
LOCK_NO White/Green → Electric strike + −
SEN_INPUT Light Green → Door magnetic sensor
GND Black
BUTTON_INPUT Yellow/Black → Door opening button (TO EXIT / PRESS)

Network interface

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)**

Face Recognition Access Control Terminal

RS485
RS485_A Orange — 485_P Blue
RS485_B Yellow — 485_N Brown

Gated Security Module

Power input
VDD12V Red — +12V
GND Black — GND

Door lock
LOCK_NC Yellow
LOCK_COM Purple → Power supply + −
LOCK_NO Gray
SEN Orange → Door magne… sensor
GND Black
BUTTON White → (TO EXIT / PRESS)

Alarm input
GND Black
ALM_IN Red → Alarm input device

Tool Preparation

- Phillips screwdriver
- ESD wrist strap or gloves
- Electric drill
- Tape measure
- Marker
- Silicone glue
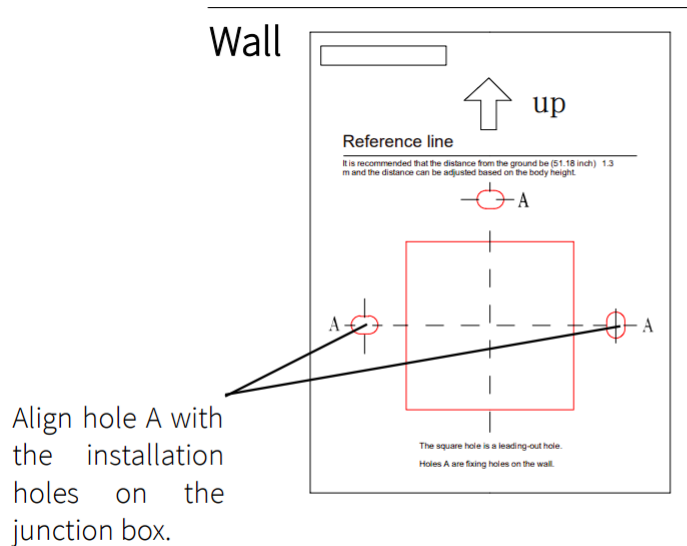- Glue gun

Installation Steps

The following installation steps are the same for different models.

1. Determine the position of the 86*86mm junction box.
   If no junction box has been buried in the wall, skip this step to step 3. The two installation holes on the box should be parallel to the ground during actual installation.
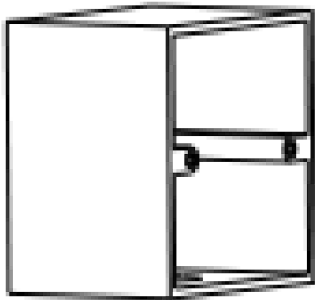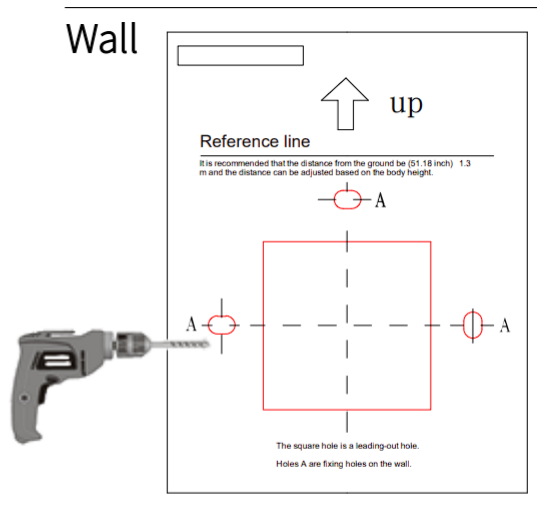
2. Paste the template.
   • With junction box: Align the two holes (A) on the drill template with the two installation holes on the junction box. See the left figure below.
   • Without junction box: Paste the drill template on the wall with the arrow perpendicular to the ground. Use a Ø6-6.5mm drill bit to drill three 30 mm-depth holes on the A position (be careful not to damage cables in the wall), then insert expansion bolts. See the right figure below.
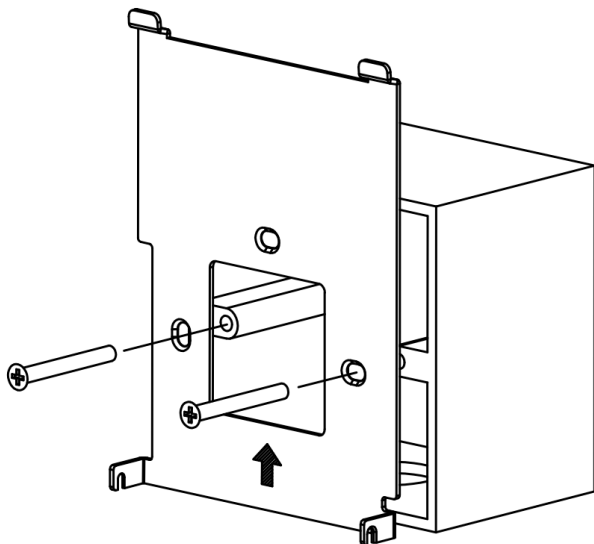

Wall

⬆ up

Reference line

It is recommended that the distance from the ground be (51.18 inch) 1.3 m and the distance can be adjusted based on the body height.

—◯— A

A —◯—   —◯— A

The square hole is a leading-out hole.

Holes A are fixing holes on the wall.

Align hole A with the installation holes on the junction box.

(With junction box)

Wall

⬆ up

Reference line

It is recommended that the distance from the ground be (51.18 inch) 1.3 m and the distance can be adjusted based on the body height.

—◯— A

A —◯—   —◯— A

The square hole is a leading-out hole.

Holes A are fixing holes on the wall.

(Without junction box)

3. Mount the bracket.
   Align bracket holes with installation holes of the junction box on the wall, and tighten the screws to fasten the bracket by using the Phillips screwdriver.
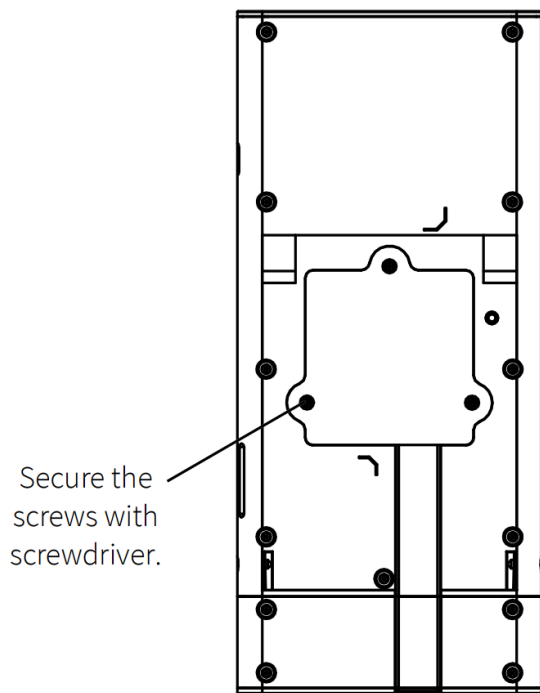

Note:
If no junction box, you need to drill the bracket holes on the wall when installation.

4. Mount the cover.
   Secure the cover by fastening the three screws using a Phillips screwdriver.

Secure the screws with screwdriver.

5. Use a T10 star wrench to unscrew the two tamper proof screws that fix the card module on both sides of the terminal.

Interference fit allows screw to be loosened but not fall off.
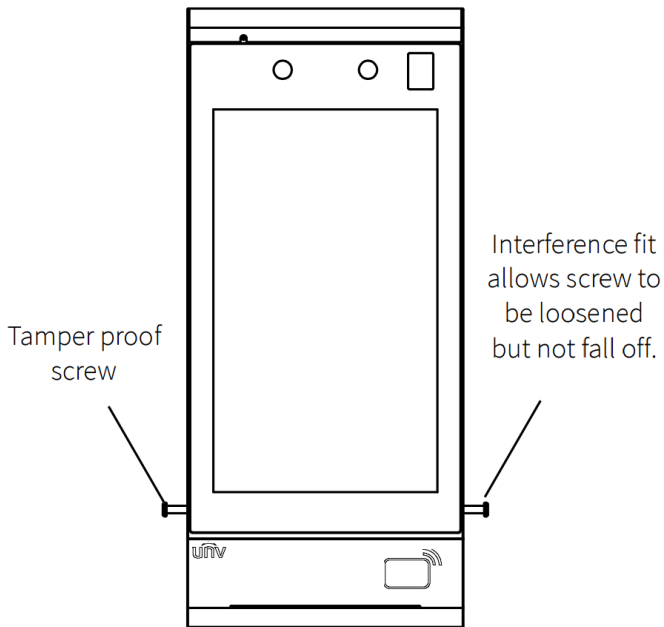
Tamper proof screw

6. Fasten the access control terminal to the bracket hook.
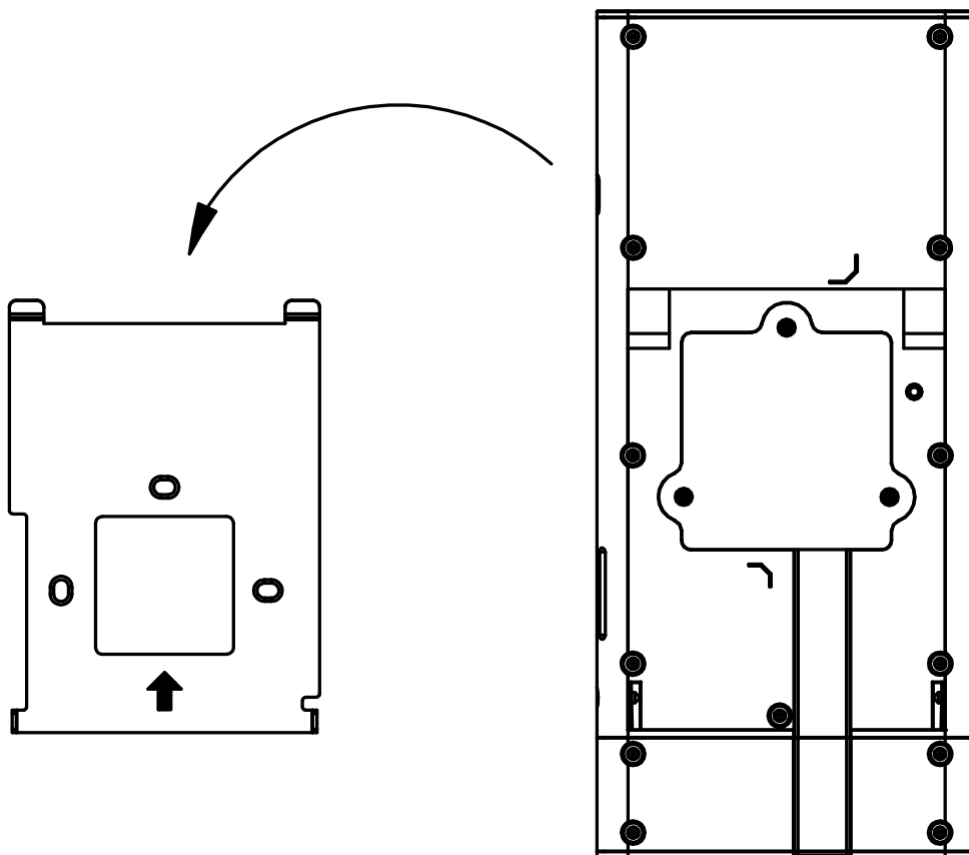
7. Use a T10 star wrench to tighten the two tamper proof screws.

Tighten the screws
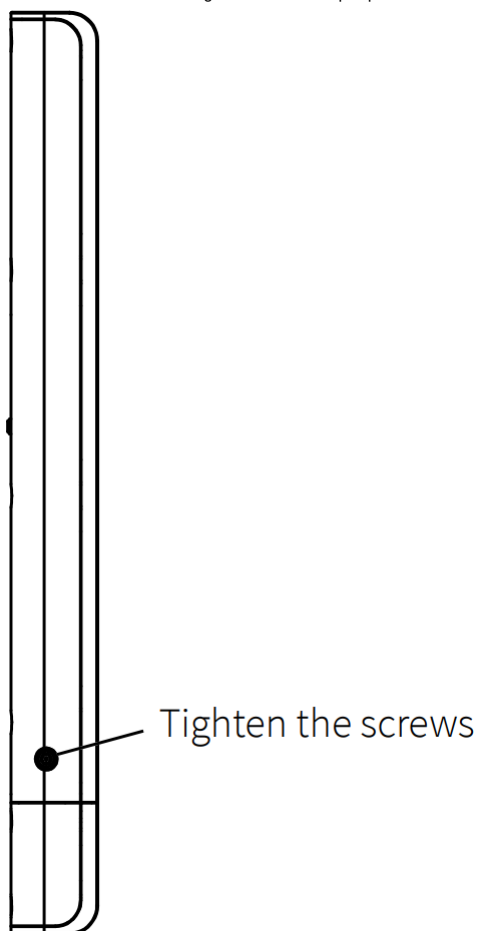
Startup

After the terminal is installed correctly, connect one end of the power adapter (purchased or prepared separately) to the mains supply and the other end to the power interface of the terminal, and then start it up. The display screen of the door station lights up, and live view is displayed on the terminal screen when the terminal is started successfully.

NOTE!

- You are required to change the activation password on the terminal screen after powering on the terminal at the first time. You are strongly recommended to set a strong password of at least nine characters including digits, letters and special characters.

- You can configure the terminal location, network and password and others on the terminal screen. For detailed operations, *see the Visual Intercom Face Recognition Terminal User Manual II.*

Web Login

You can log in to the Web page of the access control terminal to manage and maintain the terminal. The default network settings are shown in the table below and may be modified as required.

Item	Defaults
Network address	- IP address/subnet mask: 192.168.1.13/255.255.255.0 - Gateway: 192.168.1.1 **Note:** DHCP is enabled by default. If a DHCP server is deployed in your network, an IP address may be dynamically assigned to the terminal, an
Username	admin
Password	123456 **Note:** The default password is intended only for your first login. To ensure security, change the password after your first login. You are strongly r including digits, letters and special characters. If the password has been changed, keep the new password properly and use it to log in to

Follow these steps to access your terminal through the Web:

1. Open your Internet Explorer (IE9 or later), enter the IP address of the device in the address bar, and press Enter to open the login page.

   NOTE!
   You may need to install a plug-in at your first login. Follow the on-screen instructions to complete the installation. Close all browsers during installation. After the installation is completed, open the browser again to log in to the system.
2. Enter the username and password, and click **Login** to access the Web page. For detailed operations, see the *Visual Intercom Face Recognition Terminal User Manual II.*

Personnel Management

The face recognition access control terminal supports personnel management on the Web page, terminal screen, and entrance guard management platform.

- On the Web page

You can add persons (one by one or in batches), modify person's information, or delete persons (one by one or together) on the Web page. The detailed operations are described as follows:

1. Log in to the Web page.
2. Select **Setup > Intelligent > Face Library.** In the Face Library page, you can manage personnel information. For detailed operations, *see the Visual Intercom Face Recognition Terminal User Manual II.*

- On the terminal screen

1. Tap and hold the main interface of the face recognition access control terminal (for more than 3s).
2. Enter the correct activation password to go to the **Activation Config** page.
3. Tap **User Management**, and input personnel information. For detailed operations, see the Visual Intercom Face Recognition Terminal User Manual II.

- On the entrance guard management platform

You can add, modify or delete personnel information on the entrance guard management platform, and sync the personnel information to the terminal.

1. Log in to the Web page of entrance guard management platform.
2. Click ❓ Help ▼ in the upper right corner to get online help of the entrance guard management platform.

NOTE!
This method requires you to purchase the entrance guard management platform.

Appendix

Face Photo Collection

- General requirement: Facing the camera without wearing a hat, cap, etc.
- Range requirement: The photo should show both ears and the complete part from the top of the head (including hair) to the bottom of the neck of the person.
- Color requirement: True color photo.
- Makeup requirement: Heavy makeup is not allowed, including eyebrow makeup and eyelash makeup.
- Background requirement: A solid color such as white or blue is acceptable.
- Light requirement: Not too dark or too bright, and not partially dark and partially bright.

Face Recognition Position

The figure below shows the effective recognition range of the terminal. People should stand within the effective recognition range; otherwise, face collection or recognition may fail.

Note: The recognition distance is 0.5m to 2m.
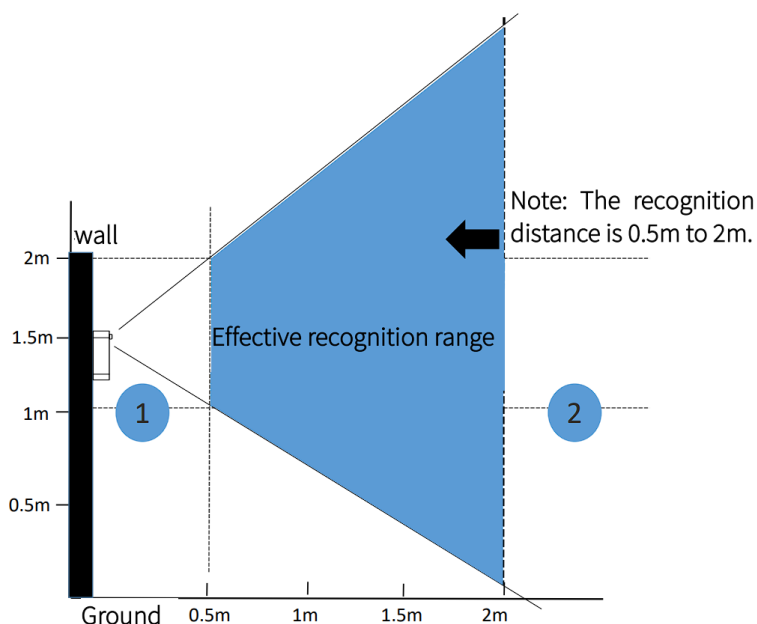
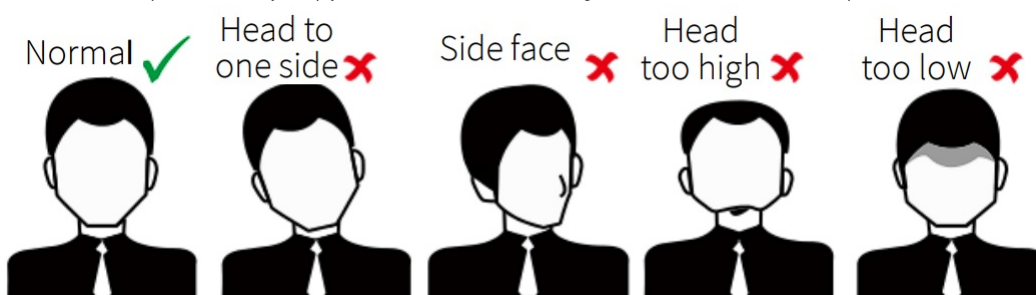**Face Expression and Head Pose**

1. Facial Expression
   To ensure face comparison accuracy, keep a natural facial expression during face collection and comparison.

2. Head Pose
   To ensure face comparison accuracy, keep your face in the center of the recognition window and avoid incorrect poses shown below.

Disclaimer and Safety Warnings

Export Compliance Statement
Uniview 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, Uniview asks you to fully understand and strictly abide by the applicable export laws and regulations worldwide.

EU Authorised Representative
UNV Technology EUROPE B.V. Room 2945,3rd Floor,Randstad 21-05 G,1314 BD,Almere,Netherlands.

Privacy Protection Reminder
Uniview 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. Uniview 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.
- Uniview 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 Uniview 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. Uniview strongly recommends that users take all necessary measures to enhance the protection of network, device, data and personal information. Uniview 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 Uniview 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 Uniview 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 Uniview's 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 Uniview's 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.
  Learn More
  You may also obtain security information under Security Response Center at Uniview's official website.

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

- Install and use the device 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:
  - Extremely high or low temperature and air pressure during use, storage and transportation.
  - 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 of 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 the battery. It can cause severe internal burns and 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.

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator and any part of your body.

IC Statements

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:

— This device may not cause interference, and

— This device must accept any interference, including interference that may cause undesired operation of the device.

This equipment complies with RSS-102 radiation exposure limits set forth for an uncontrolled environment.This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

LVD/EMC Directive

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

WEEE Directive2012/19/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.

Better Security, Better World

www.uniview.com

globalsupport@uniview.com

unv uniarch

Documents / Resources

Zhejiang Uniview Technologies 0235C68X Face Recognition Access Control Terminal [pdf] User Guide
0235C68X, 2AL8S-0235C68X, 2AL8S0235C68X, 0235C68X Face Recognition Access Control Terminal, 0235C68X, Face Recognition Access Control Terminal

References

- U **Uniview - Uniview - Leader of AIoT Solution**

Manuals+,

- **home**
- **privacy**