Face Recognition Access Control Terminal

Quick Guide

V1.00

1 Packing List

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

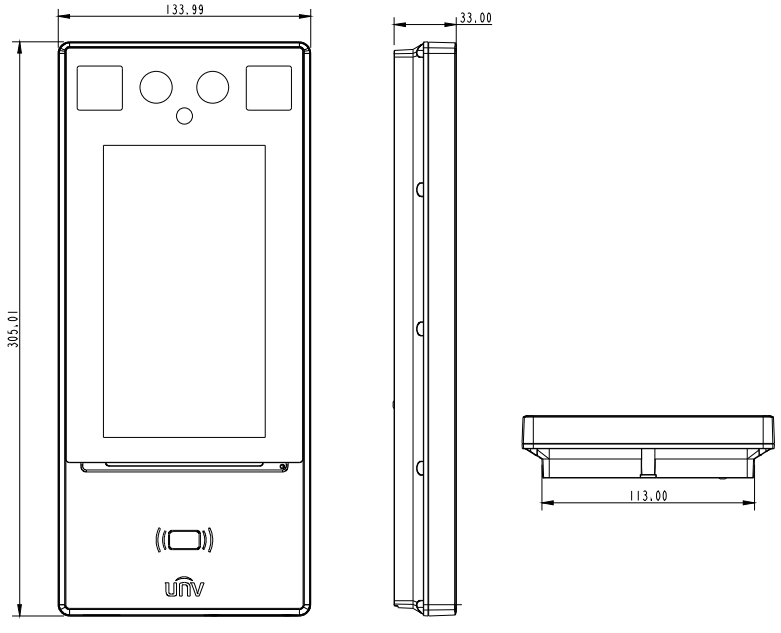
No.	Name	Qty	Unit
1	Face recognition access control terminal	1	PCS
2	Screw pack	1	Set
3	Bracket	1	PCS
4	T10 star key	1	PCS
5	Drill template	1	PCS
6	Tail cable	1	PCS
7	Cover plate	1	PCS
8	Product document	1	Set

2 Introduction

The face recognition access control terminal (hereinafter referred to as the terminal) features high performance and high reliability. Based on deep learning algorithm, it perfectly integrates face recognition technologies, and supports face authentication to control door opening, thereby implementing access control. It can be used with indoor stations to realize visual intercom. The terminal is highlighted by high recognition rate, large library capacity, fast recognition, ideal light adaptability, and is widely applicable to various building systems.

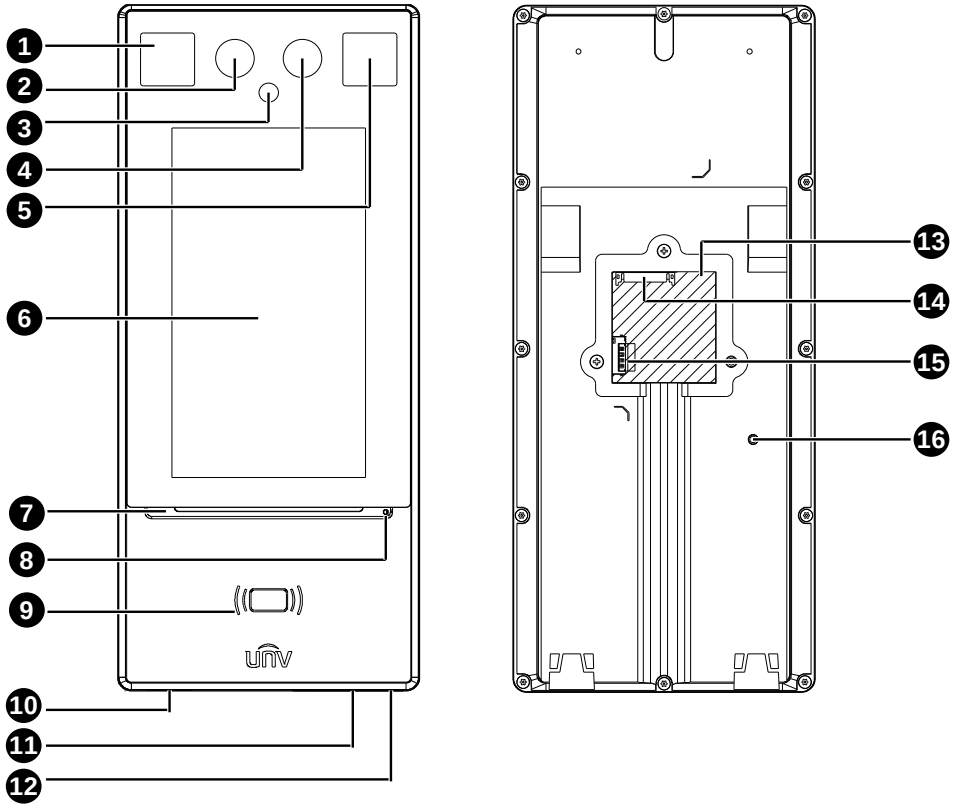
2.1 Appearance and Dimensions

The appearance and dimensions may vary with device model. The figures below are only for illustrative purpose.



2.2 Structure

The structure may vary with device model. The figures below are only for illustrative purpose.



1. Illuminator 1	2. Camera 1
3. IR illuminator	4. Camera 2
5. Illuminator 2	6. Display screen
7. Access indicator	8. Microphone
9. Card reading area	10. Loudspeaker
11. Reboot button	12. USB 2.0
13. Network interface	14. Tail cable interface
15. SIM card slot	16. Tamper proof button

3 Installation

3.1 Installation Environment

Ensure adequate lighting at the site. Avoid strong backlight or front light.

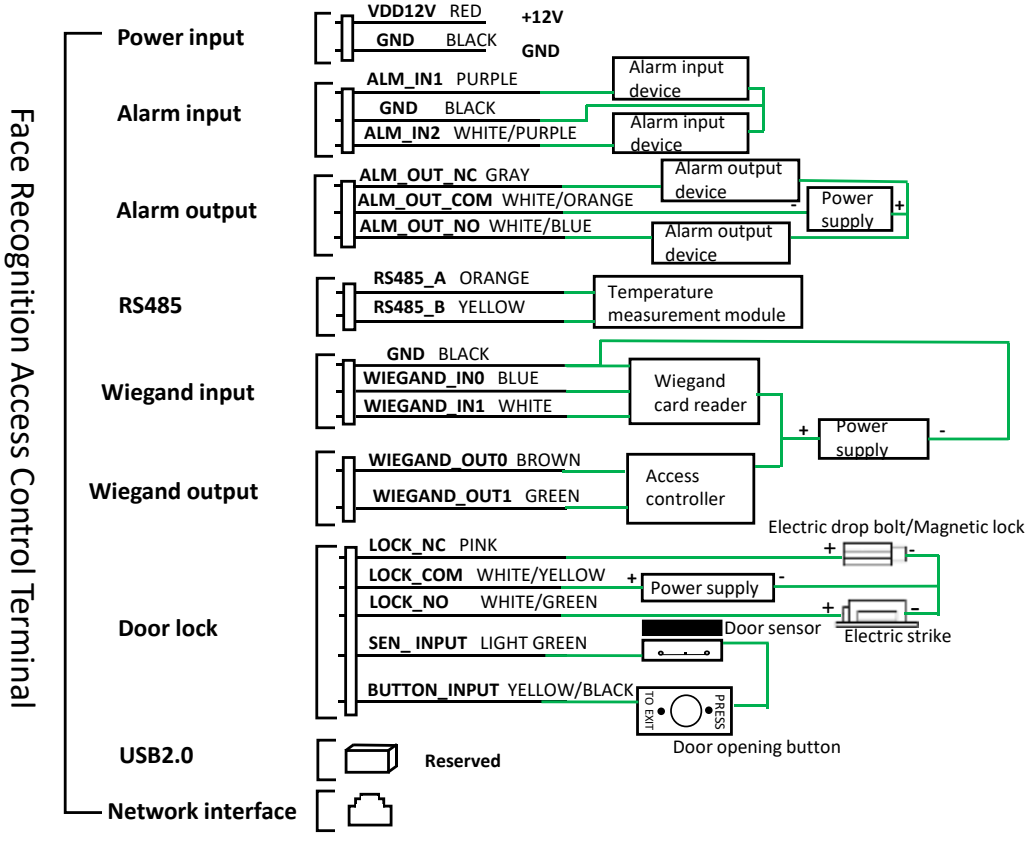
3.2 Wiring

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!

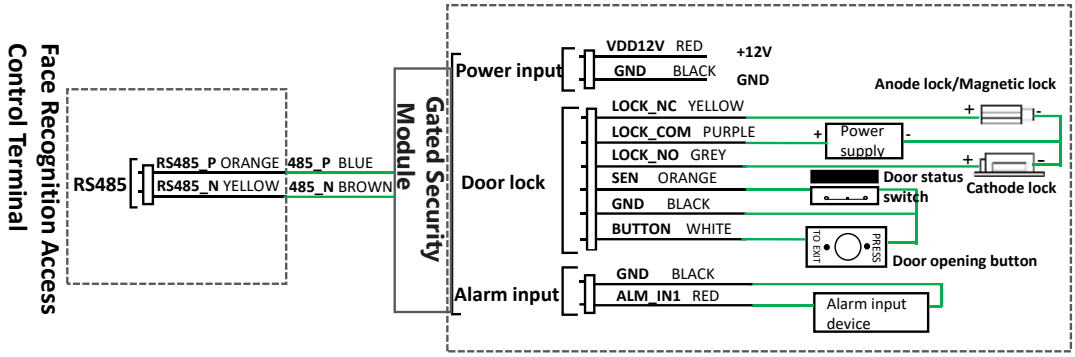
- Input devices in the diagrams below refer to devices that send signals to the terminal. Output devices refer to devices that receive signals from the terminal.
- For the wiring terminal of each device, see the operation manual of the device or consult related manufacturers.

Figure 3-1 Wiring schematic diagram (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 diagram (with security module)

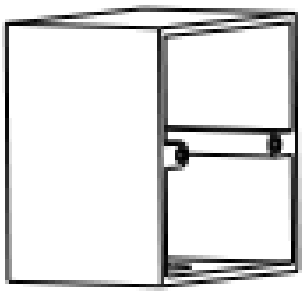


3.3 Tools

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

3.4 Installation Steps

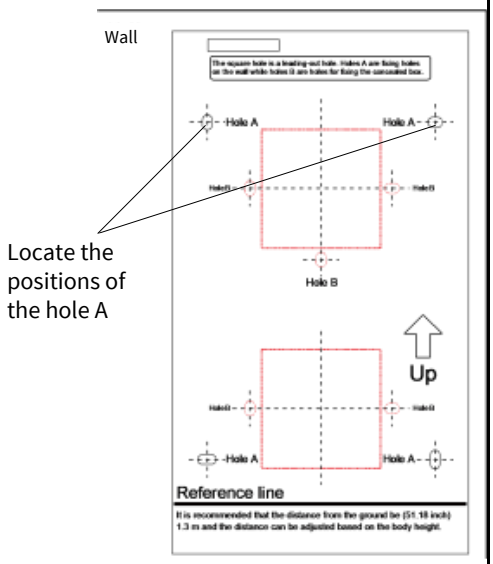
1. Determine the position of the 86*86mm junction box, and drill holes to insert the box.
   If a junction box has been buried in the wall, skip to step 2.



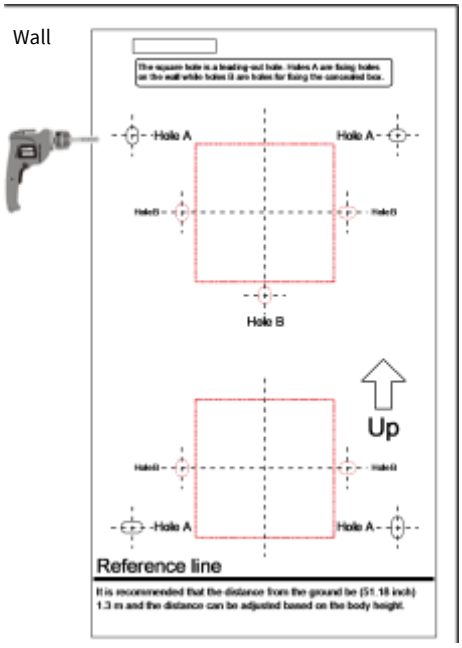
NOTE!

The junction box is sold separately. During actual installation, the two installation holes on the box should be parallel to the ground.

2. Locate the positions of the hole A on the wall by aligning the two holes B at the bottom of the drill template with the installation holes on the junction box.



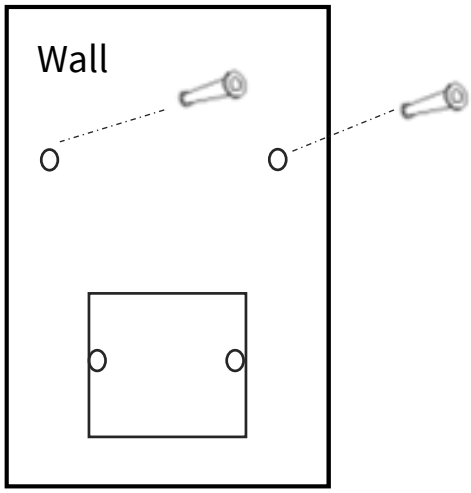
3. Use a Ø6-6.5mm drill bit to drill two 30 mm-depth holes on the hole A position.



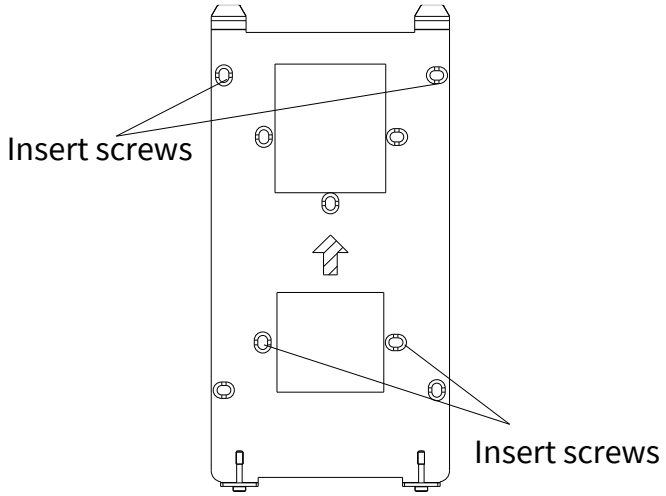
Note:

Be careful not to damage cables in the wall.

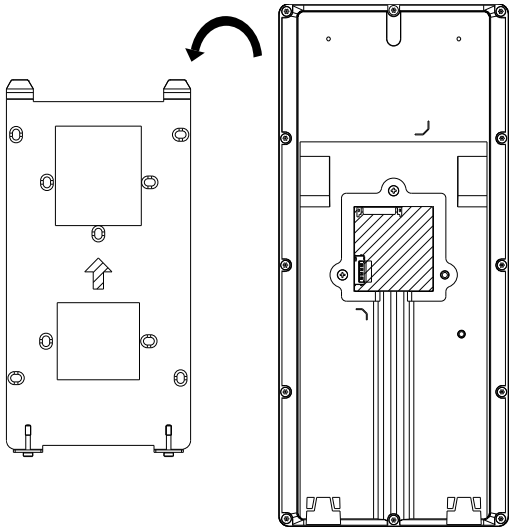
4. Knock the expansion bolts into the holes.



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



6. Fasten the terminal to the bracket hook.



7. Use a T10 star key to tighten the two tamper proof screws at the bottom of the terminal.

4 Startup

After the terminal is installed correctly, connect one end of the power adapter (user-purchased or prepared) to the power interface of the terminal and the other end to the mains supply to start it up. Live video is displayed on the terminal screen when it is started successfully.

NOTE!

- You have 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, uppercase/lowercase letters, and special characters.
- You can configure the device location, password, network settings, and others on the terminal screen.

5 Web Login

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

Item	Default Settings
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, and you need to log in with the actual IP address.
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 recommended to set a strong password of at least nine characters including all digits, letters and special characters.

Follow the steps to log in to the Web interface:

1. Open your Internet Explorer (IE9 or later), enter the IP address of the terminal in the address bar, and then press Enter.

NOTE!

You may need to install a plug-in at your first login. Close all web browsers, and then follow on-screen instructions to install the plug-in. After the installation is completed, open the browser again to log in to the system.

2. Enter the username and password, and click **Login**.

6 Personnel Management

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

- On the Web interface

The Web interface allows you to add persons (one by one or in batches), edit person information, and delete persons (one by one or together). The detailed operations are described as follows:

1. Log in to the Web interface.
2. Go to **Setup** > **Intelligent** > **Face Library**. You can manage personnel information in the **Face Library** tab.

- On the terminal screen

1. Tap and hold the main screen of the terminal (for more than 3s).
2. Enter the correct activation password to go to the **Activation Config** page.
3. Tap **User Management**, and enter person information.

- On the entrance guard server

1. The entrance guard server allows you to add, delete person information, and sync person information to the terminal.
2. Log in to the Web interface of entrance guard server.
3. Click

in the upper right corner to get online help of the entrance guard server.

NOTE!

This method requires you to purchase the entrance guard server.

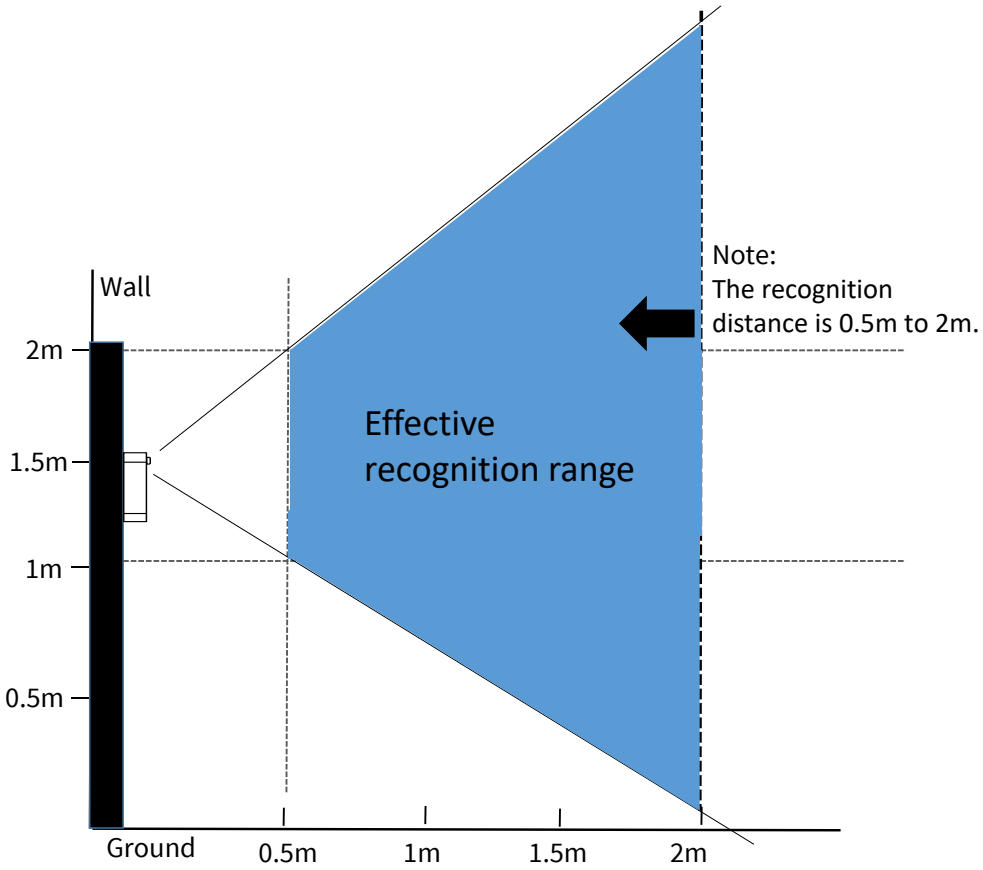
7 Face Recognition Requirements

7.1 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.

7.2 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.



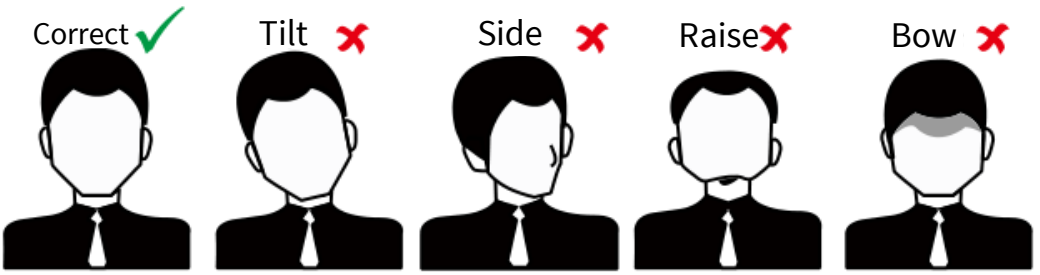
7.3 Face Expression and Head Pose

7.3.1 Facial Expression

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

7.3.2 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

Copyright Statement

©2023 Zhejiang Uniview Technologies Co., Ltd. All rights reserved.
No part of this manual may be copied, reproduced, translated or distributed in any form or by any means without prior consent in writing from Zhejiang Uniview Technologies Co., Ltd (referred to as Uniview or us hereafter).
The product described in this manual may contain proprietary software owned by Uniview and its possible licensors. Unless permitted by Uniview and its licensors, no one is allowed to copy, distribute, modify, abstract, decompile, disassemble, decrypt, reverse engineer, rent, transfer, or sublicense the software in any form or by any means.

Trademark Acknowledgements

unv uniarch are trademarks or registered trademarks of Uniview.

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

- 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.
- 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.

- 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).

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.
- 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.
- 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.
- Physical protection: Keep the device in a locked room or cabinet to prevent unauthorized physical access.
- SNMP: Disable SNMP if you do not use it. If you do use it, then SNMPv3 is recommended.

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.

Avertissement de l’utilisation de la batterie

- Lorsque utiliser la batterie, évitez:
  - Température et pression d'air extrêmement élevées ou basses pendant l'utilisation, le stockage et le transport.
  - Remplacement de la batterie.
- Utilisez la batterie correctement. Mauvaise utilisation de la batterie comme celles mentionnées ici, peut entraîner des risques d’incendie, d’explosion ou de fuite liquide de gaz inflammables.
  - Remplacer la batterie par un type incorrect;
  - Disposer d’une batterie dans le feu ou un four chaud, écraser mécaniquement ou couper la batterie;
- Disposer la batterie utilisée conformément à vos règlements locaux ou aux instructions du fabricant de la batterie.

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.

Visit http://en.univiview.com/Support/Download_Center/Product_Installation/Declaration/ for SDoC.

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

LVD/EMC Directive

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