

Face Recognition Access Control Terminal Quick Guide

V1.02

Contents

1. Packing List	3
2. Product Overview	3
2.1 Appearance and Dimension	4
2.2 Structure Description	6
3. Device Installation	8
3.1 Installation Environment	8
3.2 Tools Preparations	8
3.3 Device Wiring	9
3.4 Installation	10
3.4.1 Desktop mount	10
3.4.2 Standing pole mount	10
4. Device Startup	13
5. Web Login.....	14
6. Personnel Management	15
7. Appendix	16
7.1 Face Recognition Precautions	16
7.1.1 Face Photo Collection Requirements	16
7.1.2 Face Match Position	16
7.1.3 Face Match Posture	18
Disclaimer and Safety Warnings.....	19

1. Packing List

The attachments may vary with models, please see the actual model for details.

No.	Name	Qty	Unit
1	Face recognition access control terminal	1	PCS
2	Screw component	3	Set
3	Installation sticker	1	PCS
4	Power adapter	1	PCS
5	Power cable	1	PCS

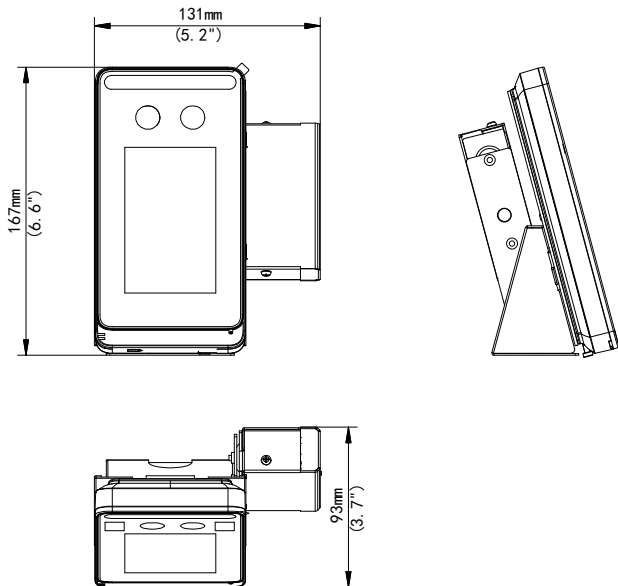
2. Product Overview

The face recognition access control terminal is a kind of access control device with precise recognition rate, large storage capacity and fast recognition. The UNV face recognition technology is perfectly integrated into the access control device, which relies on deep learning algorithm, to support face authentication to open the door and achieve precise control of human. And it can be widely applied to the scenarios of building systems, such as smart communities, public security, parks and other important areas.

2.1 Appearance and Dimension

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

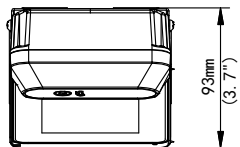
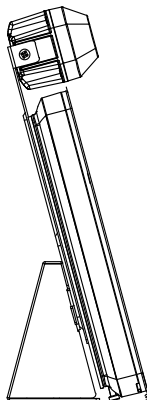
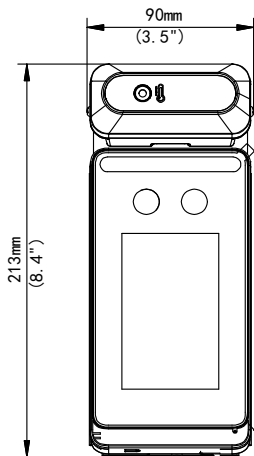
Type A :



NOTE!

Certain models may have different cameras.

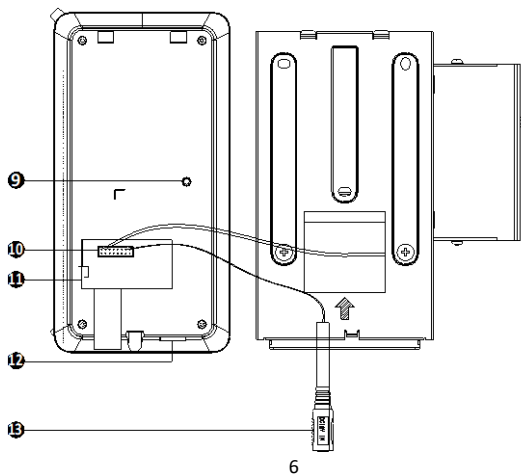
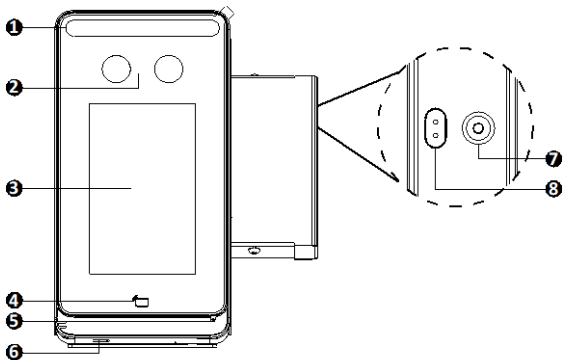
Type B :



2.2 Structure Description

The figure below shows the structure of the device. The actual device shall prevail.

Type A :



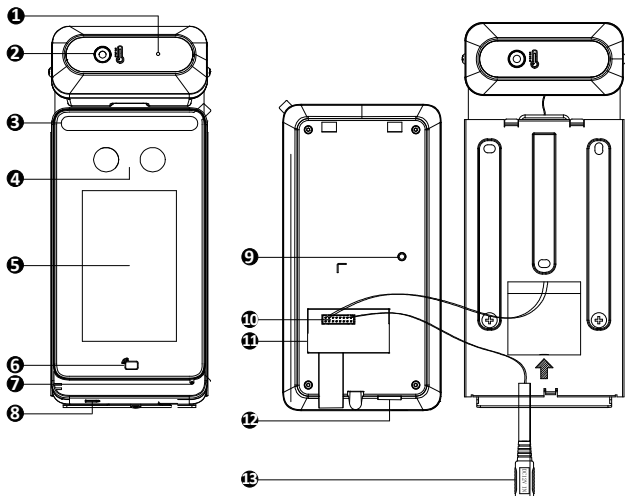
1. Light supplement lamp	2. Cameras
3. Display screen	4. Card reading area
5. Microphone	6. Reboot button
7. Temperature sensor	8. Range sensor
9. Tamper proof button	10. 16-pin interface
11. Network interface	12. Loudspeaker
13. DC 12V power cable	



NOTE!

Certain models may have different cameras.

Type B :



1. Indicator	2. Temperature sensor
3. Light supplement lamp	4. Cameras
5. Display screen	6. Card reading area
7. Microphone	8. Reboot button
9. Tamper proof button	10. 16-pin interface
11. Network interface	12. Loudspeaker
13. DC 12V power cable	

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 Tools Preparations

- Phillips screwdriver
- Antistatic wrist strap or antistatic gloves
- Drill
- Tape measure
- Marker
- Plenty of silicone rubber
- Silicone gun

3.3 Device Wiring

1 Wiring Embedding

Before installing the face recognition access control terminal, plan the layout of cables, including the power cable, network cable, door lock cable, and alarm cable. The number of cables depends on the actual networking conditions. For details, see Wiring Description.

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.

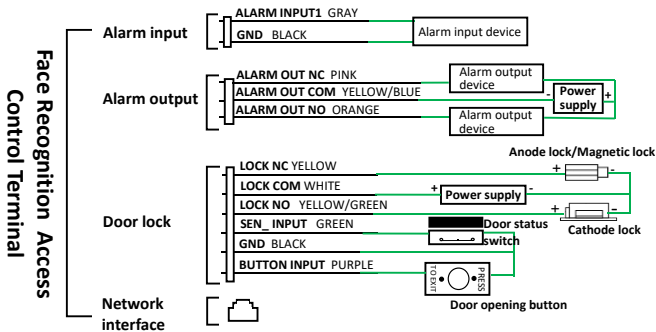


NOTE!

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



3.4 Installation

You can choose desktop mount, or standing pole mount according to your needs. The installation steps are detailed in the following part.

3.4.1 Desktop mount

Place the face recognition access control terminal to the intended position.

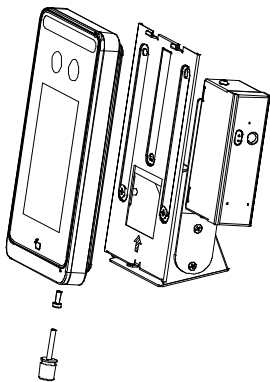
3.4.2 Standing pole mount



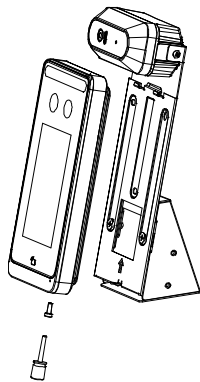
NOTE!

The standing pole is not included in the delivery and needs to be purchased separately. If you choose standing pole mount, refer to the corresponding guide to install the standing pole.

1. Loosen the anti-theft screw at the bottom, remove the desktop stand.

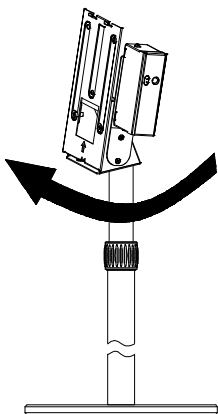


Type A

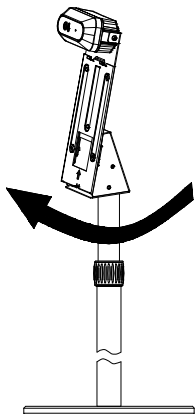


Type B

2. Rotate the stand until it is secured on the standing pole.



Type A



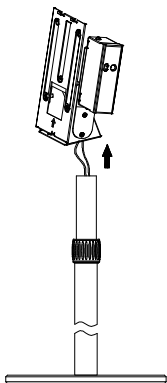
Type B

3. Insert the network and power cables into the standing pole from its bottom hole. Lead the cables all the way through the pole to its top screw hole, through the screw hole at the bottom of the stand, and then lead the cables out from the side of the desktop stand.

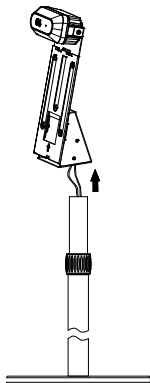


CAUTION!

Do not pull the cables; it may loosen or disconnect the connectors.



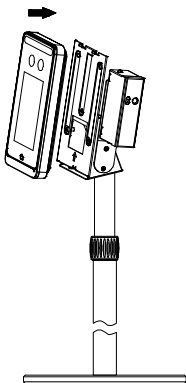
Type A



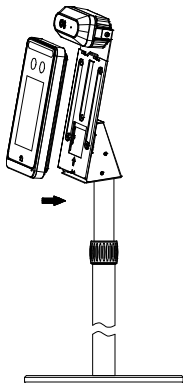
Type B

4. Connect the network cable and the power plug with the access control terminal.

5. Secure the access control terminal on the stand.

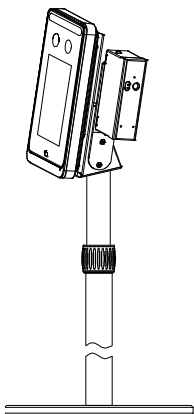


Type A

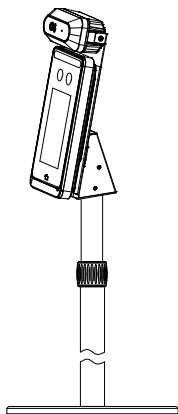


Type B

6. Tighten the anti-theft screw clockwise at the bottom of the device.
7. Place the access control terminal to the intended position to complete installation.



Type A



Type B

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 *Face Recognition Access Control 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 *Face Recognition Access Control Terminal User Manual*.

- 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 *Face Recognition Access Control Terminal User Manual*.

7. Appendix

7.1 Face Recognition Precautions

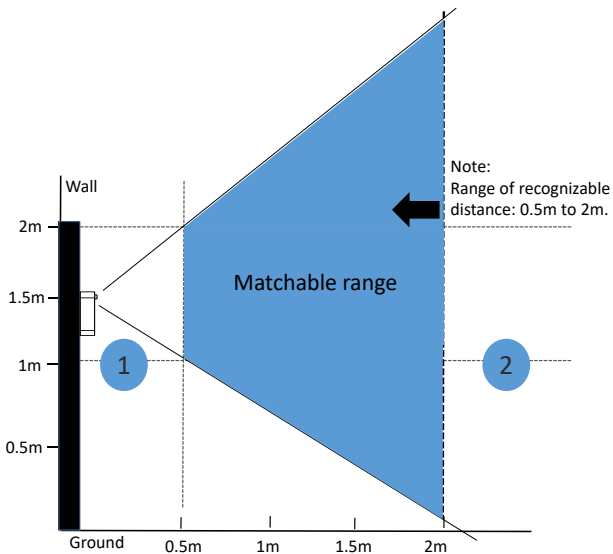
7.1.1 Face Photo Collection Requirements

- 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).

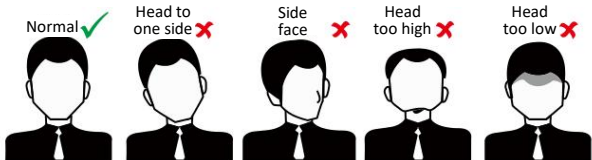
Figure 7-2 Correct Expression



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.

Figure 7-3 Correct and Incorrect Postures



Disclaimer and Safety Warnings


Copyright Statement

©2020 Zhejiang Uniview Technologies Co., Ltd. All rights reserved.

No part of this manual may be copied, reproduced, translated or distributed in any form by any means without prior content 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 by any means.

Trademark Acknowledgements

 are trademarks or registered trademarks of Uniview.

All other trademarks, products, services and companies in this manual or the product described in this manual are the property of their respective owners.

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.

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

- 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.

Avvertimento de l'utilizzazione de la batterie

- Lorsque utiliser la batterie, évitez:
 - Températures extrêmement élevées ou basses pendant l'utilisation, le stockage et le transport;
 - Pression d'air extrêmement basse, ou pression d'air basse à haute altitude.
 - 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.
- **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.
- **Avertissements de sécurité personnelle:**
 - Risque de brûlure chimique. Ce produit contient une batterie de cellules. N'ingérer pas la batterie. Si la batterie de cellule est avalée, elle peut causer de graves brûlures internes en seulement 2 heures et peut entraîner la mort.
 - Gardez les batteries nouvelles ou utilisées à l'écart des enfants.
 - Si le compartiment de la batterie ne se ferme pas en toute sécurité, cessez d'utiliser le produit et gardez-le à l'écart des enfants.
 - Si vous pensez que des piles ont pu être avalées ou placées à l'intérieur d'une partie du corps, consultez immédiatement un médecin.

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.

Compliance Information Statement refer to:

http://en.uniview.com/Support/Download_Center/Product_Installation/Declaration/

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 product 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 product 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 product 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.

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.

IC Statements

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

- (1) this device may not cause interference, and
- (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radioexempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

- (1) l'appareil ne doit pas produire de brouillage, et
- (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

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.

Better Security, Better World



www.uniview.com



globalsupport@uniview.com