

UNIVIEW OET-231KH Intelligent Recognition Access Control Terminal User Guide

Contents

- [1 UNIVIEW OET-231KH Intelligent Recognition Access Control Terminal](#)
- [2 Packing List](#)
- [3 Product Introduction](#)
- [4 Dimensions](#)
- [5 Cable](#)
- [6 Disclaimer and Safety Warnings](#)
- [7 Regulatory Compliance](#)
- [8 Documents / Resources](#)
 - [8.1 References](#)

UNIVIEW OET-231KH Intelligent Recognition Access Control Terminal

Packing List

No.	Name	Qty	Unit
1	Intelligent recognition access control terminal	1	PCS
2	Screw components	2	Set
3	Wall mount bracket	1	PCS
4	T10 screwdriver	1	PCS
5	Drill template	1	PCS
6	Tail cable	1	PCS
7	Cover	1	PCS
8	Product documents	1	Set

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

Product Introduction

The appearance, dimensions, structure, and tail cables may vary with device models.

Dimensions

Structure

The intelligent recognition access control terminal includes an intelligent recognition terminal and pluggable

verification module.

Intelligent recognition terminal

Pluggable verification module

1. Microphone
2. Camera
3. Display screen
4. Illuminator
5. Reset button
6. Cable interface
7. Speaker
8. Network interface
9. Tamper-proof button
10. Pass-through indicator
11. Card reading area
12. QR code reading area

Cable

Name	Color	Description
Door magnetic input	Light green	Door magnetic, button, and door lock cables
Button input	Yellow/Black	
Door lock_NC	Pink	
Door lock_COM	White/Yellow	
Door lock_NO	White/Green	
GND	Black	
RS485_A	Orange	RS485, Wiegand input, and Wiegand output cables
RS485_B	Yellow	
GND	Black	
Wiegand input_D0	Blue	
Wiegand input_D1	White	
Wiegand output_D0	Brown	
Wiegand output_D1	Green	Alarm input and alarm output cables
Alarm input_1	Purple	
Alarm input_2	White/Purple	
Alarm output_NC	Gray	
Alarm output_COM	White/Orange	
Alarm output_NO	White/Blue	
12V power input	Red	Power cable
GND	Black	

Device Installation

- Paste the drill template on the wall with the arrow facing upward. Use a Ø6-6.5mm drill bit to drill two 30mm-depth holes on the A position, and then insert expansion bolts. Be careful not to damage cables in the wall.
- Place the bracket straight up with the arrow facing outward. Knock the expansion bolts into the holes with the pointed tail screws.
- Connect all cables.
 - Connect one end of the network cable (user-prepared) to the network interface on the rear panel, and the other end to the switch or other network device.
 - Connect one end of the integrated cables to the corresponding cable interface on the rear panel, and the other end to the door sensor, alarm, and other devices according to the actual networking.
- Fasten the cover to the access control terminal with three short Phillips screws.
- Secure the access control terminal to the bracket.
 - Use a T10 screwdriver to loosen the tamper-proof screws on both sides of the device that fix the pluggable verification module in the counterclockwise direction (the bottom the module is designed with

an allowance, and the screws will not fall off after loosening, as shown in the left figure).

- Align the hook on the bracket with the groove on the terminal, and secure the terminal to the bracket (as shown in the right figure).
- Tighten the two tamper-proof screws again.

Startup

After the device is installed correctly, connect one end of the power adapter (user-purchased or prepared) to the power interface of the device and the other end to the main supply.

Web Login

<p>Default IP address 192.168.1.13</p> <p>Default username/password admin/123456</p>	<p>Note:</p> <p>For security, please set a strong password of at least nine characters including uppercase and lowercase letters, digits, and special characters. You are strongly recommended to regularly change the device password and keep it secure to ensure that only authorized users can log in.</p>
--	--

Note

For security, please set a strong password of at least nine characters including uppercase and lowercase letters, digits, and special characters. You are strongly recommended to regularly change the device password and keep it secure to ensure that only authorized users can log in.

Recognition Requirements

Photo Collection Requirements

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.

Recognition Position

The correct recognition position is shown in the figure below. Please avoid the person in area 1 or area 2.

Expression and Posture

Expression

Keep a natural expression as shown below.

Posture

The correct and incorrect poses are as shown below.

Disclaimer and Safety Warnings

Copyright Statement

2024 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

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.

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 on our website and get to know the ways we process your personal information. Please be aware, that 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 upgrades or regulatory requirements 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 purposes, 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 non-infringement.

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 attacks, hacking, and viruses. Uniview strongly recommends that users take all necessary measures to enhance the protection of their 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, and 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, and 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 the default password and set a 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 the network security of your device:
- Change the password regularly: Change your device password regularly and keep the password safe. Make sure only the authorized user can log in to the device.
- Enable HTTPS/SSL: Use an 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 a 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 risk 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 the Security Response Center at Uniview's official website.

Safety Warnings

The device must be installed, serviced, and maintained by a trained professional with the 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 but 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 the 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 by 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) by 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 the 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 the battery with an incorrect type;

- Dispose of a battery in a fire or a hot oven, or mechanically crushing or cutting a battery;
- Dispose of the used battery according to your local regulations or the battery manufacturer's instructions.

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.uniview.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 A digital device, under part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense. This equipment complies with FCC radiation exposure limits set forth for uncontrolled environments. This equipment should be installed and operated with a minimum distance of 20cm between the radiator & 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 responsibly.

Battery Regulation- (EU) 2023/1542

The battery in the product complies with the European Battery Regulation (EU) 2023/1542. For proper recycling, return the battery to your supplier or a designated collection point.

Documents / Resources

	<p>UNIVIEW OET-231KH Intelligent Recognition Access Control Terminal [pdf] User Guide OET-231KH Intelligent Recognition Access Control Terminal, OET-231KH, Intelligent Recognition Access Control Terminal, Recognition Access Control Terminal, Access Control Terminal, Control Terminal, Terminal</p>
---	---

References

- [User Manual](#)

[Manuals+](#), [Privacy Policy](#)

This website is an independent publication and is neither affiliated with nor endorsed by any of the trademark owners. The "Bluetooth®" word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. The "Wi-Fi®" word mark and logos are registered trademarks owned by the Wi-Fi Alliance. Any use of these marks on this website does not imply any affiliation with or endorsement.