Ethernet Switch

User Manual

Manual Version: V1.08

Preface

The content of this section is designed to ensure that users use the product correctly to prevent dangers or property loss caused by improper operation. Before using this product, be sure to read this manual carefully. Please keep this manual properly for future reference.

About This Manual

- We recommend that you use this manual under the guidance of a professional.
- This manual is designed for use with multiple product models, and it is not possible to list the appearance and functions of each product individually. Please refer to the actual product for use.
- 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.
- This manual will be updated in real time according to the laws and regulations of the relevant regions. For specific details, please refer to the product's paper copy, QR code, or official website. In case of any discrepancy between the paper copy and the electronic version, the electronic version shall prevail.

About This Product

If the product you have chosen is a video product, please strictly comply with the relevant product regulations. For specific details, please refer to Appendix, Initiative for the Proper Use of Video Products.

Instructions for Use

- This document serves as a guide for use only. All statements, information, and suggestions contained in this document do not constitute any express or implied warranty.
- We assume no responsibility for any special, incidental, consequential, or indirect damages resulting from the use of this manual or the use of our products, including but not limited to losses due to loss of business profits, data or document loss, and product malfunction or information leakage caused by cyber-attack, hacker attack, and virus infections.
- Due to uncertain factors such as the physical environment, there may be discrepancies between the actual values of some data and the reference values provided in the manual. In case of any questions or disputes, the company's final interpretation shall prevail.

Formatting Conventions

The UI formatting conventions used in this document are as follows:

Format	Meaning
Bold	Bold means UI elements (button names, menu names, window names, etc.), e.g., Click **Save**.
>	Indicate a sequence of actions, e.g., click Device Management > Add Device, which means first click Device Management, and then click Add Device.

Symbol Conventions

This document uses various distinctive symbols to highlight areas that require special attention during the operation process. The meanings of these symbols are as follows:

Symbol	Meaning
	NOTE: Provides tips and additional information related to the operation and use of the product.
	CAUTION: Alerts to matters that requires attention during operation, as improper handling may lead to product damage, data loss, or functional abnormalities.
	WARNING: The annotations following this symbol demand extra attention, as improper handling could potentially cause personal injury.

Legal Statement

Copyright Statement

©2025-2026 Zhejiang Uniview Technologies., Co., Ltd. All rights reserved.

All parts of this document, including but not limited to text, images, and graphics, are copyrighted and belong to Zhejiang Uniview Technologies Co., Ltd (hereinafter referred to as "Uniview" "we" “us”). Without our written permission, no organization or individual may excerpt, copy, translate, modify, or disseminate any part or all of the content of this manual in any form.

The products described in this manual may contain software copyrighted by us and any potential licensors. Without the permission of the relevant rights holders, no one may copy, distribute, modify, excerpt, decompile, disassemble, decrypt, reverse engineer, rent, transfer, sublicense, or engage in any other actions that infringe upon the software copyright in any form.

Trademark Acknowledgements

unv uniarch 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. Treubstraa 1, 2288 EG, Rijswijk, Netherlands.

If you have any feedback, please contact us at service@uniview.com.

Disclaimer of Liability

- We assume no responsibility and offer no compensation for any special, incidental, consequential, or indirect damages resulting from the use of this manual or our products, including but not limited to losses related to lost business profits, data, or document loss.
- 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.
- When using this product, please strictly adhere to the applicable laws and regulations to avoid infringing upon the rights of third parties, including but not limited to intellectual property rights, data rights, or other privacy rights. You must also not use this product for the purposes of developing or facilitating the use of weapons of mass destruction, biological or chemical weapons, nuclear weapons, or for any other purposes that violate international norms and regulations.

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.

Safety Precautions

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 Safety

Please use batteries properly; otherwise, there is a risk of fire or explosion.

- Warning: Using incorrect battery models can lead to explosion.
- If you need to replace the battery, it is recommended that you go to an authorized service center or have it replaced under professional supervision. We shall not be held responsible for any issues arising from unauthorized battery replacement.
- When replacing the battery, be sure to use a battery of the same type as the original! Using the wrong model for replacement (such as certain types of lithium batteries) may cause safety protection to fail.
- Batteries must not be exposed to overheat environments such as sunlight, fire, as this may lead to fire, explosion, or combustion.
- Do not dispose of batteries in fire or heating appliances. Do not squeeze, bend, or cut batteries, as it may cause explosion.
- Do not expose batteries to extremely high or low temperatures, or to very low-pressure environments, as this may cause explosion or leakage of flammable liquid/gas.
- Dispose of the used battery according to your local regulations or the battery manufacturer's instructions.
- For products or the included remote control containing a button cell battery: Do not ingest the battery - chemical burn hazard! If swallowed, a button cell battery can cause severe internal burns within 2 hours and may be fatal. Precautions (including but not limited to):
  - Keep new and used batteries away from children.
  - Stop using the product and keep it away from children if the battery compartment is not securely closed.
  - If you suspect that a battery may have been swallowed or inserted inside any part of the body, seek immediate medical attention.

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.
  - Do not include the account name or the reverse of the account name.
  - Avoid using consecutive characters, such as 123, abc, etc.
  - Do not use overlapping characters, such as 111, aaa, etc.
- **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.

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 https://global.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, pursuant to 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.

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 Regulation- (EU) 2023/1542



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

Contents

Preface ii
Legal Statement iii
Safety Precautions iv
1 Login 1
2 Forgot Password 1
3 User 2
4 Device Status 3
5 Switch Configuration 3
6 QoS 4
7 (Optional) PoE 5
8 System 5
Appendix Initiative for the Proper Use of Video Products 6

1 Login

Open a web browser and enter http://ip in the address bar to access the login page. Choose your preferred language. Enter the default username (admin) and password (123456), and then click **Login**.

NOTE!
For the first-time login, please follow the on-screen instructions to change the initial password and bind an email address in case you need to reset the password.

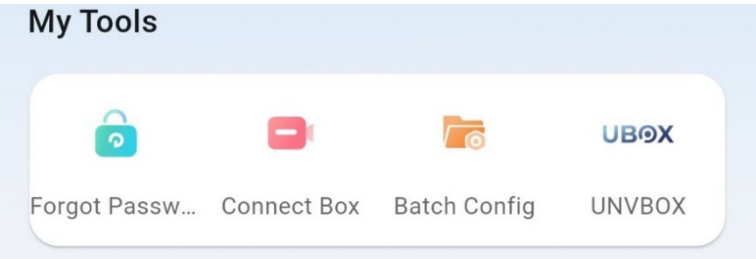
2 Forgot Password

- Method 1: Reset password via UNV-Link Pro app

  (1) On the switch's login page, click **Forgot Password**. The system will generate a QR code containing the device information.

NOTE!
The QR code can be generated regardless of whether the device is online or offline.

  (2) Open the UNV-Link Pro app, tap **Forgot Password** on the home screen, and then scan the generated QR code.

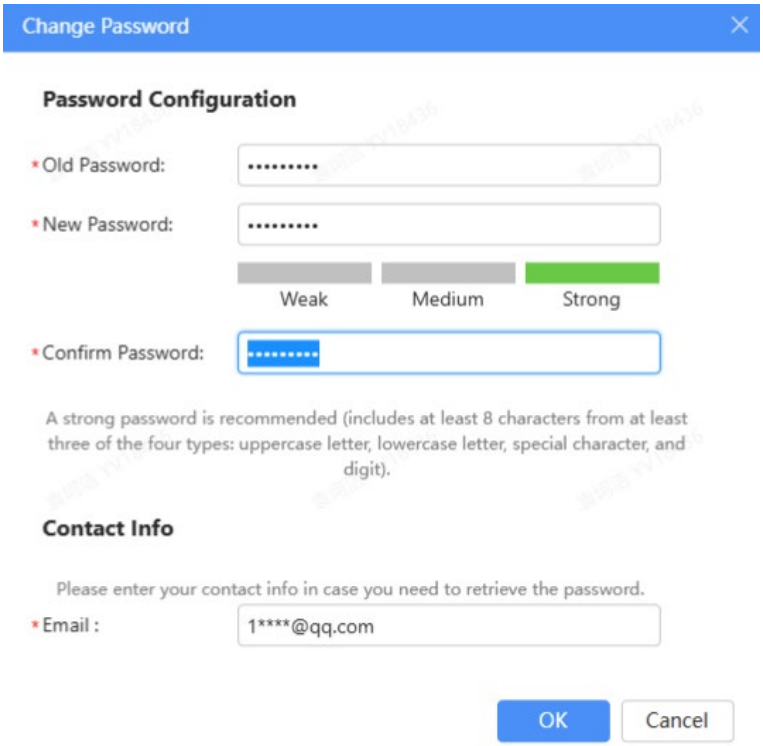


  (3) The app will recognize the device information and send a security code to the configured email address.

NOTE!
If you didn't receive the email, please verify the configured email address or check the signal strength.

  (4) Enter the received security code in the **Retrieve Password** window on the switch's webpage, and then click **OK**.

  (5) Once verified, you can set a new password.



- Method 2: Reset password via website (https://en.ezcloud.uniview.com)

  (1) Log in to https://en.ezcloud.uniview.com. Click for the switch, and then click **Retrieve Password** in the pop-up window.

  (2) Click **Send Code** to send a verification code to the set email address.

  (3) Enter the received verification code to generate a security code.

  (4) On the switch's login page, click **Forgot Password**. Enter the generated security code in the pop-up window, and then click **OK**.

  (5) Once verified, you can set a new password.

NOTE!

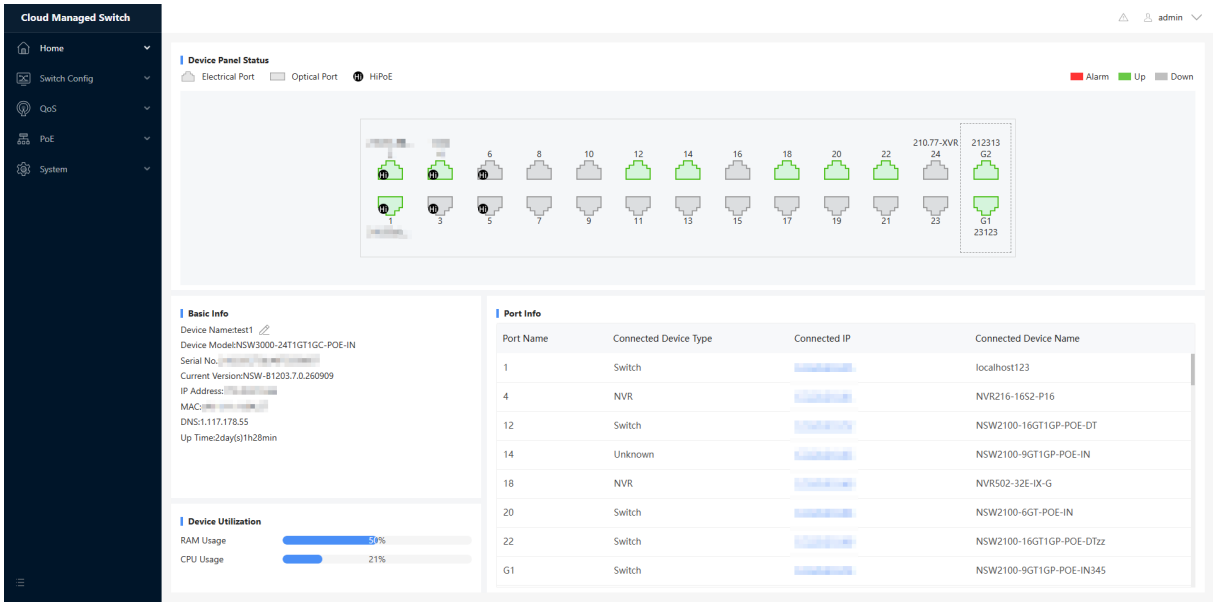
FAQ:

- QR Code Not Generated: Please check if the device is bound to an email address or try restarting the device.
- Invalid Security Code: Please verify if the email address matches the one configured on the device's web interface and check if the security code has expired (valid for only one day).
- Email Not Received: Please check the spam.
- Function Not Supported: Please contact the technical support for assistance.

3 User

Click admin in the upper right corner to expand the drop-down list. Here you can change your password and log out.

4 Device Status



- Device panel status:

Red	Port loop is blocked.
Green	Port is up.
Gray	Port is down.

The real-time port status is displayed in a scrolling manner at the top of the page. Click  to view the real-time alarm list.

NOTE!

- Alarms are categorized as minor, warning, major, and critical. Only major alarms will be displayed in the real-time alarm list.
- When you log out, all real-time alarm information will be cleared.

- Port list description:

  Multiple security devices are connected to the same physical port: The switch connected to the port is a third-party switch. Security devices connected to the switch via the ONVIF protocol will be displayed.

  Multiple switches are connected to the same physical port: The current switch and other switches are connected to an unknown switch.

5 Switch Configuration

- Traffic Statistics: View traffic statistics for each port.
- Port Loop Prevention: Enable/disable port loop detection for each port.

- Port: Enable/disable ports, port isolation, flow control; enter a port description, set the port speed, and duplex mode.
- Extension Mode: Enable/disable extension mode for each port.
- Port Mirroring: Click **Add** and configure parameters as needed.

NOTE!

- Only one port mirroring is allowed.
- For Gigabit models, only downlink ports can be configured.

- MAC Address: Displays learned MAC address information. You may clear the dynamic MAC address as needed.
- VLAN: Click **Add** to create a VLAN ID.
- Port VLAN: Make sure you have created a VLAN ID. Click in the **Operation** column for the port or select port(s) and click **Batch Config**, select the VLAN type, and configure other parameters as needed.
- Link Aggregation: Click **Add**, and select two ports for aggregation.

NOTE!

- 100 Mbps models and Gigabit PoE models support only one link aggregation group consisting of two uplink ports.
- Gigabit standard models support up to 8 link aggregation groups. However, the aggregation of one uplink port and one downlink port is not supported.

6 QoS

- Port Speed Limit:

Click in the **Operation** column for the port or select port(s) and click **Batch Config**, and then configure parameters as needed.

NOTE!

Ports with different bandwidths cannot be configured at the same time. For example, a 100Mbps port cannot be configured with a 1000Mbps port simultaneously.

- Port Storm Control:

Select a type, click , and then configure parameters as needed.

7 (Optional) PoE

- PoE Watchdog: Enable/Disable the PoE Watchdog feature. When enabled, the device monitors the status of PoE ports. If a port shows no traffic for a sustained period (3 consecutive checks at 5-minute interval), the port and PoE power supply will automatically restart in an attempt to restore normal operation.

NOTE!
After 3 consecutive restarts, the port will remain powered on and will no longer attempt to restart.

- HiPoE: Enable/Disable HiPoE power supply for supported ports. When enabled, the port can output up to 45W, suitable for connecting high-power devices.
- PoE Power Supply: Select Port > Enable/Disable. You can select multiple ports and then click to enable/disable power supply.

8 System

- Network: Set IP address, DHCP, and DNS parameters.
- Device Maintenance: Upgrade device; restore defaults; import/export configuration; export logs; restart device.
- Security: Unlock devices that have been locked due to multiple failed connections.
- Neighbor Node Info: Displays information about other switches that are on the same LAN as the current switch.
- Monitoring Node Info: Displays information about security devices connected to the switch via the ONVIF protocol.
- (Optional) Cloud Service: Enable/disable/log out of the cloud service. When enabled, you can perform operations such as managing projects, configuring devices, and viewing port information on the mobile app.
- Telnet: Enable/disable Telnet.
- Network tool: Diagnose network connectivity issues using the Ping or Trace Route diagnostic tool.

Appendix Initiative for the Proper Use of Video Products

Thank you for choosing our products.

As technology advances, its applications have a profound impact on every aspect of our lives. As a high-tech company, we have an increasingly deep understanding of the contributions of technology in enhancing efficiency and improving the quality of life. At the same time, we are also aware that the misuse of technology can cause harm. For instance, video surveillance products, due to their ability to record real, complete, and clear images, have significant value in tracing and reconstructing facts. However, improper dissemination, use, and processing of image records can also lead to issues that infringe upon the legitimate rights and interests of others. To continuously promote technology for good, we advocate that every user should use technology and video products responsibly. This includes not only adhering to legal and regulatory requirements but also following the constraints of moral customs, to jointly establish and maintain a positive social environment and atmosphere. Please read the following proposals carefully:

- Everyone has a reasonable expectation of privacy, and the installation of video products should not violate the reasonable privacy expectations of an individual. When installing video surveillance products in public places, it should be done in a reasonable and effective manner with clear indications of the surveillance area. When installing video products in non-public places, one should not infringe upon the rights and interests of others, including but not limited to not installing video surveillance products without the consent of the stakeholders, or installing highly covert video surveillance products.
- During the use of video products, real activities within specific time and space frames will be recorded under certain conditions. Users should reasonably define the rights they have within that specific range to avoid infringing upon the portrait, privacy, or other legal rights of others.
- During the use of video products, a continuous stream of video image data originating from real-life scenes, including a large amount of biometric data (such as facial data), will be generated. This data can be applied or further processed for various purposes. The video products themselves are not capable of distinguishing between good and bad uses of data. The outcomes of data usage depend on the actions of the data controllers, their intentions, and purposes. Data controllers should adhere to legal requirements and norms, as well as respect international conventions, local customs, societal ethics, public order, and moral standards - all non-mandatory regulations. It is essential for data controllers to respect individuals' privacy, likeness, and other rights during data usage.
- Considering the ongoing generation of video image data by video products, which carries the rights protection requirements, value claims, or other demands of various stakeholders, it is crucial to ensure the security of the product and its data. Users of the product and data controllers should take reasonable and necessary measures to ensure network and data security, to prevent data leaks or improper use. This includes, but is not limited to, carefully allocating the use and management permissions of the product, and establishing and continuously optimizing the security systems of various networks, such as the Internet and local area networks, that the product connects to, in conjunction with the product's usage scenarios.
- Video products have made significant contributions to enhancing societal security, and we believe these products will continue to play a positive role in more aspects of social life. Any use of these products to infringe upon human rights or engage in illegal activities is contrary to the original intent of technological innovation and product development. Therefore, we encourage every user to establish an assessment and tracking mechanism to ensure that the product is used properly, reasonably, and in good faith.