

Smart ANPR Camera

User's Manual







Foreword

General

The manual introduces the structure and installation of the smart camera with access automatic number plate recognition (hereinafter referred to as "the camera").

Safety Instructions

The following signal words might appear in the manual.

| Signal Words | Meaning |
|--|--|
|  DANGER | Indicates a high potential hazard which, if not avoided, will result in death or serious injury. |
|  CAUTION | Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results. |
|  TIPS | Provides methods to help you solve a problem or save time. |
|  NOTE | Provides additional information as a supplement to the text. |

Revision History

| Revision Content | Release Time | Revision Content |
|------------------|----------------|------------------|
| V1.0.0 | First release. | October 2022 |

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF

format) cannot be opened.

- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the device, hazard prevention, and prevention of property damage. Read carefully before using the device, comply with the guidelines when using it, and keep the manual safe for future reference.

Transportation Requirements



Transport the device under allowed humidity and temperature conditions.

Storage Requirements



Store the device under allowed humidity and temperature conditions.

Installation Requirements



- Do not connect the power adapter to the device while the adapter is powered on.
- Strictly comply with the local electrical safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the device.
- Do not connect the device to two or more kinds of power supplies, to avoid damage to the device.



- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the device in a place exposed to sunlight or near heat sources.
- Keep the device away from dampness, dust, and soot.
- Put the device in a well-ventilated place, and do not block its ventilation.
- Use an adapter or cabinet power supply provided by the manufacturer.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Please note that the power supply requirements are subject to the device label.
- The device is a class I electrical appliance. Make sure that the power supply of the device is connected to a power socket with protective earthing.
- An emergency disconnect device must be installed during installation and wiring at a readily accessible location for emergency power cut-off.
- Disconnect the device when installing and connecting the lens.

Operation Requirements



- Make sure that the power supply is correct before use.
- Do not unplug the power cord on the side of the device while the adapter is powered on.
- Operate the device within the rated range of power input and output.
- Use the device under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the device, and make sure that there is no object filled with

liquid on the device to prevent liquid from flowing into it.

- Do not disassemble the device.
- Do not aim the device at strong light sources (such as lamplight, and sunlight) when focusing it.
- Do not vibrate, squeeze or immerse the device in liquid during transportation, storage or installation.
- Do not block the ventilation near the device.
- We recommend you use the device with a lightning protection device for stronger protection against lightning. For outdoor scenarios, strictly comply with the lightning protection regulations.
- Ground the function earthing portion of the device (grounding cable or lightning surge protector) to improve its reliability. The device is a class I electrical appliance. Make sure that the power supply of the device is connected to a power socket with protective earthing.
- The device must be used with the protective cover for outdoor scenarios to avoid the risk of water damage to the device.
- Protect the line cord and wires from being walked on or squeezed particularly at plugs, power sockets, and the point where they exit from the device.
- Modify the default password of the device after first-time login to prevent the device from being stolen.

Maintenance Requirements

- Pack the device with packaging provided by its manufacturer or packaging of the same quality before sending it back for repair.
- Please do not touch the photosensitive device with your hands. Use an air blower to clean off the dust and filth on the lens.
- Clean the surface of the device with a soft dry cloth or a clean soft cloth dipped in neutral detergent.
- Use the accessories suggested by the manufacturer. Installation and maintenance must be performed by qualified professionals.

Table of Contents

- ForewordI
- Important Safeguards and Warnings..... III
- 1 Introduction 1
 - 1.1 Overview 1
 - 1.2 Features 1
- 2 Structure3
 - 2.1 Dimensions3
 - 2.2 Entire Device3
 - 2.3 Rear Panel.....4
 - 2.4 Cable4
- 3 Installation.....6
 - 3.1 Pole Mount.....6
 - 3.2 Wall Mount.....6
 - 3.3 Ceiling Mount7
- Appendix 1 Cybersecurity Recommendations.....8

1 Introduction

1.1 Overview

The camera adopts intelligent deep learning algorithm. It supports vehicle detection, license plate recognition, logo recognition, model recognition, and color recognition, and encoding mode such as H.265.

The camera consists of protective housing, illuminator, and intelligent HD camera. The intelligent HD camera adopts progressive scanning CMOS, which owns several features such as high definition, low illuminance, high frame rate, and excellent color rendition.

The camera is extensively applied to vehicle capture, and recognition of community road, parking lot, and other entrance, and exit surveillance.

1.2 Features



The features are available on select modes, and might differ from the actual camera.

Permission Management

- Each user group owns permissions. Permissions of a user cannot exceed the permissions of its group.
- 2 user levels.
- Permission of opening barrier, and blacklist alarm function.
- Device configuration, and permission management through Ethernet.

Storage

- Stores corresponding video data onto the central server according to the configuration (such as alarm, and timing settings).
- Users can record through web according to their requirements. The recorded video file will be stored on the computer where client is located.
- Supports local hot swapping of storage card, and storage when network disconnected. It overwrites stored pictures, and videos automatically when memory becomes insufficient.
- Stores 1024 log records, and user permission control.
- Supports FTP storage, and automatic network replenishment (ANR).

Alarm

- It can trigger alarm upon camera operation exceptions through network, such as memory card damage.
- Some devices can connect to various alarm peripherals to respond to external alarm input in real time (within 200 ms). It can correctly deal with various alarms according to the linkage predefined by users, and generate corresponding voice prompt (users are allowed to record voice in advance).

Network Monitoring

- Transmits video data of single channel compressed by device to network terminal, and make it reappear after decompression through network. Keep delay within 500ms when bandwidth is allowed.
- Supports maximum 10 users online at the same time.
- Supports system access, and device management through web.
- Video data transmission adopts HTTP, TCP, UDP, MULTICAST, and RTP/RTCP.

Capture, and Recognition

- Recognition of number plate, and other vehicle information, including vehicle color, logo, model, and other vehicle features.
- Supports setting OSD information, and configuring location of channel, and picture.
- Supports picture capture, and encoding. Supports picture watermark encryption to prevent pictures from being tampered.
- The captured pictures can automatically record vehicle time, location, license plate, vehicle color, and more.

Peripheral Control

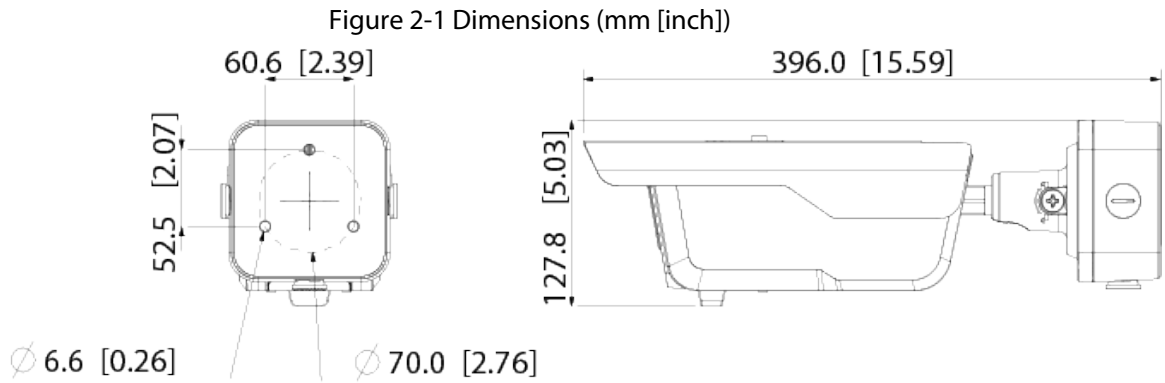
- Peripheral control: Supports setting various peripheral control protocols, and connection pages.
- Connects to external devices such as vehicle detector, signal detector, and more.

Auto Adjustment

- Auto iris: Automatically adjusts the iris opening to the changing light throughout the day.
- Auto white balance: Accurately displays the object color when light condition changes.
- Auto exposure: Automatically adjusts shutter speed according to the exposure value of the image measured by the metering system, and according to shutter, and iris exposure set by factory defaults.
- Auto gain: Automatically increases camera sensitivity when illuminance is very low, enhancing image signal output so that the camera can acquire clear, and bright image.

2 Structure

2.1 Dimensions



2.2 Entire Device

Figure 2-2 Entire device structure

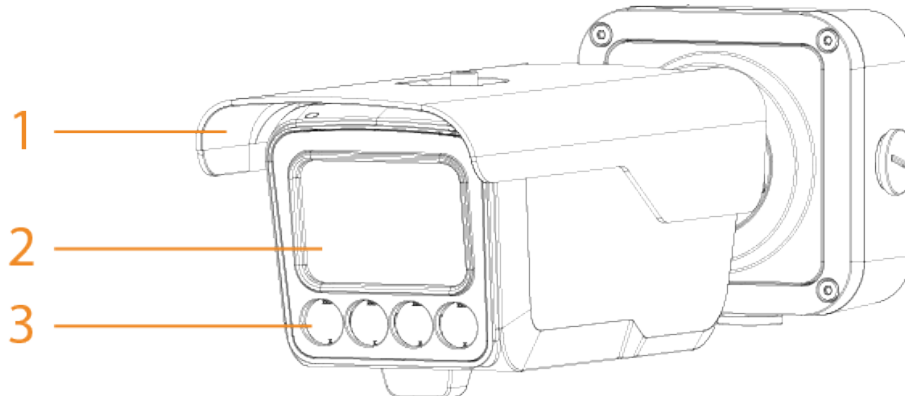


Table 2-1 Structure description

| No. | Description | No. | Description |
|-----|------------------|-----|-------------|
| 1 | Protective cover | 3 | Illuminator |
| 2 | Lens | — | |

2.3 Rear Panel

Figure 2-3 Bottom panel structure

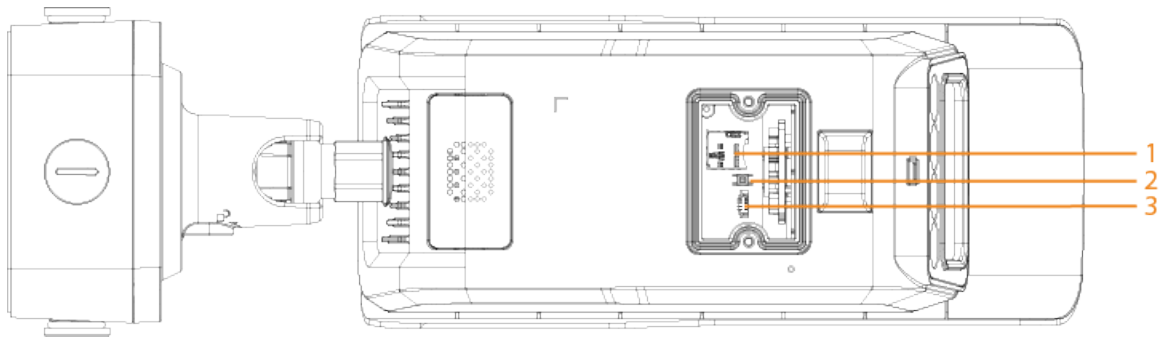


Table 2-2 Bottom panel description

| No. | Description | No. | Description |
|-----|---------------------|-----|----------------|
| 1 | Slot for an SD card | 3 | Debugging port |
| 2 | Hardware reset | — | |

2.4 Cable

Figure 2-4 Cables

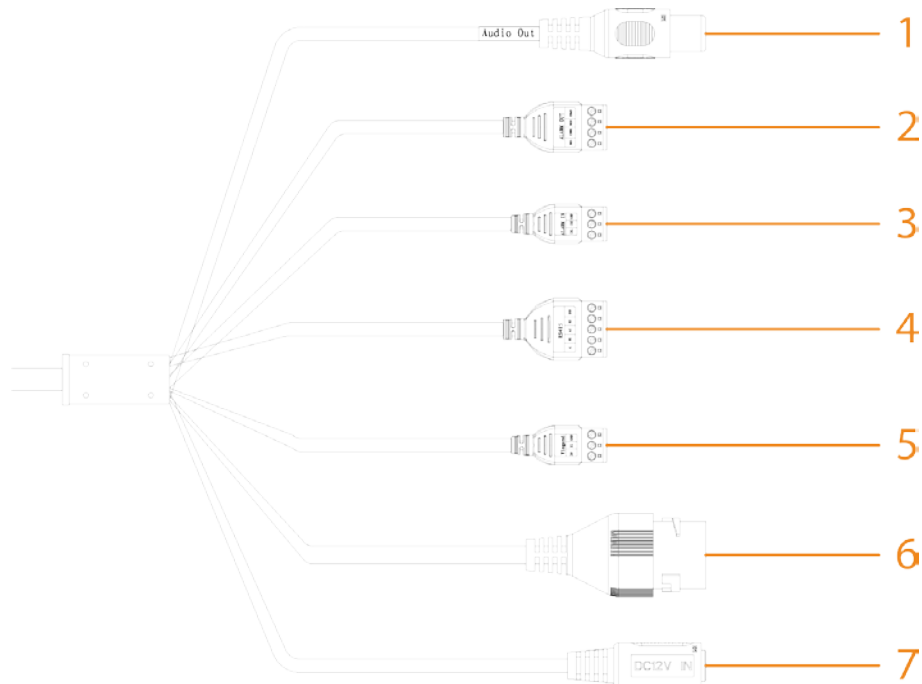



Table 2-3 Cable description

| No. | Function | Description |
|-----|-----------|---|
| 1 | AUDIO OUT | The camera sends out audio signal through this port. |
| 2 | Alarm out | Alarm output, connecting to barrier, and alarm output devices such as alarm light. |
| 3 | Alarm in | Alarm input, connecting to vehicle detector, IR detector, induction loop, and more. |

| No. | Function | Description |
|-----|----------|---|
| 4 | RS-485 | Connects to displays and other external devices. |
| 5 | Wiegand | Connects and sends number plates to access controller. |
| 6 | LAN | Connects to a network. It also supports PoE power supply. |
| 7 | 12 VDC | Connects to 12 VDC power supply.  Device damage will occur if power is not supplied correctly. |

3 Installation



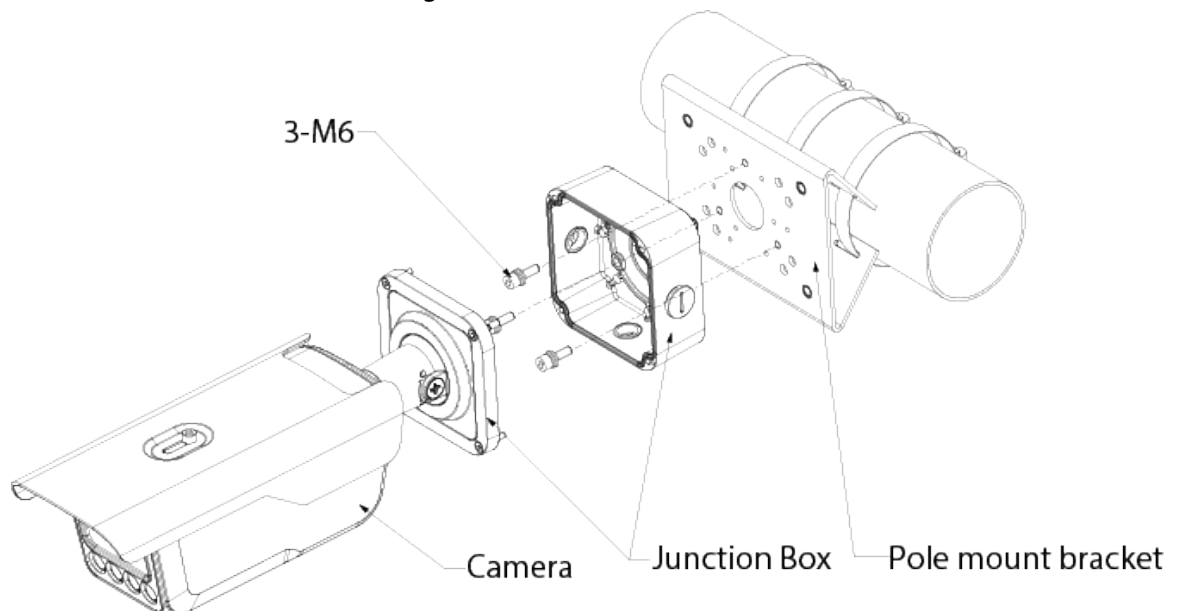
The following installation figures are for reference only, and might differ from the actual product.

3.1 Pole Mount

Procedure

- Step 1 Fix the pole mount bracket to the pole.
- Step 2 Use 3 M6 screws to fix the junction box to the pole mount bracket.
- Step 3 Tighten the screws on the end of the camera to fix it to the junction box.

Figure 3-1 Pole mount

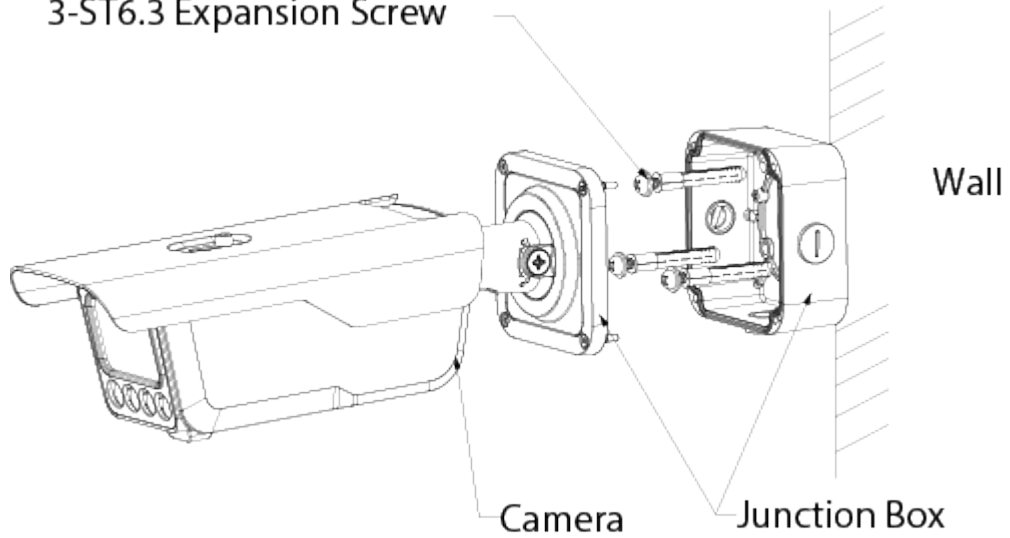


3.2 Wall Mount

Procedure

- Step 1 Drill holes on the wall according to the holes on the junction box.
- Step 2 Use 3 ST6.3 expansion screws to fix junction box to the wall.
- Step 3 Tighten the screws on the end of the camera to fix it to the junction box.

Figure 3-2 Wall mount
3-ST6.3 Expansion Screw

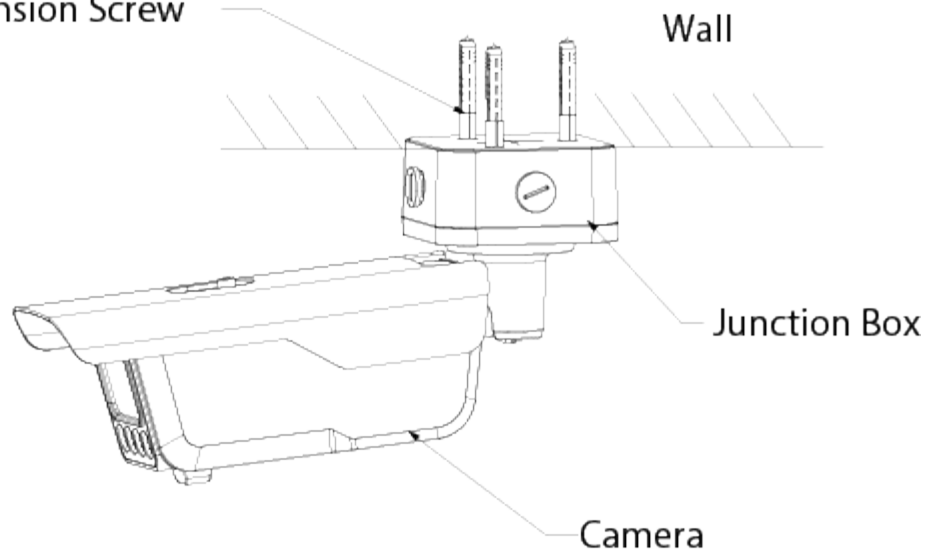


3.3 Ceiling Mount

Procedure

- Step 1 Drill holes on the ceiling according to the holes on the junction box.
- Step 2 Use 3 ST6.3 expansion screws to fix the junction box to the ceiling.
- Step 3 Tighten the screws on the end of the camera to fix it to the junction box.

Figure 3-3 Ceiling mount
3-ST6.3Expansion Screw



Appendix 1 Cybersecurity Recommendations

Mandatory actions to be taken for basic device network security:

1. Use Strong Passwords

Please refer to the following suggestions to set passwords:

- The length should not be less than 8 characters.
- Include at least two types of characters; character types include upper and lower case letters, numbers and symbols.
- Do not contain the account name or the account name in reverse order.
- Do not use continuous characters, such as 123, abc, etc.
- Do not use overlapped characters, such as 111, aaa, etc.

2. Update Firmware and Client Software in Time

- According to the standard procedure in Tech-industry, we recommend to keep your device (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the device is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
- We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your device network security:

1. Physical Protection

We suggest that you perform physical protection to device, especially storage devices. For example, place the device in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable device (such as USB flash disk, serial port), etc.

2. Change Passwords Regularly

We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. Set and Update Passwords Reset Information Timely

The device supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. Enable Account Lock

The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. Change Default HTTP and Other Service Ports

We suggest you to change default HTTP and other service ports into any set of numbers between 1024–65535, reducing the risk of outsiders being able to guess which ports you are using.

6. Enable HTTPS

We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. MAC Address Binding

We recommend you to bind the IP and MAC address of the gateway to the device, thus reducing the risk of ARP spoofing.

8. Assign Accounts and Privileges Reasonably

According to business and management requirements, reasonably add users and assign a

minimum set of permissions to them.

9. **Disable Unnecessary Services and Choose Secure Modes**

If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

- SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
- SMTP: Choose TLS to access mailbox server.
- FTP: Choose SFTP, and set up strong passwords.
- AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

10. **Audio and Video Encrypted Transmission**

If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. **Secure Auditing**

- Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
- Check device log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. **Network Log**

Due to the limited storage capacity of the device, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

13. **Construct a Safe Network Environment**

In order to better ensure the safety of device and reduce potential cyber risks, we recommend:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
- Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.