

Smart ANPR Camera

User Manual



V1.0.1

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").

Symbols

The following symbols might appear in the manual.

Symbol	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
V1.0.1	Updated the installation content.	September 2026
V1.0.0	First release.	October 2022

Privacy Protection Notice

As the device user, you might collect the personal data of individuals such as their names, email addresses, face images, audio and fingerprints. You shall be fully responsible for any activities associated with processing personal data. You commit to comply with your local privacy protection laws and regulations to protect the legitimate rights and interests of individuals, and shall implement measures which are required by applicable law, including but not limited to, providing clear and comprehensive information to individuals before processing their personal data, obtaining consent from individuals when necessary, informing individuals of the existence of the surveillance area, and providing required contact information.

Intelligent Product Usage Statement

Intelligent products utilize AI technology to effectively enhance security. The intelligent recognition and alarm functions of the product might be affected by factors such as environmental lighting, camera angles, object obstructions, and network delays, potentially leading to false alarms, missed alerts, or response delays. This intelligent product is solely intended to be used as a security assistance tool. The results from performing identification are for reference only and do not constitute absolute guarantee of personal or property safety. Users need to combine these products with necessary physical security measures to enhance overall protection. Except as otherwise provided by laws or in the event of intentional or gross negligence on the part of the company, the company shall not be liable for any losses caused by the aforementioned factors not attributable to the company.

About the Manual

- This manual is provided for general reference only. Discrepancies might exist between the product and this manual, including but not limited to printed, electronic, or any other editions.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. Specifications and documentation are subject to change without prior notice. For the latest versions, as well as legal notices, consult the printed manual, the product webpage, our official website, or scan the QR code to access the electronic edition.
- The manual will be updated as necessary to reflect product changes and applicable legal requirements. These updates will not diminish your statutory rights, nor will they remove or weaken the safety information or essential instructions provided at the time of purchase.
- Although we make every effort to ensure accuracy, errors or deviations in descriptions of functions, operations, or technical data might occur. If there is any uncertainty or controversy, we reserve the right of final explanation.
- All trademarks, registered trademarks and company names referenced in this manual are the property of their respective owners.

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.
- Pack the device with packaging provided by its manufacturer or packaging of the same quality before transporting it.
- Do not place heavy stress on the device, violently vibrate or immerse it in liquid during transportation.

Storage Requirements



- Store the device under allowed humidity and temperature conditions.
- Do not place heavy stress on the device, violently vibrate or immerse it in liquid during storage.

Installation Requirements



WARNING

- Strictly comply with the local electrical safety code and standards. Make sure that 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.
- The power supply must meet the rated voltage requirements as indicated on the device label.
- If the device uses a power adapter, ensure it meets the following requirements:
 - ◊ If a power adapter was shipped with your device, we recommend you use it. If you need to buy a separate adapter, make sure it meets the following requirements.
 - The power supply must conform to the requirements of IEC 60950-1 and IEC 62368-1 standards.
 - The voltage must meet the SELV (Safety Extra Low Voltage) requirements and not exceed ES-1 standards.

- When the power of the device does not exceed 100 W, the power supply must meet LPS requirements and be no higher than PS2.
- ◇ Do not connect the power adapter to the device while the adapter is powered on.



- 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.
- Do not place heavy stress on the device, violently vibrate or immerse it in liquid during installation.
- Put the device in a well-ventilated place, and do not block its ventilation.
- 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 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

Foreword.....	I
Important Safeguards and Warnings.....	III
1 Introduction.....	1
1.1 Overview.....	1
1.2 Features.....	1
2 Structure.....	4
2.1 Dimensions.....	4
2.2 Entire Device.....	4
2.3 Bottom Panel.....	5
2.4 Cable.....	5
3 Installation.....	7
3.1 Pole Mount.....	7
3.2 Wall Mount.....	7
3.3 Ceiling Mount.....	8
Appendix 1 Security Recommendation.....	9

1 Introduction

1.1 Overview

The camera adopts an 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 for community roads, parking lots, and other entrance and exit surveillance.

1.2 Features



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

Permission Management

- Each user group has permissions. Permissions of a user cannot exceed the permissions of its group.
- 2 user levels.
- Permission of opening barrier and blocklist 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 the web according to their requirements. The recorded video file will be stored on the computer where the 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 an alarm upon camera operation exceptions through the 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 a single channel compressed by the device to a network terminal, and makes it reappear after decompression through the network. Keep delay within 500 ms 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

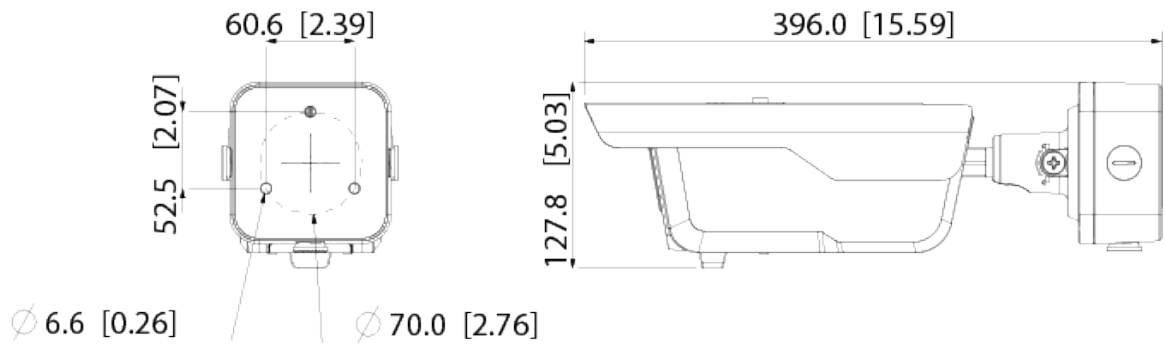
- Auto iris: Automatically adjusts the iris opening to the changing light throughout the day.
- Auto white balance: Accurately displays the object color when light condition changes.

- 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

Figure 2-1 Dimensions (mm [inch])



2.2 Entire Device

Figure 2-2 Entire device structure

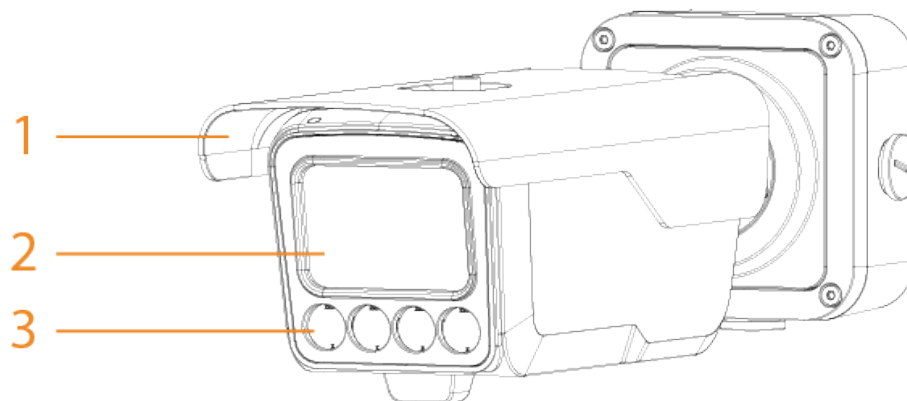


Table 2-1 Structure description

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

2.3 Bottom Panel

Figure 2-3 Bottom panel structure

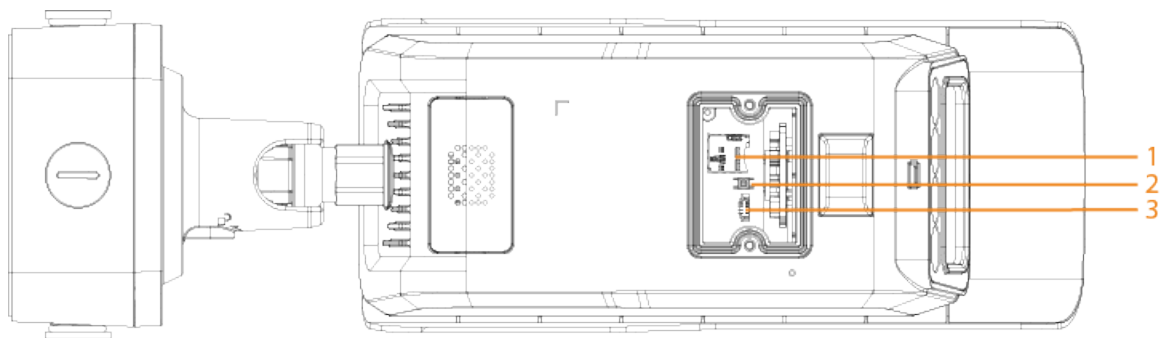


Table 2-2 Bottom panel description

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

2.4 Cable

Figure 2-4 Cables

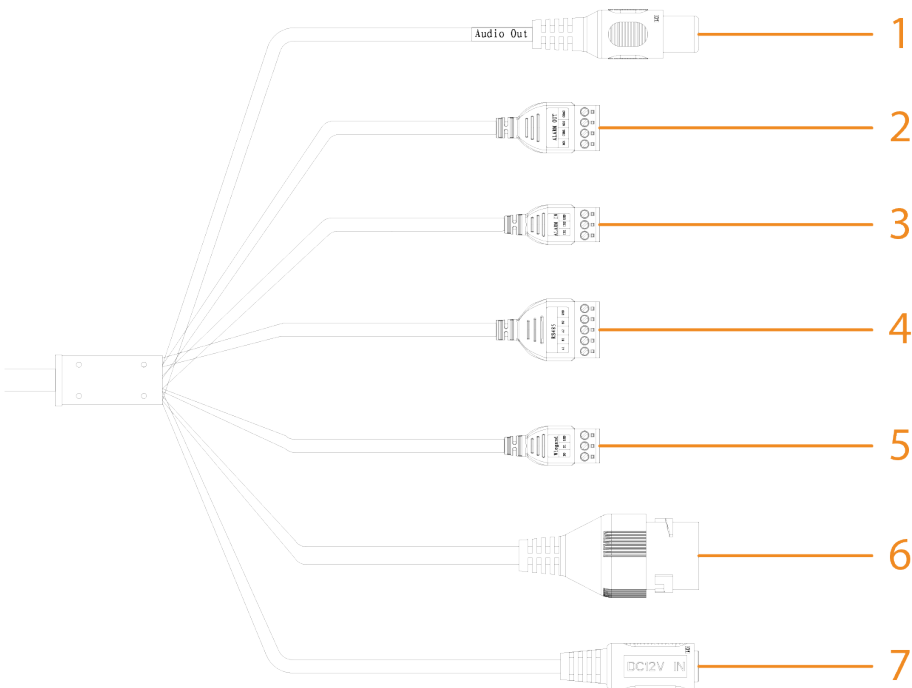


Table 2-3 Cable description

No.	Function	Description
1	AUDIO OUT	The camera sends out audio signals through this port.

No.	Function	Description
2	Alarm out	Alarm output, connecting to the barrier, and alarm output devices such as alarm light.
3	Alarm in	Alarm input, connecting to the vehicle detector, IR detector, induction loop, and more.
4	RS-485	Connects to displays and other external devices.
5	Wiegand	Connects and sends number plates to the access controller.
6	LAN	Connects to a network. It also supports Power over Ethernet (PoE).
7	12 VDC	Connects to 12 VDC power supply.  Device damage will occur if power is not supplied correctly.

3 Installation



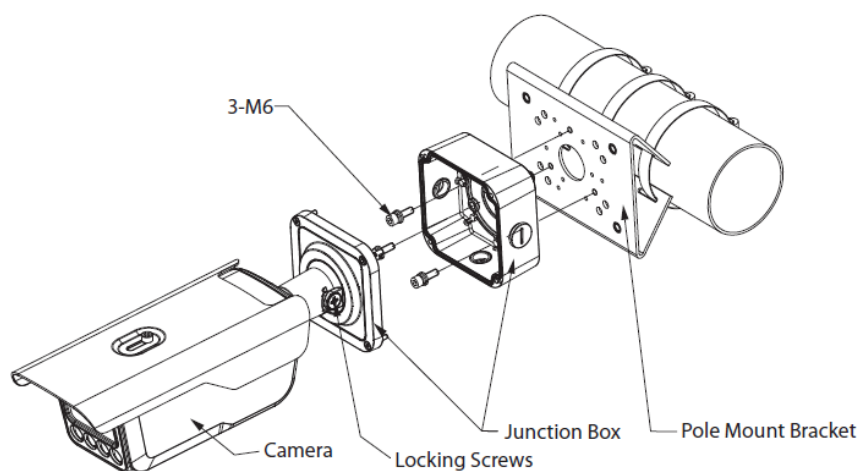
The following installation figures are for reference only, and might differ from the actual product.

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 locking screws on the end of the camera to fix it to the junction box.
- Step 4 Loosen the locking screws using the Allen wrench, and then adjust the camera angle as needed.
- Step 5 Tighten the locking screws again after adjustment is complete.

Figure 3-1 Pole mount

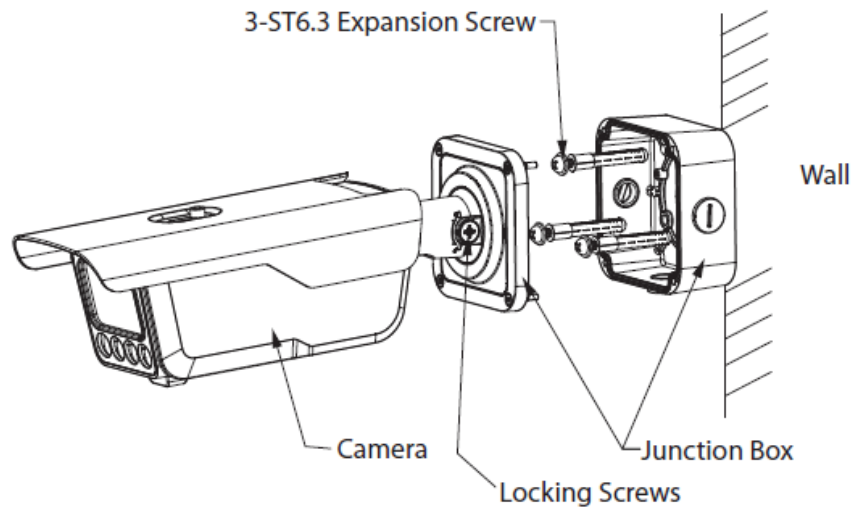


3.2 Wall Mount

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 the junction box to the wall.
- Step 3 Tighten the locking screws on the end of the camera to fix it to the junction box.
- Step 4 Loosen the locking screws using the Allen wrench, and then adjust the camera angle as needed.
- Step 5 Tighten the locking screws again after adjustment is complete.

Figure 3-2 Wall mount

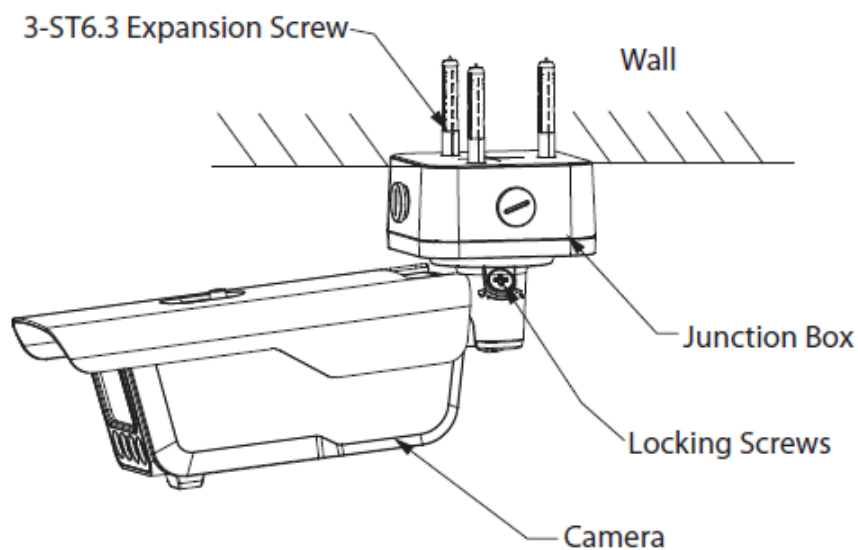


3.3 Ceiling Mount

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 locking screws on the end of the camera to fix it to the junction box.
- Step 4 Loosen the locking screws using the Allen wrench, and then adjust the camera angle as needed.
- Step 5 Tighten the locking screws again after adjustment is complete.

Figure 3-3 Ceiling mount



Appendix 1 Security Recommendation

Account Management

1. Use complex 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: 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 repeating characters, such as 111, aaa, etc.

2. Change passwords periodically

It is recommended to periodically change the device password to reduce the risk of being guessed or cracked.

3. Allocate accounts and permissions appropriately

Appropriately add users based on service and management requirements and assign minimum permission sets to users.

4. Enable account lockout function

The account lockout function is enabled by default. You are advised to keep it enabled to protect account security. After multiple failed password attempts, the corresponding account and source IP address will be locked.

5. Set and update password reset information in a timely manner

The device supports password reset function. To reduce the risk of this function being used by threat actors, if there is any change in the information, please modify it in time. When setting security questions, it is recommended not to use easily guessed answers.

Service Configuration

1. Enable HTTPS

It is recommended that you enable HTTPS to access web services through secure channels.

2. Encrypted transmission of audio and video

If your audio and video data contents are very important or sensitive, it is recommended to use encrypted transmission function in order to reduce the risk of your audio and video data being eavesdropped during transmission.

3. Turn off non-essential services and use safe mode

If not needed, it is recommended to turn off some services such as SSH, SNMP, SMTP, UPnP, AP hotspot etc., to reduce the attack surfaces.

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

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

4. **Change HTTP and other default service ports**

It is recommended that you change the default port of HTTP and other services to any port between 1024 and 65535 to reduce the risk of being guessed by threat actors.

Network Configuration

1. **Enable Allowlist**

It is recommended that you turn on the allowlist function, and only allow IP in the allowlist to access the device. Therefore, please be sure to add your computer IP address and supporting device IP address to the allowlist.

2. **MAC address binding**

It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.

3. **Build a secure network environment**

In order to better ensure the security of devices and reduce potential cyber risks, the following are recommended:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network;
- According to the actual network needs, partition the network: if there is no communication demand between the two subnets, it is recommended to use VLAN, gateway and other methods to partition the network to achieve network isolation;
- Establish 802.1x access authentication system to reduce the risk of illegal terminal access to the private network.

Security Auditing

1. **Check online users**

It is recommended to check online users regularly to identify illegal users.

2. **Check device log**

By viewing logs, you can learn about the IP addresses that attempt to log in to the device and key operations of the logged users.

3. **Configure network log**

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

Software Security

1. **Update firmware in time**

According to the industry standard operating specifications, the firmware of devices needs to be updated to the latest version in time in order to ensure that the device has the latest functions and security. If the device is connected to the public network, it is recommended to enable the online upgrade automatic detection function, so as to obtain the firmware update information released by the manufacturer in a timely manner.

2. **Update client software in time**

It is recommended to download and use the latest client software.

Physical Protection

It is recommended that you carry out physical protection for devices (especially storage devices), such as placing the device in a dedicated machine room and cabinet, and having access control and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).