

Encoding Box

Quick Start Guide



V1.0.3

Foreword

General

This manual introduces the functions and operations of the encoding box device (hereinafter referred to as "the Device").

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.
 WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate 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

Version	Revision Content	Release Time
V1.0.3	Update encode parameters configuration.	December 2024
V1.0.2	Update web photos.	June 2023
V1.0.1	Update device photos.	July 2022
V1.0.0	First release.	August 2021

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, and car 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



- Electrical Hazard

Preventive measures: Make sure the power is off when you put your hand into the device.

- Stability Hazard

Possible result: The rack might fall down and cause serious personal injury.

Preventive measures (including but not limited to):

- ◇ Before extending the rack to the installation position, read the installation instructions.
- ◇ When the Device is installed on the slide rail, do not place any load on it.
- ◇ Do not retract the slide rail while the Device is installed on it.



- Rotating Fan Blades Hazard

Avoid touching the fan blades, especially when they are moving.

-  Before installation, disconnect all the power cords.
- Connect the device to the adapter before power on.
- Strictly abide by local electrical safety standards, and make sure that the voltage in the area is steady and conforms to the power requirements of the device.
- Do not connect the device to more than one power supply. Otherwise, the device might become damaged.



- The device must be installed in a location that only professionals can access. Non-professionals are not allowed to enter the installation area.

- When installing the device, make sure that the power plug can be easily reached to cut off the power.
- Observe all safety procedures and wear required protective equipment provided for your use while working at heights.
- Do not expose the device to direct sunlight or heat sources.
- Do not install the device in humid, dusty or smoky places.
- Install the device in a well-ventilated place, and do not block the ventilator of the device.
- Use the power adapter or case power supply provided by the device manufacturer.
- Please follow the electrical requirements to power the device.
 - ◇ Following are the requirements for selecting a power adapter.
 - 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.
 - ◇ We recommend using the power adapter provided with the device.
 - ◇ When selecting the power adapter, the power supply requirements (such as rated voltage) are subject to the device label.
- Connect class I electrical appliances to a power socket with protective earthing.
- There should be enough gap between the device and the surrounding area to ensure heat dissipation.
- The rated current and power of the device are 2 A and 24 W respectively.

Operation Requirements



-  The Device or remote control contains button batteries. Do not swallow the batteries due to the risk of chemical burns.

Possible result: The swallowed button battery can cause serious internal burns and death within 2 hours.

Preventive measures (including but not limited to):

- ◇ Keep new and used batteries out of reach of children.
- ◇ If the battery compartment is not securely closed, stop using the product immediately and keep out of reach of children.
- ◇ Seek immediate medical attention if a battery is believed to be swallowed or inserted inside any part of the body.
- Battery Pack Precautions

Preventive measures (including but not limited to):

- ◇ Do not transport, store or use the batteries in high altitudes with low pressure and environments with extremely high and low temperatures.
- ◇ Do not dispose the batteries in fire or a hot oven, or mechanically crush or cut the batteries to avoid an explosion.
- ◇ Do not leave the batteries in environments with extremely high temperatures to avoid explosions and leakage of flammable liquid or gas.
- ◇ Do not subject the batteries to extremely low air pressure to avoid explosions and the leakage of flammable liquid or gas.



WARNING

- Operating the device in a domestic environment may cause radio interference.
- Place the device in a location that children cannot easily access.
-  High Current

Preventative measure: Ground the screw of the device to protective ground before you power it on.

-  Do not use multiple devices together to avoid generating high current.

Preventative measure: Ground the device to protective ground before you power it on.



- Make sure that the power supply of the device works properly before use.
- Do not pull out the power cable of the device while it is powered on.
- Only use the device within the rated power range.
- Transport, use and store the device under allowed humidity and temperature conditions.
- Prevent liquids from splashing or dripping on the device. Make sure that there are no objects filled with liquid on top of the device to avoid liquids flowing into it.
- Do not disassemble the device.
- Operating temperature: -10 °C to +45 °C.

Maintenance Requirements



DANGER

Replacing unwanted batteries with the wrong type of new batteries might result in explosion.

Preventive measures (including but not limited to):

- Replace unwanted batteries with new batteries of the same type and model to avoid the risk of fire and explosion.
- Dispose of the old batteries as instructed.
- Power off the device before maintenance.

Table of Contents

Foreword.....	I
Important Safeguards and Warnings.....	III
1 Product Overview.....	1
1.1 Product Profile.....	1
1.2 Features.....	1
2 Unpacking and Cable Connection.....	3
2.1 Unpacking and Checking.....	3
2.2 Device Structure.....	3
2.2.1 Front Panel.....	3
2.2.2 Rear Panel.....	4
3 Web Operations.....	5
3.1 Network Connection.....	5
3.2 Login.....	5
3.3 Configuring Encode Parameters.....	6
Appendix 1 Security Recommendation.....	9

1 Product Overview

1.1 Product Profile

This encoding box is a network audio and video encoding device designed for online video surveillance system. It features powerful data processing capability and stable network function. It is easy to extend, maintain, and convenient to access. This design facilitates installation, deployment, unified control and system management of the entire online video surveillance system, while substantially reducing overall system cost.

With embedded operating system, the Device guarantees that the online video surveillance system works in a safe, stable, reliable and efficient way.

1.2 Features

Table 1-1 Features

Unit	Function	Description
Encoding	Encoding performance	Collects audio and video signals through the HDMI and DP ports, and then encodes (H.264/H.265) the signal sources which are transmitted through network. You can preview images of signal source on the web.
Network	Attribute configuration	IP, gateway, subnet mask and other network parameter configuration can be controlled remotely with network.
	NTP	Synchronize system time with the NTP server.
Alarm	Buzzer alarm	Provides buzzer alarm in case of network offline, IP address conflict and MAC address conflict.
Serial port	General serial port	Device debugging console.
User management	Account management	• Add, delete, and modify users or user groups. • Modify user password.
	Authority management	Configure different authorities for different users.
	Security management	The account will be locked for 30 minutes after 5 consecutive failed login attempts.
Others	Version information	Displays important hardware port information and software version information.
	Search log	Important events are recorded in the log. You can search for the log according to category.
	Time synchronization	System time can be configured manually, or synchronized directly.
	Auto maintenance	Provides automatic maintenance of the Device at a fixed time.
	DNS	Domain name service.

Unit	Function	Description
	Program upgrade	Network upgrade.
	Development support	Provide software development kit (SDK) of the encoder, demonstration software and development description.



- For specific installation requirements of the Device, refer to engineering construction specifications and national standards.
- The cable quality and length affect the video quality. The video might blur, have noise or black edge. Sometimes the video quality might vary when the same video is output with different cables.

2 Unpacking and Cable Connection

2.1 Unpacking and Checking

When you receive the Device, check whether there is any visible damage. The protective materials used for the package of the Device can resist most of accidental collisions during transportation.

Keep the label at the bottom of the box well. You might need to present the serial number on the label when we provide after-sales service.

2.2 Device Structure

2.2.1 Front Panel

Figure 2-1 Front panel

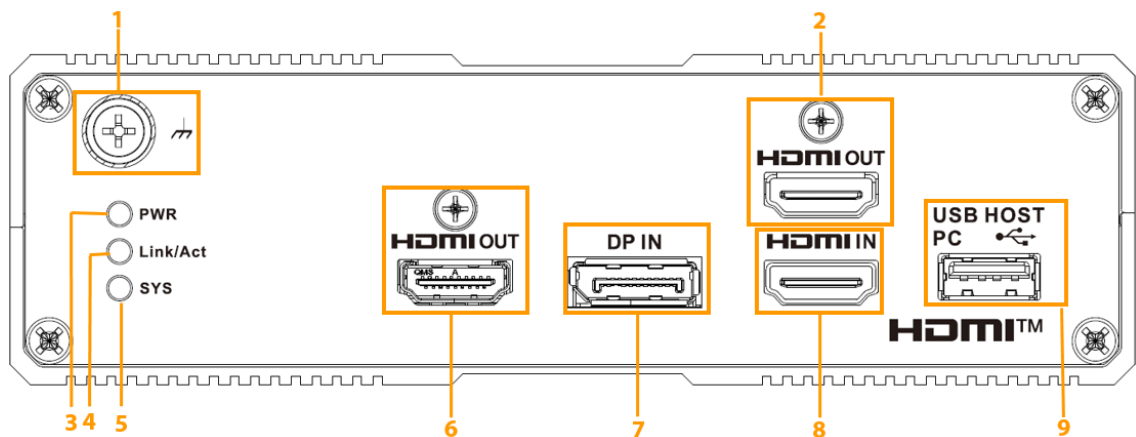


Table 2-1 Description for front panel

No.	Description	No.	Description	No.	Description
1	Ground screw.	2	HDMI video loop output. It is capable of loop outputting signals from HDMI IN.	3	Power indicator. The light is solid red when the power is on.
4	Reserved indicator.	5	Operation indicator. It is solid on when application program is operating.	6	HDMI signal output (debugging port).
7	DP signal input.	8	HDMI video input port.	9	Reserved port.

2.2.2 Rear Panel

Figure 2-2 Rear panel

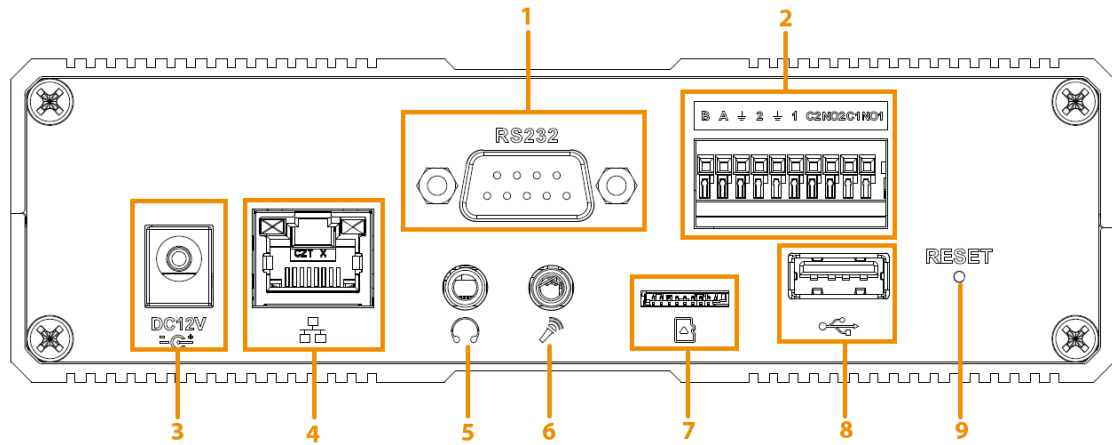


Table 2-2 Description for rear panel

No.	Description	No.	Description	No.	Description
1	RS-232 debugging serial port.	2	RS-485 port, alarm input and alarm output.	3	Power input port. Rated current: 2 A. Rated power: 24 W.
4	RJ-45 network port.	5	3.5 mm earphone port.	6	3.5 mm microphone port.
7	SD (TF) card slot (reserved).	8	USB2.0 ports (reserved).	9	Reset button. Press and hold it for 3 seconds to 5 seconds, and the system will restore to factory settings.

3 Web Operations



The webpages in this chapter are for reference only and might differ depending on the model of the device.

3.1 Network Connection

Procedure

- Step 1 Connect the Device and computer to the network.
- Step 2 Configure the device IP address, subnet mask, and gateway respectively.
- Step 3 Ping *****.***.***.***** (IP of the Device) to check if the network is available.
- Step 4 Open Internet Explorer, select **Tools > Internet Options > Security > Custom Level**. Select **Enable** or **Prompt** for all ActiveX controls and plug-ins.



We recommend IE8 or a later version.

3.2 Login

Procedure

- Step 1 Enter IP address of the Device in the address bar of the browser.
- Step 2 Read the **Software License** and **Privacy Policy** and then select **I have read and agree to the terms of the Software License Agreement and Privacy Policy**, and then click **Next**.
- Step 3 Initialize the device.
 - 1. Set a strong admin user password according to the password strength prompt.



The password must consist of 8–32 non-blank characters and contain at least two types of the following characteristics: Uppercase, lowercase, number, and special character (excluding ' " ; &). **Password** and **Confirm Password** must be the same.

Figure 3-1 Device initialization

Device Initialization

Username admin

Password

Low Middle High

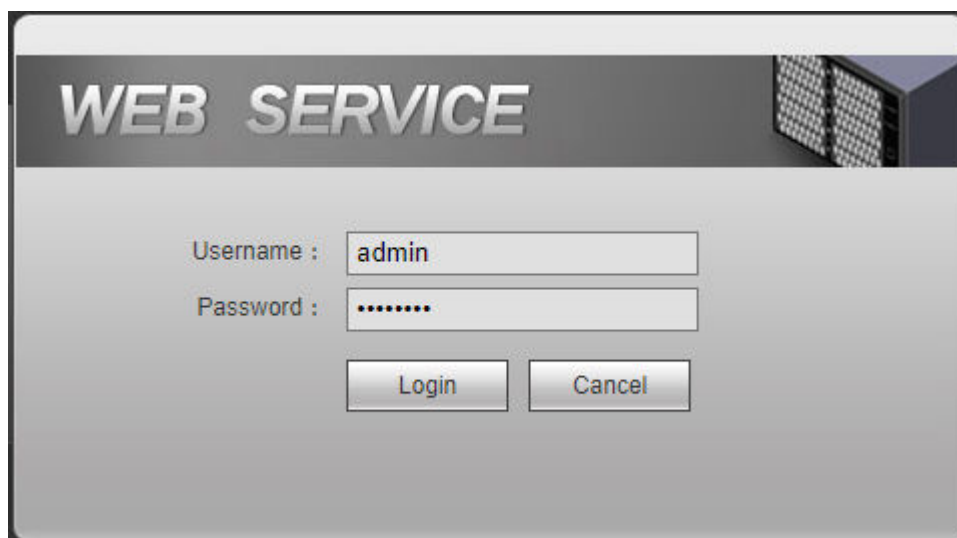
Confirm Password

OK

- 2. Click **OK**.

- Step 4 Enter username and password, and then click **Login**.

Figure 3-2 Login

The image shows a login window titled "WEB SERVICE". It has a header bar with the title and a small graphic of a server rack. Below the header, there are two input fields: "Username :" with the text "admin" and "Password :" with masked characters ".....". At the bottom, there are two buttons: "Login" and "Cancel".

WEB SERVICE

Username : admin

Password :

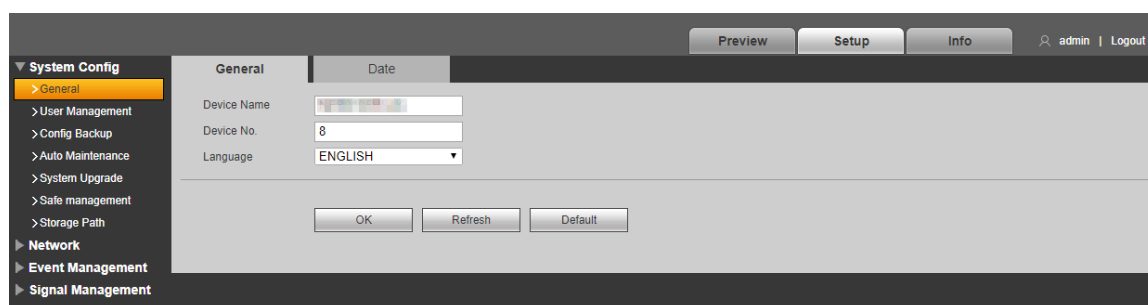
Login Cancel

Step 5 Install or load the plug-in as prompted by the system.



Click **Logout** to log out the system.

Figure 3-3 Operation page

The image shows the "Operation page" of the system. It has a dark header bar with tabs: "Preview", "Setup", and "Info". On the right of the header, it says "admin | Logout". On the left, there is a sidebar menu with "System Config" expanded, showing sub-items like "General", "User Management", "Config Backup", "Auto Maintenance", "System Upgrade", "Safe management", and "Storage Path". Below "System Config", there are "Network", "Event Management", and "Signal Management". The main content area is titled "General" and "Date". It contains fields for "Device Name", "Device No." (with the value "8"), and "Language" (with a dropdown menu showing "ENGLISH"). At the bottom of the main area, there are three buttons: "OK", "Refresh", and "Default".

Preview Setup Info admin | Logout

System Config

- > General
- > User Management
- > Config Backup
- > Auto Maintenance
- > System Upgrade
- > Safe management
- > Storage Path

Network

Event Management

Signal Management

General Date

Device Name

Device No. 8

Language ENGLISH

OK Refresh Default

3.3 Configuring Encode Parameters

You can configure encode parameters of local audio and video signals, including encode mode, stream type and resolution and so on.

Procedure

Step 1 Select **Setup** > **Signal Management** > **Local Signal** > **Encode Setup**.

Step 2 Configure the parameters.

Figure 3-4 Encode setup

The screenshot shows the 'Encode Setup' window with four tabs: 'Encode Setup', 'Input Title', 'OSD Custom', and 'Capture Custom'. The 'Encode Setup' tab is active, displaying two columns of settings for 'Main Stream' and 'Sub Stream'.

Main Stream Settings:

- Encode Mode: H.265
- Stream Type: Main Stream
- Audio Enable: ☐ Audio
- Resolution: 1080P
- Frame: 60
- Stream Control: Limit Stream
- Stream Value: 5120 ☒ Custom
- Recommended: (3584 - 5120Kbps)
- Audio Format: PCM
- Audio In: Monaural Mode
- Audio Input: HDMI
- Prompt When N... ☒

Sub Stream Settings:

- Encode Mode: H.265
- Stream Type: Sub Stream1
- Audio Enable: ☐ Audio
- Resolution: D1
- Frame: 30
- Stream Control: Limit Stream
- Stream Value: 2048 ☐ Custom
- Recommended: (512 - 3072Kbps)

At the bottom, there are 'Save' and 'Refresh' buttons.

Table 3-1 Parameter description

Parameter	Description
Encode Mode	You can select H.264 or H.265.
Stream Type	Select different encoding streams for recording events. ● Main stream: In a standard network bandwidth environment, the Device is capable of video recording and network monitoring. Within the resolution range supported by the Device, the resolution of the main stream can be set at will. ● Sub stream: When the network bandwidth is insufficient, it can be used to replace the main stream to carry out network monitoring and reduce network bandwidth utilization.
Audio Enable	Determine to encode audio or not during recording.
Resolution	Support adaptive resolution for main stream.
Frame	Self-adaptive or PAL: 1 fps – 25 fps, 1 fps – 50 fps or 1 fps – 60 fps.
Stream Control	The bit rate control type during video data transmission. You can select bit rate type from: ● CBR (Constant Bit Rate): The bit rate changes a little and keeps close to the defined bit rate value. ● VBR (Variable Bit Rate): The bit rate changes as monitoring scene changes.

Parameter	Description
Stream Value	Under VBR mode, this stream value is the upper limit of stream. Under limit stream mode, this value is a fixed value. Select Custom , and you can manually enter stream value.
Recommended	The Device recommends the optimal stream range according to the resolution and frame rate settings. • The recommended stream range for main stream is from 3584 Kbps to 5120 Kbps. • The recommended stream range for sub stream is from 512 Kbps to 3072 Kbps.
Audio Format	It supports G.711A, PCM and ACC formats. It is PCM by default.  Audio encoding mode here will affect audio stream.
Audio In	It supports monaural mode and stereo mode.
Audio Input	It supports HDMI, 3.5 mm, audio mixing and audio separation.
Prompt When No Signal is Acquired	It is enabled by default.

Step 3 Click **Save**.

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 logout function

The account logout 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 Allow list**

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

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).