

Video Matrix Platform (M60)

Quick Start Guide



Foreword

General

This manual introduces the installation, functions and operations of the video matrix platform (hereinafter referred to as "the Device"). Read carefully before using the device, and keep the manual safe for future reference.

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.

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.

Transportation Requirements



- Transport the device under allowed humidity and temperature conditions.
- Do not transport the device with its front panel facing down.

Storage Requirements



Store the device under allowed humidity and temperature conditions.

Installation Requirements



- This is a class A product. In a domestic environment this may cause radio interference in which case you may be required to take adequate measures.
- Use a cable tie to bundle the cables after they are connected to avoid risk of short circuits, overheating and electrocution caused by tangled cables.



- A 5 A overcurrent protection device is required to be installed in the external power circuit of the product as a circuit breaker. Make sure the protection device is close to the product, offering safety of cutting power during maintenance.
- Install the device near a power socket for emergency disconnect.
- A safety circuit breaker is designed on the device bottom to cut the power of the device. Make sure the breaker can be easily operated during installation.
- Make sure the product is installed by trained professionals and it must be installed in locations that only professionals can access.
- To ensure heat dissipation, the gap between the device and the surrounding area should not be less than 5 cm on the sides and 1 cm on top of the device.
- Do not block the ventilator of the device with objects, such as newspaper, table cloth or curtains.
- Do not put open flames, such as a lit candle, on the device.
- Prevent liquid from dripping or splashing on the device. Do not put any objects filled with liquid, such as a vase, on top of the device.

- Do not place or install the device in a place exposed to sunlight or near heat sources.
- Keep the device away from dampness, dust, or soot.
- Make sure the device is installed stably and levelly, allowing normal status for internal tremor resistant modules.
- 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 independent protective grounding terminal is designed at the lower-right corner of the product. Make sure the terminal is reliably grounded during installation.
- Connect the cables in sequence when linking the circuit, and connect the power cable last to avoid damaging the device.
- Make sure the negative binding post of the battery is disassembled while the device is being wired.
- 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.

Operation Requirements



- Do not ingest battery to avoid chemical burn hazard.
- The remote control supplied with this product contains a coin/button cell battery. If the coin/button cell battery is swallowed, it can cause severe internal burns in just 2 hours and can lead to death.
- If you think batteries might have been swallowed or placed inside any part of the body, seek immediate medical attention.
- Keep new and used batteries away from children.
- If the battery compartment does not close securely, stop using the product and keep it away from children.
- Please do not place the product in moist place to avoid shock hazard.



- Use the device under the allowed humidity and temperature conditions.
- Use the device within the rated range of power input and output.
- Operating temperature: $-10\text{ }^{\circ}\text{C}$ to $+50\text{ }^{\circ}\text{C}$ ($14\text{ }^{\circ}\text{F}$ to $122\text{ }^{\circ}\text{F}$).
- Do not disassemble the device.
- Do not plug or unplug RS-232, RS-485 or the audio/video signal cable with the power on to avoid damaging the ports.
-  IEC 60417-6042 (2010-11) and  IEC 60417-6172 (2012-09).
- Optional.

Maintenance Requirements



- A blown fuse does not ensure disconnection of subsequent circuit. Please be cautious during maintenance.
- Power off the device before maintenance.
- The device can only be used with batteries possessing internal protection. To prevent explosion, dispose of the old batteries as instructed.
- Make sure to use the same model when replacing the battery to avoid fire or explosion.



- The device casing provides protection for internal components. Use a screwdriver to loosen the screws before detaching the casing. Make sure the casing is put back and fixed to the original spot before power on and use the device again.
- Damp dust on the circuit board might cause the device to short circuit, resulting in device damage. Make sure to regularly clear dust from the circuit board, connectors and the case with a brush.

Table of Contents

Foreword	I
Important Safeguards and Warnings	III
1 Overview	1
1.1 Introduction.....	1
1.2 Introduction to Compression Cards	1
1.3 Host System	3
1.3.1 12U Host System Case	3
1.3.2 7U Host System Case.....	4
1.3.3 Main Control Card	5
2 Installation	7
2.1 Unpacking and Checking	7
2.2 Device Installation.....	7
2.2.1 Installation Requirements	7
2.2.2 Installation Procedures.....	8
2.2.3 Powering On and Off.....	11
3 Local Configurations.....	13
3.1 Basic Operations	13
3.2 Menu Operations.....	14
3.2.1 System Settings.....	14
3.2.2 System Information	18
3.2.3 Shutting down the Device	20
4 Web Operations	22
4.1 Network Connection	22
4.2 Login.....	22
Appendix 1 Mouse Operation.....	24
Appendix 2 Cybersecurity Recommendations	25

1 Overview

1.1 Introduction

Based on Advanced Telecommunications Computing Architecture (ATCA), the Device is a modern telecommunication-level device which combines DVR, decoder, analog matrix, and video wall controller. It is suitable for different types of network monitoring environments.

1.2 Introduction to Compression Cards

Table 1-1 System cards

Name	Model	Functional Module	Description	Note
Platform Host	M60-12U	Video matrix platform host	- One 12U host that supports 10 function cards. - One MBC0050 main control card. - Two built-in power adapters (redundant).	Standard
	M60-7U		- One 7U host that supports 5 function cards. - One MBC0050 main control card. - Two built-in power adapters (power redundancy).	
Input Module	VEC3204FB	SD BNC video encoding card	32-channel video input (BNC). - Two DVI audio input ports (32 channels). 2-channel RS-485 port.	Optional
	VEC1604HS	HD-SDI video encoding card (16 channels)	16-channel HD-SDI video input (BNC). - One DVI audio input port (16 channels). 2-channel RS-485 port.	Optional
	VEC0804HD	HD DVI video encoding card	8-channel DVI video input. - One VGA audio input port (eight channels). 2-channel RS-485 port.	Optional (support DVI,VGA, HDMI)

Name	Model	Functional Module	Description	Note
	VEC1604HF	16-channel HD optical fiber video encoding card	16-channel SFP video input (optical fiber). - One DVI audio input port (16 channels). 2-channel RS-485 port.	Optional
	VEC1604HC	16-channel HDCVI encoding card	16-channel BNC video input (HDCVI). - One DVI audio input (16 channels). 2-channel RS-485 port.	Optional
	VEC0804US	HD 3G-SDI encoding card (eight channels)	8-channel 3G-SDI video input (BNC). - One DVI audio input port (eight channels). 2-channel RS-485 port.	Optional
	VEC1605UH	16-channel UHD encoding card	16-channel HDMI video input. 4-channel VGA video input. - Two VGA audio input ports (16 channels). 1-channel RS-485 port.	Optional
	VEC0805UH	8-channel UHD encoding card	8-channel HDMI video input. 2-channel VGA video input. - One VGA audio input port (eight channels). 1-channel RS-485 port.	Optional
Output Module	VDC0905H	9-channel HDMI decoding card	9 HDMI video output ports.	Optional
	VDC1205H	12-channel HDMI decoding card	12 HDMI video output ports.	Optional
	VDC1505H	15-channel HDMI decoding card	15 HDMI video output ports.	Optional
	VDC1805H	18-channel HDMI decoding card	18 HDMI video output ports.	Optional
Platform Card	DSS	Platform Card	- Four RJ-45 ports that support 10/100/1000 Mbps network data. Two optical ports (10 gigabit). - Four USB ports. - One standard RS-232 port. - One VGA port and one HDMI port. - One audio talk port.	Optional

1.3 Host System

1.3.1 12U Host System Case

The 19-inch 12U host system case includes function card slots, power ports and intelligent temperature-controlling fans. The indicators on the front panel indicate the working status of the Device.

- A dust filter is designed behind the air intake plastic shell.
- Three groups of intelligent temperature-controlling fans that support the hot swapping function.
- Ten function card slots are labeled in sequence and used to install function cards.
- The main control card slots are marked with "M".
- Dual power module supports 220 VAC and 48 VAC power supply.

Figure 1-1 Appearance of 12U host system case



Figure 1-2 12U case indicators

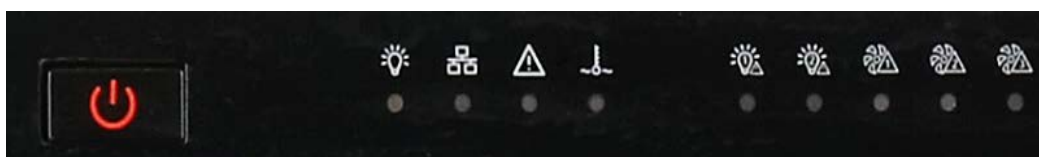


Table 1-2 12U case indicators description

Indicator	Function
	Power button.
	Running status indicator. • Red: The Device is not running after it has been powered on. • Red-blue: The device is running.
	Network indicator. • Red: The Device network is abnormal. • Off: The Device network is normal.

Indicator	Function
	Alarm indicator. - Red: Error occurred on the Device. - Off: The Device is normal.
	Temperature indicator. - Red: The compression card temperature is too high. - Off: The compression card temperature is normal.
	Power module indicator. - Red: The corresponding power module is abnormal. - Off: The corresponding power module is normal.
	Fan indicator. - Red: The corresponding fan is abnormal. - Off: The corresponding fan is normal.

1.3.2 7U Host System Case

The 19-inch 7U host system case includes function card slots, power ports and intelligent temperature-controlling fans. The indicators on the front panel indicate the working status of the Device.

- Single fan box with a dust filter, and the air intake is at the side of the Device.
- Three groups of intelligent temperature-controlling fans that support the hot swapping function.
- Five function card slots are labeled in sequence and used to install function cards.
- The main control card slots are marked with "M".
- Dual power module supports 220 VAC power supply.

Figure 1-3 Appearance of 7U host system case



Figure 1-4 7U case indicators



Table 1-3 7U case indicators

Indicator	Function
	Power supply indicator. It is green when the device is powered on normally.

Indicator	Function
	Running status indicator. - Red: The Device is not running after it has been powered on. - Red-blue: The Device is running.
	Network indicator. - Red: The Device network is abnormal. - Off: The Device network is normal.
	Alarm indicator. - Red: Error occurred on the Device. - Off: The Device is normal.
	Temperature indicator. - Red: The compression card temperature is too high. - Off: The compression card temperature is normal.
	Power module indicator. - Red: The corresponding power module is abnormal. - Off: The corresponding power module is normal.
	Fan indicator. - Red: The fan is abnormal. - Off: The fan is normal.
	Infrared remote control signal receiving port.

1.3.3 Main Control Card

Figure 1-5 Function panel of main control card

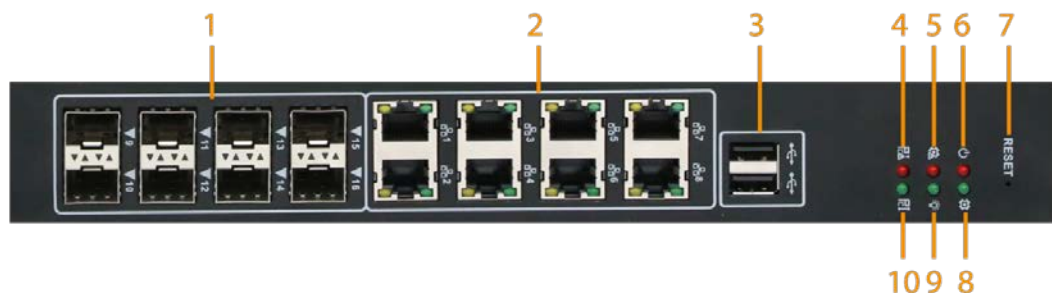


Figure 1-6 Port panel of main control card



Table 1-4 Introduction to ports of main control panel

No.	Port	Function
1	Gigabit SFP Port	Connects to the optica fiber.

No.	Port	Function
2	RJ45 Port	Transmits audio and video data and network signals.
3	USB Port	Connects to the mouse, keyboard, and USB drive.
4	PCIE Error Indicator	It is on when the PCIE (Peripheral Component Interconnect Express) link is abnormal.
5	CPU Working Status Indicator	Diaplays the working status of the CPU.
6	Power Indicator	Displays the power status of the Device.
7	Reset Button	Press the button to reset the Device to its factory settings.
8	CPU Power Indicator	Displays the power status of the CPU.
9	Run Indicator	Visualizes and monitors the running status of the system.
10	PCIE Link Indicator	It is on when the PCIE link is normal.
11	VGA	Local display output port used to connect the LCD screen.
12	RS-232 Serial Port	Connects other devices to the Device with RS-232 serial ports.
13	USB Port	Connects the mouse, keyboard, and USB drive.
14	Audio Input	Audio communication.
15	Audio Output	

2 Installation

2.1 Unpacking and Checking

When you receive the Device, check it according to the following steps.

Step 1 Check whether there is obvious damage on the Device appearance.

The packing materials are specially selected to protect the Device from becoming damaged during transportation.

Step 2 Check whether the accessories are complete against the packing list.

After confirming that all parts are included, you need to remove the protective film on the Device.

Step 3 Open the Device case to check the data cable and the power cord on the front panel, and check whether the connection between the main control card and the port pannel is tight.

Check whether the main control card, control card and function card are securely inserted.



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

2.2 Device Installation

2.2.1 Installation Requirements

The Device is usually used in the central machine rooms of monitoring systems. Its installation location must meet the national and local machine room construction standards.

The Device is a standard rack-mounted device that is attached to a cabinet. During the installation, make sure that:

- The cabinet is sturdy and able to support the weight of the Device and its accessories. During installation, avoid the danger of an uneven mechanical load.
- There is a sufficient amount of space available to install the audio and video cables. The bending radius of the cables must not be less than 5 times the outer diameter of the cables.
- The Device is well ventilated to ensure it can function safely. We recommend installing it higher than 50 cm above the ground.
- Temperature in the cabinet is between 0 °C and +50 °C.
- The humidity in the room is between 10% (RH) and 90% (RH).

Power Supply Requirements

The rated current of the device is 10 A / 5 A, and its rated power is up to 800 W. The rated voltage for The 12U product is 100–127 VAC/200–240 VAC, and for the 7U product is 100–240 VAC.

Anti-interference Requirements

- Make sure to put through all necessary anti-interference measures for the on-site power supply system.
- Do not share the working place with the ground device or lightning protection device of electrical devices, and keep them away as far as possible.
- Ground devices and lightning protection devices of electrical devices cannot be installed next to the Device. Make sure to keep them far away from the Device.
- If necessary, adopt electromagnetic shielding methods to resist interference.

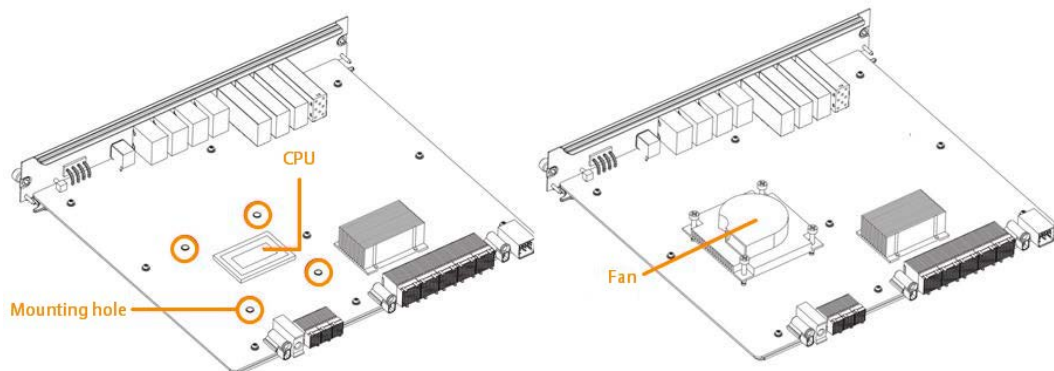
2.2.2 Installation Procedures

Step 1 Align the four mounting rings of the fan with the mounting holes of the main control card, and then attach the fan to the CPU of the main control card with screws.



- The fan and the main control card are separate, but their wires are connected, because the fan is very heavy and can damage the CPU during transportation if transported together. Please handle with care.
- Make the air outlet of CPU fan upward after main control card is inserted into the case.

Figure 2-1 Install the fan

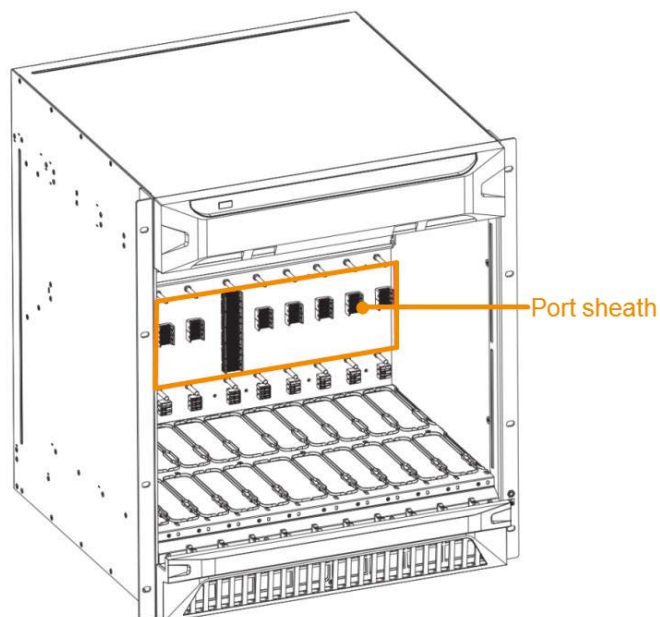


Step 2 Remove the port sheath from the rear panel of the chassis.



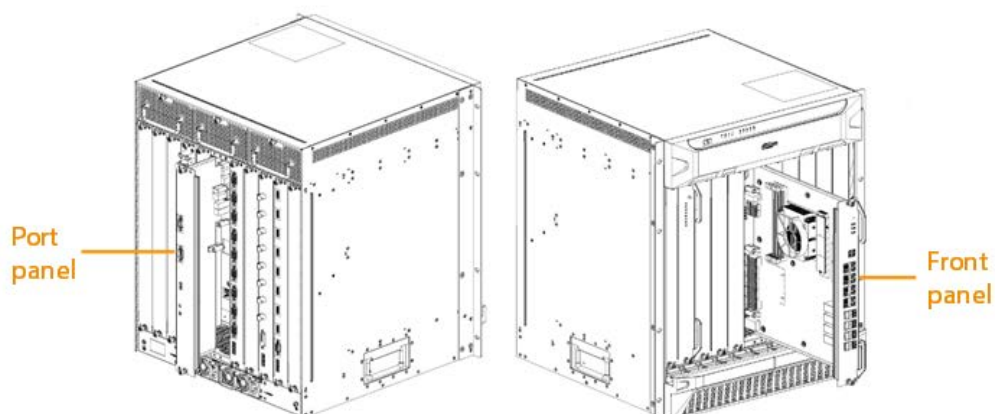
Before you insert the compression card, remove the black port sheath first.

Figure 2-2 Remove sheath



Step 3 Insert the port panel and the front panel of the main control card into the "M" slot of the chassis, and then tighten the screws.

Figure 2-3 Install board card

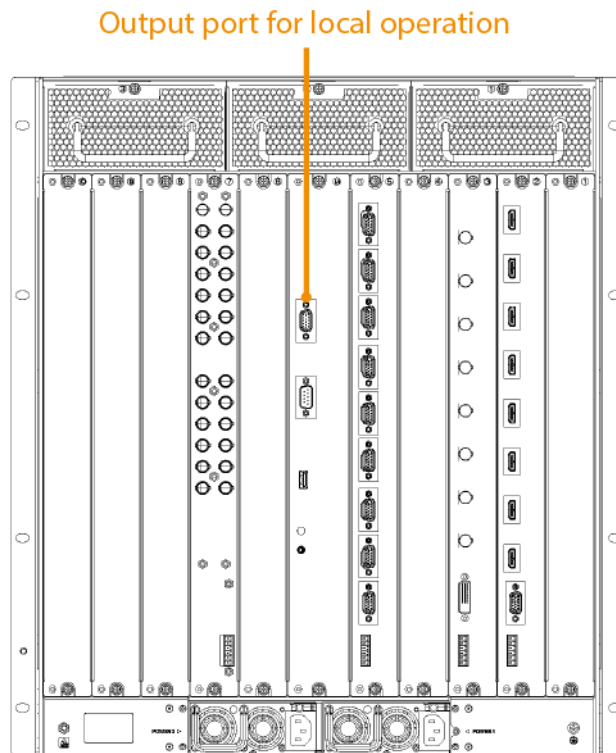


- Insert the port panel, tighten the set screws, and then insert the front panel.
- When inserting the main control card and control panel, pull the extraction tool, and then insert the panel in place by pushing the extraction tool inward.

Step 4 Insert the port panel and front panel of the function card, and then tighten the screws. The installation is the same as that of the main control card.

Step 5 Connect a local monitor to the VGA port on the port panel of the main control card.

Figure 2-4 Connect the local monitor

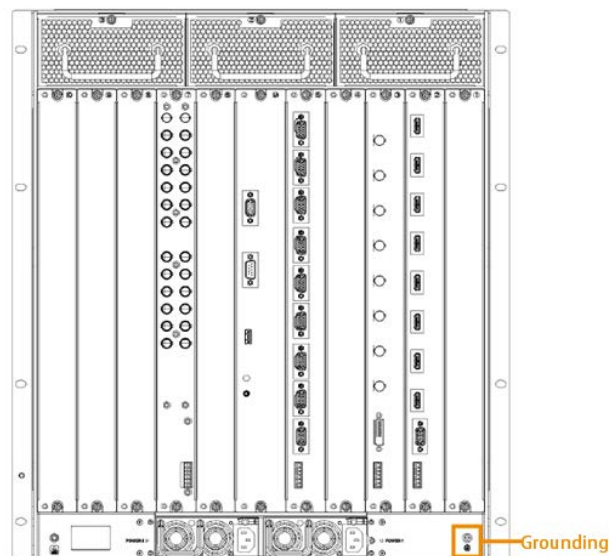


Step 6 Ground the Device properly.



For personal safety and the safety of the Device, the Device and other devices connected to the Device with cables, such as screens and computers, must be grounded.

Figure 2-5 Grounding

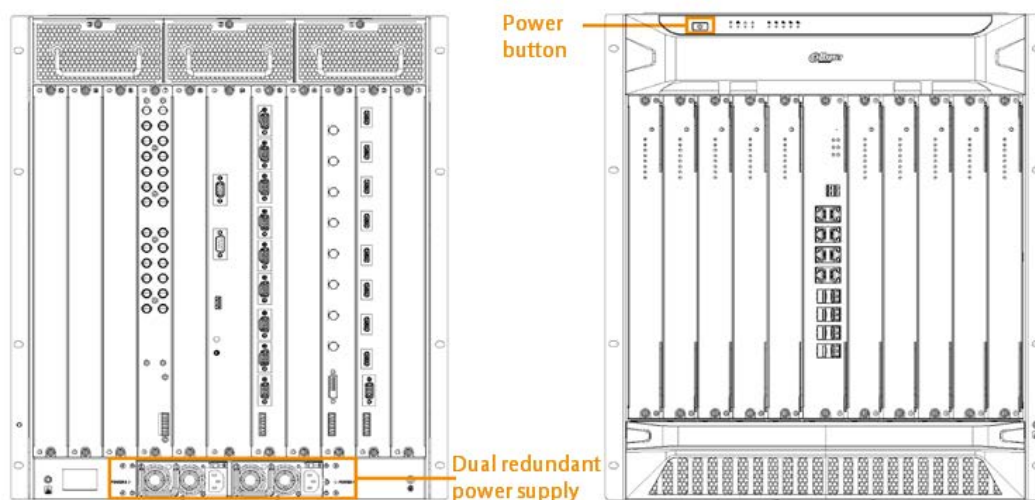


For devices with power supplies that are correctly grounded, their grounding terminals do not have to be grounded.

Step 7 Connect the network cable, VGA cable and other cables.

Step 8 Plug in the Device power cord and press the power button to power on the Device.

Figure 2-6 Power on



2.2.3 Powering On and Off

2.2.3.1 Powering On

Power on the Device, and then press the power button on the front panel, and the power indicator will light up. The whole process takes about 90 seconds depending on the number of cards.

When powering on the Device:

- Make sure that the supplied voltage is within 100-240 VAC, and 47 Hz-63 Hz. Before you press the power button, make sure that the power cord is properly connected.
- We recommend that you use a power supply with stable voltage and little interference (refer to the international standard) ensure that the device functions stably, and to extend its service life. This will also help external connected devices, such as cameras, to perform well. We highly recommend installing a UPS if possible.

2.2.3.2 Powering Off

There are two ways to power off the Device.

- Method 1: On the **Main Menu** page, click **Shut down System**, and select **Shut down Device**.
- Method 2: Press and hold the power button on the panel for 5s.



- We recommend that you use method 1 to protect the Device from damages caused by unexpected outages.
- Stop all operations of the Device before you unplug the Device.

2.2.3.2.1 Outage Recovery

In case of a sudden power outage or force shutdown while the Device is running, the Device will automatically save and restore to its previous working status after it is powered on again.

2.2.3.2.2 Replace Button Battery



Export and save your configurations before replacing the battery to avoid losing your configurations.

We recommend that you use the same type of button battery. The button battery should be replaced once a year to ensure that the system performs well and remains accurate.

3 Local Configurations

To perform local configurations, you must connect the Device to a monitor and other control devices, such as the mouse and keyboard.

3.1 Basic Operations

Step 1 Power on the Device and press the power button.

Step 2 On the software license agreement page, select **I have read and agree to all terms**, and then click **Next**.

Step 3 Enter and confirm the new password.



- The password must consist of 8–32 non-blank characters and contain at least two types of the following characters: uppercase, lowercase, numbers, and special characters (excluding ' " ; &).
- Set a high security password according to the password strength prompt.

Figure 3-1 Device initialization

Device Initialization

User admin

Password

(Min 8-digit containing letter(s) and number(s))

Confirm Password

OK

Step 4 Click **OK**.

Step 5 Right-click the page. Enter the username and password.



The account will be locked after five failed login attempts in 30 minutes.

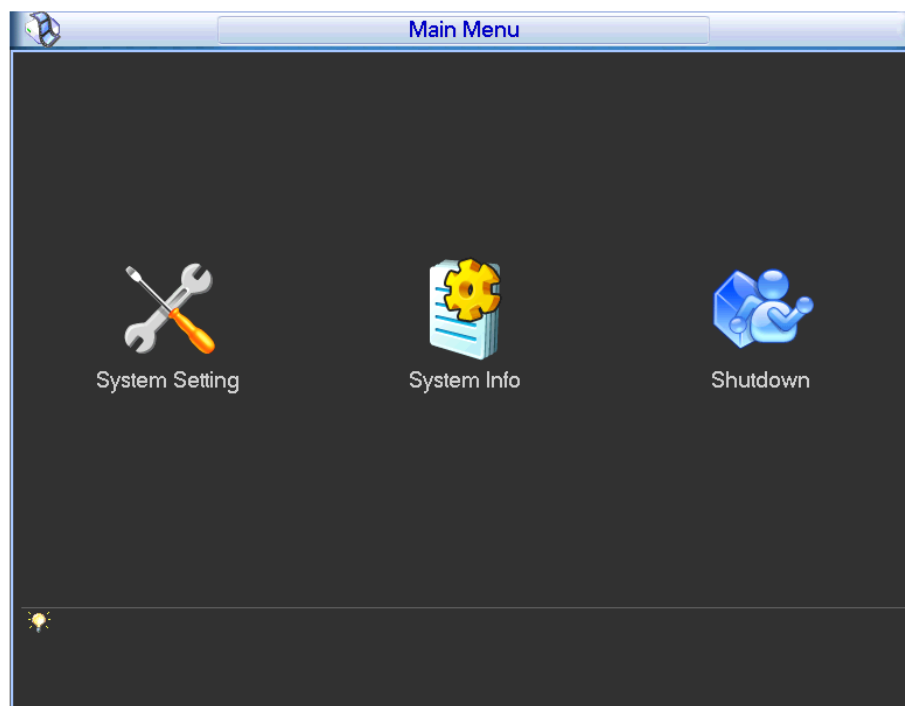
Figure 3-2 System login



Step 6 Click **OK** to log in to the system

Step 7 Right-click the home page, and then select **MAIN MENU**.

Figure 3-3 Main menu



3.2 Menu Operations

- The sub-menu settings will only take effect after you save them.
- The checkbox is selected when it is filled with ■ or has a check mark. This note applies to the whole document.

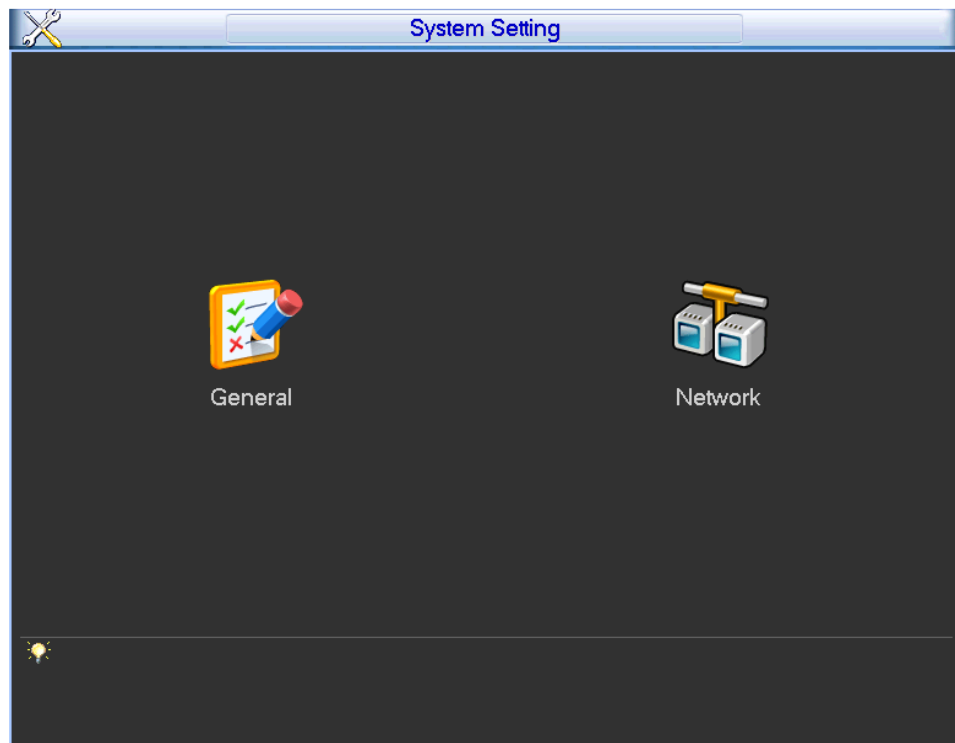
3.2.1 System Settings

You can configure the system settings, including general and network settings.



System settings can only be configured by authorized users.

Figure 3-4 System setting



3.2.1.2 General

You can configure basic information for the Device.

Step 1 On the main menu, select **System Setting** > **General**.

Figure 3-5 General

The screenshot shows a 'General' settings window. The 'System Time' is set to 2022 - 01 - 08 06 : 52 : 26. The 'Date Format' is YYYY MM DD and the 'Date Separator' is -. The 'Time Format' is 24-HOUR and the 'Language' is ENGLISH. The 'Video Standard' is PAL and the 'Device No.' is 8. The 'Device Name' is M60-12U-E. The 'Auto Logout' is set to 10 min. There are 'Save', 'Default', 'OK', and 'Cancel' buttons.

Step 2 Configure parameters.

Table 3-1 General parameters description

Parameter	Description
System Time	Modify the current system date and time, and then click Save.  System time can only be changed when it is not recording time or when the recording has stopped, otherwise you cannot search for the recorded video.
Date Format	Select date display format from YYYY MM DD, MM DD YYYY and DD MM YYYY.
Date Separator	Separator of date format.
Time Format	Select 24-hour or 12-hour.
Language	Change the language of the menu from Simplified Chinese to English, or vice versa.
Video Standard	Select the video standard. It is PAL by default.
Device No.	Customize the Device number and Device name to make it easy to identify it.
Device Name	
Auto Logout	Menu standby time can be set from 0 minutes to 60 minutes. - There is no standby time when it is set to 0 minutes. Also, the system will not log out automatically. - If the standby time is set, the system will log out the current user if there is no operation within the selected time. You need to log in again to use the menu.

Step 3 Click **OK**.

3.2.1.3 Network

Configure the Device network parameters, so that the Device can communicate with other devices on the same network.

Step 1 On the main menu, select **System Setting > Network**.

Figure 3-6 Network

Net Mode: Fault Toleranc, MAC ADDRESS icon

Network Device Name: Bond1

IP Version: IPv4

IP Address, Subnet Mask, Gateway: [input fields]

DHCP: ☐

TCP Port: 37777, HTTP Port: 80

UDP Port: 37778, RTSP Port: 554

Max Connection: 128

Buttons: Default, Save, Cancel

Step 2 Configure parameters.

Table 3-2 Network parameters description

Parameter	Description
Net Mode	The default setting is Fault Tolerance .
MAC Address	Click the icon to display the MAC address.
Network Device Name	It is Bond1 by default.
IP Version	It is IPv4 by default.
IP Address	Enter numbers to change the IP address, and then configure its subnet mask and gateway.  The IP address and gateway must be on the same network segment.
Subnet Mask	
Gateway	

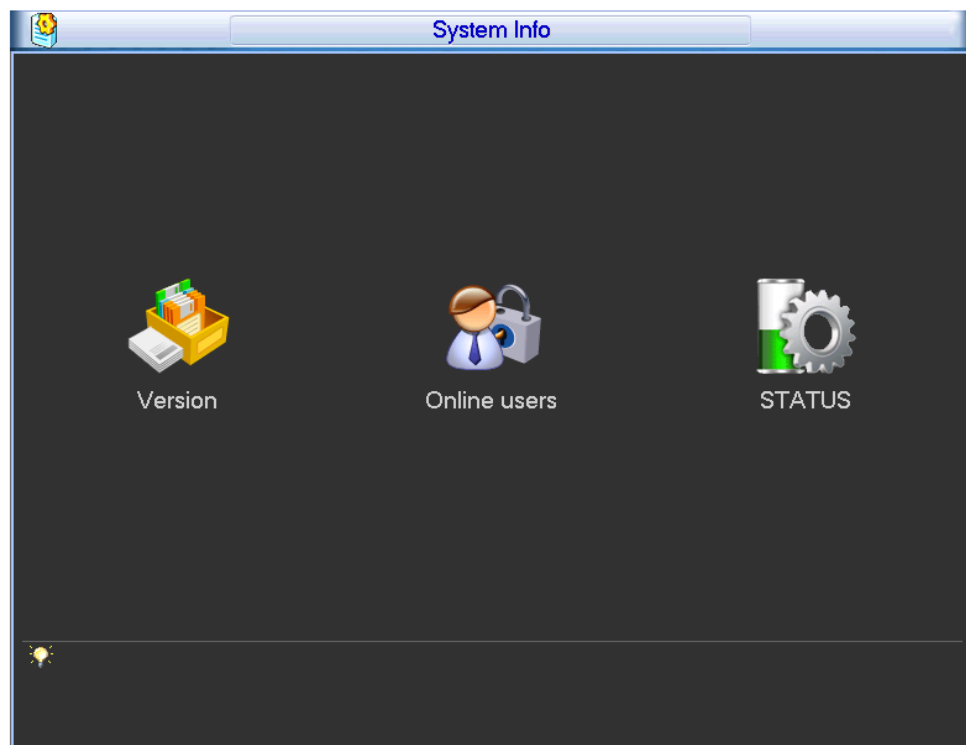
Parameter	Description
DHCP	Select the DHCP checkbox to allow the system to automatically get the IP address for you. When the DHCP function is enabled, the IP address, gateway, and subnet mask cannot be set manually. • If DHCP is enabled, the information that it gets will be displayed in the IP address box, subnet mask box and gateway box. If DHCP is not enabled, all the field boxes will contain a 0. • When DHCP is disabled, the static IP information will restore to default settings. You need to configure IP again.
TCP Port	Keep the default settings. No need to change them.
HTTP Port	
UDP Port	
RTSP Port	
Max Connection	The number of connections ranges from 0 to 128. If it is 0, network users are not allowed to connect. The maximum number of connections is 128.

Step 3 Click **Save**.

3.2.2 System Information

You can view version information, online users and system status.

Figure 3-7 System information



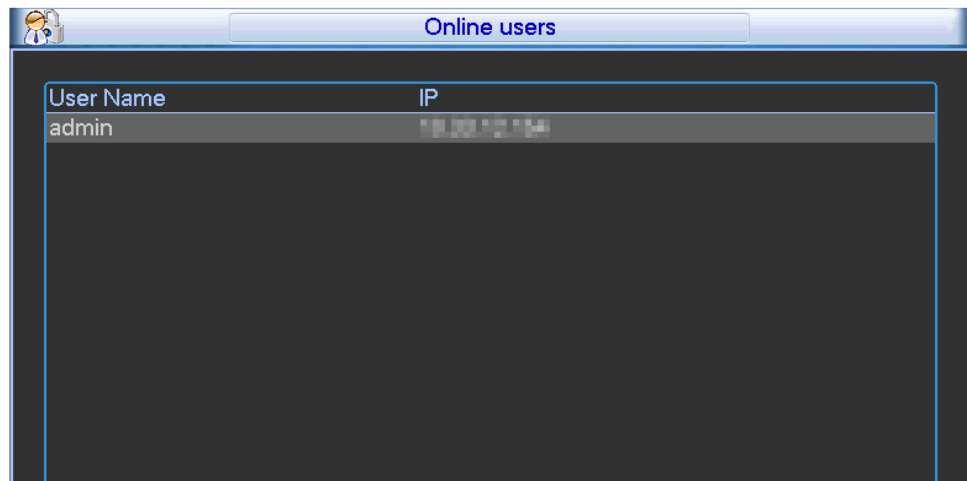
3.2.2.2 Version

You can view the version details on the version, such as system version, build date, web version and serial number.

3.2.2.3 Online Users

On the main menu, select **System Info > Online users**, and then you will be able to view the online users that remotely visit the Device.

Figure 3-8 Online users



User Name	IP
admin	192.168.1.104

3.2.2.4 Status

On the main menu, select **System Info > Status**, you will be able to view the fan speed, card information, temperature and source information, device time, net percentage, CPU percentage and memory percentage.

Figure 3-9 Status



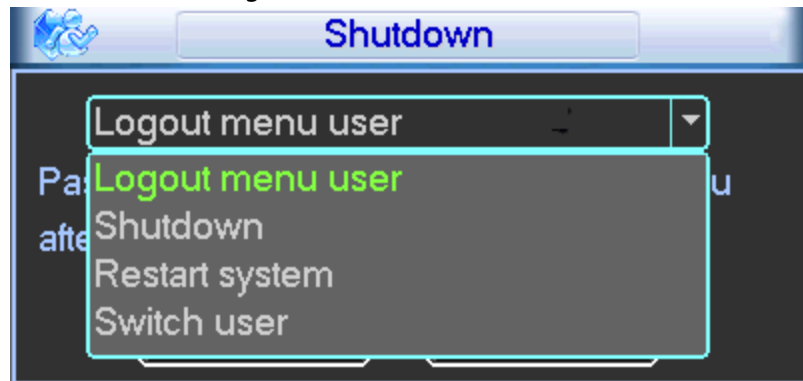
Table 3-3 System status description

Parameter	Description
Fan Speed	Displays the speed of the fans.
Card Information	Displays information on cards in the slots, and the present operating status.
Temperature Information	Displays the present temperature and status of cards.
Source Information	Displays the status of two powers.
Time	Displays the system time of the Device.
Net Percentage	Displays the receiving and transmitting rate of each network port.
CPU Percentage	Displays CPU usage.
Memory Percentage	Displays the disk space usage.

3.2.3 Shutting down the Device

On the main menu, select **Shutdown**, and you can log out of menu user, switch users, shutdown the system or restart the system.

Figure 3-10 Shutdown



- Logout menu user: Exits the menu. You need to enter the password again if you want to log back in.
- Shutdown: Exits the system, and powers off the Device.
- Restart system: Exits the system, and restarts the system.
- Switch user: Logs out of the current user, and switches to another user.

4 Web Operations

4.1 Network Connection

Step 1 Connect the Device to a computer through network.

Step 2 Configure the IP address, subnet mask and gateway of the Device and the computer respectively.



- If there is no router on the network, distribute IP address on the same network segment.
- If there is a router on the network, configure the corresponding gateway and subnet mask.

Step 3 Ping *.*.*.*.* (IP address of the Device) to check whether connection is available.

Step 4 Open the Internet Explorer, in **Tools > Internet Option > Security > Custom Level**, and select **Enable** or **Prompt** for all ActiveX controls and plug-ins.



We recommend IE8 or a later version.

4.2 Login

Step 1 Enter IP address of the Device in the address bar of the browser.

Step 2 Enter and confirm the new admin password.



- The password must consist of 8–32 non-blank characters and contain at least two types of the following characters: Uppercase, lowercase, numbers, and special characters (excluding ' " ; &).
- Set a high security password according to the prompt of password strength.

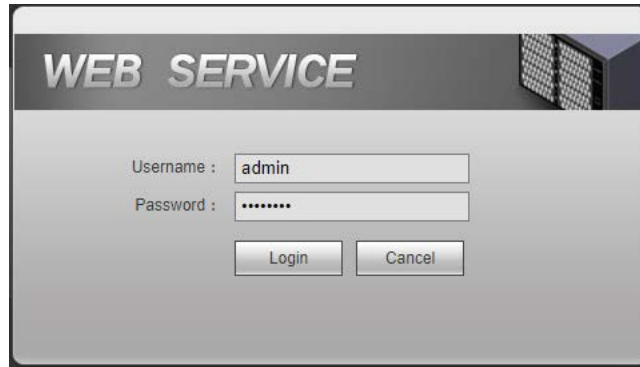
Figure 4-1 Device initialization

The screenshot shows a 'Device Initialization' window. It has a title bar with the text 'Device Initialization'. Inside, there are three labels: 'Username', 'Password', and 'Confirm Password'. The 'Username' field contains the text 'admin'. The 'Password' and 'Confirm Password' fields are empty text boxes. To the right of the 'Password' field, there are three buttons labeled 'Low', 'Middle', and 'High'. At the bottom right of the window is an 'OK' button.

Step 3 Click **OK**.

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

Figure 4-2 Login



The image shows a web service login interface. At the top, it says "WEB SERVICE" in a stylized font. Below this, there are two input fields: "Username :" with the text "admin" entered, and "Password :" with a masked password "*****". Below the password field are two buttons: "Login" and "Cancel".

Step 5 View the points for attention and highlights.



- Please conform to the points for attention.
- Click  to close the window.
- Select the **Do not show again** checkbox, and this window will not be displayed when you log in for the next time.

Figure 4-3 Operation interface



Step 6 Install or load plug-in as prompted by the system.



For details on web operations, see the user's manual.

Appendix 1 Mouse Operation

Plug a mouse with the Device through the USB port to operate the menu functions.

Appendix Table 1-1 Mouse operation description

Operation	Description
Click	The system prompts password input dialogue box if you have not logged in. During live surveillance, click to enter the main menu or open the navigation bar.
	Click the functional menu icon to enter the menu.
	Implement the control operation.
	Modify status of the checkbox or motion detection block.
	Click to prompt a pull-down list.
	 means backspace and  means space key. Click Shift to switch the input method. • In English input mode: Space key means to input a space. Backspace key means to clear one character. • In numerical input mode: Space key means to clear all of the number. Backspace key means to clear the last number. • In special symbol input mode: Space key means to input a space. Backspace key means to clear one symbol.
Double-click	Implement special control operation.
	In multi-image mode, double-click one channel image to make it full screen. Double-click it again to restore multi-image mode.
Click the right mouse button	In real-time monitoring mode, click the right mouse button to prompt the shortcut menu. The manual differs depending on the device version.
	Leave the current menu without saving the modification.
Scroll the wheel button	In numerical input box: Increase or decrease the numerical value.
	Switch items in the list.
	Page up or page down.
Move mouse	Select and move one item.
Drag mouse	Select a motion detection area with a frame.
	Select cover-area.

Appendix 2 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.