GO34A Series LED Monitor

User's Manual

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V1.0.0

Foreword

General

This manual introduces the installation, functions and operations of the GO34A device (hereinafter referred to as the "Device"). Read carefully before using the device, and keep the manual safe for future reference.

Models

DHI-LM27-GO34A

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 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

Version	Revision Content	Release Time
V1.0.0	First release.	December 2024

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.

Interface Declaration

This manual mainly introduces the relevant functions of the device. The interfaces used in its manufacture, the procedures for returning the device to the factory for inspection and for locating its faults are not described in this manual. Please contact technical support if you need information on these interfaces.

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, and comply with the guidelines when using it.

Transportation Requirements

Transport the device under allowed humidity and temperature conditions.

Storage Requirements

- Do not place the device in a place exposed to sunlight or near heat sources.
- Store the device under allowed humidity (5%–95% (RH)) and temperature (–20 °C to +60 °C, or –4 °F to +140 °F) conditions.

Installation Requirements

DANGER

Stability Hazard

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

Preventive measures (including but not limited to):

- Only use cabinets and brackets specified for the device.
- Only use furniture and structures that can safely support the device.
- Do not place the device on the edge of the furniture or structure that is supporting it.
- Always educate children about the dangers of climbing furniture to reach the device and its controller.
- Carefully arrange the cables connected to the device to avoid people tripping over them and pulling on them.
- Make sure that the device is installed on a stable surface.
- Do not put the device on tall furniture, such as cabinets and bookcases, without first ensuring that the supporting structure is stable enough to bare the device.
- Do not place the device on fabric and other similar material.
- Do not place items, such as toys and remote controls, that may entice children to climb on top of the device or furniture on which the device is placed.

WARNING

- 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 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 safety risks and damage to the device.
- 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.

- 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.
- Use an adapter or cabinet power supply provided by the manufacturer.
- 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.
- When installing the device, make sure that the power plug can be easily reached to cut off the power.
- Install the Device on a stable surface to prevent it from falling.
- Install the device in a well-ventilated place, and do not block its ventilation.
- The signal output devices and the LCD Display must be on the same grounding, and the earth impedance must be less than 1 Ω.

Operation Requirements

WARNING

- Use the standard power adapter. We will assume no responsibility for any problems caused by the use of a nonstandard power adapter.
- Use the power cords that are recommended for the region and conform to the rated power specifications.
- In a domestic environment this may cause radio interference in which case you may be required to take adequate measures.
- Ground the device to protective ground before you power it on.

- 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.
- Operate the device within the rated range of power input and output(⎓ Direct Current).
- Do not disassemble the device without professional instruction.
- Use the device under allowed humidity and temperature conditions.
- Check whether the power supply is correct before use.
- Operating temperature: 0 ℃ to 40 ℃ (32 °F to 104 °F).

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. Do not use the liquid cleaner or spray cleaner when cleaning the device.
- Use the clean and soft cloth or use the special lens wiping cloth when cleaning the surface of display screen. Do not use the wet cloth to clean the display screen. Otherwise, it may do harm to the screen.
- The appliance coupler is a disconnection device. Keep it at a convenient angle when using it.

Table of Contents

Product Information

1. Packing List

Figure 1-1 Packing List

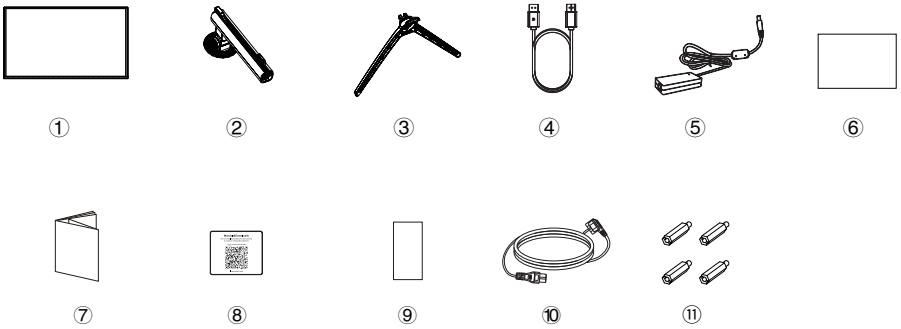


Table 1-1 Packing List

No.	Meaning
①	Display screen
②	Stand
③	Base
④	DP signal cable
⑤	Adapter
⑥	QSG
⑦	Legal and regulatory information
⑧	User's manual QR code stickers
⑨	Energy Efficiency Label
⑩	Power cord
⑪	Mount hexagon irons x 4

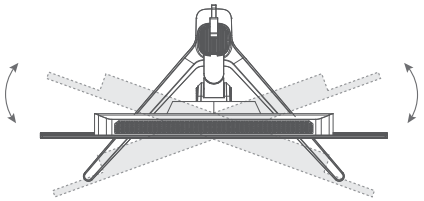
NOTE

The above appendix products are for reference only, the supporting products of different models of monitors may be slightly different from those in the figure, and everything is subject to reality.

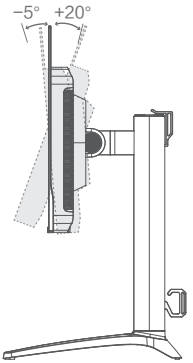
2. Monitor Adjustments

The adjustment functions of the display include tilt angle adjustment, screen vertical rotation angle adjustment, left and right rotation angle adjustment, and height adjustment, as shown in the figure below. Different types of displays have different adjustment functions, and the specific adjustment functions are subject to the actual model adjustment functions.

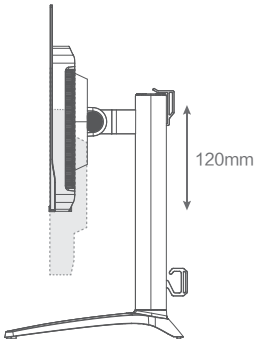
Figure 2-1 Angle Adjustment



Rotation angle
(±20°mm)



Tilting angle
(-5°- +20°)



Height adjustment
(0- 120mm)

NOTE

When adjusting the angle of the monitor, be sure not to touch or press the area of the screen.

The above figure is for reference only, and everything is subject to the actual adjustment function.

3. Button Description

Figure 3-1 Indicator and button display

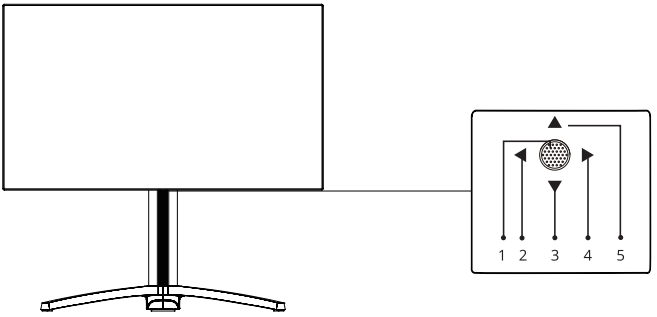


Table 3-1 Indicator description

Name	Description
LED indicator light	• Steady blue light indicates the power is on and the monitor runs normally. • Flicker indicates no video source and no horizontal or vertical signal detected or low voltage. • The light is off when the screen is turned off.

Table 3-1 OSD Buttons

OSD Button	Function
1	Centre button:Confirm key or access the main menu.
2	Left button:Exit or return to the previous menu.
3	Down button:Move down in the menu or select turn off the monitor.
4	Right button:Quickly adjust the input signal.
5	Up button:Move up in the menu or quickly adjust the Brightness.

NOTE

The above content is for reference only, and everything is subject to actual conditions.

4. Cable Connection

Figure 4-1 Input and output interface

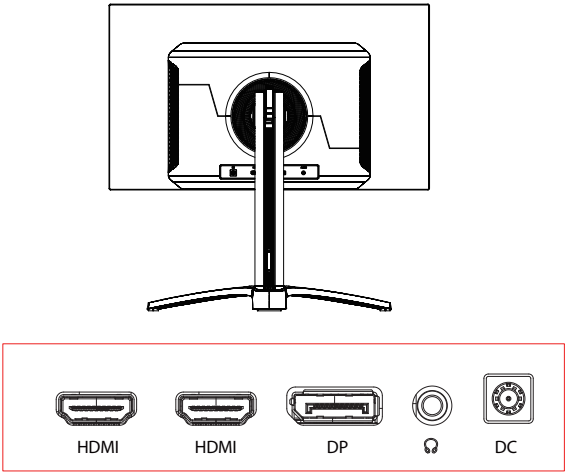


Table 4-1 Input and output ports

Port	Function
HDMI	x2/ Use the HDMI cable to connect the HDMI IN interface of the product to the HDMI OUT interface of a PC.
DP	x1/ Use the DP cable to connect to a desktop PC.
🎧	x1/ Use to connect with external sound output devices such as headphones or earphones.
DC	x1/ Used to connect power adapter, then connect the power cable to a properly grounded power outlet.

NOTE

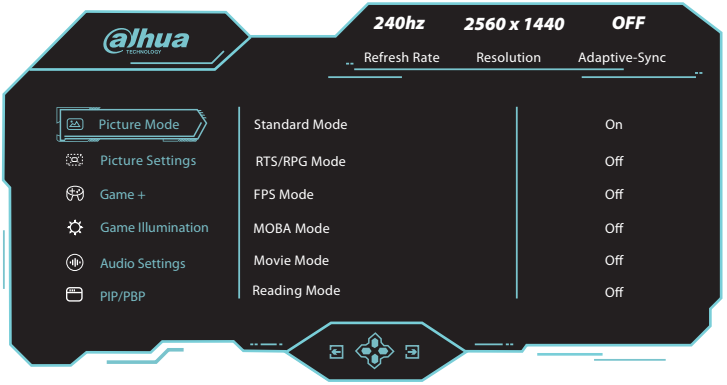
The above ports are for reference only, the actual ports of different types of monitors may be slightly different from the ports in the figure, and everything is subject to the ports and functions of the actual product.

5. Menu Description

- The color and shape of the OSD menu of the actual computer may be slightly different from that shown in the figure, and everything that has been actually displayed shall prevail.
- Specifications of the OSD menu may change with improvements of functions without prior notice.

Press the menu button on the control panel to access the monitor menu. The detailed information of each menu can be found in the following sections.

Step 1. Press **M** to enter the OSD screen.



Step 2. Press ▼or▲ to browse functions.

- Select the desired function, and rocker **M** to enter the sub-menu.
- Press ▼ or ▲ to scroll through sub-menus, and rocker **M** to select and confirm the desired function.
- Press ▼ or▲ to select one option, and rocker **M** to confirm settings and exit from the current menu.

Step 3.Press ◄ to exit the current screen.

6. Operation Menu(OSD) Function Descriptions

Table 6-1 OSD Menu description

Main Menu	Sub Menu	Option
Picture Mode	Standard Mode	Off/On (Default/Custom)
	RTS/RPG Mode	Off/On (Default/Custom)
	FPS Mode	Off/On (Default/Custom)
	MOBA Mode	Off/On (Default/Custom)
	Movie Mode	Off/On (Default/Custom)
	Reading Mode	Off/On (Default/Custom)
	Night Mode	Off/On (Default/Custom)
	Eye Care Mode	Off/On (Default/Custom)
	Mac View Mode	Off/On (Default/Custom)
	E-Book Mode	Off/On (Default/Custom)
	sRGB Mode	Off/On (Default/Custom)
	AdobeRGB Mode	Off/On (Default/Custom)
	DCI-P3 Mode	Off/On (Default/Custom)
Picture Settings	Brightness	0-100
	Brightness Mode	Normal/Highlight/ECO
	Contrast	0-100
	Low Blue Light	0-100
	Sharpness	0-5
	Gamma	1.8/2.0/2.2/2.4/2.6/S.curve
	Aspect Ratio	Wide Screen/4:3/1:1/21:9/Auto
	Color Temperature	Warm
		Natural
		Cool
		User1: 0-100(R/G/B)
		User2: 0-100(R/G/B)
		User3: 0-100(R/G/B)
	Hue	0-100(R/G/B/C/M/Y)
	Saturation	0-100(R/G/B/C/M/Y)
	Eyeshield Remind	Off/On
	Reset Picture Settings	Off/On

Main Menu	Sub Menu	Option
Game+	ALL Game Mode	Wide Screen/25"/sPX Mode/1920x1080
	HDR	Off/Auto/HDR Game/HDR Movie
	Adaptive-Sync	Off/On
	Picture Enhancement	Color Enhancement: Off/Level 1-10
		CR Enhancement: Off/Level 1-5
		Shadow Balance: 0-100
		Night Vision Mode: Off/Level 1-2/Auto Level1-2
		Super Resolution: Off/Level 1-5
		Game Rush Mode: Off/On
		Reset Picture Enhancement: Off/On
	Game Aid	Refresh Rate:Off/On/ Position(Top Right/Top Left/Bottom Right/Bottom Left)
		Game Crosshair: Off/On/Crosshair1/Crosshair2/Crosshair3/ Crosshair4/Crosshair5/Crosshair6
		Crosshair Color: Red/Yellow/Green/Cyan/Blue/Purple/ White/Auto
		Stop Watch: Off/On/15:00/30:00/45:00/60:00/ Position(Top Right/Top Left/Bottom Right/Bottom Left)
		Game Time: Off/On/15:00/30:00/45:00/60:00/ Position(Top Right/Top Left/Bottom Right/Bottom Left)
		Magnifier Mode: Off/On/Window Size/Window Position/ Night Vision Mode
		Alignment Aid: Off/On
		Reset Game Aid: Off/On
Game Illumination	Light Strip	Mode: Light/Breath/Left Water/Right Water/Left Wave/ Right Wave/Flicker/Reflect/Star
		Color: Red/Green/Blue/Cyan/Purple/Yellow/White/Rainbow/ Custom
		Speed: Level1/Level2/Level3/Level4/Level5
	Ring Light	Mode: Light/Breath/Left Water/Right Water/Left Wave/ Right Wave/Flicker/Reflect/Star
		Color: Red/Green/Blue/Cyan/Purple/Yellow/White/Rainbow/ Custom
		Speed: Level1/Level2/Level3/Level4/Level5
	Picture Rhythm	Off/Global Rhythm/2 Zone Rhythm

Main Menu	Sub Menu	Option
Game Illumination	Boot On-Off	Boot On: Mode1/Mode2
		Boot Off: Mode1/Mode2
	Brightness	Off/Low/Middle/High
	Reset Game Illumination	Off/On
Audio Settings	Volume	0-100
	Audio Mute	Off/On
	Reset Audio Settings	Off/On
PIP/PBP	PIP/PBP Mode	Off/PIP Mode/PBP 2Win 1:1
	Sub-Signal Source	DP/HDMI1/HDMI2
	Audio Source	Auto/DP/HDMI1/HDMI2
	PIP Position	Top Right/Top Left/Bottom Right/Bottom Left
	PIP Size	Small/Medium/Large
	Window Swap	Off/On
	Reset PIP/PBP	Off/On
I/O Settings	Input Signal	Auto/DP/HDMI1/HDMI2
	Quick Boot	Off/On
	DDC/CI	Off/On
	Quantization Range	RGB Limit (16~235)/RGB Full (0~255)/Auto
	Reset I/O Settings	Off/On
System Settings	Language	简体中文/English/한국어 /عربى/Portugues do Brasilazil/ Deutsch/Nederland/Suomi/Français/Ελληνικά/Indonesia/ Italiano/日本語/Malaysia/Polskie/Português/Русский/Español/ ไทย/Українська/Tiếng Việt/繁體中文/Türkçe
	OSD Time Out	5-60
	OSD H-Position	0-100
	OSD V-Position	0-100
	OSD Transparency	0-5
	Hotkey1 Setting	Brightness/Contrast/Volume/Audio Mute/Shadow Balance/ Game Crosshair/Magnifier Mode/Refresh Rate/Game Time/ Color Enhancement/Night Vision Mode/Super Resolution/ Adaptive-Sync/Picture Mode/HDR/Input Signal/ Game Illumination/PIP/PBP/ALL Game Mode
	Hotkey2 Setting	
	OSD Lock	Off/On

Main Menu	Sub Menu	Option
System Settings	Energy Saving	Power Saving: Off/Level 1
	Information	InputSource/Resolution/Picture Mode/USB FW Ver:/ HDR State:/Barcode:
	Restore Factory Settings	Yes/No
OLED Care	Pixel Shift	Slow/Medium/Fast
	Screen Saver	Strength: Slider 1-7
		Detection Rate: Slow/Fast
	Static Icon Detection	Strength:Off/Week/Strong
	Low Power Consumption	Off/On
	Taskbar Detection	Off/Week/Medium/Strong
	Boundary Detection	Off/Week/Medium/Strong
	Panel Maintenance	Off/On
	Protection Notice	Off/On
	Oled Care Mode	Custom/Strong
	Reset OLED Care	Off/On

NOTE

The OSD features in the table above are for reference only and may differ from the actual display, so the OSD features of the actual display shall prevail.

Appendix 1 Security Commitment and Recommendation

Dahua Vision Technology Co., Ltd. (hereinafter referred to as "Dahua") places great emphasis on cybersecurity and privacy protection. We continuously allocate special funds to enhance employees' awareness and capabilities in security, and ensure sufficient security protection for our products. Dahua has established a professional security team to provide comprehensive security empowerment and control throughout the entire product lifecycle, including design, development, testing, production, delivery, and maintenance. Dahua products adhere to the principle of minimum necessary data collection, service minimization, strict prohibition of backdoors, and the disabling of unnecessary and insecure services (such as Telnet).
We continuously introduce innovative security technologies to bolster the security capabilities of our products. Additionally, we go above and beyond by providing global users with security alarm and 24/7 security emergency response services. This approach ensures that we are better safeguarding their security rights and interests. At the same time, Dahua encourages users, partners, suppliers, government agencies, industry organizations and independent researchers to report potential risks or vulnerabilities to the Dahua PSIRT. They can do so by visiting the cybersecurity section on the Dahua website.
The security of software platforms not only relies on the continuous attention and efforts from manufacturers throughout R & D, production, and delivery, but also requires active participation from users. Users should remain attentive to the environment and methods to ensure its secure operation. To this end, we suggest users to safely use the software platform,
including but not limited to:

1. Account Management

1.1 Use Strong 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.

1.2 Change passwords periodically

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

1.3 Assign Accounts and Permissions Reasonably

According to business and management needs, reasonably add new users, and reasonably allocate a minimum set of permissions for them.

1.4 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.

1.5 Set and Update Passwords Reset Information Timely

The platform supports password reset function. To reduce the risk of being attacked, please set up related information for password reset in time. 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.

1.6 Enable Account Binding IP/MAC

It is recommended to enable the account binding IP/MAC mechanism to further improve access security.

2. Service Configuration

2.1 Enable HTTPS

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

2.2 Disable Unnecessary Services and Choose Secure Modes

If not needed, it is recommended to turn off some services such as SNMP, SMTP, etc., to reduce risks.
If necessary, it is highly recommended that you use safe modes,
including but not limited to the following services:

- SMTP: Choose TLS to access mailbox server.
- FTP: Choose SFTP, and set up strong passwords.

3. Network Configuration

3.1 Enable Firewall Allowlist

We suggest you to enable allowlist function to prevent everyone, except those with specified IP addresses, from accessing the system. Therefore, please be sure to add your computer's IP address and the accompanying equipment's IP address to the allowlist.

3.2 Network Isolation

The network should be isolated by partitioning the video monitoring network and the office network on the switch and router to different VLANs. This prevents attackers from using the office network to launch Pivoting attacks on the video monitoring network.

4. Security Auditing

4.1 Check Online Users

It is recommended to check online users irregularly to identify whether there are illegal users logging in.

4.2 View the Platform Log

TBy viewing the log, you can get the IP information of the attempt to log in to the platform and the key operation information of the logged-in user.

5. Physical Protection

We suggest that you perform physical protection to the device that has installed the platform.
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.

6. Perimeter Security

We suggest that you deploy perimeter security products and take necessary measures such as authorized access, access control, and intrusion prevention to protect the software platform security.

Appendix 2 Security Commitment and Recommendation

Dahua Vision Technology Co., Ltd. (hereinafter referred to as "Dahua") attaches great importance to cybersecurity and privacy protection, and continues to invest special funds to comprehensively improve the security awareness and capabilities of Dahua employees and provide adequate security for products. Dahua has established a professional security team to provide full life cycle security empowerment and control for product design, development, testing, production, delivery and maintenance. While adhering to the principle of minimizing data collection, minimizing services, prohibiting backdoor implantation, and removing unnecessary and insecure services (such as Telnet), Dahua products continue to introduce innovative security technologies, and strive to improve the product security assurance capabilities, providing global users with security alarm and 24/7 security incident response services to better protect users' security rights and interests. At the same time, Dahua encourages users, partners, suppliers, government agencies, industry organizations and independent researchers to report any potential risks or vulnerabilities discovered on Dahua devices to Dahua PSIRT, for specific reporting methods, please refer to the cyber security section of Dahua's official website.

Product security requires not only the continuous attention and efforts of manufacturers in R&D, production, and delivery, but also the active participation of users that can help improve the environment and methods of product usage, so as to better ensure the security of products after they are put into use. For this reason, we recommend that users safely use the device, including but not limited to:

1. Account Management

1.1 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.

1.2 Change passwords periodically

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

1.3 Allocate accounts and permissions appropriately

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

1.4 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.

1.5 Set and update password reset information in a timely manner

Dahua 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.

2. Service Configuration

2.1 Enable HTTPS

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

2.2 Encrypted transmission of audio and video

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

2.3 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.

2.4 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.

3. Network Configuration

3.1 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.

3.2 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.

3.3 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;
Stablish 802.1x access authentication system to reduce the risk of illegal terminal access to the private network.

4. Security auditing

4.1 Check online users

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

4.2 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.

4.3 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.

5. Software Security

5.1 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.

5.2 Update client software in time

We recommend you to download and use the latest client software.

6. 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).

ENABLING A SMARTER SOCIETY AND BETTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address: No.1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053
Email: dhovereas@dhvisiontech.com | Tel: +86-571-87688888 28933188