



LED Monitor

User's Manual



Foreword

General

This manual describes the functions, operations, and precautions of the LED Monitor (hereinafter referred to as the "Devices"). Please read the device carefully before using it, and keep the instruction manual 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.

Revision History

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

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, audio, 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, and comply with the guidelines when using it.

Operation Requirements



- 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: 0 °C to +40 °C (+32 °F to +104 °F).
- Use the device under allowed humidity and temperature conditions.
- ---: Direct current.

Installation Requirements



WARNING

- 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.



- 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.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Note that the power supply requirements are subject to the device label.
- Connect class I electrical appliances to a power socket with protective earthing.



The terms HDMI and HDMI High-Definition Multimedia Interface, and the HDMI Logo are trademarks or registered trademarks of HDMI Licensing Administrator, Inc. in the United States and other countries.

Table of Contents

Foreword	I
Important Safeguards and Warnings	III
1 Product Information	1
1.1 Appearance	1
1.2 Features	1
2 Ports	2
3 Main Menu	3
3.1 PICTURE Menu	4
3.2 IMAGE Menu	4
3.3 COLOR TEMP Menu	5
3.4 OSD SETTING Menu	5
3.5 RESET Menu	6
3.6 MISC. Menu	6
3.7 Channel Selection	7
4 FAQ	8
4.1 How to Clean Product	8
4.2 Troubleshooting	8
Appendix 1 Security Commitment and Recommendation	10

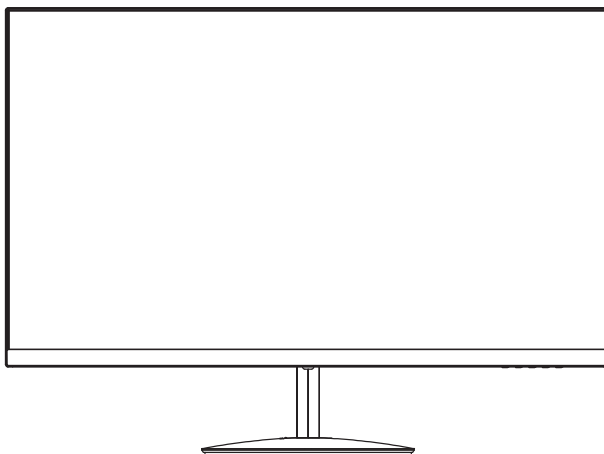
1 Product Information

1.1 Appearance



The figures in the manual are for reference only, and might differ from the actual product.

Figure 1-1 Appearance



1.2 Features

- Low energy consumption, long service life.
- High contrast ratio and high luminance.
- Automatically eliminates ghosting.
- Rapid response times, no trailing image.
- Thin and light.
- Full-HD LCD panel with top-ranking video processing chip.

2 Ports

Please connect the monitor to external devices according to the following I/O interface list. Choose the corresponding incoming signal channel.



Please turn off the power of the external device and the product when connecting.

Figure 2-1 Port A

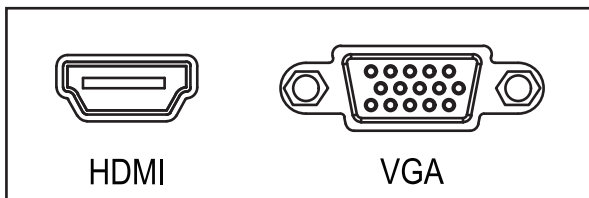


Table 2-1 Ports Description

Name	Description
HDMI INPUT	HDMI Connector
VGA INPUT	D-SUB 15 pins Connector

3 Main Menu

To activate, press the menu button on the bottom right of the bezel. The sub-menus of the main menu are: Picture menu, Image Menu, Color Temp menu, OSD Setting menu, Reset menu and Misc menu. Press the menu button to select the sub-menu item. The selected menu item will show a bordered wireframe. Press the ▲▼ button to move among the secondary menu items of the sub-menu.

Figure 3-1 5 key



Table 3-1 Icon description

Icon	Description
	Source button. Press the button to display all the signal channel menus.
	Downward button. - Press the button to move the cursor to the needed function. - Press the button to change the selected function in OSD menu item.
	Upward button. - Press the button to move the cursor to the needed function. - Press the button to change the selected function in OSD menu item.
	Menu button. - Press the button to display the OSD main menu. - Press the button to Exit the OSD menu or menu item.
	Power button. Press the button to turn on or turn off the display.

3.1 PICTURE Menu

PICTURE menu can set the brightness, contrast, black equalizer, low blue, ECO and DCR function.
Press ▲▼ button to adjust value when item is selected, press menu button to exit.

Figure 3-3 PICTURE



3.2 IMAGE Menu

IMAGE menu can set H.position, V.position, clock, phase and aspect function.

Press ▲▼ button to adjust value when item is selected, press menu button to exit.

Figure 3-4 IMAGE

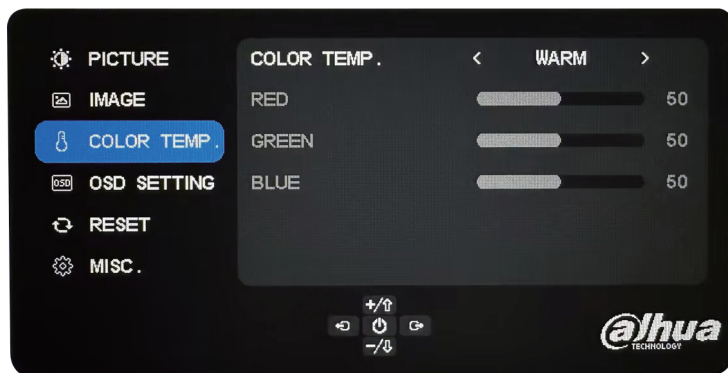


3.3 COLOR TEMP Menu

COLOR TEMP menu can set color temp function.

Press ▲▼ button to adjust value when item is selected, press menu button to exit.

Figure 3-5 COLOR TEMP

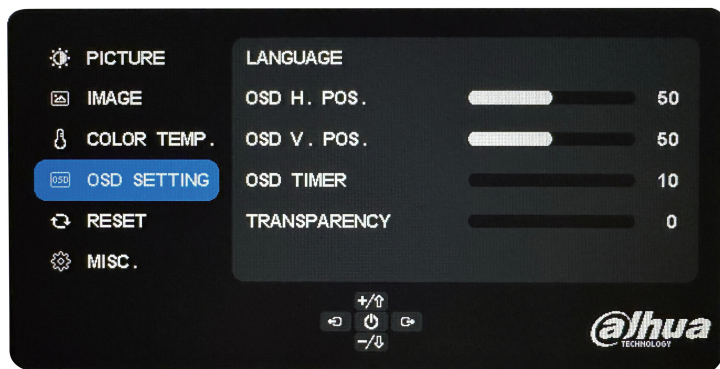


3.4 OSD SETTING Menu

OSD SETTING menu can set language, OSD H/V. POS, OSD timer and transparency function.

Press ▲▼ button to adjust value when item is selected, press menu button to exit.

Figure 3-6 OSD SETTING

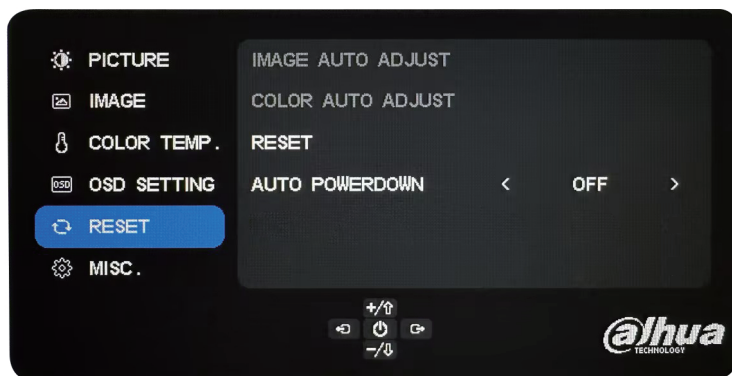


3.5 RESET Menu

RESET menu can set image auto adjust, color auto adjust, reset and auto powerdown function.

Press ▲▼ button to adjust value when item is selected, press menu button to exit.

Figure 3-7 RESET



3.6 MISC. Menu

MISC menu can set signal source function.

Press ▲▼ button to adjust value when item is selected, press menu button to exit.

Figure 3-8 MISC.



3.7 Channel Selection

"Source" menu can select channel (input). The options include VGA, HDMI.

Press ▲ ▼ button to adjust value when item is selected, press menu button to confirm.

4 FAQ

4.1 How to Clean Product

1. Please wipe dust and other particles off with a clean soft towel.
2. If it is still not clean, please use a neutral cleaner along with the clean soft towel. Wipe dry after cleaning it.
3. Rubbing or scrapping the housing with fingernails or other hard objects might scratch the housing.

4.2 Troubleshooting

Before consulting service staff, please use the following chart to attempt to diagnose the issue.

Problem	Solution									
	1	2	3	4	5	6	7	8	9	10
No image or sound	●	●	●		●				●	●
Inferior sound, normal image	●	●		●	●				●	
Inferior image, normal sound	●		●	●	●	●			●	
Poor signal	●	●	●		●				●	
Vague image	●		●		●				●	
Double image	●	●	●		●					
Interfering lines in image	●		●	●	●					
Twisty image	●		●		●				●	
Poor signal	●	●	●	●	●				●	
Rung stripe in image			●	●						
Image vertically scrolls	●		●	●					●	
Inferior color	●		●	●	●	●	●	●	●	
No color	●		●		●			●	●	

Solution	
1	Switch to another channel or input.
2	Check whether the audio signal line is connected.
3	Check whether the video signal line is connected.
4	Interference from by other electric appliance may be present.
5	Adjust fine tuning setting.
6	Adjust luminance setting.
7	Adjust contrast ratio setting.
8	Adjust color setting.
9	Check whether the system is set-up properly.
10	Check whether the power is on.

Certificate of Approval
Inspector:
Inspector date:
The product accords with the technical criteria and is allowed to sell

Appendix 1 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;

Establish 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: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188