LED Monitor

User's Manual

ZHEJIANG DAHUA VISION TECHNOLOGY CO, LTD.

V1.0.0

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.

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.

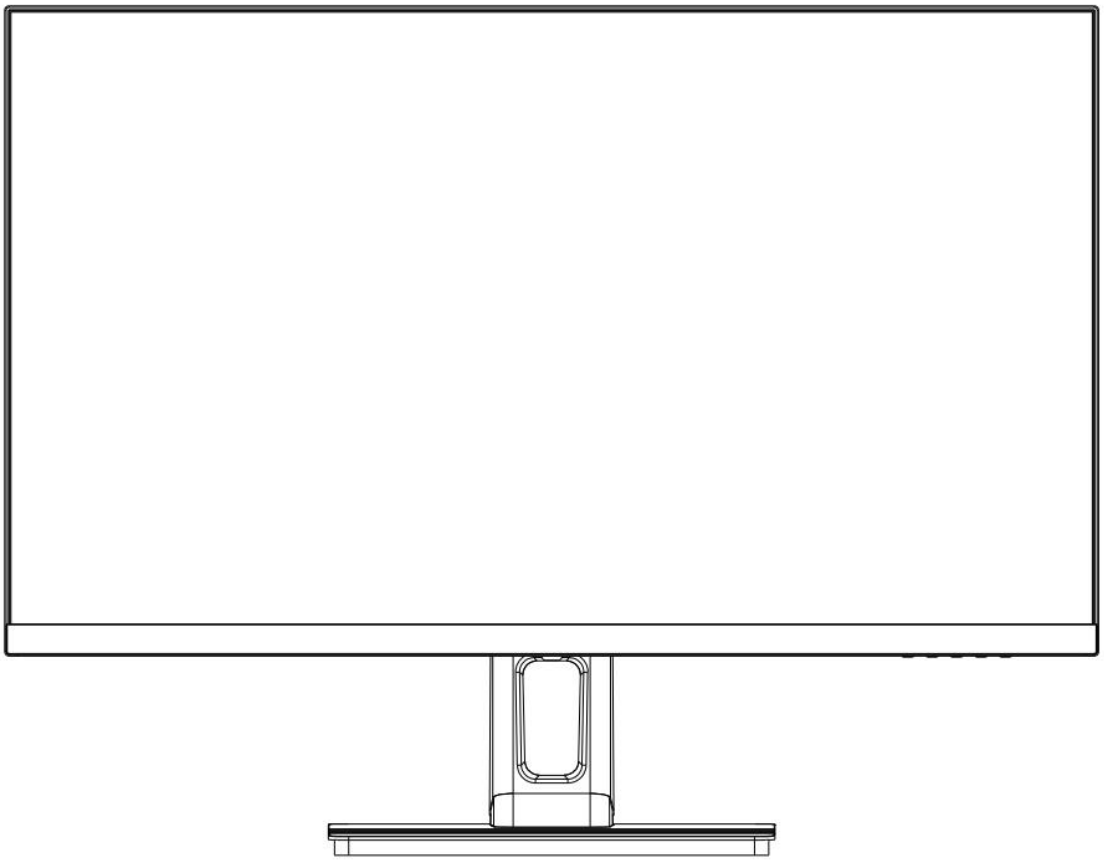
Table of Contents

1 Product Information

1.1 Appearance

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

Figure 1-1Appearance



（Photos are for reference only）

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.
- QHD 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 2-1Ports

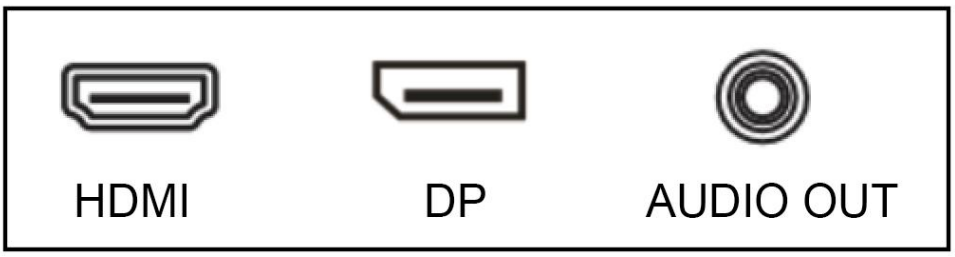
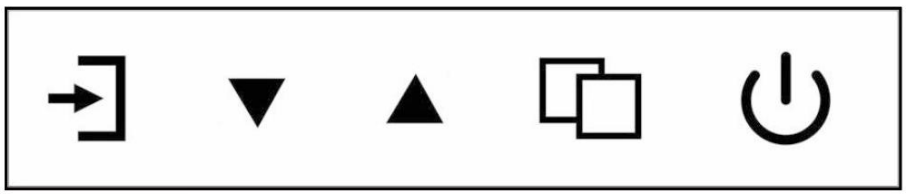


Table 2-1Port description

Name	Description
HDMI	HDMI Connector
DP	DP Connector
AUDIO OUT	3.5mm audio port

3 Main Menu

To activate, Press the button in the bottom right corner of the monitor. The sub-menus of the main menu are: PICTURE, IMAGE, COLOR TEMP, OSD SETTING, RESET and MISC.
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.



A. "Source" button

1. Press the button to display all the signal channel menus.

2. Press the button in the menu to enter the next level of menu.

B. "Downward" button

1. Press the button to move the cursor to the needed function.

C. "Upward" button

1. Press the button to move the cursor to the needed function.

D. "Menu" button

1. Press the button to display the OSD main menu.

2. Press the button to in the menu to return to the previous menu level.

E. "Power" button

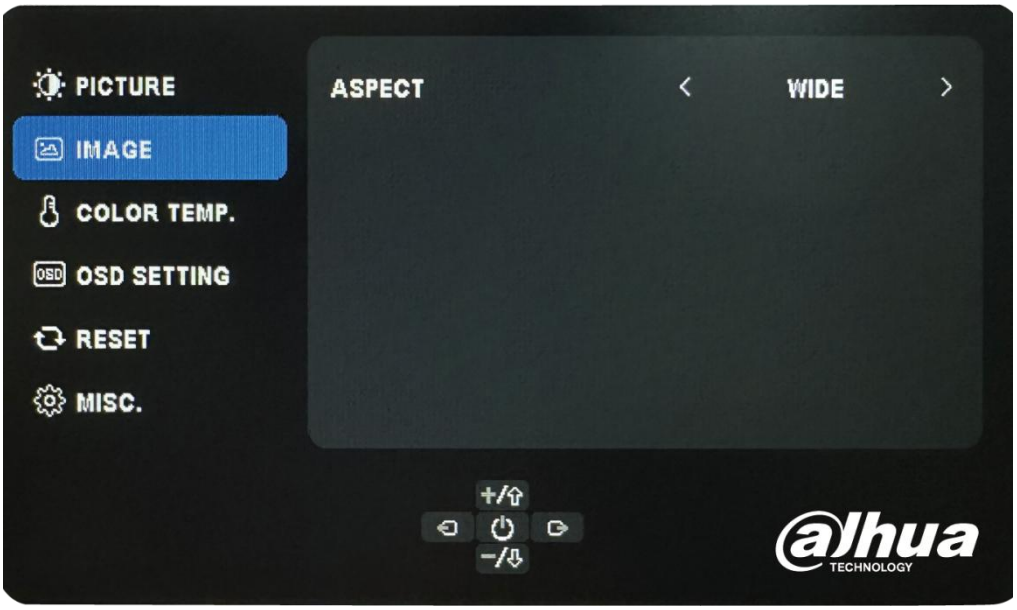
1. Press the button to turn on or turn off the display.

3.1 PICTURE MENU

BRIGHTNESS menu sets the BRIGHTNESS, CONTRAST, ECO,DCR and HDR MODE function.
Press▲▼button to adjust value when item is selected. Press the MENU to exit.

3.2 IMAGE MENU

IMAGE menu can set ASPECT function.
Press▲▼button to adjust value when item is selected. Press the MENU to exit.

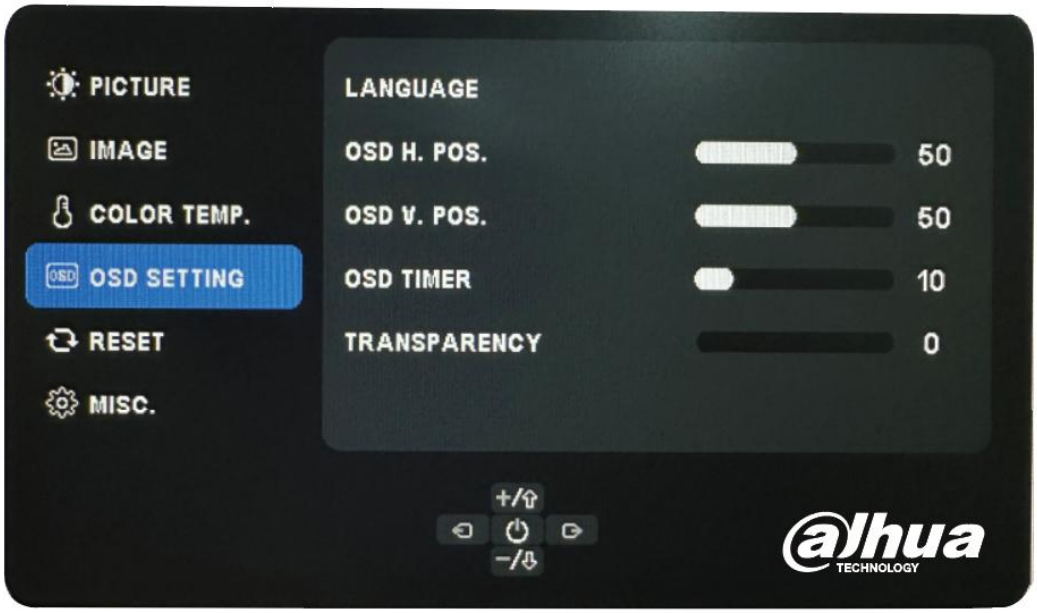


3.3 COLOR TEMP. MENU

COLOR menu can set COLOR TEMP. and LOW BLUE LIGHT function.
Press▲▼button to adjust value when item is selected. Press the MENU to exit.

3.4 OSD SETTING MENU

OSD SETTING menu can adjust LANGUAGE, OSD H. POS, OSD V. POS, OSD TIMER and TRANSPARENCY function.
Press▲▼button to adjust value when item is selected. Press the MENU to exit.



3.5 RESET MENU

RESET menu can set RESET function.

Press▲▼button to adjust value when item is selected. Press the MENU to exit.

3.6 MISC. MENU

MISC. Menu can adjust SIGNAL SOURCE, MUTE, VOLUME, FREESYNC and OD function.

Press▲▼button to adjust value when item is selected. Press the MENU to exit.

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 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations from Dahua on how to create a more secured security system.

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.

More information

Please visit Dahua official website security emergency response center for security announcements and the latest security recommendations.

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