

6 FAQ

1. The whiteboard shuts down automatically.
 - Check whether you have enabled the sleep function. You can refer to the regular PC troubleshooting procedure.
 - Check the channel of the input source. If there is no signal, the whiteboard will shut down automatically.
 - Check whether the power supply is stable.
2. The indicator light is off.
 - Check whether the power supply is normal.
 - Check whether the rocker switch of the whiteboard is turned on.
3. Missing or abnormal colors.

If the whiteboard is connected to a computer, check whether the VGA or HDMI cable is intact and correctly connected.
4. The image is not displayed in full screen or part of the image is outside the screen.
 - Check whether the resolution is 16:9.
 - If the whiteboard is connected to a computer, unplug the VGA or HDMI cable and then plug again.
5. The whiteboard displays images but has no sound.
 - Adjust the volume.
 - If the whiteboard is connected to a computer, check whether the audio cable is correctly connected.
6. Low accuracy of touch positioning.
 - Make sure to place the pen or finger on the screen vertically at a 90-degree angle.
 - Check whether other objects such as paper and sleeve are contacting the screen.
 - Check whether the resolution is 16:9.
7. Touch control is not effective.

If the whiteboard is connected to a computer, check whether the touch cable is correctly connected.

Appendix 1 Touch Operation

You can use the stylus pen or directly use your fingers to operate on the device screen.



This section uses operation with stylus pen as an example.

Appendix Table 1-1 Touch operations

Operation	Description
Tap	Tap the screen once with the stylus pen.
Double-tap	Tap the screen twice with the stylus pen (The time gap of the taps is around 0.5 s).
Right-hand button menu	Slightly touch the screen 1 s to 2 s with the stylus pen. Lift the stylus pen when there is a circle on the screen. Then, the right-hand button menu is displayed.
Drag	Hold the icon that needs to be dragged with the stylus pen and then move the stylus pen to the target place. Lift the stylus pen to finish the dragging operation.
Slide	Hold the screen (slider used for web browser, for example) that needs to be slid with the stylus pen, and then slide the stylus pen toward the direction you want. Lift the stylus pen to finish the sliding operation.
Zoom	Press and hold the window (webs, pictures, for example) that can be zoomed in and zoomed out with a stylus pen. Use another stylus pen drag the window. Hold the screen that can be zoomed (such as webpages or images) with a stylus pen. Use another stylus pen to do the dragging operation. Then, the zoom operation is finished.

Appendix 2 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 equipment 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 equipment (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 equipment 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 equipment network security:

1. Physical Protection

We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment 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 equipment (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 equipment 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 equipment, 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 equipment 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 equipment, 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 equipment 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 SAFER SOCIETY AND SMARTER LIVING

