



# Smart Interactive Whiteboard

## Quick Start Guide








# Foreword

## General

This manual introduces the functions and operations of the smart interactive whiteboard (hereinafter referred to as "the whiteboard").

## Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
 <b>DANGER</b>	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
 <b>WARNING</b>	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
 <b>CAUTION</b>	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
 <b>TIPS</b>	Provides methods to help you solve a problem or save time.
 <b>NOTE</b>	Provides additional information as a supplement to the text.

## Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	December 2021

## 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 whiteboard, hazard prevention, and prevention of property damage. Read carefully before using the whiteboard, comply with the guidelines when using it, and keep the manual safe for future reference.

## Storage Requirements



- Place the whiteboard on a sturdy work bench to prevent it from falling.
- Do not place the whiteboard in a place exposed to sunlight or near heat sources.
- Store the whiteboard under allowed humidity and temperature conditions.

## Installation Requirements



- Do not install the whiteboard in a place exposed to sunlight or near heat sources.
- Keep the whiteboard away from dampness, dust, and soot.
- Install the whiteboard on a stable place to prevent it from falling.
- Install the whiteboard in a well-ventilated place, and do not block its ventilation.
- 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.
- The whiteboard is a class I electrical appliance. Make sure that the power supply of the whiteboard is connected to a power socket with protective earthing.
- The appliance coupler is a disconnection device. Keep a convenient angle when using it.

## Operation Requirements



- High voltage inside the whiteboard. Do not disassemble the whiteboard without a qualified professional present to avoid the risk of being exposed to danger.
- Improper use of the battery might result in a fire or explosion.
- Make sure to use the same model when replacing the battery to avoid fire or explosion.
- Use the standard power adapter. We will assume no responsibility for any problems caused by the use of a nonstandard power adapter.
- Use power cords that conform to your local requirements and rated specifications.
- Make sure all cables are connected correctly before plugging the whiteboard into the power. Do not overload the power socket or pull the power code. Otherwise, it might cause fire or electric shock.



- Do not drop or splash liquid onto the whiteboard, and make sure that there is no object filled with liquid on the whiteboard to prevent liquid from flowing into it.
- 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.

- Operate the whiteboard within the rated range of power input and output.
- Do not disassemble the whiteboard.
- Use the whiteboard under allowed humidity and temperature conditions.
- The whiteboard is a class I electrical appliance. Make sure that the power supply of the whiteboard is connected to a power socket with protective earthing.
- The appliance coupler is a disconnection device. Keep a convenient angle when using it.

## Maintenance Requirements



- Unplug the power cord before cleaning the whiteboard. Do not use the liquid cleaner or spray cleaner when cleaning the whiteboard.
- 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 might damage the screen.

# Table of Contents

Foreword.....	I
Important Safeguards and Warnings.....	III
1 Introduction.....	1
2 Packing List.....	2
3 Installation .....	3
3.1 Installation Accessories.....	3
3.2 Tools .....	3
3.3 Installation Procedure.....	4
4 Appearance.....	8
Appendix 1 Cybersecurity Recommendations.....	11

# 1 Introduction

Smart interactive whiteboard is an integrated multimedia device, which integrates large-screen HD display, PC, TV, electronic whiteboard, audio amplifier, application, and central control system.

The whiteboard has the following characteristics:

- Supports 4K HD LCD display.
- Supports switch between Android and Windows systems (you need to install a PC module).
- Supports one-tap projection of devices such as mobile phones and pads.
- Supports electronic whiteboard.
- Supports Office software such as Microsoft Office and audio and video files.

## 2 Packing List

Check whether there is any obvious damage on the packing box. Unpack the box and check whether the components are complete according to the packing list.

Table 2-1 Packing list

Name	Quantity	Name	Quantity
Smart interactive whiteboard	1	Power cord	1
Stylus pen	2	Quick Start Guide	1
Quality certificate	1	Accessory package	1
Wall mount (installed on whiteboard already)	1	—	—



## 3 Installation

### 3.1 Installation Accessories

Figure 3-1 Installation accessories

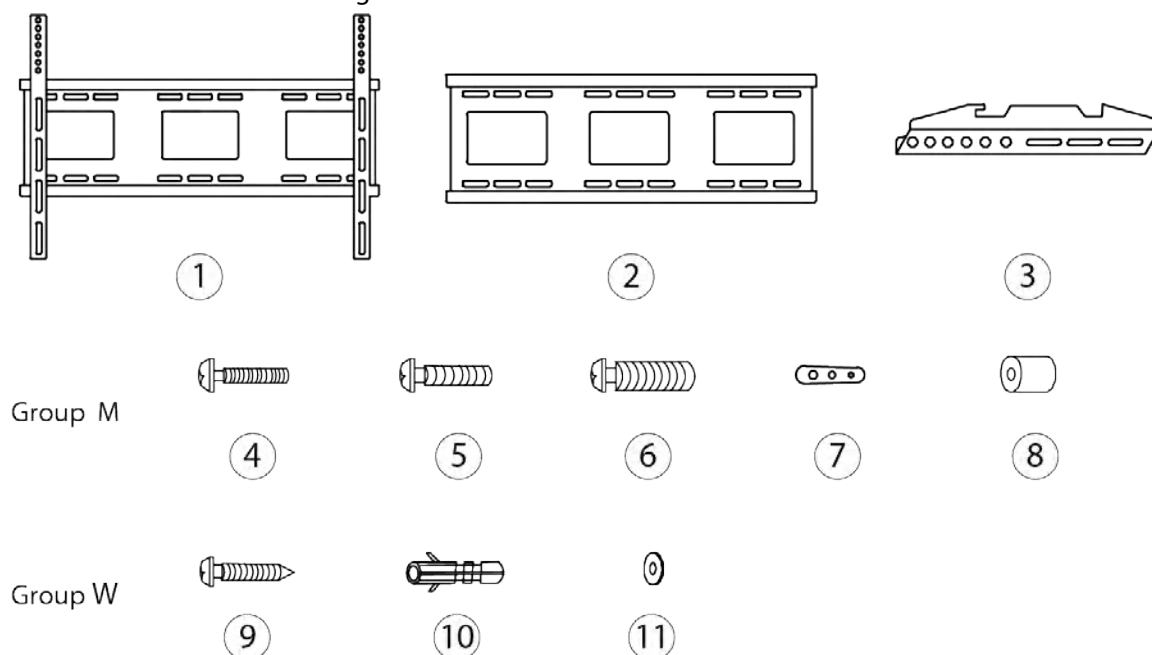


Table 3-1 Accessory description

No.	Name	No.	Name
1	Installation bracket	7	ø5/ø6/ø8 4PCS M-D
2	Wallboard× 1	8	ø13 × ø6.5 × 15 4PCS M-E
3	Hook× 2	9	M6 × 50 6PCS W-A
4	M5 × 25 4PCS M-A	10	ø10 × 50 6PCS W-B
5	M6 × 25 4PCS M-B	11	ø6 6PCS W-C
6	M8 × 25 4PCS M-C	—	—

### 3.2 Tools

The following tools do not come with the whiteboard. Purchase them as needed.

Figure 3-2 Electric drill

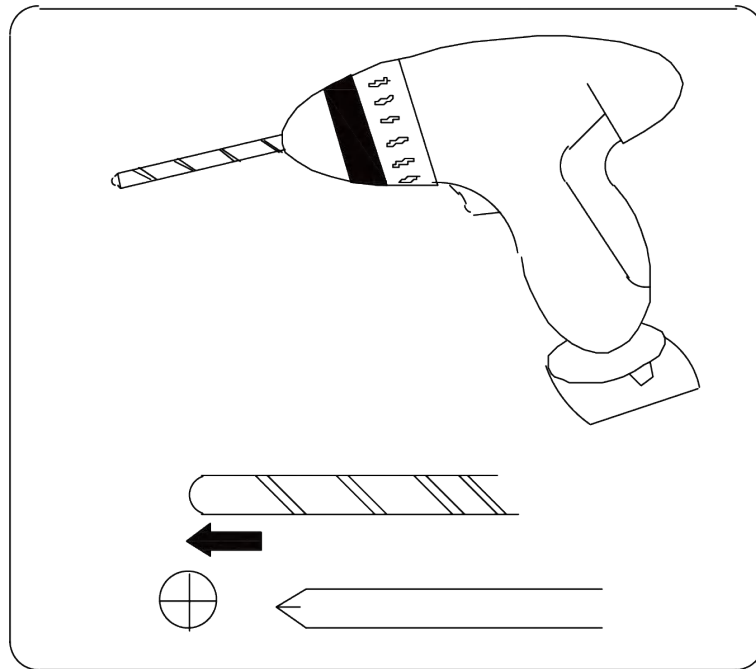
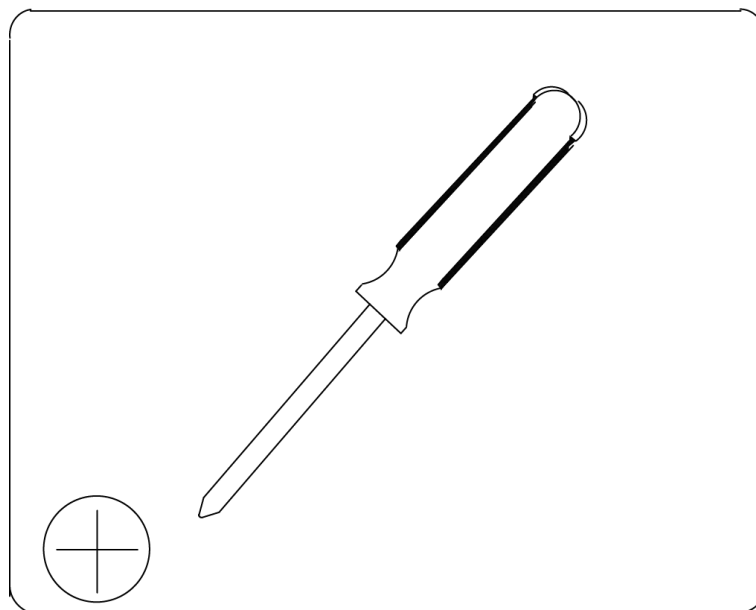


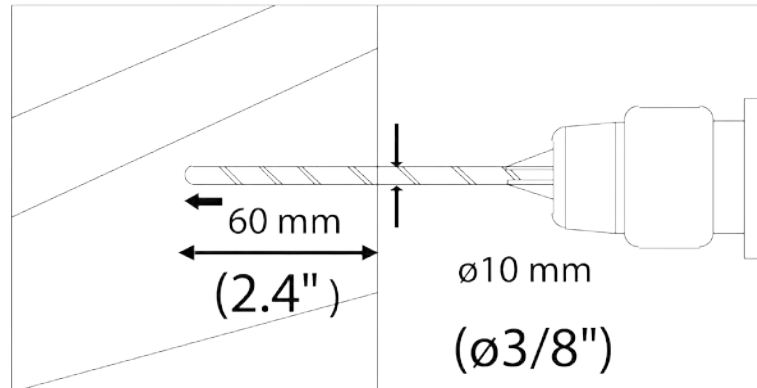
Figure 3-3 Screwdriver



### 3.3 Installation Procedure

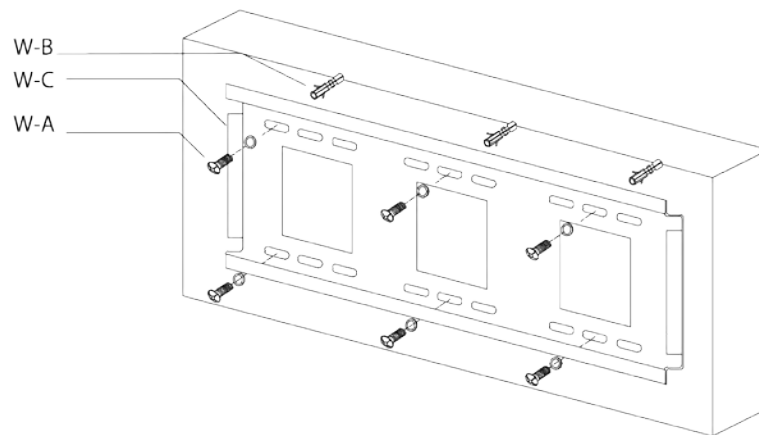
Step 1 Mark installation positions on the wall and then drill holes at the marked positions.

Figure 3-4 Required hole diameter and depth



**Step 2** Install the wallboard onto the wall and keep it horizontal.

Figure 3-5 Install wallboard



**Step 3** Install the hooks on the rear panel of the whiteboard with screws.



- The screws in the accessory package have various specifications. Select four appropriate ones and keep the rest as spare.
- If thicker gaskets are used, install the gaskets between the whiteboard and hooks.

Figure 3-6 Install hooks

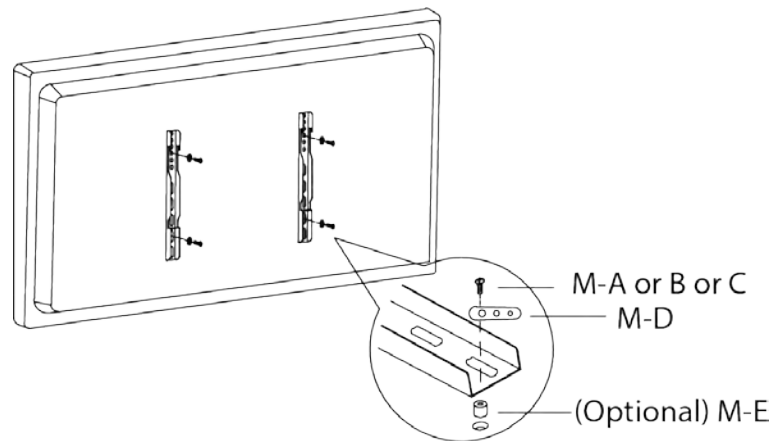
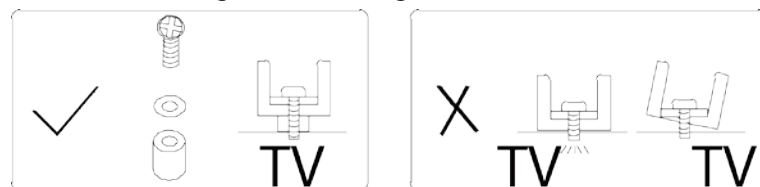


Figure 3-7 Install gasket



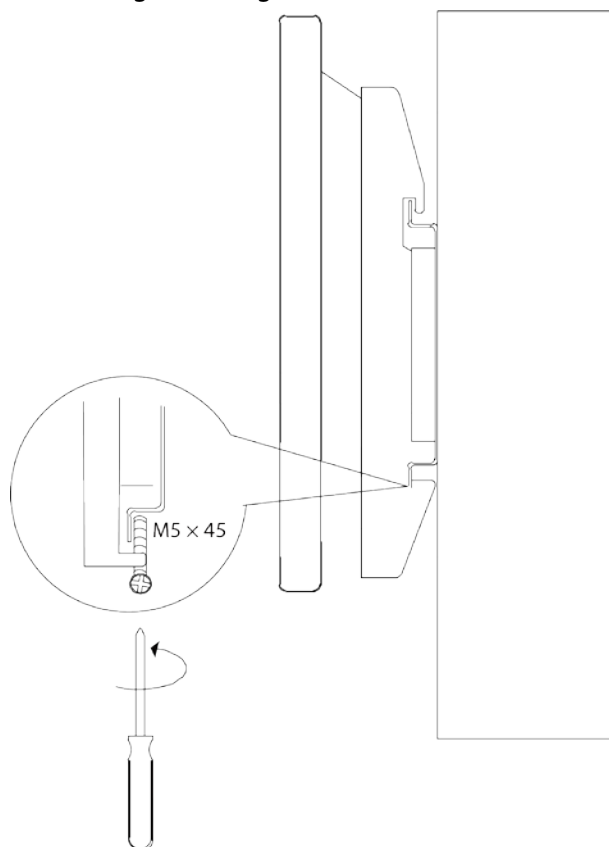
**Step 4** Hang the whiteboard on the wallboard through the hooks.

**Step 5** Tighten the screws at the bottom of the hooks to secure the bracket.



Make sure that the appropriate screwdriver is used.

Figure 3-8 Tighten hooks



## 4 Appearance

Figure 4-1 Appearance (without camera)

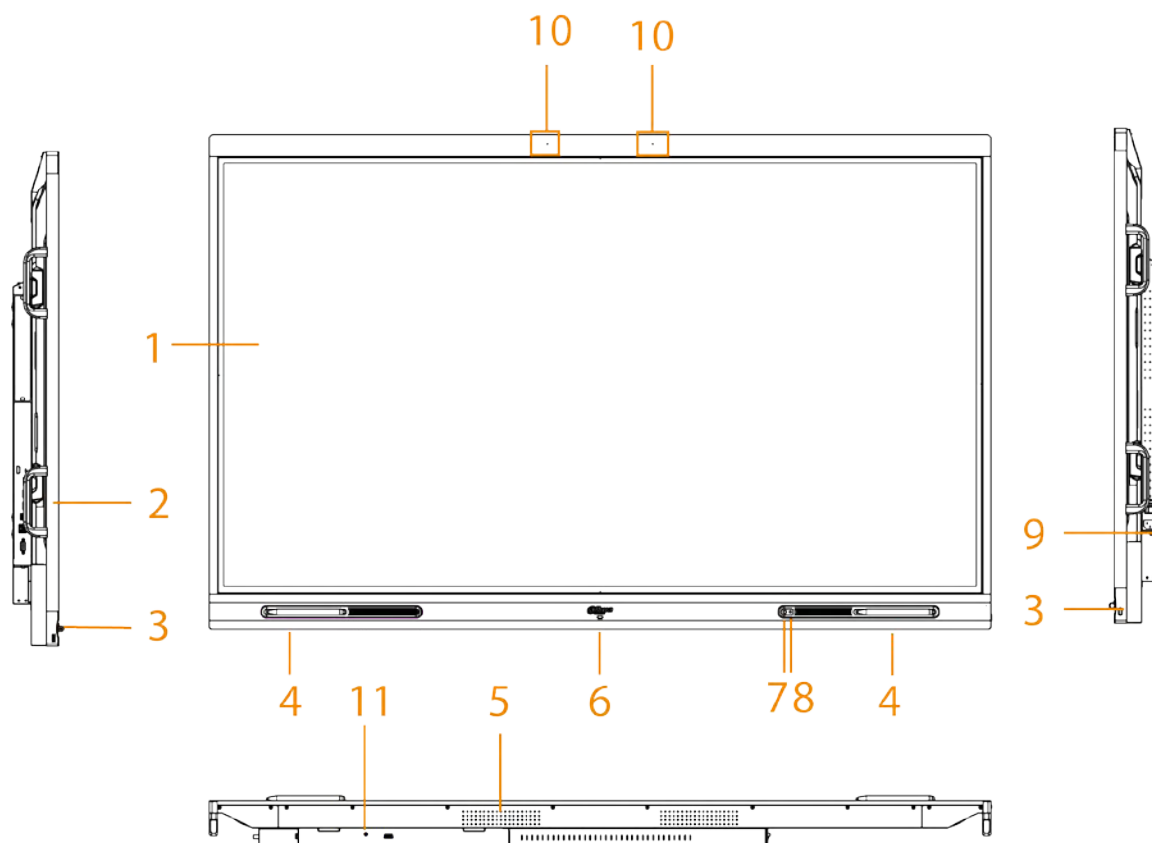


Figure 4-2 Appearance (with camera)

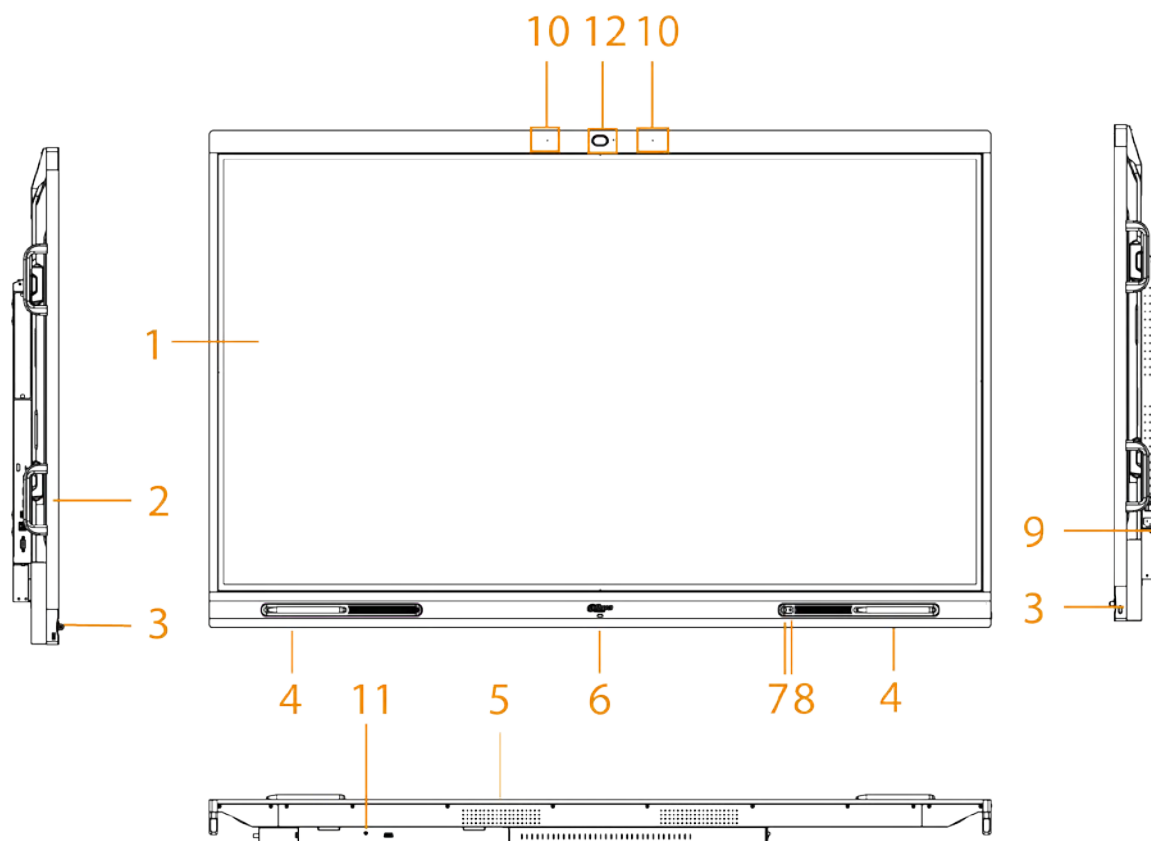


Table 4-1 Appearance description


No.	Description
1	LCD.
2	Left panel ports. For details, see Table 4-2.
3	USB 3.0 port.
4	Stylus pen area.
5	Speaker. Plays multimedia sound.
6	Indicator light. The light is red when the whiteboard is on standby and blue when the whiteboard is in normal use.
7	Light sensor. The whiteboard recognizes the ambient brightness through the light sensor and adjusts the backlight brightness automatically.
8	IR sensor. Receives signals from the remote control.
9	Power input port. Inputs 100–240 VAC power.  After connecting to power supply, press power button to turn on the whiteboard.
10	Microphones. Pick up live audio.
11	LINE OUT. An audio output port that connects to the earphone or speaker.
12	Built-in HD camera.

Figure 4-3 Ports

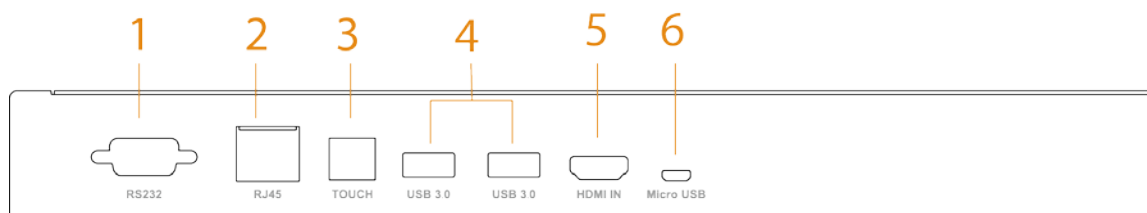


Table 4-2 Port description

No.	Name	Description
1	RS-232	Transmits data between devices. Can connect to central control devices with RS-232 port.
2	RJ-45	Network port. Connects to network cable to access network.
3	Touch	Transmits touch signals.
4	USB 3.0 (5V 0.9A)	Connects to USB devices such as mobile hard disk, USB flash drive, USB keyboard, and USB mouse, It is applicable to Android system and PC module.
5	HDMI IN	HD audio and video signal input port. Connects to PC, set-top box, and other video devices with HDMI output ports.
6	Micro USB	Only applicable to Android system. Uses for system debugging.



# 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 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



