Smart All-In-One LED Display

Quick Start Guide

Foreword

General

This manual introduces the functions and operations of the smart all-in-one LED display (hereinafter referred to as "the Device"). Read carefully before using the Device, and keep the manual safe for future reference.

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
⚠️ 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 result.
📖 NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.2	Updated the information of appearance and sturcture.	February 2024
V1.0.1	Updated the language.	September 2023
V1.0.0	First release.	August 2023

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 device, and comply with the guidelines when using it.

Storage Requirements

⚠

- Stably put the device onto a support platform that is strong enough to prevent the whiteboard from falling.
- Do not place the device in a place exposed to sunlight or near heat sources.
- Store the device under allowed humidity (10%–60% (RH)) and temperature (–20 °C to +60 °C, or –4 °F to +140 °F) conditions.

Installation Requirements

⚠

- Securely attach the device to a structure in the building or a mobile stand before you begin to use it.
- 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.
- Select a suitable wall mount with a yellow label and let it be installed by professionals.
- Do not install the device in a place exposed to sunlight or near heat sources.
- Keep the device away from dampness, dust, and soot.
- 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 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 rated power is 1,600 W (100–180 VAC) or 2,400 W (180–240 VAC).
- The appliance coupler is a disconnection device. Keep it at a convenient angle when using it.
- Make sure to install a circuit breaker or similar devices in the external power circuit.
- Place the device in a location that children cannot easily access.
- Follow the instructions to safely and correctly install the device.

Operation Requirements

⚠ DANGER

- The contact rating of the device is about 13 mA. Before you connect the device to its power supply, make sure the power supply is connected to an earthed power socket.
- Be cautious when using the device to avoid injuring people, especially children.

  ◇ Follow the recommendations of the manufacturer to select whether to install the device in a cabinet, bracket or to use other mounting methods.
  ◇ Do not allow people to climb the device and protect the power supply.

- ◇ Protect the line cord and wires from being walked on or squeezed, and organize them so people cannot trip on them.
- ◇ Do not place the device in an unstable environment.
- 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.
- Replace unwanted batteries with new batteries of the same type and model.
- 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.
- 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.

⚠️ WARNING

- Avoid using the device in an area with a lot of radio interference.
- There is high pressure in the device. To avoid the risk of electric shock, non-professionals should not open the back cover.
- Improper use of the battery might result in a fire or explosion.
- Make sure to use the same model when replacing the battery.
- 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 cord that is recommended for the region and conforms to the rated power specifications.
- Do not overload the power socket or unplug the power cord while the adapter is powered on to avoid electric shock and fires breaking out.

⚠️

- Operate the device within the rated range of power input and output.
- Do not disassemble the device.
- Use the device under allowed humidity (10%–90% (RH)) and temperature (−10 °C to +40 °C, or +14 °F to +104 °F) conditions.
- The appliance coupler is a disconnection device. Keep it at a convenient angle when using it.
- The device has sharp edges. Please be careful when you are next to it.

Maintenance Requirements

⚠️ DANGER

- Make sure to use the same model when replacing the battery to avoid fire or explosion. Dispose the battery strictly according to the instructions on it.
- Power off the device before maintenance to make sure that the device is disconnected from the power supply.

⚠️

- The front cover at the lower beam of the device is used for quick maintenance. When the bottom row of light panels is removed, you must overcome the magnetic pull of the front cover. There is a safety cable connected to the front cover of the device that protects the front cover.
- Cut off the power before cleaning the device. To clean the device, do not use liquid detergents or spray detergents.

- 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.

Table of Contents

1 Introduction

The smart all-in-one LED display is an integrated multimedia device, which integrates large screen, electronic whiteboard, application, and central control system. It can be widely used in enterprise, government and finance.

The Device supports the following functions and features:

- Ultra-light and ultra-thin design: the thickness of the screen is less than 19 mm, and the thickness of the wall-mount installation is less than 39 mm.
- With the design of privacy protection, the device adopts a built-in flip camera, which automatically pans up during use, and pans down when it stops working.
- 8 MP wide-angle camera: Diagonal: 99°, horizontal: 87°, vertical: 49°.
- With built-in fingerprint identification module, supports fingerprint for locking and unlocking screen.
- Wi-Fi 6, which is faster than Wi-Fi 5. You can select 2.4G or 5G bands.
- Screen sharing, group settings, multiple screens and moderator control.
- Reverse controlling of the screen through PAD and phone.
- Scan the QR code to share the file.
- Meeting sign-in through person recognition.
- Non-contact gestures to swipe screens or take snapshots.
- Electronic whiteboard.

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
LED column	5	Transverse beam	1
Front cover	1	Beam connector	1
Camera	1	Power cable	1
Light modules (box)	13	Remote control	1
Projector	1	Type-C cable (on the camera)	1
HDMI cable (on the camera)	1	Hub accessory package	1
LED accessory package	1	Wall mount screw (preinstalled)	16
OPS sheet metal bracket	1	Quick start guide	1
Column screw	40	M5 × 12 screw	12

3 Installation

3.1 Preparation

To ensure correct function and safety, remember to check whether your site is ready for the installation in the first place.

Table 3-1 Preparation

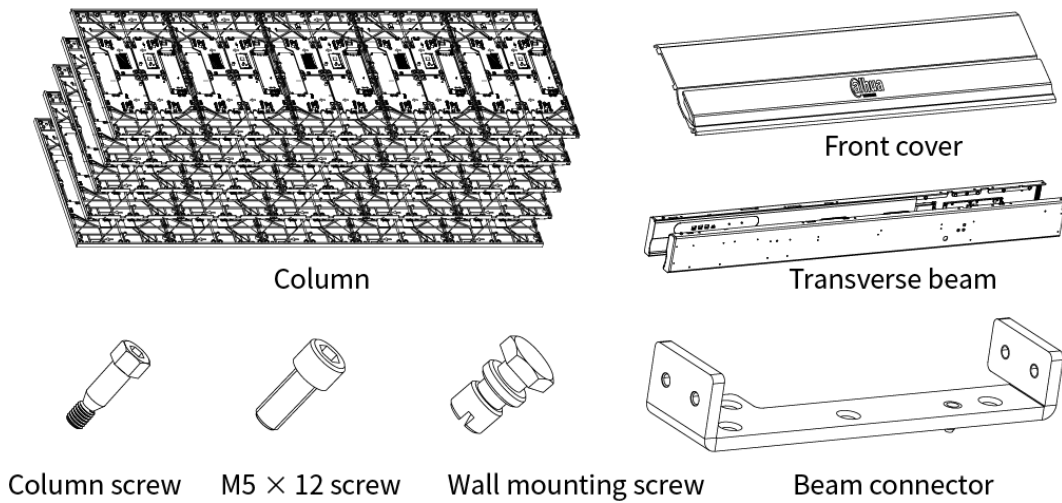| Item	Description
Grounding	The IR touchscreen requires that the site should be safely grounded.
	Check the voltage between the live and neutral wires, between the live and ground wires, and between the neutral and ground wires. If the voltage is abnormal, report the issue to the technician.
	📖
	The specific voltage requirements might vary depending on your local standards.
Power supply	The power supply circuit for the Device should be independent from lighting and other circuits to avoid interference in power frequency.
Wall	Make sure that the wall can bear a load of 160 kg or more.
Space	Make sure that there is enough space for the Device.
	The ideal reserved space is 10 mm greater than the length and height of the Device.
	📖
	If you want to embed the Device onto the wall, make sure that there is enough space for camera, OPS installation, and to use the ports and buttoms of the Device.
Tools	Prepare the installation tools.
	• To install the Device onto a mobile bracket, you need an electric hammer, allen wrench, crosshead screwdriver, slotted screwdriver, combination wrench, front maintenance tools, work gloves, and other tools.
	• To install the Device onto a wall, you need an electric hammer, impact driver, allen wrench, crosshead screwdriver, slotted screwdriver, laser level or spirit level, tape measure, front maintenance tools, work gloves, and other tools.
	📖
	You can find the allen wrench and combination wrench in the accessary package.

3.2 Accessories

Figure 3-1 Installation accessories

Column

Front cover

Transverse beam

Column screw   M5 × 12 screw   Wall mounting screw   Beam connector

Table 3-2 Quantity of installation accessories

Name	Quantity
Column	5
Front cover	1
Transverse beam	1
Beam connector	1
Column screw	40
M5×12 screw	10
Wall mounting screw	16

3.3 Bracket Installation

3.3.1 Installing Mobile Bracket

The mobile bracket comes with 2 Y-shaped vertical poles, 2 horizontal poles, 1 strengthen pole, 4 foot wheels, 8 M8 × 16 screws, 8 M8 × 45 screws, 4 mm Allen wrench and combination wrench.

Procedure

Step 1   Lock the 4 casters, and then screw them into the bottom of the 2 Y-shaped vertical poles. Use the outer hexagonal wrench to tighten the casters.

Figure 3-2 Install the casters
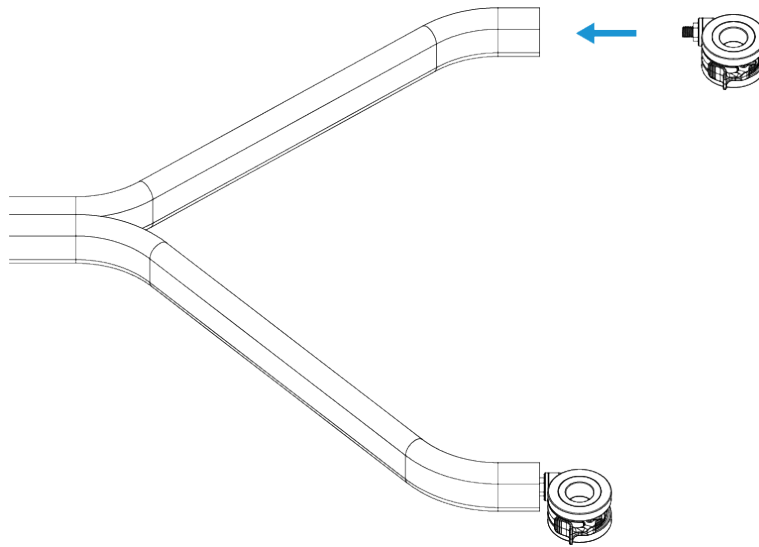
Step 2   Screw 2 M8×16 screws into the side of the 2 Y-shaped vertical poles to stand the moving
bracket upright.

Do not tighten the screws for later adjustment of the columns.
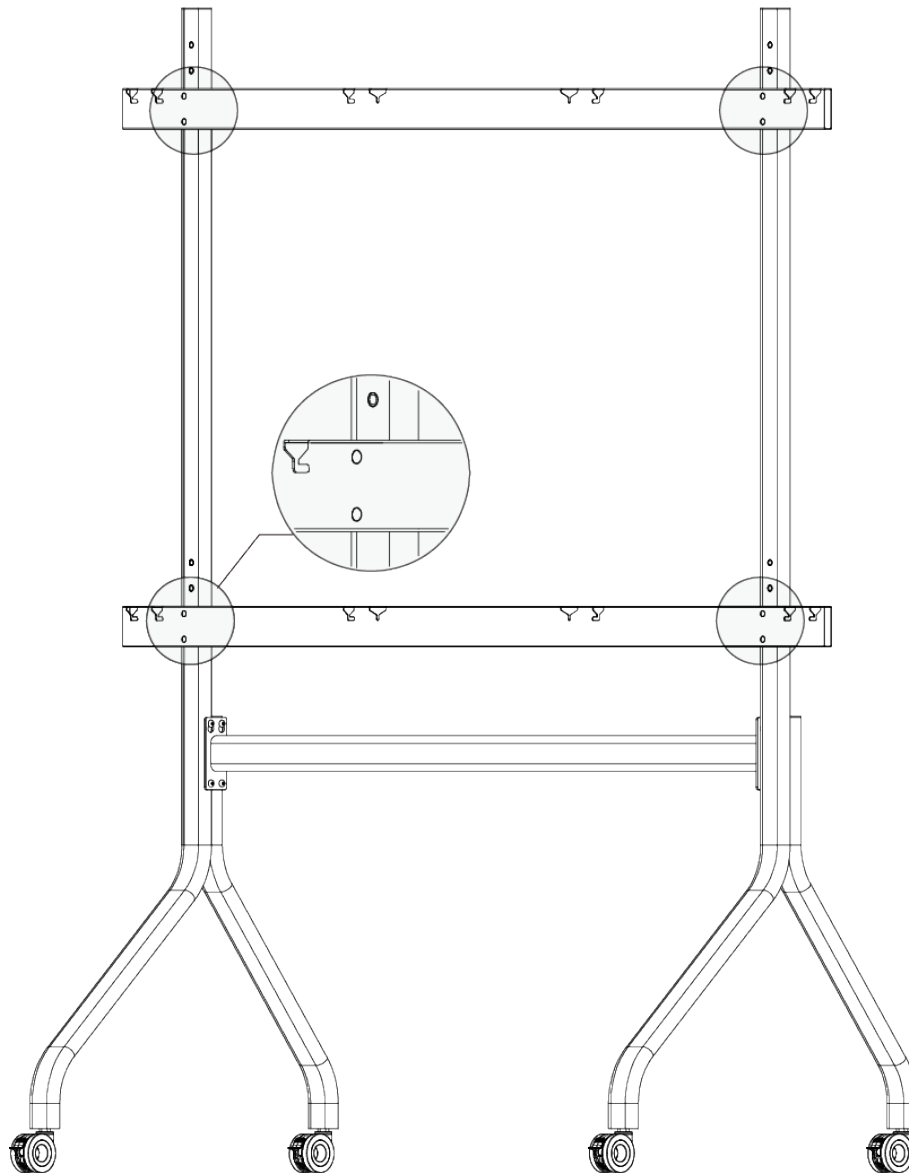
Figure 3-3 Install the strengthen pole
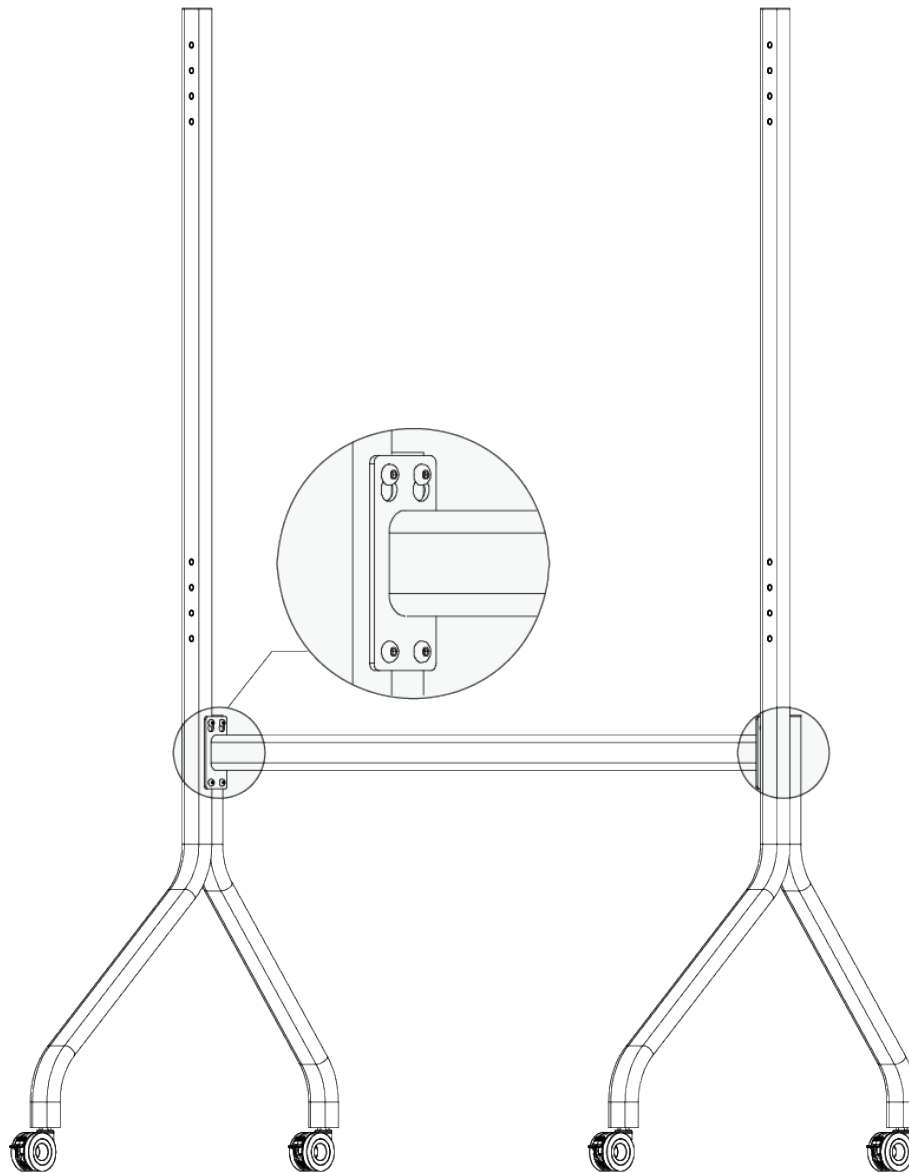
Step 3   Attach the 2 horizontal poles to the Y-shaped vertical poles with M8×45 screws.

Make sure that the mounting holes in the upper and lower part of the 2 horizontal poles align. The holes will be used to adjust the height of the screen.

Figure 3-4 Adjust the horizontal poles

Step 4   Use the 4 mm Allen wrench to tighten all the screws.

3.3.2 Installing Wall Mount Bracket

The wall mount bracket comes with 2 horizontal poles and 12 expansion screws (ST6.3).

Procedure

Step 1   Confirm and mark the installation position on the wall through tape measure or laser level.

Step 2   Drill holes on the marked positions with diameter of 10 mm and depth of 75 mm.

Step 3   Use expansion screws to install the horizontal poles on the wall. Make them level and justified.

Strictly confirm to the dimensions below.

Figure 3-5 Dimensions of wall mount bracket installation (mm [inch])
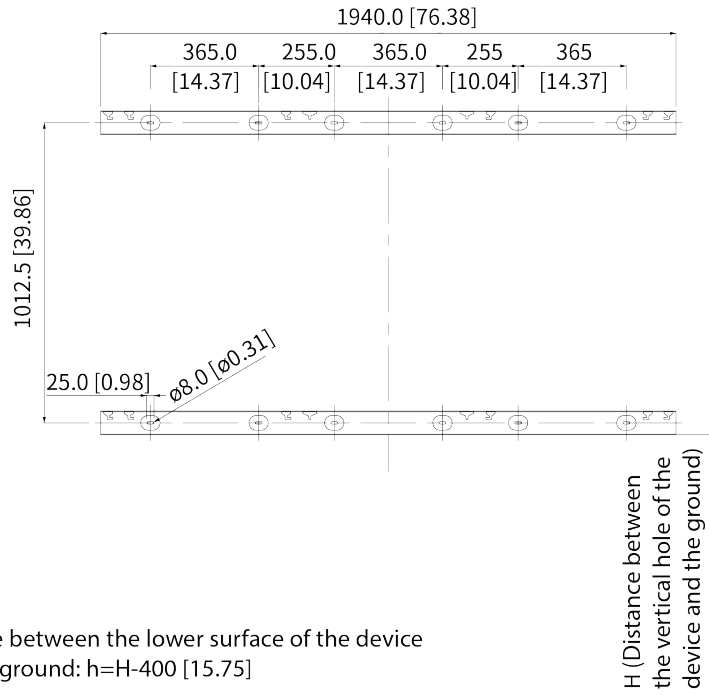
When equipped with a camera or OPS, it is necessary to reserve an area on the wall in advance.
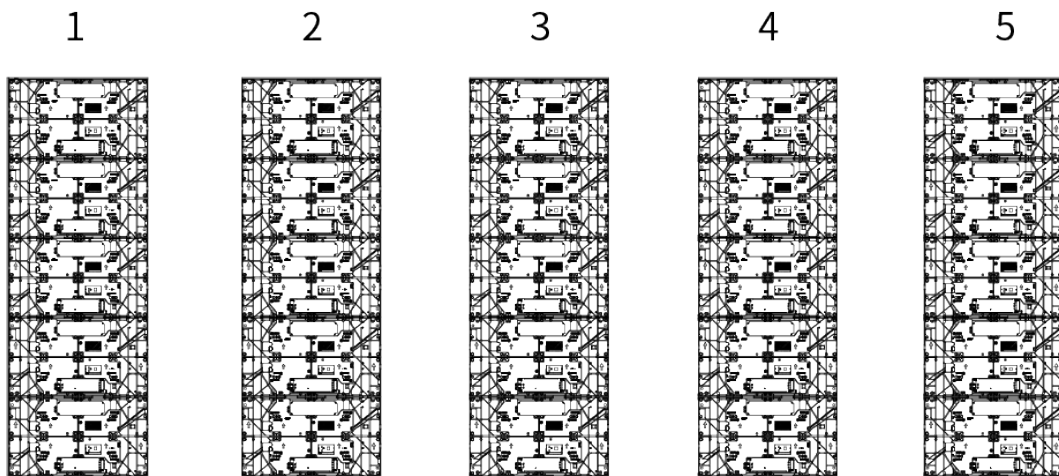
Figure 3-6 Reserve an area (mm [inch])
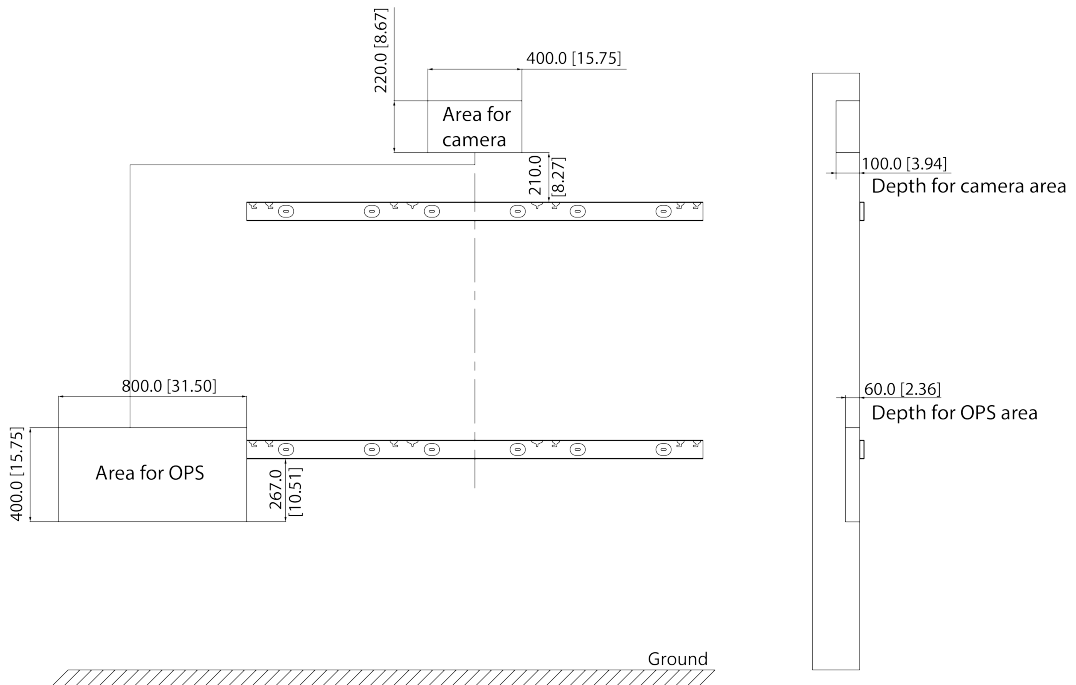
3.4 Column Installation

You can install the device on the mobile bracket or wall. Here we use the installation on the mobile bracket as an example.

The 5 columns are located in the same column. The edging strips have been pre-installed. Each column is marked with serial numbers from 1 to 5.

Figure 3-7 Pre-installed columns

The wall mounting screws were pre-installed in the specific mounting holes on the back of the columns, and the pre-installed wall mounting screws were tightened. Before attaching the column to the bracket, unscrew the wall mounting screws as shown in the image below.
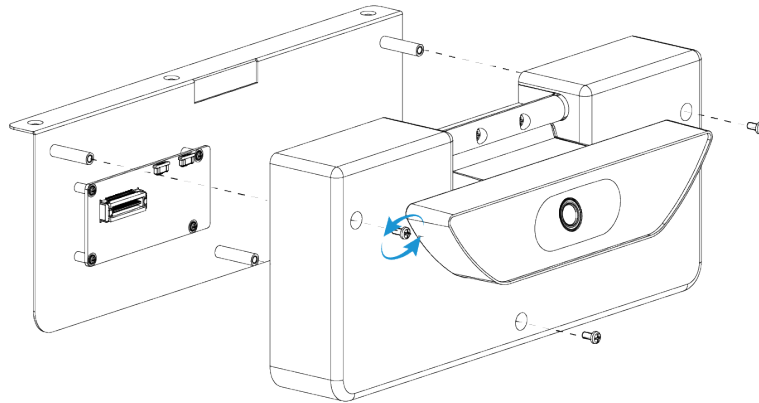
Figure 3-8 Loosen the screws
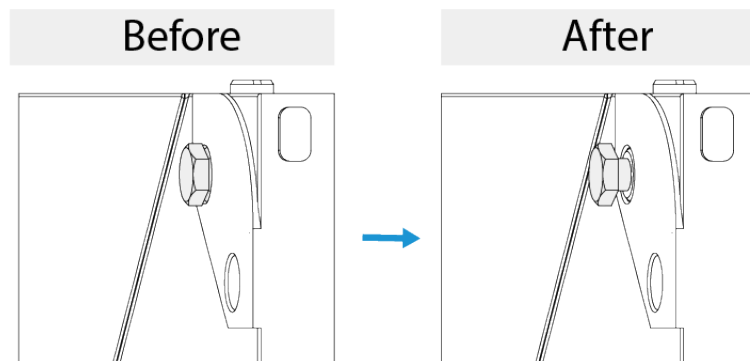
3.4.1 Installing the Middle Column

Procedure

Step 1　　Remove the screws and bracket from the camera module.

Figure 3-9 Remove the bracket

Step 2   Pass the HDMI and Type-C cables of the camera through the edging strip of the middle column and the threading hole of the bracket. Connect the cables to the adapter board, and then fix the sheet metal bracket to the top of the edging strip.
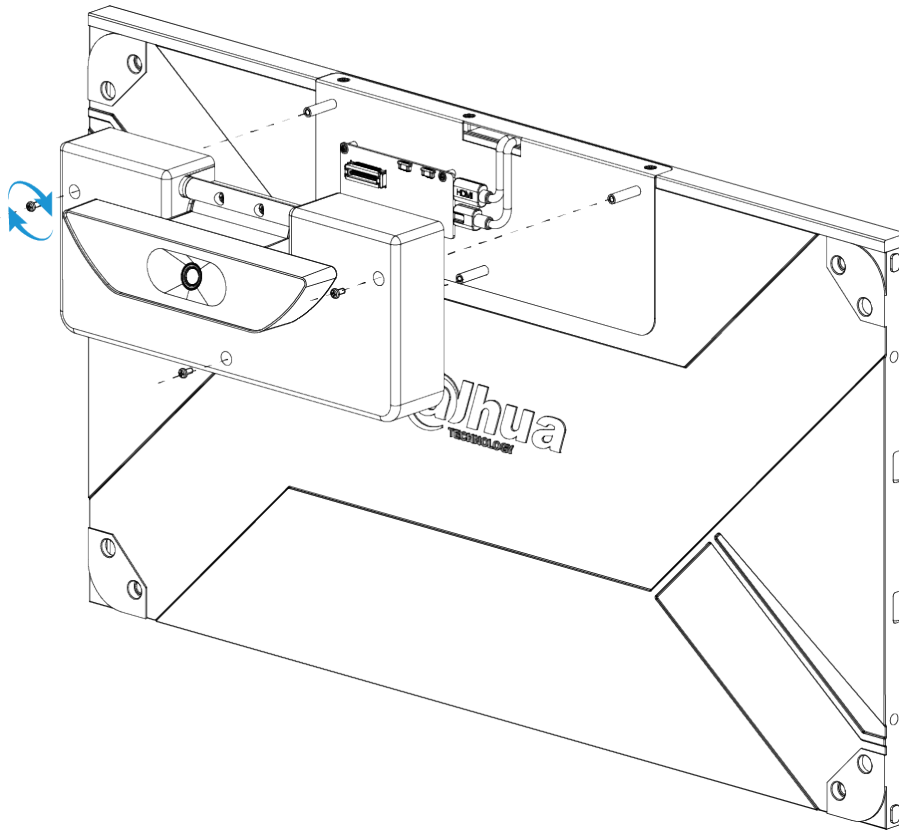
Connect the Type-C cable as below. Do not install the cable facing the wrong direction.

Figure 3-10 Fix the sheet metal bracket

The groove is facing outward
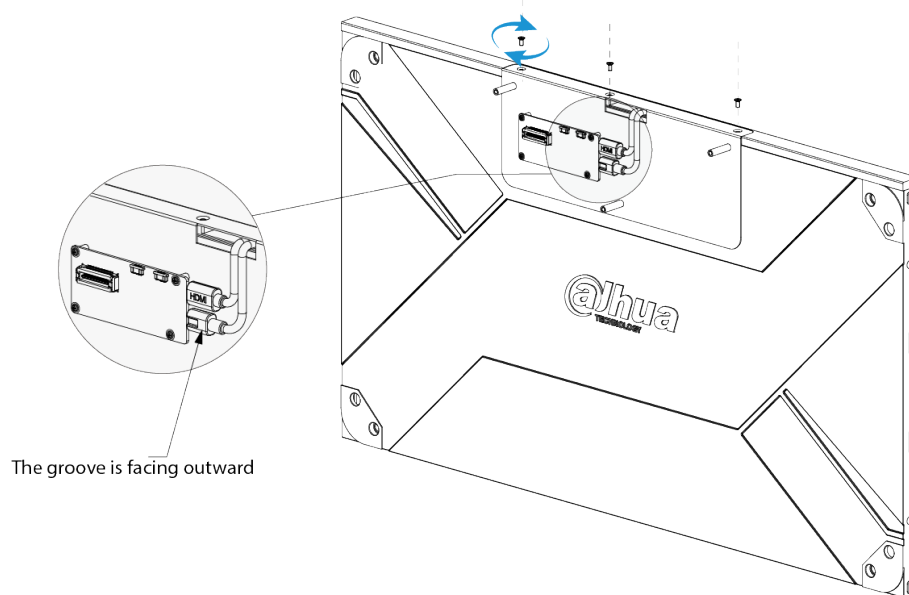
Step 3   Install the camera module on the sheet metal bracket of the camera, and then tighten it with the screws removed in step 1.

Figure 3-11 Fix the camera module

Step 4   Install the middle column where the camera module is already installed to the middle hole of the bracket by loosening the wall mounting screws.

Figure 3-12 Fix the middle column
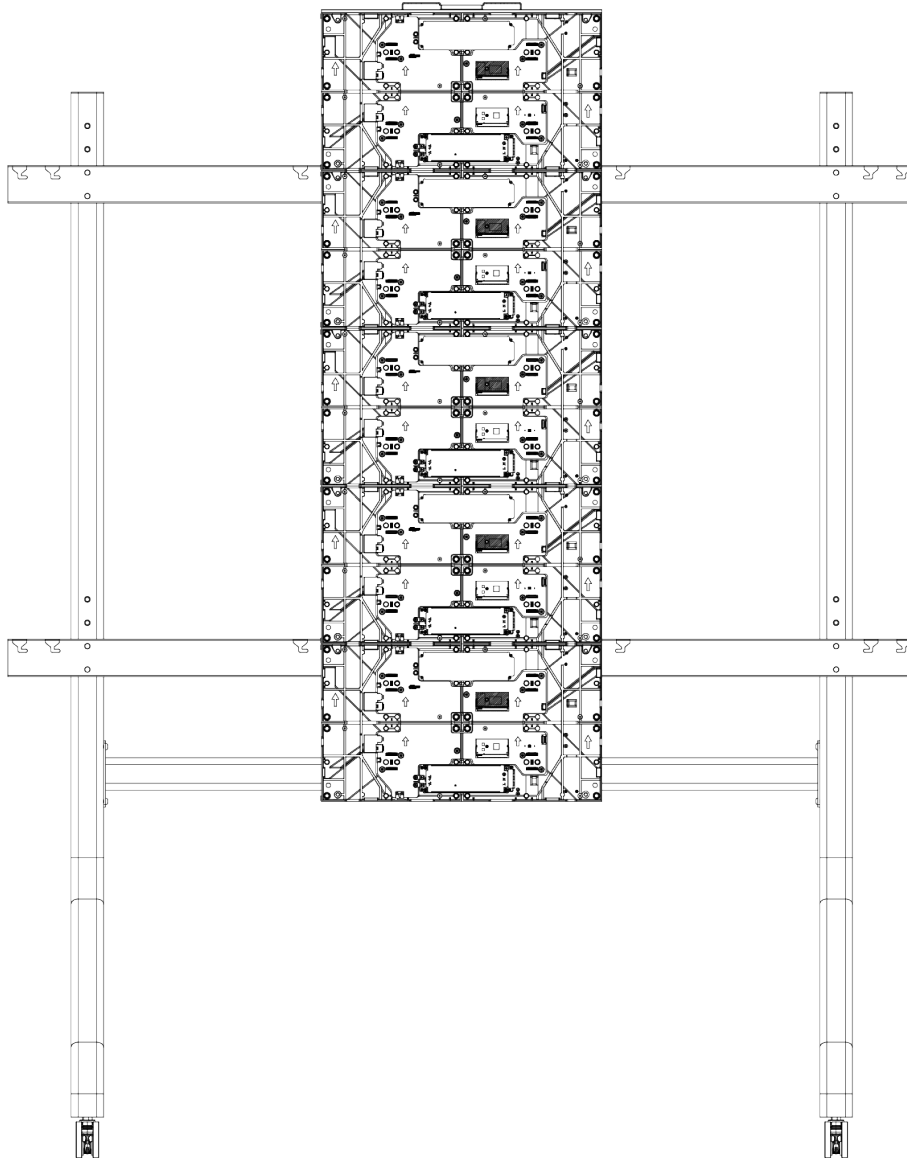
3.4.2 Installing Other Columns

Procedure

Step 1   With the middle column in the center, install the other columns on both sides. After installation, slide them to the middle to ensure that there is no gap between columns, and then use the screws to lock the columns.
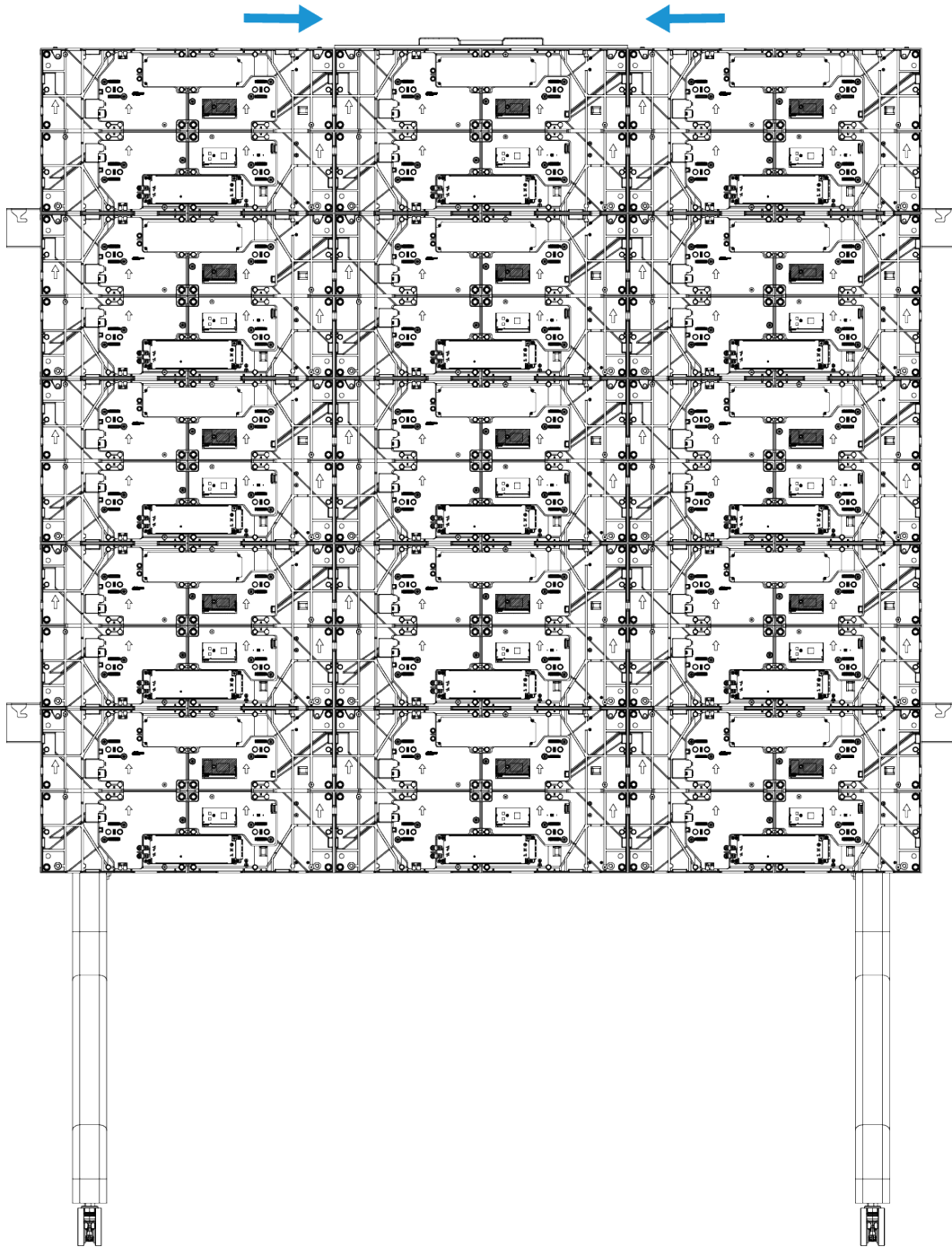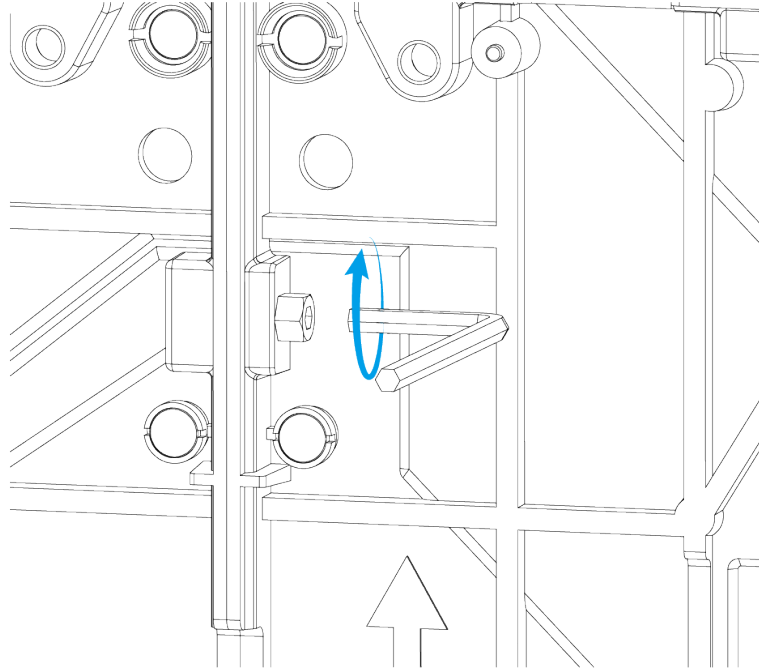
Figure 3-13 Install other columns

Figure 3-14 Lock the screws

Step 2   After all the columns are installed, use a slotted screwdriver to turn the wall mounting screws counterclockwise from the front of the column to tighten them.

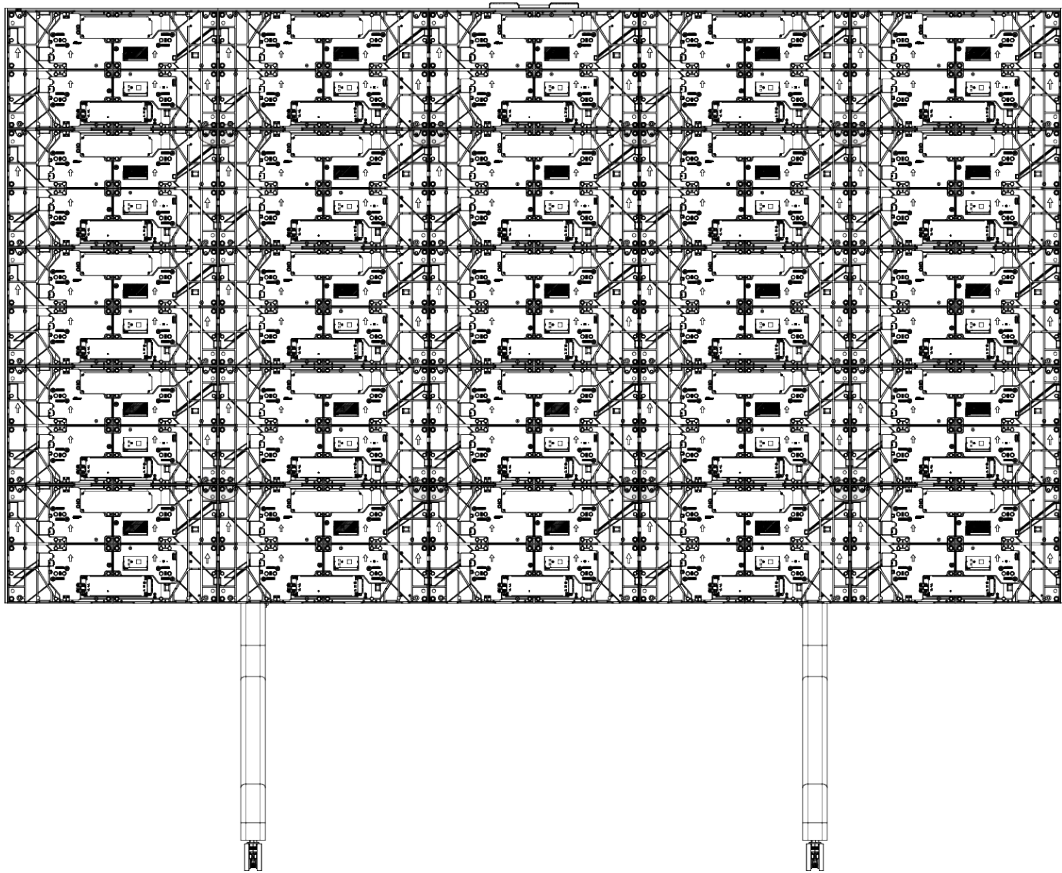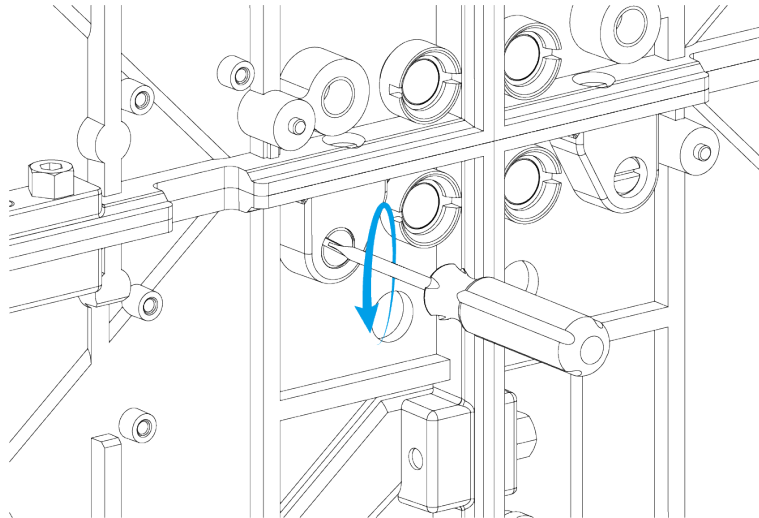Figure 3-15 Tighten the wall mounting screws (1)
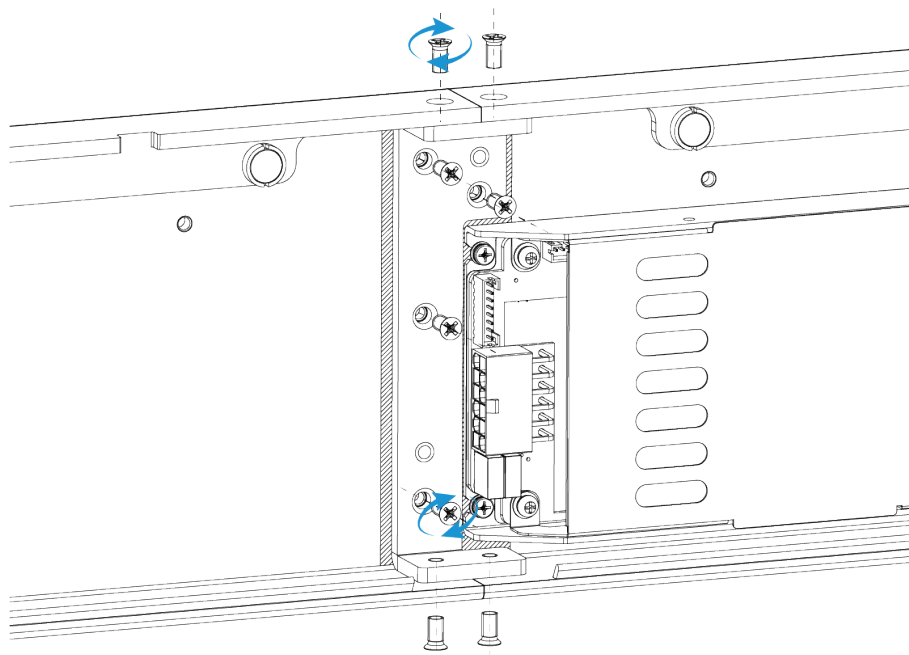
Figure 3-16 Tighten the wall mounting screws (2)

3.5 Transverse Beam Installation

Procedure

Step 1   Unfold the beam until it is flat and attach the beam connector.

Figure 3-17 Lock the transverse beam

Step 2   Align the beam to the bottom of the column and attach it with the M5×12 screws.
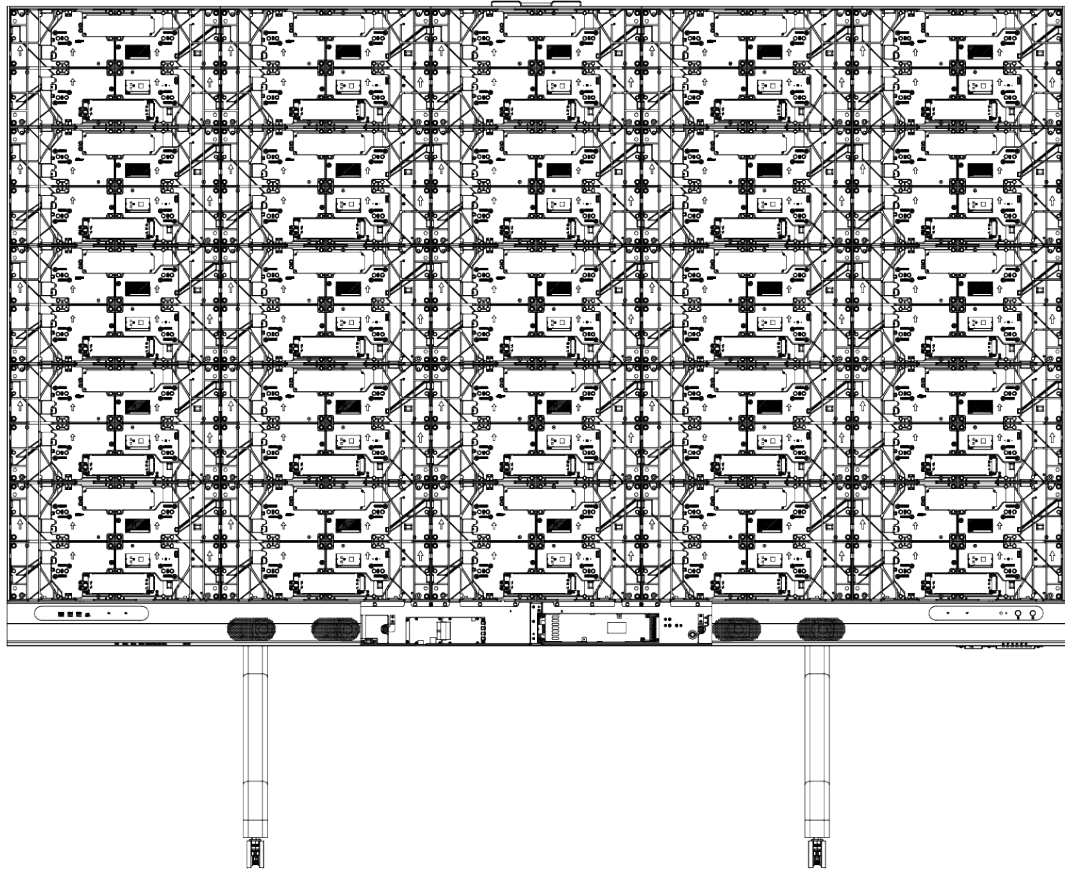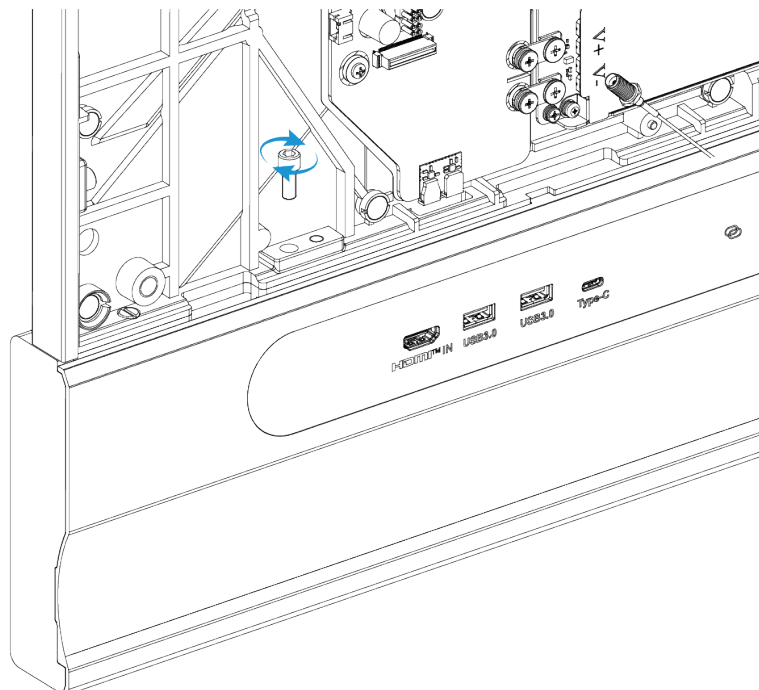
Figure 3-18 Align the beam

Figure 3-19 Tighten the screws

<u>Step 3</u> Connect the power cables.

Figure 3-20 Connect the power cables
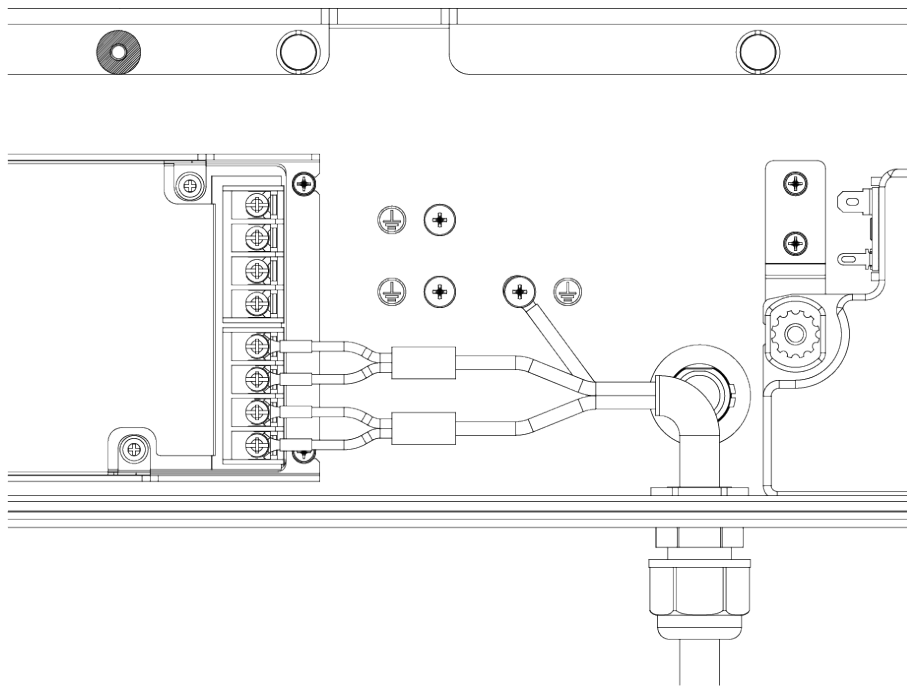
Step 4   Install the safety rope and connect the FFC connector to the front cover.

Step 5   Connect the other end of the HDMI and Type-C cables of the camera to the motherboard.

Connect the Type-C cable as below. Do not install the cable facing the wrong direction.

Figure 3-21 Connect the cable

The convex is facing outward
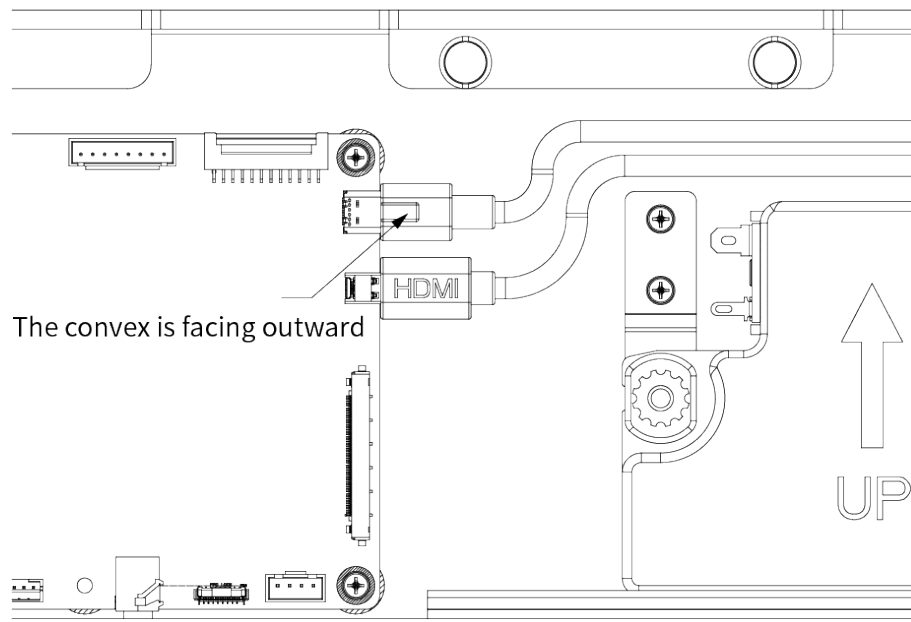
Step 6   Connect the transverse beam to the power cables and network cable of the columns, and then close the front cover.

3.6 OPS Bracket Installation

Procedure

Step 1   Remove the cover of the OPS cable outlet hole, install the FFC connector which connect to the OPS on the motherboard, and then pass the FFC connector and power cable through the cable outlet hole.

Step 2   Remove the OPS bracket and the top cover, pass the FFC connector and power cable through the OPS bracket, and then secure the OPS bracket to the bottom of the column in the lower-right corner using the preinstalled screws.

Figure 3-22 Install the OPS bracket
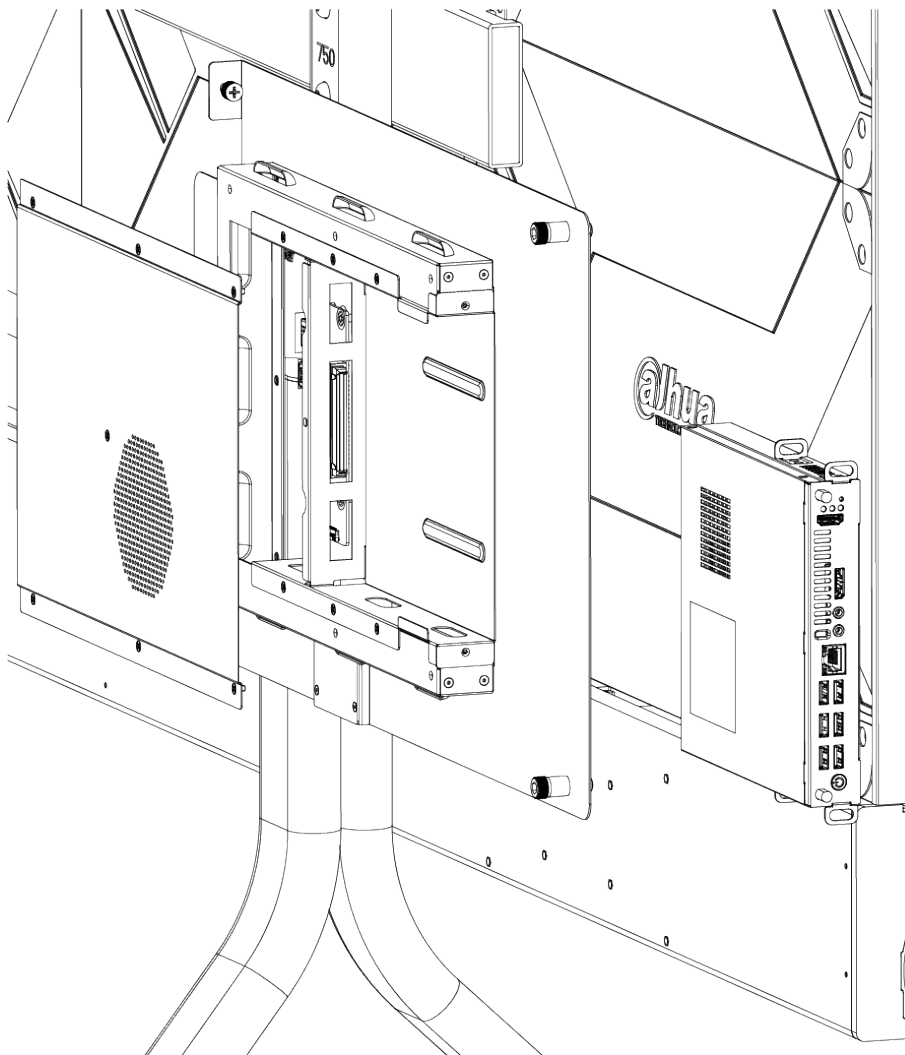
Step 3   Connect the FFC connector and power cable to their corresponding ports.

Step 4   Reattach the OPS cover, and then install the OPS as needed.

4 Appearance and Structure

Figure 4-1 Appearance
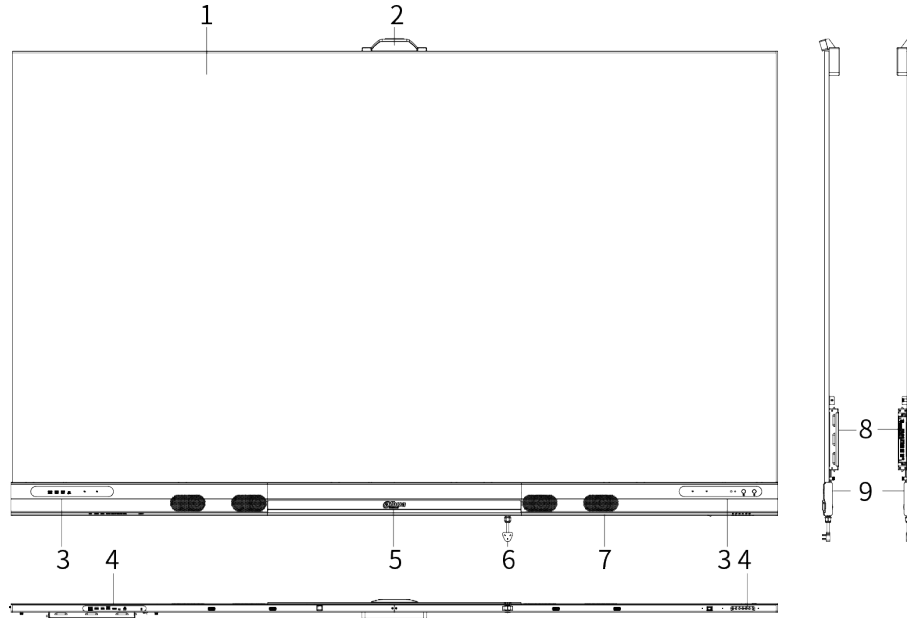
Table 4-1 Description of appearance

No.	Description
1	LED.
2	Camera.
3	Front panel.
4	Bottom panel.
5	Indicator light. The light is red when the Device is on standby and blue when the Device is in normal use. 📖 You can set the display mode of the indicator light as needed.
6	Power input port. Inputs 100–240 VAC power.
7	Speaker. Plays multi-media sound.
8	OPS module. Switches between Android and Windows system. 📖 OPS module does not come with delivery. Please purchase it as needed.
9	Transverse beam, which contains the main control modules.

Front Panel

Figure 4-2 Front panel (1)

Figure 4-3 Front panel (2)

Table 4-2 Front panel description

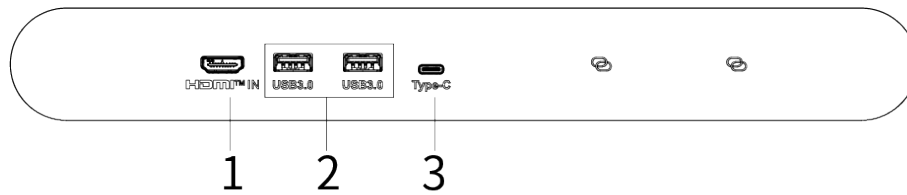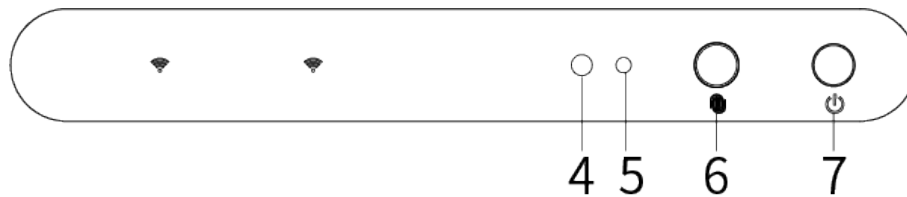| No.	Description
1	HDMI IN. HD audio and video signal input port. Connects to the computer, set-top box, and other video devices with HDMI output ports.
2	USB 3.0. Connects to USB devices such as mobile hard disk, USB flash drive, USB keyboard, and USB mouse. They are accessible both from the built-in Android system and the optional OPS computer module. USB 3.0 Type A, supports 5V 1A (MAX).
3	Type-C. Connect a laptop or other devices to the Device through the Type-C port for screen sharing and other operations. Type-C supports 5V 3A, 9V 3A, 15V 3A and 20V 3A (MAX).
4	IR sensor. Receives signals from the remote control.
5	Light sensor. The Device recognizes the ambient brightness through the light sensor and automatically adjusts the backlight brightness according to the ambient brightness.
6	Fingerprint reader. After adding your fingerprint, you can unlock the Device through fingerprint recognition.
7	Power button. Turn on or turn off the screen.

Bottom Panel

Figure 4-4 Bottom panel (1)
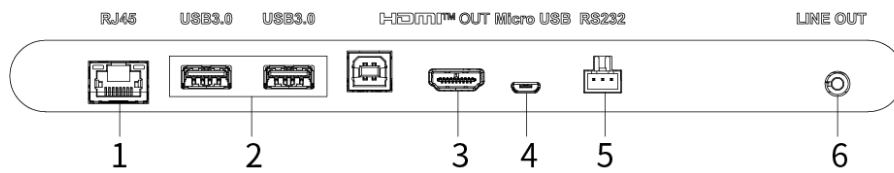
Figure 4-5 Bottom panel (2)
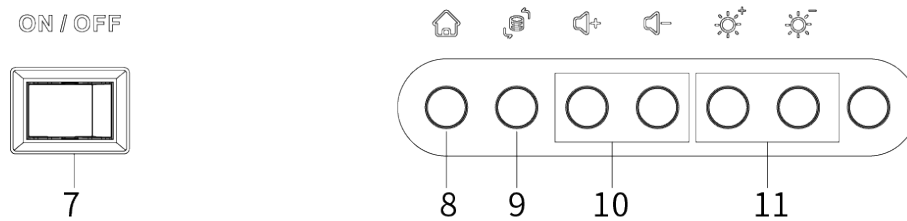
Table 4-3 Bottom panel description

No.	Description
1	Network port. Connects to network cable to access network.
2	USB 3.0 port. Connects to USB devices such as mobile hard disk, USB flash drive, USB keyboard, and USB mouse. They are accessible both from the built-in Android system and the optional OPS computer module.
3	HDMI OUT. HD audio and video signal output port. Transmits uncompressed HD video and multi-channel audio data.
4	Micro USB. Used for debugging Android system.
5	RS-232 port. Transmits data between devices. You can connect to central control devices with RS-232 port.
6	LINE OUT. An audio output port that connects to the earphone or speaker.
7	Power switch. Turn on or turn off the power supply of the Device.
8	Go back to the home screen.
9	Select signal sources.
10	Adjust the column.
11	Adjust the brightness of the screen.

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 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:

Account Management

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.

2. **Change passwords periodically**

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

3. **Allocate accounts and permissions appropriately**

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

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.

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.

Service Configuration

1. **Enable HTTPS**

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

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.

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.

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.

Network Configuration

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.

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. **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.

Security Auditing

1. **Check online users**

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

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.

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.

Software Security

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.

2. **5.2 Update client software in time**

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

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