Mobile Stand B100 for Data Collection Station

Quick Start Guide

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V1.0.0

Foreword

General

This manual introduces the functions and operations of the mobile stand B100 for the data collection station (hereinafter referred to as "the stand"). Read carefully before using the device, and keep the manual safe for future reference. Read carefully before using the stand, and keep the manual safe 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.	March 2022

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 stand, hazard prevention, and prevention of property damage. Read carefully before using the stand, and comply with the guidelines when using it. Read carefully before using the stand, and comply with the guidelines when using it.

Installation Requirements

- Improper installation might cause harm to you or the device.
- If you are not sure how to install the stand, entrust the installation to professionals.
- If any part or component of the stand is damaged, do not install the stand.
- The stand is designed to support the data collection station. Do not use the stand for other purposes.
- Net weight: 55 kg; load bearing capacity: 100 kg. To ensure safety, do not use the stand to support a load exceeding its bearing capacity.
- If you are unaware of the load bearing capacity, do not install the stand.

Table of Contents

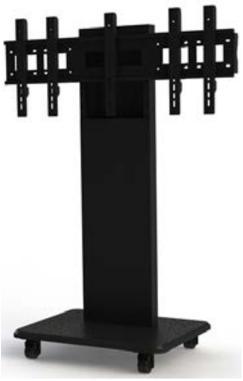
1 Introduction

1.1 Overview

The device is a mobile stand for the data collection station. It is easy to install in projects and applicable for uses in scenes such as public security, traffic police, electricity, energy, industrial parks and exhibitions.

1.2 Appearance

Figure 1-1 Appearance



1.3 Components

Figure 1-2 Base and vertical bracket

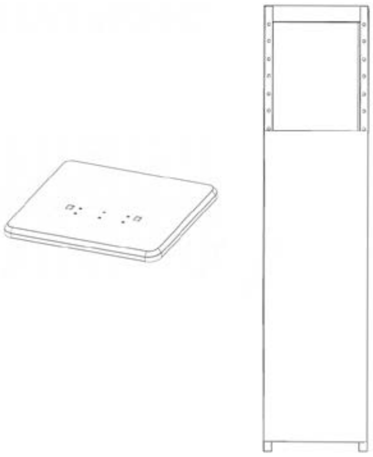


Figure 1-3 Cross beam and connector

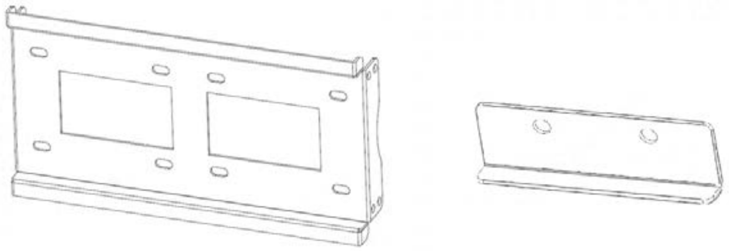
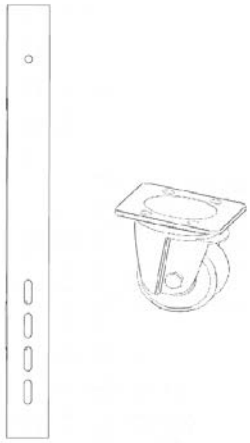


Figure 1-4 Wall-mounting bracket and swivel coaster



1.4 Accessories

Table 1-1 Accessory list

Accessory	Dimensions	Quantity	Description
Screw	M5 × 110 mm (partially threaded)	3	Fix the screws at the bottom of the wall-mounting bracket between the control module and the last data collection module.
	Inner hexagon M8 × 20	36	Use the screws to secure: ● Coasters. ● Base and vertical bracket. ● Cross beam and connector.
	Outer hexagon M8 × 25	26	Secure cross beam and wall-mounting bracket.
Gasket	M8	56	Use the gaskets together with M8 screws.
Nut	M8 (flange)	26	Use the nuts together with M8 screws.
Wrench	Inner hexagon wrench (M8)	1	Installation tool.
	Outer hexagon wrench (M5)	1	
	Inner and outer hexagon wrench	1	

2 Installation

2.1 Securing Coasters

Use M8 × 20 mm screws to secure the four coasters at the corners of the base.

Figure 2-1 Secure coasters (1)

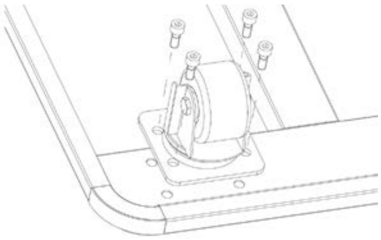


Figure 2-2 Secure coasters (2)

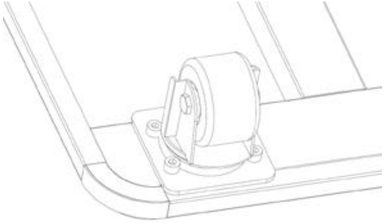
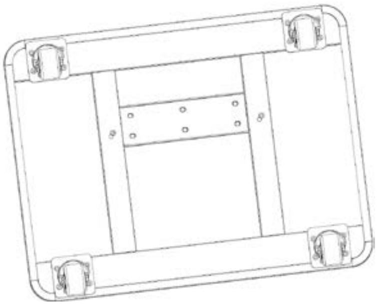


Figure 2-3 Secure coasters (3)



2.2 Securing Bracket

Secure the vertical bracket to the base and then use eight M8 × 20 mm screws to fix the base.

Figure 2-4 Secure bracket (1)

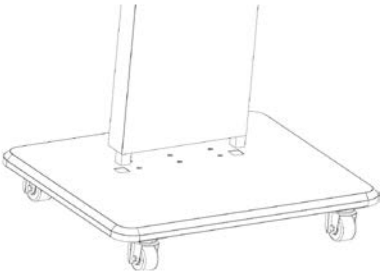


Figure 2-5 Secure bracket (2)

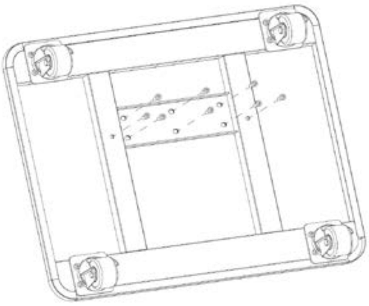


Figure 2-6 Secure bracket (3)

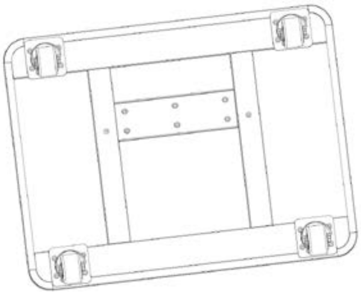
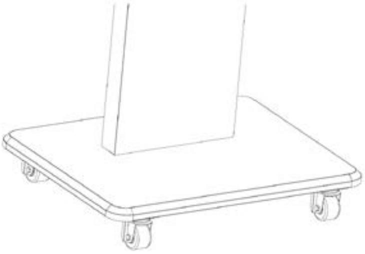


Figure 2-7 Secure bracket (4)



2.3 Connecting Cross Beam

The number of cross beams is determined by the number of connected control and data collection modules.

Table 2-1 Number of cross beams

Number of control modules	Number of data collection modules	Number of cross beams
1	1	1
1	2	2
1	3 or 4	3

Figure 2-8 Connect cross beam (1)

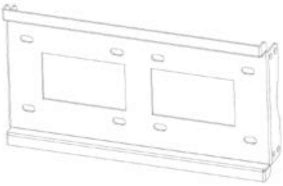


Figure 2-9 Connect cross beam (2)

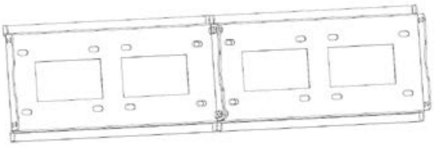


Figure 2-10 Connect cross beam (3)

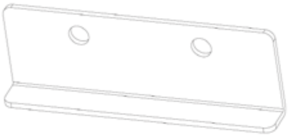
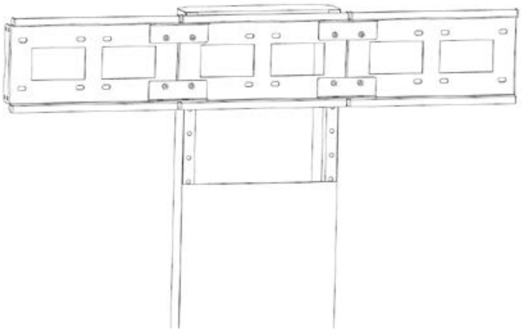


Figure 2-11 Connect cross beam (4)



2.4 Securing Wall-mounting Bracket

Use M8 screws to secure the wall-mounting bracket to the control module and then secure the bracket with M8 × 25 outer hexagon nuts.

Figure 2-12 Secure wall-mounting bracket (1)

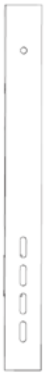


Figure 2-13 Secure wall-mounting bracket (2)

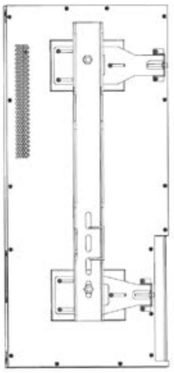
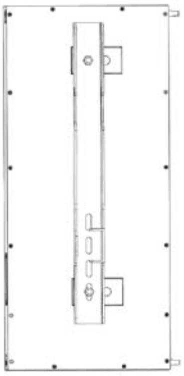


Figure 2-14 Secure wall-mounting bracket (3)



2.5 Appearance after Installation

2.5.1 1 Control Module + 1 Data Collection Module

Step 1 Prepare one cross beam.

Step 2 Install the control module first, and then the data collection module.

Step 3 Connect the two modules and then tighten the screws at the upper and lower positions.

Step 4 Install M5 screws at the bottoms of the modules.

Figure 2-15 1 control module + 1 data collection module (1)

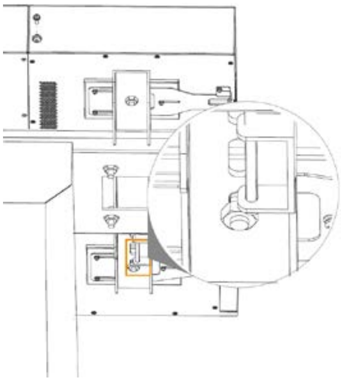
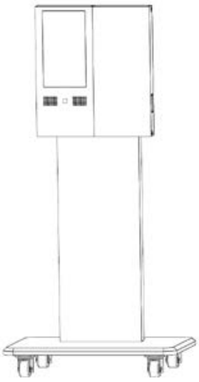


Figure 2-16 1 control module + 1 data collection module (2)



2.5.2 1 Control Module + 2 Data Collection Modules

Step 1 Prepare two cross beams.

Step 2 Install one data collection module in the middle, and then install other modules on two sides.

Step 3 Connect the three modules and then tighten the screws at the upper and lower positions.

Step 4 Install M5 screws at the bottoms of the leftmost and rightmost modules.

Figure 2-17 1 control module + 2 data collection modules (1)

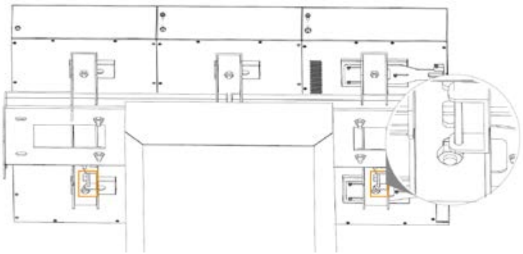
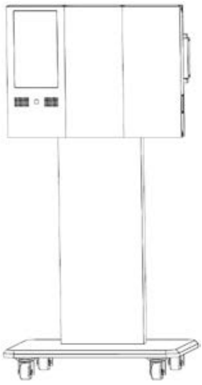


Figure 2-18 1 control module + 2 data collection modules (2)



2.5.3 1 Control Module + 3 Data Collection Modules

Step 1 Prepare three cross beams.

Step 2 Install one data collection module in the middle, and then install other modules on two sides.

Step 3 Connect the four modules, and then tighten the screws at the upper and lower positions.

Step 4 Install M5 screws at the bottoms of the leftmost and rightmost modules.

Figure 2-19 1 control module + 3 data collection modules (1)

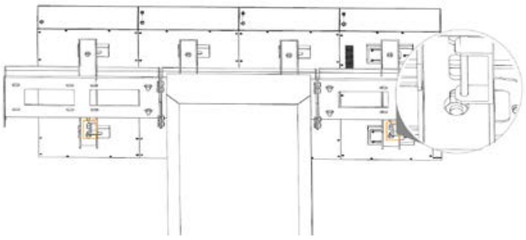
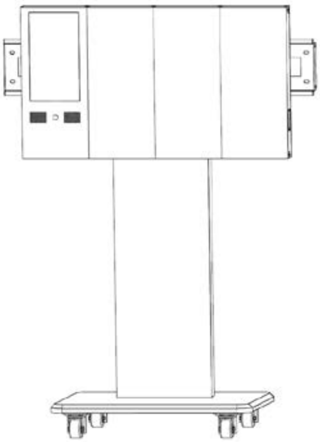


Figure 2-20 1 control module + 3 data collection modules (2)



2.5.4 1 Control Module + 4 Data Collection Modules

Step 1 Prepare three cross beams.

Step 2 Install the modules from left to right.

Step 3 Connect the five modules, and then tighten the screws at the upper and lower positions.

Step 4 Install M5 screws at the bottoms of the leftmost and rightmost modules.

Figure 2-21 1 control module + 4 data collection modules (1)

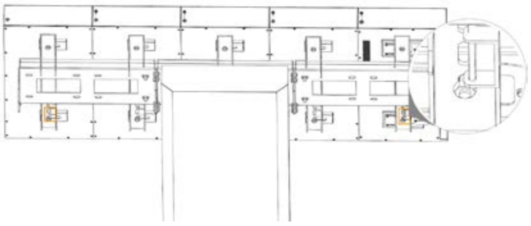
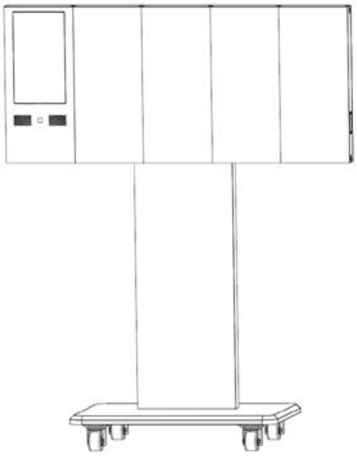


Figure 2-22 1 control module + 4 data collection modules (2)



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 SAFER SOCIETY AND SMARTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address: No.1199 Bin’an Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053
Email: overseas@dahuatech.com | Fax: +86-571-87688815 | Tel: +86-571-87688883