



Docking Station

User's Manual



Foreword

General

This manual introduces the installation, functions and operations of the wireless bridge (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
 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.	December 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 device, hazard prevention, and prevention of property damage. Read carefully before using the device, and comply with the guidelines when using it.

Transportation Requirements



Transport the device under allowed humidity and temperature conditions.

Storage Requirements



Store the device under allowed humidity and temperature conditions.

Operation Requirements



WARNING

- Do not disassemble the device without professional instruction.
- Operate the device within the rated range of power input and output.
- Make sure the device is powered off before disassembling wires to avoid personal injury.



- Use the device under allowed humidity and temperature conditions.
- 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.

Maintenance Requirements



WARNING

- Power off the device before maintenance.
- Mark key components on the maintenance circuit diagram with warning signs.

Table of Contents

- ForewordI
- Important Safeguards and Warnings..... III
- 1 Introduction 1
- 2 Features..... 2
- 3 Device Structure..... 3
 - 3.1 Dimensions 3
 - 3.2 Structure 4
- 4 Packing List and Operation 5
 - 4.1 Packing List..... 5
 - 4.2 Temperature and Humidity 5
 - 4.3 Operation..... 5
- Appendix 1 Cybersecurity Recommendations..... 6

1 Introduction

This Type-C docking, with its multiple ports, allows connecting a host PC to monitors or devices with HDMI, USB3.0 ports, and also allows the host PC to get access to fast network with its Gigabit Ethernet port. Besides, the SD/MMC and Micro SD card slot help to access the external memory of the host PC and the Type-C port can charge for the host computer with 100 W power. Supports connecting to laptops, tablets, mobile phones, game consoles and other devices.

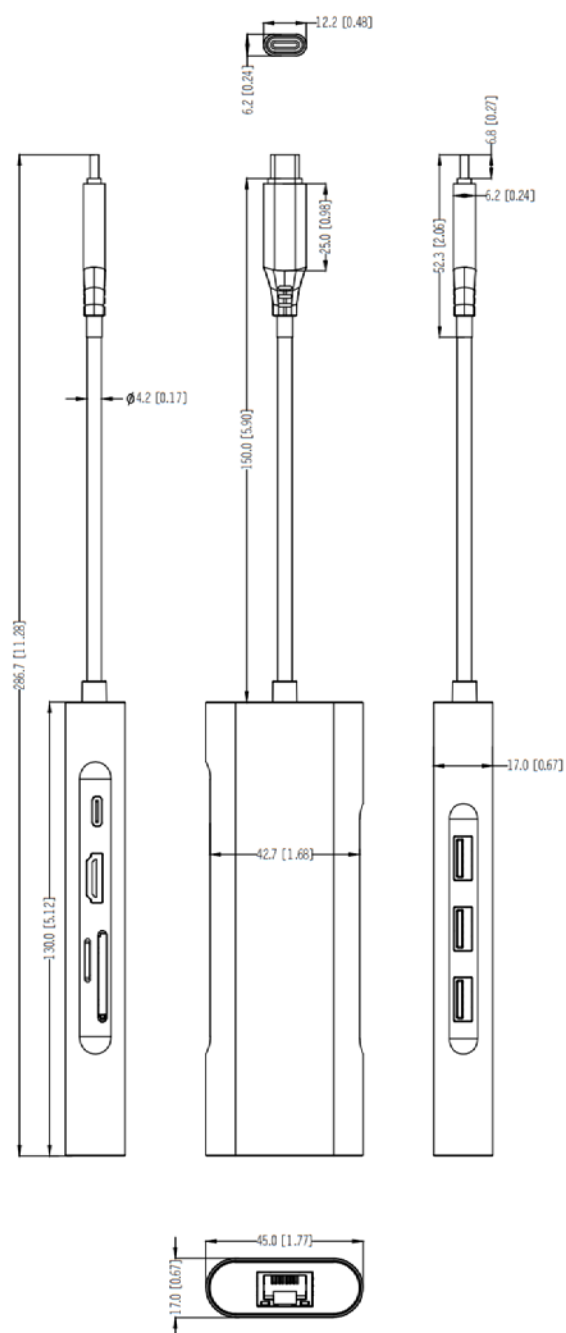
2 Features

- Support Type-C 3.1 input, USB3.0 output.
- Support HDMI port, USB3.0 port, Gigabit Ethernet, SD Card, Micro DS Card, Type-C interface.
- Support HDMI resolution up to 3840 x 2160 p@30 Hz.
- Support 10/100/1000 Mbps bandwidth.
- Support to access memory card.
- Type-C plug charging port is applicable to adaptors with Type-C ports of mainstream brands on the market.
- Multiple Type-A interfaces support plug and play, hot swap.
- Support SSD Secure Digital (Read speed up to 450 MB/s, write speed up to 450 MB/s).
- Support Multi Media Card (MMC) specification.
- Support Micro SD/SDHC/SDXC (up to 128 GB).
- Type-C plug supplies power up to 100 W (20 V, 5 A).
- Support the simultaneous use of SD card slot and Micro SD card slot, with a maximum transmission rate of 80 MB/s.

3 Device Structure

3.1 Dimensions

Figure 1-1 Dimensions (Unit: mm [inch])



3.2 Structure

Figure 1-2 Port and application scene

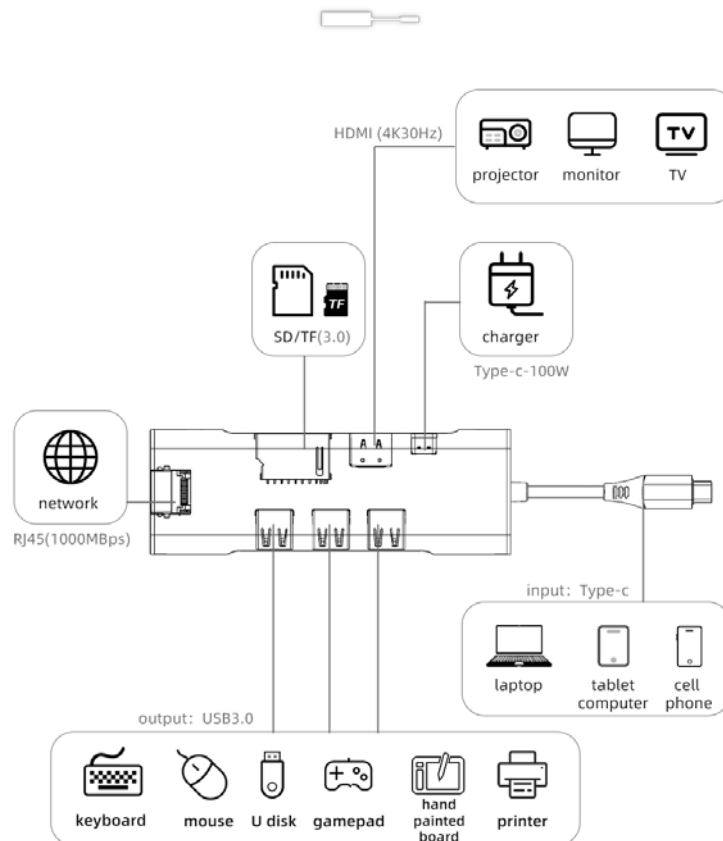


Table 1-1 Description of port

No.	Input/Output Connector	Name	Description
1	Input	Type-C connector	Connects to laptops, tablet computers, mobile phones, PS4/Switch and other devices.
2	Output	HDMI port	Resolution up to 3840 x 2160 p@30Hz.
3	Output	USB 3.0 port	Total output: 10 W (5V, 2A). One port supports max 7.5 W (5V, 1.5A). Other two ports share max 5 W (5V, 1A).
4	Output	RJ45	Bandwidth 10/100/1000 Mbps.
5	Output	SD card slot	The maximum read speed is 70 Mbps, and the maximum write speed is 90 Mbps.
6	Output	Micro SD card slot	Micro SD/SDHC (Up to 128 GB).
7	Output	Type-C plug for charging	Power supply for uplink equipment , Rated power is 100 W.

4 Packing List and Operation

4.1 Packing List

Before attempting to use this unit, please check the packaging and make sure the following items are contained in the shipping carton:

- Main unit x 1
- User Manual x 1

4.2 Temperature and Humidity

Table 1-2 Temperature and Humidity

Index	Value range
Working environment temperature	0 °C to +40 °C (32 °F to 104 °F)
Storage ambient temperature	-20 °C to +70 °C (-4 °F to 158 °F)
Working environment humidity (non-condensing)	10%—90% (RH)
Storage environment humidity (non-condensing)	10%—90% (RH)

4.3 Operation

- Connect the Type-C Plug of this product to notebooks, tablets, mobile phones, game consoles and other devices.
- Connect the three USB3.0 ports to three USB devices.
- Connect the HDMI port to HD display with one HDMI Cable.
- Connect RJ45 port of this product to Ethernet Router with an Ethernet interface device.
- Insert Micro SD and SD/MMC cards into the card reader ports.
- Connect the Type C charging port, it can charge for notebooks, tablets, mobile phones, game consoles and other devices, and support this adapter to work simultaneously.
- Support Plug and Play without installing drivers and settings, it does not require any configuration.



- When connecting the Type-C port of the adapter to device, the mouse to be connected to the USB 3.0 port might not work immediately, it might have seconds' delay, which is normal.
- When plugging in and out the PD Adapter, the connected USB devices will get disconnected flashily and then reconnect in a few seconds, so to prevent possible data loss or corruption, avoid disconnecting the PD Adapter from AC power while transferring data.
- When reading a large-capacity mobile hard disk, please connect the PD for power supplying.

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 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.

ENABLING A SAFER SOCIETY AND SMARTER 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