

|  |
| --- |
| **DSS OneBox** |
| **Quick Start Guide** |

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

# **Foreword**

Safety Instructions

The following signal words might appear in the manual.

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

Revision History

| **Version** | **Revision Content** | **Release Time** |
| --- | --- | --- |
| V1.0.0 | First release. | March, 2025 |

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**

Before using and operating this device, please read and observe the following precautions carefully to avoid dangerous or illegal operations.

Transportation Requirements

Before moving the product, please unplug the AC power cord from power socket.

Installation Requirements

Before connecting or disconnecting any signal cables, make sure that all the power cords are unplugged in advance.

Operation Requirements

● We do not recommend using the device continuously for a long time in industrial PC scenarios (such as environment with high temperature, humidity, vibration and strong electromagnetic interference).

● Please carefully read the user manual before using the product.

● To avoid damages caused by frequent start up and shutdown, please wait for at least 30 seconds before restarting the product.

● All the operations such as removal or installation shall be implemented on the electrostatic discharge (ESD) worktable, because some precision components are sensitive to electrostatic discharge.

● If there is no ESD worktable, please take the following measures to minimize possible damages from electrostatic discharge: Wear an anti-static wrist strap during operation; always touch the metal chassis of frame of the corresponding products before removal or installation of any components.

● The normal working temperature for the product is 0 °C (32 °F) to 40 °C (104 °F), and the normal working humidity is 10%–90% (RH).

● Assure good cooling and ventilation.

● There are heating hole on back cover, do not spray water to it or use damp cloth for cleaning.

Maintenance Requirements

Please call professional personnel for maintenance service.

**Table of Contents**

[**Foreword** I](#_Toc198213346)

[**Important Safeguards and Warnings** III](#_Toc198213347)

[**1 Accessories** 1](#_Toc198213348)

[**2 Appearance** 2](#_Toc198213349)

[**3 Installing the Device** 3](#_Toc198213350)

[**4 Connecting and Starting the Device** 4](#_Toc198213351)

[**5 Installing Hard Drive (Optional)** 5](#_Toc198213352)

[**Appendix 1 Security Commitment and Recommendation** 7](#_Toc198213353)

# **1 Accessories**

● 1 power cord.

● 1 power adapter.

● 1 HDMI cable.

● 1 bracket.

● 1 screw set.

# **2 Appearance**

Figure 2-1 Appearance

Table 2-1 Appearance description

| **No.** | **Description** |
| --- | --- |
| 1 | CLR CMOS (pinhole).Used for restoring BIOS settings. Press and hold the button for 3 seconds, and the configuration takes effect. |
| 2 | 3.0.Connects to USB 3.0 or USB 2.0 devices, such as USB drive, USB keyboard, and USB mouse. |
| 3 | C-OUT.Supports DP OUT, USB3.2 reversible insertion, 5 V/3 A external power supply. |
| 4 | OS REC (pinhole).System restore button. When the device is off, press and hold the button, and press the power button, until the boot screen appears. The configuration takes effect.After one-click restoration, the system will be restored to default settings, but the platform data will be kept. Please be advised. |
| 5 | Power button. |
| 6 | 2.0.Connects to USB 2.0 devices, such as USB drive, USB keyboard, and USB mouse. |
| 7 | LAN.2.5 Gbps network interface, connects to Ethernet. |
| 8 | HDMI OUT.High-definition multimedia signal output interface, connects to display devices with HDMI input. |
| 9 | AUDIO OUT.3.5 mm headphone or microphone jack. |
| 10 | DC IN.2.5 mm, 19 V power port. |

# **3 Installing the Device**

You can use the device by placing it on a desktop. If you want to install it behind a display device (such as a monitor), take the following steps.

Step 1 Attach the step screws to the VESA holes of the display device.

Figure 3-1 Attach the step screws

Step 2 Attach the wall mount bracket to the device.

Figure 3-2 Attach the wall mount bracket to the device

Step 3 Hang the device through the lug hole on the display device that is fixed with pre-locked step screws.

Figure 3-3 Hang the device


# **4 Connecting and Starting the Device**

Step 1 Complete the device connection according to the illustration.

Connect the display device to the HDMI OUT or C-OUT interface of OneBox. The HDMI cable is included in the package. For the cable for connecting to the C-OUT interface, you need to purchase it separately.

Figure 4-1 Connection illustration

Step 2 Press the power button to start the device.

Figure 4-2 Start the device


# **5 Installing Hard Drive (Optional)**

Step 1 Confirm the contents of the screw package.

Table 5-1 Screw package description

| **Name** | **Image** | **Quantity** |
| --- | --- | --- |
| CM2 × 3.5 black screw |  | 2 |
| CM2 × 3 silver screw |  | 1 |
| Staircase screws |  | 2 |
| Hexagonal pillar |  | 1 |
| Antenna latch |  | 1 |

Step 2 Invert the device.

Figure 5-1 Invert the device

Step 3 Remove the device casing.

Figure 5-2 Remove the casing

Step 4 Disassemble the built-in latch and screws from the device.

Figure 5-3 Dissassemble the latch and screws

Step 5 Take out the materials from the screw package, replace and install them as shown below.

Step 6 Install the new SSD, and then securely fasten the screws.

Figure 5-4 Install SSD

Step 7 Reassemble the bottom cover of the device.

Figure 5-5 Reassemble the bottom cover


# **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 Allowlist**

It is recommended that you turn on the allowlist function, and only allow IP in the allowlist to access the device. Therefore, please be sure to add your computer IP address and supporting device IP address to the allowlist.

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. **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).

