



DHI-SP-PIXX

User's Manual



Foreword

General

This document provides a detailed introduction to the appearance, dimensions, and installation of the product. Please read it carefully before using the product, and after reading it, please keep the document properly 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	April 2024

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



Please transport the equipment within the allowed humidity ($\leq 95\%$ RH) and temperature range ($-20\text{ }^{\circ}\text{C}$ to $+70\text{ }^{\circ}\text{C}$).

Storage requirements



Please store the equipment within the allowed humidity ($\leq 95\%$ RH) and temperature range ($-20\text{ }^{\circ}\text{C}$ to $+70\text{ }^{\circ}\text{C}$).

Installation requirements



WARNING

- To avoid electric shock to the human body or damage to the product, please turn off the AC power supply before connecting (non plug and play) devices each time.
- Avoid using this product in environments with high or low temperatures (operating temperature: $-10\text{ }^{\circ}\text{C}$ to $+50\text{ }^{\circ}\text{C}$; humidity: 10% to 95%; storage temperature: $-20\text{ }^{\circ}\text{C}$ to $+70\text{ }^{\circ}\text{C}$).
- Do not subject the product to strong impact or vibration, as it may cause equipment malfunction or damage.
- When moving the product, be sure to unplug the AC power supply.



Do not install the device in a damp place.

Maintenance and repair requirements



DANGER

- Do not use a damp cloth to clean your computer to prevent liquid from dripping into the computer and causing it to burn.
- To avoid unnecessary damage to the product caused by frequent switching on and off, wait at least 30 seconds before turning on the machine.



Do not disassemble the equipment randomly. Professional personnel must be present for maintenance and installation.

Table of Contents

1 Summarize	1
1.1 Checklist	1
2 Product Introduction	2
2.1 Product Configuration	2
2.2 IO interface	3
2.3 Power information (when plugged into AC power)	3
3 FAQ	4
Appendix 1 Security Commitment and Recommendation	7
Appendix 2 Security Commitment and Recommendation	9

1 Summarize

1.1 Checklist

Thank you for choosing our products.

Before using your product, please make sure your packaging is complete, if there have been damaged or you find any shortage, please contact your agency as soon as possible.

- OPS X 1
- Product manual X 1
- ATN Screw X 2
- Wi-Fi antenna X 2

2 Product Introduction

2.1 Product Configuration

Processor	- DHI-SP-PIXX
CPU	- Intel Core I5-12450H Processor - Intel Core I7-12650H Processor
Graphics	- Intel® UHD Graphics
Storage	- 1 x M.2 2280 SSD, Nvme/SATA, 256G/512G(Optional)
Memory	- 2 x SO-DIMM DDR4 MAX 3200MHz, 8G/16G(Optional)
Audio	- Realtek ALC897
Front IO interface	- 1 x HDMI1.4 OUT - 1 x DP1.4 OUT - 2 x USB 3.1, 2 x USB2.0, 1 x Type-C(USB3.1) - 1 x RJ45 - 1 x Line-out & MIC-In Two In One Connector - 2 x Wi-Fi/BT ANT
Rear IO interface	- 1 x 80pin JAE - 1 x 2.5/5.5 DC IN JACK
Wireless	- 1 x M.2 2230 CNVI AX101, WIFI/BT Module
Network	- Realtek RTL8111H
Watchdog	- Support
Power input	- 12-19V DC IN
Environmental requirement	- Working temperature / storage temperature: - 5 ~ 45 °C / - 20 ~ 70 °C - Working / non working humidity: 10% ~ 90% non condensing / 5% ~ 95% non condensing
OS	- Without System Image
Dimensions	- 119(L) x 180(W) x 30(H) mm

2.2 IO interface

Front IO interface



Rear IO interface



- WIFI1/2: WIFI/BT ant
- PWR: Power Switch Button
- LED: (top) hard disk indicator, (down) power indicator
- Lock: Anti-theft hole
- Audio: Audio output interface with mic
- DP: DP display interface
- HDMI: High definition multimedia display interface
- TYPE_C: TYPE_ C port
- USB3.1: USB3.1 port
- LAN: RJ-45 network interface
- USB2.0: USB2.0 port
- RESET: Reset button
- JAE 80PIN: 80 pin extension port
- DC IN: DC power interface

2.3 Power information (when plugged into AC power)

Turn off the display: after 10 minutes by default, and it also can be set after 1, 2, 3, 5, 15, 20, 25, 30, 45 minutes, 1, 2, 3, 4, 5 hours.

Put the computer to sleep: 10 minutes by default, and it also can be set after 1, 2, 3, 5, 15, 20, 25, 30, 45 minutes, 1, 2, 3, 4, 5 hours.

The computer can be wake up from sleep mode by moving the mouse, tapping the keyboard, and network remote activation.

3 FAQ

Common Faults of OPS Computer and Troubleshooting Steps and Methods

Common faults	Troubleshooting Steps	Methods
Failure to power on	①Check the power indicator of large screen. ②Re-plug and unplug the power cord and OPS Computer device. It may be caused by failure to plug the cord in place, poor contact, over-current or over-voltage protection. ③Remove OPS Computer for visual inspection and check whether there is any physical damage to OPS Computer caused by collision.	①Press down and hold the reset switch key for 5 seconds to clear CMOS. ②If the alarm sounds when the computer is powered on, please re-insert or replace the memory module.
No display	①Check whether external HDMI (VGA) display is working. ②If the Monitor is not working under the system, please confirm whether the Monitor resolution is supported and whether the Monitor driver under the system is normal or not.	①Press down and hold the reset switch key for 5 seconds to clear CMOS. ②Make depot repair.
Slowdown in access to the System; failure to access due to system breakdown	①Clear CMOS and check whether BIOS is normal or not. ②Confirm whether there is a virus in the system. ③View the disk capacity. ④View the use of memory. ⑤Replace the system disk for testing.	①Press down and hold the reset switch key for 5 seconds to clear CMOS. ②Install virus detection and anti-virus software in the Computer ③Clear the disk space, the fewer software on the desktop, the better. ④Reset the system with One-key Reset tool once the System is backed up.
The computer cannot support the best resolution of the Monitor.	①Confirm the resolution that the Monitor can support. ②Once confirmed that the Monitor is switched ON, check whether it is a wire problem. ③Confirm whether the drive is installed normally. ④Clear CMOS and update BIOS.	①Press down and hold the reset switch key for 5 seconds to clear CMOS and update BIOS. ②Check the memory of video card. ③Confirm whether the driver is installed or updated properly.
The Computer crash, breakdown and rebooting in the process of operation.	①Clear CMOS. ②Check whether the power is configured as required and is OK or not. ③Unplug the external test device. ④Troubleshoot software problems.	①Observe the host operating environment ②Press down and hold the reset switch key for 5 seconds to clear CMOS. ③Use antivirus software or Upgrade software to detect and kill virus in the

	⑤Reset the system.	Computer. ④Troubleshoot software problems: software incompatibility or installation of too many software. ⑤Reset the system with One-key Reset tool
The system cannot be booted through the tool after activation.	①Clear CMOS. ②Check the activation tool. ③Reset the system.	①Press down and hold the reset switch key for 5 seconds to clear CMOS. ②Reset the system with One-key Reset tool
Failure to reset the system and failure to install third-party software	①Clear CMOS. ②Confirm whether the third party software is abnormal or not. ③Check whether the system is set abnormally or not. ④Reset the system.	①Press down and hold the reset switch key for 5 seconds to clear CMOS. ② Check whether the third-party software can be installed on another computer to determine whether it is normal or not ③Reset the system with One-key Reset tool
Poor internet behavior and poor Wi-Fi	① Take the exchange method to prove whether it is the problem of network or the problem of computer. ② Determine whether the software Problem has any impact and determine whether the network IC is captured under the system. ③Reset the system.	① Use a normal computer to verify whether the network cable is connected normally. ② Check the network circuit for poor contact and loose plug. ③ Device Management : check whether the network hardware can be read, whether the system is disabled, whether the network settings are normal, and whether the network ID is normal ④ Confirm whether the wireless network card driver and on-board network card driver are installed normally.
Blue Screen of Death	①Clear CMOS ②Check whether the source of the installed system is secure, whether it is downloaded from the official website mirror image or reliable website, and whether it is simplified. ③Replace the system disk from the same platform.	①Press down and hold the reset switch key for 5 seconds to clear CMOS. ②Uninstall the software on your computer since it is caused by software installation conflict. ③Unplug the external device to check whether the blue screen has occurred. ④Reset the system with One-key Reset tool.
Poor sound effect	①Clear CMOS. ②Replace the system disk of the same platform for testing. ③Check the connector. ④Reset the system.	①Press down and hold the reset switch key for 5 seconds to clear CMOS. ② Replace the external device of sound output for testing. ③Check whether the sound device is turned off under the system and check the sound card driver (if there is no driver package,

		please download Driver Talent - Driver Update - Sound and Video - Start Updating - Automatically Find the Official Driver - Restart the Computer. ④Insert and remove several times or replace the device for testing to avoid contact problems.
Poor USB and No touch	①Clear CMOS. ②Reset the system. ③Troubleshoot the USB's own problems.	①Press down and hold the reset switch key for 5 seconds to clear CMOS. ②Determine whether the USB driver is normal and disabled under the system, you can view it in resource management or software tool, and update the driver in case of any exception. ③Reset the system with One-key Reset tool

Appendix 1 Security Commitment and Recommendation

Dahua Vision Technology Co., Ltd. (hereinafter referred to as "Dahua") places great emphasis on cybersecurity and privacy protection. We continuously allocate special funds to enhance employees' awareness and capabilities in security, and ensure sufficient security protection for our products. Dahua has established a professional security team to provide comprehensive security empowerment and control throughout the entire product lifecycle, including design, development, testing, production, delivery, and maintenance. Dahua products adhere to the principle of minimum necessary data collection, service minimization, strict prohibition of backdoors, and the disabling of unnecessary and insecure services (such as Telnet). We continuously introduce innovative security technologies to bolster the security capabilities of our products. Additionally, we go above and beyond by providing global users with security alarm and 24/7 security emergency response services. This approach ensures that we are better safeguarding their security rights and interests. At the same time, Dahua encourages users, partners, suppliers, government agencies, industry organizations and independent researchers to report potential risks or vulnerabilities to the Dahua PSIRT. They can do so by visiting the cybersecurity section on the Dahua website.

The security of software platforms not only relies on the continuous attention and efforts from manufacturers throughout R & D, production, and delivery, but also requires active participation from users. Users should remain attentive to the environment and methods to ensure its secure operation. To this end, we suggest users to safely use the software platform, including but not limited to:

1. Account Management

1.1 Use Strong 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.

1.2 Change Password Regularly

We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

1.3 Assign Accounts and Permissions Reasonably

According to business and management needs, reasonably add new users, and reasonably allocate a minimum set of permissions for them.

1.4 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.

1.5 Set and Update Passwords Reset Information Timely

The platform supports password reset function. To reduce the risk of being attacked, please set up related information for password reset in time. 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.

1.6 Enable Account Binding IP/MAC

It is recommended to enable the account binding IP/MAC mechanism to further improve access security.

2. Service Configuration

2.1 Enable HTTPS

We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

2.2 Disable Unnecessary Services and Choose Secure Modes

If not needed, it is recommended to turn off some services such as SNMP, SMTP, etc., to reduce risks.

If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

- SMTP: Choose TLS to access mailbox server.
- FTP: Choose SFTP, and set up strong passwords.

3. Network Configuration

3.1 Enable Firewall Allowlist

We suggest you to enable allowlist function to prevent everyone, except those with specified IP addresses, from accessing the system. Therefore, please be sure to add your computer's IP address and the accompanying equipment's IP address to the allowlist.

3.2 Network Isolation

The network should be isolated by partitioning the video monitoring network and the office network on the switch and router to different VLANs. This prevents attackers from using the office network to launch Pivoting attacks on the video monitoring network.

4. Security Auditing

4.1 Check Online Users

It is recommended to check online users irregularly to identify whether there are illegal users logging in.

4.2 View the Platform Log

By viewing the log, you can get the IP information of the attempt to log in to the platform and the key operation information of the logged-in user.

5. Physical Protection

We suggest that you perform physical protection to the device that has installed the platform. 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.

6. Perimeter Security

We suggest that you deploy perimeter security products and take necessary measures such as authorized access, access control, and intrusion prevention to protect the software platform security.

Appendix 2 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's 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:

1. Account Management

1.1 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.

1.2 Change passwords periodically

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

1.3 Allocate accounts and permissions appropriately

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

1.4 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.

1.5 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.

2. Service Configuration

2.1 Enable HTTPS

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

2.2 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.

2.3 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.

2.4 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.

3. Network Configuration

3.1 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.

3.2 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.

3.3 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.

4. Security auditing

4.1 Check online users

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

4.2 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.

4.3 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.

5. Software Security

5.1 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.

5.2 Update client software in time

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

6. 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

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