

OPS PC Module

User's Manual








Foreword

General

This manual introduces the installation, functions and operations of the device (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.	January 2024

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, audio, 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



Please transport the equipment within the allowed humidity ($\leq 95\%$ RH) and temperature range (-10°C to $+50^{\circ}\text{C}$).

Storage requirements



Please store the equipment within the allowed humidity ($\leq 95\%$ RH) and temperature range (-10°C to $+50^{\circ}\text{C}$).

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 to 50 degrees Celsius; humidity: 10% to 95% ; storage temperature: -20 to 70 degrees Celsius).
- 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 Requirements



WARNING

- 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.



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

Table of Contents

Foreword	I
Important Safeguards and Warnings	III
1 Summarize	1
2 Product Introduction	2
2.1 Product Configuration	2
2.2 IO Interface	3
Appendix 1 Cybersecurity Recommendations	4

1 Summarize

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 × 1
- Product manual × 1
- ATN Screw × 2
- Wi-Fi antenna × 2

2 Product Introduction

2.1 Product Configuration

CPU	- Intel® Tiger Lake Mobile Processor
Graphics	- Intel® Iris® Xe Graphics
Storage	- 1 x M.2 2280 size for NVMe/SATA SSD - 1 x 2.5" SATA Interface
Memory	- 2 x SO-DIMM DDR4 3200 MHz, Max 32GB
Audio	- Realtek ALC897 HD Audio IC
Front IO interface	- 1 x HDMI1.4 - 2 x USB3.1, 1 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 - 1 x Power button - 1 x Reset button
Rear IO interface	- 1 x 80pin: 1 x HDMI 2.0 out, 1 x USB3.0, 2 x USB2.0, TTL - 1 x 2.5/5.5 DC IN JACK
Wireless	- 1 x M.2 2230 WIFI/BT Module
Network	- Realtek Gigabit Ethernet
Watchdog	- Support
Power input	- 12-19 VDC 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	- Support Windows10 / Windows11 / Linux
Dimensions	- 119 x 180 x 30 mm

2.2 IO Interface

Front IO interface



Rear IO interface



- WIFI-1/2: WIFI/BT antenna
- POWER BUTTON: Power Switch Button
- LINE_OUT&MIC-IN Two in One Connector: Audio output interface with mic
- LED: (top) hard disk indicator, (bottom) power indicator
- TYPE_C: TYPE_C port
- RESET: Reset button
- Lock: Anti-theft hole
- HDMI: High definition multimedia display interface
- USB3.1: USB3.1 port
- LAN: RJ-45 network interface
- USB2.0: USB2.0 port
- JAE 80PIN: 80 pin extension port
- DC IN: DC power interface

Appendix 1 Cybersecurity Recommendations

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.