



Intelligent Video Analysis Server (TS2)

Quick Start Guide








Foreword

Model

TS2 series model

Safety Instruction

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.	November 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 to: 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 server under allowed humidity and temperature conditions.

Storage Requirements



Store the server under allowed humidity and temperature conditions.

Installation Requirements



-  Electrical Hazard

Preventive measures: Make sure the power is off when you put your hand into the device.

- Stability Hazard

Possible result: The rack might fall down and cause serious personal injury.

Preventive measures (including but not limited to):



- ◇ Before extending the rack to the installation position, read the installation instructions.
- ◇ When the device is installed on the slide rail, do not place any load on it.
- ◇ Do not retract the slide rail while the device is installed on it.



- Do not connect the power adapter to the device while the adapter is powered on.
- Strictly comply with the local electrical safety code and standards. Make sure that the ambient voltage is stable and meets the power supply requirements of the device.
- Use the standard power adapter or cabinet power supply. We will assume no responsibility for any injuries or damages caused by the use of a nonstandard power adapter.

-  Rotating Fan Blades Hazard

Avoid touching the fan blades, especially when they are moving.

-   Before installation, disconnect all the power cords.




- Do not place the device in a place exposed to sunlight or near heat sources.

- Keep the device away from dampness, dust, and soot.
- Put the device in a well-ventilated place, and do not block its ventilation.
- Install the switch horizontally on a stable surface to prevent it from falling.
- The device is a class I electrical appliance. Make sure that the power supply of the device is connected to a power socket with protective earthing.
- Use power cords that conform to your local requirements and rated specifications.
- Before connecting the power supply, make sure the input voltage matches the server power requirement.
- When installing the device, make sure that the power plug and appliance coupler can be easily reached to cut off power.
- Extra protection is necessary for the device casing to reduce the transient voltage to the defined range.
- The device must be installed in a location that only professionals can access. Non-professionals are not allowed to enter the installation area.
- It is prohibited for non-professionals and unauthorized personnel to open the device casing.
- Install the device near a power socket for emergency disconnect.

Operation Requirements



-  The device or remote control contains button batteries. Do not swallow the batteries due to the risk of chemical burns.

Possible result: The swallowed button battery can cause serious internal burns and death within 2 hours.

Preventive measures (including but not limited to):

 - ◇ Keep new and used batteries out of reach of children.
 - ◇ If the battery compartment is not securely closed, stop using the product immediately and keep out of reach of children.
 - ◇ Seek immediate medical attention if a battery is believed to be swallowed or inserted inside any part of the body.
- Battery Pack Precautions

Preventive measures (including but not limited to):

 - ◇ Do not transport, store or use the batteries in high altitudes with low pressure and environments with extremely high and low temperatures.
 - ◇ Do not dispose the batteries in fire or a hot oven, or mechanically crush or cut the batteries to avoid an explosion.
 - ◇ Do not leave the batteries in environments with extremely high temperatures to avoid explosions and leakage of flammable liquid or gas.
 - ◇ Do not subject the batteries to extremely low air pressure to avoid explosions and the leakage of flammable liquid or gas.



- In a domestic environment this may cause radio interference in which case you may be required to take adequate measures.
- The device is heavy and needs to be carried by several persons together to avoid personal injuries.
- Place the device in a location that children cannot easily access.



- Make sure that the power supply is correct before use.
- Operate the device within the rated range of power input and output.
- Use the device under allowed humidity and temperature conditions.
- Do not drip or splash liquid onto the device, make sure that there is no object filled with liquid on the device to prevent liquid from flowing into it.
- Do not disassemble the device without professional instruction.
- Your configurations will be lost after performing a factory reset. Please be advised.
- Do not restart, shut down or disconnect the power to the device during an update.
- Make sure the update file is correct because an incorrect file can result in a device error occurring.
- The system cannot upgrade different types of AI modules at the same time.
- Do not frequently turn on/off the device. Otherwise, the product life might be shortened.
- Back up important data on a regular basis when using the device.
- Operating temperature: 10 °C to 35 °C (50 °F to 95 °F).

Maintenance Requirements



- Replacing unwanted batteries with the wrong type of new batteries might result in explosion.
Preventive measures (including but not limited to):
 - ◇ Replace unwanted batteries with new batteries of the same type and model to avoid the risk of fire and explosion.
 - ◇ Dispose of the old batteries as instructed.
- Power off the device before maintenance to make sure that the device is disconnected from the power supply.



- Make sure you use the same model when replacing the battery to avoid fire or explosion. Dispose the battery strictly following the instructions.
- Power off the device before maintenance.



- AI module does not support hot plug. If you need to install or replace the AI module, unplug the device power cord first. Otherwise, it will lead to file damage on the AI module.
- The device casing provides protection for internal components. Use a screwdriver to loosen the screws before detaching the casing. Make sure to put the casing back on and secure it in its original place before powering on and using the device.
- Clean the ventilation pipe regularly to avoid obstructions.
- It is prohibited for non-professionals and unauthorized personnel to open the device casing.
- The appliance coupler is a disconnection device. Keep it at a convenient angle when using it. Before repairing or performing maintenance on the device, first disconnect the appliance coupler.

Table of Contents

Foreword..... I

Important Safeguards and WarningsIII

1 Product Introduction..... 1

1.1 Overview..... 1

1.2 Features..... 1

1.3 Structure..... 1

1.3.1 Front Panel..... 1

1.3.2 Rear Panel..... 2

Appendix 1 Security Commitment and Recommendation..... 3

1 Product Introduction

1.1 Overview

The TS2 server is applicable to the intelligent analysis server device named xxxxx-IVx-xxxxxx-xxxxx-TS2-xxxxx. It is widely used in intelligent analysis in various places.

1.2 Features

- Linux OS System is adopted which features stability, security and reliability.
- Based on video cloud architecture, with cluster deployment and dynamic performance expansion capabilities.


1.3 Structure

1.3.1 Front Panel

Figure 1-1 Front panel



Table 1-1 Panel description

No.	Name	Description
1	USB 2.0 port	Connects to external devices, such as a mouse and a keyboard.
2	Power switch	In the power-on state, press and hold the switch for 4 seconds to shut down the server.
3	UID switch and indicator	<p>UID switch and indicator are used to locate the device to be operated. Press the UID switch to turn on or shut down the locator light.</p>  <p>Press and hold UID switch for 4 seconds, and then you can reset the iBMC management system of the server.</p>

No.	Name	Description
4	Network indicator	<p>Indicates the current network status.</p> <ul style="list-style-type: none"> ● Solid green: Network connected. ● Green light flashes: Network data is being transmitted. ● Light off: Network disconnected.
5	System status indicator	<p>Indicates the running status of the server.</p> <ul style="list-style-type: none"> ● Solid green: System runs normally. ● Red light flashes: Indicates a serious error occurred on the server. ● Solid red: Indicates an urgent error occurred on the server.

1.3.2 Rear Panel

Figure 1-2 Rear panel

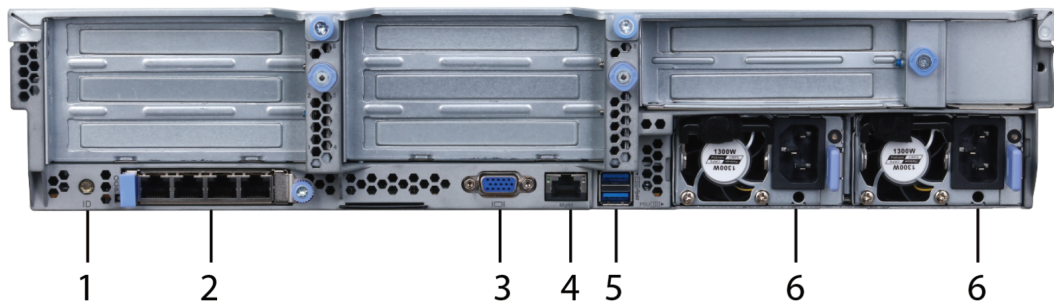




Table 1-2 Panel description

No.	Name	Description
1	ID indicator	Used to locate the device to be operated.
2	Ethernet port	Four 1000 Mbps adaptive Ethernet ports. Connects to the network cable.
3	VGA port	Connects to a VGA monitor or a physical KVM.
4	Management network port	<p>Management network port, only for access to BMC.</p> <p> It cannot be used as a data network port.</p>
5	USB 3.0 port	Connects to external devices, such as a mouse and a keyboard.
6	Power port	<p>Connects to the power supply.</p> <p> To ensure the stability and reliability of the server, we recommend connecting 2 power ports at the same time to achieve redundancy power supply. When one power supply fails, the other power supply can still supply power to the server, reducing the impact of device error or downtime.</p>

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 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.

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;
- Establish 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).

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