DSS4004-S2

Quick Start Guide

V1.0.0

Foreword

General

This manual introduces the quick start operations of the DSS general surveillance management platform.

Models

DSS4004-S2

Safety Instructions

The following categorized signal words with defined meaning might appear in the manual.

Signal Words	Meaning
⚠ CAUTION	Indicates a potential risk which, if not avoided, may result in property damage, data loss, lower performance, or unpredictable result.
🕮 NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	August 2019

Privacy Protection Notice

As the device user or data controller, you might collect personal data of others such as face, fingerprints, car plate number, Email address, phone number, GPS and so on. You need to be in compliance with the local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures include but not limited to: providing clear and visible identification to inform data subject the existence of surveillance area and providing related contact.

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper manual, CD-ROM, QR code or our official

website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.

- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our 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 the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Important Safeguards and Warnings

Operation Requirement

- Do not place or install the Device in a place exposed to sunlight or near the heat source.
- Keep the Device away from dampness, dust or soot.
- Keep the Device installed horizontally on the stable place to prevent it from falling.
- Do not drop or splash liquid onto the Device, and make sure there is no object filled with liquid on the Device to prevent liquid from flowing into the Device.
- Install the Device in a well-ventilated place, and do not block the ventilation of the Device.
- Operate the device within the rated range of power input and output.
- Do not dissemble the Device.
- Transport, use and store the Device under the allowed humidity and temperature conditions.

Electrical Safety

- Improper battery use might result in fire, explosion, or inflammation.
- When replacing battery, make sure the same model is used.
- Use the recommended power cables in the region and conform to the rated power specification.
- Use the power adapter provided with the Device; otherwise, it might result in people injury and device damage.
- The power source shall conform to the requirement of the Safety Extra Low Voltage (SELV) standard, and supply power with rated voltage which conforms to Limited power Source requirement according to IEC60950-1. Please note that the power supply requirement is subject to the device label.
- Connect the device (I-type structure) to the power socket with protective earthing.
- The appliance coupler is a disconnection device. When using the coupler, keep the angle for easy operation.

Table of Contents

1 Checklist

1.1 Package

Open the product package and then check if the product is damaged or missing.

- Package: Product unit appearance is complete without obvious damage; after package is opened, check if accessories and HDD are complete.
- Device: Product unit appearance has no scratch, damage, and protection cover has no obvious damage.
- Accessories: Type and quantity in product checklist are correct and complete. Actual accessories have no damage.

Table 1-1 Packing list

No.	Checklist	Quantity	Description
1	Server	1	–
2	Anti-vibration Screw for Hard Drive	12	–
3	Anti-vibration Mat	12	–
4	Power Cable	1	1.5 m
5	Quick Start Guide	1	–

1.2 Port Definition

Product front panel is equipped with power button, USB port and status indicators; rear panel is equipped with a single power, Ethernet port, serial port and other ports.

1.2.1 Front Panel

Figure 1-1 Front panel

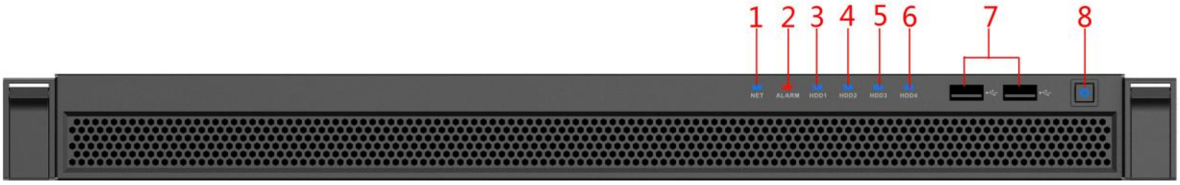


Table 1-2 Description

No.	Item	Description
1	Network Indicator	The light flashes blue when network is connected.
2	Alarm Indicator	The light flashes blue when device triggers alarm.
3	HDD1	System disk indicator. It flashes when reading disk.
4	HDD2	Hard drive indicator. It is normally on when hard drive is

No.	Item	Description
5	HDD3	inserted.
6	HDD4	
7	USB 2.0 Port	2 ports, white
8	Power Button	Press the button to start the device. The device is equipped with power status indicator (blue normally on); long press it to shut down the server.

1.2.2 Rear Panel

Figure 1-2 Rear panel

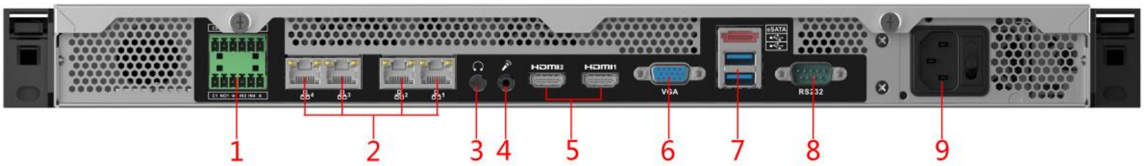


Table 1-3 Description

No.	Item	Description
1	Alarm Output and Input	Reserved. Supports RS–485 protocol access.
2	Ethernet Port	Supports 10Mbps/100Mbps/1Gbps self-adaptive dual full duplex. The platform default Ethernet port is 1.
3	Audio Output	3.5 mm audio output.
4	Audio Intercom Input	3.5 mm audio input.
5	HDMI Port	2 channels, reserved.
6	VGA Port	DB 15 pin. Supports VGA port device access.
7	eSATA Port	Supports eSATA device access.
8	RS–232	Debugging serial port.
9	Single Power	AC 100V - 240V/47 - 63Hz; supports hot plug.

1.3 Device Installation

Connect cables according to port introduction, and then connect the server to power.

2 Local Application

2.1 Function Architecture

The chapter introduces the functions of local application. See Figure 2-1. The local interface will be displayed after starting the server. See Figure 2-2.

Figure 2-1 Local application

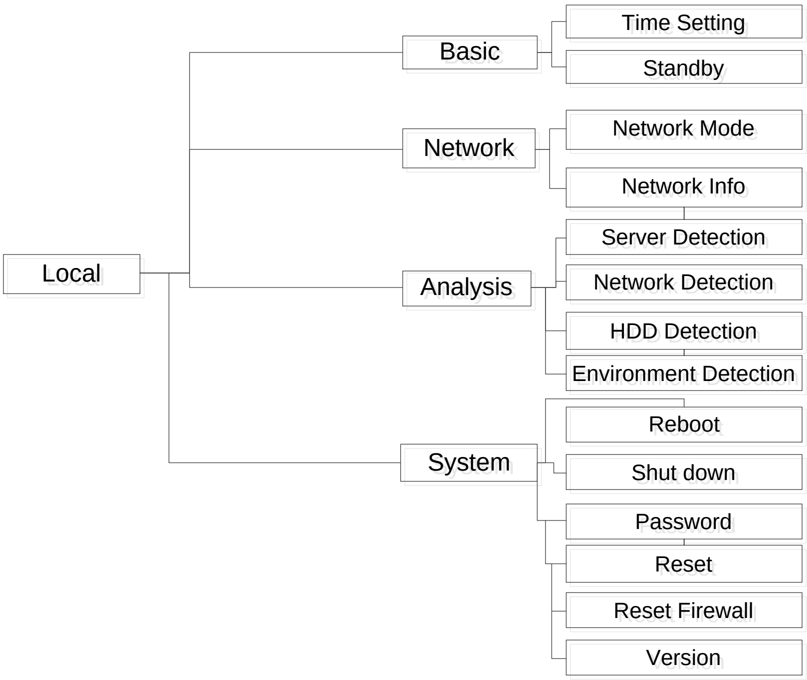
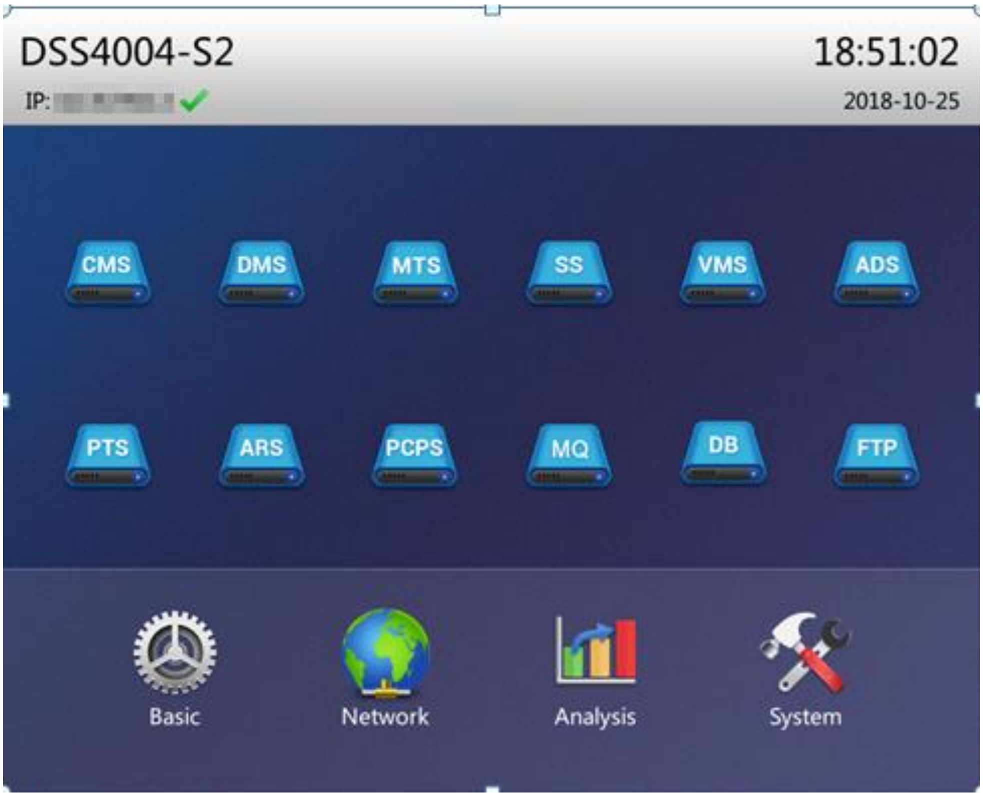


Figure 2-2 Local interface

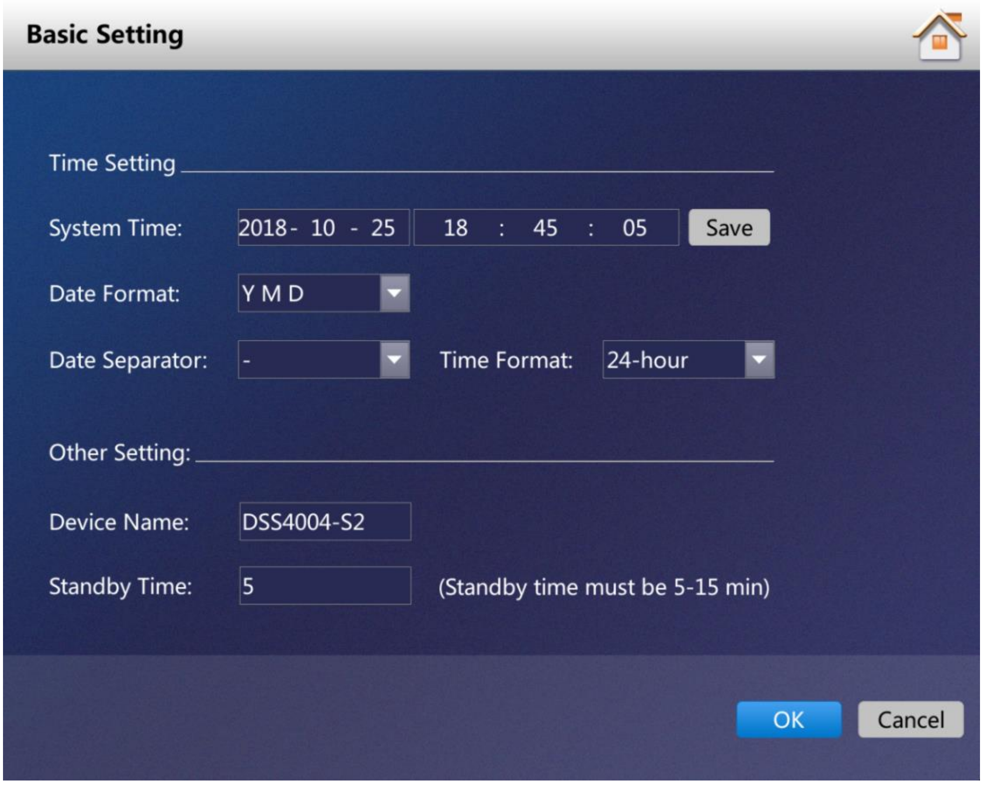


2.2 Business Configuration

2.2.1 Basic Setting

Click **Basic Setting** on the local interface, and then configure time and other settings.

Figure 2-3 Basic setting



Basic Setting

Time Setting

System Time: 2018 - 10 - 25 18 : 45 : 05

Date Format: Y M D

Date Separator: -

Time Format: 24-hour

Other Setting:

Device Name: DSS4004-S2

Standby Time: 5 (Standby time must be 5-15 min)

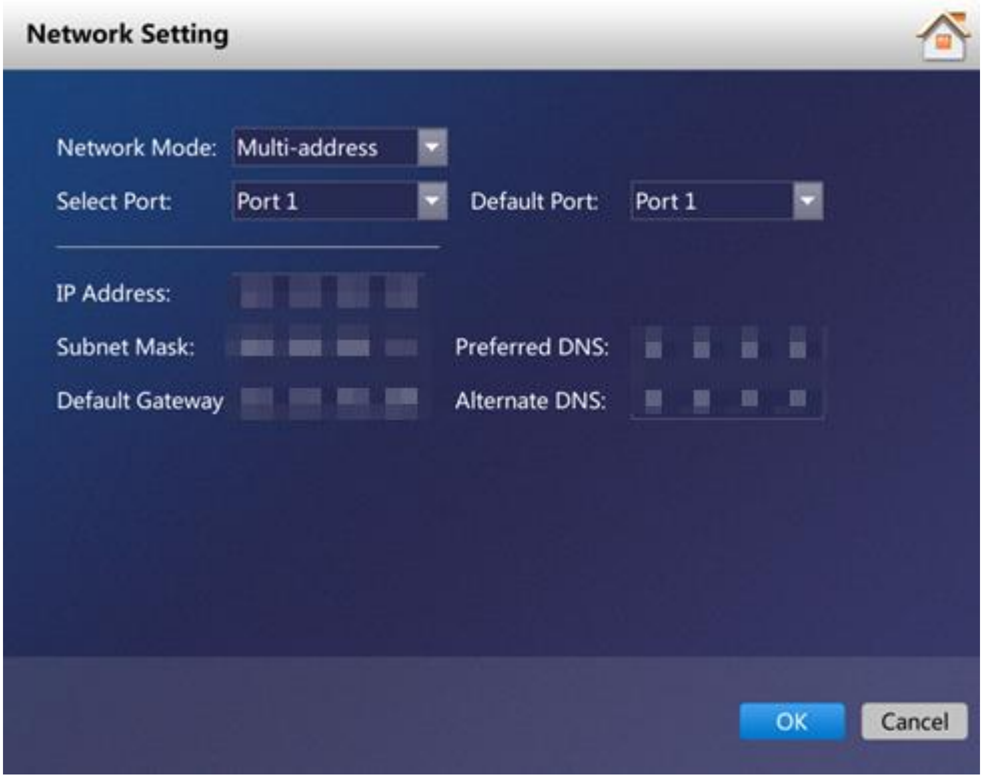
Table 2-1 Basic setting parameters description

Parameter	Description
System Time	Keep it the same as local time.
Date Format	Set data and time format of local application homepage.
Date Separator	
Time Format	
Device Name	It is the current product model name by default.
Standby Time	The server will get into standby mode when there is no operation for several minutes. Set the threshold here. The default threshold value is 5 minutes; the maximum value is 15 minutes.

2.2.2 Network Setting

Click **Network Setting** on the local interface to display enter the network setting interface.

Figure 2-4 Network setting



Network Setting

Network Mode: Multi-address

Select Port: Port 1

Default Port: Port 1

IP Address: [redacted]

Subnet Mask: [redacted]

Default Gateway [redacted]

Preferred DNS: [redacted]

Alternate DNS: [redacted]

Table 2-2 Basic setting parameter description

Parameter	Description
Network Mode	Supports 4 modes. ● Multi-address Multiple network cards can have different segments and realize multi-segment access, which is suitable for the scenario with high requirement of network reliability. For example, when configuring hot standby, you need to use network card 2 to set standby heartbeat IP; also it can be adopted in the scheme with ISCSI expansion storage. The planning of network port is shown as follows: Network port 1 is used as service communication and network port 2 is reserved; network port 3 and 4 are used as ISCSI storage. ● Fault tolerance Multiple network cards use one IP address. Generally only one network card is working, and it will automatically enable another normal network card to guarantee network smoothness when working network card fails. ● Load balancing Multiple network cards use one IP address. These network cards work together, share network load and provide network loading capacity which exceeds single network card bandwidth. When one network card is abnormal, it will distribute load to other available cards again and provide network reliability. ● Link Aggregation Through network card binding and peripheral communication, the bound network card takes part in the work and shares the network load, realizing one network card forwarding stream bigger than 1K. For example, 2 IP bound, the other 2 have different IP, then the server owns 3 IP, the bound IP bandwidth is 2K while other 2 is 1K. Link aggregation can be realized only when link aggregation is supported by directly-connected switch.
Select Port	Supports default network port configuration. The platform default port is Network Port 1 (when ten gigabit optical port is selected, only multi-address can be supported). It can be modified according to project deployment.
Default Port	Select default network card, and then the network card will forward the data packet of non-adjacent segment (such as WAN) as default port.
IP Address	After network card is selected, you can set its IP address, subnet mask, default gateway, preferred DNS server address and alternate DNS server address.
Subnet Mask	
Preferred DNS	
Default Gateway	
Alternate DNS	

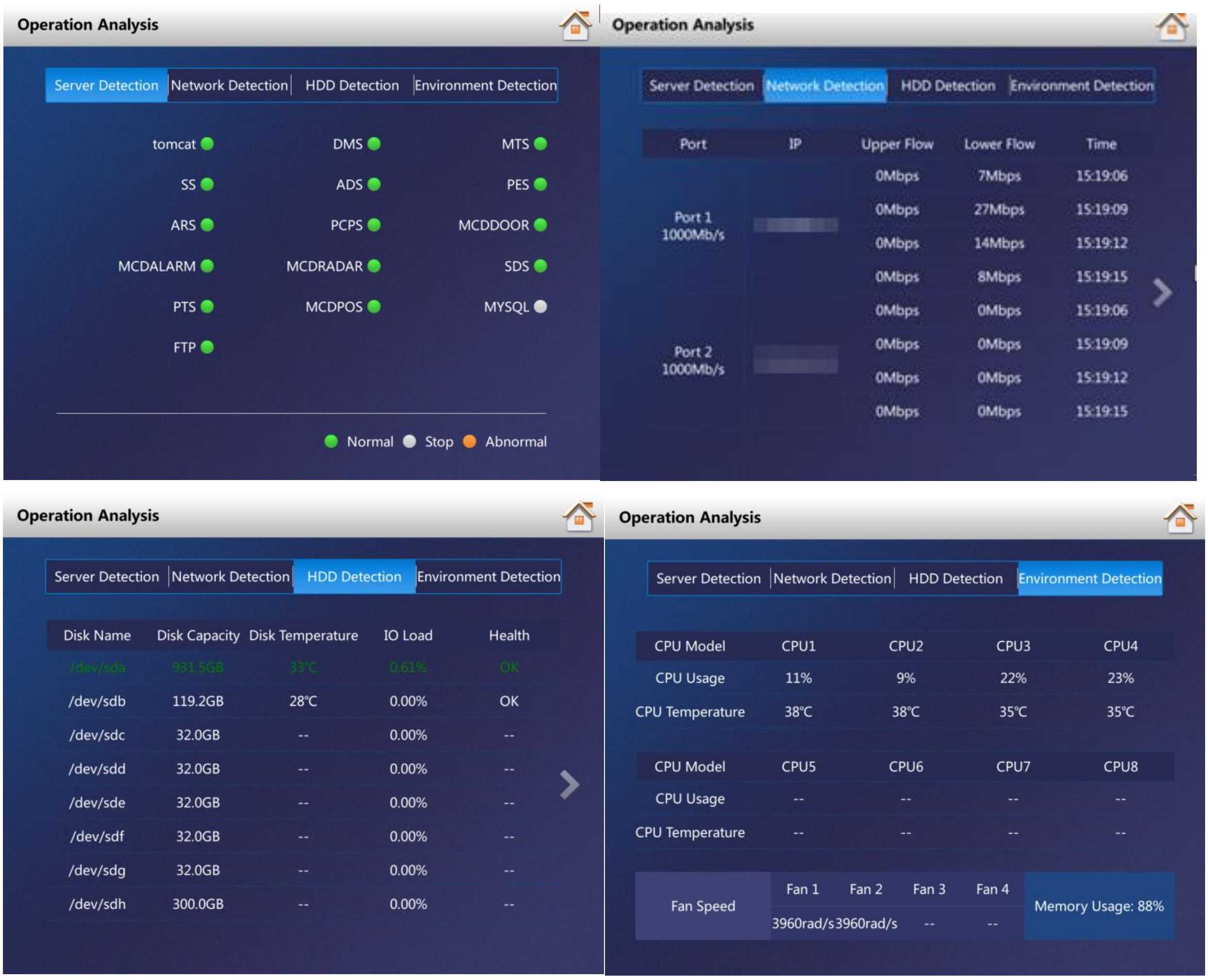
2.3 Operation Management

2.3.1 Operation Analysis

Click **Operation Analysis** at the local interface and then you can check the status detection result of platform server, network, HDD and environment.

- Server Detection: Realizes real-time detection of the status of platform server, such as normal, stop and abnormal etc.
- Network Detection: Realizes real-time detection of physical network port.
- HDD Detection: Realizes real-time detection of disk capacity, temperature, IO load and health.
- Environment Detection: Realizes real-time detection of CPU temperature, usage, fan speed and memory usage.

Figure 2-5 Operation analysis



tomcat ●	DMS ●	MTS ●
SS ●	ADS ●	PES ●
ARS ●	PCPS ●	MCDDOOR ●
MCDALARM ●	MCDRADAR ●	SDS ●
PTS ●	MCDPOS ●	MYSQL ●
FTP ●		

● Normal ● Stop ● Abnormal

Port	IP	Upper Flow	Lower Flow	Time
Port 1 1000Mb/s	[redacted]	0Mbps	7Mbps	15:19:06
		0Mbps	27Mbps	15:19:09
		0Mbps	14Mbps	15:19:12
		0Mbps	8Mbps	15:19:15
Port 2 1000Mb/s	[redacted]	0Mbps	0Mbps	15:19:06
		0Mbps	0Mbps	15:19:09
		0Mbps	0Mbps	15:19:12
		0Mbps	0Mbps	15:19:15

Disk Name	Disk Capacity	Disk Temperature	IO Load	Health
/dev/sda	931.5GB	33℃	0.61%	OK
/dev/sdb	119.2GB	28℃	0.00%	OK
/dev/sdc	32.0GB	--	0.00%	--
/dev/sdd	32.0GB	--	0.00%	--
/dev/sde	32.0GB	--	0.00%	--
/dev/sdf	32.0GB	--	0.00%	--
/dev/sdg	32.0GB	--	0.00%	--
/dev/sdh	300.0GB	--	0.00%	--

CPU Model	CPU1	CPU2	CPU3	CPU4
CPU Usage	11%	9%	22%	23%
CPU Temperature	38℃	38℃	35℃	35℃

CPU Model	CPU5	CPU6	CPU7	CPU8
CPU Usage	--	--	--	--
CPU Temperature	--	--	--	--

	Fan 1	Fan 2	Fan 3	Fan 4	
Fan Speed	3960rad/s	3960rad/s	--	--	Memory Usage: 88%

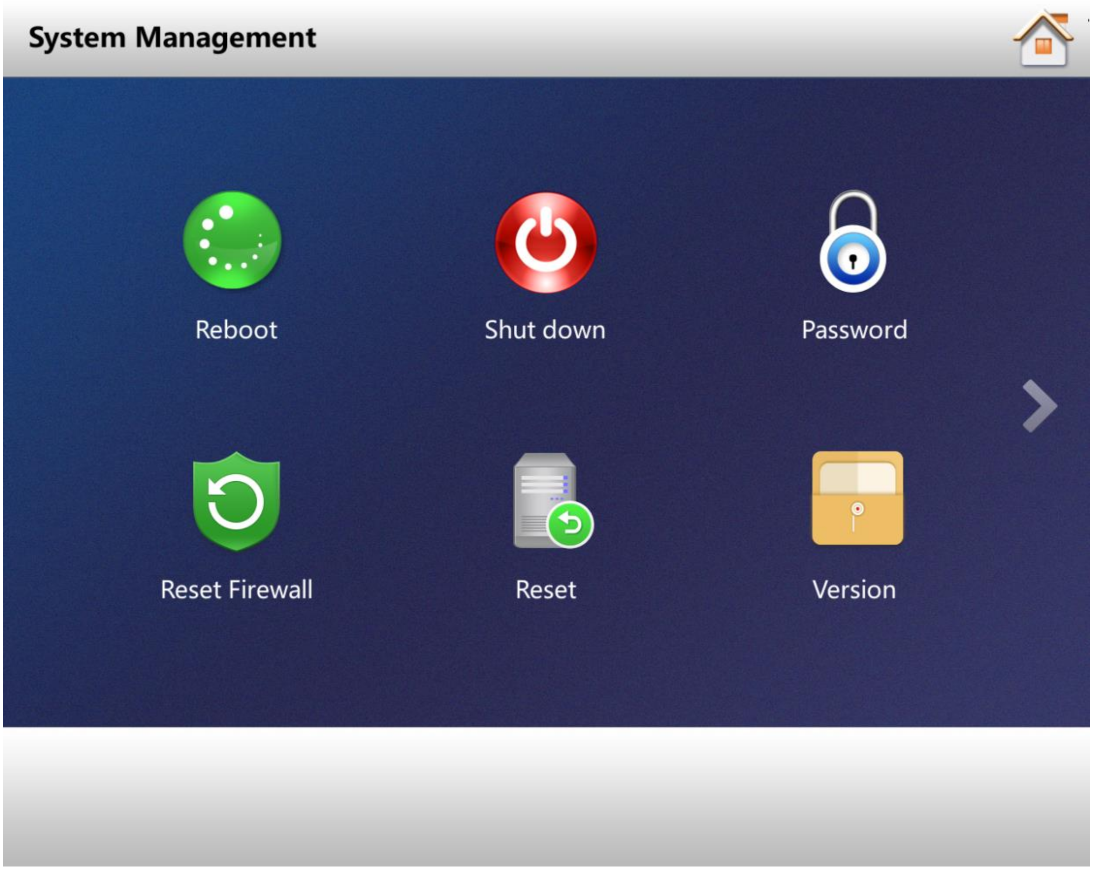
2.3.2 System Management

Click **System Management** on the local interface. You can perform the following operations.

- Reboot: Save system data before reboot.
- Shut down: Save system data before shutting it down. It is forbidden to power off directly.

- Password: Reset the current password as initialization password for admin, configuration system, system, FTP and database.
- Reset Firewall: Enable SSH (22) port again to avoid whitelist configuration error and access failure of platform.
- Version: Displays product model, product serial number, product ID and system version.

Figure 2-6 System management



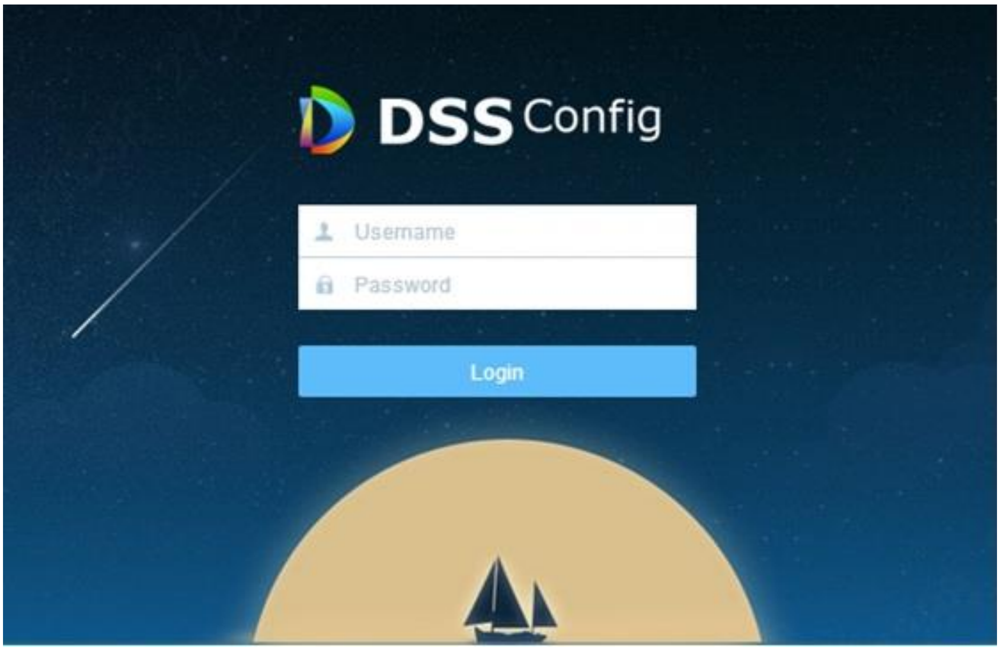
3 Configuring System

Local application only provides basic configurations, such as time, language, network and quick management. Log in to the configuration system for deeper configurations of service, cluster, storage, linkage, map, database and security. Refer to server user's manual for more details.

Access address of the configuration system is **http://IP/config**.

- Default server IP address is 192.168.1.108, default username is admin, and default password is 123456.
- Finish initialization according to system prompt for first login.

Figure 3-1 Configuration system



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 equipment 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 equipment (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 equipment 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 equipment network security:

1. **Physical Protection**

   We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment 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 equipment (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 equipment 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. **Enable Whitelist**
   We suggest you to enable whitelist 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 whitelist.
8. **MAC Address Binding**
   We recommend you to bind the IP and MAC address of the gateway to the equipment, thus reducing the risk of ARP spoofing.
9. **Assign Accounts and Privileges Reasonably**
   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.
10. **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.
11. **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.
12. **Secure Auditing**
    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check equipment log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.
13. **Network Log**
    Due to the limited storage capacity of the equipment, 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.
14. **Construct a Safe Network Environment**
    In order to better ensure the safety of equipment 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.