DSS7016D-S2

Quick Start Guide

V1.0.0

Foreword

General

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

Models

DSS7016D-S2, DSS7016DR-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

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 User's manual, CD-ROM, QR code or our official website. If there is inconsistency between paper User's 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 Guide (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 Ports

1.1 Out-of-box Checking

Check the package against the following checklist. If you find any damage or loss, contact after-sales service.

Table 1-1 Checklist

No.	Checklist	Quantity	Description
1	Server	1	–
2	Hard Drive Bracket	16	–
3	Hard Disk Screw	1 bag	68 screws, 4 for redundancy
4	Power Cable	1	1.5 m
5	Network Cable	1	2 m (Gigabit CAT 5 twisted pair)
6	Mouse	1	USB 2.0 interface (box-packed)
7	Terminal Board	1 bag	● 2 with 12 columns ● 2 with 8 columns
8	Panel Key	2	Universal for series product

⚠

After confirming that the material and accessories are complete, well store them for future use.

1.2 Panels and Ports

Product front panel is equipped with power button, USB port and status indicator (system disk, alarm and network); rear panel is equipped with power, network port, serial port and other ports. Besides, the server also has reserved alarm terminal, HDMI port and other function expansion ports.

1.2.1 Front Panel

Figure 1-1 Front panel

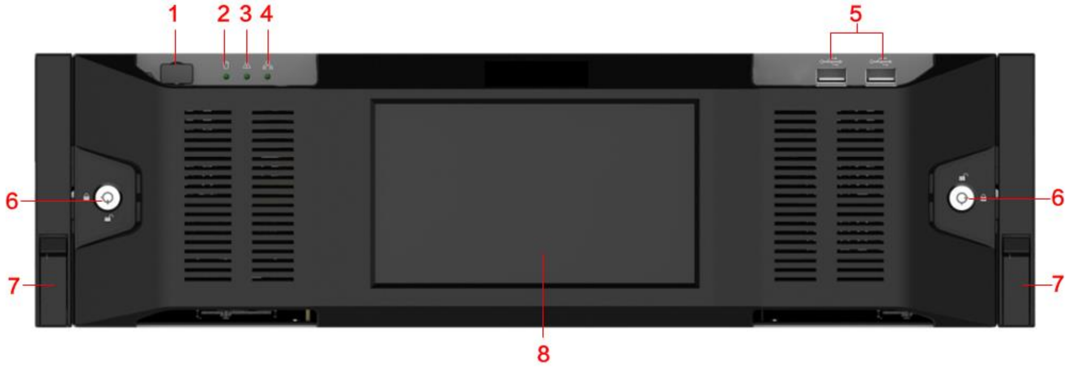


Table 1-2 Front panel description

No.	Port or Button	Description
1	Power button	Press the button to start the server. Long press it to shut down.
2	Hard drive indicator light	The light flashes during disk-reading.
3	Alarm indicator light	The blue light flashes when the server triggers an alarm.
4	Network indicator light	The blue light flashes when network is well connected.
5	USB 2.0 port	2 ports, white
6	Panel locks	Use key to unlock the front panel before taking it off the server.
7	Tab and screw hole	Used to fix the server into the standard cabinet.
8	LCD	7-inch display for local system operations.

1.2.2 Rear Panel

Figure 1-2 Rear panel (without redundancy power)

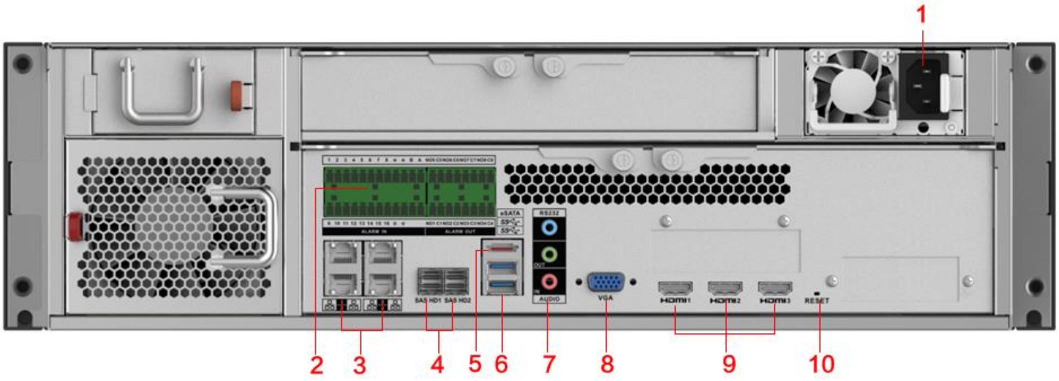


Figure 1-3 Rear panel (with redundancy power)

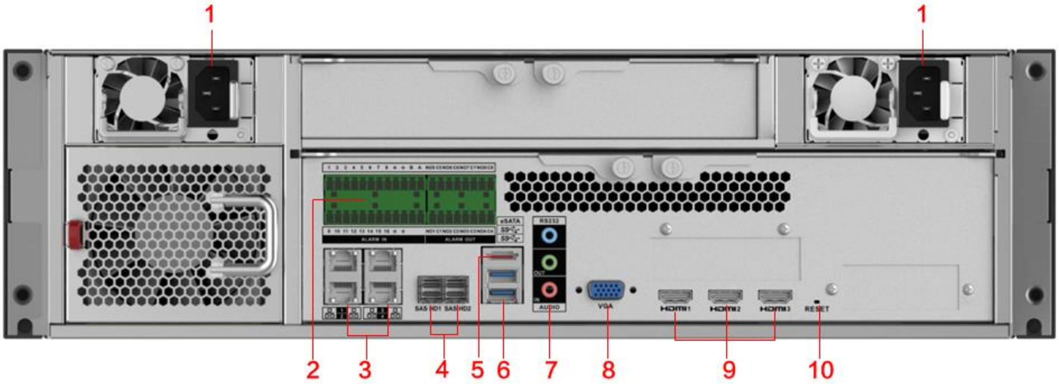


Table 1-3 Rear panel description

No.	Port or Tag	Description
1	Single power	100V AC–240V/47 AC–63Hz; supports hot swap.
2	Alarm output or input	Reserved, used to connect to external RS485 device.
3	Ethernet port	Supports 10 Mbps/100 Mbps/1 Gbps self-adaptive dual full duplex. Ethernet port 1 is the default port.
4	SAS port	Used to connect to expansion cabinet.
5	eSATA port	Supports eSATA device access.
6	USB 3.0 port	Two USB 3.0 ports for USB device access.
7	Audio input or output port	● Blue: RS-232 port ● Green: Audio output port, 3.5 mm JACK interface, outputs audio signal to earphone and other devices. ● Red: Audio input port, 3.5 mm JACK interface, inputs audio signal, and receives analog audio signal from sound pick-up and other devices.
8	VGA Port	DB 15 pin, for VGA port device access.
9	HDMI Port	3 channels, reserved.
10	RESET	Reset button. Press and hold for 4 to 5 seconds to restore factory default settings.

1.3 Connecting Cables

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

2 Local Applications

2.1 Function Architecture

The section introduces the local applications of the device. See Figure 2-1 The local interface is displayed after the server is started. See Figure 2-2.

Figure 2-1 Local functions

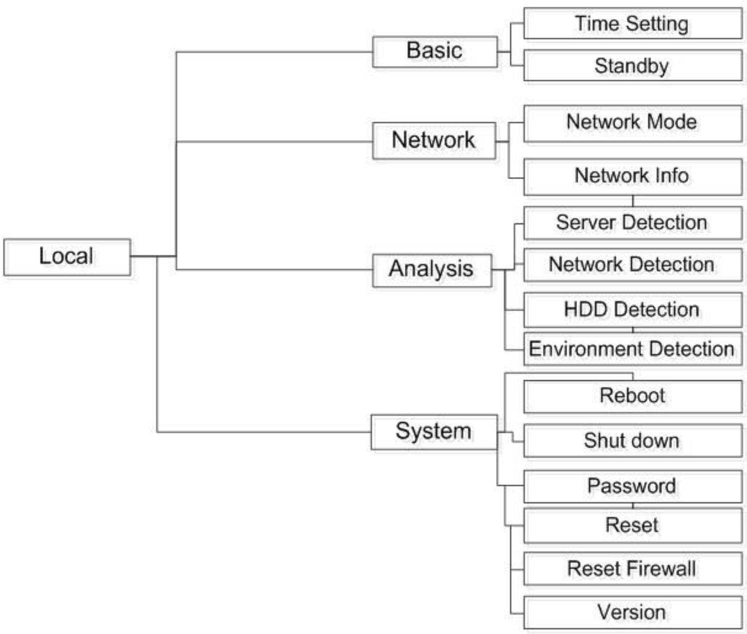
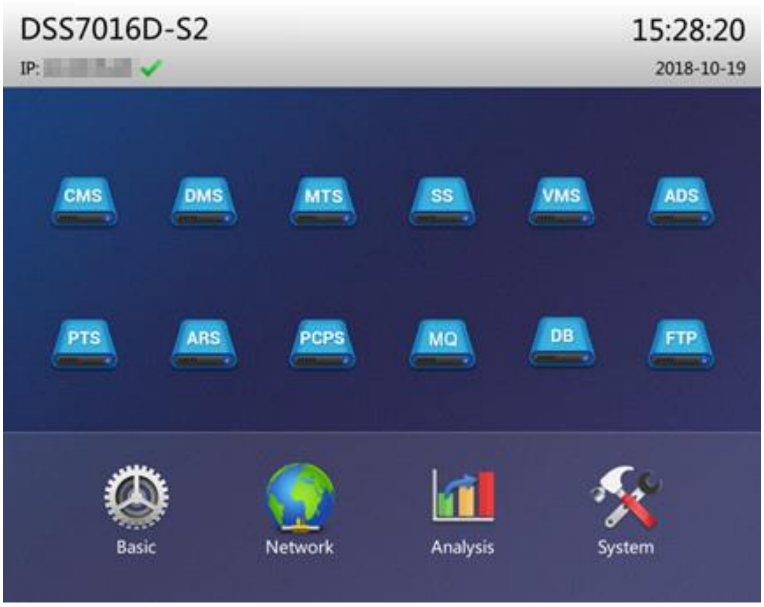


Figure 2-2 Local interface



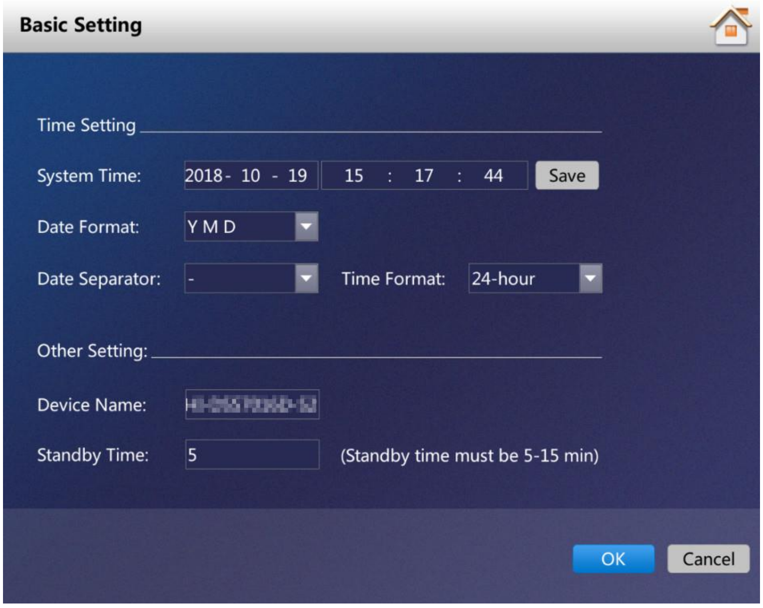
2.2 System Configuration

2.2.1 Basic Settings

Configure basic settings for the server.

Click **Basic Setting** on the local interface. The **Basic Setting** interface is displayed. See Figure 2-3. For details, see Table 2-1.

Figure 2-3 Basic settings



Basic Setting

Time Setting

System Time: 2018- 10 - 19 15 : 17 : 44

Date Format: Y M D

Date Separator: -

Time Format: 24-hour

Other Setting:

Device Name: [redacted]

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

Table 2-1 Parameter description

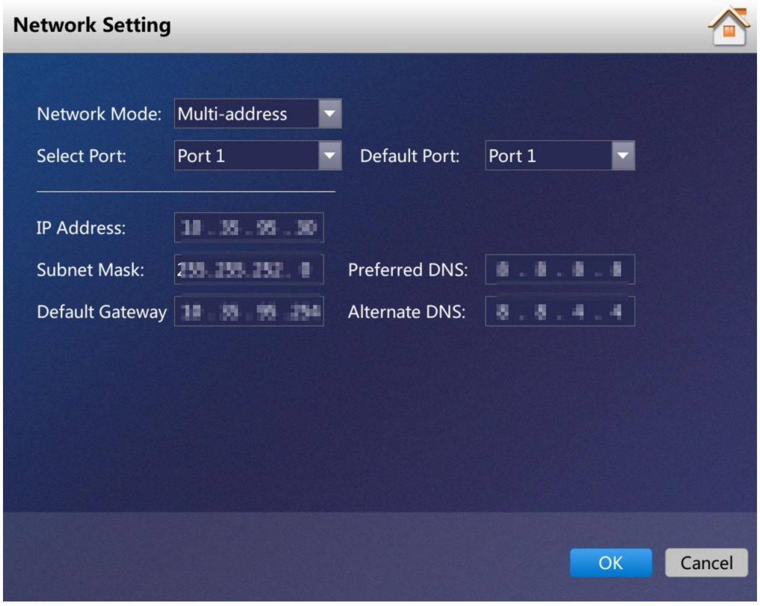
Parameter	Description
System Time	Keep it the same as local time.
Date Format	Date and time format of the local system.
Date Separator	
Time Format	
Device Name	It is the current product mode name by default.
Standby Time	Set the inactivity duration for automatically switching to the standby status. It is 5 minutes by default and cannot exceed 15 minutes.

2.2.2 Network Settings

Configure network settings for the server.

Click **Network Setting** on the local interface. The **Network Setting** interface is displayed. See Figure 2-4. For details, see Table 2-2.

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] Preferred DNS: [redacted]

Default Gateway [redacted] Alternate DNS: [redacted]

Table 2-2 Description

Parameter	Description
Network Mode	The following 4 modes are available. ● Multi-address Multiple network card (hereinafter referred to as NIC) mode. You can configure different network parameters for different NICs to achieve high network reliability. For example, to configure hot spare, the NIC 2 can be used to set spare server IP. This can also be used in ISCSI storage expansion solution. When setting ISCSI storage expansion, NIC 1 can be used for communication, NIC 2 is reserved and NIC 3 and NIC 4 can be used for ISCSI storage. ● Fault tolerance Multiple NICs share one IP. Normally, one of them works. When the working NIC fails, another one will automatically take over the job to ensure network stability. ● Load balancing Multiple NICs share one IP and work at the same time to share the network load, providing greater network capacity than the single NIC mode. When one of them fails, the network load will be re-distributed among the rest NICs to ensure network stability. ● Link Aggregation Bind NICs so that all the bound NICs work at the same time and share network load. For example, bind two NICs and set multi-address for the other two NICs. Then the server has three IPs. The bandwidth of the two bound NICs is 2K and the other two are 2K respectively. This is applicable to stream forwarding, not storage.
Select Port	Set the default network port for the server. It is Network Port 1 by default. You can modify the default port as needed. 📖 After ten gigabit optical port is selected, only multi-address can be available.

Parameter	Description
Default Port	Select the default NIC which will forward the data packet from non-adjacent segment (such as WAN).
IP Address	Select an NIC, and then 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	

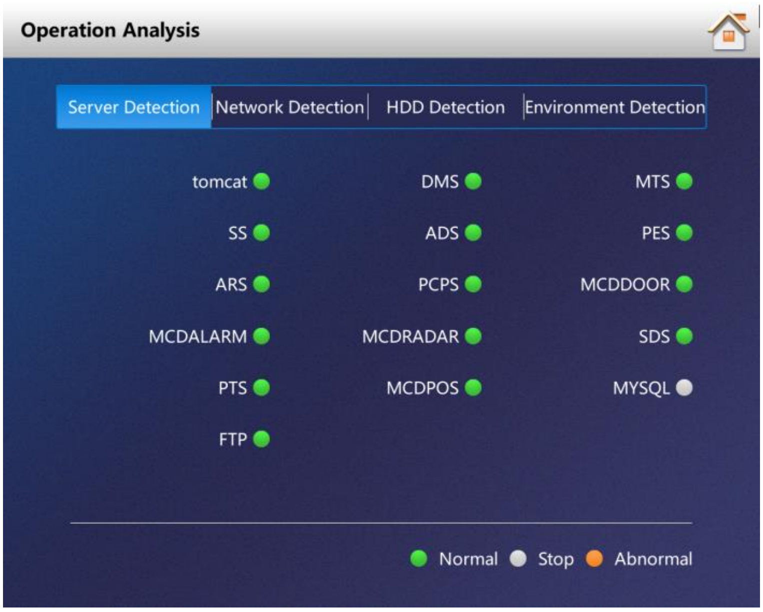
2.3 Operation Management

2.3.1 Operation Analysis

View the status of platform server, network, HDD and environment.

Click **Operation Analysis** on the local interface. The **Operation Analysis** interface is displayed. See the following figures. For details, see Table 2-3.

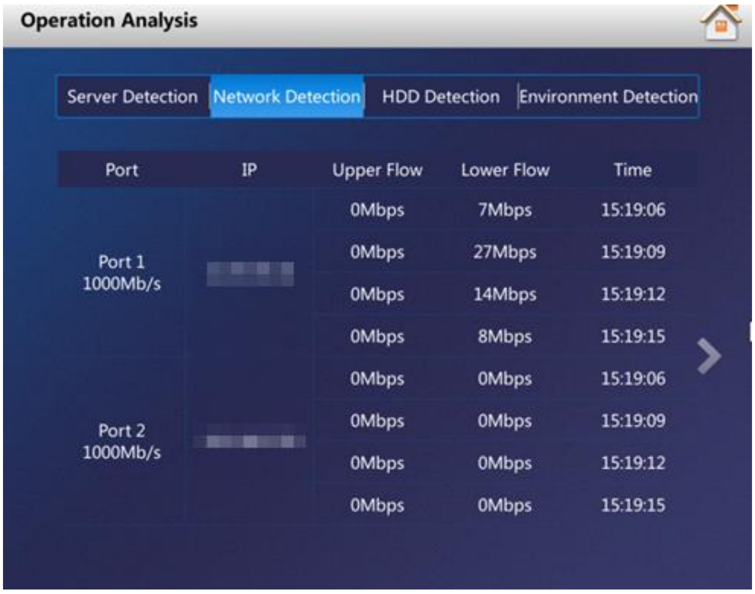
Figure 2-5 Operation Analysis (1)



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

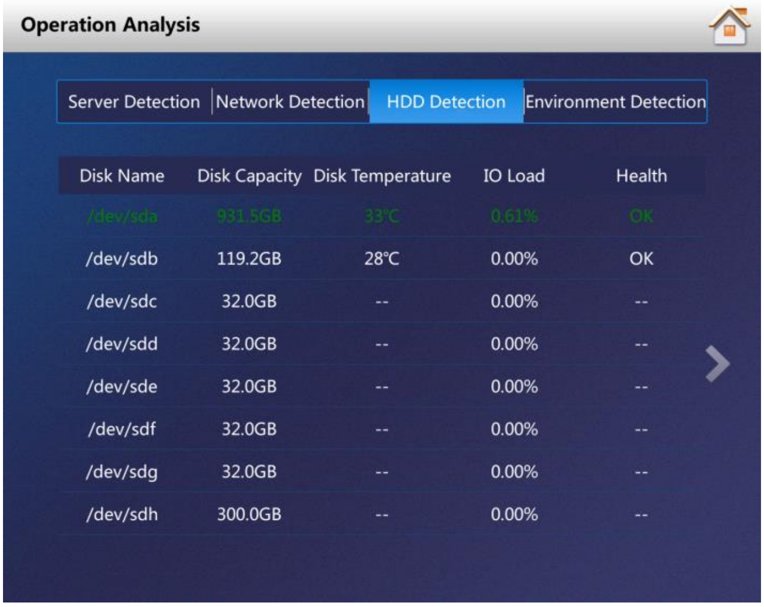
● Normal ○ Stop ● Abnormal

Figure 2-6 Operation Analysis (2)



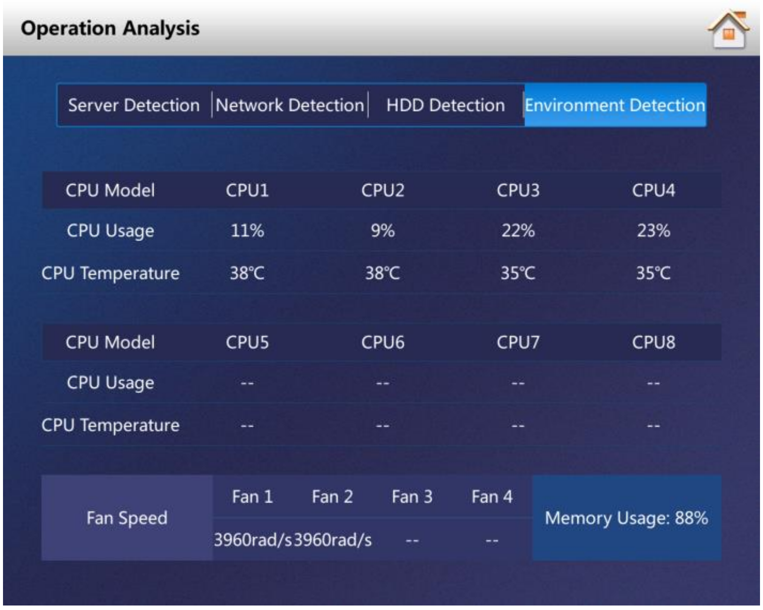
Port	IP	Upper Flow	Lower Flow	Time
Port 1 1000Mb/s	[redacted]	0Mbps	7Mbps	15:19:06
		0Mbps	27Mbps	15:19:09
		0Mbps	14Mbps	15:19:12
		0Mbps	8Mbps	15:19:15
Port 2 1000Mb/s	[redacted]	0Mbps	0Mbps	15:19:06
		0Mbps	0Mbps	15:19:09
		0Mbps	0Mbps	15:19:12
		0Mbps	0Mbps	15:19:15

Figure 2-7 Operation Analysis (3)



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%	--

Figure 2-8 Operation Analysis (4)



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

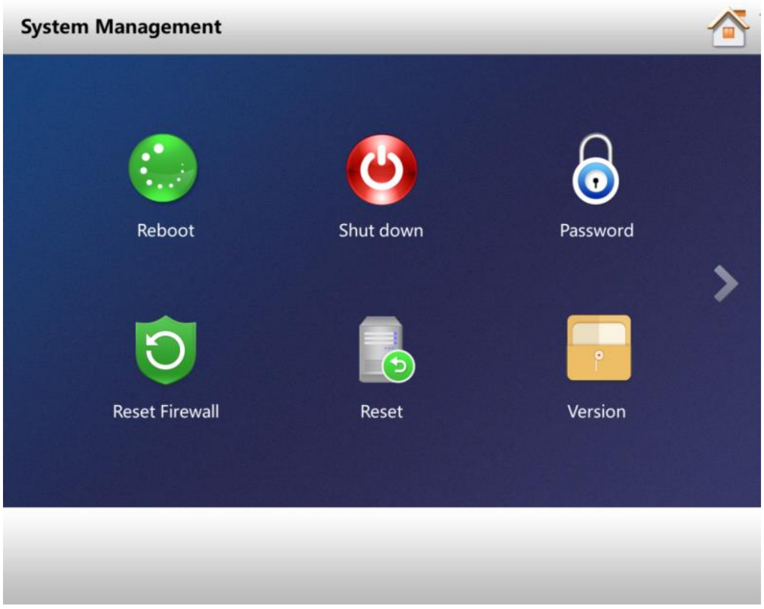
Table 2-3 Description

Detections	Description
Server Detection	Real-time detection of the status of platform server, such as normal, stop and abnormal.
Network Detection	Real-time detection of both upper and lower flow of physical network port.
HDD Detection	Real-time detection of disk capacity, temperature, I/O load and health.
Environment Detection	Real-time detection of CPU temperature, usage, fan speed and memory usage of current platform.

2.3.2 System Management

Click **System Management** at the local interface, and then you can reboot, shut down, reset password, or reset firewall settings. See Figure 2-9. For details, see Table 2-4.

Figure 2-9 System management



System Management

Table 2-4 Description

Operation	Description
Reboot	Save system data before reboot.
Shut down	Save system data before shutting down.
Password	Reset current password.
Reset Firewall	Enable SSH (22) port to avoid whitelist configuration error of the Config System or access failure to the platform.
Version	View product model, product serial number, product ID and system version.

3 Config System

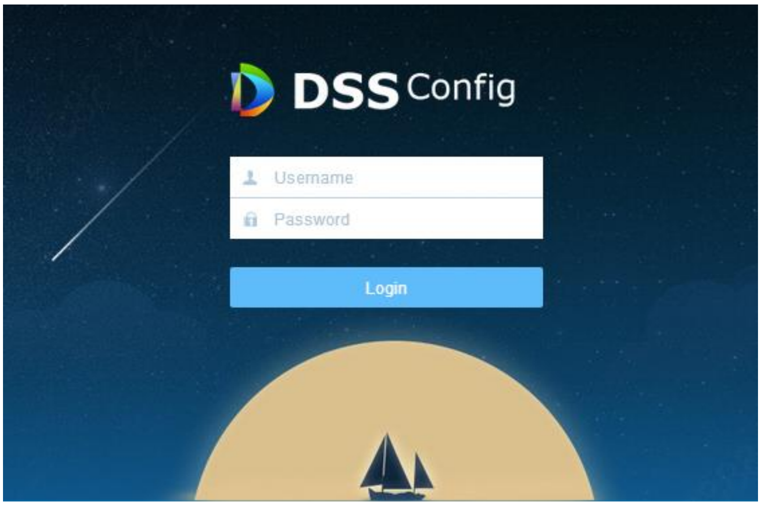
The local system only provides basic configurations, such as time, language, network and quick management. Log in to the Config System for further configurations of service, cluster, storage, linkage, map, database and security. For details, see *User's Manual*.

Enter http://IP/config in the address bar of browser to go to the Config System. The login interface is displayed. See Figure 3-1.

📖

- Server default IP address is 192.168.1.108, default username is admin, and default password is 123456.
- Follow the on-screen instructions to finish system initialization for first-time login.

Figure 3-1 Log in to Config 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.