

DSS4004S2 Quick Start Guide

V1.0.1

Cybersecurity Recommendations

Mandatory actions to be taken towards cybersecurity

1. Change Passwords and Use Strong Passwords:

The number one reason systems get “hacked” is due to having weak or default passwords. It is recommended to change default passwords immediately and choose a strong password whenever possible. A strong password should be made up of at least 8 characters and a combination of special characters, numbers, and upper and lower case letters.

2. Update Firmware

As is standard procedure in the tech-industry, we recommend keeping NVR, DVR, and IP camera firmware up-to-date to ensure the system is current with the latest security patches and fixes.

“Nice to have” recommendations to improve your network security

1) Change Passwords Regularly

Regularly change the credentials to your devices to help ensure that only authorized users are able to access the system.

2) Enable IP Filter

Enabling your IP filter will prevent everyone, except those with specified IP addresses, from accessing the system.

3) Forward Only Ports You Have to Use

As for the platform deployed inside the fire wall, it has to reduce the quantity of port mapping on the fire wall. It is recommended to only map the ports which have to be used by platform and other ports are prohibited.

4) UPnP

- UPnP will automatically try to forward ports in your router or modem. Normally this would be a good thing. However, if your system automatically forwards the ports and you leave the credentials defaulted, you may end up with unwanted visitors.
- If you manually forwarded the HTTP and TCP ports in your router/modem, this feature should be turned off regardless. Disabling UPnP is recommended when the function is not used in real applications.

5) SNMP

Disable SNMP if you are not using it. If you are using SNMP, you should do so only temporarily, for tracing and testing purposes only.

6) Multicast

Multicast is used to share video streams between two recorders. Currently there are no known issues involving Multicast, but if you are not using this feature, deactivation can enhance your network security.

7) Physically Lock Down the Device

Ideally, you want to prevent any unauthorized physical access to your system. The best way to achieve this is to install the recorder in a lockbox, locking server rack, or in a room that is behind a lock and key.

8) Isolate NVR and IP Camera Network

The network your NVR and IP camera resides on should not be the same network as your public computer network. This will prevent any visitors or unwanted guests from getting access to the same network the security system needs in order to function properly.

General



The following document is used to guide users to know the checklist, installation and configuration etc. of DSS general surveillance management platform.

Models

DSS7016D-S2, DHI-DSS7016DR-S2, DSS7016D-S2 and 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

No.	Version	Revision Content	Release Time
1	V1.0.0	First Release.	Aug. 1st. 2018
2	V1.0.1	Add local application and delete initialization config.	Oct. 25 th . 2018

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 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 disassemble 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

Cybersecurity Recommendations	I
Foreword	III
Important Safeguards and Warnings	V
1 Checklist.....	1
1.1 Package.....	1
1.2 Port Definition	1
1.2.1 Front Panel	2
1.2.2 Rear Panel.....	2
1.3 Device Installation	3
2 Local Application.....	4
2.1 Function Architecture.....	4
2.2 Business Config.....	5
2.2.1 Basic Setting.....	5
2.2.2 Network Setting	5
2.3 Operation Management.....	8
2.3.1 Operation Analysis.....	8
2.3.2 System Management.....	9
3 Config System	10

1.1 Package

Open product package to check, pay attention to product package, product unit and accessories. 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 match actual product and are complete. Actual accessories have no damage.



After you have checked that material and accessories are complete, please well store them for emergency use.

Table 1-1

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

1.2 Port Definition

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

1.2.1 Front Panel

Figure 1-1



Table 1-2

No.	Port or Tag	Definition
1	Network Indicator	The blue light flashes when network is connected.
2	Alarm Indicator	The blue light flashes 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 inserted.
5	HDD3	
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 to shut it down.

1.2.2 Rear Panel

Figure 1-2

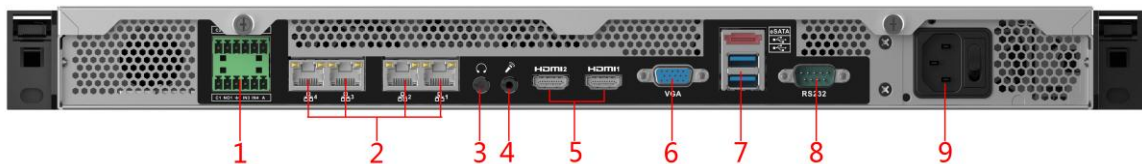


Table 1-3

No.	Port or Tag	Definition
1	Alarm Output and Input	Reserved. Supports RS485 protocol access.
2	Ethernet Port	Supports 10Mbps/100Mbps/1Gbps self-adaptive dual full duplex, platform default Ethernet port 1.
3	Audio Output	3.5mm audio output.
4	Audio Intercom Input	3.5mm 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	RS232	Debugging serial port.
9	Single Power	AC 100V - 240V/47 - 63Hz; Supports hot swap.

1.3 Device Installation

Connect cable according to port introduction, and then connect to power.

2

Local Application

2.1 Function Architecture

The chapter is to introduce the functions of the local application. See Figure 2-1. The local interface will be displayed after it starts up. See Figure 2-2.

Figure 2-1

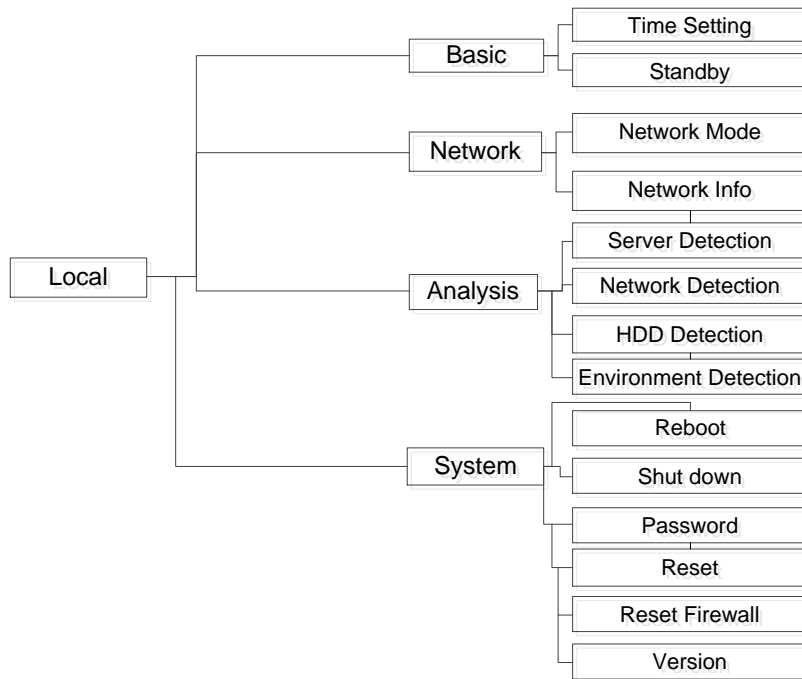
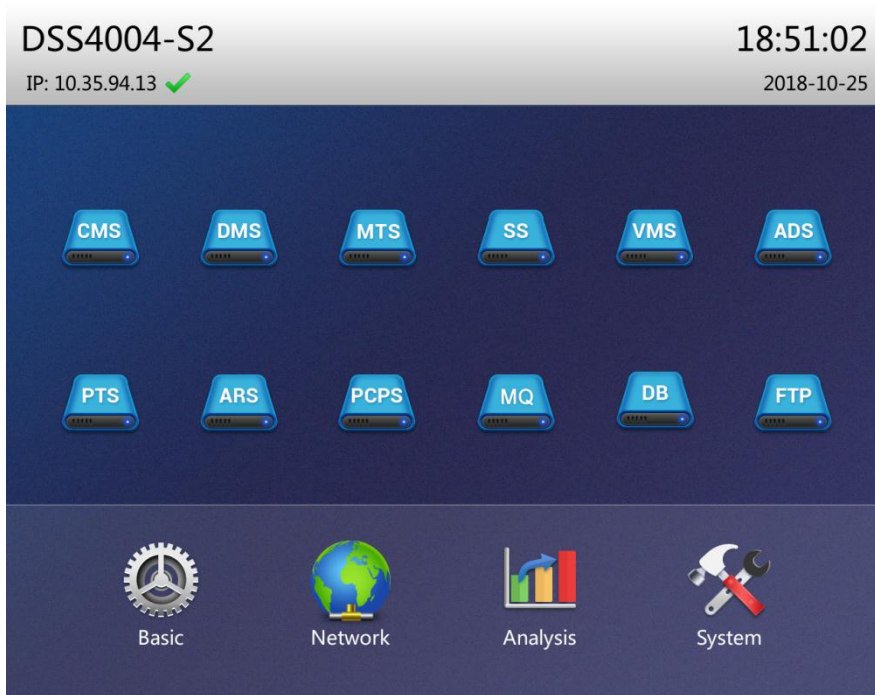


Figure 2-2



2.2 Business Config

2.2.1 Basic Setting

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

Figure 2-3 Basic setting

The screenshot shows the 'Basic Setting' configuration interface. It includes sections for 'Time Setting' and 'Other Setting'. The 'Time Setting' section contains fields for 'System Time' (2018-10-25 18:45:05), 'Date Format' (Y M D), 'Date Separator' (-), and 'Time Format' (24-hour). The 'Other Setting' section contains fields for 'Device Name' (DSS4004-S2) and 'Standby Time' (5 minutes). A 'Save' button is located next to the 'System Time' field. At the bottom right, there are 'OK' and 'Cancel' buttons.

Table 2-1 Basic setting parameter description

Parameter	Description
System Time	Keep it the same as local time.
Date Format	It mainly focuses on data and time format of local application homepage, and it is adjusted according to user experience.
Date Separator	
Time Format	
Device Name	It is the current product mode name by default. Supports customized English model but not Chinese input.
Standby Time	It is the duration from when the local interface is not operated to standby status, 5 minutes by default and it doesn't exceed max 15 minutes.

2.2.2 Network Setting

Click Network Setting on the local interface, enter the network setting interface and configure network information.

Figure 2-4 Network setting

Network Setting

Network Mode: Multi-address

Select Port: Port 1 Default Port: Port 1

IP Address: 10 . 35 . 95 . 30

Subnet Mask: 255 . 255 . 252 . 0 Preferred DNS: 8 . 8 . 8 . 8

Default Gateway 10 . 35 . 95 . 254 Alternate DNS: 8 . 8 . 4 . 4

OK Cancel

Table 2-2 Basic setting parameter description

Parameter	Note
-----------	------

Parameter	Note
Network Mode	<p>Supports following 4 modes.</p> <ul style="list-style-type: none"> Multi-address <p>It is the multi-network card mode; multiple network cards can configure different segments and realize multi-segment access, which is suitable for the scenario with high requirement of network reliability. For example, configuring dual hot standby needs to use network card 2 to configure 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 used as service communication, network port 2 reserved, network port 3 and 4 are used as ISCSI storage.</p> <ul style="list-style-type: none"> Fault tolerance <p>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.</p> <ul style="list-style-type: none"> Load balancing <p>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.</p> <ul style="list-style-type: none"> Link Aggregation <p>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, other 2 multi-address, then the server owns 3 IP, the bound IP bandwidth is 2K while other 2 is 1K; It can be applied to the scenario with forward-only stream (storage is not recommended). Link aggregation can be realized only when link aggregation is supported by directly-connected switch.</p>
Select Port	Supports default network port config, The platform default is Network Port 1 (after 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, 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	

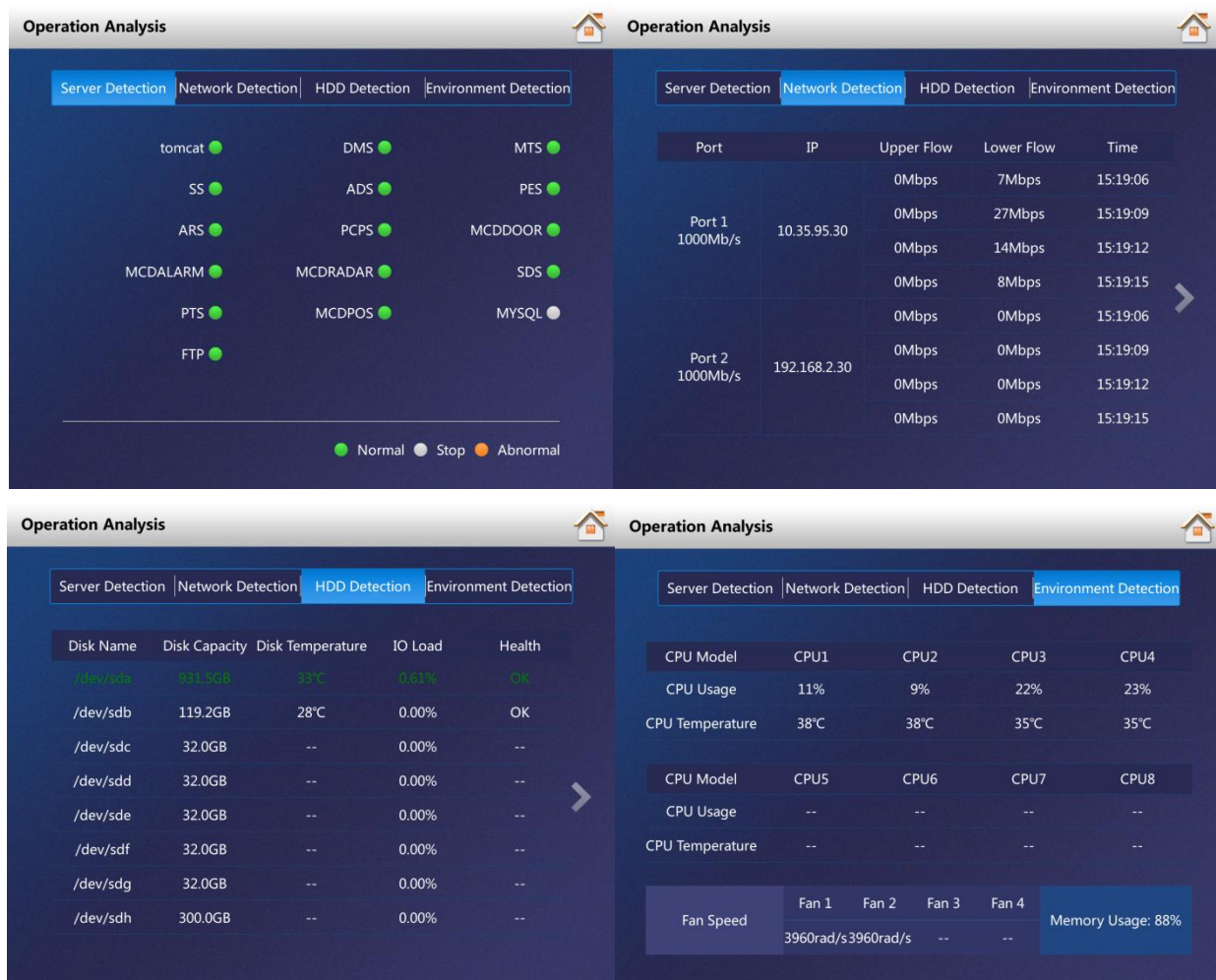
2.3 Operation Management

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 both upper and lower flow of physical network port.
- **HDD Detection:** Realizes real-time detection of disk capacity, temperature, IO load and health. The green line displays the above parameters of HDD by default.
- **Environment Detection:** Realizes real-time detection of CPU temperature, usage, fan speed and memory usage of current platform.

Figure 2-5 Operation analysis

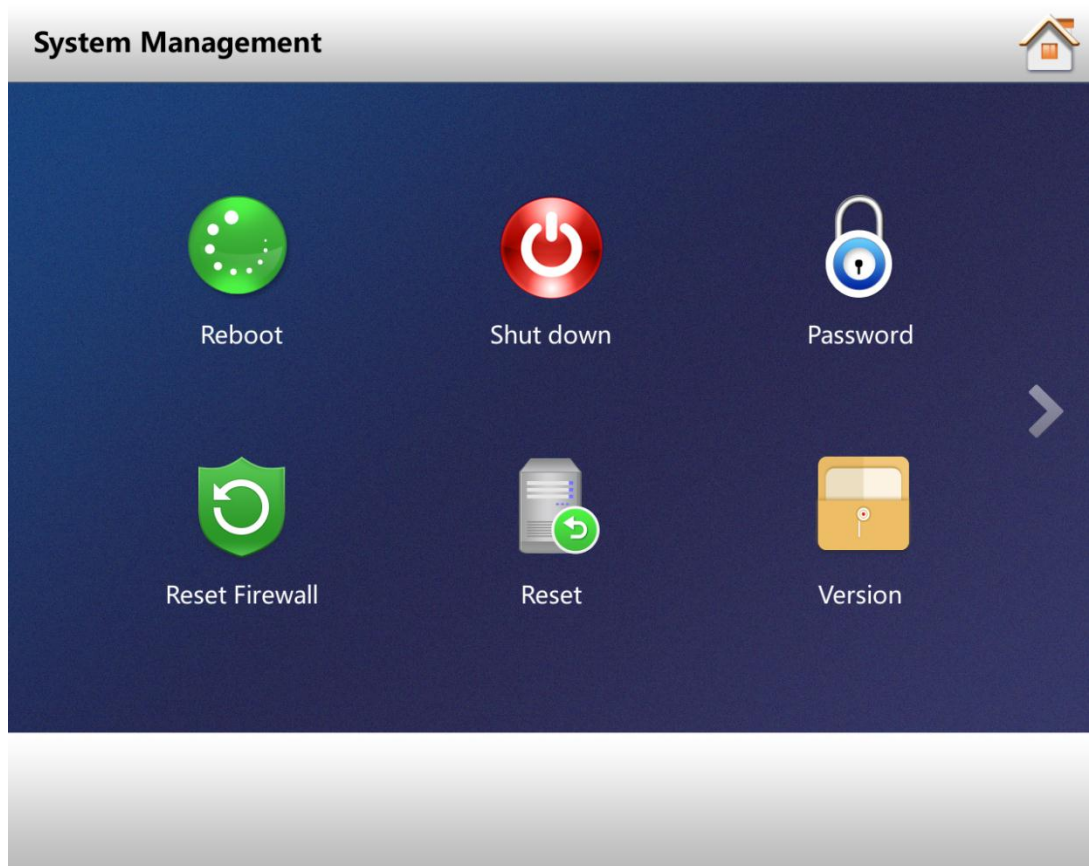


2.3.2 System Management

Click System Management at the local interface. It supports following operations.

- Reboot: Please save system data before reboot.
- Shut down: Please save system data before shut it down. It is forbidden to power off directly.
- Password: Reset the current password as initialization password for admin, config system, system, FTP and database.
- Reset Firewall: Enable SSH (22) port again, avoid whitelist config error of config system and cause access failure of platform.
- Version: Displays planning product model, product serial number, product ID and system version.

Figure 2-6



3 Configuring System

The server's local application only provides basic configurations, such as time, language, network and quick management etc. It supports primary status operation and analysis in stand-alone environment. Please log in config system for deeper configurations of service, cluster, storage, linkage, map, database and security etc. Please refer to server user's manual for more details.

Access address of config system is <http://IP/config>.



- Server default IP address is 192.168.1.108, default username is admin, default password is 123456.
- Please finish initialization according to system prompt for first login.

Figure 3-1

