

DSS Matrix Surveillance Platform

Application Deployment Manual

V1.0.0

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. Change Default HTTP and TCP Ports:

- Change default HTTP and TCP ports for systems. These are the two ports used to communicate and to view video feeds remotely.
- These ports can be changed to any set of numbers between 1025-65535. Avoiding the default ports reduces the risk of outsiders being able to guess which ports you are using.

3. Enable HTTPS/SSL:

Set up an SSL Certificate to enable HTTPS. This will encrypt all communication between your devices and recorder.

4. Enable IP Filter:

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

5. Change ONVIF Password:

On older IP Camera firmware, the ONVIF password does not change when you change the system’s credentials. You will need to either update the camera’s firmware to the latest revision or manually change the ONVIF password.

6. Forward Only Ports You Need:

- Only forward the HTTP and TCP ports that you need to use. Do not forward a huge range of numbers to the device. Do not DMZ the device's IP address.
- You do not need to forward any ports for individual cameras if they are all connected to a recorder on site; just the NVR is needed.

7. Disable Auto-Login on SmartPSS:

Those using SmartPSS to view their system and on a computer that is used by multiple people should disable auto-login. This adds a layer of security to prevent users without the appropriate credentials from accessing the system.

8. Use a Different Username and Password for SmartPSS:

In the event that your social media, bank, email, etc. account is compromised, you would not want someone collecting those passwords and trying them out on your video surveillance system. Using a different username and password for your security system will make it more difficult for someone to guess their way into your system.

9. Limit Features of Guest Accounts:

If your system is set up for multiple users, ensure that each user only has rights to features and functions they need to use to perform their job.

10. 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.

11. 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.

12. 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.

13. Check the Log:

If you suspect that someone has gained unauthorized access to your system, you can check the system log. The system log will show you which IP addresses were used to login to your system and what was accessed.

14. 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.

General









This user's manual (hereinafter referred to be "the Manual") introduces the functions and operations of the DSS (hereinafter referred to be "the Device").

Models

DSS4004-S2

Safety Instructions

The following categorized signal words with defined meaning 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, may result in property damage, data loss, lower performance, or unpredictable result.
 ELECTRICITY	Indicates dangerous high voltage. Take care to avoid coming into contact with electricity.
 LASER BEAM	Indicates a laser radiation hazard. Take care to avoid exposure to a laser beam.
 ESD	Electrostatic Sensitive Devices. Indicates a device that is sensitive to electrostatic discharge.
 TIPS	Provides methods to help you solve a problem or save you time.
 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.	August 1, 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

Electrical safety

- All installation and operation here should conform to your local electrical safety codes.
- The product must be grounded to reduce the risk of electric shock.

We assume no liability or responsibility for all the fires or electrical shock caused by improper handling or installation.

Transportation security

Heavy stress, violent vibration or water splash are not allowed during transportation, storage and installation.

Installation

- Keep upwards. Handle with care.
- Do not apply power to the Device before completing installation.
- Do not place objects on the Device.

Qualified engineers needed

All the examination and repair work should be done by the qualified service engineers. We are not liable for any problems caused by unauthorized modifications or attempted repair.

Environment

The Device should be installed in a cool, dry place away from conditions such as direct sunlight, inflammable substances, and explosive substances.

Accessories

- Be sure to use all the accessories recommended by manufacturer.
- Before installation, please open the package and check all the components are included.
- Contact your local retailer ASAP if something is broken in your package.

Lithium battery

- Improper battery use might result in fire, explosion, or personal injury.
- When replacing the battery, please make sure you are using the same type. Risk of explosion if battery is replaced by an incorrect type.
- Dispose of used batteries according to the instructions.

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
2 Config System	4
2.1 Login and Initialize Config System	4
2.2 Ethernet Config.....	5
3 Config DSS Client	8
3.1 Download and Install Client.....	8
3.2 Log in Client.....	10
3.3 Initialize Client	10

1.1 Package

Open product package to check, pay attention on 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 on 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	Description
1	Server Device	1
2	Hard Disk Anti-Seismic Screw	12
3	Seismic Mat	12
4	Power Line	1, 1.5m
5	Application Deployment Manual	1

1.2 Port Definition

Product front panel has power button, USB port and status indicator (system disk, alarm and network); rear panel has single power, Ethernet cable, serial and other ports, and reserved alarm port, HDMI and function expansion port.

1.2.1 Front Panel

Figure 1-1



Chart 1-1

No.	Port or Tag	Definition
1	Network Light	Blue light flash during connection
2	Alarm Light	Blue light flash when alarm occurs (i.e. no HDD)
3	HDD1	HDD light, normally ON after HDD is inserted
4	HDD2	
5	HDD3	
6	HDD4	
7	USB2.0 Port	2, white
8	Power Button	Press the button to boot device. Self-carried power status light (blue light is normally ON); long press to shut down.

1.2.2 Rear Panel

Figure 1-2

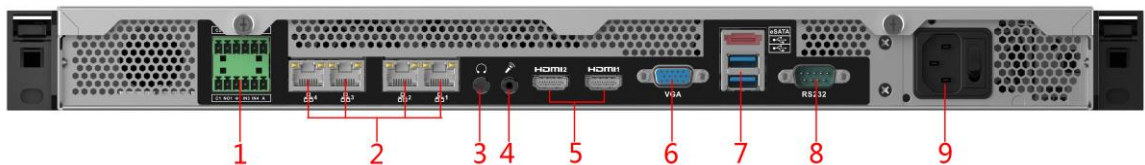


Chart 1-2

No.	Port or Tag	Definition
1	Alarm Output, Input	Reserved, support RS485 protocol input
2	Ethernet Port	Support 10Mbps/100Mbps/1Gbps self-adaptive dual full duplex, platform default Ethernet port 1
3	Audio Output	3.5mm audio input
4	Video Intercom Input.	3.5mm audio input
5	HDMI Port	2-ch, reserved
6	VGA Port	DB15-pin, support VGA port device input

No.	Port or Tag	Definition
7	eSATA Port	Support USB2.0, USB3.0 port device input
8	RS232	Debug serial
9	Single Power	AC 100V - 240V/47 - 63Hz, support hot swat

2 Config System

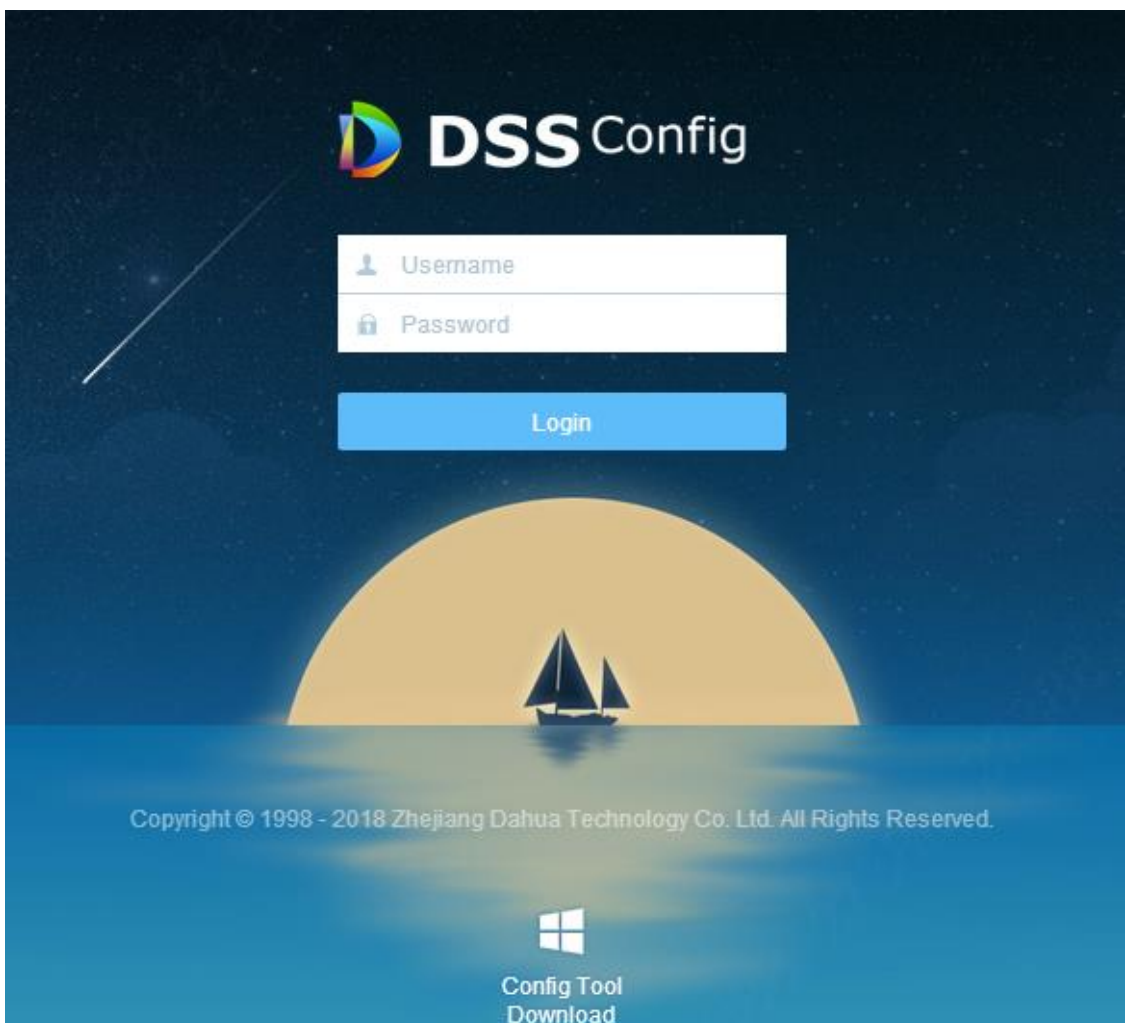
2.1 Login and Initialize Config System



Make sure PC and server are in the same network segment, if not, please change IP address of PC. Default server IP is 192.168.1.108.

Step 1 In Internet Explorer, enter “DSS platform IP address/config”, click Enter.
See Figure 2-1.

Figure 2-1



Step 2 Enter username and password (default username is admin, and default password is 123456), click Login. See

Figure 2-2

Reset Password

Reset Password

Old Password:

New Password:

Confirm:

Security Question

Security Question 1:

Answer:

Security Question 2:

Answer:

Security Question 3:

Answer:

OK

Step 3 Enter old password, new password and set three security questions.

Step 4 Click OK.

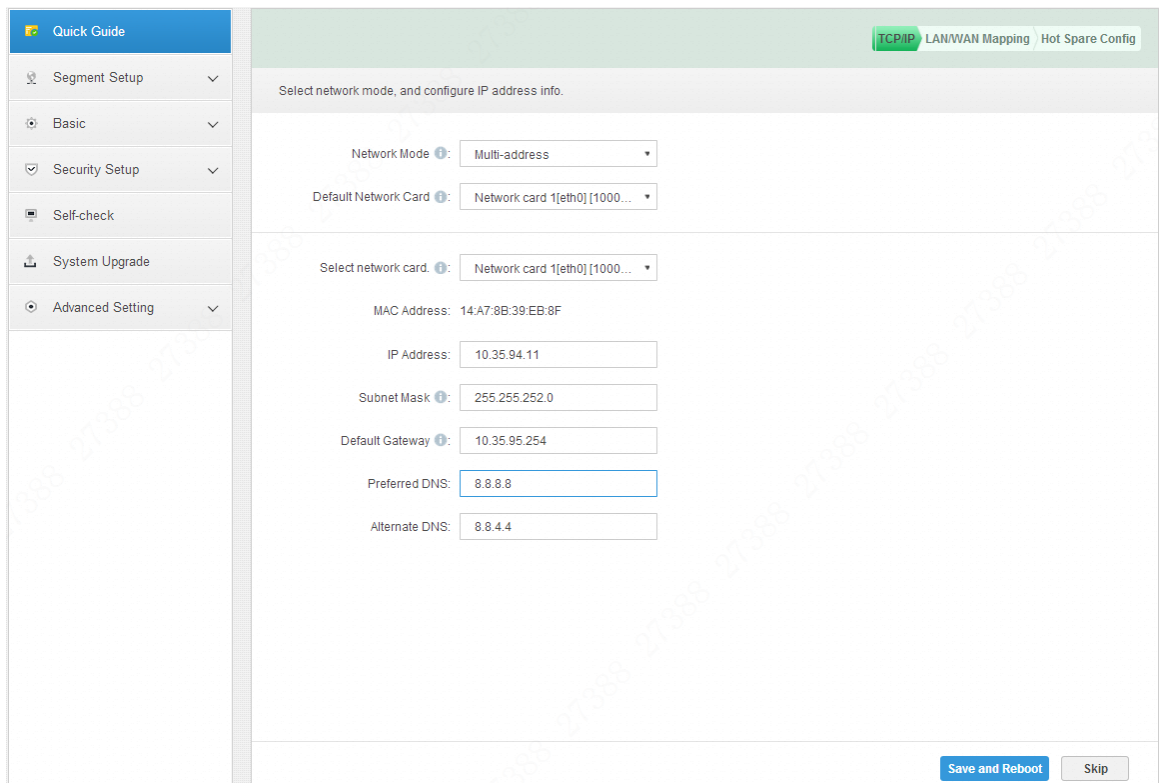
Server reboots, you shall log in again.

2.2 Ethernet Config

Select Ethernet mode and set IP info.

Step 1 Click Guide or Network Setup, see Figure 2-3.

Figure 2-3



Step 2 Set Ethernet parameter, see Table 2-1.

Table 2-1

Parameter	Note
Network Mode	<ul style="list-style-type: none"> ● Multiple Address As multi-Network card mode. Multiple Network card can set different segments to achieve access of multiple segments, suitable for scenes demanding highly reliable connection. For example: set dual hot spare device, which need Network card 2 configured spare beat IP; as well as use in plan with ISCSI expansion storage. While, plan of network port: Port 1 for server communication, Port 2 as reserved, Port 3 and Port 4 for ISCSI storage. ● Fault-tolerant Multiple Network cards use the same IP address, in general, only one Network card is working. When working Network card has fault, it auto enables another normal Network card to ensure fluency of work. ● Balance Load Multiple Network cards uses the same IP, and these Network cards take part in work at the same time, sharing network loading, with capacity exceeding a single Network card bandwidth. When an Network card is abnormal, it re-loads loading to other available Network card to improve connection reliability.

Parameter	Note
	<ul style="list-style-type: none"> ● Link <p>By binding Ethernet and external communication, now bound Ethernet port take part in work to share network loading. It achieves one Network card forwarding higher than 1K stream. For example, 2 IP are bound, and other two are multiple address. So this server can have 3 IP, bound IP with bandwidth of 2K. the other two is 1K; for scene of pure forwarding stream (not recommend to store).</p>
Network card	<p>When network mode setup is fault-tolerant, balance load or link, you shall set binding of Network card.</p> <p>Click "Add Bind Card", select Network card you want to bind, and set two bound cards.</p>
Default Network card	Select default Network card, this card will be default port forwarding to non-adjacent segments (i.e. WAN) data pack.
Select Network card	Select Network card or bind card, you can see this Network card or binding card info below.
MAC Address	Show platform server MAC address.
IP Address	After you select Network card, you can set IP address, subnet mask, default gateway, preferred DNS server address and alternate DNS server address of this Network card.
Subnet Mask	
Default Gateway	
Preferred DNS	
Alternate DNS	

Step 3 Click Save and Reboot to save config and reboot server.

3


Config DSS Client

3.1 Download and Install Client

Step 1 In Internet Explorer, enter DSS platform IP address, and click Enter. See Figure 3-1.

Figure 3-1



Step 2 Click  to download installation pack.

Client installation pack name is "DSSClient.exe".

Step 3 Double click installation pack to enter installation mode, see 错误!未找到引用源。 .
According to instructions, install the client, and see

Figure 3-2

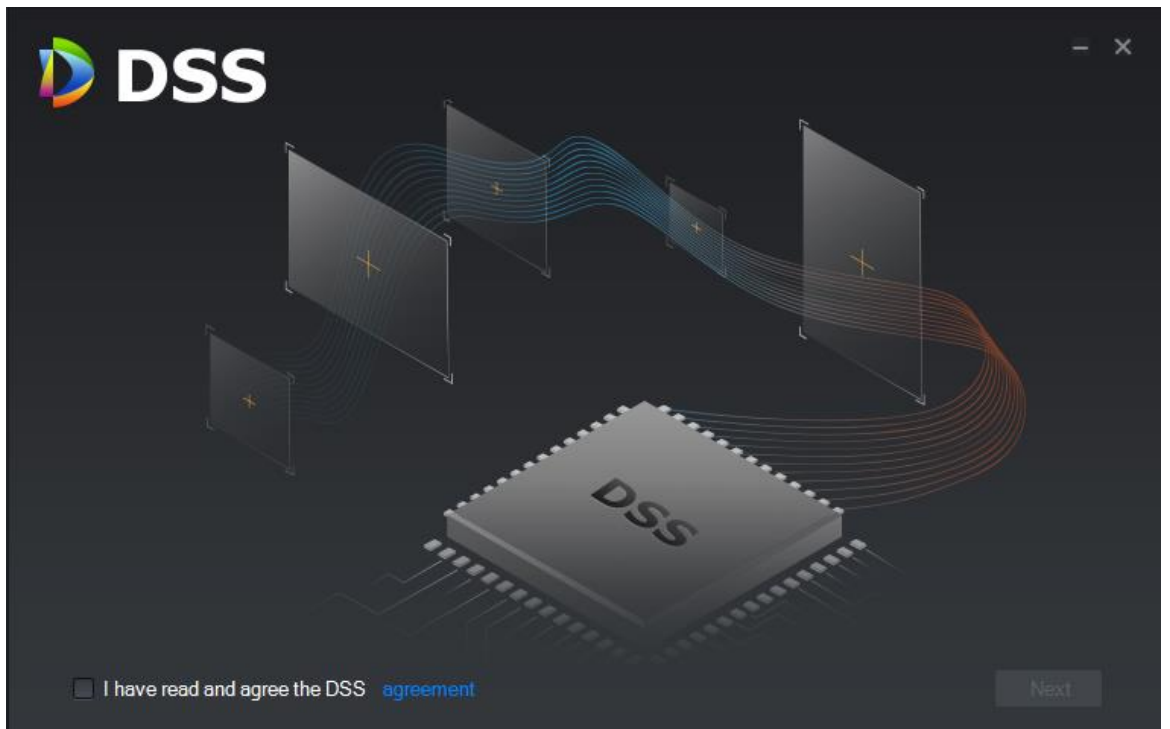
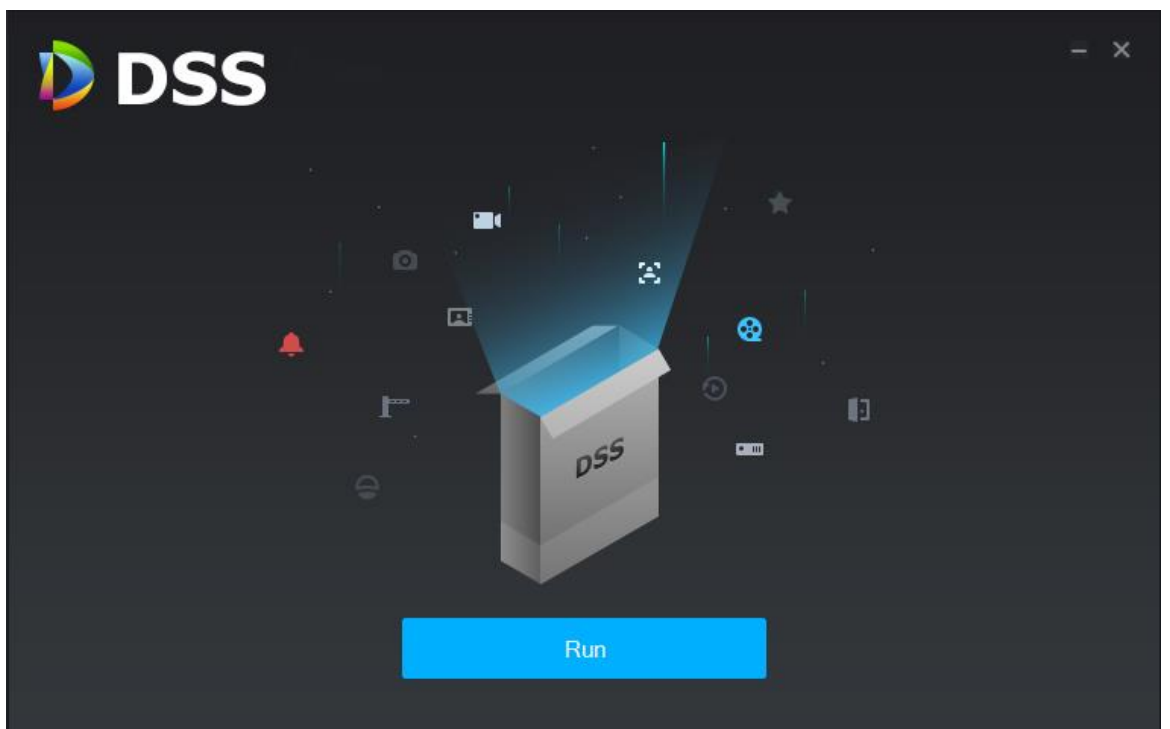


Figure 3-3



3.2 Log in Client




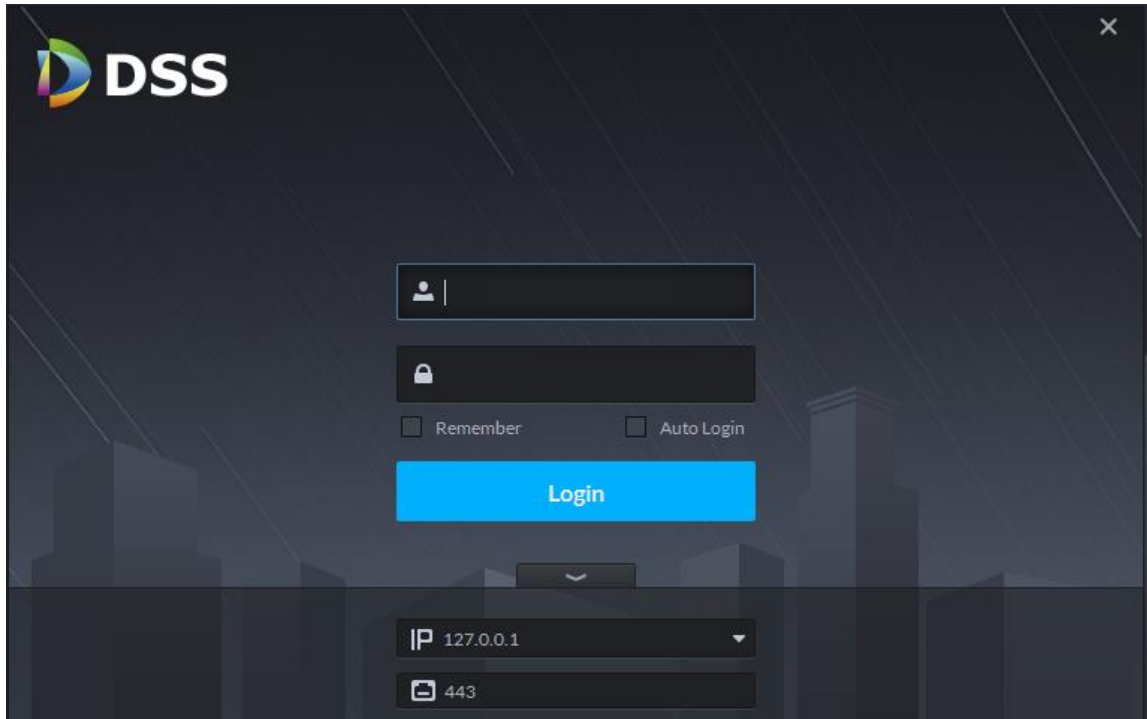
Step 1 When installation is complete, click Run, or double click  icon on desktop. System shows login page, see Figure 3-4.

Figure 3-4



Step 2 Enter username, password, platform IP address and WEB server port. Click Login to enter client page.

 **NOTE**

- Default username is system, default password is 123456. At first time login, you shall initialize username and password.
- WEB server default port is 443. If incorrect, please go to LAN/WAN mapping page to view port no.
- After you select “member password”, when you open client at next time, you are not required to enter password.
- Select “Auto Login”, when you open client at next time, it auto log in client.

3.3 Initialize Client

When you log in for the first time, you shall initialize password and set password security question.

Step 1 Log in client, see Ch 3.2.

System shows password setup page, see Figure 3-5.

Figure 3-5

Initialization

1.Set password 2.Security question

Username: system

Password:

Confirm Password:

Next

Step 2 Enter new password and confirm password, click Next. See Figure 3-6.

Figure 3-6

Initialization

1.Set password 2.Security question

Question 1: Who is your favorite athlete?

Answer:

Question 2: Who is your favorite pop star?

Answer:

Question 3: What is your favorite flower in s...

Answer:

OK

Step 3 Select 3 questions, and set answer, click OK to enter client homepage.