



DSS

Upgrade Guide



Foreword

General

This manual introduces how to upgrade the DSS products.

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, could result in property damage, data loss, lower performance, or unpredictable result.
 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

Version	Revision Content	Release Time
V1.0.0	First release.	May 2021

Table of Contents

Foreword	1
1 Upgrade from V7 to V8.....	1
1.1 Compatible Versions.....	1
1.2 Upgrade Instructions.....	1
1.3 Upgrade Methods.....	1
1.4 Upgrade Operations.....	2
2 Upgrade from V8 Express to V8 Pro	1
2.1 Compatible Version	1
2.2 Upgrade Instructions.....	1
2.3 Upgrade Methods.....	1
2.4 Upgrade Operations.....	1
Appendix 1 Cybersecurity Recommendations	7

1 Upgrade from V7 to V8

This chapter introduces the upgrade procedure from V7 to V8 for Express and Pro.

1.1 Compatible Versions

Product	Original Version	Original Program Name	New Version
DSS Express	V1.000.0000003.0	General_DSS-Express_win32_IS_V1.000.0000003.0.R.20190610.exe	V8.000.0000002.0
	V1.000.0000003.1	General_DSS-Express_win32_IS_V1.000.0000003.1.R.20190817.exe	
	V1.000.0000003.2	General_OverseasDSS-express_win32_IS_V1.000.10GP002.0.R.20210114.exe	
DSS Professional	V7.002.0000005.0	General_DSS-PRO_Win64_IS_V7.002.0000005.0.R.20200414.exe	V8.000.0000002.0
	V7.002.0000005.1	General_DSS-PRO_Win64_IS_V7.002.0000005.1.R.20200703.exe	
	V7.002.0000005.2	General_DSS-PRO_Win64_IS_V7.002.0000005.2.R.20201223.exe	



- There might be risk if you upgrade the program. Make sure that you back up the data before the upgrade to avoid failure and data corruption.
- Upgrade to Express V1.000.0000003.2 or Pro V7.002.0000005.2 before you upgrade to V8.000.0000002.0.

1.2 Upgrade Instructions



V7 Upgrade to
V8.000.0000002.0

Please refer to the form attached above for the situation of each module before and after upgrade.

1.3 Upgrade Methods

- Upgrade to Express V1.000.0000003.2 or Pro V7.002.0000005.2 before you upgrade to V8.000.0000002.0.
- One-click installation is supported for upgrading to V8.000.0000002.0.

- For DSS Pro distributed server, one-click installation upgrade is not supported. You need to uninstall the old program, and then install the latest version.
- For DSS Pro hot-standby system, close Rose software first, and then finish the normal upgrade procedure.

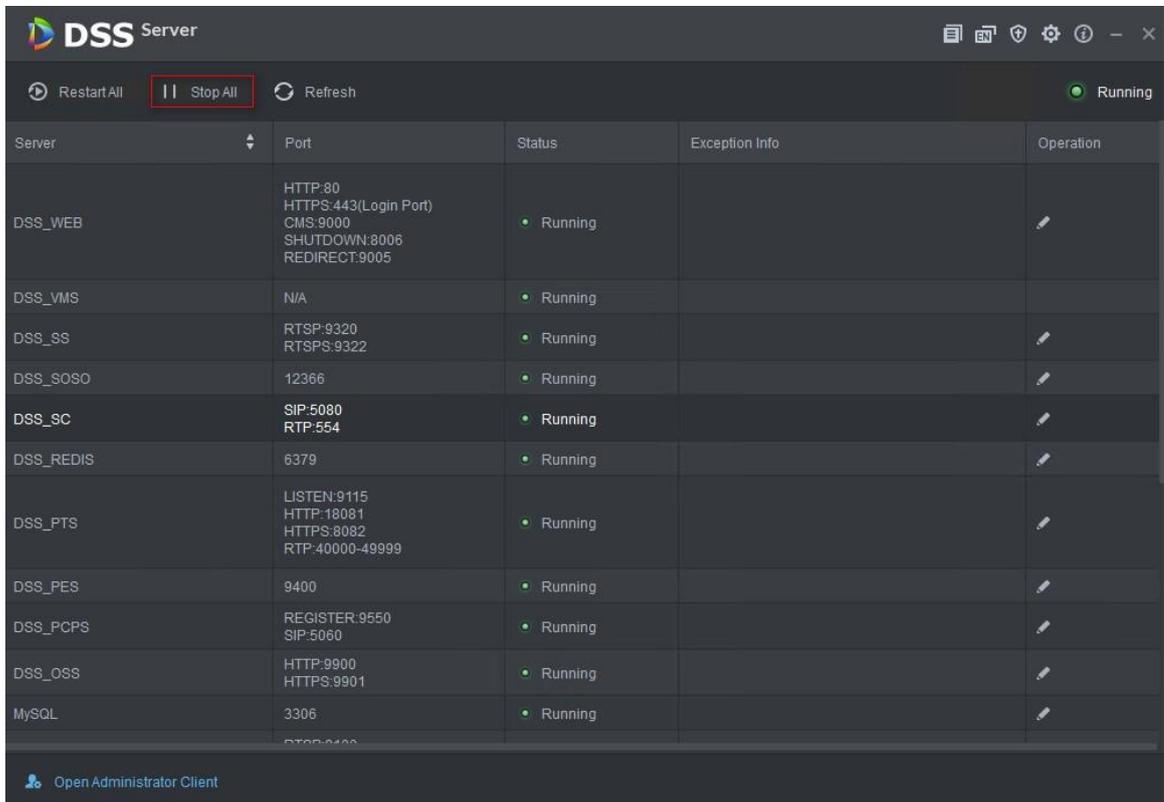
1.4 Upgrade Operations



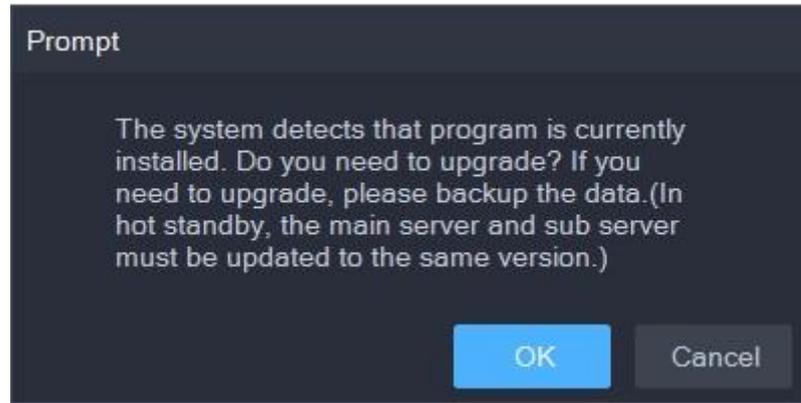
Back up your data before the upgrade to avoid failure and data corruption.

Step 1 Log in to the server of DSS Pro or DSS Express.

Step 2 Double-click  on the desktop, log in to the DSS Server, and then click **Stop All** to stop all services.



Step 3 Double-click the V8.000.0000002.0 installation program.
An upgrade prompt is displayed.

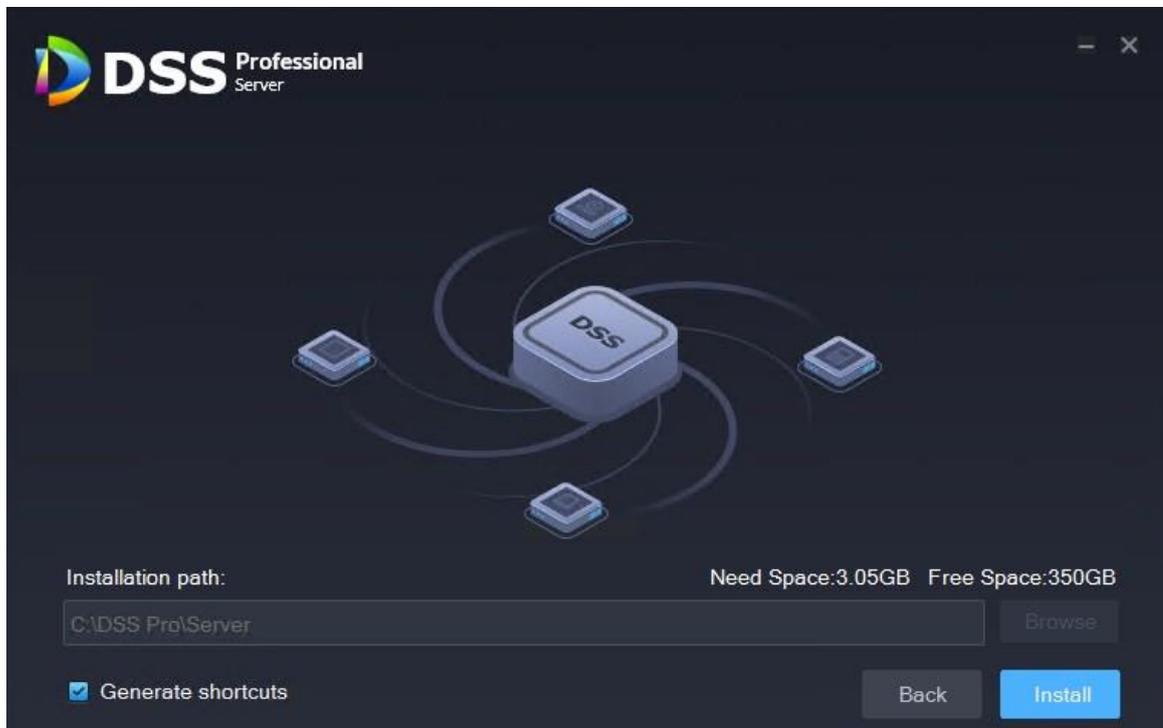


Step 4 Click **OK**.



The installation path of the old version will be detected, and you cannot edit the directory.

Step 5 Click **Install** to start the installation.



Step 6 After installation, click **Run** to run the program.



Step 7 Log in to the system configuration tool to check whether all the services are running properly.



If the word **Running** displays at the upper-right corner, it means all services are running properly. If not, check the status of each service to make sure all services are running properly.

Server	Service Category	Port	Status	Exception Info	Operation
DSS_NGINX	Basic	HTTP:801 HTTPS:443(Login Port)	Running		
DSS_SMC	Basic	HTTP:8000 HTTPS:8443 CMS:9000 SHUTDOWN:8006 REDIRECT:9005	Running		
DSS_HRS	Basic	N/A	Running		
DSS_REDIS	Basic	6379	Running		
MySQL	Basic	3306	Running		
DSS_MQ	Basic	OPENWIRE:61616 MQTT:1883 AMQP:5672 STOMP:61613 JETTY:8161	Running		
DSS_ADS	Basic	9600	Running		
DSS_MTS	Basic	RTSP:9100 RTSPS:9102	Running		
DSS_MGW	Basic	9090	Running		
DSS_SS	Storage	RTSP:9320 RTSPS:9322	Running		

Restart All | Stop All | Refresh | Running

Open Administrator Client

Step 8 Download the Client again.



Because V7 client is incompatible with the V8 client, you need to uninstall V7 client, and install

V8.

Step 9 Re-apply the V8 license and import it to your program.



The figures above is for ProV7.002.0000005.2 upgrading to V8.000.0000000.0, and for reference only.

The procedure also applies to Express upgrade process.

2 Upgrade from V8 Express to V8 Pro

2.1 Compatible Version

This chapter introduces the upgrade procedure from DSS Express V8.000.0000002.0 to DSS Pro V8.000.0000002.0.

2.2 Upgrade Instructions

- If the Express platform is a paid version, back up the license key before the upgrade.
- After DSS Express V8.000.0000002.0 is upgraded to DSS Pro V8.000.0000002.0, all business data is kept.
- After the upgrade, the alarm and face records cannot be displayed. If you need to search for the data, refer to the upgrade operations below. We recommend that you contact technical support to help you with the upgrade.

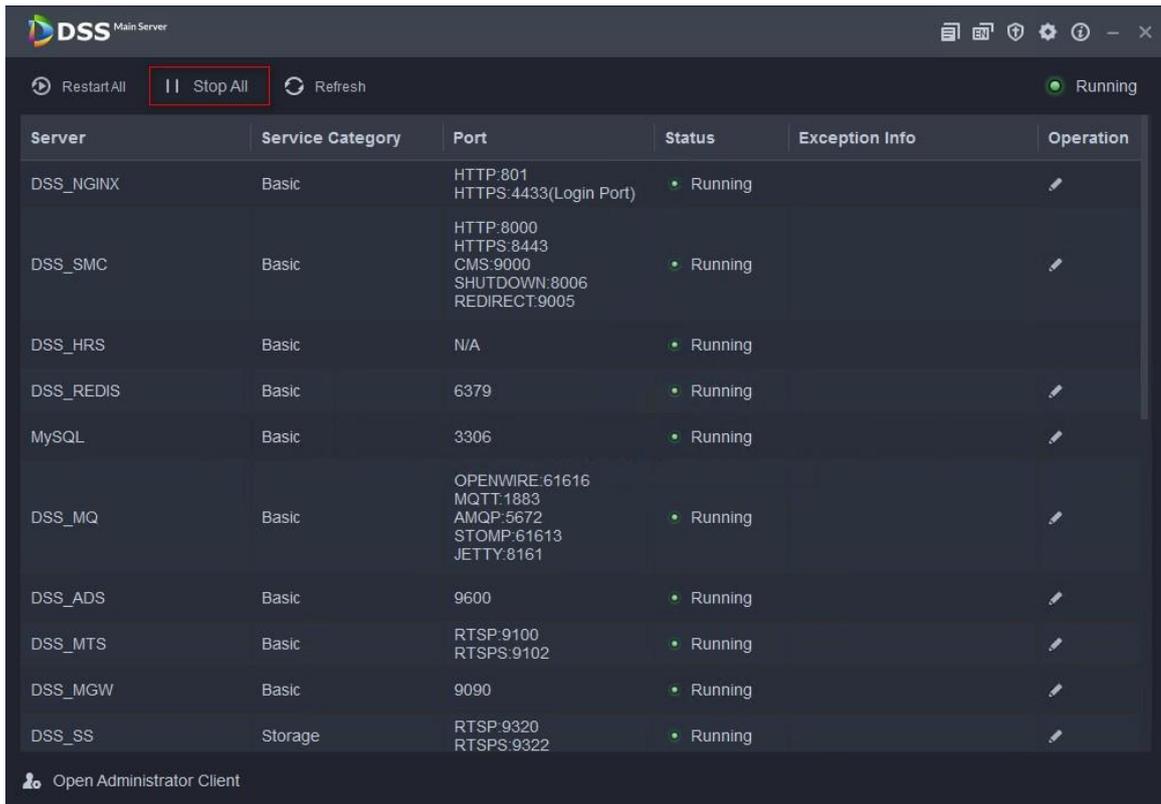
2.3 Upgrade Methods

- After the one-click upgrade, all business data except alarm and face records is kept.
- If you need to keep the alarm and face records, use the upgrade tool to perform data migration.

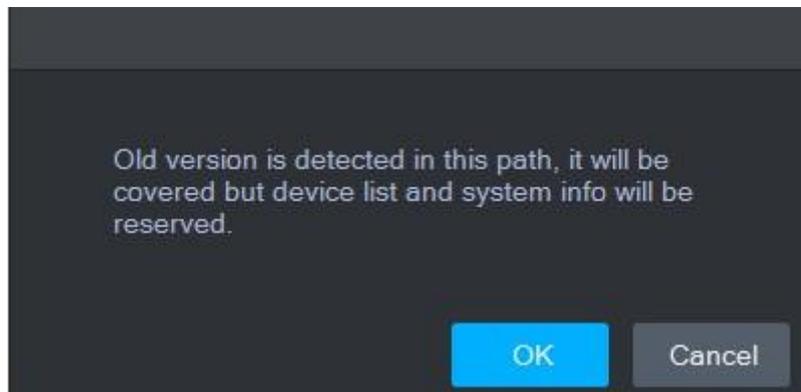
2.4 Upgrade Operations

Step 1 Log in to the server of DSS Pro or DSS Express.

Step 2 Double-click  on the desktop, log in to the DSS Server, and then click **Stop All** to stop all services.



Step 3 Double click the V8.000.0000002.0 installation program.
An upgrade prompt is displayed.



Step 4 Click **OK**.



The installation path of the old version will be detected, and you cannot edit the directory.

Step 5 Click **Install** to start the installation.



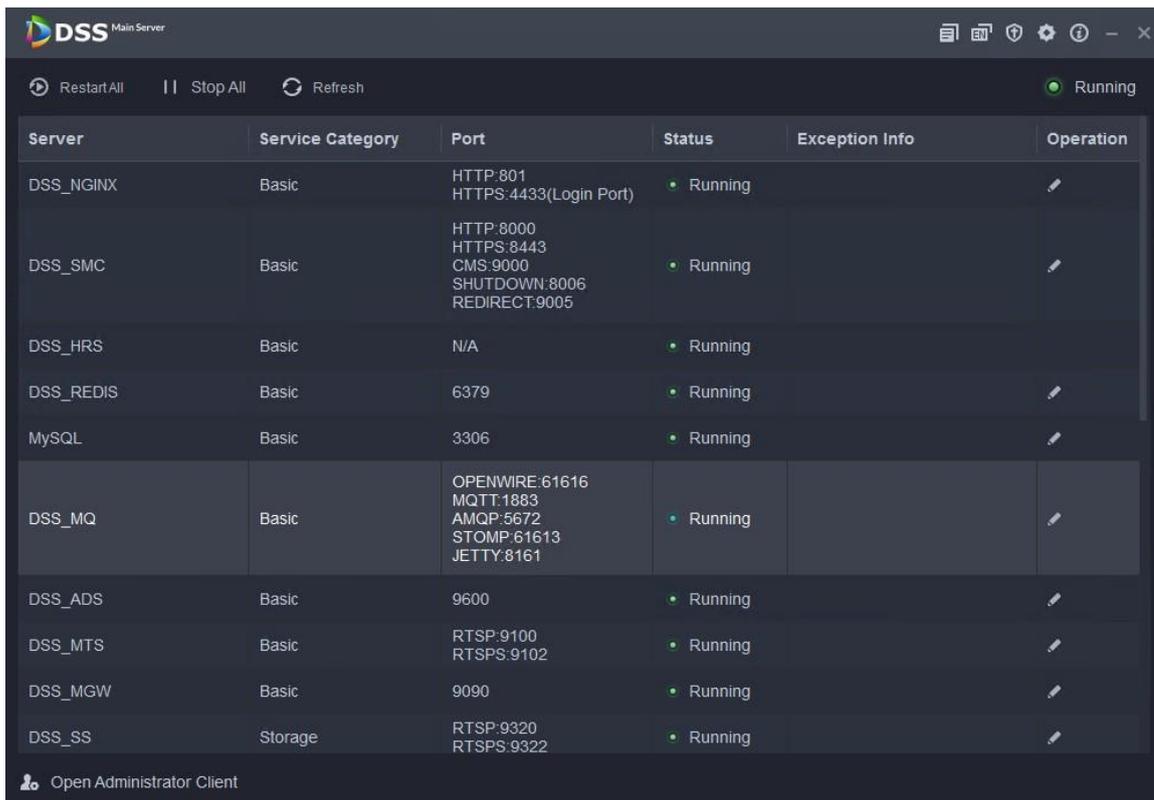
Step 6 After installation, click **Run** to run the program.



Step 7 Log in to the system configuration tool to check whether all the services are running properly.



If the word **Running** displays at the upper-right corner, it means all services are running properly. If not, check the status of each service to make sure all services are running properly.



Server	Service Category	Port	Status	Exception Info	Operation
DSS_NGINX	Basic	HTTP:801 HTTPS:4433(Login Port)	Running		
DSS_SMC	Basic	HTTP:8000 HTTPS:8443 CMS:9000 SHUTDOWN:8006 REDIRECT:9005	Running		
DSS_HRS	Basic	N/A	Running		
DSS_REDIS	Basic	6379	Running		
MySQL	Basic	3306	Running		
DSS_MQ	Basic	OPENWIRE:61616 MQTT:1883 AMQP:5672 STOMP:61613 JETTY:8161	Running		
DSS_ADS	Basic	9600	Running		
DSS_MTS	Basic	RTSP:9100 RTSPS:9102	Running		
DSS_MGW	Basic	9090	Running		
DSS_SS	Storage	RTSP:9320 RTSPS:9322	Running		

Open Administrator Client

Step 8 Log in to the Client.



The V8.0.2 Express client is compatible with V8.0.2 Pro. If a new version is available after the upgrade, there will be an update prompt. You can update the client by following the instructions.

Step 9 Update the license.

For the free or trial Express version before the upgrade, apply for the Pro V8.0.2 license, which works after it has been activated. If it is a paid Express version, you need to apply for a upgrade key to activate it after the upgrade.

- 1) Log in to the Client, click  on the homepage, and then select **License** in the **System Configuration** section.
- 2) Select **Online Activate License** or **Offline Activate License** according to the network status, and then select **Upgrade from Express**. After the upgrade, you can continue to use the functions authorized on the Express.



If you want to use more functions such as Attendance and Cascade, you can purchase a new license. For details, please refer to the corresponding user's manual.

Step 10 For data migration of the alarm and face records, please complete the following steps on the computer installed with the DSS Server.

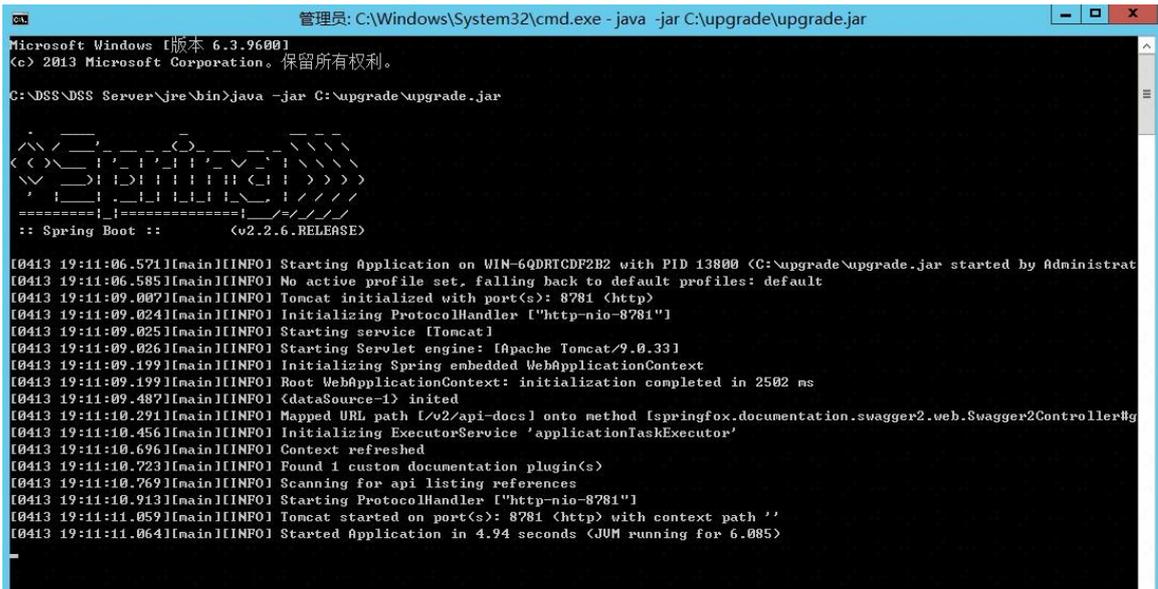
- 1) Unzip the upgrade package named "upgrade.zip" on the server.
- 2) Log in to the server at <https://127.0.0.1:443/developer/>, enter the system password for the developer page, and then click **Get Database Password** to copy the database password.
- 3) Edit the file named "application.properties" under the path of the upgrade package, and

then modify the corresponding configuration items, database link address `spring.datasource.url` and database password `spring.datasource.password`.

```
logging.config=classpath:log4j2.xml

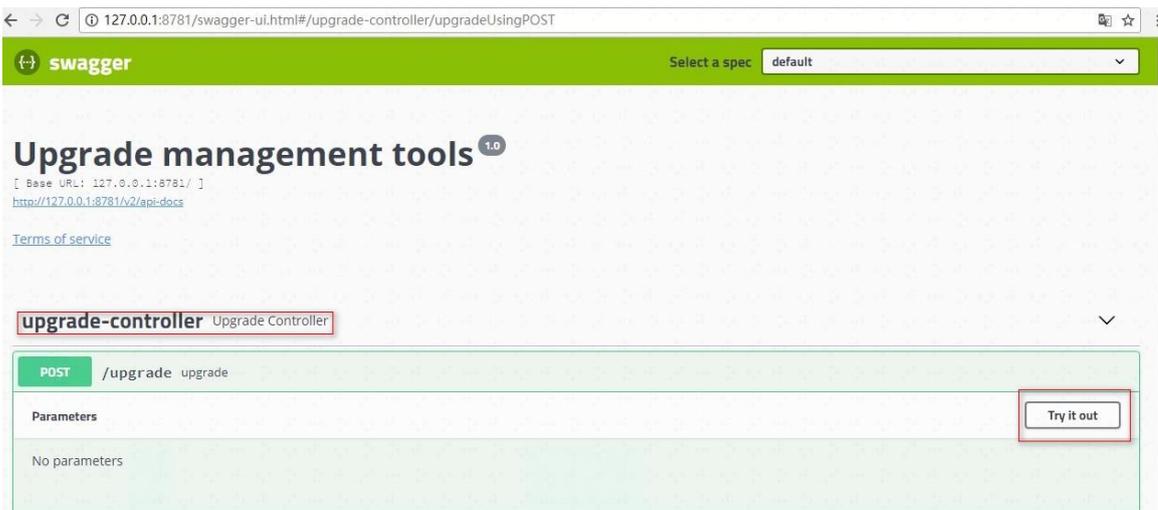
# Database
spring.datasource.url=jdbc:mariadb://127.0.0.1:3306/dss?useUnicode=true&characterEncoding=utf-8&autoReconnect=true&useSSL=false
spring.datasource.username=mysql
spring.datasource.password=5YK8BFXTWdyN9ZRx
spring.datasource.driver-class-name=org.mariadb.jdbc.Driver
```

- 4) Open the cmd command to enter the DSS jre installation directory, such as: `cd C:\DSS\DSS Server\jre\bin`
- 5) Execute `directory/upgrade.jar` where the `java -jar upgrade` package is located in.



If Started Application is displayed, it means the operation is successful; otherwise you need to check whether the steps above are correctly performed.

- 6) Open a web browser, enter `http://127.0.0.1:8781/swagger-ui.html`, and then select **Upgrade Controller > Upgrade > Try it out**.



- 7) Click **Execute** to start the update.



- 8) When the update is complete, "**Upgrade complete**" will be displayed. Make sure that the database is not interrupted during the update process. The cmd window will display the upgrade progress in real time. After the upgrade, press Ctrl+C to end the process.



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.
- It is recommended that you enable your device's firewall or blacklist and whitelist feature to reduce the risk that your device might be attacked.