



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.	July 2021

Table of Contents

Foreword	I
1 Upgrade from V8.0.2 Express/Pro to V8.0.3	1
1.1 Compatible Version	1
1.2 Upgrade Instructions	2
1.3 Upgrade Methods	2
1.4 Upgrade Operations	2
2 Upgrade from V8.0.2/V8.0.3 Express to V8.0.3 Pro	7
2.1 Compatible Version	7
2.2 Upgrade Instructions	7
2.3 Upgrade Methods	8
2.4 Upgrade Operations	8
3 Upgrade from V7 Express/Professional to V8.0.3	12
Appendix 1 Cybersecurity Recommendations	13

1 Upgrade from DSS Express/Pro V8.0.2 to V8.0.3


This chapter introduces the upgrade procedure from V8.0.2 to V8.0.3 for Express and Professional.

1.1 Compatible Version

Product	Original Version	Original Program Name	New Version
DSS Express	V8.000.00000 02.0	General_DSS-Express_win32_IS_V8.000.00000 02.0.R.20210506.exe	V8.000.0000003.0
DSS Professional	V8.000.00000 02.0	General_DSS-Professional_Win64_IS_V8.000.0 000002.0.R.20210506.exe	V8.000.0000003.0




- There might be risk if you upgrade the program. Make sure that you back up the data of DSS Express V8.0.2/DSS Professional V8.0.2 before the upgrade to avoid failure and data corruption.
- Contact local technical support for help if the upgrade fail. Uninstall the program failed to upgrade, and then reinstall DSS Express/Professional V8.0.2 to restore backup files and original DSS Express/Professional V8.0.2 data.
- Steps to backup data:

Step 1 Log in to the Client, click  on the Home page and select **Backup and Restore** in **System Config**.

Step 2 In **Manual Backup** of the **Backup** interface, select **Local** as the backup path and then click **Backup Now**.

- Steps to restore data:

Step 1 Log in to the Client, click  on the Home page and select **Backup and Restore** in **System Config**.

Step 2 In **Restore from Backup File on the Server** of the **Restore** interface, select backup files from **System Recovery File** and then click **Restore Now**.

1.2 Upgrade Instructions



Instruction list of upgrading from [

Refer to the Excel file " [Instruction list of upgrading from DSS Express and DSS Professional V8.0.2 to V8.0.3 20210730](#)" attached above for the situation of each module before and after upgrade.

1.3 Upgrade Methods

- V8.0.3 will overwrite the path of your current version.
- For DSS Professional distributed server, one-click installation upgrade is not supported. You need to uninstall the old program, and then install the latest version.
- For DSS Professional with hot-standby, close Rose software first, finish upgrade and then open the Rose software again. Other procedures are similar to those when you update DSS Professional with no hot-standby.

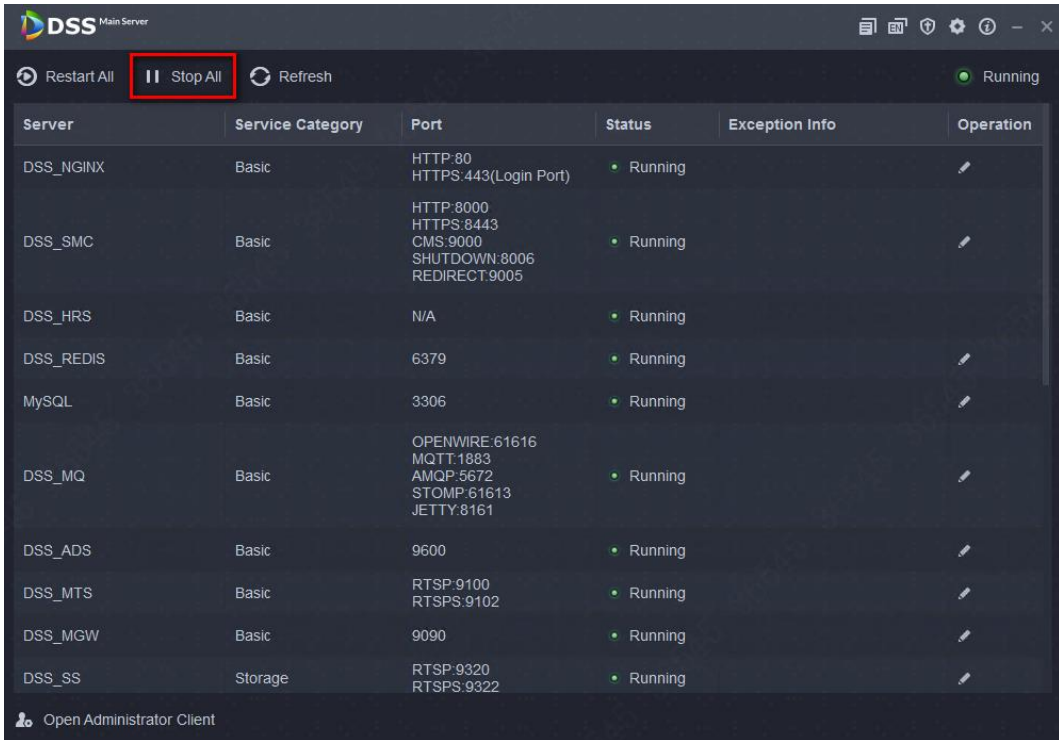
1.4 Upgrade Operations



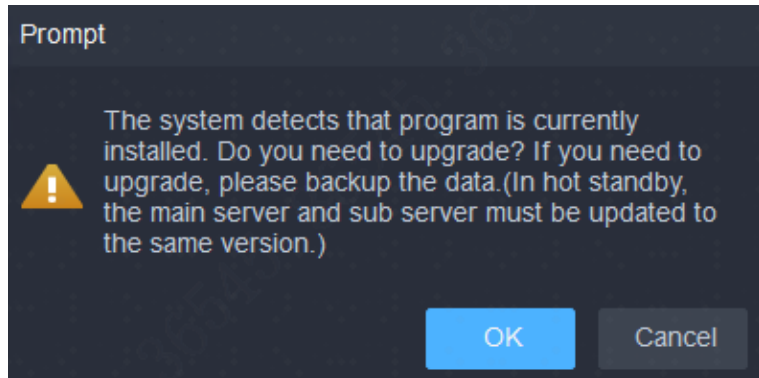
Back up your data before upgrade to avoid failure and data corruption. See "1.1 Compatible Version".

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

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



Step 3 Double-click the V8.000.0000003.0 installation program. An upgrade prompt is displayed as follows.



Step 4 Click **OK**.

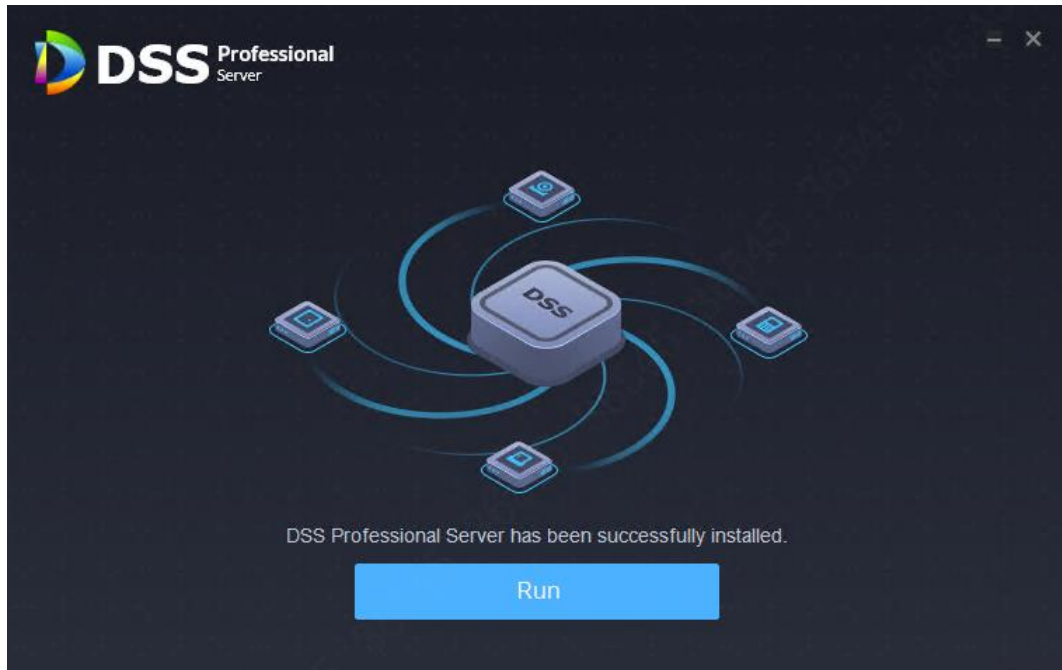


The installation path of the old version will be detected, and you cannot edit the directory.

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.

Service	Service Category	Port	Status	Exception Info	Operation
DSS_NGINX	Basic	HTTP:80 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		

Download DSS Client

Step 8 Log in to the Client again. If a new version is available after the upgrade, there will be an update prompt. You can update the client by following the instructions.



The figures above are for V8.0.2 Professional upgrading to V8.0.3, and also applicable

to V8.0.2 Express upgrading to V8.0.3 Express, but for reference only.

2 Upgrade from V8.0.2/V8.0.3 Express to V8.0.3 Pro


This chapter introduces the procedures to upgrade DSS Express V8.0.2/V8.0.3 to DSS Professional V8.0.3.

2.1 Compatible Version

Product	Original Version	Original Program Name	New Product	New Version
DSS Express	V8.000.000000 2.0	General_DSS-Express_win32_IS_V8.000.000002.0.R.20210506.exe	DSS Professional	V8.000.0000003 .0
	V8.000.000000 3.0	General_DSS-Express_win32_IS_V8.000.000003.0.R.20210729.exe		




- There might be risk if you upgrade the program. Make sure that you back up the data of DSS Express V8.0.2/DSS Express V8.0.3 before the upgrade to avoid failure and data corruption.
- Contact local technical support for help if the upgrade fail. Uninstall the program failed to upgrade, reinstall DSS Express V8.0.2/V8.0.3, and then restore the configurations with the backup file.
- Steps to backup data:

Step 1 Log in to the Client, click  on the Home page and select **Backup and Restore** in **System Config**.


Step 2 In **Manual Backup** of the **Backup** interface, select Local as the backup path and then click **Backup Now**.

- Steps to restore data:

Step 1 Log in to the Client, click  on the Home page and select **Backup and Restore** in **System Config**.

Step 2 In **Restore from Backup File on the Server** of the **Restore** interface, select backup files from **System Recovery File** and then click **Restore Now**.

2.2 Upgrade Instructions

- If the Express platform is a paid version, log in to the Client, click  on the Home page, and then select License in the System Configuration section to back up the activation code

before the upgrade.


- After DSS Express V8.000.0000002.0 is upgraded to DSS Professional V8.000.0000003.0, or DSS Express V8.000.0000003.0 to DSS Professional V8.000.0000003.0, all business data will remain the unchanged.
- After the upgrade, the alarm and face records cannot be displayed. If you need to search for the data, see Step 10 in "2.4 Upgrade Operations". Contact local technical support to help you with the upgrade.

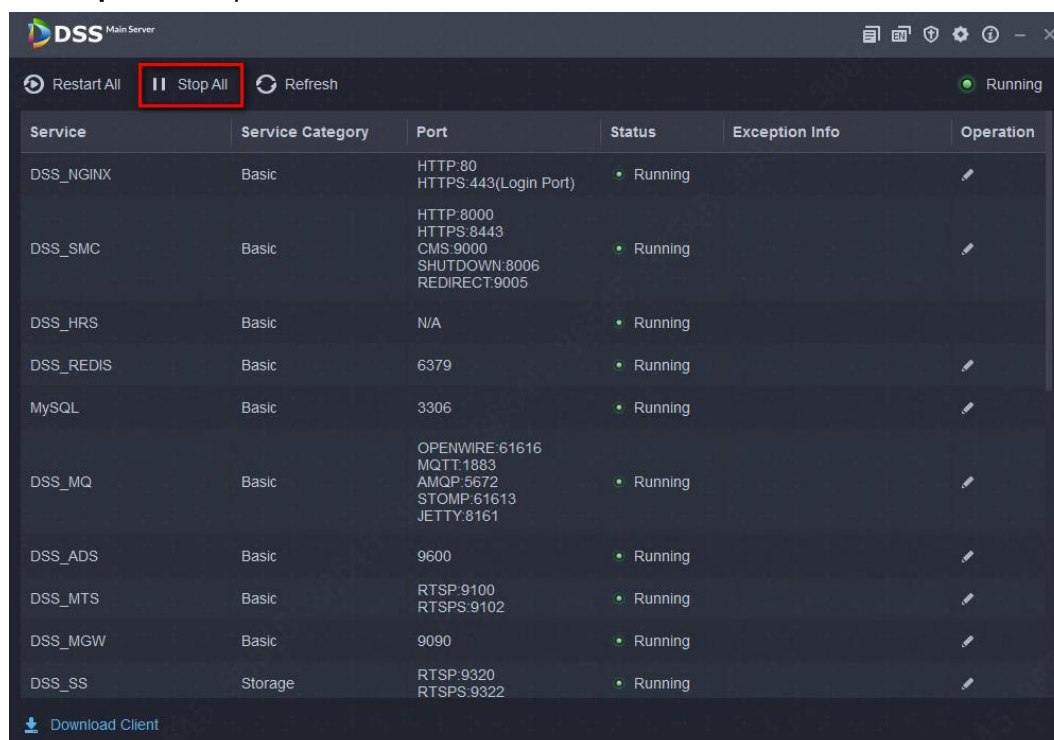
2.3 Upgrade Methods

- 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.

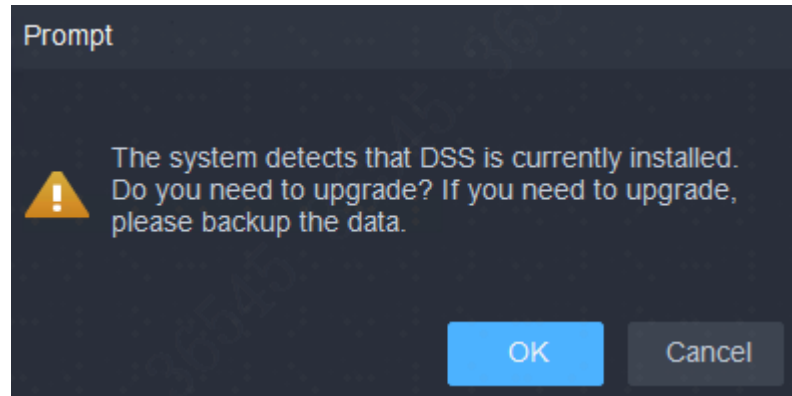
2.4 Upgrade Operations

Step 1 Log in to the DSS Express server.

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



Step 3 Double-click the V8.000.0000003.0 installation program. An upgrade prompt is displayed as follows.



Step 4 Click **OK**.

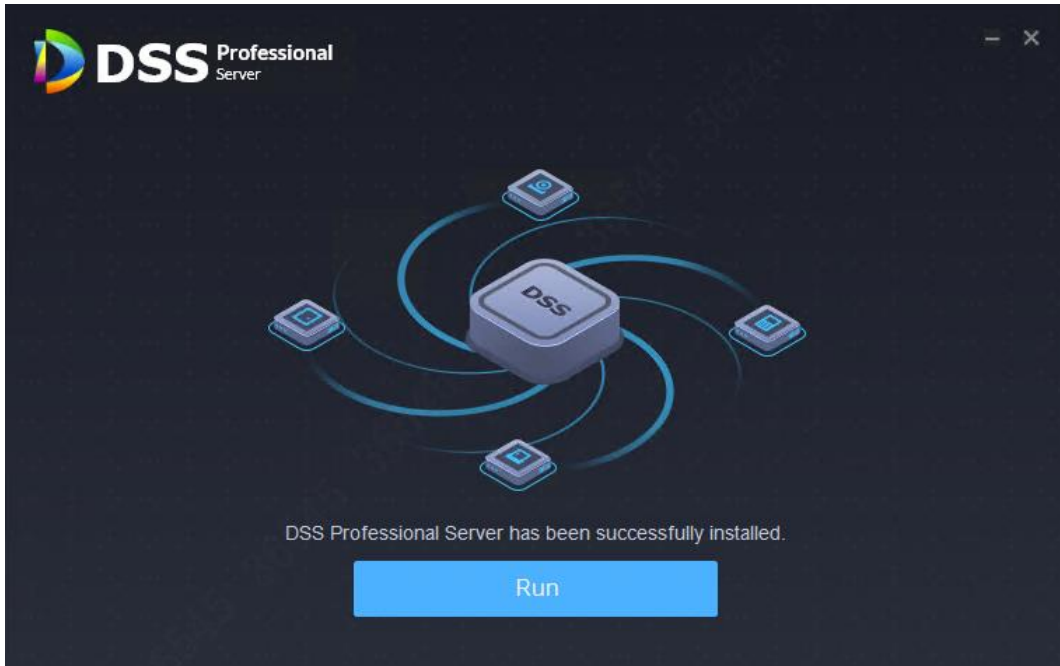


The installation path of the old version will be detected, and you cannot edit the directory.

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



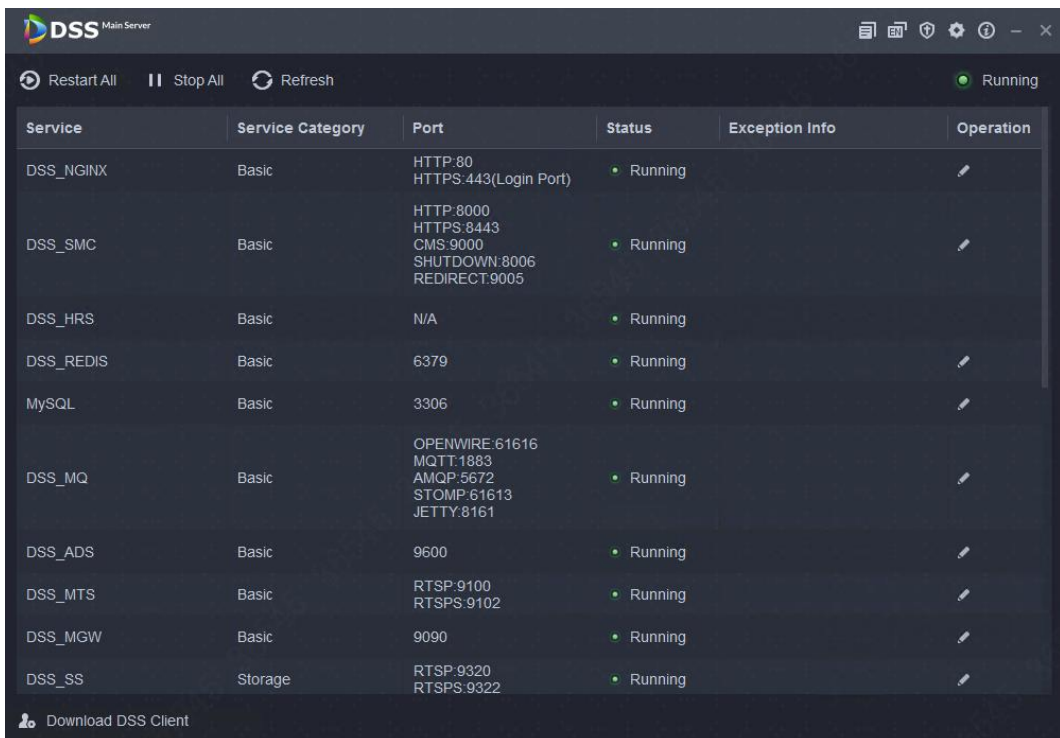
Step 6 After installation, click **Run** to run the program.



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.




Step 8 Go to the Client.

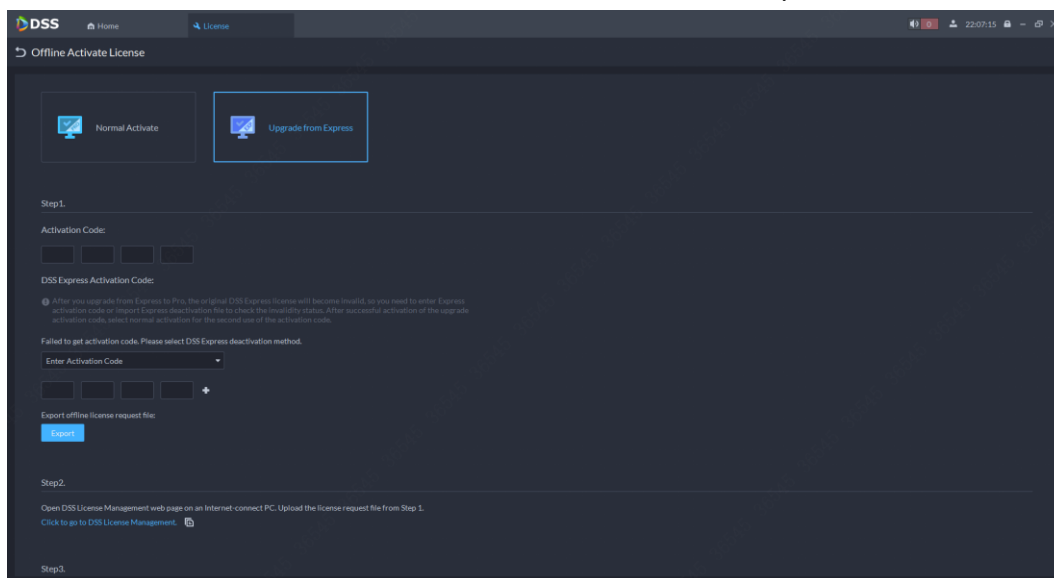


If a new version is available after the upgrade, there will be an update prompt. You can update the client by following the instructions.

Step 9 Upgrade the license.

For the free or trial Express version before the upgrade, apply for the Professional V8.0.3 license, which works after it has been activated. If it is a paid Express version, you need to apply for an 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 To upgrade alarm and face records, follow the steps below on the computer installed with the DSS Server. Contact local technical support to help you with the upgrade.



The figures above are for upgrading DSS Express V8.000.0000003.0 to DSS Professional V8.000.0000003.0, and are for reference only when upgrading to DSS Express V8.000.0000002.0 to DSS Professional V8.000.0000003.0.

3 Upgrade from V7 Express/Professional to V8.0.3

This chapter is applicable to upgrading DSS Express/Professional from V7 to V8.000.0000003.0.

- DSS Express/Professional V7 cannot be directly upgraded to V8.000.0000003.0. You need to upgrade from V7 to V8.000.0000002.0 first, and then to V8.000.0000003.0.
- To upgrade DSS Express V7 /Professional to V8.000.0000002.0, see operation steps in V8.0.2 Upgrade Guide.
- To upgrade DSS Express/Professional V8.000.0000002.0 to V8.000.0000003.0, follow the steps in "1 Upgrade from DSS Express/Pro V8.0.2 to V8.0.3".
- To upgrade DSS Express V8.000.0000002.0 to DSS Professional V8.000.0000003.0, follow the steps in "2 Upgrade from V8.0.2/V8.0.3 Express to V8.0.3 Pro".

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 device 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 device (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 device 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 device network security:

1. Physical Protection

We suggest that you perform physical protection to device, especially storage devices. For example, place the device 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 device (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 device 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. MAC Address Binding

We recommend you to bind the IP and MAC address of the gateway to the device, thus reducing the risk of ARP spoofing.

8. Assign Accounts and Privileges Reasonably

According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. 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.

10. 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.

11. Secure Auditing

- Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
- Check device log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. Network Log

Due to the limited storage capacity of the device, 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.

13. Construct a Safe Network Environment

In order to better ensure the safety of device 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.
- Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.