



DSS

Update Guide



Foreword

General

This manual introduces how to update 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.	October 2021

Table of Contents

Foreword	1
1 Updating DSS Express/Pro from V8.0.2/V8.0.3 to V8.0.4	1
1.1 Compatible Version	1
1.2 Update Instructions.....	2
1.3 Update Methods.....	2
1.4 Update Operations.....	2
2 Updating DSS Express from V8.0.2/V8.0.3/V8.0.4 to DSS Pro V8.0.4	7
2.1 Compatible Version	7
2.2 Update Instructions.....	8
2.3 Update Methods.....	8
2.4 Update Operations.....	8
3 Upgrading DSS Express/Professional from V7 to V8.0.4	13
Appendix 1 Cybersecurity Recommendations	14

1 Updating DSS Express/Pro from V8.0.2/V8.0.3 to V8.0.4

This chapter introduces how to update DSS Express/Professional from V8.0.2/V8.0.3 to V8.0.4.

1.1 Compatible Version

Table 1-1 Update description

Product	Version before Update	Program Name before Update	Product after Update	New Version
DSS Express	V8.000.0000002.0	General_DSS-Express_wi n32_IS_V8.000.0000002. 0.R.20210506.exe	DSS Express	V8.000.0000004.0
DSS Professional	V8.000.0000002.0	General_DSS-Professiona l_Win64_IS_V8.000.0000 002.0.R.20210506.exe	DSS Professional	V8.000.0000004.0
DSS Express	V8.000.0000003.0	General_DSS-Express_wi n32_IS_V8.000.0000003. 0.R.20210729.exe	DSS Express	V8.000.0000004.0
DSS Professional	V8.000.0000003.0	General_DSS-Professiona l_Win64_IS_V8.000.0000 003.0.R.20210729.exe	DSS Professional	V8.000.0000004.0



- Back up the data of DSS Express/Professional V8.0.2/V8.0.3 before update to avoid failure and data corruption.
- Contact local technical support for help if the update failed. Uninstall the failed program, and then reinstall DSS Express/Professional V8.0.2/V8.0.3 to restore backup files and the data of original DSS Express/Professional V8.0.2/V8.0.3.

Backup Data

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

Step 2 On **Manual Backup** of the **Backup** page, select backup path and then click **Backup Now**.

Restore Data

Step 1 Log in to the Client, click  on the homepage and select **Backup and Restore** in **System**

Config module.

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

1.2 Update Instructions



Note for Update
from V8.0.3 to V8

See the Excel file attached above for the situation of each module before and after update.

- After DSS Express/Professional is updated to V8.0.4, service data of V8.0.2/V8.0.3 can be kept.
- After DSS Professional is updated to V8.0.4, the metadata and ANPR records cannot be displayed. If you need to keep the records, refer to step 9 of "1.4 Update Operations". Contact local technical support for help.

1.3 Update Methods

- V8.0.4 will overwrite the path of your current version. All service data can be kept.
- After DSS Professional is updated to V8.0.4, the metadata and ANPR records cannot be displayed. If you need to keep the records, use the update tool to migrate data.
- For DSS Professional distributed server, one-click installation update 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 update and then open the Rose software again. Other procedures are similar to those when you update DSS Professional with no hot-standby.

1.4 Update Operations

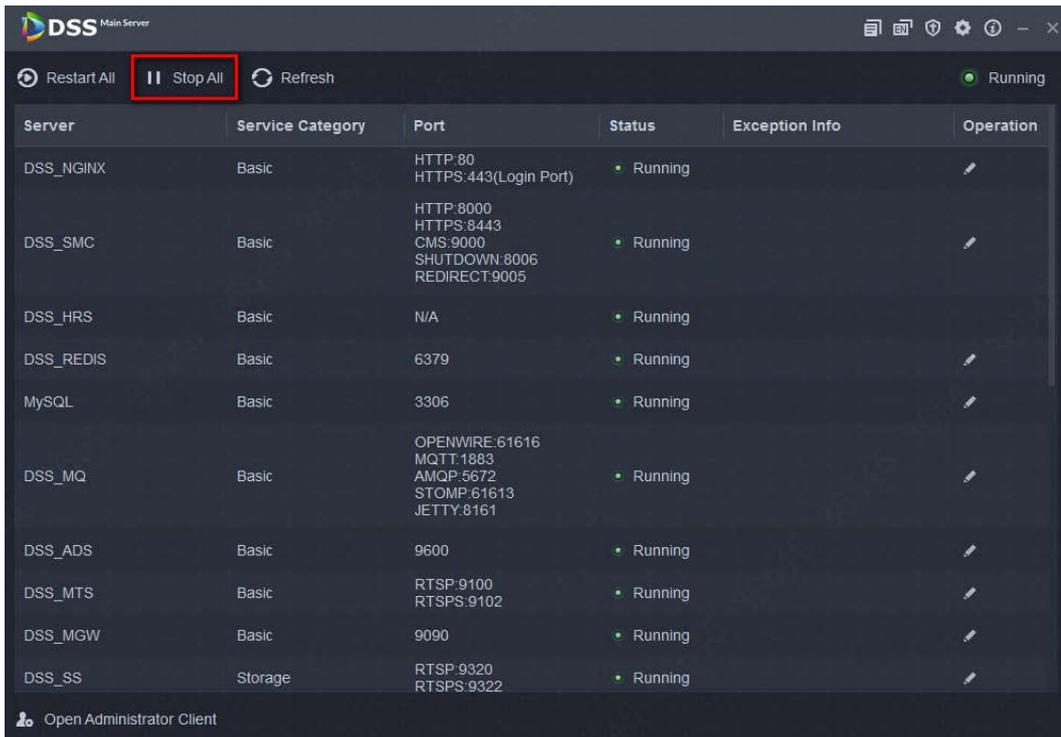
The section takes DSS Professional as an example. Update DSS Professional from V8.000.0000003.0 to V8.000.0000004.0. The figures are for reference only.



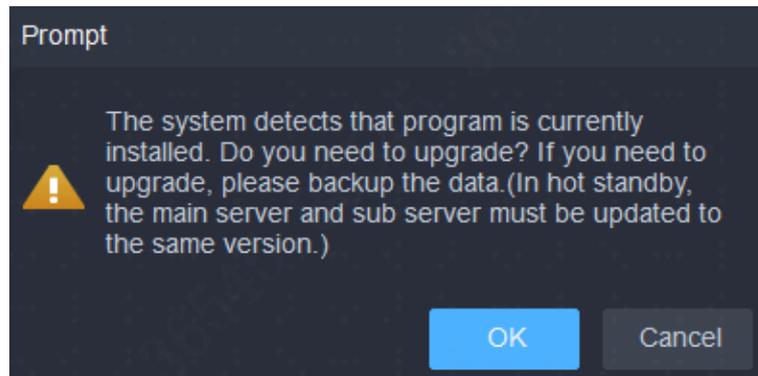
Back up your data before update to avoid failure and data corruption. See "1.1 Compatible Version".

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 V8.000.0000004.0 installation program. An update prompt is displayed as follows.

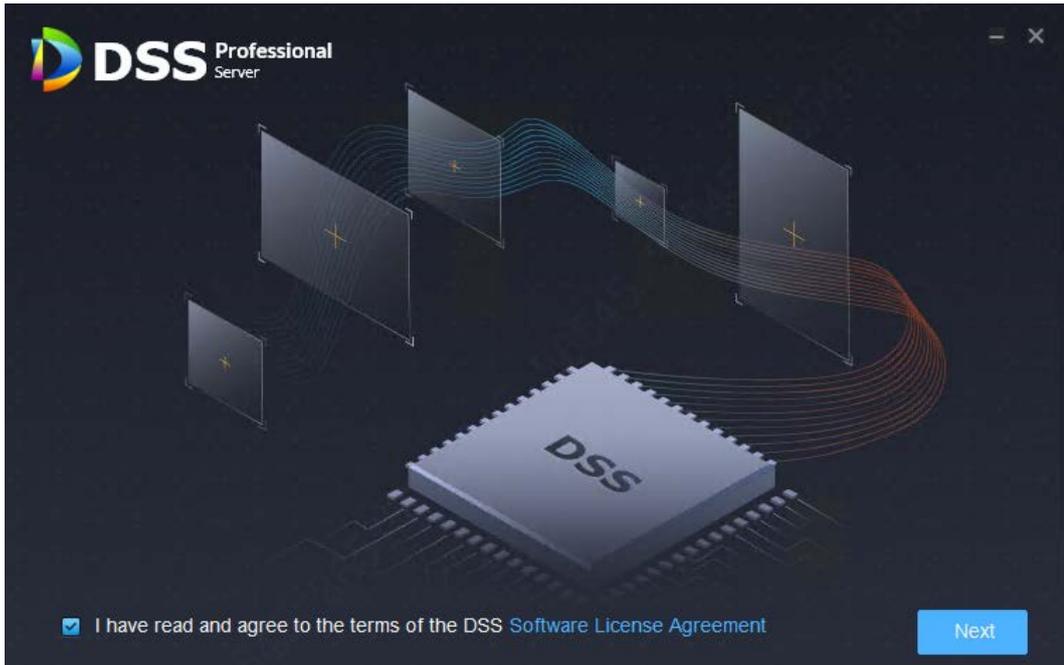


Step 4 Click **OK**.

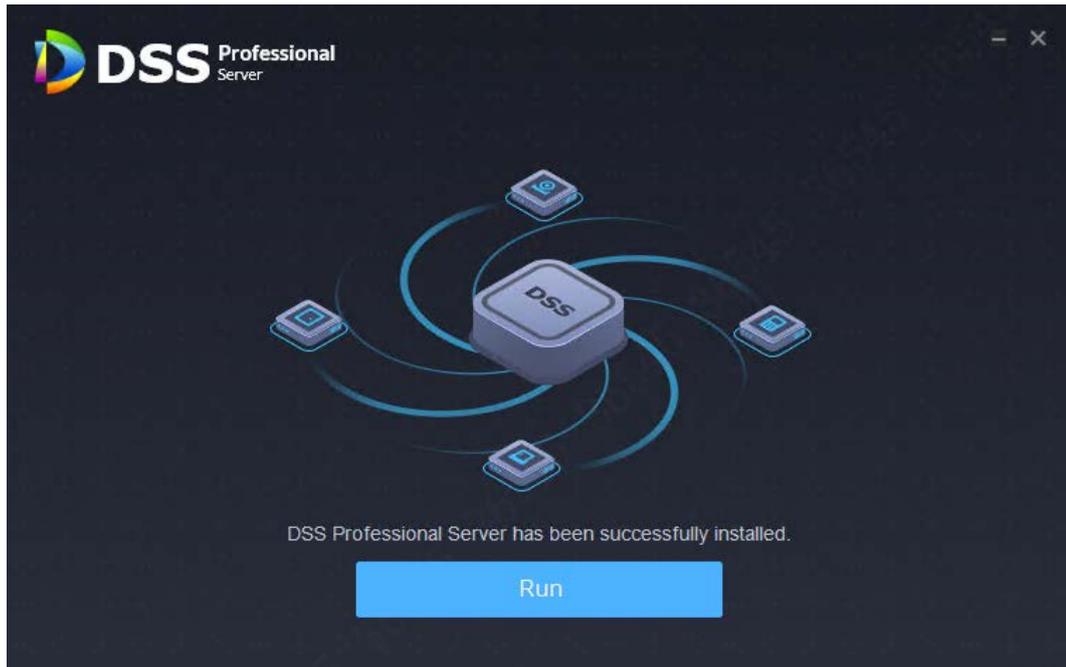


The installation path of the old version will be detected, and you cannot edit the directory.

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, there will be an update prompt. Follow steps to update the Client.

Step 9 After DSS Professional is updated to V8.0.4, the metadata and ANPR records cannot be displayed. If you need to keep the records, use the update tool to migrate data. Update the metadata and ANPR records on PC installed with DSS Server is installed. Contact local technical support for help.



The procedure can also be applied to update DSS Professional from V8.000.0000002.0 to V8.000.0000004.0, and update DSS Express from V8.000.0000002.0/V8.000.0000003.0 to V8.000.0000004.0 (Step 9 is not required for DSS Express update).

2 Updating DSS Express from V8.0.2/V8.0.3/V8.0.4 to DSS Pro V8.0.4

This chapter introduces how to update DSS Express V8.0.2/V8.0.3/V8.0.4 to DSS Professional V8.0.4.

2.1 Compatible Version

Product	Version before Update	Program Name before Update	Product after Update	New Version
DSS Express	V8.000.0000002.0	General_DSS-Express_wi n32_IS_V8.000.0000002. 0.R.20210506.exe	DSS Professional	V8.000.0000004.0
	V8.000.0000003.0	General_DSS-Express_wi n32_IS_V8.000.0000003. 0.R.20210729.exe		
	V8.000.0000004.0	General_DSS-Express_wi n32_IS_V8.000.0000004. 0.R.20211119.exe		



- Back up the data of DSS Express V8.0.2/V8.0.3/V8.0.4 before update to avoid failure and data corruption.
- Contact local technical support for help if the update failed. Uninstall the failed program, and then reinstall DSS Express V8.0.2/V8.0.3/V8.0.4 to restore backup files and the data of original DSS Express/Professional V8.0.2/V8.0.3/V8.0.4.

Backup Data

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

Step 2 On **Manual Backup** of the **Backup** page, select backup path and then click **Backup Now**.

Restore Data

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

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

2.2 Update Instructions

- If the DSS Express is a premium version, log in to the Client, click  on the homepage, and then select **License** in the **System Configuration** section to back up the activation code before update.
- After DSS Professional V8.000.0000002.0/V8.000.0000003.0/V8.000.0000004 is updated to DSS Professional V8.000.0000004.0, service data before update can be kept.
- After update, the records of alarm, face, metadata and ANPR cannot be displayed. If you need to keep the records, refer to step 9 of "2.4 Update Operations". Contact local technical support for help.

2.3 Update Methods

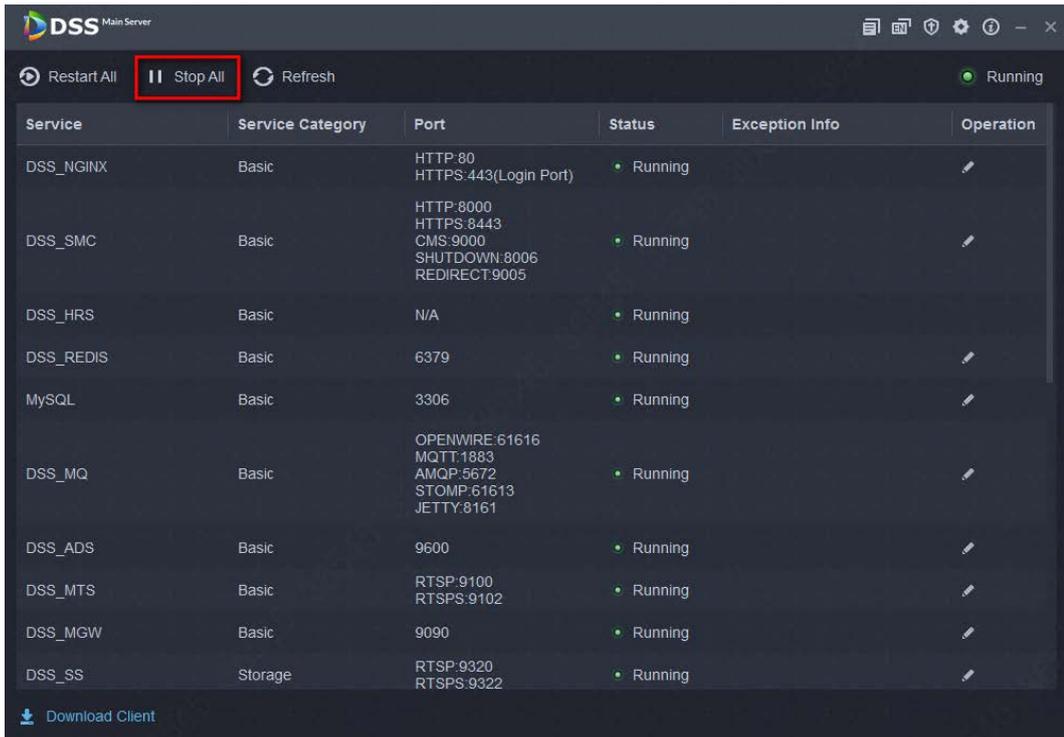
- After the one-click update, all business data is kept except the records of alarm, face, metadata, and ANPR.
- If you need to keep the records of alarm, face, metadata, and ANPR, use the update tool to migrate data.

2.4 Update Operations

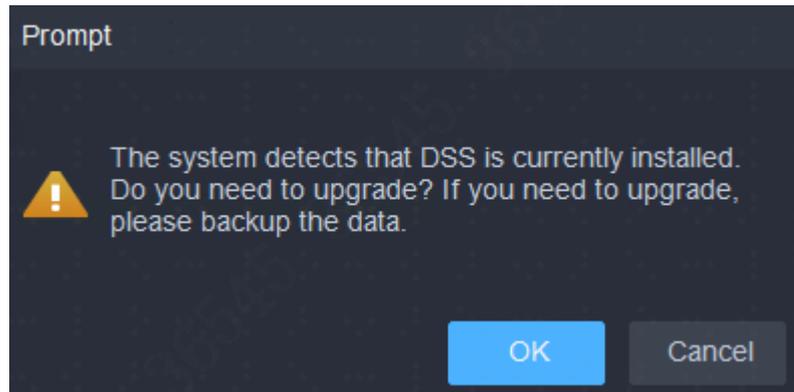
The section takes DSS Express V8.000.0000004.0 as an example. Update DSS Express V8.000.0000004.0 to DSS Professional V8.000.0000004.0. The figures are for reference only.

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 V8.000.000004.0 installation program. An update 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.



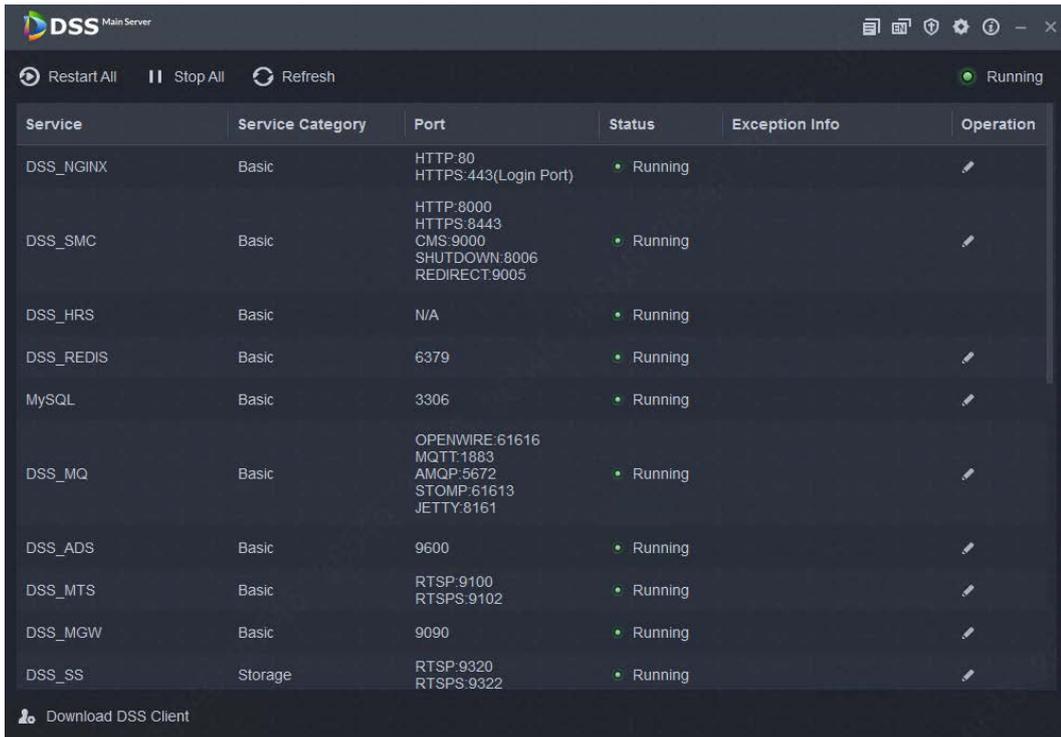
Step 6 After installation, click **Run** to run the program.



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 Log in to the Client again.

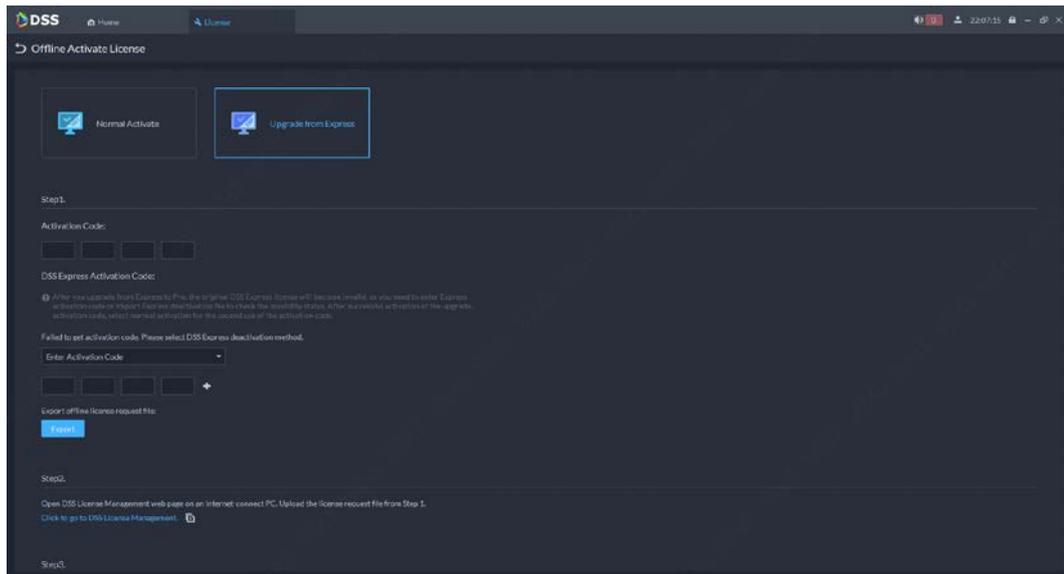


If a new version is available after update, there will be an update prompt. Follow steps to update the Client.

Step 9 Update the license.

If DSS Express before update is a free or trial version, apply for the DSS Professional V8.0.4 license after update, which works after it has been activated. If DSS Express before update is a premium version, you need to apply for an update key to activate it after update.

- 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 update, you can continue to use the functions authorized on the Express.



If you want to use more functions such as attendance, cascading, synthesis, and independent database, you can purchase a new license. For details, refer to the corresponding user's manual.

Step 10 Update the records of alarm, face, metadata, and ANPR on PC installed with the DSS Server. Contact local technical support for help you.



The procedure can also be applied to update DSS Express V8.000.0000002/V8.000.0000003.0 to DSS Professional V8.000.0000004.0.

3 Upgrading DSS Express/Professional from V7 to V8.0.4

This chapter is applicable to upgrading DSS Express/Professional from V7 to V8.000.0000004.0.

- DSS Express/Professional V7 cannot be directly upgraded to V8.000.0000004.0.
You need to upgrade from V7 to V8.000.0000002.0 first, and then to V8.000.0000004.0.
- To upgrade DSS Express V7 /Professional to V8.000.0000002.0, follow the steps in DSS V8.0.2_ Update Guide.
- To update DSS Express/Professional V8.000.0000002.0 to V8.000.0000004.0, follow the steps in "1 Updating DSS Express/Pro from V8.0.2/V8.0.3 to V8.0.4" of this document.
- To update DSS Express V8.000.0000002.0 to DSS Professional V8.000.0000004.0, follow the steps in "2 Updating DSS Express from V8.0.2/V8.0.3/V8.0.4 to DSS Pro V8.0.4" of this document.

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.

ENABLING A SAFER SOCIETY AND SMARTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Address: No.1199 Bin'an Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053

Email: overseas@dahuatech.com | Fax: +86-571-87688815 | Tel: +86-571-87688883