



DSS4004-S2 DSS7016D/DR-S2

Update Guide








Foreword

General

This manual introduces how to update the 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.	August 2021

Table of Contents

Foreword	I
1 Updating from V1.001 to V8.0.2	3
1.1 Compatible Version.....	3
1.2 Upgrade Instructions.....	3
1.3 Upgrade Methods.....	3
1.4 Update Operations.....	4
Appendix 1 Cybersecurity Recommendations	7

1 Updating from V1.001 to V8.0.2

This chapter introduces the applicable version and update procedures from V1.001 to V8.0.2 for DSS4004-S2 and DSS7016D/DR-S2.

1.1 Applicable Version

Product	Applicable version	Applicable Program Name	Target Version
DSS4004-S2	V1.001.0000000.2	General_OverseasDSS4004S2_Eng_Basic_V1.001.0000000.2.R.20201217.tar.gz	V8.0.2
DSS7016D/DR-S2	V1.001.0000001.2	General_OverseasDSS7016S2_Eng_Basic_V1.001.0000001.2.R.20201211.tar.gz	V8.0.2



There might be risk if you update the program. Make sure that you back up the data before update to avoid failure and data corruption.

1.2 Update Instructions

Refer to the following .xlsx file for the situations before and after update.



Update Note.xlsx

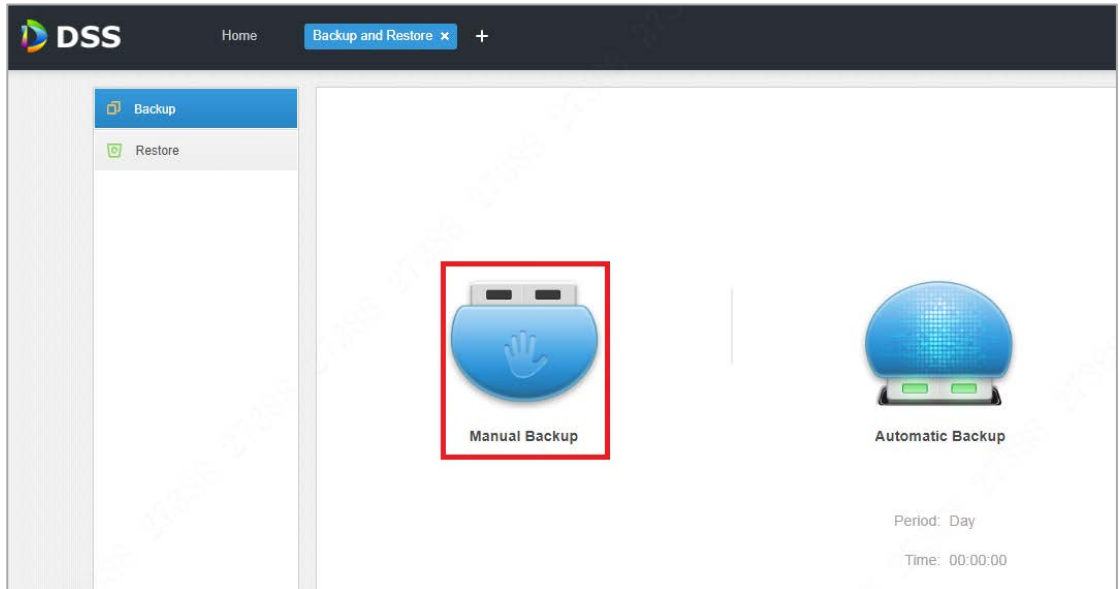
1.3 Update Methods

- Non-applicable versions cannot be directly upgraded to V8.000.0000002.0. You need to upgrade to the applicable versions first (see "1.1 Applicable Version"), and then to V8.000.0000002.0. If you upgrade to V8.000.0000002.0 directly, the system prompts an update failure. The data will not be replaced, and the original version remains after the service restarts.
- You cannot update when hot standby is configured. Remove the hot standby before updating to V8.000.0000002.0.
- After update, you need to reconfigure distributed deployment.
- After update, the program cannot be downgraded to earlier versions.
- Downgrade or update among different programs is not supported. For example, you cannot update DSS7016D/DR-S2 to DSS4004-S2, or update DSS4004-S2 to DSS7016D/DR-S2.

1.4 Update Procedures

The section takes DSS4004-S2 and DSS7016D/DR-S2 as an example, updating from V1.001 to V8.000.0000002.0. The figures are for reference only.

Step 1 Back up your data before update to avoid failure and data corruption.

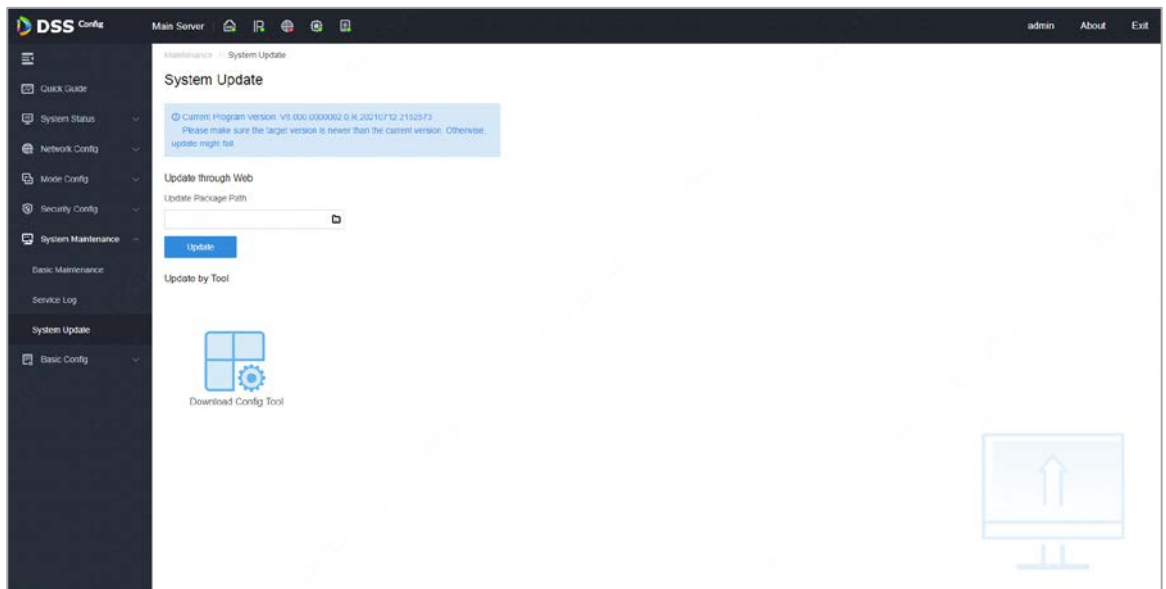


Step 2 Open browser, enter *IP/config* on the address bar, and then press Enter key.


Step 3 Enter the username and password, and then click **Login** to log in to the web configuration interface.

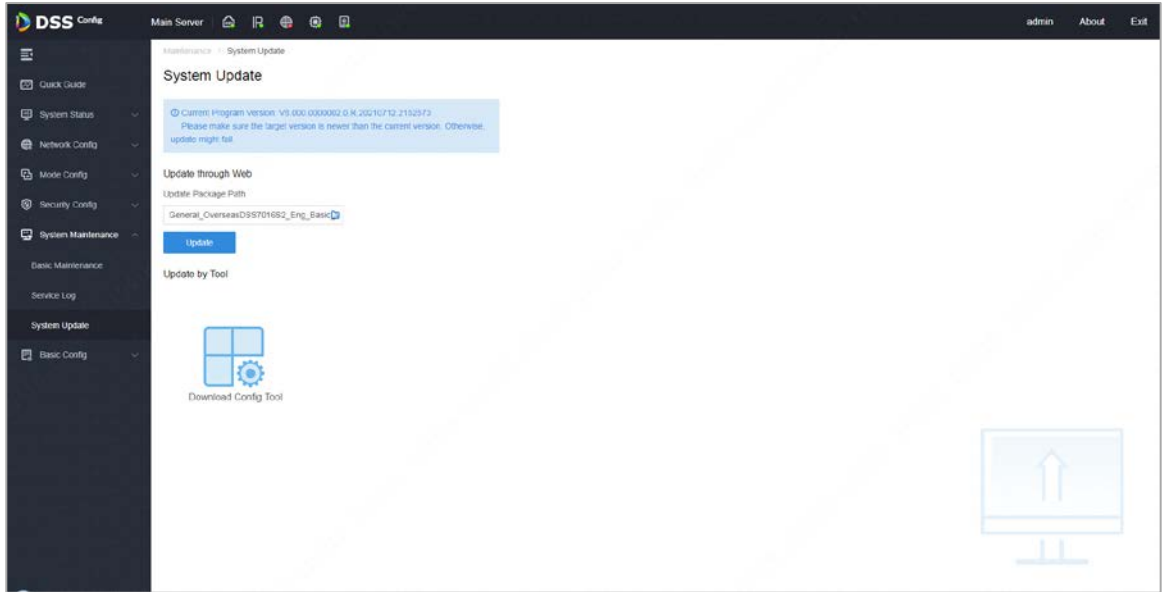
Step 4 Select **System Maintenance > System Update**.

You can update on the web interface or by the configuration tool.

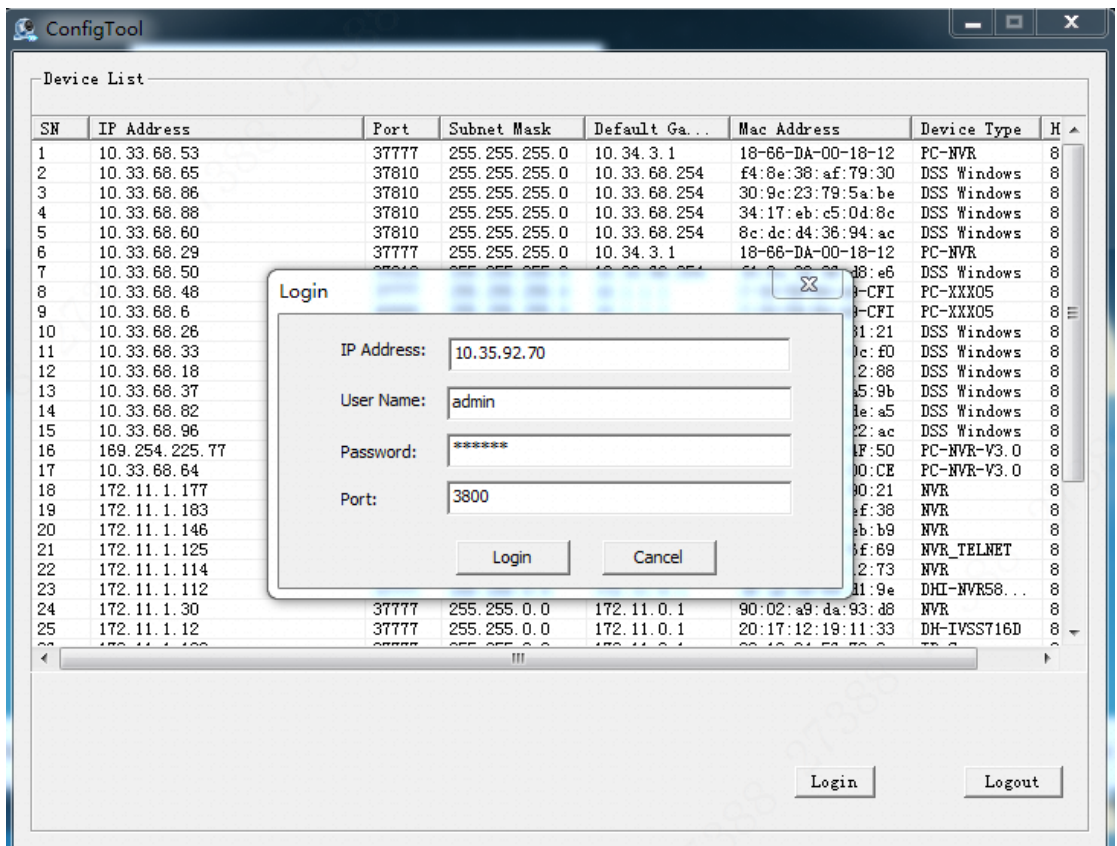


- Update on the web interface

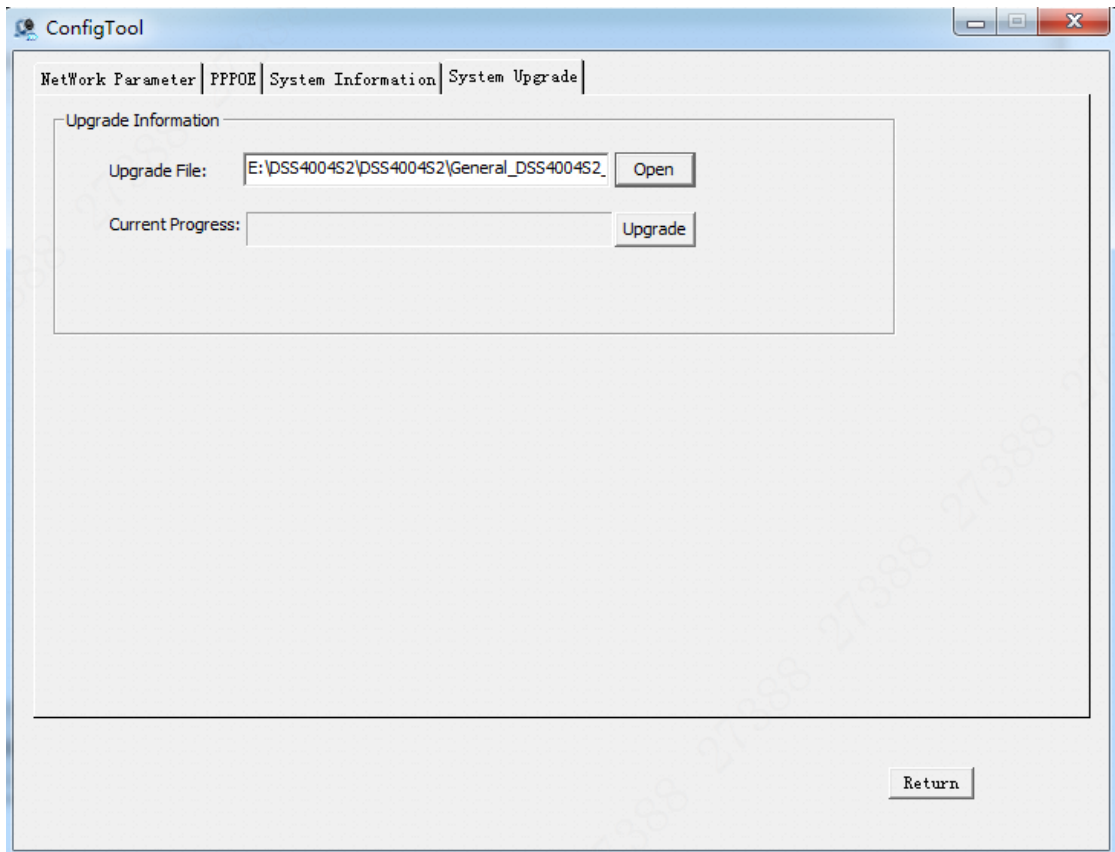
Click , select the update package in .BIN format, and then click **Update**.



- Update by configuration tool
 - 1) Click **Download Config Tool**.
 - 2) Enter IP address, username and password of the web interface, and then click **Login** to log in to the configuration tool.



- 3) Click **System Upgrade**, click **Open**, select the update package in .BIN format, and then click **Upgrade**.

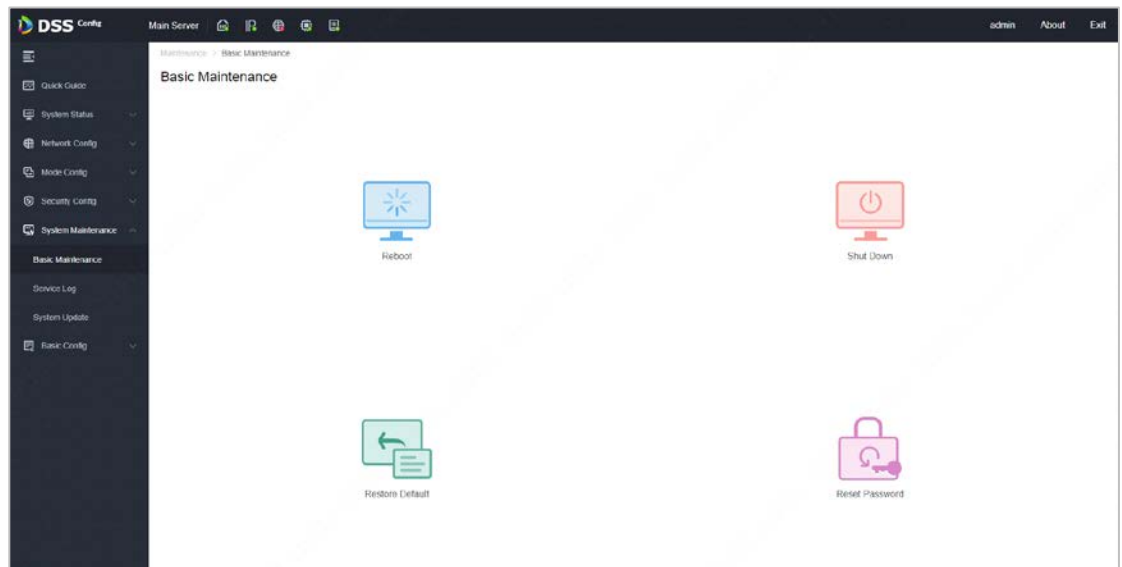


Step 5 After the update is complete, the system restarts. Log in to the web configuration interface (the username is admin by default)

Step 6 (Optional) Select **System Maintenance > Basic Maintenance > Restore Default.**



After update, if the environment is abnormal and there is no need to archive old data on site, you can perform the step, which will restore the device to factory settings and delete the old version files.



Step 7 After the update is complete, download the V8 version of the client.

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