



# **DSS7016D-S2/DR-S2 and DSS4004-S2**






## **Update Guide**



# Foreword

## Safety Instructions

The following categorized signal words with defined meaning might appear in the manual.

Signal Words	Meaning
 <b>DANGER</b>	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
 <b>WARNING</b>	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
 <b>CAUTION</b>	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
 <b>TIPS</b>	Provides methods to help you solve a problem or save you time.
 <b>NOTE</b>	Provides additional information as the emphasis and supplement to the text.

---

# Table of Contents

<b>Foreword</b> .....	<b>I</b>
<b>1 Updating DSS4004-S2 or DSS7016D-S2/DR-S2 from V8.0.2/V8.0.4/ V8.1.0 to V8.2.0</b> .....	<b>1</b>
1.1 Compatible Version .....	1
1.2 Backing Up and Restoring Data.....	2
1.3 Update P rocedures.....	2
<b>2 Updating DSS4004-S2 or DSS7016D-S2/DR-S2 from V1.001 to V8.2.0</b> .....	<b>6</b>
<b>Appendix 1 Cybersecurity Recommendations</b> .....	<b>7</b>

# 1 Updating DSS4004-S2 or DSS7016D-S2/DR-S2 from V8.0.2/V8.0.4/ V8.1.0 to V8.2.0



- After updating to V8.2.0, data from V8.0.2/V8.0.4/ V8.1.0 will be kept.
- Versions that are not listed in the following table cannot be updated to V8.2.0. You must update it to any version listed in the following table, and then to V8.2.0. If you update it anyway, update will fail, but the data will remain intact.
- For servers in hot standby, you must remove hot standby and then update the servers.
- For servers in distributed deployment, you can update each server directly.
- You cannot downgrade any version.
- You cannot update or downgrade DSS7016D-S2/DR-S2 to DSS4004-S2, or DSS4004-S2 to DSS7016D-S2/DR-S2.



For the prerecording function to work normally, the platform will store recordings prior to events in the RAM. This will occupy the prerecording bandwidth. If the prerecording bandwidth is exceeded, certain recordings might be lost. Therefore, we optimized the function in V8.001.0000000.0. If you update from V8.000.0000004.0 to V8.001.0000000.0 or a later version, the prerecording time that has been configured in any event will be reset to 0. If you need the prerecording function for an event, you can configure the prerecording time again.

## 1.1 Compatible Version


Product	Version before Update	Program before Update	New Version
DSS4004-S2	V8.000.0000002.0	General_OverseasDSS4004S 2_Eng_Basic_V8.000.000000 2.0.R.20220125.tar.gz	V8.002.0000000.0
DSS4004-S2	V8.000.0000004.0	General_OverseasDSS4004S 2_Eng_Basic_V8.000.000000 4.0.R.20211230.tar.gz	V8.002.0000000.0
DSS4004-S2	V8.001.0000000.0	General_OverseasDSS4004S 2_Eng_Basic_V8.001.000000 0.0.R.20220629.tar.gz	V8.002.0000000.0
DSS4004-S2	V8.001.0000000.1	General_OverseasDSS4004S 2_Eng_Basic_V8.001.000000 0.1.R.20221126.tar.gz	V8.002.0000000.0
DSS7016D/DR-S2	V8.000.0000002.0	General_OverseasDSS7016S 2_Eng_Basic_V8.000.000000 2.0.R.20220125.tar.gz	V8.002.0000000.0

Product	Version before Update	Program before Update	New Version
DSS7016D/DR-S2	V8.000.0000004.0	General_OverseasDSS7016S 2_Eng_Basic_V8.000.000000 4.0.R.20211230.tar.gz	V8.002.0000000.0
DSS7016D/DR-S2	V8.001.0000000.0	General_OverseasDSS7016S 2_Eng_Basic_V8.001.000000 0.0.R.20220629.tar.gz	V8.002.0000000.0
DSS7016D/DR-S2	V8.001.0000000.1	General_OverseasDSS7016S 2_Eng_Basic_V8.001.000000 0.1.R.20221126.tar.gz	V8.002.0000000.0

## 1.2 Backing Up and Restoring Data


To avoid data loss caused by update failure, make sure that you have backed up the data before update. In case of data loss, you can restore all the data from the backup file.

### Backing Up Data

Step 1 Log in to the PC Client, click  on the 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**.

### Restoring Data

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

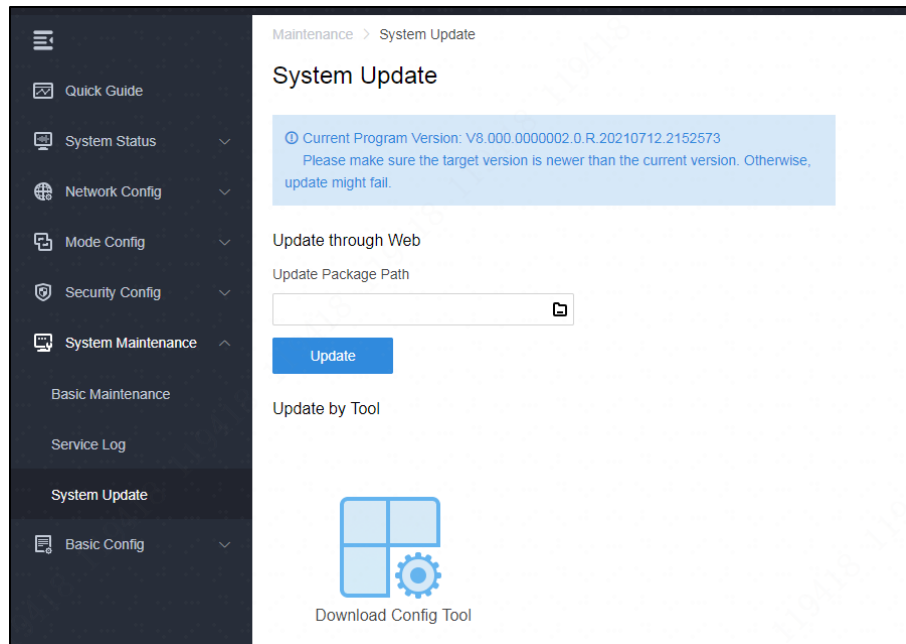
Step 2 Click , select the backup file, and then click **Restore Now**.

## 1.3 Update Procedures

Step 1 Go to <https://platform IP address/config> in the browser.

Step 2 Enter the username and password, and then click **Login** to log in to the configuration system.


Step 3 Select **System Maintenance** > **System Update**.



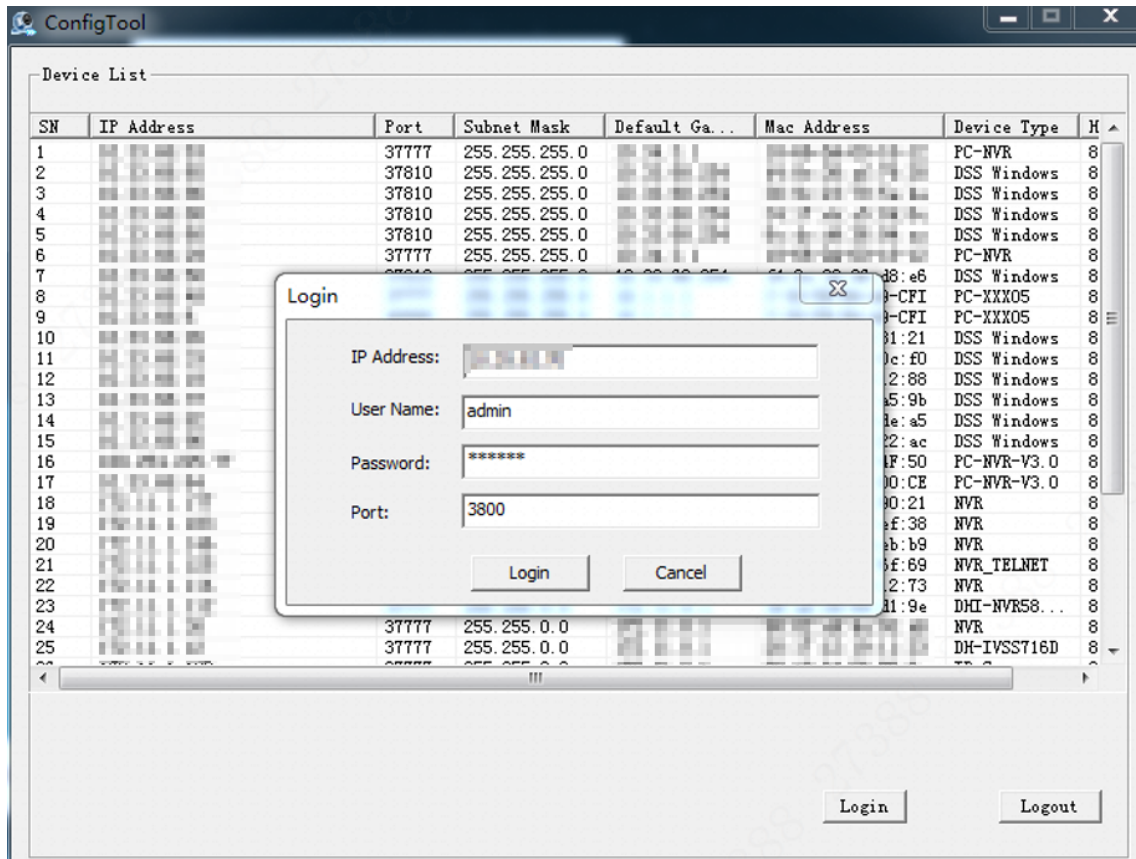
#### Step 4 Update the platform.



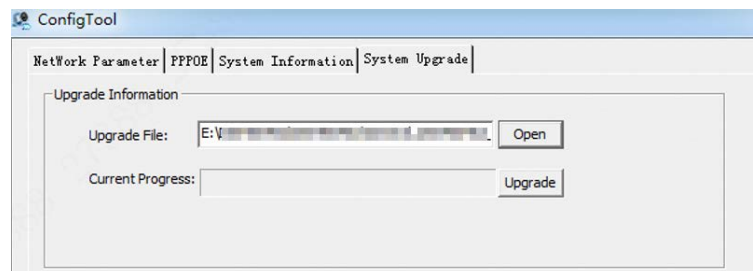
Update through the ConfigTool is only available on V8.0.2.

- Update directly in the configuration system.
  - 1) Click , select the update package in .bin format, and then click **Open**.
  - 2) Click **Update**.

After update, the platform will automatically restart.
- Update by using the Config Tool.
  - 1) Click **Download Config Tool**.
  - 2) Unzip the package you downloaded, and then double-click **ConfigTool** to run it.
  - 3) Click **Login** on the lower-right corner.
  - 4) Enter the information of the platform you want to update, and then click **Login**.



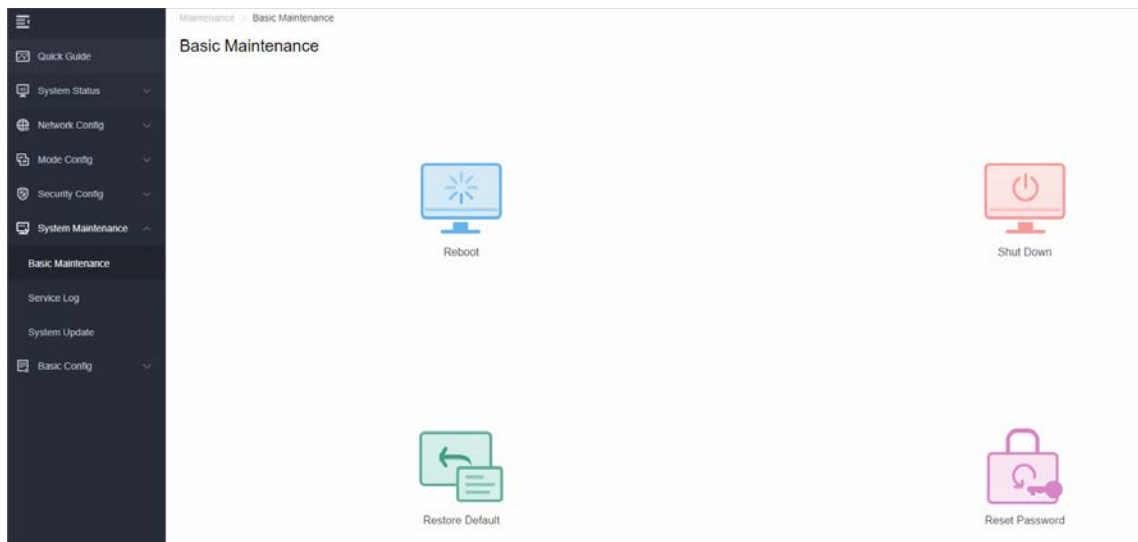
5) Click **Open**, select the update package in .bin format, and then click **Open**.



6) Click **Upgrade**.

After update, the platform will automatically restart.

Step 5 After restart, log in to the configuration system again, and then select **System Maintenance > Basic Maintenance**.



**Step 6** (Optional) Click **Restore Default** to restore the platform to its default settings.



This operation will clear all the data on the platform. Please be advised.

If the platform is working abnormally after update, you can perform this step to clear all the data generated from the old version, only if you do not need them anymore, to try to fix this issue.

**Step 7** Go to <https://platform IP address>, download and install the PC client of the latest version.



## **2 Updating DSS4004-S2 or DSS7016D-S2/DR-S2 from V1.001 to V8.2.0**

Before updating to V8.1.0, you must update V1.001 to V8.0.2, and then to V8.2.0.

Update procedures are the same as updating from V8.0.2/V8.0.4/V8.1.0 to V8.2.0. For details, see the previous chapter.

# Appendix 1 Cybersecurity Recommendations

## Security Statement

- If you connect the product to the Internet, you need to bear the risks, including but not limited to the possibility of network attacks, hacker attacks, virus infections, etc., please strengthen the protection of the network, platform data and personal information, and take the necessary measures to ensure the cyber security of platform, including but not limited to use complex passwords, regularly change passwords, and timely update platform products to the latest version, etc. Dahua does not assume any responsibility for the product abnormality, information leakage and other problems caused by this, but will provide product-related security maintenance.
- Where applicable laws are not expressly prohibited, for any profit, income, sales loss, data loss caused by the use or inability to use this product or service, or the cost, property damage, personal injury, service interruption, business information loss of purchasing alternative goods or services, or any special, direct, indirect, incidental, economic, covering, punitive, special or ancillary damage, regardless of the theory of liability (contract, tort, negligence, or other) , Dahua and its employees, licensors or affiliates are not liable for compensation, even if they have been notified of the possibility of such damage. Some jurisdictions do not allow limitation of liability for personal injury, incidental or consequential damages, etc., so this limitation may not apply to you.
- Dahua's total liability for all your damages (except for the case of personal injury or death due to the company's negligence, subject to applicable laws and regulations) shall not exceed the price you paid for the products.

## Security Recommendations

### **The necessary measures to ensure the basic cyber security of the platform:**

#### **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. Customize the Answer to the Security Question**

The security question setting should ensure the difference of answers, choose different questions and customize different answers (all questions are prohibited from being set to the same answer) to reduce the risk of security question being guessed or cracked.

### **Recommendation measures to enhance platform cyber security:**

#### **1. Enable Account Binding IP/MAC**

It is recommended to enable the account binding IP/MAC mechanism, and configure the IP/MAC of the terminal where the commonly used client is located as an allowlist to further

improve access security.

## 2. **Change Password Regularly**

We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

## 3. **Turn On Account Lock Mechanism**

The account lock function is enabled by default at the factory, and it is recommended to keep it on to protect the security of your account. After the attacker has failed multiple password attempts, the corresponding account and source IP will be locked.

## 4. **Reasonable Allocation of Accounts and Permissions**

According to business and management needs, reasonably add new users, and reasonably allocate a minimum set of permissions for them.

## 5. **Close Non-essential Services and Restrict the Open Form of Essential Services**

If not needed, it is recommended to turn off NetBIOS (port 137, 138, 139), SMB (port 445), remote desktop (port 3389) and other services under Windows, and Telnet (port 23) and SSH (port 22) under Linux. At the same time, close the database port to the outside or only open to a specific IP address, such as MySQL (port 3306), to reduce the risks faced by the platform.

## 6. **Patch the Operating System/Third Party Components**

It is recommended to regularly detect security vulnerabilities in the operating system and third-party components, and apply official patches in time.

## 7. **Security Audit**

- Check online users: It is recommended to check online users irregularly to identify whether there are illegal users logging in.
- View the platform log: By viewing the log, you can get the IP information of the attempt to log in to the platform and the key operation information of the logged-in user.

## 8. **The Establishment of a Secure Network Environment**

In order to better protect the security of the platform and reduce cyber security risks, it is recommended that:

- Follow the principle of minimization, restrict the ports that the platform maps externally by firewalls or routers, and only map ports that are necessary for services.
- Based on actual network requirements, separate networks: if there is no communication requirement between the two subnets, it is recommended to use VLAN, gatekeeper, etc. to divide the network to achieve the effect of network isolation.

## More information

Please visit Dahua official website security emergency response center for security announcements and the latest security recommendations.

ENABLING A SAFER SOCIETY AND SMARTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: [www.dahuasecurity.com](http://www.dahuasecurity.com) | Postcode: 310053

Email: [dhoverseas@dhvisiontech.com](mailto:dhoverseas@dhvisiontech.com) | Tel: +86-571-87688888 28933188