Security Advisory: Guidance for Older Dahua Camera Models

Recently, we have received reports from some users regarding anomalous behaviors on certain older models of Dahua IP cameras. Our technical team has confirmed that these incidents may result from unauthorized external access attempts.

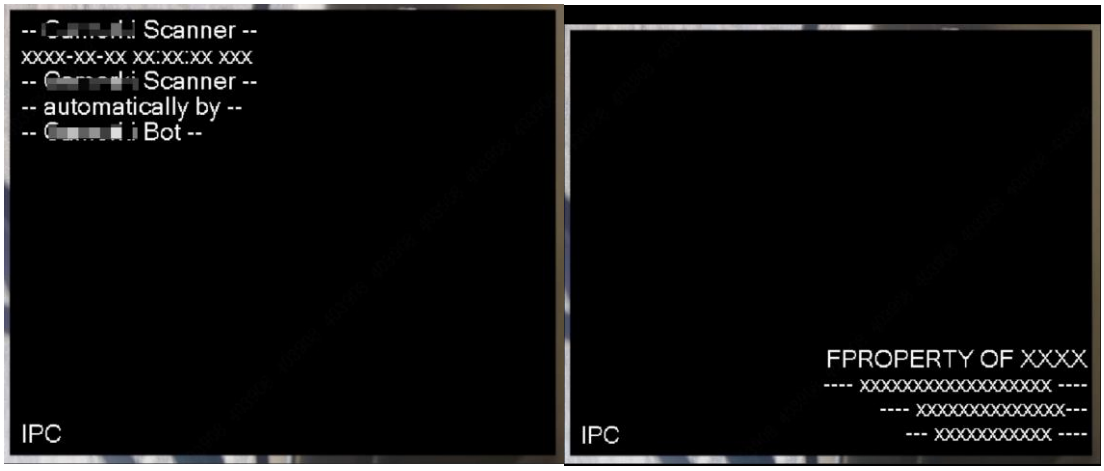
To help protect your system security and data privacy, we are issuing this advisory with step-by-step guidance for identification, recovery, and long-term hardening.

We also take this opportunity to remind you to keep upgrading your product with the latest FW.

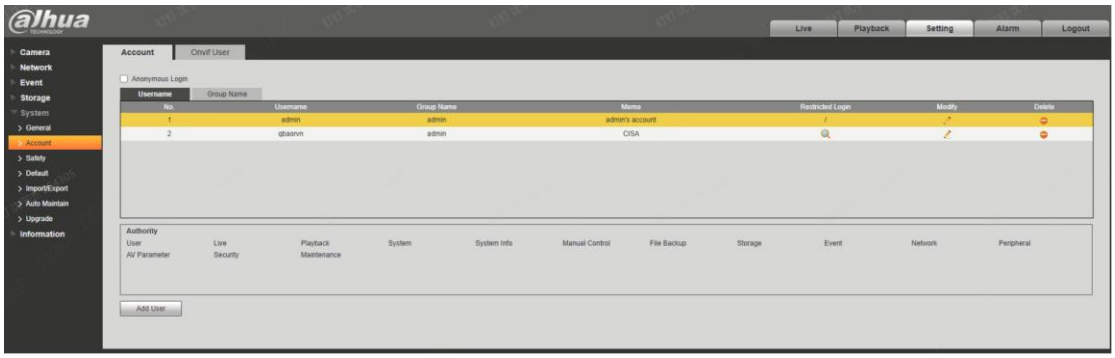
Part I. How to identify Potential Issues?

If you notice any of the following symptoms, we recommend taking immediate action to secure your device:

1. **The On-Screen Display (OSD) has been altered**, and the camera live preview displays unfamiliar sentences or watermarks like the examples provide:



2. **Unauthorized user accounts exist on the device**, suspicious usernames that were not created or authorized by you.
   Generally, the only device default account is "**admin**", other accounts may be suspicious.



Part II. Recommended Recovery steps

We recommend the following steps to solve the reported issue and enhance the protection of your device.

1. Upgrade the firmware of the affected device to latest version.

Note: Before upgrading the device, you need to acquire the latest firmware first.

Please access Dahua online firmware upgrade pack tool and follow the instruction on the website to acquire the FW. Or you can contact local technical support for help.

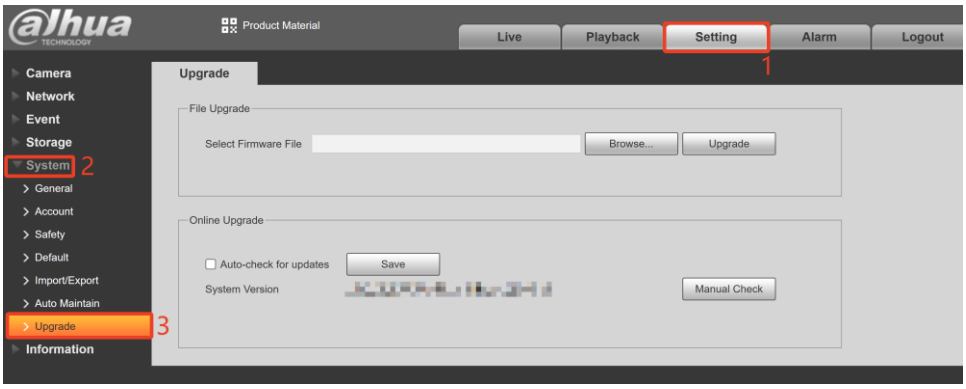
1.1. After you downloaded the upgrade pack, extract the upgrade file from the pack.

Right click the downloaded upgrade pack, select “Extract All” and choose a folder to save the extracted files. If your operating system does not support extract compressed file, please install a decompression software (7-zip, etc.) first.

1.2. Open browser and access the IP camera website.

If you do not know the device IP or address, you can install and use ConfigTool to search the device in your local network.

1.3. Go to "Setting – System – Upgrade" page.



1.4. Click "Browse" button, select the extracted file.

The file name should be like "DH_IPC-xxxxxxx-V2.xxxxxxx.bin".

1.5. Click "Upgrade" button, wait for the device finish upgrade and reboot.

⚠Caution:
Please do not disconnect the power supply of your device during upgrade, it may damage the device!

If upgrade failed or you met problem on upgrading, please contact your local technical support for help.

1.6. Log in the device website after device boot up, go to "Setting – Information – Version" page to confirm the firmware is upgraded successfully.

2. If there is any account not removable except "admin", please do factory default to restore the camera to uninitialized state.

⚠Caution:
Factory default will clear all configuration and settings on the device.
Please backup your configuration before doing factory default.

A. Find the reset button on the device, long press button for over 10 seconds, until device is rebooting.

Generally, the reset button is near the SD card slot area. Not all devices have hardware reset button. If you do not know if there is reset button on your device, please refer to the device's Quick Start Guide.

B. If there is no reset button on the device, you can use web to operate.

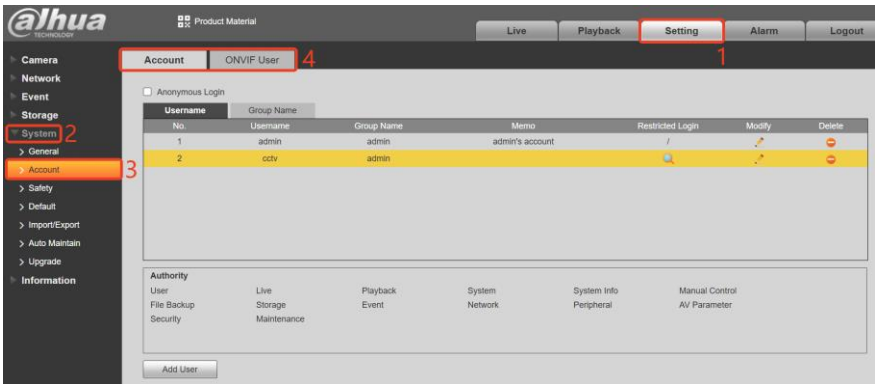
For the instruction, please refer to this document.

C. If there is no reset button and device does not support web management, please use ConfigTool to reset device to factory default.

For the instruction, please refer to Config Tool User Manual.

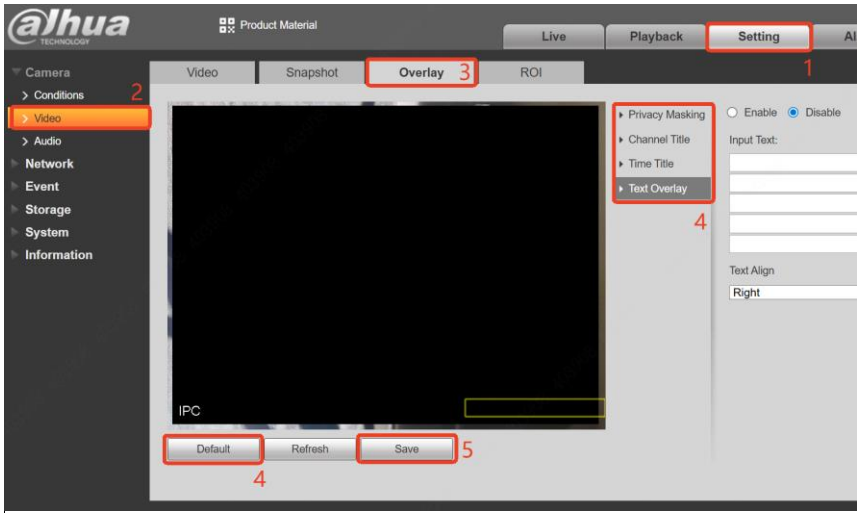
After device is reset, you need initialize it to use normally. For the initialization instruction, please refer to this document.

3. **Check the device accounts and remove accounts that were not created or are being used by the end user.**
   - **3.1.** Open browser and access the IP camera website.
   - **3.2.** Go to “Setting – System – Account” page.
   - **3.3.** Check “Account” and “ONVIF Users” tab, if there are suspicious or unknown accounts, click delete icon, only keep needed accounts.



   - **3.4.** **(Optional, but highly recommended) Change the accounts password to strong password.**

4. **Restore the device's OSD configuration to its unaltered state.**
   - **4.1.** Open browser and access the IP camera website.
   - **4.2.** Go to “Camera – Video – Overlay” page.



   - **4.3.** Click “Default” button to restore all on screen display content to default value. Or check every option in the page to customize the content.
   - **4.4.** Click “Save” button to take effects.

Appendix: Security recommendations

We *strongly* recommend implementing the following measures to improve your device’s security:

1. **Download and apply the latest available software/firmware version promptly.**
2. **Change the password for the currently used account to a strong, complex one.**

3. **Update the password regularly.**
4. **Deploy the device within a local area network (LAN) or configure access control policies to restrict access only to trusted IP addresses.**

You may also refer to our security best practices document for further configuration guidance: https://material.dahuasecurity.com/uploads/soft/20230803/Best-Practices.docx