

Title:	How to upgrade firmware to guard against potential vulnerability	Version: 1.0	Current	Date:	23/09/2021
Product:	Mixed products			Page:	1 of 9
Action Required:	Information Only				

How to Upgrade Firmware to Guard Against Potential Vulnerabilities

Summary

A command injection vulnerability in the web server of some Hikvision products has been identified. In the case of insufficient input validation, an attacker can exploit the vulnerability to launch a command injection attack by sending some messages with malicious commands.

First, identify the products affected by the vulnerability, then find that product's specific updated firmware using the following link:

[Security Notification- Command Injection Vulnerability in Some Hikvision products | Hikvision US | The world's largest video surveillance manufacturer](#)

Note: Please do not power off any device during the upgrade process.

Hikvision offers multiple ways to upgrade firmware. Users can choose from among five upgrade methods according to the device type and/or preference.

Please continue reading and select the appropriate method for your application(s).

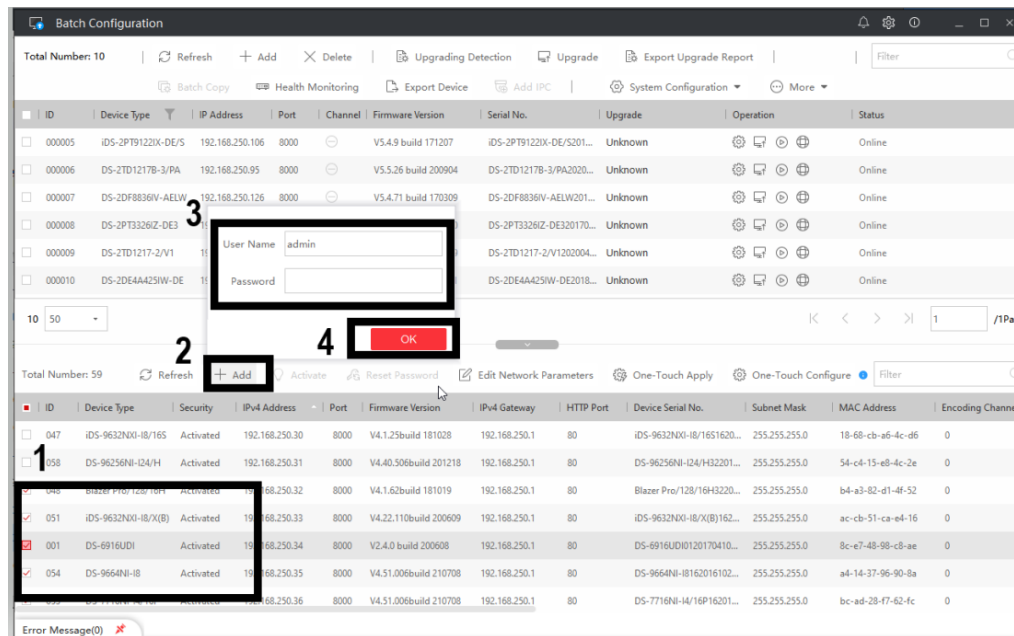
Title:	How to upgrade firmware to guard against potential vulnerability	Version: 1.0	Current	Date:	23/09/2021
Product:	Mixed products			Page:	2 of 9
Action Required:	Information Only				

Method 1: Batch Upgrade (NVR, IPC, & PTZ products)

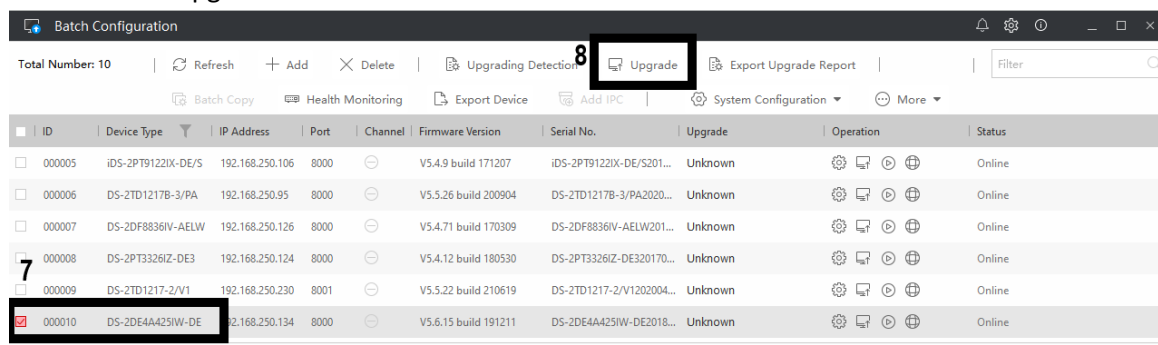
First, please download the Batch Configuration Tool at this link:

<https://us.hikvision.com/en/support-resources/downloads/tools>

1. After downloading and opening the software, click on the devices requiring the upgrade
2. Then click on “+Add”
3. Enter the User Name and Password
4. Then click “OK”

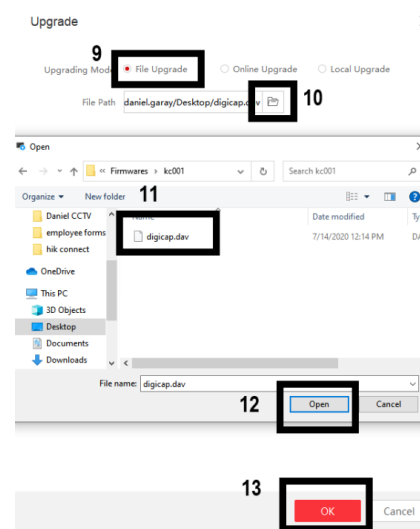


5. Search for the device on Hikvision’s official website link also provided above: [Fix Firmware Download Index](#)
6. Click on “Download” to download the firmware
7. After downloading the firmware, select the device requiring the upgrade
8. Then click on “Upgrade”



Title:	How to upgrade firmware to guard against potential vulnerability	Version: 1.0	Current	Date:	23/09/2021	
Product:	Mixed products				Page:	3 of 9
Action Required:	Information Only					

9. Select "File Upgrade"
10. Click on the file path
11. Select the Digicap.dav file
12. Click on "Open"
13. Then click "OK" to start the upgrade process



ID	Device Type	IP Address	Port	Channel	Firmware Version	Serial No.	Upgrade	Operation	Status
000001	DS-2CD7126G0/L-IZS	192.168.250.103	8000		V5.5.81 build 180910	DS-2CD7126G0/L-IZS20...	Unknown		Online
000002	DS-2CD7526G0-IZHS	192.168.250.127	8000		V5.6.0 build 190428	DS-2CD7526G0-IZHS201...	Unknown		Online
000003	PCI-LB15F2SL	192.168.250.117	8000		V5.5.160 build 210416	PCI-LB15F2SL20201119A...	Unknown		Online
000004	PTZ-N5225I-AE	192.168.250.119	8000		V5.5.3 build 180211	PTZ-N5225I-AE20170929...	Unknown		Online
000005	iDS-2PT9122IX-DE/S	192.168.250.106	8000		V5.4.9 build 171207	iDS-2PT9122IX-DE/S201...	Unknown		Online
000006	DS-2TD1217B-3/PA	192.168.250.95	8000		V5.5.26 build 200904	DS-2TD1217B-3/PA2020...	Upgrade completed.		Online
000007	DS-2DF8836IV-AELW	192.168.250.126	8000		V5.4.71 build 170309	DS-2DF8836IV-AELW201...	Unknown		Online
000008	DS-2PT3326IZ-DE3	192.168.250.124	8000		V5.4.12 build 180530	DS-2PT3326IZ-DE320170...	Unknown		Online
000009	DS-2TD1217-2/V1	192.168.250.230	8001		V5.5.22 build 210619	DS-2TD1217-2/V1202004...	Unknown		Online
000010	DS-2DE4A425IW-DE	192.168.250.134	8000		V5.6.15 build 191211	DS-2DE4A425IW-DE2018...	Unknown		Online

Title:	How to upgrade firmware to guard against potential vulnerability	Version: 1.0	Current	Date:	23/09/2021
Product:	Mixed products			Page:	4 of 9
Action Required:	Information Only				

Method 2: Upgrade via Web Interface (NVR, IPC, & PTZ products)

Step 1: Input the IP address to log in the web interface.

Step 2: Click 'Configuration'

Step 3: Click 'Maintenance'

Step 4: Click 'Browse'

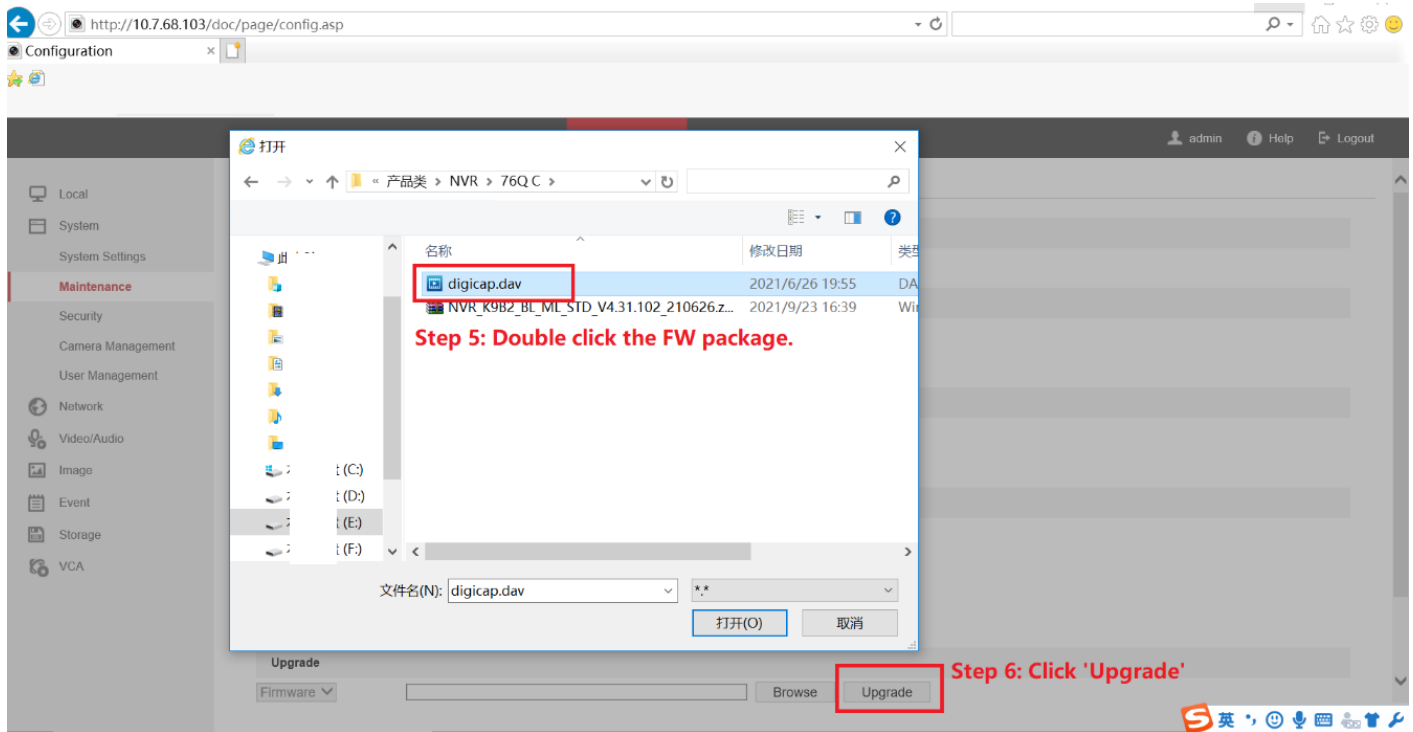
Step 1: Input the IP address to log into the web interface.

Step 2: Click on the “Configuration” tab

Step 3: Under the “System” menu, click on “Maintenance”

Step 4: Under the “Upgrade” header, click on “Browse”

Title:	How to upgrade firmware to guard against potential vulnerability	Version: 1.0	Current	Date:	23/09/2021
Product:	Mixed products			Page:	5 of 9
Action Required:	Information Only				

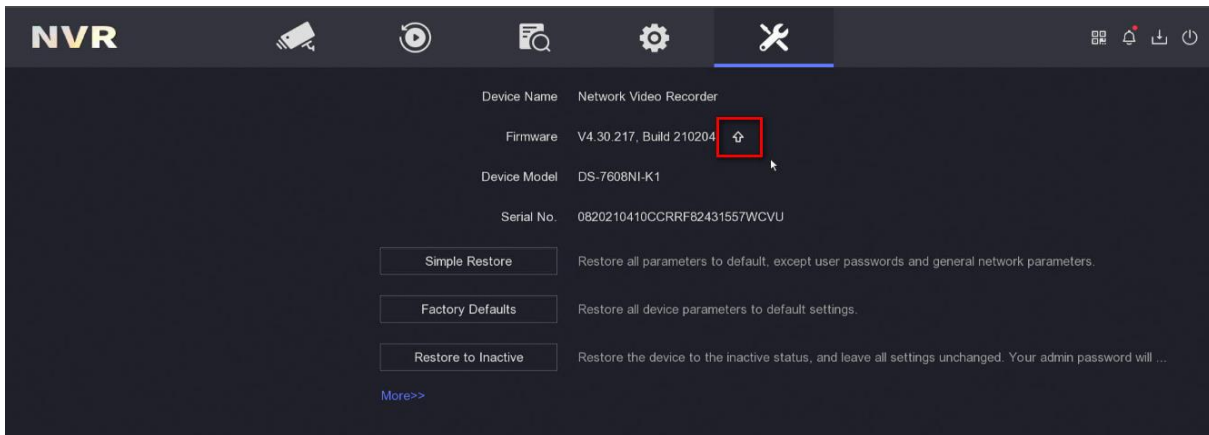


Step 5: Choose the FW package on your PC. Please note that the FW package must be decompressed.


Step 6: Click on “Upgrade.” The device will reboot automatically after upgrade is complete.

Title:	How to upgrade firmware to guard against potential vulnerability	Version: 1.0	Current	Date:	23/09/2021
Product:	Mixed products			Page:	6 of 9
Action Required:	Information Only				

Method 3: Upgrade Using Local GUI (NVRs)

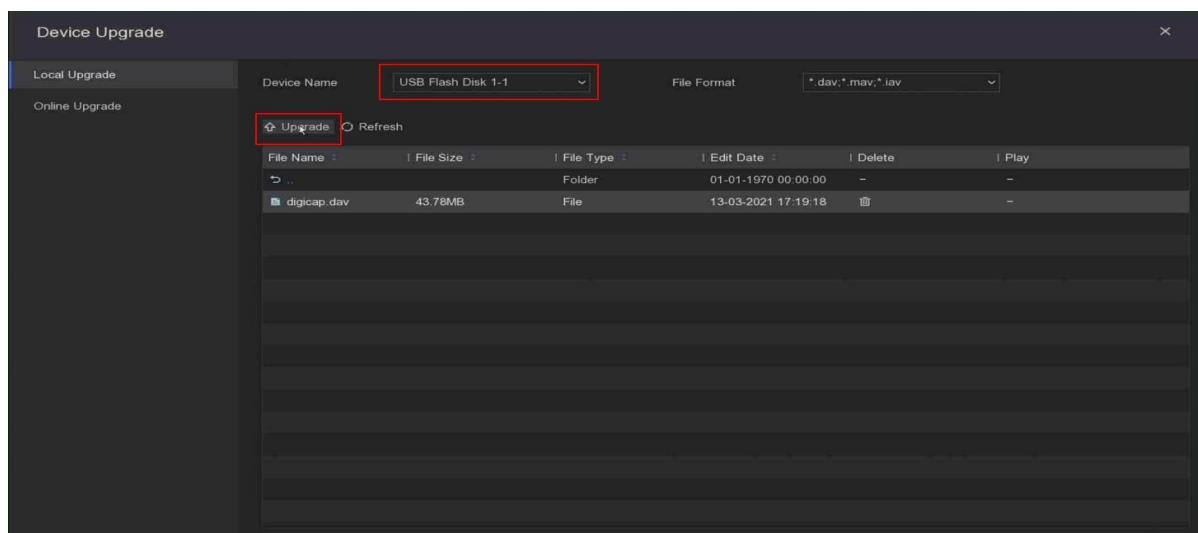


Step 1: Go to Maintenance Tab.

Step 2: Click on the icon: 

Step 3: Insert the USB drive with the FW package (this must be decompressed first); the NVR will then detect the USB drive and show the files listed. Choose the FW package from the list.

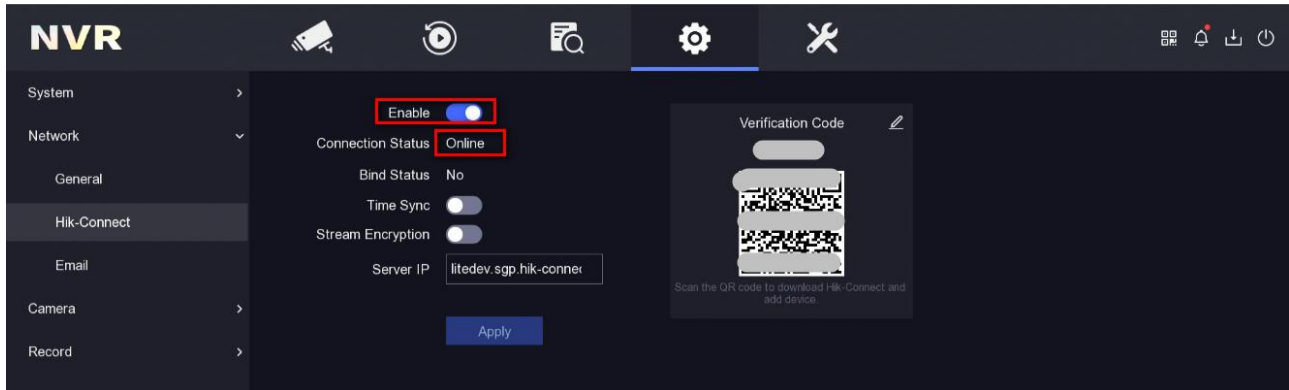
Step 4: Click on "Upgrade." The device will reboot automatically after upgrade is complete.



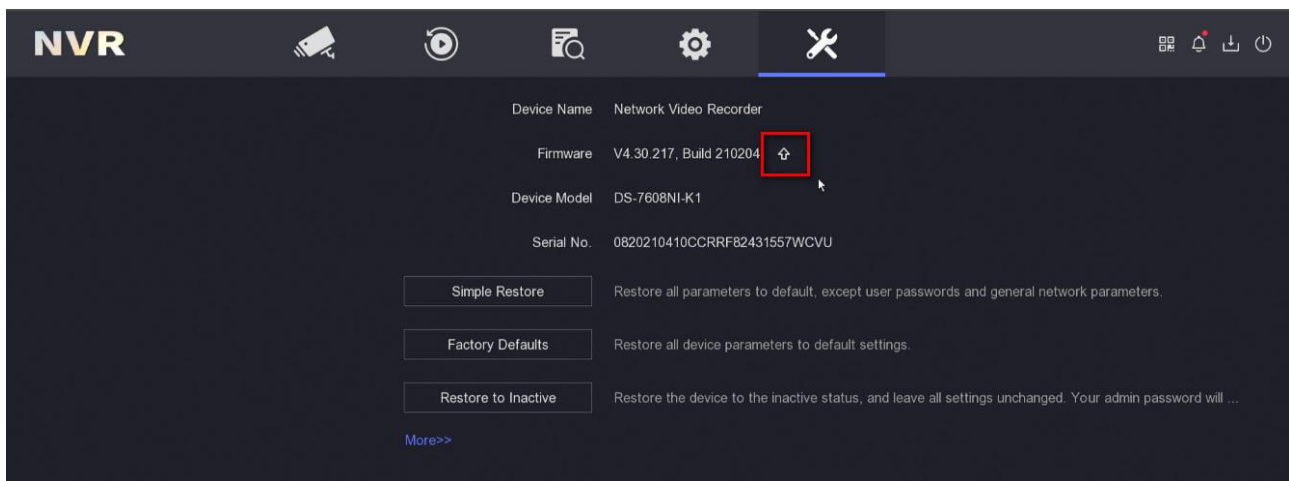
Title:	How to upgrade firmware to guard against potential vulnerability	Version: 1.0	Current	Date:	23/09/2021
Product:	Mixed products			Page:	7 of 9
Action Required:	Information Only				

Method 4: Online Upgrade Using Local GUI (NVRs)

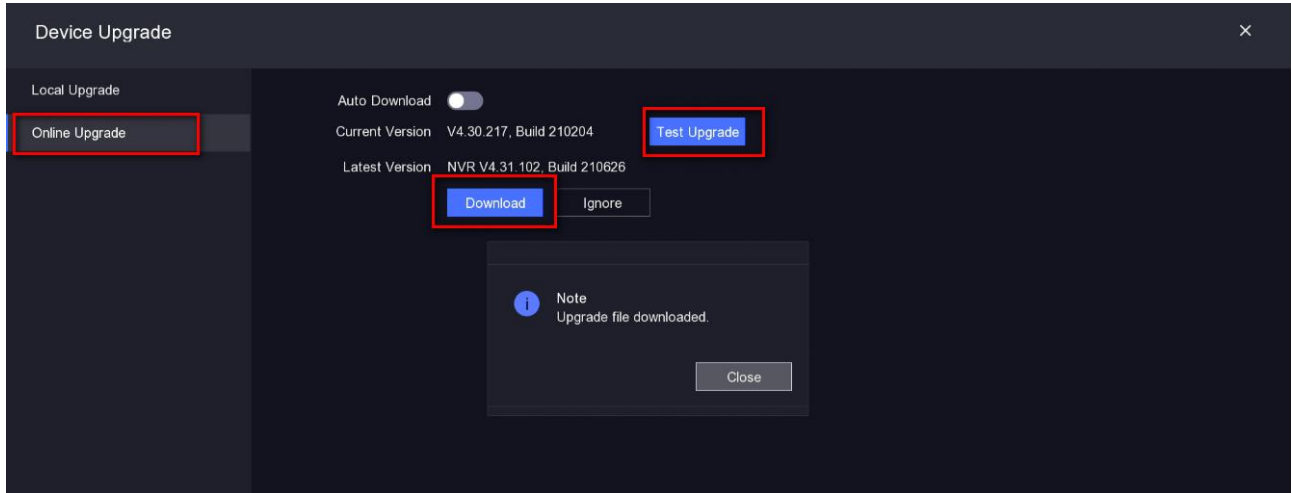
Step 1: Enable the platform in Network > Hik-Connect



Step 2: After device is online, click on the “Update” button and enter the online upgrade interface



Title:	How to upgrade firmware to guard against potential vulnerability	Version: 1.0	Current	Date:	23/09/2021
Product:	Mixed products			Page:	8 of 9
Action Required:	Information Only				



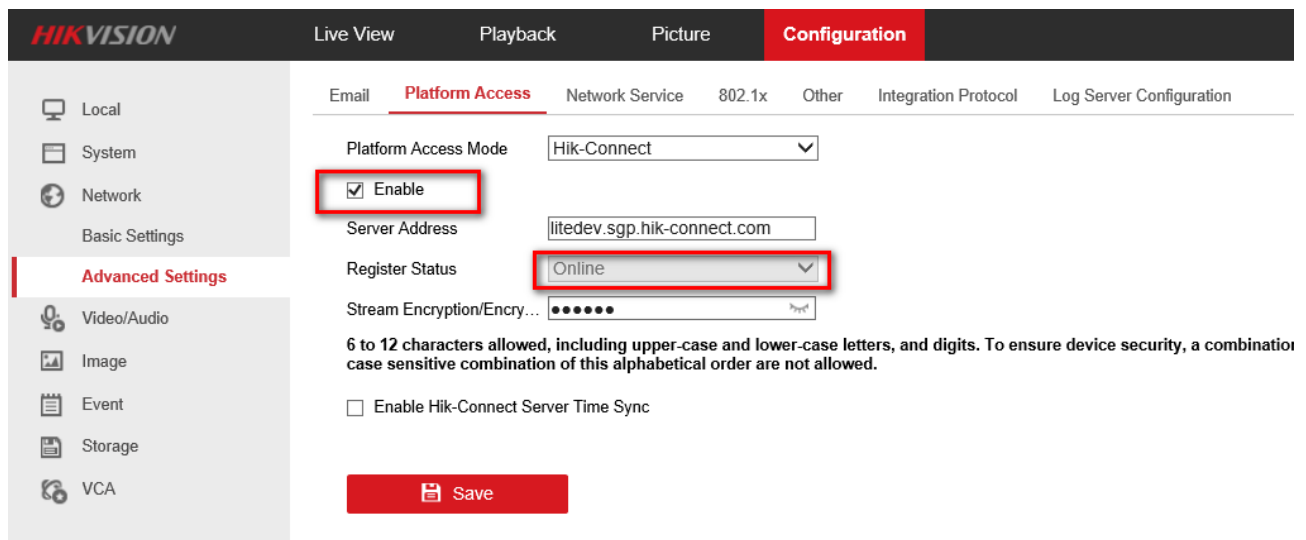
Step 3: Click “Test Upgrade” to obtain latest version, then “Download” for the firmware file and your device will be upgraded.

Title:	How to upgrade firmware to guard against potential vulnerability	Version: 1.0	Current	Date:	23/09/2021
Product:	Mixed products			Page:	9 of 9
Action Required:	Information Only				

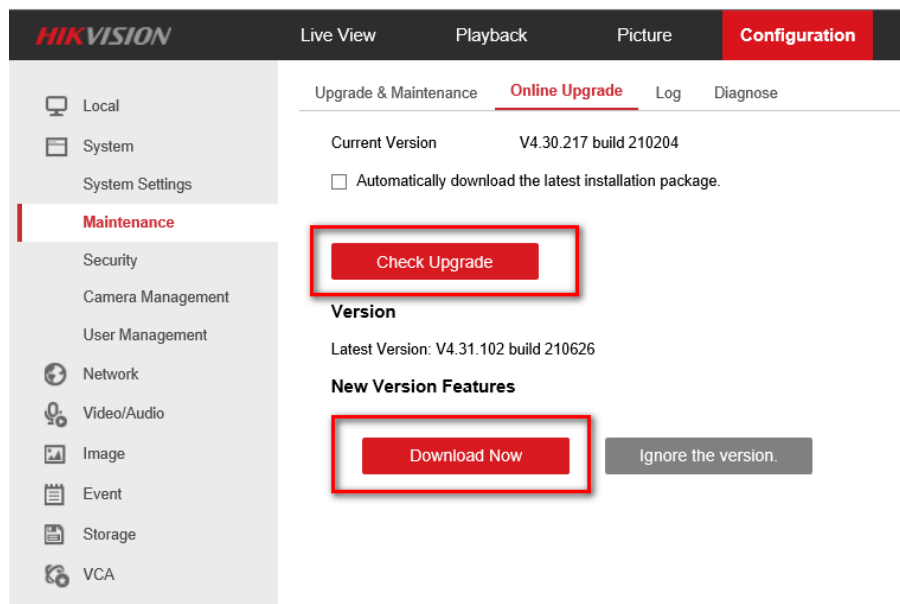
Method 5: Online Upgrade via Web Page

Step 1: First, use this path to enable the platform:

Configuration > Network > Advanced Settings > Platform Access



Step 2: After the device is online, go to Configuration > Maintenance > Online Upgrade, click on “Check Upgrade” to obtain the latest version info; then download the firmware file to upgrade your device.



Title:	How to upgrade firmware to guard against potential vulnerability	Version: 1.0	Current	Date:	23/09/2021
Product:	Mixed products			Page:	10 of 9
Action Required:	Information Only				



Hikvision USA

www.hikvision.com

Technical Support Hotline: (909) 612 - 9039