



# How to prevent your DVR from getting hacked

## 1: How to prevent the device being hacked?

Do not use the default password as login password, do not use a simple password, do not tell password to others. It will be best to change the password regularly. DVR password is 6 characters long. You can use a combination of letters (lower case or upper case letters), numbers and special characters.

### **Recommendations for Personalizing the Security Settings on your Optiview equipment**

Follow these guidelines, provided by our in-house Technical Support team, to update and personalize the security settings on your embedded DVR / NVR for maximum security.

- Create your own personal User Name & Password under the "Admin" group

- Be creative when creating your password (i.e. include uppercase, lowercase and numbers)

- Routinely change your password(s) every 60 - 90 days

- Modify the default ports for viewing your system remotely

- Limit the number of remote connections

- Change the default Lock Time from 30 minutes to the minimum available

- Setup Email Notifications for illegal log-in attempts

- Lower the number of failed log-in attempts before the DVR / NVR locks down

- Update the start / end dates for Daylight Savings Time (DST)

**MAKE SURE YOU DON'T FORGET THE PASSWORD.** Send yourself an email with the DVR password so you can retrieve it anytime, anywhere in case you forgot the password. It will take 2-3 days for us to retrieve or reset your forgotten password.

## 2: What I can do if device has been hacked?

### **DVR/NVR SYSTEM RESTORE QUICK GUIDE (for security-compromised system)**

Before starting any steps on a system that has been hacked, unplug the network cable from the DVR/NVR.

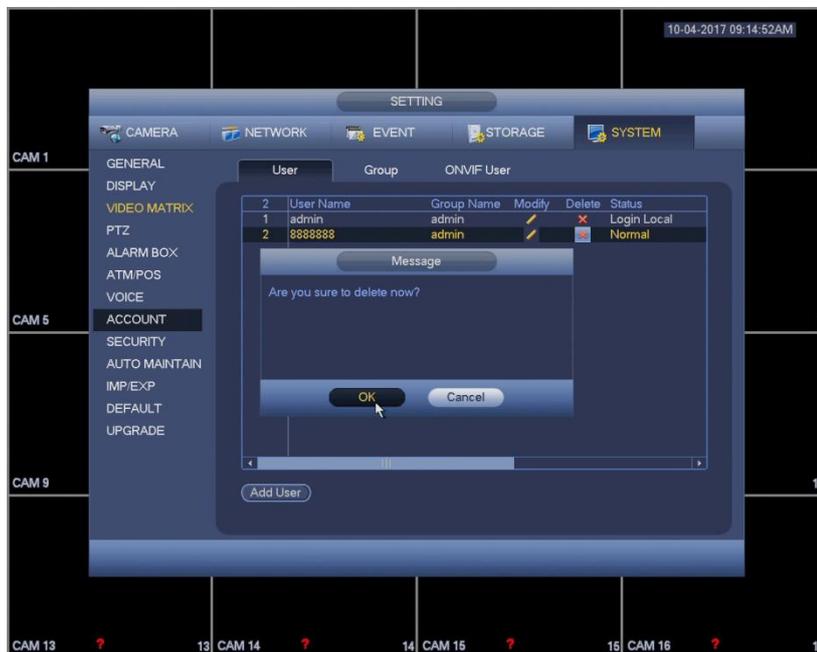
Here's a list of all the settings you need to change on your DVR/NVR system settings:

1. Delete 888888 and 666666 account names after updating the firmware;

2. Modify “admin” account password. Combine upper case & lower case letters, numbers and special characters. It must have 8-10 characters on username and password field box.
3. Restore to “Factory Default” to all the settings of all the DVR/NVR.
4. Restore correct IP address for the DVR/NVR and change ALL Connection port numbers.
5. To enable remote viewing without the need to reconfigure router/firewall, enable P2P.
6. Reconfigure your router port forwarding settings after all ports have been changed at the DVR/NVR, if you prefer using your static IP address from ISP.
7. Reconfigure your remote PC, tablet or smart phone’s connection profile to reflect with the latest passwords and port numbers that you just updated from the previous steps as mentioned above.
8. Go to [OptiviewUSA.com](http://OptiviewUSA.com) → Firmware Update web page for the latest document how to update firmware on a DVR/NVR.

### Get Started Restoring a Hacked DVR/NVR System

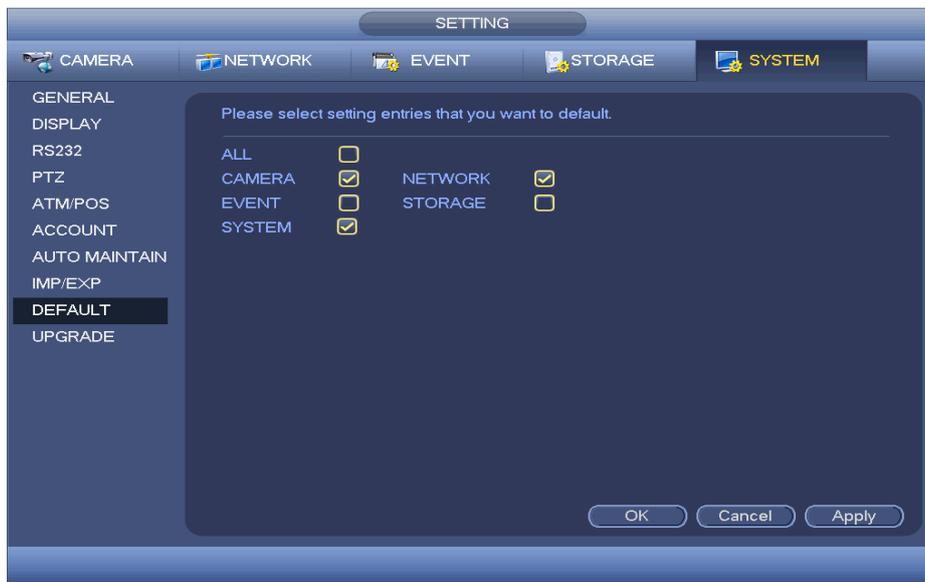
1. Delete 666666 account names. If other usernames are listed on the Account menu screen such as a “system” user name, delete it.



9. Modify “admin” account password. Combine upper case & lower case letters, numbers and special characters. Username and password field box must have 8-10 characters. Older DVR systems are limited to 6 characters for the password field.

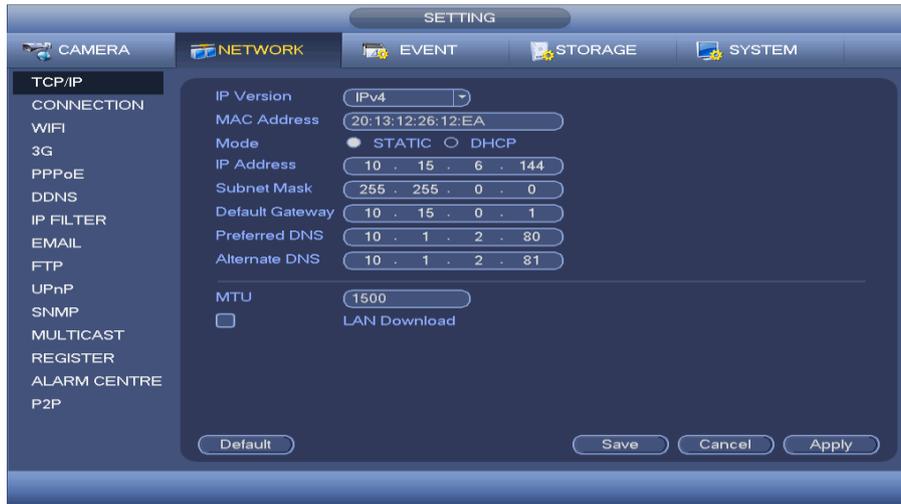


2. Restore to "Default" the color settings, camera name of all the cameras and network/IP address of the system.



3. Restore correct IP address for the DVR/NVR and change ALL Connection port numbers.

Below is an illustration for setting the IP address of the system.



If you need to use a specific IP address, click on “Static” and assign your private IP address. Otherwise, select DHCP. If your DVR is not getting an IP address from your DVR, go back to Step# 2 and this time, do an “ALL” settings factory default.

4. Change connection ports. Suggested port numbers are shown below. Remember to reconfigure your router with these new ports at the port forwarding menu of your router. This is to mitigate the possibility of unauthorized using of the common port numbers for specific connection type.

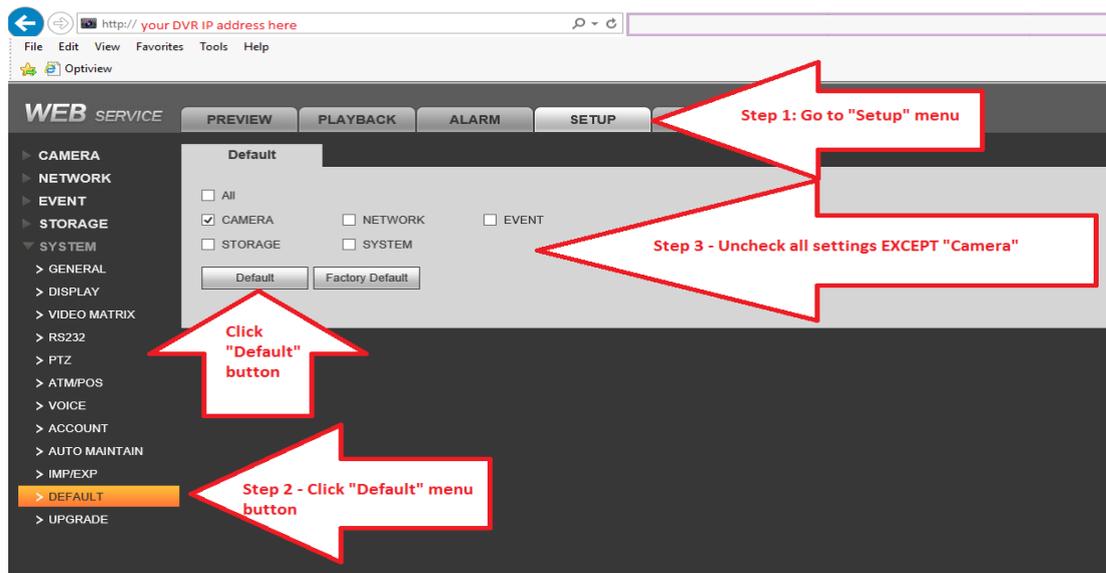


If you can access your DVR using Internet Explorer, you can do a system restore on your DVR/NVR camera image settings using the following steps:

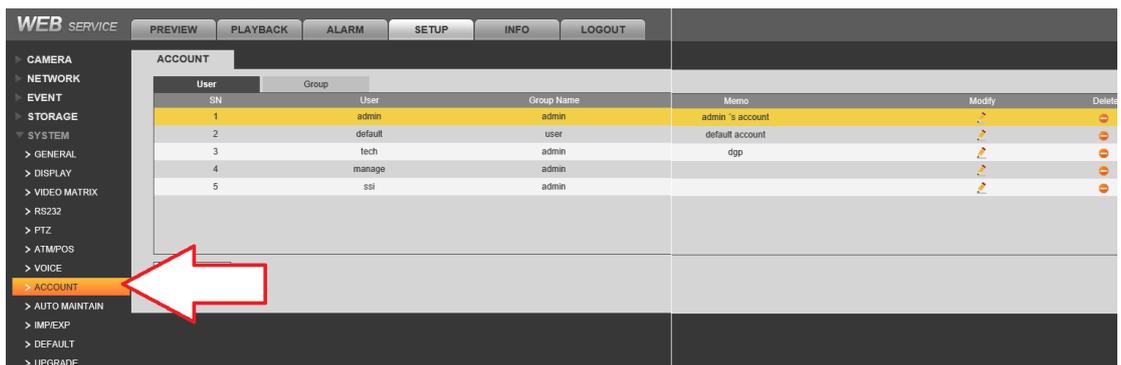
1. Open Internet explorer and enter the network address of your DVR.



- Set Camera settings to “default” by following the steps below. Do not click “Factory Default” button. Follow exactly the steps mentioned. This will restore the live camera view and removed the camera name “hacked” from the LIVE screen.



- Modify the user account information such as password or creating new user account name and password.



- Modify the default port numbers used by the DVR/NVR system. You need to be at the site when changing these ports numbers so you can still able to access the configuration menu of the system. Illustration below shows an example in changing the default port numbers at your DVR/NVR system under Network → Connection menu:

**WEB SERVICE**    PREVIEW    PLAYBACK    ALARM    **SETUP**    INFO

▶ CAMERA  
▼ NETWORK  
  > TCP/IP  
  > **CONNECTION**  
  > WIFI  
  > 3G/4G  
  > PPPoE  
  > DDNS  
  > IP FILTER  
  > EMAIL  
  > FTP  
  > UPnP  
  > SNMP  
  > MULTICAST  
  > REGISTER

**CONNECTION**

Max Connection	<input type="text" value="128"/>	(0~128)
TCP Port	<input type="text" value="57777"/>	(1025~65535)
UDP Port	<input type="text" value="57778"/>	(1025~65535)
HTTP Port	<input type="text" value="8088"/>	(1~65535)
HTTPS Port	<input type="text" value="4338"/>	(1~65535)
RTSP Port	<input type="text" value="5448"/>	(1~65535)
RTSP Format	rtsp://<User Name>:<Password>@<IP Address>:<Port>/cam/realmonitor?channel: Channel, 1-32; subtype: Code-Stream Type, Main Stream 0, Sub Stream 0-31	