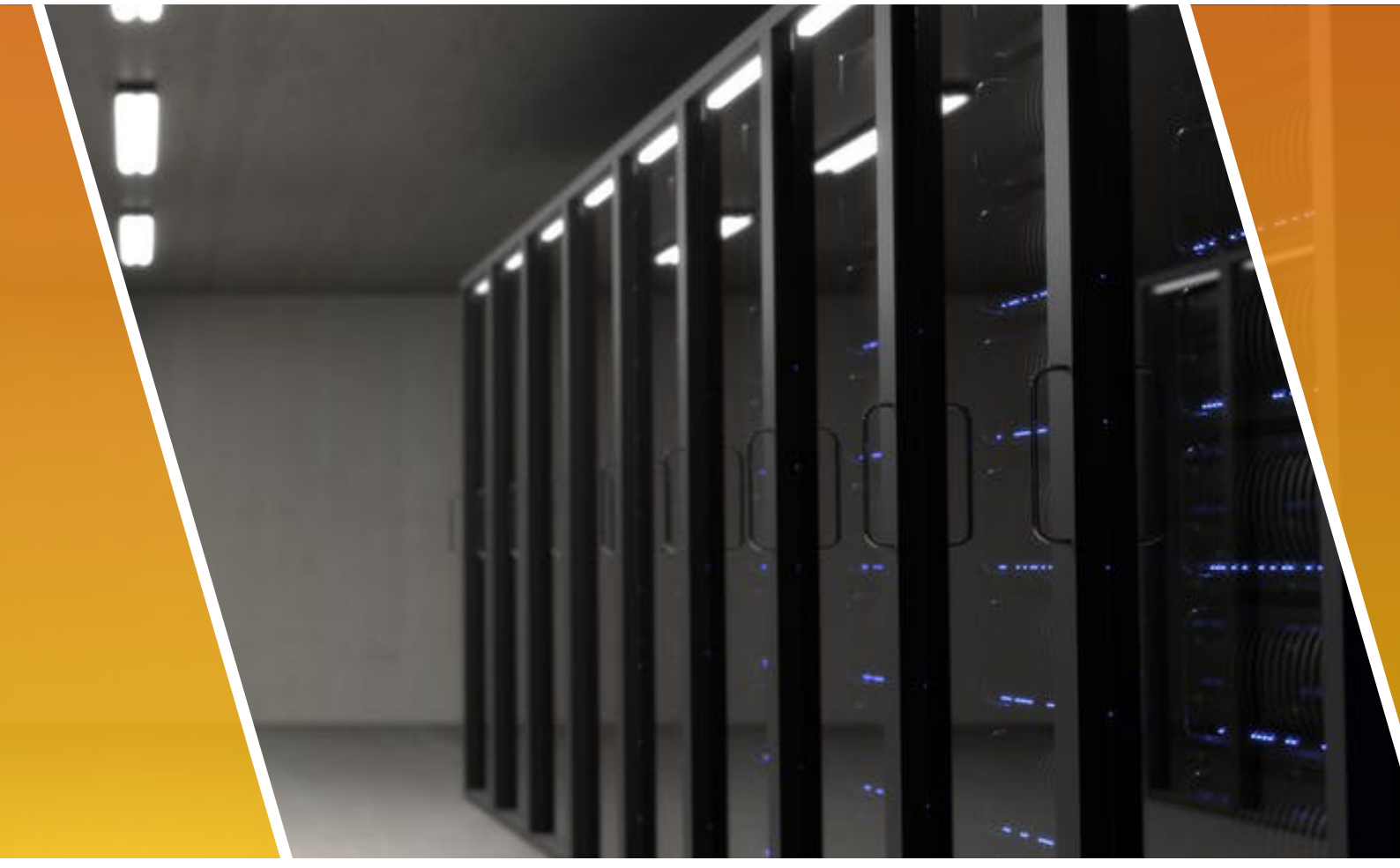


Cyber Security
Best Practice

Official UK distribution partner

tel: +44 (0)1457 874 999 | fax: +44 (0)1457 829 201 | email: sales@cop-eu.com | web: www.cop-eu.com

Cyber Security Best Practice

With the increased popularity of remote access to network video surveillance systems, many more CCTV products are being connected to the internet. Unfortunately, at the same time, any device connected to the world wide web is becoming more and more vulnerable to a cyber attack.

Please rest assured that COP security, in conjunction with our suppliers, are doing our upmost to ensure that the products we supply are as secure as current technology allows. In addition, we are providing as much information as possible to help combat the threat of cyber attacks. This includes real time security notices, and download access to the latest firmware, which can be found within the cyber security section on our website.

It should be noted that despite best efforts, no method of transmission over the Internet can be deemed as perfectly secure. No one can guarantee absolute security due to the nature of the technology and the potential problems this can create.

However, if COP Security learns of any actual or potential security breach, we will notify our customers so that appropriate protective action can be taken.

From mandatory and advisory setting changes, through to firmware upgrades, the information contained in this booklet is invaluable in helping to keep your system secure.

Mandatory actions to be taken

Change Passwords and Use Strong Passwords

Update Firmware

Recommendations to improve your network security

Use P2P

Change Default HTTP and TCP Ports

Enable IP Filter

Change ONVIF Password

Forward Only Ports You Need

Limit Features of Guest Accounts

Disable UPNP

Physically Lock Down the Device

Connect IP Cameras to the PoE Ports on the Back of an NVR

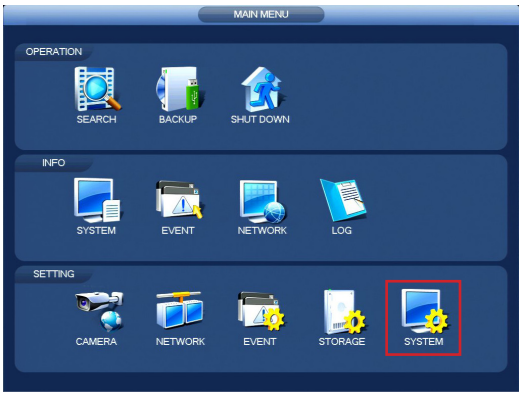
Isolate NVR and IP Camera Network

Change Passwords and Use strong passwords

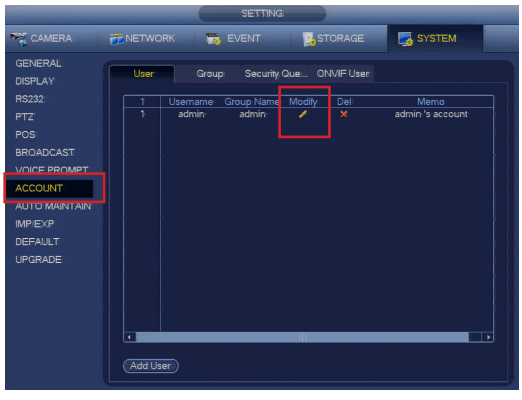
This should go without saying, but the number one reason a system is compromised is due to weak or default passwords. We recommend never using a default password and choosing a strong password whenever possible. A strong password is at least 8 characters and is made up of a combination of special characters, numbers and upper & lower case letters.

To change the password on the system follow the steps below:

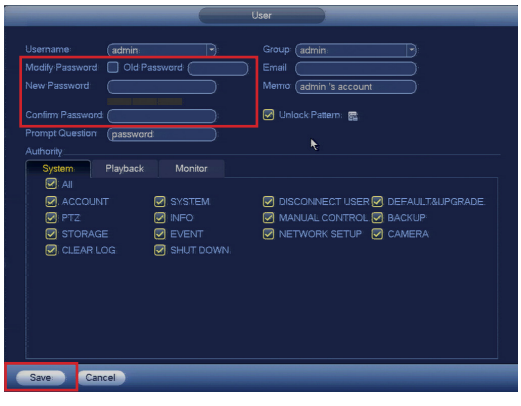
1. Enter the Main Menu (Right Click > Main Menu)



2. Select System (Bottom Right) and click Account from the left sub menu list.
   On the Account you want to change the password for, click the Modify Icon



3. Select the modify password check box and enter your current password into the old password text box. Enter your new password into the new password & confirm password text boxes. It is recommended to choose a strong password with a minimum of 8 characters combining lower case, upper case, numbers & special characters.



4. Click Save to confirm the new password changes

Changes Passwords Regularly

Regularly change the credentials of your devices to help ensure that only authorised users are able to access the system. This is especially important when an employee with access to the system leaves a company.

Mandatory actions to be taken

Updating Your Firmware

It is highly recommended that you upgrade your device to the most up to date firmware available. The latest firmware will normally include updates to features & settings and remove any bugs identified in previous versions. Firmware upgrades ensure that you have latest security updates to help protect your devices.

Checking Your Firmware

At the device, make a note of the part number, build date and version number. You will need this information to make sure any updates have been done successfully.

Find your devices part number on our website **cop-eu.com/upgrading-your-firmware** and compare version numbers. If your version number is older, please download the latest firmware. Once you have downloaded the latest firmware follow the update instructions below.

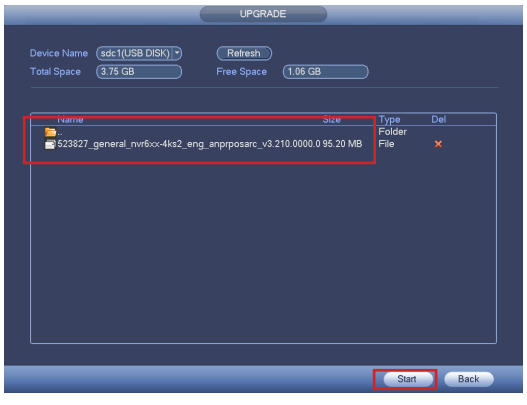
Update via USB

It is recommended that the following steps are carried out by a CCTV engineer.

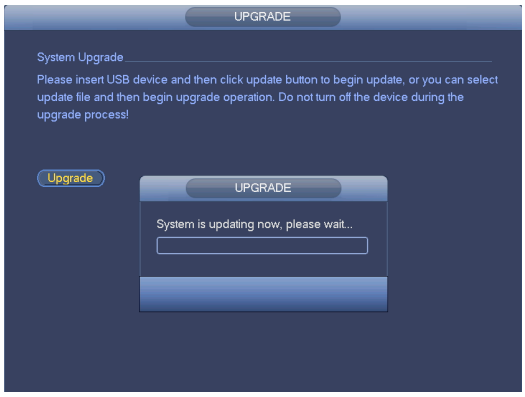
1. Copy downloaded firmware to a USB stick
2. Log into the menu of the recorder (Right Click > Main Menu) using your login credentials
3. Insert the USB stick into a USB port on your recorder
4. After a few seconds, a pop up should appear
5. Click System Upgrade

6. The Upgrade menu should now be displayed, click Upgrade

7. Locate the firmware file, select it and Click Start



9. The recorder will restart as part of the upgrade process, once the recorder has rebooted the update is complete



10. Log into the menu of the recorder (Right Click > Main Menu) using your login credentials
11. Go to System (info) > Version and compare the build date to the one you wrote down. The build date shown should be a newer date.

Firmware can also be upgraded via Web Browser and Smart PSS software. Full details can be found on our website **cop-eu.com/upgrading-your-firmware.**

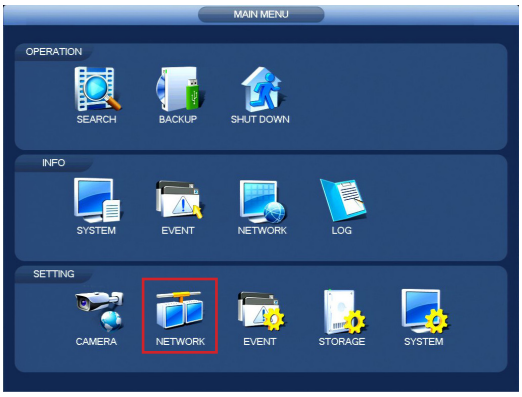
Recommendations to improve your network security

Use P2P

We recommend using P2P when connecting your device to the internet. P2P hides the device from public view.

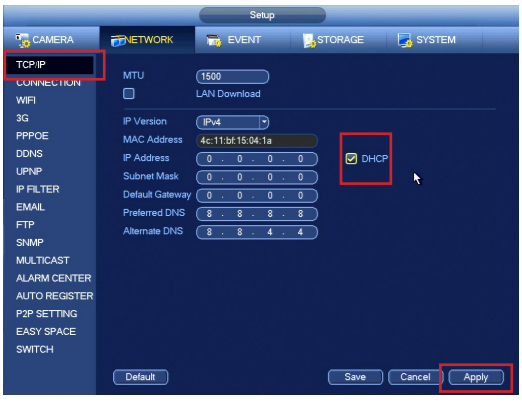
1. Connect NVR/DVR to network via Ethernet cable

2. Enter the Main Menu (Right Click > Main Menu)



3. Go to Network > TCP/IP

4.Enable DHCP and click **Apply**



5. Enter Menu > Network > P2P

6. Enable P2P option and click **Apply**

7. The Status box should now report Connect Success or Online (varies by model)

It will now be possible to connect to the system via both the mobile application and Smart PSS PC software. Select P2P as the connection method when adding the device to the software.

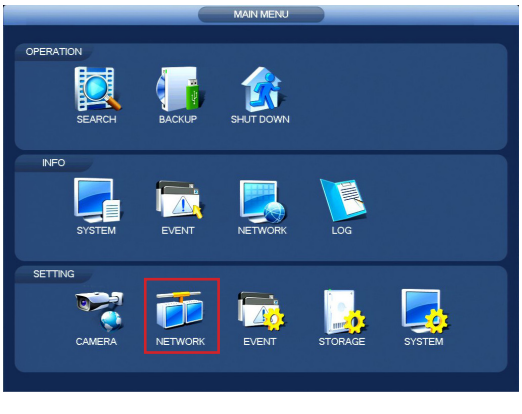
Change Default HTTP and TCP port

When configuring your device for remote access it is always recommended to change the default port numbers. For example, to access a Dahua device from a remote location using the web browser, the HTTP port (80) and TCP (37777) should be forwarded within the on site router.

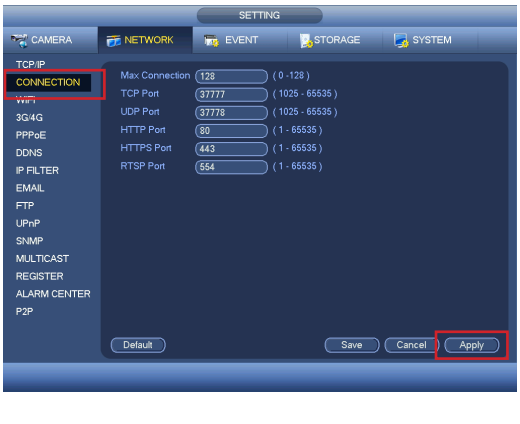
These ports can be set to anything of your choice, however it is recommended to use a number that is not commonly used by another type of application such as FTP (21), RTSP (554) etc. It is recommended to use port numbers of at least 4 digits.

To change the port numbers on your recorder, follow the steps below.

1. Enter the Main Menu (Right Click > Main Menu)



2. Go to Network > Connection



3. Select the port number you wish to change and input the new port number using the onscreen keyboard.

   Click Apply followed by Save to confirm the setting.

   If your recorder prompts to reboot to save the settings, click Yes to confirm.

Forward only the ports you need

When configuring your device for remote access there are multiple ports used by the recorder for remote access. Which ports to forward in your router depends on which services you will be using for remote access.

For remote access via applications such as DMSS or Smart PSS only the TCP port (37777) is required.

When accessing the recorder remotely using a web browser, both the HTTP port (80) and TCP port (37777) are required.

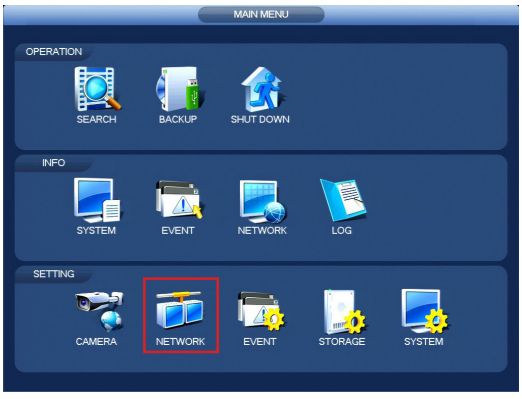
Recommendations to improve your network security

Enable IP Filter

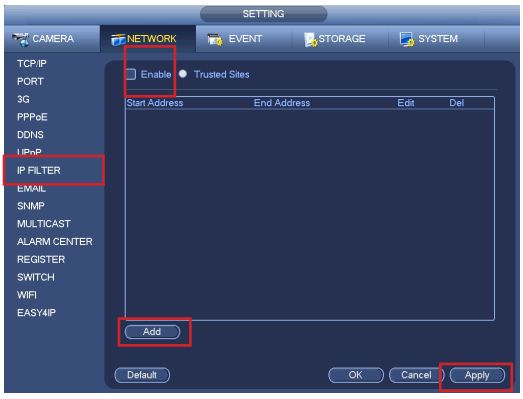
When a recorder has been configured for remote access, it is possible to secure the device further by utilising the IP Filter feature. Using this feature, remote access can be limited to specific remote IP addresses, IP address ranges or individual device MAC addresses.

To configure the IP filter, follow the steps below.

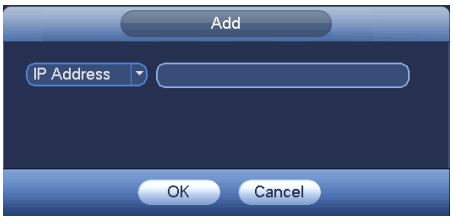
1. Enter the Main Menu (Right Click > Main Menu)



2. Go to Network > IP Filter



3. Check the enable box and click the Add button



4. There are three types of IP filter that can be selected

IP Address Enter a single IP address to grant remote access to, this is useful if the remote sites that will access the recorder have a static IP address

IP Segment Enter a range of IP addresses to grant remote access to, for example: 192.168.1.100 - 192.168.1.110

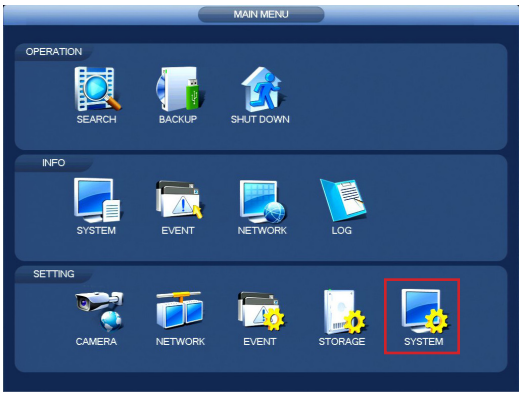
MAC Address Enter a remote devices MAC address to grant remote access to, for example a mobile phone or specific remote computer

Once all entries are added, click Apply followed by Save

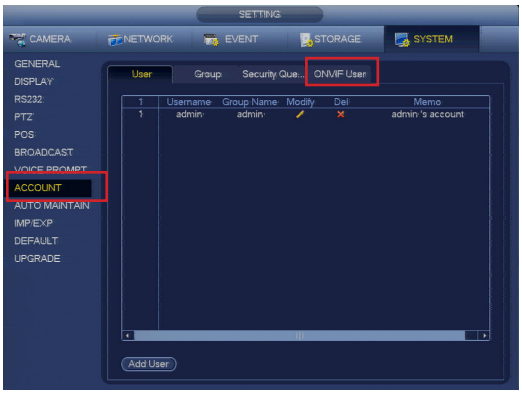
Change ONVIF Password

The ONVIF password is used when streaming camera channels from the recorder to another device using the ONVIF protocol. By default the ONVIF password is set to admin. For security reasons it is recommended to change the password to a strong password using at least 8 characters and is made up of a combination of special characters, numbers and upper & lower case letters.

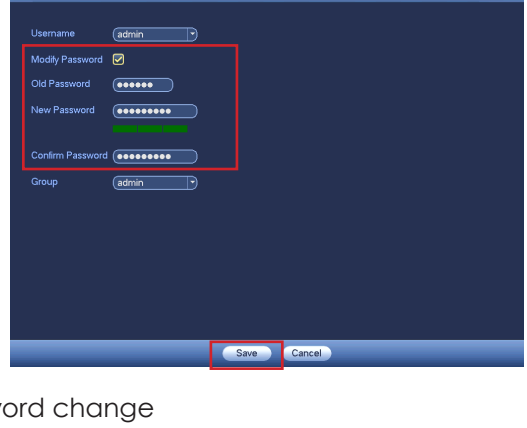
1. Enter the Main Menu (Right Click > Main Menu)



2. Select System settings (Bottom Right) and click Account from the left sub menu list followed by the ONVIF User tab



3. Check the Modify Password box and input the current password (admin by default). Enter your new password into the new password & confirm password text boxes. It is recommended to choose a strong password with a minimum of 8 characters combining lower case, upper case, numbers & special characters.



4. Click Save to confirm the password change

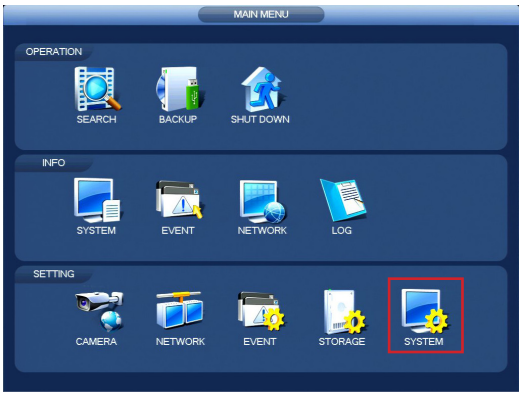
Recommendations to improve your network security

Limit Features of Guest Accounts

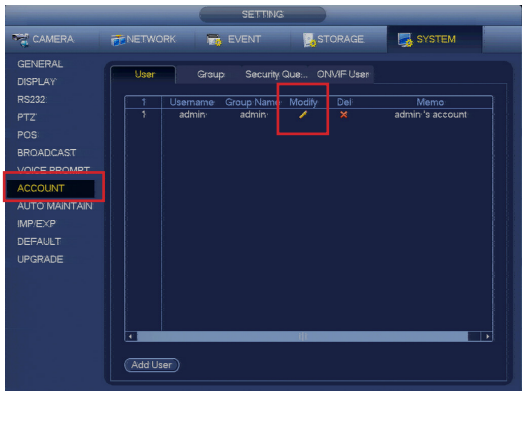
When adding additional users to the system for local or remote access, it is recommended to restrict access to certain functions not required by the user.

To edit the permissions of a specific user or guest account follow the steps below.

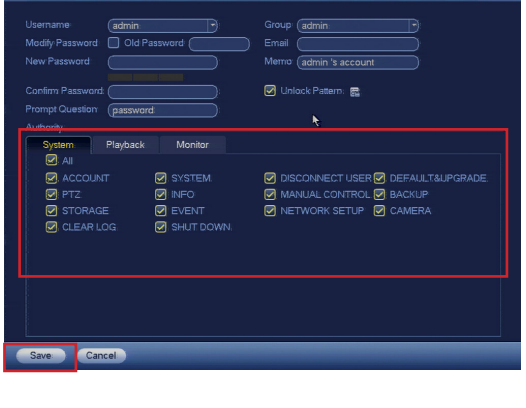
1. Enter the Main Menu (Right Click > Main Menu)



2. Select System settings (Bottom Right) and click Account from the left sub menu list. On the account you want to change the password for, click the Modify Icon



3. In the System tab uncheck any function that the user does not require, such as System, Account or Network settings. Select the Playback & Monitor tabs and uncheck any camera channels the user should not be able to view, this will hide the images on these channels from the user.

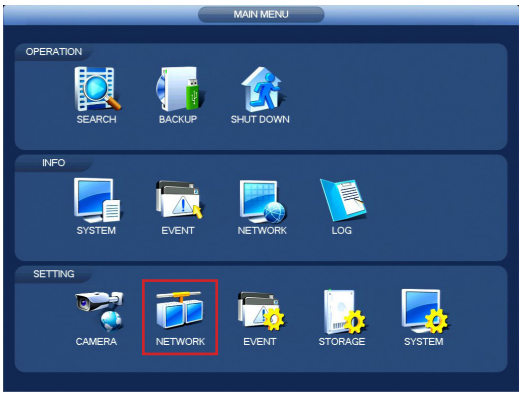


4. Click Save to confirm the new user settings

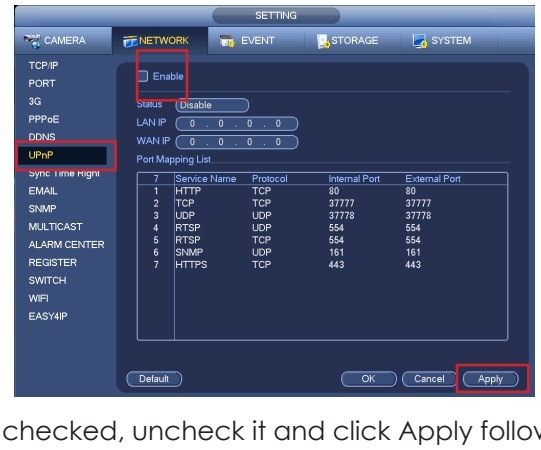
Disable UPnP

UPnP (Universal Plug and Play) is used to automatically forward the recorder ports in a compatible router. Although this feature can be useful by removing the need to configure the router manually, if the feature is not required it is recommended to disable UPnP.

1. Enter the Main Menu (Right Click > Main Menu)



2. Go to Network > UPnP



3. If the UPnP Enable checkbox is checked, uncheck it and click Apply followed by OK

Physically Lock Down the Device

It is important to remember that when choosing the installation position of a recorder, it is best practice to not only hide the recorder but to protect it in the event that it is found.

One way this can be achieved is by installing the recorder in a lockable enclosure. Cop Security have multiple lockable enclosures available to purchase.

Connect IP Cameras to the POE Ports on the Back of the NVR

When installing IP cameras on an NVR with built in POE, it is advisable to only connect the cameras to the POE ports of the NVR. When cameras are connected to the LAN computer network and streamed to the NVR, it is possible for any computer on that network to find the cameras and attempt to gain access. There is also the possibility of unauthorised access from across the internet as the cameras reside on the main computer network. When the cameras are connected to the directly to the PoE ports of the NVR, they are physically isolated from the computer network, reducing the chance of unauthorised remote access.

This is also true for recorders that do not feature built in PoE but instead have two or more network ports. These NVRs are designed with two Ethernet ports so that one port can be used for remote access via the computer network and the other port used for the camera network, isolating the two.

Isolate Recorder Network

When installing a recorder on a site for remote access, it is advisable to consider using a second broadband line for the recorder rather than installing the recorder on the computer network. This helps protect the recorder from unauthorised remote access.

COP SECURITY™

Professional CCTV

COP Security, Delph New Road, Dobcross, OL3 5BG England