

INTRODUCTION

Data Protection legislation has been in force in the EU since the late 1990s to protect how data held on individuals is stored and shared by organisations and computer systems.

The General Data Protection Regulation (GDPR) Directive comes into force 25th May 2018 - superseding Data Protection. It further protects and empowers EU citizens' data privacy and aims to reshape the way organisations consider data privacy.

For the CCTV Industry; responsibility for adherence to GDPR legislation rests with the entire vendor supply chain, the CCTV Integrator and all the way through to the end-user organisation collecting, storing and administering user data.

It is outside the scope of this document to cover the legalities of GDPR; it serves only as a Technical Guide to the CCTV Integrator in the considerations and best practices of "hardening" and securing a CCTV system - Cyber Security-wise - to help them safeguard user data towards complying with GDPR. Consider the following scenario;

An end-user organisation uses an IP-CCTV system and has in place correct and adequate procedures limiting only authorised staff to access live, archive and export data from their CCTV system in accordance with GDPR. However, direct remote Internet access to the IP cameras of the system had been left "open" to allow anyone potentially outside of the organisation to access live images – considered personal data!

The IP cameras also went on to be vulnerable to Cyber-attack and used to further exploit the end-user's internal network – as both the CCTV network and customer's Corporate network were shared!

"Hardening" a CCTV system aims to limit and control access to such data and continually review the risks. However, with increased security comes reduced "accessibility" – the Integrator therefore needs to find a balance. It also involves not only software but cameras, servers, NVRs/DVRs, networks and storage devices etc – both individually and how they are deployed into a network. Cyber Security therefore has to be a consideration from the initial planning stage of any CCTV or IP network system!

Cyber Security is an extensive subject, resulting in a Consulting industry dedicated to it, and covering the subject in great detail is outside the scope of this document; which is intended to only assist the CCTV Installer in hardening current Vista products and raise awareness of the more immediate Cyber considerations. References to other Cyber Security reading resources are provided in Appendix -1 and you are strongly recommended to make use of such resources.

Contents

| | |
|---|----------|
| INTRODUCTION | 1 |
| OVERVIEW OF BEST PRACTICES AND HARDENING | 5 |
| VISTA PRODUCT HARDENING | 6 |
| <i>IP CAMERAS</i> | 6 |
| UPGRADE TO LATEST FIRMWARE | 6 |
| SET CAMERA PASSWORD AND PERMISSIONS | 8 |
| IP CAMERA NETWORK SETTINGS AND TOPOLOGY | 9 |
| SET TIME SYNCHRONISATION | 9 |
| IP CAMERA AUDIO | 10 |
| HTTPS | 10 |
| IP FILTERING | 11 |
| OPENVPN | 13 |
| DISCOVERY SERVICES – DISABLING | 14 |
| IP MULTICAST - DISABLING | 14 |
| NAT PORT TRAVERSAL - DISABLING | 15 |
| <i>VIPER NVR\DVR HARDENING</i> | 16 |
| DEFAULT CONFIG AND REFORMAT HDD | 16 |
| UPGRADE TO LATEST FIRMWARE | 16 |
| LOGIN ACCOUNTS, PASSWORDS & PERMISSIONS | 18 |
| SET TIME SYNCHRONISATION | 19 |
| NETWORK SETTINGS & TOPOLOGY | 19 |
| ADDING IP CAMERAS WITH STRONG PASSWORDS | 20 |
| NOTIFICATION AND ALERTS | 20 |
| PERIODIC NOTIFICATION – VIA EMAIL | 23 |
| <i>QULU</i> | 24 |
| INSTALLING & DEFAULTING | 24 |
| DEFAULT CONFIG AND REFORMAT HDDs | 24 |
| UPGRADE TO LATEST VERSION | 25 |
| LOGIN ACCOUNTS, PASSWORDS & PERMISSIONS | 28 |
| TIME AND DATE SYNCHRONISATION | 29 |
| NETWORK SETTINGS & TOPOLOGY | 30 |
| ADDING IP CAMERAS WITH STRONG PASSWORDS | 31 |
| NOTIFICATION AND ALERTS | 32 |
| NOTIFICATION & ALERTS VIA EMAIL | 33 |
| AUDITING QULU SYSTEM | 35 |

| | |
|--|-----------|
| WINDOWS OPERATING SYSTEM | 36 |
| NETWORK SETTINGS & TOPOLOGY | 36 |
| LOGIN ACCOUNTS, PASSWORDS & PERMISSIONS | 36 |
| UPGRADE TO LATEST SOFTWARE – MS UPDATES | 37 |
| WINDOWS FIREWALL AND ANTI-VIRUS | 37 |
| REMOTE ACCESS SUPPORT APPLICATIONS | 38 |
| WINDOWS ERROR LOGS | 38 |
| NETWORK TOPOLOGY HARDNING | 39 |
| BASICS & ESSENTIALS | 39 |
| EXAMPLE NETWORK TOPOLOY AND FIREWALL | 40 |
| APPENDIX 1 - OTHER READING RESOURCES | 41 |
| APPENDIX 2 - VISTA AND OTHER COMMONLY USED IP PORTS | 42 |

OVERVIEW OF BEST PRACTICES AND HARDENING

Following is an overview of best practices according to system component type.

Not all may be possible, available or practical on all CCTV system scenarios and may be dependent on the size of the installation, chosen equipment and existing infrastructure. The list is also not exhaustive; in that some products and scenarios may provide additional security measures and features which you would be advised to consider using.

Later chapters in the document will expand on some of the below points.

GENERAL

- Always consider security threats from within the same network (customer's) just as likely as the Internet!
- Do not use default login IDs and passwords. Always change them!
- Passwords changed regularly and when staff leave service.
- Use "strong" passwords! Mix of alpha, numerics, special characters (\$#!...), upper/lower-case, between 8-14 characters. Where the term "Strong password" is used in this document it will imply this standard.
- Where possible, rename default IDs called Admin to something more difficult to guess
- Give details to end-user of any Admin account to lock away - not for general use.
- Provide separate "user" accounts/passwords for staff - giving absolute minimum access required to each.

IP-CAMERAS\NVR\DVR\PCs\SERVERS\CCTV-VMS

- Check vendor's web sites regularly for firmware updates and announcements of risks/vulnerabilities.
- Ensure anti-virus software installed and latest virus definitions up to date.
- Software Firewall enabled and maintained as per Antivirus. Open only necessary ports!
- VMS software: use a dedicated server! Don't install onto shared servers such as e-mail or Web server etc.
- If a feature is not required disable or don't install – such as IP camera audio support, UpnP, Bonjour etc .
- DVR\NVR\VMS physical access restricted to only authorised end-users – locked in comms room.
- Time synchronisation set between all IP devices (cameras, NVRs etc) for dependable event log analysis
- Disable PING reply (ICMP-Request) on IP devices/firewalls to hide their presence from PING sweeping.
- IP cameras: set IP source address filters, limit IP access from only NVR\VMS and CCTV Installer's Laptop.

NETWORKS

- Always provide separate dedicated IP-CCTV network. Do not share the end-users corporate network!
- Consider a firewall between IP-CCTV network and corporate network to control access to CCTV system.
- Manage Firewall policies to restrict CCTV Client PCs to access NVR\VMS only – not direct to IP cameras.
- On intelligent managed Ethernet switches, use security features such as authorised MAC address lists.
- Use SNMP V3 or Syslog capabilities to centrally report events such as login breaches/failures etc.
- Mobile devices over public WiFi; consider providing VPN connectivity between device and CCTV site.
- WiFi access points: turn off SSID advertising and placed in separate IP subnet\LAN behind firewall

VISTA PRODUCT HARDENING

The following chapters show examples for hardening various Vista products.

Hardening - or making devices more cyber secure – largely removes or restricts access to only those authorised users or source networks that are absolutely essential. The most secure device is one that is not connected to a network at all and locked away, but then becomes unusable by anyone! A balance needs to be found.

Some security features, when applied, could “break” your specific application or system. One case in point is applying HTTPS to IP cameras. While setting this adds protection when accessing a camera direct via web browser it may prevent the NVR/VMS from then recording the camera stream if it does not support HTTPS!

We indicate where caution may be required.

IP CAMERAS

The following chapters show examples for hardening Vista VK2 IP cameras.

- Upgrade to latest firmware
- Set strong passwords
- Network topology – in a dedicated IP-CCTV network!
- Time synchronising
- Disable features not required
- Apply Source IP-address filtering – limit what can connect direct to a camera

UPGRADE TO LATEST FIRMWARE

All cameras must be kept on the latest firmware. Confirm the camera model numbers and compare their current firmware version against the Vista Support Web Site's latest Release – upgrade if not on the latest!

The SmartManager VK2 IP camera utility can reduce time in updating camera firmware – download and install;

- Goto website url <http://vista-cctv.com/> and click the links **Support > Downloads > Vista IP** (fig1)
- Select the folders **VK2_IP Range** (fig 2) then the folders **VK2_Software > Smart Manager**

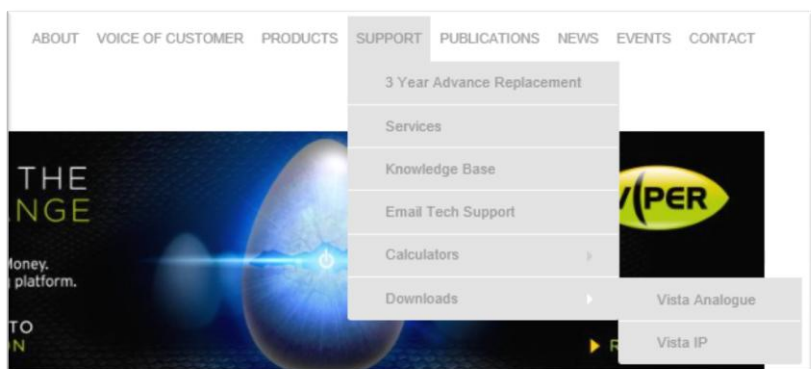


Fig1

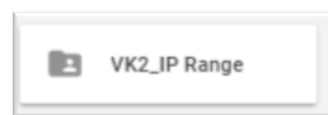


Fig 2

- Finally click the link to download **Setup Smart Manager** and install to your PC/laptop.
- Once run – all VK2 cameras on the same network as the laptop will be displayed (fig 3).
- Return to the Vista website; click the **Support > Downloads > Vista_IP** links again. Then click the folders **VK2_IP Range > VK2_IP Cameras**.
- Click the folder for each camera model number on your site and download and UNZIP if the version number shown in the file name (fig 4) is later than the version of your camera (fig 3.)

| Model Name | Name | MAC Address | IP Address | Wireless IP Address | Zero Conf. IP | Version |
|----------------------|-------------------------------|-------------------|-------------|---------------------|-----------------|------------------|
| VK2-REC16HD | 16CH Recording Server | 00:25:90:66:57:74 | 10.0.1.51 | 0.0.0.0 | 169.254.126.207 | 1.9.5-N1-release |
| VK2-HD20-SM | H.264 Network PTZ Camera | 00:07:D8:19:B7:5F | 10.0.1.86 | 0.0.0.0 | 169.254.128.87 | 2.1.7-X2_release |
| VK2-5MPVVRDIR36V1... | H.264 5M Motorized IR Do... | 00:07:D8:19:5F:BB | 10.0.1.72 | 0.0.0.0 | 169.254.185.184 | 1.5.8-XE_release |
| VK2-5MPVFD36V10re | H.264 5M Motorized Dome ... | 00:07:D8:19:5D:20 | 10.0.1.66 | 0.0.0.0 | 169.254.55.249 | 1.5.8-XE_release |
| VK2-5MPBIR36V10re | H.264 5M Motorized IR Bull... | 00:07:D8:19:5D:34 | 10.0.1.67 | 0.0.0.0 | 169.254.228.137 | 1.8.2-XE_release |
| VK2-5MP360INT | H.264 5M Fisheye Camera | 00:07:D8:19:07:0E | 10.0.1.83 | 0.0.0.0 | 169.254.145.206 | 1.5.8-XE_release |
| VK2-5MP360INT | H.264 5M Fisheye Camera | 00:07:D8:19:06:FE | 10.0.1.56 | 0.0.0.0 | 169.254.145.206 | 1.5.8-XE_release |
| VK2-3MPVFDIR37e | H.264 3M Network IR Dome... | 00:07:D8:19:50:82 | 10.0.10.109 | 0.0.0.0 | 169.254.245.125 | 1.8.2-XE_release |
| VK2-3MPMD26e | H.264 3M Network Dome C... | 00:07:D8:1A:4A:9E | 10.0.1.87 | 0.0.0.0 | 169.254.30.127 | 1.8.2-XE_release |

Fig 3

IMPORTANT: Prior to updating any camera, read the ReleaseNotes file within the firmware.zip file! You may not be able to update your camera directly to the latest version, but may first have to update to an intermediate version!

- For each camera that needs updating; right-click each camera in turn and select **Upgrade Firmware**. (fig 5) Browse to the relevant Unzipped file you downloaded.
- The file will now upload to the camera, which then reboots to the new version – allow 6-7 minutes.

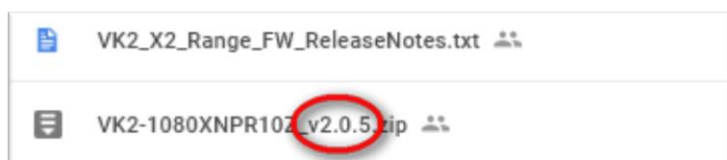


Fig 4

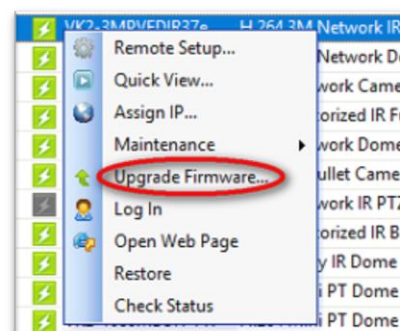


Fig 5

If the camera is being newly installed, default it as a precaution before continuing to set-up and harden the camera - simply right-click the camera in Smart Manager then select **Maintenance > Factory Default**

SET CAMERA PASSWORD AND PERMISSIONS

Change the Admin ID password to something “strong” and remove anonymous viewing of the video stream.

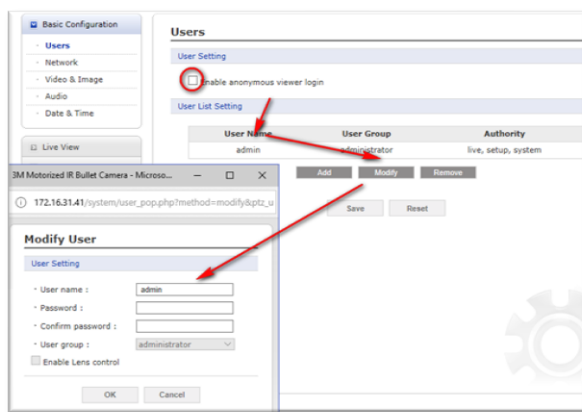
CAUTION: You will need to amend your NVR/VMS settings for each camera – setting the new camera password - otherwise new recordings will be lost!

You can set VK2 cameras passwords via two methods;

1. Individually via web browsing onto each camera and making changes
2. Use Vista's SmartManager to select and modify multiple cameras at a time

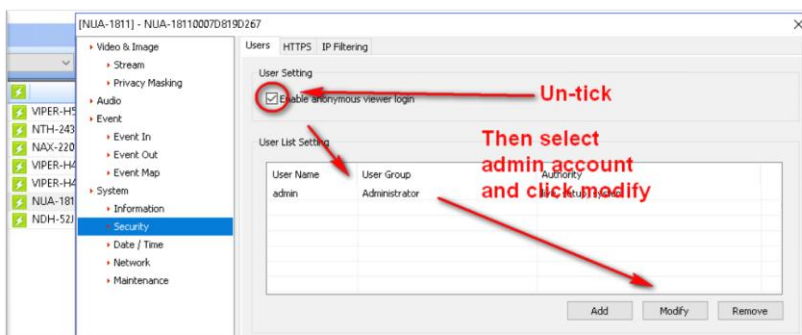
WEB BROWSER

- Web browse to the cameras IP address and select Open Web Page.
- Under the menu **Basic Configuration**, click **Users**, then highlight the Admin ID and click [Modify] (below)



SMART MANAGER

- Alternatively, open Smart Manager; shift + click to select all the cameras you wish to modify.
- Right-click then select **Remotely Manage**.
- Refer to the example below and modify accordingly, then select save.



Use caution when changing the Admin password for all cameras at the same time. Be certain to keep a note of the new password, or first create an additional login ID with Admin equivalence.

To prevent network eavesdropping when setting the admin password, do so while using a secure encrypted HTTPS connection to the camera instead. VK2 camera default settings should support both HTTP and HTTPS simultaneously. Simply web browse to the camera using [HTTPS://x.x.x.x](https://x.x.x.x) instead, then set the new password.

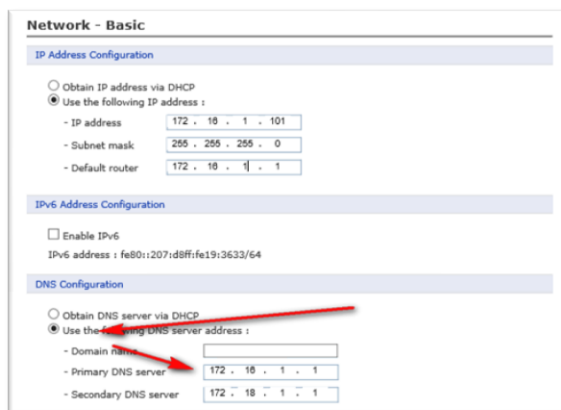
If this fails; refer to the chapter on **Enabling HTTPS on a camera** later in this section.

IP CAMERA NETWORK SETTINGS AND TOPOLOGY

Where you place IP cameras on a network, and how you assign IP addresses to them, will be largely determined by the NVR/VMS you are using. However, always ensure;

- All IP-cameras placed in a dedicated Ethernet CCTV network, not shared on customer's existing network!
- Connectivity "direct" to cameras only allowed from NVR/VMS & installer's laptop – not customer network!
- Where possible, use either static IP addresses or DHCP-via MAC Reservation.

If the use of a DNS server for the camera really is necessary, ensure the DNS server is also set via a static setting on the camera and not via DHCP – set it as per the example below – using an Internal DNS where possible as opposed to an Internet located one (8.8.8.8 etc). On-site IT Support should be able to advise or provide one.



Network - Basic

IP Address Configuration

☐ Obtain IP address via DHCP

☒ Use the following IP address :

- IP address: 172 . 16 . 1 . 101

- Subnet mask: 255 . 255 . 255 . 0

- Default router: 172 . 16 . 1 . 1

IPv6 Address Configuration

☐ Enable IPv6

IPv6 address : fe80::207:d8ff:fe19:3633/64

DNS Configuration

☐ Obtain DNS server via DHCP

☒ Use the following DNS server address :

- Domain name:

- Primary DNS server: 172 . 16 . 1 . 1

- Secondary DNS server: 172 . 16 . 1 . 1

Fig 8.

SET TIME SYNCHRONISATION

Set time synchronisation on the camera via NTP!

Point the camera, where possible, to an NTP time source or device on the local network. The NVR/VMS must also point to the same NTP source so that time is synchronised across the IP-CCTV system. On smaller networks with Internet access, the ISP router may be able to offer an NTP service – which in-turn is synchronised to Internet time within the ISP's network.

NOTE: When used in connection with Vista Viper – the NVRs should point to an NTP time source for their time sync. In turn, the IP cameras must point to the Viper NVR to synchronise their time via NTP.

- Login to camera, click **Date & Time** under **Basic Configuration** - set as below – substituting the IP address
- Click **Save**

• Time mode

☐ Synchronize with computer time
Date : 27-03-2018 Time : 17:28:15

☒ Synchronize with NTP server
NTP server : x.x.x.x NTP Interval : 12 [hour]

☐ Set manually
Date : 28-03-2018 Time : 01:25:18

IP CAMERA AUDIO

If audio recording is supported by the camera, but not specifically needed for your installation, then disable it so that it cannot be exploited by someone gaining direct access to the camera.

- Web browse or login to the camera.
- Select menu Audio > Basic and untick Enable Audio (below)

Basic Configuration

Live View

Video & Image

Audio

Basic

Event

Audio - Basic

Audio Setting

☐ Enable audio

- Compression type G.711 u-law

- Sample rate 8KHz

- Sound bitrate 64kbps

HTTPS

As default, browser access to the camera is via plain text http://. Change/force this to encrypted by setting the camera to use https:// only.

CAUTION: Vista's NVR (VIPER) and VMS (Qulu) are currently unable to support cameras using HTTPS (a forthcoming feature)! Many other manufacturers NVRs are also unable to support HTTPS at present. You are advised to test a single camera against your chosen NVR before making this setting across all cameras!

- Web browse onto camera; select menu **System > Security > HTTPS** set **Connection Mode** to **HTTPS** (below).
- From now on, connect to the camera by using the url [HTTPS://x.x.x.x](https://x.x.x.x) instead.

Security - HTTPS

HTTPS Connection Policy

Connection Mode HTTPS

Private Certificate

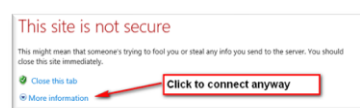
Browse... and click Upload

*** Note**
When private certificate does not exist, default certificate is used.

Your browser will prompt when connecting in future due to only a default Security Certificate being present on the camera (below). If you have your own Certificate – as issued by your chosen CA (Certificate Authority) – you can upload this from your PC to the camera.

CAUTION: VK2 cameras support .PEM certificates only!. Please convert your SSL to .PEM before uploading. Do not upload an SSL .cert or .key file!

- Web browse onto camera.
- Select menu options **System > Security > HTTPS** and click browse to select and upload the .PEMCertificate from where you have stored it on your PC.



IP FILTERING

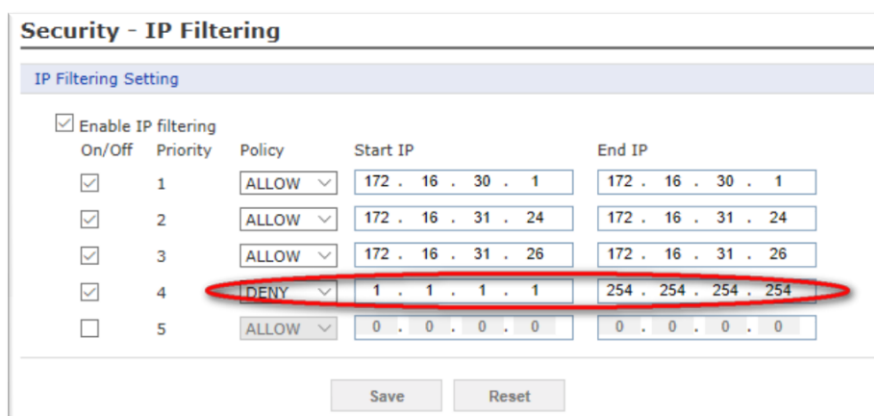
Apply IP filters on the camera to only permit incoming IP connections from valid source IP addresses, such as the NVR or VMS that records the camera's IP streams. Don't forget to also allow your PC, or limited range of IP's, for continued access by the Installer or on-site Technical Support to access the camera in future!

- Web browse to each camera in turn and add a filter;
- Click menu options **System > Security > IP filtering** – refer to example below to arrive at your required settings.

Each Filter has a priority (1 = high, 5 = low) and the first filter that “matches” the incoming IP request will be obeyed; either **ALLOW**ing or **DENY**ing the connection request! Therefore, ensure you add all the **ALLOWED** IP addresses as the highest priority first! Then add the final filter (in red) to **DENY** all other source IP addresses.

The example “DENY” statement will prevent the full remaining IP ver. 4 range of addresses - Internet included.

NOTE; be sure to exclude the customer's corporate network IP addresses from having access!



| Security - IP Filtering | | | | | |
|---|--------|----------|--------|--------------------|-----------------------|
| IP Filtering Setting | | | | | |
| <input checked="" type="checkbox"/> Enable IP filtering | On/Off | Priority | Policy | Start IP | End IP |
| <input checked="" type="checkbox"/> | 1 | 1 | ALLOW | 172 . 16 . 30 . 1 | 172 . 16 . 30 . 1 |
| <input checked="" type="checkbox"/> | 2 | 2 | ALLOW | 172 . 16 . 31 . 24 | 172 . 16 . 31 . 24 |
| <input checked="" type="checkbox"/> | 3 | 3 | ALLOW | 172 . 16 . 31 . 26 | 172 . 16 . 31 . 26 |
| <input checked="" type="checkbox"/> | 4 | 4 | DENY | 1 . 1 . 1 . 1 | 254 . 254 . 254 . 254 |
| <input type="checkbox"/> | 5 | 5 | ALLOW | 0 . 0 . 0 . 0 | 0 . 0 . 0 . 0 |

IMPORTANT: The more you restrict access via IP filters the more secure your device becomes. However, don't go too far as to restrict your own PC/laptop from having access to configure cameras in future!

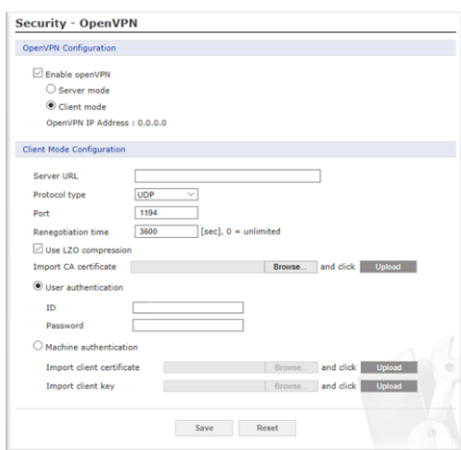
The above example would also ensure IP cameras are prevented from accessing each other. Therefore, if one becomes compromised there is less potential for it to exploit the other cameras.

NOTE: If using IP filtering, then disable IPv6 support within the camera – previous (fig 8.)

OPENVPN

OpenVPN is a Virtual Private Network using OpenSSL authentication. The camera can be set to act either as a VPN Server or Client in order that the camera can be accessed, or streamed, over insecure networks such as the Internet.

Detailed OpenVPN setup is outside the scope of this document. The follow instructions are simply those relevant to set either a Client or Server mode operation setting on the VK2 camera;



- **OpenVPN Server Mode**

- Select **Enable openVPN**, then **Server mode**, then Server Mode Configuration settings will appear.
- Set Protocol type, Port number, LZO compression and Renegotiation Time. Also export the Server certificate to file – for importing at the client-end of the VPN.
 - Protocol; UDP is preferred. Port number; default is 1194.
 - Default Renegotiation time is 3600 seconds, 0 means no verification.
 - “Use LZO compression” determines whether to use cypher compression or not.
- Click Save button

- **OpenVPN Client Mode**

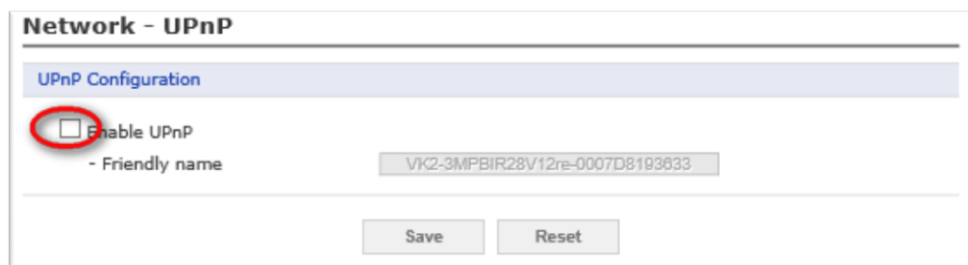
- Select **Enable openVPN** , then Client mode; Client Mode Configuration settings will appear.
- Set Server URL, Protocol type, Port number, LZO usage, and Renegotiation time.
 - Server URL is name or IP address of OpenVPN server to which the camera’s Client VPN will connect with
 - Protocol type, Port number, and LZO settings must ALL match the Servers settings.
- Upload your CA certificate as issued by the OpenVPN Server.
- Select authentication method between User authentication and Machine authentication.
 - For Machine authentication, upload the Certificate and client key that was exported at the Server.
 - For User authentication; type required ID and Password that has been set for the camera VPN.
- Click Save button.

DISCOVERY SERVICES – DISABLING

Disable non-essential services which advertise the cameras presence on a network. The first line of defence is not letting attackers know of your presence – therefore minimise it.

Disable;

- Bonjour
 - UPnP
 - Zeroconf
- Web browse into the camera and login as Admin
 - Click menu options **System > Network > UPnP** and disable (below)
 - Click **[Save]** !
 - Repeat for menu options **Bonjour | Zeroconf**

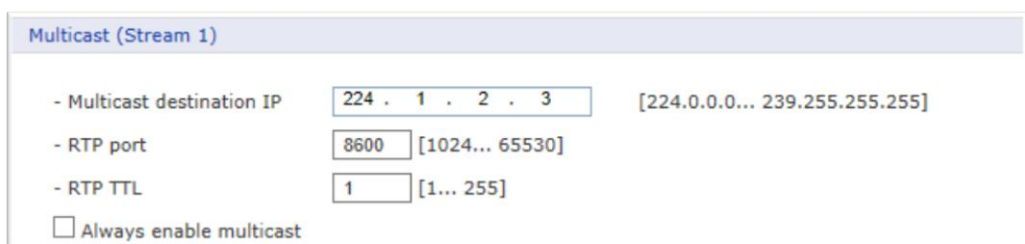


IP MULTICAST - DISABLING

If your camera or application does not specifically require IP Multicast, then disabled it on the camera. IP Multicast introduces its own security concerns – is only concerned with streaming data to the Multicast group – having no interest or knowledge in individual receiving nodes and the locations that such data is being sent!

NOTE: Multicast security concerns can be part-addressed by limiting the TTL of sent packets. They can only then pass over a limited number of hops (routers) so as to remain valid only within a rough Local or Wide network before being dropped, i.e. TTL = 1-5

- Login to the camera via browser
- Select menu System > Network > RTP and ensure multicast is disabled – for the camera globally or via each stream (below)



NAT PORT TRAVERSAL - DISABLING

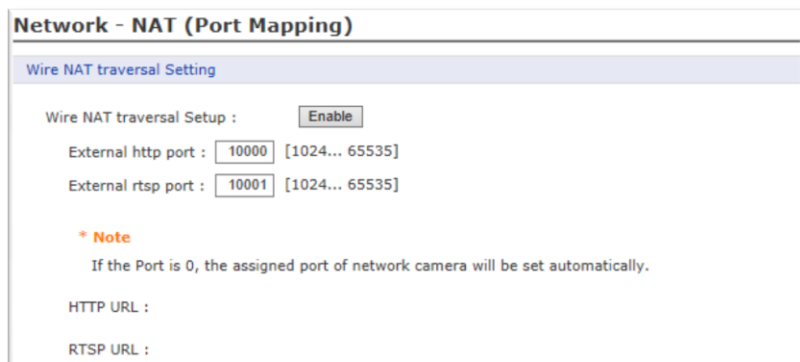
When enabled, the camera will attempt to automatically negotiate with your Internet router (via UPnP) for port forwarding to be opened to allow Internet access direct to the camera!

For normal IP-CCTV applications you are advised to disable NAT and to not allow direct internet access to cameras! Only do so if your individual application really demands this and ensure all other hardening practices are applied.

You are advised to consider a separate and dedicated DMZ/Ethernet/subnet (via a firewall) for such a device so that if it becomes compromised there is minimal risk to other internal devices and networks!

NAT Traversal is reliant on using the UPnP discovery service to find the Internet router and automatically set-up a port forward. Earlier in the procedure you were advised to also disable UPnP. For best security, disable both.

- Web browse to the camera and login as Admin
- Click menu options **System > Network > NAT** and click the [Disable] button.



VIPER NVR\DVR HARDENING

The following must be adopted or considered for deployment and security of any VMS\NVR\DVR. We use Vista's current VIPER range as an example.

- **Physical location** - secured so only accessible to authorised staff. Consider Vista QBOX part: **0473150** (right)
- **Network logical location** – on a dedicated CCTV VLAN \ IP Subnet, not shared customers network! Provide a firewall to permit remote PC access from only those PCs that are authorised.
- **Login & Password Access** – Only use “strong” passwords! Lock away and don't use the Admin account for general access! Create separate IDs for staff with minimal rights to carry out their roles.



DEFAULT CONFIG AND REFORMAT HDD

As a precaution - on any NVR\DVR being installed to a site for the first time – both default the system config as well as reformat the HDDs to protect any previous customer's data!

- Login to the NVR\DVR as Admin equivalent
- Select menus System > Config > Factory Default
- Click [Select All], then click [Default] (fig 19.)
- Next, select menu options Device > Disk
- Now click to select each HDD and click [Format] (fig 20.)



Fig 19 (Default all)

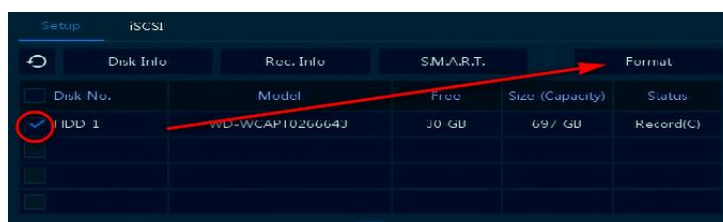


Fig 20 (format HDD)

UPGRADE TO LATEST FIRMWARE

Always maintain DVRs and NVRs on the latest version of firmware. Compare the version of your units with the latest; as held on the **Downloads** page of the Vista web site at www.vista-cctv.com

Simply follow the below and upgrade if necessary;

- Login direct on the DVR\NVR using Admin, or equivalent, account.
- Select menu options **System > System > F/W Upgrade** ; confirm the current version (fig 21.)

- Compare to the latest version held on the Vista Website (procedure below) and download if need be.
- Unzip the file and save a copy to the root of a USB drive, insert USB drive into NVR/DVR
- Click the Refresh button then click Upgrade.
- Confirm the new version has “taken”.

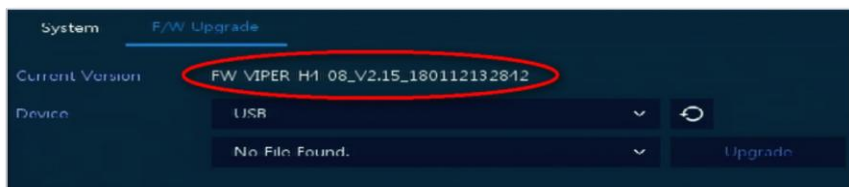


Fig 21. Firmware version currently on NVR

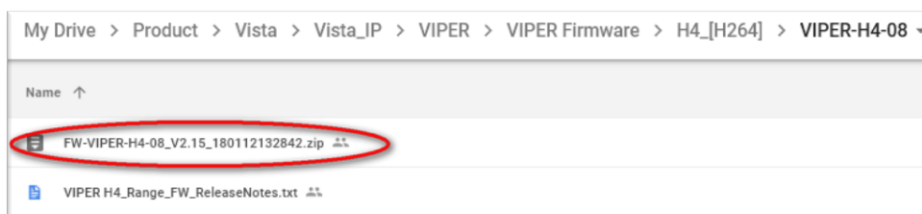


Fig 22. Shows NVR is on same version as web site

NOTE: Take special notice and care of the firmware's filename to help identify the correct firmware for your relevant chassis/device! Above example shows correct Viper H4 (H264) 08-channel NVR

- Visit www.vista-cctv.com, navigate to menus **Support | Downloads** and select either **Vista Analogue** (DVRs) or **Vista IP** (NVRs)
- Refer to the below tables to determine the download folder required

| Vista Analogue | | |
|--|-----|---|
| DVR Model-Chans | | Download Folder |
| <ul style="list-style-type: none"> HDA-08 HDA-16 | >>> | Folder Viper > Firmware > HDA |
| <ul style="list-style-type: none"> HDAL-08 HDAL-16 | >>> | Folder Viper > Firmware > HDAL |

| Vista IP | | |
|---|-----|--|
| NVR Model-chans | | Download Folder |
| <ul style="list-style-type: none"> H4-04 H4-08 H4-16 | >>> | Folder Viper > Viper Firmware > H4_[H264] |
| <ul style="list-style-type: none"> H5-32 | >>> | Folder Viper > Viper Firmware > H5_[H265] |
| <ul style="list-style-type: none"> VMC642 | >>> | Folder Viper > Firmware > VMC |

LOGIN ACCOUNTS, PASSWORDS & PERMISSIONS

Make full use of Viper user account and login features (below) and create separate IDs, passwords and group permissions for individual staff or roles.

Give only the minimum permissions according to each person's authority and role!

| Viper ID\Feature (fig 23/24) | Use |
|--|---|
| CCTV Installer ⁽¹⁾ | Create dedicated Installer Admin account – don't leave logged in! |
| Store Manager ⁽²⁾ | Create dedicated Manager's Admin account – don't leave logged in! |
| Staff ⁽³⁾ | Create non-Admin accounts for general staff with via a "low-access" permission group (fig 25 item ⁶) and add the staff IDs as members of the group. |
| Auto logout & Password change ⁽⁴⁾ | Set passwords to automatically logout on inactivity (10 mins eg) and force periodic password changes |
| Passwords | Set strong passwords – as previously outlined |
| Archive Dual Permission ⁽⁵⁾ | Enabling option will prompt for an Admin equivalent to enter their password to permit users to playback or archive footage |
| Group permission ⁽⁶⁾ | Create groups for non-admin staff and IDs and set the permissions you wish – revoke access to view individual cameras or the Setup menu as required. |

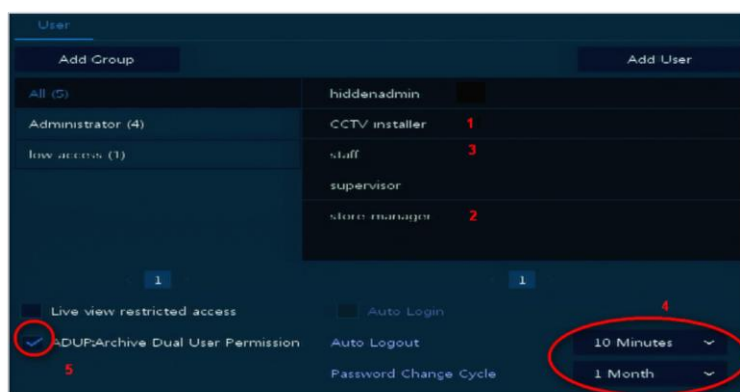


Fig 23.

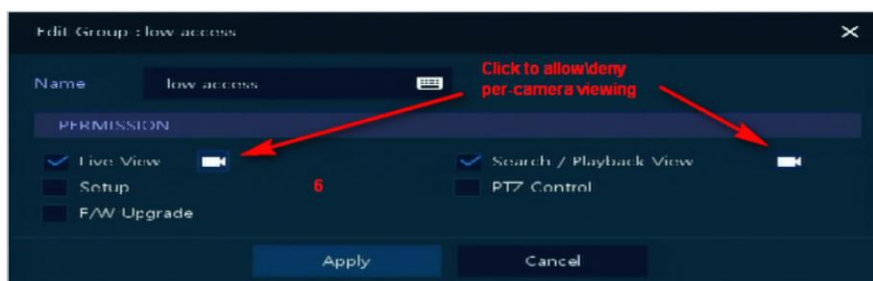


Fig 24.

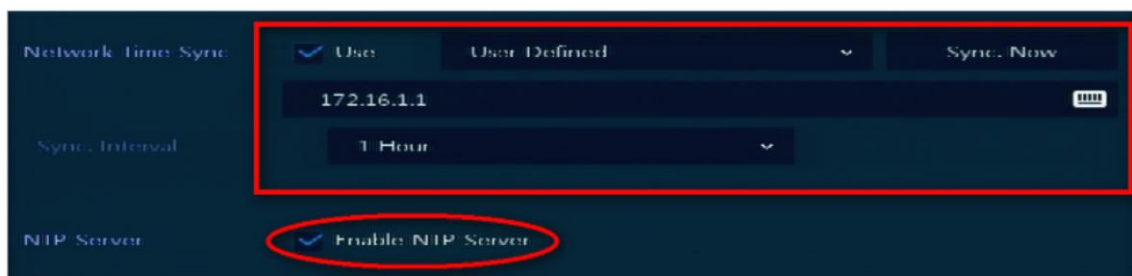
SET TIME SYNCHRONISATION

Accurate time stamping of recorded video evidence data and alarms is crucial. Set time synchronisation via NTP where possible using an NTP time source or device on the local network!

On smaller networks with Internet access, the ISP router may be able to offer an NTP relay service – which in-turn is synchronised to Internet time via the ISP's network. For larger networks consult with the on-site IT department.

Set Viper as below example;

- Select menu options **System > Time /Date > Time / Date**
- Click and enable **Network Time Sync | Use**, then User Defined from the drop-down window
- Now enter your relevant details (example below)
- Click **Enable NTP Server** so IP cameras may then use Viper to synchronise their time. Within each camera specifying the relevant Viper's WAN or PoE IP address as the cameras NTP server.



NETWORK SETTINGS & TOPOLOGY

Refer to the section on **Hardening via Network Topology** to determine the best practices on where - within a network - to deploy Viper. This will determine your IP addressing and what IP details to enter into your Viper network configuration etc.

Only apply static IP details to the Vipers configuration as the below example. Login in to Viper as Admin and;

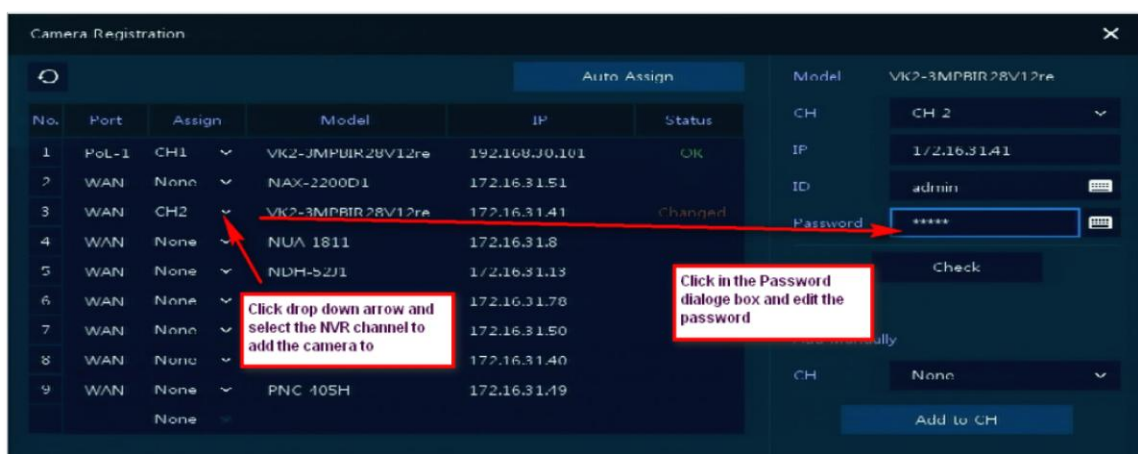
- Select menus Network > Basic > Wan Port
- Set IP address via **Static IP**
- Only set a DNS if specifically required - such as using DDNS or DVRNS features on Viper – and setting it statically and using an internal DNS server or router!
- Default WEB port is port 80. For increased security change this – consider the implications though in the rest of your system if doing so.



ADDING IP CAMERAS WITH STRONG PASSWORDS

VIPER, like many NVR\DVRs, assumes the use of default IDs and Passwords being set on IP cameras when trying to add them for recording. Follow the procedure below for amending the login details of a camera when adding to VIPER;

- Ensure IP camera configured as required and accessible on the network
- Login to VIPER locally as Admin equivalent
- Select menus **Camera > Registration**, then click **[Camera Registration]** button
- Refer to example below; for the camera you are adding, click the dropdown arrow under the Assign column and select the NVR channel to add the camera to
- Next, click in the Password dialogue box and amend the password
- Click the **[Check]** button and confirm "Connected" appears in green in the lower left.
- Now click **[Apply]**, then OK to accept changes.
- Confirm video starts to stream from the camera.



NOTIFICATION AND ALERTS

Monitoring and reporting from Viper for certain events and conditions should be considered – via e-mail or Notification Server configuration;

- Send notification of users logging in
- System restarted
- HDD disk missing

First enter details of either your Notification Server or E-mail Server;

- Login as Admin equivalent to the Viper NVR\DVR
- Click menus **Network > E-mail** and enter IP and login details for your e-mail server (fig 28.)
- Click menus **Network > Notification Server** and enter IP and login details for any Push Notification server or service that you wish to use (fig 29)
- Click the **[Test]** button on each to confirm configuration is initially working.

➤ Click menu **Event > System /Disk > System** and set notification via E-mail and/or Push for (fig 30.);

- Restart,
- User Login
- Record Transaction.



Fig 28.

NOTE: You are advised to use SMTP e-mail servers using TLS or SSL authentication so that logins and passwords are encrypted.




Fig 29.

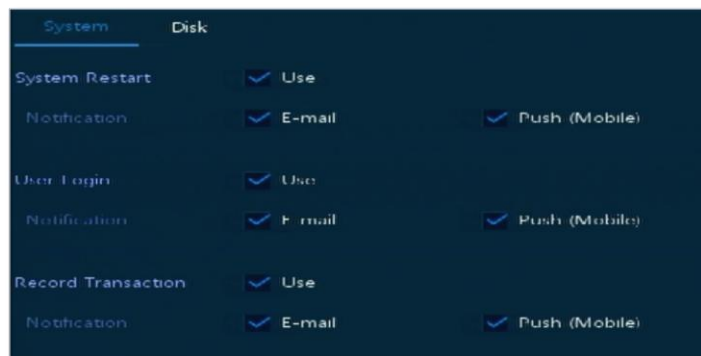


Fig 30.

- Select menu **Event > System /Disk > Disk** and tick to enable Notification by E-mail or Push (fig 31.)

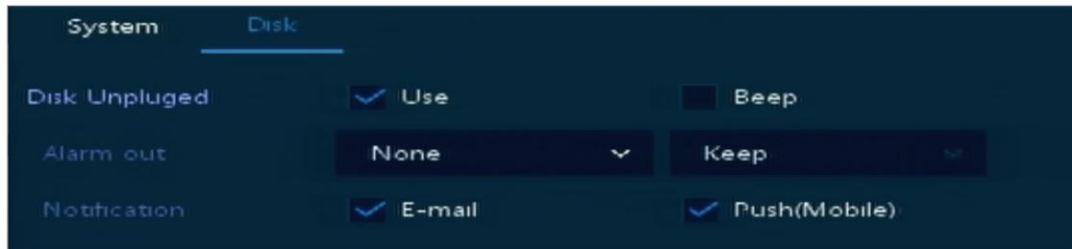


Fig 31.

- Select **Event > Notification > Schedule** and set period for Notification to be enabled (fig 32.);

Click-n-drag the mouse to select the day and hour period to configure, then click the above relevant coloured Key for the setting required. Example shows E-mail + Push set to report 24/7/365.

If an event reoccurs multiple times, the example is set to only report this ONCE in a 10 minute period.

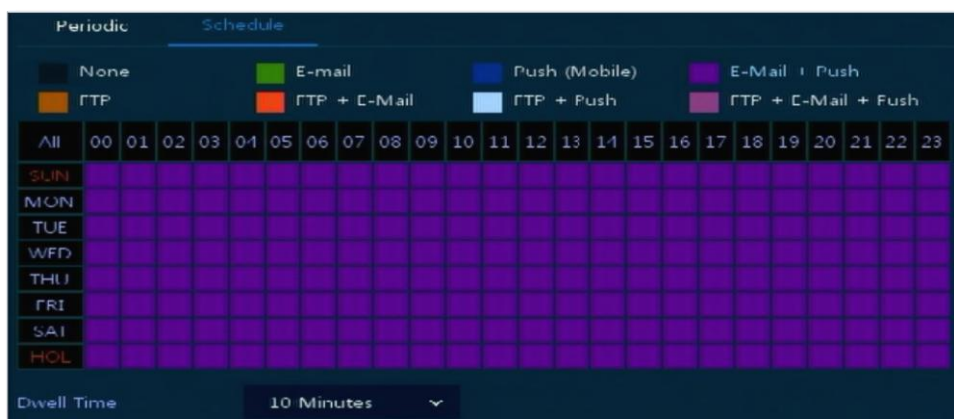


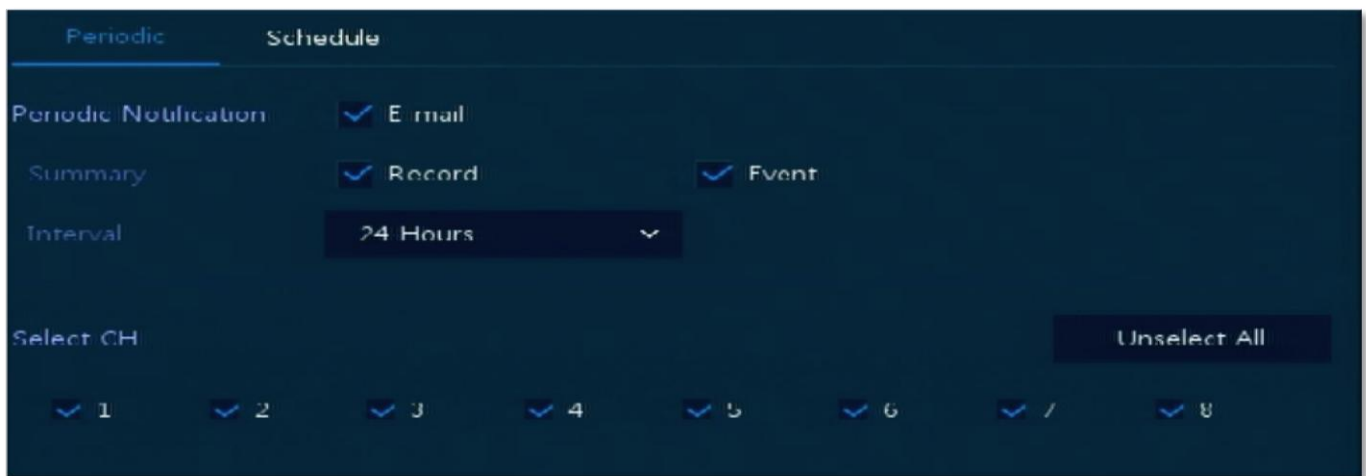
Fig 32.

PERIODIC NOTIFICATION – VIA EMAIL

As e-mail alerts should have already been setup; consider enabling Viper's Periodic Notification feature to a 24-hour period. Once, during this period, Viper sends a single e-mail summary of Recording changes or other events.

Should the periodic e-mail not be received – at the expected schedule – a possible compromise of the DVR could be assumed; either through failure of the hardware, network connection or even tampering!

- Login to Viper as Admin equivalent
- Select menus **Event > Notification > Periodic**
- Click to enable E-mail notification and the Record and Events options (example below)
- Set the required Interval and Select All cameras.



This ends the procedure. However, consider any other security features your system deployment provides and enable these to further harden overall security.

QULU

In many respects a similar Cyber Security approach needs to be taken with a VMS; just as with an NVR. However, a VMS often relies on an open and accessible underlying Operating System – such as Microsoft Windows or Linux - for managing and accessing hardware and network protocols etc. The OS therefore also has to be taken into account. A hardened VMS setup can be undermined if the OS is not also considered!

Here we use Windows Server 2012 R2 as an example with qulu – this being the OS of choice with qulu and HP server Partnership.

It is outside the scope of this document to cover all security aspects of Windows. For this you will need to refer to Microsoft's own hardening documents and suggested practices. We mention the essentials and you are advised to refer to Appendix-1 for other Microsoft resources.

Qulu Developers take extraordinary steps to maintain security including code reviews and automated testing to ensure qulu code is safe from known encryption keys, backdoors and hidden hacks.

What is secured in qulu:

- Access to a qulu system - either local or remote
- Any data (other than the video stream itself) transferred between system components (e.g. client ↔ server, server ↔ server, server ↔ cloud, client ↔ cloud)
- OpenSSL for network connections, disabled deprecated and insecure protocols and use only TLS v1+.
- Server -> Client (Mobile, Desktop, Web) Communications - HTTPS
- HTTPS is used by default for all connections.
- Email (TLS / SSL) - TLS is the default option for the Email Server.
- Salted/Hashed Passwords
- Local Credentials (e.g. local use accounts) are protected using a salted MD5 hash
- Q Cloud Credentials (e.g. qulu Q Cloud user account) use a complex multi-level hash

INSTALLING & DEFAULTING

The following assumes a clean, virus/malware-free and readily installed MS Windows Server 2012R2 is already present – as per the image provided initially on HP qulu partnered servers. Also assumed are pre-installed and hardened IP cameras.

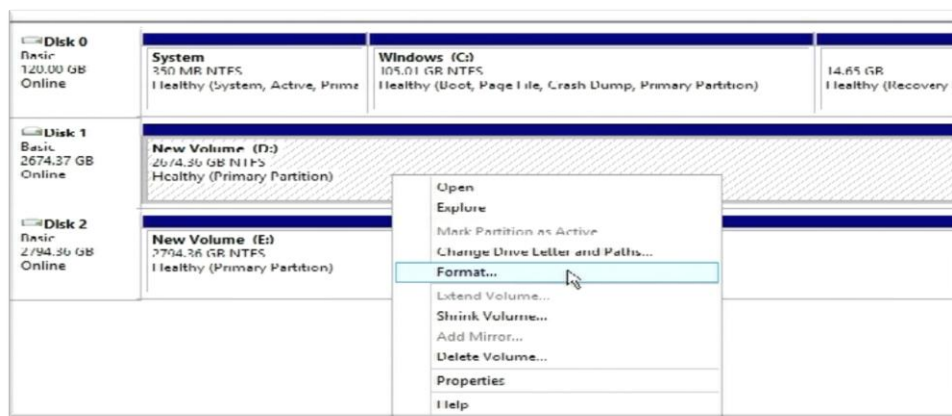
- **Physical location** - secured so as to be only physically accessible to authorised staff – locked comms room.
-
- **Network logical location** – connected to a dedicated CCTV VLAN \ IP Subnet
-
- **Login & Password Access** – “Strong” passwords and separate IDs. Minimal permissions given.

DEFAULT CONFIG AND REFORMAT HDDs

If re-utilising a Windows server – for example one being relocated from a previous customer to a differing customer site - you are responsible to ensure no unauthorised access is permitted to any previous data stored on the server! It is recommended therefore to default and re-image the Windows OS; after reformatting the video archive storage drives; D:\, E:\, F:\, G:\ etc! Then reapply the Windows OS from the qulu SPARK image.

NOTE: Re-imaging a server is lengthy and involved! Contact Vista Technical Support for the original qulu SPARK procedure. Also confirm your Microsoft Windows 2012R2 Authentication Key is present before attempting!

- Login to the Windows server as Admin
- Open Disk Manager, reformat the storage HDDs D:\, E:\, F:\ G:\ etc. Do not reformat the smaller SD Card!
- Reboot and use the SPARK procedure to reboot to SPARK and re-image the server.
- Once Windows Server reinstalled; connect to the Internet via a protected firewall.
- Reactivate Windows License
- Run MS Updates repeatedly, until the server is up to date and no more are required.



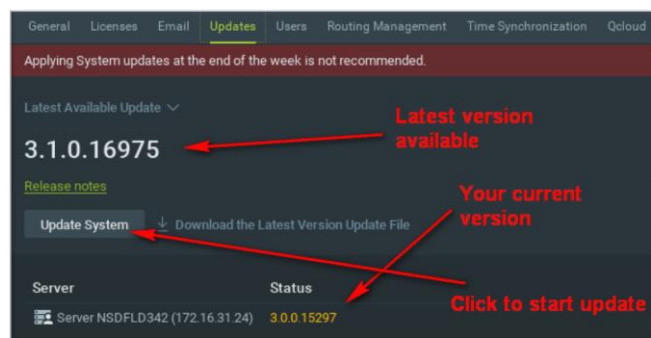
UPGRADE TO LATEST VERSION

Ensure qulu is kept up to date with the latest version. Management of updates, and upgrading, are far easier if both your qulu servers and qulu client PCs have Internet access! If not, there is an “offline” ZIP file update procedure that you can follow.

ONLINE UPDATES

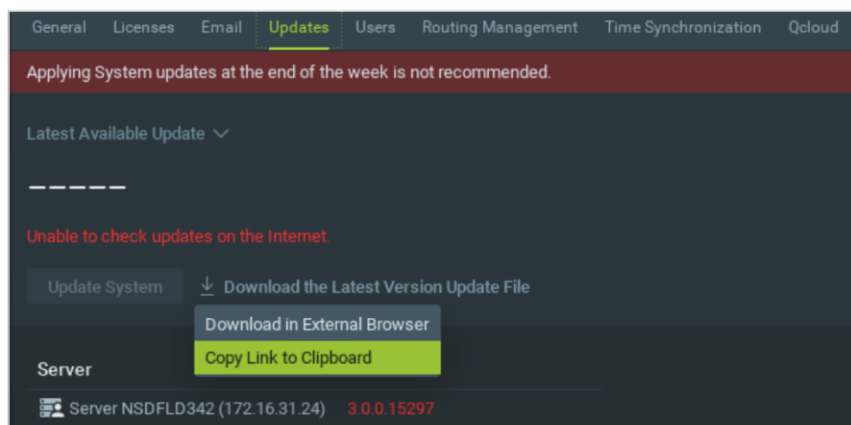
Qulu will, as default, check for updates over the internet. It will not however apply them without acknowledgment from an Administrator.

- Login to qulu client as Administrator equivalent
- Right-click the qulu System container name at the top of the Resource Tree - top-left
- Select **System Administration > Updates**.
- Screen similar to below is displayed. Click **[Update System]** to update all qulu servers in the list
- Once completed, visit each qulu client PC, exit and close qulu client, then re-open. Client will prompt to update if it is Internet connected.



OFFLINE UPDATES

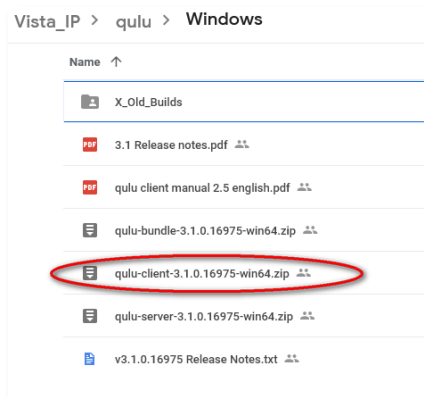
- Login to qulu client as Administrator equivalent
- Right-click the qulu System container name at the top of the Resource Tree - top-left
- Select **System Administration > Updates**.
- Screen similar to below is displayed. Click **[Download Latest Version Update File]**
- Select **[Copy Link to Clipboard]**



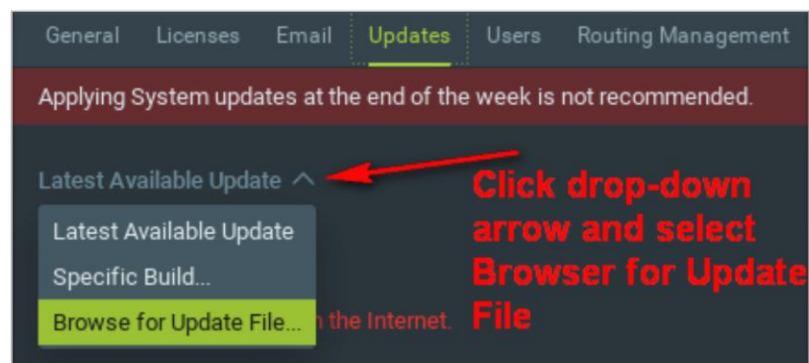
- Open Notepad and paste the Clipboard contents - will be a long web url. Save this!
- Gain access to a site or café location with Internet access; paste the url into your Internet browser.
- Click Save_As; save resulting zip file. Note the version number or qulu implied by the file's name.

Note, the above downloaded .zip file will upgrade all qulu servers on a site plus the single qulu client PC you use to perform the upgrade. If you have additional qulu clients then also download the following;

1. Go to www.vista-cctv.com Click links for **Support > Downloads > Vista IP**
2. Click folders **qulu > Windows** > a screen as below will appear. Click, download and unzip the qulu-client.zip file (example circled) ensuring it is the same version as the first zip file downloaded.
3. Do not unzip the first file you downloaded!



- Revisit the qulu site and log back into the Updates screen where you left off.
- Click the down arrow of the dialogue box [**Latest Available Update**] and select Browse for Update File.



- Browse and select the first .zip file downloaded. All servers will now update. Be patient until 100% completed!

Note: if you have additional qulu client PCs, they will need to be separately upgraded;

1. Once the servers and initial client are completed, visit each qulu client PC in turn.
2. Exit and close qulu client. Then reinstall the later qulu client by running the second file you were directed to download – the unzipped file – and select **Client Install Only**
3. Qulu client will now be updated on this PC.
4. Repeat as required.

LOGIN ACCOUNTS, PASSWORDS & PERMISSIONS

Create separate login accounts, strong passwords and only give relevant permissions according to each person's authority.

| Qulu ID\Feature | Use |
|-----------------|---|
| CCTV Installer | Create dedicated Installer Admin account |
| Store Manager | Create dedicated Manager's Admin account |
| Staff | Create non-Admin accounts for general staff – removing abilities to modify the system, add other user accounts and export evidence (if necessary) |
| Passwords | Set strong passwords – as previously outlined |
| Auto log-in | Don't enable this option on qulu clients – force users to login via entering their passwords! |

- Login to qulu as Admin equivalent
- In the left-hand Resource Tree; right-click the Users container and select New User (example below)
- Create your required individual accounts.

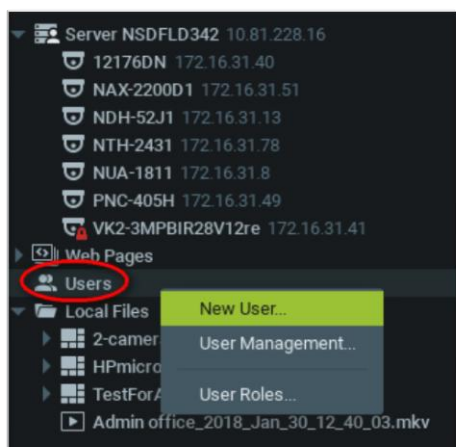


Fig 39.

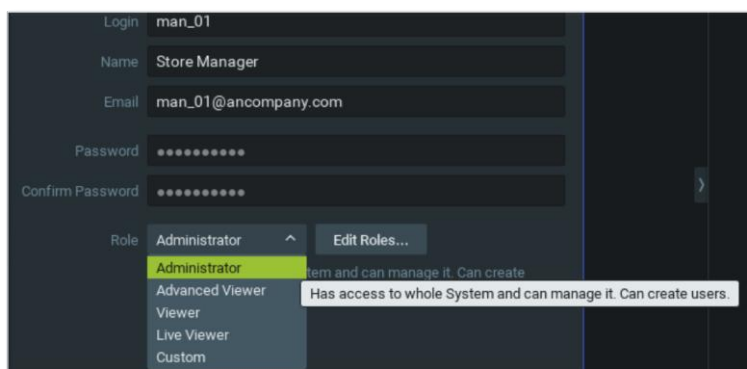


Fig 40.

- For each account set the Role that is only applicable to the user's authority; chose from **Administrator**, **Advanced Viewer**, **Viewer**, **Live Viewer** or alternatively **Custom** to define something unique (below)

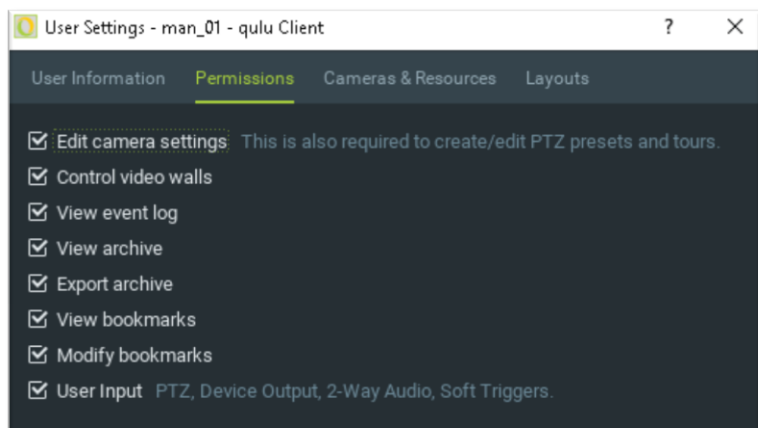


Fig 41

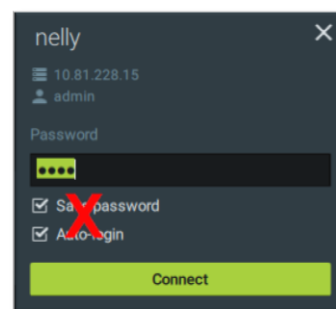


Fig 42.

NOTE: Providing Individuals with their own Login ID enables better Audit Trail reporting in qulu; as Audit entries and access to system features will be attributed to an individual as opposed to a shared office account.

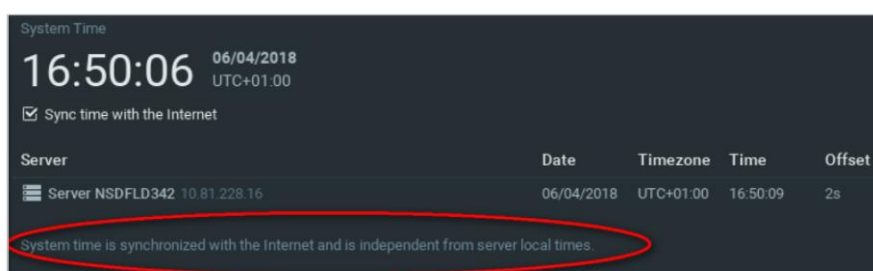
The above accounts and passwords only control and limit access within the qulu client application! They do not control who has access, and to what, on the underlying Windows Operating system!

Vista partnered HP servers supplied for use with qulu do not have the ability to display IP CCTV camera video and therefore not intended for end-users of qulu to log in to them. However, you are advised to change the default passwords for the two accounts provided for Installer and User. Refer to the Windows Server 2012 R2 Password chapter on how to complete this.

TIME AND DATE SYNCHRONISATION

Accurate time stamping of recorded video evidence and data is crucial.

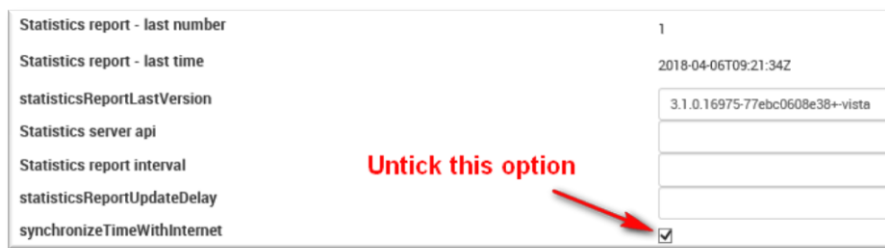
Time synchronisation via NTP is recommended and Qulu servers default to using an NTP server located within the qulu Cloud, via Internet, to determine their locale and system time (example below). If Internet access is available, you need to do nothing more – as long as the time shows as “Sync time with Internet” below.



If no Internet access is available, configure all qulu servers not to use Internet time. Then set a “nominated” qulu server to use the system time from its underlying Windows server OS instead. All other qulu servers in the network will then sync to this time. Finally, login to the nominated Windows server and set it to use your internally provided NTP instead!

- Web browse to each qulu server in- turn using url; <http://address:port/static/index.html#/advanced>
- Login using the Admin ID and password

- Scroll down to the setting **synchronizeTimeWithInternet** and untick it (fig 44)!
- Click **[Save]**
- Repeat the above on all servers.
- Next, login to qulu client as Admin
- Right-click the qulu system container at the top of the left-hand resource tree
- Select menu **System Admin > Time Synchronisation** and click to select the single server you “nominated” (fig 45.).
- Finally, login to Windows on the “nominated” server and set it to point to your internal NTP server.



Statistics report - last number: 1

Statistics report - last time: 2018-04-06T09:21:34Z

statisticsReportLastVersion: 3.1.0.16975-77ebc0608e38+-vista

Statistics server api: [empty]

Statistics report interval: [empty]

statisticsReportUpdateDelay: [empty]

synchronizeTimeWithInternet: ☒

Untick this option

Fig 44.

| | Server | Server Time | Offset |
|-------------------------------------|--|---------------------|-------------|
| <input type="checkbox"/> | Server 2 - HP Microserver (10.0.1.166) | 2016-10-12 11:09:30 | 1 second(s) |
| <input checked="" type="checkbox"/> | Server 3 - i7 (62.252.53.42) | 2016-10-12 11:09:30 | 2 second(s) |
| <input type="checkbox"/> | Q (10.0.1.168) | 2016-10-12 11:09:30 | 1 second(s) |

Fig 45.

NETWORK SETTINGS & TOPOLOGY

Refer to the section on Network Topology Hardening to determine the best practices on where, within a network, to deploy your qulu\Windows servers and cameras. This will determine your IP addressing on your network and what IP details to enter into your Windows Network settings.

Also refer to the section on Windows Hardening;

- Install qulu servers and cameras into dedicated CCTV IP Network – not shared customer network!
- IP address, subnet mask and default gateway – set statically.
- Set DNS server to point to an internal DNS – usually your ISP routers internal IP address - statically.
- Qulu's default TCP port = 7001. Use this unless the site has specific demands for an alternative.

ADDING IP CAMERAS WITH STRONG PASSWORDS

Qulu will assume default IDs and Passwords have been used on IP cameras when trying to add them for recording! Follow the procedure below for amending the login details of a camera;

- Ensure IP camera configured as required – with strong password - and accessible on the network
- Login to qulu client as Admin equivalent
- As default; qulu will AutoDetect new cameras and add them – without setting recording.
- Any camera where the incorrect Password is used will show a padlock icon (Fig 46)
- Right-click camera in the resource tree
- Select **Camera Settings > General** for the menu below (Fig 47);
- Then amend the password and click **[Apply]**
- Camera padlock should now be removed and camera then viewable from qulu.

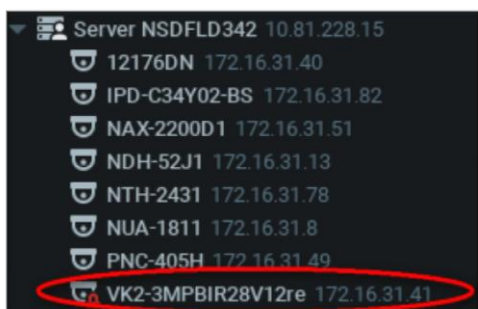


Fig 46

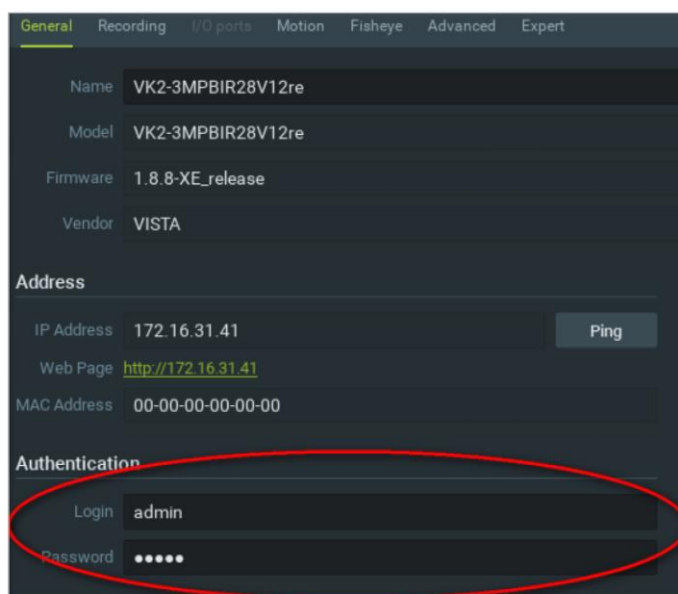


Fig 47

NOTIFICATION AND ALERTS

gulu provides powerful and flexible Event reporting and handling via the creation of Rules. Each Rule is a combination of an Event that occurs and an Action that will then be initiated.

Consider setting reporting of the below subset of Events to help protect and report on access being made to CCTV data, or any activity that could be compromising it;

| Events to Report & Log | |
|------------------------|---------------------------------|
| • | Storage Failure |
| • | Device IP Conflict |
| • | Server Failure |
| • | Servers Conflict |
| • | E-Mail Server is not Configured |
| • | Error while Sending E-Mail |
| • | Storage is not Configured |
| • | Server Started |
| • | Archive Backup Finished |

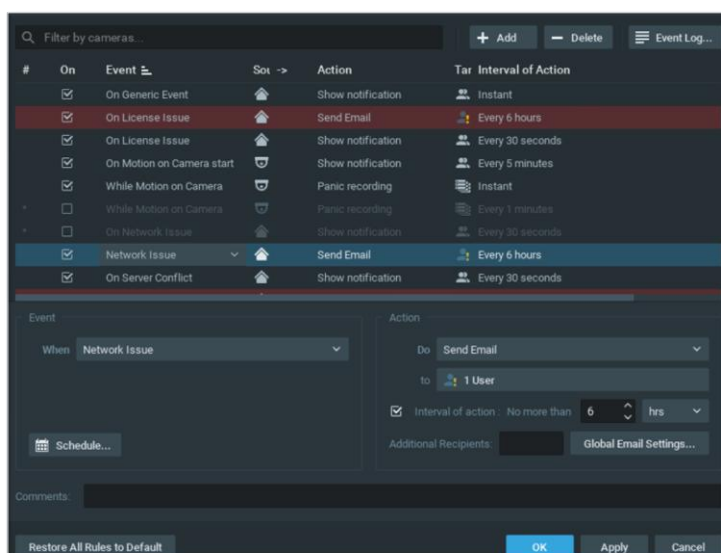
>>>>>>>>

| Possible Actions | |
|------------------|-------------------------|
| • | E-mail Notifications |
| • | Visual Event Indication |
| • | Play Sound |
| • | Notifications |
| | |
| | |
| | |
| | |
| | |

To configure gulu Rules do the following:

- Open gulu System Administration (right-click top left of system tree) and click **Alarm/Event Rules** button on the General tab (or press CTRL + E).

The following dialog will open:



To add a new Rule, click Add and configure your new Rule;

- Select **Event** on the left-hand side that needs to be monitored (refer to above suggested table)

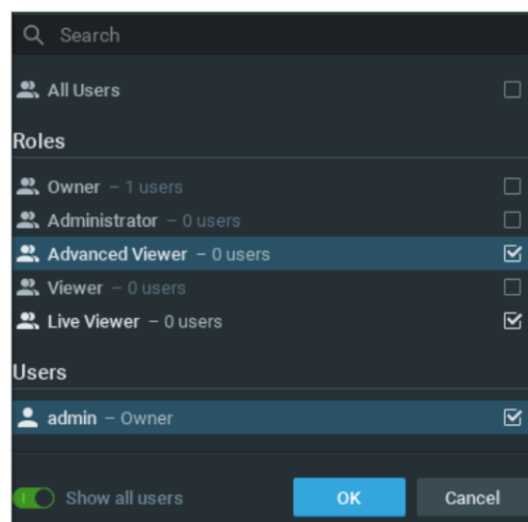
- Select **Action** on the right-hand side that needs to be performed when the Event occurs (refer above table)
- Specify basic parameters for Event and Action. Click on Source or Target column in the Rule row and choose the desired value.

IMPORTANT. If some fields are missing or incorrect, the Rule will be invalid and turn red (below)



- Set the Users that will be targeted if required for the specific Action – such as e-mail recipients (below).

- Set required Aggregation period – if blank the specified Actions will be executed every time the Events occurs.
- If any additional configuration is needed, click **Advanced**.
- Add Comments if needed and set the flag (on the left-hand side of the Rule) to enable it.
- Click **Apply** to accept changes.



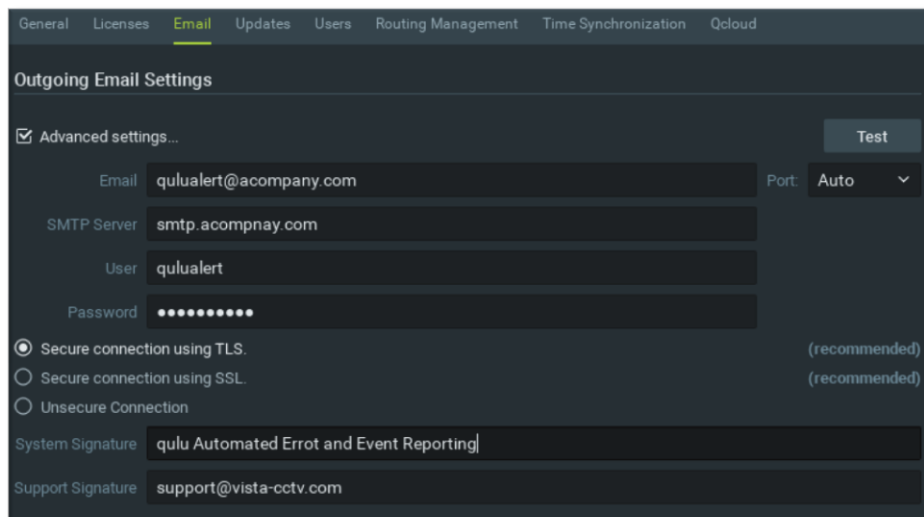
NOTE: If setting e-mail notification, remember to configure your e-mail server details into qulu and to set the e-mail address for each qulu user account!

NOTIFICATION & ALERTS VIA EMAIL

Prior to setting any Event Rules etc; ensure you configure your e-mail server details into qulu. Also enter an e-mail address for each qulu login ID that will receive alerts. Follow the below;

To set e-mail server;

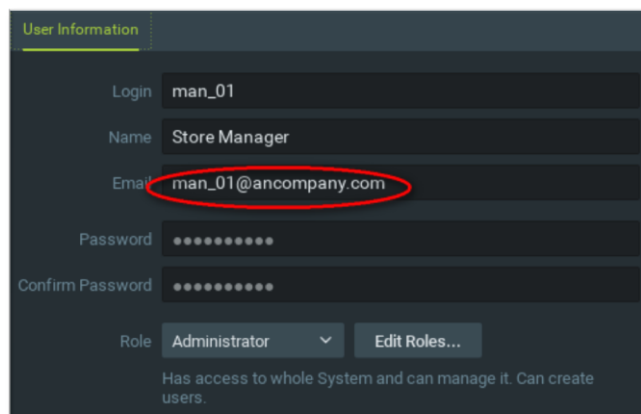
- Right-click the qulu system name at the top of the qulu resource tree, then select System Administration or press CTRL+ALT+A.
- Enter and apply details as the example below, then click Apply.



NOTE: Ensure the e-mail server you use makes use of a Secure login connection via TLS, where possible, or SSL. Do not use Unsecure Connection. This does depend on any e-mail server supplied to you supporting encryption.

- Set e-mail of each user
- In the qulu resource tree; click and expand the Users container.
- Then right-click on the relevant qulu user ID and set their individual e-mail address as below example.
- Click **Apply**.

You can now specify this user as receiving e-mail notifications within Rules Actions



AUDITING QULU SYSTEM

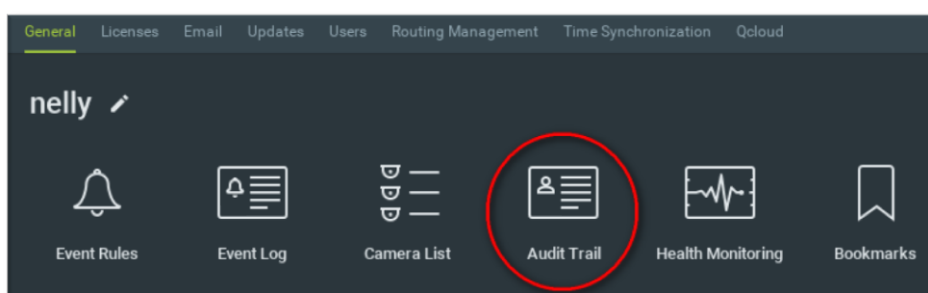
qulu tracks all user account actions and records them to log for later auditing purposes. Use the feature to regularly review who has accessed what data & footage, as well as made changes to the qulu system.

Ensure first that you adhere to the **Login Accounts and Passwords** section and suggestion that each individual user of the system has their own ID and password.

NOTE: This feature is available for Administrators only (see "Introducing User Roles").

To manage and run reports;

- Right-click qulu System name container in the qulu resource tree
- Select System Administration then click Audit Trail in the menu (below)



- Use the screen example below – self-explanatory - to then report on the Audit Trail

9/4/17 10/11/17 Search Clear Filter Refresh

☒ Login/logout
 ☒ Watching live
 ☒ Exporting video
 ☒ System actions
 ☒ Event rules
 ☒ Select all

☒ User actions
 ☒ Watching archive
 ☒ Camera actions
 ☒ Server actions
 ☒ Email settings

| Sessions | | | | | | Details | | | | | |
|---|--------------------|----------|-------|---------------|----------|----------|----------|-------|---------------|---------------|------------------------|
| Session begins | Session ends | Duration | User | IP | Activity | Date | Time | User | IP | Activity | Description |
| <input checked="" type="checkbox"/> 10/11/17 12:15 PM | 10/11/17 12:15 PM | 0m | admin | 10.1.5.169 | | 10/11/17 | 12:32 PM | admin | 10.1.5.169 | Watching live | 10/11/17 12:32 .. |
| <input checked="" type="checkbox"/> 10/10/17 10:48 AM | 10/10/17 12:51 PM | 2h 3m | admin | 192.168.0.92 | | | 12:16 PM | admin | 10.1.5.134 | Watching live | 10/11/17 12:16 .. |
| <input checked="" type="checkbox"/> 10/10/17 10:43 AM | | | admin | 10.1.5.169 | | | 12:16 PM | admin | 192.168.0.220 | Watching live | 10/11/17 12:15 .. |
| <input checked="" type="checkbox"/> 10/10/17 12:09 AM | | | admin | 192.168.0.4 | | | 12:16 PM | admin | 192.168.0.4 | Watching live | 10/11/17 12:15 .. |
| <input checked="" type="checkbox"/> 10/10/17 12:09 AM | | | admin | 192.168.0.220 | | | 12:16 PM | admin | 10.1.5.136 | Watching live | 10/11/17 12:15 .. |
| <input checked="" type="checkbox"/> 10/9/17 5:23 PM | 10/9/17 5:23 PM | 1m | admin | 192.168.0.92 | | | 12:15 PM | admin | 10.1.5.169 | Watching live | 10/11/17 12:15 .. |
| <input checked="" type="checkbox"/> 10/9/17 4:50 PM | | | admin | 192.168.0.191 | | | 12:15 PM | admin | 10.1.5.169 | Login | Nx Witness/3.1.0.16127 |
| <input checked="" type="checkbox"/> 10/9/17 3:56 PM | 10/9/17 5:17 PM | 1h 26m | admin | 192.168.0.92 | | 10/11/17 | 7:00 AM | admin | 192.168.0.5 | Watching live | 10/11/17 7:00 A.. |
| <input checked="" type="checkbox"/> 10/9/17 3:46 PM | 10/9/17 3:50 PM | 3m | admin | 192.168.0.92 | | | 6:57 AM | admin | 10.1.5.134 | Watching live | 10/11/17 6:57 A.. |
| <input checked="" type="checkbox"/> 10/9/17 3:46 PM | 10/9/17 3:46 PM | 0m | admin | 192.168.0.92 | | | 6:47 AM | admin | 10.1.5.134 | Watching live | 10/11/17 6:47 A.. |
| <input checked="" type="checkbox"/> 10/9/17 2:48 PM | 10/9/17 3:45 PM | 3h 4m | admin | 192.168.0.92 | | | 6:44 AM | admin | 10.1.5.134 | Watching live | 10/11/17 6:44 A.. |
| <input checked="" type="checkbox"/> 10/9/17 9:49 AM | Unsuccessful login | | admin | 192.168.0.82 | | | 6:39 AM | admin | 192.168.0.5 | Watching live | 10/11/17 6:39 A.. |
| <input checked="" type="checkbox"/> 10/9/17 9:48 AM | Unsuccessful login | | admin | 192.168.0.82 | | | 6:30 AM | admin | 192.168.0.5 | Watching live | 10/11/17 6:30 A.. |

- To select a session click on it or use checkbox on the left.
- To select several sessions hold CTRL and/or SHIFT
- Right-click to save to File or copy to Clipboard for saving and importing details.

WINDOWS OPERATING SYSTEM

Security and control of access to a VMS and its data has to take into account security of the underlying Operating System (OS). For example; both easy physical access to a server, and easy to guess default login IDs and passwords on the OS, could negate any security provided within the VMS.

We refer to Windows Server 2012 R2 below; as previously used by Vista qulu HP servers.

NOTE The subject of OS security is extensive and complex and is outside the scope of this document to cover in depth. We therefore highlight some of the principles for CCTV\Security usage.

Basic principles are similar to a DVR or NVR;

- **Physical location** - secured so accessible only to authorised staff – locked comms room.
- **Network logical location** – a dedicated CCTV VLAN \ IP Subnet – not shared Customers network!
- **Login & Password Access** – change all default passwords and only use “strong” passwords!
- **Install Minimal Software Required!** - only install the minimal software required to enable the VMS to operate. Other software, or freeware etc, can introduce virus\trojan\malware to the whole server!
- **Software Updates\AV** - ensure updates and AV software is installed - with definitions kept up to date.
- **Firewall** – leave enabled at all times!

NETWORK SETTINGS & TOPOLOGY

Refer to the section on Network Topology Hardening for guidance and consideration in where to logically connect the Windows server in the network for increased security. This will determine your IP addressing and network settings in order to commission the server securely.

LOGIN ACCOUNTS, PASSWORDS & PERMISSIONS

Vista qulu HP servers are provided with the below default Windows login IDs;

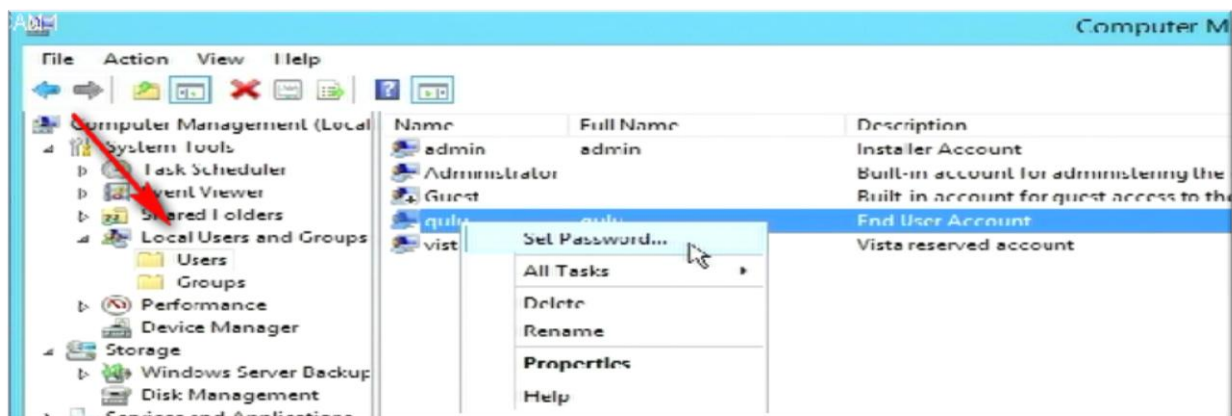
- admin = the CCTV Installers ID (administrator equivalent)
- qulu = end-user ID (user equivalent access only)

Ensure the default passwords for these Windows IDs are changed as part of the commissioning process and set to use “strong” passwords. Refer to the section earlier on “Strong Passwords”.

NOTE: As Vista qulu HP servers do not have qulu client compatible graphics cards, there should be no requirement to provide low-level user Windows login access to qulu servers!

To change the passwords follow the below;

- Login to Windows Server locally as Admin or equivalent
- Click Windows **Start button** (bottom left)
- Start to type **computer** - Windows will auto-complete this to **[Computer Manager]** – click to run
- The **Computer Manager** window will open (below). Click on **Local Users and Groups**
- Amend password as required; but do not change Administrator or Vista account passwords – unless directed to do so!



UPGRADE TO LATEST SOFTWARE – MS UPDATES

The Vista qulu HP server build has MS Updates set to the below as default;

- Check for Updates, but do not download or install.

This setting allows the CCTV Integrator/Installer to maintain control of the server and to manually run updates while in attendance onsite – avoiding the many issues associated with un-attended updates and system restarts! It also allows single qulu servers to be updated and reboot – one at a time – while other qulu servers act as fail-over during the reboot period.

Microsoft regularly updates information on their websites highlighting emerging risks and critical MS Updates & advisories. You can also register for free e-mail notifications via the **Microsoft Technical Security Notifications** web page. You are encouraged to keep up to date with such bulletins and complete Critical Updates as suggested.

WINDOWS FIREWALL AND ANTI-VIRUS

As default; the Vista qulu HP Windows 2012 R2 build has Windows Firewall security enabled. It is strongly suggested that the Firewall is left enabled to protect access to the server.

- Custom ports have already been opened for qulu etc and should not need to be modified in normal circumstances. Though to further increase security you could consider amending existing firewall rules to further restrict the source IP address, or network ranges, for devices that are permitted access to the server's listening port 7001 TCP; such as each permitted qulu client PC. Do not forget any other qulu servers in your network!
- Where Internet access is available to the server, qulu will make use of port 80 (outgoing) to check for qulu updates - and to upgrade should you click to accept the later updates. These functions in themselves do not use an actual Web browser on the server; simply port 80 is convenient and open on most networks allow outgoing access.
- The addition of Anti-virus software to the server will increase security. However, it is not recommended that you use the server's Internet Explorer, or other browser, to make use of the server as if it were a regular user PC and therefore inviting virus infection etc!
- Ensure Anti-virus software is set to exclude scanning the footage archive directories; such as D:\qulu_media, E:\qulu_media etc to minimise impact to the VMS performance.

REMOTE ACCESS SUPPORT APPLICATIONS

Permanently opened and available Remote Support applications, such as Teamviewer and Microsoft Remote Desktop, is not recommended and should be used with extreme caution. It is recommended sessions are only opened - as and when needed – then closed all while being supervised.

Default firewall policy prevents incoming Microsoft Remote Desktop connections.

WINDOWS ERROR LOGS

Regularly review Windows System and Event logs to check for security breaches or failed attempts to login.

- Click Windows **START** button (bottom left)
- Start to type **Event**
- Windows will Auto-complete and suggest **Event Viewer** (below) click to open it.
- Click and expand **[Windows Logs]** on the left, then select **[Security]**
- Review any Audit Failures – especially those that imply “Repeated failed login attempt”.

NOTE: Windows Event Viewer and Logs can produce vast amounts of entries and “false positives” – in other words entries that initially appear to be of concern; but go on to be simple configuration errors or of no concern!

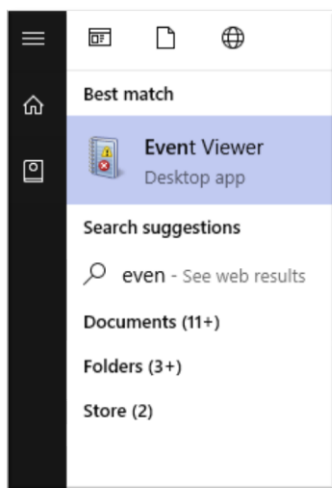


Fig 55.

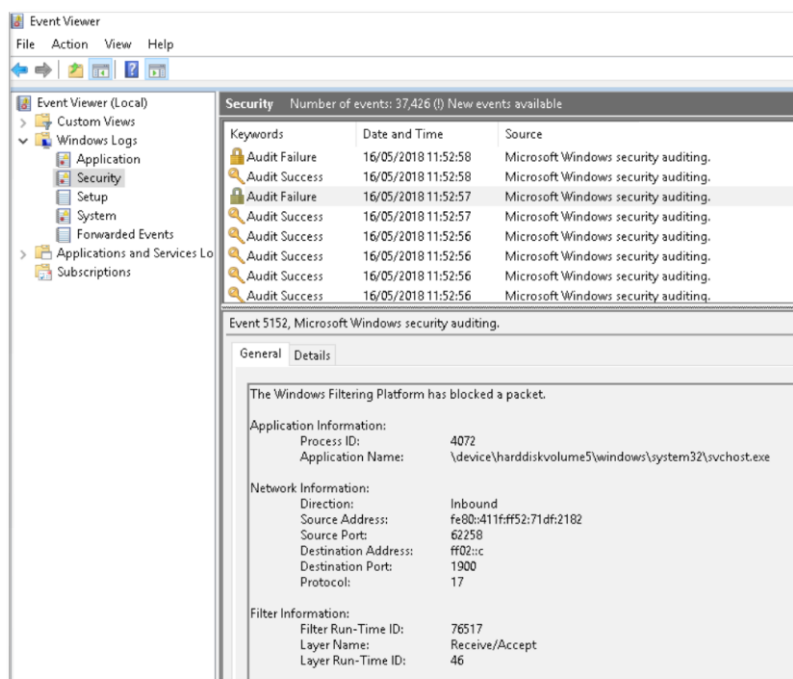


Fig 56.

NETWORK TOPOLOGY HARDNING

Every network and CCTV deployment is unique. However, there are a good many security “basics” and essentials that you are strongly advised to consider and use in every CCTV application.

Consider that it is the accessibility to personal data on a device you are protecting. Access to this is essentially either via local physical access (dealt with earlier) or remotely via network. Therefore, your consideration for any networked device has to always be, “Does everybody really need access to this?” and “Could this be used to compromise other systems\devices?” – then deploy the device accordingly.

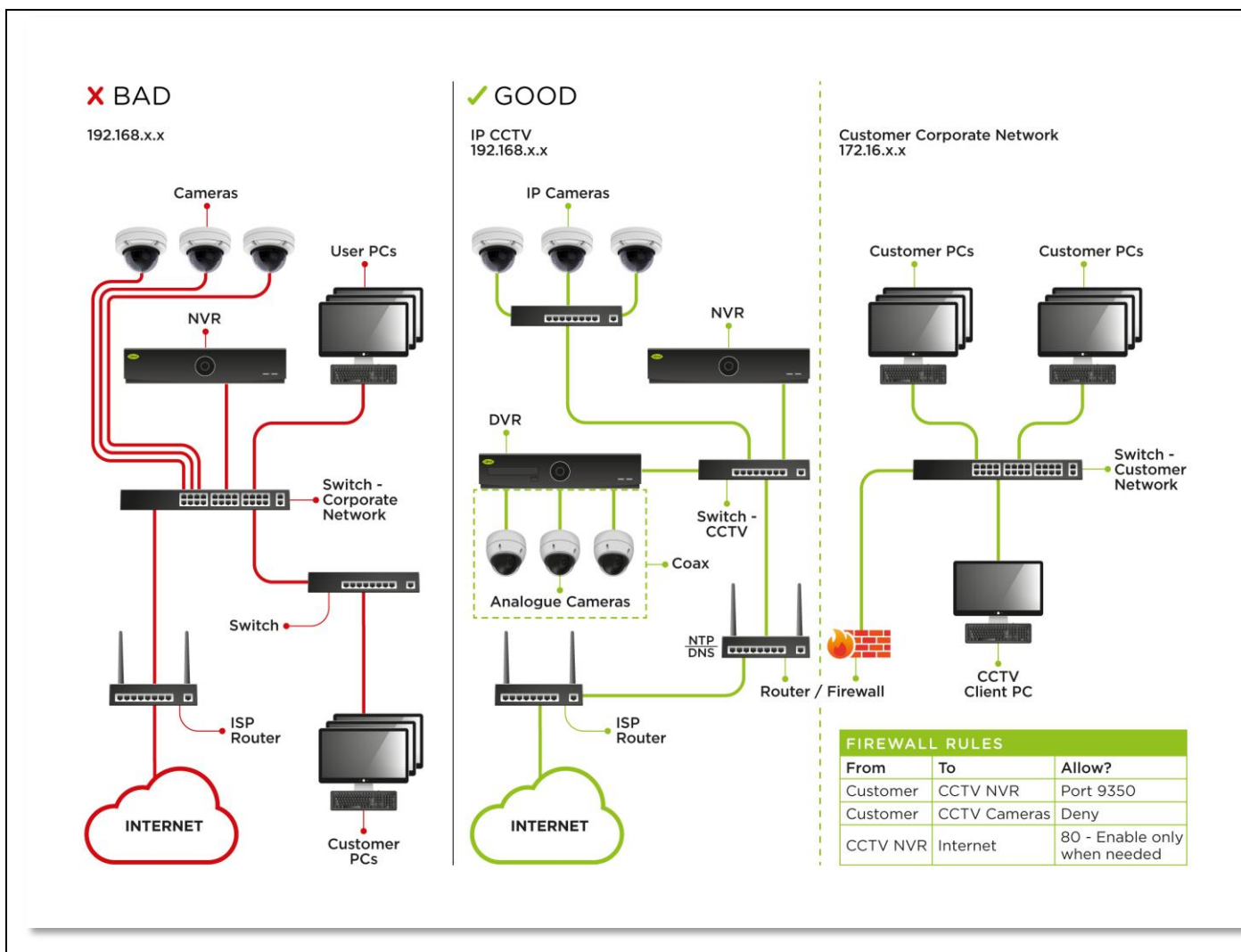
| DEVICE | WHO NEEDS DIRECT NETWORK ACCESS? |
|-------------|--|
| IP camera | <ul style="list-style-type: none"> In most cases only the NVR\VMS recorder! Not normally user’s PCs or the Internet! |
| NVR\VMS\DVR | <ul style="list-style-type: none"> Large Network - normally only individual Viewing Client PCs - not all Corporate PCs! Internet Accessible – if specifically required, reduce risk by placing NVR\DVR behind a firewall and restrict login via a VPN client |

BASICS & ESSENTIALS

- Remember always – threats from an internal network\device are just as likely as the Internet!
- Always provide separate dedicated IP-CCTV network – do not share the end-users Corporate network!
- Use a firewall between IP-CCTV network and corporate network to control access – if needed.
- Manage Firewall policies to restrict CCTV Client PCs to access NVR\VMS only – not direct to IP cameras!
- Consider placing CCTV client PCs in separate network to IP cameras and servers, if compromised they are contained by the firewall.
- Remote mobile Internet devices: consider providing VPN connectivity between device and CCTV site.
- WiFi access points: turn off SSID advertising and placed in separate IP subnet\LAN behind firewall.
- On larger sites\networks; consider Managed Ethernet switches with MAC address Port Security.
- Managed Ethernet switches\routers: all have strong passwords and IP access-list filters!
- Consider disabling unused Ethernet switch ports to deny “stray” devices from being plugged in – will have to unplug either IP camera or NVR\VMS – raising network loss events to be reported.

EXAMPLE NETWORK TOPOLOGY AND FIREWALL

The below network diagram serves to demonstrate a good and bad example of network segmentation for a CCTV application.



| EXAMPLE FIREWAL RULES FOR ABOVE NETWORK | | | | |
|---|-------------------|--------------|-------|---|
| ORDER | SOURCE | DESTINATION | PORTS | ACTION |
| 1 | NVR\VMS | Internet | 80 | Manually permit for updates – then deny ! |
| 2 | NVR\VMS | Customer NTP | 123 | Permit |
| 3 | NVR\VMS | Internet | All | Deny |
| 4 | Viewing Client PC | NVR\VMS | 7001 | Permit |
| 5 | Viewing Client PC | CCTV-Network | ALL | Deny |
| 6 | Internet | NVR\VMS | VPN | Permit |

NOTE: the above are not intended as actual firewall rules, but simply examples to convey understanding.

APPENDIX 1 - OTHER READING RESOURCES

- SANS Institute - 20 Critical Security Controls <https://uk.sans.org/critical-security-controls>
- National Institute of Standards and Technology (NIST- US) <https://www.nist.gov/cyberframework>
- Centre for Internet Security: 20 Critical Security Controls <https://www.cisecurity.org/controls/>
- IC2: 12 Ways to Protect CCTV from Cyber attack: https://www.ic2cctv.com/wp-content/uploads/2017/04/iC2-12-ways-Cyberattack_V2.pdf
- www.cyberessentials.ncsc.gov.uk
- <https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf>
- Microsoft Updates Notification <https://technet.microsoft.com/en-us/security/dd252948.aspx>
- Microsoft Security Updates Guide <https://portal.msrc.microsoft.com/en-us/>
- Vista Support and Downloads <http://vista-cctv.com/> then select Support | Downloads
- Xeno Support and Downloads <http://xeno-cctv.com/>

APPENDIX 2 - VISTA AND OTHER COMMONLY USED IP PORTS

| PORT | USE |
|----------------|---|
| 7001 | Qulu tunnelling (between qulu servers, qulu servers and client PCs etc) |
| 80, 9350, 9360 | Default Vista Viper ports for NVRs\DVRs |
| 554 | Standard for rtsp:// video stream |
| 80 | Web access and ONVIF to-from IP cameras |
| 443 | HTTPS |
| 25 | SMTP e-mail |
| 123 | NTP |
| 2000 | Vista Quantum range of DVRs |
| 3000 | Vista Smart\Tel\Disc etc |
| 9010, 80,554 | Xeno |