American Dynamics

From Tyco Security Products

VideoEdge NVR

Installation and User Guide

VideoEdge 5.2.2

8200-1765-01 B0

Notice

The information in this manual was correct when published. The manufacturer reserves the right to revise and improve its products. All specifications are therefore subject to change without notice.

Product offerings and specifications are subject to change without notice. Not all products include all features; refer to product data sheets for full feature information.

Copyright

American Dynamics

60 Congress Avenue

Boca Raton, FL 33487 U.S.A.

Customer Service

Thank you for using American Dynamics products. We support our products through an extensive worldwide network of dealers. The dealer through whom you originally purchased this product is your point of contact if you need service or support. Our dealers are empowered to provide the very best in customer service and support. Dealers should contact American Dynamics at (800) 507-6268 or (561) 912-6259 or on the Web at www.americandynamics.net.

Trademarks

Product offerings and specifications are subject to change without notice. Actual products may vary from photos. Not all products include all features. Availability varies by region; contact your sales representative.

MPEG-4 Disclaimer

H.264 Disclaimer

This product is licensed under the AVC Patent Portfolio License for the personal and non-commercial use of a consumer to (i) encode video in compliance with the AVC Standard ("AVC Video") and/or (ii) decode AVC video that was encoded by a consumer engaged in a personal and non-commercial activity and/or was obtained from a video provider licensed to provide AVC video. No license is granted or shall be implied for any other use. Additional information may be obtained from MPEG LA, LLC. See HTTP://WWW.MPEGLA.COM

License Information

Your use of this product is governed by certain terms and conditions. Please see the detailed license information at the end of this manual.

United States

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Changes or modifications not expressly approved by Sensormatic, could void the user's authority to operate the equipment.

This product was FCC verified under test conditions that included the use of shielded I/O cables and connectors between system components. To be in compliance with FCC regulations, the user must use shielded cables and connectors for all except power and alarm cables.

Canada

This Class A digital apparatus complies with Canadian ICES-003.

European Union

EMC compliance

Warning

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Only the following connections are expected to be limited to <3m cables:
USB

Only the following cables are expected to be shielded:
Video BNC cables
Monitor video cables

General Safety warnings

1 This product must be earthed. Plugs and sockets can vary between countries, ensure that the earth pin mates correctly with the socket and that an earthed socket is used.

2 For indoor use only

3 For professional installation, use and service.

4 This product is only suitable for operation below altitudes or equivalent air pressure of:

- Desktop versions - 2000m
- Rack mountable versions - 3200m

For rack mountable equipment:

a Elevated Operating Ambient - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) of 35°C. The unit operating temperature range is 5-35°C.

b Reduced Air Flow - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.

c Mechanical Loading - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.

d Circuit Overloading - Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

e Reliable Earthing - Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips).

This symbol means the product is classified as waste Electrical and Electronic equipment under the WEEE directive (2002/96/EC). It should not be placed in the normal waste stream and should be separately collected for specific recycling as WEEE.

The above symbol also covers the battery directive (2006/66/EC). The product contains a replaceable battery which should not be placed in the normal waste stream and should be separately collected for specific recycling as waste batteries.

Please check with your regional waste management authority on where to dispose of WEEE or Batteries or packaging.

This device is not intended for use in the direct field of view at visual display workplaces. To avoid incommoding reflections at visual display workplaces this device must not be placed in the direct field of view.

The 4 Channel VideoEdge Micro is intended to be supplied by the Listed Power Adapter with output rated 24Vdc, 5A minimum.

The 8 Channel VideoEdge Micro is intended to be supplied by the Listed Power Adapter with output rated 24Vdc, 7.5A minimum.

The power rating for the VideoEdge Micro NVR is Max 120W, for 4 Channel variants and Max 180W for 8 channel variants. The power rating for desktop units is 100-240V, 50-60Hz, Max 300W, Max 4.5A. The power rating for the 2U and 3U rack mountable units is 100-240V, 50-60Hz, Max 350W, Max 6.0A.

US/CAN deviations - The RJ45 connections  identified on the product as 'RJ45 Gigabit Ethernet Port' are intended for ethernet use only, NOT for telecommunication applications.

Note:
VideoEdge Micro NVR - These models provide either 4 or 8 IP video channels with an onboard PoE switch(es). Each channel is rated at 15W Max.

RTC Battery replacement

The product is fitted with an lithium metal coin-cell type CR2032, the user can replace this however a professionally trained technician is recommended to avoid damage to the internals of the product.

A coin-cell battery (CR2032) powers the real-time clock and CMOS memory. When the product is not plugged into a wall socket, the battery has an estimated life of three years. When the product is plugged in, the standby current from the power supply extends the life of the battery. The clock is accurate to ± 13 minutes/year at 25°C with 3.3 VSB applied.

When the voltage drops below a certain level, the BIOS Setup program settings stored in CMOS RAM (for example, the date and time) might not be accurate. Replace the battery with an equivalent one.

Caution

RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE.
DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS.

To replace the battery, follow these steps:

1. Observe the following precautions:
    - Disconnect the power before removing the cover. Note that there are hazardous voltages in the PSU module, and while these cannot be touched easily and are protected it may be possible to touch live parts with a small tool.
    - Take adequate ESD precautions and wear an ESD strap connected to the chassis of the products.
    - Preferably use a non-conductive tool to remove the battery, try to avoid touching the new battery with fingers.
2. Turn off all peripheral devices connected to the computer. Disconnect the computer's power cord from the AC power source (wall outlet or power adapter).
3. Remove the computer cover.
4. Locate the battery on the board.
5. With a medium flat-bladed screwdriver, gently pry the battery free from its connector. Note the orientation of the "+" and "-" on the battery.
6. Install the new battery in the connector, orientating the "+" and "-" correctly.
7. Replace the computer cover.

VideoEdge

VideoEdge is a scalable video surveillance solution. Its open platform solution supports third party devices, storage and clients, allowing management of video systems and edge devices through a single, logical interface.

VideoEdge manages a number of devices (e.g. video cameras, encoders, audio devices, text devices etc.) and records onto its configured storage. It also provides clients with secure access to live and recorded data from its devices.

VideoEdge Range

VideoEdge Micro

Small form factor 4 or 8 channel IP only VideoEdge with a built in POE Switch.

VideoEdge Desktop Hybrid NVR

Desktop Hybrid VideoEdge with 8 analog and 8 IP video channels.

VideoEdge Desktop NVR

Desktop 32 channel IP only VideoEdge.

VideoEdge 1U NVR

Rack mountable VideoEdge with 32 IP video channels and 16 PoE ports.

VideoEdge 2U Hybrid NVR

Rack mountable Hybrid VideoEdge with 16 analog and 16 IP video channels.

VideoEdge 2U NVR

Rack mountable VideoEdge with 64 IP video channels.

VideoEdge 3U Hybrid NVR

Rack mountable Hybrid VideoEdge with 32 analog and 32 IP video channels.

VideoEdge 2U NVR Server

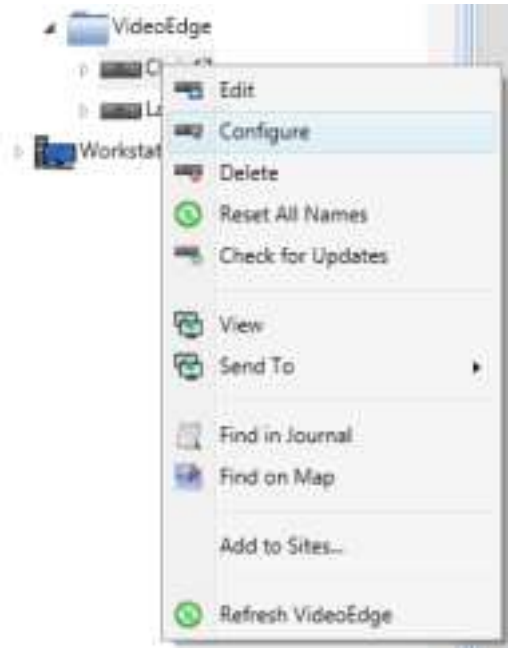
Rack mountable VideoEdge with 128 IP video channels.

VideoEdge Administration Interface

The VideoEdge Administration Interface allows users to interact with the NVR. This provides information about the server and allows you to modify its settings. There are 3 ways to access the VideoEdge Administration Interface:

- Locally on the VideoEdge by selecting the Administration Interface desktop icon. This will launch Mozilla Firefox ESR with the VideoEdge Administration Interface login page loaded.

- From the web browser of a Windows PC with network connectivity to the VideoEdge. Enter the IP address of the VideoEdge in the address bar of your web browser. Supported browsers are Microsoft Internet Explorer (9+), Google Chrome (latest version) and Mozilla Firefox (latest version).
- From victor unified client. Right click on the VideoEdge in the victor device list and select Configure. Note victor will use the version of Microsoft Internet Explorer installed so ensure a supported version (9+) is installed on the victor unified client PC.

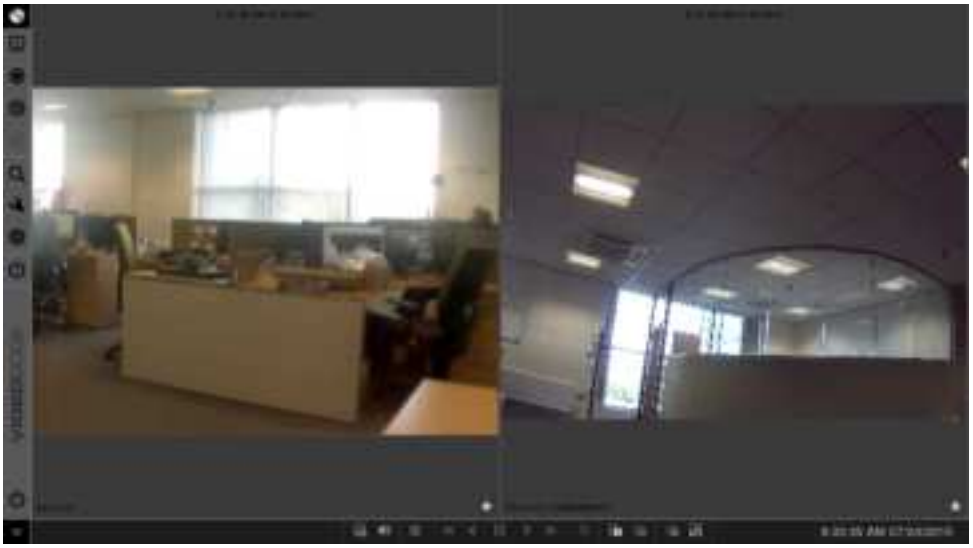


Clients

VideoEdge supports streaming of live and recorded media to a number of clients:

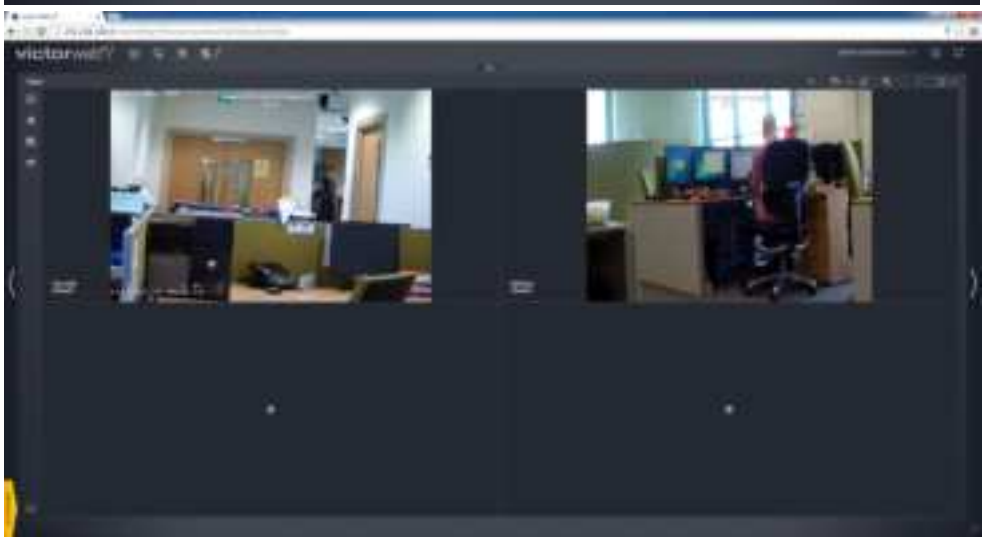
VideoEdge Client

VideoEdge Client is an integrated client installed on the VideoEdge. It can be launched from the VideoEdge desktop by selecting the VideoEdge Client icon. Users can login using the same credentials as used for the VideoEdge Administration Interface. VideoEdge Client allows monitoring of devices added to the host VideoEdge NVR. For more information, refer to the VideoEdge Client User Guide.



victor Web / victor Web LT

victor Web is a portal that allows access to live and recorded media from multiple VideoEdge recorders through a web browser. victor Web is hosted on a Windows PC and supports integration with a victor Application Server. victor Web LT is an alternative version of victor Web, and is hosted on a VideoEdge. Access victor Web or victor web LT by navigating to "xx.xx.xx.xx/victorweb" where "xx.xx.xx.xx" is the IP address of the host. Users can log in to victor Web LT using the same credentials as used for the VideoEdge Administration Interface. victor Web requires a license to run, but offers additional features that aren't available in victor Web LT. victor Web LT is included free with VideoEdge software. For more information, refer to the victor Web and victor Web LT User Guide.

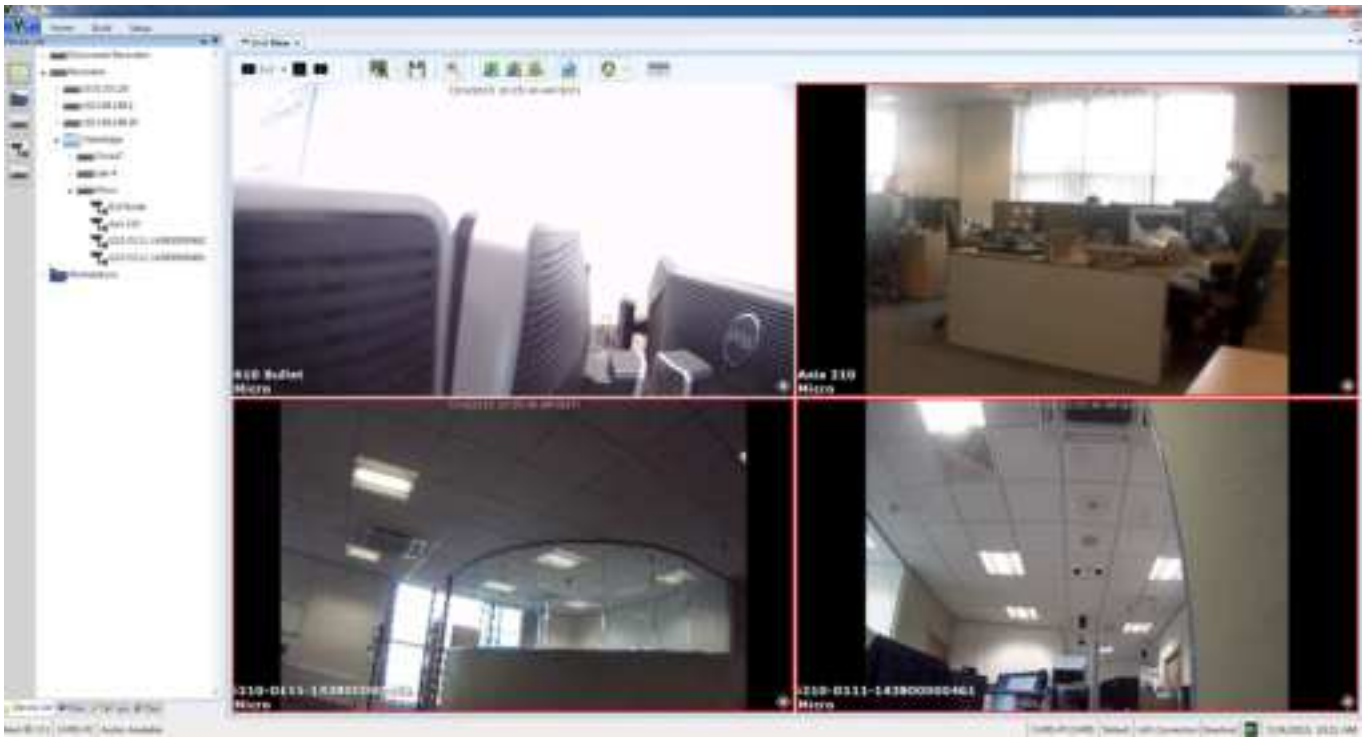


victor

victor is a full featured, Windows based rich client for VideoEdge and other video recorders from Tyco Security Products. It allows management of live and recorded video, supports multiple integrations with 3rd party security hardware and unifies with Software House C·CURE 9000, allowing unified control and monitoring of your entire security system. victor has a complete and scalable portfolio of products;

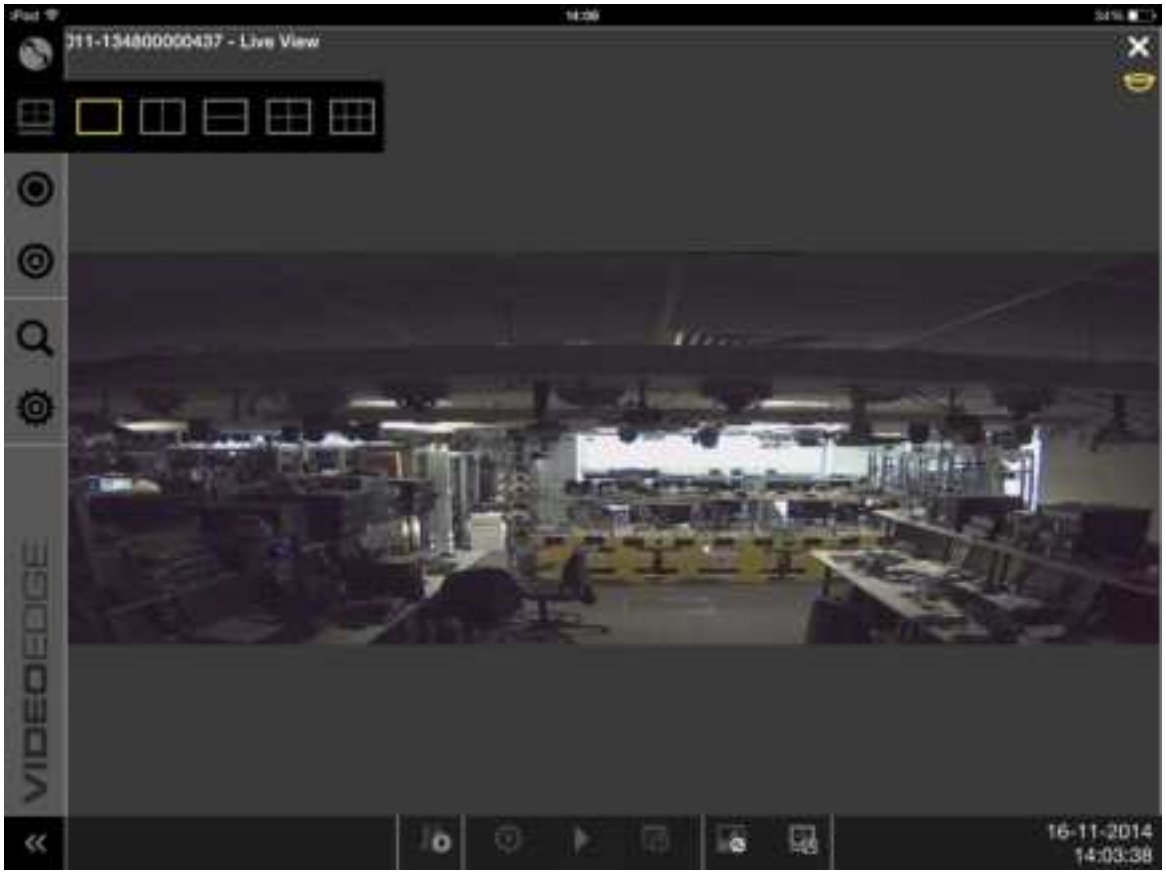
- victor Express - a one client connection version of victor with no requirement for a victor Application Server.
- victor Professional - a full featured surveillance application using server/client architecture and backed by a victor Application Server using a Microsoft SQL Server backend.
- victor Enterprise - for large and geographically dispersed systems, victor along with C·CURE 9000 supports enterprise deployments for unified control and monitoring across the enterprise.

For more information on victor, refer to the victor Configuration and Administration Guide. victor is available for download from http://www.americandynamics.net.



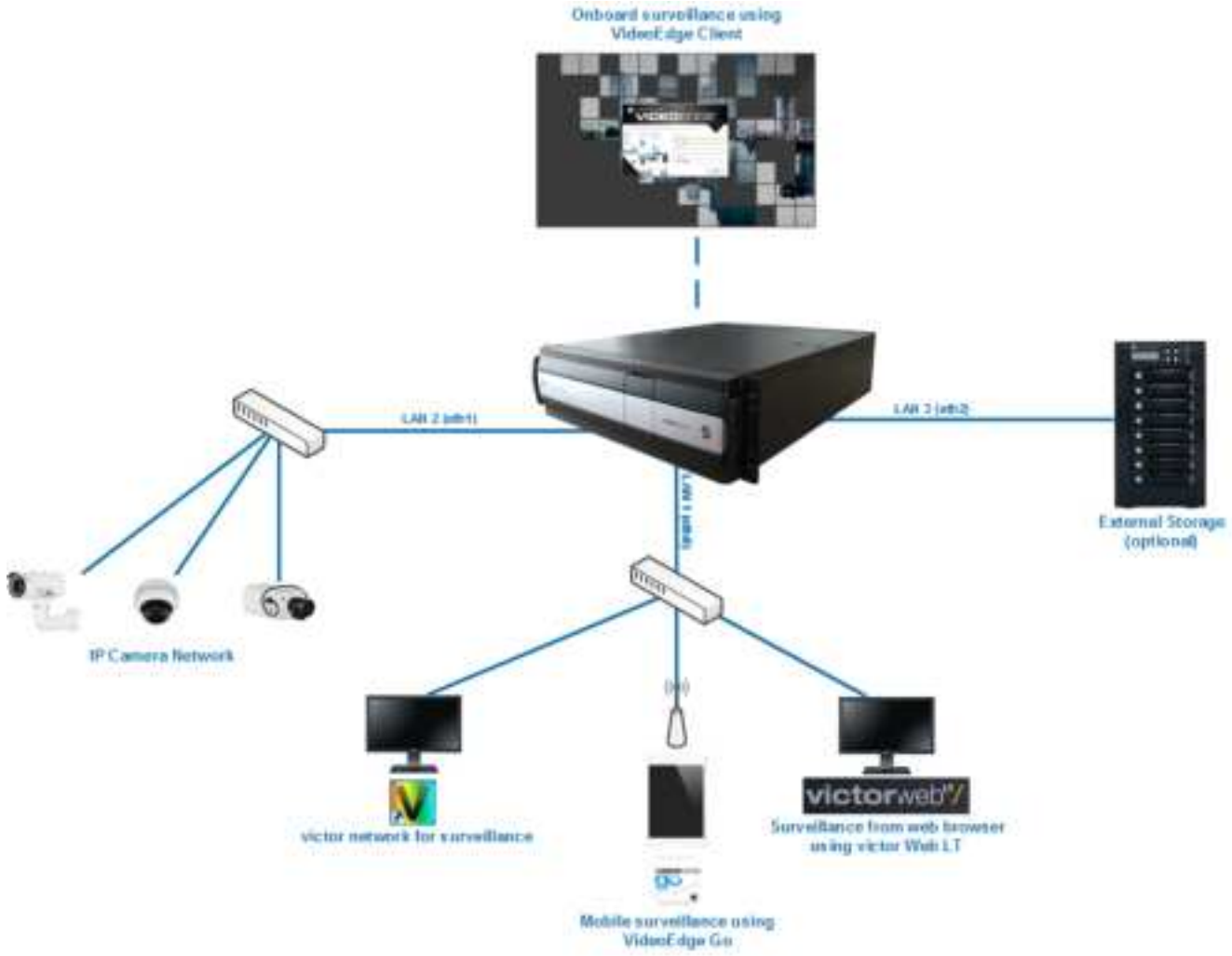
VideoEdge Go

VideoEdge Go is a fully featured video surveillance mobile application, designed to bring surveillance of VideoEdge recorders to mobile devices. VideoEdge Go is available from your devices App Store.



Network

Typical network topology of an IP only VideoEdge is shown below. In addition, Hybrid VideoEdge can have analog cameras directly connected to the BNC inputs on the rear of the NVR.



SmartStream

SmartStream is the resource management tool for VideoEdge. VideoEdge automatically manages resources in order to best reflect your network's capabilities. SmartStream resource management is applied during streaming to clients, it is achieved using transcoding which can apply reductions to resolution and frame rate. SmartStream has no effect on the VideoEdge Client.

Installing VideoEdge

Overview

VideoEdge is available in multiple platforms providing a versatile solution for your Network Video Recorder needs.

This section describes the installation and configuration process for VideoEdge, which is supplied as either:

1 Hardware and Software bundle

2 Software Only bundle

This section describes the initial setup of your VideoEdge.

Hardware and Software Bundle

When VideoEdge is supplied as a pre-configured hardware and software bundle the basic system settings including time and region are already applied. The system will also have default partitioning carried out including the required system partitions and some media partitions. If the configured media partitions are not suitable these can be edited as required after installation.

VideoEdge is supplied with NIC eth0 enabled, it's set to resolve a DHCP IP address or will be assigned a default static IP address of 10.10.10.10 if DHCP is not available. All other NICs will be supplied disabled. The network settings are configured using the Setup Wizard.

Software Only

When VideoEdge is supplied as software only, it requires full installation onto your hardware. You should ensure your hardware matches the minimum operation requirements.

Caution

Any previously configured OS on this system will be removed and overwritten.

Safety Guidelines

General Safety Warnings

1 Check the product label for power supply requirements to assure that no overloading of supply circuits or over current protection occurs. Mains grounding must be reliable and uncompromised by any connections.

2 Use an uninterruptible power supply (UPS) as standard practice to protect computing systems from power fluctuations that may cause data loss.

3 This product must be grounded. Plugs and sockets can vary between countries, ensure that the earth pin mates correctly with the socket and that an earthed socket is used.

4 For indoor use only.

5 For professional installation, use and service.

6 This product is only suitable for operation below altitudes or equivalent air pressure of:

- Desktop versions - 2000m
- Rack mountable versions - 3200m

Connecting Cameras and Peripherals

Caution

Protect the unit against lightning. If part of a cable is installed outside a building, the entire cable is vulnerable to lightning. Install surge protectors on all vulnerable cables.

Video Devices

Procedure 1
Connecting Video Devices

Step	Action
1	Connect the cameras: a Connect the video cables from the cameras to the BNC connectors labeled video inputs on the rear of the unit. Connect VideoEdge to the Camera Network using eth1.
2	Connect any External Storage Modules (ESMs).
3	Connect a monitor using either the VGA, DVI-I or HDMI ports. **Note:** VGA is only available on the VideoEdge Micro, VideoEdge Desktop Hybrid NVR and VideoEdge Desktop NVR models.
4	(Optional) Connect a spot monitor to the video output BNC connector on the Analog board to see live video. The VideoEdge 2U and 3U Hybrid NVR models have two video outputs. Video displayed from the video output is configured using the Monitor Outputs page of the Administrator Interface, refer to Monitor Outputs for further information.

- End -

Audio Devices

Procedure 2
Connecting Audio Devices

Step	Action
1	Connect the microphone or audio source to the VideoEdge through the color-coded 3.5 mm audio connectors on the back of the unit. **Note:** For the best quality sound, use a pre-amplifier with appropriate filtering with a compatible microphone.
2	Connect the audio inputs from each analog camera to the corresponding audio input on the analog rear panel. **Note:** The location of the audio inputs/outputs on the rear panel varies slightly with different variants of VideoEdge.

- End -

Optional Components

You can connect optional devices to your VideoEdge including:

1 A keyboard and mouse. Adding a keyboard to the VideoEdge unit provides access to the operating system's features such as Log Off, Shut Down and to other applications.

2 A dome controller (Sensormatic VM16E, American Dynamics ADTTE Touch Tracker, ADTT16E Advanced Dome Controller or AD2089 Analog Keyboard) to the COM2 connector.

Figure 1 ADTTE/ADTT16E Wiring Diagram

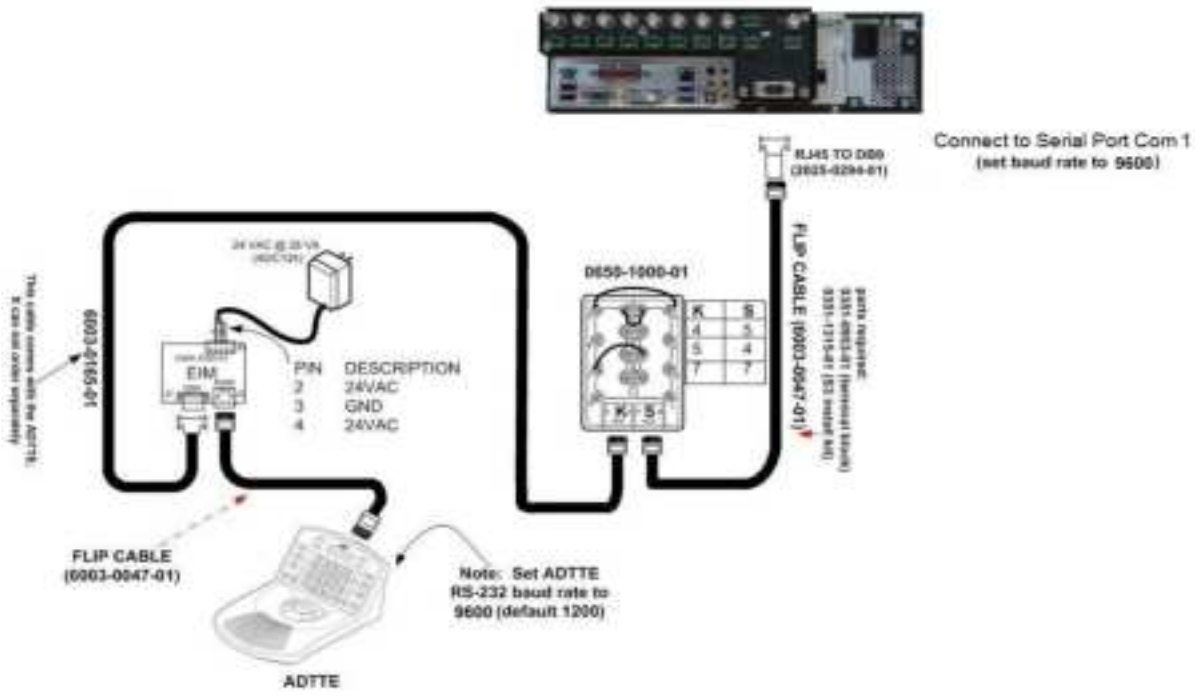
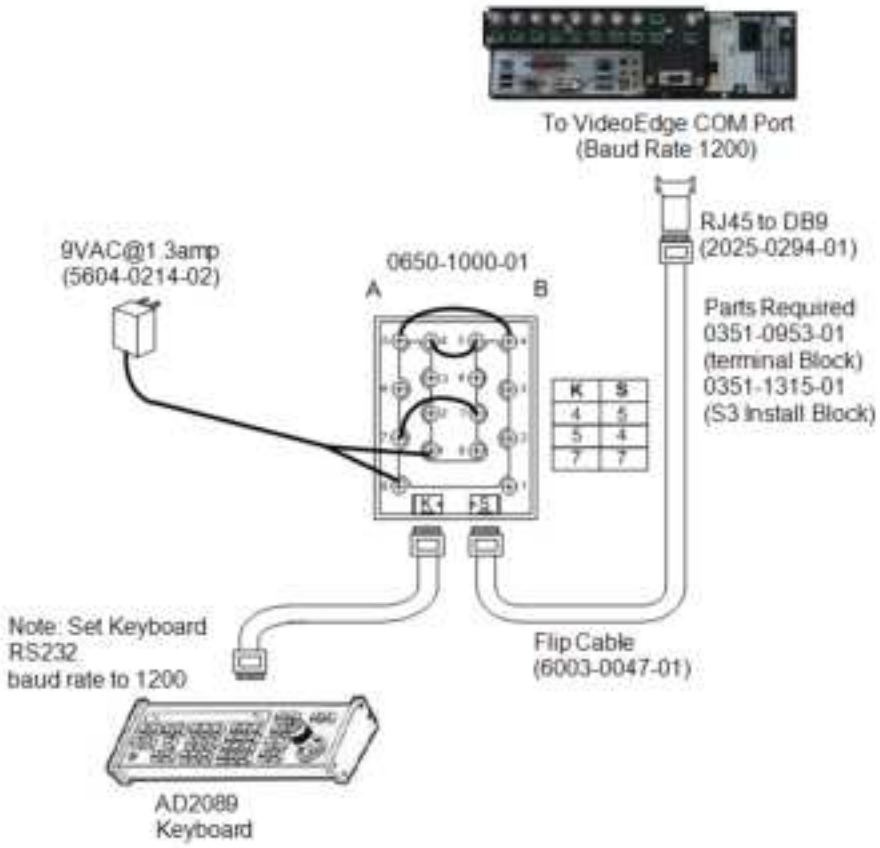


Figure 2 AD2089 Wiring Diagram



3 A matrix switcher for dome control or devices for serial text input through the USB port.

Connecting Alarms to VideoEdge

The alarm connectors on the back of the unit accept both alarm inputs and outputs. The alarm outputs are TTL outputs 5V DC, 20mA maximum.

The polarity of all alarm inputs is programmable. However, the polarity of all alarm outputs is active–high. Alarm outputs are initialized to inactive–low on power-up.

Attach the alarm inputs, outputs, and grounds to the connectors, according to the pin assignment.

Connecting VideoEdge to a Network

Connect the cable from the local area network to the Ethernet port. Use Category 5 twisted-pair Ethernet cable (CAT 5 TPE)

Connecting VideoEdge to an Analog Matrix

VideoEdge 2U and 3U Hybrid NVRs can be connected to an analog matrix providing PTZ support for dome cameras connected to the matrix. Up to 16 monitors can be connected and used to display video from the matrix. The following matrix controllers are supported:

- MegaPower 3200
- MegaPower 48 Plus

Rack Mounting the System

The VideoEdge rack mountable chassis' have pre-drilled holes to install the included rack slides. Mount the unit by attaching rack slides to the chassis and using the included front mount rack holes.

Caution

You must mount the unit in a fully supported rack. Use rails rated for a minimum of 150 pounds that attach to both sides of the unit and to the front and back of the rack. The rack must be equipped with EIA-310-D standard 19-inch front and rear mounting flanges.

Safety for Rack Mountable Equipment

1. Elevated Operating Ambient - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) For rack-mounted units is 35° C.
2. Reduced Air Flow - Installation of this equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.
3. Mechanical Loading - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
4. Circuit Overloading - Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on over current protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.
5. Reliable Grounding - Reliable grounding of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips).

Hardware and Software Bundles

Installing the VideoEdge Hardware and Software Bundles

The installation and configuration process consists of:

1. Initial boot up of VideoEdge
2. Logging into the VideoEdge Desktop
3. Configuring VideoEdge using the Setup Wizard

Initial Boot Up of VideoEdge

Procedure 3
Powering up VideoEdge for the First Time

Step	Action
1	Power up VideoEdge. A series of boot messages appear and the system is loaded to the License Agreement.
2	When the license agreement is displayed, select **Yes, I Agree to the License Agreement**.
3	Click **Next**. Set the Password for the Root User account page displays. The next stage of installation process is to create user accounts.
4	In the Password field in the Root User account page of the Installer, enter a password for the root user account

Caution

It is extremely important that you will remember this password. If necessary you should write this password down and store it securely.

5	Re-enter the password in the Confirm Password field.
6	Click Next.
7	If the system does not recognize the password as secure, a message opens. Click **Yes** to confirm the use of the weak password and continue, or click **No** to change the password. A secure password should contain both upper and lower case letters, numbers and special characters. **Note:** If the passwords entered into the Password and Confirm Password fields do not match, a message opens. Re-enter the passwords to continue.
8	To continue with the installation and configuration process you need to log in to the VideoEdge desktop.

- End -

Logging into the VideoEdge Desktop

After setting the root password and creation of the administration user you are required to login to the VideoEdge desktop to continue the installation and configuration process.

Figure 3 VideoEdge Login Screen

Procedure 4
Logging into the VideoEdge Desktop

Step	Action
1	When the system boots to the VideoEdge login screen. Enter the **Username**. Default Username: **VideoEdge**.
2	Click **Log In**.
3	Enter the **Password**. Default Password: **VideoEdge**.
4	Click **Log In**.
	On successful login, the VideoEdge desktop is displayed.

- End -

To complete the installation and configuration process you need to complete the Setup Wizard, continue to VideoEdge Setup Wizard.

VideoEdge Setup Wizard

Once VideoEdge has been installed you need to configure the basic settings via the Setup Wizard. On completion your VideoEdge will be operational. This can be accessed using the VideoEdge Administrator icon on the desktop or via a remote client. On the first time accessing the Administration Interface after installation you will be automatically be directed to the Setup Wizard.

Caution

The VideoEdge Administration icon has been added for convenience. Firefox ESR is the supported browser for use with the Administration Interface when accessing it locally on VideoEdge. When accessing the Administration Interface from a remote client PC, Internet Explorer Versions 9, 10 & 11, Firefox and Google Chrome are the supported browsers. Safari is not supported.

Note:
If you exit the Setup Wizard prior to completing all the steps, the wizard will save your progress and automatically return to the last page viewed of the Setup Wizard.

The wizard consists of the following menu items:

- Preparation
- System
- Network
- Devices
- System Security
- Finish

Procedure 5
Logging into the Wizard

Step	Action
1	Enter the Administrator **Username**.
2	Enter the Administrator **Password**.
	Note: The default username and password for the NVR administrator user role is username: **admin**, password **admin**.

- End -

Preparation

This menu item describes the preparation stage of the Setup Wizard. The Welcome tab displays.

Welcome Page

The Welcome page is the first page of the Setup Wizard. From the Welcome page you can select the language in which the Administration Interface is displayed. You can also view the current version of the VideoEdge software, or you can install a different version of the VideoEdge software. To advance to the next page click Start.

Figure 4 Welcome Page

Note:

- To install a newer version of VideoEdge, you can use an upgrade file or an OEM installation file.
- To install an older version of VideoEdge, you must use an OEM installation file.

Procedure 6
Installing a new version of VideoEdge

Step	Action
1	Insert a USB drive into the VideoEdge
2	Click **Reboot**.
3	From the confirmation popup, select **OK** to begin the installation.

- End -

Procedure 7
Selecting the Language

Step	Action
1	Select the required language from the **Choose Language** dropdown.
2	Click **Start** and advance to the next page.

- End -

System

This System menu item displays the Support ID and allows system information to be edited.

System Info Page

The System Info page is used to edit the VideoEdge hostname, location, current date and current time.

Caution

It is **critical** that you configure the correct Location and the Current Date/Time to ensure VideoEdge is fully operational on completion of the Setup Wizard and to ensure recorded media has the correct timestamp.

Figure 5 System Info Page

Procedure 8
System Info Settings

Step	Action
1	To edit the following fields: • **Hostname** • **Location** • **Current Date/Time** Select the current value. Edit the value as required. **Note:** • The VideoEdge hostname may contain alphanumeric characters, and also **.** or **-**. However, **.** and **-** are not allowed at the start or end of the hostname. • The VideoEdge hostname must not exceed 15 characters in length.

2 (Optional) De-select the **Enable Smart Search (Motion Metadata)** checkbox to disable Smart Search for all cameras that are added to the VideoEdge. This feature can be enabled/disabled on cameras being added manually or at the **Discovery** page for cameras being added using the **Auto Discovery** feature.

Note:
• The **Enable Smart Search (Motion Metadata)** checkbox is enabled by default, except for the R7 series units.
• This feature automatically enables Smart Search when you add a new device to your VideoEdge.
• After you enable Smart Search on a camera, you can enable a Motion Detection alarm for that camera from the **Alarms** page in the **Devices** menu.

3 Click 

4 Click **Continue** to advance to the next page.

- End -

Network

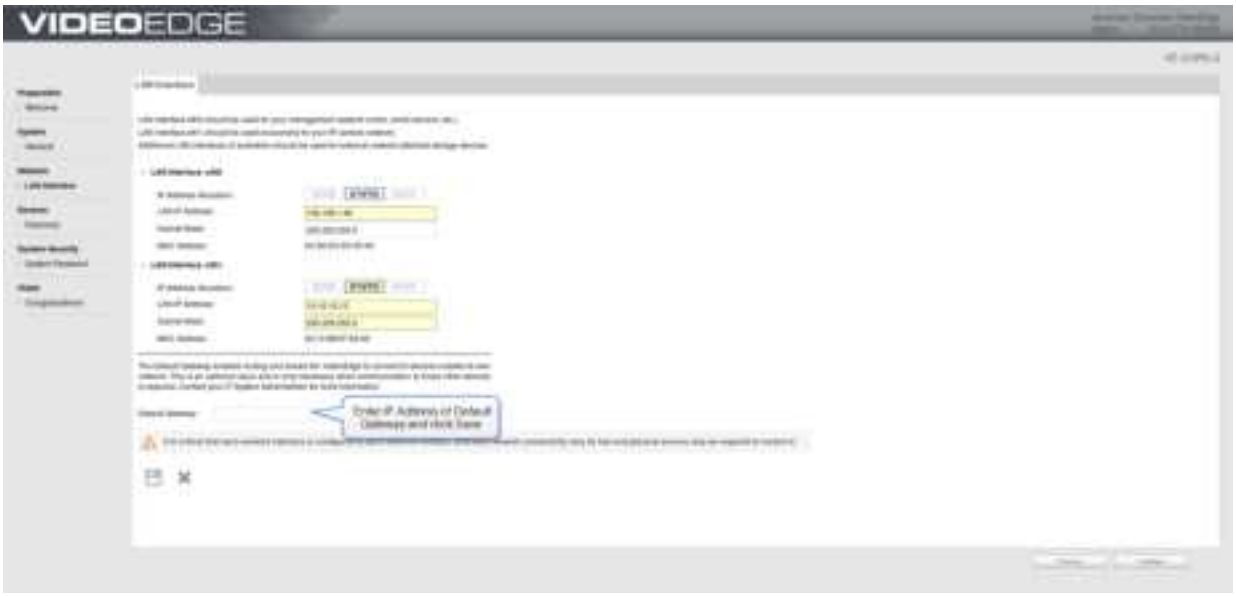
This section describes the network stage of the Setup Wizard and outline all LAN interface details.

LAN Interface Page

The LAN Interface page is used to edit the LAN interface settings for each NIC including IP address allocation, LAN IP address, subnet mask and IP broadcast.

VideoEdge can have multiple active NICs. This allows the use of dedicated camera networks.

Figure 6 LAN Interface Page



Procedure 9
LAN Interface Settings

Step	Action
1	Edit the following LAN Interface settings for the NIC that you want to modify: • **IP Address Allocation** **Note:** To open the Administration Interface the IP address of one of the NICs must be known, if all the IP addresses are dynamic they will vary in value. It is recommended that a NIC is configured with a static IP address and subnet mask for this reason. • **LAN IP Address** • **Subnet Mask** • **Default Gateway** **Note:** The Subnet Mask is defined by three classes of IP Address A, B and C which will determine its value. They are as follows:

1. **Class A** - First Octet Decimal Range 1-126, Subnet Mask Value **255.0.0.0**

2. **Class B** - First Octet Decimal Range 128-191, Subnet Mask Value **255.255.0.0**

3. **Class C** - First Octet Decimal Range 192-223, Subnet Mask Value **255.255.255.0**

Class A addresses 127.0.0.0 to 127.255.255.255 cannot be used and are reserved for loopback and diagnostic functions.

2 Edit the setting as required and click 

3 Click **Continue** to advance to the next page.

- End -

Devices

Discovery Page

The Discovery page automatically discovers all 'discoverable devices' on the network to add to VideoEdge. Multiple devices can be discovered until you reach your limit of camera licenses.

Not all cameras can be added to VideoEdge in this way as some manufacturers require cameras to be pre-configured prior to being added to a network.

Figure 7 Discovery Page

Procedure 10
Discovery Settings

Step	Action
	The Discovery page automatically displays all discovered devices. **Note:** If there are devices that you expected to be discovered, but are not displayed, you may need to add these devices manually as some manufacturers do not have Discovery configured by default.
1	Select the checkboxes for the devices you want to add to VideoEdge from the Discovered device list.
2	(Optional) De-select the **Enable Smart Search (Motion Metadata)** checkbox to disable Smart Search on the camera / cameras that are being added.
3	Click ⊕ The imported device(s) are displayed in the Video / Audio List tab
4	Click **Continue** to advance to the next page. **Note:** For further information on Camera and Device Discovery refer to Discovery for further information.

- End -

System Security

System Password page

From the System Password page you can change the root password and the VideoEdge password.

Caution

- It is highly recommended for security reasons that you change the root password and the VideoEdge password.
- To enable SSH or XRDP in VideoEdge 5.1, you must change the default VideoEdge password.

Figure 8 System Password Page

Procedure 11
Changing the System passwords

Step	Action

1 Select the **Set system password** checkbox.

Figure 9 The System Password page displays in HTTPS.

2 In the **Change System VideoEdge Password** section, update the following fields:

a Enter the **Current Password**.

b Enter the **New Password**.

c Re-enter the New Password in the **Confirm Password** field.

3 In the **Change System root Password** section, update the following fields:

a Enter the **Current Password**.

b Enter the **New Password**.

c Re-enter the New Password in the **Confirm Password** field.

Caution

It is extremely important that you remember this password. If necessary, you should write this password down and store it securely.

4 Click 

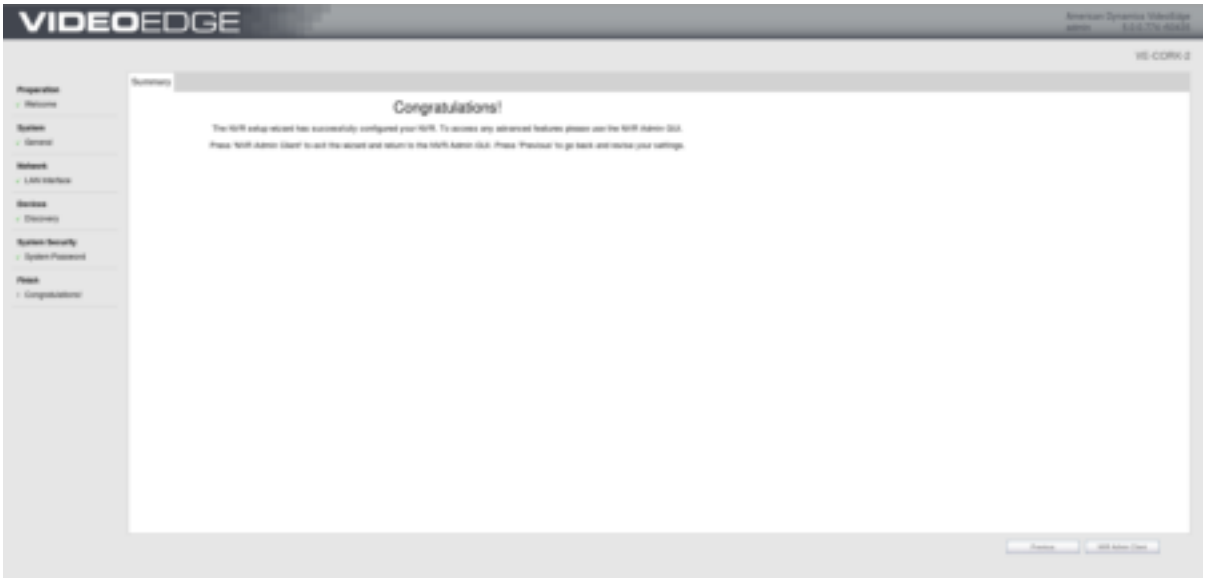
5 Click **Continue** to advance to the next page.

- End -

Finish

The Setup Wizard is now complete, you can exit the wizard to the Administration Interface.

Figure 10 Summary Page



VideoEdge Software Only

This section details the installation and configuration process for VideoEdge software only package.

Before installation you must ensure that the system drive is connected to the SATA 0 location on the motherboard.

Caution

Any previously configured OS on this system will be removed and over written.

Installing the VideoEdge Software Only

The installation and configuration process consists of:

1. Booting the system using the NVR software disk or USB
2. Accepting the license agreement
3. The Self Installer initiates
4. A system reboot after basic installation
5. Logging into the NVR desktop
6. Configuring the NVR using the Setup Wizard

Boot your Computer/Server Using the VideoEdge Software DVD or USB

To initialize the installation of VideoEdge, the system must boot from the software DVD or USB.

Procedure 12
Boot your Computer/Server Using the VideoEdge Software DVD or USB

Step	Action
1	Insert the VideoEdge software DVD into the optical drive or insert the VideoEdge Installation USB drive into one of the available USB ports and restart your computer/server. **Note:** If you are installing from a USB drive, ensure that no other USB drives are inserted during installation.
2	VideoEdge boots from the DVD or USB drive and the installation options menu opens. **Note:** If VideoEdge does not boot from the disk, intercept the Boot Loader by pressing the required function key. Please check your computer/server function key to enter Boot Loader. Then select the required drive and press Enter.
3	From the installations option menu select **Install / Restore_VideoEdge_NVR_Release_4.9.0** and press **Enter**. **Note:** After approximately 20 seconds the installation will automatically start in this mode. A Loading Linux Kernel pop up displays followed by a series of boot messages. This process may take several minutes. **Note:** The VideoEdge software will install the minimum required Linux Operating System to run the VideoEdge system (The VideoEdge software is installed as an appliance).
4	Read and Accept the license agreement by selecting **Next** and selecting **Yes**. The self-installer will initiate; progress will be displayed during installation.
5	Once self-installer has completed and **Reboot NVR** when prompted.
6	Remove installable media.
7	When the GRUB screen displays, ensure VideoEdge is selected and press **Enter**. The VideoEdge desktop will load.
8	Enter your **Username**. Default Username: VideoEdge
9	Select **Log in**.
10	Enter your **Password**. Default Password: VideoEdge
11	Select **Log in**. The Setup Wizard will be launched. Refer to the VideoEdge Setup Wizard section above for further information.

- End -

Setting up VideoEdge

When VideoEdge is installed, default partitioning is configured including the required system partitions and media partitions. If you add additional external storage to VideoEdge, you can configure the media partitions as required. Refer to Storage for more information.

VideoEdge is supplied with its NIC eth0 enabled. It is set assigned a default static IP address of 10.10.10.10. Remaining NICs will not be resolved.

The **root** VideoEdge OS account is assigned with the password **root** and is required to access the VideoEdge's desktop.

Note:
In the interest of server security, the default root password should be changed at the earliest opportunity. Ensure you make note of your chosen password as you will be unable to make administrative changes to the VideoEdge's desktop without it.

A **VideoEdge** account is created and assigned with the password **VideoEdge** and is required to access the VideoEdge Client.

System settings including date and time must be configured during the Setup Wizard. You must also enable recording on all analog channels with cameras connected during the Setup Wizard.

All other settings can be configured during the Setup Wizard or via the Administration interface once set up is complete.

System Partitions

The tables outlined in this section describe the partitions set up by default on VideoEdge. There are several model variations depending on the storage capacity supplied. For each VideoEdge approximately 500GB of storage is required for system partitions. The remaining storage available can be used for media storage and is configured as media partitions.

Models with 500GB capacity require additional external storage to be added and configured to record media. By default no media storage partitions are configured on these devices.

Media partitions are configured to create one media partition for each hard drive, therefore utilizing all available storage space.

Table 1 System Partitions

System Partitions				
	Size	**Type**	**FS Type**	**Mount Point**
All Models and All Model Types	16 GB	Linux swap	Swap	swap
	47 GB	Linux native	XFS	/var
	20 GB	Linux native	Ext3	/

Table 2 Default Partitions

Partitions					
Model	**Media Storage**	**Drive Size**	**Type**	**FS Type**	**Mount Point**

VideoEdge Desktop Hybrid NVR	**0TB**	-	-		
	2TB	2TB	Linux Native	XFS	/mediadb
	4TB	4TB	Linux Native	XFS	/mediadb
VideoEdge Desktop NVR	**0TB**	-	Linux Native		
	2TB	2TB	Linux Native	XFS	/mediadb
	4TB	4TB	Linux Native	XFS	/mediadb
VideoEdge 2U Hybrid NVR (RAID)	**18TB**	13.6TB	Linux Native	XFS	/mediadb
VideoEdge 2U Hybrid NVR (Non-RAID)	**0TB**				
	3TB	3TB	Linux Native	XFS	/mediadb
	6TB	3TB	Linux Native	XFS	/mediadb
		3TB	Linux Native	XFS	/mediadb1
	12TB	3TB	Linux Native	XFS	/mediadb
		3TB	Linux Native	XFS	/mediadb1
		3TB	Linux Native	XFS	/mediadb2
		3TB	Linux Native	XFS	/mediadb3
VideoEdge 2U NVR (RAID)	**16TB**	11TB	Linux Native	XFS	/mediadb
	24TB	18.5TB	Linux Native	XFS	/mediadb
VideoEdge 2U NVR (Non-RAID)	**0TB**				
	8TB	4TB	Linux Native	XFS	/mediadb
		4TB	Linux Native	XFS	/mediadb1
VideoEdge 3U Hybrid NVR (RAID)	**18TB**	13.6TB	Linux Native	XFS	/mediadb

VideoEdge 3U Hybrid NVR (Non-RAID)	**0TB**				
	3TB	3TB	Linux Native	XFS	/mediadb
	6TB	3TB	Linux Native	XFS	/mediadb
		3TB	Linux Native	XFS	/mediadb1
	12TB	3TB	Linux Native	XFS	/mediadb
		3TB	Linux Native	XFS	/mediadb1
		3TB	Linux Native	XFS	/mediadb2
		3TB	Linux Native	XFS	/mediadb3

The setup process consists of:

1 Initial boot up of VideoEdge

2 Run the Setup Wizard and configure at minimum:

  a System Information including Location and Current Date/Time.

3 Restart NVR Services

Procedure 13
Setting up the VideoEdge NVR

Step	Action

1 Power on the VideoEdge.

VideoEdge boots to the VideoEdge OS login window.

2 Login to VideoEdge.

  a Enter **VideoEdge** in the Username field.

  b Click **Log In**.

  c Enter **VideoEdge** in the Password field.

  d Click **Log In**.

3 Run the VideoEdge Setup Wizard.

Refer to the VideoEdge Setup Wizard section above for further information.

- End -

Using the Administration Interface

Overview

The Administration Interface allows users to interact with VideoEdge. This provides information about the server and allows you to modify its settings. The interface is accessible via a web browser, through victor unified client or locally on your hardware.

A remote workstation logging into VideoEdge using the Administration Interface must have Java 6 or above installed. If the workstation is connected to the Internet, but does not have Java installed, you must download Java from its website http://www.java.com. You must also enable javascript on your browser.

To access VideoEdge through victor unified client, you must add the VideoEdge Recorder to your recorders in the device list in victor unified client. For information on how to add a VideoEdge recorder to victor refer to Setting Up Recorder Devices in the victor Configuration and User Guide.

Logging into the Administrator Interface via a Web Browser

To access the Administrator Interface you must log in. Two of the default users have permission to do this; **System Administrator** and **Operator**.

If you log in using a **System Administrator** account you will have access to configure and edit all settings of VideoEdge. If you log in using an **Operator** account, you do not have permissions to edit any of the settings, you can only view the current settings and view live video.

Procedure 14
Logging into the Administrator Interface via a Web Browser

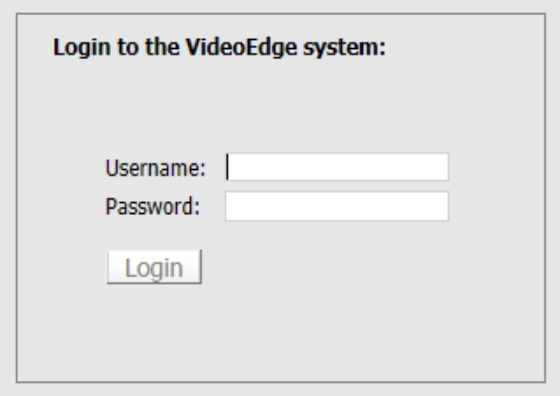
The Administration Interface supports the following web browsers:

- Microsoft Internet Explorer (9+)
- Google Chrome (latest version)
- Mozilla Firefox (latest version)

Step	Action
1	Launch your web browser and enter the VideoEdge IP address into the **URL** field. Enter **http://NVR_Server_IP_Address**, where **NVR_Server_IP_Address** is the IP address of the machine running the NVR software, for example, **http://192.187.100.21**
2	The login dialog box opens. Enter your **User name** and **Password**. User name: **admin** Default Password: **admin** Or User name: **operator** Default Password: **operator** **Note:** 1. You are asked to login/authenticate when you: - First log on to the Administrator Interface.

- Are already logged on and your user access is changed.
2. If you change your account password, use the new password in place of the default password.

Figure 11 Login Dialog



3 Click **Login**.

The Administration Interface opens.

- End -

Accessing the Administration Interface using victor

To access the victor Administration Interface you must have the VideoEdge added as a recorder in the device list on your victor unified client. For information on how to add the VideoEdge recorder to victor refer to the victor Configuration and User Guide.

By accessing the Administration Interface through victor you can configure your VideoEdge in exactly the same way as via the web browser access. However, when using victor you do not have the option to view live video. Instead use the **Surveillance** pane in the victor unified client to view cameras in live mode.

Procedure 15
Accessing the Administration Interface using victor

Step	Action
1	In the victor unified client, select **Devices**, then expand the **Recorders** menu.
2	Expand the **VideoEdge** folder.
3	Right-click on the VideoEdge recorder that you want to configure.

Figure 12 victor NVR Configure option

4	Select **Configure**. The Administration Interface opens.

- End -

Navigating the Administration Interface

Figure 13 Administration Interface

To navigate the Interface and access the required configuration settings, use the menu and sub menus listed on the left of the page.

The menu is divided into several main areas:

- **Live Video** (web only)
- **Devices**
- **Storage**
- **Archive**
- **System**
- **Network**
- **Advanced**
- **Monitor Outputs**
- **Logout** (web only)

Each menu is further divided into sub menus for easy navigation to the required configuration settings.

Logout

Use this menu item to log out of the NVR Administration Interface.

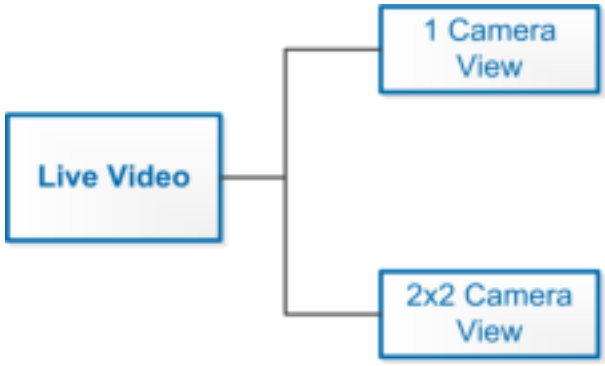
Procedure 16
Navigating the NVR Interface

Step	Action
1	Select the required menu item from the main menu on the left-hand side of the page. The selected menu item expands to display a sub menu list of items. **Note:** Live Video menu option is not available when browsing directly on VideoEdge NVR's server browser interface and is only available when connected from a remote system browser.
2	Select the required item from the sub menu list. The relevant configuration settings are displayed in the main pane of the window.
3	(Optional) Select the tabs at the top of the main pane to navigate between pages.

- End -

Once the VideoEdge has been configured you can view live video streams. You can view live video using the Live Video menu when remotely accessing the Administration Interface.

Figure 14 Live Video Menu Map



Note:
If you access the Administration Interface via victor unified client or locally from the VideoEdge, the Live Video menu item is not available. Use the Surveillance window in victor Client or the VideoEdge Client to view live video.

Live Video

The camera views on VideoEdge can display up to a maximum of 4 live video streams. You can also view Virtual camera streams from the Live Video menu. A live audio stream is not available on the Administration Interface. To listen to audio use victor unified client or VideoEdge Client.

You must have your storage and cameras configured before you can view live video.

Figure 15 Live Video View

Number	Description
1	Recording Mode - Displays the recording mode for the selected camera.
2	Camera dropdown list - Select the camera to display in the viewing window.
3	Setup - Use to edit settings for the selected camera
4	Camera viewing window

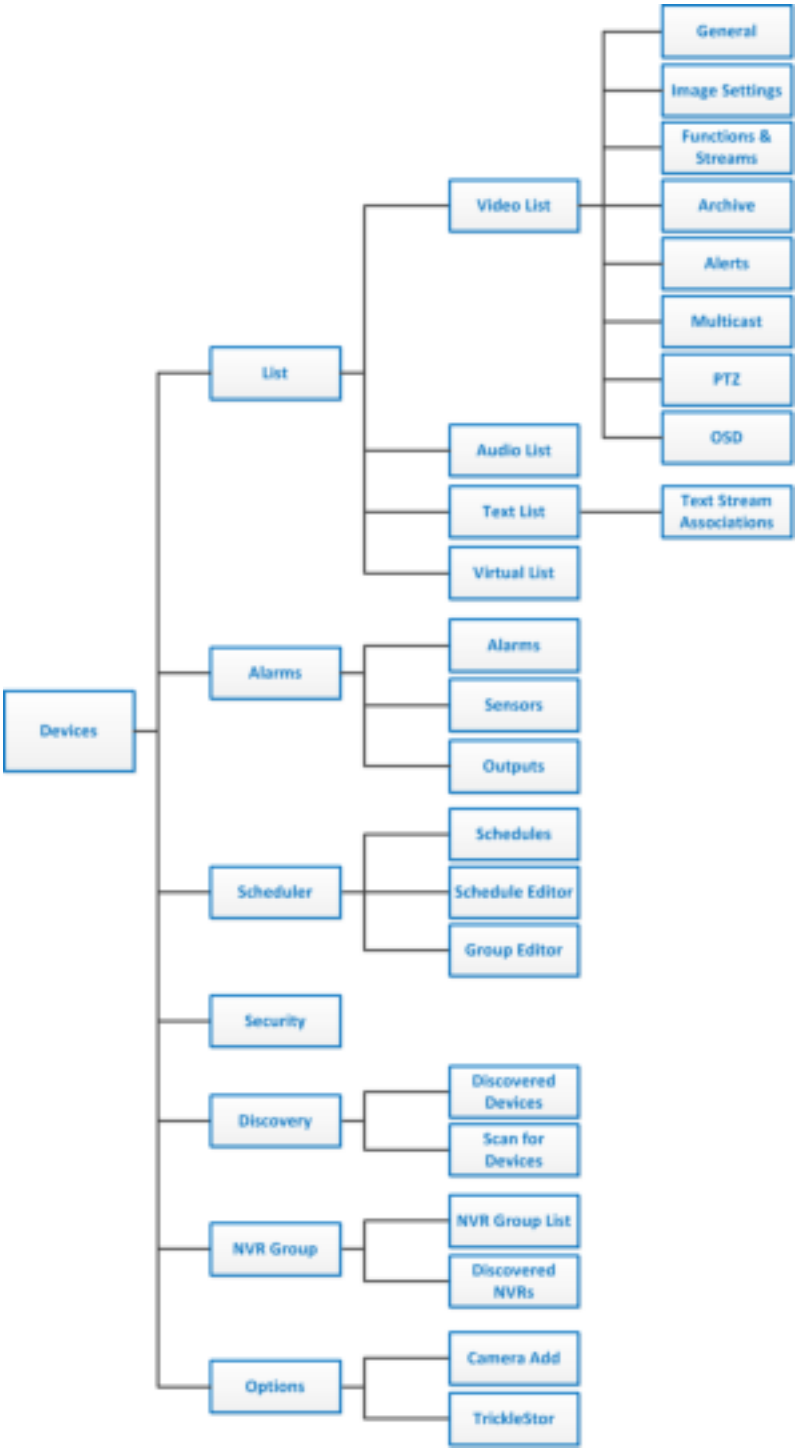
Procedure 17
Viewing Live Video

Step	Action
1	Select **Live Video** from the main menu.
2	Select the **1 Camera View** tab. Or Select the **2x2 Camera View** tab.
3	Select the cameras that you want to view from the **Select camera to view** dropdown. The camera's live video stream appears in the viewing window. **Note:** Click  to navigate to the camera's advanced configuration menu.

- End -

Cameras, audio devices and text devices are added and configured using the **Devices** menu of the Administration Interface.

Figure 16 Device List Menu Map



- **List** - From here you can view a list of all devices connected to VideoEdge and view a summary of their configuration status. You can add and remove devices or edit/batch edit cameras configuration settings.
- **Alarms** - You can create camera alarms, these may be for specific regions of a cameras view. You can also select different types of alarm trigger, for example Motion Detection or Video Intelligence. You can also add Sensors and Outputs to VideoEdge.
- **Scheduler** - The scheduler allows you to specify the recording mode (including no recording) that is active at scheduled times during the day.
- **Security** - The security page allows you to create and maintain camera password groups.
- **Discovery** - This section allows you to use auto-discovery to add cameras to VideoEdge.
- **NVR Group** - This section allows you to configure NVR groups for remote transcoding and failover.
- **Options** - This section allows you to enable Camera Add and TrickleStor settings.

List

The **List** section provides a summary of all devices connected to VideoEdge and outlines configuration settings that are available to view and edit. It is separated into four tabs displaying a list of all cameras, audio devices, text devices and virtual devices.

Viewing the Device List

The device list provides a snapshot of the basic settings available on VideoEdge for all camera, audio and text devices depending on the tab selected.

Procedure 18
Viewing the Device List

Step	Action
1	Select the **Devices** menu.
2	Select **List**. The Video List displays.
3	(Optional) To view a different device list, select one of the following options: • (Optional) Select the **Audio List** tab to view the Audio List. • (Optional) Select the **Text List** tab to view the Text List. • (Optional) Select the **Virtual List** tab to view the Virtual List.

- End -

Sorting the Device List

The device list can be sorted alphanumerically by a selected column in ascending or descending order.

Procedure 19
Sorting the Device Lists

Step	Action
1	Select the **Devices** menu.
2	Select **List**. The Video List displays.
3	(Optional) To view a different device list, select one of the following options: • (Optional) Select the **Audio List** tab to view the Audio List. • (Optional) Select the **Text List** tab to view the Text List. • (Optional) Select the **Virtual List** tab to view the Virtual List.
4	Select the column header from the device list table that you want to sort by. The list is sorted in alphanumeric order.
5	Sort in ascending or descending order: a Select  to sort in ascending order.

b Select to sort in descending order.

- End -

Filtering the Device List

The device list has a Filter feature which can be used to display specific device records. The filter feature will look at the criteria entered and compare this against all fields in the device list.

Procedure 20
Filtering the Device Lists

Step	Action
1	Select the **Devices** menu.
2	Select **List**. The Video List page displays.
3	(Optional) To view a different device list, select one of the following options: • (Optional) Select the **Audio List** tab to view the Audio List. • (Optional) Select the **Text List** tab to view the Text List. • (Optional) Select the **Virtual List** tab to view the Virtual List.
4	Enter the filter criteria into the **Filter** field. The device list is filtered to display only devices that meet the criteria entered. **Note:** The device list will filter as you type the criteria into the **Filter** field. As the criteria gets more specific the list filters accordingly.
5	(Optional - Video List only) Select to show only cameras that have errors. **Note:** • This icon only appears if the Video list contains cameras that have errors. When you select , it changes to • Select to show all cameras in the Video list.

- End -

Video List

The Video List tab displays the cameras which have been added to VideoEdge. Devices can be added, edited, removed and batch edited. Advanced settings can also be configured.

The table below provides a description of each field displayed.

Figure 17 Video List

Table 3 Video List Summary Table

Field	Description
1. No	Device slot number.
2. Name and IP Address	Device name as given when adding the device to VideoEdge. Device IP address.
3. Device Information	Device Manufacturer and Model FW: Current Firmware version on the device Communications Type.
4. Rec	Displays the device recording state. There are four available options to select: • Recording Off • Recording Always • Only Record on Alarm • Recording Always With Alarm On If the scheduler is enabled, you cannot change the device recording state and the icon, is displayed in the field.

Field	Description
5. Arch	Indicates if archiving is enabled for the device. The archiving options available are: •  Archiving Disabled •  Archive all video •  Archive only alarm video
6. Analytics	Indicates if analytics are set on the device. The analytic options are: •  Analytics Off •  Motion Detection •  Video Intelligence (This encompasses object detection, direction, linger, enter, exit and abandoned/removed). •  Edge Based
7. Associations	Indicates the device's associations, hover the cursor to display information. The following devices can be associated: •  Video •  Audio •  Text
8. Stream configuration settings	Displays the camera's stream configuration settings. Depending on the camera model, the camera may have up to three video streams. • Live - Indicates that this stream will be used for live streaming. • Alarm - Indicates that this stream will be used for any alarms that are recorded. • Rec - Indicates that this stream will be used for non-alarm recording. • Analytics - Indicates that this stream will be used for executing analytics (motion detection or video intelligence). **Note** If an alarm is raised for motion detection, the alarm stream is used to record the alarm. • Codec - The camera codec. • FPS - The camera FPS. • Resolution - The camera resolution.

Adding Devices

You can add cameras to VideoEdge from the **Video List** tab. You can add devices manually, or you can add devices from a CSV file.

Manually Adding Analog Devices

To add an analog device to VideoEdge you must connect the device directly to a port on the unit.

The analog device ports must be opened on VideoEdge by adding a device on the Device List page using the IP address, **127.0.0.1**. Once a device with this IP address is added to VideoEdge, all analog ports are opened and all devices are displayed in the Device List.

When the connection has been established between VideoEdge and the analog ports on the unit, all devices will always display on the Device List even if a device is physically disconnected from the unit.

You can ensure all cameras are connected by viewing the camera's live video in the Live Video window. If no picture is displayed for an analog camera, the camera needs to be connected to a port on the unit.

The default recording mode for analog cameras when connected to VideoEdge is Recording Off.

Note:
If you remove an analog device from the NVR you can re-add it manually using the IP address **127.0.0.1**, this will add all inputs which are not currently in the Device List. Alternatively if you un-check the **Add All Inputs on Device** checkbox you can select the inputs you want to add. This behavior is the same for all multichannel devices.

Procedure 21
Manually Adding Analog Devices

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**. The Video List page displays.
3	Click 
4	Enter a **Device Name**. **Note:** 1. All devices added as part of a multichannel encoder are named using the following conventions; - Video inputs are given a "_n" suffix, for example ***Analog_1*** and so on. - Audio inputs are given a "_n_audio" suffix for example ***Analog_2_audio***. 2. In these examples, ***Analog*** is the user defined device name. Each device can be renamed once they have been added to the NVR.
5	Enter **127.0.0.1** into the **Device IP Address** field.
6	Select the required **Security Group** from the **Security Group** dropdown.
7	Select an option from the **Auto-Configure Streams** list. • **None**: Disables the Auto Configure streams function. • **1 Additional Live Stream**: Configure one additional stream • **2 Additional Live Streams**: Configure two additional streams. This option is only available for cameras that support three streams.

8 (Optional) De-select the **Add All Inputs on Device** checkbox if you do not want to add all inputs on a device.

9 (Optional) De-select the **Default Associations** checkbox if you want to define custom associations after the devices have been added.

10 (Optional) De-select the **Enable Smart Search (Motion Metadata)** checkbox to disable Smart Search for any cameras that you add manually.

11 (Optional) Select the **Enable ONVIF** checkbox to prioritize ONVIF communication between the VideoEdge and the camera.

Note:
Before you can select this option, you must enable ONVIF from the **Options** menu.

12 Click 

If the **Default Associations** checkbox is unselected a window will open displaying the available inputs. For video devices a snapshot can be displayed.

All analog ports available on the unit are opened and all devices that are connected to VideoEdge are displayed in the Device List.

- End -

Manually Adding an IP Device

When you manually add a device to VideoEdge the default recording mode is set to "Recording Always". When you add a camera were the configuration does not support Smart Search (using either a primary or secondary stream) then the default recording mode will be "Record Always".

Note:
VideoEdge is by default configured to attempt communicating with the camera using the cameras own native commands. Using native camera handlers provides the maximum number of camera features available. If VideoEdge does not support your camera brand, it will then attempt to use the general ONVIF communications protocol to communicate with the camera. If the camera supports ONVIF you will be able to access one or more of the camera features (for example; video, audio, PTZ, dry contact events). You can determine which communication method has been employed by the NVR from the device list.

When you add an encoder to VideoEdge, all cameras associated with this encoder will have the same IP address. As a result, these cameras must be assigned to the same password group and have the same dry contact settings. If you edit either the password group or the dry contact settings for one camera associated with the encoder, these settings will be updated for all cameras.

Multicast cameras

In addition to traditional unicast IP cameras, you can add multicast cameras to your VideoEdge. Multicast camera streams can be recorded to multiple recorders simultaneously. To use multicast streaming with VideoEdge, you must select the Multicast option when you add a camera to VideoEdge.

Note:
You cannot enable multicast streaming after you add a camera. You must delete the camera, and then select the multicast streaming option when you re-add the camera.

Requirements

- A VideoEdge can include a mixture of unicast and multicast cameras

- A camera's streams must all be unicast or multicast
- Multicast streams do not currently support audio recording.

Procedure 22
Manually Adding an IP Device

Step	Action
1	Select the **Devices** menu.
2	Select **List**. The Video List page displays.
3	Click 
4	Enter the **Device Name**.
5	Enter the **Device IP Address** of the device.
6	Select the **Security Group** from the Security Group dropdown. **Note:** The **Security Group** will usually be set by default. VideoEdge will use the manufacturer's default password to connect to the camera. However, if you have changed the password for this camera, you need to assign the camera to the appropriate password group, or create a new password group.
7	Select an option from the **Auto-Configure Streams** list. • **None**: Disables the Auto Configure streams function. • **1 Additional Live Stream**: Configure one additional stream. • **2 Additional Live Streams**: Configure two additional streams. This option is only available for cameras that support three streams.
8	(Optional) De-select the **Add All Inputs on Device** checkbox if you do not want to add all inputs on a device.
9	(Optional) De-select the **Default Associations** checkbox if you want to define custom associations after the devices have been added.
10	(Optional) De-select the **Enable Smart Search (Motion Metadata)** checkbox to disable Smart Search for any cameras that you add manually.
11	(Optional) Select the **Enable ONVIF** checkbox to prioritize ONVIF communication between the VideoEdge and the camera. **Note:** Before you can select this option, you must enable ONVIF from the **Options** menu.
12	(Optional) Select the **Use Multicast Streaming** checkbox to use the camera's multicast stream to record footage.
13	Click  If the Default Associations checkbox is unselected a window will open displaying the available inputs. For video devices a snapshot can be displayed. The device is added to the device list.

14	Configure the device settings as required.

Note:
Devices can also be added to VideoEdge using Discovery. For further information refer to Discovery.

- End -

Adding Devices from a CSV file

To add multiple devices to VideoEdge simultaneously, you can import the device information from a CSV file.

The CSV file meet the following requirements:

- The CSV file must contain the following information for each device:
  - **Device name** - Name of the device
  - **Device IP** - IP address of the device
  - **Security Group** - An integer to identify a security group. Default value: 0
  - **Default Associations** - Enable or disable default device associations. Valid values: TRUE or FALSE.
  - **Enable ONVIF** - Enable or disable ONVIF. Valid values: TRUE or FALSE.

Note:
You must enable ONVIF from the options menu before you can enable ONVIF for a camera.

  - **Enable Smart Search** - Enable or disable Smart Search. Valid values: TRUE or FALSE.

Note:
To enable Smart Search you must also enable Smart Search from the General menu.

  - **Storage Set** - An integer that identifies a storage set. You can have a maximum of five security groups. Valid values: 0, 1, 2, 3, or 4
  - **Auto-Configure streams** - Enable or disable the Auto Configure streams feature. Valid values: 0,1, or 2.
- Multi-channel devices should only be added to the file once. All available channels are added automatically.

Procedure 23
Adding Devices from a CSV file

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**.
3	Select 
4	Select **Choose File**.
5	Navigate to the required file, then click **Open**.
6	Click **Add Devices**.

Note:
The CSV file must be valid for the device import to complete successfully. A validation overview shows any errors that are detected in the file.

- End -

Edit a Camera Name

You can update the name given to a camera as required.

Procedure 24
Editing a Camera Name

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**. The Video List page displays.
3	Click  in the camera row where you want to change the camera name.
4	Select the **Name** field and enter the new camera name. Or Click  in the camera row where you want to change the camera name, select the **General** tab and enter the new camera name into the **Video Name** field.
5	Click 

- End -

Procedure 25
Editing Basic Video Settings

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**. The Video List page displays.
3	Select  in the camera row for which you want to edit a video list setting. The fields available to update are ready to edit.
4	Make the required changes to: • **Name** - Use this field to update the name of the camera. • **Rec** - Use this to update the camera recording state. You can choose,  Recording Off,  Recording Always,  Only Record on Alarm, or  Recording Always With Alarm On.

Note:
To update a camera's recording state you must ensure the device recording scheduler is disabled.

- **Stream 1** / **Stream 2** / **Stream 3** settings. If the camera supports two or three streams, use these settings to select which stream to use for:
    - Live video
    - Alarms
    - Recording.

  You can assign each of these to Stream 1, Stream 2, or Stream 3 as required.

  You can also adjust the **Codec**, **FPS** and stream **Resolution** settings for each stream.

5 Click 

- End -

Removing a Device

You can remove a device from the NVR if necessary. Once you remove a device from the NVR, you will no longer be able to view live video, record media or access the device via a client.

Procedure 26
Removing a Device

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**. The Video List page opens.
3	Select the checkbox of the device(s) you want to remove.
4	Click  If you are removing a camera which has an associated audio device a dialog box opens.
5	Click **Yes** to remove the associated audio device. Or Click **No** to keep the associated audio device. A dialog box opens for confirmation that you want to remove the device(s).
6	Click **Yes** to remove the device(s). The device(s) are removed from the NVR.

- End -

Batch Camera Configuration

Some camera settings can be batch edited. The Batch Edit tab lists the cameras currently being edited in the left pane, and the setting adjustments are made in the right pane. When a change is made to a setting, the checkbox next to the setting is checked. If you deselect the checkbox, the adjustment will not be applied. When you click apply, the changes being made are previewed, with the new settings highlighted in yellow.

Note:
You cannot batch edit two-stream and three-stream cameras together. If your VideoEdge includes two-stream and three-stream cameras, you must batch edit them in separate groups.

Procedure 27
Batch Editing Camera Settings

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**.
3	Select the checkbox for each camera you want to batch edit.
4	Click  The Batch Edit tab displays.
5	Adjust the device settings:

a **Name** - Use this field to update the name of the cameras.

Note:
When you update the name of devices using batch edit, each device will have a number appended to its name. For example, **CameraName_1**, **CameraName_2**, etc.

b **Maximum Recording Storage Period** - Select from the dropdown to set the maximum duration over which media recorded for these devices will be saved without being deleted.

c **Storage Set** - Select from the dropdown which storage set the batch of devices will record to.

d **Recording Mode** - Use this to set the recording mode for these cameras. You can choose,  Recording Off,  Recording Always,  Only Record on Alarm, or  Recording Always With Alarm On.

e **Archiving Mode** - Use to set the archiving mode for these cameras. You can choose,  Archiving disabled,  Archive all videos or  Archive only alarm video.

f **Archiving Quality** - Archiving Quality is defined as a percentage of applied frame rate decimation. Archiving quality is applied in 10% intervals where 10% provides the lowest quality video and 100% provides the highest quality video for archiving.

g **Maximum Archiving Storage Period** - Select from the dropdown if an archiving storage period is Enabled or Disabled.

h **Video Analysis** - Select from the dropdown which type of analytics to apply to this batch of cameras: Motion detection, Video Intelligence, Edge Based, Face Recognition, or License Plate Recognition.

Note:
When you select an analytic, additional device settings may appear.
• Video Intelligence: Minimum object width, Minimum object height, Compensate for camera motion.
• Face Recognition: Minimum face size, Face Detection Sensitivity, Face Recognition Sensitivity, Face Search Alert, Face Verification.
• License Plate Recognition: LPR Sensitivity, Choose Countries or States.

i **Associate Audio** - Use to associate an audio device with the selected cameras.

j **Device Replacement** - Use to assign a replacement camera/encoder if the selected device has failed.

k **Video Streaming** - Enable/Disable video streaming for all selected devices.

l **Connection Protocol** - Select a camera connection protocol for all selected devices: UDP or TCP.

m **Auto-Configure Streams** - Enable/Disable auto-configuring of streams. You can enable auto-configuration for one or two streams.

n **Max GOP** - Enter the maximum GOP value for the selected cameras (Min 1, Max 1023).

Note:
• This setting only affects H264 and H264+ camera streams.
• For H264+ streams, the GOP size varies dynamically, but it cannot exceed the Max GOP value.

o **PTZ** - Enable/Disable PTZ for all selected (applicable) devices. Virtual PTZ will be unaffected.

p **Gaming Mode** - Enable/Disable Gaming Mode for all selected and supported cameras. Enabling Gaming Mode maintains a constant frame rate for all affected cameras.

q **Intelligent Guard Tour** - Enable/Disable Intelligent Guard Tour for all selected and supported cameras.

r **Stream Configurations**

- Set each stream to **Live**, **Alarm** or **Record**
- Set the stream configurations for **Codec**, **FPS**, **Resolution Quality**, **Bit Rate Control**, **Bit Rate**, **Max Bit Rate** and **Profile** in the respective dropdowns.

Note:
When you select a value for the **Codec**, **FPS**, **Resolution**, **Quality**, **Bit Rate Control**, **Bit Rate**, **Max Bit Rate** and **Profile** fields, each dropdown contains the available options followed by a number in brackets. This number appears after you select a value for the Codec, and it represents the number of cameras that support the setting over of the total number of cameras being edited. It is possible that some dropdowns will be empty if the parameter is not supported for that codec on any camera.

6 Select 

A Confirm Changes window opens with a preview of the changes being made to the selected cameras.

7 Select 

Note:

If you do not want to make these changes to all cameras, select  and update the settings as required.

8 A message box opens to confirm the changes were successful. Click **OK**.

Note:
If some of the changes are not successful, a summary page of failed updates opens with the failures highlighted in red. By hovering over  you can view more detailed error information. Click **OK** to continue.

- End -

Audio List

Audio devices which are connected to the NVR, an encoder or part of a camera can be added to the NVR using the Administration Interface. By default an audio source that is physically built into a camera will be associated with that camera. You can de-couple the audio input when you add the device manually or using Auto Discovery. The association can also be removed at any stage using the device list.

The Audio List displays the audio devices which have been added to the NVR. Table 1-3 provides a description of each field displayed.

Figure 18 Audio List

Table 4 Audio List Summary Table

Field	Description
1. No	Device slot number.
2. Name and IP Address	Device name as given when adding the device to the NVR. Device IP address.
3. Device Information	Device Manufacturer and Model. FW: Current Firmware version on the device.
4. Enabled	Indicates is audio stream is enabled/disabled
5. Rec	Displays the device recording state. There are four available options to select: • Recording Off • Recording Always • Only Record on Alarm • Recording Always With Alarm On If the scheduler is enabled, you cannot change the device recording state and the icon, is displayed in the field.2

Field	Description
6. Associations	Indicates the device's associations, hover the cursor to display information. The following devices can be associated: • Video • Text
7. Codec	The audio codec.
8. Volume	The current volume.
9. Bitrate	The current bitrate.

Procedure 28
Editing Audio Settings

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**. The Video List page displays.
3	Select the **Audio List** tab.
4	Select in the audio record for which you want to edit an audio list setting. The fields that you can update are ready to edit.
5	Make the required changes to: • **Name** - Use this field to update the name of the audio device. • **Enabled** - Use the Enabled dropdown to enable or disable audio. • **IP Address** - Use this field to update the IP address of the audio device. • **Rec** - Use this to update the camera recording state. You can choose, Recording Off or Recording Always. **Note:** To update an audio device's recording state you must ensure the device recording scheduler is disabled. • **Codec** - Use the dropdown to select the codec when available. **Note:** The supported codec for analog channels is G711mulaw. • **Volume** • **Bitrate** - Use the dropdown to select the bitrate when available. **Note:** The supported audio bit rate for analog channels is 8000.

6 Click 

- End -

Text List

Text devices can be added to the NVR either via serial or IP connections. Text devices provide a text based search ability when associated with camera and audio devices; for example a compatible cash register can be added to the NVR which will record the text data received from the register. Cameras and audio devices in the vicinity of the cash register can then be associated with it, when you perform a text based search using the VideoEdge Client, associated video and audio will be returned which was recorded at the time the text data was received.

The Text List displays the serial and IP text devices which have been added to the NVR. Table 1-4 provides a description of each field displayed.

Figure 19 Text List

Table 5 Text List Summary Table

Field	Description
1. No	Device slot number.
2. Stream Name	Device name as given when adding the device to the NVR.
3. Comms Type	Indicates Communication type in use.
4. Associations	Indicates the devices associations, hover the cursor to display information. The following devices can be associated: • Video • Audio
5. Description	Indicates configured settings.

Configuring Port Settings Prior to Adding a Serial Text Stream Device

Prior to adding a Serial Text Stream device you should ensure it is connected to one of the NVR's USB ports or its RS232 Serial port. Once connected you are required to configure that Serial Port's communication protocol for Text Stream use.

Procedure 29
Configuring Serial Port Settings for a Serial Text Stream Device

Step	Action
1	Select the **Advanced** menu.
2	Select **Serial Ports**. The Serial Ports page displays.
3	Select  next to the Serial Port you want to edit. The Port Settings dialog box opens.
4	Select **Text Stream** from the **Protocol** dropdown. The following default settings are applied: • **Baud Rate** - 4800 • **Data Bits** - 8 • **Parity** - None • **Stop Bits** - 1 • **Flow Control** - None
5	Click 

- End -

Manually Adding a Text Stream Device

Text Stream devices can be connected via serial or IP communications, using the Text list tab.

Procedure 30
Manually Adding Text Stream Devices

Step	Action
1	Select the **Devices** menu.
2	Select **List**. The Video List page displays.
3	Select the **Text List** tab.
4	Click 
5	Enter a **Text Stream Name**.
6	Select the **Connection Type** from the dropdown.
7	Select the **Encoding Type** from the dropdown. **Note:** If connecting to an ASCII-encoded Text Stream device, select **Windows-1252**. If connecting to a UTF-encoded Text Stream device, select **UTF-16**.
8	Enter the **Line Delimiter** or click **Default** to use the default value.

Note:
If the Line Delimiter does not properly match what is used in the Text Stream then text may be lost or improperly stored in the media database.

9 (IP Only) Enter the **Port**.

Note:
The port number must match the port number assigned on the Text Stream device.

Or

(Serial Only) Select the option button of the **Serial Device** you want to use.

10 (Optional - Serial Only) Select to edit the serial device settings:

a Enter the **Com Port**.

b Enter the **Protocol**.

c Select the **Baud Rate** from the dropdown.

d Select the **Data Bits** from the dropdown.

e Select the **Parity** from the dropdown.

f Select the **Stop Bits** from the dropdown.

g Select the **Flow Control** from the dropdown.

h Click

11 Click

- End -

Procedure 31
Editing Text Settings

Step	Action

1 Select **Devices** from the main menu.

2 Select **List**.

The Video List page displays.

3 Select the **Text List** tab.

4 Select in the text record for which you want to edit a text list setting.

The fields that you can update are ready to edit.

5 Make the required changes to:

- **Text Stream Name** - Use this field to update the name of the Text device.
- **Connection Type** - For information only when device is added.
- **Encoding Type** - Use this dropdown menu to select the character encoding format for the Text Stream device.
- **Line Delimiter** - Use this field to update the Line Delimiter value.
- **Port** - For information only when device is added.

6	Click 

- End -

Adding Rules and Markers

Rules are text matching instructions that can be used to define real-time Text Stream alarms using the NVR Administration Interface, or to search recorded Text Streams after-the-fact using VideoEdge Client. For example, you can use a Rule to trigger an alarm whenever the string "VOID" is detected in the stream, or you can use a Rule to search for any time a particular field is greater than $20.00.

Markers are strings that identify the beginning of a new message in the Text Stream. For example, if your Text Stream contains a stream of receipts from a POS system, you can use a Marker to identify each new receipt that comes in the stream. If your receipts always have "Store 15" printed at the top, then use this as a Marker in the stream. When "Store 15" appears in the Text Stream, all the subsequent text until the next "Store 15" is seen will be stored and displayed together as a single message.

Procedure 32
Adding a Rule to a Text Device

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**. The Video List tab displays.
3	Select the **Text List** tab.
4	Select the checkbox of the Text device you want to create a rule for.
5	Click  The Rules/Markers tab displays.
6	Click  The Rule Definition Window opens.
7	Enter the **Name**.
8	Enter a match in the **Match with** field.
9	Select the **Search Direction** from the dropdown. Forward by default.
10	Select the number of words from the **Jump N Results** dropdown, to skip after a match is found, to find the associated value. Default = 0.
11	Select one of the following **Criteria** from the dropdown: • **found** - Any results found. • **string** - A series of characters in Value 1 field. • **less than** - Less than Value 1. • **greater than** - Greater than Value 1. • **equal to** - Equal to Value 1 • **range** - Values between Value 1 and 2.

12	Enter a value in the **Value1** field. This is required when using string, less than, greater than, equal to and range Criteria.
13	Enter a value in the **Value2** field. This is required when using range criteria.
14	Click 

- End -

Procedure 33
Editing a Rule

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**. The Video List tab displays.
3	Select the **Text List** tab.
4	Select the checkbox of the Text device you want to edit a rule for.
5	Click  The Rules/Markers tab displays.
6	Select the checkbox of the Rule you want to edit.
7	Select  The Rule Definition Window opens.
8	Edit the match in the **Match with** field.
9	Select the **Search Direction** from the dropdown.
10	Select the number of words from the **Jump N Results** dropdown. Or From the **Jump N Results** dropdown, select To last entry of line to skip a variable number of entries between the last match and the text value in a receipt.
11	Select the **Criteria** from the dropdown:
12	Edit the value in the **Value1** field. This is required when using string, less than, greater than, equal to and range criteria.
13	Edit the value in the **Value2** field. This is required when using range criteria.
14	Click 

- End -

Procedure 34
Add a Marker to a Text Device

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**.

The Video List opens.

3 Select the **Text List** tab.

4 Select the checkbox of the Text device you want to create a marker for.

5 Click 

The Rules/Markers page opens.

6 Click 

The Marker Definitions Window opens.

7 Enter the marker **Name**.

8 Enter the **Beginning Marker**.

9 Click 

- End -

Procedure 35
Edit a Marker

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**. The Video List opens.
3	Select the **Text List** tab.
4	Select the checkbox of the Text device you want to edit a marker for.
5	Click  The Rules/Markers page opens.
6	Select the checkbox of the Marker you want to edit.
7	Select  The Marker Definitions Window Opens.
8	Edit the **Beginning Marker**.
9	Click 

- End -

Procedure 36
Removing a Rule or Marker from a Text Device

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**.

The Video List opens.

3 Select the **Text List** tab.

4 Select the checkbox of the Text device you want to remove a rule/marker from.

5 Click 

The Rules/Markers page opens.

6 Select the checkbox of the rule/marker you want to remove.

7 Click 

- End -

Grouping Rules

Rules can be grouped together using the Group Rules checkbox, for both Text Stream alarms and searches. Grouping rules creates an 'AND' logic so that all the grouped rules must be satisfied. When the Group Rules checkbox is selected, it applies to all rules that have been added to the alarm or search definition. Rules that have been disabled will not need to be satisfied.

Note:
When the Group Rules checkbox is applied the individual rules will not display in the Alarm Rule dropdown of an events form in the VideoEdge Client. The only selectable option available will be 'All'.

Procedure 37
Grouping Rules

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**. The Video List opens.
3	Select the **Text List** tab.
4	Select the checkbox of the Text device for which you want to group rules.
5	Click  The Rules/Markers page opens.
6	Select the **Group Rules** checkbox.

- End -

Advanced Text Device Configuration

Advanced Text Device Configuration includes creating video and audio associations with text stream devices and creating of Rules and Markers.

Creating Associations for Text Devices

Text devices can be associated with multiple cameras and audio devices.

Procedure 38
Associating Cameras and Audio Devices with Text Devices

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**. The Video List opens.
3	Select the **Text List** tab.
4	Click  in the text record for which you want to edit a text list setting. The Text Edit tab displays.
5	Select the checkboxes for the video and audio devices you want to associate with the text device.
6	Use the arrow right button  to move the selected devices to the Association list(s).
7	Click 

- End -

Procedure 39
Removing Associations from Text Devices

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**. The Video List opens.
3	Select the **Text List** tab.
4	Click  in the text record for which you want to edit a text list setting. The Text Edit tab opens.
5	Select the checkboxes for the video and audio devices you no longer want to be associated with the text device.
6	Use the arrow left button  to remove the selected devices from the Association list(s).
7	Click 

- End -

Virtual List

From the Virtual List page, you can create virtual streams. A virtual stream is a multi-view layout of multiple camera feeds, combined into a single stream. Combining multiple video feeds reduces the resources needed to display a multi-view video stream. Display of virtual streams is supported for live viewing, through the VideoEdge Live Video page, and through victor Web LT.

The following features are not supported for virtual cameras:

- Remote Transcoding

- PTZ
- vPTZ
- Playback of recorded video
- Association of audio
- Clip export

Procedure 40
Creating a Virtual Camera

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**. The Video List opens.
3	Select the **Virtual List** tab.
4	Click 
5	Enter a name for the virtual camera stream
6	Select a layout from the dropdown menu.
7	For each pane in the camera stream layout, select a camera from the dropdown list. **Note:** Virtual cameras do not support duplicate cameras - all camera entries must be unique.
8	Click 

- End -

Procedure 41
Editing a Virtual Camera

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**. The Video List opens.
3	Select the **Virtual List** tab.
4	Select the virtual camera you want to edit. **Note:** You can only edit one virtual camera at a time.
5	Click 

6	(Optional) Edit the virtual camera **Name**.
7	(Optional) Edit the virtual camera **Layout**.
8	(Optional) Edit the camera layout pane(s).
9	Click 

- End -

Procedure 42
Deleting a Virtual Camera

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**.
	The Video List opens.
3	Select the **Virtual List** tab.
4	Select the virtual camera you want to delete.
5	Click 

- End -

VideoEdge Intellex Handler

The Intellex handler is used to add video inputs from an Intellex recorder to your NVR. When you add an Intellex device to your NVR, you can add up to 4 Intellex video channels to your NVR video list.

The following functions are unsupported for devices connected to an Intellex recorder.

- Audio Streaming
- Query Device - Mac address
- PTZ
- Digital PTZ
- Dry Contact
- Reboot Device
- Power-off Device
- Reset Factory Default
- Get Device Log

Procedure 43
Adding Video devices from an Intellex recorder

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**. The Video List page opens.
3	Click 
4	Enter a **Device Name**.
5	Enter the **Device IP Address** of the Intellex recorder you want to add streams from.
6	Select the Security Group from the **Security Group** dropdown.
7	De-select the **Add all Inputs on Device** checkbox. **Note:** You can add a maximum of 4 video channels from Intellex recorders.
8	(Optional) Deselect the **Default Associations** checkbox if you want to define custom associations after the devices have been associated.
9	Click  The Intellex Device list appears.
10	Select the checkbox beside each device you want to add to the **Video List**.
11	Click 

- End -

Editing an Intellex Video Device

Intellex Video Devices can be edited in the same way as other video devices. However, not all functions are supported for Intellex Video Devices.

Note:
Any changes made to an Intellex video device (through the VideoEdge NVR) will not overwrite the device settings on the Intellex NVR.

Procedure 44
Editing Basic Video Settings

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**. The Video List page displays.
3	Select  in the camera row for which you want to edit a video list setting. The fields available to update are ready to edit.

4 Make the required changes to:

- **Name** - Use this field to update the name of the camera.
- **Rec** - Use this to update the camera recording state. You can choose,  Recording Off,  Recording Always,  Only Record on Alarm, or  Recording Always With Alarm On.

Note:
To update a camera's recording state you must ensure the device recording scheduler is disabled.

- **Analytics** - Use this to change the analytic alarm setting. You can select,  Analytics Off,  Motion Detection or  Video Intelligence.
- **Stream1** / **Stream 2** settings. If a second stream is available on the camera, use these settings to select which stream is to be used for:
  - Live video
  - Alarms
  - Recording

You can assign each of these to either Stream 1 or Stream 2 as required.

You can also adjust the **Codec**, **FPS** and stream **Resolution** settings for each stream.

5 Click 

- End -

Removing an Intellex Video Device

You can remove an Intellex video device from the NVR if necessary. Once you remove a device from the NVR, you will no longer be able to view live video, record media or access the device via a client. You can add alternative devices, as long as you keep within the 8-device limit for Intellex video devices.

Procedure 45
Removing an Intellex Device

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**. The Video List page opens.
3	Select the device(s) you want to remove.
4	Click  If you are removing a camera which has an associated audio device a dialog box opens.
5	Click **Yes** to remove the associated audio device. Or Click **No** to keep the associated audio device.

A dialog box opens for confirmation that you want to remove the device(s).

6 Click **Yes** to remove the device(s).

The device(s) are removed from the NVR.

- End -

Advanced Camera Configuration

Several advanced camera configuration settings are available in the following tabs accessed by clicking the Setup icon in the Video List tab for the corresponding camera:

- General
- Image Settings
- Function & Streams
- Archive
- Alerts
- Multicast
- PTZ including Analog Matrix Configuration
- OSD (VideoEdge Hybrid NVRs only)

General

General camera settings that can be easily updated from the General tab which can be accessed by clicking the Setup icon for the required device on the Video List tab.

Note:
The MAC Address, ID Channel and Device Type fields are for information only and are not configurable.

Security Group

If an IP camera is assigned to a security group and you have changed the password for this camera, you will need to select the new security group the camera belongs to.

Procedure 46
Changing the Security Group Assigned to an IP Camera

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**.
3	Click in the camera row that you want to assign to a new password group. The Function & Streams tab displays.
4	Select the **General** tab.
5	Select the new password group from the **Security Group** dropdown.
6	Click

Note:
If you are editing the security group for a camera, forming part of an encoder device, all cameras related to this device will be updated with the new security group. In this instance, a warning message opens informing you that multiple cameras will be updated.

- End -

Storage Set

Changing the storage set a camera is assigned to is only applicable if you have configured the NVR for advanced storage. When you change the storage set, media from the camera will now be stored on media folders in the new storage set. You can also edit the storage set a camera is assigned to by editing the advanced storage settings, refer to Advanced Camera Configuration on page 142.

Procedure 47
Changing a Camera's Storage Set

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**.
3	Click  in the camera row that you want to assign to a new storage set. The Function & Streams page opens.
4	Select the **General** tab.
5	Select the new storage set from the **Storage Set** dropdown.
6	Click 

- End -

Look-Down

Look-down should be enabled if a camera has been mounted on the ceiling pointing down to the floor. This is to facilitate POS analytics. Refer to the victor unified user guide for more information.

Procedure 48
Enable/Disable Camera Look-down

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**.
3	Click  in the camera row that you want to enable/disable look-down for.
4	Select the **General** tab.
5	Select the **Look-down** checkbox to enable look-down. Or Deselect the **Look-down** checkbox to disable look-down.
6	Click 

- End -

Image sensor type

By default, VideoEdge automatically detects a camera's image sensor type. However, if VideoEdge cannot detect the camera's sensor type, you can configure this option manually. For example, if you connect a thermal camera that uses ONVIF communications, VideoEdge may not detect the thermal image sensor.

Procedure 49
Configuring the Image sensor type

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**.
3	Click  in the camera row that you want to set the image sensor type for.
4	Select the **General** tab.
5	Select one of the following options from the **Image sensor type** list. • Autodetect • Visible Light • Thermal

- End -

Camera connection protocol

By default, VideoEdge uses UDP to communicate with cameras. If the UDP connection fails, VideoEdge uses TCP instead. However, if UDP is unsuitable for your network, you can select TCP as the default communication protocol.

Note:
• Selecting TCP may improve camera connection reliability, but may also increase latency in live video surveillance.
• You can configure Camera connection protocol from the batch edit menu.

Procedure 50
Configuring the Camera connection protocol

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**.
3	Click  in the camera row that you want to change the IP protocol. The Function and Streams tab appears.
4	Select the **General** tab.
5	Select a protocol from the **Camera connection protocol** dropdown menu.
6	Click 

- End -

Video Streaming

You can enable or disable streaming on a camera as required.

Procedure 51
Enable/Disable Video Streaming

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**.
3	Click  in the camera row that you want to modify video streaming. The Function & Streams page opens.
4	Select the **General** tab.
5	In the **Video Streaming** field select **Enabled** to enable camera streaming, Or Select **Disabled** to disable camera streaming.
6	Click 

- End -

Image Settings

Camera image settings can be configured in the Image Setting tab which can be accessed by clicking the Setup icon for the required device on the Video List tab. The settings available are dependent on the camera make/model. When the changed settings are applied, the viewer window updates to reflect the changes made.

Procedure 52
Configuring Camera Image Settings

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**.
3	Click  in the camera row you want to configure camera settings. The Function & Streams tab displays.
4	Select the **Image Settings** tab.
5	Adjust the Video Properties as required. The available settings and value ranges are dependent on the camera make/model and include: a **Video Standard** - Select the required video processing standard from the dropdown. b **Rotate Image** - Select the angle you want to rotate the image from the dropdown. c **Brightness** - Select the brightness value from the dropdown. d **Contrast** - Select the contrast value from the dropdown. e **Hue** - Select the hue value from the dropdown. f **Saturation** - Select the saturation value from the dropdown.

g **Sharpness** - Select the sharpness value from the dropdown.

h **White Balance** - Select the white balance control value from the dropdown.

i **Back Light Compensation** - Select the back light compensation value from the dropdown.

j **Image Interlaced** - Select the image interlacing setting from the dropdown.

6 Adjust the Lens/Sensor settings. The types of settings and value ranges available are camera make/model dependent and include:

a **Lens Focus** - Select a focus for the camera from the dropdown.

b **Lens Auto Focus** - Select the checkbox to enable automatic camera focus.

c **Lens Iris** - Select the iris value for the camera from the dropdown.

d **Lens Auto Iris** - Select the checkbox to enable automatic iris control.

e **Lens Day Night Mode** - Select the required mode from the dropdown.

f **Lens WDR (Wide Dynamic Range)** - Select the checkbox to enable WDR.

g **Mount Type (Vivotek Fish-eye camera only)** - Select the Mount type from the dropdown.

Note:
The mount point configured on the NVR must match the location of the Vivotek Fish-eye camera when it is installed as this will dictate the algorithm used by victor unified client for de-warping.

7 Click 

The viewer window updates to reflect the changes made to the image settings.

- End -

Function and Streams

From the Function and Streams tab you can configure the following settings:

- Recording Mode
- Video Analysis
- Motion Sensitivity (Motion Detection only)
- Maximum Retention Period
- Associate Audio
- Auto-Configure Streams
- Max GOP
- Stream Configuration

Recording Mode

The recording mode setting on the camera determines when the camera records.

Table 6 Recording Statuses

Mode	Icon	Description
Recording Off		Camera is not recording. Live video can still be viewed.
Recording Always		The camera will record continuously. In this mode you will not receive alert notifications from the NVR.
Only Record on Alarm		Camera is not recording an alarm is detected recording commences. Using this mode you will receive alert notifications from the NVR.
Recording Always with Alarm On		Camera is recording continuously with alarm detection (bump-on-alarm). Using this mode you will receive alert notifications from the NVR.

Procedure 53
Setting the Camera Recording Mode

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**.
3	Click  in the camera row you want to configure camera settings. The Function & Streams tab displays.
4	Select the required **Record Mode** option button: • **Recording Off** • **Recording Always** • **Only Record on Alarm** • **Recording Always with Alarm On**
5	Click 

Note:
You can check the recording mode of any camera in the Live Video windows. The recording mode is displayed beside the camera name.

- End -

Video Analysis

Video Analysis can be enabled using the dropdown to select one of the following:

- Motion Detection
- Video Intelligence
- Face Recognition
- Edge Analytics
- License Plate Recognition

Motion Detection

The NVR provides server-based motion detection for all cameras. The NVR supports two motion detection features:

- **Motion Search** - a VideoEdge Client or victor Client can search recorded video for motion.
- **Motion Alerts** - you can define Motion detection settings that can be used to set up motion detection rules. When a new camera is added to the NVR, a motion detection alert is automatically created with a full-view region. The name of this alert will be called “Full View”.

The Motion Detection settings allow you to define the parameters which will initiate an alarm. This will reduce the number of unwanted alarm events and is achieved using the following tools:

- Duration settings allowing you to define the time period of activity in the region of interest to activate an alarm.
- Direction settings allowing you to define the direction of motion required to activate an alarm.
- Size expressed as the minimum percentage of the region of interest with activity required before activating an alarm.

Motion Detection events create entries in the victor Application Server database. If required, you can use the Reports feature in victor unified client to retrieve event information.

Motion Sensitivity

Motion Sensitivity can be configured using the dropdown to select one of the following:

- High (most results)
- Medium high
- Medium
- Medium low
- Low (least results)

For more information on configuring motion detection refer to the Alarms chapter.

Enabling Motion Detection

A Stream Configuration is required that allows the NVR to generate meta-data for motion detection. When you add a camera to VideoEdge, you must select the **Enable Smart Search (Motion Metadata)** option. You also need to select **Motion Detection** from the **Video Analysis** dropdown. The NVR will automatically determine the required stream settings. If only one stream is configured and it does not satisfy the requirements for Motion Detection, the NVR will attempt to automatically open the second stream with settings best suited for Motion Detection. If the camera does not support dual streaming you will manually need to adjust the configuration of the configured stream.

Motion Detection may not be available on a camera if it’s minimum video resolution setting is higher than the maximum acceptable resolution for Motion Detection. The NVR will not allow you to configure a camera for Motion Detection if the resolution setting of the camera is higher than the settings in Table 10-1.

Table 7 Camera Resolutions for Motion Detection

Camera Type	Minimum Resolution	Maximum Resolution
MJPEG	QCIF	1280 x 960
MPEG-4	QCIF	CIF

The optimal stream to perform Motion Detection is 320 x 240 resolution (or the closest resolution supported by the camera), MJPEG at 7 frames per second. Lower resolution or frame rates might degrade the quality of Motion Detection. The NVR requires at least QCIF and more than 4 frames per second to perform motion detection.

Note:
Video Analytics run internally at approximately 7fps. If analytics utilizes a stream that is running at a higher frame rate that 7fps, then the analytics engine will drop frames to make sure that it is under a certain fps and CPU load.

Procedure 54
Enabling Motion Detection for a Camera

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**.
3	Click  in the camera record for which you want to configure camera settings. The Function & Streams tab displays.
4	Set the camera **Record Mode** to a setting that supports Motion Detection ( Only Record on Alarm or Recording Always with Alarm On).
5	Select **Motion Detection** from the **Video Analysis** dropdown list. **Note:** If an error message opens, the NVR cannot detect a suitable stream from the camera to support Motion Detection. You will need to change the Codec Image Resolution, or FPS of one of your camera's streams to settings that are compatible with Motion Detection.
6	Select the required level of **Motion Sensitivity**. Values range from High (most results) to Low (least results).
7	Click 

- End -

Disabling Motion Detection

When required, you can disable Motion Detection in the Video List or using the camera's Advanced Edit page. When Motion Detection is disabled you will not be able to perform some of the Motion Detection based activities, such as setting NVR Motion Detection alarms.

Procedure 55
Disabling Motion Detection for a Camera

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**.
3	Click  in the camera record where you want to disable camera Video Intelligence. The Function & Streams page opens.
4	Select **None** from the **Video Analysis** dropdown.

5 Click 

- End -

Video Intelligence

The NVR provides server based Video Intelligence for all cameras. Video Intelligence is a licensed add-on for the NVR. The NVR supports two Video Intelligence features:

- **Video Intelligence Search** - a VideoEdge Client or victor unified client can search recorded video for a specific type of event.
- **Video Intelligence Alerts** - you can define Video Intelligence settings that can be used to set up Video Intelligence rules.

There are several types of Video Intelligence rules available. These include:

- **Object Detection** - Used to detect people or objects moving into a region of interest. This search is similar to a motion search, but only detects people or objects on entry of the region of interest i.e. they will not be continuously detected if they remain within the region of interest. If the object leaves the camera view and returns, the search will detect them again. A separate event is generated for each object that enters the region, even if the objects move into the region at the same time, unlike motion detection that generates one event.
- **Object Direction** - Used to detect objects moving in a certain direction through a region of interest, for example, a car traveling the wrong way on a road.
- **Object Linger** - Used to detect objects lingering in an area of interest. An object is lingering if it remains in the region of interest.
- **Object Dwell** - Use to detect objects dwelling in a region of interest if it is mostly stationary.
- **Queue Analysis** - Use to detect a queue forming of a specified length.
- **Perimeter** - Used to detect when an object enters a protected area through a perimeter area.
- **Crowd Formation** - Use to detect when a specified number of people are in the region of interest.
- **Object Enter** - Used to detect objects entering a camera view through a region of interest, for example, a doorway or threshold.
- **Object Exit** - Used to detect objects exiting a camera view through a region of interest, for example, a doorway or threshold.
- **Object Abandoned/Removed** - Used to find changes to the background of a scene in a region of interest, for example, use it to detect when a stationary object was placed, moved or removed.

The Video Intelligence settings allow you to define the parameters which will initiate an alarm (an alarm rule). This will reduce the number of unwanted alarm events. The parameters available are dependent on the type of Video Intelligence rules which are defined.

Video Intelligence provides useful information only if recording is enabled on the camera. Your camera should be configured with **Only Record on Alarm** or **Recording Always with Alarm On** recording modes.

Video Intelligence events will create entries in the victor Application Server database. If required you can use the Reports feature in victor unified client to retrieve event information.

To carry out Video Intelligence based activities you need to enable Video Intelligence on the NVR.

Enable Video Intelligence for a Camera

To enable a camera to use Video Intelligence features, you can use the Video List tab or the Function and Stream settings tab of the camera Advanced Edit page.

You must ensure that you have a Stream Specification that allows the NVR to generate meta-data for Video Intelligence. You also need to select **Video Intelligence** in the **Video Analysis** field.

You can configure the minimum object height and width. Objects that are smaller than these dimensions do not generate Video Intelligence alerts.

The NVR will automatically determine the required settings and apply them to a stream. If the camera is configured for dual-stream, then the NVR chooses the best stream. If the NVR is unable to find a suitable video stream for Video Intelligence an error message opens.

Note:
• It is recommended that you configure Video Intelligence rules on the camera, before adding the camera to the VideoEdge.
• After you enable Video Intelligence on a camera that is already on a VideoEdge, you must restart the NVR services before VideoEdge recognizes the new configuration. You can restart the NVR services from the **Shutdown** page in the **Advanced** menu.

Video intelligence may not be available for a particular camera if the camera's video resolution setting is lower than the minimum or higher than the maximum acceptable resolution for Video Intelligence. The NVR will not allow you to configure a camera for Video Intelligence if the resolution setting of the camera is outside of the settings in the table below.

Table 8 Camera Resolutions for Video Intelligence

Camera Type	Minimum Resolution	Maximum Resolution
MJPEG	320 x 180	1280 x 960
MPEG-4	320 x 180	CIF

The optimal stream to perform Video Intelligence is CIF (320 x 240 resolution) MJPEG at 7 frames per second. The NVR requires at least 320 x 180 resolution and more than 4 frames per second to perform Video Intelligence activities.

Note:
Video Analytics run internally at approximately 7fps. If analytics utilizes a stream that is running at a higher frame rate that 7fps, then the analytics engine will drop frames to make sure that it is under a certain fps and CPU load.

Procedure 56
Enabling Video Intelligence for a Camera

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**.
3	Click  in the camera record for which you want to enable Video Intelligence. The Function & Streams tab displays.

Note:
You can also enable Video Intelligence from the Video List.

4 Set the camera **Record Mode** to a setting that supports Video Intelligence (Only Record on Alarm or Recording Always with Alarm On).

5 Select **Video Intelligence** from the **Video Analysis** dropdown.

Note:
If an error message opens, the NVR cannot detect a suitable stream from the camera to support Video Intelligence. You will need to change the Codec, Image Resolution, or FPS of one of your camera's streams to settings that are compatible with Video Intelligence.

6 Enter a value for **Minimum object width (Pixels)**.

7 Enter a value for **Minimum object height (pixels)**.

8 (Optional) Select the **Compensate for camera motion** checkbox.

9 Click

- End -

Disable Video Intelligence for a Camera

If you do not want Video Intelligence activities carried out on a camera, you can disable Video Intelligence in the NVR camera settings. When Video Intelligence is disabled you will not be able to perform any Video Intelligence searches or set Video Intelligence alarms on the camera. However, the Video Intelligence alarms defined on a camera are remembered and will become active if Video Intelligence is enabled again for that camera.

Procedure 57
Disabling Video Intelligence for a Camera

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**.
3	Click in the camera record where you want to disable camera Video Intelligence. The Function & Streams tab displays.
4	Select **None** from the **Video Analysis** dropdown.
5	Click

- End -

Face Recognition

A license can be purchased for the NVR that permits facial recognition. This can be configured to recognize individuals that have been added to the NVR's Face Enrollment database.

Enabling Face Recognition

To enable face recognition you need to populate the NVR's Face Enrollment database, refer to Face Enrollment for further information. Face recognition can be enabled in the Device List page or the Function and Stream settings tab in the camera setup pages. Enabling face recognition on a camera will allow the recognition of individuals enrolled in the database as well as detecting everyone else.

You need to select **Face Recognition** in the **Video Analysis** field.

Face Detection Sensitivity

Face Detection Sensitivity determines how easily a camera can detect a face that is present in the camera's view. Lower sensitivity levels delay detection until the face can be more easily recognized, but can result in some missed detections for faces that are not seen clearly. Higher sensitivity levels result in earlier detection and fewer undetected faces, but reduce face recognition accuracy.

Face Recognition Sensitivity

Face Recognition Sensitivity determines how accurately a detected face can be identified. Higher sensitivity levels delay recognition to occur on faces that are not seen as clearly, but can result in more misidentifications. Lower sensitivity levels reduce misidentifications, but can result in delayed recognition and more frequent failure to recognize enrolled faces.

Face Search Alert

The Face Search Alert feature enables retrospective searches and realtime alerts, based on face detection and recognition. Face Search Alerts can only be enabled if a corresponding license is available.

Face Verification

Enable Face Verification to allow face recognition to check the identity of persons using the access control system. This functionality is accessed through the Swipe-and-Show feature of the Victor client. Face Verification can only be enabled if a corresponding license is available.

Procedure 58
Enabling Face Recognition for a Camera

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**.
3	Click  in the camera record for which you want to configure camera settings. The Function & Streams tab is displayed.
4	Set the camera **Record Mode** to a setting that supports edge based analytics ( Only Record on Alarm or  Recording Always with Alarm On).
5	Select **Face Recognition** from the **Video Analysis** dropdown.
6	Select the **Minimum face size** from the dropdown menu.

7	Select the required level of **Face Recognition Sensitivity**. Values range from High (yields faster and more frequent recognition, but suffers more misidentifications) to Low (makes fewer misidentifications, but will fail to recognize enrolled personnel more frequently).
8	Select the required level of **Face Detection Sensitivity**. Values range from High (most results) to Low (least results).
9	(Optional) Select the **Face Search Alert** checkbox.
10	(Optional) Select the **Face Verification** checkbox.
11	Click 

- End -

Disabling Face Recognition

When required, you can disable face recognition in the Device List or using the camera's Setup pages.

Procedure 59
Disabling Face Recognition for a Camera

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**.
3	Click  in the camera record where you want to disable camera Video Intelligence. The Function & Streams tab displays.
4	Select **None** from the **Video Analysis** dropdown.
5	Click 

- End -

License Plate Recognition

A license can be purchased for the NVR that permits license plate recognition. License plate recognition can be configured to create a notification when the license plate of a vehicle is detected.

Enabling License Plate Recognition for a Camera

License plate recognition can be enabled in the Device List page or the Function and Stream settings tab in the camera setup pages. Enable license plate recognition on a camera to allow the recognition of license plate numbers that are either entered manually or imported when configuring alarms.

Procedure 60
Enabling License Plate Recognition for a Camera

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**.
3	Click  in the camera recorder for which you want to configure camera settings.

The **Functions & Streams** tab appears.

4 Set the camera **Record Mode** to a setting that supports VideoEdge based analytics. (Only Record on Alarm or Recording Always with Alarm On)

5 Select **License Plate Recognition** from the **Video Analysis** dropdown.

6 Select the required level of **License Plate Recognition Sensitivity** from the dropdown.

Note:
The following sensitivity levels are available: Low, Medium low, Medium, Medium high, High. A higher sensitivity level returns more results but with an increased chance of false positives (mistakes). A lower sensitivity level returns less results but with an increased chance of false negatives.

7 Select the **License Plate Recognition Countries or States**.

a Select the **Choose Countries or States** field.

b Select a continent or country from the list.

c Select a country or state from the list.

Note:
• You can select up to five countries or states.
• Only license plates from selected countries can be detected.

8 Click

- End -

Disabling License Plate Recognition for a Camera

When required you can disable license plate recognition in the Device List

Procedure 61
Disabling License Plate Recognition for a Camera

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**.
3	Click in the camera that you want to disable. The **Function & Streams** tab appears.
4	Select **None** from the **Video Analysis** dropdown.
5	Click

- End -

Edge Analytics

Edge Analytics are camera-based analytic operations which forward alarms and metadata to the NVR. This minimizes the impact on the NVRs CPU usage in comparison to Motion Detection and Video Intelligence which are both server-based operations.

Refer to the VideoEdge camera handler release notes for information about supported camera models.

The NVR supports camera-based analytics for supported cameras. The NVR supports two edge analytics features:

- **Edge-based Alarms** - A client can receive alarms for a specific type of event configured on the camera.
- **Edge-based metadata** - A client can search recorded video for a specific type of event.

The following edge-based analytic types are available on the NVR, depending on which analytics are supported and configured on the camera:

- **Blur Detection Alarms** - Blur events occur when the camera becomes out of focus in the region of interest. Edge based blur detection events are only supported in victor unified client.
- **Motion Detection Alarms** - Motion detection events occur when motion is detected in the camera's view. Edge based motion detection events are supported in both victor unified client and VideoEdge client.
- **Motion Detection metadata** - When enabled allows you to search recorded video for edge based motion detection events. Edge based motion detection searches are supported in victor unified client.
- **Face Detection Alarms** - Face detection events occur when a face is present in the camera's view. Face detection is only supported on victor unified client.
- **Face Detection metadata** - When enabled allows you to search recorded video for edge based face detection events. Face detection searches are supported in victor unified client.
- **Video Intelligence Alarms** - Video Intelligence events occur when one or more analytic rules initiate an alarm. Video Intelligence alarms are supported in victor unified client.
- **Video Intelligence metadata** - When enabled allows you to search recorded video for edge based Video Intelligence events. Video Intelligence searches are supported in victor unified client.

Note:
Only one edge based metadata type can be enabled for search at any one time, for example if you have Motion Detection metadata enabled, you cannot enable Face Detection metadata.

Before the NVR can receive edge based analytic events or metadata, this functionality must be configured and enabled on the camera or encoder. When edge analytics have been enabled on the device, you must also enable edge analytics functionality on the NVR. You must set the Video Analysis to be Edge Based in the NVR Camera Configuration.

Edge based analytics provide useful information only if recording is enabled on the camera. All three recording status will record Motion Detection metadata, Face Detection metadata or Video Intelligence metadata, provided it is enabled. This allows Edge based searching of recorded video for any of these metadata types.

For Edge based alarms your camera recording status should be set to either Only Record on Alarm or Recording Always with Alarm On.

Edge Analytic events will create entries in the victor Application Server database. If required you can use the Reports feature in victor unified client to retrieve event information.

Enabling Edge Based Analytics

To enable edge based analytics you need to configure settings on both the camera or encoder and the NVR. Refer to the User's Guide of the edge device for information on how to enable edge based analytics on the device. Once

configured on the device you can enable the NVR to use edge based analytic features on the configured camera using the Device List page or the Function and Stream settings tab in the camera setup pages.

You need to select **Edge Based** in the **Video Analysis** field.

When the NVR is configured to support Edge based analytics, certain Edge analytic functionality may be dependent on stream configuration. Refer to camera documentation for more detail.

Procedure 62
Enabling Edge Based Analytics for a Camera

Step	Action
1	Ensure edge based analytics have been configured on the camera via the camera's own interface. For further information refer to the camera's User Manual.
2	Select **Devices** from the main menu.
3	Select **List**.
4	Click  in the camera record for which you want to configure camera settings. The Function & Streams tab is displayed. **Note:** You can also enable edge based analytics from the Batch edit tab.
5	Set the camera **Record Mode** to a setting that supports edge based analytics ( Only Record on Alarm or  Recording Always with Alarm On).
6	Select **Edge Based** from the **Video Analysis** dropdown. **Note:** Refer to the camera handler release notes to ensure proper camera configuration is used for edge analytics.
7	Click 

- End -

Disabling Edge Based Analytics for a Camera

When required, you can disable edge based analytics in the Device List or using the camera's Setup pages. When edge analytics is disabled you will not be able to perform some of the edge based analytic activities, such as enabling edge based Motion Detection alarms.

Set the Maximum Retention Period

The maximum retention period is the maximum duration over which recorded video for a camera will be saved for, without being deleted. Recorded video older than this will be deleted periodically to free storage space in the storage set the camera is recording to.

Procedure 63
Setting the Maximum Retention Period

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**.
3	Click  in the camera row you want to set the recording retention period. The Function & Streams tab displays.
4	Enter the **Maximum Retention Period** in the **Days** and **Hours** fields.
5	Click 

- End -

Configuring Audio Association

The audio device you want to associate with a camera is selected using the Associate Audio dropdown.

Note:
Audio playback is not available via the NVR Administration Interface. The audio settings are used to determine how audio streams are made available to connected clients.

Audio and video are derived from the camera as two separate packet streams. Depending on the camera manufacturer and video/audio codec combination, these packet streams may not be exactly in synchronization for live streaming. The NVR's live streaming method is to pull video and audio from the camera and push it to the client straight away. This helps achieve low video latency but sometimes at the expense of live audio/video synchronization. Recorded playback of the same audio and video may give better audio/video synchronization results.

Procedure 64
Configuring Audio Association

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**.
3	Click  in the camera row you want to edit audio settings. The Function & Streams tab displays.
4	Select the Audio device you want to associate with the camera from the **Associate Audio** dropdown.
5	Click 

- End -

Auto-Configure Streams

The Auto Configure streams function allows the NVR to apply stream settings to the designated camera which will provide the best results when SmartStream resource management is applied. When a video analysis type is selected with Auto-Configure enabled, the NVR will apply the recommended settings to the chosen analytic stream.

Note:
Auto-Configure Streams is enabled by default.

Procedure 65
Enabling/Disabling Auto Configure Streams

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**.
3	Click  in the camera row for which you want to edit stream settings. The Function & Streams page opens.
4	Select an option from the **Auto-Configure Streams** list. • **None**: Disables the Auto Configure streams function. • **1 Additional Live Stream**: Configure one additional stream • **2 Additional Live Streams**: Configure two additional streams. This option is only available for cameras that support three streams.
5	Click 

- End -

Max GOP

A GOP is a group of pictures. Camera video streams comprise successive GOPs.

- For H264 camera streams, the GOP size is a fixed value. The GOP size displays in the stream configuration table.
- For H264+ camera streams, the GOP size is a variable value. The camera handler dynamically determines the GOP size.

From the Function & Streams page, you can set a maximum GOP size for a camera's H264+ stream.

Note:
To set the Max GOP size for any cameras that you add to VideoEdge, edit the Max GOP value on the Options page. For more information, see Options.

Gaming Mode

Gaming Mode is a standardization setting for video cameras. Enabling Gaming Mode for a camera will maintain a constant frame rate for that camera's video stream.

Stream Configuration

Stream Configuration defines which stream is used for live video, alarms and recording. The NVR will automatically determine the best stream to use for Motion Detection or Video Intelligence. You can also adjust the codec, FPS and resolution of each stream. Depending on what is assigned to a stream, you need to have the appropriate codec, FPS and resolution assigned. For example, the stream you are using for Video Intelligence analytics must be MJPEG or MPEG-4, with a recommended resolution of CIF and 7 FPS. For analog cameras, bit rate control, max bit rate and profile can also be configured.

Note:
If the camera supports only a single stream, the Stream 2 settings for Live Stream, Alarm Stream, Record Stream and Analytics Stream are unavailable.

Codecs

VideoEdge supports the following video codecs: H264, H264+, MPEG4, and MJPEG. The following table lists the cameras and firmware versions that can support the H264+ codec.

Camera Model	Firmware Version
Illustra Flex 3MP Compact / Mini-Dome / Bullet / Box	SS004.01.02 or above
Axis (Zipstream capable)	6.5 or above

Table 9 Camera firmware compatibility for H264+

Note:
• The H264+ codec is available for supported cameras from VideoEdge 5.1 onwards.
• For more information about supported video codecs, refer to the *VideoEdge Camera Handler Release Notes*.

Procedure 66
Configuring Stream Settings

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**.
3	Click  in the camera row for which you want to edit stream settings. The Function & Streams page opens.
4	Select the stream you want the camera to use for: a Live video b Alarms c Recording
5	Select the **Codec** for each stream:
6	Select the **FPS** for each stream.
7	Select the **Resolution** for each stream.
8	If you are using a stream for analytics, select the **Quality**.
9	If you are configuring an analog camera; a Select the **Bit Rate Control**. b Enter the **Max Bit Rate**. c Select the **Profile**.
10	Click 

- End -

Archive

The Archive tab is where you configure:

- Archiving Mode
- Archiving Quality
- Maximum Archiving Storage Period

Archive settings can be configured for each individual camera. This will determine video which is queued for archiving, not when it will be written to the archive. You can also apply frame rate decimation using the Archive Quality dropdown and define a maximum retention period for archived video.

Procedure 67
Configure Archive Settings

Step	Action
1	Select **Devices** from the menu.
2	Select **List**.
3	Click  in the camera row for which you want to edit archive mode.
4	Select the **Archive** tab.
5	Select the **Archiving Mode**.
	a Select the **Archiving disabled**  option button to disable archiving for the camera.
	Or
	b Select the **Archive all video**  option button to archive all video for the camera.
	Or
	c Select the **Archive only alarm video**  option button to archive video triggered with an alarm.
6	Select the **Archiving Quality** from the dropdown.
7	Select the **Maximum Archiving Storage Period**.
	a Select **As long as possible**.
	Or
	b Select **Custom** and enter the number of days in the **Period** field.
8	Click 

- End -

Alerts

From the Alerts tab you can configure the following settings:

- Alert Pre-Buffer (seconds)
- Alert Post-Buffer (seconds)

Buffer times range from 30 seconds to 300 seconds, defined in 10 second intervals.

- Enable / Disable Dry Contacts

Procedure 68
Configuring Alert Recording Buffers

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**.
3	Click  in the camera row for which you want to set alert recording buffers. The Function & Streams tab displays.
4	Select the **Alerts** tab.
5	Select the **Alert Pre-Buffer** time from the dropdown.
6	Select the **Alert Post-Buffer** time from the dropdown.
7	Click 

- End -

Dry Contacts (IP Cameras)

From the Alerts tab, you can associate dry contact sensors with a particular IP camera. Dry contact sensors are typically used in doorways, and are activated when a door is opened. The NVRs can command cameras to pan-tilt-zoom to predetermined locations and record video for a specified period.

Procedure 69
Enabling a Dry Contact Sensor

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**.
3	Select  for the camera for which you want to enable dry contact settings. The Function & Streams tab displays.
4	Select **Alerts** tab.
5	Select the Dry Contact Input **Enabled** checkboxes in the Dry Contacts section.
6	Click  **Note:** If you are editing the dry contact settings for a camera forming part of an encoder device, all cameras related to this device will be updated with the changes made to the dry contacts. In this instance, a warning message opens informing you that multiple cameras will be updated.

- End -

Alarm Inputs (Analog Cameras)

The NVR is supplied with a number of alarm inputs on the rear of the device (the number of inputs on the NVR varies depending on the model in use).

Alarm Inputs are used with dry contact sensors connected directly to the NVR. These are sensors typically used in doorways, and are activated, for example, when a door is opened. An Alarm Input can be associated with an analog camera and event actions in the Local Client or victor unified client.

Note:
The VideoEdge Administrator interface lists its alarm inputs beginning at 1. victor however lists alarm inputs beginning at 0. For example, if alarm input 1 activates on the VideoEdge, it registers as input 0 in victor's Activity pane.

Procedure 70
Associating an Alarm Input with an Analog Camera

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**.
3	Select  for the camera for which you want to enable dry contact settings. The Function & Streams tab displays.
4	Select the **Alerts** tab.
5	Select the Dry Contact Input **Enabled** checkboxes in the Dry Contacts section.
6	Click  A dialog box displays stating 'Warning: the selected camera is sharing a multi-channel encoder with the following cameras. The dry contact change will apply to these cameras also.' **Note:** 1. This message appears because the NVR's software recognizes the analog card as an encoder. In this instance the Alarm Input is only associated with the camera you were associating the Alarm Input with. 2. The Dry Contacts table displayed in the Alerts tab of each analog camera displays all inputs which are currently active rather than the inputs which are associated with that camera. To associate a dry contact input with another camera you must disable the input and then re-enable it in the Alerts tab of the camera you want to associate it with.
7	Click **OK**. A list of the analog cameras on the card is displayed.

- End -

Multicast

From VideoEdge 5.1 onwards, you can configure multicast streaming for supported cameras. victor operators can view live steams from multicast cameras, even while the VideoEdge is offline. The following table lists the Illustra cameras and camera firmware versions that currently support multicast streaming.

Camera Model	Firmware version
Illustra Pro 2MP / 3MP / 5MP Fixed Mini-Dome	1.3.2 or above
Illustra Flex 3MP Compact / Mini-Dome / Bullet / Box	SS004.01.02 or above

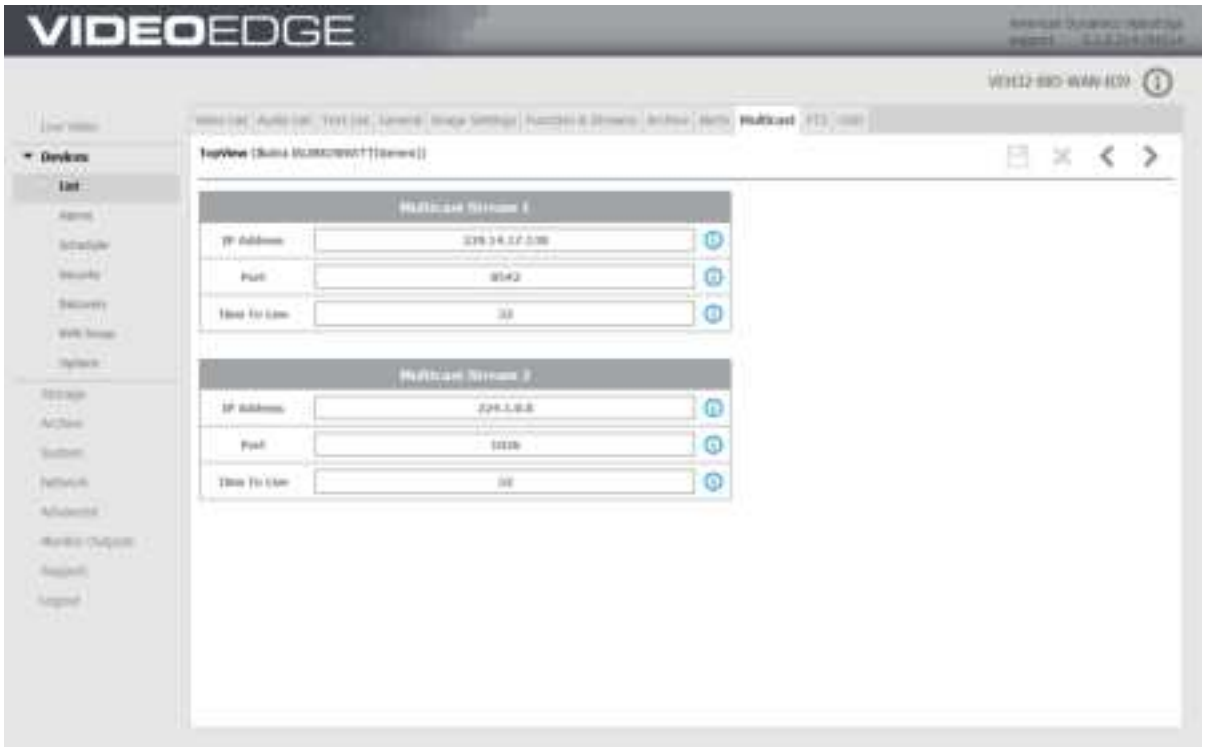
Table 10 Camera firmware compatibility for Multicast

Note:
• The Multicast tab is only available for cameras that support multicast streaming.
• For information about camera limitations, and an updated list of cameras that support multicast streaming, refer to the *VideoEdge Camera Handler Release Notes*.

From the Multicast tab, you can configure the following settings for supported multicast cameras:

- **IP Address:** Select a multicast address from the following ranges:
  - 224.0.2.0 - 224.255.255.255
  - 232.0.0.0 - 232.255.255.255
  - 234.0.0.0 - 234.255.255.255
  - 239.0.0.0 - 239.255.255.255
- **Port:** Choose an unassigned port in the range 0 to 65534. The port must be an even number, and it cannot be the same value used for a different multicast stream.
- **Time to Live:** Enter a value from 1 to 255.

Note:
To avoid streaming playback issues, ensure that each multicast camera uses a different combination of IP address and port numbers.



Procedure 71
Configuring Stream Settings

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**.
3	Select for the multicast camera that you want to configure. The Function & Streams tab displays.
4	Select the **Multicast** tab.
5	Edit Multicast Stream 1 a Enter the **IP Address**. b Enter the **Port** number. c Enter the **Time to Live** value.
6	Edit Multicast Stream 2 a Enter the **IP Address**. b Enter the **Port** number. c Enter the **Time to Live** value.
7	Click

- End -

PTZ

If a camera has PTZ capabilities you can enable or disable PTZ functionality and configure the Return to Home settings for the camera from the PTZ tab. Additionally for analog PTZ cameras you can configure PTZ serial port settings from the Advanced menu and you can view Serial Protocols from the System menu.

Enable/Disable PTZ Functionality

You can enable or disable PTZ functionality for a camera provided the camera has PTZ capabilities.

Procedure 72
Enable or Disable PTZ for IP Cameras

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**.
3	Click  in the PTZ camera row. The Function & Streams tab displays.
4	Select **PTZ** tab.
5	Select the **Enable PTZ** checkbox to enable PTZ. Or Deselect the **Enable PTZ** checkbox to disable PTZ.
6	Click 

- End -

Procedure 73
Enable or Disable PTZ for Analog Cameras

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**.
3	Click  in the PTZ camera row. The Function & Streams tab displays.
4	Select **PTZ** tab.
5	Select the **PTZ Port** from the dropdown to enable PTZ. Or Select **None** from the dropdown to disable PTZ.
6	Click 

- End -

Return to Home

When the PTZ Return to Home feature is enabled, the PTZ returns to its 'home' position after a user-defined period of inactivity. The first preset in a list of configured presets is considered to be the home position.

When the PTZ is moved, the idle timer for the camera is reset. For example, if a camera moves to a preset position, moves using the pan or tilt controls or moves as part of a tour, the idle timer will reset to zero.

Note:
If the camera is moved using the camera's own web browser controls, the timer will not reset.

The Return to Home period is defined using the dropdown. The periods available are in seconds between 60 and 600, in 60 second intervals.

Procedure 74
Enabling PTZ 'Return to Home'

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**.
3	Click  in the PTZ camera row for which you want to enable the 'Return to Home' feature. The Function & Streams tab displays.
4	Select **PTZ** tab.
5	Select the Enable PTZ checkbox for IP Cameras. Or Select the PTZ Port from the dropdown for Analog Cameras. **Note:** PTZ must be enabled to configure Return to Home settings.
6	Select the **Enable Return to Home** checkbox. The Return to Home After dropdown displays.
7	Select the desired period of inactivity before the camera 'returns to home' from the **Return to Home After** dropdown (range 1 - 10 minutes).
8	Click 

- End -

Intelligent Guard Tour

From the PTZ tab you can enable an Intelligent Guard Tour for supported PTZ cameras.

An Intelligent Guard Tour is a Guard Tour that includes motion detection and motion tracking. If VideoEdge detects motion during a guard tour, motion tracking begins. The camera continuously uses PTZ functionality to keep the moving object centered in the camera's field of view.

Note:
If motion is not detected in the field of view for three seconds, the camera resumes the original guard tour sequence.

Procedure 75
Enabling an Intelligent Guard Tour

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**.
3	Click  in the PTZ camera row that you want to configure. The Function & Streams tab displays.
4	Select the **PTZ** tab.
5	Select the **Enable Intelligent Guard Tour** checkbox.
6	Click  **Note:** After you enable the Intelligent Guard Tour feature, you must complete the following configuration steps: • Configure a Guard Tour for the camera, through victor, or though the camera's web interface. • Set the PTZ Home position for the PTZ camera.

- End -

Analog Matrix

PTZ support for cameras connected to MegaPower 3200 and MegaPower 48 Plus matrix switches can be configured in the advanced configuration settings for the camera allowing them to be controlled by the AD2089 and ADTTE matrix control keyboards.

Note:
Ensure the RS-232 Serial Port has been configured to the appropriate matrix protocol. Refer to **Serial Ports** for further information.

Procedure 76
Configuring Camera PTZ for Analog Matrix

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**.
3	Select  for the camera you want to configure PTZ settings for analog matrix.

The Function & Streams tab displays.

4 Select **PTZ** tab.

5 Select the correct camera control port from the **PTZ Port** drop down menu.

6 Enter the **PTZ Address**.

7 If required, select **Enable Camera Menu** checkbox to allow camera menu access on the PTZ / Keyboard controls.

8 Enter the **Matrix Monitor Number**.

9 Click 

- End -

On Screen Display (OSD)

You can configure OSD settings for each analog camera in the OSD tab. You can create custom values to be displayed in the top left, top right, bottom left and bottom right of the video pane. These values are embedded in the recorded video and are recorded along with the video stream. You can configure camera-specific OSD settings and global OSD settings for the font, font color and timestamp format.

Global OSD Settings

Global Settings can be applied for OSD in the OSD tab. The global settings allow you to configure the Font, font Color and Timestamp format which will be applied to all analog cameras with OSD settings enabled and OSD setting configured.

Note:
When selecting the font color it is important to consider the image being captured by the camera. A font color which contrasts the background color of the image will be easiest to distinguish.

Procedure 77
Configuring the Global OSD Settings

Step	Action
1	Select **Devices**.
2	Select **List**. The Video List tab displays.
3	Click  of the analog camera you wish to configure OSD settings for. The Function & Streams tab displays.
4	Select the **OSD** tab.
5	Select the **Font** from the drop down.
6	Enter the hex value for the font in the **Color** field. Or Click on the Color field and select the color using the palette.
7	Select the Timestamp format using the **Timestamp Format** dropdown.

8	Click 

- End -

Camera Specific OSD Settings

Each analog camera can have up to four OSD items enabled which will display on top left, top right, bottom left and bottom right corners of the video stream. Each display can include both a custom value and a Timestamp.

The transparency of each display item can be configured to provide a contrasting background behind the font if required. The level of transparency is applied to the background of the display item only and not the transparency of the font of the display item itself. The display item can be set to blink on and off every second.

Note:
If you use large amounts of text when configuring OSD items it is possible for the displays to overlap. This should be checked after OSD configuration and rectified if necessary.

Procedure 78
Configuring Camera Specific OSD Settings

Step	Action
1	Select **Devices**.
2	Select **List**. The Video List tab displays.
3	Click  in the row of the analog camera you wish to edit in the Video List. The Function & Streams tab displays.
4	Select the **OSD** tab.
5	Select  to configure the OSD Position.
6	Select the **Enabled** checkbox.
7	Enter required value in the **Text** field.
8	Use the slider to set the **Transparency**.
9	(Optional) Select the **Blink** checkbox.
10	(Optional) Select the **Timestamp** checkbox. **Note:** You must have a global Timestamp selected to allow you to enable a Timestamp on an individual OSD item.
11	Click 

- End -

OSD Inserts

OSD Inserts are predefined text commands which will display certain values when used as OSD items.

To use the OSD insert feature, enter the required OSD insert item into the text box in the OSD table. The list of supported OSD Inserts includes the following:

- **%camera%** - Displays the name of the camera.
- **%preset%** - Displays the last PTZ preset used.
- **%pattern%** - Displays the pattern being ran or the last pattern which was ran by that camera.
- **%PTZ%** - Displays the PTZ preset being ran.

Effects of Resolution on OSD

OSD is embedded into the video stream and recorded video. OSD is displayed in highest quality using D1 resolution, changing to 2CIF, CIF or QCIF lowers the resolution of the image and subsequently the OSD items making them difficult to read.

Using the transparency slider you can apply a high contrast background which will make the OSD item more readable.

Device Replacement

The NVR's device replacement functionality allows you to replace cameras, and encoders and IP text devices by changing the IP address on the existing and configured device slot. This allows you to quickly replace faulty devices or to upgrade to a device with greater capabilities.

The NVR will apply as many of the existing parameters to the new device based on shared compatibility. Where the replacement device has features which are not compatible, default settings will apply. When the new device has been added a dialog window will summarize the settings which have been successfully applied and those that cannot be applied or where a 'best effort' choice has been implemented.

Note:
When carrying out device replacement for a camera which utilizes analytics, the Region of Interest and Alarms setting will need to be manually re-applied. This ensures that analytic operations remain accurate with the new device's Field of View.

When carrying out device replacements, it's important to also consider the associations that are currently configured on your NVR. Associations configured on the NVR will be maintained by default when device replacement is carried out bar when audio from the replaced device was associated with other devices on the NVR and the new device does not have an audio input.

Replacing an Audio/Video Device

Video and audio devices can be replaced by re-assigning the IP address of the configured slot. Changes to the IP address in the Video List will also be applied to the Audio List and vice versa.

Procedure 79
Replacing a Device from the Video List Tab

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**.
3	Click  in the record of the device you want to replace.
4	Enter the IP address of the new device.

5 Click  .

. A dialog box opens stating 'Warning: Some camera settings may not be retained. Remember to verify all settings pre and post device replacement.'

6 Click **OK**.

The new device will now occupy this device slot.

- End -

Replacing a Text Device

Text device replacement can be achieved by physically replacing the faulty device. Provided the new device shares the same communication configurations as the replaced device, no configuration of the NVR will be required. IP Text devices can also be replaced by re-assigning the port number assigned to the device slot in the Text List tab.

Note:
Should a text device become faulty due to a failure with a RS-232 to USB converter; it may not be possible to carry out a successful device replacement. Some RS232 to USB converters have uniquely assigned IDs, this ID cannot be re-configured on the NVR and in this instance you will be required to delete the Text Device and add re-add. In this instance the association with recorded text data will be lost.

Procedure 80
Replacing an IP Text Device

Step	Action
1	Select **Devices** from the main menu.
2	Select **List**.
3	Select the **Text List** tab.
4	Click  in the record of the device you want to replace.
5	Enter the **Port** number being used by the new device.
6	Click **Apply**. The new device will now occupy this device slot.

- End -

Replacing Multi-Channel Encoders

Multi-channel encoders are perceived by the NVR as multiple devices, for example an eight channel encoder will occupy eight slots in the device list. The device replacement feature allows you to perform individual channel replacement or an encoder for encoder swap.

Replacing an encoder channel with and IP device

Analog devices connected via a multi-channel encoder can be replaced on a one to one basis with IP device. This provides flexibility to upgrade or replace devices gradually without having to request a new license.

The process of replacing an encoder channel with an IP device is the same as standard device replacement.

Replacing a channel on one encoder with a channel from another

You can replace the channels on one encoder with the channels from another. For example if you change the IP address of the device slot occupied to channel 3 of encoder 1 to the IP address of encoder 2, channel 3 of encoder 2 will now occupy the slot in the device list.

Replacing one encoder with another

You can replace a complete encoder with another by selecting all of the encoder's inputs from the device list and using the batch edit tool. The channels from the new encoder will occupy the corresponding device slots. For example, Channel 1 will occupy the slot assigned to channel 1 of the original encoder and so on.

Note:
If the replacement device has less available slots than the device being replaced, the operation will not succeed.

If you want to replace a larger encoder with a smaller encoder, for example, replacing an 8 channel with a 4 channel, only the required slots should be selected before advancing to batch edit.

Note:
When slots are deleted, recorded video associated with that slot can no longer be retrieved.

Audio Support/Associations

Provided the replacement encoder has adequate audio support, audio association and settings should be maintained after a replacement is carried out.

Temporary Device Replacement

Should a device become faulty and need to be disconnected for repair, temporary device can be achieved by following to following process:

1 Carry out device replacement as previously described.

Note:
The NVR will apply as many of the existing parameters to the new device based on shared compatibility. Settings which cannot be applied will be lost.

2 Once repaired reconnect the faulty device.

Note:
Ensure the device has the same IP address as previously configured prior to the fault developing.

3 Apply the NVRs template file to restore all device settings. For further information on applying a template file refer to Templates.

Alarms

Alarms can be specified to trigger when something occurs in the camera scene (e.g. motion, a face is detected, a face is recognized against a database of faces, an object is removed from the scene, etc.). Alarms from VideoEdge can then be used to raise Events or searched in clients (e.g. victor).

The Alarms menu item allows you to configure the following:

- Analytic alarms
- Sensors
- Outputs

Note:
The alarms available to be configured will depend on what Video Analysis type has been enabled in the advanced configuration settings for the camera.

Figure 20 Alarms Tab

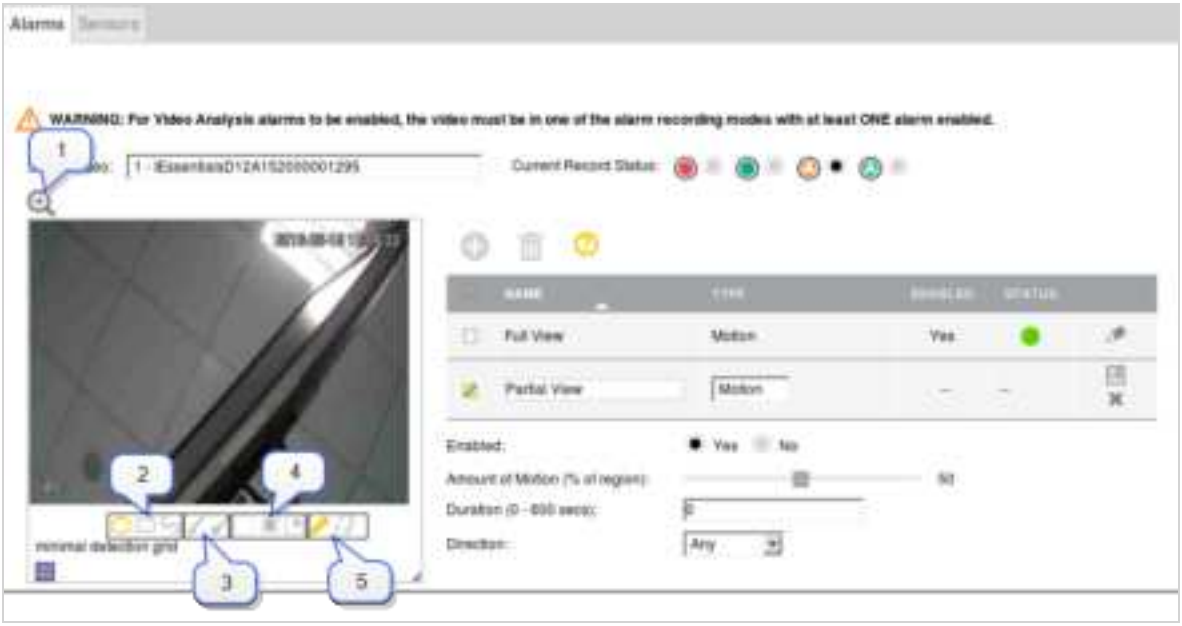


Table 11 Drawing Tools

Tool Type	Options	Description
1. Zoom	Zoom 2X	Doubles the size of the drawing window.
2. Draw Style	Freehand	Draw using freehand by clicking on the window and dragging to draw the shape. The detection area is highlighted yellow.
	Polygon	Draw a polygon by clicking once in the window, and use the lines to form the region of interest. Click again to confirm the line. Double click when the

Tool Type	Options	Description
		shape is complete to finalize the detection area. The detection area is highlighted in yellow.
	Rectangle	Draw a rectangle by clicking once in the window and dragging the cursor over the camera view to highlight the area of interest. The detection area is highlighted in yellow when the mouse button is released.
3. Brush Size	Brush size 4	You can choose the brush size when using free draw to draw a region of interest for Video Intelligence alarms. Select 4x4 to draw using a thin line. **Note** This option is not available when configuring Motion Detection alarms.
	Brush size 8	You can choose the brush size when using free draw to draw a region of interest for Video Intelligence alarms. Select 8x8 to draw using a thick line. **Note** This option is not available when configuring Motion Detection alarms.
4.Selection	Clear	Select Clear to remove all detection areas from the window.
	Select All	Select this option to make the entire window the detection area. The window is highlighted in yellow.
	Invert Selection	Select this option to swap the selected and unselected regions of the window. Highlighted sections of the window are cleared, and previously cleared sections of the window are highlighted.
5. Draw Mode	Draw	Select Draw when you want the draw style to draw a detection area.
	Erase	Select Erase when you want the draw style to erase sections of a detection area.

Motion Detection

Motion Detection Alarms

After you enable Motion Detection on a camera, you can set alarm rules that trigger an event.

Each camera can have up to 10 independent motion alarm rules defined. Each rule has an associated region of interest. In each region of interest you can define the areas in the cameras view that you want to monitor. You can name each alarm rule. It is best to use descriptive names like 'Back Door' or 'Conference Room', as these names make it easier to identify the alarm when using a client rather than an abstract name.

The areas that you want to monitor in a cameras view are configured in the drawing window, a live display of the camera view. To determine the areas of the camera view that you want monitored you need to draw on the window. Use the drawing tools to draw on the Camera Alarm Configuration window.

The status of each Video Intelligence alarm highlighted in the **Status** field. There are three alarm states:

- **Red** - Alarm is disabled. The alarm can be disabled via the **Enabled** option button.
- **Yellow** - Alarm is enabled, however, the recording mode set for the camera does NOT support alarms so the alarms will not be generated. Supported modes are **Only Record on Alarm** or **Recording Always with Alarm On**.
- **Green** - Alarm is enabled and a supported recording mode is selected. Alarms will be generated.

Motion Detection Best Practices

To ensure you get the highest quality results when using Motion Detection on the NVR it is recommended that you adhere to the following:

- An object exhibiting motion needs to be at least 8x8 pixels in size to be detected.
- The color of the object (in grayscale) should be approximately 10-15% different than the background.
- The frame rate of the video should be high enough to capture the object in one or more captured frames.
- Motion Detection events create entries in the victor Application Server database. It is important to ensure that the motion detection parameters are accurate to avoid generating false entries.
- Exclude the Time Stamp region from motion detection, because the time stamp changes constantly and could register as motion.
- Try not to point cameras into sunlight, because high brightness will prevent detection of movement of bright objects such as a person with a white shirt.
- Avoid areas with persistent motion, such as trees, blinking lights, or spinning signs, by using an appropriate region of interest.
- Do not use motion detection on moving cameras, such as PTZ cameras, cameras that vibrate due to wind or other effects, or cameras mounted on moveable fixtures.

Creating a Motion Detection Camera Alarm

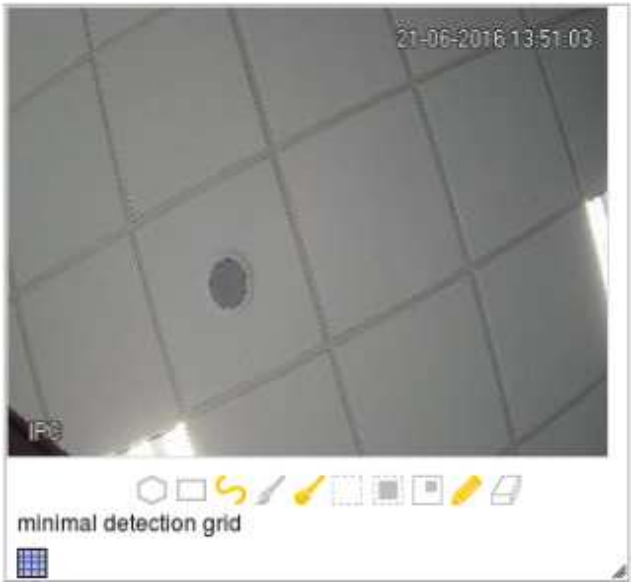
When creating Motion Detection camera alarm you must define an alarm rule. When activity in a camera's view or region of interest satisfies the criteria defined in the rule, an alarm is triggered.

To create a Motion Detection camera alarm you must have Motion Detection enabled on the camera. If you try to add a camera alarm without Motion Detection enabled you will be prompted to edit the camera settings.

Procedure 81
Creating a Motion Detection Camera Alarm

Step	Action
1	Select **Devices** from the main menu.
2	Select **Alarms**. The **Alarms** page displays.
3	Select the camera for which you want to create an alarm, from the **Select Video** dropdown.
4	Click  **Note:** If the Add button is not available, you do not have Motion Detection or Video Intelligence enabled on the camera. Enable Motion Detection to continue.
5	If required you can update the **Current Record Status** from the camera Function & Streams menu. For Motion Detection to be enabled you must select either  Recording Off,  Recording Always,  Only Record on Alarm, or  Recording Always With Alarm On. **Note:** To fully enable motion detection, select Only Record on Alarm, or select recording Always With Alarm On.
6	Enter an alarm **Name** (max 50 characters). **Note:** Use a descriptive name that will make the alarm easy to identify.
7	Ensure **Motion** is the selected **Type**. **Note:** If the **Motion** is not available in the dropdown, you do not have Motion Detection enabled on the camera, instead Video Intelligence is enabled. Enable Motion Detection to continue.
8	Use the drawing tools to draw the Motion Detection region of interest in the Camera Alarm Configuration drawing window. **Note:** You must define a region of interest.

Figure 21 Camera Alarm Configuration Drawing Window



9 Select the **Yes** option button for the **Enabled** field, to enable the alarm.

10 Use the **Amount of Motion (%)** slider to determine the percentage of the region of interest with activity present for the alarm to be triggered. The higher the percentage of the region of interest selected, the lower the number of motion detection results triggered for the alarm. A setting of 0% will trigger an alarm for any size motion.

11 Enter the **Duration (secs)** that there is sustained activity in the region of interest before the alarm is triggered. You can enter values between 0 (default) and 600. A value of 0 seconds will trigger an alarm for motion of any duration.

12 Select the **Direction** from the dropdown that the center of the activity area of motion must move, in order to trigger the alarm. If you select **ANY** it will trigger an alarm for movement in any direction.

13 Select 

- End -

Editing a Motion Detection Camera Alarm

You can make changes to camera alarm settings if required, for example, you can change the region of interest, the percentage of the region of interest that requires activity present, the duration of activity or the direction of movement.

Procedure 82
Editing a Motion Detection Camera Alarm

Step	Action
1	Select **Devices** from the main menu.
2	Select **Alarms**. The Alarms page displays.
3	Select  for the camera alarm you want to edit.
4	Use the drawing tools to edit the Motion Detection region of interest in the Camera Alarm Configuration drawing window.

5	Use the **Amount of Motion (%)** slider to edit he percentage of the region of interest with activity present for the alarm to be triggered. The higher the percentage of the region of interest selected, the lower the number of motion detection results triggered for the alarm. A setting of 0% will trigger an alarm for any size motion.
6	Edit the **Duration (secs)** that there is sustained activity in the region of interest before the alarm is triggered. You can enter values between 0 (default) and 600. A value of 0 seconds will trigger an alarm for motion of any duration.
7	Edit the **Direction** by selecting a different direction from the dropdown. The direction is the center of the activity area of motion must move, in order to trigger the alarm. If you select **ANY** it will trigger an alarm for movement in any direction.
8	Select 

- End -

Disabling a Motion Detection Camera Alarm

When a Motion Detection camera alarm is not needed at present, but will be needed in the future, the alarm can be disabled. The alarm configuration remains the same on the camera for when it is enabled again.

Procedure 83
Disabling a Camera Alarm

Step	Action
1	Select **Devices** from the main menu.
2	Select Alarms. The Alarms page displays.
3	Select the alarm record you want to disable.
4	Click 
5	Select the No option button in the **Enabled** field.
6	Click 

- End -

Deleting a Motion Detection Camera Alarm

When a Motion Detection camera alarm is no longer required, it can be deleted.

Procedure 84
Deleting a Camera Alarm

Step	Action
1	Select **Devices** from the main menu.
2	Select **Alarms**. The Alarms page displays.
3	Select the alarm record you want to delete.
4	Click 

The alarm record is removed from the alarm table.

- End -

Video Intelligence

Video Intelligence Camera Alarms

After enabling Video Intelligence on a camera, you can define alarm rules that trigger an event.

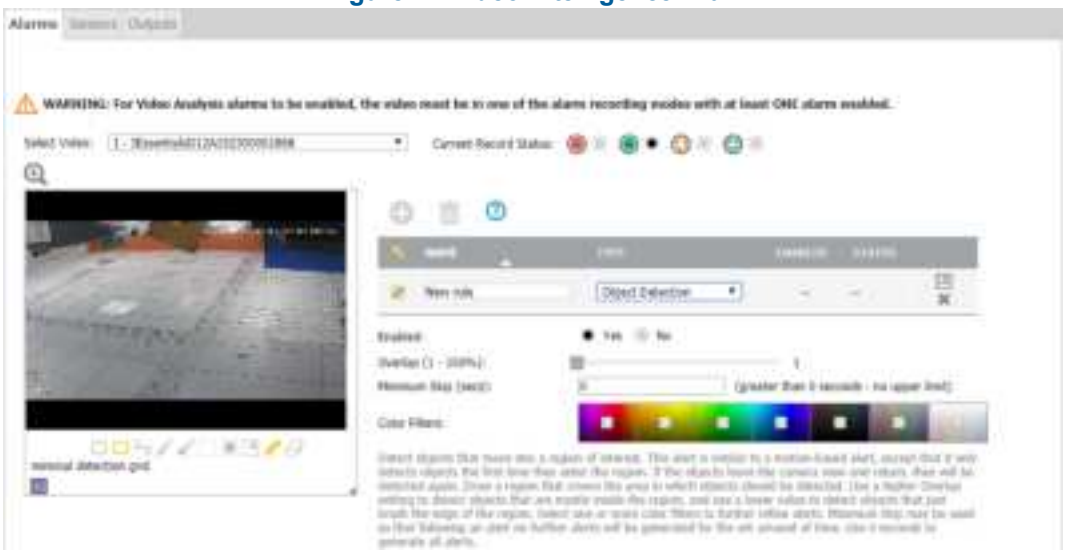
Each camera can have any number of independent Video Intelligence rules. In each rule you can define the areas in the cameras view that you want to monitor. You can name each alarm rule. It is best to use descriptive names like 'Back Door' or 'Conference Room', as these names make it easier to identify the alarm rule in the alerts log better than an abstract name. You can choose the Video Intelligence type for the rule.

The areas that you want to monitor in a cameras view are configured in the Camera Alarm Configuration drawing window, a live display of the camera view. To determine the areas of the camera view that you want monitored you need to draw on the window. Use the drawing tools to draw on the Camera Alarm Configuration window.

The status of each Video Intelligence alarm highlighted in the **Status** field. There are three alarm states:

- **Red** - Alarm is disabled. The alarm can be disabled via the **Enabled** option button.
- **Yellow** - Alarm is enabled, however, the recording mode set for the camera does NOT support alarms so the alarms will not be generated. Supported modes are **Only Record on Alarm** or **Recording Always with Alarm On**.
- **Green** - Alarm is enabled and a supported recording mode is selected. Alarms will be generated.

Figure 22 Video Intelligence Alarm



Video Intelligence Best Practices

To ensure you get the highest quality results when using Video Intelligence on the NVR it is recommended that you adhere to the following:

- An object exhibiting movement or a change in the scene background must be large enough to be detected, i.e. it must be around 1/25 of the image size.
- The color of the object (in grayscale) should be approximately 10-15% different than the background.

- The frame rate of the video should be high enough to capture the object in one or more captured frames.
- Video Intelligence events create entries in the victor Application Server database. It is important to ensure that the Video Intelligence parameters are accurate to avoid generating false log entries.
- Exclude the Time Stamp region from the region of interest, because the time stamp changes constantly and could register as movement.
- Try not to point cameras into sunlight, because high brightness will prevent detection of movement of bright objects such as a person with a white shirt.
- Avoid areas with persistent motion, such as trees, blinking lights, or spinning signs, by using an appropriate region of interest.
- Do not use Video Intelligence on moving cameras, such as PTZ cameras, cameras that vibrate due to wind or other effects, or cameras mounted on moveable fixtures.
- Choose your Video Intelligence alarms selectively. You do not want to create alarms that will trigger a high number of alerts, making the important alerts more difficult to identify.
- Situate cameras to provide the best possible views of the areas of interest, objects and people. It is best to ensure camera views separate objects from people, ensure objects and people take up a larger portion of the camera view, and keep the entire region of interest within the camera's view.
- Use the scheduler to ensure alarm recording statuses are activated at night or during non-working hours. This provides additional coverage during times when staff are not normally available.
- Use staff to help identify regions of interest to monitor based on their observations, for example, of missing merchandise or missing fixtures. Video Intelligence alarms can therefore be configured to monitor areas of potential activity.
- Use searches frequently and watch activity leading up to an alarm being triggered. This may give an indication of suspicious activity and other areas to monitor.
- Tune your alarms regularly to ensure the alarms reflect changes to the environment, for example, objects being rearranged or replaced. Monitoring these changes and re-tuning your alarms will ensure maximum effectiveness of the Video Intelligence alarms and searches.
- Use the new information that Video Intelligence provides to learn and adapt. Use it to implement changes that will improve surveillance and reduce losses, for example, eliminate blind spots, make staff aware of suspicious behavior, or re-design the environment and alarms.

Creating a Video Intelligence Camera Alarm

To create a Video Intelligence camera alarm you must have Video Intelligence enabled on the camera.

Note:
If you try to create a Video Intelligence alarm for a camera without Video Intelligence enabled you will be prompted to edit the camera settings.

Procedure 85
Creating a Video Intelligence Camera Alarm

Step	Action
1	Select **Devices** in the main menu.
2	Select **Alarms**. The Alarms page displays.
3	Select the camera for which you want to create a Video Intelligence alarm from the **Select Video** dropdown.

4 Click 

Note:

If  is not available, you do not have Motion Detection, Video Intelligence or Face Recognition enabled on the camera.

5 If required you can update the **Current Record Status**. For any alarms to be enabled you must select either **Only Record on Alarm** or **Recording Always with Alarm On**.

6 Enter an alarm **Name** (max 50 characters).

Note:
Use a descriptive name that will make the alarm easy to identify.

7 Select the Video Intelligence **Type** from the dropdown:

a **Object Detection** - Used to detect people or objects moving into a region of interest. This alarm is similar to a motion alarm, but only detects people or objects the first time they enter the region of interest. A separate event is generated for each object that enters the region, even if the objects move into the region at the same time, unlike motion detection that generates one event.

b **Abandoned / Removed** - Used to find changes to the background of a scene in a region of interest, for example, use it to detect when a stationary object was placed, moved or removed. Draw the region of interest that contains all of the area you want to search for changes.

c **Direction** - Used to detect objects moving in a certain direction through a region of interest, for example, a car traveling the wrong way on a road. It is best to use a thin region of interest to detect the direction of an object.

d **Linger** - Used to detect objects loitering in a region of interest. An object is lingering if it remains in the region of interest. The minimum amount of time an object must linger before being included in the results can be defined and you can draw a region in the area where you want to detect objects lingering. Use a higher Overlap setting to avoid detecting objects lingering nearby.

e **Dwell**: Used to detect objects lagging or tarrying in a region of interest. An object is dwelling if it is mostly stationary. The minimum amount of time an object must dwell before being included in the results can be defined. Draw a region in the area where you want to detect objects dwelling. Use a higher Overlap setting to avoid detecting objects dwelling nearby.

f **Queue Analysis**: Used to monitor length of queues, for example, in a point of sale environment or highway tollbooth. Alarms can be triggered for when a queue grows beyond or falls below a specified threshold.

g **Perimeter**: Used to detect when objects enter a protected area through a perimeter area, or detect when an object is in the perimeter area for too long. Draw regions of interest to define the perimeter area and the protected area. You must also draw regions of interest to define the minimum size and the maximum size of objects that can trigger the perimeter alarm.

h **Crowd Formation**: Used to detect and raise an alarm when a crowd forms in a specified region of interest. A minimum crowd size can be specified to trigger alarms only when the specified size is reached. For example if a particular region should not have more than 2 people at any given time the minimum crowd size should be set to 3.

i **Exit** - Used to detect objects exiting a camera view through a region of interest, for example, a doorway or threshold. It is best to draw the region of interest around the doorway or threshold to include areas in which the door can move or objects can be seen, for example, glass. This will exclude objects that can be seen in the region of interest but does not pass through it.

j **Enter** - Used to detect objects entering a camera view through a region of interest, for example, a doorway or threshold. It is best to draw the region of interest around the doorway or threshold to include areas in which the door can move or objects can be seen, for example, glass. This will exclude objects that can be seen in the region of interest but does not pass through it.

Note:
If these types are not available in the dropdown, you do not have Video Intelligence enabled on the camera, instead Motion Detection is enabled. Enable Video Intelligence to continue.

8 Use the drawing tools to draw the Video Intelligence region of interest in the Camera Alarm Configuration drawing window.

Note:
• You must define a region of interest.
• Queue Analysis and Perimeter require multiple regions of interest.

9 Enable the alarm by selecting the **Yes** option button for the **Enabled** field.

10 Complete the alarm configuration fields. Depending on the Video Intelligence type selected there will be different alarm parameters to configure.

The Color Filters parameter allows you to limit your search results to the specified color(s) only. The color filters parameter is not available on Abandoned / Removed, Perimeter, Queue Analysis, or Crowd Formation. Leaving the color filter parameter blank has the equivalent function of 'ANY' color.

Object Detection

a Overlap (%) - The amount of a detected object that must be in the region of interest before an alarm is triggered. Use a higher setting to detect objects that are mostly inside the region, and use a lower value to find objects that just brush the edge of the region.

Abandoned / Removed

a Overlap (%) - The amount of background change that must be in the region of interest before an alarm is triggered. Use a higher setting to avoid finding nearby changes or changes that are not completely in the region of interest.

b Minimum Skip (secs) - This is the period of time after an alert, during which no further alerts are generated. A setting of 0 seconds triggers all alerts.

c Fast Trigger - Enable Fast trigger to reduce the time required to assess if an object is abandoned or removed. As a result, alerts trigger more quickly, but the number of false alarms also increases.

d Wipeout Amount Changed (%) - The percentage of the region of interest that must change before an alarm is triggered. Adjust to look for either a larger or smaller change in the region.

e Wipeout Within (secs) - Time frame within which the change must occur in order to trigger the alarm. A setting of 0 seconds represents instantaneous change.

Direction

a Overlap (%) - The amount of a detected object that must be in the region of interest while moving in the specified direction for an alarm to be triggered.

b Direction - This is the general direction the object must move in to trigger an alarm. You can choose North, South, East or West.

c Traversal Time- This is the maximum amount of time which an object can take to traverse most of the region before the alarm is triggered. This is to exclude objects that move too slow.

Linger

a Overlap (%) - The amount of detected object that must be in the region of interest while lingering for an alarm to be triggered. Use a higher setting to avoid detecting objects lingering nearby.

b Linger Time- The minimum amount of time an object lingers before the alarm is triggered.

Dwell

a Overlap (%) - The amount of a detected object that must dwell in the region of interest for an alarm to be triggered.

b Dwell Time - This is the minimum amount of time that an object must dwell in the region of interest before the alarm is triggered.

Queue Analysis

a Select Area - Additional tools display when using queue analysis to highlight zones of interest; Short, Medium and Long. Use these to define the zones of interest that must be occupied to form a short medium and long queue, all 3 zones must be defined, regardless of the queue length. Each selection is highlighted via a different color (Short = green, Medium = yellow and Long = purple).

b Overlap (%) - The amount of detected object that must be in the region of interest to be identified as a person in a queue.

c Queue Length - The required minimum length for an alarm to be generated. The following options are available:

- **Empty**: this will generate an alarm when no objects are present in the designated regions of interest.
- **Not Empty**: this will generate an alarm when an object(s) is present in the designated regions of interest.
- **Short**: this will generate an alarm when objects are present in the short designated region of interest and meet the overlap requirements.
- **Medium**: this will generate an alarm when objects are present in both the short and medium designated regions of interest and meet the overlap requirements.
- **Long**: this will generate an alarm when objects are present in the short, medium and long designated regions of interest and meet the overlap requirements.

Perimeter

a Select Area - Additional tools display when using perimeter to highlight zones of interest. Use these tools to define the zones of interest for the protected area, the perimeter area, the minimum object size, and the maximum object size. Each selection is highlighted via a different color (perimeter area = green, protected area = yellow, minimum object size = purple, and maximum object size = red).

b Linger Time- The minimum amount of time an object lingers before the alarm is triggered.

Crowd Formation

a Overlap (%) - The amount of detected object that must be in the region of interest to be considered for determining the crowd size.

b Minimum Crowd Size - The minimum number of people that must be present to generate an alarm. This can be between 2-50 people.

Exit

a Overlap (%) - The amount of detected object that must be in the region of interest when the object leaves the scene for an alarm to be triggered. The object must appear in the scene while being outside the region of interest by the same amount. For best results select a higher overlap setting.

Enter

a Overlap (%) - The amount of detected object that must be in the region of interest when it first appears in the camera view. The object must leave the region of interest by the same amount before an alarm is triggered. For best results select a higher overlap setting.

11 Click 

- End -

Editing a Video Intelligence Camera Alarm

You can make changes to Video Intelligence camera alarm rules if required, for example, you can change the region of interest and update the parameters associated with that rule's Video Intelligence alarm type.

Procedure 86
Editing a Motion Detection Camera Alarm

Step	Action
1	Select **Devices** from the main menu.
2	Select **Alarms**. The Alarms page displays.
3	Select  for the camera alarm you want to edit.
4	Use the drawing tools to edit the selected alarm's region of interest in the drawing window.
5	Edit the alarm's parameters. These will be different for each type of Video Intelligence alarm. **Note:** You cannot update the Name of the alarm. If you must change the alarm name, you must create a new alarm with the new name, assign it the same parameters and delete the old alarm.
6	Select 

- End -

Disabling Video Intelligence Camera Alarm

When a Video Intelligence camera alarm is not needed at present, but will be needed in the future, the alarm can be disabled. The alarm configuration remains the same for when it is enabled again. You can also edit the alarm configuration parameters while the alarm is disabled, once enabled the changes will take effect.

Procedure 87
Disabling a Camera Alarm

Step	Action
1	Select **Devices** from the main menu.
2	Select **Alarms**.

The Alarms page displays.

3 Select the alarm record you want to disable.

4 Click 

5 Select the **No** option button in the **Enabled** field.

6 Click 

- End -

Deleting a Video Intelligence Camera Alarm

When a camera alarm is no longer required, it can be deleted.

Procedure 88
Deleting a Video Intelligence Camera Alarm

Step	Action
1	Select **Devices** from the main menu.
2	Select **Alarms**. The Alarms page displays
3	Select the alarm record you want to delete.
4	Click  The alarm record is removed from the alarm table.

- End -

Face Recognition

Face recognition is a licensable feature and works by detecting faces and comparing them to those stored in the database of enrolled faces. If a match is found, that face is labeled with the corresponding name, otherwise it will be labeled as unrecognized. When face recognition is enabled on a camera, you can create face recognition rules for that camera. Alarm rules can be configured to trigger, based on detected faces, with additional filtering options for recognized faces.

When a face recognition alarm is configured, either to detect all faces (the default setting), or with an exclude list, the alarm triggers when an unrecognized face is detected within the region of interest. Additional unrecognized faces within the region of interest will not trigger another alarm, unless the region of interest has been clear of unrecognized faces for a brief period of time.

Depending on camera conditions, a face recognition alarm can trigger after a face detection alarm triggers. This double-alarm occurs when conditions cause a delay in face recognition, which causes the face detection alarm to trigger instead. After the face is recognized, the face recognition alarm triggers.

Note:
Before configuring face recognition, the NVR and victor Application Server must be connected to the same NTP server.

Face Recognition Best Practices

To ensure you get the highest quality results when using Face Recognition on the NVR it is recommended that camera configuration and lighting conditions are setup to provide reasonable contrast while avoiding significant amounts of motion blur and image noise. If face detection or recognition accuracy are unsatisfactory, users should consider these factors in addition to portrait quality and the current recognition sensitivity settings. Face detection and face recognition settings can be adjusted from the **Function & Streams** tab of the **Advanced Camera Configuration** page.

Note:
To improve portrait quality you must minimize distortion, this can be achieved by ensuring the camera is not too close to the individual being photographed. You can also vary the type of camera being used for additional portraits.

To increase alarm accuracy, the following guidelines are recommended:

- Constrain the region of interest to an area where faces are pointed at the camera, thus making them easier to recognize.
- Adjust camera settings, orientation, and lighting according to best practices.
- Re-enroll more, better, and more recent portrait photos.
- Reduce the camera's detection sensitivity.
- Increase the camera's recognition sensitivity.

Procedure 89
Configure Face Recognition

Step	Action
1	Select **Devices** from the main menu.
2	Select **Alarms**. The Alarms page displays
3	Select the camera for which you want to create a Face Recognition alarm from the **Select Video** dropdown.
4	Click  **Note:** If  is not available, you do not have Motion Detection, Video Intelligence or Face Recognition enabled on the camera.
5	If required you can update the **Current Record Status**. For Face recognition alarms to be enabled you must select either **Only Record on Alarm** or **Recording Always with Alarm On**.
6	Enter an alarm **Name** (max 50 characters). **Note:** Use a descriptive name that will make the alarm easy to identify.
7	Select the **Enabled** or **Disabled** option button as required.
8	Select the **Include** option button in the List Type for the alarm to trigger if someone in the search list is detected.

Or

Select the **Exclude** option button in the List Type for the alarm to trigger when someone not in the search list is detected.

9 Select entries from the Enrollment List to be included/excluded in the Search List using the  and  buttons.

10 Click 

- End -

License Plate Recognition

License plate recognition is a licensable feature and works by detecting license plate numbers and comparing them to those listed in a search list. A license plate recognition alarm is configured to trigger in one of three ways.

- All - Triggers an alarm when any license plate is detected.
- Include - Triggers an alarm when a license plate from the search list is detected.
- Exclude - Triggers an alarm when a license plate not from the search list is detected.

License plate recognition alarms also support the use of wildcard characters and fuzzy matching.

Note:
In some regions, License Plate Recognition (LPR) is also called Automatic Number Plate Recognition (ANPR).

Wildcard Characters

When configuring a License Plate Recognition alarm, use wildcard characters to represent unknown or undefined characters in a license plate number.

Wildcard Character	Description	Example
*	Match zero, one or multiple characters.	ABC12*
?	Match any one character.	ABC12?

In the examples above, the asterisk character (*) represents zero or more characters. During a license plate search using *, an alarm will trigger for each license plate that contains the defined characters, ABC12, as well as any additional characters. The question mark character (?) represents one character. During a license plate search using ?, an alarm will trigger for each license plate that contains the defined characters, ABC12, and one additional character.

Fuzzy Matching

Fuzzy match enables matching on commonly mis-recognized characters. Depending on environmental conditions, visually similar characters such as B and 8 can be misread by a camera. When fuzzy matching is enabled, characters from a fuzzy match group can be matched to any other character from the same group. The following character groups are supported for fuzzy matching.

Fuzzy Match Groups
0, D, O, Q

Fuzzy Match Groups
1, 7, I
2, Z
8, B

Creating a License Plate Recognition Alarm

When creating a License Plate Recognition camera alarm you must define an alarm rule. When activity in the camera's view or region of interest satisfies the criteria defined in the rule, an alarm is triggered.

To create a License Plate Recognition camera alarm you must have License Plate Recognition enabled on the camera. If you try to add a camera alarm without License Plate Recognition enabled you will be prompted to edit the camera settings.

Procedure 90
Creating a License Plate Recognition Alarm

Step	Action
1	Select **Devices** from the main menu.
2	Select **Alarms** to open the Alarms page.
3	Select the camera that you want to create a license plate recognition alarm for from the **Select Video** dropdown menu.
4	Click  If required you can update the **Current Record Status**. For license plate recognition to be enabled you must select either  (Only Record on Alarm) or  (Recording Always with Alarm On).
5	Enter a name for the alarm (maximum 50 characters). **Note:** Use a descriptive name that will make the alarm easy to identity.
6	Select the **Yes** option button to enable the alarm.
7	Select the required **Overlap** range. **Note:** The Overlap range is used to determine how much of the license plate needs to be in the region of interest in order to trigger an alarm. For example, if overlap is set to 1%, only a very small proportion of the license plate would need to enter the area of interest to trigger the alarm. If overlap is set to 100% the entire license plate would need to be in the region of interest to trigger an alarm.
8	Select a **Alarm Type**: • All - triggers an alarm when any license plate is detected. • Include - triggers an alarm if a license plate in the search list is detected. • Exclude - triggers an alarm if a license plate not in the search list is detected.
9	(Optional) Select the **Fuzzy Match** checkbox if required.

10 Add license plate numbers to the License list.

a Click 

b Enter a license plate number in the **Plate Number** field.

c Repeat steps a and b as necessary.

Or

Import a list of license plate numbers.

a Click **Choose File**.

b Navigate to the required text file.

c Select **Open**.

11 Use the drawing tools to select an alarm's region of interest in the drawing window.

12 Click 

- End -

Editing a License Plate Recognition Alarm

Changes can be made to License Plate Recognition alarm rules if required. For example, the region of interest can be changed and associated parameters associated with that rule's license plate recognition alarm type.

Procedure 91
Editing a License Plate Recognition Alarm

Step	Action
1	Select **Devices** from the main menu.
2	Select **Alarms**. Select  for the camera alarm you want to edit
3	Select an **Alarm Type**: • All - triggers an alarm when any license plate is detected. • Include - triggers an alarm if a license plate in the search list is detected. • Exclude - triggers an alarm if a license plate not in the search list is detected.
4	Use the drawing tools to edit the selected alarm's region of interest in the drawing window.
5	Click 

- End -

Disabling a License Plate Recognition Alarm

If a license plate recognition alarm is not currently needed, but might be needed in the future, the alarm can be temporarily disabled. The alarm configuration remains the same for when it is enabled again. Alarm configurations can also be edited while the alarm is disabled.

Procedure 92
Disabling a License Plate Recognition Alarm

Step	Action
1	Select **Devices** from the main menu.
2	Select **Alarms**. The Alarms page displays.
3	Select  for the camera alarm you want to disable.
4	Select the **No** option button in the **Enabled** field.
5	Click 

- End -

Deleting a License Plate Recognition Alarm

When a camera alarm is no longer required, it can be deleted.

Procedure 93
Deleting a License Plate Recognition Alarm

Step	Action
1	Select **Devices** from the main menu
2	Select **Alarms** The Alarms page displays.
3	Select the alarm record you want to delete.
4	Click  The alarm record is removed from the alarm table.

- End -

Edge Analytics

Edge Analytics are analytics that take place on the camera rather than the recorder. The camera itself carries out the processing on its video streams.

Edge Based Analytic Alarms

The configuration of analytic camera alarms must take place using the camera's interface. Refer to the camera's User's Guide for information. Once the edge device has configured alarms, the NVR can be configured to monitor for these alarms to fire. The fired alarms can trigger recording, can be sent via email, and will be recorded in the victor activity log. You can enable or disable edge-based camera alarms using the NVR Administrator Interface.

There are three types of edge-based analytic events supported by the NVR; motion detection (detecting motion in the scene), face detection (detecting presence of a face in the scene) and blur detection (detecting that the scene is blurred).

When you have configured the alarm parameters for the camera, the alarms are available to enable or disable from the NVR Administrator interface.

The status of each Edge Based alarm is highlighted in the **Status** field. There are three alarm states:

- **Red** - Alarm is disabled. The alarm can be disabled via the **Enabled** option button.
- **Yellow** - Alarm is enabled, however, the recording mode set for the camera does NOT support alarms so the alarms will not be generated. Supported modes are **Only Record on Alarm** or **Recording Always with Alarm On**.
- **Green** - Alarm is enabled and a supported recording mode is selected. Alarms will be generated.

Edge Analytics Best Practices

To ensure you get the highest quality results when using Edge Analytics on the NVR it is recommended that you adhere to the following:

- Edge based events create entries in the victor Application Server database. It is important to ensure that the edge analytic parameters are accurate to avoid generating false entries.
- Edge based metadata is recorded in the NVR occupying storage space. It is important to ensure that the edge analytic parameters are configured accurately to prevent occupying storage space unnecessarily.
- Edge based events and metadata are created by the camera's analytics. Refer to the camera's Installation and User manual for configuring analytics to ensure proper operation.

Edge Based Analytic Metadata

After enabling edge-based analytics for a camera, edge-based analytic alarms can be triggered. You must enable Face Detection or Motion Detection Metadata in the alarms table to allow camera-based search based on this metadata in victor unified client.

Note:
Face and Motion Detection metadata will be recorded if the camera recording status is set to one of the three recording modes.

Enabling/Disabling an Edge Based Camera Alarm

You can enable a camera alarm from the Alarms page. Before enabling the alarm you must ensure all alarm parameters are configured on the camera using the camera's interface. When an edge-based camera alarm is not needed at present, but will be needed in the future, the alarm can be disabled. The alarm configuration remains the same on the camera for when it is enabled again.

Procedure 94
Enabling/Disabling Edge Based Camera Alarms and Metadata

Step	Action
1	Select **Devices** from the main menu.
2	Select **Alarms**. The Alarms page displays.
3	Select the alarm/metadata record you want to enable/disable.
4	Click 
5	To enable a camera alarm select the **Enabled** option button.

Or

To disable a camera alarm select the **Disabled** option button.

6 Click 

- End -

Sensors

Dry Contact Sensors can be added to the NVR as standalone devices. Sensors can be configured to drive the following actions -

- **Camera Recording** - A change of input state will initiate recording on the selected camera (the camera must have its recording mode set to Record-Only-On-Alarm). The length of the recording is dictated by the Alarm Pre Buffer, the selected sensor input state trigger time (if supported) and the Alarm Post Buffer.
- **Camera Start Recording** - A change of input state will initiate recording on the selected camera (the camera must have its recording mode set to Record-Only-On-Alarm). Recording (including Alarm Pre Buffer) will begin and continue indefinitely.
- **Camera Stop Recording** - A change of input state will cause recording to stop after the duration of the Alarm Pre Buffer.

Note:
The combination of the actions **Camera Start Recording** and **Camera Stop Recording** allow video recording to be configured to occur throughout the duration of a dry contact being triggered. For example -

For a door with a dry contact sensor fitted, video recording can be configured to last the duration of the door being open with the combination of two sensor events. To initiate recording a sensor entry is created using the Camera Start Recording action when the state changes to high as the door is opened. A second sensor entry is created using the Camera Stop Recording action when the state changes to low as the door is closed. This will result in the following behavior -

Door opens - Alarm Pre Buffer + state change to high, video starts recording.

Door closes - State change to low + Alarm Post Buffer, video stops recording.

- **PTZ to preset** - A change of input state will cause the selected camera to move to a designated PTZ preset.

Note:
Before adding a sensor you must enable dry contact sensors.

Procedure 95
Adding a Sensor

Step	Action
1	Select **Devices** from the main menu.
2	Select **Alarms**. The Alarms page displays.
3	Select the **Sensors** tab.

4 Click  above the Sensor table (top).

5 Enter the Sensor **Name**.

6 Select the **Yes** option button to enable the sensor.

Or

Select the **No** option button to disable the sensor.

7 Click  above the Input table (middle).

8 Select the input from the **Input** dropdown.

9 Select the state from the **State** dropdown.

10 Click  .

The Interval (Sec) field displays.

11 Enter the interval value in the **Interval (Sec)** field if required.

12 Repeat steps 7-10 to add additional inputs. To remove an input select the appropriate checkbox and click 

13 Click  above the Action table (bottom)

14 Select an action from the **Action** dropdown. If PTZ to Preset is selected the Value dropdown displays.

15 Select the device from the **Device** dropdown.

16 (PTZ to Preset only) Select the preset number from the **Value** dropdown.

17 Repeat steps 12-14 to add additional actions. To remove an action select the appropriate checkbox and click 

18 Click 

- End -

Procedure 96
Deleting a Sensor

Step	Action
1	Select **Devices** from the main menu.
2	Select **Alarms**. The Alarms page opens.
3	Select the **Sensors** tab.
4	Select the appropriate checkbox of the sensor you want to delete from the Sensors table.
5	Click 

- End -

Outputs

From the Outputs menu, you can add outputs from selected devices to the VideoEdge. You can configure a name and pulse time for each relay index that a device has. After you configure an output, you can switch it on and off, or you can enable a pulse, which switches the device on for a specified amount of time.

Supported cameras

The following table lists the Illustra cameras and camera firmware versions that are compatible with VideoEdge Outputs.

Note:
For information about camera limitations, and an updated list of cameras that support Outputs, refer to the *VideoEdge Camera Handler Release Notes*.

Camera Model	Firmware Version
Illustra Pro 2MP, 3MP, and 5MP Fixed Mini-Dome	1.3.2 or above
Illustra Pro i625 PTZ, 30x PTZ	2.1.7 or above
Illustra Flex 3MP Mini-Dome, Bullet, Box	SS004.01.02 or above
Illustra Flex i600 or i800F	3.1.5 or above
Illustra Pro Bullet LT, Micro, Compact	2.1.5 or above
Illustra Pro 12MP Fisheye	SS002.01.00.00.0620 or above
Illustra Flex PTZ	SS002.01.00.00.0620 or above

Table 12 Camera firmware compatibility for Outputs

Procedure 97
Adding an Output

Step	Action
1	Select **Devices** from the main menu.
2	Select **Alarms**. The Alarms page displays.
3	Select the **Outputs** tab.
4	Add an output device. a At the top of the Outputs page, click  b Select a device from the **Output Device** dropdown list. c Enter a name in the **Output Name** field. d (Optional) Edit the **Pulse (seconds)** field. **Note:** You can enter a Pulse value from 0 seconds - 60 seconds. e Select to add the Output Device
5	Click 

- End -

Procedure 98
Signaling an Output

Step	Action
1	Select **Devices** from the main menu.
2	Select **Alarms**. The Alarms page displays.
3	Select the **Outputs** tab.
4	Select an output device.
5	Select a signal to send to the output: • **On** - Turns the selected output on • **Off** - Turns the selected output off • **Pulse** - Turns the selected output on for a specified amount of time
6	Click 

- End -

Procedure 99
Deleting an Output

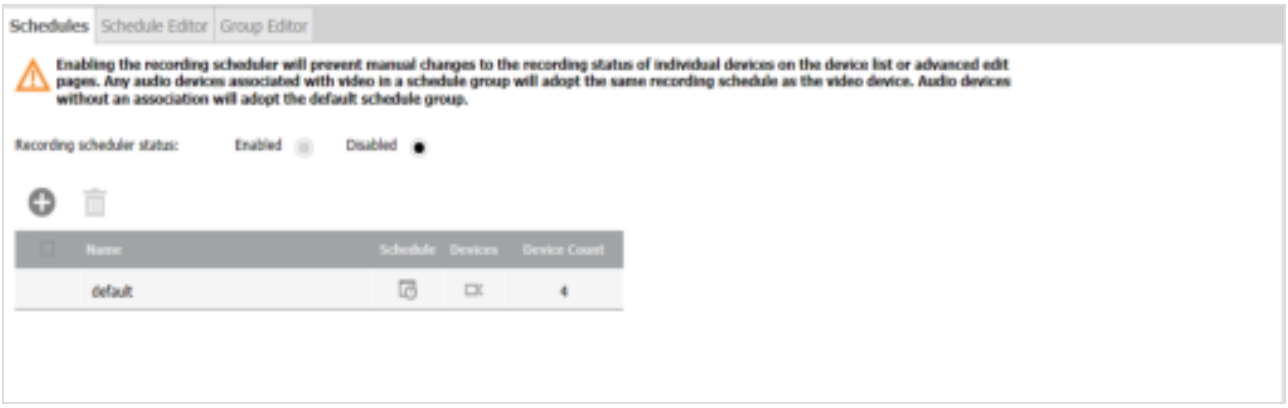
Step	Action
1	Select **Devices** from the main menu.
2	Select **Alarms**. The Alarms page opens.
3	Select the **Outputs** tab.
4	Select  for the output that you want to delete.

- End -

Scheduler

The Scheduler section describes how to set up and enable the camera scheduler. By using a camera schedule you can set the NVR to automatically change recording modes hourly. You can define camera recording modes and set camera recording times per scheduler group. You can enable or disable the camera scheduler when necessary.

Figure 23 Scheduler Page



There are three tabs within the Scheduler menu:

- **Schedules**: Where you can enable the scheduler and create or remove schedules.
- **Scheduler Editor**: Where you set the schedule times and recording modes for each period
- **Group Editor**: Where you select which cameras belong to a schedule. You can create multiple schedule groups where you can assign different cameras with different schedule times and record modes.

To create a recording schedule you need to:

1 Set up your scheduler group(s).

2 Set the schedule times and recording modes for the schedule group(s).

3 Assign camera(s) to the schedule group(s).

Schedules

Where you can enable the scheduler and create or remove schedules.

Procedure 100
Creating a Recording Schedule

Step	Action
1	Select **Devices** from the main menu.
2	Select **Scheduler**. The Schedules page displays.
3	Click  The new group is added to the schedule groups table.
4	Enter the Schedule **Name**.

5 Click 

6 Select **Edit Group Times**  , in the schedule group record you want to configure.

The Schedule Editor tab displays.

7 Select the option buttons representing the day(s) for which you want to set the recording times and the recording mode.

8 Select the required **Recording Mode** option button;

- **Recording Off**
- **Recording Always**
- **Only Record on Alarm**
- **Recording always with alarms**

9 Select the times you want the selected recording mode to be active.

10 Click 

11 To set other recording modes for different days and times, repeat steps 5 to 8 until the Schedule Times chart is set as required for the recording schedule group.

12 Select the **Group Editor** tab.

13 Select the cameras you want to be in this schedule group by selecting the checkbox(es) for the cameras from the **All other devices** list and use the arrow to move them to the **This group** list.

Note:
Each camera can only be assigned to one schedule.

14 Click 

15 Repeat steps 3 to 12 to configure additional schedule groups for the camera schedule.

- End -

Enabling/Disabling the Recording Schedule

Procedure 101
Enabling/Disabling a Camera Schedule

Step	Action
1	Select **Devices** from the main menu.
2	Select **Scheduler**. The Schedules page displays.
3	To enable the camera schedule, select the **Recording scheduler status: Enabled** option button. Or To disable the camera schedule, select the **Recording scheduler status: Disabled** option button.

- End -

Editing the Recording Schedule

You can edit all aspects of the recording schedule as required.

Edit the Group Name

You may want to update the schedule group name to reflect changes made within the schedule group.

Procedure 102
Editing the Schedule Group Name

Step	Action
1	Select **Devices** from the main menu.
2	Select **Scheduler**. The Schedules page displays.
3	Click  in the group record that you want to rename. The group name field becomes editable.
4	Enter the new group name.
5	Click 

- End -

Edit the Recording Scheduler for a Group

Within the recording schedule associated to a group you can update the recording days and times as your needs change. The following procedure describes how to edit the recording schedule.

Procedure 103
Editing the Recording Schedule for a Group

Step	Action
1	Select **Devices** from the main menu
2	Select **Scheduler**. The Schedules page displays
3	Select the **Schedule Editor** tab.
4	Select the group you want to edit from the **Group ID** drop down.
5	Edit the recording schedule as required by selecting the day(s), the recording mode and start and end hours.
6	Click 
7	If further changes are required repeat Steps 5 and 6.

- End -

Edit the Cameras Assigned to a Schedule Group

You can add or remove cameras to/from a schedule group when needed. This procedure describes how to edit cameras assigned to a specific schedule group.

Procedure 104
Editing the Cameras Assigned to a Schedule Group

Step	Action
1	Select **Devices** from the main menu.
2	Select **Scheduler**. The Schedules page displays.
3	Select the **Group Editor** tab.
4	Select the group you want to edit from the dropdown.
5	Select the required camera(s) checkbox(es) and use the  and  arrows to move cameras between the **All other Cameras list** and the **This group** list, until the cameras you want to be assigned to the selected recording group are in the **This group** list.
6	Click 

- End -

Remove a Schedule Group

You can remove unwanted schedule groups when they are no longer needed.

Note:
If you remove a schedule, the cameras in this schedule will be assigned back to the default scheduler group.

Procedure 105
Removing a Schedule Group

Step	Action
1	Select **Devices** from the main menu.
2	Select **Scheduler**. The Schedules page displays.
3	Select the checkbox in the group record(s) that you want to delete.
4	Select  The group is removed from the Schedule groups table.

- End -

Security

When an IP camera is added to a NVR, the server uses the manufacturer's default communication and security settings to communicate with the camera. Administrators can change the default settings, however, when these are changed the NVR can no longer communicate with the camera using the default settings.

If you change the security settings for a camera or a number of cameras, usually through direct web interfaces, you need to create a Security Group for those cameras and assign it the same password.

The camera Security Groups feature is applicable to IP cameras and encoders only. Analog cameras connected directly to the NVR do not have password capabilities.

Note:
1. The Security Groups feature does not change the password on the camera. It determines what password is used by the NVR to communicate with cameras.
2. You must change the password on the camera before you change the password for the security group using the Security feature, otherwise those cameras will not be able to connect to the NVR.

In addition to configuring the username and password you can also configure the port number and protocol (Security Level) used for communications.

Note:
1. Port number: This is either the HTTP or HTTPS port number which has been specified for communication. The default port number will be used to communicate with the camera unless you specify a port. You must ensure the port number is correctly configured on the corresponding camera(s) for communication to be established.
2.Security Level: This is the protocol which will be used to communicate with the camera(s).

Figure 24 Security Tab

Create a Security Group

If a password has been changed for a camera or a group of cameras, the NVR is no longer able to communicate with the camera(s). You must create a security group containing the new password and assign the camera(s) with this password to it.

Procedure 106
Creating a Security Group

Step	Action
1	Select **Devices** from the main menu.
2	Select **Security**. The Security tab displays.
3	Select  The Security Group window opens.
4	Enter a **Group Name**.
5	Enter a **Description**.
6	Enter a **Username**.
7	Enter a **Password**. **Note:** • This is the camera username and password that VideoEdge uses to connect to the cameras in this security group. • To use the camera default credentials, do not enter a Username or Password.
8	(Optional) Click and hold the password reveal icon,  , to view the password.
9	(Optional) Configure Advanced settings. a Select **Advanced**. b Select the **Security Level** from the dropdown. c Enter the **Port** number. **Note:** Ensure the **Default** checkbox is selected if you want to use the default port number. d Select the **ONVIF RTSP Authentication** checkbox if the cameras in this group use ONVIF communication protocols.
10	Select the cameras you want to assign to the security group by using the  and  buttons.
11	Click  **Note:** If you are editing the security group for a camera attached by an encoder, all cameras connected to the encoder will have the same password. Editing the security group for one camera on an encoder will result in all cameras on that encoder being assigned a new password. A message opens warning that multiple cameras will be updated.

- End -

Editing a Security Group

Security groups can be edited using the security tab.

Procedure 107
Editing a Security Group

Step	Action
1	Select **Devices** from the main menu.
2	Select **Security**. The **Security** tab displays.
3	Select  in the group record you want to edit. The Security Group window opens.
4	Edit the **Group Name** as required.
5	Edit the **Description** as required.
6	(Optional) Edit the username and password. a Select the **Set Username/Password** checkbox. b Enter a **Username**. c Enter a **Password**
7	Edit the **Security Level** using the dropdown as required.
8	Edit the **Port** as required.
9	Select the cameras you want to assign to the security group by using the  and  buttons.
10	Click 

- End -

Deleting a Security Group

When you have deleted a security group, the NVR will try to communicate with the cameras which made up the deleted group using the manufacturer's default credentials. Prior to deleting a security group, you must reconfigure each camera in the group to use the manufacturer's default credentials to ensure video streaming / recording is not interrupted. Alternatively, you can remove cameras from the security group, or reassign cameras to a new security group.

Procedure 108
Deleting a Security Group

Step	Action
1	Select **Devices** from the main menu.
2	Select **Security**. The **Security** tab displays.
3	Select the checkbox in the security group record that you want to remove.
4	Click 

- End -

Discovery

The Device Discovery feature automatically discovers video devices on the network that can be added to the NVR.

Multiple devices can be added to the NVR until the number of video licenses on the NVR is reached.

Video devices will be added with a default recording status of Record Always.

To discover devices, the NVR uses standard discovery protocols such as: MDNS, UPnP/SSDP, and ONVIF/WS-Discovery. The NVR will discover video devices on the network that have these standard protocols enabled.

The NVR discovery feature supports changing the IP addresses of AD cameras.

By default, the NVR will discover video devices using the device manufacturer's default username and password. If video devices are configured with another username and password, then Security Groups can be configured on the NVR to allow for those devices to be discovered.

NVR Discovery: By default, the NVR advertises itself on the network via UPnP/SSDP. This feature allows the Victor client to discover VideoEdge recorders.

Figure 25 Discovery Page

Discovered Devices

When the discovered devices tab is selected, information on all discovered devices is displayed. From this tab the user add a camera, change the IP address of cameras, refresh the discovered device list, create a security group, clear the list of discovered devices and view camera snapshots.

Auto-Discovery is enabled by default and can be disabled if required in the discovered devices tab.

Note:
- Enabling or disabling device discovery will also enable or disable NVR discovery.
- Auto Discovery is automatically disabled after 12 hours.

Camera snapshots can be viewed by clicking the snapshot icon in the Snapshot column for the device of interest.

Clicking the ↻ icon to will cause the NVR to probe for new devices and list all discovered devices.

Clear Table

Clicking **Clear Table** will cause the NVR to clear the list of discovered devices and begin discovering devices again.

For example, clearing the list of discovered devices can be useful if:

- user accounts are changed on the video device
- the number of encoder inputs are changed on the video device.

After the list of discovered devices is cleared, the NVR will re-discover devices with the new user account and learn the new encoder configuration.

Procedure 109
Add a Device using Auto-Discovery

Step	Action
1	Select **Devices** from the main menu.
2	Select **Discovery**.
3	Select the **Enabled** button to enable Auto Discovery.
4	(Optional) Use the **Show inputs** dropdown to display more results per page.
5	Select the checkboxes for the devices that you want to add to the NVR from the Discovered device list.
6	(Optional) Edit the device **Name**. The new device name will be applied when the device is added.
7	(Optional) Edit the **Add New Device Settings**. • De-select the **Default Associations** checkbox if video / audio association is not required. • De-select the **Enable Smart Search (Motion Metadata)** checkbox to disable Smart Search for any cameras that you add using the Auto Discovery feature. • Select the **Security Group** from the dropdown if device should be added with a specific security group. **Note:** This may be appropriate if the device supports more than one user account or security level. • Select an option from the **Auto-Configure Streams** list. **Note:** You can select one of the following options from the Auto-Configure Streams list: None, 1 Additional Live Stream, 2 Additional Live Streams.
8	Click  After each device is added, device(s) are displayed in the Video / Audio List tab.

- End -

Procedure 110
Changing the IP Address

Step	Action
1	Select **Devices** from the main menu.
2	Click **Discovery**. The Discovered Devices page automatically displays all discovered devices.
3	Select the checkbox of any device that you want to edit.
4	Click **Change IP**.
5	Select **Use DHCP** or select **Specify an IP address**.
6	If you selected **Specify an IP address**, enter the new **IP Address**. **Note:** Some cameras require a reboot to apply the new IP configuration. Within the Change IP screen, you can click refresh to check when the camera advertises itself with the new IP configuration.
7	Click 

- End -

Scan for Devices

Some cameras do not support standard discovery protocols. To discover these cameras you can use NVR to perform a manual network scan for devices. The Scan for Devices tab allows you to manually initiate a scan on a specific network interface for cameras.

Procedure 111
Scan for Devices Manually

Step	Action
1	Select **Devices** from the main menu.
2	Click **Discovery**. The Discovered Devices page automatically displays all discovered devices.
3	Select the **Scan for Devices** tab.
4	Configure the **Add New Device Settings**. a De-select the **Default Associations** checkbox if video/audio association is not required. b De-select the **Enable Smart Search (Motion Metadata)** checkbox to disable Smart Search for any cameras that you add manually. c Select a Security Group preference from the **Add With Security Group** dropdown menu. d Select an option from the **Auto-Configure Streams** list. **Note:** You can select one of the following options from the Auto-Configure Streams list: None, 1 Additional Live Stream, 2 Additional Live Streams.

5 Configure the **Device Scan Settings**.

a Select the **Security Group** from the dropdown.

b Select the **LAN Interface** from the dropdown.

6 (Optional) Configure the IP address search range.

a Select the **Specify IP Address Range** checkbox.

b Enter the **IP Address Range**.

7 Click 

Once discovered, you can now add devices to the NVR, add to a security group and view camera snapshots.

- End -

UPnP

By default, NVR UPnP advertisements are enabled to allow networked devices to be discovered by victor unified client. If required, this can be disabled.

Procedure 112
Disabling NVR UPnP Advertisements

Step	Action
1	Select **Network**.
2	Select **General**. The Network General tab displays.
3	In the UPnP row, select the **Disabled** option button.
4	Click  UPnP is now disabled.

- End -

Troubleshooting

1 **Issue**: Some video devices are not automatically discovered.

a Verify that the video device had a standard discovery protocol enabled.

If the device does not support standard discovery protocols, then the 'Scan for Device' page can be used to manually scan for these devices.

b Verify that the video device is configured with the manufacturer's default username and password.

If another username and password is configured on the device, then create Security Group on the NVR with a matching username and password.

2 **Issue**: Cannot change the IP address of a video device.

a Check if the NVR interface and device's current IP address are on the same subnet.

Some video devices perform source IP filtering.

In order to change the video device's IP address, the NVR sends commands to the device's current IP address. If the device is performing source IP filtering, it will ignore any packets from the NVR that have a source IP that do not match the device's subnet.

Workaround:

- Temporarily disable recording of any devices on the NVR.
- Temporarily change the IP configuration of the NVR interface to match the camera's current subnet configuration.
- Use the discovery feature to change the video device's IP address.
- Change the IP configuration of the NVR interface back to its original IP address.
- Enable recording of devices on the NVR, as desired.

b The IP Address can updated on most American Dynamics cameras. Refer to your camera documentation for further information.

3 **Issue**: Not able to view snapshot of video device.

a Verify that the video device is IP reachable from the NVR.

When video devices advertise themselves via standard discovery protocols, the advertisements are multicast. Depending on the customer's network configuration, it is possible that the NVR can hear multicast traffic from the device, but it cannot reach the device via unicast IP.

4 **Issue**: No snapshot icon is displayed in Snapshot column.

a Verify that NVR is configured with a Security Group with a username and password that matches the camera's username and password.

NVR Group

NVR groups can be configured between NVRs. NVR groups allow NVRs to share transcoding resources, or to be monitored for Failover.

Note:
• The support of transcode sharing and failover using the NVR Group architecture is only available using version 4.7+.
• You must enable SSH before you can add NVRs to an NVR Group.

Transcoding

Video Transcoding is the dynamic manipulation of video stream properties (e.g. codec used, frame-rate, resolution, etc.) in order to better manage network bandwidth or resources. Depending on model and hardware, VideoEdge has a finite amount of resource to dedicate to transcoding. Using NVR Groups enables all VideoEdge units in the group to share these resources as required. NVR Groups will automatically manage which VideoEdge units in the group carry out transcoding, this does not require user management. Should all transcoding resources within the NVR Group be used, VideoEdge will serve a native stream to clients.

NVR Group List and NVR Discovery

The NVR Group can be configured using the NVR Group menu item. You can manually add NVRs to the group or alternatively you can use the Discovered NVRs tab to find all discoverable NVRs. NVRs which have been added to the group can be viewed on the NVR Group List page.

Note:
You can add up to fourteen NVRs to a group. Up to two secondary NVRs, and up to twelve Primary NVRs.

Procedure 113
Manually adding an NVR to a NVR Group

Step	Action
1	Select **Devices**.
2	Select **NVR Group**. The NVR Groups page opens.
3	Select  **Note:** In the first instance you are required to select the NIC or hostname you want to use to add other NVRs. Once selected this will add the NVR to which you are currently logged on to the group.
4	Enter the **IP Address** or **hostname** for the NVR you want to add to the group. **Note:** It is not required to configure the fully qualified domain name as all NVRs in the group are configured to be in the same domain.
5	Click  **Note:** The NVR will be added with 'Non-failover NVRs' status.

- End -

Procedure 114
Adding an NVR to an NVR Group using Discovery

Step	Action
1	Select **Devices** from the main menu.
2	Select **NVR Group**. The NVR Groups page opens.
3	Select the **Discovered NVRs** tab. The Discovered NVRs page open. When Discovery is enabled, all discoverable NVRs will be displayed in the table. You can refresh the list by clicking  **Note:** Enabling or disabling NVR discovery will also enable or disable device discovery.
4	(Optional) Select the **Add by NVR name** checkbox to discover and add NVRs to the group using their hostnames.
5	(Optional) Select the **LAN Interface** from the dropdown.
6	(Optional) Select **Add NVR by Name** when DNS is configured.
7	Select the checkboxes for all discovered NVRs you want to add to the group. **Note:** Monitoring can be disabled for a secondary NVR if required.
8	Select  **Note:** The NVR will be added with 'Non-failover NVRs' status.

- End -

NVR Group Architecture

An NVR group can contain 14 NVRs (up to 12 primary and 2 secondary). Within a group, NVRs can be assigned the following status -

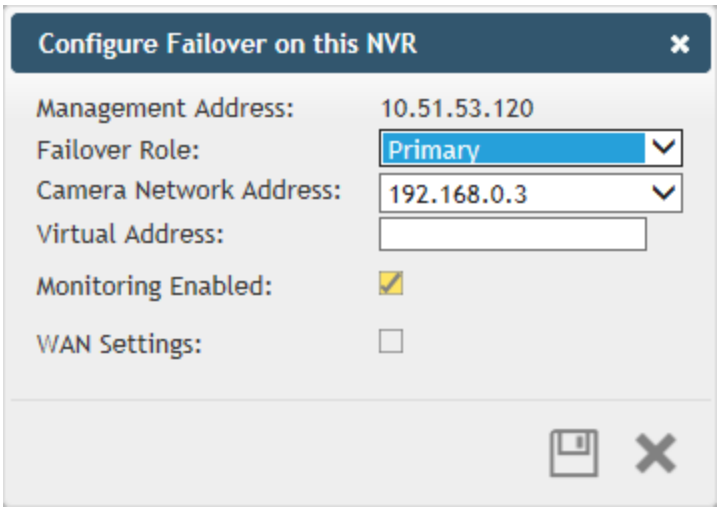
- **Non-failover NVRs** - Neither a primary nor a secondary NVR. NVRs within this status can share transcode resources but will not be included in your failover configuration.
- **Secondary NVRs** - NVRs which monitor the primary NVRs to provide redundancy should a primary fail. Secondary NVRs can share their available transcode resources with the other NVRs within the group. Should a secondary NVR enter failover mode, victor unified client may be required to restart playback on the streams which have been transcoded using the secondary's available resources. victor unified client will automatically restart playback if required.

Note:
When you purchase a license for a Secondary NVR, ensure that the license contains enough camera and analytic licenses for any of your Primary NVRs.

- **Primary NVRs** - NVRs which are monitored by the designated secondary NVRs. Primary NVRs can share their available transcode resources and the transcode resources of other NVRs within the group.

Procedure 115
Configuring a Primary NVR

Step	Action
1	Select **Devices**
2	Select **NVR Group** The NVR Groups page opens.
3	Select  in the table entry for the NVR you want to assign a new status. The configure Failover on this NVR window opens: 
4	Select **Primary** from the Failover Role dropdown.



5 Enter the **Camera Network Address** in the field or select from the dropdown.

6 Enter a **Virtual IP Address** or a **hostname** in the field.

Note:
The Virtual IP address must belong to the management interface subnet on the secondary NVR.

7 (Optional) De-select the **Monitoring Enabled** checkbox if required. This will exclude this primary from the secondary NVR(s) monitoring list.

8 (Optional) Select the **WAN Settings** checkbox if required:

a Enter the **Virtual HTTP Port** in the field

b Enter the **Virtual HTTPS Port** in the field

c Enter the **Virtual Streaming Port** in the field

9 Click 

- End -

Procedure 116
Configuring a Secondary NVR

Note:
Configuring as secondary will remove any devices from the VideoEdge. These devices will need to be re-added if the VideoEdge is reconfigured as a non-failover NVR.

Step	Action

1 Select **Devices**

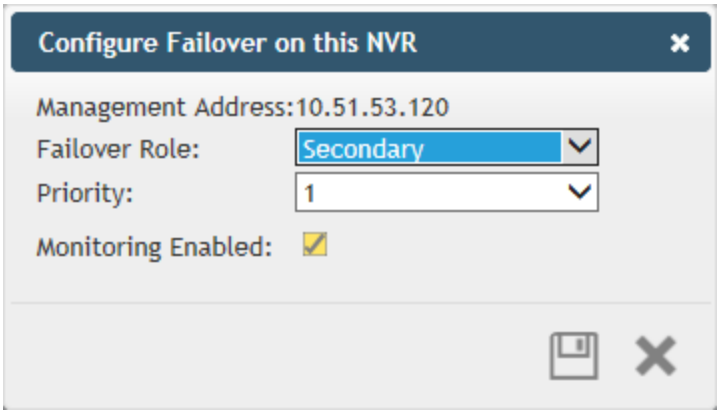
2 Select **NVR Group**

The NVR Groups page opens.

3 Select  in the table entry for the NVR you want to assign a new status.

The configure Failover on this NVR window opens:

4 Select **Secondary** from the Failover Role dropdown.



5 Select the **Priority** from the dropdown.

Note:
The value 1 dictates that when the first primary NVR fails, that this secondary NVR should take over. The value 2 dictates that when a second primary should fail that this secondary will only take over (when the other secondary is already in failover mode).

6 (Optional) De-select the **Monitoring Enabled** checkbox if required. This will disable monitoring mode on this secondary NVR.

Note:
If monitoring is disabled for a secondary NVR, then that NVR will not go active for any failed primary NVRs.

7 Click 

- End -

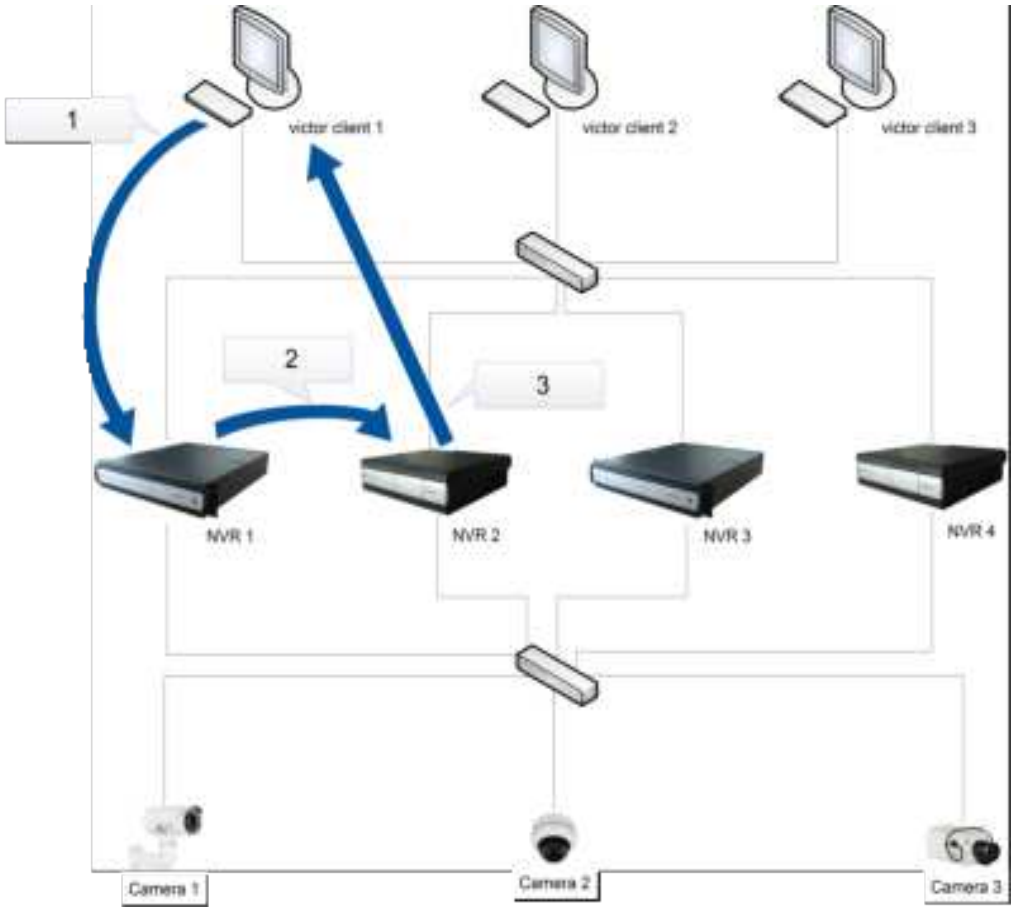
SmartStream

SmartStream is the resource management tool for VideoEdge. Transcoding is an integral part of the NVR's resource management tools, these tools provides the best all round solution for your video monitoring. Depending on your hardware, the NVR can conduct both software and hardware based transcoding. When the NVR's locally available transcoding resources are exhausted, it will utilize the transcoding resources of another member of the group.

Note:
Remote transcoding is only supported for video streams using a H.264 codec.

For example, four NVRs are in the same NVR group, an operator is using victor Client to stream video from cameras that are recording on NVR 1. NVR 1 may have enough resources available to perform transcoding locally, however when NVR 1 no longer has resources available it can use the available resources of another member of the group. (NVR 2 in the example below).

Figure 26 NVR Groups - Network Example



1 victor Client issues RTSP play request to NVR 1. NVR 1 does not have sufficient transcoding resources available to provide optimum stream to the client.

2 NVR 1 streams video to be transcoded to NVR 2.

3 NVR 2 transcodes and streams video to the victor Client.

Note:
In addition to video streaming from the source NVR to the transcoding NVR, health information and configuration messages (to configure NVR Groups) are also transmitted across the network.

NVR group members periodically share transcode statistics to learn what software and hardware transcode resources are available within the NVR group.

Note:
NVRs which are in a group share information using SNMP. All NVRs in a group must therefore have SNMP enabled, the same SNMP port configured and the same SNMP user credentials. A NVR Group admin user credential has been provided for your convenience.

In order to transcode video on a remote server in the group, group members exchange control messages over TCP. Video (either live or transcoded) is sent via RTP/UDP from the recording NVR to the NVR acting as the remote transcode server. The recording NVR decides what palette to offer to the client based on the transcode resources that are available in the NVR group. The NVR acting as the remote transcode server will transcode video and send the transcoded video to the client.

If the NVR group is oversubscribed and is therefore unable to create a full palette, the recording NVR can provide a reduced palette to the client.

NVR Failover

When you configure an NVR group, you can configure up to two NVRs in that group to act as secondary NVRs or Failover NVRs. The secondary NVRs will continuously monitor all the primary NVRs in their NVR group. In the event that a primary NVR fails, a secondary NVR will then switch into failover mode and take over providing services previously provided by the primary NVR. When the secondary NVR is in Failover mode it can no longer takeover for another primary NVR. The secondary NVR can only take over providing services for one primary NVR at a time. Using the default Failover configuration settings, the secondary NVR will detect the absence of the primary NVR after approximately 30 seconds and will initiate assuming the role of the primary NVR.

Note:
For optimum performance it is recommended to use 2 secondary NVRs to monitor a maximum of 12 primary NVRs.

When a primary NVR fails, a secondary NVR assumes the role of the failed NVR and automatically takes over its services. The secondary NVR will record all media that the primary NVR was recording, if you have Motion Detection, Video Intelligence, Edge analytics or dry contact events enabled these will also be assumed by the secondary NVR.

Failover can support both IP and analog video connections. Analog video connections are supported only when cabling is sufficiently connected between the primary NVRs and secondary NVR. The camera password group information is also transferred to allow the Failover NVR to communicate with the cameras. User account information is not transferred, therefore the primary and secondary NVRs must share the same username and password.

Failover monitoring resumes only after the damaged primary NVR is repaired or replaced, and the secondary NVR is returned to normal monitoring operation.

Note:
• A secondary NVR is intended to act as a redundant standby for the NVRs it monitors. A secondary NVR is not intended to manage cameras on its own, because these cameras would no longer be accessible when the secondary NVR takes over for a failed primary NVR. Any camera configuration changes you have made whilst a secondary NVR has taken over the primary NVR's services will be lost when failover is terminated. Camera configuration is not synced back from a secondary NVR to a primary NVR.
• During Failover the archiving configuration on the primary NVR will not be assumed by the secondary NVR. Media recorded to a secondary NVR can be archived if you configure archiving on the secondary NVR.

How Failover is Initiated

When Failover is configured the secondary NVR polls the primary NVR over the camera network. There are three possible responses from the primary NVR:

- The secondary NVR does not receive a reply from the NVR. This could occur due to a power failure, issues with the NVR hardware, loss of connection with the camera network and so on. In this instance the secondary NVR sends a video stream status request to the primary NVR over the admin network. If the primary NVR replies that there are no video streams recording when one or more streams should be recorded at the time of the request, the secondary NVR will mark this as a 'failure'. The secondary NVR will repeat the polling process until the retry count is exceeded. If the secondary NVR continues to receive a 'failure' from the primary NVR, Failover will be initiated.
- The secondary NVR receives a 'failure' from the primary NVR. This could occur due to operator action, for example if the primary NVR services are stopped. In this instance the secondary NVR will attempt to poll the primary NVR again (the number of polling attempts is determined by the retry count, for further information refer to Failover Advanced Configuration). Should the secondary NVR continue to receive a 'failure' from the primary NVR, Failover will be initiated.
- The secondary NVR receives a 'good' reply from the primary NVR. In this instance a no Failover action is taken.

Alerts

Alerts are sent to victor unified client by the secondary NVRs when the following occur:

- The secondary NVR detects the primary NVR has failed and is assuming the primary NVR's role.
- You terminate Failover mode after the primary NVR is operational again.

If Failover email alerts have been enabled, the following notifications will be sent on a Failover event:

- The secondary NVR will send an email notification stating "Activating Failover Mode for NVR at primary-IP-address"
- The primary NVR will send an email notification stating "Primary NVR transitioning to standby state"

If Failover and Reboot notification email alerts have been enabled, the following notifications will be sent on a Failover event:

- The secondary NVR will send the following email notifications stating; "Activating Failover Mode for NVR at primary-IP-address" and "NVR services are being shut down."
- The primary NVR will send the following email notifications stating; "Primary NVR transitioning to standby state" and "NVR services are being shut down."

Virtual IP Addresses

When adding a primary NVR for monitoring you will be required to enter a virtual IP address for that NVR. The virtual IP address allows you to seamlessly search and retrieve video from the secondary NVR which was recorded during the failover period.

The virtual IP address must belong to the management interface (client LAN) subnet on the secondary NVR. The NVR and victor unified client communicate over the management interface (client LAN). If the virtual IP address does not belong to one of the secondary NVR's subnets, the settings will not be applied and an error message will display. If using DHCP you must allocate a range of addresses for use as virtual IP addresses to ensure conflicts do not occur.

Recorded video on the secondary NVR is associated with the virtual IP address of the primary NVR. Should the secondary NVR be required to switch to failover mode for multiple NVRs during its operation the recorded video associated with each primary NVR can be retrieved.

Note:
When the secondary NVR's available storage is depleted, data culling will occur. To manage storage you can configure the maximum retention for each slot that may be populated by a recording device in the event of Failover.

Using an NVR in Failover Mode

When viewing Live Video on victor unified client from a primary NVR and the primary NVR fails, the secondary NVR will automatically take over the connection to view live video. The victor unified client will timeout and retry playing live video from the virtual IP address. victor unified client will automatically reconnect to the camera's live video streams to view live video.

Note:
If a search and retrieve is in progress when a primary NVR fails, the search will not be completed successfully.

Events

During Failover mode events will be sent from the secondary NVR on behalf of the primary NVR, these events include video loss, motion detection events, video intelligence events, dry contact events and so on. These events will be displayed within victor unified client as if they have been sent by the primary NVR. You can use victor unified client to view the video that is associated with these events.

When Failover mode is active the secondary NVR assumes the virtual IP address of the failed primary NVR.

The victor unified client will use the virtual IP address to receive events from the secondary NVR. When the primary NVR is active and generates an event, it sends the event to victor unified client. When Failover mode is active, media-related events will be sent by the secondary NVR providing a seamless appearance in the victor unified client. Events will appear as if they have been received from the primary NVR at all times, even when failover mode is active.

When you add a secondary NVR to victor unified client as a recorder, you should add it by a static IP address assigned to its admin network. victor unified client will receive events from the secondary NVR via its static IP address. Whether the secondary NVR is in failover mode or monitor mode, it will send unit-related events to victor unified client using its static IP address. Adding your secondary NVR in this manner will enable you to monitor its health using the Health Dashboard feature of victor unified client. For further information on this feature refer to the victor unified client User Guide.

Backup/Restore

A backup of a secondary NVR can take place while monitoring or while active for a failed NVR. Backups created will only contain information about the secondary NVR and any information about any primary NVRs will not be backed up.

Configure Failover Mode for an NVR

An NVR that is going to be used as a secondary NVR must be installed and configured in the same way as you would for a primary NVR. You need to configure media folders and storage sets. It is important to note when you are configuring storage for a secondary NVR, the storage configuration must be able to support recording of any camera configurations set up on any of the primary NVRs it is monitoring.

Note:
For seamless playback on victor unified client the primary and secondary NVRs must all share the same username and password.

The secondary NVR must have at least the same processing power as the largest primary NVR it is protecting and must be licensed for at least as many cameras as the largest associated primary NVR.

For VideoEdge Hybrid NVRs, the secondary NVR must have at least as many analog inputs as the largest primary NVR.

The network connection of the secondary NVR should have the same capability as the network connection from the primary NVRs to the client. If, for example, the secondary NVR is connected through a lower bandwidth connection than the primary NVR, you will notice a difference in performance when the secondary NVR is active if the primary NVR fails.

Terminating Failover

Once NVRs have been assigned their required status and monitoring is enabled, your failover redundancy will be in place. Should a primary NVR fail, the secondary will enter failover mode when communication with the primary cannot be established.

When a secondary NVR is in failover mode, the terminate failover icon () will be displayed in the NVR's table entry.

Procedure 117
Terminating Failover

Step	Action
1	Restore the Primary NVR.
2	Select **Devices**
3	Select **NVR Group** The NVR Groups page opens.
4	Select  in the table entry of the secondary NVR you want to return to monitoring mode. Failover will be terminated.

- End -

If Failover Doesn’t Occur

If Failover doesn’t occur ensure the following are set up as required:

- The secondary NVR is suitably license to support the highest licensed primary NVR on its server monitoring list.
- The cabling between primary and secondary NVRs is connected securely and correctly.
- Failover settings are configured correctly.
- The secondary NVR is of suitable specification to take over services for each primary NVR it monitors.

Upgrade Considerations

Failover functionality is only available when software version compatibility is satisfied i.e. both the primary and secondary NVRs have the same version of software installed. To enable N:2 Failover for an NVR group, all NVRs in the group must be upgraded to VideoEdge 4.7.

It is recommended that you should upgrade all NVR(s) in the same maintenance window when a Failover system is present to ensure the time period without failover redundancy is minimized.

Procedure 118
Upgrading NVRs when Failover is Enabled

Step	Action
1	Disable failover monitoring on your primary NVR.
2	Upgrade your primary NVR.
3	Begin upgrading your secondary NVRs. When a secondary NVR has been upgraded, failover monitoring can be re-enabled.

Note:
Security Configuration > Web server configuration (i.e. HTTP and HTTPS or HTTPS only) must be applied identically on the primary NVR and on all the secondary NVRs on its active monitoring list for failover to function correctly.

- End -

Failover and Licensing

You must purchase a local license for each of your primary and secondary NVRs. Ensure that each secondary NVR license contains sufficient cameras and analytics to effectively take over a primary NVR's streams.

Failover and Centralized Licensing

Failover is not compatible with centralized licensing. Before transferring a VideoEdge device to a centralized license, you must remove the VideoEdge from any NVR groups.

Note:
Because of the potential impact to Failover and Transcoding, you should review your NVR Group configuration before migrating a VideoEdge to centralized licensing.

Options

From the Options menu you can configure additional settings for cameras that you add to VideoEdge. From the Camera Add page, you can configure global camera settings. From the TrickleStor page, you can enable or disable offline recording for supported cameras.

Camera Add

From the Camera Add page, you can configure the following settings:

- Max GOP
- Enable Smart Search
- Video Loss Sensitivity
- Auto-Configure Streams
- Enable ONVIF

These settings automatically apply to any camera that you add to VideoEdge. However, some settings are not compatible with each brand of camera.

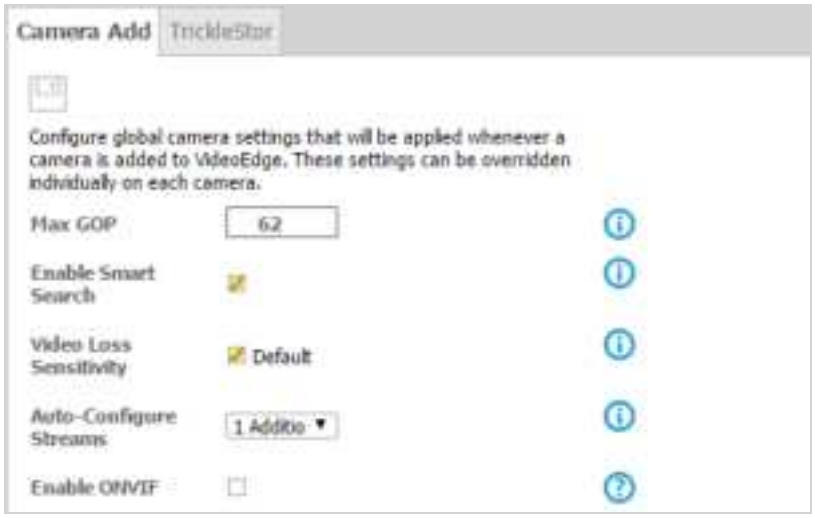


Figure 27 Camera Add Page

Max GOP

A GOP is a group of pictures. Camera video streams comprise successive GOPs. From the Options page, you can set the maximum GOP size for cameras that you add to VideoEdge. A higher GOP size helps reduce a camera stream's bandwidth and storage consumption. However, higher GOP sizes are better suited to recording scenes with low levels of motion.

Note:
• The Max GOP setting only applies to a camera's H264 and H264+ streams.
• To modify the Max GOP for cameras that are already added to VideoEdge, you can edit individual cameras from the advanced camera configuration menu, or you can batch edit cameras from the Devices menu.

Procedure 119
Configuring the Max GOP

Step	Action
1	Select **Devices** from the main menu.
2	Select **Options**. The Camera Add page opens.
3	Enter a value in the **Max GOP** field. **Note:** You can set the Max GOP to a value from 1 to 1023.
4	Click 

- End -

Smart Search

The Enable Smart Search option is selected by default for VideoEdge units after the initial software installation. Select this option to automatically enable Smart Search for any cameras that you add to VideoEdge. When you enable Smart Search from the **Camera Add** page, the **Enable Smart Search (Motion Metadata)** checkbox is selected by default at the following locations:

- The **Discovered Devices** page
- The **Scan for Devices** page
- The **Add Camera Manually** dialog box

Similarly, if you disable Smart Search from the **Camera Add** page, the checkbox is de-selected at those locations. Select the checkbox on any of these pages or dialogs to activate the feature again.

Note:
• This option will only apply the Smart Search configuration to devices that are added to the VideoEdge when the **Enable Smart Search (Motion Metadata)** checkbox is selected. If you use a backup configuration file to reinstall cameras, then the configuration for all camera devices listed in the backup file will be applied instead.
• To enable Smart Search or Motion Detection for any devices added that have not previously been configured for Smart Search or Motion Detection, edit the Advanced Camera Configuration settings in the **List** page, and edit the camera alarm settings on the **Alarms** page. For more information, see **Devices**.
• This feature is disabled by default for all R7-Series VideoEdge units.

Procedure 120
Enabling Smart Search by default

Step	Action
1	Select **Devices** from the main menu.
2	Select **Options**. The Camera Add page opens.
3	Select the **Enable Smart Search (Motion Metadata)** checkbox.

4	Click 

- End -

Video Loss Sensitivity

By default, a video loss alarm triggers if a camera's video stream is interrupted for 5 seconds. On busy or unstable networks, the video loss alarm may trigger more frequently. If required, you can modify the Video Loss Sensitivity setting, which determines the amount of time that must pass before a video loss alarm triggers.

Procedure 121
Editing the Video Loss Sensitivity

Step	Action
1	Select **Devices** from the main menu.
2	Select **Options**. The Camera Add page opens.
3	Clear the **Default** checkbox for the Video Loss Sensitivity.
4	Enter a new value for video loss duration in the text field. **Note:** • You can numerical value between 5 seconds and 20 seconds • If you re-select the **Default** checkbox, the Video Loss Sensitivity returns to 5 seconds.

- End -

Auto-Configure Streams

Enable this option to automatically configure additional streams when you add new devices to your VideoEdge.

Procedure 122
Enabling auto-configuration for camera streams

Step	Action
1	Select **Devices** from the main menu.
2	Select **Options**. The Camera Add page opens.
3	Select an option from the **Auto-Configure Streams** list. • **None**: Disables the Auto Configure streams function. • **1 Additional Live Stream**: Configure one additional stream • **2 Additional Live Streams**: Configure two additional streams. This option is only available for cameras that support three streams.

- End -

ONVIF

By default, VideoEdge uses a camera's native handler to communicate with that camera. If required, you can select ONVIF as the preferred communication method between the VideoEdge and the camera. However, you can also configure the VideoEdge to use the ONVIF protocol instead. After you enable this feature, you can select ONVIF as the preferred communication method when you add a camera to VideoEdge.

Note:
Before you enable ONVIF, try the following steps:
1. Try using the native handler to add the camera
2. Try using the generic handler to add the camera.

Procedure 123
Enabling ONVIF protocols

Step	Action
1	Select **Devices**.
2	Select **Options**.
3	Select the **Enable ONVIF** checkbox.
4	Select 

- End -

Using ONVIF protocols

When you add a camera to VideoEdge, select the **Enable ONVIF** checkbox.

For more information about adding cameras to VideoEdge, see Devices.

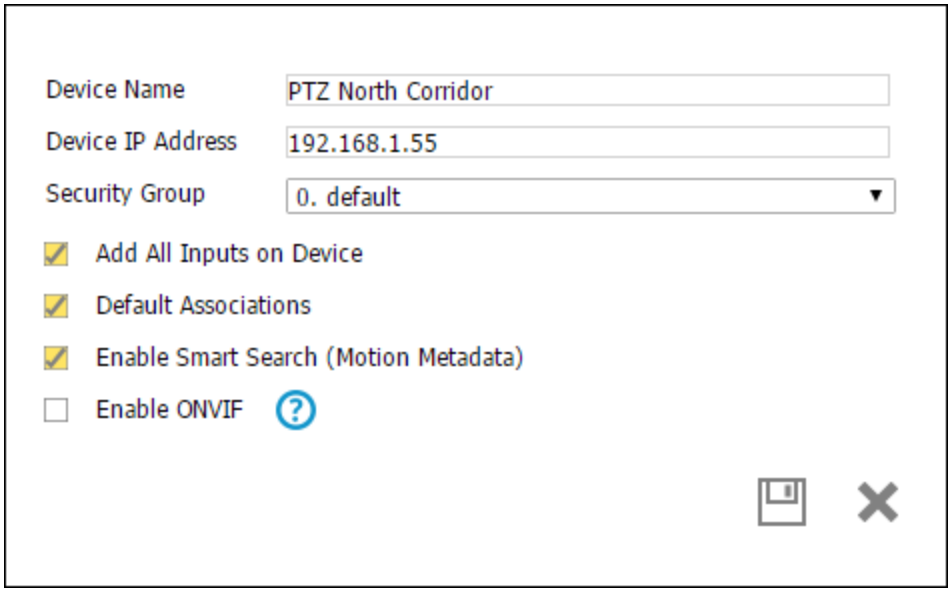


Figure 28 Adding a camera to VideoEdge

TrickleStor

From the TrickleStor page, you can enable or disable offline recording for supported Illustra Pro and Illustra Flex Gen2 cameras.

When you configure a camera for offline recording, the camera can continue to record footage while it is disconnected from VideoEdge. When VideoEdge reconnects to the camera, the camera's footage transfers to the VideoEdge. To merge the camera's footage into the gap in the VideoEdge's footage correctly, you must connect the camera and the VideoEdge to the same NTP server.

If you configured an archive for your VideoEdge, you can also transfer this footage to the archive. See Archive for more information about configuring an archive.

Note:
• Offline recording does not support audio or analytics, even if the camera normally supports these features.
• Cameras that support the offline recording process appear on the TrickleStor page. If the cameras do not appear on the TrickleStor page they may not have the latest camera firmware installed.

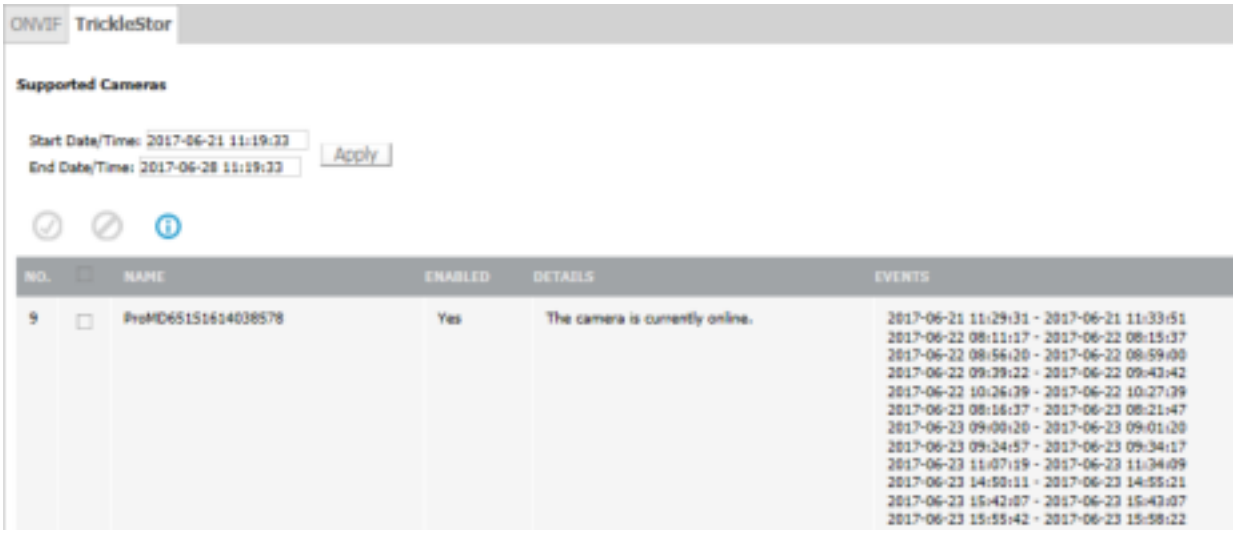


Figure 29 TrickleStor Page

Prerequisites

- You must upgrade the VideoEdge to version 5.0.0.X or higher
- You must upgrade the camera firmware to the most recent version
- The cameras must be fitted with a micro SD card so that they can record video while they are disconnected from the VideoEdge.
- You must configure the camera for Edge Recording and Offline Recording through the camera's web interface. Refer to the camera's documentation for more information.
- You must connect the VideoEdge and the cameras to the same NTP server.

When the supported cameras have been added and enabled for offline record on the VideoEdge the following parameters are automatically configured in the camera's web interface, in the Edge Recording menu:

- The **Record Settings Enable Event Record** box contains a green tick.
- **Offline Record Settings** - The VideoEdge IP address box contains the IP address of the VideoEdge camera NIC.

Procedure 124
Enabling offline recording

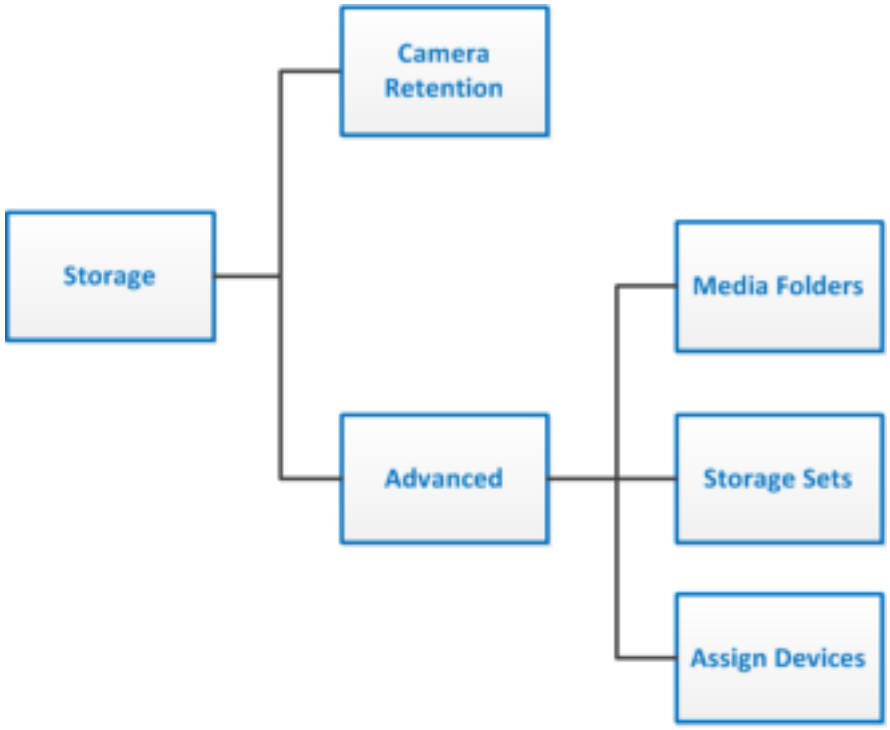
Step	Action
1	Select **Devices**.
2	Select **Options**.
3	Select the **TrickleStor** tab.
4	Select cameras from the **Supported Cameras** list.
5	Select 
6	(Optional) Filter the camera events list. a Configure the **Start Date/Time**. b Configure the **End Date/Time**. c Select **Apply**.

- End -

Storage Menu Overview

Internal and external storage which has been correctly mounted can be enabled/disabled using the **Storage** menu. In addition the Storage menu is also used to create storage sets for load management to best utilize available internal and external storage.

Figure 30 Storage Menu Map



- **Camera Retention** - From here you can set the minimum and maximum retention periods for recorded media that is stored on your devices.
- **Advanced** - From here you can create media folders and storage sets to allow for load balancing. Devices can then be assigned to storage sets as required, to best utilize your hardware.

Overview

NVRs can require a tremendous amount of storage space depending on the number of cameras, codec, resolution, frame rates, recording modes, and the duration for which you wish to preserve video recordings. At the outset of your use of the NVR system, you will need to have storage configured to record data. At the outset default storage partitions are configured to record data. From time to time, you may find it necessary to replace or add a storage device to produce a greater capacity for video storage.

This chapter describes how to configure storage devices that are physically connected to the NVR and storage devices that are networked to the NVR over a TCP/IP connection.

There are two main storage configuration types, basic and advanced configuration. Basic configuration is the default configuration type where all storage devices and cameras are contained within one storage set. By using advanced storage configuration, you can create numerous storage sets and assign storage devices and cameras to storage sets

as required to optimize disk performance. In the Camera Retention page, all devices are listed, and you can configure their retention settings. In the Advanced storage page you can view, create, edit and delete storage sets. You can also move cameras and devices between storage sets to optimize disk performance.

Overview of Storage Sets

A storage set is a group of storage drives. One storage set is set up by default on an NVR. This is storage set 1. Initially the default storage set has all enabled storage devices, their media folders and cameras assigned to it. By default one storage set per drive is set up on the VideoEdge Hybrid Appliance. If your device has RAID storage, one storage set is created by default.

A Media Folder is a location on a device where media can be recorded to. Media stored in these folders can include video, audio and analytic media. You should only have one media folder per storage device for optimum disk I/O performance. You can choose which media folders on devices are to be used for storage.

Video from the cameras assigned to a particular storage set will record to the media folders on the storage devices that are assigned to the same storage set.

You can easily create additional storage sets and configure them as required to optimize the disk performance, as media can be recorded to storage sets in parallel.

Each storage set must have at least one assigned media folder for storage. You can assign multiple media folders and cameras to a storage set. It is recommended that you assign no more than 32 devices or cameras per storage set.

Verifying Storage Devices

The Virtual Disks (aka LUNs or Volumes) may have all been detected by the NVR, but not necessarily configured for usage by the NVR. Ensure that your storage devices are listed in the table on the Media Folders page before moving on to the next section. If any expected storage is missing from the Media Folders page, then it is either physically disconnected, the storage device is not recognized due to improper configuration or lack of device driver support, and/or experiencing a storage hardware problem. This may also occur if the file system is not mounted.

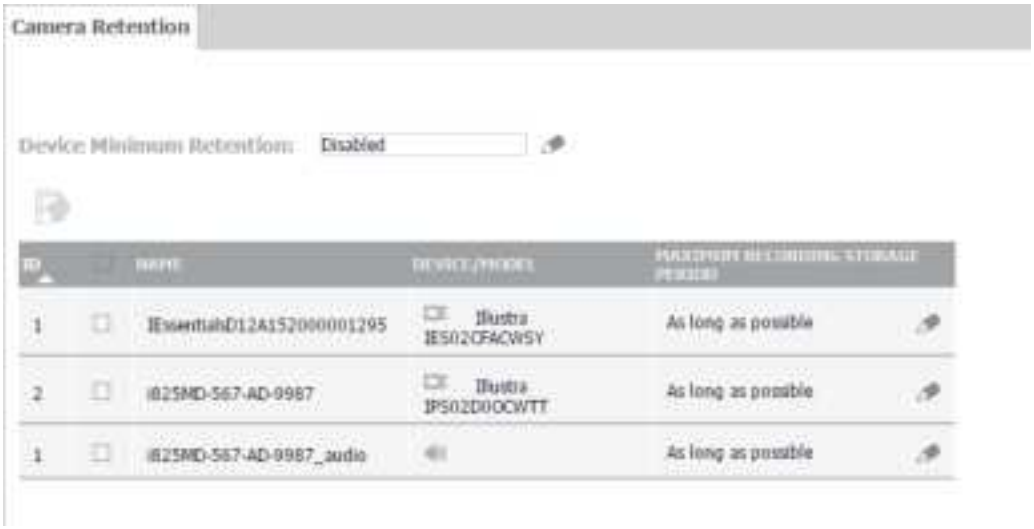
Caution

If you are using RAID storage systems, you must create disk groups and virtual disks on your RAID hardware before setting up storage on the NVR. If you are not familiar with RAID configuration, refer to your storage system's user manual for more information.

Camera Retention

From the Camera Retention page, you can view the devices that are attached to the VideoEdge, and you can configure their storage retention settings.

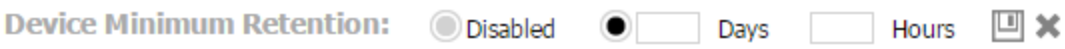
Figure 31 The Camera Retention page



Configuring the device minimum retention period

Configure the minimum retention period to enable the system to issue alerts when the configured retention for a device is not matched or to issue an alert if the configured minimum retention is at risk.

Procedure 125
Configuring the device minimum retention period

Step	Action
1	Select **Storage** from the main menu.
2	Select **Camera Retention**.
3	In the **Device Minimum Retention** field, select 
4	Enter a value for retention period.  **Note:** To disable the device minimum retention period, select the **Disabled** button.
5	Select 

- End -

Configuring the device maximum recording storage period

A device's maximum recording storage period is the maximum duration over which media recorded for that device is saved without being deleted.

By default, device recordings are stored for as long as possible. When storage space becomes unavailable, older data is culled to make room for newer recordings. If required, you can customize the maximum recording storage period for your devices. You can set the maximum number of days and hours that VideoEdge can store each device's recordings. For example, to prioritize recordings from a device, you can configure it to store recordings for as long as possible. Similarly, to de-prioritize recordings from a device, you can assign a device a custom storage period, designed to suit the parameters of your security system.

Caution

The shorter a device's maximum recording storage period, the more frequently its recordings are culled. Ensure that your device's maximum storage recording periods can be accommodated by your VideoEdge's storage configuration.

Procedure 126
Configuring the device maximum recording storage period

Step	Action
1	Select **Storage** from the main menu.
2	Select **Camera Retention**.
3	In the device's **Maximum Recording Storage Period** field, select 
4	Select the **As long as possible** button. Or a Select the custom period option button. b Enter a value in the **Days** field. c Enter a value in the **Hours** field.
5	Select 

- End -

Advanced

The Advanced Storage Configuration options allow you to be flexible in setting up the storage on the VideoEdge. You can calibrate cameras to determine the optimum recording and storage settings for each camera that is connected to the VideoEdge. You can spread media folders and cameras across storage sets to achieve higher system performance due to a lower total data rate required to record to each storage device.

Using the Advanced Storage Configuration page you can perform the following actions:

- Set the VideoEdge's vault media quota
- Add USB storage devices to VideoEdge
- Enable or disable media folders
- Create storage sets
- Delete storage sets
- Add media folders to storage sets
- Move media folders between storage sets
- Calculate a camera redistribution proposal
- Assign cameras to storage sets
- Move cameras between storage sets
- Calibrate cameras

By using a combination of the advanced configuration options and your calculated storage requirements per camera, you can configure the VideoEdge to achieve optimal efficiency and performance.

Media Folders

The Media Folders tab displays VideoEdge's basic storage configuration. From this tab, you can enable or disable the Media folders to be used for recording. All storage devices that are discovered by the VideoEdge are listed in the storage configuration table. All cameras added to the VideoEdge are also automatically assigned to the default storage set. You can select which media folders you want to use for media storage, and set the amount of space available to store media. You can also connect USB storage devices to VideoEdge, to expand VideoEdge's storage capacity. The table below describes fields used for storage configuration.

Figure 32 Media Folders tab

Table 13 Storage Configuration Fields

Field	Description
Device	A physical device detected by the NVR.
Use for Storage	Indicates whether or not the device is being used for storage. Green indicator = Enabled for storage Gray indicator = Disabled for storage Red indicator = Media folder is unhealthy
Media Folder	The location on the device where recorded media will be stored.
Type	Indicates the file system type, for example; XFS.
Size (GB)	The total size of the storage device in GB.

Adding USB storage devices to VideoEdge

From the Media Folders page, you can add USB storage devices to VideoEdge, to expand its media storage capacity.

Procedure 127
Adding USB storage devices to VideoEdge

Step	Action
1	Select the **Storage** menu.
2	Select **Advanced**. The Media Folders page opens.
3	Select 
4	Select a USB device from the table.
5	Select 

Note:
A pop-up window will open asking 'Do you wish to delete all previously recorded media from all selected USB devices?'. Click  or  as required.

- End -

Enabling Media Folders for Storage

If there are devices available in the storage configuration table, media cannot be recorded to these devices until you enable the corresponding media folders for storage. By default when a device is added to the VideoEdge, the media folder is enabled for storage. However, if VideoEdge detects recorded media on the device, the media folder is disabled. Use the following procedure to enable a media folder for storage.

Procedure 128
Enabling a Media Folder to be Used for Storage

Step	Action
1	Select the **Storage** menu.
2	Select **Advanced**. The Media Folders page opens.
3	Select the checkbox for the media folder you want to use for storage and click  **Note:** If there has been media already stored in the folder a pop-up window will open asking 'Do you wish to delete all previously recorded media from this folder?'. Click **Yes** or **No** as required.

- End -

Disabling Storage Media Folders

If you need to remove a media folder from storage, you must disable it. When a media folder is removed from storage, the recorded media in the folder is not removed by default. You are given the option to retain or remove the recorded media. Information in the media database is however removed. When you remove a media folder, if the NVR is actively recording to that folder it will automatically transition recording to another media folder in the same storage set. Once a media folder is removed from storage the NVR will no longer record to that folder.

Procedure 129
Disabling a Storage Media Folder

Step	Action
1	Select the **Storage** menu.
2	Select **Advanced**. The Media Folders page opens.
3	Select the checkbox for the media folder you want to use for storage and click 
4	Click **OK** to delete any previously recorded media. The **Use For Storage** indicator turns gray, indicating that the media folder is not being used for storage.

- End -

Data Culling

When there is not enough space in a storage set to store recorded media, media will be deleted.

If there is any media older than the maximum retention period specified for a specific camera, the media will be automatically deleted.

The available space in each storage set is determined periodically. If the available space in a storage set falls below the data-culling threshold, media will be deleted for any camera in the storage set which is older than the maximum retention period. If you do not set a maximum retention period for a camera, all media for this camera may be deleted to free up storage space, as the NVR will prioritize saving the media stored for cameras up to their maximum retention

period. The oldest media is deleted first, minute by minute, until the free space limit is reached. If there is no media older than the retention period, the oldest media in the storage set is deleted and an alarm is raised.

Note:
The media deleted will only be the oldest media available online.

The alarm is an indication that there is insufficient storage space available for the media that you want to store. To resolve this issue you can add additional storage devices to the NVR, decrease the maximum retention period for camera(s) or use Advanced Storage Configuration settings to move cameras to another storage set.

Vaulted Media

Vaulted media is specific media tagged so it will not be deleted, until specified. Vaulted media will not be deleted as part of the normal data culling process of media storage folders.

Use victor unified client to tag media as protected media using the Vault feature. You must have 'Protect' permissions to set video as protected media. To allow vaulted media to be deleted you must set it as unprotected using victor unified client and have 'Unprotected' permissions. For more information refer to the Vault chapter in the victor Configuration and User Guide.

Vault Media Quota

A vault media quota is a percentage of the total storage available that is to be used to store vaulted media only.

Over time the amount of vaulted media within a storage set will accumulate. If too much vaulted media accumulates it may result in non-vaulted media being prematurely culled when the storage space reaches its maximum capacity. A vault media quota can be set to prevent premature data culling as the amount of space for vaulted media is limited ensuring there is enough space for normal media storage.

When you are assigning media as vaulted, and if there is not enough storage space in the quota allocated to store the media as vaulted media, a warning message opens and you cannot assign the media as vaulted. You will need to increase the vault media quota or delete vaulted media.

Procedure 130
Setting a Vaulted Media Quota

Step	Action
1	Select the **Storage** menu.
2	Select **Advanced**. The Media Folders page opens.
3	Click 
4	Enter the required protected media quota, as a percentage of the total space available, in the **Vault Media Quota** field.
5	Click 

- End -

Storage Sets

By default one storage set is created for each storage drive and all analog cameras are assigned to Storage Set 1.

If your device has RAID storage, one storage set is created by default.

Note:
You can reconfigure your RAID storage to create two RAID 5 arrays. This will allow two storage sets to be created increasing throughput on the NVR to 200Mbps.

By default there is one storage set created on the NVR. It initially contains all media devices detected by the NVR and is available to view through the Storage Sets page. Once a media folder on a storage device is enabled for storage in the Media Folders page, the media folder is available for advanced configuration and is displayed in the Storage Sets page in Storage Set 1.

Figure 33 Storage Sets page

Table 14 Storage Sets Configuration Fields

Field	Description
1. Set	This is the Storage Set the media folder is assigned to.
2. Device	This is a physical device detected by the NVR
3. Media Folder	The location on the device where recorded media will be stored.
4. Type	Indicates the file system type, for example; XFS.
5. Total Size (GB)	The total size of the storage device in GB.
6. Amount to Use for Media (GB)	The total amount of space to be used for storing media before data culling begins on the stored media. **Note** The amount of space to be used for media cannot exceed the total size of the storage device.

Field	Description
7. Move to Storage Set	A dropdown list of other storage sets available on the NVR. By selecting a storage set you will move the media folder to that storage set.

Creating Storage Sets

You can create a new storage set to group particular media folders and cameras. When a new storage set is created it contains no media folders or cameras, you need to reassign these from another storage set.

Storage Set Recommendations

- If you are using RAID storage systems, American Dynamics strongly recommends assigning all virtual disks from a disk group to the same storage set.
- It is recommended that a storage set should contain a minimal number of media folders, one if possible, maximizing the virtual disk size.
- The R720 bundled server storage set performance supports a maximum of 64 cameras with 200Mbps max on each storage set. Total input into server is 400Mbps.
- The Software Only option installed on the minimum requirement hardware supports a maximum of 32 cameras with 100Mbps max on each storage set. Total input into server is 400Mbps.
- The NVR Desktop Appliance and Hybrid Desktop Appliance storage set performance supports a maximum of 32 cameras with 100Mbps max on each storage set. Total input into server is 100Mbps.
- The Hybrid Rack-Mount Appliance (32 Channel Hybrid 2U Rack Mount) storage set performance supports a maximum of 32 cameras with 100Mbps max on each storage set. Total input into server is 200Mbps.
- The Hybrid Rack-Mount Appliance (64 Channel Hybrid 3U Rack Mount) storage set performance supports a maximum of 64 cameras with 100Mbps max on each storage set. Total input into server is 300Mbps.

Procedure 131
Creating a Storage Set

Step	Action
1	Select the **Storage** menu.
2	Select **Advanced**.
3	Select **Storage Sets**. The Storage Sets page opens.
4	Click  A new storage set is created.

- End -

Media Folder Assignment for Storage Sets

When you create a new storage set you need to assign media folders and cameras to it. To assign media folders to a new storage set you need to reassign media folders from the default storage set or an existing storage set.

There is no limit to the number of media folders you can assign to a storage set. There are however some restrictions:

- You are able to add a system disk to a storage set by specifying a particular folder on the system disk. It is recommended that the folder you specify exists on a separate partition on the system disk.
- You will not be presented with Linux system file systems, for example, /proc, /sys, etc.

Note:
When allocating media folders from the same device or RAID group it is recommended to associate them with the same storage set. Hard drive thrashing can occur if media folders from the same hard drive are spread across several storage sets, this could result in the systems performance being downgraded when the hard drive is being overworked.

When a media folder is moved to another storage set, all previously recorded media will still be retrievable via clip export and playback in victor unified client and the VideoEdge Client.

Procedure 132
Assigning / Reassigning Media Folders to a Storage Set

Step	Action
1	Select **Storage** from the main menu.
2	Select **Advanced**.
3	Select the **Storage Sets** tab. The Storage Sets page opens.
4	Locate the media folder in its existing storage set that you want to move to a new storage set.
5	Select the new storage set you want to assign the media folder to from the **Move to Storage Set** dropdown. The media folder is reassigned to the new storage set.

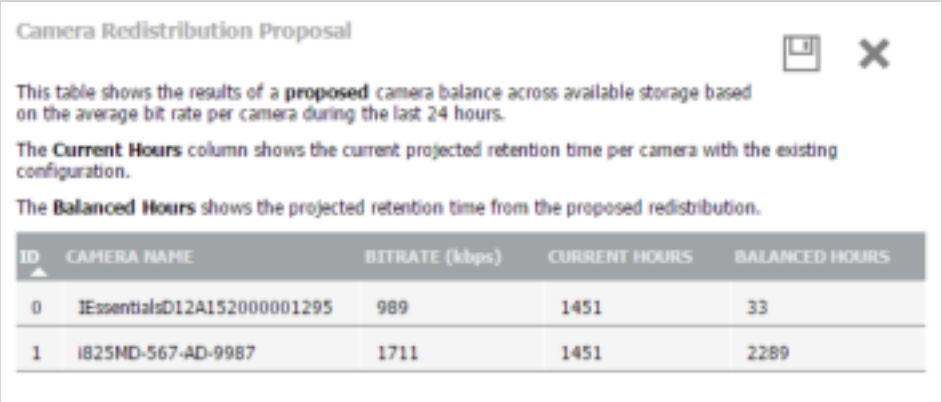
- End -

Calculating Camera Redistribution

You can use the Camera Redistribution feature to re-balance your camera storage configuration. The purpose of this feature is to improve the retention time for your cameras. To achieve this, VideoEdge creates a Camera Retention Proposal. This proposal projects the current and re-balanced retention times for each camera, based on your current storage configuration.

Note:
• Depending on your monitoring system configuration, the Camera Redistribution Proposal may not indicate retention improvement for all cameras. Ensure that you review the proposed changes before you accept the Camera Redistribution Proposal.
• A notification appears if the Camera Redistribution Proposal cannot re-balance your storage configuration.
• The camera redistribution icon,  , is not usable on certain platforms; for example, software-only deployments, such as Virtual Machines, or on platforms that have a RAID card installed..

Figure 34 Camera Redistribution Proposal



If you accept the Camera Redistribution Proposal, VideoEdge may make the following changes to your storage configuration.

- Reassign media folders to different storage sets
- Reassign cameras to different storage sets

Procedure 133
Calculating camera redistribution

Step	Action
1	Select **Storage** from the main menu.
2	Select **Advanced**.
3	Select the **Storage Sets** tab.
4	Select to create a camera redistribution proposal.
5	Select to accept the proposed camera redistribution changes. Or Select to reject the proposed camera redistribution changes.

- End -

Assign Devices

Assigning Cameras to Storage Sets

During the process of adding cameras to the NVR, if only one storage set is available, the new camera will be added to this storage set. However, if there are a number of storage sets available you will be prompted to assign the camera to the required storage set. Cameras can be reassigned to different storage sets as required without needing to remove and re-add the camera. If you are adding cameras using auto-discovery the cameras will be added to the default storage set.

Procedure 134
Reassigning a Camera to a Different Storage Set

Step	Action
1	Select **Storage** from the main menu.
2	Select **Advanced**.
3	Select the **Assign Devices** tab.
	A summary of cameras assigned to storage sets are displayed.
4	Locate the camera you want to reassign in its existing storage set.
5	Select the storage set you want to reassign the camera to from the **Move to Storage Set** dropdown.
	The camera is reassigned to the selected storage set.

- End -

Calibrating Cameras

The data transfer rate for a camera is displayed in each storage set table. This is recorded in the **Estimated Kbps** field. The data transfer rate displayed in this field usually displays the average rate over the last 24 hour period in kbps. You can use the Calibrate camera function to calculate the data transfer rate in kbps for each camera over the last two minutes. This will give an up to date data transfer rate for each camera. You can use this information to optimize the performance of your NVR by reassigning cameras to storage sets based on the current data transfer rates.

Figure 35 Assign Devices Tab

Procedure 135
Calibrating Cameras

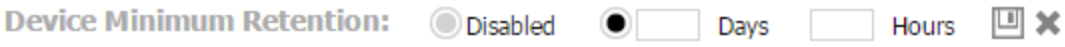
Step	Action
1	Select **Storage** from the main menu.
2	Select **Advanced**. The Storage Sets page opens.
3	Select the **Assign Devices** tab. A summary of cameras assigned to storage sets are displayed.
4	Click **Calibrate**. The **Estimated Kbps** field for each camera is updated with the data transfer rate for the last two minutes.

- End -

Configuring the Device Minimum Retention Period

Configure the minimum retention period to enable the system to issue alerts when the configured retention for a device is not matched or to issue an alert if the configured minimum retention is at risk.

Procedure 136
Configuring the Device Minimum Retention Period

Step	Action
1	Select **Storage** from the main menu.
2	Select **Advanced**.
3	Select the **Assign Devices** tab.
4	In the **Device Minimum Retention** field, select 
5	Enter a value for retention period.  **Note:** To disable the device minimum retention period, select the **Disabled** button.
6	Select 

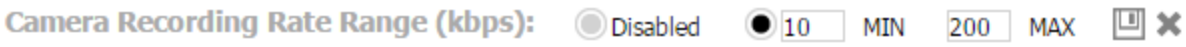
- End -

Configuring the Camera Recording Rate Range

The camera recording rate range is global setting for all cameras connected to the VideoEdge. You can configure Email Alerts to send whenever the measured recording rate of a camera falls outside recording rate range.

Procedure 137
Configuring Camera Recording Rate Range

Step	Action
1	Select **Storage** from the main menu.
2	Select **Advanced**.
3	Select the **Assign Devices** tab.
4	In the **Camera Recording Rate Range (kbps)** field, select 
5	Enter values for the minimum and maximum recording rates.



Note:
To disable the recording rate range, select the **Disabled** button.

6	Select 

- End -

Deleting Storage Sets

You can delete storage sets as required, however, the default storage set cannot be deleted.

Note:
Before you delete a storage set you need to ensure that it contains no assigned cameras or media folders. You can reassign devices to alternative storage sets from the Assign Devices page.

Procedure 138
Deleting a Storage Set

Step	Action
1	Select **Storage** from the main menu.
2	Select **Advanced**.
3	Select the **Storage Sets** tab.
4	Reassign all media folders currently assigned to the storage set you want to delete.
5	Reassign all cameras currently assigned to the storage set you want to delete.
6	Click 

Note:
If you have not reassigned all cameras and media folders the NVR will not allow you to delete the storage set.

- End -

Storage Statistics

The NVR holds and displays storage statistics for storage devices, storage sets and cameras that are being used in the NVR storage configuration. These can be accessed via the Advanced menu. Refer to Storage Statistics for more information

Storage Monitoring

All media folders assigned to a storage set will be monitored by the NVR to determine that they are operational and available for storing media.

The media folders are checked to ensure they are still mounted and read/writable. It is possible that media folders can become unmounted due to system errors, device errors or the device being unmounted by a user. A media folder could become read-only, for example, if the device has been unmounted and remounted as read-only.

If a media folder is determined as non-operational, recording will switch to the next available operational media folder in the storage set.

Non-operational media folders are highlighted as being unhealthy. To determine the health status of storage devices, view the Status in the Media Device section of Storage Statistics.

Adding External Storage

VideoEdge supports external storage solutions. This section provides instructions for connecting external storage devices and using them with the NVR. It is assumed that the storage device's Disk Groups (RAID set) and Virtual Disks (LUNs) have been properly configured and the device has been physically connected to the NVR. Use the operating system to mount any local storage device or any network storage device to the NVR.

Storage Concepts

iSCSI

- This standard is used to transmit data over local area networks (LANs), wide area networks (WANs) and can enable location-independent data storage and retrieval.
- A system that uses iSCSI requires an initiator. Initiators are iSCSI clients and they can either be in software or hardware.
- iSCSI does not require dedicated cabling; it can use existing switching and IP equipment. As a result, iSCSI is thought to be a low-cost alternative to Fiber Channel, which requires dedicated infrastructure.

Fiber Channel

- Fiber Channel, or FC, is a gigabit-speed network technology primarily used for storage networking. It got its start in the supercomputer field, but has become the standard connection type for storage area networks (SAN) in enterprise storage.
- Fiber Channel Host Bus Adapters (HBAs) are available for all major open systems, computer architectures, and buses, for example, PCI. They are needed to connect a Fiber storage device to a server.

Direct Attached Storage

- This term is used to differentiate non-networked storage from networking systems such as NAS and SAN.
- However, DAS cannot share information or space with other servers.
- DAS are usually connected via SCSI cables, along with a SCSI terminator.
- DAS can also be connected via eSATA or USB.

Storage Types

- **JBOD** – Just a Bunch of Disks
- **RAID** – Redundant Array of Inexpensive Disks

JBOD

- The JBOD storage configuration is a group of disks without any RAID features, depending on configuration in BIOS.
- In NVR systems, JBOD is rarely used with external devices.

RAID

- An umbrella term for computer data storage schemes that distribute data across multiple disks for increased input/output performance and/or better reliability.
- Since RAID systems use multiple disks, they are often referred to as disk groups.

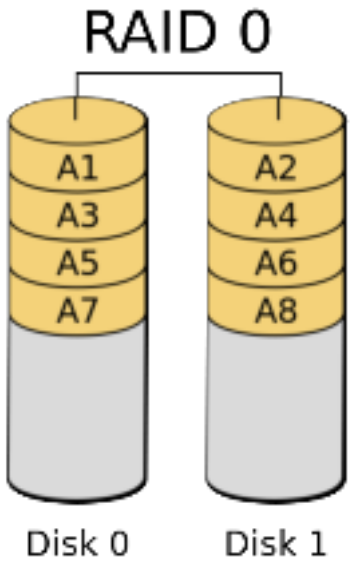
- Disk groups are also known as volumes or RAID arrays.
- There are different types of RAID configurations. Some of the best known configurations are RAID 0, 1, 5 and 6.
- Each configuration uses an approach to storage that can provide fault tolerance, additional availability of data, redundancy, additional performance, or more than one of these factors.

Key RAID Concepts

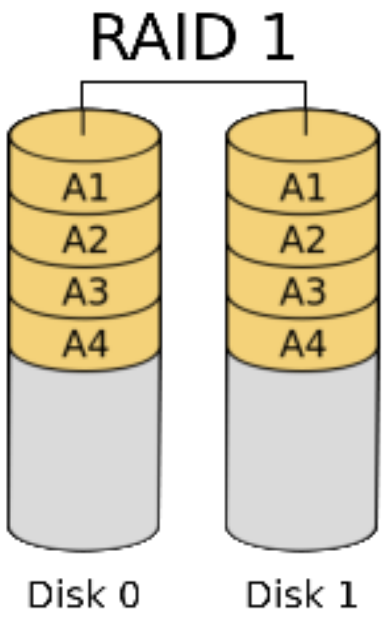
- **Mirroring** – Duplicating data to more than one disk.
- **Striping** – Splitting data across more than one disk.
- **Error Correction** – Storing redundant data so problems can be detected and possibly fixed.

Common RAID Types

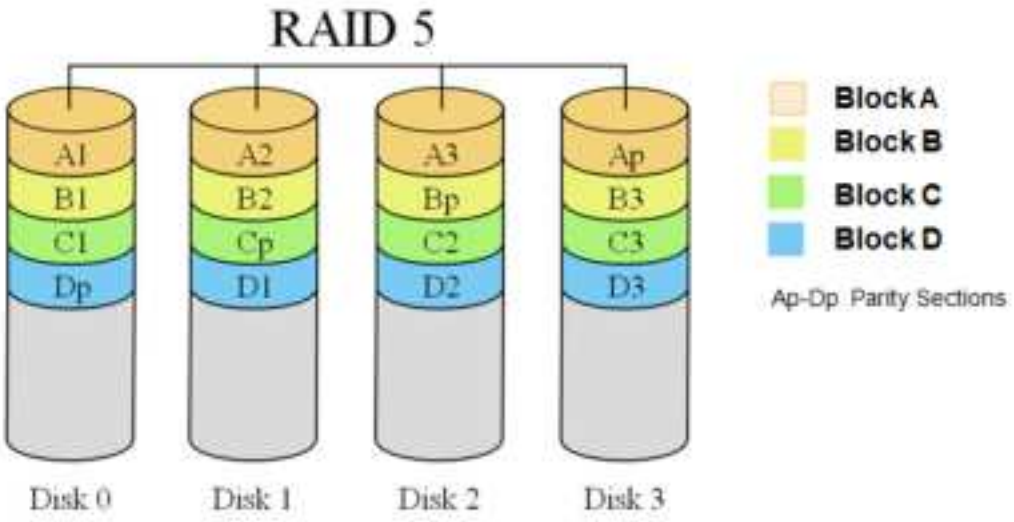
- **RAID 0** – Uses striping to provide extra performance and capacity but does not provide data protection (lack of mirroring or parity).



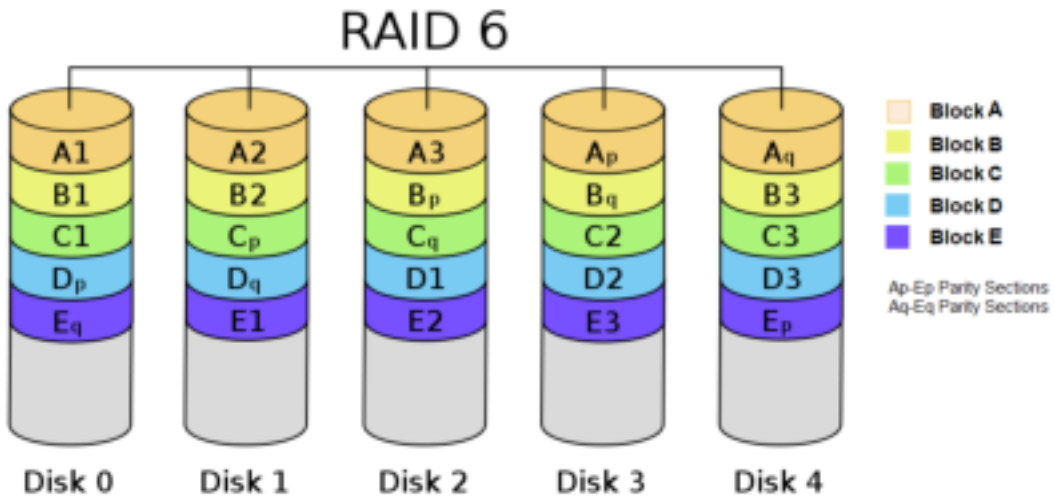
- **RAID 1** – Uses mirroring to provide 1:1 backup, which increases read performance or reliability at the expense of capacity. This configuration is often used with databases due to better transaction time and availability.



- **RAID 5** – Preserves against the loss of any one disk by combining the contents of three or more disks. However, the total storage capacity is reduced by one disk. This configuration is often used with VideoEdge because of RAID 5's performance in situations where data transfers are I/O intensive.



- **RAID 6**- Preserves against the loss of two disks by using striping. This RAID configuration can slow writing times but is excellent for environments that require long data retention periods.



Virtual Disks (Logical Unit Numbers)

1 A virtual disk represents an individually addressable (logical) SCSI device that is a partition of a physical SCSI device (target).

2 Virtual disks are also known as volumes or LUNs.

3 In enterprise-level systems, virtual disks usually represent segments of large RAID disk arrays.

Storage Strategy

In order to properly configure an NVR, it is important to understand how much storage you will require and how to configure it to maximize the overall performance.

To configure storage on an NVR you must consider:

1 Storage

- The type of storage to be used (Internal HDDs, iSCSI external storage, Fiber Optic external storage, USB external hard drives, etc).
- The storage configuration (RAID 0, RAID1, RAID 5, RAID 6, JBOD, etc).

2 Cameras

- Total number of cameras.
- Type of cameras (make/model, resolution, codec, FPS, compression, recording mode).
- The file size of the camera's video stream that is to be recorded.

3 The required recording retention period for stored video.

Below details some different storage usage examples and are compared to the NVR 4.1 storage model:

- **Example 1: Using a 20TB RAID set**

NVR 4.1: 20TB RAID set is divided into 10 2TB logical volumes. There are **10 storage devices** seen on the NVR.

NVR 4.2+: 20TB RAID set can be added as 1 20TB volume. The NVR will recognize this as **1 storage device** that can be used for storage. Alternatively you can create 10 2TB logical partitions. The NVR will recognize this as **10 storage devices** that can be used for storage.

NVR 4.2.1+ (Migrated from 4.1): 20 TB RAID set is still divided into 10 2TB logical volumes. Each 2TB volume is represented as 14 storage devices. The NVR will recognize this as **140 storage devices** that can be used for storage.

- **Example 2: Configuration Set up**

NVR 4.1: Storage configuration is performed using the NVR Administration Interface.

NVR 4.2 - 4.9.1: Storage configuration is performed using Linux YaST/Partitioner.

NVR 5.0+: VideoEdge's auto discovery software performs storage configuration when it detects a suitable storage device.

If you want to use the XFS file system for maximum throughput, additional file system options need to be configured. For Internal devices, you need to configure; **rw,noatime,nodiratime,attr2,nobarrier,noquota,allocsize=4m,inode64**. For external devices, including iSCSI and Fiber Optic, you need to configure; **rw,noatime,nodiratime,attr2,nobarrier,noquota,allocsize=4m,inode64**.

Note:
• **nobarrier** should only be used on storage devices connected to disk controllers with battery backed cache.
• For VideoEdge versions 4.9.1 or earlier, you should also use the **nofail** option for external devices. For example: **rw,noatime,nodiratime,attr2,nobarrier,noquota,allocsize=4m,inode64, nofail**

Understanding Storage Sets

The NVR uses a feature called Storage Sets. These are groups of storage drives and cameras.

For the VideoEdge NVR

By default the NVR has one storage set - Storage Set 1. Initially the default storage set has all detected storage devices, their media folders and cameras assigned to it.

For the VideoEdge Hybrid NVR

By default a storage set is created per drive and all analog cameras connected are assigned to Storage Set 1. If the VideoEdge recorder is configured with RAID storage, one storage set is created by default.

Figure 36 Default Storage Set

A Media Folder is a location on a device where media can be recorded to. Media stored in these folders can include video, audio and analytic media. You can only have one media folder per storage device partition or storage device, depending on your storage configuration. You can choose which media folders on devices are to be used for storage.

Video from the cameras assigned to a particular storage set will record to the media folders on the storage devices that are assigned to the same storage set.

You can easily create additional storage sets and configure them as required to optimize the disk performance, as media can be recorded to storage sets in parallel.

Each storage set must have at least one assigned media folder for storage. You can assign multiple media folders and cameras to a storage set. There is no limit to the number of storage sets you can create. It is recommended that you assign no more than 32 devices or cameras to a particular storage set. For example, if an NVR has a 30 camera license, you could have the following storage set options:

2 Storage Sets

- Storage Set 1 = 15 CAMs record to first set of drive(s)
- Storage Set 2 = 15 CAMs record to second set of drive(s)

Or

- Storage Set 1 = 20 CAMs record to first set of drive(s)
- Storage Set 2 = 10 CAMs record to second set of drive(s)

3 Storage Sets

- Storage Set 1 = 10 CAMs record to first set of drive(s)
- Storage Set 2 = 10 CAMs record to second set of drive(s)
- Storage Set 3 = 10 CAMs record to third set of drive(s)

Or

- Storage Set 1 = 16 CAMs record to first set of drive(s)
- Storage Set 2 = 7 CAMs record to second set of drive(s)
- Storage Set 3 = 7 CAMs record to third set of drive(s)

Note:
1. The lower number of cameras per storage set, the higher achievable throughput. This is due to a lower total data rate required to record to each storage device.
2. High bit rate cameras (e.g. megapixel) should be spread across storage sets for load balancing.

Figure 37 Multiple Storage Sets

Caution

Avoid assigning Virtual Disks from the same Disk Group to different storage sets. If this is done, there is a high probability that continuous disk thrashing will cause the storage device to lock up and cause undesirable results to the NVR.

Calculating Storage Requirements

You need to have enough storage space to fulfill your video recording requirements without data being culled unnecessarily. To ensure you do have enough storage it is important to carefully calculate your storage requirements.

Procedure 139
Calculating Storage Requirements

Step	Action
1	Determine the quantity of Edge Devices and Anticipated Settings Make/Model, Codec/Rez/FPS/Compress, Activity, Record Hours.
2	Calculate the Data Rate for each device using Vendor Calculators. For example; • AD http://www.americandynamics.net/calculators/calc_4C_VideoEdge_IP_Encoder.html • Axis http://www.axis.com/products/video/design_tool/calculator.htm

- Sony
  http://pro.sony.com/bbsccms/ext/cat/camsec/cameraCalc3/HTML/NTSC_Calculator.html

3 Enter the required information into the NVR Storage Requirement Calculator.

http://www.americandynamics.net/calculators/Calc_NVR_Storage_Requirement.html

4 The calculator output provides the **Total Storage for All Cameras** and the **Total Bandwidth for All Cameras**.

You may need to lower the camera count per NVR to meet network and storage requirements when dealing with many cameras, large resolution, or retention.

- End -

Overview of AD Fiber RAID Storage (FRS/FES)

Fiber RAID Storage is an NVR extended storage device acting as a Fiber Direct-Attached Storage (DAS) or iSCSI device.

As a Fiber device, a Fiber Host Bus Adapter (HBA) must be installed in the NVR and uses Fiber Optic cable connection.

As an iSCSI device, 3rd Gigabit Ethernet NIC must be installed in the NVR and uses CAT 5e/6 Ethernet connection. This is already installed in the NVR servers.

Second Generation American Dynamics iSCSI and Fiber RAID Storage

The second generation American Dynamics iSCSI and Fiber RAID Storage solutions are designed for high-performance recording devices. They are secure and highly scalable storage solutions that provide SAN storage for virtually any network and application.

The new Rack Mount models are available in a variety of configurations and capacities. There are iSCSI RAID, 4Gb Fiber RAID, and Expansion models which have been uniquely designed to utilize the same 3U chassis. These storage solutions come standard with redundant power supplies and fans, and nearly every component is hot-swappable, including sixteen lockable hot-swap drives. An optional battery backup module is also available for the iSCSI and Fiber RAID units.

Storage Strategy for FRS/FES RAID Device

Recommendations

- The FRS/FES supports a maximum of eight (8) Disk Groups (aka RAID sets).

- Each Disk Group can be “carved up” into one or more Virtual Disks (aka Volumes or LUNs). It is recommended to try to maximize each virtual disk size.
- It is recommended that Virtual Disks from a single Disk Group are all assigned to the same NVR Storage Set. This will eliminate the possibility of unnecessary disk thrashing caused when the same set of physical disks (DGs) are being used by different sets of cameras (aka Storage Sets).
- Verify that you have the latest firmware patch or upgrade for your controller.
- Make sure to leave a minimum of a 2U space between storage units.
- Start the camera’s recording after all the drives have been formatted and their status is “Normal”.

Connecting Additional Storage Devices

Connecting Storage to the NVR via eSATA

Note:
This task applies to Hybrid NVRs only

Before configuring external storage it is recommended that you stop NVR Services.

Once you have connected and configured external storage devices, you must restart the NVR Services.

Procedure 140
Connecting Storage to the NVR via eSATA

Step	Action
1	Power OFF the NVR and connect the eSATA Storage to the NVR via the eSATA port.
2	Reboot the NVR and log in to the NVR desktop as the Root User.

- End -

Connecting Storage to the NVR via USB

You can add USB storage to any VideoEdge model that has a USB port.

Connecting NVR to FRS/FES Using Fiber

Before configuring external storage you must stop NVR Services.

Once you have connected and configured external storage devices, you must restart the NVR Services.

Procedure 141
Connecting NVR to FRS/FES Using Fiber

Step	Action
1	Power OFF the NVR and install the Fiber HBA Kit (PCI-e). Connect the AD Fiber RAID Storage to the NVR.
2	Reboot the NVR and log in to the NVR desktop as the Root User.

- End -

Connecting NVR to FRS/FES Using iSCSI

Before configuring external storage you must stop NVR Services.

Once you have connected and configured external storage devices, you must restart the NVR Services.

Procedure 142
Connecting NVR to FRS/FES Using iSCSI

Step	Action
1	Power OFF the NVR and install the iSCSI NIC Card (LAN3) into correct and compatible slot.
2	Connect the iSCSI RAID Storage device to a switch or directly to NVR LAN3 to ensure that it is accessible.
3	Open web browser.
4	Enter the IP address of the iSCSI storage device into the **Address** field. The web configuration interface for the iSCSI storage device opens.
5	Enter the **User name**. **Note:** The default User name is **admin**.
6	Enter the **Password**. **Note:** The default Password is **admin**.
7	Set up the NIC IP settings for the iSCSI port: a Select **iSCSI Configuration** from the iSCSI RAID Rack menu. The iSCSI Configuration sub-menu items are displayed. b Select **NIC**. A summary of all NICs available in the storage device are displayed. c Check the values in the **Link** fields. If the value is **Up**, this represents that a cable is present connecting the storage device and the NVR. This is the NIC you need to configure. d Select the dropdown list in the **Name** field for the NIC with the **Link** field value set to Up. e Select **IP Settings for iSCSI ports** from the dropdown list. The NIC IP settings page opens. f If required, edit the Static **Address**, **Mask** and **Gateway**. **Note:** If there are no DHCP settings available these fields will contain the default values, Address: 10.10.10.20, Mask: 255.255.255.0 and Gateway: blank. g Click **Confirm**. The NIC settings page closes and the NIC summary details are displayed.
8	Create a Node to associate the storage NIC with an NVR port: a Select **Node** from the iSCSI Configuration sub-menu. b Click **Create**.

c Enter a **Name** for the Node.

d Select the type of **Authentication** from the dropdown list. The default is **None**.

Note:
Select **CHAP** to use a password for data transfer.

e Select the checkbox for the required **Portal**. This is the portal which contains the NIC IP address.

f Click **Confirm**.

9 Assign the required Virtual Drives a LUN:

Note:
The Virtual Drives are pre-configured on the storage device.

a Select Volume configuration from the iSCSI RAID Rack menu.

The Volume configuration menu expands.

b Select **Logical Unit**.

c Click **Attach**.

d Select the virtual disk from the **VD** dropdown list.

e Select the LUN from the **LUN** dropdown list.

f Click **Confirm**.

The Virtual Disk is assigned to the LUN and appears in the Logical unit summary table.

g Repeat Steps c to f to assign all the required Virtual Disks to a LUN.

10 Configure the Network Settings on the NVR:

a Log in to the NVR desktop as the Root user.

b Select Computer.

c Select YaST from the System menu.

d The Control Center opens.

e Select Network Settings from the Network Devices section.

The Initializing Network Configuration window displays momentarily and the Network Settings page opens.

f Select the **Overview** tab.

g Select the storage network card.

h Click **Edit**.

i Select the **Statically assigned IP Address** option button.

j Enter the **IP Address**.

k Enter the **Subnet Mask**, 255.255.255.0.

l Enter the **Hostname**.

m Click **Next**.

n Click **OK**.

o Close the Network Settings window.

11 Test the network connection between the NVR and the iSCSI storage device:

a Double-click **GNOME Terminal** on the desktop.

The Terminal window opens.

b Type ping followed by the IP address of the storage device, for example, ping 192.168.8.1. Press **[Enter]**.

Note:
If the connection is unsuccessful, a 'Destination Host Unreachable' message is displayed. Check the connections and network settings and retry.

c Close the Terminal window.

12 Connect the storage device using the iSCSI initiator:

a In the Control Center, enter iSCSI into the Filter field.

b Select **iSCSI Initiator**.

The iSCSI Initiator Overview window opens. The Discovered Targets tab displays the discovered storage devices. At this stage the value in the Connected field is False.

c Select the **Service** tab.

d Select the **When Booting** Service Start option button.

e Select the **Discovered Targets** tab.

f Click **Discovery**.

g Enter the **IP Address**.

Note:
This is the IP Address of the storage device.

h Enter the **Port**. The default port number is **3260**.

i Select the **No Authentication** checkbox.

j Click **Next**.

The iSCSI storage device is listed in the Discovered Targets table.

k Select the storage device and click **Log In**.

l In the **Startup** field select **Automatic** from the dropdown list.

m Click **Next**.

The value in the **Connected** field has been updated to True. This means the storage device is connected to the NVR.

n To confirm the storage session is connected, log into the storage web interface (see Steps 3 to 6), select the **iSCSI configuration** in the menu, select **Session** and ensure the session is connected with the correct initiator name.

- End -

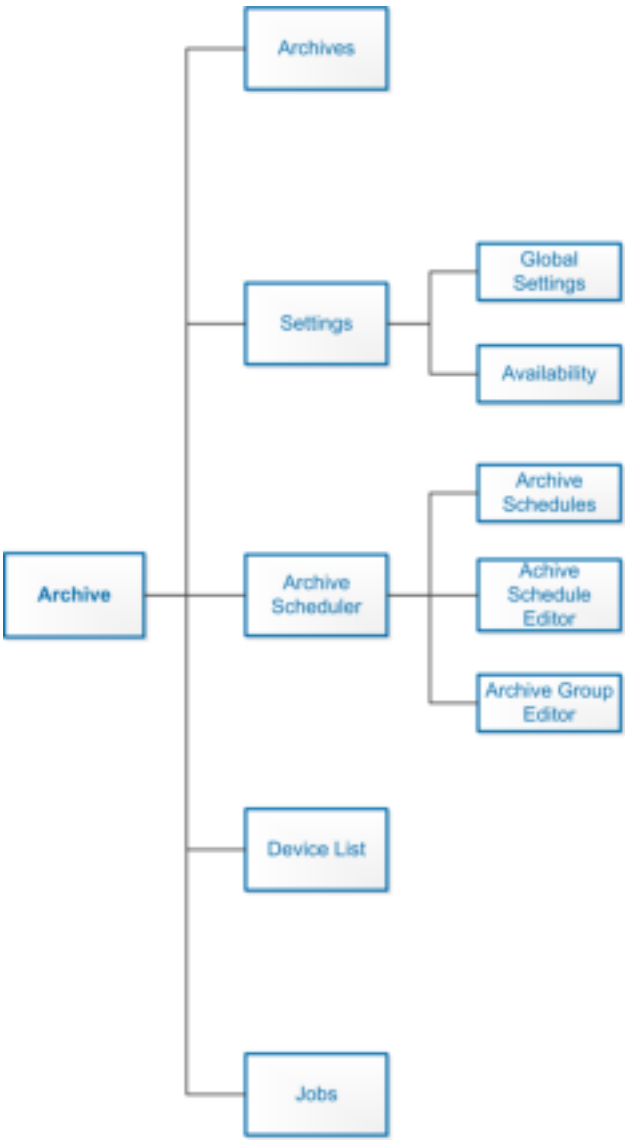
Overview

The VideoEdge's Archiving feature allows you to save to and retrieve video from long term storage in the form of a dedicated Network Attached Storage (NAS).

Note:
Network Attached Storage devices may require pre-configuration before they can be used for archiving tasks. Refer to your products Installation and User Manual for more information.

The Archive menu allows you to add and configure Archive destinations, apply global settings, select video devices for archiving and view outstanding archiving operations.

Figure 38 Archive Menu Map



- **Archives** - From here you can add, remove, enable or disable archiving destinations connected to the NVR.
- **Settings** - From here you can configure global archive settings for each archive destination, you can also configure the periods of availability where the NVR can write to the archive destination.
- **Archive Scheduler** - From here you can create Archive Groups and Schedules which define which video is to be automatically archived.
- **Device List** - From here you can enable/disable which video devices are to archive video. You can also define the archiving quality and maximum retention period of the archived video.
- **Jobs** - From here you can view a list of all outstanding archiving operations. You can also delete outstanding archiving jobs you no longer want to occur.

Archiving Considerations

Archiving is a server side function which utilizes the NVR's network bandwidth, disk I/O and CPU resources. This must be taken into account during installation and operation. The NVR can only archive video, audio cannot be archived.

Archiving of video can either be carried out manually or automatically. Manual archiving can be initiated using victor unified client, the selected video is written to the active Archive Destination. A journal entry is created on completion stating whether the archiving task was successful.

Note:
If errors are returned as a result of a manual archive requests, they only relate to issues that were detected during the queuing of the request.

Automatic archiving is configured using the NVR Administration Interface and allows you to archive video from selected cameras during scheduled times of the day. Scheduling times are set in one hour periods throughout the day, Monday through to Sunday. Video is written to the archive in defined periods of archive availability allowing you to manage CPU load on your NVR. Should archiving fall behind an alarm is generated.

Video is archived in a Common Internet File System or CIFS (also known as Server Message Block or SMB) file structure organized by camera and date and written in an open format allowing playback in 3rd party media players. Video is archived in files of 5 minutes in length. Additional configuration data such as login credentials, domain and server IP Addresses are entered using the VideoEdge Administration Interface.

Archiving with offline recording

When you enable the TrickleStor feature, cameras can continue to record footage while the VideoEdge is offline.

When the VideoEdge reconnects to the cameras, the camera footage transfers back to the VideoEdge. If you include these cameras in an archiving schedule, any camera footage from the scheduled archive time is transferred to the archive.

Archives

Archive Destinations

Adding an Archiving destination is carried out using the Archive menu item in the NVR Administration Interface. You can add multiple Archive Destinations to the NVR, but only one Archive Destination can be used at a time. When you add an Archive Destination it is listed in the Archives Table.

Note:
You must create an Archive Destination before you can archive video.

Figure 39 Archives Page

The NVR will write to the selected Archive Destination only. Archive Destinations can be assigned one of three states:

- **Locked** - The NVR will not modify any of the data on the destination either by culling or writing new data.
- **Unlocked and not the active destination** - The NVR will not modify any of the data on the destination either by culling or writing new data.
- **Unlocked and the active destination** - Only one destination can be enabled and active, the NVR will cull data and write new archive data to this destination.

Note:
For installation and user instructions when using a dedicated NAS device refer to its Installation and User Manual.

Procedure 143
Adding an Archive Destination

Step	Action
1	Select **Archive** from the main menu.
2	Select **Archives**. The Archives page opens.
3	Click ⊕ A configuration window opens.
4	Enter the **Archive Name**.

Note:
Archive Name can consist of alphanumeric characters plus 'space', "_", "-" and "."

5 Enter the **Network Path**.

Note:
The Network Path consists of either a device hostname when DNS is in use or an IP address when it is not. For example:

1. With DNS and a shared folder named **NvrShare** - \\Hostname\NvrShare\
2. With no DNS and a shared folder named **NvrShare** - \\0.0.0.0\NvrShare\

6 (Optional) Enter the **Domain**.

7 Enter the **Username** required to access the shared directory on the Archive Destination.

8 Enter the **Password** required to access the shared directory on the Archive Destination.

9 (Optional) Select the **Locked** checkbox to make the destination read only.

10 (Optional) Click **Test Connectivity** to check the destination is correctly configured.

11 (Optional) Select the **Enabled** checkbox to enable the destination as the active archive.

12 Click 

- End -

Editing Settings in the Archives Table

Archive Destination settings can be edited in the Archives Table; these include Archive name, destination and lock status on the Archive Configure Page.

Procedure 144
Editing the Archive Destination Details in the Archives Table

Step	Action
1	Select **Archive** from the main menu.
2	Select **Archives**. The Archives page opens
3	Select  A configuration window opens.
4	Edit the **Archive Name** in the Name field.
5	Edit the **Network Path** in the Network Path field.
6	(Optional) Edit the **Domain** in the Domain field.
7	Edit the **Username** required to access the shared directory on the Archive Destination.
8	Enter the **Password** required to access the shared directory on the Archive Destination.
9	(Optional) Select the **Locked** checkbox to make the destination read only.
10	(Optional) Click **Test Connectivity** to check the destination is correctly configured.
11	(Optional) Select the **Enabled** checkbox to enable the destination as the active archive.

12	Click 

- End -

Locked and Unlocked Archives

Archive Destinations can be locked or unlocked. When an archive is locked it is read only and can only be used to retrieve archived video.

Procedure 145
Locking Archives in the Archives Table

Step	Action
1	Select **Archive** from the main menu.
2	Select **Archives**. The Archives page opens
3	Select  A dialog box opens notifying that 'This will Lock the destination named: xxxx'
4	Click **OK**.

- End -

Procedure 146
Unlocking Archives in the Archives Table

Step	Action
1	Select **Archive** from the main menu.
2	Select **Archives**. The Archives page opens
3	Select  A dialog box opens notifying that 'This will unlock the destination named: xxxx'
4	Click **OK**.

- End -

Enabling/Disabling an Archive Destination

An Archive Destination can be selected as the active destination by enabling it. Alternatively an Archive Destination can be deselected as the active destination by disabling it.

Procedure 147
Enabling an Archive Destination

Step	Action
1	Select **Archive** from the main menu.
2	Select **Archives**. The Archives page opens
3	Select the checkbox in the Archives Table for the destination you want to enable.
4	Click 

- End -

Procedure 148
Disabling an Archive Destination

Step	Action
1	Select **Archive** from the main menu.
2	Select **Archives**. The Archives page opens
3	Select the checkbox in the Archives Table for the destination you want to disable.
4	Click 

- End -

Manually Archiving Video

Video can be manually selected for archiving using victor unified client. When video is archived manually it is written to the active Archive Destination.

You can view the status of the archive requests using the NVR Administration Interface and a journal entry is created on completion stating if the archiving task was successful.

For further information on manually archiving video refer to the victor unified client User Guide.

Retrieving Archived Video Using victor unified client

Archived video can be retrieved using victor unified client. For more information refer to the victor unified client User Guide.

Viewing Archived Video in a 3rd Party Media Player

Archived Video is saved in an MP4 format. Archive video can be viewed by a 3rd Party Media Player.

Video is archived in a user interpretable fashion; for example when a CIFS destination is used for archiving, the folder structure will contain folders for camera, year, month, day and so on with the relevant MP4 files contained within. The folders can then be navigated to find the required archived video file for playback with a 3rd party application.

Note:
3rd Party Media Players are unable to validate video.

Procedure 149
Viewing Archive Video in a 3rd Party Media Player

Step	Action
1	Navigate to the required MP4 file in the archive folder structure.
2	Right click on the MP4 file and select Open with.
3	Select the 3rd Part Media Player from the list.

- End -

Settings

Global Settings

Global settings are available on the Settings menu item in the Archives menu. Global settings allow you to quickly enable/disable automatic archiving, the active Archive Destination and FIFO archive culling.

Note:
• If you create an archiving schedule before you enable automatic archiving, you may have an archiving backlog. When you enable Automatic archiving, the earliest footage in the backlog is archived first. To skip the archiving backlog, and begin archiving from the time when Automatic archiving is enabled, select the **Skip archiving backlog checkbox**.
• FIFO (First In, First Out) archive culling is a basic form or data culling which will cull data based on the date it was written to the archive, i.e. the oldest data is culled. Archive culling can also be configured based on retention rules.

Figure 40 Global Setting Page

You can also configure a retry count and retry interval which dictates the NVR's behavior should archiving be unsuccessful due to a loss of connection with the archive, the archive becoming unreadable, or the destination being full and culling is disabled.

For example if a retry count of 2 is applied with 30 minute intervals, when the NVR attempts to archive the clip and a failure to write occurs the system will wait 30 minutes and then re-attempt to write the data. After the second failure to write the system will not try again. In this instance you will have to manually archive the data.

Procedure 150
Applying System Wide Settings

Step	Action
1	Select **Archive** from the main menu.
2	Select **Settings**.
	The Global Settings page opens.
3	Click the **Enabled** option button to enable Automatic Archiving.
	Or
	Click the **Disabled** option button to disable Automatic Archiving.
4	Select the **Archive Destination** from the Archive Destination dropdown.
5	(Optional) Select the **Skip archiving backlog** checkbox if required.
6	Click the **Enabled** option button to enable Archive culling.

Or

Click the **Disabled** option button to disable Archive culling.

Note:
• Archive culling starts when the archive reaches 95% capacity.
• If you disable archive culling, archiving stops when the archive is full.

7 Enter a **value for the Retry count** in the Retry count field.

8 Enter a **value for the Retry interval** in the Retry interval field.

9 Click  .

- End -

Availability

Archive availability schedules are user configured times when the NVR can archive video. This can be used to minimize the effect of archiving on the NVR's network bandwidth, disk I/O and CPU resources by scheduling archiving when minimal activity is expected.

Note:
The Archive availability schedule does not affect manual archiving.

Procedure 151
Configuring an Archive Availability Schedule

Step	Action
1	Select **Archive** from the main menu.
2	Select **Settings**. The Global Settings page opens.
3	Select the **Availability** tab.
4	Select the **Availability schedule Enabled** option button. A dialog box opens stating 'This will enable the availability scheduler. Select OK to continue'. Click **OK**. **Note:** When the Availability schedule is disabled, archiving will not be restricted when automatic archiving is configured, i.e. the NVR will write to the archive 24 hours a day.
5	To allocate defined time windows of archive availability: a Select the Archiving availability **Available** option button to assign availability Or Select the **Not Available** option button to remove availability. b Select individual cells to assign/remove availability. Or c Select the row heading to assign/remove availability for an entire day.

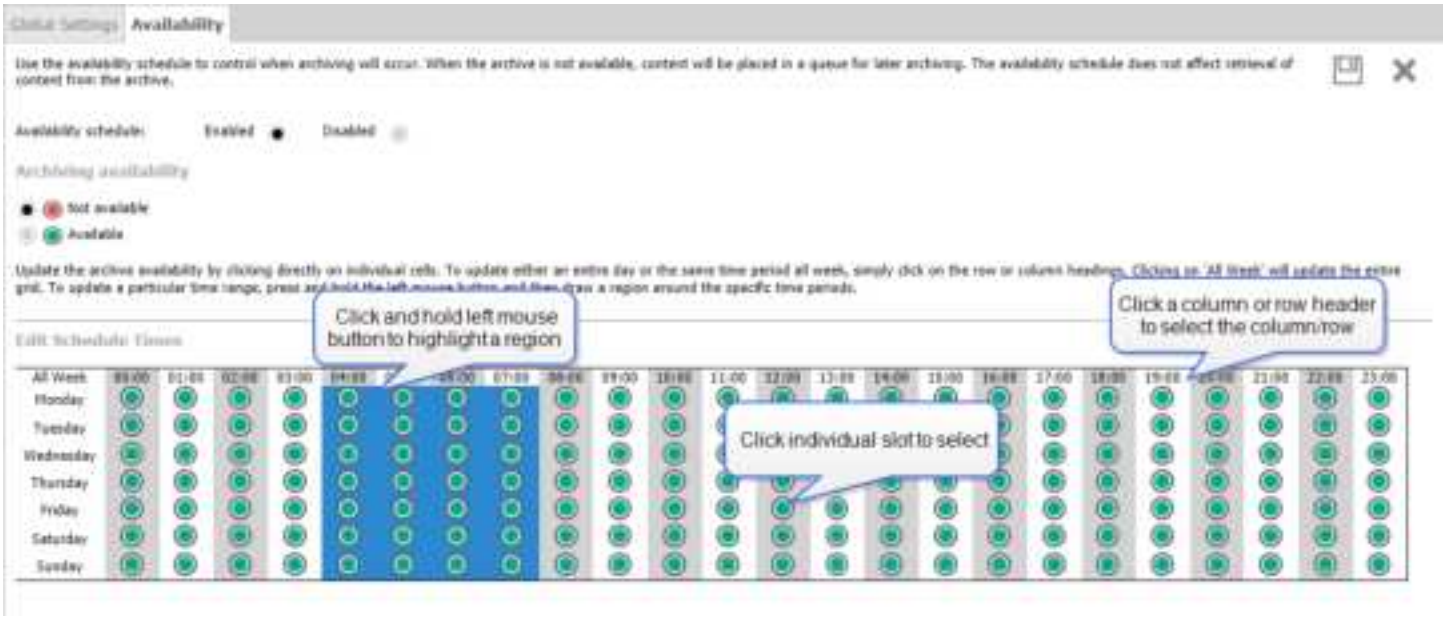
Or

d Select the column heading to assign/remove availability to the same hour for every day of the week.

Or

e Press and hold the left mouse button, then draw a region around specific time slots to assign/remove availability.

Figure 41 Archive Availability Schedule



6 Click 

- End -

Archiving Quality (Framerate Decimation)

Archiving Quality is defined as a percentage of applied Framerate Decimation. You can use Framerate Decimation to reduce the amount of data which is archived. This is achieved by reducing the frame rate of the video being archived, for example by applying an Archiving Quality of 50% you are reducing the frame rate by 50%. Framerate decimation does not have any effect on the video's resolution.

Archiving quality can be applied in 10% intervals where 10% provides the lowest quality video and 100% provides the highest quality video for archiving.

Note:
This function may have limitations based on codec, for example H.264 and MPEG-4 only support decimation at key frame level

Procedure 152
Configuring the Archiving Quality

Step	Action
1	Select **Devices**.
2	Select **List**. The Device List page opens.
3	Click  in the device record you want to edit.
4	Select the **Archive** tab.
5	Select the **Archiving Quality** from the dropdown.
6	Click 

- End -

Archive Management

Archive management is achieved automatically by configuring the NVR to automatically remove video based on retention rules.

When you configure the NVR to automatically manage an archive, video will be removed as per its retention period or culling will occur when the archive storage is full, similar to the management of video on local storage.

The ability to automatically remove video from the archive may be dependent on the capabilities of a specific Archive destination.

Maximum Archiving Retention Period

You can configure the NVR to cull archived data using a retention period. The NVR will cull data once it has exceeded the retention period.

Procedure 153
Enabling the Maximum Archiving Retention Period for individual cameras

Step	Action
1	Select **Devices**.
2	Select **List**. The Device List page opens.
3	Click  in the device record you want to edit.
4	Select the **Archive** tab.
5	Select the Archiving Mode. **Note:** To enable archiving, you must select one of the following option buttons: **Archive all video** or **Archive only alarm video**.
6	Configure the Maximum Archiving Storage Period.

Select **Custom** from the dropdown menu, then enter a retention period in the **Period** field.

Or

Select **As long as possible** from the dropdown menu.

7 Click 

- End -

Archive Scheduler

The NVR can be configured for automatic archiving by utilizing the Archiving Scheduler. The Archiving Scheduler allows you to define time periods during which video is queued for archiving. This schedule is configured in the Archive Schedules tab. After you configure an Archive schedule, you can assign one or more cameras to that schedule, these cameras form a group. Each group can have scheduled times and archiving modes assigned for queuing video for archiving.

Video that is queued for archiving will be transferred to the archive destination when the next period of archive availability in the Archive Availability Schedule is reached. This schedule is configured in the Archive Availability tab. Archive Schedules and Archiving Modes can be applied to reduce the amount of video that is archived.

Note:
If you disable the Archive Availability Schedule, the NVR can write video to the archive at any time of the day.

Use the Schedules page to enable or disable the Archiving Scheduler. Archiving Schedules can be created and edited from the Archive Schedules page.

Procedure 154
Enabling/Disabling the Archiving Scheduler

Step	Action
1	Select **Archive** from the main menu.
2	Select **Archive Scheduler**. The Archive Schedules page opens.
3	To enable the Archiving Scheduler, click the **Enabled** option button. Or To disable the Archiving Scheduler, click the **Disabled** option button.

- End -

Procedure 155
Creating an Archiving Schedule

Step	Action
1	Select **Archive** from the main menu.
2	Select **Archive Scheduler**. The Archive Schedules page opens.
3	Click 
4	Enter a name in the **Schedule Name** field.
5	Click 

- End -

Procedure 156
Renaming an Archive Schedule

Step	Action
1	Select **Archive** from the main menu.
2	Select **Archive Scheduler**. The Archive Schedules page opens.
3	Click  next to the Archive Schedule name you want to edit.
4	Enter the new name in the text field.
5	Click 

- End -

Schedule Editor and Group Editor Pages

When you create an Archiving Schedule using the Archiving Scheduler, you need to assign cameras to that schedule, these cameras form a group. Groups can consist of an individual camera or groups of cameras. Each group can have scheduled times and archiving modes assigned for queuing video for archiving.

There are three archiving modes available in the Archiving Scheduler:

- Automatic archiving disabled
- Automatically archive all recorded video
- Archive only recorded alarm video.

You can assign multiple archiving modes to a group, only one mode can be selected at any one scheduled time. For example you can schedule a group to queue video for archiving by selecting the mode **Automatically archive all recorded video** between 09:00 to 18:00 Monday through to Friday, and schedule the same group to archive only recorded alarm video by selecting the mode **Archive only recorded alarm video** between 19:00-23:00 Monday through to Friday.

Procedure 157
Assigning Cameras to a Group

Step	Action
1	Select **Archive** from the main menu.
2	Select **Archive Scheduler**. The Archive Schedules page opens.
3	Select  of the Archive Schedule you want to edit. The Archive Group Editor page displays.

Figure 42 Archive Group Editor

4 To add cameras to a group:

a Select the checkbox of the camera you want to add from the **All other devices** list.

b Click

Or

To remove cameras from a group:

a Select the checkbox of the camera you want to remove from the **This group** list.

b Click

5 Click

- End -

Procedure 158
Editing the Queuing Times of an Archive Schedule

Step	Action

1 Select **Archive** from the main menu.

2 Select **Archive Scheduler**.

The Schedule page opens.

3 Select of the Archive Schedule you want to edit.

The Archive Schedule Editor tab displays.

4 To configure queuing times for archiving:

a Select the **Automatic archiving disabled** option button to disable queuing for archiving during selected time increments.

Or

Select the **Automatically archive all recorded video** option button to queue for archiving all video during selected time increments.

Or

Select the **Archive only recorded alarm video** option button to queue for archiving all video recorded under alarm conditions during selected time increments.

b Select individual cells to assign/remove availability.

Or

c Select the row heading to assign/remove availability for an entire day.

Or

d Select the column heading to assign/remove availability to a time slot for an entire week.

Or

e Select **All Week** to assign/remove availability to all time slots within a week.

Or

f Press and hold the left mouse button, then draw a region around specific time slots to assign/remove availability.

5 Click 

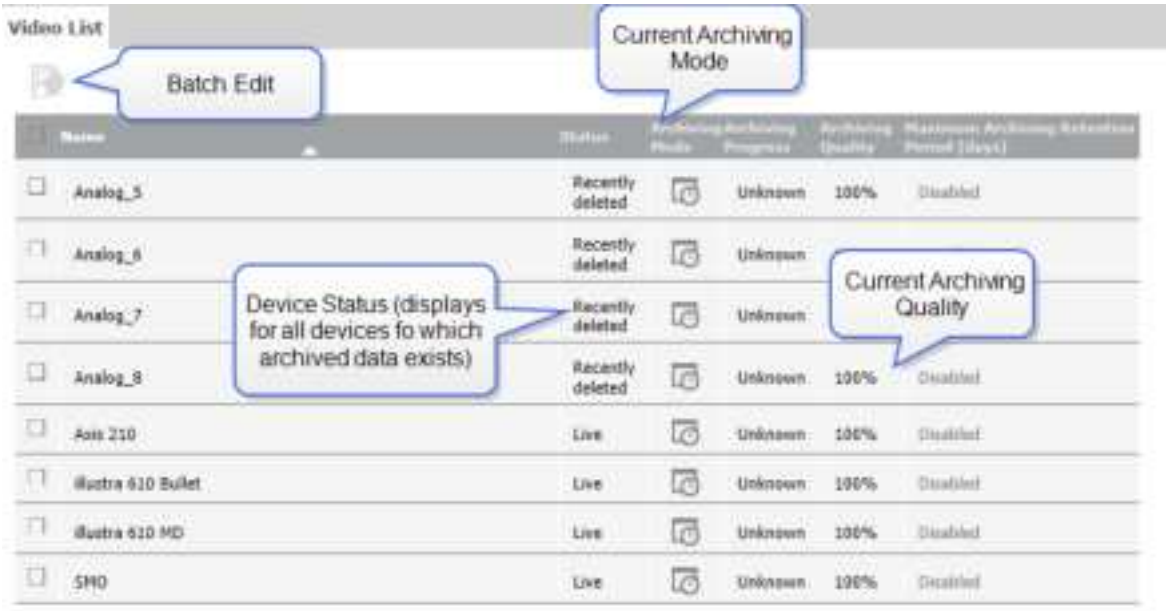
- End -

Device List

The Device List menu item displays a list of all devices which have been added and have recorded video on the NVR's memory. Devices which have been deleted will remain on the device list until all their remaining video has been culled from the NVR's memory.

You can batch edit the Archiving Mode, Archiving Quality and Maximum Archiving Retention Period for the video devices found in the Archiving Device List.

Figure 43 Archiving Device List



Procedure 159
Batch Editing Archive Settings using the Device List sub menu

Step	Action
1	Select **Archive** from the main menu.
2	Select **Device List**. The Video List page opens.
3	Select the checkboxes of the cameras you want to edit.
4	Click  The Batch Edit page opens.
5	Select the checkbox followed by the required **Archiving Mode** option button: • **Archiving disabled** • **Archive all video** • **Archive only alarm video**
6	Select the checkbox followed by the required **Archiving Quality** setting from the dropdown.
7	Select the checkbox followed by the required **Maximum Archiving Retention Period** from the dropdown.

8 Click 

- End -

Jobs

The Jobs page lists all outstanding queued archiving tasks.

Viewing and Deleting Manual Archiving Tasks

You can view current manual archiving tasks in the Jobs page. Tasks which you no longer want to be carried out can be deleted.

Procedure 160
Viewing/Deleting Current Manual Archiving Tasks

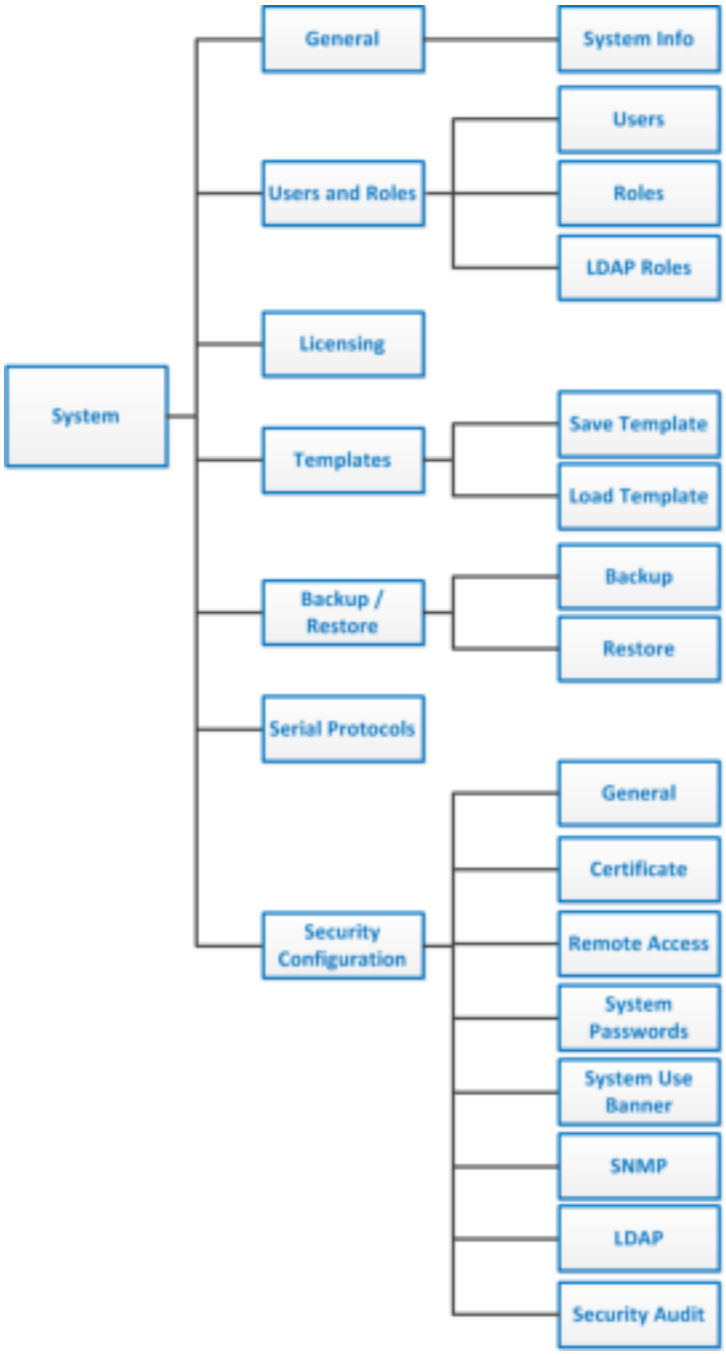
Step	Action
1	Select **Archive** from the main menu.
2	Select **Jobs**. The Job page opens.
3	(Optional) Select the checkboxes next to the tasks you want to delete.
4	Click 

- End -

System Menu Overview

The **System** Menu allows you to configure the NVR's basic system settings; Users and Roles, Licensing, Template files, Backup/Restore, software updates, Serial Protocols and the NVR's Security Configuration.

Figure 44 System Menu Map



- **General** - From here you can edit the Hostname, Location, Date & Time and Language. You can also download the public key.
- **Users and Roles** - From here you can create new user accounts, edit existing accounts, apply lockout polices and auto logout (Lockout and logout polices are OFF by default).You can also designate role types for LDAP groups.
- **Licensing** - From here you can apply a license file to your NVR, configure Software Service Agreement notifications and generate your NVR's Host ID.
- **Templates** - From here you can create a Template file or alternatively load a Template file.
- **Backup/Restore** - From here you can create a Backup file or alternatively restore an NVR from a Backup file.
- **Serial Protocols** - From here you can view the Serial Protocols supported by your NVR and their default settings.
- **Security Configuration** - From here you can edit the Auto-logout settings, Certificate settings, Remote Access settings, System Passwords, System Use Banner, SNMP and LDAP settings. Enhanced security configuration is OFF by default. From the security Audit menu you can review a summary of the VideoEdge's security settings.

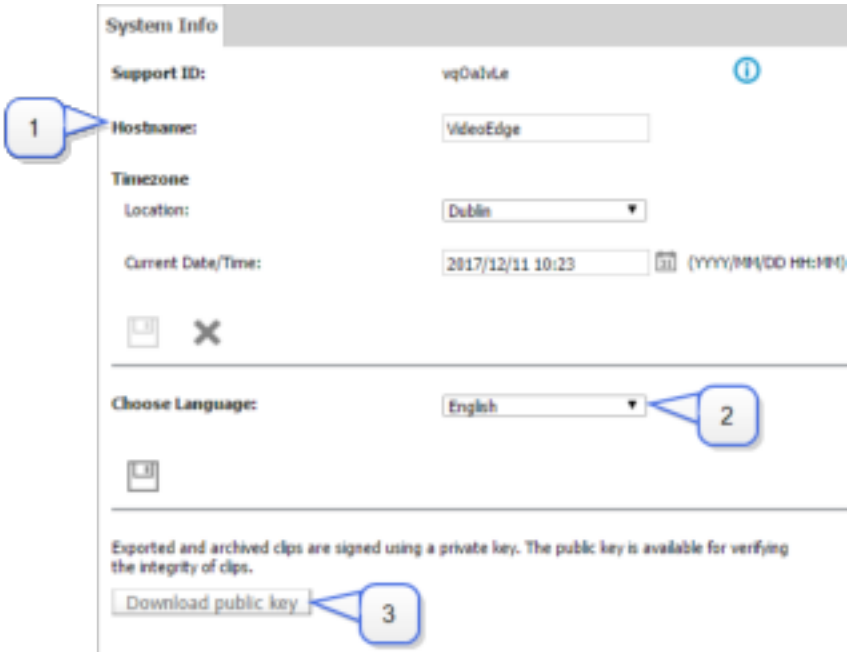
General

The General System Information page allows you to edit the hostname, i.e. the name assigned to the NVR, the location, date and time, selected language and download the public key.

For playback to work reliably it is imperative that the time between the client and the NVR is synchronized. This is best achieved using an NTP server to synchronize the time on both the client and the NVR.

Note:
• The same NTP server should be used to synchronize the time settings on both the client and the NVR. This can be achieved using a NTP server on the internet or by configuring an NVR to act as a NTP server.
• The VideoEdge hostname must not exceed 15 characters in length.

Figure 45 System Info Page



Key	Definition
1	Configure Hostname, Location and Date/Time.
2	Select language.
3	Download the public key.

Hostname

The Hostname of the NVR can be changed. This provides you the ability to use a bespoke hostname to identify multiple NVRs on a network and in victor client. When the hostname of an NVR is changed it will automatically change in the device list within victor client.

Procedure 161
Editing the Hostname

Step	Action
1	Select **System** from the main menu.
2	Select **General**. The System Info tab displays.
3	To edit the **Hostname** select the current value. Update the Hostname as required. **Note:** The NVR hostname may contain alphanumeric characters, dots, and hyphens. However, the dot and the hyphen are not allowed at the start or the end of the hostname.
4	Click 

- End -

Location

The location of the NVR can be defined. A dropdown list provides a list of cities for you to choose from. If the current location of the NVR is not included in the list, it is recommended that you select the nearest city available.

Note:
When using an NTP Server the location is used to define the time and date as NTP servers use UTC time.

Procedure 162
Editing the Location

Step	Action
1	Select **System** from the main menu.
2	Select **General**. The System Info tab displays.
3	To edit the **Location** select the city of the NVR or nearest city listed from the dropdown.
4	Click 

- End -

Current Date and Time

The current date and time on an NVR can be manually edited. When using an NTP Server the Time will be synchronized with the server.

Note:
When using a NTP Server the location is used to define the time and date as NTP servers uses UTC time.

Caution

It is critical that you configure the correct Location and Current Date/Time to ensure the VideoEdge NVR is fully operational on completion of the setup wizard and to ensure recorded media has the correct timestamp.

Procedure 163
Editing the Current Date and Time

Step	Action
1	Select **System** from the main menu.
2	Select **General**. The System Info tab displays.
3	To edit the **Current Date** and **Time**, select the current value. Update the Current Date and time as required, enter the date in the field in the following format; **YYYY/MM/DD** for example 2012/01/01. Or a Select  The Calendar opens. b Select the date from the calendar.
4	Enter the time in hours and minutes after the date. You can also use the sliders to adjust the time. **Note:** Time must be entered in 24 hour format.
5	Click 

- End -

Language Setting

The displayed language of the NVR Administration Interface can be changed using the System Info page.

Procedure 164
Changing the Selected Language

Step	Action
1	Select **System** from the main menu.
2	Select **General**. The System Info page opens.
3	Select the required language from the **Choose Language** dropdown.
4	Click 

- End -

Downloading the Public Key

Each NVR has a unique public key which can be downloaded from the System Info page. The public key is used for clip verification using either victor player or victor unified client.

Note:
Verification using the NVR's public key can only be carried out on exported packages, i.e. the zip container with its corresponding ExportInfo.Xml.

Procedure 165
Downloading the NVR's Public Key

Step	Action
1	Select **System** from the main menu.
2	Select **General**. The System Info page opens.
3	Click **Download public key**. A Windows dialog box opens.
4	Click  The public key is saved as a PEM File and can be viewed using Windows Notepad.

- End -

Users and Roles

You can create custom user credentials for each of your NVR's users. Each user credential can be assigned a role which denotes its permissions and lockout options.

Caution

For improved security, you are strongly advised to change the account passwords, configure appropriate lockout settings and enable auto logout.

You can also configure role permissions for LDAP groups which have been configured on your LDAP server.

Users

From the Users page you can create, edit and delete user credentials for users and edit the passwords for the nine default users i.e. softwareadmin, admin, nvrgroupadmin, operator, snmpuser, support, viewer1, viewer2 and viewer3. The default users cannot be deleted.

Note:
Each of the default user types have a corresponding role. These roles determine user account permissions on the VideoEdge.

New users can be created by clicking  . You can assign a username and password for a new user. The user's role can be selected from the **Role** dropdown list; the following roles are available:

- **softwareadmin** - Allows access to the software update page only. This credential is used solely for carrying out software updates and installing camera handler packs. The default password for this role is **softwareadmin**.
- **admin** - Allows viewing and editing of the VideoEdge Administration Interface and full functionality of the VideoEdge Client. The default password for this role is **admin**.

Note:
Only user accounts with the admin role can change or reset passwords for other users.

- **operator** - Allows viewing of the VideoEdge Administration Interface and full functionality of the VideoEdge Client. The default password for this role is **operator**.
- **support** - The support user role is solely for the use of American Dynamics Technical Support.

Note:
For systems which are not part of the VideoEdge Hybrid product range, user roles viewer1, viewer2 and viewer3 cannot be used when creating user credentials as they do not permit access to the NVR Administration Interface.

- **viewer1** - Allows full functionality of the VideoEdge Client. Unable to view or edit the VideoEdge Administration Interface. The default password for this role is **viewer1**.
- **viewer2** - Allows full functionality of the VideoEdge Client with exception of Analog (Real) PTZ. Unable to view or edit the VideoEdge Administration Interface. The default password for this role is **viewer2**
- **viewer3** - Allows full functionality of the VideoEdge Client with exception of Analog (Real) and Digital PTZ, Still Image Capture and Clip Export. Unable to view or edit the VideoEdge Administration Interface. The default password for this role is **viewer3**.

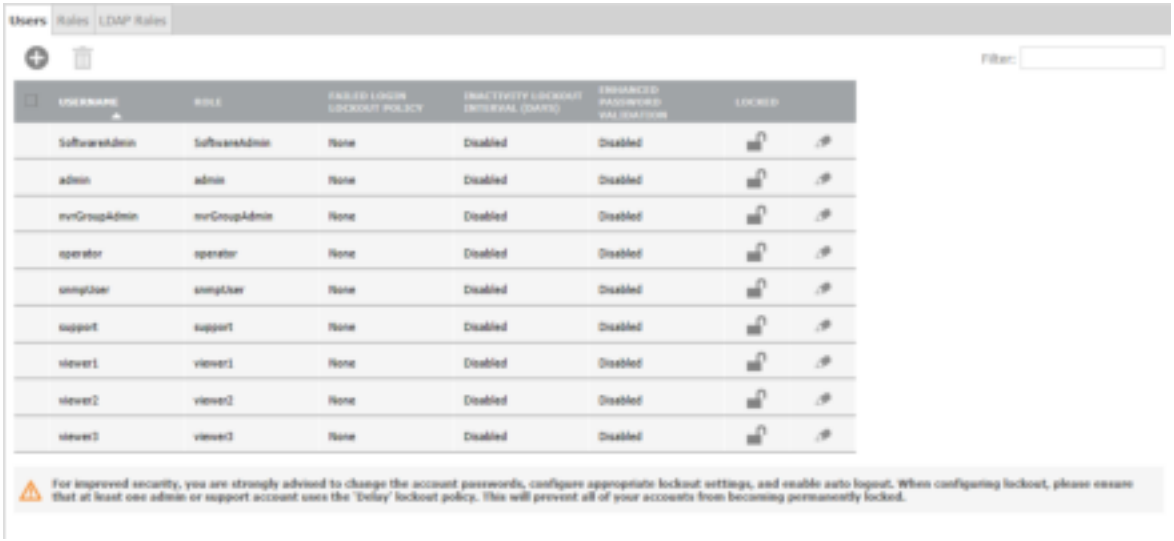
The following roles are for use with the NVR groups functionality only and cannot be assigned to created users:

- **nvrgroupadmin** - This user credential is used for communication between NVRs in a group. The default password for this role is **nvrgroupadmin**.

Note:
You cannot sign in to the VideoEdge Administrator Interface with the nvrgroupadmin credential.

- **snmpuser** - This user credential is used for SNMP communication between NVRs in a group. The default password for this role is **snmpuser**.

Figure 46 Users Page



Procedure 166
Adding a new user

Step	Action
1	Select **System** from the main menu.
2	Select **Users and Roles**. The Users page displays.
3	Click  The Add New User window opens.
4	Enter your account password in the **admin Password** or **support Password** field. **Note:** • You must have an admin or support role to create new user accounts. • You must enter your account password when you create a new user account.
5	Enter the user name in the **Username** field.
6	Enter the password in the **New Password** field.
7	Re-enter the password in the **Confirm Password** field.

Note:
When entering the user name and password note the use of upper and lower case. The user must enter their user name and password as it has been entered at this stage.

8 Select the role from the **Role** dropdown.

9 Click 

- End -

Editing a user account

Users with the admin or support role can change or reset passwords for other users.

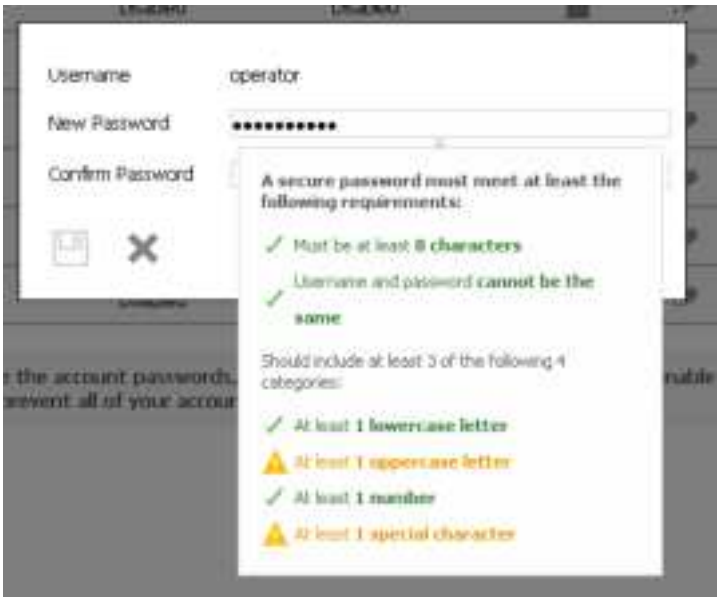
For the default admin and support accounts:

- You can change the password for any user account. To change the password of the default admin or support accounts, you must know their current password.

For custom users with the admin or support role:

- You can change the password for any user account. To change the password of the default admin or support accounts, or to change your own password, you must know the current password.

Note:
• Before you can edit a user's password, you must enter the password for your own admin-level or support-level account.
• When you edit a user password, a validation popup appears. Follow the guidelines in the validation popup to ensure that the new password meets security requirements.



Procedure 167
Editing a user account

Step	Action
1	Select **System** from the main menu.
2	Select **Users and Roles**. The Users page displays.
3	Select  beside the user account that you want to edit. The edit window opens.
4	Enter your account password in the **admin Password** or **support Password** field. **Note:** You must enter your account password before you can edit another user's account.
5	Select the **Reset Password** checkbox.
6	Enter the new password in the **New Password** field. **Note:** Follow the guidelines in the validation popup to ensure that the new password meets security requirements.
7	Confirm the new password by entering it in the **Confirm Password** field.
8	(Optional - Custom user accounts only) Select a new role from the **Role** dropdown.
9	Click 

- End -

Locked Accounts

When an account is locked, the user cannot access the VideoEdge Administration Interface (Provided this function is permitted by their configured role). The VideoEdge's Lockout Policies also apply to the VideoEdge Client and to victor unified client.

Note:
Users with admin or support credentials can manually lock other user accounts.

Should an account be locked or delayed, you will be unable to access the VideoEdge Client or access the NVR Administration Interface through victor unified client. A locked account can quickly be identified using the Users table in the Users page, locked accounts are indicated by a white padlock symbol.

Accounts can be unlocked by a user with either the admin or support role assigned to their account. Accounts can be unlocked directly from the Users table or by using the edit icon located with each table entry in the Users page.

Note:
User accounts which have been assigned the admin or support role can only be unlocked by other users with either the admin or support role assigned.

Procedure 168
Locking accounts from the Users table

Step	Action
1	Select **System** from the main menu.
2	Select **Users and Roles**. The Users page displays.
3	Select  in the user credential row that you want to lock.
4	Enter your account password in the **admin Password** or **support Password** field.
5	Slick **OK**.

- End -

Procedure 169
Unlocking accounts from the Users table

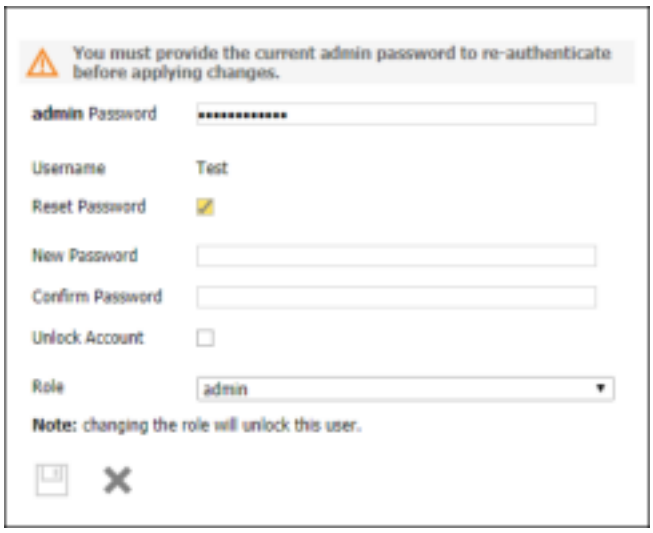
Step	Action
1	Select **System** from the main menu.
2	Select **Users and Roles**. The Users page displays.
3	Select  in the user credential row you want to unlock.
4	Enter your account password in the **admin Password** or **support Password** field.
5	Click **OK**.

- End -

Procedure 170
Unlocking accounts using the edit icon

Step	Action
1	Select **System** from the main menu.
2	Select **Users and Roles**. The Users page displays.
3	Select  in the user account row you want to unlock.
4	Enter your account password in the **admin Password** or **support Password** field.
5	(Optional for custom user accounts) Select the **Reset Password** checkbox when logged in as an admin or support user to create a new password for the locked user account.

Figure 47 Unlocking a Custom User Account



Note:
You are not required to know the current password to assign a new password or unlock the account.

6 Select the **Unlock Account** checkbox to unlock the account.

7 (Optional) Select the **Role** from the dropdown if you want to assign a new role to the account.

8 Click

- End -

Removing a User

User accounts with admin privileges can remove user accounts using the button. Only user accounts which have been created can be removed, default users cannot be removed from the NVR.

Procedure 171
Removing a User

Step	Action
1	Select **System** from the main menu.
2	Select **Users and Roles**. The Users page displays.
3	Select the checkboxes next to the users you want to remove.
4	Click A dialog box opens.
5	Enter your account password in the **admin Password** field.
6	Click **OK**.

- End -

Roles

The Roles page allows you to configure several security features for the NVR's user credentials. These include:

- **Inactivity Lockout Interval** - Credentials can be configured to lock out after a configured number of days of inactivity is reached.
- **Failed Login Lockout Policy** - There are three Lockout Polices available for use; None, Lockout and Delay. When Lockout is enabled the user will be locked out of the account should they incorrectly enter the account password consecutively a set number of times. Alternatively when Delay is enabled the user will only be unable to access their user account for a configurable period of time should they incorrectly enter the account password a set number of times.
- **Auto Logout** - Credentials can be configured to automatically log out after a configured period of inactivity.
- **Enhanced Password Validation** - If enhanced password security is required, enhanced password validation will not permit a password that fails to meet the following criteria:
    - Password must consist of a minimum of eight characters
    - Password must not be a duplicate of the previous three passwords associated with that credential
    - Password must differ by a minimum of three characters from the previously assigned password
    - Password must obey at least three of the following rules -
        - Must contain an uppercase letter
        - Must contain a lowercase letter
        - Must contain a number
        - Must contain one of the following special characters [ ] { } ( ) ^ $ # + _ - ~ ! * %
- **Password History** - You can set a password history limit, that stores the previous 'n' passwords for a Role. This feature limits users from reusing previous passwords.

Note:
By default, these security features are not configured.

Caution

It is recommended that you do not configure all the NVR's roles with lockout enabled. If the passwords for each of the accounts were to become unknown, access to the NVR Administration Interface could be lost.

Figure 48 Roles Page

Configuring additional security features on roles

Security features such as Lockout etc, are assigned to the NVR's roles, these security features then roll out to all user credentials which have been assigned that role.

Procedure 172
Configuring additional security on roles

Step	Action
1	Select **System** from the main menu.
2	Select **Users and Roles**. The Users page displays.
3	Select the **Roles** tab.
4	Select of the role you want to edit. A configuration window opens.
5	Select **Lockout** from the Lockout Policy dropdown.

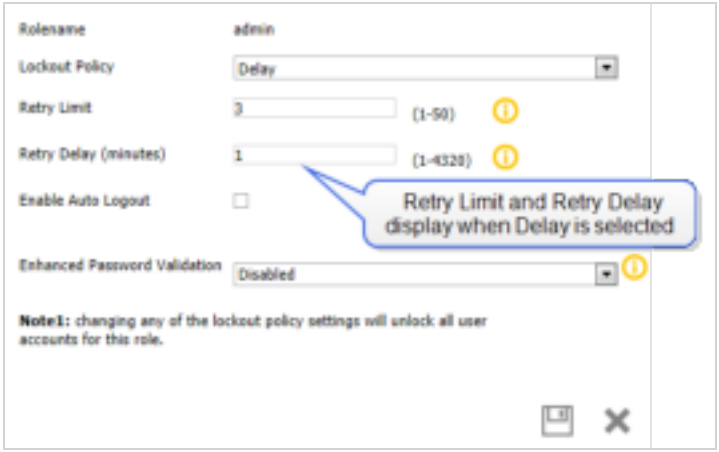
Figure 49 Lockout Selected

Enter the number of failed password attempts in the **Retry Limit** field that are required for the account to lockout. (Minimum 1, maximum 50)

Or

Select **Delay** from the Lockout Policy dropdown.

Figure 50 Delay Selected

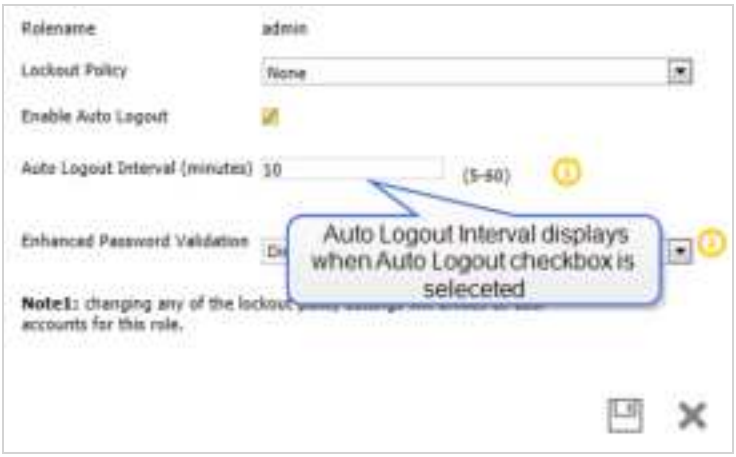


Enter the number of failed password attempts in the **Retry Limit** field that are required to initiate a delay before the user can re-attempt to enter their credentials.

Enter the number of minutes in the **Retry Delay** that are to pass before the user can re-attempt to enter their credentials. (Minimum 1, maximum 4320)

6 (Optional) Select the **Enable Auto Logout** checkbox.

Figure 51 Auto Logout Selected



(Optional) Enter the **Auto Logout Interval (minutes)** in the field. (Minimum 5, maximum 60)

7 (Optional) Configure Enhanced Password Validation settings:

a Select **Enabled** from the **Enhanced Password Validation** dropdown.

b Enter the **Remembered Passwords** field. (Minimum 3, Maximum 10)

8 Click

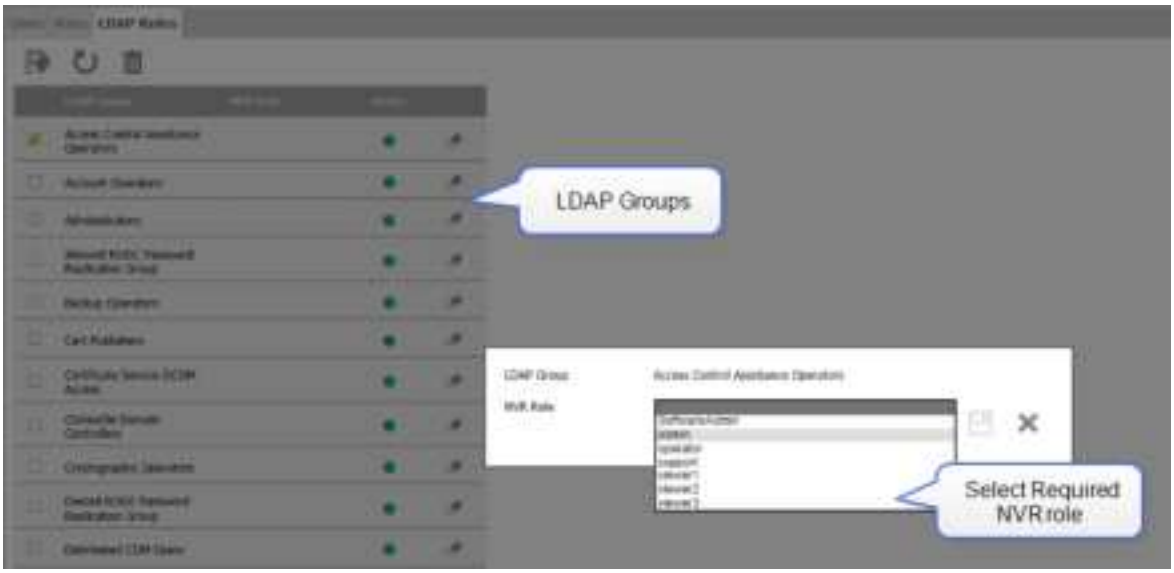
- End -

LDAP Roles

Once an LDAP server has been configured on VideoEdge, you can link LDAP Groups to VideoEdge Roles. This means that all users in the LDAP Group will be assigned the linked role on VideoEdge.

Procedure 173
Assigning LDAP Roles

Step	Action
1	Select **System** from the main menu.
2	Select **Users and Roles**. The Users page displays.
3	Select the **LDAP Roles** tab.
4	Select to retrieve all LDAP Groups.
5	Enter the **LDAP server password** in the field. All LDAP groups in the directory will be displayed.
6	Select the checkboxes of the LDAP groups you want to assign an NVR role.
7	Click A configuration window opens.



8 Select the required NVR role from the dropdown.

9 Click 

Note:
You can also batch edit NVR LDAP Roles.

- End -

Licensing

Overview

The following topic details how to apply for a license from American Dynamics. There are three types of license available for VideoEdge.

- Temporary - This is the 60 day trial license that is supplied with VideoEdge.
- Local - The local license for a single VideoEdge.
- victor Centralized - A Centralized license is a victor license that contains both victor and VideoEdge features. victor Centralized licenses are not stored on the VideoEdge - they are stored on a victor Application Server. To access the Centralized license features, you must configure your VideoEdge to connect to the victor Application Server.

Licensing is based on the number of IP connected cameras used by the VideoEdge. You can use the temporary license supplied to configure your VideoEdge, add cameras and configure motion detection before you apply for a license. The VideoEdge Hybrid recorders come standard with a software license that supports all analog video inputs.

An IP camera uses one license. An encoder with a single IP address can support multiple channels using a single license. There are two types of encoders. One type of encoder contains a single IP address. The other type of encoder contains multiple IP addresses.

- Single IP address encoder/device - If the encoder/device has a single IP address, then it will only consume 1 x IP license (the encoder/device will use up "N" channels of the recorder (where N is the number of channels added to the VideoEdge).
- Multiple IP addresses - Some encoders have multiple IP addresses and for these devices an IP license will be required for each channel.

Note:
• Depending on the VideoEdge model that you purchase, the maximum number of channels and camera licenses can vary.
• When the trial period expires, the camera and storage functions disable automatically. You must purchase a Local or victor Centralized license to allow permanent recording.

Table 15 Maximum Camera Count

Model	Maximum number of channels	Maximum number of analog cameras
32 Channel IP only Desktop	32	0
16 Channel Hybrid Desktop	16	0 - 8
32 Channel Hybrid 2U Rack Mount (Raid and Non-Raid)	32	0 - 16
64 Channel Hybrid 3U Rack Mount (Raid and Non-Raid)	64	0 - 32

You can combine both single IP cameras and multiple analog cameras that are attached with an encoder. For example, you can use up to 16 channels on a VideoEdge Desktop Hybrid. Of these channels, you can connect 16 IP cameras or you can connect a mix of analog and IP cameras. If you connect a fully populated 8 channel IP encoder, and 8 single IP cameras, this is counted as a total of 16 channels.

To apply a license, use the Licensing page in the VideoEdge Administration interface. From here you can Generate a Host ID, Apply a Local License, Enable Centralized Licensing, edit the Software Service Agreement (SSA) message, add/edit SSA Contacts and add/edit the SMTP Server.

The Licensing Status section provides the following information:

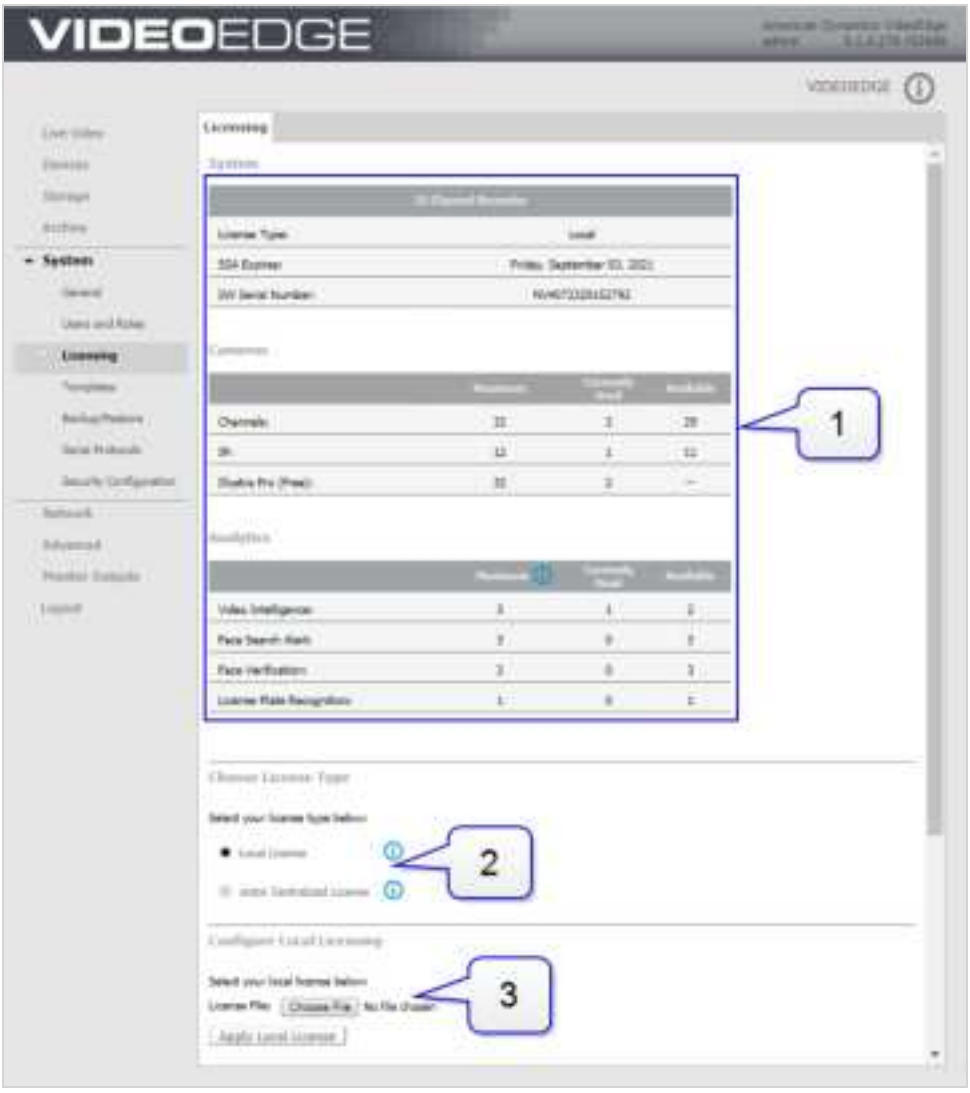
Field	Description
Channels	The total number of channels that the VideoEdge can support. IP cameras use one IP license and one channel. Analog cameras do not use a license, but they use a channel. Encoders use a single license, but can use multiple channels.
Analog Devices	The total number of analog devices that the VideoEdge can support. Analog devices do not require a license.
IP Licenses	The total number of IP licensed cameras available for your VideoEdge. An IP camera uses one license while an encoder/device with a single IP address can support multiple channels with a single license. An encoder with multiple IP addresses will require more than a single license.
Complementary Illustra Pro	The total number of Illustra Pro cameras that are available for your VideoEdge. From 5.1 onwards, VideoEdges that you purchase from American Dynamics can add Illustra Pro cameras without consuming a license. For this to happen the VideoEdges must be using either a 5.1 (or later) license or using Centralized Licensing. These cameras will contribute to the maximum number of cameras that your VideoEdge can support. Also, to enable analytics on your Illustra Pro camera, you must purchase an analytic license.
Analytic Devices, Face Verification Devices and Face Search Alert Devices	For each of these camera analytics, the Licensing Status section displays the number of analytic licenses that are available. If you use Centralized licensing, the **Maximum** column displays the recommended number of each analytic that the VideoEdge can process. If you use Local licensing, the **Maximum** column displays the number of each analytic that you have on your VideoEdge license.
SSA Expires	The expiry date for your Software Service Agreement.
License Type	The type of license for the VideoEdge: Temporary, Local or victor Centralized.
SW Serial Number	The software serial number for your VideoEdge.

A license is generated based on the number of devices attached to the VideoEdge. This can be either a camera or a camera encoder with multiple analog cameras attached. A license generated for one VideoEdge cannot be used with another VideoEdge, however, you can replace cameras and devices on the VideoEdge without requiring a license change.

The VideoEdge has optional licensable features consisting of:

- Analytics channels
- Face Search Alert Devices
- Face Verification Devices
- License Plate Recognition Devices

Figure 52 Licensing page



Key	Description
1	Current license information.
2	Choose license type - victor Centralized or Local.
3	Configure licensing. If you select Local licensing, you must select the new license file. If you select victor Centralized licensing, you must configure the victor Application Server that stores the Centralized license.

Licensing the VideoEdge (Local License)

To apply a Local license the VideoEdge you must generate a Host ID specific to your VideoEdge and enter the ID on the online registration page. You can access the online registration page from the American Dynamics website or using the VideoEdge Licensing Activation Icon on the VideoEdge Desktop. After you receive the license file you can then apply the Local license to your VideoEdge.

Generating a Host ID

When it is time to renew your Local VideoEdge License or upgrade your software the Generate Host ID tool is used to generate a Host ID specific to your VideoEdge device which should be entered on the VideoEdge registration page on the American Dynamics website. The website can be accessed via the VideoEdge Licensing Activation Icon on the VideoEdge Desktop or by going to the following address:

http://americandynamics.net/support/registerdirect.aspx

Note:
• Before you generate the VideoEdge Host ID, you must ensure that all Network Interface Cards (NICs) intended to be used with the VideoEdge, for example, a Client LAN, Camera LANs or a Storage LANs, are already installed on the server.
• For VideoEdges that you assign as Secondary NVRs, do not generate a host ID while the Secondary NVR is in Failover mode.

Procedure 174
Generating a Host ID

Step	Action
1	Select **System** from the main menu.
2	Select **Licensing**.
	The Licensing page opens.
3	Click **Generate Host ID** in the Upgrades section.
	A file download window opens.
4	Click **Open** to view the Host ID. Alternatively you can click **Save** to select the location where you want to save the Host ID.

- End -

Applying a software license

When you receive your software license from the American Dynamics website, you can apply your Local license.

Procedure 175
Applying a Local License

Step	Action
1	Select **System**.
2	Select **Licensing**.
	The Licensing page opens.
	In the **Choose License Type** section, select **Local License**.
3	In the **Configure Local Licensing** section, click **Browse**.
4	Locate the license file and click **Open**.
	The file path is displayed in the **License File** field.
5	Click **Apply Local License**.

- End -

Licensing the VideoEdge (victor Centralized License)

From VideoEdge version 4.9 onwards, you can choose a victor Centralized Licensing solution. Centralized licenses are victor licenses that include VideoEdge license information. Centralized licenses are stored centrally on a victor Application Server. When you purchase a victor Centralized license, you can also purchase VideoEdge components as part of that license. Alternatively, you can transfer the contents of an existing VideoEdge license into a victor Centralized license.

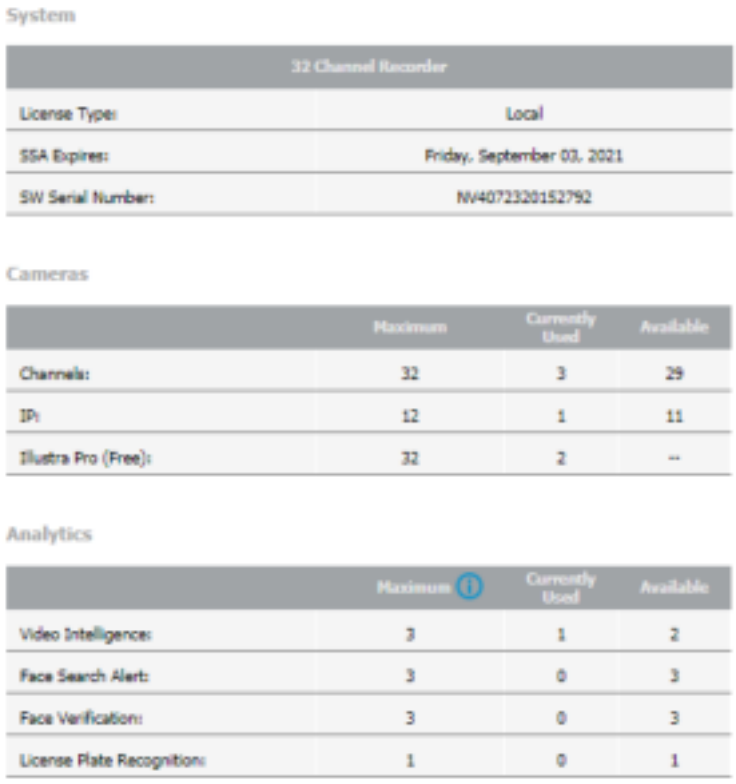
To access licenses for objects such as cameras, analytics, facial recognition and facial verification devices, you must configure VideoEdge to connect to the victor Application Server. Unlike Local licensing, Centralized camera, analytic, facial verification and facial recognition licenses are not linked to a specific VideoEdge. Any VideoEdge connected to the same victor Application Server can request from the same pool of licenses, but only one VideoEdge can use each license at one time. During startup, the VideoEdge requests licenses from the licensing server. These licenses become available after the VideoEdge is shut down.

You can view VideoEdge licensing information from three locations:

- On the VideoEdge unit: The Licensing page of the VideoEdge Administration Interface.
- On the victor Application Server: From the VideoEdge tab of the License Manager.
- On victor Client: From the License tab.

Note:
You must install the victor Application Server that is used for Centralized License management on a 64-bit OS.

Figure 53 License status - VideoEdge Admin GUI



Centrally-licensed VideoEdges do not have a maximum number of analytic, face search or face verification licenses; instead, they have a maximum recommended number of licenses.

Note:
For optimum performance, do not exceed the maximum recommended number of camera, analytic, face search, or face verification licenses.

Prerequisites for victor Centralized Licensing

- You must install the victor Application Server that is used for Centralized License management on a 64-bit OS.
- The VideoEdge and the victor Application Server must be updated to version 4.9 or higher.
- Confirm that routing and firewalls are configured correctly to allow the VideoEdge to access the victor Application Server on port 27000 - 27010.
- The Centralized license server must have enough available licenses to accommodate the VideoEdge items being transferred. For example, to register a VideoEdge with 20 cameras and 10 analytics, there must be at least 20 camera licenses and 10 analytic licenses available on the victor Application Server.
- (Optional) Enable SMTP and email alerts on the VideoEdge.

Transferring a VideoEdge License

Use the American Dynamics website to transfer a VideoEdge license to a victor Centralized license. The VideoEdge license contents are transferred to the victor license, and the VideoEdge license is invalidated. A VideoEdge license can be transferred to a victor Centralized license in one of two ways:

- Manual: Transfer the VideoEdge license to a victor Centralized license from the American Dynamics website. VideoEdge license information must be entered manually during this process.
- Automatic: Use the License Manager Application to transfer VideoEdge license information into a victor System Information file. This file is used in the victor Centralized license application process on the American Dynamics website. The License Manager Application is included in a victor Application Server installation. The Automatic process is suitable for transferring multiple VideoEdge licenses to victor Centralized licenses simultaneously.

Note:
• To transfer a VideoEdge license to a victor Centralized license, the victor license must include the Centralized Licensing feature.
• (Optional) To receive notifications for license misconfiguration or communications issues between the VideoEdge and the victor Application Server, enable Email Alerts.
• VideoEdge Failover units configured with a secondary Failover role are not compatible with victor Centralized Licensing.
• When a VideoEdge device is transferred to a victor Centralized license, the original VideoEdge license is no longer valid.

License Manager Application

You can manage victor Centralized Licensing through the License Manager application. The License Manager is installed on a system as part of a victor Application Server installation. This application is used to generate a System Information file, apply product licenses and to display license status. The license status of the VideoEdge recorders is displayed on a per recorder, per license type basis. Ensure that each of the VideoEdge devices have a unique name in order to see which device is using which licenses on the license server.

To register you require the following:

- An Internet connection.
- A valid email account.

- A valid login for either the Software House or American Dynamics website.
- A valid Software Service Agreement.
- The System Information file.

Note:
• The System Information file must be generated on the computer for which the license is intended. The XML file contains information specific to the machine on which it was generated. Therefore the license created is exclusive to that computer and will not work on any other.
• It may take one business day to receive your license.

Transferring a VideoEdge License (Automatic)

Use the License Manager application to include VideoEdge unit information into a victor Centralized license application.

Note:
• For this procedure, use the License Manager that is installed on the victor Application Server.
• After a VideoEdge license is transferred to a victor Centralized license, the VideoEdge license is no longer usable. VideoEdge license information is zeroed out on the American Dynamics database, and the individual licenses for cameras and analytics are transferred to the victor license.

Prerequisites

Before you transfer a VideoEdge license, the VideoEdge device must meet the following criteria:

- The VideoEdge must be upgraded to version 4.9 or higher.
- The VideoEdge must be added to victor.
- The VideoEdge must not be configured with a secondary Failover role.

Procedure 176
Transferring a VideoEdge License (Automatic)

Step	Action
1	Double-click the **Licensing** icon on the desktop. The License Manager displays.
2	Select **Generate**. A popup asks you to confirm VideoEdge transfer to a victor Centralized license.
3	Review the list of recorders to be transferred.
4	Click **Yes** to generate the system information XML file. **Note:** The system information file is used in the victor license application process and it also contains a list of the VideoEdge licenses to be transferred.
5	Select a destination to save the XML file and select **Save**.
6	Apply for a victor license at http://americandynamics.net
	- End -

Apply a victor Centralized License

After you receive your software license from the American Dynamics website, you can apply your victor Centralized license to the victor Application Server.

Note:
• For this procedure, use the License Manager that is installed on the victor Application Server.
• Use the License Manager to view the current license information, selecting the VideoEdge tab. From this tab you can view the number of camera, analytic, facial recognition and facial verification licenses available from the victor Application Server.
• If you encounter any problems, see the licensing instructions PDF that is included with the license e-mail.

Procedure 177
Apply a victor Centralized license

Step	Action
1	Save the license file (.LIC) to a local directory.
2	Double-click the **Licensing** icon on the desktop. The License Manager displays.
3	Select **Add New License**. The Open screen displays.
4	Browse to the .LIC license file and select **Open**.
5	Select **Yes** to confirm the License update and service restart.

Note:
1. Use the License Manager to view the current license information, selecting the VideoEdge tab. From this tab you can view the number of camera, analytic, facial recognition and facial verification licenses available from the victor Application Server.
2. If you encounter any problems, see the licensing instructions PDF that is included with the license e-mail.

- End -

Configure the VideoEdge for victor Centralized Licensing

After the victor Centralized license is applied to the victor Application server, the VideoEdge must be configured to use this server as the Centralized license server. You can manually activate victor Centralized Licensing on a VideoEdge by VideoEdge basis, or you can automatically transfer all eligible VideoEdge units on a system to victor Centralized Licensing using the License Manager application.

Procedure 178
Manually Activate victor Centralized Licensing

Note:
For this procedure, use the VideoEdge Administration Interface.

Step	Action
1	Select **System**.
2	Select **Licensing**. The Licensing page opens. In the **Choose License Type** section, select **victor Centralized License**.
3	Configure the Centralized license server. a Enter the **victor Application Server** address. **Note:** The IP address of the victor Application Server must be entered. Domain name is not supported. b Enter the **Port Number**. c (Optional) Enter **Email recipients**. **Note:** • Email recipients receive email notification of any license misconfiguration or communications loss with the victor Application Server. • To enable alert notifications, you must configure email alert settings for the VideoEdge. For more information, see Email Alerts. d 
4	Click **Activate Centralized Licensing**.

- End -

Procedure 179 Automatically Activate victor Centralized Licensing

Note:
For this procedure, use the License Manager that is installed on the victor Application Server.

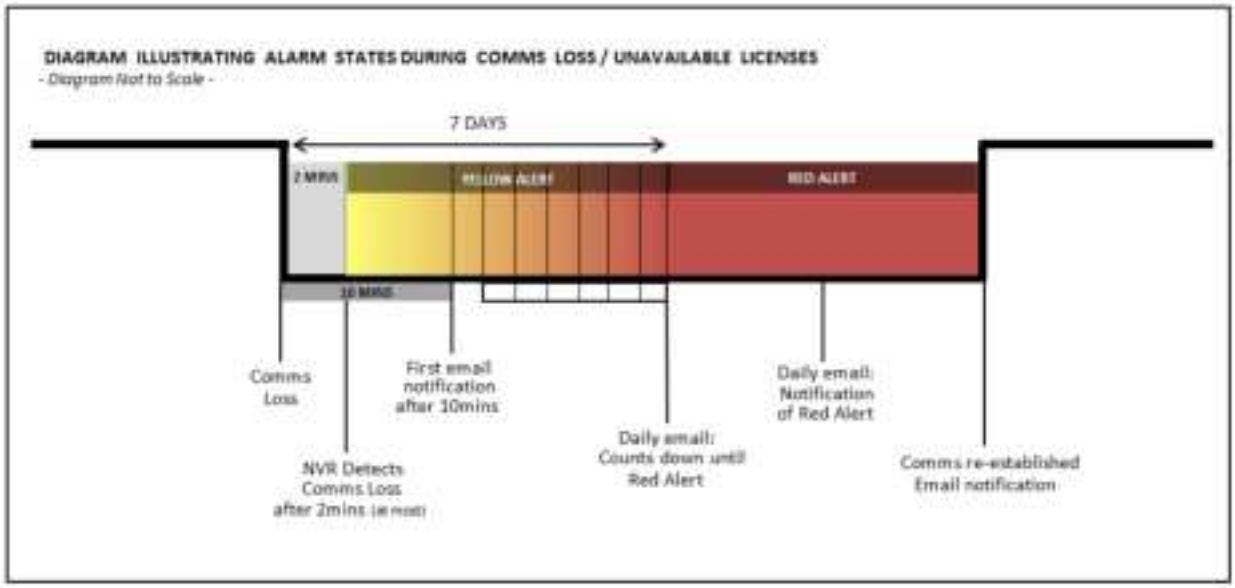
Step	Action
1	Select the VideoEdge tab in the License Manager.
2	Select **Centralize Licenses**. The VideoEdge Centralized License Transfer dialog opens.
3	Review the information to ensure that all required VideoEdge units will be transferred.
4	Confirm IP address and port number for the license server.
5	Enter an email recipient address. **Note:** • Email recipients receive email notification of any license misconfiguration or communications loss with the victor Application Server. • To enable alert notifications, you must configure email alert settings for the VideoEdge. For more information, see Email Alerts.
6	Select **Yes, Transfer**. A summary of the transferred recorders appears.

7 Select **OK**.

- End -

Centralized Licensing - Alerts

If communication is lost between the VideoEdge and the victor Application Server, the VideoEdge enters Amber Alert mode. Any authorized Email Alert recipients will receive a notification about the VideoEdge status change. After being in Amber Alert mode for 7 days, the recorder enters Red Alert mode. Any authorized Email Alert recipients will receive daily email notifications about the VideoEdge device status. After communication with the victor Application Server is restored, the Red or Amber alert will end.



Note:
Email Alerts must be configured before any Amber and Red alert email notifications can be sent.

VideoEdge license status can be viewed in victor Unified Client. VideoEdge units can be monitored from the Licensing menu, from the Health Dashboard and in Reports. For more information about victor unified client, see the *victor unified client and victor Application Server Administration/Configuration Guide*.

Software Service Agreement Notifications

The Software Service Agreement (SSA) section allows you to configure a message to alert you when the Local license is close to expiry. You can add/edit contact email addresses to receive the SSA expiry message and edit the SMTP Server. You can also send a test email message to confirm the settings entered are correct.

Note:
To be able to use SSA notifications you must ensure that your VideoEdge is configured with a valid Domain Name and Default Gateway.

Edit the SSA Message

You can edit the SSA message that is sent to you when the VideoEdge license is close to expiry.

Procedure 180
Edit the SSA Message

Step	Action
1	Select **System** from the main menu.
2	Select **Licensing**. The Licensing page opens.
3	In the **Software Service Agreement** section, click **Change Message**. The SSA Expire Message editing window opens.
4	To edit the message subject, enter the desired text in the **Subject** field.
5	To edit the message body, enter the desired text in the **Message** field.
6	(Optional) Click **Restore Default** to revert to the default SSA Expire Message.
7	Click 

- End -

Edit SSA Contacts

The SSA contacts, are those who will receive the SSA message to alert them when the VideoEdge license is about to expire. To receive the message you must add at least one contact's email address to the contacts list. You can add and remove contacts to/from the contact list when required.

Procedure 181
Edit SSA Contacts

Step	Action
1	Select **System** from the main menu.
2	Select **Licensing**. The Licensing page opens.
3	In the **Software Service Agreement** section, click **Edit Contacts**. The SSA Contacts editing window opens.
4	To add a contact, enter their email address in the **Add Email** field.
5	Click  The email address is added to the contacts list.
6	(Optional) To add additional contacts to the contacts list repeat Steps 4 and 5.
7	To remove an email address from the contact list, click **Remove** next to the Email address to be removed. The contact's email address is no longer in the contacts list.
8	Click  to exit.

- End -

Set the SMTP Server Address

You can set your email SMTP server from the Email Alerts page. You can access Email Alerts from the **Advanced** menu, or you can select the **Email Alerts** button from the licensing page. For more information about configuring an outbound mail server, see Email Alerts.

Send an SSA Test Message

When you have configured the SSA settings, you can send a test message to the contacts on the SSA contacts list.

Procedure 182
Sending an SSA Test Message

Step	Action
1	Select **System** from the main menu.
2	Select **Licensing**. The Licensing page opens.
3	Click **Send Test Message** in the Software Service Agreement section. A test message is sent to the mailbox of those on the contacts list.
4	A message opens to confirm if the email has been sent or if it has failed. Click **OK**.
	Note: If the message has failed to send check your contact's email addresses and the SMTP server address to confirm they are correct, and re-send.

- End -

SSAs and victor Centralized Licensing

VideoEdge devices using victor Centralized Licensing use the victor SSA shown in the victor Application Server. This SSA expiry date can be viewed from the VideoEdge Administration Interface or from the Unified tab of the victor Application Server License Manager.

Templates

With the NVR, you can save a server's configuration data to a template. You can import the template to another NVR and the configuration settings of the NVR will be configured according to the settings on the imported template. You can store a template file on a USB or local disk.

Figure 54 Save Template Page

Save a Configuration Template

You can create a configuration template using the Templates functionality in the NVR interface. You can choose the type of configuration settings to be stored in the template. If you want to save camera configuration settings to a template you must ensure that those cameras are connected to the NVR before the template is created.

Procedure 183
Creating a Configuration Template

Step	Action
1	Select **System** from the main menu.
2	Select **Templates**. The Save Template page opens.
3	Select the required checkboxes for the configuration settings that you want saved to the template: a All b Device Settings c Storage Settings

d User Information

e Network Settings

f Email Settings

g Failover Settings

h Discovery Settings

i Security Settings

4 Click **Save Template**.

5 Select **Save As**.

6 Navigate to the folder where you want to save the template.

7 Enter a **Filename** for the template and click  .

Note:
A default template file name is given; this is made up of VideoEdgeNVRTemplate, followed by the NVR name and the date and time the template was created.
Example:
VideoEdgeNVRTemplate-ServerName-YYYY-MM-DDT00_00.xml
VideoEdgeNVRTemplate-linux-adnvr-2012-03-26T14_02.xml

- End -

Import a Template File

You can import NVR configuration settings saved as a template. When you are configuring a NVR for the first time, you can load a saved template file, which will configure the NVR with the settings in the file. When applying a template file to an NVR that is already configured, the settings on the NVR will update with the settings saved in the template file. If there are camera configuration settings in the template to be imported, the relevant cameras must be connected to the NVR.

Note:
For template files which include security settings you will be required to activate these settings when prompted to enable them on the NVR.

Procedure 184
Importing a Template File

Step	Action
1	Select **System** from the main menu.
2	Select **Templates**. The Save Template page opens.
3	Select the **Load Template** tab.
4	Click **Browse**.
5	Navigate to the template file you want to import.
6	Select the file and click **Open**. The file path of the template file appears in the **Template File** field.

7 Click **Apply Template**.

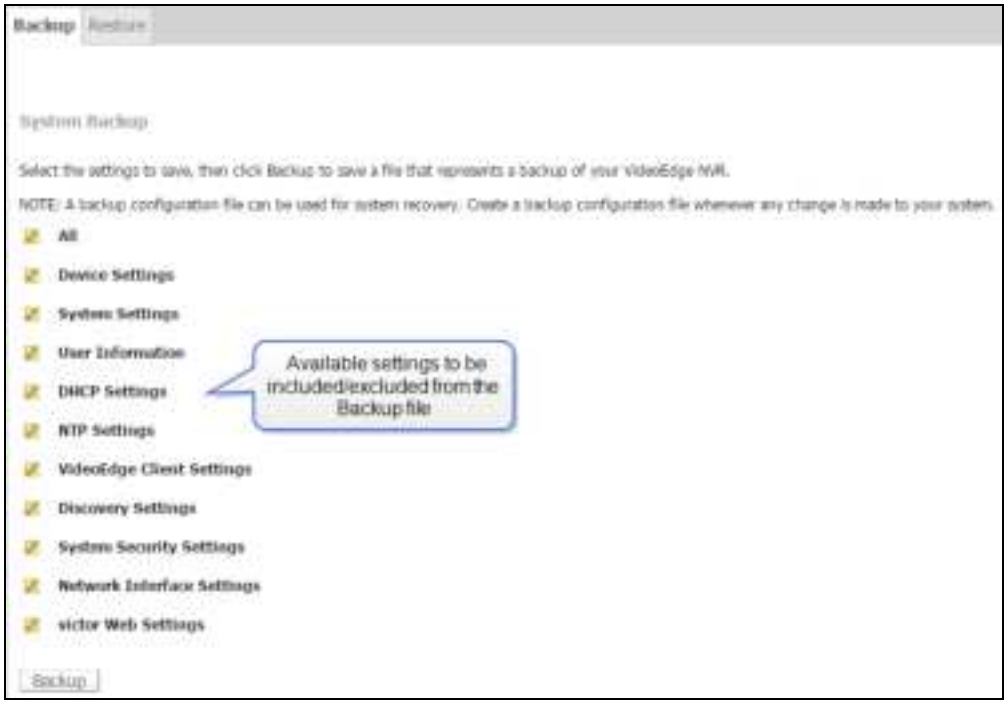
Note:
If any errors occur during the template import process, a summary of the errors are displayed.

- End -

Backup\Restore

With the NVR, you can recover a server's configuration data in the event of a system failure. A system backup file can be stored to a USB or local disk. The backup files can then be imported to the NVR where the saved configuration can be restored.

Figure 55 Backup Page



Create a Backup File

You can create a backup file using the Backup/Restore functionality in the NVR Administration Interface. You can choose the type of configuration settings to be stored in the backup file.

Note:
Operating System settings cannot be stored in the configuration backup file. However, the system will also automatically export a text file containing the OS settings which can be used as reference for manually configuring the OS settings.

Procedure 185
Creating a Backup File

Step	Action
1	Select **System** from the main menu.
2	Select **Backup/Restore**. The Backup page opens.
3	Select the required checkboxes for the configuration settings that you want saved to the template in the Templates section: • All

- Device Settings
- System Settings
- User Information
- DHCP Settings
- NTP Settings
- Failover Settings
- VideoEdge Client Settings
- Discovery Settings
- System Security Settings
- Network Interface Settings
- victor Web Settings

4 Click **Backup**.

5 Select **Save As**.

6 Navigate to the folder where you want to save the backup file.

Note:
To use the backup file during a system recovery procedure you must save the file to an external location, for example, a USB drive.

7 Enter a **File name** for the backup file and click  .

Note:
A default backup file name is given; this is made up of VideoConfBackup, followed by the NVR name and the date and time the file was created.
Example:
VideoConfBackup-ServerName- yYYYY-mMM-dDD-h00-m00-s00_files.zip
VideoConfBackup-ServerName- y2012-m03-d26-h14-m02-s43_files.zip

- End -

Restore an NVR

System backup files contain NVR configuration information. The type of information contained in a particular file is dependent on the settings selected when the file was being created. When the backup file is applied, the NVR is restored as per the saved configurations.

Note:
• Only a licensed server can be restored.
• You cannot restore from a previously saved VideoEdge NVR 4.1 backup configuration file.

Caution
To maintain all configured Tours and Salvos relating to your NVR in victor unified client, you should complete the System Restore procedure before reconfiguring the NVR's LAN Interface Settings.

Procedure 186
Restoring an NVR from a Backup File

Step	Action
1	Select **System** from the main menu.
2	Select **Backup/Restore**.
	The Backup page opens.
3	Select the **Restore** tab.
4	Click **Browse**.
5	Navigate to the backup file you want to use, select the file and click **Open**.
6	Click **Upload Backup**.
	A message box opens, asking you if you want to recover any media that is part of storage being restored.
7	Click **Yes** if you want to recover media, otherwise click **No**.
8	A recovery progression bar opens and updates as the recovery progresses.
	If you are recovering media this may take some time.
9	A message box opens informing you that the recovery is complete.
10	Click **OK**.
	Note: If you are restoring DHCP and/or NTP settings you need to restart your DHCP and/or NTP server.

- End -

Update Software

Software updates, patches and update camera handler packs can be applied to the NVR manually or using the Push Update feature of victor unified client.

Note:
To carry out a manual software update you must log in to the VideoEdge Administration Interface with the **softwareadmin** user credential.

Push Updates

Software updates can be initiated by victor unified client using the Push Updates feature. The user will be required to have the appropriate permissions to carry out a Push Update. For further information refer to the victor unified client User Guide.

Applying Software Updates using the Administration Interface

You can apply software updates or patches to the NVR, or to victor Web LT, using the softwareadmin user credential. The current version of the installed software is displayed. To update the software you must upload a new software package and then install the update.

Caution
NVR Services are stopped during a software update; this results in a pause in recording until the operation is completed and the system reboots. You will be prompted to reboot the VideoEdge when the update completes.

Upgrading to VideoEdge 4.9.0

You cannot upgrade to VideoEdge 4.9.0 through the VideoEdge Administration Interface, or through a Push Update. You must use the VideoEdge Updater to upload and install VideoEdge 4.9 updates. For more information about the VideoEdge Updater, see the *VideoEdge Updater User Guide*.

After you upgrade to VideoEdge 4.9.0, you can upgrade through the VideoEdge Updater, through the VideoEdge Administration Interface or through a Push Update.

VideoEdge Upgrade path

The following image illustrates the VideoEdge upgrade path.

- For all VideoEdge versions except 4.9.0, you can upgrade the VideoEdge through a Push Update, or you can upgrade manually, through the Administration Interface.
- For VideoEdge versions earlier than 4.4.4.122, you must upgrade the VideoEdge to version 4.4.4.122 before you can upgrade further.
- To upgrade to VideoEdge 4.9.0, you must use the VideoEdge Updater.
- To upgrade to VideoEdge 4.9.1+, you must upgrade from VideoEdge 4.9.0.496 or greater.

Figure 56 Upgrading to VideoEdge v4.4.4.122

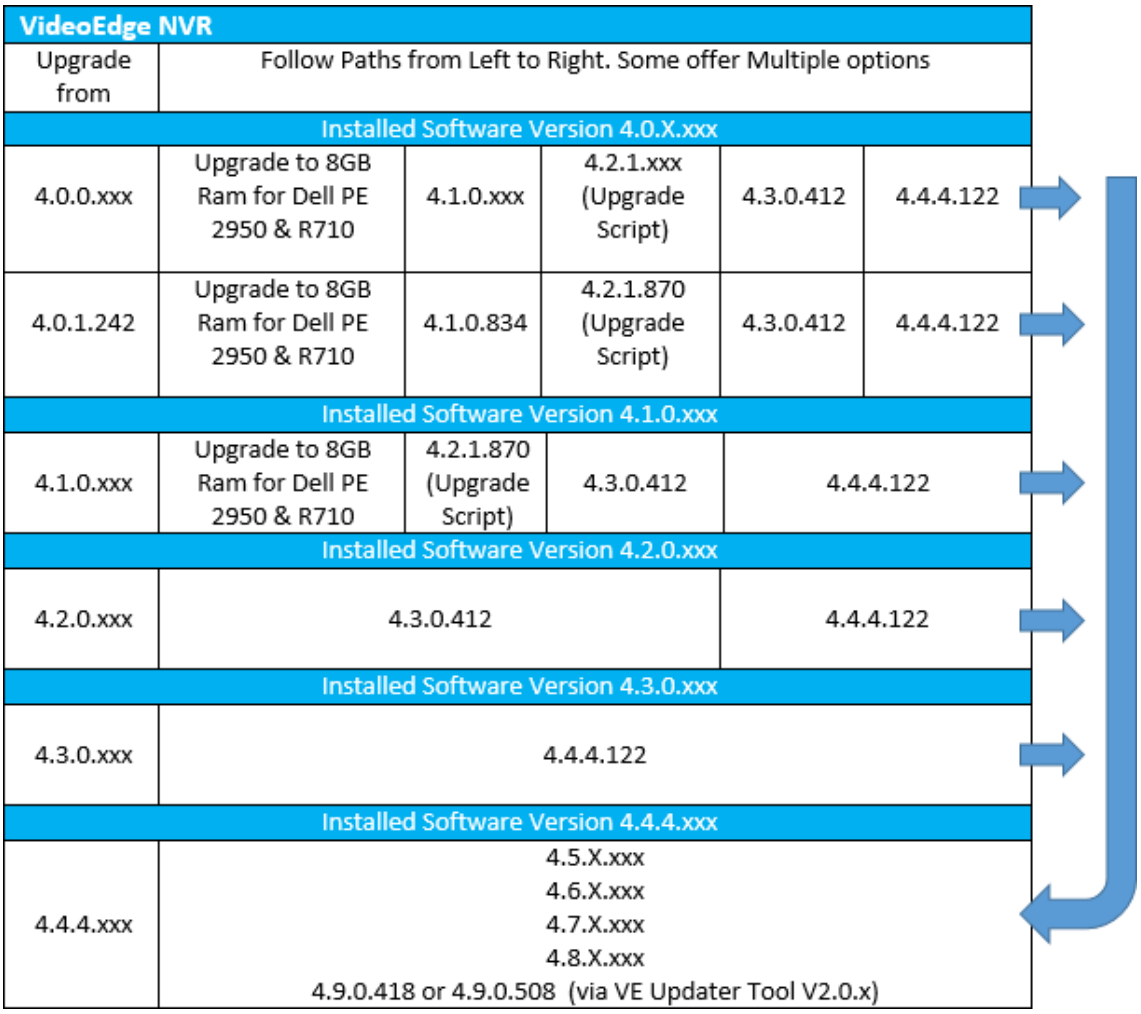


Figure 57 Upgrading from VideoEdge 4.4.4.122

VideoEdge NVR	
Upgrade from	Follow Paths from Left to Right. Some offer Multiple options
Installed Software Version 4.4.4.xxx	
4.4.4.xxx	4.5.X.xxx 4.6.X.xxx 4.7.X.xxx 4.8.X.xxx 4.9.0.418 or 4.9.0.508 (via VE Updater Tool V2.0.x)
Installed Software Version 4.5.X.xxx	
4.5.X.xxx	4.6.X.xxx 4.7.X.xxx 4.8.X.xxx 4.9.0.418 or 4.9.0.508 (via VE Updater Tool V2.0.x)
Installed Software Version 4.6.0.xxx	
4.6.0.xxx	4.7.X.xxx 4.8.X.xxx 4.9.0.418 or 4.9.0.508 (via VE Updater Tool V2.0.x)
Installed Software Version 4.7.X.xxx	
4.7.X.xxx	4.8.X.xxx 4.9.0.418 or 4.9.0.508 (via VE Updater Tool V2.0.x)
Installed Software Version 4.8.X.xxx	
4.8.X.xxx	4.9.0.418 or 4.9.0.508 (via VE Updater Tool V2.0.x)
Installed Software Version 4.9.0.xxx	
4.9.0.418	4.9.0.496 or 4.9.0.508
4.9.0.496	4.9.0.508 or 4.9.1.374 or 5.0.0.862 or 5.1.0.380 or 5.2.0.272 or 5.2.1.80 or 5.2.2.24
4.9.0.508	or 4.9.1.374 or 5.0.0.862 or 5.1.0.380 or 5.2.0.272 or 5.2.1.80 or 5.2.2.24
4.9.0.602	4.9.1.374 or 5.0.0.862 or 5.1.0.380 or 5.2.0.272 or 5.2.1.80 or 5.2.2.24
Installed Software Version 4.9.1.xxx	
4.9.1.374	5.0.0.862 or 5.1.0.0.380 or 5.2.0.272 or 5.2.1.80 or 5.2.2.24
Installed Software Version 4.9.2.100 (1U NVR Only)	
4.9.2.100	5.0.0.862 or 5.1.0.380 or 5.2.0.272 or 5.2.1.80 or 5.2.2.24
Installed Software Version 5.0.0.xxx	
5.0.0.862	5.1.0.380 or 5.2.0.272 or 5.2.1.80 or 5.2.2.24
Installed Software Version 5.1.0.xxx	
5.1.0.380	5.2.0.272 or 5.2.1.80 or 5.2.2.24
Installed Software Version 5.2.0.272	
5.2.0.272	5.2.1.80 or 5.2.2.24
Installed Software Version 5.2.1.80	
5.2.1.80	5.2.2.24

Procedure 187
Updating the VideoEdge

Step	Action
1	Log in using the SoftwareAdmin user credential: a Enter **softwareadmin** in the username field. b Enter your password. **Note:** The default password for the softwareadmin user credential is **softwareadmin** The Update Software page opens.
2	Click **Browse**.
3	Select the update or patch file and click **Open**. The name and file path of the patch file appears in the Upload New Package field.
4	Click **Upload**. The uploaded package is displayed in the Uploaded Packages list.
5	Select the new package from the list and click **Install**. **Note:** The software upgrade process will interrupt recording and the recorder will automatically reboot, as necessary.
6	Once the NVR has been rebooted, select the uploaded package and click **Delete**.
7	Select **Logout**. A dialog box opens asking 'Are you sure you want to logout?'.
8	Click **OK**.

- End -

Incremental Updates

This feature is not for use in VideoEdge 5.1 or earlier, but will be used in future VideoEdge versions.

Updating Camera Handler Packs

Existing camera handlers can be updated or new camera handler packs installed on the NVR, without the need to reload or reboot. Camera handlers can be installed using the softwareadmin user credential. The current camera pack version is displayed when the Update Software page opens.

Caution

Recording and dry contact processing will be stopped for any camera using a handler that is being updated.

Procedure 188
Updating a Camera Handler Pack

Step	Action
1	Log in using the softwareadmin user credential: a Enter **softwareadmin** in the username field. b Enter your password. **Note:** The default password for the SoftwareAdmin user credential is **softwareadmin**. The Update Software page opens.
2	Click **Browse**.
3	Select the camera handler pack and click **Open**. The name and file path of the pack appears in the Upload New Package field.
4	Click **Upload**. The uploaded package is displayed in the Uploaded Packages list.
5	Select the new package from the list and click **Install**.
6	Select **Logout**. A dialog box opens asking 'Are you sure you want to logout?'.
7	Click **OK**.

- End -

Failover Considerations

When a software update is applied either via a push update or applied manually using the Administration Interface, NVR services will restart. Temporary NVR service outage should therefore be expected when an update is applied.

It is recommended that you should schedule when NVR upgrades are applied and expect a loss of video when services restart. When upgrading NVRs which are being monitored by a secondary (Failover) NVR you need to stop Server Monitoring to prevent the secondary NVR taking over when the upgraded primary NVR's services stop.

Failover in VideoEdge 4.4 - 4.7.1

In VideoEdge version 4.4, you must configure Failover by IP address. In version 4.8+, you can configure Failover by IP address or by fully qualified domain names. For detailed information on the software upgrade process for the VideoEdge NVR, see the **VideoEdge v4.4 Installation and User Guide**.

Note:
If you are upgrading from 4.4.0.800 and want to retain your failover settings, please contact your local Tyco representative.

Serial Protocols

The Serial protocols which are supported by your NVR can be viewed on the **Serial Protocols** page. The default settings for each protocol can also be viewed.

Figure 58 Serial Protocols Page

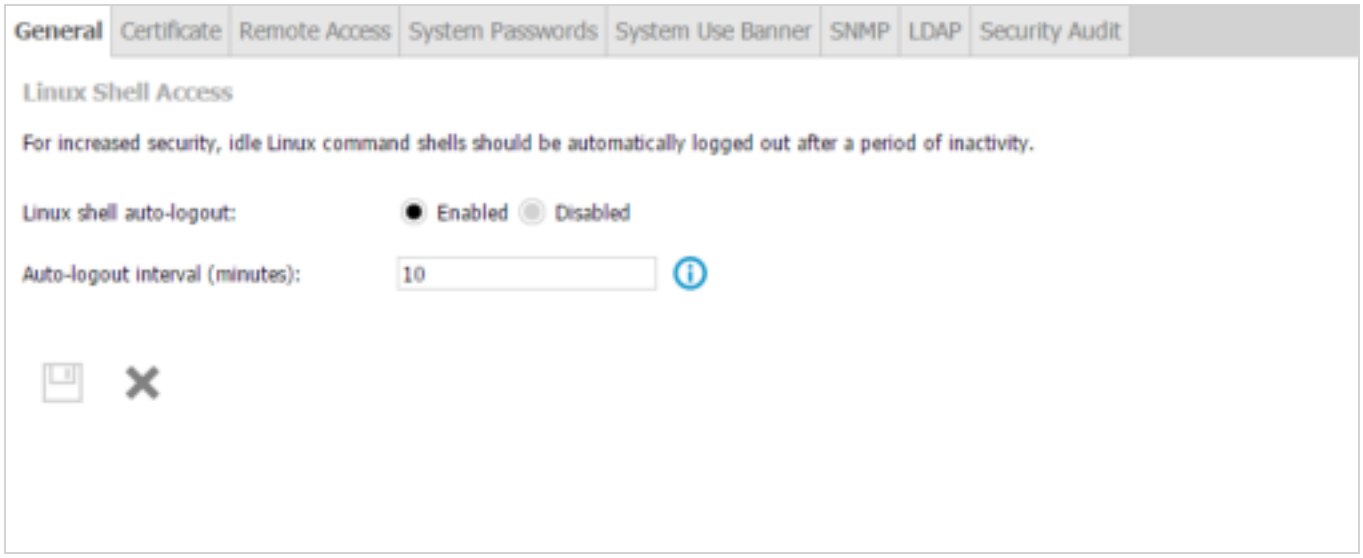
Procedure 189
Viewing Serial Protocols

Step	Action
1	Select **System** form the main menu.
2	Select **Serial Protocols**. The Serial Protocols page opens.

- End -

General

From the General tab, you can enable the Linux shell auto-logout option. This feature automatically logs users out of Linux command shells after a period of inactivity.



Procedure 190
Enabling auto-logout for VideoEdge

Step	Action
1	Select **System**.
2	Select **Security Configuration**.
3	Click **Enabled** to enable Auto-logout.
4	(Optional) Edit the **Auto-logout interval**. The minimum value is 5 minutes and the maximum value is 300 minutes.
5	Select 

- End -

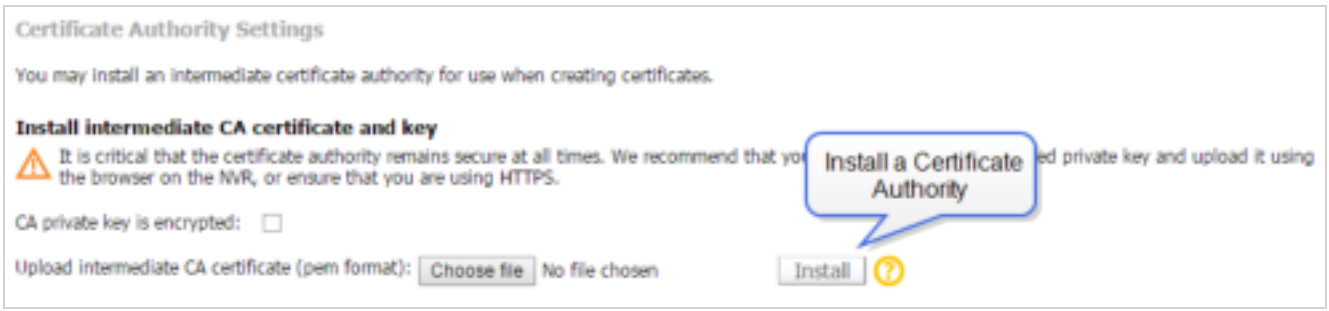
Security Configuration

You can configure enhanced security settings on your NVR including certificate settings, remote access, web server configuration, System Passwords, System Use Banner, SNMP and LDAP.

Note:
NVR-generated certificates (self-signed and CA-signed) and certificate signing requests use the SHA-256 algorithm in VideoEdge 4.7+ providing enhanced security.

Certificate Authority Settings

The “Certificate Authority Settings” section allows an intermediate certificate authority to be installed on the NVR for use in signing the NVR’s certificate. It is the responsibility of the customer to deploy the appropriate certificate chain to client computers. The uploaded certificate authority should be PEM-encoded and should contain the CA certificate and encrypted private key.



After you install the Certificate Authority, the details of the CA are visible on the Certificates Page.

Procedure 191
Installing a Certificate Authority

Note:
It is recommended that you use the browser on the NVR, or access the page using HTTPS, when installing the intermediate CA. This is to protect the decryption password from interception on the network.

Step	Action
1	Select **System**.
2	Select **Security Configuration**.
3	Select the **Certificate** tab.
4	(Optional) Select the **CA private key is encrypted** checkbox if required.
	a Enter the **Decryption Password** in the field.
5	Click **Browse**.
6	Navigate and select the required .PEM file.
7	Click **Open**.
8	Click **Install**.

- End -

When you generate a new certificate for the NVR, you can choose to use the installed CA to sign the certificate. To automatically include IP addresses from the certificate or certificate request, select the "Allow IP Addresses" checkbox.

CA-signed certificates can be identified in the "Installed certificates" section of the "Certificate" page, under "Issuer" details.

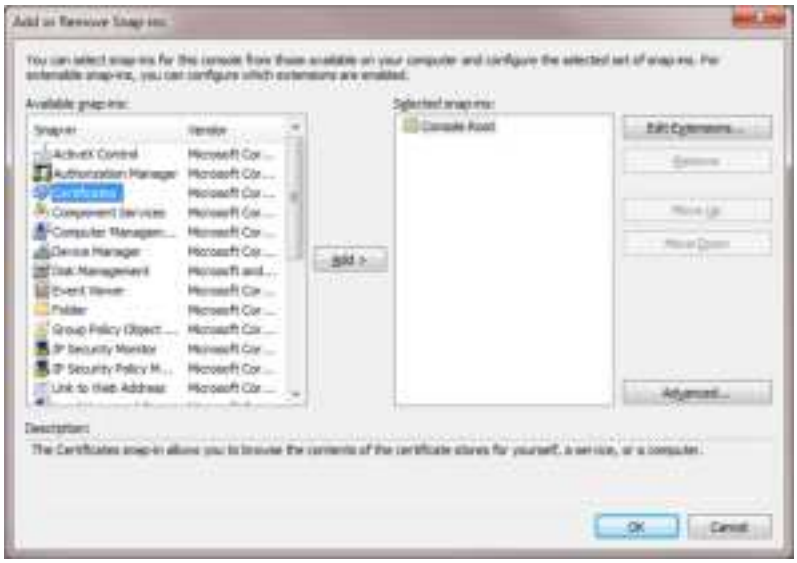
Installing Root and Intermediate Certificates

When using an installed CA or using a 3rd Party CA you will be required to install the Root and Intermediate certificate on your victor unified client PC.

Procedure 192
Installing Root / Intermediate Certificates

Step	Action
1	Open Microsoft Management Console (MMC). **Windows Button** > **MMC** > **Return** MMC will launch.

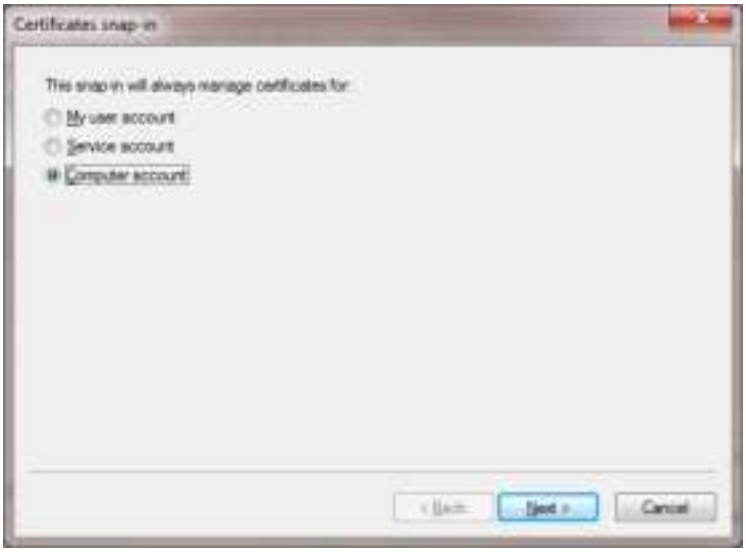
2	In MMC select **File** > **Add/Remove Snap-In**.
3	Select **Certificates** from the Available snap-ins.



4 Click **Add >**.

The Certificates snap-in Wizard launches.

5 Click the **Computer Account** option button.



6 Click **Next**.

7 Click the **Local Computer** option button (selected by default).

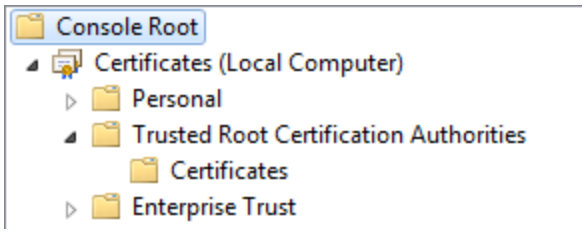
8 Click **Finish**.

9 Click **OK**.

A certificates dropdown menu will appear under the Console Root. Located on the left hand module of MMC.

10 Select the **Certificates** menu dropdown.

11 Select **Trusted Root Certification Authorities** dropdown.

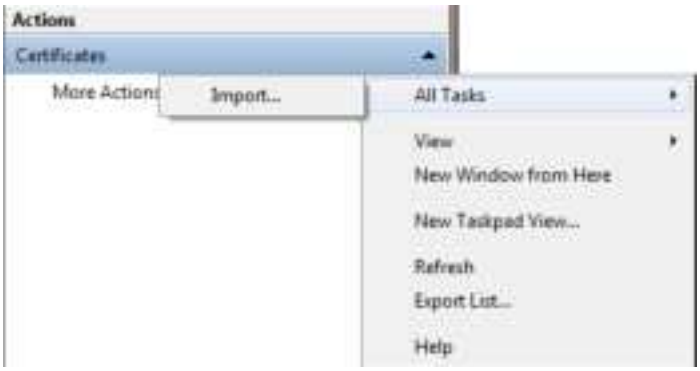


12 Select **Certificates**.

13 Select **More Actions**. Located on the right hand module of MMC.

14 Navigate to **All Tasks**.

15 Select **Import...**.



The Certificate Wizard launches.

16 Click **Next**.

17 Click **Browse**.

18 Navigate to your Root Certificate and click **Open**.

19 Click **Next**.

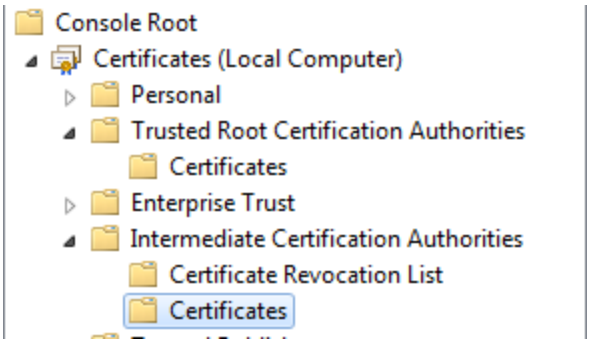
20 Click **Next**.

21 Click **Finish**.

A message stating "import was successful" displays.

22 Under certificates menu on the left hand module of MMC, select **Intermediate Certification Authorities**.

23 Select **Certificates**.



24 Select **More Actions**. Located on the right hand module of MMC.

25 Navigate to **All Tasks**.

26 Select **Import...**.

The Certificate Wizard launches.

27 Click **Next**.

28 Click **Browse**.

29 Navigate to your Intermediate Certificate and click **Open**.

30 Click **Next**.

31 Click **Next**.

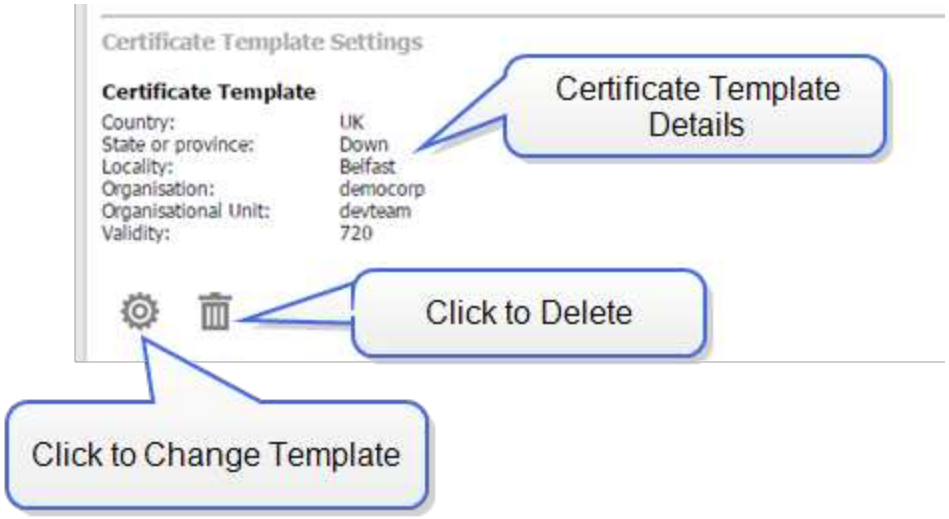
32 Click **Finish**.

A message stating "import was successful" displays.

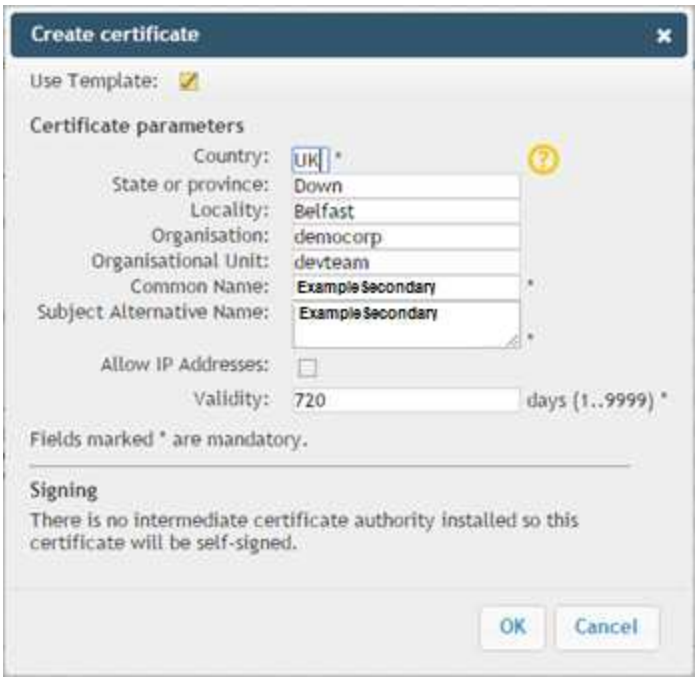
- End -

Certificate Template Settings

You can define a template for use when generating certificates or certificate signing requests.



When a template has been specified, you will have the option to use it when creating a certificate or certificate signing request.



Procedure 193
Create a Certificate Template

Step	Action
1	Select **System**.
2	Select **Security Configuration**.
3	Select the **Certificate** tab.
4	Select  . The Edit certificate template window opens.
5	Enter the **Country Code**.
6	(Optional) Enter the **State or province**.
7	(Optional) Enter the **Locality**.
8	(Optional) Enter the **Organisation**.
9	(Optional) Enter the **Organisational Unit**.
10	Enter the **Validity**.
11	Click 

- End -

Certificate Automatic Generation

Certificate automatic generation can be enabled and disabled, using the option button. A certificate template must be created before you can enable certificate automatic generation. If the certificate template is deleted, certificate automatic generation will be disabled. By default, certificate automatic generation is disabled.

When automatic generation is enabled, the NVR will generate a new certificate when it detects that the certificate does not contain all of the names and IP addresses that are currently configured on the NVR. When a certificate is automatically generated, it is created with the certificate template.

Procedure 194
Enabling Certificate Automatic generation

Step	Action
1	Select **System** from the main menu.
2	Select **Security Configuration**.
3	Select the **Certificate** tab.
4	Scroll to the Certificate Automatic Generation section of the page.
5	Click the **Enabled** option button.
6	Click 

- End -

Certificate Settings

When using HTTPS communication, a PKI certificate is required to provide secure encrypted communications and identify the NVR to the connecting device. VideoEdge supports the creation of a self-signed certificate or use of a certificate provided by a 3rd-party Certificate Authority. A certificate sourced from a 3rd-party Certificate Authority typically provides a higher level of security than a self-signed certificate.

Note:
The VideoEdge is provided with a default certificate. After you configure your VideoEdge you should install an NVR-specific certificate. You can generate a self-signed certificate on the VideoEdge, or you can upload a CA-signed certificate after creating a certificate-signing request on the VideoEdge.

Creating a self-signed certificate

For users with a lower security requirement, you can create a self-signed certificate which can then be installed on victor unified client and victor Application Server allowing communication between the recorder and the client.

Figure 59 Certificate Page

Procedure 195
Creating a self-signed certificate

Step	Action
1	Select **System** from the main menu.
2	Select **Security Configuration**.
3	Select the **Certificate** tab.
4	Click **Create Certificate**.
5	Enter the **Country** code in the field.
	Note: The country code must be entered as per the standard SSL Certificate Country Code.
6	(Optional) Enter the **State or province** in the field.
7	(Optional) Enter the **Locality** in the field.
8	(Optional) Enter the **Organisation** in the field.
9	(Optional) Enter the **Organisational Unit** in the field.
10	Edit the **Common Name** if required.
11	Edit the **Subject Alternative Name** if required.
12	Edit the **Validity** if required.
13	Click  . The new certificate is activated.
14	Click  and restart your browser.

- End -

Creating a request for a signed certificate

For users with more stringent security requirements, you can create a certificate-signing request for your CA. Once the CA has issued a signed certificate you can then install it using the Security Configuration page.

Procedure 196
Creating a certificate request

Step	Action
1	Select **System** from the main menu.
2	Select **Security Configuration**.
3	Select the **Certificate** tab.
4	Click **Create Certificate Signing Request**.
5	Enter the **Country** code in the field.
	Note: The country code must be entered as per the standard SSL Certificate Country Code.
6	(Optional) Enter the **State or province** in the field.
7	(Optional) Enter the **Locality** in the field.
8	(Optional) Enter the **Organization** in the field.
9	(Optional) Enter the **Organizational Unit** in the field.
10	Edit the **Common Name** if required.
11	Edit the **Subject Alternative Name** if required.
12	Click  . The certificate request is displayed in PEM format.
13	Copy and paste the request into email or alternative file for sending to the CA.
14	Click  .
	Note: A summary of the certificate request will be displayed on the Certificates page. To delete an awaiting certificate request, click  .

- End -

Uploading a Signed Certificate

Once your CA has issued a signed certificate, it can be uploaded using the Security Configuration tab.

Procedure 197
Uploading a Signed Certificate

Step	Action
1	Select **System** from the main menu.
2	Select **Security Configuration**.
3	Select the **Certificate** tab.
4	Click **Browse**.
5	Use the windows file explorer to locate the signed certificate.
6	Click **Open**.
7	Click **Install**.

- End -

Remote Access Services

You can enable or disable SSH and XRDP remote access to the VideoEdge operating system using the Security Configuration menu item to suit your network's security requirements.

Note:
• You cannot enable SSH or XRDP until you change the default VideoEdge password and system password. This requirement does not apply if you upgrade to VideoEdge 5.0 SP1 from an earlier version.
• In VideoEdge 5.0 or earlier, SSH and XRDP are enabled by default.

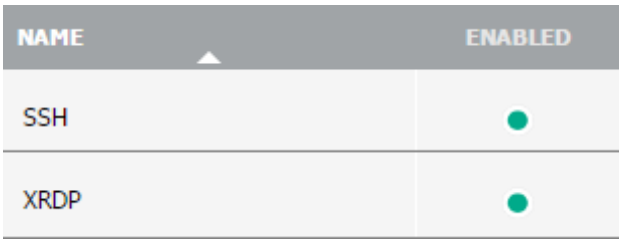
SSH (Secure Shell) is an encrypted network protocol for text based sessions on remote machines (e.g. VideoEdge) from another machine that has network access. 'PuTTY' is a common piece of software used to access remote machines by SSH.

RDP (Remote Desktop Protocol) is a graphical desktop sharing protocol developed by Microsoft. It allows control of remote machines (e.g. VideoEdge) from another machine that has network access. 'Remote Desktop Connection' available in Windows is a common piece of software used to access remote machines using the VideoEdge's XRDP client.

Note:
When accessing the VideoEdge remotely, you should log in using the "VideoEdge" user account.

Procedure 198
Enabling and Disabling Remote Access Services

Step	Action
1	Select **System** from the main menu.
2	Select **Security Configuration**.
3	Select the **Remote Access** tab.
4	Navigate to the Remote Access Services table.



5 Click the **Enabled** icon in the entry you want to enable or disable remote access.

A dialog box opens.

6 Click **OK**.

- End -

Remote Web Access

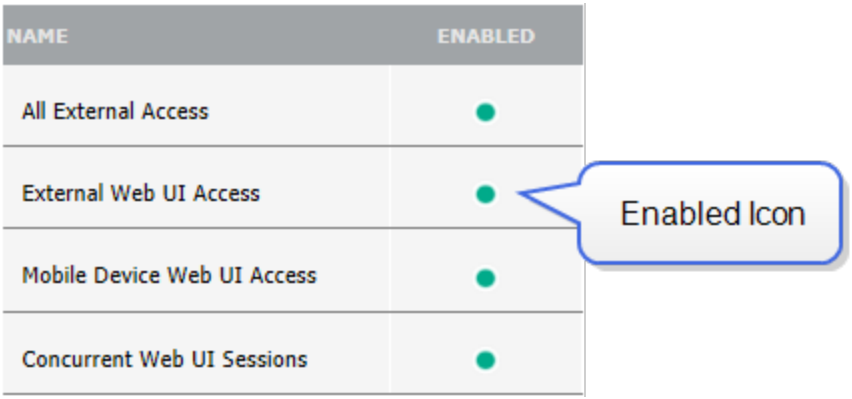
Note:
Remote Web Access Services are enabled by default.

You can enable/disable or restrict remote web access to the VideoEdge Administration Interface using the Security Configuration menu item to suit your network's security requirements.

Note:
Disabling Remote Web Access to your VideoEdge will disable access to the VideoEdge Administration Interface from everywhere except on the VideoEdge unit itself. This includes the ability to play video from the recorder. Video recording is unaffected.

Procedure 199
Enabling/Disabling and Restricting Remote Web Access

Step	Action
1	Select **System** from the main menu.
2	Select **Security Configuration**.
3	Select the **Remote Access** tab.
4	Navigate to the Remote Web Access table.



5 Click the **Enabled** icon in the entry you want to enable or disable remote access.

A dialog box opens.

6 Click **OK**.

- End -

Web Server Protocol Configuration

Note:
The web server supports HTTP and HTTPS protocols by default. The HTTP Port has a default value of 80 and the HTTPS Port has a default value of 443.

You can configure the communication type (HTTP or HTTPS) being used by the NVR to communicate with clients. You can also assign ports to be used for HTTP or HTTPS communication.

HTTP vs HTTPS

HTTP is the default protocol used by VideoEdge to communicate with clients (e.g. victor unified client). HTTPS is a more secure version of HTTP, providing bidirectional encryption of communication between VideoEdge and its clients.

TLS

Transport Layer Security (TLS) 1.0 is disabled by default in VideoEdge. If you need to add VideoEdge securely to a version of victor that is earlier than 4.9.1, you must enable TLS v1.0 first.

Note:
After you add VideoEdge to victor, disable TLSv1.0.

Procedure 200
Editing the Web Server Configuration

Step	Action
1	Select **System** from the main menu.
2	Select **Security Configuration**.
3	Select the **Remote Access** tab.
4	Navigate to the Web Server Ports and Protocols section.

Figure 60 Web Server Ports and Protocols

5 Select the **HTTP and HTTPS** option button.

Or

Select the **HTTPS only** option button.

a Enter the **HTTP port** you want to use in the field.

b Enter the **HTTPS port** you want to use in the field.

Note:
You can only configure one value at a time. To edit the HTTP Port and HTTPS port value you must edit one and save before you can edit the other.

6 (Optional) Select the **Enabled** button to enable TLSv1.0.

7 Click 

- End -

System Passwords

From the System Passwords menu, you can change the system VideoEdge password, and the system root password. The root account provides full administrative access to the VideoEdge's embedded operating system. Changing the default root password to a unique password enhances the security of the product.

Caution

• It is highly recommended for security reasons that you change the root password and the VideoEdge password.

• In VideoEdge 5.0SP1, you cannot enable SSH or XRDP until you change the default system password. This requirement does not apply if you upgrade to VideoEdge 5.0 SP1 from an earlier version.

Note:
• For security reasons, the System Password page must run under HTTPS.

Procedure 201
Changing the System VideoEdge password

Step	Action
1	Select **System** from the main menu.
2	Select **Security Configuration**.
3	Select the **System Passwords** tab.
4	(When viewing in HTTP Only) Click **Change to HTTPS**. A browser warning page displays to state there is a problem with the website's security certificate. This warning only displays when the default NVR certificate or a certificate not signed by a trusted root CA is installed.
5	Select **Continue to this website (not recommended)**. **Note:** Wording may differ between browsers.
6	Change the System VideoEdge password. a Enter the **Current Password**. **Note:** The default system VideoEdge password is 'VideoEdge' b Enter the **New Password**. c Re-enter the New Password in the **Confirm Password** field.

Caution

It is extremely important that you remember this password. If necessary, you should write this password down and store it securely.

7	Click 

- End -

Procedure 202
Changing the System root password

Step	Action
1	Select **System** from the main menu.
2	Select **Security Configuration**.
3	Select the **System Passwords** tab.
4	(When viewing in HTTP Only) Click **Change to HTTPS**. A browser warning page displays to state there is a problem with the website's security certificate. This warning only displays when the default NVR certificate or a certificate not signed by a trusted root CA is installed.

5 Select **Continue to this website (not recommended)**.

Note:
Wording may differ between browsers.

6 Change the System root password.

a Enter the **Current Password**.

Note:
The default system root password is 'root'

b Enter the **New Password**.

c Re-enter the New Password in the **Confirm Password** field.

Caution

It is extremely important that you remember this password. If necessary, you should write this password down and store it securely.

7 Click 

- End -

System Use Banner

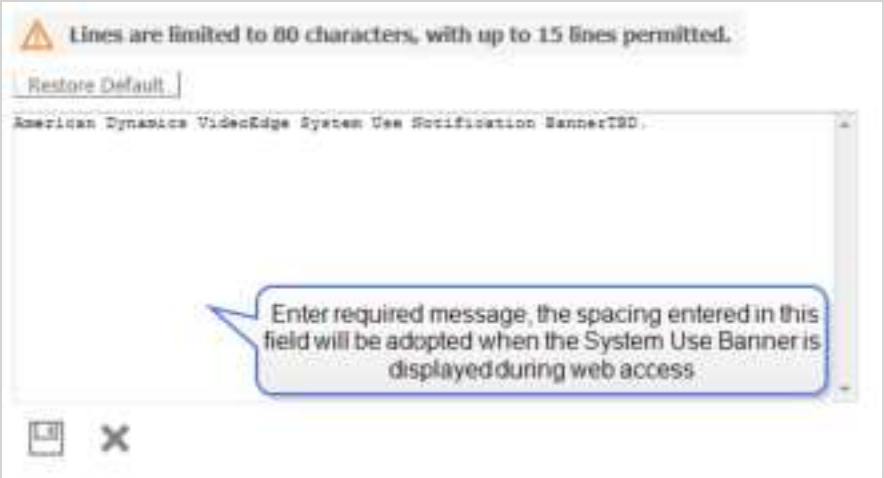
The System Use Banner can be configured to display an approved system use notification message or banner which is displayed before the user logs on to the system either locally or remotely. It can be used to provide privacy and security notices consistent with applicable federal laws, executive orders, directives, polices, regulations, standards and guidances.

Note:
The System Use Banner is not populated by default.

Procedure 203
Configuring the System User Banner for non-XDRP Clients

Step	Action
1	Select **System** from the main menu.
2	Select **Security Configuration**.
3	Select the **System Use Banner** tab.

Figure 61 System Use Banner Field



Note:
The format entered in the system use banner field is preserved in both the VideoEdge Administrator Interface login page and during SSH login. When logging into the NVR locally the VideoEdge OS (VEOS) login window will display the use banner in a justified format.

4 Enter the required notifications in the text field.

Note:
If the text field is empty, the System Use Banner will not be displayed during login.

5 Click .

- End -

Procedure 204
Configuring the System User Banner for XDRP Clients

This System Use Banner will display when connecting to a VideoEdge using an RDP client such as Windows Remote Desktop Connection. By default, the 'VEOS Linux Enterprise Desktop Remote desktop connection' image will display when connecting by RDP.

Step	Action
1	Select **System** from the main menu.
2	Select **Security Configuration**.
3	Select the **System Use Banner** tab.
4	Click **Browse**. A file explorer window opens.
5	Select the file you want to use for the System Use Banner.

Note:
Only bitmap files are supported, they can be identified by the **.bmp** file extension. Some XDRP clients may be sensitive to the .bmp image size.

6 Click **Open**.

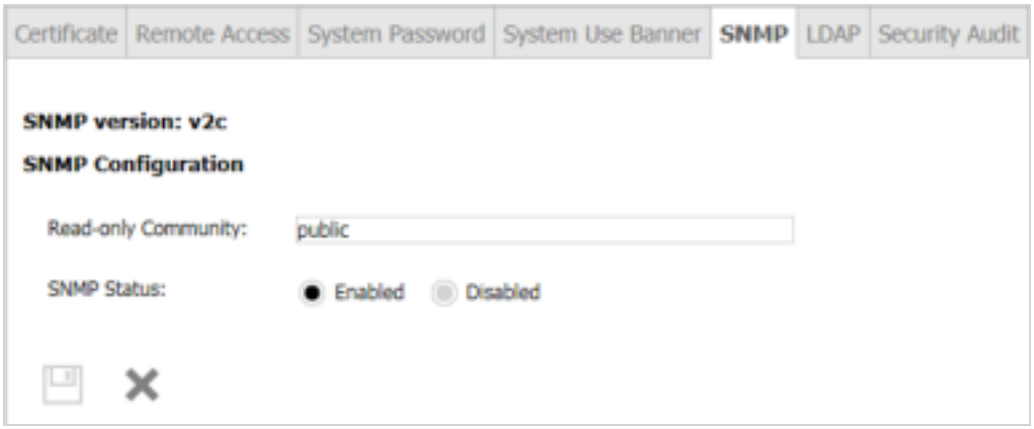
7 Click **Upload XRDP Banner**.

- End -

SNMP Configuration

SNMP (Simple Network Management Protocol) is a common protocol used by network administrators to manage devices on their network remotely. For VideoEdge, NVRs that are in an NVR group use SNMP to share information. Each NVR in the group must have the same SNMP port configured and use the same SNMP user credentials. You can enable or disable SNMP Services from the **Security Configuration** menu.

Note:
• SNMP Services are enabled by default.
• When accessing the VideoEdge remotely, you should log in using the "VideoEdge" user account.



Procedure 205 Enabling/Disabling SNMP Services

Step	Action
1	Select **System** from the main menu.
2	Select **Security Configuration**.
3	Select the **SNMP** tab.
4	Click the **Enabled** button to enable SNMP services. Or Click the **Disabled** button to disable SNMP services.
5	Click 

- End -

LDAP Configuration

Note:
LDAP is not configured by default.

VideoEdge supports the use of a Lightweight Directory Access Protocol (LDAP) server to authenticate users of both the VideoEdge Administration Interface and VideoEdge Client. This minimizes configuration of users on VideoEdge and enables multiple NVRs to share one centralized server for user management.

Note:
If the LDAP server is offline, access to the VideoEdge Administration Interface/VideoEdge Client can only be achieved using the local on board credentials.

VideoEdge LDAP supports the use of active directory and a secure connection. To establish a secure connection, install the Certificate Authority certificate that was used to sign the LDAP server certificate. It is recommended that you establish a secure connection before you perform the following actions:

- Log in to the VideoEdge as an LDAP user.
- Retrieve a list of LDAP groups on the LDAP Roles page.

See **Users and Roles** for more information on LDAP Roles.

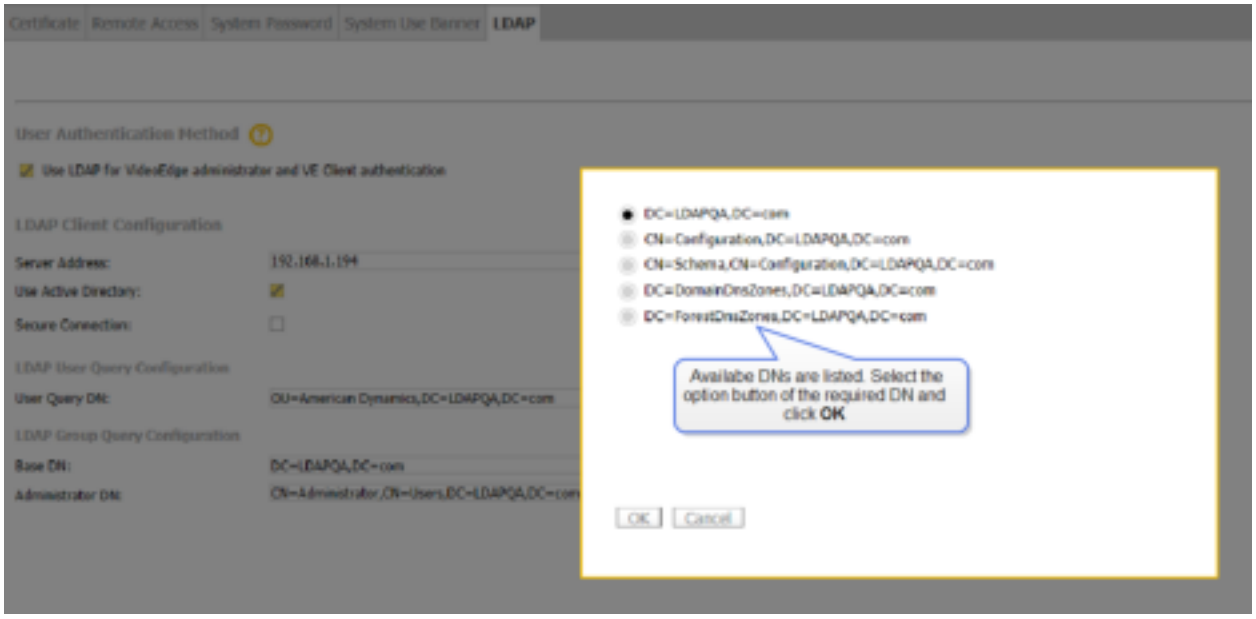
Procedure 206
Enabling LDAP Support

Step	Action
1	Select **System** from the main menu.
2	Select **Security Configuration**.
3	Select the **LDAP** tab.
4	Select the **Use LDAP for VideoEdge administrator and VE Client authentication** checkbox.
5	Enter the LDAP Server IP address in the **Server Address** field.
6	(Optional) If using Active Directory on your LDAP server, select the **Use Active Directory** checkbox.
7	(Optional) Select the **Secure Connection** checkbox.
8	Click **Browse** to search for the LDAP server certificate. A file explorer window opens. **Note:** If you require an LDAP server certificate to be issued, contact your IT department.
9	Navigate to the required location and select the certificate.
10	Click **Open**.
11	Click **Install**. A dialog box displays to notify the success of the installation.
12	Click **OK**.
13	Enter the **User Query DN** in the field.

Note:
The User Query DN should be the distinguished name of the organizational unit that the user belongs to.

14 Enter the **Base DN** in the field. Click **Fetch DN** to view a list of available Base DNs.

Figure 62 Fetch DN Configuration Window



Note:
The Base DN is the starting point for the search. Only groups within the specified Base DN will be retrieved. The value must be a distinguished name that currently exists in the database.

15 Enter the **UPN Suffix** in the field.

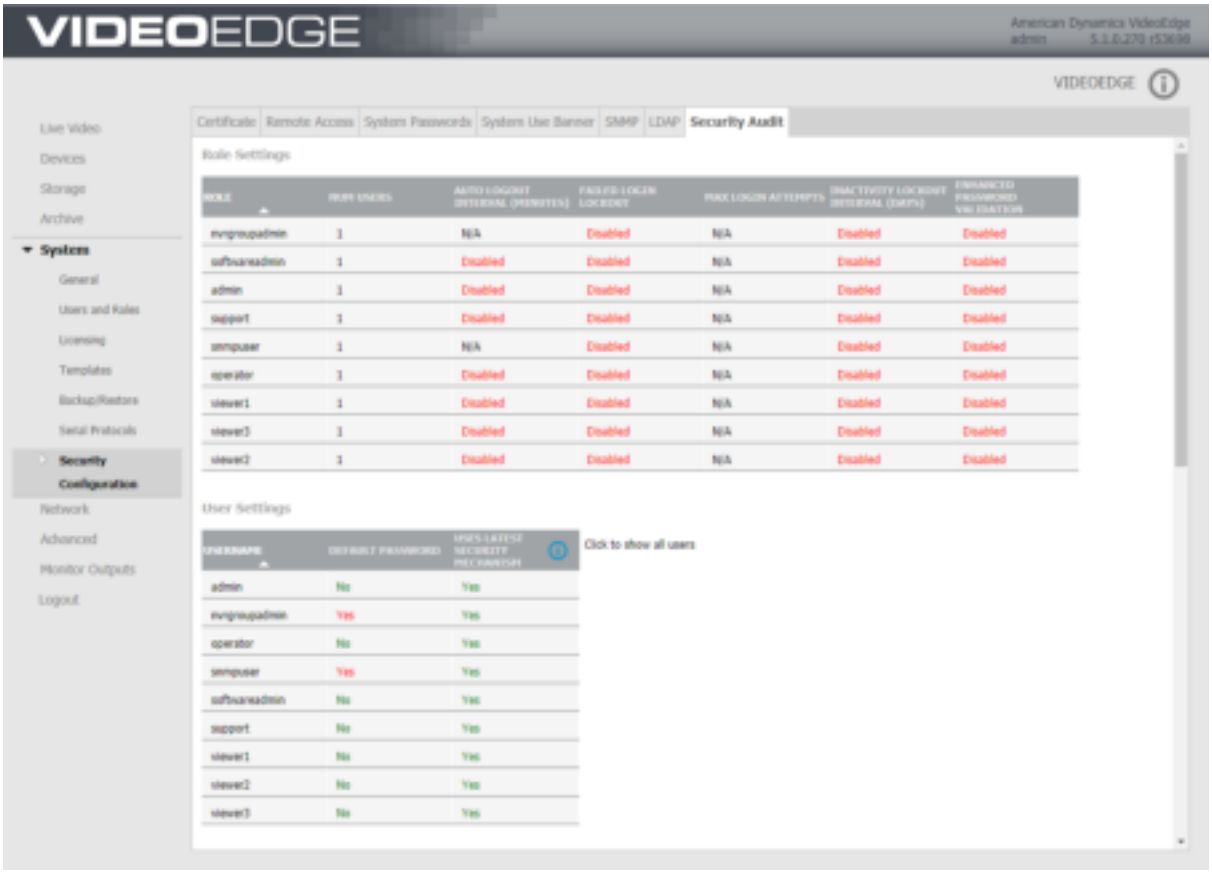
16 Enter the **Administrator DN** in the field.

Note:
The Administrator DN is used to authenticate to the server. The value must be a distinguished name with the authority to search for groups. This is the sole purpose of the Administrator DN.

17 Click  .

- End -

Security Audit



The Security Audit page contains a read-only status summary for the following NVR settings:

- Role Settings
- User Settings
- Linux user Settings
- Web Server Ports and protocols
- Remote Access
- Certificate settings
- Certificate Authority settings
- System Robustness

In addition, the NVR settings that are shown on the Security Audit page are color-coded. The color assigned indicates if recommendation for changing the setting is required.

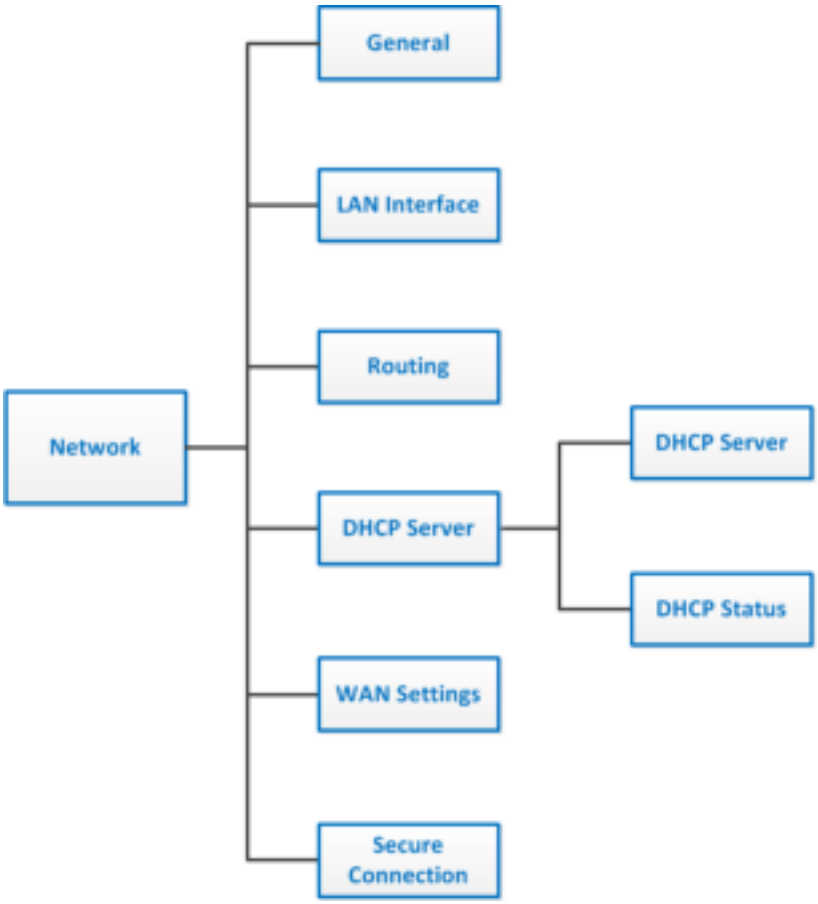
- Black - The setting does not require assessment.
- Red - The setting is not secure. It is strongly recommended that you change this setting.
- Amber - The setting is partially secure. It is strongly recommended that you change this setting.

Note:
You should review the Security Audit page every time you change your VideoEdge security settings.

Network Menu Overview

The **Network** Menu allows you to configure the NVR's network settings including general network settings, LAN Interface settings, DHCP Server settings, and WAN settings.

Figure 63 Network Menu Map



- **General** - From here you can configure general network settings including -
  - Domain Name
  - Domain Name Servers
  - Default Gateway
  - RTSP Port
  - RTSP Encryption
  - SNMP Port
  - UPnP
  - Multicasting
  - NTP Status

- WAN and LAN Bitrate Caps

- **LAN Interface** - From here you can edit the LAN settings for each installed NIC.
- **Routing** - From here you can configure network routing properties.
- **DHCP Server** - From here you can configure the NVR to host a DHCP Server on each of its installed NICs.
- **WAN Settings** - From here you can configure the NVR to operate in a wide area network.

Configuring the NVR Network Settings

The NVR is designed to use a network topology utilizing multiple LAN connections. It can also be configured to utilize a WAN network to connect to remote clients via the internet. The design provides the user an extra layer of security for the cameras and reduces the network traffic on the LAN backbone. It also helps prevent accidental or unauthorized changes to the configuration. The example illustrated below is only one possible configuration as the NVR can be set up in a number of configurations to meet your bespoke requirements. Each variant of the NVR is supplied with two Network Interface Controllers (NICs), however if desired additional network cards can be fitted to increase the number of connections. Contact American Dynamics for more information.

The NVR's network connections can be configured to meet your specific requirements. The primary NIC (eth0) is used as the LAN backbone and allows the NVR to connect to client PCs.

The secondary NIC (eth1) is used to connect to a camera network. This is particularly advantageous as the NVR acts as a firewall between users and the cameras. The users do not have direct access to the cameras on LAN 2 and must access the NVR in order to view and configure the cameras. By using a separate camera network on LAN 2, bandwidth is distributed optimizing the performance of both network connections.

An additional NIC can be used to connect to iSCSI network storage increasing the storage space available to the NVR.

Figure 64 Network Diagram Example (VideoEdge Hybrid NVR)

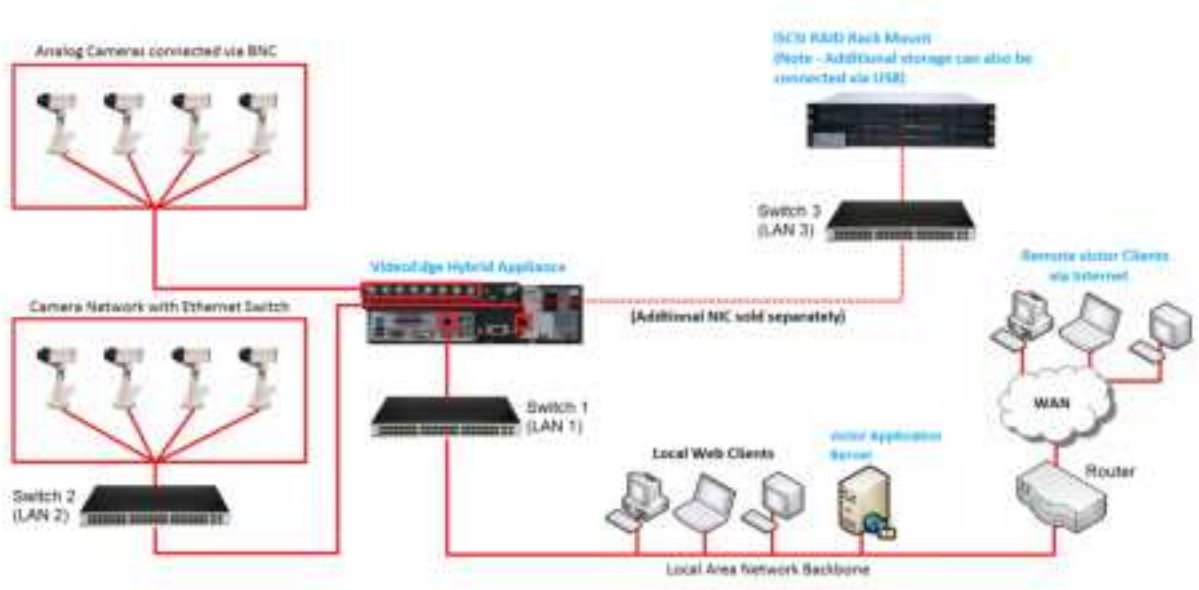
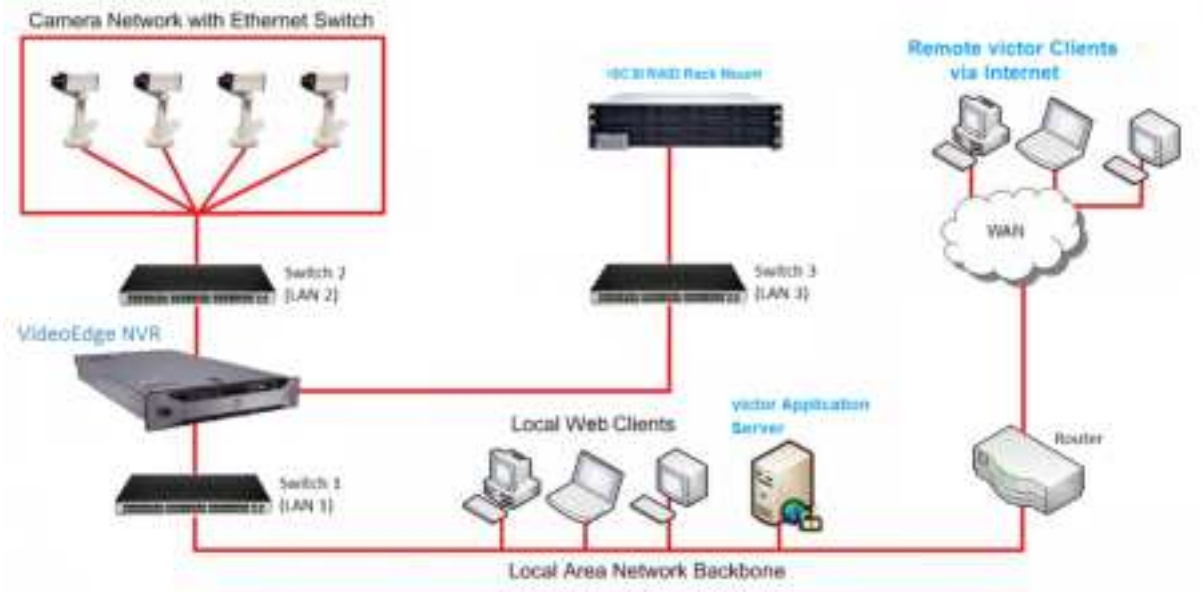


Figure 65 Network Diagram Example (VideoEdge NVR)



LAN 1 - Connects the NVR to the network with client PCs. Client PCs typically access the NVR through this port.

Note:
LAN 1's default IP Address for an NVR supplied as a hardware and software bundle is **10.10.10.10**.

LAN 2 - Connects the camera network to the NVR. With this architecture, the NVR acts as a firewall between users and the cameras.

Alternatively, if Switch 2 has network routing capabilities (for example, Layer 3 Switch), you can extend the camera network to include cameras in multiple subnets from the main network. See Routing for more information about configuring network routes.

LAN 3 - If required an additional NIC can be fitted to the NVR, this allows the addition of a network storage array. Alternatively additional storage can be connected using the NVR's USB ports.

The users do not have direct access to the cameras on LAN 2 and must access the NVR in order to view and configure the cameras. As the LAN 2 cameras are not on the main network, they use less network bandwidth from the main network.

In this example DHCP is enabled on LAN 2 so that the NVR can automatically assign IP addresses to cameras that are added to LAN 2. The NVR can have DHCP enabled for each of its NICs.

LAN 3 - Connects network storage devices to the NVR.

Caution

Connecting an NVR running a DHCP server to a network that already has a DHCP server can disrupt network service on that network.

If you have more than one NVR on LAN 2, you will need to disable DHCP on all but one of the LAN 2 NVRs, so that cameras are receiving IP Addresses from only one DHCP server.

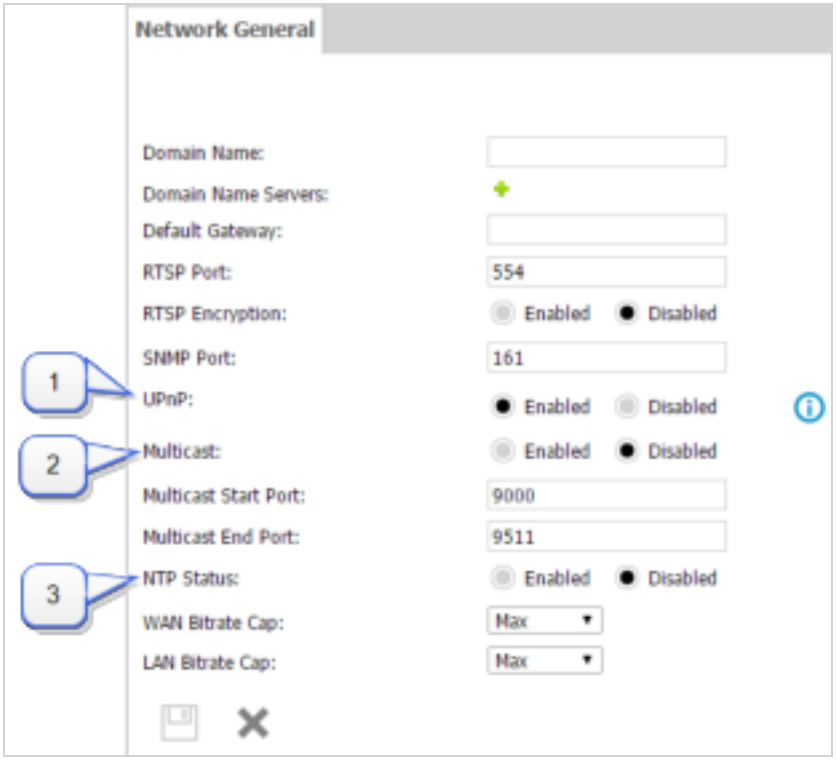
Note:
When the NVR is supplied as a hardware and software bundle only LAN 1 will be enabled, all other NICs will be disabled.

The Hybrid NVR can act as a DHCP server and assign dynamic IP addresses to devices on each network it is connected to, provided the devices are configured to function with a DHCP Server.

General

The Network General page provides you the option to configure your NVR's general network settings.

Figure 66 General Network Settings



Number	Description
1	UPnP advertisements used for NVR discovery.
2	Enables NVR Multicasting.
3	Synchronize date and time with an NTP server.

Domain Name and Domain Name Servers

You can assign a bespoke Domain Name and create a list of DNS which provide name resolution services i.e. convert IP addresses to hostnames.

Procedure 207
Edit the Domain Name and Domain Name Servers

Step	Action
1	Select **Network**.
2	Select **General**. The Network General page opens.
3	Enter the **Domain Name** in the corresponding field.

Note:
victor unified client supports adding recorders via a FQDN.

4 To add a Domain Name Server select

A text field opens.

5 Enter the **DNS IP Address** in the field.

6 To enter several IP Addresses select to add an additional fields.

7 Click

- End -

Default Gateway

You can edit the IP Address of the Default Gateway. The default gateway must be set manually if the NVR is not using a DHCP server. The default gateway allows the NVR to have connectivity with IP addresses beyond the directly connected subnets of its own NICs.

Procedure 208
Editing the Default Gateway

Step	Action
1	Select **Network**.
2	Select **General**. The Network General page opens.
3	Enter the **Default Gateway** IP address in the corresponding field.
4	Click A warning dialog will display stating 'Changing the default gateway may result in your NVR becoming inaccessible. If this happens, you will need to physically connect to the NVR to re-enable network access. Are you sure you want to proceed?'.
5	Click **OK**.

- End -

RTSP Settings

If required you can modify the default RTSP Streaming Port for your NVR to conform to your network rules. You can also enable or disable RTSP encryption.

Note:
RTSP encryption is disabled by default.

Procedure 209
Editing the RTSP settings

Step	Action
1	Select **Network**.
2	Select **General**. The Network General page opens.
3	Enter the required **RTSP Port** in the corresponding field.
4	(Optional) Select the **Enabled** button to enable RTSP encryption.
5	Click  **Note:** The default RTSP Port number is **554**.

- End -

SNMP Port

The NVR uses SNMP for communication purposes when using the NVR Groups functionality. If required you can modify the default SNMP port for your NVR to conform to your network rules.

Procedure 210
Editing the SNMP Port

Step	Action
1	Select **Network**.
2	Select **General**. The Network General page opens.
3	Enter the required **SNMP Port** in the corresponding field.
4	Click  **Note:** The default SNMP Port number is **161**. You must ensure that the same SNMP port value is assigned on all members of an NVR group, if not, communication will not be established.

- End -

UPnP

By default the NVR sends UPnP advertisements to allow victor unified client to discover it on a network. You can enable or disable UPnP advertising as required.

Procedure 211
Enabling/Disabling NVR UPnP Advertisements

Step	Action
1	Select **Network**.
2	Select **General**. The Network General page opens.
3	Select the UPnP **Enable** or **Disable** option button.
4	Click 

- End -

Multicasting

VideoEdge can provide streams to connected clients via multicast. This can be enabled or disabled as required.

Note:
Multicast is disabled by default. You should contact your IT Administrator for configuration of your network to support multicasting if required.

Procedure 212
Enabling/Disabling Multicast

Step	Action
1	Select **Network**.
2	Select **General**. The Network General page opens.
3	Select the Multicast **Enable** or **Disable** option button.
4	(Optional) Edit the Multicast Start Port by entering the **start port value** in the field.
5	(Optional) Edit the Multicast End Port by entering the **end port value** in the field. **Note:** If multiple VideoEdge NVRs are streaming multicast to a single victor unified client, ensure that the NVRs are configured so that their port ranges do not overlap.
6	Click 

- End -

Network Time Protocol

You can use external NTP servers to synchronize your NVR's date and time.

Note:
You should setup all NVRs and client systems to use the same NTP Server, to synchronize date and time settings.

Procedure 213
Enabling/Disabling NTP

Step	Action
1	Select **Network**.
2	Select **General**. The Network General page opens.
3	Select the NTP Status **Enable** or **Disable** option button. (When Enable is selected) The NTP Servers menu item displays. a To edit the **NTP Servers** click . b Enter the NTP Server IP Address in the field. c To enter several IP Addresses, click
4	Click

- End -

WAN and LAN Bitrate Caps

To assist network balancing you can assign both a WAN and LAN bitrate cap. A bitrate cap limits the amount of streaming data (i.e. video) leaving the NVR to remote clients or clients connected using VPN. The WAN and LAN bitrate caps can be set to either a predefined value from the dropdown menus or alternatively a custom value can be entered in the field.

Note:
The WAN bitrate cap cannot exceed the LAN bitrate cap.

Procedure 214
Configuring the WAN and LAN Bitrate Caps

Step	Action
1	Select **Network**.
2	Select **General**. The Network General page opens.
3	Navigate to the **WAN** or **LAN Bitrate Cap**s.
4	To use a predefined value open the dropdown and select the required value from the list. **Note:** To apply no limit, select **Max**. Or a To use a custom value, select **Custom** from the dropdown. The custom entry field displays. b Enter the required value in the field.

Note:
The custom value must be entered in **kbps**. For example to enter a value of 5.5Mbps you would type a value of 5500.

5 Click 

- End -

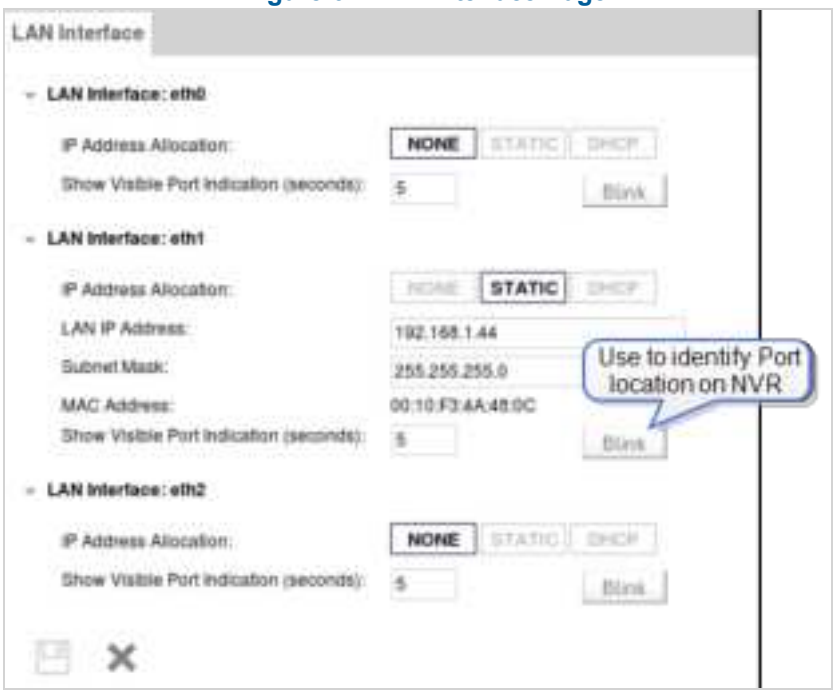
LAN Interface

The LAN Interface page allows you to enable and disable the NICs of the NVR. Each NIC provides a LAN interface for the NVR.

The LAN Interface page also allows you to edit the available LAN Interfaces. In the LAN Interface page the NIC's associated with the NVR will be displayed and available for editing. The LAN Interface page allows you to edit the IP Address Allocation, LAN IP Address and Subnet Mask. The page will also display the MAC address for each NIC on the NVR.

Note:
If you are configuring or editing the LAN Interface Settings for a primary NVR when Failover mode is in use on your network, the units Virtual IP address will also display on this page. It cannot be edited.

Figure 67 LAN Interface Page



Procedure 215
Enabling NICs

Step	Action
1	Select **Network**.
2	Select **LAN Interface**. The LAN Interface page opens.
3	Choose the LAN Interface you want to edit.
4	Select **DHCP** to allow a DHCP Server on the LAN to assign an IP address for that NIC of the NVR. **Note:** The use of DHCP for all of the NVR's NICs is not recommended. To open the NVR Administrator Interface the IP address of one of the NICs must be known, if all the IP addresses are dynamic they

will vary in value. It is recommended that a NIC is configured with a static IP address and subnet mask for this reason.

Or

Select **STATIC** to permanently assign an IP address and subnet mask to the NVR.

When using Static IP addresses you will be required to enter the IP address and subnet mask in the corresponding fields.

5 Click 

A dialog box displays advising that changing network interface settings may result in your NVR becoming inaccessible.

6 Click **OK**.

- End -

Procedure 216
Disabling NICs

Step	Action

1 Select **Network**.

2 Select **LAN Interface**.

The LAN Interface page opens.

3 Choose the LAN Interface you want to edit.

4 Select **NONE** from the IP Address Allocation dropdown.

When **NONE** is selected the LAN Interface options for that NIC will collapse leaving only the IP Address Allocation displayed.

5 Click 

A dialog box displays advising that changing network interface settings may result in your NVR becoming inaccessible.

6 Click **OK**.

Note:
If you disable eth0 using the NVR Administration Interface it will terminate its connection on that NIC. To re-establish connection you can access the Administration Interface using the IP Address of one of the other active NIC's.

- End -

Procedure 217
Editing the LAN Interface Values

Step	Action

1 Select **Network**.

2 Select **LAN Interface**.

The LAN Interface page opens.

3 Choose the LAN Interface you want to edit.

4 To edit the **LAN IP Address**, enter the desired IP Address in the field.

5 To edit the **Subnet Mask**, enter the desired Subnet Mask in the field.

6 Click 

Note:
The displayed MAC Address cannot be edited.

- End -

Show Visible Port Identification

You can use the Show visible port identification feature to identify the physical location of each LAN interface on the NVR to aid correct connection to the appropriate network.

Note:
This feature is available for each LAN Interface provided it is supported by the installed network card.

Procedure 218
Using the Show Visible Port Identification feature

Step	Action
1	Select **Network**.
2	Select **LAN Interface**. The LAN Interface page opens.
3	Enter the **time** (in seconds) you want the LED indicator to blink.
4	Click **Blink**.

- End -

DHCP Server

The DHCP Server page provides the option to configure the NVR to host a DHCP Server for each network card plugged into the system. This allows the NVR to allocate IP addresses from the range specified when other devices request IP allocation. The page allows you to edit the DHCP Status and the Start and End Range of IP Addresses to be included during automatic searching for IP Devices.

Caution

You should only set up the NVR as a DHCP Server if you are positive the LAN does not already have a DHCP Server, and the NVR has been assigned a static IP Address. Otherwise you could have two different DHCP Servers giving out IP addresses, and this could cause network problems.

Figure 68 DHCP Server Page

Procedure 219
Editing the DHCP Server Settings

Step	Action
1	Select **Network**.
2	Select **DHCP Server**. The DHCP Server settings page opens.
3	Select next to the LAN Interface you want to enable as a DHCP server. **Note:** NICs which have been configured with a DHCP IP Address Allocation will be grayed out and not available to be used to host DHCP Servers. A message is also displayed stating 'DHCP cannot be enabled on this interface unless the IP allocation method is set to STATIC on the 'LAN Interface' page.'
4	To edit the DHCP Status select either the **Enable** or **Disable** option buttons. When Enabled is selected the DHCP options for that NIC expand.

5 To edit the DHCP Start Range and End range enter the lowest and highest IP address to be assigned, respectively. For example, if your network addresses were between 10.11.12.50 and 10.11.12.100, you could type 10.11.12.50 for DHCP Range Start and 10.11.12.100 for DHCP Range End.

6 Click 

Note:
Subnet and Netmask cannot be edited in this page. The DHCP Start Range and End Range can only be entered when the DHCP Status is set to **Enabled**.

- End -

DHCP Status

From the DHCP Status page, you can view a list of devices that are managed by the VideoEdge DHCP server. You can also reserve the IP address that is assigned to a device. Reserved IP addresses are not re-allocated to other devices, even when the assigned device is inactive. The DHCP Status page displays the following device information:

- Hostname
- IP address
- Lease end time
- MAC address
- IP address reservation status

Figure 69 DHCP Status Page

Procedure 220
Viewing the DHCP Status

Step	Action
1	Select **Network**.
2	Select **DHCP Server**.
	The DHCP Server settings page opens.
3	Select the **DHCP Status** page.
	The DHCP Status page opens.

- End -

Procedure 221
Reserving a DHCP address

Step	Action
1	Select **Network**.
2	Select **DHCP Server**. The DHCP Server settings page opens.
3	Select the **DHCP Status** page. The DHCP Status page opens.
4	Select  Or Click the icon in the Reserved column.

- End -

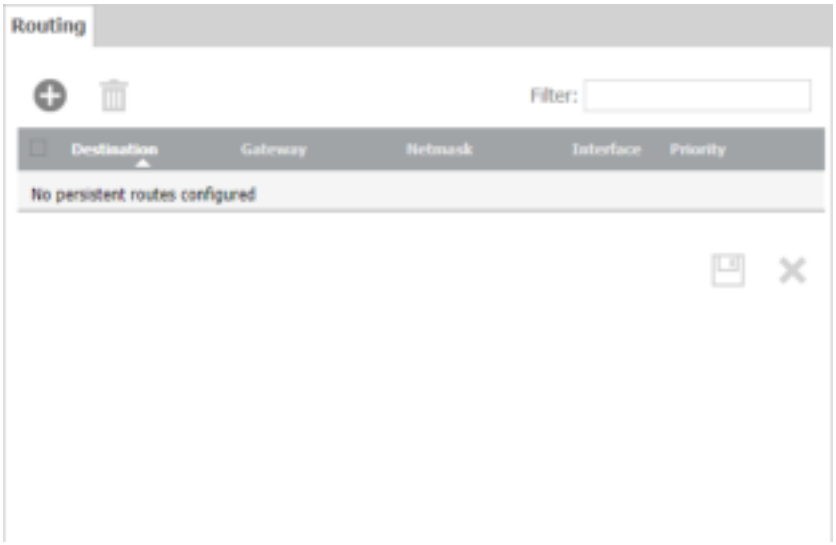
Procedure 222
Canceling a DHCP reservation

Step	Action
1	Select **Network**.
2	Select **DHCP Server**. The DHCP Server settings page opens.
3	Select the **DHCP Status** page. The DHCP Status page opens.
4	Select  Or Click the icon in the Reserved column.

- End -

Routing

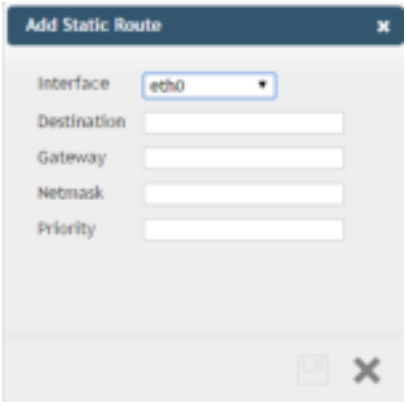
From the Routing page, you can configure a static route from your VideoEdge to another network.



Parameter	Description
Destination	The destination network or destination host.
Gateway	The gateway address
Netmask	The netmask for the destination network: Enter 255.255.255.255 for a host destination Enter 0.0.0.0 for the default route
Interface	The interface that packets for this route are sent to.
Priority	To specify a priority metric to determine which route has a higher priority.

Procedure 223
Adding a Static Route

Step	Action
1	Select **Network** from the main menu.
2	Select **Routing** to open the Network Routing page.
3	Select  The Add Static Route window appears.



4 Select a network interface from the **Interface** dropdown list.

5 Configure the destination network settings.

a Enter the network IP address in the **Destination** field.

b Enter the gateway IP address in the **Gateway** field.

c Enter the netmask in the **Netmask** field.

d (Optional) Enter route priority in the **Priority** field.

Note:
• Use an IPv4 address for the network and gateway addresses.
• If you specify more than one default route, you must assign route priority to each route. Lower values indicate higher priority.

6 Select to apply the route.

7 (Optional) Add additional routes if required.

8 In the Routing page, select to save the configuration changes.

- End -

Procedure 224
Editing a Static Route

Step	Action
1	Select **Network** from the main menu.
2	Select **Routing** to open the Network Routing page.
3	Click in the routing table row that you want to edit. The **Edit Static Route** window appears.
4	Edit the static route settings as required.
5	Select to apply the changes to the route.
6	In the Routing page, select to save the configuration changes.

- End -

Procedure 225
Deleting a Static Route

Step	Action
1	Select **Network** from the main menu.
2	Select **Routing** to open the Network Routing page.
3	Select the checkbox for the route that you want to delete. Or Select the **All Routes** checkbox to delete all routes.
4	Click  to delete the selected routes.
5	Select  to apply the configuration changes.

- End -

WAN Settings

The WAN Settings page allows you to configure the NVR to operate in a wide area network (WAN) configuration. The WAN Settings page lets you specify the name or IP address that can be used to access an NVR located behind a NAT firewall (such as a corporate LAN) that presents a single public address for connections from outside the LAN. You can also specify the ports that are used for HTTP, secure HTTP and streaming (RTSP) connections to the NVR. You can also enter a list of allowed IP addresses. In addition, the General Settings page allows you to change the RTSP Streaming Port.

Note:
For a new install, the Setup WAN fields display the default values. If you upgrade the NVR, these fields will display the previously assigned values however if you carry out an appliance install the values will be lost unless a template has been created and applied. If you enter a value into any of these fields, that value is saved, and is displayed until modified.

Figure 70 WAN Port Mapping Exam

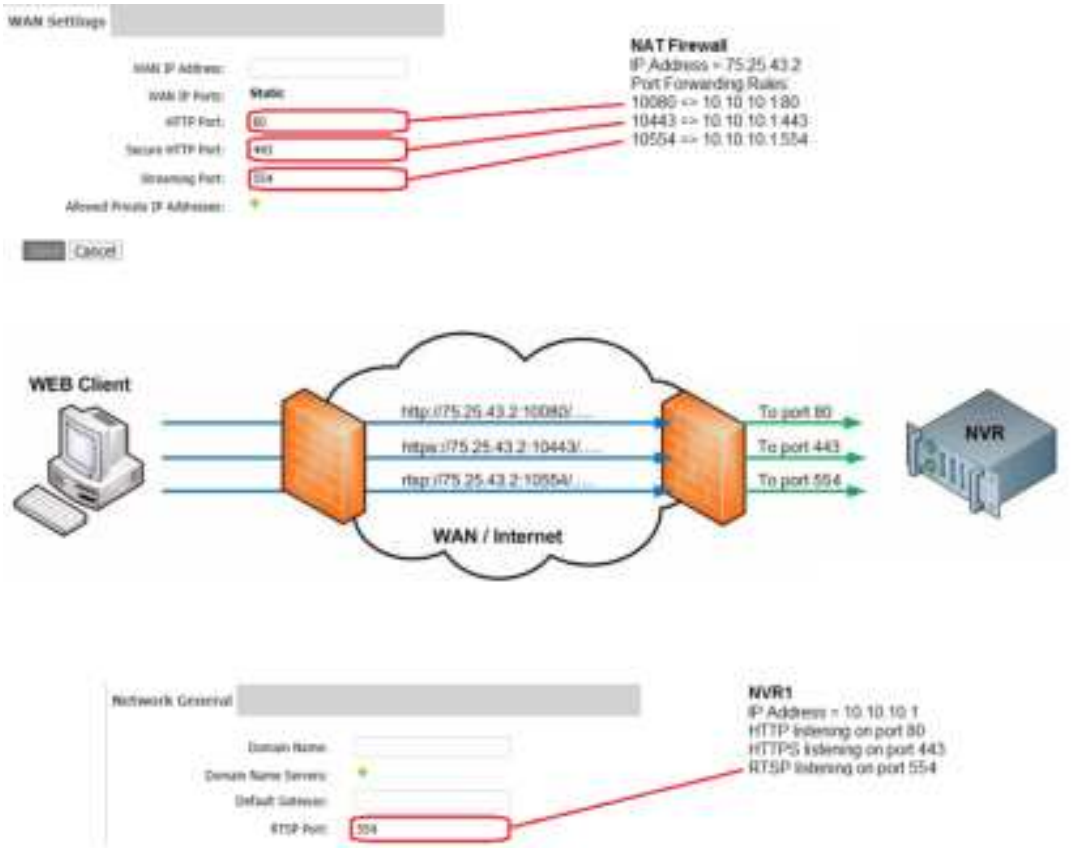
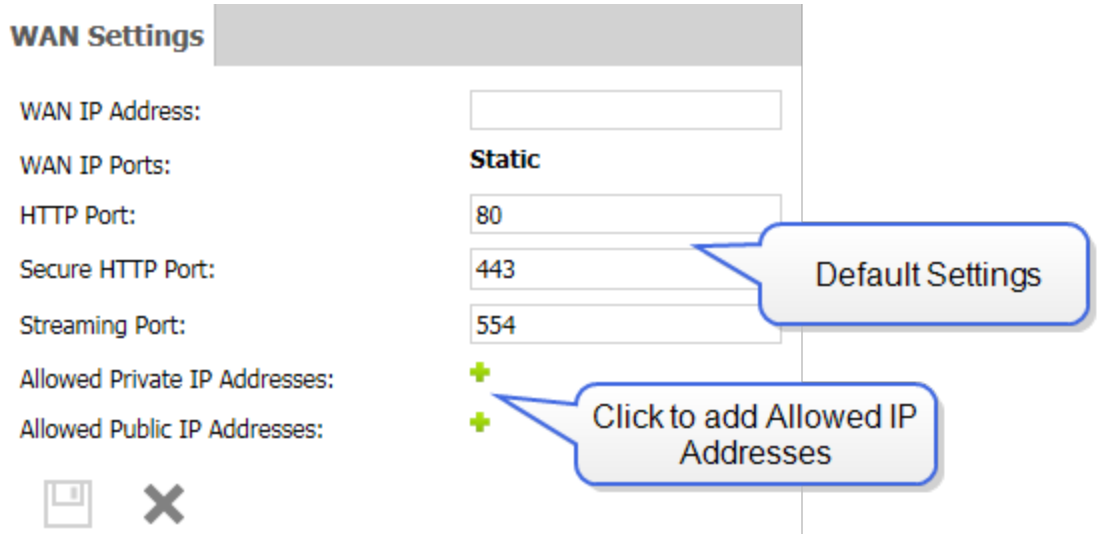


Figure 71 WAN Settings Page



WAN IP Address

Under the WAN Settings you can edit the WAN IP Address.

Procedure 226
Editing the WAN IP Address

Step	Action
1	Select **Network**.
2	Select **WAN Settings**.
	The WAN settings page opens.
3	To edit the **WAN IP Address** select the current value. Update the WAN IP Address as required.
4	Click

- End -

HTTP Port

This is the port number used to identify this NVR if more than one NVR is behind the NAT firewall.

In the HTTP address typed by the user when accessing an NVR, a port number can be specified (for example, http://70.30.22.81:80. Port 80 is normally assumed by default. However, if two NVRs are behind the same NAT firewall, they are both exposed as the same public address, so the only way to distinguish between them is by port forwarding rules at the firewall level. This means that both NVRs will still listen on port 80 for HTTP requests but that publicly NVR1 might be contactable as http://70.30.22.81:80, while NVR2 is contactable as http://70.30.22.81:10080. The firewall is configured to accept NVR2 requests at http://70.30.22.81:10080 and forward them to http://<NVR2 private IP>:80.

This field must be set in scenarios where multiple NVRs are situated behind the same NAT firewall. In this example, this field on NVR2 must be set to 10080.

Note:
If Failover functionality is active the Failover HTTP Port will be displayed for your information. It cannot be edited.

Procedure 227
Editing the HTTP Port

Step	Action
1	Select **Network**.
2	Select **WAN Settings**. The WAN settings page opens.
3	To edit the **HTTP Port** select the current value. Update the HTTP Port as required.
4	Click  **Note:** The default HTTP Port value is **80**.

- End -

Secure HTTP Port

This is the port number used to identify this NVR if more than one NVR is behind the NAT firewall, and a secure connection (https) is being made.

If an HTTPS address is being used to access an NVR, a port number can be specified (for example, https://70.30.22.81:443. Port 443 is normally assumed by default. However, if two NVRs are behind the same NAT firewall, they are both exposed as the same public address, so the only way to distinguish between them is by port forwarding rules at the firewall level. This means that both NVRs will still listen on port 443 for HTTPS requests but that publicly NVR1 might be contactable as https://70.30.22.81:443, while NVR2 is contactable as https://70.30.22.81:100443. The firewall is configured to accept NVR2 requests at https://70.30.22.81:100443 and forward them to https://<NVR2 private IP>:443.

This field must be set in scenarios where multiple NVRs are situated behind the same NAT firewall. In this example, this field on NVR2 must be set to 10443.

Procedure 228
Editing the Secure HTTP Port

Step	Action
1	Select **Network**.
2	Select **WAN Settings**. The WAN settings page opens.
3	To edit the **Secure HTTP Port** select the current value. Update the Secure HTTP Port as required.
4	Click  **Note:** The default HTTP Port value is **443**.

- End -

Streaming Configured Port

This is the port number used for the real time streaming protocol (RTSP) connection to this NVR if more than one NVR is behind the NAT firewall, when video is being streamed to a client programmatically via RTSP.

Port 554 is the default port for RTSP connection. However, if two NVRs are behind the same NAT firewall, they are both exposed as the same public address, so the only way to distinguish between them is by setting up port forwarding rules at the firewall level. This means that both NVRs listen on port 554 for HTTPS requests but that publicly NVR1 might be contactable as https://70.30.22.81:554, while NVR2 is contactable as https://70.30.22.81:100554. The firewall is configured to accept NVR2 requests at https://70.30.22.81:100554 and forward them to https://<NVR2 private IP>:554.

This field must be set in scenarios where multiple NVRs are situated behind the same NAT firewall. In this example, this field on NVR2 must be set to 10554.

Note:
If Failover functionality is active the Failover Streaming Port will be displayed for your information. It cannot be edited.

Procedure 229
Editing the Streaming Configured Port

Step	Action
1	Select **Network**.
2	Select **WAN Settings**. The WAN settings page opens.
3	To edit the **Streaming Port** select the current value. Update the Streaming Port as required.
4	Click  **Note:** The default HTTP Port value is **554**.

- End -

Allowed IP Addresses

Allowed Private and Public IP Addresses

These are the private IP addresses that are permitted for use with the VideoEdge. A public IP address is one that is not in the following ranges:

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

You can add a maximum of 20 Allowed IP Addresses to the VideoEdge.

Procedure 230
Adding allowed IP addresses

Step	Action
1	Select **Network**.
2	Select **WAN Settings**. The WAN Settings page opens.
3	Add an IP Address to the **Allowed Private IP Addresses** list. Or Add an IP address to the **Allowed Public IP Addresses** list. **Note:** The procedure is the same for public and private IP addresses. Select the + icon beside the option that you require. a Click + The IP Address and Subnet Mask text boxes display. b Enter the IP address in the **IP Address** field. c Enter the subnet mask in the **Subnet Mask** field. **Note:** To add additional IP addresses, repeat steps a - c. You can add up to 20 IP addresses.
4	Click 

- End -

Secure Connection

From the Secure Connection page, you can enable or disable victor Secure Connection (vSC) software for VideoEdge 5.2.2.

This solution provides a secure communication path between a victor Security System Server on a corporate network and a VideoEdge NVR on a remote network. The vSC solution resides between the victor Application server and the VideoEdge NVR. To facilitate secure communication, the vSC agent running on the VideoEdge device must be configured on this page

For more information about configuring vSC , refer to the *victor Secure Connection User Guide*.

Procedure 231
Enabling victor Secure Connection software in Standard Provisioning Mode

Step	Action
1	Select **Network**.
2	Select **Secure Connection**.
3	Click **Enabled**.
4	Select **Standard** from the **Provisioning Mode** list.
5	Enter the **Activation URL**.
6	Enter the **Password key**.
7	Click 

- End -

Procedure 232
Enabling victor Secure Connection software in Advanced Provisioning Mode

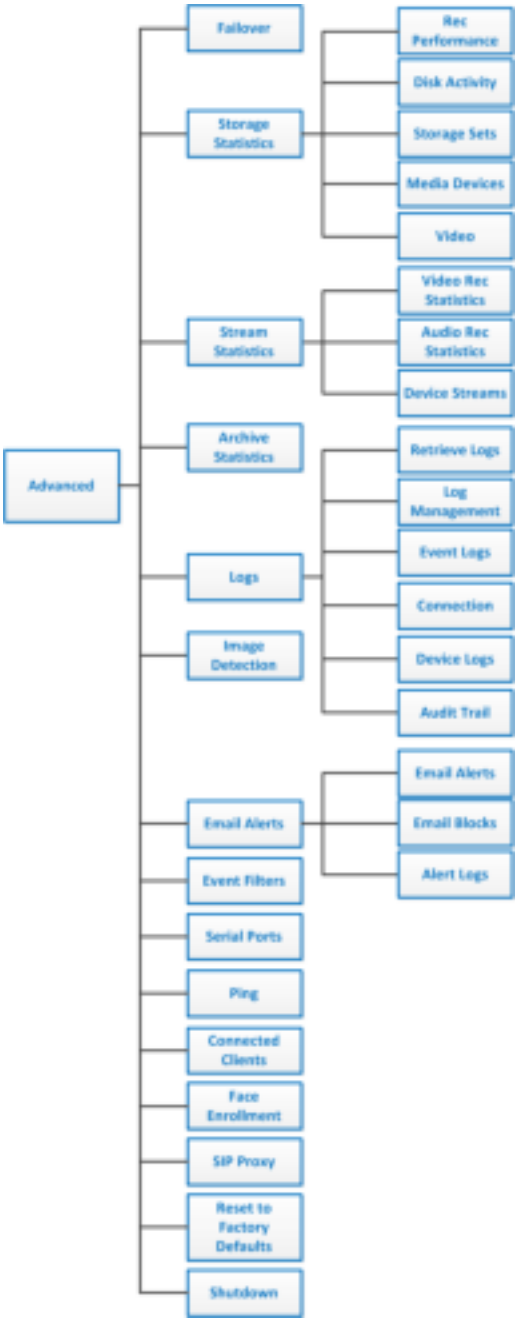
Step	Action
1	Select **Network**.
2	Select **Secure Connection**.
3	Click **Enabled**.
4	Select **Advanced** from the **Provisioning Mode** list.
5	Enter the **Gateway URL**.
6	Enter the **Gateway SSH Port**.
7	Click 

- End -

Advanced Menu Overview

The **Advanced** Menu allows you to configure/view the NVR's advanced system settings and information including Failover, storage, statistics, logs, Dark Image Detection, email alerts, serial ports, connected clients, reset to factory defaults and shutdown options.

Figure 72 Advanced Menu Map



- **Failover** - From here you can view the Failover Events report.
- **Storage Statistics** - From here you can view statistics relating to storage.
- **Stream Statistics** - From here you can view statistics relating to recorded video and audio streams.
- **Archive Statistics** - From here you can view statistics relating to archiving.
- **Logs** - From here you can generate log files for use by American Dynamics Technical Support.
- **Dark Image Detection** - From here you can enable dark image detection and apply a darkness threshold.
- **Email Alerts** - From here you can enable and configure email alerts.
- **Event Filters** - From here you can enable and configure event filters.
- **Serial Ports** - From here you can configure the NVR's serial ports.
- **Ping** - From here you can ping devices on the NVRs network for diagnostic purposes.
- **Connected Clients**- From here you can view a list of all clients which have an active connection with the NVR.
- **Face Enrollment** - From here you can add personnel entries to the facial enrollment database.
- **Reset to Factory Defaults** - From here you can reset the NVR's settings to the factory defaults. Options are provided to erase all media, maintain all media or re index all media.
- **Shutdown** - From here you can stop or restart NVR services, victor Web services, web videoserver services, or Support services. You can also reboot the NVR, enable Lockdown, or shutdown the NVR.

Failover Events Report

The occurrences and timing of Failover events can be queried using the Failover Events page on either a primary or secondary NVR.

Note:
Times are displayed in UTC unless you select the **Use Local Time** checkbox.

Procedure 233
Displaying Failover Events

Step	Action
1	Select **Advanced** from the main menu.
2	Select **Failover**. The Failover Events page opens.
3	Select the Virtual IP address you want to query from the **Virtual IP Address** dropdown list. **Note:** To query all virtual IP addresses which have been monitored by a secondary, select ANY from the dropdown list. When using the Failover Events feature on a Primary NVR only failover events relating to that primary will be displayed.
4	(Optional) Select the **Use Local Time** checkbox to display failover event times in local time.

5 Select the **Start Date/Time** and the **End Date/Time** to search a time range for Failover Events. Select the current value and update the date and time as required. Enter the date and time in the field in the following format; **YYYY/MM/DD Hours:Minutes:Seconds**, for example 2013/04/01 12:30:30.

Or

a Click on the current value.
The Calendar opens

b Select the date from the calendar.

c Use the sliders to adjust the time.

Note:
Time must be entered in 24 hour format.

d Click **Done**.

6 Click **Get Failover Events**.

All Failover Events within the configured time range display in the table

- End -

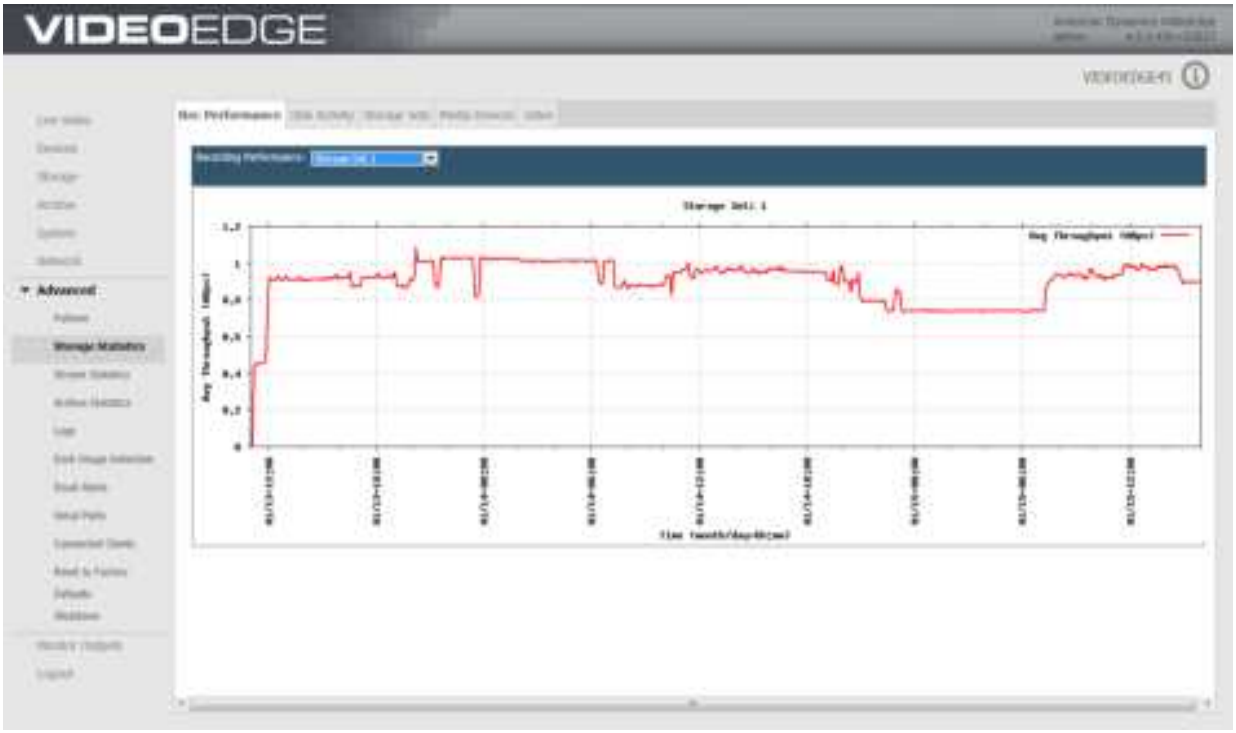
Storage Statistics

The Storage Statistics menu item allows you to view statistical information for Recording Performance, Disk Activity, Storage Sets, Media Devices and Video.

Recording Performance

The Recording Performance tab contains a graph displaying the average throughput over time for a selected storage set.

Figure 73 Recording Performance tab



Procedure 234
Viewing the Recording Performance Statistics

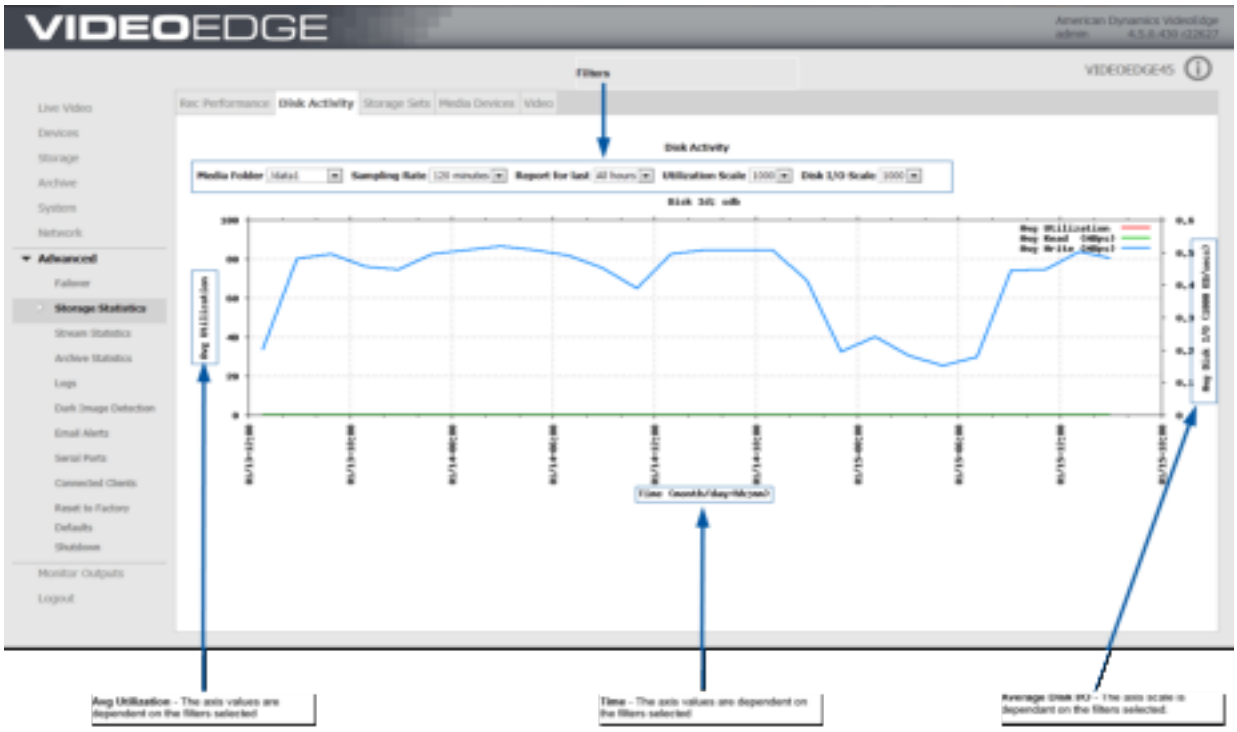
Step	Action
1	Select **Advanced** from the main menu.
2	Select **Storage Statistics**. The Rec Performance tab opens.
3	Select the storage set you want to view the recording performance for from the **Recording Performance** dropdown list. The graph updates displaying details for the selected storage set.

- End -

Disk Activity

The Disk Activity tab contains a graph outlining the disk activity for a specified media folder over a specified period of time. The graph can be customized by selecting the required filters. There are three values the graph depicts. The Average Utilization (red), the Average Read (green) and the Average Write (blue) over the time period selected.

Figure 74 Disk Activity Statistics tab



Procedure 235
Filtering the Disk Activity Graph

Step	Action
1	Select **Advanced** from the main menu.
2	Select **Storage Statistics**. The Rec Performance tab opens.
3	Select the **Disk Activity** tab.
4	Select the **Media Folder** you want the graph to display disk activity for from the dropdown.
5	Select the required **Sampling Rate** from the dropdown. You can select ranges between 1 minute and 120 minutes.
6	Choose the number of hours you want the graph to display disk activity for. Select this from the **Report for last** dropdown.
7	Select the **Utilization Scale** from the dropdown.
8	Select the **Disk I/O Scale** from the dropdown. The graph adjusts to display the disk activity as per the filters selected.

- End -

Storage Set Statistics

The Storage Set tab contains statistics for the total amount of storage available in each storage set. This is the combined storage available from all storage devices assigned to the storage set and does not contain information on individual device statistics. The storage set section also contains statistics for each camera assigned to each storage set.

Figure 75 Storage Statistics tab

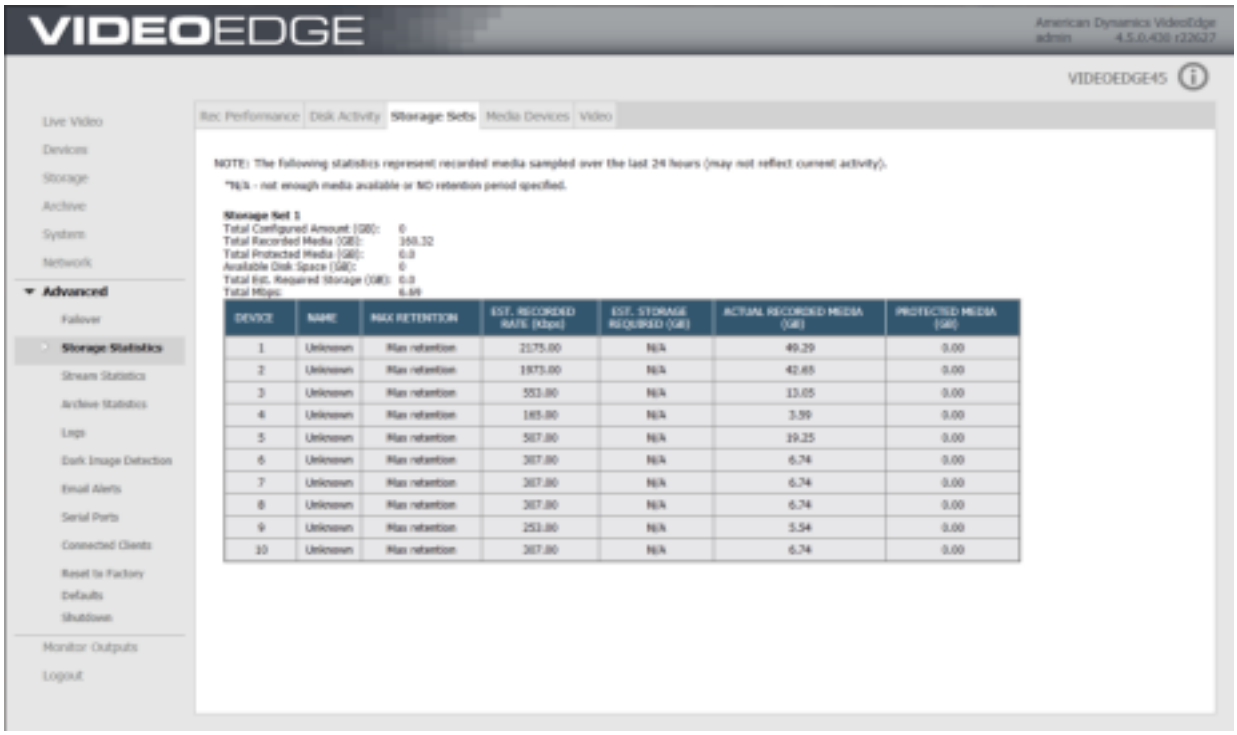


Table 16 Storage Set Statistics

Field		Description
Storage	Storage Total Configured Amount (GB)	Total configured amount of storage that will be used in this storage set.
	Total Recorded Media (GB)	Current total amount of recorded media in this storage set.
	Total Protected Media (GB)	Current total amount of protected media in this storage set.
	Available Disk Space (GB)	Total available disk space in this storage set.
	Total Est. Required Storage (GB)	If a retention period is defined on any camera this will show the total required storage needed to support those retention values, otherwise 0.0.
	Total Mbps	Current calculated Mbps for this storage set.

Field		Description
Device	Device	Device Input number.
	Name	Device Name
	Max Retention	Current configured retention period.
	Est. Record Rate (Kbps)	Current Kbps over last 24 hour period (if less than 24 hours will display N/A)
	Est. Storage Required (GB)	If a retention period is specified, this will indicate the required storage needed to support that retention period.
	Actual Recorded Media (GB)	Actual amount of recorded media for this camera in this storage set.
	Protected Media (GB)	Amount of current protected media for this camera in this storage set.

Note:
If a camera has stored media in a storage set but has now been assigned to another or has been deleted, the camera number will be displayed followed by **. This indicates the camera is not currently configured in this storage set. The Max Retention, Recorded Rate (Kbps) and Est. Storage Required (GB) will display as **Unknown**. The Actual Recorded Media (GB) and Protected Media (GB) will display their values.

Media Device Statistics

The Devices tab contains storage statistics per individual storage device.

Figure 76 Storage Statistics per Media Device

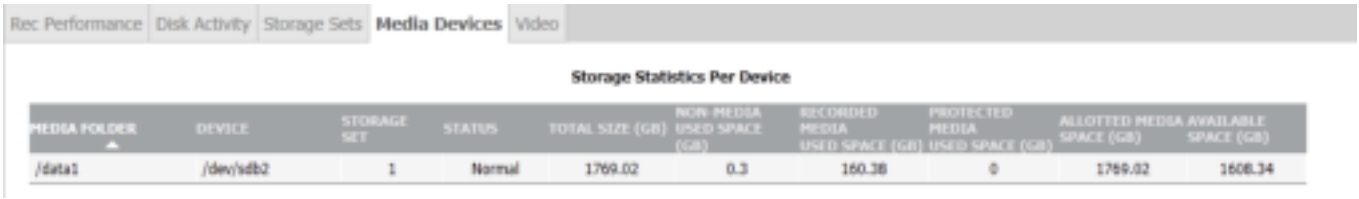


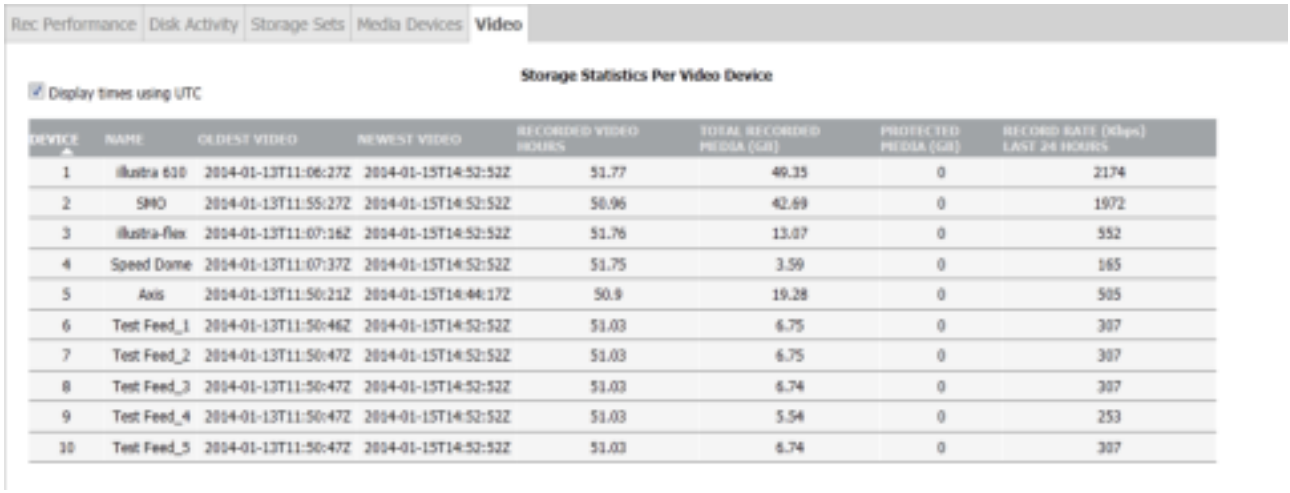
Table 17 Storage Device Statistics

Field	Description
Media Folder	Name of the media folder used by storage.
Device	Associated device on which this media folder is located.
Storage Set	Storage set this media folder is assigned to.
Status	Current Status of this folder (Normal, Degraded and so on).
Total Size (GB)	Total size of this device.
Non-Media Used Space (GB)	Total amount of space used by non NVR media files (if any) on this device.
Recorded Media Used Space (GB)	Total amount of space used for NVR recorded media at this time.
Protected Media Used Space (GB)	Total amount of space used for protected media on this device.
Allotted Media Space (GB)	Configured amount to use for storage on this device.
Available Space (GB)	Current total available unused space on this device.

Storage Statistics per Video Device

The Video tab details the storage statistics for each camera.

Figure 77 Storage Statistics per Video Device



DEVICE	NAME	OLDEST VIDEO	NEWEST VIDEO	RECORDED VIDEO HOURS	TOTAL RECORDED MEDIA (GB)	PROTECTED MEDIA (GB)	RECORD RATE (Kbps) LAST 24 HOURS
1	illustra 610	2014-01-13T11:06:27Z	2014-01-15T14:52:52Z	51.77	49.35	0	2174
2	SMO	2014-01-13T11:55:27Z	2014-01-15T14:52:52Z	50.96	42.69	0	1972
3	illustra-flex	2014-01-13T11:07:16Z	2014-01-15T14:52:52Z	51.76	13.07	0	552
4	Speed Dome	2014-01-13T11:07:37Z	2014-01-15T14:52:52Z	51.75	3.59	0	165
5	Axis	2014-01-13T11:50:21Z	2014-01-15T14:44:17Z	50.9	19.28	0	505
6	Test Feed_1	2014-01-13T11:50:46Z	2014-01-15T14:52:52Z	51.03	6.75	0	307
7	Test Feed_2	2014-01-13T11:50:47Z	2014-01-15T14:52:52Z	51.03	6.75	0	307
8	Test Feed_3	2014-01-13T11:50:47Z	2014-01-15T14:52:52Z	51.03	6.74	0	307
9	Test Feed_4	2014-01-13T11:50:47Z	2014-01-15T14:52:52Z	51.03	5.54	0	253
10	Test Feed_5	2014-01-13T11:50:47Z	2014-01-15T14:52:52Z	51.03	6.74	0	307

Table 18 Video Device Storage Statistics

Field	Description
Device	Input number.
Name	Device Name.
Oldest Video	Time of oldest video for this camera across all storage sets.
Newest Video	Time of newest video for this camera across all storage sets.
Recorded Video Hours	Total number of recorded video hours for this camera across all storage sets.
Total Recorded Media (GB)	Total amount of recorded media for this camera across all storage sets.
Protected Media (GB)	Total amount of protected media for this camera across all storage sets.
Record Rate (Kbps) Last 24 Hours	Record rate for this camera over the last 24 hours (N/A -if less than 24 hours of data).

Procedure 236
Viewing Storage Statistics

Step	Action
1	Select **Advanced** from the main menu.
2	To view storage set statistics select **Storage Sets** tab. Or To view device statistics select **Media Device** tab. Or To view camera statistics select **Video** tab. The required statistics are displayed.

- End -

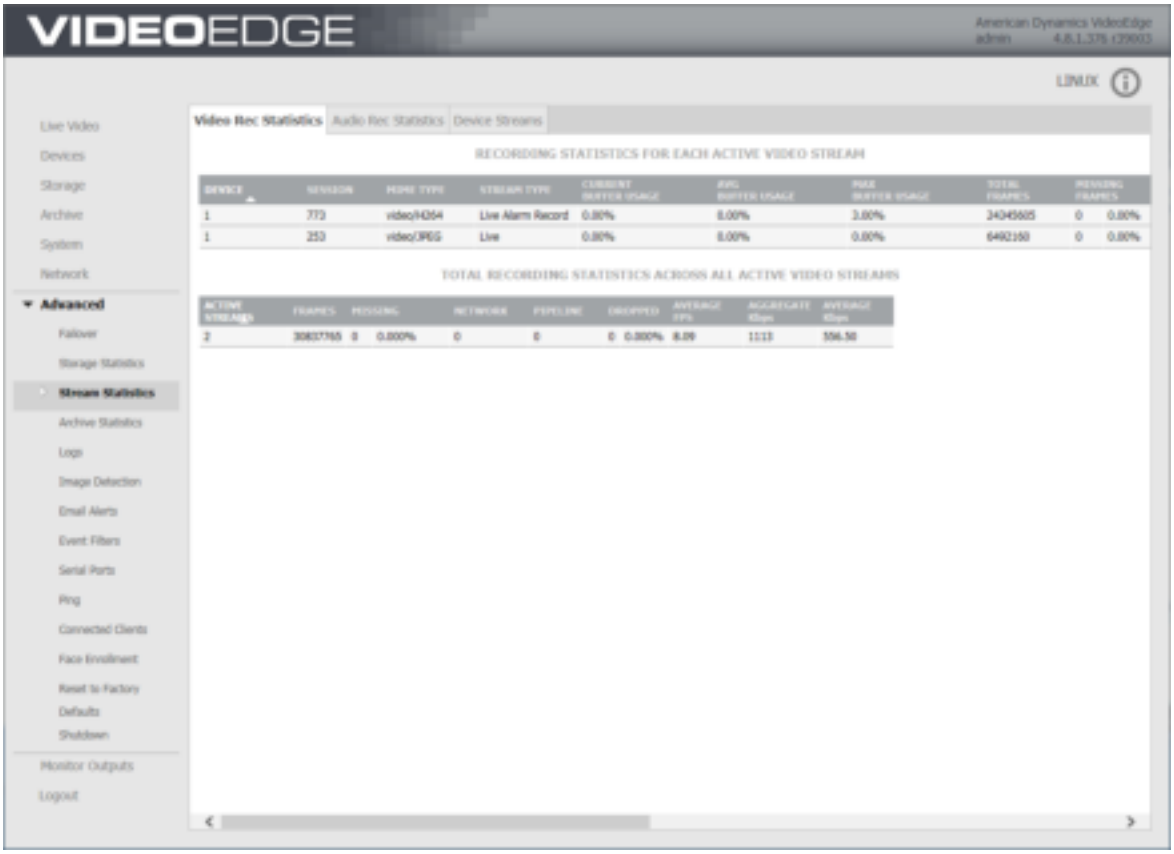
Stream Statistics

You can use the Stream Statistics menu item to view statistics on video recording, audio recording and an overview of streaming settings on each device.

Video and Audio Recording Statistics

The Video and Audio Recording Statistics tabs display recording statistics for each device configured on the NVR. There is also a Totals summary table displaying recording statistics for the total of all devices on the NVR.

Figure 78 Recording Statistics Page



Device Streams

The Device Streams page provides a read-only summary of the configured streams for any cameras that are connected to the VideoEdge.

Figure 79 Device Streams Page

Table 19 Recording Statistics

Field	Description
Device	Device input number.
Session	Current active media database session ID associated with stream type for this camera (Note: there will be multiple sessions for the same camera depending on the stream types).
MIME Type	Provided details on codec of data recorded in session.
Stream Type	Indicates what type of stream recorded for this session, i.e. live, alarm, and or record.
Current Buffer Usage	Usage Current percent used of the internal frame buffer (will be 0% if no buffering is occurring, i.e. frames are being written to the disk as they are received).
Avg Buffer Usage	Average percent used of the internal frame buffer.
Max Buffer Usage	Maximum percent used of the internal frame buffer.
Total Frames/Packets	Total number of frames recorded for video devices or total number of packets recorded for audio devices in the session.
Missing Frames/Packets	Total number of missing frames for video devices or total number of missing packets for audio devices in the session/percent missing.
Dropped Frames/Packets	Total number of dropped frames for video devices or total number of dropped packets for audio devices in the session (frames/packets inserted into buffer, but the frames/packets were removed before being written due to buffer overflow).
FPS/PPS	Actual FPS recorded for this video device for this session or actual PPS recorded for this audio device for this session.

Field	Description
Kbps	Calculated Kbps of this device for this session.
Avg Queue Latency	Average time between when frame is received and when inserted into queue (seconds).
Avg Disk Latency	Average time from queue insertion to disk write (seconds).
Max Disk Latency	Maximum time from queue insertion to disk write (seconds).
Last Add	Time of last added frame in this session.
Last Drop or Miss	Time of last frame dropped/missed if applicable (N/A indicates no frame dropped/missed).

Table 20 Total Recording Statistics

Field	Description
Active Streams	Current total number of active streams.
Frames	Total number of frames for all devices.
Missing	Total number of missing frames across all devices.
Network	Total number of frames dropped between devices and NVR (lost over network).
Pipeline	Total number of frames dropped from buffer (inserted into buffer but not written).
Dropped	Total number of dropped frames across all devices/percent dropped of total frames.
Average FPS	Average FPS of all devices.
Aggregate Kbps	Aggregate Kbps across all devices.
Average Kbps	Average Kbps across all devices.

Table 21 Configured Streams on Each Device

Field	Description	
Device name	Device name as given when adding the device to VideoEdge.	
Device ID	Device slot number.	
Stream ID	Device stream number.	
Purpose	Live	Indicates that this stream will be used for live streaming.
	Preferred	Indicates that this stream is the preferred stream for the device.
	Alarm	Indicates that this stream will be used for any alarms that are recorded.
	Record	Indicates that this stream will be used for non-alarm recording.
Codec	The camera codec.	
FPS	The camera FPS.	
Resolution	The camera resolution	
Analytics	Indicates if analytics are set on the device.	

Field	Description
	The analytic options are:  Analytics Off  Motion Detection  Video Intelligence (This encompasses object detection, direction, linger, enter, exit and abandoned/removed).  Edge Based.  Face Recognition (This includes Face Search Alert and Face Verification).
Type	This field shows how the camera is added to VideoEdge: manually or by auto-configuration streams.

Procedure 237
Viewing the Video and Audio Recording Statistics

Step	Action
1	Select **Advanced** from the main menu.
2	Select **Stream Statistics**. The Rec Performance page opens.
3	Select the **Video Rec Statistics** tab. The Video Recording Statistics page opens. Or Select the **Audio Rec Statistics** tab. The Audio Recording Statistics page opens. Or Select the **Device Streams** tab. The Device Streams page opens.
4	Details of these statistics are outlined in the Recording Statistics table or the Total Recording Statistics table.

- End -

Archive Statistics

You can use the Archiving Statistics menu item to view graphical representation of the Total throughput for archiving for your NVR and the Throughput per archive destination.

Procedure 238
Viewing Archiving Statistics

Step	Action
1	Select **Advanced**.
2	Select **Archive Statistics**. The Archive Statistics page opens.
3	You can display/hide the following items on the graphs using checkboxes. a Points b Lines c Write throughput d Read throughput e Write rate per archive f Read rate per archive
4	To zoom in, click and drag on the area you want to enlarge.
5	To zoom out, click 

- End -

Logs

The NVR tracks important types of system events. You can view logs of the following:

- Administrative changes
- Camera alerts
- Changes to cameras
- System events (used by American Dynamics technical support)

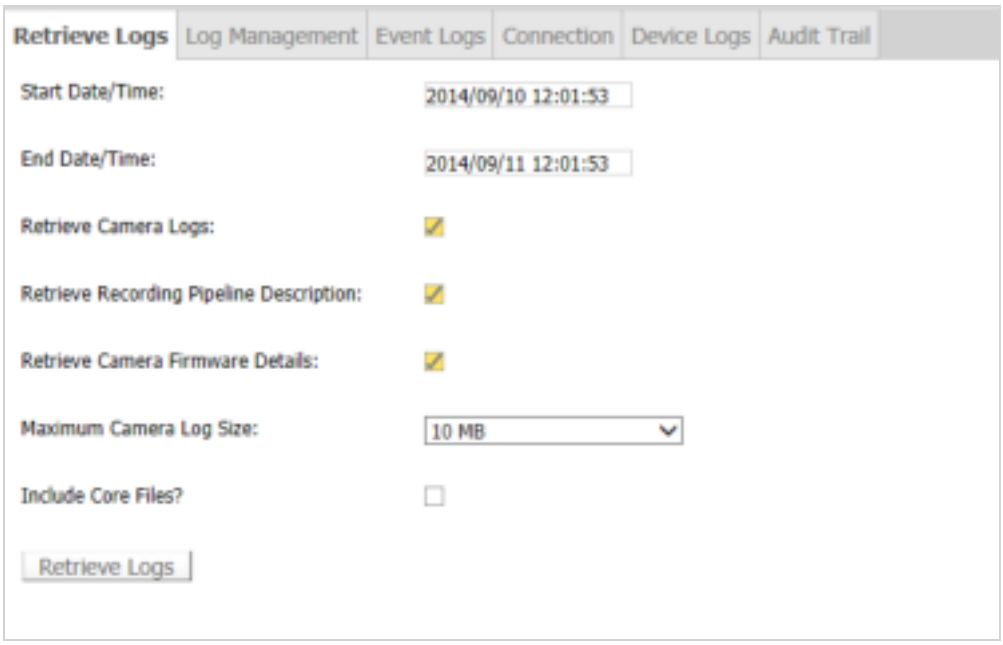
The Logs page provides access to the NVRs log settings, this allows you to retrieve logs, edit the FTP Log Management settings, filter searches for Events Logs, view Camera Connection Errors, Camera Logs and an Audit Trail.

Retrieving Logs

The Retrieve Logs page provides you the ability to customize the search criteria for retrieving log files. The editable criteria includes a date and time range, selection options for retrieving camera logs, recording pipeline descriptions, camera firmware details and core files. Core files (also known as memory dump or system dump files) record the current state of memory. Technical Support may ask you to provide these files. A dropdown also provides selectable maximum camera log sizes of; 1Mb, 5Mb, 10Mb, 25Mb and 50Mb.

The retrieved log file is in zipped format, it can either be opened as a temporary folder or saved local using the Windows file download window or other OS equivalent.

Figure 80 Retrieve Logs Page



Procedure 239
Retrieving Logs

Step	Action
1	Select **Advanced**.
2	Select **Logs**. The Retrieve Logs page opens.
3	Type the Start Date/Time in the **Start Date/Time** text box. **Note:** Enter in the following format; Year/Month/Date Hours:Minutes:Seconds. For example for 1pm on 21st January 2012 would be **2012/01/21 13:00:00**. Or Select the Start Date/Time field and a calendar opens. You can use the calendar to select the date and use the sliders to adjust the time.
4	Type the End Date/Time in the **End Date/Time** text box in the same format described in step 3.
5	Select/deselect the **Retrieve Camera Logs** check box as required.
6	Select/deselect the **Retrieve Recording Pipeline Description** checkbox as required.
7	Select/deselect the **Retrieve Camera Firmware details** checkbox as required.
8	Using the **Maximum Camera Log Size** dropdown select the maximum camera log size.
9	Select/deselect the **Include Core Files** checkbox as required.
10	Click **Retrieve Logs**.
11	When the File Download window displays Click **Open** or **Save**. The Logs folder is now ready to be viewed.

- End -

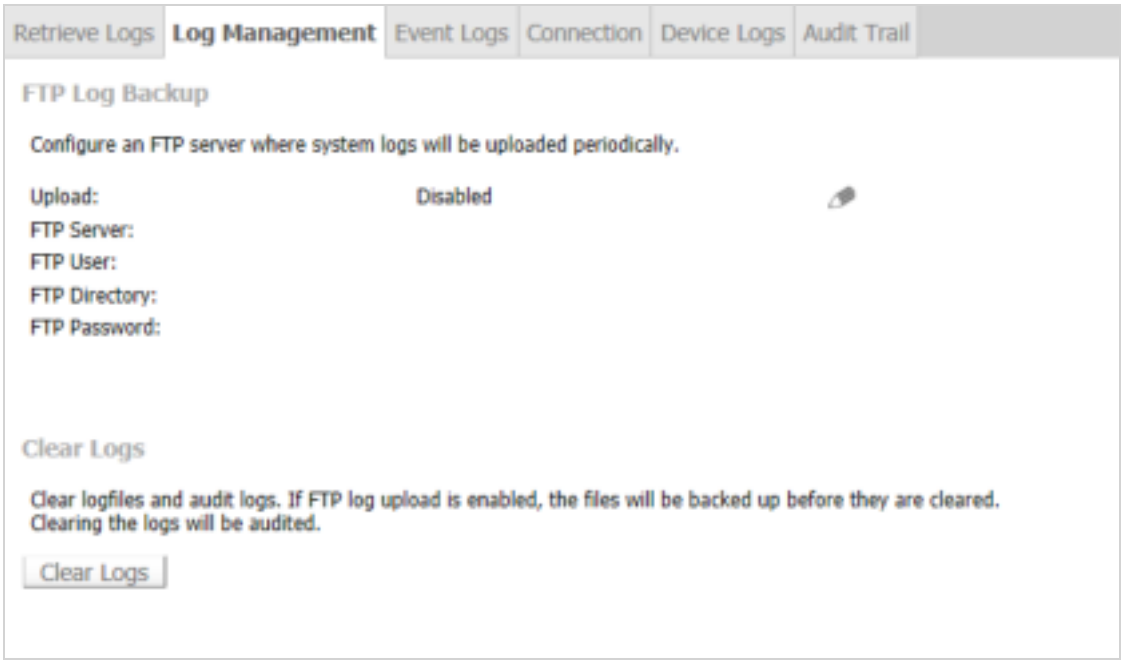
FTP Log Management

The Log Management page allows you to configure FTP server settings where system logs will be uploaded periodically. The Event Log is rotated (all entries are cleared) when it is full. To preserve the Events Log this function should be configured and enabled.

Note:
Only syslog files are uploaded when using this feature.

The Log Management page allows you to input the FTP server IP Address, FTP Username, remote FTP Directory and FTP Password.

Figure 81 Log Management Page



Procedure 240
Editing Settings for the Log FTP Server

Step	Action
1	Select **Advanced**.
2	Select **Logs**.
3	Select the **Log Management** tab. The Log Management page opens.
4	Select
5	Select the **Enabled** option button to enable Event Log upload to the FTP Server.
6	Enter the IP Address in the **FTP Server** field.
7	Enter the username in the **FTP User** field.
8	Enter the directory in the **FTP Directory** field.
9	Enter the password in the **FTP Password** field.
10	Enter the password again in the **Confirm Password** field.
11	Click

Note:
When FTP Log upload is enabled, a **Test Upload** button displays. This button can be used to verify the FTP server settings. A successful upload test will create a test file on the specified location of the FTP Server.

- End -

Clearing System Logs

If FTP log upload is enabled, system files will be backed up before they are cleared. You can use the Clear Logs button to manually clear the system log files. Using this function will appear in the NVR Audit Trail.

Procedure 241
Clearing System Logs

Step	Action
1	Select **Advanced**.
2	Select **Logs**.
3	Select the **Log Management** tab. The Log Management page opens.
4	Click **Clear Logs**.

- End -

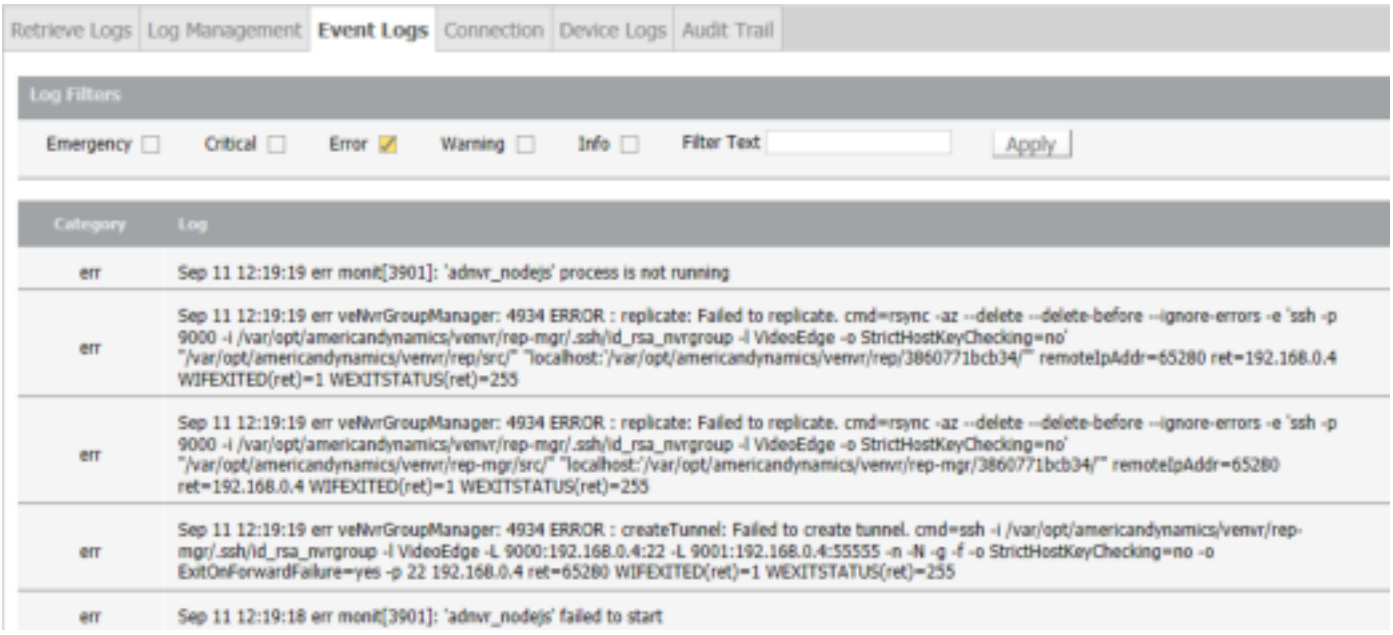
Event Logs

The Event Logs page is used primarily by American Dynamics technical support for troubleshooting. The Event Log shows informational and error-related events that have occurred on the NVR system.

When the Event Log is full, the file is rotated (all entries are cleared) and a new Event Log is started.

The Event Log page provides a filter feature. You can filter by the following criteria; Emergency, Critical, Error, Warning, Info and Filter Text.

Figure 82 Event Logs Page



Procedure 242
Viewing Event Logs

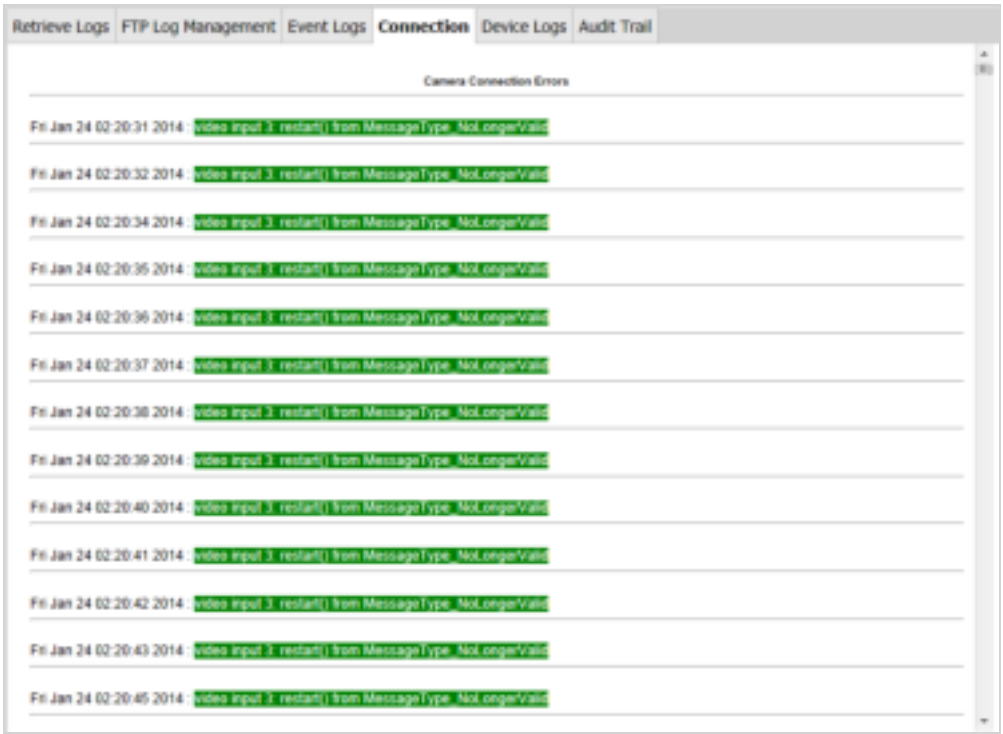
Step	Action
1	Select **Advanced**.
2	Select **Logs**.
3	Select the **Event Logs** tab.
	The Event Logs page opens.
4	To include emergency event logs, select the **Emergency** checkbox.
5	To include critical event logs, select the **Critical** checkbox.
6	To include error event logs, select the **Error** checkbox.
7	To include warning event logs, select the **Warning** checkbox.
8	To include info event logs, select the **Info** checkbox.
9	To include specific filter text, enter the desired filter text in the **Filter text** textbox.
10	Click **Apply**.

- End -

Camera Connection Errors

The Connection page displays the Camera Connection Errors that have occurred.

Figure 83 Connection Page



Procedure 243
Viewing Camera Connection Errors

Step	Action
1	Select **Advanced**.
2	Select **Logs**.
3	Select the **Connection** tab. You are prompted to enter your Username and Password.
4	Click **OK**. The Connection page opens.

- End -

Device Logs

The Device Logs page provides information on camera reboots, changes to camera recording status, and the use of the Pan-Tilt-Zoom (PTZ) and other controls.

Figure 84 Device Logs Page

Table 22 Device Logs Definitions

Column	Description
Date/Time	Displays the Date and Time that the camera reported a change.
Category	Lists the type of action or change that occurred.
Camera	Lists the camera number, name and IP Address.
Details	Displays the details of the action or change that occurred.
Operator	Displays the name of the user who initiated the action.
Client Machine	Lists the IP Address of the client machine from which the user-initiated action originated.

Procedure 244
Viewing the Camera Logs

Step	Action
1	Select **Advanced**.
2	Select **Logs**.
3	Select the **Device Logs** tab. The Device Logs page opens.

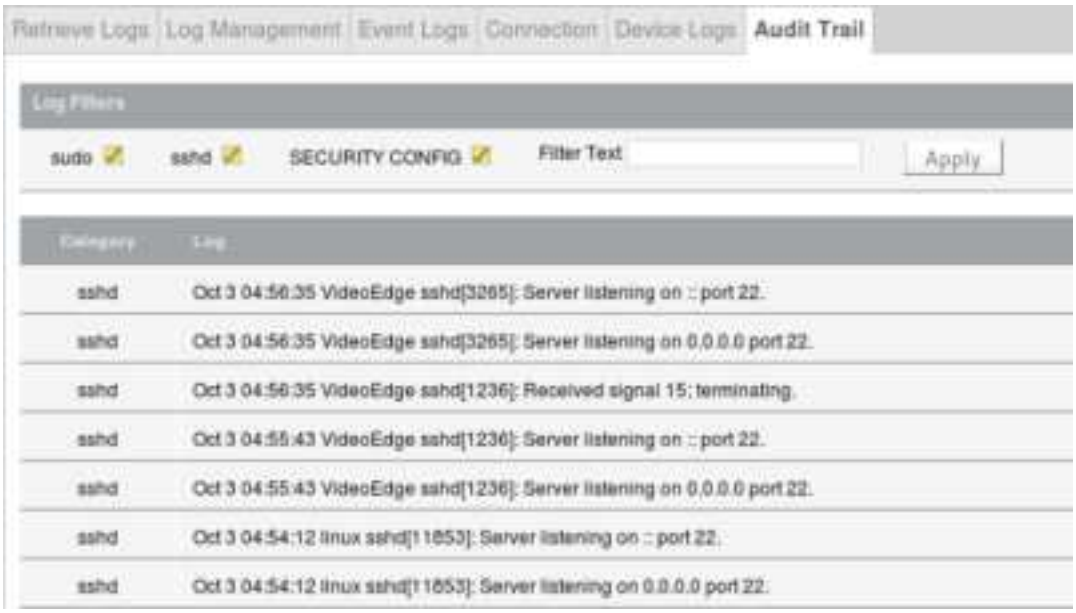
- End -

Audit Trail

The Audit Trail page displays a log of system changes which have been made by a privileged user. The system changes which are logged in the Audit Trail are:

1. System Date and Time
2. Software upgrade
3. FTP Log Management settings
4. User Login Passwords
5. Network Settings

Figure 85 Audit Trail Page



Procedure 245
Viewing the Audit Trail

Step	Action
1	Select **Advanced**.
2	Select **Logs**.
3	Select the **Audit Trail** tab.
	The Audit Trail page opens.
4	To include errors, select the **Error** checkbox.
5	To include alerts, select the **Alert** checkbox.
6	To include notice messages, select the **Notice** checkbox.
7	To include info messages, select the **Info** checkbox.
8	To include specific filter text, enter the desired filter text in the **Filter text** textbox.
9	Click **Apply**.

- End -

Image Detection

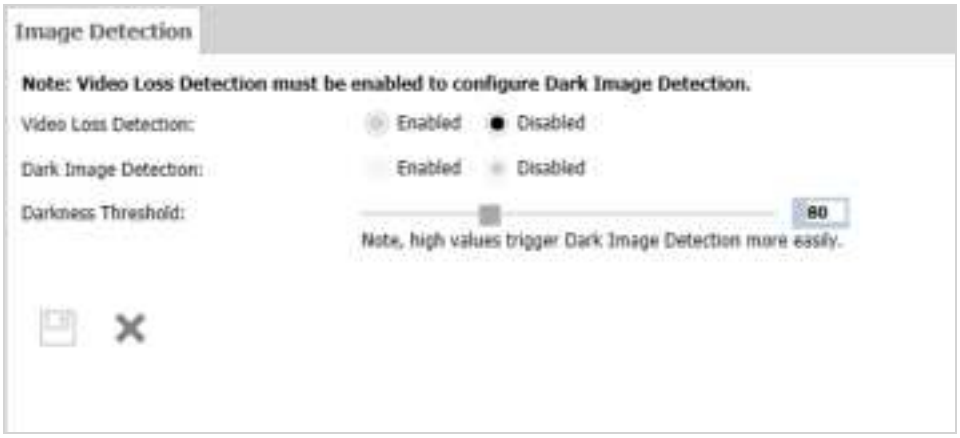
The NVR can perform an Image Detection test on every camera in the network. You can use this test to determine if the NVR has a camera that is recording a very dark, or potentially black video. The test runs for each camera once a minute, it counts the number of pixels with intensity values less than the Darkness threshold which is defined in the Dark Image Detection page. The Darkness threshold can be set from 1 (darkest) to 255 (brightest), with a default setting of 80.

For example, with a Darkness threshold setting of 80, a pixel with RGB values of 70, 70, 70 is considered dark, while a pixel with RGB values of 70, 70, 81 is not considered dark. If 90% of all pixels are dark (have intensities less than the threshold you have set), then a 'Video Loss' alert is activated.

You can also enable Camera Loss Detection. If the camera goes offline a 'Video Loss' alert is triggered.

In victor client use the Activity Log page or in the VideoEdge Client use the Event Viewer to see if any cameras have generated any 'Video Loss' alert events.

Figure 86 Image Detection Page



Enable Image Detection

Before Image Detection can be enabled you must enable the Camera Loss Detection option. When dark image detection occurs, a "Video Loss" alert is activated. Both camera loss detection and dark image detection alerts can be viewed in the victor client Activity List or via the Reports feature. In the VideoEdge client you can view video loss alerts via the Event Viewer.

Procedure 246
Enable Image Detection

Step	Action
1	Select **Advanced**.
2	Select **Image Detection**.
	The Image Detection page opens.
3	To enable Video Loss Detection, click the **Enabled** option button.
4	To enable Image Detection click the **Enabled** option button.
	The area behind the option buttons changes to yellow indicating a change has been made.
5	To edit the Darkness Threshold use the slider to select the **Darkness Threshold** value.

The slider color changes to yellow indicating a change has been made.

6 Click 

Confirmation messages display.

- End -

Enable/Disable Video Loss Detection

When video loss detection is enabled, a video loss alert is triggered when communication is lost between a camera and the NVR.

When video loss detection is disabled, a video loss alert will not be triggered and the Dark Image Detection feature cannot be enabled.

Procedure 247
Enabling/Disabling Video Loss Detection

Step	Action
1	Select **Advanced**.
2	Select **Image Detection**. The Image Detection page opens.
3	Click the **Enabled** option button to enable Video Loss Detection. Or Click the **Disabled** option button to disable Video Loss Detection The area behind the option buttons changes to yellow indicating a change has been made.
4	Click  A confirmation message displays.

- End -

Face Enrollment

The NVR when licensed can be used as a facial enrollment database for use with facial detection and recognition analytics. This allows the NVR to identify individuals who are uploaded to it's on board database in addition to performing simple face detection which does not require enrollment.

You can create/remove entries to the database using the Face Enrollment page. You can also replace images of entries in the enrollment database when required.

Procedure 248
Enrolling Personnel on the Face Enrollment Database

Step	Action
1	Select **Advanced** from the main menu.
2	Select **Face Enrollment**. The Face Enrollment page opens.
3	Click 
4	Enter the individuals **Name**.
5	Click Browse to search for Picture(s) of the individual to add to the database. **Note:** Up to 12 images can be uploaded for each entry in the face enrollment database. For best results, when selecting pictures for the database they should adhere to the following requirements - 1. Picture should be suitable illuminated 2. Individual pictured should not be smiling 3. The face of the individual pictured should be vertically-aligned and directly facing the camera 4. Multiple pictures should be enrolled for each individual, they should be taken in differing lighting, from differing angles, and on different days to improve recognition accuracy
6	Click  **Note:** Enrollment will fail if the portrait is rotated or if the overall quality is insufficient.

- End -

Procedure 249
Replacing Portrait Images for Entries in the Enrollment Database

Step	Action
1	Select **Advanced** from the main menu.
2	Select **Face Enrollment**. The Face Enrollment page opens.
3	Select the required personnel entry.
4	Click 

5 Click Browse to search for Picture(s) of the individual to add to the database.

Note:
Previously uploaded portraits will be replaced.

6 Click 

Note:
Enrollment will fail if the portrait is rotated or if the overall quality is insufficient.

- End -

Deleting Entries from the Enrollment Database

Entries which are no longer required for Face Recognition can be deleted from the enrollment database.

Caution

When an entry has been deleted from the enrollment database, it can no longer be searched for using victor unified client. If you re-enroll an entry you will be unable to use it for face recognition searches of time spans prior to the re-enrollment.

Procedure 250
Deleting Entries from the Enrollment Database

Step	Action
1	Select **Advanced** from the main menu.
2	Select **Face Enrollment**. The Face Enrollment page opens.
3	Select the required personnel entry/entries.
4	Click  A dialog box opens.
5	Click **OK**.

- End -

Email Alerts

The Email Alerts page consists of the Email Alerts page, the Email Blocks page and the Alert Logs page. Email Alerts can be setup in the NVR to send notifications to selected email addresses regarding several different categories.

The Email Blocks page is used to block specified email alerts being sent from specified devices.

The Alert Logs page is used to display all of the email alerts that have been transmitted.

Note:
In order to use the email notification feature, you must have the IP address of an SMTP switch or a mail server; ask your IT administrator for details.

Figure 87 Email Alerts Page

Table 23 Email Alerts List Summary Table

Field	Description
1. Alert Category	Displays the name of the alert type.
2. Recipient List	Displays any recipient email addresses associated with the alert.
3. Minimum Repetition Interval	The minimum time (in seconds) between sending repeat alert emails.
4. Return To Normal Interval	The time to wait before sending out the "return to normal" email. The alert itself may already have cleared.
5. Enabled	Displays "Yes" if the alert is enabled.
6. Edit	Select the edit icon to edit the alert settings.
7. Test	Select the "Test" button to send a test alert email to the assigned recipients.

Note:
Before you use the "Test" feature, you must complete the following tasks:

- Advance Preparation for Email Alerts
- Configuring the Outbound Mail Server
- Building the Recipient List
- Enabling and Disabling Email Alerts

Advance Preparation

Prior to configuring email alerts you must ensure that you have a valid Domain Name and Default Gateway configured in the network settings of the NVR network.

Procedure 251
Advance Preparation for Email Alerts

Step	Action
1	Select **Network**.
2	Select **General**. The Network General page opens.
3	To edit the **Domain Name** select the current value. Update the Domain Name as required. The field background changes to yellow indicating a change has been made.
4	To edit the **Default Gateway** select the current value. Update the Default Gateway as required. The field background changes to yellow indicating a change has been made.
5	Click  A validation message displays. **Note:** The NVR will send notifications to email addresses sharing its own domain. Additionally, it can send notifications to email addresses in other domains provided those domains' SMTP servers have allowed incoming emails from the NVR's domain. Owners of email addresses in other domains should contact their email administrator to ensure they will be able to receive alert notifications from the NVR's domain. The delivery of email notifications sent to email addresses provided by Internet Service Providers (ISPs, such as, Yahoo or Gmail) cannot be guaranteed because those ISPs have their own restrictions that may interfere.

- End -

Setting Up Email Alerts

To set up email notifications you are required to build the recipient list and enable the notifications each address on the recipient list is to receive.

Outbound Mail Server

To allow the Email Alerts functionality with the NVR, you must enter the outbound mail server's, IP address or hostname. In addition to the IP address/hostname the following options are also available for configuration:

- **Server requires authentication** - Select to enter the username and password required to authenticate the NVR with the mail server.
- **Encryption** - The SMTP connection between the NVR and the SMTP server can be encrypted using TLS or SSL.

Note:
The use of a hostname is mandatory when using TLS or SSL encryption. The hostname must match the entry in the CN (Common Name) field of the server's certificate.

- **Custom Sender** - Allows you to enter a custom sender's address when username authentication is required by the SMTP server. When not configured an automatically generated sender address will be used.

In VideoEdge 4.9+, you can configure a secondary outbound email server.

Procedure 252
Configuring the Outbound Mail Server

Step	Action
1	Select **Advanced**.
2	Select **Email Alerts**. The Email Alerts page opens.
3	Click  next to the Outbound mail server field.
4	Enter the Outbound mail server **IP address or hostname** in the field.
5	(Optional) Select the **Server requires authentication** checkbox. The username and password fields display. a Enter your **username** in the field. b Enter your **password** in the field.
6	Select the required encryption type; **None**, **TLS** or **SSL**. **Note:** When the SSL option button is selected you must select the Server TCP port from the dropdown.
7	(Optional) Select the **Custom sender** checkbox. The Sender email address field displays. a Enter an **email address** in the field.
8	Click 

- End -

Alert Category	Description
Analog Handler Reboot	Sent when any device controller stops responding. The device handler will be automatically restarted to re-establish communication with the camera.

Alert Category	Description
Archive	Sent when the archive is unhealthy, the archive is falling behind, data deleted before being archived and when archive is nearing full
Audio Malfunction	Sent when audio malfunctions occur.
Blur Detection	Generated when a configured camera becomes out of focus.
Camera Dark Frame	Sent when the camera images cross a configured threshold of darkness. This alert indicates that the camera may be obscured.
Camera Processing Malfunction	Sent when a camera refuses to respond.
Camera Video Loss	Sent when the record pipeline detects that there is no video coming from the camera.
Device Not Recording	Generated when recording does not occur on one or more cameras.
Dry Contact	Sent when a dry contact is triggered.
Face Detection	Generated when a face is present in a camera's configured view.
Failover	Sent when a failover is detected. The IP address of the NVR which has failed will be included.
Log Storage Space Low	Sent when less than 5% of the log storage area is available.
Motion Detection	Generated by motion detection alerts. Does not include image attachments.
Security Alert	Sent when a user is temporarily and permanently locked out of their account.
Security Config Change	Sent if any security settings on the system are changed.
Storage	Transmitted when storage is not healthy.
Storage Activation	Generated when no storage can be activated.
Storage Config	Sent when storage configuration errors occur.
Storage Retention	Transmitted when storage capacity is almost reached.
System	All general system alerts not included in other categories.
System Reboot	Sent when the system is rebooted.
Text Stream	Sent when user defined Text Stream exception rules are met.
Video Intelligence	Generated by video intelligence alerts.

Building the Recipient List

The recipient list is made up of email addresses which will receive email alerts. The alerts that each address will receive is defined by the alert category associated with that address and whether or not that category has been

enabled.

Procedure 253
Building the Recipient List

Step	Action
1	Select **Advanced**.
2	Select **Email Alerts**. The Email Alerts page opens.
3	Click  The Add/Update Alert Recipient pop up displays.
4	Select the **New Recipient Email Address** option button.
5	Enter the recipient's email address in the field. Or If the user is already receiving notifications, you can choose the user's email address from the **Use Recipient Email address** dropdown menu.
6	Select the **Alert Categories** using the checkboxes.
7	Click 
8	Verify that the email address has been added to the recipient list for each alert category. You can check by viewing recipients for each alert category listed in the table on the Email Alerts page.
9	To send a test email to a recipient list, select the alert you want to test and click **Test**.
10	Once you have the email recipients configured, you need to enable alerts.

- End -

Enabling and Disabling Email Alerts

Once recipient addresses have been entered and alert categories assigned you can configure which email alerts should be enabled for each recipient.

Procedure 254
Enabling and Disabling Email Alerts

Step	Action
1	Select **Advanced**.
2	Select **Email Alerts**. The Email Alerts page opens.
3	Select the checkbox for each alert you want to enable from the **Alert Category** list.
4	Click  or 
5	After enabling email alerts, an email is sent to the selected recipients when the appropriate alert is triggered.

- End -

Disabling Email Alerts for a Camera

You can disable Email Alerts for a specific camera. This allows you to suppress email alerts from cameras which are known to be malfunctioning.

Caution

This procedure will disable the cameras ability to stream live video.

Attempting to modify some of the parameters of the camera such as Password Group or PTZ will not be possible when the camera is disabled.

Procedure 255
Disabling Email Alerts for a Camera

Step	Action
1	Select **Devices**.
2	Select **List**. The Video List page opens.
3	Click in the camera record of the camera you want to disable email alerts. The Function & Streams page opens.
4	Select the **General** tab. The General page opens.
5	Click the Camera **Video Disable** option button.
6	Click In the camera record on the Video List page the IP address indicates **DISABLED**.

- End -

Procedure 256
Re-enabling Email Alerts for a Camera

Step	Action
1	Select **Devices**.
2	Select **List**. The Video List page opens.
3	Click in the camera record of the camera you want to re-enable email alerts. The Function & Streams page opens.
4	Select the **General** tab. The General page opens.
5	Click the Camera Streaming **Enable** option button.
6	Click

In the camera record on the Video List page the IP address no longer indicates **DISABLED**.

- End -

Removing an Address from the Recipient List

You can remove recipient addresses from each alert category.

Procedure 257
Remove an Address from the Recipient List

Step	Action
1	Select **Advanced**.
2	Select **Email Alerts**. The Email Alerts page opens.
3	Scroll to the Alert Category you want to remove a recipient's address from.
4	Select 
5	Select the checkbox next to the address you want to remove.

6	Select  The page refreshes and the address is removed from the recipient list.

- End -

Email Blocks

You can block the NVR from sending alerts. On the Email Blocks page, you can choose which alert category to block, and you can apply the block to a specific device.

Procedure 258
Blocking an Email Alert category

Step	Action
1	Select **Advanced**.
2	Select **Email Alerts**.
3	Select the **Alert Blocks** tab.
4	Select 
5	From the **Category** dropdown menu, select the alert category you want to block.
6	From the **Device Id** dropdown menu, select the device slot number.

Note:
Your device slot numbers are displayed in the device **List** menu.

7 Select 

- End -

Alert Logs

The Alert Logs page displays a list of email alerts which have been sent by the NVR. Each entry includes the recipient email address, alert type and information sent with the time and date the alert occurred.

Procedure 259
Displaying the Email Alerts Log

Step	Action
1	Select **Advanced**.
2	Select **Email Alerts**.
3	Select the **Alert Logs** tab. The Alert Logs page opens.

- End -

Clearing the Alert Logs Page

All email alerts can be cleared from the Alert Logs page.

Procedure 260
Clearing the Alert Logs Page

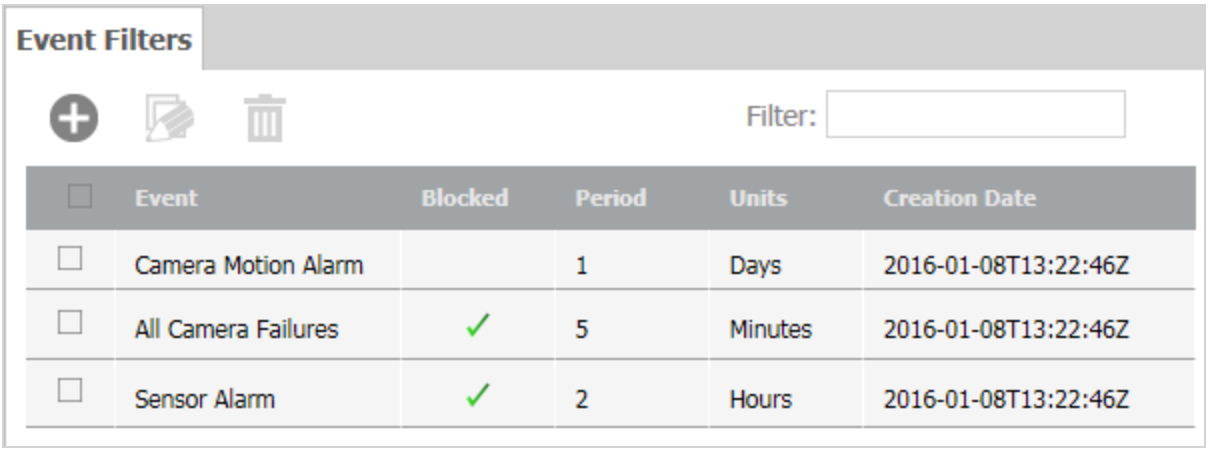
Step	Action
1	Select **Advanced**.
2	Select **Email Alerts**.
3	Select the **Alert Logs** tab. The Alert Logs page opens.
4	Click **Clear Logs**.

- End -

Event Filters

Enable Event Filters to control the flow of events from VideoEdge to victor and C·CURE. You can configure an Event Filter to block specific event notifications from being sent, or you can configure a time range for the Event filter. During this time, only one alert for that event type is generated.

Figure 88 Event Filters Page



Procedure 261
Creating an Event Filter

Step	Action
1	Select **Advanced**.
2	Select **Event Filters**. The Event Filters page opens.
3	Select  The **Add Filter** menu opens.
4	Select an event from the **Event Names** dropdown menu.
5	Select the **Blocked** checkbox to permanently enable the event filter. Or Configure the filter **Period**. a Enter a value for the **Period** duration. b Select the **Unit** type. Available Unit types include: Seconds, Minutes, Hours, Days and Weeks.
6	Click 

- End -

Procedure 262 Editing an Event Filter

Step	Action
1	Select **Advanced**.
2	Select **Event Filters**. The Event Filters page opens.
3	Select an Event Filter.
4	Select  The **Add Filter** menu opens.
5	(Optional) Select an event from the **Event Names** dropdown menu.
6	(Optional) Select the **Blocked** checkbox to permanently enable the event filter.
7	(Optional) Configure the filter **Period**. a Enter a Period duration. b Select the Unit type. Available Unit types include: Seconds, Minutes, Hours, Days and Weeks.
8	Click 

- End -

Procedure 263 Deleting an Event Filter

Step	Action
1	Select **Advanced**.
2	Select **Event Filters**. The Event Filters page opens.
3	Select an Event Filter to be deleted.
4	Click 

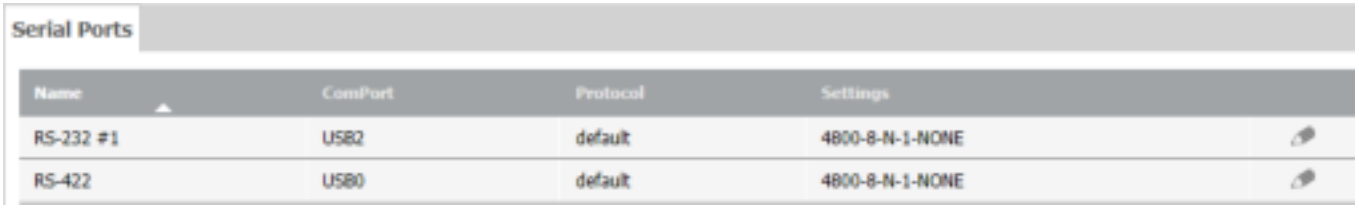
- End -

Serial Ports

Configuring Serial Ports

Serial Ports can be configured using the Serial Ports page in the Advanced Menu. Each serial protocol has default values for baud rate, data bits, parity, stop bits and flow control, you can edit each of these values if required.

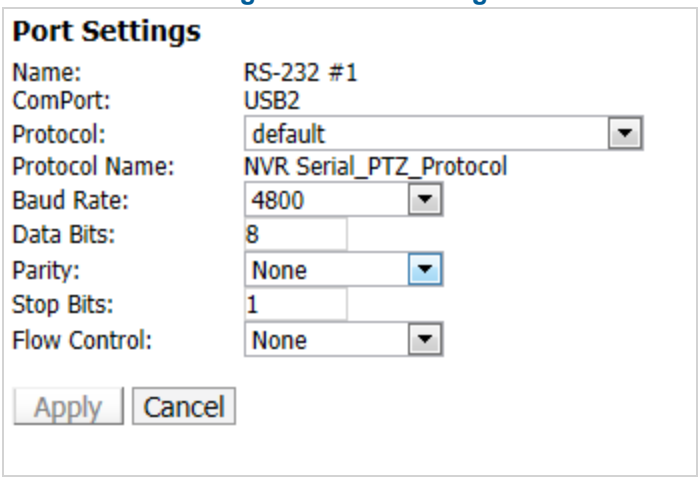
Figure 89 Serial Ports Page



Procedure 264
Configuring the Serial Ports

Step	Action
1	Select **Advanced**.
2	Select **Serial Ports**. The Serial Ports page opens.
3	Click  next to the port you wish to configure. The Port Settings pop up displays.

Figure 90 Port Settings



4	Select the **Protocol** from the dropdown.
5	Select the **Baud Rate** from the dropdown.
6	Enter the **Data Bits** in the field.
7	Select the **Parity** from the dropdown.
8	Enter the **Stop Bits** in the field.
9	Select the **Flow Control** from the dropdown.

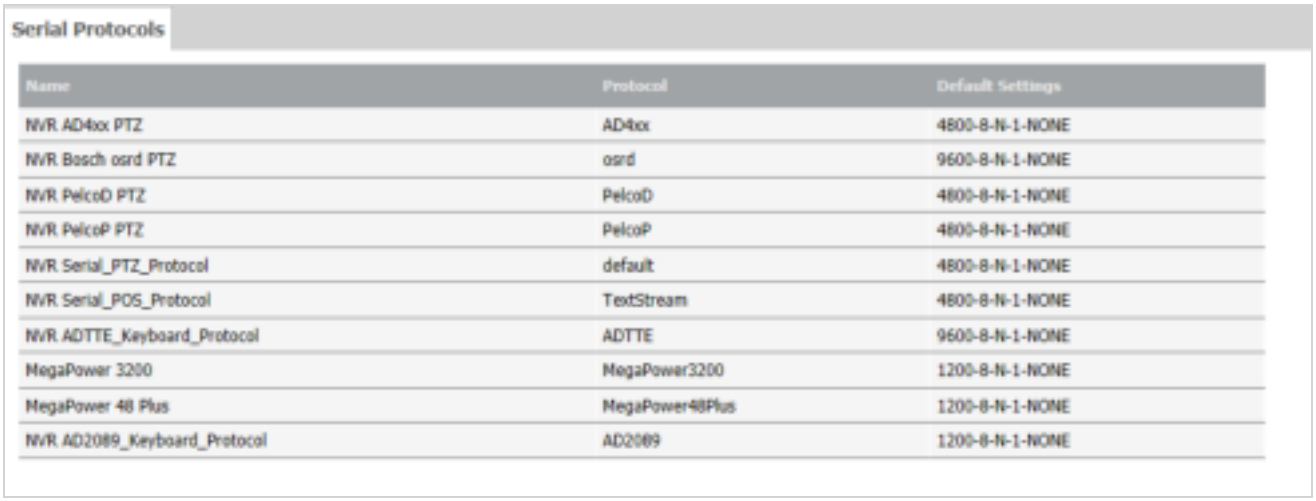
10 Click 

- End -

Viewing the Serial Protocols

You can view the Serial Protocols on the Serial Protocols page located in the System Menu.

Figure 91 Serial Protocols Page



Procedure 265
Viewing the Serial Protocols

Step	Action
1	Select **System.**
2	Select **Serial Protocols**. The Serial Protocols page opens.

- End -

Setting the PTZ Address

Serial ports can only support one protocol at any single time, however multiple cameras can be supported by a single protocol allowing multiple cameras using the same protocol to be controlled from a single port. Not all serial protocols can support the control of multiple cameras, the protocols which do support multiple cameras are:

- AD-422 over RS-422 and RS-485 multi-drop.
- Bosch OSRM over RS-422 and RS-485 multi-drop.
- Pelco P over RS-422 and RS-485 multi-drop.
- Pelco D over RS-422 and RS-485 multi-drop.
- Sensornet through an adapter module (ADACSNETH) - AD-422 should be selected as the protocol in use when using Sensornet.

The PTZ address field is used when multiple cameras are being used on the same serial port. The PTZ address is used to identify each of the cameras in use on the port. Typically the address is configured on a serial camera by means of changing dip switches. The configured address value on the NVR must match the configured camera value for PTZ functionality to work correctly.

Procedure 266
Setting the PTZ Address

Step	Action
1	Select **Devices**.
2	Select **List**. The Video List page opens.
3	Click  of the analog camera you want to configure PTZ settings for. The Function & Streams page opens.
4	Click the **PTZ** tab. The PTZ page opens.
5	Select the **PTZ Port** in use from the dropdown.
6	Enter the camera address number in the **PTZ Address** field.
7	Click 

- End -

PTZ settings specific to Optima/Optima LT Cameras

When using Optima and Optima LT Cameras with the PTZ port set to RS-422 communication using the AD4xx protocol, two additional checkboxes will display on the Camera PTZ page. They are:

1. **Simplex - Optima LT** - This should be enabled to allow simplex communications with Optima LT cameras. Optima LT cameras only support simplex communications when using RS-422 communication and the AD4xx protocol.
2. **Enable Camera Menu** - This should disabled when using Optima and Optima LT cameras when the PTZ port is set to RS-422 communication using the AD4xx protocol.

Note:
If these settings have not been applied your Optima/Optima LT cameras may not function as required.

Procedure 267
Configuring Optima/Optima LT Bespoke Settings when using RS-422

Step	Action
1	Select **Devices**.
2	Select **List**. The Video List page opens.
3	Click  of the analog camera you want to configure PTZ settings for. The Function & Streams page opens.

4 Click the **PTZ** tab.

The PTZ page opens.

5 Select the **PTZ Port** in use from the dropdown.

6 Enter the camera address number in the **PTZ Address** field.

7 (For Optima LT cameras) Select the **Simplex-Optima LT** checkbox.

8 De-select the **Enable Camera Menu** checkbox.

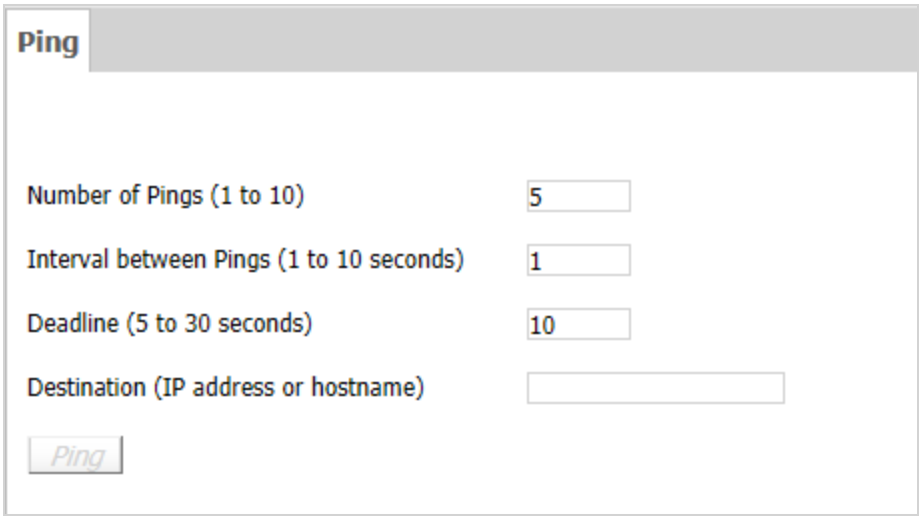
9 Click 

- End -

Ping

The Ping page allows you to verify the operation and confirm communication with cameras and devices on the NVR's network(s).

Figure 92 Ping Page



Procedure 268
Pinging other Devices

Step	Action
1	Select **Advanced**.
2	Select **Ping**. The Ping page opens.
3	Enter the **Number of Pings** to send to the selected device (Min 1, Max 10).
4	Enter the **Interval between Pings** (Min 1 second, Max 10 seconds).
5	Enter the **Deadline** the NVR is to wait for a response (Min 5 seconds, Max 30 seconds).
6	Enter the **Destination (IP address or hostname)**. **Note:** A DNS must be present to ping a device via a hostname.
7	Click **Ping**. Results will be displayed below the Ping button.

- End -

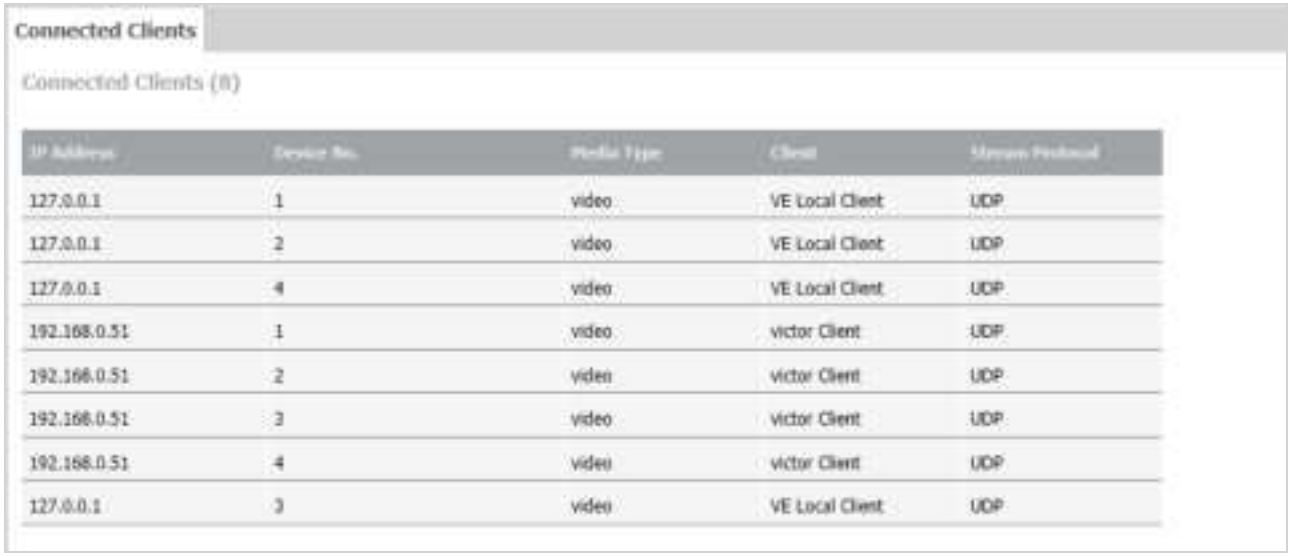
Connected Clients

You can view the clients currently connected to the NVR using the Connected Clients sub menu. The NVR will only register a client as connected if it is actively receiving a video/audio stream from the NVR.

The Connected Client page displays information relating to the clients currently connected to the NVR and their activity. The following information is displayed when a client is connected to the NVR:

- The IP Address of the device which is streaming audio and video from the NVR via a client.
- The Camera Number for each camera being streamed from the NVR for each client connected to the NVR.
- The Media Type being streamed; either audio or video or both.
- The Client type, for example victor unified client or QuickTime.
- The Streaming Protocol being used.

Figure 93 Connected Clients Page



Procedure 269
Viewing Connected Clients

Step	Action
1	Select **Advanced**.
2	Select **Connected Clients**. The Connected Clients page opens.

- End -

SIP Proxy

From the SIP Proxy page, you can enable or disable the SIP proxy, and you can select the inbound and outbound interfaces. When you enable VideoEdge's SIP Proxy, the SIP client can access SIP-enabled devices on a separate network, as long as the VideoEdge is connected to both networks.

Note:
SIP audio communication is available through the victor client. For more information, see the *victor Unified Client and victor Application Server Administration / Configuration Guide*.

Procedure 270
Enabling an SIP proxy

Step	Action
1	Select **Advanced**.
2	Select **SIP Proxy**.
3	Set **SIP Proxy Status** to **Enabled**.
4	Select a network port from the **Inbound Interface** list.
5	Select a network port from the **Outbound Interface** list. **Note:** • Set the Inbound Interface to the network that contains your SIP clients. • Set the Outbound Interface to the network that the FreeSWITCH server is connected to.
6	Enter the **FreeSWITCH Server IP Address**.
7	Enter the **FreeSWITCH Server Port**.
8	Select 

- End -

Reset to Factory Defaults

There are two ways in which the VideoEdge Recorder can be reset to factory default settings. The first method of resetting factory defaults is by using the Reset Factory Defaults page on the administration interface. The second method of resetting is via the reset pinhole button. Resetting via the Administration interface allows you to reset NVR settings whereas resetting via the pinhole button allows you to reset Operating System settings.

Reset Factory Defaults (Administration Interface)

The Reset Factory Defaults functionality allows you to revert several of the NVR's characteristics back to their default settings. It will however not implement any changes to the server's Linux Operating System. During a Reset Factory Defaults function the recorder will not be able to record or display live video until the process is complete.

Once the Reset Factory Defaults is complete you will have to reconfigure the NVR using the Setup Wizard.

The following settings will be affected when carrying out a Reset Factory Defaults function:

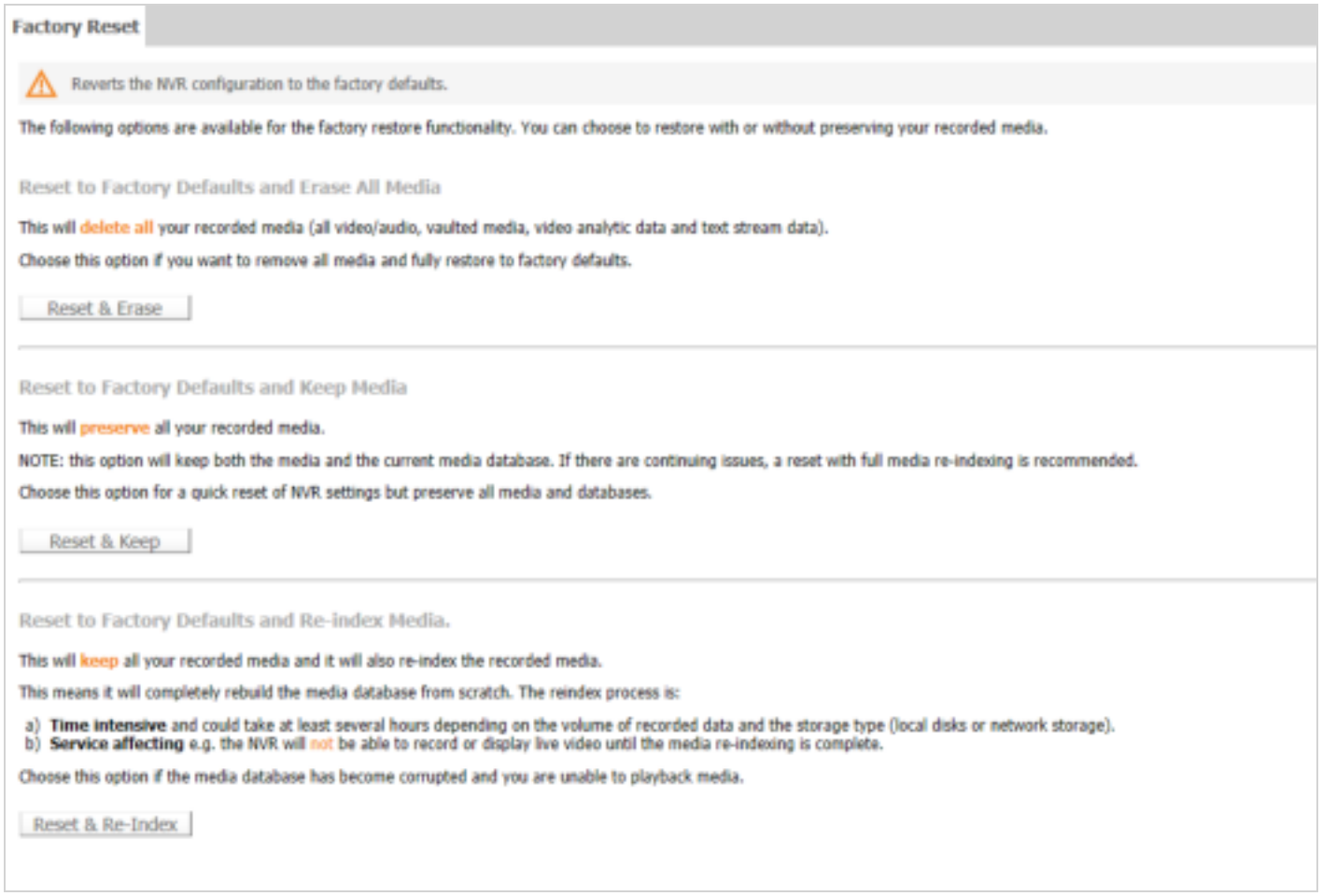
- **Storage** settings, configured using the NVR Administration interface will be erased.
- **Failover** settings, if configured will be erased.
- **User Passwords** for all user roles will be reset to the factory defaults.
- **Alarm** settings, if configured will be erased.
- **NVR Group** settings, if configured will be erased on the reset NVR. All other NVRs which have the reset NVR as a member of their NVR group will be unable to utilize its available resources for transcoding. NVR Group settings must be reconfigured on the reset NVR or a backup file applied.
- **Saved Media files (video/audio)**, the NVR supports several options for keeping or deleting the Saved Media files, they are as follows:
    - **Reset to Factory Defaults AND Erase All Media** - This will delete all your recorded media (video/audio, protected media and video analytic data). Choose this option if you want to remove all media and fully restore to factory defaults.
    - **Reset to Factory Defaults AND Keep Media** - This will preserve all your recorded media. Choose this option for a quick reset of NVR settings but preserve all media and databases.

Note:
This option will keep both the media and the current media database. If there are continuing issues a reset with full media re-indexing is recommended.

- **Reset to Factory Defaults AND Re-index Media** - This will keep all your recorded media and it will also re-index the recorded media. The media database will be completely rebuilt during this process. Choose this option if the media database has become corrupt and you are unable to playback media.

Note:
The re-index process is time intensive and can take several hours to complete depending on the volume of recorded data and the storage type (local disks or network storage). The NVR will not be able to record or display live video until the media re-indexing is complete.

Figure 94 Factory Reset Page



- **Email Alerts** will all be disabled and any email addresses entered for alert notifications will be erased. The SMTP Server address will also be erased.
- **WAN Settings** will be reset to factory defaults.
- **Cameras** will be erased leaving the Video List empty.

> **Note:**
> Settings linked to the OS will not be affected. These include Network Settings, Services (e.g. NTP, DHCP and so on) and the System Settings. The NVR License will also not be affected.

Procedure 271
Reset to Factory Defaults

Step	Action
1	Select **Advanced**.
2	Select **Reset Factory Defaults** The Reset Factory Defaults page opens.
3	Select one of the three Reset Factory Defaults options available: **Reset & Erase**

Or

Reset & Keep

Or

Reset & Re-index.

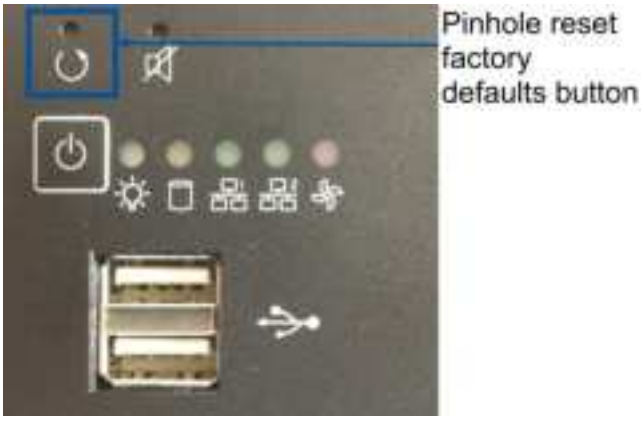
4 A warning message displays, click **Yes** to continue.

- End -

Reset Factory Defaults (Pinhole Reset)

There is a reset factory defaults pinhole button on the VideoEdge Appliance units. Resetting the factory defaults using the pinhole button allows you to reset Operating System settings but does not reset any of the NVR settings. This functionality is available on the 32 Channel Hybrid 2U Rack Mount and 64 Channel Hybrid 3U Rack Mount models. The reset button is on the front of the units.

Figure 95 Rack Mount Models - Location of Reset Button



Use the reset pin provided to press the button. When pressed this restores the following settings to the factory defaults:

- The IP Address of the LAN Interface on the motherboard is reset to **10.10.10.10**.
- The IP Address of all other NICs are reset. To use these you must reconfigure their settings.
- The Default Gateway settings are reset to **0.0.0.0**.

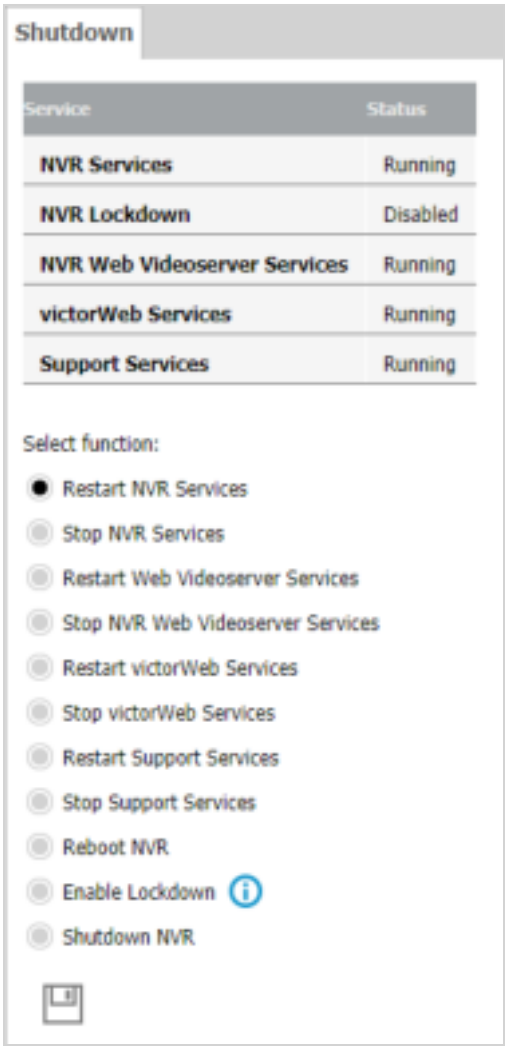
Note:
If your camera network requires the use of the Linux default gateway, resetting may affect your camera network.

The password for the VideoEdge OS **root** account will reset to **root**. The password for the **VideoEdge** account will be reset to **VideoEdge**. All additional VideoEdge OS accounts that have been created are deleted.

System Shutdown

The Shutdown page allows you to Stop or Restart the NVR, NVR Services, Web Videoserver Services, victor Web Services and Support Services. In addition, you can enable or disable Lockdown mode for the NVR.

Figure 96 Shutdown Page



NVR Services and victor

From version 5.1 onwards, victor operators can access camera footage while NVR services are stopped.

- victor operators can view live steams from multicast cameras, even while the VideoEdge is offline.
- victor operators can access recorded camera footage for search retrieve operations, and for clip exports.

Restart NVR Services

The Shutdown page allows you to restart the NVR services, this will restart the NVR software such as recording and playback services, however it will not restart the operating system. Restarting NVR services is faster than rebooting

the NVR. For a short period of time, while services are restarting, VideoEdge Administration Interface will have reduced functionality or be inaccessible.

Procedure 272
Restart NVR Services

Step	Action
1	Select **Advanced**.
2	Select **Shutdown**. The Shutdown page opens.
3	Select **Restart NVR Services** option button.
4	Click 

- End -

Stop NVR Services

NVR Services can be stopped permanently.

Note:
It is highly recommended that you stop NVR Services before configuring storage.

Procedure 273
Stop NVR Services

Step	Action
1	Select **Advanced**.
2	Select **Shutdown**. The Shutdown page opens.
3	Select **Stop NVR Services** option button.
4	Click  A message box opens, “This will stop NVR Services. Are you sure you want to continue?”
5	Click **Yes**. The confirmation message, “NVR Services have stopped - The NVR will not record or display live media until the services are restarted” displays and the NVR services are disabled.” **Note:** When you have stopped NVR services, use the Restart NVR Services option to restart the services.

- End -

Restart Web Videoserver Services

You can restart Web Videoserver services if you experience issues with your video feed. Restarting Web Videoserver services will not affect other victor Web users.

Procedure 274
Restart Web Videoserver Services

Step	Action
1	Select **Advanced**.
2	Select **Shutdown**. The Shutdown page opens.
3	Select **Restart Web Videoserver Services** option button.
4	Click 

- End -

Stop NVR Web Videoserver Services

NVR Web Videoserver Services can be stopped permanently. Users will still have access to all of the victor Web features, but cannot stream any video.

Procedure 275
Stop NVR Web Videoserver Services

Step	Action
1	Select **Advanced**.
2	Select **Shutdown**. The Shutdown page opens.
3	Select **Stop NVR Web Videoserver Services** option button.
4	Click 

- End -

Restart victorWeb Services

By restarting victorWeb Services, you will restart the Node and Health Server. You would typically restart these servers if you experience and victor Web issues without affecting the NVR.

Procedure 276
Restart victorWeb Services

Step	Action
1	Select **Advanced**.
2	Select **Shutdown**. The Shutdown page opens.
3	Select **Restart victorWeb Services** option button.
4	Click 

- End -

Stop victorWeb Services

victorWeb Services can be stopped permanently. Choosing this option prohibits all access to victor Web.

Procedure 277
Stop victorWeb Services

Step	Action
1	Select **Advanced**.
2	Select **Shutdown**. The Shutdown page opens.
3	Select **Stop victorWeb Services** option button.
4	Click 

- End -

Restart Support Services

Select this option to restart Support Services. You would typically restart these services if you experience any issues with Bluetooth transmission.

Procedure 278
Restart Support Services

Step	Action
1	Select **Advanced**.
2	Select **Shutdown**. The Shutdown page opens.
3	Select **Restart Support Services** option button.
4	Click 

- End -

Stop Support Services

Support Services can be stopped permanently. Choose this option to stop the VideoEdge from broadcasting any Bluetooth services.

Procedure 279
Stop Support Services

Step	Action
1	Select **Advanced**.
2	Select **Shutdown**. The Shutdown page opens.
3	Select **Stop Support Services** option button.
4	Click 

- End -

Reboot the NVR

Choosing this option will reboot the NVR.

Procedure 280
Reboot the NVR

Step	Action
1	Select **Advanced**.
2	Select **Shutdown**. The Shutdown page opens.
3	Select **Reboot NVR** option button.
4	Click 

- End -

Lockdown mode

From the Shutdown page, you can enable or disable Lockdown mode for the VideoEdge. During Lockdown, the VideoEdge's recording and data culling services are disabled. You can enable this feature when you need to prevent any changes to the VideoEdge's recorded footage for an extended period of time.

For example, if the VideoEdge records an incident that requires legal investigation, enable Lockdown mode to preserve any recorded video from being overwritten. While the VideoEdge is locked down, it can be taken off-site for further investigation. Users can search, retrieve, and play any recorded video through the local clients: victor Web LT and the VideoEdge Client.

Note:
The VideoEdge remains in Lockdown mode until you disable it.

During Lockdown, a notification banner appears in the VideoEdge Administration interface.

Procedure 281
Enabling or Disabling Lockdown mode

Step	Action
1	Select **Advanced**.
2	Select **Shutdown**.
3	Select the **Enable Lockdown** option button. **Note:** If Lockdown is already enabled, the **Disable Lockdown** option button displays instead. Or Select the **Disable Lockdown** option button.
4	Click  **Note:** • When you select the save icon, the VideoEdge shuts down. • When you restart the VideoEdge, it remains in Lockdown mode until you disable it.

- End -

Shutdown the NVR

The Shutdown page allows you to shut down the NVR, this will cause the NVR to fully power down when applied.

Procedure 282
Shutdown the NVR

Step	Action
1	Select **Advanced**.
2	Select **Shutdown**. The Shutdown page opens.
3	Select **Shutdown NVR** option button.
4	Click  **Note:** To restart the NVR after it has been shut down it must be manually turned on at the server.

- End -

Overview

The NVR provides the ability to create monitor output views using the Monitor Output Views page on the web interface. When a monitor output view is saved it is listed in the monitor outputs table. You can select the view you want to display on the selected monitor. The monitor output views can contain a combination of analog cameras, IP cameras and camera tours.

Figure 97 Monitor Outputs Menu Map

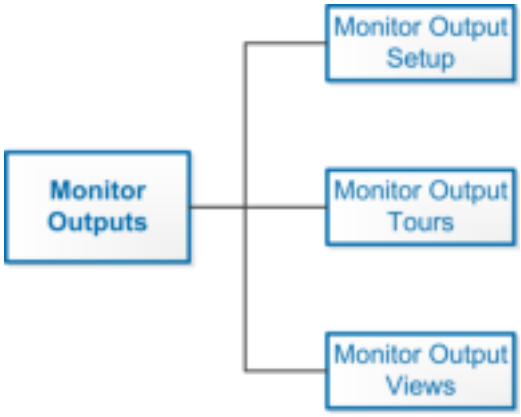
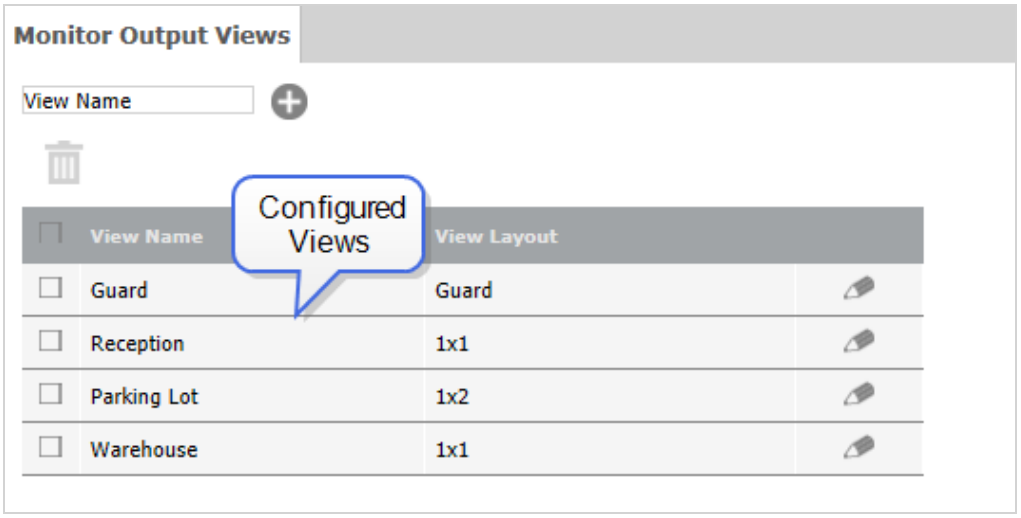


Figure 98 Monitor Output Views



Monitor Output Views

A monitor output view allows users to display multiple video inputs and tours simultaneously, providing a methodological and effective way to monitor multiple areas of interest. The presets are based on default layouts set within the NVR.

The NVR view layouts available are:

- 1x1
- 2x2
- 3x3
- 4x4
- Guard
- 12+1
- 2+8
- 1x2
- 2+3
- 2x1
- 2x3

Views are created in the Active Layout Editor page. Information on the View Name, Monitor, Available IP camera slots and IP cameras used by this configuration are displayed. You must ensure when configuring the monitor output view that only one IP camera is selected. If you do exceed this value you will not be able to display or save the monitor output view. Each analog camera can only be used once in a monitor output view.

Procedure 283
Viewing a Saved a Monitor Output View

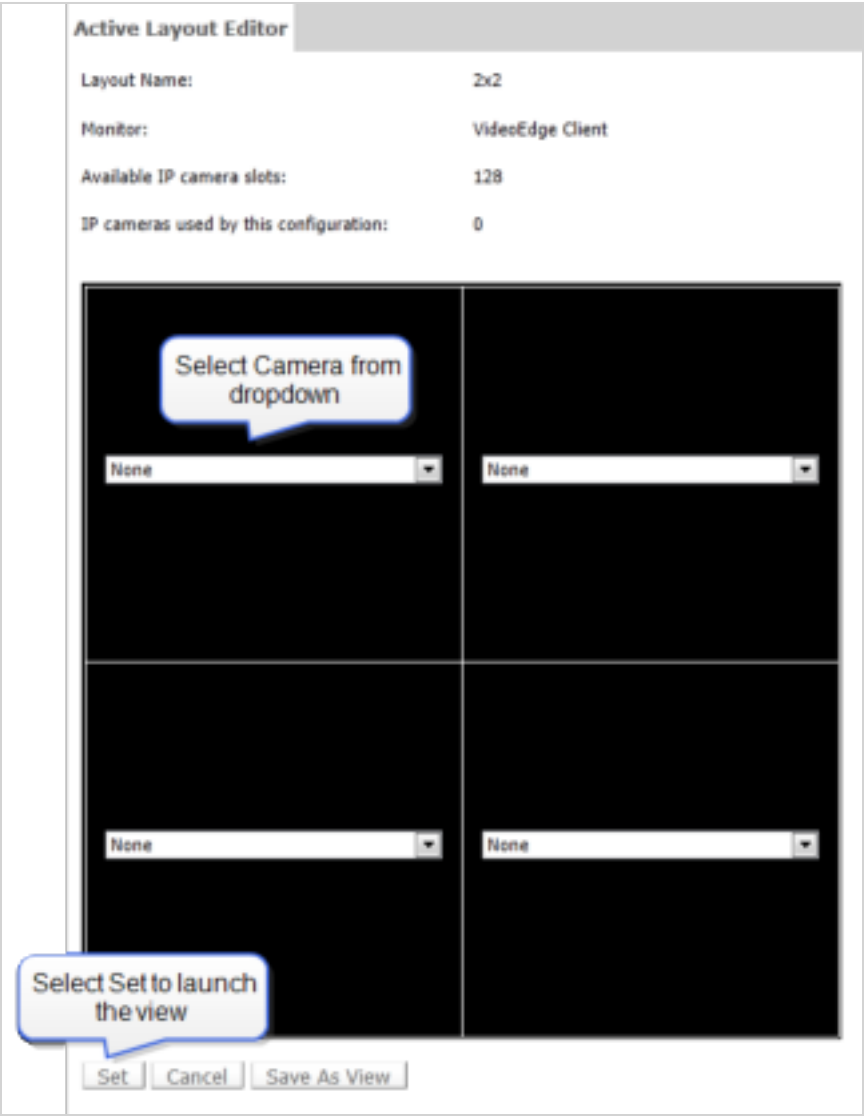
Step	Action
1	Select **Monitor Outputs** from the main menu.
2	Select **Monitor Output Setup**. The Monitor Outputs page opens.
3	In the Monitor Outputs table select the monitor you want the view to be displayed on from the required **Monitor** dropdown.
4	Select **Launch** in the monitor output view record you want to view. The selected monitor view is displayed on the monitor selected.

- End -

Procedure 284
Manually Use a Monitor Output View

Step	Action
1	Select **Monitor Outputs** from the main menu.
2	Select **Monitor Output Setup**. The Monitor Outputs page opens.
3	Select the required layout from the **Layout** dropdown.
4	Select  The Active Layout Editor opens.

Figure 99 Active Layout Editor



5 In each pane select the camera or tour you want to display from the dropdown list.

Note:
• You can only select one IP camera in a view. If you already have an IP camera selected in a pane, you cannot select another IP camera in another pane or select a tour with an IP camera in its rotation.
• You cannot select the same analog camera in two panes in a view.

6 Click **Set**.

The view is displayed in the output monitor.

Or

Click **Save As View**, enter a **View Name** and click 

- End -

Procedure 285
Save a Monitor Output View

Step	Action
1	Select **Monitor Outputs** from the main menu.
2	Select **Monitor Output Views**. The Monitor Output Views page opens.
3	Enter a **View Name**.
4	Click  The Active Layout Editor page opens.
5	Select a layout for the preset from the **Used layout** dropdown. The monitor display window shows the selected layout.
6	In each pane of the layout select the camera or tour you want to display from the dropdown. **Note:** • You can only select one IP camera in a view. If you already have an IP camera selected in a pane, you cannot select another IP camera in another pane or select a tour with an IP camera in its rotation. • You cannot select the same analog camera in two panes in a view.
7	Click **Set**.

- End -

Procedure 286
Edit a Monitor Output View

Step	Action
1	Select **Monitor Outputs** from the main menu.
2	Select **Monitor Output Views**. The Monitor Output Views page opens.
3	Select  in the view record you want to update.
4	Make the required changes to the view layout. **Note:** If you change the name of the view, when you click **Set** a new view will be saved in that name and changes made to the view will also be saved. The original view will also remain in the output monitor views table.
5	Click **Set**.

- End -

Procedure 287
Delete a Monitor Output View

Step	Action
1	Select **Monitor Outputs** from the main menu.
2	Select **Monitor Output Views**. The Monitor Output Views page opens.
3	Select the checkboxes of the presets you want to remove.
4	Click 

- End -

Assigning Secondary ADTT16E Keyboard Control

You can assign secondary keyboard control when you have a secondary ADTT16E configured.

Procedure 288
Assigning Secondary ADTT16E Keyboard Control

Step	Action
1	Select **Monitor Outputs** from the main menu.
2	Select **Monitor Output Setup**. The Monitor Outputs page opens.
3	Navigate to the ADTT16E Call Monitor Selection table and select either the required **Monitor Out** or **VideoEdge Client** from the Monitor dropdown.
4	Click 

- End -

Monitor Output Tours

A monitor output tour is a collection of different camera views, displayed in predefined sequences for specified durations. You can create multiple tours to be used as part of a monitor output view. You can also edit tours or remove tours that are no longer required.

Procedure 289
Create a Monitor Output Tour

Step	Action
1	Select **Monitor Outputs** from the main menu.
2	Select **Monitor Output Tours**. The Monitor Output Tours page opens.
3	Enter a **Tour Name**.
4	Click 

A configuration window opens.

Figure 100 Tour Configuration Window

5 Select a camera from the Available Cameras list. Use to move the camera to the Cameras In This Group list.

Note:
You can only use 1 IP camera in a tour as only one IP camera can be displayed in a view.

6 Enter the **Dwell Time** in seconds.

7 Repeat steps 5 and 6 until all cameras have been added to the tour.

8 The order of the Cameras In This Group list represent the order of the cameras that will display during the camera rotation tour. To reorder the list click a camera and drag it to the required location in the tour.

9 Click

- End -

Procedure 290
Edit a Monitor Output Tour

Step	Action
1	Select **Monitor Outputs** from the main menu.
2	Select **Monitor Output Tours**. The Monitor Output Tours page opens.
3	Select in the tour record you want to edit.
4	Make the required changes to the tour.
5	Click

- End -

Procedure 291
Remove a Monitor Output Tour

Step	Action
1	Select **Monitor Outputs** from the main menu.
2	Select **Monitor Output Tours**. The Monitor Output Tours page opens.
3	Select the checkboxes for the tours you want to remove.
4	Click 

- End -

Appendix A - VideoEdge Troubleshooting

Overview

This topic covers useful troubleshooting procedures to aid you in the use of your NVR. For configuring settings through the NVR's embedded operating system YaST Control Center is used.

You must log in to the VideoEdge desktop as a root user in order to access the YaST Control Center.

A Remote Desktop Connection can also be established allowing you to edit the network settings using the NVR desktop from a remote client.

Exiting the VideoEdge Client

When the VideoEdge Client is open it does not present the user with an option to close the client. To carry out the procedures in this appendix users will be required to close the client using the following process:

Procedure 292
Closing the VideoEdge Client

Step	Action
1	Press **Win** and **H** simultaneously. The Client is minimized and the NVR Desktop displays.
2	Right-click the **[veLocalClient]** tab on the task bar.
3	Select **Close**.

- End -

Monitor Resolution Settings

The VideoEdge Client user interface consists of menus which are fixed in display size. If your resolution settings are not correctly configured menu items might be hidden from view.

The supported resolution settings for displaying the VideoEdge Client are 1920 x 1080 and 1280 x 1024.

Changing the Monitor Resolution

You can change the NVRs monitor resolution from the Displays menu.

Procedure 293
Changing the Monitor Resolution

Step	Action
1	Select **Applications** from the NVR Desktop.
2	Select **System Tools**.
3	Select **Settings**.
4	Select **Displays**.

5 On the Displays menu, select your monitor.

6 Select a resolution from the **Resolution** dropdown list.

7 Click **Apply**.

- End -

Accessing the Remote Desktop

RDP Remote Desktop

The following procedures will allow you to log on and log off RDP remote desktop.

Procedure 294
Logging in to RDP Remote Desktop

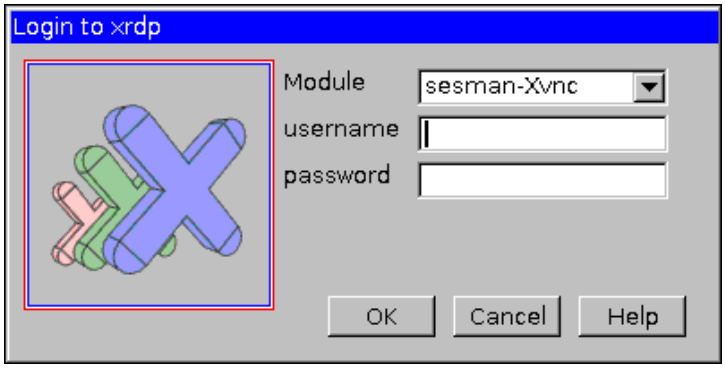
Step	Action
1	Click **Start** in the Windows taskbar.
2	Select **All Programs**.
3	Select **Accessories**.
4	Select **Remote Desktop Connection**. The Remote Desktop Connection application opens.

Figure 101 Remote Desktop Connection

5	Enter the **NVR's IP Address** in the Computer field.
6	Click **Connect**. A warning displays.

7 Click **Yes**.

The NVR's Desktop Login window opens.



8 Enter the **username** and **password** in the corresponding fields.

Note:
• You must use the default **Module** option:dropdown - sesman-Xvnc.
• Only the **VideoEdge** user credential can be used to access the NVR remotely.

9 Click **OK**.

- End -

Logging Out of RDP Remote Desktop

When using RDP remote desktop it is important to logout correctly. Failure to do so will leave a high CPU process running on the NVR which will affect performance.

Procedure 295
Logging Out of RDP Remote Desktop

Step	Action

1 Click  .

A popup window opens.

Figure 102 Logout Icon

2 Expand the Log Out menu and select **Log Out**.

A Logout popup displays.

Figure 103 Logout Popup

3 Select Log Out.

Remote Desktop window closes.

4 Select  to close the Remote Desktop Connection application.

- End -

Editing Storage Partitions Using Partitioner

Configuring System Partitions on a Previously Configured Device

If you are installing or upgrading the NVR software on a device which has been previously configured, there may be system partitions created already which will require re-configuration. To ensure your NVR is set up correctly, all existing partitions should be deleted.

The requirements for configuration are three system partitions in addition to the media storage partitions. The system partitions are needed for regular operation of the NVR's operating system. The required system partitions that need to be created are outlined in the table below. Each partition size in the table is the recommended minimum value.

Note:
When the Linux system starts, it scans the hardware for all system devices. When it finds disks and partitions it assigns them unique names. Linux does not follow DOS or Windows XP style partition or drive naming convention. Linux uses a combination of bus type and alphanumeric suffixes.

The next part of the naming convention is an alphabetic designation for each physical drive, as an example the primary drive of a system using SCSI drives would be ***sda***. The secondary physical SCSI drive naming prefix would be ***sdb***. Tertiary physical drive would be ***sdc*** and so on.

As mentioned above the next part of the naming convention is a numerical suffix that denotes the partition. Each hard drive has a limit of 4 primary partitions. For example the primary SCSI drive of a system with four partitions would be named as follows: sda1, sda2, sda3 and sda4. As an example of the naming convention for the secondary drive it would be as follows: sdb1, sdb2, etc

One primary partition per drive can be assigned as an extended partition containing as many logical partitions as you require.

Table 24 Default Partitions Required for NVR

Size (GB)	Type	FS Type	Mount Point
16	Linux swap	Swap	swap
47	Linux native	XFS	/var
20	Linux native	Ext3	/

Procedure 296
Configuring System Partitions on a Previously Configured Device

Step	Action
1	In the Suggested Partioning page of the Partitioner Wizard, click **Create Partition Setup**.
2	Select **Custom Partitioning (for experts)**. The Expert Partitioner page displays.
3	**Select the disk** on which you want to create the system partitions from the system view tree.
4	**Delete** all of the existing partitions, by selecting the partition and clicking Delete.
5	Click **Add**.
6	Select **Primary Partition**.
7	Enter the required partition size by selecting **Custom Size** and entering the amount of disk space (GB) you want to allocate to the partition.
8	Select **Next**.
9	Select the desired option from the **File System** dropdown. For swap select **Swap**, for var select **XFS** and for root select **Ext3**.
10	Enter the **Mount Point** for the media partition. For swap enter **swap**, for var enter **/var** and for root enter **/**.

11 Click **Finish**.

12 Create the required media storage partitions. Refer to Installing VideoEdge for more information.

- End -

Editing Media Partition Configurations

If you have completed the installation of the NVR hardware and software bundle, default media partitions will be configured on the NVR. You can change these media partitions to suit your specific requirements.

If you want to edit media partition configurations on a storage device you must remove all media folders already configured to be used by the NVR from the NVR configuration.

Note:
If a storage set contains only media folders from the device you want to edit media partition configurations on, you must move camera recording to other storage sets first.

NVR Services should also be stopped prior to changing partition configurations on devices that have already been added to the NVR.

Procedure 297
Editing Media Partitions

Step	Action
1	Select **Applications** from the NVR desktop.
2	Select **System Tools**.
3	Select **YaST**.
4	Enter the root password.
5	Select **Continue**. The Control Center opens.
6	Select **Partitioner** from the System menu.
7	A warning message opens. Click **Yes** to continue. The Expert Partitioner page opens.
8	Select the disk containing the media partitions you want to edit from the system view tree.
9	To edit the size of a partition: a Select the partition in the table and click **Resize**. b Select either **Maximum Size**, **Minimum Size** or **Custom Size** and enter the required partition size. c Click **OK**. Or To add a new partition: a Click **Add**. b Select either **Primary Partition** or **Extended Partition**. c Select the partition size. Select either **Maximum Size** or **Custom Size** and enter the required partition size. If preferred you can choose an allocated region of the disk by entering a **Start Cylinder** and an **End Cylinder**.

d Select **Next**.

e Select the **Role**. Select either **Operating System**, **Data and ISV Applications**, **Swap** or **Raw Volume (unformatted)**.

f Select **Next**.

g If you are creating an extended partition, continue to step o otherwise continue to step h.

h Click the **Format Partition** option button.

i Select **XFS** from the **File System** dropdown.

j Enter the **Mount Point** for the media partition, for example, **/data/media1**.

k Select the **Fstab Options...** button.

l Select the **Device ID** option button.

m Enter **rw,noatime,nodiratime,attr2,nobarrier,noquota,allocsize=4m,inode64** in the **Arbitrary option** value field.

Note:
nobarrier should only be used on storage devices connected to disk controllers with battery backed cache.

n Click **Finish**.

Or

To delete a partition:

a Select the partition you want to delete.

b Click **Delete**.

c Click **Yes** to delete the partition.

10 Click **Next**.

The Expert Partitioner page opens displaying the changes to be made to the partitions.

11 Click **Finish**.

The changes are made to the partitions.

- End -

System Disk Recovery

VideoEdge NVR

Should the NVR's system disk fail or the system disk becomes corrupt, the following procedure should be used for its recovery. You will need the following items:

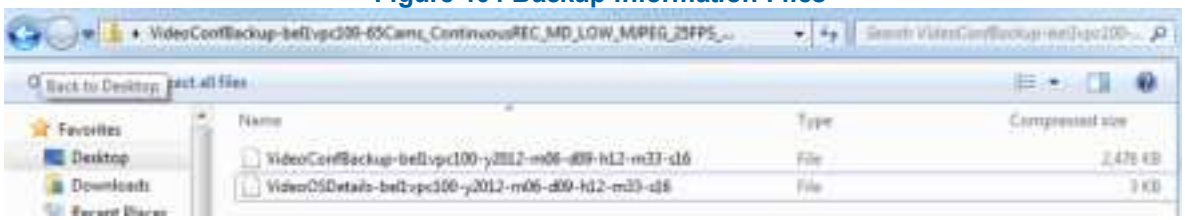
1 A License file for the NVR.

2 A system backup file (from NVR 4.2+ only).

Note:
You must have carried out a "backup" procedure after all NVR configuration was completed at time of install. This is a zip file which when expanded contains two files. One of the files is the NVR backup information (Named

“VideoConfBackup-xxxxxxxxxxx.zip”. The other is a text file detailing Network and storage mount information. This text file, VideoOSDetails-xxxxxxxx.zip, is required to complete the recovery procedure.

Figure 104 Backup Information Files



3 A replacement disk greater than the existing system disk (if applicable).

4 NVR Software CD or USB drive.

Caution

To maintain all configured Tours and Salvos relating to your NVR in victor unified client, you should complete the VideoEdge System Disk Restore procedure before reconfiguring the NVR’s LAN Interface Settings.

Procedure 298
VideoEdge NVR System Disk Recovery

Step	Action
1	Power **OFF** the NVR.
2	(Optional) Replace the system disk. This step is required if the system disk becomes corrupt.
3	Ensure all external connections are present.
4	Boot the NVR from the Software CD or USB drive.
5	Complete the Installation process as far as the VideoEdge Setup Wizard stage. Refer to Installing VideoEdge
6	Using YaST configure any iSCSI storage devices and connect to them.
7	Unzip the backup file in windows. Extract the file “**VideoOSDetails-VideoEdge-XXXXXXXX**” and save to a USB.
8	On the NVR, open the file “**VideoOSDetails-VideoEdge-XXXXXXXX**” from the USB in a text editor.
9	Copy all information from the Filesystem details section of the file.
10	Paste the copied text into a new file, **/tmp/fstab_backup** on the NVR. a Open the Terminal window. b Type **cat>/tmp/fstab_backup**. Press **[Enter]**. c Paste the copied text from the clipboard. Press **[Enter]**. d Press **[CTRL]** + **[D]**.
11	In the Terminal window type **videoedge# /opt/americandynamics/venvr/bin/restore_fstab/tmp/fstab_backup** and press **[Enter]**. Running this command restores all previous mountpoints.
12	On the NVR desktop double-click on the **NVR Administrator** icon, or on a remote machine use Internet Explorer to log into the NVR Configuration Interface. The default credentials are Username: **admin**, Password: **admin**. The Setup Wizard opens at the Welcome page.

13 Click **Start** to begin the Setup Wizard.

14 Continue through the Setup Wizard until you reach the Network section of the wizard. Open the "**VideoOSDetails-xxxxxxxx**" file and use the network settings to help you configure the following:

- Domain Name
- Domain Name Servers
- Default Gateway
- RTSP Port
- NTP Status
- NTP Servers

15 Complete the remaining stages of the Setup Wizard.

When complete the NVR Configuration Interface opens at the Video List page.

16 Select **System**.

17 Select **Backup/Restore**.

The Backup page opens.

18 Select the **Restore** tab.

The Restore page opens.

19 Click **Browse**.

20 Navigate to and select the NVR backup file, "**VideoConfBackup-xxxxxxxxxxx.zip**".

Note:
You must use the zip file and not an individual sub file.

21 Click **Upload Backup**.

22 You will be prompted for media recovery, click **Yes**. Media recovery will take approximately 1 minute per 90-100GB of Storage.

Status messages will display informing you of current progress.

23 Once complete verify that all configuration parameters are correct.

- End -

Heartbeat control in VideoEdge 4.9 Administration Interface

Issue

In previous versions of VideoEdge (4.4, 4.5, 4.5.1 and 4.6) , the heartbeat settings which dictated when Failover would engage could be configured using the NVR's Administration Interface. In version 4.7+ the Failover heartbeat is configured at its optimum default settings. The default settings are:

Polling Interval: 3

Retry Count: 3

Config Update Interval: 60

Solution

If required to suit your deployment scenario, the heartbeat parameters can be manually changed by the following procedure.

Procedure 299
Editing Failover heartbeat parameters

Step	Action
1	Log into the VideoEdge NVR locally or remotely and open GNOME Terminal.
2	To open GNOME Terminal - a Select **Applications** (located lower left of VideoEdge desktop) b Click **Utilities** c Select **GNOME Terminal** Note – GNOME Terminal will be pinned to the Applications Menu.
3	(Remote Login only) Type `su` and press RETURN.
4	(Remote Login only) Type `rootpassword` and press RETURN.
5	`cd /var/opt/americandynamics/venvr/`
6	`xdg-open failoverstate.json` A gedit window launches showing the file in text format

7	Edit the bolded fields as required -
	`"failoverparams" : {`
	`"failoverpollinterval" : 10,`
	`"heartbeatblackoutinterval" : 120,`
	`"failoverretrycount" : 3,`
	`"configurationcheckinterval" : 60`
	`}`

8	Click **Save**.
9	Close gedit.
10	In terminal, press CTRL+C.
11	Type `exit` and press RETURN.
12	Close Gnome Terminal.

- End -

Below is the content of the entire failoverstate.json file for a secondary NVR -

VEFailover16:/var/opt/americandynamics/venvr # cat failoverstate.json

{

"monitornvrparams" : [

{

"heartbeatblackout" : "0",

"id" : "c58c6c1d-5671-5a7d-8e64-f1e7086a34aa",

"eventseqnum" : "328861"

},

{

"heartbeatblackout" : "0",

"id" : "e91dcc38-0cea-5715-b455-c88d77174ce1",

"eventseqnum" : "306670"

}

],

"failover" : [

{

"managementip" : "10.38.25.16",

"priority" : -1,

"id" : "3e626b38-a2ea-5db1-b372-7a84b134209b",

"role" : "secondary",

"state" : "secondary_monitoring"

}

],

"failoverparams" : {

"failoverpollinterval" : 10,

"heartbeatblackoutinterval" : 120,

"failoverretrycount" : 3,

"configurationcheckinterval" : 60

}

}

Enabling VideoEdge as an NTP Server

Issue

For security reasons, the NTP Server functionality of the VideoEdge NVR is disabled by default in VideoEdge 4.5.

Solution

The VideoEdge NVR can be enabled as an NTP Server if necessary.

Caution

• Enabling this service will leave the VideoEdge NVR more vulnerable to attack.

• For security reasons, you should limit the number of devices that connect to a VideoEdge NTP server

Procedure 300
Enabling the VideoEdge NVR as an NTP Server

Step	Action
1	Login to the VideoEdge NVR.
2	From the VideoEdge desktop, select **Applications**.
3	Select **Utilities**.
4	Select **GNOME Terminal**.
5	Type the following commands:
	a Type *su* and press ENTER
	b Password of root user account and press ENTER
	c *service ntp stop* and press ENTER
	d *vi /etc/ntp.conf*
6	Using your arrow keys, navigate to the line "restrict default ignore."
7	Type the following commands
	a *dd*
	b *:wq* and press ENTER
	c *service ntp start* and press ENTER
	d */sbin/chkconfig ntp on* and press ENTER
	e *exit* [Enter]

- End -

The following steps should be carried out on a VideoEdge unit to enable it to receive time synchronization commands from a VideoEdge acting as an NTP Server:

Procedure 301
Synchronizing the time between VideoEdge devices and a VideoEdge NTP server.

Step	Action
1	Login to the VideoEdge.
2	From the VideoEdge desktop, select **VideoEdge Administrator**.
3	Login as an Administrator.
4	Navigate to the **Network>General** menu.
5	Select **Enabled** next to **NTP Status**.

6 Select the green '+' icon and enter the IP address of your NTP Server VideoEdge.

7 Select **Save**.

8 Minimize the NVR Administrator interface.

9 From the VideoEdge desktop, select **Applications**.

10 Select **Utilities**.

11 Select **GNOME Terminal** to open one instance of GNOME Terminal. Select **GNOME Terminal** again to open a second instance of GNOME Terminal.

12 In both terminal windows, type the following commands:

   a *su* [Enter]

   b Password of root user account [Enter]

13 In terminal window one, type the following commands:

   a *tail –F /var/log/ntp* [Enter]

14 In terminal window two, type the following commands:

   a *service ntp stop* [Enter]

   b *ntpd –q* [Enter]

15 In terminal window one, press keys [CTRL] + [c] to stop the tail command.

16 In terminal window two, type the following commands:

   a *service ntp start* [Enter]

   b *sbin/chkconfig ntp on* [Enter]

17 In both terminal windows, type the following commands:

   a *exit* [Enter]

18 NTP synchronization is set up. This may take a few minutes to synchronize and can be verified by logging in as a support user then navigating to the **Support>NTP Status** menu.

- End -

Appendix B - ISO 3166 Country Codes

AF	AFGHANISTAN
AX	ÅLAND ISLANDS
AL	ALBANIA
DZ	ALGERIA
AS	AMERICAN SAMOA
AD	ANDORRA
AO	ANGOLA
AI	ANGUILLA
AQ	ANTARCTICA
AG	ANTIGUA AND BARBUDA
AR	ARGENTINA
AM	ARMENIA
AW	ARUBA
AU	AUSTRALIA
AT	AUSTRIA
AZ	AZERBAIJAN
BS	BAHAMAS
BH	BAHRAIN
BD	BANGLADESH
BB	BARBADOS
BY	BELARUS
BE	BELGIUM
BZ	BELIZE
BJ	BENIN
BM	BERMUDA
BT	BHUTAN
BO	BOLIVIA, PLURINATIONAL STATE OF
BQ	BONAIRE, SINT EUSTATIUS AND SABA
BA	BOSNIA AND HERZEGOVINA
BW	BOTSWANA
BV	BOUVET ISLAND
BR	BRAZIL
IO	BRITISH INDIAN OCEAN TERRITORY
BN	BRUNEI DARUSSALAM
BG	BULGARIA
BF	BURKINA FASO
BI	BURUNDI
KH	CAMBODIA
CM	CAMEROON
CA	CANADA
CV	CAPE VERDE
KY	CAYMAN ISLANDS
CF	CENTRAL AFRICAN REPUBLIC
TD	CHAD
CL	CHILE
CN	CHINA
CX	CHRISTMAS ISLAND
CC	COCOS (KEELING) ISLANDS
CO	COLOMBIA

KM	COMOROS
CG	CONGO
CD	CONGO, THE DEMOCRATIC REPUBLIC OF THE
CK	COOK ISLANDS
CR	COSTA RICA
CI	CÔTE D'IVOIRE
HR	CROATIA
CU	CUBA
CW	CURAÇAO
CY	CYPRUS
CZ	CZECH REPUBLIC
DK	DENMARK
DJ	DJIBOUTI
DM	DOMINICA
DO	DOMINICAN REPUBLIC
EC	ECUADOR
EG	EGYPT
SV	EL SALVADOR
GQ	EQUATORIAL GUINEA
ER	ERITREA
EE	ESTONIA
ET	ETHIOPIA
FK	FALKLAND ISLANDS (MALVINAS)
FO	FAROE ISLANDS
FJ	FIJI
FI	FINLAND
FR	FRANCE
GF	FRENCH GUIANA
PF	FRENCH POLYNESIA
TF	FRENCH SOUTHERN TERRITORIES
GA	GABON
GM	GAMBIA
GE	GEORGIA
DE	GERMANY
GH	GHANA
GI	GIBRALTAR
GR	GREECE
GL	GREENLAND
GD	GRENADA
GP	GUADELOUPE
GU	GUAM
GT	GUATEMALA
GG	GUERNSEY
GN	GUINEA
GW	GUINEA-BISSAU
GY	GUYANA
HT	HAITI
HM	HEARD ISLAND AND MCDONALD ISLANDS
VA	HOLY SEE (VATICAN CITY STATE)
HN	HONDURAS
HK	HONG KONG
HU	HUNGARY
IS	ICELAND

IN	INDIA
ID	INDONESIA
IR	IRAN, ISLAMIC REPUBLIC OF
IQ	IRAQ
IE	IRELAND
IM	ISLE OF MAN
IL	ISRAEL
IT	ITALY
JM	JAMAICA
JP	JAPAN
JE	JERSEY
JO	JORDAN
KZ	KAZAKHSTAN
KE	KENYA
KI	KIRIBATI
KP	KOREA, DEMOCRATIC PEOPLE'S REPUBLIC OF
KR	KOREA, REPUBLIC OF
KW	KUWAIT
KG	KYRGYZSTAN
LA	LAO PEOPLE'S DEMOCRATIC REPUBLIC
LV	LATVIA
LB	LEBANON
LS	LESOTHO
LR	LIBERIA
LY	LIBYA
LI	LIECHTENSTEIN
LT	LITHUANIA
LU	LUXEMBOURG
MO	MACAO
MK	MACEDONIA, THE FORMER YUGOSLAV REPUBLIC OF
MG	MADAGASCAR
MW	MALAWI
MY	MALAYSIA
MV	MALDIVES
ML	MALI
MT	MALTA
MH	MARSHALL ISLANDS
MQ	MARTINIQUE
MR	MAURITANIA
MU	MAURITIUS
YT	MAYOTTE
MX	MEXICO
FM	MICRONESIA, FEDERATED STATES OF
MD	MOLDOVA, REPUBLIC OF
MC	MONACO
MN	MONGOLIA
ME	MONTENEGRO
MS	MONTSERRAT
MA	MOROCCO
MZ	MOZAMBIQUE
MM	MYANMAR
NA	NAMIBIA
NR	NAURU

NP	NEPAL
NL	NETHERLANDS
NC	NEW CALEDONIA
NZ	NEW ZEALAND
NI	NICARAGUA
NE	NIGER
NG	NIGERIA
NU	NIUE
NF	NORFOLK ISLAND
MP	NORTHERN MARIANA ISLANDS
NO	NORWAY
OM	OMAN
PK	PAKISTAN
PW	PALAU
PS	PALESTINE, STATE OF
PA	PANAMA
PG	PAPUA NEW GUINEA
PY	PARAGUAY
PE	PERU
PH	PHILIPPINES
PN	PITCAIRN
PL	POLAND
PT	PORTUGAL
PR	PUERTO RICO
QA	QATAR
RE	RÉUNION
RO	ROMANIA
RU	RUSSIAN FEDERATION
RW	RWANDA
BL	SAINT BARTHÉLEMY
SH	SAINT HELENA, ASCENSION AND TRISTAN DA CUNHA
KN	SAINT KITTS AND NEVIS
LC	SAINT LUCIA
MF	SAINT MARTIN (FRENCH PART)
PM	SAINT PIERRE AND MIQUELON
VC	SAINT VINCENT AND THE GRENADINES
WS	SAMOA
SM	SAN MARINO
ST	SAO TOME AND PRINCIPE
SA	SAUDI ARABIA
SN	SENEGAL
RS	SERBIA
SC	SEYCHELLES
SL	SIERRA LEONE
SG	SINGAPORE
SX	SINT MAARTEN (DUTCH PART)
SK	SLOVAKIA
SI	SLOVENIA
SB	SOLOMON ISLANDS
SO	SOMALIA
ZA	SOUTH AFRICA
GS	SOUTH GEORGIA AND THE SOUTH SANDWICH ISLANDS
SS	SOUTH SUDAN

ES	SPAIN
LK	SRI LANKA
SD	SUDAN
SR	SURINAME
SJ	SVALBARD AND JAN MAYEN
SZ	SWAZILAND
SE	SWEDEN
CH	SWITZERLAND
SY	SYRIAN ARAB REPUBLIC
TW	TAIWAN, PROVINCE OF CHINA
TJ	TAJIKISTAN
TZ	TANZANIA, UNITED REPUBLIC OF
TH	THAILAND
TL	TIMOR-LESTE
TG	TOGO
TK	TOKELAU
TO	TONGA
TT	TRINIDAD AND TOBAGO
TN	TUNISIA
TR	TURKEY
TM	TURKMENISTAN
TC	TURKS AND CAICOS ISLANDS
TV	TUVALU
UG	UGANDA
UA	UKRAINE
AE	UNITED ARAB EMIRATES
GB	UNITED KINGDOM
US	UNITED STATES
UM	UNITED STATES MINOR OUTLYING ISLANDS
UY	URUGUAY
UZ	UZBEKISTAN
VU	VANUATU
VE	VENEZUELA, BOLIVARIAN REPUBLIC OF
VN	VIET NAM
VG	VIRGIN ISLANDS, BRITISH
VI	VIRGIN ISLANDS, U.S.
WF	WALLIS AND FUTUNA
EH	WESTERN SAHARA
YE	YEMEN
ZM	ZAMBIA
ZW	ZIMBABWE

Appendix C - SmartStream

Overview

This topic provides more information on SmartStream. SmartStream is the resource management tool for VideoEdge. Resource management is achieved using a video palette comprising of native and transcoded streams.

Transcoding

Transcoding is an integral part of how the NVR streams media to a client, transcoding is the process of reducing frames per second and/or resolution. All streams being forwarded to a client may be subject to transcoding at various levels to provide the best all round solution for your video monitoring. Transcoding is also allied to the client's configuration; reductions in resolution are applied where the viewed image is smaller, for example in a 3x3 layout a high resolution frame provides no added detail. This will be dictated to the NVR by the streaming client.

The number of streams which can be transcoded at any one time is dependent on your VideoEdge hardware platform. For legacy platforms released prior to software version 4.4.2 the VideoEdge can transcode up to 4 streams at any one time. VideoEdge Micro NVRs can transcode up to 2 streams at any one time. VideoEdge Appliance platforms released after software version 4.4.2 can transcode up to 14 streams at any one time once they have been upgraded to software version 4.5.1 and onwards.

Video Palette

Resource management is achieved using a video palette. At any one time a video palette consisting of native and transcoded streams is available for streaming to the client. The palette offerings will be affected by the following factors:

- The number of transcode streams already in use either on your client or on others streaming from the NVR.
- The capabilities of your NVR hardware.
- The number of native streams the designated camera is capable of delivering.
- The Camera Codec in use.
- The WAN/LAN bitrate cap.
- If you have an NVR group configured, the number of transcode streams that are already in use on any NVR within the NVR group.

The stream which provides an optimized result will be selected for streaming to the client. Selection of the optimized stream will be dictated by the following:

1 **Client side settings -**

- Whether the client has been configured to prefer optimized frame rate or resolution.
- Native streams will be selected when the LAN checkbox has been selected.

Note:
If a bandwidth cap has been applied on the client, this overrides the LAN checkbox and re-enables standard resource management rules.

- The NVR connection WAN vs VPN.
- The bitrate cap setting.
- Whether video hiding is on or off.

2 **Client side hardware -**

- Monitor resolution.

3 **Physical size of the window -**

- Window size as influenced by the client side hardware.
- Surveillance pane size as influenced by the client hardware.
- Other panes snapped to the surveillance pane, for example if the activity window is side by side to the surveillance pane.
- The layout in use.

4 **Bit Rate -**

- Changes in a scene, for example quiet to busy and vice versa, PTZ and so on. (Estimated bit rate over/below the actual bit rate.)
- Number of streams running concurrently. This includes streams from other recorders.

Note:
Search and retrieve also affects palette selection. When a clip download is in progress, the available bandwidth is reduced. SmartStream will adjust the palette selection to reflect this.

- Configured camera codec.
- Configured FPS setting.
- Camera GOV (Group of Video) setting.
- Camera type and firmware in use.

5 **User Interaction with the client -**

Note:
Changes made to the client can cause palette reselection.

- Entering/exiting Instant Playback.
- Changes made to the bandwidth cap.
- Changes to Instant Playback changes.
- Launching and clearing streams.
- Entering and exiting virtual PTZ.
- Switching Layouts.
- Resizing windows.
- Connection dropouts and subsequent reconnection.
- Changes to resource management system values. Occurs when the stop video when not visible checkbox is selected.

Note:
Option is selected by default in victor.

Appendix D - Hardware Configurations

Overview

Prior to using your NVR for the first time, it is important that it has been connected with its ancillaries correctly. The following section details the hardware configuration for the different models of VideoEdge Appliances.

Hardware Configurations

The VideoEdge Appliance is available in several different configurations, they are as follows:

1. **VideoEdge Micro NVR** - This model provides either 4 or 8 IP video channels with an on board PoE switches.
2. **VideoEdge Desktop Hybrid NVR** - This model provides 8 analog and 8 IP video channels.
3. **VideoEdge Desktop NVR** - This model provides 32 IP video channels.
4. **VideoEdge 1U NVR** - This model provides 32 IP video channels and 16 PoE ports.
5. **VideoEdge 2U Hybrid NVR** - This model is rack mountable and provides 16 analog and 16 IP video channels.
6. **VideoEdge 2U NVR** - This model provides 64 IP video channels.
7. **VideoEdge 2U NVR Server** - This model is rack mountable and provides 128 IP video channels.
8. **VideoEdge 3U Hybrid NVR** - This model is rack mountable and provides 32 analog and 32 IP video channels.

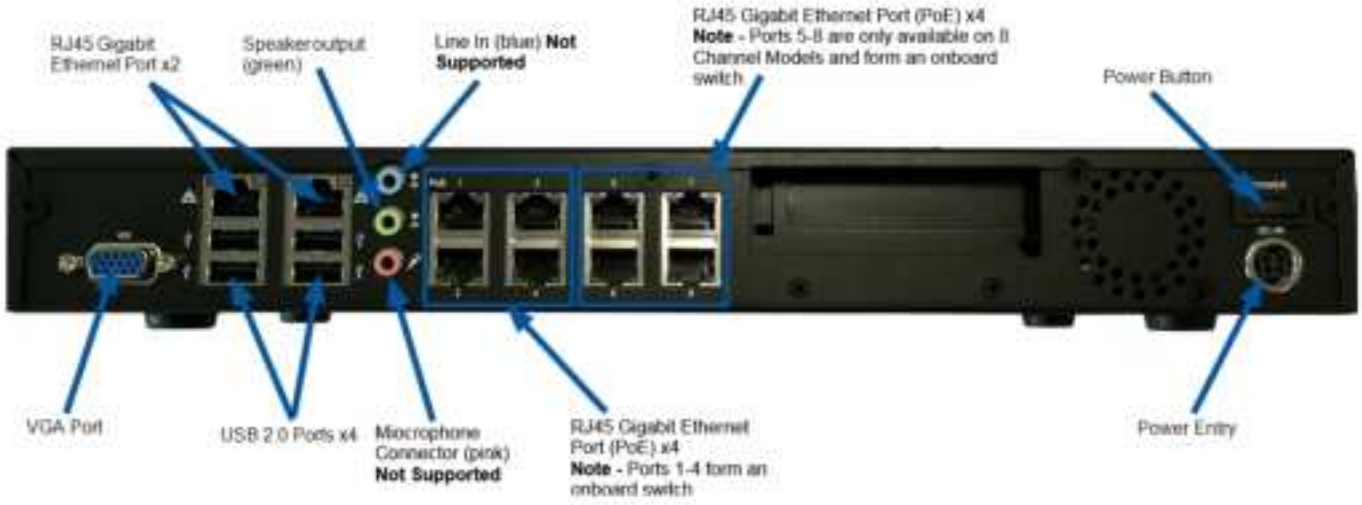
VideoEdge Micro NVR

Table 25 VideoEdge Micro NVR Configuration

Connector Type	Quantity
USB 2.0 Ports	4
3.5mm Microphone Socket (Not Supported)	2
3.5mm Headphone Socket (Not Supported)	1
3.5mm Line In Socket (Not Supported)	1
3.5mm Speaker Out Socket	1
RJ45 Gigabit Ethernet Ports	2
RJ45 PoE Gigabit Ethernet Ports	4/8
VGA Ports	1

Figure 105 VideoEdge Micro NVR Front Panel

Figure 106 VideoEdge Micro NVR Rear Panel



VideoEdge Desktop Hybrid NVR

Table 26 VideoEdge Desktop Hybrid NVR Configuration

Figure 107 16 VideoEdge Desktop Hybrid NVR Front Panel

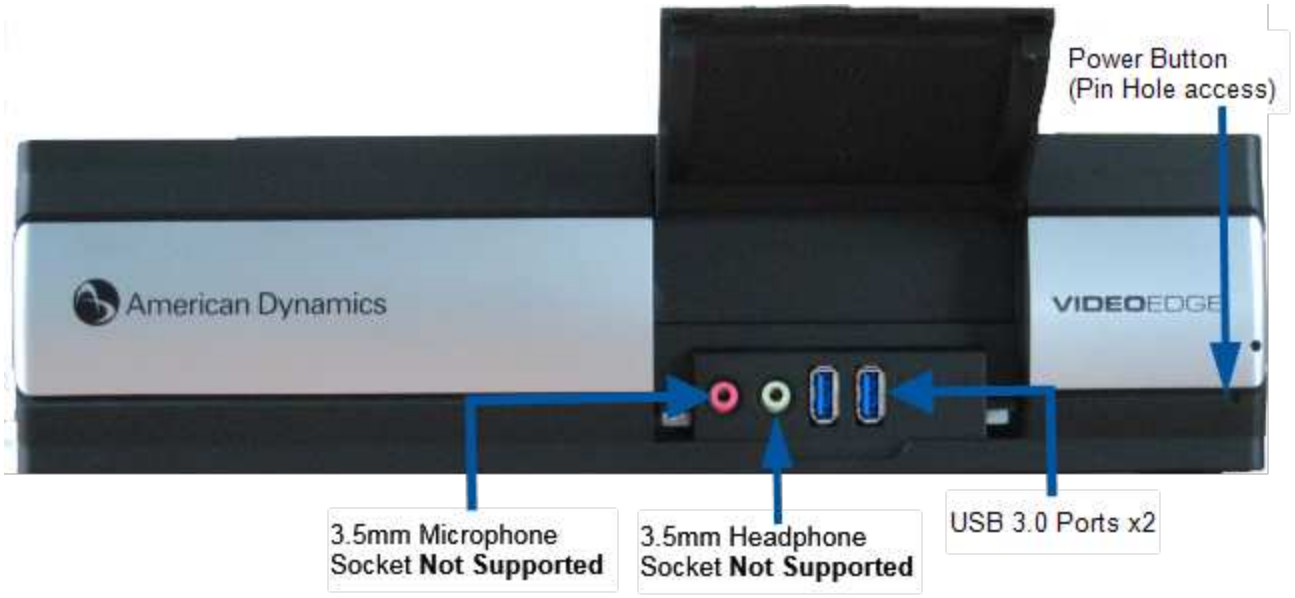
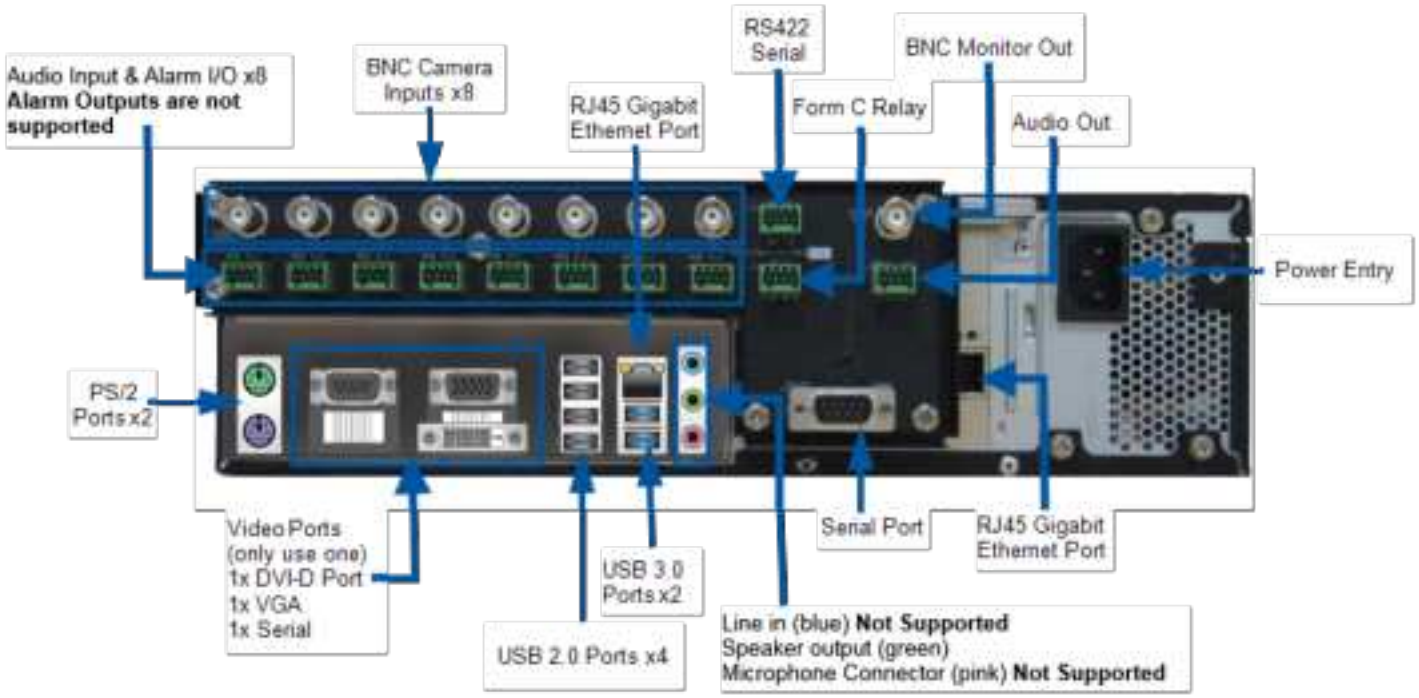


Figure 108 VideoEdge Desktop Hybrid NVR Rear Panel



VideoEdge Desktop NVR

Table 27 VideoEdge Desktop NVR Configuration

Connector Type	Quantity
USB 2.0 Ports	6
USB 3.0 Ports	4
3.5mm Microphone Socket (Not Supported)	2
3.5mm Headphone Socket (Not Supported)	1
3.5mm Line In Socket (Not Supported)	1
3.5mm Speaker Out Socket	1
PS/2 Ports	2
VGA Ports	1
Serial Ports	1
DVI-D Ports	1
RJ45 Gigabit Ethernet Ports	2

Figure 109 VideoEdge Desktop NVR Front Panel

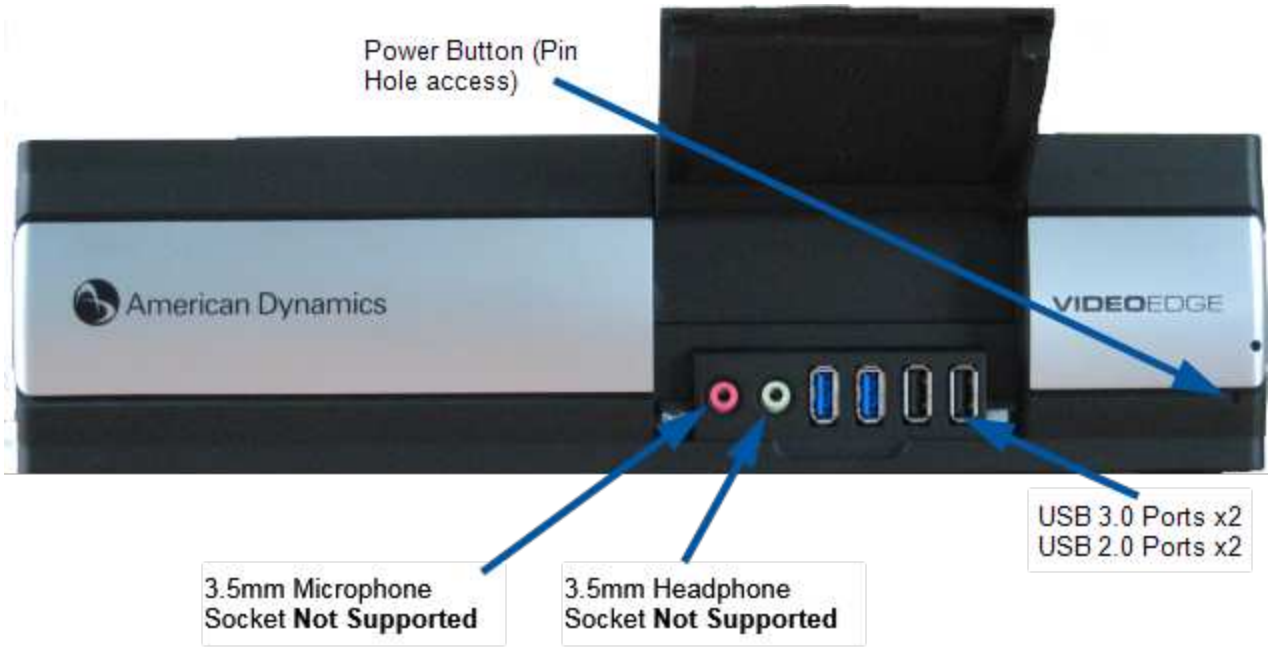
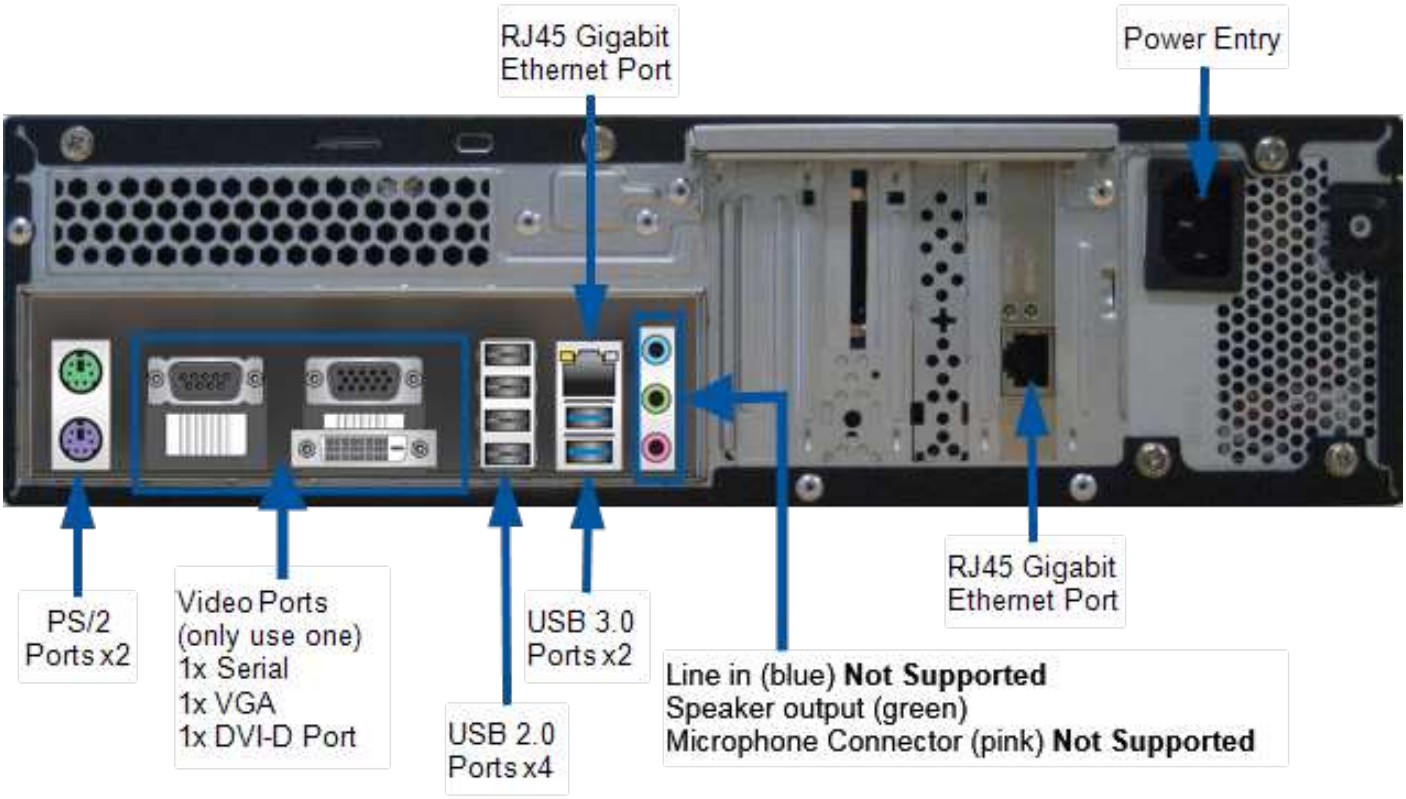


Figure 110 VideoEdge Desktop NVR Rear Panel



VideoEdge 1U NVR

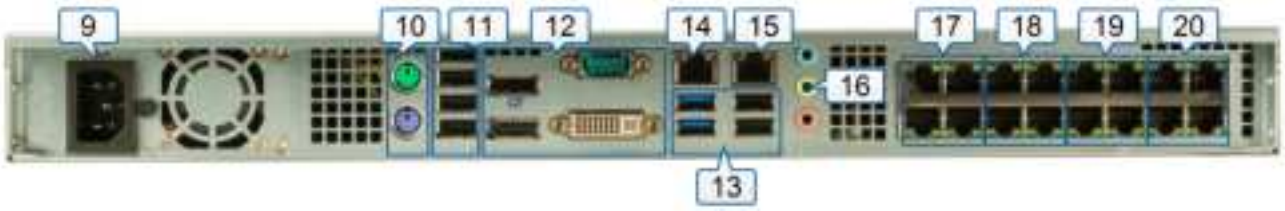
Table 28 VideoEdge 1U NVR Configuration

Connector Type	Quantity
USB 2.0 Ports	7
USB 3.0 Ports	2
3.5mm Microphone Socket (Not Supported)	2
3.5mm Line In Socket (Not Supported)	1
3.5mm Speaker Out Socket	1
PS/2 Ports	2
Serial Ports	1
DVI-I Ports	1
DisplayPort Ports	2
RJ45 Gigabit Ethernet Ports	18

Figure 111 VideoEdge 1U NVR with Front Panel

Figure 112 VideoEdge 1U NVR without Front Panel

Figure 113 VideoEdge 1U NVR Rear Panel



Number	Description
1	Bezel (removable)
2	Bezel Lock (1x key located behind Bezel)
3	USB port (1 x 2.0)
4	Factory Reset Button
5	Power Indicator LEDs
6	Power button
7	PoE Status Indicator LEDs
8	Drives (removable)
9	Power Connector (1 x 100 ~ 240VAC)
10	PS/2 Ports (2 x Legacy PS/2 Option)
11	USB Ports (4 x 2.0)
12	Video Ports (2 x DisplayPort, 1x Serial Port, 1 x DVI-I, Only use one)
13	USB Ports (2 x 3.0, 2 x 2.0)
14	1 GbE Network Port (1x eth0 LAN1 Corporate)
15	1 GbE Network Port (1x eth1 LAN2 Camera)
16	Speaker Out Socket (1x 3.5mm Green)
17	10mb/100mb POE network ports (4x PoE eth2 for 1 ~ 4 Cameras)
18	10mb/100mb POE network ports (4x PoE eth2 for 5 ~ 8 Cameras)
19	10mb/100mb POE network ports (4x PoE eth2 for 9 ~ 12 Cameras)
20	10mb/100mb POE network ports (4x PoE eth2 for 13 ~ 16 Cameras)

VideoEdge 2U Hybrid NVR

Table 29 VideoEdge 2U Hybrid NVR Configuration

Connector Type	Quantity
USB 2.0 Ports	6
USB 3.0 Ports	2
USB C Port (Not Supported)	1
PS/2 Mouse / Keyboard Combo Port	1
3.5mm Microphone Socket (Not Supported)	1
3.5mm Line In Socket (Not Supported)	1
3.5mm Speaker Out Socket	1
DVI-D Ports	1
VGA Ports	1
RJ45 Gigabit Ethernet Ports	2
BNC Video Inputs	16
BNC Video Through Loop Connectors	16
BNC Monitor Outputs	2
Audio Inputs	16
Alarm Inputs	18
Alarm Outputs (Not Supported)	16
Form C Relay Output	1
Serial Ports 2	2
RS422 Ports 1	1

Figure 114 VideoEdge 2U Hybrid NVR Front Panel

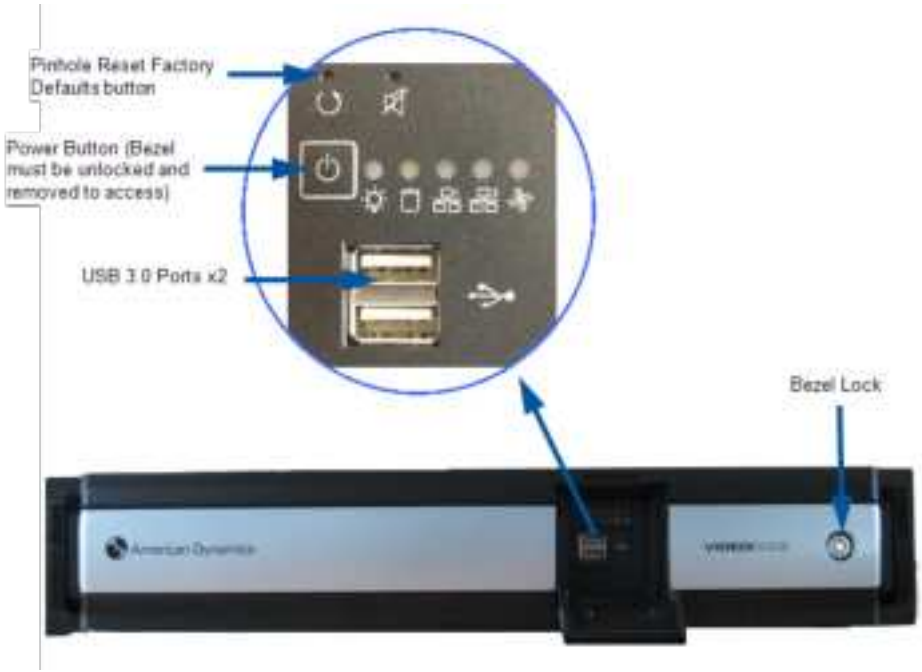
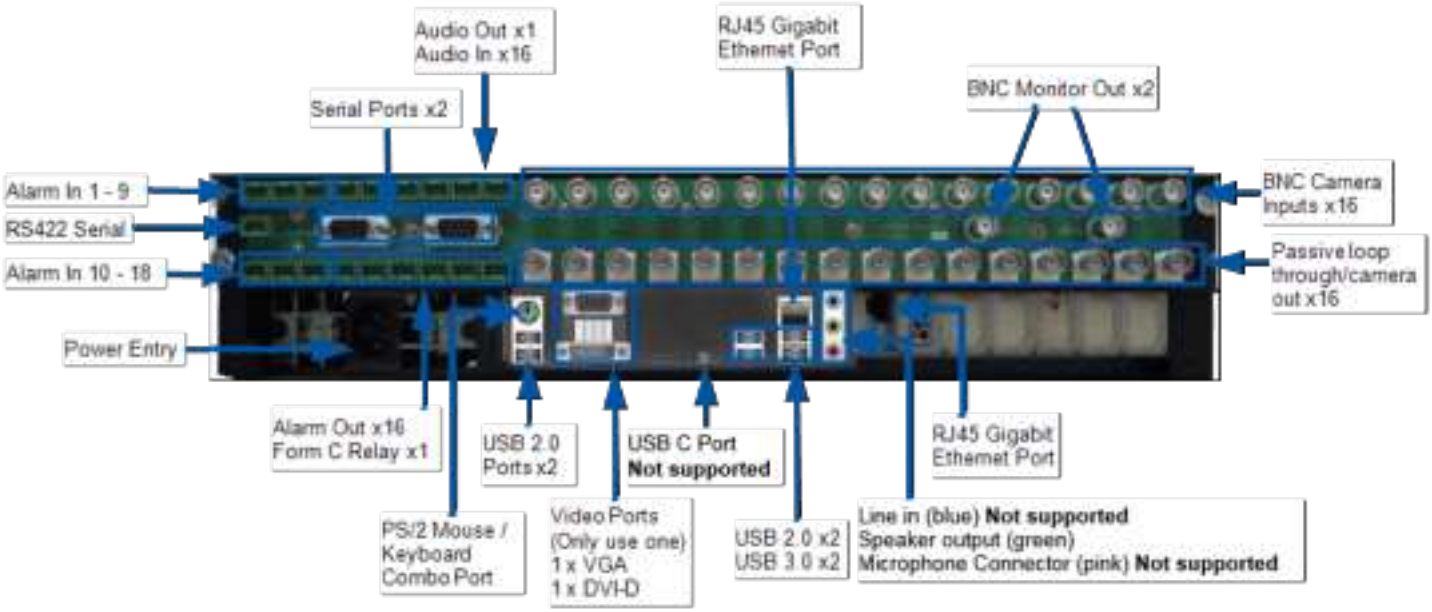


Figure 115 VideoEdge 2U Hybrid NVR Rear Panel



VideoEdge 2U NVR

Table 30 VideoEdge 2U NVR Configuration

Connector Type	Quantity
USB 2.0 Ports	4
USB 3.0 Ports	4
USB C Port (Not Supported)	1
3.5mm Microphone Socket (Not Supported)	1
3.5mm Line In Socket (Not Supported)	1
3.5mm Speaker Out Socket	1
PS/2 Mouse/Keyboard Combo Port	1
DVI-D Ports	1
VGA Ports	1
RJ45 Gigabit Ethernet Ports	4

Figure 116 VideoEdge 2U NVR Front Panel

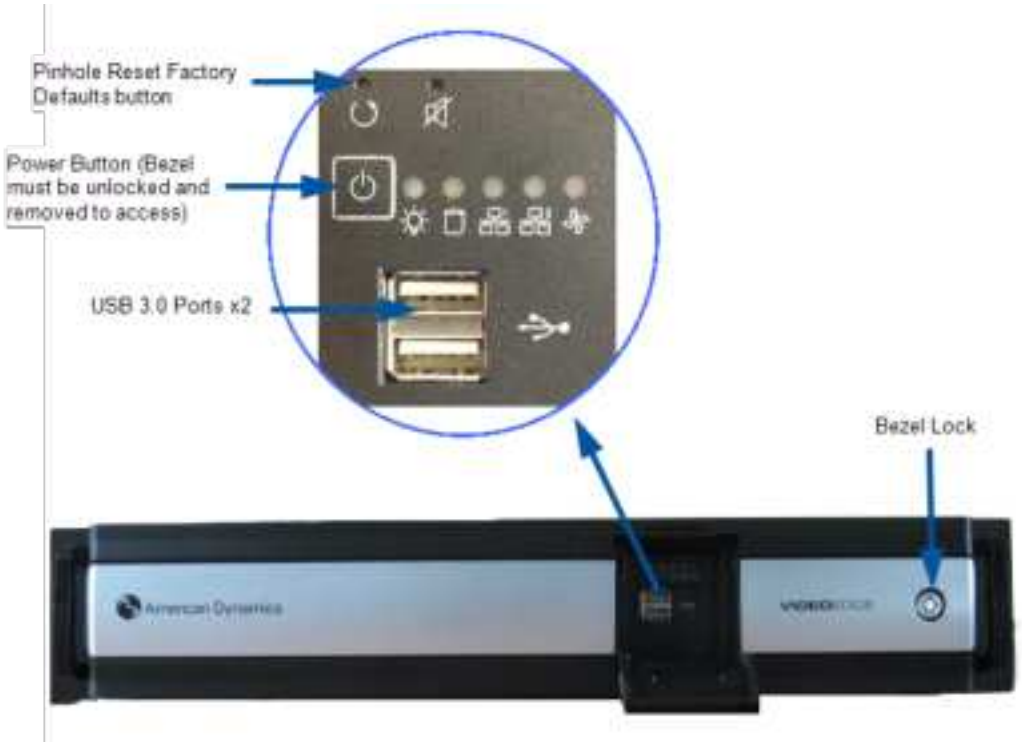
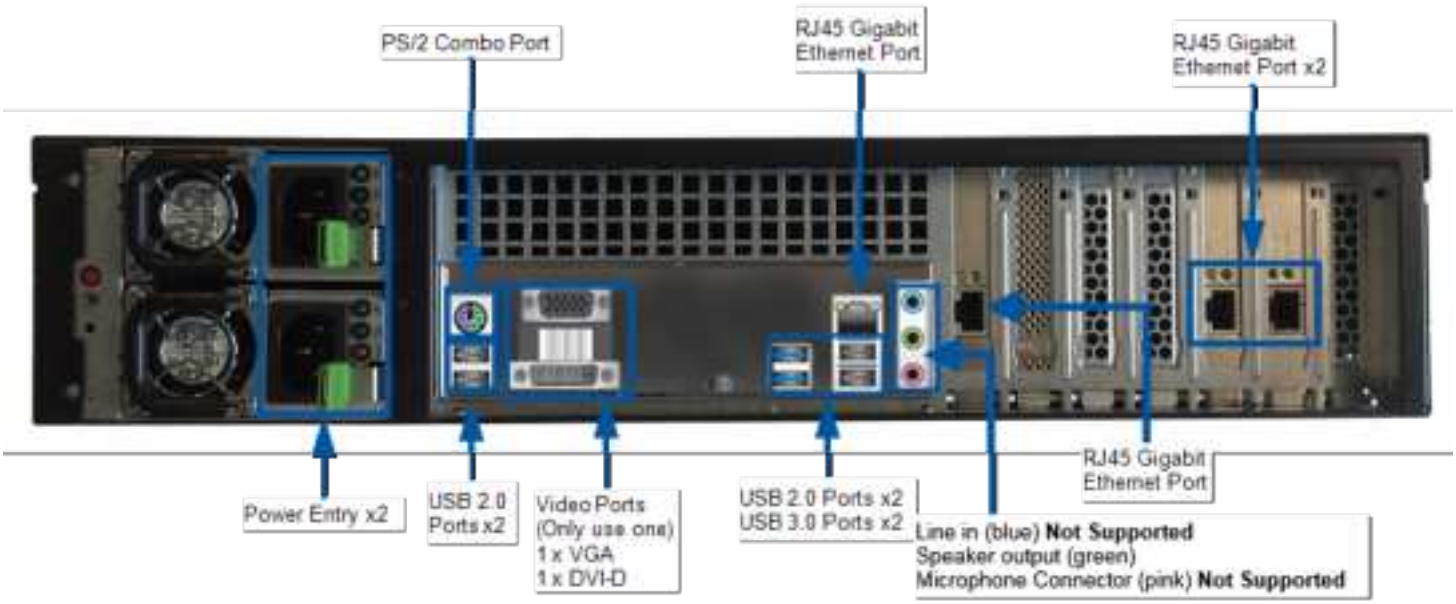


Figure 117 VideoEdge 2U NVR Rear Panel



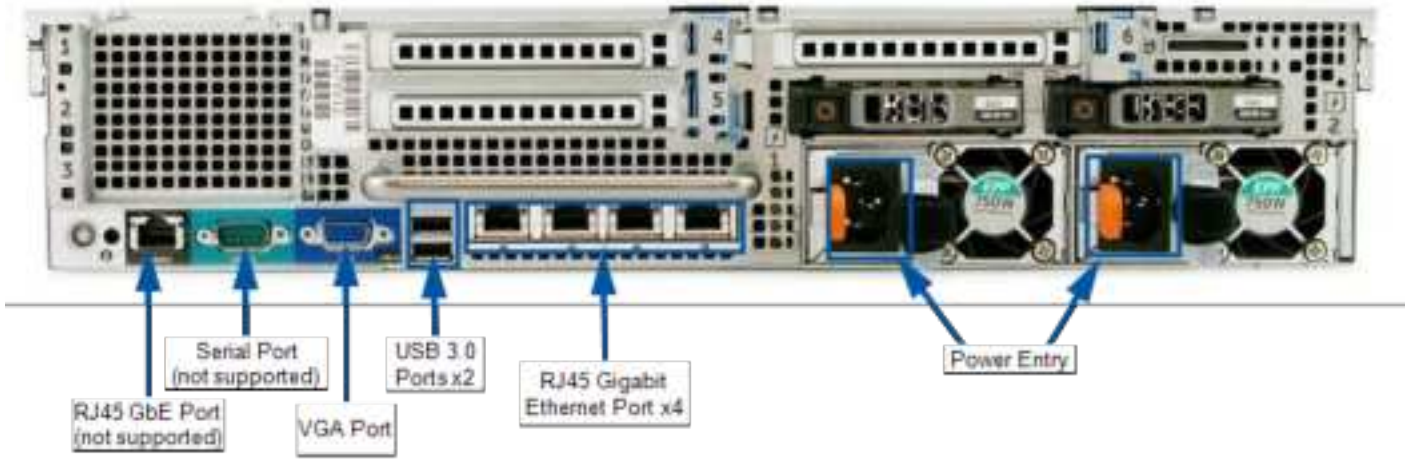
VideoEdge 2U NVR server

Table 31 VideoEdge 2U NVR Server Configuration

Connector Type	Quantity
USB 2.0 Ports	1
USB 3.0 Ports	2
VGA Ports	1
RJ45 Gigabit Ethernet Ports	5

Figure 118 VideoEdge 2U NVR Server Front Panel

Figure 119 VideoEdge 2U NVR Server Rear Panel



VideoEdge 3U Hybrid NVR

Figure 120 VideoEdge 3U Hybrid NVR Configuration

Connector Type	Quantity
USB 2.0 Ports	4
USB 3.0 Ports	4
3.5mm Microphone Socket (Not Supported)	1
3.5mm Line In Socket (Not Supported)	1
3.5mm Speaker Out Socket	1
PS/2 Mouse/Keyboard Combo Port	1
DVI-D Ports	1
VGA Ports	1
RJ45 Gigabit Ethernet Ports	2
BNC Video Inputs	32
BNC Video Loop Through Connectors	32
BNC Monitor Outputs	2
Audio Inputs	32
Alarm Inputs	36
Alarm Outputs (Supported from VideoEdge 5.1 onwards)	32
Form C Relay Output	2
Serial Ports	2
RS422 Ports	1

Figure 121 VideoEdge 3U Hybrid NVR Front Panel

Figure 122 VideoEdge 3U Hybrid NVR Rear Panel

Number	Description
1	Factory Reset Button (1x Pin-Hole Under Front Flap)
2	Power Button (1x Under Front Flap)
3	USB Ports (2x 3.0 Under Front Flap)
4	Bezel Lock (1x Key Located Behind Bezel)
5	Power Connector (1x 100~240VAC)
6	PS/2 Mouse/Keyboard Combo Port
7	USB Ports (2x 2.0)
8	Video Ports (1 x VGA or 1 x DVI-D, Only Use One)
9	USB C port (Not supported)
10	1GbE Network Port (1x eth0 LAN1 Corporate)
11	USB Ports (2x 3.0, 2 x 2.0)
12	Audio (Line In: Blue; Line Out: Green; Microphone: Pink)
13	1GbE Network Port (1x eth1 LAN2 Camera)
14	Alarm In (9x) [28 – 36] & Alarm Out (16x) [17 – 32] & Form C Relay (1x)
15	Alarm In (9x) [19 – 27] & Audio Out (1x) [2] & Audio In (16x) [17 – 32]
16	RS422 Port (1x)
17	Serial Connector (2x)
18	Alarm In (9x) [10 – 18] & Alarm Out (16x) [1 – 16] & Form C Relay (1x)
19	Alarm In (9x) [1 – 9] & Audio Out (1x) [1] & Audio In (16x) [1 – 16]
20	BNC Video (01~16 Analog Camera Inputs)
21	BNC Video (01~16 Passive Loop Through/Camera Out)
22	BNC Video (17~32 Analog Camera Inputs)
23	BNC Video (17~32) Passive Loop Through/Camera Out)
24	BNC Video (2x Monitor Outputs)

Connector Pin Outs

Table 32 VideoEdge Desktop Hybrid NVR Alarm and Audio Input Pin Outs

Alarm and Audio Input Pin Outs	
Pin No.	**Assignment**
AU1-I	Audio Input 1
AL1-I	Alarm Input 1
AL1-O	Alarm Output 1
G	Ground
AU2-I	Audio Input 2
AL2-I	Alarm Input 2
AL2-O	Alarm Output 2
G	Ground
AU3-I	Audio Input 3
AL3-I	Alarm Input 3
AL3-O	Alarm Output 3
G	Ground
AU4-I	Audio Input 4
AL4-I	Alarm Input 4
AL4-O	Alarm Output 4
G	Ground
AU5-I	Audio Input 5
AL5-I	Alarm Input 5
AL5-O	Alarm Output 5
G	Ground
AU6-I	Audio Input 6
AL6-I	Alarm Input 6
AL6-O	Alarm Output 6
G	Ground
AU7-I	Audio Input 7
AL7-I	Alarm Input 7
AL7-O	Alarm Output 7
G	Ground
AU8-I	Audio Input 8

Alarm and Audio Input Pin Outs	
Pin No.	**Assignment**
AL8-I	Alarm Input 8
AL8-O	Alarm Output 8
G	Ground

Note:
Alarm Outputs are supported from VideoEdge 5.1.

Table 33 VideoEdge Desktop Hybrid NVR Audio Output Pin Outs

Audio Output Pin Outs	
Pin No.	**Assignment**
G	Ground
S	Signal Out
G	Ground
G	Ground

Table 34 VideoEdge Desktop Hybrid NVR Form C Relay Pin Outs

Form C Relay Pin Outs	
Pin No.	**Assignment**
C	Common
NC	Normally Closed
NO	Normally Open
G	Ground

Table 35 VideoEdge Desktop Hybrid NVR RS422 Pin Outs

RS422 Pin Outs	
Pin No.	**Assignment**
RX +	Receive +
RX -	Receive -
TX -	Transmit -
TX +	Transmit +

Table 36 VideoEdge 2U Hybrid NVR Alarm Pin Outs

Alarm In		Alarm Out	
Pin No.	Assignment	Pin No.	Assignment
1	Input 1	1	Output 1
2	Input 2	2	Output 2
G	Ground	G	Ground
3	Input 3	3	Output 3
4	Input 4	4	Output 4
5	Input 5	5	Output 5
G	Ground	G	Ground
6	Input 6	6	Output 6
7	Input 7	7	Output 7
8	Input 8	8	Output 8
G	Ground	G	Ground
9	Input 9	9	Output 9
10	Input 10	10	Output 10
11	Input 11	11	Output 11
G	Ground	G	Ground
12	Input 12	12	Output 12
13	Input 13	13	Output 13
14	Input 14	14	Output 14
G	Ground	15	Output 15
15	Input 15	16	Output 16
16	Input 16	N/A	N/A
17	Input 17	N/A	N/A
G	Ground	N/A	N/A
18	Input 18	N/A	N/A

Note:
Alarm Outputs are not supported.

Table 37 VideoEdge 2U Hybrid NVR Audio Pin Outs

Audio Pin Outs	
Pin No.	**Assignment**
Audio Out	
S	Signal Out
G	Ground
Audio In	
G	Ground
1	Input 1
2	Input 2
3	Input 3
G	Ground
4	Input 4
5	Input 5
6	Input 6
G	Ground
7	Input 7
8	Input 8
9	Input 9
G	Ground
10	Input 10
11	Input 11
12	Input 12
G	Ground
13	Input 13
14	Input 14
15	Input 15
G	Ground
16	Input 16

Table 38 VideoEdge 2U Hybrid NVR Form C Relay Pin Outs

Form C Relay Pin Outs	
Pin No.	**Assignment**
G	Ground
NO	Normally Open
C	Common
NC	Normally Closed

Table 39 VideoEdge 2U Hybrid NVR RS422 Pin Outs

RS422 Pin Outs	
Pin No.	**Assignment**
RX +	Receive +
RX -	Receive -
TX -	Transmit -
TX +	Transmit +

Table 40 VideoEdge 3U Hybrid NVR Alarm Pin Outs

Alarms In		Alarms Out	
Pin No.	**Assignment**	**Pin No.**	**Assignment**
1	Input 1	1	Output 1
2	Input 2	2	Output 2
G	Ground	G	Ground
3	Input 3	3	Output 3
4	Input 4	4	Output 4
5	Input 5	5	Output 5
G	Ground	G	Ground
6	Input 6	6	Output 6
7	Input 7	7	Output 7
8	Input 8	8	Output 8
G	Ground	G	Ground
9	Input 9	9	Output 9
10	Input 10	10	Output 10
11	Input 11	11	Output 11
G	Ground	G	Ground

Alarms In		Alarms Out	
Pin No.	Assignment	Pin No.	Assignment
12	Input 12	12	Output 12
13	Input 13	13	Output 13
14	Input 14	14	Output 14
G	Ground	15	Output 15
15	Input 15	16	Output 16
16	Input 16	17	Output 17
17	Input 17	18	Output 18
G	Ground	G	Ground
18	Input 18	19	Output 19
19	Input 19	20	Output 20
20	Input 20	21	Output 21
G	Ground	G	Ground
21	Input 21	22	Output 22
22	Input 22	23	Output 23
23	Input 23	24	Output 24
G	Ground	G	Ground
24	Input 24	25	Output 25
25	Input 25	26	Output 26
26	Input 26	27	Output 27
G	Ground	G	Ground
27	Input 27	28	Output 28
28	Input 28	29	Output 29
29	Input 29	30	Output 30
G	Ground	31	Output 31
30	Input 30	32	Output 32
31	Input 31	N/A	N/A
32	Input 32	N/A	N/A
G	Ground	N/A	N/A
33	Input 33	N/A	N/A
34	Input 34	N/A	N/A
35	Input 35	N/A	N/A

Alarms In		Alarms Out	
Pin No.	Assignment	Pin No.	Assignment
G	Ground	N/A	N/A
36	Input 36	N/A	N/A

Note:
Alarm Outputs are supported from VideoEdge 5.1.

Table 41 VideoEdge 3U Hybrid NVR Audio Pin Outs

Audio Pin Outs	
Pin No.	**Assignment**
Audio Out 1	
S	Signal Out
G	Ground
Audio In	
G	Ground
1	Input 1
2	Input 2
3	Input 3
G	Ground
4	Input 4
5	Input 5
6	Input 6
G	Ground
7	Input 7
8	Input 8
9	Input 9
G	Ground
10	Input 10
11	Input 11
12	Input 12
G	Ground
13	Input 13
14	Input 14
15	Input 15
G	Ground
16	Input 16
Alarm Out 2	
S	Signal Out
G	Ground
Audio In	

Audio Pin Outs	
Pin No.	**Assignment**
G	Ground
17	Input 17
18	Input 18
19	Input 19
G	Ground
20	Input 20
21	Input 21
22	Input 22
G	Ground
23	Input 23
24	Input 24
25	Input 25
G	Ground
26	Input 26
27	Input 27
28	Input 28
G	Ground
29	Input 29
30	Input 30
31	Input 31
G	Ground
32	Input 32

Table 42 VideoEdge 3U Hybrid NVR Form C Relay Pin Outs

Form C Relay Pin Outs	
Pin No.	**Assignment**
G	Ground
NO	Normally Open
C	Common
NC	Normally Closed

Table 43 VideoEdge 3U Hybrid NVR RS422 Pin Outs

RS422 Pin Outs	
Pin No.	**Assignment**
RX +	Receive +
RX -	Receive -
TX -	Transmit -
TX +	Transmit +

End User License Agreement (EULA)

Use of the software is subject to the following End User License:

End User License Agreement (EULA)

IMPORTANT - READ THIS END-USER LICENSE AGREEMENT ("EULA") CAREFULLY BEFORE OPENING THE DISK PACKAGE, DOWNLOADING THE SOFTWARE OR INSTALLING, COPYING OR OTHERWISE USING THE SOFTWARE.

THIS EULA IS A LEGAL AGREEMENT BETWEEN YOU AND SENSORMATIC ELECTRONICS, LLC ("TYCO"), WHICH SOFTWARE INCLUDES COMPUTER SOFTWARE AND MAY INCLUDE MEDIA, PRINTED MATERIALS, AND "ON-LINE" OR ELECTRONIC DOCUMENTATION (COLLECTIVELY, THE "SOFTWARE"). BY BREAKING THE SEAL ON THIS PACKAGE, DOWNLOADING THE SOFTWARE OR INSTALLING, COPYING OR OTHERWISE USING THE SOFTWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS EULA. IF YOU DO NOT AGREE TO ALL OF THE TERMS AND CONDITIONS OF THIS EULA, DO NOT OPEN, DOWNLOAD, INSTALL, COPY OR OTHERWISE USE THE SOFTWARE.

1. SCOPE OF LICENSE. The Software may include computer code, program files and any associated media, hardware or software keys, printed material and electronic documentation. The Software may be provided to you pre-installed on a storage device (the media) as part of a computer system or other hardware or device ("System"). The Software is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. All title and intellectual property rights in and to the Software (including but not limited to any images, photographs, and text incorporated into the Software), the accompanying printed materials, and any copies of the Software, are owned by Tyco and/or its suppliers. The Software is licensed, not sold. All rights not expressly granted under this EULA are reserved by Tyco and its suppliers.

2. GRANT OF LICENSE. This EULA grants you the following rights on a non-exclusive basis:

a. General. This EULA permits you to use the Software for which you have purchased this EULA. Once you have purchased licenses for the number of copies of the Software that you require, you may use the Software and accompanying material provided that you install and use no more than the licensed number of copies at one time. The Software is only licensed for use with specified Licensor-supplied Systems. If the Software is protected by a software or hardware key or other device, the Software may be used on any computer on which the key is installed. If the key locks the Software to a particular System, the Software may only be used on that System.

b. Locally Stored Components. The Software may include a software code component that may be stored and operated locally on one or more devices. Once you have paid the required license fees for these devices (as determined by Tyco in its sole discretion), you may install and/or use one copy of such component of the Software on each of the devices as licensed by Tyco. You may then use, access, display, run or otherwise interact with ("use") such component of the Software in connection with operating the device on which it is installed solely in

the manner set forth in any accompanying documentation or, in the absence of such, solely in the manner contemplated by the nature of the Software.

c. Remotely Stored Components. The Software may also include a software code component for operating one or more devices remotely. You may install and/or use one copy of such component of the Software on a remote storage device on an internal network with all of the devices and may operate such component with each device over the internal network solely in the manner set forth in any accompanying documentation or, in the absence of such, solely in the manner contemplated by the nature of the Software; provided however, you must still acquire the required number of licenses for each of the devices with which such component is to be operated.

d. Embedded Software/Firmware. The Software may also include a software code component that is resident in a device as provided by Tyco for operating that device. You may use such component of the Software solely in connection with the use of that device, but may not retrieve, copy or otherwise transfer that software component to any other media or device without Tyco's express prior written authorization.

e. Backup Copy. You may make a back-up copy of the Software (other than embedded software) solely for archival purposes, which copy may only be used to replace a component of the Software for which you have current valid license. Except as expressly provided in this EULA, you may not otherwise make copies of the Software, including the printed materials.

3. OTHER RIGHTS AND LIMITATIONS. Your use of the Software is subject to the following additional limitations. Failure to comply with any of these restrictions will result in automatic termination of this EULA and will make available to Tyco other legal remedies.

a. Limitations on Reverse Engineering and Derivative Works. You may not reverse engineer, decompile, or disassemble the Software, and any attempt to do so shall immediately terminate this EULA - except and only to the extent that such activity may be expressly permitted by applicable law notwithstanding this limitation. You may not make any changes or modifications to any portion of the Software, or create any derivative works, without the written permission of an officer of Tyco (except as provided in Section 3(f) of this EULA with respect to "open source" software). You may not remove any proprietary notices, marks or labels from the Software. You shall institute reasonable measures to ensure compliance with the terms and conditions of this EULA by your personnel and agents.

b. Copyright Notices. You must maintain all copyright notices on all copies of the Software.

c. Transfer. You may only transfer your rights under this EULA (i) as part of a permanent sale or transfer of all of the devices for which the Software is licensed as applicable; (ii) if you transfer all of the Software (including all component parts, the media and printed materials, any upgrades and this EULA); (iii) if you do not retain any copies of any portion of the Software; (iv) if the recipient agrees to the terms of this EULA; and (v) if the Software is an upgrade, such transfer must also include all prior versions of the Software. You agree that failure to meet all of these conditions renders such transfer null and void.

d. Termination. Without prejudice to any other rights, Tyco may terminate this EULA if you fail to comply with the terms and conditions herein. In such event, you must immediately destroy all copies of the Software and all of

its component parts. To the extent the Software is embedded in hardware or firmware, you will provide prompt access to Tyco or its representative to remove or lock Software features or functionality as Tyco determines.

e. Subsequent EULA. Tyco may also supersede this EULA with a subsequent EULA pursuant to providing you with any future component, release, upgrade or other modification or addition to the Software. Similarly, to the extent that the terms of this EULA conflict with any prior EULA or other agreement between you and Tyco regarding the Software, the terms of this EULA shall prevail.

f. Incorporation of "Open Source" and other Third Party Software. Portions of the Software may be subject to certain thirty party license agreements governing the use, copying, modification, redistribution and warranty of those portions of the Software, including what is commonly known as "open source" software. A copy of each applicable third party license can be found in the file README.TXT or other documentation accompanying the Software. By using the Software you are also agreeing to be bound to the terms of such third party licenses. If provided for in the applicable third party license, you have a right to receive source code for such software for use and distribution in any program that you create, so long as you in turn agree to be bound to the terms of the applicable third party license, and your programs are distributed under the terms of that license. A copy of such source code may be obtained free of charge by contacting your Tyco representative.

g. Trademarks. This EULA does not grant you any rights in connection with any trademarks or service marks of Tyco, its affiliates or its suppliers.

h. Rental. You may not sublicense, rent, lease or lend the Software. You may not make it available to others or post it on a server or web site or otherwise distribute it.

i. Software Keys. The hardware/software key, where applicable, is your proof of license to exercise the rights granted herein and must be retained by you. Lost or stolen keys will not be replaced.

j. Demonstration and Evaluation Copies. A demonstration or evaluation copy of the Software is covered by this EULA; provided that the licenses contained herein shall expire at the end of the demonstration or evaluation period.

k. Registration of Software. The Software may require registration with Tyco prior to use. If you do not register the Software, this EULA is automatically terminated and you may not use the Software.

l. Additional Restrictions. The Software may be subject to additional restrictions and conditions on use as specified in the documentation accompanying such Software, which additional restrictions and conditions are hereby incorporated into and made a part of this EULA.

m. Upgrades and Updates. To the extent Tyco makes them available, Software upgrades and updates may only be used to replace all or part of the original Software that you are licensed to use. Software upgrades and updates do not increase the number of copies licensed to you. If the Software is an upgrade of a component of a package of Software programs that you licensed as a single product, the Software may be used and transferred only as part of that single product package and may not be separated for use on more than one computer or System. Software upgrades and updates downloaded free of charge via a Tyco authorized World Wide Web or FTP site may be used to upgrade multiple Systems provided that you are licensed to use the original Software on those Systems.

n. Tools and Utilities. Software distributed via a Tyco-authorized World Wide Web or FTP site (or similar Tyco-authorized distribution means) as a tool or utility may be copied and installed without limitation provided that the Software is not distributed or sold and the Software is only used for the intended purpose of the tool or utility and in conjunction with Tyco products. All other terms and conditions of this EULA continue to apply.

o. Government Regulations. The Software may be subject to additional restrictions and conditions on use as specified by local, state, and/or federal laws, rules and regulations. It is up to you to determine what law, rules and/or regulations apply to your use of the Software, and to comply with such laws, rules and/or regulations when using the Software.

4. EXPORT RESTRICTIONS. You agree that you will not export, re-export or transfer any portion of the Software, or any direct product thereof (the foregoing collectively referred to as the "Restricted Components"), to IRAN, NORTH KOREA, SYRIA, CUBA and SUDAN, including any entities or persons in those countries, either directly or indirectly ("Tyco's Position"). You also agree that you will not export, re-export or transfer the Restricted Components to any other countries except in full compliance with all applicable governmental requirements, including but not limited to applicable economic sanctions and constraints administered by the U.S. Treasury Department and applicable export control measures administered by the U.S. Department of Commerce and U.S. Department of State, any other U.S. government agencies, and measures administered by the European Union or the government agencies of any other countries. Any violation by you of the applicable laws or regulations of the U.S. or any other government, or where you breach Tyco's Position notwithstanding whether or not this is contrary to any aforementioned applicable laws or regulations, will result in automatic termination of this EULA.

5. U.S. GOVERNMENT RESTRICTED RIGHTS. The Software is Commercial Computer Software provided with "restricted rights" under Federal Acquisition Regulations and agency supplements to them. Any use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFAR 255.227-7013 et. seq. or 252.211-7015, or subparagraphs (a) through (d) of the Commercial Computer Software Restricted Rights at FAR 52.227-19, as applicable, or similar clauses in the NASA FAR Supplement. Contractor/manufacturer is Sensormatic Electronics, LLC, 6 Technology Park Drive, Westford, MA 01886.

6. LIMITED WARRANTY.

a. Warranty. Tyco warrants that the recording medium on which the Software is recorded, hardware key, and the documentation provided with it, will be free of defects in materials and workmanship under normal use for a period of ninety (90) days from the date of delivery to the first user. Tyco further warrants that for the same period, the Software provided on the recording medium under this license will substantially perform as described in the user documentation provided with the product when used with specified hardware. THE FOREGOING EXPRESS WARRANTY REPLACES AND IS IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING BUT NOT LIMITED TO, ANY IMPLIED OR OTHER WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT OR NON-MISAPPROPRIATION OF INTELLECTUAL PROPERTY RIGHTS OF A THIRD PARTY, CUSTOM, TRADE, QUIET ENJOYMENT, ACCURACY OF INFORMATIONAL CONTENT, OR SYSTEM INTEGRATION. TYCO

MAKES NO WARRANTY THAT ANY PORTION OF THE SOFTWARE WILL OPERATE ERROR-FREE, FREE OF ANY SECURITY DEFECTS OR IN AN UNINTERRUPTED MANNER. TYCO SHALL NOT BE RESPONSIBLE FOR PROBLEMS CAUSED BY CHANGES IN THE OPERATING CHARACTERISTICS OF THE DEVICE(S) UPON WHICH THE SOFTWARE IS OPERATING, OR FOR PROBLEMS IN THE INTERACTION OF THE SOFTWARE WITH NON-TYCO SOFTWARE OR HARDWARE PRODUCTS. TYCO NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON PURPORTING TO ACT ON ITS BEHALF TO MODIFY OR TO CHANGE THIS WARRANTY, NOR TO ASSUME FOR IT ANY OTHER WARRANTY OR LIABILITY CONCERNING THIS SOFTWARE. THE WARRANTY MADE BY TYCO MAY BE VOIDED BY ABUSE OR MISUSE. THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS UNDER MANDATORY LAW THAT VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

b. Exclusive Remedy. Tyco's entire liability and your exclusive remedy under the warranty set forth in this Section 6 will be, at Tyco's option, to (i) attempt to correct Software errors with efforts Tyco believes suitable to the problem, (ii) replace at no cost the recording medium, Software or documentation with functional equivalents as applicable, or (iii) refund a pro-rated portion of the license fee paid for such Software (less depreciation based on a five-year life expectancy) and terminate this EULA, provided, in each case, that Tyco is notified in writing of all warranty problems during the applicable warranty period. Any replacement item will be warranted for the remainder of the original warranty period. No remedy is provided for failure of the Software if such failure is the result of accident, abuse, alteration or misapplication with respect to the Software or any hardware on which it is loaded. Warranty service or assistance is provided at the original point of purchase.

7. LIMITATION OF LIABILITY & EXCLUSION OF DAMAGES.

a. LIMITATION OF LIABILITY. IN NO EVENT WILL TYCO'S AGGREGATE LIABILITY (INCLUDING, BUT NOT LIMITED TO, LIABILITY FOR NEGLIGENCE, STRICT LIABILITY, BREACH OF CONTRACT, MISREPRESENTATION AND OTHER CONTRACT OR TORT CLAIMS) ARISING FROM OR RELATED TO THIS EULA, OR THE USE OF THE SOFTWARE, EXCEED THE AMOUNT OF FEES YOU PAID TO TYCO OR ITS RESELLER FOR THE SOFTWARE THAT GIVES RISE TO SUCH LIABILITY.

b. EXCLUSION OF OTHER DAMAGES. UNDER NO CIRCUMSTANCES SHALL TYCO OR ANY OF ITS RESELLERS OR LICENSORS BE LIABLE FOR ANY OF THE FOLLOWING: (I) THIRD PARTY CLAIMS; (II) LOSS OR DAMAGE TO ANY SYSTEMS, RECORDS OR DATA, OR LIABILITIES RELATED TO A VIOLATION OF AN INDIVIDUAL'S PRIVACY RIGHTS; OR (III) INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, PUNITIVE, RELIANCE, OR COVER DAMAGES (INCLUDING LOST PROFITS AND LOST SAVINGS), IN EACH CASE EVEN IF TYCO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. YOU ARE SOLELY RESPONSIBLE AND LIABLE FOR VERIFYING THE SECURITY, ACCURACY AND ADEQUACY OF ANY OUTPUT FROM THE SOFTWARE, AND FOR ANY RELIANCE THEREON. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, OR THE LIMITATION ON HOW LONG AN IMPLIED WARRANTY LASTS, SO SOME OF THE ABOVE LIMITATIONS MAY APPLY TO YOU ONLY TO THE EXTENT PERMITTED BY THOSE LAWS.

8. GENERAL. If any provision of this EULA is found to be unlawful, void, or for any reason unenforceable, then that provision shall be severed from this EULA and shall not affect the validity and enforceability of the remaining provisions. You should retain proof of the license fee paid, including model number, serial number and date of payment, and present such proof of payment when seeking service or assistance covered by the warranty set forth in this EULA. This EULA is governed by the laws of the State of New York, without regards to its conflicts of law principles. The parties hereby irrevocably agree that they submit themselves to the personal jurisdiction of the state and federal courts of New York for purposes of resolving any and all disputes arising under or related to these terms and conditions. The parties specifically exclude the application of the provisions of the United Nations Convention on Contracts for the International Sale of Goods.