tyco | American Dynamics

VideoEdge NVR

Installation and User Guide

July 2020 8200-1966-01 A0

5.6

www.americandynamics.net

Johnson Controls

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

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

Windows® is a registered trademark of Microsoft Corporation. PS/2® is a registered trademark of International Business Machines Corporation.

The trademarks, logos, and service marks displayed on this document are registered in the United States [or other countries]. Any misuse of the trademarks is strictly prohibited and Tyco Security Products will aggressively enforce its intellectual property rights to the fullest extent of the law, including pursuit of criminal prosecution wherever necessary. All trademarks not owned by Tyco Security Products are the property of their respective owners, and are used with permission or allowed under applicable laws.

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

This product is licensed under the MPEG-4 Visual Patent Portfolio License for the personal and non-commercial use of a consumer to (i) encoding video in compliance with the MPEG-4 visual standard (“MPEG-4 Video”) and/or (ii) decoding MPEG-4 video that was encoded by a consumer engaged in a personal and non-commercial activity and/or was obtained from a video provider licensed by MPEG LA to provide MPEG-4 video. No license is granted or shall be implied for any other use. Additional information including that relating to promotional, internal and commercial uses and licensing may be obtained from MPEG LA, LLC. See HTTP://WWW.MPEGLA.COM

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

H.265 Disclaimer

This product is licensed under and covered by one or more claims of the patents listed at www.hevcadvance.com

This product is licensed under the MPEG LA HEVC patent portfolio.

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 <3 m 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. Use an earthed socket, and ensure that the earth pin connects correctly with the socket.
2. This product is for indoor use only.
3. This product is for professional installation, use and service.
4. This product is only suitable for operation below altitudes or equivalent air pressure of:
   - VideoEdge Micro NVR, VideoEdge Desktop NVR, and VideoEdge 1U NVR - 2000m
   - VideoEdge 2U NVR, VideoEdge 2U Hybrid NVR, VideoEdge 3U Hybrid NVR, VideoEdge Rack Mount NVR - 3200m
5. 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.

Safety warnings for rack-mountable equipment

1 Elevated Operating Ambient - If the equipment is installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Consider installing the equipment in an environment compatible with the maximum ambient temperature (TMA) of 95°F (35°C). The unit operating temperature range is between 41°F and 95°F (5°C and 35°C).

2 Reduced Air Flow - When installing the equipment in a rack, do not compromise the amount of air flow required for the safe operation of the equipment.

3 Mechanical Loading - When mounting the equipment, ensure that the mechanical loading is even.

4 Circuit Overloading - Pay attention 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. Consult the equipment's nameplate ratings when addressing this concern.

5 Reliable Earthing - Maintain reliable grounding of rack-mounted equipment. Pay particular attention to power supply connections other than the direct connections to the branch circuit, such as the connection of equipment using power strips.

Recycling and disposal of equipment

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.

This 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.

Check with your regional waste management authority about where to dispose of WEEE or Batteries or packaging.

Power supply and network port information

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

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

The VideoEdge Micro NVR models provide either 4 or 8 IP video channels with onboard PoE switches. Each channel is rated at 15 W Max.

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

US/CAN deviations - The RJ45 connections () identified on the product as ‘RJ45 Gigabit Ethernet Port’ are intended for Ethernet use only, and not for telecommunication applications.

RTC battery replacement

The product is fitted with a 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, which include the date and time settings, 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, complete the following 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, and 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 "-" symbols on the battery.
6. Install the new battery in the connector, orientating the "+" and "-" symbols correctly.
7. Replace the computer cover.

VideoEdge Overview

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

VideoEdge manages a number of devices, such as video cameras, encoders, audio devices, and text devices. Data from such devices is recorded to VideoEdge's configured storage. VideoEdge provides clients with secure access to live and recorded data from its devices.

VideoEdge network video recorder (NVR) range

- **VideoEdge Micro NVR** - Small form factor IP-only VideoEdge, with either 4 or 8 PoE ports.
- **VideoEdge Desktop NVR** - Desktop IP-only VideoEdge with 32 IP video channels.
- **VideoEdge 1U NVR** - Rack mountable IP-only 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 IP-only 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 IP-only VideoEdge with 128 IP video channels.
- **VideoEdge Compact Desktop NVR** - Compact form factor IP-only VideoEdge, with 32 IP video channels.

VideoEdge Administration Interface

Users interact with the VideoEdge NVR using the VideoEdge Administration Interface. Access information about the NVR, modify settings, and add and configure devices through the interface. There are three ways to access the VideoEdge Administration Interface.

- From the VideoEdge NVR: Double-click the VideoEdge Administrator icon on the VideoEdge desktop. This will launch Mozilla Firefox ESR and open the VideoEdge Administration Interface login page.
- 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. The 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 click Configure. Note that 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 live and recorded media to a number of clients.

VideoEdge Client

VideoEdge Client is an integrated client installed on the VideoEdge NVR. To launch VideoEdge Client, double-click the VideoEdge Client icon on the VideoEdge Desktop. The login credentials for VideoEdge Client are the same as those used for the VideoEdge Administration Interface.

Monitor devices added to the host VideoEdge NVR using VideoEdge Client. For more information, refer to the *VideoEdge Client User Guide*.

victor Web / victor Web LT

victor Web is a portal used to access live and recorded media from multiple VideoEdge recorders. 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 in a web browser to "xx.xx.xx.xx/victorweb" where "xx.xx.xx.xx" is the IP address of the host. The login credentials for victor Web LT are the same as those used for the VideoEdge Administration Interface.

victor Web LT is included free with VideoEdge software. victor Web requires a license to run, but offers additional features that aren't available in victor Web LT. For more information, refer to the *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. victor manages live and recorded video, supports multiple integrations with 3rd party security hardware, and unifies with Software House C·CURE 9000, providing 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, backed by a victor Application Server using a Microsoft SQL Server backend.
- victor Enterprise - for large and geographically dispersed systems. victor and C·CURE 9000 support 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 full-featured video surveillance mobile application that provides access to VideoEdge recorders from mobile devices. VideoEdge Go is available from your device's app store.

Installing VideoEdge

VideoEdge is supplied as either a hardware and software bundle, or a software-only bundle.

Hardware and software bundle

When VideoEdge is supplied as a hardware and software bundle, the basic system settings, including time and region, are preconfigured. Default partitioning, including the required system partitions and some media partitions, is also preconfigured. If the preconfigured media partitions are not suitable, they can be edited as required after installation.

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

Software-only bundle

When VideoEdge is supplied as software only, you must install it onto your hardware. Ensure that your hardware meets the minimum operation requirements.

Caution

Any previously configured OS on your hardware will be removed and overwritten.

General safety warnings

1. Check the product label for power supply requirements to ensure 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) to protect computing systems from power fluctuations that may cause data loss.
3. This product must be earthed. Plugs and sockets can vary between countries. Use an earthed socket, and ensure that the earth pin connects correctly with the socket.
4. This product is for indoor use only.
5. This product is for professional installation, use and service.
6. This product is only suitable for operation below altitudes or equivalent air pressure of:
   - VideoEdge Micro NVR, VideoEdge Desktop NVR, and VideoEdge 1U NVR - 2000m
   - VideoEdge 2U NVR, VideoEdge 2U Hybrid NVR, VideoEdge 3U Hybrid NVR, VideoEdge Rack Mount NVR - 3200m

Connecting devices

External devices, such as cameras, monitors, microphones, controllers, alarms, and storage modules can be connected to the VideoEdge NVRs using the hardware interfaces.

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.

Connecting video devices

VideoEdge supports IP cameras, and IP encoders on all of its NVR units. The VideoEdge Hybrid NVR series feature local BNC inputs for analog cameras.

IP cameras

IP cameras are connected to the VideoEdge two different ways.

- IP cameras can be connected directly to the VideoEdge Micro NVR and VideoEdge 1U NVR using the onboard PoE ports.
- Multiple IP cameras can be connected to a single network port on the VideoEdge using a network switch.

For more information on the network configuration for IP cameras, see the *Network* section.

Analog cameras

Analog cameras are connected to the VideoEdge two different ways.

- Analog cameras can be connected directly to VideoEdge Hybrid NVRs using the BNC video inputs.
- Multiple analog cameras can be connected to a single network port on the VideoEdge using an IP encoder.

The number of available network ports, PoE ports, and BNC video inputs varies by model. For more information, see *Appendix C - Hardware Configurations*.

Monitors

VideoEdge NVRs feature a number of different video outputs for monitors. Depending on the model, VGA, DVI-I, DVI-D, DisplayPort, and HDMI are supported.

On the Hybrid series, additional monitors can be connected to the NVR using the BNC video outputs at the rear of the units.

For more information on the type of video ports that are supported on each model, see *Appendix C - Hardware Configurations*.

Connecting audio devices

VideoEdge NVRs feature a number of inputs and outputs for audio devices. Audio sources can be connected to the VideoEdge using the 3.5mm line in, or mic in ports. Headphones or speakers can be connected to the VideoEdge using the line out or headphone out ports.

On the Hybrid series, audio outputs from analog cameras can be connected to the NVR using the analog inputs at the rear of the units.

The number and type of available audio inputs and outputs varies by model. For more information, see *Appendix C - Hardware Configurations*.

Connecting alarms to VideoEdge

Connect alarm inputs and outputs to the VideoEdge NVR at the rear of the unit. The alarm outputs are transistor-transistor logic (TTL) with output rated 5 VDC, 20 mA 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 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

Connecting other devices

You can connect additional optional devices to your VideoEdge.

- A keyboard and mouse: Connect a keyboard and mouse to the PS/2 ports or USB ports. Use a keyboard and mouse to directly interact with the VideoEdge NVR, and access the operating system and related features locally.
- An external storage module (ESM): Connect ESMs to the VideoEdge to add additional storage.
- A dome controller: Connect dome controllers such as the Sensormatic VM16E, American Dynamics ADTTE Touch Tracker, ADTT16E Advanced Dome Controller, or AD2089 Analog Keyboard to the COM2 serial port.

Figure 1 ADTTE/ADTT16E wiring diagram

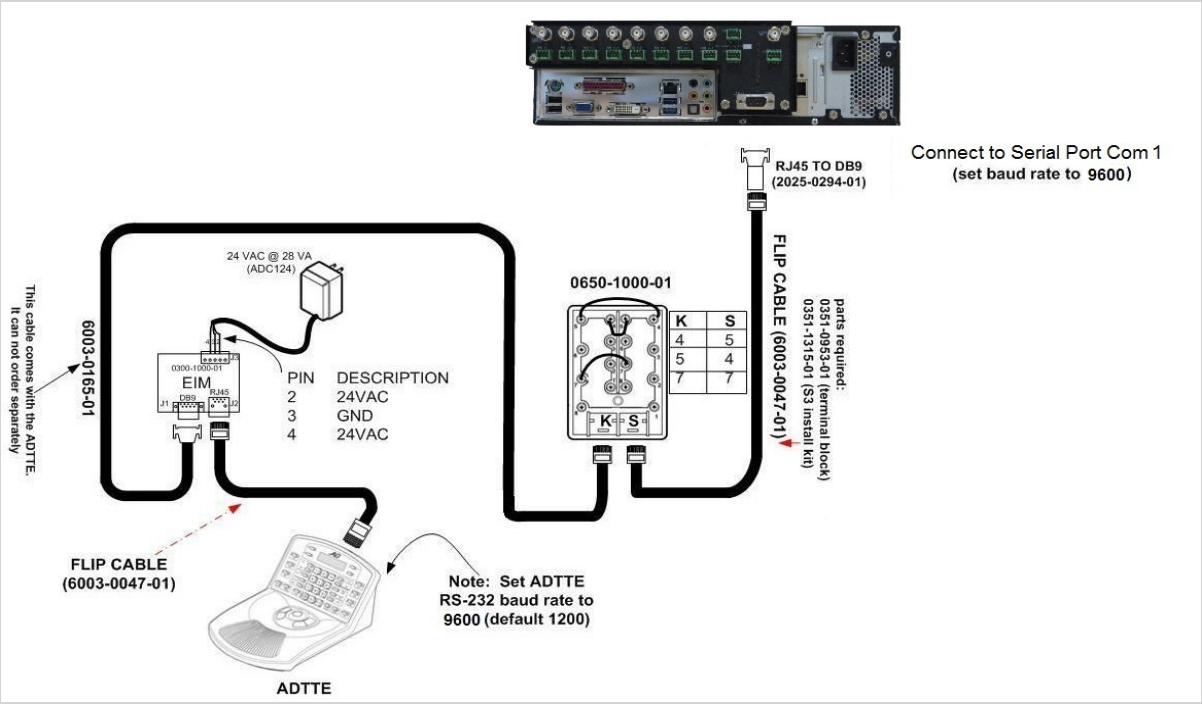
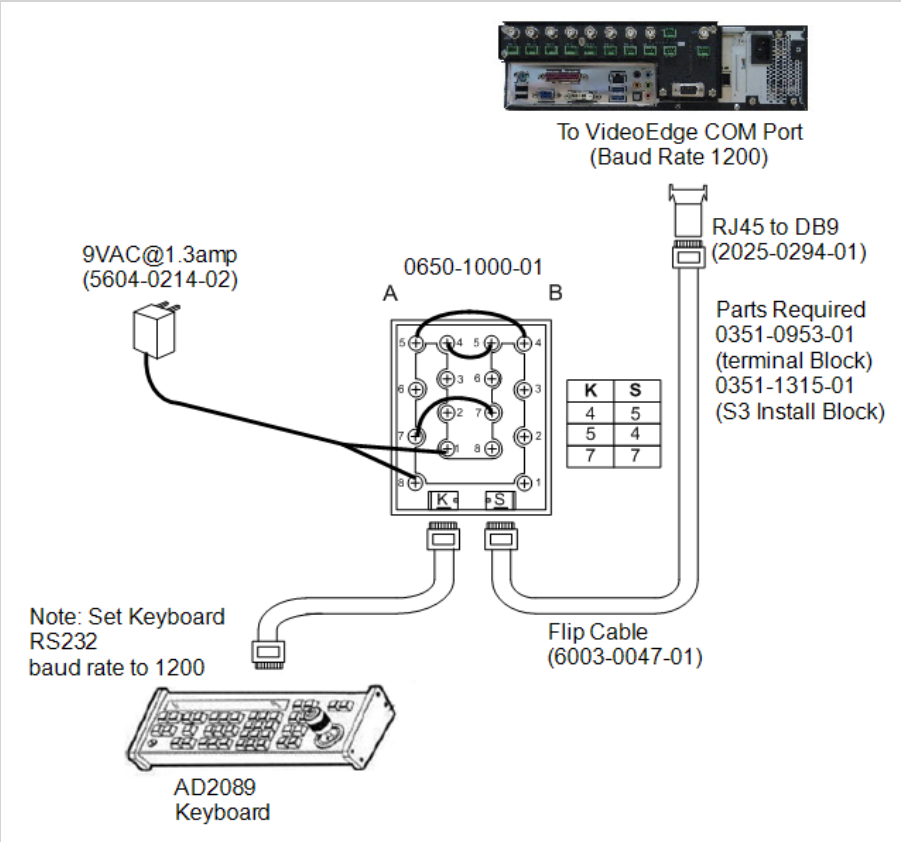


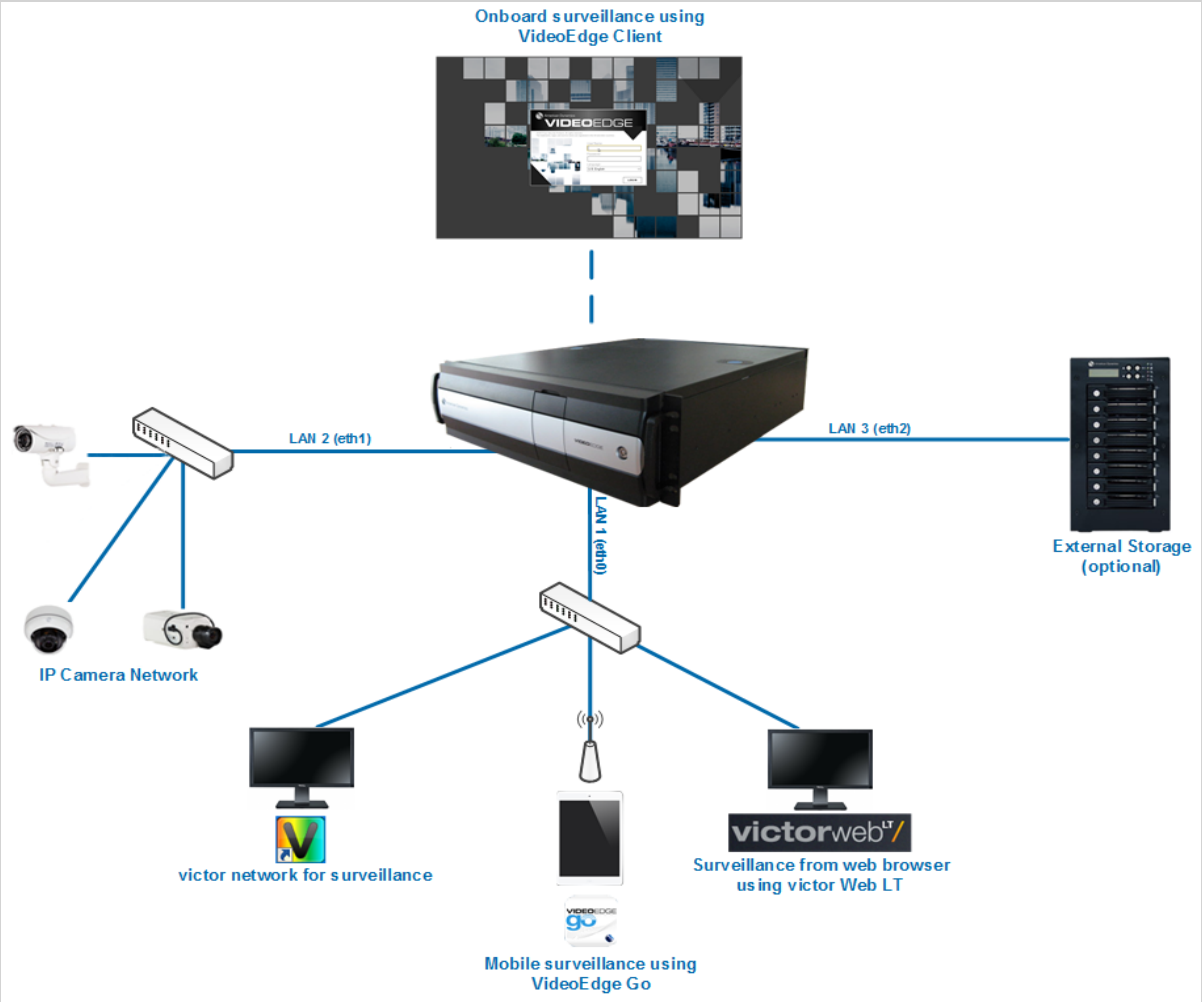
Figure 2 AD2089 wiring diagram



Connecting VideoEdge to a Network

Connect the VideoEdge NVR to the local area network (LAN) using a network port at the rear of the unit. Use Category 5 twisted-pair Ethernet cable (CAT 5 TPE).

Figure 3 Network topology of an IP-only VideoEdge NVR



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 500 GB of storage is required for system partitions. The remaining available storage can be used for media storage, and is configured as media partitions.

For VideoEdge NVR models with 500 GB capacity, you must add and configure additional external storage 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 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
VideoEdge Compact Desktop NVR	**0TB**				
	4TB	4TB	Linux Native	XFS	/mediadb
	6TB	6TB	Linux Native	XFS	/mediadb
	10TB	10TB	Linux Native	XFS	/mediadb

Rack mounting VideoEdge

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 lb (68 kg) 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 (482.6 mm) front and rear mounting flanges.

Safety warnings for rack-mountable equipment

1. Elevated Operating Ambient - If the equipment is installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Consider installing the equipment in an environment compatible with the maximum ambient temperature (TMA) of 95°F (35°C). The unit operating temperature range is between 41°F and 95°F (5°C and 35°C).
2. Reduced Air Flow - When installing the equipment in a rack, do not compromise the amount of air flow required for the safe operation of the equipment.
3. Mechanical Loading - When mounting the equipment, ensure that the mechanical loading is even.
4. Circuit Overloading - Pay attention 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. Consult the equipment's nameplate ratings when addressing this concern.
5. Reliable Earthing - Maintain reliable grounding of rack-mounted equipment. Pay particular attention to power supply connections other than the direct connections to the branch circuit, such as the connection of equipment using power strips.

Hardware and software bundles

This section details the installation and configuration process for VideoEdge hardware and software bundles.

There are three stages to setting up and installing VideoEdge hardware and software bundles:

1. Booting up VideoEdge for the first time.
2. Logging in to the VideoEdge desktop.
3. Configuring VideoEdge using the Setup Wizard.

Procedure 1 Booting up VideoEdge for the first time

1. Turn on the VideoEdge NVR.
   A series of boot messages appear and the system is loaded to the License Agreement.
2. Click **Next**.
3. When the license agreement is displayed, select **Yes, I Agree to the License Agreement**.

Passwords for logging on to the VideoEdge desktop

When the system boots to the VideoEdge login screen, log on to the VideoEdge desktop to continue the installation and configuration process.

For general users, the preconfigured VideoEdge account password is **VideoEdge**. Use this account to log on to the desktop to use VideoEdge Client.

For system administrators, the preconfigured root account password is **root**.
Use this account to log on to the desktop. The root account is intended for use by system administrators only.

For more information, see *System Passwords*.

Caution

For optimum security, change the VideoEdge account password and the root account password immediately. Ensure

that you remember your new passwords. You cannot make administrative changes to the desktop without a password.

Procedure 2 Logging on to the VideoEdge desktop

1. Enter the **Username**. The default username is **VideoEdge**
2. Click **Next**.
3. Enter the **Password**. The default password is **VideoEdge**
4. Click **Sign In**.

VideoEdge NVR Setup Wizard

Once VideoEdge is installed, you must configure the basic settings using the VideoEdge NVR Setup Wizard. After completing the Setup Wizard, your VideoEdge will be operational. Access the Setup Wizard using the VideoEdge Administrator icon on the desktop, or by using a remote client.

You are automatically directed to the Setup Wizard the first time you log in to the Administration Interface after installation. If you exit the Setup Wizard prior to completing all the steps, your progress will be saved, and you will be automatically directed to the last page viewed when you return to the Setup Wizard.

Note: To complete System Security in the Setup Wizard, you must do the following:

- Create a digital certificate in the Security Settings section. If you do not want to create a certificate, revert to HTTP and HTTPS mode. For more information, see Web Server Protocol Configuration.
- Create new passwords for each preconfigured default user account and service account in the User Accounts section in both Standard Security Mode and Enhanced Security Mode. For more information, see Preconfigured User Accounts in the Setup Wizard

Procedure 3 Configuring VideoEdge using the Setup Wizard

1. Enter the Administrator **Username**. The default username is **admin**
2. Enter the Administrator **Password**. The default password is **admin**
3. Click **Login**.The VideoEdge NVR Setup Wizard begins.
4. Complete the Setup Wizard.

Software-only bundles

This section details the installation and configuration process for VideoEdge software-only bundles. 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 overwritten.

There are four stages to setting up and installing VideoEdge software-only bundles:

1. Booting the system using the NVR software disk or USB drive.
2. Rebooting the system after basic installation.
3. Logging in to the NVR desktop.
4. Configuring the NVR using the Setup Wizard.

Booting your computer or server using the VideoEdge software DVD or USB drive

To initialize the installation of VideoEdge, you must boot the system from the software DVD or USB. If you are installing from a USB drive, ensure that no other USB drives are inserted during installation.

Procedure 4 Booting your computer or server using the VideoEdge software DVD or USB drive

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.
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. Select the required drive and press Enter.

2 From the installations option menu select **Install / Restore_VideoEdge_NVR_Release_x.x.x.xxx**, where **x.x.x.xxx** is the software version you are installing, and press **Enter**.
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).

3 Read and accept the license agreement by selecting **Next**, and then selecting **Yes**.
The self-installer initiates; progress will be displayed during installation.
4 Once the self-installer has completed, click **Reboot NVR** when prompted.
5 Remove the software DVD or USB drive used for the installation.
6 When the GRUB screen displays, ensure VideoEdge is selected and press **Enter**.
The VideoEdge desktop loads.
7 Enter your **Username**. The default username is **VideoEdge**
8 Click **Log in**.
9 Enter your **Password**. The default password is **VideoEdge**
10 Click **Log in**.
The setup wizard launches. For more information on completing the setup wizard, see the *VideoEdge setup wizard* section.

VideoEdge Virtual NVR

The VideoEdge Virtual NVR appliance is supported on VMware installations ESXI 6.0 and later. The VideoEdge Virtual NVR is distributed as an OVA file. Use this OVA file with a VMware Client to install and configure a virtual machine (VM).

Note:
A working knowledge of the key concepts of storage and network virtualization are required for installation. For more information, refer to the appropriate VMware Appliances user guide.

The VMware Client validates the OVA file before it is imported. If the OVA file is not compatible with the server, the validation will fail. Before you import the OVA file, use the hardware resourcing guidelines in Table 3 to review the VM system settings.

Before you begin

- You must create at least one media disk for media recording. See the hardware resourcing guidelines in Table 3 for creating appropriate storage size.

Note:
The greater the storage size, the greater the media data retention period.

- For optimum performance, use thick-provisioned Eager Zeroed disk creation over thick-provisioned Lazy Zeroed disk creation. This will require additional time to complete.
- For optimum performance, resource the VM for a single socket where possible. If you require more cores than a single socket provides, balance the cores across the sockets.

Hardware resourcing

The following table shows the recommended VM system specifications for the VideoEdge Virtual NVR. These recommendations are based on the number of cameras or data throughput for the VideoEdge Virtual NVR.

Note:
The VideoEdge Virtual NVR requires a specific VideoEdge VM license in addition to the standard licensable features. This specific license can be purchased with the Local or Centralized License. The VideoEdge software version must be 5.4.2 or later.

Table 3 Hardware resourcing

Virtual VideoEdge NVR					
		Up to 32 cameras or 100 MB/s throughput	Up to 64 cameras or 300 MB/s throughput	Up to 128 cameras or 600 MB/s throughput	Up to 300 cameras or 1200 MB/s throughput
Virtual server	VMware ESXi 6.0 or higher	Yes	Yes	Yes	Yes
Operating system	VideoEdge OS built on openSUSE Linux	Included with Installer	Included with Installer	Included with Installer	Included with Installer
CPU	vCPU	4 vCPU	8 vCPU	12 vCPU	28 vCPU
	CPU reservation	7000 MHz	12000 MHz	20000 MHz	47600 MHz
RAM	Memory reservation	8 GB	8 GB	16 GB	38 GB
NIC	Dedicated Ethernet	(2) 1GbE	(2) 1GbE	(2) 1GbE	(2) 10GbE
	Boot/OS/DB	200 GB	200 GB	200 GB	200 GB
	Minimum video storage	1TB	4TB	4TB	6TB
	Average IOPS (ISCSI SAN RAID 10)	220	260	400	500
Optical	DVD+/-R dual-layer	Yes	Yes	Yes	Yes
USB	2.0 or 3.0	Yes	Yes	Yes	Yes

Note:

- **Virtual server:** Preconfigure resource pools for VMware to allow the NVR to run in a virtual environment.
- **Virtual server, CPU, RAM, NIC, optical, USB:** Operating supported chipset, such as Ethernet, storage controller, or RAID controller.
- **Operating system:** A JeOS (Just Enough Operating System) is included with the VideoEdge installer package within the OVA.
- **Dedicated Ethernet:** Separate camera and video management interfaces, such as victor Client, are recommended at the specified minimum connection speed.
- **Minimum video storage:** The VM maximum video storage throughput is based on the data store configuration for the host or cluster. The figures provided here are based on an external iSCSI storage array configured in a RAID 10 configuration and connected using a 10 GbE NIC. Use a thick provisioned Eager zeroed disk creation over a Lazy zeroed disk creation.

Using the Administration Interface

Users interact with the VideoEdge NVR using the VideoEdge Administration Interface. You can access information about the NVR, modify settings, and add and configure devices through the interface. You can access the interface using a web browser, through victor unified client, or locally on your hardware.

To access VideoEdge through victor unified client, you must add the VideoEdge NVR to your recorders in the device list in victor unified client. For information on how to add a VideoEdge recorder to victor refer to the *victor Client Administration and Configuration Guide*.

Logging on to the Administration Interface using a web browser

A System Administrator can log on to the VideoEdge Administration Interface using a web browser. If you log on using a System Administrator account, you can configure and edit VideoEdge settings and view live video. There are two System Administrator accounts: Admin and Operator.

Note:
The Admin account is a default account. The Operator account is a predefined role. You can create an Operator user during the Setup Wizard.

You must log on or authenticate yourself when you first log on to the Administrator Interface, or when you are already logged on and your user access is changed. If you change your account password from the default password, ensure that you use your new password when logging on.

The Administration Interface supports the following web browsers:

- Microsoft Internet Explorer 11
- Microsoft Edge: latest version
- Google Chrome: latest version
- Mozilla Firefox: latest version

Procedure 5 Logging on to the Administration Interface using a web browser

1. Launch your web browser and enter the VideoEdge IP address into the **URL** field.
   Enter **https://NVR_Server_IP_Address**, where **NVR_Server_IP_Address** is the IP address of the machine running the NVR software, for example, **https://192.187.100.21**
   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. Ensure that you install a trusted certificate when the NVR is set up.
2. Click **Continue to this website (not recommended)**.
   Wording may differ between browsers.
3. When the login window displays, enter your **Username** and **Password**.
   For the System Administrator, the default username is **admin**. The default password is **admin**
   For the Operator, the default username is **operator**. The default password is **operator**.
4. Click **Login**.
   The Administration Interface opens.

Accessing the Administration Interface using victor

To access the VideoEdge Administration Interface through victor unified client, you must add the VideoEdge NVR to your recorders in the device list in victor unified client. For information on how to add a VideoEdge recorder to victor refer to the *victor Client Administration and Configuration Guide*.

You can configure and edit VideoEdge settings by accessing the Administration Interface through victor. However, when using victor you do not have the option to view live video. To view cameras in live mode using victor unified client, use the **Surveillance** pane.

Procedure 6 Accessing the Administration Interface using victor

1 In the victor unified client, click **Devices**, and then expand the **Recorders** menu.
2 Expand the **VideoEdge** folder.
3 Right-click on the VideoEdge recorder that you want to configure.
4 Click **Configure**.
The Administration Interface opens.

Navigating the Administration Interface

Figure 4 Administration Interface

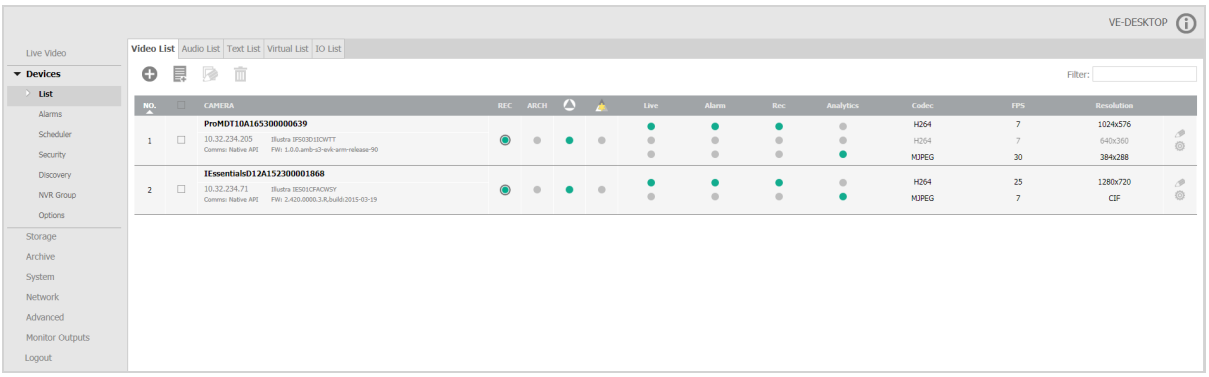


Table 4 Administration Interface

Item	Description
Main Menu	Located on the left side of the interface. Navigate the main menu sections. Select a menu item to display its submenu.
Live Video	Located at the top of the main menu. Select this menu item to access live video. This option is not available when browsing directly on the VideoEdge NVR's server browser.
Submenus	Located within the main menu. Submenu options are displayed when a selection is made in the main menu.
Main Pane	This area forms the main body of the interface - Configure the NVR and associated device settings.
About	Located in the top right of the interface. Click to display NVR and system information. The user account currently in use and the current software version are displayed.

To navigate the Administration Interface and access the required configuration settings, use the menu and submenus 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 submenus. These submenus are described in the relevant chapters.

Adding, editing, and removing in VideoEdge

Table 5 Add, Edit, and Remove icons

Icon	Function
	This is the **Add** icon. Use this icon to add physical devices such as cameras, text devices, and storage; and software configurations such as accounts, templates, and monitor tours. Click the Add icon to begin the process of adding a device or configuration. The Add icon appears throughout the VideoEdge Admin Interface, and is usually located at the top left of the page.
	This is the **Edit** icon. Use this icon to edit the settings on added devices or software configurations. Click the Edit icon of the device or configuration you want to edit. Alternatively, for some procedures, select the checkbox of the device or configuration, and then click the Edit icon. The Edit icon appears throughout the VideoEdge Admin Interface, and is usually located at the top left of the page and within device lists and tables.
	This is the **Remove** icon. Use this icon to delete or remove an added device or software configuration. Select the checkbox of the device or configuration you want to remove, and then click the Remove icon. The Remove icon appears throughout the VideoEdge Admin Interface, and is located in different places depending on the page and function.

Live Video

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

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.

The **Live Video** menu contains the following sections: **1 Camera View**, and **2x2 Camera View**.

Viewing 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. Live audio streams are not available on the Administration Interface. To listen to audio streams, use victor unified client or VideoEdge Client.

Storage and cameras must be configured before you can view live video.

In the Live Video view, the recording mode is displayed in the lower-left corner. The camera list, where you can select available cameras to display, is below the viewing window. The setup icon, where you can edit settings for the selected camera, is in the lower-right corner.

Procedure 7 Viewing Live Video

1. Click the **Live Video** menu.
2. Click the **1 Camera View** tab, or the **2x2 Camera View** tab.
3. Select the cameras that you want to view from the **Select camera to view** list.
   The camera's live video stream appears in the viewing window.

Devices

Cameras, audio devices, text devices, and input/output (I/O) devices are added and configured using the Devices menu of the Administration Interface. The Devices menu contains the following submenus:

- **List** - View a list of all devices connected to the VideoEdge, and a summary of their configuration status. Add and remove devices, and edit or batch edit camera configuration settings. The List submenu contains the following sections: **Video List**, **Audio List**, **Text List**, **Virtual List**, and **IO List**.
- **Alarms** - Create and configure camera alarms. Select different types of alarm triggers, like Motion Detection or Video Intelligence. Add and configure sensors and outputs. The Alarms submenu contains the following sections: **Alarms**, **Sensors**, and **Outputs**.
- **Scheduler** - Specify the recording mode that is active at scheduled times during the day. The Scheduler submenu contains the following sections: **Schedules**, **Schedule Editor**, and **Group Editor**.
- **Security** - Create and maintain password groups.
- **Discovery** - Scan for devices, and use auto-discovery to add cameras to VideoEdge. The Discovery submenu contains the following sections: **Discovered Devices** and **Scan for Devices**.
- **NVR Group** - Configure NVR groups for remote transcoding and failover. The NVR Group submenu contains the following sections: **NVR Group List** and **Discovered NVRs**.
- **Options** - Configure global camera settings that are applied whenever a camera is added to VideoEdge. Enable TrickleStor and configure settings. The Options submenu contains the following sections: **Camera Add** and **TrickleStor**.

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 five tabs, displaying a list of all cameras, audio devices, text devices, virtual devices, and IO devices.

List icons table

Table 6 List icons

Icon	Name	Function
	**Add New Device**, **Add Text Stream**, **Add Virtual Camera**, **Add IO Device**	Add a device.
	**Add Devices from CSV file**	Add devices from a CSV file.
	**Batch Edit**	Edit multiple devices.
	**Remove Device**, **Remove Text Stream**, **Remove Virtual Camera**, **Remove IO Device**, **Remove**	Remove the device from the list.
	**Edit**	Edit
	**Setup**	Open Advanced Camera Configuration.
	**Save**	Save

Icon	Name	Function
	**Cancel**	Cancel
	**Rules/Markers**	Open the Rules/Markers page.
	**Add Rule**	Add a Rule.
	**Add Marker**	Add a Marker.
	**Add Security Group**	Create a Security Group.
	**Show only cameras with errors**	Show only cameras that have errors in the list.
	**Arrow up**	Sort list in ascending order.
	**Arrow down**	Sort list in descending order.
	Right Arrow	Move selected device to the Association list.
	Left Arrow	Remove selected device from the Association list.

Device Lists

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. To access the different device lists, navigate to the List submenu of the Devices menu, and then select the required tab at the top of the page.

The device lists can be sorted alphanumerically, by a selected column, in ascending or descending order. Use the **Arrow up** icon to sort the list in descending order, and the **Arrow down** icon to sort the list in ascending order.

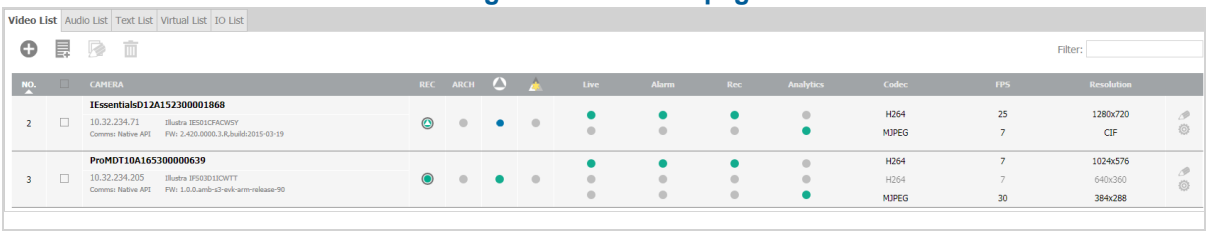
The device lists have a filter feature which can be used to display specific device records. The filter feature looks at the criteria you enter in the Filter field and compares this against all fields in that device list. The Filter field is located in the upper right of the page.

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 *Video List summary table* provides a description of each field displayed.

Figure 5 Video List page



Video List summary table

Table 7 Video List summary

Field	Description
NO.	Device slot number.
CAMERA	Device name as given when adding the device to VideoEdge. Device IP address. Device Manufacturer and Model FW: Current Firmware version on the device Communications Type.
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 **Edit Group Times** icon is displayed in the field.
ARCH	Indicates if archiving is enabled for the device. The archiving options available are: • Archiving Disabled • Archive all video • Archive only alarm video
	Analytics. Indicates if analytics are set on the device. The analytic options are: • Analytics Off • Motion Detection • Video Intelligence • Deep Intelligence • Intelligent Search - Person • Edge Based • Face Recognition including Face Search Alert and Face Verification

Field	Description
	Associations. Indicates the device's associations. Hover the cursor over the icon to display information. The following devices can be associated: • Video • Audio • Text
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. **Codec** - The camera codec. **FPS** - The camera FPS. **Resolution** - The camera resolution.

Adding devices to VideoEdge

You can add video devices to VideoEdge from the Video List tab. You can add devices manually, or you can add devices from a CSV file. Devices can also be added to VideoEdge using Discovery. For further information, see the *Discovery* section.

Manually adding analog devices

To add an analog device to VideoEdge, connect the device directly to a port on the VideoEdge NVR. 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 is 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, connect the camera to a port on the unit.

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

If you remove an analog device from the NVR, you can re-add it manually using the IP address, **127.0.0.1**. This adds all inputs which are not currently in the Device List. Alternatively, if you uncheck 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 8 Manually adding analog devices

1. Click the **Devices** menu.
2. Click **List**.
3. Click the **Add New Device** icon.
4. Enter a name in the **Device Name** field.

Note:
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***
• Audio inputs are given a "_n_audio" suffix, for example ***Analog_2_audio***
Here, ***Analog*** is the user-defined device name. Each device can be renamed after they have been added to the NVR.

5. Enter **127.0.0.1** into the **Device IP Address** field.
6. Select the camera manufacturer from the **Manufacturer** list.

If you do not want to specify the manufacturer, or the manufacturer doesn't appear in the list, select Auto Detect.

7 (Optional) Select a Security Group from the **Security Group** list, or create a new Security Group.

8 (New Security Group only) Select New Security Group from the **Security Group** list.
   a Enter a **Group Name**.
   b Enter a **Description**.
   c (Optional) Enter a **Username**.
   d (Optional) Enter a **Password**.
   e (Optional) Select a Security Level from the **Security Level** list.
   f (Optional) If you want to use a different port to the default, clear the **Default** checkbox and enter the new port number in the **Port** field.
   g (Optional) Select the **ONVIF RTSP Authentication** checkbox if the devices in this group use ONVIF communication protocols.

9 (Optional) Click **Additional Settings** to configure additional device settings.

10 (Optional) Select a device type from the **Device Type** list.

11 (Optional) Select an option from the **Auto-Configure Streams** list.
   - **None**: Disables the Auto Configure streams function.
   - **1 Additional Live Stream**: Configures one additional stream
   - **2 Additional Live Streams**: Configures two additional streams. This option is only available for cameras that support three streams.

12 (Optional) Select a specific camera slot from the **Slot** list. Selecting **Auto** auto-configures device slot allocation.

13 (Optional) Clear the **Add All Inputs on Device** checkbox if you do not want to add all inputs on a device. Specific camera slots can also be allocated when manually adding the inputs on a device.

14 (Optional) Clear the **Default Associations** checkbox if you want to define custom associations after the devices have been added.

15 (Optional) Clear the **Enable Smart Search (Motion Metadata)** checkbox to disable Smart Search for any cameras that you add manually.

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

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 that does not support Smart Search, using either a primary or secondary stream, the default recording mode is set to Record Always.

VideoEdge, by default, is configured to communicate with a camera using the camera's 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, such as video, audio or PTZ. The communication method used by the VideoEdge NVR and the camera is displayed in 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. 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.

Note:
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 9 Manually adding an IP device

1 Click the **Devices** menu.
2 Click **List**.
3 Click the **Add New Device** icon.
4 Enter the **Device Name**.
5 Enter the **Device IP Address** of the device.
6 Select the camera manufacturer from the **Manufacturer** list.
If you do not want to specify the manufacturer, or the manufacturer doesn't appear in the list, select Auto Detect.
7 (Optional) Select a Security Group from the **Security Group** list, or create a new Security Group.
8 (New Security Group only) Select New Security Group from the **Security Group** list.
   a Enter a **Group Name**.
   b Enter a **Description**.
   c (Optional) Enter a **Username**.
   d (Optional) Enter a **Password**.
   e (Optional) Select a Security Level from the **Security Level** list.
   f (Optional) If you want to use a different port to the default, clear the **Default** checkbox and enter the new port number in the **Port** field.
   g (Optional) Select the **ONVIF RTSP Authentication** checkbox if the devices in this group use ONVIF communication protocols.
9 (Optional) Click **Additional Settings** to configure additional device settings.
10 (Optional) Select a device type from the **Device Type** list.
11 (Optional) Select an option from the **Auto-Configure Streams** list.
   - **None**: Disables the Auto Configure streams function.
   - **1 Additional Live Stream**: Configures one additional stream
   - **2 Additional Live Streams**: Configures two additional streams. This option is only available for cameras that support three streams.
12 (Optional) Select a specific camera slot from the **Slot** list. Selecting **Auto** auto-configures device slot allocation.
13 (Optional) Clear the **Add All Inputs on Device** checkbox if you do not want to add all inputs on a device. Specific camera slots can also be allocated when manually adding the inputs on a device.
14 (Optional) Clear the **Default Associations** checkbox if you want to define custom associations after the devices have been added.
15 (Optional) Clear the **Enable Smart Search (Motion Metadata)** checkbox to disable Smart Search for any cameras that you add manually.
16 (Optional) Select the **Use Multicast Streaming** checkbox to use the camera's multicast stream to record footage.
17 Click the **Save** icon.
If the **Default Associations** checkbox is unselected, a window will open displaying the available inputs. For video devices, a snapshot can be displayed.

Procedure 10 Adding an RTSP stream

1 Click the **Devices** menu.
2 Click **List**.
3 Click the **Add New Device** icon.
4 Enter the **Device Name**.
5 (Optional) Select a Security Group from the **Security Group** list, or create a new Security Group.
6 (New Security Group only) Select New Security Group from the **Security Group** list.
   a Enter a **Group Name**.
   b Enter a **Description**.
   c (Optional) Enter a **Username**.

d (Optional) Enter a **Password**.
e (Optional) Select a Security Level from the **Security Level** list.
f (Optional) If you want to use a different port to the default, clear the **Default** checkbox and enter the new port number in the **Port** field.
g (Optional) Select the **ONVIF RTSP Authentication** checkbox if the devices in this group use ONVIF communication protocols.

7 Click **Additional Settings**.
8 Select **RTSP** from the **Device Type** list.
9 Enter the **RTSP URL** of the RTSP stream.
10 (Optional) Select a specific device slot from the **Slot** list. Selecting **Auto** auto-configures device slot allocation.
11 Click the **Save** icon.

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 must 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 in the **Devices > Options** 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.
  - **Camera Slot (optional)** - An integer to identify the camera slot. If omitted, the slot number is assigned automatically.
- Multichannel devices should only be added to the file once. All available channels are added automatically.

Procedure 11 Adding devices from a CSV file

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

Procedure 12 Editing basic video settings

1 Click the **Devices** menu.
2 Click **List**.
3 Click the **Edit** icon of the camera you want to edit.
4 Make the required changes:

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

Note:
Before updating a camera's recording state, 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, and 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 the **Save** icon.

Configuring dual recording for a camera

Using the dual recording feature, you can record both a low-resolution and a high-resolution stream from a single camera. If you have limited or low bandwidth, you can retrieve clips and view recorded video at a lower resolution.

Enabling recording on two streams will increase how much storage the camera uses.

Procedure 13 Configuring dual recording for a camera

1 Click the **Devices** menu.
2 Click **List**.
3 Click the **Edit** icon for the camera that you want to configure.
4 In the **Rec** column, select the checkboxes for the two streams that you want to record.
You must assign the camera's Alarm functionality to at least one of the streams that you want to record.
5 Click the **Save** icon.
A message displays to inform the user that two streams will now be recorded, increasing storage usage.
6 Click **OK**.
After you enable dual recording, the camera's Rec column displays a green radio button in each stream that you select for recording.

Batch editing camera settings

Some camera settings can be batch edited using the Batch Edit page. The cameras currently being edited are listed in the left pane. Camera settings are edited 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.

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 14 Batch editing camera settings

1 Click the **Devices** menu.
2 Click **List**.
3 Select the checkbox for each camera you want to batch edit.
4 Click the **Batch Edit** icon.
The Batch Edit page displays.
5 Adjust the device settings as required:
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**, or **CameraName_2**.

b **Maximum Recording Storage Period** - Select the maximum duration that media recorded for these devices will be saved without being deleted.
c **Storage Set** - Select which storage set the batch of devices will record to.

d **Recording Mode** - Use this to set the recording mode for the cameras. 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. Choose Archiving disabled, Archive all videos, or Archive only alarm video.
f **Archiving Quality** - Archiving Quality is defined as a percentage of applied framerate 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 if an archiving storage period is Enabled or Disabled.
h **Video Analysis** - Select which type of analytics to apply to this batch of cameras: Motion detection, Video Intelligence, Deep Intelligence, Edge Based, Face Recognition, or License Plate Recognition.

Note:
When you select an analytic, additional device settings may appear. For more information, see the *Advanced Camera Configuration* section.

i **Associate Audio** - Use to associate an audio device with the selected cameras.
j **Device Replacement** - Use to assign a replacement camera or encoder if the selected device fails.
k **Video Streaming** - Enable or 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 or 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 or disable PTZ for all selected, applicable devices. Virtual PTZ will be unaffected.
p **Gaming Mode** - Enable or disable Gaming Mode for all selected and supported cameras. Enabling Gaming Mode maintains a constant framerate for all affected cameras.
q **Intelligent Guard Tour** - Enable or disable Intelligent Guard Tour for all selected and supported cameras.
r **Stream Configurations**- Set each stream to **Live**, **Alarm** or **Record**, and 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 Click the **Save** icon.
A Confirm Changes window opens, with a preview of the changes being made to the selected cameras.
7 Click the **Save** icon to confirm the changes.
If you do not want to make these changes to all cameras, click the **Cancel** icon.
8 When a message box opens to confirm the changes were successful, click **OK**.
If some of the changes are not successful, a summary page of failed updates opens with the failures highlighted in red. Click **OK** to continue.

Audio List

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

The Audio List displays the audio devices which have been added to the NVR. The *Audio List summary table* provides a description of each field displayed.

Figure 6 Audio List page

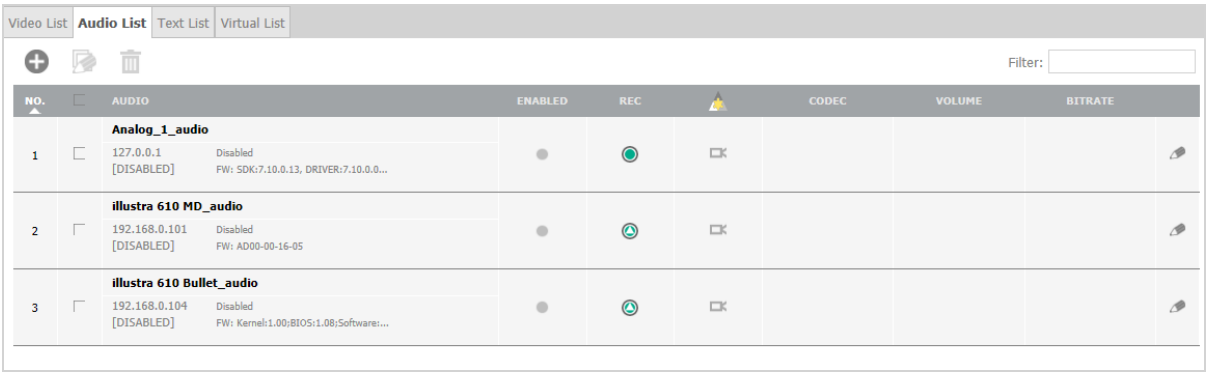


Table 8 Audio List summary table

Field	Description
NO.	Device slot number
AUDIO	Device name as given when adding the device to the NVR. Device IP address. Device Manufacturer and Model. FW: Current Firmware version on the device.
ENABLED	Indicates if the audio stream is enabled or disabled.
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 **Edit Group Times** icon is displayed in the field
	Associations. Indicates the device's associations. Hover the cursor over the icon to display information. The following devices can be associated: • Video • Text
CODEC	The audio codec.
VOLUME	The current volume.
BITRATE	The current bitrate.

Procedure 15 Editing Audio settings

1 Click the **Devices** menu.
2 Click **List**.
The Video List page displays.

3 Click the **Audio List** tab.
4 Click the **Edit** icon of the device you want to edit.
The fields that you can update are ready to edit.
5 Make the required changes to:
- **Name** - Update the name of the audio device.
- **Enabled** - Enable or disable audio.
- **IP Address** - Update the IP address of the audio device.
- **Rec** - Update the camera recording state. You can choose Recording Off, or Recording Always.

Note:
Before updating an audio device's recording state, ensure the device recording scheduler is disabled.

- **Codec** - Select the codec, when available.

The supported codec for analog channels is G711mulaw.
- **Volume** - Select the volume.
- **Bitrate** - Select the bitrate, when available.

The supported audio bit rate for analog channels is 8000.
6 Click the **Save** icon.

Text List

Text devices can be added to the NVR's serial ports or IP ports. 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 to 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 which was recorded at the time the text data was received, will be returned.

The Text List displays the serial and IP text devices that have been added to the NVR. The *Text List summary table* provides a description of each field displayed.

Figure 7 Text List page

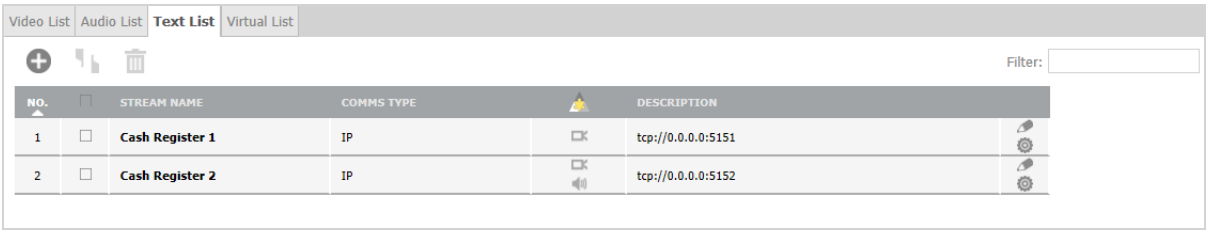


Table 9 Text List summary table

Field	Description
NO.	Device slot number.
STREAM NAME	Device name as given when adding the device to the NVR.
COMMS TYPE	Indicates the communication type in use.
	Associations. Indicates the device's associations. Hover the cursor to display information. The following devices can be associated: •  Video •  Audio

Field	Description
DESCRIPTION	Indicates the configured settings.

Configuring Serial Port settings for a serial text stream device

Prior to adding a serial text stream device, ensure it is connected to one of the NVR's USB ports or its RS232 Serial Port. When connected, configure that Serial Port's communication protocol for text stream use.

Procedure 16 Configuring Serial Port settings for a serial text stream device

1. Click the **Advanced** menu.
2. Click **Serial Ports**.
3. Click the **Edit** icon next of the serial port you want to edit.
   The Port Settings dialog box opens.
4. Select **Text Stream** from the **Protocol** list.
5. Configure the following settings if required:
   - **Baud Rate**
   - **Data Bits**
   - **Parity**
   - **Stop Bits**
   - **Flow Control**
6. Click the **Save** icon.

Manually adding a text stream device

Text stream devices can be connected to the NVR's serial ports or IP ports, and then added on the Text List page.

Procedure 17 Manually adding a text stream device

1. Click the **Devices** menu.
2. Click **List**.
3. Click the **Text List** tab.
4. Click the **Add Text Stream** icon.
5. Enter a **Text Stream Name**.
6. Select the **Connection Type** from the list.
7. Select the **Encoding Type** from the list.
   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** value, or click **Default** to use the default value.
   If the Line Delimiter does not properly match what is used in the text stream, text may be lost or improperly stored in the media database.
9. (IP Only) Enter the **Port**.
   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 the **Edit** icon to edit the serial device settings:
    a. Enter the **Com Port**.
    b. Enter the **Protocol**.
    c. Select the **Baud Rate** from the list.
    d. Select the **Data Bits** from the list.
    e. Select the **Parity** from the list.
    f. Select the **Stop Bits** from the list.
    g. Select the **Flow Control** from the list.
    h. Click the **Save** icon.

11 Click the **Save** icon.

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 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 18 Adding a Rule to a text device

1 Click the **Devices** menu.
2 Click **List**.
3 Click the **Text List** tab.
4 Select the checkbox of the Text device you want to create a rule for.
5 Click the **Rules/Markers** icon.
The Rules/Markers tab displays.
6 Click the **Add Rule** icon.
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 list. Forward by default.
10 Select the number of words to skip after a match is found to find the associated value, from the **Jump N Results** list. Default = 0.
11 Select one of the following **Criteria** from the list:
- **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 **Value 1** field. This is required when using string, less than, greater than, equal to, and range criteria.
13 Enter a value in the **Value 2** field. This is required when using range criteria.
14 Click the **Save** icon.

Procedure 19 Adding a Marker to a text device

1 Click the **Devices** menu.
2 Click **List**.
3 Click the **Text List** tab.
4 Select the checkbox of the Text device you want to create a marker for.
5 Click the **Rules/Markers** icon.
The Rules/Markers page opens.
6 Click the **Add Marker** icon.
The Marker Definitions window opens.
7 Enter the marker **Name**.
8 Enter the **Beginning Marker**.
9 Click the **Save** icon.

Procedure 20 Removing a Rule or Marker from a text device

1 Click the **Devices** menu.
2 Click **List**.
The Video List page displays.
3 Click the **Text List** tab.
4 Select the checkbox of the Text device you want to remove a rule or marker from.
5 Click the **Rules/Markers** icon.
The Rules/Markers page opens.
6 Select the checkbox of the Rule or Marker you want to remove.
7 Click the **Remove** icon.

Grouping Rules

Rules can be grouped together for both text stream alarms and searches, using the Group Rules checkbox. 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.

When the Group Rules checkbox is selected, the individual rules will not display in the Alarm Rule list of an events form in the VideoEdge Client. The only selectable option available will be **All**.

Procedure 21 Grouping Rules

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

Associating video and audio devices with text devices

Text devices can be associated with multiple video and audio devices on the Text Stream Associations page. Associations can also be removed using this page.

Procedure 22 Associating video and audio devices with text devices

1 Click the **Devices** menu.
2 Click **List**.
3 Click the **Text List** tab.
4 Click the **Setup** icon in the text record that you want to edit a text list setting for.
The Text Stream Associations page displays.
5 Select the checkboxes for the video and audio devices you want to associate with the text device.
6 Click the **Right Arrow** icon to move the selected devices to the Association lists, or click the **Left Arrow** icon to remove the selected devices from the Association lists.
7 Click the **Save** icon.

Procedure 23 Removing Associations from text devices

1 Click the **Devices** menu.
2 Click **List**.
3 Click the **Text List** tab.
4 Click the **Setup** icon for the text device that you want to edit a text list setting for.
The Text Edit tab opens.
5 Select the checkboxes for the video and audio devices you no longer want to associate with the text device.
6 Click the **Left Arrow** icon to remove the selected devices from the Association lists.

7 Click the **Save** icon.

Virtual List

You can create virtual streams on the Virtual List page. 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. You can view live virtual streams using the VideoEdge Live Video page, and using victor Web LT.

The following features are not supported for virtual cameras: PTZ, vPTZ, remote transcoding, playback of recorded video, association of audio, and clip export.

Procedure 24 Creating a Virtual Camera

1 Click the **Devices** menu.
2 Click **List**.
3 Click the **Virtual List** tab.
4 Click the **Add Virtual Camera** icon.
5 Enter a **Name** for the virtual camera stream
6 Select a layout type from the **Layout** list.
7 For each pane in the camera stream layout, select a camera from the dropdown list.
Virtual cameras do not support duplicate cameras. All camera entries must be unique.
8 Click the **Save** icon.

I/O List

From the I/O List page, you can add and configure input/output (I/O) devices such as dry contacts and relay outputs. The added dry contacts and relay outputs can be used to configure events and actions on the Sensors page.

If required, you can associate added I/O devices with particular cameras.

Note:
If using victor 5.2 or earlier, I/O devices added through an NVR with VideoEdge 5.3 must be associated with cameras for correct functionality.

Procedure 25 Manually adding an I/O device

1 Click the **Devices** menu.
2 Click **List**.
3 Click the **IO List** tab.
4 Click the **Add IO Device** icon.
5 Enter a name in the **IO Device Name** field.
6 Enter the IP address of the device in the **IP Address** field.
7 Select a Security Group from the **Security Group** list.
8 Click the **Save** icon.
The **Select Interfaces to Add** window displays.
9 Select the checkboxes of the interfaces that you want to add.
10 (Optional) Select a camera to associate the interface with from the **Camera Association** list.
11 Click the **Save** icon.

Procedure 26 Testing the input state of the I/O device

1 Click the **Devices** menu.
2 Click **List**.
3 Click the **IO List** tab.
4 Click **Test** on the device that you want to test.
A popup window displays.

5 Click **Get State**.
The current state displays.
6 (Relay Output only) Click **On**, **Off**, or **Pulse** to configure the state as required.
7 Click the **Cancel** icon to return to the **IO List** page.

VideoEdge Intellex Handler

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

Intellex video devices can be edited in the same way as other video devices. However, not all functions are supported for Intellex video devices. Any changes made to an Intellex video device made through the VideoEdge NVR will not overwrite the device settings on the Intellex NVR.

The following functions are unsupported for devices connected to an Intellex recorder: PTZ, digital PTZ, audio streaming, query device - mac address, dry contact, reboot device, power off device, reset factory default, get device log.

Procedure 27 Adding video devices from an Intellex recorder

1 Click the **Devices** menu.
2 Click **List**.
3 Click the **Add New Device** icon.
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** list.
7 Clear the **Add All Inputs on Device** checkbox.
8 (Optional) Deselect the **Default Associations** checkbox if you want to define custom associations after the devices have been associated.
9 Click the **Save** icon.
The Intellex Device list appears.
10 Select the checkbox beside each device you want to add.
11 Click the **Save** icon.

Advanced camera configuration

Advanced camera settings can be configured by clicking the **Setup** icon in the Video List for the required camera. The Advanced Camera Configuration page features the following tabs: General, Image Settings, Function & Streams, Archive, Alerts, Multicast, Controls, and OSD.

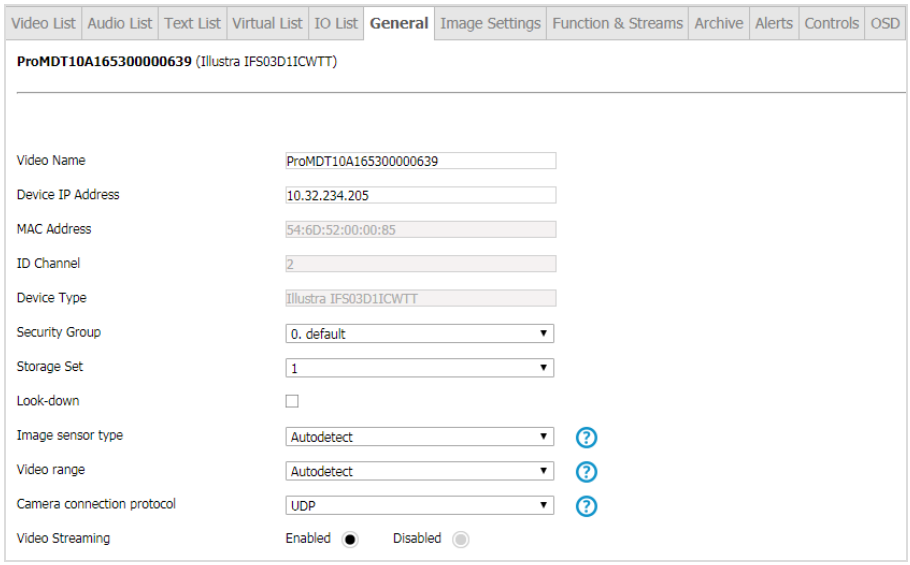
General

You can edit the following camera settings from the Advanced Camera Configuration General page: Video Name, Device IP Address, Security Group, Storage Set, Look-down, Image sensor type, Video range, Camera connection protocol, and Video Streaming.

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

After you change the camera settings, click the **Save** icon in the top right of the screen.

Figure 8 Advanced Camera Configuration - General page



Changing the Security Group assigned to an IP camera

If an IP camera is assigned to a security group, and you change the password for the camera, you must select the new security group the camera belongs to.

If you are editing the security group for a camera that forms 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.

Changing a camera's 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 be stored on media folders in the new storage set.

Enabling or disabling camera Look-down

Enable look-down if a camera has been mounted on the ceiling pointing down to the floor. Look-down cameras can better facilitate point of sale (POS) analytics.

Configuring the 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. The available options are Autodetect, Visible Light, and Thermal.

Configuring the 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. You can also configure the Camera connection protocol from the Batch Edit menu.

Note:
Selecting TCP may improve camera connection reliability, but may also increase latency in live video surveillance.

Enabling or disabling Video Streaming

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

Image Settings

Camera image settings can be configured in the Image Settings tab. The settings available are dependent on the camera make and model. When the settings are applied, the viewer window updates to reflect the changes made.

Procedure 28 Configuring Image Settings

1. Click the **Devices** menu.
2. Click **List**.
3. Click the **Setup** icon in the camera row you want to configure camera settings.
   The Function & Streams tab displays.
4. Click the **Image Settings** tab.
5. Adjust the video properties as required. The available settings and value ranges are dependent on the camera make and model. The configurable settings include the following:
   a. **Video Standard** - Select the required video processing standard from the list.
   b. **Rotate Image** - Select the angle you want to rotate the image from the list.
   c. **Brightness** - Select the brightness value from the list.
   d. **Contrast** - Select the contrast value from the list.
   e. **Hue** - Select the hue value from the list.
   f. **Saturation** - Select the saturation value from the list.
   g. **Sharpness** - Select the sharpness value from the list.
   h. **White Balance** - Select the white balance control value from the list.
   i. **Back Light Compensation** - Select the back light compensation value from the list.
   j. **Image Interlaced** - Select the image interlacing setting from the list.
6. Adjust the Lens or Sensor settings. The types of settings and value ranges available are dependent on the camera make and model. The configurable settings include the following:
   a. **Lens Focus** - Select a focus for the camera from the list.
   b. **Lens Auto Focus** - Select the checkbox to enable automatic camera focus.
   c. **Lens Iris** - Select the iris value for the camera from the list.
   d. **Lens Auto Iris** - Select the checkbox to enable automatic iris control.
   e. **Lens Day Night Mode** - Select the required mode from the list.
   f. **Lens WDR (Wide Dynamic Range)** - Select the checkbox to enable WDR.
   g. **Mount Type (Vivotech Fish-eye camera only)** - Select the Mount Type from the list.

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

Function and Streams

You can configure the following settings in the Function & Streams tab: Recording Mode, Video Analysis, Motion Sensitivity, Maximum Retention Period, Associate Audio, Auto-Configure Streams, Max GOP, and Stream Configuration. After you change the camera settings, click the **Save** icon in the top right of the screen.

Record Mode

The record mode setting on the camera determines when the camera records. Select the required record mode and click the **Save** icon in the top right of the page to set that record mode on the camera. The *Record Mode* table describes each recording mode.

Table 10 Record Mode

Mode	Icon	Description
Recording Off		The 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		The camera is not recording. When an alarm is detected, recording commences. In this mode you will receive alert notifications from the NVR.
Recording Always with Alarm On		The camera is recording continuously with alarm detection (bump-on-alarm). In this mode you will receive alert notifications from the NVR.

Video Analysis

Depending on the VideoEdge NVR model, the following types of video analysis are available: Motion Detection, Video Intelligence, Deep Intelligence, Face Recognition, License Plate Recognition, Intelligent Search - Person, and Edge Analytics. To enable a video analytic using the camera's Advanced camera configuration page, select the required analytic from the **Video Analysis** list.

If required, you can disable a video analytic using the camera's Advanced Camera Configuration page. To disable a video analytic, select **None** from the **Video Analysis** list. When a video analytic is disabled, you will not be able to use any of the features offered by that type of video analysis. Searches and alarms based on the analytic will not be available until the analytic is enabled again.

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

Select one of the following settings from the Motion Sensitivity list: High (most results), Medium high, Medium, Medium low, Low (least results).

For more information on configuring motion detection see the *Alarms* chapter.

Enabling Motion Detection for a camera

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 its 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 11 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 framerates 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 29 Enabling Motion Detection for a camera

1. Click the **Devices** menu.
2. Click **List**.
3. Click the **Setup** icon 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** 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 the **Save** icon.

Video Intelligence and Deep Intelligence

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

Deep Intelligence is a licensed add-on for the NVR, but is only available on supported NVRs, with an integrated GPU card. While Video Intelligence is mostly used to detect objects, Deep Intelligence is used to detect people. Although Video Intelligence and Deep Intelligence use different analytic engines, they feature most of the same rules. However, the Abandon / Remove rule is only available in Video Intelligence

Note:
For more information on Deep Intelligence, refer to the *Deep Intelligence Best Practices* guide.

The NVR supports two features for Video Intelligence and Deep Intelligence:

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

There are several types of Video Intelligence and Deep 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** - (Video Intelligence only) 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.
- **Tripwire** - Used to count the number of people that cross a region of interest or calculate area occupancy over a specified area. People are counted going in, and out.

The Video Intelligence and Deep 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 or Deep Intelligence rules which are defined.

Video Intelligence and Deep Intelligence provide 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 and Deep 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 use Video Intelligence features, you must enable Video Intelligence on the NVR. To use Deep Intelligence features you must enable Deep Intelligence on the NVR.

Enabling Video Intelligence or Deep Intelligence for a Camera

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

Ensure that you have a Stream Specification that allows the NVR to generate meta-data for Video Intelligence or Deep Intelligence. You must select either **Video Intelligence** or **Deep Intelligence** from the **Video Analysis** list as required.

You can configure the minimum object height and width. Objects that are smaller than these dimensions do not generate Video Intelligence or Deep 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. For both Video Intelligence and Deep Intelligence, an error message opens if the NVR is unable to find a suitable video stream for that type of Video Analysis.

Note:

• It is recommended that you configure Video Intelligence and Deep Intelligence rules on the camera, before adding the camera to the VideoEdge.

• After you enable Video Intelligence or Deep 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 that type of Video Analysis. You cannot configure a camera for Video Intelligence if the resolution setting of the camera is outside of the settings in the table below.

Table 12 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.

On the analytics stream, the NVR requires at least 480 x 480 resolution and a frame rate of 7fps to perform Deep Intelligence activities.

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

Procedure 30 Enabling Video Intelligence for a camera

1. Click the **Devices** menu.
2. Click **List**.
3. Click the **Setup** icon of the camera 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** list.

   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 the **Save** icon.

Procedure 31 Enabling Deep Intelligence for a camera

1. Click the **Devices** menu.
2. Click **List**.
3. Click the **Setup** icon in the camera record for which you want to enable Deep Intelligence.
   The Function & Streams tab displays.

   Note:
   You can also enable Deep 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 **Deep Intelligence** from the **Video Analysis** list.

Note:
If an error message opens, the NVR cannot detect a suitable stream from the camera to support Deep 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 Deep Intelligence.

6 Select the detection sensitivity from the **Deep Intelligence Detection Sensitivity** list.
7 Click the **Save** icon.

Face Recognition

Face Recognition is a licensed add-on for the VideoEdge NVR. You can enroll people in a face recognition database for use with facial detection and recognition analytics. You can use this type of video analysis to identify individuals who are uploaded to the face enrollment database, or perform simple face detection which does not require enrollment. You can create, edit and remove entries to the database using victor. For more information, refer to the *Identity Management* section of the *victor Unified Client Administration & Configuration Guide*.

The Face Recognition analytic offers two features: Face Search Alert, which requires a Face Recognition license, and Face Verification, which requires a Face Verification license.

With a Face Recognition or Face Verification license, you must purchase a Face Enrollment tier. There are four tiers available. Each tier has a maximum supported people count:

- Tier 1: Up to 25 people
- Tier 2: Up to 100 people
- Tier 3: Up to 1000 people
- Tier 4: Up to 10,000 people

Face Recognition concepts

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

Enabling Face Recognition for a camera

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.

Procedure 32 Enabling Face Recognition for a camera

1 Click the **Devices** menu.
2 Click **List**.
3 Click the **Setup** icon of the camera you want to configure camera settings for.
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 the **Save** icon.

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 33 Enabling License Plate Recognition for a camera

1 Click the **Devices** menu.
2 Click **List**.
3 Click the **Setup** icon in the camera record 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 the **Save** icon.

Intelligent Search – Person

Intelligent Search – Person is a licensed add-on analytic for supported VideoEdge hardware. For a list of supported hardware, see *Intelligent Search - Person supported hardware*.

You can enable a camera in VideoEdge with the Intelligent Search - Person analytic, and perform a search of a saved image or Still Image Capture across multiple cameras and NVRs in victor Client.

- Watch recordings of unauthorized incidents
- Sort search results by relevance or time
- Combine all search results into a single clip that can be saved and exported

For more information, refer to the *victor Unified Client Administration and Configuration Guide*.

In VideoEdge, Intelligent Search - Person is not supported by Video Analytic alarms but detected objects can be viewed in the hit boxes as follows:

1. Open the **Devices** menu.
2. Click **Alarms**.
3. Select a camera configured with the **Intelligent Search – Person** analytic.
   Live video displays showing any object detections on that camera.

Intelligent Search - Person licensing

The Intelligent Search – Person analytic requires a license for each configured camera input. Licenses are supported for both local and centralized licensing.

To view the current Intelligent Search - Person licensing configuration:

1. Click the **System** menu
2. Click the **Licensing** menu.
3. Scroll down to the **Analytics** section. The **Intelligent Search – Person** row shows the following information:
   - The maximum cameras that can use this analytic
   - The number of licenses currently in use
   - The number of licenses still available for use

Enabling Intelligent Search - Person on a camera

1. Click the **Devices** menu
2. Click **List**. The **Video List** displays.
3. From the **Video List**, find the camera that is being configured and click the **Setup** icon. The **Functions & Streams** tab appears.
4. In the **Record Mode** list, select the record mode settings by clicking on the appropriate icon.
5. In the **Video Analysis** list, select **Intelligent Search – Person**.
   Note: The Intelligent Search - Person analytic appears in the list as visible, but will be disabled when:
   - It is a supported feature on the hardware platform
   - There are no licenses
   - All licenses are already in use
6. In the **Maximum Recording Storage Period** list, select the appropriate recording settings.
7. In the **Associate Audio** list, select the appropriate audio device or select **No Audio**.
8. In the **Auto-Configure Stream** list, select the appropriate streaming settings or select **None**.For more information, see *Enabling or disabling Auto-Configure streams*.
9. In the **Stream Configuration** box, select the appropriate camera stream settings. For more information, see *Configuring stream settings*.
10. Click **Save**.
11. In the **Video List** tab, check that the **Analytic** icon status light is purple indicating the **Intelligent Search - Person** analytic is running for the selected camera.

Enabling Intelligent Search - Person on multiple cameras

The Intelligent Search – Person analytic can be enabled on multiple cameras using the Batch Edit feature. For more information, see *Batch editing camera settings*

Intelligent Search - Person supported hardware

Table 13 Intelligent Search - Person supported hardware

VideoEdge Rack Mount NVR	
ADVER140R5DJ	140TB RAID 5, (160 Total), (2) 1Gb NIC, (2) 10Gb NIC, 2 Storage Sets, Redundant PS
ADVER100R5DJ	100TB RAID 5, (120 Total), (2) 1Gb NIC, (2) 10Gb NIC, 2 Storage Sets, Redundand PS
ADVER88R5DJ	88TB RAID 5, (96 Total), (2) 1Gb NIC, (2) 10Gb NIC, Redundant PS
ADVER72R5DJ	72TB RAID 5, (80 Total), (2) 1Gb NIC, (2) 10Gb NIC, Redundant PS
ADVER64R5DJ	64TB RAID 5, (72 Total), (2) 1Gb NIC, (2) 10Gb NIC, Redundant PS
ADVER50R5DJ	50TB RAID 5, (60 Total), (2) 1Gb NIC, (2) 10Gb NIC, Redundant PS
ADVER40R5DJ	40TB RAID 5, (48 Total), (2) 1Gb NIC, (2) 10Gb NIC, Redundant PS
ADVER30R5DJ	30TB RAID 5, (40 Total), (2) 1Gb NIC, (2) 10Gb NIC, Redundant PS
ADVER16R5DJ	16TB RAID 5, (24 Total), (2) 1Gb NIC, (2) 10Gb NIC, Redundant PS
ADVER08R0DJ	8TB RAID 0, (2) 1Gb NIC, (2) 10Gb NIC, Redundant PS
VideoEdge 2U NVR	
ADVER50R5N2G	50TB, RAID 5, (60 Total) 4 NIC, Redundant PS
ADVER40R5N2G	40TB, RAID 5, (50 Total) 4 NIC, Redundant PS
ADVER30R5N2G	30TB, RAID 5, (36 Total) 4 NIC, Redundant PS
ADVER18R5N2G	18TB, RAID 5, (24 Total) 4 NIC, Redundant PS
ADVER12R5N2G	12TB, RAID 5, (16 Total) 4 NIC, Redundant PS
ADVER10R0N2G	10TB, RAID 0, 4 NIC, includes RAID controller and redundant PS
ADVER20N0N2G	20TB, JBOD, 4 NIC, Redundant PS
ADVER10N0N2G	10TB, JBOD, 4 NIC, Redundant PS
ADVER00N0N2G	0TB, JBOD, 4 NIC, Redundant PS
VideoEdge 32 Channel Hybrid NVR	
ADVER50R5H3G	32 analog channels, 50TB, RAID 5, (60 Total), 2 NIC
ADVER40R5H3G	32 analog channels, 40TB, RAID 5, (50 Total), 2 NIC
ADVER30R5H3G	32 analog channels, 30TB, RAID 5, (36 Total), 2 NIC
ADVER18R5H3G	32 analog channels, 18TB, RAID 5, (24 Total), 2 NIC
ADVER30N0H3G	32 analog channels, 30TB, JBOD, 2NIC
ADVER20N0H3G	32 analog channels, 20TB, JBOD, 2 NIC
ADVER10N0H3G	32 analog channels, 10TB, JBOD, 2 NIC
ADVER00N0H3G	32 analog channels, 0TB, storage, 2 NIC
ADVER12N0H3G	32 analog channels, 12TB, JBOD, 2 NIC

Wearable cameras

You can add wearable cameras to VideoEdge and view the retrieved video clips in victor Client. Video clips are added to VideoEdge using a supported wearable camera management system. A security group specifies the username and password that VideoEdge uses to communicate with the supported wearable camera management system.

Note:
For more information on supported wearable camera management systems, refer to the *Wearable Camera Management Systems App Note*.

To add a wearable camera to VideoEdge, you must create a security group. You can add a security group before you add a wearable camera to VideoEdge. See *Creating a security group for a wearable camera*. You can also create a security group while adding a wearable camera to VideoEdge. See *Adding a wearable camera*.

Note:
Each wearable camera requires one IP camera license.

Creating a security group for a wearable camera

1. From the VideoEdge Admin Interface, click the **Devices** menu.
2. Click **Security**.
3. Click the **Add New Group** icon. The **Security Group** window opens.
4. In the **Group Name** and **Description** fields, enter an appropriate group name and description.
5. In the **Username** and **Password** fields, enter a username and password that VideoEdge will use to communicate with the supported wearable camera management system whose cameras will be added to VideoEdge.
6. **Optional:** Configure **Advanced Settings**.
   a. Click **Advanced**.
   b. From the **Security Level** list, select the required security level.
   c. In the **Port** section, enter the required port number.

   Note: To use the default port number, ensure the **Default** check box is selected.
7. Click the **Save** icon. The security group is added.

Adding a wearable camera

1. Click the **Devices** menu.
2. Click **List**.
3. Click the **Add New Device** icon. The **Add Device** window opens.
4. Click **Additional Settings**. More options appear in the **Add Device** window.
5. From the **Device Type** list, select **Wearable Camera**.
6. In the **Device Name** field, type a device name.
7. In the **Device IP Address** field, type the IP address of the supported wearable camera management system.
8. In the **Security Group** list, select one of the following:
   - The name of the security group you previously created. See, *Creating a security group for a wearable camera*.
   - **New Security Group**. More options appear in the **Add Device** window. For information on completing these options, see *Creating a security group for a wearable camera*.
9. From the **Slot** list, select a device slot.

   Note: Select **Auto** to auto-configure allocation of the device slot.
10. Click the **Save** icon. A page opens listing the wearable cameras that the supported wearable camera management system supports, and have not yet been added to VideoEdge.
11. Select the wearable cameras you want to add from the list.
12. In the **Slot** list, select a device slot for the selected wearable cameras.
13. To enable audio, click **Enable audio for all selected inputs**.

14 Click the **Save** icon.
15 When VideoEdge successfully adds the wearable cameras, they are displayed on the **Video List** page.

Video Upload Status for wearable cameras

The Video Upload Status page shows the status of videos being retrieved from wearable cameras and stored on VideoEdge.

To open the Video Upload Status page:
1 From the VideoEdge Admin Interface, click **Devices**.
2 Click **Options**.
3 Click the **Wearable Cameras** tab. The **Video Upload Status** page opens showing the Video Upload status table for each wearable camera.

Table 14 Video Upload Status table for wearable cameras

Status heading	Description
Camera	Name of the wearable camera
Video	Size of the video file Start and end times of the video recording
Retrieval	Start and end times for retrieving the video from the Wearable Camera Management System
Storage	Starts and end times for storing the video on the VideoEdge NVR
Status	Current status of the video uploading process
Details	Additional details of the video uploading process

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 analytics

To enable edge based analytics you must 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 can also enable edge based analytics from the Batch edit tab.

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 34 Enabling Edge analytics for a camera

1. Click the **Devices** menu.
2. Click **List**.
3. Click the **Setup** icon 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 edge based analytics (Only Record on Alarm, or Recording Always with Alarm On).
5. 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.
6. Click the **Save** icon.

Disabling a video analytic on a camera

When required, you can disable a video analytic on the Video List page, or using the camera's Advanced Camera Configuration page. When a video analytic is disabled, you will not be able to use any of the features offered by that type of video analysis. Searches and alarms based on the analytic will not be available until the analytic is enabled again.

Procedure 35 Disabling a video analytic on a camera

1. Click the **Devices** menu.
2. Click **List**.
3. Click the **Setup** icon in the camera row where you want to disable the video analytic.
   The Function & Streams page opens.
4. Select **None** from the **Video Analysis** list.
5. Click the **Save** icon.

Configuring Audio association

Select the audio device you want to associate with the camera from the **Associate Audio** list.

Audio playback is not available on 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 audio and video codec combination, these packet streams may not synchronize for live streaming. The NVR's live streaming method is to pull video and audio from the camera and push it to the client instantly. This helps achieve low video latency but sometimes at the expense of live audio and video synchronization. Recorded playback of the same audio and video may improve synchronization.

Procedure 36 Configuring Audio association

1. Click the **Devices** menu.
2. Click **List**.
3. Click the **Setup** icon 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 the **Save** icon.

Enabling or disabling 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 Streams enabled, the NVR will apply the recommended settings to the chosen analytic stream.

Auto-Configure Streams is enabled by default. To edit the Auto-Configure Streams settings, 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.

Max GOP

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

- For H264 and H265 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.

Set a maximum GOP size for a camera's H264+ stream by entering value in the **Max GOP** field.

Set the global maximum GOP size on the Options page. For more information, see the *Options* section.

Gaming Mode

Gaming Mode is a standardization setting for video cameras. Enabling Gaming Mode for a camera will maintain a constant framerate 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 must 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.

VideoEdge supports the following video codecs: H264, H264+, H265, MPEG4, and MJPEG. For more information about supported video codecs, refer to the *VideoEdge Camera Handler Release Notes*.

Codecs

VideoEdge supports the following video codecs: H264, H264+, H265, MPEG4, and MJPEG. For more information about supported video codecs, refer to the *VideoEdge Camera Handler Release Notes*.

Procedure 37 Configuring stream settings

1 Click the **Devices** menu.
2 Click **List**.
3 Click the **Setup** icon in the camera row for which you want to edit stream settings.
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 the **Save** icon.

Archive

From the Archive tab, you can configure Archiving Mode, Archiving Quality, and the 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 framerate decimation using the Archive Quality dropdown and define a maximum retention period for archived video.

Procedure 38 Configuring Archive settings

1 Click the **Devices** menu.
2 Click **List**.
3 Click the **Setup** icon in the camera row for which you want to edit archive mode.
4 Click the **Archive** tab.
5 Select the **Archiving Mode**
   - Select the **Archiving disabled** option button to disable archiving for the camera.
   - Select the **Archive all video** option button to archive all video for the camera.
   - Select the **Archive only alarm video** option button to archive video triggered with an alarm.
6 Select the **Archiving Quality** from the list.
7 Select the **Maximum Archiving Storage Period** from the list.
(Optional) If selecting **Custom**, enter the number of days in the **Period** field.
8 Click the **Save** icon.

Alerts

From the Alerts tab you can configure the Alert Pre-Buffer and Alert Post-Buffer. Buffer times range from 30 seconds to 300 seconds, defined in 10 second intervals.

The Alerts page provides a link to the **I/O List** page, where you can configure dry contacts and relay outputs.

Procedure 39 Configuring Alert recording buffers

1. Click the **Devices** menu.
2. Click **List**.
3. Click the **Setup** icon in the camera row for which you want to set alert recording buffers.
   The Function & Streams tab displays.
4. Click 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 the **Save** icon.

Multicast

You can configure multicast streaming for supported cameras. victor operators can view live steams from multicast cameras, even while the VideoEdge is offline. The Multicast tab is only available for cameras that support multicast streaming. For information about camera limitations, and 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.

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

Procedure 40 Configuring Multicast stream settings

1. Click the **Devices** menu.
2. Click **List**.
3. Select the **Setup** icon for the multicast camera that you want to configure.
   The Function & Streams tab displays.
4. Click 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 the **Save** icon.

Controls

From the Controls page, you can configure PTZ and Fisheye control settings for a selected camera.

PTZ Control Settings

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

Procedure 41 Enabling or disabling PTZ for cameras

1. Click the **Devices** menu.
2. Click **List**.
3. Click the **Setup** icon in the PTZ camera row.
   The Function & Streams tab displays.
4. Click the **Controls** tab.
5. Depending on whether you are using an analog or an IP camera, complete one of the following steps:
   - For IP cameras, select the **Enable PTZ** checkbox to enable PTZ, or deselect the **Enable PTZ** checkbox to disable PTZ.
   - For analog cameras, select the **PTZ Port** from the list to enable PTZ, or select **None** from the list to disable PTZ.
6. Click the **Save** icon.

Procedure 42 Enabling or disabling PTZ for analog cameras

1. Click the **Devices** menu.
2. Click **List**.
3. Click the **Setup** icon in the PTZ camera row.
   The Function & Streams tab displays.
4. Click the **Controls** tab.
5. Select the **PTZ Port** from the list to enable PTZ, or select **None** from the list to disable PTZ.
6. Click the **Save** icon.

PTZ 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.

Select a value from the **Return to Home** list. The available range of values is between 60 seconds and 600 seconds, in 60 second intervals.

Procedure 43 Enabling PTZ Return to Home

1. Click the **Devices** menu.
2. Click **List**.
3. Click the **Setup** icon in the PTZ camera row for which you want to enable the 'Return to Home' feature.
   The Function & Streams tab displays.
4. Click the **Controls** tab.
5. Select the **Enable PTZ** checkbox for IP Cameras, or select the **PTZ Port** from the list for analog cameras.
6. Select the **Enable Return to Home** checkbox.
   The Return to Home After list displays.

7 Select the desired period of inactivity before the camera returns to the home position from the **Return to Home After** list.
8 Click the **Save** icon.

Intelligent Guard Tour

From the Controls 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.

After you enable the Intelligent Guard Tour feature, you must configure a guard tour for the camera, through victor, or though the camera's web interface, and set the PTZ Home position for the PTZ camera.

Procedure 44 Enabling an Intelligent Guard Tour

1 Click the **Devices** menu.
2 Click **List**.
3 Click the **Setup** icon in the PTZ camera row that you want to configure.
The Function & Streams tab displays.
4 Click the **Controls** tab.
5 Select the **Enable Intelligent Guard Tour** checkbox.
6 Click the **Save** icon.

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.

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

Procedure 45 Configuring camera PTZ for an analog matrix

1 Click the **Devices** menu.
2 Click **List**.
3 Select the **Setup** icon for the camera you want to configure PTZ settings for analog matrix.
The Function & Streams tab displays.
4 Click the **Controls** tab.
5 Select the correct camera control port from the **PTZ Port** list.
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 the **Save** icon.

Fisheye Control Settings

If an unsupported fisheye camera model is added to the VideoEdge as a generic camera model, fisheye may not be supported automatically for the camera. Consequently, victor client may not recognize the device as a fisheye camera. Use the Fisheye Mode feature to force the selected device to work as a fisheye camera, or to prevent it from working as a fisheye camera. The following options are available from the Fisheye Mode list:

- **Auto** - Sets the Fisheye Mode to auto-detect so that fisheye is detected as normal.
- **Enabled** - Force enables the device to work as a fisheye camera.

- **Disabled** - Force disables the device from working as a fisheye camera.

Procedure 46 Configuring Fisheye Mode

1 Click the **Devices** menu.
2 Click **List**.
3 Click the **Setup** icon in the camera row for which you want to configure the Fisheye Mode.
4 Click the **Controls** tab.
5 Select the required mode from the **Fisheye Mode** list.
6 (Enabled mode only) Select the camera mount position from the **Mount Position** list.
7 (Enabled mode only) Select the fisheye type from the **Fisheye Type** list.
8 Click the **Save** icon.

Preset Control Settings

From the Controls page, you can configure preset control settings for wiper and speed dry features for supported PTZ cameras.

In the Preset Control Settings area, you can assign the Wiper Preset and the Speed Dry Preset to corresponding PTZ preset buttons in supported clients. After successfully configuring a preset control setting in VideoEdge, selecting the assigned preset button in supported clients triggers that action.

Only one feature can be assigned to a button at a time. The Preset Control Settings area is only available on the Controls page if it is supported for the selected camera. Currently, only Axis cameras are supported.

Procedure 47 Configuring Preset Control Settings

1 Click the **Devices** menu.
2 Click **List**.
3 Click the **Setup** icon in the camera row for which you want to configure the Preset Control Settings.
4 Click the **Controls** tab.
5 Select the required preset button from the **Wiper Preset** list.
6 Select the required preset button from the **Speed Dry Preset** list.
7 Click the **Save** icon.

OSD

You can configure on-screen display (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.

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. Use the transparency slider to apply a high contrast background which will make the OSD item more readable

Configuring the 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.

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 48 Configuring the Global OSD settings

1 Click the **Devices** menu.
2 Click **List**.
The Video List tab displays.

3 Click the **Setup** icon of the analog camera you wish to configure OSD settings for.
The Function & Streams tab displays.
4 Click the **OSD** tab.
5 Select the **Font** from the list.
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** list.
8 Click the **Save** icon.

Configuring 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.

If you use large amounts of text when configuring OSD items it is possible for the displays to overlap. Review this after configuring OSD settings, and rectify, if necessary.

Procedure 49 Configuring camera-specific OSD settings

1 Click the **Devices** menu.
2 Click **List**.
The Video List tab displays.
3 Click the **Setup** icon in the row of the analog camera you wish to edit in the Video List.
The Function & Streams tab displays.
4 Click the **OSD** tab.
5 Click the **Edit** icon 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 the **Save** icon.

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, 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.

If you are temporarily replacing a device that requires repair, replace the faulty device as described in the *Replacing an Audio or Video device* section. Once repaired, reconnect the faulty device. Apply the NVRs template file to restore all device settings. For further information on applying a template, file see the *Templates* section.

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

Replacing an Audio or Video device

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

Procedure 50 Replacing an Audio or Video device

1. Click the **Devices** menu.
2. Click **List**.
3. Click the **Edit** icon in the record of the device you want to replace.
4. Enter the IP address of the new device.
5. Click the **Save** icon.
6. Click **OK**.

Replacing an IP 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 re-add. The association with recorded text data will be lost.

Procedure 51 Replacing an IP Text device

1. Click the **Devices** menu.
2. Click **List**.
3. Click the **Text List** tab.
4. Click the **Edit** icon in the record of the device you want to replace.

5 Enter the **Port** number being used by the new device.
6 Click **Apply**.

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

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

Alarms

Alarms can be configured to trigger an action when something occurs in the camera scene. Alarms from VideoEdge can be used to raise an event, or searched in clients such as victor. The type of alarm available depends on what type of Video Analysis has been enabled in the advanced configuration settings for the camera. You can create, configure, disable, and delete alarms on the Alarms page.

For more detailed information on Video Analysis, refer to the *Video Analysis Best Practices Guide*.

Figure 9 Alarms page

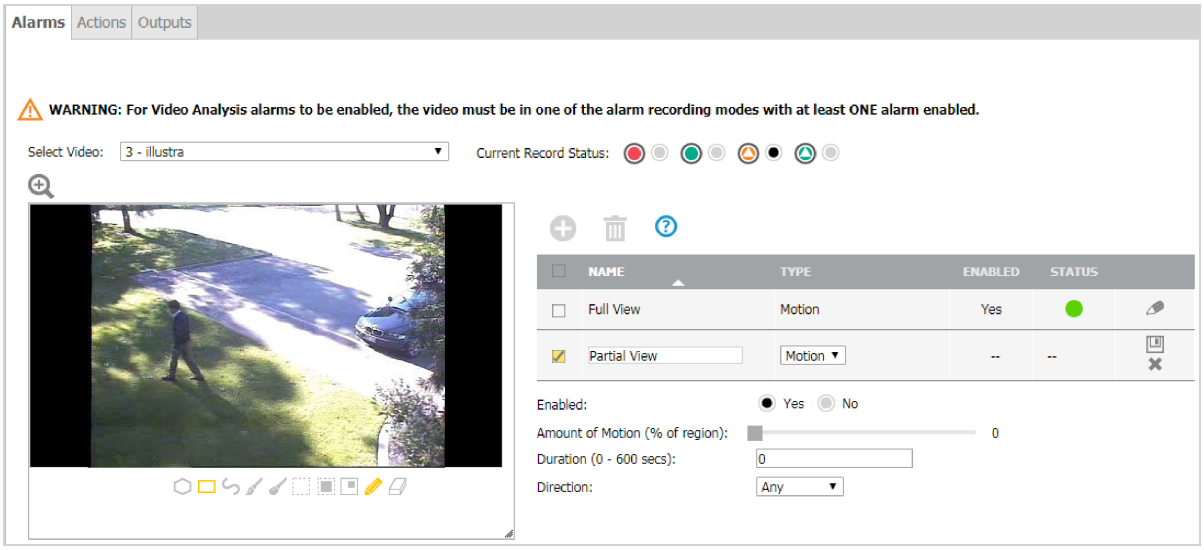


Table 15 Alarms page

Field	Description
Select Video	Select the camera for which you want to configure an alarm.
Current Record Status	Displays the current recording mode for the selected camera. The recording modes that support alarms are Only Record on Alarm, and Recording Always with Alarms.
Drawing window	Located in the left side of the page. Use the drawing tools to configure the areas that you want to monitor in the camera view
NAME	Displays the name of the alarm.
TYPE	Displays the type of alarm.
ENABLED	Displays whether or not the alarm is enabled.
STATUS	Displays the current status of the alarm. • **Red** - The alarm is disabled. Alarms will not be generated. • **Yellow** - The alarm is enabled. However, the selected recording mode does not support alarms. Alarms will not be generated. • **Green** - The alarm is enabled, and the selected recording mode supports alarms. Alarms will be generated.
Alarm configuration area	Located below the Alarms table. Configure settings and edit parameters for the alarm. The configurable options available are dependent on the alarm type selected.

Figure 10 Drawing tools

Table 16 Drawing tools

Tool Type	Options	Description
Zoom	Zoom 2X	Doubles the size of the drawing window.
Draw Style	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 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.
	Freehand	Draw using freehand by clicking on the window and dragging to draw the shape. The detection area is highlighted yellow.
Brush Size	Brush size 4	You can choose the brush size when using free draw to draw a region of interest for Video Intelligence, and Deep Intelligence alarms. Select 4x4 to draw using a thin line. 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, and Deep Intelligence alarms. Select 8x8 to draw using a thick line. This option is not available when configuring Motion Detection alarms.
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.
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.

Alarms icons table

Table 17 Alarms icons table

Icon	Name	Function
	**Zoom In**	Zoom in on the camera alarm configuration window.
	**Add**	Add new alarm, rule, trigger, or action.
	**Delete**	Delete an alarm, rule, trigger, or action.
	**Edit**	Edit an alarm, rule, trigger, or action.
	**Save**	Save
	**Cancel**	Cancel

Motion Detection alarms

After you enable Motion Detection on a camera, you can set alarm rules to trigger events.

Each camera can have up to 10 independent motion alarm rules defined. Each rule has an associated region of interest (ROI). In each ROI, you can define the areas in the camera view that you want to monitor. You can name each alarm rule. Use descriptive names like ‘Back Door’ or ‘Conference Room’, as these names make it easier to identify the alarm when using a client.

Configure the areas that you want to monitor in a camera view using the drawing window. Use the drawing tools to draw on the Camera Alarm Configuration window.

Creating a Motion Detection camera alarm

When creating a Motion Detection camera alarm you must define an alarm rule. When the activity in a cameras 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 52 Creating a Motion Detection camera alarm

1. Click the **Devices** menu.
2. Click **Alarms**.
3. Select the camera for which you want to create an alarm, from the **Select Video** list.
4. Click the **Add** icon.

   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, update the **Current Record Status**. To fully enable an alarm, use the **Only Record on Alarm**, or **Recording Always With Alarm On** recording modes.
6. Enter an alarm **Name** (max 50 characters).
7. Click the **Yes** button in the **Enabled** area to enable the alarm.
8. Select **Motion** from the **Type** list.

Note:
If **Motion** is not available in the **Type** list, you do not have Motion Detection enabled on the camera. Enable Motion Detection to continue.

9 Use the drawing tools to draw the Motion Detection region of interest (ROI) in the Camera Alarm Configuration drawing window.

Note:
You must define a ROI.

10 Use the **Amount of Motion (%)** slider to determine the percentage of the ROI with activity present for the alarm to be triggered. The higher the percentage 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 ROI 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 list 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 Click the **Save** icon.

Video Intelligence and Deep Intelligence camera alarms

Although Video Intelligence and Deep Intelligence use different analytic engines, they feature most of the same rules. As a result, these two separate but similar types of Video Analysis are discussed together in this section.

After enabling Video Intelligence or Deep Intelligence on a camera, you can define alarm rules that trigger events.

Each camera can have any number of independent Video Intelligence or Deep Intelligence rules. In each rule you can define the areas in the camera view that you want to monitor. You can name each alarm rule. Use descriptive names like ‘Back Door’ or ‘Conference Room’, as these names make it easier to identify the alarm rule in the alerts log.

Configure the areas that you want to monitor in a camera view using the drawing window. Use the drawing tools to draw on the Camera Alarm Configuration window.

Creating a Video Intelligence or Deep Intelligence camera alarm

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

To create a Deep Intelligence camera alarm, you must have Deep Intelligence enabled on the camera. Deep Intelligence is only available on supported NVRs, with an integrated GPU card.

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. If you try to create a Deep Intelligence alarm for a camera without Deep Intelligence enabled, you will be prompted to edit the camera settings.

Procedure 53 Creating a Video Intelligence or Deep Intelligence camera alarm

1 Click the **Devices** menu.
2 Click **Alarms**.
3 Select the camera for which you want to create an alarm from the **Select Video** list.
4 Click the **Add** icon.

Note:
If the **Add** icon is not available, you do not have Motion Detection, Video Intelligence, Deep Intelligence, or Face Recognition enabled on the camera.

5 If required, update the **Current Record Status**. To fully enable an alarm, use the **Only Record on Alarm**, or **Recording Always With Alarm On** recording modes.
6 Enter an alarm **Name** (max 50 characters).
7 Click the **Yes** button in the **Enabled** area to enable the alarm.
8 Select the alarm type from the **Type** list:

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** - (Video Intelligence only) 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.

k **Tripwire** - Used to count the number of people that cross a region of interest or calculate area occupancy over a specified area. People are counted going in, and out. Draw a tripwire and set the in direction, and out direction. You can set a count threshold, and a reset time. You can also group edge devices into a single object.

Note:
If these alarm types are not available in the **Type** list, you may have a different type of Video Analysis enabled. Enable Video Intelligence or Deep Intelligence to access these alarm types. The Abandon / Remove alarm type is only available in Video Intelligence.

9 Use the drawing tools to draw the region of interest (ROI) in the Camera Alarm Configuration drawing window.

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

10 Click the **Yes** button in the **Enabled** area, to enable the alarm.

11 Complete the alarm configuration fields. Depending on the Video Intelligence or Deep 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.

Tripwire

a Count Threshold - Adjust the slider to configure the count threshold. Once the threshold is reached, the counter will reset to 0.

b Reset Time - Enter a time in the 24-hour format. At the reset time, the running total resets.

12 Click the **Save** icon.

Face Recognition

Face recognition is a licensable feature that works by detecting faces and comparing them to those stored in the database of enrolled faces. To enable face recognition you must populate the NVR's Face Enrollment database. You can create, edit and remove entries to the database using victor. For more information, refer to the *Identity Management* section of the *victor Unified Client Administration & Configuration Guide*.

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, or with an exclude list, the alarm triggers when an unrecognized face is detected within the region of interest (ROI). Additional unrecognized faces within the ROI will not trigger another alarm unless the ROI 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.

Procedure 54 Creating a Face Recognition camera alarm

1 Click the **Devices** menu.
2 Click **Alarms**.
3 Select the camera for which you want to create a Face Recognition alarm from the **Select Video** list.
4 Click the **Add** icon.

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

5 If required, update the **Current Record Status**. To fully enable an alarm, use the **Only Record on Alarm**, or **Recording Always With Alarm On** recording modes.
6 Enter an alarm **Name** (max 50 characters).
7 Click the **Yes** button in the **Enabled** area to enable the alarm.
8 Click the **Include** button in the List Type for the alarm to trigger if someone in the search list is detected.
Or
Click the **Exclude** 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 or excluded in the Search List using the **Left Arrow** icon and **Right Arrow** icon.
10 Click the **Save** icon.

License Plate Recognition

License plate recognition is a licensable feature that 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 misrecognized 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
1, 7, I

Fuzzy Match Groups
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 55 Creating a License Plate Recognition alarm

1. Click the **Devices** menu.
2. Click **Alarms**.
3. Select the camera that you want to create a license plate recognition alarm for from the **Select Video** dropdown menu.
4. Click the **Add** icon.
5. If required, update the **Current Record Status**. To fully enable an alarm, use the **Only Record on Alarm**, or **Recording Always With Alarm On** recording modes.
6. Enter an alarm **Name** (maximum 50 characters).
7. Click the **Yes** button in the **Enabled** area to enable the alarm.
8. 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.
9. 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.
10. (Optional) Select the **Fuzzy Match** checkbox if required.
11. Add license plate numbers to the License list.
    a. Click the **Add** icon.
    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. Click **Open**.
12. Use the drawing tools to select an alarm's region of interest in the drawing window.
13. Click the **Save** icon.

Edge Analytics

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

You must configure edge based analytic alarms using the camera's interface. Refer to the camera's user guide for information. When you have configured alarms on the edge device, you can configure the NVR to monitor these alarms. The alarms can trigger recording and email alerts, and will be recorded in the victor activity log. You can enable or disable the alarms from the NVR Admin Interface.

There are three types of edge based analytic events supported by the NVR: motion detection, face detection, and blur detection.

Enabling Edge based camera alarms and metadata

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.

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 searches using this metadata in victor unified client.

Note:
Face Detection and Motion Detection metadata will be recorded if the camera recording status is set to Recording Always, Only Record on Alarm, or Recording Always with Alarms.

Procedure 56 Enabling Edge based camera alarms and metadata

1. Click the **Devices** menu.
2. Click **Alarms**.
3. Click the **Edit** icon for the camera alarm or metadata you want to enable.
4. Click the **Yes** button in the **Enabled** area.
5. Click the **Save** icon.

Elevated Skin Temperature

VideoEdge can connect to an Illustra Pro3 5MP Thermal Bullet EST camera and detect elevated skin temperatures using Edge Face Detection analytics. A report is sent to the VideoEdge recorder that triggers an alarm event that is viewable in live video surveillance in victor Client.

Enabling an Elevated Skin Temperature alarm

Note:
Before you begin, you must configure the Illustra camera to detect temperatures. For more information, refer to the relevant Illustra manual.

1. Enable Edge analytics on the Illustra camera. For more information, see Edge analytics.
2. Click the **Devices** menu.
3. Click **Alarms**. The **Alarms** page displays.

   Note:
   You can also open the **Alarms** page after enabling Edge analytics. When you have completed the setup on the **Functions & Streams** page, click **Configure Alarms**.
4. From the **Select Video** list, select the camera you are configuring. The camera's Edge Face Detection Alarm displays.
5. Click the **Edit** icon.
6. In the **Enabled** section, click **Yes**.
7. Click the **Save** icon. When you open the configured camera on the **Alarms** page, the status light is green when the Edge Face Detection Alarm is enabled.

Disabling a camera alarm

When a 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 57 Disabling a camera alarm

1 Click the **Devices** menu.
2 Click **Alarms**.
3 Click the **Edit** icon the alarm you want to disable.
4 Click the **No** button in the **Enabled** area.
5 Click the **Save** icon.

Actions

Event-based rules can be configured from the Actions page. Events are based on state changes and can involve camera alarms, system changes within the NVR itself, or added dry contact sensors. You can create and configure rules to cause the following actions:

- **Camera Recording** - A change of input state will initiate recording on the selected camera. Note that 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. Note that 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 and the state changes to high, the video starts recording.
• **Door closes** - The state changes to low and Alarm Post Buffer, the video stops recording.

- **PTZ to preset** - A change of input state will cause the selected camera to move to a designated PTZ preset.
- **Relay output** - A change of input state will set the selected relay output to Off, On, or Pulse.

Procedure 58 Adding a Rule

1 Click the **Devices** menu.
2 Click **Alarms**.
3 Click the **Actions** tab.
4 Click the **Add** icon above the **Rules** table.
5 Enter a rule **Name**.
6 Click **Yes** in the **Enabled** area to enable the rule, or click **No** to disable the rule.
7 Click the **Add** icon above the Triggers table.
8 Select an event from the **Event** list.
9 Select the state from the **State** list.
10 Select a device from the **Device** list.
11 Select a value from the **Alarm** list.
12 Enter the interval value in the **Interval (Sec)** field, if required.
13 Repeat steps 7-10 to add additional triggers. To remove a trigger, select the appropriate checkbox and click the **Delete** icon.

14 Click the **Add** icon above the Actions table.
15 Select an action from the **Action** list. If PTZ to Preset is selected, the Value list displays.
16 Select the device from the **Device** list.
17 (PTZ to preset only) Select the preset number from the **Value** list.
18 (Relay output only) Select Off, On, or Pulse from the **Value** list.
19 Repeat steps 14-18 to add additional actions. To remove an action, select the appropriate checkbox and click the **Delete** icon.
20 Click the **Save** icon.

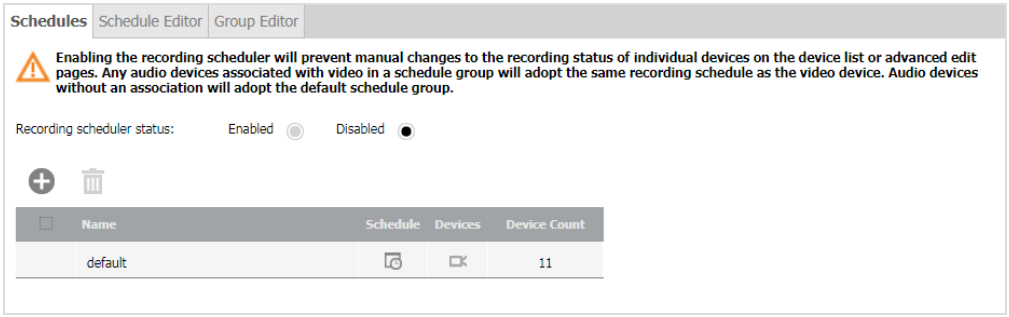
Outputs

The Outputs page features a link which redirects you to the IO List page. See the *IO List* section for more information.

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 11 Scheduler page



There are three tabs within the Scheduler menu.

- **Schedules**: Enable or disable the scheduler, create or remove schedules, and edit schedule names.
- **Scheduler Editor**: Set and edit the schedule times and recording modes for each period. Select the schedule you want to edit from the **Group ID** list.
- **Group Editor**: 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 must set up your scheduler groups, set the schedule times and recording modes for the schedule groups, and assign cameras to the schedule groups.

Scheduler icons table

Table 18 Scheduler icons

Icon	Name	Function
	Add Schedule Group	Add schedule group.
	Remove Schedule Group	Remove schedule group.
	Edit group times	Open Schedule Editor to edit group schedule times.

Icon	Name	Function
	**Edit group cameras**	Open Group Editor to edit camera groups.
	**Save**	Save
	**Cancel**	Cancel
	Right Arrow	Move selected cameras to a group.
	Left Arrow	Remove selected cameras from a group.
	**Edit**	Edit a schedule name.

Procedure 59 Creating a recording schedule

1 Click the **Devices** menu.
2 Click **Scheduler**.
3 Click the **Add** icon.
The new group is added to the schedule groups table.
4 Enter the Schedule **Name**.
5 Click the **Save** icon.
6 Select the **Edit Group Times** icon in the schedule group record you want to configure.
The Schedule Editor tab displays.
7 Select the option buttons representing the days 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 the **Save** icon.
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 Click the **Group Editor** tab.
13 Select the cameras you want to be in this schedule group by selecting the checkboxes for the cameras from the **All other devices** list, and use the **Left Arrow** icon to move them to the **This group** list.

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

14 Click the **Save** icon.
15 (Optional) Repeat steps 3 to 12 to configure additional schedule groups for the camera schedule.

Procedure 60 Enabling or disabling a camera schedule

1 Click the **Devices** menu.
2 Click **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.

Editing 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.

Procedure 61 Editing the Recording Schedule for a group

1 Click the **Devices** menu
2 Click **Scheduler**.
3 Click the **Schedule Editor** tab.
4 Select the group you want to edit from the **Group ID** list.
5 Edit the recording schedule as required by selecting the days, the recording mode, and start and end hours.
6 Click the **Save** icon.
7 (Optional) If further changes are required repeat Steps 5 and 6.

Editing the cameras assigned to a Schedule Group

You can add or remove cameras to and from a schedule group as required.

Procedure 62 Editing the cameras assigned to a Schedule Group

1 Click the **Devices** menu.
2 Click **Scheduler**.
3 Click the **Group Editor** tab.
4 Select the group you want to edit from the dropdown.
5 Select the required camera checkboxes and use the **Left Arrow** icon and **Right Arrow** icon to move cameras between the **All other devices** 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 the **Save** icon.

Security

When an IP device such as a camera, encoder, dry contact, or relay output, is added to an NVR, the server uses the manufacturer's default communication and security settings to communicate with the device. Administrators can change the default settings. However, when these are changed the NVR can no longer communicate with the device using the default settings.

If you change the security settings for a device or a number of devices, usually through direct web interfaces, you must create a Security Group for those devices and assign it the same password.

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

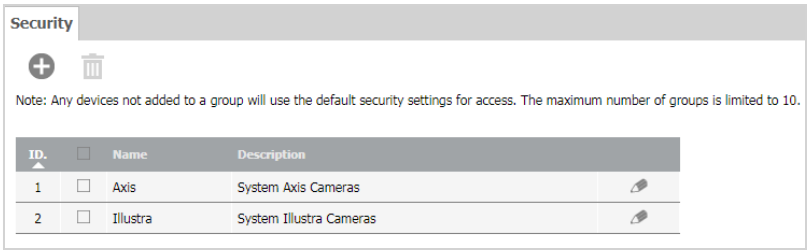
The Security Groups feature does not change the password on the device. It determines what password is used by the NVR to communicate with devices. You must change the password on the device before you change the password for the security group using the Security feature. Otherwise those devices will not be able to connect to the NVR.

In addition to configuring the username and password, you can also configure the Port Number and Security Level used for communications.

The Port Number is the HTTP or HTTPS port number which has been specified for communication. The default port number will be used to communicate with the device unless you specify a port. You must ensure the port number is correctly configured on the corresponding device for communication to be established.
The Security Level is the protocol which will be used to communicate with the devices.

After you delete a security group, the NVR will try to communicate with the devices which made up the deleted group using the manufacturer's default credentials. Prior to deleting a security group, reconfigure each device in the group to use the manufacturer's default credentials to ensure video streaming and recording is not interrupted. Alternatively, you can remove devices from the security group, or reassign devices to a new security group.

Figure 12 Security page



Security icons table

Table 19 Security icons

Icon	Name	Function
	Add New Group	Add new security group.
	Remove Group	Remove security group.
	Password Reveal, **Press to reveal the password**	Reveal the entered password.
	Right Arrow	Move selected cameras to a group.
	Left Arrow	Remove selected cameras from a group.
	Save	Save
	Cancel	Cancel
	Edit	Edit a security group.

Creating a Security Group

If a password has been changed for a device, the NVR is no longer able to communicate with the device. You must create a security group containing the new password and assign the device with this password to it.

Procedure 63 Creating a Security Group

1. Click the **Devices** menu.
2. Click **Security**.
3. Click the **Add New Group** icon.
   The Security Group window opens.
4. Enter a **Group Name**.
5. Enter a **Description**.
6. Select the **Set Username/Password** checkbox.
7. Enter a **Username**.
8. Enter a **Password**.

Note:
This is the device username and password that VideoEdge uses to connect to the devices in this security group. To use the device's default credentials, do not enter a username or password.

9 (Optional) Click and hold the **Password Reveal** icon, to view the password.

10 (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 devices in this group use ONVIF communication protocols.

11 Select the devices you want to assign to the security group by using the **Right Arrow** icon and **Left Arrow** icon.

12 Click the **Save** icon.

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.

Discovery

The Auto 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.

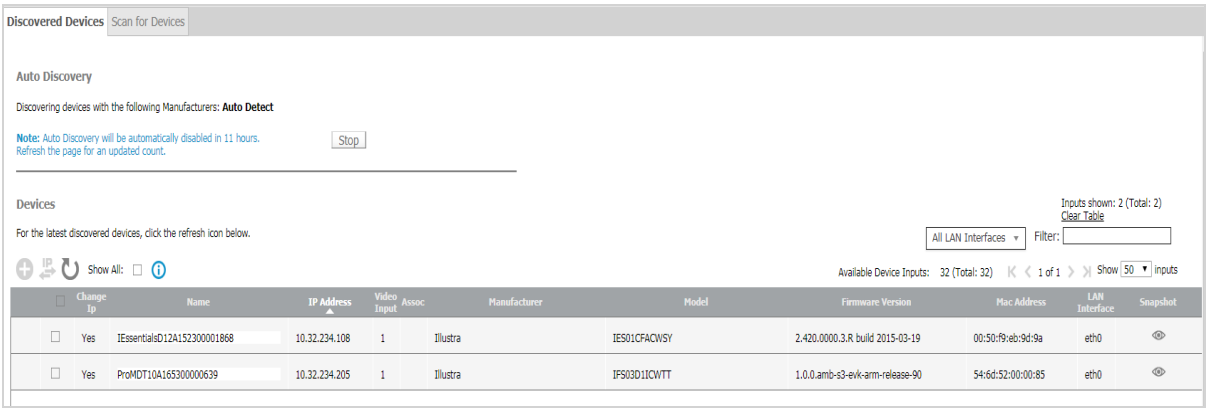
To discover devices, the NVR uses standard discovery protocols such as: MDNS, UPnP/SSDP, and ONVIF/WS-Discovery. The NVR will discover video devices on the network that have these standard protocols enabled.

The NVR discovery feature supports changing the IP addresses of American Dynamics 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, you can configure Security Groups 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 13 Discovery page



Discovery icons table

Table 20 Discovery icons

Icon	Name	Function
	**Add New Device**	Add discovered device.
	Change IP	Change the IP address of a device.
	**Refresh**	Refresh the Devices list.
	**Add Security Group**	Add security group.
	**Snapshot**	View a camera snapshot
	**Arrow up**	Sort list in ascending order.
	**Arrow down**	Sort list in descending order.
	**Save**	Save
	**Cancel**	Cancel

Discovered Devices

Information on all discovered devices is displayed on the Discovered Devices page. From this page, you can add cameras, 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 searches for devices using Auto Detect.

Starting Auto Discovery will also enable NVR discovery. Auto Discovery will remain active for 12 hours once started.

The discovered devices are displayed in the Devices table. You can view technical information about the device and configure some device settings, such as the device name and IP address, from the Devices table.

Click the **Refresh** icon to begin a new search for the latest discovered devices.

Click **Clear Table** to clear the Devices table of discovered devices. Clearing the Device table can be useful if the user accounts on a device change, or if the number of encoder inputs on a device change. 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.

View camera snapshots by clicking the **Snapshot** icon for the relevant camera in the Devices table.

Procedure 64 Adding a device using Auto Discovery

1. Click the **Devices** menu.
2. Click **Discovery**.
   If Auto Discovery is running and you want to specify different manufacturers, click **Stop**.
3. Select the device manufacturers you want to search for from the **Manufacturers** list.
   If you do not want to specify the manufacturer, or the manufacturer doesn't appear in the list, select **Auto Detect**.
4. Click **Start**.
5. (Optional) Click the **Add Security Group** icon to create a new security group.

6 Select the checkboxes for the devices that you want to add to the NVR from the **Devices** table.
7 (Optional) Edit the device **Name**.
The new device name will be applied when the device is added.
8 Click the **Add New Device** icon.
The Add New Device Settings window displays.
9 (Optional) Select a Security Group from the **Add With Security Group** list.
10 (Optional) Select the number of additional live streams from the **Auto-Configure Streams** list.
11 (Optional) Clear the **Default Associations** checkbox.
12 (Optional) Clear the **Enable Smart Search (Motion Metadata)** checkbox.
13 Click the **Save** icon.
After a device is added, it is displayed in the Video List or Audio List tabs.

Procedure 65 Changing the IP address of a device

1 Click the **Devices** menu.
2 Click **Discovery**.
3 On the **Devices** table, select the checkbox of the 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 the **Save** icon.

Scanning for devices manually

Some cameras do not support standard discovery protocols. To discover these cameras you can use the NVR to perform a manual network scan for devices. You can specify manufacturers, security groups, and network interfaces when scanning for devices.

Procedure 66 Scanning for devices manually

1 Click the **Devices** menu.
2 Click **Discovery**.
3 Click the **Scan for Devices** tab.
4 Select the device manufacturers you want to search for from the **Manufacturers** list.
If you do not want to specify the manufacturer, or the manufacturer doesn't appear in the list, select **Auto Detect**.
5 (Optional) Select the Security Group from the **Scan With Security Group** list.
6 (Optional) Select the LAN Interface from the **LAN Interface** list.
7 (Optional) Configure the IP address search range.
a Select the **Specify IP Address Range** checkbox.
b Enter the **IP Address Range**.
8 Click **Start**.
After the scan is complete, the discovered devices are displayed in the **Devices** table.
9 (Optional) Click the **Add Security Group** icon to create a new security group.
10 Select the checkboxes for the devices that you want to add to the NVR from the **Devices** table.
11 Click the **Add New Device** icon.
The Add New Device Settings window displays.
12 (Optional) Select a Security Group from the **Add With Security Group** list.
13 (Optional) Select the number of additional live streams from the **Auto-Configure Streams** list.
14 (Optional) Clear the **Default Associations** checkbox.
15 (Optional) Clear the **Enable Smart Search (Motion Metadata)** checkbox.

16 Click the **Save** icon.
After a device is added, it is displayed in the Video List or Audio List tabs.

Disabling NVR UPnP advertisements

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 67 Disabling NVR UPnP advertisements

1 Click the **Network** menu.
2 Click **General**.
3 In the UPnP row, select the **Disabled** option button.
4 Click the **Save** icon.
UPnP is now disabled.

Troubleshooting Auto Discovery

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 enables NVRs to share transcoding resources, or to be monitored for failover. You must enable SSH before you can add NVRs to an NVR Group.

NVR Group icons table

Table 21 NVR Group icons

Icon	Name	Function
	**Add**	Add new group, or discovered NVR.
	**Remove**	Remove NVR group
	**Refresh**	Refresh group lists.
	**Configure Failover**	Open window to configure the failover role for the NVR.
	**Submit**	Save the failover role settings.
	**Close**	Close window without saving failover settings.

Transcoding

Video Transcoding is the dynamic manipulation of video stream properties, such as the codec used, frame-rate, resolution, and more, in order to better manage network bandwidth or resources. Depending on the 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 automatically manages which VideoEdge units in the group perform the transcoding, and 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.

You can add up to fourteen NVRs to a group; up to two secondary NVRs, and up to twelve primary NVRs.

Procedure 68 Manually adding an NVR to an NVR Group

1 Click the **Devices** menu.
2 Click **NVR Group**.
3 Click the **Add** icon.

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 the **Save** icon.
The NVR will be added with 'Non-failover NVRs' status.

Procedure 69 Adding an NVR to an NVR Group using Discovery

1 Click the **Devices** menu.
2 Click **NVR Group**.
The NVR Group List page opens.
3 Select the **Discovered NVRs** tab.
The Discovered NVRs page opens. When Discovery is enabled, all discoverable NVRs will be displayed in the table. You can refresh the list by clicking the **Refresh** icon.

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 Click the **Add** icon.
The NVR is added with 'Non-failover NVRs' status.

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 70 Configuring a Primary NVR

Note:
You cannot enable failover for a system if there are more than 128 cameras configured. You cannot add more than 128 cameras to a failover-configured system.

1 Click the **Devices** menu.
2 Click the **NVR Group**.
3 Click the **Edit** icon 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** list.
5 Enter the **Camera Network Address** in the field or select from the list.
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 the **Save** icon.

Procedure 71 Configuring a Secondary NVR

1 Click the **Devices** menu.
2 Click **NVR Group**.
3 Click the **Edit** icon 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** list.
5 Select the **Priority** from the list.

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 the **Save** icon.

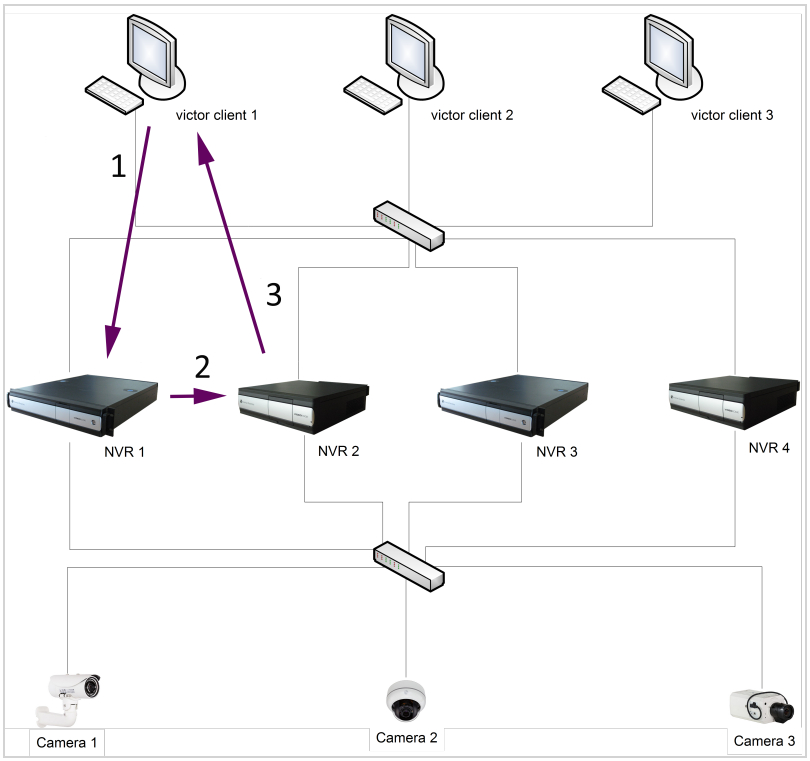
SmartStream

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.

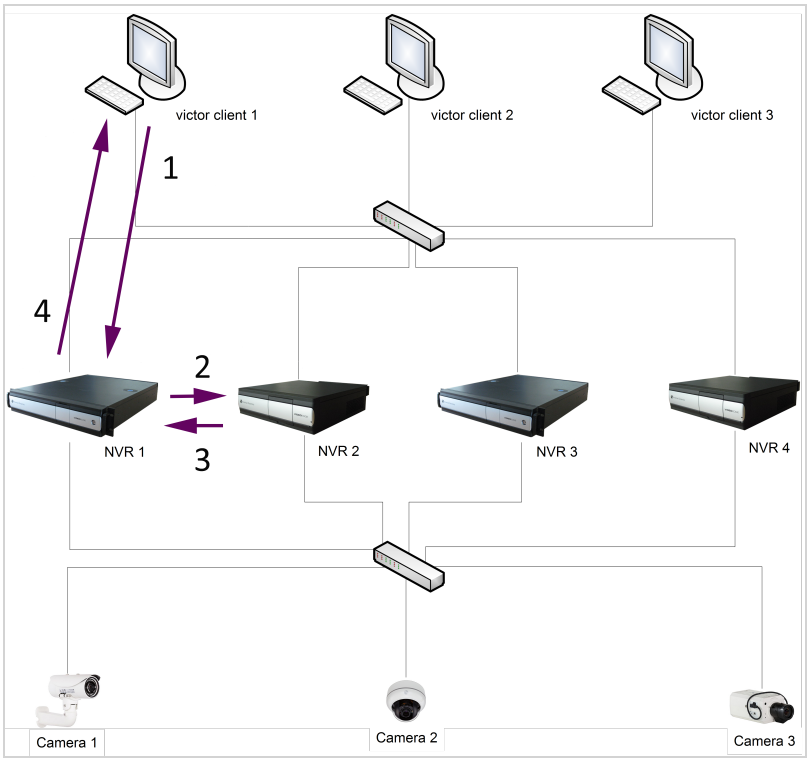
The examples below illustrate the remote transcoding process, firstly over user datagram protocol (UDP), and secondly, over transmission control protocol (TCP) and wide area network (WAN). Four NVRs are in the same NVR group, and an operator is using victor Client to stream video from cameras that are 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 14 NVR Groups - Network Example using UDP



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.

Figure 15 NVR Groups - Network Example using TCP or WAN



1 victor Client issues request for transcoded video over TCP, while no local transcode resources are available.
2 NVR 1 sends the source video to NVR 2.
3 NVR 2 transcodes the video and sends it back to NVR 1.
4 NVR 1 sends the transcoded video to the victor Client.

In addition to video streaming from the source NVR to the transcoding NVR, health information and configuration messages 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. An 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 management 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.

Configuring Failover Mode for an NVR

You must install and configure an NVR that is going to be used as a secondary NVR in the same way as a primary NVR. You must configure media folders and storage sets. 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:
You cannot enable failover for a system if there are more than 128 cameras configured. You cannot add more than 128 cameras to a failover-configured system.

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 secondary NVR's network connection should have the same capability as the network connection from the primary NVRs to the client. If the secondary NVR is connected using a lower bandwidth connection than the primary NVR, there may be 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 72 Terminating Failover

1. Restore the Primary NVR.
2. Click the **Devices** menu.
3. Click **NVR Group**.
   The NVR Groups page opens.
4. Click the **Terminate Failover** icon in the table entry of the secondary NVR you want to return to monitoring mode.

If Failover doesn’t occur

If Failover doesn’t occur ensure the following are set up as required:

- The secondary NVR is suitably licensed 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 Failover for an NVR group, all NVRs in the group must be upgraded to at least VideoEdge 4.7.

Note:
Failover does not function when the software running on a Secondary NVR is older than that running on any of the Primary NVRs.

It is recommended that you should upgrade all NVRs in the same maintenance window when a Failover system is present to ensure the time period without failover redundancy is minimized.

Procedure 73 Upgrading NVRs when Failover is enabled

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 (default HTTPS) must be applied identically on the primary NVR and on all the secondary NVRs on its active monitoring list for failover to function correctly.

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 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.

Options icons table

Table 22 Options icons

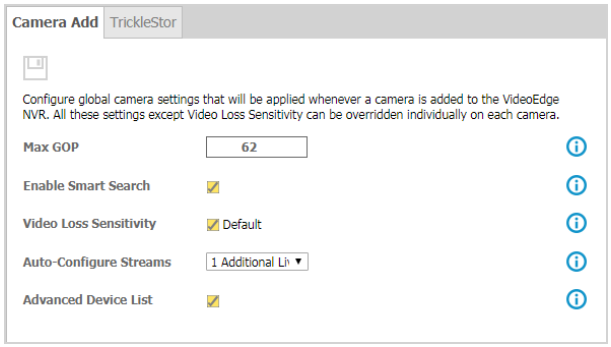
Icon	Name	Function
	**Save Changes**, **Save**	Save
	**Cancel**	Cancel
	**Enable Offline Recording**	Enable offline recording for selected camera.
	**Disable Offline Recording**	Disable offline recording for selected camera.

Camera Add

From the Camera Add page, you can configure Max GOP, Enable Smart Search, Video Loss Sensitivity, Auto-Configure Streams, and Advanced Device List settings.

These settings automatically apply to any camera that you add to VideoEdge. However, some settings are not compatible with every brand of camera.

Figure 16 Camera Add page



Max GOP

A GOP is a group of pictures. Camera video streams are comprised of 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. 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.

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 on the Discovered Devices page, the Scan for Devices page, and the Add Camera Manually dialog box. If you disable Smart Search from the Camera Add page, the checkbox is de-selected at these locations. Select the checkbox on any of these pages or dialogs to activate the feature.

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, 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 on the List page, and edit the camera alarm settings on the Alarms page. For more information, see the *Devices* section.

This feature is disabled by default for all R7-Series VideoEdge units.

Procedure 74 Enabling Smart Search by default

1 Click the **Devices** menu.
2 Click **Options**.
3 Select the **Enable Smart Search (Motion Metadata)** checkbox.
4 Click the **Save** icon.

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 75 Editing the Video Loss Sensitivity

1 Click the **Devices** menu.

2 Click **Options**.
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 set a numerical value between 5 seconds and 20 seconds.
• If you re-select the **Default** checkbox, the Video Loss Sensitivity returns to 5 seconds.

Enabling auto-configuration for camera streams

The Auto-Configure Streams setting can be enabled to automatically configure additional streams when you add new devices to your VideoEdge.

Procedure 76 Enabling auto-configuration for camera streams

1 Click the **Devices** menu.
2 Click **Options**.
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.
4 Click the **Save** icon.

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. The transfer rate can be configured on the TrickleStor page. 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.

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.

If you configured an archive for your VideoEdge, you can also transfer this footage to the archive. See the *Archive* section for more information about configuring an archive.

Note:
Offline recording does not support audio or analytics, even if the camera normally supports these features.

Prerequisites for TrickleStor

- You must upgrade the VideoEdge to version 5.0 or higher
- You must upgrade the camera firmware to the most recent version
- The cameras must be fitted with a microSD 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 77 Enabling offline recording

1. Click the **Devices** menu.
2. Click **Options**.
3. Click the **TrickleStor** tab.
4. Select cameras from the **Supported Cameras** list.
5. Click the **Enable Offline Recording** icon.
6. (Optional) Set the transfer rate.
   a. Select the transfer rate from the **Transfer Bitrate Cap** list.
   b. Click the **Save** icon.
7. (Optional) Filter the camera events list.
   a. Configure the **Start Date/Time**.
   b. Configure the **End Date/Time**.
   c. Click **Apply**.

Storage

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. The Storage menu contains the following submenus:

- **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. You can view the RAID status of your NVR, and if applicable, configure some software RAID settings. The Advanced submenu contains the following sections: **Media Folders**, **Storage Sets**, **Assign Devices**, and **RAID**.

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. The limit per storage set is based on the throughput of the NVR platform. However, when exceeding 32 devices or cameras, ensure storage sets are load balanced. Ensure that storage sets do not exceed 100 mb/s on JBOD platforms. Single HDD platforms permit only one 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.

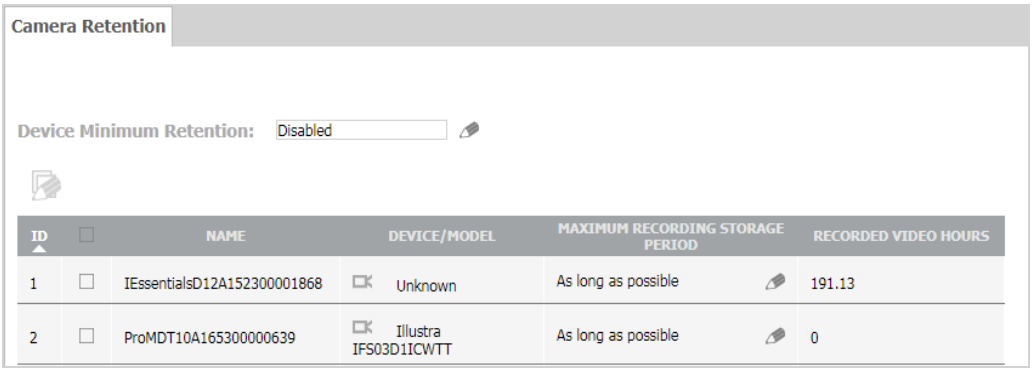
Caution

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 17 Camera Retention page



Camera Retention icons table

Table 23 Camera Retention icons

Icon	Name	Function
	Edit	Edit
	Batch Edit	Edit multiple cameras.
	Save	Save
	Cancel	Cancel

Configuring the device minimum retention period

The Device Minimum Retention period is used to generate a warning notification on the system if previously recorded video will not be kept, or is at risk of not being kept, for the defined expected minimum retention storage period. The Device Minimum Retention setting is disabled by default. Configure the custom value for the expected retention period. This will be applied to all cameras on the list.

Note:
This is just a warning notification. Recorded media will be culled automatically when the Media Storage has reached 95% storage fill, to allow space for the newly recorded camera video.

Procedure 78 Configuring the device minimum retention period

1 Click the **Storage** menu.
2 Click **Camera Retention**.
3 In the **Device Minimum Retention** field, click the **Edit** icon.
4 Enter a value for the retention period in the **Days** and **Hours** fields.

Note:
To disable the device minimum retention period, select the **Disabled** button.

5 Click the **Save** icon.

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, the recorded video per camera will be kept for as long as possible. However, there are some circumstances under which you may choose to keep video for a shorter retention period than the minimum overall retention period, as defined in the **Device Minimum Retention** field. You can define for lower priority cameras a custom maximum value per camera which will always be less than the minimum, thus deleting their video earlier, and creating space for higher priority cameras.

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 79 Configuring the device maximum recording storage period

1 Click the **Storage** menu.
2 Click **Camera Retention**.
3 In the device's **Maximum Recording Storage Period** field, click the **Edit** icon.
4 Click **As long as possible**, or click the custom period button, and enter a value for the retention period in the **Days** and **Hours** fields.
5 Click the **Save** icon.

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
- View the status of RAID storage
- Recorder Deactivation on Storage Failure

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.

Advanced Storage icons table

Table 24 Advanced Storage icons

Icon	Name	Function
	**Edit**	Edit
	**Add USB Device**	Add USB device.
	**Enable Media Folder**	Enable selected media folder.
	**Disable Media Folder**	Disable selected media folder.
	**Save**	Save
	**Cancel**	Cancel
	**Add**, **Add Storage Set**	Add storage set or device.
	**Run Load Balancer**	Create a camera redistribution proposal.
	**Delete**	Delete
	**Batch Edit**	Edit multiple devices.

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. 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 18 Media Folders page

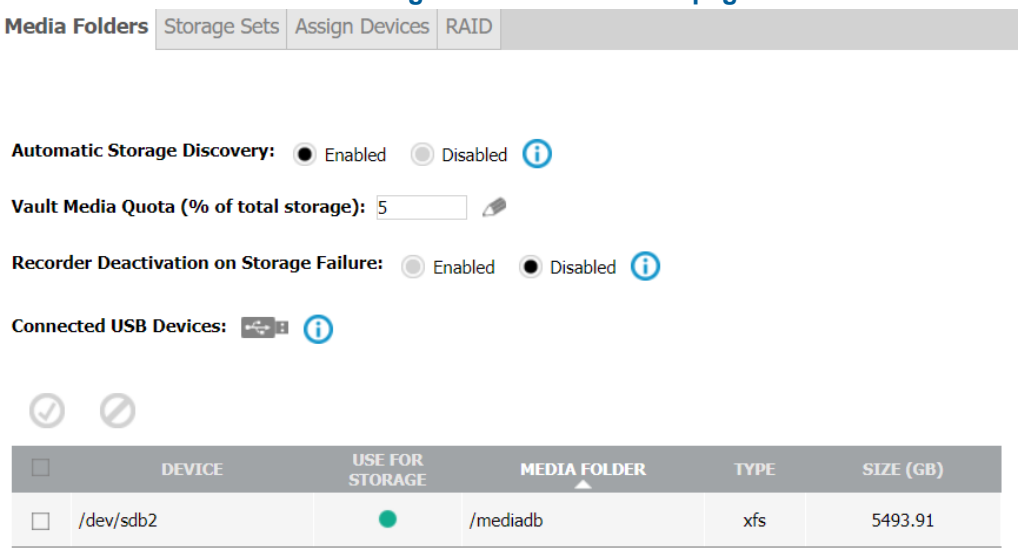


Table 25 Storage configuration fields

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 80 Adding USB storage devices to VideoEdge

1. Click the **Storage** menu.
2. Click **Advanced**.
3. Click the **Add USB Device** icon.
4. Select a USB device from the table.
5. Click the **Add USB Device** icon.

Note:
A pop-up window opens asking 'Do you wish to delete all previously recorded media from all selected USB devices?'. Click the **Yes** icon or **Cancel** icon as required.

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 81 Enabling media folders for storage

1 Click the **Storage** menu.
2 Click **Advanced**.
3 Select the checkbox for the media folder you want to use for storage and click the **Enable Media Folder** icon.

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.

Disabling a storage media folder

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 82 Disabling a storage media folder

1 Click the **Storage** menu.
2 Click **Advanced**.
3 Select the checkbox for the media folder you want to use for storage and click the **Disable Media Folder** icon.
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.

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 83 Setting a Vaulted Media quota

1 Click the **Storage** menu.
2 Click **Advanced**.
3 Click the **Edit** icon next to the **Vaulted Media Quota (% of total storage)** field.
4 Enter a value in the **Vaulted Media Quota (% of total storage)** field.
5 Click the **Save** icon.

Recorder Deactivation on Storage Failure

When you enable Recorder Deactivation on Storage Failure, a storage failure that prevents recording will trigger the automatic shutdown of the VideoEdge NVR. This enables a secondary failover NVR to compensate for the primary NVR's storage failure.

When services have been shut down because of a storage failure, a message displays in the Web GUI:

Service currently shut down due to recording failure

Enabling an NVR for Recorder Deactivation on Storage Failure

1 Click the **Storage** menu.
2 Click **Advanced**. The Media Folder window displays.
3 On the **Recorder Deactivation on Storage Failure** list, select **Enabled**. A warning message displays. Click **OK**. The settings are configured.

Note: If a storage error is detected, an error message displays. Click on the error message for more information. When the error is resolved, the error message disappears.

Creating an NVR group with Recorder Deactivation on Storage Failure

For more information on NVR groups, see NVR Group

1 Click **Devices**.
2 Click **NVR Group**. The **NVR Group List** tab opens.

Note:
You can also create an NVR group using the **Discovery** tab. See*Adding an NVR to an NVR Group using Discovery*.

3 Click the **Add** icon. The **Add NVR** window displays.
4 From the **Add NVR** list, select the name or local interface of the NVR to add to the NVR group.
5 Click the **Save** icon. The NVR appears in the Non-failover NVRs list.
6 The **Add NVR** window displays. You can add additional NVRs by typing the NVR address into the field.
7 Chose an NVR for Primary failover and click the **Edit** icon. The **Configure Failover on this NVR** window opens.
8 In the **Failover Role** list, change the default from **No Failover Role** to **Primary**. The **Deactivate when unable to record** checkbox is automatically enabled when you select **Primary** failover for the NVR.
9 Chose an NVR for Secondary failover and click the **Edit** icon. The **Configure Failover on this NVR** window opens.
10 In the **Failover Role** list, select a failover role. The default is **Current Setting**.

11 Continue to configure the remaining NVRs in the NVR group. For more information, see *NVR Group Architecture* .

Storage Sets

By default, one storage set is created for each storage drive and all analog cameras are assigned to Storage Set 1.

The default storage set created on the NVR 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 19 Storage Sets page

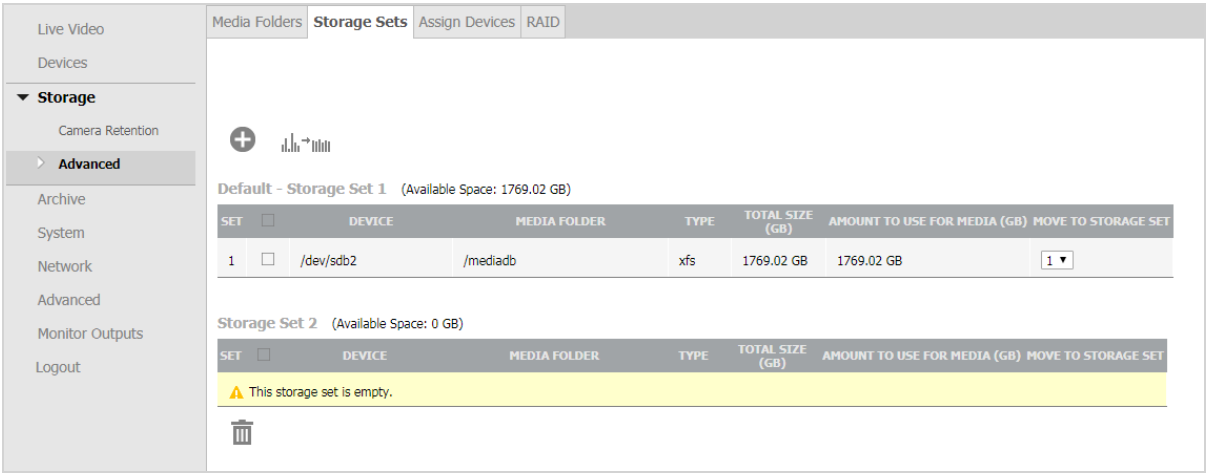


Table 26 Storage Sets configuration fields

Field	Description
Set	This is the Storage Set the media folder is assigned to.
Device	This is a physical device detected by the NVR
Media Folder	The location on the device where recorded media will be stored.
Type	Indicates the file system type, for example; XFS.
Total Size (GB)	The total size of the storage device in GB.
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.
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.

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.

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 must reassign these from another storage set.

Procedure 84 Creating Storage Sets

1. Click the **Storage** menu.
2. Click **Advanced**.
3. Click **Storage Sets**.
4. Click the **Add Storage Set** icon.
   A new storage set is created.

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 system's 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 85 Assigning / Reassigning media folders to a Storage Set

1. Click the **Storage** menu.
2. Click **Advanced**.
3. Click the **Storage Sets** tab.
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** list.
   The media folder is reassigned to the new storage set.

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.

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, on software-only deployments, such as Virtual Machines, or on platforms that have a RAID card installed.

If you accept the Camera Redistribution Proposal, VideoEdge may make the following changes to your storage configuration.

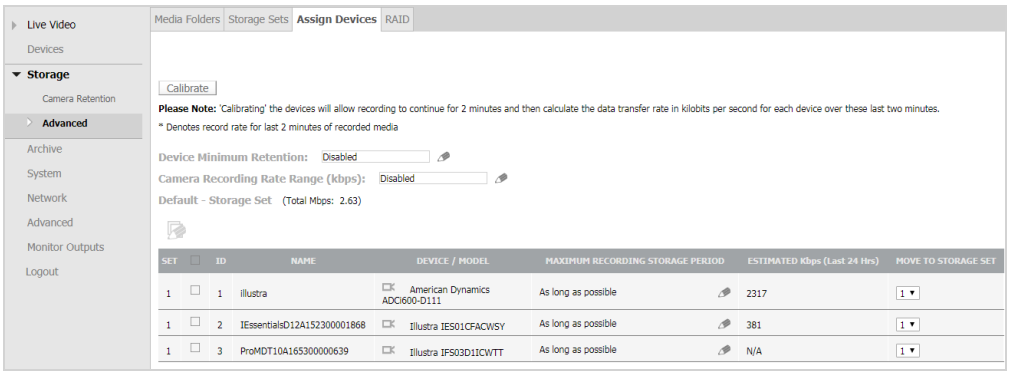
- Reassign media folders to different storage sets
- Reassign cameras to different storage sets

Procedure 86 Calculating camera redistribution

1. Click the **Storage** menu.
2. Click **Advanced**.
3. Click the **Storage Sets** tab.
4. Click the **Run Load Balancer** icon to create a camera redistribution proposal.
5. Click the **Save** icon to accept the proposed camera redistribution changes, or click the **Cancel** icon to reject the proposed camera redistribution changes.

Assign Devices

Figure 20 Assign Devices page



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 87 Reassigning a camera to a different storage set

1. Click the **Storage** menu.
2. Click **Advanced**.
3. Click 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** list.
   The camera is reassigned to the selected storage set.

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.

Procedure 88 Calibrating cameras

1. Click the **Storage** menu.
2. Click **Advanced**.
3. Select the **Assign Devices** tab.
   A summary of cameras assigned to storage sets is displayed.
4. Click **Calibrate**.
   The **Estimated Kbps** field for each camera is updated with the data transfer rate for the last two minutes.

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 89 Configuring the device minimum retention period

1. Click the **Storage** menu.
2. Click **Advanced**.
3. Click the **Assign Devices** tab.
4. In the **Device Minimum Retention** field, click the **Edit** icon.
5. Enter a value for the retention period in the **Days** and **Hours** fields.

   Note:
   To disable the device minimum retention period, select the **Disabled** button.

6. Click the **Save** icon.

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 90 Configuring the camera recording rate range

1. Click the **Storage** menu.
2. Click **Advanced**.
3. Click the **Assign Devices** tab.
4. In the **Camera Recording Rate Range (kbps)** field, click the **Edit** icon.
5. Enter values in the **MIN** and **MAX** fields.

   Note:
   To disable the recording rate range, select the **Disabled** button.

6. Click the **Save** icon.

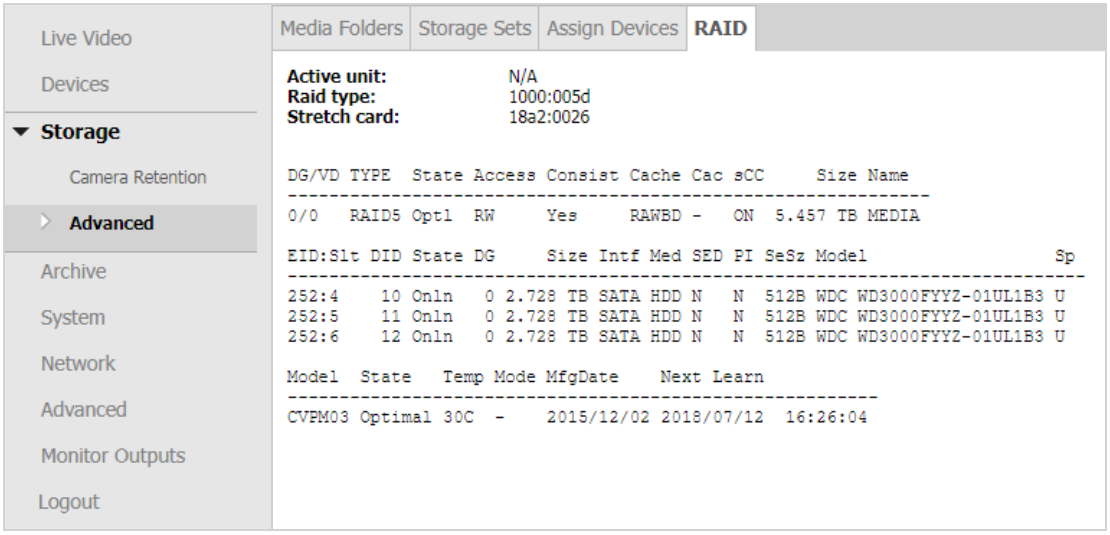
RAID

The RAID page has different functionality depending on the type of VideoEdge NVR you are using, and if it is configured for RAID storage. The format of the RAID page may differ depending on the hardware RAID controller installed on the NVR.

If the NVR has no RAID storage, the page displays, "No RAID units detected".

If the NVR has RAID storage configured, the page displays the status of the RAID.

Figure 21 RAID page

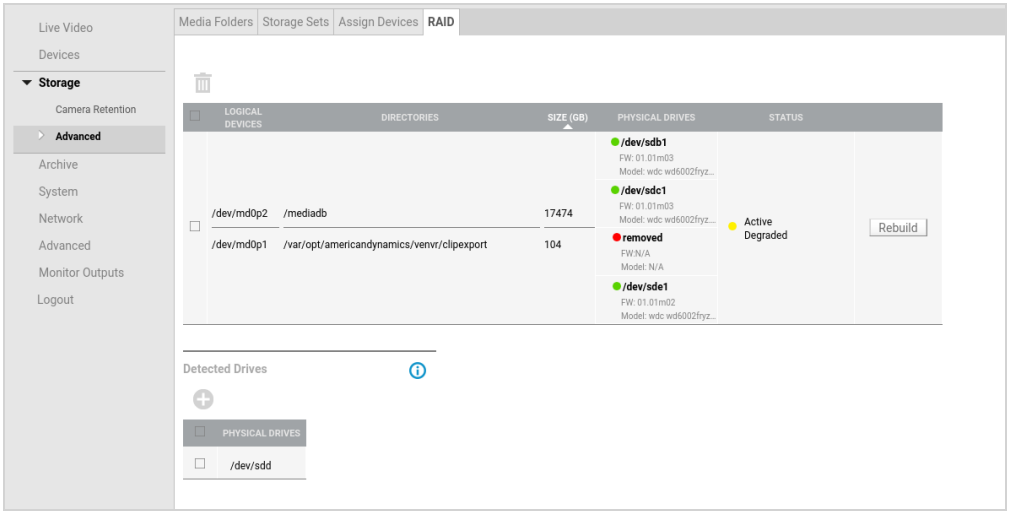


If you are using a VideoEdge 1U NVR that has been configured for RAID storage during OEM installation, you can view the status of the RAID. If the RAID is in an unhealthy state, you can rebuild it. If you want to switch to a JBOD configuration from a RAID configuration, you can remove the software RAID. You can add a physical drive to the RAID to replace a faulty drive, if required.

Caution

Rebuilding a RAID, or removing a RAID to switch to a JBOD storage configuration, will irretrievably destroy all existing data on the current RAID. Adding a physical drive to a RAID will irretrievably destroy all existing data on the physical drive being added.

Figure 22 RAID page on VideoEdge 1U NVR



Note:
When configuring for RAID, only RAID5 is supported on the VideoEdge 1U NVR.

For more information on RAID, and other storage concepts, see *Adding External Storage*.

Procedure 91 Rebuilding an unhealthy RAID

Caution

Rebuilding a RAID will irretrievably delete all existing data on the current RAID.

1. Click the **Storage** menu.
2. Click **Advanced**.
3. Click the **RAID** tab.
4. Click **Rebuild**.

   Note:
   The Rebuild feature is only available if the RAID is in a corrupt or unhealthy state.

5. Click **Yes** when the first popup warning displays.
6. Click **Yes** when the second popup warning displays.

Procedure 92 Adding a physical drive to a RAID

Caution

Adding a physical drive to a RAID will irretrievably delete all existing data on the drive being added.

1. Click the **Storage** menu.
2. Click **Advanced**.
3. Click the **RAID** tab.
4. Select the checkbox of the drive you want to add from the **Physical Drives** list.
5. Click the **Add** icon.
6. Click **Yes** when the first popup warning displays.
7. Click **Yes** when the second popup warning displays.

Procedure 93 Removing a software RAID

Caution

Removing a RAID will irretrievably delete all existing data on the current RAID.

1. Click the **Storage** menu.
2. Click **Advanced**.
3. Click the **RAID** tab.
4. Select the checkbox of the software RAID you want to remove.
5. Click the **Remove** icon.
6. Click **Yes** when the first popup warning displays.
7. Click **Yes** when the second popup warning displays.
   The RAID is removed, and replaced with a JBOD storage configuration

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 from the Advanced menu. See the *Storage Statistics* section 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 the 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

- 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 - Redundant Array of Inexpensive Disks

- 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.

Virtual Disks (Logical Unit Numbers)

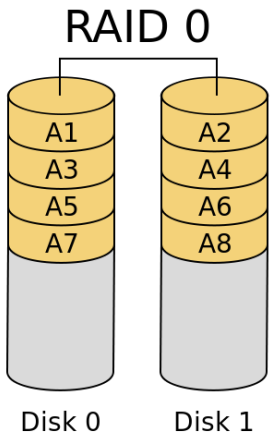
- A virtual disk represents an individually addressable (logical) SCSI device that is a partition of a physical SCSI device (target).
- Virtual disks are also known as volumes or LUNs.
- In enterprise-level systems, virtual disks usually represent segments of large RAID disk arrays.

Key RAID concepts

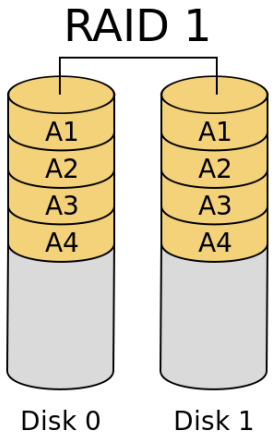
- **Mirroring** – Duplicating data to more than one disk.
- **Striping** – Splitting data across more than one disk.
- **Error Correction** – Storing redundant data so problems can be detected and possibly fixed.

Common RAID types

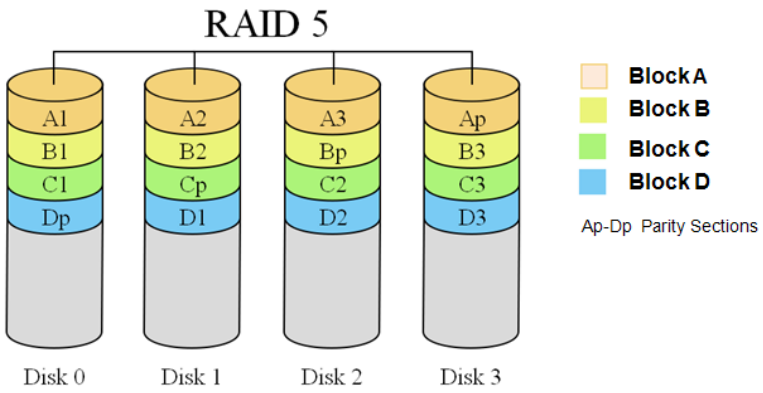
- **RAID 0** – Uses striping to provide extra performance and capacity but does not provide data protection (lack of mirroring or parity).



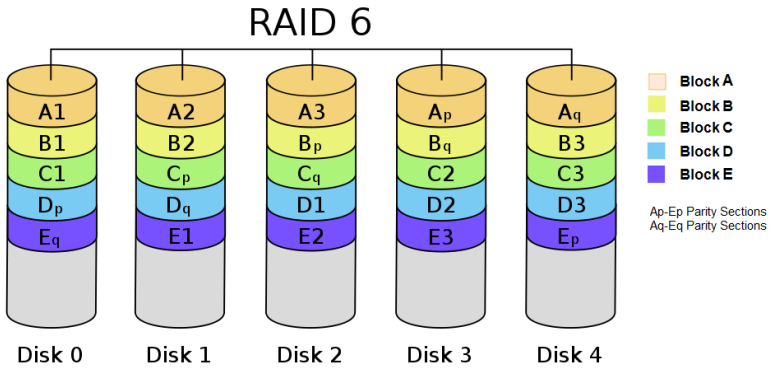
- **RAID 1** – Uses mirroring to provide 1:1 backup, which increases read performance or reliability at the expense of capacity. This configuration is often used with databases due to better transaction time and availability.



- **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.



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.

Before configuring storage on an NVR, consider the following factors:

- Storage
  - The type of storage to be used. For example, Internal HDDs, iSCSI external storage, Fiber Optic external storage, or USB external hard drives.
  - The storage configuration. For example, RAID 0, RAID1, RAID 5, RAID 6, or JBOD.
- Cameras
  - Total number of cameras.
  - Type of cameras and the configuration settings.
  - The file size of the camera's video stream that is to be recorded.
- The required recording retention period for stored video.

This section details some different storage usage examples that 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.

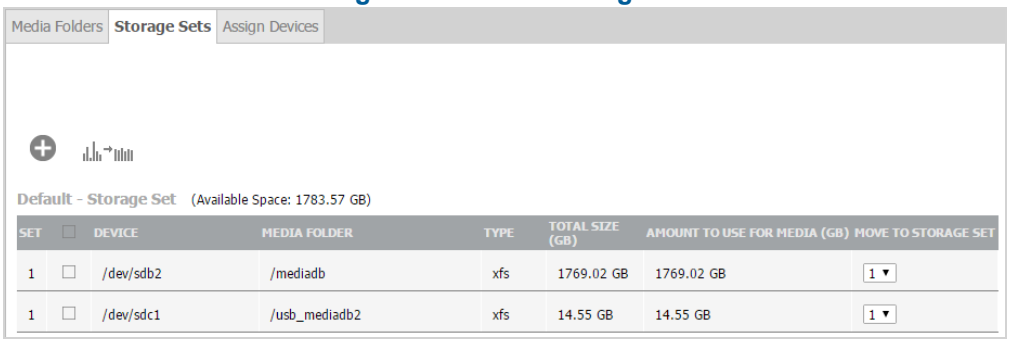
For the VideoEdge NVR

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 23 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)

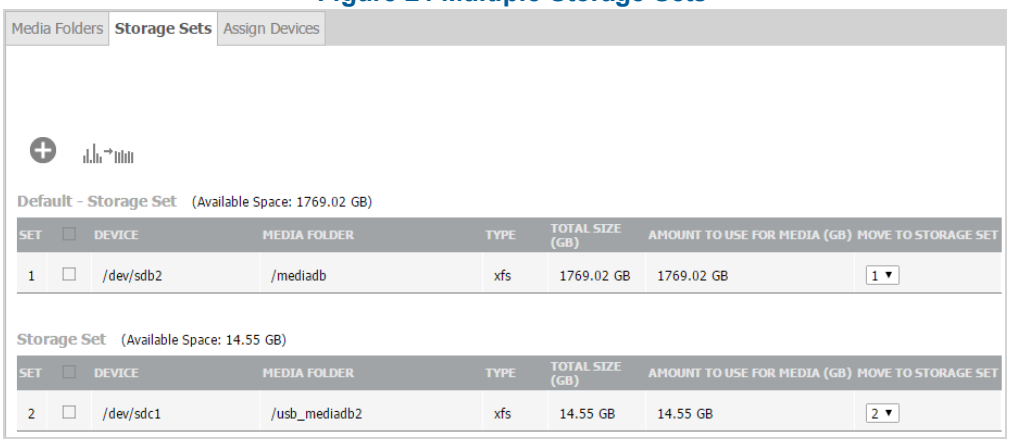
Or

- 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 24 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 94 Calculating storage requirements

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.

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

Consider the following storage strategy recommendations for FRS or FES RAID devices:

- 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 using 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 95 Connecting storage to the NVR using eSATA

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.

Connecting storage to the NVR using USB

You can add USB storage to any VideoEdge model that has a USB port.

Connecting the 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 96 Connecting the NVR to FRS/FES using Fiber

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.

Connecting the 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 97 Connecting the NVR to FRS/FES using iSCSI

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 **Username**.

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.

Archive

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:
NAS devices may require pre-configuration before they can be used for archiving tasks. Refer to your product's Installation and User Manual for more information.

Use the Archive menu to add and configure archive destinations, apply global settings, select video devices for archiving and view outstanding archiving operations. The Archive menu contains the following submenus:

- **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. The Settings submenu contains the following sections: **Global Settings**, and **Availability**.
- **Archive Scheduler** - From here you can create Archive Groups and Schedules which define which video is to be automatically archived. The Archive Scheduler submenu contains the following sections: **Archive Schedules**, **Archive Schedule Editor**, **Archive Group Editor**.
- **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. The Device List submenu contains the **Video List** section.
- **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 icons table

Table 27 Archive icons

Icon	Name	Function
	**Add Archive**, **Add Schedule Group**	Add new archive; add new schedule group.
	**Remove Archive**, **Remove Schedule Group**, **Delete archive job**	Remove archive; remove schedule group; delete archive job.
	**Enable Archive**	Enable selected archive.
	**Disable Archive**	Disable selected archive.
	**Save**	Save
	**Cancel**	Cancel
	**Edit**, **Rename**	Edit; rename schedule group.
	**Unlock**	Unlock the archive
	**Lock**	Lock the archive
	**Edit group times**	Open Archive Schedule Editor to edit group schedule times.
	**Edit group cameras**	Open Archive Group Editor to edit camera groups.
	**Batch Edit Device**	Edit multiple devices.

Adding an archive destination

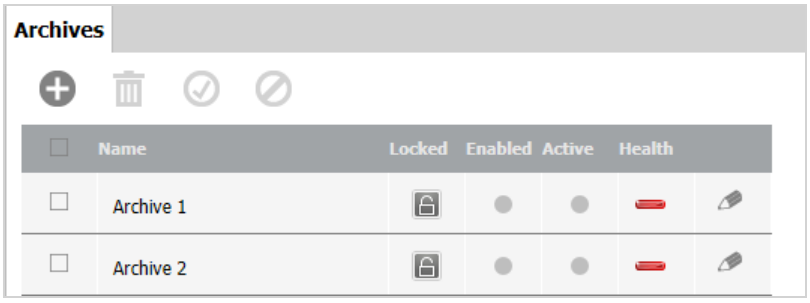
You must create an archive destination before you can archive video. You can add multiple archive destinations to the NVR, but only one archive destination can be used at a time. When you add an archive destination it is listed in the Archives table.

You can edit archive destination settings or remove archive destinations as required.

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.

An archive destination can be locked or unlocked. When an archive is locked, it is read-only and can only be used to retrieve archived video.

Figure 25 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.

Procedure 98 Adding an archive destination

1. Click the **Archive** menu.
2. Click **Archives**.
3. Click the **Add Archive** icon.
   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:
   • With DNS and a shared folder named **NvrShare** - \\Hostname\NvrShare\
   • 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 the **Save** icon.

Locking or unlocking archives in the archives table

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 99 Locking or unlocking archives in the archives table

1. Click the **Archive** menu.
2. Click **Archives**.
3. Click the **Unlock** icon to unlock the archive, or click the **Lock** icon to lock the archive.
4. Click **OK**.

Enabling or 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 100 Enabling or disabling an archive destination

1. Click the **Archive** menu.
2. Click **Archives**.
3. Select the checkbox in the archives table for the destination you want to enable or disable.
4. Click the **Enable Archive** icon to enable the archive destination, or the **Disable Archive** icon to disable the archive destination

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. A journal entry is created on completion stating if the archiving task was successful. Archived video can also be retrieved using victor unified client

For more information 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, and can be viewed using 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.

Settings

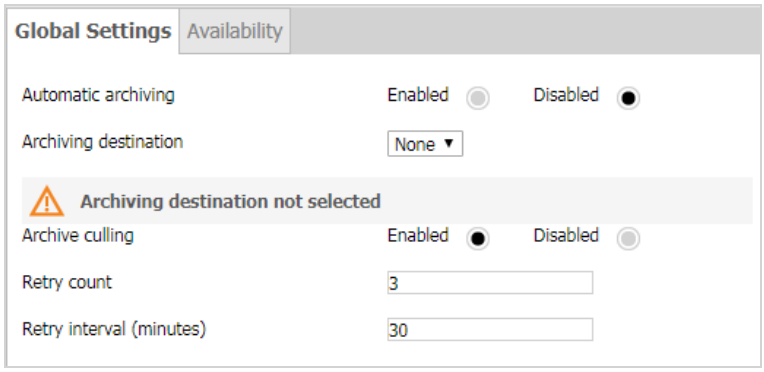
Global settings

From the Global Settings page, you can enable or disable automatic archiving, set the active archive destination, and configure first in, first out (FIFO) archive culling.

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 archive culling is a basic form or data culling which will cull data based on the date it was written to the archive, with the oldest data being culled first. Archive culling can also be configured based on retention rules. Archive culling starts when the archive reaches 95% capacity. If you disable archive culling, archiving stops when the archive is full.

Figure 26 Global settings 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 101 Applying global archive settings

1. Click the **Archive** menu.
2. Click **Settings**.
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 list.
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.
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 the **Save** icon.

Configuring an archive availability schedule

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. The Archive availability schedule does not affect manual archiving.

When the Availability schedule is disabled, archiving will not be restricted when automatic archiving is configured. The NVR will write to the archive 24 hours a day.

Procedure 102 Configuring an archive availability schedule

1. Click the **Archive** menu.
2. Click **Settings**.
3. Click the **Availability** tab.
4. Select the **Availability schedule Enabled** option button.
   A dialog box opens.
5. Click **OK**.
6. Select the Archiving availability **Available** option button to assign availability, or select the **Not Available** option button to remove availability.
7. Select the schedule times you want to edit in one of the following ways:
   - Select individual cells to assign or remove availability.
   - Select the row heading to assign or remove availability for an entire day.

- Select the column heading to assign or remove availability to the same hour for every day of the week.
- Press and hold the left mouse button, and then draw a region around specific time slots to assign or remove availability.

8 Click the **Save** icon.

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 framerate of the video being archived, for example by applying an archiving quality of 50%, you are reducing the framerate 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. This function may have limitations based on codec. For example, H.264 and MPEG-4 only support decimation at key frame level

Procedure 103 Configuring the archiving quality

1 Click the **Devices** menu.
2 Click **List**.
3 Click the **Setup** icon in the device record you want to edit.
4 Click the **Archive** tab.
5 Select the **Archiving Quality** from the list.
6 Click the **Save** icon.

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.

Enabling the Maximum Archiving Retention Period for individual cameras

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 104 Enabling the Maximum Archiving Retention Period for individual cameras

1 Click the **Devices** menu.
2 Click **List**.
3 Click the **Setup** icon for the device you want to edit.
4 Click 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 Select **Custom** from the dropdown menu, and then enter a retention period in the **Period** field, or select **As long as possible** from the dropdown menu.
7 Click the **Save** icon.

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 105 Enabling or disabling the Archiving scheduler

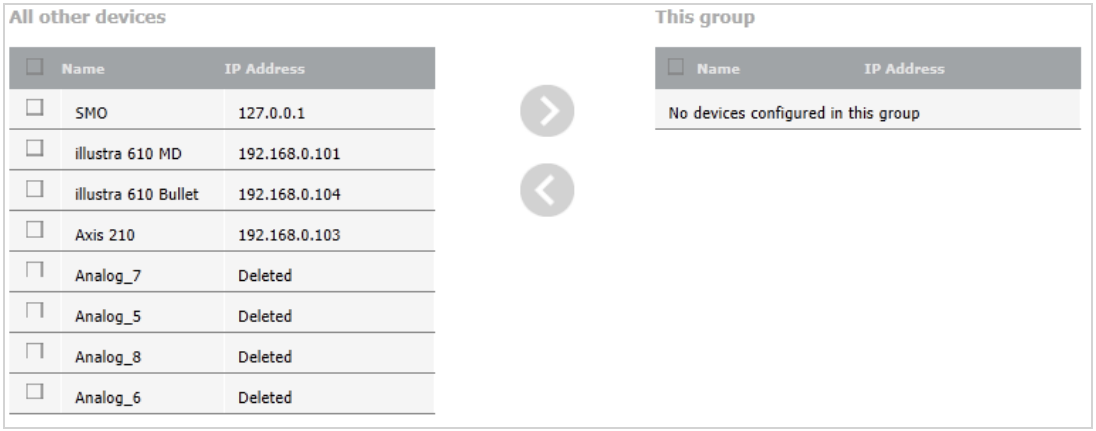
1 Click the **Archive** menu.
2 Click **Archive Scheduler**.
3 To enable the Archiving Scheduler, click the **Enabled** option button, or to disable the Archiving Scheduler, click the **Disabled** option button.

Procedure 106 Creating an Archive schedule

1 Click the **Archive** menu.
2 Click **Archive Scheduler**.
3 Click the **Add Schedule Group** icon.
4 Enter a name in the **Schedule Name** field.
5 Click the **Save** icon.

Schedule Editor and Group Editor pages

Figure 27 Archive Group Editor



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 107 Assigning cameras to a group

1. Click the **Archive** menu.
2. Click **Archive Scheduler**.
3. Click the **Edit group cameras** icon of the Archive Schedule you want to edit.
4. Select the required camera checkboxes and use the **Left Arrow** icon and **Right Arrow** icon to move cameras between the **All other devices** list and the **This group** list, until the cameras you want to be assigned to the selected archive group are in the **This group** list.
5. Click the **Save** icon.

Procedure 108 Editing the queuing times of an Archive schedule

1. Click the **Archive** menu.
2. Click **Archive Scheduler**.
3. Click the **Edit group times** icon of the Archive Schedule you want to edit.
4. Select an Archiving Mode:
   - Select the **Automatic archiving disabled** option button to disable queuing for archiving during selected time increments.
   - Select the **Automatically archive all recorded video** option button to queue for archiving all video during selected time increments.
   - Select the **Archive only recorded alarm video** option button to queue for archiving all video recorded under alarm conditions during selected time increments.
5. Select the schedule times you want to edit in one of the following ways
   - Select individual cells to assign or remove availability.
   - Select the row heading to assign or remove availability for an entire day.
   - Select the column heading to assign or remove availability to a time slot for an entire week.
   - Select **All Week** to assign or remove availability to all time slots within a week.
   - Press and hold the left mouse button, and then draw a region around specific time slots to assign or remove availability.
6. Click the **Save** icon.

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.

Procedure 109 Batch editing archive settings using the Device List submenu

1. Click the **Archive** menu.
2. Click **Device List**.
3. Select the checkboxes of the cameras you want to edit.
4. Click the **Batch Edit Device** icon.
5. Select the checkbox, followed by the required **Archiving Mode** option button
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 the **Save** icon.

Jobs

The Jobs page lists all outstanding queued archiving tasks.

Viewing and deleting manual archiving tasks

You can view and delete manual archiving tasks on the Jobs page.

Procedure 110 Viewing and deleting manual archiving tasks

1. Click the **Archive** menu.
2. Click **Jobs**.
3. (Optional) Select the checkboxes next to the tasks you want to delete.
4. Click the **Delete archive job** icon.

Use the System menu to configure the NVR's basic system settings. The System menu contains the following submenus:

- **General** - From here you can edit the Hostname, Location, Date & Time and Language. You can view the Operational Mode of the VideoEdge, and also download the public key. The General submenu contains the **System Info** section.
- **Users and Roles** - From here you can create new user accounts, edit existing accounts, and change settings for users and roles. You can also designate role types for LDAP groups. The Users and Roles submenu contains the following sections: **Users**, **Roles**, and **LDAP Roles**.
- **Licensing** - From here you can view the channel and license information for your VideoEdge, 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. The Templates submenu contains the following sections: **Save Template**, and **Load Template**.
- **Backup/Restore** - From here you can create a Backup file or alternatively restore an NVR from a Backup file. The Backup/Restore submenu contains the following sections: **Backup**, and **Restore**.
- **Serial Protocols** - From here you can view the Serial Protocols supported by your NVR and their default settings.
- **Security Configuration** - From here you can view and configure security settings. The Security Configuration submenu contains the following sections: **General**, **Certificate**, **Remote Access**, **System Passwords**, **System Use Banner**, **SNMP**, **LDAP**, and **Security Audit**.

System icons table

Table 28 System icons

Icon	Name	Function
	**Save**	Save.
	**Select Date/Time**	Open calendar to edit date and time.
	**Add new user**	Add new user.
	**Remove user**, **Remove template**	Remove user; remove template.
	**Unlocked**	Lock user.
	**Locked**	Unlock user.
	**Edit**	Edit
	**Cancel**	Cancel
	**Batch Edit**	Edit multiple roles or LDAP roles.

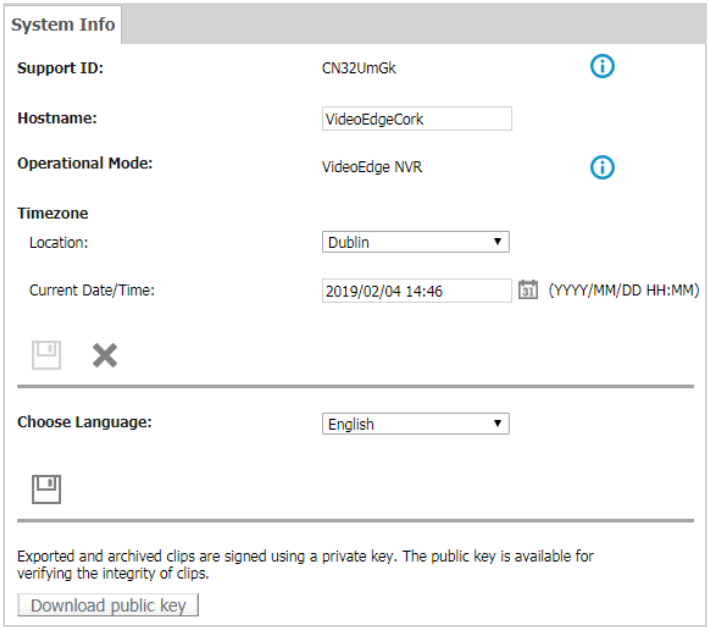
Icon	Name	Function
	Camera Access Settings, **Change template**	Open the camera access list, or edit certificate template
	Right Arrow	Move selected cameras to Access Denied group.
	Left Arrow	Move selected cameras to Access Granted group.
	Retrieve LDAP Groups	Retrieve LDAP groups from LDAP server.

General

From the General System Info page you can edit the hostname, the location, the date and time, the 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. 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. When using an NTP server, the location is used to define the time and date, as NTP servers use UTC time

Figure 28 System Info page



Licensing

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 29 Maximum Camera Count

Model	Maximum number of channels	Maximum number of analog cameras
32 Channel IP only Desktop	32	0
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.

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
License Type	The type of license on your VideoEdge: Temporary, Local or victor Centralized.
Time Remaining	The time remaining on your license. This only appears if your VideoEdge has a Temporary license.
SSA Expires	The expiry date for your Software Service Agreement.
SW Serial Number	The software serial number for your VideoEdge.
Channel Status	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	The total number of analog devices that the VideoEdge can support. Analog devices do not require a license.
IP	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.

Field	Description
Illustra Pro	The total number of Illustra Pro cameras currently installed on your VideoEdge. From VideoEdge 5.1 onwards, Illustra Pro cameras do not require a license if you add them to VideoEdge NVRs purchased from American Dynamics. **Note:** This only applies to physical systems purchased from American Dynamics, and not software bundles. However, VideoEdge NVRs require a license. With the exception of Motion Detection, any analytic function for cameras, including Illustra Pro cameras, require a license.
Total Used and Available	The combined totals of currently used and available analog devices, IP licensed cameras, and Illustra Pro camera licenses, on your VideoEdge.
Analytics	The Analytics section displays the number of analytic licenses available for each camera analytic. 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.

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 the following licensable video analysis features: Video Intelligence, Facial Recognition, Facial Verification, License Plate Recognition, and Deep Intelligence.

Face Recognition enrollment tiers

With a Face Recognition or Face Verification license, you must purchase a face enrollment tier. There are four tiers available. Each tier has a maximum supported people count:

- Tier 1: Up to 25 people
- Tier 2: Up to 100 people
- Tier 3: Up to 1000 people
- Tier 4: Up to 10,000 people

If you are upgrading to 5.4.2 or later, from 5.4.1 or earlier, Tier 3 is assigned by default. Downgrading the face enrollment tier license is not supported.

If you are using victor Centralized Licensing, you must have the same tier on all NVRs that are centralized with the victor tier.

VideoEdge Virtual NVR licensing

The VideoEdge Virtual NVR requires a specific license; a standard VideoEdge license does not work. If you want to license a Virtual NVR using victor Centralized Licensing, the victor software version must be 5.4.1 SP1 or later, and the VideoEdge software version must be 5.4.2 or later.

Note:
You cannot use Illustra Pro cameras without a camera connection license on virtual and software-only VideoEdge distributions. Contact your sales representative for more information.

Licensing the VideoEdge (Local License)

To apply a Local license to the VideoEdge you must generate a Host ID specific to your VideoEdge and enter the ID on the online registration page. 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, use the Generate Host ID tool to generate a Host ID specific to your VideoEdge device, and enter the ID on the online registration page on the American Dynamics website. You can access the online registration page from the American Dynamics website or using the VideoEdge Licensing Activation Icon on the VideoEdge Desktop.

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.

Note:
For VideoEdges that you assign as Secondary NVRs, do not generate a host ID while the Secondary NVR is in Failover mode.

Procedure 111 Generating a Host ID

1. Select **System** from the main menu.
2. Select **Licensing**.
3. Click **Generate Host ID** in the Upgrades section.
   Depending on the browser used, the file either downloads automatically, or a download dialog window opens. Proceed as required.

Applying a Local License

When you receive your software license from the American Dynamics website, you can apply your Local license.

Procedure 112 Applying a Local License

1. Click **System**.
2. Click **Licensing**.
3. In the **Choose License Type** section, click **Local License**.
4. In the **Configure Local Licensing** section, click **Browse**.
5. Locate the license file and click **Open**.
   The file path is displayed in the **License File** field.
6. Click **Apply Local License**.

Licensing the VideoEdge (victor Centralized License)

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.

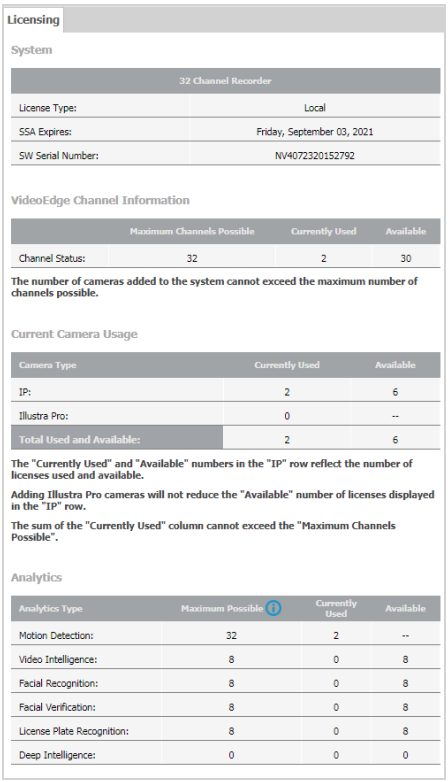
To access licenses for objects such as cameras, analytics, facial recognition and facial verification devices, you must configure VideoEdge to connect to the victor Application Server. Unlike Local licensing, Centralized camera, analytic, facial verification and facial recognition licenses are not linked 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 29 License status - VideoEdge Admin GUI



When using victor Centralized Licensing, the number of analytic licenses available on the victor Application Server may exceed the number of devices that the VideoEdge can support. Therefore, Centrally-licensed VideoEdges do not have a maximum number of analytic licenses; instead, they have a maximum recommended number of analytic licenses. For optimum performance, do not exceed the maximum recommended number of analytic licenses.

Note:
Motion Detection analytics are included with the VideoEdge license, and do not need to be purchased.

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.

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 113 Transferring a VideoEdge License (Automatic)

1. Double-click the **Licensing** icon on the desktop.
   The License Manager displays.
2. Click **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 click **Save**.
6 Apply for a victor license at http://americandynamics.net

Applying 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 114 Applying a victor Centralized license

1 Save the license file (.LIC) to a local directory.
2 Double-click the **Licensing** icon on the desktop.
The License Manager displays.
3 Click **Add New License**.
The Open screen displays.
4 Browse to the .LIC license file and select **Open**.
5 Click **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.

Configuring 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 115
Manually activating victor Centralized Licensing

Note:
For this procedure, use the VideoEdge Administration Interface.

1 Click the **System** menu.
2 Click **Licensing**.
3 In the **Choose License Type** section, select **victor Centralized License**.
4 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 Click the **Save** icon.

5 Click **Activate Centralized Licensing**.

Procedure 116 Automatically activating victor Centralized Licensing

Note:
For this procedure, use the License Manager that is installed on the victor Application Server.

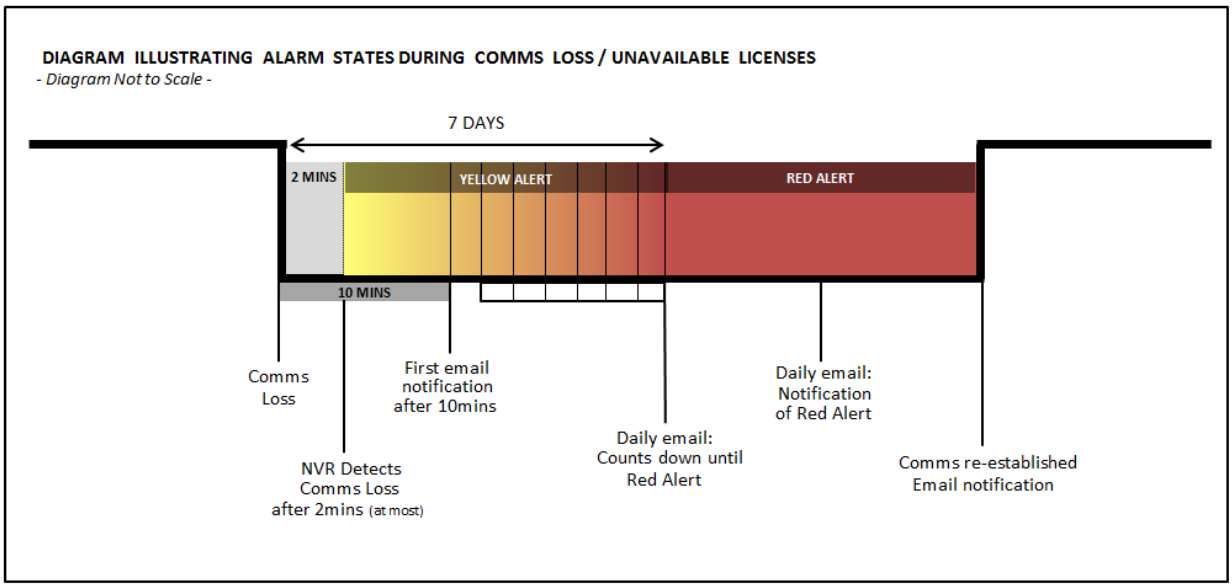
1 Click the VideoEdge tab in the License Manager.
2 Select **Centralize Licenses**.
The VideoEdge Centralized License Transfer dialog opens.
3 Review the information to ensure that all required VideoEdge units will be transferred.
4 Confirm IP address and port number for the license server.
5 Enter an 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 Click **Yes, Transfer**.
A summary of the transferred recorders appears.
7 Click **OK**.

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.

Editing the SSA message

You can edit the SSA message that is sent to you when the VideoEdge license is close to expiry.

Procedure 117 Editing the SSA message

1. Click the **System** menu.
2. Click **Licensing**.
3. In the **Software Service Agreement** section, click **Change Message**.
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 the **Save** icon.

Editing 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 118 Editing SSA contacts

1. Click the **System** menu.
2. Click **Licensing**.
3. In the **Software Service Agreement** section, click **Edit Contacts**.
4. To add a contact, enter their email address in the **Add Email** field.
5. Click the **Add** icon.
   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.
8. Click the **Cancel** icon to exit.

Setting 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.

Sending 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 119 Sending an SSA test message

1. Click the **System** menu.
2. Click **Licensing**.
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 contacts' email addresses and the SMTP server address to confirm they are correct, and re-send.

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.

Users and Roles

When configuring VideoEdge in the Setup Wizard, there are four preconfigured user accounts. For more information see Preconfigured User Accounts in the Setup Wizard .

There are also default user credentials that denote permissions and lockout options. For more information, see Default User Accounts credentials. You can also create custom user credentials for each NVR user. For more information, see Roles .

Note: You can also configure role permissions for LDAP groups which have been configured on your LDAP server.

Caution

For optimum security, change account passwords, configure appropriate lockout settings, and enable auto logout.

Optional NVR Accounts in the Setup Wizard

There are two types of optional NVR accounts that can be created in the User Accounts page of the Setup Wizard: Recommended NVR Accounts and Other NVR Accounts. For details, see the following table.

Note: Optional accounts can be configured in Standard Security Mode and Enhanced Security Mode.

Table 30 Optional NVR Accounts in the Setup Wizard

Recommended NVR Accounts	Other NVR Accounts
softwareadmin	operator
	viewer1
	viewer2
	viewer3

Note: If you do not create optional NVR accounts in the Setup Wizard, you can create them in the Admin GUI For more information, see Adding a new user.

Preconfigured User Accounts in the Setup Wizard

There are four preconfigured user accounts in the User Accounts page of the Setup Wizard.

In **Standard Security Mode**, each user account has a preconfigured Username and requires a new password.

In **Enhanced Security Mode**, each user account has a preconfigured User Role and requires a new username and a new password.

Table 31 Preconfigured user accounts and update requirements

Standard Security Mode		Enhanced Security Mode	
Linux User Accounts		**Linux User Accounts**	
Username	**Required update**	**User Role**	**Required update**
VideoEdge	New password	VideoEdge	New username New password
root	New password	root	New username New password
Required NVR Accounts		**Required NVR Accounts**	
Username	**Required update**	**User Role**	**Required update**
admin	New password	admin	New username New password
support	New password	support	New username New password
nvrgroupadmin	New password	nvrgroupadmin	New password

Standard Security Mode		Enhanced Security Mode	

Note: The **VideoEdge** username and user role is **Tyco** when the unit is a Tyco Analytics Appliance or Tyco Transcoder.

Default User Accounts credentials

Default user accounts have corresponding roles. These roles determine user account permission in VideoEdge. Note the following:

- Only user accounts with the admin role can change or reset passwords for other users
- For systems that are not part of the VideoEdge Hybrid product range, user roles viewer1, viewer2 and viewer3 cannot be used when creating user credentials. These roles do not permit access to the NVR Administration Interface.

Table 32 Default User Accounts credentials

User Accounts	Credentials
softwareadmin	Access the software updates page only Camera firmware updates Installing camera handler packs
admin	View and edit the VideoEdge Administration Interface Full functionality of VideoEdge Client Change or reset user passwords
operator	View the VideoEdge Administration Interface Full functionality of VideoEdge Client
support	American Dynamics Technical Support only
viewer1	Full functionality of the VideoEdge Client Unable to view or edit the VideoEdge Administration Interface
viewer2	Full functionality of the VideoEdge Client with exception of Analog (Real) PTZ Unable to view or edit the VideoEdge Administration Interface
viewer3	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

Note: If you are upgrading VideoEdge, passwords can be the default passwords. Default passwords will be the same as the user account name. For example, the default password for operator will be **operator**.

Editing User Accounts credentials

In the Admin GUI, you can edit User Accounts credentials. For more information, see Roles .

Service Accounts roles

Service accounts roles are used for communication between NVRs, or communication with the victor Web LT application.

Note:
These roles cannot be assigned to created users.

Table 33 Service Accounts roles

Role	Description	Password
nvrgroupadmin	Communication between NVRs in a group The password can be changed for this role but the same password must be used on all NVRs in a group	Default: **nvrgroupadmin**
nvrserviceuser	Communication between NVRs	Auto-generated after an OEM install or Reset to Factory Default (RFD)
victorwebserviceuser	Communication between the victor Web LT application and the host NVR	Auto-generated after an OEM install Reset to Factory Default (RFD)

Note:
Service accounts roles cannot be used to sign on to the VideoEdge Administration Interface.

Adding a new user

1. Click the **System** menu.
2. Click **Users and Roles**.
3. Click the **Add new user** icon.
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 username 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 username and password as it has been entered at this stage.
8. Select the role from the **Role** list.
9. Click the **Save** icon.

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 120 Locking or unlocking accounts from the Users table

1. Click the **System** menu.
2. Click **Users and Roles**.
3. Click the **Lock** icon in the user credential row that you want to lock, or click the **Locked** icon 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**.

Procedure 121 Unlocking accounts using the edit icon

1. Click the **System** menu.
2. Click **Users and Roles**.
3. Click the **Edit** icon 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.

   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 list if you want to assign a new role to the account.
8. Click the **Save** icon.

Roles

Use the Roles page to configure several security features for the NVR's user credentials:

- **Inactivity Lockout Interval** - Configure credentials to lock out a user after a configured number of days of inactivity is reached.
- **Failed Login Lockout Policy** - Configure the Lockout Policy for users who reach the configured Failed Login Retry Limit. Select None, Lockout, or Delay. When None is selected, there is no lockout policy. When Lockout is selected, the user is locked out of the account once they reach the Failed Login Retry Limit. When Delay is selected, the user is unable to log in for a configured period of time once they are locked out.
- **Failed Login Retry Limit** - Set the number of consecutive login failures after which the user is locked out.
- **Failed Login Retry Delay** - Set the delay time between login attempts when a user is locked out.
- **Auto Logout** - Configure credentials to automatically log out a user after a configured period of inactivity.
- **Enhanced Password Validation** - If enabled, enhanced password validation does 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 at least one lowercase letter
    - Must contain at least one uppercase letter

- Must contain at least one number
- Must contain at least one of the following special characters [ ] { } ( ) ^ $ # + _ - ~ ! * %

- **Remembered Passwords** - Set the number of previously used passwords that cannot be reused.
- **Camera Access** - Configure camera access for particular roles.

Note:
By default, these security features are not configured in Standard Security Mode. A default configuration is applied in Enhanced Security Mode.

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.

Configuring additional security on roles

Security features, such as Lockout or Auto Logout, are assigned to the NVR's roles. These security features are applied to all users that have been assigned that role.

Procedure 122 Configuring additional security on roles

1. Click the **System** menu.
2. Click **Users and Roles**.
3. Click the **Roles** tab.
4. Click the **Edit** icon for the role you want to edit.
5. Select a lockout policy from the **Lockout Policy** list.
6. (Lockout selected) Enter the number of failed password attempts in the **Retry Limit** field that are required for the account to lockout.
7. (Delay selected)
   a. 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.
   b. Enter the number of minutes in the **Retry Delay** that are to pass before the user can re-attempt to enter their credentials.
8. (Optional) Select the **Enable Auto Logout** checkbox, and enter the number of minutes of inactivity after which the user is logged out in the **Auto Logout Interval (minutes)** field.
9. (Optional) Select a value from the **Inactivity Lockout Interval (days)** list.
10. (Optional) Configure Enhanced Password Validation settings:
    a. Select **Enabled** from the **Enhanced Password Validation** list.
    b. Enter the number of previously used passwords that cannot be reused in the **Remembered Passwords** field.
11. Click the **Save** icon.

Configuring role-based camera access

Use the Roles page to configure camera access for the **viewer1**, **viewer2**, and **viewer3** roles. Filter camera permissions using the **Camera Access List** window. The **Access Granted** list features cameras that the role currently has access to, and the **Access Denied** list features cameras currently hidden from the role.

Note:
To view full lists of restricted cameras for each role, see the Security Audit page.

Procedure 123 Configuring role-based camera access

1. Click the **System** menu.
2. Click **Users and Roles**.
3. Click the **Roles** tab.
4. Click the **Camera Access Settings** icon on a role to open its **Camera Access List** window.

5 Select the checkboxes of the cameras you want to grant or deny access to. You can use shift-click to select multiple cameras.
6 Click the **Right Arrow** icon to move the camera to the **Access Denied** list, or click the **Left Arrow** to move the camera to the **Access Granted** list.
7 Click the **Save** icon.

Assigning 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. You can also batch edit NVR LDAP Roles.

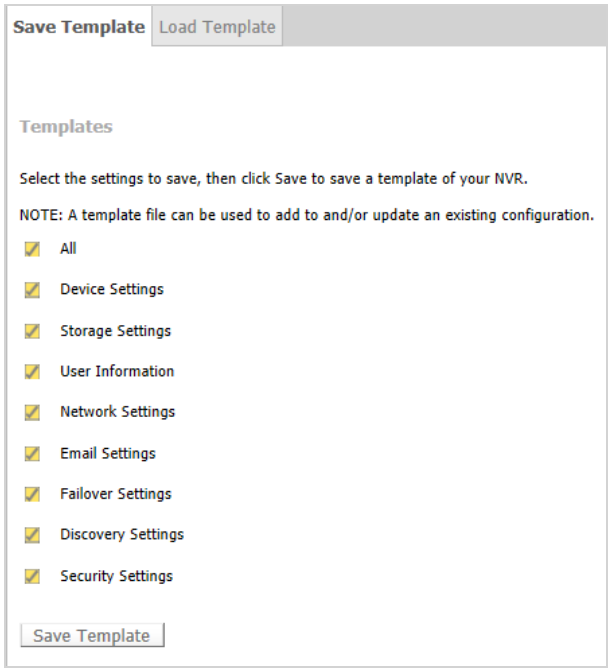
Procedure 124 Assigning LDAP Roles

1 Click the **System** menu.
2 Click **Users and Roles**.
3 Click the **LDAP Roles** tab.
4 Click the **Retrieve LDAP Groups** icon to retrieve all LDAP Groups.
5 Enter the **LDAP server password** in the field.
All LDAP groups in the directory are displayed.
6 Select the checkboxes of the LDAP groups you want to assign an NVR role.
7 Click the **Batch Edit** icon.
8 Select the required NVR role from the **NVR Role** list.
9 Click the **Save** icon.

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 30 Save Template page



Creating 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 125 Creating a configuration template

1. Click the **System** menu.
2. Click **Templates**.
3. Select the required checkboxes for the configuration settings that you want saved to the template.
4. Click **Save Template**.
5. Click **Save As**.
6. Navigate to the folder where you want to save the template.
7. Enter a **File name** for the template and click the **Save** icon.

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

Importing 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. For template files which include security settings you will be required to activate these settings when prompted to enable them on the NVR.

Procedure 126 Importing a template file

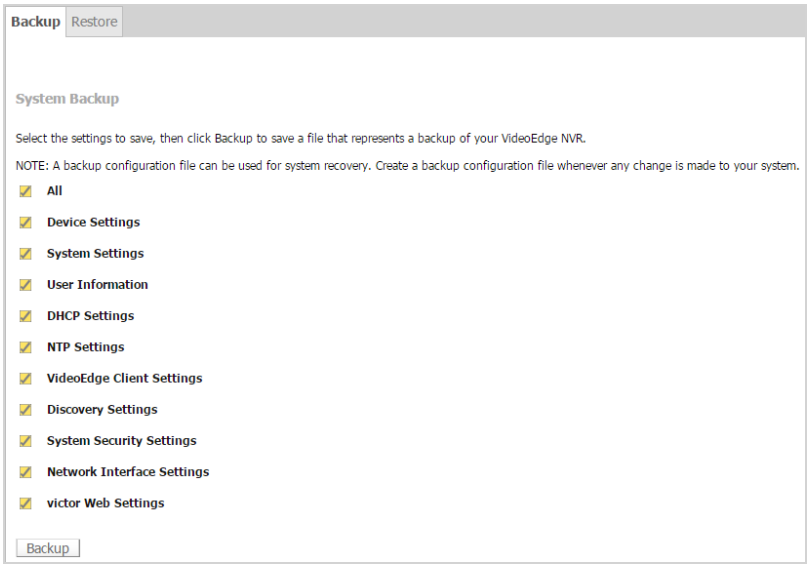
1. Click the **System** menu.
2. Click **Templates**.
3. Click the **Load Template** tab.
4. Click **Browse**.
5. Navigate to the template file you want to import.
6. Select the file and click **Open**.
   The file path of the template file appears in the **Template File** field.
7. Click **Apply Template**.

Note:
If any errors occur during the template import process, a summary of the errors are displayed.

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 31 Backup page



Creating 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 127 Creating a backup file

1. Click the **System** menu.
2. Click **Backup/Restore**.
3. Select the required checkboxes for the configuration settings that you want saved to the backup file.
4. Click **Backup**.
5. Click **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 the **Save** icon.

   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

Restoring an NVR from a backup file

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 128 Restoring an NVR from a backup file

1. Click the **System** menu.
2. Click **Backup/Restore**.
3. Click the **Restore** tab.
4. Click **Browse**.
5. Navigate to the backup file you want to use, select the file and click **Open**.
6. If the Backup file is encrypted, select the **Backup file is encrypted** checkbox.
7. Click **Upload Backup**.
   A message box opens, asking you if you want to recover any media that is part of storage being restored.
8. Click **Yes** if you want to recover media, or click **No** if you do not want to recover media.
   A recovery progression bar opens and updates as the recovery progresses. If you are recovering media, this may take some time. A message box opens informing you that the recovery is complete.
9. Click **OK**.

Note:
If you are restoring DHCP and/or NTP settings you need to restart your DHCP and/or NTP server.

Update Software

Software updates, firmware updates, patches, and update camera handler packs can be applied to the NVR manually, or by using the Push Update feature of victor Client. To perform a manual software update, you must log in to the VideoEdge Administration Interface with the **softwareadmin** user credential. The default password for the softwareadmin user credential is `softwareadmin`.

Note:
If your software service agreement (SSA) has expired, you cannot upgrade your software

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.

There are different upgrade paths depending on the software version you are currently using, and the software version you want to update to. Refer to the *Upgrade options for victor & VideoEdge* guide for more information.

Caution

NVR Services stop during a software update. Recording is paused 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

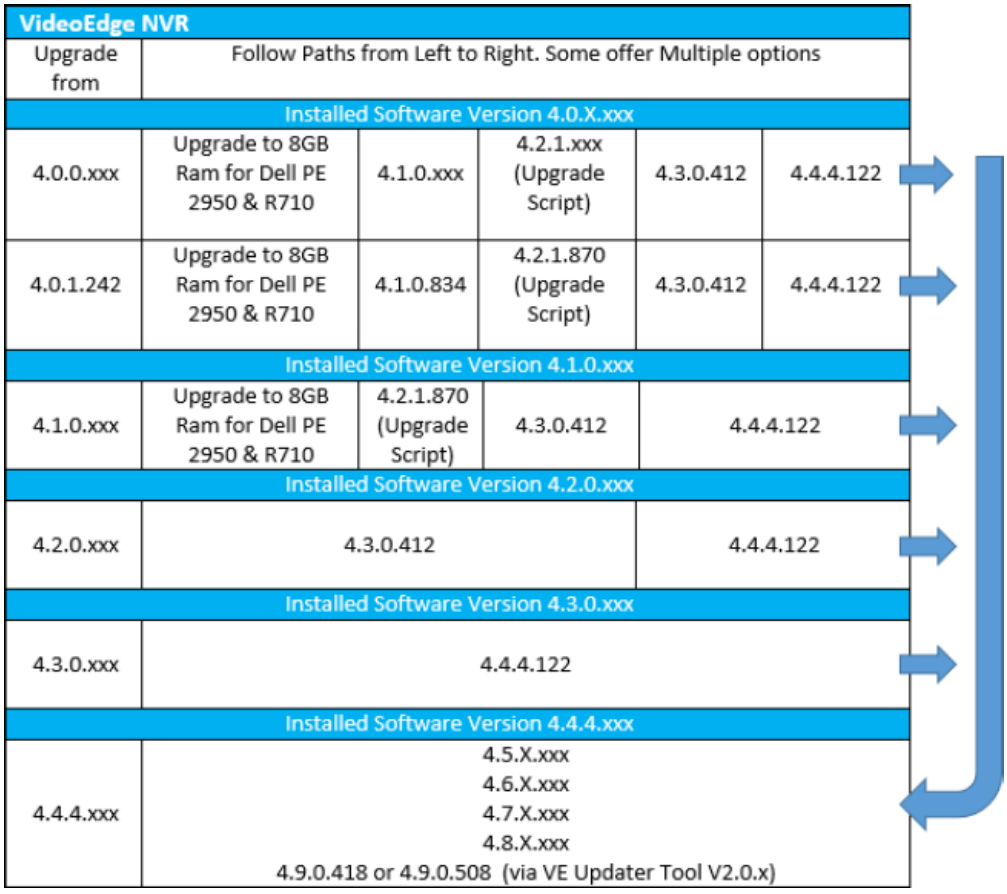
You cannot upgrade to VideoEdge 4.9.0 through the VideoEdge Administration Interface, or through a Push Update. You must use the VideoEdge Updater to upload and install VideoEdge 4.9 updates. For more information about the VideoEdge Updater, see the *VideoEdge Updater User Guide*.

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.



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 or 5.3.0.xxx
4.9.0.508	4.9.0.602 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 or 5.3.0.xxx
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 or 5.3.0.xxx
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 or 5.3.0.xxx
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 or 5.3.0.xxx
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 or 5.3.0.xxx
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 or 5.3.0.xxx
Installed Software Version 5.2.0.272	
5.2.0.272	5.2.1.80 or 5.2.2.24 or 5.3.0.xxx
Installed Software Version 5.2.1.80	
5.2.1.80	5.2.2.24 or 5.3.0.xxx
Install Installed Software Version 5.2.2.24	
5.2.2.24	5.3.0.xxx

Procedure 129 Updating the VideoEdge

1 Log in using the softwareadmin user credential:
   a Enter **softwareadmin** in the username field.
   b Enter your password. The default password for the softwareadmin user credential is **softwareadmin**
   The Update VideoEdge Software page opens.
2 Click **Browse**.

Note:
The name of the button may vary depending on the browser used.

---

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 files** 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 Click **Logout**.
8 Click **OK**.

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 VideoEdge Software page opens.

Caution

Recording and dry contact processing will be stopped for any camera using a handler that is being updated.

Procedure 130 Updating Camera Handler Pack

1 Log in using the softwareadmin user credential:
   a Enter **softwareadmin** in the username field.
   b Enter your password. The default password for the softwareadmin user credential is **softwareadmin**
   The Update VideoEdge Software page opens.
2 Click **Browse**.

Note:
The name of the button may vary depending on the browser used.

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 files** list.
5 Select the new package from the list and click **Install**.
6 Click **Logout**.
7 Click **OK**.

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.

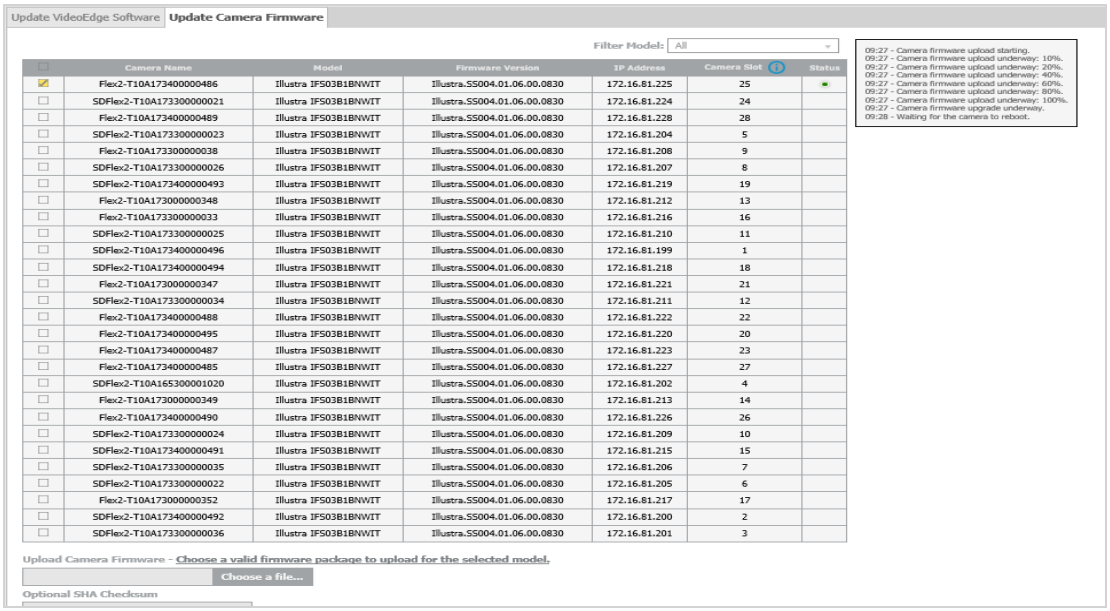
It is recommended that you should schedule when NVR upgrades are applied and expect a loss of video when services restart. When upgrading NVRs which are being monitored by a secondary (Failover) NVR you need to stop Server Monitoring to prevent the secondary NVR taking over when the upgraded primary NVR's services stop.

Applying camera firmware updates using the Administration Interface

You can apply camera firmware updates using the softwareadmin user credential. The Update Camera Firmware page lists the cameras currently added to the VideoEdge whose firmware can be updated. To update camera firmware, you must upload a new camera firmware package and then install the update. When a camera's firmware is being upgraded, a progress status displays to the right of the camera table.

Note:
Firmware uploaded for a camera model is deleted and replaced with any firmware subsequently uploaded for that same model.

Figure 32 Update Camera Firmware page



Procedure 131 Updating Camera Firmware

1 Log in using the softwareadmin user credential:
   a Enter **softwareadmin** in the username field.
   b Enter your password. The default password for the softwareadmin user credential is **softwareadmin**
   The Update VideoEdge Software page opens.
2 Click the **Update Camera Firmware** tab.
3 Select the checkbox of the camera model you want to associate the firmware with.

Note:
You can use the **Filter Model** list to filter the camera list. When you select a camera model from the **Filter Model** list, all updatable cameras of that model type are selected.

---

4 Click **Choose a file**.
5 Select the firmware package file and click **Open**.
   The name of the package file appears in the **Upload Camera Firmware** field.
6 (Optional) Enter the checksum in the **Optional SHA Checksum** field.
7 Click **Upload**.
   The uploaded package is displayed in the **Firmware Package** list.
8 Select the checkbox of the firmware package you want to apply.
9 (Optional) Select the **Initial Reboot** checkbox to reboot the camera prior to the firmware upgrade.
10 Click **Upgrade**.

Procedure 132 Deleting an uploaded Firmware Package

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 VideoEdge Software page opens.
2 Click the **Update Camera Firmware** tab.
3 Select the checkbox of the firmware package you want to delete.
4 Click **Delete**.

5 Click **OK**.

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. To view the serial protocols, select the Serial Protocols submenu from the System menu.

Procedure 133 Viewing Serial Protocols

1 Click the **System** menu.
2 Click **Serial Protocols**.

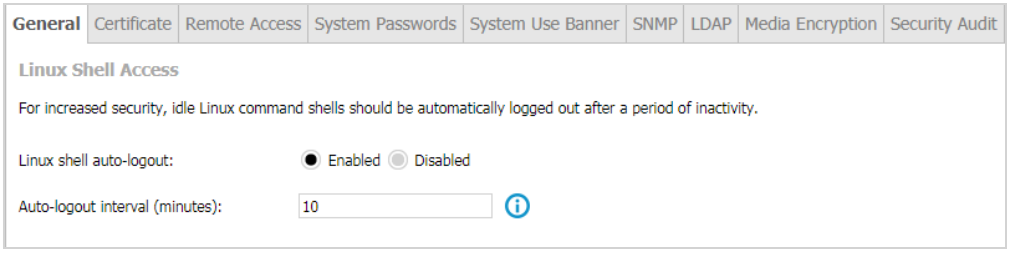
Security Configuration

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.

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.

Figure 33 Security Configuration - General page

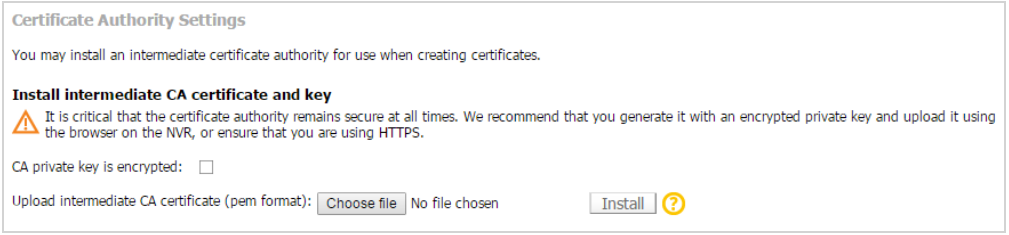


Procedure 134 Enabling auto-logout for VideoEdge

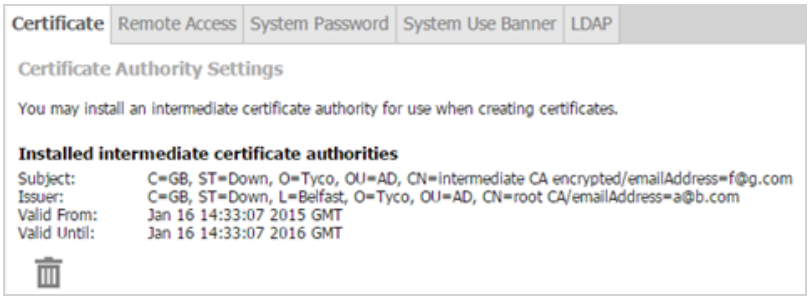
1 Click the **System** menu.
2 Click **Security Configuration**.
3 Click **Enabled** to enable Auto-logout.
4 (Optional) Edit the **Auto-logout interval**. The minimum value is 5 minutes and the maximum value is 300 minutes.
5 Click the **Save** icon.

Certificate Authority Settings

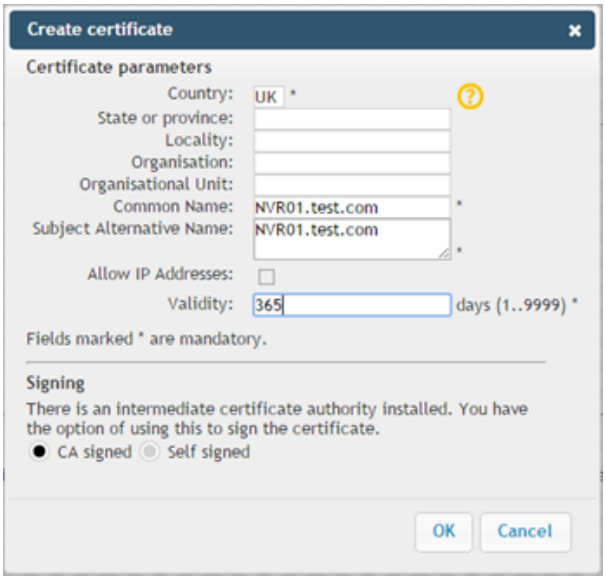
The Certificate Authority Settings section allows an intermediate certificate authority to be installed on the NVR for use in signing the NVR's certificate. It is the responsibility of the customer to deploy the appropriate certificate chain to client computers. The uploaded certificate authority should be PEM-encoded and should contain the CA certificate and encrypted private key.



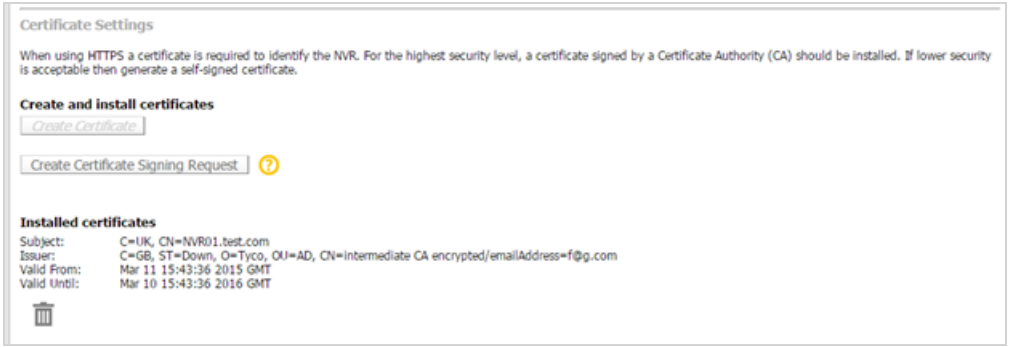
After you install the Certificate Authority, the details of the CA are visible on the Certificates Page.



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.



Procedure 135 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.

1 Click the **System** menu.
2 Click **Security Configuration**.

3 Click 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**.

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 136 Installing Root and Intermediate Certificates

1 Open Microsoft Management Console (MMC). **Windows Button** > **MMC** > **Return**.
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 appears 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.

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 137 Creating a Certificate Template

1 Click the **System** menu.
2 Click **Security Configuration**.
3 Click the **Certificate** tab.
4 Click the **Settings** icon.
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 **Organization**.
9 (Optional) Enter the **Organizational Unit**.
10 Enter the **Validity**.
11 Click the **Save** icon.

Enabling 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 138 Enabling Certificate Automatic Generation

1 Click the **System** menu.
2 Click **Security Configuration**.
3 Click the **Certificate** tab.
4 Scroll to the Certificate Automatic Generation section of the page.
5 Click the **Enabled** option button.
6 Click the **Save** icon.

Certificate Settings

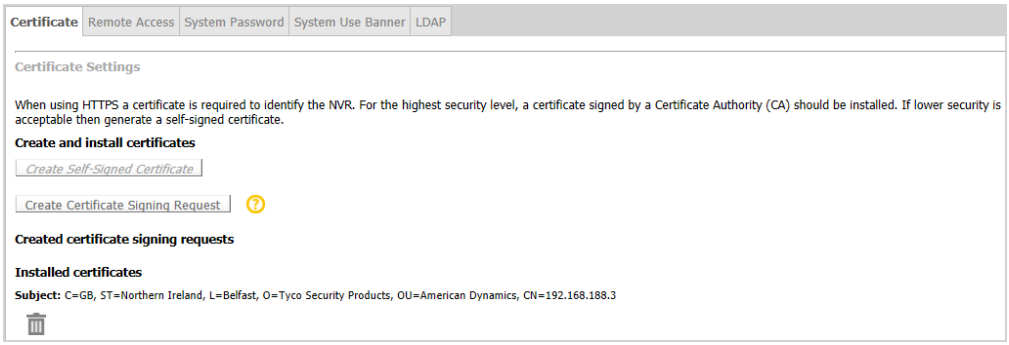
When using HTTPS communication, a PKI certificate is required to provide secure encrypted communications and identify the NVR to the connecting device. VideoEdge supports the creation of a self-signed certificate or use of a certificate provided by a 3rd-party Certificate Authority. A certificate sourced 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 34 Certificate page



Procedure 139 Creating a self-signed certificate

1 Click the **System** menu.
2 Click **Security Configuration**.
3 Click 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 **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 Edit the **Validity** if required.
13 Click the **Save** icon.
The new certificate is activated.
14 Click the **Cancel** icon and restart your browser.

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 140 Creating a request for a signed certificate

1 Click the **System** menu.
2 Click **Security Configuration**.
3 Click 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 **Save** icon.

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 the **Cancel** icon.

Note:
A summary of the certificate request will be displayed on the Certificates page. To delete an awaiting certificate request, click the **Delete** icon.

Uploading a signed certificate

Once your CA has issued a signed certificate, it can be uploaded using the Security Configuration tab.

Procedure 141 Uploading a signed certificate

1 Click the **System** menu.
2 Click **Security Configuration**.
3 Click the **Certificate** tab.
4 Click **Browse**.
5 Use the windows file explorer to locate the signed certificate.
6 Click **Open**.
7 Click **Install**.

Remote Access Services

You can enable or disable SSH and XRDP remote access to the VideoEdge operating system using the Security Configuration menu.

You cannot enable SSH or XRDP until you change the default VideoEdge password and system password.

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, log in using the **VideoEdge** user account.

Procedure 142 Enabling and disabling Remote Access Services

1 Click the **System** menu.
2 Click **Security Configuration**.
3 Click 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.
6 Click **OK**.

Enabling, disabling and restricting Remote Web Access

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.

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 143 Enabling, disabling and restricting Remote Web Access

1 Click the **System** menu.
2 Click **Security Configuration**.
3 Click 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.
6 Click **OK**.

Web Server Protocol Configuration

When installing VideoEdge for the first time, the web server supports Secure HTTP (HTTPS) communication protocol by default. The HTTPS port has a default value of 443 and is configurable.

When upgrading VideoEdge from a previous version, the existing web server protocol settings are retained. The HTTP port has a default value of 80 and the HTTPS port has a default value of 443. You can configure the communication protocol and port type as HTTP or HTTPS.

HTTP vs. HTTPS

HTTP transmits the data between your browser and a website. HTTPS encrypts the data between your browser and a website, providing bidirectional encryption between VideoEdge and its clients.

For optimum security:

• Use HTTPS only

• Change default ports to defend against non-targeted attacks.

• Create a digital certificate

TLS

Transport layer security (TLS) v1.2 is the default on VideoEdge. TLS v1.0 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. After you add VideoEdge to victor, disable TLS v1.0.

Note:TLS v1.0 will not be supported in future releases.

Creating a digital certificate

When VideoEdge is in default HTTPS mode, you must create a digital certificate to complete the Install Wizard. While HTTPS encrypts web traffic, it does not verify the identity of a remote host without the use of a digital certificate. Creating a unique certificate for an individual NVR allows your web browser and victor Client to verify its identity.

Note: VideoEdge is provided with a default certificate. When configuring VideoEdge, install a unique digital certificate for an individual NVR.

Create a digital certificate as follows:

- **Self-signed certificate:** Use a digital certificate generated as a self-signed certificate on VideoEdge. For more information, see Creating a self-signed certificate.
- **Certificate signing request:** For optimum security, use a digital certificate provided by a certificate authority (CA) after creating a certificate-signing request. For more information, see Creating a request for a signed certificate. A certificate can be created in the Install wizard or the Admin GUI post-installation.

Note: For optimum security, use the default HTTPS mode. However, if you do not want to create a certificate, revert to HTTP and HTTPS mode. For more information, see Procedure 145 Editing the Web Server configuration.

Procedure 144 Editing the Web Server configuration

1 Click the **System** menu.
2 Click **Security Configuration**.
3 Click the **Remote Access** tab.
4 Navigate to the Web Server Ports and Protocols section.
5 Select the **HTTP and HTTPS** option button, or select the **HTTPS only** option button.
6 (HTTP and HTTPS only)
  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.

7 (Optional) Select the **Enabled** button to enable TLSv1.0.
8 Click the **Save** icon.

System Passwords

From the System Passwords page, you can change the VideoEdge Linux account password, and the root Linux account password.

In Enhanced security mode, the pre-configured Linux accounts, VideoEdge and root, are replaced with new user accounts during the Setup Wizard. Ensure that you remember the respective account names and passwords for the replacement accounts, as they will be required for password changes.

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.

You can enable and disable access for the Linux support user from the System Passwords page.

You cannot enable SSH or XRDP until you change the VideoEdge password. For security reasons, the System Password page must run under HTTPS.

Caution

It is highly recommended for security reasons that you change the root password and the VideoEdge password.

Procedure 145 Changing the VideoEdge Linux account password

1 Click the **System** menu.
2 Click **Security Configuration**.
3 Click 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 In the **Linux Account: VideoEdge** section, change the VideoEdge Linux account password.
  a Enter the **Current Password**.

Note:
The default VideoEdge Linux account password in Standard security mode 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 the **Save** icon at the top of the page.

Procedure 146 Changing the root Linux account password

1 Click the **System** menu.
2 Click **Security Configuration**.
3 Click 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 Click **Continue to this website (not recommended)**.

Note:
Wording may differ between browsers.

6 In the **Linux Account: root** section, change the root Linux account password.
a Enter the **Current Password**.

Note:
The default root Linux account password in Standard security mode 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 the **Save** icon at the top of the page.

Procedure 147 Configuring Linux support user access

1 Click the **System** menu.
2 Click **Security Configuration**.
3 Click the **System Passwords** tab.
4 In the **Linux User Access: support** section, configure Support Access:
- Select **Enabled** to enable access for the Linux support user.
- Select **Disabled** to disable access for the Linux support user.

Note:
Selecting **Enabled** or **Disabled** will automatically change access permissions for the Linux support user. No save is required.

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. The System Use Banner is not populated by default.

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.

Procedure 148 Configuring the System Use Banner for non-XRDP Clients

1 Click the **System** menu.
2 Click **Security Configuration**.
3 Click the **System Use Banner** tab.
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 the **Save** icon.

Procedure 149 Configuring the System Use Banner for XRDP 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.

1 Click the **System** menu.
2 Click **Security Configuration**.
3 Click 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 XRDP clients may be sensitive to the .bmp image size.

6 Click **Open**.
7 Click **Upload XRDP Banner**.

SNMP Configuration

Simple Network Management Protocol (SNMP) 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. SNMP Services are enabled by default.

Note:
When accessing the VideoEdge remotely, you log in using the **VideoEdge** user account.

Procedure 150 Enabling and disabling SNMP services

1 Click the **System** menu.
2 Click **Security Configuration**.
3 Click the **SNMP** tab.
4 Click the **Enabled** button to enable SNMP services, or click the **Disabled** button to disable SNMP services.
5 Click the **Save** icon.

LDAP Configuration

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. LDAP is not configured by default.

Note:
If the LDAP server is offline, access to the VideoEdge Administration Interface and 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 151 Enabling LDAP support

1 Click the **System** menu.
2 Click **Security Configuration**.
3 Click 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.

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 the **Save** icon.

Media Encryption

From the Media Encryption page you can view the media encryption status of the NVR, import an encryption key, and export the encryption key. You can only export the encryption key if Media Encryption is enabled. Media Encryption is set during the Setup Wizard, and is not configurable after the setup wizard is complete.

Media Encryption provides an additional layer of security for protecting your data. If a hard drive is lost or stolen, or is transferred to another NVR, the encryption key is required to decrypt and access stored media.

Exporting the media encryption key

If you enabled Media Encryption during the setup wizard, you can export the encryption key. If a hard drive with encrypted media is transferred to another NVR, this exported encryption key must be imported to the new NVR to decrypt and access the stored media.

Procedure 152 Exporting the media encryption key

1. Click the **System** menu.
2. Click **Security Configuration**.
3. Click the **Media Encryption** tab.
4. Click **Export encryption key** and save the file to a location.
   Ensure that you store the encryption key securely.

Importing the media encryption key

To decrypt encrypted media from an added hard drive, you must import the appropriate encryption key.

Caution

If you install an encrypted hard drive on a system that already has media, importing the encryption key will render the existing system media inaccessible. Importing an incorrect encryption key on a system with encrypted media, or importing an encryption key on a system with unencrypted media, will render the existing media inaccessible.

Procedure 153 Importing the media encryption key

1. Click the **System** menu.
2. Click **Security Configuration**.
3. Click the **Media Encryption** tab.
4. Click **Browse...**.
   The name of this button may differ depending on what browser you are using.
5. Navigate to where you have stored the encryption key and click **Open**.
6. Click **Import encryption key**.

Security Audit

The Security Audit page contains a read-only status summary for the following NVR settings: Role Settings, User Settings, Camera Restrictions, Linux User Settings, Web Server Ports and Protocols, Remote Access, Certificate Settings, Certificate Authority Settings, SNMP Settings, and System Robustness.

The NVR settings shown on the Security Audit page are color-coded. The color assigned indicates the current security level of the setting, and whether or not a security change is recommended.

- Green - 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:
Review the Security Audit page every time you change your VideoEdge security settings.

Network

Use the Network menu to configure the NVR's network settings, including general network settings, LAN Interface settings, DHCP Server settings, and WAN settings. The Network menu contains the following submenus:

- **General** - The General menu contains the **Network General** section. From here you can configure general network settings.
- **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. The DHCP Server submenu contains the following sections: **DHCP Server**, and **DHCP Status**.
- **WAN Settings** - From here you can configure the NVR to operate in a wide area network.
- **Secure Connection** - From here you can enable or disable victor Secure Connection software. The Secure Connection submenu contains the **victor Secure Connect Settings** section.

Network icons table

Table 34 Network icons

Icon	Name	Function
	**Save**, **Save static route configuration**	Save
	**Cancel**	Cancel
	**Add new static route**	Add new static route.
	**Remove static route** **or** **Mark Group for deletion**	Remove static route or Mark a failover group for deletion
	**Apply**, **Enable**	Apply the static route settings; reserve a DHCP address.
	**Disable**	Cancel a DHCP reservation.
	**Edit**	Edit
	Green Add	Open the IP Address and Subnet Mask fields.
	Red Cancel	Clear the IP Address and Subnet Mask fields.

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 35 Network diagram example (VideoEdge Hybrid NVR)

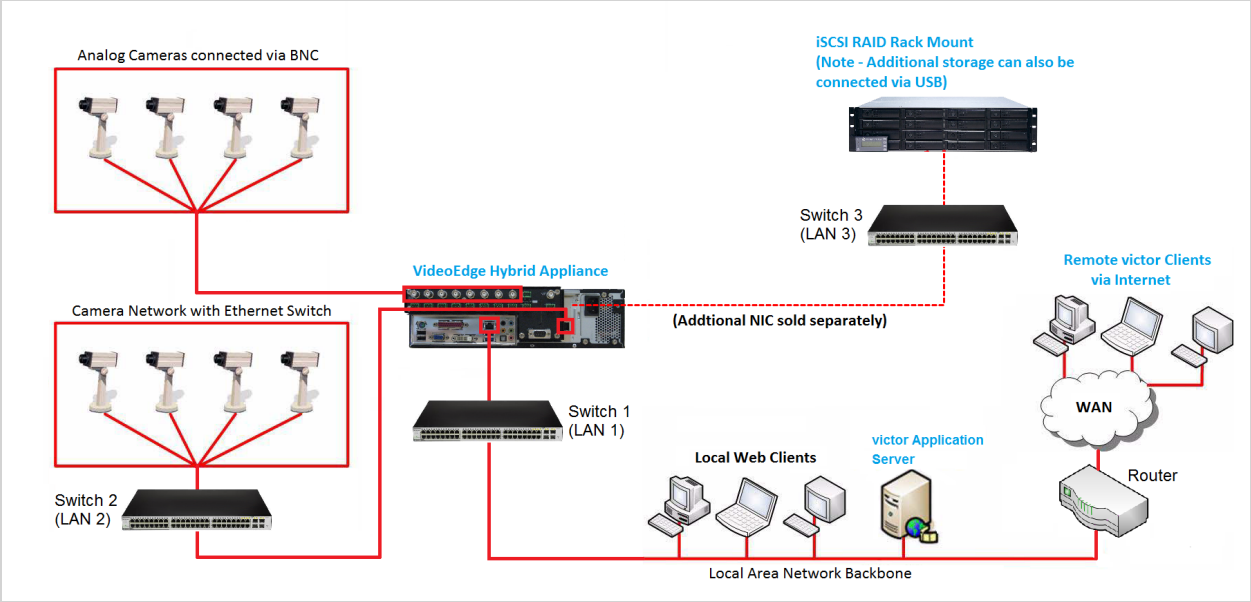
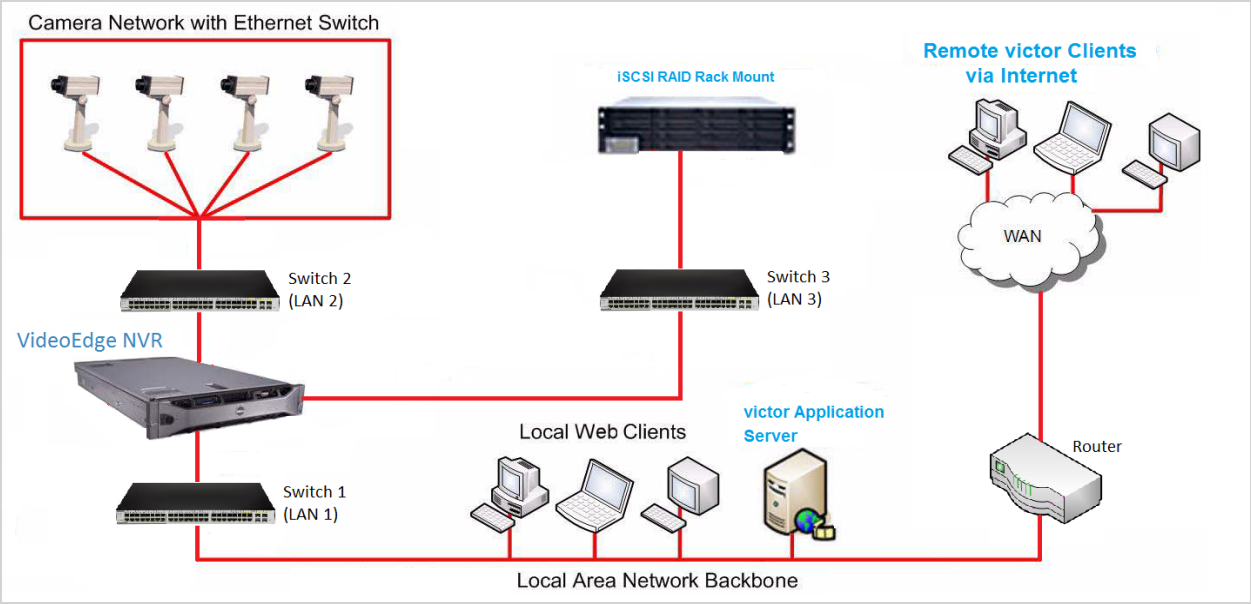


Figure 36 Network Diagram Example (VideoEdge NVR)



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.

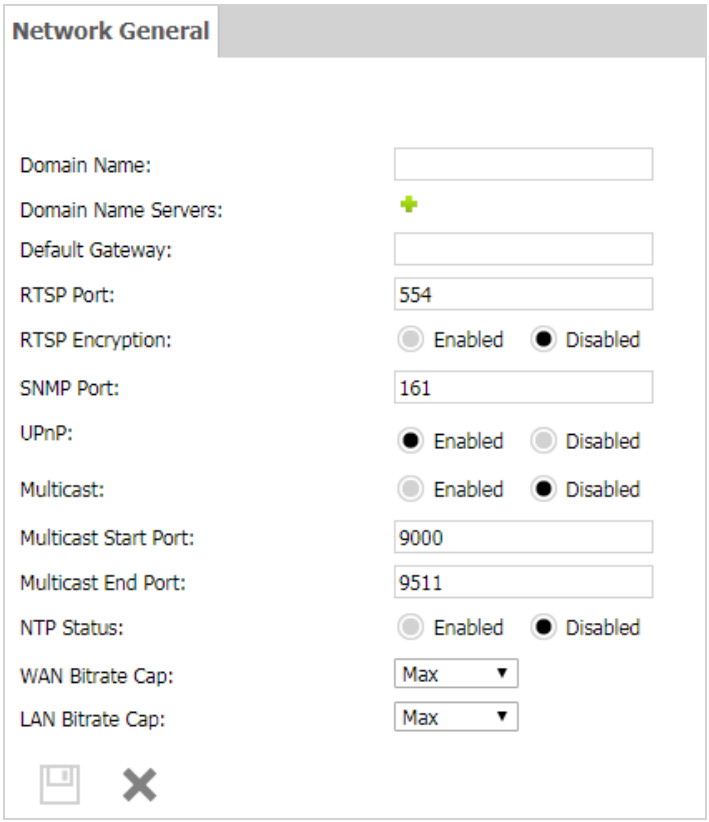
Note:
When the NVR is supplied as a hardware and software bundle only LAN 1 will be enabled, all other NICs will be disabled.

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

From the Network General page you can configure your NVR's general network settings. When you configure the required setting, click the **Save** icon to complete the change.

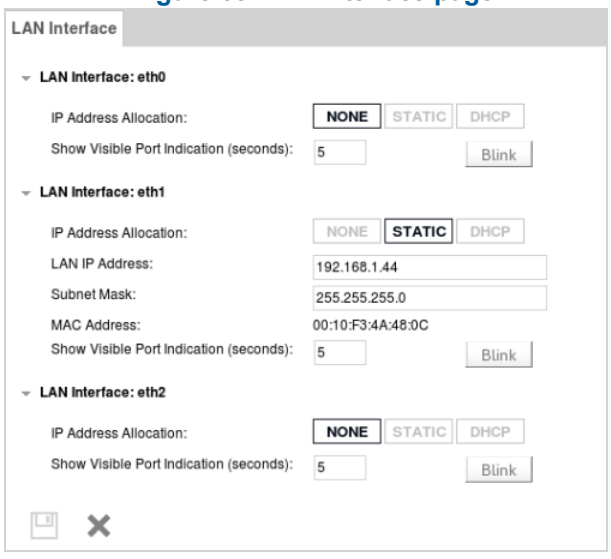
Figure 37 General Network page



LAN Interface

You can enable and disable the NVR's network interface controllers (NICs) from the LAN Interface page. Each NIC provides a LAN interface for the NVR. You can edit the IP Address Allocation, LAN IP Address and Subnet Mask of available NICs. The MAC address for each NIC is displayed, but cannot be edited.

Figure 38 LAN Interface page



When selecting an IP Address Allocation, the following options are available:

- **NONE**: Select this to disable the NIC. If you disable eth0 using the NVR Administration Interface, it will terminate its connection on that NIC. To re-establish connection, access the Administration Interface using the IP Address of one of the other active NICs.
- **STATIC**: Select this to permanently assign an IP address and subnet mask to the NIC.
- **DHCP**: Select this to permit a DHCP server on the LAN to assign an IP address for the NIC.

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.

If supported, you can use the **Show Visible Port Identification** setting to identify the physical location of each LAN interface on the NVR to aid correct connection to the appropriate network. Enter a value in seconds, and click **Blink**.

If you are configuring or editing the LAN Interface settings for a primary NVR when failover mode is in use on your network, the unit's Virtual IP address will also display on this page. It cannot be edited.

Procedure 154 Enabling NICs

1 Click the **Network** menu.
2 Click **LAN Interface**.
3 Choose the LAN Interface you want to edit.
4 Click **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
Click **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 the **Save** icon.
6 Click **OK**.

Procedure 155 Disabling NICs

1 Click the **Network** menu.
2 Click **LAN Interface**.
3 Choose the LAN Interface you want to edit.
4 Select **NONE** from the **IP Address Allocation** list.
When **NONE** is selected the LAN Interface options for that NIC will collapse leaving only the IP Address Allocation displayed.
5 Click the **Save** icon.
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.

Procedure 156 Configuring the LAN Interface values

1 Click the **Network** menu.
2 Click **LAN Interface**.
3 Choose the LAN Interface you want to edit.
4 Select an **IP Address Allocation** option.
You must select **STATIC** to edit the LAN IP Address and Subnet Mask.

5 Enter the required IP address in the **LAN IP Address** field.
6 Enter the required subnet mask in the **Subnet Mask** field.
7 Click the **Save** icon.

NIC failover

You can create a failover group by teaming NICs. This facilitates a failover to a backup NIC if the primary fails so that connectivity is maintained. Events are raised in response to changes in the health of a failover group, such as when a NIC in a group fails or recovers.

Configuring a NIC failover group

You can configure up to two NIC failover groups with two NICs per group. You can only configuring one NIC failover group at a time.

1 Click the **Network** menu and then click **LAN Interface**.The LAN Interface page opens.
2 Click the **Add LAN Interface Failover Group** icon.
3 Select a LAN Interface from the **Members** section. The group inherits the LAN Interface's IP Address, Subnet Mask, and IP Address Allocation method.

Note:
You can change the inherited configurations.

4 Select a second LAN Interface from the **Members** section. This pairs the LAN Interfaces.

Note:
The group does not inherit the LAN Interface's IP Address, Subnet Mask, and IP Address Allocation method from the secondary LAN Interface.

5 Select the **Save** icon. A warning message displays.
6 Click **OK**. The updates are applied.
7 **Optional:** If you need to delete a group:
   a Click the **Mark Group for deletion icon**. A warning message displays.
   b Click **OK**.
   c In the **Group Update** section a message displays. Click the **Save** icon to apply the changes. Click the **Cancel** icon to undo the changes.

Using the Show Visible Port identification feature

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 157 Using the Show Visible Port identification feature

1 Click the **Network** menu.
2 Click **LAN Interface**.
3 Enter the **time** in seconds you want the LED indicator to blink.
4 Click **Blink**.

Routing

From the Routing page, you can configure a static route from your VideoEdge to another network. The following table describes the parameters in the Add Static Route window.

Table 35 Add Static Route window

Parameter	Description
Interface	The interface that packets for this route are sent to.
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.
Priority	To specify a priority metric to determine which route has a higher priority.

Procedure 158 Adding a Static Route

1 Click the **Network** menu.
2 Click **Routing**.
3 Click the **Add new static route** icon.
The Add Static Route window appears.
4 Select a network interface from the **Interface** 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 Click the **Apply** icon.
7 (Optional) Add additional routes if required.
8 In the Routing page, click the **Save static route configuration** icon to save the configuration changes.

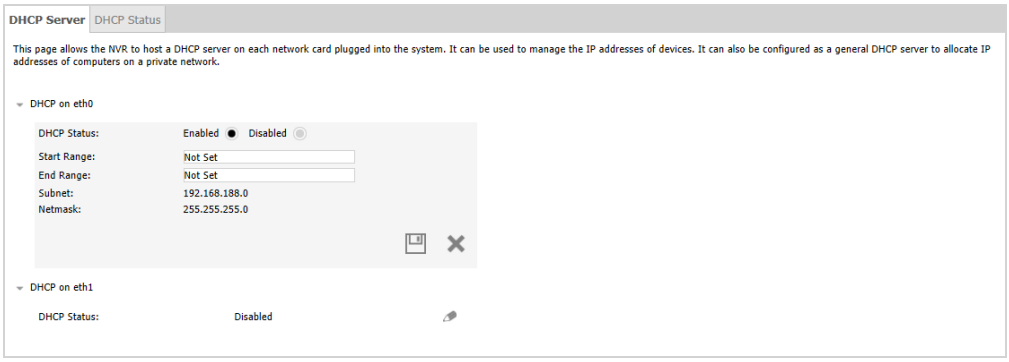
DHCP Server

The DHCP Server page provides the option to configure the NVR to host a DHCP server for each network card plugged into the system. The NVR can then allocate IP addresses from the range specified when other devices request IP allocation. You can view the DHCP status, and edit 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 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 providing IP addresses, and this could cause network problems.

Figure 39 DHCP Server page



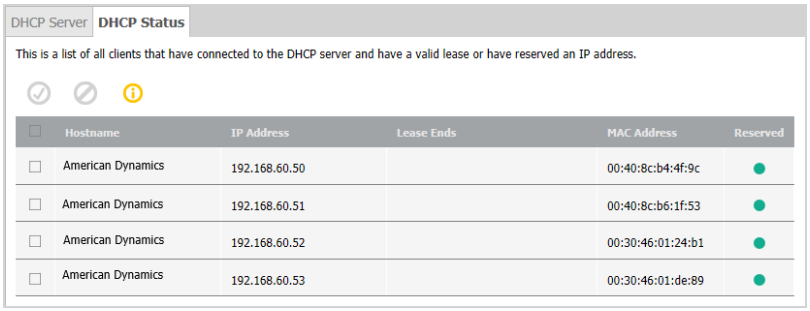
Procedure 159 Configuring the DHCP server settings

1. Click the **Network** icon.
2. Click **DHCP Server**.
3. Click the **Edit** icon next to the LAN Interface you want to enable as a DHCP server.
   NICs which have been configured with a DHCP IP Address Allocation will be grayed out and not available to host DHCP Servers.
4. To edit the DHCP Status, click **Enable** or **Disable**.
   You must click **Enabled** to edit the DHCP Start Range and End Range.
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 are between 10.11.12.50 and 10.11.12.100, you could enter 10.11.12.50 in the **Start Range** field and 10.11.12.100 in the **End Range** field.
   Subnet and Netmask cannot be edited in this page.
6. Click the **Save** icon.

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, and the IP address reservation status.

Figure 40 DHCP Status page



Procedure 160 Reserving a DHCP address

1. Click the **Network** icon.
2. Click **DHCP Server**.
3. Click the **DHCP Status** tab.
4. Click the **Enable** icon, or click the icon in the **Reserved** column.

Procedure 161 Canceling a DHCP reservation

1 Click the **Network** icon.
2 Click **DHCP Server**.
3 Click the **DHCP Status** tab.
4 Click the **Disable** icon, or click the icon in the **Reserved** column.

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. After you edit the WAN settings, click the **Save** icon to complete the changes.

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 installation, 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 41 WAN Port Mapping Exam

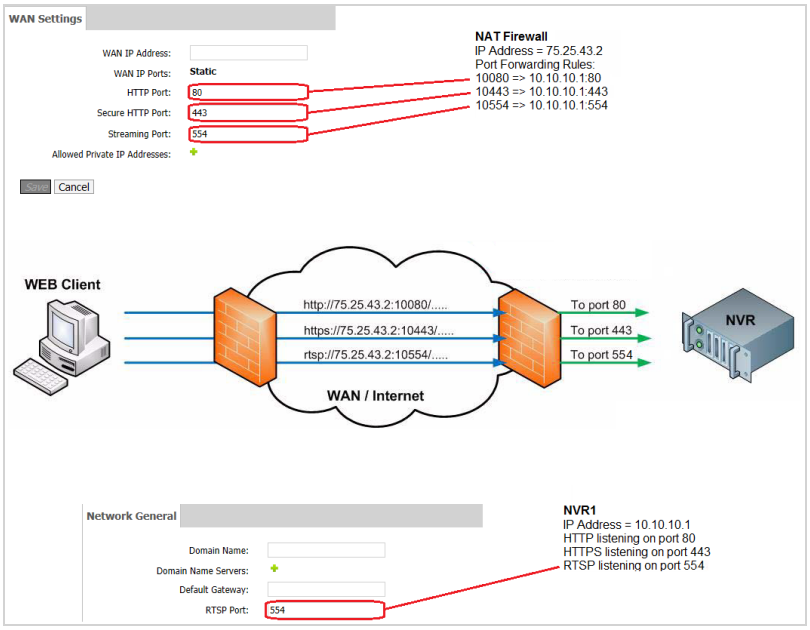
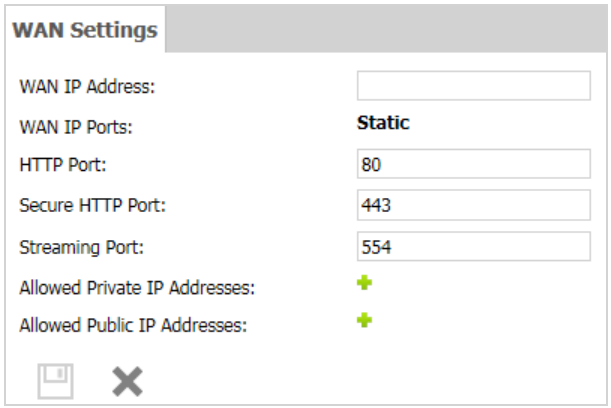


Figure 42 WAN Settings page



Secure Connection

From the Secure Connection page, you can enable or disable victor Secure Connection (vSC) software for VideoEdge. 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.

Procedure 162 Enabling victor Secure Connection software in Standard Provisioning Mode

1. Click the **Network** icon.
2. Click **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 the **Save** icon.

Procedure 163 Enabling victor Secure Connection software in Advanced Provisioning Mode

1. Click the **Network** icon.
2. Click **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 the **Save** icon.

Advanced

Use the Advanced menu to view and configure the NVR's advanced system settings. The Advanced menu contains the following submenus:

- **Failover** - From here you can view the Failover Events report.
- **Storage Statistics** - From here you can view statistics relating to storage. The Storage Statistics submenu contains the following sections: **Rec Performance**, **Disk Activity**, **Storage Sets**, **Media Devices**, and **Video**.
- **Stream Statistics** - From here you can view statistics relating to recorded video and audio streams. The Stream Statistics submenu contains the following sections: **Video Rec Statistics**, **Audio Rec Statistics**, and **Device 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. The Logs submenu contains the following sections: **Retrieve Logs**, **Log Management**, **Event Logs**, **Connection**, **Device Logs**, and **Audit Trail**.
- **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. The Email Alerts submenu contains the following sections: **Email Alerts**, **Email Blocks**, and **Alert Logs**.
- **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.
- **SIP Proxy** - From here you can enable or disable an SIP Proxy, and you can select the inbound and outbound interface.
- **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.

Advanced icons table

Table 36 Advanced icons

Icon	Name	Function
	**Zoom out**	Zoom out
	**Refresh**	Refresh
	**Edit**	Edit
	**Save**, **Submit**	Save, submit image.
	**Cancel**	Cancel
	**Delete**, **Remove Email Block**, **Remove**, **Delete the selected Equivalent Models**	Delete; remove email block; remove; delete selected equivalent model.

Icon	Name	Function
	**Add/Update Alert Recipient**, **Add New Email Block**, **Add**, **Add new Equivalent Model**	Add or update an alert recipient; add email block; add event filter; add new equivalent model.
	**Enable Alert**	Enable selected alert.
	**Disable Alert**	Disable selected alert.
	**Edit**	Edit
	**Setup**	Open camera configuration.

Failover

The occurrences and timing of Failover events can be queried using the Failover Events page on either a primary or secondary NVR.

Times are displayed in UTC unless you select the **Use Local Time** checkbox. The time values in the Start Date/Time and End Date/Time must be entered in 24-hour format.

Procedure 164 Displaying Failover Events

1. Click the **Advanced** menu.
2. Click **Failover**.
3. Select the Virtual IP address you want to query from the **Virtual IP Address** list.
   Select **ANY** to query all virtual IP addresses which have been monitored by a secondary. 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:
   a. Select the current value.
   b. Enter the required date and time in the field in the format **YYYY/MM/DD Hours:Minutes:Seconds**. Alternatively, select the date from the calendar, and use the sliders to adjust the time.
   c. Click **Done**.
6. Click **Get Failover Events**.
   All Failover Events within the configured time range display in the table.

Storage Statistics

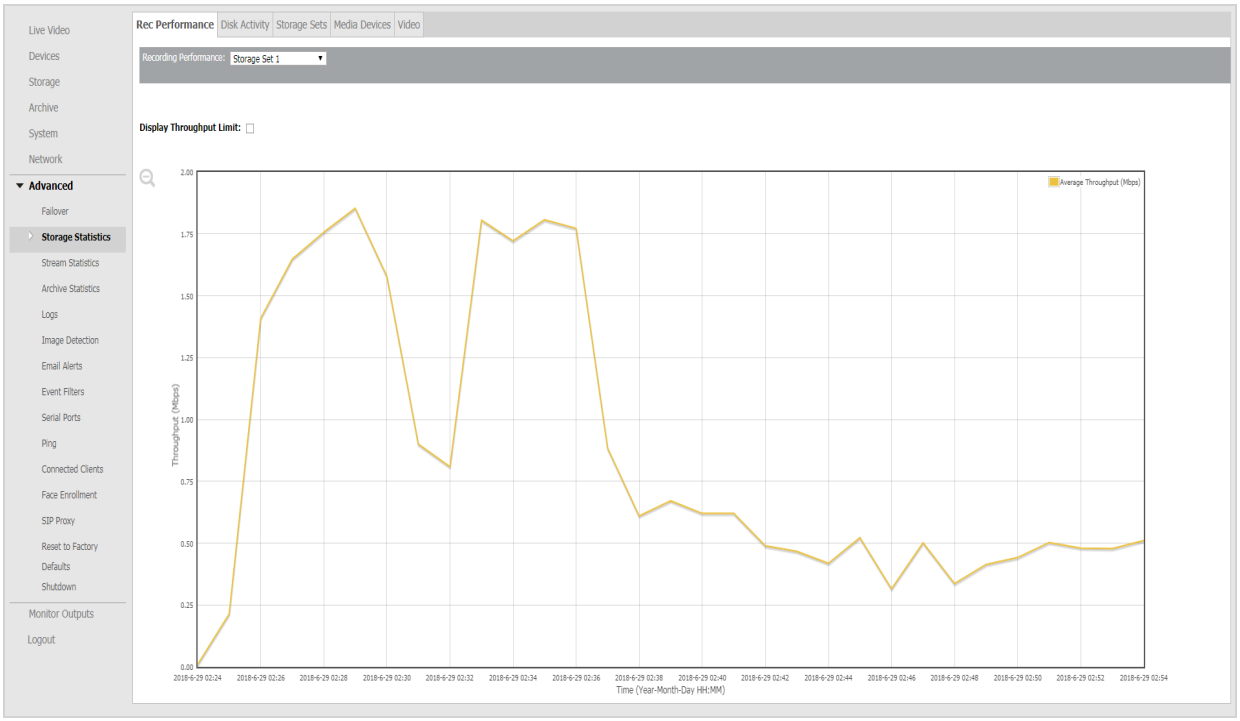
The Storage Statistics menu item allows you to view statistical information for Recording Performance, Disk Activity, Storage Sets, Media Devices and Video.

Recording Performance

The Recording Performance tab contains a graph displaying the average throughput over time for a selected storage set.

Select the storage set you want to view the recording performance for from the **Recording Performance** list. Select the **Display Throughput Limit** checkbox to show the throughput limit on the graph. Hover over points on the graph to show more specific detail. Click and drag over a specific time to zoom in on that time period. Click the **Zoom Out** icon to return to the default view.

Figure 43 Recording Performance tab



Procedure 165 Viewing the Recording Performance statistics

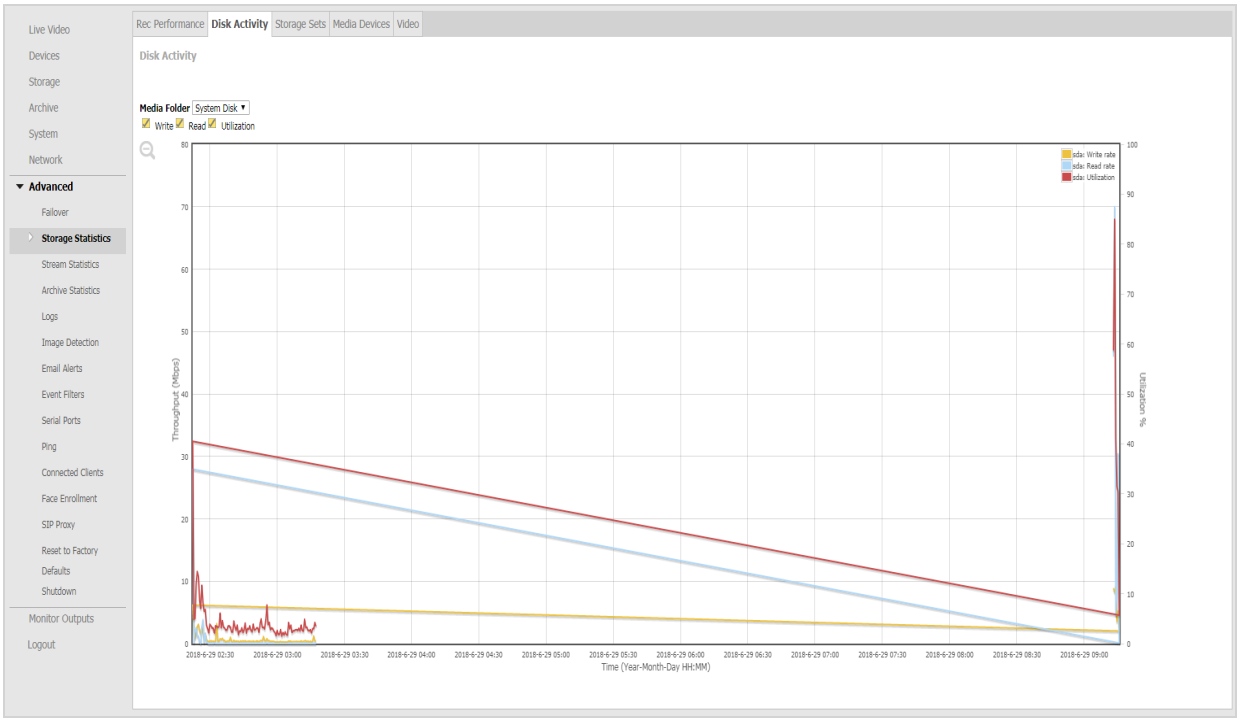
1 Click the **Advanced** menu.
2 Click **Storage Statistics**.
3 Select the storage set you want to view the recording performance for from the **Recording Performance** list.

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. Three disk activity values are shown on the graph: Average Utilization (red), Average Read (blue), and Average Write (yellow).

Select the required media folder from the **Media Folder** list. Select or deselect the **Write**, **Read**, and **Utilization** checkboxes to display the required information. Hover over points on the graph to show more specific detail. Click and drag over a specific time to zoom in on that time period. Click the **Zoom Out** icon to return to the default view.

Figure 44 Disk Activity statistics tab



Procedure 166 Filtering the Disk Activity Graph

1. Click the **Advanced** menu.
2. Click **Storage Statistics**.
   The Rec Performance tab opens.
3. Click the **Disk Activity** tab.
4. Select the **Media Folder** you want the graph to display disk activity for from the list.
5. Select the required **Sampling Rate** from the list. 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** list.
7. Select the **Utilization Scale** from the list.
8. Select the **Disk I/O Scale** from the list.
   The graph adjusts to display the disk activity as per the filters selected.

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 45 Storage Sets tab

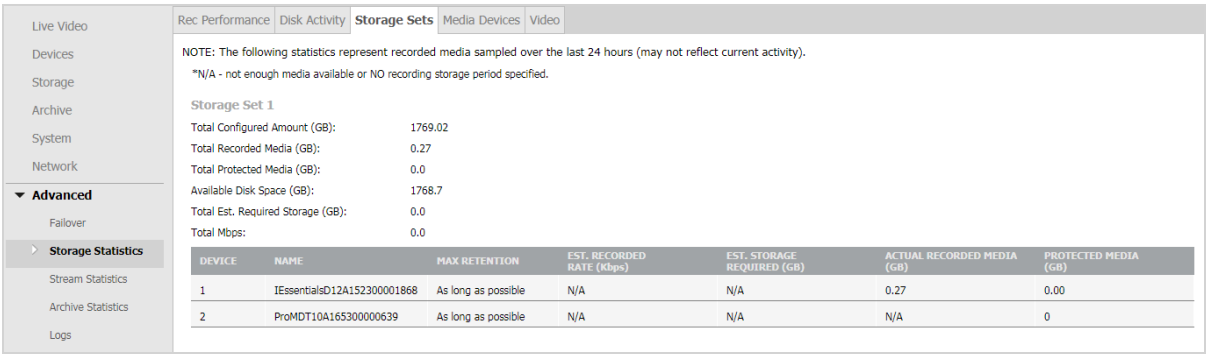


Table 37 Storage Sets Statistics

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.
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 46 Storage Statistics per Media Device

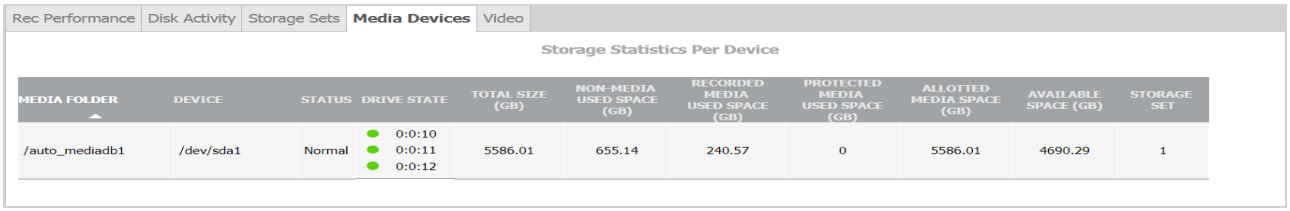


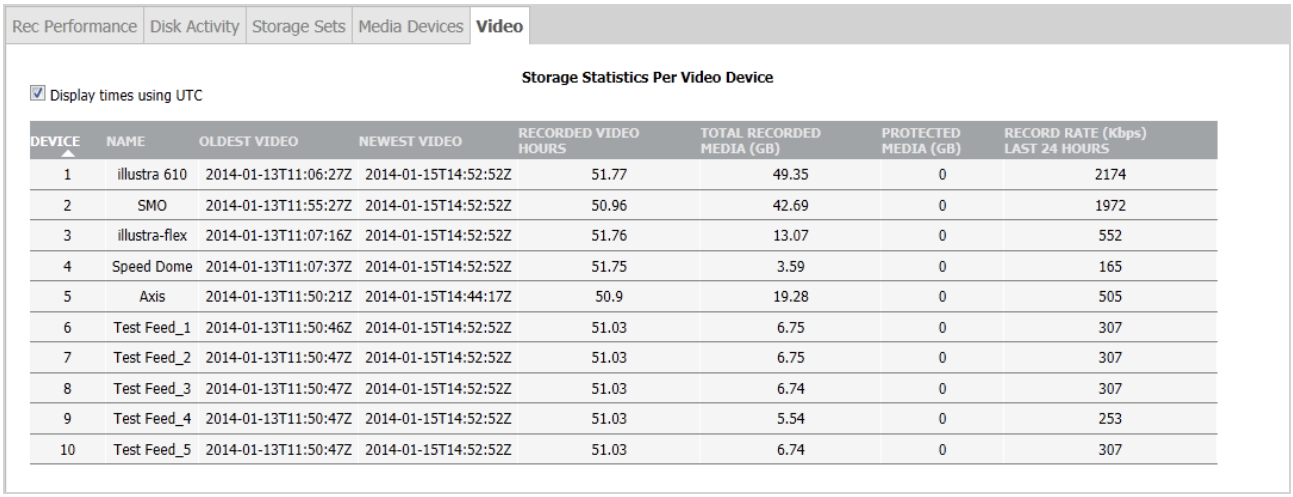
Table 38 Storage Device Statistics

Field	Description
Media Folder	Name of the media folder used by storage.
Device	Associated device on which this media folder is located.
Status	Current Status of this folder (Normal, Degraded and so on).
Drive State	Indicates the health of the physical drives associated with each media folder.
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 Set	Storage set this media folder is assigned to.

Video Device statistics

The Video tab details the storage statistics for each camera.

Figure 47 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 39 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 167 Viewing Storage statistics

1 Click the **Advanced** menu.
2 Select the required tab:
- To view storage set statistics, click the **Storage Sets** tab.
- To view device statistics, click the **Media Devices** tab.
- To view camera statistics, click the **Video** tab.

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 Rec Statistics and Audio Rec Statistics tabs display recording statistics for each device configured on the NVR. The **Reset Stats** button on the Video Recording Statistics tab resets video recording statistics for all cameras, while the **Reset Stats** button on the Audio Recording Statistics tab resets audio recording statistics for all devices. There is also a Totals summary table displaying recording statistics for the total of all devices on the NVR.

Figure 48 Recording Statistics page

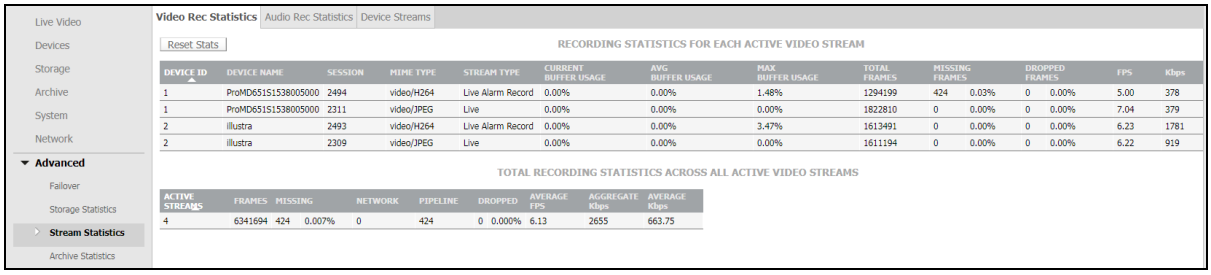


Table 40 Recording Statistics

Field	Description
Device ID	Device input number.
Device Name	Device name as given when adding the device to VideoEdge.
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.
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 41 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.

Procedure 168 Viewing the Video and Audio Recording Statistics

1 Click the **Advanced** menu.
2 Click **Stream Statistics**.
3 Select the required tab:
- To view video recording statistics, click **Video Rec Statistics** tab.
- To view audio recording statistics, click the **Audio Rec Statistics** tab.

Details of these statistics are outlined in the Recording Statistics table or the Total Recording Statistics table.

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 49 Device Streams page

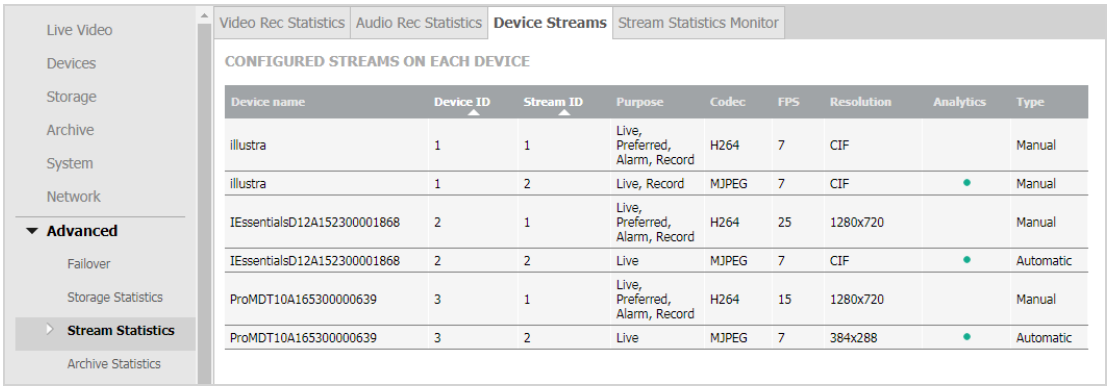


Table 42 Configured Streams on each device

Field	Description
Device name	Device name as given when adding the device to VideoEdge.
Device ID	Device slot number.
Stream ID	Device stream number.

Field	Description	
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. The analytic options are:  Analytics Off  Motion Detection  Video Intelligence (This encompasses object detection, direction, linger, enter, exit and abandoned / removed).  Deep Intelligence  Intelligent Search - Person  Edge Based  Face Recognition including Face Search Alert and Face Verification	
Type	This field shows how the camera is added to VideoEdge: manually or by auto-configuration streams.	

Stream Statistics Monitor

The Stream Statistics Monitor page provides insights on stream performance over time. You can select specific types of streaming data to display on the monitor. The streaming data from multiple cameras can be displayed on the monitor at the same time.

Typically, data from the previous seven days is available on the Stream Statistics Monitor. However, the number of previous days that data is available for can vary depending on the number of cameras connected to the NVR. When you open the Stream Statistics Monitor page, the initial view shows the data from the previous 24 hours.

Figure 50 Stream Statistics Monitor

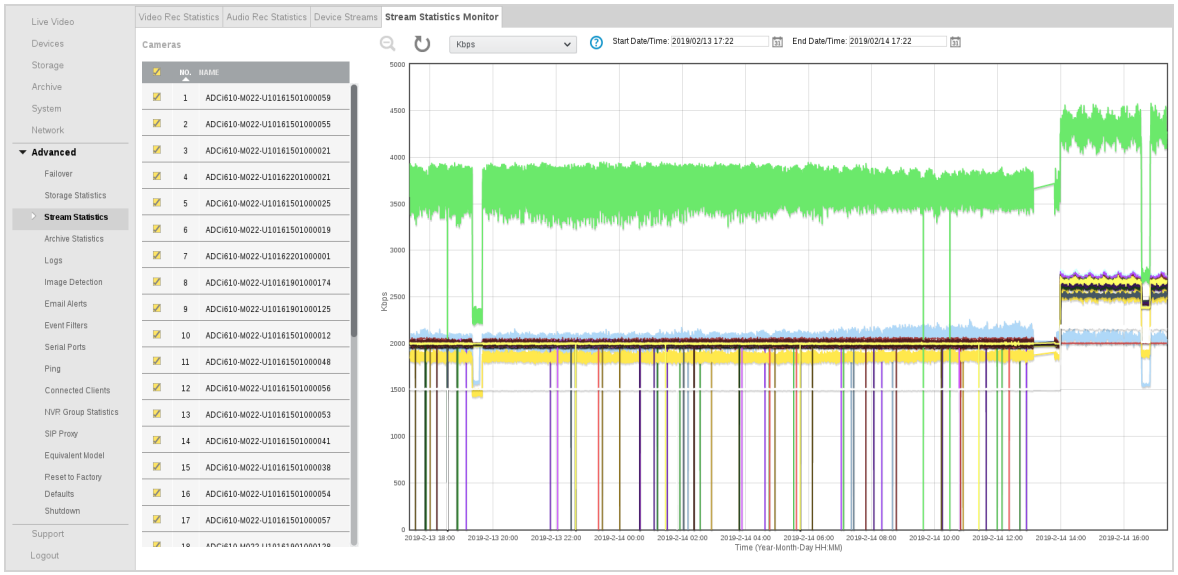


Table 43 Stream Statistics

Field	Description
Kbps	The kilobit per second transfer rate of the device.
Current Stream Buffer Usage	The percentage of the stream buffer currently being used by frames waiting to be written to disk. Higher values may indicate write delays to the disk.
Max Stream Buffer Usage	The highest Stream Buffer Usage reached for frames waiting to be written to disk since stream start or statistics reset. Higher values may indicate write delays to the disk.
Missed Frames	The number of frames that were missed in the stream. This may indicate network problems between the camera and the VideoEdge.
Dropped Frames	The number of frames dropped while waiting to write to disk. This may indicate write delays to media storage, or a maximum throughput violation.
Buffer Frame Count	The total number of frames in the stream buffer. This number includes the frames waiting to be written to disk, and frames that have already been written to disk
Buffer GoP Count (H264 only)	The total number of GoPs (group of pictures) in the stream buffer. Less than two GoPs may cause live stream startup delays.

Procedure 169 Viewing the Stream Statistics Monitor

1 Click the **Advanced** menu.
2 Click **Stream Statistics**.
3 Click the **Stream Statistics Monitor** tab.
The Stream Statistics Monitor page displays. All cameras are selected by default.
4 In the **Cameras** table, clear or select the camera checkboxes as required.
Select a camera's checkbox to display its streaming data in the monitor. Clear the checkbox to hide the data.
5 (Optional) Click the **Refresh** icon to refresh the Stream Statistics Monitor.
6 Select the type of streaming data you want to view from the list at the top of the page:

- **Kbps**
- **Current Stream Buffer Usage**
- **Max Stream Buffer Usage**
- **Missed Frames**
- **Dropped Frames**
- **Buffer Frame Count**
- **Buffer GoP Count (H264 only)**

7 (Optional) Specify a time period to view by selecting a **Start Date/Time** and **End Date/Time**.
8 (Optional) Hover over points on the graph to show more specific detail.
9 (Optional) In the monitor, click and drag over a specific time to zoom in on that time period. Click the **Zoom Out** icon to return to the default view.

Archive Statistics

From the Archive Statistics page, you can view the graphical representation of the total throughput for archiving for your NVR and the throughput per archive destination. Select or deselect the **Points**, **Lines**, **Display write throughput**, **Display read throughput**, **Write rate per archive**, and **Read rate per archive** checkboxes to display the required information. Click and drag over a specific time to zoom in on that time period. Click the **Zoom Out** icon to return to the default view.

Procedure 170 Viewing Archive Statistics

1 Click the **Advanced** menu.
2 Click **Archive Statistics**.
The Archive Statistics page opens.
3 Display or hide the following items as required on the graphs using checkboxes:
- Points
- Lines
- Write throughput
- Read throughput
- Write rate per archive
- Read rate per archive

4 To zoom in, click and drag on the area you want to enlarge.
5 To zoom out, click the **Zoom Out** icon.

Logs

The NVR tracks important types of system events. You can view the following types of logs: Administrative changes, camera alerts, changes to cameras; and system events, which are used by American Dynamics technical support.

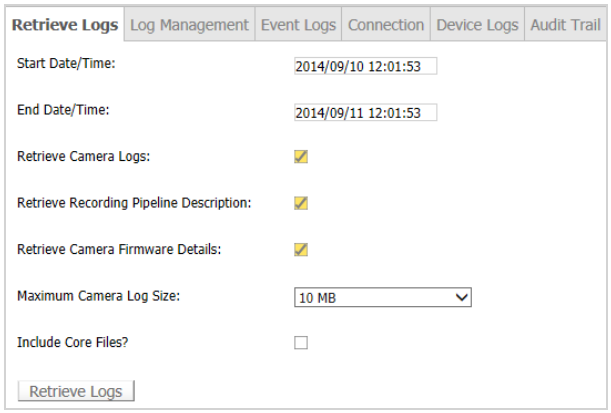
The Logs page provides access to the NVRs log settings. From the Logs page you can retrieve logs, edit the FTP Log Management settings, filter searches for Events Logs, and view Camera Connection Errors, Camera Logs and the Audit Trail.

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 51 Retrieve Logs page



Procedure 171 Retrieving Logs

1 Click the **Advanced** menu.
2 Click **Logs**.
3 Select the **Start Date/Time** and the **End Date/Time** for a time range for retrieving logs:
   a Select the current value.
   b Enter the required date and time in the field in the format **YYYY/MM/DD Hours:Minutes:Seconds**. Alternatively, select the date from the calendar, and use the sliders to adjust the time.
   c Click **Done**
4 Select or clear the **Retrieve Camera Logs** check box as required.
5 Select or clear the **Retrieve Recording Pipeline Description** checkbox as required.
6 Select or clear the **Retrieve Camera Firmware details** checkbox as required.
7 Select the maximum camera log size from the **Maximum Camera Log Size** list.
8 Select or clear the **Include Core Files** checkbox as required.
9 Click **Retrieve Logs**.
10 When the File Download window displays Click **Open** or **Save**.
The Logs folder is now ready to be viewed.

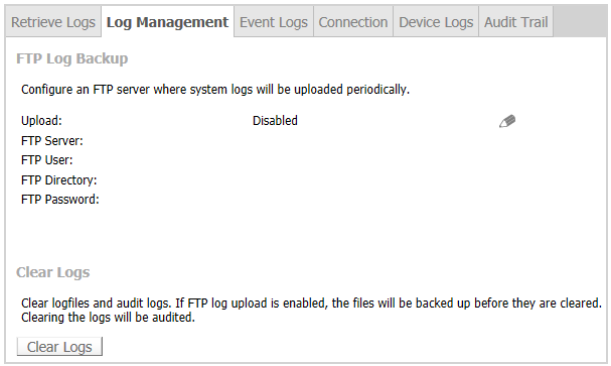
FTP Log Management

From the Log Management page, you can configure FTP server settings where system logs will be uploaded periodically. When the Event Log is full, all entries are cleared. To preserve the Events Log, this function should be configured and enabled. Click the **Clear Logs** button to manually clear the logs. This action will appear in the NVR Audit Trail.

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.

Only syslog files are uploaded when using FTP Log Backup.

Figure 52 Log Management page



Procedure 172 Editing settings for the Log FTP server

1 Click the **Advanced** menu.
2 Click **Logs**.
3 Click the **Log Management** tab.
4 Click the **Edit** icon.
5 Click **Enabled** 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 the **Save** icon.

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 173 Clearing System Logs

1 Click the **Advanced** menu.
2 Click **Logs**.
3 Click the **Log Management** tab.
4 Click **Clear Logs**.

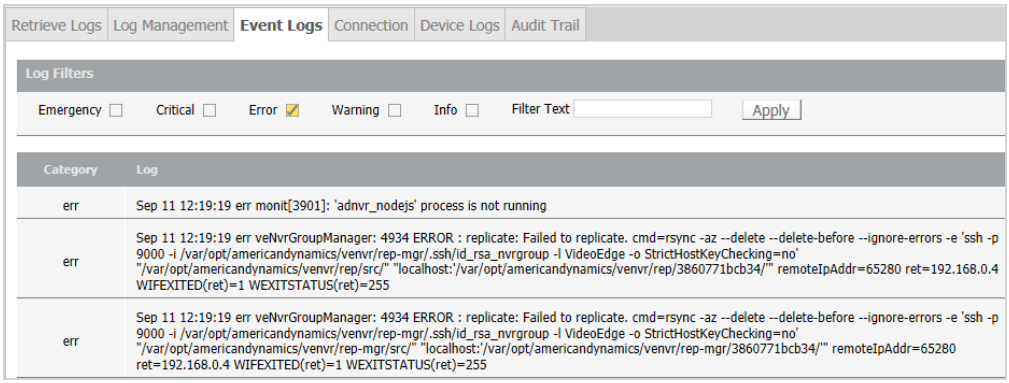
Event Logs

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, 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 53 Event Logs page



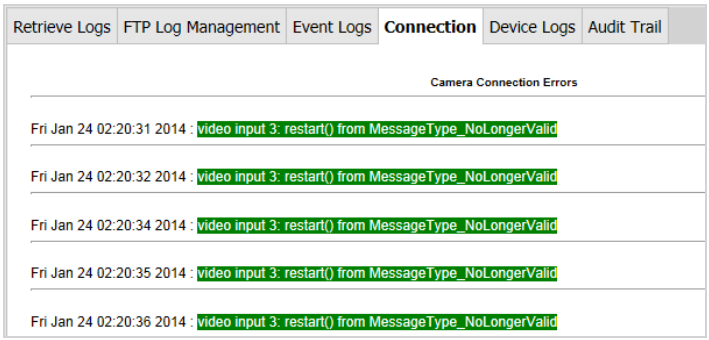
Procedure 174 Viewing Event Logs

1 Click the **Advanced** menu.
2 Click **Logs**.
3 Click the **Event Logs** tab.
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**.

Viewing Camera Connection errors

The Connection page displays the Camera Connection errors that have occurred.

Figure 54 Connection page



Procedure 175 Viewing Camera Connection errors

1 Click the **Advanced** menu.
2 Click **Logs**.
3 Click the **Connection** tab.
You are prompted to enter your Username and Password.
4 Click **OK**.

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 55 Device Logs page

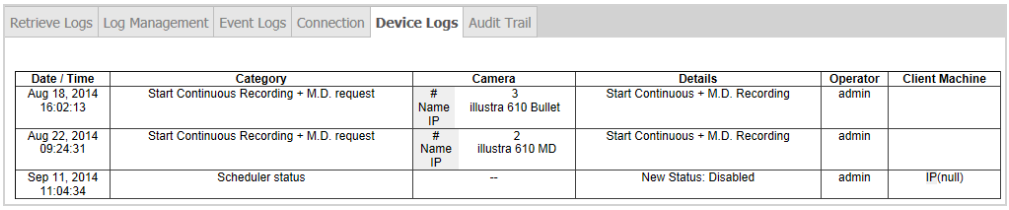


Table 44 Device Logs definitions

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.

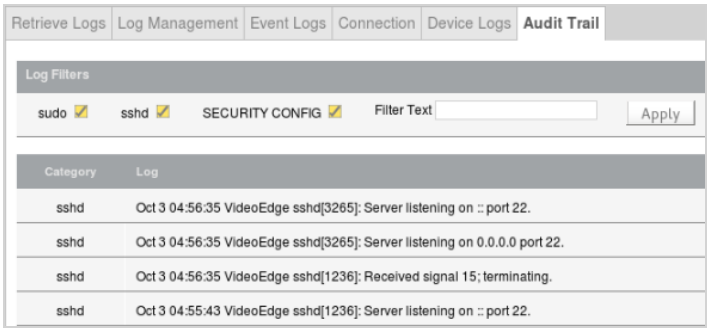
Procedure 176 Viewing the Device Logs

1 Click the **Advanced** menu.
2 Click **Logs**.
3 Click the **Device Logs** tab.

Audit Trail

The Audit Trail page displays a log of system changes which have been made by a privileged user. The following system changes are logged in the Audit Trail: System Date and Time, Software upgrades, FTP Log Management settings, User Login passwords, and Network Settings.

Figure 56 Audit Trail page



Procedure 177 Viewing the Audit Trail

1 Click the **Advanced** menu.
2 Click **Logs**.
3 Click the **Audit Trail** tab.
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**.

Image Detection

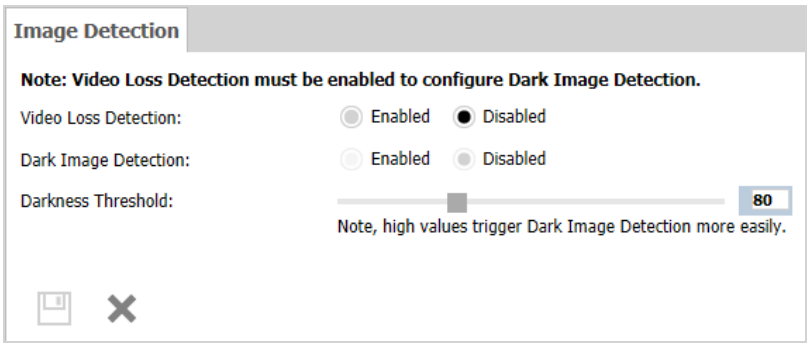
The NVR can perform an Image Detection test on every camera in the network. You can use this test to determine if the NVR has a camera that is recording a very dark, or potentially black video. The test runs for each camera once a minute, it counts the number of pixels with intensity values less than 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 57 Image Detection page



Enabling Image Detection

Before Image Detection can be enabled you must enable the Video 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 using the Reports feature. In the VideoEdge client you can view video loss alerts via the Event Viewer.

Procedure 178 Enabling Image Detection

1 Click the **Advanced** menu.
2 Click **Image Detection**.
3 To enable Video Loss Detection, click the **Enabled** option button.
4 To enable Dark Image Detection, click the **Enabled** option button.
5 Use the **Darkness Threshold** slider to select the Darkness Threshold value.
6 Click the **Save** icon.

Enabling or disabling 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 179 Enabling or disabling Video Loss Detection

1 Click the **Advanced** menu.
2 Click **Image Detection**.
3 Click the **Enabled** option button to enable Video Loss Detection, or click the **Disabled** option button to disable Video Loss Detection
4 Click the **Save** icon.

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 set up in the NVR to send different types of notifications to selected email addresses.

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. Contact your IT administrator for details.

The following table describes the different elements of the Email Alerts list summary table.

Table 45 Email Alerts list summary table

Field	Description
Alert Category	Displays the name of the alert type.
Recipient List	Displays any recipient email addresses associated with the alert.
Minimum Repetition Interval	The minimum time (in seconds) between sending repeat alert emails.
Return To Normal Interval	The time to wait before sending out the "return to normal" email. The alert itself may already have cleared.
Enabled	Displays **Yes** if the alert is enabled.
Edit	Select the edit icon to edit the alert settings.
Test	Select the **Test** button to send a test alert email to the assigned recipients.

Configuring the Domain Name and Default Gateway

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.

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 Google cannot be guaranteed because those ISPs have their own restrictions that may interfere.

Procedure 180 Configuring the Domain Name and Default Gateway

1 Click the **Network** menu.
2 Click **General**.
3 Enter the domain name in the **Domain Name** field.
4 Enter the default gateway in the **Default Gateway** field.
5 Click the **Save** icon.

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.

Configuring the Outbound Mail server

To use Email Alerts, you must enter the outbound mail server's IP address or hostname. A primary and secondary outbound mail server are available. You can also configure the following settings:

- **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.

Procedure 181 Configuring the Outbound Mail server

1 Click the **Advanced** menu.
2 Click **Email Alerts**.
3 Click the **Edit** icon next to the **Primary Outbound mail server** field.
4 Enter the IP address or hostname in the **Primary Outbound mail server** 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** button.

Note:
If you select SSL, you must select the server TCP port from the **Server TCP port** list.

7 (Optional) Select the **Custom sender** checkbox.
The Sender email address field displays.
  a Enter an **email address** in the field.
8 Click the **Save** icon.

Figure 58 Alert categories

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.
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.

Alert Category	Description
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 Analytics	Generated by video analytics alerts.

Building the Recipient list

The recipient list is made up of email addresses which will receive email alerts. The alerts that each address receives is defined by the alert category associated with that address, and whether or not that category has been enabled.

Procedure 182 Building the Recipient list

1. Click the **Advanced** menu.
2. Click **Email Alerts**.
3. Click the **Add** icon.
   The Add/Update Alert Recipient pop up displays.
4. Click **New Recipient Email Address**.
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** list.
6. Select the **Alert Categories** using the checkboxes.
7. Click the **Save** icon.
   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. To send a test email to a recipient list, select the alert you want to test, and click **Test**. After you configure the email recipients, you must enable alerts.

Enabling and disabling Email Alerts

After recipient addresses have been entered and alert categories have been assigned, you can configure which email alerts should be enabled for each recipient.

Procedure 183 Enabling and disabling Email Alerts

1 Click the **Advanced** menu.
2 Click **Email Alerts**.
3 Select the checkbox for each alert you want to enable from the **Alert Category** list.
4 Click the **Enable Alert** icon or the **Disable Alert** icon, as required.

Enabling or disabling Email Alerts for a camera

You can enable or disable Email Alerts for a specific camera. By disabling email alerts, you can suppress email alerts from cameras which are known to be malfunctioning.

Caution

Disabling email alerts for a camera will disable the camera's ability to stream live video.

You cannot modify settings like Password Group or PTZ when the camera is disabled.

Procedure 184 Enabling or disabling Email Alerts for a camera

1 Click the **Devices** menu.
2 Click **List**.
3 Click the **Setup** icon of the camera you want to re-enable email alerts.
The Function & Streams page opens.
4 Click the **General** tab.
5 Click Video Streaming **Enabled** to enable email alerts for the camera, or click Video Streaming **Disabled** to disable email alerts for the camera.
6 Click the **Save** icon.

Procedure 185 Enabling or disabling Email Alerts for a camera

1 Click the **Devices** icon.
2 Click **List**.
3 Click the **Setup** icon in the camera record of the camera you want to re-enable email alerts.
The Function & Streams page opens.
4 Click the **General** tab.
5 Click Video Streaming **Enabled** to enable email alerts for the camera, or click Video Streaming **Disabled** to disable email alerts for the camera.
6 Click the **Save** icon.

Removing an address from the Recipient list

You can remove recipient addresses from each alert category.

Procedure 186 Remove an address from the Recipient list

1 Click the **Advanced** menu.
2 Click **Email Alerts**.
3 Click the **Edit** icon of the Alert Category you want to remove a recipient's address from.
4 Select the checkbox next to the address you want to remove.
5 Click the **Save** icon.
6 Click **OK**.

Blocking an Email Alert category

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 187 Blocking an Email Alert category

1 Click the **Advanced** menu.
2 Click **Email Alerts**.
3 Click the **Email Blocks** tab.
4 Click the **Add New Email Block** icon.
5 Select the alert category you want to block from the **Category** list.
6 Select the camera from the **Camera** list.
7 Click the **Save** icon.

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.

When you select the Alerts Log tab, you may have to enter your username and password to view the logs. You can click **Clear Logs** to delete the email alert logs.

Procedure 188 Displaying the Email Alerts Log

1 Click the **Advanced** menu.
2 Click **Email Alerts**.
3 Click the **Alert Logs** tab.

Clearing the Alert Logs Page

All email alerts can be cleared from the Alert Logs page.

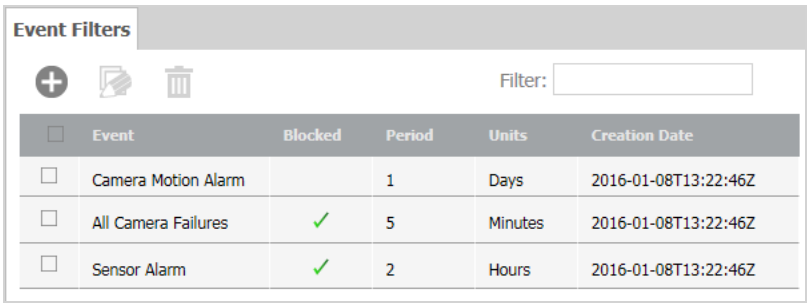
Procedure 189 Clearing the Alert Logs Page

1 Click the **Advanced** menu.
2 Click **Email Alerts**.
3 Click the **Alert Logs** tab.
4 Click **Clear Logs**.

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. You can edit or delete an Event Filter as required.

Figure 59 Event Filters page



Procedure 190 Creating an Event Filter

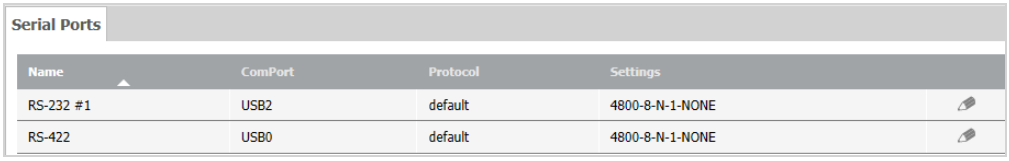
1 Click the **Advanced** menu.
2 Click **Event Filters**.
3 Click the **Add** icon.
The Add Filter menu opens.

4 Select an event from the **Event Names** list.
5 Select the camera from the **Camera** list.
6 Select the **Blocked** checkbox to permanently enable the event filter, or configure the filter period.
7 (If using **Period** field only) If manually setting the event filter period, complete the following steps:
   a Enter a value in the **Period** field.
   b Select **Seconds**, **Minutes**, **Hours**, **Days**, or **Weeks** from the **Unit** list.
8 Click the **Save** icon.

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. You can view the serial protocols on the Serial Protocols page of the System Menu

Figure 60 Serial Ports page



Procedure 191 Configuring the Serial Ports

1 Click the **Advanced** menu.
2 Click **Serial Ports**.
3 Click the **Edit** icon next to the port you wish to configure.
The Port Settings popup displays.
4 Select the **Protocol** from the list.
5 Select the **Baud Rate** from the list.
6 Enter the **Data Bits** in the field.
7 Select the **Parity** from the list.
8 Enter the **Stop Bits** in the field.
9 Select the **Flow Control** from the list.
10 Click the **Save** icon.

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 192 Setting the PTZ Address

1 Click the **Devices** menu.
2 Click **List**.

3 Click the **Setup** icon 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 list.
6 Enter the camera address number in the **PTZ Address** field.
7 Click the **Save** icon.

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.

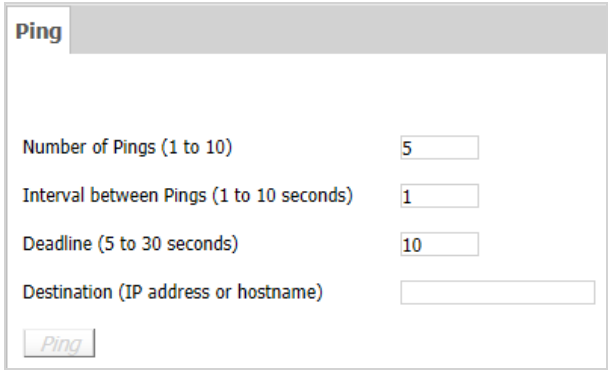
Procedure 193 Configuring Optima/Optima LT bespoke settings when using RS-422

1 Click the **Devices** menu.
2 Click **List**.
3 Click the **Setup** icon of the analog camera you want to configure PTZ settings for.
The Function & Streams page opens.
4 Click the **PTZ** tab.
5 Select the **PTZ Port** in use from the list.
6 Enter the camera address number in the **PTZ Address** field.
7 (For Optima LT cameras) Select the **Simplex - Optima LT** checkbox.
8 Clear the **Enable Camera Menu** checkbox.
9 Click the **Save** icon.

Ping

From the Ping page, you can verify the operation of, and confirm communication with, cameras and devices on the NVR's networks.

Figure 61 Ping page



Procedure 194 Pinging other devices

1 Click the **Advanced** menu.
2 Click **Ping**.

3 Enter the **Number of Pings** to send to the selected device.
4 Enter the **Interval between Pings**.
5 Enter the **Deadline** the NVR is to wait for a response.
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 are displayed below the Ping button.

Connected Clients

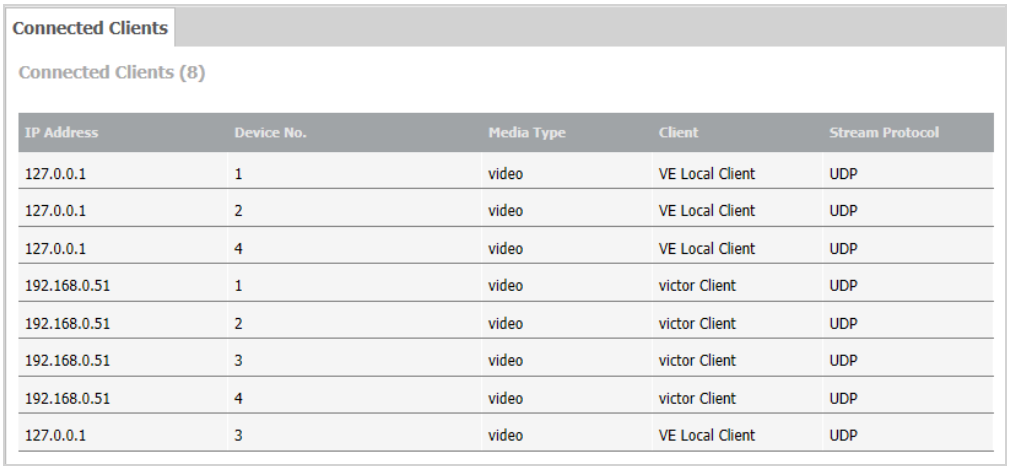
You can view the clients currently connected to the NVR using the Connected Clients sub menu. The NVR will only register a client as connected if it is actively receiving a video/audio stream from the NVR.

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.

You can view the Connected Clients page by going to **Advanced > Connected Clients**.

Figure 62 Connected Clients page



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 195 Enabling a SIP proxy

1 Click the **Advanced** menu.
2 Click **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 Click the **Save** icon.

Equivalent Model

When an unsupported camera model is added to VideoEdge, some device features may not be immediately available. For manufacturers that do not support the auto-discovery of a device's features, you can use the Equivalent Model feature to configure VideoEdge to treat the unsupported model as a similar supported model from the same manufacturer. The Equivalent Model feature is supported for the following manufacturers: Arecont Vision, Bosch, FLIR, Hanwha/Samsung, Panasonic, Sony, and Vivotek.

For the Equivalent Model feature to function correctly, the unsupported model must communicate with the NVR in the same way the unsupported model does. New iterations of an existing camera model often do this.

The unsupported model and the supported model should share a feature set, as features available on the unsupported model that are not on the supported model will not be accessible.

Note:
Configuring Equivalent Model does not guarantee that all features of the unsupported model will be supported.

Configuring Equivalent Model for a device

Configure the Equivalent Model before adding the device to VideoEdge. If you have already added the device, remove and re-add it, or restart NVR Services. Restarting NVR Services will interrupt ongoing recordings.

Procedure 196 Configuring Equivalent Model for a device

1 Select **Advanced** from the main menu.
2 Select **Equivalent Model**.
3 Click the **Add new Equivalent Model** icon.
4 Select a manufacturer from the **Manufacturer** list.
5 Enter the model name of the unsupported device in the **New Model** field.
6 Select a model from the **Equivalent Model** list.
7 Click the **Save** icon.

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)

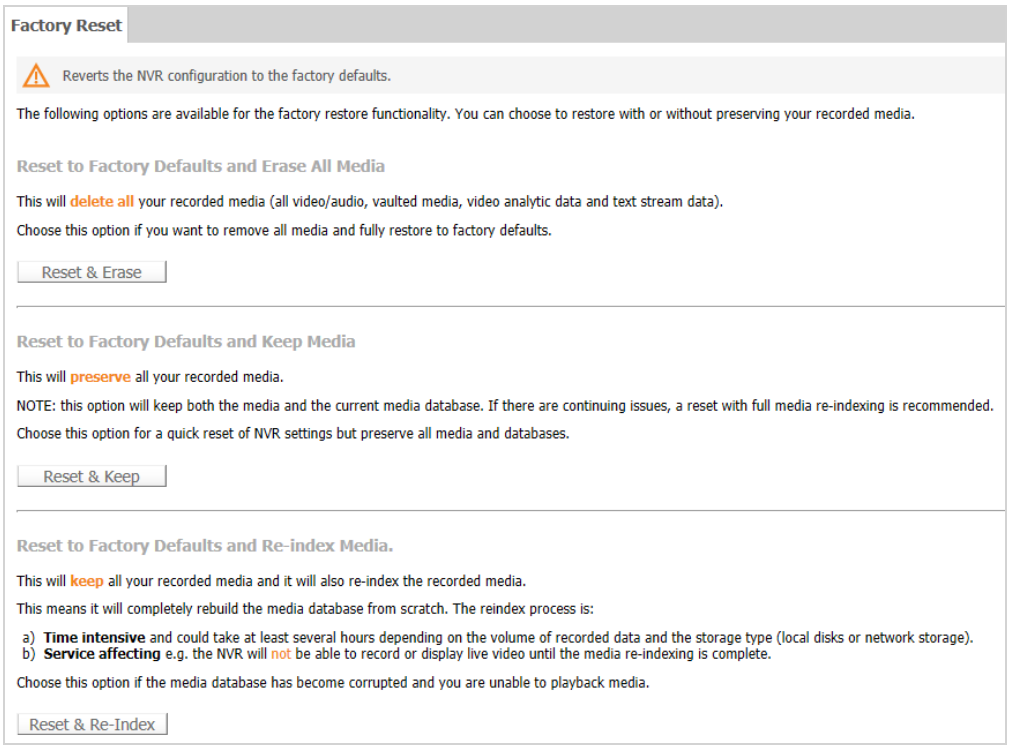
The Reset Factory Defaults functionality allows you to revert several of the NVR's characteristics back to their default settings. It will however not implement any changes to the server's Linux Operating System. During a Reset Factory Defaults function the recorder will not be able to record or display live video until the process is complete.

Once the Reset Factory Defaults is complete you must 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 the following options for keeping or deleting the Saved Media files:
    - **Reset to Factory Defaults AND Erase All Media** - This will delete all your recorded media, that is, 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. 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. 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. The NVR will not be able to record or display live video until the media re-indexing is complete.

Figure 63 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, and the System Settings. The NVR License will also not be affected.

Procedure 197 Reset to Factory Defaults

1 Click the **Advanced** menu.
2 Click **Reset Factory Defaults**.
3 Click **Reset & Erase**, **Reset & Keep**, or **Reset & Re-index**.
4 Click **Yes** to continue when the warning message displays.

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.

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**.

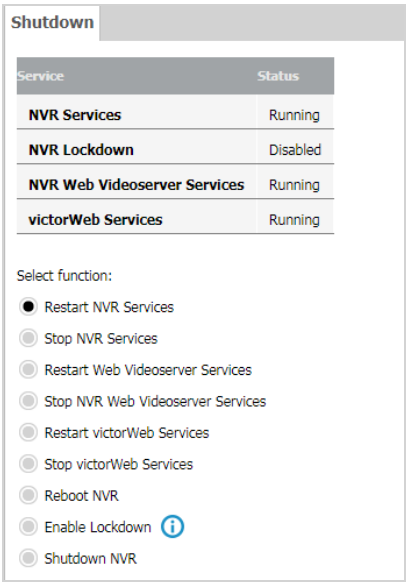
Note:
If your camera network requires the use of the Linux default gateway, resetting may affect your camera network.

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.

Shutdown

From the Shutdown page, you can stop or restart the NVR, NVR Services, Web Videoserver Services, and victor Web Services, and also enable or disable Lockdown mode for the NVR. Click the required function in the Select function area, and then click the **Save** icon.

Figure 64 Shutdown page



NVR Services and victor

victor operators can access camera footage while NVR services are stopped, and view live steams from multicast cameras while the VideoEdge is offline. victor operators can access recorded camera footage for search retrieve operations, and for clip exports.

Restarting NVR Services

This function 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.

Stopping NVR Services

NVR Services can be stopped permanently. Use the **Restart NVR Services** option to restart the services

Note:
It is highly recommended that you stop NVR Services before configuring storage.

Restarting 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.

Stopping 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.

Restarting victorWeb Services

By restarting victorWeb Services, you restart the Node and Health Server. Use this function to restart these servers if you experience victor Web issues, without affecting the NVR.

Stopping victorWeb Services

victorWeb Services can be stopped permanently. Choosing this option prohibits all access to victor Web.

Rebooting the NVR

Choosing this option will reboot the NVR.

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.

The VideoEdge remains in Lockdown mode until you disable it. If Lockdown mode is enabled, the **Disable Lockdown** button displays instead. Click this button, and then click the **Save** icon to disable Lockdown mode.

During Lockdown, a notification banner appears in the VideoEdge Administration interface.

Procedure 198 Enabling or disabling Lockdown mode

1 Select **Advanced**.
2 Select **Shutdown**.
3 Click **Enable Lockdown**.

Note:
If Lockdown is already enabled, the **Disable Lockdown** option button displays instead.

Or
Click **Disable Lockdown**.
4 Click the **Save** icon.

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.

Shutting down the NVR

Use this function to shut down the NVR. To restart the NVR after it has been shut down, you must turn it on manually at the server.

Monitor Outputs

Use the Monitor Outputs menu to create and configure monitor output views and tours. 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. The Monitor Outputs menu contains the following submenus:

- **Monitor Output Setup** - View saved monitor output views and assign secondary ADTT16E controllers.
- **Monitor Output Tours** - Create and configure monitor tours.
- **Monitor Output Views** - Create and configure monitor output views.

Monitor Outputs icons table

Table 46 Monitor Outputs icons

Icon	Name	Function
	**Save**	Save
	**Create Tour**, **Create View**	Create new tour; create new monitor view
	Right Arrow	Move selected camera to a tour group.
	Left Arrow	Remove selected camera from a tour group.
	**Cancel**	Cancel
	**Remove Tour**, **Remove View**	Remove selected tour; remove selected view
	**Edit**	Edit

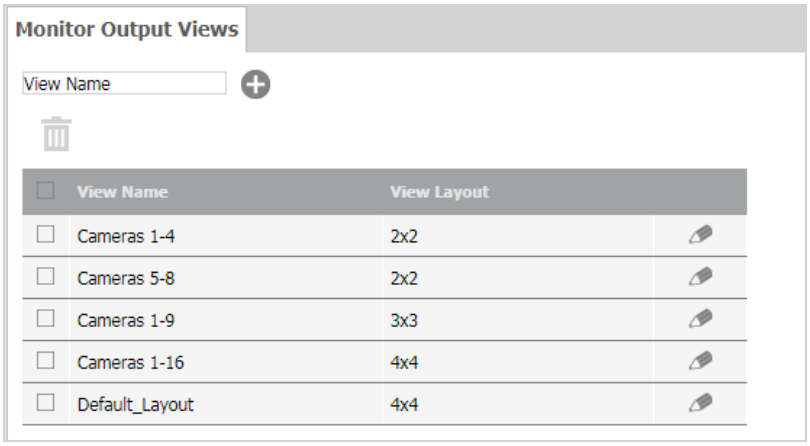
Monitor Output Views

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. You can edit or delete created monitor output views as required.

The following NVR view layouts are available: 1x1, 2x2, 3x3, 4x4, Guard, 12+1, 2+8, 1x2, 2+3, 2x1, and 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.

Figure 65 Monitor Output Views



Procedure 199 Viewing a saved Monitor Output View

1 Click the **Monitor Outputs** menu.
2 Click **Monitor Output Setup**.
3 In the Monitor Outputs table select the monitor you want the view to be displayed on from the required **Monitor** list.
4 Click **Launch** in the monitor output view record you want to view.
The selected monitor view is displayed on the monitor selected.

Procedure 200 Manually using a Monitor Output View

1 Click the **Monitor Outputs** menu.
2 Click **Monitor Output Setup**.
3 Select the required layout from the **Layout** list.
4 Click the **Edit** icon.
The Active Layout Editor opens.
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**, or click **Save As View**, enter a **View Name**, and click the **Save** icon.

Procedure 201 Saving a Monitor Output View

1 Click the **Monitor Outputs** menu.
2 Click **Monitor Output Views**.
3 Enter a **View Name**.
4 Click the **Create View** icon.
The Active Layout Editor page opens.
5 Select a layout for the preset from the **Used layout** list.
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**.

Assigning secondary ADTT16E keyboard control

You can assign secondary keyboard control when you have a secondary ADTT16E configured.

Procedure 202 Assigning secondary ADTT16E keyboard control

1. Click the **Monitor Outputs** menu.
2. Click **Monitor Output Setup**.
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 the **Save** icon.

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 203 Creating a Monitor Output Tour

1. Click the **Monitor Outputs** menu.
2. Click **Monitor Output Tours**.
3. Enter a **Tour Name**.
4. Click the **Create Tour** icon.
   A configuration window opens.
5. Select a camera from the **Available Cameras** list. Click the **Right Arrow** icon 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.
   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.
8. Click the **Save** icon.

Appendix A - VideoEdge Troubleshooting

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.

Closing 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 204 Closing the VideoEdge Client

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. Click **Close**.

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 205 Changing the Monitor Resolution

1. Click **Applications** on the NVR Desktop.
2. Click **System Tools**.
3. Click **Settings**.
4. Click **Displays**.
5. On the Displays menu, select your monitor.
6. Select a resolution from the **Resolution** list.
7. Click **Apply**.

RDP Remote Desktop

The following procedures allow you to log on and log off RDP remote desktop.

Procedure 206 Logging in to RDP Remote Desktop

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.
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**.

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 207 Logging Out of RDP Remote Desktop

1 Click the **Power** icon.
A popup window opens.

2 Expand the Log Out menu and Click **Log Out**.
A Logout popup displays.

3 Click **Log Out**.
Remote Desktop window closes.

4 Click the **Close Window** icon to close the Remote Desktop Connection application.

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, and so on.

One primary partition per drive can be assigned as an extended partition containing as many logical partitions as you require.

Table 47 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 208 Configuring System Partitions on a Previously Configured Device

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.

Editing Media Partitions

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 209 Editing Media Partitions

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 **Arbitraryoption** 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.

VideoEdge NVR System Disk Recovery

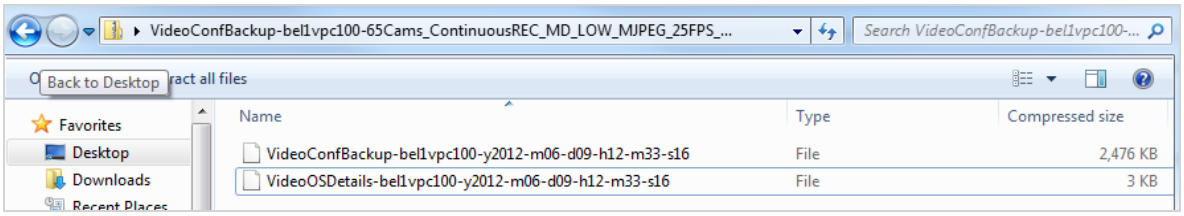
Should the NVR's system disk fail or the system disk becomes corrupt, the following procedure should be used for its recovery. You will need the following items:

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 66 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 210 VideoEdge NVR System Disk Recovery

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. See 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-xxxxxxxxxx.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.

Editing Failover heartbeat parameters

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 211 Editing Failover heartbeat parameters

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.

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 the VideoEdge NVR 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 212 Enabling the VideoEdge NVR as an NTP Server

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]

Synchronizing the time between VideoEdge devices and a VideoEdge NTP server

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 213 Synchronizing the time between VideoEdge devices and a VideoEdge NTP server

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.

Appendix B - SmartStream

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 framerate 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 C - Hardware Configurations

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.

VideoEdge Micro NVR

Figure 67 VideoEdge Micro NVR Front

Figure 68 VideoEdge Micro NVR Rear

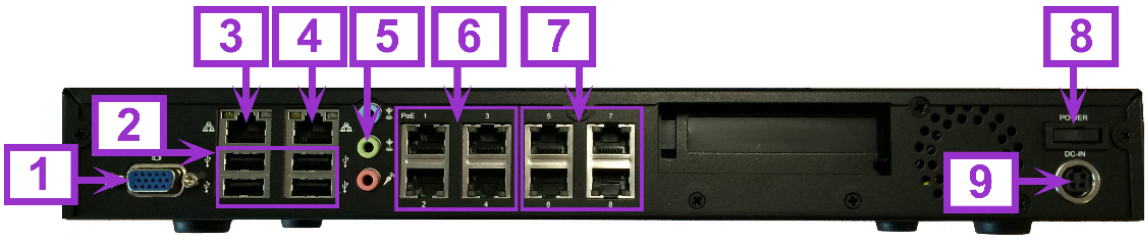


Table 48 VideoEdge Micro NVR Configuration

Number	Description
1	Video Port (VGA Port)
2	USB 2.0 Port (x4)
3	1 GbE Network Port (eth0 LAN1)
4	1 GbE Network Port (eth1 LAN2)
5	3.5 mm Line Out Port (speaker/headphones)
6	1 GbE Network Ports (4x PoE eth2 for cameras 1 ~ 4)
7	1 GbE Network Ports (4x PoE eth2 for cameras 5 ~ 8)
8	Power Button
9	Power Entry Connector

VideoEdge Desktop NVR

Figure 69 VideoEdge Desktop NVR Front

Figure 70 VideoEdge Desktop NVR Rear

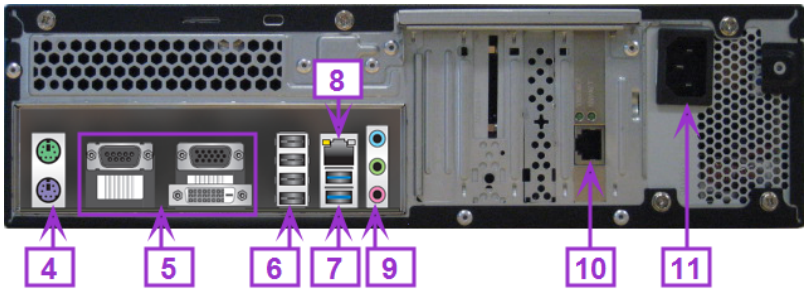


Table 49 VideoEdge Desktop NVR Configuration

Number	Description
1	Hard drive activity LED
2	Power Button/LED (Pinhole)
3	USB 2.0 Ports (x2) and USB 3.0 Ports (x2) (Under front flap)
4	PS/2 Ports
5	Video Ports (VGA or DVI-D; Serial not supported)
6	USB 2.0 Ports (x4)
7	USB 3.0 Ports (x2)
8	1 GbE Network Port (eth0 LAN1)
9	Audio Ports (Line In, Line Out, Microphone) **Note:** Line In and Mic not supported
10	1 GbE Network Port (eth1 LAN2)
11	Power Entry Connector (100~240VAC)

VideoEdge 1U NVR

Figure 71 VideoEdge 1U NVR Front

Figure 72 VideoEdge 1U NVR Front (Panel removed)

Figure 73 VideoEdge 1U NVR Rear

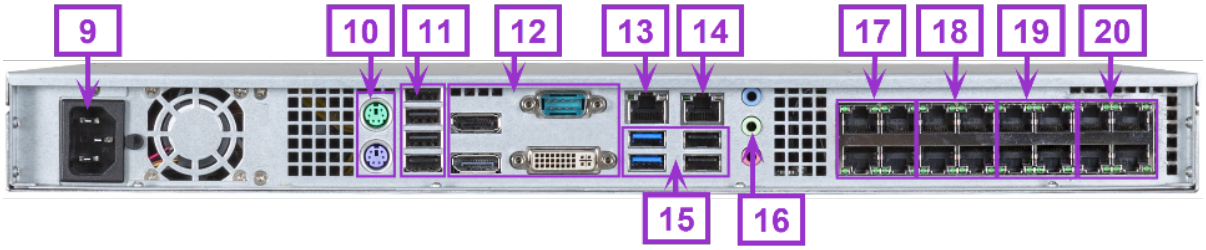


Table 50 VideoEdge 1U NVR Configuration

Number	Description
1	Bezel (removable)
2	Bezel Lock (Key located behind bezel)
3	USB 2.0 Port
4	Factory Reset Button
5	Power Indicator LEDs
6	Power Button
7	PoE Status Indicator LEDs
8	Drives (removable)
9	Power Connector (100 ~ 240VAC)
10	PS/2 Ports
11	USB Ports (4 x 2.0)
12	Video Ports (DisplayPort x2, Serial Port, DVI-I Port)
13	1GbE Network Port (eth0 LAN1)

Number	Description
14	1GbE Network Port (eth1 LAN2)
15	USB 3.0 Ports (x2) and USB 2.0 Ports (x2)
16	3.5 mm Line Out Port (speaker/headphones)
17	10mb/100mb PoE Network Ports (4x PoE eth2 for cameras 1 ~ 4)
18	10mb/100mb PoE Network Ports (4x PoE eth2 for cameras 5 ~ 8)
19	10mb/100mb PoE Network Ports (4x PoE eth2 for cameras 9 ~ 12)
20	10mb/100mb PoE Network Ports (4x PoE eth2 for cameras 13 ~ 16)

VideoEdge 2U Hybrid NVR

Figure 74 VideoEdge 2U Hybrid NVR Front

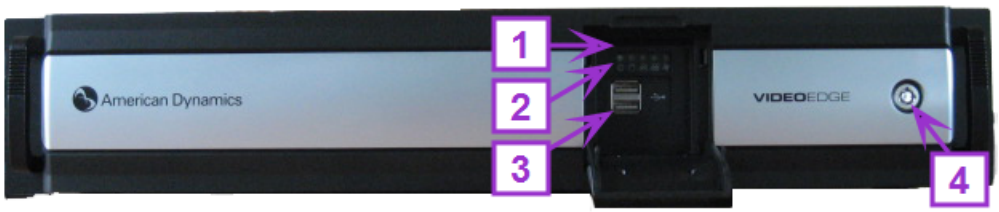


Figure 75 VideoEdge 2U Hybrid NVR Rear

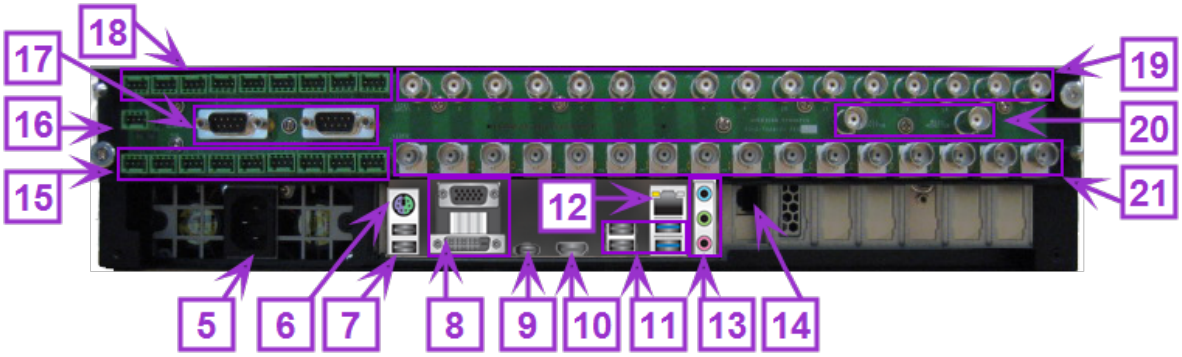


Table 51 VideoEdge 2U Hybrid NVR Configuration

Number	Description
1	Factory Reset Button (Under front flap)
2	Power Button (Under front flap)
3	USB 3.0 Ports (x2, under front flap)
4	Bezel Lock (Key located behind bezel)
5	Power Entry Connector (100~240VAC)
6	PS/2 Combo Port
7	USB 2.0 Ports (x2)

Number	Description
8	Video Ports (VGA, or DVI-D)
9	USB 5Gb/s Type C Port (Not supported)
10	HDMI Port (Not supported)
11	USB 2.0 Ports (x2) and USB 3.0 Ports (x2)
12	1 GbE Network Port (eth0 LAN1)
13	Audio Ports (Line In, Line Out, Microphone) **Note:** Line In and Mic not supported
14	1 GbE Network Port (eth1 LAN2)
15	Alarm In (x9), Alarm Out (x16) and Form C Relay
16	RS422 Port
17	Serial Port
18	Alarm In (x9), Audio In (x16) and Audio Out
19	BNC Video (Analog Camera Inputs x16)
20	BNC Video (Analog Monitor Outputs x 2)
21	BNC Video (Loop Through/Camera Out x 16)

VideoEdge 2U NVR

Figure 76 VideoEdge 2U NVR Front

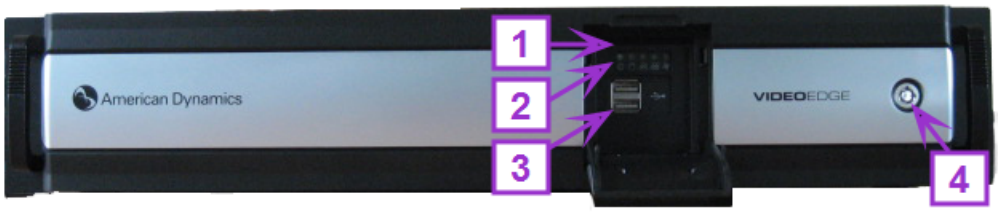


Figure 77 VideoEdge 2U NVR Rear

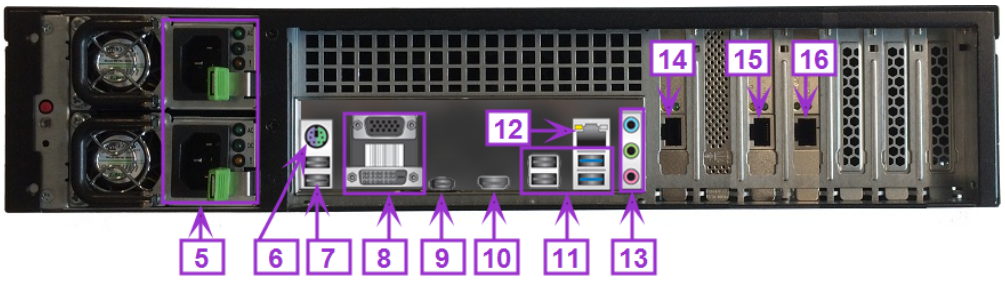


Table 52 VideoEdge 2U NVR Configuration

Number	Description
1	Factory Reset Button (Under front flap)
2	Power Button (Under front flap)
3	USB 3.0 Ports (x2, under front flap)
4	Bezel Lock (Key located behind bezel)
5	Power Entry Connector (x2, 100~240VAC)
6	PS/2 Combo Port
7	USB 2.0 Ports (x2)
8	Video Ports (VGA, or DVI-D)
9	USB 5Gb/s Type C Port (Not supported)
10	HDMI Port (Not supported)
11	USB 2.0 Ports (x2) and USB 3.0 Ports (x2)
12	1 GbE Network Port (eth0 LAN1)
13	Audio Ports (Line In, Line Out, Microphone) **Note:** Line In and Mic not supported
14	1 GbE Network Port (eth1 LAN2)
15	1 GbE Network Port (eth2 LAN3)
16	1 GbE Network Port (eth3 LAN4)

VideoEdge Rack Mount NVR

Figure 78 VideoEdge Rack Mount NVR Front

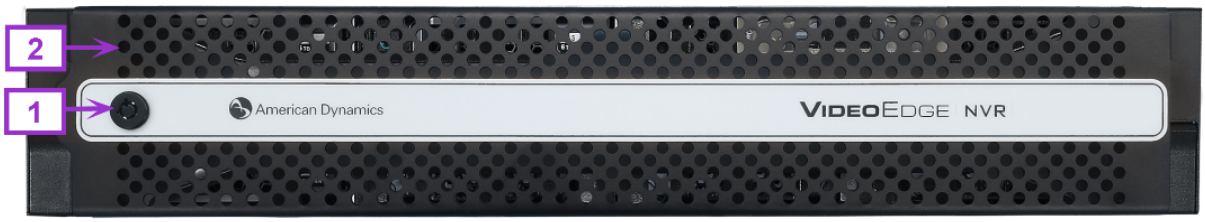


Figure 79 VideoEdge Rack Mount NVR Rear

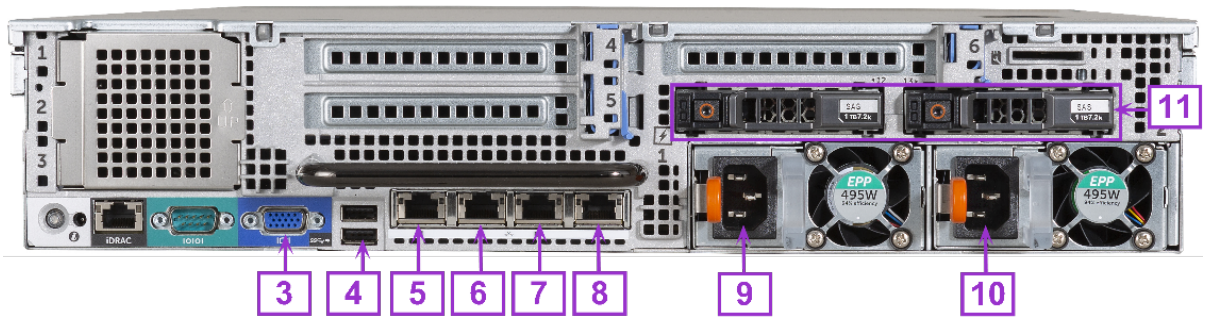


Table 53 VideoEdge Rack Mount NVR Configuration

Number	Description
1	Bezel Lock (Key located behind bezel)
2	Power Button (Behind bezel)
3	VGA Port
4	USB 3.0 Ports (x2)
5	1 GbE Network Port (eth 0 LAN1)
6	1 GbE Network Port (eth1 LAN2)
7	1 GbE Network Port (eth2 LAN3)
8	1 GbE Network Port (eth3 LAN4)
9	Power Entry Connector (100~240VAC)
10	Power Entry Connector (100~240VAC)
11	Hard Drives (2x RAID-1 OS Drives)

VideoEdge 3U Hybrid NVR

Figure 80 VideoEdge 3U Hybrid NVR Front Panel

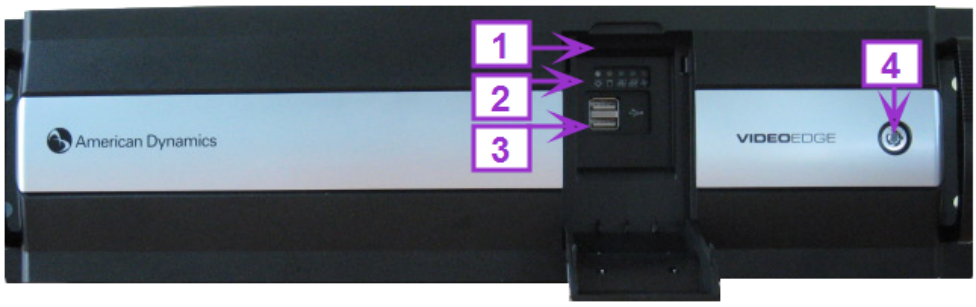


Figure 81 VideoEdge 3U Hybrid NVR Rear Panel

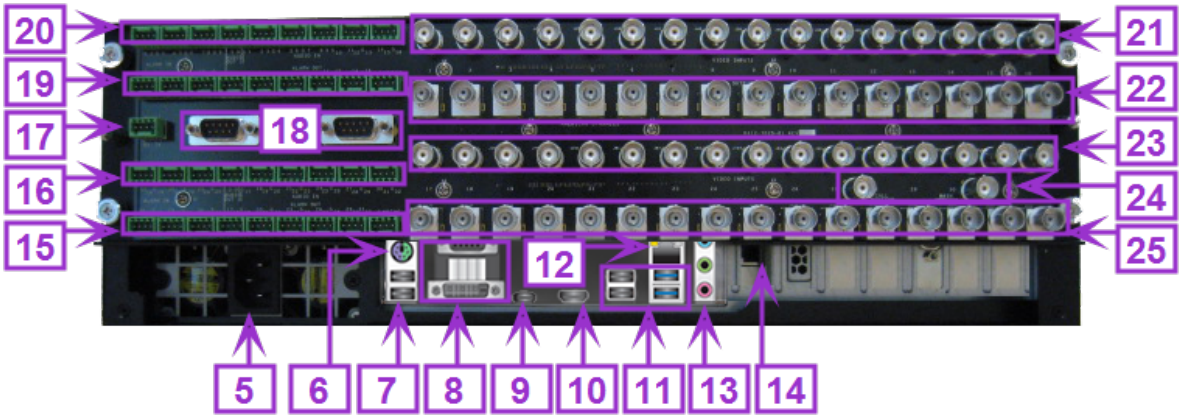


Table 54 VideoEdge 3U Hybrid NVR

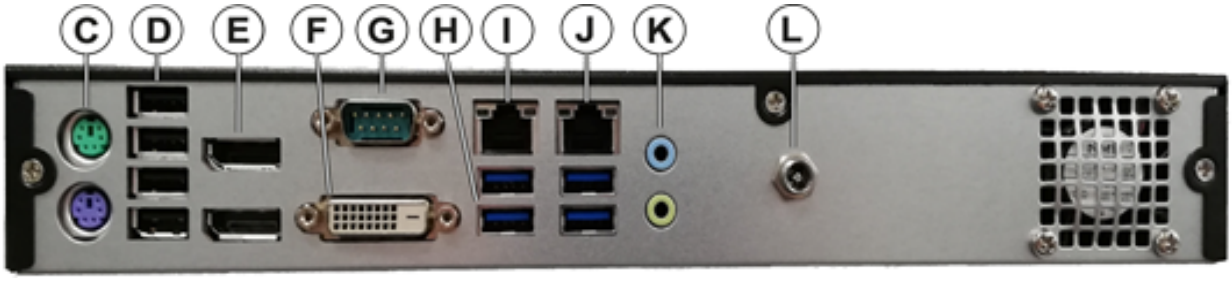
Number	Description
1	Factory Reset Button (Under front flap)
2	Power Button (Under front flap)
3	USB 3.0 Ports (x2, under front flap)
4	Bezel Lock (Key located behind bezel)
5	Power Entry Connector (100~240VAC)
6	PS/2 Combo Port
7	USB 3.0 Ports (x2)
8	Video Ports (VGA, or DVI-D)
9	USB 5Gb/s Type C Port (Not supported)
10	HDMI Port (Not supported)
11	USB 2.0 Ports (x2) and USB 3.0 Ports (x2)
12	1 GbE Network Port (eth0 LAN1)
13	Audio Ports (Line In, Line Out, Microphone) **Note:** Line In and Mic not supported
14	1 GbE Network Port (eth1 LAN2)
15	Alarm In (x9), Alarm Out (x16) and Form C Relay
16	Alarm In (x9), Audio In (x16), and Audio Out
17	RS422 Port
18	Serial Port (x2)
19	Alarm In (x9), Alarm Out (x16) and Form C Relay
20	Alarm In (x9), Audio In (x16), and Audio Out

Number	Description
21	BNC Video (Analog Camera Inputs x 16)
22	BNC Video (Loop Through/Camera Out x 16)
23	BNC Video (Analog Camera Inputs x 16)
24	BNC Video (Analog Monitor Outputs x 2)
25	BNC Video (Loop Through/Camera Out x 16)

VideoEdge Compact Desktop NVR

Figure 82 VideoEdge Compact Desktop NVR front view

Figure 83 VideoEdge Compact Desktop NVR back view



Callout	Description	Callout	Description
A	Reset Button	G	Serial Port
B	Power Button	H	USB 3.0 Ports (x4)
C	PS/2 Ports	I	1GbE Network Port (eth0 LAN1)
D	USB 2.0 Ports (x4)	J	1GbE Network Port (eth1 LAN2)
E	DisplayPorts (x2)	K	Audio Ports (Not supported)
F	DVI-D Port	L	Power Entry Connector (12 V, 10 A DC)

Connector Pin Outs

Table 55 VideoEdge 2U Hybrid Pin Outs

Pin No.	Assignment	Pin No.	Assignment
Alarm In		**Alarm Out**	
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
Audio Out Pin Outs			
S	Signal Out	G	Ground
Audio In Pin Outs			
G	Ground	9	Input 9
1	Input 1	G	Ground
2	Input 2	10	Input 10
3	Input 3	11	Input 11

Pin No.	Assignment	Pin No.	Assignment
G	Ground	12	Input 12
4	Input 4	G	Ground
5	Input 5	13	Input 13
6	Input 6	14	Input 14
G	Ground	15	Input 15
7	Input 7	G	Ground
8	Input 8	16	Input 16
Form C Relay Pin Outs			
G	Ground	C	Common
NO	Normally Open	NC	Normally Closed
RS422 Pin Outs			
RX +	Receive +	TX -	Transmit -
RX -	Receive -	TX +	Transmit +

Table 56 VideoEdge 3U Hybrid Pin Outs

Pin No.	Assignment	Pin No.	Assignment
Alarm In		**Alarm Out**	
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

Pin No.	Assignment	Pin No.	Assignment
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
G	Ground	N/A	N/A
36	Input 36	N/A	N/A

Pin No.	Assignment	Pin No.	Assignment
Audio Out Pin Outs			
S	Signal Out	G	Ground
Audio In Pin Outs			
G	Ground	9	Input 9
1	Input 1	G	Ground
2	Input 2	10	Input 10
3	Input 3	11	Input 11
G	Ground	12	Input 12
4	Input 4	G	Ground
5	Input 5	13	Input 13
6	Input 6	14	Input 14
G	Ground	15	Input 15
7	Input 7	G	Ground
8	Input 8	16	Input 16
Alarm Out Pin Outs 2			
S	Signal Out	G	Ground
Audio In Pin Outs 2			
G	Ground	25	Input 25
17	Input 17	G	Ground
18	Input 18	26	Input 26
19	Input 19	27	Input 27
G	Ground	28	Input 28
20	Input 20	G	Ground
21	Input 21	29	Input 29
22	Input 22	30	Input 30
G	Ground	31	Input 31
23	Input 23	G	Ground
24	Input 24	32	Input 32
Form C Relay Pin Outs			
G	Ground	C	Common
NO	Normally Open	NC	Normally Closed
RS422 Pin Outs			
RX +	Receive +	TX -	Transmit -
RX -	Receive -	TX +	Transmit +

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 OR ITS AFFILIATES AS APPLICABLE FOR THE PARTICULAR SOFTWARE (“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. Compliance with Law. Certain functions of the Software may require compliance by You with local, national and international laws and regulations. You are solely responsible for compliance with all applicable laws and regulations relating to your use of this Software and those functions, including but not limited to those laws and regulations pertaining to personal data protection, privacy and security, any laws relating to the collection and sharing of facial recognition with third parties, or any laws requiring notice or consent of persons with respect to Your use of facial recognition.

d. 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.

e. 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.

f. 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.

g. 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.

h. Trademarks. This EULA does not grant you any rights in connection with any trademarks or service marks of Tyco, its affiliates or its suppliers.

i. 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.

j. 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.

k. 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.

l. 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.

m. 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.

n. 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.

o. 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.

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. SPECIAL PROVISIONS APPLICABLE TO SALES TO U.S. GOVERNMENT END USERS. The following provisions apply to U.S. Government end users only..

a. The Software is Commercial Computer Software provided with "restricted rights" under Federal Acquisition Regulations ("FARs") 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.

b. Notwithstanding anything in this EULA or the Preamble to the contrary, acceptance of this EULA is governed by any applicable federal laws, FARs, including without limitation, FAR 1.601(a) and 43.102.

c. "You" within this EULA shall mean the Agency itself and shall not apply to, nor bind (i) the individual(s) who utilize the Tyco Site or Services on the Agency's behalf, or (ii) any individual users who happen to be employed by, or otherwise associated with, the Agency. Tyco will look solely to Agency to enforce any violation or breach of the EULA by such individuals, subject to federal law.

d. Notwithstanding anything in this EULA to the contrary, any changes in the terms and conditions of this EULA may be made only by written agreement of the parties in accordance with any applicable federal laws and FARs, including without limitation FAR 52.212-4(c).

e. Notwithstanding anything in this EULA to the contrary, termination of this EULA shall be subject to any applicable federal laws and FARs, including without limitation FAR 52.233-1 Disputes.

f. Nothing in this EULA is intended to alter, impair or limit the U.S. Government's rights or remedies under any third party agreement, GSA Schedule contract, FARs, any Federal Fraud Statute, or the Contract Disputes Act, 41 USC 7101-7109.

g. This EULA does not alter, impair or limit any warranties provided by any party to a GSA Schedule contract (including without limitation GSA Schedule 70) under FAR 52.212-4(o). In the event of a breach of any warranty by a party to a GSA Schedule contract, the U.S. Government reserves all rights and remedies under the GSA schedule contract the Federal Acquisition Regulations and the Contract Disputes Act, 41 USC 7101-7109.

h. This EULA shall not impair the U.S. Government's right to recover for fraud or crimes arising out of or related to this EULA under any federal fraud statute, including the False Claims Act, 31 USC 3729-3733. Furthermore, this clause shall not impair nor prejudice the U.S. Government's right to seek from any party to a GSA Schedule contract the express remedies provided in the GSA Schedule contract (e.g., clause 552.238-75 – Price Reductions, clause 52.212-4(h) – Patent Indemnification, and GSAR 552-215-72 – Price Adjustment – Failure to Provide Accurate Information).

i. This EULA is governed by the laws of the United States only. Any dispute arising out of this EULA must be resolved in accordance with the Contract Disputes Act, 41USC 7101-7109 or the Federal Tort Claims Act.

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. End User is solely responsible for (a) ensuring full compliance with the Installation Guide for the applicable Software; and (b) the establishment, operation, maintenance, access, security and other aspects of its computer network, as well as network performance and compatibility issues. 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)in exchange for return of the software, 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 GREATER OF USD$5.00 OR THE AMOUNT OF FEES YOU PAID TO TYCO OR ITS RESELLER FOR THE SOFTWARE THAT GIVES RISE TO SUCH LIABILITY. BECAUSE AND TO THE EXTENT THAT SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSIONS OR LIMITATIONS OF LIABILITY ABOVE, THESE MAY NOT APPLY TO YOU.

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.