American Dynamics

VideoEdge NVR Installation and User Guide

www.americandynamics.net

A16381YMGC Rev A

6.1.1

Johnson Controls

Contents

Preface

Notice

The information in this manual was correct when published. The manufacturer reserves the right to revise and improve its products. All specifications are 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 can contact American Dynamics at (800) 507-6268 or (561) 912-6259, or at http://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 can 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 can be obtained from MPEG LA, LLC. See https://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 can be obtained from MPEG LA, LLC. See https://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. 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: ICES

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

European Union: EMC Compliance

⚠ CAUTION
Can cause radio interference.

Only the following connections are expected to be limited to < 3 m cables:This is a Class A product. In a domestic environment, this product can cause radio interference in which case the user may be required to take adequate measures.

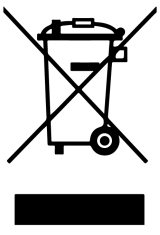
- USB

Only the following cables are expected to be shielded:

- Video BNC cables
- Monitor video cables

Recycling and disposal of equipment

Figure 1: WEEE symbol



This is a Class A product. In a domestic environment,This symbol means the product is classified as waste Electrical and Electronic equipment under the WEEE directive (2012/19/EU). It should not be placed in the normal waste stream and should be separately collected for specific recycling as WEEE.

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

Power supply and network port information

This product is intended to be supplied by a UL listed (Certificate) power supply, output rated 54Vdc, 3.33A minimum, TMA 40 degree C minimum, and altitude 5000 M. If you need further assistance, please contact American Dynamics, div. of Sensormatic Electronics LLC or visit us at https://americandynamics.net/.

The VideoEdge Micro NVR models provide 8 IP video channels with onboard PoE switches with speeds of 10/100Mbps, 802.3af/at compliance with a total 120W. Each channel is rated at 15 W Max.

The equipment power supply cord must be connected to a socket-outlet with earthing connection.

The power rating for the VideoEdge Micro NVR is a total of 120 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.

ⓘ **Note:** The VideoEdge Micro NVR can be used as either a desktop unit or rack mounted with use of a rack tray. Connect ITE to PoE networks without routing to the outside plant.

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.

General safety warnings

- **Circuit overloading:** 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.
- **Power supply:** Use an uninterrupted power supply (UPS) to protect computing systems from power fluctuations that can cause data loss.
- **Earthing:** 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.
- **Indoor use:** This product is for indoor use only.
- **Professional use:** This product is for professional installation, use and service.
- **Air pressure:** This product is only suitable for operation below altitudes or equivalent air pressure as follows:
  - VideoEdge Micro NVR, VideoEdge Desktop NVR, VideoEdge Desktop Hybrid NVR, and VideoEdge 1U NVR: 2,000 m.
  - VideoEdge 2U NVR, VideoEdge 2U Hybrid NVR, VideoEdge 3U Hybrid NVR, and VideoEdge Rack Mount NVR: 3,200 m.
- **Field of view:** 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.

Replacing RTC batteries

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.

Risque d'explosion de la batterie si celle-ci est remplacée par un modèle incorrect.

Les batteries doivent être ises au rebut selon les instructions.

⚠ WARNING

Network Video Recorders are not intent for use by children. This product is not suitable for use in locations where children are likely to be present.

Keep the product away from children.

⚠ WARNING

This product contains a coin battery. If it is swallowed, it can cause severe internal burns in just two hours and can lead to death.

Never open the equipment. For safety reasons, the equipment should be opened only by a qualified, skilled person. Keep new and used batteries away from children. If the battery compartment does not close securely, stop using the product and keep it away from children. Seek immediate medical attention if you think batteries might have been swallowed or placed inside any part of the body.

To replace the battery, complete the following steps:

⚠ CAUTION

Risk of injury.

Take adequate ESD precautions, and wear an ESD strap connected to the chassis of the products.

1. Disconnect the power before you remove the cover. Note that there are hazardous voltages in the PSU module, and while these cannot be touched easily, and are protected, it can be possible to touch live parts with a small tool.
2. Turn off all peripheral devices that connect 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 polarity symbols on the battery.
   - Preferably, use a non-conductive tool to remove the battery, and avoid touching the new battery with fingers.
6. Install the new battery in the connector, observing the correct polarity.
7. Replace the computer cover.

Safety warnings for rack mountable equipment

Elevated operating ambient: If the equipment is installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment can 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).

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.

Mechanical loading: When mounting the equipment, ensure that the mechanical loading is even.

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 over-current protection and supply wiring. Consult the equipment's nameplate ratings when addressing this concern.

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.

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 NVR product range

Table 1: VideoEdge Network Video Recorder (NVR) product range

Product	Description
VideoEdge Micro NVR	Small form factor IP-only VideoEdge, 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

Figure 2: VideoEdge NVR range

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 launches Mozilla Firefox ESR.
- Open the VideoEdge Administration Interface log-in 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 select 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 logon 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

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.

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

victor product range

Table 2: victor product range

victor	Description
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 or client architecture, backed by a victor Application Server using a Microsoft SQL Server back-end.
victor Enterprise	For large and geographically dispersed systems victor and C·CURE 9000 support enterprise deployments for unified control and monitoring across the enterprise.

victor Web

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.

Access victor Web by navigating in a web browser to `xx.xx.xx.xx/victorweb` where `xx.xx.xx.xx` is the IP address of the host.

victor Web requires a license to run.

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.

Installation

The screen lock can activate during the initial install process.

After 10 minutes of inactivity, the VideoEdge desktop automatically locks and displays a screen saver. This locking method increases security by restricting desktop access. To release the screen lock, click on the window or press any key to display an unlock prompt screen. On the unlock prompt screen, use `root` as the password.

Device connection

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.

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 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 can be connected directly to VideoEdge 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 Hardware configurations.

Monitors

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

On the VideoEdge 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 Hardware configurations.

Audio devices

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

ⓘ **Note:** On the VideoEdge Hybrid NVR 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 types of available audio inputs and outputs varies by model. For more information, see Hardware configurations.

Alarms

Connect alarm inputs and outputs to VideoEdge 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.

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

Other devices

You can connect optional devices to your VideoEdge as follows:

- **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.
- **External storage module (ESM):** Connect ESMs to the VideoEdge to add additional storage.
- **Dome controllers:** Connect dome controllers to the COM2 serial port, such as the Sensormatic VM16E, American Dynamics ADTTE Touch Tracker, ADTT16E Advanced Dome Controller, or AD2089 Analog Keyboard.

Wiring

Figure 3: ADTTE/ADTT16E wiring diagram

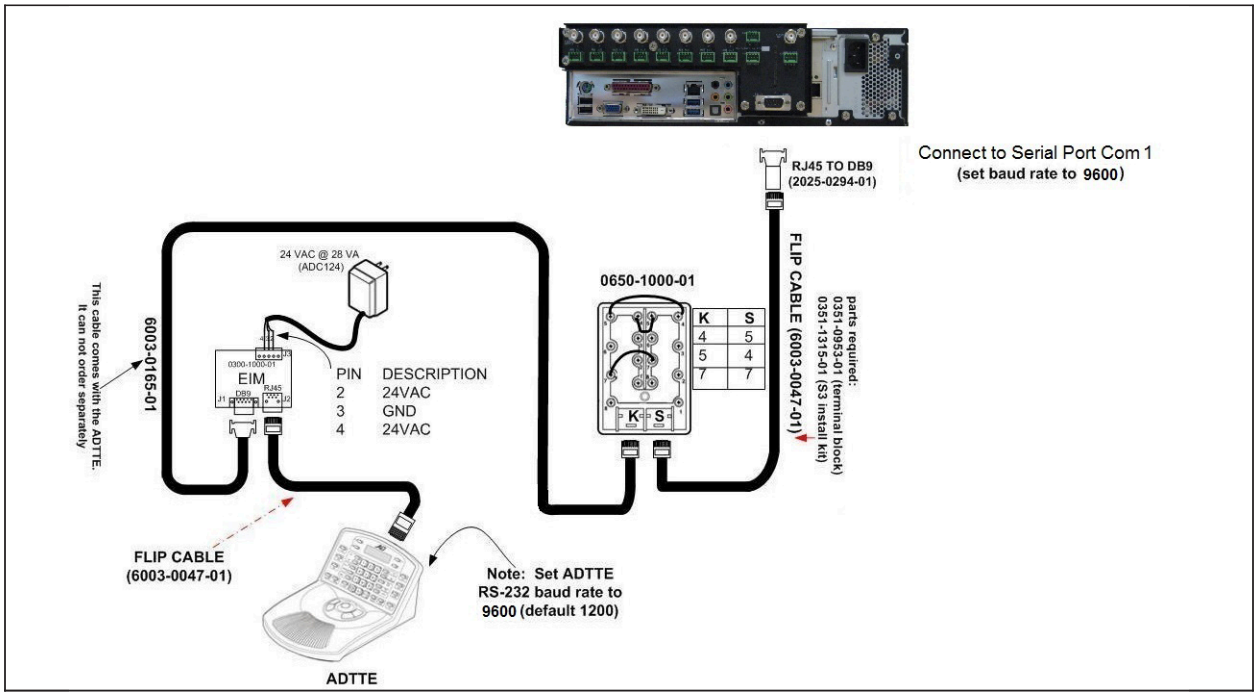
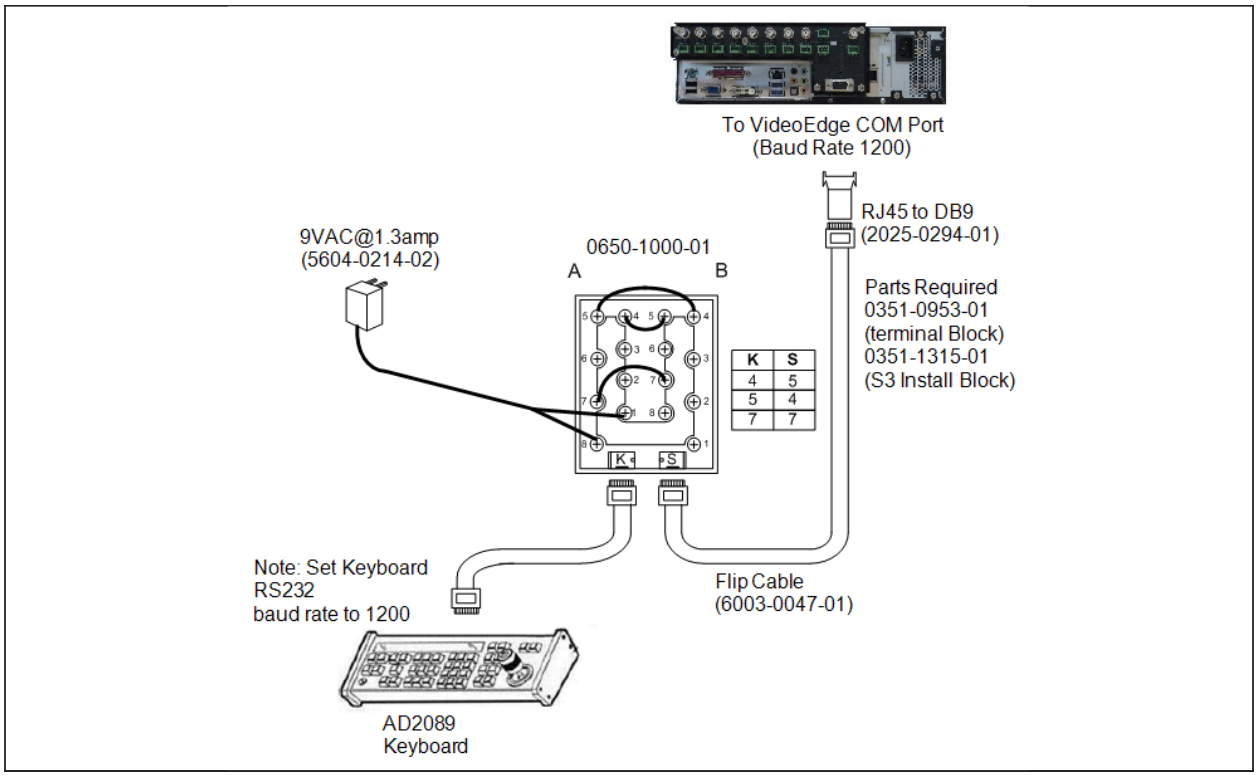


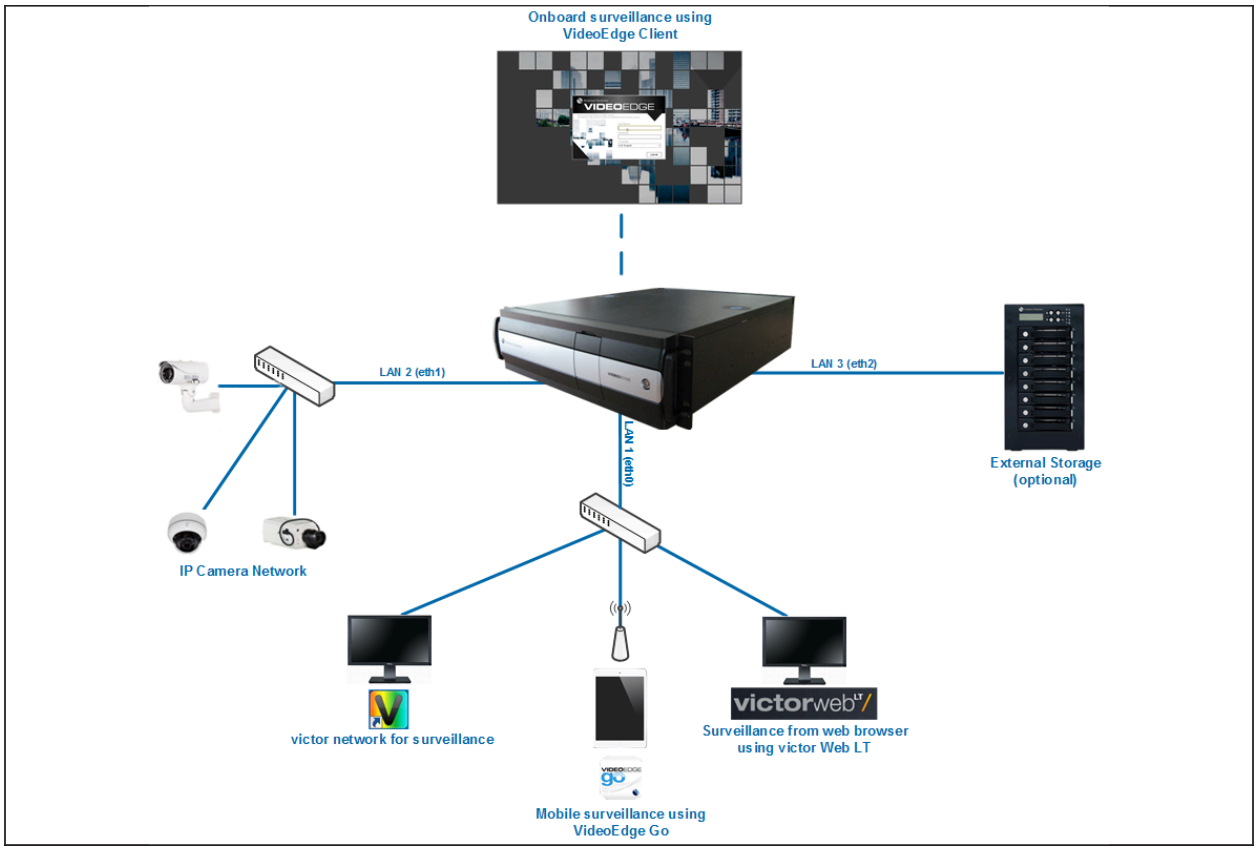
Figure 4: AD2089 wiring diagram



Networks

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 5: Network topology of an IP-only VideoEdge NVR



System partitions

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, 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 and therefore use all available storage space.

System partitions reference table

Table 3: System partitions

System partitions				
All models and model types	**Size**	**Type**	**FS type**	**Mount point**
	16 GB	Linux swap	Swap	`swap`
	47 GB	Linux native	XFS	`/var`
	20 GB	Linux native	Ext3	`/`
	50 GB	Linux native	XFS	`/var/opt/americandynamics/venvr/secure`

Default partitions reference table

Table 4: Default partitions

Default partitions					
Model	**Media storage (TB)**	**Drive size (TB)**	**Type**	**FS type**	**Mount point**
VideoEdge Desktop Hybrid NVR	0	-	-		
	2	2	Linux native	XFS	/mediadb
	4	4	Linux native	XFS	/mediadb
VideoEdge Desktop NVR	0	-	Linux native		
	2	2	Linux native	XFS	/mediadb
	4	4	Linux native	XFS	/mediadb
VideoEdge 2U Hybrid NVR (RAID)	18	13.6	Linux native	XFS	/mediadb
VideoEdge 2U Hybrid NVR (Non-RAID)	0				
	3	3	Linux native	XFS	/mediadb
	6	3	Linux native	XFS	/mediadb
		3	Linux native	XFS	/mediadb1
	12	3	Linux native	XFS	/mediadb
		3	Linux native	XFS	/mediadb1
		3	Linux native	XFS	/mediadb2
		3	Linux native	XFS	/mediadb3
VideoEdge 2U NVR (RAID)	16	11	Linux native	XFS	/mediadb
	24	18.5	Linux native	XFS	/mediadb
VideoEdge 2U NVR (Non-RAID)	0				
	8	4	Linux native	XFS	/mediadb
		4	Linux native	XFS	/mediadb1
VideoEdge 3U Hybrid NVR (RAID)	18	13.6	Linux native	XFS	/mediadb
VideoEdge 3U Hybrid NVR (Non-RAID)	0				
	3	3	Linux native	XFS	/mediadb
	6	3	Linux native	XFS	/mediadb
		3	Linux native	XFS	/mediadb1
	12	3	Linux native	XFS	/mediadb
		3	Linux native	XFS	/mediadb1
		3	Linux native	XFS	/mediadb2
		3	Linux native	XFS	/mediadb3

Rack mounting

The VideoEdge rack-mountable chassis has pre-drilled holes to install the included rack slides. To mount the unit, attach slides to the chassis and use the included front mount rack holes.

⚠ CAUTION

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. Use a rack equipped with EIA-310-D standard 19 in. (482.6 mm) front and rear mounting flanges.

Safety warnings for rack-mountable equipment

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).

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.

Mechanical loading

When mounting the equipment, ensure that the mechanical loading is even.

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 over-current protection and supply wiring. Consult the equipment's nameplate ratings when addressing this concern.

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.

VideoEdge bundles

VideoEdge is supplied as one of the following bundles:

- Hardware and software
- Software only

Hardware and software bundle

When VideoEdge is supplied as a hardware and software bundle, the following are preconfigured:

- Basic system settings, including time and region.
- Default partitioning, including the required system partitions and some media partitions.

  ⓘ **Note:** If the preconfigured media partitions are not suitable, they can be edited 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.

Installing a hardware and software bundle

There are three stages to set up and install VideoEdge hardware and software bundles:

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

Booting up VideoEdge for the first time

1. Turn on the VideoEdge NVR.
   A series of boot messages appear and then system loads to the License Agreement.
2. Click **Next**.
3. When the license agreement displays, click **Yes, I Agree to the License Agreement**.

Software only bundle

When VideoEdge is supplied as a software-only bundle, you must install it onto your hardware. Before installing the VideoEdge software, ensure that:

- The hardware meets the minimum operation requirements.
- The system drive is connected to the SATA 0 location on the motherboard.

Installing a software only bundle

ⓘ **Note:** Any previously configured operating system are removed and overwritten.

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

1. Booting the system using the software DVD or USB drive.
2. Rebooting the system after basic installation.
3. Logging on to the VideoEdge desktop.
4. Configuring VideoEdge using the Setup Wizard.

Booting the system using the software DVD

1. Insert the software DVD into the optical drive and restart the computer or server. VideoEdge boots 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.

Rebooting the system after basic installation

1. From the **Installation Options** menu, select and press Enter:
   Install/Restore_VideoEdge_NVR_Release_x.x.x.xxx
   where **x.x.x.xxx** is the software version you are installing.

   After approximately 20 seconds, the installation automatically starts in this mode. A**Loading Linux Kernel** pop-up displays, followed by a series of boot messages. This process can take several minutes.

   ⓘ **Note:** The VideoEdge software installs the minimum required Linux operating system to run the VideoEdge system. VideoEdge software is installed as an appliance.

2. Read and accept the license agreement, click **Next** and **Yes**. The self-installer initiates. The progress displays during installation.
3. When the self-installer is complete, click **Reboot NVR** when prompted.

Booting the system using the USB drive

Ensure that no other USB drives are inserted during installation.

1. Insert the installation USB drive into an available USB port and restart the computer or server. VideoEdge boots and the Installation Options menu opens.
2. 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.

Operational modes

VideoEdge can operate in the following additional operational modes:

- **Analytic Appliance:** Provides additional video analysis resources to devices that are added to it. Video analysis can be resource-intensive. Video analytics like Video Intelligence, Face Recognition, and License Plate Recognition can be offloaded to the Analytics Appliance from external devices. Camera streams added from external devices can be configured for video analysis on the Analytics Appliance.
- **Transcoder:** The Transcoder appliance is an auxiliary device that can provide additional transcoding resources to NVRs in an NVR group. You can use the VideoEdge Administration Interface to add the appliance to an NVR Group.

ⓘ **Note:** The operational modes are set by default on the hardware units that support them.

Logging on to the VideoEdge desktop

1. Enter the default user name `VideoEdge` and click **Next**.
2. Enter the default password `VideoEdge` and click **Sign In**.

   ⓘ **Note:** When the unit is an Analytics Appliance or Transcoder, use the following credentials:
   - **Username:** `Tyco`
   - **Password:** `Tyco`

Passwords for logging on to the VideoEdge desktop

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

General users

The preconfigured VideoEdge account password is `VideoEdge`.

ⓘ **Note:** When the unit is an Analytics Appliance or Transcoder, use the following credentials:
- **Username:** `Tyco`
- **Password:** `Tyco`

System administrators

The preconfigured root account password is `root`.

ⓘ **Note:** The root account is intended for use by system administrators only.

For more information, see System Passwords.

Important

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

You require your password to make administrative changes to the desktop.

Setup Wizard

After installing VideoEdge, configure basic settings using the Setup wizard.

You are automatically directed to the Setup Wizard the first time you log on to the Administration Interface after installation.

Note: To access the Setup Wizard, use the VideoEdge or Appliance Administrator icon on the desktop, or a remote client.

If you exit the Setup Wizard before you complete all of the steps, your progress saves, and when you return to the Setup Wizard you are automatically directed to the last page you viewed.

When the Setup Wizard is complete, your VideoEdge is operational.

Configuring VideoEdge using the Setup Wizard

1. Enter the default administrator username: `admin`
2. Enter the default administrator password: `admin`.
3. Click **Login**. The VideoEdge Setup Wizard begins.
4. Complete the Setup Wizard.

Completing system security in the Setup Wizard

To complete system security in the Setup Wizard, you must create a digital certificate and create new passwords for each preconfigured default user account and service account.

Digital certificate

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.

Preconfigured account passwords

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

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, review the VM system settings using the hardware resourcing guidelines.

Create at least one media disk for media recording. For guidelines on creating appropriate storage size, see the hardware resourcing guidelines.

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

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.

For optimum performance, use thick-provisioned Eager Zeroed disk creation over thick-provisioned Lazy Zeroed disk creation. This will require additional time to complete.

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 5: Hardware resourcing

VideoEdge Virtual 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 open SUSE 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) 1 GbE	(2) 1 GbE	(2) 1 GbE	(2) 1 GbE
	CPU reservation	Boot/OS/DB	200 GB	200 GB	200 GB
	Minimum video storage	1 TB	4 TB	200 GB	200 GB
	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 the following:

- **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 and 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.

Administration Interface

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

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

Accessing the Administration Interface on a web browser

A System Administrator can use a web browser to log on to the VideoEdge Administration Interface. You can configure and edit VideoEdge settings and view live video.

There are two types of System Administrator accounts: admin and operator. Admin is the default account. An operator account is a predefined role. You can use the Setup Wizard to create an operator account.

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

To log on to the Administration Interface on a web browser, complete the following steps:

1. On a web browser, enter the VideoEdge IP address as follows: http://NVR_Server_IP_Address, where `NVR_Server_IP_Address` is the IP address of the machine running the NVR software. For example, http://192.187.100.21

   ⓘ **Note:** A warning page states there is a problem with the website's security certificate. This warning displays only 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)**.

   ⓘ **Note:** The wording can differ between browsers.

3. When the logon window displays, enter the default username and password.
   For a system administrator, enter the following default credentials:
   - **Username:** `admin`
   - **Password:** `admin`

   For an operator, enter the following default credentials:
   - **Username:** `operator`
   - **Password:** `operator`
4. Click **Login**.

Accessing the Administration Interface in victor

You can configure and edit VideoEdge settings by accessing the Administration Interface through victor.

To access the VideoEdge Administration Interface through victor Unified Client, add the VideoEdge NVR to your recorders in the Devices list in victor Unified Client. For information, refer to the *victor Client Administration and Configuration Guide*.

ⓘ **Note:** You cannot view live video in victor Unified Client. To view cameras in live mode, use the Surveillance pane.

To log on to the Administration Interface in victor, complete the following steps:

1. In victor Unified Client, click **Devices** and 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

To navigate the Administration Interface and access the required configuration settings, use the menu and submenus listed on the left of the page. Each menu is further divided into submenus. These submenus are described in the relevant chapters. The main menu lists the following menu options:

- Live Video. This menu option is available only on a web browser.
- Devices.
- Storage.
- Archive.
- System.
- Network.
- Advanced.
- Monitor Outputs.
- Logout. This menu option is available only on a web browser.

Table 6: 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 in the main menu. Submenu options display when you select a menu option from 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. You can also view the user account currently in use and the current software version.

Administration Interface icons

Table 7: Add, Edit, and Remove icons

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

Live video

After you configure VideoEdge, you can view live video streams using the Live Video menu, when remotely accessing the Administration Interface.

If you access the Administration Interface using victor Unified Client or locally from the VideoEdge, the Live Video menu item is not available. Use the Surveillance window in victor Client or 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 Inter-

face. 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.

1. Click the **Live Video** menu.
2. Click the **1 Camera View** tab or the **2x2 Camera View** tab.
3. From the **Select camera to view** list, select the cameras you want to view.
   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 in the Administration Interface.

Devices menu and submenus

Table 8: Devices menu and submenus

Menu	Description	Submenus
List	View a list of all devices connected to the VideoEdge and a summary of their configuration status. Add and remove devices Edit or batch edit camera configuration settings.	Video List Audio List Text List Virtual List 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.	Alarms Sensors Outputs
Scheduler	Specify the recording mode that is active at scheduled times during the day.	Schedules Schedule Editor Group Editor
Discovery	Scan for devices, and use auto-discovery to add cameras to VideoEdge.	Discovered Devices Scan for Devices
Security	Create and maintain password groups.	
NVR Group	Configure NVR groups for remote transcoding and failover.	NVR Group List Discovered NVRs
Options	Configure global camera settings that are applied whenever a camera is added to VideoEdge. Enable TrickleStor and configure settings.	Camera Add 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.

Table 9: 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
	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

Devices List

The Devices 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 Devices List 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 use the Arrow down icon to sort the list in ascending order.

The Devices List has 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 options of video devices you have added to VideoEdge.

- View the cameras that have been added to VideoEdge.
- Add, edit, remove, and batch edit devices.
- Configure Advanced Settings.

Table 10: Video List summary

Field	Description
NO.	Device slot number.
CAMERA	Device name as given when adding the device to VideoEdge. **Note:** When you add a camera by hostname or FQDN (when DNS is configured), hover over the address to see the corresponding IP Address. Device IP address. Device Manufacturer and Model. Current version of camera firmware on camera. 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, the Edit Group Times icon displays in the field and you cannot change the device recording state.
ARCH	Indicates if archiving is enabled for the device. The archiving options available are: •  Archiving Disabled •  Archive all video •  Archive only alarm video

Table 10: Video List summary

Field	Description
	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
	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 can 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 a device

Use the Video List tab to add a device manually or from a CSV file.

ⓘ **Note:** You can also add a device using the **Discovery** tab. For further information, see the *Discovery* section.

Analog device

Before you manually add an analog device complete the following steps.

1. 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 Devices List page using the IP address, 127.0.0.1. After a device with this IP address is added to VideoEdge, all analog ports open, and all devices display in the Devices List.
2. When the connection is established between VideoEdge and the analog ports on the unit, all devices 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 displays for an analog camera, connect the camera to a port on the unit.

3. Ensure the default recording mode for analog cameras, when first connected to VideoEdge, is Recording Off.
4. 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 clear the Add All Inputs on Device check box, you can select the inputs you want to add. This behavior is the same for all multichannel devices.

Manually adding an analog device

The following conventions name all devices added as part of a multichannel encoder:

- Video inputs are given a _n suffix. For example Analog_1.
- Audio inputs are given a _n_audio suffix. For example Analog_2_audio where Analog is the user-defined device name.

ⓘ **Note:** Each device can be renamed after it is added to the NVR.

1. Expand the **Devices** menu and click **List**.
2. Click the **Add New Device** icon.
3. In the **Device Name** field, enter a device name.
4. In the **Device Address** field, enter `127.0.0.1`.
5. From the **Manufacturer** list, select the camera manufacturer.

   ⓘ **Note:** If you do not want to specify the manufacturer or the manufacturer doesn't appear in the list, select **Auto Detect**.
6. Ignore the **Security Group** list. It is not relevant to analog cameras.
7. **Optional:** From the **Security Group** list, select **New Security Group**.
   a. Enter a **Group Name**.
   b. Enter a **Description**.
   c. **Optional:** Enter a **Username** and **Password** or leave these fields blank to use the camera's default credentials.
   d. **Optional:** Select a Security Level from the **Security Level** list.
   e. **Optional:** To use a different port to the default port, clear the **Default** check box and enter the new port number in the **Port** field.
   f. **Optional:** Select the **ONVIF RTSP Auth** check box if the devices in this group use ONVIF communication protocols.
8. **Optional:** Expand **Additional Settings** to configure additional device settings:

   ⓘ **Note:** Each of these Additional Settings are optional.

   a. Select a device type from the **Device Type** list.
   b. 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.

        ⓘ **Note:** This option is only available for cameras that support three streams.
   c. Select a specific camera slot from the **Slot** list.

      ⓘ **Note:** Selecting **Auto** auto-configures device slot allocation.
   d. Clear the **Add All Inputs on Device** check box if you do not want to add all inputs on a device.

ⓘ **Note:** Specific camera slots can also be allocated when manually adding the inputs on a device.

e. Clear the **Default Associations** check box if you want to define custom associations after the devices have been added.
f. Clear the **Enable Smart Search (Motion Metadata)** check box to disable Smart Search for any cameras that you add manually.

9. Click the **Save** icon.

ⓘ **Note:** If the **Default Associations** check box is not selected, a window will open displaying the available inputs. For video devices, a snapshot can be displayed.

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 attempts to use the general ONVIF communications protocol to communicate with the camera. If the camera supports ONVIF, you are 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 Devices 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.

Manually adding an IP device

1. Expand the **Devices** menu.
2. Click **List**.
3. Click the **Add New Device** icon.
4. Enter the device name in the **Device Name** field.
5. Enter the IP address in the **Device Address** field.

ⓘ **Note:** If the DNS server is configured and added to the VENVR, the Hostname or FQDN can be entered in the **Device 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:** To use a different port to the default port, clear the **Default** check box and enter the new port number in the **Port** field.
   g. **Optional:** Select a **Streaming Security Level** from the list.

ⓘ **Note:** For more information on Streaming Security Levels for supported Illustra cameras, refer to Illustra Secure Video.

h. **Optional:** Select the **ONVIF RTSP Authentication** check box 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** check box 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** check box if you want to define custom associations after the devices have been added.
15. **Optional:** Clear the **Enable Smart Search (Motion Metadata)** check box to disable Smart Search for any cameras that you add manually.
16. **Optional:** Select the **Use Multicast Streaming** check box to use the camera's multicast stream to record footage.
17. Click the **Save** icon.
    If the **Default Associations** check box is unselected, a window opens displaying the available inputs. For video devices, a snapshot can be displayed.

Axis body worn camera (BWC) device

When a body worn camera (BWC) is added to an Axis Body Worn System (BWS), this information is pushed to the VideoEdge. As a result the BWC is automatically added to the VideoEdge. The Axis BWC appears on the VideoEdge Device List page alongside non-BWCs.

For information on preparing the VideoEdge for Axis BWCs, in the **Advanced** section, see Axis Body Worn System.

Removing a BWC

When an Axis BWC is no longer in use, you must first remove it from the Axis BWS, and not from the VideoEdge Device List page.

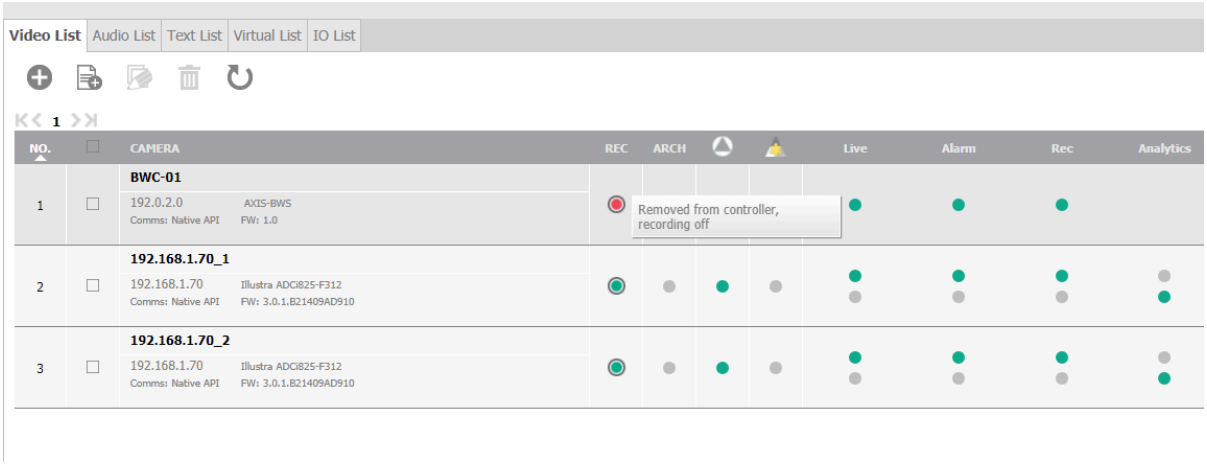
About this task:
When a camera is removed from the Axis BWS, the Axis controller informs VideoEdge of its removal, and the camera's REC mode displays as recording off. A tool tip on the REC mode icon informs the user that the camera has been removed from the Axis Controller. This indicates that it is safe to remove from the VideoEdge. You can still view media stored for this device when the REC mode is off.

You can remove an Axis BWC from the VideoEdge Device List page when the BWC is no longer in use and the associated recordings are no longer required. Do this only after the BWC has been removed from the Axis BWS. Under exceptional circumstances, such as, an Axis controller hardware failure, you can remove an Axis BWC from the VideoEdge before it is removed from the Axis BWS.

1. Expand the **Devices** menu, and click **List**.
2. On the **Video List** tab, locate the BWC row that you require.

3. In the **Rec** column, verify that the icon is red. This indicates that recording mode is off.
4. Select the check box for the BWC row.
5. To remove the BWC device, click the **Remove device** icon.

Figure 6: Removing a BWC



Docking a BWC after use

When you use Axis BWC for recordings, the BWC is docked with the Axis controller, the Axis BWS uploads the recordings to the VideoEdge. The recordings are stored on the VideoEdge and are available for playback.

About this task:
If VideoEdge is unable to associate a media file with a matching BWC, VideoEdge can retain the media file and record the failure in the Wearable Cameras tab.

1. Expand the **Devices** menu, and click **Options**.
2. On the **Wearable Cameras** tab, you can view the status of the media file uploads.

   ⓘ **Note:** The maximum duration of a media file that the Axis BWS uploads to the VideoEdge is 15 minutes. For example, a 35-minute recording sends as two 15 minutes files and one 5 minute file. Use the Wearable Cameras tab to view the status of the media file uploads.

3. Manually remove the media file when the disk space is low on the partition mounted at the following location: `/var/opt/americandynamics/venvr/clipexport/`.

   ⓘ **Note:** Locate failed media files at the following location: `/var/opt/americandynamics/venvr/clipexport/MediaUpload/axis-bws/failed/`.

Enabling a multicast camera

ⓘ **Note:** You cannot enable multicast streaming after you add a camera.

1. When adding a camera to VideoEdge, select the **Multicast** option.
2. To enable multicast streaming after you have added a camera:
   a. Delete the camera.
   b. Re-add the camera and select multicast streaming.

Adding an RTSP stream

1. Expand the **Devices** menu and click **List**.
2. Click the **Add New Device** icon.

3. Enter the **Device Name**.
4. **Optional:** Select a Security Group from the **Security Group** list, or create a new Security Group.
5. **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** check box and in the **Port** field, enter the new port number.
   g. **Optional:** Select the **ONVIF RTSP Authentication** check box if the devices in this group use ONVIF communication protocols.
6. Click **Additional Settings**.
7. Select **RTSP** from the **Device Type** list.
8. Enter the **RTSP URL** of the RTSP stream.
9. **Optional:** Select a specific device slot from the **Slot** list. Selecting **Auto** auto-configures device slot allocation.
10. Click the **Save** icon.

CSV file prerequisites

You can add multiple devices to VideoEdge simultaneously by importing the device information from a CSV file. The CSV file must contain the following information for each device:

Table 11: CSV file prerequisites

Prerequisite	Description
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 options: TRUE or FALSE.
Enable ONVIF	Enable or disable ONVIF. Valid options: 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 options: 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 options: 0, 1, 2, 3, or 4
Auto-Configure streams	Enable or disable the Auto Configure streams feature. Valid options: 0,1, or 2.
Optional: Camera Slot	An integer to identify the camera slot. If omitted, the slot number is assigned automatically. ⓘ **Note:** Add multichannel devices to the file once. All available channels are added automatically.

Adding devices from a CSV file

1. Expand the **Devices** menu and click **List**.
2. Click the **Add Devices from CSV file** icon.
3. Click **Choose File**.
4. Navigate to the required file, and click **Open**.
5. Click **Add Devices**. The CSV file must be valid for the device import to complete successfully. A validation overview displays any errors detected in the file.

Editing basic video settings

1. Expand the **Devices** menu and click **List**.
2. Click the **Edit** icon for the camera that you want to edit.
3. 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.
4. Click the **Save** icon.

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.

Configuring dual recording for a camera

1. Expand the **Devices** menu and click **List**.
2. Click the **Edit** icon for the camera that you want to configure.
3. In the **Rec** column, select the check boxes for the two streams that you want to record.

   ⓘ **Note:** You must assign the camera's Alarm functionality to at least one of the streams that you want to record.

4. Click the **Save** icon. A message displays informing the user that two streams will now be recorded, increasing storage usage.
5. 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

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 check box next to the setting is checked. If you deselect the check box, 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

Batch editing camera settings

1. Expand the **Devices** menu and click **List**.
2. Select the check box for each camera that you want to batch edit.
3. Click the **Batch Edit** icon to open the **Batch Edit** page.
4. 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 the devices using batch edit, each device gets 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 frame rate decimation. Archiving quality is applied in 10% intervals where 10% provides the lowest quality video and 100% provides the highest quality video for archiving.
   g. **Maximum Archiving Storage Period:** Select 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 lists.

Note: When you select a value for the Codec, FPS, Resolution, Quality, Bit Rate Control, Bit Rate, Max Bit Rate, and Profile fields, each list 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 lists can be empty if the parameter is not supported for that Codec on any camera.

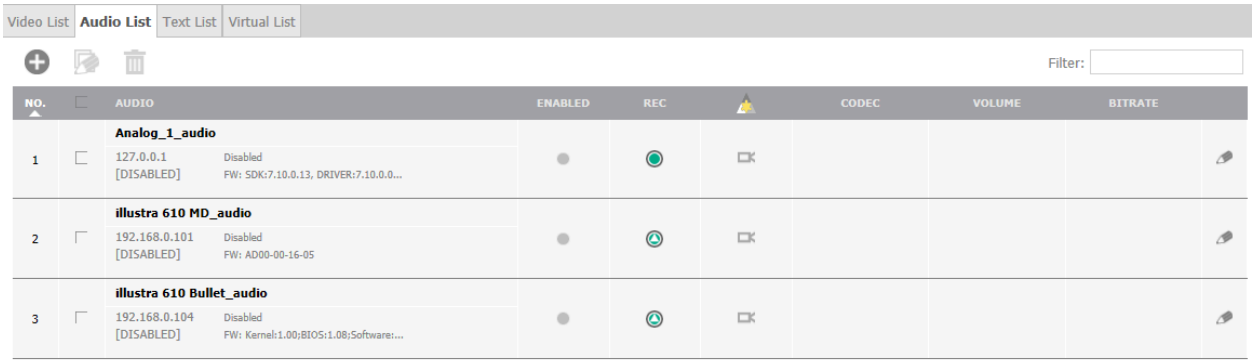
5. Click the **Save** icon.
6. To confirm the changes, on the **Confirm Changes** window, click the **Save** icon. If you do not want to make these changes to all cameras, click the **Cancel** icon.
7. When a message box opens to confirm the changes were successful, click **OK**.
8. If some of the changes are not successful, a summary page of failed updates opens with the failures highlighted in red. Click **OK** to continue.

Audio List

Audio devices that 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 is 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 7: Audio List page



Audio List summary table

Table 12: Audio List summary

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.

Table 12: Audio List summary

Field	Description
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

Editing audio settings

1. Expand the **Devices** menu.
2. Click **List**.
3. Click the **Audio List** tab.
4. Click the **Edit** icon in the audio row you want to edit.
5. Make the required changes:
   - **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.

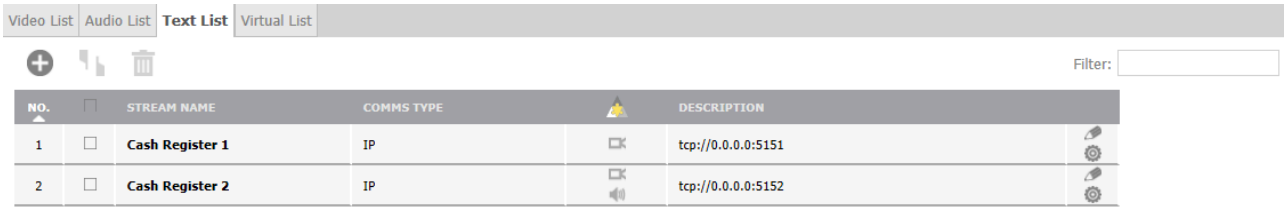
Text List

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 8: Text List page



Text List summary table

Table 13: Text List summary

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 • Text
Description	Indicates the configured settings.

Configuring serial port settings for a serial text stream device

Before you add a serial text stream device, ensure it is connected to one of the NVR USB ports or its RS232 Serial Port. After you connect the device, configure the relevant serial port's communication protocol for text stream use.

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

1. Expand the **Devices** menu, and then click **List**.
2. Click the **Text List** tab, and then click the **Add Text Stream** icon.
3. Enter a **Text Stream Name**.
4. Select the **Connection Type** from the list.
5. 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**.
6. 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.
7. **IP only:** Enter the **Port**.
   The port number must match the port number assigned on the text stream device.
8. **Serial only:** Select the option button of the **Serial Device** you want to use.
9. **Serial only:** Select the **Edit** icon to edit the serial device settings, if required:
   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.
10. Click the **Save** icon.

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.

Adding a rule to a text device

1. Expand the **Devices** menu, and then click **List**.
2. Click the **Text List** tab.
3. Select the check box of the text device you want to create a rule for.
4. Click the **Rules/Markers** icon.
5. Click the **Add Rule** icon.
   The **Rule Definition** window opens.
6. Enter the **Name**.
7. Enter a match in the **Match with** field.

8. Select the **Search Direction** from the list.
9. Select the number of words to skip after a match is found to find the associated value, from the **Jump N Results** list.
10. 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.
11. Enter a value in the **Value 1** field. This is required when using string, less than, greater than, equal to, and range criteria.
12. Enter a value in the **Value 2** field. This is required when using range criteria.
13. Click the **Save** icon.

Adding a marker to a text device

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

Removing a rule or marker from a text device

1. Expand the **Devices** menu, and then click **List**.
2. Click the **Text List** tab.
3. Select the check box of the text device you want to remove a rule or marker from.
4. Click the **Rules/Markers** icon.
5. Select the check box of the rule or marker you want to remove.
6. Click the **Remove** icon.

Grouping rules

Rules can be grouped together for both text stream alarms and searches, using the Group Rules check box. Grouping rules creates an ‘AND’ logic so that all the grouped rules must be satisfied. When the Group Rules check box is selected, it applies to all rules that have been added to the alarm or search definition. Rules that have been disabled do not need to be satisfied.

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

1. Expand the **Devices**menu, and click **List**.
2. Click the **Text List** tab.
3. Select the check box of the text device that you want to group rules for.
4. Click the **Rules/Markers** icon.
5. On the **Rules/Markers** page, select the **Group Rules** check box.

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.

1. Expand the **Devices** menu, and then click **List**.
2. Click the **Text List** tab.
3. Click the **Setup** icon in the text record that you want to edit a text list setting for.
4. Select the check boxes for the video and audio devices you want to associate with the text device.
5. 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.
6. Click the **Save** icon.

Removing associations from text devices

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

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

Creating a virtual camera

1. Expand the **Devices** menu, and then click **List**.
2. Click the **Virtual List** tab.
3. Click the **Add Virtual Camera** icon.
4. Enter a **Name** for the virtual camera stream
5. Select a layout type from the **Layout** list.
6. For each pane in the camera stream layout, select a camera from the drop-down list. Virtual cameras do not support duplicate cameras. All camera entries must be unique.
7. 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 using an NVR with VideoEdge 5.3 or higher must be associated with cameras for correct functionality.

Manually adding an I/O device

1. Expand the **Devices** menu, and then click **List**.
2. Click the **IO List** tab.
3. Click the **Add IO Device** icon.
4. Enter a name in the **IO Device Name** field.
5. Enter the IP address of the device in the **IP Address** field.
6. Select a Security Group from the **Security Group** list.
7. Click the **Save** icon.
   The **Select Interfaces to Add** window opens.
8. Select the check boxes of the interfaces that you want to add.
9. **Optional:** Select a camera to associate the interface with from the **Camera Association** list.
10. Click the **Save** icon.

Testing the input state of the I/O device

1. Expand the **Devices** menu.
2. Click **List**.
3. Click the **IO List** tab.
4. Click **Test** on the device that you want to test.
5. Click **Get State**.
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 to an Intellex video device made through the VideoEdge NVR does 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.

Adding video devices from an Intellex recorder

1. Expand 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** check box.
8. **Optional:** Clear the **Default Associations** check box if you want to define custom associations after the devices have been associated.
9. Click the **Save** icon.
   The **Intellex Device** list displays.
10. Select the check box of each device you want to add.

11. Click the **Save** icon.

Advanced camera configuration

To configure advanced camera settings, click the Setup icon for the required camera in the Video List. 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 window.

ⓘ **Note:** When you add a camera by name, the Device IP Address and IP Address fields will be visible.

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.

Camera 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.

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.

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.

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.

Video streaming

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

Image settings

Camera image settings can be configured on 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.

Configuring image settings

The available settings and value ranges are dependent on the camera make and model.

1. Expand the **Devices** menu, and click **List**.
2. On the row of the camera that you want to configure, click the **Setup** icon.
3. Click the **Image Settings** tab.
4. Adjust the **Video Properties** settings as required. The configurable settings include the following:
   - **Video Standard:** select the required video processing standard from the list.
   - **Rotate Image:** select the angle you want to rotate the image from the list.
   - **Brightness:** select the brightness value from the list.
   - **Contrast:** select the contrast value from the list.
   - **Hue:** select the hue value from the list.
   - **Saturation:** select the saturation value from the list.
   - **Sharpness:** select the sharpness value from the list.
   - **White Balance:** select the white balance control value from the list.
   - **Back Light Compensation:** select the back light compensation value from the list.
   - **Image Interlaced:** select the image interlacing setting from the list.
5. Adjust the **Lens/Sensor** settings as required. The configurable settings include the following:
   - **Lens Focus:** select a focus for the camera from the list.
   - **Lens Auto Focus:** select the check box to enable automatic camera focus.
   - **Lens Iris:** select the iris value for the camera from the list.
   - **Lens Auto Iris:** select the check box to enable automatic iris control.
   - **Lens Day Night Mode:** select the required mode from the list.
   - **Lens Image Stabilisation:** select the check box to enable or clear the check box to disable.
   - **Lens WDR (Wide Dynamic Range):** select the check box to enable WDR.
   - **Defog Mode:** select a defog level to apply to the camera.
   - **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, because this will dictate the algorithm used by victor unified client for de-warping.
6. Click the **Save** icon.

Function & 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 window.

AXIS Virtual IO support

You can configure support for the integration of Virtual IOs for Axis cameras using event and action services, and virtual inputs. You can:

- Create a rule on the Axis camera. A notification is sent to VideoEdge when the device detects an occurence, such as the triggering of any analytic installed on the device.

  ⓘ **Note:** When creating the rule on the Axis camera, you must use the following parameters in the Name field: `videoedge_<number of rule>`

- Configure VideoEdge to trigger an event on the Axis camera, such as playing an audio clip.

Creating a rule for Virtual IO support

Complete this procedure on the **Rules** page of the Axis camera user interface. For more information, refer to the relevant Axis camera user manual.

1. Use the following parameters in the **Name** field: `videoedge_<number of rule>`

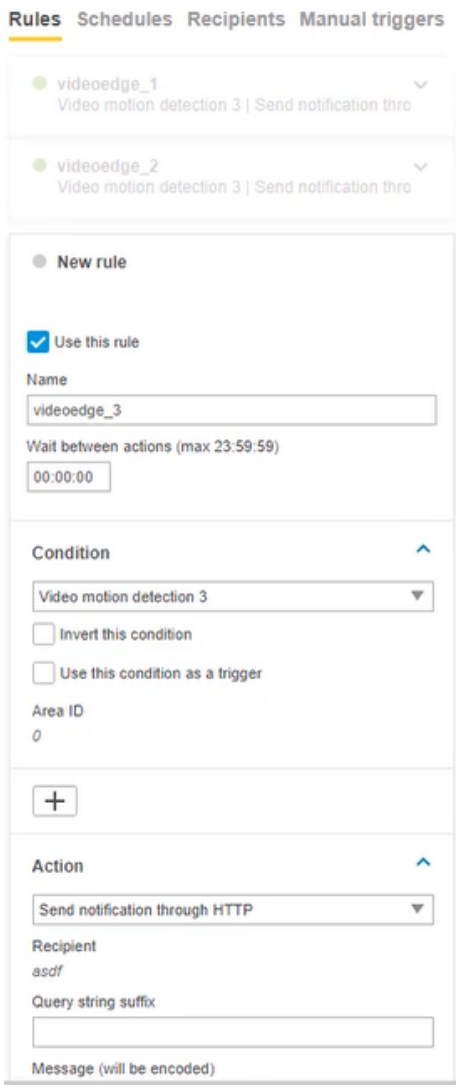
   ⓘ **Note:**
   - Rules should be named in a numbered sequence: videoedge_1, videoedge_2, and so on.
   - The Axis handler will count a rule name with the videoedge_<number of rule> parameter and count it as an extra dry contact.

2. From the **Condition** list, select a rule condition.
3. From the **Action** list, select **Send notification through HTTP**.

   ⓘ **Note:** The recipient can be any address. VideoEdge will configure this when creating the dry contact.

4. Click **Save**.

Figure 9: Rules page for an Axis camera



Creating a dry contact or relay for Virtual IO support

1. From the **Devices** menu, click **List**, and then click **IO List**.
2. Click the **Add IO Device** icon. The **Add Relay/Dry Contact Device** window opens.
3. In the **IO Device Name** field, enter the Axis camera name.
4. In the **IP Address** field, enter the camera IP Address.
5. From the **Security Group** list, select **Axis**.
6. Click the **Save** icon. The **Select Interfaces to Add** window opens.
7. Select the interfaces you want to add and then click the **Save** icon.
   The selected devices are added and displayed in the IO List tab. The default names of the virtual interfaces will be named as either:
   - virtual_dry_contact
   - virtual_relay

   ⓘ **Note:** The selected devices are added and display in the **Devices List** in victor Client.

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 icons table describes each recording mode.

Record mode icons

Table 14: Record mode icons

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, Edge Analytics, and License Plate Recognition. 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 cannot use any of the features offered by that type of video analysis. Searches and alarms based on the analytic are not available until the analytic is enabled again.

Edge Object Identification

You can configure an object classification on an Illustra Pro Gen 4 camera in VideoEdge. When an object is detected on a capable camera and configured on VideoEdge, data on the object is stored by VideoEdge and sends this data to a capable client.

ⓘ **Note:** This feature is supported with Illustra Pro Gen 4 cameras only.

Edge Object Sub-classification

When enabled to do so, VideoEdge stores object characteristics data. The data is collected from capable cameras and stored on a per frame basis, and also provides summarized, prevalent characteristics data.

ⓘ **Note:** Object Sub-classification is only supported on Illustra Pro Gen 4 cameras and Flex Gen 4. To activate this feature configure the camera and enable the feature on VideoEdge.

ⓘ **Note:**

victor's user interface does not yet support search for objects based on their sub-classification.

Object classification	Object sub-classification	Cameras that support this feature	Firmware required	Search available on victor
Person	Upper clothing color	Illustra Pro Gen 4, Flex Gen 4	Latest update	No
Person	Lower clothing color	Illustra Pro Gen 4, Flex Gen 4	Latest update	No
Vehicle	Color	Illustra Pro Gen 4, Flex Gen 4	Latest update	No

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 Detection prerequisites

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 menu. 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 15: 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 7fps. Lower resolution or framerates might degrade the quality of Motion Detection. The NVR requires at least QCIF and more than 4fps to perform motion detection.

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

Enabling Motion Detection on a camera

1. Expand the **Devices** menu and then click **List**.
2. Click the **Setup** icon in the camera row you want to configure.
3. Set the camera **Record Mode** to a setting that supports Motion Detection (Only Record on Alarm, or Recording Always with Alarm On).
4. 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.

5. Select the required level of **Motion Sensitivity**.
   Values range from High (most results) to Low (least results).
6. Click the **Save** icon.

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*section.

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; 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 Identification**Identifies the object type, such as person or vehicle.

- **Object Sub-classification**Determines the characteristics of the object type such as vehicle color or the color of a person's upper of lower clothing.
- **Object Direction:** Used to detect objects moving in a certain direction through a region of interest, for example, a car traveling in the wrong direction 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:** For 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. 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. Configure your camera 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 on a camera

To enable a camera to use Video Intelligence or Deep Intelligence features, you can use the Video List tab, or the Function & Streams 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: 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.

Enabling Video Intelligence on a camera

1. Expand the **Devices** menu and then click **List**.
2. Click the **Setup** icon in the camera row you want to configure.

   Note: You can also enable Video Intelligence from the Video List.
3. Set the camera **Record Mode** to a setting that supports Video Intelligence (Only Record on Alarm, or Recording Always with Alarm On).
4. 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.
5. Enter a value for **Minimum object width (pixels)**.
6. Enter a value for **Minimum object height (pixels)**.
7. **Optional:** Select the **Compensate for camera motion** check box.
8. Click the **Save** icon.

Enabling Deep Intelligence on a camera

1. Expand the **Devices** menu and then click **List**.
2. Click the **Setup** icon in the camera row you want to configure.

   Note: You can also enable Deep Intelligence from the Video List.
3. Set the camera **Record Mode** to a setting that supports Video Intelligence (Only Record on Alarm, or Recording Always with Alarm On).
4. 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.
5. Select the detection sensitivity from the **Deep Intelligence Detection Sensitivity** list.
6. 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 on 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.

1. Expand the **Devices** menu, and then click **List**.
2. Click the **Setup** icon in the camera record for which you want to configure camera settings.
3. Set the camera **Record Mode** to a setting that supports edge based analytics (Only Record on Alarm, or Recording Always with Alarm On).
4. Select **Face Recognition** from the **Video Analysis** list.
5. Select the **Minimum face size** from the drop-down list.
6. 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).
7. Select the required level of **Face Detection Sensitivity**.
   Values range from High (most results) to Low (least results).
8. **Optional:** Select the **Face Search Alert** check box.
9. **Optional:** Select the **Face Verification** check box.
10. 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.

1. Expand 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 opens.
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** list.
6. Select the required level of **License Plate Recognition Sensitivity** from the drop-down list. 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.
   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*.

Person Detection Sensitivity

When you enable a camera for the Intelligent Search - Person analytic, you can also adjust how easily people are detected in a camera view using the Person Detection Sensitivity feature. This is a selectable value of 1 to 100 with a default value of 50. See Enabling Intelligent Search - Person on a camera.

Any detected people are surrounded by a bounding box that is viewable on the Alarms page. This allows you to maximize person identification and search accuracy. See Viewing Intelligent Search - Person bounding boxes.

Note: Higher settings produces more results, but can lead to false or duplicated detections.

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, complete the following steps:

1. Expand 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 that are currently in use.
   - The number of licenses that are still available for use.

Enabling Intelligent Search - Person on a camera

1. Expand the **Devices** menu, and click **List**.
2. From the **Video List**, locate the camera that is being configured, and click the **Setup** icon.
3. In the **Record Mode** section, select the record mode setting by clicking on the appropriate icon.
4. From the **Video Analysis** list, select **Intelligent Search – Person.**

   ⓘ **Note:** The Intelligent Search - Person analytic appears in the list as visible, but disable if any of the following issues occur:

   - It is not a supported feature on the hardware platform.
   - There are no licenses.
   - All licenses are already in use.
5. From the **Person Detection Sensitivity** list, select a value.

   ⓘ **Note:** The default value is 50.
6. From the **Maximum Recording Storage Period** list, select the appropriate recording settings.
7. From the **Associate Audio** list, select the appropriate audio device or select **No Audio**.
8. From 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

Use the Batch Edit feature to enable the Intelligent Search – Person analytic on multiple cameras. For more information, see Batch editing camera settings.

Viewing Intelligent Search - Person bounding boxes

In VideoEdge, Intelligent Search - Person is not supported by video analytic alarms, but you can view detected objects in detection boxes.

1. Expand the **Devices** menu, and click **Alarms**.

2. Select a camera configured with the Intelligent Search – Person analytic. Live video displays and detected objects are surrounded with a bounding box. See Intelligent Search - Person bounding box descriptions.

Intelligent Search - Person bounding box descriptions

Table 16: Bounding box descriptions

Bounding box	Description
Solid lines	Indicates a detected person. ⓘ **Note:** Only objects with solid lines are searchable.
Stars on top	The number of stars indicates how close the image size is to optimum results. ⓘ **Note:** Four stars indicates optimum results.
Dashed lines	Indicates that the object is not searchable because it is too small.

To optimize results:

- Increase the resolution of the analytics stream on the camera's stream configuration page.
- Adjust the zoom settings or lens of the camera so that objects appear larger in the frame.
- Adjust the camera's physical location so it is closer to the objects of interest.

Intelligent Search - Person supported hardware

Table 17: Intelligent Search - Person supported hardware

System	Description
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
ADVER36R5DF	36TB of usable RAID 5 configured video storage
ADVER90R5DG	90TB of usable RAID 5 configured video storage
ADVER66R5DG	66TB of usable RAID 5 configured video storage
ADVER48R5DG	48TB of usable RAID 5 configured video storage
ADVER36R5DG	36TB of usable RAID 5 configured video storage
ADVER18R5DG	18TB of usable RAID 5 configured video storage
ADVER06N0DG	6TB of usable RAID 0 configured video storage
VideoEdge 2U NVR	
ADVER50R5N2G	50TB, RAID 5, (60 Total) 4 NIC, Redundant PS
ADVER40R5N2G	40TB, RAID 5, (50 Total) 4 NIC, Redundant PS

Table 17: Intelligent Search - Person supported hardware

System	Description
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

Edge assisted Intelligent Search

Intelligent Search places large demands on VideoEdge, and can limit the number of cameras that this analysis can be performed on in a single VideoEdge. Some camera models are capable of performing aspects of video analysis, so by offloading a portion of intelligent search to the camera, a single VideoEdge can support video analysis of more cameras. This is referred to as edge assisted Intelligent Search.

ⓘ **Note:** When you enable this feature you also enable video analytics metadata. Only one type of metadata can be used at a time. If another type of metadata is being used, you must disable it before you enable this feature.

To enable edge assisted Intelligent Search - Person, complete one of the following procedures:

- Enabling edge assisted Intelligent Search - Person
- Enabling edge assisted Intelligent Search - Person on the Alarms page
- Enabling edge assisted Intelligent Search - Person on the Batch Edit page

Enabling edge assisted Intelligent Search - Person

To use edge assisted Intelligent Search - Person an administrator must complete the following tasks:

- Enable AI Object Classification on a camera that supports the feature.
- Enable edge based video analysis and select Intelligent Search - Person in VideoEdge.

1. To enable AI Object Classification on the camera, complete the following steps:
   a. Expand the **Devices** menu, and click **List**.
   b. On the **Direct Camera Access** tab, click the **AI Object Classification** tab.
   c. Select the **Enable AI Object Classification** check box.

2. To enable edge based video analysis, complete the following steps:
   a. Expand the **Devices** menu, click **List**, and click the **Functions & Streams** tab.
   b. In the **Function Configuration** area, from the **Video Analysis** list, select **Edge based**.
   c. Select the **Intelligent Search - Person** check box.
   d. On the tool tip dialog box for Intelligent Search-Person, click **OK**.

   ⓘ **Note:** Edge based Intelligent Search - Person requires Edge Video analytics metadata. The metadata automatically enables when required. On the Alarms page, a tool tip indicates why you cannot disable Edge Video Analytics Metadata.

Enabling edge assisted Intelligent Search - Person on the Alarms page

1. Enable edge-based analytics mode on the camera.
2. Expand the **Devices** menu, and click **Alarms**.
3. Complete one of the following options:
   - On the **Alarms** tab, from the **Select Camera** list, select the camera that you require.
   - On the **Function & Streams** page for a camera, in the **Function Configuration** area, in the **Alarms** row, click **Configure**.
4. On the **Alarms** tab, in the second table, enable **Edge Video Analytics Metadata** and **Intelligent Search - Person**.
5. **Optional:** To verify that metadata is coming from the camera, ensure that metadata overlay boxes around people display in the video feed.

Enabling edge assisted Intelligent Search - Person on the Batch Edit page

1. On the Camera List page, select one or more cameras.
2. Above the camera table, click the **Batch Edit** icon.
3. On the **Batch Edit** page, from the **Video Analysis** list, select **Edge Based**.
4. Select the **Intelligent Search - Person** check box.
5. Click the **Save** icon.
6. **Optional:** To confirm, navigate to the Alarms page for the chosen cameras and confirm the feature is enabled.

Direct Camera Access

You can access a camera Web GUI and configure camera firmware on a private network through the VideoEdge Web GUI or victor Client.

ⓘ **Note:**
- This feature supports Illustra cameras that support the iAPI3 device handler only. For a list of supported Illustra cameras, refer to the *VideoEdge Camera Handler Release Notes*.
- For more information on accessing this feature in victor Client, refer to the *victor User Guide.*

Using Direct Camera Access

1. Expand the **Devices** menu, and then click **List**.
2. From the **Video List** page, select the camera that is being configured and then click the **Setup** icon.
   The **Functions & Streams** tab opens.
3. **Optional:** Complete the **Function Configuration** section and the **Stream Configuration** section.
4. From the **Direct Camera Access** section:
   a. Click **Configure** to open the camera Web GUI. User login credentials are entered

automatically.

b. Click **Log In Page** to open the camera Web GUI landing page. Change the Web GUI language from the **Language** list.

ⓘ **Note:**

- Direct Camera Access appears disabled if the camera does not support this feature.
- Camera firmware upgrade is only supported using victor and VideoEdge Administration Interface.

Wearable and Illustra body worn cameras

You can add wearable cameras and Illustra body worn cameras to VideoEdge and view the retrieved video clips in victor Client.

- **Wearable cameras:** video clips are added to VideoEdge using a supported wearable camera management system. A security group specifies the user name 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*.

- **Illustra body worn cameras:** video clips are added to VideoEdge using a supported Illustra body worn camera management system. A security group specifies the user name and password that VideoEdge uses to communicate with the supported camera management system.

  ⓘ **Note:** For more information on supported Illustra body worn cameras management systems, refer to the *Illustra Body Worn Camera Configuration Guide*.

To add a wearable or Illustra body worn camera to VideoEdge, you must create a security group. You can add a security group before you add the camera to VideoEdge, as outlined in Creating a security group for a wearable or Illustra body worn camera. You can also create a security group while adding the camera to VideoEdge, as outlined in Adding a wearable or Illustra body worn camera.

ⓘ **Note:** Each wearable camera or Illustra body worn camera requires one IP camera license.

Creating a security group for a wearable or Illustra body worn camera

1. Expand the **Devices** menu, and click **Security**.
2. Click the **Add New Group** icon.
3. In the **Security Group** window, in the **Group Name** and **Description** fields, enter the appropriate information.
4. In the **Username** and **Password** fields, enter the user name and password that VideoEdge uses to communicate with the supported camera management system whose cameras are to added to VideoEdge.
5. **Optional:** To configure the **Advanced Settings**, complete the following steps:
   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, select the **Default** check box.
6. Click the **Save** icon.

Adding a wearable or Illustra body worn camera

1. Expand the **Devices** menu, and click **List**.

2. Click the **Add New Device** icon.
3. In the **Add Device** window, in the **Device Name** field, enter a device name.
4. In the **Device Address** field, enter the IP address of the supported camera management system.
5. In the **Security Group** list, select one of the following options:
   - The name of the security group that you previously created.
   - **New Security Group:** more options display in the **Add Device** window.

   ⓘ **Note:** For information, see Creating a security group for a wearable or Illustra body worn camera.
6. Click **Additional Settings** and more options display in the **Add Device** window.
7. From the **Device Type** list, select one of the following options:
   - If you are adding a wearable camera, select **Wearable Camera**.
   - If you are adding an Illustra body worn camera, select **Illustra Body Worn Camera**.

   ⓘ **Note:** If you select the incorrect device type, an error dialog appears indicating that you must select the correct device type.
8. From the **Slot** list, select a device slot.

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

Result
When VideoEdge successfully adds the wearable or Illustra body worn cameras, they display on the **Video List** page.

Video upload status for wearable or Illustra body worn cameras

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

1. Expand the **Devices** menu, and click **Options**.
2. To view the video upload status, click the **Wearable Cameras** tab.
   The **Video Upload Status** page opens and displays the **Video Upload Status** table for each camera.

   Table 18: Video upload status table

Name	Description
Camera	Name of the wearable or Illustra body worn camera.
Video	Size of the video file, and start and end times of the video recording.
Retrieval	Start and end times for retrieving the video from the camera management system.
Storage	Start 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 analytic events

Edge analytic events are camera-based analytic operations that occur when a camera detects noteworthy information. These events cause the camera to 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 the following edge analytics features:

- Edge-based events: Edge-based events occur when a camera detects noteworthy information.
- **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.
- **Edge Audio Analytics:** Audio Analytics track edge event detection for significant audio events.

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 modes 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, configure your camera recording mode 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.

Multi-channel edge analytics

VideoEdge can connect to an Illustra Multisensor camera to receive edge analytic alerts and metadata for multiple channels. Each channel generates its own alarms and metadata information for each of its analytic event types.

Enabling edge analytics on a camera

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. After you configure edge based analytics, you can enable the NVR to use edge based analytic features on the configured camera using the Device List page, the Function and Stream settings tab in the camera setup pages, or 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.
If the firmware on the camera and NVR are not compatible, the NVR uses the older edge assisted re-identification feature which is more resource-intensive. A clickable compatibility warning appears to inform you of this.

1. Expand the **Devices** menu, and then click **List**.
2. Select the camera you want to configure and then click the **Setup** icon.
3. Set the camera **Record Mode** to a setting that supports edge based analytics (Only Record on Alarm, or Recording Always with Alarm On).
4. From the **Video Analysis** list, select **Edge Based**.

   ⓘ **Note:** To ensure the correct camera configuration is used for edge analytics, refer to the *Camera Handler Release Notes*.

5. Click the **Save** icon.

Disabling a video analytic on a camera

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

1. Expand the **Devices** menu, and then click **List**.
2. Click the **Setup** icon in the camera row where you want to disable the video analytic.
3. Select **None** from the **Video Analysis** list.
4. Click the **Save** icon.

Audio analytics

Audio Analytics offer an edge generated alert when enabled on a device connected to VideoEdge. The analytics track edge event detection for significant audio.

Camera audio alerts will populate on victor when the camera has been triggered by a significant audio event such as when glass breaks.

Enabling Audio Analytic Alerts

Before you begin:

- Make sure the camera supports audio analytics, for example Illustra Pro Gen 4.
- Upgrade the camera to the latest firmware.
- Upgrade VideoEdge to the latest build.
- In victor, upgrade to the latest build on vAS and victor Client.

About this task:

You can enable audio analytics on devices in the Video List from the Advanced configuration menu.

1. After adding a new camera, from the prompt screen or the **Video List** select the **Setup** icon on the device you want to configure to open the **Functions and Streams** page.
2. From this page **Enable Edge Alerts**.
3. Select **Record Always** with **Alarms** for the Record Mode and **Edge Based** for the Video Analytics.
4. Click **Save** and click **Alarms: Configure**.
5. On the **Alarms** page select **Edge Sound Detection Alarms**, click **Enable** and **Save**.
6. Audio Analytic alerts are now enabled.

ⓘ **Note:** Before enabling audio analytics alerts, you must enable audio analysis, upgrade your videoedge to the latest version and add the camera to videoedge.

Edge analytics metadata

When objects are detected using Video Intelligence and Motion Detection, for each object recorded, VideoEdge generates metadata to define the object and stores the object metadata. VideoEdge also detects further information on these defined objects giving more detailed insights into their characteristics.

ⓘ **Note:** This can only be achieved using cameras that are capable of color detection, including the Illustra Pro Gen 4. Edge analytics must be enabled see Edge assisted Intelligent Search

The VideoEdge collects information on the following object characteristics:

- Vehicles: color
- Person: upper clothing color, lower clothing color

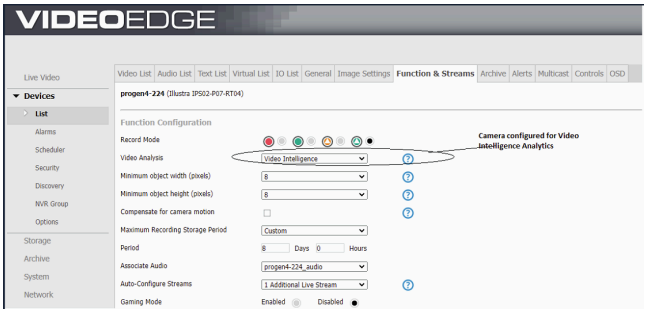
When an object is classified by color, this is done in two ways:

- On a per frame basis
- An agregate of the most prevalent color detected

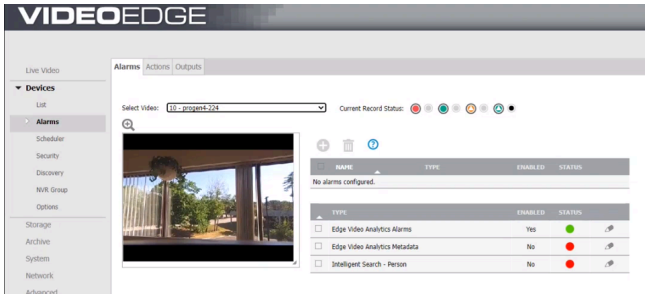
Edge-based alarms with video intelligence or motion

About this task:
When a camera is configured for video intelligence analytics or motion detection, it is possible to enable any edge-based alarms that are supported on that camera.

1. From the **Devices** list, on the **Functions and streams** tab, use the **Video Analysis** drop down to select video intelligence or motion detection.



2. If a camera supports edge-based alarms, configure the alarms with the following steps:
   a. From the **Devices** list, select **Alarms**to configure the alarms for this device.
   b. From the **Select video** list, select the stream you wish to configure.
   c. From the **Type** window edit the alarms or view their status from the . Choose to enable or disable any of the available alarm types.



Mask Detection

VideoEdge can connect to an Illustra Thermal camera to receive mask detection alarms using edge based face detection analytics.

Enabling Mask Detection analytics on an camera

Before you begin:
Enable edge based face detection alarms and mask detection alarms on the Illustra Thermal camera. For more information, refer to the relevant Illustra Thermal Camera user manual.

1. Enable edge based analytics for the Illustra Thermal camera. For more information, see Enabling edge analytics on a camera.
2. Expand the **Devices** menu, and then click **Alarms**.
3. From the **Select Video** list, select the camera you are configuring.
   The camera's **Edge Face Detection Alarm** displays.
4. Click the **Edit** icon.
5. In the **Enabled** section, click **Yes** and then click the **Save** icon.

   ⓘ **Note:** When you open the configured camera on the **Alarms** page, the status light is green when the Edge Face Detection Alarm is enabled.

Illustra Secure Video

You can stream videos from supported Illustra cameras with secure and encypted protocols by choosing a Security Streaming Level.

Security Streaming Level

There are three Streaming Security Levels available: Default: Prefer Secure, Force Secure, and Prefer Insecure. You can configure the Streaming Security Level when you add a device or create a security group. For more information, see Manually adding an IP device, and Creating a security group.

ⓘ **Note:**

- If a camera and its handler supports secure streaming (any type of encrypted streaming), VideoEdge will stream secure video when the Prefer Secure or Force Secure option is selected.
- If a camera and its handler does not support secure streaming and Force Secure is selected, an error message displays and the camera will fail to be added.

Illustra Auto Security

Illustra Auto Security enables the auto configuration of an Illustra camera when it is added to the NVR. When you create an appropriate Security Group for the camera, you can set it as Standard Security Mode or Enhanced Security Mode. Adding an Illustra camera to the NVR using this Security Group will automatically push the security credentials to the camera and speed up deployment.

ⓘ **Note:** This feature is currently only supported by Illustra Pro 4 cameras.

Configuring Illustra Auto Security

Before you begin:
Assign an IP address to the camera in the appropriate network. The NVR needs access to this network.

1. Expand the **Devices** menu, and then click **Security**.
2. Click the **Add New Group** icon.
3. Enter a name and description in the **Group Name** field and **Description** field.
4. In the **Username** field:
   a. **For Standard Security Mode:** Do not change the default username: `admin`
   b. **For Enhanced Security Mode:** Enter a new username in the **Username** field.
5. Enter a new password in the **Password** field.
6. Select **Advanced** to configure advanced settings.
7. From the **Security Level** list:
   a. **For Standard Security Mode:** Select **Default** or select **Low (HTTP/Basic)**.
   b. **For Enhanced Security Mode:** Select **High (HTTPS)**.
8. Click the **Save** icon.

To add the Illustra Pro 4 camera to the NVR using the Security Group:

9. Expand the **Devices** menu and then click **List**.
10. Click the **Add New Device** icon.
11. Enter a name for the camera in the **Device Name** field.
12. Enter the camera IP Address in the **Device Address** field.
13. From the **Manufacturer** list, select `Illustra/American Dynamics`.
14. From the **Security Group** list, select the new Security Group.
15. Click the **Save** icon.

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.

Configuring Audio association

1. Expand the **Devices** menu, and then click **List**.
2. Click the **Setup** icon in the camera row you want to edit audio settings. The **Function and Streams** tab displays.
3. Select the audio device you want to associate with the camera from the **Associate Audio** menu.
4. Click the **Save** icon.

Enabling or disabling auto-configure streams

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

from the **Auto-Configure Streams** list as follows:

- **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.

Gaming Mode

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

Stream configuration

Stream configuration defines which stream is used for live video, alarms and recording. The NVR will automatically determine the best stream to use for Motion Detection or Video Intelligence. You can also adjust the codec, FPS and resolution of each stream. Depending on what is assigned to a stream, you must have the appropriate codec, FPS and resolution assigned. For example, for Video Intelligence, use a stream that is MJPEG or MPEG-4, with at least a 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*.

Configuring stream settings

1. Expand the **Devices** menu, and then click **List**.
2. Click the **Setup** icon in the camera row for which you want to edit stream settings.
3. Select the stream you want the camera to use for:
   a. Live video
   b. Alarms
   c. Recording
4. Select the **Codec** for each stream:
5. Select the **FPS** for each stream.
6. Select the **Resolution** for each stream.
7. If you are using a stream for analytics, select the **Quality**.
8. If you are configuring an analog camera, complete the following steps:
   a. Select the **Bit Rate Control**.
   b. Enter the **Max Bit Rate**.
   c. Select the **Profile**.

9. Click the **Save** icon.

General object classification

The general object classification feature extends existing analytic searches and alerts to support object class parameters.

The general object classification feature encompasses Tyco AI support. Server-side alarms for edge analytics, and new object class-based filtering for many searches and alerts.

Using a Tyco AI server for object classification

To use one or more Tyco AI servers to support object classification, you must configure the servers on the VideoEdge NVR.

1. Expand the **Devices** menu, and click **Options**.
2. Click the **Tyco AI Servers** tab.
3. To add a Tyco AI server, click the **Add** icon.
4. In the **Add Tyco AI Server** window, complete the following steps:
   a. In the **Server Address** field, enter the address of the device.
   b. From the **Security Group** list, select a security group.

      ⓘ **Note:** The security group identifies the credentials used to connect and communicate to the Tyco AI server. You can use an existing security group or define a new security group.

   c. To complete the **Security Group Details** area, refer to the *Tyco AI Server User's Guide* for details regarding configuring credentials.
   d. To configure the Tyco AI server, click the **Save** icon. The VideoEdge NVR attempts to connect to the server using the specified address and credentials.
5. Verify that the server appears in the list of configured servers. Each Tyco AI server entry displays its unique Host ID, server address, associated security group, its available camera capacity, and the current connection status.

   ⓘ **Note:** The available capacity figure indicates the number of available camera licenses that the VideoEdge NVR can access. This number determines how many VideoEdge NVR camera devices can be configured to use the Tyco AI metadata engine.

6. To modify the security group associated with this server, click the **Edit** icon.

Configuring security groups for Tyco AI servers

You can configure multiple security groups to be associated with Tyco AI servers.

1. Expand the **Devices** menu, and click **Options**.
2. Click the **Tyco AI Servers** tab.
3. Click **Manage Security Groups**.
4. Use the **Manage Tyco AI Server Security Groups** window, to add new security groups, modify existing security groups, or delete security groups.

Enabling a camera for Tyco AI Analytics

Use the Tyco AI Analytics mode to configure alarms and searches that use various video intelligence rules with the additional capability to specify object classification parameters.

ⓘ **Note:** The live configured stream is processed by the Tyco AI server and indicated as the analytics stream. The minimum 10 FPS and 640 x 450 resolution is required to use this mode on the user configured live stream.

1. Expand the **Devices** menu, and click **Lists**.
2. Access the camera's **Functions & Streams** tab.
3. In the **Function Configuration** area, from the **Video Analysis** list, select **Tyco AI Analytics**.

   ⓘ **Note:** The Tyco AI Analytics option is disabled if there are no Tyco AI servers configured or if there is no capacity on any of the configured servers.
4. Click **Configure**.

Configuring alarms for Tyco AI Analytics enabled cameras

ⓘ **Note:** Not all rule types support object classification. The option to configure object classification related parameters is available only to those that support it.

1. Expand the **Devices** menu, and click **Alarms**.
2. From the **Select Video** list, select the camera that you require. Create and configure the rules the same as for the existing video intelligence alarms, but with the additional ability to configure object classification parameters.
3. To add a new rule, click the **Add** icon.
4. From the **Object Class** list, select the required object classes.

   ⓘ **Note:** The list of available object classes is determined by those supported by the existing Tyco AI server engine.
5. Select one of the following check boxes:
   - **Include:** to trigger an alarm for only the objects specified.
   - **Exclude:** to trigger an alarm for any objects other than the objects specified.
6. In the **Confidence** area, set the confidence that the object identified matches the selected class.

Enabling Edge-based cameras for object classification

To support the ability to configure existing video intelligence alarms and searches with object classification, use the Edge-based analytics mode. Enable this mode to configure alarms and searches that use various video intelligence rules with the additional capability to specify object classification parameters.

ⓘ **Note:** To support the use of object classification with alarms, you must enable AI Object Classification on the Edge camera.

1. Expand the **Devices** menu, and click **Lists**.
2. Access the camera's **Functions & Streams** tab.
3. In the **Function Configuration** area, from the **Video Analysis** list, select **Edge Based**.
4. Click **Configure**.

Configuring alarms for Edge-based cameras

ⓘ **Note:** To configure video intelligence rules with optional object classification, you must enable Edge video analytics metadata.

1. Expand the **Devices** menu, and click **Alarms**.
2. From the **Select Video** list, select the camera that you require.
3. To add a new rule, click the **Add** icon.

4. From the **Object Class** list, select the required object classes.
5. Select one of the following check boxes:
   - **Include:** to trigger an alarm for only the objects specified.
   - **Exclude:** to trigger an alarm for any objects other than the objects specified.
6. In the **Sensitivity** area, increasing the sensitivity generally increases the total number of alarms, at the risk of including more errors. Tuning for each application is recommended.

Defog mode

Use the Image Settings page to apply Defog mode to a camera. Defog mode improves the image quality in poor weather conditions by using an image processing algorithm. An image of a raining or foggy environment can lose contrast, and appear pale, lacking detail, lacking strong blacks or whites, and contain a high gray content. When you apply defog mode, each selection dynamically alters the actual amount of the defog function that is applied to an image, it changes as the scene changes.

Use defog mode on the Illustra Pro 4 camera to determine if the contrast in an image requires adjustment. Support for additional cameras is added to upcoming handler releases. If Defog mode support on VideoEdge has not been implemented for a given camera, on the Image Settings page for that camera, the Defog Mode fields are hidden. For updated Defog mode support information, refer to the *Camera Handler Release Notes*.

ⓘ **Note:** Smart defog has some limitations and is not available when used with Certain Dynamic Ranges.

To apply smart defog to an image, choose from the following levels:

- **Off:** no defog action.
- **Low:** defog action can dynamically be between 2 and 5, depending on the scene.
- **Mid:** defog can be between 2 and 7.
- **High:** defog can be between 2 and 9.

If you test smart defog without fog, you see a change in the camera image when going from Off to Low, when enabled, gamma and mid tone contrast are altered for increased clarity.

In the following images you can see how to use of smart defog in an image with heavy drizzle. When you set the smart defog to mid you can see the trees in the background, and increasing it to high provides more detail everywhere in the image.

Figure 10: Defog mode: off

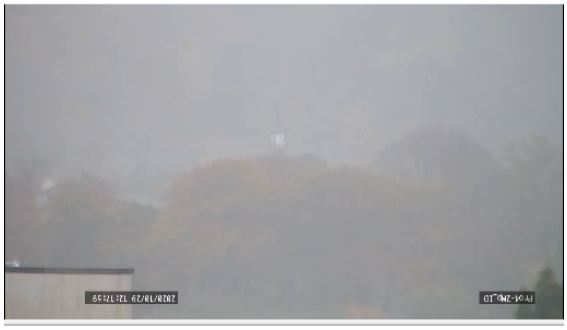


Figure 11: Defog mode: low

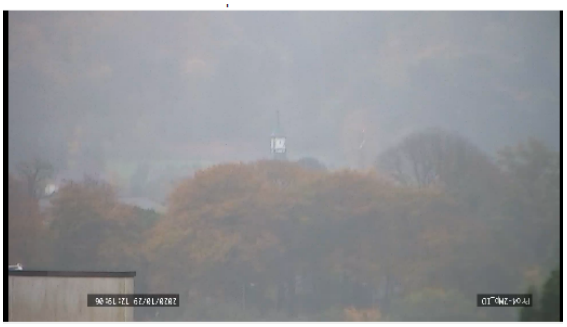


Figure 12: Defog mode: mid

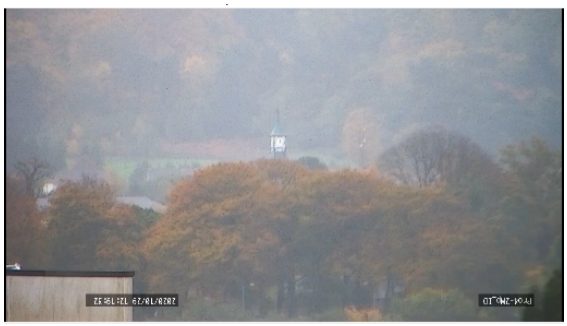
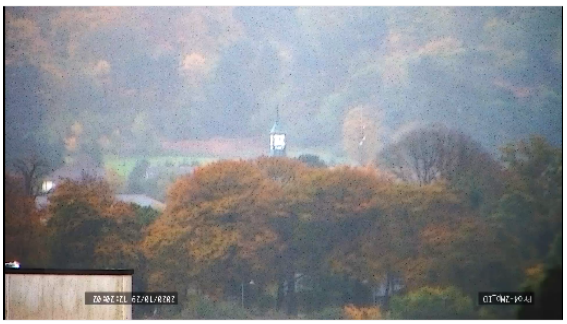


Figure 13: Defog mode: high



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 frame rate decimation using the Archive Quality menu and define a maximum retention period for archived video.

Configuring archive settings

1. Expand the **Devices** menu, and then click **List**.
2. Click the **Setup** icon in the camera row for which you want to edit the archive mode.
3. Click the **Archive** tab.
4. Select the **Archiving Mode** as follows:
   - **Archiving disabled** disables archiving for the camera.
   - **Archive all video** archives all video for the camera.
   - **Archive only alarm video** archives video triggered with an alarm.
5. Select the **Archiving Quality** from the list.
6. Select the **Maximum Archiving Storage Period** from the list.
7. **Optional:** If you select **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.

Configuring alert recording buffers

1. Expand the **Devices** menu, and then click **List**.
2. Click the **Setup** icon in the camera row for which you want to set alert recording buffers.
3. Click the **Alerts** tab.
4. Select the **Alert Pre-Buffer** time from the list.
5. Select the **Alert Post-Buffer** time from the list.
6. Click the **Save** icon.

Multicast streaming

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.

Configuring multicast stream settings

1. Expand the **Devices** menu.
2. Click **List**.
3. Click the **Setup** icon for the multicast camera that you want to configure.
   The Function & Streams page opens.
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.

Enabling or disabling PTZ for cameras

1. Expand the **Devices** menu, and then click **List**.
2. Click the **Setup** icon in the PTZ camera row.
   The **Function & Streams** page opens.
3. Click the **Controls** tab.
4. Depending on whether you are using an analog camera or an IP camera, complete one of the following steps:
   - **Analog camera:** Select the **PTZ Port** from the list to enable PTZ, or select **None** from the list to disable PTZ.
   - **IP Camera:** Select the **Enable PTZ** check box to enable PTZ, or deselect the **Enable PTZ** check box to disable PTZ.
5. Click the **Save** icon.

Enabling or disabling PTZ for analog cameras

1. Expand the **Devices** menu, and then click **List**.
2. Click the **Setup** icon in the PTZ camera row.
3. Click the **Controls** tab.
4. Depending on whether you are using an analog or an IP camera, complete one of the following steps:
   a. For IP cameras, select the **Enable PTZ** check box to enable PTZ, or deselect the **Enable PTZ** check box to disable PTZ.
   b. For analog cameras, select the PTZ Port from the list to enable PTZ, or select **None** from the list to disable PTZ.
5. 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.

Enabling PTZ Return to Home

1. Expand the **Devices** menu, and then click **List**.
2. Click the **Setup** icon in the PTZ camera row for which you want to enable the **Return to Home** feature.
3. Click the **Controls** tab.
4. Select the **Enable PTZ** check box for IP Cameras, or select the **PTZ Port** from the list for analog cameras.

5. Select the **Enable Return to Home** check box.
   The **Return to Home After** list displays.
6. Select the required period of inactivity before the camera returns to the home position from the **Return to Home After** list.
7. Click the **Save** icon.

Intelligent Guard Tour

You can enable an Intelligent Guard Tour for supported PTZ cameras. An Intelligent Guard Tour 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 an Intelligent Guard Tour feature:

- Configure a guard tour for the camera through victor or through the camera's web interface.
- Set the PTZ Home position for the PTZ camera.

Enabling an Intelligent Guard Tour

1. Expand the **Devices** menu, and then click **List**.
2. Click the **Setup** icon in the PTZ camera row that you want to configure.
   The **Function & Streams** page opens.
3. Click the **Controls** tab.
4. Select the **Enable Intelligent Guard Tour** check box.
5. Click the **Save** icon.

Intelligent Guard Auto Track

ⓘ **Note:** Intelligent Guard Auto Track is supported on Illustra Pro Gen 4 PTZ cameras only.

You can set the Intelligent Guard Auto Track mode to person based, face based, or off:

- **Person based:** Enables the AI object classification analytic on the camera and the person based auto track itself.
- **Face based:** Enables the face detection analytic on the camera and the face based auto track itself. You must install a face detection license to use this setting.
- **Off:** Disables auto track mode. This will not turn off the face detection analytic or AI object classification analytic.

Configuring Intelligent Guard Auto Track

1. Expand the **Devices** menu, and then click **List**.
2. Click the **Setup** icon in the supported camera row that you want to configure and then click the **Controls** tab.
3. From the **Intelligent Guard Auto Track mode** list, select the appropriate setting.

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.

Configuring camera PTZ for an analog matrix

1. Expand the **Devices** menu, and then click **List**.
2. Click the **Setup** icon for the camera you want to configure PTZ settings for analog matrix.
3. Click the **Controls** tab.
4. Select the correct camera control port from the **PTZ Port** list.
5. Enter the **PTZ Address**.
6. If required, select **Enable Camera Menu** check box to allow camera menu access on the PTZ / Keyboard controls.
7. Enter the **Matrix Monitor Number**.
8. 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.

Configuring Fisheye Mode

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

Preset control settings

From the Controls page, you can configure preset control settings for supported PTZ cameras.

In the Preset Control Settings area, you can assign features 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 feature.

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 and Illustra cameras are supported.

Configuring preset control settings

1. Expand the **Devices** menu, and then click **List**.
2. Click the **Setup** icon in the camera row that you want to configure, and then click the **Controls** tab.
3. In the **Preset Control Settings** section, select the required settings for the following:
   - Wiper Preset
   - Speed Dry Preset
   - PTZ Shake Dry Preset

- Auto Focus Preset
- IR Illumination Toggle Preset

4. Click the **Save** icon.

On-screen display

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 global OSD settings

1. Expand the **Devices** menu, and then click **List**.
2. Click the **Setup** icon of the analog camera you want to configure OSD settings for.
3. Click the **OSD** tab.
4. Select the **Font** from the list.
5. Enter the hex value for the font in the **Color** field, or click the **Color** field and select the color using the palette.
6. Select the **Timestamp** format using the **Timestamp Format** list.
7. Click the **Save** icon.

Configuring camera specific OSD settings

1. Expand the **Devices** menu, and then click **List**.
2. Click the **Setup** icon of the analog camera you want to configure.
3. Click the **OSD** tab.
4. Click the **Edit** icon to configure the OSD Position.
5. Select the **Enabled** check box.
6. Enter required value in the **Text** field.
7. Use the slider to set the **Transparency**.
8. **Optional:** Select the **Blink** check box.
9. **Optional:** Select the **Timestamp** check box.

   ⓘ **Note:** You must have a global time stamp selected to allow you to enable a time stamp on an individual OSD item.

10. Click the **Save** icon.

OSD inserts

OSD inserts are predefined text commands that 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 displays the following information:

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

- **%PTZ%:** 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 is added a dialog window will summarize the settings which have been successfully applied and those that cannot be applied.

ⓘ **Note:** When carrying out device replacement for a camera that uses 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 is important to also consider the associations that are currently configured on your NVR. Associations configured on the NVR will be maintained by default when a device is replaced except 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. After repairing the device, reconnect it to the NVR. 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

1. Expand the **Devices** menu, and then click **List**.
2. Click the **Edit** icon in the row of the device you want to replace.
3. Enter the IP address of the new device.
4. Click the **Save** icon.
5. Click **OK**.

Replacing an IP text device

1. Expand the **Devices** menu, and then click **List**.
2. Click the **Text List** tab.
3. Click the **Edit** icon in the row of the device you want to replace.
4. Enter the **Port** number being used by the new device.
5. Click **Apply**.

Replacing multi-channel encoders

Multi-channel encoders are recognized as multiple devices by the NVR. For example, an eight channel encoder will occupy eight slots in the device list. You can use the device replacement feature to perform individual channel replacement, or an encoder-for-encoder swap.

- **Replacing an encoder channel with an IP device:** Analog devices connected using 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 performed.

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 14: Alarms page

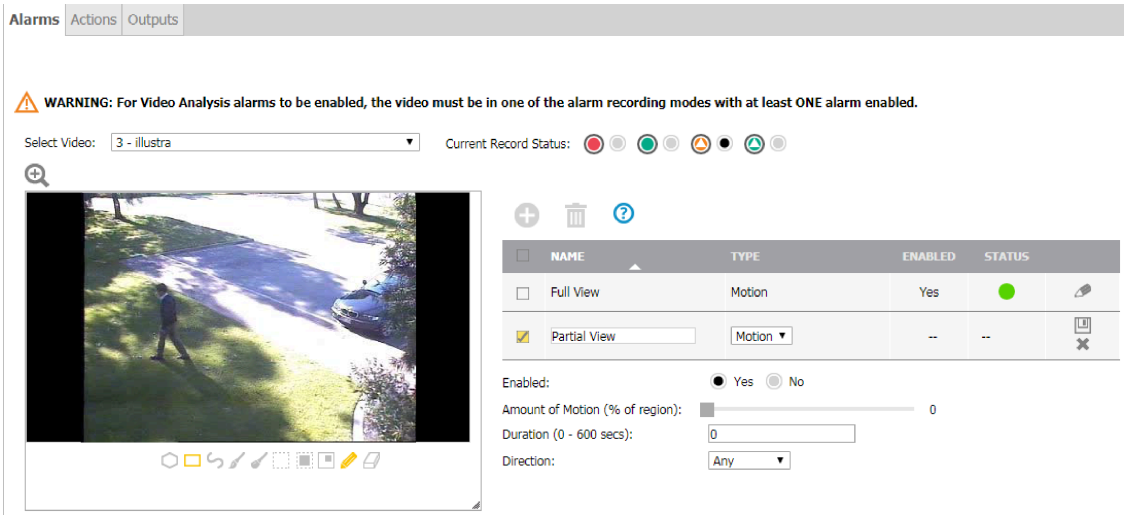


Table 19: Alarms page

Field	Description
Select Video	Select the camera 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 • Recording Always with Alarms
Drawing window	Use the drawing tools to configure the areas 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 as follows:. • **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.

Drawing tools

Figure 15: Drawing tools

Table 20: 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 21: Alarms icons

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

Table 21: Alarms icons

Icon	Name	Function
	**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', because 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 alarm

When creating a Motion Detection camera alarm, 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, enable Motion Detection on the camera. If you try to add a camera alarm without Motion Detection enabled, you are prompted to edit the camera settings.

1. Expand the **Devices** menu, and then click **Alarms**.
2. Select the camera for which you want to create an alarm from the **Select Video** list.
3. 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.
4. 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.
5. Enter an alarm **Name** (max 50 characters).
6. Click the **Yes** button in the **Enabled** area to enable the alarm.
7. 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.
8. Use the drawing tools to draw the Motion Detection region of interest (ROI) in the Camera Alarm Configuration drawing window.

   ⓘ **Note:** You must define an ROI.
9. 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.
10. 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.

11. 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.
12. 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.

Video Intelligence and Deep Intelligence alarm types

Table 22: Video Intelligence and Deep Intelligence alarms types

Alarm type	Description	Configuration
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.	**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	For 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.	**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. **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. **Fast Trigger:** Enables 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. **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. **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.

Table 22: Video Intelligence and Deep Intelligence alarms types

Alarm type	Description	Configuration
Direction	Used to detect objects moving in a certain direction through a region of interest, for example, a car traveling in the wrong direction on a road. It is best to use a thin region of interest to detect the direction of an object.	**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. **Direction:** This is the general direction the object must move in to trigger an alarm. You can choose North, South, East, or West. **Traversal Time:** The maximum amount of time 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	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.	**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. **Linger Time:** The minimum amount of time an object lingers before the alarm is triggered.
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.	**Overlap (%):** The amount of a detected object that must dwell in the region of interest for an alarm to be triggered. **Dwell Time:** The minimum time an object must dwell in the region of interest before the alarm is triggered.

Table 22: Video Intelligence and Deep Intelligence alarms types

Alarm type	Description	Configuration
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.	**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 three zones must be defined. Each selection is highlighted using a different color; Short is green, Medium is yellow and Long is purple). **Overlap (%):** The amount of detected object that must be in the region of interest to be identified as a person in a queue. **Queue Length:** The required minimum length for an alarm to be generated. The following options are available: • **Empty:**Generates an alarm when no objects are present in the designated regions of interest. • **Not Empty:** Generates an alarm when objects are present in the designated regions of interest. • **Short:** Generates an alarm when objects are present in the short designated region of interest and meet the overlap requirements. • **Medium:** Generates an alarm when objects are present in both the short and medium designated regions of interest and meet the overlap requirements. • **Long:** Generates an alarm when objects are present in the short, medium, and long designated regions of interest and meet the overlap requirements.
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.	**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 using a different color (perimeter area = green, protected area is yellow, minimum object size is purple, and maximum object size is red). **Linger Time:** The minimum time an object lingers before the alarm is triggered.

Table 22: Video Intelligence and Deep Intelligence alarms types

Alarm type	Description	Configuration
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 two people at any given time the minimum crowd size should be set to three.	**Overlap (%):** The amount of detected object that must be in the region of interest to be considered for determining the crowd size. **Minimum Crowd Size:** The minimum number of people that must be present to generate an alarm. This can be between 2–50 people.
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.	**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	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.	**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	Used to count the number of people that cross a region of interest. 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.	**Count Threshold:** Adjust the slider to configure the count threshold. When the threshold is reached, the counter will reset to zero. **Reset Time:** Enter a time in the 24-hour format. At the reset time, the running total resets.

ⓘ **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.

Creating a Video Intelligence or Deep Intelligence camera alarm

To create a Video Intelligence camera alarm, enable Video Intelligence on the camera. If you try to create a Video Intelligence alarm for a camera without Video Intelligence enabled, you are prompted to edit the camera settings.
To create a Deep Intelligence camera alarm, enable Deep Intelligence on the camera. Deep Intelligence is only available on supported NVRs, with an integrated GPU card. If you try to create a Deep Intelligence alarm for a camera without Deep Intelligence enabled, you are prompted to edit the camera settings.

1. Expand the **Devices** menu, and click **Alarms**.
2. Select the camera for which you want to create an alarm from the **Select Video** list.
3. 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.
4. 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.
5. Enter an alarm **Name** using a maximum of 50 characters.
6. To enable the alarm, in the **Enabled** area click the **Yes** button.
7. Select the alarm type from the **Type** list. For more information, see the Video Intelligence and Deep Intelligence alarm types table.
8. 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.
9. Click the **Yes** button in the **Enabled** area, to enable the alarm.
10. Complete the alarm configuration fields. For more information, see the Video Intelligence and Deep Intelligence alarm types table.

    ⓘ **Note:** 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.
11. 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.

Creating a Face Recognition camera alarm

1. Expand the **Devices** menu, and click **Alarms**.
2. Select the camera for which you want to create a **Face Recognition** alarm from the **Select Video** list.
3. 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.
4. 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.
5. Enter an alarm **Name** using a maximum of 50 characters.
6. To enable the alarm, in the **Enabled** area click the **Yes** button.
7. 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.
8. Select entries from the Enrollment List to be included or excluded in the Search List using the **Left Arrow** icon and **Right Arrow** icon.
9. Click the **Save** icon.

License plate recognition

License plate recognition is a licensable feature that detects license plate numbers and compares 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.

Table 23: Wildcard characters

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

In the previous examples, 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 Matching enables matching on commonly unrecognized 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:

- 0, D, O, Q
- 1, 7, I
- 2, Z
- 8, B

Creating a License Plate Recognition alarm

When creating a License Plate Recognition camera alarm:

- 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.
- Enable License Plate Recognition on the camera. If you try to add a camera alarm without License Plate Recognition enabled you are prompted to edit the camera settings.

1. Expand the **Devices** menu, and then click **Alarms**.
2. Select the camera that you want to create a license plate recognition alarm for from the **Select Video** list.
3. Click the **Add** icon.
4. 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.
5. Enter an alarm **Name** (maximum 50 characters).
6. Click the **Yes** button in the **Enabled** area to enable the alarm.
7. Select the required **Overlap** range.

   ⓘ **Note:** The Overlap range is used to determine how much of the license plate needs to be in the region of interest in order to trigger an alarm. For example, if overlap is set to 1%, only a very small proportion of the license plate would need to enter the area of interest to trigger the alarm. If overlap is set to 100% the entire license plate would need to be in the region of interest to trigger an alarm.
8. Select 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.
9. **Optional:** Select the **Fuzzy Match** check box if required.
10. 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.
    An alternative way to import a list of license plate numbers is click **Choose File**, navigate to the required text file, and click **Open**.
11. Use the drawing tools to select an alarm's region of interest in the drawing window.

12. 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 numerous types of edge based analytic events supported by the NVR: edge audio analytics, video intelligence, 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, Edge Audio Analytics or Motion Detection metadata in the alarms table to allow camera-based searches using this metadata in victor unified client.

ⓘ **Note:** Edge analytics metadata will be recorded if the camera recording status is set to Recording Always, Only Record on Alarm, or Recording Always with Alarms.

1. Expand the **Devices** menu, and then click **Alarms**.
2. Click the **Edit** icon for the camera alarm or metadata you want to enable.
3. Click the **Yes** button in the **Enabled** area.
4. 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

Before you begin:
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. Expand the **Devices** menu, and click **Alarms**.

   ⓘ **Note:** You can also open the Alarms page after enabling Edge analytics. When you have completed the setup on the Functions and Streams page, click **Configure Alarms**.
3. From the **Select Video** list, select the camera you are configuring. The camera's **Edge Face Detection Alarm** displays.
4. Click the **Edit** icon.
5. In the **Enabled** section, click **Yes**.
6. 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.

Configuring edge object classification

You can configure edge object classification or sub-classification, such as color, on an Illustra Pro 4 camera and compatible Axis cameras in VideoEdge. An alert sends to victor when an object is

detected using edge analytics. For more information, refer to the *Edge Object Classification* section of the *victor Administration Guide*.

ⓘ **Note:** This feature supports Illustra Pro 4 and compatible Axis cameras only. For information on which Axis cameras are compatible, refer to the Axis website, https://www.axis.com/products/axis-object-analytics#compatible-products.

Configuring Object Classification alarms

1. Expand the **Devices** menu, click **List**, and then click **Functions & Streams**.
2. In the Record Mode section, select **Record Only on Alarm** or **Record Always with Alarms**.
3. From the **Video Analysis** list, select **Edge Based**.
4. In the **Alarms** section, click **Configure**.
5. In the **Type** section, enable the following edge alarms:
   - Edge Video Analytic Alarms
   - Edge Video Analytics Metadata

   ⓘ **Note:** For more information on edge based alarms, see Edge analytics.

Disabling a camera alarm

When a camera alarm is not needed, but will be needed in the future, you can disable the alarm. The alarm configuration remains the same on the camera for when it is enabled again.

1. Expand the **Devices** menu, and then click **Alarms**.
2. Click the **Edit** icon of the alarm you want to disable.
3. Click the **No** button in the **Enabled** area.
4. Click the **Save** icon.

Events, rules, and 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. For more information on creating and configuring rules, see the Events, rules, and actions configuration table .

Events, rules, and actions configuration table

Table 24: Events, rules, and actions configuration

Rule	Action
Camera Recording	A change of input state initiates recording on the selected camera. ⓘ **Note:** 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 initiates recording on the selected camera. ⓘ **Note:** The camera must have its recording mode set to Record Only On Alarm. Recording, including Alarm Pre Buffer, will begin and continue indefinitely.

Table 24: Events, rules, and actions configuration

Rule	Action
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 when the door is opened. A second sensor entry is created using the Camera Stop Recording action when the state changes to low when 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.

Adding a rule

1. Expand the **Devices** menu, and click **Alarms**.
2. Click the **Actions** tab.
3. Above the **Rules** table, click the **Add** icon.
4. Enter a rule **Name**.
5. To enable the rule, in the **Enabled** area, click **Yes**, or to disable the rule, click **No**.
6. Above the **Triggers** table, click the **Add** icon.
7. From the **Event** list, select an event.
8. From the **State** list, select the state.
9. From the **Device** list, select a device.
10. From the **Alarm** list, select a value.
11. If required, in the **Interval (Sec)** field, enter the interval value.
12. **Optional:** Repeat Step 6 to Step 10 to add additional triggers. To remove a trigger, select the appropriate check box and click the **Delete** icon.
13. Above the Actions table, click the **Add** icon.
14. From the **Action** list, select an action. If PTZ to Preset is selected, the Value list displays.
15. From the **Device** list, select the device.
16. **PTZ to preset only:** From the **Value** list, select the preset number.
17. **Relay output only:** From the **Value** list, select **Off**, **On**, or **Pulse**.
18. **Optional:** Repeat Steps 13 to Step 17 to add additional actions. To remove an action, select the appropriate check box and click the **Delete** icon.
19. Click the **Save** icon.

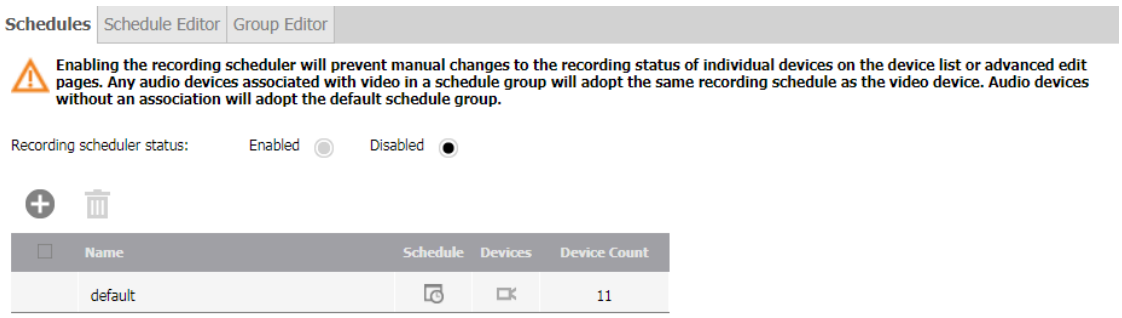
Outputs

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. Use a camera schedule to set the NVR to automatically change recording modes hourly. You can define camera recording modes and set camera recording times for scheduler groups. You can enable or disable the camera scheduler when necessary.

Figure 16: 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 25: 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.
	Edit group cameras	Open Group Editor to edit camera groups.
	Save	Save
	Cancel	Cancel

Table 25: Scheduler icons

Icon	Name	Function
	Right Arrow	Move selected cameras to a group.
	Left Arrow	Remove selected cameras from a group.
	**Edit**	Edit a schedule name.

Creating a recording schedule

1. Expand the **Devices** menu, and then click **Scheduler**.
2. Click the **Add** icon.
   The new group is added to the schedule groups table.
3. Enter the Schedule **Name**.
4. Click the **Save** icon.
5. Select the **Edit Group Times** icon in the schedule group record you want to configure.
6. Select the option buttons representing the days for which you want to set the recording times and the recording mode.
7. Select the required **Recording Mode** option button:
   - **Recording Off**
   - **Recording Always**
   - **Only Record on Alarm**
   - **Recording always with alarms**
8. Select the times you want the recording mode to be active.
9. Click the **Save** icon.
10. **Optional:** To set other recording modes for different days and times, repeat steps 4 – 7 until the Schedule Times chart is set as required for the recording schedule group.
11. Select the **Group Editor** tab.
12. Select the cameras you want to be in this schedule group by selecting the check boxes 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.
13. Click the **Save** icon.
14. **Optional:** Repeat steps 2 – 11 to configure additional schedule groups for the camera schedule.

Enabling or disabling a camera schedule

1. Expand the **Devices** menu, and then click **Scheduler**.
2. To enable the camera schedule, select **Recording scheduler status: Enabled**.
3. To disable the camera schedule, select **Recording scheduler status: Disabled**.

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.

1. Expand the **Devices** menu, and then click **Scheduler**.
2. Click the **Schedule Editor** tab.

3. Select the group you want to edit from the **Group ID** list.
4. Edit the recording schedule as required by selecting the days, the recording mode, and start and end hours.
5. Click the **Save** icon.
6. **Optional:** If further changes are required repeat steps 4 and 5.

Editing the cameras assigned to a Schedule Group

About this task:
You can add or remove cameras to and from a schedule group as required.

1. Expand the **Devices** menu and then click **Scheduler**.
2. Click the **Group Editor** tab.
3. Select the group you want to edit from the menu list.
4. Select the required camera check boxes 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.
5. 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.

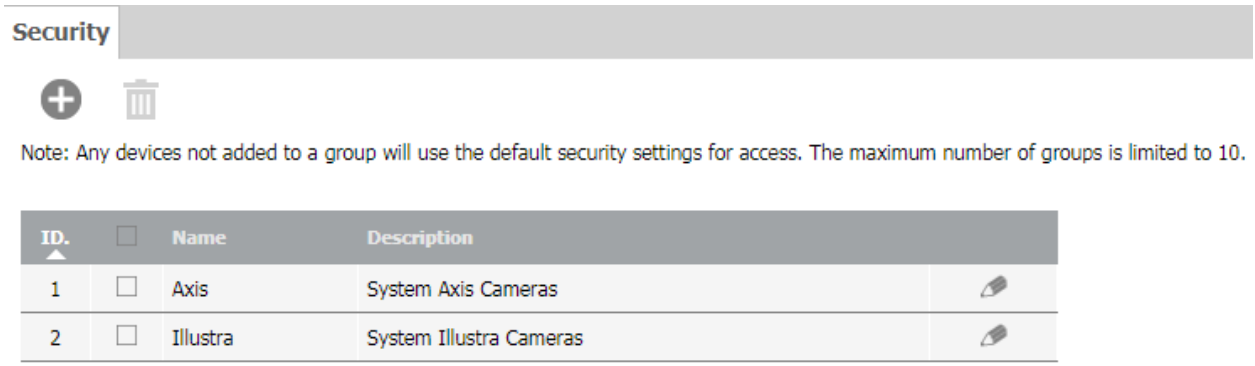
In addition to configuring the username and password, you can also configure the Port Number and Security Level used for communications.

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 17: Security page



Security icons table

Table 26: Security icons

Icon	Name	Function
	Add New Group	Add new security group.
	Remove Group	Remove security group.
	Password Reveal	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.

1. Expand the **Devices** menu, and click **Security**.
2. Click the **Add New Group** icon. The **Security Group** window opens.
3. Enter a **Group Name** and **Description** or leave the fields blank to use the camera's default credentials.
4. Enter a **Username** and **Password** or leave the fields blank to use the device's default credentials.

   ⓘ **Note:** This is the device username and password that the VideoEdge uses to connect to the devices in this security group.
5. **Optional:** Click and hold the **Password Reveal** icon, to view the password.
6. **Optional:** Click the tool tip button, to view more information on how to enable standard and enhanced auto configuration.

7. **Optional:** To configure **Advanced Settings**:
   a. Select **Advanced**.
   b. Select a **Streaming Security Level** from the list.
   c. **Optional:** For Illustra Auto Security, use the following settings.
      - For Standard security, select Default or Low (HTTP/Basic), use `admin` as the username, and choose a password..
      - For Enhanced security, select High (HTTPS), choose a username and password. Do not use `admin` as the username.

      ⓘ **Note:** For more information on Streaming Security Levels for supported Illustra cameras, see Illustra Secure Video. For information on manually adding an IP device, see Manually adding an IP device

   d. Ensure the **Default** check box is selected to use the default port number. To use a different port to the default port, clear the **Default** check box and enter the new port number in the **Port** field.
   e. If the devices in this group use ONVIF communication protocols, select the **ONVIF RTSP Authentication** check box.
8. Select the devices that you want to assign to the Security Group from the **Available Devices** box.
9. Click the **Right Arrow** icon to move these devices into the **Devices in This Group** box.
10. 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.

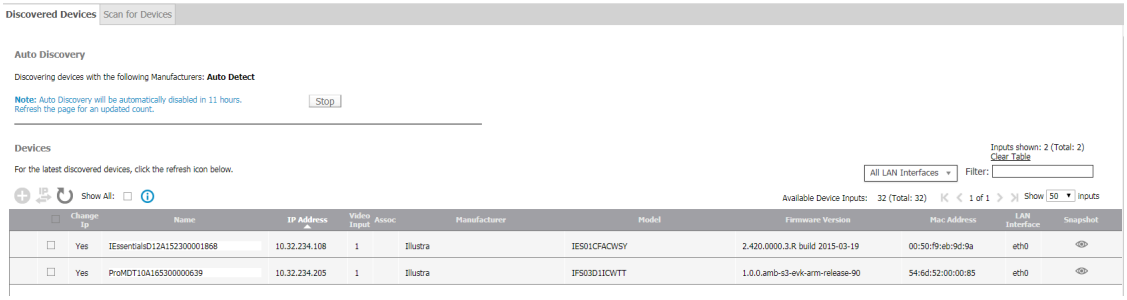
To discover devices, the NVR uses standard discovery protocols such as: MDNS, UPnP/SSDP, and ONVIF/WS-Discovery. The NVR will discover video devices on the network that have these standard protocols enabled.

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 using UPnP/SSDP. This feature allows the victor client to discover VideoEdge recorders.

Figure 18: Discovery page



Discovery icons table

Table 27: 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 after starting.

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.

Adding a device using Auto Discovery

1. Expand the **Devices** menu, and then click **Discovery**.
2. 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 check boxes 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 is applied when the device is added.
8. Click the **Add New Device** icon. The **Add New Device Settings** window opens.
9. **Optional:** From the **Add With Security Group** list, select a **Security Group**.
10. **Optional:** From the **Auto-Configure Streams** list, select the number of additional live streams.
11. **Optional:** Clear the **Default Associations** check box.
12. **Optional:** Clear the **Enable Smart Search (Motion Metadata)** check box.
13. Click the **Save** icon. When a device is added, it displays in the Video List or Audio List tabs.

Changing the IP address of a device

1. Expand the **Devices** menu, and then click **Discovery**.
2. On the **Devices** table, select the check box of the device that you want to edit.
3. Click **Change IP**.
4. Select **Use DHCP** or select **Specify an IP address**.
5. 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 window, you can click refresh to check when the camera advertises itself with the new IP configuration.

6. 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.

1. Expand the **Devices** menu, and click **Discovery**.
2. Click the **Scan for Devices** tab.
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. **Optional:** Select the Security Group from the **Scan With Security Group** list.
5. **Optional:** Select the LAN Interface from the **LAN Interface** list.
6. **Optional:** Configure the IP address search range.
   a. Select the **Specify IP Address Range** check box.
   b. Enter the **IP Address Range**.
7. Click **Start**. When the scan is complete, the discovered devices are displayed in the **Devices** table.

8. **Optional:** Click the **Add Security Group** icon to create a new security group.
9. Select the check boxes for the devices that you want to add to the NVR from the **Devices** table.
10. Click the **Add New Device** icon. The **Add New Device Settings** window opens.
11. **Optional:** Select a Security Group from the **Add With Security Group** list.
12. **Optional:** Select the number of additional live streams from the **Auto-Configure Streams** list.
13. **Optional:** Clear the **Default Associations** check box.
14. **Optional:** Clear the **Enable Smart Search (Motion Metadata)** check box.
15. Click the **Save** icon. When a device is added, it displays 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.

1. Expand the **Network** menu, and click **General**.
2. In the **UPnP** row, click **Disabled**.
3. Click the **Save** icon. UPnP is now disabled.

Troubleshooting Auto Discovery

Table 28: Troubleshooting Auto Discovery

Issue	Workaround
Some video devices are not automatically discovered.	• Verify that the video device has 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. • 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.
Cannot change the IP address of a video device.	• 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. Try the following workarounds: - 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 required. • The IP Address can updated on most American Dynamics cameras. Refer to your camera documentation for further information.

Table 28: Troubleshooting Auto Discovery

Issue	Workaround
Not able to view snapshot of video device.	• Verify that the video device is IP reachable from the NVR. When video devices advertise themselves using 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 using unicast IP.
No snapshot icon is displayed in Snapshot column.	• 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 enable NVRs to share transcoding resources, or to be monitored for failover.

NVR group prerequisites

ⓘ **Note:** For failover, all prerequisites listed are required. In addition, primary and secondary NVRs must all be added to victor using the same username and password.

Table 29: Prerequisites for communication between NVR Group members

Prerequisite	Description	Configuration
SSH	Enable SSH. ⓘ **Note:** You must change the VideoEdge default password to enable SSH.	System > Security Configuration > Remote Access
SNMP	Enable SNMP. All group members must share the same community string.	System > Security > Configuration > SNMP
User account	All group members must have an nvrgroupadmin user account. All group members must have the same password.	System > Users and Roles > users

NVR group icons table

Table 30: 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, frame-rate, and resolution. This enables you to better manage network bandwidth or resources. Depending on the model and hardware, VideoEdge has a finite amount of resources to dedicate to transcoding.

When you use an NVR Group, all the VideoEdge units in the group can share these resources as required. The VideoEdge units, including transcoders, in the group performing the transcoding are automatically managed and do not require user management. If all the transcoding resources in the NVR Group are in use, VideoEdge serves a native stream to clients.

NVR group list and NVR discovery

From the NVR Group page, you can manually add NVRs to the group. Alternatively, you can use the Discovered NVRs tab to find all discoverable NVRs. NVRs added to the group can be viewed on the NVR Group List page.

You can add up to 14 NVRs to a group. If configuring failover, you can configure up to two group members as secondary NVRs and up to twelve group members as primary NVRs

Manually adding an NVR to an NVR group

1. Expand the **Devices** menu, and then click **NVR Group**.
2. 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. When selected, this will add the NVR to which you are currently logged on to the group.
3. 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.
4. Click the **Save** icon. The NVR is added with non-failover NVRs status.

Adding an NVR to an NVR group using discovery

1. Expand the **Devices** menu, and click **NVR Group**.
2. Click the **Discovered NVRs** tab. The **Discovered NVRs** page opens. When Discovery is enabled, all discoverable NVRs display in the table. To refresh the list, click the **Refresh** icon.

   ⓘ **Note:** Enabling or disabling NVR discovery will also enable or disable device discovery.
3. **Optional:** Select the **Add by NVR name** check box to discover and add NVRs to the group using their hostnames.
4. **Optional:** Select the **LAN Interface** from the menu.
5. **Optional:** Select **Add NVR by Name** when DNS is configured.
6. Select the check boxes for all discovered NVRs you want to add to the group.

   ⓘ **Note:** Monitoring can be disabled for a secondary NVR if required.
7. Click the **Add** icon. The NVR is added with Non-failover NVRs status.

NVR group architecture

An NVR group can contain up to 14 NVRs. If configuring failover, you can configure up to two group members as secondary NVRs and up to twelve group members as primary NVRs. Within a group, NVRs can be assigned the following statuses:

- **Non-failover NVRs:** Neither a primary nor a secondary NVR. NVRs with this status can share transcode resources but are not included in your failover configuration.
- **Secondary NVRs:** NVRs which monitor the primary NVRs to provide redundancy if a primary NVR fails. Secondary NVRs can share their available transcode resources with the other NVRs within the group. If a secondary NVR enters 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.

Configuring a primary NVR

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. Expand the **Devices** menu and click **NVR Group**.
2. Click the **Edit** icon in the table entry for the NVR that you want to assign a new status. The **Configure Failover on this NVR** window opens.
3. From the **Failover Role** list, select **Primary**.
4. Enter the **Camera Network Address** in the field or select from the list.
5. 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.
6. **Optional:** Clear the **Monitoring Enabled** check box if required. This excludes the primary from the secondary NVR monitoring list.
7. **Optional:** Select the **WAN Settings** check box 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
8. Click the **Save** icon.

Configuring a secondary NVR

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. Expand the **Devices** menu, and click **NVR Group**.
2. 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.
3. From the **Failover Role** list, select **Secondary**.
4. From the list, select the **Priority**.
   - If you select **1**, when the first primary NVR fails, this secondary NVR takes over.

- If you select **2**, when a second primary NVR fails, this secondary NVR takes over, when the other secondary NVR is already in failover mode.

5. **Optional:** Clear the **Monitoring Enabled** check box if required. This disables monitoring mode on this secondary NVR.

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

6. Click the **Save** icon.

SmartStream

SmartStream is the resource management tool for VideoEdge. Transcoding is an integral part of the NVRs resource management tools. These tools provide 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 NVRs local transcoding resources are exhausted, it uses the transcoding resources of another member of the group.

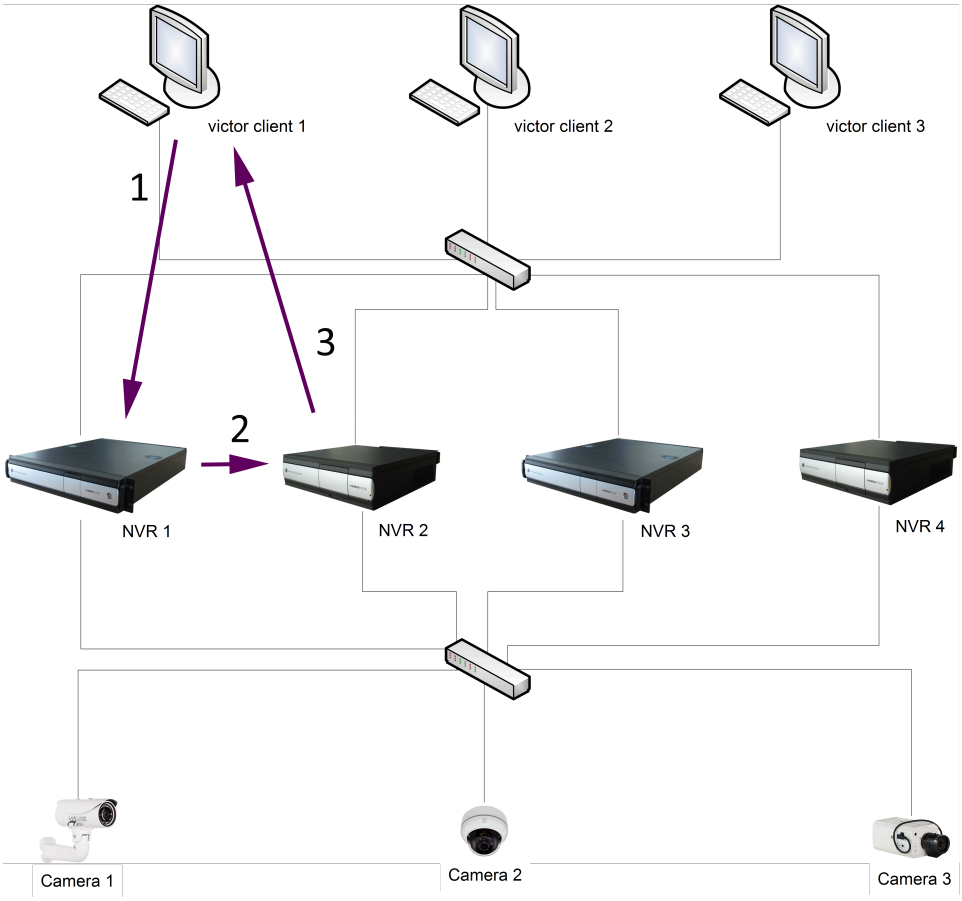
ⓘ **Note:** Remote transcoding is supported for video streams only using a H.264 codec.

The following figures illustrate the remote transcoding process over user datagram protocol (UDP), and 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 can have enough resources available to perform transcoding locally. 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.

1. victor Client issues RTSP play request to NVR 1. NVR 1 does not have sufficient transcoding resources available to provide optimum stream to the client.
2. NVR 1 streams video to be transcoded to NVR 2.
3. NVR 2 transcodes and streams video to the victor Client.

ⓘ **Note:** NVR 2 in the following figure can also be a Trancoder Appliance.

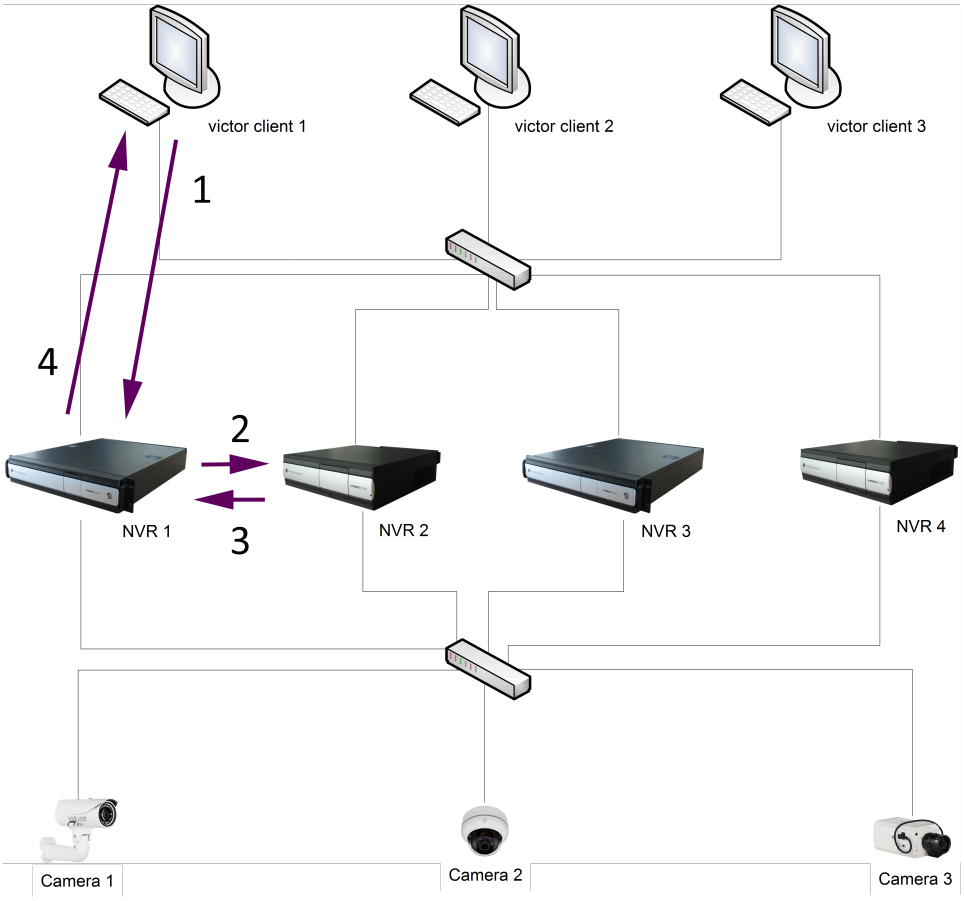
Figure 19: NVR groups: network example using UDP



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.

ⓘ **Note:** NVR 2 in the following figure can also be a Trancoder Appliance.

Figure 20: NVR groups: network example using TCP or WAN



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 with the NVR group.

In order to transcode video on a remote server in the group, group members exchange control messages over TCP. Live or transcoded video is sent using 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 transcodes video and sends the transcoded video to the client.

If the NVR group is oversubscribed and 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 continuously monitor all the primary NVRs in their NVR group. If a primary NVR fails, a secondary NVR switches into failover mode and assumes the services previously provided by the primary NVR. When the secondary NVR is in failover mode, it can no longer assume services for another primary NVR. The secondary NVR can only assume services for one primary NVR at a time. If you use the default failover configuration settings, the secondary NVR detects the absence of the primary NVR after approximately 30 seconds and assumes the role of the primary NVR.

Note: For optimum performance, use two secondary NVRs to monitor a maximum of 12 primary NVRs.

When a primary NVR fails, a secondary NVR assumes the role and services of the failed NVR. The secondary NVR records all media that the primary NVR was recording. If Motion Detection, Video Intelligence, Edge Analytics, or dry contact events are enabled, the secondary NVR assumes these functions.

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 transferred to allow the failover NVR to communicate with the cameras.

User account information is not transferred; therefore, the primary and secondary NVRs must be added to victor using the same username and password, and must share the same nvrgroupadmin password and SNMP community string as noted in NVR group prerequisites.

Failover monitoring resumes only after you repair or replace the damaged primary NVR, and return the secondary NVR 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 make during the time a secondary NVR has taken over the primary NVR's services is 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 is not 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 you configure failover, 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 other reasons. 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 repeats the polling process until the retry count is exceeded. If the secondary NVR continues to receive a 'failure' from the primary NVR, failover is 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 attempts to poll the primary NVR again. The number of polling attempts is determined by the retry count, for further information, see Failover in the Advanced section. If the secondary NVR continues to receive a 'failure' from the primary NVR, failover is initiated.
- The secondary NVR receives a 'good' reply from the primary NVR. In this instance, no failover action is taken.

Alerts

Alerts are sent to victor unified client by the secondary NVRs when the following occurs:

- 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 are enabled, the following notifications are sent on a failover event:

- The secondary NVR sends an email notification as follows: Activating Failover Mode for NVR at primary-IP-address.
- The primary NVR sends an email notification as follows: Primary NVR transitioning to standby state.

If failover and reboot notification email alerts are enabled, the following notifications are sent on a failover event:

- The secondary NVR sends the following email notifications as follows: Activating Failover Mode for NVR at primary-IP-address and NVR services are being shut down.
- The primary NVR sends the following email notifications as follows: 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 can be populated by a recording device in the event of Failover.

Using an NVR in failover mode

If you are viewing Live Video on victor unified client from a primary NVR and the primary NVR fails, the secondary NVR automatically assumes the connection to view live video. The victor unified client times out, and tries playing live video from the virtual IP address. victor unified client automatically reconnects 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 are 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 more. Events are 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 uses 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 are sent by the secondary NVR, providing a seamless appearance in the victor unified client. Events appear as if they have been received from the primary NVR at all times, even when failover mode is active.

When adding a secondary NVR to victor unified client as a recorder, add it using a static IP address assigned to its admin network. victor unified client receives events from the secondary NVR using its static IP address. If the secondary NVR is in failover mode or monitor mode, it sends unit-related events to victor unified client using its static IP address. Adding your secondary NVR this way enables 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 Administration and Configuration Guide*.

Backup/Restore

A backup of a secondary NVR can be performed while monitoring, or while active for a failed NVR. Backups created during this time only contain information about the secondary NVR, and any information about primary NVRs is not 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, ensure that the primary and secondary NVRs share the same username and password

The secondary NVR must have at least the same processing power as the largest primary NVR it is monitoring, 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

After you assign NVRs their required status and enable monitoring, your failover redundancy is set up. If a primary NVR fails, the secondary NVR enters failover mode when communication with the primary cannot be established.
When a secondary NVR is in failover mode, the Terminate Failover icon is displayed in the NVR's table entry. To terminate failover, complete the following steps.

1. Restore the Primary NVR.
2. Expand the **Devices** menu, and then click **NVR Group**.
3. Click the **Terminate Failover** icon in the table entry of the secondary NVR you want to return to monitoring mode.

If failover does not occur

If failover does not occur, ensure that the following conditions 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, that is, 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.

Upgrade all NVRs in the same maintenance window when a Failover system is present to ensure the time period without failover redundancy is minimized.

Upgrading NVRs when failover is enabled

1. Disable failover monitoring on the secondary NVR.
2. Upgrade the secondary NVR.
3. Re-enable monitoring on the upgraded secondary NVR.

   ⓘ **Note:** Security Configuration > Web server configuration, that is, HTTP and HTTPS or HTTPS only, must be applied identically on the primary NVR and on all the secondary NVRs on its active monitoring list for failover to function correctly.
4. Repeat steps 1 to 3 for any other secondary NVRs.
5. Upgrade each primary NVR in sequence.

   Each primary NVR will trigger failover as it is upgraded.
6. Terminate failover after each primary NVR is successfully upgraded and then upgrade the next primary NVR.

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 assume 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, ensure that you 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 31: Options icons

Icon	Name	Function
	**Save Changes**, **Save**	Save
	**Cancel**	Cancel

Table 31: Options icons

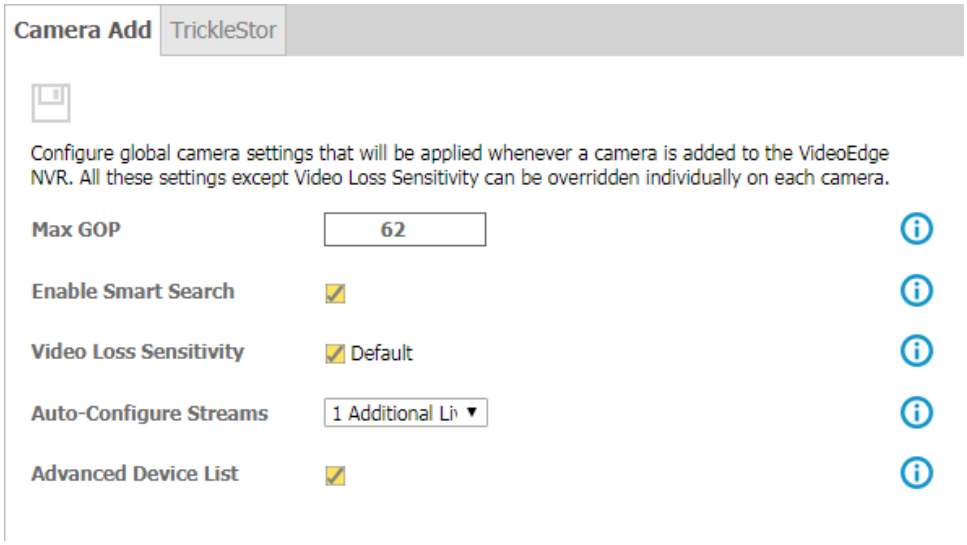
Icon	Name	Function
	Enable Offline Recording	Enable offline recording for selected camera.
	Disable Offline Recording	Disable offline recording for selected camera.

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 21: 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) check box 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 check box clears at these locations. Select the check box on any of these locations to activate the feature.

ⓘ **Note:** This option only applies the Smart Search configuration to devices that are added to the VideoEdge when the Enable Smart Search (Motion Metadata) check box is selected. If you use a backup configuration file to reinstall cameras, the configuration for all camera devices listed in the backup file is 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.

Enabling Smart Search by default

1. Expand the **Devices** menu, and then click **Options**.
2. Select the **Enable Smart Search (Motion Metadata)** check box.
3. 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.

Editing video loss sensitivity

1. Expand the **Devices** menu, and click **Options**.
2. Clear the **Default** check box for the Video Loss Sensitivity.
3. Enter a new value for video loss duration in the text field.

   ⓘ **Note:** You can have a numerical value between 5 seconds and 20 seconds. If you re-select the **Default** check box, 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.

1. Expand the **Devices** menu, and then click **Options**.
2. 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.
3. 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.

TrickleStor prerequisites

- 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.

Enabling offline recording

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

Storage

You can configure storage devices that are physically connected to the NVR, and storage devices that are networked to the NVR over a TCP/IP connection.

NVRs can require a large amount of storage space. This depends on the number of cameras, codec, resolution, frame rates, recording modes, and the duration for which you want to preserve video recordings.

When you first use your NVR system, you need to have storage configured to record data. At the outset, default storage partitions are configured to record data. It might be necessary to replace or add a storage device to produce a greater capacity for video storage when required.

Storage menu

From the Storage menu, you can complete the following tasks:

- Enable or disable internal and external storage that has been correctly mounted.
- Create storage sets for load management. This optimizes internal and external storage.

Storage configuration types

There are two storage configuration types: basic and advanced.

Basic configuration is the default configuration type. All storage devices and cameras are contained within one storage set. Advanced configuration allows you to create numerous storage sets. You can then assign storage devices and cameras to the storage sets. For more information on storage sets, see Storage sets.

Table 32: Storage menu and submenus

Menu	Description	Submenus
Camera Retention	View all devices and configure their retention settings.	—
Advanced	Create media folders for load balancing.	Media Folders
	Create storage sets for load balancing.	Storage Sets
	Assign devices to storage sets.	Assign Devices
	Configure applicable software RAID settings.	RAID

Verifying storage devices

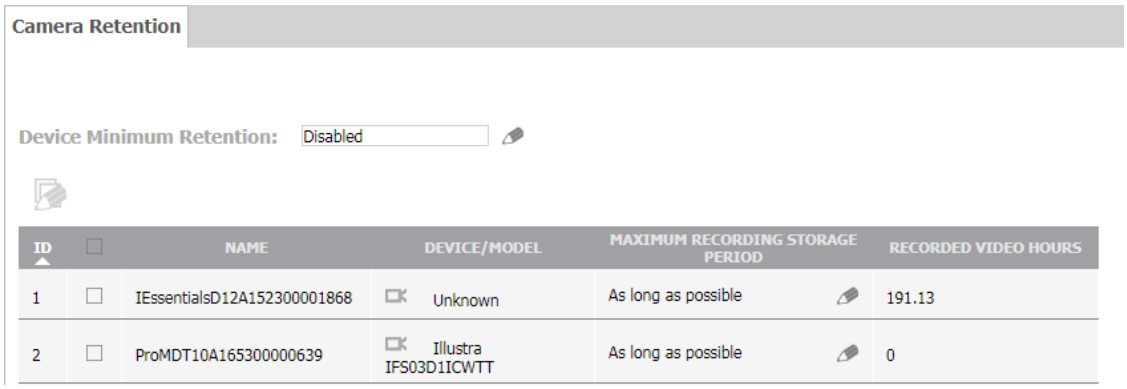
The Virtual Disks, also referred to as LUNs or Volumes, have all been detected by the NVR, but not necessarily configured for usage by the NVR. Ensure that your storage devices are listed in the table on the Media Folders page before moving on to the next section. If any expected storage is missing from 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. 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 VideoEdge and configure their storage retention settings.

Figure 22: Camera Retention page



Camera retention icons

Table 33: Camera Retention icons

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

Device minimum retention

You can use the Device Minimum Retention feature to enable system alerts when:

- Previously recorded video will not be kept for the configured minimum retention storage period.
- Previously recorded video is at risk of not being kept for the configured minimum retention storage period

This 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. This allows space for the newly recorded camera video.

Configuring the device minimum retention period

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

   ⓘ **Note:** To disable the device minimum retention period, click **Disabled**.
4. Click the **Save** icon.

Maximum recording storage period

The Maximum Recording Storage Period shows the maximum time that recorded media from a device is saved without being deleted.

By default, the recorded video for each 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 for each 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 a device's maximum storage recording periods can be accommodated by the VideoEdge storage configuration.

Configuring the maximum recording storage period

1. Expand the **Storage** menu, and then click **Camera Retention**.
2. Locate the device you want to configure.
3. In the **Maximum Recording Storage Period** field, click the **Edit** icon.
4. **Optional:** Click **As long as possible**.
5. **Optional:** To customize a storage period, click **Days** and then enter a value in the **Days** and **Hours** fields.
6. 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.

On the Advanced Storage Configuration page, you can:

- Set the VideoEdge 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 for each camera, you can configure the VideoEdge to achieve optimal efficiency and performance.

Advanced icons

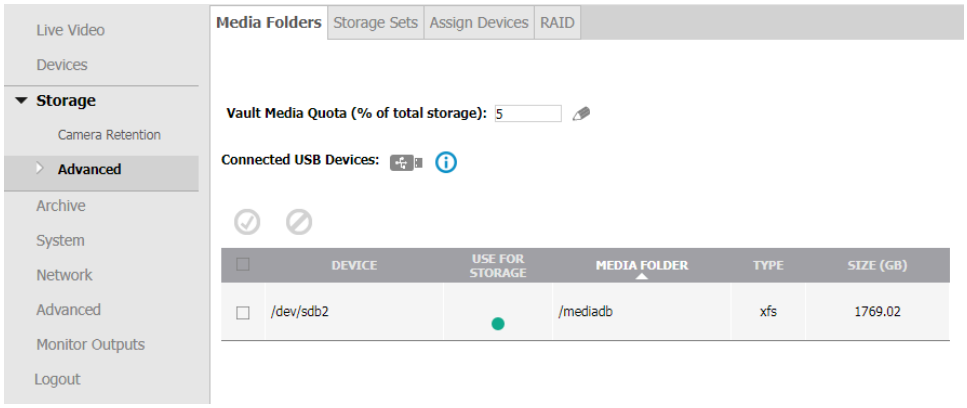
Table 34: Advanced icons

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 device
	Run Load Balancer	Create a camera redistribution proposal
	Delete	Delete
	Batch Edit	Edit multiple devices

Media folders

The Media Folders page displays the basic storage configuration. You can enable or disable the media folders used for recording. All storage devices discovered by VideoEdge are listed in the storage configuration table. All cameras added to 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 storage capacity.

Figure 23: Media Folders page



Storage configuration table

Table 35: Storage configuration

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

From the **Media Folders** page, you can add USB storage devices to VideoEdge to expand its media storage capacity.

1. Expand the **Storage** menu, and then click **Advanced**.
2. Click the **Add USB Device** icon.
3. Select a USB device from the table.
4. Click the **Add USB Device** icon.

   A pop-up window opens and displays the following message: Do you wish to delete all previously recorded media from all selected USB devices?.
5. Click the **Yes** icon or the **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.

1. Expand the **Storage** menu, and then click **Advanced**.
2. Select the check box for the media folder you want to use for storage, and then click the **Enable Media Folder** icon.

   If there has been media already stored in the folder, a pop-up window opens and displays the following message: 'Do you want to delete all previously recorded media from this folder?'.
3. **Optional:** If there has been media already stored in the 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. After a media folder is removed from storage, the NVR will no longer record to that folder.

1. Expand the **Storage** menu, and then click **Advanced**.
2. Select the check box for the media folder you want to use for storage and then click the **Disable Media Folder** icon.
3. 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 is deleted. If there is any media older than the maximum retention period specified for a specific camera, the media is 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 is deleted for any camera in the storage set that 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, because the NVR prioritizes 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 a specific media tagged so it will not be deleted, until specified. Vaulted media is not 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, and note the following:

- To set video as protected media, you must have 'Protect' permissions.
- To allow vaulted media to be deleted, set it as unprotected using victor Unified Client. You must have 'Unprotected' permissions.
- For more information, refer to the *Vault* section of the *victor Configuration and User Guide*.

Vaulted media quota

A vault media quota is a percentage of the total storage available used to store vaulted media only.

Over time, the amount of vaulted media within a storage set accumulates. If too much vaulted media accumulates, it may result in non-vaulted media being prematurely culled when the storage space reaches its maximum capacity. Set a vault media quota to prevent premature data culling – the amount of space for vaulted media is limited and this ensures there is enough space for normal media storage.

If there is not enough storage space in the quota allocated to store the media as vaulted media, a warning message displays and you cannot assign the media as vaulted. You should increase the vault media quota or delete vaulted media.

Setting a vaulted media quota

1. Expand the **Storage** menu, and then click **Advanced**.
2. In the **Vaulted Media Quota (% of total storage)** field, click the **Edit** icon.
3. In the **Vaulted Media Quota (% of total storage)** field, enter a value.
4. 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 are shut down because of a storage failure, a message displays as follows: Service currently shut down due to recording failure.

Enabling recorder deactivation on storage failure

1. Expand the **Storage** menu, and then click **Advanced**.
2. From the **Recorder Deactivation on Storage Failure** list, select **Enabled**.

   A warning message displays.
3. Click **OK**.

   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 for recorder deactivation on storage failure

1. Expand the **Devices** menu, and then click **NVR Group**.

   Note: You can also create an NVR group using the Discovery tab. For more information, see Adding an NVR to an NVR Group using Discovery.
2. Click the **Add** icon.
3. From the **Add NVR** list, select the name or local interface of the NVR to add to the NVR group.
4. Click the **Save** icon. The NVR appears in the **Non-failover NVRs** list and the **Add NVR** window opens.
5. **Optional:** Add additional NVRs by typing the NVR address into the field.
6. Chose an NVR for **Primary** failover and then click the **Edit** icon. The **Configure Failover on this NVR** window opens.
7. From the **Failover Role** list, change the default from **No Failover Role** to **Primary**. The **Deactivate when unable to record** check box is automatically enabled when you select **Primary failover** for the NVR.
8. Chose an NVR for **Secondary** failover and then click the **Edit** icon. The **Configure Failover on this NVR** window opens.
9. From the **Failover Role** list, select a failover role. The default role is **Current Setting**.
10. Continue to configure the remaining NVRs in the NVR group. For more information, see NVR group architecture

Storage sets

A storage set is a configuration item used for grouping storage and cameras. This optimizes storage use and recording throughput when multiple media storage devices are present.

Note: Each mounted storage device is referred to as a Media Folder in the Administration Interface.

Each storage set must have at least one assigned media folder for storage. For more information, see Media folders for storage sets guidelines.

Figure 24: Storage Sets page

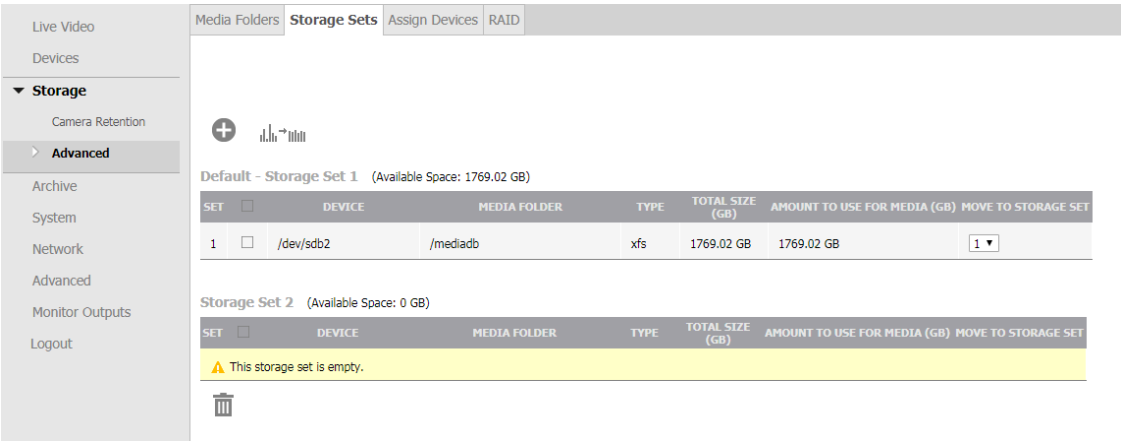


Table 36: Storage Sets page configuration table

Field	Description
Set	The storage set the media folder is assigned to.
Device	The physical device detected by the NVR
Media Folder	The location on the device where recorded media will be stored.
Type	The file system type. For example, XFS.
Total Size (GB)	The 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 list of other storage sets available on the NVR. Select a storage set you to move the media folder to that storage set.

Default storage sets

VideoEdge NVR

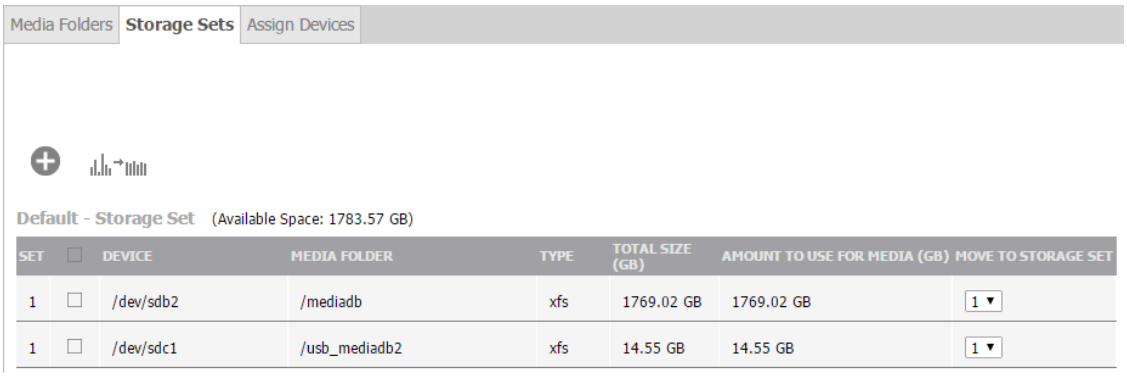
Each NVR starts with a single default storage set that cannot be deleted: Default-Storage Set 1. All detected storage devices, and their media folders and cameras are assigned to this default storage set.

VideoEdge Hybrid NVR

A single storage set is created by default for all existing drives: Default-Storage Set 1. All connected analog cameras are assigned to this storage set.

ⓘ **Note:** If the NVR is configured with RAID storage, one storage set is created by default.

Figure 25: Default-Storage Set table



You can view Default-Storage Set 1 on the Storage Sets page. When you enable a media folder for storage on a storage device, the media folder is available for advanced configuration and is displayed in the Storage Sets page in Default-Storage Set 1.

Media folders for storage sets

A media folder is a location on a device for recording media. Media stored in a media folder can include video, audio, and analytic media. Videos from the cameras that are assigned to a storage set will record to the media folders on the storage devices that are assigned to the same storage set. Media can be recorded to storage sets in parallel, so you can create additional storage sets and configure them as required to optimize disk performance.

For more information on media folders, see Media folders.

Media folders for storage sets guidelines

Use the following guidelines when creating media folders for storage sets:

- Each storage set must have at least one assigned media folder for storage.
- When you create a storage set, it contains no media folders or cameras. You can assign multiple media folders or cameras to the default storage set or an existing storage set.
- Media folders and cameras can be moved or assigned across these additional storage sets. This distributes the record load across the storage devices and avoids I/O saturation of storage devices.

  ⓘ **Note:** When you move a media folder to another storage set, you can retrieve all previously recorded media using clip export and playback in victor Unified Client and VideoEdge Client.

- Use a minimal number (one if possible) of media folders for each storage set to maximize the virtual disk size.
- There is no limit to how many media folders or cameras you can assign to a storage set. However, data throughput is limited to avoid I/O saturation and potential data loss during recording. For more information, see Example storage set assignments.

  ⓘ **Note:** On most NVRs, there is only one media folder, so there is no need to create additional storage sets.

- You can only have one media folder for each storage device partition or storage device, depending on your storage configuration. You can choose the media folders on devices to be used for storage.
- When using RAID storage systems, assign all virtual disks from a disk group to the same storage set.

Optimizing disk performance

To avoid I/O saturation and potential data loss during recording, use the following guidelines when assigning or reassigning media folders to storage sets:

- To add a system disk to a storage set, specify a particular folder on the system disk. This folder should exist on a separate partition on the system disk.

  ⓘ **Note:** You will not be presented with Linux system file systems. For example, */proc* or */sys*.

- When you allocate media folders from the same device or RAID group, associate them with the same storage set. Hard drive thrashing can occur if media folder from the same hard drive are spread across several storage sets. When the hard drive is being overworked, it can result in a downgrade of system performance.
- Avoid assigning virtual disks from the same disk group to different storage sets. Otherwise, there is a high probability that continuous disk thrashing will cause the storage device to lock up and cause undesirable results to the NVR.
- Spread high bit rate cameras across storage sets for load balancing. The lower the number of cameras for each storage set, the higher the achievable throughput. This is because a lower total data rate is required to record to each storage device. For more information, see Example storage set assignments.

Example storage set assignments

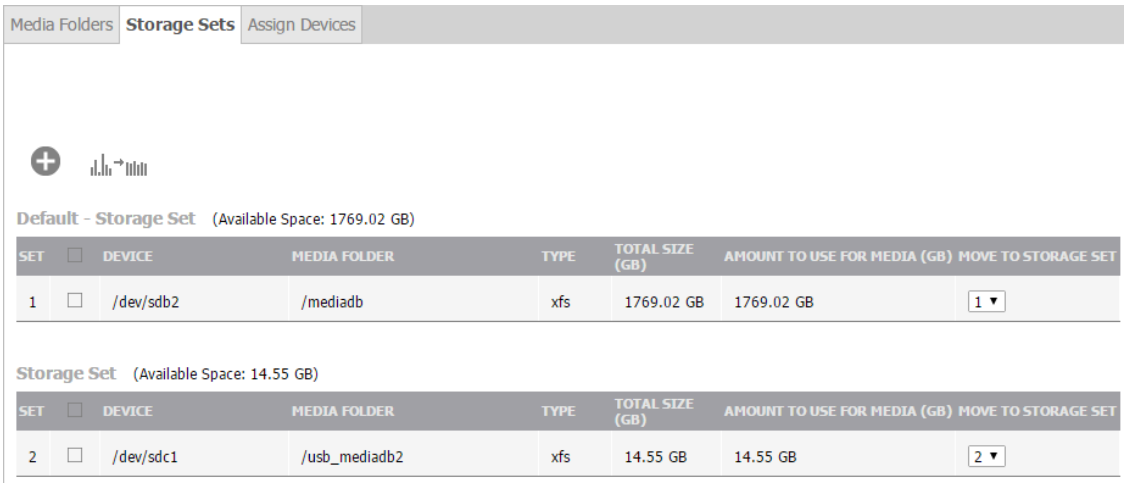
While there is no limit to how many media folders or cameras you can assign to a storage set, data throughput is limited to avoid I/O saturation and potential data loss during recording.

The following shows an NVR with a 30 camera license using various storage set options.

Table 37: Example storage set assignments

NVR with 30 camera license			
Number of storage sets	**Storage set number**	**Number of cameras**	**Set of drive(s) cameras are recording to**
2	1	15	First
	2	15	Second
2	1	20	First
	2	10	Second
3	1	10	First
	2	10	Second
	3	10	Third
3	1	16	First
	2	7	Second
	3	7	Third

Figure 26: 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.

Performance support on storage sets

Table 38: Performance support on each storage set

Device		Maximum camera support	Maximum support (Mbps)	Total server input (Mbps)
R720 bundled server		64	200	400
Software Only option (installed on the minimum required hardware)		32	100	400
NVR Desktop Appliance		32	100	100
Hybrid Desktop Appliance		32	100	100
Hybrid Rack-Mount Appliance	32 Channel Hybrid 2U Rack Mount	32	100	200
	64 Channel Hybrid 3U Rack Mount	64	100	300

Creating a storage set

1. Expand the **Storage** menu, click **Advanced**, and click **Storage Sets**.
2. Click the **Add Storage Set** icon. A new storage set is created.

Assigning media folders

1. Expand the **Storage** menu, click **Advanced**, and then click **Storage Sets**.
2. Locate the media folder you want to assign or reassign from the list of existing storage sets.
3. From the **Move to Storage Set** list, select the new storage set where you want the media folder to be assigned.
   The media folder will appear in the storage set list.

Recording with storage sets

Note the following when recording with storage sets:

- Cameras will only record to the media folders of the storage set where they are assigned.

- Each storage set must have at least one media folder and one camera assigned for successful recording.
- Media folders and cameras can be moved between storage sets at any time without causing an interruption to recording.
- When multiple media folders exist in a storage set, all cameras assigned to the storage set record to one media folder at a time.

  ⓘ **Note:** The total storage space for a storage set is the sum of the media folders assigned.

Camera redistribution

Camera redistribution improves the retention time for your cameras by re-balancing your camera storage configuration. You can create a Camera Retention Proposal that projects the current and re-balanced retention time for each camera. The proposal is based on your current storage configuration.

Note the following when calculating camera redistribution:

- The Camera Redistribution Proposal depends on your monitoring system configuration and may not indicate retention improvement for all cameras. Ensure you review the proposed changes before you accept the Camera Redistribution Proposal.
- The Run Load Balancer icon for camera redistribution is not usable on certain platforms. For example, 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 reassign media folders or cameras to different storage sets.

Calculating camera redistribution

1. Expand the **Storage** menu, click **Advanced**, and then click **Storage Sets**.
2. Click the **Run Load Balancer** icon to display the **Camera Redistribution Proposal**.

   ⓘ **Note:** A notification appears if the Camera Redistribution Proposal cannot re-balance your storage configuration.

   ➤ **Important:** Ensure you review the proposed changes before you accept the Camera Redistribution Proposal. For more information, see Camera redistribution .
3. Click the **Save** icon to accept the proposed camera redistribution changes, or click the **Cancel** icon to reject the proposed camera redistribution changes.

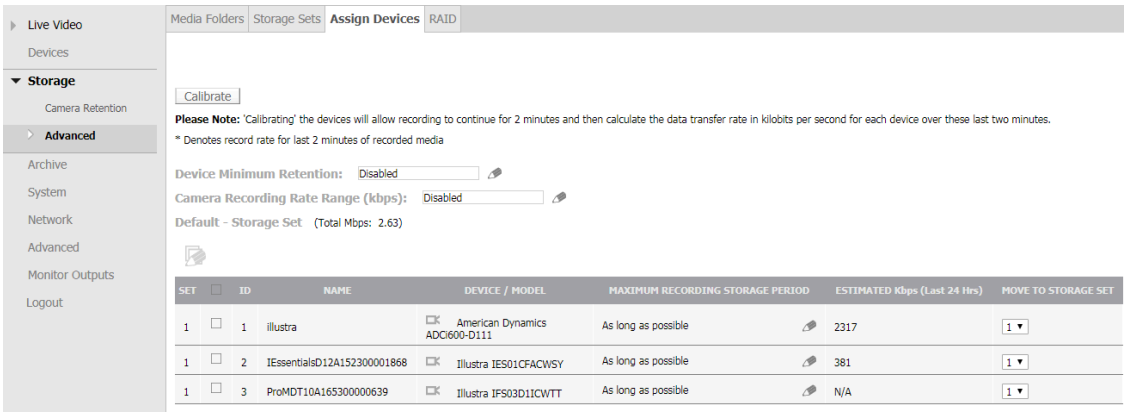
Assign devices

When assigning a device to a storage set, note the following:

- A camera can be assigned to a different storage set as required. You do not need to remove and re-add a camera.
- If only one storage set is available, the new camera will be added to this storage set.
- If there are multiple storage sets available, you will be prompted to assign the camera to the required storage set.

  ⓘ **Note:** If you are using auto-discovery to add cameras, they will be added to Default-Storage Set 1.

Figure 27: Assign Devices page



Assigning a camera to a different storage set

1. Expand the **Storage** menu, click **Advanced**, and then click **Assign Devices**.
2. Locate the camera you want to reassign from the list of existing storage sets.
3. From the **Move to Storage Set** list, select the new storage set where you want the camera to be assigned.

Camera calibration

From the Assign Devices page, you can view the data transfer rate for a camera in each storage set table. The data transfer rate is recorded in the Estimated Kbps (Last 24 Hrs) field and usually displays the average rate over the last 24 hour period.

You can use the Calibrate feature to calculate the data transfer rate in Kbps for each camera over the last two minutes. This gives a current data transfer rate for each camera. This optimizes the performance of your NVR by reassigning cameras to storage sets based on the current data transfer rates.

Configuring camera calibration

1. Expand the **Storage** menu, click **Advanced**, and click **Assign Devices**.
2. Click **Calibrate**. The **Estimated Kbps (Last 24 hrs)** field for each camera is updated with the data transfer rate for the last two minutes.

Device minimum retention

For information about the Device Minimum Retention feature, see Device minimum retention.

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.

Configuring the camera recording rate range

1. From the **Storage** menu, click **Advanced**, and then click **Assign Devices**.
2. In the **Camera Recording Rate Range (kbps)** field, click the **Edit** icon.
3. **Optional:** Enter values in the **MIN** and **MAX** fields.
4. **Optional:** To disable the recording rate range, click **Disabled**.
5. Click the **Save** icon.

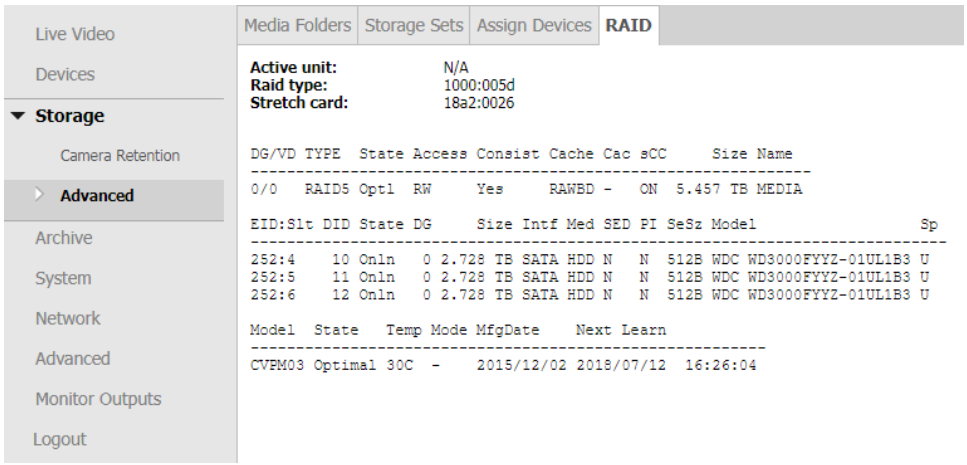
RAID

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.

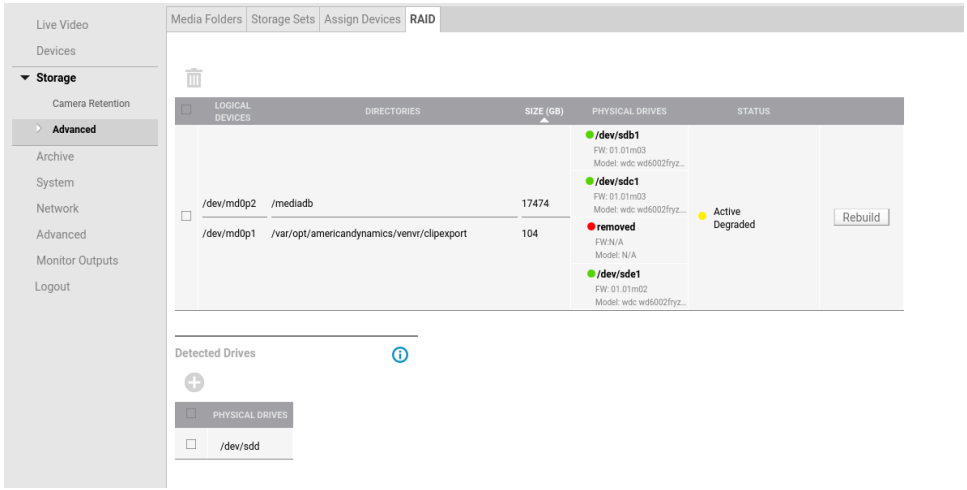
Figure 28: RAID page



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 29: 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.

Rebuilding an unhealthy RAID

⚠ **CAUTION:** Rebuilding a RAID will irretrievably delete all existing data on the current RAID.

1. Expand the **Storage** menu, click **Advanced**, and then click the **RAID** tab.
2. Click **Rebuild**.

   ⓘ **Note:** The Rebuild feature is only available if the RAID is in a corrupt or unhealthy state.
3. Click **Yes** when the first popup warning display.
4. Click **Yes** when the second popup warning displays.

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. Expand the **Storage** menu, click **Advanced**, and then click the **RAID** tab.
2. From the **Physical Drives** list, select the check box of the drive you want to add.
3. Click the **Add** icon.
4. Click **Yes** when the first popup warning displays.
5. Click **Yes** when the second popup warning displays.

Removing a software RAID

⚠ **CAUTION:** Removing a RAID will irretrievably delete all existing data on the current RAID.

1. Expand the **Storage** menu, click **Advanced**, and then click the **RAID** tab.
2. Select the check box of the software RAID you want to remove.
3. Click the **Remove** icon.
4. Click **Yes** when the first popup warning is displayed.
5. Click **Yes** when the second popup warning is displayed.
   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. For more information, see the Storage Statistics section.

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 using SCSI cables, along with a SCSI terminator.
- DAS can also be connected using 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

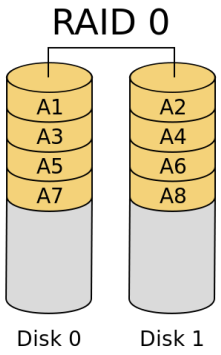
- **Mirroring:** Duplicating data to more than one disk.
- **Striping:** Splitting data across more than one disk.
- **Error Correction:** Storing redundant data so problems can be detected and possibly fixed.

Common RAID types

RAID 0

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

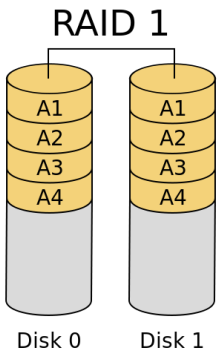
Figure 30: RAID 0



RAID 1

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.

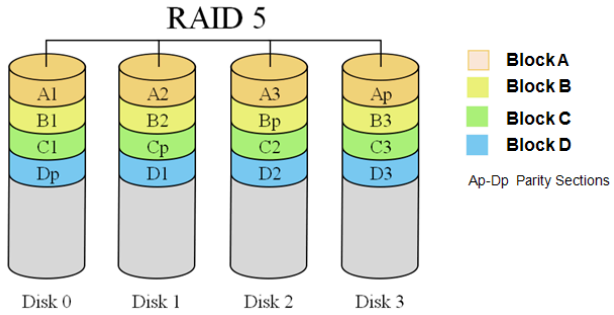
Figure 31: RAID 1



RAID 5

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.

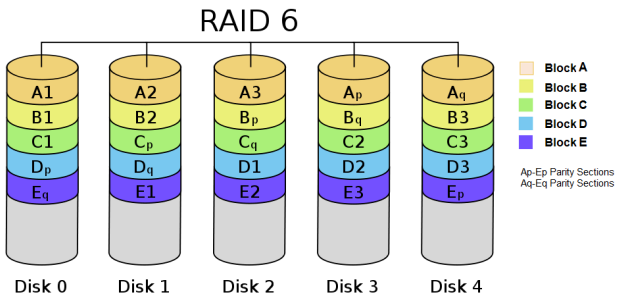
Figure 32: RAID 5



RAID 6

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.

Figure 33: RAID 6



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.

Recording retention period

- 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.

Storage usage examples

The following details storage usage examples that are compared to the NVR 4.1 storage model.

Example 1: Using a 20 TB 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 auto-discovery software performs storage configuration when it detects a suitable storage device.

XFS file system

If you want to use the XFS file system for maximum throughput, additional file system options need to be configured.

Table 39: File system options for using the XFS file system

Device	Required configuration
Internal	*rw,noatime,nodiratime,attr2,nobarrier,noquota,allocsize=4m,inode64*
External including iSCSI and Fiber Optic	*rw,noatime,nodiratime,attr2,nobarrier,noquota,allocsize=4m,inode64*

Note the following:

- From VideoEdge version 5.7.0, the *nobarrier* mount option is not supported.

  ⚠ **CAUTION:** Using the *nobarrier* mount option from VideoEdge 5.7.0+ will cause a failure to mount a filesystem.

- Only use **nobarrier** 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`

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.

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**.

   ⓘ **Note:** You may need to lower the camera count for each NVR to meet network and storage requirements when dealing with many cameras, large resolution, or retention.

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 use 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.

Figure 34: Rack Mount example

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 Disk Groups (aka RAID sets).
- Each Disk Group can be carved up into one or more Virtual Disks (aka Volumes or LUNs). Try to maximize each virtual disk size.
- Assign all Virtual Disks from a single Disk Group 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.

Additional storage devices

You can connect additional storage device using eSATA, USB, Fiber, and iSCSI.

Connecting storage to the NVR using eSATA

Before you begin:

- Stop the NVR services.
- When you have connected and configured external storage devices, restart the NVR services.

Note: This task applies to Hybrid NVRs only.

1. Turn off the NVR.
2. Connect the eSATA Storage to the NVR using the eSATA port.
3. Restart the NVR.
4. Log on 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 you begin:

- Stop the NVR services.
- When you have connected and configured external storage devices, restart the NVR services.

1. Turn off the NVR.
2. Install the Fiber HBA Kit (PCI-e).
3. Connect the AD Fiber RAID Storage to the NVR.
4. Restart the NVR.
5. Log on to the NVR desktop as the root user.

Connecting the NVR to FRS/FES using iSCSI

Before you begin:

- Stop the NVR services.
- When you have connected and configured external storage devices, restart the NVR services.

1. Turn off the NVR.
2. Install the iSCSI NIC Card (LAN3) into the correct and compatible slot.
3. Connect the iSCSI RAID storage device to a switch or directly to NVR LAN3 to ensure that it is accessible.
4. Open a web browser. In the Address field, enter the IP address of the iSCSI RAID storage device. The iSCSI RAID storage device web configuration interface opens.
5. Enter the following default username and password:
   - `admin/admin`
6. To set up the NIC IP settings for the iSCSI port, complete the following steps:
   a. From the **iSCSI RAID Rack** menu, select **iSCSI Configuration**. The **iSCSI Configuration** sub-menu items display.
   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**, a cable is present connecting the storage device and the NVR. This is the NIC that you need to configure.
   d. In the **Name** field of the NIC that has a **Link** value **Up**, select **IP Settings for iSCSI ports**. The **NIC IP** settings page opens.
   e. **Optional:** If required, edit the Static **Address**, **Mask** and **Gateway**.

ⓘ **Note:** If there are no DHCP settings available, the fields contain the following default values:

- Address: 10.10.10.20
- Mask: 255.255.255.0
- Gateway: blank

f. Click **Confirm**. The **NIC settings** page closes and the **NIC summary details** display.

7. To create a **Node** to associate the storage NIC with an NVR port, complete the following steps:
   a. From the **iSCSI Configuration** menu, select **Node**.
   b. Click **Create** and enter a name for the node.
   c. From the list, select a type of **Authentication**. The default is **None**.

      ⓘ **Note:** Select **CHAP** to use a password for data transfer.

   d. Select the check box for the required **Portal**. This is the portal that contains the NIC IP address.
   e. Click **Confirm**.
8. To assign the required Virtual Drives a LUN, complete the following steps:

   ⓘ **Note:** The Virtual Drives are pre-configured on the storage device.

   a. From the **iSCSI RAID Rack** menu, select **Volume configuration**.
   b. Select **Logical Unit** and click **Attach**.
   c. From the **VD** list, select the virtual disk.
   d. From the **LUN** list, select the LUN and click **Confirm**.

      ⓘ **Note:** The Virtual Disk is assigned to the LUN and appears in the Logical unit summary table.

   e. Repeat the steps to assign all of the required Virtual Disks to a LUN.
9. To configure the **Network Settings** on the NVR, complete the following steps:
   a. Log on to the NVR desktop as the root user and select **Computer**.
   b. From the **System** menu, select **YaST**. The **Control Center** opens.
   c. From the **Network Devices** section, select **Network Settings**. The **Initializing Network Configuration** window displays momentarily and the **Network Settings** page opens.
   d. Click the **Overview** tab and select the storage network card.
   e. Click **Edit** and click the Statically assigned IP address option button.
   f. Enter the **IP Address**.
   g. Enter the **Subnet Mask**: 255.255.255.0.
   h. Enter the **Hostname**.
   i. Click **Next** and click **OK**.
   j. Close the **Network Settings** window.
10. Test the network connection between the NVR and the iSCSI storage device:
    a. Double-click **GNOME Terminal** on the desktop.
    b. In the Terminal window, type ping followed by the IP address of the storage device, for example, `ping 192.168.8.1`.
    c. Press Enter.

       ⓘ **Note:** If the connection is unsuccessful, a Destination Host Unreachable message displays. Check the connections and network settings and retry.

    d. Close the Terminal window.

11. Connect the storage device using the iSCSI initiator:
    a. In the Control Center, enter iSCSI in 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** check box.
    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 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 onto the storage web interface, select the **iSCSI configuration** in the menu, select **Session** and ensure that the session is connected with the correct initiator name.

Archive

The Archive feature allows you to save to and retrieve video from long term storage in the form of a dedicated network attached storage (NAS). Additionally, archiving is optionally available using AD Cloud Services.

ⓘ **Note:** NAS devices can require pre-configuration before they can be used for archiving tasks. For more information, refer to your product's installation and user manual.

ⓘ **Note:** AD Cloud Services requires additional cloud configuration and an active cloud storage subscription. Please contact American Dynamics sales or professional services to setup a cloud account and determine storage subscription options.

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:** Add, remove, enable, or disable archiving destinations connected to the NVR. Switch archive storage between CIFS protocol and AD Cloud Services.
- **Settings:** 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:** Create Archive Groups and Schedules that define which video is to be automatically archived. The Archive Scheduler submenu contains the following sections: Archive Schedules, Archive Schedule Editor, and Archive Group Editor.
- **Device List:** Enable and disable the video devices that 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:** View a list of all outstanding archiving operations. You can also delete outstanding archiving jobs you no longer want to occur.

Table 40: 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.

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 can be performed 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. If archiving falls 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.

AD Cloud Services are supported on VideoEdge and provide additional archiving options. Media archive information can be accessed through the Web Admin on the Archived Clip Media page.

Video is archived in files of five minutes in length for CIFS and one minute in length for cloud archiving. 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.

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.

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.

Adding an archive destination

1. Expand the **Archive** menu, and then click **Archives**.
2. Click the **Add Archive** icon.
3. Enter the **Archive Name**.

   ⓘ **Note:** This can consist of alphanumeric characters plus 'space', "_", "-" and "."
4. From the drop down list, select the appropriate archive type.

   ⓘ **Note:** Select CIFS to archive media information to server storage, or, for cloud media information archive, select AD Cloud Services.
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**.

ⓘ **Note:** The Domain configuration item is only applicable when configuring cloud archiving.

7. Enter the **Username** and **Password** required to access the shared directory on the Archive Destination.
8. For AD Cloud Services, enter the related **Partner Name**, and **Account Name**.
9. **Optional:** Select the **Locked** check box to make the destination read only.
10. **Optional:** Click **Test Connectivity** to check the destination is correctly configured.
11. **Optional:** Select the **Enabled** check box 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.

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

1. Expand the **Archive** menu, and then click **Archives**.
2. Select the check box in the archives table for the destination you want to enable or disable.
3. Click the **Enable Archive** icon to enable the archive destination, or the **Disable Archive** icon to disable the archive destination.

Manual video archiving

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 whether the archiving task was successful or not. If an automatic archive attempt fails, the VideoEdge reverts to the manual archive. The status page displays manual archive tasks created after a failed automatic archive attempt. The Job Type column shows whether a job is a retry or manual. Archived video can also be retrieved using victor unified client.

For more information refer to the *victor unified client User Guide*.

Archived video in victor Unified Client

Archived video can be retrieved using victor Unified Client. For more information refer to the *victor unified client User Guide*.

Archived video in third party media players

Archived Video is saved in an MP4 format, and can be viewed using a third 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 third party application.

ⓘ **Note:** Third party media players are unable to validate video.

Global settings

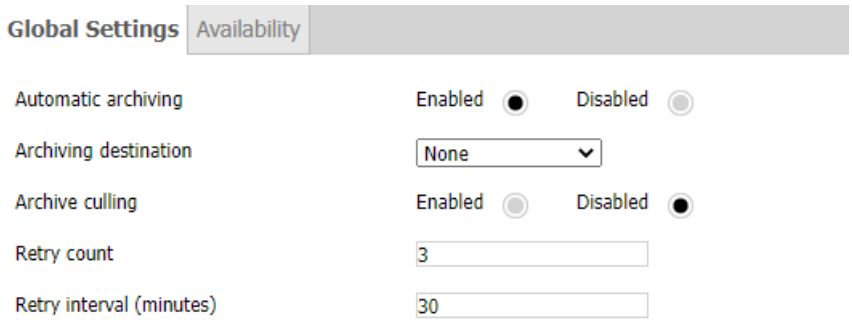
From the Global Settings page, you can enable or disable automatic archiving, set the active archive destination, and configure first in, first out (FIFO) archive culling.

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 check box.

FIFO archive culling is a basic form of 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.

The Network Video Recorder does not perform archive data culling when AD Cloud Services is enabled. Instead this is done on the cloud storage through the subscriptions service.

Figure 35: Global Settings page



You can also configure a retry count and retry interval which dictates the NVR's behavior if archiving is unsuccessful due to a loss of connection with the archive, the archive becoming unreadable, or the destination is 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.

Applying global archive settings

1. Expand the **Archive** menu, and then click **Settings**.
2. On the **Global Settings** page, select **Enabled** to enable **Automatic Archiving**, or select **Disabled** to disable **Automatic Archiving**.
3. From the **Archive Destination** list, select the **Archive Destination**.
   a. If the **Archive Destination** is set to **None**, select **Enabled** to enable Archive culling, or select **Disabled** to disable Archive culling.
   b. If the **Archive Destination** is set to **Cloud**, set the **Age of media to be archived (days)** value. Click the orange warning icon to view more information on Archive Media Age.
4. **Optional:** Select the **Skip archiving backlog** check box if required.
5. Select **Enabled** to enable Archive culling, or select **Disabled** to disable Archive culling.

6. Enter a **value for the Retry count** in the **Retry count** field.
7. Enter a **value for the Retry interval** in the **Retry interval** field.
8. 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.

1. Expand the **Archive** menu and click **Settings**.
2. Click the **Availability** tab.
3. For the Availability schedule, select **Enabled**.
4. On the dialog box, click **OK**.
5. For Archiving availability, select **Available** to assign availability, or select **Not Available** to remove availability.
6. Select the schedule times that you want to edit using one of the following methods:
   - 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.
7. 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

Configuring the archiving quality

1. Expand the **Devices** menu, and then click **List**.
2. Click the **Setup** icon in the device row you want to edit.
3. Click the **Archive** tab.
4. Select the **Archiving Quality** from the list.
5. 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 in accordance with 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 when it has exceeded the retention period.

1. Expand the **Devices** menu, and then click **List**.
2. Click the **Setup** icon in the device row you want to edit.
3. Click the **Archive** tab.
4. Select the Archiving Mode.

   ⓘ **Note:** To enable archiving, select one of the following: **Archive all video** or **Archive only alarm video**.

5. Select **Custom** from the list, and then enter a retention period in the **Period** field or select **As long as possible** from the list.
6. Click the **Save** icon.

   ⓘ **Note:** For cloud archiving, data retention is set by the cloud service provider.

Archiving 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.

Enabling or disabling the archiving scheduler

1. Expand the **Archive** menu, and then click **Archive Scheduler**.
2. Select **Enabled** to enable the **Archiving Scheduler**, or select **Disabled** to disable the **Archiving Scheduler**.

Creating an archive schedule

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

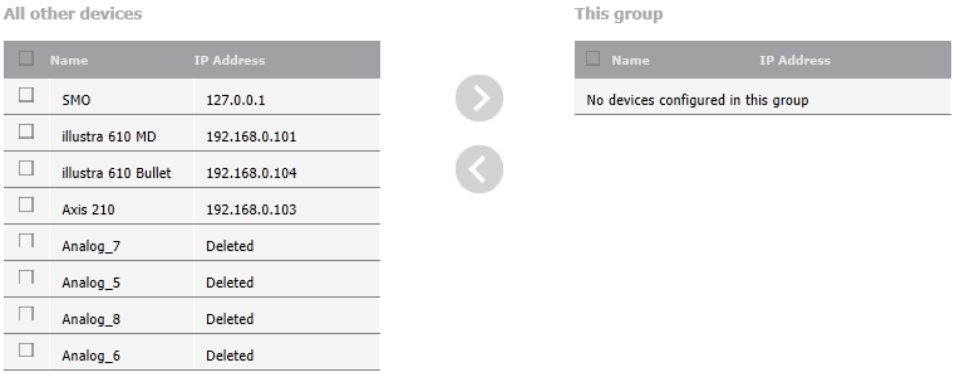
Renaming an archive schedule

1. Expand the **Archive** menu, and then click **Archive Scheduler**.
2. Click the **Rename** icon next to the Archive Schedule name you want to edit.

3. Enter the new name in the text field.
4. Click the **Save** icon.

Schedule editor and group editor pages

Figure 36: 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.

Assigning cameras to a group

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

Editing the queuing times of an archive schedule

1. Expand the **Archive** menu, and then click **Archive Scheduler**.
2. Click the **Edit group times** icon of the **Archive Schedule** you want to edit.
3. Select an Archiving Mode:
   - **Automatic archiving disabled:** Disables queuing for archiving during selected time increments.

- **Automatically archive all recorded video:** Queue for archiving all video during selected time increments.
- **Archive only recorded alarm video:** Queue for archiving all video recorded under alarm conditions during selected time increments.

4. Select the schedule times you want to edit using one of the following:
   - 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.
5. 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.

Batch editing archive settings

1. Expand the **Archive** menu, and then click **Device List**.
2. Select the check boxes of the cameras you want to edit.
3. Click the **Batch Edit Device** icon.
4. Select the **Archiving Mode** check box, and then select the required **Archiving Mode**.
5. Select the **Archiving Quality** check box, and then select the required **Archiving Quality** setting from the list.
6. Select the **Maximum Archiving Retention Period** check box, and then select the required **Maximum Archiving Retention Period** from the list.
7. Click the **Save** icon.

Jobs

The Jobs page lists all outstanding queued archiving tasks.

Viewing and deleting manual archiving tasks

1. Expand the **Archive** menu, and then click **Jobs**.
2. **Optional:** Select the check boxes next to the tasks you want to delete.
3. Click the **Delete archive job** icon.

System

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

- **General:** 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:** 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:** 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:** Create a Template file or alternatively load a Template file. The Templates submenu contains the following sections: Save Template, and Load Template.
- **Backup/Restore:** 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:** View the Serial Protocols supported by your NVR and their default settings.
- **Security Configuration:** 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 41: 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.
	**Camera Access Settings**, **Change template**	Open the camera access list, or edit certificate template.
	Right Arrow	Move selected cameras to Access Denied group.

Table 41: System icons

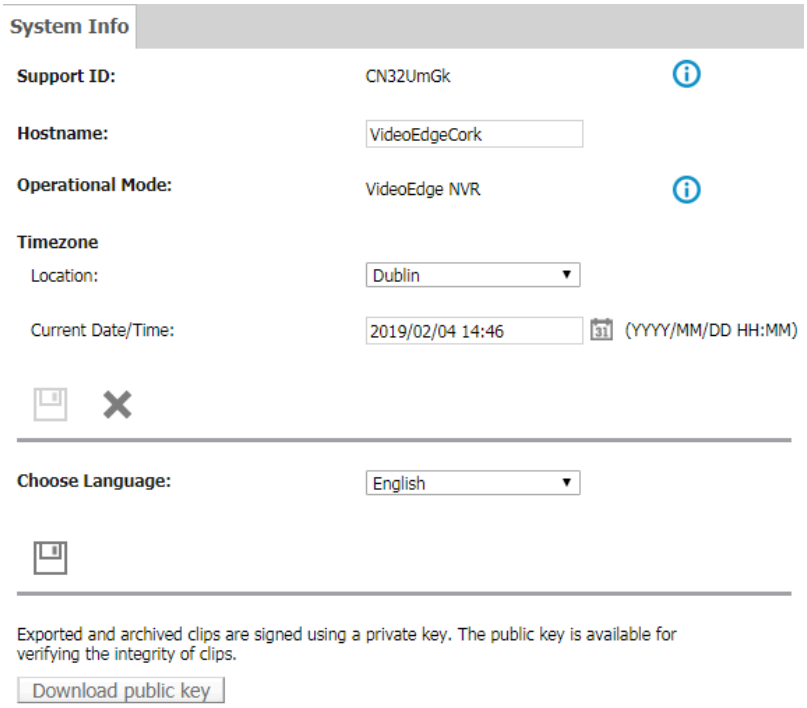
Icon	Name	Function
	Left Arrow	Move selected cameras to Access Granted group.
	Retrieve LDAP Groups	Retrieve LDAP groups from LDAP server.

General

From the General System Info page, you can download the public key, edit the hostname, location, date, time, and language.

For playback to work reliably, it is imperative that the time between the client and the NVR is synchronized. Use the same NTP server 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, because NTP servers use UTC time.

Figure 37: System Info page



Licensing

There are three license types 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 VideoEdge. You can use the temporary license supplied to configure your VideoEdge, add cameras, and configure Motion Detection before you apply for a license.

ⓘ **Note:** VideoEdge Hybrid recorders come standard with a software license that supports all analog video inputs.

Licensing requirements

Licensing is based on the number of IP connected cameras used by VideoEdge. You can use the temporary license supplied to configure your VideoEdge, add cameras, and configure Motion Detection before you apply for a license.

ⓘ **Note:** 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. Encoders can have a single IP address or multiple IP addresses.

- **Single IP address encoder or device:** If the encoder or 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. 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 42: 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. For example, you can use up to 16 channels on a VideoEdge Desktop Hybrid. Of these channels, you can connect 16 IP cameras or you can connect a mix of analog and IP cameras. If you connect a fully populated 8 channel IP encoder, and 8 single IP cameras, this is counted as a total of 16 channels.

Licensing status

The Licensing Status section provides the following information:

Table 43: Licensing Status section

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.

Table 43: Licensing Status section

Field	Description
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.
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.

Applying a license

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.

Licensable features

VideoEdge has the following licensable video analysis features:

- Video Intelligence
- Facial Recognition
- Facial Verification
- License Plate Recognition

- Deep Intelligence

Face Recognition license 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 from version 5.4.1 or earlier to version 5.4.2 or later, 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 license

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.

Local License

To apply a Local license to 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.

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.

Generating a Host ID

Before you begin:
Ensure that all network interface cards (NICs) used with VideoEdge are already installed on the server. For example, a Client LAN, Camera LANs, or Storage LANs.

Important: For NVRs that you assign as Secondary NVRs, do not generate a Host ID while the Secondary NVR is in Failover Mode.

1. Expand the **System** menu, and then click **Licensing**.
2. Click **Generate Host ID** in the **Upgrades** section.
   Depending on the browser, the file 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 li-

cense.

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

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.

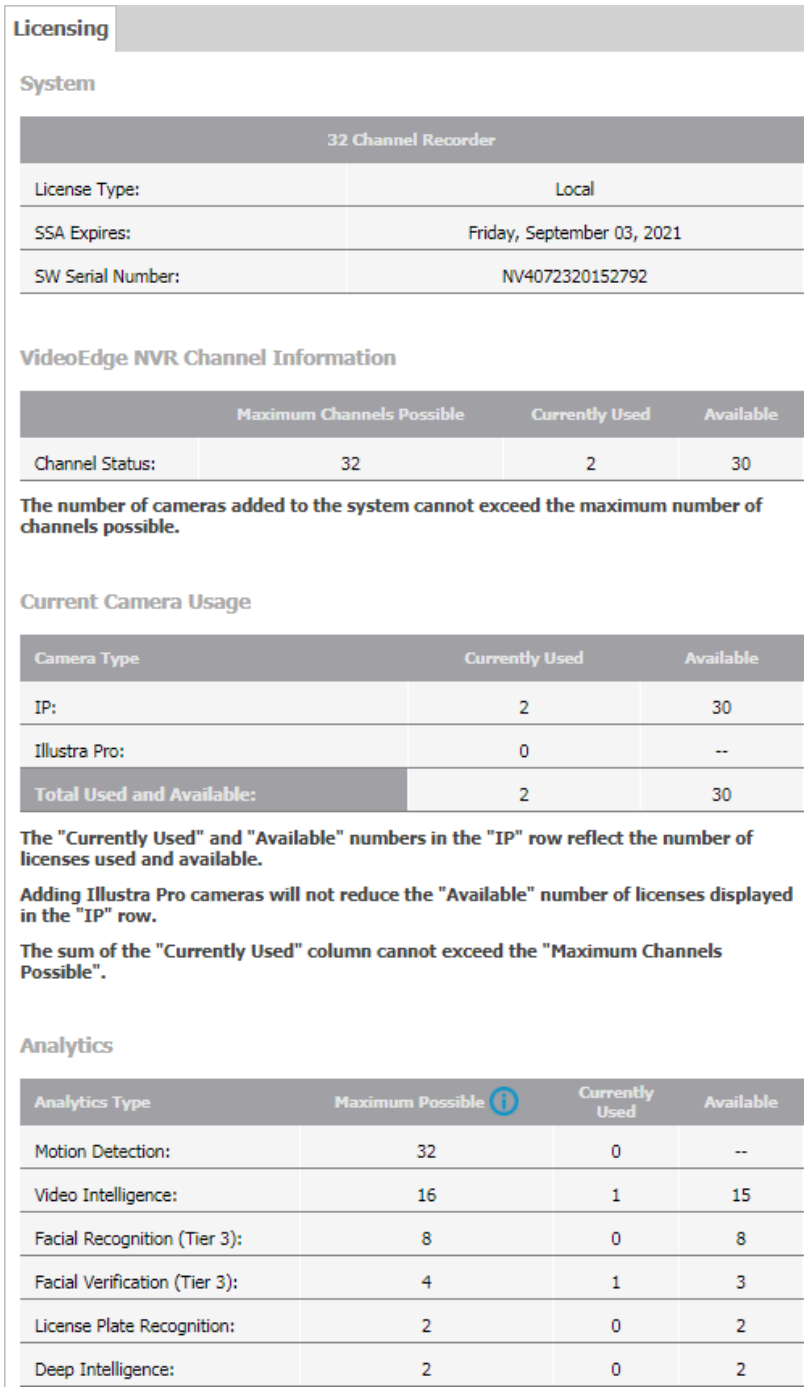
To access licenses for objects such as cameras, analytics, facial recognition, and facial verification devices, you must configure VideoEdge to connect to the victor Application Server. Unlike Local licensing, Centralized camera, analytic, facial verification and facial recognition licenses are not linked 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 38: Licensing status it the VideoEdge Admin GUI



Licensing

System

32 Channel Recorder	
License Type:	Local
SSA Expires:	Friday, September 03, 2021
SW Serial Number:	NV4072320152792

VideoEdge NVR Channel Information

	Maximum Channels Possible	Currently Used	Available
Channel Status:	32	2	30

The number of cameras added to the system cannot exceed the maximum number of channels possible.

Current Camera Usage

Camera Type	Currently Used	Available
IP:	2	30
Illustra Pro:	0	--
Total Used and Available:	2	30

The "Currently Used" and "Available" numbers in the "IP" row reflect the number of licenses used and available.

Adding Illustra Pro cameras will not reduce the "Available" number of licenses displayed in the "IP" row.

The sum of the "Currently Used" column cannot exceed the "Maximum Channels Possible".

Analytics

Analytics Type	Maximum Possible	Currently Used	Available
Motion Detection:	32	0	--
Video Intelligence:	16	1	15
Facial Recognition (Tier 3):	8	0	8
Facial Verification (Tier 3):	4	1	3
License Plate Recognition:	2	0	2
Deep Intelligence:	2	0	2

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.

victor Centralized Licensing prerequisites

- 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.

VideoEdge license transfer

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.
- 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.

victor Centralized 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 display license status. The license status of the VideoEdge recorders is displayed on a recorder, and license-type basis.

Note: 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, ensure you have 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.

Automatically transferring a VideoEdge license

Before you begin:

- Use the License Manager installed on the victor Application Server to include VideoEdge unit information into a victor Centralized license application.

  Note: 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.

- Ensure VideoEdge is:
  - Upgraded to version 4.9 or higher.
  - Added to victor.
  - Not configured with a secondary failover role.

1. Double-click the **Licensing** icon on the desktop.
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 select **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. To view the current license information, click the VideoEdge tab and then click License Manager. 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.

1. Save the license file (.LIC) to a local directory.
2. Double-click the **Licensing** icon on the desktop.
3. Click **Add New License**.
4. Browse to the .LIC license file and select **Open**.
5. Click **Yes** to confirm the License update and service restart.

ⓘ **Note:** 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, refer to the licensing instructions PDF that is included with the license e-mail.

Configuring 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.

Manually activating victor Centralized Licensing

Use the **VideoEdge Administration Interface** to complete this task.

1. Expand the **System** menu, and then click **Licensing**.
2. In the **Choose License Type** section, select **victor Centralized License**.
3. Configure the Centralized license server as follows:
   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.
4. Click **Activate Centralized Licensing**.

Automatically activating victor Centralized Licensing

1. Click the **VideoEdge** tab in the **License Manager** that is installed in the **victor Application Server**.
2. Click **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 the 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.

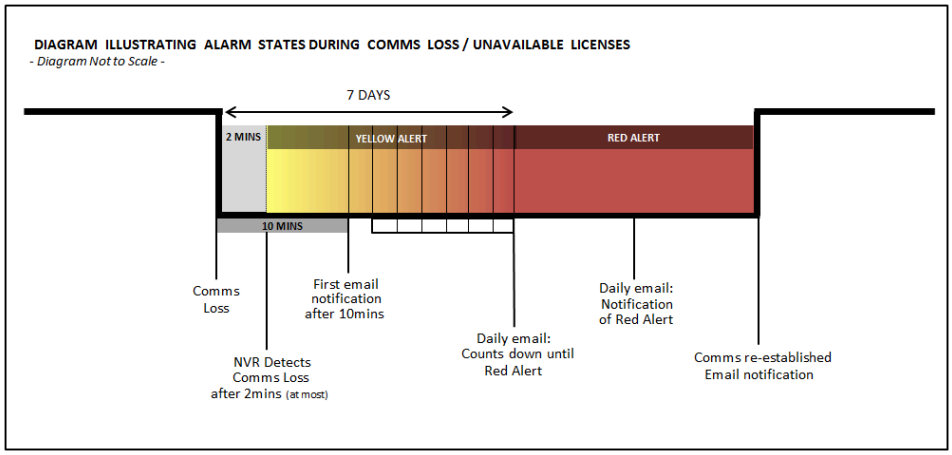
6. Click **Yes, Transfer**. A summary of the transferred recorders appears.
7. Click **OK**.

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.

Figure 39: Centralized Licensing Alerts



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 use SSA notifications you must configure your VideoEdge 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.

1. Expand the **System** menu, and then click **Licensing**.
2. In the **Software Service Agreement** section, click **Change Message**.
3. To edit the message subject, enter the required text in the **Subject** field.
4. To edit the message body, enter the required text in the **Message** field.
5. **Optional:** Click **Restore Default** to revert to the default SSA Expire Message.
6. Click the **Save** icon.

Editing SSA contacts

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, add at least one contact email address to the contacts list. You can add and re-

move contacts to/from the contact list when required.

1. Expand the **System** menu, and then click **Licensing**.
2. In the **Software Service Agreement** section, click **Edit Contacts**.
3. To add a contact, enter their email address in the **Add Email** field.
4. Click the **Add** icon.
   The email address is added to the contacts list.
5. **Optional:** To add additional contacts to the contacts list, repeat Steps 4 and 5.
6. To remove an email address from the contact list, click **Remove** next to the Email address to be removed.
7. 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.

1. Expand the **System** menu, and then click **Licensing**.
2. Click **Send Test Message** in the **Software Service Agreement** section.
   A test message is sent to the mailbox of those on the contacts list.
3. A message opens to confirm if the email has been sent or if it has failed. Click **OK**.

   ⓘ **Note:** If the message fails 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 and default user credentials that denote permissions and lockout options. You can create custom user credentials for each NVR user and can configure role permissions for LDAP groups that have been configured on your LDAP server.

⚠ **CAUTION:** For optimum security, change account passwords, configure appropriate lockout settings, prevent password re-use, and enable auto log off.

Optional NVR accounts in the Setup Wizard

Two types of optional NVR accounts can be created in the User Accounts page of the Setup Wizard, recommended NVR accounts and other NVR accounts.

ⓘ **Note:** You can configure optional accounts in Standard Security Mode and Enhanced Security Mode.

Table 44: Optional NVR accounts in the Setup Wizard

Recommended NVR accounts	Other NVR accounts
softwareadmin	operator
	viewer1
	viewer2
	viewer3

Preconfigured user accounts in the Setup Wizard

In the User Accounts page of the Setup Wizard there are four preconfigured user accounts. User accounts require updates depending on the security mode:

- **Standard security mode:** Each user account has a preconfigured user name and requires a new password.
- **Enhanced security mode:** Each user account has a preconfigured user role and requires a new user name and a new password.

Table 45: Preconfigured user accounts and update requirements

Standard security mode		Enhanced security mode	
Linux user accounts		**Linux user accounts**	
User name	**Required update**	**User role**	**Required update**
VideoEdge	New password	VideoEdge	New user name New password
root	New password	root	New user name New password
Required NVR accounts		**Required NVR accounts**	
admin	New password	admin	New user name New password
support	New password	support	New user name New password
nvrgroupadmin	New password	nvrgroupadmin	New user name New password

Note: When the unit is an Analytics Appliance or Transcoder, the VideoEdge user name and user role is `Tyco`.

Preventing a Linux user from reusing a password

To prevent a Linux user from reusing passwords, you can securely store the password history for each user.

Important: For security reasons, you cannot disable the password history feature after you enable it.

1. Access the **User Accounts** tab.
2. In the **Configure Linux User Security Settings** pane, in the **Remembered Passwords** field, enter the number of previous passwords to store.

   Note: You can select from a minimum of three passwords, a maximum of ten passwords, or use the default of 5 passwords. This applies to root, VideoEdge, Tyco or their enhanced security mode replacements.

3. Click the **Save** icon.

Default user accounts credentials

Default user accounts have corresponding roles. These roles determine user account permissions 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 46: 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 the exception of Analog (Real) and Digital PTZ, Still Image Capture, and Clip Export. • Unable to view or edit the VideoEdge Administration Interface.

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

ⓘ **Note:** These roles cannot be assigned to created users.

Table 47: 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 NVRs. • 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. Expand the **System** menu, and then click **Users and Roles**.
2. Click the **Add new user** icon.
3. Enter your account password in the **admin Password** field or the **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.
4. Enter the user name in the **Username** field.
5. Enter the password in the **New Password** field.
6. Re-enter the password in the **Confirm Password** field.

   ⓘ **Note:** When entering the user name and password, note the use of upper and lower case. The user must enter their user name and password as it has been entered at this stage.
7. From the **Role** list, select the role.
8. 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.

If an account is 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.

Locking or unlocking accounts from the users table

1. Expand the **System** menu, and then click **Users and Roles**.
2. 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.
3. Enter your account password in the **admin Password** field or the **support Password** field.
4. Click **OK**.

Unlocking accounts using the edit icon

1. Expand the **System** menu, and then click **Users and Roles**.
2. Click the **Edit** icon in the user account row you want to unlock.
3. Enter your account password in the **admin Password** field or the **support Password** field.
4. **Optional: (Customer user accounts only)** Select the **Reset Password** check box 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.
5. Select the **Unlock Account** check box to unlock the account.
6. **Optional:** Select the **Role** from the list if you want to assign a new role to the account.
7. 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 when they reach the Failed Login Retry Limit. When Delay is selected, the user is unable to log in for a configured period of time when 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:** 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.

1. Expand the **System** menu, click **Users and Roles**, and then click the **Roles** tab.
2. Click the **Edit** icon on the role you want to edit.
3. From the **Lockout Policy** list, select **Lockout selected** or **Delay selected**.
4. **Lockout selected:** In the **Retry Limit** field, enter the number of failed password attempts required for the account to lockout.
5. **Delay selected:**
    a. In the **Retry Limit** field, enter the number of failed password attempts required to initiate a delay before the user re-attempts to enter their credentials.
    b. In the **Retry Delay** field, enter the number of minutes to pass before the user re-attempts to enter their credentials.
6. **Optional:** Configure auto logout as follows:
    a. Select the **Enable Auto Logout** check box.
    b. In the **Auto Logout Interval (minutes)** field, enter the number of minutes of inactivity when the user is logged out.
7. **Optional:** From the **Inactivity Lockout Interval (days)** list, select a value.
8. **Optional:** Configure **Enhanced Password Validation** as follows:
    a. Select **Enabled** from the **Enhanced Password Validation** list.
    b. In the **Remembered Passwords** field, enter the number of previously used passwords that cannot be reused.
9. 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.

1. Expand the **System** menu, click **Users and Roles**, and then click the **Roles** tab.
2. Click the **Camera Access Settings** icon on a role to open its **Camera Access List** window.
3. Select the check boxes of the cameras you want to grant or deny access to. You can use shift-click to select multiple cameras.
4. 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.
5. Click the **Save** icon.

Assigning LDAP roles

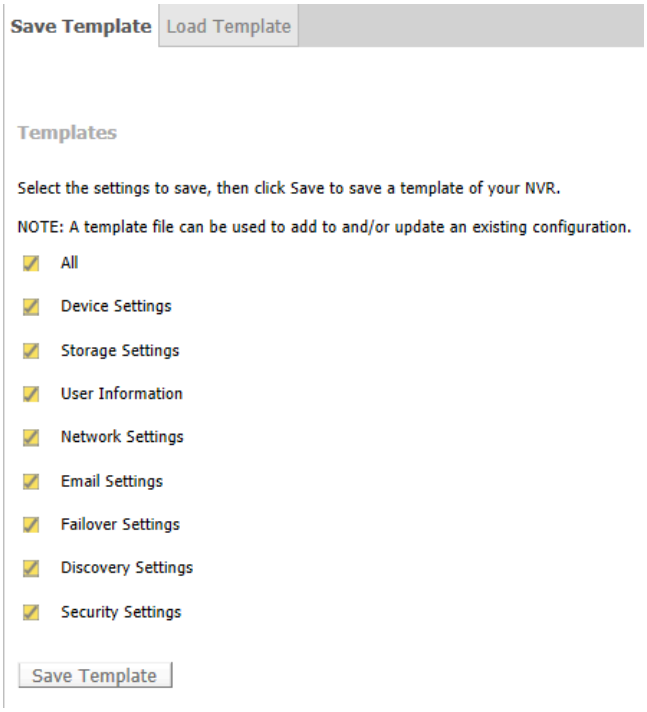
When an LDAP server has been configured on VideoEdge, you can link LDAP Groups to VideoEdge Roles. This means that all users in the LDAP Group are assigned the linked role on VideoEdge. You can also batch edit NVR LDAP Roles.

1. Expand the **System** menu, click **Users and Roles**, and then click the **LDAP Roles** tab.
2. Click the **Retrieve LDAP Groups** icon to retrieve all LDAP Groups.
3. Enter the **LDAP server password** in the field.
   All LDAP groups in the directory are displayed.
4. Select the check boxes of the LDAP groups that you want to assign an NVR role.
5. Click the **Batch Edit** icon.
6. Select the required NVR role from the **NVR Role** list.
7. 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 40: Save Template page



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.

Creating a configuration template

1. Expand the **System** menu, and then click **Templates**.

2. Select the required check boxes for the configuration settings that you want saved to the template.
3. Click **Save Template**, and then click **Save As**.
4. Navigate to the folder where you want to save the template.
5. Enter a **File name** for the template and then 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, for example,

   VideoEdgeNVRTemplate-ServerName-YYYY-MM-DDT00_00.xml VideoEdgeNVRTemplate-linux-adnvr-2012-03-26T14_02.xml

Template file

You can import NVR configuration settings saved as a template. When configuring an NVR for the first time, you can load a saved template file. This configures 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 update with the settings saved in the template file.

Importing a template file

Before you begin:
If there are camera configuration settings in the template to be imported, the relevant cameras must be connected to the NVR. For template files that include security settings, activate these settings when prompted to enable them on the NVR.

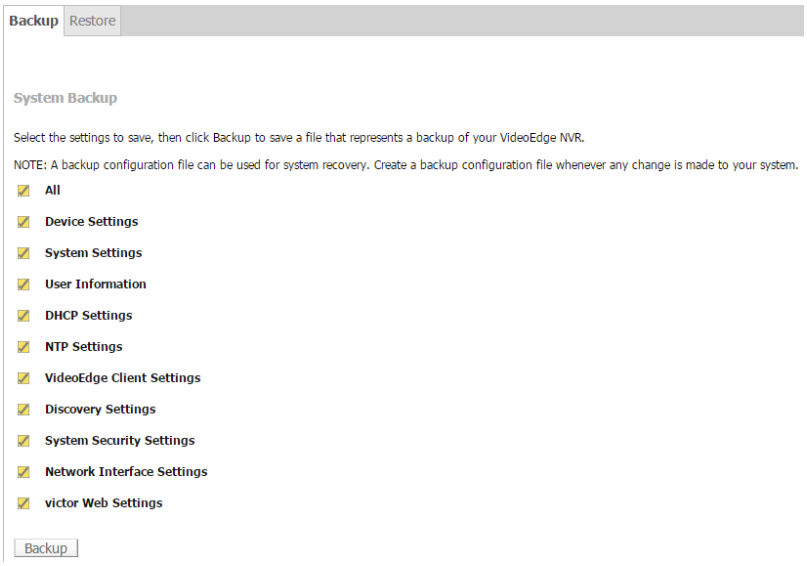
1. Expand the **System** menu, and then click **Templates**.
2. Click the **Load Template** tab and then click **Browse**.
3. Navigate to the template file you want to import.
4. Select the file and then click **Open**.
   The file path of the template file appears in the **Template File** field.
5.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

   ⓘ **Note:** If any errors occur during the template import process, a summary of the errors displays.

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 41: Backup page



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 also automatically exports a text file containing the OS settings which can be used as reference for manually configuring the OS settings.

Creating a backup file

1. Expand the **System** menu, and then click **Backup/Restore**.
2. Select the required check boxes for the configuration settings that you want saved to the backup file.
3. Click **Backup** and then click **Save As**.
4. Navigate to the folder where you want to save the backup file.

   Note: To use the backup file during a system recovery procedure, save the file to an external location, such as a USB drive.

5. 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. For example:

   VideoConfBackup-ServerName- yYYYY-mMM-dDD-h00-m00-s00_files.zip
   VideoConfBackup-ServerName- y2012-m03-d26-h14-m02-s43_files.zip

NVR 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 in accordance with the saved configurations.

Note: Only a licensed server can be restored. You cannot restore from a previously saved VideoEdge backup configuration file.

⚠ **CAUTION:** To maintain all configured Tours and Salvos relating to your NVR in victor Unified Client, complete the System Restore procedure before reconfiguring the LAN Interface Settings on the NVR.

Restoring an NVR from a backup file

1. Expand the **System** menu, and then click **Backup/Restore > Restore > Browse**.
2. Navigate to the backup file you want to use, select the file, and then click **Open**.
3. If the backup file is encrypted, select the **Backup file is encrypted** check box.
4. Click **Upload Backup**.
   A message displays, asking if you want to recover any media that is part of storage being restored.
5. 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.
6. 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. To perform a manual software update, 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.

Applying software updates

You can apply software updates or patches to the NVR, 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 *Upgrade options for victor and VideoEdge*.

After you upgrade to VideoEdge 4.9.0, you can upgrade using the following:

- VideoEdge Updater
- VideoEdge Administration Interface
- Push update
- Incremental update

VideoEdge upgrade path

You can upgrade all VideoEdge versions, except version 4.9.0, using a push update, incremental update, or manually through the Administration Interface.

Note:

- 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.
- To upgrade to VideoEdge 5.9.0+ you must upgrade from VideoEdge 5.7.1.174 or greater.

Table 48: VideoEdge upgrade paths

Upgrade from	Follow paths from left to right				
4.0.0.xxx	Upgrade to 8 GB RAM for Dell PE 2950 and R710	4.1.0.xxx	4.2.1.xxx (upgrade script)	4.3.0.412	4.4.4.122
4.0.1.242	Upgrade to 8 GB RAM for Dell PE2950 and R710	4.1.0.834	4.2.1.870 (upgrade script)	4.3.0.412	4.4.4.122
4.1.0.xxx	Upgrade to 8 GB RAM for Dell PE2950 and R710	4.2.1.870 (upgrade script)	4.3.0.412	4.4.4.122	
4.2.0.xxx	4.3.0.412			4.4.4.122	
4.3.0.xxx	4.4.4.122				
4.4.4.xxx	4.9.0.418 or 4.9.0.508 using VE Updater Tool V2.0x				
4.5.X.xxx	4.9.0.418 or 4.9.0.508 using VE Updater Tool V2.0x				
4.6.0.xxx	4.9.0.418 or 4.9.0.508 using VE Updater Tool V2.0x				
4.7.X.xxx	4.9.0.418 or 4.9.0.508 using VE Updater Tool V2.0x				
4.8.X.xxx	4.9.0.418 or 4.9.0.508 using VE Updater Tool V2.0x				
4.9.0.418	4.9.0.496 or 4.9.0.508				
4.9.0.496+	Any version up to and including 5.7.1.xxx				
5.7.1.174	5.7.1.204 or 5.9.0.280 or 6.0.0.328 or 6.1.0.256				
5.7.1.204	5.9.0.280 or 6.0.0.328 or 6.1.0.256				
5.9.0.226	5.9.0.280 or 6.0.0.328 or 6.1.0.256				
5.9.0.234	5.9.0.280 or 6.0.0.328 or 6.1.0.256				
5.9.0.280	6.0.0.328 or 6.1.0.256				
6.0.0.318	6.0.0.328 or 6.1.0.256				
6.0.0.328	6.0.0.328 or 6.1.0.256				
6.1.0.256	6.1.1.410				

Updating VideoEdge

1. Log on using the softwareadmin user credential:
   a. In the **Username** field, enter `softwareadmin`.
   b. In the **Password** field, 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.
3. Select the update or patch file, and then click **Open**. The name and file path of the patch file appears in the **Upload New Package** field.
4. Click **Upload**. The uploaded package displays in the **Uploaded files** list.
5. Select the new package from the list, and then click **Install**.

   ⓘ **Note:** The software upgrade process interrupts recording and the recorder automatically reboots, as necessary.
6. After the NVR reboots, select the uploaded package and then click **Delete**.
7. Click **Logout** and then click **OK**.

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 displays 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.

Updating camera handler packs

1. Log in using the softwareadmin user credentials:
   a. In the **Username** field, enter `softwareadmin`.
   b. In the **Password** field, 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 can vary depending on the browser.
3. Select the camera handler pack, and then click **Open**. The name and file path of the pack appears in the **Upload New Package** field.
4. Click **Upload**. The uploaded package displays in the **Uploaded files** list.
5. Select the new package from the list, and then click **Install**.
6. Click **Logout**, and then click **OK**.

Failover considerations

When a software update is applied either using a push update or applied manually using the Administration Interface, NVR services will restart. Temporary NVR service outage is expected when an update is applied.

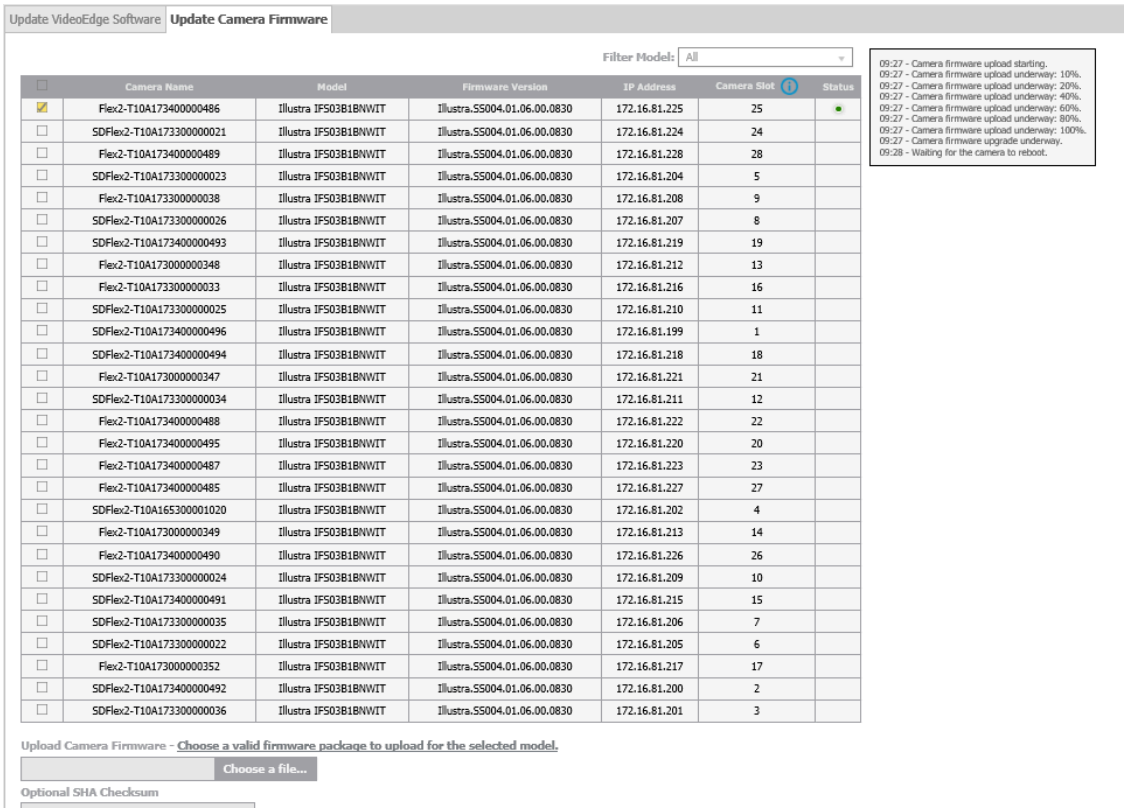
Schedule when NVR upgrades are applied and expect a loss of video when services restart. When upgrading NVRs which are being monitored by a secondary (Failover) NVR you need to stop Server Monitoring to prevent the secondary NVR taking over when the upgraded primary NVR's services stop.

Applying camera firmware updates

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 is displayed 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 42: Update Camera Firmware page



Updating camera firmware

1. Log in using the softwareadmin user credentials:
   a. In the **Username** field, enter `softwareadmin`.
   b. In the **Password** field, 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 check box 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 then 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 displays in the **Firmware Package** list.
8. Select the check box of the firmware package you want to apply.
9. **Optional:** Select the **Initial Reboot** check box to reboot the camera prior to the firmware upgrade.
10. Click **Upgrade**.

Deleting an uploaded firmware package

1. Log in using the softwareadmin user credentials:
   a. In the **Username** field, enter `softwareadmin`.
   b. In the **Password** field, 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 check box of the firmware package you want to delete.
4. Click **Delete**, and then click **OK**.

Serial protocols

The serial protocols that are supported by your NVR can be viewed on the Serial Protocols page. The default settings for each protocol can also be viewed.

Viewing serial protocols

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

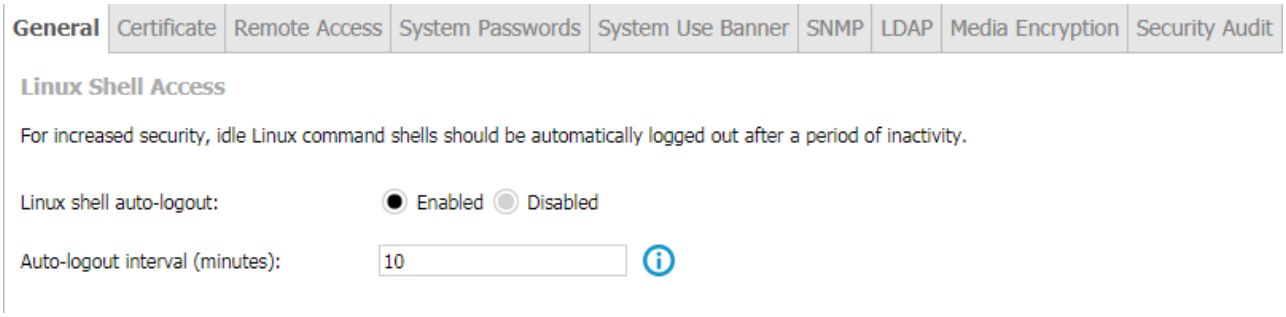
Security configuration

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 43: Security Configuration on the General page



Configuring shell auto-logout for Linux users

1. Expand the **System** menu, and then click **Security Configuration**. The **General** page opens on the Linux Shell Access configuration.

2. Click **Enabled** to enable Linux shell auto-logout or click **Disabled** to disable Linux shell auto-logout.
3. **Optional:** Edit the **Auto-logout interval** time. The minimum value is 5 minutes and the maximum value is 300 minutes.
4. Click the **Save** icon. A re-authentication window opens.
5. Enter your admin password and then click **OK**. A message displays as follows: Saved successfully.

Certificate

From the Certificate page, configure Certificate Authority Settings, Certificate Template Settings, and Certificate Settings.

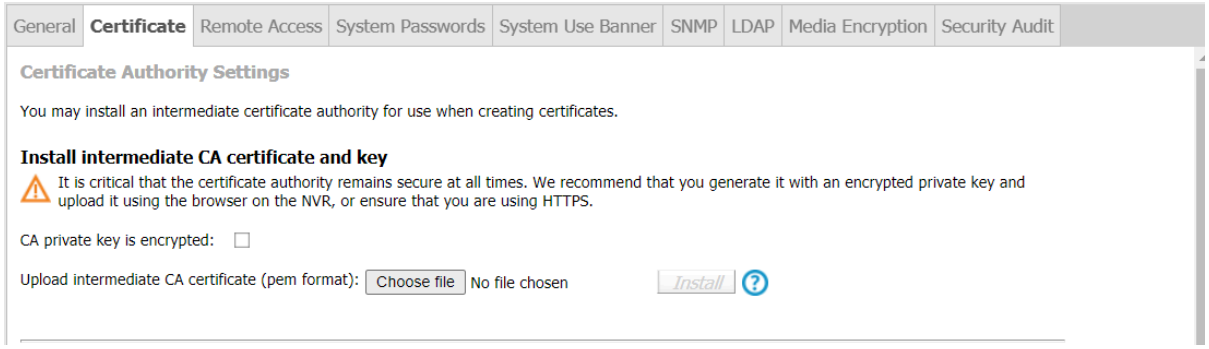
Certificate authority settings

Install an intermediate certificate authority (CA) on VideoEdge from the Certificate Authority Settings section of the Certificate page. Use this CA when signing the NVR certificate.

Note:

- Deploy the appropriate certificate chain to client computers.
- The CA must be PEM-encoded and contain the CA certificate and encrypted private key.

Figure 44: Certificate authority settings



When the CA installation is complete, view the details in the Certificate Authority Settings section of the Certificate page.

Figure 45: Installed intermediate CA

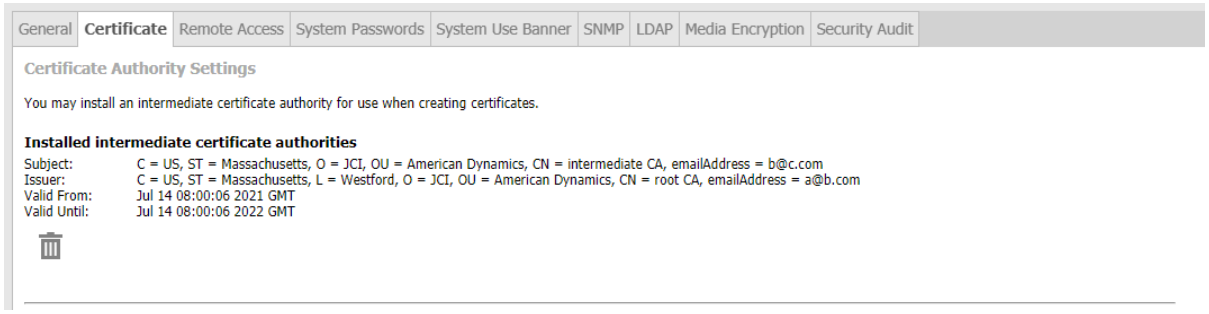


Figure 46: Create certificate with no CA

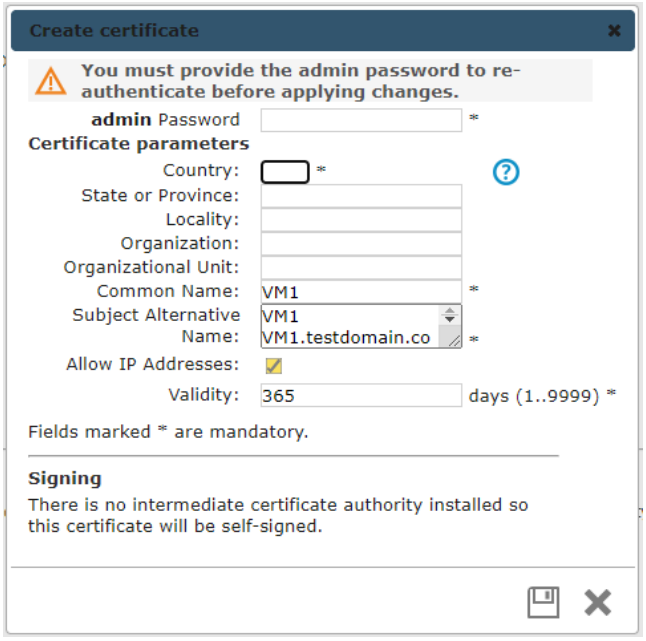
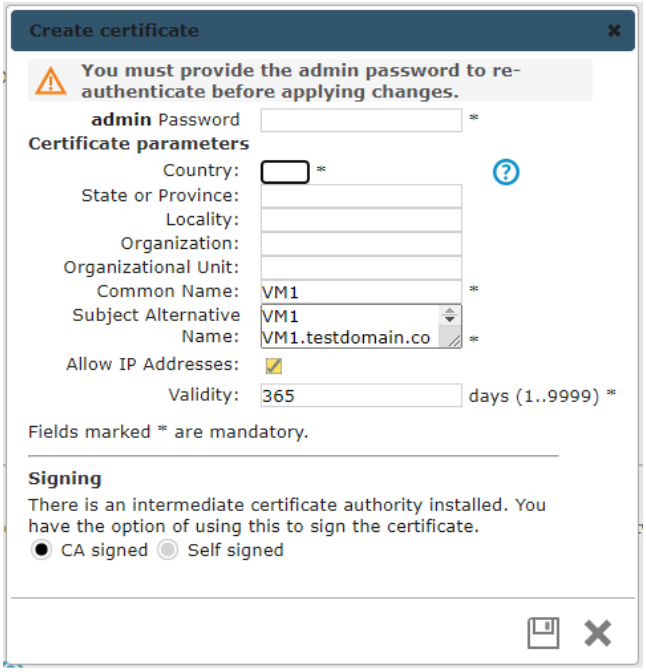
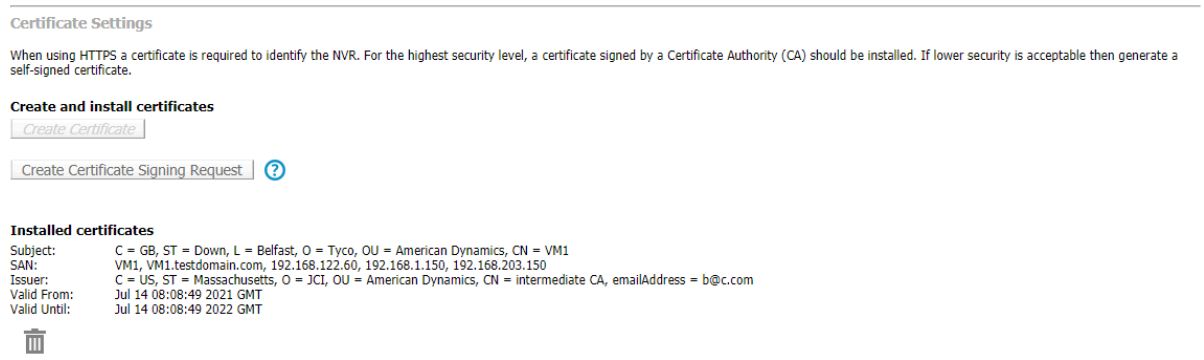


Figure 47: Create certificate with a CA



When you generate a new certificate for the NVR, you can choose to use the installed CA to sign the certificate. CA-signed certificates can be identified in the Installed certificates section of the Certificate page, under Issuer details.

Figure 48: Certificate Settings



Installing a certificate authority for VideoEdge

Before you begin:
To protect the decryption password from interception on the network, use the NVR browser or access the page using HTTPS.

1. From the **System** menu, click **Security Configuration** and then click **Certificate**.
2. **Optional:** Select the **CA private key is encrypted** check box, and then enter a **Decryption Password**.
3. Click **Choose file**.
4. Navigate to the required .PEM file, click **Open**, and then click **Install**.

Installing root and intermediate certificates for victor

Before you begin:
When using an installed CA or third party CA, you must install the root and intermediate certificate on your victor Unified Client PC.

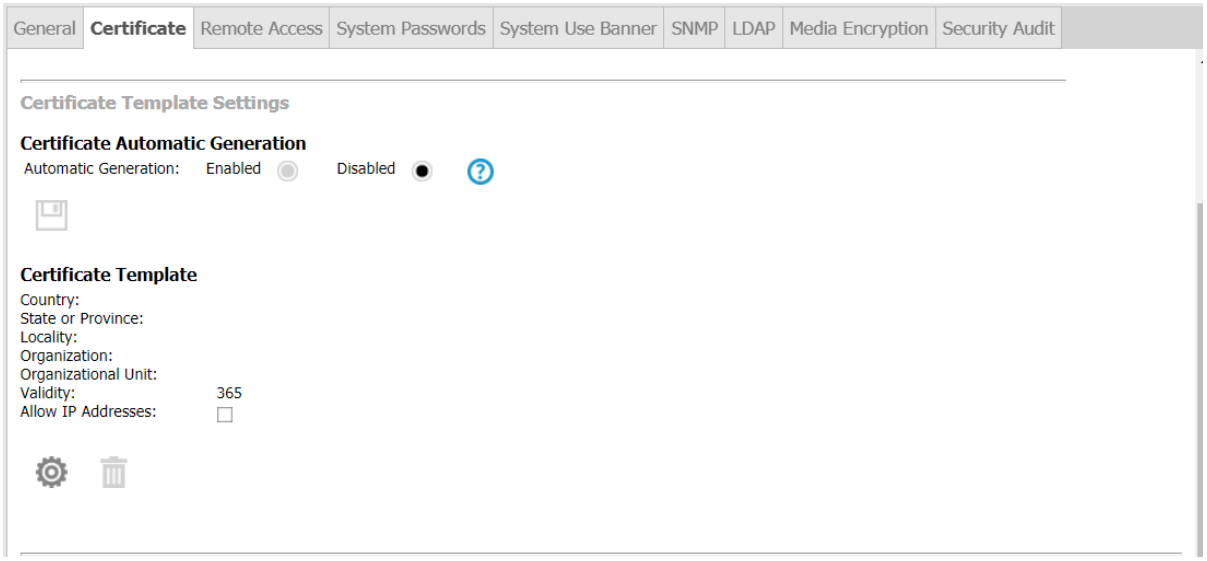
1. Open the **Microsoft Management Console** (MMC) by clicking **Windows** > **MMC** > **Return**.
2. Click **File**, and then click **Add/Remove Snap-In**.
3. From the **Available snap-ins**, select **Certificates**, and then click **Add**. The **Certificates snap-in Wizard** launches.
4. Click **Computer Account**, and then click **Next**.
5. Ensure the **Local Computer** option is selected. This is enabled by default.
6. Click **Finish**, and then click **OK**. A certificates menu appears under the **Console Root**, located on the left hand module of MMC.
7. Select the **Certificates** menu.
8. Select **Trusted Root Certification Authorities** and then select **Certificates**.
9. Select **More Actions**, located on the right hand module of MMC.
10. Navigate to **All Tasks**, and then click **Import**.
    The **Certificate Wizard** launches.
11. Click **Next**, and then click **Browse**.
12. Navigate to your **Root Certificate**, click **Open**, and then click **Next**.
13. Click **Next**, and then click **Finish**. A message displays that the import was successful.
14. From the certificates menu on the left hand module of MMC, click **Intermediate Certification Authorities**.
15. Select **Certificates**, and then select **More Actions**.
16. Navigate to **All Tasks**, and then click **Import**. The **Certificate Wizard** launches.

17. Click **Next**, and then click **Browse**.
18. Navigate to your **Intermediate Certificate**, click **Open**, and then click **Next**.
19. Click **Next**, and then click **Finish**. A message displays that the import was successful.

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.

Figure 49: Certificate Template Settings



Creating a certificate template

1. From the **System** menu, click **Security Configuration**, and then click **Certificate**.
2. Click the **Change template** icon.
3. Complete the **Certificate parameters** window as follows:
   a. In the Country field, enter the country code.
   b. **Optional:** Enter the **State or Province**.
   c. **Optional:** Enter the **Locality**.
   d. **Optional:** Enter the **Organization**.
   e. **Optional:** Enter the **Organizational Unit**.
   f. **Optional:** Ensure **Allow IP Addresses** is enabled.
   g. Enter the **Validity**.
4. Click the **Save** icon.

Enabling certificate automatic generation

You must create a certificate template to enable certificate automatic generation. By default, certificate automatic generation is disabled. If the certificate template is deleted, 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.

1. From the **System** menu, click **Security Configuration**, and then click **Certificate**.
2. In the **Certificate Automatic Generation** section, click **Enabled**.
3. Click the **Save** icon.

Certificate settings

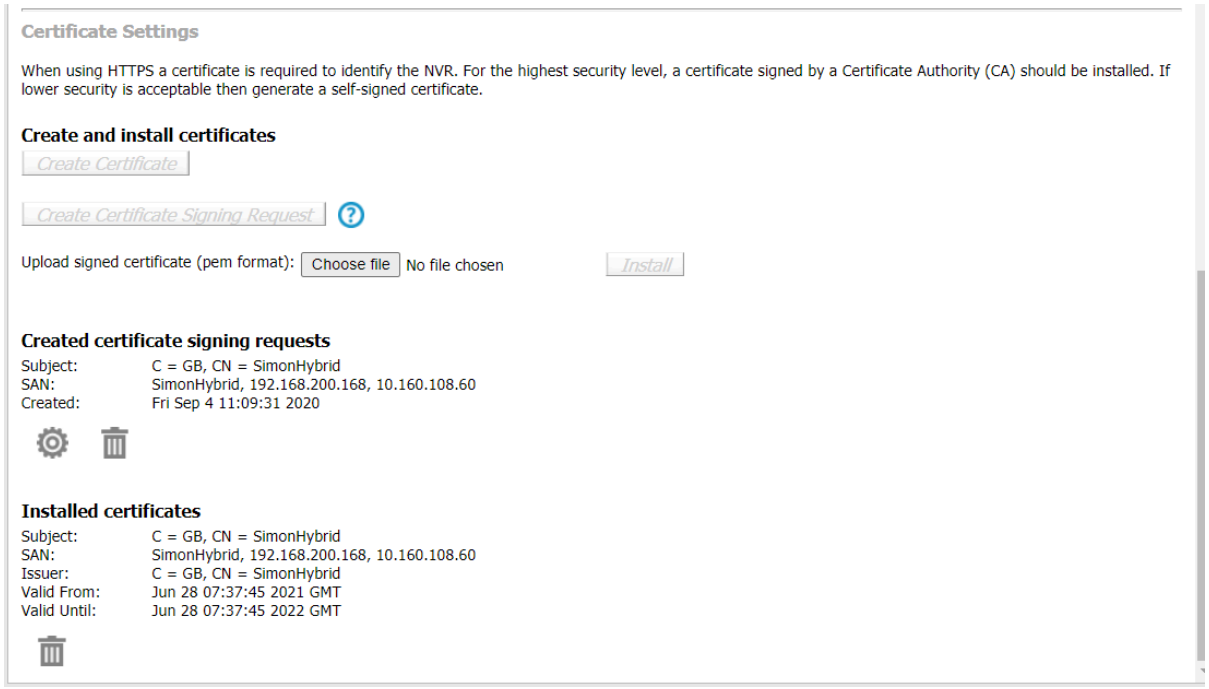
VideoEdge is provided with a default certificate. After you configure VideoEdge, install an NVR-specific certificate. Depending on your security requirements, you can then use one of the following certificate options:

- **Create a self-signed certificate:** If you have a lower security requirement, create a self-signed certificate. Installing the certificate on victor Unified Client and victor Application Server allows communication between the recorder and the client.
- **Create a certificate authority (CA) signing request:** If you have stringent security requirements, create a certificate signing request for a third party certificate authority (CA) and then upload the certificate to VideoEdge. This third party CA provides a higher level of security.

ⓘ **Note:**

- When using an installed CA or third party CA, you must install the root and intermediate certificate on your victor Unified Client PC.
- When using HTTPS communication, you must use a PKI certificate to provide secure encrypted communications and identify the NVR to the connecting device.

Figure 50: Certificate Settings



Creating a self-signed certificate

1. From the **System** menu, click **Security Configuration**, and then click **Certificate**.
2. Click **Create Certificate**.
3. For re-authentication, enter your password.
4. Complete the **Certificate parameters** as follows:
   a. In the **Country** field, enter the country code.

      ⓘ **Note:** You must enter the country code as it appears in the standard SSL Certificate Country Code.

   b. **Optional:** Enter the **State or Province**.
   c. **Optional:** Enter the **Locality**.

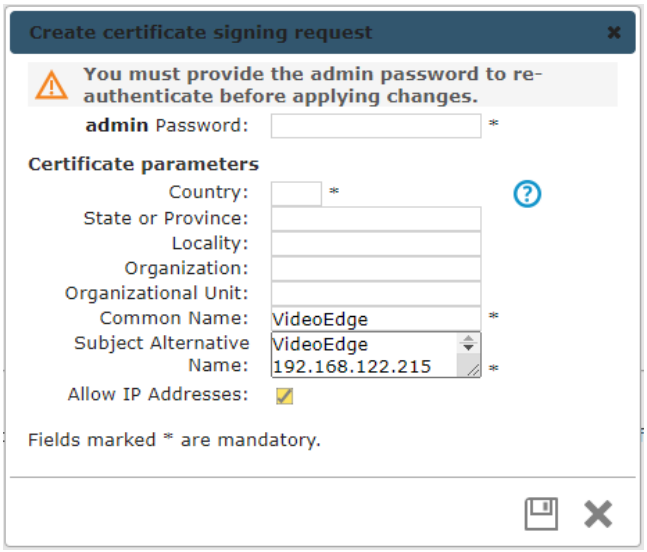
d. **Optional:** Enter the **Organization**.
e. **Optional:** Enter the **Organizational Unit**.
f. **Optional:** Edit the **Common Name**.
g. **Optional:** Edit the **Subject Alternative Name**.
h. **Optional:** Ensure **Allow IP Addresses** is enabled.
i. **Optional:** Edit the Validity.

5. Click the **Save** icon. The new certificate is activated.
6. Click the **Cancel** icon, and then restart your browser.

Creating a certificate signing request

1. From the **System** menu, click **Security Configuration**, and then click **Certificate**.
2. Click **Create Certificate Signing Request**.

Figure 51: Certificate signing request



3. For re-authentication, enter your password.
4. Complete the **Certificate parameters** as follows:
   a. In the **Country** field, enter the country code.

      Note: You must enter the country code as it appears in the standard SSL Certificate Country Code.

   b. **Optional:** Enter the **State or Province**.
   c. **Optional:** Enter the **Locality**.
   d. **Optional:** Enter the **Organization**.
   e. **Optional:** Enter the **Organizational Unit**.
   f. **Optional:** Edit the **Common Name**.
   g. **Optional:** Edit the **Subject Alternative Name**.
   h. **Optional:** Ensure **Allow IP Addresses** is enabled.
5. Click the **Save** icon. The certificate request displays in PEM format.
6. Copy and paste the request into an email or alternative file for sending to the CA.
7. Click the **Cancel** icon.

Result

A summary of the certificate request displays on the Certificates page. To delete an awaiting certificate request, click the **Delete** icon.

Installing a CA signed certificate

1. From the **System** menu, click **Security Configuration**, and then click **Certificate**.
2. Click **Browse**, and then navigate to the signed certificate.
3. Click **Open**, and then click **Install**.

Remote access services

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

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

Secure shell (SSH) is an encrypted network protocol for text based sessions on remote machines from another machine that has network access. 'PuTTY' is a common piece of software used to access remote machines by SSH.

Remote desktop protocol (RDP) is a graphical desktop sharing protocol developed by Microsoft. It allows control of remote machines, such as VideoEdge, from another machine that has network access. RDP is available in Windows, and is a common piece of software used to access remote machines using VideoEdge XRDP client.

ⓘ **Note:** When accessing VideoEdge remotely, log on using the **VideoEdge** user account.

Enabling and disabling remote access services

1. Expand the **System** menu.
2. Click **Security Configuration**, and then click **Remote Access**.
3. Navigate to the **Remote Access Services** table.
4. Click the **Enabled** icon in the entry you want to enable or disable remote access.
5. Click **OK**.

Remote web access services

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.

Enabling, disabling, and restricting Remote Web Access Services

1. Expand the **System** menu.
2. Click **Security Configuration**, and then click **Remote Access**.
3. Navigate to the **Remote Web Access** table.
4. Enable or disable a **Remote Web Access** type as follows:
   a. Select the **Enabled** icon to enable a **Remote Web Access** type. The **Enabled** icon is green when selected.
   b. Deselect the **Enabled** icon to disable a **Remote Web Access** type. The **Enabled** icon is gray when deselected.
5. A re-authentication window opens. Enter your admin password, and then 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.

Transport Layer Security

VideoEdge supports Transport Layer Security (TLS) v1.2 only.

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.

Editing the web server configuration

1. Expand the **System** menu.
2. Click **Security Configuration**, and then click **Remote Access**.
3. Navigate to the **Web Server Ports and Protocols** section.
4. **Optional:** Click **HTTP and HTTPS** to enable HTTP and HTTPS communication.
5. **Optional:** Click **HTTPS only** to enable HTTPS communication only.
6. Click the **Save** icon. A re-authentication and warning message displays.
7. Enter your admin password, and then click **OK**. When the web server configuration is complete, a message displays as follows: Saved successfully.

System passwords

On the System Passwords page, you can change the VideoEdge or Tyco Linux account password, and the root Linux account password.

In Enhanced security mode, the pre-configured Linux accounts 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 are 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.

On the System Passwords page you can enable and disable access for the Linux support user.

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

⚠ **CAUTION:** For security reasons, ensure that you change the Linux account passwords for VideoEdge/Tyco, and root.

Changing the VideoEdge Linux account password

1. Expand the **System** menu, and click **Security Configuration**.
2. Click the **System Passwords** tab.
3. **When viewing in HTTP only:** Click **Change to HTTPS**.
   A browser warning page displays stating there is a problem with the website security certificate. This warning only displays when the default NVR certificate or a certificate not signed by a trusted root CA is installed.
4. Click **Continue to this website (not recommended)**.

   ⓘ **Note:** The wording may differ depending on the browser.
5. In the **Linux Account: VideoEdge** section, change the VideoEdge Linux account password as follows:
   a. Enter the **Current Password**.

      ⓘ **Note:** The default VideoEdge Linux account password in Standard security mode is **VideoEdge**.

   b. Enter the **New Password**.
   c. In the **Confirm Password** field, re-enter the new password .

      ⚠ **CAUTION:** It is extremely important that you remember this password. If necessary, write this password down and store it securely.
6. Click the **Save** icon at the top of the page.

Changing the Tyco Linux account password

1. Expand the **System** menu, and click **Security Configuration**.
2. Click the **System Passwords** tab.
3. **Optional:** When viewing in HTTP, click **Change to HTTPS**.
   A browser warning page displays stating there is a problem with the website security certificate. This warning only displays when the default NVR certificate or a certificate not signed by a trusted root CA is installed.
4. Click **Continue to this website (not recommended)**.

   ⓘ **Note:** The wording can differ depending on the browser.
5. In the **Linux Account: Tyco** section, to change the Tyco Linux account password, complete the following steps:
   a. Enter the **Current Password**.

      ⓘ **Note:** The default Tyco Linux account password in standard security mode is `Tyco`.

   b. Enter the **New Password**.

c. In the **Confirm Password** field, re-enter the new password.

⚠ **CAUTION:** It is extremely important that you remember this password. If necessary, write this password down and store it securely.

6. At the top of the page, click the **Save** icon.

Changing the root Linux account password

1. Expand the **System** menu, and then click **Security Configuration**.
2. Click the **System Passwords** tab.
3. **When viewing in HTTP only:** Click **Change to HTTPS**.
   A browser warning page displays stating there is a problem with the website security certificate. This warning only displays when the default NVR certificate or a certificate not signed by a trusted root CA is installed.
4. Click **Continue to this website (not recommended)**.

   ⓘ **Note:** The wording may differ depending on the browser.

5. In the **Linux Account: root** section, change the root Linux account password as follows:
   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, write this password down and store it securely.

6. Click the **Save** icon at the top of the page.

Configuring Linux support user access

1. Expand the **System** menu, and then click the **System Configuration**.
2. Click the **System Passwords** tab.
3. In the **Linux User Access: support** section, configure **Support Access** as follows:
   - 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** automatically changes access permissions for the Linux support user. No save is required.

Preventing Linux user password reuse

To prevent a Linux user from reusing passwords, you can securely store the password history for each user.

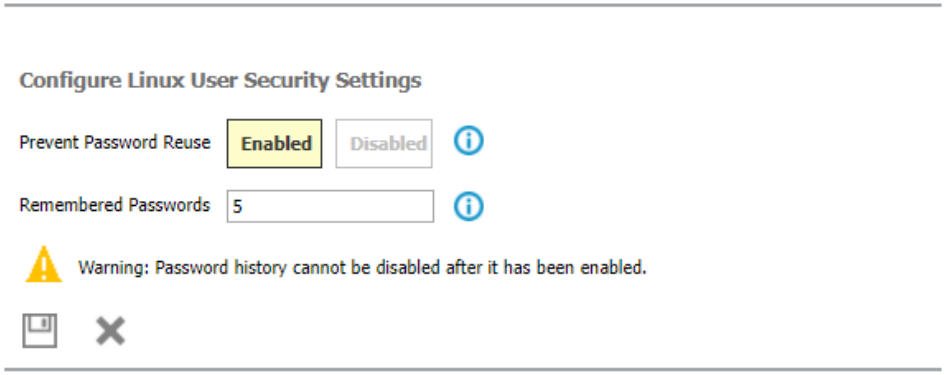
➤ **Important:** For security reasons, you cannot disable the password history feature after you enable it.

1. Expand the **System** menu, and click **Security Configuration**.
2. Click the **System Passwords** tab.
3. In the **Configure Linux User Security Settings** pane, complete the following steps:
   a. In the **Prevent Password Reuse** row, click **Enabled**.
   b. In the **Remembered Passwords** field, enter the number of previous passwords to store.

      ⓘ **Note:** You can select from a minimum of three passwords, a maximum of ten passwords, or use the default of 5 passwords. This applies to root, VideoEdge, Tyco or their enhanced security mode replacements.

c. Click the **Save** icon.

Figure 52: Linux user password validation dialog



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.

Configuring the system use banner for non-XRDP clients

1. Expand the **System** menu, and then click **Security Configuration**.
2. Click the **System Use Banner** tab.
3. Enter the required notifications in the text field.

   ⓘ **Note:** If the text field is empty, the **System Use Banner** will not display during login.
4. Click the **Save** icon.

Configuring the system use banner for XRDP clients

The system use banner displays 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 displays when connecting by RDP.

1. Click the **System** menu and **Security Configuration**.
2. Click the **System Use Banner** tab.
3. Click **Browse**.
4. Select the file you want to use for the system use banner, and click **Open**.

   ⓘ **Note:** Only bitmap files are supported, they can be identified by the **.bmp** file extension. Some XRDP clients can be sensitive to the .bmp image size.
5. 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 VideoEdge remotely, use the VideoEdge user account to log on. When accessing Analytic Appliance or Transcoder remotely, use the Tyco user account to log on.

Enabling and disabling SNMP services

1. Expand the **System** menu.
2. Click **Security Configuration**, and then click **SNMP**.
3. On the **SNMP Configuration** page, in the **Read-only Community** field, enter a value.
4. In the **SNMP Status** section, click **Enabled** to enable SNMP services, or click **Disabled** to disable SNMP services.
5. Click the **Save** icon.
6. On the re-authentication window, enter your admin password and click **OK**.
   The following message displays: The SNMP configuration has been successfully changed.

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. Establish a secure connection before you perform the following actions:

- Log on to 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.

Enabling LDAP support

1. Expand the **System** menu.
2. Click **Security Configuration**, and then click **LDAP**.
3. Select the **Use LDAP for VideoEdge administrator and VE Client authentication** check box.
4. In the **Server Address** field, enter the LDAP Server IP address.
5. **Optional:** If you are using Active Directory on your LDAP server, select the **Use Active Directory** check box.
6. **Optional:** If you are installing an LDAP server certificate, select the **Secure Connection** check box.

   ⓘ **Note:** Contact your IT department if you require an LDAP server certificate.
7. Enter the **User Query DN**.

   ⓘ **Note:** Use the distinguished name of the organizational unit where the user belongs when entering the User Query DN.
8. Enter the **Base DN**, or to view a list of available Base DNs, click **Fetch DN**.

   ⓘ **Note:** The Base DN is the starting point for the search. Only groups in the specified Base DN are retrieved. The value must be a distinguished name that currently exists in the database.

9. **Optional:** If you have selected **Use Active Directory**, enter the **UPN Suffix**.
10. Enter the **Administrator DN**.

    ⓘ **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.

11. In the **Search Filter** field, enter a search.
12. If you selected **Secure Connection**:
    a. In the **Install LDAP server certificate** field, click **Choose file**.
    b. Navigate to the certificate, and click **Open**.
    c. In the **Install LDAP server certificate** field, click **Install**. A message displays that the installation is successful.
    d. Click **OK**.
13. Click the **Save** icon.

    ⓘ **Note:** A re-authentication window opens.

14. Enter your admin password, and click **OK**. When LDAP support is enabled, the following message displays: Saved successfully.

Media encryption

From the Media Encryption page you can view the media and license plate metadata encryption status of the NVR, import encryption keys, and export encryption keys. Export of encryption keys include all keys used for encryption, which include media encryption and LPR encryption. Media encryption status is set during the setup wizard, and is not configurable after the setup wizard is complete. License plate metadata encryption status is automatically enabled.

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

License plate recognition encryption protects specifically license plate information captured by LPR cameras. An encryption key is required to decrypt sensitive information such as vehicle owner details, registration numbers, and other identifying information.

Exporting the media encryption key

If you enable media encryption during the Setup Wizard, you can export the media encryption key. However, you can always export the license plate metadata encryption key since the license plate metadata encryption status is always enabled.

If you transfer a hard drive with encrypted media or license plate recognition data to a new NVR, you must import the exported encryption keys to the new NVR to decrypt and access the stored data.

Complete the following steps to export an encryption key:

1. Expand the **System** menu, and click **Security Configuration**.
2. Click the **Media Encryption** tab.
3. Click **Export encryption key**.

   ⓘ **Note:** Ensure that you store the encryption keys securely.

Importing the media encryption key

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

⚠ **CAUTION:** Importing an incorrect encryption key on a system with encrypted data, or importing an encryption key on a system with unencrypted data, will render the existing data inaccessible.

Complete the following steps to import an encryption key:

1. Expand the **System** menu, and click **Security Configuration**.
2. Click the **Media Encryption** tab.
3. Click **Browse**.

   ⓘ **Note:** The name of this button can differ depending on what browser you are using.
4. Navigate to where you have stored the encryption key and click **Open**.
5. 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. Ensure that you change this setting.
- Amber: The setting is partially secure. Ensure 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 the general network settings, LAN Interface settings, DHCP Server settings, and WAN settings. The Network menu contains the following submenus:

- **General:** configure general network settings.
- **LAN Interface:** edit the LAN settings for each installed NIC.
- **Routing:** configure network routing properties.
- **DHCP Server:** 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:** configure the NVR to operate in a wide area network.
- **Secure Connection:** enable or disable victor Secure Connection software. The Secure Connection submenu contains the victor Secure Connect Settings section.

Table 49: Network icons

Icon	Name	Function
	**Save**, **Save static route configuration**	Save
	**Cancel**	Cancel
	**Add new static route**	Add new static route
	**Remove static route**	Remove static route

Table 49: Network icons

Icon	Name	Function
	**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

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 using the Internet. This design provides 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 NVR can be set up in a number of configurations to meet your bespoke requirements. For examples, see the Figure 53 and the Figure 54.

Network interface controllers

Each variant of the NVR is supplied with two Network Interface Controllers (NICs). You can install additional network cards to increase the number of connections, if required. For more information, contact American Dynamics.

Network connections

The NVR 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 advantageous because 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.

ⓘ **Note:** An additional NIC can also be used to connect to iSCSI network storage increasing the storage space available to the NVR.

Network settings example

Figure 53: VideoEdge Hybrid NVR example

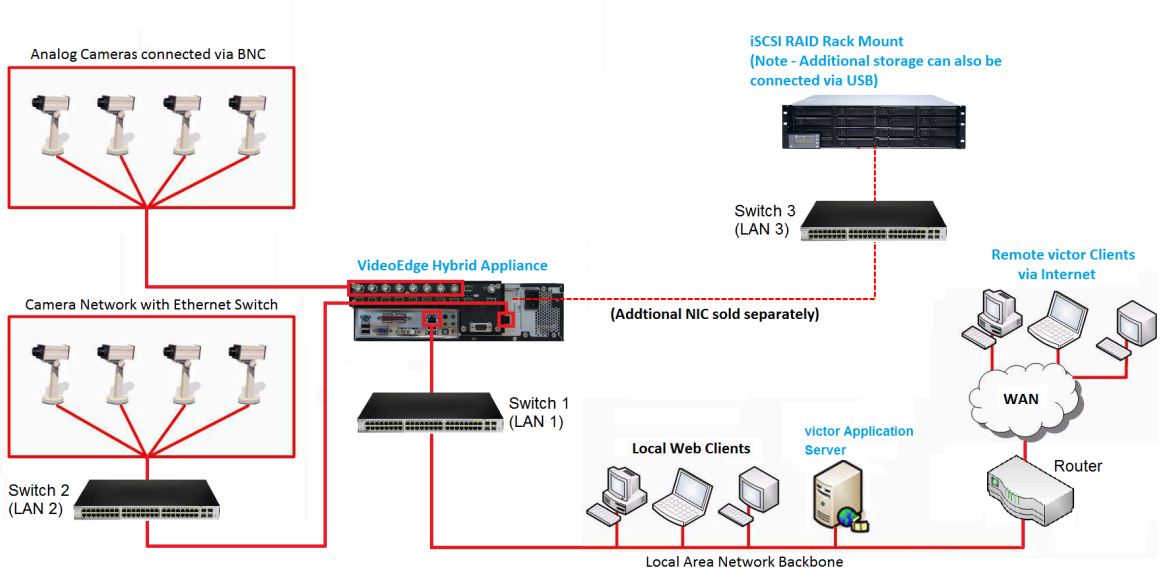
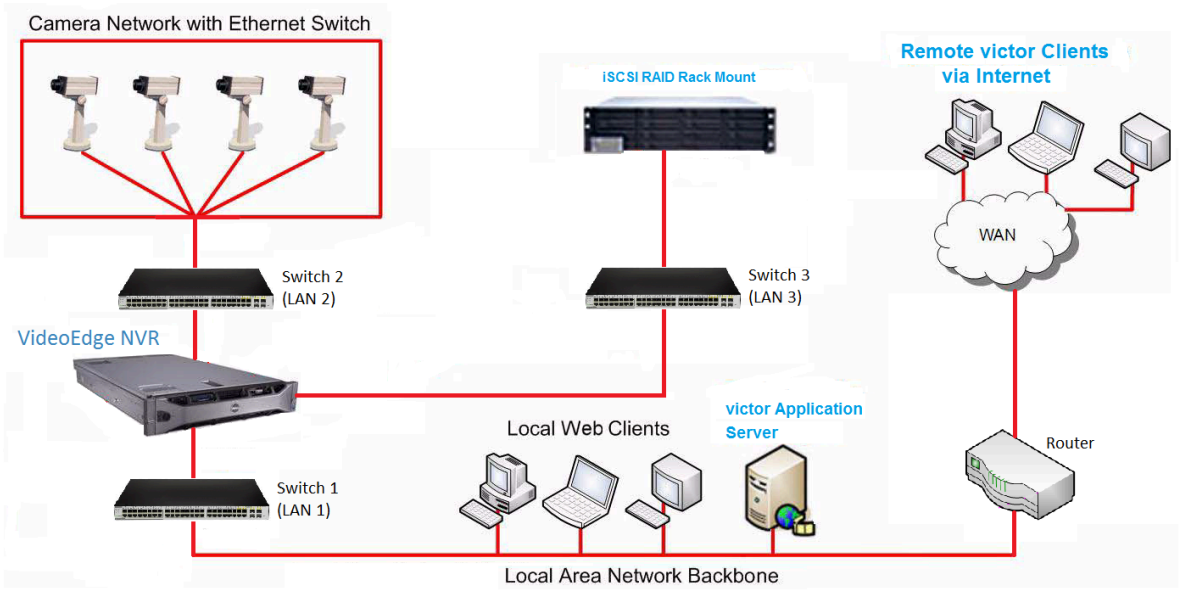


Figure 54: VideoEdge NVR example



- **LAN 1:** connects the NVR to the network with client PCs. Client PCs usually access the NVR through this port.

ⓘ **Note:** The LAN 1 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. For more information about configuring network routes, see Routing.

- **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 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. Because 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 the 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

Use the Network General page to configure the general network settings for an NVR. When you configure the required setting, to complete the change, click the Save icon.

Table 50: Network General page

Field	Description
Domain Name	The domain portion of the VideoEdge's full name. For example, if you have a machine with the name `videoedge.company.org`, use the domain name `company.org`.
Domain Name Servers	A list of DNS servers that you can use to perform hostname to IP address lookups.
Default Gateway	The IP address of the router that can reach non-local networks.
RTSP Port	The TCP port that clients use, such as victor, to request video streams.
RTSP Encryption	Defines if RTSP messages are to be encrypted for extra security.
SNMP Port	The UDP port that the SNMP server uses.
UPnP	When enabled clients can discover VideoEdge. For example, victor uses this mechanism to discover VideoEdge recorders.
Multicast	Allows a single RTSP stream to be used when being viewed by multiple clients, rather than creating a new stream for every new client.
Multicast Start and End Ports	Select the port range that the RTSP multicast stream is available on. This allows more than one client to have access to the same RTSP stream that is hosted on a port in the range.

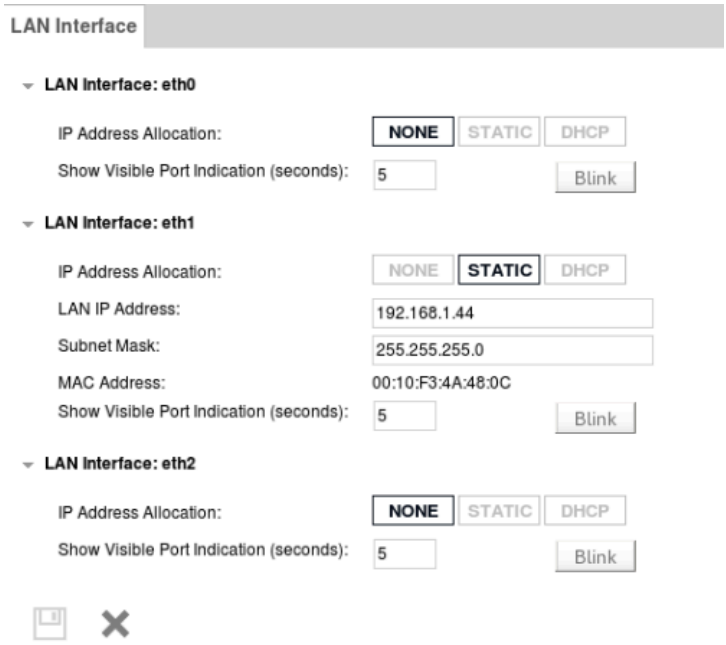
Table 50: Network General page

Field	Description
NTP Status	Allows VideoEdge to synchronize with an external time reference. Use NTP to improve time consistency between cameras, VideoEdge, and victor Clients. This can improve media search results.
WAN Bandwidth Target	The WAN bandwidth that VideoEdge uses, by targeting an average bandwidth usage over a period of time.
LAN Bandwidth Target	The LAN bandwidth that VideoEdge uses, by targeting an average bandwidth usage over a period of time.
Client Traffic Smoothing	Pace packet transmission over a period of time to reduce micro-bursting in the network and prevent packet drops due to congestion. Pacing can add a small amount of additional latency to client streams. Use the Client traffic smoothing value to set the packet transmission window. The system caps the specified value to the frame duration.

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 55: 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:** Do not use DHCP for all of the NVR's NICs. 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. Configure at least one NIC 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.

Enabling NICs

1. Expand the **Network** menu and click **LAN Interface**.
2. Select the LAN Interface that you want to edit.
3. To allow a DHCP Server on the LAN to assign an IP address for that NIC of the NVR, click **DHCP**.

   ⓘ **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.
4. To permanently assign an IP address and subnet mask to the NVR, click **STATIC**.

   ⓘ **Note:** When using Static IP addresses you are required to enter the IP address and subnet mask in the corresponding fields.
5. Click the **Save** icon.
6. Click **OK**.

Disabling NICs

1. Expand the **Network** menu and click **LAN Interface**.
2. Select the LAN Interface that you want to edit.
3. From the **IP Address Allocation** list, select **NONE** .

   ⓘ **Note:** When you select **NONE**, the LAN Interface options for that NIC collapse leaving only the IP Address Allocation displayed.
4. Click the **Save** icon.
5. Click **OK**.

   ⓘ **Note:** If you disable eth0 using the NVR Administration Interface it terminates 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 NICs.

Configuring LAN interface values

1. Expand the **Network** menu and click **LAN Interface**.
2. Select the LAN Interface that you want to edit.
3. Select an **IP Address Allocation** option. You must select **STATIC** to edit the LAN IP address and subnet mask.
4. In the **LAN IP Address** field, enter the required IP address.
5. In the **Subnet Mask** field, enter the required subnet mask.
6. 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

ⓘ **Note:** 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. Expand the **Network** menu and then click **LAN Interface**.
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:** 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.

1. Expand the **Network** menu and click **LAN Interface**.
2. Enter the time in seconds that you want the LED indicator to blink.
3. 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 51: Add Static Route window parameters

Parameter	Description
Interface	The interface that packets for this route are sent to.
Destination	The destination network or destination host.
Gateway	The gateway address.

Table 51: Add Static Route window parameters

Parameter	Description
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.

Adding a static route

1. Expand the **Network** menu and click **Routing**.
2. Click the **Add new static route** icon.
3. On the **Add Static Route** window, from the **Interface** list, select a network interface.
4. Configure the destination network settings.
   a. In the **Destination** field, enter the network IP address.
   b. In the **Gateway** field, enter the gateway IP address.
   c. In the **Netmask** field, enter the netmask.
   d. **Optional:** In the **Priority** field, enter route priority.

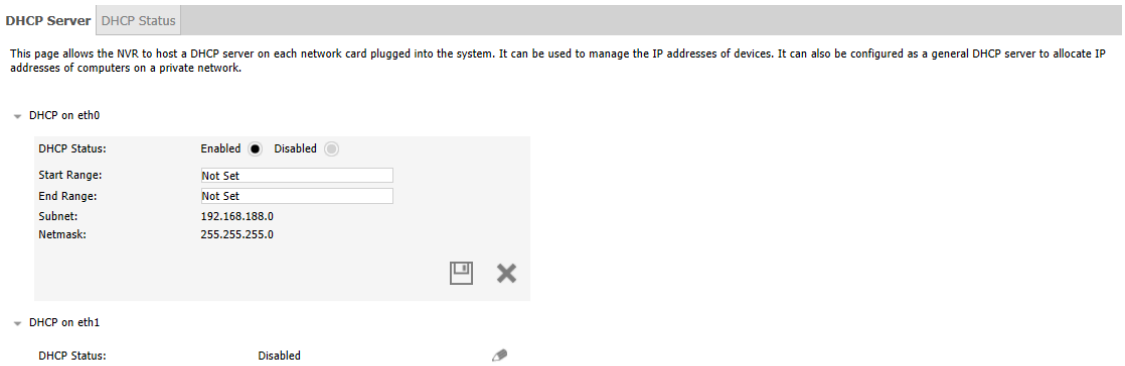
   ⓘ **Note:** Use an IPv4 address for the network and gateway addresses. If you specify more than one default route, you must assign route priority to each route. Lower values indicate higher priority.
5. Click the **Apply** icon.
6. **Optional:** Add additional routes if required.
7. To save the configuration changes, on the **Routing** page, click the **Save static route configuration** icon.

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:** 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 56: DHCP Server page



Configuring the DHCP server settings

1. Expand the **Network** menu and click **DHCP Server**.
2. Click the **Edit** icon next to the LAN Interface that you want to enable as a DHCP server. NICs configured with a DHCP IP Address Allocation are grayed out and are not available to host DHCP Servers.
3. To edit the DHCP Status, click either the **Enabled** or **Disabled** buttons. To edit the DHCP Start Range and End Range, click **Enabled**.
4. 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.

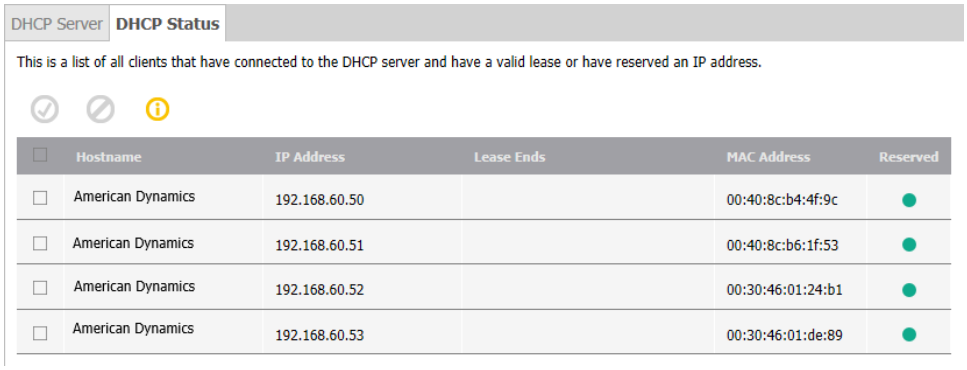
   ⓘ **Note:** The Subnet and Netmask cannot be edited on this page.

5. 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 57: DHCP Status page



Reserving a DHCP address

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

Canceling a DHCP reservation

1. Expand the **Network** menu and click **DHCP Server**.
2. Click the **DHCP Status** tab.
3. 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. You can 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. From the General Settings page, you can 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 display the previously assigned values. However, if you perform an appliance installation, the values are 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 58: WAN port mapping exam

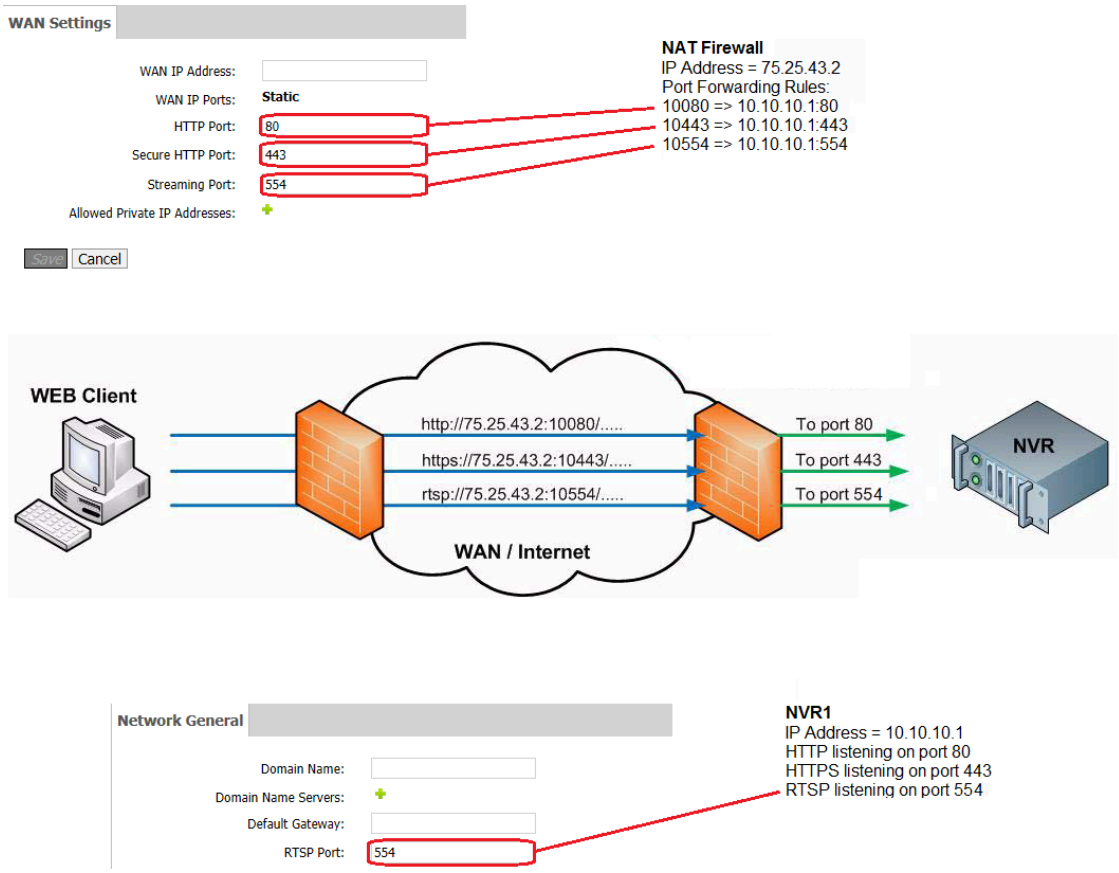
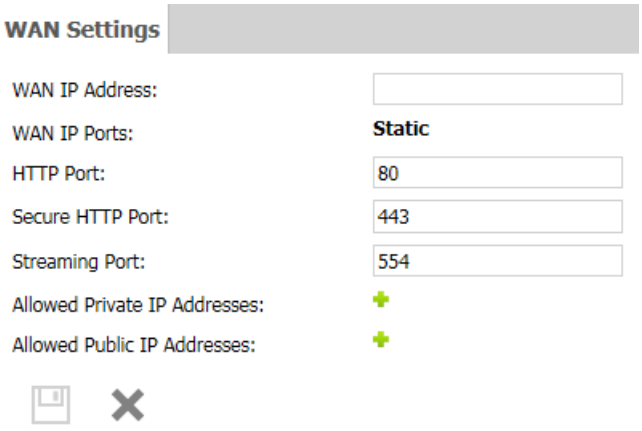


Figure 59: WAN Settings page



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.

Enabling victor Secure Connection software in Standard Provisioning Mode

1. Expand the **Network** menu.
2. Click **Secure Connection**, and then click **Enabled**.
3. Select **Standard** from the **Provisioning Mode** list.
4. Enter the **Activation URL**.
5. Enter the **Password key**.
6. Click the **Save** icon.

Enabling victor Secure Connection software in Advanced Provisioning Mode

1. Expand the **Network** menu.
2. Click **Secure Connection**, and then click **Enabled**.
3. Select **Advanced** from the **Provisioning Mode** list.
4. Enter the **Gateway URL**.
5. Enter the **Gateway SSH Port**.
6. 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:** view the Failover Events report.
- **Storage Statistics:** 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:** 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:** view statistics relating to archiving.
- **Logs:** 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:** enable dark image detection and apply a darkness threshold.
- **Email Alerts:** enable and configure email alerts. The Email Alerts submenu contains the following sections: Email Alerts, Email Blocks, and Alert Logs.
- **Event Filters:** enable and configure event filters.
- **Serial Ports:** configure the NVR's serial ports.
- **Ping:** ping devices on the NVR's network for diagnostic purposes.
- **Connected Clients:** view a list of all clients which have an active connection with the NVR.
- **SIP Proxy:** enable or disable an SIP Proxy, and you can select the inbound and outbound interface.

- **Equivalent Model:** use the Equivalent Model feature to configure VideoEdge to treat the unsupported model as a similar supported model from the same manufacturer
- **External Integration:** use to configure the VideoEdge for use with external integrations.
- **Reset to Factory Defaults:** 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:** 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 52: 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.
	**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 check box. The time values in the Start Date/Time and End Date/Time must be entered in 24-hour format.

Displaying failover events

1. Expand the **Advanced** menu and click **Failover**.
2. From the **Virtual IP Address** list, select the Virtual IP address that you want to query. Click **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.
3. **Optional:** To display failover event times in local time, select the **Use Local Time** check box.

4. To search a time range for Failover Events, select the **Start Date/Time** and the **End Date/Time**.
   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**.
5. Click **Get Failover Events**. All Failover Events in 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 check box 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 60: Recording Performance tab

Viewing the recording performance statistics

1. Expand the **Advanced** menu and click **Storage Statistics**.
2. From the **Recording Performance** list, select the storage set that you want to view the recording performance for.

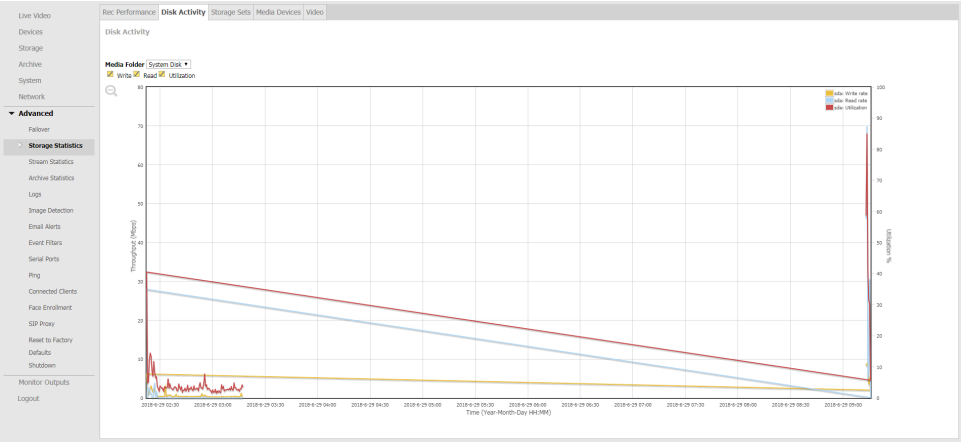
Disk activity

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 check boxes 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 61: Disk Activity statistics tab



Filtering the disk activity graph

1. Expand the **Advanced** menu and click **Storage Statistics**. The **Rec Performance** tab opens.
2. Click the **Disk Activity** tab.
3. From the list, select the **Media Folder** that you want the graph to display disk activity for.
4. From the list, select the required **Sampling Rate**. You can select ranges between 1 minute and 120 minutes.
5. From the **Report for last** list, select the number of hours that you want the graph to display disk activity for.
6. Select the **Utilization Scale** from the list.
7. Select the **Disk I/O Scale** from the list.

ⓘ **Note:** The graph adjusts to display the disk activity as the filters selected.

Storage set statistics

The Storage Set page 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 62: Storage Sets tab

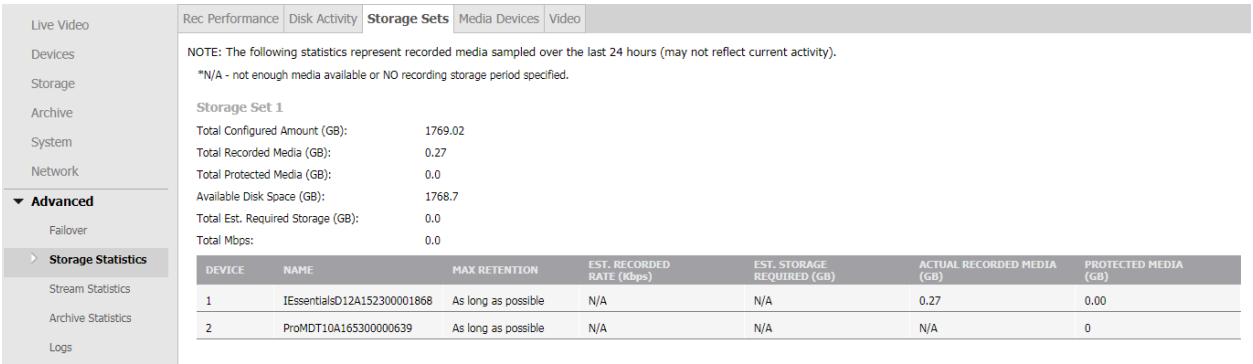


Table 53: Storage Set statistics

Field		Description
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 Media Devices page contains storage statistics for each storage device.

Figure 63: Media Devices page

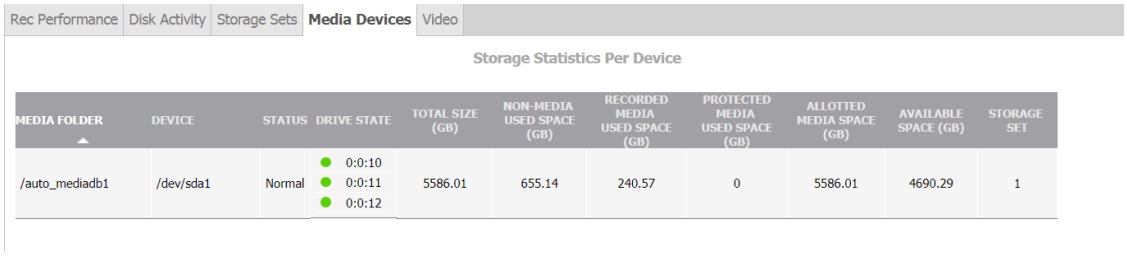


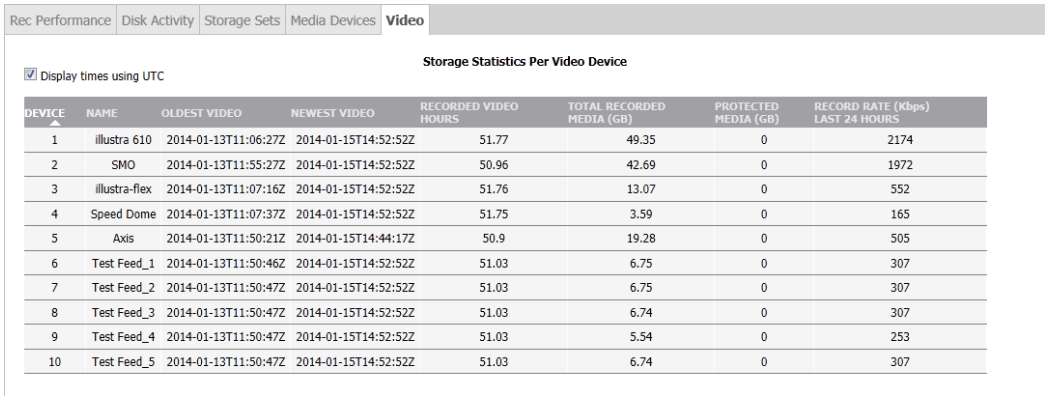
Table 54: Storage Device statistics

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 page details the storage statistics for each camera.

Figure 64: Storage Statistics Video page



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 55: 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.

Table 55: Video Device Storage statistics

Field	Description
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).

Viewing storage statistics

1. Expand 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.

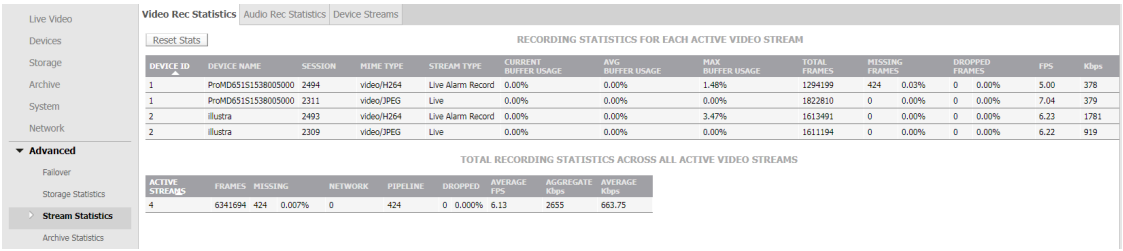
Stream statistics

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 pages 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 65: Recording Statistics page



Recording statistics

Table 56: 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.

Table 56: Recording statistics

Field	Description
Stream Type	Indicates what type of stream recorded for this session, such as live, alarm, or record.
Current Buffer Usage	Usage Current percent used of the internal frame buffer. This will be 0% if no buffering is occurring, that is, frames are 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).

Total recording statistics

Table 57: 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.

Viewing video and audio recording statistics

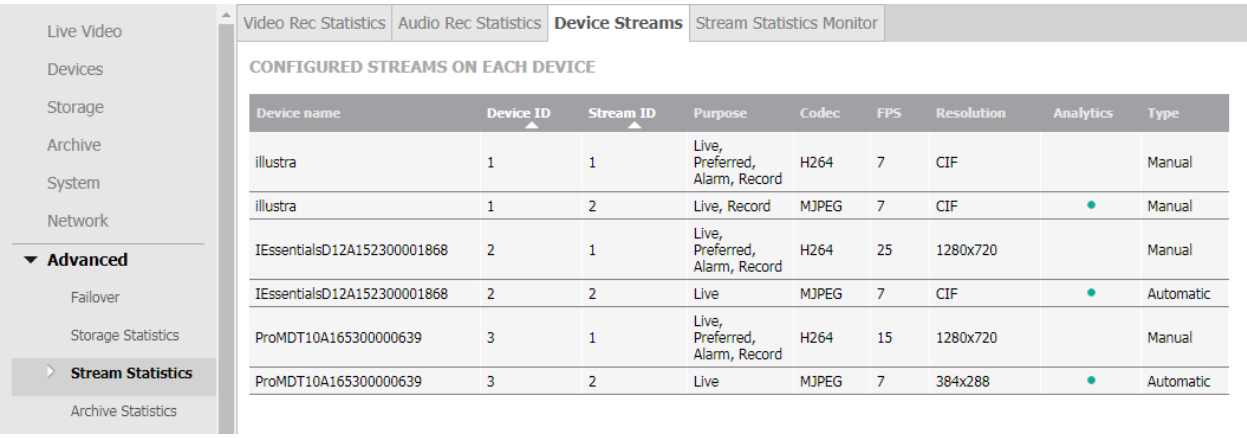
1. Expand the **Advanced** menu and click **Stream Statistics**.
2. Select the required tab:
   - To view video recording statistics, click **Video Rec Statistics** tab.
   - To view audio recording statistics, click the **Audio Rec Statistics** tab.

   ⓘ **Note:** Details of these statistics are outlined in the **Recording Statistics** or the **Total Recording Statistics** tables.

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 66: Device Streams page



Configured streams on each device

Table 58: Configured streams on each device

Field	Description
Device name	Device name as given when adding the device to VideoEdge.
Device ID	Device slot number.
Stream ID	Device stream number.
Purpose	Live: Indicates that this stream will be used for live streaming. Preferred: Indicates that this stream is the preferred stream for the device. Alarm: Indicates that this stream will be used for any alarms that are recorded. Record: Indicates that this stream will be used for non-alarm recording.
Codec	The camera codec.
FPS	The camera FPS.
Resolution	The camera resolution

Table 58: Configured streams on each device

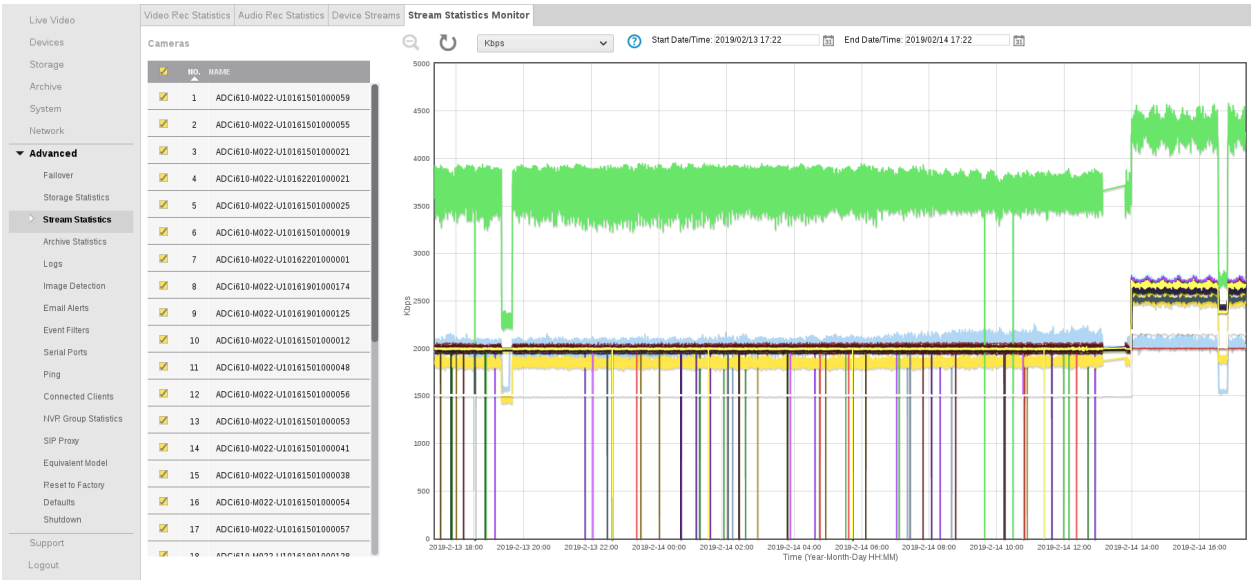
Field	Description
Analytics	Indicates if analytics are set on the device. The analytic options are: Analytics Off Motion Detection Video Intelligence (This encompasses object detection, direction, linger, enter, exit and abandoned / removed). Deep Intelligence Intelligent Search - Person Edge Based.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

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.

Usually, 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 67: Stream Statistics Monitor



Stream statistics

Table 59: 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.

Viewing the stream statistics monitor

1. Expand the **Advanced** menu and click **Stream Statistics**.
2. Click the **Stream Statistics Monitor** tab.

   ⓘ **Note:** The **Stream Statistics Monitor** page opens. All cameras are selected by default.
3. In the **Cameras** table, clear or select the camera check boxes as required.

   ⓘ **Note:** Select a camera's check box to display its streaming data in the monitor. Clear the check box to hide the data.
4. **Optional:** To refresh the Stream Statistics Monitor, click the **Refresh** icon.
5. Select the type of streaming data that 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)**
6. To specify a time period to view by, select a **Start Date/Time** and **End Date/Time**.
7. To show more specific detail, hover over points on the graph.
8. To zoom in on a time period, in the monitor, click and drag over a specific time.
9. To return to the default view, click the **Zoom Out** icon.

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 check boxes 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.

Viewing archive statistics

1. Expand the **Advanced** menu.
2. Click **Archive Statistics**.
3. Display or hide the following items as required on the graphs using check boxes:
   - 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.

Retrieve logs

The Retrieve Logs page provides you with 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 drop down also provides selectable maximum camera log sizes of; 1Mb, 5Mb, 10Mb, 25Mb and 50Mb.

The downloaded log file is zipped and can either be opened as a temporary folder or saved locally.

Viewing retrieve logs

1. Expand the **Advanced** menu and click **Logs**.
2. 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**
3. Select or deselect the **Retrieve Camera Logs** check box as required.
4. Select or deselect the **Retrieve Recording Pipeline Description** check box as required.
5. Select or deselect the **Retrieve Camera Firmware details** check box as required.
6. From the **Maximum Camera Log Size** list, select the maximum camera log size.
7. Select or deselect the **Include Core Files** check box as required.
8. Click **Retrieve Logs**.

9. When the **File Download** window opens, click **Open** or **Save**. The Logs folder is now ready to be viewed.

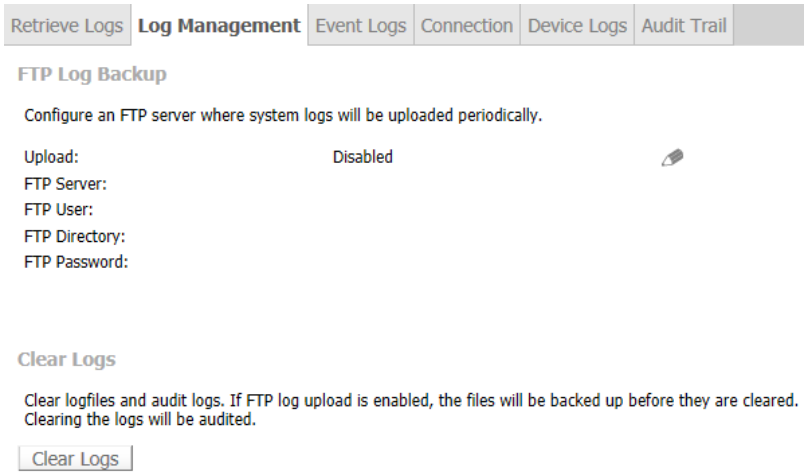
FTP log management

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, configure and enable this function. 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 is displayed. 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 68: Log Management page



Editing settings for the Log FTP server

1. Expand the **Advanced** menu.
2. Click **Logs**, and then click the **Log Management** tab.
3. Click the **Edit** icon.
4. Select the **Enabled** option button to enable Event Log upload to the FTP Server.
5. Enter the IP Address in the **FTP Server** field.
6. Enter the username in the **FTP User** field.
7. Enter the directory in the **FTP Directory** field.
8. Enter the password in the **FTP Password** field.
9. Enter the password again in the **Confirm Password** field.
10. Click the **Save** icon.

Clearing system logs

If FTP log upload is enabled, system files are backed up before they are cleared. You can use the Clear Logs button to manually clear the system log files. Using this function appears in the NVR Audit Trail.

1. Expand the **Advanced** menu and click **Logs**.
2. Click the **Log Management** tab.
3. 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.

Viewing event logs

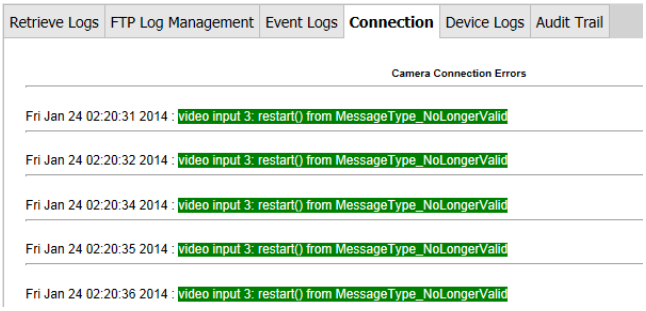
1. Expand the **Advanced** menu.
2. Click **Logs**, and then click the **Event Logs** tab.
3. To include emergency event logs, select the **Emergency** check box.
4. To include critical event logs, select the **Critical** check box.
5. To include error event logs, select the **Error** check box.
6. To include warning event logs, select the **Warning** check box.
7. To include info event logs, select the **Info** check box.
8. To include specific filter text, enter the required filter text in the **Filter text** text box.
9. Click **Apply**.

Viewing camera connection errors

The Connection page displays the camera connection errors that have occurred.

1. Expand the **Advanced** menu and click **Logs**.
2. Click the **Connection** tab. You are prompted to enter your user name and password.
3. Click **OK**.

Figure 69: Connection page



Audit trail

The Audit Trail page displays a log of system changes that 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 Logon passwords, and Network Settings. The Audit Trail provides information on camera reboots, changes to camera recording status, and the use of Pan-Tilt-Zoom (PTZ) and other controls.

Viewing the audit trail

1. Expand the **Advanced** menu.
2. Click **Logs**, and then click the **Audit Trail** tab.
3. To include errors, select the **Error** check box.
4. To include alerts, select the **Alert** check box.
5. To include notice messages, select the **Notice** check box.

6. To include info messages, select the **Info** check box.
7. To include specific filter text, enter the required filter text in the **Filter text** text box.
8. Click **Apply**.

Image Detection

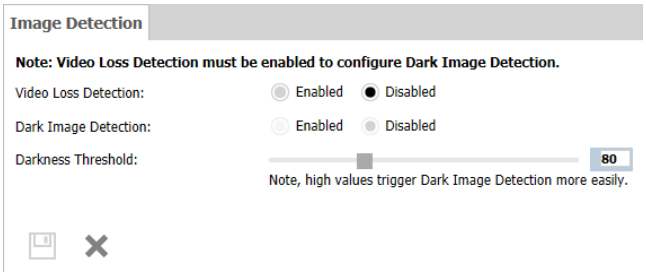
The NVR can perform an Image Detection test on every camera in the network. You can use this test to determine if the NVR has a camera that is recording a very dark, or potentially black video. The test runs for each camera once a minute, it counts the number of pixels with intensity values less than 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 70: Image Detection page



Enabling Image Detection

Before you enable image detection, 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 using the Event Viewer.

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

1. Expand the **Advanced** menu and click **Image Detection**.
2. Click the **Enabled** option button to enable **Video Loss Detection**, or click the **Disabled** option button to disable **Video Loss Detection**.
3. 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 60: 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

Before you configure 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. If you own email addresses in other domains, contact your email administrator to ensure that you 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 can interfere.

1. Expand the **Network** menu and click **General**.
2. In the **Domain Name** field, enter the domain name.
3. In the **Default Gateway** field, enter the default gateway.
4. 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.

1. Expand 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** check box.
   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** check box.
   The Sender email address field displays.
   a. Enter an **email address** in the field.
8. Click the **Save** icon.

Alert categories

Table 61: 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 is deleted before being archived, or when archive is nearly full.
Audio Malfunction	Sent when audio malfunctions occur.
Blur Detection	Sent when a 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 Media Injection	Sent when media injection from a worn camera fails.

Table 61: Alert categories

Alert Category	Description
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.
Clip Storage	Sent when clip storage falls below a low clip storage threshold.
Device Not Recording	Sent when recording does not occur on one or more cameras.
Dry Contact	Sent when a dry contact is triggered.
Face Detection	Sent when a detected face matches the rules configured for the alarm.
Failover	Sent when a failover is detected. The IP address of the NVR which has failed will be included.
License Plate Recognition	Sent when a detected license plate matches the rules configured for the alarm.
Log Storage Space Low	Sent when less than 5% of the log storage area is available.
Motion Detection	Sent by motion detection alerts. Does not include image attachments.
NIC	Sent in response to NIC redundancy events: • Failover to a redundant NIC occurred (Redundancy failover) • Failover to a redundant NIC failed (Redundancy failed) • A redundant NIC failed (Redundancy degraded) • A redundant NIC that had previously failed is operational again (Redundancy improved) • A redundant NIC that had previously failed is operational again and no other redundant NICs are in a failed state (Redundancy normal)
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	Sent when storage is not healthy.
Storage Activation	Generated when no storage can be activated.
Storage Config	Sent when storage configuration errors occur.
Storage Retention	Sent when storage capacity is almost reached.
System	Sent in response to 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 Abandoned/ Removed	Sent when a stationary object is placed, moved or removed.
Video Analytics Crowd Formation	Sent when more than a certain number of people or objects are in a region of interest.
Video Analytics Direction	Sent when objects move in a certain direction through a region of interest.

Table 61: Alert categories

Alert Category	Description
Video Analytics Dwell	Sent when objects dwell in a region of interest. An object is dwelling if it is mostly stationary.
Video Analytics Enter	Sent when objects enter the camera view through a doorway or threshold.
Video Analytics Exit	Sent when objects exit the camera view through a doorway or threshold.
Video Analytics Linger	Sent when objects linger in a region of interest. An object is lingering if it remains in the ROI.
Video Analytics Object Detection	Sent when objects move into a region of interest.
Video Analytics Perimeter	Sent when an object enters a protected area through a perimeter area, or when an object is in the perimeter area too long.
Video Analytics Queue Analysis	Sent when a queue is a certain length.
Video Analytics Tripwire	Sent when an object crosses the tripwire.

Building the recipient list

The Recipient list is made up of email addresses that 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.

1. Expand the **Advanced** menu and click **Email Alerts**.
2. Click the **Add** icon. The **Add/Update Alert Recipient** pop-up opens.
3. Click the **New Recipient Email Address** button.
4. 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.
5. Select the **Alert Categories** using the check boxes.
6. Click the **Save** icon.

ⓘ **Note:** 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 are enabled for each recipient.

1. Expand the **Advanced** menu and click **Email Alerts**.
2. From the **Alert Category** list, select the check box for each alert that you want to enable.
3. Click the **Enable Alert** icon or the **Disable Alert** icon.

Enabling or disabling email alerts for a camera

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

Note: You cannot modify settings like Password Group or PTZ when the camera is disabled.

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

1. Expand the **Devices** menu and click **List**.
2. Click the **Setup** icon in the camera record of the camera you want to re-enable email alerts.
3. Click the **General** tab.
4. Click Video Streaming **Enabled** to enable email alerts for the camera, or click Video Streaming **Disabled** to disable email alerts for the camera.
5. Click the **Save** icon.

Removing an address from the recipient list

You can remove recipient addresses from each alert category.

1. Expand the **Advanced** menu and click **Email Alerts**.
2. Click the **Edit** icon of the **Alert Category** that you want to remove a recipient's address from.
3. Select the check box next to the address you want to remove.
4. Click the **Save** icon.
5. Click **OK**.

Blocking an email alert category

You can block the NVR from sending alerts. On the Email Blocks page, you can select the alert category to block, and you can apply the block to a specific device.

1. Expand the **Advanced** menu and click **Email Alerts**.
2. Click the **Email Blocks** tab.
3. Click the **Add New Email Block** icon.
4. From the **Category** list, select the alert category that you want to block .
5. From the **Camera** list, select the camera.
6. 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.

Displaying the email alerts log

1. Expand the **Advanced** menu and click **Email Alerts**.
2. Click the **Alert Logs** tab.

Clearing the alert logs page

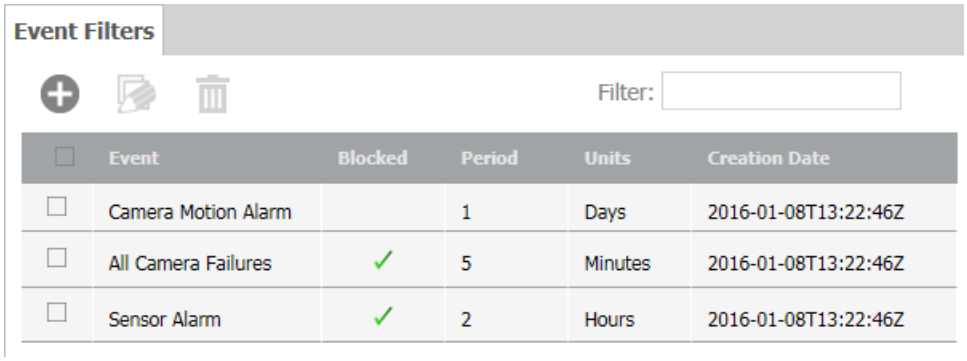
All email alerts can be cleared from the Alert Logs page.

1. Expand the **Advanced** menu and click **Email Alerts**.
2. Click the **Alert Logs** tab.
3. 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 71: Event Filters page



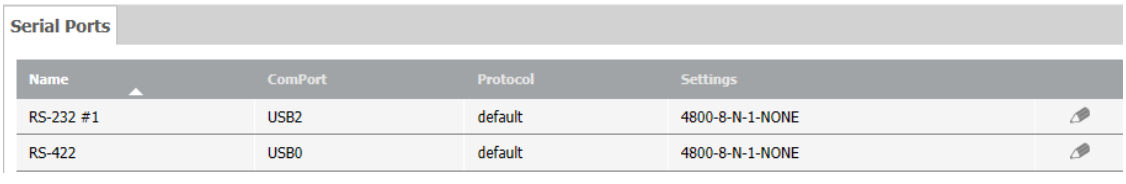
Creating an event filter

1. Expand the **Advanced** menu and click **Event Filters**.
2. Click the **Add** icon. The **Add Filter** menu opens.
3. From the **Event Names** list, select an event.
4. From the **Camera** list, select the camera.
5. To permanently enable the event filter, or configure the filter period, select the **Blocked** check box.
6. **Optional:** If you are 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.
7. 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 72: Serial Ports page



Configuring the serial ports

1. Expand the **Advanced** menu.
2. Click **Serial Ports**.
3. Click the **Edit** icon next to the port you want to configure.

The **Port Settings** pop-up opens.

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 that 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) - Select AD-422 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. Usually, 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.

1. Expand the **Devices** menu and click **List**.
2. Click the **Setup** icon of the analog camera that you want to configure PTZ settings for.
3. Click the **PTZ** tab.
4. From the list, select the **PTZ Port** in use.
5. In the **PTZ Address** field, enter the camera address number.
6. Click the **Save** icon.

PTZ settings specific to Optima and Optima LT cameras

When you use Optima and Optima LT Cameras with the PTZ port set to RS-422 communication using the AD4xx protocol, the following additional check boxes display on the Camera PTZ page:

- **Simplex - Optima LT:** Select this check box to allow simplex communications with Optima LT cameras. Optima LT cameras only support simplex communications when using RS-422 communication and the AD4xx protocol.
- **Enable Camera Menu:** Clear this check box 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 and Optima LT cameras cannot function as required.

Configuring Optima and Optima LT bespoke settings when using RS-422

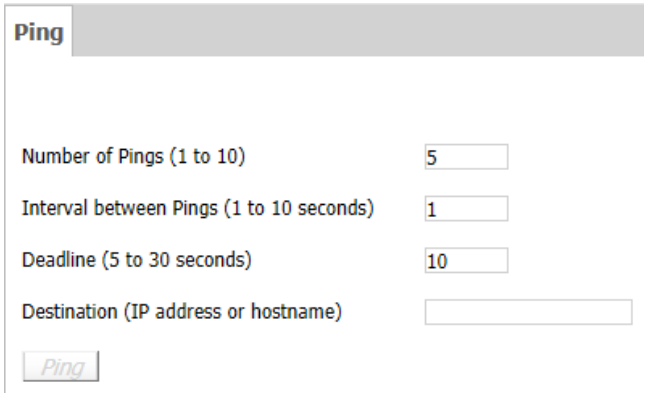
1. Expand the **Devices** menu.
2. Click **List**.
3. Click the **Setup** icon of the analog camera you want to configure PTZ settings for.
4. Click the **PTZ** tab.

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 only:** Select the **Simplex - Optima LT** check box.
8. Deselect the **Enable Camera Menu** check box.
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 73: Ping page



Pinging other devices

1. Expand 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 using 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.

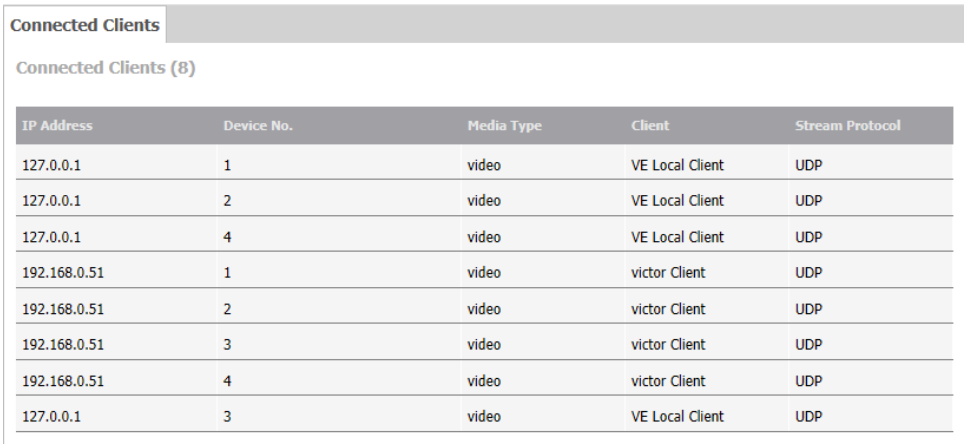
The Connected Client page displays information relating to the clients currently connected to the NVR and their activity. The following information is displayed when a client is connected to the NVR:

- The IP Address of the device which is streaming audio and video from the NVR through 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 74: 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*.

Enabling a SIP proxy

1. Expand 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 Equivalence 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.

Ensure that the unsupported model and the supported model share a feature set, because 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.

1. Expand the **Advanced** menu.
2. Click **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.

External Integration

Use the External Integration menu to configure VideoEdge for use with external integrations.

Axis Body Worn System

VideoEdge provides support for an Axis BWS. For more information on an Axis BWS, refer to the Axis web site.

VideoEdge provides centralized storage for Axis BWC recordings and media playback. In Axis BWS terminology the VideoEdge is referred to as a content destination. When configured, an Axis BWS pushes BWC wearer and recordings to the VideoEdge. The VideoEdge admin does not add Axis BWCs or wearers to the VideoEdge, this is done automatically by the Axis BWS, simplifying configuration on the VideoEdge.

For information on adding and removing an Axis BWC, in the Devices section, see Axis body worn camera (BWC) device.

To prepare the VideoEdge for use with an Axis BWS, complete the following procedures:

- Configuring the Axis BWS content destination settings
- Creating an Axis BWS connection file

Configuring the Axis BWS content destination settings

The VideoEdge Axis BWS feature is disabled by default. Enable the feature to use the VideoEdge as a content destination by the Axis BWS.

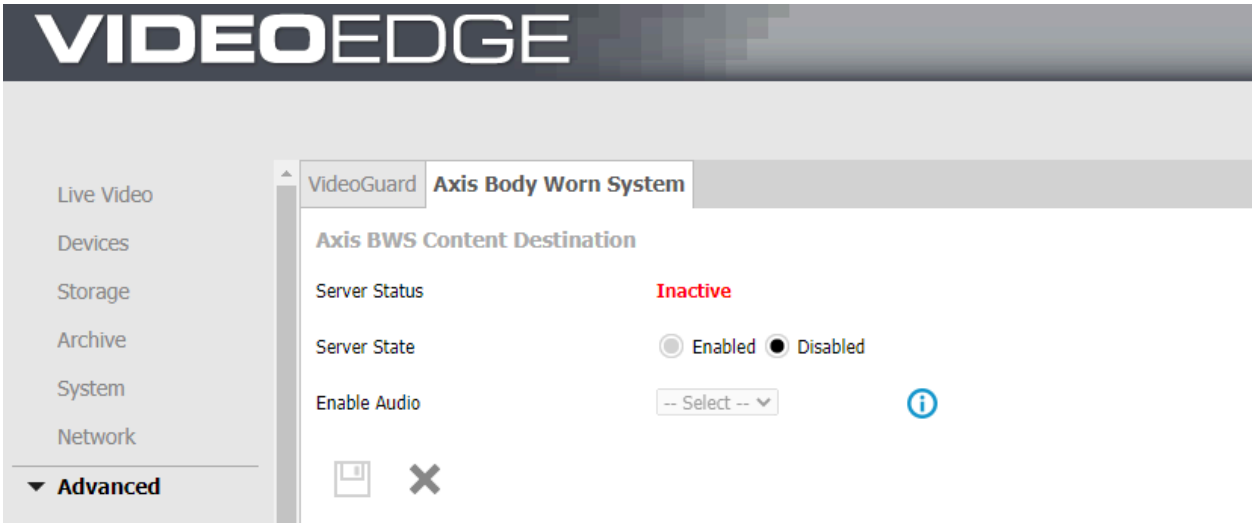
1. Expand the **Advanced** menu, and click **External Integration**.
2. Click the **Axis Body Worn System** tab.
3. In the **Axis BWS Content Destination** area, in the **Server State** row, select the **Enabled** check box.

   ⓘ **Note:** By default, the server state is disabled.
4. To select an audio recording setting, from the **Enabled Audio** list, select an audio option.

ⓘ **Note:** This setting does not determine if an Axis BWC records audio, that is determined by a setting on the Axis BWS. The audio recording setting is applied when the BWC is added to VideoEdge. For information on how to adjust the audio setting for individual Axis BWCs, that have already been added to VideoEdge, see Audio List.

5. Click the **Save** icon.

Figure 75: Axis BWS Content Destination



Creating an Axis BWS connection file

To complete the configuration of an W800 controller you require a connection file. Generate the connection file to create an Axis BWS user. Use the Axis BWS Connection File area to generate and download a connection file.

➧ **Important:** You must generate the connection file on this page and not create it manually. The generation process creates an Axis BWS user on the VideoEdge that is used by the Axis controller.

1. From the menu, click **Advanced** and **External Integration**.
2. Click on the **Axis Body Worn System** tab.
3. In the **Axis BWS Connection File** area, in the fields, enter the required parameters. For more information, see the following table.
4. To generate a connection file, click **Generate Connection File**.

Table 62: Axis BWS connection file parameters

Name	Description	Default value
Site Name	Name of the content destination server.	VideoEdge NVR [hostname]
Username	User name that the Axis W800 controller uses to connect to the VideoEdge.	axisbwsuser
Password	User password.	No default
Container	The container type of BWC recorded media. For example, MP4 or MKV.	MP4
Communication	HTTP or HTTPS.	HTTPS

Table 62: Axis BWS connection file parameters

Name	Description	Default value
VideoEdge Address	IP address that the AXIS BWS uses to connect to this VideoEdge. If this VideoEdge is part of a failover group, this is the virtual IP address of the failover group, otherwise it is the IP address of the VideoEdge.	The first interface of this VideoEdge
VideoEdge Port	IP port.	Port #443 for HTTPS secure communications

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 using the reset pinhole button. Resetting using the Administration interface allows you to reset NVR settings whereas resetting using the pinhole button allows you to reset Operating System settings.

Reset factory defaults in the 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.

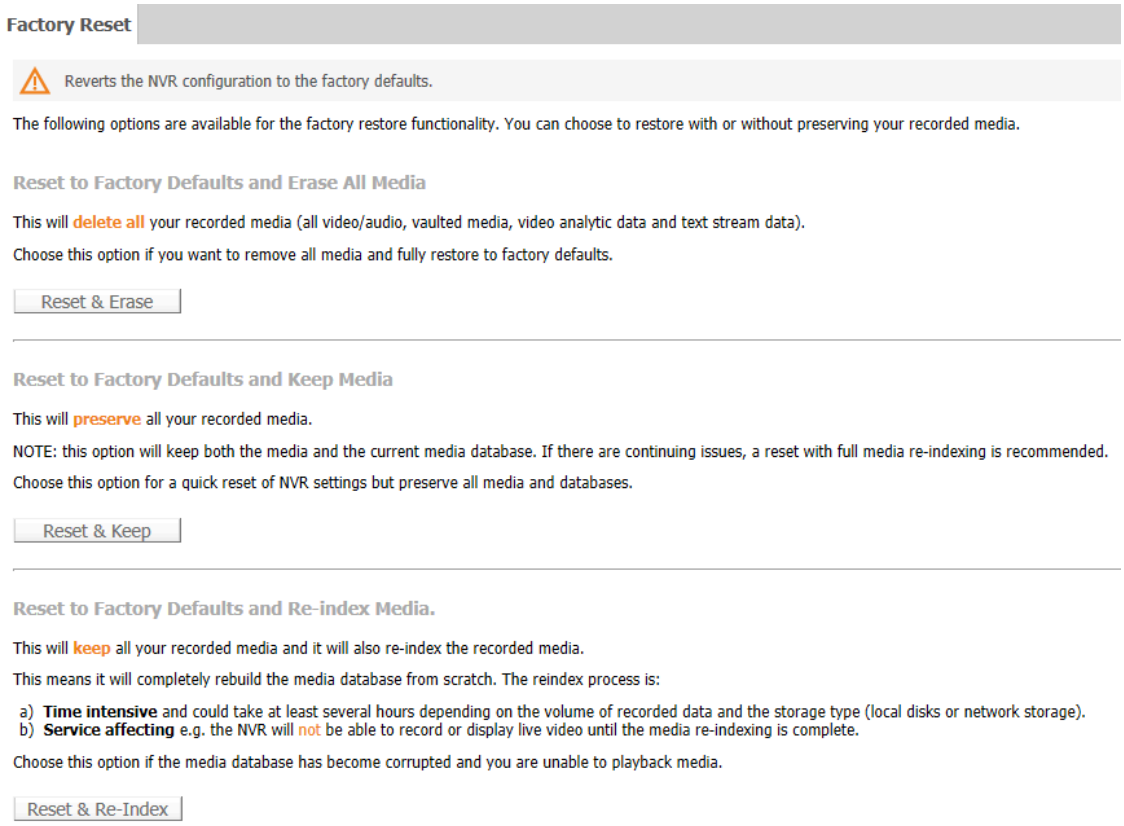
After the Reset Factory Defaults is complete, you must reconfigure the NVR using the Setup Wizard.

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 use 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, perform a reset with full media re-indexing.

- **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 76: 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.

Resetting to factory defaults

1. Expand 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 opens.

Reset factory defaults: pinhole reset

On the VideoEdge Appliance units there is a reset factory defaults pinhole button. 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 provided reset pin to press the button. When you press the button the following settings restore 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 can affect your camera network.

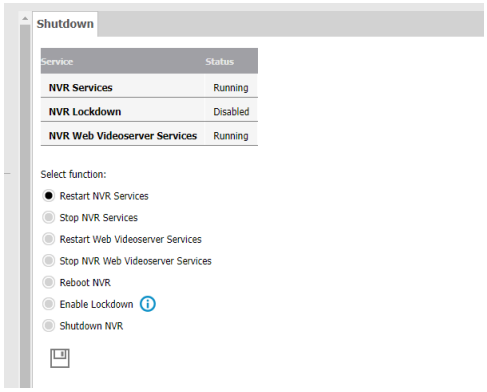
All Linux and administration interface user names and passwords reset to their default values. Additional Linux accounts that have been created are deleted.

Shutdown

From the Shutdown page, you can stop or restart the NVR, NVR Services, and Web Videoserver 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.

Note: From VideoEdge 6.1.1, victorwebLT is no longer available or supported on VideoEdge.

Figure 77: 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 restarts 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: Stop NVR Services before configuring storage.

Restarting Web Videoserver Services

You can restart Web Videoserver Services if you experience issues with your video feed in CCURE IQ or the VideoEdge admin user interface.

Stopping NVR Web Videoserver Services

NVR Web Videoserver Services can be stopped permanently. This stops video streaming in CCURE IQ and in the VideoEdge admin user interface.

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 VideoEdge client.

The VideoEdge remains in Lockdown mode until you disable it. If Lockdown mode is enabled, the **Disable Lockdown** button is displayed 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.

Enabling or disabling Lockdown mode

1. Expand the **Advanced** menu, and then click **Shutdown**.
2. Click **Enable Lockdown** or **Disable Lockdown**.

   ⓘ **Note:** If Lockdown is already enabled, the **Disable Lockdown** option displays instead.
3. 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, 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 63: 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

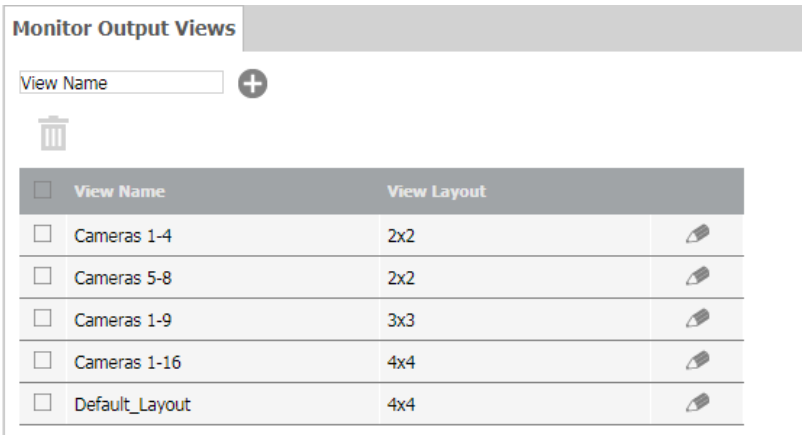
Monitor output views

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 78: Monitor Output Views



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. Select **Launch** in the monitor output view record you want to view.
   The selected monitor view displays on the monitor selected.

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 drop-down 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.

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** drop-down menu.
   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 drop-down menu.

   ⓘ **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.

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** list.
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.

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. From the **Available Cameras** list, select a camera. Click the **Right Arrow** icon to move the camera to the **Cameras In This Group** list.

   ⓘ **Note:** You can only use one IP camera in a tour as only one IP camera displays 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 represents 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.

Appendices

For more information, see the following appendices.

VideoEdge troubleshooting

For configuring settings through the NVR's embedded operating system YaST Control Center is used. You must log on 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 perform the procedures in this appendix and to close the client, complete the following steps:

1. Press **Win** and **H** simultaneously. The Client is minimized and the NVR Desktop is displayed.
2. On the task bar, right-click the **[veLocalClient]** tab.
3. Click **Close**.

Monitor resolution settings

The VideoEdge Client user interface consists of menus that are fixed in display size. If your resolution settings are not correctly configured, menu items can be hidden from view.

VideoEdge Client supports the following display resolution settings:

- 1920 x 1080
- 1280 x 1024

Changing the monitor resolution

Use the **Displays** menu to change the NVRs monitor resolution.

1. On the NVR Desktop, click **Applications**.
2. Click **System Tools > Settings > Displays**.
3. From the **Displays** menu, select your monitor.
4. From the **Resolution** list, select a resolution.
5. Click **Apply**.

Logging on to the remote desktop protocol

1. On the Windows taskbar, click **Start**.
2. Click **All Programs** and **Accessories**.
3. Click **Remote Desktop Connection**. The **Remote Desktop Connection** application opens.
4. In the **Computer** field, enter the **NVR's IP Address**.
5. Click **Connect**. A warning displays. Click **Yes**.
6. On the **NVRs Desktop Login** window, in the corresponding fields, enter the **username** and **password**.
7. Use the default **Module** option: dropdown - sesman-Xvnc.

   ⓘ **Note:** Only the VideoEdge and Tyco user credentials, or their enhanced security mode replacements, can be used to access the NVR remotely.

8. Click **OK**.

Logging off of the remote desktop protocol

⚠ **CAUTION:** Log off of the remote desktop protocol (RDP) correctly. Failure to log off correctly will leave a high CPU process running on the NVR that will affect performance.

1. Click the **Power** icon. A pop-up window opens.
2. Expand the **Log Out** menu and click **Log Out**. A Logout pop-up opens.
3. Click **Log Out**. The remote desktop windows closes.
4. Click the **Close Window** icon to close the **Remote Desktop Connection** application.

System partitions on a previously configured device

If you are installing or upgrading the NVR software on a device that has been previously configured, there may be system partitions created already that require re-configuration.

⚠ **CAUTION:** To ensure your NVR is set up correctly, delete existing partitions.

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.

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. An example of the naming convention for the secondary drive is as follows: sdb1, sdb2, and so on. One primary partition for each drive can be assigned as an extended partition containing as many logical partitions as you require.

Required default system partitions

The requirements for configuration are three system partitions and the media storage partitions. The system partitions are needed for regular operation of the NVR operating system. The required system partitions that need to be created are outlined in the following table. Each partition size in the table is the recommended minimum value.

Table 64: Required default system partitions

Size (GB)	Type	FS type	Mount point
16	Linux swap	Swap	swap
47	Linux native	XFS	/var
20	Linux native	Ext3	/

Configuring system partitions on a previously configured device

1. In the **Suggested Partitioning** page of the **Partitioner Wizard**, click **Create Partition Setup**.
2. Select **Custom Partitioning (for experts)**. The **Expert Partitioner** page opens.
3. Select the disk that 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 required option from the **File System** list. 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.

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.

Editing media partitions

ⓘ **Note:** Stop NVR services before changing partition configurations on devices that have already been added to the NVR.

Deleting a partition

1. Select the partition you want to delete.
2. Click **Delete**.
3. Click **Yes** to delete the partition.

4. Click **Next**. The **Expert Partitioner** page opens displaying the changes to be made to the partitions
5. Click **Finish**. The changes are made to the partitions.

Selecting the disk containing the media partitions

1. Click **Applications** from the NVR desktop.
2. Click **System Tools**, and then click **YaST**.
3. Enter the root password and then click **Continue**.
   The **Control Center** opens.
4. Click **Partitioner** from the **System** menu. A warning message opens.
5. Click **Yes** to continue.
   The **Expert Partitioner** page opens.
6. Select the disk containing the media partitions you want to edit from the system view tree.

Editing the size of a media partition

1. Select the partition in the table and then click **Resize**.
2. Select either **Maximum Size**, **Minimum Size**, or **Custom Size** and enter the required partition size.
3. Click **OK**.

Adding a new media partition

1. Click **Add**.
2. Select either **Primary Partition** or **Extended Partition**.
3. Select the partition size. Select either **Maximum Size** or **Custom Size** and enter the required partition size.

   ⓘ **Note:** You can also choose an allocated region of the disk by entering a **Start Cylinder** and an **End Cylinder**.
4. Click **Next**.
5. Select a **Role** as follows:
   - Select either **Operating System**, **Data and ISV Applications**, **Swap**, or **Raw Volume (unformatted)**.
6. Click **Next**.
7. **Optional:** If you are creating an extended partition, go to step 21.
8. Click **Format Partition**.
9. Select **XFS** from the **File System** list.
10. Enter the **Mount Point** for the media partition, for example, `/data/media1`.
11. Click **Fstab Options...**.
12. Click **Device ID**.
13. In the **Arbitraryoption** field, enter the following:
    `rw,noatime,nodiratime,attr2,nobarrier,noquota,allocsize=4m,inode64`

    ⓘ **Note:** Only use `nobarrier` on storage devices connected to disk controllers with battery backed cache.
14. Click **Finish**.

Deleting a media partition

1. Select the partition you want to delete.
2. Click **Delete**.

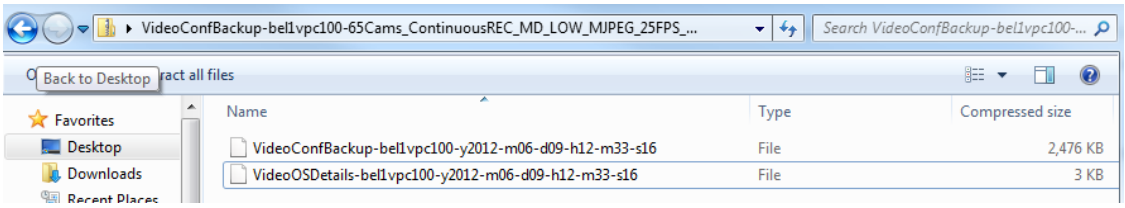
3. Click **Yes** to delete the partition.
4. Click **Next**. The Expert Partitioner page opens displaying the changes to be made to the partitions
5. Click **Finish**. The changes are made to the partitions.

System disk recovery

If the NVR system disk fails or becomes corrupt, the following items are required for the recovery procedure:

- A license file for the NVR.
- A system backup file, from NVR 4.2+ only. A backup procedure must have been performed after the NVR configuration was completed at the time of install. This is a zip file containing two files as follows:
  - NVR backup information: VideoConfBackup-xxxxxxxxxxx.zip
  - Network an storage mount information text file: VideoOSDetails-xxxxxxxx.zip. This text file is required to complete the recovery procedure.

Figure 79: Backup information files



- A replacement disk greater than the existing system disk, if applicable.
- NVR software CD or USB drive.

⚠ **CAUTION:** To maintain all configured Tours and Salvos relating to your NVR in victor Unified Client, complete the VideoEdge System Disk Restore procedure before reconfiguring the NVR LAN interface settings.

Restoring previous mountpoints

1. Power **OFF** the NVR.
2. **Optional:** Replace the system disk. This step is required if the system disk becomes corrupt.
3. Ensure that 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.
6. Use **YaST** to configure any iSCSI storage devices and connect to them.
7. Unzip the backup file in Windows.
8. Extract the file `VideoOSDetails-VideoEdge-XXXXXXXX`, and save it to a USB.
9. On the NVR, from the USB, use a text editor to open the following file: `VideoOSDetails-VideoEdge-XXXXXXXX`.
10. Copy all of the information from the **Filesystem** details section of the file.
11. 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*, and press Enter.
    c. Paste the copied text from the clipboard and press Enter.
    d. Press CTRL + D.

12. In the Terminal window run the following command and then click Enter:
videoedge# /opt/americandynamics/venvr/bin/restore_fstab/tmp/fstab_backup
Running this command restores all previous mountpoints.

Completing the Setup Wizard

1. To open the **Setup Wizard**, use one of the following options:
   - **NVR desktop:** click the NVR Administrator icon.
   - **Remote machine:** open Internet Explorer and log on to the NVR Configuration Interface.

   ⓘ **Note:** The default credentials are **Username**: `admin`, and **Password**: `admin`.
2. To begin the **Setup Wizard**, click **Start**.
3. Continue through the **Setup Wizard** until you reach the **Network** section.
4. Open the `VideoOSDetails-xxxxxxxx` file and use the network settings to configure the following topics:
   - Domain Name
   - Domain Name Servers
   - Default Gateway
   - RTSP Port
   - NTP Status
   - NTP Servers
5. Complete the remaining stages of the **Setup Wizard**. When complete, the **NVR Configuration Interface** opens on the **Video List** page.

Uploading the backup file

1. From the **Video List** page, click **System**, and then click **Backup/Restore**.
The **Backup** page opens.
2. Click the **Restore** tab, and then click **Browse**.
3. Navigate to and select the NVR backup file: VideoConfBackup-xxxxxxxxxxx.zip.

   ⓘ **Note:** You must use the zip file and not an individual sub file.
4. Click **Upload Backup**.
5. You are prompted for media recovery. Click **Yes**.
Media recovery takes approximately 1 minute for 90–100 GB of storage. Status messages display informing you of current progress.
6. After completion, verify that all configuration parameters are correct.

Failover heartbeat parameters

In previous versions 4.4, 4.5, 4.5.1, and 4.6, the heartbeat settings that dictated when Failover would engage were configured using the Administration Interface. In version 4.7+, the Failover heartbeat is configured at its optimum default settings.

The default settings are as follows:

- Polling Interval: 3
- Retry Count: 3
- Config Update Interval: 60

The heartbeat parameters can be manually changes if required to suit your deployment scenario.

Editing failover heartbeat parameters

1. Log on to the VideoEdge NVR locally or remotely and open **GNOME Terminal** as follows:
   a. Click **Applications** on the lower left of the VideoEdge desktop.

b. Click **Utilities**
c. Click **GNOME Terminal**

ⓘ **Note:** GNOME Terminal is pinned to the **Applications** menu.

2. Remote Logon only: Type `su` and press RETURN.
3. Remote Logon only: Type `rootpassword` and press RETURN.
4. Type `cd /var/opt/americandynamics/venvr/`
5. Type `xdg-open failoverstate.json`
   A gedit window launches showing the file in text format.
6. Edit the bolded fields as required:
   ```
   "failoverparams": {
   "failoverpollinterval": 10,
   "heartbeatblackoutinterval":120,
   "failoverretrycount":3,
   "configurationcheckinterval"60
   }
   ```
7. Click **Save**.
8. Close gedit.
9. In terminal, press CTRL+C.
10. Type `exit` and press RETURN.
11. Close the **GNOME Terminal**.

Failoverstate file for a secondary NVR

The following 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"
: "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
}
}
```

VideoEdge as an NTP server

For security reasons, the NTP server functionality of VideoEdge is disabled by default in VideoEdge 4.5. VideoEdge can be enabled as an NTP server if necessary.

⚠ **CAUTION:** VideoEdge is more vulnerable to attack when it is enabled as an NTP server. For security reasons, limit the number of devices that connect to a VideoEdge NTP server.

Enabling VideoEdge as an NTP Server

1. Log on to VideoEdge.
2. From the VideoEdge desktop, click **Applications**.
3. Click **Utilities**.
4. Click **GNOME Terminal**.
5. Complete the following commands:
   a. Type `su`, and the click ENTER
   b. Enter the root user password, and then click ENTER
   c. Type `service ntp stop`, and then click ENTER
   d. Type `vi /etc/ntp.conf`.
6. Using your arrow keys, navigate to the line `restrict default ignore`.
7. Complete the following commands
   a. Type `dd`.
   b. Type `:wq`, and then click ENTER
   c. Type `service ntp start`, and then click ENTER
   d. Type `/sbin/chkconfig ntp on`, and then click ENTER
   e. Type `exit`, and then click [Enter]

Synchronizing the time between VideoEdge devices and a VideoEdge NTP server

Perform this procedure on a VideoEdge unit to enable it to receive time synchronization commands from a VideoEdge acting as an NTP Server:

1. Log on to VideoEdge.
2. From the VideoEdge desktop, click **VideoEdge Administrator**.
3. Log on as an Administrator.
4. Navigate to the **Network>General** menu.
5. Click **Enabled** next to **NTP Status**.

6. Select the green **+** icon, and then enter the IP address or hostname of your NTP server VideoEdge.
7. Click **Save**.
8. Minimize the NVR **Administration Interface**.
9. From the VideoEdge desktop, click **Applications**.
10. Click **Utilities**.
11. Click **GNOME Terminal** to open one instance of **GNOME Terminal**. Click **GNOME Terminal** again to open a second instance of **GNOME Terminal**.
12. In both terminal windows, type the following commands:
    a. Type `su`, and then click [Enter].
    b. Enter the root user password, and then click [Enter].
13. In terminal window one, type `tail –F /var/log/ntp`, and then click [Enter].
14. In terminal window two, type the following commands:
    a. Type `service ntp stop`, and then click [Enter].
    b. Type `ntpd –q`, and then click [Enter].
15. In terminal window one, press [CTRL] + [c] to stop the tail command.
16. In terminal window two, type the following commands:
    a. Type `service ntp start`, and then click [Enter].
    b. Type `sbin/chkconfig ntp on`, and then click [Enter].
17. In both terminal windows, type `exit` and then click [Enter].

Result
NTP synchronization is set up. This may take a few minutes to synchronize and can be verified by logging in as a support user and then navigating to the **Support>NTP Status** menu.

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 (FPS) and/or resolution. All streams 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 that can be transcoded simultaneously is dependent on your VideoEdge hardware platform.

- For legacy platforms released before software version 4.4.2 the VideoEdge can transcode up to 4 streams simultaneously.
- VideoEdge Micro NVRs can transcode up to 2 streams simultaneously.
- VideoEdge Appliance platforms released after software version 4.4.2 can transcode up to 14 streams simultaneously, after they have been upgraded to software version 4.5.1 and onwards.
- Transcoder Compact Desktop platform can transcode up to 20 streams simultaneously.

High resolution transcoding

Higher resolution native streams have the following transcode options to victor:

- 1080p (1920 x 1080)
- 720p (1280 x 720)
- D1 (720 x 480)

The transcode options available depend on the size of the native stream:

- 1MP or higher native stream will offer D1
- 4MP or higher native stream will offer D1 and 720p
- 8MP or higher native stream will offer D1, 720p, and 1080p

ⓘ **Note:** AXIS P1428-E camera supports an 8 MP resolution.

You can force select palettes by setting these 2 reg keys:

PaletteOverride: Set to 1

PaletteEntry: Set the value to a decimal so it is a zero based number. To force palette stream 1, set the value to zero. For palette stream 10, use 9.

ⓘ **Note:** Both are DWORD and both live in the MediaKit registry hive.

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 can 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 in the NVR group.

The stream that provides an optimized result is selected for streaming to the client. Selecting the optimized stream is dictated by the following:

1. **Client side settings:**
   - Whether the client has been configured to prefer optimized frame rate or resolution.
   - Native streams are selected when the LAN check box has been selected.

     ⓘ **Note:** If a bandwidth cap has been applied on the client, this overrides the LAN check box 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 or 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 or 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 check box is selected.

   ⓘ **Note:** Option is selected by default in victor.

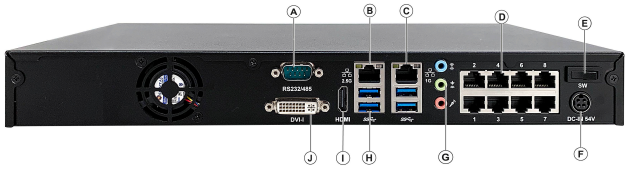
Hardware configurations

Before 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 80: VideoEdge Micro NVR front view

Figure 81: VideoEdge Micro NVR rear view

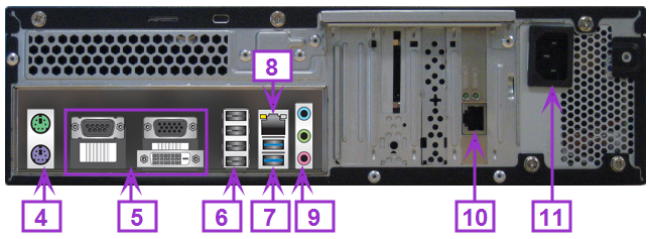


Callout	Description
A	RS232/RS485 serial port
B	2.5GbE (eth0 LAN1)
C	1GbE network ports (eth1 LAN2)
D	1GbE network ports (eight PoE eth2 for cameras)
E	Power switch
F	DC-IN 54V power entry connector, see note
G	Audio out
H	Four USB 3.0 ports
I	HDMI port
J	DVI port

VideoEdge Desktop NVR

Figure 82: VideoEdge Desktop NVR front view

Figure 83: VideoEdge Desktop NVR rear view



Callout	Description
1	Hard drive activity LED
2	Power button/LED (Pinhole)
3	USB 2.0 ports x 2 and USB 3.0 Ports x 2. This is located under the front flap.

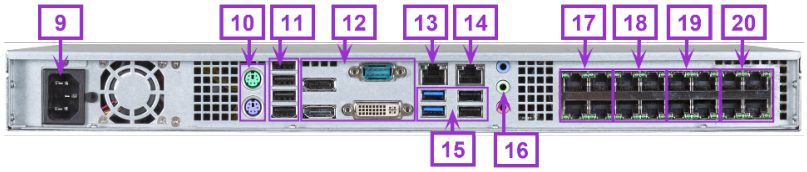
Callout	Description
4	PS/2 ports
5	Video ports: VGA or DVI-D. ⓘ **Note:** Serial is not supported.
6	USB 2.0 ports x 4
7	USB 3.0 ports x 2
8	1 GbE network port (eth0 LAN1)
9	Audio ports: Line in, line out, microphone ⓘ **Note:** Line In and Mic are not supported
10	1 GbE network port (eth1 LAN2)
11	Power entry connector (100~240VAC)

VideoEdge 1U NVR

Figure 84: VideoEdge 1U NVR front view

Figure 85: VideoEdge 1U NVR front view without the panel

Figure 86: VideoEdge 1U NVR front view



Number	Description
1	Bezel. This is removable.
2	Bezel lock. The key is located behind the bezel.
3	USB 2.0 port
4	Factory reset button
5	Power indicator LEDs
6	Power button
7	PoE status indicator LEDs
8	Drives ⓘ **Note:** These are removable.
9	Power connector (100 ~ 240VAC)
10	PS/2 ports

Number	Description
11	USB ports (4 x 2.0)
12	Video ports: DisplayPort x2, serial port, DVI-I port
13	1GbE network port (eth0 LAN1)
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 87: VideoEdge 2U Hybrid NVR front view

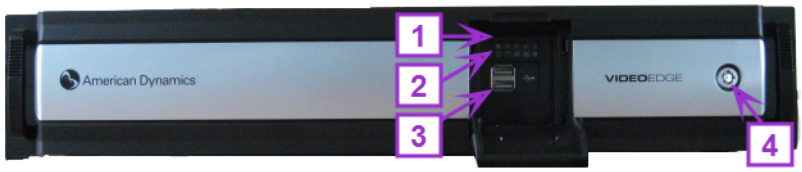


Figure 88: VideoEdge 2U Hybrid NVR rear view

Callout	Description
1	Factory reset button. This is located under the front flap.
2	Power Button. This is located under the front flap.
3	USB 3.0 ports x 2 . These are located under the front flap.
4	Bezel lock. The key is located behind the bezel.
5	Power entry connector (100~240VAC).
6	PS/2 combo port.
7	USB 2.0 ports x 2.
8	Video ports: VGA or DVI-D.
9	USB 5Gb/s Type C port. ⓘ **Note:** This is not supported.

Callout	Description
10	HDMI Port. ⓘ **Note:** This is not supported.
11	USB 2.0 ports x 2 and USB 3.0 ports x 2.
12	1 GbE network port (eth0 LAN1).
13	Audio ports: line in, line out, microphone. ⓘ **Note:** Line in and Mic are not supported.
14	1 GbE network port (eth1 LAN2).
15	Alarm in x 9, alarm out x 16, and Form C Relay.
16	RS422 port.
17	Serial port.
18	Alarm in x 9, audio in x 16, and audio out.
19	BNC video: Analog camera outputs x16.
20	BNC video: Analog monitor outputs x 2.
21	BNC video: Loop through/camera out x 16.

VideoEdge 2U NVR

Figure 89: VideoEdge 2U NVR front view

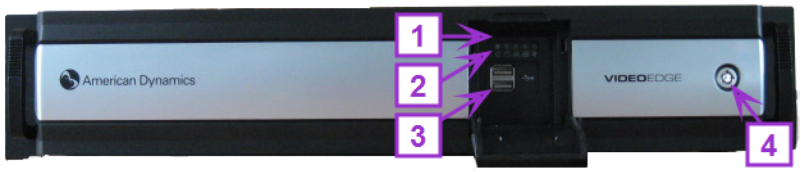
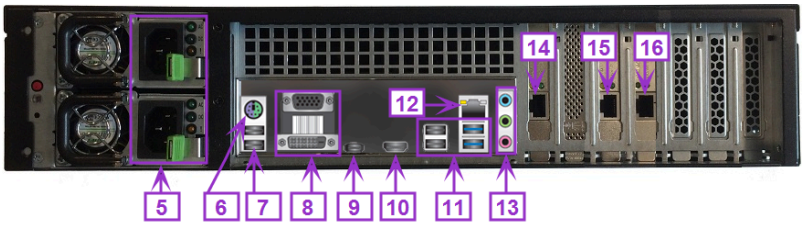


Figure 90: VideoEdge 2U NVR rear view



Callout	Description
1	Factory reset button. This is located under the front flap.
2	Power button. This is located under the front flap.
3	USB 3.0 ports x2. This is located under the front flap.
4	Bezel lock. The key is located behind the bezel.
5	Power entry connector x2 (100~240VAC)
6	PS/2 combo port
7	USB 2.0 ports x 2
8	Video ports: VGA or DVI-D

Callout	Description
9	USB 5Gb/s Type C port ⓘ **Note:** This is not supported.
10	HDMI port ⓘ **Note:** This is not supported.
11	USB 2.0 ports x2 and USB 3.0 ports x 2
12	1 GbE network port (eth0 LAN1)
13	Audio ports: Line in, line out, microphone ⓘ **Note:** Line in and Mic are not supported.
14	1 GbE network port (eth1 LAN2)
15	1 GbE network port (eth2 LAN3)
16	1 GbE network port (eth3 LAN4)

VideoEdge 2U HC NVR

Figure 91: VideoEdge 2U HC NVR front view with cover

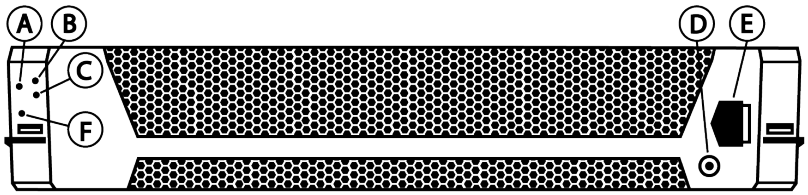


Figure 92: VideoEdge 2U HC NVR front view without cover

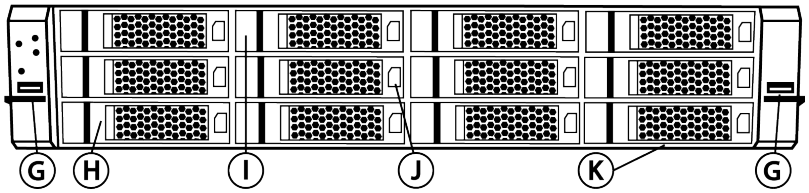
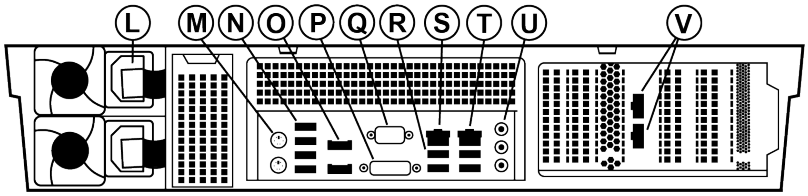


Figure 93: VideoEdge 2U HC NVR back view



Callout	Description	Callout	Description
A	Pin hole for power on/off. Solid blue LED light when power is on.	M	PS/2 ports
B	Operating system status light: Flashes green when accessing	N	USB 2.0 ports (black) × 4

Callout	Description	Callout	Description
C	Hardware storage error light: Solid red with audible alarm when a RAID error is detected	O	Display ports × 2
D	Bezel lock	P	DVI-D port
E	Lever	Q	Serial port
F	Software reset	R	USB 3.0 ports (blue) × 4
G	USB	S	1 GbE network port (eth0 LAN1)
H	Hard drives	T	1 GbE network port (eth1 LAN2)
I	HDD caddy release	U	Audio connectors
J	HDD number	V	Dual NIC Top: 1 GbE network port (eth3 LAN4) Bottom: 1 GbE network K port (eth2 LAN3)
K	Pull tab: Contains the drive map and service label.		
L	Power entry connectors × 2 100 VAC – 240 VAC		

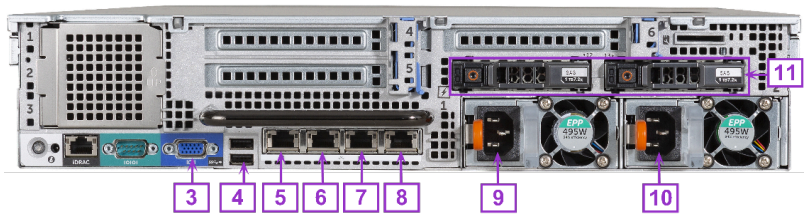
Table 65: IEC safety symbols

Symbol	Language	Meaning	Location	Description	IEC Standard
	English	Stand-by	Stand-by switch	The equipment is switched on and is in stand-by condition	IEC 60417-5009
	English	CAUTION Risk of electric shock	Multiple power sources	This equipment causes risk of electric shock	IEC 60417-60 42 (2010-11)
	English	Disconnection, all power plugs	Multiple power sources	All power sources shall be disconnected before servicing to avoid shock hazard.	IEC 60417-6172 (2012-09)

VideoEdge Rack Mount NVR

Figure 94: VideoEdge Rack Mount NVR front view

Figure 95: VideoEdge Rack Mount NVR rear view



Callout	Description
1	Bezel lock. The key is located behind the bezel
2	Power button. The key is located behind the bezel
3	VGA port
4	USB 3.0 ports x 2
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: 2 x RAID-1 OS drives

VideoEdge 3U Hybrid NVR

Figure 96: VideoEdge 3U Hybrid NVR front view

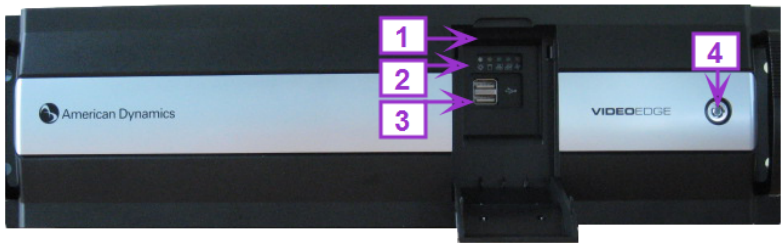
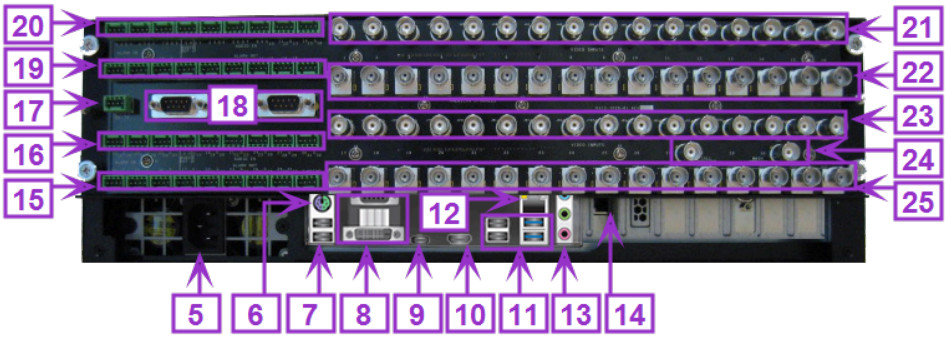


Figure 97: VideoEdge 3U Hybrid NVR rear view



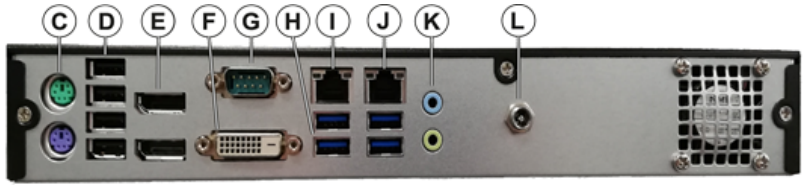
Callout	Description
1	Factory reset button. This is located under the front flap.
2	Power button. This is located under the front flap.
3	USB 3.0 ports x2. These are located under the front flap.
4	Bezel lock. This key is located behind the bezel.
5	Power entry connector (100~240VAC)
6	PS/2 combo port

Callout	Description
7	USB 3.0 ports x2
8	Video ports: VGA or DVI-D
9	USB 5Gb/s Type C port. ⓘ **Note:** This is not supported.
10	HDMI port. ⓘ **Note:** This is not supported.
11	USB 2.0 ports x 2 and USB 3.0 ports x 2
12	1 GbE network port (eth0 LAN1)
13	Audio ports: Line in, line out, microphone ⓘ **Note:** Line in and Mic are not supported.
14	1 GbE network port (eth1 LAN2)
15	Alarm in x 9, Alarm out x 16, Form C Relay
16	Alarm in x 9, Audio in x 16, Audio out
17	RS422 port
18	Serial port x 2
19	Alarm in x 9, Alarm out x 16, Form C Relay
20	Alarm in x 9, Alarm out x 16, Audio out
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 98: VideoEdge Compact Desktop NVR front view

Figure 99: VideoEdge Compact Desktop NVR rear view



Callout	Description
A	Reset button
B	Power button

Callout	Description
C	PS/2 ports
D	USB 2.0 ports x4
E	Display ports x2
F	DVI-D port
G	Serial port
H	USB 3.0 ports x4
I	1 GbE network port (eth0 LAN1)
J	1 GbE network port (eth0 LAN2)
K	Audio ports ⓘ **Note:** This is not supported.
L	Power entry connector: 12 V, 10 A DC

Connector pin outs

Table 66: VideoEdge 2U Hybrid pin outs

Pin number	Assignment	Pin number	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

Table 66: VideoEdge 2U Hybrid pin outs

Pin number	Assignment	Pin number	Assignment
Audio out			
S	Signal Out	G	Ground
Audio in			
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
Form C relay			
G	Ground	C	Common
NO	Normally Open	NC	Normally Closed
RS422			
RX +	Receive +	TX -	Transmit -
RX -	Receive -	TX +	Transmit +

Table 67: VideoEdge 3U Hybrid pin outs

Pin number	Assignment	Pin number	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

Table 67: VideoEdge 3U Hybrid pin outs

Pin number	Assignment	Pin number	Assignment
12	Input 12	12	Output 12
13	Input 13	13	Output 13
14	Input 14	14	Output 14
G	Ground	15	Output 15
15	Input 15	16	Output 16
16	Input 16	17	Output 17
17	Input 17	18	Output 18
G	Ground	G	Ground
18	Input 18	19	Output 19
19	Input 19	20	Output 20
20	Input 20	21	Output 21
G	Ground	G	Ground
21	Input 21	22	Output 22
22	Input 22	23	Output 23
23	Input 23	24	Output 24
G	Ground	G	Ground
24	Input 24	25	Output 25
25	Input 25	26	Output 26
26	Input 26	27	Output 27
G	Ground	G	Ground
27	Input 27	28	Output 28
28	Input 28	29	Output 29
29	Input 29	30	Output 30
G	Ground	31	Output 31
30	Input 30	32	Output 32
31	Input 31	N/A	N/A
32	Input 32	N/A	N/A
G	Ground	N/A	N/A
33	Input 33	N/A	N/A
34	Input 34	N/A	N/A
35	Input 35	N/A	N/A
G	Ground	N/A	N/A
36	Input 36	N/A	N/A
Audio out			
S	Signal Out	G	Ground
Audio in			
G	Ground	9	Input 9
1	Input 1	G	Ground
2	Input 2	10	Input 10

Table 67: VideoEdge 3U Hybrid pin outs

Pin number	Assignment	Pin number	Assignment
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			
G	Ground	C	Common
NO	Normally Open	NC	Normally Closed
RS422			
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 can 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 can 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 can also include a software code component that is resident in a device as provided by Tyco for operating that device. You can use such component of the Software solely in connection with the use of that device, but cannot 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 can 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 can 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. 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).
    g. 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.

4. LIMITED WARRANT:
    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.
5. LIMITATION OF LIABILITY and 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.

6. 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.