3xLOGIC

VIGIL Server 13.0 User Guide

Video Management Desktop Software

62368-1

CAN ICES-003 (A) / NMB-003(A)

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.

2. This device must accept any interference received, including interference that may cause undesired operation.

Note: 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.

Notice: This product is covered by one or more claims of the HEVC Patents listed at patentlist.accessadvance.com

Table of Contents

3xLOGIC

1 INTRODUCTION

Welcome to 3xLOGIC's VIGIL Server Software Service user guide.

VIGIL Server is cutting edge video management software service with an abundance of powerful features, toolsets and accompanying utilities. Server's enhanced integration with video analytics-capable cameras, micro-management style settings and POS/ATM capability are just a few examples of the features that can help to improve the efficiency and stability of your business. Its intuitive design provides ease of use for the most basic user while providing virtually unlimited flexibility for the advanced. As of v11.60.000, VIGIL Server has been converted to a 64-bit service and has been engineered to be securely and seamlessly accessible via 3xLOGIC's remote VIGIL Client software giving you access to your Server and all its data from single or multiple remote location(s). As of v12.50.0000, Server can also be configured and setup locally or remotely using the VIGIL Settings Management Utility (VSMU).

This guide will familiarize you with the software interface of the VIGIL Server and the VSMU. This user guide will detail VIGIL Server's many features but do not hesitate to contact us with any questions, concerns or suggestions. See "Contact Information" on page 120.

Welcome to 3xLOGIC's VIGIL Server.

This user guide is current as of VIGIL Server 13.00.0000 for Microsoft Windows®.

Disclaimer: *This application has been optimized for use Windows 7, Windows 8.1 and Windows 10. 3xLOGIC does not actively support other operating systems. Installing this application on operating systems other than the those mentioned above may have undesirable consequences.

3xLOGIC

2 SOFTWARE FEATURES

This section describes some of the features of VIGIL Server.

Feature	Details
VIGIL Settings Management Utility (VSMU)	Use the VSMU to connect to a local or remote VIGIL Server and configure its settings.
Individual Camera Settings	Configure each camera independently: brightness, contrast, sharpness, hue, resolutions, and more.
Configurable CODEC Settings	Change CODEC settings for each camera such as compression, quality, and more.
IP Camera Support	VIGIL Server supports up to 96 IP hi-resolution cameras (dependent on recorder model) without the need for an installed capture card. With full support for ONVIF Profile S, VIGIL Server is compatible with most modern IP cameras.
POS Integration	Built-in support for several popular serial and IP POS systems with advanced VIGIL Client POS search for data, events and exceptions available with additional VIGIL POS (V-POS) licensing.
DIO / Alarms / Relays	VIGIL Server features support for several popular physical DIOs (e.g. ADAM 6060) and also contains built-in Virtual DIO / Alarm / Relay functionality.
Full Video Search Capabilities via VIGIL Client	Retrieve a list of stored footage for specified cameras from a start date / time to an end date / time and a variety of other search criteria using Server's companion software, VIGIL Client.
Footage Restriction and Footage Locking	Restrict footage to allow only users with sufficient permissions to review it. Lock footage to prevent it from being scavenged, preserving the footage for playback on the system, regardless of age. Restricting and locking footage, as well as management of locked and restricted footage is performed only via the VIGIL Client interface.
Two-Way Audio	VIGIL Server's *Audio Talk* feature allows for easy two-way audio communication via properly configured camera's with two-way audio capability. After configuration, the audio talk controls can be accessed via VIGIL Client.
Exporting / Saving Video and Images	Powerful export capabilities via VIGIL Client enable you to save video footage in AVI or Authentic Video (MJPG) formats. Save still shots in JPEG or BMP formats. Export to local or remote destinations via VIGIL Client.
Full VIGIL Suite Support	VIGIL Server is a service and is intended to be interfaced with all products comprising the VIGIL VMS Software Suite. This includes VIGIL Client, VIGIL Central Management, VIGIL VDM, View Lite II Mobile App, VIGIL CLOUD (via the VIGIL CLOUD NVR Plugin) and more. In conjunction with the VIGIL Suite, VIGIL Server offers a complete and comprehensive set of tools to meet the needs of any user, from single-point applications to enterprise-level networks.
infinias™ Integration	Integration with 3xLOGIC's infinias CLOUD and Intelli-M Mobile Access Control products provides a scalable video surveillance and access management solution, and a seamless, consistent user experience encompassing two of 3xLOGIC's cornerstone products. Uses can configure and access a VIGIL Server's integrated infinias interface via the VIGIL Client application.

3 ACCESSING VIGIL SERVER

3.1 System Tray Server Icon – Right Click Menu

To access a VIGIL Server via VSMU, right-click the 🅅 VIGIL Server System Tray icon.
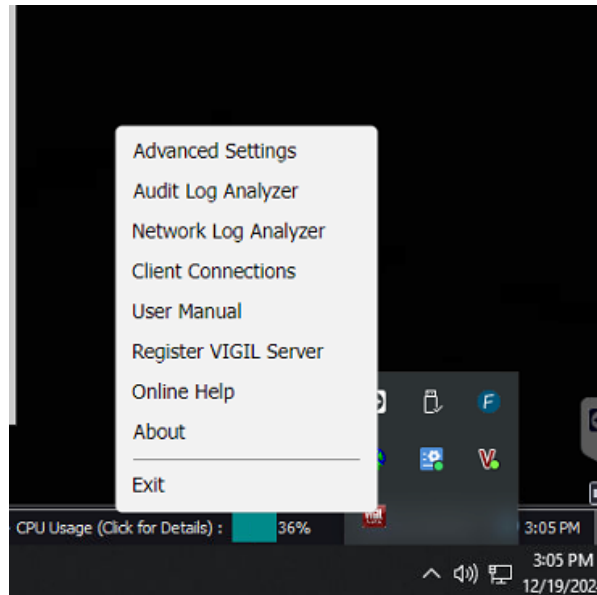
Figure 3-1:VIGIL Server System Tray Icon- Right-Click Menu

All options will be inaccessible (except *User Manual* and *About*) until the user has logged into a VIGIL Server. Select **Advanced Settings** and you will be prompted to login to a VIGIL Server with VSMU. Menu options are detailed below.

- **Advanced Settings** - Opens the *VIGIL Settings Management Utility*, the main interface for configuring and settings up a VIGIL Server and its many features. All available settings are described in the proceeding sections of this user guide. This can also be launched by navigating to the Start Menu>Programs>VIGIL folder

  » Use the login prompt to login to your local VIGIL Server for settings configuration. To login to a remote VIGIL Server, launch VSMU from *Program Files\ VIGIL \ Server \ VSMU \ VigilServer.Settings.UI.exe*.
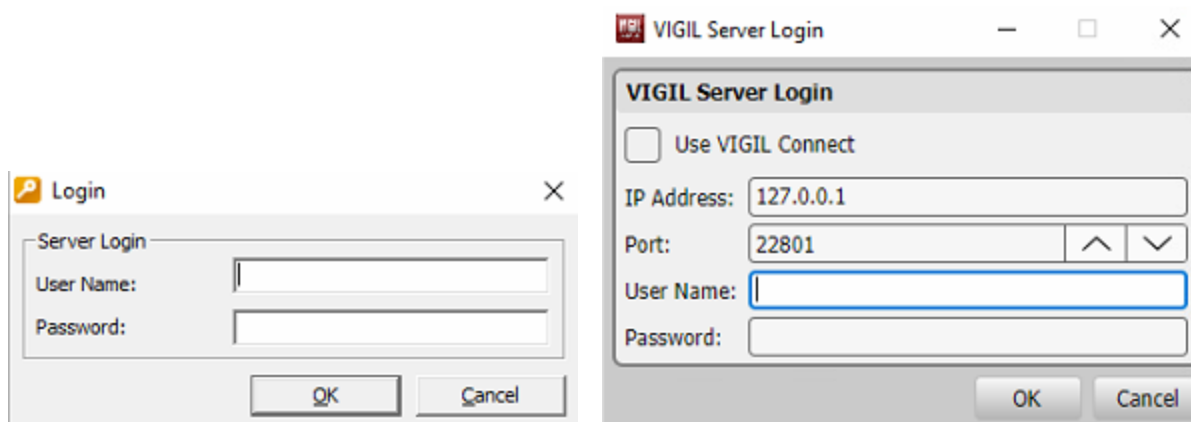
Figure 3-2: VSMU - Login to Local (Left) or Remote (Right) VIGIL Server

- ■ **Audit Log Analyzer** - Open the *Audit Log Analyzer*. See "Audit Log Analyzer" on page 107 for more information.

- ■ **Network Log Analyzer** - Open the *Network Log Analyzer.*

- ■ **Client Connections** - Open the *Client Connections* window. See "Tools" on page 106 for more information.

- ■ **Register VIGIL Server** - Open VIGIL Registration Utility. See "Registration" on page 104 for more information.

- ■ **User Guide** - Launch the VIGIL Server User Guide.

- ■ **Online Help** - Launches the VIGIL VMS Online Help portal. See What's New in the latest VIGIL release, access user guides in a modern browser-based format for easy searching, and access critical support materials for VIGIL VMS applications. External internet connection required.

- ■ **About** - Opens the *About 3xLOGIC Inc. VIGIL Server System* window that contains information such as:

  - » *Remaining Trial Period Time*
  - » *Registration information*
  - » *Serial number / VIGIL Connect alias*
  - » *QR Code for instant integration of a Server with the View Lite smartphone app.*
  - » *Software version (including IP Camera and POS .dll file versions).*
  - » *SUP(Software Upgrade Plan) Activation.*

- ■ **Exit** - Quit the VIGIL Server application.

3×LOGIC

4 VSMU – CAMERA SETUP TAB

VIGIL Server is a diverse software application that interfaces with a wide variety of hardware configurations. A comprehensive control set is available to configure the VIGIL Server as required. The proceeding sections will describe the available settings in detail.

To access settings, right-click the system tray VIGIL icon and select **Advanced Settings**. The *VIGIL Settings Management Utility - Advanced Settings* window will deploy with the *Camera Setup Tab* displayed by default. DVR / NVR Type and version will be displayed in the window header. Select a camera from the left-side list.

The order of the Cameras channel list can be edited by selecting a camera and using the ⬆ Move Up and ⬇ Move Down buttons. Other VIGIL utilities interfaced with VIGIL Server (i.e VIGIL Client, etc...) will display the cameras in the configured order. Click the **Reset** button to reset camera ordering to the default camera channel.
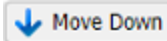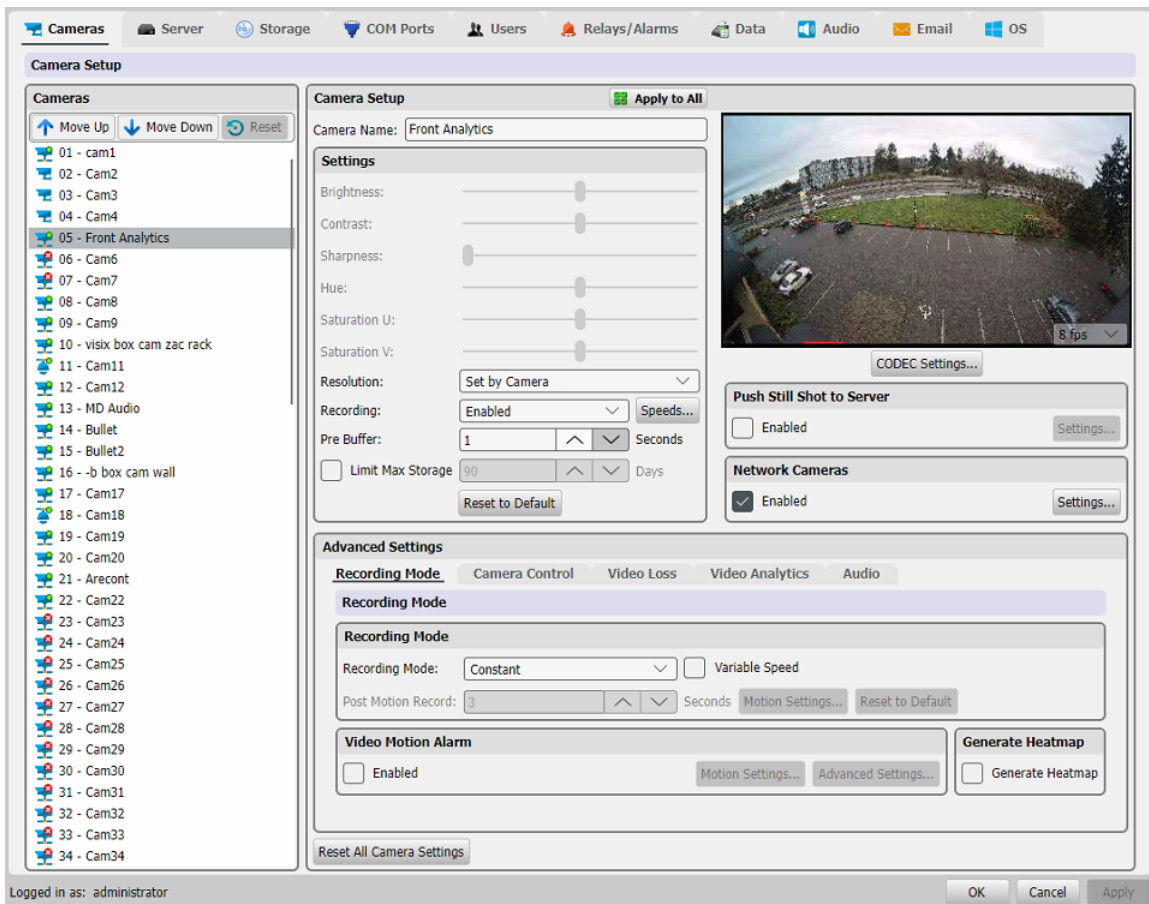
Figure 4-1: Settings - Camera Setup Tab

The *Camera Setup Settings* allow configuration of the camera image, resolution, recording speed, buffering and CODEC. Network cameras are also enabled under the *Camera Setup* tab.

- **Camera Name** - Configure the selected camera's name. This is how it will be reference in the VIGIL suite.

■ **Apply to All** - Click the *Apply to All* button at the top of the window to apply the same settings to all cameras. Settings that will be applied to all cameras will be indicated by **BOLD** headings.

Note: Only changes made after clicking *Apply to All* will be applied to every camera.

4.1 Camera Setup Tab – Camera Settings

■ **Brightness** - Adjusts the brightness of the video footage.

■ **Contrast** - Adjusts the contrast of the video footage.

■ **Sharpness** - Adjusts the sharpness of the video footage.

■ **Hue** - Adjusts the color of the video footage.

■ **Saturation U and V** - Adjusts the U and V color difference signals used in YUV color format for the video footage. Note that not all cameras use a YUV color format, in which case, adjusting the *Saturation U* slider will adjust the color saturation while the *Saturation V* slider will have no effect.

■ **Resolution** - Select a recording resolution from the drop-down menu. Options range from 352x240 to 704x480 resolution. If a network camera is enabled on the channel, this option will not be available.

■ **Recording** - Use the drop-down menu to enable or disable recording of the selected camera. If the selected camera is not available, *Inactive* will be displayed here.

■ **Speeds** - Opens the *Recording Speed* window. The recording speed can be set individually for *Constant, Motion* and *Alarm* Recording Mode. Use the drop-down menu to select the desired number of frames per second (fps).

Note: Network cameras will often record and play back at a slower rate than what was set in the *Recording Speed* window, depending on the bandwidth and camera.
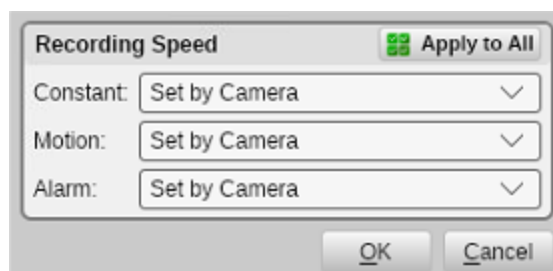
Figure 4-2: Recording Speed Window

■ **Pre Buffer** - The number of seconds of footage to record prior to a motion detection or alarm event. For JPEG Camera streams the recommended setting is 1. For H264 Camera streams it is recommended to set the pre buffer to the key frame rate.

■ **Limit Max Storage** - If enabled, this setting will limit retention for footage and data from this camera to the designated number of days, configured in the available selection field.

■ **Reset to Default** - Returns the camera settings to their default values.

3xLOGIC

4.1.1 Push Still Shot to Server

The *Push Still Shot to Server Settings* window allows a still shot from the camera to be copied periodically to another location. To enable this feature for the selected camera, check the *Enabled* box. Click the *Settings…* button to configure the destination for the still shots. This applies to all cameras.
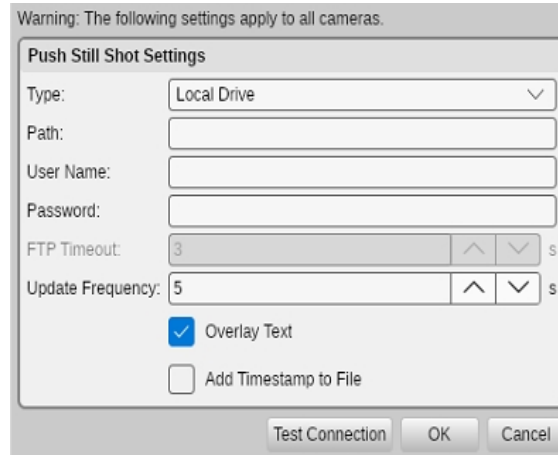
Figure 4-3: Push Still Shot Settings Window

- **Type** - The type of storage location. Options are *FTP Location, Windows Network Share* and *Local Drive*.

- **Path** - The path where the image files will be uploaded (only pre-existing directories can be used).
    - » **Local Drive**:C:\Images.
    - » **Windows Network Share**: \\ComputerName\SharedFolder.
    - » **FTP Location**: ftp://ftpserver/folder.
- **FTP User Name and Password** - If required, enter the user name and password for the FTP Site.
- **FTP Timeout** - The time to wait in seconds before a timeout occurs.
- **Overlay Text** - Check this to have an overlay of the camera name, date, and time on the still shot.
- **Update Frequency** - The frequency, in seconds, at which the image file is uploaded to the specified path.
- **Add Timestamp to File** - Enable this option to append still-shot file names with a timestamp.
- **Test Connection** - Tests the connection using the specified parameters. A window will display a message stating whether the connection is successful or not.

4.2 CODEC Settings

The *CODEC Settings* window allows advanced configuration of the recording CODEC used for storing video footage recorded from a camera.

Click the [CODEC Settings...] button to open the *CODEC Settings* window.

Figure 4-4: CODEC Settings

- **CODEC** - Select between AZTECH and MPEG4 encoding.

  Note: Normally, two video encoding CODECs are currently available for recording video footage: *AZTECH and MPEG4 CODEC*s. However, some models support Hardware CODECs, which have slightly different customization options.

- **Reset to Default** - Resets the CODEC settings to their default values.

- **Picture Quality** - Adjusts the picture quality of the recorded video. Higher quality video will occupy more space on the video storage drive. The arrows, the text box, or the slide bar can be used to change the value.
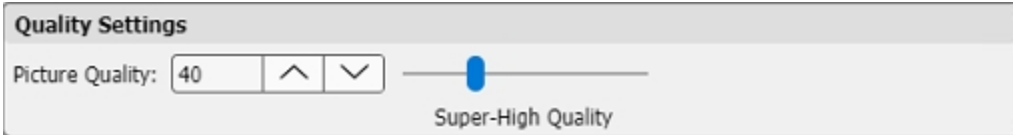
Figure 4-5: Quality Settings

How Picture Quality Can Affect Total Disk Usage:
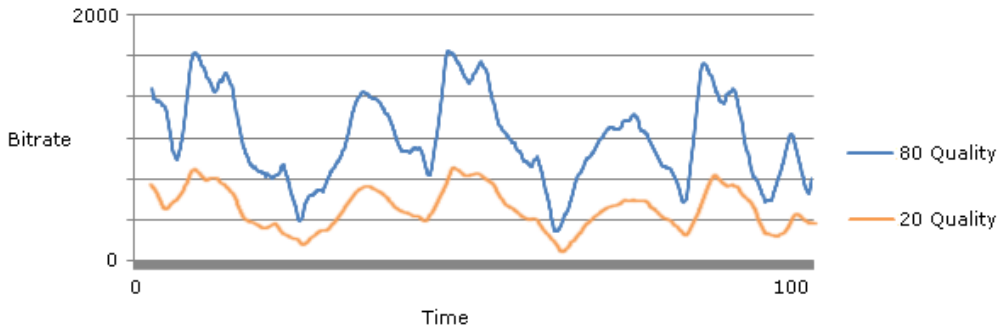
Figure 4-6: Video Quality Disk Usage

4.2.1 AZTECH™ CODEC Settings

The AZTECH™ CODEC is the default CODEC for most systems. To switch the recording CODEC to *AZTECH,* select the *AZTECH* option from the *CODEC* drop-down menu.
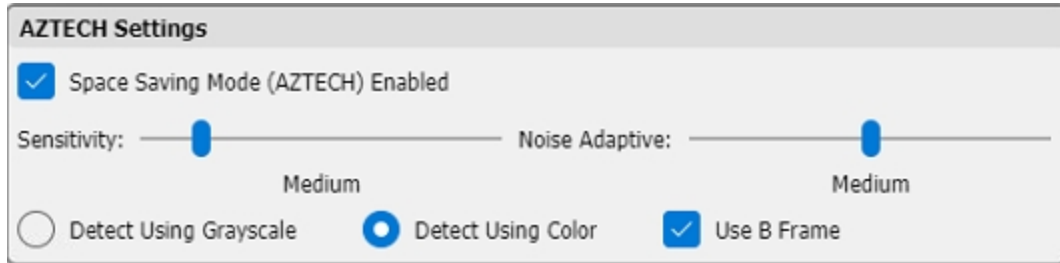
Figure 4-7:AZTECH CODEC Settings Tab

- **Space Saving Mode (AZTECH) Enabled** - Enables advanced compression technology to decrease the file size of recorded footage.

> **Note:** This is a CPU intensive setting.

- **Sensitivity** - Adjusts the threshold used by the CODEC to identify areas of change between frames. The higher the sensitivity, the smaller a change is encoded.
- **Noise Adaptive** - Adjusts the noise threshold used by the comparison algorithm when determining whether a block contains a change. When this value is increased, more noise is allowed in the block without triggering change for that block. This feature does not decrease noise in an image.
- **Detect Using Grayscale/ Color** - Determines whether grayscale or color will be used to detect changes.

> **Note:** Color detection is a CPU intensive setting.

- **Use B Frame** - Uses bi-directional frames to decrease the file size of recorded footage.

> **Note:** This is a CPU intensive setting.

4.2.2 MPEG4 CODEC Settings

To switch the recording CODEC to *MPEG4,* select the *MPEG4* option from the *CODEC* drop-down menu.
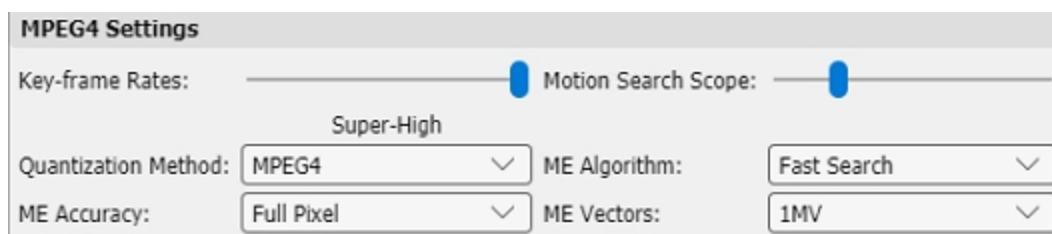
Figure 4-8:MPEG4 CODEC Settings

- **Key-frame Rate** - Sets the number of key-frames recorded per second. The higher the value, the greater the data space needed for recording, but the higher the quality of the video.

- **Motion Search Scope** - Changes the size of the regions used to detect motion.

- **Quantization Method** - Selects the type of compression. *H263* offers less compression than *MPEG4* but requires more CPU usage.

- **ME Accuracy** - Motion Estimation Accuracy includes two options: *Full Pixel* and *Half Pixel*. Full Pixel checks for motion comparing differences of full pixels. Half Pixel will check for motion using an interpolation method that detects finer movements.

> **Note:** Half Pixel is a CPU intensive setting.

- **ME Algorithm** - The *Motion Estimation Algorithm* changes the shape of the area used for motion detection and includes two options: *Full Search* and *Fast Search*. *Fast Search* will save CPU time but *Full Search* is more accurate.

- **ME Vectors** - Sets the number of vectors tested for motion from 1 to 4. The greater the number, the more CPU processing is required.

3xLOGIC

4.3 Network Camera Settings

Enabling the Network Camera setting on a camera or clicking on the Network Camera - Settings button opens the *Network Camera Settings* form, pictured below. The form consists of four tabs: *Stream* (open by default), *Encoder*, *Image* and *Management*.

Note: Depending on camera make and model, the *Encoder, Image* and *Management* tab's availability and the availability of features contained within may differ. The *Stream* tab will always be visible for all devices but some options (on-board analytics, multiple camera setup) will depend on make, model and camera type. Refer to your camera manufacturer's hardware documentation for descriptions of settings available in the Encoder, Image and Management tabs. The most common settings are pictured in the proceeding sections below as reference only.

Figure 4-9: Network Camera Settings Window

4.3.1 Network Camera Stream Settings

VIGIL Server is able to receive video from one or many network cameras connected to a LAN or WAN. VIGIL Server currently supports several types of network cameras.

To setup or change a network camera, check the *Network Camera* box, then click the *Settings…* button. This will open the *Network Camera Settings > Stream Tab* window. Descriptions for each of the form's fields are as follows:

- **Type** - The type of network camera being configured. See " Network Camera Types " on page 18 for more information on common network camera types.

  Warning: Due to the substantial overhead associated with HTTP, attempting to record HTTP camera feeds over the Internet is not recommended. High speed LAN or WAN configurations are recommended for HTTP camera use. If the network bandwidth is insufficient, the message *Signal Loss* will be displayed in place of the live feed.

  - » **Detect Cameras** - If an applicable camera type is selected, this option will be visible. Choose this option to open the associated camera detection utility (Detect Network Cameras Utility, etc...)

  - » **Web / Camera Settings** - Connects to the camera's web interface to make changes to the camera's internal settings. For some camera types, this will open a *Camera Settings* window instead of connecting to the web interface.

» **On-Board Analytics** - If the configured camera has on-board analytics rule processing, this button will launch the On-Board Analytics form (formerly referred to as the VIGIL Analytics Bridge) so the user may interface the camera's rules with VIGIL Server.
For details on the On-Board Analytics window, See "On-Board Analytics" on page 102.

■ **Address** - The IP or HTTP address of the camera. It is not necessary to include http:// at the beginning of the HTTP address.

■ **Data / RTSP Port** - The network ports used to connect with the camera.

■ **HTTPS** - Enable if HTTPS if required for the camera.

■ **RTSP Stream Type** - Select the camera's preferred RTSP Stream Type(also known as the RTSP Transfer Protocol; UDP or TCP).

■ **...** - Opens additional configuration options for *File Stream* camera type.

■ **Stream Type** - Select the video stream type for the camera: *MPEG4, JPEG, or H264/H265*. Some kinds of network cameras can only have one stream type for all cameras of its kind.

■ **Timeout** - The number of seconds to attempt to connect to the camera before timing out. If the timeout is reached, *Signal Loss* displays in the *Live Viewer* window.

■ **User / Password** - The user name and password to connect to the camera. The default values are automatically entered.

■ **Camera Number** - Some *Network Camera* types also support encoders. Select the camera number on the encoder to use for this network camera.

■ **Mainstream / Substream URL** - Set the broadcast URL for the camera's mainstream and sub-stream (if applicable). The substream URL field will not be editable if a sub-stream is not enabled for the camera.

■ **AZTech Recompress** - This will recompress the image using AZTECH™ codec.

> **Note:** AZTech Recompression is a CPU and RAM intensive process.

■ **Fast Decompression** - If the JPG image provided by the HTTP camera supports fast decompression, select this option to significantly reduce the number of CPU cycles needed for rendering the network camera feed.
Not all network cameras support fast decompression. Disable *Fast Decompression* if the image does not display or appears distorted when this feature is enabled.

■ **DIO (Digital Input/Output)** - If the Network Camera supports DIO, enable the checkbox to automatically add the camera as a DIO device.

■ **Audio Recording** - If the Network Camera supports audio, enable the checkbox and enter a Name for the audio channel to automatically add the camera as an audio device.

■ **Camera Control** - If the Network Camera supports *PTZ (Pan/Tilt/Zoom)*, enable the checkbox to allow PTZ controls to be utilized from within VIGIL Server (via VIGIL Client).

■ **Audio Talk** - If the Network Camera supports *Audio Talk*, this feature can be enabled to allow for two-way audio talk.

3xLOGIC

- **Substream** - Enable this checkbox to make the *Sub Stream* from the Network Camera available to applications that connect to the Server such as VIGIL Client.
- **Web Interface in Client** - Grants a right-click menu option to quickly access the camera's web interface from a built-in browser. .
- **Default Settings** - Changes the network camera settings to their default values.

4.3.2 Network Camera Encoder Settings

The Network Camera form's *Encoder Tab* allows the user to view, configure and push encoder profile settings from applicable camera models.

Figure 4-10: Network Camera - Encoder Tab Settings

To edit encoder settings:

1. Review and configure settings as required. Refer to your camera's documentation for information on available encoder profile settings.

2. If changes are made, click **Push Settings to Camera** to save the new encoder settings on the camera.

- Click **Set to Main Stream** to save the current *Stream URL* value to the Stream Tab's *Main Stream URL* field.

- Click **Set to Sub Stream** to save the current *Stream UR*L value to the Stream Tab's *Sub Stream URL* field.

4.3.3 Network Camera Image Settings

The Network Camera form's *Image Tab* allows the user to view, configure and push video image settings to / from applicable camera models.

The Image tab form features common video image settings.

1. Review and configure settings as needed. Refer to your camera's documentation for information on available image settings.
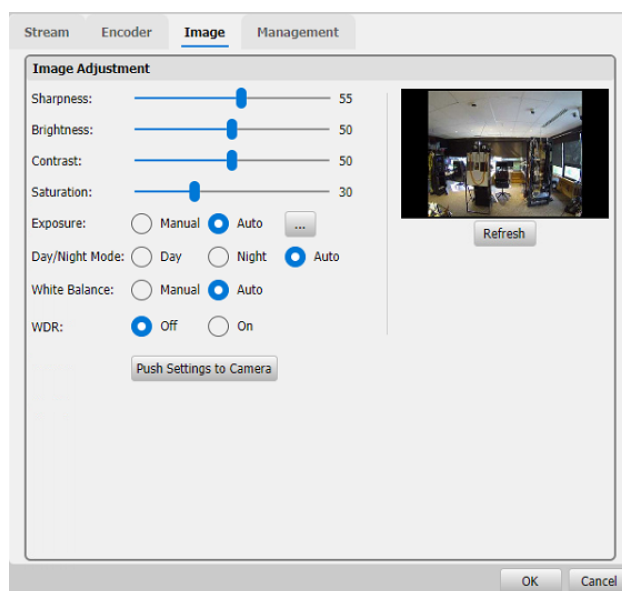
Figure 4-11: Network Camera Image Settings

2. If changes are made, click **Push Settings to Camera** to save the new image settings on the camera. Click the **Refresh** button to view the result in the available preview thumbnail.

4.3.4 Network Camera Management Tab

The Network Camera form's *Management Tab* allows the user to view, configure and push settings related to general management and maintenance of applicable camera models.
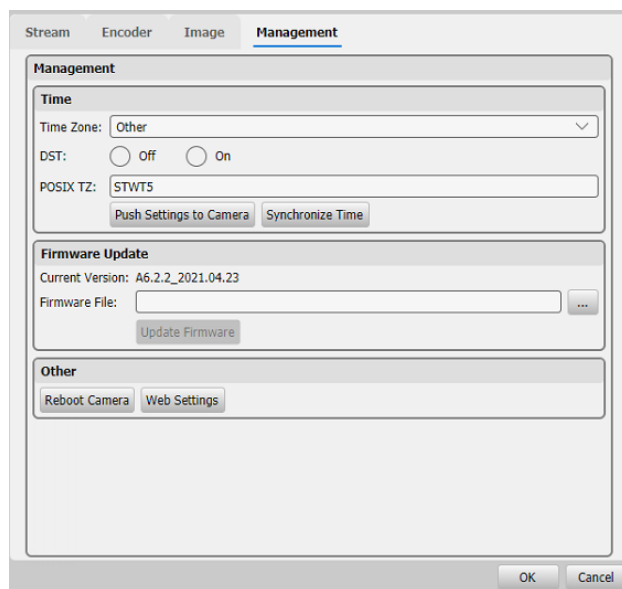
Figure 4-12: Network Camera Management Tab

To update Time settings for an applicable camera:

3xLOGIC

1. Review and edit time settings as required. If desired, click **Synchronize Time** to sync the camera's time with the VIGIL Server's current time. Review your camera's documentation for full descriptions of available time settings.

2. If changes are made to *Time* settings, click **Push Settings to Camera** to save the new image settings on the camera.

To update an applicable camera's firmware:

1. Under *Firmware Update,* click **...** to locate a firmware file on your local system then click **Update Firmware** to update the camera's firmware. This process can take several minutes. Refer to your camera's documentation for more information.

Other available settings include **Reboot Camera** and **Web Settings** (opens the camera's web UI in your default browser).

4.3.5 VCA Settings

As of v13.0 of the VIGIL VMS Suite, users can configure VCA analytics rules and settings directly in VSMU for applicable VISIX Gen III cameras(VCAEdge Plugin v1.1.131 or higher required) that have been interfaced with VIGIL Server. The *Network Camera Settings > VCA Tab* allows users to edit and configure these VCA settings and rules.

> **Note:** This section will provide an outline to aid users in navigation of the VCA interface within VSMU. For full details on VCA settings, rule types and rule configuration, refer to the latest VISIX Gen III VCA User Guide.
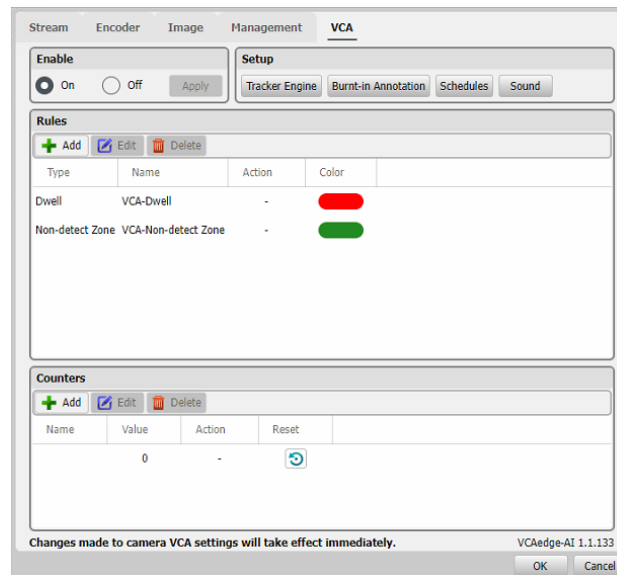
Figure 4-13: Network Camera Settings - VCA Settings

> **Warning:** Any changes to VCA settings will take effect immediately. Manually revert any unwanted settings changes.

- ■ **Enable** - To enable VCA, click the **On** toggle and click **Apply**.
- ■ **Tracker Engine** - To switch between object *Tracker Engines*, click the **Tracker Engine** button and select the desired tracker.
- ■ **Burnt-in Annotation** - To configure *Burnt-in Annotation* (OSD) settings, click the **Burnt-in Annotation** button. The BIA settings window will deploy. From here, a user can enable BIA, choose the associated stream and configure which data to display on-screen.
- ■ **Sound** - To configure sound settings, including custom alarm sounds (.wav) and voice models, click the **Sound** button. the *Sound* settings window will deploy. Configure settings as desired.
- ■ **Add / Edit / Delete Rule** - Use these settings to add, edit or delete VCA rules on the camera. See "Add VCA Rule" below for more information.
- ■ **Add / Edit / Delete Counter** - Use these settings to add, edit or delete VCA counters on the camera. See "Add VCA Counter" on the facing page for more information.

For further details on any of the above settings or options, refer to the latest VISIX Gen III VCA User Guide. Continue through the remainder of this section for information on configuring VCA *Rules* and *Counters* via VSMU.

Add VCA Rule

Click the **Add** button on the Network Camera Settings - VCA Tab's *Rules* section to add a VCA rule.

Before rule settings deploy, a rule type must be selected. Selected the desired type from the available menu. Once selected, the VCA rule configuration window will deploy.

Note: Depending on the selected rule type, available fields and options may differ from those depicted below. Refer to the latest version of the VISIX Gen III VCA User Guide for full details on available rule types and their configuration.

3xLOGIC
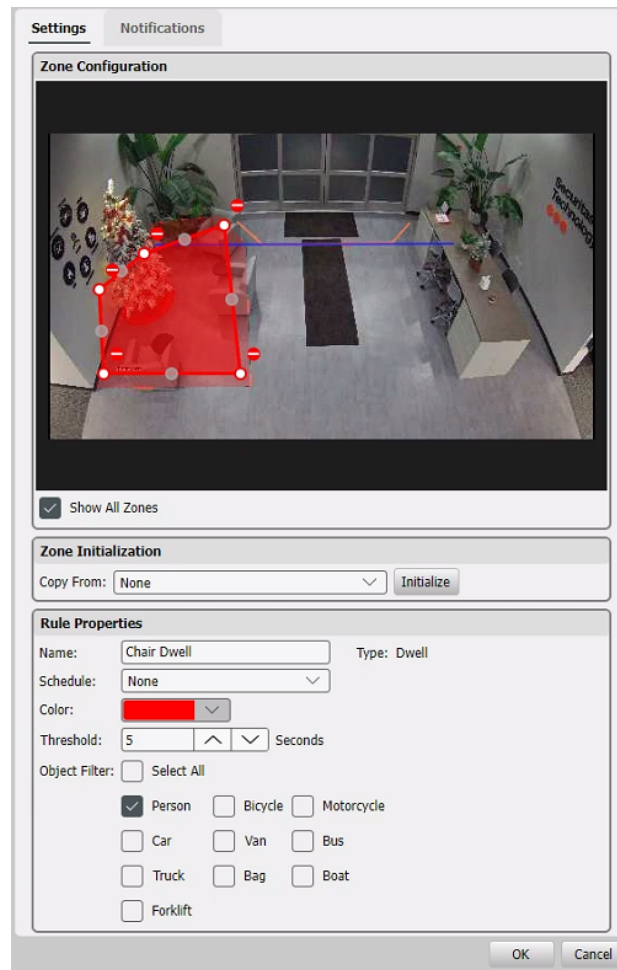
Figure 4-14: Configuring a VCA Rule

The *Rule Configuration* window contains two tabs. The **Settings** tab contains *Rule Properties* and *Zone Initialization* settings. The **Notifications** settings tab contains settings related to event notifications for the rule.

To create a VCA rule:

1. Configure *Rule Properties* as required for your application.

2. Draw any required zones or lines within the preview image.

3. Configure *Notifications Settings* as desired.

4. Click **OK** to leave configuration.

For full details on any of the above settings, options or processes, refer to the VISIX Gen III VCA User Guide.

Add VCA Counter

Click the **Add** button on the Network Camera Settings - VCA Tab's *Counters* section to add a VCA Counter. The VCA Counter configuration window will deploy.
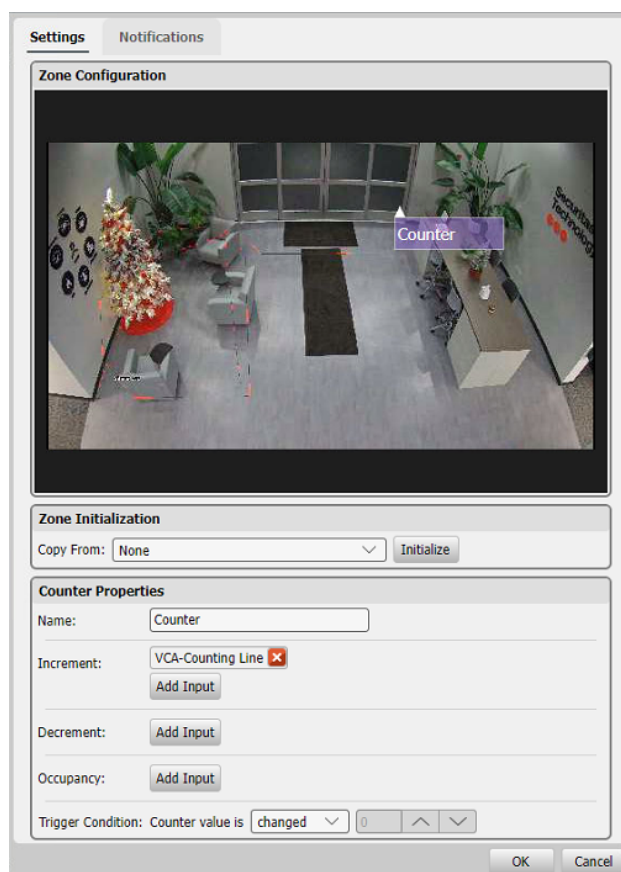
Figure 4-15: Configuring a VCA Rule

The *Counter Configuration* window contains two tabs. The **Settings** tab contains *Counter Properties* and *Zone Initialization* settings. Counter properties can be configured to allow for an on-screen "count" of tracked objects. The **Notifications** settings tab contains settings related to the counter's value.

To create a VCA Counter:

1. Configure *Counter Properties* as required for your application.
2. Place the counter at the desired location using the preview image.
3. Configure *Notifications Settings* as desired.
4. Click **OK** to leave configuration.

For full details on any of the above settings, options or processes, refer to the latest VISIX Gen III VCA User Guide.

4.3.6 Network Camera Types

VIGIL Server maintains direct support for several camera makes and models, and with full ONVIF Profile S compliance, compatibility is extended to any camera compliant with the ONVIF Profile S standard. The following section contains basic descriptions and / or minor configuration instructions on common network camera types utilized in VIGIL Server.

> **Note:** Depending on the selected Camera Type, each tab in the Network Camera Settings field may feature varying fields and options.

VISIX IP Camera - Network Camera Type

VISIX IP Cameras, by 3xLOGIC Inc, come in all shapes and styles and offer the performance and clarity you demand. When coupled with a VIGIL Server, users can take full advantage of the adaptive compression capabilities resulting from our exclusive AZTECH™ Compression Codec and proprietary RapidStream™ Technology, letting users toggle between bandwidth-conserving compressed video and the native high-resolution video seamlessly with just a click.

To configure a 3xLOGIC VISIX Camera:

1. Select **3xLOGIC VSX-IP** in the *Network Camera Settings >Stream Tab'*s **Camera Type** field. Newer cameras generations are referred to as *3xLOGIC VSX-IP-A* or *3xLOGIC VSX-IP-B*.

VIGIL Server features an embedded camera detection tool for detecting and adding VISIX cameras on your network to VIGIL Server. After selecting the camera type on the *Network Camera Settings* form, click **Detect Cameras** to launch the tool.

If you select the incorrect VISIX-IP type for your camera, the utility will automatically detect and correct the type when saving the camera back to VIGIL Server. Conversely, if you are manually entering camera information into the *Network Camera Settings* form, be sure to select the type as defined in your camera's documentation. Proceed below for instructions on operating the detection tool.

Adding a VISIX Camera to VIGIL Server

> ⚠ **Warning:** If adding new 3xLOGIC VISIX Cameras, the camera password must be changed before the camera will stream to VIGIL Server. This is a security precaution. Refer to your camera documentation for steps on changing the default password.
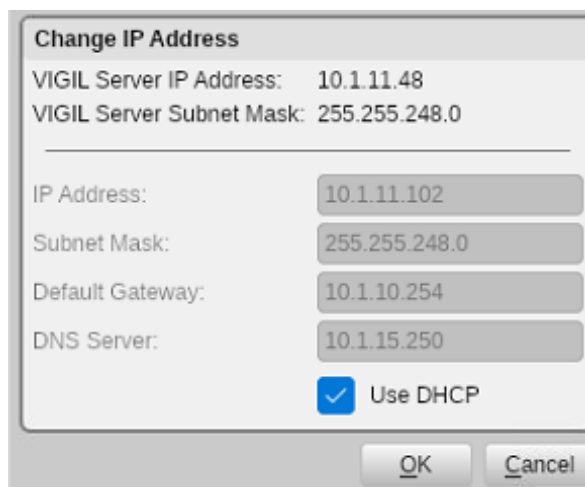
After the tool launches, a list of VISIX and ONVIF cameras discovered on your network will be generated. Click **Refresh Results** and / or **Restart Probe** (bottom-left) to update results list and available camera information respectively.

Type	IP	MAC	Hardware	Name	Manufacturer	Detected From	VIGIL Channel	Notes	
3xLOGIC VISIX-IP-B	10.1.11.103	1C:82:59:18:DF:EA	VX-5M20-B-RIAW	IP-Camera	3xLOGIC	10.1.11.48/21 (enp2s0)			
3xLOGIC VISIX-IP	10.1.11.104	64:DB:8B:11:7A:96	VX-4V28-OD-I	VX-4V28-OD-I		10.1.11.48/21 (enp2s0)			
3xLOGIC VISIX-IP-A	10.1.11.106	00:13:23:08:22:D3	VX-2A-B-IWD	VISIX 2 MP Analytic IR Wide Dynamic Bullet Camera		10.1.11.48/21 (enp2s0)			
3xLOGIC VISIX-IP	10.1.11.108	44:19:B6:5A:11:22	VX-3M20-B-RIAWD	VX-3M20-B-RIAWD		10.1.11.48/21 (enp2s0)	5 - Cam5		
3xLOGIC VISIX-IP	10.1.11.109	28:57:BE:04:7A:20	DS-2DF5286-AEL	DS-2DF5286-AEL		10.1.11.48/21 (enp2s0)			
3xLOGIC VISIX-IP-B	10.1.11.111	1C:82:59:19:E0:B9	VX-8M-OD-RIAW-X	IP-Camera	3xLOGIC	10.1.11.48/21 (enp2s0)			
ONVIF	10.1.11.116	54:C4:15:75:0D:17		HIKVISION iDS-2CD6810F_C		10.1.11.48/21 (enp2s0)			
3xLOGIC VISIX-IP-B	10.1.11.132	00:0D:F1:21:85:59	VX-5M4-MD-IAW	IP-Camera	3xLOGIC	10.1.11.48/21 (enp2s0)			
3xLOGIC VISIX-IP-A	10.1.11.135	00:13:23:E0:17:28	IPN302HD	VISIX 2 MP Analytic Mini Dome Camera		10.1.11.48/21 (enp2s0)			
3xLOGIC VISIX-IP-A	10.1.11.136	00:13:23:E0:11:1F	VX-2A-IMD-X	VISIX 2MP Analytic Mini Dome Camera		10.1.11.48/21 (enp2s0)			
3xLOGIC VISIX-IP-A	10.1.11.138	00:13:23:E0:17:73	VX-2A-IMD-X	VISIX 2 MP Analytic Mini Dome Camera		10.1.11.48/21 (enp2s0)			
3xLOGIC VISIX-IP-A	10.1.11.140	00:13:23:E0:17:9C	IPN302HD	VISIX 2 MP Analytic Mini Dome Camera		10.1.11.48/21 (enp2s0)			
3xLOGIC VISIX-IP-A	10.1.11.141	00:13:23:E0:17:4E	IPN302HD	VISIX 2 MP Analytic Mini Dome Camera		10.1.11.48/21 (enp2s0)			
3xLOGIC VISIX-IP-A	10.1.11.144	00:13:23:E0:17:91	VX-2A-IMD-X	VISIX 2 MP Analytic Mini Dome Camera		10.1.11.48/21 (enp2s0)			
3xLOGIC VISIX-IP-A	10.1.11.146	00:13:23:E0:17:1C	VX-2A-IMD-X	VISIX 2 MP Analytic Mini Dome Camera		10.1.11.48/21 (enp2s0)			

Restart Probe | Refresh Results | Devices Detected: 181 — Change IP Address | OK | Cancel

Figure 4-16: Detect Network Camera Tool

To add a camera to VIGIL:

1. Select the desired camera from the results list.
2. If IP settings changes for the camera are required, click the **Change IP Address** button.
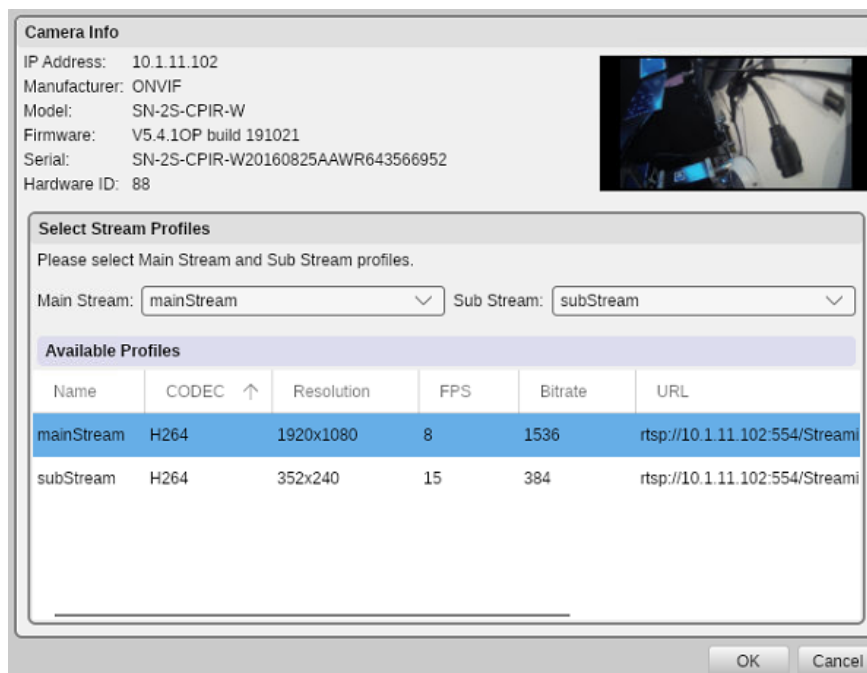
Figure 4-17: Detect Network Camera Tool- Change IP Address

3. DHCP is used by default. Disable **Use DHCP** and configure *IP Address, Subnet Mask, Default Gateway* and *DNS Server* values as required. Click **OK** to save the new IP settings. You will be returned to the detection utility.

4. With the camera selected, click **OK**. If you did not change IP settings, you will be prompted to login to the camera. If required enter login info and click **OK**.

If login is successful, the camera's info window will deploy. The camera's *IP Address,Manufactuer* (or *Type*), *Models*, *Firmware*, *Serial Number* and *Hardware ID* are displayed alongside a camera preview.

Figure 4-18: Detect Network Camera Tool- Camera Info

3xLOGIC

5. Under the *Select Stream Profiles* section, review profile configurations and assign stream pro-files to the cameras Mainstream and Substream (if applicable).

6. Click **OK**. The camera settings will now populate the Network Camera Settings form in VIGIL.

Adding a VISIX Camera to Server Using the Detect Network Cameras Utility

⚠️ **Warning:** If adding new 3xLOGIC VISIX Cameras, the camera password must be changed before the camera will stream to VIGIL Server. This is a security precaution. Refer to your camera doc-umentation for steps on changing the default password.

Although VIGIL Server now features an embedded detection utility, support is still maintained for the legacy Detect Network Cameras Utility. For instructions on operating the utility, read the remainder of this section.

Launch the utility from *Start>VIGIL> VISIXIP Utility.exe*. After from the utility launches, a list of VISIX and ONVIF cameras discovered on your network will be generated:

1. Select the desired camera.
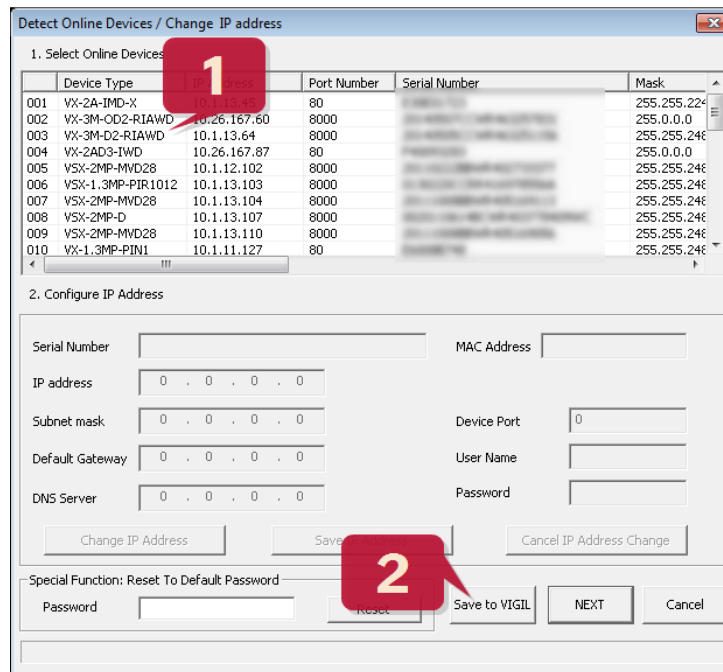
Figure 4-19: Detect Network Cameras Utility - Saving a Camera to VIGIL Server

2. Click the **Save to VIGIL** button. If the camera support multiple streams, this will deploy the camera's stream settings window.

3. In the camera's stream settings, a user can assign the camera's Main Stream and Substream profiles. When finished, select **OK.**

All appropriate camera settings will now populate the Network Camera Settings form fields.

4. Select **OK** to save the new camera configuration.

Repeat the above process for all desired VISIX cameras on your network.

Detect Network Cameras Utility Properties

When launched externally, the Detect Network Cameras Utility's main UI will deploy as pictured below(the right-hand Advanced Settings portion will not be visible):
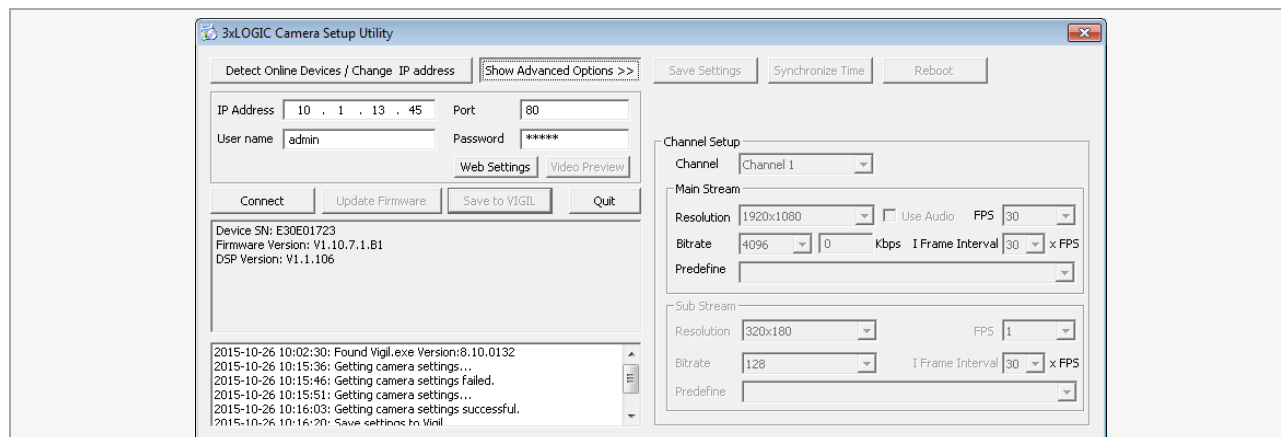
Figure 4-20: 3xLOGIC (VSX IP) Camera Setup Utility - Main User Interface

Detect Online Devices/ Change IP address	This will launch the Detect Online Devices/ Change IP address menu (this menu is automatically deployed when the utility is launched from within VIGIL Server). Once the desired camera has been located and settings have been configured as desired, click the **Next** button to return to the main screen of the utility.
Web Settings	*Web Settings* will launch the camera's web page in a web browser.
Video Preview	Opens a video preview from the selected camera.
Connect/ Disconnect	This button will allow users to toggle between establishing a connection and disconnecting from the IP Camera.
Update Firmware	Users can update firmware within the utility by clicking on the Update Firmware button and navigating to the stored firmware file.
Save to Vigil	Upon completion of camera configuration, click the Save to VIGIL button to return to the VIGIL Server Network Camera Settings form.
Quit	Exit the Detect Network Cameras Utility.
Advanced Settings	Opens the Advanced Settings portion of the setup utility. See "Detect Network Cameras Utility - Advanced Settings" below for more information.

Detect Network Cameras Utility - Advanced Settings

Advanced Settings allows a user to modify the resolution, bitrate, FPS, and I Frame interval for the camera's Main Stream and Substream. Other configuration options are described below:

- **Synchronize Time** - Users can synchronize the camera's time to server time by clicking the Synchronize Time button. This option may not be available across some camera models or firmware versions.

- **Reboot** - Users can reboot the camera within the utility by clicking the Reboot button.

- **Save Settings** - Users should save all changes made within the utility by clicking the Save Settings button.

ONVIF - Network Camera Type

ONVIF is an interoperability standards for IP based Network Cameras. As long as a camera supports ONVIF, it can be configured with this standard instead of the brand specific standard. ONVIF is the

3xLOGIC

predominate standard currently being utilized by manufacturers.

When configuring an ONVIF supported camera through the *Network Camera Settings > Stream* tab and the *Detect Cameras* button is clicked, the *Detect Network Cameras* tool will launch. See "Adding a VISIX Camera to VIGIL Server" on page 19 for more information.

Multiple Cameras (VIGIL Multiview™ Technology) - Network Camera Type

When selecting a Network Camera *Type*, a user may select the *Multiple Cameras* option. This camera type uses VIGIL Multiview™ technology to multiplex(mux) a customized number of your camera feeds into a single, bandwidth friendly image stream. This stream can then be viewed in Server or other VIGIL Products such as VIGIL Client like a traditional IP camera.

To setup a Multiview stream, open / enable *Network Camera* settings on a camera channel, then:
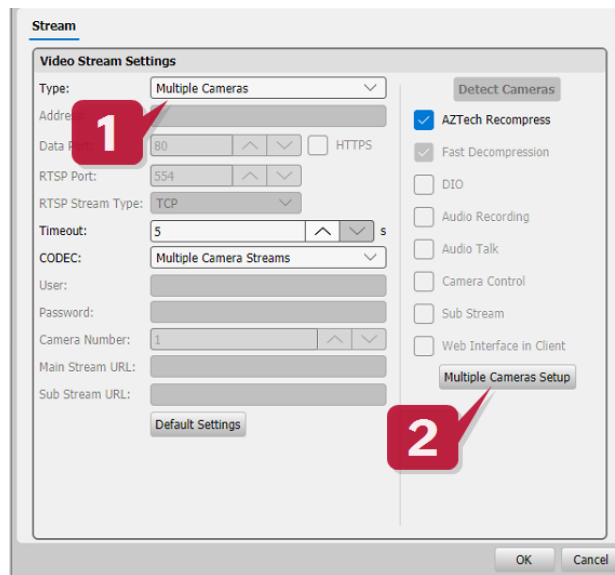
Figure 4-21: Network Camera Types - Adding a VIGIL Multiview Channel

1. Select **Multiple Cameras** in the*Network Camera Settings > Stream* form's *Type* field.
2. Click the **Multiple Cameras Setup** button.

This will open the *Multiple Camera Settings* window(pictured below).

Multiview layouts are configured by row. By default, the first row will already exist.

To add a new row:

1. Select the *Add* button located within the Rows portions of the Multiple Camera Settings window.

To add a camera to a row:

1. Select the desired row using the Rows drop-down menu.
2. Select the *Add* button located within the Camera portion of the Multiple Camera Settings window.
3. Set Camera Width to designate how much of the row a camera frame will occupy. Use this to make some camera images more prominent.

Rows and cameras may be deleted by selecting the camera or row to be deleted and clicking their respective *Delete* buttons.
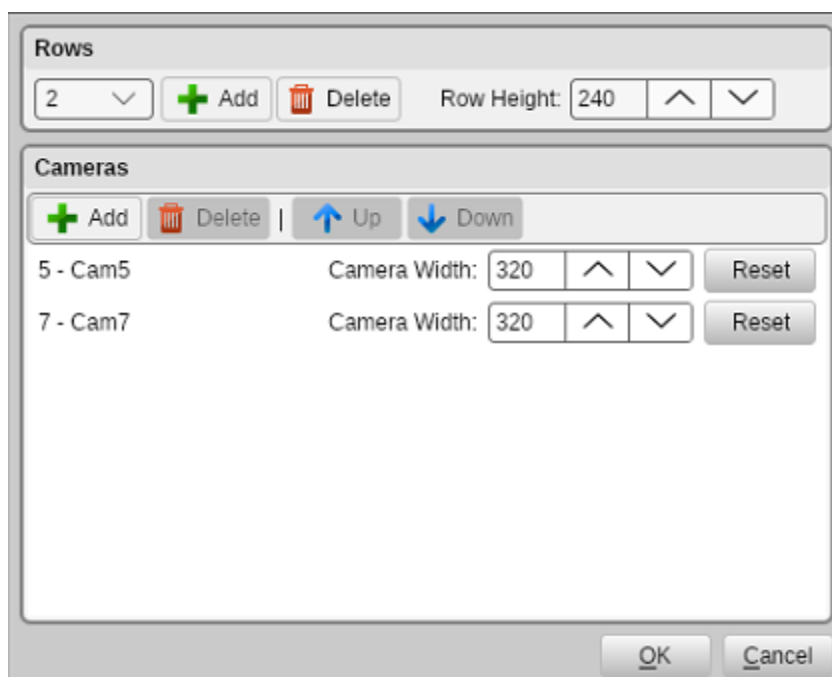
Figure 4-22: Network Camera Types - Multiview - Multiple Cameras Settings Window

After exiting the Multiple Camera Settings window, Click **OK** in all remaining settings windows to save the new multiview. The Multiview will now be visible in the configured camera channel in the Live Viewer.

Multiple Cameras Stitched - Network Camera Type

Note: This camera type will only be available for systems with an interfaced capture card.

Designed for use with video analytics on DRX systems, the *Multiple Cameras Stitched*option is used to configure multiple analog video feeds as one video image. This is used to piece together camera images directly beside one another into one large image.
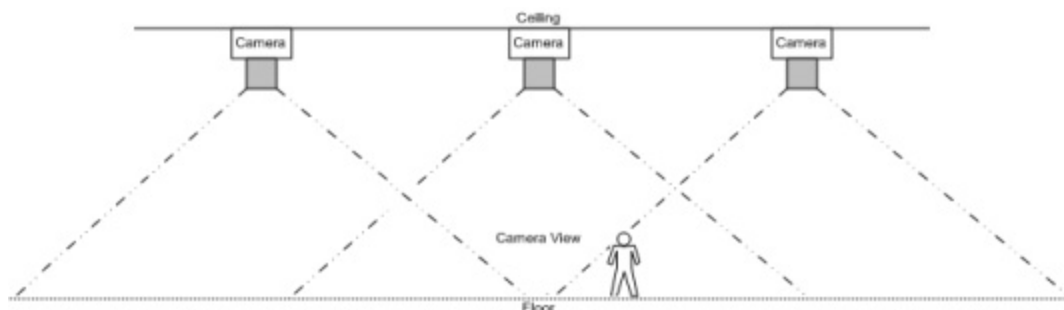
Figure 4-23: Stitched Images - Camera Overlap Example

There must be the correct amount of overlap between the images to prevent fluctuation of the person size as a person moved between images.
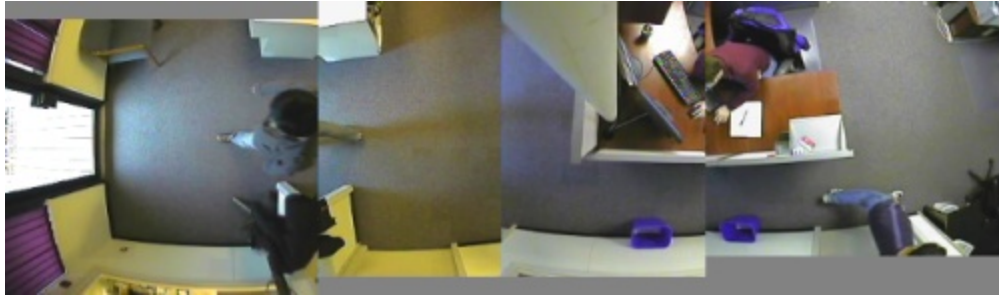
Figure 4-24: Stitched Image Example

VIGIL Server - Network Camera Type

Another VIGIL Server can be connected in the same way you would connect to a *Network Camera*. This will display any camera that the VIGIL Server receives and allows you to relay analog video from one recording VIGIL Server with a capture card installed to another (with or without a capture card).
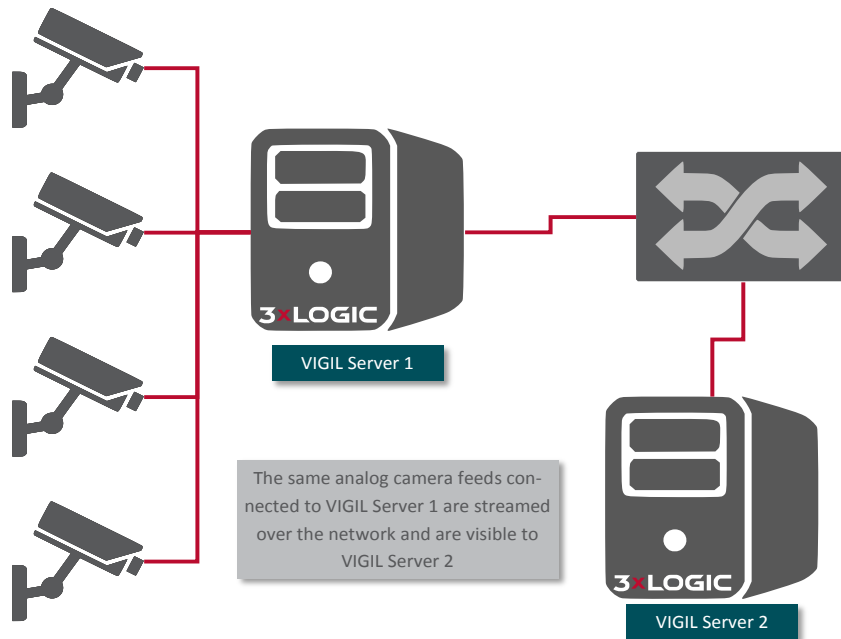
Figure 4-25: Selecting VIGIL Server as Network Camera Type - Analog Camera Relay

To set up this configuration, select the **VIGIL Server** type in the *Network Camera >Stream tab'*s **Type** field. The recommended settings for this setup are:

- **Address** - IP Address of the VIGIL Server.
- **Port** - Live Video Port, default 22802.
- **Camera Number** - The camera input number on the remote VIGIL Server to be used.

- **User / Password** - The username and password used to log into the remote VIGIL Server, if applicable.

©2024 3xLOGIC Inc. | www.3xlogic.com | (877) 3xLOGIC | helpdesk@3xlogic.com

4.4 Camera Setup Tab - Advanced Settings

At the bottom of the Camera Setup tab are several sub-tabs that makeup the *VSMU Camera Setup Advanced Settings*.

4.4.1 Recording Mode Tab

Figure 4-26: Settings - Camera Setup - Recording Mode Tab

Recording Modes

There are four *Recording Mode* options encompassing a full range of recording possibilities. These modes are accessible by selecting the appropriate option from the *Recording Mode* drop-down menu.

- **Constant** - Always recording, 24 hours, 7 days a week.
  - » When choosing constant, the user will also have the option of enabling *Variable Speed Recording*. Variable speed recording will drop camera FPS to 1 when no motion is detected and will resume full frame rate when motion is present. This settings can be highly beneficial in low-bandwidth environments. Motion settings will also be available for configuration when Variable is enabled.
  - » Check off *Variable* (only visible when Constant is selected as Recording Type) to enable Constant Variable Speed Recording.
- **Schedule** - Records based on a schedule. The easy to use graphical interface provides a full overview of a week's schedule in 15-minute intervals. This mode offers full control over recording times and any combination of constant or motion controlled recording modes.
- **Motion** - Records only when motion is detected. Full configuration over motion area, amount of motion, size of motion and post motion recording time makes this a very versatile recording mode.
- **Alarm Only** - Records in alarm mode when any alarm is detected. The alarms can be of any type including *Video Analytics, Video Motion, Digital Input* and *POS Alarms*.

Scheduled Recording

If *Schedule* is selected from the *Recording Mode* drop-down menu, the *Schedule* window will appear. To edit an existing schedule click the … button to open the *Schedule* window. To modify a schedule, click the appropriate recording mode button (*Const* or *Motion*), and then click-and-drag across a time slot. Areas that are blank (no color) have no recording modes defined for that time and will not record any footage.
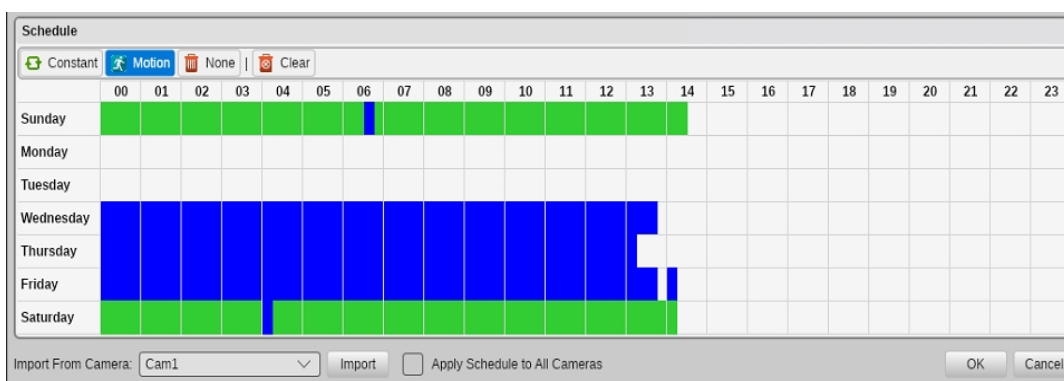
Figure 4-27: Scheduled Recording - Scheduler Window

Note: The smallest time interval that can be used is a 15 minute period.

To view time for a specific point in the schedule, mouse over the desired point in the scheduler. The corresponding day and times of your cursors location are displayed near the top-right corner of the *Schedule* window. Hover the mouse over any part of the section to display the time. See below for descriptions of the remaining scheduling tools.

- **Constant** - Sets to *Constant* recording mode; these time periods are colored green.

- **Motion -** Sets to *Motion* recording mode; these time periods are colored blue.

  - » **Change Record Mode** - Click the desired recording type and drag over an existing section of schedule to overwrite it.

- **Import from Camera** - Select the camera from the *Import From Camera* drop-down menu, and then click *Import*. This will overwrite the current schedule.

- **None / Erase** - Select the *None* recording type then click and drag where desired to erase existing recording mode schedules.

- **Clear** - Click the *Clear* button to delete the entire schedule.

- **Apply Schedule To All Cameras** - When marked, this checkbox will apply the created schedule to all cameras that have been set to *Schedule* recording mode.

Motion Recording Settings

When recording in Motion mode or if looking to configure Video Motion Alarm Motion Settings, click the *Motion Settings…* button to access the *Motion Settings* window. Here you configure which regions of the video image are to be used for motion detection. To do this, simply draw on the video. A semi-transparent overlay will be drawn over the video; this marks the motion detection region. To clear a motion detection region, click and draw on it.

3xLOGIC
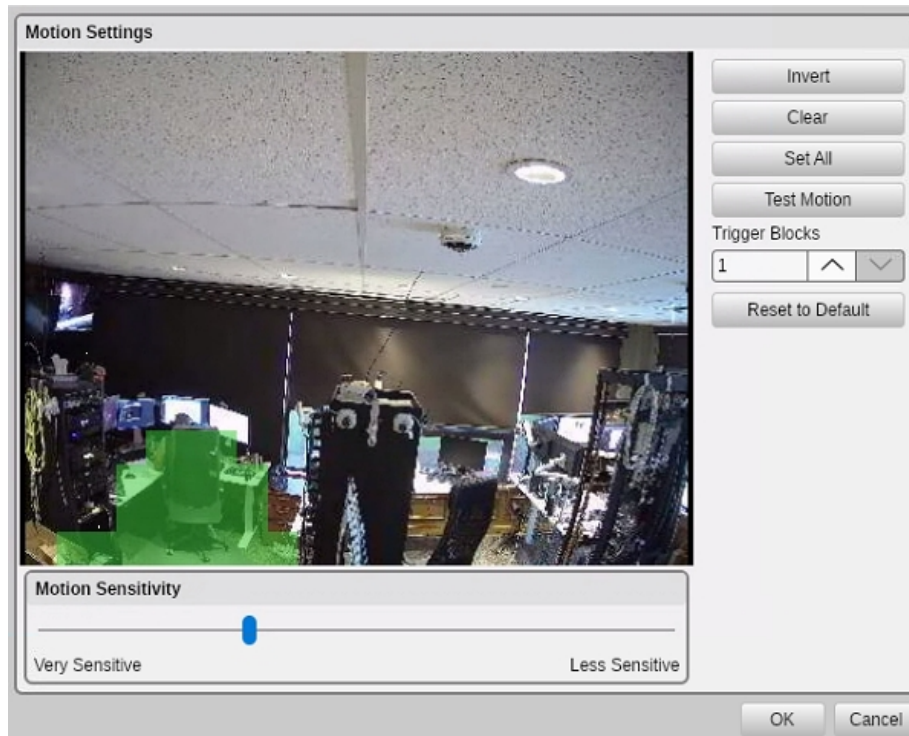
Figure 4-28: Motion Recording Settings Window

- **Invert** - Swaps masked and clear regions.
- **Clear** - Clears all masked regions.
- **Set All** - Masks the entire image.
- **Test Motion** - When latched on, the preview window will display motion detection blocks and their real-time motion values overlaid on masked regions of the video. When motion is detected based on the sensitivity, values are highlighted in green.

Figure 4-29: Test Motion

- **Trigger Blocks** - Determines how many motion blocks must meet the motion sensitivity requirement to trigger motion recording.
- **Motion Sensitivity** - Adjust the Motion Sensitivity slider to control the amount of motion required to trigger recording. Use a very sensitive setting to detect almost all motion, or a less sensitive setting to require only very large movements to trigger recording.

Click **Reset to Default** to return all settings to default state. Click **OK** to save new settings. Click **Cancel** to close the form without saving.

Video Motion Alarm - Motion Settings

The *Video Motion Alarm* settings allow you to configure powerful motion detection alerts that include full control over motion quantity, size, area, speed and direction of motion. In addition to the alarm itself, a wide variety of alarm notification settings are available. *Video Motion Alarms* can be used in conjunction with any other recording mode.

> **Note:**When *Video Motion Alarm* is enabled and a motion alarm is detected, the VIGIL Server will record in alarm mode regardless of any other recording mode defined, and an alarm event will be triggered.

Click the *Motion Settings* button to launch the *Motion Settings* window. See "Motion Recording Set-tings" on page 28 for more information on Motion Recording Settings. The below tools will also be available in the Motion Recording Settings when video motion alarm is enabled:

Motion Vector Draw Region Set Vector Clear Motion Timeout `1` ∧ ∨ s	A motion vector is composed of two or more motion detection regions and one vector. It represents an object moving through specific areas of the image in a set direction. If motion is detected in two of the regions in the general direction indicated by the vector arrow, the *Motion Alarm* will be triggered.

■ **Draw Region** - Draws a motion detection region as an alternative to using the mouse and drawing by hand. You cannot draw on a motion detection region to create a clear region.

> **Note:**Regions with sides that are touching or overlapped are detected as one region. To use a motion vector, you must have at least 2 motion regions that do not border each other.

■ **Set Vector** - Specify a direction of movement that will trigger a motion alarm; draw a direction by clicking and dragging the mouse. An arrow will be drawn on the preview window.

Figure 4-30: Example of Motion Vector

3xLOGIC

- **Clear** - Remove the applied motion vector.
- **Motion Timeout** - Determines the speed required to trigger the alarm. Motion must be detected in two or more of the regions in the desired direction within this time. If the object moves so slowly that it does not move from one region to the next within the Motion Timeout period, then a motion alarm will not be triggered.

Video Motion Alarm Advanced Settings

The advanced settings include scheduling when the alarm is active, *Output Relay Options,* and *Notification Settings.*

General Tab

Video Motion Alarm Schedule

Click the checkbox to enable a schedule for when the *Video Motion Alarm* will be active. Click **...** to configure the schedule.

Click-and-drag to set when the *Video Motion Alarm* is active, marked in green. The schedule functions the same as in *Recording Mode Tab – Scheduled Recording* but applies only to video motion alarm (no constant recording mode).
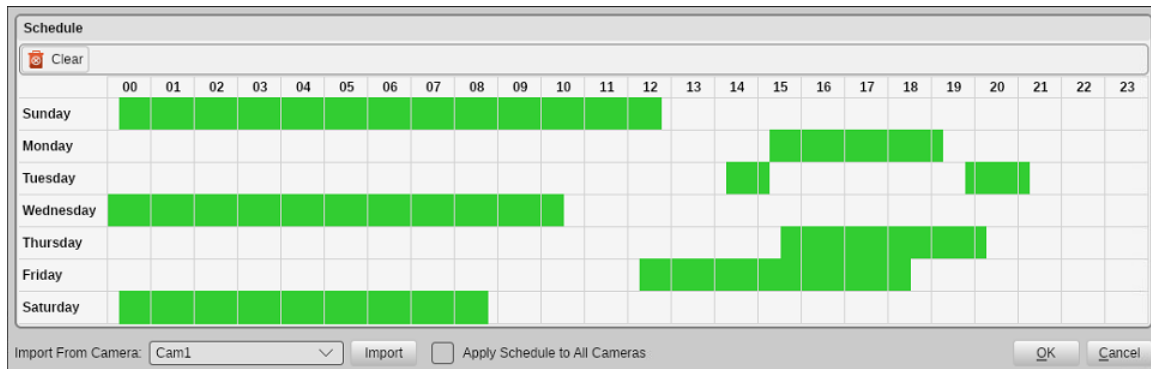
Figure 4-31:VA Alarm Schedule - Scheduler

Output Relay

Select an *Output Relay* to be triggered from the drop down box. The trigger options are *Latched* (for the duration of the alarm), or *Momentary* (2 seconds, regardless of alarm duration).
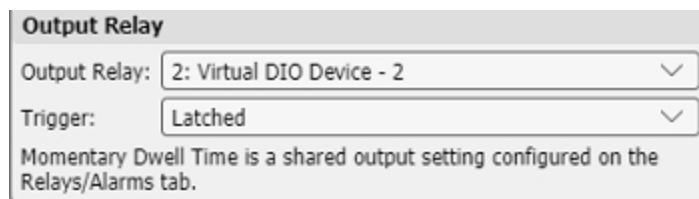
Figure 4-32: Output Relay Configuration

Post Motion Record

Post motion recording time for *Video Motion Alarms* is set here and is independent of any other post motion recording settings. The default is 3 seconds.
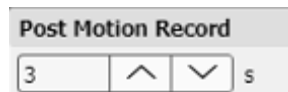
Figure 4-33: Post Motion Record Settings

Local Alarm

This setting will cause the alarm to only be visible on the VIGIL Server and not be relayed to other VIGIL products.
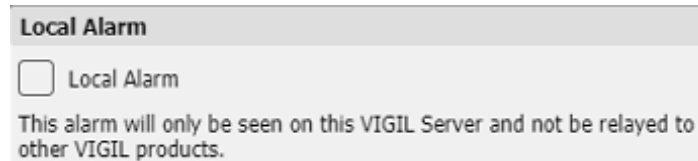
Figure 4-34: Enable Local Alarm Only Mode

Linked Camera

Select other cameras that will also record when the video motion alarm is triggered on the current camera.
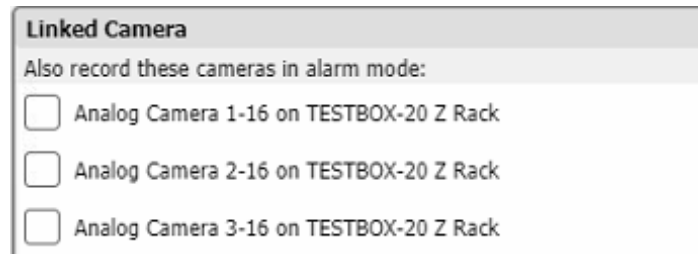
Figure 4-35: Linked Cameras

3xLOGIC

Notifications Tab

Local Notification Settings

Figure 4-36: Local Notification Settings

- ■ **Monitor Output** - Select an analog output monitor to display the triggered camera at the time of the motion alarm.
- ■ **Audio Notification Settings** - Enables audio notification when a motion alarm is triggered. Two audio notification types are available:
  - » **System Beep** - Sounds a system beep.
  - » **Wave File**– Plays a WAV audio file.
- ■ **Auto Acknowledge** - Enables the automatic acknowledge for *Motion Alarm* notifications after the specified number of seconds.

Email Notification Settings

Figure 4-37: Email Notification Settings

When this feature is enabled, an email is sent to all recipients informing them that a motion alarm has been triggered.

- To configure timed suppression for email notifications, enable *Minimum time between email*s and configure a time suppression duration. This will prevent notification recipients from receiving multiple notifications from the same DIO event.

- Click the *Enabled* check box to enable *Email Notification*s and click the ... button to open the *Email Settings* window. *Email Header Option*s are described below:

Email Header Options

From (Name): TESTBOX-20-HV   From (Address): vigilserver@127.0.0.1

Subject: Motion Alarmed

Email Body: Motion alarm was triggered on a camera.

Alarm Type: Motion Alarms
Camera: 1 - Cam1
Site Name: VIGIL Server

☐ Attach Still Shot

☐ Attach Pre-Alarm Video

Pre-Alarm Time: 5 ⌃ ⌄ seconds

Figure 4-38: Email Header Options

Form Field	Description
From (Name)	The name of the entity that will be sending the emails.
From (Address) -	The email address of the entity that will be sending the emails.
Subject -	The text that will be the subject line of the emails.
Email Body -	The text that will be included in the body of the emails.
Attach Still Shot -	Allows a still image from that camera to be attached to the outgoing email. The image is always from the beginning of the motion alarm event.
Attach Pre-Alarm Video	Attach pre-alarm footage to the email notification. Use the available *Pre-Alarm Time* drop-down to configure the amount of pre-alarm footage (in seconds) to attach.
Recipients	These are the lists of recipients who will receive *Motion Alarm* notifications. There are three lists of recipients, direct recipients, carbon copied recipients and blind carbon copied recipients. Recipients can be added, deleted and edited. **To** CC BCC **To** ➕ Add ✏️ Edit 🗑 Delete Address ☑ test@testaddress.com **Figure 4-39:**Email Notification Recipients Configuration Window

Heatmap

Generate Heatmap

☐ Generate Heatmap

Figure 4-40: Settings - Camera Setup - Generate Heatmap

3xLOGIC

A Camera Image *Heatmap* is essentially a graphical overlay used to represent high-activity (motion) areas of a camera's image.
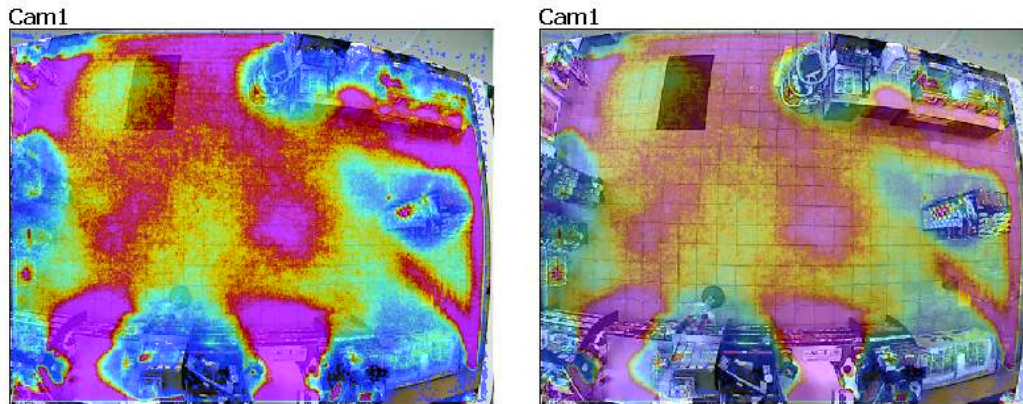

Figure 4-41: Heatmap Examples

■ To enable Heatmap generation for a camera, check-off *Generate Heatmap.* Checking this option enables data collection for use with the heat map functionality. No further camera configuration is required for heatmap use.

» Heatmaps are generally used in conjunction with the VIGIL Trends Analytics Reporting Platform and can be reviewed by logging into your VIGIL Trends account.

» Heatmaps can also be reviewed by retrieving them from the VIGIL Server directly using VIGIL Server HTTP commands. For instructions on accessing heat maps using this method, please reference document *120003 VIGIL Server HTTP Commands Reference Guide*. Contact a 3xLOGIC support representative to receive the latest available version of this document.

4.4.2 Camera Control Tab

Some PTZ cameras can be operated remotely by VIGIL Server. To configure a camera for remote control, click on the *Camera Control* tab. Select the camera type, the *COM* port and the address. These settings are determined by the camera itself and the *COM* port on your VIGIL Server that the camera is connected to. For IP *Network Cameras* , simply select the *Camera Type*. Other custom settings such as the *Digital Presets* button, login prompts or camera labels may appear depending on the selected camera type.
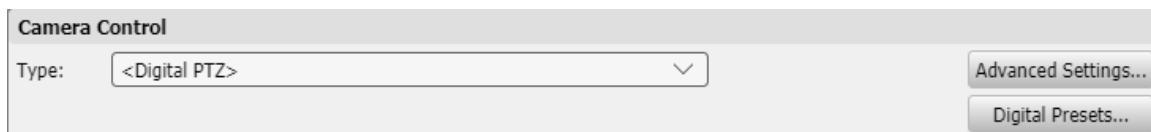
Figure 4-42: Settings - Camera Setup Tab - Camera Control Tab

■ **Type** - The type of PTZ camera that is connected to your VIGIL Server. If *Digital PTZ* is the selected camera type, the *Digital Presets* button will appear. See "Digital Presets" on page 38

■ **COM Port** - The COM port on the VIGIL Server that the PTZ camera is connected to. If a message titled *CONFLICT* appears below the camera type drop-down menu, then there is another camera or data connection that is set up to use that COM port or Address. Determine which device is connected to the COM port and Address, and then modify the camera settings

appropriately.

- **Address** - The address of the camera when multiple cameras are attached via the COM port. See your camera's user guide for details

Camera Control Advanced Settings

Auto Restart PTZ

Automatically runs a *Pattern*, *Preset,* or *Tour* after the camera has been manually controlled by a user, after a *DIO Alarm Event* has ended, or when a *Video Analytics Alarm* is triggered.

Figure 4-43: Auto Restart PTZ Settings

- **Mode** - Select which action to apply after the timeout has been reached: *Patterns*, *Presets* or *Tours*.
- **Timeout** - The number of minutes after the camera control ends before the automatic restart is activated.
- **Name / Number** -Enter the name or number of the pattern, preset, or tour to run after the timeout period has elapsed.

DIO Alarm PTZ Event

DIO Alarms can be used to trigger PTZ events. The *DIO Alarm* must be enabled and assigned to the Camera, See *Settings – Relays / Alarms Tab* for details. Multiple *DIO Alarms* can be assigned to one camera, click the checkbox beside the *Alarm Name* to enable it.

Figure 4-44: DIO Alarm PTZ Events

Video Analytics Alarm PTZ Events

Video Analytics Alarms can also be used to Trigger PTZ events. Multiple *Video Analytics Alarms* can be assigned to one camera. All *Video Analytics Rules* configured on the Server will show in the list, click the checkbox beside the *Rule Name* to enable it.

Clicking the checkbox will open the *PTZ Configuration* window.

Figure 4-45: Video Analytics Alarm PTZ Events

Motion Alarm Event

Motion Alarm Events can also be used to trigger PTZ events. A Video Motion alarm must be enabled and assigned to the Camera. See "Video Motion Alarm - Motion Settings" on page 30 for more

---

3xLOGIC

information. Multiple alarm events can be assigned to one camera, click the checkbox beside the *Alarm Name* to enable it.

Motion Alarm Event						
Camera Name	Mode	Preset	Mode After Alarm	Preset After Alarm	Dwell Time	
☐ 1: Analog Camera 1-16 on TESTBOX-20 Z Rack	Disabled		Disabled		0	
☐ 2: Front Parking #1	Disabled		Disabled		0	
☐ 3: 3xLogic front door - Hallway	Disabled		Disabled		0	

Figure 4-46: Motion Alarm PTZ Events

During Alarm

When an alarm is enabled, the user can select what action to apply during the DIO Alarm.

Figure 4-47: During Alarm Settings

- ■ **Mode** - Select *Patterns, Presets* or *Tours* from the drop-down box.
- ■ **Name / Number** - Enter the *Name* or *Number* of the *Pattern, Preset* or *Tour*.

After Alarm

Figure 4-48: After Alarm Settings

When an alarm is enabled, the user can select what action to apply after the *DIO Alarm* has ended. To do nothing after the alarm, select *Disabled* from the mode drop-down.

- ■ **Mode** - Select *Disabled, Patterns, Presets* or *Tours* from the drop-down box.
- ■ **Name / Number** - Enter the Name or Number of the *Pattern, Preset* or *Tour*.
- ■ **Dwell Time** - The amount of time from when the DIO Alarm is triggered until the *After Alarm* event occurs. If *Dwell Time* is not checked the *After Alarm* event will trigger when the DIO Alarm ends.

Control Interface

Control Interface ☐ Push Button Controls	Enables the *Push Button Directional* controls for the camera in place of the virtual joystick.
☑ Region Control	*Region Control* is a setting that is only accessible on certain PTZ camera models. It is an alternative to the traditional push button, joystick or on-screen drag method for controlling *PTZ* movement. *Region Control* enables you to simply click on-screen to shift the cameras line-of-sight toward the region that has been clicked.

Digital Presets

When *Digital PTZ* is the selected camera control*Type*, the *Digital Presets* button will become available.
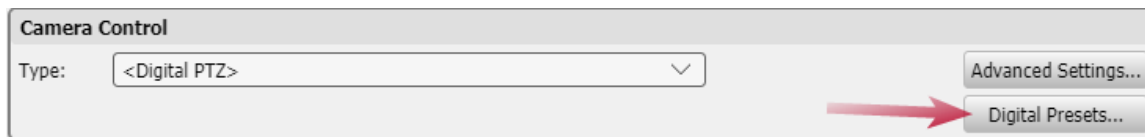
Figure 4-49: Settings - Camera Setup - Camera Control Tab - Launching a Camera's Digital Preset Settings

A Digital PTZ Preset is a saved portion of a camera's full image, where the original camera image has been manipulated by a user using digital PTZ commands to focus on a specific area-of-interest. Once saved. this manipulated version of the image can than be instantly opened as a camera digital preset in VIGIL Client. Digital Presets can also be configured in VIGIL Server as a POS Priority Camera. Multiple digital presets can be created for a single camera.

To configure and save a digital preset(s), click the *Digital Presets* button to launch the selected camera's *Digital Preset Configuration* window (pictured below).
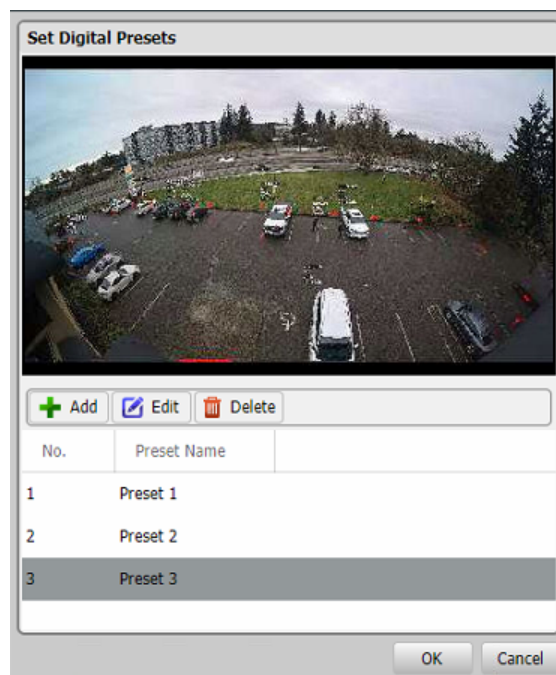
Figure 4-50: Settings - Camera Setup - Camera Control Tab - Digital Preset Configuration

The controls located on the window are described below:

- ■ **Add** - Add a digital preset. A window will deploy where the user can enter a name for the preset.
- ■ **Edit** - Edit the selected preset. Both preset positioning and preset name can be edited.
- ■ **Delete** - Delete the selected preset.

Adding / Editing a Digital Preset

To add a new preset:

3xLOGIC

1. Click the **Add** button. The *Add Preset* window will deploy.
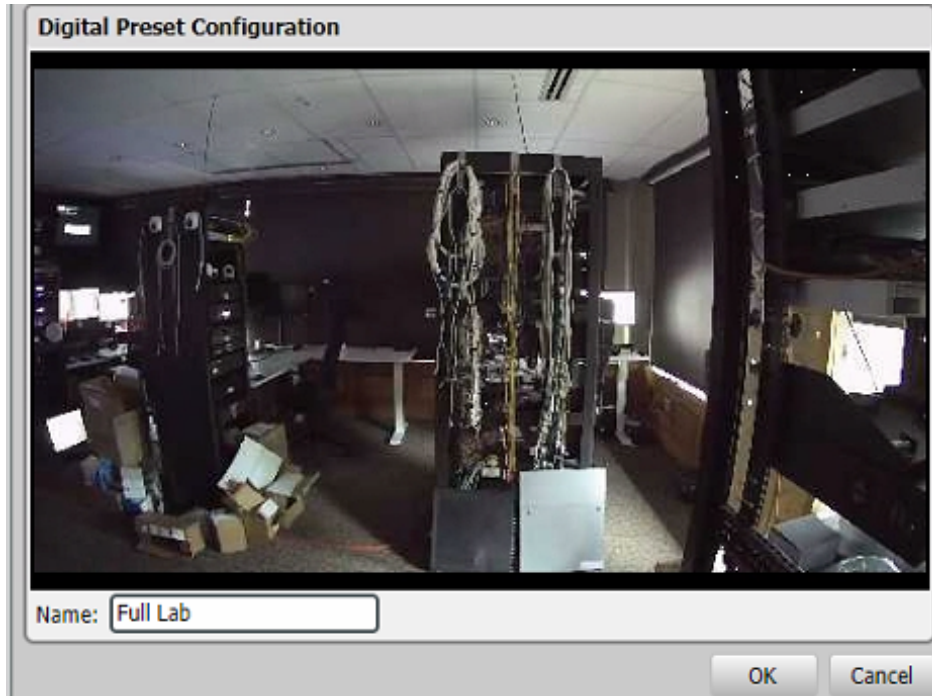
Figure 4-51: Settings - Camera Setup - Camera Control Tab - Adding / Editing a Digital Preset

1. **Name** the preset.
2. Manipulate the image as required. Use mouse wheel to zoom in / out of the image and click and drag to pan around the image when zoomed.
3. Click **OK** to save the preset.

Repeat the above process to add multiple presets.

To edit an existing preset:

1. Select the preset from the list. Click **Edit**. The *Edit Preset* window will deploy.
2. Manipulate the image as desired using standard Digital PTZ Controls. Click **OK** to save the preset.

When you have finished configuring presets, click the *OK* button to exit the *Digital Preset Configuration* window.

Viewing a Digital Preset

Aside from the configuration process on VIGIL Server, Digital Presets can only be accessed using a VIGIL Client that has been interfaced with the VIGIL Server. A user can interact with saved digital presets in VIGIL Client in the same manner as a camera; Digital Presets maintain both live and playback functionality. Please reference the VIGIL Client User Guide for more information.

Digital Presets can also be configured as a POS/ATM Priority Camera. See "Priority Camera Settings " on page 84

4.4.3 Video Loss Tab

If the video signal is lost from an enabled camera, you can specify an action to take in the *Video Loss* tab.

Figure 4-52: Settings - Camera Setup Tab - Video Loss Tab

Video Loss Mode

- **Active Signal Detection** - Enables hardware signal loss detection if the VIGIL Server capture card supports this feature. This option will only be visible on applicable systems.
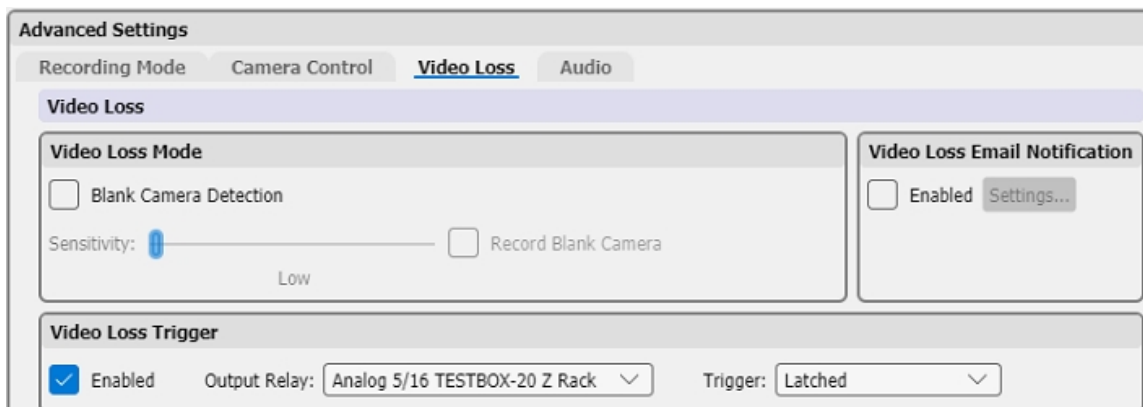
- **Sensitivity** - Adjusts the *Sensitivity* of the software signal loss detection.

- **Blank Camera Detection** - When enabled, the software detects a signal loss when the live video is all black or white. This is useful if the camera is covered or blocked, and can be used in addition to or in place of hardware signal loss detection.

- **Record Blank Camera** - When enabled, the VIGIL Server continues recording the camera feed during a signal loss. The Recording Mode for the camera must be set to *Constant* for this feature to work.

Video Loss Trigger

When enabled, *Video Loss Detection* triggers a DIO Relay.

- **Output Relay** - Select the DIO Relay.

- **Trigger** - Select the type of trigger for the DIO Relay: *Momentary*, which lasts two seconds or *Latched*, which lasts until the video is recovered.

Video Loss Email Notification

When enabled, an e-mail will be sent to the recipients configured in *Email Settings...* For details on how to set up e-mail recipients, see Video Motion Alarm Advanced Settings – Email Notification Settings.

4.4.4 Camera Setup – Advanced – Video Analytics Tab

From *Camera Setup > Video Analytics* tab, a user can view and edit an applicable camera's video analytics rules which have been synchronized with VIGIL Server via the embedded On-Board Analytics utility. See "On-Board Analytics" on page 102 for more information on this process.

3xLOGIC

Note: VIGIL Server offers support for VCA video analytics from analytic-capable cameras. VCA Video analytics rules are configured either from VSMU's Network Camera Settings (as of VIGIL 13) or, alternatively, directly on camera and are then synchronized with VIGIL Server via an embedded on-board analytics tool (formerly VIGIL Analytics Bridge). Contact your 3xLOGIC representative for more information.

Note: If you have updated a pre-v9 copy of VIGIL Server to v9 or newer, advanced calibration and rules settings may be configurable for rules configured on the host VIGIL Video analytics (no longer supported). Please refer to VIGIL Server 8.5 User Guide or older for configuration confirmation regarding VIGIL Video Analytics.
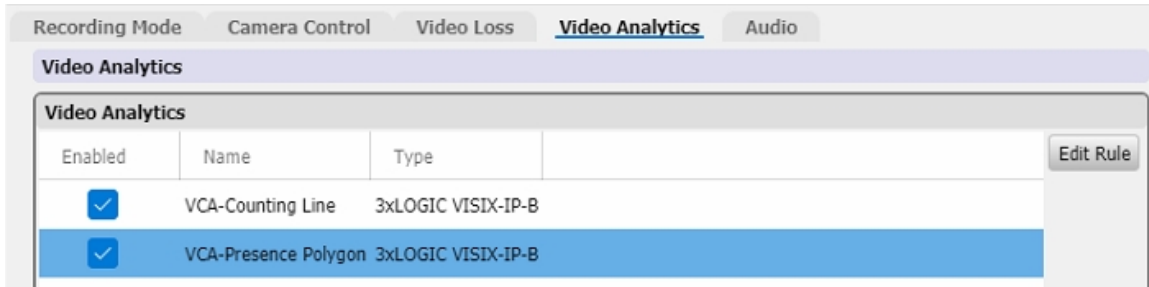
Figure 4-53: Settings - Video Analytics Tab

- **Edit Rule** - Opens the *Rule Settings* window for the selected rule.

To enable a rule, mark the check-box under the enabled column for the desired rule. Rule data will now be recorded by VIGIL Server. To edit a rule, select a rule from the list and click *Edit.* .

Editing an Analytics Rule

After selecting a rule and choosing *Edit Rule,* the *Rule Settings* window will deploy. The Rule Settings window consists of 3 tabs. *General, Alert Settings* and *Rule Settings.* As most analytics settings are configured on the camera itself, minimal settings can be edited from VIGIL Servers.

General

Figure 4-54: Video Analytics - Rules Settings - General Tab

■ From the General Settings window, a user may re-name the rule, select a *Display Option* (*Never Show Rule, Always Show Rule, Show Rule when Alarmed*) for on-screen rule information and enter a description for the rule.

Alert Settings
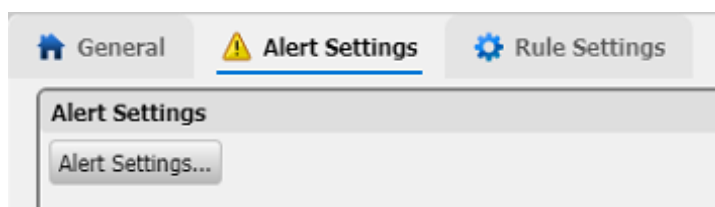
Figure 4-55: Video Analytics - Rules Settings - Alert Settings Tab

■ Clicking this tab reveals an Alert Settings button which opens the *Video Analytics Alert Settings* window which allows a user to schedule the alarm recording period an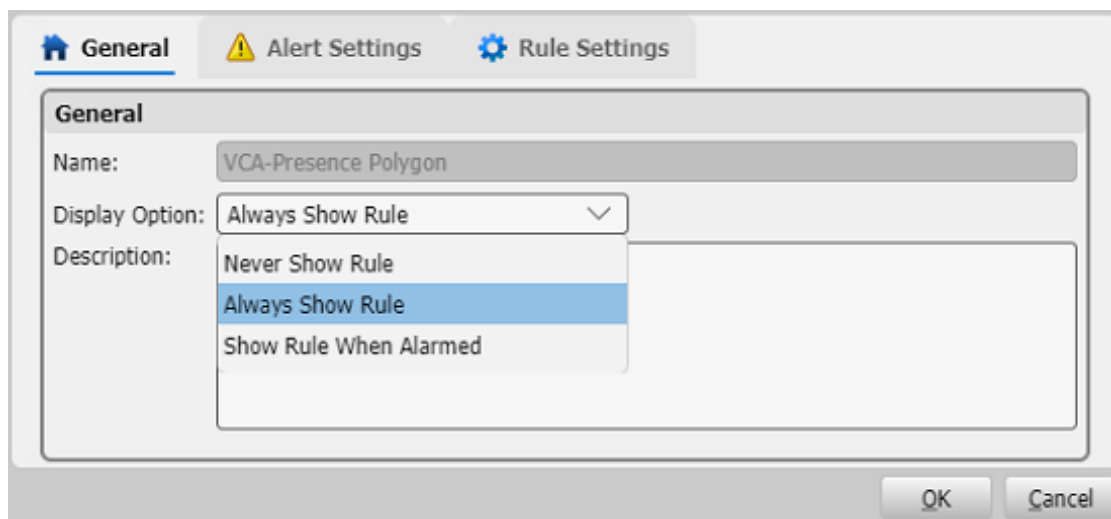d configure alerts / notifications. The *Video Analytics Alert Settings* window is the same as the *Video Motion Alarm Advanced Settings* window.See "Video Motion Alarm Advanced Settings" on page 31 for configuration information.

Rule Settings
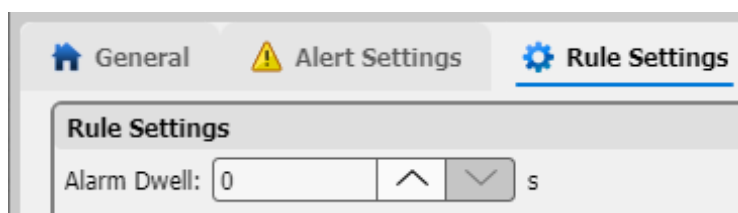
Figure 4-56: Video Analytics - Rules Settings - Rules Settings Tab

■ On the *Rules Settings* tab, a user may set the *Alarm Dwell* time for the selected rule.

> **Warning:** If the embedded VIGIL on-board analytics utility is used to retrieve rule info from a camera and the rules are re-synced with VIGIL Server, any rule changes configured on VIGIL Server will be overwritten with the new settings from the camera.

4.4.5 Advanced Camera Setup – Audio Tab

The *Audio* tab allows you to choose a *Priority Audio* channel and *Audio Talk* device for each camera.
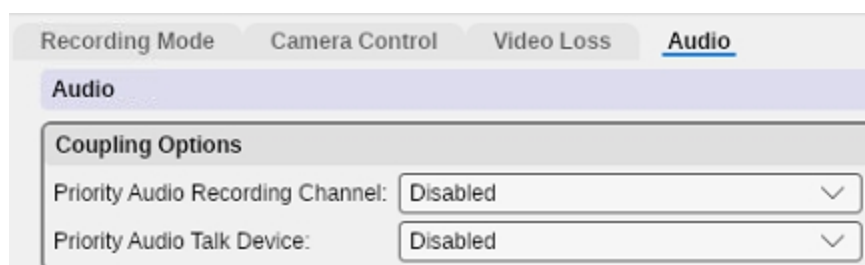
Figure 4-57: Settings - Camera Setup Tab - Audio Tab

3xLOGIC
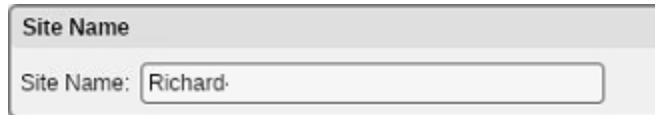
- **Priority Audio Recording Channel** - Select the *Audio Channel* that will be associated with this camera. *Audio Channels* are configured on the *Settings - Audio Tab*. See "VSMU - Audio Tab" on page 91 for more information.

- **Priority Audio Talk Device** - Select the *Audio Talk Device* that will be associated with this camera. *Audio Talk* devices are configured on the *Settings - Audio Tab*. See "VSMU - Audio Tab" on page 91 for more information.

5 VSMU – SERVER SETTINGS TAB

5.1 Server Settings Tab – Basic Settings

The *Server Settings* tab contains settings related to the software and hardware configuration of a VIGIL Server.

5.1.1 Site Name
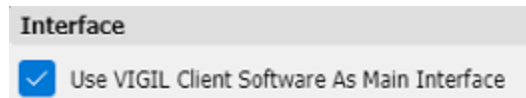
Figure 5-1: Server Settings Tab - Site Name Settings

- **Site Name** - The name of the *Site* where VIGIL Server is located. The site name is included when saving still images.

5.1.2 Interface

Figure 5-2:VIGIL Server Settings Tab- Interface Settings
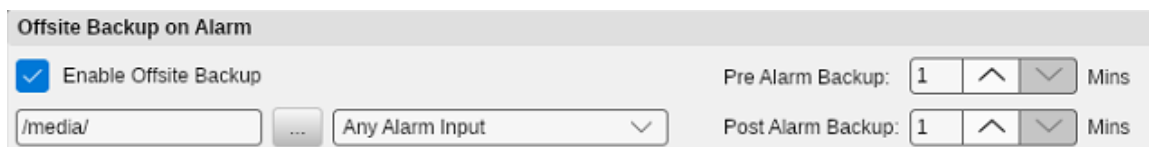
- **Use Client As Main Interface** - Allows the use of VIGIL Client as your VIGIL suite main interface. Many configuration options available in server will now only be accessible through Client. This allows a unified user experience whether using our VIGIL Server system or connecting remotely.

  > **Note:** As of VIGIL 11.60.0000, VIGIL Server has been fully converted to a service and some of the functionality gained in Client by enabling *Client as Main* in previous versions is now available in VIGIL Client by default

5.1.3 Offsite Backup on Alarm

Enable automatic export of footage to the specified off-site location when a DIO alarm occurs.

Figure 5-3: Server Settings Tab - Offsite Backup on Alarm Settings

- **Enable Offsite Backup** - Click the check box to enable this option. Click   …   to a location where the footage will be saved.

- **Alarm Input** - Use the drop-down to select the DIO alarm input that will trigger the off-site backup or select *Any Alarm Input*.

- **Pre / Post Alarm Backup** - Specifies the number of minutes of footage to save prior to and after the *Alarm* event.

5.2 General Tab
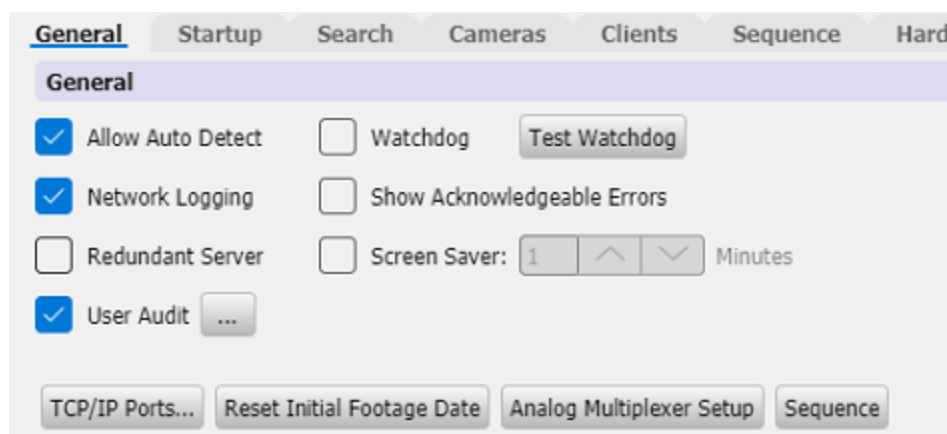
Figure 5-4: Server Settings - General Tab

- **Allow Auto Detect** - Allow VIGIL suite applications with Auto-Detect to see this VIGIL Server when using their auto-detect function.

- **Network Logging** - Logs network activity that can be reviewed in the *Network Log Analyzer*

- **Redundant VIGIL Server** - A redundant VIGIL Server is used for backup recording in case of a VIGIL Server failure. If *Redundant VIGIL Server* is enabled, the Sentinel service will not display an error if there is no footage recorded in 24 hours. Redundant VIGIL Servers are normally used only in systems set up with *VIGIL Server Health Monitor* configured to use a Matrix switch for failover. Please contact 3xLOGIC for more information about this feature.

- **User Audit** - Enable *User Audit.* Click the ... button to launch user audit settings. See "User Audit" on page 47 for more information.

- **Watchdog** - When enabled, the watchdog circuit on the video capture card is used to verify that VIGIL Server is responsive. If the software becomes unresponsive, then the watchdog will reboot the VIGIL Server. You can test that the watchdog circuit is functioning by clicking the *Test Watchdog* button. The VIGIL Server should reboot within a few minutes if the watchdog is functioning correctly. This function only works with Analog Capture Cards that support this feature. This feature is not available on NVRs. .

- **Screen Saver** - Starts the VIGIL screen saver after a set number of minutes of system inactivity have lapsed.

- **Show Acknowledgeable Errors** - When enabled, the *Error Alert* window will display nin VIGIL Client if an error is recorded in the *Audit Log*; this window will display until the error has been acknowledged by a user:

3xLOGIC

Figure 5-5: Error Alert Window

» **Audit Log Analyzer** - Opens the *Audit Log Analyzer* where error alerts can be reviewed for the active VIGIL Server.

» **Acknowledge All** - Acknowledges all error alerts.

» **Remind Me Later** - Closes the *Error Alert* window and opens it again after the set number of minutes.

> **Note:** When the *Show Acknowledgeable Errors* feature is first enabled, the *Error Alert* window may display alerting of past errors that may already be resolved.

■ **TCP/IP Ports** - Allows the configuration of the TCP/IP ports used by VIGIL Server to connect with VIGIL Clients.
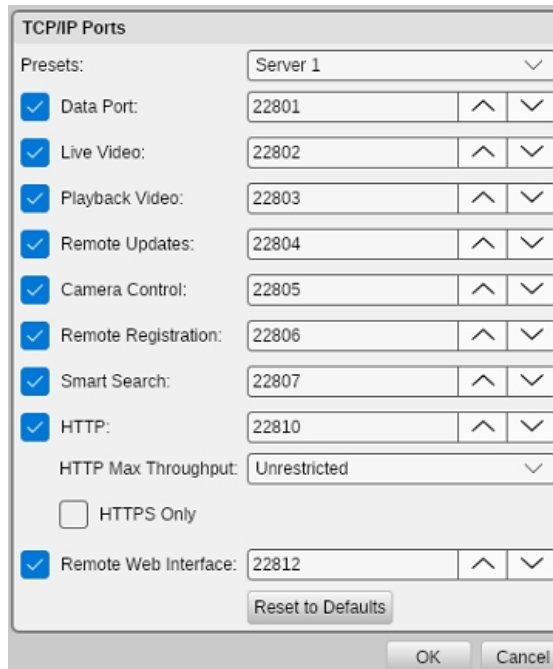
Figure 5-6: TCP/IP Ports Window

» **Presets** - Select a preset from the drop-down menu to change all of the ports to that preset.

» **Change a Port** - Type a port number in the appropriate field.

» **Disable a Port** - Uncheck the appropriate box. If a port is disabled, VIGIL Clients connecting

to the server will be unable to use the feature corresponding to that port.

> **Reset to Defaults** - Resets the ports to the default port numbers.

■ **Reset Initial Footage Date** - The VIGIL Server Health Monitor software uses the initial footage date in VIGIL Server to determine if the VIGIL Server is recording the proper number of days of video storage. Click the *Reset* button to reset the cached date of the first video footage recorded by the VIGIL Server to the oldest footage currently on the VIGIL Server.

■ **Analog Multiplexer Setup** - Opens the Analog Multiplexor Setup window. Use this window to configure the layout of your analog output multiplexor. .

Note: This feature is only available for capture card systems with analog output.

■ **Sequence** - Open up the Sequence selector. Choose a Monitor sequence from the available list. See "Sequence Tab" on page 57 for information on configuring sequences. .

Figure 5-7: Sequence Selector

5.2.1 User Audit

When *User Audit* is enabled, an audit trail of user activity is created based on criteria configured on a per user or group basis.

User Audit Configuration

Enable *User Audit* and click the ... button to open the *User Performance Criteria* window. *Performance Criteria* can be configured on a per user or group basis.

Note: If a user has *Performance Criteria* configured, and is also a member of a group with *Performance Criteria* enabled, the *User Criteria* will be used.

3xLOGIC

Figure 5-8: User Audit - User Performance Criteria Window

- **All Users** - Select *All Users* to configure generalized options for all system users.

- **Individual User** - Select Individual User and choose the User Name from the drop-down box to configure options for a specific user.

- **User Group** - Select *User Group* and choose the *Group Name* from the drop-down box to configure options for a *Group*.

- **Edit** - Edit the selected performance criteria.

- **Idle Time** - Enter the time in *Seconds* that the system will wait before it begins to log the user as idle.

- **Show Monthly Performance Percentage in Performance Meter** - Replace the daily usage performance percentage in the Performance Indicator (located in the Icon toolbar of both VIGIL Server and Client) with the monthly performance percentage.

Performance Criteria

Enable the Report Type (checkbox)to configure the Minimum Value and the Time Span (Daily, Weekly or Monthly):

- **Footage Viewed** - The amount of time spent playing video footage.

- **Frames Viewed** - The number of video frames viewed during playback.

- **POS Query** - The number of POS searches done. A query is counted each time the POS Data button is latched on and the Search button is clicked in the Search window.

- **Searches Done** - The number of searches made. A *Search* is counted each time the *Search* button is clicked in the *Search* window.

- **Time Logged In** - The amount of time logged in to VIGIL Server.

- ■ **Active Time** - The amount of time logged that the user is actively interacting with VIGIL server. This is tracked via cursor activity or other input such as keystrokes.
- ■ **VPOS Events Flagged** - The number of VPOS events the user has flagged.
- ■ **VPOS Events Flagged %** - The percentage of VPOS Events which were flagged by the user the previous day.

Usage Performance Indicator (VIGIL Client)

When a user who is configured for *User Performance Monitoring* logs into the VIGIL Server via VIGIL Client, the *Usage Performance* status bar will is displayed. The user can click the *Details* button to view their performance usage details (See User Performance Report - Sample Report below for an example report).
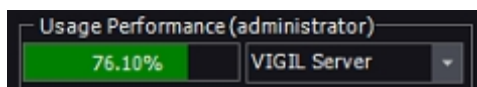
Figure 5-9: User Audit - Main Toolbar Usage Performance Indicator

User Audit Report (VIGIL Client)

To open the User Audit Report tool, select it from a VIGIL Server's tree menu in VIGIL Client. The *User Audit Report* tool provides detailed reports on the report types that are configured.
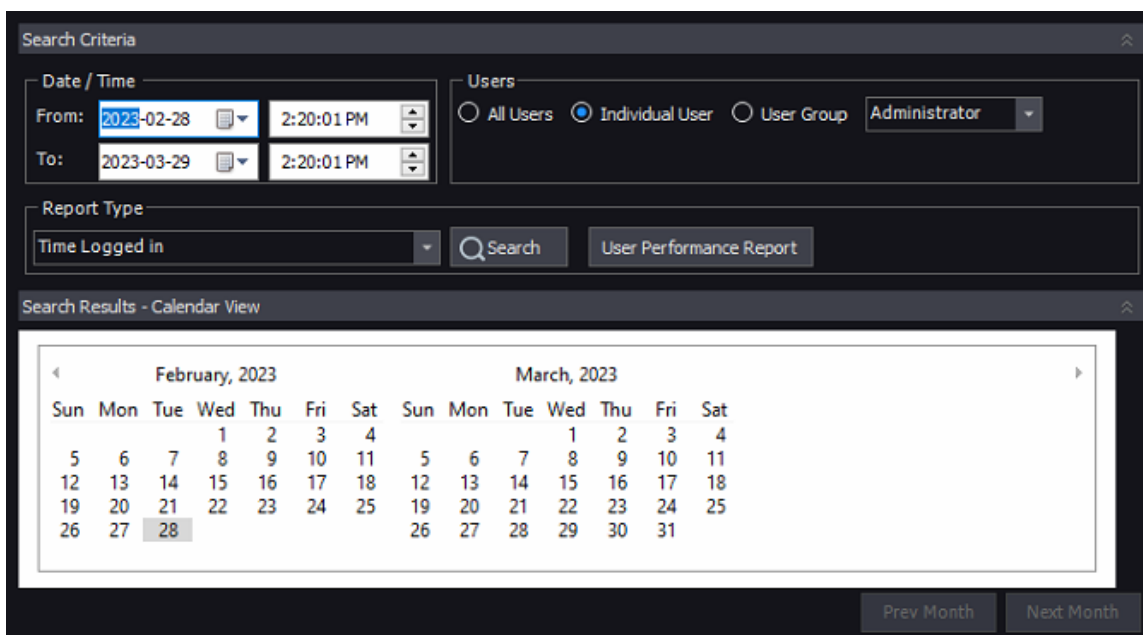
Figure 5-10: User Audit Report - Search Window

Report Types

- ■ **Time Logged In** - Details on login information for each session.
  - » *Idle time* is counted when there is no user input.
  - » *Active time* is counted while the user is actively manipulating the system.

3xLOGIC

- **Footage Viewed** - Details on video playback including the camera number, footage start and end times, number of frames viewed and the total time watched.
- **POS/ATM Query** - Details on the search criteria used for POS queries.
- **Searches Done** - Details on the searches performed including the camera numbers, search times and footage types.
- **User Login Failed** - Details on failed user logins.
- **Shift Analysis Tags Viewed** - Provides details on tags viewed by the user using the shift analysis reporting tool.
- **Daily User Performance** - A detailed report regarding a users daily performance based on configured user performance audit crtieria.
- **All Report Types Summary** - A summary report of the users activity similar to the usage performance details

User Audit Report - Sample Report

Below is an example of a completed *Time Logged In-User Audit* search query.

Figure 5-11: User Audit - VIGIL Client - Sample User Audit Report Search Results

For more information on a user's usage history regarding individual audit entries, double click an entry in the *Search Results* section. A user usage summary report regarding the selected audit entry will open in a separate window.

An example of the usage summary report is pictured below.

User Audit Report - Example Usage Summary Report

Administrator's Usage Summary

Report Generated: *6/20/2013 12:33:09 PM*

User is currently **logged in** since *6/20/2013 10:47:09 AM* with **1h 46m** of total time this session (active time: **29m**, idle time: **1h 17m**).

Total **logged in time** for all sessions this period is **53m**.
Total **active time** for all sessions this period is **13m**.
Total **idle time** for all sessions this period is **40m**.

Usage Item	Value
Footage Viewed	0 Min(s)
Frames Viewed	16898 Frames
POS/ATM Query	2 Queries
Searches Done	1 Searches
Idle Time	40 Min(s)
Time Logged In	53 Min(s)
Active Time	13 Min(s)

Figure 5-12: User Audit - Usage Summary Report - Example

User Performance Report (VIGIL Client)

Figure 5-13: User Audit - VIGIl Client - User Performance Report Configuration

■ **Users** - Under the *Users* section of the form, two settings related to the audited user can be configured:

》 **View Performance For** - Choose the user whose performance statistics will be reported.

》 **Exclusion Dates** - When clicked, this button will open an *Exclusion Dates* window where dates that need to be excluded from the performance reported can be chosen.

3xLOGIC

- **Timespan** - Select the amount of days to audit by selecting a *Check for Last x Days* value and an appropriate *Prior To* date. In the above example, the 28 days leading up the 5/1/2015 will be audited for user performance.

- **Performance Criteria** - Under *Performance Critieria*, the following user performance settings can be configured:

  - » **Active Time Per Day** - Set the amount of acceptable active daily usage.

  - » **Acceptable Performance** - Set the acceptable performance percentage(the user will pass or fail the Performance Report based on this percentage.)

Click **Calculate** to generate a *User Performance* report.

User Performance Report - Sample Report

User Performance Report

Report Generated: *4/19/2015 10:32:14 AM*

Date Range:	**3/22/2015 to 4/18/2015**
Site Name:	**Demo Test**
Employee:	**Administrator**

Performance Criteria

Footage Viewed:	**60 Min(s) Daily**
Frames Viewed:	**3000 Frames Daily**
POS/ATM Query:	**5 Queries Daily**
Daily Performance:	**100%**

Performance Summary

Total Days:	**28**
Excluded Days:	**0**
Days with at least 100%:	**26**
Days with less than 100%:	**2**

Overall Performance: 0.00%

Details

Date	Status	Footage Viewed (Min(s))	Frames Viewed (Frames)	POS/ATM Query (Queries)
3/22/2015	100%	113.00	4168	7
3/23/2015	95%	52.13	2616	5

Figure 5-14: User Audit - User Performance Report

The User Performance Report contains detailed report info(date, site, audited user), the required performance criteria aluminium values, and the user's performance summary. The user will be awarded an Overall Performance percentage which is then followed by a list of all audit data entries.

5.3 Startup Tab

The *Startup* tab allows configuration of VIGIL Server's startup behavior, as well as scheduling of system reboots.
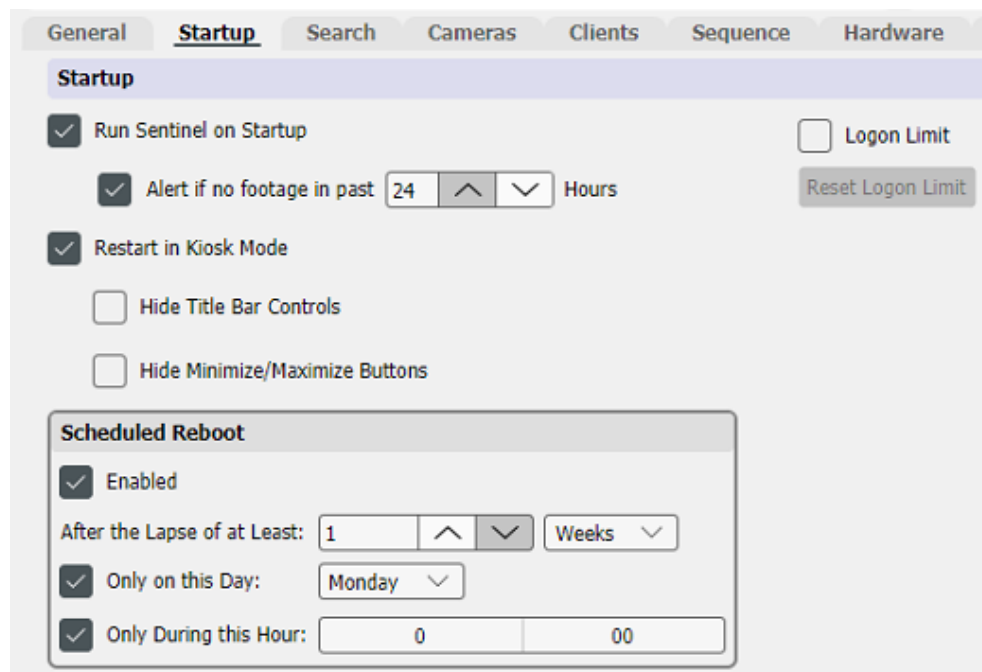
Figure 5-15: Server Settings - Startup Tab

- **Run Sentinel on Startup** - When enabled, the *Sentinel* program will run as soon as VIGIL Server launches. The *Sentinel* program monitors critical VIGIL Server functions and warns the user in event of failure.

- **Alert if no footage in past ... hour(s)** - Displays an alert if VIGIL Server detects that there is no footage recorded in the amount of time set in the drop-down menu. Choose any hour increment between 1 and 24.

- **Restart in Kiosk Mode** - When enabled, VIGIL Server will restart in *Kiosk* mode. *Kiosk* mode hides the Windows shell program so that the Windows desktop, taskbar, Start button and other Windows shell features are not available. .

  - » **Hide Title Bar Controls** - When running *Client as Main Interface* mode, enabling this option will hide the Windows title bar controls (Close, Minimize, Maximize). .

  - » **Hide Client Minimize / Maximize Button** - When running *Client as Main Interface* in *Kiosk Mode*, this option will disable the Client maximize and minimize buttons to avoid lower-tier users from pulling the Client out of full-screen mode. .

- **Scheduled Reboot** - When enabled, the VIGIL Server will automatically reboot after the specified amount of time has lapsed but only during the day and time indicated.

- **Logon Limit** - When enabled, User accounts are restricted to 3 logon attempts. If 3 incorrect attempts are made, the account will be locked out for a period of one hour. A user with administrative rights can reset the lockouts with the *Reset Logon Limit* button.

3xLOGIC

5.4 Search Tab

The *Search* tab defines search parameter and settings for the VIGIL Server. Searches are performed via VIGIL Client.
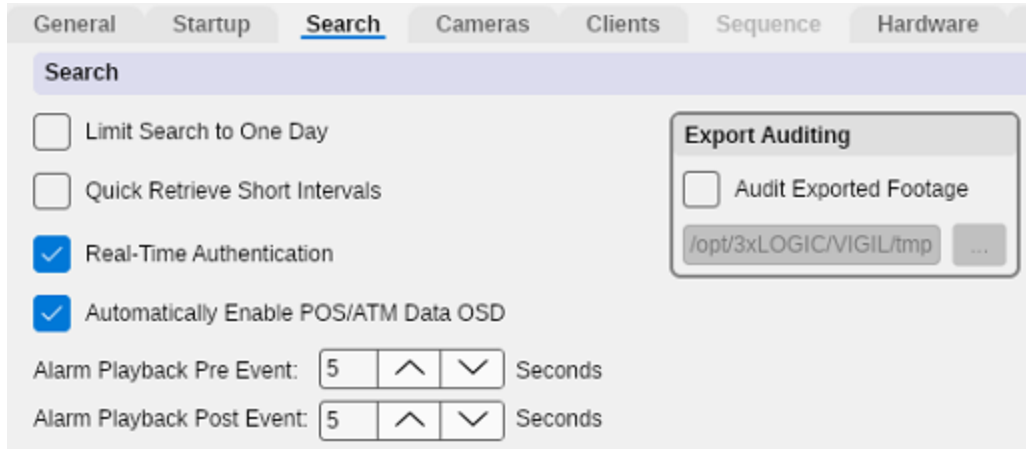
Figure 5-16: Settings - Server Settings Tab - Search Tab

- **Limit Search To One Day** - When enabled, the VIGIL Client *Search* window will be limited to performing searches for a single day only for this VIGIL Server.

- **Quick Retrieve Short Intervals** - When enabled, the *Quick Retrieve* drop-down menu in the VIGIL Client *Search* window offers a selection of short intervals of 15 and 30 minutes in addition to the standard choices.

- **Real-Time Authentication** - When enabled, video footage is checked for authenticity while played back from the VIGIL Client*Search* window.

- **Automatically Enable POS/ATM OSD** - When enabled, *POS/ATM Data On Screen Display (OSD)* will be automatically enabled in VIGIL Client when playing back a camera that is set as a Priority POS/ATM Data Camera on the VIGIL Server.

- **Alarm Playback Pre / Post Event** - Set the amount of time to playback prior to / after an *Alarm* when playing *Alarm* footage in VIGIL Client's *Server Alarms* window.

- **Export Auditing** - Enables mandatory auditing of all video exports. Choose the path where the audit text files will be saved.

5.5 Cameras Tab

The *Cameras* tab specifies the type of cameras being recorded and the scheduling of still shots.
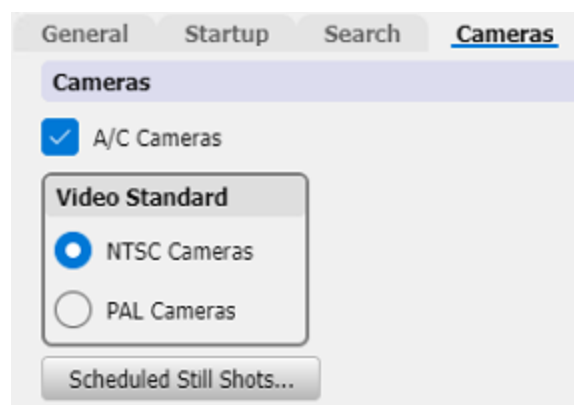
Figure 5-17: Settings - Server Settings Tab - Cameras Tab

- **A/C Cameras** - Enable *A/C Cameras* to set VIGIL Server to record footage from A/C powered cameras. Disable it to record footage from D/C powered cameras.

- **NTSC / PAL Cameras** - Select the appropriate broadcast standard for your cameras: NTSC or PAL. Choosing the wrong video standard will result in poor video quality.

- **Configure OSD...** - On systems containing a capture card, configure the display of the *On-Screen Display Font settings, Camera Name* and *Date / Time* information on the camera live view.

> ⚠️ **Warning:** This will only enable OSD for the capture card.

- **Scheduled Still Shots** - Open the Schedule Still Shots dialogue. See "Schedule Camera Still Shots" below for more information.

5.5.1 Schedule Camera Still Shots

To schedule camera still shots:

1. Click the **Schedule Still Shots** button on the *Server Settings Tab> Cameras Tab*. The *Schedule Still Shots* dialogue will deploy.

3xLOGIC

Figure 5-18: Schedule Still Shots

2. Select the cameras you want to schedule still shots from in the available list. Click the **Select All** button to select all available cameras. To clear the current selection, click **Select None**.

3. Set an **Image Size** from the drop down.

4. Use the settings under the *Schedule* section to configure the schedule as desired.

   ■ If an email with still images attached is desired whenever the schedule runs, enable **Email Still Shots** and click the **...** button to launch email settings. Scheduled Still Shot Email settings are configured using the same process as other email notification settings in VIGIL Server. See "Email Notification Settings" on page 33 for more information on this process.

   ■ If desired, click **FTP Still Shots** to enable an FTP export destination for the stills. Click the ... button to deploy the destination configuration window. Configure FTP settings and click **OK** to save the destination. Stills will be exported to the destination at the scheduled intervals.

Figure 5-19: Scheduled Stills - FTP Destination Settings.

5.6 Clients Tab

The *Clients* tab indicates how client connections should be handled. A *Client Connection* represents a network connection to the VIGIL Server from an outside source(VIGIL Client, View Lite Smart Device App, 3xCLOUD, VIGIL Web, etc.)

Figure 5-20: Settings - Server Settings Tab - Client Tab

- **Allow RapidStream on Live / Playback -** When enabled, the Live and / or Playback window in VIGIL Client will have the option to playback video using *RapidStream* technology when streaming video from this Server.

- **Disable RapidStream if Server CPU Usage Exceeds... -** The *RapidStream* playback on Client is handled by the Server before sending the playback stream to the Client. To ensure functionality of the VIGIL Server is not adversely affected, the *RapidStream* playback will be disabled if the CPU on the Server reaches the specified percentage. When the CPU usage drops back below the percentage the *RapidStream* option will again be available. This can happen dynamically during playback.

- **Max Network Connections -** Enter the maximum number of simultaneous client connections allowed. Three types of connections are available.

  - » *Max Live Connections*
  - » *Max Playback Connections*
  - » *Max Other Connections*

5.7 Sequence Tab

Note: This tab is only applicable to capture cards systems with analog monitor output.

The *Sequence* tab configures the camera display sequences for the analog output monitors or the analog live viewer. A sequence can be configured for hardware rendered live view using analog or IP cameras.

3xLOGIC

Figure 5-21: Settings - Server Settings Tab - Sequence Tab

- **Monitor Number** - Select the analog output monitor number for the sequence.
- **Auto Start Sequence** - When enabled, the sequence for the selected analog output monitor is started automatically when VIGIL Server starts.
- **Add** - Add a new camera to the sequence with a specified dwell time.
- **Edit** - Modify the dwell time of the selected camera.
- **Delete** - Remove the selected camera from the sequence.
- **Up / Down** - Moves the selected camera up / down in the sequence.

5.8 Hardware Tab

The *Hardware* tab informs VIGIL Server of the specific hardware you may have installed.

Figure 5-22: Settings - Server Settings Tab - Hardware Tab

- **Substream Motion Detection** - When enabled, VIGIL will attempt to detect motion via sub-stream. If sub-stream is not available, VIGIL will revert to detecting motion on main stream. If sub-stream is in signal loss, VIGIL will revert to mainstream after 10 seconds. This feature must be licensed though a 30-day free trial is included. Contact your 3xLOGIC representative for more information.

  > ⚠ **Warning:** For the *Substream Motion Detection* feature to function successfully with VISIX IP cameras and / or systems with capture cards, the substream needs to be configured for 1 or more key frames per second. For capture cards, this is the equivalent to a GOP (Group of Pictures) value of equal to or less than the FPS configured on the substream.

- **Hard Drive Temperature Threshold** - Set the maximum temperature for the VIGIL Server's hard drives. If a hard drive exceeds this temperature, a warning will be displayed and an entry placed in the *Audit Log*. The *View* button will open a window to display Information about the Hard Drives in the system, including *Temperature, Model, Serial Number* and *Firmware* version.

- **Scavenger Threshold** - Set the VIGIL *Scavenger Threshold* percentage. When a media drive's available capacity falls under the allotted threshold, VIGIL will begin scavenging the oldest footage / data on the drive to free up storage space.

- **Max Locked Video Disk Usage** - Set the maximum amount (as a percentage of your total video storage) of locked video than can be stored on the Server. When this threshold is reached, older locked video must be released to allow for new video locking.

- **AUX Device Settings...** - Open the *AUX Device Settings* window for configuring other attached devices such as DIO boards and encoders. See "Aux Device Settings" on page 82 for more information.

- **Sub Stream Settings...** - This button is only visible on applicable capture card systems. Set the sub-stream image settings for analog cameras. Click the *Sub Stream Settings...* button to launch the below window.
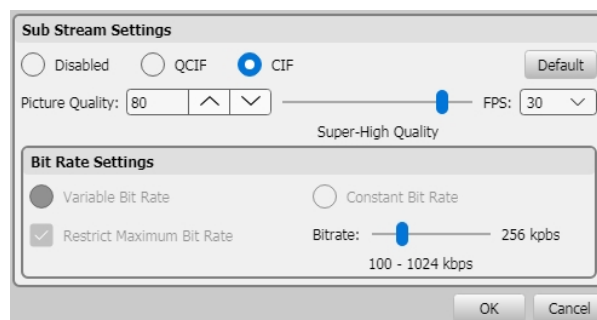
Figure 5-23:VIGIL Server Settings- Hardware Tab - Substream Settings (Analog)

Note:

- On some capture card systems (3xLOGIC's v250, v500, etc..), this option will be replaced by the VIGIL Analog Settings Utility (accessed via VIGIL Server Settings>Camera Setup Tab).

- On PROSERIES Cards, you can enable sub stream video feed for analog video channels. *Resolution, Quality, FPS* and *Bitrate* can be set. The *Sub-Stream* will be available to VIGIL Clients connected to the VIGIL Server.

- **Reset PoE Power** - Clicking this button will power cycle the system's embedded PoE card.

- **Keyboard Settings...** - Allows you to add, edit, or remove a special camera control keyboard, such as the Pelco KBD300A. .

Note: The Pelco KBD300A F1 and F2 buttons can be used to latch on and off VIGIL Server Relays #1 and #2.

3xLOGIC

5.9 VIGIL Connect Tab

VIGIL Connect allows for simplified connections to Server. When VIGIL Connect is enabled, you can configure a VIGIL Client to connect with either the system's *Serial Number* or an *Alias* instead of the IP Address. This is especially useful in situations where the IP Address of the VIGIL Server may change without notice.

To utilize a VIGIL Connect Alias, click *Enable VIGIL Connect*. The following information prompt will deploy:
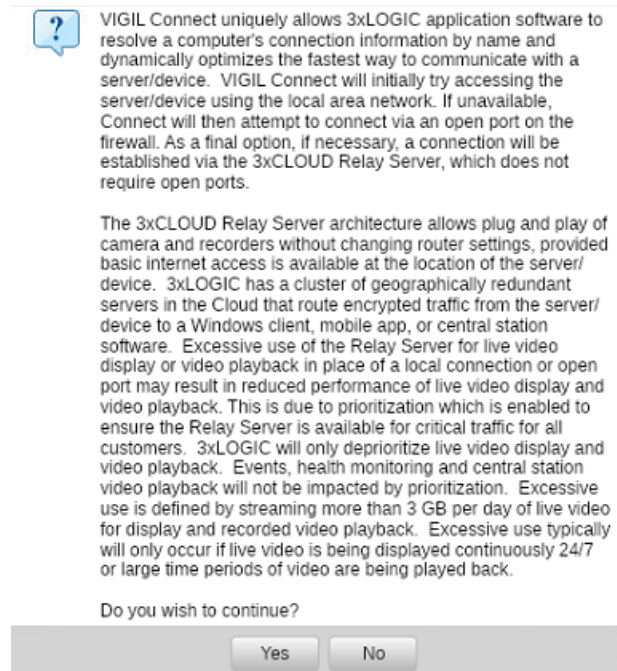
Figure 5-24:VIGIL Connect Info Prompt

If you have read and are in agreement with the information in the prompt, click *Yes* to enable VIGIL Connect. The below interface will deploy. VIGIL Connect settings are contained on the left-side with disclaimer information available at-right.
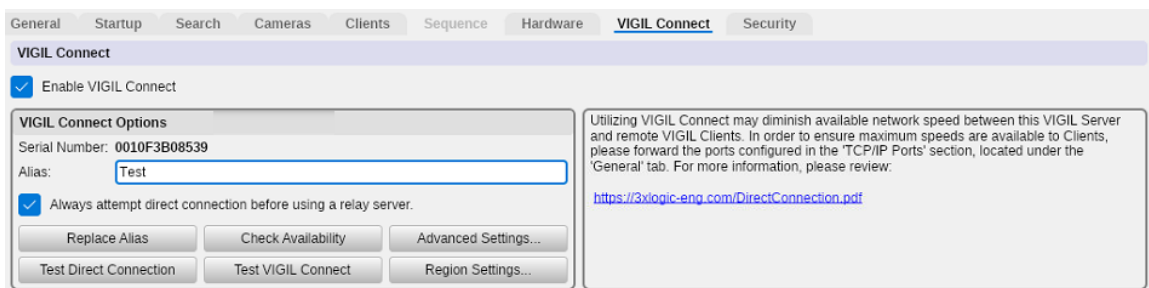
Figure 5-25: Settings - Server Settings Tab - VIGIL Connect Tab

- ■ **Enable VIGIL Connect** - Check to enable VIGIL Connect. The first time you enable this option the system will check if your router is UPnP enabled. If it is, the port forwarding will be auto-matically created in the router for you. If it is not, you will receive a message stating this and that you will need to create the port forwarding in the router yourself. Please consult the

documentation for your specific router for how to configure port forwarding.

- **Serial Number** - The *Serial Number* of the VIGIL Server.

- **Alias** - You can configure an easy to remember *Alias* for the VIGIL Server so you do not have to remember the Serial Number. The alias is **case sensitive.**

- **Always attempt direct connection...** - Enable this option to always attempt direct connection first when using the VIGIL Connect service. If direct connection is unavailable, VIGIL will then util-ize the VIGIL Connect Relay service to interface your VIGIL Server with VIGIL Connect-enabled devices and software. .

- **Replace Alias** - If a user is receiving a *Duplicate VIGIL Connect Alias* warning, or if a motherboard has recently been swapped on the system and desired alias is assigned to the old motherboard, clicking *Replace Alias* will open the Alias Swap web portal.

  » Follow the instructions on the web page to swap the alias from the old motherboard to the new motherboard. The old motherboard's MAC address is required to perform the Alias replacement..

- **Check Availability** - Click this button to communicate with the VIGIL Connect Central Server and determine if the *Alias* is available. All aliases must be unique and if the check fails, the user will be prompted accordingly.

- **Advanced Settings...** - Opens the *VIGIL Connect Settings* window. If UPnP was not detected by VIGIL Server, you may retrieve port Internal Port and Port Mapping values here to manually enter into your router's port forwarding. Available ports are dependent on UPnP and enabled / disabled ports in Server Settings > General > TCP / IP Ports.

Figure 5-26:VIGIL Connect Advanced Settings

- **Test Direct Connection** - Clicking the *Test Direct Connection* button will open the below window. Every port will be tested and its status will be indicated with either a ❌ (connection failure) or a ✅ (connection success.)

3xLOGIC

» Click the *Test Connection* button to run the test again.
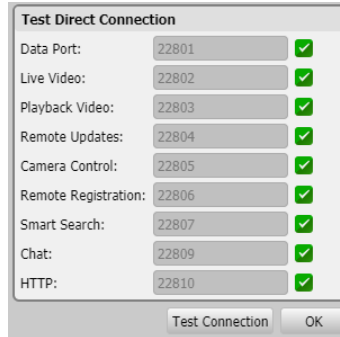
Figure 5-27:VIGIL Connect - Test Direct Connection Window

- **Test VIGIL Connect** - Tests VIGIL Connect using your current configuration.
- **Region Settings...** - Opens the VIGIL Connect Region Settings. Specify your region for improved VIGIL Connect performance.
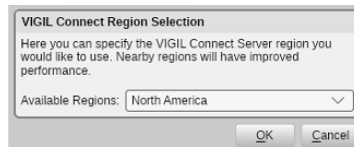
Figure 5-28:VIGIL Connect - Region Settings

5.10 Security

The Security tab features configuration options for security features of the VIGIL Server.
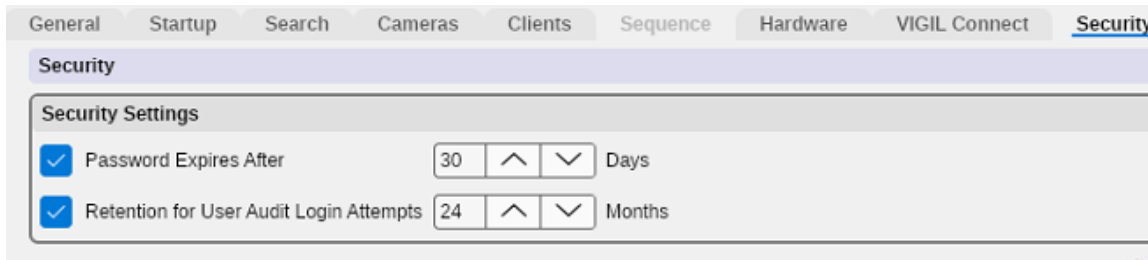
Figure 5-29:VIGIL Server Settings - Server Settings - Security Tab

- **Password Expires After** - IF enabled, the user can set the VIGIL Server USer password expiry interval (in days)

- **Retention for User Audit Login Attempts** - If enabled, the user can choose the maximum amount of time (in Months) to log login attempts for user audit reporting purposes.

3xLOGIC

6 VSMU - STORAGE TAB

The Storage tab configures video recording destinations and export destinations for the VIGIL Server.

Figure 6-1: Settings - Storage Tab

There are three types of media storage drives: Video Storage Drives, Alternate Video Storage Drives, and Export Destinations. *Alternate Video Storage Drives* are only used if every *Video Storage Drive* is offline.

- ■ **Add** - Opens the Media Control window to configure a storage location.
- ■ **Edit** - Edit the selected location.
- ■ **Delete** - Deletes the selected location.
- ■ **Partition Priority** - If data partitioning is enabled, the priority can be set to Alarm or POS/ATM Data Alarm footage. For example, if a motion alarm and a POS/ATM data alarm occur on the same piece of footage, the priority determines into which partition the footage will be saved.
- ■ **Limit Maximum Days of Video/Audio Storage** - Enable this option to set a maximum limit (in days) for footage and audio storage. Enter a maximum value in the available field. When this feature is enabled, the default value is 90 days.

> **e.g.** **Example:** If this maximum value is set to 45 days, VIGIL will begin to scavenge footage and audio once 45 days of footage/audio retention has been reached.

> **Note:**Deleting a location does not remove the physical destination, only the reference to it within VIGIL Server.

> **Note:**If a *VideoStorage Drive* or *Alternate Storage Drive* is deleted, the user will be prompted whether they also want to delete any database records of the footage at that location and whether they want to delete any saved footage at that location.

6.1 Video Storage Drives

Video Storage Drives are the main drives where video footage is stored. If a *Video Storage Drive* becomes full, VIGIL Server will switch to the next *Video Storage Drive* for recording. Also, if all of the Video Storage Drives are offline, the *Alternate Video Storage Drives* will be used until they return online.

When adding or editing a video storage drive, the *Media Control* window is displayed.

Figure 6-2: Settings - Media Drives Tab - Media Control Window

- ■ **Destination Name** - The name for the video storage location.
- ■ **Destination Path** - The hard drive and folder path to record video data to.
- ■ **Alarm Reserved** - The amount of storage to be reserved for Alarm video footage.

3xLOGIC

- **POS/ATM Alarm** - The amount of storage to be reserved for POS/ATM Alarm video footage.
- **Remaining** - The amount of remaining available storage.

6.2 Data Partitioning for Video and POS/ATM Alarm Video Footage

Data partitioning has been added to VIGIL Server allowing for better user input as to how data is saved to the hard drive. Data partitioning allows you to set up logical divisions between standard alarm video files, POS/ATM alarm video files, and normally recorded video. This allows the video scavenging process to skip alarm video files and allows you to save these types of video footage for longer periods of time.

Instead of copying alarm footage under the normal areas for storage, it will be recorded to a special folder that is considered a separate entity. Normal video storage is scavenged and deleted as new footage is written, however these special folders are not scavenged normally; they will retain as much data as you have allotted for them in the *Media Control* window. Once they reach capacity, they will be scavenged, and the oldest video data will be removed to write new data. Since alarm and POS/ATM alarm data is less storage intensive, this data can have a much longer 'shelf life' on your VIGIL Server, depending on the size of the partition you create.

Note: This feature is not enabled by default.

6.3 Alternate Video Storage Drives

Alternate Video Storage Drives are emergency backup drives that are used only if all of the Video Storage Drives are offline. If an alternate video drive is being used, VIGIL Server will beep and a flashing *Critical Warning* message will be displayed. When the *Video Storage Drives* return online, the *Critical Warning* message will disappear; the Server will stop beeping and will switch back to recording to the main *Video Storage Drives*.

When adding or editing an *Alternate Video Storage Drive*, the *Media Control* window is displayed.

Figure 6-3: Alternate Video Storage Drives - Media Control Window

- **Destination Name** - The name for the *Alternate Video Storage* destination.
- **Destination Path** - The hard drive and folder path to record video data to.

6.4 Export Destinations

Video Export Destinations are used to store exported video footage. You must set up destinations here before you can save video footage or still images from VIGIL Server using the VIGIL Client application.

When an export destination is added or edited, the *Media Control* window is displayed.

Figure 6-4: Settings - Media Drives Tab - Export Destinations - Media Control Window

- **Destination Name** - The name for the export destination.

- **Destination Path** - The path for the export destination. Click ... to browse to the destination.

- **Destination Type** - This setting affects how the destination appears in the export list.

    - » **Default On** - The destination checkbox will be selected.

    - » **Default Off** - The destination checkbox will not be selected.

    - » **Silent Send** - All exports will also be sent to this destination without notifying the user.

- **Remember Last...** - When enabled, *Remember Last Selected State* remembers the previous state of the *Export Destination > Media Control* form. This feature is enabled by default.

- **Include Export Audit** - Saves a text file that contains a log of export activity to the destination. When this is enabled, users will be required to fill out a form each time they export.
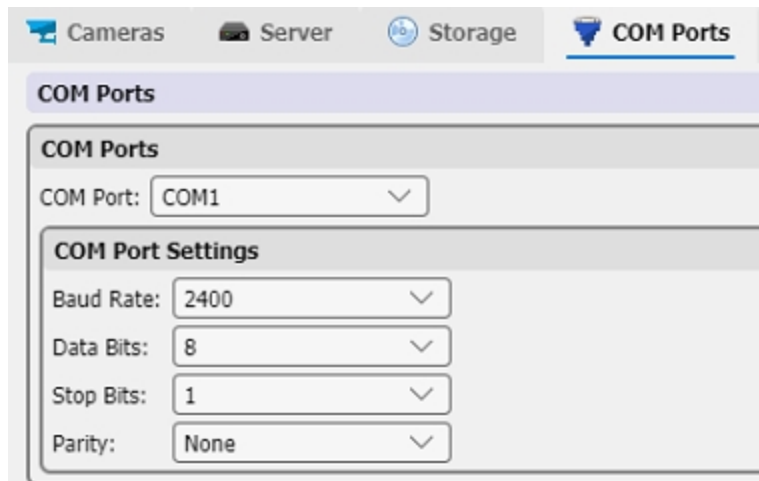
    Note: Must be enabled in conjunction with the Audit Exported Footage feature in the search settings for it to work.

- **Include Audit Log** - Saves a complete copy of the *Audit Log* to the same destination each time an export is done.

- **Include DV Player** - Saves the *Digital Video (DV) Player* to the same destination each time an export is done. This setting is normally used for CD-R or DVD-R media type destinations. See the VIGIL Client User Guide for details on operating DV Player. .

- **Include AutoRun Files** - Due to some Anti-Virus applications detecting all AutoRun files as a potential threat, disable this option to not include the AutoRun files with the export. If the AutoRun files are included, the DV Player install will run when the DVD is inserted to a system that does not already have *DV Player* installed.

3xLOGIC

■ **Include AutoRun Files** - Due to some Anti-Virus applications detecting all AutoRun files as a potential threat, disable this option to not include the AutoRun files with the export. If the AutoRun files are included, the DV Player install will run when the DVD is inserted to a system that does not already have *DV Player* installed.

7 VSMU - COM PORTS TAB

The *COM Ports Settings* tab configures the installed COM ports for communication with connected hardware such as POS data Connections and camera control.

Figure 7-1: Settings - COM Ports Tab

Select the desired *COM Port* from the drop-down menu and adjust the *Baud Rate, Data Bits, Stop Bits* and *Parity* to match that of the connected hardware.

8 VSMU – USER AND GROUP MANAGEMENT TAB

The Users tab allows the configuration of users on the VIGIL Server with specific permissions. Each *User* belongs to a *Group* and each *Group* has a set of permissions which can also be configured within this tab. User permissions are derived from their group's permissions.

8.1 Users Tab

Click the *Users* tab to access the *User* configuration options.
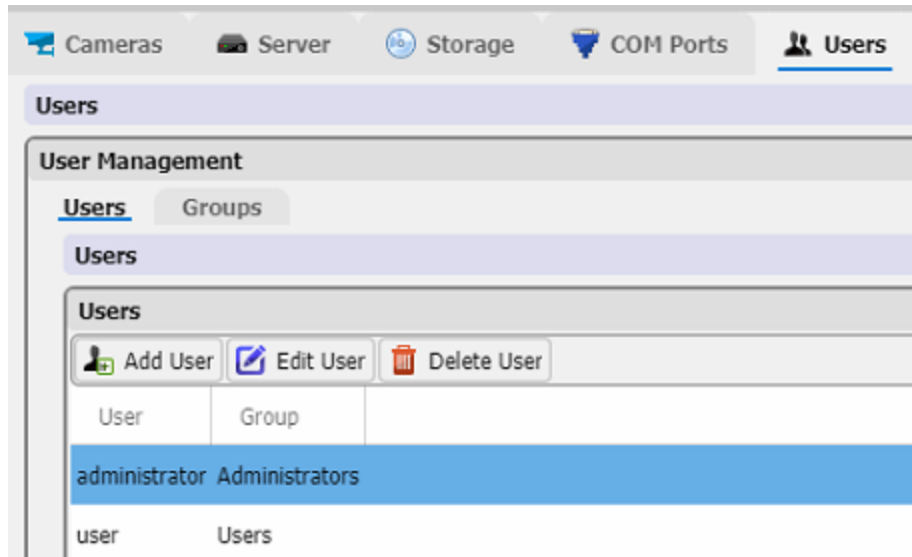
Figure 8-1: Settings - User and Group Management Tab - Users Tab

- ■ **Add a User** - Click the *Add User* button to bring up the below window, select a *Group* and enter a password in the *Add New User* window. 3xLOGIC highly recommends the use of a secure, complex password for all user accounts to best safeguard your system.

> ⚠ **Warning:** VIGIL Server will prompt a user on login to create a more secure password whenever an insecure password is detected. Secure passwords should contain a mix of letters (lower and upper case), numbers and special characters.

Figure 8-2: Add User Form

- ■ **Edit a User** - Select a *User* from the drop-down menu and click the *Edit* button. The user's group or password can be changed, the user's name cannot.
- ■ **Delete a User** - Select a *User* from the drop-down menu and click the *Delete* button.

- **Users Managed by VCM** - This option is only visible if this server has been configured for user management VCM-side. If this checkbox is toggled, than the VIGIL Server's users are currently being managed by VCM. The *VIGIL Server Settings- User Tabs* will display the following information text when this checkbox is toggled:

   The users for this VIGIL Server are currently set to be managed by a VCM. Any user or password changed will need to be performed on the VCM system and then the VCM will automatically update this VIGIL Server.

   The "Users Managed by VCM: option can be disabled if a VCM is no longer being used. It is important to verify that VCM is no longer managing the users before disabling this settings since any user list from VCM will take precedence and all changes done locally will be lost.

8.2 Groups Tab

Click the *Groups* tab to access the *Group* configuration options.
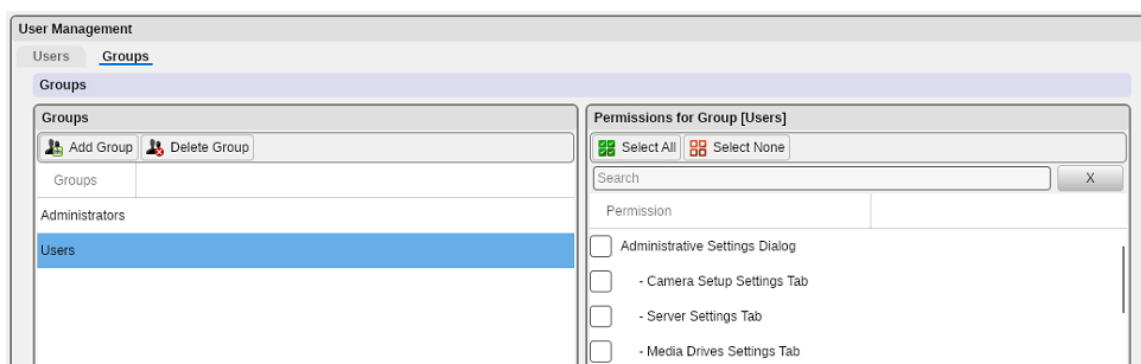
Figure 8-3: Settings - User and Group Management Tab - Groups Tab

- **Add a Group** - Click the *Add* button and enter a group name in the *Add New Group* window.
- **Permissions** - Select a group from left-hand *Group* menu and enable the check box beside each permission that the group will have in the right hand window. To disable permissions for the group, uncheck the box beside the permission. These permissions are useful for maintaining access controls to VIGIL server and can keep your settings safe from accidental and malicious tampering. To filter down the permissions list, enter a search term into the available search bar. Matching permission swill be displayed in the permissions list.

   See "User and Group Permissions List" on the facing page for a description of each permission.

- **Select All / None** - Enable all permissions or disable all permissions.
- **Search** - Utilize the search function to quickly narrow down larger group lists.
- **Delete Group** - Select a *Group* from the left-hand window and click the *Delete* button.

8.3 User and Group Permissions List

Below is a list of all VIGIL Server User / Group permissions with accompanying descriptions of the actions they permit. Permissions are applied to Groups and not individual Users. Thus, every user in the group will share the same permissions. Users can only be applied to a single group.

Permission	Description
Administrative Settings Dialogue: (Server Settings Tabs)	Selecting this permission will also give you permissions to all Advanced Settings Tabs for VIGIL Server, including: ■ Camera Setup Tab ■ Relays/Alarms Settings Tab ■ Server Settings Tab ■ Data Settings Tab ■ Media Drives Settings Tab ■ Audio Settings Tab. ■ COM Port Settings Tab ■ Email Overview Settings Tab ■ User Management Tab ■ OS Settings Tab Uncheck the tabs that you want to exclude access for the selected Group.
User Management Tab	Aside from granting individual access to the User Management tab , granular permissions for *Modifying User / Group Permissions* and *Adding Users / Group*s and *Adding Users to Own Group* also exist forgroups.
Codec Settings	Group has access to adjust codec settings for cameras on the server.
Recorder Controls	Enables / Disables access to the Recorder window in VIGIL Client.
Allow Video Playback	Video Playback on VIGIL Client.
Allow Still Image Export	Export Still Images using VIGIL Client.
Allow Still Image Email	Send email notification with attached still image
Allow AVI Export	Export Video in AVI format in VIGIL Client.
Allow Authentic Video Export	Export authentic video (MJPG) format in VIGIL Client..
Allow AVI Export (RapidStream)	Export video in AVI format compressed with RapidStream in VIGIL Client.
Allow Authentic Video Export (RapidStream)	Export video in Proprietary MJPG format compressed with RapidStream in VIGIL Client.
Allow Data Export	Export data associated with a camera in VIGIL Client.
Allow Audio Export	Export audio associated with a camera in VIGIL Client.
Allow Video Tagging	Ability to tag footage in VIGIL Client
Allow Live View	View live video at VIGIL Client
Allow Relay Control	Ability to change the state of a Relay
Allow Client Live Speeds Over 1 frame	If unchecked, the user cannot live view video at more than 1 FPS.
Allow Rapidstream on Live / Playback (Local or Remote)	Allows access to live view or playback using the RapidStream codec, either locally or remotely depending on the selected permission.
Allow Substream on Live (Local or Remote)	Allows access to live view or playback using the RapidStream codec, either locally or remotely depending on the selected permission.
Socket Activity Form	This is the Client Connections window, access from the toolbar
Allow Relay Control	Enables the user to toggle configured relays on and off via VIGIL Client

Permission	Description
Allow Export File Browsing	Ability to view the contents of the Exports folder through Client in main interface mode, remote browsing is covered by another permission.
Allow Export Delete	Ability to delete exported video from VIGIL Client.
Audio Recorder Control	Access to the Audio Recorder Controls tab in Server Settings > Audio > Other Settings.
Allow Audio Live	Stream audio associated with camera in live display in Client
Allow Audio Playback	Playback audio associated with a camera on search in VIGIL Client.
Allow Audio Talk	Two-way Audio controls in VIGIL Client
Allow Camera Control	Ability to manipulate a camera in VIGIL Client for PTZ cameras.
Allow Analog Output Configuration	Access to analog I/O configuration on a VIGIL Server
Allow Analog Sequence Control	Access to the Sequence window which controls the sequences configured in the settings -> server settings tab -> Sequences sub tab.
Allow Chat	Chat function between Clients connected to a VIGIL Server.
Auto reply Chat Audio Request	Automatically connect an audio chat request.
Allow Software Updating	This enables the update button in the server settings in client, VCM is not affected by this setting.
Allow Access to Custom Help Application	This turns on / off the button itself, if off, you will just see the regular About button.
Exit VIGIL Server	Users without this permission cannot exit server.
Shut Down VIGIL Server (Kiosk Mode)	Shut down the VIGIL Server within Kiosk Mode.
V-POS Administrator	Access to the Exceptions and the VPOS Settings forms in VIGIL Client.
Client Administrator- Main Interface Mode	Allows user to adjust VIGIL Client settings when Server option Use Client as Main Interface is checked.
Allow Footage Date / Time Range in Client	Ability to see the Footage Date / Time Range window.
Allow VIGIL Archive Import / Export	Allows the user to use VIGIL Archive's import / export function.
Allow Audit Log	Allow access to User Audit in VIGIL Client.
Display Usage Performance Meter	This is the performance bar on the toolbar in VIGIL Client
User Audit Reports	Run a User Audit Report in VIGIL Client. This will enable the User Audit in the Treeview.
User Audit Settings	Access to modify User Audit Settings in VIGIL Client.
User Audit Exclusion	Enabling this permission will exclude the user groups data from being audited by the VIGIL User Audit tool.
Server Alarms	View server alarms in VIGIL Client.
POS/ATM Live	Ability to view POS/ATM Data in live mode. Option under Other tab in VIGIL Client.
Allow Remote Exports in Client	When exporting in client, users can choose to perform the export on the remote VIGIL Server.

3xLOGIC

Permission	Description
V-POS Events	Run a report for all exceptions in VIGIL Client. Option under V-POS tab in VIGIL Client. Enables the VPOS Events Treeview option.
V-POS POS/ATM Search	Search data in Playback within the VIGIL Client software. Enables Treeview option and option under POS/ATM tab in Search.
V-POS Quick Search	Enables the Treeview option, quick search lets you bring up footage / data with only and Event ID or a receipt # or an IDX.
Clearing V-POS Event Flags in Client	Allows the user to clear V-POS Event flags via the VIGIL Client ui.
Allow Camera Web Interface in Client	Ability to access a camera's web interface through VIGIL Client.
Allow Remote Export Browser in Client	Enables the remote export browser from which the user on client can copy exports on the remote server or to the client.
Allow to use VIGIL Relay Server (VIGIL Connect)	Enables the user to access features and services requiring the VIGIL Connect Relay Server(non-direct connections).
Allow Printing	Enables printing capability for the user.
Allow Screen Record in Client	Enables the use of the VIGIL Client Screen Record function.
Advanced Reporting	Enables the use of the VIGIL Client Advanced Reporting feature.
Allow Remote Main Stream	Enables the use of a camera's mainstream when connecting in from VIGIL Client.
View Restricted	Enables a user to view restricted footage when connecting in from a VIGIL Client.
Allow to Restrict Video	Enables the ability for a user to restrict footage when connecting in from a VIGIL Client.
Manage, View and Restrict Video	Enables the ability for a user to manage, view and restrict video when connecting in from a VIGIL Client.
Allow to Lock Video	Enables the user to lock video (prevent footage scavenging) when connecting in from a VIGIL Client.
Manage and Lock Video	Enables the user to lock video and manage locked video when connecting in from a VIGIL Client.
Advanced Reporting: Employee Exceptions	Enables the user to access the Advanced Reporting > Employee Exceptions report in VIGIL Client.
Advanced Reporting: People Counting	Enables the user to access the Advanced Reporting > People Counting report when connecting in from a VIGIL Client.
Advanced Reporting: Average Dwell Time	Enables the user to access the Advanced Reporting > Average Dwell Time report when connecting in from a VIGIL Client.
Advanced Reporting: Shift Analysis	Enables the user to access the Advanced Reporting > Shift Analysis report when connecting in from a VIGIL Client.
Advanced Reporting: Shift Analysis Settings	Enables the user to access the Advanced Reporting > Shift Analysis Settings.
Advanced Reporting: Heatmaps	Enables the user to access the Advanced Reporting Heatmaps when connecting in from a VIGIL Client.
Audio Channel	Enables the user access to configured / edit the specified audio channel. All configured audio channels will be listed to allow for indivdual permission configuration per channel.

Permission	Description
Camera	Access to view a camera in VIGIL Client . If you want to make the camera covert for a specified Group, deselect the camera in permissions.

3xLOGIC

8.4 Active Directory Integration

VIGIL Active Directory permits users to login to VIGIL Server using the same login credentials used on their local Windows domain network.

VIGIL Active Directory utility is installed alongside VIGIL Server. So long as the VIGIL Server VMS system is part of a Windows domain / work network or can communicate with the desired domain, VIGIL Active Directory will automatically detect the active user directory, and, if configured to do so, will allow login to VIGIL using existing Windows domain network user credentials.

VIGIL Active Directory can be launched from *Start Menu>Program Files> VIGIL>Utility>Active Directory Manager.*

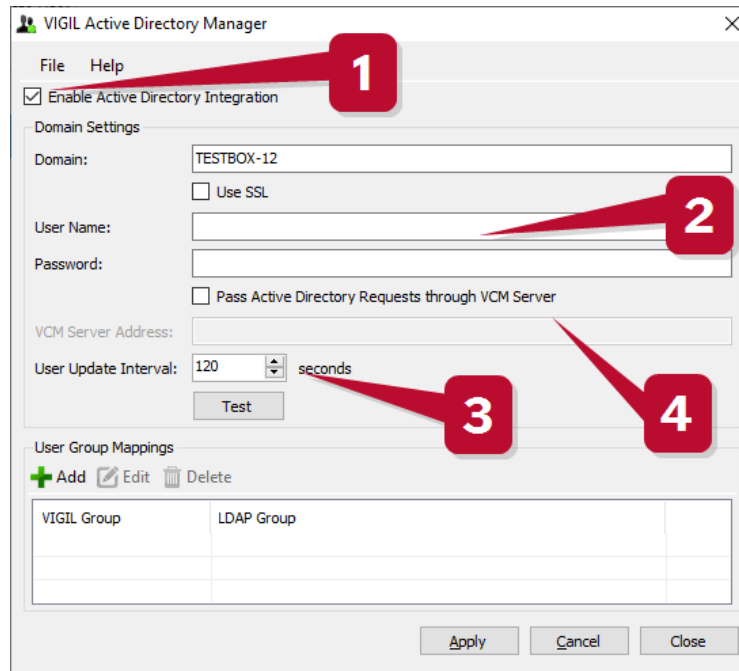After launching, the application will deploy:

Figure 8-4: VIGIL Active Directory Manager - Enabling Active Directory Integration

1. Click the **Enable Active Directory Integration** button
2. Enter in your domain login credentials. This will allow VIGIL to query the Windows active user directory.
3. Configure a *User Update Interval.* The user list will be updated per the configured time interval (in seconds).
4. If Active Directory is being managed by VCM Server, enable **Pass Active Directory Requests through VCM Server** and enter a VCM Server address.

Adding a Set of User Group Mapping to VIGIL Active Directory Manager

Each set of User Group Mappings define which users from the Windows user directory will be allowed to login to VIGIL using their Windows domain network credentials. To add a set of user group mappings:
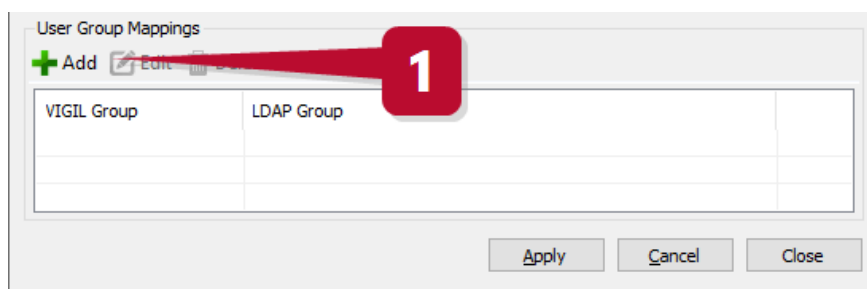
Figure 8-5: VIGIL Active Directory Manager - Adding Windows User Group Mappings

1. Click the *Add* button.

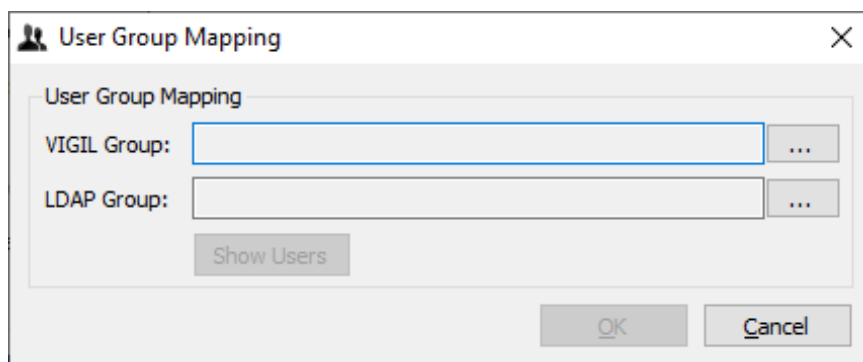This will open the User Group Mapping configuration window(pictured below.)

Figure 8-6: VIGIL Active Directory Manager - User Group Mapping Window

In this window, a user must select both a VIGIL Group and LDAP Group to configure User Group Mappings. These groups MUST be pre-configured in VIGIL and Windows.

- ■ **VIGIL Group** – This menu will feature any user groups currently configured in VIGIL. All users from the selected LDAP group will be added to chosen VIGIL Group.

- ■ **LDAP Group** – This menu features all LDAP(Lightweight Directory Access Protocol) user groups configured on the system's Windows domain network. Users contained within the selected group will be added to the selected VIGIL Group. Please note the menu will contain several entries which are default Windows domain user groups .Click the … button to preview list of users from the selected LDAP group.

1. Click **OK** to save the new User Group Mappings.

If you would like to make changes to this group in the future, simply select the group from the list and select the Edit button.

> **Note:** Server logins are refreshed and updated in 2 minute intervals by default. Adjust the User Update Interval to increase or decrease this value.
>
> VIGIL Active Directory has been engineered for use with Windows Active Directory **ONLY**. Other technologies utilizing LDAP are not tested against VIGIL Active Directory and may not function successfully.

After creating the desired user group mapping, users belonging to the selected LDAP group should now be able to login to VIGIL Server using their Windows domain network login credentials.

3xLOGIC

9 VSMU - RELAYS / ALARMS TAB

The *Relays / Alarms* tab configures the input alarms and associated notifications settings for the VIGIL Server.

Figure 9-1: Settings - Relays / Alarms Tab

If no DIO device is configured, the form will be grayed out and will display the following warning:

Figure 9-2: Advanced Settings - Relays / Alarms - No DIO Warning

If the user needs to edit DIO device settings, click the **AUX Device Settings** at the bottom-left of the window to open the settings form for configuring attached devices.

Digital inputs are alarms triggered by external circuits. The input alarm can be used to trigger video recording, audio recording or PTZ events.

9.1 Input

9.1.1 Input Number

Select the Input number from the *Input Enabled* drop-down list. Click the *Edit...* button to rename the input for easier identification. To enable the input, click the check box for *Input Enabled*. If this input should only be active when another input is triggered, select the desired input from the *Depends on Input* drop-down.

9.1.2 Settings Tab

Configure the settings for the selected input. A *Camera* or *Audio Channel* must be selected for the *Digital Input* to remain enabled.

- ■ **Alarm Priority** - Set a priority level for the alarm between 1-10. These levels can be used to quickly assess the importance of multiple alarms. These priorities can also be used in conjunction with VIGIL Client's *Minimum Alarm Priority* setting to ensure only alarms of the specified priority deploy an alarm pop-up in VIGIL Client. See *Alarms Tab - Automatically Display Inbound Alarms From Server* in the VIGIL Client user guide for more information.

- ■ **Dwell Timer -** The number of seconds the *Digital Input* remains active after a *Trigger* occurs.

- ■ **Input State: Normal Open / Closed** - Set the normal state for the *Digital Input*. When the *Digital Input* changes state, the alarm will be triggered.

- ■ **Auto Acknowledge** - When enabled the *Alarm* will be automatically acknowledged after the selected number of seconds have passed.

- ■ **Schedule** - Check *Enabled* and click ... to configure a schedule for when the *Digital Input* will be active. The Relay Schedule functions identically to Recording Mode Schedule. See "Scheduled Recording" on page 27

- ■ **Push Still Shot to Server** - When *Enabled,* a still shot from the selected camera will be uploaded to the configured server when a *Digital Input Alarm* is Triggered.

- ■ **Local Alarm** - When Client as Main UI is active and this *Local Alarm* is enabled, alarms will only be recieved on the Client as Main. Alarms will not eb realyed to other connected VIGIL products.

- ■ **Cameras** - Select the *Camera(*s) to be associated with the *Digital Input.*

- ■ **Audio Channels** - Select the *Audio Channel(s)* to be associated with the *Digital Input*.

9.1.3 Notification Settings Tab

Configure *Notification* and *Relay* settings for the selected *Digital Input*.

Figure 9-3: Settings - Relays / Alarms Tab - Notification Settings Tab

©2024 3xLOGIC Inc. | www.3xlogic.com | (877) 3xLOGIC | helpdesk@3xlogic.com

3xLOGIC

Email Notification

When enabled, an email is sent when an alarm is triggered.

To configure timed suppression for email notifications, enable *Minimum time between emails* and configure a time suppression duration. This will prevent notification recipients from receiving multiple alarms from the same prolonged VA alarm events.

Click *Email Settings...* to configure the email recipients and contents. Enter the appropriate details for the email that will be sent. To add, edit, or remove email recipients, use the *Recipients* section and the appropriate buttons. Enabling *Attach Still Shot* will add a still image of the selected cameras to the outgoing email. This image is from the beginning of the triggered alarm event.

> **Note:** For email options to function properly, a valid SMTP server must be set up correctly in the *Email Overview Settings* tab.

Output Relay

Select the Output Relay to trigger when the *Digital Input Alarm* is triggered. The *Output Relay* can be set to *Latched* or *Momentary*.

Notification Settings

- **Monitor Output** - To display the Camera feed associated with the *Digital Input* on a Monitor during an alarm, choose the *Monitor Number* or *All Monitors* from the Drop-Down. This will be visible when connected with a VIGIL Client.

- **Suppress Email Notification** - This option, which will only work in conjunction with enabling the *Popup Alarm* Window, will prevent a flood of email alerts being sent out. It will only send out one email alert until the alerts have been acknowledged on the *Popup Alarm* window. If alerts have been set to auto acknowledge, it will send out an email after each period of auto acknowledgement has passed.

- **Audio Notification** - Enables *Audio Notification* which plays a system beep or wave file when an alarm is triggered. When *Wave File* is selected, click the *…* button to browse for the .wav file that will be played.

9.1.4 Output

Output Relay Settings

Select Outputs from the top of the *Relays / Alarms* tab page.
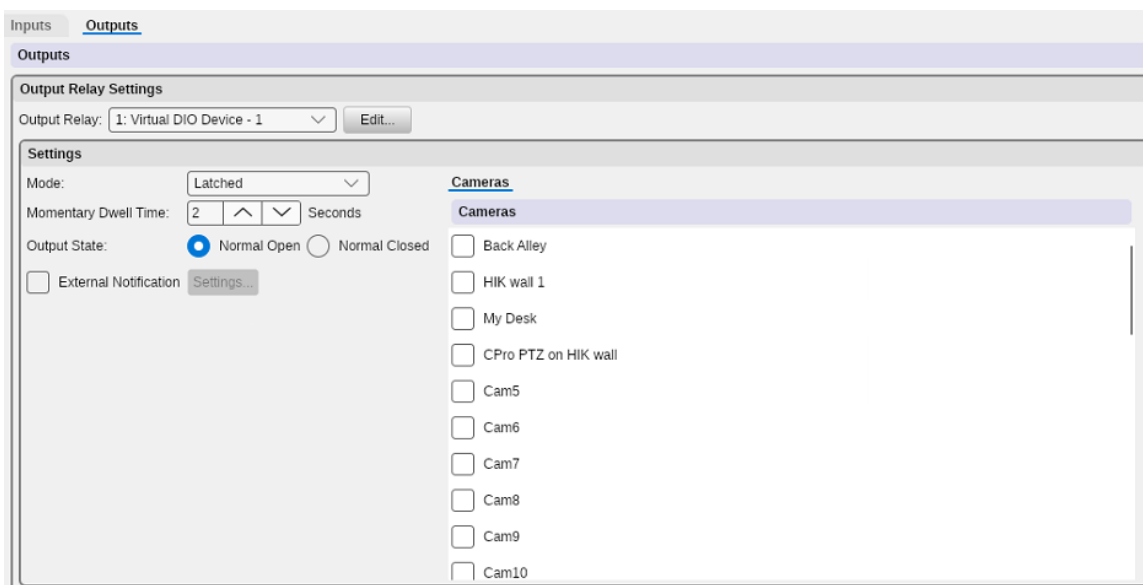
Figure 9-4: Settings - Relays / Alarms Settings - Output Relay Settings

To configure an output:

1. Select an *Output Relay* from the drop-down. Select *Edit...* to configure Output settings.

2. Configure *Mode* and *Momentary Dwell Time* under the *Settings* section and assign the output to a camera via the *Cameras* list.

3. Select a default *Output State* (Normal Open, Normal Closed).

Output - External Notification Settings

If extneral noification for the selected output is desired, enable *External Notification* and click *Settings*.
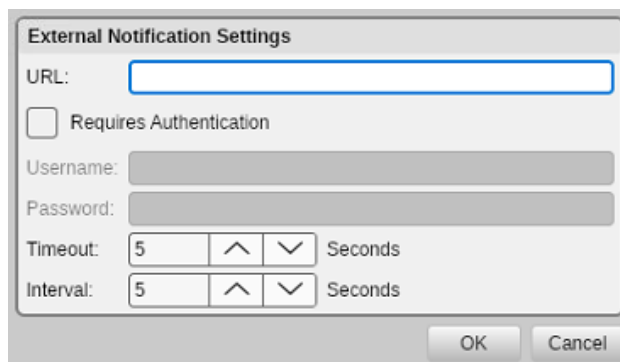
Figure 9-5: Output - External Notification Settings

When these settings are configured, anytime the selected output occurs, the configured URL will be visited by VIGIL Server. This can be used for third party applications that can generate alarm events / notifications any time the configured URL is hit.

1. Configure connection settings as required

2. Click **OK** to save.

3xLOGIC

Output - Relay Override

This logical function is used to override a relay when another relay is in use. This will cause a relay which would normally trigger to remain inactive when another specific relay has already been tripped.

9.2 Remote Client Retry Settings

Figure 9-6: Settings - Relays / Alarms Tab - Remote Client Retry Settings

- **Connection Attempts** - The number of times to retry sending an alarm to a remote Client.
- **Retry Delay** - The number of seconds to wait between connection attempts.

9.3 Aux Device Settings

Click the *AUX Device Settings* button under *Auxiliary Devices* to configure other attached devices such as DIO boards and encoders.

Note: AUX Device Settings can also be launched from the Server Settings > Hardware Tab.

Figure 9-7:AUX Device Settings

Add / Edit form fields will change depending on the selected devices (e.g the *DIO Quantity Settings* fields for *Virtual DIO Devices*, etc...).

9.3.1 Virtual DIO Device

The Virtual DIO device is a configurable device in VIGIL's AUX Device Settings.

For VIGIL's virtual DIO, the outputs (relays) are tied into the inputs of corresponding position. Toggling the virtual relay will thus toggle the input and generate an alarm. Whereas outputs can trigger an alarm which can be used to trigger other events in VIGIL, inputs can only be toggled via VGIL SDK.

Figure 9-8: Edit Virtual DIO Device Window

9.3.2 ONVIF DIO Alarm Events

When ONVIF Device is selected as the AUX / DIO Device Type, VIGIL can detect and interface with alarm events configured on the device.

1. Select ONVIF Device from the Type dropdown and fill in the required Network Settings.

Figure 9-9:ONVIF DIO Alarm Events

2. In the *ONVIF Alarm Event Settings* form , select **ONVIF** from the Camera Type dropdown

3. Click **Detect** to detect ONVIF alarm events and DO quantity. The form will populate with detected events.

> **Note:** If any of the existing legacy options are selected [3xLOGIC VSX-IP, VSX IP-B, LG] and the detect feature is used, the *Camera Type* will switch to *ONVIF* as AUX device event detection detection is performed via the ONVIF protocol

4. Click **OK** to save the device settings.

3xLOGIC

10 VSMU - DATA TAB

The VIGIL Server software can be configured to receive and record information from POS/ATM data connections. The *Data* tab allows configuration of the *POS/ATM Connection Settings*.
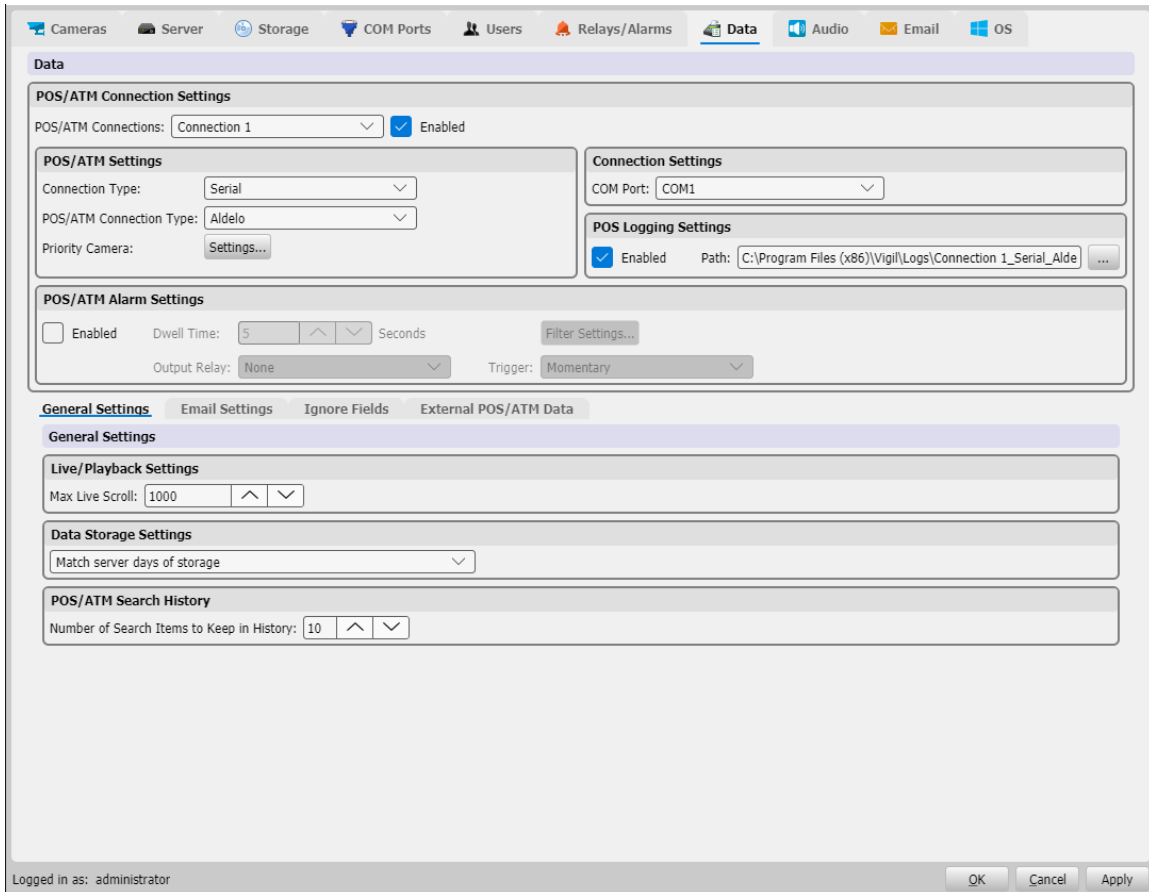
Figure 10-1: Settings - Data Tab

10.1 POS/ATM Connection Settings

■ **POS/ATM Connections** - Enable the POS/ATM Connection.

■ **Enabled** - Enable the POS/ATM Connection.

10.1.1 POS/ATM Settings

■ **Connection Type** - Select whether the POS/ATM Data stream uses a Serial or IP based connection.

■ **POS/ATM Connection Type** - Set the type of Connection for the POS Data stream.

■ **Priority Camera** - Opens the Priority Camera Settings window.

Priority Camera Settings

The camera that is pointed directly at a POS/ATM Register is referred to as a *Priority Camera*. *Priority Cameras* are assigned to the a specific POS *Connection* and *Register Numbers*. Multiple *Con-*

nection / Register Numbers can be assigned to a single *Priority Camera*. A camera's *Digital Presets* can also be used as a priority camera.
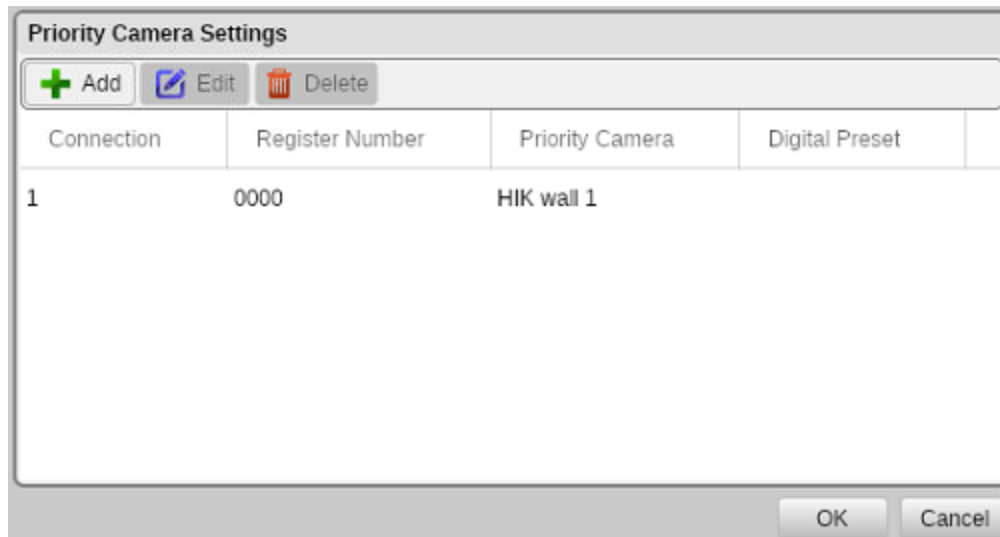
Figure 10-2: Settings - Data Tab - POS/ATM Settings - Priority Camera Settings

✎ **Note:**Priority Cameras are global across Internal and External POS/ATM Data Sources.

Click the *Add* button to add a priority camera. The *Add / Edit a Priority Camera* window will deploy. The window features the configurable priority camera settings as well as a camera preview from the camera currently assigned as priority.
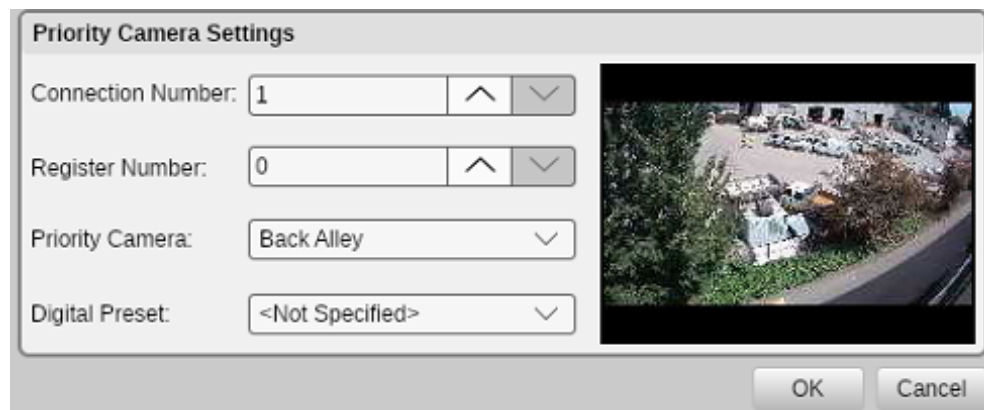
Figure 10-3: Settings - Data Tab - POS/ATM Settings - Priority Camera Settings - Add / Edit a Priority Camera

- ■ **Connection Number** - Set the POS/ATM Connection number to associate with the priority camera.
- ■ **Register Number** - Set the POS Register number to associate with the priority camera.
- ■ **Priority Camera** - Select the VIGIL Server camera to be assigned as the priority camera.
- ■ **Digital Presets** - If desired, select one of the chosen priority camera's *Digital Presets*. The preset will be used as the Priority Camera in place of the original camera image. If the camera currently

3xLOGIC

selected in the *Priority Camera* field has no digital presets configured, this menu will be blank. See "Digital Presets" on page 38 for more information on configuring *Digital PTZ Presets.*

10.1.2 Connection Settings

- **COM Port** - When the POS/ATM connection type is set to Serial, select the COM port the Serial connection will use from the Drop-Down list.

- **Port** - When the POS/ATM connection type is set to IP Server, enter the Port that VIGIL Server will listen on for the POS/ATM Data stream.

POS Logging Settings

- **Enabled** - Check off this box to enable *POS Logging.* This log collects raw POS data before it is parsed. Click the ... button to select a log destination. When troubleshooting POS system issues, users may refer to this raw POS data log for information. The log file defaults to the naming convention of *Connection number - Connection Type - Parser Name. i.e Connection 1_Serial_Verifone Sapphire.log)*

10.1.3 POS/ATM Alarm Settings

This setting becomes available once *Priority Cameras* are configured.

- **Enabled** - Enable specific *POS/ATM Data* items to trigger an *Alarm Event*. This alarm event will be recorded to the POS Partition if data partitions have been enabled.

- **Dwell Time** - The time in seconds that the POS/ATM alarm event will record Video footage for.

- **Output Relay** - Select an *Output Relay* from the Drop-Down list to trigger when a *POS/ATM Data Alarm* occurs.

- **Trigger** - Select whether the Relay will be triggered momentary, or latched on for the durations of the *Dwell Time*.

Filter Settings...

Open the *POS/ATM Alarm Filters* window to configure POS/ATM events that will trigger *POS/ATM Data Alarms.*

Figure 10-4: Settings - Data Tab - POS/ATM Alarm Settings - Filter Settings

- **No Sale** - Enable *POS/ATM Alarms* for all 'No Sale' items.

- **Void** - Enable *POS/ATM Alarms* for all 'Void' items.

- **Value** - A *POS/ATM Alarm* will trigger for any item with the value that is configured. Choose *Greater than*, *Less than* or *Equal to* from the Drop-Down box, and set a value in the first entry field. If you select *Between*, enter a value in each box tor Acevedo entries that fall between the two specified prices.

- **Item / Codes Tabs** - Add or delete specific *Item* names or codes that will trigger a *POS/ATM Alarm*. The text must be an exact match for the POS/ATM data record including spaces, but it is not case sensitive.

- **Filter Method** - Select *AND* to meet all criteria listed before a *POS/ATM Alarm* is triggered. Select *OR* for any criteria to trigger a *POS/ATM Alarm.*

3xLOGIC

10.2 General Settings Tab

The *General Settings* tab controls the display and storage of POS/ATM Data.

Figure 10-5: Settings - Data Tab - General Settings Tab

Live / Playback Settings	
Max Live Scroll	The maximum number of lines to display in the *POS/ATM Data (Live)* window.
Max Playback Scroll	The maximum number of lines to display in the *Data Search Results* pane of the *Search* window.
Data Storage Settings	
Records of Data Storage	The maximum number of POS/ATM data records to retain in the database.
POS Search History	
Number of Search Items to Keep in History	The number of items to retain in the *Item* drop-down in the *Search* window.

10.3 Email Settings Tab

The *Email Settings* tab allows users to configure email notifications containing filtered POS/ATM Data.
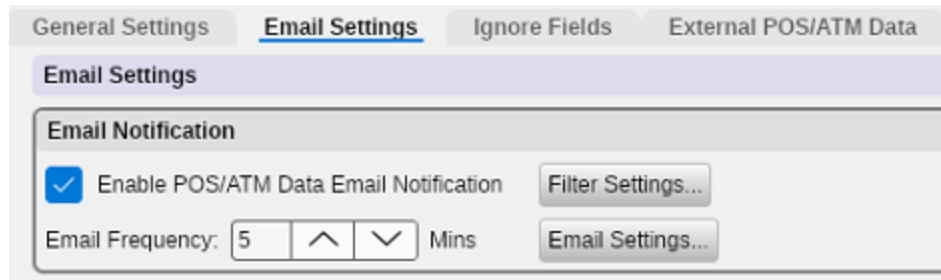
Figure 10-6: Settings - Data Tab - Email Settings Tab

- **Enable POS/ATM Data Email Notification** - When enabled, an email with POS/ATM Data will be sent to specified recipients. POS/ATM Data recorded since the last email and meet the criteria set in *Filter Settings...* are included in the email.

- **Email Frequency** - Specifies the time interval between outgoing emails.

- **Filter Settings...** - Opens the*Data Email Notification Filters* window where you can specify which conditions to filter when sending POS data emails.

> **Note:**Leave the Filter Settings blank to receive POS data email notifications that include all POS/ATM Data since the last sent email.

- **Email Settings...** - Opens the *Email Settings* window, where details for the outgoing email may be entered.

> **Note:**For email options to function properly, a valid SMTP Server must be configured in VIGIL Server *Email Overview Settings* tab.

10.4 Ignore Fields Tab
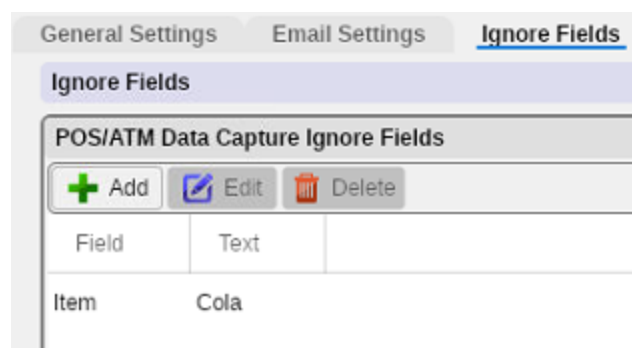
Figure 10-7: Settings - Data Tab - Ignore Fields Tab

The *Ignore Fields* tab allows POS/ATM data records to be ignored in the *POS/ATM Data (Live)* window and POS/ATM Search if they match the specified criteria.

3xLOGIC

Note:POS/ATM data email notifications will not be sent for the items added to the ignore fields list.

Figure 10-8:POS/ATM Data Capture Filter Configuration

- **Field** - Select Item or Code from the Drop-Down menu.
- **Text** - Enter the Text to ignore.

10.5 External POS/ATM Data Tab

This feature reconfigures data display windows for external data source capability and requires a 3rd party interface to operate. The *Priority Cameras* list is *Global* between *Internal* and *External* POS/ATM Data Types.

Figure 10-9: Settings - Data Tab - External POS/ATM Data Tab

11 VSMU – AUDIO TAB

The *Audio* tab allows users to add *Audio Channels* and *Audio Talk Devices* to VIGIL Server and configure how they are recorded. Like footage, audio can be listened to live or via playback using VIGIL Client.
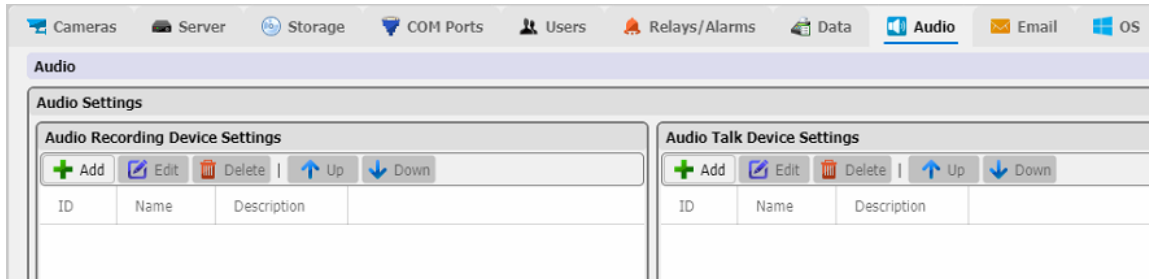
Figure 11-1: Settings - Audio Tab

11.1 Audio Recording Device Settings

Audio Recording Device settings are used to configure *Audio Sources* to be recorded on the VIGIL Server. These can be IP Cameras, IP Audio Devices, Capture Card Inputs or VIGIL Server Sound Card Inputs.

Figure 11-2: Settings - Audio Tab - Audio Settings Window.

> **Note:** Capture card inputs and VIGIL Server audio inputs only require configuration of the *Channel Name* and *Compression*. The form will change to reflect this when either of these types is selected in the *Device* drop-down menu.

■ **Channel Name** - Enter a name for the audio channel. This can be used to describe the location of the audio source.

- **Device** - Select the type of audio device. IP Audio from a supported IP Camera, Capture card inputs or VIGIL Server audio inputs.

- **Use settings from camera** - Enable to use settings from a currently connected IP camera. Some cameras require this option to be used or no audio will record.

- **Type** - Select the type of IP camera.

- **Address** - The IP address of the IP camera.

- **Port** - The Port used on the IP camera.

- **URL** - The camera URL for certain camera types.

- **User Name / Password** - The user name and password for the IP camera.

- **Timeout** - The period of time in seconds before a disconnection is determined to have occurred.

- **Compression** - Select *PCM* for no compression, or *High* for a compression ratio of 16 to 1.

- **Limit Max Storage** - Configure th e maximum amount storage (in days) for audio.

- **Enable Scheduled Audio Recording** - Enables scheduled audio recording. Click the **...** button to open the scheduler (see below). Click and drag across the schedule to confgure recording times. To import a schedule from an existing audio schedule, select the channel in the *Import from Audio Channel* drop-down and click **Import**. To apply the current schedule to all channels, toggle **Apply Schedule to All Audio Channels**.
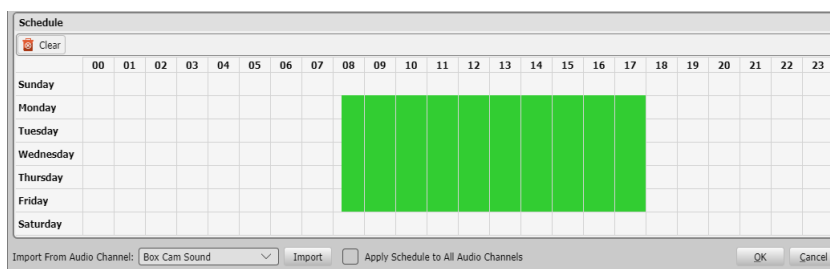

Figure 11-3: Audio Recording Scheduler

11.2 Audio Talk Device Settings

Audio Talk Device settings are used to configure Remote Audio Talk Devices for VIGIL Server to be used with VIGIL Client Audio Talk interface.. These can be IP Cameras or IP Audio Devices.

3xLOGIC

Figure 11-4: Settings - Audio Tab - Audio Talk Device Settings Window

- **Name** - Enter a name for the Audio Talk Device. This can be used to describe the location of the Audio Talk Device.

- **Type** - Select the type of Audio Talk Device. This can be an Audio Talk capable IP Camera or IP Audio Device.

- **Address** - The IP address of the Audio Talk Device.

- **Data Port** - The Data Port used on the Audio Talk Device.

- **RTSP Port** - The RTSP Port used on the Audio Talk Device.

- **User Name / Password** - The user name and password for the Audio Talk Device.

- **Web Settings** - Opens the device's browser UI, if available (dependent on device). Users can edit audio talk settings directly on the device from this UI.

11.3 Live Audio Settings

- **Force to User Software Live** - When enabled, live audio will be routed through the VIGIL Server's audio output instead of the capture card's audio output.   This function is only available with some capture cards.

11.4 Audio Storage Drives

Create and configure *Audio Storage Drives*.

Figure 11-5: Settings - Audio Tab - Audio Storage Drives

Audio Storage Drives are defined in the same way as *Video Storage Drives*. It is recommended that the *Audio Storage Drive* be on a different drive than the *Video Storage Drive(s).*

11.5 Audio Talk / Chat

■ **Audio Device** - Select the audio device that will be used by the VIGIL Server for voice communication in *Audio Talk Mode*. Set to *None* to disable Audio Chat.

11.6 Other Settings - Audio - Recorder Settings

Figure 11-6: Audio Settings - Other Settings - Audio Recorder Controls

Click the **Audio** button under the *Other Settings* portion of the *Audio Settings* form. This will launch the *Recorder Settings* window.
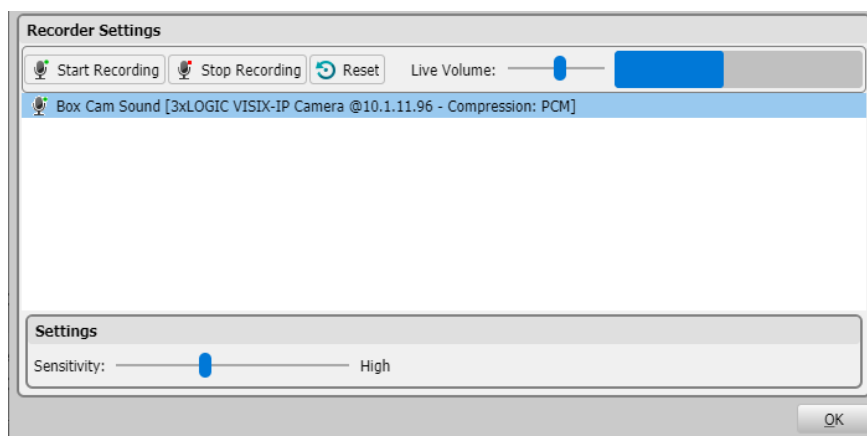
Figure 11-7: Audio Settings - Other Settings - Recorder Settings

From this interface the user can monitor Live Audio for the selected audio channel and view the incoming audio signal to help with sensitivity and volume adjustments. Available channels will be listed under the VIGIL Server node in the bottom portion of the form. The following icons act as recording indicators for the channels:

Indicator	Description
🎤	The channel is currently recording audio.
🎤	The channel is set to record, but there is no audio detected.
🎤	Audio recording has been stopped on this channel.

Adjust *Live Volume* using the slider bar and use the audio visualizer to help preview sensitivity and recording volume. Click the **Audio** button and select **Stop Monitor** to stop monitoring audio. The user can also view audio channel status and to manually stop or start the recording of specific audio channels. See below for descriptions of the available options / controls.

3×LOGIC

- **Start Recording** - Starts recording audio on the selected channel.

- **Stop Recording** - Stops recording audio on the selected channel.

- **Sensitivity** - Controls the sensitivity of the audio detection. Higher sensitivity will trigger audio recording at the slightest noise while lower sensitivity will only trigger audio recording with louder noise. Positioning the slider far left will set the audio channel's record mode to *Always On*. Positioning the slider far-right will set the audio channel's record mode to *Alarm Only.*

- **Reset** - Reset the current configuration to default settings.

12 VSMU – EMAIL OVERVIEW TAB

From the *E-Mail Overview* tab, a user can configure the VIGIL Server's outgoing email settings includ-ing SMTP configuration and e-mail details.

Also available are an *E-Mail Address Master List* and a list of local *Configured Email Recipients.*

Figure 12-1:VIGIL Server Settings - Email Overview Tab

- ■ **SMTP Server Location** - The SMTP Server location.
- ■ **Port** - The E-Mail Server port.
- ■ **Requires SSL** - Check-off this box if SSL certification is required.
- ■ **Requires TLS** - Check-off this box if TLS certification is required.
- ■ **Requires Authentication** - If the Email Server requires authentication, check-off this box and enter the appropriate email / username and password.
- ■ **Default From Name** - The default From name in outgoing emails sent from this VIGIL Server.
- ■ **Default From Address** - The default From Address in outgoing emails sent from this VIGIL Server. *VIGILServer@127.0.0.1* (local host) is used by default, however a custom address can be entered if the correct SMTP Server settings are configured. If SMTP authentication is required for your mail server, the *From*address will be the user name / email that was entered when enabling *Requires Authentication,* regardless of what is entered in this field.
- ■ **Test Email...** - Click this button to test the connection and confirm the details you have con-figured are accurate.

E-Mail Address Masterlist

All e-mail addresses configured on the VIGIL Server will be compiled here. New addresses can also be added from this window. Click *Add* and enter a new address to add another entry to the list. To

edit an existing entry, select it in the list and click the *Edit* button. To delete an existing entry, select it in the list and click *Delete*. Addresses in the masterlist may or may not be configured as an email recipient.

Configured Email Recipients

All email recipients on the VIGIL Server will be compiled in this list alongside information regarding their notifications settings.

E-Mail recipients can also be configured in this list, though the recipient address must exist in the Email Address Masterlist before being added as a recipient.

To disable / enable a recipient, toggle the check-box next to the address entry.

Click *Add* to add a new e-mail recipient. To edit an existing recipient, select the entry from the list and click *Edit.*. To delete an existing entry, select the entry from the list and click *Delete.*

Adding an Email Recipient

When Adding or Editing an e-mail recipient, the Email Notification Recipient Settings window will deploy.

Figure 12-2: Email Notification Recipient Settings Form

When adding or editing an e-mail recipient, the *Email Notification Recipient Settings* window will deploy.

- **E-mail Address** - Select an e-mail address. Addresses must be present in the E-mail Address Masterlist to be added to a recipient.

- **Recipient Type** - Select recipient type. To, CC and BCC are available.

- **Notification Type** - Select the notification type. Available options include: *Video Loss, Video Motion Alarm, POS/ATM Data, Digital Input, V-POS Exceptions, Video Analytics* and *V-POS Event Flag* Each type represents different notification trigger. Recipients can also be added from the appropriate settings form related to your notification type.

- **Camera** - Select the associated camera.

- **Digital Input** - If Notification Type is set to Digital Input, select the input number here.

- **V-POS Exception** - If the Notification Type is set to V-POS Exception, select the configured exception here.

- **V-POS Event Flag** - If the Notification Type is set to V-POS Exception, select the configured flag here.

- **Analytics Rule** - IF the Notification Type is set to Video analytics, select the configured rule here.

Click *OK* to save the new recipient.

3xLOGIC

13 VSMU - DECODERS TAB

✏️ **Note:** The VIGIL Decoder Setup Utility is installed independently of VIGIL Server. The VIGIL Server Settings - Decoder Tab will only appear on systems where the utility has been installed. Contact your 3xLOGIC representative to request the latest available version of the VIGIL Decoder Setup Utility.

From the Decoders tab, a user may launch the VIGIL Decoder Setup Utility.
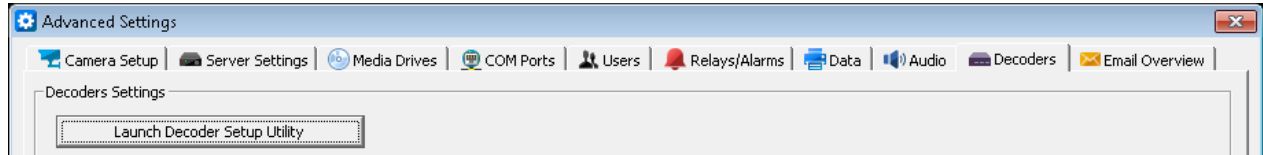
Figure 13-1:VIGIL Server Settings - Decoders Tab

Click the *Launch Decoder Setup Utility* button to launch the utility.

13.1 VIGIL Decoder Setup Utility

After clicking the launch button, the decoder setup utility will deploy. The landing page for the decoder utility is the detected decoder list.
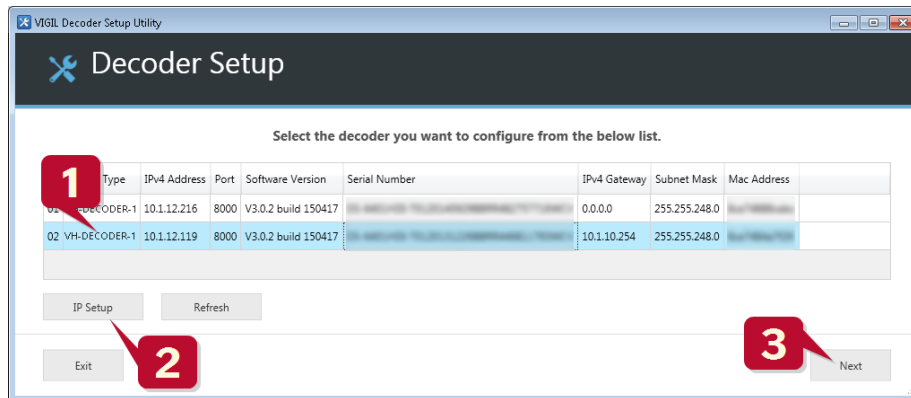
Figure 13-2:VIGIL Decoder Setup Utility - Detected Decoders

The utility will automatically detect VISIX decoders on your network and display them in the list. To update the list, click the *Refresh* button. To activate a decoder, select the desired decoder and click *Activate*. Follow the on-screen instructions to complete the activation process. To configure a decoder's IP settings and camera layout:

1. Select the desired decoder from the list.

2. Click *IP Setup*. A small window will deploy where the user can enter new connection details (IP, Subnet Mask, Default gateway).

3. After selecting the desired decoder and configuring IP settings as desired, click *Next.*

You will be prompted to login to the selected decoder.

4. Enter the login credentials and click *OK* to continue.

The *Camera Settings* window will deploy.

From the Camera Settings window, a user may configure decoder name and output settings and well as monitor layout settings for the camera streams that will be decoded.

Decoder Name	The name that will be assigned to this decoder to identify it throughout the VIGIL suite.
Output Type	Select the output type to use for the decoder. Select between HDMI, BNC or VGA.
Resolution / Video Format	Select the video output resolution. Available options include XGA, SXGA, 720p, 1080p and UXGA.
	When BNC is the selected Output Type, this field will become the Video format field. The user may choose between PAL or NTSC, depending on the requirements of their region.

Warning: JPEG Streams are not currently supported from VIGIL Server Cameras. Only H.264 is currently supported.

After configuring settings as required:

5. Select your desired layout from the right-side layout list.
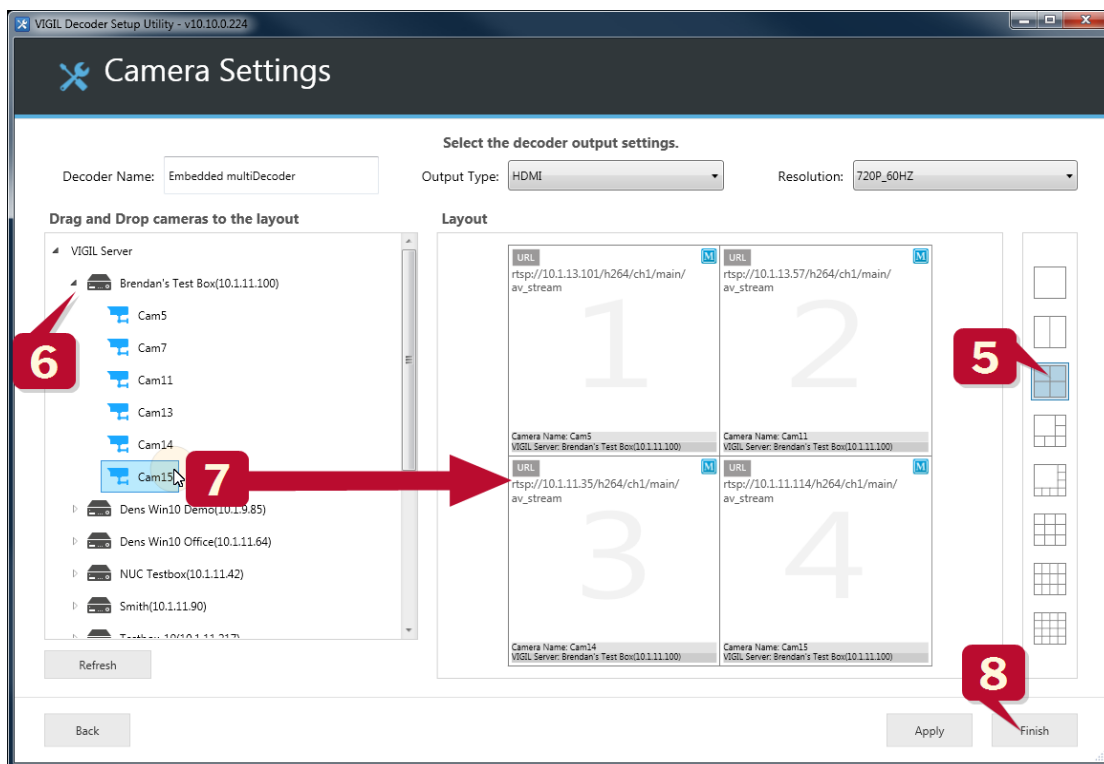
Figure 13-3:VIGIL Decoder Setup Utility - Camera Settings

6. Expand a VIGIL Server or VIGIL Camera nodeand reveal available cameras.
7. Drag desired cameras from the list to the desired layout frame in the preview. A stream URL will be displayed in the frame to indicate which camera stream it will display.
8. When you have configured your desired layout, click *Finish.*

Your streams will now be decoded and should be displayed on a monitor connected to the Decoder via the previously selected *Output Type.*

3xLOGIC

14 VSMU – OPERATING SYSTEM (OS) TAB

The Operating System tab features general settings related to the system's OS.
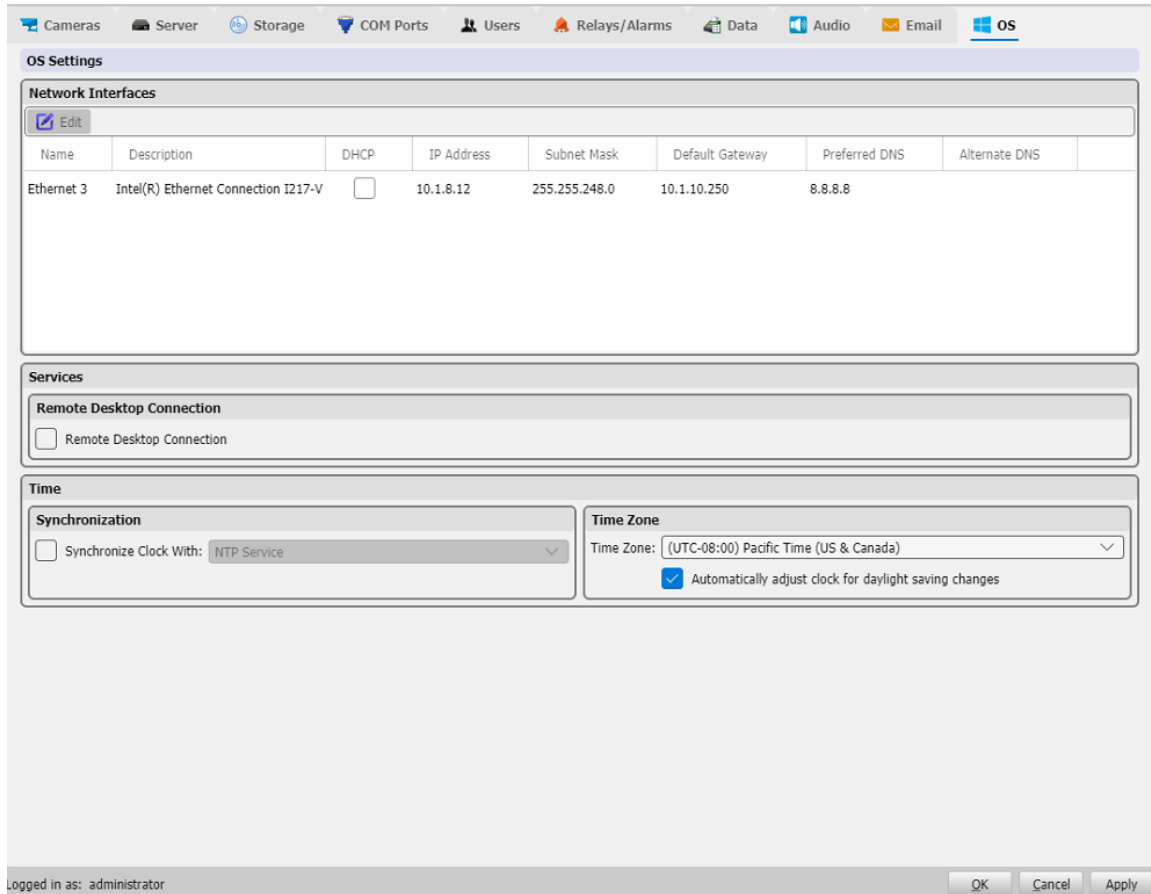
Figure 14-1: VSMU - OS Tab

14.1 Network Interface

To edit system network adapter settings, select the desired NIC from the list and click the *Edit* button. The *Edit Network Interface* window will launch.

Figure 14-2: Edit Network Interface

Fill in adapter settings required. *Name, IP Address, Subnet Mask, Default Gateway, Preferred DNS* and *Alternate DNS* can be configured in this form.

14.2 Services

■ **Remote Desktop Connection** - Enables Remote Desktop for the systme.

14.3 OS Time Settings

■ **Synchronize Clock With** - VIGIL Server can connect to a time server to synchronize the VIGIL Server time. When enabled, you can choose to sync with either an NTP server or to another PC that can respond to a NET TIME request. You must specify which N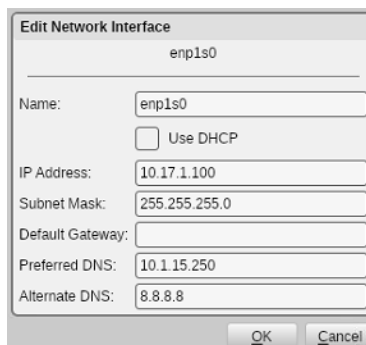TP or NET TIME PC to synchronize with. If the VIGIL Server system's time is off by more than twelve hours, the time will not be synchronized. See below for for descriptions of required fields unique to NTP.

» **NTP Server -** Etner the NTP server's domain name.

» **Sync Frequency** - Set this value (in hours) to configure how often the VIGIL Server will sync with the NTP Server.

» **Initial Sync Time** - Set this value to configure the initial synchronization time. If the *Sync Frequency* value is set to any other value than 24 hours, the initial sync time will only be used for the initial synchronization and any future auto-synchronizations will be performed according to the *Sync Frequency* value.

» **Test NTP** - Attempts to synchronize the time on the VIGIL Server system immediately

Note: The NTP test will not record an event in the Windows Event log if the time is already correct.

■ **Time Zone** - Select the Time Zone for the VIGIL Server.

» **Automatically adjust clock for daylight savings time** - Enable this option to have VIGIL automatically adjuts the clock for daylight savings time.

3xLOGIC

15 ON-BOARD ANALYTICS

When configuring a VISIX Camera with available on-board VCA analytics, the *On-Board Analytics* button will be visible on the *VSMU>Camera Setup >Network Camera Settings* form. Click the **On-Board Analytics** button to launch the *On-Board Analytics* utility.

Figure 15-1: On-Board Analytics Window

This window will display connection information for the camera (automatically populated by VIGIL Server) as well as VCA rules options. It will also list all VCA analytics rules that have been constructed on the camera. VCA rules will populate the *Event Trigger* list. Each component of the *On-Board Analytics* utility is described below.

- **Enabled** - Click this button to enable VIGIL Server to detect on-board analytics rules on the camera.

- **Device Type** - List the type of device / camera being edited or added. If a VCA Server is the desired source of data, select VCA Server from the drop-down menu. The standard On-board Analytics form fields will change when this device type is selected. See "VCA Server" on the next page for more information .

- **HTTP Port** - One of two ports used to connect to the camera's analytics data.

- **Username / Password** - Login credentials are required to sign in to the camera. These fields will be auto-populated by VIGIL Server.

- **Collect Counters** - Enables the collection of data counters

- **Collect Statistics** - Enables the collection of analytics statistics

- **Collected Data is Private** - This feature prevents VIGIL Central Management from acquiring analytics information collected by the camera and will overrule VCM Sync if enabled for a rule / event trigger.

- **Collect Object Data** - Enables the collection of VCA Object metadata. This data can be used in conjunction with VIGIL Client's Analytics Object Reporting.

- **ANPR** - Enables the collection of ANPR data from applicable cameras. This data can be used in conjunction with VIGIL Client's ANPR integration.

VCA Server

If *VCA Server* is selected as the *Device Type*, the following form fields will deploy in place of the standard fields:

- **IP Address** - Enter IP Address of the VCA Server
- **HTTP Port** - Enter HTTP Port number for the VCA Server
- **Username / Password** - Enter login crednetials for the VCA Server
- **Channel** - Select the appropriate channel from the VCA Server. VCA data from this channel will inserted into the VIGIL database.

Event Trigger Configuration

- **Reload from Device** - Reload rules from the connected camera. The rule list will be updated with rules currently configured on the camera.
- **Edit** - Edit the rule's *Display Options* (*Always Show Rule, Never Show Rule, Show Rule When Alarmed*).
- **Enabled** - Click this rule to enable rule data insertion in the VIGIL database. This will be enabled by default.
- **Alarm** - Enable ths option to trigger an alarm in VIGIL Server when the rule is triggered.
- **VCM Sync** - Enable this option to insert event rule data into the VCM Central Analytics datbase (if VCM has been configred to Manage Analytics for the VIGIL Server). If *Collected Data is Private* is enabled for this camera, this setting will be ignored.
- **Name** - The Name of the rule.
- **Display Option** - The current *Display Option* for the rule. Display options can be edited by selecting a rule and clicking **Edit**.
- **Alarm Priority** - Assign a priority level for alarms triggered by this event rule.

Once a rule is added to VIGIL Server, VCA analytics data generated by the rule will be inserted into the VIGIL database. VIGIL Server's VA rule settings can be viewed from the *Camera Setup > Video Analytics tab*. See *"Camera Setup - Advanced - Video Analytics Tab"* on page 40 for more information.

3xLOGIC

16 REGISTRATION

If modules of VIGIL Server are in use during the 30 day trial period, a screen will pop up to remind the user that there are active unregistered modules. The reminder screen will only list modules that are actively being used, pressing *Remind Me Later* will repeat the reminder in 24 hours.

To register VIGIL Server modules, shut down the VIGIL Server software then click the Windows®Start menu and select *Programs >VIGIL > Register* The VIGIL Registration utility will launch.
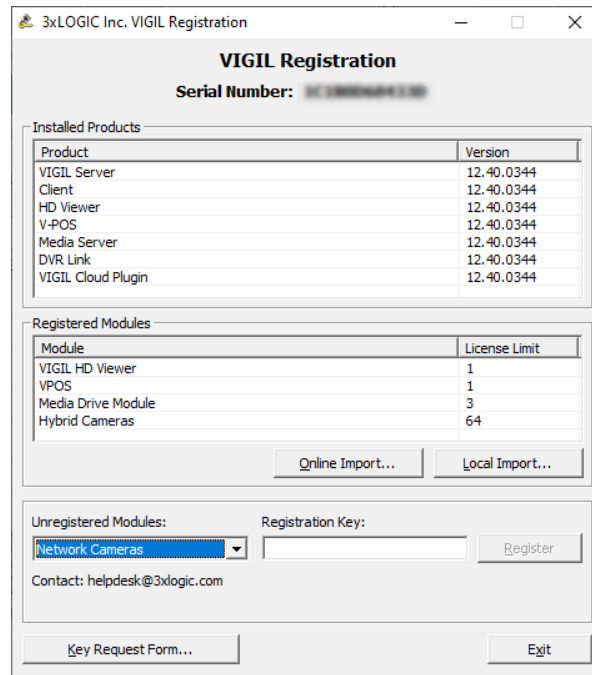
Figure 16-1:VIGIL Registration Utility

16.1 Manual Registration

To manually register modules:

1. Choose the desired module from the *Unregistered Modules* drop-down.
2. Enter the registration key provided to you by your sales representative.
3. Click **Register.**

The registration process for the selected module is complete.

16.2 Auto-Registration

As an alternative to manual reigstration, a user can use **Online Import** to automatically import all keys associated with the system's serial numbera via 3xLOGIC WebReg. Simply click the button and allow the import to complete. Alternatively, you may use an auto-registration XML fileusing the **Local Import** option if you have received one from your sales representative . To use a local xml file.

1. Click the **Local Import** button.
2. Locate the file .xml license file in the available file explorer and click **Open.**

All modules associated with the.xml file will now be automatically registered.

16.2.1 Requesting Registration Keys

If you have yet to receive registration keys, keys can be requested. To request keys:

1. Click the **Key Request Form...** button
2. Check-off the appropriate modules for which you require registration keys and click **Save**.
3. Send the resulting .xml file to your 3xLOGIC sales representative.

The representative will contact you to complete the transaction and will provide you with the appropriate keys for the auto-registration XML file.

16.3 Re-Registering Upgraded Modules

e.g. **Example:** A VIGIL Server system currently has 8 Network Camera Channels licensed and registered. The VIGIL Server's owner has purchased a new 8 Network Camera Channel license to double the VIGIL Server's camera capacity to 16. The owner has been supplied the appropriate registration key for the new license by their sales representative. The below steps must be followed to successfully re-register the upgraded module to allow for access to the new camera channels.

To re-register an upgraded module:

1. Select the module from the *Registered Modules* list and press the **Delete** key on the keyboard to remove the original module.
2. Re-select the module from the bottom *Unregistered Modules* list. Enter the upgraded module's new license key and click **Register**. If you have been provided an .xml license file, you can use the alternate auto-registration method (outlined in Section 1.2 of this tech tip) to complete registration.
3. Launch VIGIL Server.

The re-registered module will now be active. If the VIGIL Server software was not shut down during registration, a software restart is required for changes to take effect.

3xLOGIC

17 TOOLS

Several secondary tools can be accessed from the system tray icon right-click menu or the *Start Menu>Programs>VIGIL* folder. These tools can be used to view important connection and usage information about the VIGIL Server. Tools outlined in the proceeding sections are listed below.

17.1 Client Connections

The *Client Connections* window displays a list of current connection activity from other applications, for example VIGIL Client stations. To open the *Client Connections* window, select the *Client Connections* option from the VIGIL Server Quick Tray icon's right-click menu.

The table provides the following information: the client's remote host IP address or name, the remote host connection port, the locally connected port and the last activity time of the connection.

Remote Host	Remote Port	Local Port	Last Activity
206.116.106.153	52768	22802	2023-05-04 08:50:08
206.116.106.153	60561	22802	2023-05-04 08:50:08
206.116.106.153	53082	22802	2023-05-04 08:50:07
206.116.106.153	60559	22802	2023-05-04 08:50:07
10.1.11.14	56455	22802	2023-05-03 11:14:18
10.1.11.14	56456	22802	2023-05-03 11:14:18
10.1.11.14	56457	22802	2023-05-03 11:14:18

Figure 17-1: Client Connections Report

17.2 Network Log Analyzer

The *Network Log Analyzer* provides a simple way to check for network activity of VIGIL software. It will log IP addresses and VIGIL user names of all connections made. To open the *Network Log Analyzer*, right-click the VIGIL system tray icon and selectt *Network Log Analyzer.*

17.3 Audit Log Analyzer

The *Audit Log Analyzer* provides a way to analyze, search and monitor various errors and general information for the VIGIL Server software. Essentially, it allows you to search the logs by using a variety of criteria such as date / time, error code, IP address, or module

To open the *Audit Log Analyzer,* right-click the VIGIL system tray con and select Audit Log Analyzer.

Search sorting and filter tools as well as search filter criteria make up the top portion of the analyzer. After performing a search, the bottom portion will be populated with a list of log entries matching your search criteria and filters.
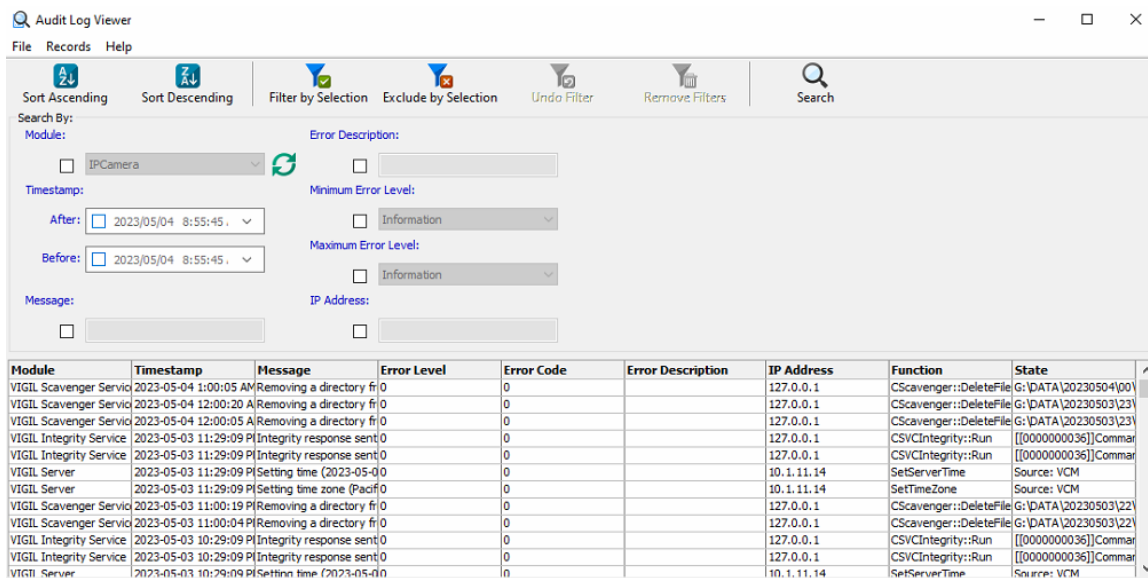

Figure 17-2:VIGIL Server Audit Log Analyzer

- ■ **Sort Ascending** - Sort log entries from newest to oldest.
- ■ **Sort Descending** - Sort log entries from oldest to newest.
- ■ **Filter by Selection** - Search only for log entries of the currently selected log entry type.
- ■ **Exclude by Selection** - Exclude the currently selected log entry type from the search.
- ■ **Undo Filter** - Exclude the currently selected log entry type from the search.
- ■ **Redo Filter** - Redo the last used filter.
- ■ **Search** - Perform a search of the audit log.
- ■ **Search By** - A list of search criteria the user may use to narrow down their audit log entry search. Criteria includes: *Module, Timestamp (Before and/or After) Message, Error Description, Minimum Error Level, Maximum Error Level, IP Address.*

For descriptions of the different log entries you may encounter, see *Tech Tip 160017 VIGIL Server - Audit Log Legend.* Contact 3xLOGIC support to receive the latest revision of TT 160017.

3xLOGIC

17.4 VIGIL Server System Database Utility

The VIGIL Server System Database Utility is an advanced management utility for data drive and database management.

Warning: If your VIGIL Server is experiencing issues, please contact your system administrator or 3xLOGIC technical support before using the database manager utility. Please See "Contact Information" on page 120

The VIGIL Server System Database Utility contains features that may cause a system failure or other undesired effects if operated incorrectly. Only advanced users with an understanding ot eh VIGIL database should use this utility.

The utility can be launched from *Start>Programs>VIGIL>Database Manager*. You will have to login to the utility before being able to modify any settings; a VIGIL administrator account must be used.

Figure 17-3: Database Utility Login Window

17.4.1 Drive Management Tab

In the *Drive Management* tab, three types of media drives can be set up: *Video Storage Drives, Alternate Video Storage Drives* and *Audio Storage Drives*. VIGIL Server must be shut down to make changes on this Tab.
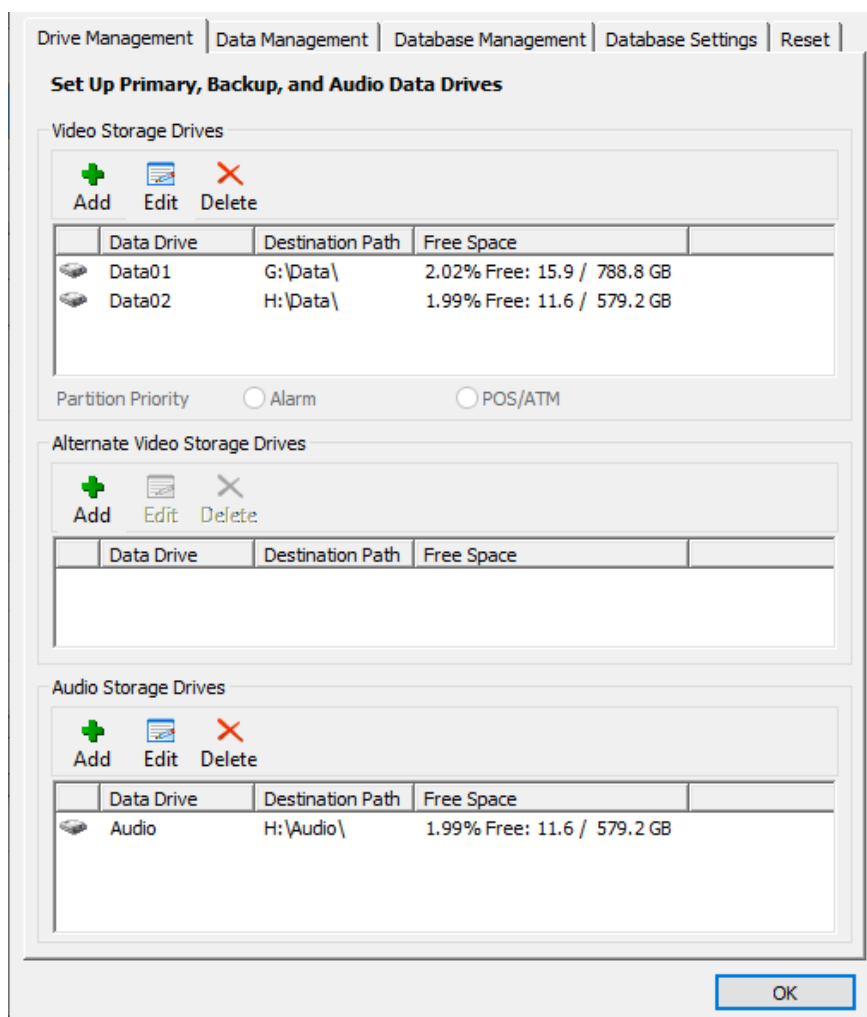

Figure 17-4: VIGIL Server Database Utility

- ■ **Video Storage Drives –** Video Storage Drives are the main drives where video footage is stored. If all of the Video Storage Drives are offline, the Alternate Video Storage Drives will be used until the Video Storage Drives return online.

- ■ **Alternate Video Storage Drives –** Alternate Video Storage Drives are emergency backup drives that are used only if all of the Video Storage Drives are offline. If an Alternate Video Drive is being used, the VIGIL Server will beep and a warning message will be displayed. When the Video Storage Drives return online, a warning message will disappear, the audio alarm will stop beeping, and the VIGIL Server will switch back to recording to the main Video Storage Drives.

- ■ **Alternate Video Storage Drives –** Alternate Video Storage Drives are emergency backup drives that are used only if all of the Video Storage Drives are offline. If an Alternate Video Drive is being used, the VIGIL Server will beep and a warning message will be displayed. When the Video

3xLOGIC

Storage Drives return online, a warning message will disappear, the audio alarm will stop beep-ing, and the VIGIL Server will switch back to recording to the main Video Storage Drives.

- **Audio Storage Drives –** Audio Storage Drives are the drives where audio data is stored.

17.4.2 Data Management Tab

Maintenance operations on the VIGIL Server Database can be performed on this tab. These operations can be performed while VIGIL Server is running.

Purge Data

To purge data:

1. Select the type of data you wish to purge; *Video / Audio Footage, POS Data* or *Video Analytics Data*.

2. Specify a date range in the **From** and **To** boxes or toggle **Purge All** on.

3. Click the **Purge** button to purge the selected data.

Figure 17-5: Database Utility - Data Management Tab - Purge Data Options

Note:VIGIL Server is designed to manage the purging of data; it will delete the oldest hour of video footage or the oldest POS / Video Analytics Data automatically before the data drives become full. Under normal operating conditions, there is no need to manually purge Data.

Warning: This is a permanent deletion of the data itself.

Rebuild Database

The *Rebuild Database* feature rebuilds the database entries for all of the footage on the selected drives. To rebuild the database:

1. *Click the* **Rebuild** *button*

2. Select the drive(s) to rebuild.

3. Click **OK** to rebuild the selected drives.

During the rebuild process the Sentinel 'No Footage Recorded within the last 24 hours' warning may appear, this is expected as the database of the footage is being rebuilt.

You may choose the utilities post-rebuild action by checking *When The Rebuild is Completed Successfully*: and choosing either *Close this Utility* or *Automatically Reboot the Server*.
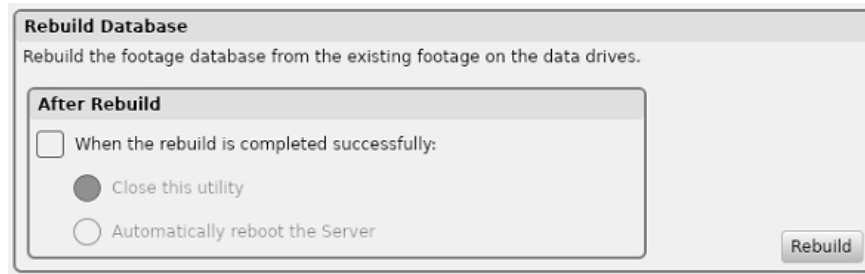
3xLOGIC

Figure 17-6: Database Utility - Data Management Tab - Rebuild Database Options

Reset Initial Footage Date

The VIGIL Server Health Monitor software uses the initial footage date in VIGIL Server to determine if the VIGIL Server is recording the proper number of days of video storage.

■ Click the *Reset* button to reset the cached date of the first video footage recorded by the VIGIL Server to the oldest footage currently on the VIGIL Server. Please refer to the VIGIL VCM software Users Guide Health Monitor section, or contact 3xLOGIC for more information.
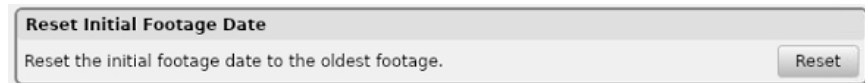
Figure 17-7: Database Utility - Data Management Tab - Reset Initial Footage Date

Clear Last Scavenged Folder Details

Figure 17-8: Database Utility - Data Management Tab - Clear Last Scavenged Folder Details

The VIGIL Server Health Monitor software uses the Last Scavenged Folder details in VIGIL Server to determine if the VIGIL Server is scavenging footage too early. A warning in VCM will be displayed when this occurs.

■ Click the *Reset* button to reset the last scavenged folder details in VIGIL Server and clear the related warning in VCM Health Monitor.

17.4.3 Database Management Tab

The Database Management Tab allows for configuration and maintenance of the VIGIL Server Database.

Backup / Restore Database

Creates a backup image of the video footage database or restores the database from an existing backup image. Click the *Browse* button to select the image folder. Click *Backup* to backup the database in the selected folder. Click *Restore* to restore the database from the backup image in the selected folder.
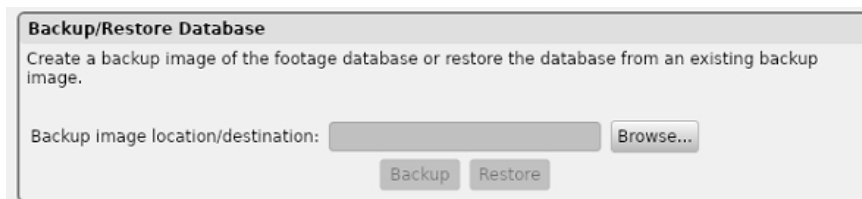
Figure 17-9: VIGIL Server Database Utility -Database Management Tab - Backup / Restore Database Settings

Database Performance

In the case that the database index becomes corrupt, the *Database Performance* feature will repair the index files and compact the memory usage of the video footage database to tune its performance.
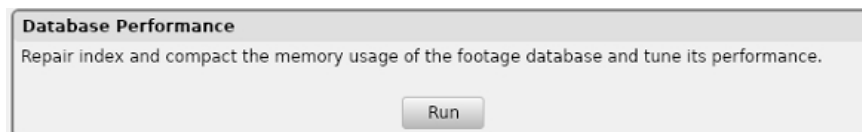
Figure 17-10: VIGIL Server Database Utility - Database Management Tab - Database Performance

Database Integrity

Runs an integrity health check on the VIGIL Server database. If errors are found, the user will be presented with available repair options. This tool is helpful database integrity issues are suspected to be causing poor VIGIL Server performance.
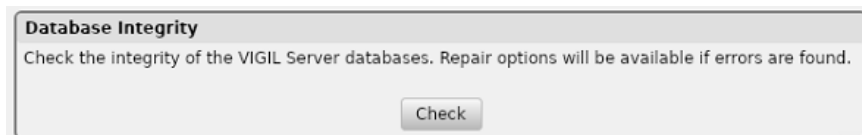
Figure 17-11: VIGIL Server Database Utility - Database Management Tab - Repair Database Settings

17.4.4 Database Settings Tab

The *Database Settings* tab is used to change settings within the VIGIL Server database.

Local Database Administrator Password Settings

Figure 17-12: Database Settings Tab - Local Database Administrator Password Settings

To change the SQL Server Administrator account (sa) password, enter the old password, new password and lick Set Password.
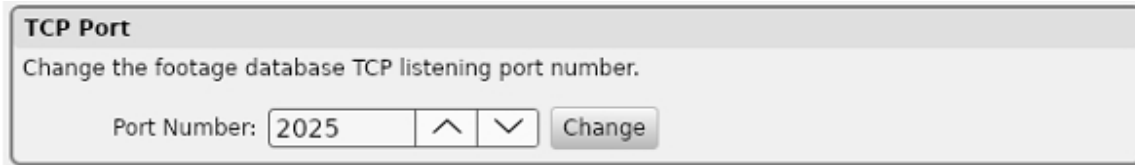
3xLOGIC

TCP Port

Figure 17-13: Database Settings Tab - TCP Port Settings

Enter in the desired port number and click Change to change the listening TCP port number of the SQL Server database.

Local Database Memory Usage

Figure 17-14: Database Settings Tab - Local DB Memory Usage Settings

The *Database Memory Usage* section is used to limit the amount of memory used by the local SQL database. This will not affect the disk space usage of the database - only the memory usage. Minimum memory usage should always be set to 0 MB. Maximum memory usage should be set according to the amount of memory installed in the VIGIL Server (see table below). Setting the appropriate maximum memory usage level for the VIGIL Server will improve VIGIL Server performance. To change the maximum memory usage, drag the slide bar to the appropriate MB amount. Check *Adjust SQL Server Memory Automatically* checkbox to have the memory set automatically.

MB of RAM Installed in VIGIL Server	Max MB of Memory Usage Recommended
512MB	250MB
1024MB	700MB
2048Mb	1536Mb

17.4.5 Reset Tab

This tab contains a button that will initiate a full data wipe and settings restore for the VIGIL Server.

Warning: This button shuts down services, purges all data, recreates all databases and clears key portions of the registry to return the VIGIL software to its factory state. Please make appropriate backups before proceeding.
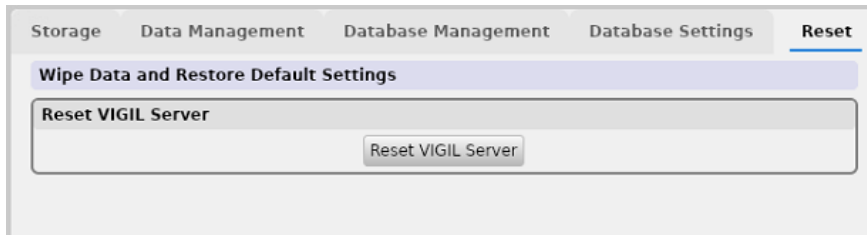
Figure 17-15:VIGIL Database Manager - Reset

17.5 VIGIL Server Backup Utility

The *VIGIL Server Backup Utility* allows administrators to backup large amounts of recorded video footage to a local hard drive or DVD.
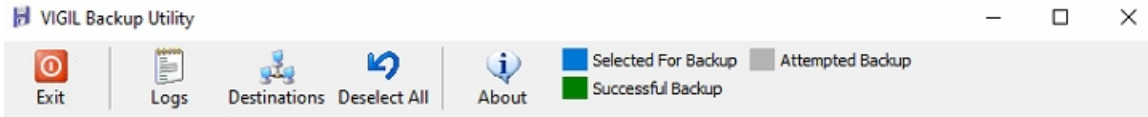

Figure 17-16:VIGIL Backup Utility

- **Exit** - Close the *VIGIL Server Backup Utility*.

- **Logs** - Open the *Backup Log* window, where a user may search for backups.

- **Destinations** - Opens the *Destinations* window, where backup destinations can be added, edited, deleted or prioritized. At least one backup destination must be configured for the *Backup* button to become available.

- **Deselect All** - Deselects all highlighted dates in the main *VIGIL Server Backup Utility* window.

Figure 17-17:VIGIL Backup Utility - Date Selection

Select dates to backup by clicking the appropriate date on the calendar. Dates selected for backup are highlighted in blue. Dates that have been successfully backed up are highlighted in green. Dates with backups that have failed are highlighted in grey. Selecting successful backups (highlighted in green, above) on the calendar will reveal information about the backup

Footage Start	Footage Ends	User	Export Date	Media Serial #	Destination
2023-05-05	2023-05-05	administrator	2023-05-06	AADFF0EA	Z:\

Figure 17-18:VIGIL Backup Utility - Backup Log

Backing up Server is as simple as selecting a destination and running the utility.
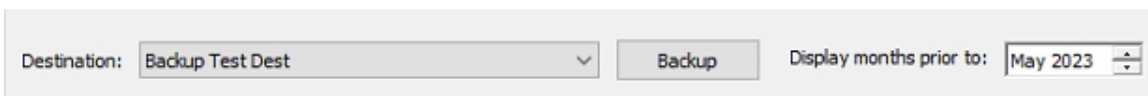

Figure 17-19:VIGIL Backup Utility - Settings

- **Destination** - Select the backup destination from the drop-down list. Destinations must be configured in the *Destinations* window to appear in this drop-down.

- **Backup** - Click *Backup* to begin the backup process.

- **Display Months Prior to:** - The Calendar displays one year prior to the month selected here.

17.6 VIGIL Update Utility

Use the VIGIL Update Utility to locate files locally and update your VIGIL system using VGL update files. The utility can be launched via *Start Menu>Programs>VIGIL> Update*.
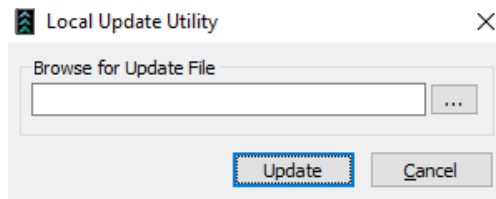

Figure 17-20:VIGIL Local Update Utility

To perform an update:

1. Click the *...* button to open the file explorer. Locate the file, open it and click *Update* in the utility to perform the update. Follow the on-screen instructions to complete the update.

17.7 v500 Analog PoE Settings Utility (Legacy)

This utility will auto-run on applicable (VIGIL v500, etc...) systems and be opened from the system tray. The utility is used to check the status of the different PoE ports on systems with an internal PoE NIC card. Utility functions are as follows:

Note: The appearance of the utility may very depending on the NVR on which its installed.
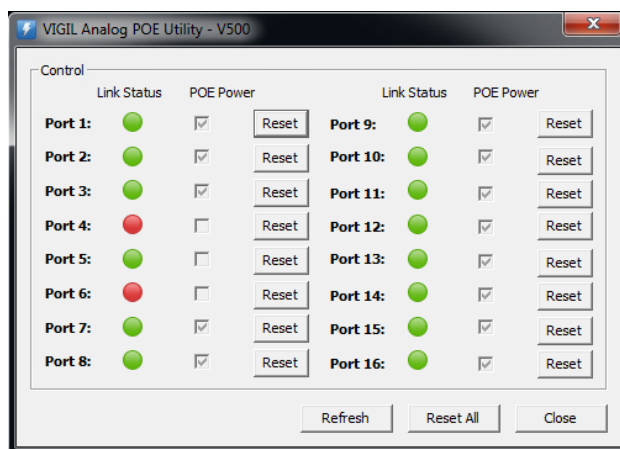

Figure 17-21:VIGIL Analog POE Utility

» If a camera is plugged into a PoE port, the *Link Status* indicator will be green. If a port is unused, the indicator will be red. On some NVRs, status indicators will be replaced by simple "Online" or "Offline" text.

» The *POE Power* check box indicates if a connected camera is currently utilizing PoE.

» Click the **Reset** button on a desired port to cut and restore power, effectively forcing a camera reset.

3xLOGIC

17.8 Settings Utility

The *Settings Utility* is used to export and import VIGIL Server settings to other VIGIL Servers. The exported files will include all settings found in the *VIGIL Server Settings* window.
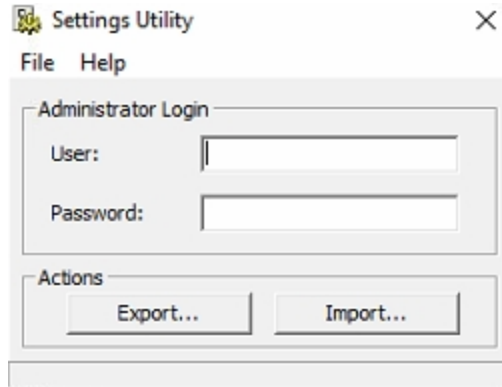

Figure 17-22:VIGIL Server Settings Utility

Enter an administrator username and password to use the *Export* and *Import* features. The administrator account must exist on the local VIGIL Server.

- **Export** - Click the *Export* button to export the current VIGIL Server settings.
- **Import** - Click the *Import* button to import VIGIL Server settings from a previously exported settings file

Warning: A settings import will erase all existing VIGIL Server settings. Please check that *Media Drives* settings are correct after performing an import.
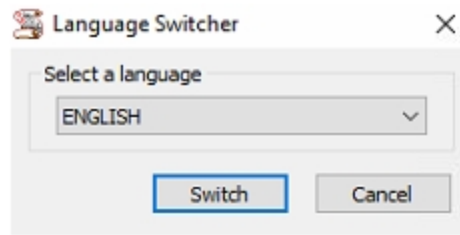
17.9 Language Switcher

Figure 17-23:VIGIL Language Switcher

VIGIL Server can be run in English, French, Spanish, Chinese and Hebrew. The *Language Switcher* can be run from the Windows Start menu.

To begin:

1. Select *Programs > VIGIL> Language Switcher*.
2. Select the desired language from the drop-down menu and click *Switch*.

A prompt will show informing that a system reboot is required to complete the language change. Choose the following:

■ Click *Yes* to reboot immediately.
■ Click *No* to have the update applied the next time the system is restarted.

Note: The prompt will display in the language that is being switched to.

3xLOGIC

18 CONTACT INFORMATION

3xLOGIC has offices in Victoria BC, Canada and in Fishers, Indiana, USA. Please visit our 3xLOGIC web site at www.3xlogic.com. Please contact us by e-mail at helpdesk@3xlogic.com (technical support), or using the following contact information:

3xLOGIC Technical Support:

Toll Free:(877) 3XLOGIC
(877) 395-6442
Email:helpdesk@3xlogic.com
Website:www.3xlogic.com

3xLOGIC USA Main Office:

11899 Exit 5 Parkway, Suite 100
Fishers, IN 46037
United States. (303) 430-1969