3xLOGIC

VIGIL
Server 11.5
Video Management Software Service
User Guide

Revised: July 23rd 2020

3xLOGIC Inc.
11899 Exit 5 Parkway, Suite 100
Fishers, IN 46037
United States. (303) 430-1969

Disclaimer
Information in this document is subject to change without notice and does not represent a commitment on the part of 3xLOGIC Inc. The software and/or databases described in this document are furnished under a license agreement or nondisclosure agreement. They may be used or copied only in accordance with the terms of the agreement. It is against the law to copy the software on any medium except as specifically allowed in the license or nondisclosure agreement. The purchaser may make one copy of the software for backup purposes. No part of this manual and/or databases may be reproduced or transmitted in any form or by any means, electronic or mechanical, including (but not limited to) photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, without the express written permission of 3xLOGIC Inc.

Table of Contents

1 Introduction

This guide describes the operation of 3xLOGIC’s VIGIL Server Software Service.

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 v11.50.0000, 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).

The following guide will familiarize you with the software interface and its many features but do not hesitate to contact us with any questions, concerns or suggestions, See "Contact Information" on page 122

Welcome to 3xLOGIC's VIGIL Server.

This user guide is current as of VIGIL Server 11.50.0000.

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.

2 Software Features

This section describes some of the features of VIGIL Server.

Feature	Details
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, noise reduction, and more.
IP Camera Support	VIGIL Server supports up to 64 IP hi-resolution cameras 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.
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, 3xCLOUD 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 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 VIGIL Server, right-click the V VIGIL Server System Tray icon .

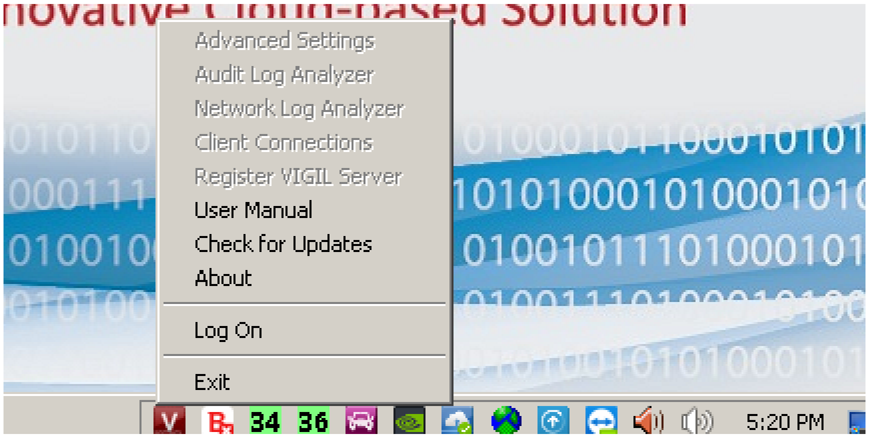


Figure 3-1:VIGIL Server Sysem Tray Icon- Right-Click Menu

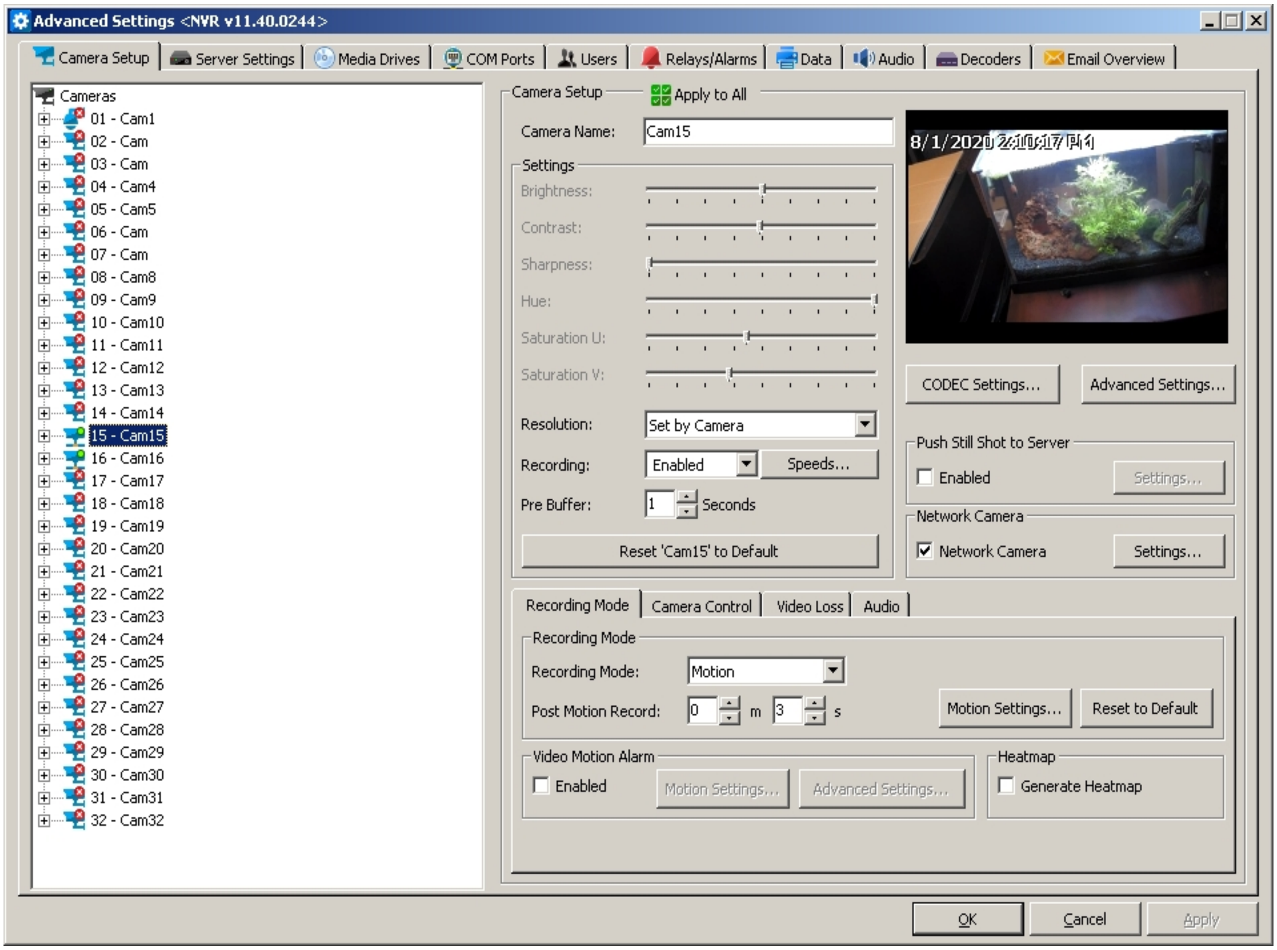
All options will be inaccessible (except *User Manual*, *Check for Updates* and *About*) until the user has logged into VIGIL Server. Click **Logon**, enter your user credentials and click **Login**. All tray icon menu items will now be accessible.

Menu Option	Description
Advanced Settings	Opens the *Advanced Settings* window. All available settings are described in the proceeding sections of this user guide.
Audit Log Analyzer	Open the *Audit Log Analyzer*. See "Audit Log Analyzer" on page 106 for more information.
Network Log Analyzer	Open the *Network Log Analyzer.*
Client Connections	Open the *Client Connections* window. See "Client Connections" on page 106 for more information.
Register VIGIL Server	Open VIGIL Registration Utility. See "Registration" on page 110 for more information.
User Manual	Launch the VIGIL Server User Guide.
Check for Updates	Launches the VIGIL Remote Updater. Please see the latest version of the VIGIL Remote Updater User Guide for more information.
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.
Log On / Log Off	Log on or off of the VIGIL Server.
Exit	Quit the VIGIL Server application.

4 Advanced Settings – Camera Setup Tab

VIGIL Server is a diverse software application that interfaces with a wide variety of hardware configurations. A comprehensive set of customization controls is available to configure the VIGIL Server as required. This section will describe the available settings in detail.

To access settings, right-click the system tray VIGIL icon and select **Advanced Settings**. The *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.



Advanced Settings <NVR v11.40.0244>

Cameras
01 - Cam1
02 - Cam
03 - Cam
04 - Cam4
05 - Cam5
06 - Cam
07 - Cam
08 - Cam8
09 - Cam9
10 - Cam10
11 - Cam11
12 - Cam12
13 - Cam13
14 - Cam14
15 - Cam15
16 - Cam16
17 - Cam17
18 - Cam18
19 - Cam19
20 - Cam20
21 - Cam21
22 - Cam22
23 - Cam23
24 - Cam24
25 - Cam25
26 - Cam26
27 - Cam27
28 - Cam28
29 - Cam29
30 - Cam30
31 - Cam31
32 - Cam32

Camera Name: Cam15

Resolution: Set by Camera

Recording: Enabled

Pre Buffer: 1 Seconds

Push Still Shot to Server: □ Enabled

Network Camera: ☑ Network Camera

Recording Mode: Motion

Post Motion Record: 0 m 3 s

Video Motion Alarm: □ Enabled

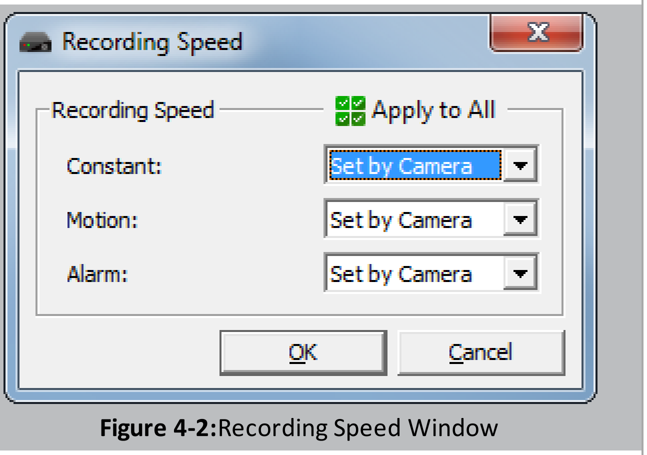
Heatmap: □ Generate Heatmap

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.

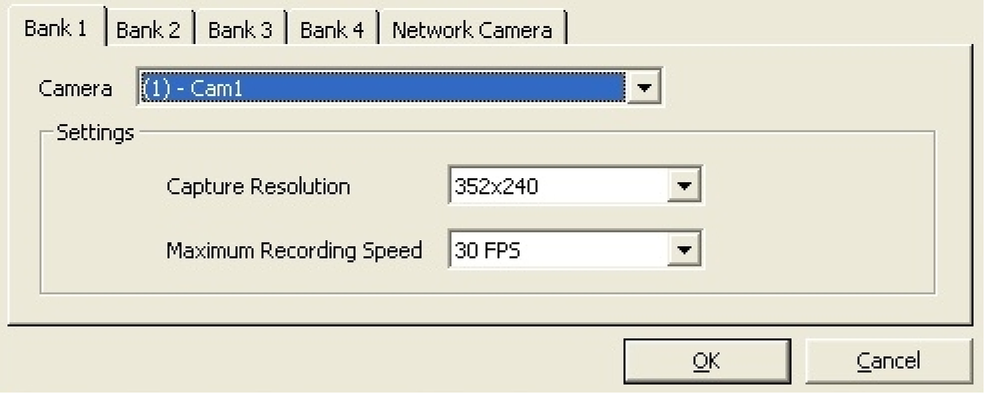
Apply to All	Click the *Apply to All* button at the top of the window to apply the same settings to all cameras. Settings that will be applied to all cameras will be indicated by **BOLD** headings. **Note:** Only changes made after clicking *Apply to All* will be applied to every camera.

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.
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.
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.  Recording Speed Recording Speed Constant: Set by Camera Motion: Set by Camera Alarm: Set by Camera **Figure 4-2:**Recording Speed Window
Reset 'Cam#' to Default	Returns the camera settings to their default values.

4.1.1 Advanced Settings

In the *Advanced Settings* window, the cameras are grouped into *Bank* tabs that represent the physical camera banks in the VIGIL Server. This allows the user to maximize the capture resolution and recording speeds for each camera bank. When the number of FPS is changed in the *Advanced Settings* window, it is applied to all recording modes.



Camera: (1) - Cam1

Settings

Capture Resolution: 352x240

Maximum Recording Speed: 30 FPS

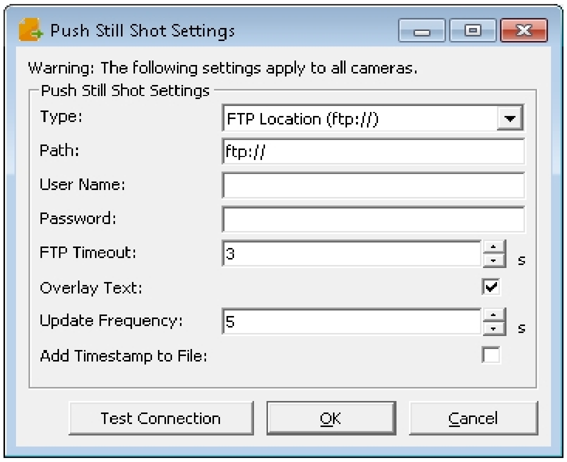
Figure 4-3: Advanced Settings - Camera Banks

Note: The number of banks and the cameras in each bank is determined by the capture card installed, which cannot be configured. There are many possible layouts of banks and channels per bank.

Camera	Select a camera number within the current *Bank* tab to change its settings.
Capture Resolution	Select the desired recording resolution from the drop-down menu.
Recording Speed	Select the desired number of frames per second. Each bank has a set amount of FPS that can be set to its cameras. Values will change depending on the recording speeds for other cameras within the same bank.
Network Camera Tab	Network cameras are automatically detected and the analog feed is disabled for that camera number. Network camera speeds are independent of other cameras and do not change the maximum allowable FPS for cameras belonging to the same camera bank.

4.1.2 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.



Warning: The following settings apply to all cameras.

Push Still Shot Settings

Type: FTP Location (ftp://)

Path: ftp://

User Name:

Password:

FTP Timeout: 3 s

Overlay Text: ☑

Update Frequency: 5 s

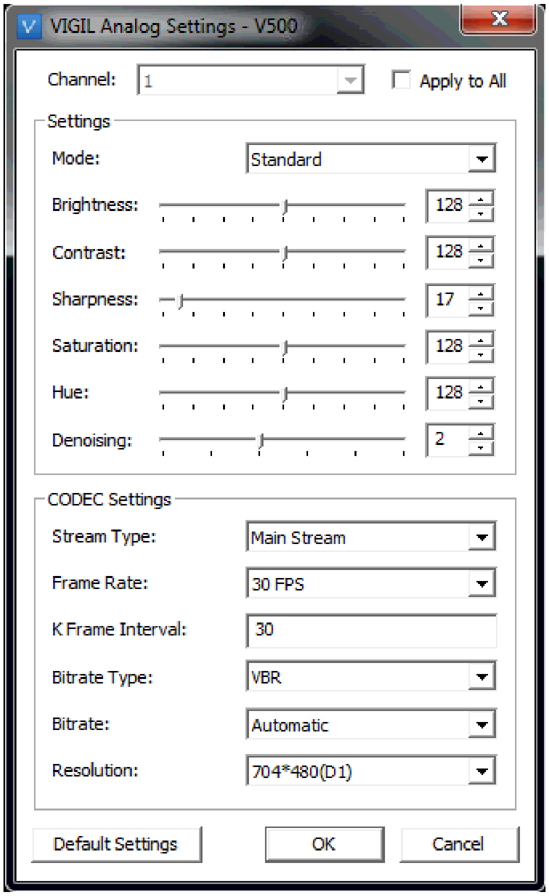
Add Timestamp to File: ☐

Figure 4-4: 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 Directory**:C:\Images. **Network Directory**: \\*ComputerName**SharedFolder*. **FTP site**: 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.

4.1.3 VIGIL Analog Settings Utility

On some capture card systems (3xLOGIC's v250 Hybrid, v500, etc…), the Camera Settings section of the Camera Setup tab will be replaced with an *Analog Settings* button. Click the *Analog Settings* button to launch the VIGIL Analog Settings Utility (pictured below).



Channel: 1

□ Apply to All

Settings

Mode: Standard

Brightness: 128

Contrast: 128

Sharpness: 17

Saturation: 128

Hue: 128

Denoising: 2

CODEC Settings

Stream Type: Main Stream

Frame Rate: 30 FPS

K Frame Interval: 30

Bitrate Type: VBR

Bitrate: Automatic

Resolution: 704*480(D1)

Figure 4-5:VIGIL Analog Settings Utility

The Channel option will reflect the camera channel which was selected when the utility was launched.. Toggle *Apply to All* to enable global analog settings.

Available settings include standard analog image settings (*Brightness, Contrast, Sharpness, Hue* and *Saturation*). The *Denoising* level can also be set to a custom value between 1-256. Select a pre-configured settings*Mode* from the available drop-down menu. Available modes include Standard, Indoor, Outdoor. Alternatively, select *Custom* as the *Mode* and configure the settings as desired.

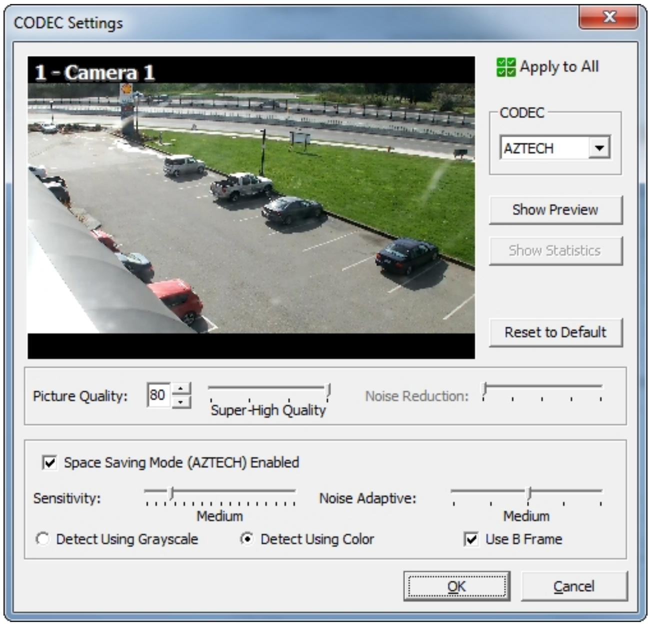
The bottom portion of the utility interface features CODEC Settings for the selected channel.

CODEC Setting	Description
Stream Type	Select the stream type you would liek to edit the CODEC settings for. Options include *Mainstream* and *Substream*.
Frame Rate	Set the selected stream's frame rate. Available values (in FPS) are 30, 20, 16, 12, 10, 8, 6, 4, 2 and 1.
K Frame Interval	Set the selected stream's K-Frame Interval rate. The default rate is 30.
Bitrate Type	Set the stream's bitrate type. Available options are *VBR* and *CBR.*
Bitrate	Select the stream's bitrate. Automatic is selected by default but available static options range from 320K - 16384K.
Resolution	Select the stream's resolution. Available options will depend on the camer associated with the selected channel.

4.2 CODEC Settings

The *CODEC Settings* window allows advanced configuration of the recording CODEC used for storing video footage recorded on analog cameras.

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



CODEC: AZTECH

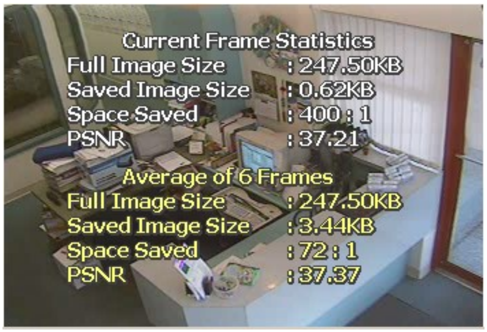
Picture Quality: 80 Super-High Quality Noise Reduction:

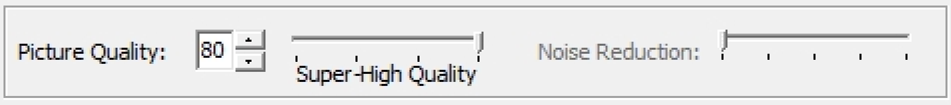
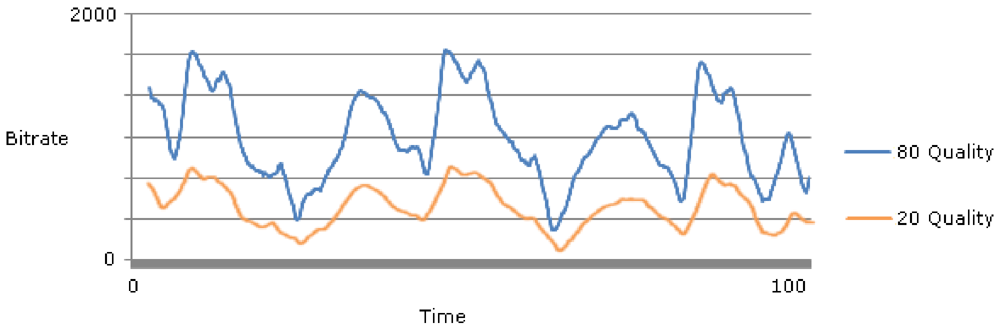
☑ Space Saving Mode (AZTECH) Enabled

Sensitivity: Medium Noise Adaptive: Medium

○ Detect Using Grayscale ● Detect Using Color ☑ Use B Frame

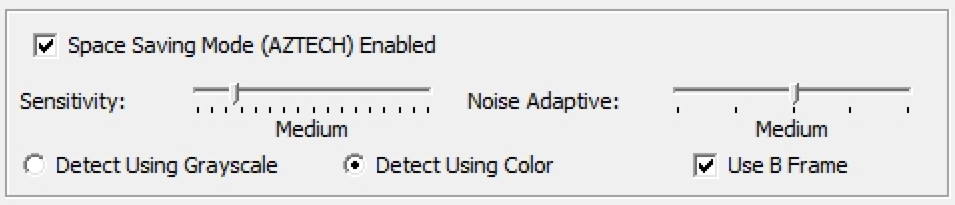
Figure 4-6:CODEC Settings

Apply to All	Click the *Apply to All* button at the top of the window to apply the same CODEC settings to all cameras. Settings that will be applied to all cameras will be indicated by **BOLD** headings. Only changes made after clicking *Apply to All* will be applied to every camera.	
CODEC	Select between AZTECH and MPEG encoding. **Note:**Normally, two video encoding CODECs are currently available for recording video footage: *AZTECH and MPEG4 CODECs*. However, some models support Hardware CODECs, which have slightly different customization options.	
Show Preview	Plays the camera footage as it encodes the preview window with the settings that are configured.	
Show Statistics	 Current Frame Statistics Full Image Size : 247.50KB Saved Image Size : 0.62KB Space Saved : 400 : 1 PSNR : 37.21 Average of 6 Frames Full Image Size : 247.50KB Saved Image Size : 3.44KB Space Saved : 72 : 1 PSNR : 37.37	If *Show Preview* is enabled, *Show Statistics* can also be clicked to display compression statistics on the preview window.

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.  Picture Quality: 80 Super-High Quality Noise Reduction: How Picture Quality Can Affect Total Disk Usage: 
Noise Reduction	Adjusts the level of video noise for grainy video.

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.



☑ Space Saving Mode (AZTECH) Enabled

Sensitivity: Medium

Noise Adaptive: Medium

○ Detect Using Grayscale ● Detect Using Color ☑ Use B Frame

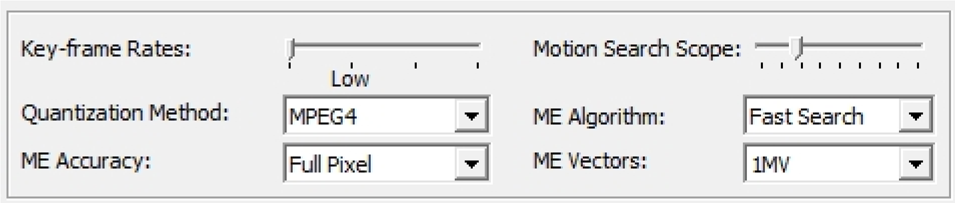
Figure 4-7:AZTECH CODEC Settings Tab

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 Gray-	Determines whether grayscale or color will be used to detect changes.

scale/ Color	**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.



Key-frame Rates: Low

Motion Search Scope:

Quantization Method: MPEG4

ME Algorithm: Fast Search

ME Accuracy: Full Pixel

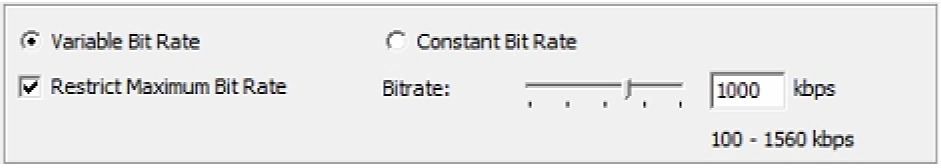
ME Vectors: 1MV

Figure 4-8:MPEG4 CODEC Settings

Key-frame Rates	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.

4.2.3 Hardware CODEC Settings

Depending on the VIGIL Server model, it may use *Hardware CODEC* recording, which has slightly different customization options. For some types of cards the CODEC used can be changed in the *VIGIL Server Settings | Hardware Tab* via the *Hardware CODEC* drop-down box.



● Variable Bit Rate ○ Constant Bit Rate

☑ Restrict Maximum Bit Rate

Bitrate: 1000 kbps

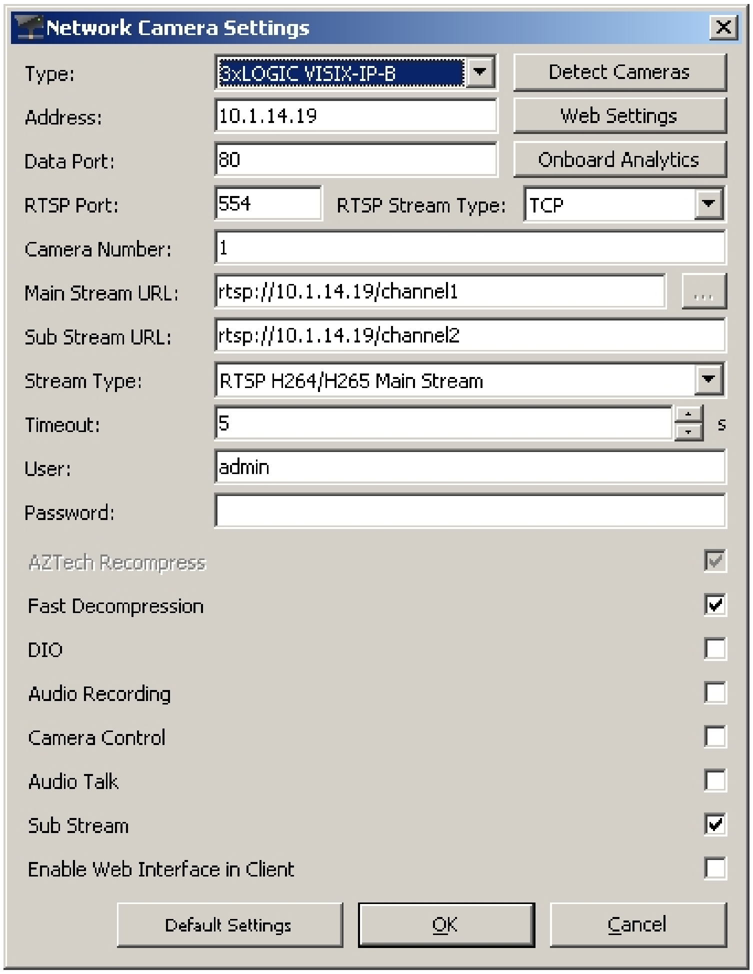
100 - 1560 kbps

Figure 4-9: Hardware CODEC Settings Tab

Variable Bit Rate	The default setting of *Variable Bit Rate* allows the encoder to change its recording bit rate automatically as required. This option offers the best combination of file size and visual quality.
Constant Bit Rate	Changes a variable bit rate into a constant bit rate. A setting of *Constant Bit Rate* with a very high bit rate selected will provide the maximum video quality settings, although this is at the expense of storage space. Usee the slider or manually enter a bit rate (in kbps) into the available field to set the constant bit rate value.
Restrict Maximum Bit Rate	Sets a hard limit on the maximum quality that can be recorded. Use the slide bar to select the desired maximum bit rate.

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.



Network Camera Settings

Type: 3xLOGIC VISIX-IP-B

Address: 10.1.14.19

Data Port: 80

RTSP Port: 554 RTSP Stream Type: TCP

Camera Number: 1

Main Stream URL: rtsp://10.1.14.19/channel1

Sub Stream URL: rtsp://10.1.14.19/channel2

Stream Type: RTSP H264/H265 Main Stream

Timeout: 5 s

User: admin

Password:

AZTech Recompress ☑

Fast Decompression ☑

DIO □

Audio Recording □

Camera Control □

Audio Talk □

Sub Stream ☑

Enable Web Interface in Client □

Figure 4-10: Network Camera Settings Window

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* 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 16 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 Camera	IF an applicable camera type is selected, this option will be visible. Choose this option to open the associated camera detection utility (3xLOGIC IP Camera Setup Utilityy,

	ONVIF Device Manager, etc...)
Address	The IP or HTTP address of the camera. It is not necessary to include http:// at the beginning of the HTTP address.
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 windowSee "On-Board Analytics" on page 108
RTSP Stream Type	Select the camera's preferred RTSP Stream Type(also known as the RTSP Transfer Protocol; UDP or TCP).
Data / RTSP Port	The network ports used to connect with the camera.
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 substream (if applicable). The substream URL field will not be editable if a sub-stream is not enabled for the camera.
...	Opens additional configuration options for some cameras.
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.
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.
Audio Talk	If the Network Camera supports *Audio Talk*, enable the checkbox to enable audio talk.
Sub Stream	Enable this checkbox to make the *Sub Stream* from the Network Camera available to

	applications that connect to the Server such as VIGIL Client.
Enable 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.

4.3.1 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.

VISIX 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, select **3xLOGIC VSX-IP**in the *Network Camera Settings - Camera Type* field. Newer cameras generations are referred to as **3xLOGIC VSX-IP-A** or **3xLOGIC VSX-IP-B** Refer to your camera's setup documentation to confirm its camera type.

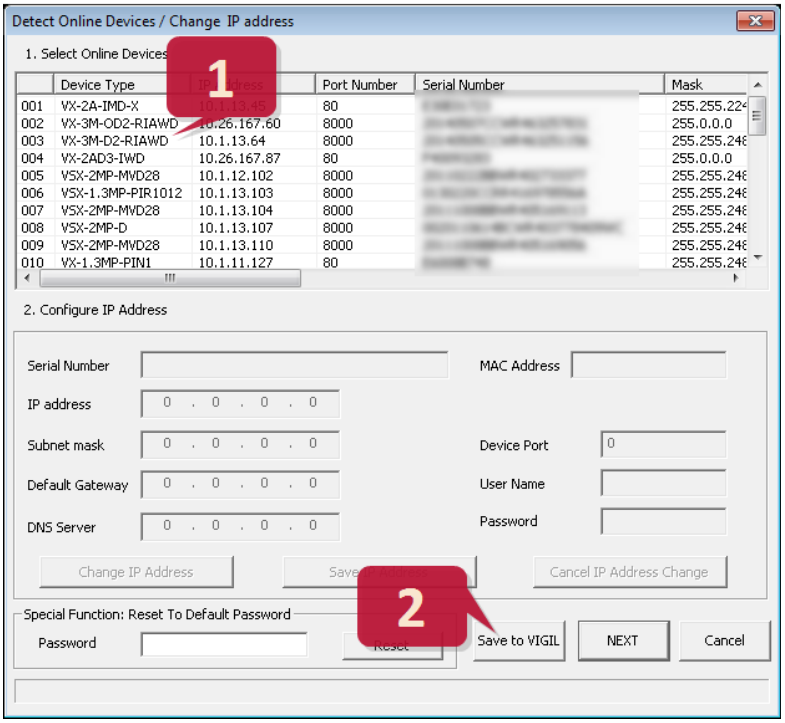
VIGIL Server features an included camera detection utility for detecting and adding VISIX cameras on your network to VIGIL Server. After selecting the camera type, click **Detect Cameras** to launch the 3xLOGIC IP Camera Setup Utility. If you select the incorrect VSX-IP type for your camera, the utility will automatically detect and correct the type when saving the camera backto 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 3xLOGIC (VISIX IP) Camera Setup Utlity.

Adding a VISIX Camera to Serve Using 3xLOGIC (VSX IP) Camera Setup Utility

After the utility launches, a list of VISIX cameras discovered on your network will be generated:

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.

1. Select the desired camera.



1. Select Online Devices

	Device Type	IP Address	Port Number	Serial Number	Mask
001	VX-2A-IMD-X	10.1.13.45	80	[redacted]	255.255.224
002	VX-3M-OD2-RIAWD	10.26.167.60	8000	[redacted]	255.0.0.0
003	VX-3M-D2-RIAWD	10.1.13.64	8000	[redacted]	255.255.248
004	VX-2AD3-IWD	10.26.167.87	80	[redacted]	255.0.0.0
005	VSX-2MP-MVD28	10.1.12.102	8000	[redacted]	255.255.248
006	VSX-1.3MP-PIR1012	10.1.13.103	8000	[redacted]	255.255.248
007	VSX-2MP-MVD28	10.1.13.104	8000	[redacted]	255.255.248
008	VSX-2MP-D	10.1.13.107	8000	[redacted]	255.255.248
009	VSX-2MP-MVD28	10.1.13.110	8000	[redacted]	255.255.248
010	VX-1.3MP-PIN1	10.1.11.127	80	[redacted]	255.255.248

2. Configure IP Address

Serial Number
MAC Address
IP address 0 . 0 . 0 . 0
Subnet mask 0 . 0 . 0 . 0
Device Port 0
Default Gateway 0 . 0 . 0 . 0
User Name
DNS Server 0 . 0 . 0 . 0
Password

Special Function: Reset To Default Password
Password

Figure 4-11:3xLOGIC IP Camera Setup 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.**

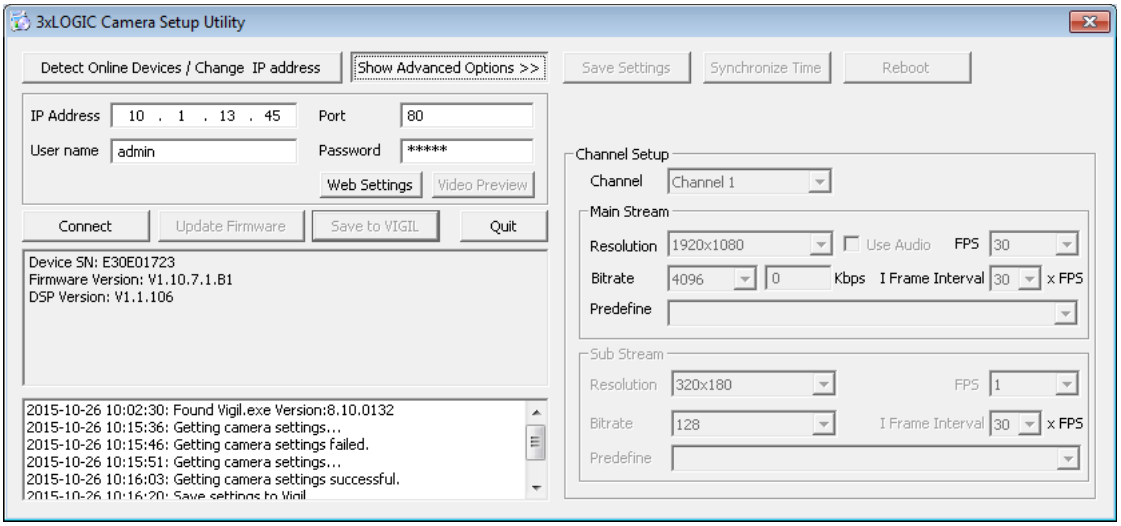
All appropriate camera settings will now populate the Network Camera Settings form fields.

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

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

3xLOGIC (VSX IP) Camera Setup Utility Properties

When launched externally, the 3xLOGIC (VSX IP) Camera Setup Utilities' main UI will deploy as pictured below(the right-hand Advanced Settings portion will not be visible):



IP Address 10 . 1 . 13 . 45
Port 80
User name admin
Password *****

```
Device SN: E30E01723
Firmware Version: V1.10.7.1.B1
DSP Version: V1.1.106
```

```
2015-10-26 10:02:30: Found Vigil.exe Version:8.10.0132
2015-10-26 10:15:36: Getting camera settings...
2015-10-26 10:15:46: Getting camera settings failed.
2015-10-26 10:15:51: Getting camera settings...
2015-10-26 10:16:03: Getting camera settings successful.
2015-10-26 10:16:20: Save settings to Vigil
```

Channel Setup
Channel: Channel 1

Main Stream
Resolution: 1920x1080; FPS: 30
Bitrate: 4096; 0 Kbps; I Frame Interval: 30 x FPS
Predefine:

Sub Stream
Resolution: 320x180; FPS: 1
Bitrate: 128; I Frame Interval: 30 x FPS
Predefine:

Figure 4-12:3xLOGIC (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 3xLOGIC Camera Setup Utility.
Web Settings	*Web Settings* will launch the camera's web page in a web browser.
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 3xLOGIC Camera Setup 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 3xLOGIC Camera Setup Utility.
Advanced Settings	Opens the Advanced Settings portion of the setup utility. See "3xLOGIC (VSX IP) Camera Setup Utility - Advanced Settings" below

3xLOGIC (VSX IP) Camera Setup 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:

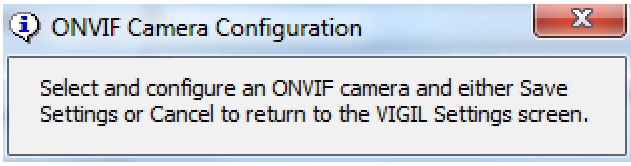
Synchronize Time	Users can synchronize the camera's time to server time by clicking the Synchronize Time button. This option may not be available across some camera models or firmware versions.
Reboot	Users can reboot the camera within the utility by clicking the Reboot button.
Save Settings	Users should save all changes made within the utility by clicking the Save Settings button.

ONVIF and PSIA - Network Camera Type

ONVIF and PSIA are interoperability standards for IP based Network Cameras. As long as a camera supports either of these standards, it can be configured with this standard instead of the brand specific standard. ONVIF is the predominate standard currently being utilized by manufacturers. When configuring an ONVIF supported camera through the *Network Camera Settings*, the ONVIF device manager is opened.

ONVIF Device Manager

After selecting the ONVIF type in your *Network Camera* settings, the *Web Settings* button will change to *Detect Cameras.* Select this option to proceed to the *ONVIF Device Manager*. You will first be met with a small notification pictured below while the *ONVIF Device Manager* loads.

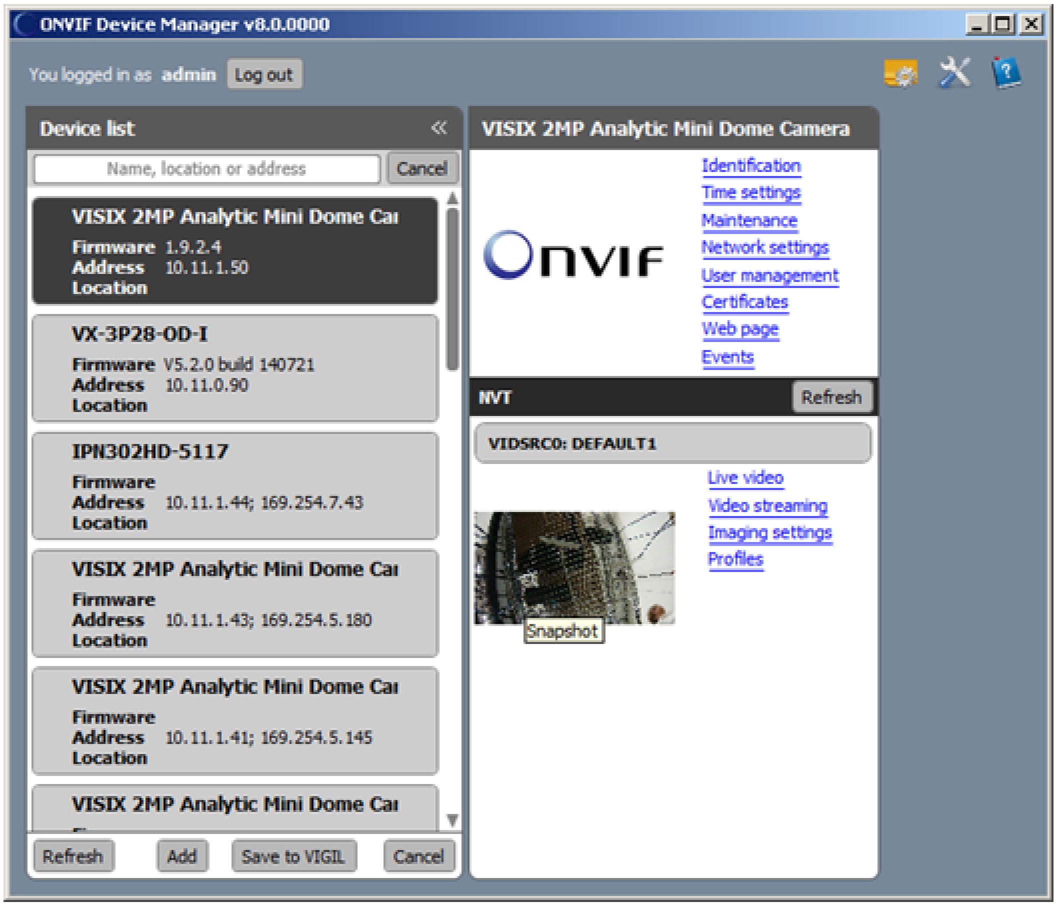


ONVIF Camera Configuration

Select and configure an ONVIF camera and either Save Settings or Cancel to return to the VIGIL Settings screen.

Figure 4-13:ONVIF Camera Configuration Prompt

After a few seconds, the *ONVIF Device Manager* will deploy and you will be met with the interface pictured below.



ONVIF Device Manager v8.0.0000

You logged in as admin

Device list

VISIX 2MP Analytic Mini Dome Cai
Firmware 1.9.2.4
Address 10.11.1.50
Location

VX-3P28-OD-I
Firmware V5.2.0 build 140721
Address 10.11.0.90
Location

IPN302HD-5117
Firmware
Address 10.11.1.44; 169.254.7.43
Location

VISIX 2MP Analytic Mini Dome Cai
Firmware
Address 10.11.1.43; 169.254.5.180
Location

VISIX 2MP Analytic Mini Dome Cai
Firmware
Address 10.11.1.41; 169.254.5.145
Location

VISIX 2MP Analytic Mini Dome Cai

VISIX 2MP Analytic Mini Dome Camera

NVT

VIDSRC0: DEFAULT1

Figure 4-14:ONVIF Device Manager - Main Screen

The *ONVIF Device Manager* offers a large selection of settings to help configure all of your cameras using the ONVIF standard to your personal preferences. The manager consists of three panes.

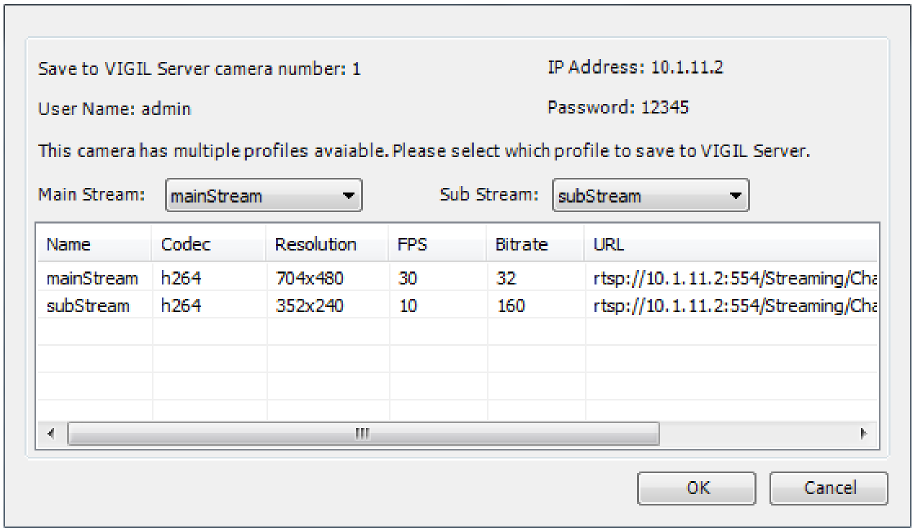
The left pane is the *Device List* which hosts a list of all available camera using the ONVIF standard.

The second (middle) pane hosts a list of camera settings and options and the third pane(right side of the UI, not pictured above) is where the chosen settings are configured and changed. See "ONVIF Device Manager Properties" on the facing page for a descriptions of all configurable camera options and settings in the ODM.

Saving Camera To VIGIL

Interfacing an ONVIF camera with VIGIL Server is fast and simple with the ODM. To begin:

1. Select a camera from the list of discovered devices.
2. Click **Save to VIGIL** to save the feed to a VIGIL Server camera channel. You will receive the prompt (pictured below) where a user can choose which stream profiles to use in VIGIL.



Save to VIGIL Server camera number: 1 IP Address: 10.1.11.2

User Name: admin Password: 12345

This camera has multiple profiles avaiable. Please select which profile to save to VIGIL Server.

Main Stream: mainStream Sub Stream: subStream

Name	Codec	Resolution	FPS	Bitrate	URL
mainStream	h264	704x480	30	32	rtsp://10.1.11.2:554/Streaming/Cha
subStream	h264	352x240	10	160	rtsp://10.1.11.2:554/Streaming/Cha

Figure 4-15: Saving Camera to VIGIL- Stream Profile Selection

3. Click OK to save the camera to VIGIL.

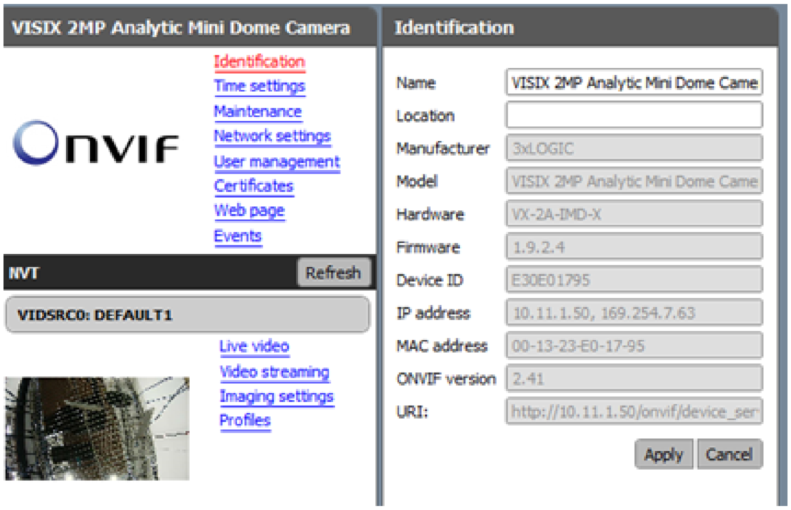
ONVIF Device Manager Properties

The ONVIF Device Manager can also be used to configure several of an ONVIF camera's settings.

Available settings and configuration options are described below:

Identification

Identification options will provide the user with currently selected camera's configuration information.

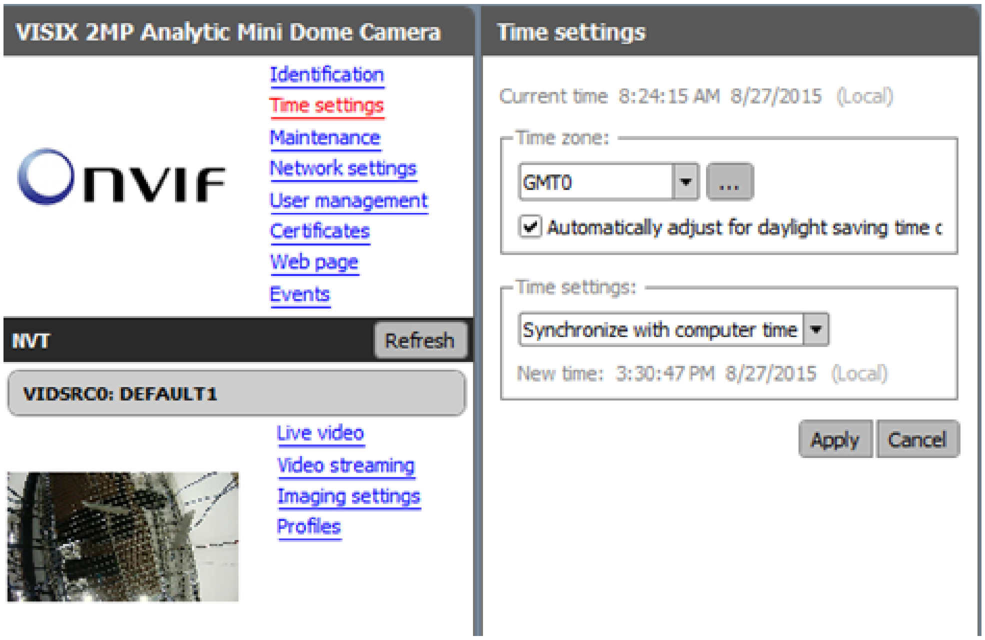


Name	VISIX 2MP Analytic Mini Dome Came
Location	
Manufacturer	3xLOGIC
Model	VISIX 2MP Analytic Mini Dome Came
Hardware	VX-2A-IMD-X
Firmware	1.9.2.4
Device ID	E30E01795
IP address	10.11.1.50, 169.254.7.63
MAC address	00-13-23-E0-17-95
ONVIF version	2.41
URI:	http://10.11.1.50/onvif/device_ser

Figure 4-16:ONVIF Device Manager - Identification Settings

Time Settings

Time settings allow users to adjust the time zone settings of the camera. Furthermore, users can sync the camera to server time.



Current time 8:24:15 AM 8/27/2015 (Local)

Time zone: GMT0

☑ Automatically adjust for daylight saving time c

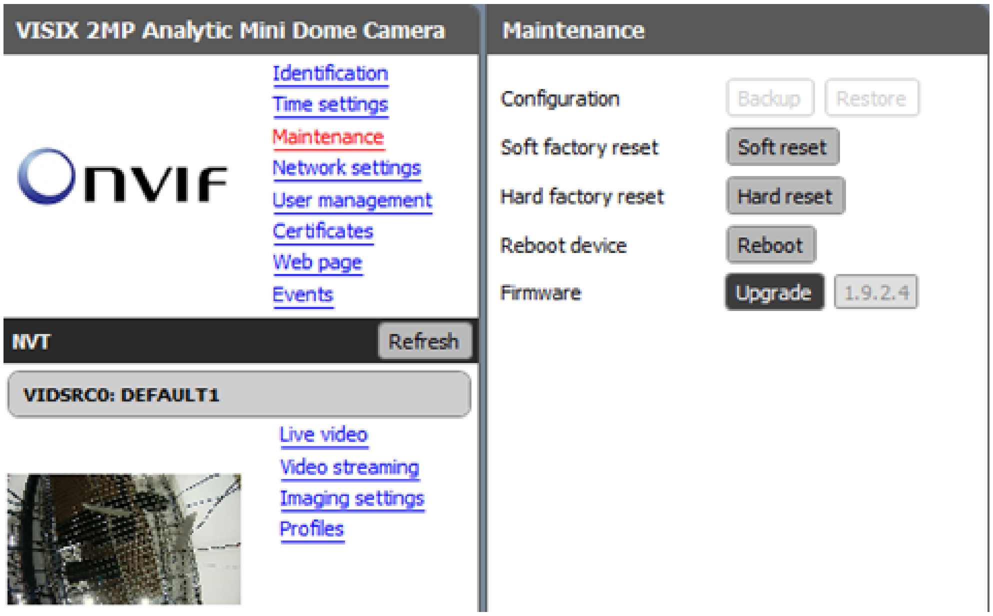
Time settings: Synchronize with computer time

New time: 3:30:47 PM 8/27/2015 (Local)

Figure 4-17:ONVIF Device Manager - Time Settings

Maintenance

The Maintenance settings allow users to either Soft factory reset (Factory reset that saves all IP Configuration), Hard factory reset (Completely restores all setting back to factory, including IP Configuration), Reboot device, and Upgrade Firmware.



Configuration

Soft factory reset

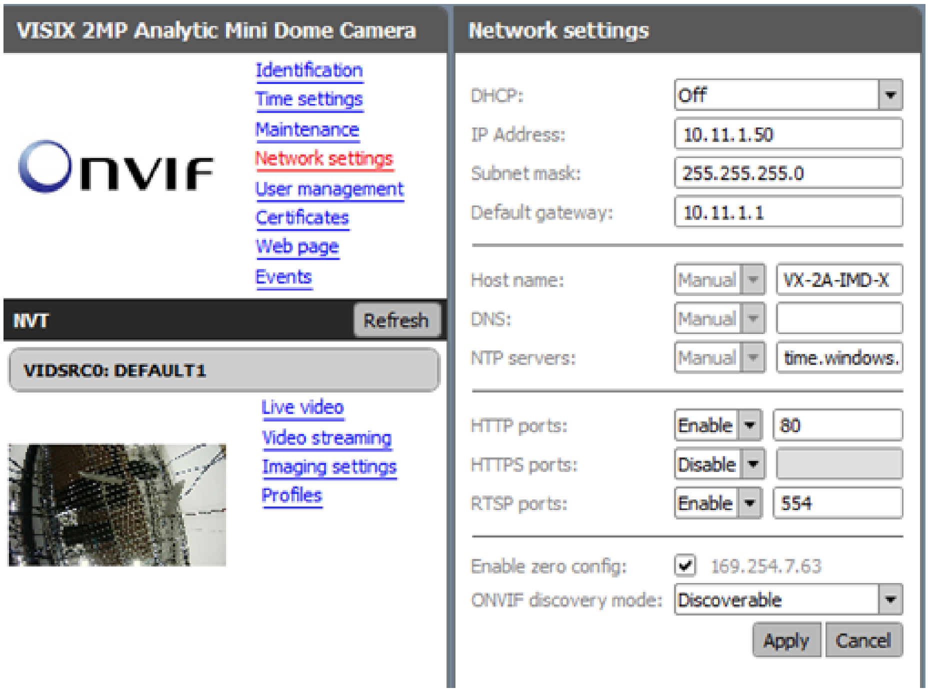
Hard factory reset

Reboot device

Firmware 1.9.2.4

Network Settings

Network Settings allow users to set a static IP Address of the camera, from the utility.

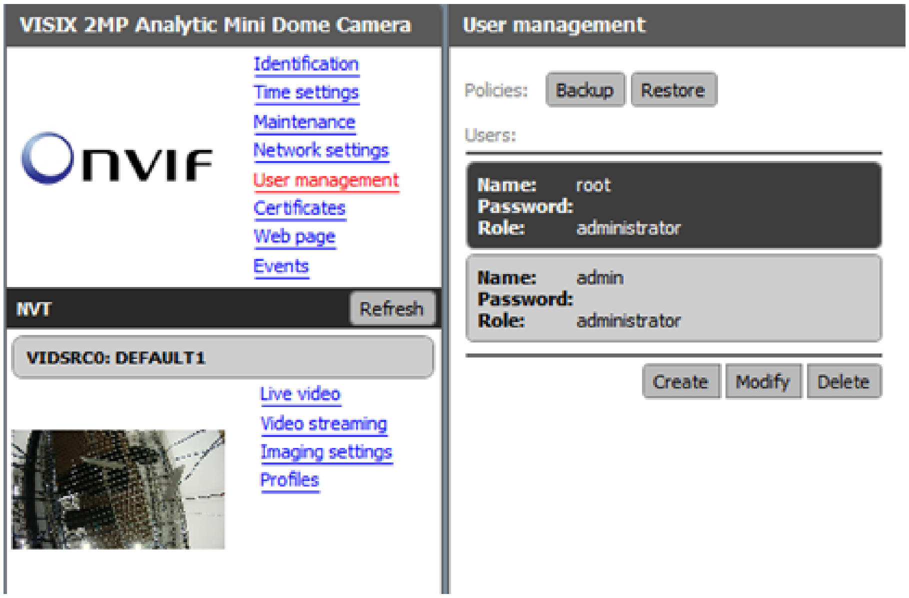


DHCP: Off
IP Address: 10.11.1.50
Subnet mask: 255.255.255.0
Default gateway: 10.11.1.1
Host name: Manual VX-2A-IMD-X
DNS: Manual
NTP servers: Manual time.windows.
HTTP ports: Enable 80
HTTPS ports: Disable
RTSP ports: Enable 554
Enable zero config: ☑ 169.254.7.63
ONVIF discovery mode: Discoverable

Figure 4-18:ONVIF Device Manager - Network Settings

User Management

The User Management settings allow users to create, modify, and delete camera users.



Name: root
Password:
Role: administrator

Name: admin
Password:
Role: administrator

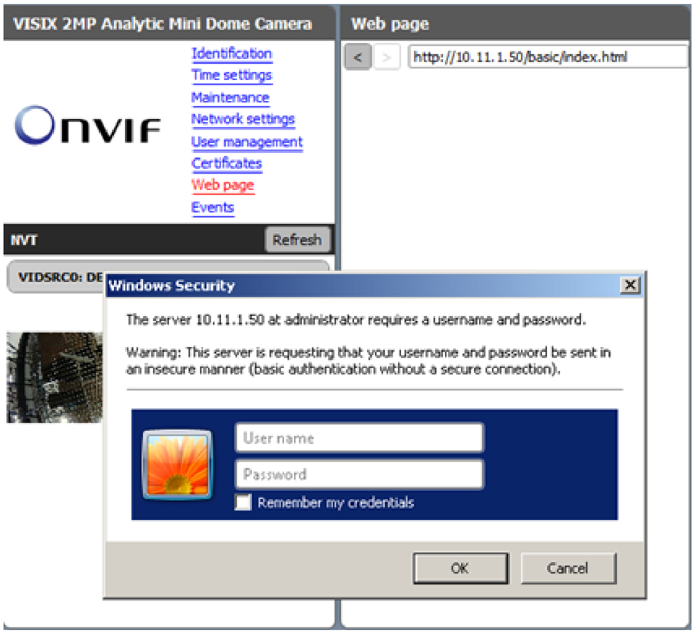
Figure 4-19:ONVIF Device Manager - User Management Settings

Certificates

The Certificates settings window will give details on camera's security certificates. These certificates signal a camera's ability to transfer data via a secure connection.

Web Page

The Web Page link allow users to connect and display the camera’s web interface



The server 10.11.1.50 at administrator requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

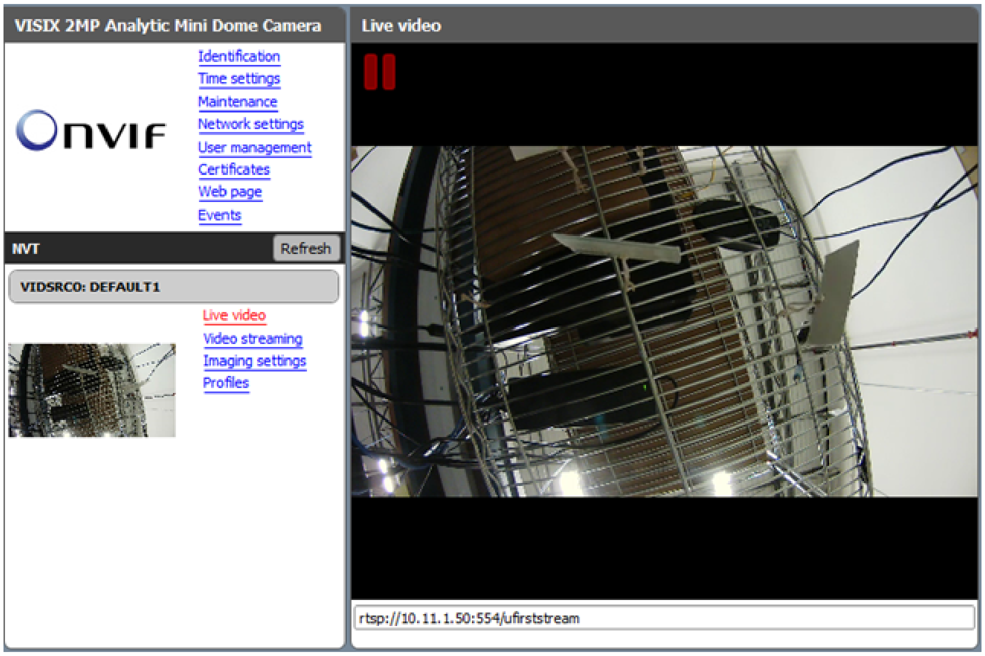
Figure 4-20:ONVIF Device Manager - Web Page Settings

Events

Events allow users to see all the camera's logged event information.

Live Video

The Live Video option will deploy a live video stream preview from the selected camera.

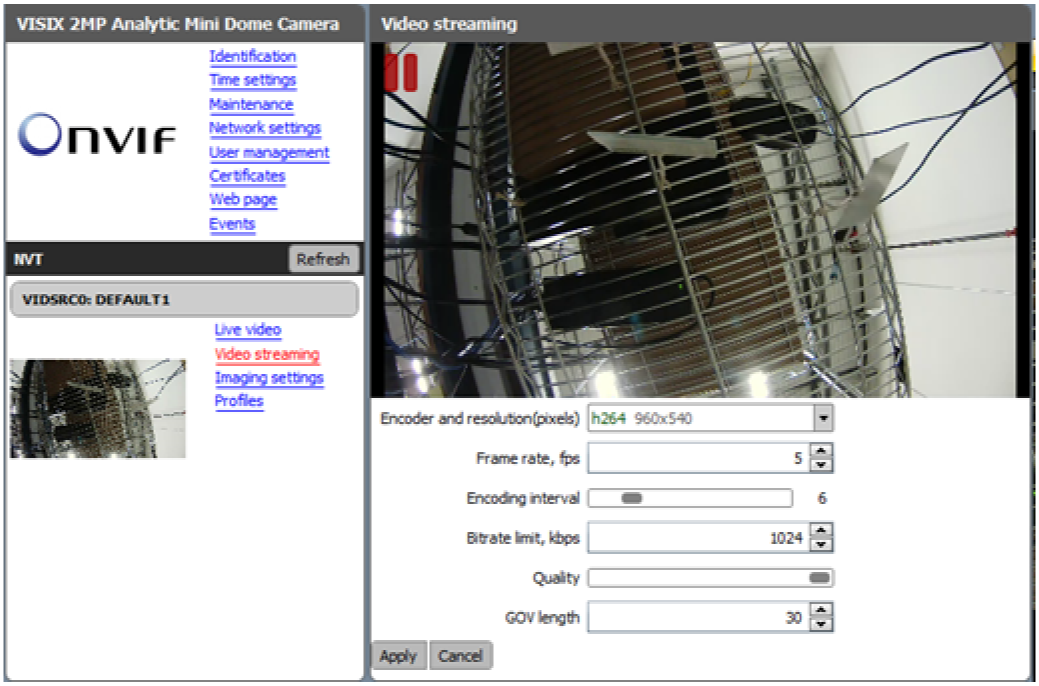


rtsp://10.11.1.50:554/ufirststream

Figure 4-21:ONVIF Device Manager - Live Video

Video Streaming

The Video Streaming settings will allow users to configure the recording and streaming parameters of the camera's primary stream.



Encoder and resolution(pixels) h264 960x540

Frame rate, fps 5

Encoding interval 6

Bitrate limit, kbps 1024

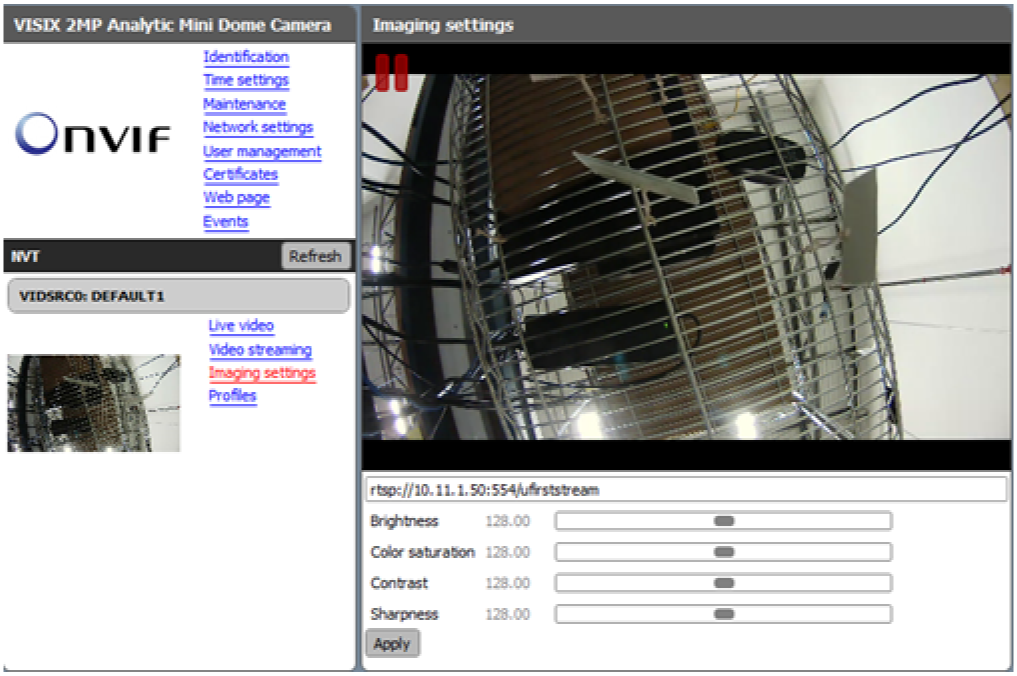
Quality

GOV length 30

Figure 4-22:ONVIF Device Manager - Video Streaming Settings

Image Settings

Image Settings allow users to configure the brightness, saturation, contrast, and sharpness of the camera's primary stream.



rtsp://10.11.1.50:554/ufirststream

Brightness 128.00

Color saturation 128.00

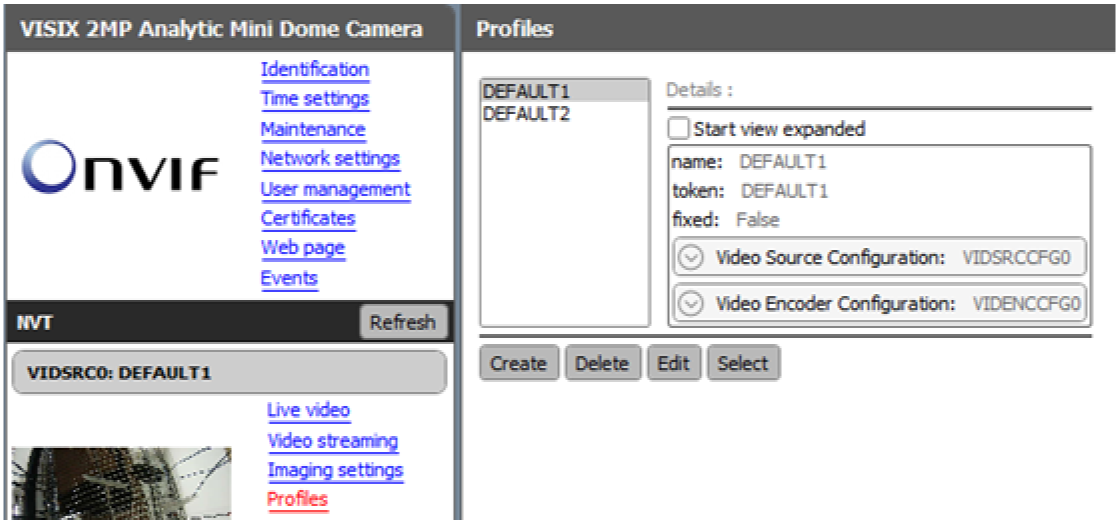
Contrast 128.00

Sharpness 128.00

Figure 4-23:ONVIF Device Manager - Video Streaming Settings

Profiles

The Profiles form allow users to create, edit, and delete camera profiles for streams.



□ Start view expanded

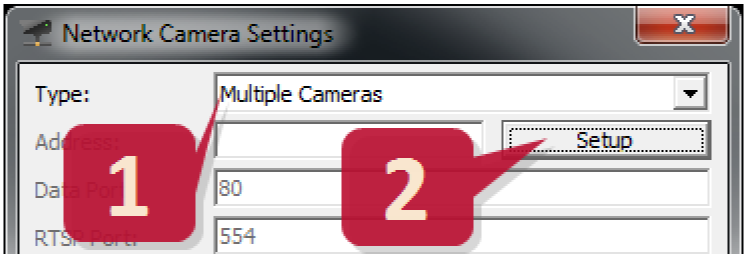
name: DEFAULT1
token: DEFAULT1
fixed: False
Video Source Configuration: VIDSRCCFG0
Video Encoder Configuration: VIDENCCFG0

Figure 4-24:ONVIF Device Manager - Profile Settings

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:



Network Camera Settings

Type: Multiple Cameras

Address:

Data Port: 80

RTSP Port: 554

Figure 4-25: Network Camera Types - Adding a VIGIL Multiview Channel

1. Select *Multiple Cameras* in the*Network Camera Settings* form *Type* field.
2. Click the *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.

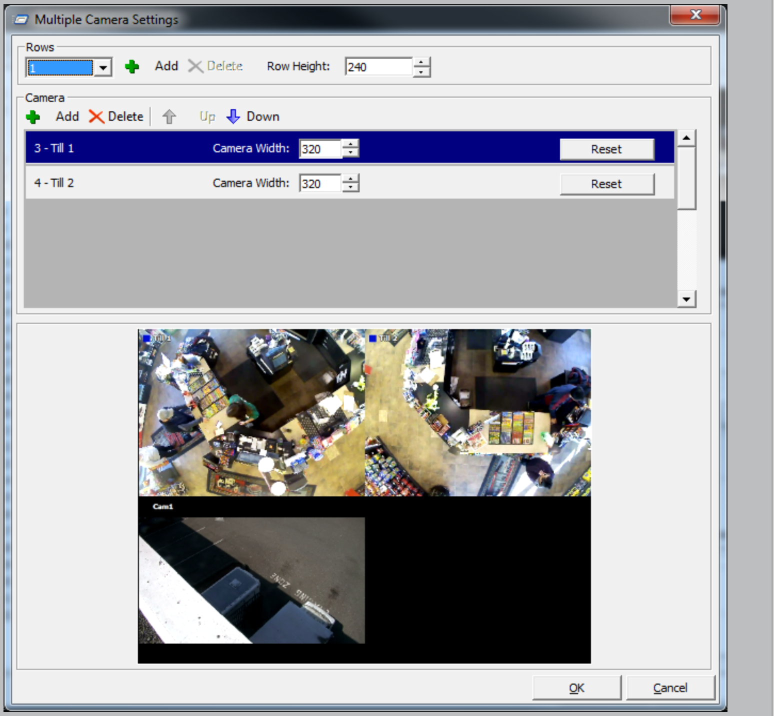
To add a new row:

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. A preview of the current Multiview is located at the bottom of the screen. After achieving your desired layout in the preview, click OK to save the settings.

Rows and cameras may be deleted by selecting the camera or row to be deleted and clicking their respective *Delete* buttons.



Multiple Camera Settings

Rows: 1

Row Height: 240

Camera

3 - Till 1 Camera Width: 320

4 - Till 2 Camera Width: 320

Figure 4-26: 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 Together Into One Image - Network Camera Type

Designed for use with video analytics on DRX systems, the *Network Camera, Multiple Cameras* 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.

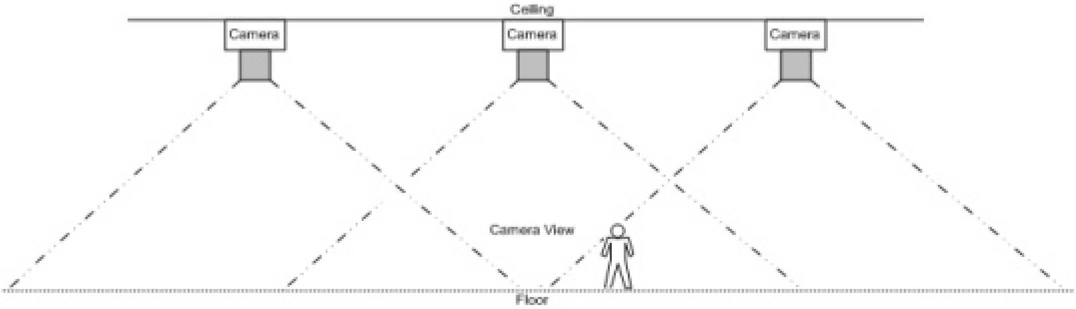


Figure 4-27: Stitched Images - Camera Overlap Example

There must be the correct amount of overlap between the images to prevent fluctuation of the person size as a person moved between images.

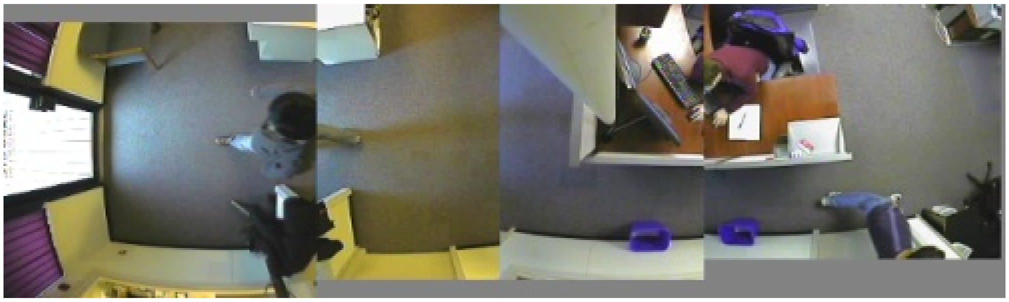


Figure 4-28: Stitched Image Example

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 to another.

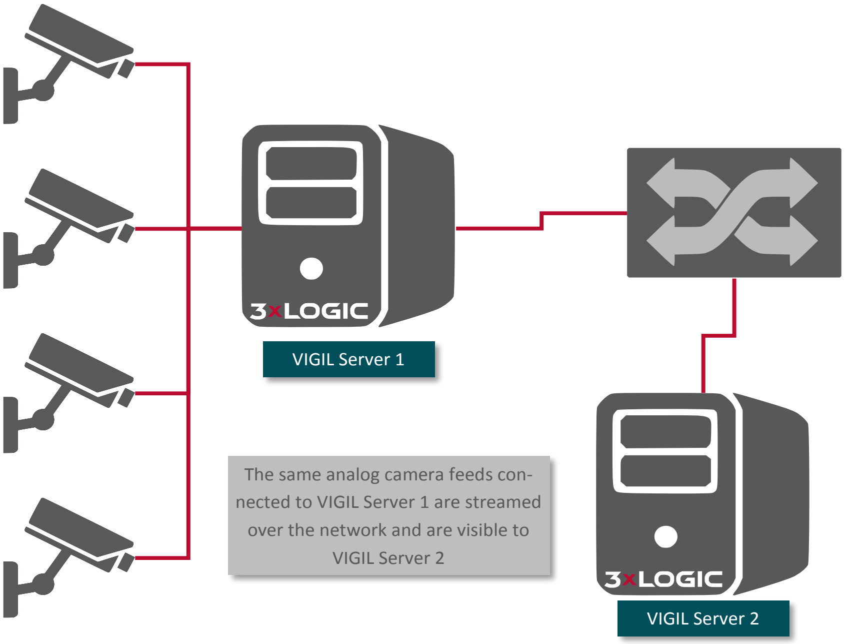

3xLOGIC
VIGIL Server 1
The same analog camera feeds connected to VIGIL Server 1 are streamed over the network and are visible to VIGIL Server 2
3xLOGIC
VIGIL Server 2

Figure 4-29: Selecting VIGIL Server as Network Camera Type - Analog Camera Relay

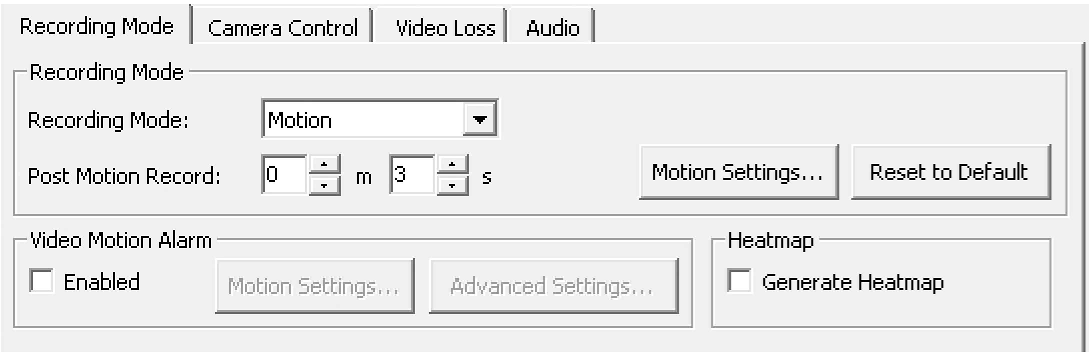
To set up this configuration, select the VIGIL Server type in the *Network Camera* window. The recommended settings for this setup are:

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.

USB Camera - Network Camera Type

VIGIL Server can record from USB Cameras connected to the Server. The USB camera drivers need to be installed for VIGIL Server to be able to detect the camera.

4.4 Recording Mode Tab



Recording Mode: Motion

Post Motion Record: 0 m 3 s

☐ Enabled

☐ Generate Heatmap

Figure 4-30: Settings - Camera Setup - Recording Mode Tab

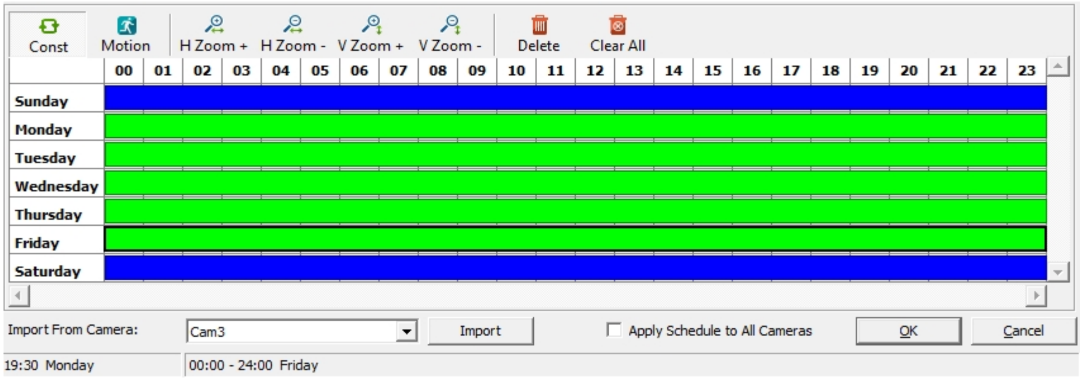
4.4.1 Recording Modes

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 Constant Recording*. Variable constant 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 Variable Constant 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*.

4.4.2 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.



Import From Camera: Cam3 Import

☐ Apply Schedule to All Cameras

OK Cancel

19:30 Monday

00:00 - 24:00 Friday

Figure 4-31: Scheduled Recording - Scheduler Window

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

Const	Sets or changes the section to *Constant* recording mode; these time periods are colored green.
Motion	Sets or changes section to *Motion* recording mode; these time periods are colored blue.
HZoom+/-	Expands and contracts the schedule horizontally; this allows for better precision in setting time periods.
VZoom+/-	Expands and contracts the schedule vertically.
Move a Time Period	Click and hold the *Shift* key, then click-and-drag the section.
Copy a Time Period	Click and hold the *Ctrl* key, then click-and-drag the section.
Change Record Mode	Click a section of the schedule, and then click the appropriate button (*Const* or *Motion*) to change the recording mode for that section.
Change the Start / End Time	Select the section by clicking on it and then click-and-drag the right or left edge of the section.
Importing from Another Camera	Select the camera from the *Import From Camera* drop-down menu, and then click *Import*. This will overwrite the current schedule.
Viewing Start and End Times of a Section	Select the section by clicking on it. The start and end times of the section are displayed near the bottom left corner of the *Schedule* window. Hover the mouse over any part of the section to display the time.
Deleting a Time Period	To select a section, click on it and then click *Delete*.
Deleting a Schedule	Click the *Clear All* 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.

4.4.3 Motion Recording Settings

When recording in Motion mode, 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.

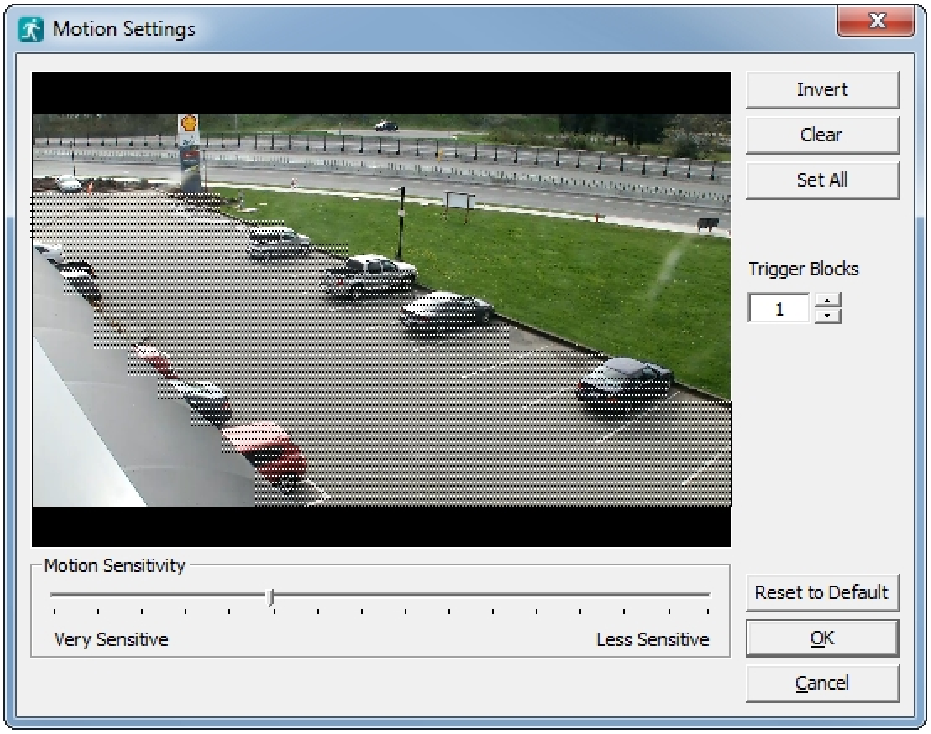


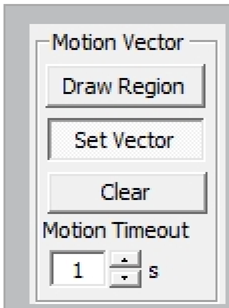
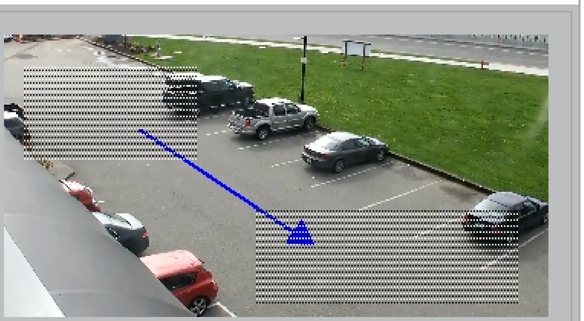
Figure 4-32: Motion Recording Settings Window

Invert	Swaps masked and clear regions.
Clear	Clears all masked regions.
Set All	Masks the entire image.
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.

4.4.4 Video Motion Alarm

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. For the basic configuration options , See "Motion Recording Settings" on page 1.

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.

 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. **Note:**If there is no motion vector arrow specified, any of the selected regions will trigger a motion alarm.  **Example of Motion Vector**
Clear	Removes 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.

4.4.5 Video Motion Alarm Advanced Settings

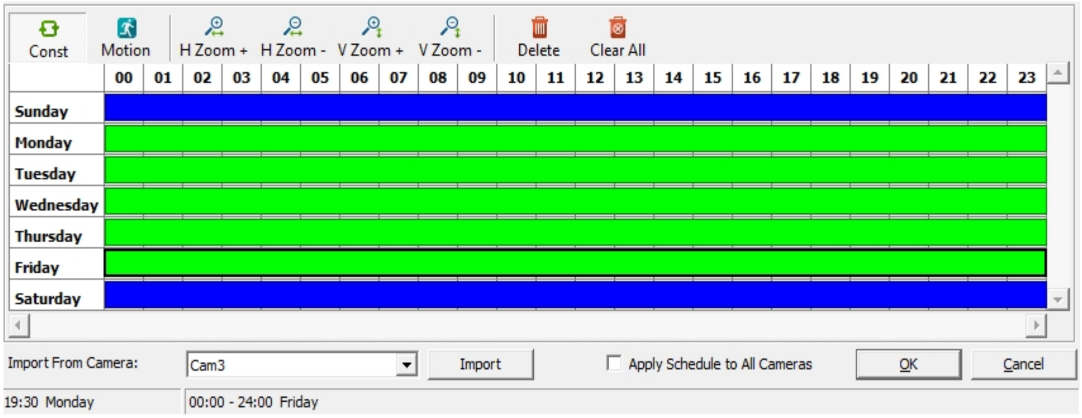
The advanced settings include scheduling when the alarm is active, *Output Relay Options,* and *Notification Settings*.

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.*



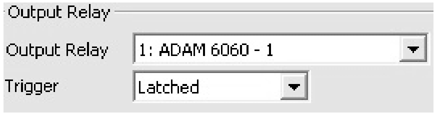
Import From Camera: Cam3

19:30 Monday | 00:00 - 24:00 Friday

Figure 4-33: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).



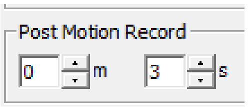
Output Relay: 1: ADAM 6060 - 1

Trigger: Latched

Figure 4-34: 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.

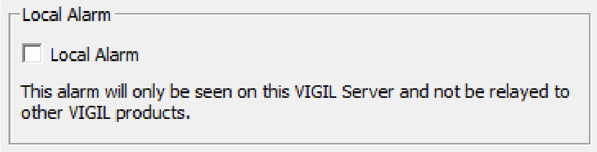


0 m 3 s

Figure 4-35: 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.



Local Alarm

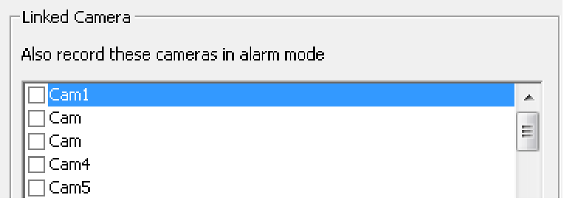
□ Local Alarm

This alarm will only be seen on this VIGIL Server and not be relayed to other VIGIL products.

Figure 4-36: 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.



Linked Camera

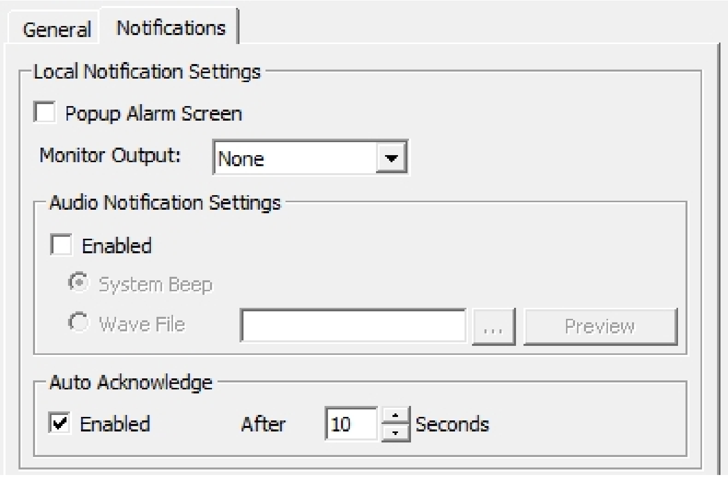
Also record these cameras in alarm mode

□ Cam1
□ Cam
□ Cam
□ Cam4
□ Cam5

Figure 4-37: Linked Cameras

Notifications Tab

Local Notification Settings



Local Notification Settings

□ Popup Alarm Screen

Monitor Output: None

Audio Notification Settings

□ Enabled

● System Beep

○ Wave File

Auto Acknowledge

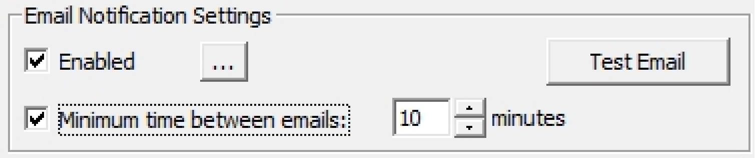
☑ Enabled After 10 Seconds

Figure 4-38: Local Notification Settings

Popup Alarm Window	Select this option to have the *Alarm* window automatically displayed when a motion alarm is triggered.
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



☑ Enabled

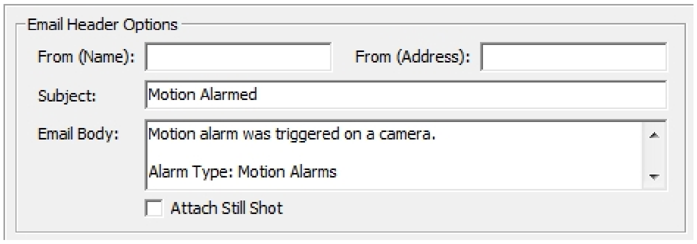
☑ Minimum time between emails: 10 minutes

Figure 4-39: 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 emails* 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 Notifications* and open the *Email Settings* window.



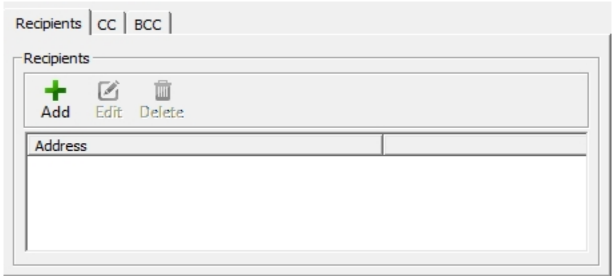
From (Name):
From (Address):
Subject: Motion Alarmed
Email Body: Motion alarm was triggered on a camera.

Alarm Type: Motion Alarms

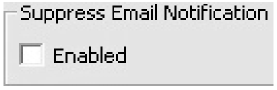
□ Attach Still Shot

Figure 4-40: Email Header Options

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.
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.

	 Recipients CC BCC Recipients Add Edit Delete Address **Figure 4-41:**Email Notification Recipients Configuration Window
Test Email	Sends a test email based on your notification settings and email configuration. **Note:**For email to function properly, a valid SMTP Server must be configured in the VIGIL Server Settings tab.

Suppress Email Notification



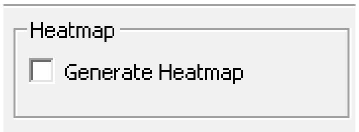
Suppress Email Notification

□ Enabled

Figure 4-42: Enable Email Notification Suppression

This option, located on the *Video Motion Alarm Advanced Settings - General Tab,*and will only work in conjunction with enabling *Popup Alarm Screen*, prevents a flood of email alerts being sent out. It will only send out one email alert until the alerts have been acknowledged in the piper *Alarm* window. If alerts have been set to *Auto Acknowledge*, it will send out an email after each period of auto acknowledgement has passed.

4.4.6 Heatmap



Heatmap

□ Generate Heatmap

Figure 4-43: Settings - Camera Setup - Generate Heatmap

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

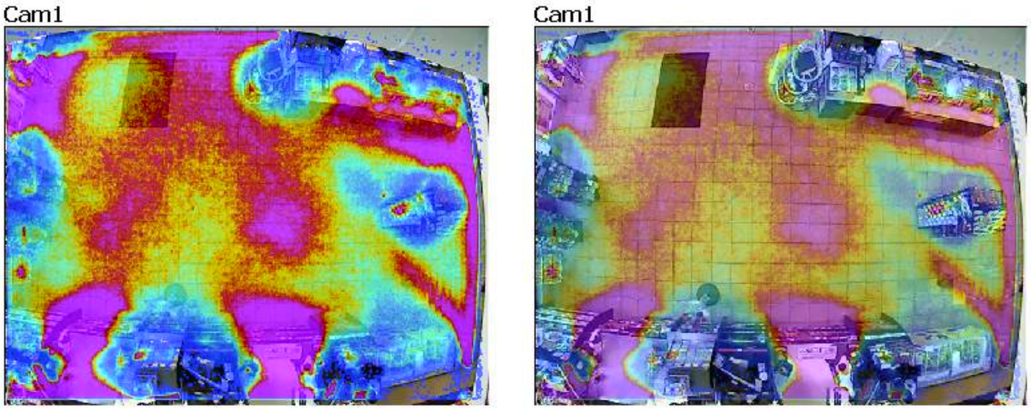


Figure 4-44: Heatmap Examples

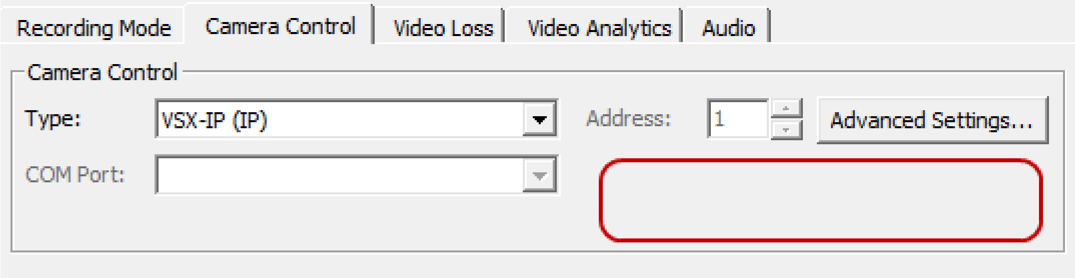
To enable Heatmap generation for a camera, check-off *Generate Heatmap.* Checking this option enables data collection for use with the heat map functionality. No further camera configuration is required for heatmap use.

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.

4.5 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 in the blank area circled in red depending on the selected camera type.



Type: VSX-IP (IP)

Address: 1

COM Port:

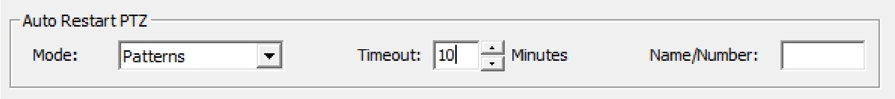
Figure 4-45: Settings - Camera Setup Tab - Camera Control Tab

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 39
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.

4.5.1 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.



Mode: Patterns

Timeout: 10

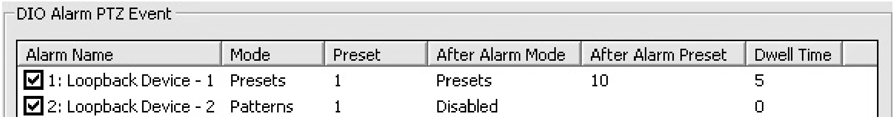
Name/Number:

Figure 4-46: 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.



DIO Alarm PTZ Event

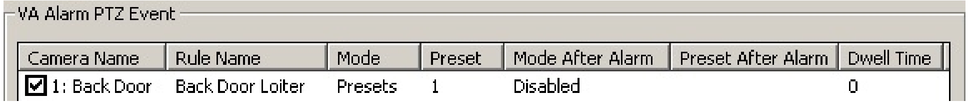
Alarm Name	Mode	Preset	After Alarm Mode	After Alarm Preset	Dwell Time
☑ 1: Loopback Device - 1	Presets	1	Presets	10	5
☑ 2: Loopback Device - 2	Patterns	1	Disabled		0

Figure 4-47:DIO Alarm PTZ Events

Video Analytics Alarm PTZ Events

Video Analytics Alarms can also be used to Trigger TPZ 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.



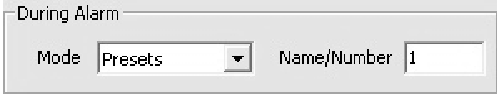
VA Alarm PTZ Event

Camera Name	Rule Name	Mode	Preset	Mode After Alarm	Preset After Alarm	Dwell Time
☑ 1: Back Door	Back Door Loiter	Presets	1	Disabled		0

Figure 4-48: Video Analytics Alarm PTZ Events

During Alarm

Select what action to apply during the DIO Alarm.



During Alarm

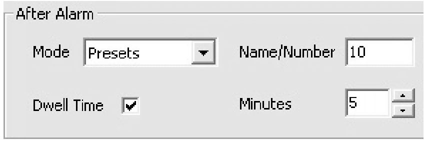
Mode: Presets

Name/Number: 1

Figure 4-49: 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



After Alarm

Mode: Presets

Name/Number: 10

Dwell Time ☑

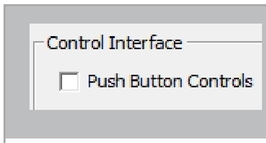
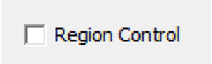
Minutes: 5

Figure 4-50: After Alarm Settings

Select what action to apply after the *DIO Alarm* has ended. To do nothing after the alarm, select *Disabled* from the mode drop-down.

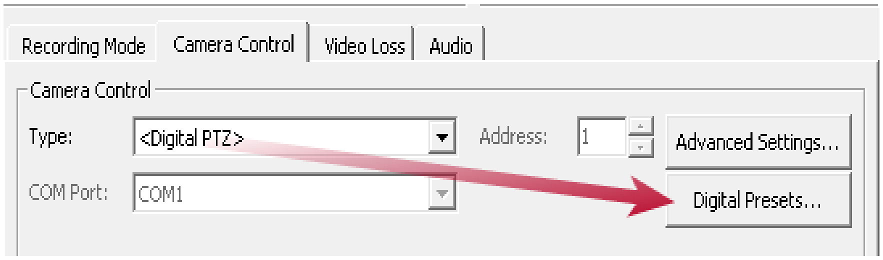
Mode	Select *Disabled*, *Patterns*, *Presets* or *Tours* from the drop-down box.
Name / Number	Enter the Name or Number of the *Pattern*, *Preset* or *Tour*.
Dwell Time	The amount of time from when the DIO Alarm is triggered until the *After Alarm* event occurs. If *Dwell Time* is not checked the *After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

4.5.2 Digital Presets

When *Digital PTZ* is the selected camera control*Type*, the *Digital Presets* button will become available.



Camera Control

Type: <Digital PTZ>

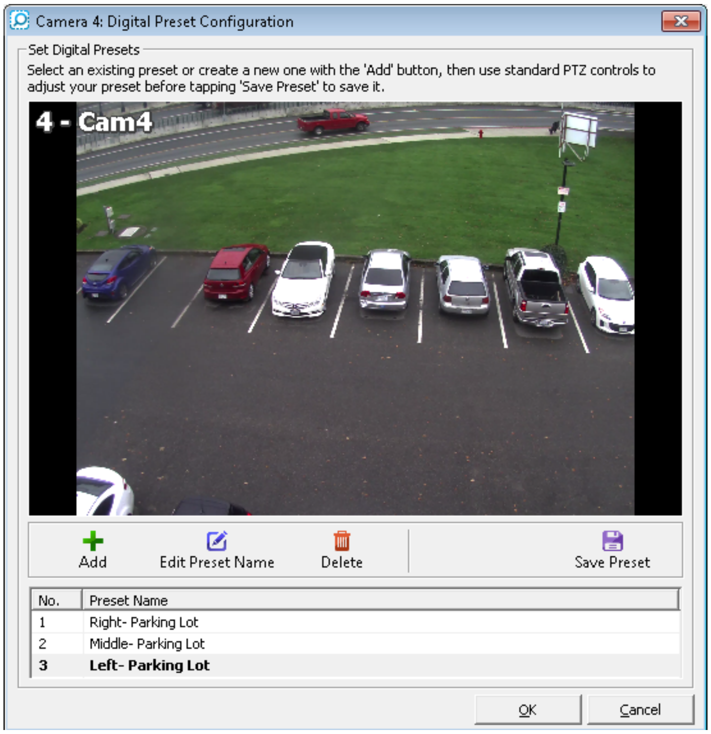
Address: 1

COM Port: COM1

Figure 4-51: 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 cna 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).



Camera 4: Digital Preset Configuration

Set Digital Presets

Select an existing preset or create a new one with the 'Add' button, then use standard PTZ controls to adjust your preset before tapping 'Save Preset' to save it.

No.	Preset Name
1	Right- Parking Lot
2	Middle- Parking Lot
3	**Left- Parking Lot**

Figure 4-52: 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 Preset Name	Edit the selected preset's name.
Delete	Delete the selected preset.
Save Preset	Save the current image to the selected preset.

Adding / Editing a Digital Preset

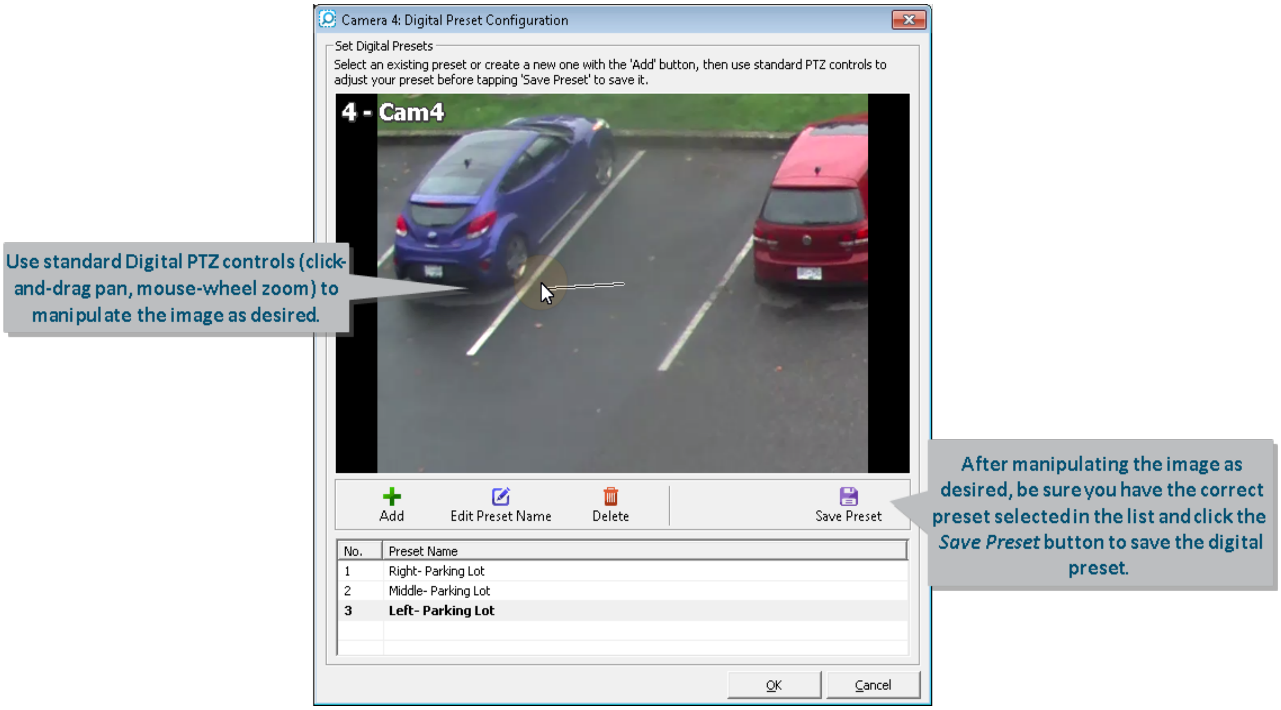
To add a new preset:

1. Click the *Add* button and name the preset. The preset will be added to the list and will be the actively selected preset.
2. Manipulate the image as required and click *Save Preset* to save the current image to the selected preset number.

Repeat the above process to add multiple presets.

To edit an existing preset:

1. Select the preset from the list.
2. Manipulate the image as desired using standard Digital PTZ Controls.
3. Click *Save Preset*.



Camera 4: Digital Preset Configuration

Set Digital Presets

Select an existing preset or create a new one with the 'Add' button, then use standard PTZ controls to adjust your preset before tapping 'Save Preset' to save it.

No.	Preset Name
1	Right- Parking Lot
2	Middle- Parking Lot
3	**Left- Parking Lot**

Use standard Digital PTZ controls (click-and-drag pan, mouse-wheel zoom) to manipulate the image as desired.

After manipulating the image as desired, be sure you have the correct preset selected in the list and click the *Save Preset* button to save the digital preset.

Figure 4-53: Settings - Camera Setup - Camera Control Tab - Adding / Editing a Digital Preset

- To edit a preset name, select the preset from the list and click *Edit Preset Name.*
- To delete a preset, select it from the list and click *Delete.*

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

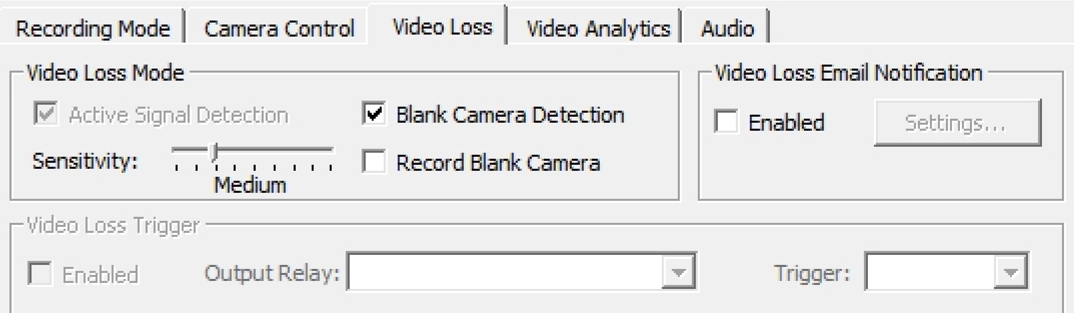
Viewing a Digital Preset

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 89

4.6 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.



Video Loss Mode

☑ Active Signal Detection

☑ Blank Camera Detection

Sensitivity: Medium

☐ Record Blank Camera

Video Loss Email Notification

☐ Enabled

Video Loss Trigger

☐ Enabled

Output Relay:

Trigger:

Figure 4-54: Settings - Camera Setup Tab - Video Loss Tab

4.6.1 Video Loss Mode

Active Signal Detection	Enables hardware signal loss detection if the VIGIL Server capture card supports this feature.
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.

4.6.2 Video Loss Trigger

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

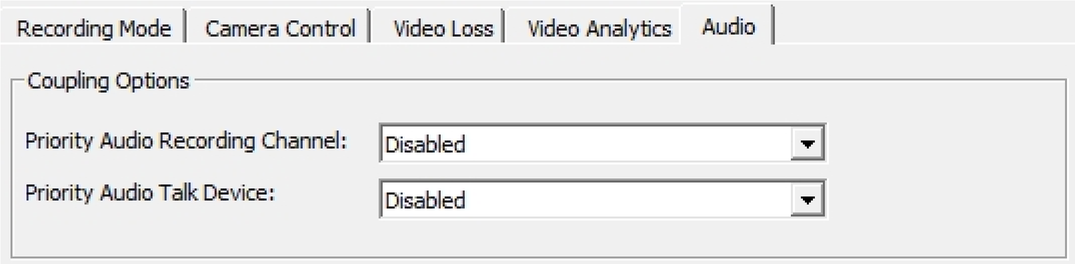
Output Relay	Select the DIO Relay.
Trigger	Select the type of trigger for the DIO Relay: *Momentary*, which lasts two seconds or *Latched*, which lasts until the video is recovered.

4.6.3 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.

4.7 Audio Tab

The *Audio* tab allows you to choose a *Priority Audio* channel and *Audio Talk* device for each camera.



Coupling Options

Priority Audio Recording Channel: Disabled

Priority Audio Talk Device: Disabled

Figure 4-55: Settings - Camera Setup Tab - Audio Tab

Priority Audio Recording Channel	Select the *Audio Channel* that will be associated with this camera. *Audio Channels* are configured on the *Settings - Audio Tab*.
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*.

4.8 Live Overlay Tab

VIGIL Server Systems with *Live Overlay* cards will enable the *Live Overlay* tab. The *Brightness, Contrast* and *U/V Saturation* can be modified for the *Live Overlay* image.

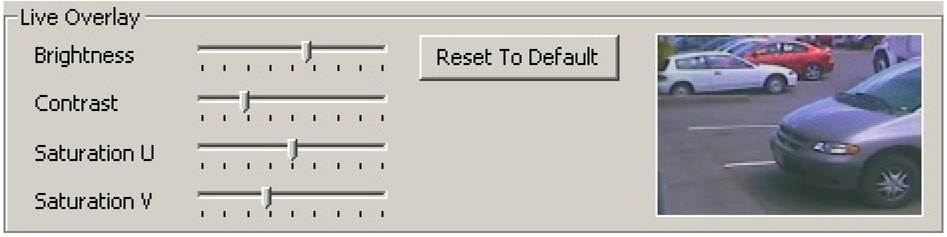


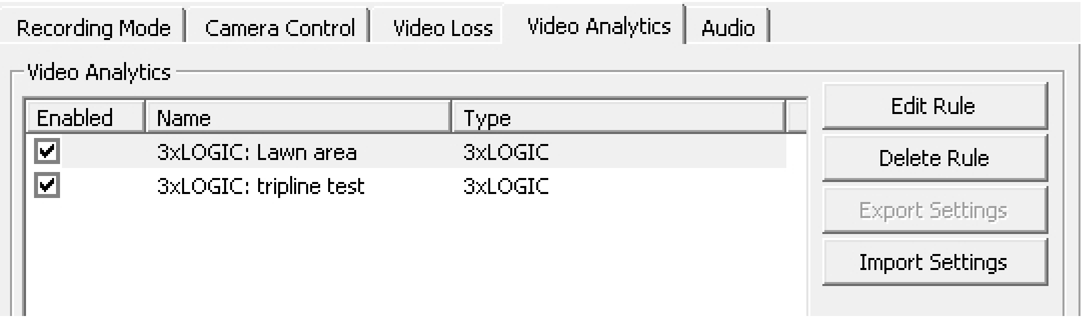
Figure 4-56: Settings - Camera Setup Tab - Live Overlay Tab

5 Advanced Settings - Video Analytics Tab

From the Video Analytics tab, a user can view, delete and edit video analytics rules which have been synchronized with VIGIL Server.

Note: VIGIL Server offers support for VCA video analytics from analytic-capable cameras. VCA Video analytics rules are synchronized with VIGIL Server via the VIGIL Analytics Bridge. Contact your 3xLOGIC representative to acquire a compatible version of the VIGIL Analytics bridge.

Note: If you have updated a pre-version 9 copy of VIGIL Server to 9 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..



Enabled	Name	Type
☑	3xLOGIC: Lawn area	3xLOGIC
☑	3xLOGIC: tripline test	3xLOGIC

Figure 5-1: Settings - Video Analytics Tab

Edit Rule	Opens the *Rule Settings* window for the selected rule.
Delete Rule	Deletes the selected rule.
Export Settings	Export the video analytics *Rules* settings for this camera to a .dat file. This option allows a camera to be moved to a different physical input without having to reconfigure the analytics.
Import Settings	Import video analytics *Rules* settings to this Camera from a .dat file. This option allows a camera to be moved to a different physical input without having to reconfigure the analytics.

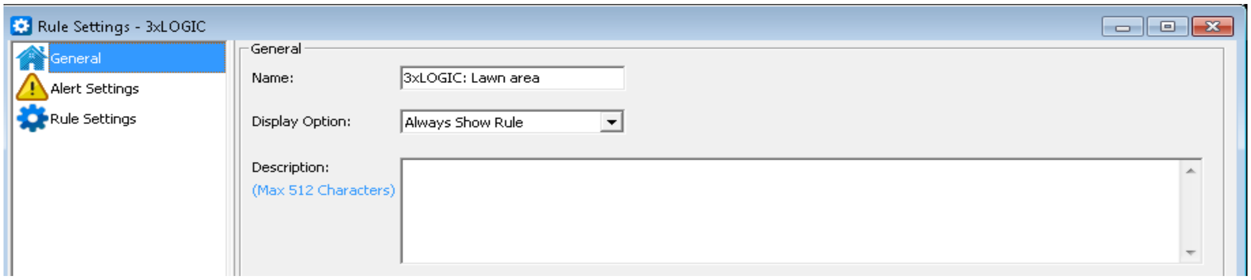
To delete a rule, select the rule from the list and click Delete.

To edit a rule, select a rule from the list and click *Edit.* .

5.1 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



Name: 3xLOGIC: Lawn area

Display Option: Always Show Rule

Description: (Max 512 Characters)

Figure 5-2: 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

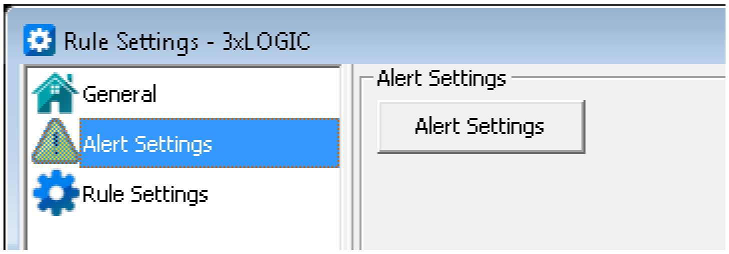
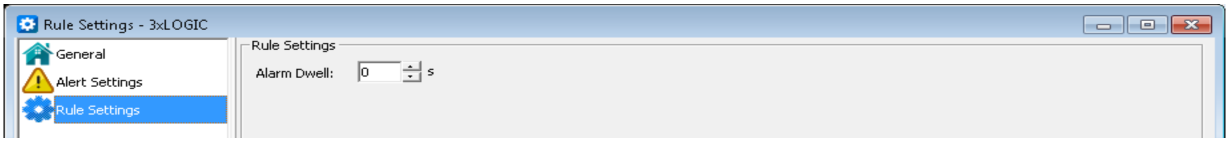


Figure 5-3: Video Analytics - Rules Settings - Alert Settings Tab

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 and configure alerts / notifications. The Video Analytics Alert Settings window is the same as the Video Motion Alarm Advanced Settings Window.See "Recording Mode Tab" on page 29under the Recording Settings Tab for configuration information.

Rule Settings



Alarm Dwell: 0 s

Figure 5-4: Video Analytics - Rules Settings - Rules Settings Tab

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

Click OK at the bottom of the windows to save the new settings.

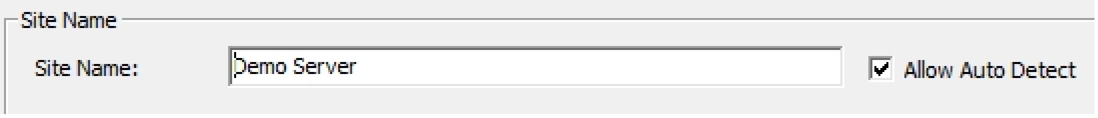
Warning: If VIGIL Analytics Bridge is used to retrieve rule info from a camera and the rules are re-synced with VIGIL Server, any rule changes configured on VIGIL Server will be overwritten with the new settings from the camera.

6 Advanced Settings - Server Settings Tab

6.1 Server Settings Tab - Basic Settings

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

6.1.1 Site Name



Site Name

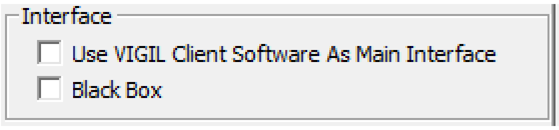
Site Name: Demo Server

☑ Allow Auto Detect

Figure 6-1: 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.
Allow Auto Detect	Allow the Server to be auto-detected by VIGIL Central Management (VCM) and VIGIL Client software.

6.1.2 Interface



Interface

□ Use VIGIL Client Software As Main Interface

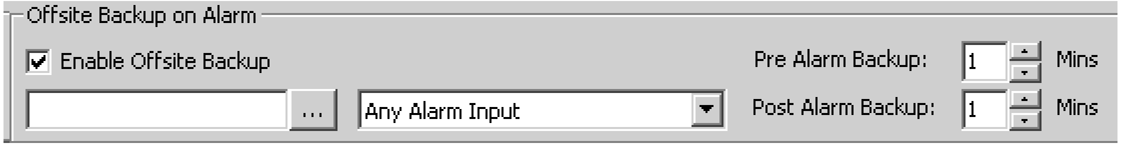
□ Black Box

Figure 6-2: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 11.50.0000, 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 are now available in VIGIL Client by default
Black Box	Allows VIGIL Server to run in *Black Box* mode. *Black Box* mode causes Server to run without much of its functioning interface, essentially becoming a background application. This is often used with systems which are rarely altered or are only connected to via a remote connections. When enabling this option, the user will be prompted with the following warning: "This VIGIL Server system has been configured to Black Box Mode. Many of the local interface options including viewing live footage, searching footage, and use of VIGIL Client are disabled. A remote Client will be required to perform these tasks."

6.1.3 Offsite Backup on Alarm

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



Offsite Backup on Alarm

☑ Enable Offsite Backup

Any Alarm Input

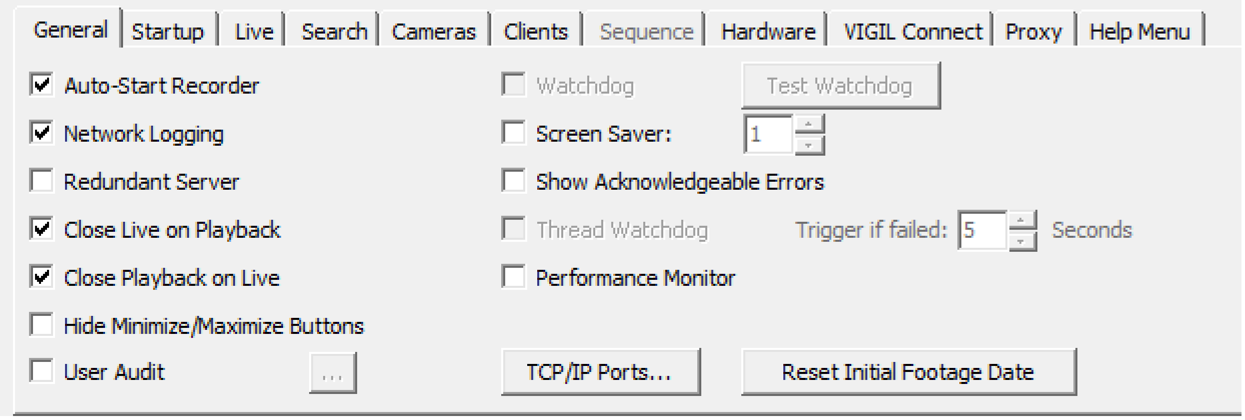
Pre Alarm Backup: 1 Mins

Post Alarm Backup: 1 Mins

Figure 6-3: Server Settings Tab - Offsite Backup on Alarm Settings

Enable Offsite Backup	Click the check box to enable this option. *Click* … and select Windows or VFS Path to browse to a network location where the footage will be saved.
Alarm Input	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.

6.2 General Tab



☑ Auto-Start Recorder
☑ Network Logging
□ Redundant Server
☑ Close Live on Playback
☑ Close Playback on Live
□ Hide Minimize/Maximize Buttons
□ User Audit
□ Watchdog
□ Screen Saver: 1
□ Show Acknowledgeable Errors
□ Thread Watchdog Trigger if failed: 5 Seconds
□ Performance Monitor

Figure 6-4: Server Settings - General Tab

Auto-Start Recorder	When enabled, the VIGIL Server starts recording footage as soon as the VIGIL Server program is launched. When disabled, the user must manually start the recorder using the controls in the Recorder Controls window.
Network Logging	Logs network activity that can be reviewed in the *Network Log Analyzer*.
Redundant VIGIL Server	This feature only applies to Analog Cameras. 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.
Close Live On Playback	When enabled, the *Live Viewer* window will close when the *Search* window is opened in order to conserve system resources.
Close Playback on Live	When enabled, the *Search* window will close when the *Live Viewer* window is opened in order to conserve system resources.
Hide Minimize Maximize Buttons	When enabled, hides the *Minimize* and *Maximize* window buttons on the main VIGIL Server screen.
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 if an error is recorded in the *Audit Log*; this window will display until the error has been acknowledged by a user.

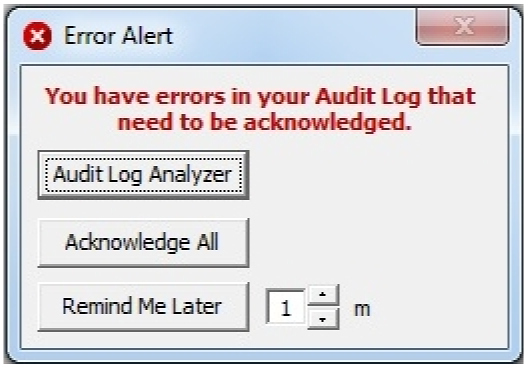
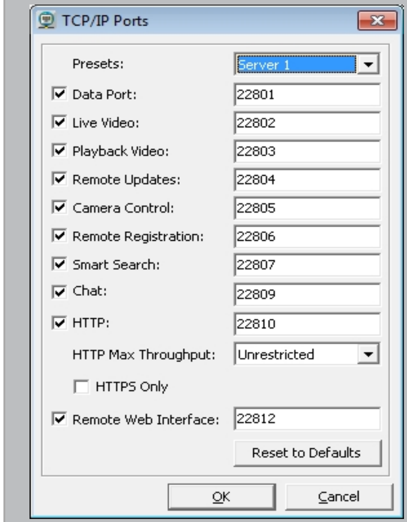
<table>
<tr><td rowspan="4"></td><td rowspan="3">Error Alert
You have errors in your Audit Log that need to be acknowledged.

Figure 6-5: Error Alert Window</td><td>**Audit Log Analyzer**</td><td>Opens the *Audit Log Analyzer* where error alerts can be reviewed.</td></tr>
<tr><td>**Acknowledge All**</td><td>Acknowledges all error alerts.</td></tr>
<tr><td>**Remind Me later**</td><td>Closes the *Error Alert* window and opens it again after a set number of minutes.</td></tr>
<tr><td colspan="3">**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.</td></tr>
<tr><td>**Thread Watchdog**</td><td colspan="3">For systems with advanced video stream freeze detection hardware, enabling this feature will make VIGIL Server monitor video request threads. If a thread stops responding after the configured amount of time, it will be restarted. This can help with video signals that tend to freeze.</td></tr>
<tr><td>**Performance Monitor**</td><td colspan="3">Enables VIGIL Server performance monitoring for diagnostic purposes.
⚠ **Warning:** Because continuous use of this function will adversely affect VIGIL Server performance, enabling Performance Monitor is not generally recommended.</td></tr>
</table>

TCP/IP Ports	Allows the configuration of the TCP/IP ports used by VIGIL Server to connect with VIGIL Clients.		
	 TCP/IP Ports Presets: Server 1 ☑ Data Port: 22801 ☑ Live Video: 22802 ☑ Playback Video: 22803 ☑ Remote Updates: 22804 ☑ Camera Control: 22805 ☑ Remote Registration: 22806 ☑ Smart Search: 22807 ☑ Chat: 22809 ☑ HTTP: 22810 HTTP Max Throughput: Unrestricted ☐ HTTPS Only ☑ Remote Web Interface: 22812 **Figure 6-6:**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.		

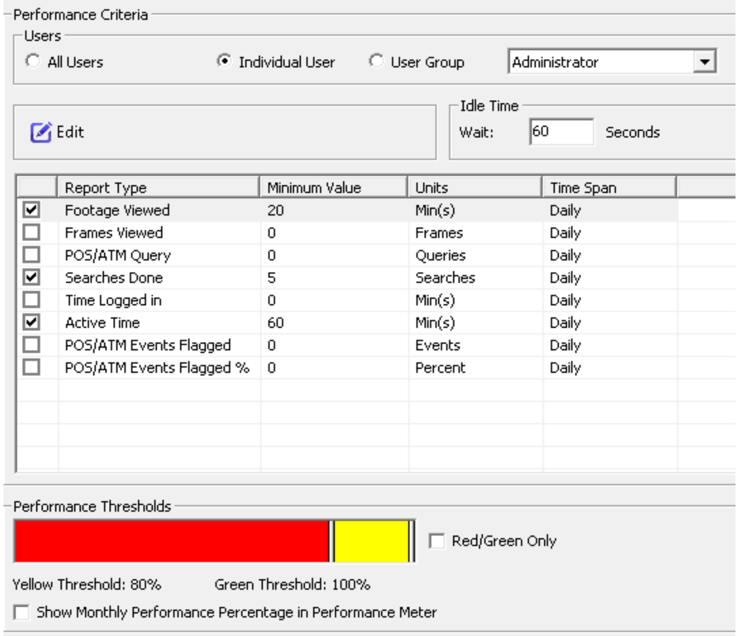
6.2.1 User Audit

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.



Performance Criteria

Users

○ All Users ● Individual User ○ User Group Administrator

Edit

Idle Time

Wait: 60 Seconds

	Report Type	Minimum Value	Units	Time Span
☑	Footage Viewed	20	Min(s)	Daily
□	Frames Viewed	0	Frames	Daily
□	POS/ATM Query	0	Queries	Daily
☑	Searches Done	5	Searches	Daily
□	Time Logged in	0	Min(s)	Daily
☑	Active Time	60	Min(s)	Daily
□	POS/ATM Events Flagged	0	Events	Daily
□	POS/ATM Events Flagged %	0	Percent	Daily

Performance Thresholds

□ Red/Green Only

Yellow Threshold: 80% Green Threshold: 100%

□ Show Monthly Performance Percentage in Performance Meter

Figure 6-7: 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 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

When a user logs in who is configured for *User Performance Monitoring* 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).

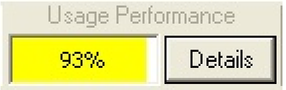


Figure 6-8: User Audit - Main Toolbar Usage Performance Indicator

User Audit Report

To open the User Audit Report tool, select it from the top *Tools* menu. The *User Audit Report* tool provides detailed reports on the report types that are configured.

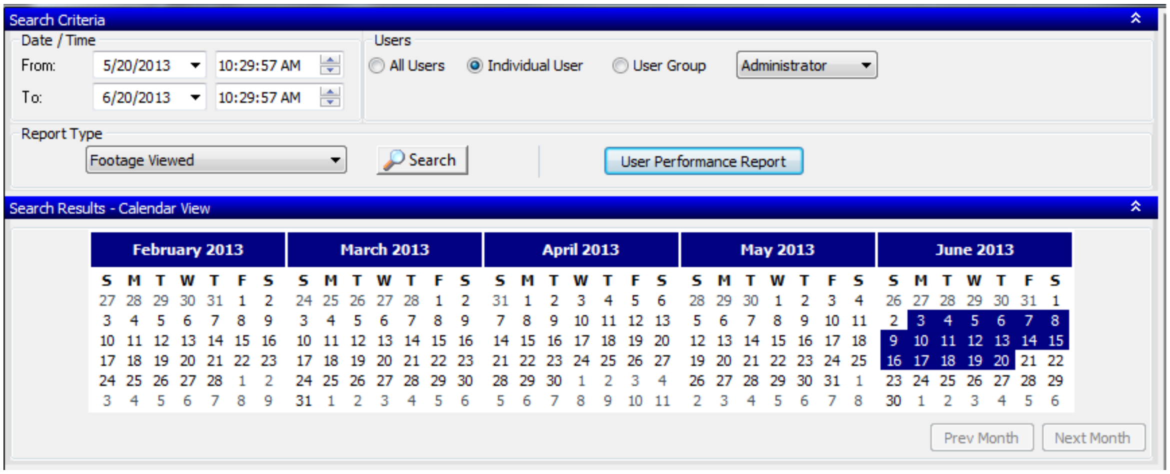


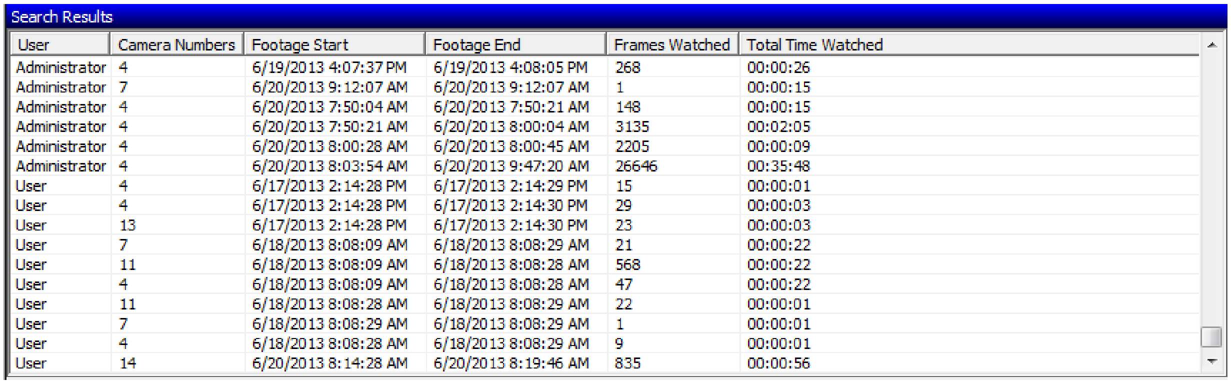
Figure 6-9: User Audit Report - Search Window

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.
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.
Usage Summary – All Report Types	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* query.



Search Results

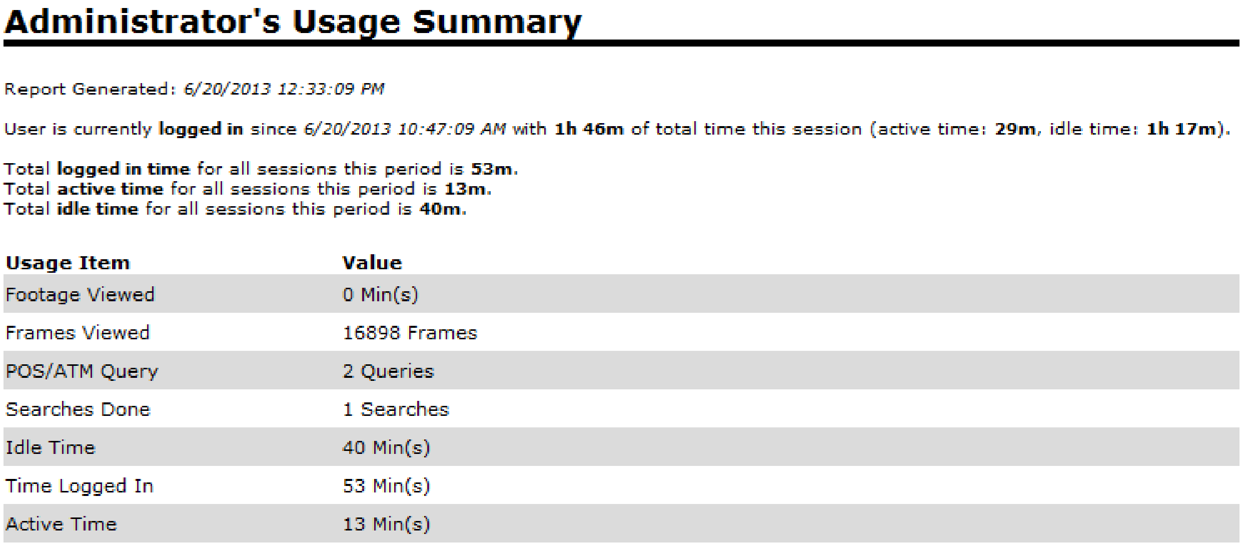
User	Camera Numbers	Footage Start	Footage End	Frames Watched	Total Time Watched
Administrator	4	6/19/2013 4:07:37 PM	6/19/2013 4:08:05 PM	268	00:00:26
Administrator	7	6/20/2013 9:12:07 AM	6/20/2013 9:12:07 AM	1	00:00:15
Administrator	4	6/20/2013 7:50:04 AM	6/20/2013 7:50:21 AM	148	00:00:15
Administrator	4	6/20/2013 7:50:21 AM	6/20/2013 8:00:04 AM	3135	00:02:05
Administrator	4	6/20/2013 8:00:28 AM	6/20/2013 8:00:45 AM	2205	00:00:09
Administrator	4	6/20/2013 8:03:54 AM	6/20/2013 9:47:20 AM	26646	00:35:48
User	4	6/17/2013 2:14:28 PM	6/17/2013 2:14:29 PM	15	00:00:01
User	4	6/17/2013 2:14:28 PM	6/17/2013 2:14:30 PM	29	00:00:03
User	13	6/17/2013 2:14:28 PM	6/17/2013 2:14:30 PM	23	00:00:03
User	7	6/18/2013 8:08:09 AM	6/18/2013 8:08:29 AM	21	00:00:22
User	11	6/18/2013 8:08:09 AM	6/18/2013 8:08:28 AM	568	00:00:22
User	4	6/18/2013 8:08:09 AM	6/18/2013 8:08:28 AM	47	00:00:22
User	11	6/18/2013 8:08:28 AM	6/18/2013 8:08:29 AM	22	00:00:01
User	7	6/18/2013 8:08:29 AM	6/18/2013 8:08:29 AM	1	00:00:01
User	4	6/18/2013 8:08:28 AM	6/18/2013 8:08:29 AM	9	00:00:01
User	14	6/20/2013 8:14:28 AM	6/20/2013 8:19:46 AM	835	00:00:56

Figure 6-10: User Audit - Sample User Audit Report

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*

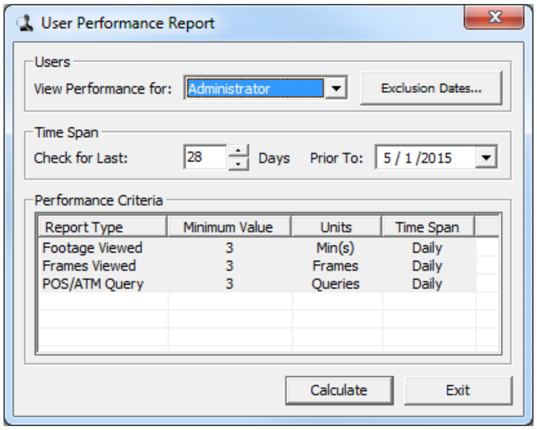
User is currently **logged in** since *6/20/2013 10:47:09 AM* with **1h 46m** of total time this session (active time: **29m**, idle time: **1h 17m**).

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 6-11: User Audit - Usage Summary Report - Example

User Performance Report



View Performance for: Administrator

Check for Last: 28 Days Prior To: 5 / 1 /2015

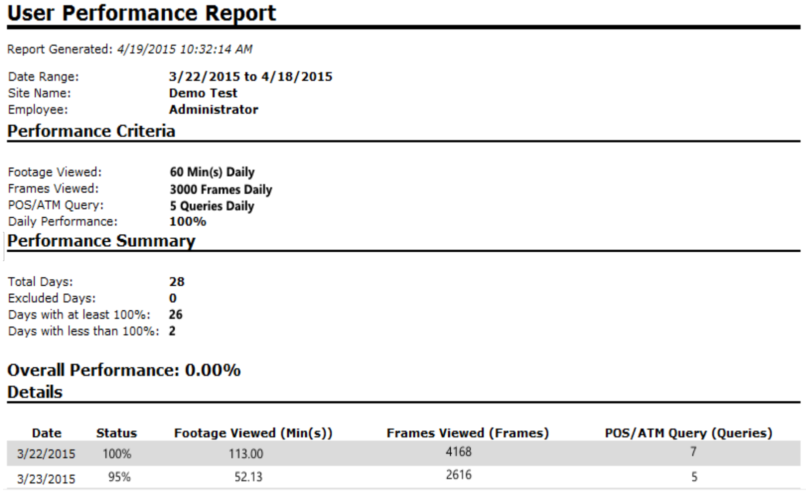
Report Type	Minimum Value	Units	Time Span
Footage Viewed	3	Min(s)	Daily
Frames Viewed	3	Frames	Daily
POS/ATM Query	3	Queries	Daily

Figure 6-12: User Audit - User Performance Report Configuration

Users	**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.
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	**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 the *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

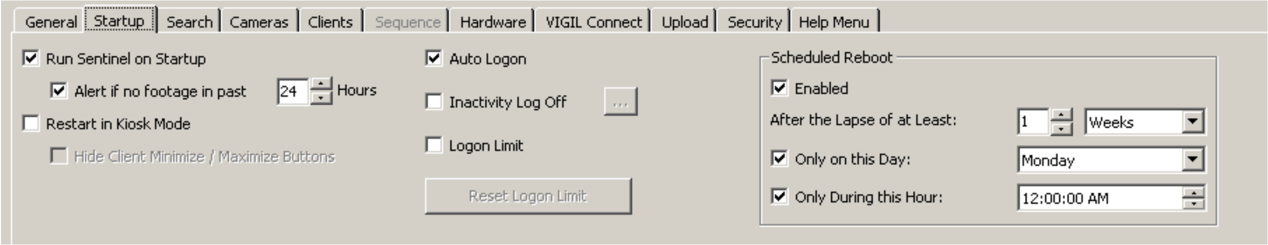
Date	Status	Footage Viewed (Min(s))	Frames Viewed (Frames)	POS/ATM Query (Queries)
3/22/2015	100%	113.00	4168	7
3/23/2015	95%	52.13	2616	5

Figure 6-13: 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.

6.3 Startup Tab

The *Startup* tab allows configuration of VIGIL Server's startup behaviour, as well as scheduling of system reboots.



☑ Run Sentinel on Startup

☑ Alert if no footage in past 24 Hours

☐ Restart in Kiosk Mode

☐ Hide Client Minimize / Maximize Buttons

☑ Auto Logon

☐ Inactivity Log Off

☐ Logon Limit

Scheduled Reboot

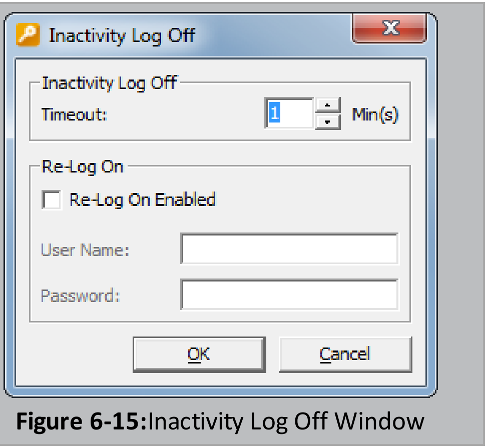
☑ Enabled

After the Lapse of at Least: 1 Weeks

☑ Only on this Day: Monday

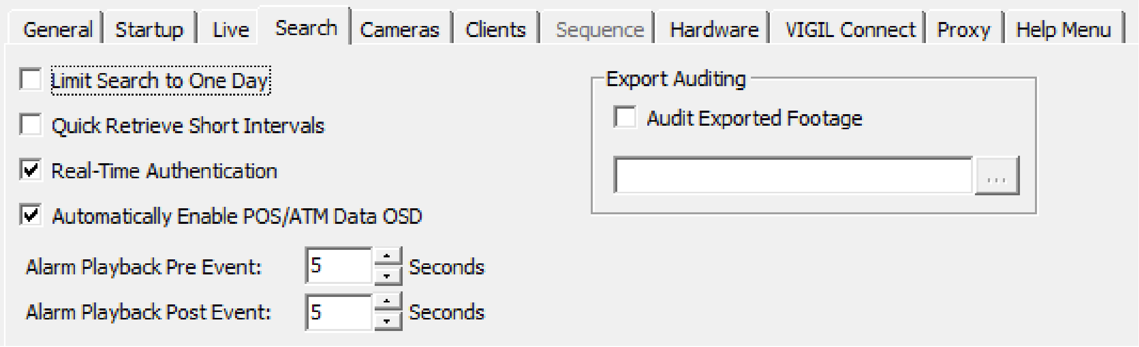
☑ Only During this Hour: 12:00:00 AM

Figure 6-14: 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 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.
Auto Logon	When enabled, a specified user is automatically logged into VIGIL Server upon startup. If disabled, VIGIL Server will prompt for a login every time it starts up.
Inactivity Logoff	When enabled, the current user will be logged off the VIGIL Server after a number of minutes of no activity. **Auto Re-Logon** - When enabled, another user is automatically logged in after the number of minutes specified for the *Auto Logoff Timeout.*  Inactivity Log Off Inactivity Log Off Timeout: 1 Min(s) Re-Log On ☐ Re-Log On Enabled User Name: Password: OK Cancel **Figure 6-15:**Inactivity Log Off Window
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.
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.

6.4 Search Tab

The *Search* tab defines search parameter and settings for the VIGIL Server. Searches are performed via VIGIL Client.



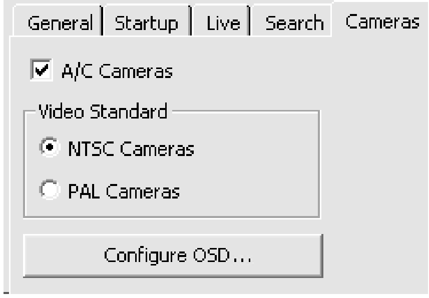
☐ Limit Search to One Day
☐ Quick Retrieve Short Intervals
☑ Real-Time Authentication
☑ Automatically Enable POS/ATM Data OSD
Alarm Playback Pre Event: 5 Seconds
Alarm Playback Post Event: 5 Seconds
☐ Audit Exported Footage

Figure 6-16: 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 onlyfor 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 ClientSearch 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.

6.5 Cameras Tab

The *Cameras* tab specifies the type of cameras being recorded.



☑ A/C Cameras
● NTSC Cameras
○ PAL Cameras

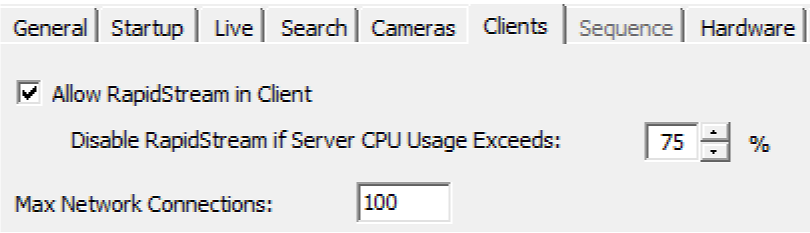
Figure 6-17: Settings - Server Settings Tab - Cameras Tab

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.

6.6 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.)



☑ Allow RapidStream in Client

Disable RapidStream if Server CPU Usage Exceeds: 75 %

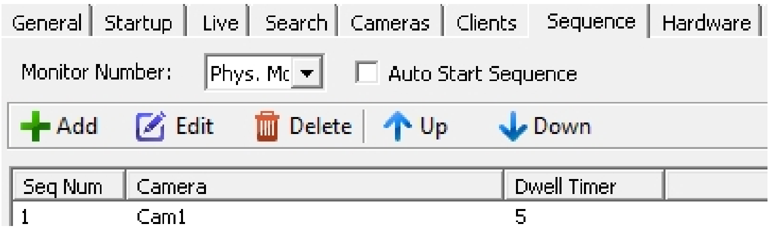
Max Network Connections: 100

Figure 6-18: Settings - Server Settings Tab - Client Tab

Allow RapidStream in Client	When enabled, the Playback window in VIGIL Client will have the option to playback video at *Full Resolution* or at a *CIF Resolution* using *RapidStream* technology.
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.

6.7 Sequence Tab

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.



Monitor Number: Phys. Mc ▾ □ Auto Start Sequence

Seq Num	Camera	Dwell Timer
1	Cam1	5

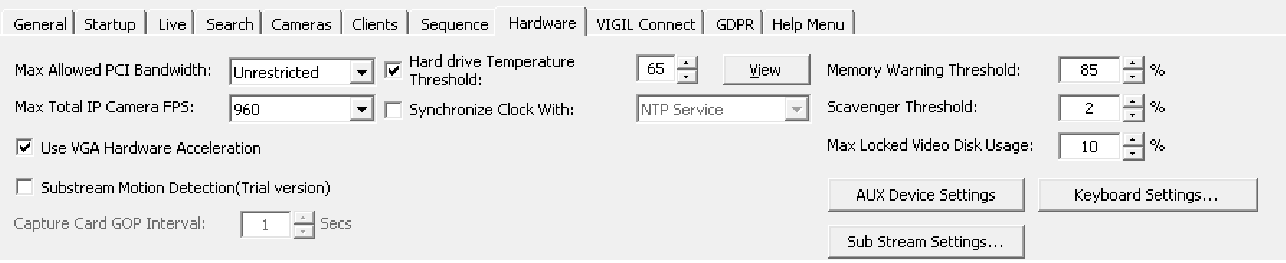
Figure 6-19: Settings - Server Settings Tab - Sequence Tab

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.

6.8 Hardware Tab

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



Max Allowed PCI Bandwidth: Unrestricted

☑ Hard drive Temperature Threshold: 65

Memory Warning Threshold: 85 %

Max Total IP Camera FPS: 960

☐ Synchronize Clock With: NTP Service

Scavenger Threshold: 2 %

☑ Use VGA Hardware Acceleration

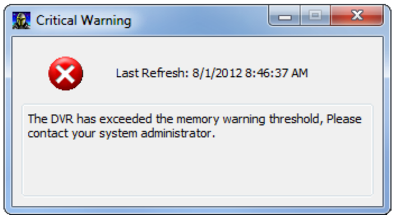
Max Locked Video Disk Usage: 10 %

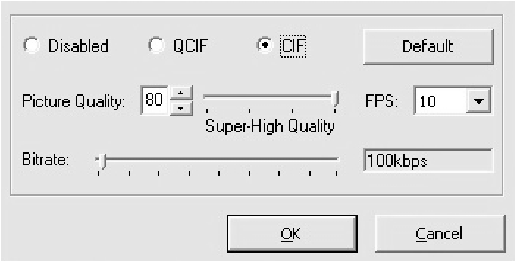
☐ Substream Motion Detection(Trial version)

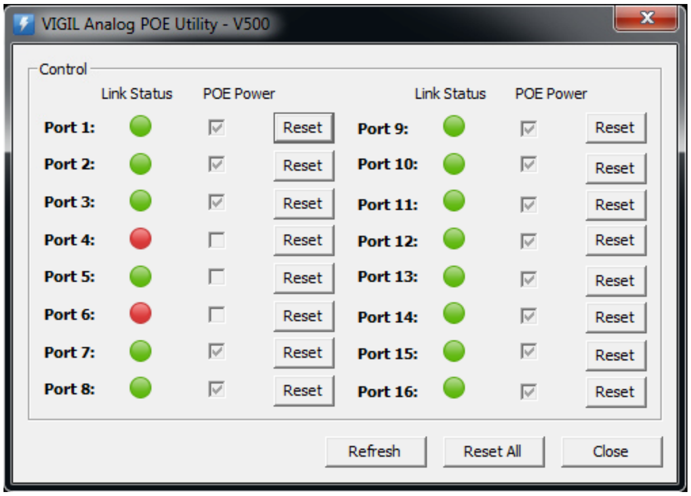
Capture Card GOP Interval: 1 Secs

Figure 6-20: Settings - Server Settings Tab - Hardware Tab

Max Allowed PCI Bandwidth	Restricts the amount of data the video capture card can push through the PCI bus.
Max Total IP Camera FPS	Restricts the combined total frame rate for all network cameras. Lower the setting from default if the VIGIL Server experiences performance issues when the *Live Viewer* is open.
Use VGA Hardware Acceleration	When enabled, software rendered *Live Viewer* (and IP cameras in hardware Live Viewer) will be rendered using *Hardware Acceleration* (YUV), when disabled they will be rendered using GDI.
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. After enabling Substream Motion Detection, the user must configure a Capture Card GOP Interval. **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.
Hardware CODEC	On *PROSERIES* systems or hybrid NVRs, select the hardware CODEC to use, MPEG4 or H264/H265. Changing the Hardware CODEC requires a system reboot.
Skip Channel	On *PROSERIES* systems, enable *Skip Channel* to only use even numbered channels. This reduces the number of inputs by half, allowing each input to reach maximum

		FPS and resolution.
Non Real Time Capture		On *PROSERIES HCI* version cards, enable this option to enable recording at higher resolution then 352x240. Enabling this option will cause the feed to not record in real time.
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.
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 NTP 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.
	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 sychronization and any future auto-synchronizations will be perfomred according to the *Sync Frequency* value.
	Test NTP	Attempts to synchronize the time on the VIGIL Server system immediately.
	View Report	Opens the *Windows Event Viewer*. Select the System log and look for an entry at the top of the list with the Source "W32Time" to synchronize with. **Note:**The NTP test will not record an event in the Windows Event log if the time is already correct.
Memory Warning Threshold		This setting monitors the memory usage of the VIGIL Server process. Due to limitations in Windows there is a limit on the amount of memory a single process can address. If the process reaches the configured threshold, a warning will pop up indicating that the memory usage is high. If this warning pops up please contact your system administrator or support department.  Critical Warning Last Refresh: 8/1/2012 8:46:37 AM The DVR has exceeded the memory warning threshold, Please contact your system administrator. **Figure 6-21:**Memory Threshold Warning Popup
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.

	Example: If the Scavenger Threshold value is set to 10%, VIGIL will begin to scavenge footage whenever a media drive reaches 90% capacity.
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. Dynamic loading of ONVIF alarm events can also be performed via the AUX Device Settings.
Sub Stream Settings...	Set the sub-stream image settings for analog cameras. Click the *Sub Stream Settings...* button to launch the below window.  ○ Disabled ○ QCIF ● CIF Picture Quality: 80 Super-High Quality FPS: 10 Bitrate: 100kbps **Figure 6-22:**VIGIL Server Settings- Hardware Tab - Substream Settings **Note:** - One 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.
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.
Launch POE Settings Utility...	Launches the VIGIL Analog PoE Settings Utility (pictured below). **Note:** This button is only visible on VIGIL NVRs with Analog PoE (Power-over-Ethernet) capability and is not pictured in the example at the beginning of this section. The appearance of the utility may very depending on the NVR on which its installed.



	Link Status	POE Power			Link Status	POE Power	
Port 1:	🟢	☑	Reset	**Port 9:**	🟢	☑	Reset
Port 2:	🟢	☑	Reset	**Port 10:**	🟢	☑	Reset
Port 3:	🟢	☑	Reset	**Port 11:**	🟢	☑	Reset
Port 4:	🔴	□	Reset	**Port 12:**	🟢	☑	Reset
Port 5:	🟢	□	Reset	**Port 13:**	🟢	☑	Reset
Port 6:	🔴	□	Reset	**Port 14:**	🟢	☑	Reset
Port 7:	🟢	☑	Reset	**Port 15:**	🟢	☑	Reset
Port 8:	🟢	☑	Reset	**Port 16:**	🟢	☑	Reset

Figure 6-23:VIGIL Analog POE Utility

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:

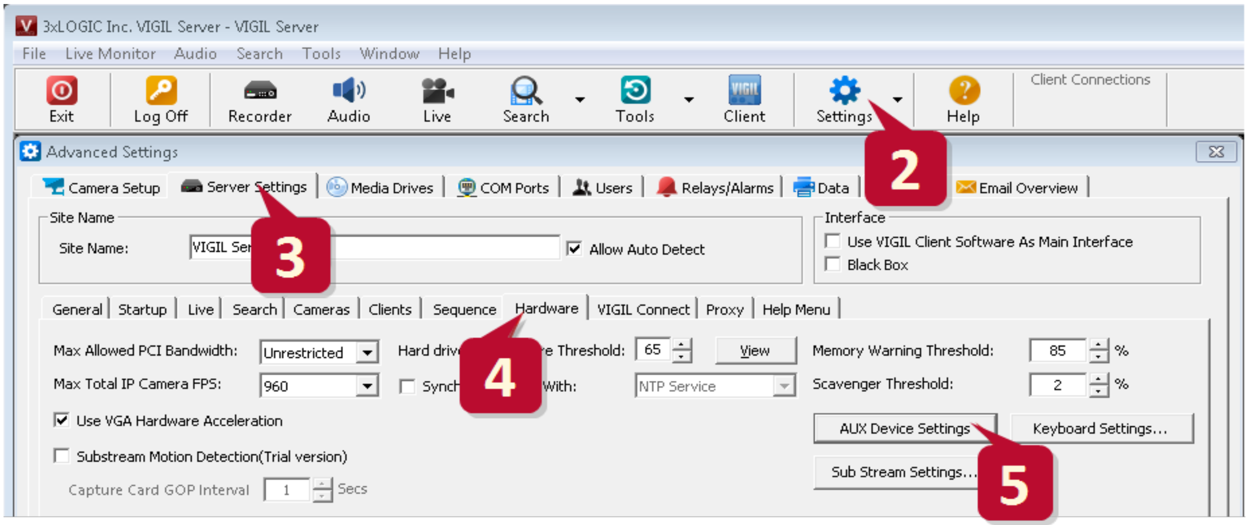
- If a camera is plugged into a PoE port, the *Link Status* indicator will be green. If a port is unused, the indicator will be red. On some NVRs, status indicators will be replaced by simple "Online" or "Offline" text.
- The *POE Power* check box indicates if a connected camera is currently utilizing PoE.
- Click the **Reset** button on a desired port to cut and restore power, effectively forcing a camera reset.

6.8.1 AUX Device Settings - Dynamically Loading ONVIF Alarm Events from XML Config File

As of VIGIL Server v9, Alarm Events (DIO) for ONVIF devices can be dynamically loaded from an xml file located in the VIGIL Server root directory. This allows the quick addition of ONVIF-based alarm events from newer camera models without the need for a VIGIL Server update. Replacing (with an updated file) or updating the xml file and reloading are the only requirements to update available ONVIF DIO alarm events.

ONVIF alarm events can be loaded via the *VIGIL Server Settings >Server Settings>Hardware>AUX Device Settings* form. To begin:

1. Login to VIGIL Server



Site Name: VIGIL Ser

☑ Allow Auto Detect

☐ Use VIGIL Client Software As Main Interface

☐ Black Box

Max Allowed PCI Bandwidth: Unrestricted

Max Total IP Camera FPS: 960

Hard driv... e Threshold: 65

☐ Synch... With: NTP Service

Memory Warning Threshold: 85 %

Scavenger Threshold: 2 %

☑ Use VGA Hardware Acceleration

☐ Substream Motion Detection(Trial version)

Capture Card GOP Interval 1 Secs

Figure 6-24: Dynamically Loading ONVIF Alarm Events - Opening the AUX Device Settings

2. Click the Settings button in the icon menu toolbar.
3. On the Settings window, select the Server Settings tab.
4. Select the Hardware tab.
5. Click the AUX Device Settings button.

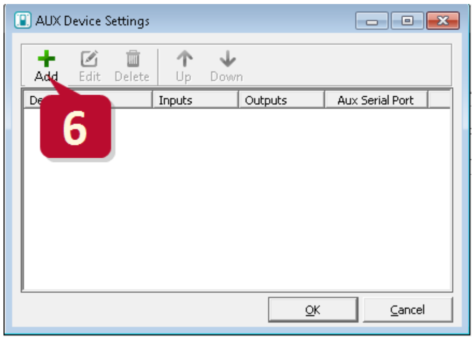
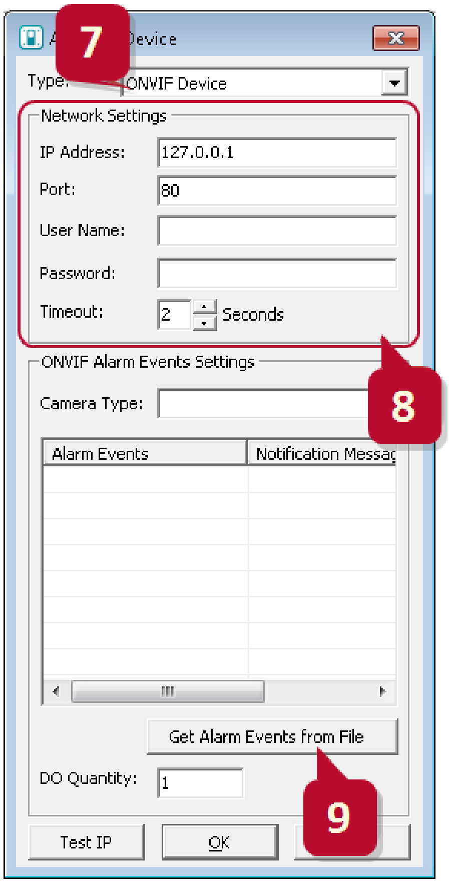


Figure 6-25: Dynamically Loading ONVIF Alarm Events - Adding ONVIF Aux Device

6. Select Add (or choose an existing ONVIF device from the list and select Edit).

The Add DIO Device window will now deploy. A user may configure a new DIO device from this window.

7. Select ONVIF Device in the Type dropdown menu. The Add DIO Device form will expand.



A Device

Type: ONVIF Device

Network Settings

IP Address: 127.0.0.1

Port: 80

User Name:

Password:

Timeout: 2 Seconds

ONVIF Alarm Events Settings

Camera Type:

Alarm Events	Notification Messag

DO Quantity: 1

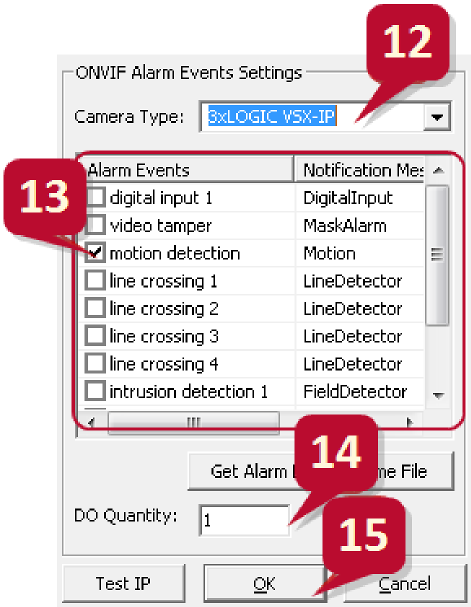
Figure 6-26: Dynamically Loading ONVIF Alarm Events - Retreiving Events from Config File

8. Fill out basic Network Settings.

After filling in basic network connection values, you may now load alarm events from the alarm events configuration file. To begin:

9. Select Get Alarm Events from File. A Windows file browser will deploy.
10. Navigate to your VIGIL Server install directory (e.g C:\\Program Files\VIGIL\Server)
11. Select the alarmevents.xml file.

The Alarm Events list will now populate with events for the selected Camera Type (3xLOGIC VSX-IP is the default Camera Type).



Alarm Events	Notification Mes
□ digital input 1	DigitalInput
□ video tamper	MaskAlarm
☑ motion detection	Motion
□ line crossing 1	LineDetector
□ line crossing 2	LineDetector
□ line crossing 3	LineDetector
□ line crossing 4	LineDetector
□ intrusion detection 1	FieldDetector

Figure 6-27: Dynamically Loading ONVIF Alarm Events - Selecting Events Loaded from Config File

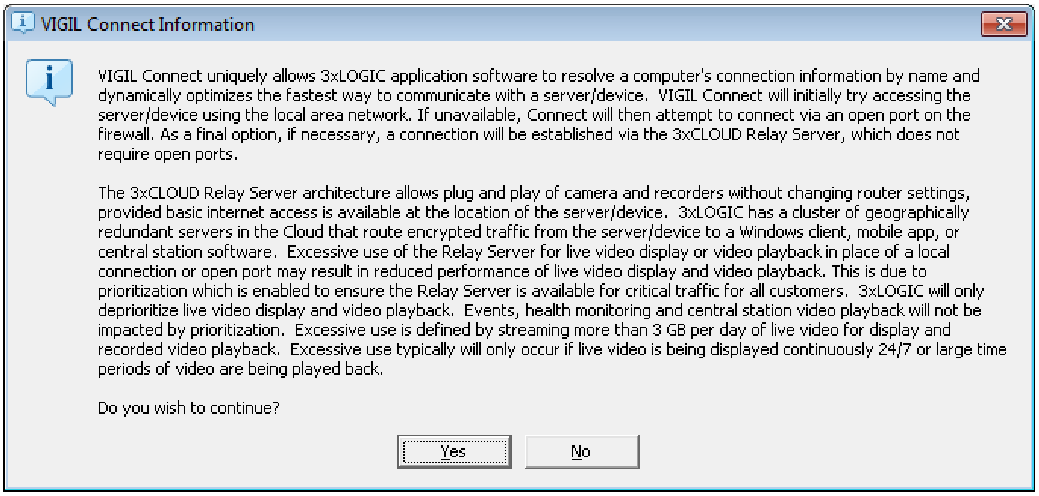
12. Select the desired Camera Type. Alarm events configured within the xml file that correspond to the chosen camera type will populate the list.
13. Check-off desired Alarm Events
14. Set a DO Quantity.
15. Click OK to add the new DIO device.

The DIO Device will now be configured in VIGIL Server using the chosen Alarm Events. To update ONVIF DIO Alarm events in the future, overwrite the alarmevents.xml file in the VIGIL install directory with a newer version provided to you by 3xLOGIC.

6.9 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:



VIGIL Connect Information

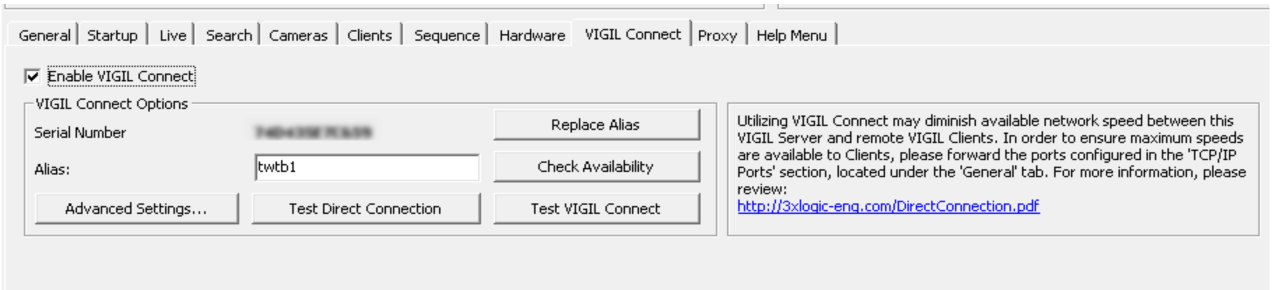
VIGIL Connect uniquely allows 3xLOGIC application software to resolve a computer's connection information by name and dynamically optimizes the fastest way to communicate with a server/device. VIGIL Connect will initially try accessing the server/device using the local area network. If unavailable, Connect will then attempt to connect via an open port on the firewall. As a final option, if necessary, a connection will be established via the 3xCLOUD Relay Server, which does not require open ports.

The 3xCLOUD Relay Server architecture allows plug and play of camera and recorders without changing router settings, provided basic internet access is available at the location of the server/device. 3xLOGIC has a cluster of geographically redundant servers in the Cloud that route encrypted traffic from the server/device to a Windows client, mobile app, or central station software. Excessive use of the Relay Server for live video display or video playback in place of a local connection or open port may result in reduced performance of live video display and video playback. This is due to prioritization which is enabled to ensure the Relay Server is available for critical traffic for all customers. 3xLOGIC will only deprioritize live video display and video playback. Events, health monitoring and central station video playback will not be impacted by prioritization. Excessive use is defined by streaming more than 3 GB per day of live video for display and recorded video playback. Excessive use typically will only occur if live video is being displayed continuously 24/7 or large time periods of video are being played back.

Do you wish to continue?

Figure 6-28: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.



☑ Enable VIGIL Connect

VIGIL Connect Options

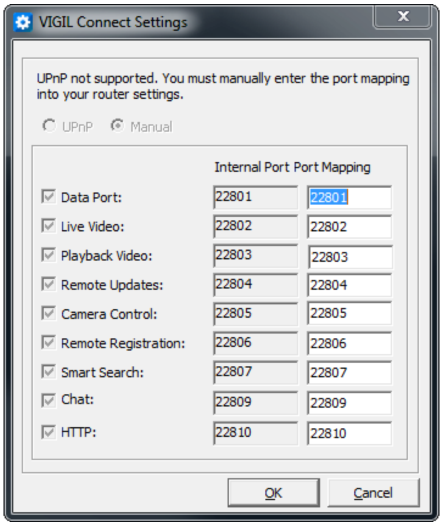
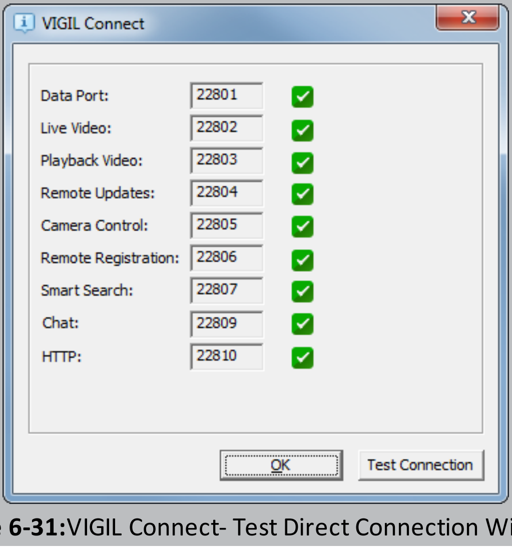
Serial Number [redacted]

Alias: twtb1

Utilizing VIGIL Connect may diminish available network speed between this VIGIL Server and remote VIGIL Clients. In order to ensure maximum speeds are available to Clients, please forward the ports configured in the 'TCP/IP Ports' section, located under the 'General' tab. For more information, please review:
http://3xlogic-eng.com/DirectConnection.pdf

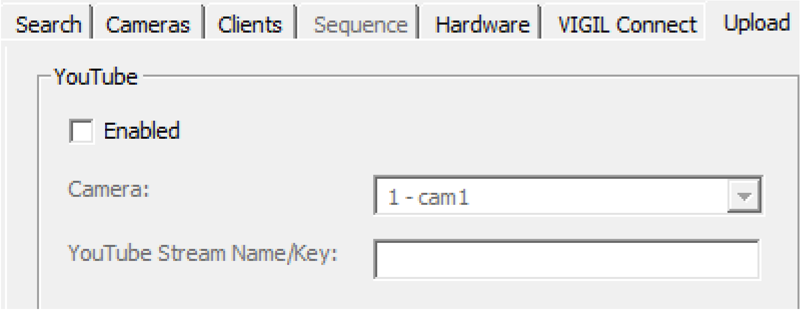
Figure 6-29: Settings - Server Settings Tab - VIGIL Connect Tab

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 automatically 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 create 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.**
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.  UPnP not supported. You must manually enter the port mapping into your router settings. ○ UPnP ● Manual Internal Port Port Mapping ☑ Data Port: 22801 22801 ☑ Live Video: 22802 22802 ☑ Playback Video: 22803 22803 ☑ Remote Updates: 22804 22804 ☑ Camera Control: 22805 22805 ☑ Remote Registration: 22806 22806 ☑ Smart Search: 22807 22807 ☑ Chat: 22809 22809 ☑ HTTP: 22810 22810 **Figure 6-30:**VIGIL Connect Settings Window
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.) Click the *Test Connection* button to run the test again.  Data Port: 22801 ✓ Live Video: 22802 ✓ Playback Video: 22803 ✓ Remote Updates: 22804 ✓ Camera Control: 22805 ✓ Remote Registration: 22806 ✓ Smart Search: 22807 ✓ Chat: 22809 ✓ HTTP: 22810 ✓ **Figure 6-31:**VIGIL Connect- Test Direct Connection Window
Test VIGIL Connect	Tests VIGIL Connect using your current configuration.

6.10 Upload

The Upload tab provides configuration for pushing a live stream to external video platforms.



□ Enabled

Camera: 1 - cam1

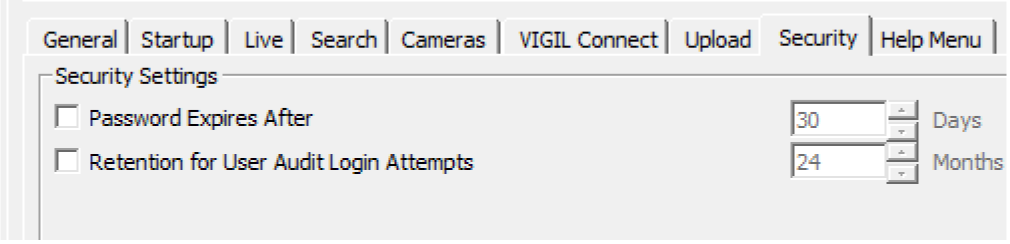
YouTube Stream Name/Key:

Figure 6-32:VIGIL Server Settins - Server Settings - Upload Tab

To enable streaming to YouTube, toggle the Enabled option and select the desired *Camera.* Enter your *YouTube Stream Name / Key*. Save the settings to begin streaming footage from the selected camera.

6.11 Security

The Security tab features configuration options for security features of the VIGIL Server.



Security Settings

□ Password Expires After 30 Days

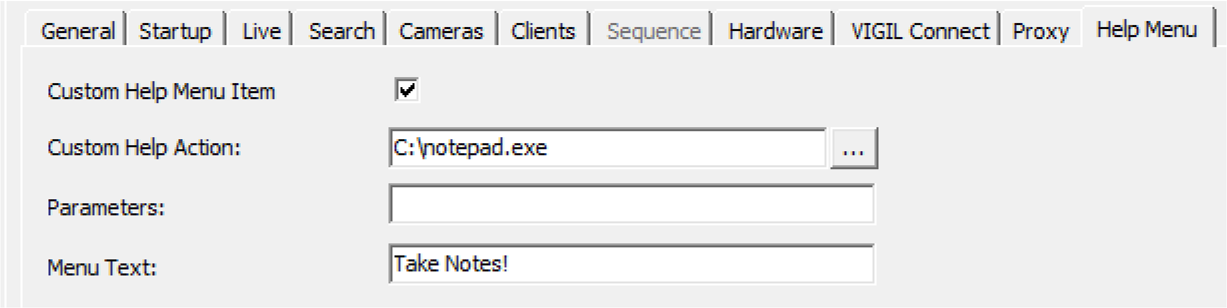
□ Retention for User Audit Login Attempts 24 Months

Figure 6-33:VIGIL Server Settings - Server Settings - Security Tab

Password Expires After	IF enabled, the user can set the VIGIL Server USer password expiry interva (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.

6.12 Help Menu Tab

The *Help Menu* tab allows the user to configure an application that can be run the system tray icon right-click menu.



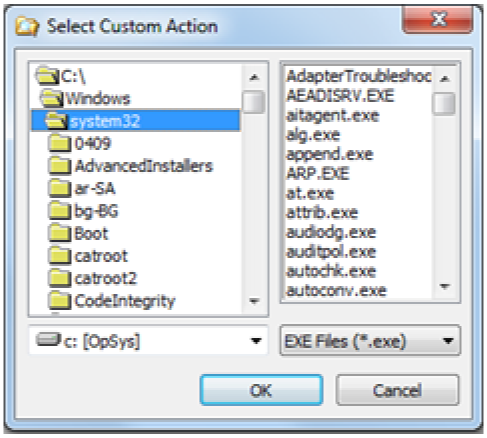
Custom Help Menu Item ☑

Custom Help Action: C:\notepad.exe

Parameters:

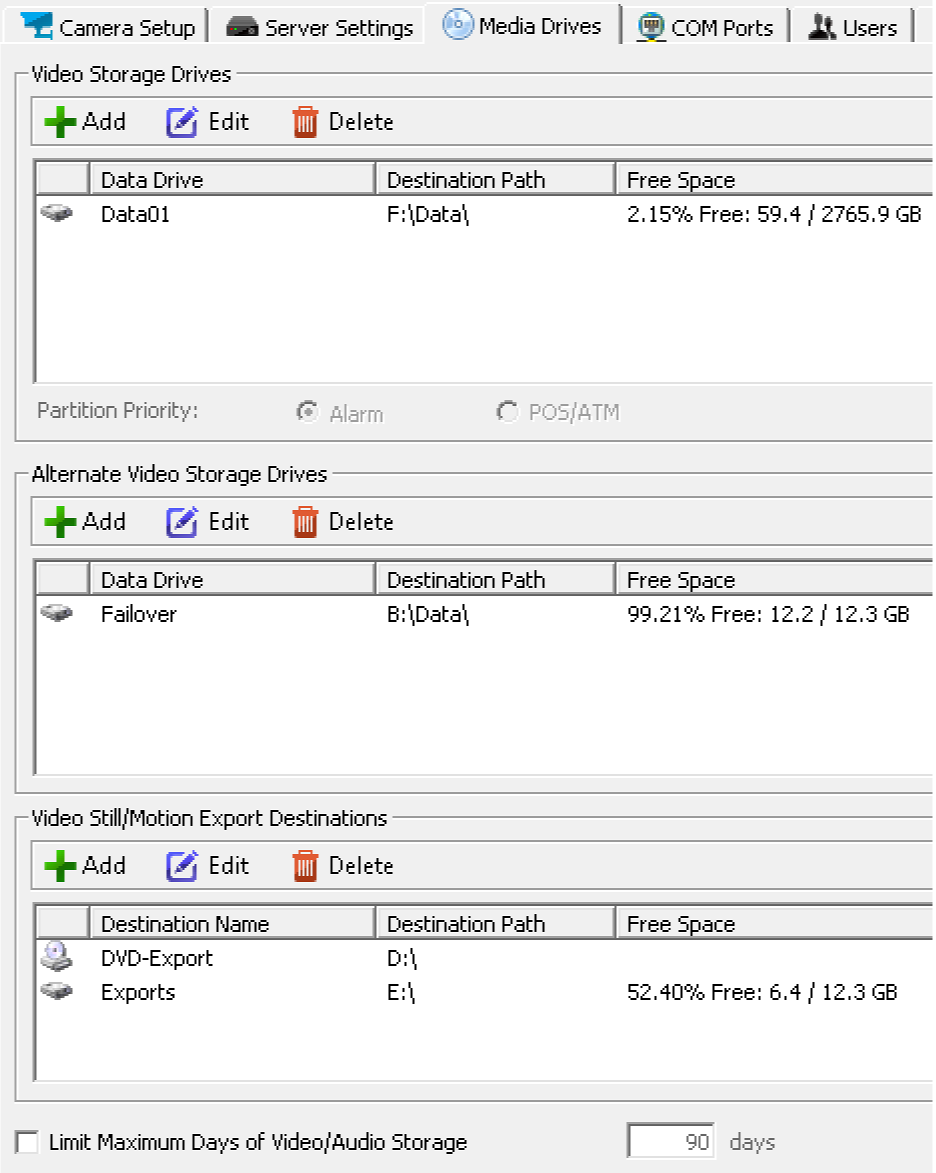
Menu Text: Take Notes!

Figure 6-34: Settings - Server Settings Tab - Help Menu Tab

Custom Help Menu Item	Enables the *Customized Help Menu Item*. Check this box to begin creating a custom help icon / item for your system tray right-click menu.	
Custom Help Action	Set a directory path to the command you are planning to assign to your custom icon. Click the ... button to browse the list of commands directly. Essentially, the chosen command is what will run when the new custom icon is clicked. Files that are commonly mapped to custom help icons include .exe, .chm, and .htm.	 Select Custom Action C:\ Windows system32 0409 AdvancedInstallers ar-SA bg-BG Boot catroot catroot2 CodeIntegrity AdapterTroubleshoo AEADISRV.EXE aitagent.exe alg.exe append.exe ARP.EXE at.exe attrib.exe audiodg.exe auditpol.exe autochk.exe autoconv.exe c: [OpSys] EXE Files (*.exe) OK Cancel
Parameters	Enter the command line argument(s) that specify an action to take. If no additional actions are required, leave this box blank. (i.e. you have assigned a .exe to your custom help item, you could set it to *Run as Administrator*.	
Menu Text	This text will display as a label for your new custom help item in the VIGIL Server system tray icon right-click menu. Custom help item is displayed above *Exit* in the menu.	

7 Advanced Settings - Media Drives Tab

The *Media Drives* tab configures video recording destinations and export destinations for the VIGIL Server.



Video Storage Drives

	Data Drive	Destination Path	Free Space
	Data01	F:\Data\	2.15% Free: 59.4 / 2765.9 GB

Partition Priority: ● Alarm ○ POS/ATM

Alternate Video Storage Drives

	Data Drive	Destination Path	Free Space
	Failover	B:\Data\	99.21% Free: 12.2 / 12.3 GB

Video Still/Motion Export Destinations

	Destination Name	Destination Path	Free Space
	DVD-Export	D:\	
	Exports	E:\	52.40% Free: 6.4 / 12.3 GB

☐ Limit Maximum Days of Video/Audio Storage 90 days

Figure 7-1: Settings - Media Drives Tab

There are three types of media 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.

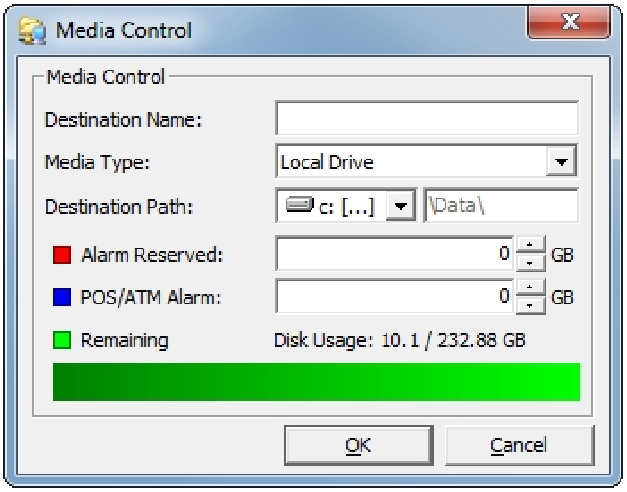
Note: Deleting a location does not remove the physical destination, only the reference to it within VIGIL Server.

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.

7.1 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.



Media Control

Media Control

Destination Name:

Media Type: Local Drive

Destination Path: c: [...] \Data\

🟥 Alarm Reserved: 0 GB

🟦 POS/ATM Alarm: 0 GB

🟩 Remaining Disk Usage: 10.1 / 232.88 GB

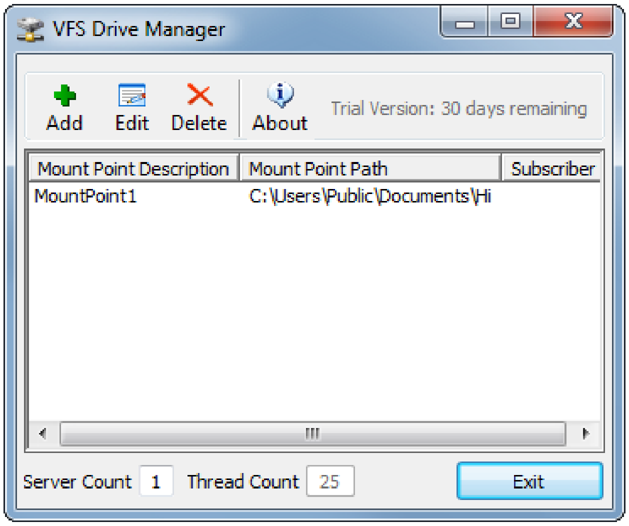
Figure 7-2: Settings - Media Drives Tab - Media Control Window

Destination Name	The name for the video storage location.
Media Type	The media type can be either a Local Drive on the VIGIL Server System, or a Network Drive located on a *Virtual File Server* (VFS) System.
Destination Path	The hard drive and folder path to record video data to. When using a Network drive, this will change to *VFS Server* name and path.
Alarm Reserved	The amount of storage to be reserved for Alarm video footage.
POS/ATM Alarm	The amount of storage to be reserved for POS/ATM Alarm video footage.

7.2 Using a Virtual File Server for Video Storage

It is possible to use a drive on a network server as a video storage destination via the installation of a *Virtual File Server (VFS)* on a Windows PC. Due to the method that Windows networking utilizes to write files across the network it is not suitable for a VIGIL Server to use mapped drives. VFS uses a proprietary method of writing the files across the network. VFS is only used for writing files across a local network, it is not meant for writing files across the Internet.

Install the *Virtual File Server* on the Windows PC with the Hard Drives for network storage. Run the VFS Manager software (Start | Programs | VIGIL and open VFS Manager). You will be met with the window pictured below.



Trial Version: 30 days remaining

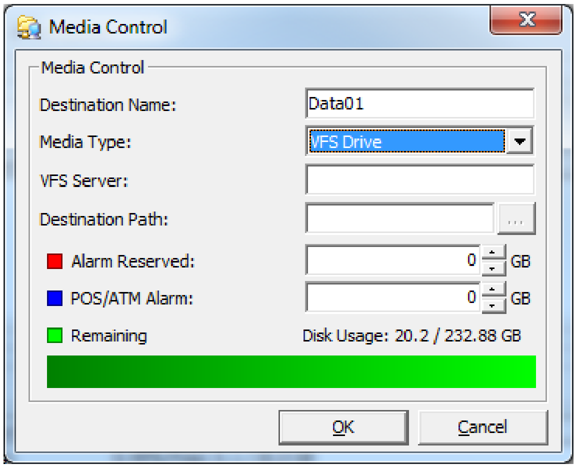
Mount Point Description	Mount Point Path	Subscriber
MountPoint1	C:\Users\Public\Documents\Hi	

Server Count 1 Thread Count 25

Figure 7-3: Settings - Media Drives Tab -VFS Drive Manager

Add a Network/VFS Drive to VIGIL Server

Now, when adding a Video Storage Drive to Server, the user may select *VFS Drive* in the *Media Type* field. The Media Control window will appear as pictured below.



Media Control

Destination Name: Data01

Media Type: VFS Drive

VFS Server:

Destination Path: ...

🟥 Alarm Reserved: 0 GB

🟦 POS/ATM Alarm: 0 GB

🟩 Remaining Disk Usage: 20.2 / 232.88 GB

Figure 7-4: Adding a Network/VFS Drive

VFS Server	Enter the IP Address or Computer Name of the computer the VFS Manager is running on.
Destination Path	Click the ... button to open a list of available network shares on the VFS Server.

7.3 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.

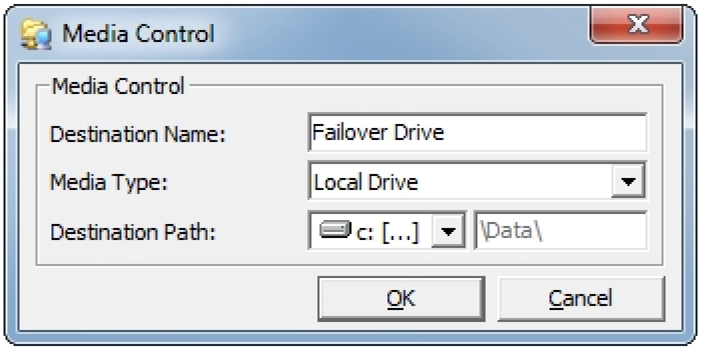
Instead of copying alarm footage under the normal areas for storage, it will be recorded to a special folder that is considered a separate entity. Normal video storage is scavenged and deleted as new footage is written, however these special folders are not scavenged normally; they will retain as much 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 often much rarer, 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.

7.4 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.


Media Control

Media Control

Destination Name: Failover Drive

Media Type: Local Drive

Destination Path: c: [...] \Data\

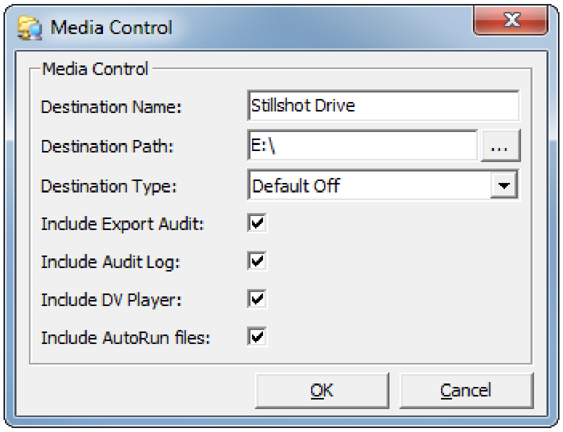
Figure 7-5: Settings - Media Drives Tab - Alternate Video Storage Drives - Media Control Window

Destination Name	The name for the *Alternate Video Storage* destination.
Media Type	The media type can be either a *Local Drive* on the VIGIL Server System, or a *Network Drive* located on a *Virtual File Server (VFS)* System.
Destination Path	The hard drive and folder path to record video data to. When using a *Network Drive*, this will change to *VFS Server* name and path.

7.5 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 us the VIGIL Client application.

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



Media Control

Media Control

Destination Name: Stillshot Drive

Destination Path: E:\

Destination Type: Default Off

Include Export Audit: ☑

Include Audit Log: ☑

Include DV Player: ☑

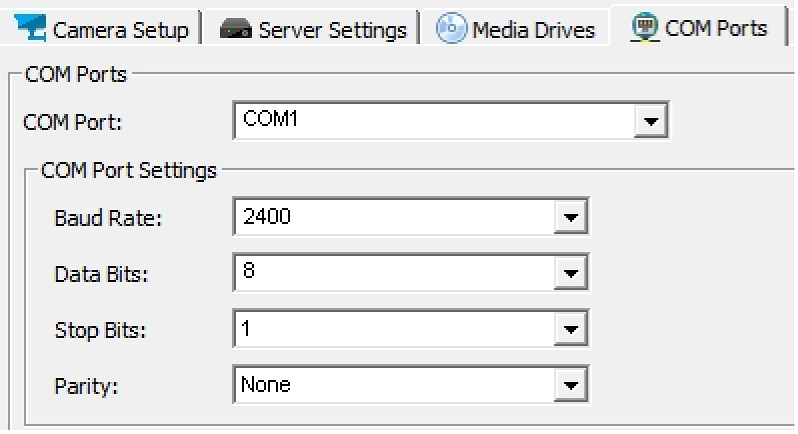
Include AutoRun files: ☑

Figure 7-6: 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.
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.		

8 Advanced Settings - 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.



COM Ports

COM Port: COM1

COM Port Settings

Baud Rate: 2400

Data Bits: 8

Stop Bits: 1

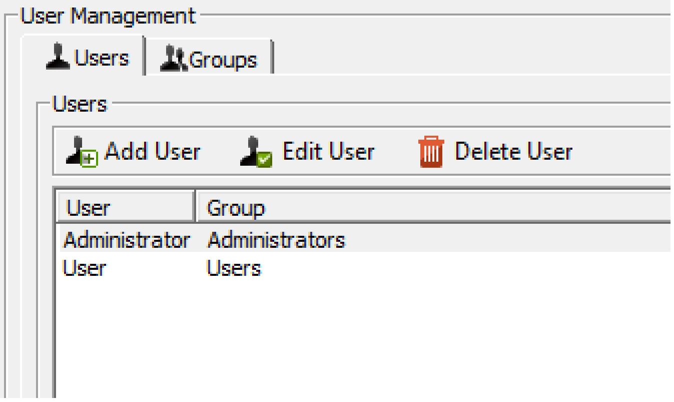
Parity: None

Figure 8-1: 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.

9 Advanced Settings - 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.

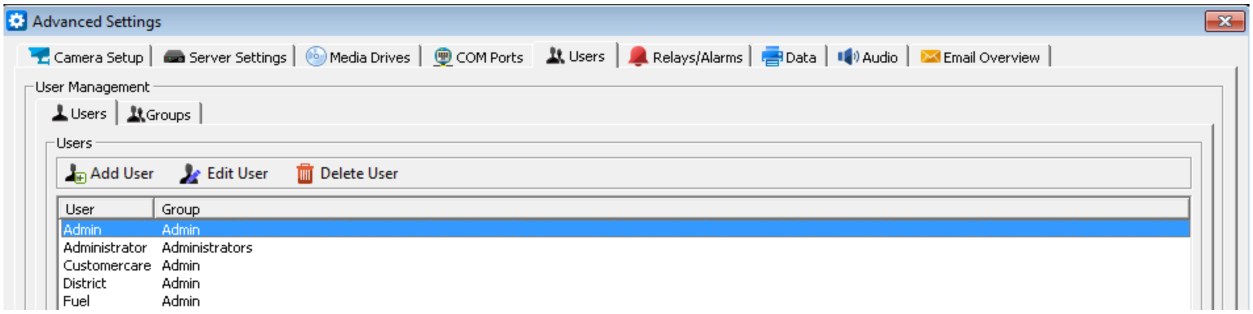


User	Group
Administrator	Administrators
User	Users

Figure 9-1: Settings - User and Group Management Tab - Users Tab

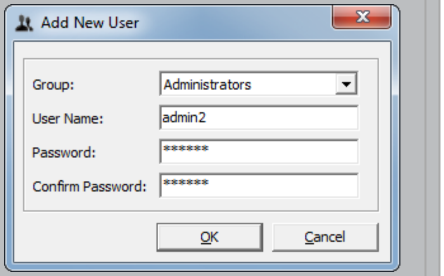
9.1 Users Tab

Click the *Users* tab to access the *User* configuration options.



User	Group
Admin	Admin
Administrator	Administrators
Customercare	Admin
District	Admin
Fuel	Admin

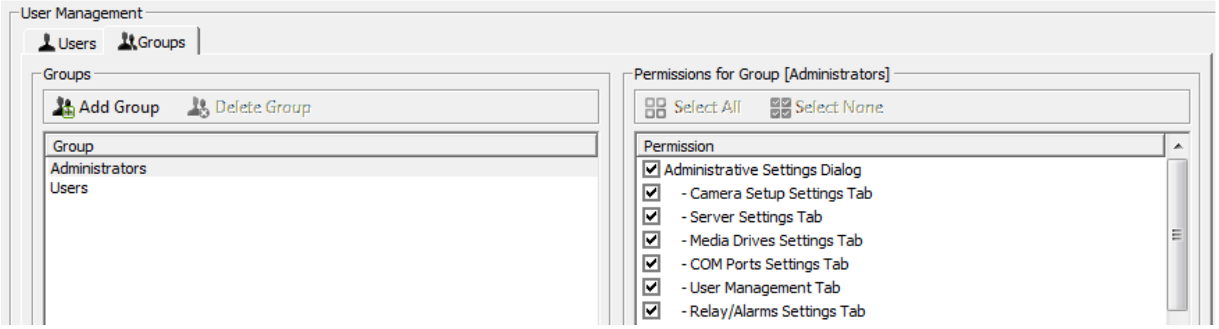
Figure 9-2:VIGIL Server Advanced Settings - Users Tab

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.  Group: Administrators User Name: admin2 Password: ****** Confirm Password: ******
Edit a User	Select a *User* from the drop-down menu and click the *Edit* button. The user’s group or pass-

	word 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	**Note:** This checkbox will only become possible after user management has been activated from the managing VCM and users have been pushed to the VIGIL Server in question. 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.

9.2 Groups Tab

Click the *Groups* tab to access the *Group* configuration options.



Group
Administrators
Users

Permission
☑ Administrative Settings Dialog
☑ - Camera Setup Settings Tab
☑ - Server Settings Tab
☑ - Media Drives Settings Tab
☑ - COM Ports Settings Tab
☑ - User Management Tab
☑ - Relay/Alarms Settings Tab

Figure 9-3: 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. 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.
Delete Group	Select a *Group* from the left-hand window and click the *Delete* button.

9.3 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.

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 ▪ Server Settings Tab ▪ Media Drives Settings Tab ▪ COM Port Settings Tab ▪ User Management Tab ▪ Relays/Alarms Settings Tab ▪ Data Settings Tab ▪ Audio Settings Tab. Uncharged the tabs that you want to exclude access for the selected Group.
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.
Socket Activity Form	This is the Client Connections window, access from the toolbar
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 server and client workstations.
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.
Camera:	Access to view a camera in VIGIL Client . If you want to make the camera covert for a specified Group, deslect the camera in permissions.
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 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.
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.
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.
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: 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.

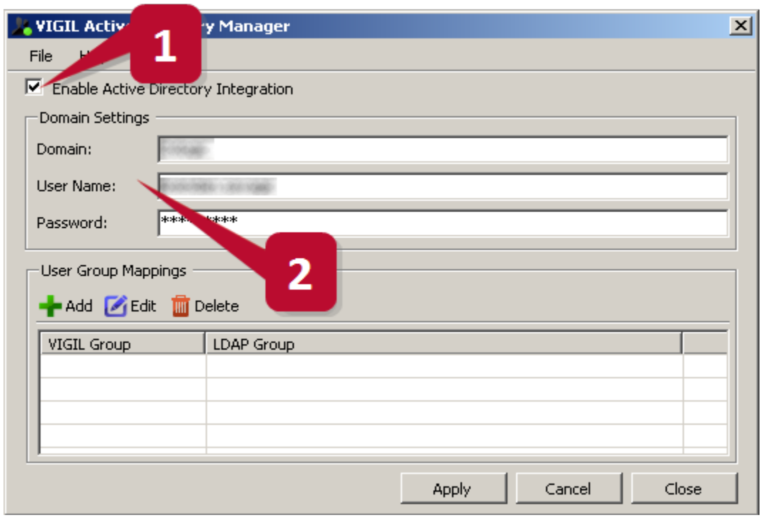
9.4 Active Directory Integration

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:



☑ Enable Active Directory Integration

Password: *** ****

Figure 9-4: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

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:

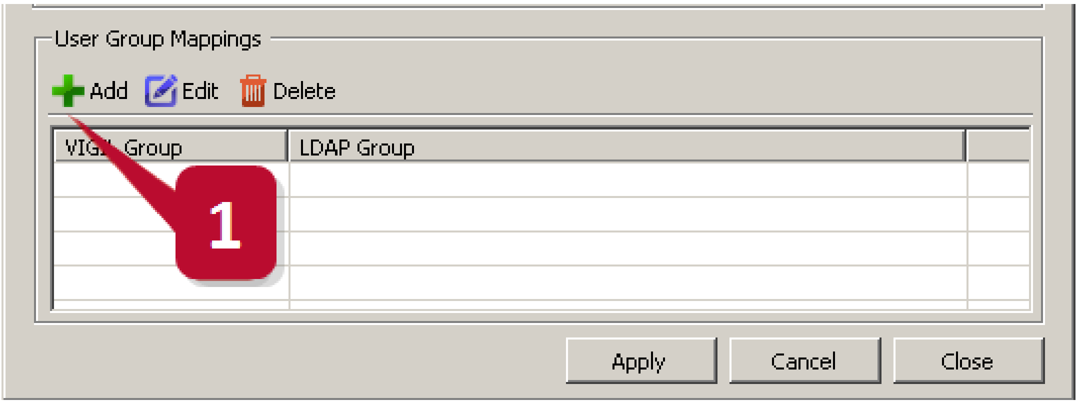


Figure 9-5:VIGIL Active Directory Manager - Adding Windows User Group Mappings

1. Click the *Add* button.

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

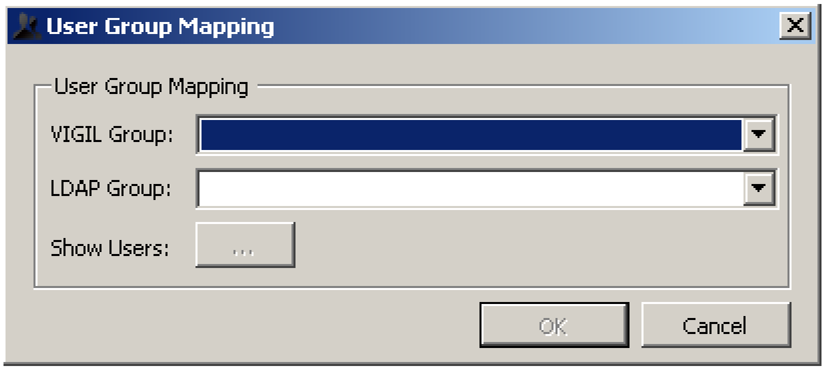


Figure 9-6:VIGIL Active Directory Manager - User Group Mapping Window

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.

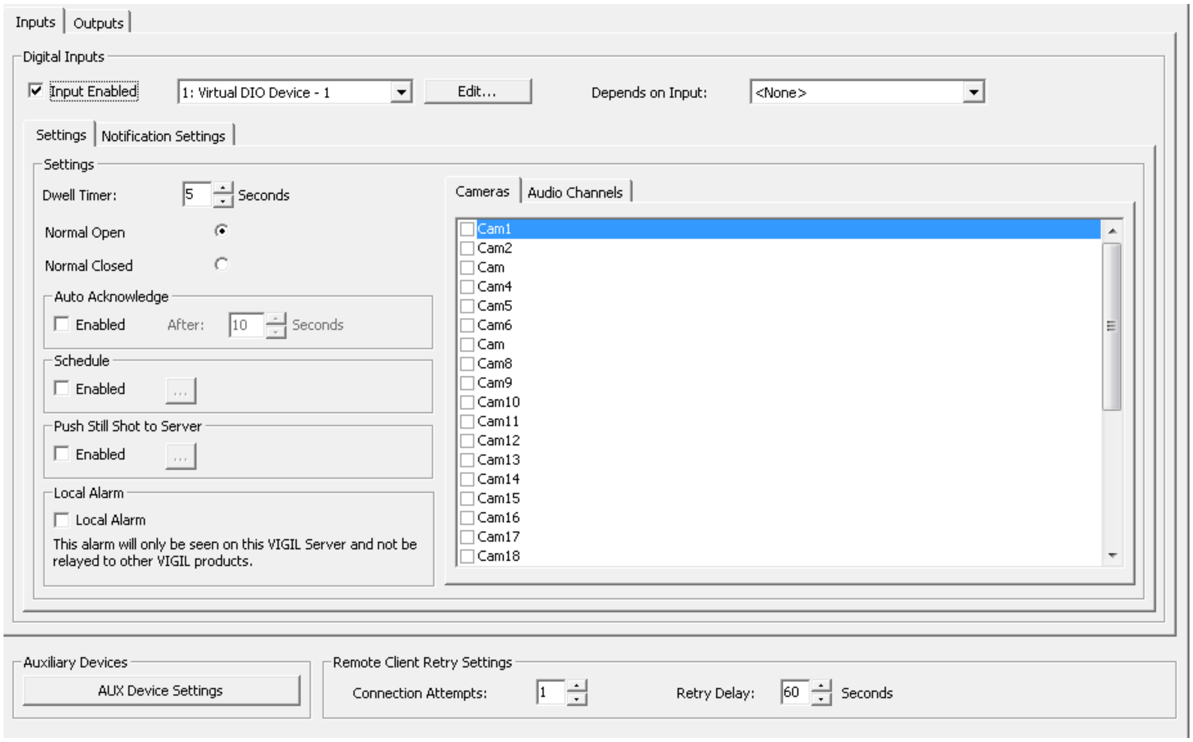
Note: Server logins are refreshed and updated in 2 minute intervals. LDAP Users added to VIGIL Server may take up to 2 minutes to appear in the VIGIL Server UI.

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.

10 Advanced Settings - Relays / Alarms Tab

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



Inputs | Outputs

Digital Inputs

☑ Input Enabled   1: Virtual DIO Device - 1   Edit...   Depends on Input: <None>

Settings | Notification Settings

Settings

Dwell Timer: 5 Seconds

Normal Open ●

Normal Closed ○

Auto Acknowledge

☐ Enabled   After: 10 Seconds

Schedule

☐ Enabled ...

Push Still Shot to Server

☐ Enabled ...

Local Alarm

☐ Local Alarm

This alarm will only be seen on this VIGIL Server and not be relayed to other VIGIL products.

Cameras | Audio Channels

☐ Cam1
☐ Cam2
☐ Cam
☐ Cam4
☐ Cam5
☐ Cam6
☐ Cam
☐ Cam8
☐ Cam9
☐ Cam10
☐ Cam11
☐ Cam12
☐ Cam13
☐ Cam14
☐ Cam15
☐ Cam16
☐ Cam17
☐ Cam18

Auxiliary Devices

AUX Device Settings

Remote Client Retry Settings

Connection Attempts: 1   Retry Delay: 60 Seconds

Figure 10-1: Settings - Relays / Alarms Tab

If the user needs to edit DIO device settings, click the **AUX Device Settings** at the bottom-left of the windowto 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.

10.1 Input

10.1.1 Input Number

Select the Input number from the 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*.

10.1.2 Settings Tab

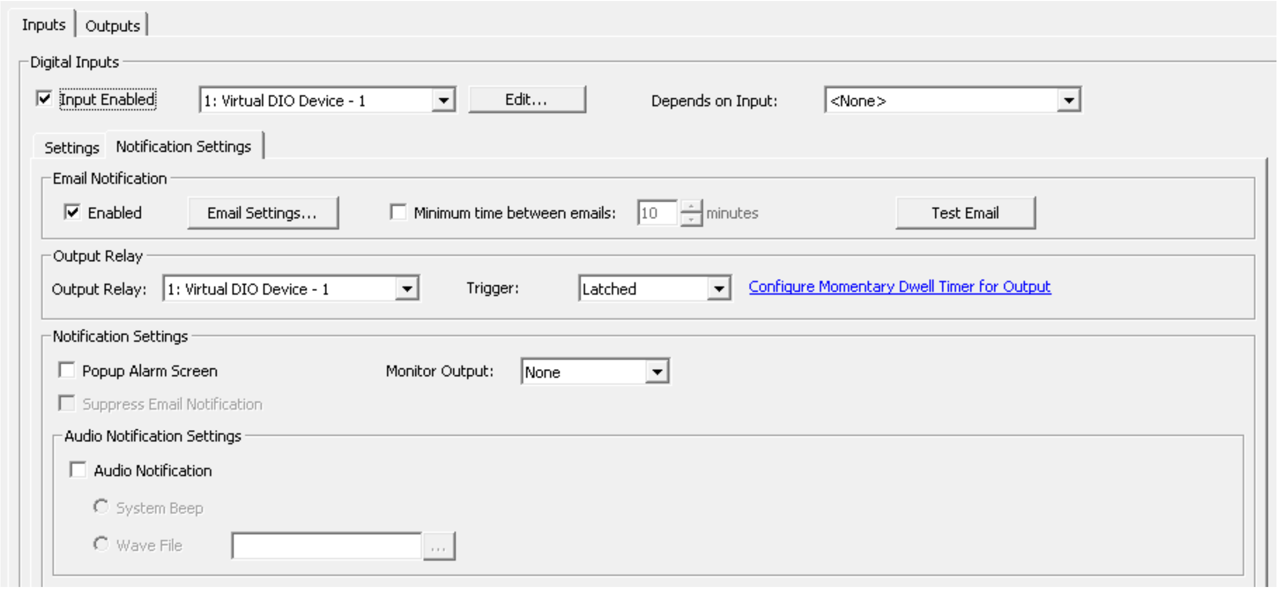
Configure the settings for the selected input. A *Camera* or *Audio Channel* must be selected for the *Digital Input* to remain enabled.

Dwell Timer	The number of seconds the *Digital Input* remains active after a *Trigger* occurs.
Normal Open / Closed	Set the normal state for the *Digital Input*. When the *Digital Input* changes state, the alarm will be triggered.
Auto Acknow-ledge	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 29
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*.

10.2 Notification Settings Tab

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



Inputs | Outputs

Digital Inputs

☑ Input Enabled   1: Virtual DIO Device - 1   Edit...   Depends on Input: <None>

Settings | Notification Settings

Email Notification

☑ Enabled   Email Settings...   □ Minimum time between emails: 10 minutes   Test Email

Output Relay

Output Relay: 1: Virtual DIO Device - 1   Trigger: Latched   Configure Momentary Dwell Timer for Output

Notification Settings

□ Popup Alarm Screen   Monitor Output: None

□ Suppress Email Notification

Audio Notification Settings

□ Audio Notification

○ System Beep

○ Wave File   ...

Figure 10-2: Settings - Relays / Alarms Tab - Notification Settings Tab

10.2.1 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.

10.2.2 Output Relay

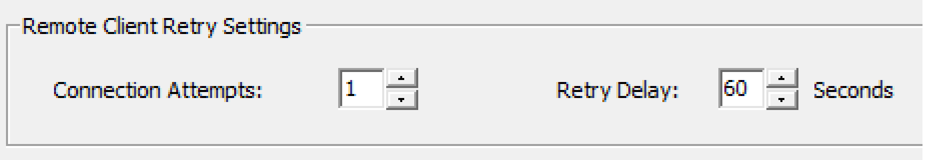
Select the Output Relay to trigger when the *Digital Input Alarm* is triggered. The *Output Relay* can be set to *Latched* or *Momentary*.

10.2.3 Notification Settings

Popup Alarm Screen	When a *Digital Input* alarm is triggered, opens an Alarm window on connected VIGIL Clients.
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.

10.3 Remote Client Retry Settings


Remote Client Retry Settings

Connection Attempts: 1

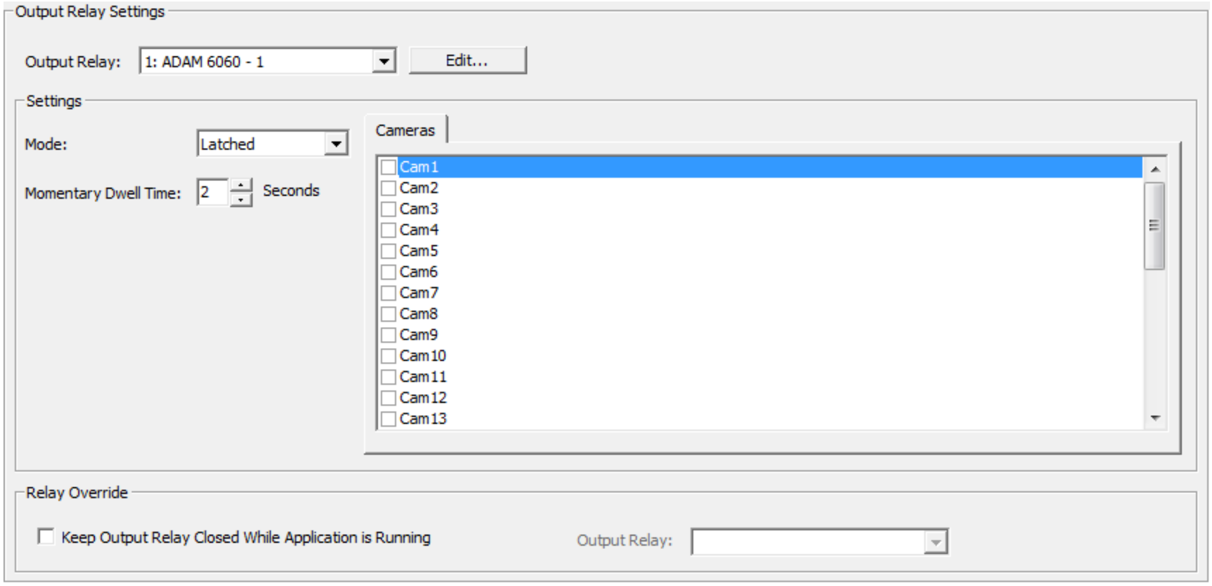
Retry Delay: 60 Seconds

Figure 10-3: 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.

10.4 Output Relay Settings

Select Outputs from the top of the *Relays / Alarms* tab page.


Output Relay Settings

Output Relay: 1: ADAM 6060 - 1

Settings

Mode: Latched

Momentary Dwell Time: 2 Seconds

□ Cam1
□ Cam2
□ Cam3
□ Cam4
□ Cam5
□ Cam6
□ Cam7
□ Cam8
□ Cam9
□ Cam10
□ Cam11
□ Cam12
□ Cam13

Relay Override

□ Keep Output Relay Closed While Application is Running

Output Relay:

Figure 10-4: Settings - Relays / Alarms Settings - Output Relay Settings

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

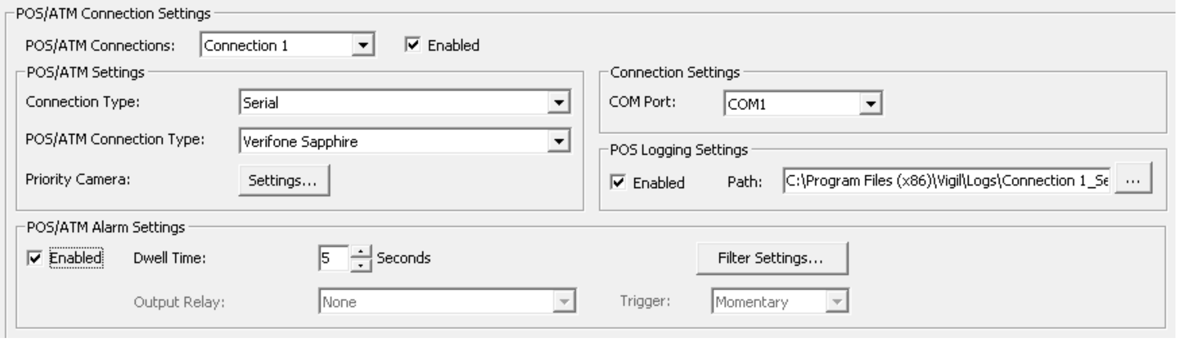
Configure *Mode* and *Dwell* time under the *Settings* section and assigning the output to a camera via the *Cameras* list.

10.4.1 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.

11 Advanced Settings - 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*.



POS/ATM Connection Settings

POS/ATM Connections: Connection 1 ☑ Enabled

POS/ATM Settings
Connection Type: Serial
POS/ATM Connection Type: Verifone Sapphire
Priority Camera: Settings...

Connection Settings
COM Port: COM1

POS Logging Settings
☑ Enabled Path: C:\Program Files (x86)\Vigil\Logs\Connection 1_Se ...

POS/ATM Alarm Settings
☑ Enabled Dwell Time: 5 Seconds Filter Settings...
Output Relay: None Trigger: Momentary

Figure 11-1: Settings - Data Tab

11.1 POS/ATM Connection Settings

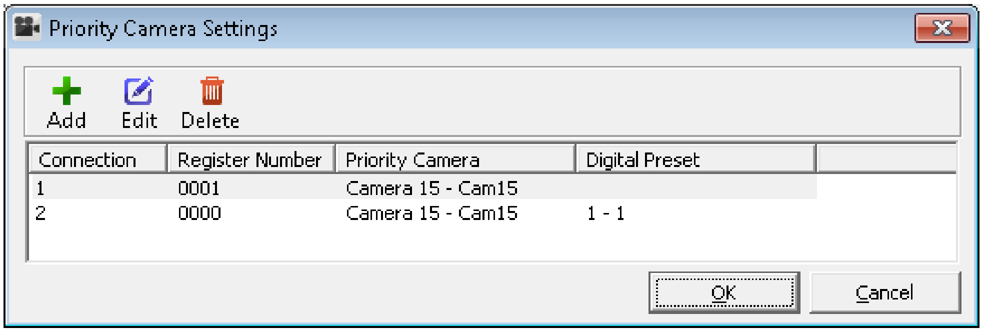
POS/ATM Connections	Select the Connection Number for the POS/ATM Data stream from the Drop-Down Menu.
Enabled	Enable the POS/ATM Connection.

11.1.1 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 *Connection / Register Numbers* can be assigned to a single *Priority Camera*. A camera's *Digital Presets* can also be used as a priority camera.



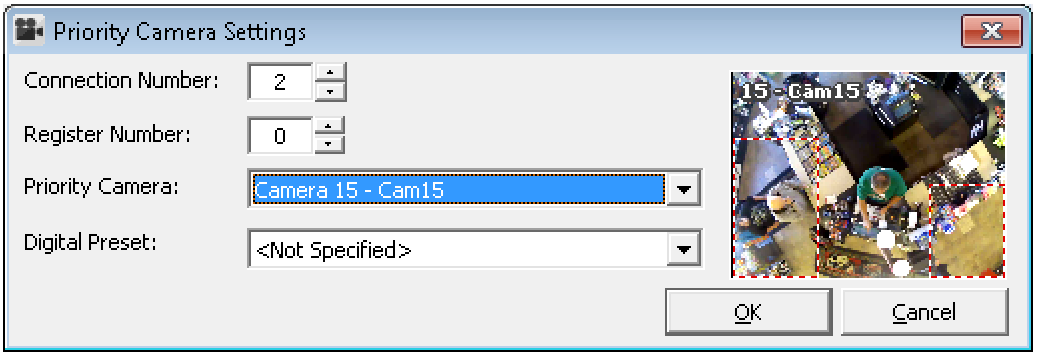
Priority Camera Settings

Connection	Register Number	Priority Camera	Digital Preset
1	0001	Camera 15 - Cam15	
2	0000	Camera 15 - Cam15	1 - 1

Figure 11-2: 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.



Connection Number: 2

Register Number: 0

Priority Camera: Camera 15 - Cam15

Digital Preset: <Not Specified>

Figure 11-3: 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 thepriority 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 selected in the *Priority Camera* field has no digital presets configured, this menu will be blank. See "Digital Presets" on page 39 for more information on configuring *Digital PTZ Presets.*

11.1.2 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)*

11.1.3 POS/ATM Alarm Settings

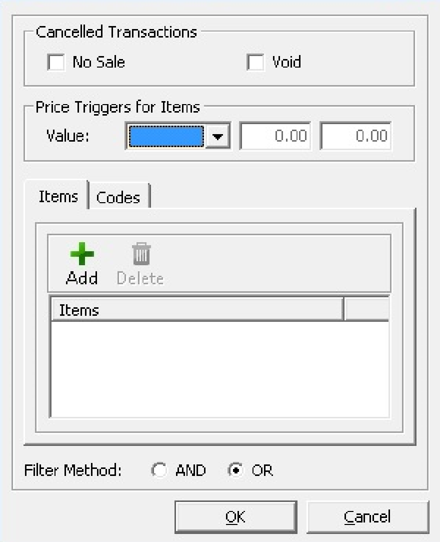
This setting becomes available once *Priority Cameras* are configured.

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.*



Cancelled Transactions

□ No Sale □ Void

Price Triggers for Items

Value: 0.00 0.00

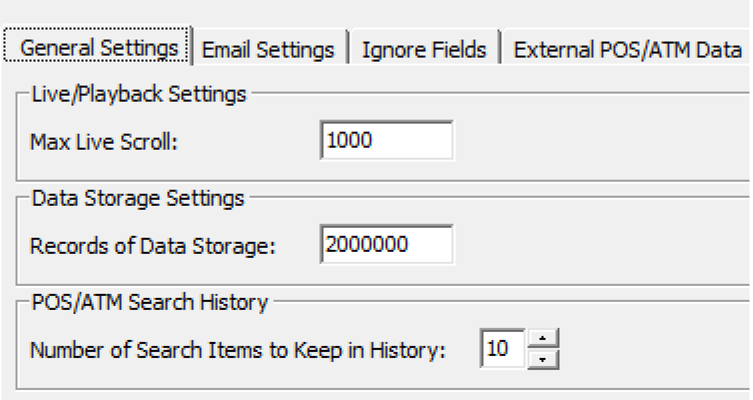
Filter Method: ○ AND ● OR

Figure 11-4: 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.*

11.2 General Settings Tab

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



Live/Playback Settings

Max Live Scroll: 1000

Data Storage Settings

Records of Data Storage: 2000000

POS/ATM Search History

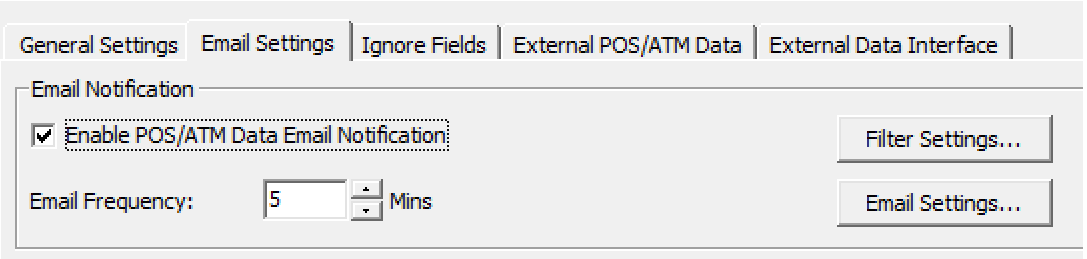
Number of Search Items to Keep in History: 10

Figure 11-5: 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.

11.3 Email Settings Tab

The *Email Settings* tab allows users to configure email notifications containing filtered POS/ATM Data.



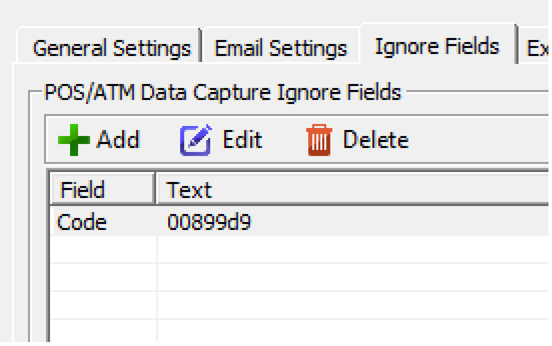
☑ Enable POS/ATM Data Email Notification

Email Frequency: 5 Mins

Figure 11-6: 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.

11.4 Ignore Fields Tab

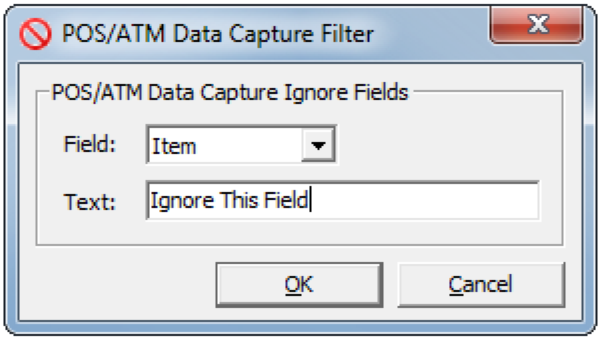


Field	Text
Code	00899d9

Figure 11-7: 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.

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



POS/ATM Data Capture Filter

POS/ATM Data Capture Ignore Fields

Field: Item

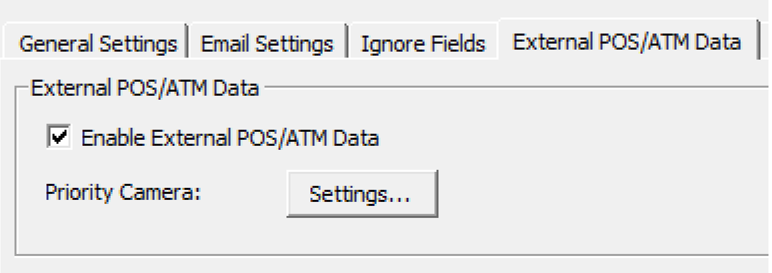
Text: Ignore This Field

Figure 11-8:POS/ATM Data Capture Filter Configuration

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

11.5 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.



External POS/ATM Data

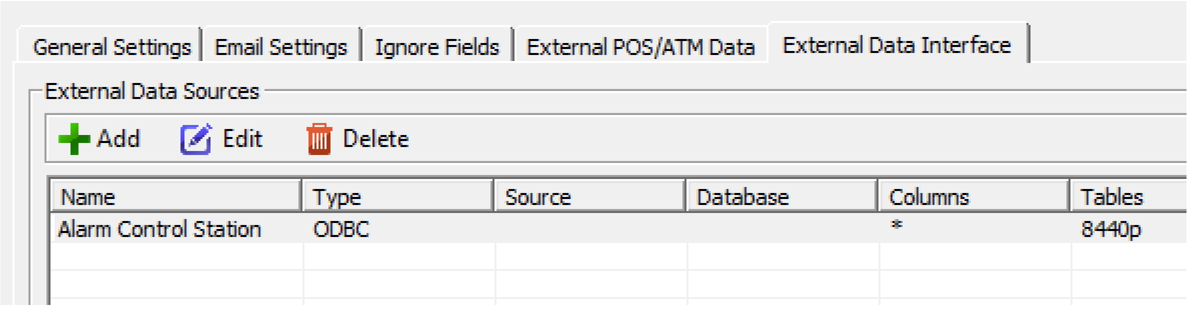
☑ Enable External POS/ATM Data

Priority Camera:

Figure 11-9: Settings - Data Tab - External POS/ATM Data Tab

11.6 External Data Interface Tab

VIGIL Server has the ability to connect and read data from third party databases, such as access control panels, coin counters, GPS data, etc. The data source must be network accessible by the VIGIL Server. The *External* data is available when searching video footage. Data can be retrieved from a configured data source and viewed alongside video data.



External Data Sources

Name	Type	Source	Database	Columns	Tables
Alarm Control Station	ODBC			*	8440p

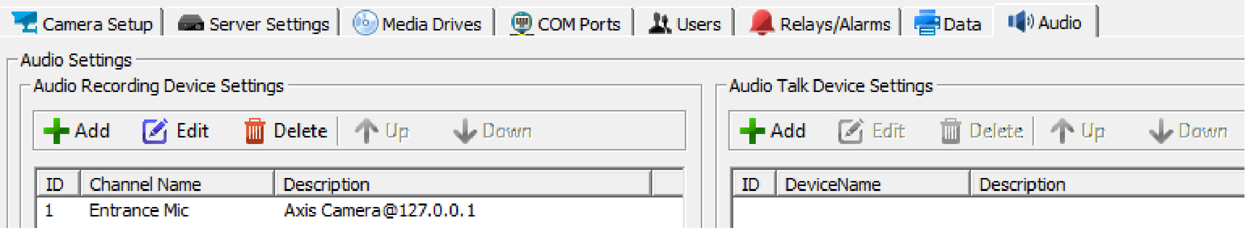
Figure 11-10: Settings - Data Tab - External Data Interface Tab

Click *Add* or select an existing data source and press *Edit*. Different connection information is required depending on the *Data Source Type* selected. Common information is listed here.

Name	The name the data source will be listed as.
Data Source Type	Select the type of data source from the drop-down list. Supported *Data Source* types are: ODBC, SQL Server or Microsoft Access. If the SQL Server type is selected, the default port of 1433 will be used.
Table	The table within the *Data Source* from which data will be retrieved.
Timestamp Column	In order to display video synchronized with the *External Data,* a timestamp must be used. Select the column within the table that contains the most accurate timestamp information.
Priority Camera	If a *Priority Camera* is selected, then that camera will be used when no other camera is currently selected in the playback window.
Column Selection	The columns entered into the *Column Selection* area will be displayed in the search results in the search window. Each *Column Selection* has a *Columns* area indicating the column as it is in the data-base and a *Name,* which will be displayed at the top of the column in the search results. To remove a column, select the *Columns* and press delete or backspace.

12 Advanced Settings - 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.



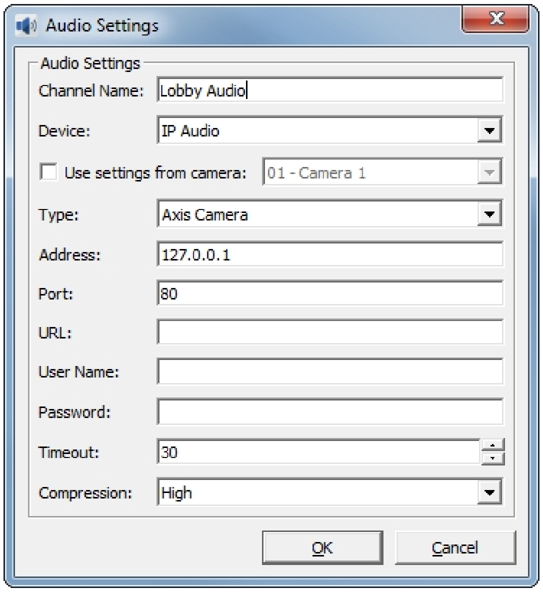
ID	Channel Name	Description
1	Entrance Mic	Axis Camera@127.0.0.1

ID	DeviceName	Description

Figure 12-1: Settings - Audio Tab

12.1 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.



Channel Name: Lobby Audio

Device: IP Audio

☐ Use settings from camera: 01 - Camera 1

Type: Axis Camera

Address: 127.0.0.1

Port: 80

URL:

User Name:

Password:

Timeout: 30

Compression: High

Figure 12-2: Settings - Audio Tab - Audio Settings Window.

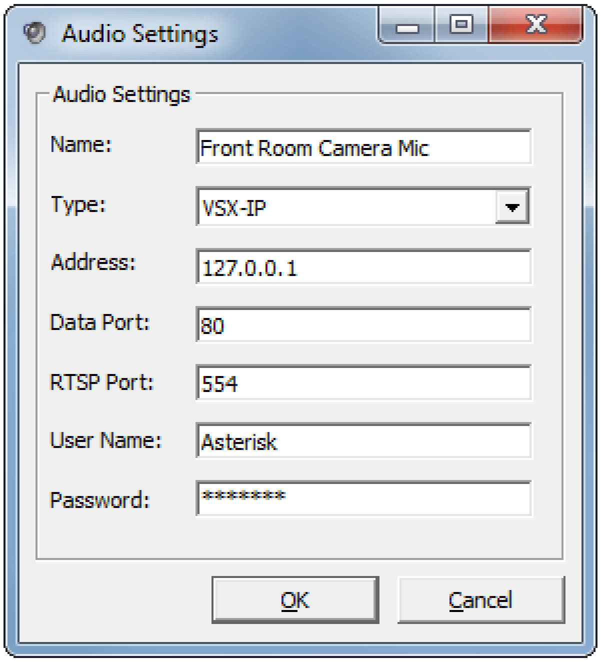
Note: Capture card inputs and VIGIL Server audio inputs only require configuration of the *Channel Name* and *Compression*. The form will change to reflect this when either of these types is selected in the *Device* drop-down menu.

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.

12.2 Audio Talk Device Settings

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



Audio Settings

Name: Front Room Camera Mic

Type: VSX-IP

Address: 127.0.0.1

Data Port: 80

RTSP Port: 554

User Name: Asterisk

Password: ********

Figure 12-3: Settings - Audio Tab - audio Talk Device Settings Window

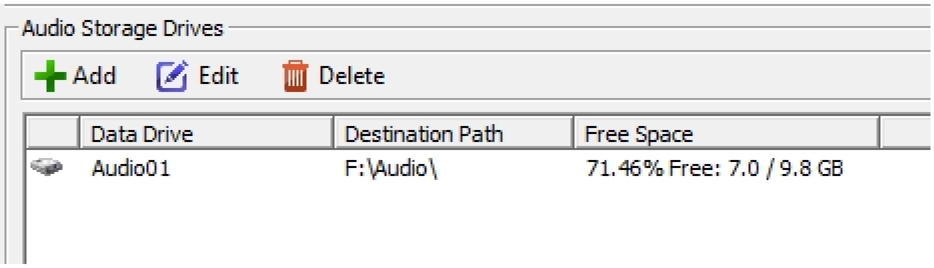
Name	Enter a name for the Audio Talk Device. This can be used to describe the location of the Audio Talk Device.
Type	Select the type of Audio Talk Device. This can be an Audio Talk capable IP Camera or IP Audio Device.
Address	The IP address of the Audio Talk Device.
Data Port	The Data Port used on 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.

12.3 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.

12.4 Audio Storage Drives

Create and configure *Audio Storage Drives*.



Data Drive	Destination Path	Free Space
Audio01	F:\Audio\	71.46% Free: 7.0 / 9.8 GB

Figure 12-4: 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).*

12.5 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.

12.6 Other Settings - Audio Recorder Controls

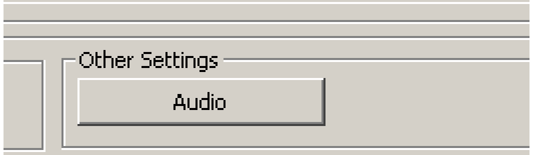
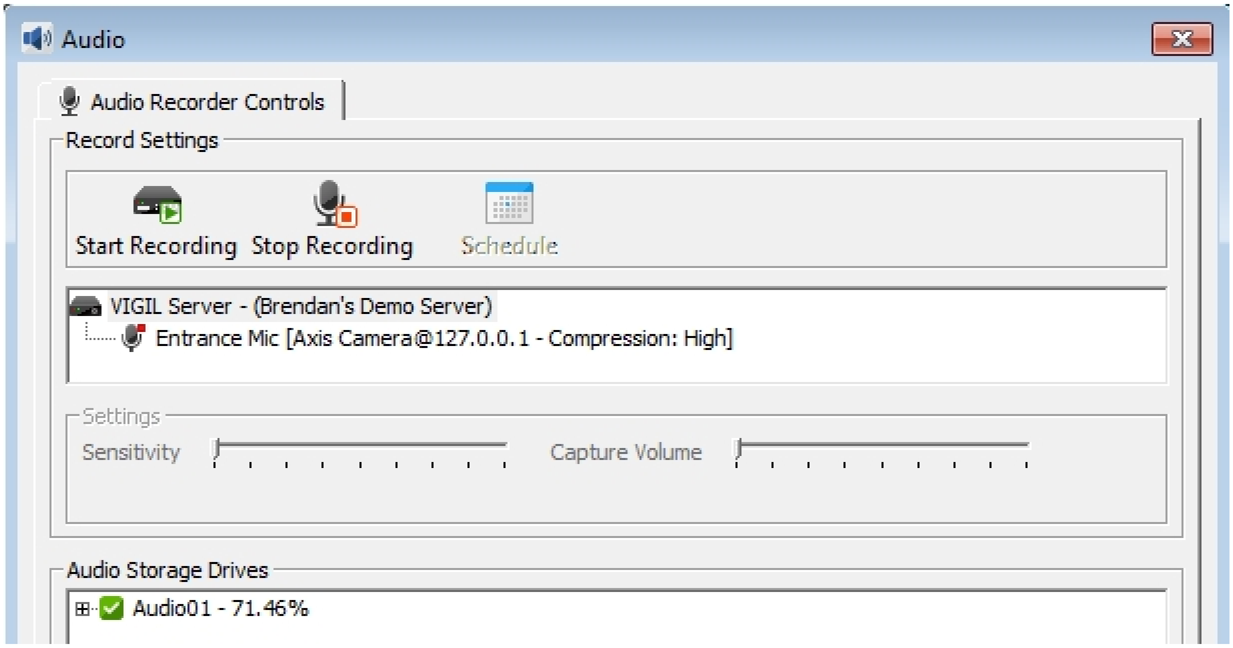


Figure 12-5: Audio Settings - Other Settings - Audio Recorder Controls

Click the **Audio** button under the *Other Settings* portion of the *Audio Settings* form to open the *Audio Recorder Controls*.

The *Audio Recorder Controls* window is used to view audio channel status and to manually stop or start the recording of specific audio channels.



VIGIL Server - (Brendan's Demo Server)
Entrance Mic [Axis Camera@127.0.0.1 - Compression: High]

Audio01 - 71.46%

Figure 12-6: Audio Recorder Controls Tab

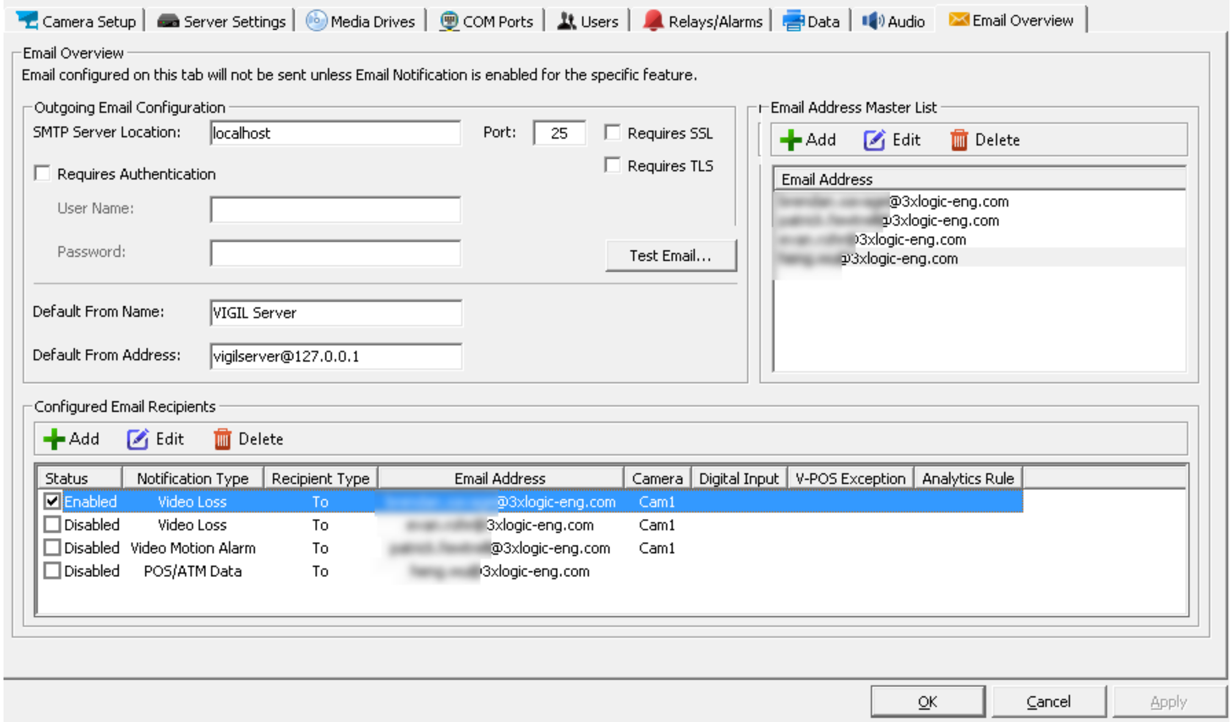
🎙🟢	The channel is currently recording audio.
🎙	The channel is set to record, but there is no audio detected.
🎙🟥	Audio recording has been stopped on this channel.
Start Recording	Starts recording audio on the selected channel.
Stop Recording	Stops recording audio on the selected channel.
Schedule	Opens the schedule calendar where a recording schedule can be configured.
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.*
Capture Volume	Use the slide bar to adjust the live volume of the selected audio channel. This setting is only available on VIGIL Server systems using a capture card.
Drive Information	The drive information section gives the current status of the VIGIL Server audio storage drives: ✓ Configured drive ✅ Currently recording on this drive ⚠ Drive warning ☒ Drive error, contact your system administrator

13 Advanced Settings - Email Overview Tab

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

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



Email Overview

Email configured on this tab will not be sent unless Email Notification is enabled for the specific feature.

Outgoing Email Configuration

SMTP Server Location: localhost

Port: 25

☐ Requires SSL

☐ Requires TLS

☐ Requires Authentication

User Name:

Password:

Test Email...

Default From Name: VIGIL Server

Default From Address: vigilserver@127.0.0.1

Email Address Master List

Add Edit Delete

Email Address
[redacted]@3xlogic-eng.com
[redacted]@3xlogic-eng.com
[redacted]3xlogic-eng.com
[redacted]@3xlogic-eng.com

Configured Email Recipients

Add Edit Delete

Status	Notification Type	Recipient Type	Email Address	Camera	Digital Input	V-POS Exception	Analytics Rule
☑ Enabled	Video Loss	To	[redacted]@3xlogic-eng.com	Cam1			
☐ Disabled	Video Loss	To	[redacted]3xlogic-eng.com	Cam1			
☐ Disabled	Video Motion Alarm	To	[redacted]@3xlogic-eng.com	Cam1			
☐ Disabled	POS/ATM Data	To	[redacted]3xlogic-eng.com				

Figure 13-1:VIGIL Server Settings - Email Overview Tab

E-Mail Configuration Setting	Definition
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 configured 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.

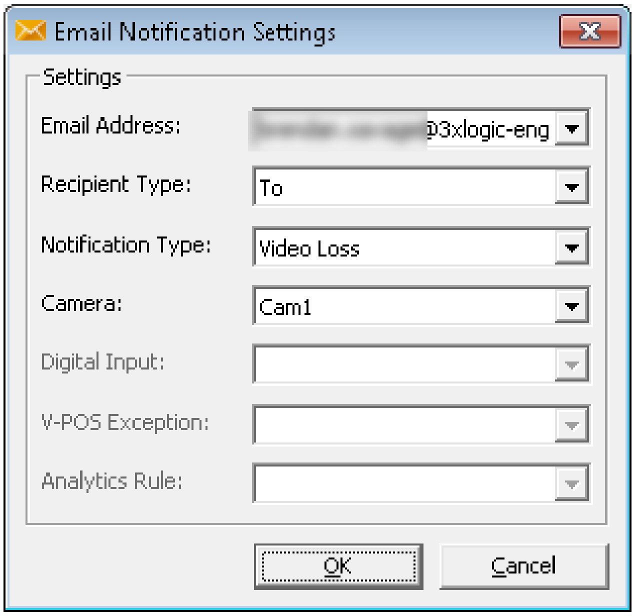
E-Mail recipients can also be configured in this list, though the recipient address must exist in the Email Address Masterlist before being added as a recipient.

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.



Email Notification Settings

Settings

Email Address: [redacted]@3xlogic-eng

Recipient Type: To

Notification Type: Video Loss

Camera: Cam1

Digital Input:

V-POS Exception:

Analytics Rule:

Figure 13-2: 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.* 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.
Analytics Rule	IF the Notification Type is set to Video analytics, select the configured rule here.

Click *OK* to save the new recipient.

14 Advanced Settings - 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.

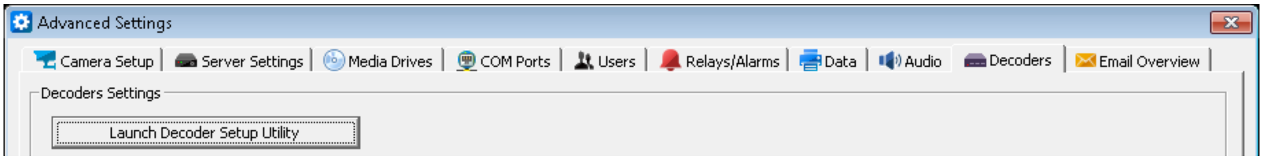
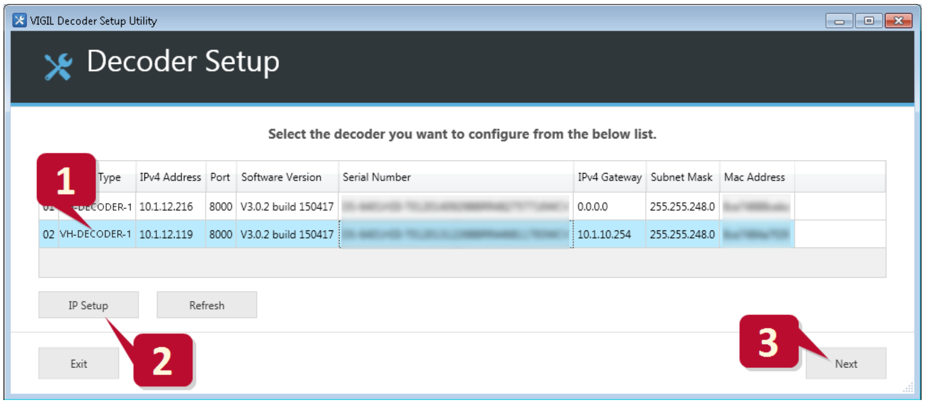


Figure 14-1:VIGIL Server Settings - Decoders Tab

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

14.1 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.



Select the decoder you want to configure from the below list.

	Type	IPv4 Address	Port	Software Version	Serial Number	IPv4 Gateway	Subnet Mask	Mac Address
01	-DECODER-1	10.1.12.216	8000	V3.0.2 build 150417	[redacted]	0.0.0.0	255.255.248.0	[redacted]
02	VH-DECODER-1	10.1.12.119	8000	V3.0.2 build 150417	[redacted]	10.1.10.254	255.255.248.0	[redacted]

Figure 14-2: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.

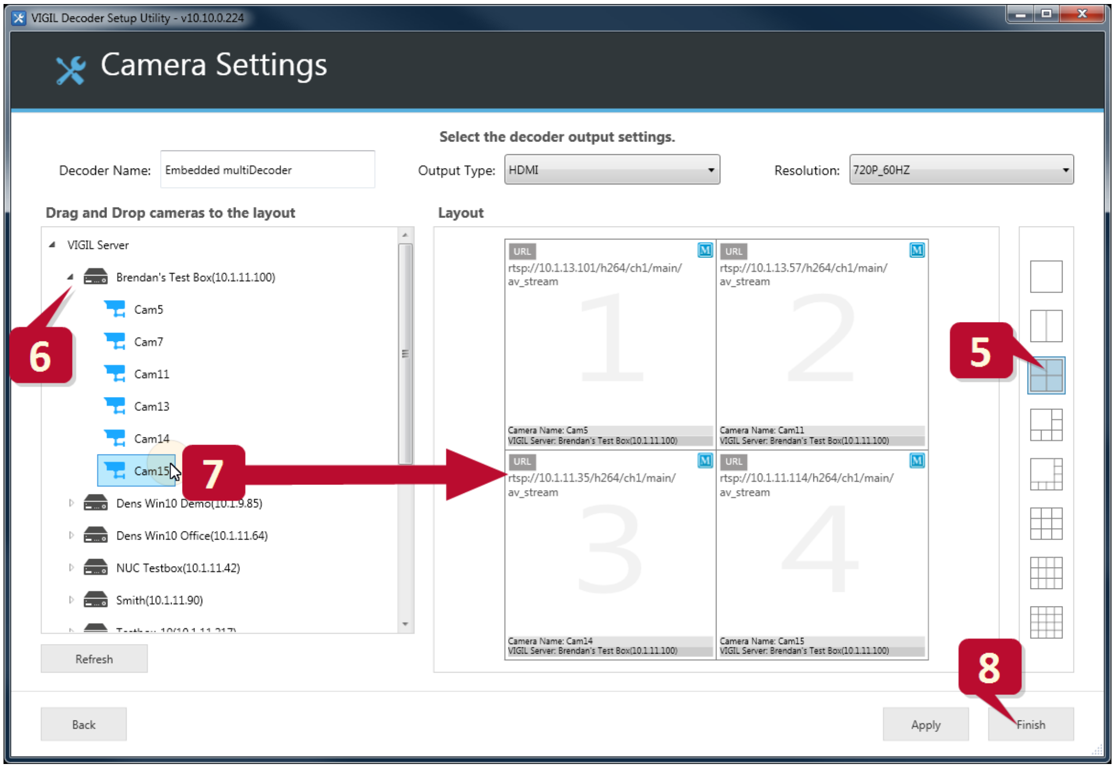
From the Camera Settings window, a user may configure decoder name and output settings and well as monitor layout settings for the camera streams that will be decoded.

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.



VIGIL Decoder Setup Utility - v10.10.0.224

Camera Settings

Select the decoder output settings.

Decoder Name: Embedded multiDecoder

Output Type: HDMI

Resolution: 720P_60HZ

Drag and Drop cameras to the layout

- VIGIL Server
  - Brendan's Test Box(10.1.11.100)
    - Cam5
    - Cam7
    - Cam11
    - Cam13
    - Cam14
    - Cam15
  - Dens Win10 Demo(10.1.9.85)
  - Dens Win10 Office(10.1.11.64)
  - NUC Testbox(10.1.11.42)
  - Smith(10.1.11.90)

Layout

1: rtsp://10.1.13.101/h264/ch1/main/av_stream
Camera Name: Cam5
VIGIL Server: Brendan's Test Box(10.1.11.100)

2: rtsp://10.1.13.57/h264/ch1/main/av_stream
Camera Name: Cam11
VIGIL Server: Brendan's Test Box(10.1.11.100)

3: rtsp://10.1.11.35/h264/ch1/main/av_stream
Camera Name: Cam14
VIGIL Server: Brendan's Test Box(10.1.11.100)

4: rtsp://10.1.11.114/h264/ch1/main/av_stream
Camera Name: Cam15
VIGIL Server: Brendan's Test Box(10.1.11.100)

Figure 14-3: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.*

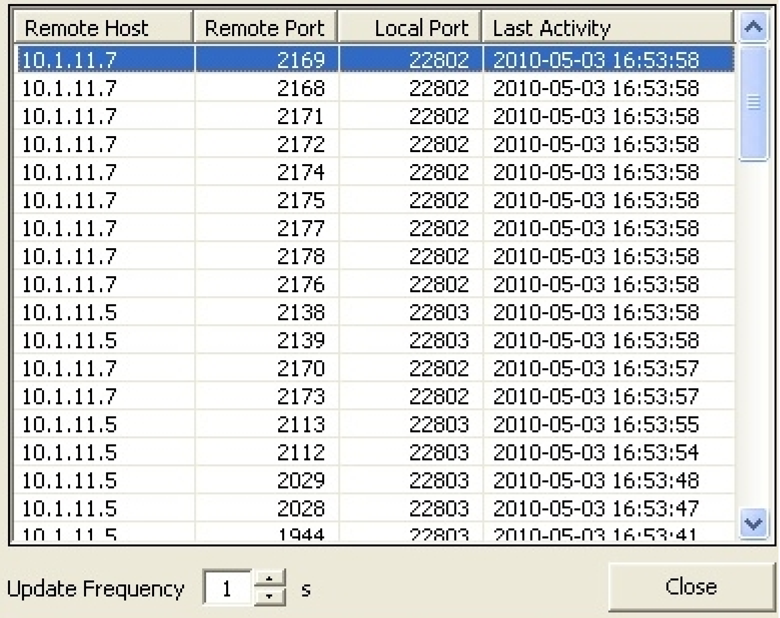
15 Report Tools

Client Connections, *Audit Log Analyzer* and *Network Log Analyzer* can all be accessed from the system tray icon right-click menu. These tools can be used to view important connection and usage information about the VIGIL Server. For details on these reporting tools, see the below sections.

15.1 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 *Tools* icon drop-down menu in the main VIGIL Server window. You can also double-click the *Client Connections* status bar.

The table provides the following information: the client’s remote host name or IP address, 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
10.1.11.7	2169	22802	2010-05-03 16:53:58
10.1.11.7	2168	22802	2010-05-03 16:53:58
10.1.11.7	2171	22802	2010-05-03 16:53:58
10.1.11.7	2172	22802	2010-05-03 16:53:58
10.1.11.7	2174	22802	2010-05-03 16:53:58
10.1.11.7	2175	22802	2010-05-03 16:53:58
10.1.11.7	2177	22802	2010-05-03 16:53:58
10.1.11.7	2178	22802	2010-05-03 16:53:58
10.1.11.7	2176	22802	2010-05-03 16:53:58
10.1.11.5	2138	22803	2010-05-03 16:53:58
10.1.11.5	2139	22803	2010-05-03 16:53:58
10.1.11.7	2170	22802	2010-05-03 16:53:57
10.1.11.7	2173	22802	2010-05-03 16:53:57
10.1.11.5	2113	22803	2010-05-03 16:53:55
10.1.11.5	2112	22803	2010-05-03 16:53:54
10.1.11.5	2029	22803	2010-05-03 16:53:48
10.1.11.5	2028	22803	2010-05-03 16:53:47
10.1.11.5	1944	22803	2010-05-03 16:53:41

Update Frequency: 1 s

Figure 15-1: Client Connection Report

Update Frequency	Adjusts the update frequency of the table every set amount of seconds entered in the corresponding box.

15.2 Network Log Analyzer

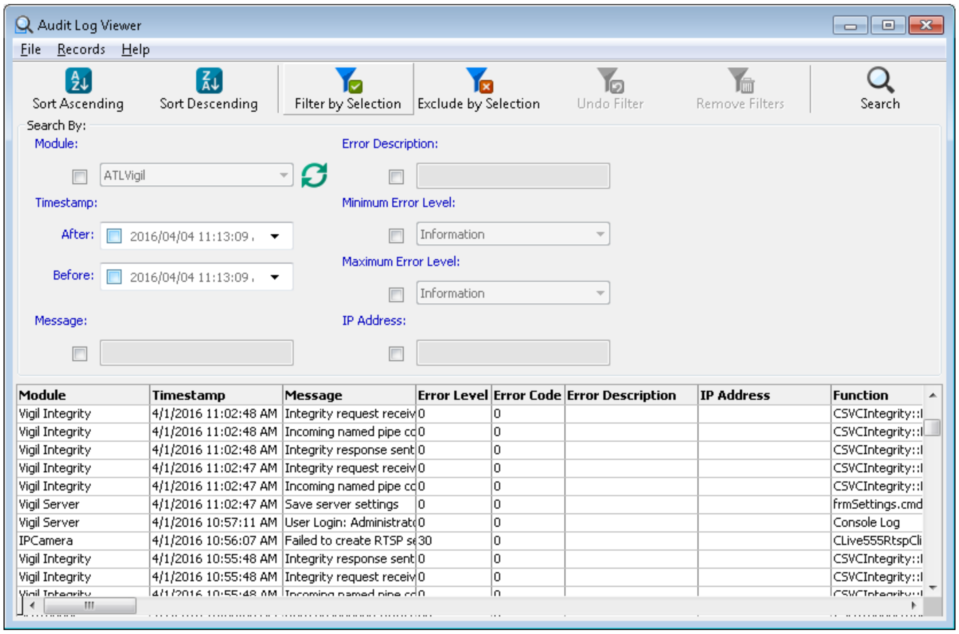
The *Network Log Analyzer* provides a simple way to check for network activity of VIGIL software. It will log IP addresses and VIGIL user names of all connections made. To open the *Network Log Analyzer*, select *Tools* from the main menu bar and select *Network Log Analyzer.*

15.3 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*, select *Tools* from the main menu bar and select *Audit Log Analyzer*. The Audit Log Viewer window will deploy.

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.



Search By:

Module: □ ATLVigil

Error Description: □

Timestamp:

After: □ 2016/04/04 11:13:09

Before: □ 2016/04/04 11:13:09

Minimum Error Level: □ Information

Maximum Error Level: □ Information

Message: □

IP Address: □

Module	Timestamp	Message	Error Level	Error Code	Error Description	IP Address	Function
Vigil Integrity	4/1/2016 11:02:48 AM	Integrity request receiv	0	0			CSVCIntegrity::I
Vigil Integrity	4/1/2016 11:02:48 AM	Incoming named pipe cc	0	0			CSVCIntegrity::I
Vigil Integrity	4/1/2016 11:02:48 AM	Integrity response sent	0	0			CSVCIntegrity::I
Vigil Integrity	4/1/2016 11:02:47 AM	Integrity request receiv	0	0			CSVCIntegrity::I
Vigil Integrity	4/1/2016 11:02:47 AM	Incoming named pipe cc	0	0			CSVCIntegrity::I
Vigil Server	4/1/2016 11:02:47 AM	Save server settings	0	0			frmSettings.cmd
Vigil Server	4/1/2016 10:57:11 AM	User Login: Administrat	0	0			Console Log
IPCamera	4/1/2016 10:56:07 AM	Failed to create RTSP se	30	0			CLive555RtspCli
Vigil Integrity	4/1/2016 10:55:48 AM	Integrity response sent	0	0			CSVCIntegrity::I
Vigil Integrity	4/1/2016 10:55:48 AM	Integrity request receiv	0	0			CSVCIntegrity::I
Vigil Integrity	4/1/2016 10:55:48 AM	Incoming named pipe cc	0	0			CSVCIntegrity::I

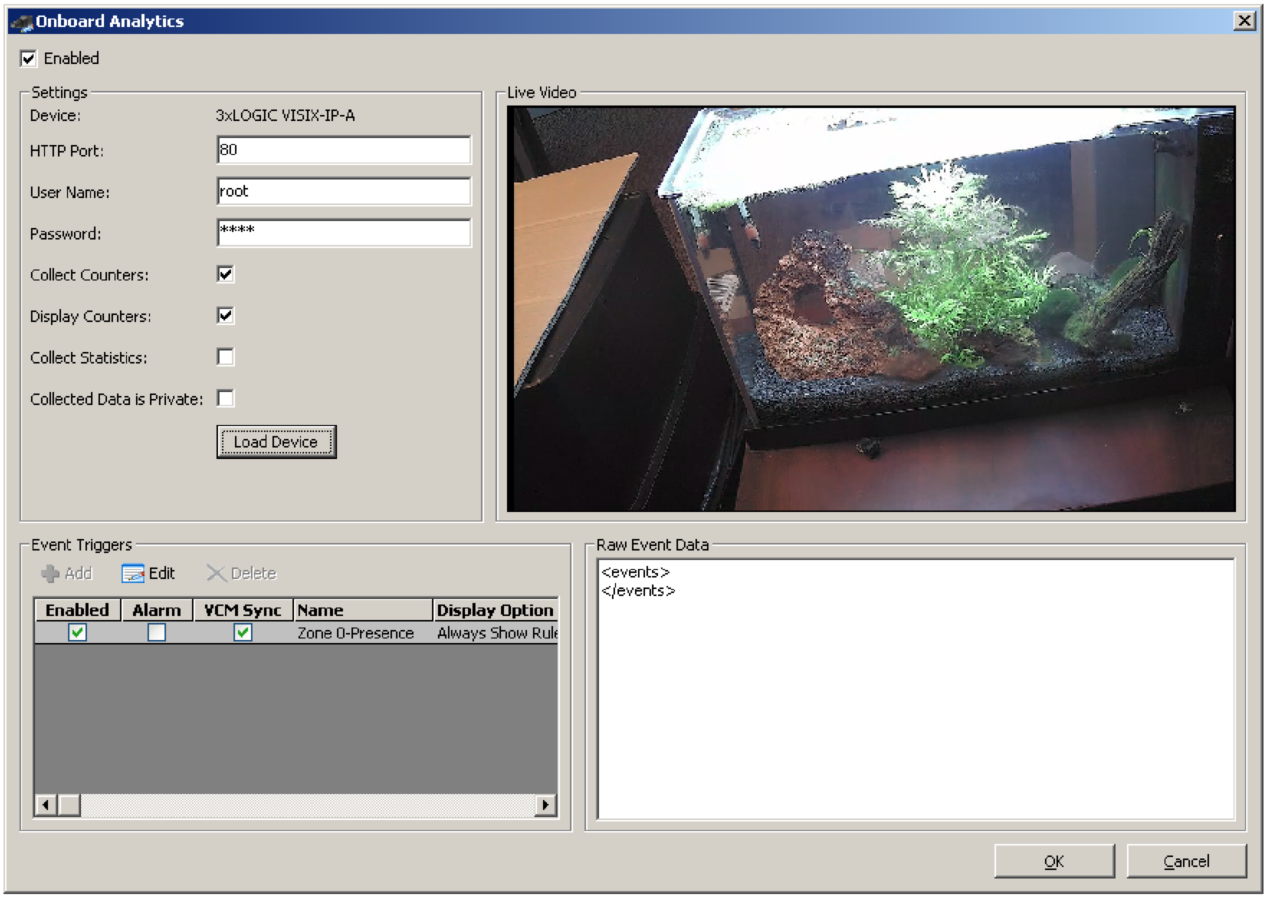
Figure 15-2:VIGIL Server Audit Log Analyzer

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	Undo the latest filter.
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.

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 *Network Camera Settings* form. Click the **On-Board Analytics** button to launch the *On-Board Analytics* utility.



☑ Enabled

Device: 3xLOGIC VISIX-IP-A

HTTP Port: 80

User Name: root

Password: ****

Collect Counters: ☑

Display Counters: ☑

Collect Statistics: □

Collected Data is Private: □

Enabled	Alarm	VCM Sync	Name	Display Option
☑	□	☑	Zone 0-Presence	Always Show Rule

```
<events>
</events>
```

Figure 15-3: 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.

Component	Description
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.
HTTP Port	One of two ports used to connect to the camera's analytics data.
Username	Username required to sign in to the camera. This will be auto-populated by VIGIL Server.
Password	Password required to sign in to the camera. This 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. .
Load Device	Click this button after the other device / camera settings have been correctly input. The

	device / camera’s feed will be displayed in the Live Video window to the right, if available.
Raw Event Data	Contains a raw dump of analytics event data coming from the camera.
Event Triggers	
Edit	Edit the *Rule Name* and te 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**.

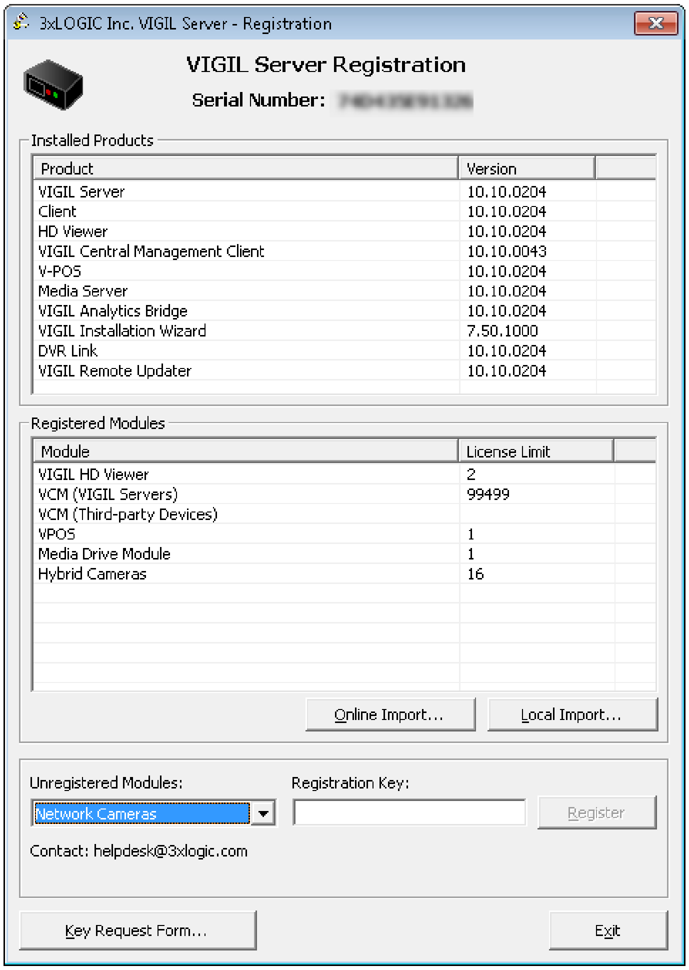
Once a rule is added to VIGIL Server, VCA analytics data generated by the rule will be inserted into the VIGIL database. VIGIL Server's VA rule settings can be edited from the *Camera Setup > Video Analytics tab*. See "Advanced Settings - Video Analytics Tab" on page 44 for more information.

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 VIGIL.*

The VIGIL Registration utility will launch.



3xLOGIC Inc. VIGIL Server - Registration

VIGIL Server Registration

Serial Number: [redacted]

Installed Products

Product	Version
VIGIL Server	10.10.0204
Client	10.10.0204
HD Viewer	10.10.0204
VIGIL Central Management Client	10.10.0043
V-POS	10.10.0204
Media Server	10.10.0204
VIGIL Analytics Bridge	10.10.0204
VIGIL Installation Wizard	7.50.1000
DVR Link	10.10.0204
VIGIL Remote Updater	10.10.0204

Registered Modules

Module	License Limit
VIGIL HD Viewer	2
VCM (VIGIL Servers)	99499
VCM (Third-party Devices)	
VPOS	1
Media Drive Module	1
Hybrid Cameras	16

Unregistered Modules: Network Cameras

Registration Key:

Contact: helpdesk@3xlogic.com

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 **Onine 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.

17 Language Switcher

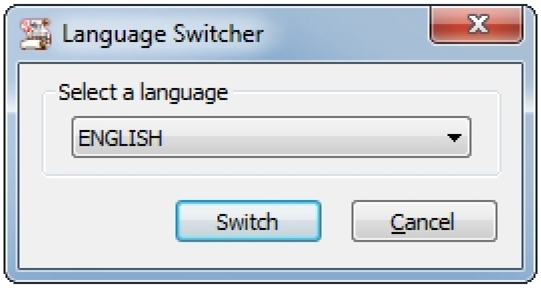


Figure 17-1:VIGIL Language Switcher

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.

18 VIGIL Server System Database Utility

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

Warning: The VIGIL Server System Database Utility contains features that may cause a system failure or other undesired effects.

If the VIGIL Server is experiencing issues, please contact your system administrator or 3xLOGIC technical support. Please See "Contact Information" on page 122

You will have to login to the utility before being able to modify any settings; a VIGIL administrator account must be used.

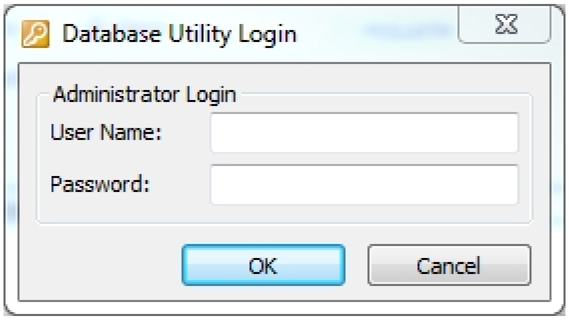
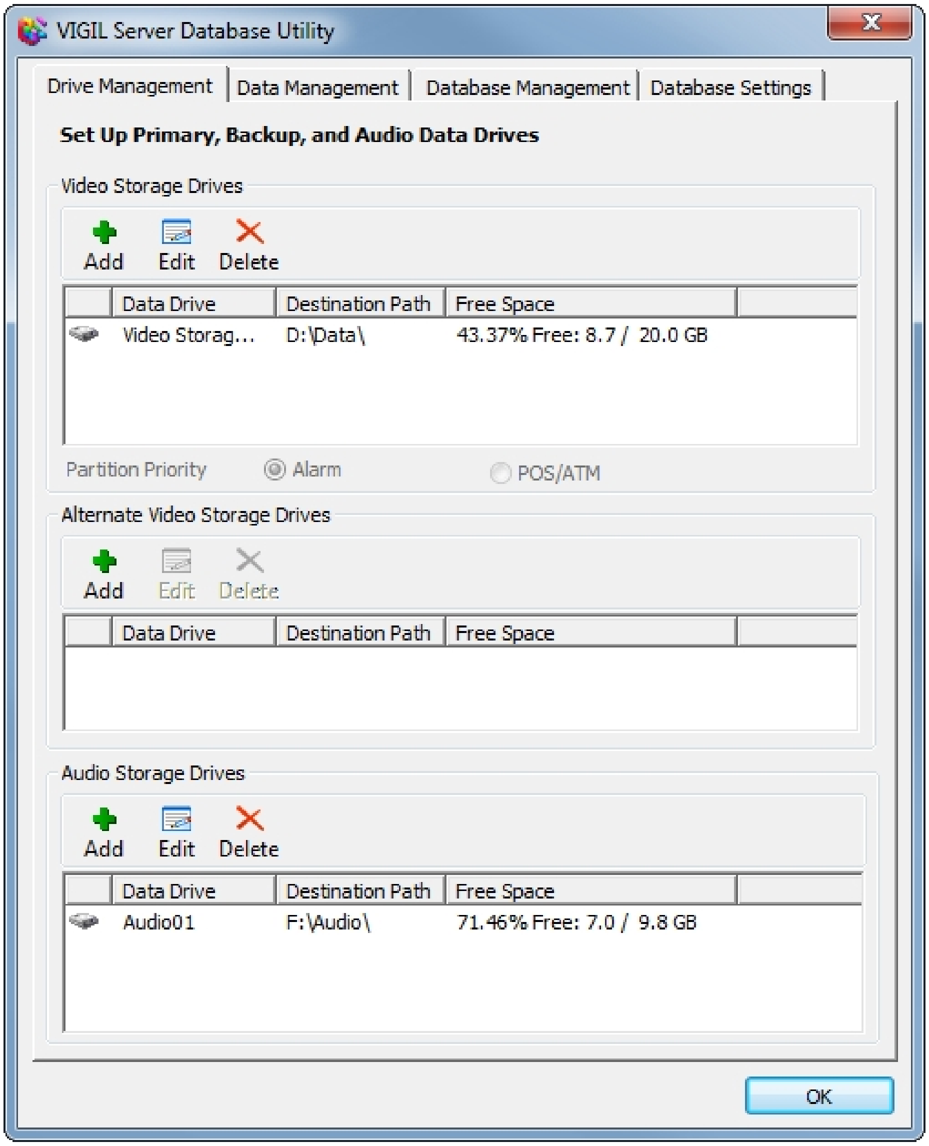


Figure 18-1: Database Utility Login Window

18.1 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.



Set Up Primary, Backup, and Audio Data Drives

Video Storage Drives

	Data Drive	Destination Path	Free Space
	Video Storag...	D:\Data\	43.37% Free: 8.7 / 20.0 GB

Partition Priority ● Alarm ○ POS/ATM

Alternate Video Storage Drives

	Data Drive	Destination Path	Free Space

Audio Storage Drives

	Data Drive	Destination Path	Free Space
	Audio01	F:\Audio\	71.46% Free: 7.0 / 9.8 GB

Figure 18-2: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.

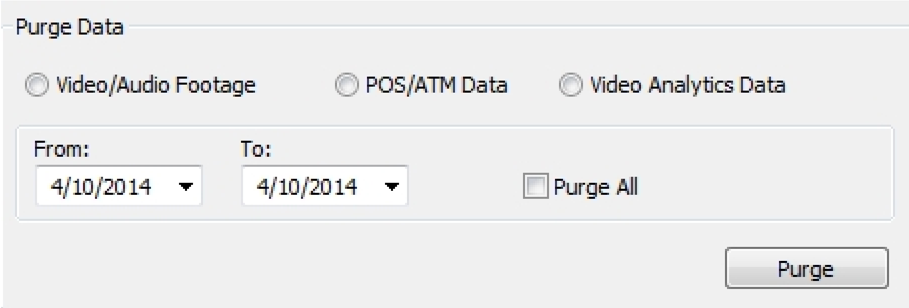
Audio Storage Drives – Audio Storage Drives are the drives where audio data is stored.

18.2 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, select the type of data you wish to purge; *Video / Audio Footage, POS Data or Video Analytics Data*. Specify a date range in the *From* and *To* boxes or choose *Purge All*, click the *Purge* button to purge the *Selected Data*.



Purge Data

○ Video/Audio Footage ○ POS/ATM Data ○ Video Analytics Data

From: 4/10/2014 To: 4/10/2014 □ Purge All

Figure 18-3:VIGIL Server Database Utility - Data Management Tab - Purge Data Options

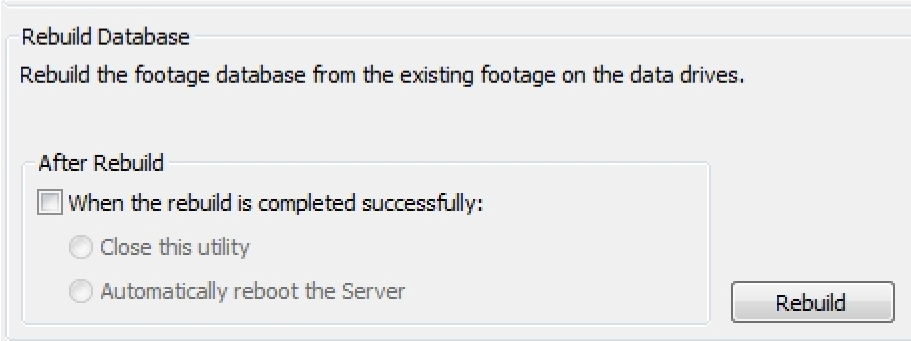
Note:VIGIL Server is designed to manage the purging of data; it will delete the oldest hour of video footage or the oldest POS / Video Analytics Data automatically before the data drives become full. Under normal operating conditions, there is no need to manually purge Data.

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. Click the *Rebuild* button, select the drive(s) to rebuild and 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*.



Rebuild Database

Rebuild the footage database from the existing footage on the data drives.

After Rebuild

□ When the rebuild is completed successfully:

○ Close this utility

○ Automatically reboot the Server

Figure 18-4:VIGIL Server 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 Server Health Monitor software Users Guide, or contact 3xLOGIC for more information.

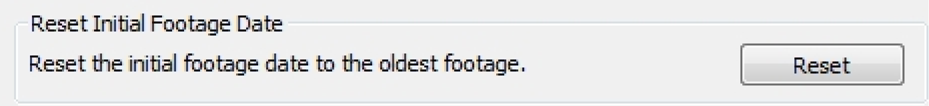

Reset Initial Footage Date
Reset the initial footage date to the oldest footage.
Reset

Figure 18-5:VIGIL Server Database Utility - Data Management Tab - Reset Initial Footage Date

Reset POS/ATM Database

Below the *Reset Initial Footage Date* option, users may also select the Reset POS/ATM Database function. This process will only clear POS/ATM data from the VIGIL POS Database. Any existing POS/ATM data within the standard VIGIL Server database will remain and will be copied over to the VIGIL POS database once it has been cleared and reset. Use this function to attempt to repair the VIGIL POS database if it has fallen into an error state.

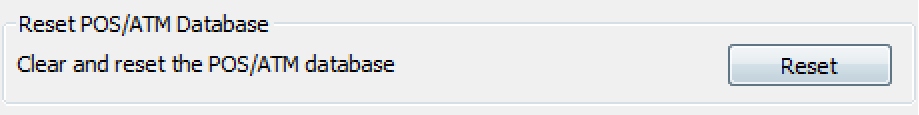
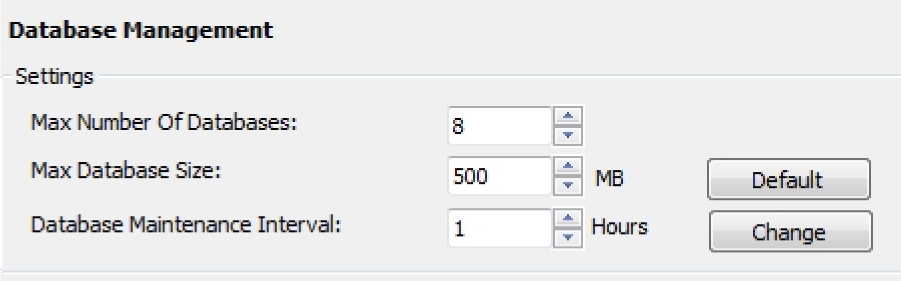


Figure 18-6:VIGIL Server Database Utility - Data Management Tab - Reset POS/ATM Database

18.3 Database Management Tab

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

Settings


Database Management

Settings

Max Number Of Databases: 8

Max Database Size: 500 MB

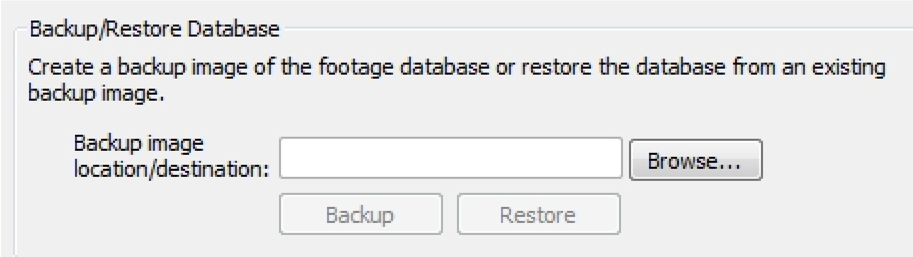
Database Maintenance Interval: 1 Hours

Figure 18-7:VIGIL Server Database Utility - Database Management Settings

Max Number of Databases	Set the maximum amount of databases that will be created.
Max Database Size	Set the maximum size a database can grow to before a new database is created.
Database Maintenance Interval	Set the time interval, in hours, between when database maintenance scripts will be run.
Default	Reset the values to default.
Change	Apply the changes.

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.


Backup/Restore Database

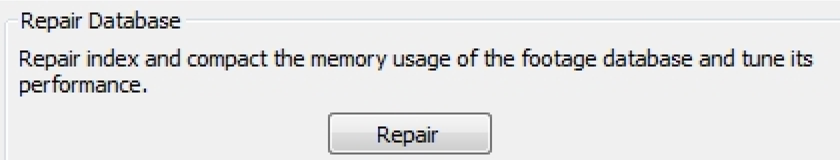
Create a backup image of the footage database or restore the database from an existing backup image.

Backup image location/destination:

Figure 18-8:VIGIL Server Database Utility -Database Management Tab - Backup / Restore Database Settings

Repair Database

In the case that the database index becomes corrupt, the *Repair Database* feature will repair the index files and compact the memory usage of the video footage database to tune its performance.


Repair Database

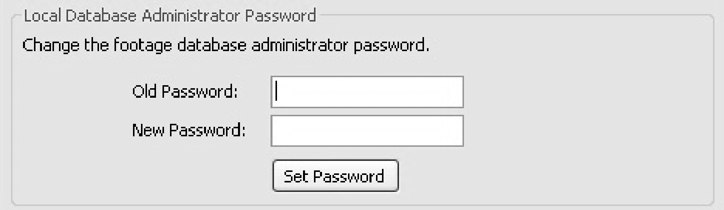
Repair index and compact the memory usage of the footage database and tune its performance.

Figure 18-9:VIGIL Server Database Utility - Database Management Tab - Repair Database Settings

18.4 Database Settings Tab

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

Local Database Administrator Password Settings


Local Database Administrator Password

Change the footage database administrator password.

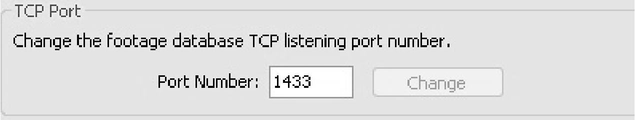
Old Password:

New Password:

Figure 18-10:VIGIL Server Database Utility - 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.

TCP Port


TCP Port

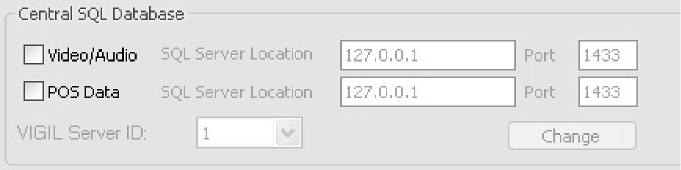
Change the footage database TCP listening port number.

Port Number: 1433

Figure 18-11:VIGIL Server Database Utility - 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.

Central SQL Database



Central SQL Database

□ Video/Audio SQL Server Location 127.0.0.1 Port 1433

□ POS Data SQL Server Location 127.0.0.1 Port 1433

VIGIL Server ID: 1

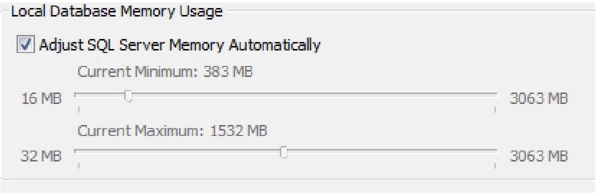
Figure 18-12:VIGIL Server Database Utility - Database Settings Tab - Central SQL DB Settings

The central SQL database feature is used to record data references into a database on a different PC. The custom database configuration utility for central database support must be run on the central database for this feature to function.

Warning: Incorrect use of the Central SQL Database settings can cause a system failure. If the VIGIL Server is experiencing database issues, please contact your system administrator or 3xLOGIC technical support.

Video / Audio	Enables video and audio information to be stored on a central SQL database.
POS Data	Enables POS data information to be stored on a central SQL database.
SQL Server Location	The network path of the central SQL database. It is possible to use two different servers for each video / audio and POS data by inputting 2 different server locations.
Port	SQL Server port being used on the server running the central SQL database
VIGIL Server ID	Each VIGIL Server connecting to the central SQL database must have a unique VIGIL Server ID.

Local Database Memory Usage



Local Database Memory Usage

☑ Adjust SQL Server Memory Automatically

Current Minimum: 383 MB

Current Maximum: 1532 MB

Figure 18-13:VIGIL Server Database Utility - 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

18.5 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.

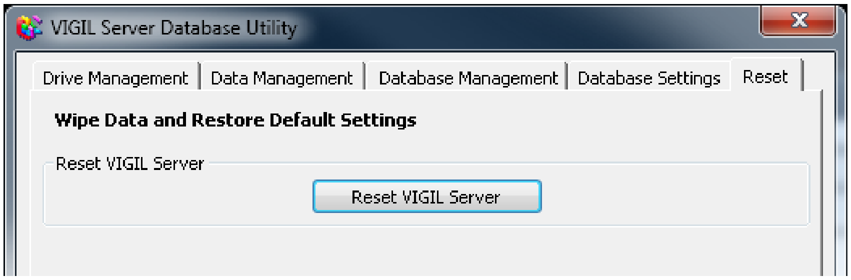


Figure 18-14:VIGIL Database Manager - Reset

19 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.

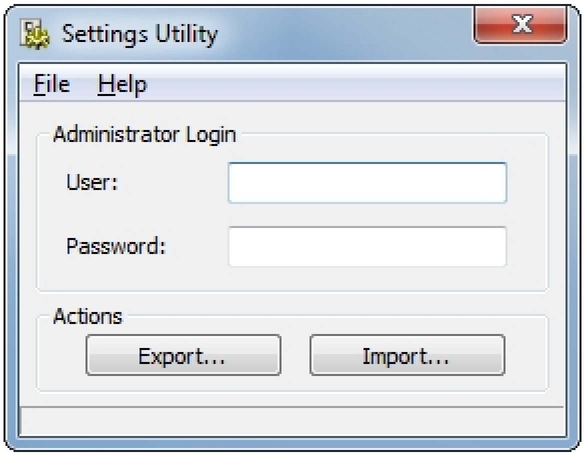


Figure 19-1:VIGIL Server Settings Utility

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.

20 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.

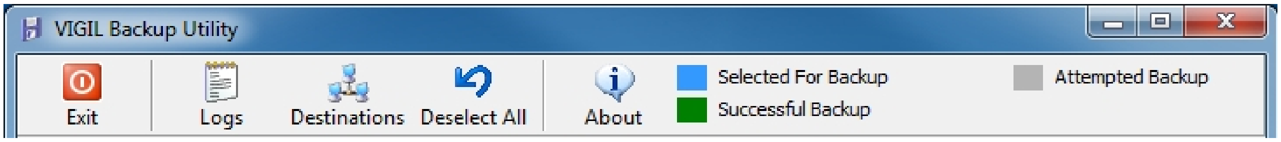
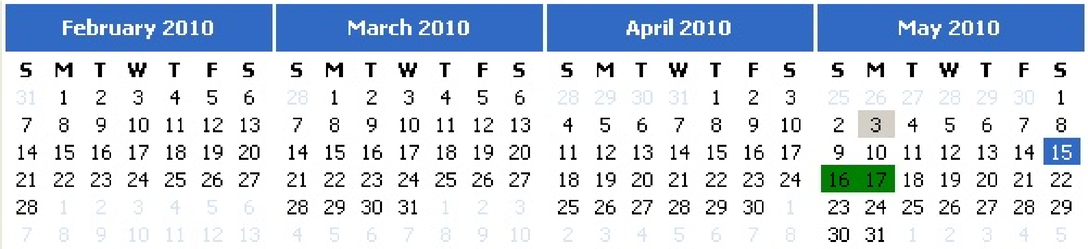


Figure 20-1:VIGIL Backup Utility

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.



February 2010

S	M	T	W	T	F	S
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	1	2	3	4	5	6
7	8	9	10	11	12	13

March 2010

S	M	T	W	T	F	S
28	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	1	2	3
4	5	6	7	8	9	10

April 2010

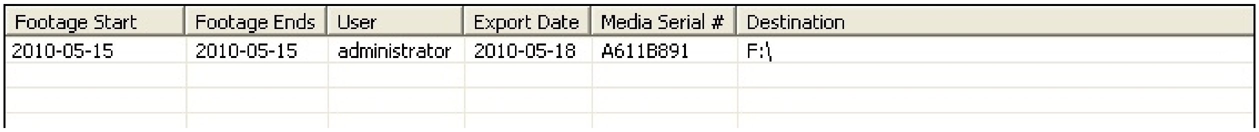
S	M	T	W	T	F	S
28	29	30	31	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	1
2	3	4	5	6	7	8

May 2010

S	M	T	W	T	F	S
25	26	27	28	29	30	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	1	2	3	4	5

Figure 20-2:VIGIL Backup Utility - Date Selection

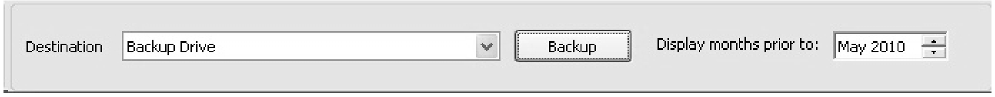
Select dates to backup by clicking the appropriate date on the calendar. Dates selected for backup are highlighted in blue. Dates that have been successfully backed up are highlighted in green. Dates with backups that have failed are highlighted in grey. Selecting successful backups (highlighted in green,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



Footage Start	Footage Ends	User	Export Date	Media Serial #	Destination
2010-05-15	2010-05-15	administrator	2010-05-18	A611B891	F:\

Figure 20-3:VIGIL Backup Utility - Backup Log

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



Destination: Backup Drive

Backup

Display months prior to: May 2010

Figure 20-4:VIGIL Backup Utility - Settings

Destination	Select the location to backup to 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.

21 Contact Information

3xLOGIC has offices in Victoria BC, Canada and in Fishers, Indiana, USA. Please visit our 3xLOGIC web site at www.3x-logic.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

3xLOGIC

VIGIL 11.5

Simple. Scalable. Secure.