Fike Video Analytics
Video Management Software

User's Guide

Fike®

Video Analytics Corporation

Table of Contents

GENERAL INFORMATION

ABOUT THIS MANUAL

The purpose of this software guide is for you to become familiar with the Fike Video Management Software's main user interface elements, how the software works, and how you should interact with it. This guide is structured to follow the general layout of the software. It does not reflect the actual process that should be taken to set up the Fike Video Analytics system for operation.

The information presented in this guide is general in nature since each site and system is unique. The Fike Video Analytics system at your site has been designed by professionals to meet your location's specific fire and security requirements. Please refer to site-specific instructions provided by your Fike Video Analytics representative to determine the exact operation of your system.

HOW VIDEO ANALYTICS TECHNOLOGY WORKS

Video Analytics is enabling a rapidly growing number of video products such as smart cameras and intelligent digital video recorders (DVRs) with automated capabilities that would have required human monitoring just a few years ago. Broadly, video analytics is the extraction of meaningful and relevant information from digital video. Video Analytics builds upon research in computer vision, pattern analysis, and machine intelligence and is also called video content analysis (VCA) or intelligent video.

Like human vision, which has a perceptual and cognitive aspect, video analytics uses computer vision algorithms that enable it to perceive or see, and machine intelligence to interpret, learn, and draw inferences. The goal of video analytics is scene understanding, which differs from motion detection. In addition to detecting motion, analytics qualifies the motion as an object, understands the context around the object, and can track the object through the scene.

Fike Video Analytics has two options for video fire detection; a UL listed, Factory Mutual approved, NFPA compliant camera with analytics internal to the camera, and computer software that can monitor and analyze video from off-the-shelf cameras (ONVIF). Fike analytics includes four standard algorithms to detect smoke (also used for oil mist detection), flame, reflected flame (called Offsite), and motion.

Smoke: In the most basic sense, video analytics algorithms for smoke detection monitor the image for movement of light patterns relative to a stable background. If the movement is consistent with "known" smoke movement patterns and preset alarm zone, sensitivity, and time delay thresholds are met, an alarm is generated.

Flame detection: The analytics monitor the same stable background and look for groups of pixels indicating slow-changing brightness accompanied by known dynamic flicker signatures.

Offsite (reflected flame): The algorithm is similar to flame in that it detects slow-changing brightness and flicker, however, spread over a larger area.

Motion: Can be detected and tracked, if desired, to monitor for the motion of people, vehicles, or depending on the sensitivity settings, rodents have been tracked.

The technology has been successfully applied in various hazards from light hazard airports, catering facilities, and museums to power plants, aircraft hangars, ship engine rooms, and outdoor chemical processing.

TERMINOLOGY

Throughout this guide, the following terms are used interchangeably.

Term	Legend
Fike Video Analytics	Proprietary technology for fire and smoke detection utilizing digital imaging devices. That may include digital video cameras with embedded firmware or standalone processing units capable of processing digital or analog video signals captured by third-party devices. It also includes systems or devices supporting the video fire and smoke detection system, such as remote operator workstations, video recording/storage systems, etc.
Fike Video Analytics IP Camera	Refers to Digital Network Camera with embedded fire and smoke detection capabilities
FSM-IP (NVR)	Fire, Smoke, Motion – Internet Protocol, refers to Event Management and Video Storage server also known as Network Video Recorder (NVR)
Server ID	A combination of the Server's network name (or IP address) with the TCP connection port used to connect to FSM-IP NVR.
Operator (guard)	A person dedicated to monitoring the facility. The operator can be physically located on the premises or dial into the system from a remote location in remote monitoring.
Administrator (admin)	A person that has been delegated the rights to configure the system
Main Window	The main Video Management Software window

SYMBOLS

Throughout the software, you will see the following symbols used to depict status.

ⓘ	**Alarm**	Throughout the application, this symbol indicates that a camera is in a general alarm state: this could be any combination of flame, smoke, offsite, motion, or guard alarms.
	Disconnected	Throughout the application, this symbol indicates a network connectivity problem between a server and a camera. It can indicate that the camera is not powered or there is no valid network path between the server and the camera.
⚠	**Fault**	Throughout the application, this symbol indicates that a camera is in a fault state: this could be any combination of content or focus faults.
🔥	**Flame**	Throughout the application, this symbol indicates that a camera is experiencing a flame alarm.
🏃	**Motion**	Throughout the application, this symbol indicates that a camera is experiencing a motion alarm.
	Offline	Throughout the application, this symbol indicates that a server is offline.
💧	**Smoke**	Throughout the application, this symbol indicates that a camera is experiencing a smoke alarm.
🧍	**User**	Throughout the application, this symbol indicates that a camera is experiencing a User alarm. User alarms are initiated manually by a user through the Video Management Software.
🔧	**Maintenance**	Throughout the application, this symbol indicates that a camera has been placed into maintenance mode (ONVIF cameras only).
🟢	**Calibration**	Throughout the application, this symbol indicates that a camera has been placed into calibration mode (ONVIF cameras only).

FIKE VIDEO ANALYTICS SYSTEM OVERVIEW

The Fike Video Analytics system is comprised of at least one IP camera, a video management system, and a video management monitoring station. You can connect any number of IP cameras and network recorders via a standard LAN / Ethernet network to expand the system to meet system requirements. There is no predetermined limit on the number of cameras and NVRs deployed on one network; however, bandwidth limitations on a particular network can significantly affect the actual performance. The number of NVRs that the Video Management Software (VMS) can handle is unlimited, and built-in smart bandwidth management limits the network video transfers to only those channels that the operator currently observes. Therefore, there is no deterioration of the frame rate observed by the operator.

There are many acceptable ways to configure the Fike Video Analytics system architecture. Three of the most basic and most implemented methods are described as follows.

FSM-IP NVR SYSTEM ARCHITECTURE

The FSM-IP Network Video Recorder (NVR) event management server is designed to network with up to 32 Fike Video Analytics IP cameras and an unlimited number of VMS monitoring stations [Figure 1]. The software contained within each Fike Video Analytics IP camera uses analytics to continually process video in real-time, frame-by-frame, to detect anomalies characteristic of smoke, fire, and motion. When an event occurs, the camera(s) will transmit the video over the network to the FSM-IP NVR and the VMS workstation. The on-duty guard receives an early warning notification along with live video from the location. The FSM-IP NVR provides digital storage for the constant recording of the video images from the Fike Video Analytics IP cameras. The NVR also acts as an information conduit between the VMS monitoring station(s) and the cameras themselves. The NVR allows on-request playback of prerecorded videos at multiple VMS workstations simultaneously. This architecture is most commonly used when 24/7 monitoring is present, and personnel can respond quickly to an event.
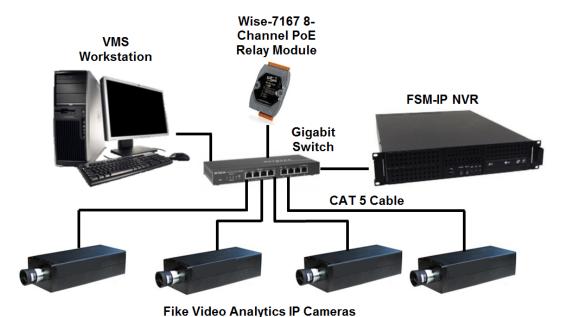
Figure 1: FSM-IP NVR Networked System Architecture (not UL Listed)

FSM-IP NVR System Connected to a Fire Alarm System

A variation of the FSM-IP NVR system architecture expands upon the system using the integral dry relay contacts provided on each Fike Video Analytics IP camera to transmit event signals to a Fire Alarm Control Panel (FACP) [Figure 2]. This system architecture is most commonly used in installations that may not have 24/7 guards and want to ensure a response to an event. In this configuration, the Fike Video Analytics IP cameras must be powered by one of the following: 1) FACP, 2) an approved security and fire camera power supply with battery backup, or 3) as a supplemental means, a PoE switch with battery backup.
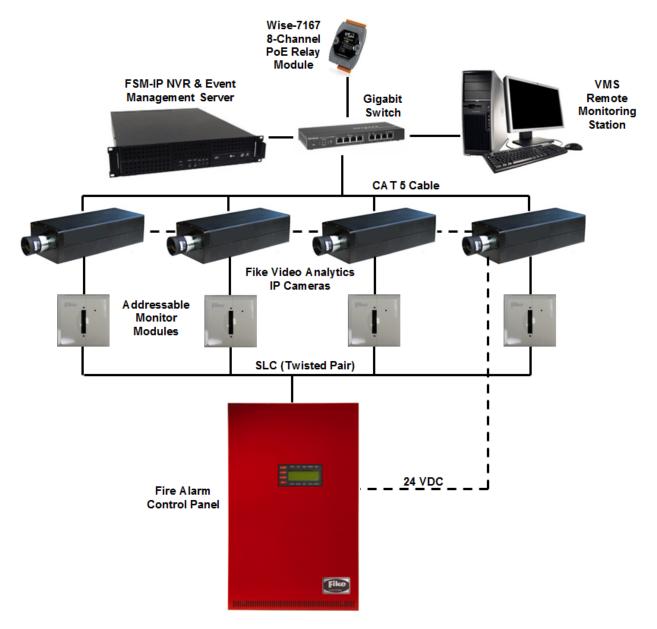
Figure 2: FSM-IP NVR Networked System Connected to an FACP (UL Listed)

EVENT MANAGEMENT SERVER SYSTEM ARCHITECTURE

The Fike Video Analytics event management server is designed to network with up to 16 ONVIF IP cameras and an unlimited number of VMS monitoring stations [Figure 3]. Unlike the FSM-IP server system, the analytics for processing the camera video is not contained within the cameras but in the Server itself. The Server comes loaded with the appropriate software that allows it to process video in real-time, frame-by-frame, to detect anomalies characteristic of smoke, fire, and motion. When an event occurs, the server will transmit the video over the network to the VMS workstation. The on-duty guard receives an early warning notification along with live video from the location. The Server provides digital storage for the constant recording of the video images from the ONVIF cameras. The Server also acts as an information conduit between the VMS monitoring station(s) and the cameras themselves. The Server allows on-request playback of prerecorded videos at multiple VMS monitoring stations simultaneously. This architecture is most commonly used when existing ONVIF compliant security cameras are installed.
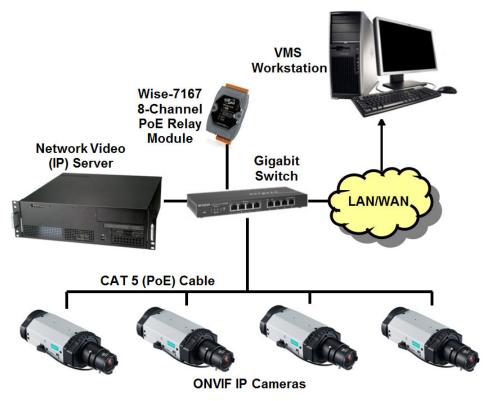
Figure 3: Event Management Server Networked System Architecture (not UL Listed)

VIDEO MANAGEMENT SOFTWARE USER INTERFACE

The Video Management Software (VMS) is a customizable surveillance and alarm monitoring software designed to provide a user interface for the Fike Video Analytics system. The software is designed so that it can monitor one or more Fike Video Analytics server installations simultaneously. What makes the VMS software rather unique is its ability to configure access to video channels according to your organization's organizational, geographical, and topological structure. The advantage of this is that you can navigate the system across the facilities using simple terms such as sites, buildings, levels, suites, etc., instead of servers and channel numbers.

STARTING THE PROGRAM

To start the Video Management Software, double-click on the program icon located on your computer desktop [Figure 4] or simply double-click on an existing configuration file if you have previously created one. The software's Main Window [Figure 5] will be displayed.

Figure 4: Program Icon

MAIN WINDOW INTERFACE

The software's Main Window [Figure 5] contains the following elements:
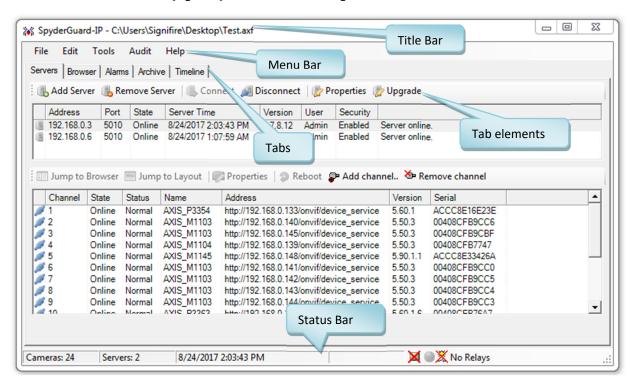
Figure 5: Video Management Software Main Window Layout

Title Bar

At the top of the program window, this bar displays the name of the active configuration file and provides tools for managing the program and the program window. At the left end of the title bar is the program icon, which you click to display commands to restore, move, size, minimize, maximize, and close the program window. To the right of the program icon, the name of the active document will be displayed. At the far right end of the title bar are three buttons that allow you to Minimize, Maximize, and Close the program.

Menu Bar

Below the title bar, all of the commands used to navigate through the general configuration options for the Video Management Software are gathered together in this central location so that you can work efficiently with the program [Figure 6].
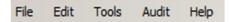
Figure 6: Menu Bar

Tabs

Below the menu bar is a set of five tabs. Clicking a tab displays an associated set of commands that correspond to the name of the tab where they reside [Figure 7].
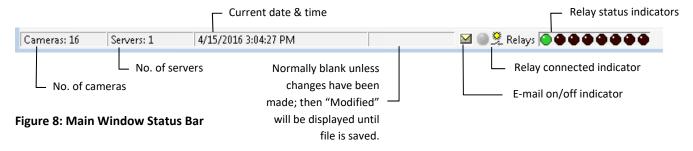
Figure 7: Tabs

A brief description of the functionality of each tab is as follows:

Servers	Allows you to manage all FSM-IP servers and their respective channels that are part of the current configuration.
Browser	Allows you to create a custom organizational structure for navigating all the cameras that are part of the current configuration.
Alarms	Allows you to quickly observe all alarms propagated to the Video Management Software monitoring station from the remote FSM-IP servers. A video of the channel responsible for the alarm will automatically appear in this view. VMS may be configured to maximize the window as new alarms come along and switch to the Alarms view.
Archive	Allows you to search through past alarms as well as view and/or download previously recorded videos.
Timeline	Displays the recorded alarms in a graphic chart and lets you replay prerecorded videos, including those channels and time periods that were not under alarm conditions.

Status Bar

Across the bottom of the program window, this bar displays information about the current system configuration [Figure 8].

Figure 8: Main Window Status Bar

MENU BAR ELEMENTS

FILE MENU

The file menu provides the following selection of user interface elements:
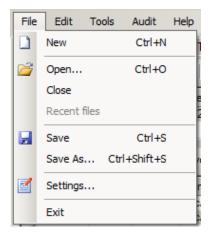
Figure 9: File Menu

- **New**

  Unloads the current configuration file and creates a new empty one.

- **Open…**

  Opens Windows Explorer to allow you to search for configuration files.

- **Close**

  Closes the current configuration file.

- **Recent files**

  Opens a list of the most recently opened configuration files.

- **Save**

  Saves the current configuration using the same file name and location.

- **Save As…**

  Save the current configuration file prompting for a new file name and location.

- **Settings…**

  Displays the Video Management Software settings dialog box [Figure 10].

The *Language* tab [Figure 10] allows you to change the language that the application will use.
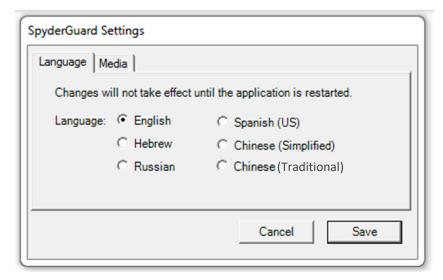
Figure 10: Application Language Settings

The *Media* tab [Figure 11] is used to set the video quality that the system will use during video recording (Low/Medium/High). This setting impacts the required server storage space. The higher the video quality setting, the greater the storage space needed on the NVR.
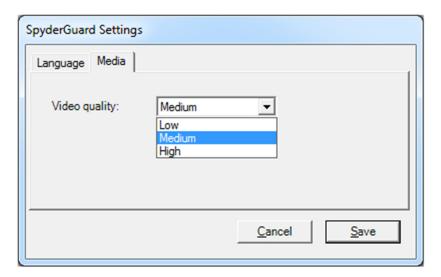
Figure 11: Application Media Setting

The Video Management Software must be restarted before any setting changes will take effect.

- **Exit**

  Closes the program.

EDIT MENU

The Edit menu [Figure 12] is used to add, remove, and modify the properties of the elements associated with the *Organizational Tree* shown in the *Browser* tab. The *Edit* menu can also be accessed by right-clicking anywhere in the *Organizational Tree* area in the *Browser* tab.
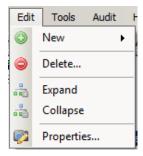
Figure 12: Edit Menu

- **New**

  Used to add new organizational elements [Figure 13] to the browser tree as children of the currently selected organizational element. You must start with an organization as the top-level (root) element. The newly created element will be added to the Organizational Tree in the Browser tab. To view the Organizational Tree, you must select the Browser tab.

  Figure 13: Adding Elements to the Organizational Browser Tree

  Each element in the *Organizational Tree* has different information associated with it that can be customized to provide meaningful information for the added element, as shown in the following figures.

  - **Organization:** Adds a new organization element to the browser tree [Figure 14].

  Figure 14: Organization Element Added to Browser Tree

– **Site:** Adds a new site element under an existing organization in the browser tree [Figure 15].
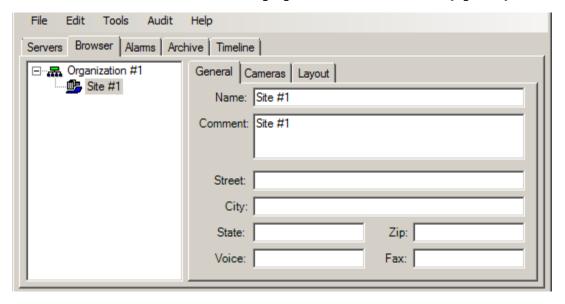
Figure 15: Site Element Added to Browser Tree

– **Building:** Adds a new building element under an existing site in the browser tree [Figure 16].
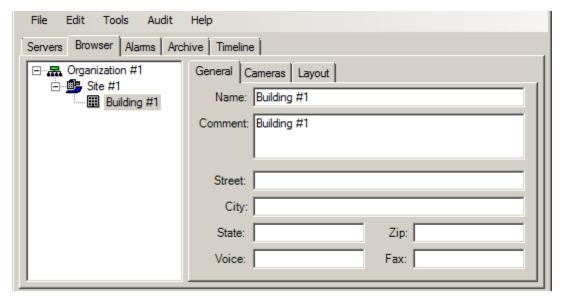
Figure 16: Building Element Added to Browser Tree

– **Floor:** Adds a new floor element under an existing building in the browser tree [Figure 17].
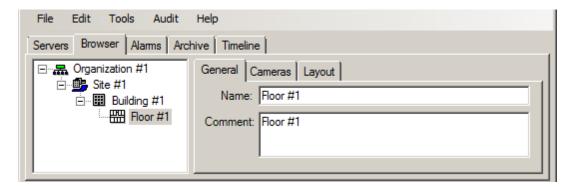
Figure 17: Floor Element Added to Browser Tree

– **Suite:** Adds a new suite element under an existing floor in the browser tree [Figure 18].
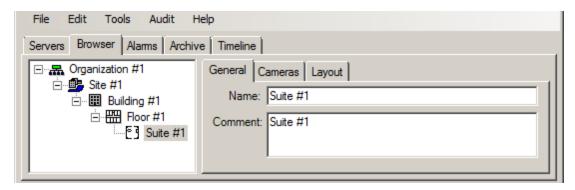
Figure 18: Suite Element Added to Browser Tree

- – **Camera:** Adds a new camera under an existing site, building, floor, or suite element in the browser tree [Figure 19]. Refer to Page 55 for additional information about adding cameras to the organizational tree.
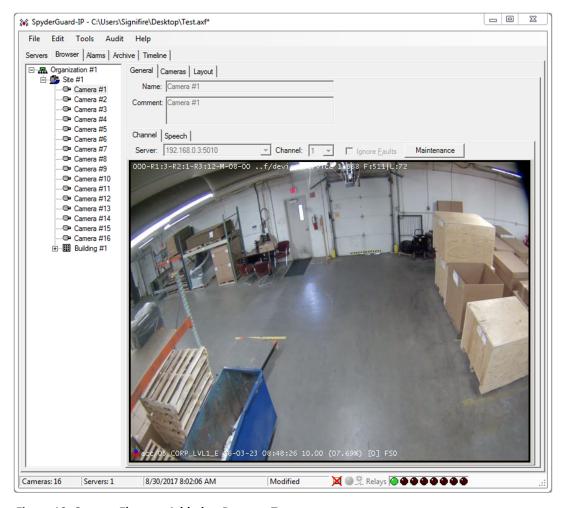
Figure 19: Camera Element Added to Browser Tree

- **Delete**

  Deletes the selected Organizational Tree element from the browser tree.

- **Expand**

  Expands the selected browser tree element to display all of the element's children.

- **Collapse**

  Collapses the selected browser tree element to hide all of the element's children.

- **Properties**

  If the selected element in the Organizational Tree is a camera, this menu item will become accessible. Clicking Properties… will load the *Channel Settings* dialog box [Figure 20].

Channel Settings

The *Channel Settings* dialog box [Figure 20] allows you to change the camera's operational settings. The settings are stored on the physical camera and cached on the server that owns the channel.
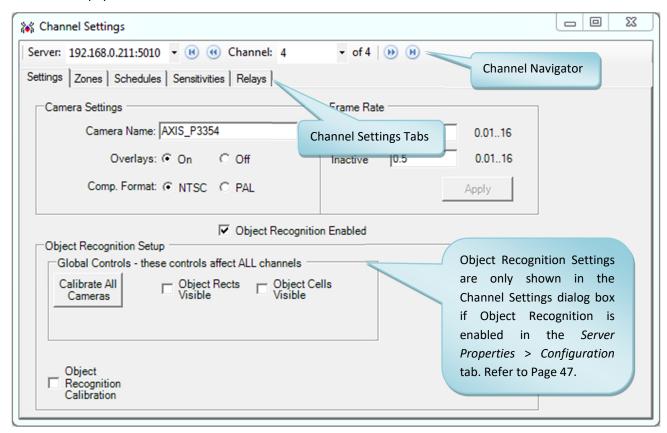
Figure 20: Channel Settings Dialog Box

CHANNEL NAVIGATOR BAR

The Channel Navigator bar [Figure 21] provides quick access to each Server and their respective channels.
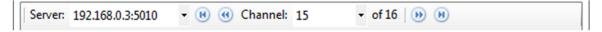
Figure 21: Channel Navigator Bar

CHANNEL SETTINGS TABS

Below the *Channel Navigator* bar is a set of five tabs. Clicking a tab displays an associated set of commands that correspond to the name of the tab where they reside [Figure 22].

Figure 22: Channel Settings Tabs

SETTINGS TAB

The *Settings* tab [Figure 23] allows you to adjust the settings for each camera associated with the Video Management Software application. Click *Apply* to accept the setting changes.
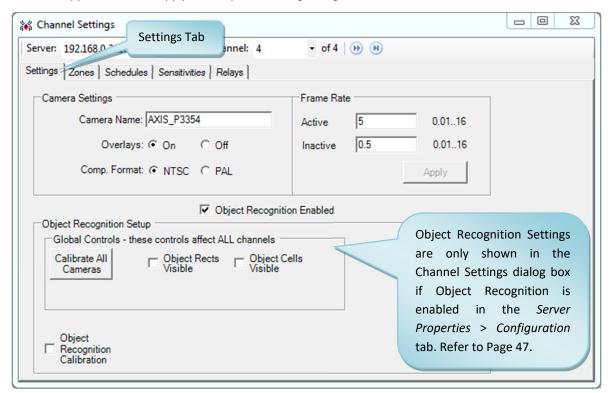
Figure 23: Channel Settings - Settings Tab

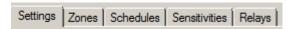| Camera Name:	Used to assign a custom name to identify the camera. It does not need to be unique.
Overlays:	Used to turn On and Off all onscreen text and graphics associated with the channel.
Comp. Format:	Toggles the camera between NTSC and PAL modes, which are two color encoding systems that affect the composite output (visual quality) of the content viewed. The camera must be rebooted for this change to take effect.
Active Frame Rate	Used to adjust the camera frame rate for active alarm video recording.
Inactive Frame Rate	Used to adjust the camera frame rate for inactive (play on motion) video recording.
Object Recognition Enabled †	If checked, the camera will utilize Object Recognition, subject to the disclaimer on the next page. See the next page for a description of this feature.
Calibrate All Cameras †	Initiates calibration of all cameras connected to the selected Server for object recognition operation. The calibration icon will flash on all cameras connected to the selected Server in the organizational tree.
Object Rects Visible †	If checked, the camera image will show the calibration boxes (yellow) associated with the object recognition calibration.
Object Cells Visible †	If checked, the camera image will show the blocking boxes (red) associated with the object recognition calibration.
Object Recognition Calibration †	Used to initiate the calibration of the currently selected camera only for object recognition operation. The calibration icon will flash for the selected camera in the organizational tree.

† These settings only become available if the system server is enabled for Object Recognition operation.

> **Object Recognition Disclaimer:** The customer acknowledges and agrees that activation of the Video Management System (VMS) Object Recognition Feature is at the customer's sole discretion. Object recognition is optimal for smoke generated by smoldering fires. A rapid rise of concentrated, high volume smoke may result in delayed recognition of such a hazard by the VMS when the object recognition feature is in use.

OBJECT RECOGNITION OPERATION

Fike Video Analytics detects the outline of smoke or fuel mist within its field of view to initiate an alarm. False alarms can occur where objects in the camera's field of view have similar motion or color to smoke. One example of an object in the field of view that can trigger such false alarms is a human being, particularly those wearing light clothing.

Fike Video Analytics utilizes Object Recognition to identify whole or partial images of people in the frame to reduce the number of false alarms triggered by human beings. Object Recognition works by locating the human being in the image and creating a temporary blocking zone for Smoke alarms in that localized area. This is done by the analytics automatically, without user intervention. If a person has been identified and blocked, the smoke outline will still appear in the video, but no alarm will be triggered.

CALIBRATING CAMERAS FOR OBJECT RECOGNITION

The Object Recognition algorithm is efficient at identifying portions of the human form. Because of this, it is possible to identify objects in the video frame that may appear to be part of a person. An example of this would be pipes that appear to be legs. In this circumstance, a Smoke blocking zone shouldn't be formed in this region of the camera frame. To manage this, Object Recognition Calibration is used to identify areas of the video frame that appear to be a part of a human being but are, in fact, inanimate objects.

Object Recognition Calibration is accomplished in two ways. First, a manual calibration is performed at install time that quickly identifies objects in the room and marks those regions as not to be blocked by Object Recognition. Second, Object Recognition processing continually evaluates all located objects and marks objects determined to be inanimate so as not to be blocked by Object Recognition. This process is known as Auto Calibration. In this way, if an object is carried into the room that approximates the form of a person, Auto Calibration will learn that this object is inanimate over time. The region around this object will no longer block Smoke alarms.

> **Note:** Manual calibration must be performed on all cameras at the time of install for the Object Recognition algorithm to operate correctly. In addition, if a camera view changes, a manual calibration should be performed. It's recommended that manual calibration be performed with no personnel present in the area served by the camera.

> **Note:** By default, the Video Management Software regularly performs the camera calibration process on all cameras connected to the Server. This process is known as Auto Calibration. Auto calibration takes place with no interaction from the user and is constantly adjusting the system to the camera view.

ZONES TAB

The *Zones* tab [Figure 24] allows you to create zones to define specific regions of the camera image for event monitoring. Each zone, once created, provides special treatment to events that originate within the defined zone based on programming. Zoning information is stored on the Video Management Server and will be seen on other VMS monitoring stations.
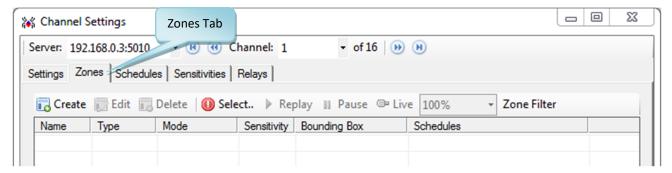

Figure 24: Channel Settings – Zones Tab

By default, no zones are set up in the camera(s). Cameras will detect and record all flame, offsite, and smoke events across the camera image without zones. Motion detection is unique in that a detection zone needs to be set up for the motion algorithms to be active. Detection zones are areas of the camera image where the system will watch for changes and generate the appropriate alarms.

Multiple zones can be assigned to each camera image, with each zone being algorithm-dependent. For example, a flaming fire within a smoke-blocking zone will be detected by the camera. A second flame block zone would have to be created to block the flame alarm from occurring.

Zones can be scheduled to become active or inactive for specific times/days/months. To do so, you will need to create a schedule for each zone. Refer to Page 25 for detailed information on setting schedules. With no schedules present for the zone, the zone will always be in the active state.

SUMMARY OF ZONING FEATURES

- Each zone is independent

- Each blocking zone blocks the alarm, not the algorithm process

- Each zone is specific to the event type (i.e., flame, motion, offsite, smoke)

- Each zone can be given its own schedule

- The zones do not work together to mask a cumulative area

ZONES TOOL BAR

The *Zones* tool bar [Figure 25] allows you to create, edit and delete camera zones.

Figure 25: Zones Tab Tool Bar

CREATE

Clicking the *Create* button will open the Zone editor dialog box [Figure 26], allowing you to create and define a zone for the selected camera.
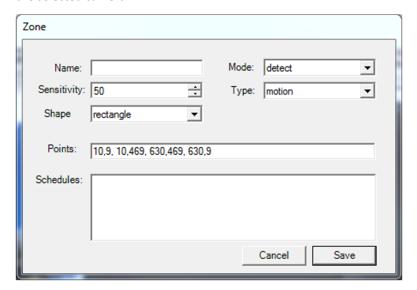

Figure 26: Zone Editor Dialog Box

Name	Enter a unique and meaningful name for the zone (no spaces allowed). This field is only editable when creating a new zone.
Sensitivity	Defines how sensitive a motion zone is to motion (0 – 3000). A small number is more sensitive, and a higher number is less sensitive. Not applicable to other event types.
Shape	Defines the shape of the zone (rectangle or polygon).
Mode	Defines the function of the zone as either detect or block. **Detect** = Area defined by the shape will detect the event type selected for the zone. **Block** = Area defined by the shape will block the event type selected for the zone.
Type	Defines the event type the zone will react to. Only flame, smoke, and motion are valid options.
Points	Defines the display coordinates for the zone.
Schedules	If assigned, it determines when the zone will be active. If no schedules are attached to the zone, then the zone is always active.

Clicking the *Save* button will add the new zone to the *Zones* list [Figure 27], which will display the zone settings.
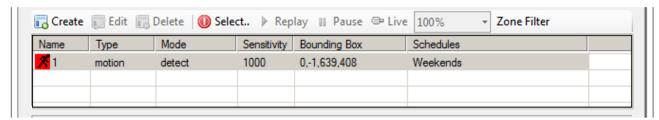

Figure 27: Camera Zones List

The newly created zone will be overlaid onto the video image [Figure 28]. You may move or resize the zone by selecting and dragging the *Geometry Control* handles. Standard practice is to place the zone in the image areas that make sense to monitor for the specified event type while avoiding areas that do not require monitoring.
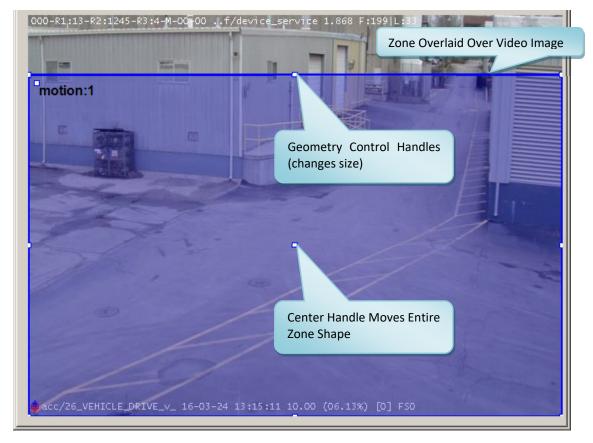
Figure 28: Zone Boundary Overlaid Over Video Image

EDIT Edit

At any time, you can edit the selected zone settings by clicking the *Edit* button on the *Zones Toolbar*. This will open the *Zone Editor* dialog box [Figure 26], allowing you to change the zone settings.

DELETE Delete

You can delete the selected zone by clicking the *Delete* button on the *Zones Toolbar*. The zone will be removed from the *Zones* list.

SELECT Select..

The software allows you to select and replay previously recorded events associated with the selected camera to assist you with the setup of the camera zoning. This will enable you to review the past events while editing the zone to ensure you are correctly sizing and positioning the zone.

Clicking the *Select* button opens the *Event Selector* dialog box [Figure 29]. From this screen, you can filter the event types to be displayed in the list for playback.
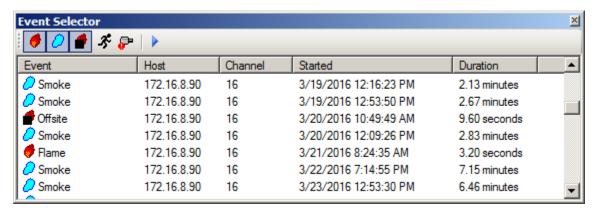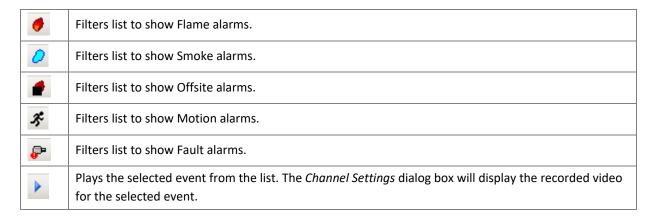
Figure 29: Event Selector Dialog Box

	Filters list to show Flame alarms.	
	Filters list to show Smoke alarms.	
	Filters list to show Offsite alarms.	
	Filters list to show Motion alarms.	
	Filters list to show Fault alarms.	
	Plays the selected event from the list. The *Channel Settings* dialog box will display the recorded video for the selected event.	

VIDEO PLAYBACK OPTIONS

The video can be paused and replayed during playback, and the playback speed adjusted using the tools available in the *Zones* toolbar.
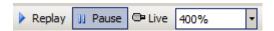
Figure 30: Video Playback Options

REPLAY BUTTON
Replays the selected event.

PAUSE BUTTON
Pauses the currently playing video.

LIVE BUTTON
Switches the selected camera to the live video feed.

PERCENTAGE DROPDOWN
Allows you to set the video playback speed.

ZONE FILTER

Clicking the Zone Filter button opens the Zone Filter dialog box [Figure 32]. You can select what zone types and modes will be displayed in the Camera Zones List from this screen.


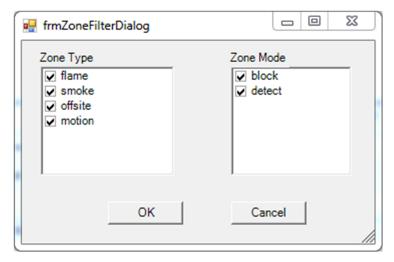**Figure 31: Zone Filter Option**

Figure 32: Zone Filter Dialog Box

SCHEDULES TAB

The *Schedules* tab [Figure 33] allows you to create schedules that can be attached to the zones, so they are only active during the scheduled time frame. Each camera can have a unique set of zones and schedules.
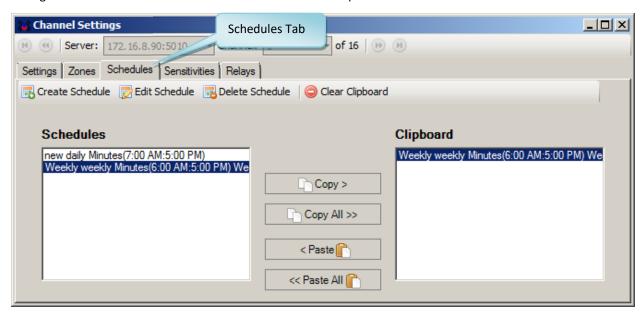

Figure 33: Channel Schedules

CREATE SCHEDULE Create Schedule

You can add a new schedule to the schedules list by clicking the *Create Schedule* button. This will open the *Schedule* dialog box [Figure 34], allowing you to define the schedule settings.
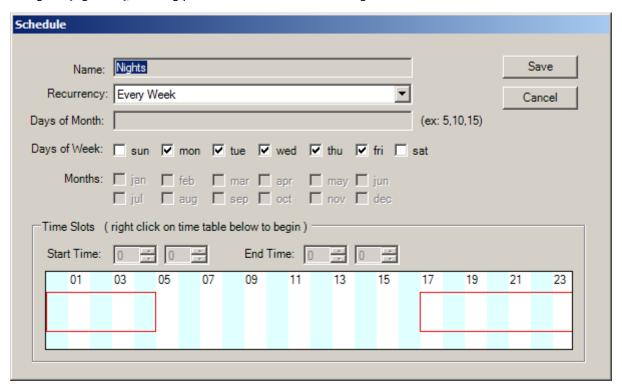
Figure 34: Schedules Editor Dialog Box

Name:	Enter a unique name for the schedule.
Recurrence:	Defines the period over which the schedule reoccurs (One Time, Every Day, Every Week, Every Month, Every Year).
Days of Month:	Defines the days of the month (separated by commas) on which this schedule should be active (e.g., 5,10,15).
Days of Week:	Defines the days of the week on which this schedule should be active.
Months:	Defines the months of the year on which this schedule should be active.
Time Slots	Defines the times of the day on which this schedule should be active. You must create at least one time slot for the schedule to be valid.

TIMESLOT EDITOR

To create a timeslot, right-click on the Time Table to display the context editor [Figure 35]. The context menu allows you to add a new time slot, delete the selected time slot, or delete all.
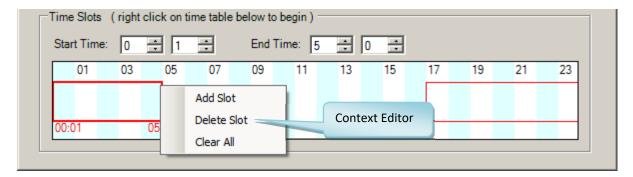
Figure 35: Timeslot Editor

To edit a time slot, select it and drag the left and right edges of the box, or alternately you can type in the hours and minutes in the *Start Time* and *End Time* fields. Note that all hours are in 24-hour format (military time). In addition, time slots cannot overlap.

EDIT SCHEDULE 📝 Edit Schedule

You can edit an existing schedule by selecting the schedule from the *Schedules* list and then clicking the *Edit Schedule* button. This will open the *Schedule* dialog box [Figure 32], allowing you to edit the schedule settings.

DELETE SCHEDULE Delete Schedule

You can delete an existing schedule by selecting the schedule from the *Schedules* list and then clicking the *Delete Schedule* button.

SCHEDULES CLIPBOARD

You can easily share schedules between cameras by using the Schedules Clipboard [Figure 33]. The clipboard allows you to copy and paste existing schedules that you want to share with other cameras to the clipboard. Once copied to the clipboard, the schedule(s) can then be selected and pasted to any other camera. Use the *Clear Clipboard* button Clear Clipboard to clear the clipboard.

SENSITIVITIES TAB

The *Sensitivities* tab [Figure 36] allows you to adjust three different detection algorithms for the selected channel. Choosing correct sensitivities is part of the system tuning process. Sensitivities are set up for each category of alarm (flame, smoke, and offsite). Each category has preset sensitivity settings that you can set to make the camera more or less sensitive. Each detection algorithm has a delay setting that prevents the alarm from triggering for a specified time interval (0 – 254 seconds).
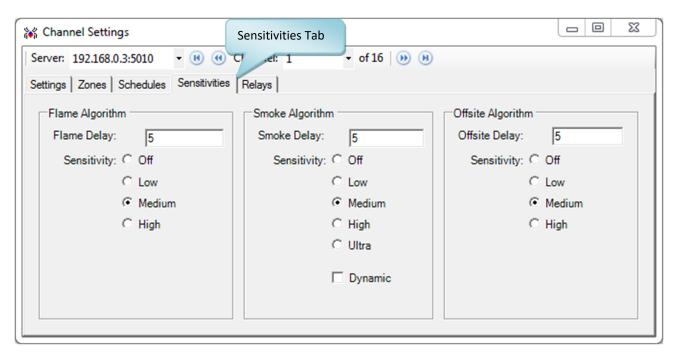
Figure 36: Channel Sensitivity Settings

Delay:	Controls the amount of time the algorithm (Flame, Smoke, Offsite) must be in alarm before the camera enters an alarm state. This setting can be used to filter out nuisance faults.
Sensitivity:	Controls how sensitive the algorithm (Flame, Smoke, Offsite) is to an event. Turning the algorithm off will disable the detection algorithm (Flame, Smoke, Offsite).
Dynamic	When enabled, it forces the smoke algorithm to verify the event before initiating an alarm.

RELAYS TAB

The *Relays* tab [Figure 37] allows you to control the operation of the three dry contact relays on the back of the Fike Video Analytics IP camera(s). Each relay can be independently programmed to close on different conditions and set for Automatic or Manual configuration.
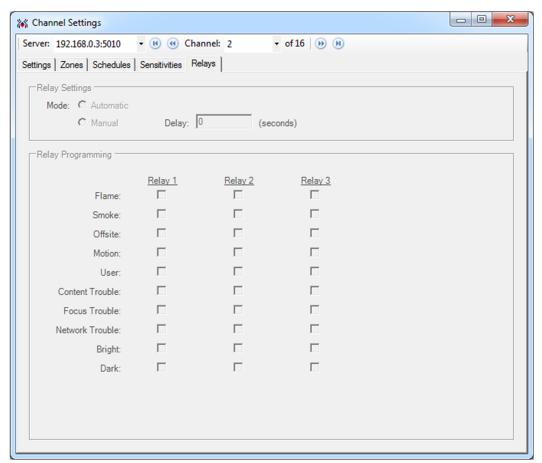

Figure 37: Channel Relay Settings

Automatic Mode	The camera will automatically close any relay for which the corresponding alarm has occurred.
Manual Mode	The camera begins a countdown for the specified number of seconds defined in the delay field as soon as the event condition is met. The system operator will receive the video and alarm and have the option to delay, stop or confirm the event. Confirming the event will cause immediate closure of the relay. Delaying the event will reset the countdown timer to the initial position delay period and begins the count down again, providing more time to investigate. The operator could also reset the camera, which will clear the alarm.
Relay Programming	Controls which relays will activate in response to the selected alarm event.

> **Note:** Relay 2 is inverted in the normal state, meaning it is closed in a non-alarm state, so when power fails, the relay will open, signaling an alarm state. Relays 1 and 3 are normally open in a non-alarm state.
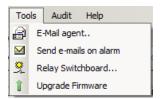
TOOLS MENU

Figure 38: Tools Menu

E-Mail agent..

The *E-Mail Agent* dialog box [Figure 39] allows you to configure the VMS application to send an e-mail to a designated e-mail address in response to system events.

Figure 39: E-Mail Agent Dialogue Box

Mail to be sent to	Enter the e-mail address where the event message is to be sent. Multiple e-mails can be entered separated by a semicolon ';.'
Mail originated from	Enter the e-mail address of the system where the message was sent from.
Subject	Defines prefix phrase for the subject that will be followed by the description of an alarm such as "Fire Alert."
Mail Server	Specifies a valid SMTP server that is authorized to relay e-mails from the account of the guard. (Verify with an IT Administrator)
Mail Server Port	Enter the dedicated port (default 25)
Select only these events	Select which events will initiate an e-mail message (Fire, Smoke, Offsite, Motion, Fault).
Send e-mails on alarm	Turns the E-Mail Agent function ON or OFF. The e-mail status icon ✉ in the main window status bar will indicate the active state of the e-mail function. If the status icon appears with a red cross, the e-mail agent is turned off. The e-mails will not be sent until the agent is turned on. The E-Mail Agent function can also be turned ON or OFF using the Tools/Send e-mails on alarm command on the main menu [Figure 38].
Test	Tests the validity of entries by sending a test message. If recipients do not exist or specified Mail Server is unavailable or not authorized for the relay, the VMS application will respond with an error message.
Use Authentication	Enables the use of authentication with the SMTP server.

After configuring the agent and receiving the test message, you may close the E-mail Agent configuration form. When turning the E-Mail Agent ON or OFF, the VMS will send a message. When an alarm occurs, the agent will send the message with a snapshot of the video captured from the channel that caused the alarm [Figure 40].
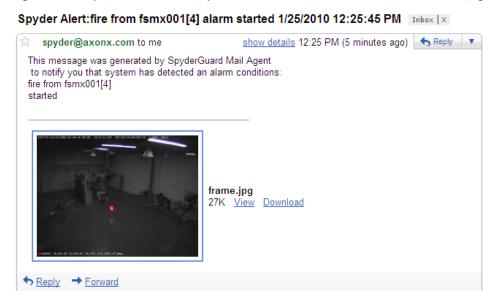

Figure 40: Alarm Notification Messages (Gmail client)

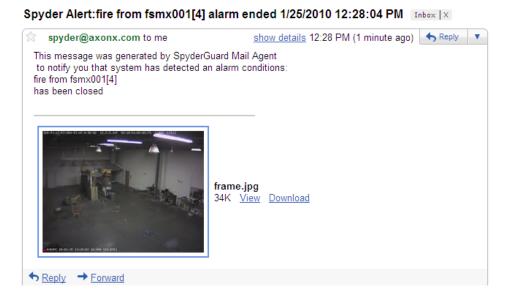Similarly, when alarm conditions recede, another message will be sent [Figure 41].

Figure 41: Alarm Ended Notification Messages (gmail client)

Relay Switchboard…

A monitoring station can support a single Ethernet relay module (Wise 7167); however, when multiple monitoring stations are connected to a common network, only one monitoring station shall have a relay module connected. The module provides eight dry relay contacts, seven of which can be independently programmed. Before the relay switchboard can be used to configure the relay, it must first be connected to the monitoring station.

ADDING WISE RELAY MODULE

To add the Wise relay module to the system, click on the "*No Relays*" icon on the VMS status bar located at the bottom of the main program window [Figure 42].

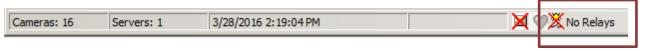| Cameras: 16	Servers: 1	3/28/2016 2:19:04 PM		✕ ❤ ✕ No Relays

Figure 42: Main Window Status Bar

The *Relay Module Setup* dialog box [Figure 43] will open. Select the relay module type (Wise_7167) and enter the designated IP address assigned to the module. Click *Verify* to establish communication with the relay module. "Searching for device…" will be displayed until communication with the device is established.
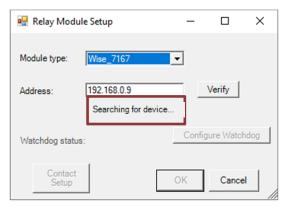

Figure 43: Adding an External Relay

Once the communication is established, the configurable settings for the relay will become available [Figure 44]. Click Configure Watchdog to enable the relays Watchdog operation (optional feature). Click Contact Setup to configure the relays for normally open or closed operation.
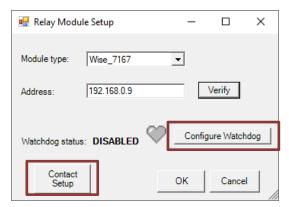

Figure 44: Relay Module Setup

CONFIGURE RELAY WATCHDOG OPERATION

Wise Relay modules equipped with Firmware version 1.33 can be configured for Watchdog operation. This is an optional function, that when enabled, automatically configures coil 2 on the relay module for NC fail-safe operation. When the watchdog operation is enabled, VMS software will initiate a supervisory "heartbeat" every 20 seconds to the connected servers. Should a server fail to respond within 2 minutes of the heartbeat initiation, the VMS software will activate the relay (coil 2) to indicate the loss of communication. In addition, if the VMS software itself should be shut down for any reason, the relay (coil 2) will activate as well.

By default, the Watchdog operation on all Wise Relay modules are disabled and must enabled by clicking Enable Watchdog [Figure 45].
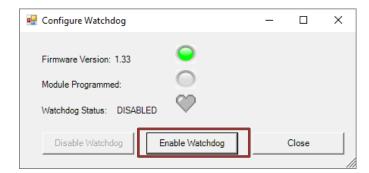

Figure 45: Configure Watchdog

If the firmware version of the relay being configured is not version 1.33, the following error message [Figure 46] will be displayed. This message indicates that the relay module's latest firmware needs to be uploaded to enable the watchdog feature. Click OK to close the message.
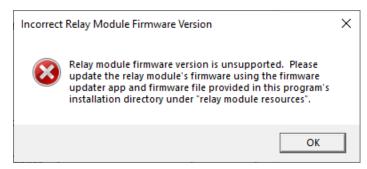

Figure 46: Incorrect Relay Module Firmware Version Message

To update the Wise Relay firmware, you must navigate to the VMS software's program installation directory [Figure 47] under "relay module resources". Locate the WISE Firmware Uploader Setup V2.5.1 app and the WISE-7167v133.HEX firmware file.
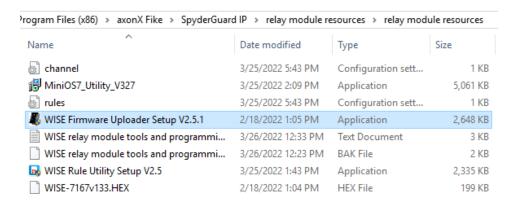
Figure 47: WISE Relay Module Resources Folder

Double-click on the WISE Firmware Uploader application to execute the application [Figure 48]. Select WISE 4000, 71xx and 790x Series as the Module Type. Type the relays IP Address. Navigate to and select the WISE-7167v133.HEX firmware file. Click Upload Firmware to initiate the firmware update.
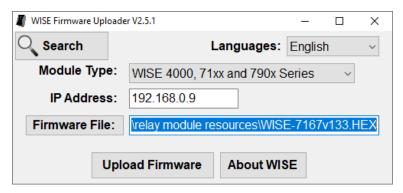

Figure 48: WISE Firmware Uploader

Close the uploader screen and return to the Configure Watchdog screen after the update is complete. Click Enable Watchdog to complete the process. The Configure Watchdog screen should indicate the Enabled status of the Watchdog feature. Click Close to return to the Relay Module Setup screen [Figure 45].

Figure 49: Watchdog Feature Enabled

CONFIGURE RELAY CONTACT TYPE

The Relay Contact Configuration screen [Figure 50] will be displayed. From this screen, each of the seven relays available on the module can be configured for normally open (NO) or normally closed (NC) operation. By default, all relays will be set to normally open, unless the optional relay Watchdog feature is enabled. Then Coil 2 is defaulted to normally closed (NC) for fail-safe operation. Click each coil to select NO or NC operation; then, click OK to exit the Relay Contact Setup screen [Figure 44].
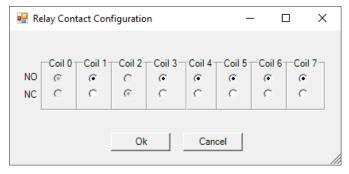

Figure 50: Setting Relay Contact Types

Note: All relay contacts will default to the normally open state if power to the Wise relay module is lost.

Once all settings (i.e., watchdog and contacts) for the relay module have been completed, Click OK to accept the changes and exit setup.

Figure 51: Relay Module Setup Complete

Once the relay module is connected, communication is established, and configuration changes made, the *Main Window* status bar [Figure 52] will change to indicate the status of the Watchdog, connected status of the external relay module, and the state of the module's eight relays. The Watchdog heart will change from being grayed out to red to indicate the activate status of the watchdog's heartbeat. The relay status indicator will change from indicating "No Relays" to indicating "Relays," and a green indicator will illuminate to show the connected status of the relay module. The remaining indicators will illuminate (red) upon activation of each relay.

Figure 52: External Relay Status Bar

Note: Should a communication problem with one or more servers occur with the watchdog feature enabled, a "Watchdog check failed" error message will be displayed.

CONFIGURING RELAY OPERATION

The *Relay Switchboard* dialog box [Figure 47] can now be used to configure the external relay module. Within the Relay Switchboard window, you will find two tabs. The features within the tabs will allow you to generate new rules, arrange the order of the rules, edit rules, delete rules, and test relay functionality.

RULES TAB

The *Rules* tab displays a list of created rules that will be initially empty. Right-click within the list box and select "New rule…" or click the New Rule button to populate the list. In response, the VMS application will open the *Relay Rule Wizard* [Figure 53].
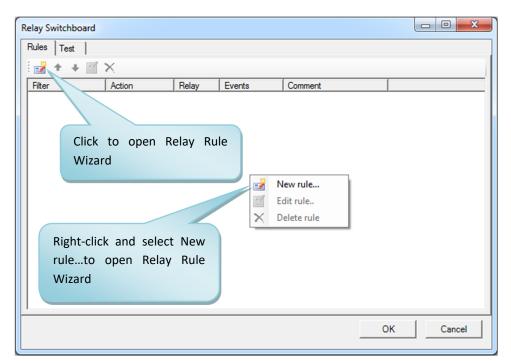

Figure 53: Relay Switchboard Form

NEW RULE

Adds a new rule to the rules list.

MOVE RULE UP ⬆

Moves the currently selected rule up one position in the list.

MOVE RULE DOWN ⬇

Moves the currently selected rule down one position in the list.

EDIT RULE

Opens the *Relay Rule Wizard* dialog box allowing you to edit the currently selected rule.

DELETE RULE ✕

Deletes the currently selected rule.

Each rule defines the action for a single relay. The Wise-7167 relay module has eight relays, with one reserved for status, which leaves seven relays (1-7) for user-defined rules.

Figure 54: Relay Rule Wizard

Source	Sets the IP address of the camera that will trigger the selected relay to activate. Use the asterisk to define all the channels or select channels individually.
Filter	Sets the event type(s) that will trigger the selected relay.
Action	Sets which relays will activate in response to the event. Include=Relay will be engaged when any of the filtered alarm types takes place. Exclude=Relay state will override any other engaging rule.
Comment	Enter a description of the function of the relay or any other comment associated with the relay operation.

TEST TAB

The *Test* tab [Figure 55] allows you to manually test each relay (1-7) on the Wise relay module. Selecting the check-box for each relay will turn it on.
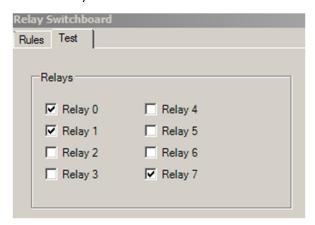

Figure 55: Relay Switchboard Test Tab

Upgrade Firmware:

Upgrade Firmware dialog box [Figure 56] allows you to upgrade the firmware on Fike Video Analytics IP cameras from within the VMS application without disconnecting the camera(s) from the system.
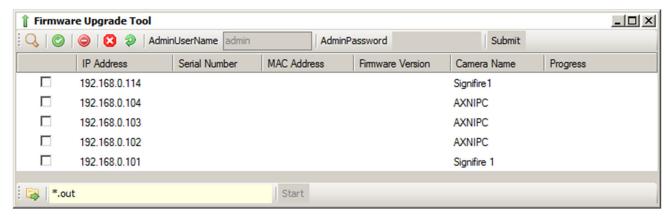

Figure 56: Fike Video Analytics IP Camera Firmware Upgrade

DISCOVER

Discovers cameras connected to the VMS monitoring station. Camera information is displayed in the camera list.

SELECT ALL

Selects all cameras in the camera list.

DESELECT ALL

Deselects all cameras in the camera list.

CANCEL UPGRADE

Cancels the firmware upgrade process.

RESTART CAMERA

Restarts the selected camera(s).

ADMINUSERNAME

Enter the administration level user name.

ADMINPASSWORD

Enter the administration level password.

SUBMIT

Submits the user name and password to the selected Fike Video Analytics IP cameras.

CHOOSE FILE

Opens Windows Explorer allowing you to locate the firmware upgrade file (*.out).

START

Starts the firmware upgrade process

IP Address	Displays the IP address of the camera.
Serial Number	Displays the serial number of the camera.
MAC Address	Displays the MAC (media access control) address of the camera.
Firmware Version	Displays the current firmware version of the camera.
Camera Name	Displays the unique name given to the camera.
Progress	Displays the progress of the firmware upgrade process.

AUDIT MENU

Figure 57: Audit Menu

Generate..

Generates a system audit report [Figure 58]. The audit report is used to provide a hard paper copy of the Fike Video Analytics system configuration. This is useful for documenting and checking the system configuration during system maintenance to ensure the system has not been compromised.
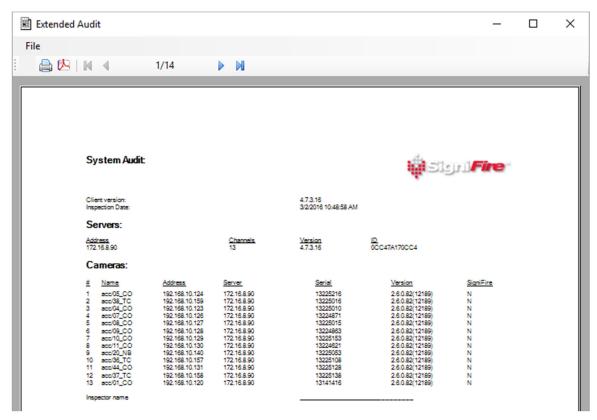

Figure 58: System Audit Report

The report can then be saved as an .audit file by selecting **File>Save data…** or closed by selecting **File>Exit** from the File menu [Figure 59].
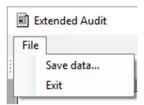

Figure 59: Extended Audit File Menu

The utility bar at the top of the audit report window provides the following functions associated with the report results.

PRINT

Prints the Audit report to a connected printer.

SAVE AS ACROBAT PDF

Prints the Audit report to an Adobe PDF file.

START

Skips to the first page of the Audit.

PREVIOUS

Steps one page back.

NEXT

Steps one page forward.

LAST

Skip to the last page of the Audit.

Verify..

Opens a saved audit report and compares it to the current Fike Video Analytics system settings. This is useful for documenting and checking system configuration settings during maintenance to ensure the system has not been compromised. If a setting has been changed, the verify feature highlights the change so corrective action can be taken.

To verify an audit, select *Verify* from the *Audit Menu*. You will be prompted to browse for an old audit file to compare the current settings too. Once selected, the VMS application will compare all the camera settings, including the field of view, and display the results for review in the audit list [Figure 60].

> **Note:** Verify will only work with a saved .audit file.
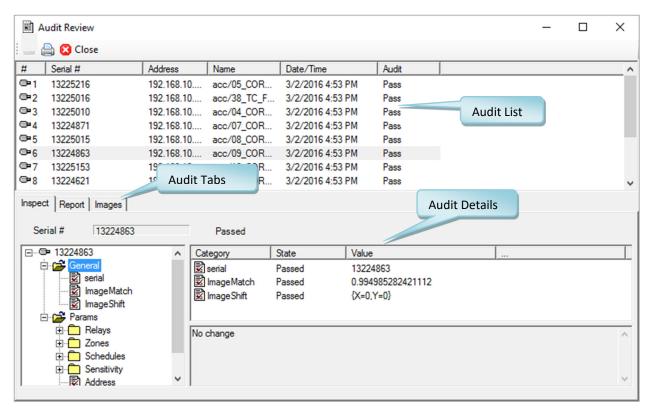

Figure 60: Audit Review Display

The audit list displays the following information pertaining to the audit.

#	Channel number of the camera being audited.
Serial #	Serial number of the camera being audited.
Address	IP address of the camera being audited.
Name	Name of the camera being audited.
Date/Time	Time audit was performed.
Audit	Audit results (Pass/Fail).

If a problem is detected during the audit review, it will be highlighted on the camera icon, and a fail grade will exist for the camera in the audit column [Figure 61]. A fail can occur for several reasons and does not necessarily mean the system is not functioning. For example, if enough of the image's content has changed, the image match could get a failing grade even though the camera is properly aligned and correctly covers the hazard area. The fail indicator means further examination is required to ensure the system is working correctly.
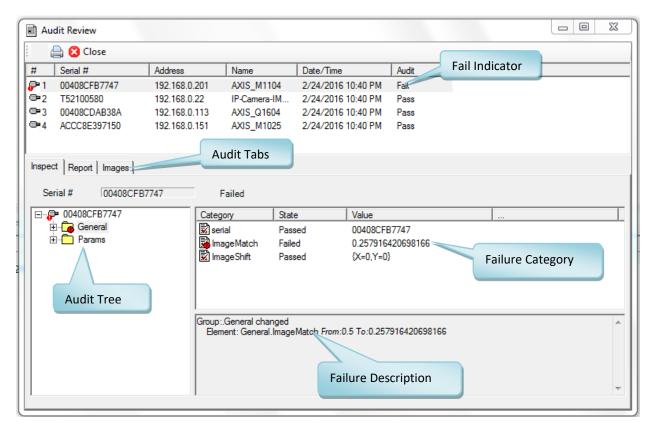

Figure 61: Audit Review Fail Display

Within the *Audit Review,* you can drill down into each camera's settings and audit results using the three audit review tabs located on the middle left of the *Audit Review* screen.

INSPECT TAB

The *Inspect* tab [Figure 61] provides detailed information regarding the *Audit Review* results. Upon selecting a channel number from the audit list, the three windows will display details concerning the camera's inspection results.

REPORT TAB

The *Report* tab [Figure 62] allows you to generate a printable version of the audit report for the selected channel. The report shows a side-by-side comparison between the saved audit report and the current system configuration. Any changes detected during the audit will be visually indicated in the report.

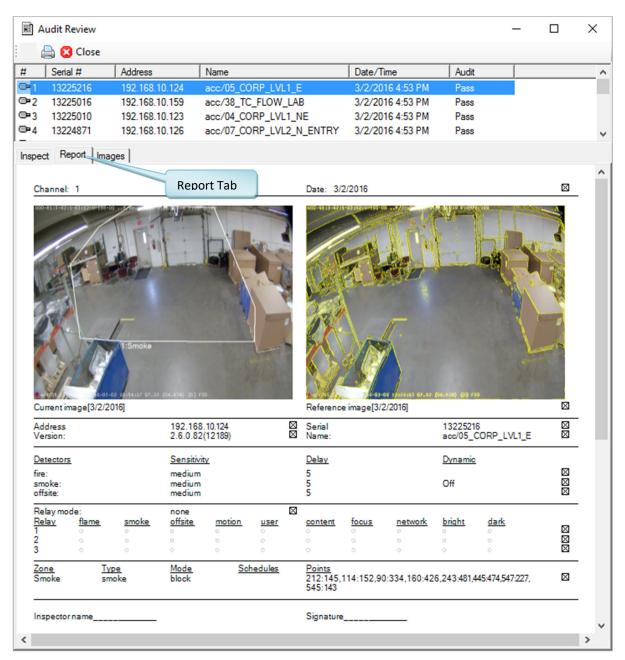The print button 🖶 enables you to print a copy of the report.

Figure 62: Audit Report Printout

IMAGES TAB

The Images tab [Figure 63] allows you to compare the previously recorded image to the current camera image to ensure that the camera's field of view has not changed.
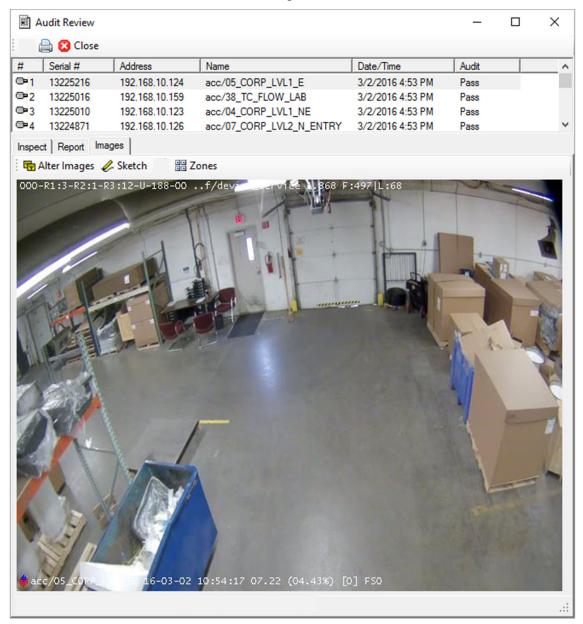

Figure 63: Comparing Camera Images in Audit Review

ALTER IMAGES

If the audit review detects a difference between the saved audit image and the current image, the software will rapidly switch between the images to allow you to determine the difference between the two images. If no difference is detected, this feature will be greyed out.

SKETCH MODE

Generates a black and white sketch of the camera images for comparison.

SHOW ZONES

Displays any zone boundaries assigned to the camera.

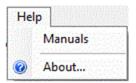## Review..

Opens a saved audit report for review.

HELP MENU

Figure 64: Help Menu

Manuals

Manuals are available at www.fike.com.

About…

Displays a splash screen indicating the firmware version of the software.

MAIN WINDOW TABS

The working area of the main window consists of five tab-selectable views [Figure 65]. Each tab view performs a specific function of the system.
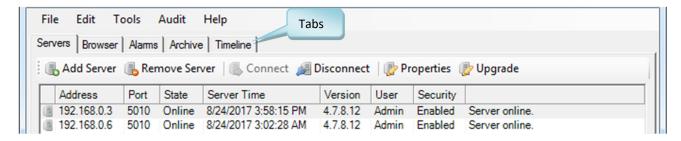

Figure 65: Main Window Tabs

SERVERS TAB

The *Servers* tab [Figure 66] allows you to manage FSM-IP servers and their respective channels (cameras). The screen is broken into two main sections: servers on the top and channels on the bottom. The channels displayed in the channels section are always the channels connected to the currently selected Server.
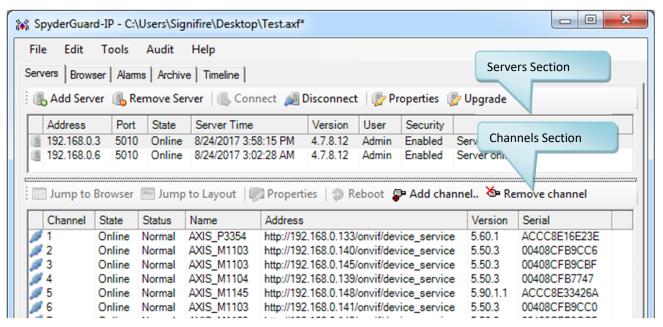

Figure 66: Servers Tab

Servers Section

Displays all of the servers currently connected to the VMS monitoring station. The *Servers* section [Figure 67] includes a server toolbar and a server list.
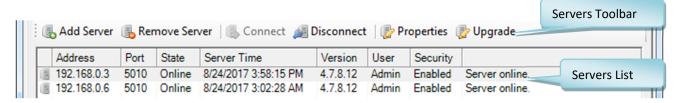

Figure 67: Servers Section

SERVERS TOOLBAR

The server toolbar [Figure 68] allows you to perform functions associated with configuring an FSM-IP server for operation with the Spyder*Guard*-IP software. Once a server is added to the Spyder*Guard*-IP configuration, it will be displayed in the server list.

Figure 68: Servers Toolbar

ADD SERVER

Adds a new server to the current VMS configuration or switches a server between *Guard* or *Administrator* mode. When clicked, the *Server Editor* dialog box [Figure 69] will be displayed, enabling you to enter the parameters for the new Server. If server security is enabled, a password must be entered to save changes made in the *Server Editor*.
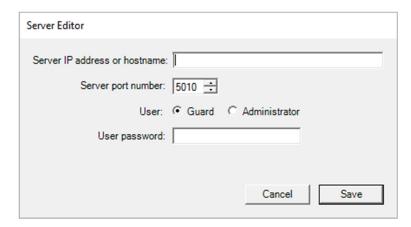

Figure 69: Server Editor

Server IP address or hostname	Enter either the IP address of the Server or its accessible DNS hostname.
Server port number	Enter the server's port number; the default port number is 5010 and should not be changed in most cases. You must ensure that a firewall does not block this port number on the computer running the server software.
User	Select the user access level you want to use to connect to the Server. The Server has two security profiles: Guard and Administrator. Guard mode does not allow editing of server or channel properties. User must be set to Administrator to perform necessary system configuration.
User password	The server is configured with security access turned off by default, so the password field will be blank. You can connect to the Server using either profile without the password being required. If security is enabled, you must enter the correct password for the profile you want to use.

Once *Save* is selected, the new Server will be added to the server list [Figure 70]. The server list displays the following details for each Server that is added to the VMS monitoring station. If the VMS application cannot connect to a server, the error message *Invalid IP or host name* will appear. Verify the address and connectivity to the Server to potentially resolve the situation.
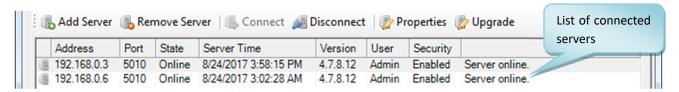

Figure 70: Server List Information

Address	Displays the IP address or hostname of the Server
Port	Displays the network port number of the Server
State	Displays the status of the Server (online or offline)
Server Time	Displays the local time and date on the Server
Version	Displays the current firmware version of the Server
User	Displays the current security access level the VMS application is using (Administrator or Guard)
Security	Displays if security (password protected) is enabled on the Server
	Displays the status of the Server (Server online or Server offline)

REMOVE SERVER   Remove Server

Removes the selected Server from the current VMS configuration.

CONNECT   Connect

Connects the VMS monitoring station to the selected Server.

DISCONNECT

Disconnects the selected Server and its associated channels from the VMS monitoring station.

PROPERTIES

Allows you to configure the different aspects of the selected Server. It is essential to understand that all the server properties are stored on the Server and not in the current VMS configuration. Any changes to the server properties will be immediately saved on the Server: however, enabling security will not force existing clients to authenticate. You will need to restart the Server or force all clients to reconnect.

The *Server Properties* dialog box is divided into two tabs, *Security* and *Licensing*, that allow you to set properties associated with the Server.

SECURITY TAB

The *Security* tab [Figure 71] is used to enable and disable server security.

Figure 71: Server Properties Security Tab

Enable server security	Check-box is used to enable or disable server security. You must enter and confirm a password for the guard and admin profiles if you enable security.
Show Passwords	Check-box forces the VMS application to display the security passwords versus hiding them. This feature enables an admin to recover the security password in the event it is forgotten. This feature has no bearing on server security.
Guard Account	Used to set and enter the Guard Account password.
Administrator Account	Used to set and enter the Administrator Account password.

LICENSING TAB

The *Licensing* tab [Figure 72] displays the current licensing key and shows the number of channels that can be connected to the Server under the current license.
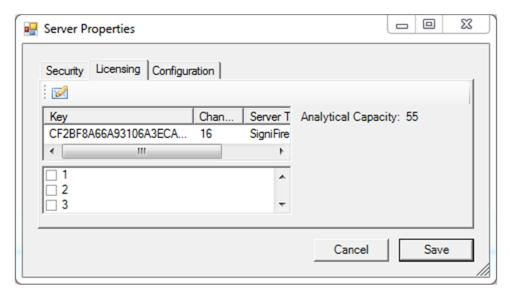

Figure 72: Server Properties Licensing Tab

Each Server is licensed for a certain number of channels. To expand the channel capacity of the Server, a new license must be purchased from the factory and uploaded into the Server using the *Upgrade* button.

CONFIGURATION TAB

The *Configuration* tab [Figure 73] is used to enable and disable the *Object Recognition* feature for the Server. By default, *Object Recognition* is disabled. Refer to page 19 for a description of the *Object Recognition* feature.
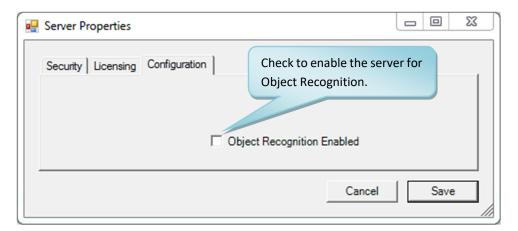

Figure 73: Server Properties Configuration Tab

Note: Customer acknowledges and agrees that activation of the Video Management System (VMS) Object Recognition Feature is at the customer's sole discretion. Object recognition is optimal for smoke generated by smoldering fires. A rapid rise of concentrated, high volume smoke may result in delayed recognition of such a hazard by the VMS when the object recognition feature is in use.

UPGRADE   Upgrade

Allows you to update the current license on the Server. Requires entry of a product key issued by Fike. Selecting and then right-clicking on a server in the list will open a *Server* menu [Figure 74] for that Server. The server menu allows you to perform most of the same functions found on the *Servers* toolbar with one added feature, *Restart*, which is used to restart the selected Server.
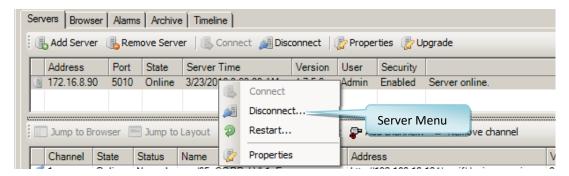

Figure 74: Server List Options

Channels Section

Displays all the channels (cameras) connected to the currently selected Server. The *Channels* section [Figure 75] includes a channel toolbar and a channel list.

Figure 75: Channel Section

CHANNEL TOOLBAR

The *Channel* toolbar [Figure 76] is used to perform functions associated with setting up a channel (camera) for operation with the VMS monitoring station. Once a camera is added to the configuration, it will be displayed in the channel list. When a server is shipped from the factory, it is not configured to connect to any cameras, so the channel list will be empty. Channels must be manually added using the *Add Channel* button on the toolbar.

Figure 76: Channel Toolbar

JUMP TO BROWSER

Becomes available once a channel is selected from the *Channel* list. Switches to the *Browser* tab [Figure 77] and displays the first camera in the *Organizational Tree* with this channel bound to it.
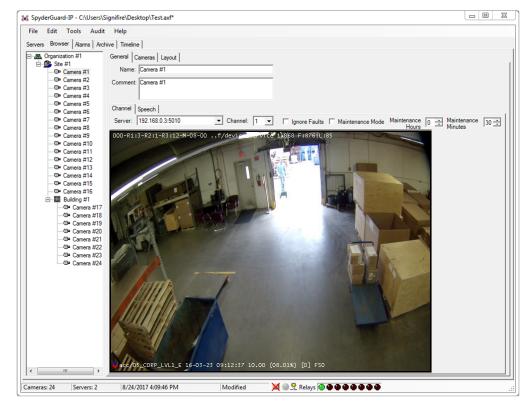

Figure 77: Browser Tab

JUMP TO LAYOUT   Jump to Layout

Becomes available once a channel is selected from the *Channel* list. Switches to the *Browser/Layout* tab [Figure 78] and displays the first item in the *Organizational Tree* with this channel as a child.

The background images used in the layout tab are custom-defined to suit each project. Any level of the *Organizational Tree*, except a camera, may be associated with a graphical layout such as floor plans, satellite photos, logos, etc., that can be viewed from the *Layout* tab.

If the selected *Organization Tree* element has camera objects as children, the image will be overlaid with iconic camera designators showing the general location of the cameras with respect to the background image. Otherwise, each child object will be highlighted by rectangles that define the area where the event is occurring.
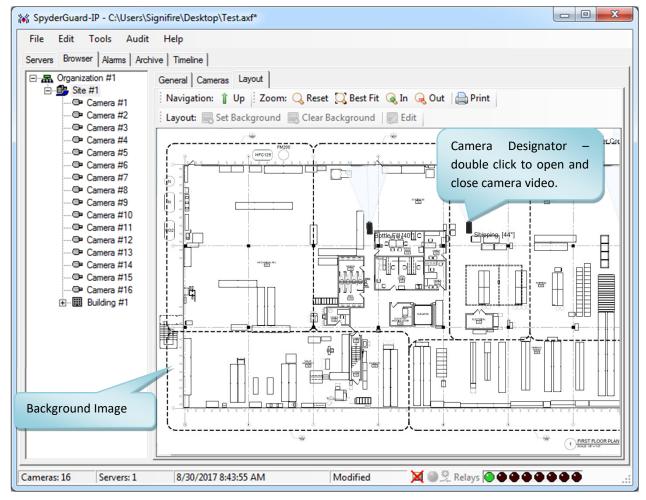

Figure 78: Browser/Layout Tab

PROPERTIES   Properties

Displays the *Channel Settings* dialog box for the selected channel. This dialog box can also be accessed through the **Edit>Properties** menu. Refer to Channel Settings on Page 18 for the features and functions available in the *Channel Settings* dialog box.

REBOOT   Reboot

Restarts the selected Fike Video Analytics IP camera. The reboot event will appear in the *Alarms* tab. Not applicable to ONVIF cameras.

ADD CHANNEL..

Displays the *Select Available Camera* dialog box [Figure 79], which can be used to add channels to the VMS configuration. The dialog box has two sub-tabs that allow you to either add Fike Video Analytics IP or Generic (ONVIF) cameras to the configuration.

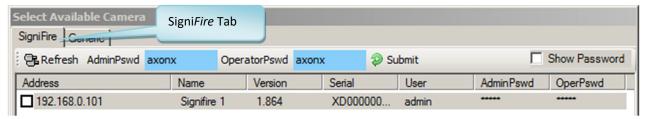### ADDING FIKE VIDEO ANALYTICS IP CAMERAS

Figure 79: Adding Fike Video Analytics cameras to the Video Analytics Software configuration

REFRESH LIST

Refreshes the list of available cameras that can be added to the configuration.

ADMINPSWD

Enter the Admin password for the camera.

OPERATORPSWD

Enter the Operator password for the camera.

SUBMIT

Applies the user entered credentials and refreshes the list of available cameras.

SHOW PASSWORD ☑

Shows the camera passwords in the list of available cameras when checked.

ADDING GENERIC (ONVIF) CAMERAS

Select the camera(s) that you would like the Server to connect to. Multiple cameras can be selected and added. Click "OK" to close the dialog box.
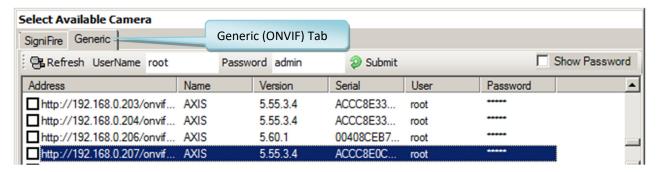

Figure 80: Adding Generic ONVIF cameras to the VMS configuration

Refresh	Refreshes the list of available cameras that can be added to the configuration.
UserName	Enter the camera user name.
Password	Enter the camera password.
Submit	Applies the user entered credentials and refreshes the list of available cameras.
Show Password	Shows the camera passwords in the list of available cameras.

CHANNEL LIST

After closing, the Server will disconnect and reconnect within a matter of a few seconds, and the newly added channels will be listed in the *Channel* list [Figure 81]. The list displays the following details for each channel that has been added to the Server.
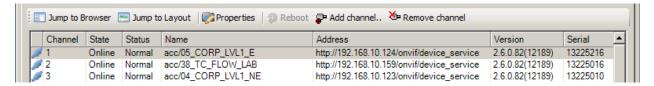

Figure 81: Channel List

Channel	Displays the unique channel ID assigned to the camera by the Server
State	Displays the status of the camera (online or offline)
Status	Displays the alarm status of the camera
Name	Displays the unique name assigned to the camera
Address	Displays the IP address of the camera
Version	Displays the firmware version running on the camera
Serial	Displays the serial number of the camera

CHANNEL MENU

Selecting and then right-clicking on a channel in the list will open a *Channel* menu [Figure 82] for that channel. The *Channel* menu is used to perform most of the same functions found on the *Channels* toolbar with one additional function added: *Force alarm in channel*.
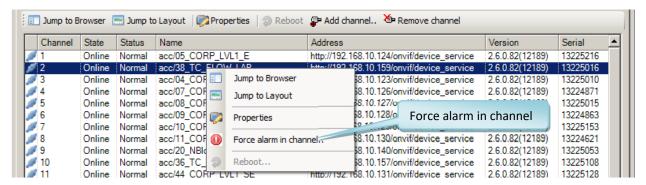

Figure 82: Server List Menu Options

Force alarm in channel can be used to manually cause a specific event type in the selected channel. This is useful for functionally testing the client software Alarm activity, including the Annunciator LED and Wise relay if connected. Also, functionality testing of the FVA-IP camera's dry relay contacts and the fire alarm control panel's signaling line circuit. When selected, the Invoke *Alarm* dialog box will appear [Figure 83].

To force an event to occur, you must first select the kind of alarm event you want to initiate and the duration (how long) that the event should remain active (10 to 180 seconds). Select OK to invoke the event. The event will appear in the *Alarms* tab and be highlighted and logged as the selected event type in the timeline for the set duration plus an additional 15 seconds.
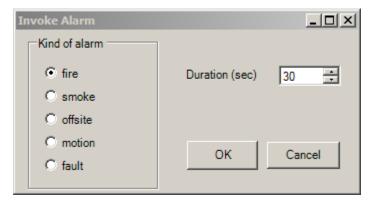
Figure 83: Invoke Alarm dialog box

REMOVE CHANNEL

Used to remove the selected channel or channels from the *Channel* list. The Select Channel dialog box [Figure 84] will appear. Select the channels from the list that you wish to remove; then click "OK" to remove the selected channels.
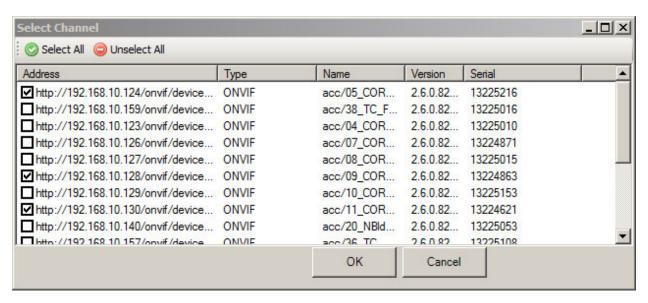

Figure 84: Removing a channel from the Channel list

BROWSER TAB

The *Browser* tab [Figure 85] is used to model the organizational structure of the system. Depending upon the complexity and size of the facility, a complete organizational structure can have multiple sites, with each having multiple buildings, floors, suites, and cameras. The minimum organization structure required for video monitoring operation should consist of ***Organization > Site > Cameras***.
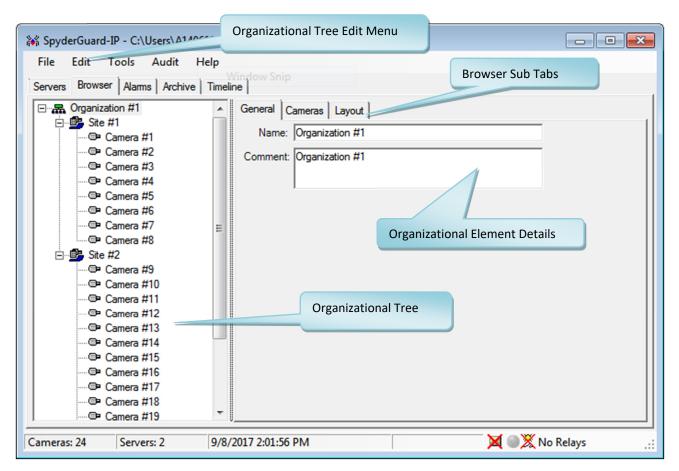
Figure 85: Browser Tab

Elements can be added to the *Organizational Tree* by using either the *Edit* menu located on the main toolbar or right-clicking anywhere within the *Organizational Tree* window to display the same *Edit* menu [Figure 86].
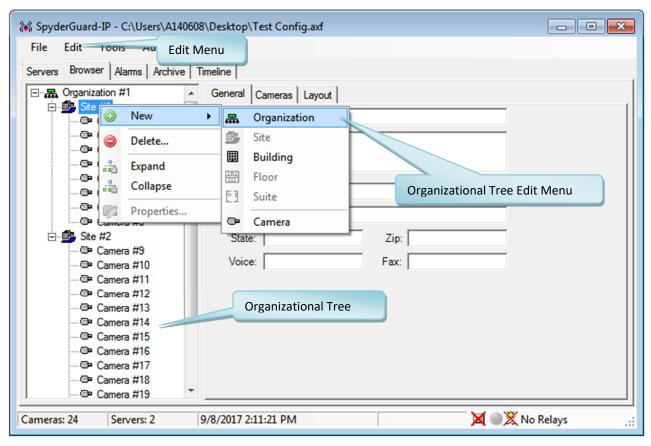
Figure 86: Adding elements to the Organizational Tree

Once the *Organizational Tree* is set up, it can be used to navigate the organizational hierarchy providing quick access to cameras and floor plans.

The *Browser* tab has three sub-tabs: *General, Cameras*, and *Layout*. Each tab provides content that is used to set up the elements of the *Organizational Tree*. The content of each tab varies depending upon the selected *Organizational Tree* element. Refer to the *Edit* menu on Page 13. Each element in the *Organizational Tree*, except for cameras, may be associated with a graphic such as floor plans, satellite photos, logos, etc. Cameras elements will only show the video image associated with the camera.

General Sub Tab

The *General* sub-tab [Figure 87] allows you to view and edit certain features of the selected organizational element. Each element in the *Organizational Tree* has different information associated with it that can be customized. Refer to Page 13 for details concerning adding elements to the *Organizational Tree*.

If the organizational element is a camera, two additional configuration sub-tabs become available under the *General* sub-tab: *Channel* and *Speech*.

CHANNEL SUB TAB

The *Channel* sub-tab [Figure 87] allows you to initiate several functions associated with the channel selected in the organizational tree.
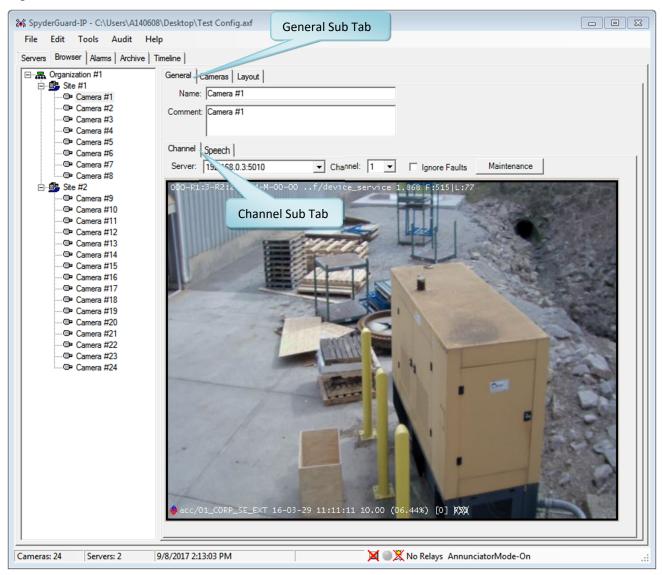
Figure 87: Channel Sub Tab

SERVER/CHANNEL

Displays the currently selected camera channel and the Server it is connected to.

IGNORE FAULTS

This feature allows you to set the selected channel to ignore faults due to Low Lumens (low light) in the camera view. When selected, the VMS application will NOT display faults caused by Low Lumens in the Browser or Alarms tab.

MAINTENANCE MODE

This feature allows you to put the selected channel (ONVIF cameras only) in maintenance mode for a specified period of time. When selected, the *Maintenance Setup* form [Figure 88] will be displayed, allowing you to set up and initiate the maintenance mode on the selected camera.
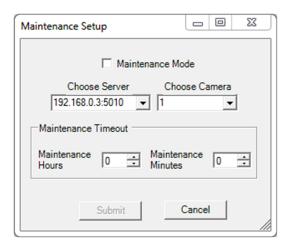
Figure 88: Maintenance Setup Form

Maintenance Mode	Enables maintenance mode on the selected channel (ONVIF cameras only).
Choose Server	Allows you to choose the Server.
Choose Camera	Allows you to choose the camera.
Maintenance Timeout	Allows you to set the length of the maintenance timeout in hours and minutes.
Submit	Begins a maintenance timeout event on the selected channel. The icon for the chosen camera in the organizational tree will change to a flashing maintenance mode icon 🔧 to provide a positive indication that the camera is in maintenance mode. After the timer expires, the camera will automatically return to normal operation.
Cancel	Exits the Maintenance Setup screen.

Note: This feature is used to prevent the camera from responding to nuisance smoke alarms. While in maintenance mode, the camera will respond to all other system events.

Right-clicking on the camera image will bring up a *Channel* menu [Figure 89] that provides additional camera functions.
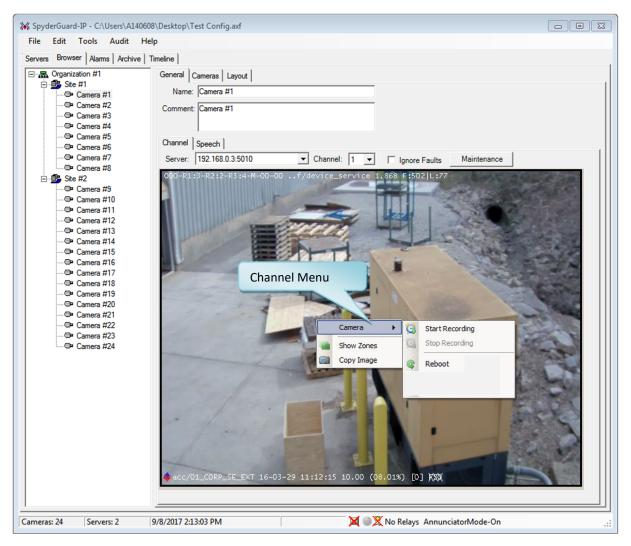

Figure 89: Channel Menu Options

CAMERA (CHANNEL MENU)

Allows you to initiate the following functions associated with the selected camera.

Start Recording	Begins a User event on the selected channel
Stop Recording	Ends a User event on the selected channel
Reboot	Reboots the camera

SHOW ZONES

When active, the video image will display any defined zones associated with the channel [Figure 90].
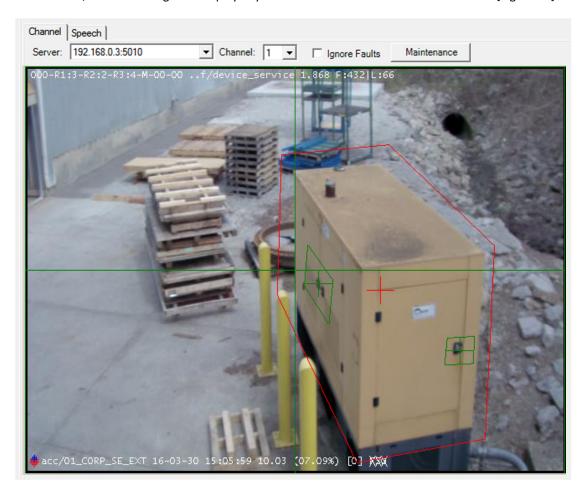
Figure 90: Images Shown on channel image

COPY IMAGE

Allows you to copy and paste the current channel image into another program.

SPEECH SUB TAB

The *Speech* sub-tab [Figure 91] allows you to change the voice settings associated with the selected channel. By default, all alarms are announced through the speech system. Each channel's settings are stored in the local configuration file.
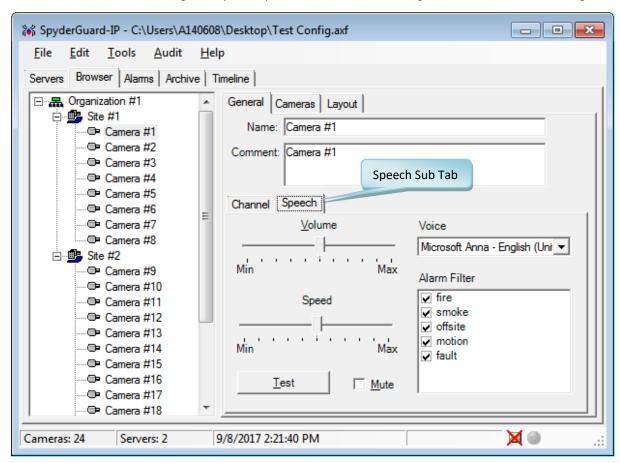
Figure 91: Speech Sub Tab

VOLUME (SLIDER)	Sets the speech volume level for the channel.
SPEED (SLIDER)	Sets the speech voice speed for the channel.
VOICE	Sets the speech voice that will be used by the channel (Uses Microsoft Windows text to speech files.)
ALARM FILTER	Sets which event types will have voice announcements made in response to the event being active.
TEST	Tests the voice configuration using the current settings.
MUTE ☑	Un-checking the "On" check-box will mute all voice announcements for the channel.

Cameras Sub Tab

The *Cameras* sub-tab [Figure 92] displays the cameras under the current *Organizational Tree* selection. Selecting an individual camera will display the image for that channel only. As shown below, selecting an item higher up in the Organizational Tree may display several cameras associated with the selection.

The Organizational Tree selection requires multiple camera images to be shown. The software allows you to adjust how many camera images will be displayed on the screen by adjusting the number of columns to display. The *Best Fit* button will adjust the current camera image to fill the viewing area.
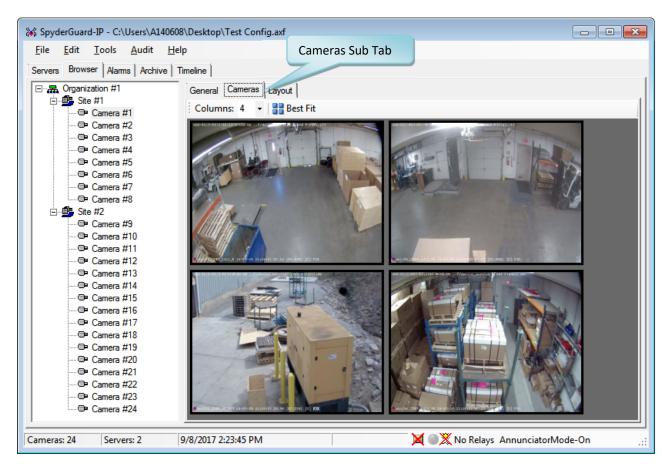
Figure 92: Cameras Views for Selected Organizational Tree Element

You can right-click on any of the camera images to access the *Channel* menu for the camera. Refer to Page 58 for a description of the menu functions. From this screen, you can also double-click on a camera image to view it in full-screen mode.

Layout Tab

Any element of the *Organization Tree,* except a camera, may have a graphical layout such as floor plans, satellite photos, logos, etc., associated with it that can be observed from the *Layout* tab [Figure 93]. The background images used in the *Layout* tab are custom-defined to suit each project. An example of a system layout is shown below.
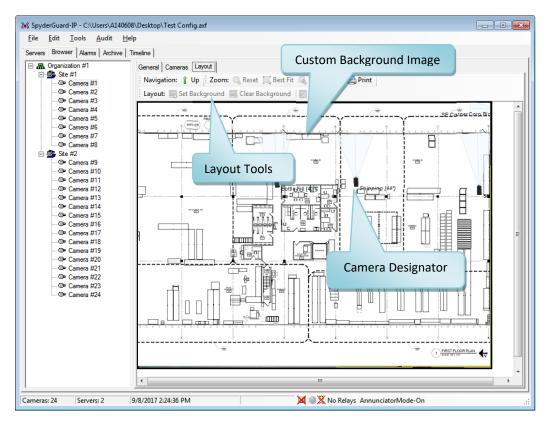

Figure 93: Layout View with Camera Designators

The *Layout* tab is equipped with several tools to customize the layout to suit the project.

UP ↑ Up - Moves up one level in the organizational tree unless the current selection is a root-level organization.

RESET Reset - Resets the layout to the default zoom level.

BEST FIT Best Fit - Attempts to perform a best-fit zoom of the layout.

IN In - Zooms in on the layout.

OUT Out - Zooms out on the layout.

PRINT Print - Prints the current layout.

SET BACKGROUND Set Background - Opens Windows Explorer, allowing you to select an image file as the background image for the select organizational element (jpg, gif, tif, png, and bmp file types).

CLEAR BACKGROUND Clear Background - Deletes the current background image for the selected organizational element.

EDIT Edit - Changes the layout view into Edit mode so organizational elements can be moved around and positioned over the background image.

CREATING A CUSTOM LAYOUT

After you have finished building the Organizational Tree, you can create the custom layouts for the tree elements. Each element in the tree (excluding cameras) will have predefined zones based on the hierarchy of the elements within the organizational tree. Cameras can be added to the following elements: sites, building, floors and suites. Each element in the *Organizational Tree*, except for cameras, may be associated with a graphic such as floor plans, satellite photos, logos, etc. Cameras elements will only show the video image associated with the camera. The minimum organization structure required should consist of **Organization > Site > Cameras**.

The following process should be used to customize the layouts for the organizational tree elements.

Step 1: With the appropriate element selected in the organizational tree and the *Layout* tab, click on the *Set Background* button. This will open Windows Explorer, allowing you to locate and select the image you would like to use for the layout background. Once you have chosen your background image, click *Open* to add the image to the layout. It is recommended that the size and image quality of the background file be suited to fit the size of the screen that VMS is running on.

Step 2: To maximize the background image, click *Best Fit* to resize the image to fit the viewing window. Click *Save* to set the size of the background image

Step 3: Elements that do not have cameras added will have one or more zone windows automatically overlaid onto the chosen background image. You can now adjust the positioning and size of the zone window for the selected element by clicking on the *Edit* button. Use the outside nodes to resize the zone window and use the center node to reposition the window. You can also move the element's name by selecting its node and repositioning the text. The zone name and zone window are tied together and will move as one.

Step 4: Elements with cameras added to them (i.e., sites, buildings, floors, and suites) will have camera icons automatically overlaid onto the chosen background image [Figure 88]. The camera icons can be repositioned using the element node to indicate their correct location and position with respect to the background image. The viewing angle and coverage area of the cameras can also be adjusted.
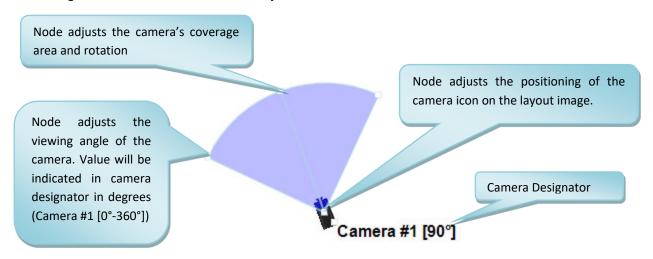

Figure 94: Typical Camera Icon Showing Nodes

ALARMS TAB

The *Alarms* tab [Figure 95] displays active and inactive alarm events. Real-time video images of all active events will populate the video area of the *Alarms* tab. When detecting events, VMS can be set to automatically maximize the *Alarms* tab window if minimized or bring the *Alarms* tab forward if another screen is open. This allows you to start assessing the situation immediately. By default, the alarm view functionality is enabled during the system setup.
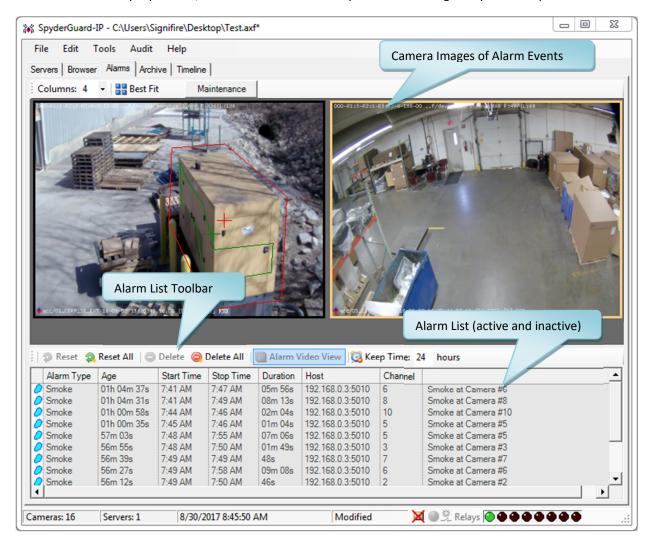

Figure 95: Alarms Tab

- **Maintenance Mode (ONVIF cameras only)**

  The *Maintenance* button, shown in Figure 95, allows you to put the selected channel in maintenance mode for a specified period of time. When selected, the *Maintenance Setup* form [Figure 81] will be displayed, allowing you to set up and initiate the maintenance mode on the selected camera.

Note: This feature is used to disable a camera when maintenance is being performed in the area the camera serves to prevent false smoke alarms. While in maintenance mode, the camera will respond to all other system events.

The alarm list toolbar has a row of action buttons that lets you handle the alarm events. The toolbar includes the following actions.

RESET 🔁 - Resets the image analysis algorithms of the selected channel. This action is useful for clearing smoke alarm events. Reset does not affect an active flame alarm. Also, resets any active Fike Video Analytics IP camera relays or Wise relays configured for this camera. There will be a 15-second delay resetting the Wise relay after a camera reset.

RESET ALL 🔁 - Resets all active events in the list. Same effect as above, but applies to all active events.

DELETE ⊖ - Deletes the selected event from the alarm list if it has been completed.

DELETE ALL ⊖- Deletes all completed events from the active alarm list.

ALARM VIDEO VIEW 🔲 - Switches view to Alarms tab whenever an event is activated. Note that the optional annunciator will only work if this feature is enabled.

KEEP TIME ⏰ - Sets the amount of time to keep closed alarm events in Alarm view. Note that all events in the database will be visible in Archive and Timeline view.

Alarm Details

Each time VMS registers an event, a line item will be added to the alarm list [Figure 96]. The events are ordered by age, with the oldest events at the top and the newest at the bottom. While the conditions continue that caused the alarm, the alarm is in an active state indicated by the "*In progress"* message in the *Stop time* column [Figure 96]. Once the alarm condition is no longer present, the alarm becomes inactive.
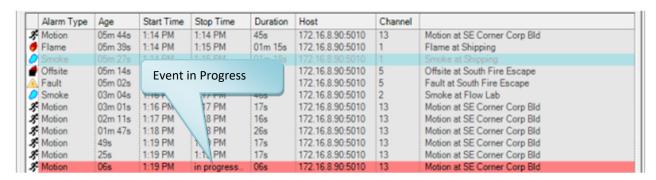
Figure 96: Alarm List Details

Alarm Type	Event type associated with the alarm
Age	Time since the alarm started
Start Time	Local time when the event started
Stop Time	Local time when the event ended
Duration	How long the event remained active
Host	IP address of the Server where the alarm originated
Channel	Channel number that the event originated from
Comment	Description of the event

After the alarm event becomes inactive, the video recordings of the event can be deleted or played back. To playback the event, right-click the event in the alarm list and select *Play Event* [Figure 97]. To remove inactive alarms from the list, you can use the *Delete* or *Delete All* buttons in the alarm list toolbar or right-click the event in the alarm list and select *Delete*. Removing inactive alarms does not remove them from the NVR storage. Older alarms still can be observed in the *Archive* and *Timeline* tabs.
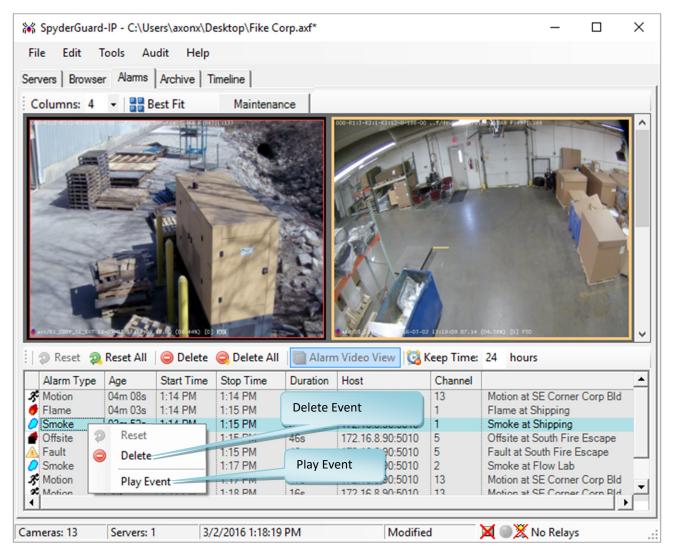
Figure 97: Event Playback

Reading the Camera Image

Two informational lines are superimposed onto each camera image [Figure 98].

Figure 98: Reading Camera View Image

The information line located at the top of the image provides the following information:

000-	Indicates the state of the Fike Video Analytics IP cameras integral relays (1-3). 0 = relay in normal state and 1 = relay is in alarm state
R1:-R2:-R3:-	Event codes for each camera relay (1-3). The event codes indicate what condition is required for the relay to close. Event codes are: 1-Flame 2-Smoke 3-Offsite 4-Motion 5-User 6-External (not used) 7-Dark 8-Bright 9-Featureless (content) 0-Focus A-Network **Example**: R3:24, shown in Figure 92, indicates that relay three will engage on smoke and motion.
A-159-00	Relay countdown display **Example:** A-159-00, shown in Figure 92, means Automatic countdown, 159-second delay, and the countdown state.
10.0.0.174	IP address of the camera
00:1B:5A:00:00:97	MAC address of the camera
1.868	Firmware version of the camera
801	Image quality of the camera
1	Number of connections
38	Camera illumination (lux)

The information line located at the bottom of the image provides the following information:

Warehouse_Camera_1	Name of the camera.
14-08-26	Current date (Y/MM/DD)
09:06:27	Current time
15:18	Camera Frame Rate
(58:00%)	CPU Usage
[18]	Cycle Process Time (milliseconds)
FSO	Active Algorithm Indicator. If any of these detection algorithms have been turned off, you will see an "X" over the corresponding letter. F = flame; S = smoke; O = offsite; H = system enabled for object recognition[1]; h = selected camera enabled for object recognition[1]
38	Camera illumination (lux)

[1] These indicators will only show if object recognition is enabled for the system.

Optional Annunciator

An optional annunciator [Figure 99] can be added to the VMS system. The annunciator plugs into an available USB port on the VMS monitoring PC to indicate system alarm events as follows.

Flashing Green – The event has been acknowledged but is still recording the event. Once the event is no longer in progress, the light will turn off.

Flashing Red – Alarm event is active, and the Alarm dialog box is displayed on the Alarms tab screen.

Note: The annunciator will only work if the *Alarm Video View* feature is enabled in the Alarms tab. See page 66.
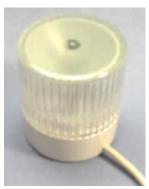
Figure 99: Annunciator

Once the annunciator is plugged into the PC's USB port, VMS will provide a positive indication in the status bar at the bottom of the Main Window that the software recognizes that the annunciator is attached [Figure 100].

Figure 100: Annunciator Attached Indicator

With Annunciator Mode on, VMS will display an *Alarms* dialog box [Figure 101] on the *Alarms* tab in response to an alarm event. The dialog box will indicate the event type and the assigned name given to the channel (camera) in the *Organizational Tree*.

Figure 101: Alarm Notification and Response Dialog Box

Minimize Spyder*Guard*-IP	Allows you to minimize the VMS application window.
Silence Alarms for _ mins	Allows you to silence the active alarm events shown in the Alarm dialog box for a set number of minutes (1 to 100 min.).
Acknowledge	Allows you to confirm that the event has been acknowledged. The annunciator will flash green.

ARCHIVE TAB

The *Archive* tab [Figure 102] provides search functionality for finding past events and their associated video recordings. The records can be played, downloaded, or saved. Here the list of events can be generated according to set search criteria. Once the filter settings for the search criteria are set up, selecting the *Search* button will produce a list of events that satisfy previously set criteria. Now you may choose a particular alarm of interest and playback the video recording made at the time when it occurred.
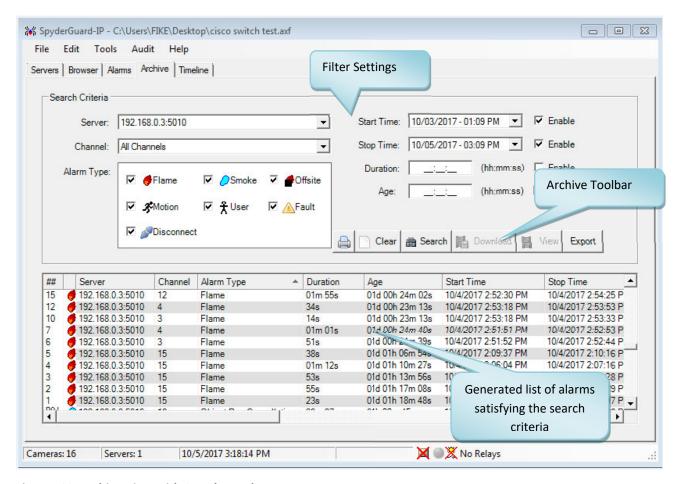
Figure 102: Archive View with Search Results

The following quick-search parameters are provided to filter the alarms in the list.

Server

The Server to search by; defaults to all servers.

Channel

The channel to search by; defaults to all channels.

Alarm Type

The alarm type to search by; defaults to all alarm types.

Start Time

The start time to filter results by; defaults to include all alarms started within the last 24 hours. This search option can be enabled or disabled (enabled by default).

Stop Time

The stop time to filter results by. This search option can be enabled or disabled (disabled by default).

Duration

The duration to filter results by. Duration is the length of time the alarm was active. This search option can be enabled or disabled (disabled by default).

Age

The age to filter results by. The age is how old the alarm is. This search option can be enabled or disabled (disabled by default).

Events meeting the search criteria will be displayed in the search results list [Figure 103].
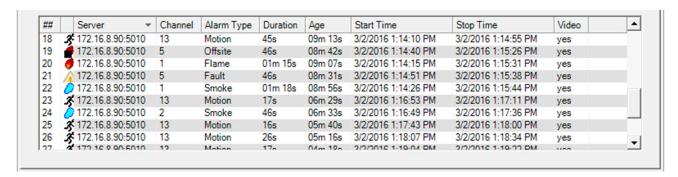
Figure 103: Archive Search Results List

Server	IP address or hostname and port number of the FSM-IP Server where the alarm data is stored.
Channel	Channel number the alarm occurred on.
Alarm Type	Type of alarm that occurred.
Duration	How long the alarm lasted.
Age	Time passed since the beginning of the alarm.
Start Time	Date and time when the alarm started.
Stop Time	Date and time when the alarm stopped.
Video	Alarm has an associated video

Selecting and then right-clicking on an individual event in the list will display a menu that allows you to perform additional functions associated with the selected event [Figure 104].
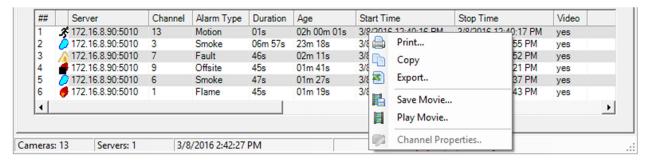
Figure 104: Single Event Options

PRINT...	Prints the current search results list
COPY	Copies the search list results (txt format)
EXPORT..	Exports the current search results list to a CSV file.
SAVE MOVIE...	Saves the selected event movie as an AXONX media file (*.axm) or Windows Media file (*.wmv)
PLAY MOVIE..	Plays the selected event movie using VLC Media Player
CHANNEL PROPERTIES	Not accessible in guard mode

ARCHIVE TOOLBAR

Figure 105: Archive Toolbar

Print

Prints the list of generated events

Clear

Clears the event list

Search

Initiates a search criterion using selected search criteria

Download

Allows you to download the video file associated with the selected event onto your local machine. The system will prompt you for the VMS video file (AXM or WMV) and will download and save the file. Once saved, the software will give you the option to play the video now.

View

Allows you to playback any selected event that has a video using VLC Media Player. To use the media player, simply click the View button.

Export

Exports a list of all system events included in the search criteria.

Video Player

The video player [Figure 106] streams the archived videos from the NVR and displays them on the screen.
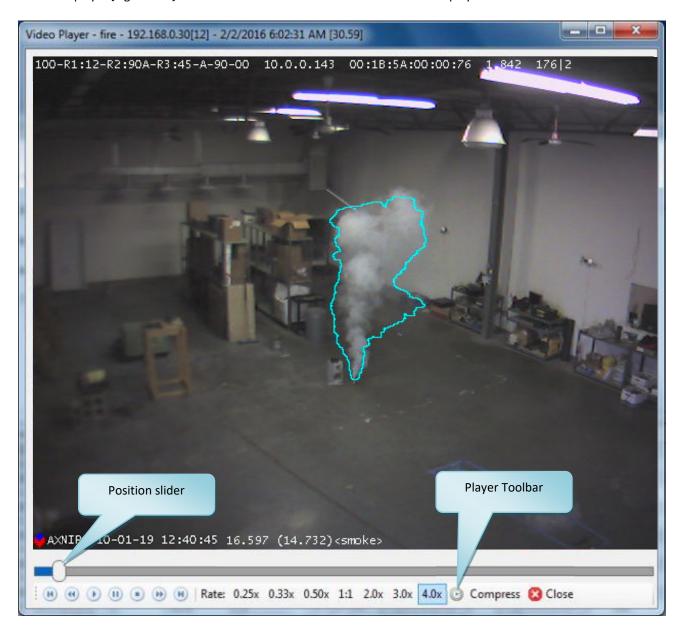
Figure 106: Video Player Window Layout

The video player provides several features that allow you to control how the video is played, including a position slider that enables you to select any point in the video to begin playback, along with a toolbar that provides the following functions.

⏮	**Skip Backward**	Skips one frame backward
⏪	**Step Backward**	Steps one frame backward
▶	**Play**	Plays the video
⏸	**Pause**	Pauses the video
⏹	**Stop**	Stops the video; resets playback position to zero
⏩	**Step Forward**	Steps one frame forward
⏭	**Skip Forward**	Skips one frame forward
	Rate:	Rate settings allow you to increase or decrease the general playback speed.
🔄 Compress	**Compress**	Compression allows you to filter out the long-time sections from the video where only idle frames were recorded.
❌ Close	**Close**	Closes the video player.

TIMELINE TAB

The *Timeline* tab [Figure 107] allows you to review the events and video recordings stored in the archive in a Gantt chart showing the alarm events in each channel of the selected NVR server. In addition to viewing video recordings of alarms, with the timeline, you can see video recordings from any channel and at any point in time within the capacity of the NVR.
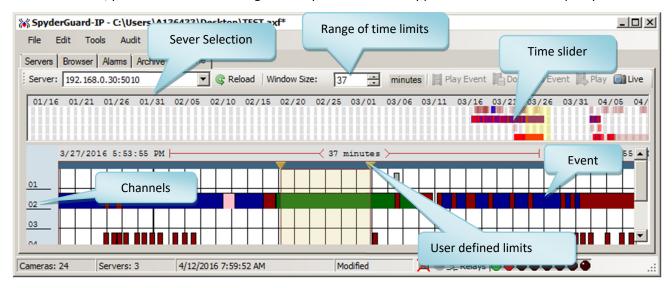
Figure 107: Timeline Window

Before *Timeline* can display the events, you need to select the Server. Choose the Server from the list of all available online servers in the Server selector. VMS will respond by filling up the channel bars indicating events that took place on each particular channel within the selected time window. Each horizontal bar represents a specific channel. The time window default value is 30 minutes but can be altered by selecting an alternative value in the *Window size* selector. The starting time position of the timeline window is controlled by sliding the timeline bar. By default, the timeline display is positioned to cover a range up until the last event. At any time, the display can be refreshed by clicking the *Reload* button.

Events Display

Events are displayed as color-coded horizontal bars with the following colors representing the different types of events:

Flame events	red
Smoke events	blue
Offsite events (RFL)	purple
Motion events	green
User events	orange
Fault events	yellow
Disconnect events	grey

In addition, Tool-tips will provide extensive information on each event when the mouse pointer is hovering over the event bar [Figure 108].
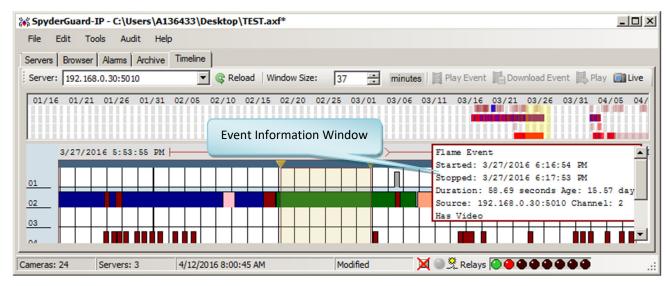
Figure 108: Timeline Window Tool-tips

Playing Back Events

To playback or download an event, right-click on the event and select the appropriate option [Figure 109]: *Play Event Movie..*; *Download Event Movie*.
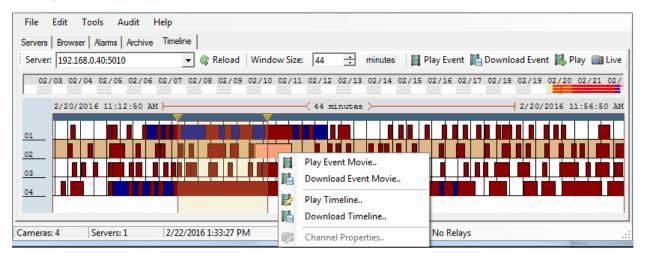
Figure 109: Playing or Downloading Single Alarm Events

Playing Back Arbitrary Time Ranges

Timeline view [Figure 110] allows you to set arbitrary time limits and playback the video recorded from any channel. To set up the time limits, drag the inverted rectangles (orange) located at the top edge of the timeline diagram as desired, select the channel *View* in the *Selected Time* group. You can then right-click the channel within the selected time limits and choose "*Play Timeline..*" or "*Download Timeline..*".
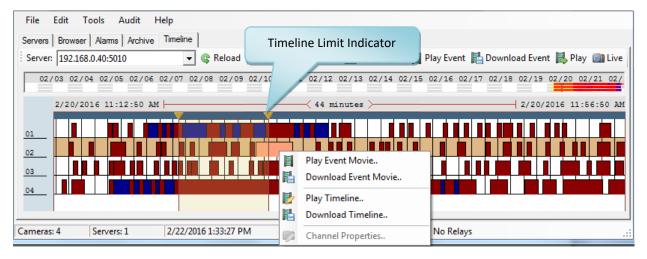
Figure 110: Timeline Chart of activities with guard defined time range set

TESTING, MAINTENANCE, AND SERVICE

Fike factory-trained service technicians shall only conduct testing, Maintenance, and Service of the Fike Video Analytics system in accordance with published instructions. Any attempt to test, maintain or service the system using untrained personnel may achieve undesired and invalid results, leading to improper operation of the system.

INDEX OF FIGURES

This page intentionally left blank.

REVISION HISTORY

Revision	Date	Description
0	04/16	New Release (Version 4.7.5.0)
1	10/16	New Release (Version 4.7.7.0)
2	11/17	Revised to reflect software changes (Version 5.0.0.0) and removal of all references to Signi*Fire* and Spyder*Guard*.
3	2/18	Revised to include Object Recognition configuration settings.
4	9/18	Revised to reflect software V5.0.1.0.
5	3/19	Updated email agents per latest release of SpyderGuard.
6	6/19	Removed all references to software version.
7	8/21	Added note to page 69 indicating that the LED annunciator will only work if the *Alarm Video View* feature is enabled in the Alarms tab.
8	4/22	Added Watchdog feature to Relay Switchboard… on page 31.

Fike®

Video Analytics Corporation

CONTACT US

Fike Video Analytics Corporation
704 SW 10th Street
Blue Springs, Missouri 64015 USA
Tel: +001 844-345-3843

For a list of contact information for Fike offices around the world, visit the Global Locations section of Fike.com