

Video Analytics

Version 4

Reference Guide

Reference Guide

Revisions

Issue	Date	Revisions
A	09/09	New document.
B	09/10	Updated for V4.7 software release; added additional Honeywell IP cameras support; added Alarm Suspension Rules functionality to Chapter 13 ; replaced inside/outside zones with counting line for people counting (Figure 6-8 , Figure 6-12 , Figure 6-16 , Figure 6-20); added Appendix C, Active Alert Performance Counter .

Contents

About This Document	19
Overview of Contents	20
Related Documents	21
An Important Note on Operating Conditions	21
Before Running the Software	21
Typographical Conventions	22
1 Introduction	23
System Overview	23
Software Features	26
Product Packages	28
Backward Compatibility	30
Software Installation	32
2 Operating Conditions and Camera Setup	33
Selecting the Appropriate Camera	33
Understanding Operating Conditions	35
Managing Environmental Conditions	37
Excluding a Zone of Irrelevant Motion in a Scene	37
Reflective Surfaces	38
Motion of Doors and Gates	39
Motion of Trees or Foliage	40
Object Size Filtering	40
3 User Management	41
Setting Up User Accounts and Permissions	41
Adding or Deleting Users	43
Changing Permissions for Existing Users	44
Changing a Password	45
4 Configuration Basics	47
Using the Configuration Tool	47
Launching the Configuration Tool	47
Configuration Tool Menu Bar	48
Navigating the Configuration Tool	48
Setting Up Video Inputs	49
Types of Video Sources	50
Adding Video Sources	52
Adding a Video Source from a Fusion DVR	54
Changing Properties of a Video Source	55
Deleting a Video Source	56
Uploading the Configuration to a Server	56
Product Licenses	57
Updating the License Key	57

Channel Setup: Configuring Each Channel	58
Selecting a Video Channel	59
Setting Up the Scene	59
Scene with People	60
Scene with Cars	61
Overhead Counting	62
High Sensitivity	62
Zone Definition	63
Zoom Tooltip	65
Defining a Restricted Zone	66
Defining a Direction Zone	66
Defining a Trespass Line	67
Defining a Sterile Zone	67
Defining Inside and Outside Zones for Car Counting	68
Defining Car Lane Counter	69
Defining a U-Turn Zone	71
Defining a Target Zone	72
Comparing an Image Zone to a Ground Zone	73
Customizing the Events	74
Adding an Event Associated to a Zone	74
Adding a Event for the Entire Scene	75
Editing an Event	75
Alarm Threshold Control	76
Camera Tamper Detection	76
Configuring Tamper Detection	77
Adjusting Tamper Detection Parameters	78
Uploading the Configuration to the Server	82
Uploading a Partial Configuration to the Server	82
Managing Your Configuration	83
Resolving Configuration Conflicts	84
5 Premium Event Configuration	85
Object Left Unattended and Object Removed Events	85
Conditions for Deploying Premium Events	85
Configuring an Object Left Unattended Event	86
Configuring an Object Removed Event	89
Possible Theft	91
6 Overhead People Counting	95
Deploying Environment Requirements—Single Camera	95
Positioning Overhead Camera—Single Camera	97
Verifying the Camera Placement	98
Verifying the Camera Position	99
Verifying the Floor Coverage	99
Configuring Door Threshold and Door Span Scene Objects	100
Ignoring Door Movement	101
Using Object-Block Zone	101
Using an Exclusion Zone	102
Configuring Counting Line	103
Configuring Inside and Outside Zones	106
Inside and Outside Zones—Object-Block Zone at a Door	107
Using Inside and Outside Zones With an Exclusion Zone	110
Verifying Placement of All Zones	112
Setting Up Zone-Based People Counting Events	113
Counter Reset Schedule	114
Wide-Entrance People Counting	114
Special Requirements	115

- Field Testing and Tuning Procedure 116
 - Scene Object Adjustment 117
 - Zone Adjustment 118
- 7 Camera Groups 119**
 - Counting Data by Camera Groups 119
 - Using Camera Groups for Wide Entrance People Counting. 119
 - Configuring a Camera Group 120
 - Adding a Camera Group 121
 - Editing a Camera Group 122
 - Deleting a Camera Group 123
 - Uploading the New Configuration to a Server 124
- 8 Camera Calibration 125**
 - Calibration Targets 125
 - Selecting a Camera Pair to Calibrate. 127
 - Adding a Pair of Calibration Points 128
 - Modifying a Pair of Calibration Points 129
 - Deleting a Pair of Calibration Points 129
 - Saving Mapping 130
 - Deleting Calibrated Camera Views. 131
 - Sending Changes to the Server 131
- 9 System Configuration 133**
 - Setting A Default Alarm Threshold 134
 - Counter Reset Schedule 134
 - Entering the License Key 135
 - Changing Database Properties. 136
- 10 Live Monitoring Station 137**
 - Logging On to Live Monitoring 137
 - Using the Live Monitoring Station 138
 - Reset Scene Changed Alarm. 144
 - Event Display and Threshold Settings 147
 - Image Display. 148
- 11 Forensics Tool 149**
 - Logging On to the Server 149
 - Starting a Search 151
 - Viewing the Latest Alarm/Event, Object, or Frame Search Results 152
 - Retrieving Alarms and Events 153
 - Viewing an Event Key Frame 153
 - Viewing an Object Trajectory in Alarm/Event Retrieval. 154
 - Adding a Comment to Alarm or Event 154
 - Retrieving Objects 155
 - Viewing an Object Snapshot and Object Trajectory 155
 - Retrieving the Event History for a Particular Object 156
 - Adding a Comment to an Object in Object Retrieval. 157
 - Retrieving Frames 158
 - Viewing Frames. 158
- 12 Reporting Tool 159**
 - Reports Generator 161
 - Configuring Reports Generator. 161
 - Report Examples 166
 - Reports Scheduler 168

Using the Reports Scheduler	169
Reports Health Monitor	176
Using the Reports Health Monitor	176
13 Alarm Management	179
Alarm Management Overview	179
Alarm Watch Admin	182
Logging On to Alarm Watch Admin	182
Connection Time-out Due to Inactivity	183
Configuring Alarm Watch Admin	184
Managing Video Analytics Servers	185
Adding an Analytics Server	185
Managing Alarm Acknowledgement States	189
Managing Alarm Suspension Rules	192
Filtering the Alarm Suspension Rules List	194
Adding an Alarm Suspension Rule	195
Modifying an Alarm Suspension Rule	204
Enabling or Disabling Alarm Suspension Rules	204
Deleting an Alarm Suspension Rule	204
Viewing the Scope of an Alarm Suspension Rule	205
Refreshing the Alarm Suspension Rule Display	205
Managing the Holiday and Exception Date Lists	206
Adding a Holiday or Exception List	207
Modifying a Holiday or Exception List	209
Deleting Holiday or Exception Lists	209
Managing Schedules	209
Adding a Schedule	210
Modifying a Schedule	212
Deleting Schedules	212
Managing AMS User Accounts	213
AMS System Configuration	215
Alarm Watch Station	216
Logging On to Alarm Watch Station	217
Alarm Watch Station Menu Bar	219
Configuring the Alarm Watch Station	220
Alarm Watch Station Status	222
Alarm Watch Station — Alarm Suspension Rules	222
Receiving the Latest Alarm	223
The Alarm List	225
Viewing and Modifying Alarm Status	226
Acknowledging an Alarm	228
Assigning an Alarm Classification	229
Modifying an Alarm Acknowledgement State	229
Adding an Alarm Comment	230
Defining Alarm Filters	231
Alarm Watch Station Startup	233
Alarm Backfill	234
14 Alarm Watch	237
User Administration	238
Using Alarm Watch Manager	240
Configuring Servers	241
Configuring Clients	243
Validating the Configuration	245
Confirming the Software Copyright and Version	245
Alarm Watch Email Client	246
Alarm Watch MCC Relay Client	250

Alarm Watch Health Monitor	252
Appendix A Event Library	257
Object Motion Events	259
Object Entered	259
Object Exited	259
Object Entered Restricted Zone	260
Object Exited Restricted Zone	260
Object Started Moving	260
Object Stopped	261
Object Started Moving in the Wrong Direction	261
Object Stopped Moving in the Wrong Direction	262
Object Trespassing	262
Object in Sterile Zone	263
Objects Merged	263
Objects Split	264
Objects Left Unattended	264
Objects Removed	264
People Events	265
Person Entered Restricted Zone	265
Person Exited Restricted Zone	265
Person Loitering in Restricted Zone	266
Person Started Moving in the Wrong Direction	266
Person Stopped Moving in the Wrong Direction	267
Person Trespassing	267
Person in Sterile Zone	268
Person Started Running	268
Person Stopped Running	269
Person Running in the Wrong Direction	269
Person on Fence Line	270
People Converged	270
People Passed By	270
Possible Theft	271
Person Entered Target Zone	271
Person Staying in Target Zone	272
Traffic Events	272
Car Started Driving in the Wrong Direction	272
Car Stopped Driving in the Wrong Direction	273
Car Entered Restricted Area	273
Car Exited Restricted Area	273
Car Parked in Restricted Area	274
Car Trespassing	274
Car in Sterile Zone	275
Car Made an Illegal U-Turn	275
Car Parked in Handicapped Zone	275
Car Pulled Off the Road	276
Car Needs Assistance	276
Car Speeding	277
Counting Events	277
Person Counted as Entering	277
Person Counted as Exiting	278
Car Entered Lot	279
Car Exited Lot	280
Car Counted in Lane	280
Video Events	281
Video Lost	281
Video Restored	282

Appendix B	Zone Library	.283
	Zones for Managing Information	284
	Exclusion Zone	284
	Object-Block Zone	284
	Zones for Enabling Specific Events	285
	Restricted Zone	285
	Direction Zone	285
	Trespass Line	286
	Fence Zone	286
	Sterile Zone	287
	Counting Line	287
	Inside and Outside Zones	288
	Car Lane Counter	288
	Detection Zone	289
	Asset Zone	289
	U-turn Zone	290
	Handicapped Zone	290
	Shoulder Zone	291
	Theft Zone	291
	Target Zone	292
Appendix C	Active Alert Performance Counter	.293
	Using PerfMon to View Active Alert Performance Counters	294
	Generating Performance Counter Logs	298
Appendix D	Solutions	.305
	License Messages	306
	Video Setup Messages	307
	Camera Group and Calibration Messages	308
	Configuration and Network Messages	308
	Scene Object, Zone, and Event Messages	312
	Overhead View Settings	314
	User Configuration Messages	315
	System Level Messages	316
	Live Monitoring Station Messages	317
	Forensics Tool Messages	319
	Reports Generator Messages	319
	Reports Scheduler Messages	320
	Reports Health Monitor Messages	322
	Alarm Management Messages	322
	Technical Support	330
Index		331

Figures

Figure 1-1	Honeywell Video Analytics Software	25
Figure 2-1	An Exclusion Zone	38
Figure 2-2	An Object-Blocking Zone	39
Figure 3-1	Server Login Dialog	42
Figure 3-2	Main Dialog	42
Figure 3-3	Add User Dialog Box.	44
Figure 3-4	Delete User (Logged On As) Message	44
Figure 3-5	Change Password Dialog	45
Figure 4-1	Server Login	47
Figure 4-2	Configuration Tool–File Menu	49
Figure 4-3	Configuration Tool Main Screen–Video Setup Page	50
Figure 4-4	Add Analog Sources.	52
Figure 4-5	Video Source Properties–Add Live Analog Input	53
Figure 4-6	Video Source Properties–Add Axis IP Live Video.	53
Figure 4-7	Fusion Server Properties	54
Figure 4-8	Fusion DVR Camera Selection	55
Figure 4-9	Configuration Uploaded Confirmation.	57
Figure 4-10	Channel Setup Page.	58
Figure 4-11	Scene Setup–Specifying Expected Object Types	60
Figure 4-12	Scene Setup Examples	61
Figure 4-13	High Sensitivity Setting	63
Figure 4-14	Zone Definitions–Restricted Zone.	65
Figure 4-15	Zone Definitions–Directional Zone	66
Figure 4-16	Zone Definitions–Trespass Line.	67
Figure 4-17	Zone Definitions—Sterile Zone	68
Figure 4-18	Define Inside and Outside Zones in a Parking Lot	69
Figure 4-19	Exclude Traffic in the Opposite Direction	70
Figure 4-20	Define Car Lane Counters	71
Figure 4-21	Define a U-turn Zone.	72
Figure 4-22	Define a Target Zone	73
Figure 4-23	Add an Event.	74
Figure 4-24	Modify an Event	75
Figure 4-25	Tamper Detection	77
Figure 4-26	Enable Camera Tamper Detection	78
Figure 4-27	Tamper Detection Thresholds	79

Figures

Figure 4-28	Blinding—Example of Partial and Total Blinding	79
Figure 4-29	Blurring—Example	80
Figure 4-30	Scene Change—Example	81
Figure 4-31	Configuration Changed Notification	84
Figure 4-32	Configuration Conflicts Message	84
Figure 5-1	Setup of a Detection Zone for Object Left Unattended	87
Figure 5-2	Event Parameters for Object Left Unattended.	88
Figure 5-3	Alarm Screen for Object Left Unattended Event	89
Figure 5-4	Examples of Asset Zones to Detect Object Removed	90
Figure 5-5	Alarm Screen for Object Removed Event	91
Figure 5-6	Zone Definition - Theft Line	92
Figure 5-7	Event Parameters for Possible Theft Event	92
Figure 5-8	Alarm Screen for Possible Theft Event	93
Figure 6-1	Single, 3-Ft Door Opening Example.	98
Figure 6-2	Double, 6-Ft Door Opening Example	98
Figure 6-3	Overhead Camera Placement Verification—Red Box	99
Figure 6-4	Define the Door Threshold—Green Bar	100
Figure 6-5	Define a Door Span—Blue Bar and a Fixed Height Horizontal Bar.	101
Figure 6-6	Object-Block Zone Used to Filter Out Door Movement	102
Figure 6-7	Exclusion Zone Used to Mask Out Door Movement	103
Figure 6-8	Counting Line for People Counting	104
Figure 6-9	Counting Line - Add or Delete a Joint	105
Figure 6-10	Line-Based People Counting Events	106
Figure 6-11	Message Reconfiguration	107
Figure 6-12	Define an Inside Zone—Door to a Meeting Room	107
Figure 6-13	Outside Zone—Placed at the West Side of a Corridor	108
Figure 6-14	Outside Zone Examples	109
Figure 6-15	View All Inside and Outside Zones	109
Figure 6-16	Define an Inside Zone—Door to a Meeting Room	110
Figure 6-17	Outside Zone—Added to the West Side of a Corridor	111
Figure 6-18	Outside Zone Examples	112
Figure 6-19	View All Zones	113
Figure 6-20	Add Person Counted as Entering Event.	114
Figure 6-21	Wide Entrance People Counting—Appropriate Camera Placement	116
Figure 7-1	Camera Group Initial Screen	120
Figure 7-2	Camera Group Properties Screen.	121
Figure 7-3	Assign Group Name in Properties Screen	121
Figure 7-4	Camera Groups with Assigned Cameras	122
Figure 7-5	Camera Group Properties Modifications	123
Figure 7-6	Camera Group Deletion Prompt.	123
Figure 8-1	Camera Group Selection	126
Figure 8-2	Camera Pair Calibration	127
Figure 8-3	Camera Group Calibration Point Example	129
Figure 8-4	Calibrated View With Eight Pairs of Calibration Points	130
Figure 8-5	Save Mapping	132

Figure 9-1	System Setup Configuration Parameters	133
Figure 9-2	Set Default Alarm Threshold	134
Figure 9-3	Schedule Counter Reset Time	135
Figure 9-4	Enter License Key	136
Figure 9-5	Database Properties	136
Figure 10-1	Server Login Dialog	137
Figure 10-2	Live Monitoring Station, Showing Areas of Interest	139
Figure 10-3	Alarm Display	142
Figure 10-4	Alarm View Window	144
Figure 10-5	Show Group Counts	144
Figure 10-6	Normal Camera View	145
Figure 10-7	Scene Change Alarm	146
Figure 10-8	Reset Scene Change Alarm	147
Figure 10-9	Event Key Frame	148
Figure 11-1	Server Login Dialog	150
Figure 11-2	Forensics Tool	151
Figure 11-3	Event Retrieval	154
Figure 11-4	Event Comment Dialog	155
Figure 11-5	Object Retrieval, Viewing Object Snapshot and Trajectory	156
Figure 11-6	Object and Associated Events Retrieval	157
Figure 11-7	Object Comment Dialog	157
Figure 11-8	Frame Retrieval	158
Figure 12-1	Reporting Tool Package	160
Figure 12-2	Server Login	161
Figure 12-3	Reports Generator File Menu	162
Figure 12-4	Reports Generator Main Screen	162
Figure 12-5	Cameras or Camera Groups Selection	164
Figure 12-6	Specify Report File Name	165
Figure 12-7	Generating Report	165
Figure 12-8	File Menu in Reports Generator	166
Figure 12-9	Sample Table Report	167
Figure 12-10	Sample Chart Report	168
Figure 12-11	Reports Scheduler Server Logon	169
Figure 12-12	Reports Scheduler Main Screen	170
Figure 12-13	Server Template Logon	171
Figure 12-14	Configure Report Template	171
Figure 12-15	Add an Existing Report Template	172
Figure 12-16	Set up Reporting Schedule	173
Figure 12-17	Apply Schedule Settings to the Selected Report Template	173
Figure 12-18	Warnings for Incomplete Settings	174
Figure 12-19	SMTP Configuration	175
Figure 12-20	Test SMTP Settings	175
Figure 12-21	SMTP Test Results	176
Figure 12-22	Reports Health Monitor Logon	176
Figure 12-23	Reports Health Monitor Main Screen	177

Figures

Figure 13-1	Alarm Management Server System Diagram	181
Figure 13-2	Alarm Watch Admin User Login	182
Figure 13-3	Alarm Watch Admin Initial Window	185
Figure 13-4	HVA Server Properties Dialog	186
Figure 13-5	Analytics Server Added to the List.	187
Figure 13-6	Deletion of an HVA Server From the List	188
Figure 13-7	Deleted HVA Servers Displayed	188
Figure 13-8	Alarm Suspension Rules Message	189
Figure 13-9	Alarm States Tab.	190
Figure 13-10	Alarm Acknowledgment State Properties Dialog	190
Figure 13-11	New Acknowledgement State Added	191
Figure 13-12	Alarm Suspension Rules Tab	192
Figure 13-13	Alarm Suspension Rule Wizard	196
Figure 13-14	Holidays/Exceptions Tab	206
Figure 13-15	Schedules Tab	210
Figure 13-16	Alarm Management Server Users Tab	214
Figure 13-17	AMS System Setup Tab	215
Figure 13-18	AMS Database Properties	216
Figure 13-19	Alarm Watch Station Login Dialog.	217
Figure 13-20	Alarm Watch Station Live Tab	219
Figure 13-21	Alarm Watch Station View Menu Options	220
Figure 13-22	Alarm Watch Station Configuration	220
Figure 13-23	Dismissed Alarms Prompt	222
Figure 13-24	Alarm Watch Station Status	222
Figure 13-25	Alarm Suspension Rules.	223
Figure 13-26	Latest Alarm	224
Figure 13-27	Alarm List	226
Figure 13-28	Selected Alarm.	227
Figure 13-29	Alarm Classification	229
Figure 13-30	Alarm Acknowledgement State	230
Figure 13-31	Alarm Comment	230
Figure 13-32	Alarm Filter	231
Figure 13-33	Acknowledgement Filter Criteria.	232
Figure 13-34	Alarm List with Filter Enabled	233
Figure 13-35	Alarm Start Fill	234
Figure 14-1	Alarm Watch Module.	237
Figure 14-2	Alarm Watch Login Dialog.	238
Figure 14-3	No Users Found Prompt Message	239
Figure 14-4	Password Confirmation Message	239
Figure 14-5	Password Confirmation Failed Error Message	239
Figure 14-6	Admin Added Successfully Message	239
Figure 14-7	Alarm Watch Manager Logon Error Message	239
Figure 14-8	Alarm Watch Manager Main Window	240
Figure 14-9	Alarm Watch Servers Tree View	241
Figure 14-10	Removal Confirmation Message.	241

Figure 14-11 New Server Configuration 242

Figure 14-12 Save Settings Changes 243

Figure 14-13 New Client Configuration 244

Figure 14-14 Server Error Messages 245

Figure 14-15 Help ► About Command 245

Figure 14-16 Localhost Directory in Alarm Watch Manager. 246

Figure 14-17 Clients Sub-Directory in Alarm Watch Manager. 246

Figure 14-18 E-mail Configuration Screen. 247

Figure 14-19 Sample Configuration 248

Figure 14-20 Test E-mail Success Message. 249

Figure 14-21 Test E-Mail Failure Message (Invalid SMTP Server) 249

Figure 14-22 Test E-mail 249

Figure 14-23 E-mail Status in Alarm Watch Health Monitor 250

Figure 14-24 Alarm Watch Manager with MCC Relay Client 251

Figure 14-25 Alarm Watch MCC Relay Client Selection. 252

Figure 14-26 Notification Area with Alarm Watch Health Monitor 252

Figure 14-27 Notification Area with Alarm Watch Health Monitor Alert 253

Figure 14-28 Alarm Watch Health Monitor Notification Icon Menu 253

Figure 14-29 Alarm Watch Health Monitor Main Screen 253

Figure 14-30 Alarm Watch Health Monitor Server Status 253

Figure 14-31 Alarm Watch Error Messages 254

Figure 14-32 Client Status Area 254

Figure 14-33 Client Errors 254

Figure 14-34 Help ► About Menu Command 255

Tables

Table 1-1	Video Analytics Software Applications	24
Table 1-2	Software Feature Set	26
Table 1-3	Product Packages	28
Table 1-4	Events Contained in Product Packages	29
Table 1-5	Software Compatibility Matrix.	30
Table 2-1	Operating Conditions	35
Table 2-2	Object Throughput During Peak Loading	37
Table 3-1	User Permission Types	43
Table 4-1	Video Source Properties	55
Table 4-2	Zone Types	63
Table 4-3	Zone Shapes	64
Table 4-4	Blind Threshold Values	80
Table 4-5	Blur Threshold Values	81
Table 4-6	Scene Change Threshold Values	82
Table 5-1	Premium Events Operating Conditions	86
Table 5-2	Object Left Unattended Event Parameters	88
Table 5-3	Possible Theft Event Parameters	92
Table 6-1	People Counting Environment Considerations—Single Camera	96
Table 6-2	People Counting Camera Placement Requirements.	97
Table 6-3	Common Specification for Camera Mounting and Lens	97
Table 6-4	Wide Entrance People Counting Requirements	115
Table 10-1	Server Status Options	140
Table 10-2	Display Format and Layout Options	140
Table 10-3	Alarm Display Options	143
Table 10-4	Image Display Options	148
Table 11-1	Search Field Definitions	151
Table 13-1	Alarm Watch Admin Tasks	184
Table 13-2	Alarm Suspension Rules Columns	193
Table 13-3	Time Specifier Tab Field Descriptions	196
Table 13-4	Holidays/Exceptions Tab Field Descriptions	206
Table 13-5	Add Holiday/Exception List Field Descriptions.	207
Table 13-6	Schedules Tab Field Descriptions	210
Table 13-7	Add Schedule Field Descriptions.	211
Table 13-8	Alarm Watch Station Configuration Field Descriptions.	221
Table 13-9	Alarm Watch Station Latest Alarm Field Descriptions	224

Tables

Table 14-1	Alarm Watch Package Modules	238
Table 14-2	Server Configuration Settings	242
Table 14-3	Client Configuration Settings	244
Table 14-4	Server Configuration Settings	247
Table A-1	Events Contained in Product Packages	257
Table D-1	License Message	306
Table D-2	Video Setup Messages	307
Table D-3	Camera Group and Calibration Messages	308
Table D-4	Configuration and Network Messages	308
Table D-5	Scene Object, Zone and Event Messages	312
Table D-6	Overhead View Settings Messages	314
Table D-7	User Configuration Messages	315
Table D-8	System Level Messages	316
Table D-9	Live Monitoring Station Message Troubleshooting	317
Table D-10	Forensics Tool Message Troubleshooting	319
Table D-11	Reports Generator Messages	319
Table D-12	Reports Scheduler Messages	320
Table D-13	Health Monitor Messages	322
Table D-14	Alarm Watch Admin Software Messages	322
Table D-15	Health Monitor Software Messages	329

About This Document

Honeywell Video Analytics is an intelligent software system that automates video surveillance tasks. The software can perform real-time surveillance tasks including the detection and tracking of moving objects, detection of specific events, and triggering alarms. The software also provides video indexing and retrieval capabilities that allow users to search for specific types of events or objects detected and stored by the system.

This guide describes in detail how to:

- Install the Video Analytics software
- Use the Configuration Tool to configure the software. You will be guided step-by-step, from preparing video input and camera placement to analytics configuration and system control.
- Use the Live Monitoring Station application to receive live video streams remotely with analytics annotations as well as real-time events and alarms across multiple Analytics servers
- Use the Reporting Tool to generate statistics reports from one or more server(s) at a remote location connected via the network
- Use the Forensics Tool to search and retrieve past incidents
- Use the add-on component Alarm Watch to set up e-mail alarm and relay output delivery mechanisms. Alarm Watch Station allows a security operator to receive real-time alarms from the Analytics servers with low bandwidth requirements.

This guide is written for system administrators and site managers alike who need in-depth knowledge on how to place cameras and configure the analytics software for their intended applications. The installation section is written for system integrators and engineers to prepare for proper deployment of hardware components for maximum system performance.

Overview of Contents

This document contains the following chapters and appendixes:

- [Chapter 1, Introduction](#), introduces the Honeywell Video Analytics software suite, and gives a functional overview of its components.
- [Chapter 2, Operating Conditions and Camera Setup](#), gives guidance on camera selection and the appropriate camera setup for your unique requirements.
- [Chapter 3, User Management](#), describes how to add or remove users and change user permissions and passwords.
- [Chapter 4, Configuration Basics](#), provides procedures for setting up the video input and channel configuration. It also describes how to upload the configuration to your server as well as ongoing configuration management.
- [Chapter 5, Premium Event Configuration](#), covers how to set up cameras and configure the events that are available in the Honeywell Video Analytics Premium package.
- [Chapter 6, Overhead People Counting](#), provides guidelines on overhead camera placement and describes how to properly configure zones for people counting events.
- [Chapter 7, Camera Groups](#), describes counting data by camera groups and explains how to configure camera groups for wide entrance people counting.
- [Chapter 8, Camera Calibration](#), covers how to calibrate adjacent cameras for wide entrance people counting.
- [Chapter 9, System Configuration](#), provides procedures for configuring system-wide settings.
- [Chapter 10, Live Monitoring Station](#), describes how to use this application for daily surveillance tasks.
- [Chapter 11, Forensics Tool](#), covers how to use this application remotely for search and retrieval of past incidents.
- [Chapter 12, Reporting Tool](#), explains the Reporting Tool software package and how to use it to generate statistics reports from a remote location.
- [Chapter 13, Alarm Management](#), covers this central station monitoring application that allows security operators to monitor real-time alarms from a large number of Video Analytics servers.
- [Chapter 14, Alarm Watch](#), describes how to use this add-on component to enable real-time alarm delivery mechanisms and to monitor alarm delivery activities.
- [Appendix A, Event Library](#), is a quick reference to all the events in the Honeywell Video Analytics software.
- [Appendix B, Zone Library](#), is a quick reference to all the zones in the Honeywell Video Analytics software.
- [Appendix C, Active Alert Performance Counter](#), covers the custom Active Alert performance counter objects that can be used to monitor the proper operation of the Video Analytics software.
- [Appendix D, Solutions](#), provides possible solutions for common system error messages.
- The [Index](#) is a quick reference to facilitate finding required information fast.

Related Documents

This document is a necessary prerequisite for understanding the Video Analytics software suite, and for using the Configuration Tool to set up security rules for various cameras monitored by the system. For more information on the software system, please refer to the following documents:

Document title	Part number	Description
<i>Video Analytics V4 Getting Started Guide</i>	800-00923	Covers the basic information for quickly setting up your system.
<i>Video Analytics V4 Installation Guide</i>	800-00294	Explains the hardware requirements for running the Video Analytics server and client applications. The Installation Guide also provides step-by-step instructions on how to install the entire software package.
<i>ReleaseNotes.txt</i>		For late-breaking information about this release, please see the <i>ReleaseNotes.txt</i> on the product CD.

An Important Note on Operating Conditions

This release of Honeywell Video Analytics software is intended for use in typical indoor or outdoor environments where stationary security cameras are placed.

Before Running the Software

To ensure a correct hardware configuration and optimal performance of the software, please see [Chapter 2, Operating Conditions and Camera Setup](#).

Typographical Conventions

This document uses the following typographical conventions:

Font	What it represents	Example
Helvetica	Keys on the keyboard	Press Ctrl+C
Lucida	Values of editable fields that are mentioned in the body text of the document for reference purposes, but do not need to be entered as part of a procedure	The Time from field can be set to Hours:Minutes:Seconds.
	Text strings displayed on the screen Syntax	The message Unauthorized displays. (object) entered
Swiss721 BT Bold	Words or characters that you must type. The word “enter” is used if you must type text and then press the Enter or Return key.	Enter the password .
	Menu titles and other items you select	Double-click Open from the File menu.
	Buttons you click to perform actions	Click Exit to close the program.
<i>Italic</i>	Placeholders: words that vary depending on the situation	<i>user name</i>
	Cross-reference to external source	Refer to the Video Analytics V4 Getting Started Guide .
	Cross-reference within document	See Introduction .

Introduction

Honeywell Video Analytics is an intelligent software system that automates video surveillance tasks. This release runs on Microsoft® Windows®-based platforms. The software is designed to make daily surveillance tasks effective and dependable by automating the detection of suspicious activities in video, triggering real-time alarms, and enabling fast search and retrieval for forensics purposes. It turns a conventionally passive and labor-intensive CCTV-based surveillance system into an active and cost-effective real-time video security system. As a result, the security operator can focus their attention on the relevant information and take timely actions instead of continuously watching the video display, which often leads to fatigue and boredom.

This chapter covers:

- An overview of the Honeywell Video Analytics software
- The various components in the software package—including the server and client modules—as well as the features each client application provides
- The product package components
- Backward compatibility information

System Overview

The Honeywell Video Analytics system is shown in *Figure 1-1*. The software system takes video inputs from multiple live cameras, analyzes the video content in real-time, and extracts relevant information in the video. The system includes analytics servers, which analyze the content of the video, and various client GUI applications that can connect to the analytics servers to perform specific management or monitoring tasks.

The applications can be launched either directly from the server or from a separate client personal computer (PC) that can access the server through a TCP connection. The five client applications included in the software suite are:

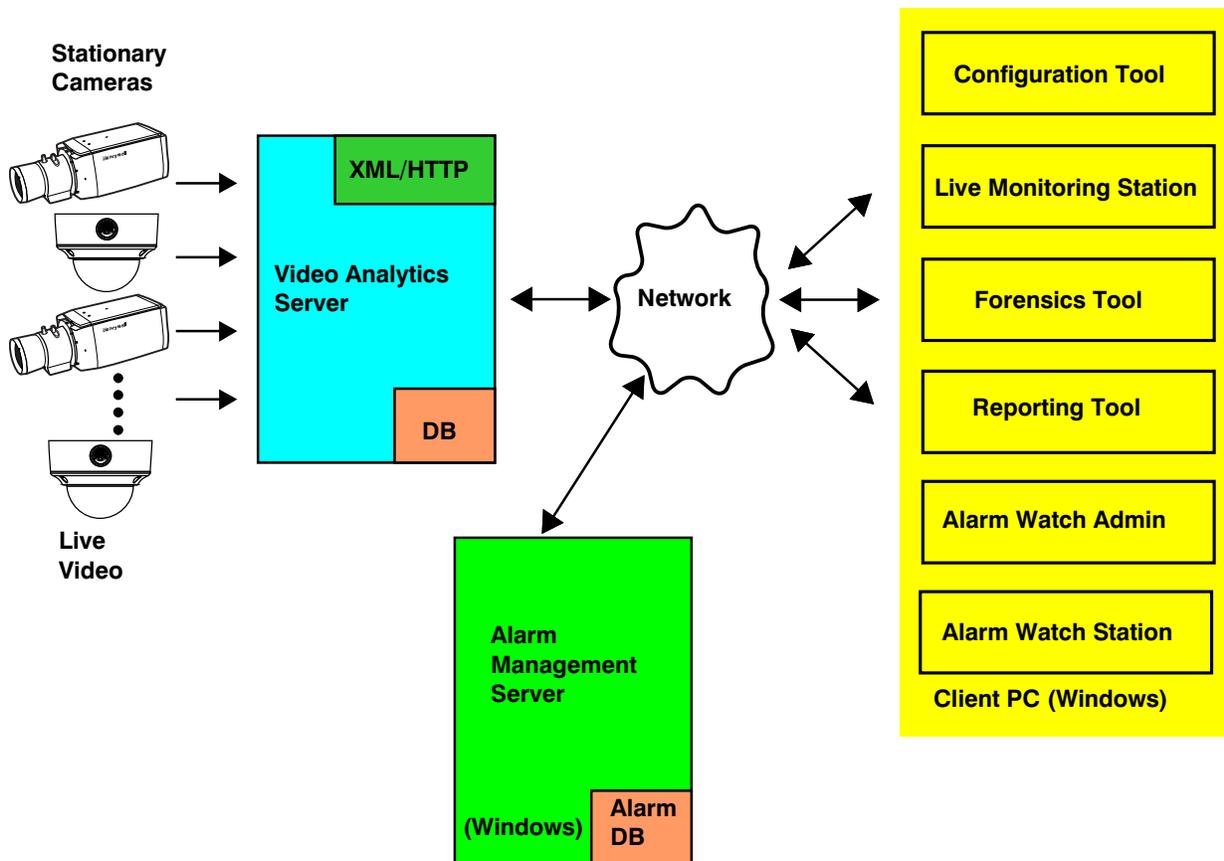
Table 1-1 Video Analytics Software Applications

Component	Description	For detailed information, see ...
Configuration Tool	<p>The Configuration Tool allows you to configure the specific types of events or alarms for the system to detect in each camera view. Correct camera placement and software configuration play a critical role for achieving optimal performance and obtaining the maximum benefits from the software. System administrators and site managers should refer to this guide for details on how to configure and use the software.</p>	<ul style="list-style-type: none"> • Chapter 2 to set up cameras for best analytical performance. • Chapter 3 to manage user access to the system. • Chapter 4 to configure video input and channel configuration. It also describes uploading the configuration to your server and ongoing configuration management. • Chapter 5 to set up cameras and configure the events. • Chapter 6 to place overhead camera placement and configure zones for people counting events. • Chapter 7 to configure camera groups for wide entrance people counting. • Chapter 8 to calibrate adjacent cameras for wide entrance people counting. • Chapter 9 to configure system-wide settings.
Live Monitoring Station	<p>Both the Live Monitoring Station and the Forensics Tool are essential for the security operator to effectively perform their daily surveillance tasks.</p> <p>As live video is being processed, moving objects in the camera view are identified and tracked and real-time events are reported. Using the Live Monitoring Station, you can view the live processing results from the connected servers, such as monitoring currently tracked objects and receiving all the detected events through on-screen display. Suspicious events and alarms are also reported instantaneously through visual and audio announcement.</p>	<p>Chapter 10 to learn how to set up your Live Monitoring Station client application to use for your daily surveillance tasks.</p>
Forensics Tool	<p>In addition, detected objects and events are stored in the database on the server for later review. The Forensics Tool provides an easy-to-use interface to retrieve relevant data from the database based on user defined query. You can specify the type of information, video channels, date and time ranges for the search, and explore the relationships between objects and events.</p>	<p>Chapter 11 to learn how to use the Forensics Tool client application to retrieve alarms, events, objects, and key frames stored in the Analytics server database.</p>

Table 1-1 Video Analytics Software Applications

Component	Description	For detailed information, see ...
Reporting Tool	The Reporting Tool provides statistics report generation for any of the events detected in the system, including counting data as well as surveillance types of events. You can configure the reporting template and also set up scheduled e-mail reporting.	Chapter 12 to generate statistics reports, and set up the Reports Scheduler and Reports Health Monitor applications.
Alarm Management	The Alarm Management component allows a security operator to monitor real-time alarms at a central station from multiple Video Analytics servers.	Chapter 13 to enable alarm monitoring and management across a large number of video analytics servers.
Alarm Watch	The Alarm Watch module is an add-on component that is included in the Video Analytics — Full package. This module enables additional alarm notification mechanisms, including e-mail alarm, and relay output for real-time alarm key frame monitoring for remote locations that lack broadband connection.	Chapter 14 to set up the Alarm Watch Manager and learn how to use the Alarm Watch Health Monitor for alarm delivery activities.

Figure 1-1 Honeywell Video Analytics Software



Software Features

Table 1-2 lists the new features in the current V4.7 release and the features in previous releases.

Table 1-2 Software Feature Set

Feature	Description
V4.7 New Features	
Alarm management	The new, dedicated, Alarm Management Server receives alarms from a large number of Video Analytics servers and stores the alarm data in a centralized database. With the next generation Alarm Watch Station client software, alarms can be classified and tagged with user-definable acknowledgement states. alarm views can also be shared by multiple operators to provide maximum operational efficiency and easy collaboration.
Localized package	Multi-lingual analytics server and alarm management server can support fully localized client applications running in English, French, Italian, Spanish, German, Dutch, and Japanese. The user can select the language of the client applications during installation.
Honeywell EQUIP™ Series camera interface	V4.7 allows the user to select Honeywell EQUIP Series of IP cameras as the video input. The supported models include Honeywell HD4DIP, HD3MDIP, HCD554IP, HCS554IP, and ACUIX™ digital PTZ dome (only in fixed position).
Line-based people counting	V4.7 allows the user to configure overhead people counting using a single multi-segmented counting line. This replaces the inside and outside zone pairs for an easier setup.
V4.7 New Features	
Greater product package flexibility	Product packages can be mixed and matched on a single server. The most appropriate product package can be assigned for each camera in the system, enabling the desired features for that camera. A combination of product packages can be selected to run on each analytics server to best address particular deployment needs.
Camera grouping and wide-door people counting	<ul style="list-style-type: none"> Cameras can be grouped to enable live counts display or counting report generation by group. Grouping overhead cameras at a single wide entrance extends people counting functionality with multiple cameras. These cameras are calibrated to avoid double counting in adjacent cameras. <p>Note Wide-Door People Counting is not currently available on video analytics for Honeywell Rapid Eye™ or Fusion DVRs.</p>
Camera detection	<ul style="list-style-type: none"> Detecting camera blinding, blurring or scene change to protect the camera from intentional or non-intentional act. Users can adjust the sensitivity of all three types of camera tamper detection independently on a per camera basis.
Alarm output to relay	Customizable relay hold time to interface to external devices.
Report generation	The Reporting Tool now allows you to generate statistics reports from camera groups.

Table 1-2 Software Feature Set

Feature	Description
Live monitoring	The Live Monitoring Station now allows you to display video from camera groups in real-time.
Fusion DVR interface	<p>This version of analytics software can use a Honeywell Fusion or Rapid Eye DVR as a video input source to provide live video to a separate analytics server, which then enables:</p> <ul style="list-style-type: none"> • Alarm video playback in the Forensics Tool client software • Events and alarms streaming to the DVR for viewing analytics results on the DVR. <p>Requires additional configuration on the DVR. Please refer to the <i>DVR Quick Scene Setup for Video Analytics</i> documentation that comes with your Fusion system.</p>
V4.3 and Earlier Features	
Video input	<ul style="list-style-type: none"> • Processing analog (NTSC or PAL) or compatible IP network video at 320 x 240 (CIF) or 160 x 120 (QCIF) resolution per channel. QCIF resolution is preferred for overhead people counting views. The number of video inputs that can be processed on each server depends on the server hardware configuration. • The incoming video frame rate for each channel must meet a minimum of 10 frames per second.
Object and Event detection	<ul style="list-style-type: none"> • Detected and tracked objects are classified into person, car, or small object, provided that a clear view of the object exists in the video. • Users can customize the list of events to be detected in each camera view, set the severity level for each event, and adjust the system alarm threshold. • Multiple zones of various types can be defined for each camera view. There is no limitation on the maximum number of zones per camera. • You can define multiple events for each camera view or multiples of the same type of event with different date/time conditions. There is no limit on the maximum number of events per camera.
Live monitoring	<ul style="list-style-type: none"> • Detected and tracked objects are highlighted on-screen in real-time as video is being processed. • Detected events are reported in real time, in an on-screen event log. • Events trigger real-time visual and audio (voice) alarms if the severity exceeds the alarm threshold. • Alarm video popup allows simultaneous key frame and live display of the camera view. • Live counts are displayed on screen in real-time as video is being processed.

Table 1-2 Software Feature Set

Feature	Description
Alarm delivery	<ul style="list-style-type: none"> • Offers real-time processing and delivers real-time alarms as they occur. • Displays real-time on-screen alarm image display. • Delivers audio and graphical alarms. • Customizable event settings and event severity levels for each individual channel. • Delivers e-mail alarm to user-specified list of recipients. • Offers add-on feature to provide relay output (Form A or Form C) to external devices or alarm panels.
Search and retrieval	<ul style="list-style-type: none"> • All object and event data are stored in a database for future retrieval. • To retrieve object and event data, you can provide queries based on object type, event type, alarm type, camera name, and time quantifiers. • For each retrieved object, the system can display the full path or trail of the object in the field of view, a representative snapshot of the object, and the history of events and interactions that involved this object. • For each retrieved event, the system links all the objects involved in this event, and displays key video frames captured at the time the event occurred. • Key frames allow a user to save significant time in finding relevant information during forensic investigation.
Report generation	<ul style="list-style-type: none"> • The Reporting Tool allows you to generate statistics reports by specifying: <ul style="list-style-type: none"> • Reporting period • Intervals • Events • Selected cameras • Reporting style: table or chart • Output format, including Text (to be imported to Excel spreadsheet), PDF, HTML • You can configure the tool to deliver scheduled e-mail reports on a daily or hourly basis.

Product Packages

Currently there are five product packages in the Honeywell Video Analytics offering:

Table 1-3 Product Packages

Product Package	Description
Active Alert Base	Basic, entry-level package of Active Alert.
Active Alert Standard	Full-featured, standard package that includes the widely deployable security features and traffic counting features.

Table 1-3 Product Packages

Product Package	Description
Active Alert Premium	Full-featured package that includes all the features in Active Alert Standard plus the premium features.
People Counting	Includes people counting features only.
Smart Impressions	Designed for traffic statistics data collection, this package includes all traffic counting features for people and vehicles.

This version of Honeywell Video Analytics software supports product package mix-and-match. Depending on the type of events to be detected in each camera, you can assign the product package that provides the required features for that camera. Each product package enables a list of analytics features (that is, events) included in each package. The event availability in each package is summarized in [Table 1-4](#). See [Appendix A](#) for more details on each event in the current event library.

Table 1-4 Events Contained in Product Packages

Event	Honeywell Video Analytics Package				
	Base	Standard	Premium	People Counting	Smart Impressions
People Events					
person entered restricted zone	X	X	X		
person exited restricted zone	X	X	X		
person loitering in restricted zone		X	X		
person started moving in wrong direction	X	X	X		
person stopped moving in wrong direction	X	X	X		
person on fence line		X	X		
person started running			X		
person stopped running			X		
people converged		X	X		
people passed by		X	X		
person trespassing - tripwire	X	X	X		
person running in wrong direction			X		
person in sterile zone		X	X		
Car Traffic Events					
car started moving in wrong direction	X	X	X		
car stopped moving in wrong direction	X	X	X		
car entered restricted zone	X	X	X		
car parked in restricted zone		X	X		
car speeding			X		
car made illegal u-turn		X	X		
car parked in handicapped zone		X	X		
car pulled off road		X	X		

Table 1-4 Events Contained in Product Packages

Event	Honeywell Video Analytics Package				
	Base	Standard	Premium	People Counting	Smart Impressions
car needs assistance		X	X		
car exited restricted zone	X	X	X		
car trespassing - tripwire	X	X	X		
car in sterile zone		X	X		
Video/Camera Events					
video signal lost	X	X	X	X	X
video signal restored	X	X	X	X	X
Counting Events					
person counted as entering		X	X	X	X
person counted as exiting		X	X	X	X
car entered lot		X	X		X
car exited lot		X	X		X
car counted in lane			X		X
Premium Events					
object left unattended			X		
object removed			X		
possible theft			X		
Smart Impressions					
entering target zone					X
staying in target zone					X

Backward Compatibility

Table 1-5 lists the current compatibility of Honeywell Video Analytics software versions.

Table 1-5 Software Compatibility Matrix

	HVA Server 4.2 (Stand-alone)	HVA Server 4.3 (Fusion DVM)	HVA Server 4.6 (Stand-alone, Rapid Eye, Fusion, DVM)	HVA Server 4.7 (Stand-alone, Rapid Eye, Fusion, DVM)
HVA Client 4.2 (Stand-alone)	✓	X	X	X
HVA Client 4.3 (Fusion, DVM)	✓	✓	X	X
HVA Client 4.6	✓	✓	✓	X

Table 1-5 Software Compatibility Matrix

	HVA Server 4.2 (Stand-alone)	HVA Server 4.3 (Fusion DVM)	HVA Server 4.6 (Stand-alone, Rapid Eye, Fusion, DVM)	HVA Server 4.7 (Stand-alone, Rapid Eye, Fusion, DVM)
HVA Client 4.7 (English)	✓	✓	✓	✓
HVA Client 4.7 (non-English)	✓ ^a	✓ ^a	✓ ^a	✓
Alarm Management Server 4.7	✓ ^b	✓ ^b	✓ ^{bc}	✓

Stand-alone: Server-based Video Analytics
 Fusion: Embedded Video Analytics running on a Honeywell Fusion DVR
 Rapid Eye: Embedded Video Analytics running on a Honeywell Rapid Eye DVR
 DVM: Video Analytics integrated with Honeywell Digital Video Manager

Note Wide-door people counting is not currently available on Rapid Eye or Fusion DVRs.

- ^a Partial; A mixed languages will appear on the GUI as HVA Server 4.2 (stand-alone), HVA Server 4.3 on Fusion and DVM, HVA Server 4.6 on all platforms are English only.
- ^b Backward compatibility (without alarm backfill) to HVA 4.2 and HVA 4.3 is only supported with Alarm Management Server up to V4.7.0.52. No backward compatibility to HVA 4.2 and 4.3 is supported with later versions of Alarm Management Server; therefore, HVA servers must be upgraded.
- ^c Backward compatibility to HVA 4.6 on Rapid Eye only works for Rapid Eye Multimedia V8.2.47 and later, and requires HVA clients V4.7.0.15 or later.

Note Backward compatibility between Alarm Management Server (AMS) and Rapid Eye requires the user to run Rapid Eye Admin to add the Rapid Eye unit to the list and run Rapid Eye View to enable access to this unit. The user can then run ActivEye User Configuration to add regular HVA users for AMS to connect to the analytics server.

For details on Rapid Eye Admin and View, please refer to the *Video Analytics Rapid Eye™ DVR Integration Application Note*.

For details on ActivEye User Configuration, see [Chapter 4](#).

Software Installation

You can install the Honeywell Video Analytics software on a PC with most Microsoft® Windows® operating systems. The software takes video inputs from various types of live camera inputs, including analog video through a frame grabber device and IP network video from network cameras.

Please refer to the [Video Analytics V4 Installation Guide](#). This guide contains:

- A list of all the system requirements for running Video Analytics server and client software
- Step-by-step procedure explaining how to install the Honeywell Video Analytics software
- The procedure for installing:
 - The 3rd party Euresys™ MultiCam™ driver
 - An optional add-on module on the server PC to provide relay output when an alarm occurs
 - Adobe Reader

Operating Conditions and Camera Setup

To ensure optimal performance, it is critical that you meet the operating conditions of the software, and set up cameras correctly. Please read this chapter carefully before proceeding to [Chapter 3](#).

The operating conditions closely follow those used for designing a video security system that does not include intelligent software. In a good, conventional video security design, careful consideration of the placement, direction, lens and type of camera is critical for the usefulness of the video produced.

This chapter covers:

- Selecting the appropriate camera
- Optimal system operating conditions
- Managing environmental conditions

Selecting the Appropriate Camera

The field of view (FOV) of the camera is one of the first key decisions during setup and installation. This determines whether the system can be used for Observation, Recognition or Identification.

Observation Systems

For Observation systems, the goal is to monitor the activities of each individual object to determine if an event has occurred. This could be a person entering either a room or an outdoor space that is restricted. This requires a wide area, mid to far range surveillance view for tracking the object's activities in the area.

Recognition Systems

For Recognition systems, the goal is to be able to recognize that person or object in the video, either by the surveillance personnel or automatically by the system. This requires the size of the object in the image to be relatively greater than in the Observation case.

Identification Systems

For Identification systems, the goal is to use the video images in a court of law to positively identify the person or object by either a jury member or the judge. The industry standard in the Identification case is that the head of the person or the entire object be at least 20% but not more than 95% of the image height.

The Honeywell Video Analytics software is designed for use only with Observation cameras to observe the motion and behavior of individual objects in the scene.

In addition to understanding the importance of the more conventional parameters of a video security system including lighting, camera placement and field of view, it is important to note that this version of Honeywell Video Analytics software works with stationary cameras. The incoming video frame rate for each channel must meet a minimum of 10 frames per second. The typical pan-tilt-zoom (PTZ) cameras found in many security installations cannot be used unless the camera is positioned correctly and the PTZ capabilities are not used during analysis.

Scene Type

Honeywell requires all Video Analytics software users to carefully consider the scene type found in the input images. Just as in the video produced for examination by human operators, the amount of traffic, the size of objects (as previously discussed), and the speed of objects must be taken into account when setting up the camera. For example, a crowded scene of many small, fast moving objects would defeat the ability of a human operator to detect an event. For similar reasons, the camera field of view for Honeywell Video Analytics must be examined and matched with operating conditions expected by the software.

Lighting Conditions

Proper lighting conditions are critical for successful outcome. When placing and directing a camera at a glass door or a wall containing one or more windows, you should assess the lighting conditions of both the room inside and the lighting environment outside.

For example, a camera aimed to include a window that faces due east produces images as the sun is rising that may include too much sunlight and wash out the indoor image. An auto-gain camera or a camera with a wide dynamic range may improve the overall image contrast in this case. If a washed out scene is presented to the Video Analytics software, someone entering the room in the morning may not be detected correctly due to an improper image contrast level falling outside the operational parameters of the system.

For use of Honeywell Video Analytics under low light (or night time) conditions, a minimum of 2 lux of illumination is required on all targets to be detected in the field of view.

Understanding Operating Conditions

To summarize, a conventional video security system depends on knowledge of:

- Field of view - includes distance to objects of interest and range of view.
- Goal: Observation, Recognition or Identification
- Camera placement and direction/aim
- Scene type
- Amount of traffic
- Occlusion level
- Size of objects relative to the entire image
- Speed of objects appearing in the image
- Lighting or contrast level examined during the entire period of use, which may be 24 hours per day
- Camera type: Stationary

With these terms in mind, we can now specify the required operating conditions for a video security system enabled by the Honeywell Video Analytics software. The system is expected to perform its intended automatic surveillance tasks and reach its optimal performance when the following operating conditions are met:

Table 2-1 Operating Conditions

Condition	Explanation
Occlusion level	No object is completely hidden from view by another object in the scene. In more specific terms: total occlusion of an object occurs (in a typical situation) less than 10% of the time and the duration of total occlusion does not exceed 5 seconds. Additionally, the average occlusion amount of a single object should not exceed 60% of its size.
Traffic amount	The scene involves low to medium traffic; that is, less than 30% of the field of view coverage.
Object size	Within the field of view, moving objects (normally people or vehicles) appear to have medium size in the image. The minimum object size requirement is 18 pixels for the software to detect and track the object. The object dimension (horizontal or vertical) range should be between 5% to 80% of the image width or height, as it moves around in the scene to ensure a continuous track of the object's movement. For best performance, object height should range between 20% to 40% of the height of the field of view.

Table 2-1 Operating Conditions

Condition	Explanation
Object speed or duration	To be detected, an object must appear for at least 10 consecutive frames of the video input. In addition, the speed of an object in the camera view must be such that the object appears in view for at least 2 seconds. If you find in your current camera setup that an object appears to move too fast in the image and its duration in the scene is too short, you may want to place your camera further away, or use a wider-angle lens to widen the field of view. In overhead camera views for people counting applications, the required duration is 1 second.
Lighting condition or contrast	Special attention should be used if a camera is installed outdoors or in a room lit by a large amount of outdoor lighting (for example, a loading dock or a green house). In these cases, lighting conditions can vary considerably throughout the day. You must use a camera with auto-gain capability to ensure sufficient image contrast for conducting the surveillance tasks provided by the software. Be aware that even with an auto-gain camera, the image may still not have sufficient contrast for the software to detect objects within the field of view. For low light conditions, a minimum of 2 lux of illumination is required.
System load	See System Load Operating Condition below.

System Load Operating Condition

The processing power in the server specification is designed for a typical customer who experiences different levels of activity in each camera, at different times of day. The typical user is expected to have moderate object traffic, 10 – 20 objects per minute for a maximum of 16 hours per 24 hour period. In the remaining 8 hour period, the typical user normally experiences much lighter traffic— fewer than 3 objects per minute, on average. These average numbers are designed to provide guidelines for what types of cameras are best used with Honeywell Video Analytics.

You should also consider peak loading numbers. This same processing power in the server specification is designed to handle extremely busy scenes where the object traffic is as dense as 90 – 120 objects per minute. Some end users may have extremely busy periods that coincide with large numbers of arrivals of people, deliveries of goods, and so on. However, the rest of the time, there should be average or limited traffic through the view. Prior to deployment, please check [Table 2-2](#) which shows how to consider a customer's peak usage. If an installation reaches peak needs most of the time, the server specification may need to be adjusted to use increased disk space for additional storage. For any

installation with peak needs that fall outside [Table 2-2](#), please check with Honeywell Sales Support (see [page 330](#)) to determine if specification modification, including increased hard drive storage and higher performance disks, is required.

Table 2-2 Object Throughput During Peak Loading

Object throughput (# of objects/min.)	Maximum number of peak hours/24 hours	Average throughput (# of objects/min) during non-peak hours
120	4	1
90	5	2.6
75	6	2.8
50	8	6.25
25	20	12.5

Managing Environmental Conditions

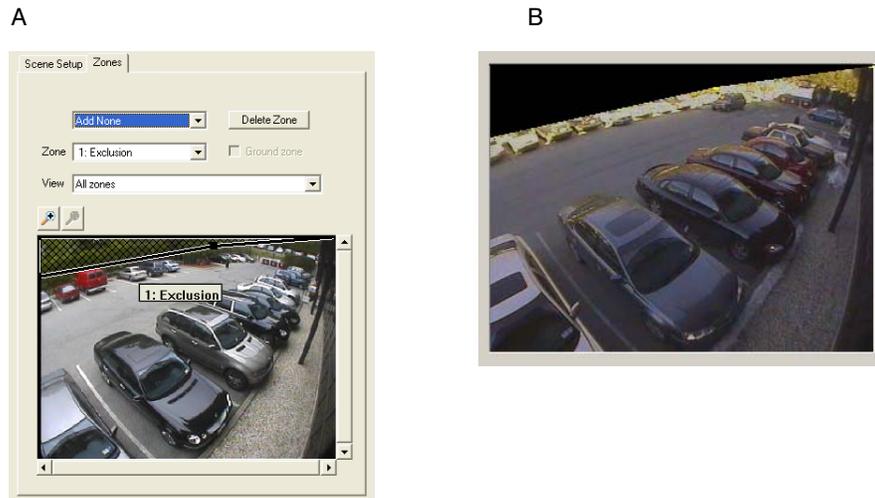
The Honeywell Video Analytics software adjusts to changing environmental conditions such as changes in lighting or fluttering of leaves on tree branches, and it automatically learns to ignore such image changes and constantly adapting to what the scene looks like. This learning occurs automatically.

However, certain scenes may pose special difficulties for a fully automated system and a customer may prefer to manually filter out such conditions. For example, in a scene containing a mirror or a reflective surface (for example, glass, metal, or marble), the camera may see a passing object. In addition, the reflection of the object may also appear. A video motion based system detects both the object and its reflection and this result is typically not desirable. Therefore, the system provides several tools that allow you to supply extra information about the scene and fine-tune the detection performance. In this section, we discuss the most frequent sources of environmental noise and the recommended methods to eliminate them.

Excluding a Zone of Irrelevant Motion in a Scene

Use an **exclusion zone** to exclude irrelevant motion in the scene. There may be parts of the camera field of view that show motion of real objects, but they are of no interest to the user. For example, there may be a busy highway at the far end of the scene, or a patch of sky in the camera view where you are not interested in detecting any objects or events.

Figure 2-1 An Exclusion Zone



In such situations, set up one or more **exclusion zones** (see [Excluding a Zone of Irrelevant Motion in a Scene](#), page 37 and [Zone Definition](#), page 63), to mask any activity occurring within one or more selected image area(s). This allows the system to focus only on the relevant parts of the scene.

Example

In the image in [Figure 2-1 \(A\)](#), the bushes at the back of the parking lot are not interesting. In such an area, there will not be any relevant objects for the daily parking lot surveillance task. As in [Figure 2-1 \(A\)](#), an **exclusion zone** is defined using a yellow quadrilateral to cover the bushes.

The effect is that the software completely ignores the entire area in the exclusion zone, as if there were no data within that zone at all as depicted in [Figure 2-1 \(B\)](#). In addition to removing irrelevant motion in the scene, the use of **exclusion zones** also saves computation power by processing only relevant portions in the camera field of view.

Reflective Surfaces

Because of the unique characteristics created by reflective surfaces in a video scene, Honeywell has developed **object-block zones** to enable special filtering capabilities. Reflective surfaces, such as mirrors, glass doors and windows, marble buildings, or polished metal, may show reflections of real objects that appear very similar to the actual object. Unless the system is 'told' about such surfaces, both the object and the reflection of the object will be tracked and reported.

It is possible to block out reflective surfaces by using an **exclusion zone**. However, in many cases there will be objects of interest appearing in front of the reflective surface. The **exclusion zone** would not only remove the reflections, but would also remove the relevant objects when they appear in the excluded part of the image. To address this problem, we use **object-block zones**.

An **object-block zone** acts as an intelligent exclusion zone. Any object that appears from within the zone and stays in the zone is ignored and not reported by the system although it is tracked internally by the software. A reflection of a person walking by a shiny glass door is a good example of this. Objects that appear in the scene outside of the blocking-zone are not affected by the zone at all. The person who walks by the shiny glass door and continues on to his car is a good example. Finally, objects that appear inside the zone and then leave the zone are reported as soon as they leave the zone and their full trajectory (including the trajectory within the zone) is kept by the system. A person coming out of a shiny glass door from inside a building, who waits a moment by the door to get his keys from his pocket before going to his car is a good example. In this case, if an object-block zone is used to mark the glass door area, once the person starts walking out of the glass door, his entire path, including the origin point inside the zone, will be kept by the system and can trigger relevant events set up by the user.

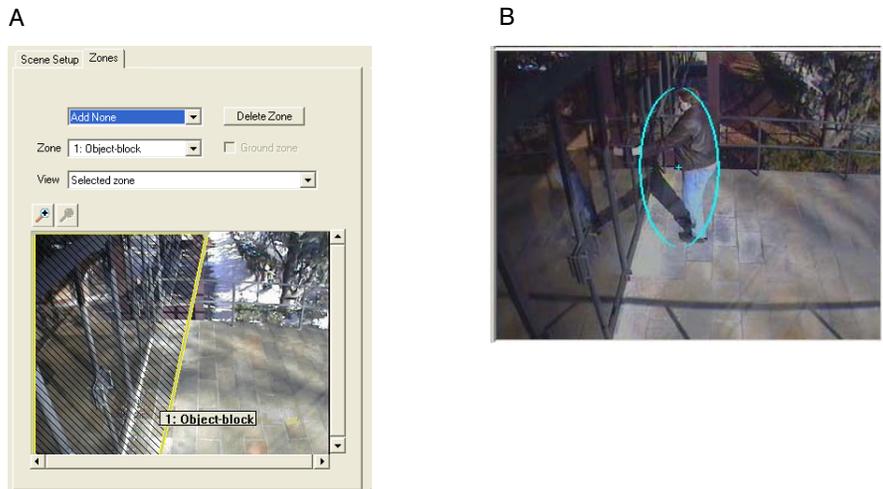
By using the **object-block zone** instead of the exclusion zone to cover a mirror, you can ensure that the system ignores reflections because those reflections can appear only in the mirror and will therefore stay within the blocking zone. Although they are tracked internally, their movement and activities are not reported. On the other hand, people and cars that appear elsewhere in the scene are reported even when they appear in front of the mirror.

Figure 2-2 demonstrates a typical use of an object-block zone. The area of the reflective glass door is covered by an object-block zone as shown in *Figure 2-2* (A).

Motion of Doors and Gates

The Honeywell Video Analytics system detects motion of objects in the scene. An opening door is a real object and is detected as such by the system. Frequent, repetitive opening and closing of doors (especially revolving doors) may be learned by the system. But doors or gates that open infrequently, or reflective glass doors that change appearance, are best handled by object-block zones. The zone should cover the area that includes both the door in the closed position and the door in the open position. The object-block zone prevents reporting of the door as a relevant object, but it still allows reporting of people passing through the door. The same approach can be used for car gates, or windows that open and close.

Figure 2-2 An Object-Blocking Zone



Motion of Trees or Foliage

You can also use the **object-block** and **exclusion zones** to reduce false alarms generated due to motion caused by gusts of wind. Again, **object-block zones** are preferred over exclusion zones if other objects appear in front of or next to the tree branches, to avoid compromising detection of relevant objects.

Object Size Filtering

The performance of the system is further improved by providing good examples of object size for different object classes (see [Setting Up the Scene](#), page 59). These examples tell the system about the expected size of people and cars at various locations in the scene and can also be used to suppress reporting of falsely detected objects that have sizes inconsistent with the provided scene setup or scene perspective.

User Management

In the Honeywell Video Analytics software, all the client applications require a valid user account to log on to the server and perform various tasks. Live User Configuration is the account management tool that is installed in the Honeywell Video Analytics Server package which allows the administrator to manage the user accounts for accessing the Video Analytics server in the system.

Note The Live User Configuration is only available on the server machine.

This chapter covers:

- Setting up user accounts and permissions
- Changing permissions
- Changing passwords

Setting Up User Accounts and Permissions

To set up user accounts and permissions:

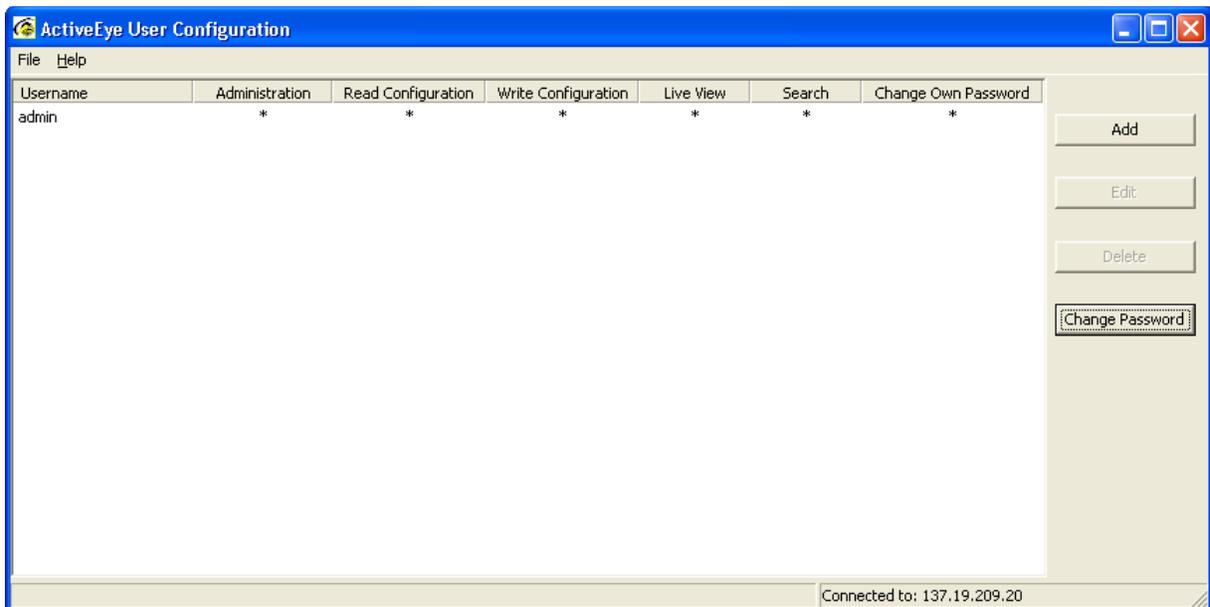
1. Go to **Start ► Honeywell Video Analytics ► ActivEye User Configuration**. The Server Login dialog box appears (see [Figure 3-1](#)).
2. In the **Host:** field, enter the hostname or IP address of the Honeywell Video Analytics server to connect to.
3. When you log on for the first time, the only account that is present in the system is the administrator account (**admin**) that was set up during the server installation process. Type the password you used during installation.

Figure 3-1 Server Login Dialog



4. After a successful log on, the main dialog page appears (see [Figure 3-2](#)). The existing users are listed in the list. The permissions for the selected user are shown in the **Permissions:** field. For user **admin**, all the permissions are granted. [Table 3-1](#) lists the six types of permissions that can be granted to each user.

Figure 3-2 Main Dialog



Note If you log on as a user without administration permission, you will only be able to see your own user. Only a user with Administrator permissions can view and manage all user accounts on the analytics server.

Table 3-1 User Permission Types

User types	You can ...
Administration	Access the User Configuration application to add users, set their permissions, or delete users.
Read Configuration	Read and open configuration on the server
Write Configuration	Write and upload configuration to the server
Live View	Run the Live Monitoring Station for real-time monitoring of alarms and events
Search	Run the Forensics Tool and Reporting Tool for search and retrieval of past alarms and events stored in the database or to generate statistics reports for various events
Change Own Password	A user can change their password, which otherwise can only be changed by the administrator with Administrator permission

Adding or Deleting Users

To add or delete users:

1. Log on as a user with Administrator permission.
2. Click **Add**. The Add User dialog box appears (see [Figure 3-3](#)).
3. Type the user name and password for this new user, and set up the permissions as required.

Figure 3-3 Add User Dialog Box

Active Eye User Properties

Username:

Password:

Confirm password:

User Permissions

Administration

Read Configuration

Write Configuration

Live View

Search

Change Own Password

OK Cancel

To delete a user:

1. Log on as a user with Administrator permission.
2. Select and highlight the user in the list, and then click **Delete User**. You are prompted to confirm the deletion.

If you are deleting the user you logged on as, you are prompted to confirm the deletion (see [Figure 3-4](#)). Upon deletion of this user, you are required to log on again as a different user.

Figure 3-4 Delete User (Logged On As) Message

Delete User?

Are you sure you wish to delete the account under which you are currently logged in? (After the deletion, you will be forced to login again).

Yes No

Changing Permissions for Existing Users

An administrator (with the Administrator permission) can change the permissions of any existing user at any time.

1. Select and highlight an exiting user.
2. Set up the permissions granted to this user
3. Click **Edit**. Edit the permissions you want to grant to the user.

Note You can only edit the permissions for yourself and not for other users, unless you have Administrator permission.

4. Click **OK**.

Changing a Password

You will be able to change your own password if you are granted with the **Change Own Password** permission. In this case, click **Change Password** to open the dialog box where you can change the password (see [Figure 3-5](#)).

Figure 3-5 Change Password Dialog



The image shows a standard Windows-style dialog box titled "Change Password". It has a blue title bar with a close button (X) in the top right corner. The dialog contains two text input fields: "New Password:" and "Confirm Password:". Below the input fields are two buttons: "OK" and "Cancel".

Configuration Basics

This chapter describes the use of the Configuration Tool to configure the rules in each camera view for your daily surveillance or operational needs. This includes:

1. Setting up video sources and camera inputs
2. Selecting and setting up scene types
3. Configuring the rich sets of zones and events

Using the Configuration Tool

After the system is installed and user accounts have been established on the server(s), you can now configure the Video Analytics system.

Launching the Configuration Tool

1. Click **Start** on your Windows taskbar.
2. Select **All Programs** (or **Programs** if using Windows 2000).
3. Select the **Honeywell Video Analytics** program group, and then click **ActiveEye Configuration Tool** to launch the configuration program.

When the Configuration Tool starts, you are prompted to designate the hostname or IP address of a server, and the user name and password to gain access to configure the server (see [Figure 4-1](#)). This enables the software to connect to the server and obtain a list of valid video inputs.

Figure 4-1 Server Login



If the connection fails, the software reports an error (for example, unable to connect, invalid user name or password, and so on). You can modify the settings and attempt to connect again by using the **File ► Connect to remote server** command in the main menu.

Figure 4-3 shows the Configuration Tool main screen. There is a Menu Bar on top and two tabs to select between two pages: Video setup, and Channel setup.

Configuration Tool Menu Bar

The **File** menu has the following options:

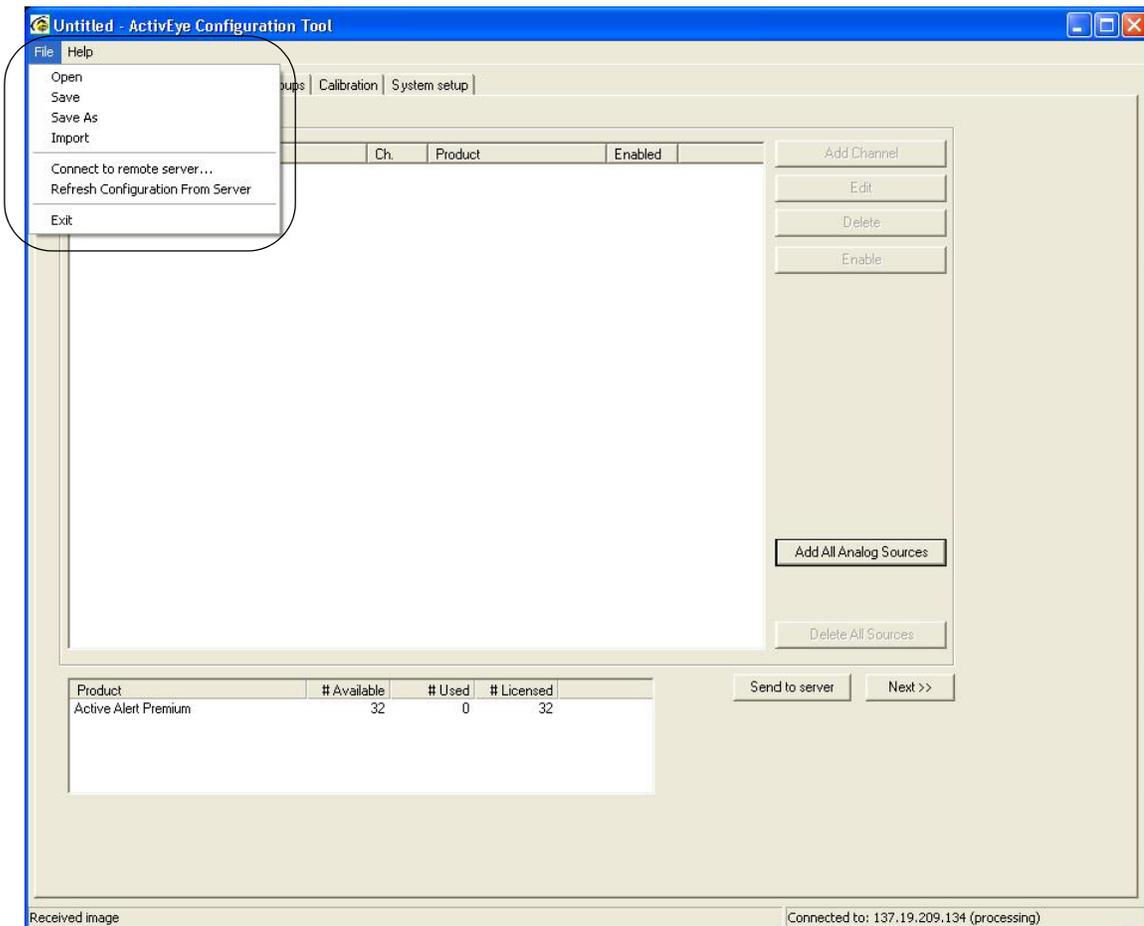
Use this File menu Item	To do this ...	For more information, see ...
Open	Open previously saved configuration	page 83
Save	Save the current configuration	page 83
Save As	Save the current configuration to a different file	page 83
Import	Import the configuration settings of a video input	page 49
Connect to remote server	Connect and log on to an analytics server	
Refresh configuration from server	Current configuration changes will be replaced with those of the analytics server	page 82

Some of the menu bar functionalities are detailed in subsequent sections.

Navigating the Configuration Tool

To navigate the Configuration Tool to go from one page to the next to proceed configuring the system, click **Next>>** to go to the next page (see *Figure 4-3*). Please note that by navigating to the next page, any changes to the configuration made in the Configuration Tool remains local on the client machine. To make the changes effective on the analytics server, you must upload the configuration by clicking **Send to server**. This function is accessible from all pages.

Figure 4-2 Configuration Tool–File Menu

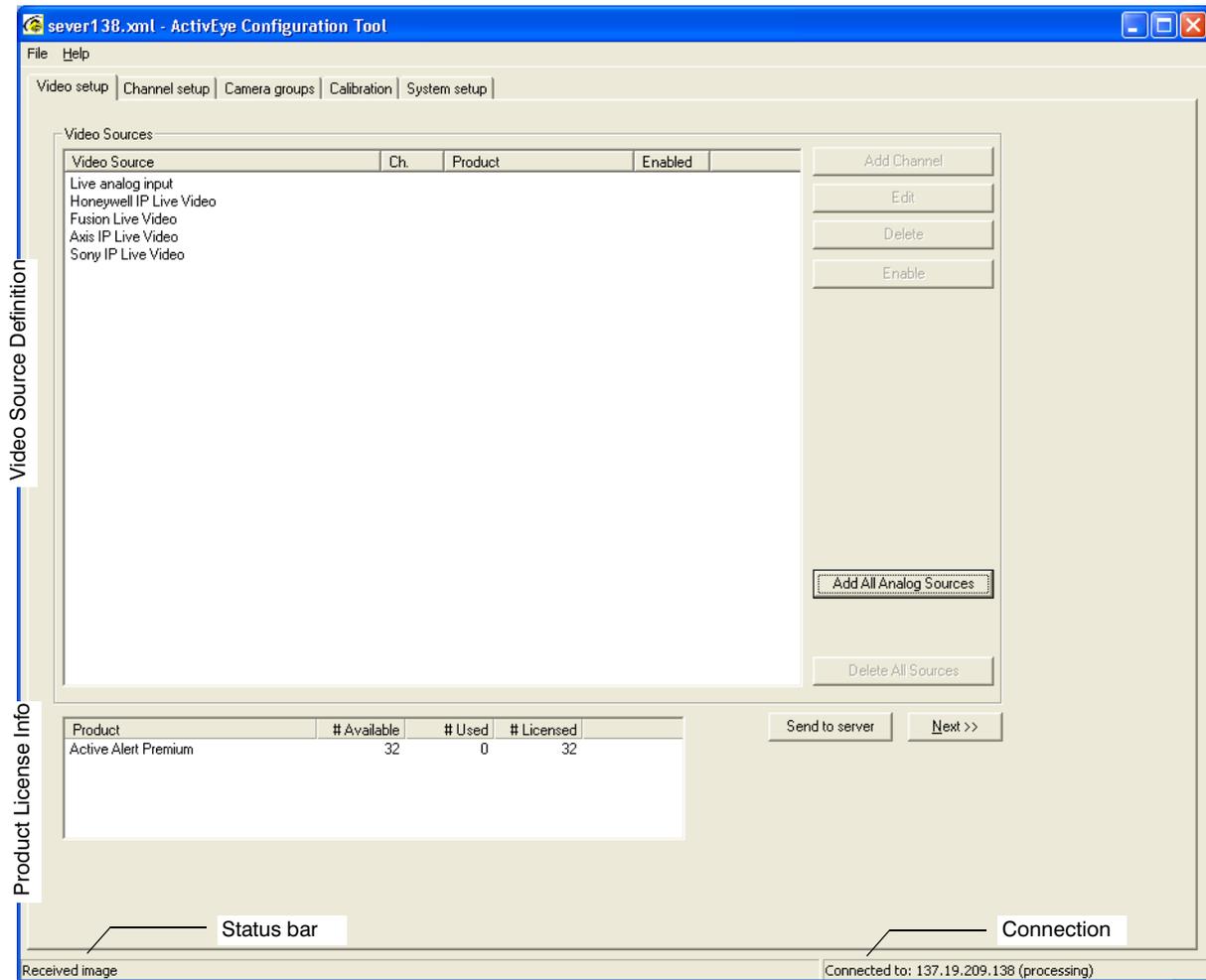


Setting Up Video Inputs

The Configuration Tool starts with the Video setup page (see [Figure 4-3](#)). There are two areas in the Video setup page:

- **Video Source Definition** section that lists the available video sources and the existing video sources
- **Product License** information that displays the number of licenses available for the product packages that are licensed.

Figure 4-3 Configuration Tool Main Screen–Video Setup Page



Types of Video Sources

The following types of video sources are available in the system:

Live Analog Input

For using the analog input from the compatible frame grabber cards. The system recognizes multiple frame grabber cards that are correctly installed on the system. If Live analog input is selected, you can specify the Input board and the Input number to be associated with this video source (see [Figure 4-5](#)). The number of available input boards and the number of inputs on each board depends on the available hardware on the server.

Axis IP Live Video

For using Axis network cameras or streamers as video input. When you select Axis IP Live Video or Sony IP Live Video as the Video Source, you can specify the hostname (that is, IP address), port, user name, and password for establishing the connection to the Axis camera (see [Figure 4-6](#)).

The following Axis IP network cameras and video servers are supported:

Axis 206, 207, 210, 211, 2120 (discontinued model), 212PTZ, 216FD, 221, 225FD, 2400 (discontinued model), 241Q, 241S, 243Q, 243Q(1) Blade, 243Q(2) Blade, 243Q(3) Blade, 243Q(4) Blade, Q7401, Q7404, Q7406

Sony IP Live Video

For using Sony network cameras or streamers as video input. You can specify the hostname (that is, IP address), port, user name, and password for establishing the connection to the Sony camera.

The following Sony IP network cameras are supported:

Sony SNC-RZ20N, SNC-RZ30N, SNC-RZ50N/P

Honeywell IP Live Video

For using Honeywell EQUIP™ Series of IP network cameras as video input. You can specify the hostname (or IP address), port, user name, and password for establishing the connection to the Honeywell IP camera.

The following Honeywell EQUIP Series IP cameras are supported:

Honeywell HD4DIP, HCD554IP, HCS554IP, ACUIX™ IP PTZ (only in fixed position), HD3MDIP, HD4MDIP, as well as the HNVE1 network encoder.

Note To use Honeywell EQUIP Series IP network cameras with analytics software, the primary stream of the camera must be set to CIF (320x240 in NTSC or 320x288 in PAL) sized image of at least 15 fps. For cameras that support 720P resolution (HD3MDIP and HD4MDIP), due to their wide aspect ratio, the CIF format results in 320 x 192 image while the QCIF format results in 160 x 96 resolution when processed by Honeywell Video Analytics.

Note that since the primary stream is shared amongst all devices (typically recording devices like Fusion or DVM), **all devices must have the same setting** (CIF, 15 fps). You can check the current setting by using the web browser to connect to the cameras, but you need to fix the setting on all devices.

If the analytics server detects the frame rate setting to be lower than 10 fps, it will re-issue the request to the camera to reset the frame rate back to 15 fps.

Fusion Live Video

For using the Honeywell Fusion DVR as video input. When you select Fusion Live Video as the video source, you can specify the hostname (that is, IP address), port, user name, and password for establishing the connection to the Fusion DVR. After the connection is made, you can select up to six cameras that are available on one Fusion DVR for analytics processing (see [Figure 4-6](#)).

Note With this option, the analytics algorithms are running on the stand-alone server, not on the embedded server on Fusion.

Adding Video Sources

There are two ways to add video sources.

Method One—Analog Live Inputs Only

To add all analog video sources enabled by the frame grabber(s) installed on the server:

1. Click **Add All Analog Sources**. The Add Analog Sources dialog appears (see [Figure 4-4](#)).
2. Specify the image size of the video sources to be processed by the Video Analytics server.

All analog video sources available on the server will then be added to the Video Source dialog (see [Figure 4-3](#)).

To delete all the existing video sources, simply click **Delete All Sources**.

Figure 4-4 Add Analog Sources



Method Two

You can also select the Video Source type, and then click **Add Channel** to add one video source using the Video Source Properties dialog (see [Figure 4-5](#)). In this dialog you can specify:

- Channel ID
- Camera name
- Enabled / disabled
- Product assignment
- Image size

Figure 4-5 Video Source Properties–Add Live Analog Input

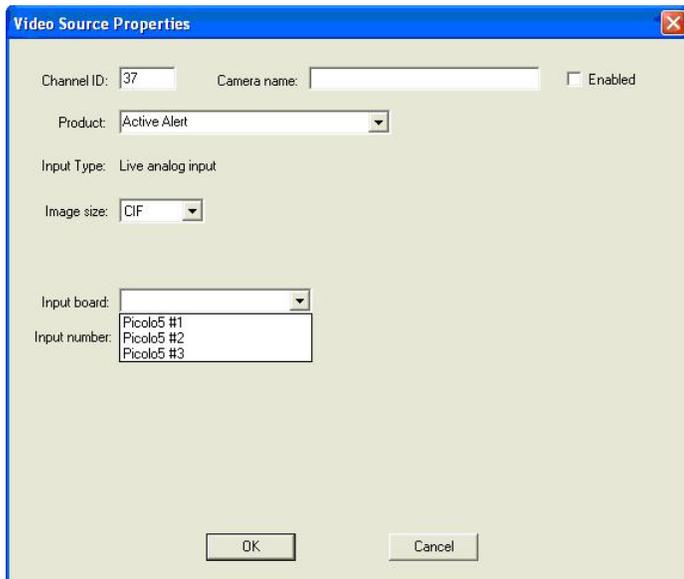
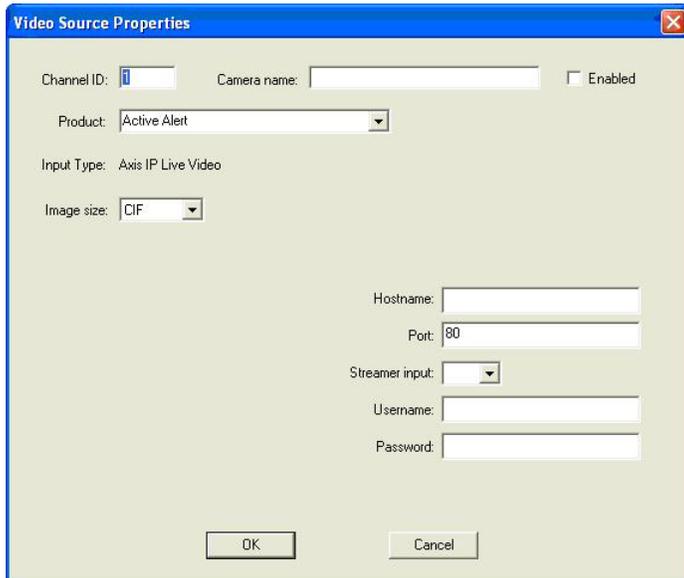


Figure 4-6 Video Source Properties–Add Axis IP Live Video

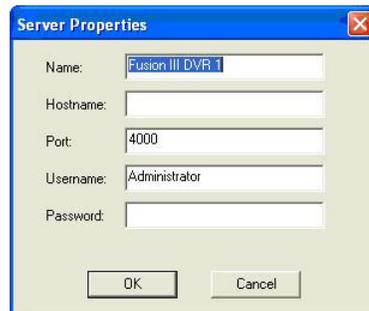


Adding a Video Source from a Fusion DVR

To add a Fusion Video Source:

1. On the Video Setup page (see [Figure 4-3](#)) select **Fusion Live Video** from the Video Sources section
2. Click **Add Fusion DVR**.
3. The Fusion Server Properties dialog box appears. You may specify the hostname (or IP address), port number, and login information to connect to the DVR (see [Figure 4-7](#)).

Figure 4-7 Fusion Server Properties



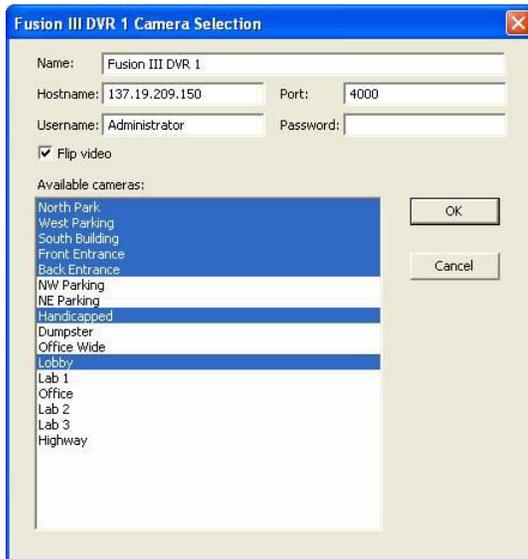
4. If the connection is successful, the Fusion DVR Camera Selection dialog box appears to allow you to select cameras on the DVR as video input sources (see [Figure 4-8](#)). From the list of all available cameras on the DVR, select up to a maximum of six cameras to use as video inputs and then click **OK**. You can make multiple selections by holding down Shift.

Adding Cameras from Multiple Fusion DVRs

To add cameras from multiple Fusion DVRs, simply repeat these steps.

If the video from the Fusion DVR is upside down, check **Flip video** in the Fusion III DVR Camera Selection dialog box (see [Figure 4-8](#)) to rotate the video.

Figure 4-8 Fusion DVR Camera Selection



Changing Properties of a Video Source

To change the properties of a video source:

1. On the Video Setup page (see *Figure 4-3*) select the video source in the Video Source section and then click **Edit**. Alternatively, double-click on the video source.
2. The Video Source Properties dialog appears. Modify the specification as required. *Table 4-1* lists the available properties that may be edited.
3. Click **OK**.

Table 4-1 Video Source Properties

Properties	Description
Channel ID	An ID number for the channel, (default value starts from 1). You may assign a different channel ID if permitted. Note For video inputs from external devices (for example, Fusion DVR), this field may not be editable.
Camera name	The name of the camera provided by the user or default by the system. It must be unique so that it can be used to identify this camera view. Note For video inputs from external devices (for example, Fusion DVR), this field may not be editable.
Enabled	A checkbox to indicate whether this channel is currently enabled. Only enabled channels are processed by the analytics server and they are counted against used licenses for the assigned product.

Table 4-1 Video Source Properties

Properties	Description
Product	The product package assigned to this channel. You must access all the features (for example, zones and events) available in the assigned product package when configuring this channel.
Image Size	The resolution of the image—CIF or QCIF
Host name	The hostname or IP address of a network device such as an IP camera or a network DVR
Port	The port number for connecting to a network device
Streamer Input	The input number on a network video streamer with multiple inputs
Username	The user name used to log on to a device that requires authentication.
Password	The password used to log on to a device that requires authentication.

Deleting a Video Source

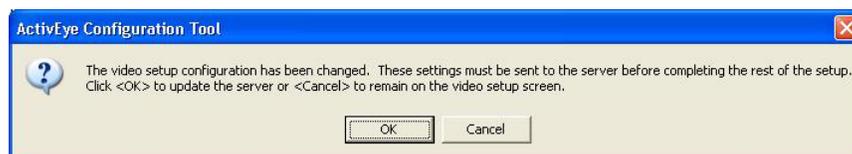
To delete a video source:

1. Select the video source in the Video Source dialog.
2. Click **Delete**.

Uploading the Configuration to a Server

After you finish configuring all the camera views:

1. Click **Send to server** on the Video setup page to upload the updated configuration to the Video Analytics server. If any modification has been made from the existing configuration downloaded from the server, you must send the configuration to the server before you can navigate to a different tab. Otherwise, a warning message appears as shown below.



2. Click **OK** to send the updated configuration to the server or **Cancel** to remain in the current Video setup screen.
3. When the configuration is successfully uploaded, a confirmation message appears as in [Figure 4-9](#). This indicates that the server has accepted the new configuration and is currently processing channels with the completed configuration. If there are any

channels that are left with an uncompleted configuration, a warning message appears to indicate how many channels are being processed and how many channels are yet to be configured.

Figure 4-9 Configuration Uploaded Confirmation



Product Licenses

Product licenses are listed at the bottom of the Video Setup page. You can see:

- The number of licenses that are available (or unassigned)
- The number of licenses that are in use through enabled channels
- The total number of licenses the license key allows.

You cannot process more channels than the license key allows.

If you have exhausted all the licenses that are licensed and you attempt to add more channels to a given product, you can disable a currently processed channel to allow the license to be used by another channel. If you attempt to process more channels than you are licensed for, a warning message appears to alert you that there are no more licenses for the specified product.



Updating the License Key

To update the license key:

1. On the Configuration Tool, select the **System setup** tab (see [Figure 4-3](#)).
2. Click **Enter license key**. See [Entering the License Key](#), page 135 for more detail.

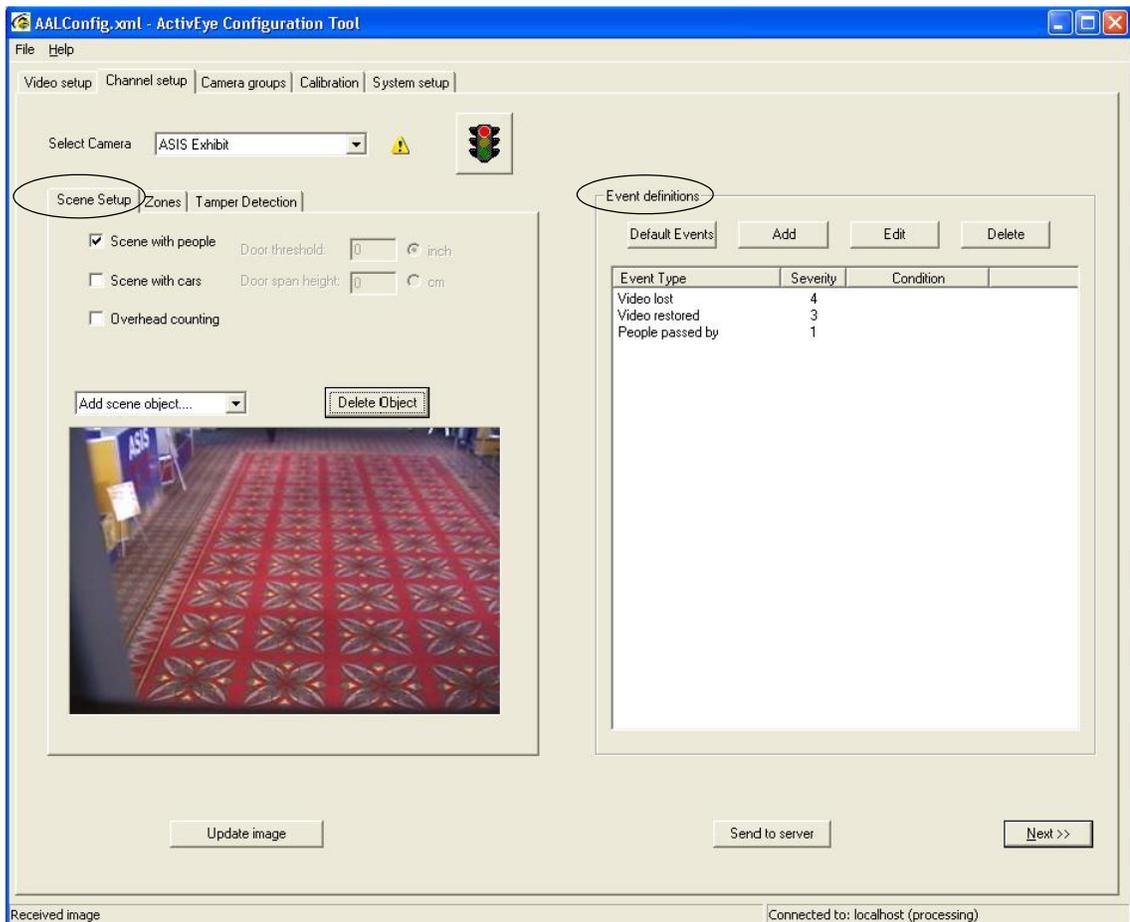
Channel Setup: Configuring Each Channel

This section shows you how to properly configure the application. Channel setup allows you to customize the setting for each video-input channel independently. It includes the following steps:

1. Select a video channel.
2. Define the scene type.
3. Define zones and directions for event detection.
4. Customize the event list.

Figure 4-10 shows there are two areas in the Channel setup page: Scene/Zones setup and Event Definitions.

Figure 4-10 Channel Setup Page



Selecting a Video Channel

To change the settings of a video channel:

1. From the **Select Camera** drop-down list, select a camera to change the settings for the corresponding channel. Each video input channel can have separate list of events, scene setup, and associated zones.
2. Click **Update image** below the image display anytime to update the live image. You may find this button quite useful during the following configuration steps.

Setting Up the Scene

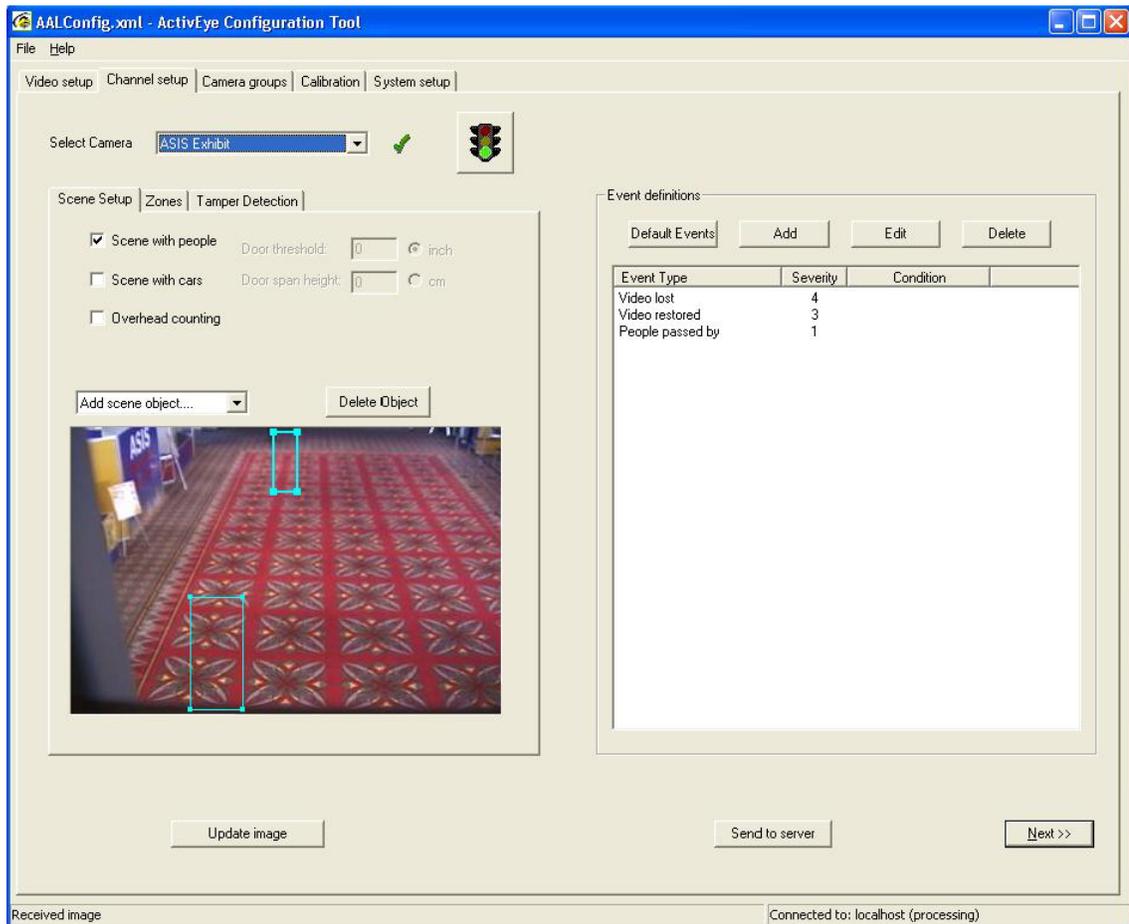
On the Scene Setup sub page you can provide information about the scene in the input video. There are two kinds of scene information:

- Types of objects expected in the scene
- Minimum size of these objects in the various parts of the scene

To select one of the three scene types, click the corresponding check box (see [Figure 4-11](#)).

- Scene with people
- Scene with cars
- Overhead counting

Figure 4-11 Scene Setup—Specifying Expected Object Types



Scene with People

1. Select the **Scene with people** checkbox for scenes that contain human activities. This selection can co-exist with **Scene with cars** if you are monitoring both human and vehicular activities in the camera view.
2. With this selection, you must specify at least two examples of *person*, which provides the average person size information to the system. To specify the average persons in the scene, click **Add scene object ...** from the drop-down box and then select **Add person example** to add a *person* example. A default blue rectangle is shown in the display area.
3. Place the mouse cursor inside the rectangle, press and hold the left mouse button and move the rectangle to the desired location where the person size is specified. Release the button.
4. To define the person size, place the mouse cursor on one of the anchors, press and hold the left mouse button and move the anchor to the desired location. Release the button. See [Figure 4-12](#). The size of the box should be the minimum expected of a car that should be detected. In order for the person size information to provide the scene

perspective, repeat the previous steps for at least two person examples. Preferably, the two examples are placed far apart from each other vertically — one close to the camera and the other far away.

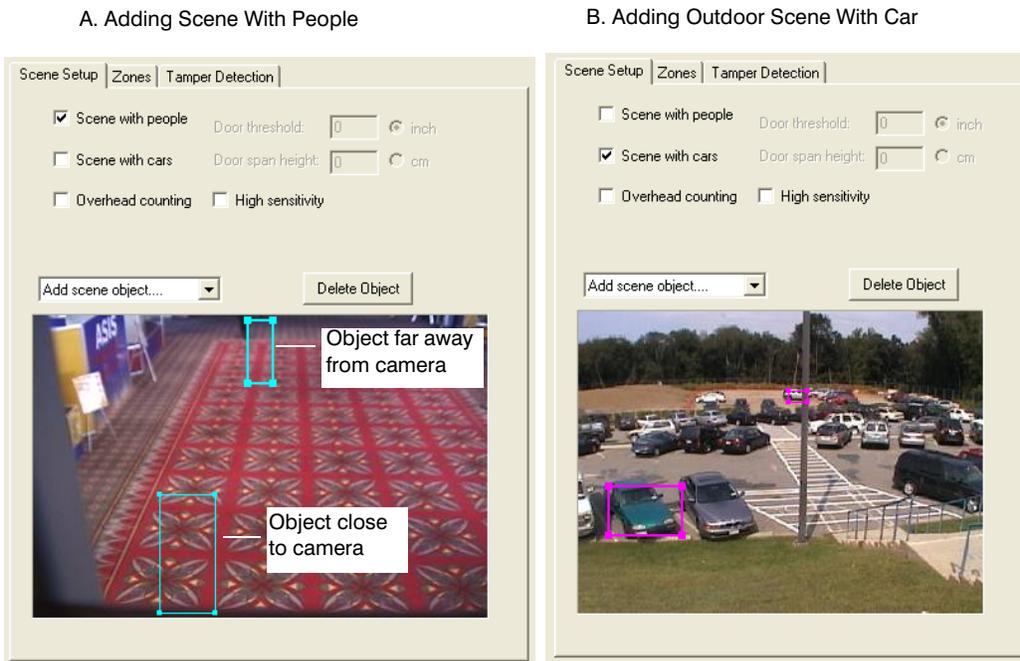
To redefine an object example:

1. Select the example by clicking inside the object rectangle.
2. Modify its location and anchors as described above.

To delete an object example:

1. Select the example by clicking inside the object rectangle.
2. Click **Delete Object**.

Figure 4-12 Scene Setup Examples



Scene with Cars

1. Select the **Scene with cars** checkbox for scenes that contain vehicular activities. This selection can co-exist with **Scene with people** if you are monitoring both human and vehicular activities in the camera view.
2. With this selection, you must specify two examples of *car* to provides the average car size information to the system.
3. To specify the average cars in the scene:
 - a. Click **Add scene object ...** from the drop-down box
 - b. Select **Add car example** to add a *car* example. A default pink rectangle is shown in the display area.

4. Place the mouse cursor inside the rectangle, press and hold the left mouse button and move the rectangle to the desired location where the car size is specified. Release the button.
5. To define the car size, place the mouse cursor on one of the anchors, press and hold the left mouse button and move the anchor to the desired location. Release the button (see [Figure 4-12](#)). For the car size information to provide the correct scene perspective, repeat the previous steps to add a minimum of two car examples. Preferably, the two examples are placed far apart from each other vertically — one close to the camera and the other far away.

You can redefine or delete a car example in a similar manner as for the person example.

Overhead Counting

The scene type **Overhead counting** is strictly used for counting people in an overhead camera view. When you select this check box, the software automatically selects **Scene with people** and de-selects **Scene with cars**. It also grays out both selections as you cannot change them. Overhead people counting is a widely used feature that requires a very specific setup procedure to achieve the best performance. For the detailed setup procedure, see [Chapter 6](#).

High Sensitivity

For scenes with low contrast, such as under low light conditions or under infrared cameras, you can increase the detection sensitivity in the software by checking the High Sensitivity checkbox. Low contrast or low visibility can be caused by insufficient lighting or dark scenes, targets with similar characteristics as the background, or hazy weather with reduced visibility. This setting allows the software to better discern the difference between the static background and object movement.

This setting can be used in conjunction to all scene types, including Scene with people, Scene with cars or Overhead counting. [Figure 4-13](#) shows an example of using high sensitivity mode for a low contrast scene under infrared illumination.

Figure 4-13 High Sensitivity Setting



Zone Definition

Select the **Zones** tab in the **Channel setup** window to set up zones. The available zones may differ from one product package to another. Collectively, there are eighteen zone types included in the current Honeywell Video Analytics offering:

Table 4-2 Zone Types

Zones	Purpose
Exclusion	The system completely ignores any activities in the zone.
Object-block	The system filters out possible false alarms that are confined in a localized area, such as wildly waving tree branches or object reflection on a reflective surface
Restricted	The system detects entry, exit, parking, and loitering in the zone.
Direction	The system detects motion in the wrong direction.
Trespass	The system detects trespassing of a virtual perimeter.
Fence	The system detects a person climbing on a fence.
Sterile	The system detects approaching and breaching to the virtual perimeter.
Counting line	Used for overhead people counting. It replaces the use of inside and outside zone pairs to simplifies people counting setup.

Table 4-2 Zone Types

Zones	Purpose
Inside Outside	These paired groups are used to count the number of instances of entering and exiting between the two groups of zones.
Car lane counter	The system counts the number of cars passing through individual lanes on the highway.
Detection	Used for some premium events, including Object left unattended , Person running , and Vehicle speeding to mark the area where the detection is in effect.
Asset	The system detects an asset being removed from the scene.
U-turn	The system detects cars making illegal u-turns.
Handicapped	The system detects parking in the zone.
Shoulder	The system detects a car pulling off the road, which often indicates the need for assistance.
Theft	The system detects suspicious shopper behavior when the shopper reaches in to the shelf and quickly grabs too many items of merchandise.
Target	The system collects information on customer activities for marketing purposes.



Caution Inside zones must not overlap with outside zones, and vice versa. Failure to abide by these rules will result in incorrect system functioning.

All other zones can be completely separate, partially overlapping, or fully overlapping.

Zone Shapes

Table 4-3 Zone Shapes

Zone shapes	Purpose
Quadrilateral	Exclusion, object-block, restricted, fence, inside/outside, car lane, counter, detection, asset, handicapped, shoulder, and target zones.
Trespass lines	Include a line segment to mark the virtual boundary and an arrow to indicate the allowed traffic direction. Theft lines have a similar look to the trespass lines, where the arrow indicates the direction and the distance of the arm reach into the shelf.

Table 4-3 Zone Shapes

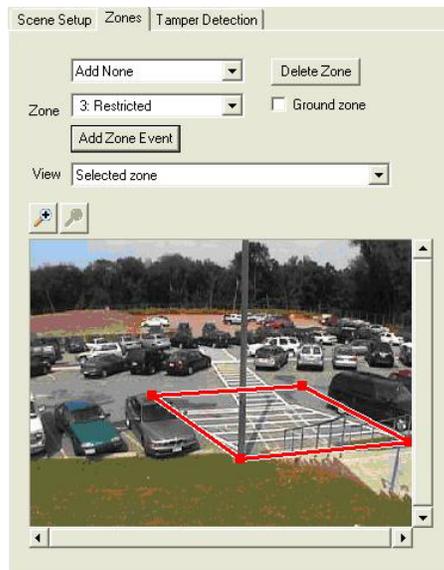
Zone shapes	Purpose
Counting line	A counting line can have multiple segments to define the counting boundary that best matches to the physical environment. An arrow on the line indicates the direction of enter , and the opposite direction defines exit .
Quadrilateral with direction edges	Direction zones are quadrilateral with two directional edges for defining the allowed traffic direction.
Two quadrilaterals with a common edge	A u-turn zone is made of two quadrilaterals with a common edge. It also has two directional edges on one quadrilateral and the arrows define the starting direction of the u-turn.

Zoom Tooltip

On the **Zones** tab, there are zoom tool tips that allow for zooming in and out of the image (see *Figure 4-14*). Use them to help better define the zone, especially when a precise zone boundary is required. Each time you click the zoom-in icon, the image will be magnified 2x.

Point and drag the entire image or use the scroll bars to move to the desired area in the image where you want to place the zone.

Figure 4-14 Zone Definitions–Restricted Zone



Defining a Restricted Zone

To define a restricted zone:

1. Select **Add restricted zone** from the **Add zone** drop-down list. A quadrilateral is shown in the display area.
2. Place the mouse cursor on one of the anchors, press and hold the left mouse button and move the anchor to the desired location. Release the button to affix that anchor.
3. The other three anchors can be defined in the same way (see [Figure 4-14](#)). All quadrilateral zones can be defined in a similar way.
4. Click **Add Zone Event** to add more events associated with the currently selected restricted zone.

As a restricted zone is added, a set of events defined upon the restricted zone automatically appears in the **Event Definitions** area on the right.

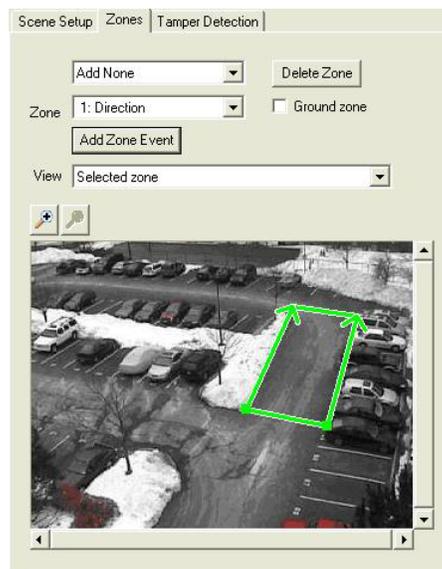
Defining a Direction Zone

To define a direction zone:

1. Select **Add direction zone** from the **Add zone** drop-down list. A default quadrilateral with two directional edges is shown in the display area.
2. Move the anchors to the desired locations. The allowed direction of the motion is defined by the two directional edges (see [Figure 4-15](#)).
3. Click **Add Zone Event** to add more events associated with the currently selected restricted zone.

As a direction zone is added, the event **Started moving in the wrong direction** automatically appears in the **Event Definitions** area on the right.

Figure 4-15 Zone Definitions–Directional Zone



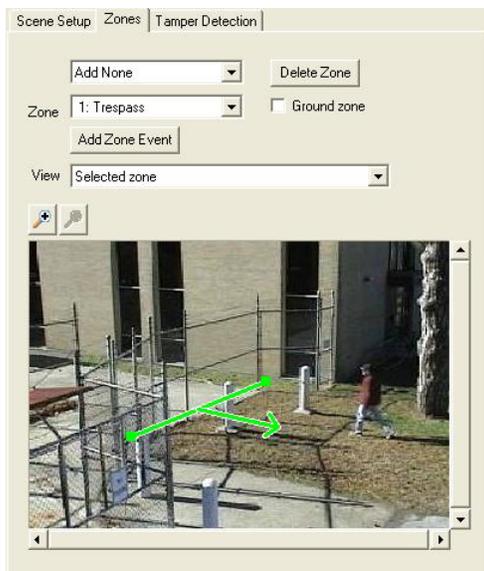
Defining a Trespass Line

The trespass line is a useful zone for detecting a breach of a virtual perimeter. To define a trespass line:

1. Select **Add trespass** from the **Add Zone** drop-down list. A default trespass line appears. It includes a line segment that defines the virtual perimeter placed on the ground plane, and an intersecting directional line indicating the allowed direction to pass the line (see [Figure 4-16](#)).
2. Move the anchors to the desired locations to define your virtual perimeter and the one-way allowed traffic direction. Any object passing the trespass line in the opposite direction will trigger the **Object trespassing** event. The arrow indicates only the allowed line-crossing direction. Its angle and length have no effect on the result.
3. Click **Add Zone Event** to add more events associated with the currently selected trespass line.

When a trespass line is added, the **Trespassing** event automatically appears in the **Event Definitions** area on the right.

Figure 4-16 Zone Definitions–Trespass Line



Defining a Sterile Zone

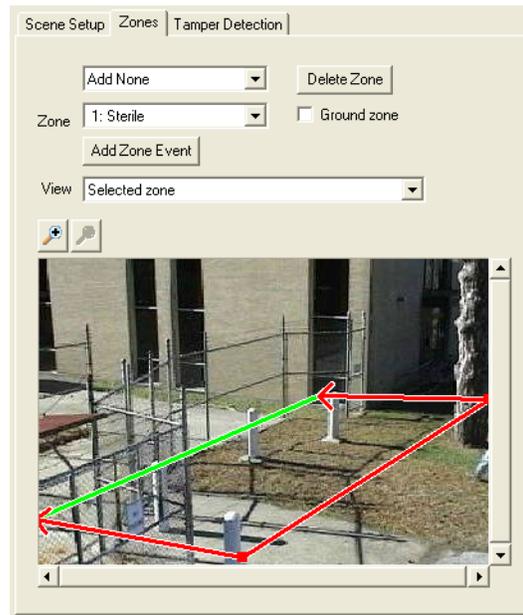
The sterile zone is useful for detecting people or cars approaching a virtual perimeter. It is a quadrilateral zone that has three red borders (including a pair of directional edges), and one green border. The green border defines the allowed entry point into the zone and it is usually drawn along the virtual perimeter line. The red arrows specify the disallowed direction of movement towards the virtual perimeter inside the zone. Upon entry into the zone through a red border, if the object moves beyond the original entry point and gets closer to the virtual perimeter, an alarm will trigger.

To define a sterile zone:

1. Select **Add sterile** from the Add Zone drop-down list. A default sterile zone appears. (see [Figure 4-17](#)).
2. Move the anchors to the desired locations to define the area where directional approach to the virtual perimeter should be alerted. Have the green border specify the virtual perimeter line.
3. Click **Add Zone Event** to add more events associated with the currently selected sterile zone.

When a sterile zone is added, the default Object in Sterile Zone event automatically appears in the Event Definitions area on the right.

Figure 4-17 Zone Definitions—Sterile Zone



Defining Inside and Outside Zones for Car Counting

Inside and **outside** zones can be paired to be used for counting vehicles in camera views. For overhead people counting, see [Chapter 6](#). This section describes inside and outside zones for counting vehicles in and out of a parking lot.



Caution For highest accuracy in people counting, the camera must be positioned in an overhead position. Please see [Chapter 6](#) for details instructions on configuring the system for overhead people counting.

You may configure multiple inside and outside zones in each camera view. The number of zones you need depends on the physical layout of your facility. For example, you may need three quadrilateral outside zones to cover all three directions (west, south, and east) where a person may come into the corridor and then enter the meeting room through the inside zone that has been defined.

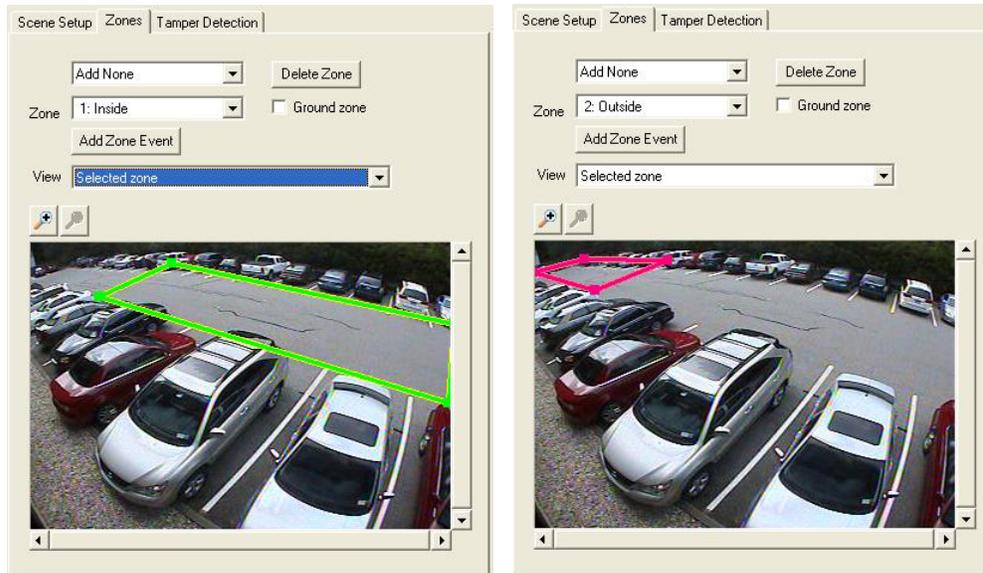
Multiple inside or outside zones can be used to cover the entry/exit points in the camera field of view. *Figure 4-18 (A)* shows an inside zone in a parking lot that covers the 'inside' of the parking lot. *Figure 4-18 (B)* shows an outside zone that covers the entry/exit point that connects to the outside of the lot.

After you have both inside and outside zones defined, you can then add the events **Car entered lot** and **Car exited lot** to the event list.

Figure 4-18 Define Inside and Outside Zones in a Parking Lot

A. Inside zone

B. Outside zone



Defining Car Lane Counter

For highway traffic counting, typically the camera is mounted on a high pole to provide sufficient coverage. For optimal result, the camera should face incoming traffic. To measure highway traffic flow by tracking and counting each vehicle passing through the highway, we recommend you use **Car lane counter**.

For a traffic scene as shown in *Figure 4-19*, the focus is on counting the head-on traffic towards the camera. Traffic along the opposite direction that is partially seen should be excluded by placing an exclusion zone as shown in *Figure 4-19*.

Figure 4-19 Exclude Traffic in the Opposite Direction

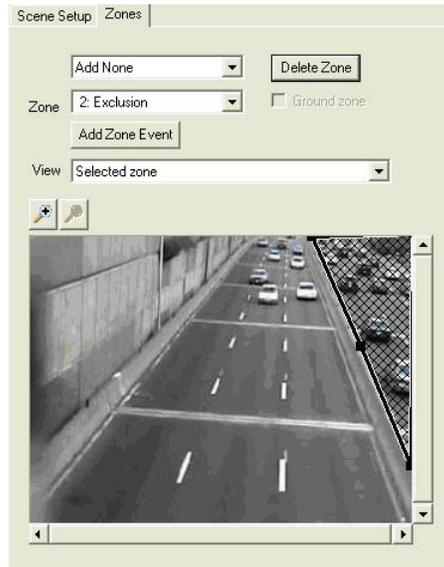


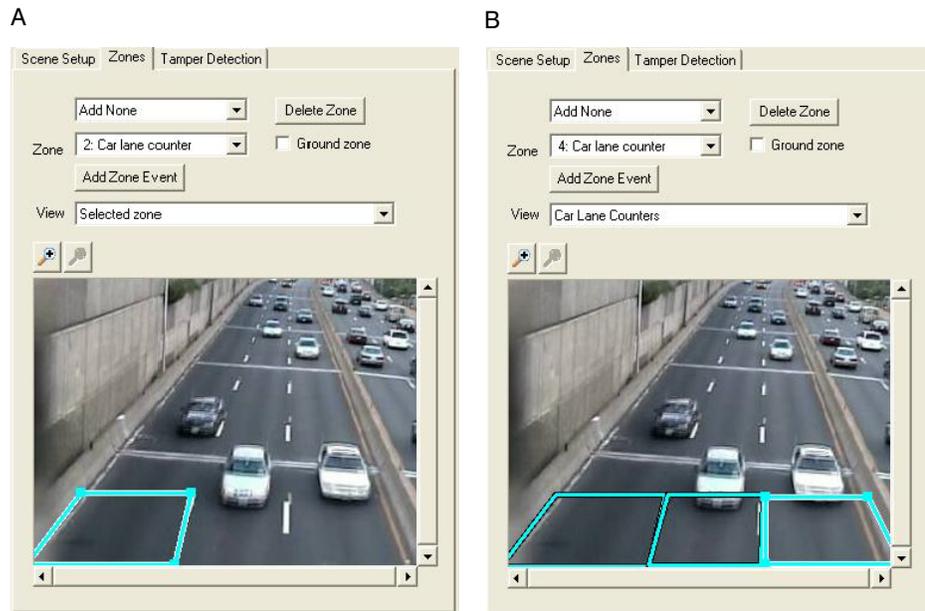
Figure 4-20 shows an example of traffic counting using the car lane counter zone.

The car lane counter is intended to be placed to cover each lane on the highway. The car lane counter provides vehicle counts for each individual lane on the highway. *Figure 4-20* (a) shows an example of car lane counters that cover the right lane on the highway.

Note The best placement for the car lane counter is at the frame boundary closest to the camera. This ensures that the location for counting has the best view in the entire image.

There is no limit to how many car lane counters you can have in one view. You can add multiple car lane counting zones to cover the left and right lanes in the same camera view.

Figure 4-20 Define Car Lane Counters



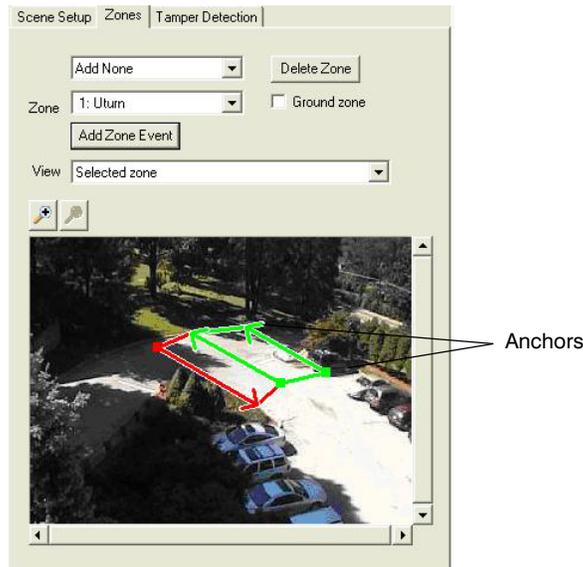
Select **View Car Lane Counters** to view all the car lane counters currently defined for the camera view. [Figure 4-20](#) (B) shows all the car lane counters that correspond to individual lanes on the highway for per-lane traffic counting.

Defining a U-Turn Zone

To define a U-turn Zone:

1. Select **Add u-turn zone** from the **Add Zone** drop-down list.
A default u-turn zone made up of two quadrilaterals with a common edge shows in the display area.
2. Move the anchors to the desired locations. The allowed direction is defined by the two directional edges (see [Figure 4-21](#)).
3. Click **Add Zone Event** to add more events associated with the currently selected restricted zone.

Figure 4-21 Define a U-turn Zone



Defining a Target Zone

A target zone can be used to automatically collect information on customer activities in a store for marketing purposes. Such information may include how many people stopped to look at the merchandise on sale or how many people stopped for more than 30 seconds in front of the display of a new promotional item. To monitor these types of people activities in addition to counting people, you can use a target zone. By placing a target zone around the monitored area, you can enable events including **Person entered target zone** and **Person staying in target zone** for more than a specified amount of time.

To define a target zone:

1. Select **Add target zone** from the **Add zone** drop-down list.
A quadrilateral shows in the display area.
2. Place the mouse on one of the anchors, press and hold the left mouse button, and then move the anchor to the desired location. Release the button to affix that anchor.
3. Define the other three anchors, as required, in the same way (see [Figure 4-22](#)).
4. Click **Add Zone Event** to add more events associated with the currently selected restricted zone.

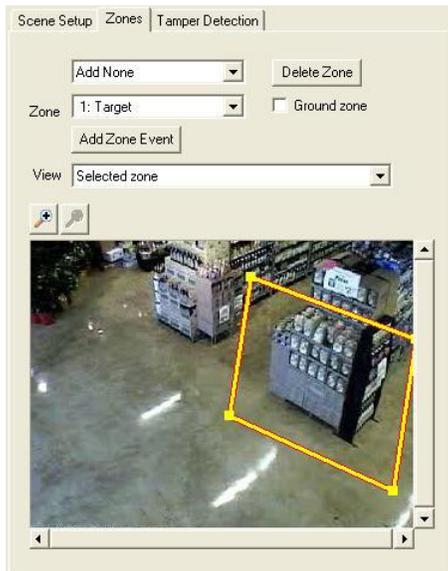
As a restricted zone is added, a set of events defined using the target zone automatically appear in the Event Definitions section on the right.

To view or to redefine a zone, select the zone from the **Zone** drop-down list.

To delete a zone:

1. Select the zone from the **Zone** drop-down list.
2. Click **Delete**.

Figure 4-22 Define a Target Zone



Comparing an Image Zone to a Ground Zone

All the zones can be configured as **image zone** or **ground zone**. A zone is an image zone by default. An object is considered to be within an image zone if the center of the object is within the boundaries of the zone. In contrast, an object is considered to be within a ground zone if the foot of the object is within the zone boundaries. Therefore, an image zone should include an area in the image where the main body of the object is expected to appear.

A ground zone should include the area in the image that corresponds to the actual floor space in the three-dimensional world. A person is considered to be within a ground zone when their feet are within the zone boundaries. Check the **Ground zone** checkbox in the **Zone Setup** section to set the zone to a ground zone.

Note In the overhead camera view, all the zones should be configured as image zones because the feet are not typically visible in such a view. Setting the zone to be ground zone in the overhead view may lead to incorrect results.

Customizing the Events

After the video source and the number of input video channels are selected in the **Video setup** page, the default list of events to be detected appears in the **Event List** window in the **Event Definitions** area. The Event Definitions area allows you to customize your settings for event detection.

Adding an Event Associated to a Zone

To add an event that is associated with a zone, in the Zones tab, click **Add Zone Event**. Those events that are associated with the selected zone are listed for selection. An Event Properties dialog box appears to input:

- Severity level
- Time conditions (date, time, day of the week)
- Associated zones (when applicable) of the event

Figure 4-23 Add an Event

The screenshot shows the 'Event Properties' dialog box. It has a title bar with 'Event Properties' and a close button. The main area contains the following fields and options:

- Event type:** A dropdown menu set to 'Person counted as entering'.
- Severity:** A dropdown menu set to '3'.
- Zone1:** A dropdown menu set to 'Outside zones'.
- Zone2:** A dropdown menu set to 'Inside zones'.
- Time conditions:** A section with a title 'Time conditions' and a list of options:
 - Date from: 6/16/2004 to: 6/16/2004
 - Time from: 1:52:44 PM to: 1:52:44 PM
 - Sunday
 - Monday
 - Tuesday
 - Wednesday
 - Thursday
 - Friday
 - Saturday

At the bottom of the dialog are two buttons: 'OK' and 'Cancel'.

For zone definitions, see [page 63](#). For example, you can define an enter event relative to a restricted zone and set a high severity at night and have another enter event with a low severity during the day.

Adding a Event for the Entire Scene

To add an event that does not require a zone, in the Event Definition section click **Add**. The Event Properties dialog box appears for you to customize the event. This type of event is applied to the entire scene.

Editing an Event

To change the settings of an event:

1. Either click the event to highlight and then click **Edit**, or double click that event. The Event Properties dialog box appears (see [Adding an Event Associated to a Zone](#), page 74).
2. You can change the severity level in the **Severity** drop down list. Severity setting ranges from **1** (lowest) to **10** (highest).
3. To set the time conditions for the event you are customizing, check the box of **Date from:** and/or **Time from:** to set the date and time range for the event.
4. You can also set the day of the week when the property settings of the event will apply. Select the check box for the days of the week that to which the settings will apply.

To delete an event, click the event to highlight, and then click **Delete**.

To reset the list of events to a standard list, click **Default Events**.

Figure 4-24 Modify an Event

The screenshot shows the 'Event Properties' dialog box. It includes the following elements:

- Event type:** Entered
- Severity:** 7
- Zone1:** None
- Zone2:** None
- Time conditions:**
 - Date from: 10/10/2003 to: 10/10/2003
 - Time from: 6:00:00 PM to: 10:00:00 PM
 - Sunday
 - Monday
 - Tuesday
 - Wednesday
 - Thursday
 - Friday
 - Saturday
- Buttons:** OK, Cancel

Note For each video channel, only events defined in the **Event List** window are detected in real-time as they occur. These detected events are stored in the database for later search and retrieval, as well as for generating statistics report.

Alarm Threshold Control

There is a global alarm threshold control on a per-server basis. This alarm threshold applies to all the video channels processed on the server to which the Configuration Tool is currently connected. For real-time alarm triggering, you can set the alarm threshold from the **Alarm Threshold** drop-down list. The default alarm threshold is set to **4**. Select the alarm threshold that is suitable for your operation. Any event with severity level equal to or greater than the alarm threshold generates an alarm in real-time. The alarm can be delivered in various forms including visual, audio, e-mail, and relay output.

Camera Tamper Detection

Video Analytics software V4.7 includes camera tamper detection. This feature is designed to protect the cameras that are processed by the analytics server to alert the user when the camera has been tampered with. Camera tamper includes blinding, blurring, or a change in the field of view of the camera. Automatically detecting camera tampering is an important functionality in a video surveillance system. A robust video surveillance system should be able to detect when such conditions occur and provide timely alert to the owner or the security operator. This is particularly important, both for security as well as service reasons, especially in systems with large numbers of cameras where it may not be possible to regularly review all the cameras in detail.

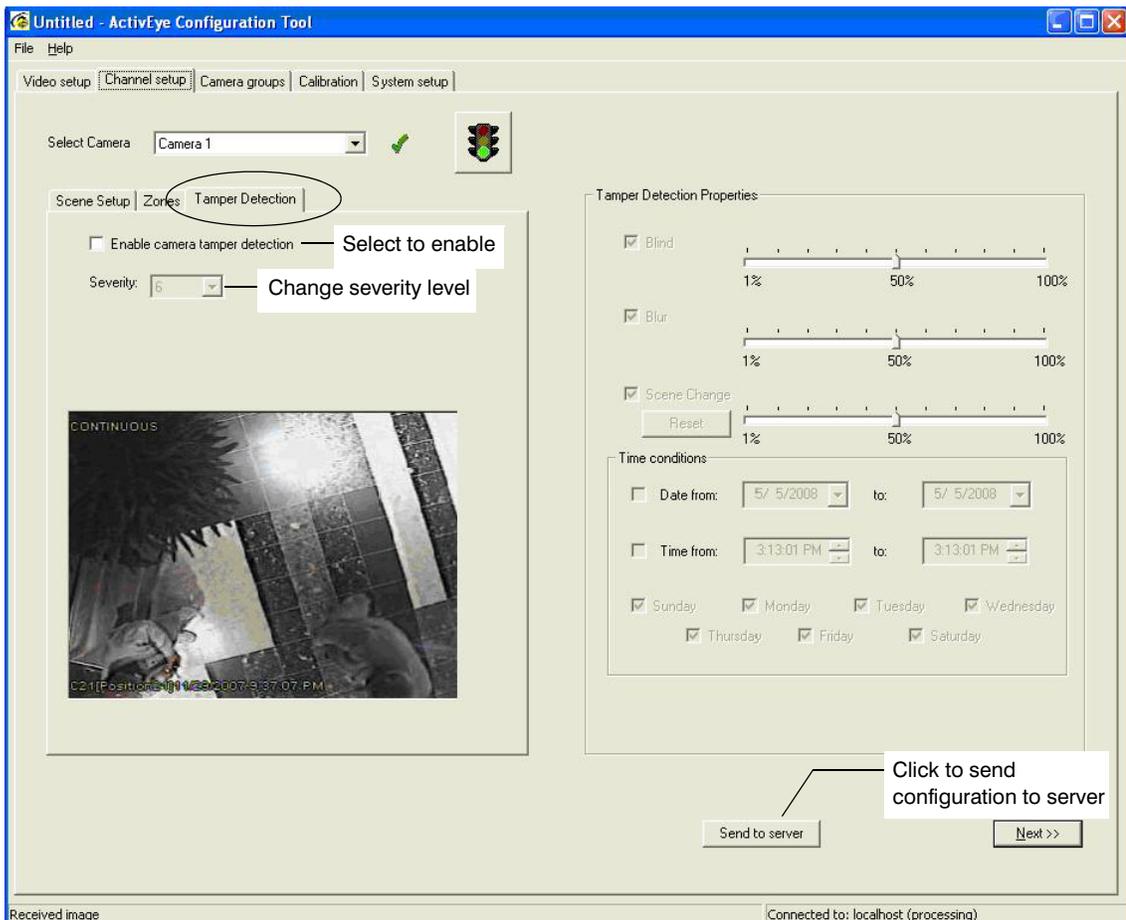
Currently three types of camera tamper detection are provided:

- **Blind:** Detects when the lens of a camera is covered, or the scene has very low contrast which may be a result of someone blocking the camera view. Blinding also reports the loss of video for network video streamers that do not provide specific video loss alarms.
- **Blur:** Detects when the lens of the camera is out of focus.
- **Scene change:** Detects when the camera is no longer watching the original scene, that is, when the field of view has changed.

Configuring Tamper Detection

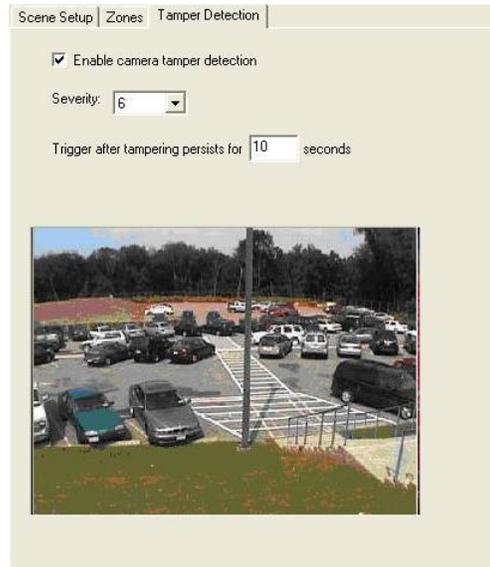
1. On the Configuration Tool, select the **Channel setup** page, then select the **Tamper Detection** tab (see [Figure 4-25](#)).

Figure 4-25 Tamper Detection



2. To use Camera Tamper Detection, you must first enable the feature by selecting the **Enable Camera Tamper Detection** checkbox.
3. You can change the severity of the Tamper Detection events by changing the value of the **Severity** level for camera tamper alarms as shown in [Figure 4-26](#).
4. You may want to specify the duration for the camera tamper measurement to remain above the specified threshold value before an alarm is triggered. Modify the parameter **Trigger after tampering persists for** to specify such duration in seconds. Increase this value to avoid frequent repeated alarms if the tamper measurement quickly jumps above and below the threshold. The default value is 10 seconds.
5. Remember to click **Send to server** to make these changes in effect.

Figure 4-26 Enable Camera Tamper Detection



It is important to understand that, similar to the analytics software, the camera tamper detection is designed to use with stationary cameras with fixed views. To avoid raising false alarms, Honeywell recommends that you disable camera tamper detection when the following conditions apply:

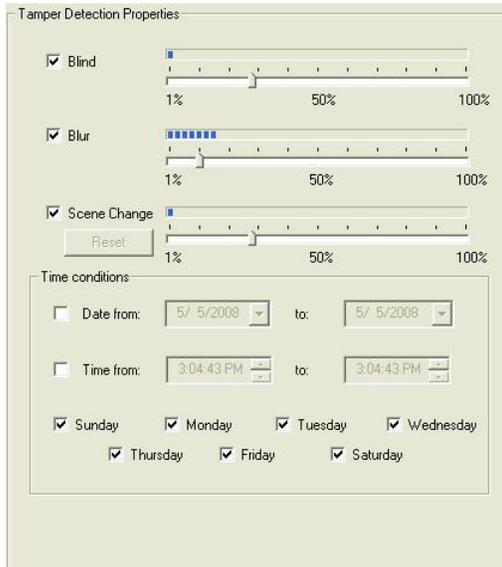
- While operating a PTZ device
- While a preset or mimic tour is running
- If the video display becomes too dark

Adjusting Tamper Detection Parameters

Each type of camera tamper detection—blind, blur, and scene change—can be enabled independently by selecting the check box for each type (see [Figure 4-27](#)). You can also adjust the threshold parameter for each type independently. This threshold is represented as a percentage value ranging from 1% to 100%. If the camera tamper measurement exceeds the threshold value and persists for the specified duration, an alarm of the corresponding type of camera tamper will be triggered. The default threshold is 50% for all three types of camera tamper. The lower the percentage threshold, the more sensitive the camera tamper detection is and the more prone to false alarms, as it is easier for the measurement to exceed the specified threshold.

When camera tamper detection is enabled, both the image and the camera tamper measurement of all three types are updated in real time at regular intervals (see [Figure 4-27](#)). This allows you to observe these measurements under the normal camera view and thus make any adjustments on the threshold values. Honeywell recommends that you adjust these thresholds settings to the desired values.

Figure 4-27 Tamper Detection Thresholds



Similar to analytics events, you can apply date/time conditions to enable camera tampering detection as well. Modify the Time conditions section as shown in [Figure 4-27](#).

Remember that your changes do not take effect until you click **Send to server**.

Blinding

Blinding occurs when the camera is obscured or the image is uniformly degraded to an unacceptably low level of contrast. This may be a result of an object placed in front of the camera lens, lens being covered with spray paint, mud or other substances, or direct bright light towards the camera (see [Figure 4-28](#)). To detect camera blinding, a significant portion of the field of view must be affected. If the camera is partially obscured, the blinding measure will remain low and not be able to trigger an alarm.

Figure 4-28 Blinding—Example of Partial and Total Blinding

Normal Scene



Partially Blinding; Tamper Not Detected



Total Blinding



Adjusting Camera Blind Threshold

1. Select the **Blind** check box (see *Figure 4-27*).
2. Adjust the Blind threshold by moving the sliding bar. *Table 4-4* provides recommended guidelines for setting the Blind threshold.

Table 4-4 Blind Threshold Values

Value	To detect ...
High (80%)	Maximum blinding. The alarm is reported when the camera view is blinded 80% or higher.
Medium (50%)	Medium blinding. The alarm is reported when the camera view is blinded 50% or higher.
Low (30%)	Minimum blinding. The alarm is reported when the camera view is blinded 30% or higher.

Blurring

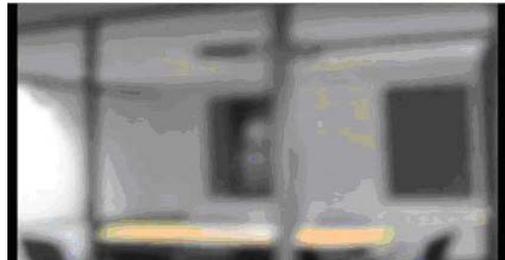
Blurring occurs when the camera lens is out of focus. When camera blur is detected, an alarm can be triggered so that an immediate action such as refocusing the lens can be taken to rectify the situation. Blur detection is not sensitive to the image resolution, type of image (black and white or color), or movement in the scene.

Figure 4-29 Blurring-Example

Normal Scene



Blurring



Adjusting Camera Blur Threshold

1. Select the **Blur** check box (see *Figure 4-27*).

- Adjust the Blur threshold by moving the sliding bar. [Table 4-5](#) provides recommended guidelines for setting the Blur threshold.

Table 4-5 **Blur Threshold Values**

Value	To detect ...
High (80%)	Maximum video blurring. The alarm is reported when the camera view is blurred 80% or higher.
Medium (50%)	Medium blurring. The alarm is reported when the camera view is blurred 50% or higher.
Low (30%)	Minimum blurring. The alarm is reported when the camera view is blurred 30% or higher.

Scene Change

Another method of camera tampering is to change the camera field of view or line of sight from its intended position. When this situation is detected, an alarm can be raised to notify the operator. When the camera's position is restored and the scene matches the original one before the alarm state, the alarm will clear automatically.

If the alarm does not automatically clear, the user can click **Reset** to manually reset the alarm state. By resetting the scene change alarm, the current scene is considered the reference view for subsequent scene change detection. The scene change alarm can also be manually reset in the Live Monitoring Station client. Please refer to [Chapter 10](#) for more detailed information.

Figure 4-30 **Scene Change–Example**

Intended Camera View



Camera View After Scene Change Tampering



Adjusting Camera Scene Change Threshold

- Select the **Scene Change** check box (see [Figure 4-27](#)).

- Adjust the Scene Change threshold by moving the sliding bar. [Table 4-6](#) provides recommended guidelines for setting the Scene Change threshold.

Table 4-6 Scene Change Threshold Values

Value	To detect ...
High (80%)	Maximum change in the camera field of view. The alarm is reported when the measure of the change in the field of view is 80% or higher.
Medium (50%)	Medium change in the camera field of view. The alarm is reported when the measure of the change in the field of view is 50% or higher.
Low (30%)	Minimum change in the camera field of view. The alarm is reported when the measure of the change in the field of view is 30% or higher.

Uploading the Configuration to the Server

After you finish configuring all the camera views, you can upload the entire configuration settings to the Video Analytics server by clicking **Send to server**. A successful upload is indicated when the status bar shows `Command sent successfully` and you receive a message notifying you that the configuration has been successfully uploaded to the server. The server automatically restarts the processing using the new configuration.

Uploading a Partial Configuration to the Server

This version of analytics software allows you to send the configuration to the server even though some channels may only be partially configured. The traffic light icon on the Channel setup page (see [Figure 4-10](#) on [page 58](#)) indicates whether or not enabled channels will be processed:

Traffic Light Icon	Indicates ...
Green 	All enabled channels will be processed.
Yellow 	Some enabled channels will not be processed. To see the first channel that will not be processed, click the yellow light.
Red 	No channels will be processed.

There are two different types of processing that the HVA server can perform on a channel:

- **Event Detection.** This processing is performed when a channel's scene setup is complete and at least one event is enabled in the Event definitions pane for that channel. If a channel's scene setup has not been completed, this type of processing will not be performed even if there are events enabled for the channel.



A green check mark in between the channel name (in the drop down list) and the traffic light indicates that scene setup for the channel is complete and event processing will be performed for the channel.



A yellow caution triangle indicates that the scene setup for the channel is not complete and event processing will NOT be performed for the channel (though camera tamper detection will still be performed if enabled).

- **Camera Tamper Detection.** This processing is performed when at least one type of camera tamper detection (blind, blur, or scene change) is enabled on the channel's Tamper Detection tab.

The traffic light icon considers that a channel will be processed if at least one of these two types of processing occurs. If tamper detection is enabled for all channels but scene setup has not been completed, the traffic light still shows green.

Managing Your Configuration

After you finish configuring the rules for all the camera views in your system, Honeywell strongly recommends that you save the configuration. To save all the settings in the **Video setup** page and the **Channel setup** page to a local configuration file:

1. From the menu bar, select **File ► Save As**.
2. After you save configuration files in your system, you can then open a local configuration file using the **File ► Open** command.
3. To modify an opened configuration file, select **File ► Save** to overwrite the current configuration file.
4. When you modify the camera input list and are about to change the current configuration, the system warns you and prompts you to save the configuration first. Follow [step 1](#) to [step 3](#) to save the current configuration.

Note The analytics server automatically backs up previous configurations on the server in the Config folder under the installed directory. This allows you to retrieve older copies of configuration if needed. It will store up to 500 backup copies of previous configurations loaded to this server.

Resolving Configuration Conflicts

Configuration conflicts may occur when:

- Multiple users are accessing the same analytics server through a Configuration Tool session
- A user is accessing the same analytics server from more than one Configuration Tool session

In either of these cases, configuration changes may occur almost simultaneously. The Configuration Tool session that sends an updated configuration to the analytics server first will succeed, and the other connected Configuration Tools will be notified of a configuration change in the order in which they are sent (see [Figure 4-31](#)).

Figure 4-31 Configuration Changed Notification



This indicates that another user or another copy of the Configuration Tool has submitted configuration change to the analytics successfully. In this case, if you have modified the same section in the configuration and click Send to Server when you finish, the configuration conflicts message shown in [Figure 4-32](#) appears.

Figure 4-32 Configuration Conflicts Message



One way to resolve the conflict is to abandon your change to the configuration by loading the current configuration from the server again. Select **File ► Refresh Configuration** from the Remote Server option. You can then re-edit your changes and send it to server when you finish.

Alternatively:

1. Select **File ► Save** to save your copy of the configuration to a file on your local machine
2. Select **File ► Open** to open this configuration file.
3. Click **Send to Server** to upload the configuration to the server.

A configuration loaded directly from a saved configuration file overwrites the existing configuration on the server and therefore no conflicts will occur.

Premium Event Configuration

There are some additional events that are only available in the Honeywell Video Analytics Active Alert Premium package. These events require specific camera setup and additional operating conditions.

This chapter covers the conditions and how to configure these premium events.

Object Left Unattended and Object Removed Events

Conditions for Deploying Premium Events

To achieve high detection rate of these advanced events, the following operating conditions must be met.

Note This list contains additional operating conditions to the standard operating conditions for using the software as described in [Chapter 4](#).

Table 5-1 Premium Events Operating Conditions

Condition	Explanation
Camera position	Camera must be placed to cover the entire area where this event may occur.
Camera angle	Must minimize potential occlusion between various moving people in the scene. Avoid any visual barriers in the scene (such as pillars, poles, and trees) if possible. If visual barriers cannot be avoided, Honeywell recommends adding a second camera, which offers a second angle for viewing.
Object position in scene	The part of the scene where the object is left unattended must be fully contained inside the scene. If it is placed at the scene boundary, there is the potential for poor detection and performance.
Minimum size of object	Must be at least 5% of the size of a <i>typical</i> person (as configured in the person examples during scene setup) or occupying at least 20 pixels in the camera view, whichever is greater.
Maximum size of object	Must be at most 70% of a person (as configured in the person examples during scene setup).
Time duration	The object must stay in the scene before the alarm triggers a minimum of 2 seconds to a maximum of 120 seconds.
Maximum distance of the object to the camera	For an object the approximate size of 1 foot (30 cm) cube, the maximum distance of the object to the camera is approximately 50 feet (15.24 m), assuming 1/3-inch CCD sensor and 4 mm lens, to 100 feet (30.48 m), assuming the camera sensor has 1/3-inch CCD and 8mm lens.
Detection zone	A <i>detection zone</i> must be used to mark the area where the detection of this event is in effect.

Configuring an Object Left Unattended Event

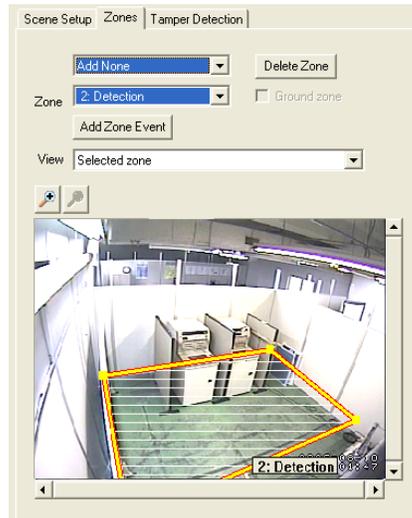
The **Object Left Unattended** event is designed to detect an object being left unattended (usually by a person). Given the wide variety of objects that a person may deposit in a scene and leave unattended, the aforementioned operating conditions must be strictly met for proper use of this advanced event.

An example scene is shown in [Figure 5-1](#). To configure an **Object Left Unattended** event:

1. Add a detection zone to mark this monitored area.

Note The detection zone needs to cover the image area where, if an object is left unattended, it should cause an alarm condition.

Figure 5-1 Setup of a Detection Zone for Object Left Unattended



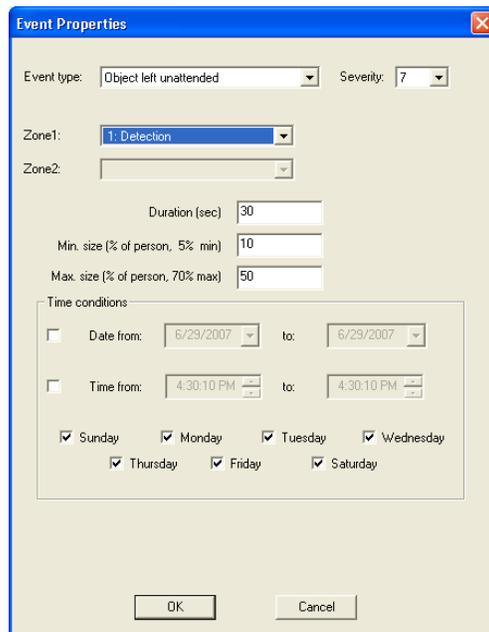
2. After you configure the detection zone, you can add the **Object Left Unattended** event.

There are three additional parameters for this event that you can adjust (see [Figure 5-2](#)):

Table 5-2 Object Left Unattended Event Parameters

Parameters	Description
Duration (sec)	The duration (in seconds) for the object to be left in the scene before an alarm triggers. For applications where an immediate alarm is required, set this to a short duration such as 2 to 5 seconds. For most applications, a longer duration is more suitable to ensure that the object has been left in an unattended fashion and will, in fact, be abandoned. The default value is 30 seconds. The software allows a minimum of 2 seconds and a maximum of 120 seconds for this parameter.
Minimum size (% of person)	The minimum size of the object to be detected, represented by a percentage of the person size which is set up as person example boxes during scene setup. The software allows a minimum object size to be 5% of a representative person or 30 pixels regardless of where the object appears in the detection zone.
Maximum size (% of person)	The maximum size of the object to be detected, represented by a percentage of the person size which is set up as person example boxes during scene setup. The software allows a maximum object size to be 70% of a representative person in the scene regardless of where the object appears in the scene.

Figure 5-2 Event Parameters for Object Left Unattended



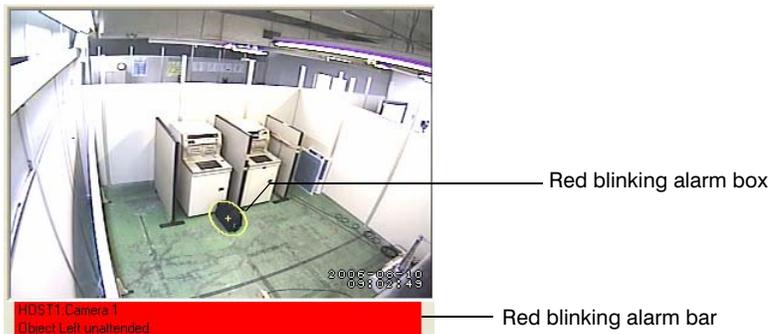
Camera placement is crucial to deliver optimal performance of this feature. The ideal camera position is:

- High above ground with minimum potential occlusion between various moving objects in the scene
- No pillars or other visual barriers that can block the view of the left object

The primary monitoring area should also be at the near range in the camera view and centered in the image. Should the action (leaving the object) take place near the image boundary such that the object is only partially seen, detection performance will be low. In such cases, Honeywell recommends that you install a second camera centered on the image boundary of the first camera with the **Object Left Unattended** event enabled.

Figure 5-3 shows the alarm screen on the Live Monitoring Station client application when the **Object Left Unattended** event is detected. A red blinking alarm box is positioned around the unattended object and a red blinking alarm bar appears for the alarmed camera view.

Figure 5-3 Alarm Screen for Object Left Unattended Event



Configuring an Object Removed Event

The **Object Removed** event is designed to detect a specific object (marked by an asset zone) being removed from the scene. Given the wide variety of objects that need to be protected from being removed in the scene, the operating conditions listed in [Configuring an Object Left Unattended Event](#), page 86 must be strictly met for proper use of this advanced event.

In *Figure 5-4* there are two asset zones set up to mark the two garbage bins in the scene to protect them from being removed. It is critical that the asset zone matches closely to the boundary of the protected asset, as depicted in the example. If the asset is moved to a different location, the asset zones must be re-configured to match the new location of the asset.

Figure 5-4 Examples of Asset Zones to Detect Object Removed



Use the **Zoom** tooltip on the left of the image to zoom in to carefully draw the asset zone along the boundary of the object you want to protect from being removed (see [Figure 5-4](#)). Click **Zoom-in** to zoom in 2x, 4x, 8x, and so on. In the zoomed-in mode, you can also point and drag the entire image or use the scroll bars to move the focus to the desired area in the image.

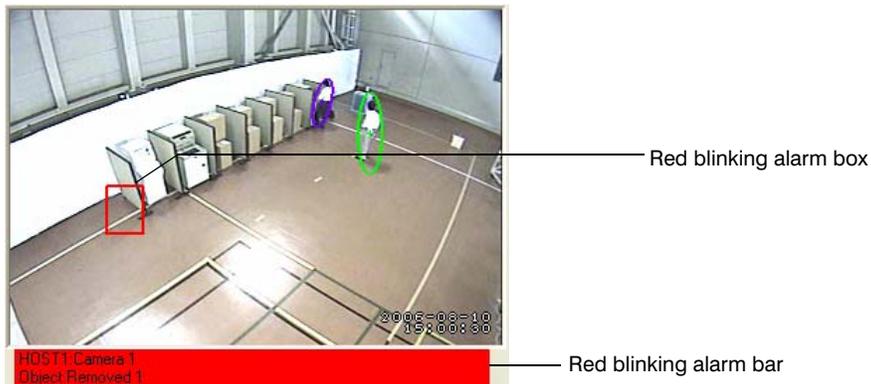
Similar to the detection of **Object Left Unattended**, camera placement plays a crucial role to deliver optimal performance of the detection of **Object Removed** event. The ideal camera position is:

- High above ground with minimum potential occlusion between various moving objects in the scene
- No pillars or other visual barriers that can block the view of the left object

The primary monitoring area should also be at the near range in the camera view and centered in the image.

[Figure 5-5](#) shows the alarm screen as it appears in the Live Monitoring Station client application when the **Object Removed** event is detected. A red blinking alarm box is positioned around the original location of the removed asset and a red blinking alarm bar will appear for the alarmed camera view.

Figure 5-5 Alarm Screen for Object Removed Event



Possible Theft

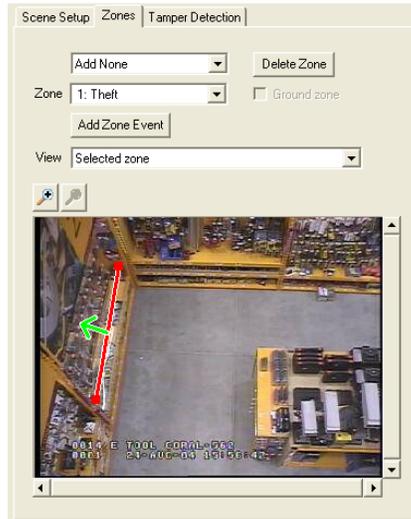
The **Possible Theft** event is designed to detect anyone reaching into a specific retail shelf more than the maximum allowed number of times.

Please keep in mind that this event is designed to only draw the attention of the security operator, or to annotate interesting sections of video for later forensics. It is called possible theft precisely because human judgment is required to evaluate each particular situation.

An example scene is shown in [Figure 5-6](#), where the shelf in the upper left corner holds merchandise that is often stolen. To set up the Possible Theft event:

1. Select a theft zone, which consists of a line and an arrow.
 - a. The line should be placed between people standing in the aisle and the protected merchandise, so that a person has to reach across the line to remove any items from the shelf.
 - b. The arrow tip points inside the shelf.
 - c. The length of the arrow controls how deep the person has to reach in - each reach-in that is at least 25% of the arrow length gets counted. The recommended length of the arrow depends on the exact situation, but it tends to be about arm's length in the camera view.

Figure 5-6 Zone Definition - Theft Line



2. The **Possible theft event** has two additional parameters (see [Figure 5-2](#)):

Table 5-3 Possible Theft Event Parameters

Parameters	Description
Duration (sec)	If the person is next to the shelf for less than the minimum duration parameter, the event is not reported. The duration must be between 1 and 120 seconds. The default duration is 10 seconds.
Number of reaches	In most situations, this second parameter is more important. If the number of reaches is set to 5, a person is allowed to reach into the shelf 4 times. An alarm is raised when they reach into the shelf for the fifth time. The counter resets after the alarm and if the person continues to reach into the shelf, a second alarm is raised on reach number 10, and so on. The number of reaches must be between 1 and 20. The default is 5 times.

Figure 5-7 Event Parameters for Possible Theft Event

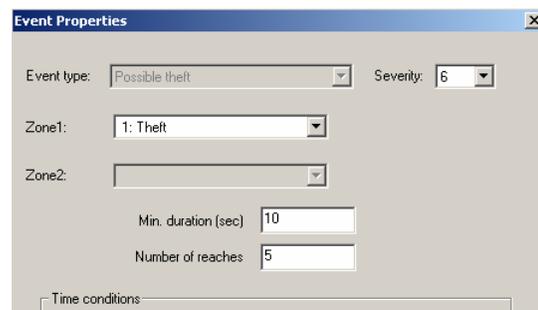
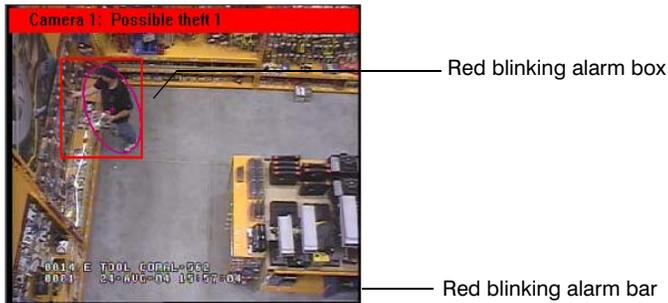


Figure 5-8 Alarm Screen for Possible Theft Event



Camera placement is crucial to guarantee good performance of this event detector. The ideal camera position is overhead above the shelf, looking straight down. If the person can reach between multiple shelves, the camera should be offset slightly (1 ft.) into the aisle, so that more of the hand is visible.

The view in *Figure 5-8* is slightly less ideal, because there may be occlusion if multiple customers stand side by side. But the view can be used, because the camera can see a person reaching in to the shelf to take the merchandise.

Note It is not possible, in this view, to detect customers reaching into the far shelf in the upper part of the image. The camera would see the back of the customer but the hand reaching into the shelf would not be visible at all.

Overhead People Counting

The Honeywell Video Analytics People Counting is a product package that is specific to people counting applications. People counting is a feature that requires very detailed and careful setup. This chapter describes how to set up overhead people counting, including:

- [Deploying Environment Requirements—Single Camera](#) describes the environment requirements including the ceiling height, door width, and type of door as well as lighting conditions. It also describes how to place the camera and select a lens.
- Checking the placement of a camera (see [page 97](#))
- Configuring the software for optimal performance (see [page 106](#))
- Testing and tuning your configuration (see [page 116](#))

Note For best performance and highest efficiency, use QCIF size image instead of CIF for overhead people counting.

This version of Video Analytics software also supports wide-entrance people counting that uses multiple cameras along a single wide entrance. See the following section for deployment requirements. Wide-entrance people counting requires set up of camera groups and calibration procedure to ensure the correct functionality of this feature. See [Chapter 7, Camera Groups](#) and [Chapter 8, Camera Calibration](#) for details.

Deploying Environment Requirements—Single Camera

At a standard interior door using a single camera, the People Counting feature can reach over 95% accuracy when deployed in a suitable environment with strictly overhead camera placement. This section lists the deployment environment requirements for optimal performance.

The most common deployment scenario is to install a single camera to count people passing through either a single (3-foot) or double (6-foot) door. To determine if your environment is suitable for people counting, consider the environment requirements in [Table 6-1](#).

Table 6-1 People Counting Environment Considerations—Single Camera

Consideration	Description
Ceiling height	<p>The height of the ceiling dictates the height of the camera or the distance from the camera lens to the person that passes under the camera. The minimum distance from the lens to the floor is 10 feet.</p> <p>Note If the ceiling type or ceiling height does not allow such distance, do not use the overhead people counting feature.</p>
Door width	<p>Given a ceiling height between 10 to 12 feet, the door width cannot be more than 6 to 8 feet, respectively, to use a single camera for overhead people counting.</p> <p>Caution For wider doors or passages that require multiple cameras, the door or entrance width can be extended to a maximum of 48 feet. See page 115 for detailed requirements.</p>
Door type	<p>Open passages through a corridor with proper width and without a door opening or closing is the simplest door type. If all other requirements are met, this type of environment is suitable for overhead people counting.</p> <p>For swinging doors, it is important to know the direction of the door swing, and sometimes the speed of the door swing. The direction of the door swing affects the camera placement. You should always place the camera on the opposite direction of the door swing (see page 97). In the case of covering an entrance or exit, most building codes require that the door swings out. In these cases, the camera should be placed inside. The swinging speed may affect your decision on which types of zones to configure to ignore the movement of the swinging door (page 106).</p> <p>Sliding doors are generally a good environment for deploying overhead people counting.</p> <p>Note The current people counting feature should not be deployed at transparent or glass doors that open out to an outdoor environment with direct sunlight. However, transparent doors in an indoor environment with ambient lighting can be suitable for overhead people counting.</p>
Lighting conditions	<p>Uniform artificial light is the best lighting condition for overhead people counting.</p> <p>Lighting environments that are not suitable for the people counting feature are:</p> <ul style="list-style-type: none"> • Where strong direct sunlight is present most of the time. • Where there is strong direct sunlight during a time of high traffic, such as a building doorway at change of shift.

After carefully considering the environment where people counting deployment is proposed, the specification of the camera placement and lens must also be examined (see [Positioning Overhead Camera—Single Camera](#), page 97).

Positioning Overhead Camera—Single Camera

Table 6-2 lists a few requirements in camera placement for overhead people counting.

Table 6-2 People Counting Camera Placement Requirements

Requirement	Description
Orientation	The camera must be placed overhead, pointing strictly down towards the floor. See page 99 on how to verify the camera is correctly placed in the overhead position.
Height	From the camera lens to the floor, there must be a minimum distance of 10 feet. Generally speaking, a higher camera placement provides a better view and therefore higher counting accuracy. Typically, for a 3 to 6 foot door, the optimal camera height is within the range of 10 to 12 feet (3.05 m to 3.66 m) from the floor.
Position	For a swinging door, the camera must be placed on the opposite side of the door swing to have maximum visibility of the persons and minimum door movement in the field of view (FOV). Typically the camera is mounted on the ceiling approximately 1 to 2 feet (0.3 m to 0.6 m) away from the door.

Honeywell suggests several possible camera placements that suit most indoor environments for people counting. The first choice is recommended for single door (3-ft. wide) and the second choice is preferred for double-door (6-ft. wide) openings (see [Figure 6-1](#) and [Figure 6-2](#)). The camera should be mounted so that the door opens away from the camera. If the camera must be mounted where the doors swing towards the camera, the mounting point should be further away from the door, as in [Figure 6-2](#).

When considering a camera lens, Honeywell recommends selecting a lens that provides an additional 4 feet (1.22 m) of floor coverage on either side of the door threshold. For a 6-foot door opening, the minimum floor coverage should be 14 feet by 10 feet (4.27 m x 3.05 m) in the FOV of the camera (see [Table 6-3](#)). Three parameters affect the FOV:

- Ceiling or camera height
- Size of the CCD array within the camera
- Lens size

Table 6-3 Common Specification for Camera Mounting and Lens

Choice	Height (ft)	CCD (inch)	Lens (mm)	FOV (ft)
1	10	1/3	4.0	12 x 9
2	12	1/3	4.0	14 x 10

The wider the lens, the wider the floor coverage. Therefore, for wider doors, you may need to use a wider-angle lens (< 3.6 mm) to have sufficient camera coverage. The widest camera lens that can be used with Honeywell Video Analytics software is 2.8 mm with a 1/3 inch CCD.

Figure 6-1 Single, 3-Ft Door Opening Example

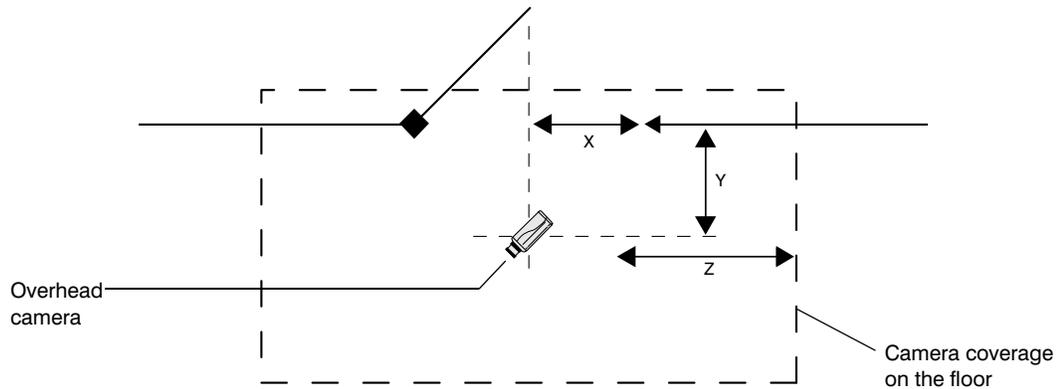
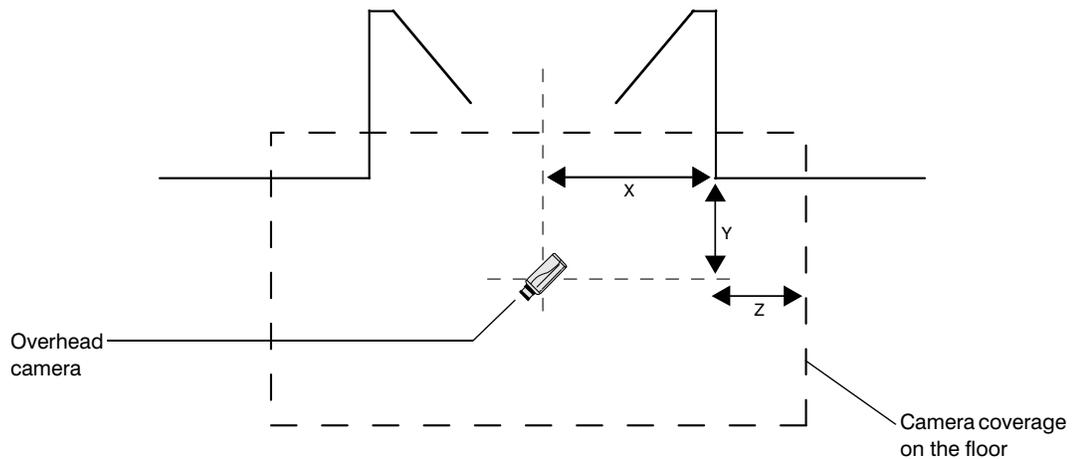


Figure 6-2 Double, 6-Ft Door Opening Example



In both cases (see [Figure 6-1](#) and [Figure 6-2](#)):

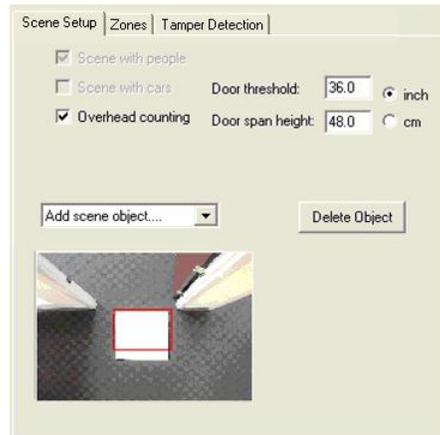
- Distance **X** should be one half of the opening width, so that the camera is centered with respect to the single or double door.
- Distance **Y** should ideally be 3 feet (.91 m). Depending on the ceiling structure, it may not be possible to mount it exactly at that distance > Any distance between 2 and 5 feet (0.6 and 1.5 m) is acceptable.
- Distance **Z** is the additional floor coverage outside the door threshold. It should be a minimum of 4 feet (1.22 m). This ensures that people who lean next to the door frame while passing through the door are clearly visible in the camera view.

Verifying the Camera Placement

After mounting the camera with the proper lens, you must verify the overhead camera placement:

1. Verify the camera is pointed strictly down in an overhead position.
2. Verify there is sufficient floor coverage given the camera height and lens combination.

Figure 6-3 Overhead Camera Placement Verification—Red Box



Verifying the Camera Position

To verify the overhead camera position:

1. Place a 2 foot x 2 foot sheet of paper on the floor directly under the camera. We suggest the use of a plum line (weighted string) to verify the placement of the paper.
2. Start the Configuration Tool client.
3. Add the camera as a video source and select this camera for processing.
4. In the **Scene Setup** section on the **Channel setup** page, check **Overhead counting**.
5. A red box appears in the center of the image, which is the image center marker. Make sure that the 2' x 2' sheet you have placed on the floor appears in the center of the red box (see [Figure 6-3](#)). If not, re-adjust the camera angle to have it point straight down and repeat this step.

Verifying the Floor Coverage

The camera FOV should allow floor coverage that exceeds the door width by 4 feet from either end of the door threshold to allow tracking of people passing through the door from all possible directions. Examine the camera view to make sure the camera coverage is wide enough. If not, either raise the camera height or use a wider angle lens to gain more floor coverage.

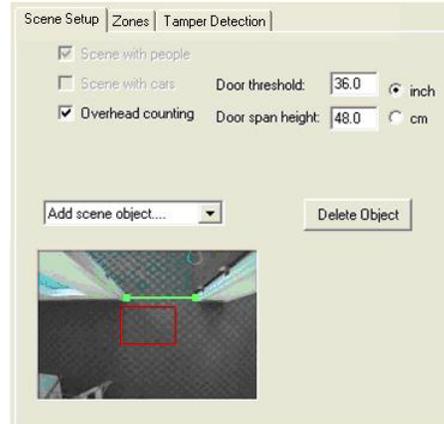
Configuring Door Threshold and Door Span Scene Objects

To increase the accuracy and performance of the people counter feature, knowledge of the doorway location and size is required. This configuration procedure maps the physical structure in the scene (including the door threshold and an imaginary horizontal bar called the door span) to the image coordinates. By having these measurements, the system can achieve high accuracy in people counting.

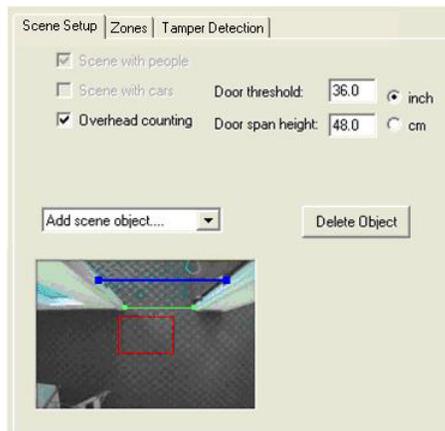
To configure a doorway, you need to specify the location and width of the door threshold and the height of a second line specifying the doorway span:

1. Select **Overhead view, Add scene object ...**
2. There are two choices in the drop down box: Add door threshold and Add door span.
3. Select **Add door threshold**.
A green line appears on the image.
4. Move your mouse to one endpoint of the line, then left-click and drag the point to one end of the door threshold in the image. Move the other endpoint to the other end of the door threshold (see [Figure 6-4](#)).
5. In the **Door threshold** field, type the actual length of the door threshold (in inches or centimeters). The default is 30 inches for a standard 3-foot door.

Figure 6-4 Define the Door Threshold—Green Bar



6. To configure the second parameter, select **Add door span** to define a line that goes across the width of the door at a known height.
A blue line appears on the image.
7. Move your mouse to one endpoint of the line, then left-click and drag the point to one end of the line that goes across the width of the door.
8. Move the other endpoint to the other end of the door span at the opposite side of the door frame at the same height (see [Figure 6-5](#)).
9. In the **Door span height** field, type the actual height of the horizontal door span (in inches or centimeters). The minimum door span height is 48 inches.
You must define exactly one door threshold and one door span.

Figure 6-5 Define a Door Span—Blue Bar and a Fixed Height Horizontal Bar

Ignoring Door Movement

In some cases the software sees door movement in the camera view. There are various ways to configure the scene so that such door movement may be ignored by the software for more accurate counting.

Using Object-Block Zone

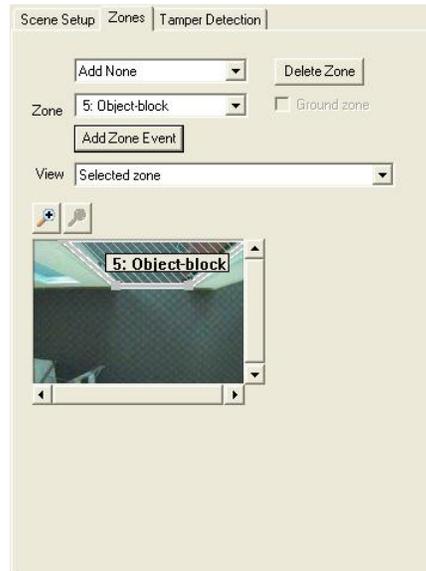
Since the people counter camera is typically installed above a doorway, the door itself is normally within the camera FOV. We recommend using an **object-block zone** to filter out the repetitive motion of the door opening and closing.

To define an object-block zone:

1. Select **Add object-block zone** from the **Add zone** drop-down list. A quadrilateral is shown in the display area.
2. Using *Figure 6-6* as an example, the camera view covers the door movement area, as well as the see-through and reflective glass panel next to the door. Therefore, the best use of the object-block zone is to place one zone over the door (including door hinges), and another covering the glass panel.

Note **Object-block zone** can overlap other zone types, including inside and outside zones, without impeding people tracking and counting capabilities.

Figure 6-6 Object-Block Zone Used to Filter Out Door Movement



If an object-block zone is used for filtering out the door movement, see [page 106](#) to configure the inside and outside zones.

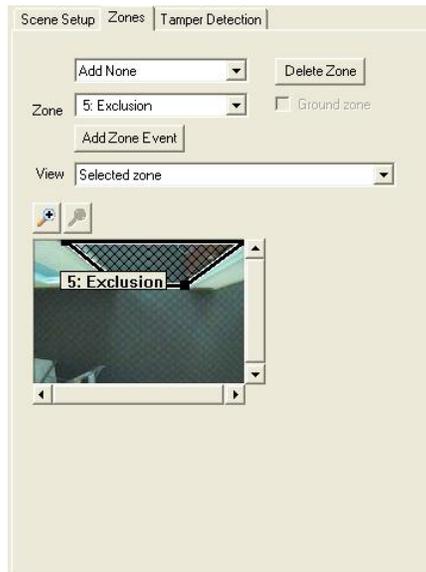
Using an Exclusion Zone

Occasionally, you may face a very slow moving swinging door, or a door that has a see-through window that allows drastic light change. In this case, consider an alternative configuration that uses an **exclusion zone** to completely mask out the entire door area for better counting accuracy.

To define an exclusion zone:

1. Select **Add exclusion zone** from the **Add zone** drop-down list.
A quadrilateral is shown in the display area. Place an exclusion zone to cover the entire door area (see [Figure 6-7](#)).
2. If the door area covers too much area in the image, Honeywell recommends that you move the camera mounting location further away from the door but still pointing the camera straight down (that is, overhead view). This way, you can reduce the door area in the image and therefore reduce the area that is completely excluded from processing.

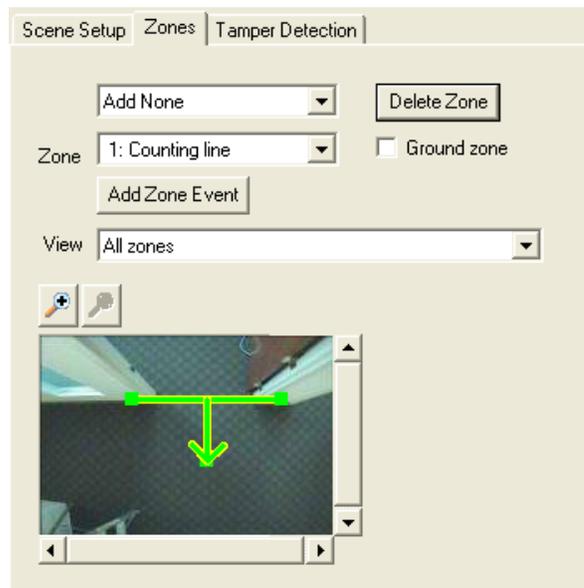
If an exclusion zone is used for filtering out the door movement, see [page 106](#) on how to configure the inside and outside zones.

Figure 6-7 Exclusion Zone Used to Mask Out Door Movement

Configuring Counting Line

For overhead people counting, the counting line is used. The counting line is a multi-segment line that contains multiple user-defined joints to shape the line to match the physical border that separates the interior space from the exterior space. From the middle of the line, an arrow points to one side of the counting line to indicate the enter direction. A person who goes across the line along this direction will be counted as **enter**. Someone crossing the line in the opposite direction will be counted as **exit**.

Figure 6-8 Counting Line for People Counting



To configure a counting line:

1. Select **Add Counting line** from the **Add zone** drop-down list. A line segment with an arrow (similar to a trespassing line) is shown in the display area (see [Figure 6-8](#)).
2. To reposition the line, place the mouse on either end of the line, then press and hold the left mouse button and move the end point to the desired location. Release the button to affix that anchor.
3. To define the enter direction, place the mouse on the arrowed head of the line, then press and hold the left mouse button and move the arrowed head to point to the enter direction.
4. You can add or delete a joint add or remove a segment of the line, as follows:
 - a. Place the mouse on any joint of the line, then press and hold the right mouse button. A pop-up menu with Add and Delete options will appear.
 - b. Move the mouse to the desired selection (see [Figure 6-9](#)). A maximum of 24 segments are allowed to form the line.
5. The line-base people counting events person counted as entering (line) and person counted as exiting (line) will be added to the event list automatically with the default severity level (see [Figure 6-10](#)). Double-click on the event in the Event definitions section to change its severity level to the desired level.

Figure 6-9 Counting Line - Add or Delete a Joint

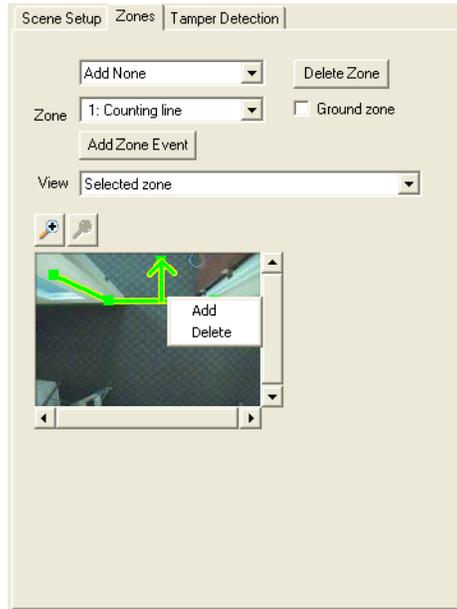
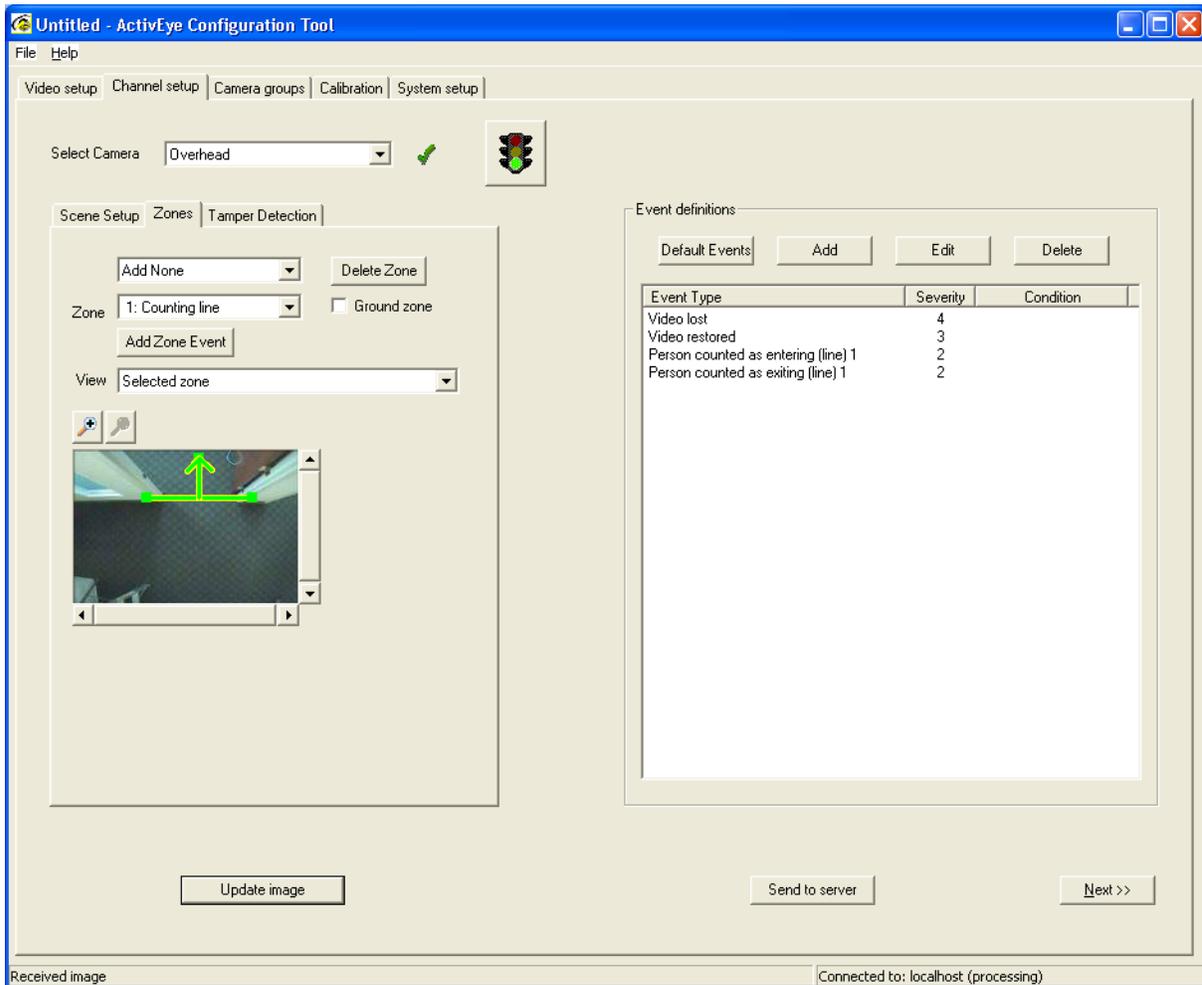


Figure 6-10 Line-Based People Counting Events



Configuring Inside and Outside Zones

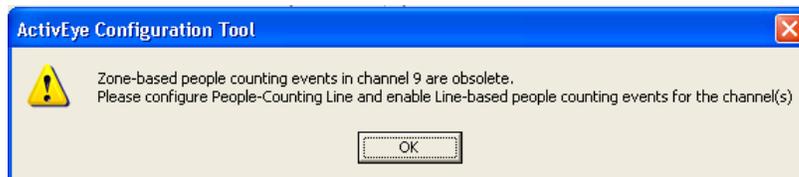
Note This section—covering the use of inside and outside zones for overhead people counting—applies to systems using or upgraded from Video Analytics V4.7 and earlier with a legacy configuration.

If any enabled channel uses zone-based people counting, you will be prompted to convert the configuration to use counting line instead (see [Figure 6-11](#)). After you have converted to counting line, the inside and outside zones will be disassociated with the people

counting events and no longer available to use for that channel. You must have both inside and outside zones defined to enable counting events such as **person counted as entering** and **person counted as exiting**.

Depending on whether you use an **object-block zone** or an **exclusion zone** to filter out the door movement, you need to set up the inside and outside zones in different ways. The following sections describe the preferred setup for each configuration.

Figure 6-11 Message Reconfiguration

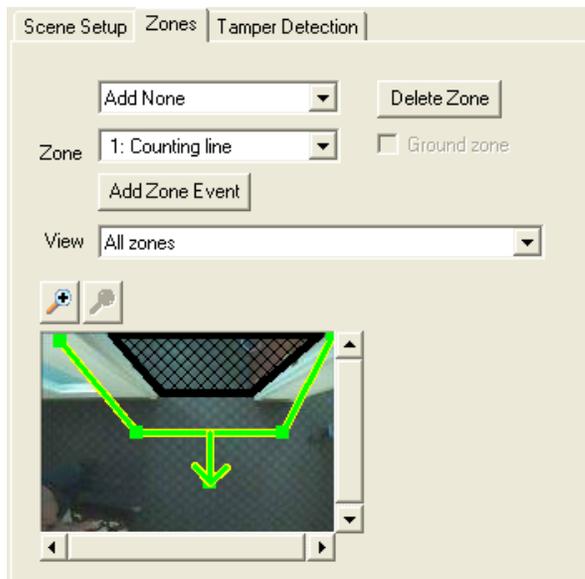


Inside and Outside Zones—Object-Block Zone at a Door

When an **object-block zone** is used, there is more available room in the image for you to place inside and outside zones. To define an inside zone:

1. Select **Add inside zone** from the **Add zone** drop-down list. A quadrilateral is shown in the display area.
2. Place the mouse on one of the anchors, press and hold the left mouse button and move the anchor to the desired location. Release the button to affix that anchor.
3. The other three anchors can be positioned in the same way (see [Figure 6-12](#)).

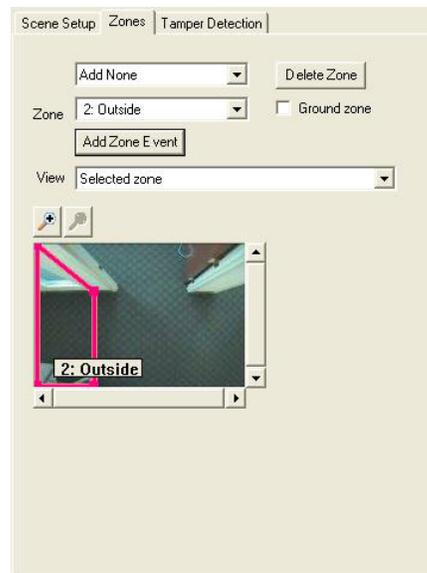
Figure 6-12 Define an Inside Zone—Door to a Meeting Room



4. Place the inside zone to cover the area where it is considered *inside*. As in [Figure 6-12](#), the inside zone is placed at the doorway into the meeting room, as it is considered inside while the corridor is considered outside. The system is now set up to count people entering the meeting room and exiting from the meeting room.

Note The best placement of an inside or outside zone is starting from the frame boundary to allow the maximum distance between an inside and an outside zone. Also, the thickness of the zone along the travel direction should be able to contain at least one person. These settings ensure optimal system performance.

Figure 6-13 Outside Zone—Placed at the West Side of a Corridor



You may configure multiple inside zones and multiple outside zones in each camera view. The number of zones you need depends on the physical layout of your facility. For example, in [Figure 6-13](#), you may need three quadrilateral outside zones to cover all three directions (west, south, and east) where a person may come to the corridor and then enter the meeting room through the inside zone that has been defined.

To add an outside zone:

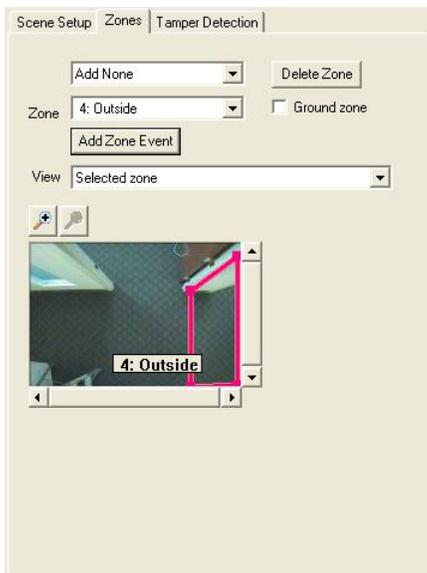
1. Select **Add outside zone** from the **Add zone** drop-down list.
2. Place the first outside zone at the west direction of the corridor, aligning with the frame boundary, as in [Figure 6-13](#).

Note Be aware that an outside zone must not overlap with an inside zone. Check your zones and make sure they do not overlap.

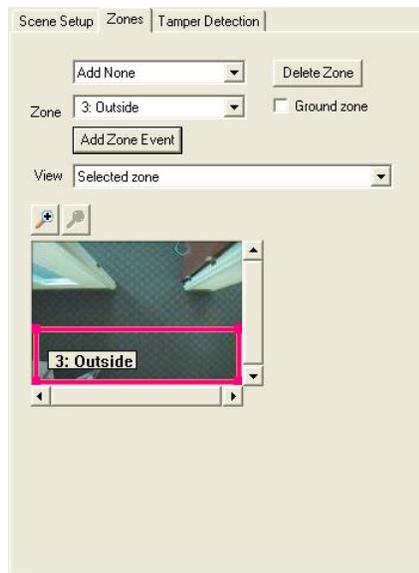
3. Select **Add outside zone** again to add two more outside zones to cover the east side and the south side of the corridor (see [Figure 6-14](#)). The outside zones can overlap to ensure a complete coverage of all possible entry points to the corridor area. Similarly, if you need multiple inside zones for a different camera field of view, the inside zones can also overlap with one another.

Figure 6-14 Outside Zone Examples

A. Added to the East Side of a Corridor

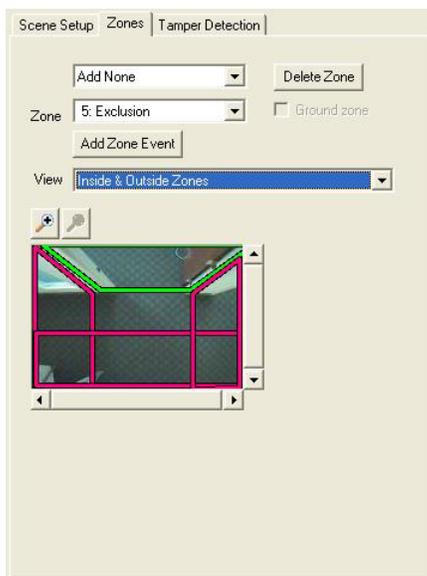


B. Added to the South Side of a Corridor



You can select **View Inside & Outside Zones** to view all the inside and outside zones currently defined for the camera view, as shown in [Figure 6-15](#). This makes it easy to verify that all the traffic paths are covered and the two groups of zones do not overlap.

Figure 6-15 View All Inside and Outside Zones



Legend

Green = inside zone
Pink = outside zone

Using Inside and Outside Zones With an Exclusion Zone

When an **exclusion zone** is used, you lose some of the image area where inside and outside zones can be placed since they must be placed outside of the exclusion zone to take effect. Therefore, the best placement for both inside and outside zones is different from the previous case where no exclusion zone was used to block the door.

To define an inside zone:

1. Select **Add inside zone** from the **Add zone** drop-down list. A quadrilateral is shown in the display area.
2. Place the mouse on one of the anchors, press and hold the left mouse button and move the anchor to the desired location. Release the button to affix that anchor.
3. If desired, position the other three anchors in the same way (see [Figure 6-12](#)).
4. Since the exclusion zone is used to mask out the entire door area, place the inside zone to cover the area immediately outside the door (below the exclusion zone). An example of this is shown in [Figure 6-12](#). This essentially pushes the inside zone outwards.

Figure 6-16 Define an Inside Zone—Door to a Meeting Room

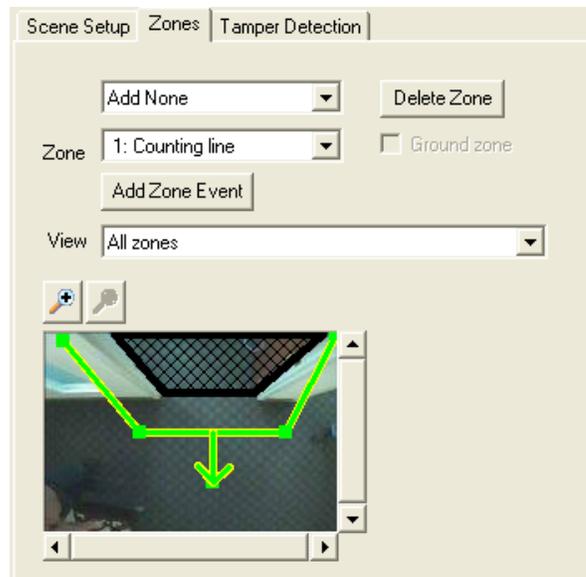
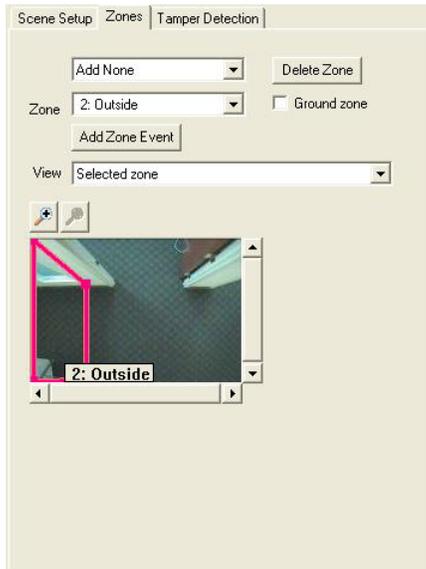


Figure 6-17 Outside Zone—Added to the West Side of a Corridor

You may configure multiple inside zones and multiple outside zones in each camera view. The number of zones you need depends on the physical layout of your facility. For example, in [Figure 6-17](#), you may need three quadrilateral outside zones to cover all three directions (west, south, and east) where a person may come to the corridor and then enter the meeting room through the inside zone that has been defined.

To add an outside zone:

1. Select **Add outside zone** from the **Add zone** drop-down list.
2. Place the first outside zone at the west direction of the corridor, aligning with the frame boundary, as in [Figure 6-17](#).

Note Be aware that an outside zone must not overlap with an inside zone. Check your zones and make sure they do not overlap.

3. Select **Add outside zone** again to add two more outside zones to cover the east side and the south side of the corridor (see [Figure 6-18](#)). The outside zones can overlap to ensure a complete coverage of all possible entry points to the corridor area. Similarly, if you need multiple inside zones for a different camera field of view, the inside zones can also overlap with one another.

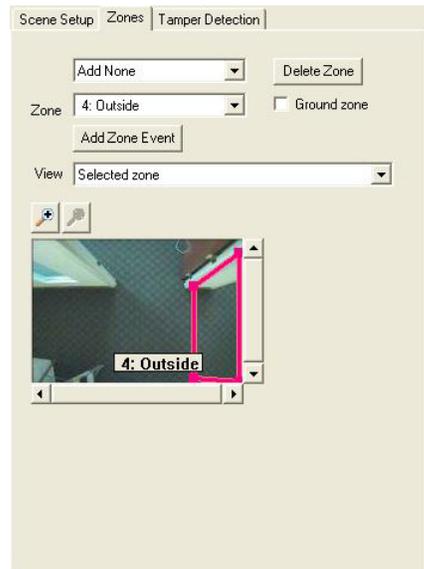
Note The outside zones are configured in a similar way to the previous case when Object-block zone is used, but moved outwards to accommodate the shifted location of the inside zone (seen [Figure 6-17](#) and [Figure 6-18](#)).

With this slight variation, you can still set up the system to count people entering and exiting the meeting room.

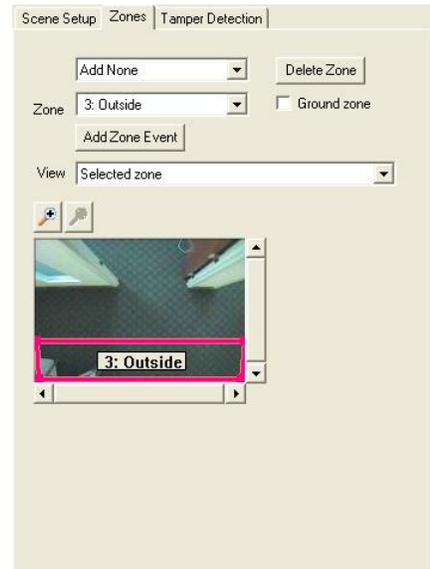
Note The best placement of an inside or outside zone is starting from the exclusion zone boundary to allow the maximum distance between an inside and an outside zone. Also, the thickness of the zone along the travel direction should be able to contain at least one person. These settings will ensure optimal system performance.

Figure 6-18 Outside Zone Examples

A. Added to the East Side of a Corridor



B. Added to the South Side of a Corridor

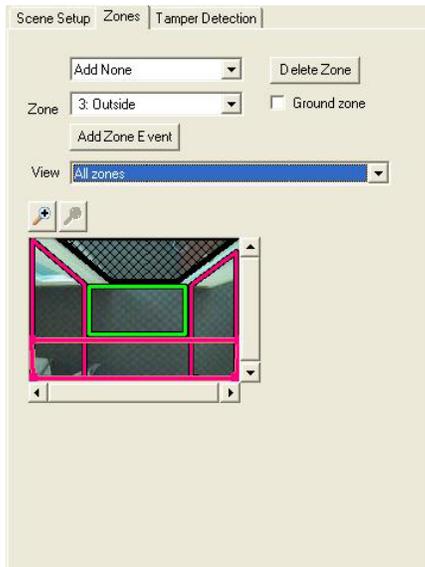


Verifying Placement of All Zones

To ensure that all traffic paths are covered:

1. Select **View All Zones** to view all the inside and outside zones as well as the exclusion zone that are currently defined for the camera view (see [Figure 6-19](#)).
This makes it easy to verify that all inside and outside zones are placed correctly to cover all the traffic paths and the two groups of zones do not overlap.
2. Also, Honeywell recommends that you verify that the inside and outside zones are not masked out by the exclusion zone.

Figure 6-19 View All Zones

**Legend**

Green = inside zone
 Pink = outside zone
 Black = exclusion zone

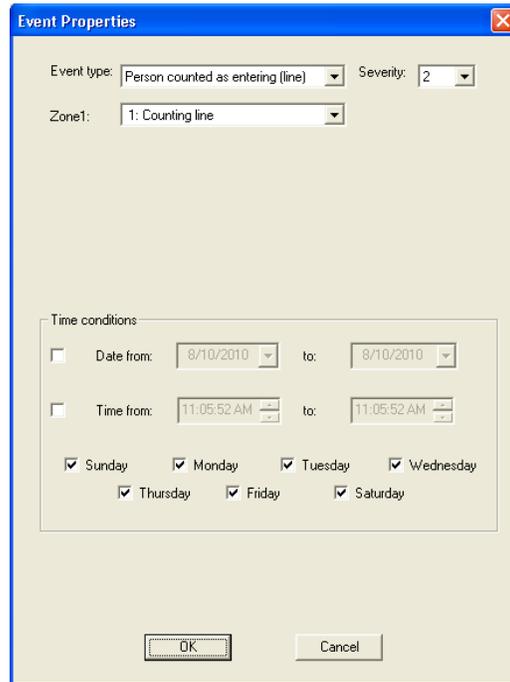
Setting Up Zone-Based People Counting Events

To set up zone-based **people counting** events:

1. With either an Inside or Outside zone selected, click **Add Zone Event** in the Zone tab on the **Channel setup** page.
2. An Event Properties dialog box appears. From the **Event type:** drop down list, select **Person counted as entering zone**.

You will see the **Zone1:** and **Zone2:** fields are automatically filled as **Zone1: Outside zones** and **Zone2: Inside zones** (see [Figure 6-20](#)). Change the severity level to the desired level for this event.

Figure 6-20 Add Person Counted as Entering Event



3. Similarly, click **Add Zone Event** again in the Zone tab to add the **person counted as exiting (zone)** event. Set it to the desired severity level.

Counter Reset Schedule

You can set the counter daily reset schedule for both people counting and car counting events.

Wide-Entrance People Counting

There are situations where the door or entrance spans beyond a standard single or double door, and multiple cameras must be used in order to cover the entire entrance way in order to accurately count all the people entering and exiting through the entrance. By proper positioning of multiple cameras lined up along the wide entrance and correct calibration of adjacent cameras with overlapping views, the wide-entrance people counting feature extends the capability of the standard single-camera based people counting system to suit a wider range of deploying environments.

Special Requirements

Each single camera in a wide entrance people counting system must meet the same deployment environment requirements as the single camera setup described in [Deploying Environment Requirements—Single Camera](#), page 95.

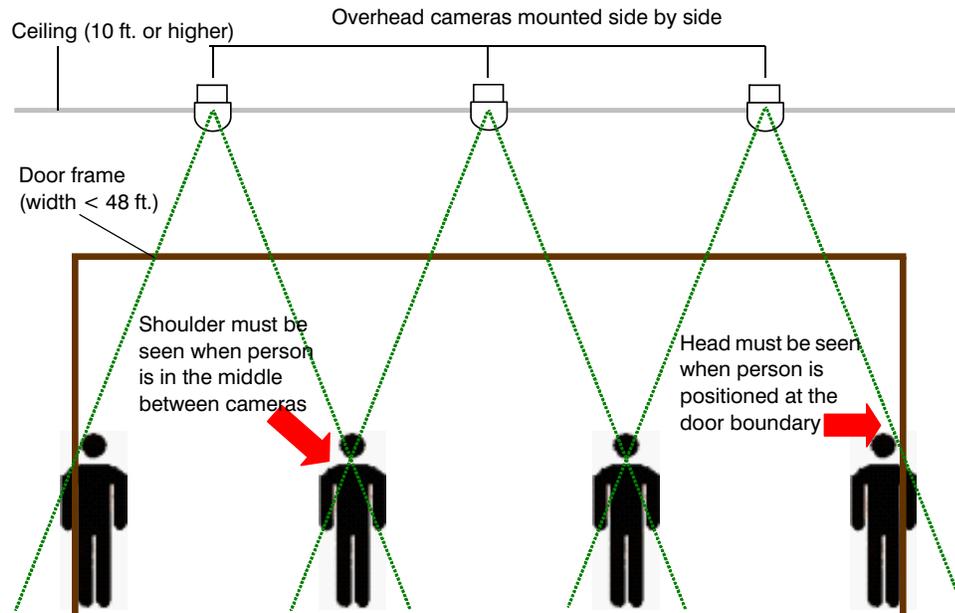
For wide-entrance people counting applications, there are some additional requirements for camera placement in order to achieve the best performance. These requirements are listed in [Table 6-4](#).

Table 6-4 Wide Entrance People Counting Requirements

Requirement	Description
Alignment	Cameras must be placed along a straight line that spans across the wide entrance. They must be properly aligned to be at the same horizontal distance to the door frame.
Overlapping views	Adjacent cameras must have overlapping views, so that if a person stands right in the middle between the two cameras, his or her shoulder (at approximately 80% of the person height) must be visible in both cameras. Moreover, only adjacent camera pairs should have overlapping views. That is, a person is only seen in at most two cameras.
Coverage	The complete camera coverage must include extra floor space outside of the door frame or the end wall, so that if a person leans at the boundary of the door or at the wall, his or her head (full height) will be visible in one of the cameras.
Maximum door/entrance width	The width of each wide door or entrance way must be no more than 48 feet.

[Figure 6-21](#) shows the appropriate multiple-camera placement for wide-door people counting application.

Figure 6-21 Wide Entrance People Counting—Appropriate Camera Placement



The setup of inside/outside zones and counting events for each people counting camera at a wide entrance remains the same as in the single-camera case as detailed in previous sections of this chapter. Additional setup procedure required for wide entrance people counting including setting up camera groups and calibration data are described in [Chapter 7](#) and [Chapter 8](#).

Field Testing and Tuning Procedure

To ensure highest counting accuracy, conduct field testing and tuning after you have configured the system either for the first time or after a readjustment. The testing and tuning procedure should be applied for each single counting camera independently.

This section describes how to field test and tune the system to best adapt to the variations in height and shape of people in the environment.

There are two types of adjustments:

- Scene object adjustment
- Zone adjustment

This procedure may require a few other people on site to assist you in the process, preferably covering a range of body types.

Scene Object Adjustment

This procedure tests the settings of the door threshold and span to ensure they are optimal for best counting accuracy. Test with the door open the entire time, so that there is no door movement. Place a door stop or some object to hold the door open during the test.

There are two parts in this adjustment procedure: single person test and two people test.

Single Person Test

With a minimum of two people on location (one small build and a big and tall person):

1. Have the small person pass through the door back and forth a few times. Check that the person is counted properly in both the enter and exit directions.
2. Have the big person pass through the door back and forth a few times. Check that the person is counted properly in both the enter and exit directions. If the small person is not counted (missed count), go to [step 3](#).
3. Decrease the numerical value in the **Door span height:** field, by a decrement of 0.5. For instance, if originally the door span height is 50.0 inches, change it to 49.5 inches. Repeat the test from [step 1](#) until both the small person and the big person are counted correctly. Otherwise, if the big person is counted double (that is, incrementing count by 2), go to [step 4](#).
4. Increase the numerical value in the **Door span height:** field, by an increment of 0.5. For instance, if originally the door span height is 50.0 inches, change it to 50.5 inches. Repeat the test from [step 1](#) until both the small person and the big person are counted correctly.

Two People Test

A two people test requires a minimum of three people (one small person and two big and tall people).

1. Have the small person and one big person lean next to each other (side by side). Pass through the door together back and forth a few times. Check if the group gets counted double (that is, incrementing count by 2) in both the enter and exit directions.
2. Have two big people lean next to each other (side by side). Then have them pass through the door together back and forth a few times. Check if the group gets counted double (that is, incrementing count by 2) in both the enter and exit directions.
3. If either group gets only a single count (that is, incrementing count by only 1), do the following:
 - a. Decrease the numerical value in the **Door span height:** field, by a decrement of 0.5. For instance, if originally the door span height is 50.0 inches, change it to 49.5 inches.
 - b. Repeat the two people test from [step 1](#) until both the small person and the big person are counted correctly.

If adjusting the door span height does not improve the results, trying adjusting the door threshold width using the same procedure above. Periodically, with higher ceilings, the door threshold width has more effect on the overhead scene setup.

Zone Adjustment

Resume the door to its natural position. If you have placed a door stop or any object to hold the door open in the previous procedure, remove the door stop. There are two parts in the zone adjustment:

1. First, compare the use of **Object-block zone** vs. **Exclusion zone** for filtering out the door movement.
2. Second, examine the placement of **Inside** and **Outside zones** in the deploying environment.

Object-Block Zone vs. Exclusion Zone

A general guideline is to use the **Exclusion zone** for slow moving doors, an opaque door with a small see through window, or transparent doors. Otherwise, use **Object-block zone**.

1. Save two different configurations, one using the **Object-block zone**, the other using the **Exclusion zone** to mark the door area.

Note Make sure the inside and outside zones are configured properly for each scenario.

2. Have one person pass through the door back and forth a few times.
3. Compare the counting accuracy of each configuration.
4. Pick the configuration that gives the better performance.

Adjusting Inside and Outside Zones

The purpose of adjusting inside and outside zones is to make sure counting performs equally well in both enter and exit directions, and regardless of where the person is coming from (left, right, top or bottom),

1. Have a person pass through the door back and forth many times. Compare *enter* and *exit* counts. If *enter* counts more accurately than *exit*, go to [step 2](#). If *exit* counts more accuracy than *enter*, go to [step 3](#).
2. Recede outside zones by either reducing their sizes or by moving them further away from the inside zones. Then, increase the area of the inside zones by pushing the inside/outside zone boundaries towards the outside zones.
3. Recede inside zones by either reducing their sizes or moving them more away from the outside zones. Then, increase the area of the outside zones by pushing the inside/outside zone boundaries towards the inside zones.
4. Repeat [step 1](#) until the counts in both enter and exit directions are balanced.
5. Have a person passing through the door in all possible directions. If any direction or particular path always gives biased counts, fine tune the inside and outside zones along this path based on the guidelines described in [step 2](#) and [step 3](#).

Camera Groups

Cameras can be grouped based on their spatial proximity or functional similarity to enable specific features in the software. Camera groups can be used to:

- Provide counting information based on Camera Groups in addition to individual cameras
- Enable linking and calibration of spatially adjacent cameras for Wide Entrance People Counting.

This chapter covers:

- Counting data by camera groups
- Using camera groups for wide entrance people counting
- Configuring a camera group

Counting Data by Camera Groups

Camera groups are used to combine counting data of all cameras in the same group. With the use of camera groups, the Live Monitoring Station can display total counts by group in real-time. For more information on how group counts are displayed in Live Monitoring Station, see [Chapter 10](#). The camera groups are also used in the Reporting Tool to provide statistics reports based on camera groups, in addition to individual cameras. The user can choose to have the occurrence of selected events for reporting based on the group total. For more information on this feature of the Reporting Tool see [Chapter 12](#).

Using Camera Groups for Wide Entrance People Counting

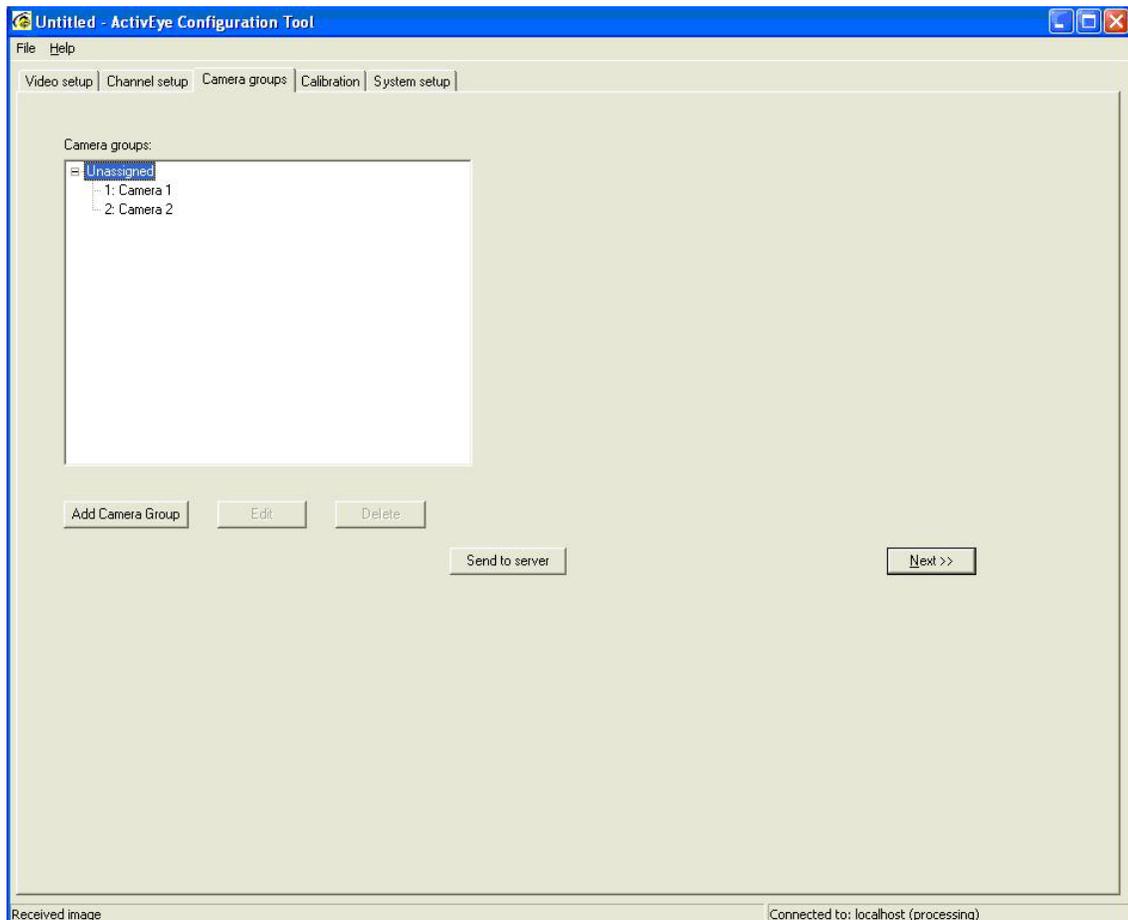
As described in [Chapter 6](#), for wider entrances, multiple cameras must be used to cover the entire opening of the doorway or entrance way to properly detect and count the number of people passing through the wider entrance.

To calibrate cameras at the same wide entrance in a people counting system, all the cameras that cover the entrance must belong to the same camera group. By proper grouping, adjacent cameras with overlapping views can be calibrated to achieve the optimal counting performance. See [Chapter 8](#) on how to calibrate adjacent cameras in the same camera group.

Configuring a Camera Group

On the Camera groups page, initially all the cameras are Unassigned in the Camera Groups list (see [Figure 7-1](#)). You can Add, Edit, or Delete a camera group as described in the following sections.

Figure 7-1 Camera Group Initial Screen

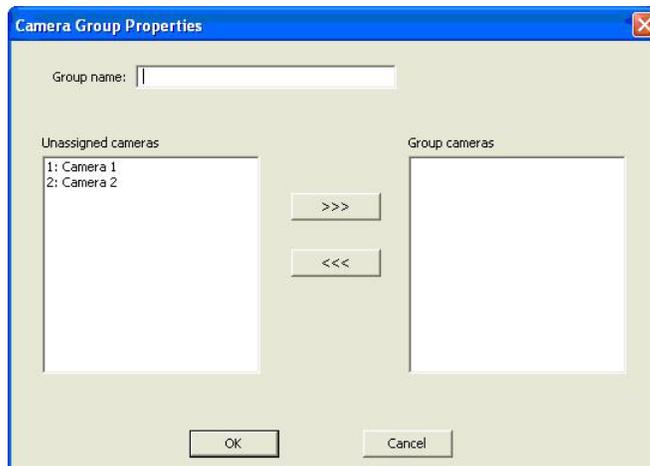


Adding a Camera Group

To add a camera group:

1. Click **Add Camera Group**. The Camera Group Properties dialog box appears (see *Figure 7-2*).

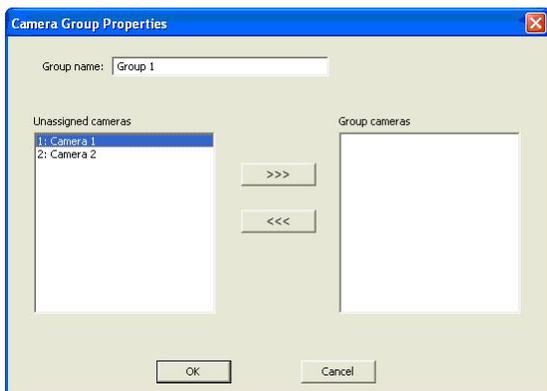
Figure 7-2 Camera Group Properties Screen



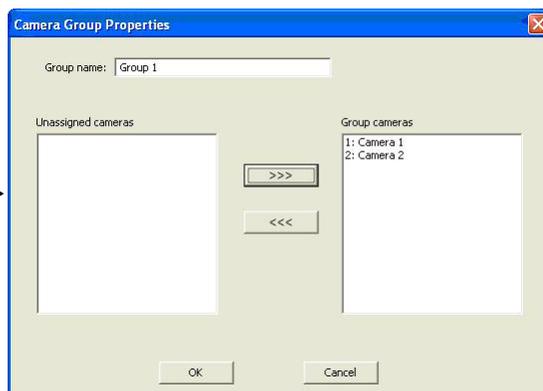
2. Enter the name for the camera group in the **Group name** field as in *Figure 7-3 (A)*. The name must be unique for each camera.
3. Select camera(s) in the Unassigned cameras list on the left box. Hold the Ctrl key to select multiple cameras.
4. Click >>> to move these cameras to the current group. As in *Figure 7-3 (B)*, all the selected cameras have been moved to the Group cameras list.

Figure 7-3 Assign Group Name in Properties Screen

A. Select cameras in Unassigned cameras list



B. Cameras in Group cameras list

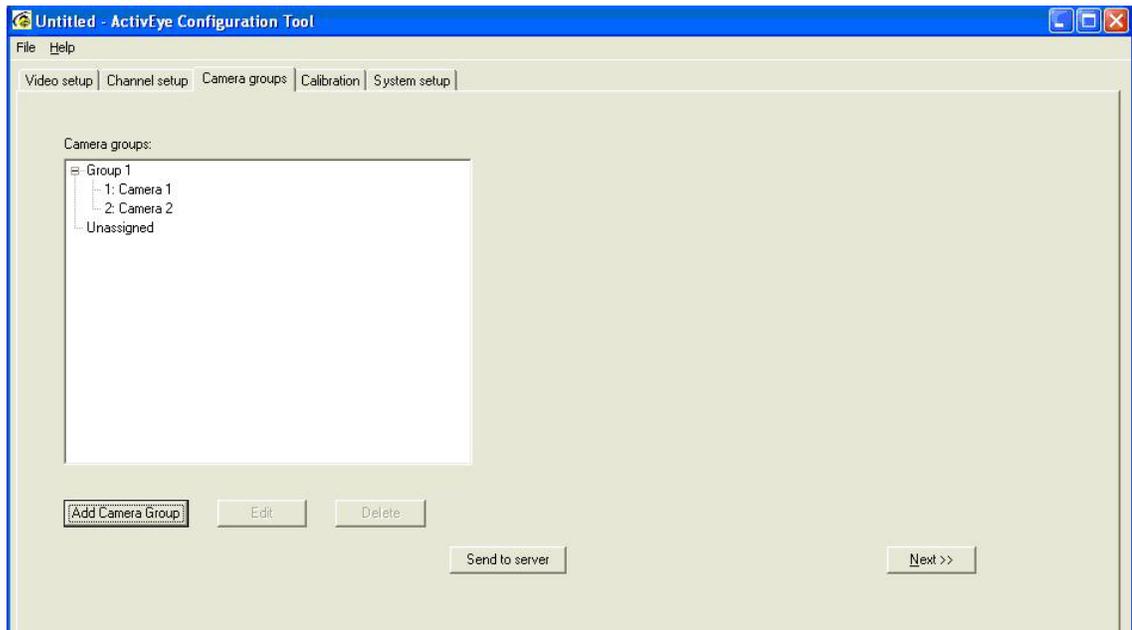


Removing a Camera From the Group

To remove a camera from the group:

1. Click <<<. The selected cameras are moved from the Group cameras list back to the Unassigned list.
2. Click **OK** to confirm the change.
3. If you click Cancel, all your changes will be discarded. *Figure 7-4* shows the Camera Group 1 which contains two selected cameras.

Figure 7-4 Camera Groups with Assigned Cameras



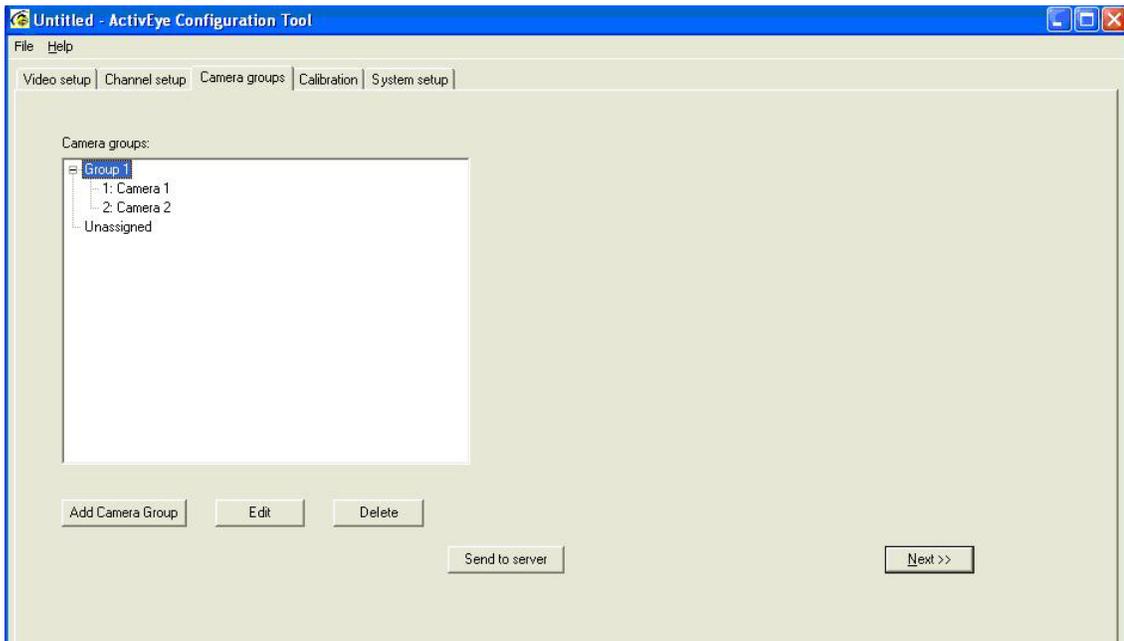
To add more camera groups, click **Add Camera Group** and follow all the steps outlined in [Adding a Camera Group](#), page 121.

Editing a Camera Group

To edit a camera group:

1. Select the camera group that requires modification as shown in *Figure 7-5* and then click **Edit**.
2. Modify the camera group properties in the Camera group properties dialog box (see *Figure 7-3*). You can rename the group or modify the list of cameras associated with the selected group as described in the previous section.

Figure 7-5 Camera Group Properties Modifications



Deleting a Camera Group

To delete a camera group:

1. Select the camera group that you want to delete (see [Figure 7-5](#)).
2. Click **Delete** to delete the camera group.
3. You are prompted to confirm the deletion (see [Figure 7-6](#)). Click **OK** to continue or **Cancel** to stop the deletion.

Figure 7-6 Camera Group Deletion Prompt



Uploading the New Configuration to a Server

You must upload your changes to the video analytics server to have them take effect.

1. Click **Send to Server**.

Alternatively, you can wait until you finish all the changes in the Configuration Tool and then submit all the changes to the server altogether.

2. Click **Next** to continue to the next page for more configuration changes.

Camera Calibration

Adjacent cameras in a wide-entrance people counting system must be properly calibrated so that the system provides accurate counts. Camera calibration allows the system to recognize the same person seen in both cameras and avoid double counting of the same person.

This chapter covers how to calibrate adjacent cameras for wide-entrance people counting.

Calibration Targets

Calibration targets are visible features that appear in both camera views. They can be used as markers to correspond the same physical location in one view to the other. They must be located on the floor surface for the calibration parameters to be valid. Calibration targets can be used to create calibration points required for the system to compute calibration parameters to geometrically relate one view to another. A calibration target can come from the texture or pattern that naturally exist in the scene, such as floor tiles or carpet patterns.

If there are no natural calibration targets in the overlapping scenes, you can use Post-it notes placed randomly on the floor where the views are overlapping, so that they can be seen in both cameras. Please note that the randomness is important. Make sure that they do not form straight lines or rectangular patterns. It is also better to spread them around so that they scatter across the overlapping areas in the camera views. At least six calibration point pairs are required for each overlapping camera pair, and more calibration point pairs will help the accuracy of the camera calibration. The recommended number of pairs is 8 to 10 pairs, or up to a maximum of 16. [Figure 8-2](#) illustrates placement of the Post-It notes.

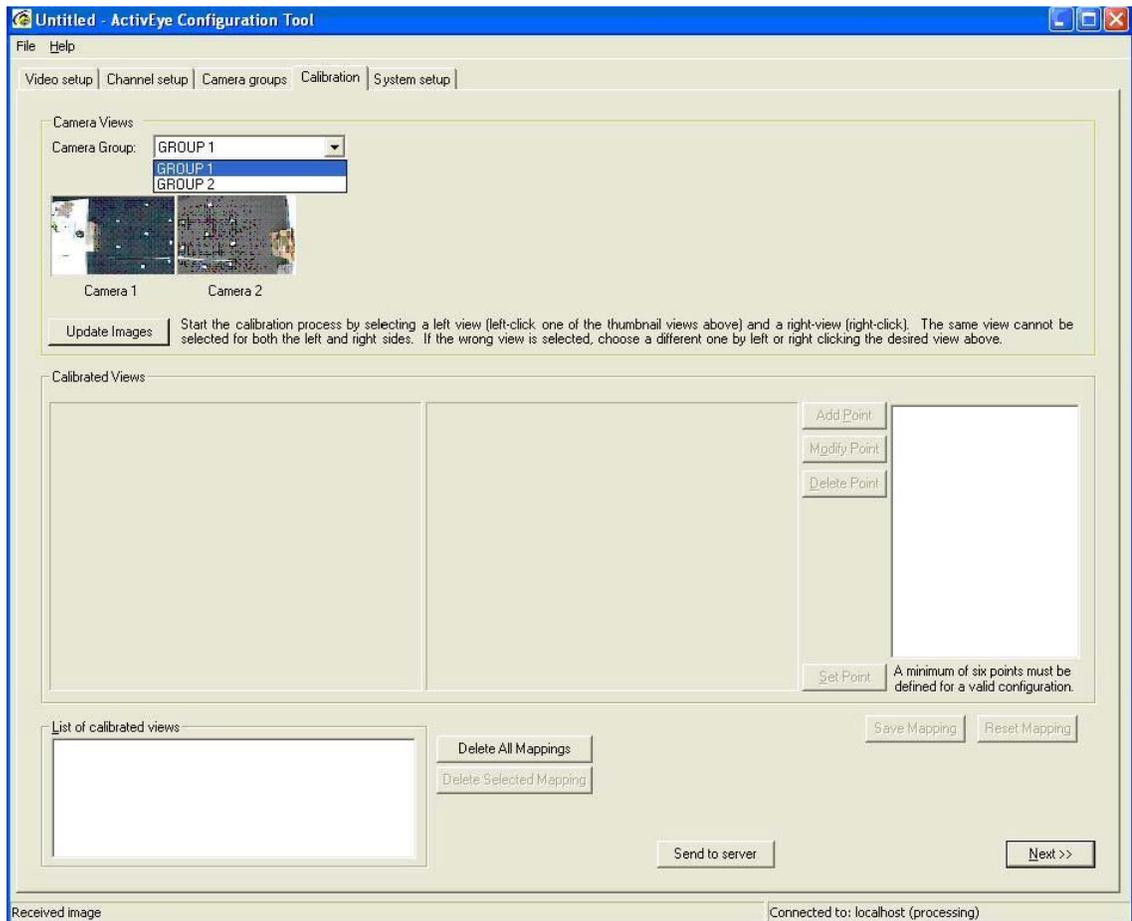
After you have either identified suitable calibration targets, or have placed some calibration targets in the scene, you are ready for the calibration step.

Before calibrating adjacent cameras at the same wide entrance, all cameras that are spatially linked must belong to the same camera group. On the Calibration tab, select the camera group from the Camera Group drop-down list as in Thumbnail views of the overhead cameras from the selected camera group will appear to be selected for calibration.

Note Only cameras with scene type Overhead people counting are displayed. If there are cameras in the selected group that are not configured for overhead people counting, they are hidden from the calibration page. In this version of Video Analytics software, camera calibration is only applicable to overhead cameras for people counting purposes.

To get the latest view of the overhead cameras in the selected group, click **Update Images**.

Figure 8-1 Camera Group Selection



Thumbnail views of the overhead cameras from the selected camera group appear and can be selected for calibration.

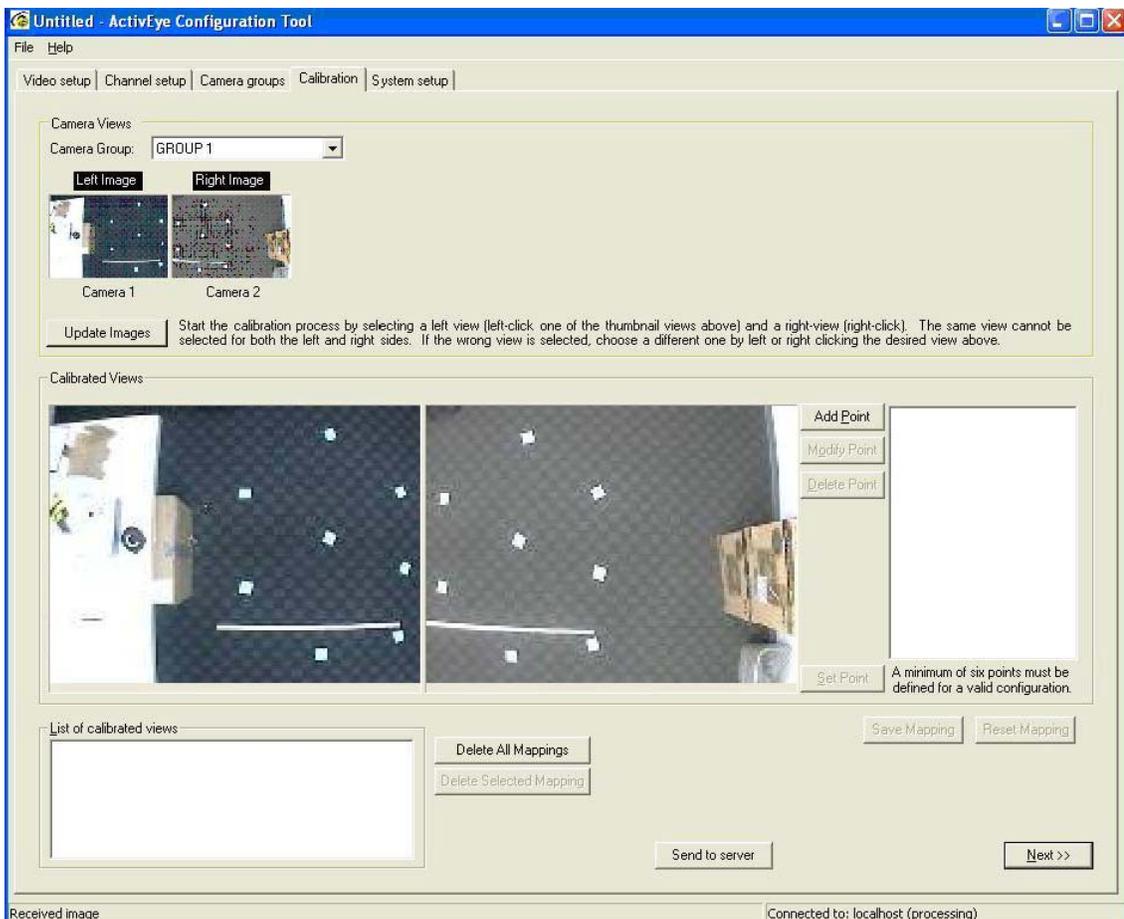
To get the latest view of the overhead cameras in the selected group, click **Update Images**.

Selecting a Camera Pair to Calibrate

You need to calibrate a pair of adjacent cameras with overlapping views each time.

1. Select the camera pair to define their calibration point pairs.
2. Move the mouse over the thumbnail of the first camera and left-click. This places the first camera view to the left display window.
3. Similarly, move the mouse over the thumbnail of the second camera and right-click to place the second camera view to the right display window. *Figure 8-2* shows a pair of overlapping camera views that have been selected and displayed in the working area.
4. If you need to reverse the order of the two views, switch the selection order.
5. After you have a pair of overlapping camera views in the working area, you can start to add calibration point pairs to calibrate this camera pair. A calibration point pair consists of two matching points, one from the left image, and the other from the right. For example, in *Figure 8-3* the red cross in the left image matches with the red cross in the right image and they form a calibration point pair.

Figure 8-2 Camera Pair Calibration



Now you can add, modify, or delete calibration points for the selected pair of camera views.

Adding a Pair of Calibration Points

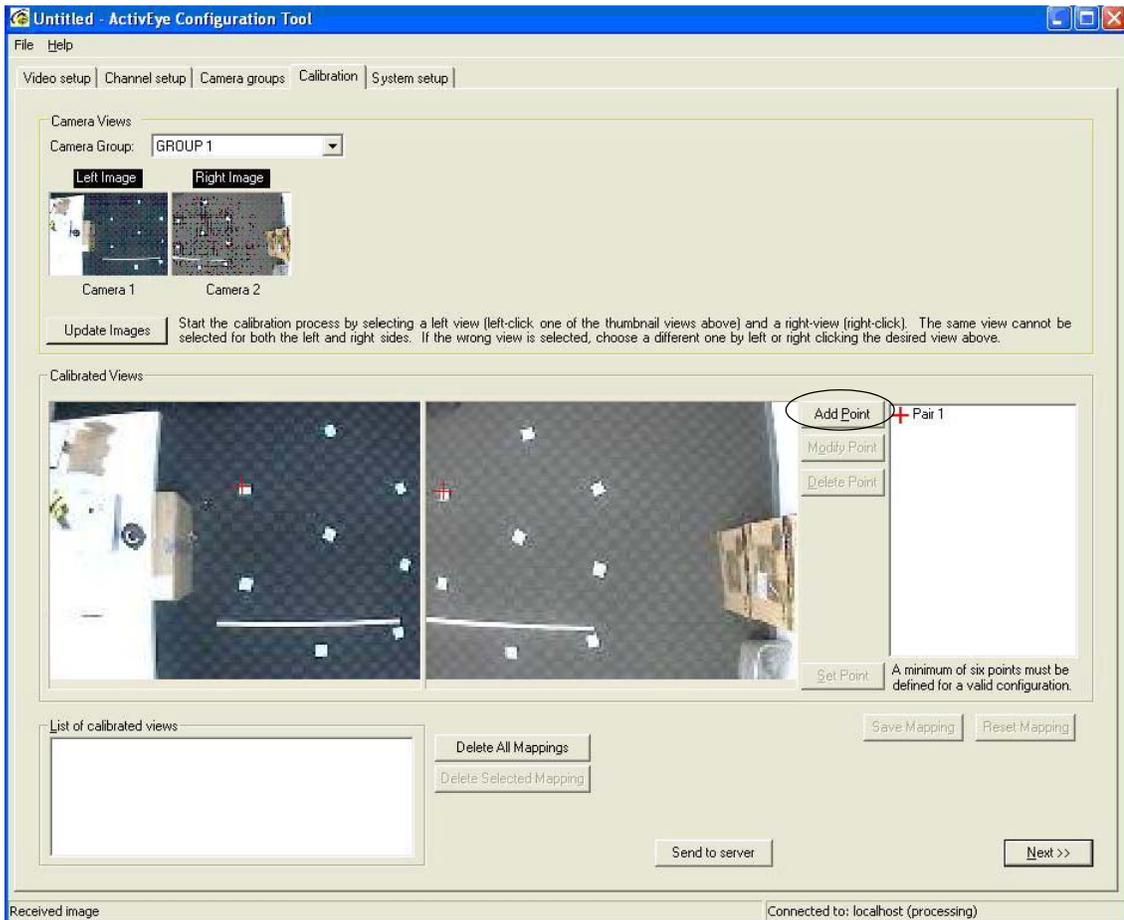
To add a pair of calibration points:

1. Click **Add Point**.
2. Move the mouse to point at the location in the left image where the calibration target is located, and left-click the mouse to define the point. A flashing cross appears at the location where you clicked.
3. Move the mouse to point at the same calibration target in the right image, then left-click. A flashing cross of the same color appears in the right image.
4. To adjust the locations of the points, simply point the mouse to the new location on either the left or the right image and left-click again.
5. After you have both flashing crosses at the desired locations, click **Set Point** to confirm.

This newly defined pair appears in the list of defined point pairs, marked by the same color. For example, in [Figure 8-3](#) the red crosses form Pair 1 in the list.

6. Repeat these steps to define additional calibration point pairs. The system requires at least 6 pairs of calibration points to be defined to compute calibration parameters to relate the geometry between the two camera views. More calibration point pairs increase the mathematical stability and result in more accurate calibration parameters. In [Figure 8-4](#), 8 calibration point pairs have been defined. Note that the points are widely spread across the overlapping area in the camera views to ensure mathematical stability in computing the calibration parameters between the two camera views.

Figure 8-3 Camera Group Calibration Point Example



Modifying a Pair of Calibration Points

To modify or delete a defined calibration point pair:

1. Click to select the pair you want to modify from the list of defined point pairs.
2. The selected pair is now highlighted.
3. Click **Modify Point**. The selected point pair is removed from the views.
4. You can now move the mouse to the desired location and left-click to define the new location of the calibration point in both views.
5. Click **Set Point** to confirm your change.

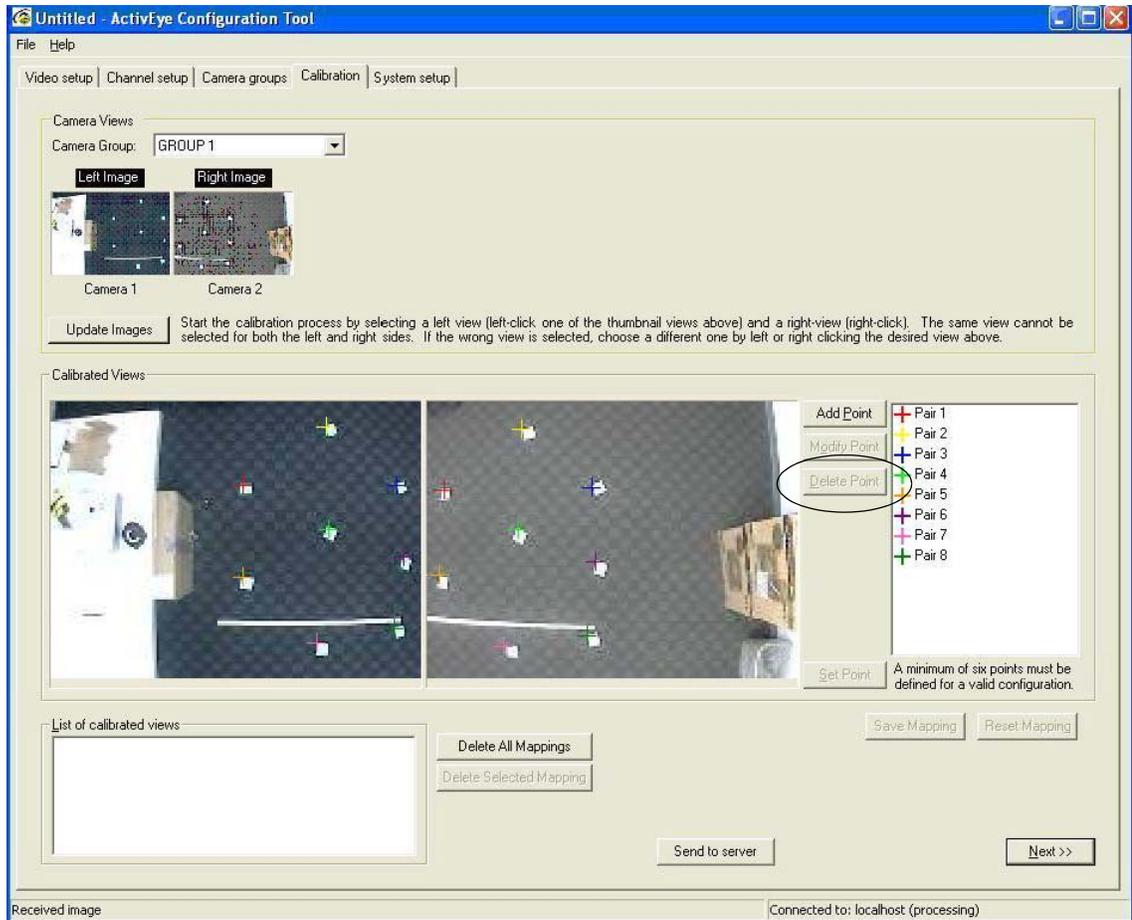
Deleting a Pair of Calibration Points

To delete a defined calibration point pair:

1. Select the pair you want to delete from the list of defined point pairs

- Click **Delete Point**. The selected point pair is removed from the list.

Figure 8-4 Calibrated View With Eight Pairs of Calibration Points



Saving Mapping

After you have defined all the calibration point pairs for the overlapping camera pairs, click **Save Mapping** to save all the points for this pair of camera views. The camera pair appears in the List of Calibrated Views at the bottom of the page, and the working area is cleared to be ready for the next pair of adjacent cameras to be calibrated. As shown in *Figure 8-5*, the mapping from Channel 1 -> Channel 2 is added to the list of calibrated views.

Reviewing Mapping

You can review the mapping by clicking to select this calibrated pair, which then brings this camera pair back to the working area.

If you have more overlapping camera pairs that need to be calibrated, you can repeat the previous procedure by selecting the next camera pair and placing them in the working area.

Resetting Mapping

Click **Reset Mapping** to delete all the calibration point pairs for the current camera pair in the working area.

Deleting Calibrated Camera Views

To delete a calibrated camera view:

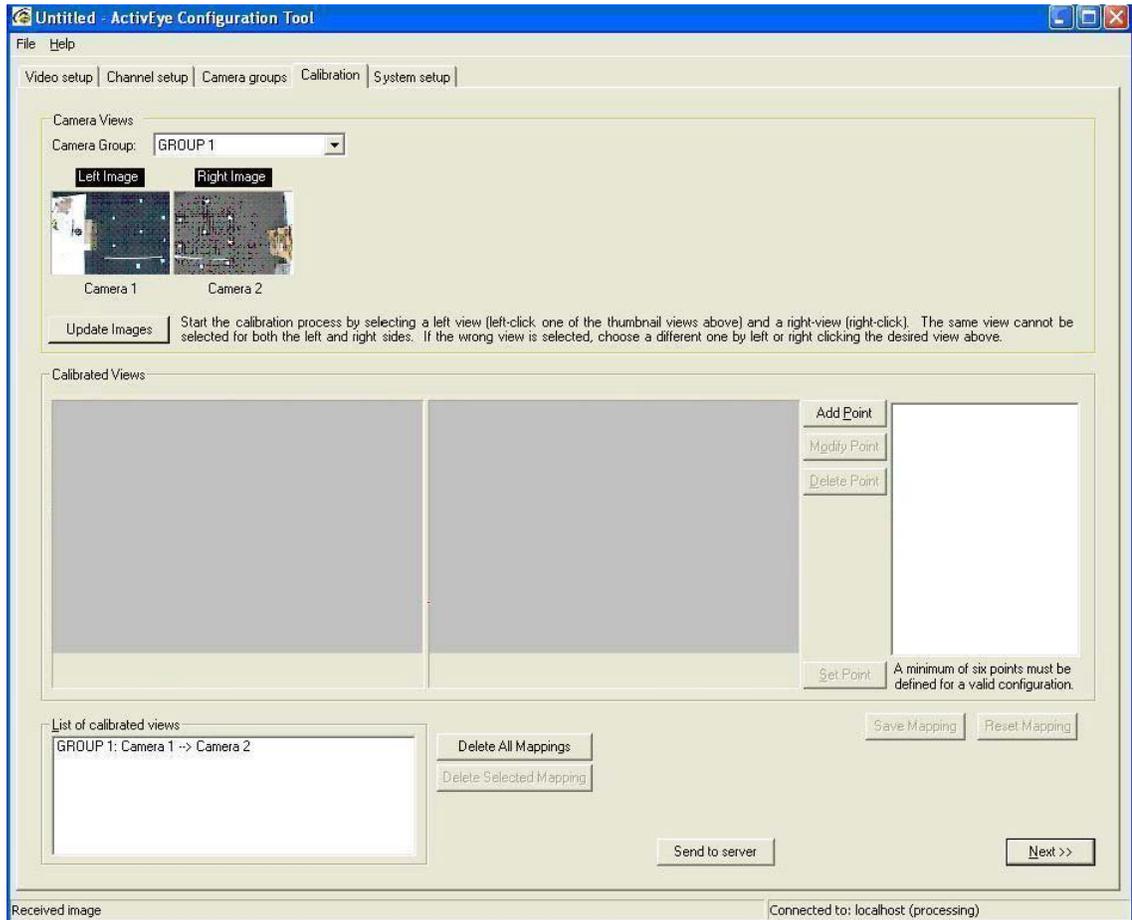
1. From the list of calibrated views, select a calibrated camera pair.
2. Click **Delete Selected Mapping** to delete the selected camera pair.
3. To delete all camera pairs that have been calibrated, click **Delete All Mappings**.

Sending Changes to the Server

You must submit the changes you made to the server to make them in effect. To submit the changes to the video analytics server:

1. Click **Send to Server**. Alternatively, you can wait until you finish all the changes in the Configuration Tool and then upload all the changes to the server altogether.
2. Click **Next** to continue to the next page for more configuration changes.

Figure 8-5 Save Mapping



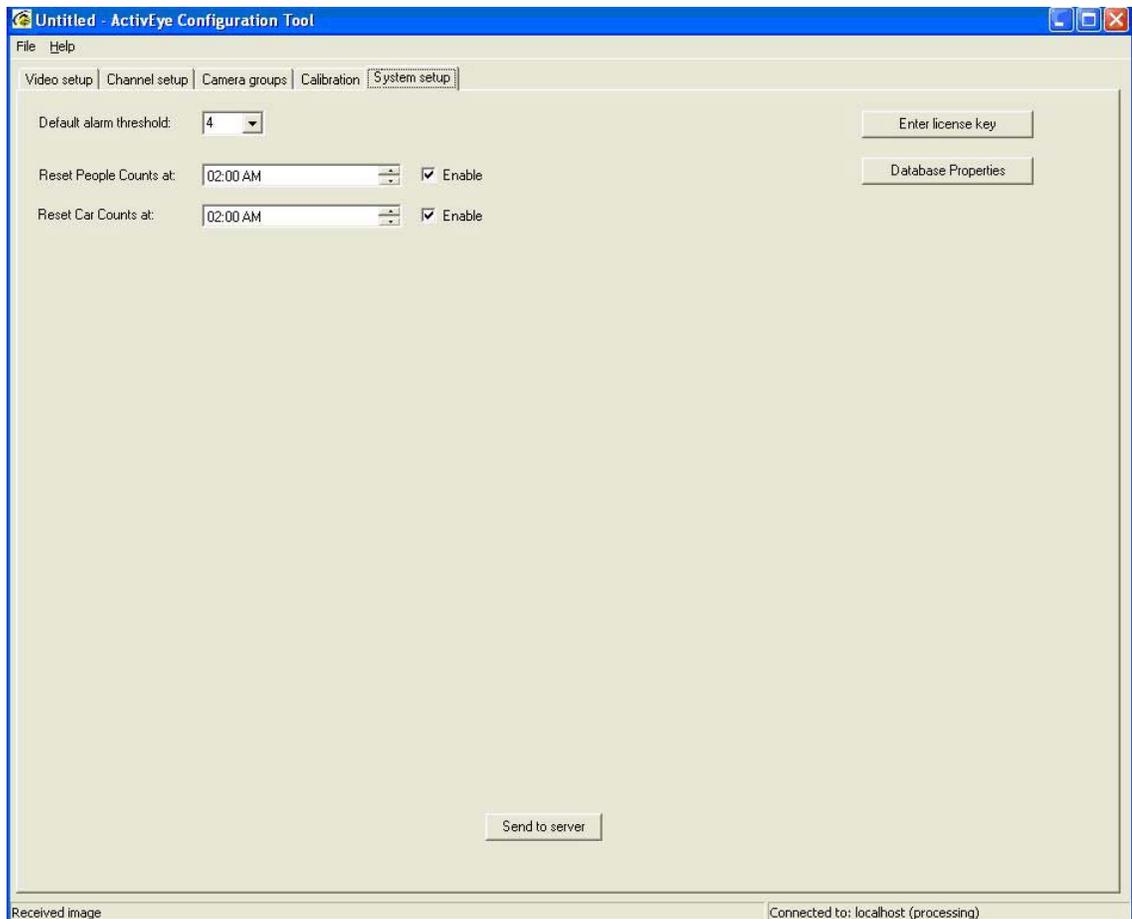
System Configuration

Some settings are system-wide and they can be configured in the System setup tab.

This chapter covers:

- Setting a default alarm threshold
- Setting a counter reset schedule
- Entering the license key
- Changing the database properties

Figure 9-1 System Setup Configuration Parameters

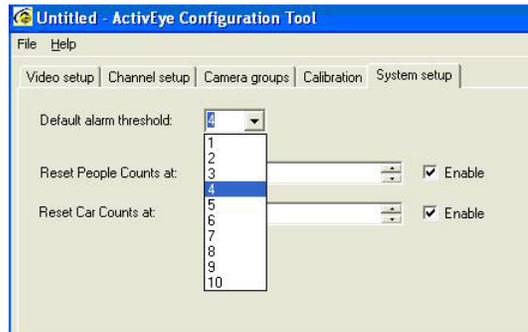


Setting A Default Alarm Threshold

Any event with severity level equal to or greater than the alarm threshold generates an alarm in real-time. You can set the global alarm threshold from the Alarm Threshold drop-down list (see [Figure 9-2](#)). This threshold applies to all the channels being processed by this analytics server. The default alarm threshold is set to 4. Select the alarm threshold that is suitable for your operation.

Note Remember to click **Send to server** to have this change taken in effect.

Figure 9-2 Set Default Alarm Threshold

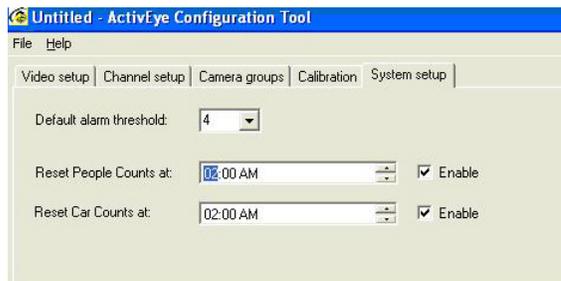


Counter Reset Schedule

You can set the counter daily reset schedule for both people counting and car counting events (see [Figure 9-3](#)). This resets the counter values displayed on the Live Monitoring Station client application only. It has no effect on storage of all the counting events in the database. To set the reset schedule for people counting events (that is, person counted as entering and person counted as exiting) and also the Car Counting:

1. Set the time when you want the counters (both enter and exit) to be reset to 0 on a daily basis. The default reset time is set to 2:00 AM.
2. Select the **Enable** checkbox. To disable the daily reset schedule for the counter, clear the Enable check box.
3. Click **Send to server** to send the change to the server.

Figure 9-3 Schedule Counter Reset Time



Entering the License Key

This version of Honeywell Video Analytics software supports only license key string (not dongle). Typically, the license key is set up when the software is installed or automatically converted during an upgrade from prior dongle-based system. If you choose to later upgrade your system or for some reason the license key string is lost, you may need to re-enter the license key string.

Your license key can vary in length depending on the number of product packages your system is licensed for. The license key string controls the number of licenses and expiration date for each product package in your license.

1. On the System setup tab, click **Enter license key** (see [Figure 9-1](#)).
2. To receive a valid license key, you must provide the Server ID to HVSsupport@honeywell.com.
3. Type the license key and then click **OK**.
4. Click **Send to server** to send the updated license key to the server. After a successful upload, the new license is in effect.



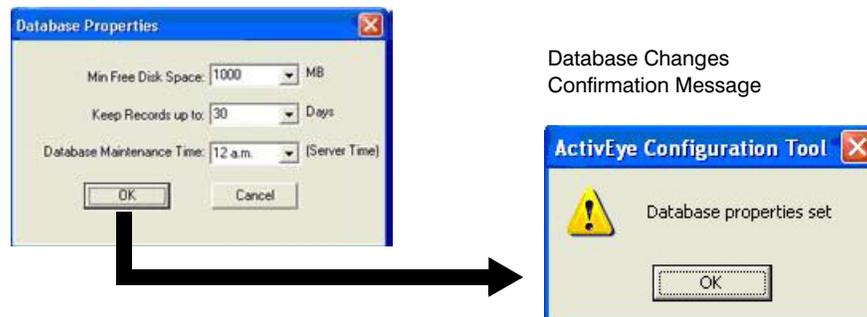
Caution Make sure that the connection to the server has been established and remember to click **Send** to server after entering the key string.

Figure 9-4 Enter License Key

Changing Database Properties

To ensure continuous system operations, the system automatically monitors disk usage on the server and manages the size of the recording database. To view and modify the database properties:

1. Click **Database Properties**. The Database Properties dialog (see [Figure 9-5](#)) appears.
2. Set the minimum free disk space and the number of days of records to keep on the server.
3. You can also specify the time for daily database maintenance to the hour. Honeywell recommends that you specify a time when there is a minimum load on the server; that is, when the scenes are quiet.
4. Click **OK**.
5. Click **Send to server** to send the changes to the server. The message Database properties set (see [Figure 9-5](#)) indicates that the change has been successfully uploaded to the server. Changes are in effect at the next database maintenance time.

Figure 9-5 Database Properties

Live Monitoring Station

Live Monitoring Station is a client application used to connect to Analytics servers in the Honeywell Video Analytics software system. It allows remote users to receive live video streams with analytics annotations as well as real-time events and alarms across multiple Analytics servers. Running Live Monitoring Station requires a TCP connection to at least one Video Analytics server.

This chapter describes in detail how to use the Live Monitoring Station for your daily surveillance tasks. The Graphical User Interface (GUI) allows you to configure the screen layout and real-time information displayed on this monitoring station.

Logging On to Live Monitoring

To use Live Monitoring, identify the servers you want to connect to using the logon dialog as shown in *Figure 10-1*.

Figure 10-1 Server Login Dialog



You can connect to up to three servers simultaneously. If connecting to less than three servers, leave the other host name fields blank.

User Name and Password

The user name and password must be the same for all of the servers and must have the *Live View* permission on all of the servers. For instance, if your system administrator has defined the *guest* user on all of the servers, you can leave the user name and password fields blank to connect as a *guest*.

Note Only the administrator can manage user accounts. For detailed information, see [Chapter 3](#).

Slow Network Connection

If you have a slow network connection to any of the servers, you may enter a smaller number for the FPS Limit (frames per second). The default is 15 FPS, the maximum allowed frame rate. You can go down to as little as 5 FPS and still be able to view smooth live video.

Note This only limits the amount of video data that the server sends to you for viewing and has no effect on the processing frame rate on the server.

The server may further limit your video streaming rate if it detects that your network connection is getting bogged down.

The server will not send video at a rate higher than the rate at which the server actually captures/processes the frames.

Using the Live Monitoring Station

After selecting the server(s) and entering a valid user name and password pair, you are taken to the Live Monitoring Station main window as shown in [Figure 10-2](#).

Note There may be a slight delay before the main window displays if any of the servers are down or unreachable.

Note If the server is not in the Processing state when the Live Monitoring Station is launched, no channel is displayed. Please see [Server Status](#) on page 140.

Figure 10-2 Live Monitoring Station, Showing Areas of Interest

The screenshot shows the 'ActivEye Live Monitoring Station' interface. On the left, there are several control panels:

- Server Status (see [Server Status](#)):** A table showing server names and their status.

Server	Status
nist2	processing
nist5	processing
nist1	processing
- Display Format (see [page 140](#)):** Settings for 'Display Format' (4x4 @ 160x120) and 'Channels' (1-16). It also includes a 'Camera Display Text' dropdown set to 'Camera name/time'.
- Alarm Display (see [page 141](#)):** Checkboxes for 'Audio alarms', 'Show alarm popup', 'Show alarm video', and 'Show group counts'. A 'Time Zone' dropdown is set to 'Server Time'.
- Event Display (see [page 147](#)):** A table of events.

Ch	ID	Type	Event	ID2	Sev.	Time
9	169...	Person	Trespassing line 16		4	16:58:38
9	169...	Person	Trespassing line 16		4	16:58:38
16	135...	Person	Trespassing line 16		4	16:56:36
11	160...		Entered		1	16:58:38
8	5465		Exited		1	16:56:39
2	3804		Exited		1	16:56:39

The main area displays a 4x4 grid of camera feeds. The bottom-right feed (NIST1: Camera 4) is highlighted in red and labeled 'Person Trespassing line 16'. The status bar at the bottom shows 'processing' and 'nist2'.

Display threshold (see [page 147](#)). Image display (see [page 148](#)).

There are six areas of interest in the Live Monitoring Station:

- Server Status
- Display Control
- Video Display Panels
- Event Display
- Threshold Settings
- Image Display

The following sections explain these areas of interest and how you control what you see.

Server Status

This area shows the current status of each of the servers you are monitoring. [Table 10-1](#) lists the available server statuses.

Table 10-1 Server Status Options

Option	Description
Processing	The server is currently processing live video. This is the normal state.
Configuring	The server is currently being reconfigured. This is a temporary state and the status should return to Processing after the new configuration has been uploaded to the server.
Needs license	The server does not have a valid license.
Checking database	The server is currently checking the database and does not accept client connection. The client should try to connect back at a later time.
Off	The server is not currently running.

Display Format and Layout

This area allows you to set the display format and layout settings. [Table 10-2](#) describes the field options.

Table 10-2 Display Format and Layout Options

Field	Description
Display Format	Select the number of cameras that are displayed at one time, the size they are displayed in, and the layout on the screen. The choices in the drop-down list depend on the total number of active cameras on the servers you are connected to as well as the native image sizes on the servers. The drop-down list does not appear when there is only one available choice.
Channels	Select which range of cameras are displayed. It only appears if the selected Display Format shows less than the total number of cameras that are being monitored. The range is based on the <i>channel numbers</i> that Live Monitoring Station assigns to each camera. Channels numbers are assigned sequentially starting from 1; from the first server to the next and so on.
Camera Display Text	Select the live information displayed below each camera image in the Video Display panel.

Table 10-2 Display Format and Layout Options (cont'd)

Field	Description
Camera name/time	(default setting) The first line shows the camera name and the name of the server the camera is connected to in the format of <i>Server:[Camera name]</i> . The second line shows the server's date and time corresponding to the currently displayed video frame.
Enter/exit counts	Shows people and/or vehicle entry and exit counts for the cameras that have people and/or vehicle enter/exit counting enabled.
Lane counts	For cameras that have car-in-lane traffic counting enabled, this shows the total counts (1st line) and the lane counts (2nd line).
Tamper measure	For cameras that have tamper detection enabled, this shows the current tamper measure in real time (see Figure 10-2). For detailed information on tamper detection, please see Configuring Tamper Detection , page 77.
Combined counts	Shows both enter/exit and lane counts. If a camera has both traffic and enter/exit counting enabled, only the lane counting display is shown for that camera.

Alarm Display

Whenever an alarm is received for a camera that is currently displayed on the screen, a red alarm bar appears below the channel image with blinking text announcing the type of alarm. At the same time, the objects involved in the alarm will also be highlighted in a blinking red box overlaid on the video image to alert the user (see [Figure 10-3](#) and [Figure 10-4](#)).

Figure 10-3 Alarm Display

The screenshot shows the 'ActivEye Live Monitoring Station' software interface. The main window displays a video feed from 'NIST1: Camera 4' showing a parking lot with a red circle highlighting a person. A red 'Alarm bar' is overlaid on the video feed with the text 'NIST1: Camera 4' and 'Person Trespassing line 16'. To the left of the video feed is a 'Display control area' containing various settings and a table of events.

Display control area

ALARM!
NIST1: Camera 4:
Person Trespassing
line 16

Server	Status
nist2	processing
nist5	processing
nist1	processing

Display Format: 1x1 @ 320x240 Channels: 16

Camera Display Text: Camera name/time

Audio alarms
 Show alarm popup
 Show alarm video
 Show group counts

Ch	ID	Type	Event	ID2	Sev.	Time
16	240...	Person	Entered		1	09:52:41
16	240...	Person	Started moving		2	09:52:45
2	260...	Object	Exited		1	09:53:02
9	186...	Person	Trespassing line 16		4	09:55:06
9	186...	Person	Trespassing line 16		4	09:55:06
16	240...	Person	Trespassing line 16		4	09:53:04

Display threshold: 1

Image display:
 Video input
 Tracked objects
 None

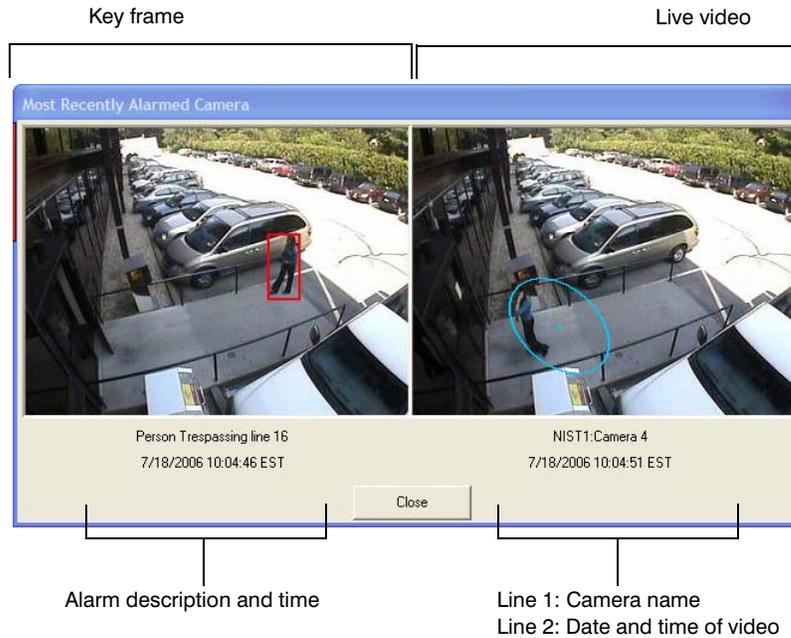
processing nist2

Table 10-3 describes the alarm display fields.

Table 10-3 Alarm Display Options

Field	Description
Audio alarms	Select to hear a voice announcement whenever an alarm is received from the connected servers, regardless of whether the channel is displayed.
Show alarm popup	Select to display a red alarm window on the upper left corner of the screen (see Figure 10-3) the moment an alarm is received from the servers, regardless of whether the channel is displayed on the video display panels. The alarm window appears on top of all other windows so you do not miss the alarm. The alarm window automatically disappears after a few seconds; you can dismiss it sooner by clicking it.
Show alarm video	Select to display the Most Recently Alarmed Camera window (see Figure 10-4) whenever an alarm is received (regardless of whether the channel is displayed on the video display panels). The left pane in the window shows the key frame at the time of the alarm and the right pane shows the current live video from this camera. Both are shown in the native image size from the server regardless of the size you have selected in Display Format. The red bounding box overlaid in the key frame shows the object that has triggered the alarm. In the example in Figure 10-4 , the person enclosed in the red bounding box crossed a trespassing line, thus triggering an alarm.
Show group counts	Select to display the total enter and exit counts per camera group (see Figure 10-5). A separate window appears for group counts display. This window remains on top. The counts are accumulated counts since the counter reset time, which may be the last time a channel has been restarted.

Figure 10-4 Alarm View Window



This window automatically disappears 15 seconds after last alarm. To dismiss it sooner, click **Close**.

Note You can also select the time zone displayed to be one of the following: the Server Time, Local Time or GMT (UTC).

Figure 10-5 Show Group Counts

Group Counts		
localhost		
People Counts Since 7/2/2008 10:28:08		
	Enter	Exit
Retail-NE	35	86
Retail-NW	43	65
137.19.209.134		
Vehicle Counts Since 7/2/2008 2:00:02		
	Enter	Exit
Group 1	0	0
Group 2	50	0
Group 3	11353	14674

Reset Scene Changed Alarm

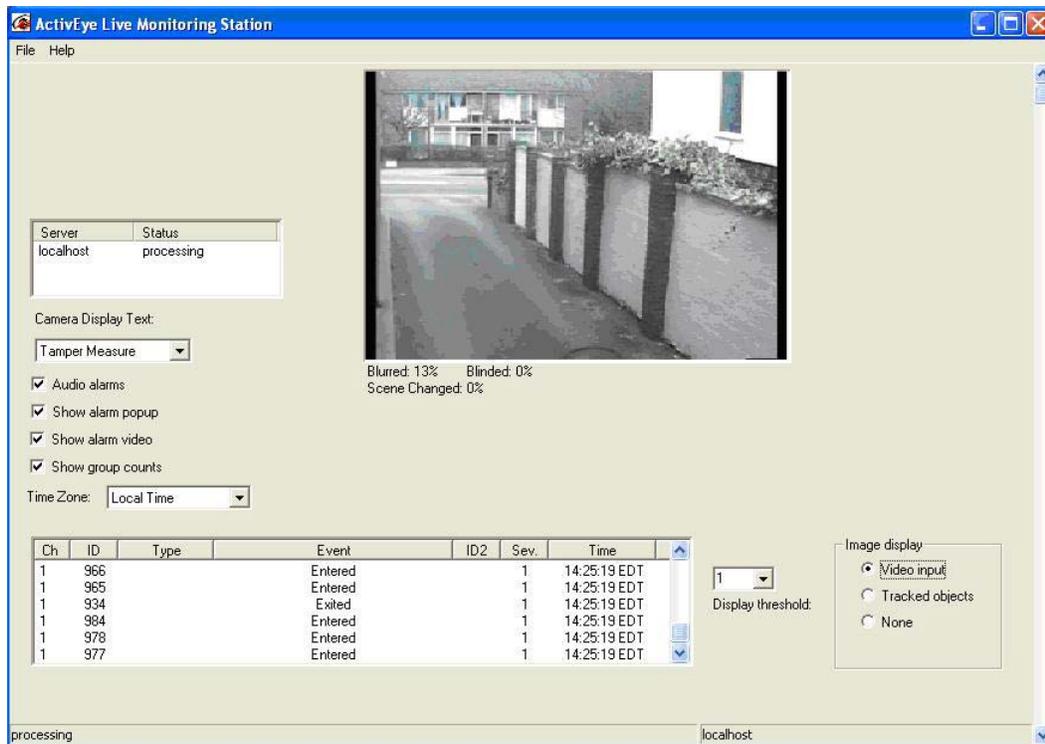
This version of video analytics software provides Camera Tamper Detection, which detects if the camera is being blinded, blurred or the scene has changed. For this feature to work, you must enable Tamper Detection using the Configuration Tool (see [Configuring Tamper Detection](#), page 77).

If Tamper Detection is enabled for a specific camera, the Live Monitoring Station displays the current tamper measure of blind, blur, and scene change level in real-time on screen.

Note Tamper Measure must be selected as the Camera Display format.

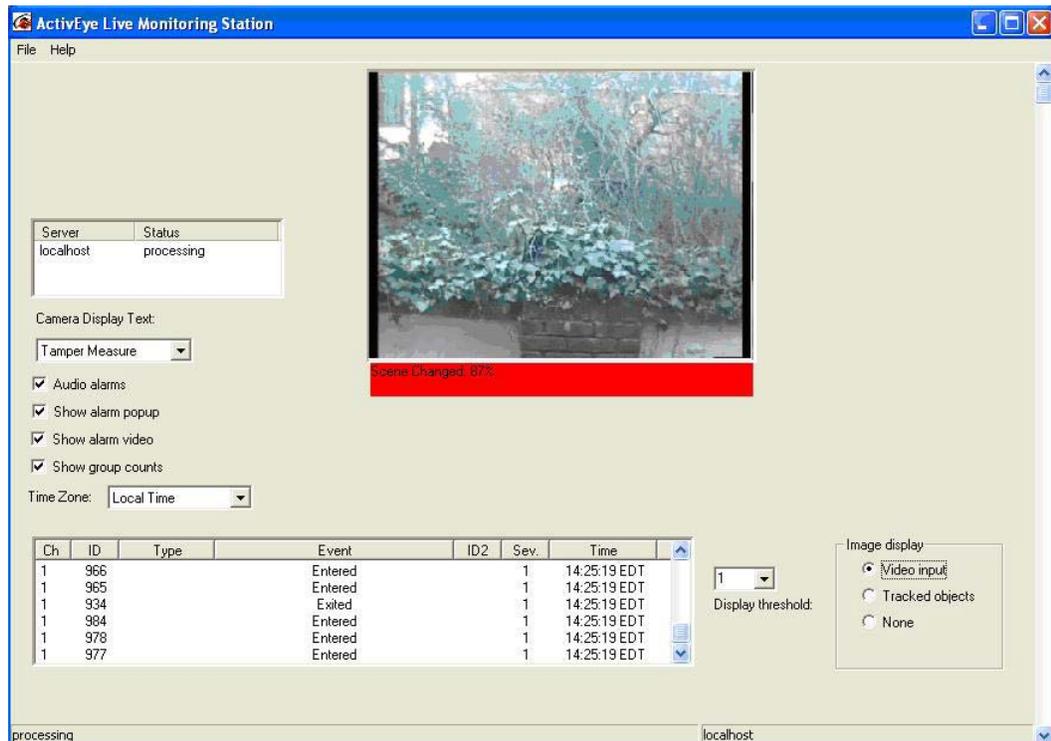
In the normal state (see *Figure 10-6*), the Tamper Measure values that are shown under the image frame indicate the percentage values in the tamper measure for this camera.

Figure 10-6 Normal Camera View



As shown in *Figure 10-7*, when the scene change level exceeds the specified threshold and reaches the alarm level, the scene change alarm displays on the Live Monitoring Station screen. The current Scene Changed level percentage displays (see the red bar under the video in *Figure 10-8*).

Figure 10-7 Scene Change Alarm



After detection, the scene change alarm remains until the camera view resumes to its original view. In some situations, you may want to reset the scene change alarm (for instance, the change of the camera view is intentional or the scene change alarm does not clear automatically). In the former case, you must also adjust the configuration for this camera since the view has changed.

There are two ways to reset the scene change alarm:

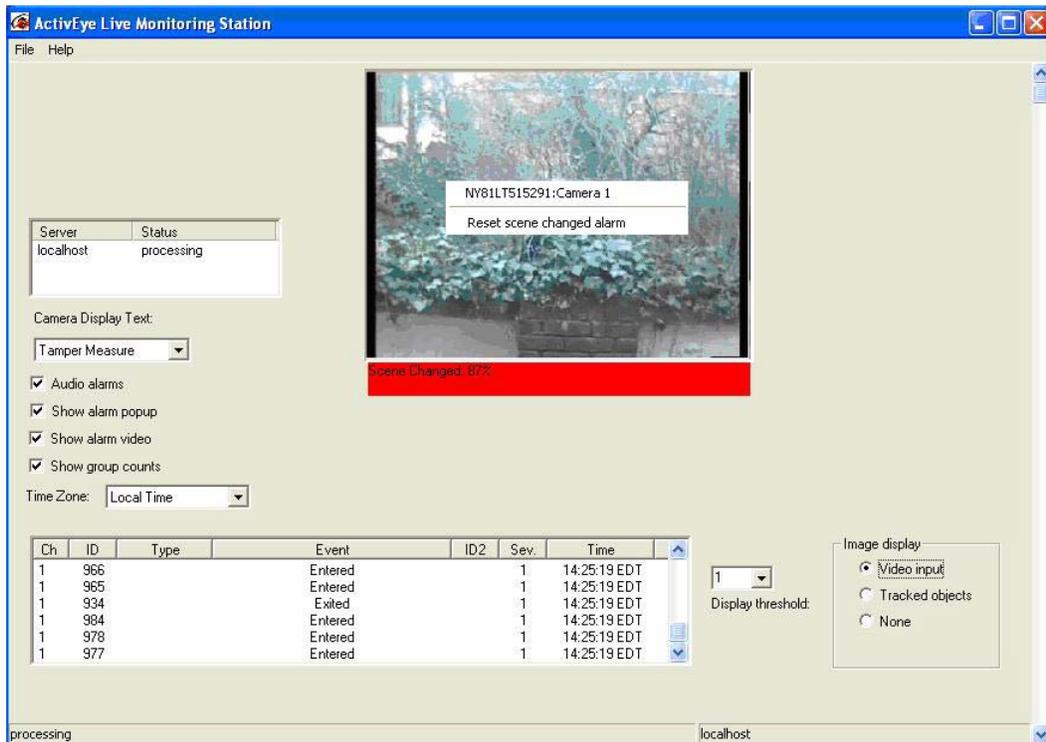
- Right-mouse click the scene in the Live Monitoring Station which displays the alarm state, and then select **Reset scene changed alarm** to clear the alarm state (see [Figure 10-8](#)).

Note You must have Write Configuration permission level to reset the alarm directly in the Live Monitoring Station.

- Using the Configuration Tool, on the Channel Setup page, select the camera with the persisting scene change alarm, and then click **Reset below the Scene** change slide bar off the Tamper Detection tab.

Please see [Configuring Tamper Detection](#), page 77 for more information.

Figure 10-8 Reset Scene Change Alarm



Event Display and Threshold Settings

All detected objects and events are stored in databases. The most recent events are also displayed in the Event Display window to provide instant information. The **Display Threshold** drop-down list in the Threshold Settings area (see [Figure 10-2](#)) controls which events are displayed. Only events with severity equal to or higher than the selected threshold are shown in the window.

In the Event Display area, double-click a line in the Event Display window to display the key frame (still photo from time of event) associated with that event (see [Figure 10-9](#)).

Figure 10-9 Event Key Frame



Click **Prev** and **Next** to browse sequentially through the key frames of the event.

Note Other events are stored in the databases.

Image Display

Table 10-4 describes the image display fields.

Table 10-4 Image Display Options

Field	Description
Video input	Displays the raw live video.
Tracked objects	Displays live video with colored ellipses around objects that are being tracked and flashing red/gray boxes around objects involved with currently displayed alarms.
None	No display

Forensics Tool

The Forensics Tool is a client application that is used to connect to Analytics servers in the Honeywell Video Analytics software system. It allows remote users to connect to the Video Analytics database on the server to conduct search and retrieval of past incidents. Running the Forensics Tool requires a TCP connection to the database on at least one Analytics server through port 3306.

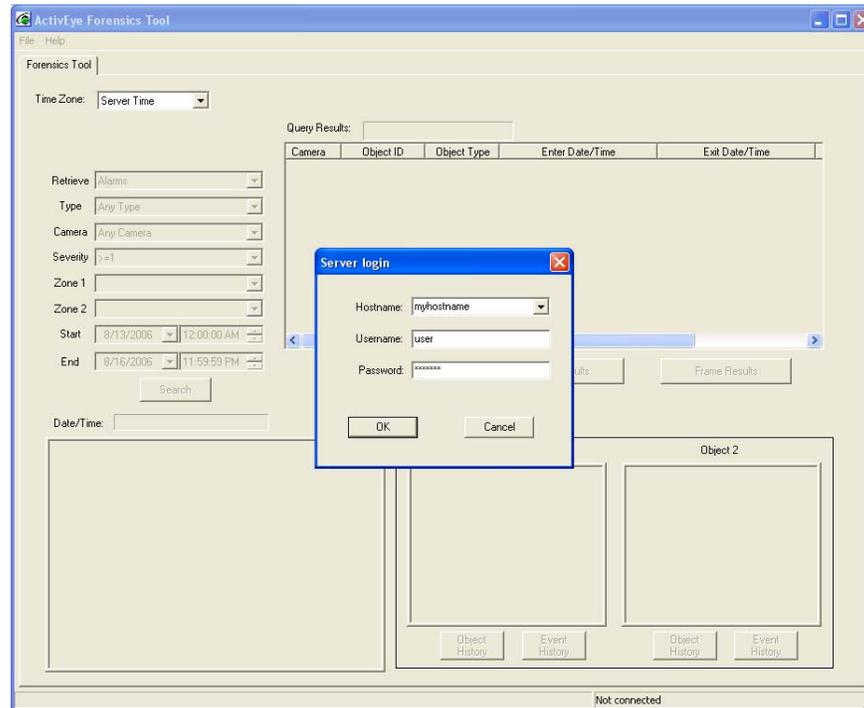
This chapter describes how to use the Forensics Tool to retrieve alarms, events, objects, and key frames stored in the Analytics database on the server.

Logging On to the Server

1. Launch the Forensics Tool.
2. At the Server Logon dialog box, enter the sever host name, user name and password
3. Click **OK** (see [Figure 11-1](#)).

You can also connect to the Analytics server by selecting **Connect to remote server** from the **File** menu.

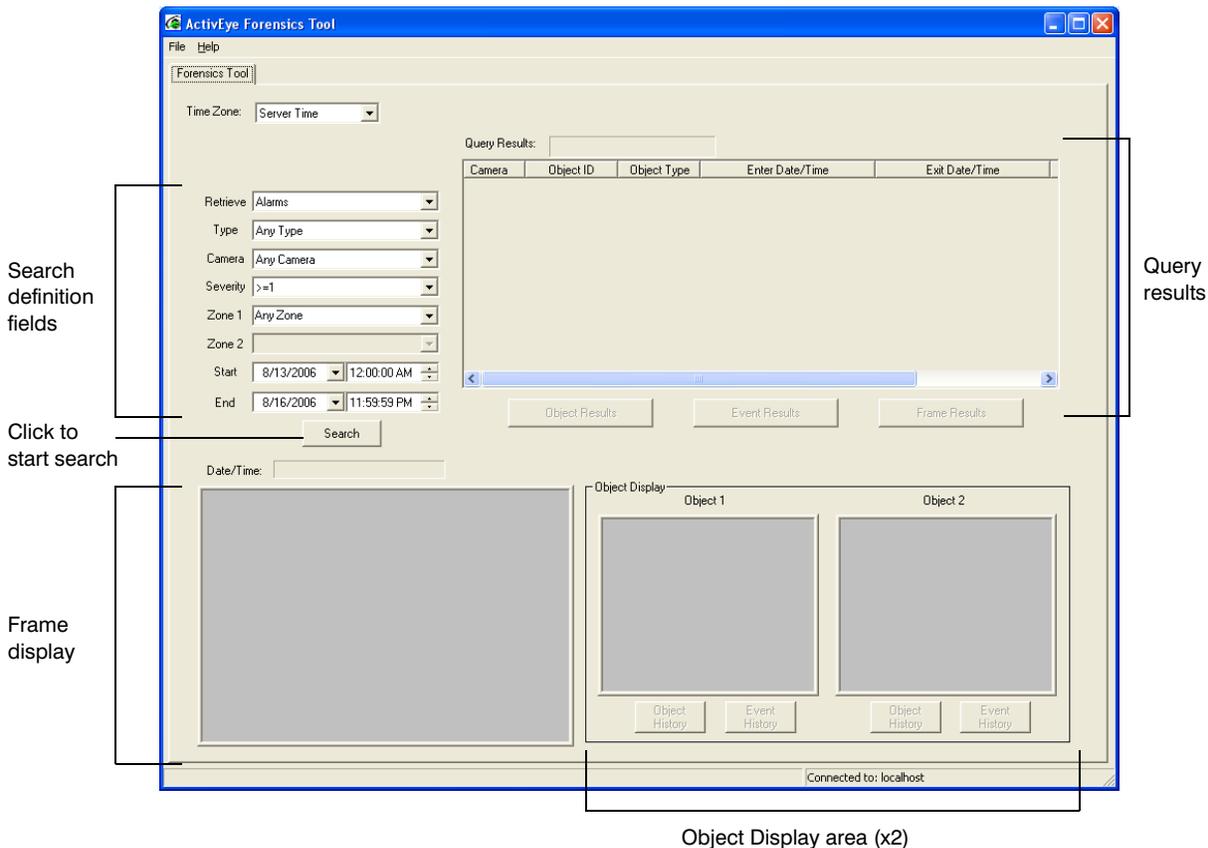
Figure 11-1 Server Login Dialog



The four areas in the GUI for live retrieval are:

- Search Definition (containing multiple drop-down lists)
- Query Results
- Frame Display
- Two Object Display windows

Figure 11-2 Forensics Tool



Starting a Search

To search the database on the Analytics server:

1. Define the query by setting some or all of the following fields:

Table 11-1 Search Field Definitions

Field	Description
Time Zone	Perform the search using Server Time, Local Time, or GMT (UTC, Greenwich Mean Time).
Retrieve	Select to search for Alarms, Events, Objects, or image Frames.
Type	Refine a search using a type of event alarm, or object. The default is All Types .
Camera	Select one camera or many. The default is All Cameras .
Severity	Retrieve events or alarms at the designated severity level.
Zone 1	Further refine a search for events or alarms associated with a specific zone.

Table 11-1 Search Field Definitions (cont'd)

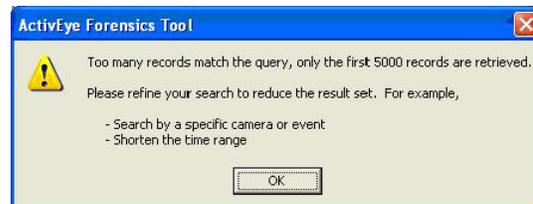
Field	Description
Zone 2	For an event that links two zones, define the second zone in addition to the first one (Zone 1) that is associated with the event.
Start	Specify the starting time of a search period.
End	Specify the ending time of a search period.

2. Click **Search** to start the search.

The search results display in the **Query Results** area on the right side of the screen. The total number of results that match the search query are shown in the text bar above Query Results.

Note Narrow your search parameters to retrieve fewer search results.

Note If the query result has more than 5,000 items, a warning message appears. In this case, only 5,000 items will be displayed. You must modify the query to reduce the search range to view all search results.



Viewing the Latest Alarm/Event, Object, or Frame Search Results

To view the latest alarm/event, object, or frame search results:

1. Click **Event Results**, **Object Results** or **Frame Results** under the Query Results area.
2. The Query Results display returns to the last event, object, or frame search results.

Retrieving Alarms and Events

To retrieve alarms or events:

1. Select **Alarms** or **Events** respectively from the **Retrieve** drop-down list.
2. Refine the search as required using the Type, Camera, Severity, Zone and Time quantifiers.
3. Click **Search**.

The results display in the Query Results area.

For the retrieved events, the Query Results displays camera, alarm, severity, object type, object ID, event type, zone ID, date/time, and comment fields for these events.

4. Click the column title to sort the result list in ascending or descending order. The default result list is ordered by camera name.

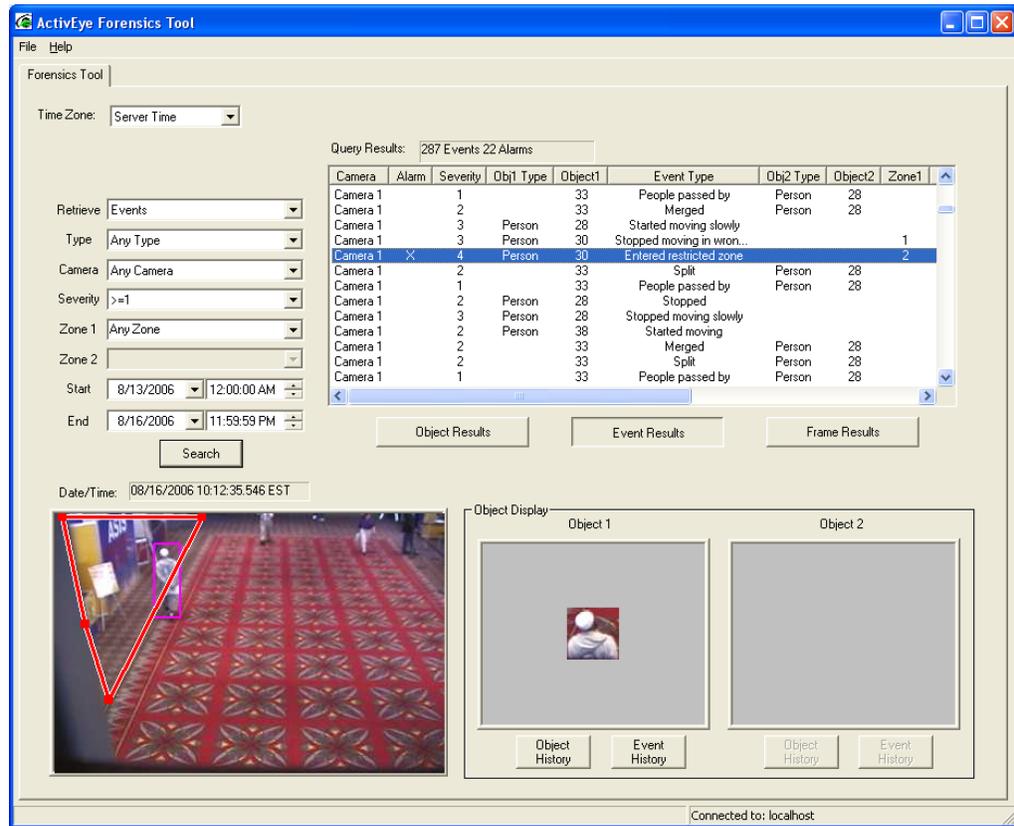
Viewing an Event Key Frame

To view the key frame of an event, click the event to highlight it in the Query Results area.

The event key frame displays in the Frame Display area on the lower left of the screen. The date and time of the key frame displays in the Date/Time field above the key frame. If the event is associated with any zone, the zone is also overlaid on the key frame.

On the right side of the Frame Display, the snapshots of object(s) involved in this event also display in the Object Display area (see [Figure 11-3](#)).

Figure 11-3 Event Retrieval



Viewing an Object Trajectory in Alarm/Event Retrieval

To view the object trajectory during alarm or event retrieval:

1. Click **Object History**.

The trajectory of the object is overlaid on the alarm or event key frame in the Frame Display area.

2. To view all the events of a specific object, click **Event History** under its snapshot in the Object Display area.

The Query Results area refreshes to list all the events of this object.

When an event in the list is selected, its corresponding frame when the event was detected also shows in the Frame Display area on the lower left of the screen.

Adding a Comment to Alarm or Event

To add a comment to an alarm or an event:

1. Double-click the alarm or event in the Query Results area.

2. An Event Comment dialog appears. Enter the comment for the alarm or event in the **Comment:** field.
3. Click **OK** to close the dialog box (see [Figure 11-4](#)).

Figure 11-4 Event Comment Dialog



Retrieving Objects

To retrieve objects:

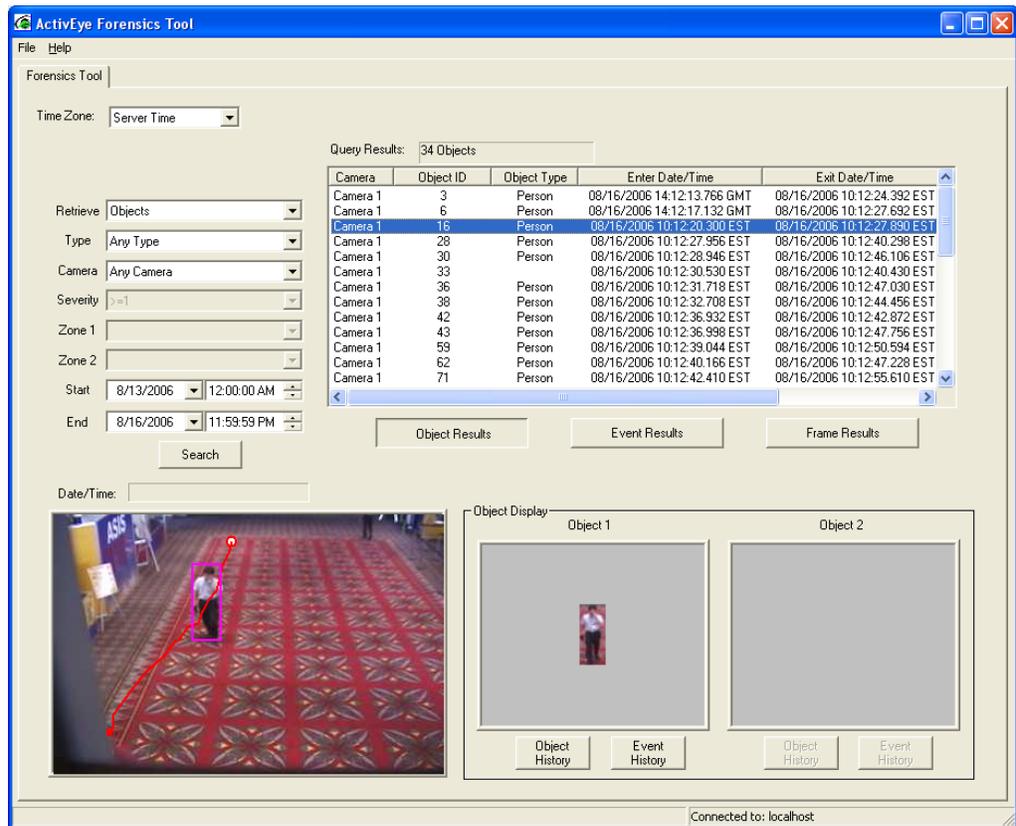
1. Select **Objects** from the Retrieve drop-down list.
2. Click **Search**.
3. If required, refine the search by specifying the object type, camera, and search time range.
The Query Results area displays camera, object ID, object type, enter time, exit time, and comment fields for the retrieved objects.
4. Click the column title to sort the result list in ascending or descending order. The default result list is ordered by camera name.

Viewing an Object Snapshot and Object Trajectory

To view the snapshot of an object, click to highlight the object in the Query Results area. The object snapshot displays in the Object Display area for Object 1.

At the same time, both the bounding box and the object trajectory are overlaid on the representative key frame in the Frame Display area (see [Figure 11-5](#)).

Figure 11-5 Object Retrieval, Viewing Object Snapshot and Trajectory

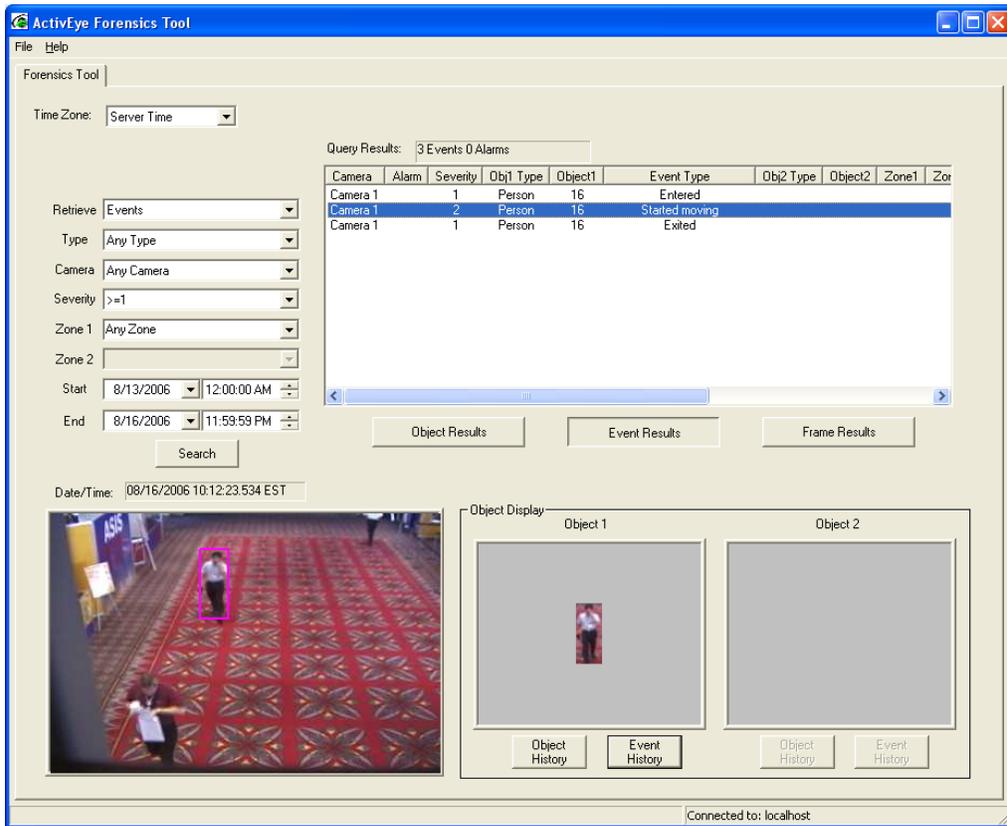


Retrieving the Event History for a Particular Object

To view all the events of the selected object:

1. Click **Event History** under the Object Display window.
The results are returned in the Query Results area.
2. The key frame shows in the Frame Display area if an event is clicked and highlighted.
The date and time of the key frame displays in the Date/Time field above the key frame (see [Figure 11-6](#)).

Figure 11-6 Object and Associated Events Retrieval



Adding a Comment to an Object in Object Retrieval

To add a comment to an object:

1. Double-click the object in the Query Results area.
2. An Object Comment dialog appears (see [Figure 11-7](#)). Enter the comment for the object in the **Comment:** field.
3. Click **OK** to close the dialog box.

Figure 11-7 Object Comment Dialog



Retrieving Frames

To retrieve frames:

1. Select **Frames** from the Retrieve drop-down list.
2. Click **Search**.
3. If required, refine the search by specifying a camera and search time range.

The results display in the Query Results area.

For the retrieved frames, the results show camera and date/time information for each frame.

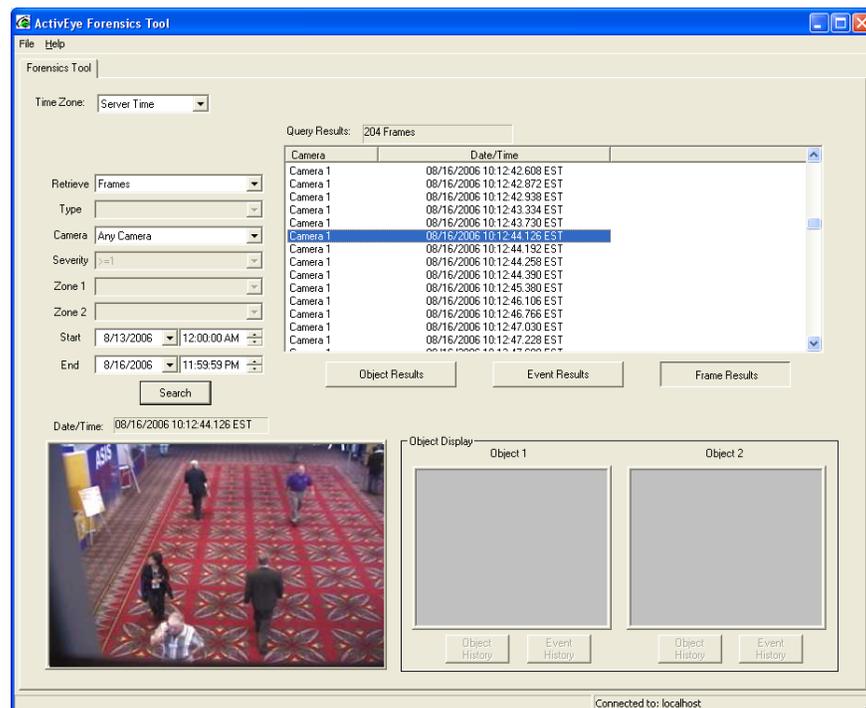
4. Click the column title to sort the list in ascending or descending order. The default result list is ordered by camera name.

Viewing Frames

To view a retrieved frame, click and highlight the frame in the Query Results area.

The frame displays in the Frame Display area on the lower left corner of the screen. The date and time of the frame is shown in the Date/Time field above the frame (see [Figure 11-8](#)).

Figure 11-8 Frame Retrieval



Reporting Tool

The Reporting Tool software package includes several components that may be installed either on the Honeywell Video Analytics processing server or on a client personal computer (PC), or sometimes both. The software is designed to work with the Honeywell Video Analytics suite to generate statistics reports from one or more server(s) at a remote location connected via the network.

The Reporting Tool software package has a client/server structure (see *Figure 12-1*). It contains a Reports Scheduler service and three client applications:

- **Reports Generator.** This is the client for generating statistics reports from a Honeywell Video Analytics server on the network.
- **Reports Scheduler.** The management tool for the Reports Scheduler, which allows the user to specify the Video Analytics servers the Reports Scheduler Service is connecting to and to set the schedule for automatic report delivery by e-mail.
- **Reports Health Monitor.** A small utility program that monitors the connection status between the Reports Scheduler server and the Video Analytics server, as well as the e-mail delivery activities.

Reports Generator

Video Analytics servers are installed at monitored locations to process live video inputs for traffic monitoring. The Reports Generator can connect to multiple Video Analytics servers through the network, enabling report generation from a remote location, such as a traffic management or building management office. It connects to the database on remote servers and generates event statistics reports based on user specification. You can specify:

- Reporting period
- Counting intervals
- List of cameras or camera groups
- Selected event and zone
- Reporting format
 - Text (to be imported into Excel Spreadsheet)
 - PDF
 - HTML
 - Microsoft® Office® Excel

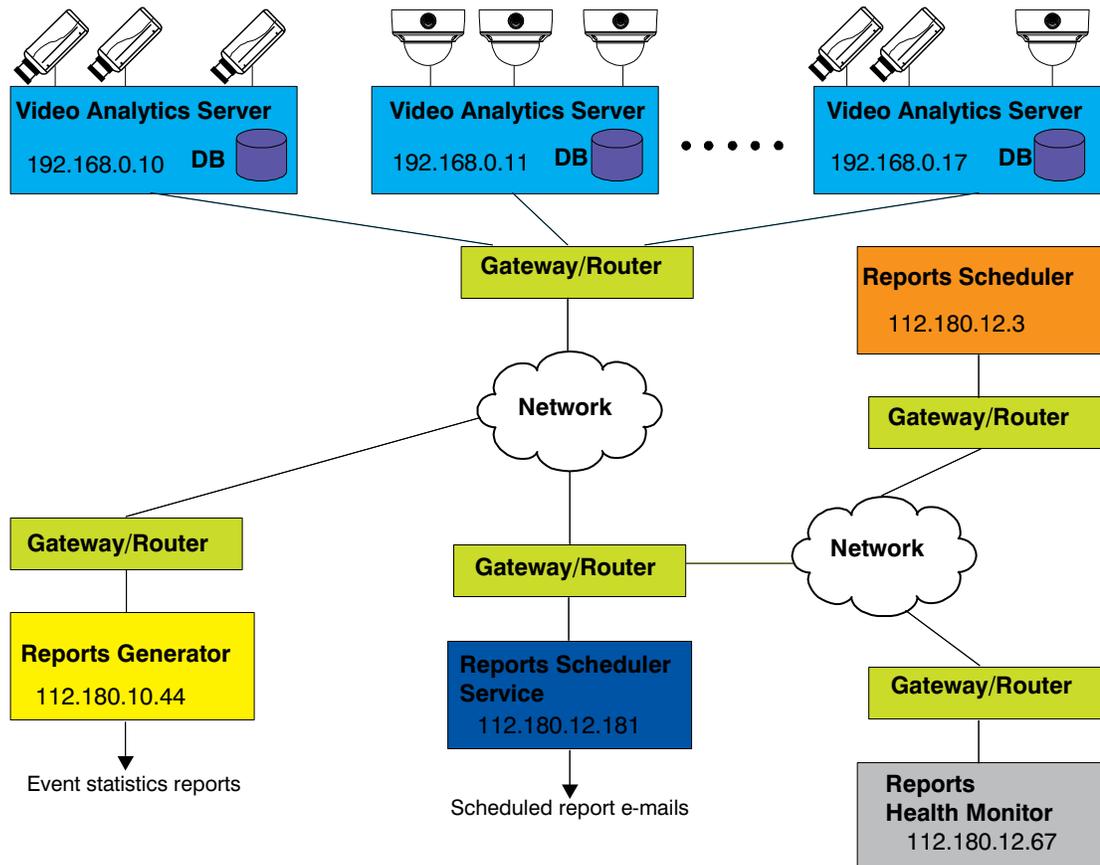
Reports Scheduler

Similarly, the Reports Scheduler Service can connect to multiple Video Analytics servers through the network to generate event statistics reports on schedules specified by the user. The scheduler service is typically installed on the Video Analytics server, or a PC that is connected to the network all the time. To configure the report template and the e-mail schedule, you can launch the Reports Scheduler application from a remote location on the network. This client tool allows you to specify the daily or hourly schedule for a report to be automatically generated and e-mailed.

Reports Health Monitor

The Reports Health Monitor allows a remote user to check the status of the report generation schedule and e-mail activities.

Figure 12-1 Reporting Tool Package



Reports Generator

The Reports Generator can be used to generate event statistics reports from Video Analytics server databases. You can run Reports Generators on the server, or on a remote client computer.

Caution To use the Reports Generator, you must have at least one printer installed on the machine where you run this application. This may be the server, the remote client computer, or both.

Configuring Reports Generator

Starting the Program

1. To start the program:
 - a. Click **Start** on your Windows taskbar.
 - b. Select **All Programs** (or Programs if using Windows 2000).
 - c. Select the **ActivEye Reporting Tool** program group, and then click **ActivEye Reports Generator** to start the program.
2. The logon dialog (see [Figure 12-2](#)) displays, prompting you to enter the hostname or IP address of a Video Analytics server, and the user name and password to gain access to the server database.

Figure 12-2 Server Login



If the connection fails, the software reports the error (for example, unable to connect, invalid user name or password). You can modify the settings and attempt to connect again by selecting **File ► Connect to remote server....**

Figure 12-3 Reports Generator File Menu

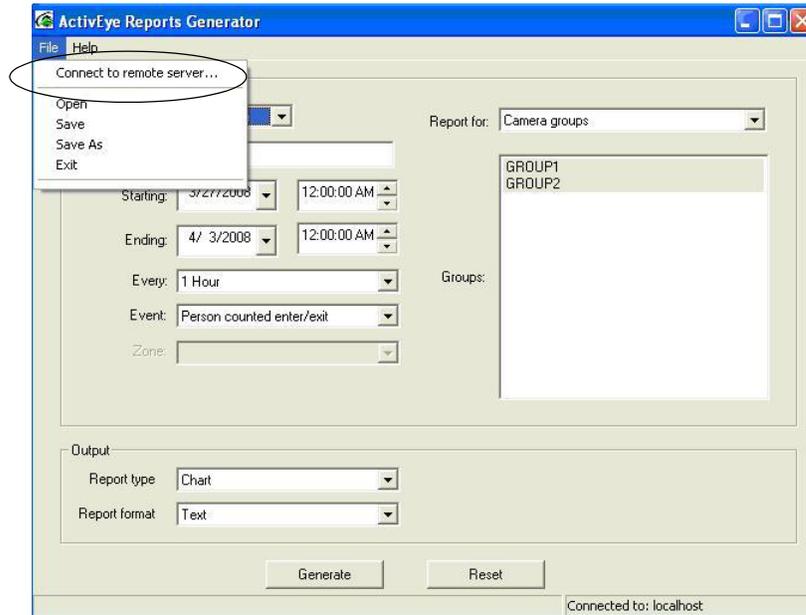
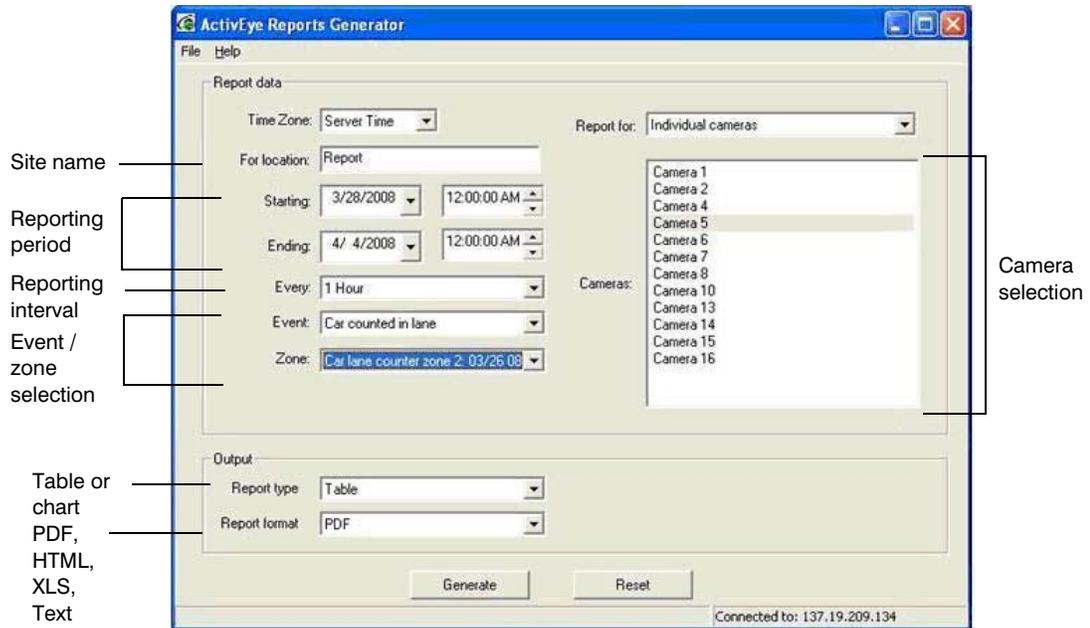


Figure 12-4 shows the Reports Generator main screen.

Figure 12-4 Reports Generator Main Screen



Specifying Site Name, Reporting Period, Time Zone

1. Enter your site name in the **For location:** field (see *Figure 12-4*).

2. If desired, specify the reporting period by modifying the **Starting:** and **Ending:** date and time.
3. In the **Time Zone** field, select: **Server Time**, **Local Time**, or **GMT (UTC)**.
4. Select a reporting interval in the **Every** field.

The generated report includes the statistics of the selected event during the specified time period with the frequency that you specify in the **Every** field, as explained in the next section.

Specifying Reporting Interval

To specify the reporting interval, select the appropriate reporting interval in the **Every** field (see [Figure 12-4](#)). The interval can be:

- Every 1, 5, 15, or 30 minutes
- Every 1, 2, 4, 8, or 12 hours
- 1 day
- 1 week

Selecting Cameras or Camera Groups

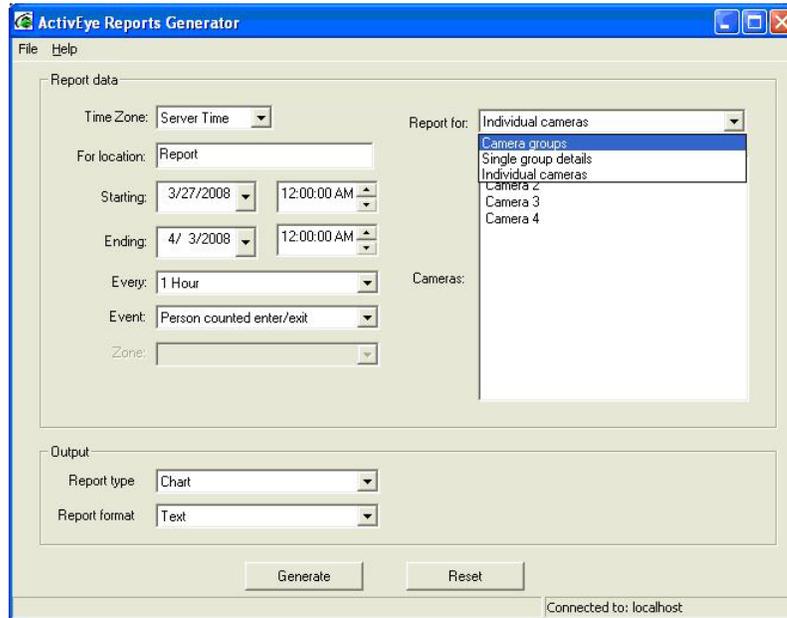
You can select the cameras or camera groups that you want to generate the reports for. In the **Report for** field, there are three options (see [Figure 12-5](#)):

- **Camera groups:** You can make multiple selection of all the available camera groups during the reporting period. The generated report will be structured on a per group basis. For more information on camera groups, please see [Chapter 7](#).
- **Single group details:** You can select a single camera group from the list of available camera groups. The generated report will be structured to contain statistics for each individual camera that belongs to the selected camera group.
- **Individual Cameras:** You can make multiple selections of all the available cameras during the reporting periods. The generated report will be structured on a per camera basis.

Every time the reporting period is modified, the list of available cameras or camera groups updates accordingly.

To make multiple selections from the list of available cameras or camera groups, press and hold **Shift** while left-clicking your mouse to add multiple selections.

Figure 12-5 Cameras or Camera Groups Selection



Selecting the Event and Zone for Generating Report

1. From the **Event:** list you can select the event for which you want to generate the statistics report (see [Figure 12-4](#)).
2. In the case where only one camera is selected, the **Zone:** list shows the zones configured for the selected event during the specified reporting period. If you do not select one of the zones, the Report Generator collects statistics for all zones (default setting).

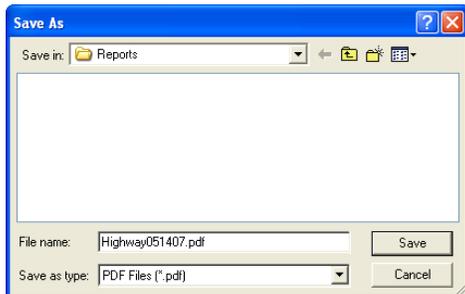
Specifying Reporting Type and Format

1. On the bottom section of the main screen (see [Figure 12-4](#)), select the **Report type** as either Chart (default) or Table.
2. From the **Report format** drop-down list, select: **PDF** (default), **HTML**, or Text.
3. Click **Save As** to specify the filename for the report to be generated.

Generating a Report

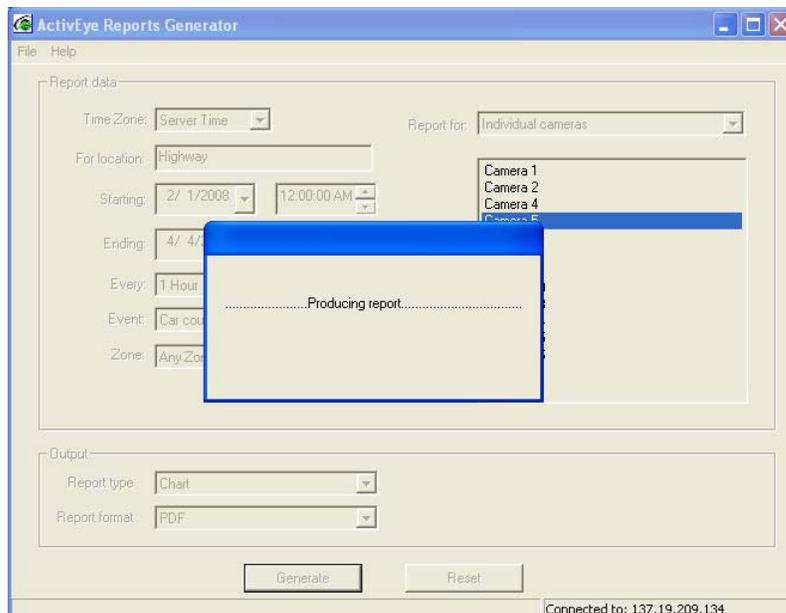
1. Click **Generate** to create the report (see [Figure 12-4](#)).
2. You are prompted to specify the file name for the report to be generated ([Figure 12-6](#)).

Figure 12-6 Specify Report File Name



3. When the report is being generated, a progress window displays (see [Figure 12-7](#)).

Figure 12-7 Generating Report



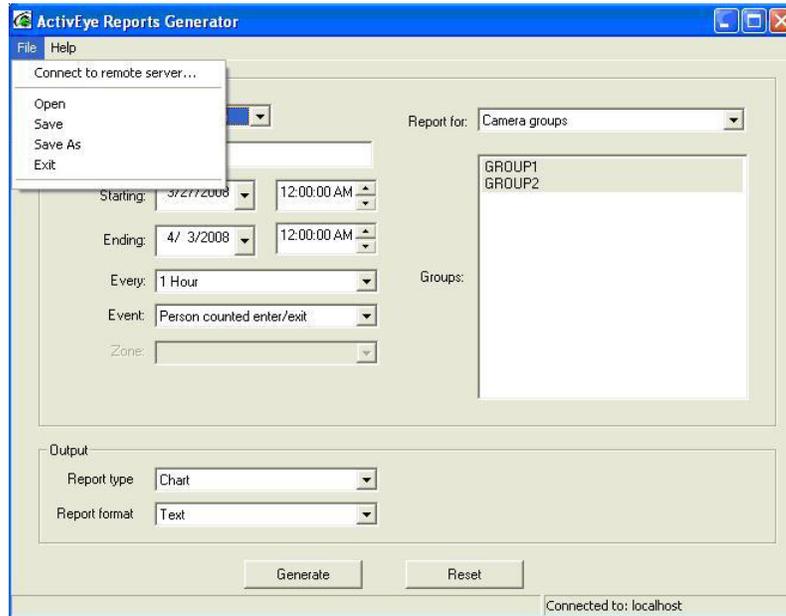
4. To reset all settings to their defaults, click **Reset**.

Saving Report Templates

To save the report template:

1. Select **File ► Save** (for an existing file) or **Save As** (for a new file), as shown in [Figure 12-8](#).
2. To open an existing report template file, select **File ► Open**.
3. By default, the extension of the configuration files is *.rep*.

Figure 12-8 File Menu in Reports Generator



Report Examples

Table Report

Figure 12-9 shows an example of a table report and Figure 12-10 shows an example report in chart (bar graph) format.

Figure 12-9 Sample Table Report

ActivEye Report

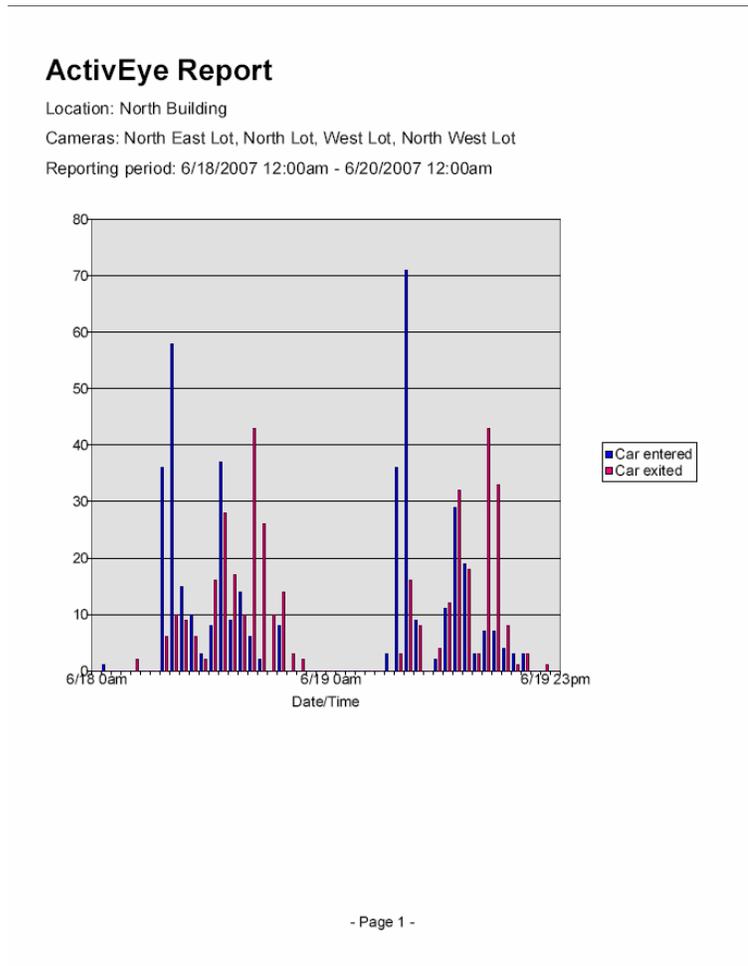
Location: North Building

Cameras: North East Lot, North Lot, West Lot, North West Lot

Reporting period: 6/18/2007 12:00am - 6/20/2007 12:00am

Date/Time	North East Lot		North Lot		West Lot		North West Lot		All cams	
	Enter	Exit	Enter	Exit	Enter	Exit	Enter	Exit	Enter	Exit
6/18 0am	0	0	0	0	0	0	0	0	0	0
6/18 1am	0	0	0	0	0	0	1	0	1	0
6/18 2am	0	0	0	0	0	0	0	0	0	0
6/18 3am	0	0	0	0	0	0	0	0	0	0
6/18 4am	0	0	0	2	0	0	0	0	0	2
6/18 5am	0	0	0	0	0	0	0	0	0	0
6/18 6am	0	0	0	0	0	0	0	0	0	0
6/18 7am	3	0	10	2	13	2	10	2	36	6
6/18 8am	6	1	18	2	17	3	17	4	58	10
6/18 9am	0	0	5	3	5	3	5	3	15	9
6/18 10am	1	0	3	2	3	2	3	2	10	6
6/18 11am	0	1	1	1	1	0	1	0	3	2
6/18 12pm	2	2	1	4	1	4	4	6	8	16
6/18 13pm	3	1	12	9	11	9	11	9	37	28
6/18 14pm	2	1	1	4	3	6	3	6	9	17
6/18 15pm	0	0	4	3	5	3	5	4	14	10
6/18 16pm	0	4	2	10	2	15	2	14	6	43
6/18 17pm	0	1	0	8	1	8	1	9	2	26
6/18 18pm	0	1	0	1	0	4	0	4	0	10
6/18 19pm	2	3	2	3	2	4	2	4	8	14
6/18 20pm	0	0	0	1	0	1	0	1	0	3
6/18 21pm	0	0	0	1	0	0	0	1	0	2
6/18 22pm	0	0	0	0	0	0	0	0	0	0
6/18 23pm	0	0	0	0	0	0	0	0	0	0
6/19 0am	0	0	0	0	0	0	0	0	0	0
6/19 1am	0	0	0	0	0	0	0	0	0	0
6/19 2am	0	0	0	0	0	0	0	0	0	0
6/19 3am	0	0	0	0	0	0	0	0	0	0
Page totals:	19	15	59	56	64	64	65	69	207	204

Figure 12-10 Sample Chart Report



Reports Scheduler

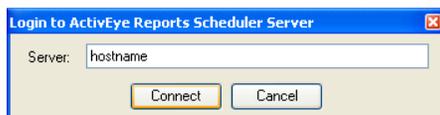
The Reports Scheduler can be used to set up the schedule for generating event statistics reports and delivering them by e-mail. After an initial setup you will receive scheduled e-mail reports to stay informed of the event statistics update.

Using the Reports Scheduler

Starting the Program

1. To start the program:
 - a. Click **Start** on your Windows taskbar.
 - b. Select **All Programs** (or Programs if using Windows 2000).
 - c. Select the **ActivEye Reporting Tool** program group, and then click **ActivEye Reports Scheduler** to start the program.
2. The logon dialog (see [Figure 12-11](#)) displays, prompting you to enter the hostname or IP address of a Video Analytics server.

Figure 12-11 Reports Scheduler Server Logon



If the connection fails, the software reports the error (for example, unable to connect, invalid machine name). You can modify the settings and attempt to connect again by selecting **File** ► **Login**.

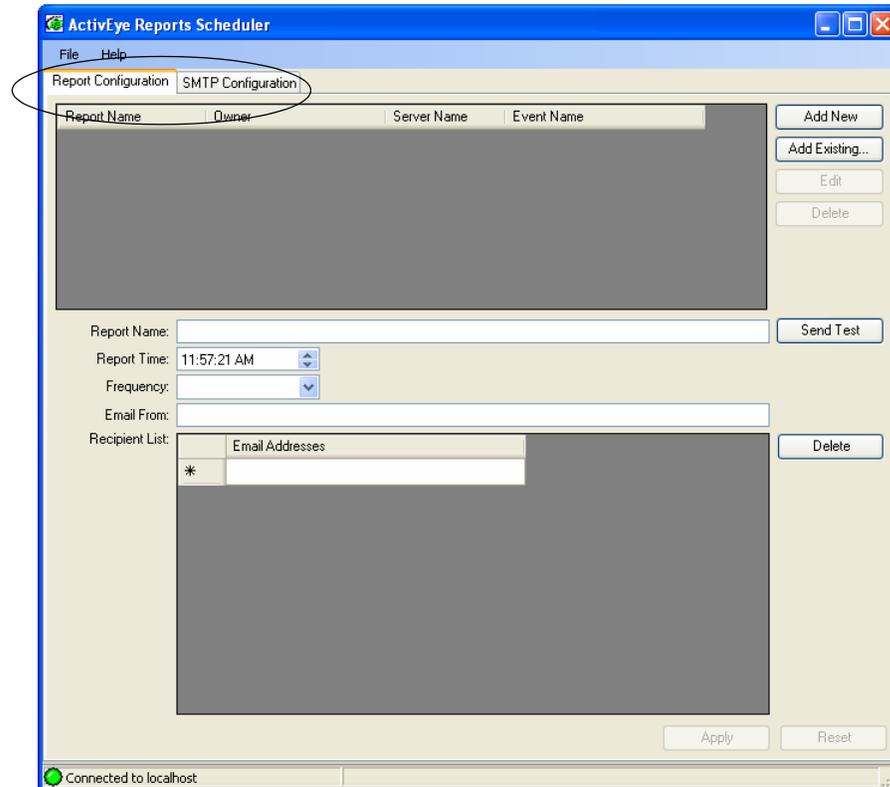


After the connection to the Reports Scheduler server is established, the Reports Health Monitor displays the status of the server and the upcoming report schedule (see [Figure 12-12](#)). A green dot indicates that the server is working properly. A red dot indicates that the server is disabled or the connection to the server is lost.

The Reports Scheduler main window is shown in [Figure 12-12](#). There are two pages on the main screen:

- On the Report Configuration page you can add multiple report templates, set up the reporting time and frequency, and specify the e-mail recipients for each of the reports. On the SMTP Configuration page you can set up the parameters to be used to send e-mails from the Reports Scheduler server.

Figure 12-12 Reports Scheduler Main Screen

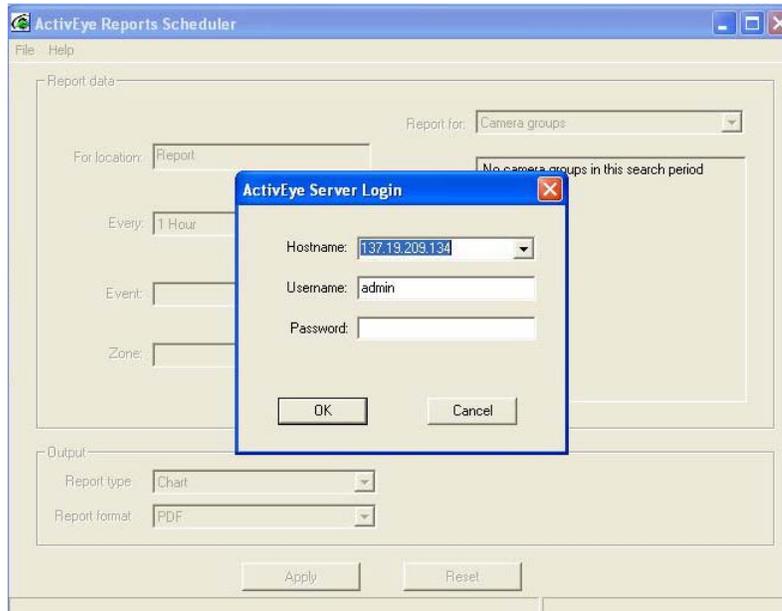


Adding a New Report Template

To add a new report template:

1. Click **Add New** on the upper right of the Report Configuration page.
2. You are prompted to log on (see [Figure 12-13](#)). Specify the hostname or IP address of a Video Analytics server, and the user name and password to gain access to the server database.

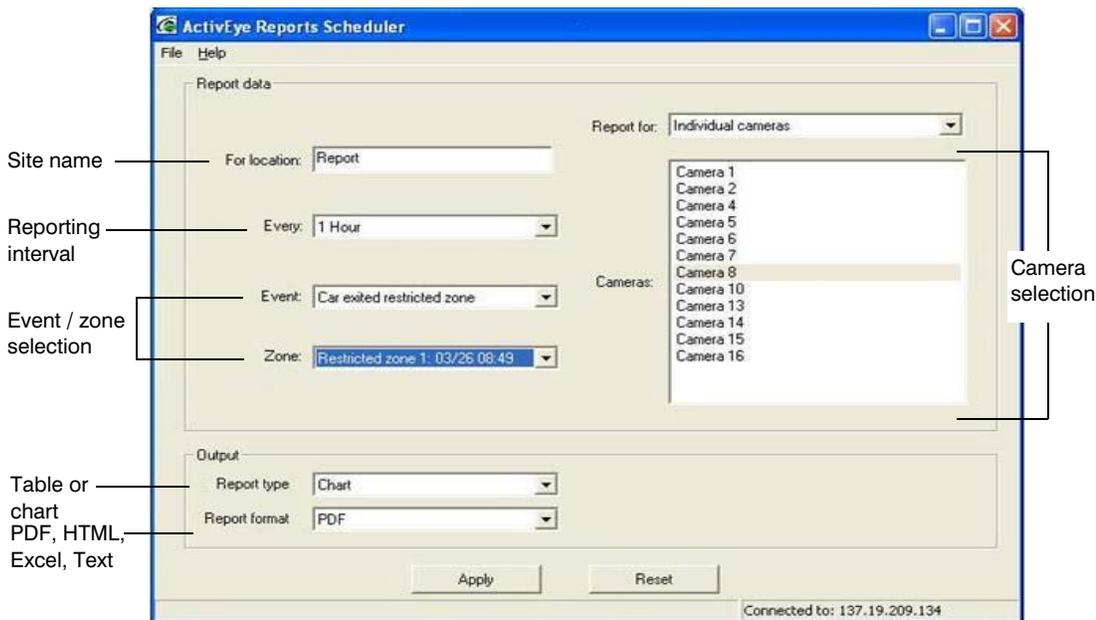
Figure 12-13 Server Template Logon



If the connection fails, the software reports the error (for example, unable to connect, invalid user name or password). Modify the settings and attempt to connect again.

3. After a connection is established with the Video Analytics server, you can configure a report template by specifying the site name, reporting interval, cameras, event and zone, report type and format (see Figure 12-14).

Figure 12-14 Configure Report Template



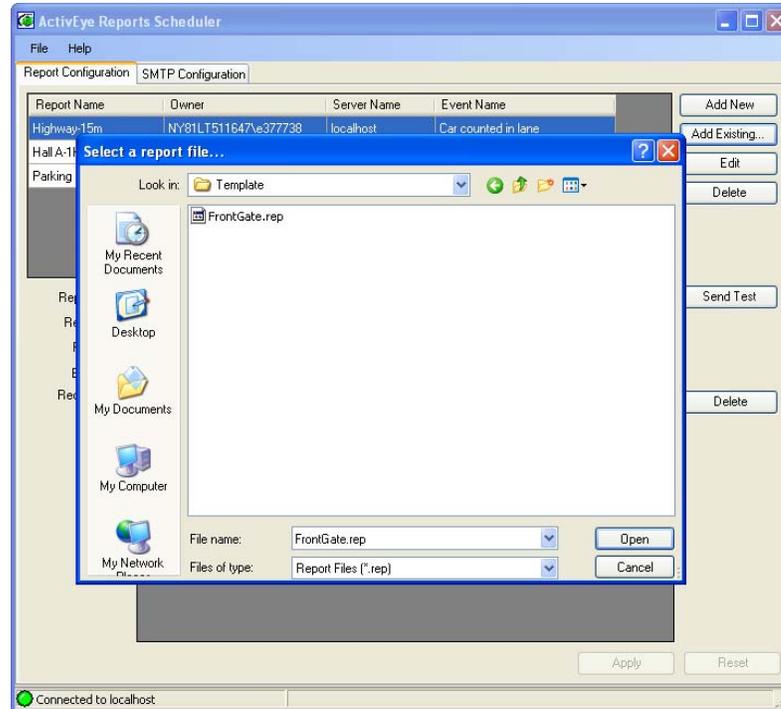
4. Click **Apply** to have the settings take effect.

Adding an Existing Report Template

Alternatively, you can add a report template previously saved by the Reports Generator.

1. Click **Add Existing**.
2. Locate the report template on the disk.
3. Click **Open** to add the report template to the Reports Scheduler (see [Figure 12-15](#)).

Figure 12-15 Add an Existing Report Template

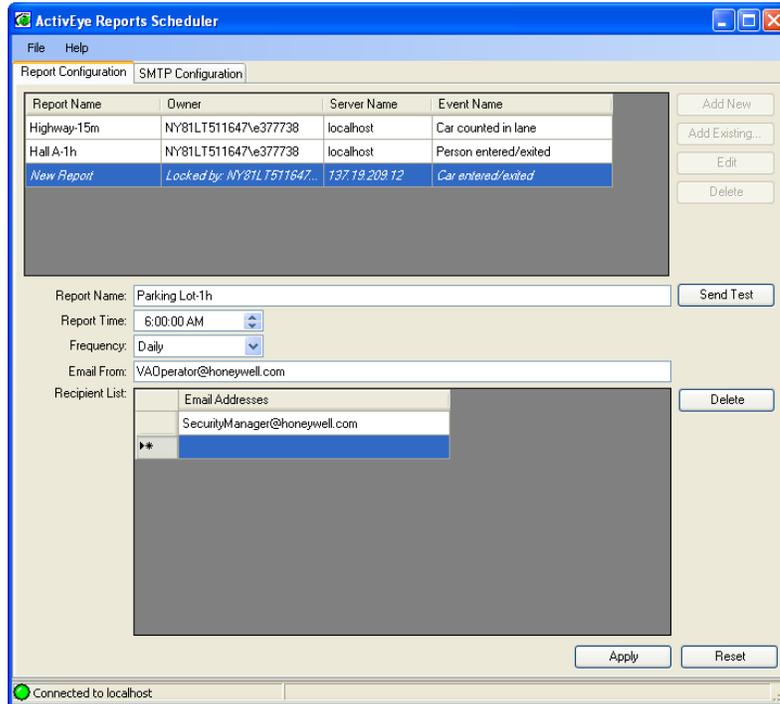


Setting Up a Reporting Schedule

After a report template is added or selected, the fields for setting the schedule are activated for editing (see [Figure 12-16](#)).

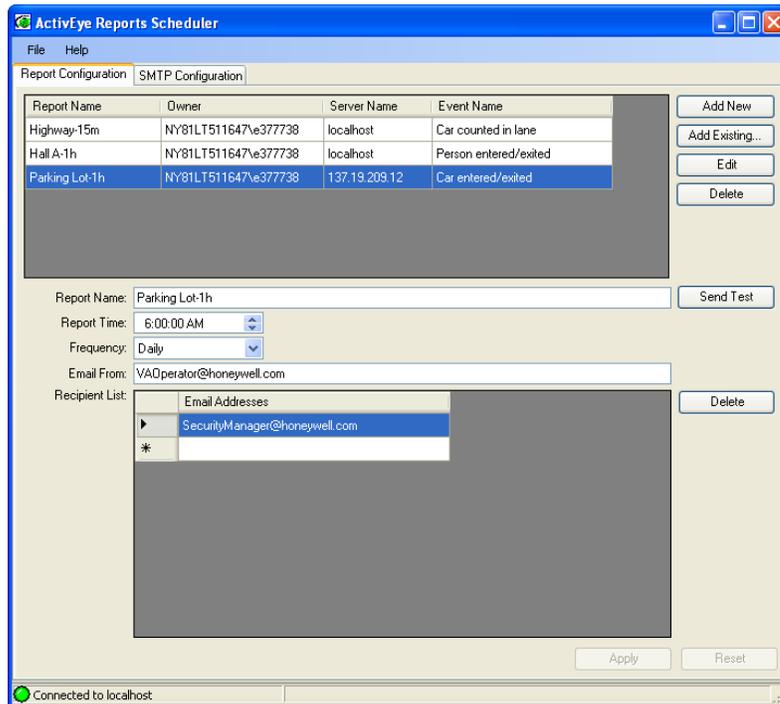
1. In the **Report Name** field, type in the name of the report.
2. Set the next time the report will be sent in the **Report Time** field.
3. You can set the frequency of sending the report to be either **Daily** or **Hourly**.
4. In the **Email from** field, type in the address that you want to appear as the sender in the recipient's mailbox.
5. You can add a list of recipients in the **Recipient List** field by typing in a valid e-mail address in an empty slot.
6. To delete an e-mail recipient:
 - a. Select the e-mail address
 - b. Click **Delete** on the right of the Recipient List field.

Figure 12-16 Set up Reporting Schedule



- After you finish setting up the reporting schedule the selected report, click **Apply** to have the changes take effect (see [Figure 12-17](#)).

Figure 12-17 Apply Schedule Settings to the Selected Report Template



Modifying a Report Template or Report Schedule

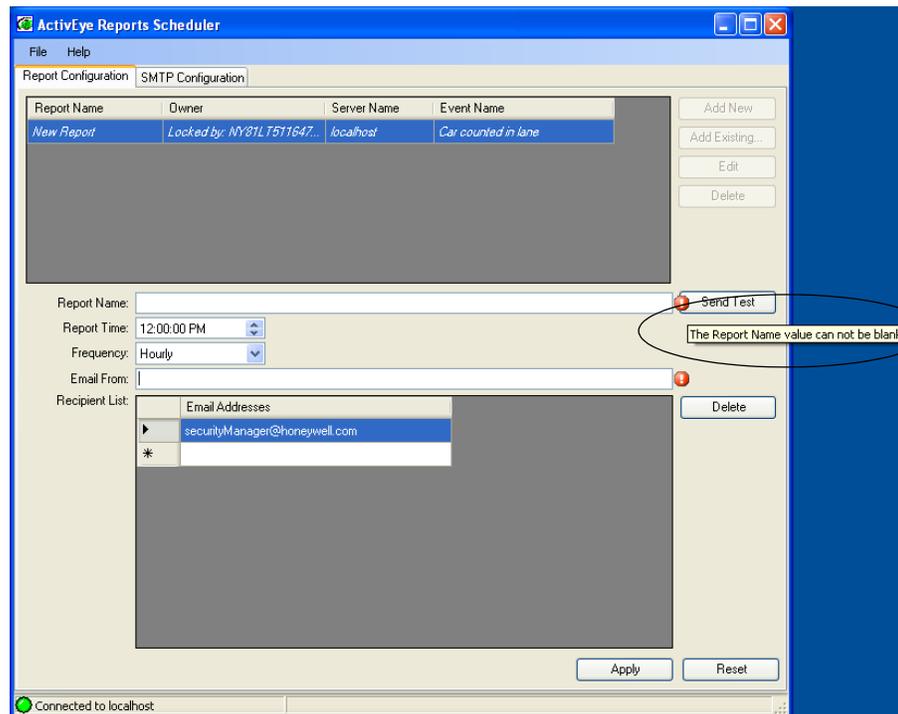
To modify any report template and its reporting schedule:

1. Select the report template in the list
2. Click **Edit**.

Similarly, you can delete a report template by selecting it from the list and then click **Delete**.

If any of the required fields is left blank, a warning message appears as the mouse is moved over to where the warning occurs. See [Figure 12-18](#) for an example.

Figure 12-18 Warnings for Incomplete Settings

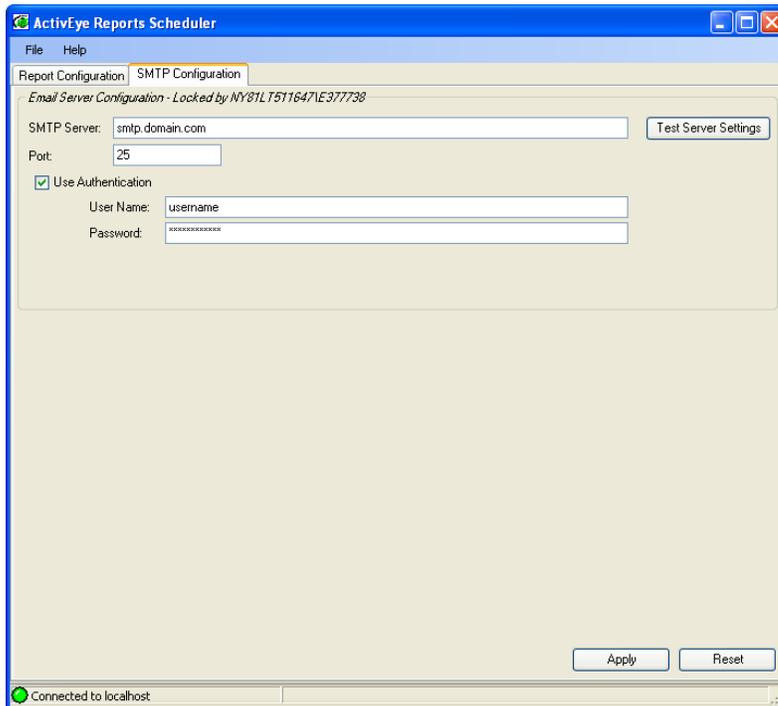


Testing the SMTP Configuration

You must set up and test the SMTP Configuration to complete the scheduling setup.

1. Enter the hostname or IP address and the port number of your SMTP server (see [Figure 12-19](#)).
2. If your SMTP server requires authentication, check **Use Authentication**.
3. Provide the **User Name** and **Password** pair for authentication purpose.

Figure 12-19 SMTP Configuration



4. Click **Test Server Settings** to make sure the report e-mail will be sent out properly.
5. The Test SMTP Settings dialog box displays (see [Figure 12-20](#)). Fill in the **Email To** and **Email From** fields.
6. Click **Send**.
7. Check the message in the SMTP Test Results dialog (see [Figure 12-21](#)) and modify the SMTP settings accordingly. The recipient specified in the **Email To** field should receive an e-mail with both the subject line and e-mail body containing the text **ActivEye Reports Scheduler SMTP Settings Test Message**.
8. Click **Apply** to save the SMTP configuration.

You can also test if the e-mail recipients list for each report template is correct.

1. Select the Report Configuration tab to switch back to the Report Configuration page.
2. Select a report template.
3. Click **Send Test** on the middle right of the window.

All the recipients specified in the Recipient List field should receive an e-mail with both the subject line and e-mail body containing the text **ActivEye Reports Scheduler Email Settings Test Message**.

Figure 12-20 Test SMTP Settings

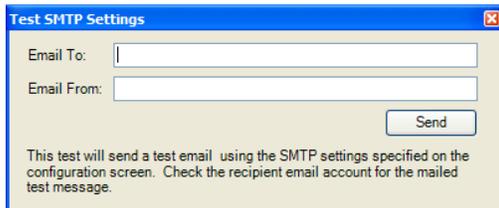
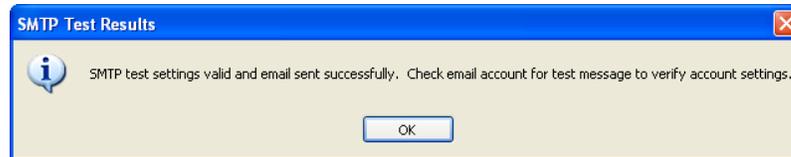


Figure 12-21 SMTP Test Results



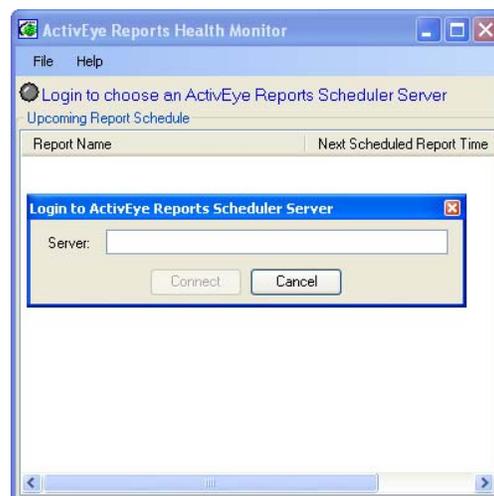
Reports Health Monitor

The Reports Health Monitor can be used to monitor the e-mail activities on the Reports Scheduler server.

Using the Reports Health Monitor

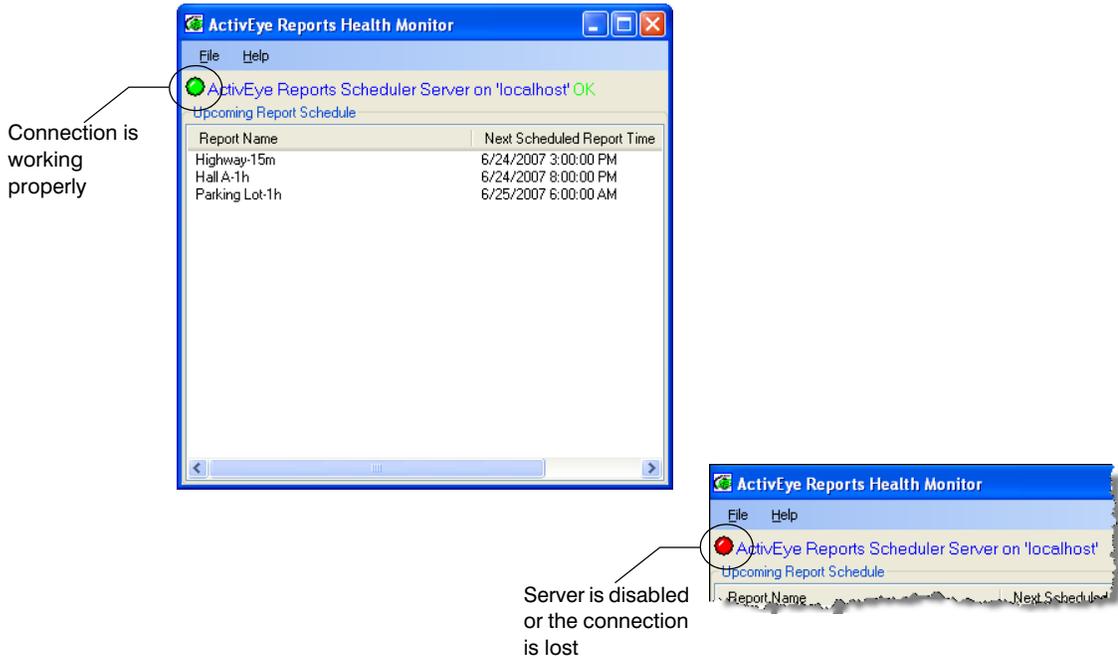
1. To start the program:
 - a. Click **Start** on your Windows taskbar.
 - b. Select **All Programs** (or Programs if using Windows 2000).
 - c. Select the **ActivEye Reporting Tool** program group, and then click **ActivEye Reports Health Monitor** to start the program.
2. The login dialog (see [Figure 12-22](#)) displays, prompting you to enter the hostname or IP address of a Reports Scheduler server.

Figure 12-22 Reports Health Monitor Logon



After the connection to the Reports Scheduler server is established, the Reports Health Monitor displays the status of the server and the upcoming report schedule (Figure 12-23). A green dot indicates that the server is working properly. A red dot indicates that the server is disabled or the connection to the server is lost.

Figure 12-23 Reports Health Monitor Main Screen



Alarm Management

The Alarm Management component allows a security operator to monitor real-time alarms at a central station from multiple Video Analytics servers.

This chapter covers the alarm management capability offered in the Honeywell Video Analytics product via the use of the following two client applications:

- **Alarm Watch Admin.** Used for configuring the Alarm Management Server (AMS), selecting analytics servers to connect to, adding user-defined alarm acknowledgement states, setting up AMS user accounts and database properties, and for configuring alarm suspension rules.
- **Alarm Watch Station.** Used for monitoring, handling and acknowledging alarms, and for viewing alarm details and acknowledgement states.

Alarm Management Overview

In Honeywell Video Analytics V4.7, the Alarm Management mechanism has been redesigned. The Alarm Management Server (AMS) is a service that connects to multiple Honeywell Video Analytics servers to receive analytics alarms from these servers.

The Alarm Management Server has its own alarm database which stores alarm data, acknowledgement states, and user comments for real-time alarm management.

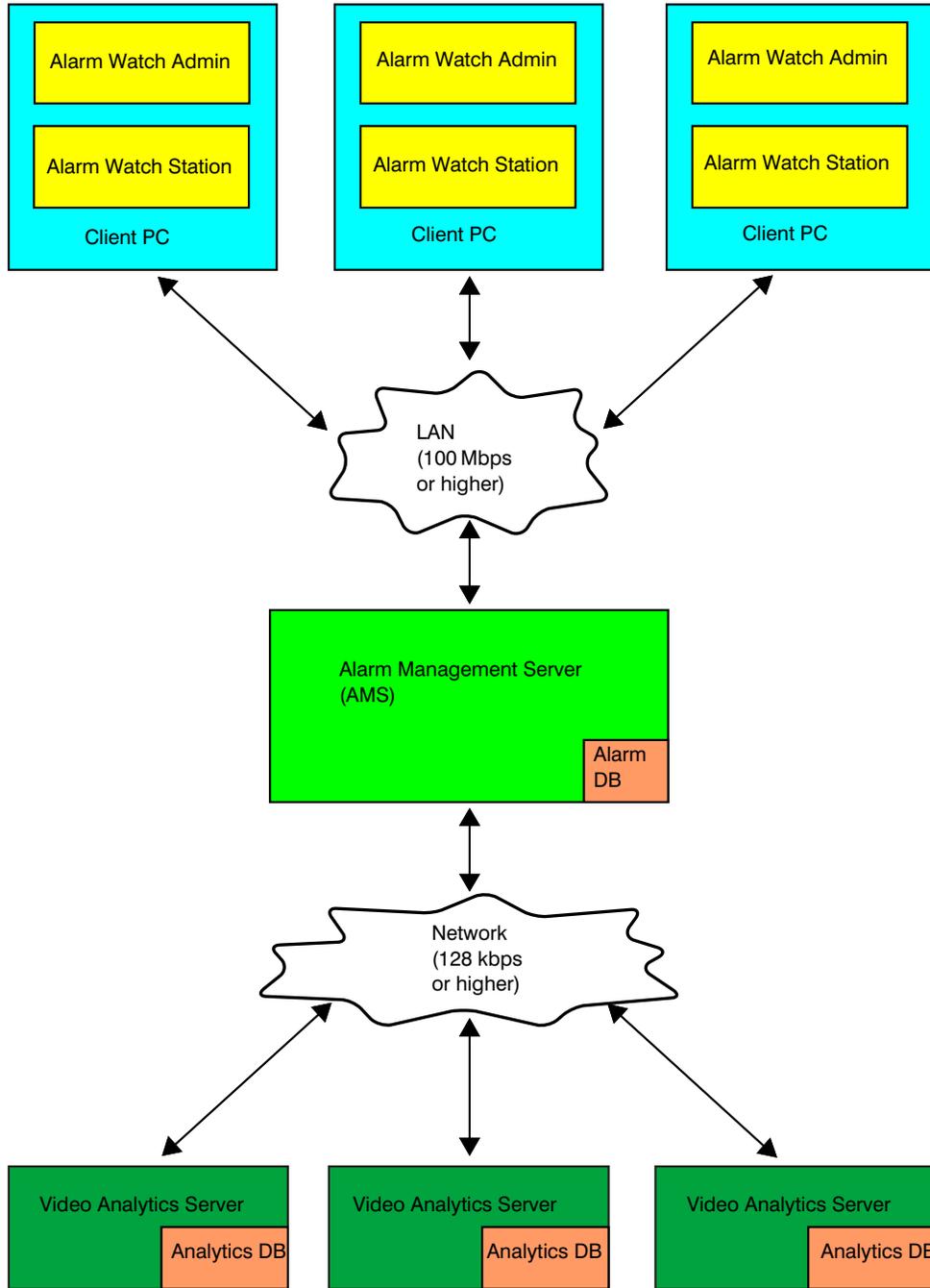
Now not only can security operators can monitor real-time alarms coming from multiple Video Analytics servers; they can also share the monitoring responsibility and work in a fully collaborative environment. Multiple security operators on separate workstations can run simultaneous Alarm Watch Station (AWS) client applications to connect to the Alarm Management Server and collaboratively manage real-time alarms coming from a number of Analytics servers. The alarm acknowledgement state modified by one operator can be seen on the Alarm Watch Station GUI by all other operators in real-time.

There are three components in the software that enable Alarm Management functionality:

- **Alarm Management Server.** The AMS runs as a Windows service on the Alarm Management Server PC. It serves as a communication interface between all Video Analytics servers and the Alarm Watch Station client applications. AMS connects to the servers, stores all the incoming alarms into a local database, and sends these alarms to all connected Alarm Watch Stations.
- **Alarm Watch Admin.** A client application that allows the user to configure the Alarm Management Server. The user can configure connected Video Analytics servers, define alarm acknowledgement states that best suit their own alarm management operation, create AMS user accounts, and create alarm suspension rules (times when alarms are not generated by AMS). Alarm Watch Admin is included in the Honeywell Video Analytics - Client package.
- **Alarm Watch Station.** A redesign from the previous version of Alarm Watch Station, this client application now works with the Alarm Management Server to allow the user to view and manage all the alarms coming from the HVA servers connected to AMS. The user can view and modify the status of any alarm; this status is shared across all connected Alarm Watch Station clients. Alarm Watch Station is included in the Honeywell Video Analytics - Client package.

Figure 13-1 illustrates the components that make up the Alarm Management System. The AMS Administrator can add, modify, or delete any configuration setting in the AMS. Alarm Watch Station also communicates with the AMS and displays live and historical alarms. The AMS receives alarms from all the Video Analytics servers that have successfully connected to it, and distributes these alarms to all the Alarm Watch Stations to which the server has successfully connected.

Figure 13-1 Alarm Management Server System Diagram



Alarm Watch Admin

Alarm Watch Admin allows you to connect to the Alarm Management Server to modify its configuration settings. The user must be assigned administrator permission to use Alarm Watch Admin.

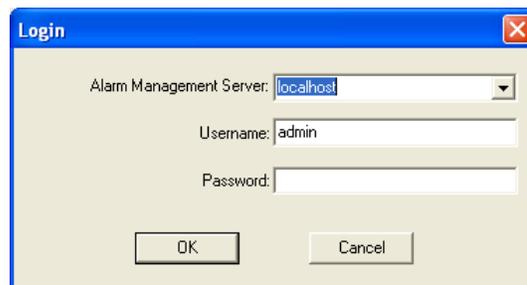
Note The default administrator created during installation of AMS has **admin** permission.

Logging On to Alarm Watch Admin

To log on to Alarm Watch Admin:

1. Type the hostname or the IP address of the Alarm Management Server on your network (see [Figure 13-2](#)). Type **admin** as the user name and enter the password that you set up during the installation process.
2. Click **OK**.

Figure 13-2 Alarm Watch Admin User Login



If you see the following message, verify the host name or IP address entered, and verify that AMS is running on the specified server. This message indicates that the specified AMS could not be found.



Providing an incorrect user name or password causes an authorization failure.

Only one Alarm Watch Admin application can connect to a single AMS at a time. A second Alarm Watch Admin user trying to log on will be blocked (see the error message below).

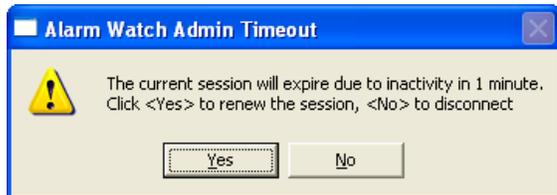


Connection Time-out Due to Inactivity

The connection of Alarm Watch Admin to Alarm Management Server will be automatically terminated due to inactivity. This safeguard:

- Prevents unauthorized users making changes to the Alarm Management Server from a currently unattended logon session.
- Ensures that the Alarm Management Server does not get inadvertently locked as only one administrator may be connected to an alarm Management Server concurrently.

When there has been inactivity for 15 minutes, the Administrative user is prompted to renew the current session. Click **Yes** to renew the session or **No** to terminate the session and disconnect from Alarm Management Server.



When there is no response, the current session is automatically terminated.



You must reconnect to Alarm Management Server to restart a new session. From Alarm Watch Admin, select **File ► Connect to Alarm Management Server (AMS)...**

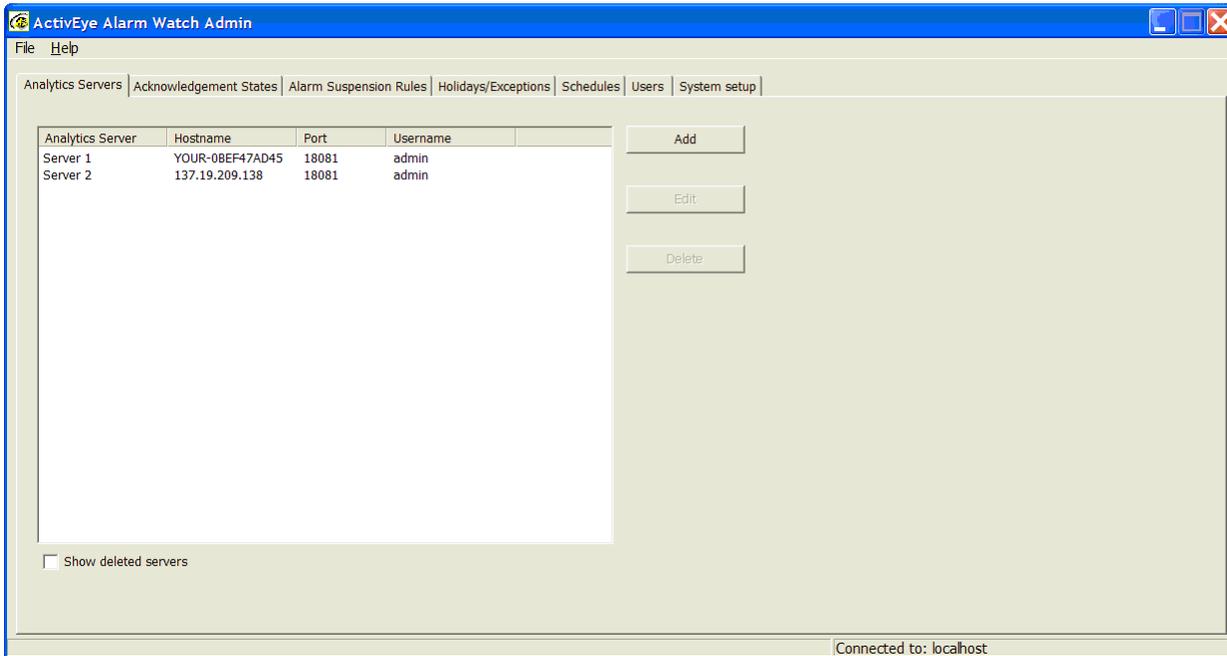
Configuring Alarm Watch Admin

When you have successfully logged on to Alarm Watch Admin, you can make the following configuration changes for the Alarm Management Server to which you are currently connected:

Table 13-1 Alarm Watch Admin Tasks

Configuration Change	Where to Access Information
Add, modify or remove Honeywell Video Analytics (HVA) servers	On the Analytics Servers page (1st tab) See page 187 .
Add, modify or remove alarm acknowledgement states	On the Acknowledgement States page (2nd tab) See page 190 .
Add, modify or remove alarm suspension rules	On the Alarm Suspension Rules page (3rd tab) See page 195 .
Add, modify or remove holiday and exception date lists for alarm suspension	On the Holidays/Exceptions page (4th tab) See page 206 .
Add, modify or remove schedules for alarm suspension	On the Schedules page (5th tab) See page 209 .
Add, modify or remove AMS users and their privileges	On the Users page (6th tab) See page 213 .
Modify system level configuration of the Alarm Management Server	On the System Setup page (7th tab) See page 215 .

Figure 13-3 Alarm Watch Admin Initial Window



The following sections describe how to make configuration changes in Alarm Watch Admin.

Managing Video Analytics Servers

Alarm Management Server acts as a central hub for analytics alarms generated by Analytics servers. In Alarm Watch Admin, the administrator user can define the Analytics servers connected to the Alarm Management Server.

Adding an Analytics Server

To add an Analytics server to AMS:

1. Click **Add**.

2. The HVA Server Properties dialog appears (see [Figure 13-4](#)). Fill in the following information for the Analytics server being added:

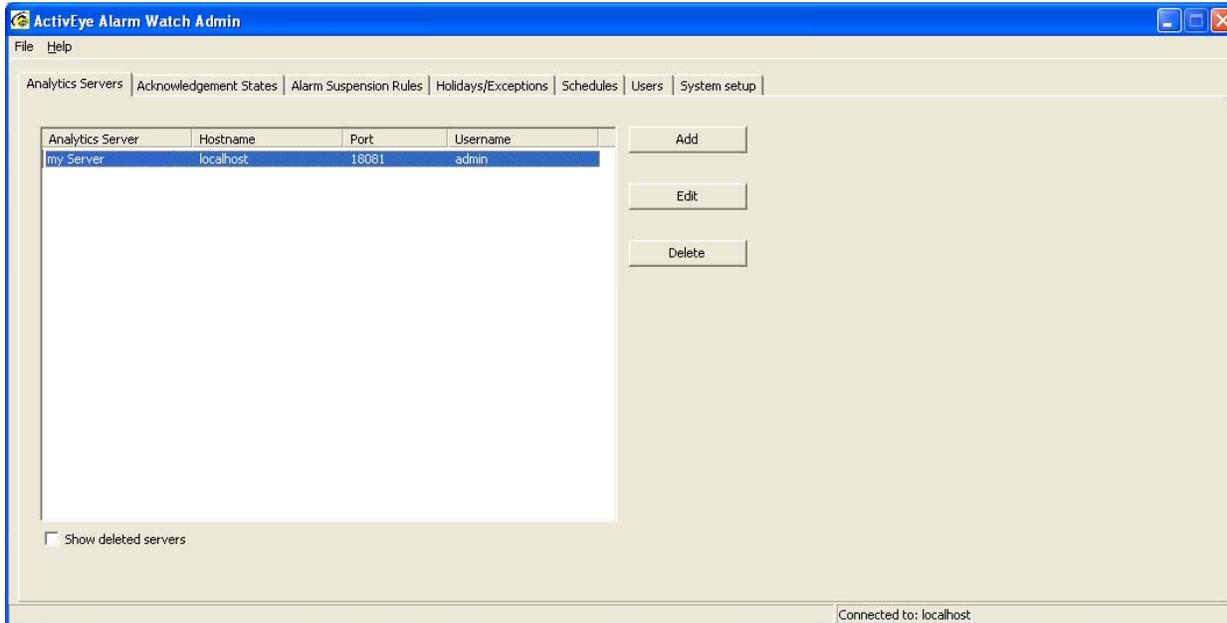
Display name	A user-defined name that uniquely identifies this HVA server
Hostname/IP address	Computer name or IP address of the HVA server
Username	A valid user name for connecting to the HVA server. This user must be in the Analytics user database as configured by ActivEye User Configuration (see Chapter 3, User Management) with both Live View and Search permissions.
Password	A valid password for this user

Figure 13-4 HVA Server Properties Dialog



3. Click **OK**.
4. AMS attempts to connect to the HVA server. On a successful connection, the HVA server is added to the Analytics Server list.

Figure 13-5 Analytics Server Added to the List



In the unlikely event the connection fails, the following error message displays. A connection failure may be caused by the HVA server not currently running, an incorrect hostname or port number, or user authentication failure on the HVA server.



Modifying an Analytics Server

To modify the properties of an HVA server:

1. Select the Analytics sever you want to modify in the list, then click **Edit**.
You may also double click on any selected server in the list.
2. Make your modifications.
3. Click **OK** to apply your changes or **Cancel** to discard your changes.

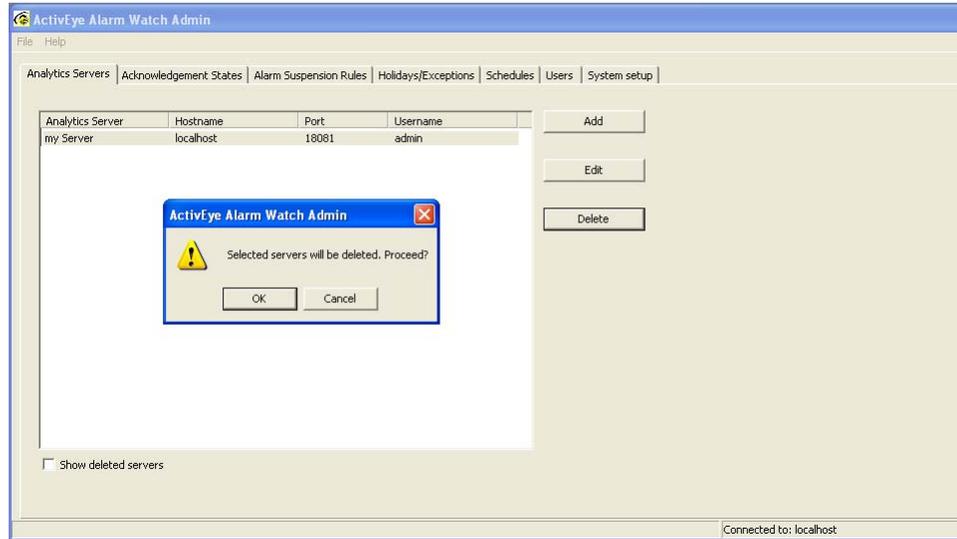
Deleting or Restoring an Analytics Server

To delete an HVA server from the Analytics servers list:

1. Select the server you want to delete, then click **Delete**.
2. You are prompted to confirm the deletion (see [Figure 13-6](#)). Click **OK** to confirm the deletion or **Cancel** to cancel the deletion.

After you confirm deletion of the HVA server, it will be removed from the Analytics Server list. A deleted server can be restored if you later decide to add the server back to the list.

Figure 13-6 Deletion of an HVA Server From the List

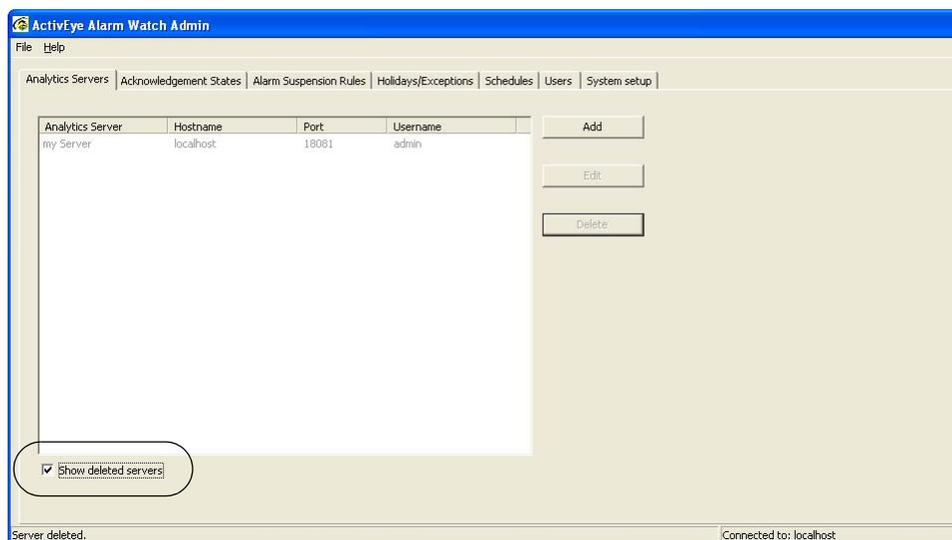


Restoring a Deleted Analytics Server

To restore a deleted HVA server:

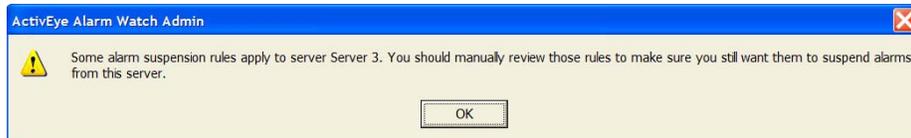
1. Select the **Show deleted servers** check box on the bottom of the page. Deleted servers appear as grayed out items in the list (see [Figure 13-7](#)).
2. Select the server you want to restore, then click **Restore**. The selected HVA server being restored must be running for the restore to succeed.

Figure 13-7 Deleted HVA Servers Displayed



If there are existing alarm suspension rules (that is, they existed before this server was deleted) that have cameras connected to this server, the following message appears.

Figure 13-8 Alarm Suspension Rules Message



To resolve this issue:

1. Go to the **Alarm Suspension Rules** tab,
2. Deselect **System**.
3. Check this server so that only the rules applying to this server are displayed.
4. Review the rules to determine if you still want them to apply.

Managing Alarm Acknowledgement States

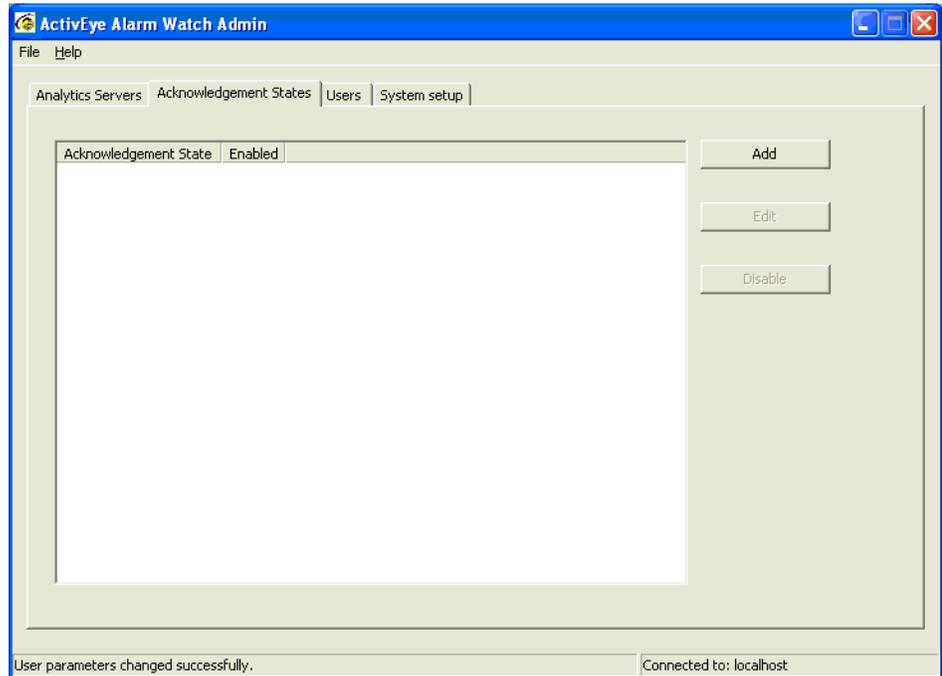
Alarm acknowledgement states are user-defined text that can be associated with an acknowledged alarm. You can customize these tags to suit your specific alarm management protocol.

For instance, a central monitoring station may require all operators to select appropriate tags upon acknowledging any alarm received at the monitoring console. Any actual break-in event must be tagged as **break-in**, any minor offence must be tagged as **minor**, and any nuisance alarm must be tagged as **false**. The Administrator can define three alarm acknowledgement states: break-in, minor or false in the Alarm Watch Admin application. The security operators can then associate each alarm with one of these acknowledgement states.

To set up alarm acknowledgement states:

1. Select the **Acknowledgement States** tab (see [Figure 13-9](#)).
2. Add, modify, or disable Alarm Acknowledgement states as desired (see following sections).
3. Click **OK** to confirm your setting.

Figure 13-9 Alarm States Tab



Adding an Alarm Acknowledgement State

To add an Alarm Acknowledgement State:

1. On the **Acknowledgement States** tab, click **Add**. The Alarm Acknowledgement State Properties dialog appears.

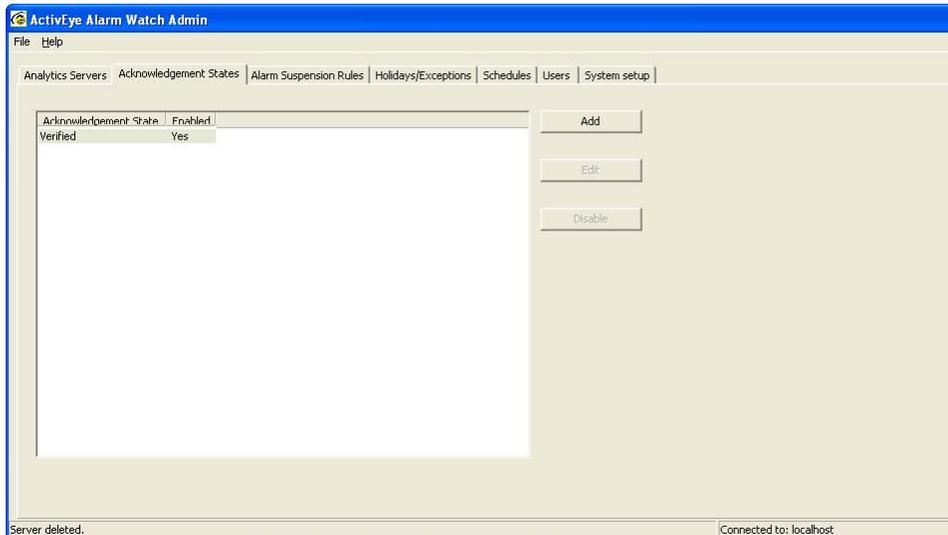
Figure 13-10 Alarm Acknowledgment State Properties Dialog



2. Type a text string into the **Alarm Acknowledgment State** field. Any new item is **Enabled** by default.

3. Click **OK**. The new state is added to the Alarm Management server. The newly added item appears in the Acknowledgement States list. This new acknowledgment state is now available across all Alarm Watch Stations connected to the same AMS.

Figure 13-11 New Acknowledgement State Added



Modifying an Alarm Acknowledgement State

To modify an Alarm Acknowledgement State:

1. Select the item you want to modify in the list, then click **Edit**,
OR
Double-click an item in the list.
2. In the Alarm Acknowledgement State Properties dialog, modify the text as required.
3. Click **OK**.

Enabling/Disabling an Alarm Acknowledgement State

To enable/disable an Alarm Acknowledgement State:

1. Select the item you wish to enable/disable in the list.
2. Click **Disable/Enable** to toggle the enabled state.

Note Alarm Watch Station operators may only assign enabled alarm acknowledgement states to selected alarms.

Managing Alarm Suspension Rules

Alarm suspension rules allow an administrator to suppress reporting of alarms from selected cameras at specified times. Possible uses for this functionality include:

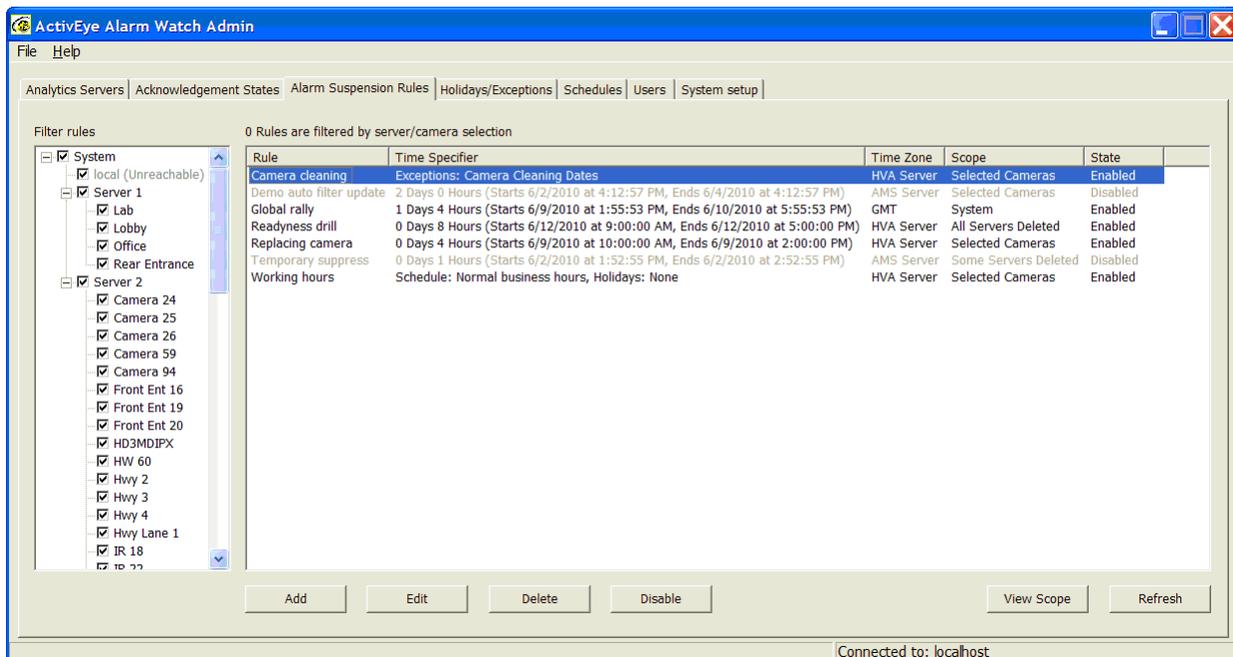
- Suspend alarms when a maintenance crew is scheduled to work in the area covered by a camera.
- Temporarily suspend alarms from a camera that is having a problem.

If the Alarm Management Server (AMS) does not support alarm suspension, the Alarm Suspension Rules, Holidays/Exceptions, and Schedules tabs have all content hidden and the following message displays in the middle of each tab:

The Alarm Management Server you are connected to does not support alarm suspension. Please upgrade Alarm Management Server to the latest version.

Alarm suspension rules are managed on the Alarm Suspension Rules tab.

Figure 13-12 Alarm Suspension Rules Tab



Expired and disabled rules are grayed out. Expired rules may be re-enabled by editing the rule and modifying the Time Specifier. The expired state of all rules is only refreshed after you click **Refresh**.

Table 13-2 explains the column options.

Table 13-2 Alarm Suspension Rules Columns

Column	Options	Description
Time Specifier		
Shows one of the following (depending on the time specifier selected for the rule)		
	X Hours Y Days	X Days Y Hours (Starts [Date] at [Time], Ends [Date] at [Time])
	Time Range	From [Date] at [Time] to [Date] at [Time]
	Custom Schedule	Schedule: [Schedule Name], Holidays: [Holiday List]
	Custom Exception	Exceptions: [Exception List]
Scope		
Shows one of the following:		
	System	When all the servers and cameras that exist in AMS match all the servers and cameras specified in the rule.
	Selected Cameras	When all the servers and cameras specified in the rule are found in AMS but the rule does not include every server/camera.
	Some Servers Deleted	When one or more of the servers specified in the rule are found in AMS, but not all are found.
	All Servers Deleted	When none of the servers specified in the rule are found in AMS; the rule refers only to servers that have been removed from AMS.
State		
Shows one of the following:		
	Enabled	The rule is enabled and will cause alarms to be suspended.
	Disabled	The rule has been manually disabled. The entire rule is grayed out in the list.
	Expired	The rule is for a time range that is in the past so the rule is no longer in effect. The entire rule is grayed out in the list.

Each rule is independent of the others and any rule settings such as dates, selected cameras, and scheduling may overlap other rules. An incoming alarm is suspended (not displayed in Alarm Watch Station) if one or more enabled rules apply to that camera at the time of the alarm.

Filtering the Alarm Suspension Rules List

The tree on the left pane of the Alarm Suspensions Rules tab is used to filter the rules that are displayed in the list on the right side of the screen. Any rule that contains at least one camera that is checked in the filter tree is displayed. Other rules are hidden (the caption above the rule list gives the number of rules that are currently filtered out/hidden by the server/camera selection in the filter tree). The tree contains the following node types:

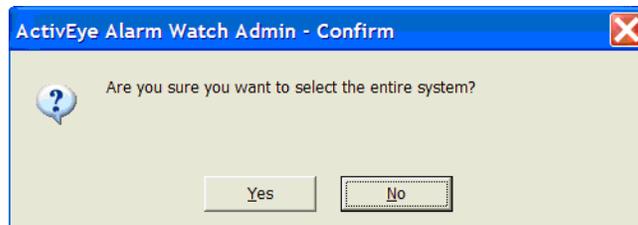
System node The system node represents/controls filtering for all the servers/cameras in the system. The check box may be:

- **Solid checked:** All cameras/servers are selected. All rules are shown. This is the initial state when Alarm Watch Admin (AWA) starts.

Clicking the check box while in this state displays the following warning. Doing this causes all server and camera nodes to become unchecked and all rules to be hidden. Additionally, the entire tree automatically expands to show all of the servers and cameras.



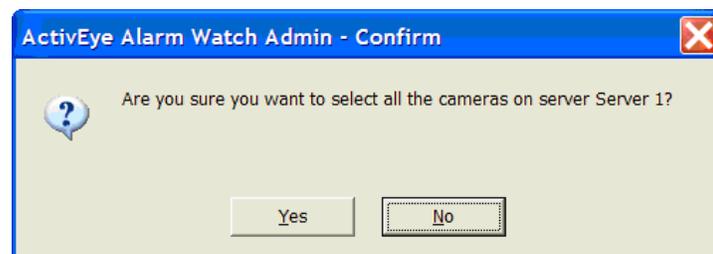
- **Unchecked:** No cameras/servers selected. All rules are hidden. Clicking the check box while in this state causes all server and camera nodes to become solid checked / all rules to be displayed.
- **Gray checked:** Some cameras/servers are selected, some are not. Only rules that apply to one or more of the selected cameras are shown. Clicking the check box while in this state displays the following prompt.



Clicking **Yes** causes all of the server's cameras to become checked. Clicking **No** causes the filter tree to remain unchanged.

Server nodes Server nodes appear indented under the System node. Each server node represents/controls filtering for the cameras for a single HVA server. There is one node corresponding to each server listed on the Analytics Servers tab. Deleted servers are not shown in the tree. The name is the display name from the Analytics Server tab. The check box is a tri-state:

- **Solid checked:** All of the server's cameras are selected. Clicking the check box while in this state causes all of the server's cameras to become unchecked. Additionally, if the server node is currently collapsed, it automatically expands to show the cameras beneath it.
- **Unchecked:** None of the server's cameras are selected. Clicking the check box while in this state cause all of the server's cameras to become checked.
- **Gray checked:** Some of the server's cameras are selected, some are not. Clicking the check box while in this state displays the following prompt.



Clicking **Yes** causes all of the server's cameras to become checked.
Clicking **No** causes the filter tree to remain unchanged.

Camera node Camera nodes appear indented under each server node. All cameras configured for the Video Analytics server appear (regardless of whether they are enabled on the server). If a Video Analytics server has been offline/unreachable since AMS started, then instead of displaying cameras underneath it, the server node is grayed out.

Each camera node represents/controls filtering for a single camera. The check box will either be:

- **Checked:** The camera is selected. Rules that apply to the camera will be shown.
- **Unchecked:** The camera is not selected. Rules that apply ONLY to that camera will not be shown. Rules that apply to other cameras may still be shown (depending on what other cameras in the tree are selected).

Initially the tree is collapsed; that is, only the System node is shown.

Click the + sign to the left of the system node to show the servers (which initially display collapsed).

Click the + sign to the left of any server to show the camera nodes for that server.

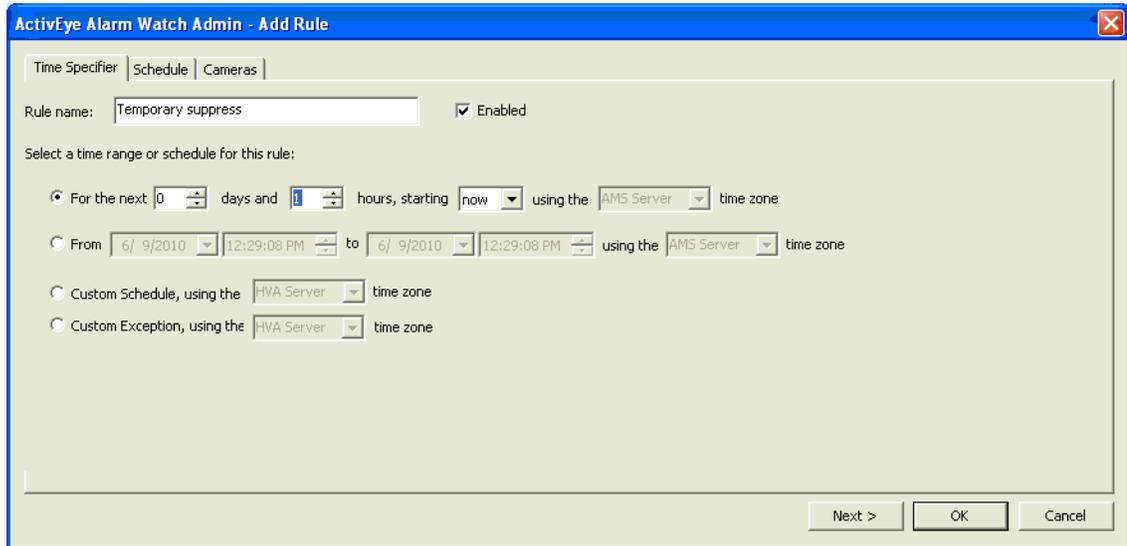
Click the - sign to the left of the system node to collapse the entire tree.

Click the - sign to the left of any server node to collapse that server.

Adding an Alarm Suspension Rule

1. Click **Add** on the **Alarm Suspension Rules** tab to start the Add/Edit Suspension Rule wizard.

Figure 13-13 Alarm Suspension Rule Wizard



LEGEND - Navigation Buttons

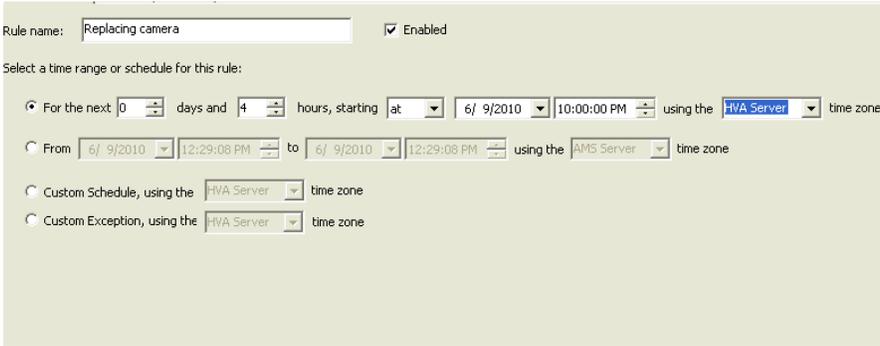
- Next >** = Moves to the next tab in the sequence *
 - < Back** = Moves to the previous tab in the sequence *
 - OK** = Sends changes to AMS
 - Cancel** = Exits the wizard without sending additions/changes to AMS
- * Based on what has been configured so far. Tabs that are not applicable are automatically skipped.
2. When you change tabs (by clicking on the tab or clicking **Next >** or **< Back**) or click **OK**, the application automatically checks the configured settings. If anything needs to be fixed, a message appears with the details.

Time Specifier Tab

Table 13-3 Time Specifier Tab Field Descriptions

Field / Option	Description
Rule name	Each rule must be given a unique name. It is recommended that you choose a name that reflects the purpose of the rule.
Enabled	By default new rules are automatically enabled. If unchecked, the rule is disabled and alarms will not be suspended by the Alarm Management Server.
Select a time range or schedule for this rule	In this area you can specify when the rule applies. Select one of the four time specifier options and complete the additional fields. Fields that do not apply to your selection are grayed out.

Table 13-3 Time Specifier Tab Field Descriptions

Field / Option	Description
For the next ...	Suspend alarms for a specific number of hours and/or days starting either now (default, as shown in <i>Figure 13-13</i>) or at a specific time in the future (see below).
	
	<p>The days range is 0 to 30. The hours range is 0 to 24. At least one of these must be set greater than 0. Change the values by entering a number or using the Up/Down arrows.</p> <p>The at drop-down list has two options that determine when the alarm suspension starts:</p> <p>now: The starting date and time is the current time (in the time zone of the AMS) at the time the rule is sent to the AMS. The time zone is that of the AMS Server and cannot be changed. The starting date and time fields are hidden.</p> <p>at: Select from the drop-down lists. For a new rule, these must be set to a future time. When editing an existing rule, the original starting time for the rule displays, including rules originally created using the now option.</p>
From ...	Suspend alarms for a specific period of time. Enter starting (From) and ending (to) times. The ending date/time must be in the future and must be later than the starting date/time.
Custom Schedule, using the ...	Suspend alarms during times indicated on a schedule. The schedule and (optional) holiday list are selected on the Schedule tab.
Custom Exception, using the ...	Suspend alarms during selected times for dates in a list of exception dates. The time(s) of day and list of dates are selected on the Schedule tab.

time zone All the time specifier lines end with using the X time zone. The time zone selection controls which time zone is used to evaluate alarms against the times specified. This is particularly useful when there are servers in different time zones. You can choose one of the following:

- **HVA Server:** Use the time zone of the HVA server the alarm came from. This is appropriate when alarm suspension is based on things happening at a site (for example, a regular cleaning schedule).

Example

One HVA server is in New York City (EST), another HVA server is in Denver, Colorado (MST, two hours behind NY), managed by an AMS in Los Angeles, California (PST, three hours behind NY). You have a schedule that suspends alarms for these two HVA servers from 6 pm to 8 pm in HVA Server time on weekdays. Alarms for the NY server will be suspended from 6 pm to 8 pm NY time (3 pm to 5 pm CA time). Alarms for the Denver server will be suspended from 6 pm to 8 pm Denver time (5 pm to 7 pm CA time).

- **AMS Server:** Use the time zone of the AMS. This is appropriate when you want to suspend alarms for the next hour (irrespective of the local time on each HVA server) or when you want to suspend alarms for something that is happening simultaneously in multiple locations (that is, at different local times for each time zone).

Example

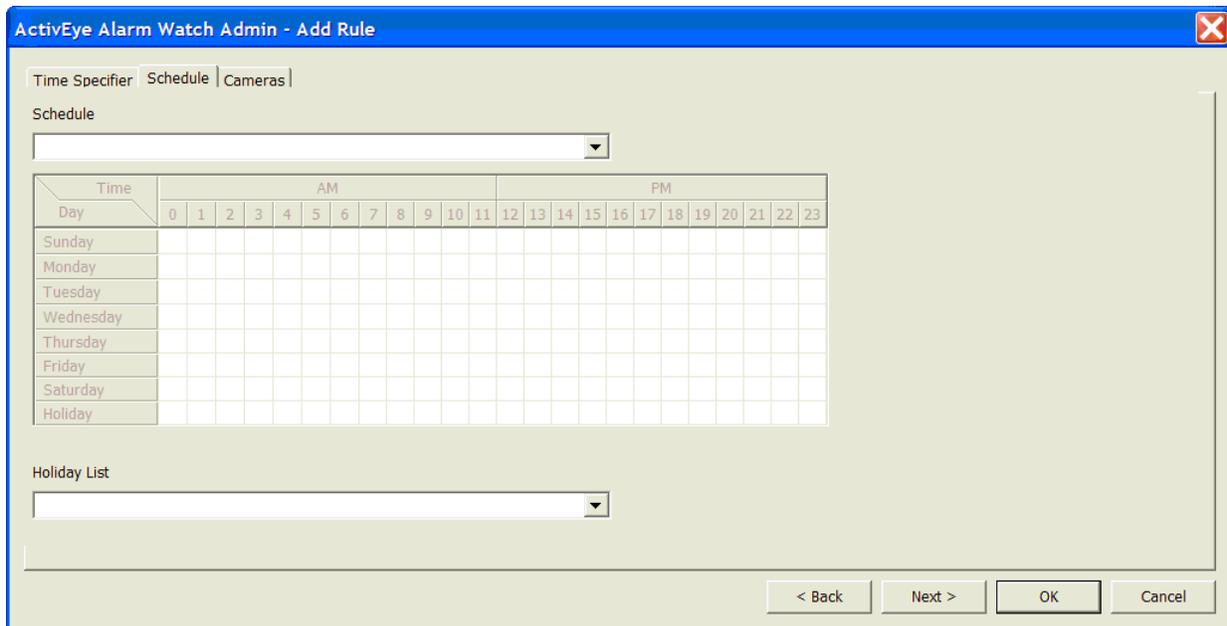
Take the same two HVA servers and AMS in the above example. Now suppose at 3 pm CA time you add a rule to suspend alarms from both servers for the next hour starting now. Alarms will be suspended from 3 pm to 4 pm CA time (for the Denver server, that is 4 pm to 5 pm Denver time and for the NY server, is 6 pm to 7 pm NY time).

- **GMT:** Use Greenwich Mean Time. This is an alternative to AMS Server time zone for suspending alarms for something that is happening simultaneously in multiple locations. You might use this when you run AWA from a different location/time zone than AMS and you are not sure what the AMS time zone is.

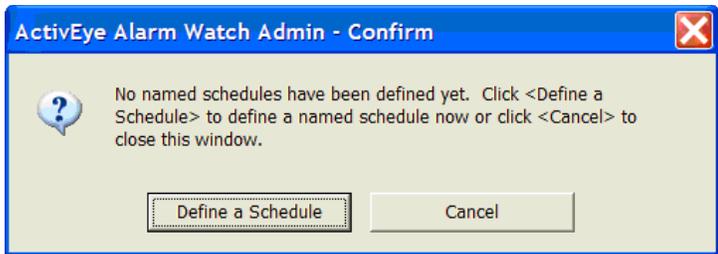
Setting a Custom Schedule

To set a custom schedule to suspend alarms during times indicated on a schedule:

1. Select **Custom Schedule** on the **Time Specifier** tab.
2. Complete the schedule details on the **Schedule** tab.

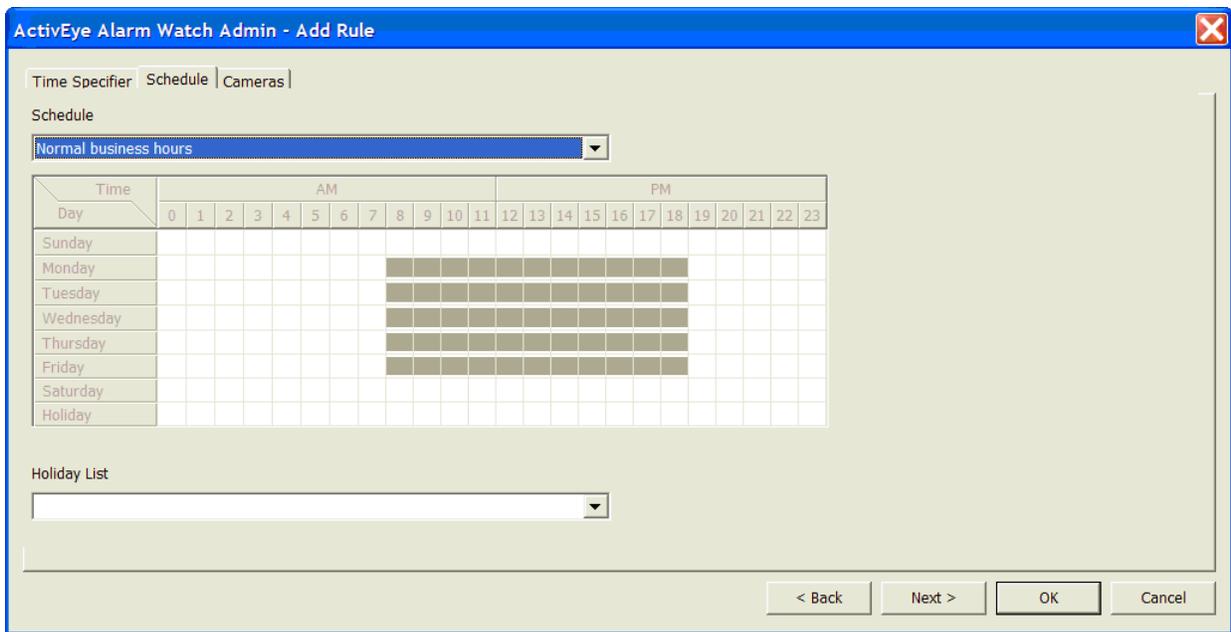


- In the **Schedule** drop-down list, select a schedule to use for the rule.
Schedules are maintained on the Schedules tab of AWA. If no schedules have been defined, clicking on the Schedule drop-down list displays the following message.



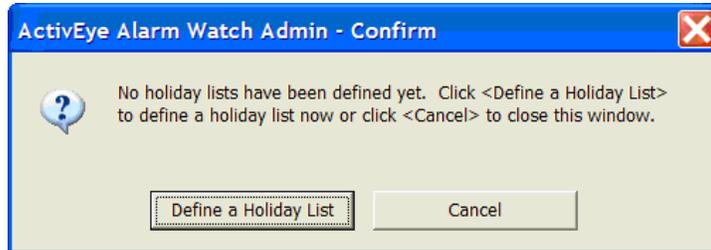
Click **Define a Schedule** to add a schedule (see [Adding a Schedule](#), page 210).

- After a schedule is selected, the day/time grid updates to show the times the schedule will suspend alarms. For example, in the example below alarms are suspended from 8:00:00 am to 6:59:59 pm Monday to Friday except for holidays.
The schedule grid in this screen is for display. To make any changes to the schedule times, see [Modifying a Schedule](#), page 212.



- In the **Holiday List** drop-down list, you can select a holiday list.
Schedules allow you to set alarm suspension times for each day of the week and also separate times for holidays. On holidays, the times in the Holiday row are used instead of the times for the applicable day of the week. In the above example, there will not be any alarm suspension on holidays, even if it is a week day.
To enable separate holiday times for the rule, you must select a holiday list. If you do not need separate holiday times, select **None**.

Holiday lists are maintained on the Holidays/Exceptions tab of AWA. If no holiday lists have been defined, clicking on the Holiday List drop-down list displays the following message.



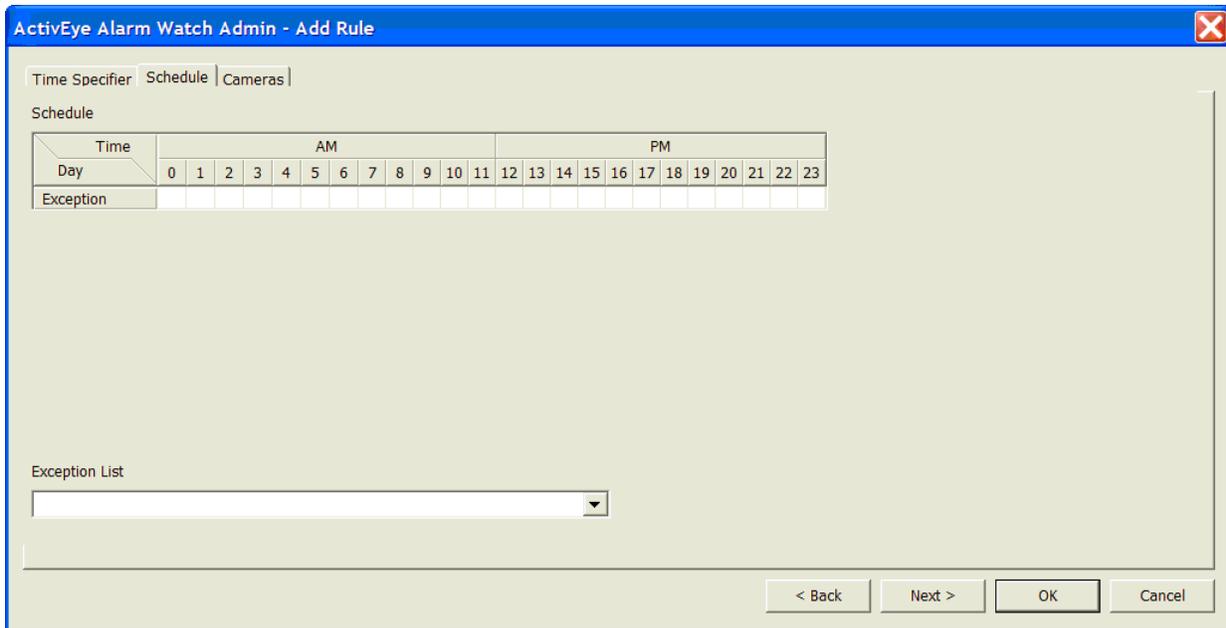
Click **Define a Holiday List** to display the Add Holiday/Exception List (see [Adding a Holiday or Exception List](#), page 207).

To select **None**, first click **Cancel**.

Setting a Custom Exception Schedule

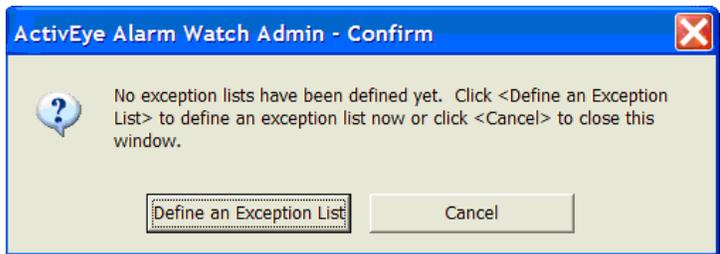
To set a custom exception schedule to suspend alarms during times on a list of exception dates:

1. Select **Custom Exception** on the **Time Specifier** tab.
2. Complete the schedule details on the **Schedule** tab.



3. Select or clear cells in the Time/Day grid, as needed to indicate the time(s) of day that you wish alarm suspension to be ON for dates in the Exception list. At least one block must be turned ON. Use the following options to set up the schedule:
 - **Cell-by-cell:** Click the cells of the schedule grid, as needed. Clicking the cells toggles a time between ON (dark) and OFF (light).
 - **A block of cells:** Drag the mouse pointer over multiple cells. When you release the mouse button, a menu appears showing the Fill Block and Clear Block commands. Click a command, as needed.
 - **Globally:** Right-click the mouse button to display a menu of commands for customizing more than one cell at once (Clear Row, Fill Row, and so on).
4. Select an exception date list from the **Exception List** drop-down list for which these alarms will be suspended.

Exception lists are maintained on the Holidays/Exceptions tab of AWA. If you click the Exception List drop-down list and no exception lists have been defined, the following dialog appears.



Click **Define an Exception List** to display the Add Holiday/Exception List dialog (see [Adding a Holiday or Exception List](#), page 207).

Cameras Tab

Use the Cameras tab to select the cameras to which the rule applies.



The camera/server tree works like the filter tree in [Filtering the Alarm Suspension Rules List](#) but with the following differences:

- Selecting (placing a check mark beside) a camera means the rule will apply to it.
- When adding a new rule, initially there are no cameras selected. At least one camera must be selected to be able to save the rule.
- Unreachable servers (displayed grayed out) cannot be selected to add them to a rule. However, when editing a rule, if a server previously selected for the rule is currently grayed out as unreachable, the check mark is retained unless you clear it (which would remove all of the cameras from that server from the rule).
- When there are one or more unreachable servers, attempting to select or deselect the System node, shows the following message.



In this case, you must individually deselect the (currently reachable) servers to remove them from the rule.

Note Unreachable servers may not be selected after they have been deselected.

Note Selecting an entire server only selects the cameras currently defined on that HVA server. If additional cameras are later added to that HVA server, they do not automatically become part of the rule. If you want the rule to apply to them you must manually add them to the rule after they are added to the HVA server.

Similarly, selecting the entire system only selects the HVA servers currently monitored by AMS (and only the cameras currently defined on those servers). If additional HVA servers are later added, they will not automatically become part of the rule. If you want the rule to apply to them you must manually add them to the rule after they are added to AMS.



Caution Do not change channel IDs of existing cameras in HVA server configurations when using alarm suspension. Since alarm suspension is based on channel ID, changing the IDs at the HVA servers can have unexpected alarm suspension results.

Submitting Changes to Server

When you are satisfied with all the rule settings, click **OK** to add the new rule to AMS. If there is a problem adding the rule to AMS, an error message appears and you are returned to the Add Rule wizard so that you may resolve the problem and submit the rule again.

If the rule is successfully added to AMS, you will be returned to the main rule list display where the newly added rule is selected. If the camera selection for the rule is such that the rule is not visible based on the current filter settings, the following message displays.



Clicking **Keep Hidden** will keep the current filter settings and the new rule will not appear (and will not be selected). Clicking **Show All Rules** causes the filter to have all servers/cameras checked and the views to refresh so that the newly created or edited rule will be shown and selected.

Modifying an Alarm Suspension Rule

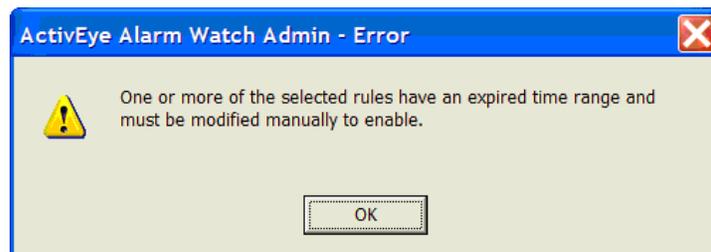
To modify an alarm suspension rule:

1. Click **Edit** or double click a rule on the Alarm Suspension Rules tab (see [Figure 13-12](#)) to start the Add/Edit Suspension Rule wizard.
The Edit button is enabled when only one rule is selected.
2. Follow the Edit Rule wizard, which works similarly to the Add Rule wizard (see [Adding an Alarm Suspension Rule](#), page 195).

Enabling or Disabling Alarm Suspension Rules

To enable/disable an alarm suspension rule, click **Enable/Disable** on the Alarm Suspension Rules tab (see [Figure 13-12](#)). This toggle button is enabled only when one rule is selected or when all the selected rules are in the same enabled or disabled state. Clicking Enable/Disable changes the state of the suspension rule without a prompt for confirmation.

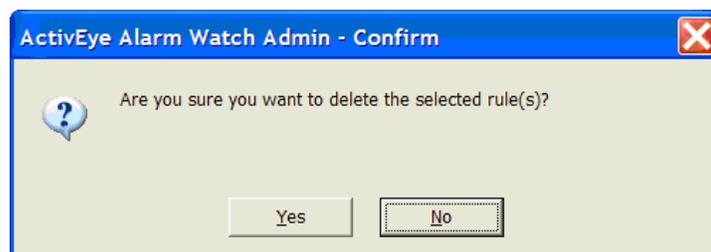
If the current time range of a rule has expired, clicking Enable does not enable the rule. Instead the following message displays. If multiple rules were selected and this error is displayed, none of the selected rules will be enabled.



Deleting an Alarm Suspension Rule

To delete an alarm suspension rule:

1. Click **Delete** on the Alarm Suspension Rules tab (see [Figure 13-12](#)) to remove one or more alarm suspension rules from the system.
This button is enabled when one or more rules are selected.
2. You are prompted to confirm that you want to delete the selected rule(s).

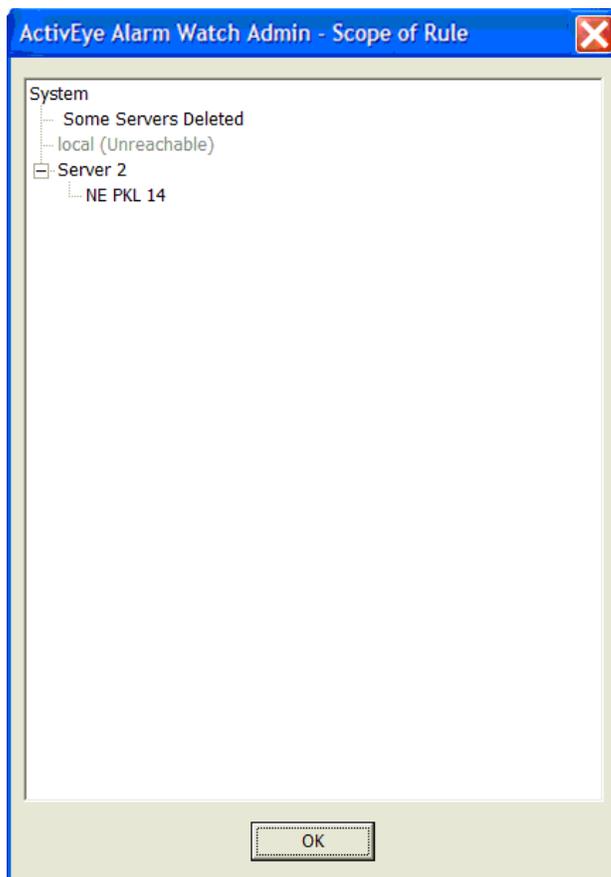


Clicking **No** means that none of the rules are deleted.

Clicking **Yes** means that AWA deletes the rules from AMS one at a time. In the unlikely event there is an error deleting any of the rules from AMS, an error message displays and the rules that were not deleted remain selected.

Viewing the Scope of an Alarm Suspension Rule

Click **View Scope** on the Alarm Suspension Rules tab (see *Figure 13-12*) to view the scope of a rule. This button is only enabled when one rule is selected. The tree view only shows nodes applicable to the selected rule.



Refreshing the Alarm Suspension Rule Display

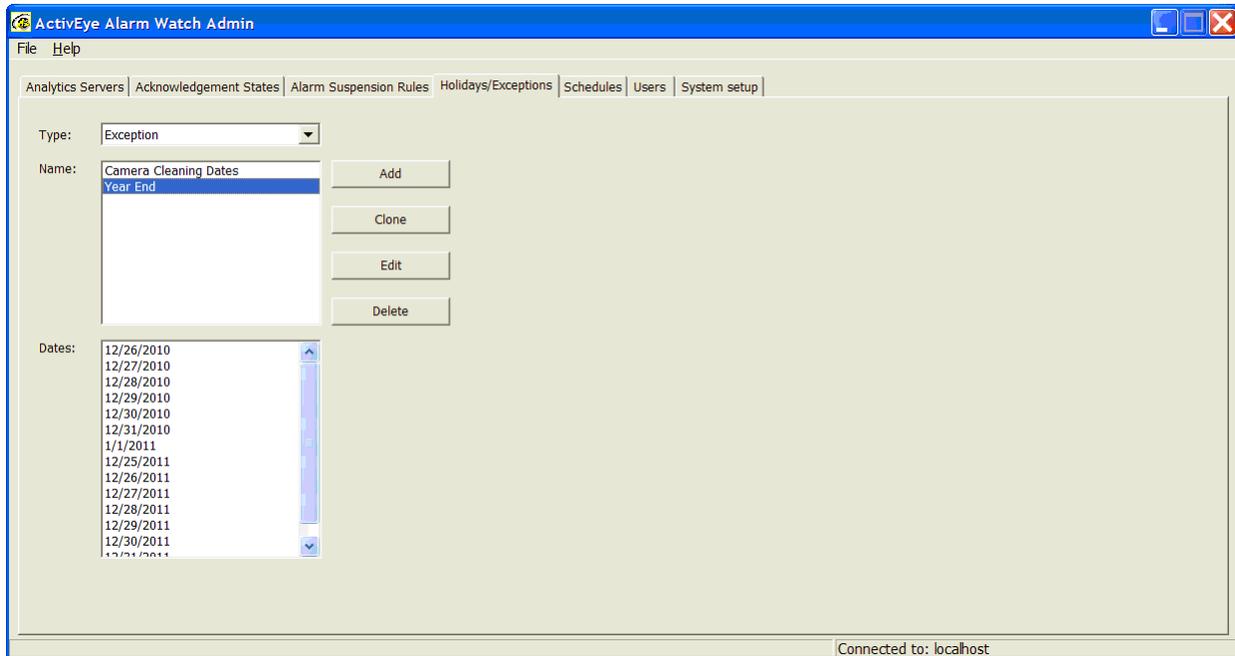
Click **Refresh** on the Alarm Suspension Rules tab (see *Figure 13-12*) to update the camera list display (in the filter tree) and the rule list with the most current information (including expiration status) from the AMS.

Managing the Holiday and Exception Date Lists

To view, add, edit, and delete named holiday and exception date lists:

1. Select the **Holidays/Exceptions** tab.

Figure 13-14 Holidays/Exceptions Tab



2. *Table 13-4* describes the fields on the Holidays/Exceptions tab.

Table 13-4 Holidays/Exceptions Tab Field Descriptions

Field	Description
Type	Controls what type of list is displayed or added.
Holiday	Shows holiday lists
Exception	Shows exception lists
Name	Displays the currently defined holiday or exception lists.
Dates	When you select one holiday/exception list in the Name list, the Dates area shows the list of dates in the selected holiday/exception list. If more than one name is selected in the name list, no dates are shown. The dates are sorted in ascending order starting from the oldest date. The dates in the list are not selectable; this is for information only.

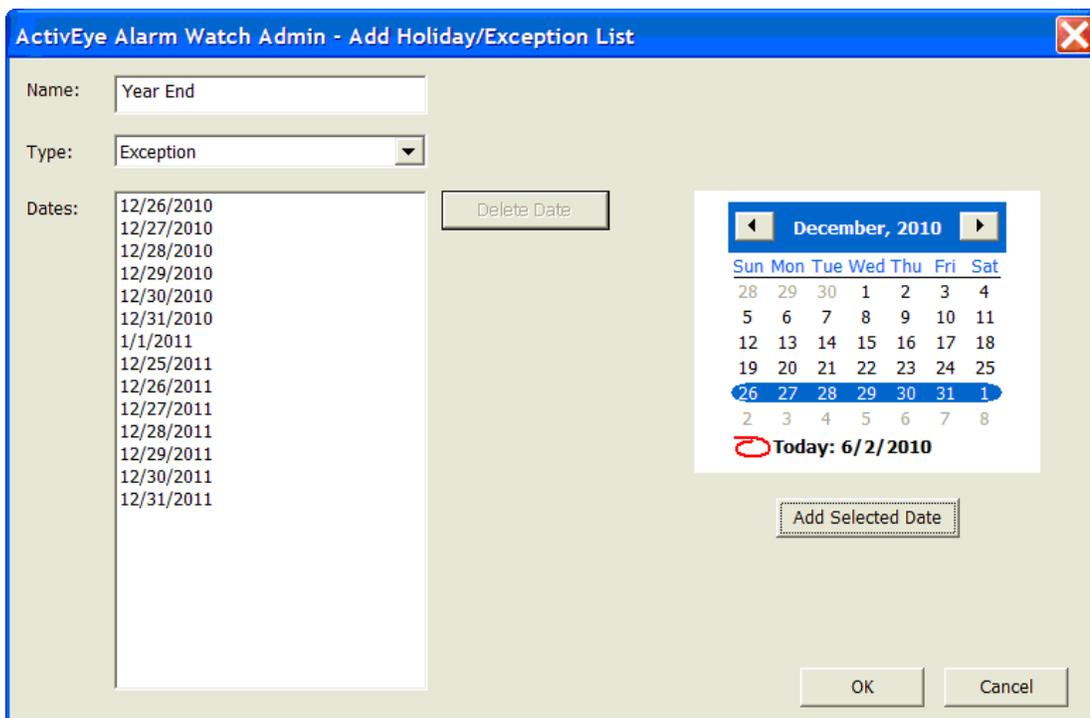
Adding a Holiday or Exception List

To add a holiday/exception list:

1. Click **Add** on the Holidays/Exceptions tab (see [Figure 13-14](#)) to define a new holiday or exception list starting from scratch.

Alternatively, you can select an existing list and then click **Clone** to make a new list starting from a copy of the existing list. The Clone functionality is only enabled when a single list is selected in the **Name** list.

The Add Holiday/Exception List dialog opens.



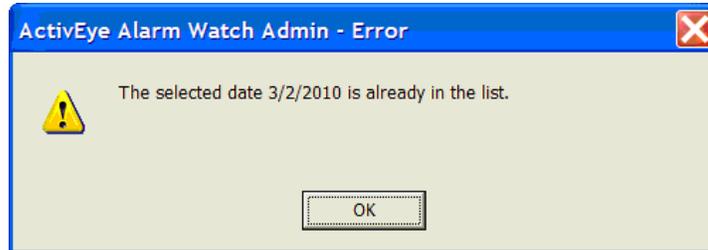
2. Follow [Table 13-5](#) to complete new holiday/exception list.

Table 13-5 Add Holiday/Exception List Field Descriptions

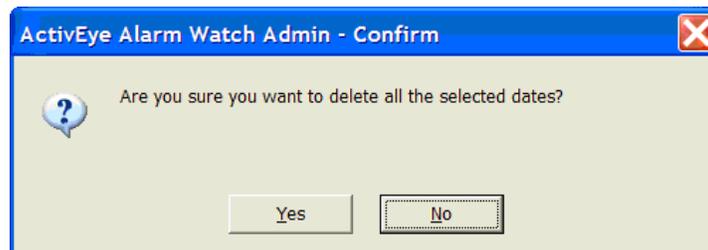
Fields	Description
Name	A user-defined name that uniquely reflects the purpose of the list.
Type	Select the type of list (holiday or exception). The default is the type that was selected to filter the Holidays/Exception tab. This is editable when adding/cloning a list. You cannot change the type of an existing list.
Dates	Shows the list of dates in the holiday/exception list, sorted in ascending order starting from the oldest date.

3. Use the calendar control to add dates to the list. To add a single date, click the date and then click **Add Selected Date**.

4. To add a consecutive range of dates (for example, two weeks) click the start date, shift click the end date (to highlight the range), and then click **Add Selected Date**. If you attempt to add one or more dates that are already in the list, the following error message advises that the dates will not be added.



Clicking **Delete** removes one or more dates from the system. The Delete button is enabled when one or more dates are selected. If more than one date is selected, you are prompted to confirm that you want to delete the selected dates.



If only one date is selected, it is deleted from the list without the above confirmation. If you delete a date by accident, click **Cancel** to abandon the list changes and start again.

5. When you are satisfied with the list settings, click **OK** to save the list changes and send them to AMS. If any of the dates added to the date list are before the date created, you are prompted to confirm that you want to add the dates to the rule and the past dates will be automatically selected.



If there is a failure adding the list to AMS, an error message appears, after which you will be returned to the Add Holiday/Exception List dialog so that you may resolve the problem and submit the list again.

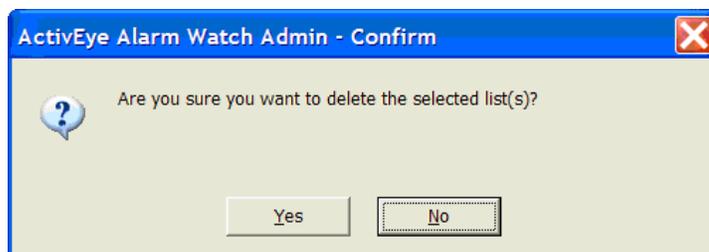
If the list is successfully added to AMS, you will be returned to the main holiday/exception list display and the newly added list will be selected.

Modifying a Holiday or Exception List

To modify a holiday/exception list, click **Edit** on the Holidays/Exceptions tab (see [Figure 13-14](#)). This button is enabled when only one list is selected. The functionality is the same as for adding a list.

Deleting Holiday or Exception Lists

Click **Delete** on the Holidays/Exceptions tab (see [Figure 13-14](#)) to remove one or more lists from the system. This button is enabled when one or more lists are selected. You are prompted to confirm this action.



Clicking **No** means that none of the lists are deleted.

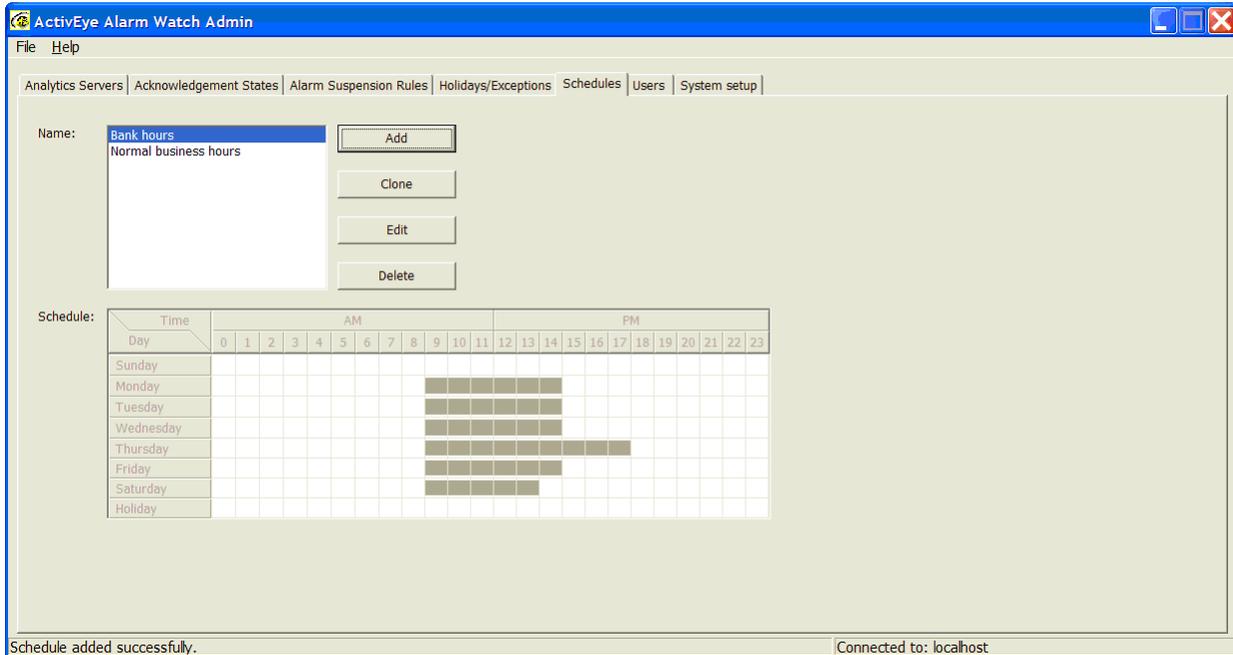
Clicking **Yes** means that AWA will delete the lists from AMS one at a time. If there is an error deleting any of the lists from AMS, then an error message displays and the lists that were not deleted remain selected.

Managing Schedules

To view, add, edit, and delete schedules:

1. Select the **Schedules** tab.

Figure 13-15 Schedules Tab



2. [Table 13-6](#) describes the areas on the Schedules tab.

Table 13-6 Schedules Tab Field Descriptions

Fields	Description
Name	This list shows the currently defined schedules.
Schedule	When a single schedule is selected in the Name list, the Schedule grid shows the schedule information. If more than one name is selected in the name list, no schedule information is shown. The schedule grid is not selectable; this information is status only.

Adding a Schedule

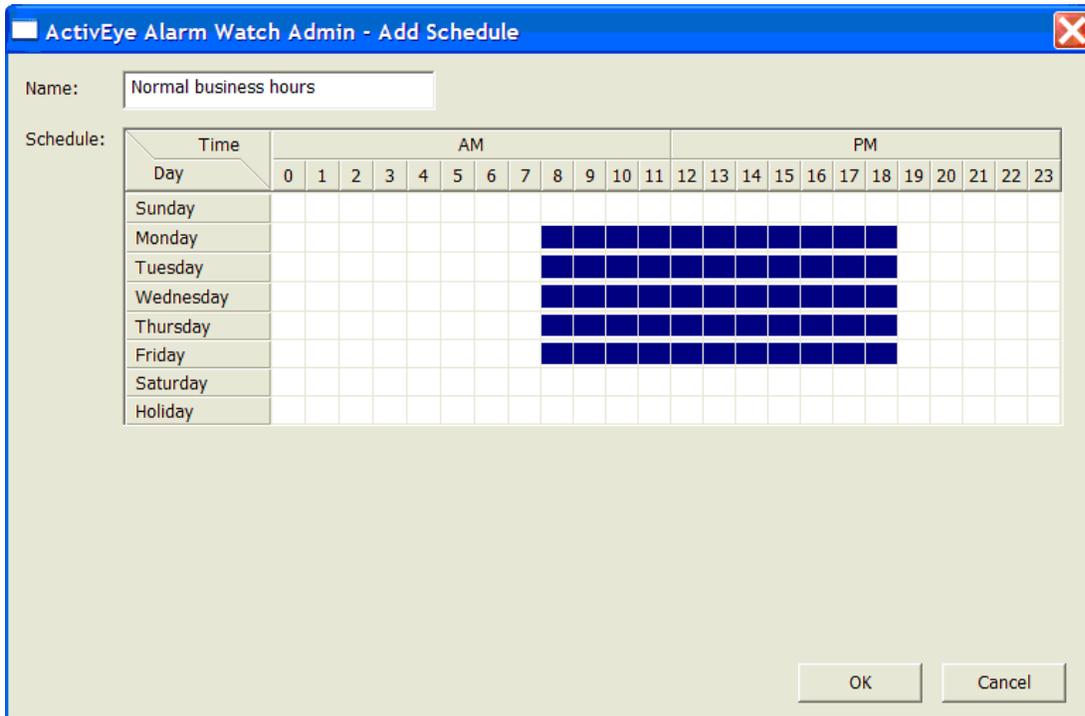
To add a schedule:

1. Click **Add** on the Schedules tab (see [Figure 13-15](#)) to define a new schedule starting from scratch.

OR

Select an existing schedule and then click **Clone** to make a new schedule starting from a copy of the existing schedule. The Clone functionality is enabled only when a single schedule is selected in the **Name** list.

The Add Schedule dialog opens.



2. Follow [Table 13-7](#) to complete the schedule.

Table 13-7 Add Schedule Field Descriptions

Fields	Description
Name	A user-defined name that uniquely reflects the purpose of the schedule.
Schedule	<p>Select (ON) or deselect (OFF) cells in the Time/Day grid, as needed to indicate the time(s) of day that alarm suspension will be ON.</p> <p>Each block in the grid represents a single hour for a single day of the week. If a block is ON (dark) for an hour, then alarms that come in during that hour of that day of the week are suspended. At least one block in the grid must be turned ON.</p>
Holiday	Use this row to provide different alarm suspension times for holidays. Holidays are determined by selecting a holiday list along with a schedule when defining a rule (see Setting a Custom Schedule , page 198). If an alarm arrives on a date that is in the holiday list associated with a rule, the Holiday row times are used in place of the day of the week times when deciding whether to suspend that alarm. In other words, the holiday schedule replaces the normal day-of-week schedule when a day falls on a holiday.

Use the following options to set up the schedule:

Cell-by-cell: Click the cells of the Basic schedule grid, as needed. Clicking a cell toggles a time between ON (dark) and OFF (light).

By a block of cells: Drag the mouse pointer over cells. When you release the mouse button, a menu appears showing the Fill Block and Clear Block commands. Click a command, as needed.

Globally: Right-click the mouse button to display a menu of commands for customizing more than one cell at once (Clear Row, Fill Row, and so on).

3. When you are satisfied the schedule settings are correct, click **OK** to save the schedule changes and send them to AMS.

In the unlikely event there is a problem adding the schedule to AMS, an error message appears, after which you are returned to the Add Schedule dialog so that you can attempt to resolve the problem and resubmit the schedule.

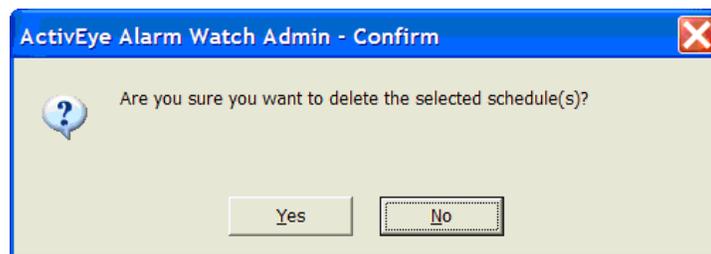
If the schedule is successfully added to AMS, you are returned to the main schedule display and the newly added schedule is selected.

Modifying a Schedule

To modify a schedule, click **Edit** on the Schedules tab (see [Figure 13-15](#)). The Edit button is enabled when only one schedule is selected. The same functionality is used for editing a schedule as for adding one.

Deleting Schedules

Click **Delete** to remove one or more schedules from the system. This button is enabled when one or more schedules are selected. You are prompted to confirm this action.



Clicking **No** means that none of the schedules will be deleted.

Clicking **Yes** means that the AWA deletes the schedules from AMS one at a time. If there is an error deleting any of the schedules from AMS, then an error message advises that the schedules were not deleted. Schedules that were not deleted remain selected.

Managing AMS User Accounts

In Alarm Watch Admin, the Administrator can manage user accounts used by the Alarm Management Server. Alarm Management Server user accounts are completely separate from those assigned to individual Video Analytics servers; that is, those created through the User Configuration application (see [Chapter 3](#)).

There are four types of permission that can be assigned to an AMS user:

Admin	Required permission for use of Alarm Watch Admin to configure an Alarm Management Server. Only Administrators with this permission can log on to Alarm Watch Admin to make configuration changes to the Alarm Management Server.
	Note The Admin permission does not assume any of the following permissions. For the Administrator user to log on to Alarm Watch Station, at least one of the following permissions is required.
View Live Alarms	Enables the user to view live alarms in Alarm Watch Station. The user may not make any alarm annotations if only granted this permission.
Modify Alarm State	Enables the user to acknowledge an alarm and modify the alarm state in Alarm Watch Station. Granting this permission automatically grants the View Live Alarms permission as a user must be able to view live alarms to modify their states.
Search	Enables the user to search alarms in the alarm database on the Alarm Management Server. With Video Analytics V4.7, full search functionality is not yet supported. Granting this permission automatically grants the View Live Alarms permission as a user must be able view live alarms to search for specific groups of alarms.

Adding a User

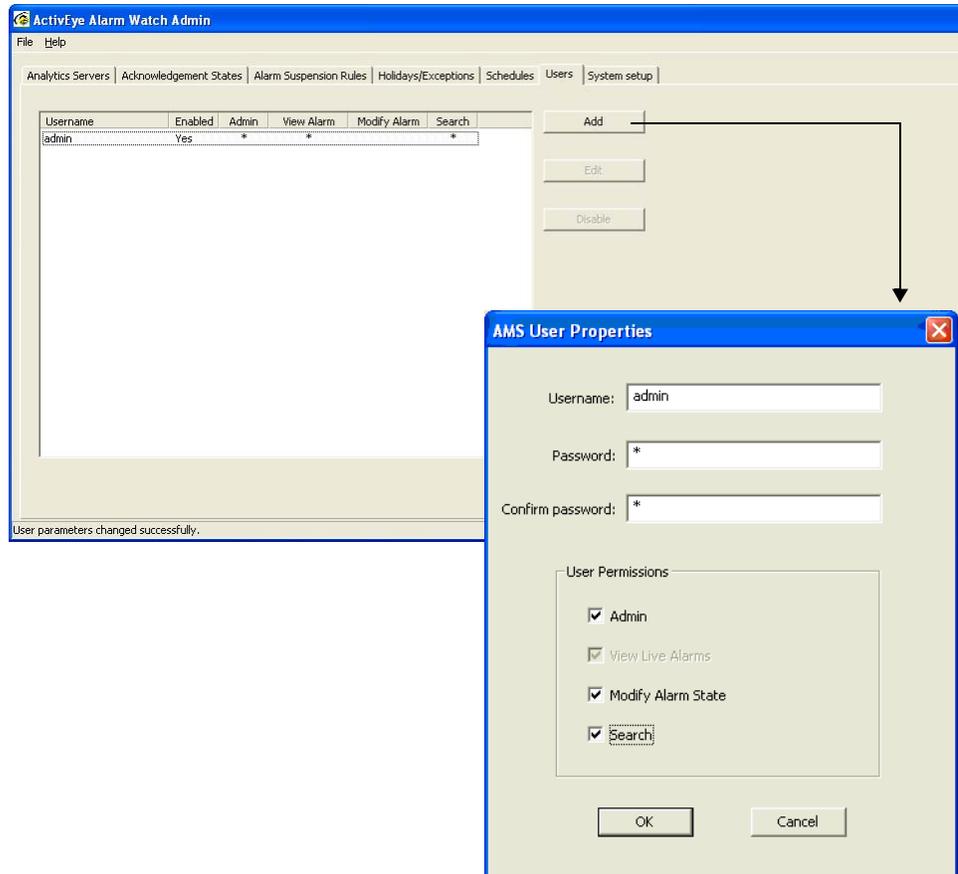
To add an AMS user account:

1. Select the **Users** tab.
2. Click **Add**. The AMS User Properties dialog appears (see [Figure 13-16](#)).
3. Enter the user name and password for the new user.
4. Assign the permission levels by selecting any combination of the four permission types.

Note Default permissions will be automatically set. See above.

5. Click **OK**.

Figure 13-16 Alarm Management Server Users Tab



If the new user's name duplicates an existing user name, the dialog below displays. Click **OK**, then correct the user name and resubmit the request.



Modifying User Properties

To modify user account information:

1. Select the user in the list, then click **Edit**,
OR
Double-click an item in the list.
2. In the AMS User Properties dialog, make the desired changes as required. You can change the password, the permission levels, or disable a user account.

3. Click **OK**.

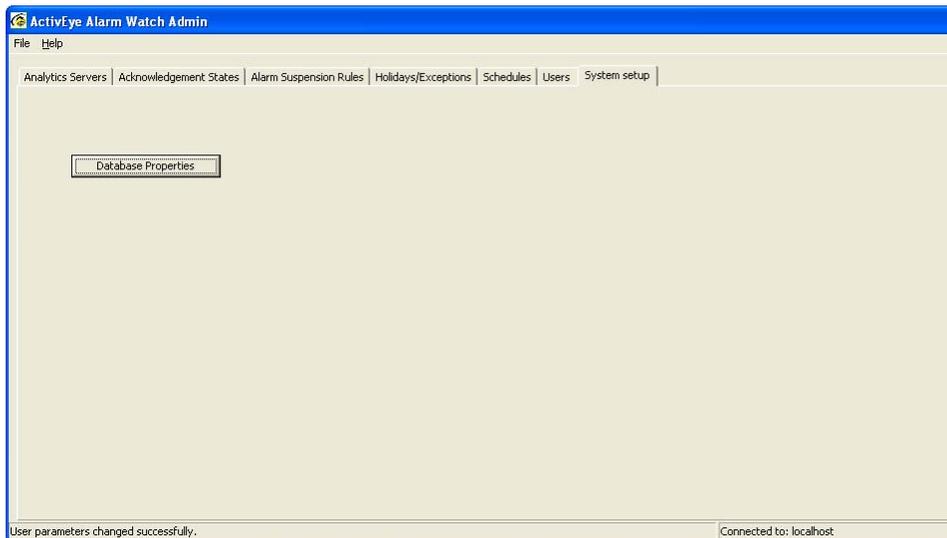
Note If a user account is disabled, but the user is already logged on to Alarm Watch Station, the change only takes effect the next time the user logs on.

Permission changes are effective immediately, whether or not the user is currently logged on.

AMS System Configuration

Currently, the only Alarm Management Server system setting that can be configured is the Alarm Management Server's database properties (see [Figure 13-1](#)).

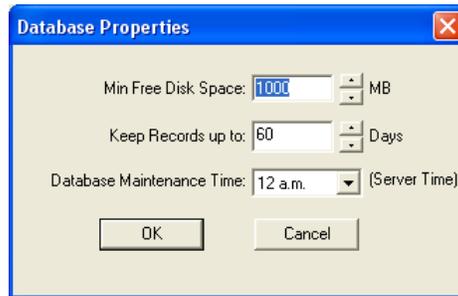
Figure 13-17 AMS System Setup Tab



To modify the AMA database properties:

1. Select the **System setup** tab.
2. Click **Database Properties**.

Figure 13-18 AMS Database Properties



3. Modify the following properties as required.

Minimum Free Disk Space	The default minimum free disk space is set to 1 GB. If the available disk space falls below this minimum amount, AMS automatically begins deleting records in the database, starting with the oldest records.
Keep Records up to	Number of days to keep the alarm records (default 60 days). If there is not enough disk space to store alarm data for the specified number of days, AMS deletes records in the database, starting with the oldest records.
Database Maintenance Time	Specify the time for the AMS database to run its daily maintenance task (default is 12 A.M.) Honeywell recommends that you specify a time when there is a minimum load on the AMS server; that is, when there are the fewest alarms received by the system.

4. Click **OK** for your changes to take effect or **Cancel** to cancel the changes. Changes do not take effect until the next database maintenance time.

Note To ensure continuous system operations, the system automatically monitors disk usage on the AMS and manages the size of the recording database.

Alarm Watch Station

Alarm Watch Station is the monitoring and management console for security operators to monitor and manage alarms generated by a large number of Analytics servers to which the Alarm Management Server is connected. Security operators at a central monitoring station can run Alarm Watch Stations from multiple workstations to connect to the same Alarm

Management Server to monitor all the cameras processed by the list of Analytics servers. Operators can easily share their monitoring responsibility and collaborate on alarm management tasks. The operator can perform any of the following tasks:

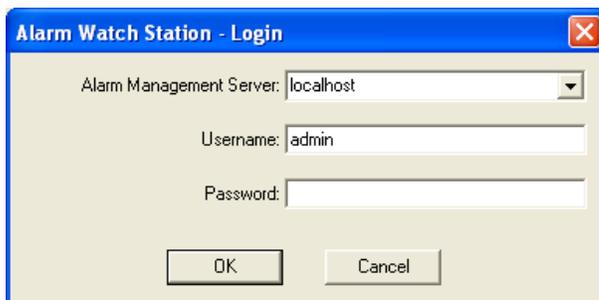
- View live Alarms as they occur
- View past alarms up to the selected default time period
- View a subset of alarms by use of alarm filter
- Classify alarms to any of the preset classifications
- Assign alarm acknowledge state to any selected alarms
- Enter detailed comment to any selected alarms
- View alarm acknowledgement trail
- Monitor the current connection status of the Alarm Management Server, and all the Analytics servers in the network
- Configure the preference settings of the Alarm Watch Station
- View alarm suspension rules
- View which cameras are currently suspended by alarm suspension rules

Logging On to Alarm Watch Station

To log on to Alarm Watch Station:

1. Launch Alarm Watch Station.
2. You are prompted to log on (see *Figure 13-19*).

Figure 13-19 Alarm Watch Station Login Dialog



3. To successfully connect to the Alarm Management Server, you must provide:
 - The host name and IP address of the AMS
 - A valid user name with the required permission levels
 - The correct password.

Failure to provide an invalid host name or IP address, or if the AMS is not reachable, results in an HTTP connection error.



An incorrect user name or password results in an authorization error message.



Note To successfully log on, the user must have one of the following permissions: View Alarm, Modify Alarm, or Search. If a permission error message displays, contact your Administrator to add or modify the necessary permission levels.

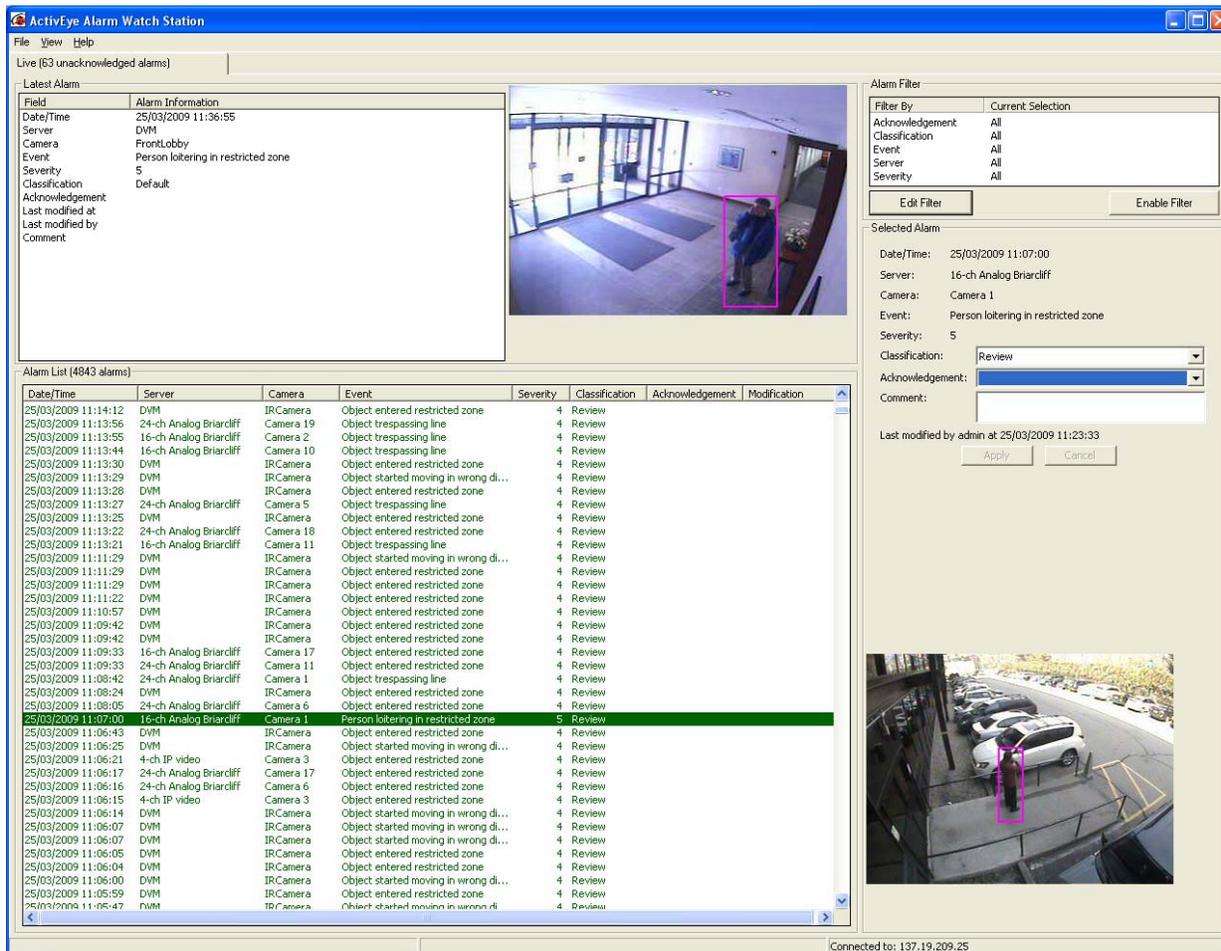
In the unlikely event your log on fails, or if you need to connect to another Alarm Watch Server, try logging on again using the **File ► Login...** command.



- When you have successfully connected to the Alarm Management Server, the main Alarm Watch Station window appears (see [Figure 13-20](#)). There is a single Live tab that contains the following six areas:

Live tab header	Displays the total number of unacknowledged alarms
Latest Alarm	Displays detailed information of the latest alarm
Alarm List	Lists all alarms from the user-configured duration (see The Alarm List , page 225). A maximum of 5,000 alarms can be displayed in the list. This can be an unfiltered (default) or a filtered view, depending on whether the alarm filter is currently enabled (see Defining Alarm Filters , page 231).
Alarm Filter	Displays the current filter criteria and allows the user to edit the filter and enable/disable the filter
Selected Alarm	Displays detailed information of the currently selected alarm(s) from the Alarm List. In this area the user can acknowledge the selected alarm(s) by assigning the alarm classification, acknowledgement state, or add detailed comments.
Status Bar	Displays the current connection status to the Alarm Management server.

Figure 13-20 Alarm Watch Station Live Tab



Alarm Watch Station Menu Bar

The Alarm Watch Station menu bar consists of the following menu options:

File	Log on to the Alarm Management server or exit the application
View	
Configuration...	Configure preference settings of the current Alarm Watch Station (see Configuring the Alarm Watch Station , page 220)
Show Status	View the current connection status to the Alarm Management server and all Video Analytics servers in the server list (see Viewing and Modifying Alarm Status , page 226)
Alarm Suspension Rules	View alarm suspension rules and current suspension state of cameras (see Alarm Watch Station — Alarm Suspension Rules , page 222).
Help	View information about the current version of Alarm Watch.

Figure 13-21 Alarm Watch Station View Menu Options



Configuring the Alarm Watch Station

To set your preferences for the Alarm Watch Station:

1. Select **View ► Configuration....**
2. The Alarm Watch Station Configuration dialog appears. Use [Table 13-8](#) as a guide to set how you want Alarm Watch Station to handle alarms.

Figure 13-22 Alarm Watch Station Configuration



Table 13-8 Alarm Watch Station Configuration Field Descriptions

Enable Audio Alarm	Select this check box to enable audio alarms to be played when live alarms are received. Clear to disable audio alarms and mute the Alarm Watch Station.
Hide Dismissed Alarms	Select this check box to hide all alarms that are classified as Dismissed from being displayed in the Alarm List. Clear to display dismissed alarms. Note This setting affects the default setting of the Alarm Filter. When this box is selected, the filter setting changes to include alarms of all classifications except Dismissed. When this box is cleared, the filter setting changes to include alarms of all classification, including Dismissed since they are no longer to be hidden. When you modify this box, a message prompts you to check your alarm filter setting as it would have been modified by the software to the default setting that matches the selection you have made here (see Figure 13-23).
Exempt Filter Rule for Latest Alarm	Select this check box to allow the latest alarm to always be displayed, regardless of the alarm filter settings, when the filter is enabled. Clear to apply the same filter rule to the latest alarm when the filter is enabled.
Maximum number of alarms	Sets the maximum number of past alarms to be displayed in the Alarm List (up to 5,000, the default setting). As new live alarms arrive, when the total number of displayed alarms exceeds the maximum number specified, the older alarms are purged from the list, starting from the oldest alarm. Note The 5,000 limit includes all alarms that have been dismissed, regardless of whether they are hidden or not.
Show Alarms for	Sets the default time period for the past alarms to be displayed in the Alarm List. Options are: Today only. Only the current day's alarms are displayed. The last number of day starting at a given time. Alarms since the specified time from the last specified number of days are displayed. For example, a setting of The last 1 day(s), starting 12:00:00 AM means that all alarms since 12 midnight yesterday are displayed. A setting of The last 1 day(s) starting 6:00:00 PM means that all alarms since 6 PM yesterday are displayed.
The last number of hours	Alarms since the last number of specified hours are displayed.

- Click **OK**. These settings apply to the Alarm Watch Station application running on the current client PC, regardless of which user logs on.

Figure 13-23 Dismissed Alarms Prompt

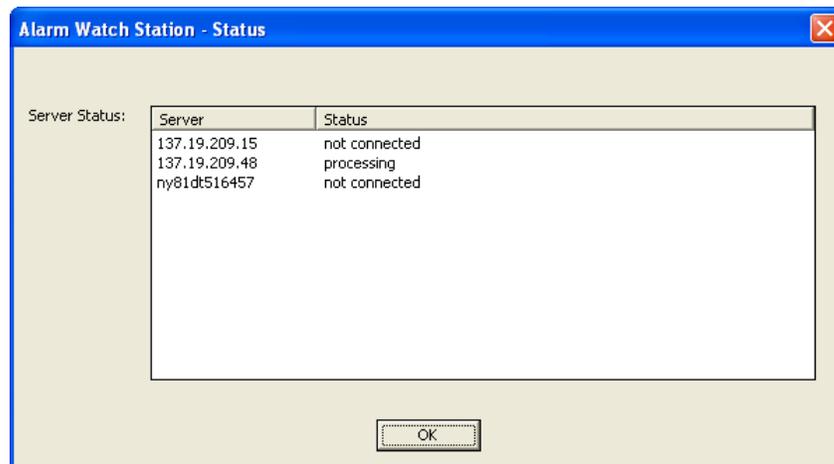


Alarm Watch Station Status

To view the connection status of all Video Analytics servers that are included in the server list for Alarm Management Server to connect to:

1. Select **View ► Show Status**.
2. The Alarm Watch Station - Status window appears. The normal status is **processing**; this indicates that Analytics server is currently processing live videos to detect analytics events.

Figure 13-24 Alarm Watch Station Status



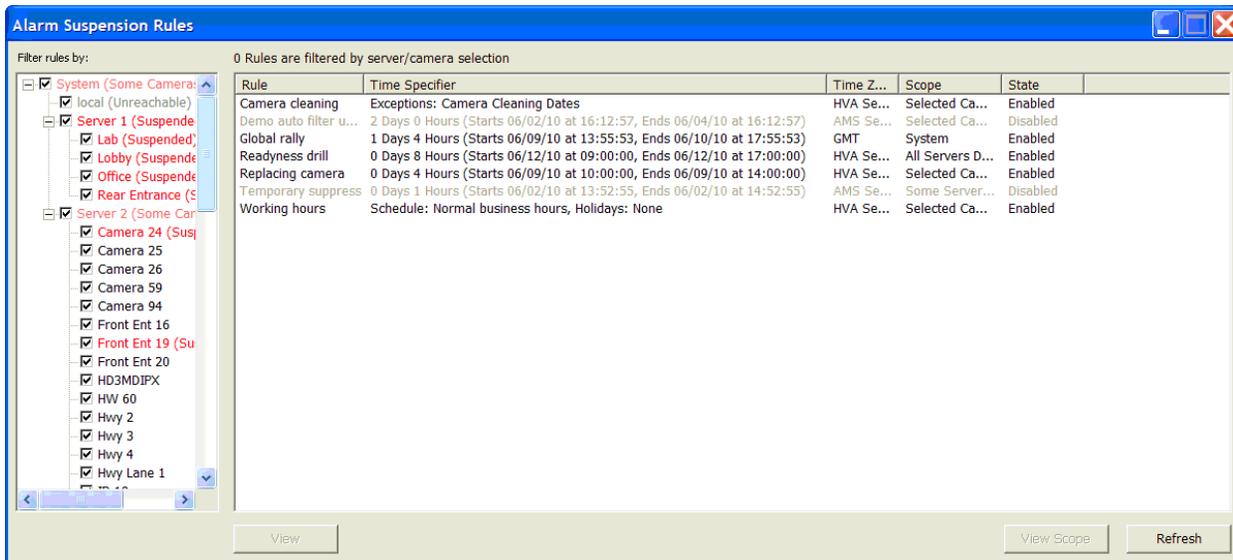
3. Click **OK** to return to the Alarm Watch Station Live tab.

Alarm Watch Station — Alarm Suspension Rules

To view the alarm suspension rules in Alarm Watch Station:

1. Select **View ► Alarm Suspension Rules**.
2. The Alarm Watch Station - Alarm Suspension Rules window displays.

Figure 13-25 Alarm Suspension Rules



This window is similar to the Alarm Suspension Rules tab in Alarm Watch Admin (see [Managing Alarm Suspension Rules](#), page 192). However it does not allow rules to be changed.

In addition to the AWA functionality, the filter tree on the left pane shows which cameras are currently having their alarms suspended. Servers/Cameras that are currently suspending alarms are highlighted in red and have the word (Suspended) added to the name. Servers that have some but not all cameras suspending alarms show in a lighter shade of red and have the text (Some Cameras Suspended) appended to the server name.

Click **Refresh** to refresh the screen, including the alarm suspension state in the filter tree.

Click **View** when a single rule is selected to view the settings for that rule in the Rule Suspension wizard (see [Adding an Alarm Suspension Rule](#), page 195). All settings in the wizard are disabled (grayed out) since alarm suspension rules cannot be changed from AWS.

Receiving the Latest Alarm

As a new live alarm arrives from any of the Analytics servers, it displays in the Latest Alarm area. If audio alarm is enabled, the audio alarm plays back when the live alarm arrives (see [Figure 13-26](#)). [Table 13-9](#) describes the information that is displayed or updated for the latest live alarm that has been received.

Figure 13-26 Latest Alarm

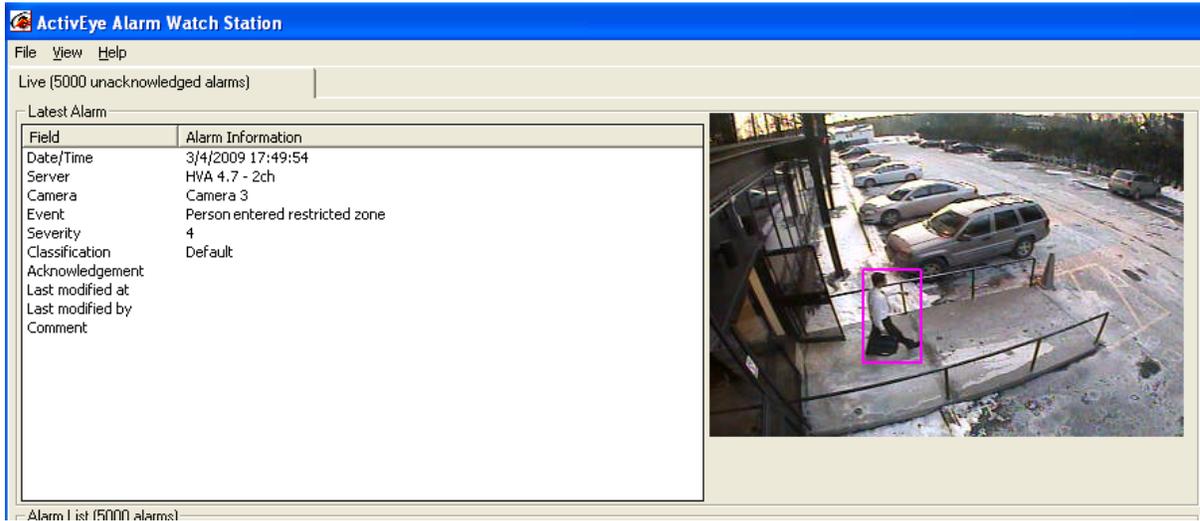


Table 13-9 Alarm Watch Station Latest Alarm Field Descriptions

Date/Tim	Timestamp of the alarm; that is, the actual timestamp of the alarm as detected on the Analytics server, converted to the local time on the client PC. If there is a time difference between the two, the timestamp may appear to be lagging or ahead of the current client PC clock.
Server	Displays the name of the Analytics server where the alarm was generated. This name is configured in Alarm Watch Admin (see Alarm Watch Admin , page 182).
Camera	Camera name on the Analytics server where the alarm was detected.
Event	Event type of the alarm.
Severity	Severity level of the alarm.
Classification	When the newest live alarm arrives, this field displays as Default . When the user acknowledges the alarm by changing its classification, this field updates to show the current classification.
Acknowledgment	Alarm acknowledgement state. When the newest live alarm first arrives, this field is blank. After the user acknowledges the alarm by assigning an alarm acknowledgement state to it, this field updates to show the current acknowledgement state.
Last modified at	When the newest live alarm first arrives, this field is blank. After the user acknowledges the alarm, this field displays the timestamp of the acknowledgement.

Table 13-9 Alarm Watch Station Latest Alarm Field Descriptions

Last modified by	When the newest live alarm first arrives, this field is blank. When the user acknowledges the alarm, the user name of that person displays.
Comment	Detailed comment of the alarm. This field is blank when the newest live alarm first arrives.
Key frame	On the right side of the textual description of the newest live alarm, the alarm key frame displays.

Note Only the latest live alarm that arrives in real time is displayed in this area. Past alarms that fall inside the user-specified time period to be displayed populate in the Alarm List when Alarm Watch Station is launched. They are not considered to be live alarms.

The Alarm List

The Alarm List displays all the alarms that meet the currently configured time duration up to the maximum number of alarms as configured in the Configuration dialog (see [Defining Alarm Filters](#), page 231). When the alarm filter is enabled, the Alarm List displays a subset of the alarms that match the current filter criteria.

You can sort alarms currently displayed in the list by clicking on individual column headings (see [Figure 13-27](#)). By default, alarms are sorted by Date/Time and listed in reverse chronological order according to the alarm timestamp in local time.

Note If the Video Analytics servers and the Alarm Management server are not fully time synchronized, a live alarm originated from a Video Analytics server with a lagging time may not appear as the top item in the list. It is important to ensure that all Video Analytics servers, Alarm Management Server, as well as the client PCs, all have synchronized clocks.

The total number of alarms in the list displays in the header of this area.

Figure 13-27 Alarm List

Alarm List (5000 alarms)

Date/Time	Server	Camera	Event	Severity	Classification	Acknowledgement	Modification
3/4/2009 17:38:28	HVA 4.7 - 2ch	Camera 2	Object entered restricted zone	4	Default		
3/4/2009 17:38:24	HVA 4.7 - 2ch	Camera 2	Object entered restricted zone	4	Default		
3/4/2009 17:37:36	HVA 4.7 - 2ch	Camera 2	Object entered restricted zone	4	Default		
3/4/2009 17:37:30	HVA 4.7 - 2ch	Camera 2	Object entered restricted zone	4	Default		
3/4/2009 17:37:07	HVA 4.7 - 2ch	Camera 2	Object entered restricted zone	4	Default		
3/4/2009 17:37:04	HVA 4.7 - 2ch	Camera 2	Object entered restricted zone	4	Default		
3/4/2009 17:36:47	HVA 4.7 - 2ch	Camera 2	Object entered restricted zone	4	Default		
3/4/2009 17:36:47	HVA 4.7 - 2ch	Camera 2	Object entered restricted zone	4	Default		
3/4/2009 17:36:47	HVA 4.7 - 2ch	Camera 3	Object entered restricted zone	4	Default		
3/4/2009 17:36:39	HVA 4.7 - 2ch	Camera 2	Object entered restricted zone	4	Default		
3/4/2009 17:36:08	DVM - 2ch	IRCamera	Object entered restricted zone	4	Default		
3/4/2009 17:34:59	HVA 4.7 - 2ch	Camera 3	Object entered restricted zone	4	Default		
3/4/2009 17:34:34	HVA 4.7 - 2ch	Camera 2	Object entered restricted zone	4	Default		
3/4/2009 17:32:54	HVA 4.7 - 2ch	Camera 2	Object entered restricted zone	4	Default		
3/4/2009 17:32:16	DVM - 2ch	IRCamera	Object started moving in wrong di...	4	Default		
3/4/2009 17:31:52	HVA 4.7 - 2ch	Camera 2	Object entered restricted zone	4	Default		
3/4/2009 17:31:12	HVA 4.7 - 2ch	Camera 2	Object entered restricted zone	4	Default		
3/4/2009 17:30:41	HVA 4.7 - 2ch	Camera 2	Object entered restricted zone	4	Default		
3/4/2009 17:30:41	HVA 4.7 - 2ch	Camera 2	Object entered restricted zone	4	Default		
3/4/2009 17:30:32	DVM - 2ch	IRCamera	Object started moving in wrong di...	4	Default		
3/4/2009 17:30:29	DVM - 2ch	IRCamera	Object started moving in wrong di...	4	Default		
3/4/2009 17:30:29	DVM - 2ch	IRCamera	Object entered restricted zone	4	Default		
3/4/2009 17:30:24	DVM - 2ch	IRCamera	Object entered restricted zone	4	Default		
3/4/2009 17:30:24	DVM - 2ch	IRCamera	Object entered restricted zone	4	Default		
3/4/2009 17:30:24	DVM - 2ch	IRCamera	Object entered restricted zone	4	Default		
3/4/2009 17:30:14	DVM - 2ch	IRCamera	Object started moving in wrong di...	4	Default		
3/4/2009 17:30:06	DVM - 2ch	IRCamera	Object entered restricted zone	4	Default		
3/4/2009 17:30:01	DVM - 2ch	IRCamera	Object entered restricted zone	4	Default		
3/4/2009 17:30:00	DVM - 2ch	IRCamera	Object started moving in wrong di...	4	Default		
3/4/2009 17:29:53	DVM - 2ch	IRCamera	Object entered restricted zone	4	Default		
3/4/2009 17:29:45	HVA 4.7 - 2ch	Camera 3	Object entered restricted zone	4	Default		
3/4/2009 17:29:24	HVA 4.7 - 2ch	Camera 2	Object entered restricted zone	4	Default		
3/4/2009 17:28:41	HVA 4.7 - 2ch	Camera 2	Object entered restricted zone	4	Default		
3/4/2009 17:28:39	HVA 4.7 - 2ch	Camera 2	Object entered restricted zone	4	Default		
3/4/2009 17:28:38	HVA 4.7 - 2ch	Camera 3	Object entered restricted zone	4	Default		
3/4/2009 17:28:25	DVM - 2ch	IRCamera	Object started moving in wrong di...	4	Default		
3/4/2009 17:28:23	DVM - 2ch	IRCamera	Object entered restricted zone	4	Default		

Viewing and Modifying Alarm Status

To view or modify the alarm status in the Alarm List:

1. Select a single alarm from the list, then click it.

To select multiple alarms in a contiguous group, click the first one in the group, press Shift and click on the last one in the group.

To select multiple alarms that are not in a contiguous group, press Ctrl while you click on the individual alarms.

2. The detailed information along with the alarm key frame for the selected alarm or alarms displays in the Selected Alarm area (see [Figure 13-28](#)). If multiple alarms are selected and detailed information for all of them cannot be displayed, you see (multiple selections) on those affected fields.

Figure 13-28 Selected Alarm

Selected Alarm

Date/Time: 3/4/2009 17:39:14
Server: DVM - 2ch
Camera: IRCamera
Event: Person entered restricted zone
Severity: 4
Classification: Default
Acknowledgement:
Comment:

Apply Cancel



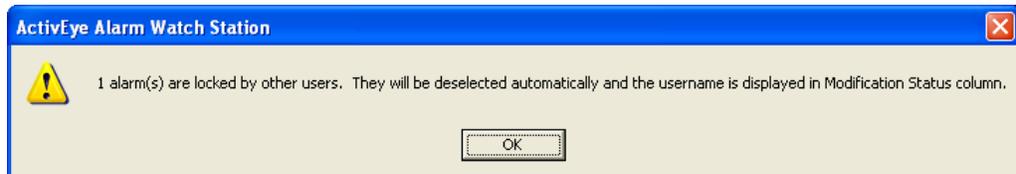
Acknowledging an Alarm

After you select alarm(s), you can:

- Acknowledge the selected alarm(s) by modifying the Classification and/or Acknowledgement State.
- For a single alarm, you can also enter the detailed comment for the selected alarm. You must have the Modify Alarm permission to modify the alarm state and acknowledge the alarm (see [Managing AMS User Accounts](#), page 213). If you do not have the required permission, an error message displays when you attempt to modify the alarm.



When you start modifying the alarm or multiple alarms that you have selected, a lock is placed on the selected alarm(s) to prevent other users from modifying the same alarm(s). The lock remains in effect until you click **Apply** to submit your changes. Other users who attempt to modify the same alarm will be notified of the lock placed by you (see below). Similarly, if some of the alarm(s) you have selected are currently locked by another user, you will receive the same notification. Those alarms that are currently locked by another user will be deselected from your selection. In addition, the user name of the user that is currently locking these alarms displays in the Modification column in the Alarm List.



To prevent a user from locking selected alarm(s) for extended period of time due to inactivity, if the lock has been in effect and there has been inactivity for more than one minute and the user has not clicked Apply to submit the changes, the user is prompted to continue editing the alarm(s), which renews the lock (see below). If the user fails to respond in a timely manner, the lock is automatically released and the changes that have not been submitted are discarded.



Assigning an Alarm Classification

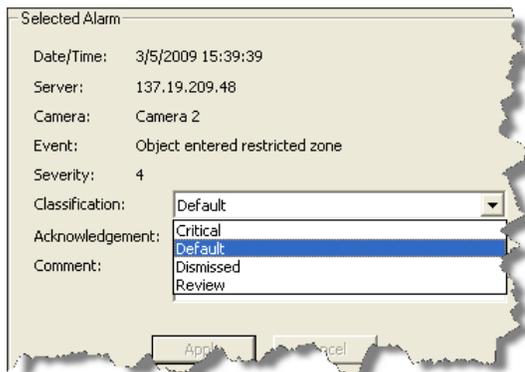
To assign an alarm classification:

1. Select an alarm (or multiple alarms) in the Alarm List. The Selected Alarm dialog appears (see [Figure 13-28](#)).
2. In the Classification drop-down list, select one of the following options:

Default	All new alarms are classified as Default as they arrive.
Dismissed	Depending on the configuration setting, alarms that are classified as Dismissed may be hidden from the Alarm List (default setting). To display dismissed alarms, change the configuration to deselect Hide Dismissed Alarms (see Configuring the Alarm Watch Station , page 220). Dismissed alarms have the lowest priority.
Review	These alarms have a priority above Dismissed and below Critical. This classification type may be used to indicate that these alarms require further review.
Critical	These alarms have the highest priority and are displayed in red in the Alarm List.

3. Click **Apply** to submit your changes or **Cancel** to discard your changes.
 After an alarm is acknowledged, it is displayed in **green** in the Alarm List. The user who acknowledged the alarm and the acknowledgement timestamp also display in the Selected Alarm area, under the Comment field.

Figure 13-29 Alarm Classification



Modifying an Alarm Acknowledgement State

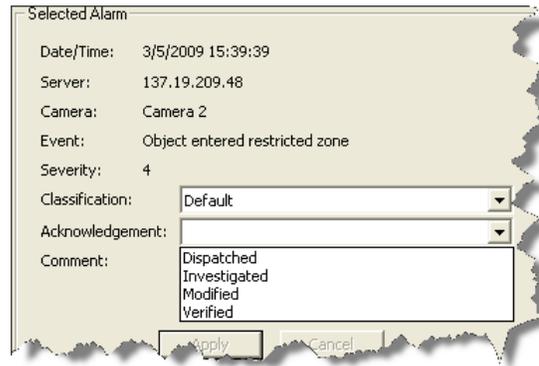
When an Administrator user defines Alarm acknowledgement states using the Alarm Watch Admin client application, the enabled alarm acknowledgement states become available to assign to a single or multiple selected alarm(s) (see [Figure 13-30](#)).

1. Select the acknowledgement state you want to assign to the alarm(s) you have selected.

2. Click **Apply** to submit your changes or **Cancel** to discard the changes.

After the alarm is acknowledged, it displays in **green** in the Alarm List. The user who acknowledged the alarm and the acknowledgement timestamp also display in the Selected Alarm area, under the Comment field.

Figure 13-30 Alarm Acknowledgement State



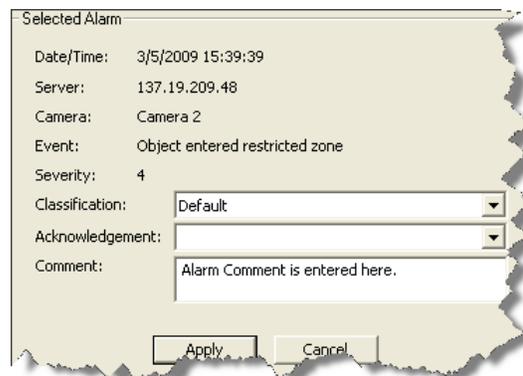
Adding an Alarm Comment

To add a comment to a single selected alarm:

1. Double-click the alarm in the Alarm List. The Selected Alarm dialog displays (see [Figure 13-31](#)).
2. Type in a detailed comment (maximum 250 characters). If the comment is non-ASCII or multibyte, the character limit is less than 250.
3. Click **Apply** to submit the comment or **Cancel** to discard the comment.

After the alarm is acknowledged, it displays in **green** in the Alarm List. The user who acknowledged the alarm and the acknowledgement timestamp also display in the Selected Alarm area, under the Comment field.

Figure 13-31 Alarm Comment

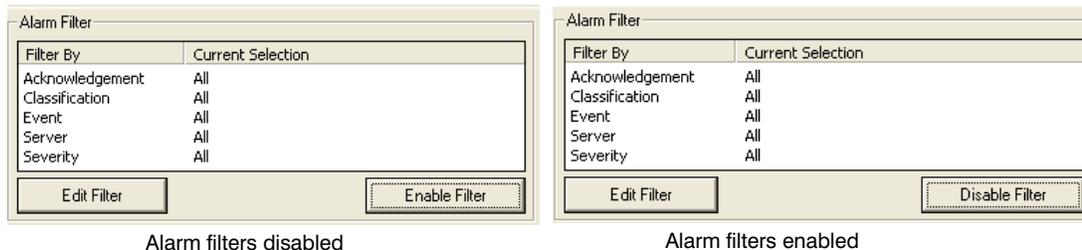


Defining Alarm Filters

To view a subset of the alarms in the Alarm List, create a filter criteria based on the following alarm fields:

- Acknowledgement state
- Classification
- Event type
- Server name
- Severity

Figure 13-32 Alarm Filter



To define an alarm filter:

1. Click **Edit Filter**. The Add Filter Criteria dialog appears.
2. Select the field to filter in the **Filter By** drop-down list (see [Figure 13-33](#)). By default, all acknowledgement states are included in the filter.

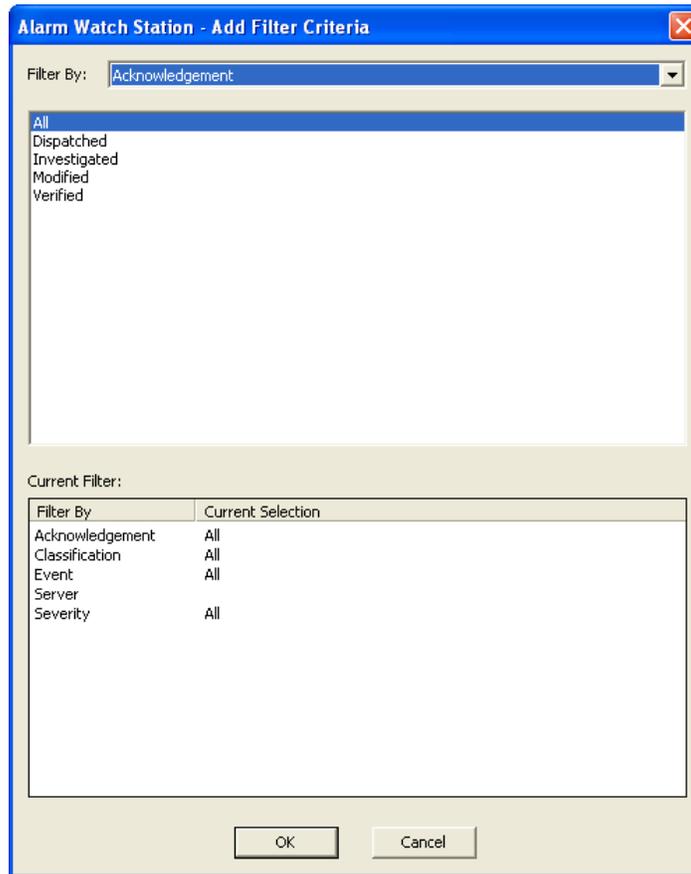
To select multiple acknowledgement states, press Ctrl while selecting items.

Change the Filter By option to define your filter.

3. Repeat [step 2](#) to select the combinations to be included for each field.
4. Click **OK** to make the filter rule take effect and exit the dialog. Click **Cancel** to discard your changes.

The detail of the currently defined filter displays in the Alarm Filter area.

Figure 13-33 Acknowledgement Filter Criteria

**TIP! Typical Scenario**

As a security operator, you may find it useful to select a subgroup of Analytics servers to be included in your filter, while another security operator may select a different subgroup of Analytics servers to be included in their filter. Monitoring tasks can be partitioned as each operator monitors alarms based on specific, different subgroups of Analytics servers. This is particularly useful in environments where a large number of Analytics servers are monitored.

Alternatively, you can partition servers by deploying multiple Alarm Management Servers and each AMS connects to a specific subgroup of Analytics servers. This has an added advantage of reducing the load on a single AMS for an environment with high alarm throughputs in the entire system.

Enabling or Disabling Alarm Filters

After defining the filter criteria:

- Click **Enable Filter** to apply the filter to the Alarm List. The border of the Alarm List area changes to light blue to indicate that this is now a filtered view (see [Figure 13-34](#)). The number of total alarms in the Alarm List and the number of alarms currently hidden by the filter are both displayed when the Alarm List switches to the filtered view.
- Click **Disable Filter** to turn off the filter and return to the default, unfiltered, view.

Figure 13-34 Alarm List with Filter Enabled

Alarm List (659 alarms, 28 hidden by filter)							
Date/Time	Server	Camera	Event	Severity	Classification	Acknowledgement	Modification
3/16/2009 10:44:13	localhost	Camera 2	Object entered restricted zone	4	Default		
3/16/2009 10:44:11	localhost	137.19.209....	Person stopped moving in wrong ...	4	Default		
3/16/2009 10:44:10	localhost	137.19.209....	Person exited restricted zone	4	Default		
3/16/2009 10:44:06	localhost	137.19.209....	Person trespassing line	4	Default		
3/16/2009 10:44:06	localhost	137.19.209....	Object trespassing line	4	Default		
3/16/2009 10:44:05	localhost	137.19.209....	Person started moving in wrong di...	4	Default		
3/16/2009 10:44:05	localhost	137.19.209....	Object started moving in wrong di...	4	Default		
3/16/2009 10:44:05	localhost	137.19.209....	Object started moving in wrong di...	4	Default		
3/16/2009 10:44:04	localhost	137.19.209....	Entered target zone	4	Default		
3/16/2009 10:44:04	localhost	137.19.209....	Entered target zone	4	Default		
3/16/2009 10:44:03	localhost	137.19.209....	Person entered restricted zone	4	Default		
3/16/2009 10:44:03	localhost	137.19.209....	Object entered restricted zone	4	Default		
3/16/2009 10:44:03	localhost	137.19.209....	Object entered restricted zone	4	Default		
3/16/2009 10:43:55	localhost	137.19.209....	Object started moving in wrong di...	4	Default		
3/16/2009 10:43:55	localhost	137.19.209....	Object started moving in wrong di...	4	Default		
3/16/2009 10:43:53	localhost	137.19.209....	Object entered restricted zone	4	Default		
3/16/2009 10:43:53	localhost	137.19.209....	Object entered restricted zone	4	Default		
3/16/2009 10:43:52	localhost	137.19.209....	Entered target zone	4	Default		
3/16/2009 10:43:52	localhost	137.19.209....	Entered target zone	4	Default		
3/16/2009 10:43:45	localhost	137.19.209....	Person exited restricted zone	4	Default		
3/16/2009 10:43:42	localhost	137.19.209....	Entered target zone	4	Default		
3/16/2009 10:43:42	localhost	137.19.209....	Entered target zone	4	Default		
3/16/2009 10:43:39	localhost	137.19.209....	Object entered restricted zone	4	Default		
3/16/2009 10:43:39	localhost	137.19.209....	Person entered restricted zone	4	Default		
3/16/2009 10:43:39	localhost	137.19.209....	Object entered restricted zone	4	Default		
3/16/2009 10:43:27	localhost	137.19.209....	Person stopped moving in wrong ...	4	Default		
3/16/2009 10:43:21	localhost	137.19.209....	Person exited restricted zone	4	Default		
3/16/2009 10:43:17	localhost	137.19.209....	Person trespassing line	4	Default		
3/16/2009 10:43:17	localhost	137.19.209....	Object trespassing line	4	Default		
3/16/2009 10:43:17	localhost	137.19.209....	Object started moving in wrong di...	4	Default		
3/16/2009 10:43:17	localhost	137.19.209....	Person started moving in wrong di...	4	Default		
3/16/2009 10:43:17	localhost	137.19.209....	Object started moving in wrong di...	4	Default		
3/16/2009 10:43:13	localhost	137.19.209....	Object entered restricted zone	4	Default		
3/16/2009 10:43:13	localhost	137.19.209....	Person entered restricted zone	4	Default		
3/16/2009 10:43:13	localhost	137.19.209....	Object entered restricted zone	4	Default		
3/16/2009 10:43:11	localhost	137.19.209....	Entered target zone	4	Default		
3/16/2009 10:43:11	localhost	137.19.209....	Entered target zone	4	Default		

Alarm Watch Station Startup

When Alarm Watch is launched, it has to retrieve older alarms that fall into the Live View period (or maximum number of alarms allowed) from the AMS alarm database. Therefore, during startup there may be a slight delay before the alarm list gets populated especially in the case where there have been a large number of alarms since the last time Alarm Watch Station has been running or when the default Live View period is long. When start fill is taking place, the message `Filling older alarms...` displays in the status bar as shown in [Figure 13-35](#).

Figure 13-35 Alarm Start Fill

Date/Time	Server	Camera	Event	Severity	Classification	Acknowledgement	Modification
3/16/2009 12:07:38	HVA 4.7 - 2ch	Camera 3	Object entered restricted zone	4	Default		
3/16/2009 12:07:10	HVA 4.7 - 2ch	Camera 3	Object entered restricted zone	4	Default		
3/16/2009 12:07:04	HVA 4.7 - 2ch	Camera 3	Object entered restricted zone	4	Default		
3/16/2009 12:02:02	HVA 4.7 - 2ch	Camera 3	Object entered restricted zone	4	Default		
3/16/2009 12:01:45	HVA 4.7 - 2ch	Camera 3	Object entered restricted zone	4	Default		
3/16/2009 11:50:38	HVA 4.7 - 2ch	Camera 3	Object entered restricted zone	4	Default		
3/16/2009 11:49:18	HVA 4.7 - 2ch	Camera 3	Object entered restricted zone	4	Default		
3/16/2009 11:39:46	HVA 4.7 - 2ch	Camera 3	Object entered restricted zone	4	Default		
3/16/2009 11:29:16	HVA 4.7 - 2ch	Camera 3	Object entered restricted zone	4	Default		
3/16/2009 11:27:41	HVA 4.7 - 2ch	Camera 3	Object entered restricted zone	4	Default		
3/16/2009 11:07:29	HVA 4.7 - 2ch	Camera 3	Object entered restricted zone	4	Default		
3/16/2009 11:03:10	HVA 4.7 - 2ch	Camera 3	Object entered restricted zone	4	Default		
3/16/2009 11:02:58	HVA 4.7 - 2ch	Camera 3	Object entered restricted zone	4	Default		
3/16/2009 10:59:23	HVA 4.7 - 2ch	Camera 3	Object entered restricted zone	4	Default		
3/16/2009 10:46:57	HVA 4.7 - 2ch	Camera 3	Object entered restricted zone	4	Default		
3/16/2009 10:44:38	HVA 4.7 - 2ch	Camera 3	Object entered restricted zone	4	Default		
3/16/2009 10:44:07	HVA 4.7 - 2ch	Camera 3	Object entered restricted zone	4	Default		
3/16/2009 10:42:46	HVA 4.7 - 2ch	Camera 3	Object entered restricted zone	4	Default		
3/16/2009 10:42:35	HVA 4.7 - 2ch	Camera 3	Object entered restricted zone	4	Default		
3/16/2009 10:41:25	HVA 4.7 - 2ch	Camera 3	Object entered restricted zone	4	Default		
3/16/2009 10:38:33	HVA 4.7 - 2ch	Camera 3	Object entered restricted zone	4	Default		
3/16/2009 10:38:19	HVA 4.7 - 2ch	Camera 3	Object entered restricted zone	4	Default		
3/16/2009 10:36:31	HVA 4.7 - 2ch	Camera 3	Object entered restricted zone	4	Default		
3/16/2009 10:33:49	HVA 4.7 - 2ch	Camera 3	Object entered restricted zone	4	Default		
3/16/2009 10:32:24	HVA 4.7 - 2ch	Camera 3	Object entered restricted zone	4	Default		
3/16/2009 10:32:23	HVA 4.7 - 2ch	Camera 3	Object entered restricted zone	4	Default		
3/16/2009 10:32:23	HVA 4.7 - 2ch	Camera 3	Object entered restricted zone	4	Default		
3/16/2009 10:32:08	HVA 4.7 - 2ch	Camera 3	Object entered restricted zone	4	Default		
3/16/2009 10:32:04	HVA 4.7 - 2ch	Camera 3	Object entered restricted zone	4	Default		
3/16/2009 10:30:33	HVA 4.7 - 2ch	Camera 3	Object entered restricted zone	4	Default		
3/16/2009 10:29:58	HVA 4.7 - 2ch	Camera 3	Object entered restricted zone	4	Default		
3/16/2009 10:29:13	HVA 4.7 - 2ch	Camera 3	Object entered restricted zone	4	Default		
3/16/2009 10:27:14	HVA 4.7 - 2ch	Camera 3	Object entered restricted zone	4	Default		
3/16/2009 10:25:59	Fusion - 2ch	Position1	Object entered restricted zone	4	Default		
3/16/2009 10:20:07	HVA 4.7 - 2ch	Camera 3	Object entered restricted zone	4	Default		
3/16/2009 10:20:04	HVA 4.7 - 2ch	Camera 3	Object entered restricted zone	4	Default		
3/16/2009 10:14:57	HVA 4.7 - 2ch	Camera 3	Object entered restricted zone	4	Default		

erver errors - View status for details Filling older alarms... Connect

Alarm Backfill

Start fill refers to the start-up fill of older alarms when Alarm Watch Station is launched and it has to retrieve older alarms that fall into the Live View period (or maximum number of alarms allowed) from AMS alarm database.

There may be an occasional instance where the Alarm Management Server is down, the Alarm Management Service has stopped, or there is a network issue that prevents the Alarm Management Server from reaching an Analytics server in the server list. When this happens, alarms generated on the Analytics servers cannot be delivered to the Alarm Management Server and they are only stored in the analytics database that is local to that server. When the Alarm Management Service restarts, it re-establishes connection to all analytics servers. Alarms generated during the time when Alarm Management Service is offline will start to be backfilled from the analytics server to the Alarm Management Server to ensure that there is no 'gap' in the alarm database on the Alarm Management Server. After an alarm is backfilled, it will be delivered from Alarm Management Service to any connected Alarm Watch Station client applications.

It is potentially possible that the communication between the Alarm Management Server and any Analytics server is down for an extended period of time. During such period a large number of alarms may have been generated. To prevent the backfilled alarms from maxing out the load on the Alarm Management Server and blocking live alarms, alarm backfill runs in a lower priority and it may take some time for alarms from this gap period to be fully backfilled.

Alarm Watch

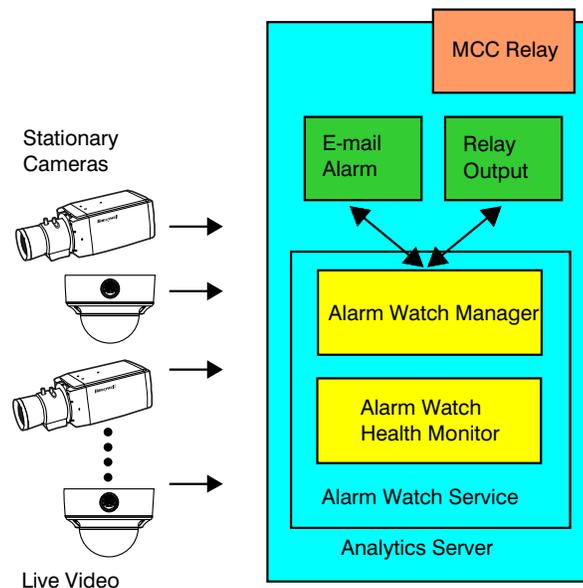
The Alarm Watch module is an add-on component to the Honeywell Video Analytics software suite. This module enables additional alarm delivery mechanisms, including e-mail alarms and relay outputs.

The Alarm Watch module is included with the Honeywell Video Analytics — Full package and is intended to be installed on the Video Analytics process server.

The detailed block diagram of the Alarm Watch module is depicted in [Figure 14-1](#). The Alarm Watch software includes The Alarm Watch Server Service along with the following two GUI components:

- **Alarm Watch Manager:** This is the configuration tool for Alarm Watch, which allows the user to configure which Analytics servers the Alarm Watch Service is connecting to, and which alarm outputs to enable such as e-mail and MCC relay output. It also allows the Administrator to set up users for accessing the Alarm Watch Service.
- **Alarm Watch Health Monitor:** This is a small utility program that monitors the connection status from the Alarm Watch Server Service to the Analytics servers and the alarm delivery activities.

Figure 14-1 Alarm Watch Module



The Alarm Watch is typically installed on the Analytics server although it can be installed on a separate PC solely for handling e-mail and relay outputs when alarms occur.

Table 14-1 Alarm Watch Package Modules

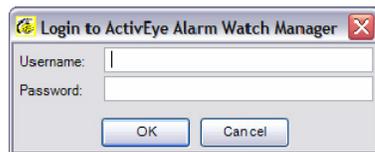
Alarm Watch Module	Installed on ...	For the purpose of ...
E-Mail Client	Local	E-mail alarm output that enables analytics alarms to be delivered to a user-specified list of recipients when they occur.
MCC Client	Local	Provides the relay output that can be added to the system. Please refer to the Video Analytics V4 Installation Guide for a list of supported MCC relay board models.

User Administration

The Alarm Watch Manager requires an authorized Alarm Watch user to log on to connect to the Alarm Watch Service when the application is started (see [Figure 14-2](#)).

Note The user administration for Alarm Watch is separate from the Account Manager for users connecting to the Analytics server (see [Chapter 3](#)).

Figure 14-2 Alarm Watch Login Dialog



Logging On the First Time

The first time you use the Alarm Watch Manager, there will be no users in the system and you can set yourself up as an administrator (see [Figure 14-3](#)). The OK button on this dialog is grayed out until you enter a user name.

Figure 14-3 No Users Found Prompt Message



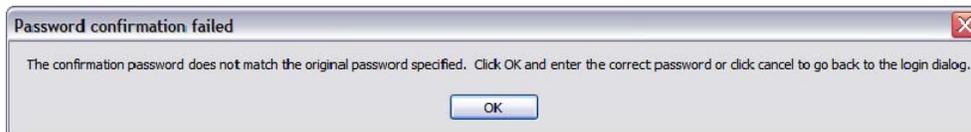
If you enter a password, and then click **OK**, a confirmation dialog (*Figure 14-4*) displays prompting you to re-enter the password.

Figure 14-4 Password Confirmation Message



If you enter the confirmation password incorrectly, the following failure dialog displays (*Figure 14-5*). Click **OK** to go back to the password confirmation dialog.

Figure 14-5 Password Confirmation Failed Error Message



The following confirmation dialog (*Figure 14-6*) indicates you have successfully created the administrative user.

Figure 14-6 Admin Added Successfully Message

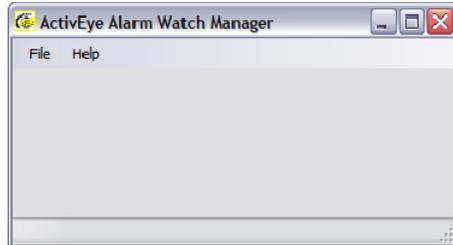


If the Alarm Watch Server Service is not available (which might happen if the service is shut down), the following error dialog displays (*Figure 14-7*). After you confirm the error, the Logon dialog appears again.

Figure 14-7 Alarm Watch Manager Logon Error Message



If you cancel out of the Logon dialog, a blank main window displays (Figure). From this window, use the **File ► Login** command to log on.



Using Alarm Watch Manager

After logging on, the Alarm Watch Manager main window displays (Figure 14-8).

Figure 14-8 Alarm Watch Manager Main Window



1. Click the **localhost** directory of the Alarm Watch Servers tree to expand and display the different configurable components of Alarm Watch.
2. From here you can add or remove Servers and Users, and configure Clients (see [Figure 14-9](#)).

Sub-directory	Description
Servers	Where the Analytics servers are configured
Clients	Options are Alarm Watch Email Client, or MCC Relay Client.
Users	Lists Alarm Watch users only; this user information is not necessarily related to the users accounts configured for a specific analytics and it is only intended to grant permissions to the Alarm Watch system.

Figure 14-9 Alarm Watch Servers Tree View



The Add and Remove buttons on the Alarm Watch Main Window are only active when the related action is legal; that is, **Add** is available when the Servers or Users node is selected and **Remove** is available when a specific Server or User is selected.

3. Click **Remove** to remove the selected server or user after you click **Yes** in the confirmation dialog (see *Figure 14-10*). The Clients list is pre-populated automatically and an entry is added for each type of Alarm Watch client module that is currently installed on the system.

Figure 14-10 Removal Confirmation Message



Configuring Servers

To configure servers:

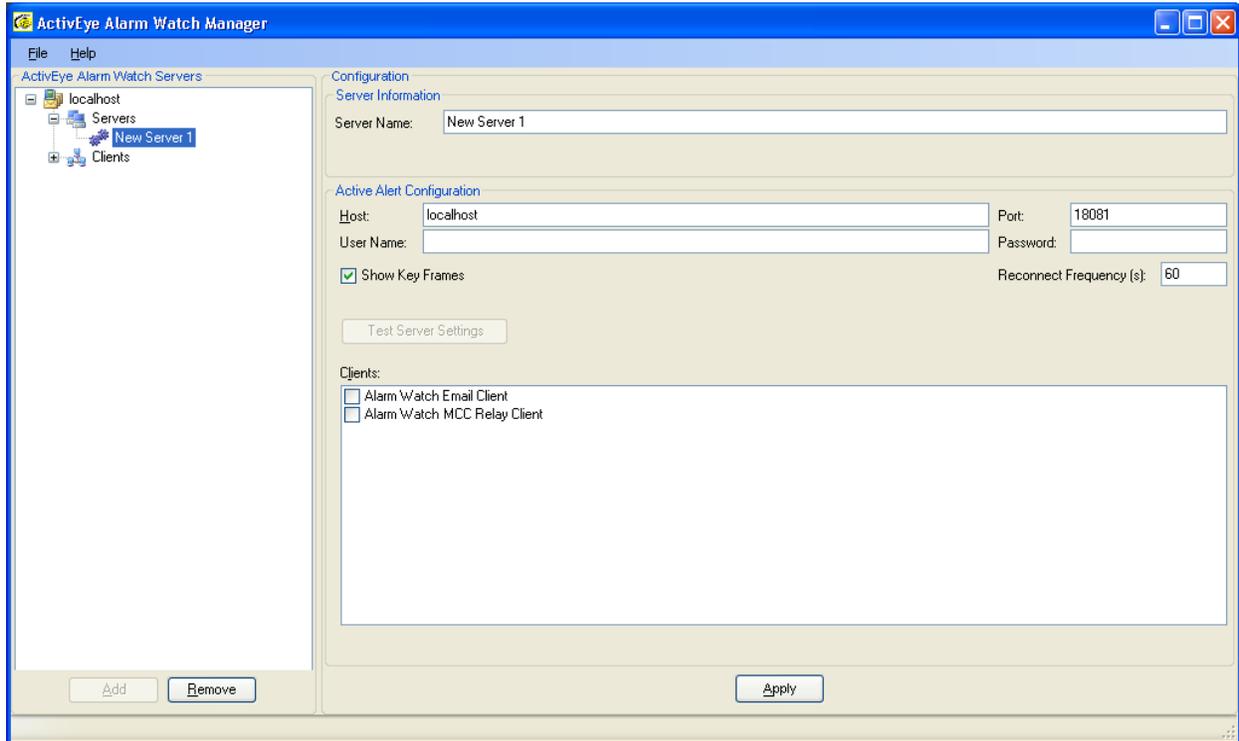
1. Click **Add** when the Servers node is selected,

OR

Select an existing server under the Servers sub-directory in the Alarm Watch Servers area. A new or selected server configuration displays in the right-hand (Configuration) pane.

Figure 14-11 shows an example of the default server configuration for new servers.

Figure 14-11 New Server Configuration



2. Follow [Table 14-2](#) to complete a server configuration settings.

Table 14-2 Server Configuration Settings

Setting	Required Field	Description
Server Name		User-friendly server name. There are no restrictions on the server name, but the name should be something that is suggestive of the source of the alarms.
Host		Computer name or IP address of the Analytics server host computer.
Port		TCP port number of the Analytics server host computer (default is 18081).
User Name	✓	A generic user account that has Live View permission on the Analytics server. This should not be any user account but should be one created especially for use by Alarm Watch.
Password	✓	Password for the user specified in User Name.
Show Key Frames		Specifies whether or not alarm key frames will be requested from the Analytics server. Default is checked.

Table 14-2 Server Configuration Settings (cont'd)

Setting	Required Field	Description
Reconnect Frequency (s)		Time in seconds between reconnection attempts when the Alarm Watch Server detects a connection failure to the Analytics server specified.
Test Server Settings		Use to verify if the Analytics server settings and user settings are correct.
Clients		Lists all available client modules. Checked items are client modules to which alarms are sent.

Note The Username and Password fields are required. If you try to apply changes with a blank user name or password, the following dialog appears.

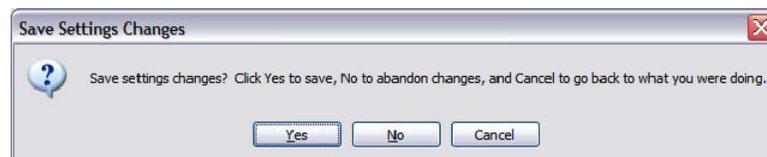


3. Click **Apply** when you are done modifying settings.
4. If you attempt to change sub-directories (for example, from Servers to Clients) before applying changed settings, you are prompted to save your setting changes (see [Figure 14-12](#)).

Click **Yes** to save the changes and change sub-directories, **No** to abandon changes and change sub-directories, or **Cancel** to go back to the server settings.

Trying to exit the application without clicking Apply will show the same dialog.

Figure 14-12 Save Settings Changes



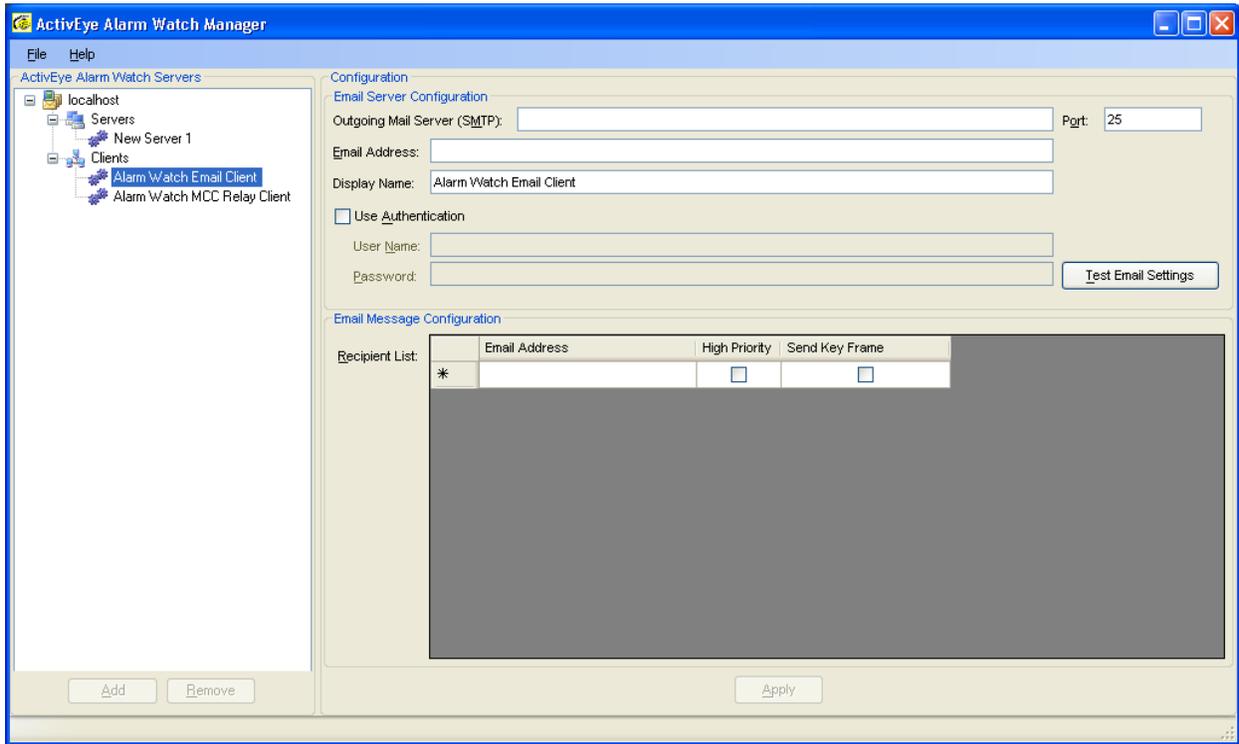
Configuring Clients

To configure clients:

1. Select an existing client under the Clients sub-directory in the Alarm Watch Servers area to see the selected client configuration in the right-hand (Configuration) pane.

[Figure 14-13](#) shows an example of the default Alarm Watch Station Client configuration for new clients.

Figure 14-13 New Client Configuration



2. Follow [Table 14-3](#) to configure an Alarm Watch Station Client.

Table 14-3 Client Configuration Settings

Setting	Description
Message Expiration	The amount of time for which an Alarm is held until a client receives it. This is predominately used when it is expected that the Alarm Watch Station Client may not always be running and alarms should eventually expire after a certain amount of time.

Validating the Configuration

Alarm Watch Manager informs the user if a known configuration will cause problems. When the user attempts to exit the program, warning dialogs display if there are no servers defined (see *Figure 14-14 A*), any server without at least one client is selected (see *Figure 14-14 B*), or a User list with no User at the selected User level (see *Figure 14-14 C*).

Figure 14-14 Server Error Messages

A. Server Missing Error Message



B. Selected Clients Missing Error Message



C. User Level Missing User Error Message



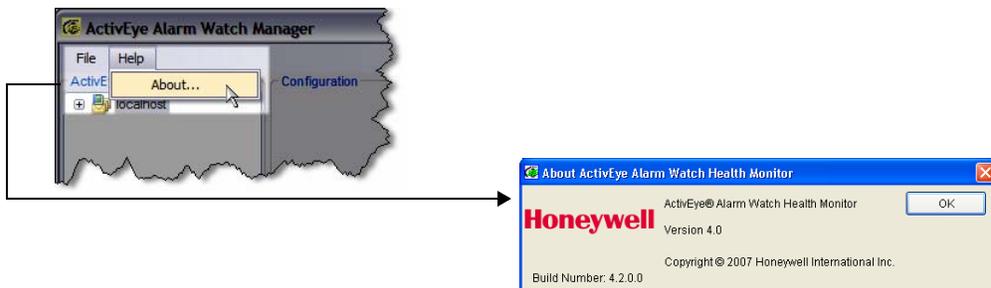
In each case, you can click **OK** to ignore the error, but this is not recommended as Alarm Watch will not work properly in the state that prompted any of these dialogs to be displayed.

Click **Cancel** to close the dialog and either add one or more Servers, select one or more Clients for the specified server, or add a User level with a valid user to the Users list.

Confirming the Software Copyright and Version

From the **Help** menu, select **About** to display the About window showing the copyright and version number of the software (see *Figure 14-15*).

Figure 14-15 Help ► About Command



Alarm Watch Email Client

The Alarm Watch Email Client provides a mechanism for sending alarm e-mails from the Alarm Watch module. It is typically installed with the Honeywell Video Analytics Suite–Server package and is designed to be running on the Analytics server. This chapter describes how to configure the Alarm Watch Email Client.

The Alarm Watch Email Client configuration is managed using the Alarm Watch Manager.

1. Launch Alarm Watch Manager.
2. Expand the localhost directory by double-clicking **localhost** or, Click the plus symbol to the left of localhost (see [Figure 14-16](#)).

Figure 14-16 Localhost Directory in Alarm Watch Manager



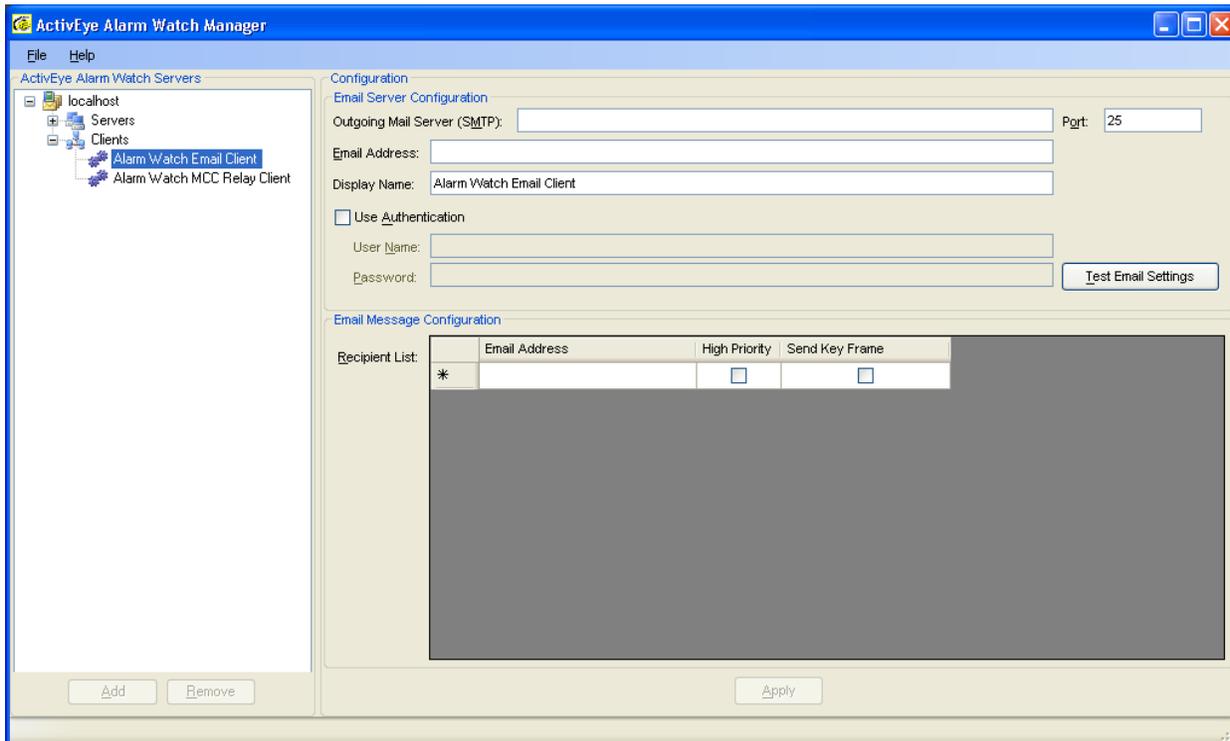
3. Expand the Clients sub-directory underneath that by double-clicking **Clients** or clicking the plus symbol to the left of the Client icon. If Alarm Watch Email Client is available on your system, it is displayed under Clients (see [Figure 14-17](#)).

Figure 14-17 Clients Sub-Directory in Alarm Watch Manager



4. Select **Alarm Watch Email Client** to display the configuration window on the right side of the screen (see [Figure 14-18](#)).

Figure 14-18 E-mail Configuration Screen



5. Follow [Table 14-2](#) to configure the Alarm Watch Email Client.

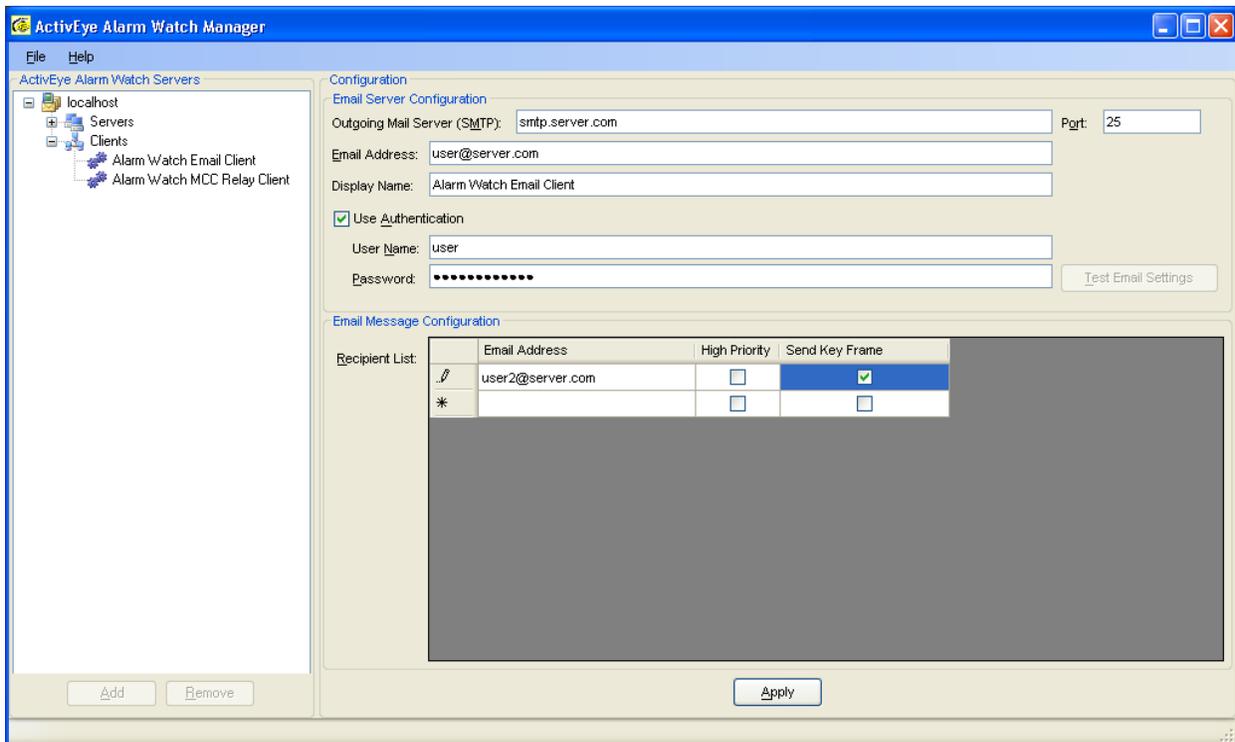
Table 14-4 Server Configuration Settings

Setting	Description
Outgoing Mail Server (SMTP)	Server name of the mail server through which e-mails are sent. The format for this field is typically: smtp.server.com
Port	Port number of the SMTP server. The default value is 25, which is the well known port number for SMTP servers.
Email Address	E-mail address from which this e-mail will be sent.
Display Name	Friendly name that appears in the From field of the e-mail message. The default value is Alarm Watch Email Client.
Use Authentication	Check this if your server requires authentication. This enables the User Name and Password fields.
User Name	User name to present to the SMTP server when generating e-mails.
Password	Password to present to the SMTP server when generating e-mails.
Recipient List	One or more e-mail addresses to which the alarm e-mail is sent.

Table 14-4 Server Configuration Settings

Setting	Description
Recipient List: Email Address	E-mail address for a given recipient.
Recipient List: High Priority	Send the e-mail with the high priority flag set.
Recipient List: Send Key Frame	It is possible to send the alarms without key frames so as to inform recipients without sending larger e-mail messages. Check this box to include key frames in the e-mail message.

A typical configuration is shown in [Figure 14-19](#).

Figure 14-19 Sample Configuration

- Clicking **Test Email Settings** (see [Figure 14-19](#)) sends a test e-mail to all recipients in the recipient list. A confirmation dialog appears showing success (see [Figure 14-20](#)). If there is a problem you will see an error message similar to [Figure 14-21](#), indicating an invalid SMTP server.
- The test e-mail should appear as shown in [Figure 14-22](#). The Test Email Settings button will not be enabled when modified settings have not yet been applied. Click **Apply** before testing configuration settings.
- To delete a recipient from the recipient list, click the cell to the left of the e-mail address and then press **Delete**.

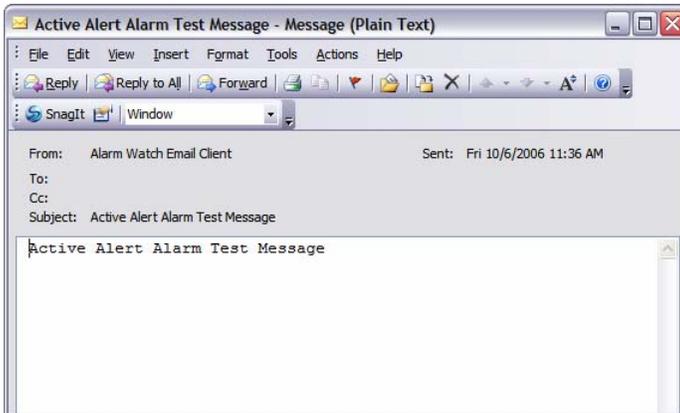
Figure 14-20 Test E-mail Success Message



Figure 14-21 Test E-Mail Failure Message (Invalid SMTP Server)



Figure 14-22 Test E-mail



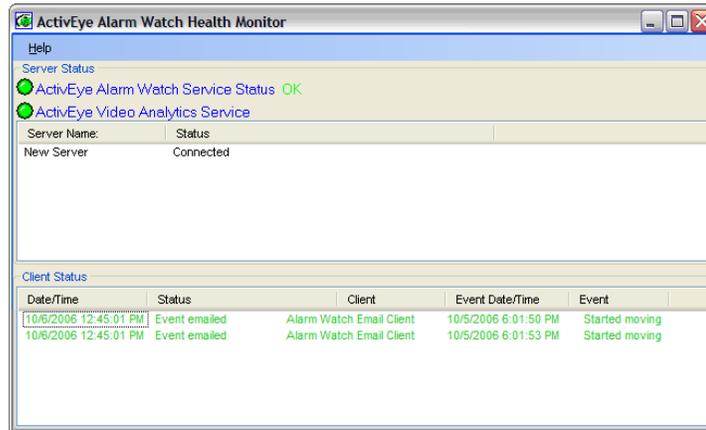
The configuration tool alerts the user to common problems, like entering an incorrectly formatted e-mail address.



Caution **IMPORTANT**
Alarm e-mails will not be sent unless at least one server is configured to send e-mails. See [Configuring Clients](#), page 243 for details on configuring Clients for any specific server.

After the Alarm Watch Email Client has been configured and at least one server is configured to send e-mails, the e-mail status can be seen using the Alarm Watch Health Monitor (see [Figure 14-23](#)). For more details, see [Alarm Watch Health Monitor](#), page 252.

Figure 14-23 E-mail Status in Alarm Watch Health Monitor



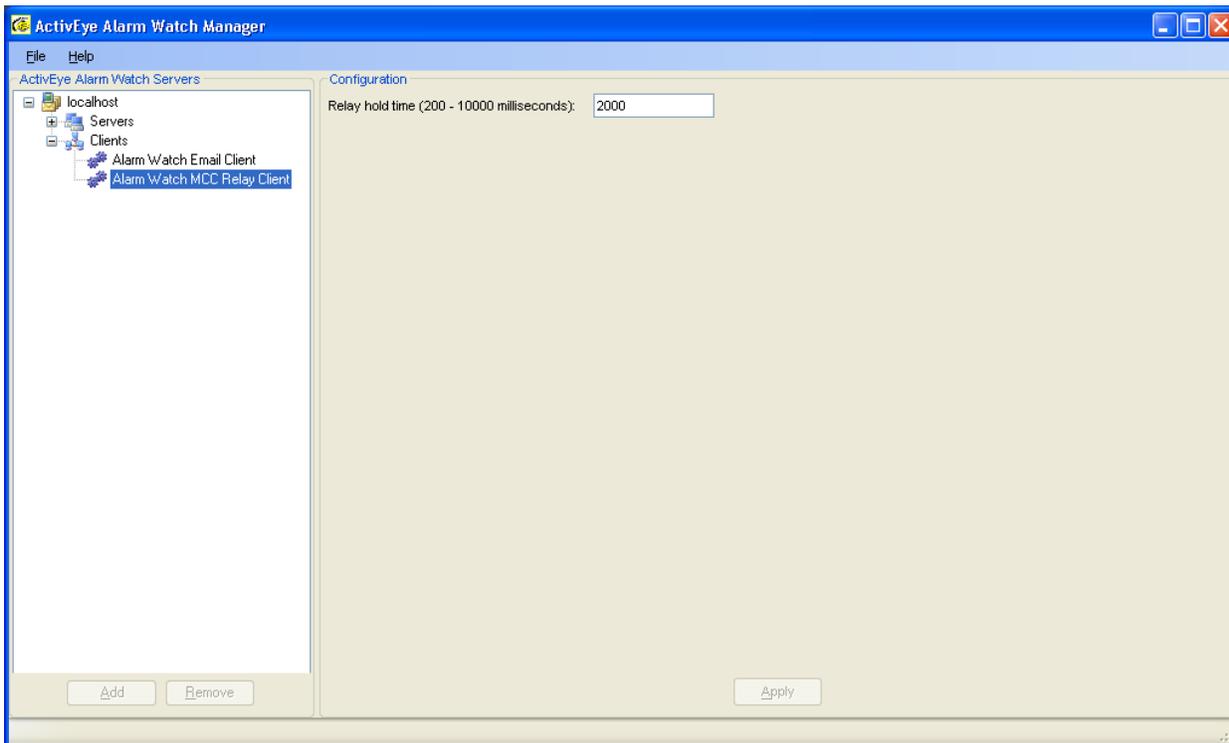
Alarm Watch MCC Relay Client

The Alarm Watch MCC Relay Client is an alarm output module that can be enabled in your system to provide the relay output functionality. The Relay Client is installed as part of the Honeywell Video Analytics Suite–Server package. It requires a certified MCC relay board to be installed on the server machine.

This chapter describes how to enable the Alarm Watch MCC Relay Client.

1. After installing the Alarm Watch MCC Relay client, launch the Alarm Watch Manager. The installed Relay Client under the Clients sub-directory (see [Figure 14-24](#)).

Figure 14-24 Alarm Watch Manager with MCC Relay Client



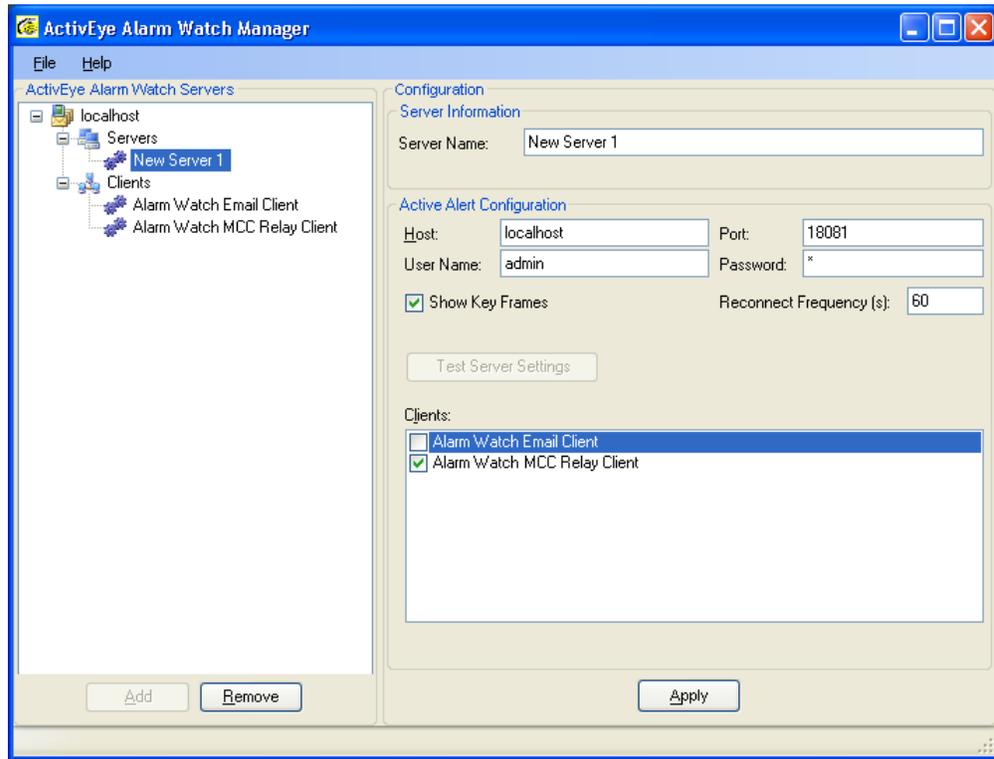
2. Select the server from the Alarm Watch Servers list from which alarms will be sent to the relay.
3. Ensure that the **Alarm Watch MCC Relay Client** check box is selected in the Clients list (See [Figure 14-25](#)). There is a one-to-one correspondence between the camera and the relay output on the board. If the relay board has 8 outputs, enabling the MCC Relay Client sends the alarms from the first 8 channels (with channel ID 1 to 8) to the 8 outputs on the relay card. No other configuration is necessary.

If the relay board has 16 or more relay outputs, alarms from channel ID 1 to 16 are sent to the first 16 relays on the board. Channel ID higher than the supported number of relays are not mapped to any relay.



Caution Only one relay module can be connected to each analytics server. Therefore, the number of relay outputs on the relay module must match the number of channels being processed on the analytics server.

Figure 14-25 Alarm Watch MCC Relay Client Selection



4. Configure the relay hold time in milliseconds. This is the duration the relay remains open when the alarm occurs before it returns to the normally closed state. The default value is 2000 milliseconds (or 2 seconds). If multiple alarms arrive consecutively for the same camera, the duration for the relay to remain open is prolonged, depending on how many alarms have arrived and are waiting in the queue to trigger the relay.

Alarm Watch Health Monitor

The Alarm Watch Health Monitor application runs on the Analytics server to provide a real-time status display for the Alarm Watch system. With this application, you can monitor the Alarm Watch Server Service, its connection to Analytics servers, and Alarm Watch Clients that do not provide a user interface, such as the Alarm Watch Email Client and the Alarm Watch MCC Relay Client.

The Alarm Watch Health Monitor is installed to normally run in a minimized state and to be accessible in the notification area of the Windows taskbar (see [Figure 14-26](#)).

Figure 14-26 Notification Area with Alarm Watch Health Monitor



The icon contains a small LED-like indicator that shows whether or not there are currently any server problems. The indicator flashes **red** when there is a problem that needs to be addressed or shows **solid green** (see *Figure 14-27*).

Figure 14-27 Notification Area with Alarm Watch Health Monitor Alert



1. Right-click the notification icon to display a menu with two options:
 - Open Alarm Watch Health Monitor
 - Exit (see *Figure 14-28*).

Figure 14-28 Alarm Watch Health Monitor Notification Icon Menu



2. Select **Open Alarm Watch Health Monitor** (or double-click the notification icon) to display the main window of the application (see *Figure 14-29*).

Figure 14-29 Alarm Watch Health Monitor Main Screen



The Server Status area (see *Figure 14-30*) describes the Alarm Watch Service Status and any Analytics servers configured to connect with the Alarm Watch Service. As long as both indicators are **green**, the status is OK and the system will run correctly.

Figure 14-30 Alarm Watch Health Monitor Server Status



Typically, the only problems that can occur are the Alarm Watch Server Service being disabled (see *Figure 14-31 A*), or a particular Analytics server is either disabled or configured incorrectly (see *Figure 14-31 B*).

Figure 14-31 Alarm Watch Error Messages

A. Server Not Found



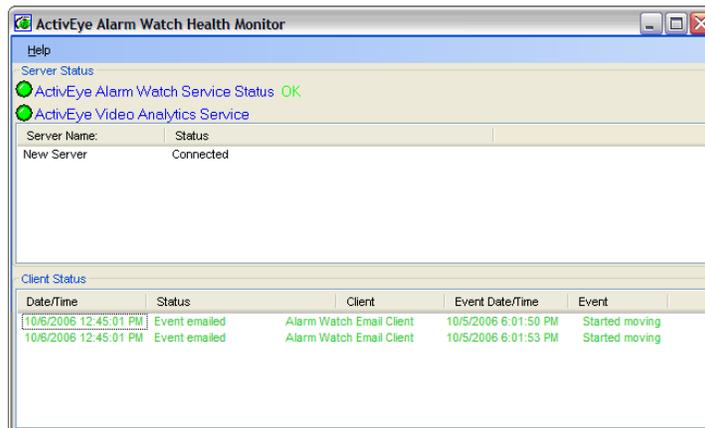
B. Service Status Failure



The client status area of the window displays all events and the actions pertaining to those events that are being handled by Alarm Watch Clients that do not contain a user interface of their own (for example, Alarm Watch Station).

The example shown in *Figure 14-32* demonstrates the display when two alarms are e-mailed.

Figure 14-32 Client Status Area

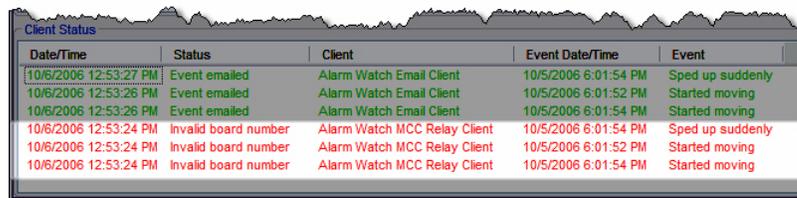


Legend

- Date/Time** = when alarm was e-mailed
- Status** = the action taken
- Client** = which client handled the alarm
- Event Date/Time** = actual time of the event
- Event** = event description

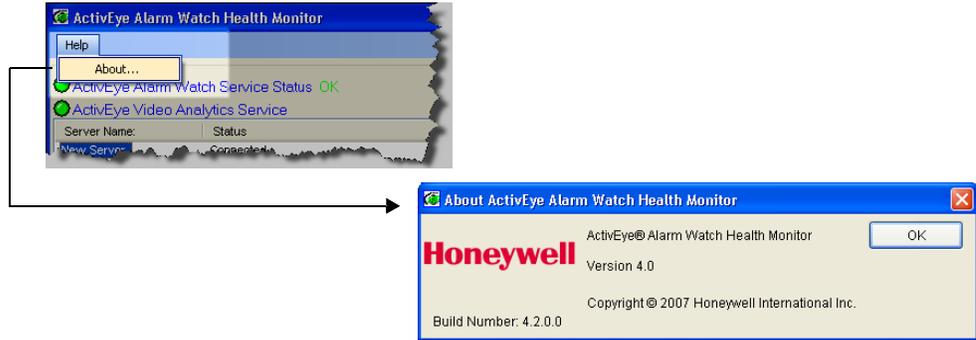
If there are any errors, these will appear in the Client Status as well. *Figure 14-33* shows errors from having an MCC Relay Card Client configured but not connected when alarms are received.

Figure 14-33 Client Errors



3. To close the application, click **Exit** (see *Figure 14-28*) exits the application.
Click **X** in the system menu to minimize the application back to the notification bar. Minimizing the application by clicking the minimize button in the system menu will minimize the application to the task bar.
4. Select **Help ► About...** (see *Figure 14-34*) to view the copyright and version number of the software.

Figure 14-34 Help ► About Menu Command



A

Event Library

This release of Honeywell Video Analytics software offers an event library that collectively contains 46 events across all product packages. These events can be detected in real-time as video is being processed.

This appendix lists the definition and usage for each event. The events are listed and grouped into five categories:

- Object Motion Events
- People Events
- Traffic Events
- Counting Events
- Video Events

[Table A-1](#) provides a quick reference for the events contained in each product package.

Table A-1 Events Contained in Product Packages

Event	Honeywell Video Analytics Package				
	Base	Standard	Premium	People Counting	Smart Impressions
People Events					
person entered restricted zone	X	X	X		
person exited restricted zone	X	X	X		
person loitering in restricted zone		X	X		
person started moving in wrong direction	X	X	X		
person stopped moving in wrong direction	X	X	X		
person on fence line		X	X		
person started running				X	
person stopped running				X	
people converged		X	X		
people passed by		X	X		
person trespassing - tripwire	X	X	X		
person running in wrong direction				X	
person in sterile zone		X	X		
Car Traffic Events					
car started moving in wrong direction	X	X	X		
car stopped moving in wrong direction	X	X	X		
car entered restricted zone	X	X	X		

Table A-1 Events Contained in Product Packages

Event	Honeywell Video Analytics Package				
	Base	Standard	Premium	People Counting	Smart Impressions
car parked in restricted zone		X	X		
car speeding			X		
car made illegal u-turn		X	X		
car parked in handicapped zone		X	X		
car pulled off road		X	X		
car needs assistance		X	X		
car exited restricted zone	X	X	X		
car trespassing - tripwire	X	X	X		
car in sterile zone		X	X		
Video/Camera Events					
video signal lost	X	X	X	X	X
video signal restored	X	X	X	X	X
Counting Events					
person counted as entering		X	X	X	X
person counted as exiting		X	X	X	X
car entered lot		X	X		X
car exited lot		X	X		X
car counted in lane			X		X
Premium Events					
object left unattended			X		
object removed			X		
possible theft			X		
Smart Impressions					
entering target zone					X
staying in target zone					X

Object Motion Events

Object Entered

This event informs the user any time the object enters the field of view as long as the object size is at least 18 pixels.

	Description
Syntax	(object) entered
Object type	Person, car, object
Zone setting	No zone is required.
Default severity level	1
Remarks	None
See also	<i>Object Exited</i>
Availability	Active Alert Standard, Active Alert Premium, Smart Impressions

Object Exited

This event will inform the user any time any currently tracked object exits the field of view.

	Description
Syntax	(object) exited
Object type	Person, car, object
Zone setting	No zone is required.
Default severity level	1
Remarks	None
See also	<i>Object Entered</i>
Availability	Active Alert Standard, Active Alert Premium, Smart Impressions

Object Entered Restricted Zone

An object has entered a restricted area.

	Description
Syntax	(object) entered (zone)
Object type	Person, car, object
Zone setting	restricted zone
Default severity level	4
Remarks	None
See also	<i>Object Exited Restricted Zone, Person Entered Restricted Zone, Person Exited Restricted Zone, Car Entered Restricted Area, Car Exited Restricted Area</i>
Availability	Active Alert Base, Active Alert Standard, Active Alert Premium

Object Exited Restricted Zone

An object has exited a restricted area.

	Description
Syntax	(object) exited (zone)
Object type	Person, car, object
Zone setting	restricted zone
Default severity level	3
Remarks	None
See also	<i>Object Entered Restricted Zone, Person Entered Restricted Zone, Person Exited Restricted Zone, Car Entered Restricted Area, Car Exited Restricted Area</i>
Availability	Active Alert Base, Active Alert Standard, Active Alert Premium

Object Started Moving

An object has started to move (that is, from a stationary state to a moving state).

	Description
Syntax	(object) started moving
Object type	Person, car, object
Zone setting	No zone is required
Default severity level	2

	Description
Remarks	None
See also	Object Stopped Moving in the Wrong Direction
Availability	Active Alert Standard, Active Alert Premium

Object Stopped

An object has stopped (that is, from a moving state to a stationary state).

	Description
Syntax	(object) stopped
Object type	Person, car, object
Zone setting	No zone is required.
Default severity level	2
Remarks	None
See also	Object Started Moving
Availability	Active Alert Standard, Active Alert Premium

Object Started Moving in the Wrong Direction

An object has started moving in the wrong direction.

	Description
Syntax	(object) started moving in the wrong direction (zone)
Object type	Person, car, object
Zone setting	Directional zone
Default severity level	4
Remarks	None
See also	Object Stopped Moving in the Wrong Direction , Person Started Moving in the Wrong Direction , Person Stopped Moving in the Wrong Direction , Car Started Driving in the Wrong Direction , Car Stopped Driving in the Wrong Direction
Availability	Active Alert Base, Active Alert Standard, Active Alert Premium

Object Stopped Moving in the Wrong Direction

An object has stopped moving in the wrong direction.

	Description
Syntax	(object) stopped moving in the wrong direction (zone)
Object type	Person, car, object
Zone setting	Directional zone
Default severity level	3
Remarks	None
See also	<i>Object Started Moving in the Wrong Direction, Person Started Moving in the Wrong Direction, Person Stopped Moving in the Wrong Direction, Car Started Driving in the Wrong Direction, Car Stopped Driving in the Wrong Direction</i>
Availability	Active Alert Base, Active Alert Standard, Active Alert Premium

Object Trespassing

An object has trespassed the virtual perimeter.

	Description
Syntax	(object) trespassing (line)
Object type	Person, car, object
Zone setting	Trespass line
Default severity level	4
Remarks	The trespass line zone includes a line segment that defines the virtual perimeter, and an intersecting vector that defines the <i>allowed</i> moving direction passing the trespass line. An Object Trespassing event is detected when an object has trespassed this virtual perimeter by moving against the allowed direction.
See also	<i>Object Trespassing, Person Trespassing, Car Trespassing, Object Started Moving in the Wrong Direction</i>
Availability	Active Alert Base, Active Alert Standard, Active Alert Premium

Object in Sterile Zone

An object has entered the sterile zone and is moving towards the virtual perimeter.

	Description
Syntax	(object) in (sterile zone)
Object type	Person, car, object
Zone setting	Sterile zone
Default severity level	5
Remarks	The sterile zone is a quadrilateral zone that includes 3 red borders and 1 green border. The green border defines the allowed entry at the virtual perimeter into the zone. If the object enters the zone through any of the red borders and moves beyond the original entry point to approach the virtual perimeter, this event will be generated.
See also	Object Entered Restricted Zone , Object Trespassing , Person in Sterile Zone , Car in Sterile Zone
Availability	Active Alert Standard, Active Alert Premium

Objects Merged

One object has merged with another object.

	Description
Syntax	(object 2) merged to (object 1)
Object type	Object 1: person, car, object Object 2: person, car, object
Zone setting	No zone is required.
Default severity level	1
Remarks	An Objects Merged event is detected when an object (or group of objects) comes close to another object (or group of objects). When objects merge, there may be no occlusion, partial occlusion or full occlusion. Camera placement and the amount of occlusion play an important role in object tracking. Please see Selecting the Appropriate Camera , page 33 to revisit the operating conditions for optimal system setup.
See also	Objects Split
Availability	Active Alert Standard, Active Alert Premium, Smart Impressions

Objects Split

One object has split from another object.

	Description
Syntax	(object 2) split from (object 1)
Object type	Object 1: person, car, object Object 2: person, car, object
Zone setting	No zone is required.
Default severity level	1
Remarks	Objects Split is the reverse event of Objects Merged . An Objects Split is detected when two objects (or groups of objects), which had been merged, become separate from one another.
See also	Objects Merged
Availability	Active Alert Standard, Active Alert Premium, Smart Impressions

Objects Left Unattended

An object has been left unattended.

	Description
Syntax	(object) left unattended
Object type	Object
Zone setting	Detection zone
Default severity level	7
Remarks	None
Availability	Active Alert Premium

Objects Removed

An object has been removed from its original location as marked by the asset zone.

	Description
Syntax	(object) removed
Object type	Object
Zone setting	Asset zone

	Description
Default severity level	7
Remarks	None
Availability	Active Alert Premium

People Events

Person Entered Restricted Zone

A person has entered a restricted area.

	Description
Syntax	(object) entered (zone)
Object type	Person
Zone setting	Restricted zone
Default severity level	4
Remarks	None
See also	Person Exited Restricted Zone , Person Loitering in Restricted Zone , Car Entered Restricted Area , Car Exited Restricted Area
Availability	Active Alert Base, Active Alert Standard, Active Alert Premium

Person Exited Restricted Zone

A person has exited a restricted area.

	Description
Syntax	(object) exited (zone)
Object type	Person
Zone setting	Restricted zone
Default severity level	3
Remarks	None
See also	Person Entered Restricted Zone , Person Loitering in Restricted Zone , Car Entered Restricted Area , Car Exited Restricted Area
Availability	Active Alert Base, Active Alert Standard, Active Alert Premium

Person Loitering in Restricted Zone

A person is loitering in a restricted area.

	Description
Syntax	(person) loitering in restricted (zone)
Object type	Person
Zone setting	Restricted zone
Default severity level	5
Remarks	A person is considered loitering in a restricted area after they stay in the restricted area for more than a user-defined duration, such as 60 seconds. The maximum duration can be 5 minutes (300 seconds).
See also	Person Entered Restricted Zone , Person Exited Restricted Zone
Availability	Active Alert Standard, Active Alert Premium

Person Started Moving in the Wrong Direction

A person has started moving in the wrong direction.

	Description
Syntax	(object) started moving in the wrong direction (zone)
Object type	Person
Zone setting	Directional zone
Default severity level	4
Remarks	None
See also	Person Stopped Moving in the Wrong Direction , Car Started Driving in the Wrong Direction , Car Stopped Driving in the Wrong Direction
Availability	Active Alert Base, Active Alert Standard, Active Alert Premium

Person Stopped Moving in the Wrong Direction

A person has stopped moving in the wrong direction.

	Description
Syntax	(object) stopped moving in the wrong direction (zone)
Object type	Person
Zone setting	Directional zone
Default severity level	3
Remarks	None
See also	Person Started Moving in the Wrong Direction , Car Started Driving in the Wrong Direction , Car Stopped Driving in the Wrong Direction
Availability	Active Alert Base, Active Alert Standard, Active Alert Premium

Person Trespassing

A person has trespassed the virtual perimeter.

	Description
Syntax	(person) trespassing (line)
Object type	Person
Zone setting	Trespass line
Default severity level	4
Remarks	The trespass line zone includes a line segment that defines the virtual perimeter, and an intersecting vector that defines the <i>allowed</i> moving direction passing the trespass line. A Person Trespassing event is detected when a person has trespassed this virtual perimeter by moving against the allowed direction.
See also	Object Trespassing , Person Trespassing , Car Trespassing , Person Started Moving in the Wrong Direction
Availability	Active Alert Base, Active Alert Standard, Active Alert Premium

Person in Sterile Zone

A person has entered the sterile zone and is moving towards the virtual perimeter.

	Description
Syntax	(person) in (sterile zone)
Object type	Person
Zone setting	Sterile zone
Default severity level	5
Remarks	The sterile zone is a quadrilateral zone that includes 3 red orders and 1 green border. The green border defines the allowed entry at the virtual perimeter into the zone. If the person enters the zone beyond the original entry point to approach the virtual perimeter, this event will be generated.
See also	Person Entered Restricted Zone , Person Trespassing , Object in Sterile Zone , Car in Sterile Zone
Availability	Active Alert Standard, Active Alert Premium

Person Started Running

This event is triggered when a person that is tracked in the scene is moving at a speed that is considered running. The default person running speed is set to 7 mph (11.2 Km/h).

	Description
Syntax	(person) started running
Object type	Person
Zone setting	Detection zone
Default severity level	7
Remarks	There is a <i>Maximum allowed speed (mph)</i> parameter that the user can specify for this event. The default speed threshold is 7 mph (11.2 Km/h). It is important to have a proper camera placement to detect this event. The camera placement for detecting a person running should also be a lateral view to allow the maximum person movement in the image. This will allow an optimal estimation of the speed of movement.
See also	Person Started Moving , Person Stopped Running
Availability	Active Alert Premium

Person Stopped Running

This event is triggered when a running person has resumed normal moving speed, and is considered stopped running.

	Description
Syntax	(person) stopped running
Object type	Person
Zone setting	Detection zone
Default severity level	3
Remarks	None
See also	Person Stopped , Person Stopped Running
Availability	Active Alert Premium

Person Running in the Wrong Direction

This event is triggered when a person that is tracked in the scene is running against the allowed direction. The default person running speed is set to 7 mph (11.2 Km/h).

	Description
Syntax	(person) running in the wrong direction
Object type	Person
Zone setting	Directional zone
Default severity level	5
Remarks	Similar to the Person Started Running event, there is a <i>Maximum allowed speed (mph)</i> parameter that the user can specify for this event. The default speed threshold is 7 mph (11.2 Km/h). Like all running events, it is important to have a proper camera placement in order to detect this event. The camera placement for detecting a person running should also be a lateral view to allow the maximum person movement in the image. This allows for an optimal estimation of the speed of movement.
See also	Person Started Running , Person Stopped Running
Availability	Active Alert Premium

Person on Fence Line

A person is on the fence line (that is, the fence zone).

	Description
Syntax	(person) on fence line
Object type	Person
Zone setting	Fence zone
Default severity level	4
Remarks	None
Availability	Active Alert Standard, Active Alert Premium

People Converged

Two people have merged for a period of time.

	Description
Syntax	(person 1) converged (person 2)
Object type	Person
Zone setting	No zone required
Default severity level	3
Remarks	This event is detected if Object Merged between two people is detected and the two people remain merged for a period of time.
See also	<i>Objects Merged</i> , <i>People Passed By</i>
Availability	Active Alert Standard, Active Alert Premium

People Passed By

A person has passed by (gone across) another person.

	Description
Syntax	(person 1) has passed by (person 2)
Object type	Person
Zone setting	No zone required
Default severity level	1

	Description
Remarks	This event is detected if Object Merged between two people is detected, and then quickly followed by Object Split between the same two people.
See also	Objects Merged , Objects Split , People Converged
Availability	Active Alert Standard, Active Alert Premium

Possible Theft

A possible shoplifting behavior where a shopper has grabbed too many items of merchandise within a short duration of time as defined by the user.

	Description
Syntax	possible theft
Object type	Person
Zone setting	Theft zone
Default severity level	6
Remarks	None
Availability	Active Alert Premium

Person Entered Target Zone

A person has entered a target zone. Used for evaluating customer interest in merchandising.

	Description
Syntax	(person) entered target (zone)
Object type	Person
Zone setting	Target zone
Default severity level	4
Remarks	None
See also	Person Staying in Target Zone
Availability	Smart Impressions

Person Staying in Target Zone

A person is staying inside the target zone. Used for evaluating customer interest in merchandising and dwell time estimation.

	Description
Syntax	(person) staying in target (zone)
Object type	Person
Zone setting	Target zone
Default severity level	3
Remarks	None
See also	Person Entered Target Zone
Availability	Smart Impressions

Traffic Events

Car Started Driving in the Wrong Direction

A car has started moving against the user-defined direction.

	Description
Syntax	(car) started moving in the wrong direction (zone)
Object type	Car
Zone setting	Directional zone
Default severity level	4
Remarks	None
See also	Car Started Driving in the Wrong Direction , Person Started Moving in the Wrong Direction , Person Stopped Moving in the Wrong Direction
Availability	Active Alert Base, Active Alert Standard, Active Alert Premium

Car Stopped Driving in the Wrong Direction

A car has stopped moving against the user-defined direction.

	Description
Syntax	(car) stopped moving in the wrong direction (zone)
Object type	Car
Zone setting	Directional zone
Default severity level	3
Remarks	None
See also	Car Started Driving in the Wrong Direction , Person Started Moving in the Wrong Direction , Person Stopped Moving in the Wrong Direction
Availability	Active Alert Base, Active Alert Standard, Active Alert Premium

Car Entered Restricted Area

A car has entered a restricted zone.

	Description
Syntax	(car) entered (zone)
Object type	Car
Zone setting	Restricted zone
Default severity level	4
Remarks	None
See also	Car Exited Restricted Area
Availability	Active Alert Base, Active Alert Standard, Active Alert Premium

Car Exited Restricted Area

A car has exited a restricted zone.

	Description
Syntax	(car) exited (zone)
Object type	Car
Zone setting	Restricted zone
Default severity level	3

	Description
Remarks	None
See also	Car Entered Restricted Area
Availability	Active Alert Base, Active Alert Standard, Active Alert Premium

Car Parked in Restricted Area

A car has parked in a restricted zone.

	Description
Syntax	(car) parked in restricted (zone)
Object type	Car
Zone setting	Restricted zone
Default severity level	5
Remarks	This event is detected if a car has entered a restricted zone (Car Entered Restricted Area has been detected), and then it stopped and parked in the zone; that is, stopped for a user-defined duration, such as 30 seconds. The maximum duration can be 1 minute (60 seconds).
See also	Car Entered Restricted Area
Availability	Active Alert Standard, Active Alert Premium

Car Trespassing

A car has trespassed the virtual perimeter.

	Description
Syntax	(car) trespassing (line)
Object type	Car
Zone setting	Trespass line
Default severity level	4
Remarks	The trespass line zone includes a line segment that defines the virtual perimeter, and an intersecting vector that defines the <i>allowed</i> moving direction passing the trespass line. A Car Trespassing event is detected when a car has trespassed this virtual perimeter by moving against the allowed direction.
See also	Object Trespassing , Person Trespassing , Car Trespassing , Car Started Driving in the Wrong Direction
Availability	Active Alert Base, Active Alert Standard, Active Alert Premium

Car in Sterile Zone

A car has entered the sterile zone and is moving towards the virtual perimeter.

	Description
Syntax	(car) in (sterile zone)
Object type	Car
Zone setting	Sterile zone
Default severity level	5
Remarks	The sterile zone is a quadrilateral zone that includes 3 red borders and 1 green border. The green border defines the allowed entry at the virtual perimeter into the zone. If the car enters the zone through any of the red borders and moves beyond the original entry point to approach the virtual perimeter, this event will be generated.
See also	Car Entered Restricted Area , Car Trespassing , Object in Sterile Zone , Person in Sterile Zone
Availability	Active Alert Standard, Active Alert Premium

Car Made an Illegal U-Turn

A car has made an illegal U-turn.

	Description
Syntax	(car) made illegal U-Turn (zone)
Object type	Car
Default severity level	5
Zone setting	U-turn zone
Remarks	None
Availability	Active Alert Standard, Active Alert Premium

Car Parked in Handicapped Zone

A car has parked in a handicapped parking zone.

	Description
Syntax	(car) parked in handicapped (zone)
Object type	Car
Zone setting	Handicapped zone

Description	
Default severity level	5
Remarks	This event is detected if a car has entered a handicapped zone, and then it stopped and parked in the zone; that is, stopped for a user-defined duration, such as 30 seconds. The maximum duration can be 1 minute (60 seconds).
Availability	Active Alert Standard, Active Alert Premium

Car Pulled Off the Road

A car has pulled off the road onto a shoulder zone.

Description	
Syntax	(car) pulled off the road (zone)
Object type	Car
Zone setting	Shoulder zone
Default severity level	4
Remarks	None
Availability	Active Alert Standard, Active Alert Premium

Car Needs Assistance

A car has stopped in the shoulder zone and needs assistance.

Description	
Syntax	(car) needs assistance (zone)
Object type	Car
Zone setting	Shoulder zone
Default severity level	5
Remarks	This event is detected if a car has entered a shoulder zone, and then it stopped and parked in the zone; that is, stopped for a user-defined duration, such as 30 seconds. The maximum duration can be 1 minute (60 seconds).
Availability	Active Alert Standard, Active Alert Premium

Car Speeding

This event is triggered when the speed of a moving vehicle has exceeded a specified speed limit. The speed estimate is an average over a brief time window.

	Description
Syntax	car speeding
Object type	Car
Zone setting	Detection zone
Default severity level	4
Remarks	There is a <i>Maximum allowed speed (mph)</i> that the user can specify for this event. It is important to place the camera correctly in order to detect this event. The camera placement should be a lateral view to allow the maximum vehicle movement in the image. This allows an optimal estimation on the vehicle speed. For example, the best camera placement will see vehicles in the detection zone travel mostly horizontally (from left side of the camera to the right or vice versa), rather than vertically (head-on towards the camera or heading away from the camera).
See also	Person Started Running
Availability	Active Alert Premium

Counting Events

Person Counted as Entering

Line-Based: A person has been counted as entering, after crossing the counting line from one side to the other, following the direction of the arrow.

Zone-Based: A person has been counted as entering, after moving from a group of outside zones to a group of inside zones.

	Description
Syntax	(person) counted as entering (line) (person) counted as entering from (outside zone) to (inside zone)
Object type	Person
Zone setting	Line-Based: Zone 1: Counting line Zone-Based: Zone 1: outside zones (that is, all outside zones defined in camera view) Zone 2: inside zones (that is, all inside zones defined in camera view)
Default severity level	2
Remarks	This is a people counting event. All counting events are optimized when the camera is mounted overhead. For line-based setup, a single counting line is required. The event is triggered when a person goes across the line from one side to the other along the direction specified by the arrow. For zone-based setup (legacy only), one or more outside zones and one or more inside zones may be used. The event is triggered when a person moves from any outside zone to any inside zone.
See also	Person Counted as Exiting , Car Entered Lot , Car Exited Lot
Availability	Active Alert Standard, Active Alert Premium, People Counting Smart Impressions

Person Counted as Exiting

Line-Based: A person has been counted as exiting, after crossing the counting line from one side to the other, against the direction of the arrow.

Zone-Based: A person has been counted as exiting, after moving from a group of inside zones to a group of outside zones.

	Description
Syntax	(person) counted as exiting (line) (person) counted as exiting from inside zone) to (outside zone)
Object type	Person
Zone setting	Line-Based: Zone 1: Counting line Zone-Based: Zone 1: inside zones (that is, all inside zones defined in camera view) Zone 2: outside zones (that is, all outside zones defined in camera view)
Default severity level	2
Remarks	This is a people counting event. All counting events are optimized when the camera is mounted overhead. For line-based setup, a single counting line is required. The event is triggered when a person goes across the line from one side to the other against the direction specified by the arrow. For zone-based setup (legacy only), one or more inside zones and one or more outside zones may be used. The event is triggered when a person moves from any inside zone to any outside zone.
See also	Person Counted as Entering , Car Entered Lot , Car Exited Lot
Availability	Active Alert Standard, Active Alert Premium, People Counting, Smart Impressions

Car Entered Lot

A car entered a parking lot.

	Description
Syntax	(car) entered lot from (outside zone) to (inside zone)
Object type	Car
Zone setting	Zone 1: counting zone outside of the lot Zone 2: counting zone inside the lot
Default severity level	2

	Description
Remarks	<p>This event is reported when a car moves into a parking lot. It is defined by linking a pair of counting zones; zone 1 is on the outside of the lot (for example, before the entrance gate), and zone 2 is inside the lot (for example, after the entrance gate).</p> <p>The car has to move from zone 1 to zone 2 to be counted. For example, a car driving past the entrance gate without entering the lot may pass through zone 1, but will not pass through zone 2. Consequently, no event will be triggered in this example.</p>
See also	Car Exited Lot
Availability	Active Alert Standard, Active Alert Premium, Smart Impressions

Car Exited Lot

Car exited a parking lot.

	Description
Syntax	(car) exited lot from (inside zone) to (outside zone)
Object type	Car
Zone setting	Zone 1: counting zone inside the lot Zone 2: counting zone outside of the lot
Default severity level	2
Remarks	<p>This event is reported when a car moves from a parking lot. It is defined by linking a pair of counting zones: zone 1 is inside the lot (for example, before the exit gate), zone 2 is outside of the lot (for example, after the exit gate).</p>
See also	Car Entered Lot
Availability	Active Alert Standard, Active Alert Premium, Smart Impressions

Car Counted in Lane

Car counted in a specific lane on a highway.

	Description
Syntax	(car) counted in lane (zone)
Object type	Car
Zone setting	Car lane counter

	Description
Default severity level	2
Remarks	<p>Because this is a counting event, the camera should be placed in the overhead view for optimal performance. This event allows the user to count vehicles in an individual traffic lane. In a typical scenario, one zone per lane is set up, so that both per-lane and overall traffic can be measured.</p> <p>Any vehicle that passes through the zone is counted and reported.</p>
Availability	Active Alert Premium, Smart Impressions

Video Events

Video Lost

This event is triggered when the video is lost.

	Description
Syntax	video lost
Object type	None
Zone setting	None
Default severity level	4
Remarks	<p>This event detects that the video signal is lost, most likely due to a bad connection. For IP video, sometimes a black frame may be transmitted when the video is lost. In such case, the detection of this event depends on the API from the IP video vendor.</p>
See also	Video Restored
Availability	Active Alert Base, Active Alert Standard, Active Alert Premium, People Counting, Smart Impressions

Video Restored

This event is triggered when the video is restored from a video loss.

Description	
Syntax	video restored
Object type	None
Zone setting	None
Default severity level	3
Remarks	This event detects that the video signal has come back after a video loss. Similar to the Video Lost detection, the detection of such event for IP video depends on the API from the IP video vendor.
See also	Video Lost
Availability	Active Alert Base, Active Alert Standard, Active Alert Premium, People Counting, Smart Impressions

Zone Library

This release of Honeywell Video Analytics software offers 16 types of zones across all product packages. Among them, the **exclusion** zone and **object-block** zone allow you to manage to completely exclude or perform special filtering on specific areas in the camera view. The other zone types are associated to specific events. Once added, you can enable the corresponding events.

This appendix contains a list of all the zones available in this release with a description of how they link to specific events, if any. For examples of using various types of zones, please see [Zone Definition](#), page 63. For detailed description on any specific event, please see [Appendix A](#).

The zones are listed in the following order, in two categories:

Managing Information Reporting

- Exclusion
- Object Block

Enabling or Associated with Specific Events

- Restricted
- Direction
- Trespass
- Fence
- Sterile
- Counting line
- Inside
- Outside
- Car Lane Counter
- Detection
- Asset
- U-turn
- Handicapped
- Shoulder
- Theft
- Target

Zones for Managing Information

Exclusion Zone

The **exclusion** zone is used to mask out or completely exclude an area in the image from being processed. The image within an exclusion zone is entirely ignored and therefore no objects or events are detected in the exclusion zone.

	Description
Enabled events	None
Remarks	Please see page 37 for detailed information on when to use an exclusion zone.
See also	Object-Block Zone
Availability	Active Alert Base, Active Alert Standard, Active Alert Premium, People Counting, Smart Impressions

Object-Block Zone

The **object-block** zone is used to mark certain areas in the camera view where false moving objects are expected to appear. Special filtering are performed within an object-block zone to ignore false objects whose movement is confined within the zone. Please see [page 107](#) for an example of the object-block zone.

	Description
Enabled events	None
Remarks	Typical usage of an object-block zone includes areas covered by moving trees, reflective surfaces, sliding or moving doors. Please see Managing Environmental Conditions , page 37 for more details.
See also	Exclusion Zone
Availability	Active Alert Base, Active Alert Standard, Active Alert Premium, People Counting, Smart Impressions

Zones for Enabling Specific Events

Restricted Zone

The **restricted** zone is used to mark areas with restricted entry. It is a quadrilateral with four moveable anchor points.

	Description
Enabled or associated events	<p>This zone enables the following two events. It is required for use of these events.</p> <ul style="list-style-type: none"> Object/Person/Car entered restricted zone (default severity = 4) Object/Person/Car exited restricted zone (default severity = 3) Car parked in restricted zone (default severity level = 5) Person loitering in restricted zone (default severity level = 5)
Default events when zone is added	Object entered restricted zone
Remarks	None
See also	Trespass Line
Availability	Active Alert Base, Active Alert Standard, Active Alert Premium

Direction Zone

The **direction** zone is used to specify the allowed traffic direction. Movement against the allowed direction is detected. It is a quadrilateral with two arrowed edges at opposite sides, defining the allowed traffic direction.

	Description
Enabled or associated events	<p>This zone enables the following two events. It is required for use of these events.</p> <ul style="list-style-type: none"> Object/Person/Car started moving in the wrong direction (default severity = 4) Object/Person/Car stopped moving in the wrong direction (default severity = 3) Person started running in the wrong direction (default severity = 5)
Default events when zone is added	Object started moving in the wrong direction
Remarks	None
Availability	Active Alert Base, Active Alert Standard, Active Alert Premium

Trespass Line

The **trespass line** is used to detect a breach through a perimeter. It is directional, with an arrow indicating the allowed direction. A breach from the opposite direction is detected. It is often used at a fence area or perimeters along a critical facility.

	Description
Enabled or associated events	This zone enables the following events. It is required for use of these events. <ul style="list-style-type: none"> Object trespassing line (default severity = 5) Person trespassing line (default severity = 5) Car trespassing line (default severity = 5)
Default events when zone is added	Object started moving in the wrong direction
Remarks	If passing the perimeter from either direction is disallowed, two back-to-back trespassing lines can be used.
See also	Restricted Zone
Availability	Active Alert Base, Active Alert Standard, Active Alert Premium

Fence Zone

The **fence** zone is used to mark the fence area along the perimeter. It differs from the trespass line zone in that it is non-directional. A person approaching the fence zone from any direction will be detected.

	Description
Enabled or associated events	This zone enables the following events: <ul style="list-style-type: none"> Object in sterile zone (default severity = 5) Person in sterile zone (default severity = 5) Car in sterile zone (default severity = 5)
Default events when zone is added	Object in sterile zone
Remarks	None
Availability	Active Alert Standard, Active Alert Premium

Sterile Zone

The **sterile** zone is used to protect a virtual perimeter by detecting any object that enters from disallowed entry point and approaches the virtual perimeter.

	Description
Enabled or associated events	The sterile zone enables the following events. <ul style="list-style-type: none"> Object in sterile zone (default severity = 5) Person in sterile zone (default severity = 5) Car in sterile zone (default severity = 5)
Default events when zone is added	Object in sterile zone
Remarks	The sterile zone is a quadrilateral zone that has 3 red borders (including a pair of directional edges), and 1 green border. The green border defines the allowed entry point into the zone and it is usually drawn along the virtual perimeter line. The red arrows specify the disallowed direction of movement towards the virtual perimeter inside the zone. Upon entry into the zone through a red border, if the object moves beyond the original entry point and gets closer to the virtual perimeter, an alarm will trigger.
See also	Restricted Zone , Trespass Line
Availability	Active Alert Standard, Active Alert Premium

Counting Line

The counting line is used for people counting. The line is a multi-segment line with user-defined joints to partition the space into interior and exterior.

	Description
Enabled or associated events	The counting line enables the following events. <ul style="list-style-type: none"> Person counted as entering (line) (default severity = 2) Person counting as exiting (line) (default severity = 2)
Default events when zone is added	Person counted as entering (line) Person counted as exiting (line)
Remarks	This zone replaces inside and outside zones for people counting.
See also	Inside and Outside Zones
Availability	Active Alert Standard, Active Alert Premium, People Counting, Smart Impressions

Inside and Outside Zones

The **inside** and **outside** zones form two paired groups of zones. They are used to enable events related to counting cars. It is critical that the inside zone group cannot overlap with the outside zone group. Both types need to exist to enable the associated events.

	Description
Enabled or associated events	<p>The inside and outside zone pair enables the following events. Both types are required for use of these events.</p> <ul style="list-style-type: none"> Car entered lot (default severity = 2) Car exited lot (default severity = 2) <p>Legacy configuration (HVA V4.7 and earlier) only:</p> <ul style="list-style-type: none"> Person counted as entering (zone) (default severity = 2) Person counted as exiting (zone) (default severity = 2)
Default events when zone is added	None; you must add these events after adding the inside and outside zones.
Remarks	None
See also	Car Lane Counter
Availability	Active Alert Standard, Active Alert Premium, People Counting, Smart Impressions

Car Lane Counter

The **car lane counter** is used to count traffic passing through individual lanes on the highway. Multiple car lane counters can be used for a multi-lane highway, one counter per lane.

	Description
Enabled or associated events	<p>This zone enables the following event. It is required for use of this event.</p> <p>Car counted in lane (default severity = 2)</p>
Default events when zone is added	Car counted in lane
Remarks	None
See also	Inside and Outside Zones
Availability	Active Alert Premium, Smart Impressions

Detection Zone

The **detection** zone can be used to mark the effective area for detecting events like person running or vehicle speeding. When used, such events are only detected if they occur within the detection zone.

	Description
Enabled or associated events	<p>This zone enables the following events. It is required to enable these events.</p> <ul style="list-style-type: none"> Person started running (default severity = 3) Person stopped running (default severity = 3) Car speeding (default severity = 4) Object left unattended (default severity = 7)
Default events when zone is added	None. The user must add the event after adding the detection zone.
Remarks	None
See also	Car Lane Counter
Availability	Active Alert Premium

Asset Zone

The **asset** zone can be used to mark the asset to be protected from being removed from the scene. It is used to detect and object removed event.

	Description
Enabled or associated events	<p>This zone is associated to the following event. It is required to enable this event.</p> <p>Object removed (default severity = 7)</p>
Default events when zone is added	Object removed
Remarks	None
Availability	Active Alert Premium

U-turn Zone

The **U-turn** zone is used to mark the section of the road where illegal U-turns are prohibited. Cars making a U-turn within this zone will be detected. The arrowed green section marks the normal traffic direction, while the red section marks the illegal turn along the opposite traffic direction.

	Description
Enabled or associated events	This zone enables the following event. It is required for use of this event. Car made illegal U-turn (default severity = 5)
Default events when zone is added	Car made illegal U-turn
Remarks	None
See also	Direction Zone
Availability	Active Alert Standard, Active Alert Premium

Handicapped Zone

The **handicapped** zone is used to mark the handicapped parking area. A car parked in this zone will be detected.

	Description
Enabled or associated events	This zone enables the following event. It is required for use of these events. Car parked in handicapped zone (default severity = 5)
Default events when zone is added	Car parked in handicapped zone
Remarks	None
Availability	Active Alert Standard, Active Alert Premium

Shoulder Zone

The **shoulder** zone is used to mark the shoulder area or the median area on the highway. Vehicles moving in the shoulder zone or stopped in the shoulder zone for a user-specified amount of time will be detected.

	Description
Enabled or associated events	This zone enables the following events. It is required for use of these events. <ul style="list-style-type: none"> Car pulled off road (default severity = 4) Car needs assistance (default severity = 4)
Default events when zone is added	<ul style="list-style-type: none"> Car pulled off road Car needs assistance
Remarks	None
Availability	Active Alert Standard, Active Alert Premium

Theft Zone

The **theft** zone (or theft line) is used to mark the shelf line for detecting the possible theft event. It includes a line segment to mark the stretch of the shelf, and an arrow to point towards the inside of the shelf to indicate how far the arm may reach in.

	Description
Enabled or associated events	This zone is associated to the following event. It is required to enable this event. Possible theft (default severity = 6)
Default events when zone is added	Possible theft
Remarks	None
Availability	Active Alert Premium

Target Zone

The **target** zone is used to mark the asset to be protected from being removed from the scene. It is used to detect the object removed event.

	Description
Enabled or associated events	This zone is associated to the following events. It is required to enable these events. <ul style="list-style-type: none">• Person entered target zone (default severity = 4)• Person staying in target zone (default severity = 3)
Default events when zone is added	<ul style="list-style-type: none">• Person entered target zone• Person staying in target zone
Remarks	None
Availability	Smart Impressions

Active Alert Performance Counter

This version of Honeywell Video Analytics software includes custom Active Alert performance counter objects that can be used to monitor the proper operation of the Video Analytics software. These custom performance counter objects are built on Windows performance counter classes, which can be monitored using Windows Performance Monitor (*PerfMon.exe*) as well as using SNMP (Simple Network Management Protocol) to provide IT administrators with quantitative data to ensure the proper operation of the Honeywell Video Analytics software. For example, all configured channels are being processed and the processing frame rates for all channels meet the requirement of the system. It also allows easy integration with third party network and system monitoring tools (for example, Nagios).

The delivery of counter values relies on the HVA Performance Counter Client service to be running on your system. When you install the Honeywell Video Analytics full package, this service is automatically installed and running on your system.

There are two custom performance objects that collect data from the Honeywell Video Analytics software:

- **ActiveAlert-Analytics.** Provides the current processing frame rate for all the channels that are being processed as well as whether there is video lost on any of these channels. There are two counters for this counter object:
 - **Processing Frame Rate.** Currently processing frame rate for the channel
 - **Lost Video.** If the video signal on the channel is lost (1 if lost video; 0 if not)Each counter contains multiple instances, which map to the channel IDs of individual channels that are currently being processed by the video analytics server service. There is also a system instance that shows the lowest processing frame rate across all channels, or the total number of lost videos across all channels.
- **ActiveAlert-System.** Provides counters related to the video analytics server service as a whole on the analytics server, including:
 - **Number of Processing Channels.** Total number of channels currently being processed by the analytics server.
 - **Number of Configured Channels.** Total number of channels that are configured on the analytics server .

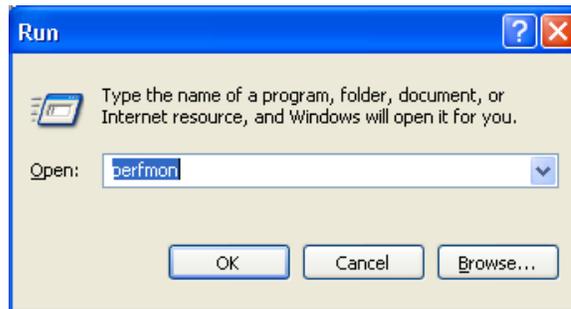
Note This includes enabled channels with incomplete configuration that are not currently being processed)
- **Keep Alive.** Rotating values from 0 to 65535.

The Keep Alive counter is designed for diagnostic purposes to ensure that both the Video Analytics Service and the HVA Performance Counter Client Service are working properly. When they are, the Keep Alive counter should keep incrementing its value every second or so. When it reaches its maximum value 65535, it resets back to 0 and starts over.

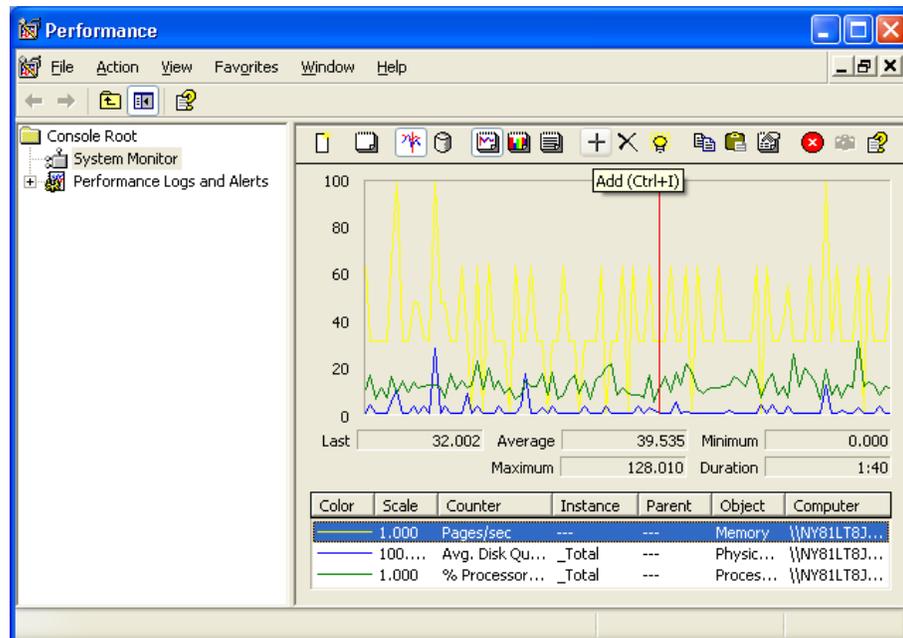
Using PerfMon to View Active Alert Performance Counters

To use the Windows performance monitoring tool (*Perfmon.exe*) to view Active Alert Performance Counters.

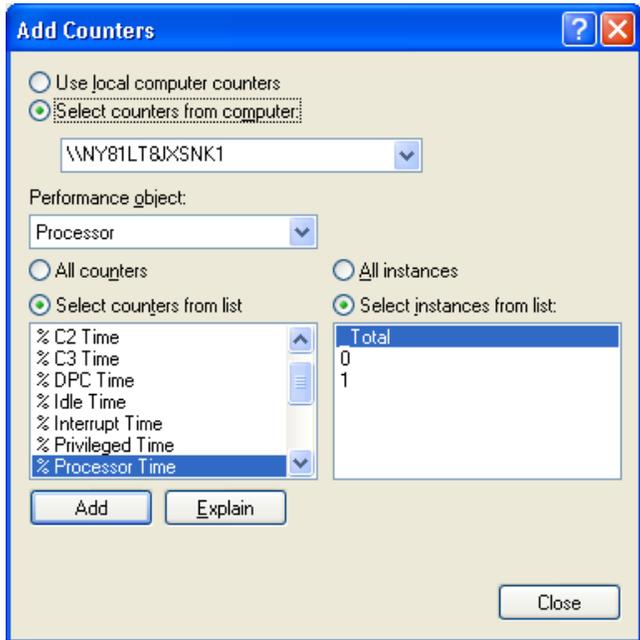
1. Start Windows Performance Monitor
 - a. Select **Start » Run**.
 - b. In the **Open** field, enter **perfmon**.
 - c. Click **OK**.



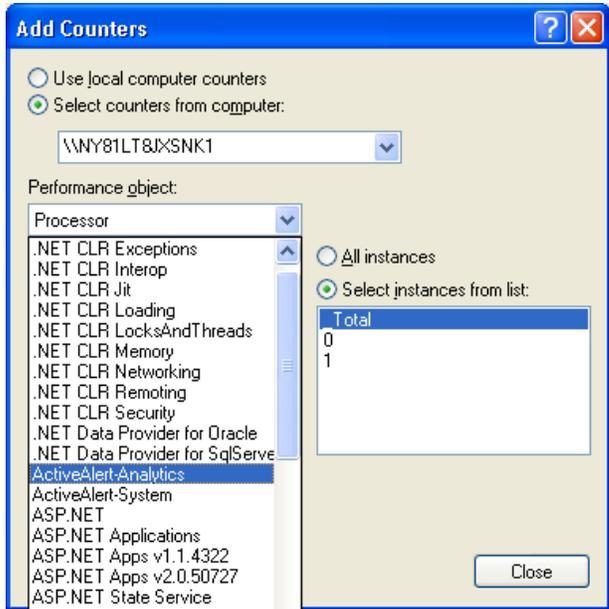
2. The Performance dialog opens.

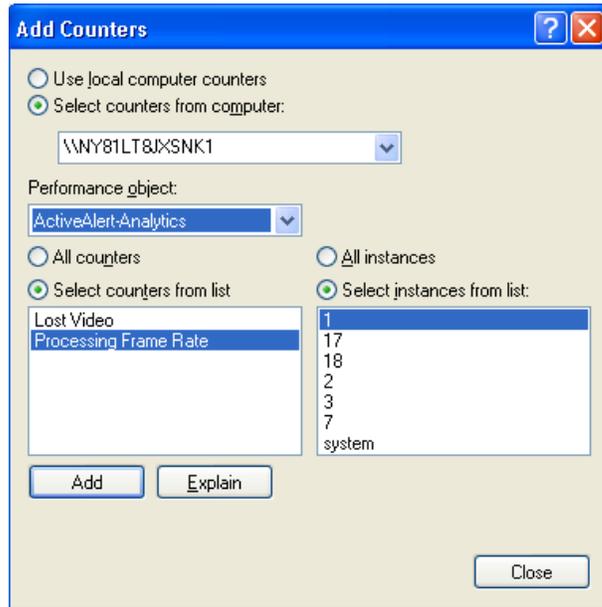


Click  on the tool bar to open the Add Counters dialog.

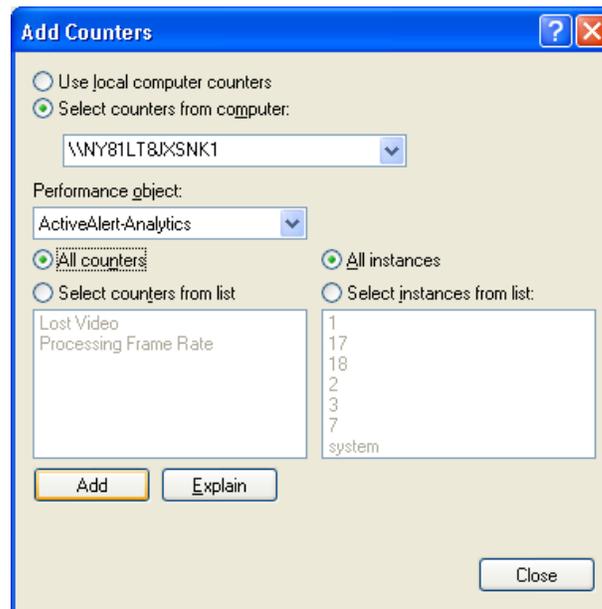


- Expand the **Performance object** drop-down list, and select **ActiveAlert-Analytics** from the list.

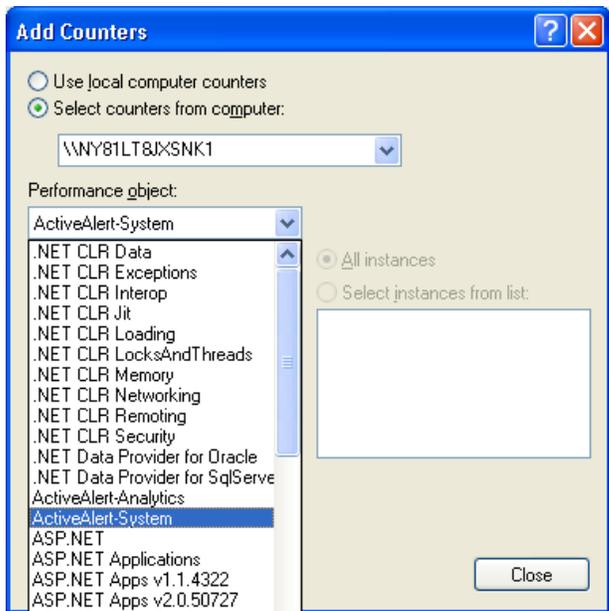




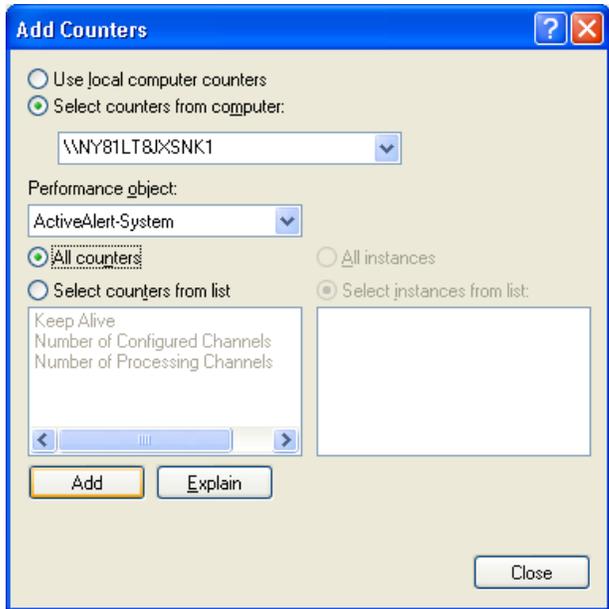
4. For the ActiveAlert-Analytics performance object, select **All counters** and **All instances**. Then click **Add** to add all of them to the counter list.



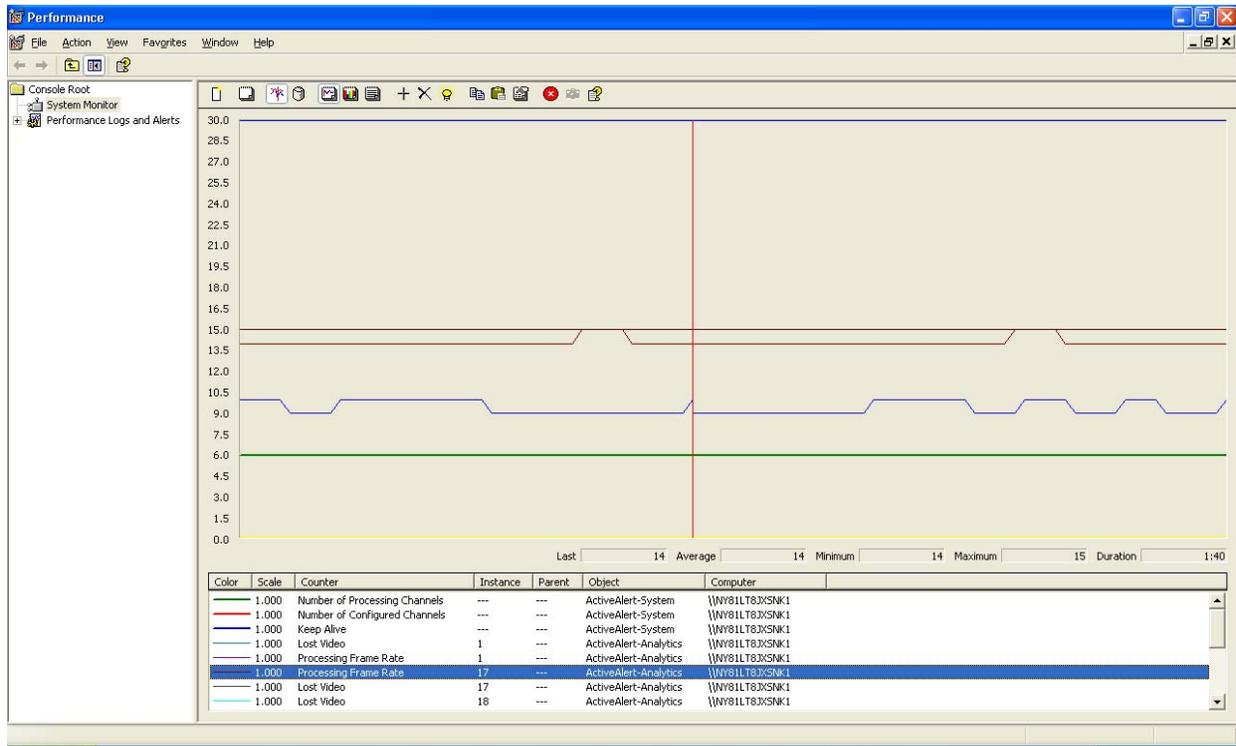
- Again, expand the **Performance object** drop-down list, and this time select **ActiveAlert-System** from the list.



- For the ActiveAlert-Analytics performance object, select **All counters** and **All instances**. Then click **Add** to add all of them to the counter list.



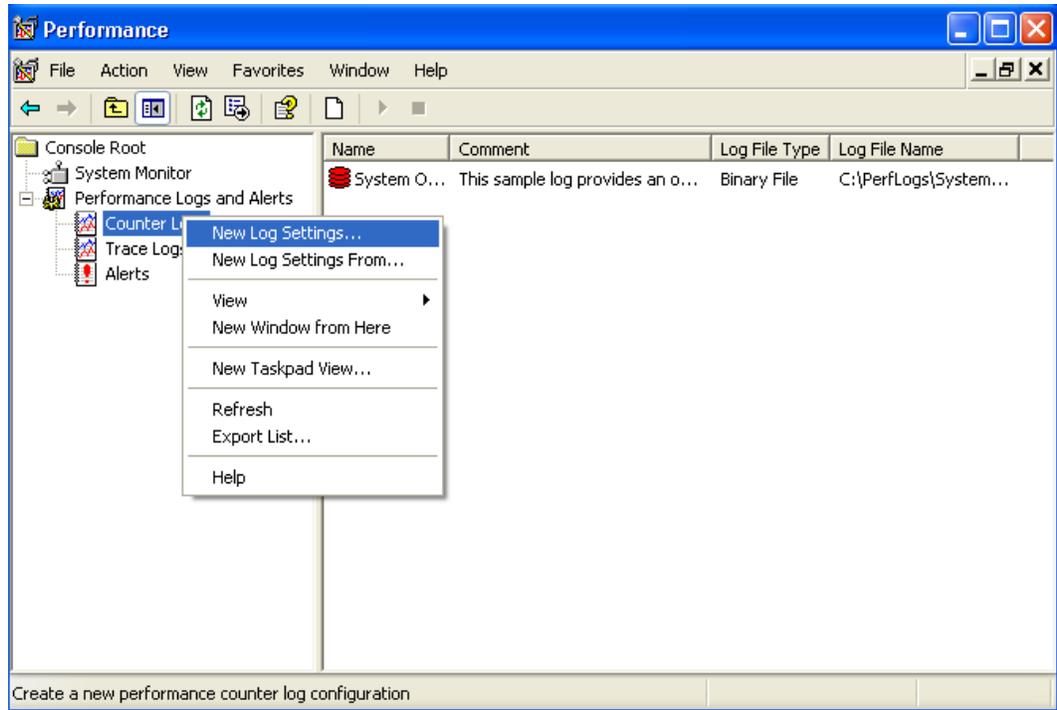
- Click **Close** to close the Add Counters dialog. A list of ActiveAlert custom counters are listed at the bottom of the Performance tab. You can select any of the counters in the list and see its last value, average value, minimum and maximum over a short duration.



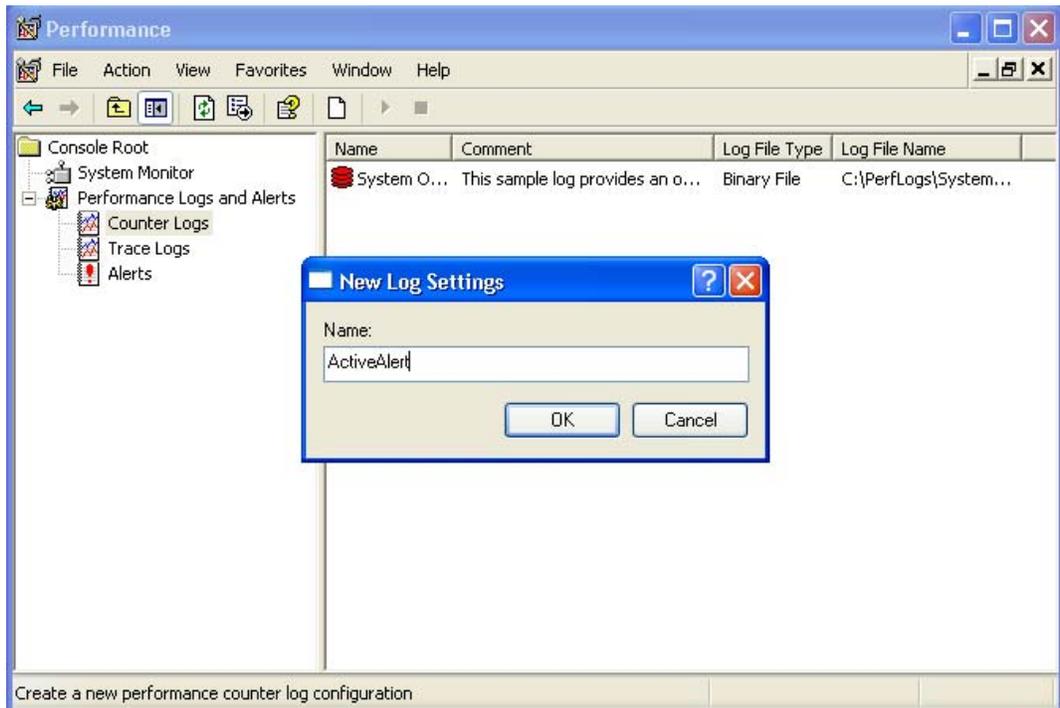
Generating Performance Counter Logs

To generate performance counter logs using the Windows Performance tool:

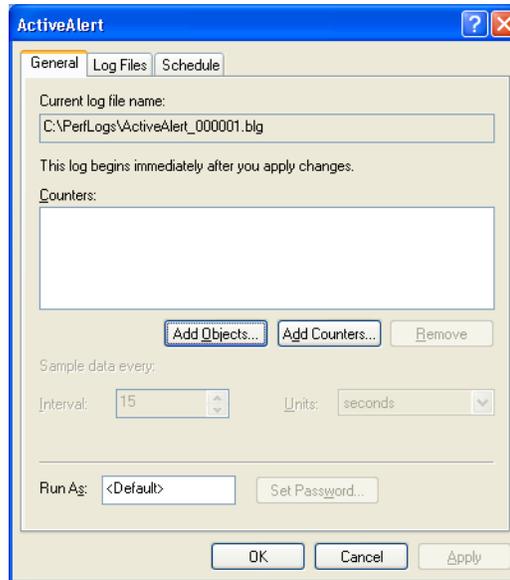
1. On the left pane in the Performance dialog, click **Performance Logs and Alerts**. Right-click **Counter Logs**, then select **New Log Settings...**



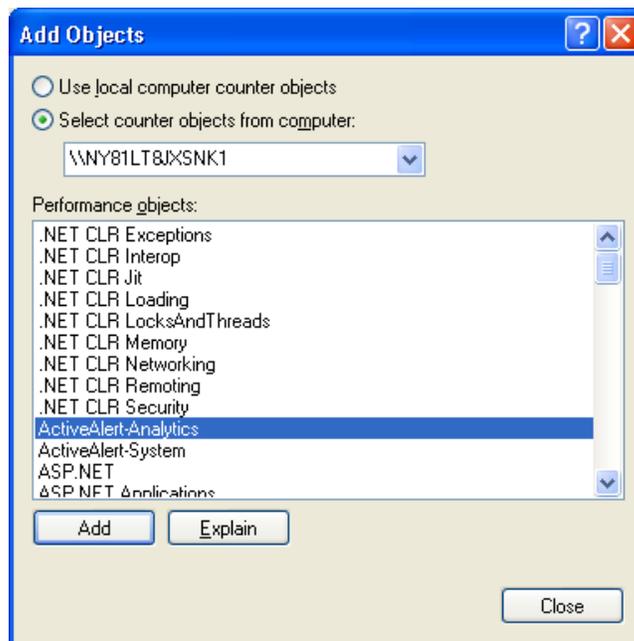
2. The **New Log Settings** dialog opens. Enter a name for this new log (for example, ActiveAlert), then click **OK**.



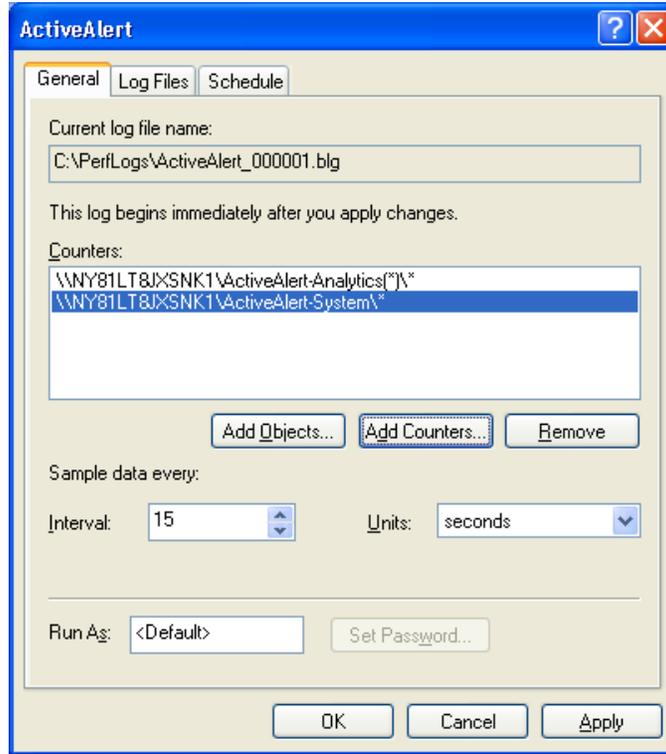
3. Now you can add performance objects or specific counters to the ActiveAlert counter logs. Click **Add Objects...** to select performance objects to add to the log.



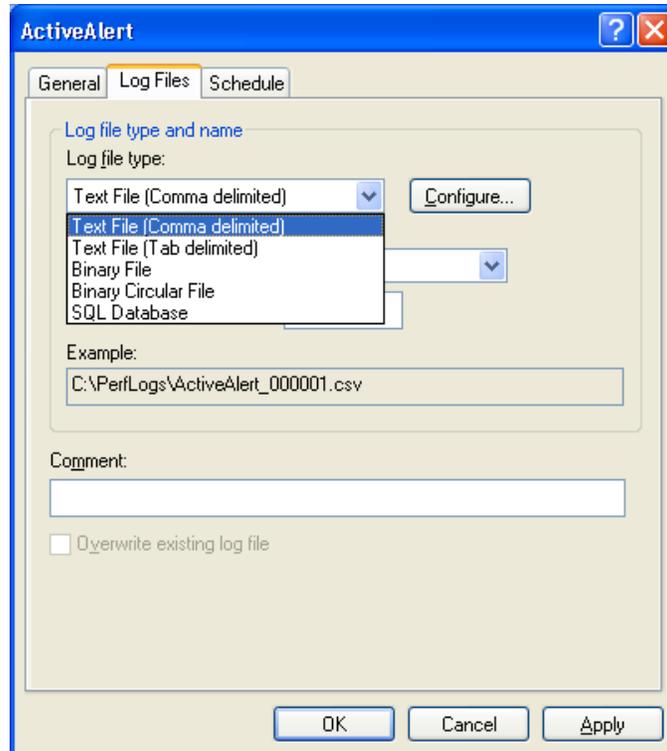
4. In the **Performance objects** list:
 - a. Select **ActiveAlert-Analytics**, then click **Add**.
 - b. Select **ActiveAlert-System** from the list, then click **Add**.
 - c. Click **Close** when you finish adding performance objects for this log.



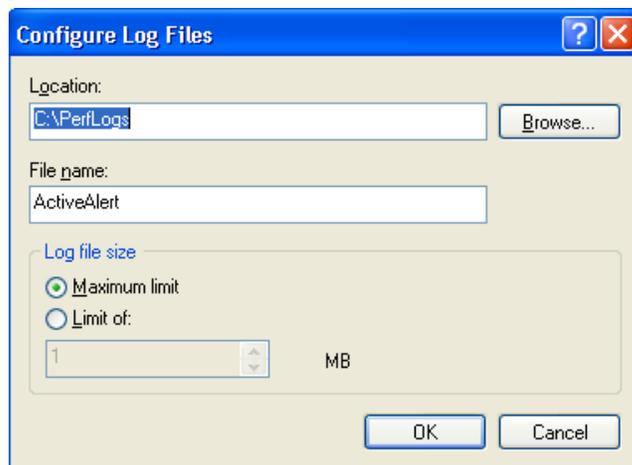
- Both performance objects and all counters from these objects have been added to the list for the logging. Adjust the data sample rate as needed.



- Click the **Log Files** tab. Select the Log file type to the format you want [for example, Text File (Comma delimited)] which allows you to open the log file using Microsoft Excel. Then click **Configure** to configure the log files.



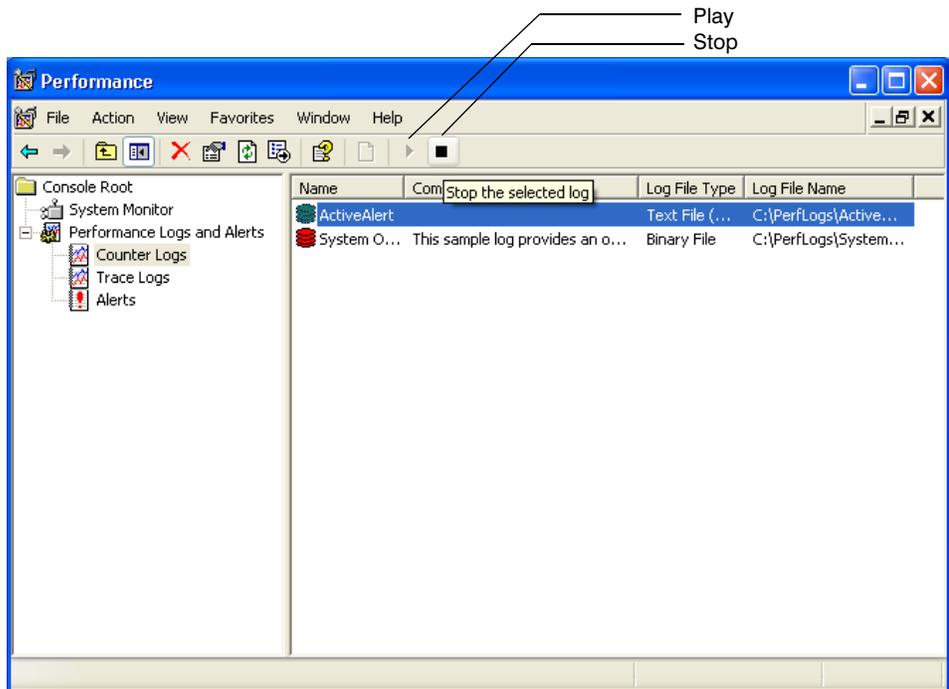
- Here you can select the location where the log file will be saved (for example, C:\PerfLogs). If the folder does not exist, you are prompted to create the folder. Set a maximum size for the log file if needed. When you are finished, click **OK**.



- Click the **Schedule** tab. You can configure the log to be generated automatically on schedule, or start and stop manually inside the Performance tool. Click **OK** when you finalize the schedule.



- To manually start and stop the log, click the play and stop buttons respectively on the Performance dialog.



You can find more information on the Windows Performance Monitor on the internet. For example, Microsoft TechNet can be found at <http://technet.microsoft.com/en-us/library/cc749249.aspx>.

D

Solutions

This appendix provides answers for common technical issues. If the message you see is not listed in these tables, please make a note of the error message and then contact Honeywell Technical Support (see [Technical Support](#), page 330).

License Messages

Table D-1 License Message

Message	Problem	Solution
Expired or mismatched license dongle on the server. Please contact technical support.	The license dongle has expired or it does not have a matching product code.	Contact Technical Support to either renew the license or correct the product code in the license dongle. Both can be done remotely.
The license for product <product package> expires in <number> day(s).	The license for the product package will expire in the specified number of days.	Contact Technical Support to renew the license or correct the product code in the license key. Both can be done remotely.
The license for product <product package> has expired. Processing for channel <ID> (<product package>) will halt.	The license for the product package has expired. The processing for the channels assigned to this product package will stop.	Contact Technical Support to renew the license or correct the product code in the license key. Both can be done remotely.
The licensed number of channels for product <product package> is already in use. You must disable some other channel in order to enable the selected channel.	All available licenses for the product package have been used.	Disable some other channel that is currently using this product package before enable the selected channel for this product package.
Not enough licenses for product <product package>. Please adjust product assignments.	This may happen when you enter a new license key that has fewer licensed channels of a specific product from before.	Reassign the product package to no more than the licensed number of channels.
No license string found	The license string is empty.	Make sure the correct license key string is sent to the server.
Software license not valid.	The license key is invalid for this server.	Contact Technical Support to acquire the correct license string for your system. You will need the server ID for your system.
Software license key expired	The license key has expired.	Contact Technical Support to renew the license or correct the product code in the license key. Both can be done remotely.

Video Setup Messages

Table D-2 Video Setup Messages

Message	Problem	Solution
Please select at least one camera input. Please enable at least one video input.	All inputs were set to OFF.	At least one valid camera must be selected before a camera configuration can be submitted.
Channel ID <ID> already used. Please select a unique ID.	The channel ID is already used by some other channel.	Change the channel ID to some other number which is not being used.
No image available for camera <ID>	There is no image for this camera.	Check that there is live video connected to the frame grabber (for analog video) or the source of the network video is available (for an IP camera or video from a Fusion DVR).
Please input username and password to access the network camera.	When connecting to certain network camera models, you need to provide a user name and password to gain access to the video stream.	Input user name and password for the specified network camera.
Bad request: No image available for camera N. Unable to initialize video input. Unable to capture input frame.	The server was not able to capture a live image from the specified camera.	For analog camera inputs, verify the video cable connections and check that the video signal from the camera is available on the specified input. For IP network cameras, verify the specified IP address, port and other settings.
	A camera was selected for multiple inputs.	This is not possible with the software: the same camera cannot provide video to multiple inputs. Please adjust the settings so that each camera is selected at most once.
At most 6 cameras from <Fusion DVR> can be enabled. Please adjust camera selections.	More than 6 cameras from the selected Fusion DVR have been enabled for analytics. This exceeds the limit.	Disable some cameras from the Fusion DVR to meet the 6-camera limit.

Camera Group and Calibration Messages

Table D-3 Camera Group and Calibration Messages

Message	Problem	Solution
Please specify at least one camera	There is no camera assigned to the camera group.	Add at least one camera to the camera group.
Up to 16 point pairs are allowed. Please save mapping and send to server.	For each pair of cameras to be calibrated, a maximum of 16 calibration points are allowed.	You can only delete existing calibration point before adding new ones, as the maximum number of allowed calibration point pairs is reached. Make sure you save the mapping and send the calibration data to the server when you finish.

Configuration and Network Messages

Table D-4 Configuration and Network Messages

Message	Problem	Solution
Failed to connect to http server <server name>: <port>.	The application was unable to connect to the Video Analytics service running on the specified server.	Verify that the network connection to the server is available. Verify that the Video Analytics service is running on the server.
Unauthorized: Authorization required.	The Video Analytics server did not accept the provided user name or password.	Double check the user name and password to ensure they are correct. Also verify that the user has configuration privileges on the server.
Unable to save configuration file	Saving of a configuration file on the client computer has failed.	There was an error saving a configuration file locally. Verify that the disk is not full and that the user has permissions to create files in the specified directory.
Configuration not loaded - please first connect to a server.		

Table D-4 Configuration and Network Messages

Message	Problem	Solution
	The application wasn't connected to any server when a configuration file is being opened.	Verify that the network connection to the server is available. Verify that the Video Analytics service is running on the server. Reload the configuration file again.
Input file is not found or not readable. Please correct the filename.		
	Loading of a file on the client computer has failed. There was an error loading a configuration file or video file locally.	Verify that the file exists and that the user has permissions to read that file.
Configuration file has been altered and cannot be loaded. Please re-configure all channels.		
	The configuration file was altered without using the Configuration Tool and therefore is no longer valid.	Re-configure all channels.
Error in reading configuration file <file name>. Invalid zone and/or event found and discarded. Invalid calibration data found and discarded. Failed to remove invalid events from configuration.		
	Error found in the configuration file.	Check the current configuration. Save the configuration file using the Save or Save As command in the File menu.
Invalid configuration received from server. Invalid database properties received from server. Invalid supported zones received from server. Invalid supported events received from server. Internal error: Invalid command for control.xml: code = <error code>.		
	There was an error in the configuration received from the server.	Check the current configuration and verify that the network connection to the server is available. Re-send the configuration to the server. If the problem persists, please contact technical support for further assistance.
Unable to save configuration file.		
	Saving of a configuration file on the client computer has failed. There was an error saving a configuration file locally.	Verify that the disk is not full and that the user has permissions to create files in the specified directory.
Operation failed: out of memory.		
	The system is running out of memory.	Close other applications to provide more memory. If this is not possible or does not resolve the issue, the client computer may have to be rebooted.
Connection to server failed. Failed to request information from server. Failed to request configuration from server. Failed to send configuration to server. Failed to send license key to server.		

Table D-4 Configuration and Network Messages

Message	Problem	Solution
	There was an error in communication with the server.	<p>The most likely cause of these errors is a network connectivity problem. Verify that the network connection to the server is available. Verify that firewall settings do not prevent communication with the server.</p> <p>If the network settings are correct and the problem persists, please contact Technical Support for further assistance (see page 317).</p>
Configuration has been changed on server <server IP address>. Unable to auto-refresh settings because you have made changes that haven't been sent to the server yet.	The configuration has been modified locally, but has not been sent to the server. However, the configuration on the server has been modified by another user since the last time auto-refresh.	Send the configuration to the server. If the modification is done at a different section, the server will merge the modification into the configuration. If not, a conflict will occur. In such case, the user can (!) either abandon his local modification, or (2) save the configuration to a file, and then open and upload the configuration to the server to overwrite the existing configuration.
You have made configuration changes that haven't been sent to the server yet. Refreshing the configuration from the server will discard your changes.	The configuration has been modified locally, but has not been sent to the server. However, the configuration on the server has been modified by another user since the last time auto-refresh.	Send the configuration to the server. If the modification is done at a different section, the server will merge the modification into the configuration. If not, a conflict will occur. In such case, the user can (!) either abandon his local modification, or (2) save the configuration to a file, and then open and upload the configuration to the server to overwrite the existing configuration.
Conflicts in configuration with changes made by other workstations.	The configuration change is inconsistent with the change made by another user in the same section, which causes conflicts.	Either abandon the changes or overwrite the existing configuration by first saving the configuration to a file, then open and upload the configuration to the server.
You have made configuration changes that haven't been sent to the server yet. Click send to server to submit them before trying to do this.	The configuration has been modified locally but has not been sent to the server.	Send the configuration to the server.
Processing <completely configured number> of <total number> selected channels. Please configure the remaining <incompletely configured number> channels.		

Table D-4 Configuration and Network Messages

Message	Problem	Solution
	Some of the channels have incomplete configuration and are not currently being processed.	Complete the configuration for those channels and then send the configuration change to the server.
The video setup configuration has been changed. These settings must be sent to the server before completing the rest of the setup. Click <OK> to update the server or <Cancel> to remain on the video setup screen.		
	The list of video sources has been modified.	Either send the change to the server or cancel to remain in the Video Setup screen until you are ready to send the change to the server.
Failed to connect to http server.		
	The client failed to connect to the analytics server.	The analytics server may not be running. Check that ActivEye Video Analytics Service is running on the server. If the service is running and the problem persists, restart the service. Also check that Windows firewall setting does not block TCP port 18081 used by the analytics server.
Authorization required.		
	The user is not authorized.	Correct the user name and password and log on again.
No username provided for authentication.		
	The username is not provided for authentication.	Correct the user name and password and log on again.
User is not authorized for requested function.		
	The user does not have permission for the requested function.	Run User Configuration and check the permission settings for this user.
Created time out of range - please fix your clock.		
	The system clocks between the server machine and the client machine differ by more than five minutes.	Correct the system clocks on either or both machines to make sure they are synchronized.
Unable to receive video streams from Honeywell IP cameras. Please check your Windows firewall settings and refer to the Solutions section in the Reference Guide for details.		
	Video streaming from one or more Honeywell IP cameras is being blocked by a firewall. UDP ports 6456, 6457, 6458 and 6459 are needed for the video streams.	Check your windows firewall settings to make sure that there are exceptions defined for ActiveAlertLiveService.exe and/or the listed UDP ports. Also check any firewalls between the HVA server and Honeywell IP cameras and make sure they allow traffic on the listed UDP ports.

Scene Object, Zone, and Event Messages

Table D-5 Scene Object, Zone and Event Messages

Message	Problem	Solution
Please set the zones associated with this event.	Suitable zones were not selected for an event that requires them.	This message may appear during editing of event properties. Events that are tied to a certain zone type require that the user select appropriate zones before confirming the event.
Please define type of scene for camera <camera name>.	On the Channel Setup page, the user did not define a type of scene from the check boxes on the Scene Setup sub page.	On the Channel Setup page, select the Scene Setup sub page and check one or more of Scene with people , Scene with cars , a user-defined duration, such as 30 seconds). The maximum duration can be 1 minute (60 seconds).
Please define two person example scene objects for camera <camera name>.	On the Scene Setup sub page of the Channel Setup page, the user has selected Scene with people and has not specified two person example scene objects.	On the Scene Setup sub page of the Channel Setup page, from the Add scene object... select list, select Add person example and size the newly created object to the size of a person within some portion of the scene. The user must then create a second person example and size the object to the size of a person in another portion of the scene.
Please define a second person example scene object for camera <camera name>.	On the Scene Setup sub page of the Channel Setup page, the user has selected Scene with people and has not specified a second person example scene object. Two such objects are required.	On the Scene Setup sub page of the Channel Setup page, from the Add scene object... select list, select Add person example and size the newly created object to the size of a person in a different portion of the scene from the first person example object previously defined.
Please define two car example scene objects for camera <camera name>.	On the Scene Setup sub page of the Channel Setup page, the user has selected Scene with cars and has not specified two car example scene objects.	On the Scene Setup sub page of the Channel Setup page, from the Add scene object... select list, select Add car example and size the newly created object to the size of a car within some portion of the scene. The user must then create a second car example and size the object to the size of a car in another portion of the scene.
Please define a second car example scene object for camera <camera name>.		

Table D-5 Scene Object, Zone and Event Messages

Message	Problem	Solution
	On the Scene Setup sub page of the Channel Setup page, the user has selected Scene with cars and has not specified a second car example scene object. Two such objects are required.	On the Scene Setup sub page of the Channel Setup page, from the Add scene object... select list, select Add car example and size the newly created object to the size of a car in a different portion of the scene from the first car example object previously defined.
Channel <ID>: Event <event type> not valid for product <product package>. Disabling event.		
	The channel configuration contains an event that is not supported by the assigned product package. The event will be temporarily disabled, and will be re-enabled if the channel is reassigned to a different product package that supports this event.	No specific action required.
Channel <ID>: Zone <zone type> not valid for product <product package>. Disabling event.		
	The channel configuration contains a zone that is not supported by the assigned product package. The zone will be temporarily disabled, and will be re-enabled if the channel is reassigned to a different product package that supports this zone.	No specific action required.
Invalid value (<value>) for <parameter name>. Value must be between <minimum> and <maximum> (default is <default value>).		
	The parameter is out of range.	Modify the parameter setting for this event to be within the allowed range.
To add events to this zone you must add an inside zone first. To add events to this zone you must add an outside zone first.		
	Both inside and outside zones must exist before counting events can be added.	Add both inside and outside zones first, before adding counting events for people or cars.

Overhead View Settings

Table D-6 Overhead View Settings Messages

Message	Problem	Solution
Please define a door threshold for camera <camera name>.	On the Scene Setup sub page of the Channel Setup page, the user has selected Overhead view and has not specified a door threshold example.	On the Scene Setup sub page of the Channel Setup page, from the Add scene object... select list, select Add door threshold and place and size the newly created object to a door threshold on the floor.
Please define a door span for camera <camera name>.	On the Scene Setup sub page of the Channel Setup page, the user has selected Overhead view and has not specified a door span example.	On the Scene Setup sub page of the Channel Setup page, from the Add scene object... select list, select Add door span at fixed height and place and size the newly created object to a door threshold on the floor.
Only one door threshold is allowed. Only one door span is allowed.	On the Scene Setup sub page of the Channel Setup page, the user has attempted to add a second door threshold example or a second door span example.	For overhead views, exactly one door threshold example and one door span example are required. Instead of adding a second such example, you can adjust the existing example by dragging the object with a mouse.
Invalid width of door threshold. Invalid height of door span.	On the Scene Setup sub page of the Channel Setup page, the user has entered a negative value for the door threshold width or for the door span height.	For overhead views, the door threshold width and the door span height must be positive numbers. Change any negative values entered in the user interface.
Door span must be longer than door threshold.	On the Scene Setup sub page of the Channel Setup page, the user has drawn a door span example that is shorter in length than the door threshold example.	For overhead views, the door span must be longer than the door threshold. Increase the door span until it is longer than the door threshold.

User Configuration Messages

Table D-7 User Configuration Messages

Message	Problem	Solution
Username length invalid - must be between 3 and 16	The user name is too short or too long	Make sure that the user name contains at least 3 characters and not more than 16 characters.
Invalid character in username - must be letters and digits only	The user name contains characters other than letters (A~Z, a~z) and digits (0~9).	Make sure that the user name contains only the allowed characters.
Invalid username - must have at least one letter	The user name contains no letter.	Make sure that the user name contains at least one letter.
Password length invalid - must be between 0 and 32	The password is too long.	Make sure that the password contains no more than 32 characters.
Invalid password - can only use printable/displayable characters	The password contains some non-printable characters.	Make sure that the password contains only printable characters.
Unable to connect to user management database	The databases may not be running or the user management database might be corrupted.	This indicates a system issue. Please contact Technical Support for further assistance.
Username and password cannot be the same	The user name and password are identical.	Make sure that the user name and password are different.
Username <username> not found	The user name does not exist in the user management database.	The user management database may be corrupted. Please contact Technical Support for further assistance.

System Level Messages

Table D-8 System Level Messages

Message	Problem	Solution
Channel %d (%s) processing at %.1f fps.	The channel is being processed at a slow frame rate. This may be caused by either an overloaded analytics server, or a slow network video feed.	Check if the CPU is overloaded on the analytics server. If not, then the video feed through the network is slow. This may be due to lack of bandwidth on the network or too many connections to the IP camera.
Failed to update configuration	The configuration failed to be uploaded to the server.	The analytics server may not be running. Check that ActivEye Video Analytics Service is running on the server. If the service is running and the problem persists, restart the service.
Configuration not applied. Please try again later.	The configuration change cannot be applied to the server.	The database is being repaired and the server is temporarily not responding to requests. Wait a few minutes and try again. If the problem persists, contact Technical Support for further assistance.
Database properties not set. Please try again later.	The database property change is not accepted by the server.	The database is being repaired and the server is temporarily not responding to requests. Wait a few minutes and try again. If the problem persists, contact Technical Support for further assistance.
Configuration not available. Please try again later.	The configuration cannot be acquired from the server.	The database is being repaired and the server is temporarily not responding to requests. Wait a few minutes and try again. If the problem persists, contact Technical Support for further assistance.
Server busy repairing database	The server is repairing the database.	The database is being repaired and the server is temporarily not responding to requests. Wait a few minutes and try again. If the problem persists, contact Technical Support for further assistance.
Unable to connect to database with new parameters. Changes rejected.		

Table D-8 System Level Messages

Message	Problem	Solution
	Connection to database failed.	Check the database service Mysql is running. Also check that Windows firewall setting does not block TCP port 3306 used by Mysql. If it is and the problem persists, contact Technical Support for further assistance.
Database indexing not started due to insufficient diskspace. Please adjust the database properties for this server.		
	There is not sufficient disk space left on the system to store analytics metadata.	Check the database properties under the System setup page. Reduce the minimum disk space requirement or shorten the storage duration on the server.
There was a problem starting database indexing.		
	There is some problem storing analytics metadata on the server.	Check that the database service Mysql is running. If the service is running and the problem persists, contact Technical Support for further assistance.
A minimum of [disk space size] MB free disk space is required for a [num of channels]-channel server.		
	The analytics server enforces a minimum of 250 MB of disk storage per licensed channel on an analytics server. You cannot set the Min Free Disk Space below this required minimum. For example, if the HVA server has a license for 4 channels, the required minimum will be 1,000 MB.	Please make sure that you have at least the required minimum free disk space on the analytics server. Usually this is the extra free space the system must have after it has stored analytics data for the specified number of days.

Live Monitoring Station Messages

While running the software, windows may appear describing problems and the actions that should be taken in response. You may see other messages in certain situations. If the message is not in the list below, please contact Technical Support for further assistance.

Table D-9 Live Monitoring Station Message Troubleshooting

Message	Problem	Solution
"Windows sockets initialization failed."		
	The Windows communications library failed.	Close the program and retry. If this fails a second time, reboot after closing the program.
"Invalid username or password."		

Table D-9 Live Monitoring Station Message Troubleshooting (cont'd)

Message	Problem	Solution
	You have typed an invalid user name and/or password.	<p>Similar to the Windows user logon, make sure Caps Lock is turned off. Remember that the user name and password are case sensitive.</p> <p>Check that you have the correct user name and password and that it is the same on all the servers to which you are trying to connect.</p> <p>Confirm the correct user name and password with your System Administrator.</p>
<hr/>		
"Error connecting to server <server name>: <port>."	The application was unable to connect to the Video Analytics service running on the specified server.	<p>Verify that the network connection to the server is available.</p> <p>Verify that the Video Analytics service is running on the server.</p>
<hr/>		
"Internal error: Invalid command for control.xml: code=<error code>."	There was an error in communication with the server.	<p>The most likely cause of these errors is a network connectivity problem. Verify that the network connection to the server is available. Verify that firewall settings do not prevent communication with the server.</p> <p>If the network settings are correct and the problem persists, please contact Technical Support for further assistance.</p>

Forensics Tool Messages

Table D-10 Forensics Tool Message Troubleshooting

Message	Problem	Solution
Unable to connect to the database server.	The Forensics Tool cannot connect to the database server on the analytics server. This may be due to <i>mysql</i> service not running on the server.	Contact your System Administrator to check the server status and restart the database server on the Video Analytics server. Make sure that port 3306 is not blocked by the Windows firewall.
Invalid username or password.	You have typed an invalid user name and/or password.	<p>Similar to the Windows user logon, make sure Caps Lock is turned off. Remember that the user name and password are case sensitive.</p> <p>Check that you have the correct user name and password and that it is the same on all the servers you are trying to connect to.</p> <p>Confirm the correct user name and password with your System Administrator.</p>

Reports Generator Messages

Table D-11 Reports Generator Messages

Message	Problem	Solution
Unable to connect to the database server	The Reports Generator cannot connect to the database server on the server. This may be due to <i>mysql</i> service not running on the server.	Contact your system administrator to check the server status and restart the database server on the Video Analytics processing server. Ensure that port 3306 is not blocked by Windows firewall.
Invalid username or password	You did not enter the reporting period or the specified reporting period is not valid.	Specify a valid reporting period.
Please specify the reporting period.	You did not enter the reporting period or the specified reporting period is not valid.	Specify a valid reporting period.

Table D-11 Reports Generator Messages

Message	Problem	Solution
Please specify at least one camera.	You did not select any camera for generating reports.	Specify at least one camera number.
Please specify an event.	You did not select any event for generating reports.	Specify an event for generating reports.
Please specify report type.	You did not select the report type.	Specify the report type to be either Chart or Table.
Please specify report format.	You did not select the report format.	Specify the report format to be PDF, HTML, or Text.
Failed to generate report. Please check input parameters.	Some of the libraries files for generating reports may be missing in your system.	Please contact Technical Support.

Reports Scheduler Messages

Table D-12 Reports Scheduler Messages

Message	Problem	Solution
Connection Error Could not connect to <hostname>	The application was unable to connect to the Reports Scheduler service running on the specified server.	Verify that the network connection to the server is available. Verify that the Reports Scheduler service is running on the server.
The configuration has been locked by <username> - wait until lock has been removed to edit configuration format. Could not delete report, report is locked by <username> The report configuration is locked by <username> - the configuration can't be changed now	Another user <username> is editing the same configuration that you are trying to modify.	Wait until user <username> finishes editing and then unlock the configuration.
The report could not be added/updated.	One or more report templates are corrupted.	Quit the application and then reconfigure the report templates.

Table D-12 Reports Scheduler Messages

Message	Problem	Solution
The report name <name> is already in use by another report.		
	You specified the same report name for two different report templates.	Use different names for different report templates.
The Report Name value can not be blank"		
	You did not enter a name for the report template.	Specify a name for the report.
The email address <email address> is not valid (format is incorrect).		
	You entered an invalid email address.	Check that the e-mail address uses the format <user@domain.xyz.>
The email address cannot be blank.		
	You did not enter an e-mail address.	Specify an e-mail address in the required field.
There must be at least one email recipient for a report.		
	You did not enter any e-mail recipient.	Specify at least one e-mail recipient.
The SMTP configuration is locked by <username> - the configuration can't be changed now		
The SMTP configuration could not be locked - check the connection status		
The SMTP configuration is locked by <username> - wait until the lock is released to update the SMTP configuration.		
	Another user <username> is editing the SMTP configuration that you are trying to modify.	Wait until user <username> finished editing and then unlock the SMTP configuration.
The SMTP server name is not specified		
	You did not enter the SMTP server name.	Specify the SMTP server name.
The SMTP port must be a value between 0 and 65536		
	The port number you entered is invalid.	Enter a valid number for the SMTP port.
Authentication is enabled - User Name must be specified		
Authentication is enabled - Password must be specified		
	You did not enter a username or password.	Specify the username and the password.
At least one SMTP setting is invalid - switch to the SMTP Configuration tab to correct invalid setting(s).		
Invalid SMTP Settings		
At least one SMTP setting is invalid - this will cause the scheduled emailed reports to not be sent. Do you want to correct the settings <Yes>, ignore the invalid settings and not receive scheduled reports <No>, or stay on this screen <Cancel>?		
	The SMTP setting you entered is invalid.	Click Reset on the SMTP Configuration page. Reconfigure the SMTP settings with valid values.

Reports Health Monitor Messages

Table D-13 Health Monitor Messages

Message	Problem	Solution
Connection Error. \ Could not connect to <hostname>	The application was unable to connect to the Reports Scheduler service running on the specified server.	Verify that the network connection to the server is available. Verify that the Reports Scheduler service is running on the server.

Alarm Management Messages

While running the Alarm Watch, messages may appear in certain situations. [Table D-14](#) lists messages you may encounter while running Alarm Watch Admin. [Table D-15](#) lists messages you may encounter while running the Alarm Watch Health Monitor and provides possible solutions.

Table D-14 Alarm Watch Admin Software Messages

Message	Situation	Solution
AMS is unable to communicate with analytics server [server name]: [error message]	The Alarm Management Server is unable to communicate with the analytics server [server name] with the error states in [error message].	<p>If [error message] is an HTTP connection error, the Analytics server may not be running or there may be a network connectivity issue to the Analytics server.</p> <p>If [error message] is a user authentication error. You may have typed in incorrect user name or password. If it is a permission error, the user name you have entered does not have required permission to log on from this application.</p>
Logon failed: only one user may be logged in at a time. User [user name] is currently logged in.		

Table D-14 Alarm Watch Admin Software Messages

Message	Situation	Solution
	The Alarm Management Server only allows one Alarm Watch Admin (AWA) user at a time. There is already another copy of AWA logged onto the AMS. The user name that the other copy of AWA is logged in with is provided as part of the message.	Either wait for the other user to finish their changes and log out from Alarm Watch Admin, or contact the other user to ask them to log out.
Invalid character(s) (?<">',&;) in server display name.		
	You have tried to use invalid characters in the display name for the analytics server.	Remove the invalid characters from the display name.
The analytics server hostname and port must be unique.		
	You are trying to add an Analytics server twice. Any given Analytics server can only be added once (to prevent duplicate alarms).	Correct the host name and/or port number if you typed them incorrectly, and try again.
HVA server display name [display name] is already in use. The server display name must be unique.		
	You are trying to add an Analytics server twice. Any given Analytics server can only be added once (to prevent duplicate alarms).	Correct the host name and/or port number if you typed them incorrectly and try again.
Hostname [host name] port [port number] is already in use by HVA server [display name]. The analytics server hostname and port must be unique.		
	You are trying to add an Analytics server twice. Any given Analytics server can only be added once (to prevent duplicate alarms).	Correct the host name and/or port number if you typed them incorrectly and try again.
IP address [IP address] (hostname [hostname]) port [port number] is already in use by HVA server [display name] (hostname [server host name]). The analytics server hostname and port must be unique		
	You are trying to add an Analytics server twice. Any given Analytics server can only be added once (to prevent duplicate alarms).	Correct the host name and/or port number if you typed them incorrectly and try again.
HVA user [username] on server [server name] is missing permissions required by AMS: [permission required]		
AMS requires an HVA user with these permissions: [permission required]		

Table D-14 Alarm Watch Admin Software Messages

Message	Situation	Solution
	The user name you supplied is missing one or more of those permissions required in order to login to AMS. The specific permissions that are missing are listed in the error message.	In Alarm Watch Admin, under Analytics Server Properties, use a different user with the required permissions to log on to this HVA server. Or, run ActivEye User Configuration tool to log on to this Analytics server and grant the user the required permission. You can also add a new user with the required permission. Then in Alarm Watch Admin, use this new user to log on to this analytics server.
A minimum of [disk space size] MB free disk space is required for Alarm Management Server.		
	The Alarm Management Server enforces a minimum of 1,000 MB of disk storage. You cannot set the Min Free Disk Space below this required minimum.	Please make sure that you have at least the required minimum free disk space on the AMS server. Usually this is the extra free space the system must have after it has stored alarm data for the specified number of days.
Please correct the parameters to keep at least 1 day of data.		
	You cannot set the value of "Keep Records up to" to be less than 1 day.	Change the value of "Keep Records up to" to be at least 1 day.
The current session will expire due to inactivity in 1 minute. Click <Yes> to renew the session, <No> to disconnect.		
	You are logged into Alarm Watch Admin but haven't made any changes for 15 minutes. If you don't click Yes within the next 1 minute, your session will be automatically logged out so that other AWA users can log in.	If you still want to make changes, click Yes to maintain your session. If you are done making changes, click No to log out. If you do not respond within 1 minute, you will be automatically logged out.
The AMS session has expired due to inactivity. Please reconnect to AMS to continue.		
	You are logged into Alarm Watch Admin but have not made any changes for 15 minutes. You have been automatically logged out.	If you need to make more changes, reconnect to AMS (File » Connect to Alarm Management Server (AMS)...).
A minimum screen resolution of 1280x800 is required. Please increase the screen resolution for optimal view of the application.		
	Screen resolution of the primary monitor is set to less than 1280 pixels wide and/or less than 800 pixels high. Alarm Watch Station can run at the lower resolution, but the display will be less than optimal and some display elements may be truncated or reduced in size.	Go to Display Settings in the Windows Control Panel and change the resolution of monitor number 1 to be at least 1280 pixels wide, and at least 800 pixels high. If this makes the print on the monitor too small, change the monitor DPI to large fonts or change the font sizes in display/desktop properties, or get a larger monitor.

Table D-14 Alarm Watch Admin Software Messages

Message	Situation	Solution
Are you sure you want to close Alarm Watch Station? Click <OK> to close or <Cancel> to continue using the application.		
	You have clicked exit that will close the Alarm Watch Station.	To close Alarm Watch Station, click OK . Otherwise, click Cancel .
Closing the application while modifying an alarm will abandon all changes submitted. Are you sure you want to close Alarm Watch Station now? Click <OK> to close or <Cancel> to continue using the application.		
	You started modifying an alarm and then clicked exit that will close the Alarm Watch Station.	To save the alarm changes you have made, click Cancel and then click Apply in the Selected Alarm section of Alarm Watch Station. To discard the alarm changes you have made and close Alarm Watch Station, click OK .
Due to insufficient disk space alarm data before [date/time] will be deleted. Please free up some additional disk space or adjust your database properties.		
	Disk space has dropped below the Min Free Disk Space set in Database Properties. The server is no longer able to keep data for the number of days specified by the user and is deleting the oldest data to get disk space back above the minimum.	Check the free disk space on the server. Delete unused files or folders to free up enough disk space to allow the server to store analytics or alarm data for the specified duration. If that is not possible, reduce the number of days to store the data, or reduce the free disk space required on the system (which cannot fall below the hard minimum set by the system) in the Database Properties dialog.
Error processing database request: [error message]		
	The Alarm Management Server encountered an error while trying to write your changes to the database.	If the error message indicates a problem with one of your inputs, then correct the value and try again. If this does not resolve the issue, contact technical support for further diagnostics. Please have the log files ready. The log files are located in the software install directory (usually C:\Program Files\Honeywell Video Systems\ActivEye\Active Alert if it is installed under C drive at the default directory).
You may not select [All] and separate filter items. [single selections] will be removed from the selection.		
	You have tried to select All and specific values for filtering at the same time. You cannot do both.	Alarm Watch Station automatically deselects All if specific selections are made in the filter. To include all items for a particular filter type, select All instead of selecting all individual items
The user does not have permission to access the image directory [directory]. Please correct and restart the application.		

Table D-14 Alarm Watch Admin Software Messages

Message	Situation	Solution
	Alarm Watch Station needs permission to save keyframe images to the identified directory.	Change the permissions on the identified directory to allow writing.
Cannot locate sound files. No audio alarms will be played.		
	Alarm Watch Station is unable to locate its sound files for audio alarms.	Check to see if there is a Sounds folder under the software installed directory (usually C:\Program Files\Honeywell Video Systems\ActivEye\Active Alert if it is installed under C drive at the default directory). If the Sounds folder is missing or if the problem is not corrected, reinstall the client programs.
Do you wish to save your currently modified alarm? Click <Yes> to save, <No> to abandon your changes, or click <Cancel> continue editing.		
	After modifying an alarm (or multiple alarms), you tried selecting another alarm without first clicking Apply to submit your changes to AMS for the current selection.	If you want to save the alarm changes you have made, click Yes . To discard the changes, click No . To continue making changes to the currently selected alarm(s), click Cancel .
[number of alarms] alarm(s) are locked by other users. They will be deselected automatically and the username is displayed in Modification Status column.		
	One or more of the alarms you have selected and tried to modify is currently being modified by another user. You cannot modify them until the other user has finished.	You can continue to modify the alarms that are not locked by other users. If you still want to modify any of the alarms that are locked by other users, you have to wait until they have finished their changes and then reselect those alarms.
XML parsing error	Unexpected error parsing response from server	This is a rare error. If it happens, please contact Technical Support. Please have the log files ready. The log files are located in the software install directory (usually C:\Program Files\Honeywell Video Systems\ActivEye\Active Alert if it is installed under C drive at the default directory).
Server errors - View status for details		

Table D-14 Alarm Watch Admin Software Messages

Message	Situation	Solution
	Alarm Management Server is not receiving alarms from at least one of the configured Analytics servers.	In Alarm Watch Station, click View » Show Status to see the current status of all the configured Analytics servers. An error indicates that the Analytics server is not reachable from AMS and the possible reasons are: <ul style="list-style-type: none"> • Network connectivity problem - check your network connection in this case; • User permission issue - check the permission of the user that is set to connect to this specific Analytics server in Alarm Watch Admin. • Analytics server is not running - restart the server.
Connection Lost. Reconnecting in [time interval] seconds to [hostname or IP address]		
	The connection from Alarm Watch Station to Alarm Management Server has been lost. Alarm Watch Station will try to automatically reconnect to the Alarm Management Server every 30 seconds until it succeeds.	Check the following: <ul style="list-style-type: none"> • There is no network connectivity issue between Alarm Watch Station and AMS. • The Alarm Management Server is running. You may want to restart HVA Alarm Management Service on the AMS server.
Logging into another AMS while modifying an alarm will abandon all current changes. Are you sure you want to login to another AMS now? Click <OK> to continue or <Cancel> to stay in current session.		
	You started modifying an alarm without submit the changes and then clicked File » Login to log on to another AMS or relog on to the current AMS.	To save the alarm changes you have made, click Cancel and then click Apply in the Selected Alarm section of Alarm Watch Station. To discard the alarm changes you have made and log on to a different Alarm Management Server, click OK .
Dismissed alarms are excluded from the filter and your filter setting has been modified. Please check your filter setting.		
	You have changed your configuration by selecting Hide Dismissed Alarms . This resets the filter selection for alarm classification back to Default to include the following classification types: Default, Review and Critical.	Check the alarm filter and the filter selection for alarm classification. Click Edit Filter to modify it to the selection you want.
Dismissed alarms are included in the filter and your filter setting has been modified. Please check your filter setting.		
	You have changed your configuration by deselecting Hide Dismissed Alarms . This resets the filter selection for alarm classification back to All .	Check the alarm filter and the filter selection for alarm classification. Click Edit Filter to modify it to the selection you want.
AMS is shutting down. Please wait a few minutes and then try to reconnect to AMS to continue.		

Table D-14 Alarm Watch Admin Software Messages

Message	Situation	Solution
	The Alarm Management Server is shutting down, so it has forcibly disconnected your Alarm Watch Admin session.	Wait for AMS to restart and then log on again.
The connection to AMS has been lost. Please reconnect to AMS to continue.		
	The connection from Alarm Watch Admin to Alarm Management Server has been lost.	<p>Check the following:</p> <ul style="list-style-type: none"> • There is no network connectivity issue between Alarm Watch Station and AMS. • The Alarm Management Server is running. You may want to restart HVA Alarm Management Service on the AMS server.
Failed connecting to AMS database - keyframe cannot be displayed.		
	Unable to connect to database on Alarm Management Server to retrieve the keyframe for an old alarm.	<p>Check the following:</p> <ul style="list-style-type: none"> • There is no network connectivity issue between Alarm Watch Station and AMS. • The Alarm Management Server is running. You may want to restart HVA Alarm Management Service on the AMS server. • The Mysql service is running on the AMS server. You may need to restart the Mysql service.
Failed to find keyframe in AMS database - keyframe cannot be displayed.		
	Keyframe for old alarm not found in database on Alarm Management Server.	<p>Check if the same alarm key frame is present on the Analytics server using the Forensics Tool. If there is, the problem may be that Alarm Management Server did not receive the key frame and store it in the database. If there is not, then the key frame is not available. Please contact Technical Support for further diagnostics. Please have the log files ready. The log files are located in the software install directory (usually C:\Program Files\Honeywell Video Systems\ActivEye\Active Alert if it is installed under C drive at the default directory).</p>
The alarm change session has expired due to inactivity.		

Table D-14 Alarm Watch Admin Software Messages

Message	Situation	Solution
	You started to modify the selected alarm(s) in Alarm Watch Station and did not submit/cancel your change or renew your editing session within 90 seconds.	Reselect the alarms you want to modify, make your changes and submit the change within 90 seconds, or renew the editing session if you need more time.
The alarm editing session will expire due to inactivity. Click OK to continue editing the alarm.		
	You started to modify one or more alarms and stopped for 60 seconds. Your changes are discarded if you don not click OK within 15 seconds.	Click OK if you want to renew the editing session. Submit your change when you finish.

Table D-15 Health Monitor Software Messages

Message	Situation	Solution
Failure sending mail	This message is from the Email Client. The Alarm Watch module failed to send the alarm email.	Check the setting of the Email Client, especially the SMTP server settings and user authentication information. This can also be a network problem. Make sure that the SMTP server is reachable.
No relay boards were found		
	The relay board is not found or recognized by the system.	Run Instacal from MCC. Check if the relay board is in the list of boards connected to the machine. If not, add the relay board and close Instacal. Restart Alarm Watch Server Service.
MCC Error on board 0: Digital device is not responding - Is base address correct?		
	The message is from the MCC Relay Client. The Alarm Watch module failed to trigger the relay when the alarm arrived.	Check that the relay board is connected to the server and it is working. You can use the InstaCal problem from MCC to test the relay board. If the relay is connected and it passes the tests in InstaCal, restart the Alarm Watch Server Service.
Unable to load DLL 'cbw32.dll': The specified module could not be found.		

Table D-15 Health Monitor Software Messages

Message	Situation	Solution
Alarm Watch Health Monitor shows status "Relay signaled", but no clicking on the relay.	The MCC relay driver is missing or not found on the system.	Reinstall the MCC driver and then restart the PC.
	The relay hold time in the saved configuration may not be correct (too short). This may happen after upgrade from an older version of Alarm Watch.	Check the setting of the MCC Relay Client. Make sure that the relay hold time is set to at least 200 milliseconds and at most 10000 milliseconds. Click Apply to reapply the setting. Then, restart the Alarm Watch Server Service.

Technical Support

During your installation and operation of Honeywell Video Analytics software, if you have any questions, please contact Honeywell Technical Support.

Contact Information	For ...
Calling Honeywell in North America 1.800.796.2288 For locations outside North America, see the back cover of this publication.	Honeywell Video technical support is available for help with training or to resolve technical issues.
E-mailing Honeywell HVSupport@honeywell.com	Honeywell Video technical support can be reached by e-mail at the address on the left.
Whether you call or e-mail, please have on hand the information listed below: Your operating system used to run Honeywell Video Analytics software on the PC (for example, Windows® XP Pro®) The digital video recorder (DVR) used. For example, Rapid Eye. Any information you found about this or any Video Analytics user guide.	

Index

A

-
- adding [207](#)
 - alarm acknowledgement states [189](#)
 - alarm list
 - acknowledging alarms [228](#)
 - adding a comment [230](#)
 - classifying [229](#)
 - modifying alarm status [226](#)
 - alarm management
 - alarm suspension rules [192](#)
 - described [25](#)
 - overview [179](#)
 - alarm management server
 - described [180](#)
 - system configuration [192](#)
 - alarm suspension rules
 - adding [195](#)
 - cameras tab [202](#)
 - custom schedule [198](#)
 - deleting [204](#)
 - disabling [204](#)
 - enabling [204](#)
 - filtering [194](#)
 - managing [192](#)
 - modifying [204](#)
 - refreshing display [205](#)
 - time specifier [196](#)
 - viewing in alarm watch station [222](#)
 - viewing scope [205](#)
 - alarm watch
 - e-mail client [247](#)
 - health monitor [253](#)
 - messages [322](#)
 - alarm watch admin
 - acknowledgement states [190](#)
 - configuring [184](#)
 - database properties [216](#)
 - described [180](#)
 - logging on [182](#)
 - user accounts [213](#)
 - users tab [214](#)
 - alarm watch admin messages [322](#)
 - alarm watch health monitor
 - messages [329](#)
 - alarm watch manager
 - clients, configuring [243](#)
 - configuration [181](#)
 - logging on [238](#)
 - running [240](#)
 - servers [241](#)
 - user administration [238](#)
 - validating configuration [245](#)
 - alarm watch station
 - alarm suspension rules [222](#)
 - configuring [220](#)
 - described [25](#), [179](#), [180](#)
 - latest alarm [224](#)
 - live tab [219](#)
 - logging on [217](#)
 - menu bar [219](#)
 - status [222](#)
 - view menu [220](#)
 - viewing status [222](#)
 - alarms
 - comment [154](#)
 - display [141](#)
 - features [28](#)
 - group counts [143](#)
 - object left unattended [89](#)
 - object removed [91](#)
 - object trajectory, viewing [154](#)
 - possible theft event [93](#)
 - retrieval [153](#)
 - setting threshold [134](#)
 - threshold control [76](#)
 - view window [144](#)
 - viewing latest [152](#)
 - analytics servers, managing [185](#)
 - asset zone
 - defined [64](#), [289](#)
 - setting up [90](#)
 - Axis IP live video, explained [51](#)

B

blinding

- described [79](#)
- threshold values [80](#)

blurring

- described [80](#)
- threshold values [81](#), [82](#)

C

calibration messages [308](#)

calibration targets [125](#)

camera [97](#)

- adjusting blind threshold [80](#)
- adjusting blur threshold [80](#)
- adjusting scene change threshold [81](#)
- blind threshold values [80](#)
- blinding described [79](#)
- blur threshold values [81](#), [82](#)
- events [258](#)
- groups
 - adding [121](#)
 - counting data [119](#)
 - messages [308](#)
- scene change [81](#)
- selecting [33](#)
- tamper detection [76](#)
- tamper detection thresholds [79](#)
- tamper detection types [76](#)
- tamper detection, adjusting [78](#)
- tamper detection, configuring [77](#)
- video setup messages [307](#)

camera blurring, described [80](#)

camera calibration [125–132](#)

camera events [30](#)

camera group

- messages [308](#)

camera placement

- object left unattended [89](#)
- object removed [90](#)
- overhead people counting [97](#)
- possible theft event [93](#)
- premium events [86](#)
- verifying overhead [98](#)

camera tamper detection [141](#), [144](#)

car counted in lane event [280](#)

car entered lot event [69](#), [279](#)

car entered restricted area event [273](#)

car events, listed [29](#), [257](#)

car exited lot event [69](#), [280](#)

car exited restricted area event [273](#)

car lane counter zone [64](#), [69](#), [71](#), [288](#)

car made illegal u-turn event [275](#)

car needs assistance event [276](#)

car parked in handicapped zone event [275](#)

car parked in restricted area event [274](#)

car pulled off road event [276](#)

car speeding event [277](#)

car started driving in wrong direction event [272](#)

car stopped driving in wrong direction event [273](#)

car trespassing event [274](#)

channel

- changing settings [59](#)

- saving settings [83](#)

- setting up [58](#)

chart report [168](#)

client applications [24](#)

clients, configuring [243](#)

comment

- alarms, adding [154](#)

- event, adding [154](#)

- object, adding [157](#)

configuration tool

- uploading changes to server [131](#)

configuration

- clients [243](#)

- conflicts [84](#)

- messages [308](#)

- resolving conflicts [84](#)

- saving [83](#)

- uploading to server [56](#), [82](#), [124](#)

- validating [245](#)

configuration tool

- defined [24](#)

- file menu [48](#)

- logging on [47](#)

- navigating [48](#)

- setting up system [47–84](#)

connection time-out [192](#)

counter reset schedule [114](#), [134](#)

counting

- line [63](#)

counting events [30](#), [258](#), [277–281](#)

counting line

- configuring [103](#)

- description [26](#)

custom exception schedule, setting [200](#)

D

database

- viewing, maintaining [136](#)

deleting [209](#)

detection zone

- defined [64](#), [289](#)

- object left unattended [87](#)

direction zone

- defined [63](#), [66](#), [285](#)

- zone definitions [66](#)

display format [140](#)

door motion [39](#)
doorway, setting up [100](#)

E

e-mail setup [172](#)
environmental conditions, described [37](#)

event
 comment [154](#)
 display [147](#)
 history, retrieving [156](#)
 key frame, viewing [153](#)
 object trajectory, viewing [154](#)
 retrieval [153](#)
 viewing latest [152](#)
event detection features [27](#)
event messages [312](#)

events

- adding [74](#)
- car [29](#), [257](#)
- car counted in lane [280](#)
- car entered lot [69](#), [279](#)
- car entered restricted area [273](#)
- car exited lot [69](#), [280](#)
- car exited restricted area [273](#)
- car made illegal u-turn [275](#)
- car needs assistance [276](#)
- car parked in handicapped zone [275](#)
- car parked in restricted area [274](#)
- car pulled off road [276](#)
- car speeding event [277](#)
- car started driving in wrong direction [272](#)
- car stopped driving in wrong direction [273](#)
- car trespassing [274](#)
- counting [277–281](#)
- counting [30](#), [258](#)
- modifying [75](#)
- object entered [259](#)
- object entered restricted zone [260](#)
- object exited [259](#)
- object exited restricted zone [260](#)
- object left unattended [86](#), [88](#), [89](#)
- object left unattended alarm [89](#)
- object motion [259–262](#)
- object removed [264](#)
- object removed event, configuring [89](#)
- object removed, alarms [91](#)
- object removed, camera placement [90](#)
- object started moving [260](#)
- object started moving in wrong direction [261](#)
- object stopped [261](#)
- object stopped moving in wrong direction [262](#)
- object trespassing [67](#), [262](#)
- objects left unattended [264](#)
- objects merged [263](#)
- objects split [264](#)
- overhead people counting [95](#)
- people [29](#), [257](#), [265–272](#)
- people converged [270](#)
- people counting [29](#), [113](#), [114](#), [257](#)
- people passed by [270](#)
- person counted as entering [114](#), [277](#)
- person counted as exiting [278](#)
- person entered restricted zone [265](#)
- person entered target zone [271](#)
- person exited restricted zone [265](#)
- person loitering in restricted zone event [266](#)
- person on fence line [270](#)
- person running in wrong direction [269](#)
- person started moving in wrong direction [266](#)
- person started running [268](#)
- person staying in target zone [272](#)
- person stopped moving in wrong direction [267](#)

- person stopped running [269](#)
- person trespassing [267](#)
- possible theft [91](#), [271](#)
- premium [29](#), [30–93](#), [257](#), [258](#)
- severity level [75](#)
- smart impressions [30](#), [258](#)
- started moving in the wrong direction [66](#)
- traffic [272–277](#)
- video [30](#), [258](#), [281–282](#)
- video lost [281](#)
- video restored [282](#)
- exclusion zone [37](#), [38](#), [40](#), [118](#), [284](#)
 - defined [63](#)
 - overhead people counting [102](#)
 - with inside/outside zones [110](#)

F

features

- alarm delivery [28](#)
- alarm watch [25](#)
- live monitoring [27](#)
- object and event detection [27](#)
- report generation [28](#)
- search and retrieval [28](#)

fence zone, defined [63](#), [286](#)

field testing [116](#)

floor coverage, verifying [99](#)

foliage motion [40](#)

forensics tool

- alarms, retrieving [153](#)
- comment [154](#), [157](#)
- defined [24](#)
- error messages [319](#)
- event history, retrieving [156](#)
- event key frame, viewing [153](#)
- events, retrieving [153](#)
- frames, retrieving [158](#)
- frames, viewing [158](#)
- logon [149](#)
- main window [151](#)
- messages [319](#)
- object snapshot, viewing [155](#)
- object trajectory, viewing [154](#), [155](#)
- objects, retrieving [155](#)
- requirements [149](#)
- search field definitions [151](#)
- search, starting [151](#)
- viewing latest [152](#)

frame

- retrieval [158](#)

- viewing [158](#)

frame search results, viewing latest [152](#)

Fusion

- adding a video source [54](#)
- live video, explained [52](#)
- selecting multiple cameras [55](#)

G

- gate motion [39](#)
- ground zone, defined [73](#)

H

- handicapped zone, [64](#), [290](#)
- high sensitivity [62](#)
- holidays/exceptions lists [207](#), [209](#)
 - managing [206](#)
- Honeywell IP live video, explained [51](#)

I

- identification systems [34](#)
- image display [148](#)
- image zone, setting up [73](#)
- inside zone
 - adjusting [118](#)
 - defined [64](#), [288](#)
 - meeting room [107](#), [110](#)
 - setting up [68](#)
 - with exclusion zones [110](#)

L

- latest alarm [224](#)
- layout [140](#)
- license key
 - entering [135](#)
 - updating [57](#)
- licenses
 - messages [306](#)
 - viewing [57](#)
- lighting conditions, described [34](#)

- live monitoring station [137](#)
 - alarm display [141](#)
 - alarm view window [144](#)
 - defined [24](#)
 - display format [140](#)
 - event display [147](#)
 - features [27](#)
 - image display [148](#)
 - layout [140](#)
 - logon [137](#)
 - main window [139](#)
 - messages [317](#)
 - normal camera view window [145](#)
 - program running [138](#)
 - requirements [137](#)
 - reset scene change alarm window [147](#)
 - scene change alarm window [146](#)
 - server status [140](#)
 - threshold settings [147](#)
- live video
 - adding [52](#)
 - adding source [53](#)
 - selecting from Fusion [54](#)
- logon
 - forensics tool [149](#)
 - live monitoring station [137](#)
 - report scheduler [169](#)
 - reports generator [161](#)
 - reports health monitor [176](#)

M

- managing information zones [284](#)
- messages
 - alarm watch admin [322](#)
 - alarm watch health monitor [329](#)
 - camera group and calibration [308](#)
 - camera group, calibration [308](#)
 - configuration, network [308](#)
 - forensics tool [319](#)
 - license [306](#)
 - live monitoring station [317](#)
 - overhead view settings [314](#)
 - reports generator [319](#)
 - reports scheduler [320](#)
 - scene object, zone, event [312](#)
 - system level [316](#)
 - user configuration [315](#)
 - video setup [307](#)
- modifying [209](#)
- motion
 - doors [39](#)
 - foliage [40](#)
 - gates [39](#)
 - trees [40](#)

N

network connection, slow [138](#)
network messages [308](#)

O

object
 comment [157](#)
 retrieval [155](#)
 snapshot, viewing [155](#)
 trajectory [154](#)
 trajectory, viewing [155](#)
 viewing latest [152](#)
object detection features [27](#)
object entered event [259](#)
object entered restricted zone event [260](#)
object exited event [259](#)
object exited restricted zone event [260](#)
object left unattended event
 alarm screen [89](#)
 defined [86](#)
 parameters [88](#)
object motion events [259–262](#)
object removed event
 alarm screen [91](#)
 camera placement [90](#)
 configuring [89](#)
object started moving event [260](#)
object started moving in wrong direction event [261](#)
object stopped event [261](#)
object stopped moving in wrong direction event [262](#)
object trajectory, viewing [154](#), [155](#)
object trespassing event [67](#), [262](#)
object-block zone [63](#), [118](#), [284](#)
 overhead people counting [101](#)
object-block zones [38](#), [40](#)
objects left unattended event [264](#)
objects merged event [263](#)
objects removed event [264](#)
objects split event [264](#)
observation systems [33](#)
operating conditions
 premium events [85](#)
 types [35](#)
outside zone
 adjusting [118](#)
 corridor [108](#), [109](#), [111](#), [112](#)
 defined [64](#), [288](#)
 setting up [68](#)
 with exclusion zones [110](#)

overhead people counting event [95](#)
 exclusion zone [102](#)
 object-block zone [101](#)
 requirements [96](#)
 verifying camera placement [98](#)
overhead view settings messages [314](#)

P

password [138](#)
password, changing [45](#)
people converged event [270](#)
people counting events
 listed [29](#), [257](#)
 setting up [113](#)
 wide entrance [114](#), [119](#)
people events [29](#), [257](#), [265–272](#)
people passed by event [270](#)
permission types [43](#)
person counted as entering [114](#)
person counted as entering event [277](#)
person counted as exiting event [278](#)
person entered restricted zone event [265](#)
person entered target zone event [271](#)
person exited restricted zone event [265](#)
person loitering in restricted zone event [266](#)
person on fence line event [270](#)
person running in wrong direction event [269](#)
person started moving in wrong direction event [266](#)
person started running event [268](#)
person staying in target zone event [272](#)
person stopped moving in wrong direction event [267](#)
person stopped running event [269](#)
person trespassing event [267](#)
possible theft event
 alarm [93](#)
 camera placement [93](#)
 defined [271](#)
 setting up [91](#)
premium events [30–93](#), [258](#)
 camera placement [86](#)
 listed [29](#), [257](#)
 object left unattended [86](#), [88](#), [89](#)
 object removed [89](#)
 operating conditions [85](#)
 possible theft [91](#)
product licenses [57](#)

R

recognition systems [33](#)
reflective surfaces, described [38](#)
report generation features [28](#)
reporting tool
 defined [25](#)

- reporting tool, using [28](#)
- reports generator
 - chart report [168](#)
 - defined [159](#)
 - generating report [164](#)
 - logging on [161](#)
 - main screen [162](#)
 - report type [164](#)
 - selecting cameras [163](#)
 - selecting event [164](#)
 - selecting report type [164](#)
 - setting up [161](#)
 - specify reporting interval [163](#)
 - table report [166](#)
 - templates [165](#)
- reports generator messages [319](#)
- reports health monitor
 - defined [159](#), [160](#)
 - logging on [176](#)
 - main screen [177](#)
 - setting up [176](#)
- reports health monitor messages [322](#)
- reports scheduler
 - defined [159](#), [160](#)
 - edit template [174](#)
 - e-mail setup [172](#)
 - existing template [172](#)
 - logging on [169](#)
 - main screen [170](#)
 - new template [170](#)
 - schedule [172](#)
 - setting up [169](#)
 - SMTP configuration [174](#)
- reports scheduler messages [320](#)
- restricted zone [65](#), [285](#)
 - defined [63](#), [285](#)
 - setting up [66](#)
- retrieving
 - alarms [153](#)
 - event history [156](#)
 - events [153](#)
 - frames [158](#)
 - group counts [143](#)
 - objects [155](#)
- scene change [81](#)
 - alarm [146](#)
 - threshold values [81](#)
- scene-object messages [312](#)
- schedule, setting up [172](#)
- schedules
 - adding [210](#)
 - deleting [212](#)
 - managing [209](#)
 - modifying [212](#)
- search
 - field definitions [151](#)
 - starting [151](#)
- search and retrieval features [28](#)
- server status [140](#)
- servers, configuring [241](#)
- setup
 - reports generator [161](#)
 - reports health monitor [176](#)
 - reports scheduler [169](#)
- severity level, setting [75](#)
- shoulder zone, defined [64](#), [291](#)
- smart impressions events [30](#), [258](#)
- SMTP configuration [174](#)
- software
 - copyright [245](#)
 - version [245](#)
- Sony IP live video, explained [51](#)
- started moving in the wrong direction event [66](#)
- sterile zone [63](#)
 - zones
 - sterile [287](#)
- sterile zone, defining [67](#)
- system
 - configuring [47–84](#)
 - features [26](#)
 - overview [23](#)
 - setting database properties [136](#)
- system level messages [316](#)
- system load [36](#)
- systems
 - identification [34](#)
 - observation [33](#)
 - recognition [33](#)

S

- scene
 - add car [61](#)
 - adding [61](#)
 - adjusting [117](#)
 - overhead counting [62](#)
 - selecting type [59](#)
 - types [34](#)
 - with cars [60](#), [61](#)
 - with people [60](#)

T

- table report [166](#)
- tamper detection [81](#), [141](#), [144](#)
 - adjusting parameters [78](#)
 - blinding [79](#)
 - blurring [80](#)
 - configuring [77](#)
 - defined [76](#)
 - thresholds [79](#)
 - types [76](#)

tamper measure values [145](#)
target zone
 defined [64](#), [292](#)
 setting up [72](#)
TCP connection [137](#), [149](#)
technical support contacts [317](#)
template
 modifying [174](#)
 reports scheduler [170](#), [172](#)
testing
 field [116](#)
 inside/outside zones [118](#)
 single person [117](#)
 two people [117](#)
theft zone
 defined [64](#), [291](#)
threshold settings [147](#)
time-out [192](#)
traffic counting [70](#)
traffic events [272–277](#)
tree motion [40](#)
trespass line zone
 defined [67](#), [286](#)
 definitions [67](#)
trespass zone, defined [63](#)

U

user administration [238](#)
user configuration messages [315](#)
user name [138](#)
users
 adding [43](#)
 changing password [45](#)
 changing permissions [44](#)
 deleting [44](#)
 permission types [43](#)
 setting up [41](#)
u-turn zone
 defined [64](#), [290](#)
 defined [71](#)

V

video
 from AXIP IP [51](#)
 from Fusion DVR [52](#)
 from Honeywell IP [51](#)
 from Sony IP [51](#)
 lost event [281](#)

video events [30](#), [258](#), [281–282](#)
video input
 changing settings [59](#)
 saving settings [83](#)
 setting up [58](#)
video restored event [282](#)
video setup messages [307](#)
video source
 adding [52](#)
 adding a Fusion source [54](#)
 changing properties [55](#)
 deleting [56](#)
 live analog [53](#)
 live video [53](#)
 setting up [49](#)
 types [50](#)
viewing
 car lane counters [71](#)
 event key frame [153](#)
 frames [158](#)
 latest [152](#)
 object snapshot [155](#)
 object trajectory [154](#), [155](#)

W

wide entrance people counting [119](#)
window, alarm view [144](#)

Z

zone definition
 car lane [71](#)
 direction zone [66](#)
 inside in parking lot [69](#)
 inside meeting room [110](#)
 inside meeting room door [107](#)
 object left unattended [87](#)
 object removed [90](#)
 outside corridor [108](#), [109](#), [111](#), [112](#)
 restricted zone [65](#)
 target zone [73](#)
 theft line [92](#)
 trespass line [67](#)
 u-turn zone [72](#)
zone messages [312](#)
zone types [63](#), [64](#)

zones

- adjusting [118](#)
- asset [64](#), [289](#)
 - object removed [90](#)
- car lane counter [64](#), [69](#), [71](#), [288](#)
- counting line [63](#)
- detection [64](#), [289](#)
- detection, object left unattended [87](#)
- direction [63](#), [285](#)
- direction, defining [66](#)
- enabling specific events [285](#)
- exclusion [37](#), [38](#), [40](#), [63](#), [102](#), [110](#), [284](#)
- fence [63](#), [286](#)
- ground, defined [73](#)
- handicapped [64](#), [290](#)
- image, setting up [73](#)
- inside [64](#), [288](#)
- inside meeting room [107](#), [110](#)
- inside, setting up [68](#)
- managing information [284](#)
- object block [101](#)
- object-block [38](#), [40](#), [63](#), [284](#)
- outside [64](#), [288](#)
- outside corridor [108](#), [109](#), [111](#), [112](#)
- outside, setting up [68](#)
- restricted [65](#), [285](#)
- restricted zone [63](#)
- restricted zone, setting up [66](#)
- shapes [64](#)
- shoulder [64](#), [291](#)
- sterile [63](#)
- sterile, defining [67](#)
- target [64](#), [292](#)
- target, setting up [72](#)
- theft [64](#), [291](#)
- trespass [63](#)
- trespass line [286](#)
- trespass line, defined [67](#)
- u-turn [64](#), [290](#)
- u-turn, defined [71](#)
- viewing all [109](#), [113](#)
- viewing all inside & outside [109](#)

zoom tooltips [65](#), [90](#)

Honeywell Systems Group (Head Office)

2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299, USA
www.honeywellvideo.com
☎ +1.800.796.2288

Honeywell Systems Group Europe/South Africa

Aston Fields Road, Whitehouse Industrial Estate
Runcorn, Cheshire, WA7 3DL, UK
www.honeywell.com/security/uk
☎ +44.01928.754028

Honeywell Systems Group Caribbean/Latin America

9315 NW 112th Ave.
Miami, FL 3378, USA
www.honeywellvideo.com
☎ +1.305.805.8188

Honeywell Systems Group Pacific

Level 3, 2 Richardson Place
North Ryde, NSW 2113, Australia
www.honeywellsecurity.com.au
☎ +61.2.89353.7000

Honeywell Systems Group Asia

35F Tower A, City Center, 100 Zun Yi Road
Shanghai 200051, China
www.asia.security.honeywell.com
☎ +86 21.5257.4568

Honeywell Systems Group Middle East/N. Africa

Post Office Box 18530
LOB Building 08, Office 199
Jebel Ali, Dubai, United Arab Emirates
www.honeywell.com/security/me
☎ +971.04.881.5506

Honeywell Systems Group Northern Europe

Ampèrestraat 41
1446 TR Purmerend, The Netherlands
www.honeywell.com/security/nl
☎ +31.299.410.200

Honeywell Systems Group Deutschland

Johannes-Mauthe-Straße 14
D-72458 Albstadt, Germany
www.honeywell.com/security/de
☎ +49.74 31.8 01.0

Honeywell Systems Group France

Immeuble Lavoisier
Parc de Haute Technologie
3-7 rue Georges Besse
92160 Antony, France
www.honeywell.com/security/fr
☎ +33.(0).1.40.96.20.50

Honeywell Systems Group Italia SpA

Via della Resistenza 53/59
20090 Buccinasco
Milan, Italy
www.honeywell.com/security/it
☎ +39.02.4888.051

Honeywell Systems Group España

Avenida de Italia, nº 7
P.I. - C.T.C. Coslada
28820 Coslada, Madrid, Spain
www.honeywell.com/security/es
☎ +34.902.667.800

Honeywell

www.honeywellvideo.com
+1.800.796.CCTV (North America only)
HVSsupport@honeywell.com

Document 800-04267 – Rev B – 09/10

© 2010 Honeywell International Inc. All rights reserved. No part of this publication may be reproduced by any means without written permission from Honeywell. The information in this publication is believed to be accurate in all respects. However, Honeywell cannot assume responsibility for any consequences resulting from the use thereof. The information contained herein is subject to change without notice. Revisions or new editions to this publication may be issued to incorporate such changes.