

# **Rapid Eye Software**

## **Using ADMIN and VIEW to Configure Multi-Media Units and Manage Accounts**

# **System Administrator's Guide**



## Revisions

Issue	Date	Revisions
K5403V10 Rev A	2004, October	Honeywell template.
V10.B	2004, December	Formatting: pagination; minor edits.
V11 Rev A	2006, January	Updates to: time needed to clear storage, network address translation (NAT) for connection to unit, NAT for connection to alarm station, continuous and boosted settings for video recording, group of sites in Admin and View, DSP Maxer, configuration—camera, enhanced preview, PTZ, PIT/NETPIT, serial ports and removal of Restore button—, PTZ presets, PTZ controller, video smoothing, user account: site and camera selection, resolution gauges for live and recording, response schedule and rules, schedules' GUI, motion search reports, supported Microsoft Windows OS, LocalView: PTZ controller and passwords.
K14392 Rev A	2006, August	Pub number changed. Re-formatting (headings, pagination, figure captions). Added notes from previous release, updates to Scheduling: Configuration, The Enhanced Preview of Resolution, Rapid Eye Storage Estimator, System Clock: Manual Setting, Correcting the Clock, Programming a PTZ Dome Camera, NetPIT and PIT Devices and new features: User Management, Recording Video: Continuous Recording Settings, estimating the video archive, using Audio and Support for Older Models of Units. Back cover update, 21/08.
K14392V1 Rev A	2007, July	New features: ACUIX Dome Camera, Camera Sabotage: Detection. Updates to: Start Here, Using Higher Values When Recording Video, Simultaneous Sessions From One Unit and NetPIT and PIT Devices. "Boosted" recording changed to "Event" recording, but a "Boost" button remains. Section breaks added: Multi-Media Site: Connection Configuration and Pan, Tilt, and Zoom (PTZ) Setup.



# Table of Contents

<b>The Administration of a Rapid Eye System.....</b>	<b>19</b>
Start Here.....	19
About Using a PC to Operate Rapid Eye Units.....	19
About Using LocalView Onsite .....	20
Using a PC: Installing Rapid Eye Software .....	20
For the Multi SA Only: Admin <i>and</i> View Software .....	20
First Use: Running Admin Software .....	21
Customizing a Unit: View Software.....	21
For Questions .....	22
<b>Multi-Media Site: Name.....</b>	<b>23</b>
Preparations .....	23
Site Setup: Checklist .....	24
Naming / Renaming a Site .....	24
Site Naming Tips.....	25
After Dealing with a Site.....	25
Grouping Sites.....	26
To Create a Folder .....	26
To Assign a Site to a Folder.....	26
To Rename a Folder .....	27
To Delete a Folder .....	27
Grouping Folders.....	27
Removing a Site .....	28
To Delete a Site.....	28
Mistakenly Deleting a Secured Site Definition .....	28
<b>Multi-Media Site: Connection Configuration .....</b>	<b>29</b>
Types of Connection .....	29
Dial-up Connection: to a Unit.....	30
Setting a Dial-Up Connection .....	31
Area Code: Irregular Use .....	32
To Force a Long-distance Dial-up Using a Local Area Code .....	32
Forcing a Local Dial-up Across Area Codes .....	33
Dial-up Technical Note .....	33
Offering Many Dial-Up Connections to the Same Unit.....	34
Using Network Access .....	34
To Set a Network Connection.....	35
Standalone Unit and a PC that Has a Network Card .....	36
Network Address Translation .....	37
Adjusting a Unit's IP Settings for NAT .....	39
Setting a Router's Mappings .....	40
Updating a Unit's Connection.....	41
Refreshing the Multi-Media Local Db .....	41
Dynamic Host Configuration Protocol .....	41
To Configure DHCP Using Microsoft's Server2000 (or 2003) .....	41
Choosing the Computer Name or a Static IP.....	42

Table of Contents

- Many Connections to a Unit..... 43
  - To Specify Dial-up and Network Connections ..... 43
- RAS Server ..... 44
  - Planning to Connect to One Unit at a Time..... 44
  - To Set a Connection to a RAS..... 45
  - Using a RAS Server before Connecting to a Unit ..... 47
- Connections: Report and Customization..... 48
  - The Automatic Naming of Connections ..... 48
  - Changing the Automatic Suffix in a Connection's Name ..... 48
- Firewall: Technical Note ..... 49
- Cascading Alarm Stations..... 49
  - To Sequence a Site's Alarm Stations ..... 50
  - Quickly Assigning a Site to Many Alarm Stations ..... 50
  - Setting a Site to Not Report Alarms to a Specific Station ..... 50
- Customizing a Dial-Up Connection to an Alarm Station..... 51
  - To Customize the Dial-up Connection to an Alarm Station ..... 52
  - To Cancel the Customization of a Telephone Number..... 52
- Unit Configuration: Basics..... 53**
  - Maintenance Session ..... 53
    - To Start a Maintenance Session ..... 54
    - Support for Older Models of Units..... 54
  - Making a Site Operational..... 55
  - Unit's Time Zone and Clock..... 56
    - To Indicate the Time Zone of a Multi-Media Unit ..... 57
    - Conflicting Time Zones ..... 57
  - SNTP: Setting the Clock Automatically..... 58
  - System Clock: Manual Setting..... 59
    - Adjusting the Clock on a PC Running Rapid Eye Software..... 59
    - Using a PC's Clock to Set a Unit's Clock Manually ..... 59
    - Adjusting the Time on an Operational Unit ..... 60
    - Correcting the Clock..... 60
    - Securing a Site..... 61
    - Rebooting a Unit ..... 61
  - Maintenance Reference ..... 62
    - Ending Maintenance..... 62
    - Using Apply..... 62
    - Maintenance Topics..... 62
    - Maintenance Tasks ..... 63
    - Feedback Box Reference ..... 64
- Video Feed Setup..... 65**
  - Cameras ..... 65
    - Renaming a Camera..... 65
    - Adjusting a Video Feed..... 66
      - To Re-enable One Camera's Feed ..... 66
      - To Re-enable All Newly Connected, Powered Cameras..... 66
      - To Adjust All Cameras at Once..... 66
      - To Disable a Camera ..... 66
    - Resolution of Live Video in View Software ..... 66
    - Other Video Settings..... 67
  - Recording Video: Continuous Recording Settings..... 68
    - To Enable the Recording of a Video Feed ..... 68

Customizing Settings for Recorded Video.....	69
Resolution Setting.....	69
Frame Rate Setting.....	70
Quality Setting.....	70
To Duplicate Settings.....	70
Continuous Recording and Event Recording.....	71
Estimating Storage Capacity.....	71
Optimizing Recorded Video.....	72
Automatic Maximization of DSP Performance.....	72
Making Optimized Resolution and Frame Rate Settings.....	74
The Enhanced Preview of Resolution.....	74
Resolution Tips.....	75
Comparing the Resolutions of Recorded Video.....	76
Security and Presence.....	77
Camera Tips for Identification: Quality and Resolution.....	79
Resolution Gauge for Retrieval Session.....	79
Resolution Reference: Recorded Video.....	81
Customizing Windows for a PC Monitor's Settings.....	82
PC Monitor's Refresh Rate.....	82
Microsoft Dual View and Rapid Eye View Software.....	82
Larger Monitors and Microsoft Windows.....	83
Environmental Interference for Video Feeds.....	84
Physical Compromise.....	84
<b>Pan, Tilt, and Zoom (PTZ) Setup.....</b>	<b>85</b>
Serial Device Settings for PTZ.....	85
To Assign and Set a New PTZ Device.....	86
Video Tab Settings for PTZ.....	86
To Enable a PTZ Camera.....	87
Using a PTZ Camera.....	88
To Display the PTZ Dartboard Control.....	88
Using the Dartboard Control.....	89
Toggling between Zonal Mode and Pull Mode.....	89
Pulling the Rubber-Band.....	90
Using Zonal Mode.....	90
Programming a PTZ Dome Camera.....	91
To Configure a Preset on a PTZ Camera.....	91
To Test a Preset.....	92
Behavior of PTZ After a Session Closes.....	93
Support for RapidDome PTZ Features.....	95
RapidDome PTZ Tours.....	95
RapidDome Mimic Tour.....	96
To Test a Mimic Tour on a RapidDome Camera.....	96
RapidDome Preset Tour.....	96
To Setup a Tour of Presets on a RapidDome Camera.....	97
Testing a Preset Tour on a RapidDome Camera.....	98
Privacy Zones for RapidDome.....	98
To Set a Privacy Zone.....	98
ACUIX Dome Camera.....	99
Configuring the Intellibus Device for a Rapid Eye Unit.....	99
To Configure an ACUIX Dome Camera for PTZ Use.....	100
Discovery of ACUIX Dome Cameras.....	100
Backing Up an ACUIX Configuration File to a PC.....	100
Downloading a Configuration File to an ACUIX Dome Camera.....	101
Identifying the Model of the Camera.....	102
Upgrading the Firmware of an ACUIX Dome Camera.....	102

<b>Enhancing Video for Security .....</b>	<b>103</b>
Event Recording: Configuration .....	103
Using Higher Settings for Video Recorded During an Event .....	103
Setting Lower Values for Continuous Recording .....	104
Event Recording on Demand, Using the Boost Button .....	104
Automating Event Recording: Events of Interest .....	105
Scheduling: Configuration .....	105
Making Use of a Schedule.....	107
To Add a Schedule .....	107
Customizing a Schedule.....	107
To Assign a Schedule to a Camera, or Group of Cameras .....	108
Using a 15-minute Increment in a Schedule .....	108
To Rename a Schedule .....	109
To Delete a Schedule.....	109
Alarms and Scheduling.....	109
Holiday and Exception.....	110
Adding Holidays and Exceptions .....	111
Event Recording for Video: Scheduling a Response .....	112
Trigger: an Event of Interest .....	112
Displaying the Response Panel Used for Making Rules.....	113
Checklist for Setting a Rule in the Response Schedule.....	113
Renaming a Rule.....	114
Rule Status: Icons .....	114
Managing the Response to a Rule .....	115
Assigning a Schedule to a Response Rule .....	115
Disabling a Response Rule.....	115
Motion Detection .....	116
To Configure Motion Detection.....	117
Customizing Detection: Masking.....	117
Example: Masking an Area of the Video Feed .....	117
To Mask Part of a Video Feed from Motion Detection .....	118
False Positives .....	118
Customizing Detection: Scheduling .....	118
Motion Detection Reference .....	119
Motion Search .....	120
Camera Sabotage: Detection.....	120
To Configure CSD.....	121
Calibration of CSD .....	121
Moved-type CSD: Learning and Rearming Alarms .....	122
Computing the Length of the Video Archive.....	122
Rapid Eye Storage Estimator .....	123
Number of Cameras, Audio .....	124
Scheduling Cameras .....	125
Frame Rate for Continuous Recording.....	125
Quality .....	125
Resolution .....	126
Using Higher Values When Recording Video .....	127
A Multi-Media Unit's Storage Statistics .....	127
To Obtain a Unit's Statistics.....	128



**Configuring Other Hardware ..... 129**

- Clearing Storage ..... 129
- Preventing Users from Clearing Storage..... 130
- To Trace the Clearing of Storage ..... 131
- Updating Security on a Multi-Media Unit ..... 131
- System Files ..... 132
  - To Download a File from a Multi-Media Unit ..... 132
- System Tab in a Maintenance Session..... 134
  - Logging System Messages ..... 134
  - System Monitor..... 134
  - Making the FAULT RELAY Operational ..... 135
  - Camera Signal Format..... 135
  - LAN/WAN Communications..... 136
  - Changing a Unit's Network Settings ..... 136
  - Changing the Maximum Network Data Rate ..... 137
  - TCP Ports ..... 137
  - Default System Values for a Multi-Media Unit ..... 137
- Serial Device: Modem ..... 138
  - Viewing/Changing Modem Settings ..... 138
  - PPP: IP Settings Reserved for Modem Connection ..... 139
  - To Set an External Modem ..... 139
- Serial Device: PTZ ..... 140
  - To Assign and Set a PTZ Device ..... 140
- Hardware Report ..... 140
- Public Display Monitor: Using Monitor Output 1 ..... 141
  - External Hardware Control of a Public Display Monitor ..... 141
  - Using LocalView As an Additional Public Display Monitor ..... 142
- Customer Data and Customer-Device Events ..... 143
  - Adding a Customer Device That Sends Data to a Unit..... 143
  - Adding an Event Rule for a Data-recording Device ..... 144
  - Search Rule and Regular Expressions: Reference ..... 145
  - NetPIT and PIT Devices ..... 146
- Multi Audio ..... 147
  - Audio Hardware ..... 147
  - Using Multi Audio..... 148
  - Audio Interference..... 148
  - Audio with LocalView ..... 148
  - To Enable Audio for Use Onsite, by LocalView..... 149
  - To Disable Audio for LocalView..... 149
  - Multi-Media LT Audio Resources..... 149
  - Eagle Audio ..... 149
- Events ..... 149
- Simultaneous Sessions From One Unit..... 149
- Simultaneous Use of Many Units by One Operator ..... 150

**Users..... 151**

- Key Facts ..... 151
  - Before Creating User Accounts ..... 152
- Default User ..... 152
- User Management..... 153
  - Local User Management..... 154
  - Central User Management..... 154
  - Setting a Unit to "Central" User Management ..... 155

Adding an Account, Using Admin and View .....	155
Naming Restrictions.....	156
User Groups.....	157
Updating an Account .....	157
Adding an Account in LocalView .....	157
Updating an Account in LocalView.....	158
Granting Rights.....	158
To Customize the Rights in an Account .....	158
To Base Rights On Those of Another User .....	159
User Rights and Security .....	159
To Deny Access.....	159
Removing a User's Account .....	160
To Delete an Account Used Onsite, to Access LocalView.....	160
<b>Security for a Multi-Media System .....</b>	<b>161</b>
Security Options.....	161
Securing the Multi System .....	161
Security Priorities .....	162
Limiting the Use of Admin.....	163
To Limit Access to Admin Documentation .....	163
Password Guidelines .....	163
Passwords.....	164
Multi Database Security.....	165
SQL-Server Option.....	165
SQL-server Type Logon, Reserved for Multi Operators.....	165
System Password.....	166
Road Map to Setting the System Password.....	167
Changing the System Password, Part 1 (of 3): Using Admin.....	168
Changing System Password, Part 2: Multi-Media Units .....	168
Changing System Password, Part 3: Updating Users .....	169
Status Report .....	169
Removing a System Password .....	169
Remove From All Units .....	170
Remove on One of Many Units.....	171
System Password Extras .....	172
Replacing a Unit .....	172
To Replace a Unit when a System Password Is in Force .....	173
Last Valid Password.....	174
If A Used Unit Comes from Another Multi System .....	174
To Re-enter a Site Definition for a Unit with a System Password .....	175
To Check if the Correct System Password Was Typed .....	176
User Password .....	176
Administrator Password.....	176
To Set the Administrator Account's Password.....	177
Rights of User Accounts.....	178
Guidelines .....	179
To View the Rights of a User and the Sites He may Access.....	179
Right to Use Admin .....	180
To Grant Access to Admin.....	180
Right to Use Maintenance.....	180
Right to Use View .....	181
Right to Access a Site.....	182
To Define an Account's Access to Certain Sites.....	182
Limiting the Time that a Unit Can Be Used .....	183
To Limit Use of Cameras: Camera Partitioning.....	183
High-Security Considerations.....	184

Events Defined .....	187
Setting an Event to Trigger an Alarm or to Be Logged .....	187
Setting an Alarm.....	188
To Set an Event to Report an Alarm .....	188
Logging an Event.....	189
Event Reference .....	190
Tracing Events.....	191
Event Session: to Search the Log of Events .....	193
To Input Times and Dates.....	194
To Set the Date of a Retrieval Using the Calendar Utility.....	194
Results.....	194
To Print a Log Entry .....	194
System Failure.....	194
A Multi-Media Alarm Station.....	195
Alarm Notification: Response Priority.....	195
PPP Connectivity .....	196
Denying Access.....	196
To Stop a Session on a Networked Multi-Media Unit .....	197
Denying Access .....	198
To Deny Access to a User of Your Multi System.....	198
Removing Multi-Media Software .....	199
<b>Multi-Media Alarm Stations .....</b>	<b>201</b>
Overview .....	201
Checklist to Configure a Multi-Media Alarm Station .....	202
Operator Needs .....	202
Multi SA Needs.....	202
System Administrator Needs .....	202
Adding an Alarm Station: Name and Reports .....	203
Identifying and Defining a Connection .....	203
The PPP Fields in an Alarm Station's Definition .....	204
Network Connection to an Alarm Station.....	205
To Setup a Network Connection to an Alarm Station .....	205
Network Address Translation for Alarm Stations .....	206
To Prepare a Multi-Media Unit for NAT, Using Admin.....	207
Dial-up Connection to an Alarm Station .....	208
Preparing a Dial-up Connection to an Alarm Station .....	208
To Setup a Dial-up Connection to an Alarm Station .....	209
Entering Area Codes in Site and Alarm Station Definitions .....	210
Customizing a Dial-Up Connection to an Alarm Station .....	211
To View "Update Station to Call in Case of Alarms" .....	213
To Use a Local Call Across Area Codes .....	213
Toll-Free Numbers .....	213
To Use a Long Distance Call in One Area Code .....	213
To Delay the Speed of Dialing .....	213
To Delay the Extension Suffix .....	214
International Dial-up.....	214
To Change Long-distance Prefixes .....	215
RAS Connection to an Alarm Station.....	216
To Setup a Connection to a RAS Server .....	217
Making an Alarm Station Operational .....	218
Using More than one Alarm Station .....	218
Creating Extra Alarm Station Definitions for the same PC .....	218
Disconnection Note .....	218
To List Successful Alarm Callbacks after an Interruption .....	219

Removing an Alarm Station.....	219
Disabling/Enabling Dial-up Server.....	219
Alarms from a De-listed or Unregistered Unit.....	219
To Trace the Unit Sending the Alarm.....	219
To Set a Site to Not Report to a Specific Alarm Station.....	220
<b>Touring Many Sites.....</b>	<b>221</b>
Preliminary Checklist.....	221
Adding a Site Tour.....	222
Default Amount of Time to Display a Unit During a Site Tour.....	222
Customizing a Tour.....	223
To Change the Order of Sites in a Tour.....	223
To Change the Time Spent at a Site, During a Tour.....	224
To Select Another Connection to a Site, During a Tour.....	225
Removing a Tour.....	225
<b>Alarm Log.....</b>	<b>227</b>
Viewing the Log.....	227
To view the log.....	227
Sorting the Log.....	228
Selecting Log Items.....	228
Filtering the Log.....	229
Printing the Log.....	229
To Print a List of Alarms.....	229
Archiving the Log.....	229
To Archive Alarms.....	230
Removing Log Items.....	230
To Delete Alarms.....	230
Alarm Log Data Reference.....	230
<b>Multi Database.....</b>	<b>231</b>
Starting Admin.....	232
To Start Admin.....	232
Obtaining a Multi db.....	232
Using the Default Multi Db.....	233
Contrasting Db Engines.....	233
Using Another Db: Converting.....	234
To Use Another Multi Db.....	234
Impact on View.....	235
Creating a Multi Db.....	235
Naming Restriction.....	236
To Create an Empty, MS-Access-Compatible Multi Db.....	236
SQL-Server Template.....	237
An Empty Multi Database Using Microsoft SQL-Server.....	237
Using Admin to Create a SQL-compatible Multi Database.....	238
Db Based On Another.....	239
To Make a Copy of a Multi Db.....	239
Renaming a Multi Db.....	240
Multi Db: MinAdmin.....	240
Upgrading a Multi db.....	241
Upgrading a Local Database.....	241
To Upgrade a Local Database, without a Connection to the Multi Db.....	242
Producing a Local Database.....	242
To Make a Local Database.....	242

Logging On.....	243
View: Setting the Db .....	243
To Set a Multi Db for View .....	244
Refreshing a Local Database.....	244
To Refresh a Local Database while Running View.....	245
Deleting a Database .....	245
"Cannot Open Db" .....	245
<b>Index .....</b>	<b>247</b>

## Figures

Figure 1–1. To Install View Software, Run the Multi-Media View CD-ROM.	20
Fig. 1–2. To Install <i>Admin</i> Software, Run the Multi-Media Admin CD-ROM.	20
Fig. 1–3. Desktop Icon for Admin software.	21
Fig. 2–1. Where to Click when Adding a Site.	24
Fig. 3–1. Selecting a Network or Dial-up Connection.	30
Fig. 3–2. Dial-up Connection.	30
Fig. 3–3. Automatic Tag Added to a Connection's Name.	31
Fig. 3–4. Irregular Use of Area Codes.	32
Fig. 3–5. Operating a Multi-Media Unit Over a Network.	34
Fig. 3–6. Site Tab's Report of Primary Connections.	35
Fig. 3–7. Using a Direct Connection to Operate a Multi-Media Unit.	36
Fig. 3–8. NAT Configuration for Operating a Multi-Media Unit Over a WAN.	37
Fig. 3–9. NAT Configuration: Changing the IP Address of a Multi-Media Unit.	39
Fig. 3–10. NAT Configuration: Router Settings.	40
Fig. 3–11. Operating a Unit through Many Connections.	43
Fig. 3–12. Listing of Connections (Two) to a Site.	44
Fig. 3–13. Connecting to a Rapid Eye Site through a RAS Server, Transparently.	45
Fig. 3–14. RAS Server's Telephone Number and PPP Information.	46
Fig. 3–15. Connecting to a RAS Server, Before Running View to Operate Units.	47
Fig. 3–16. For Local Calls that Need an Area Code, Customize Dial-up.	51
Fig. 3–17. Customizing an Alarm Station's Telephone Number.	52
Fig. 4–1. Multi-Media Unit Serial Number and Version of Unit Software.	55
Fig. 4–2. Unit Time Using SNTP as a Reference.	56
Fig. 4–3. Different Rules May Apply for Daylight Savings Time in one Time Zone.	58
Fig. 4–4. Setting a Multi-Media Unit's Clock Manually.	59
Fig. 5–1. The Video Tab: Camera Names and Image Settings.	65
Fig. 5–2. The Video Tab: Color, Recording Settings, Motion and PTZ.	67
Fig. 5–3. The Recording Tab, Showing that Three Cameras Are Recording.	68
Fig. 5–4. A Red Dot Is Added to the Icon of a Camera that Is Recording.	69
Fig. 5–5. The Menu for Duplicating Recording Settings (1) or for Restoring Defaults (2).	70
Fig. 5–6. Estimating a Unit's Video Archive.	71
Fig. 5–7. Load on DSP Resources.	72
Fig. 5–8. The Automatic DSP Performance Maximization Window.	73

Fig. 5–9.	The Configure Automatic Optimizations Command.	74
Fig. 5–10.	The Enhanced Preview Window.	75
Fig. 5–11.	Using High or Moderate Resolution, 320 × 240 (NTSC), to Identify a Subject.	76
Fig. 5–12.	Using Low Resolution, 160 x 120 (NTSC) to Show Presence.	77
Fig. 5–13.	To Establish Presence, Lower-Resolutions May Suffice.	78
Fig. 5–14.	Camera Distance Can Be more Important than High Resolutions.	79
Fig. 5–15.	Resolution Gauge for Recordings Made with NTSC Cameras.	80
Fig. 5–16.	Resolution Gauge for Recordings Made with PAL Cameras.	80
Fig. 5–17.	Microsoft Windows' Screen Area Settings.	83
Fig. 6–1.	Assigning a PTZ Driver to a Port on the Multi-Media Unit.	85
Fig. 6–2.	Configuration Settings (4) for a PTZ (3) Camera (2), on the Video Tab (1).	87
Fig. 6–3.	Dartboard Control for PTZ camera, Showing Command Feedback.	89
Fig. 6–4.	Dragging the Mouse Pointer in a PTZ Camera Window.	90
Fig. 6–5.	Using PTZ Zonal Mode.	90
Fig. 6–6.	PTZ Dome Camera without Auto-focus (1) or with, Between the Dots (2).	91
Fig. 6–7.	Programming a PTZ Preset.	92
Fig. 6–8.	Testing Presets on a PTZ Camera.	92
Fig. 6–9.	PTZ Camera: Behavior after Use.	93
Fig. 6–10.	Detail of PTZ Setup for the RapidDome Driver.	95
Fig. 6–11.	Right-clicking in the Tour Programming table reveals the Insert command.	96
Fig. 6–12.	Location of the Program Vector Button.	98
Fig. 6–13.	Setting Up a Privacy Zone on a RapidDome PTZ Camera.	98
Fig. 6–14.	Communication Settings for Intellibus on the Serial Devices Tab.	99
Fig. 6–15.	The Manage Files Dialog Box.	101
Fig. 7–1.	Continuous Recording and Event Recording, on the Recording Tab.	103
Fig. 7–2.	Boost Button.	104
Fig. 7–3.	Example of a Schedule Assigned to a Camera.	106
Fig. 7–4.	Customizing a Schedule.	107
Fig. 7–5.	Breakdown of a Cell into Fifteen-minute Sections.	108
Fig. 7–6.	Using a Schedule for Alarms.	110
Fig. 7–7.	Specifying a Holiday for the Next Few Years.	111
Fig. 7–8.	A Rule's Trigger, Response and Schedule.	112
Fig. 7–9.	Customizing a Rule: Visual Steps.	113
Fig. 7–10.	Status Icons for a Response Rule.	114
Fig. 7–11.	Motion Detection Configuration.	116
Fig. 7–12.	Mask for Motion Detection.	117
Fig. 7–13.	Motion Detection Menu.	119
Fig. 7–14.	CSD Panel, on the Video Tab.	120
Fig. 7–15.	Calibration of Blind-type CSD.	121
Fig. 7–16.	Storage Estimator.	124
Fig. 7–17.	Detail of the Statistics Tab, Showing Storage Statistics.	127
Fig. 8–1.	Statistics Tab, Showing the Clear Storage Button.	129
Fig. 8–2.	Securing a Unit, after Changing Passwords.	131
Fig. 8–3.	File Transfers: to a Unit or from a Unit.	132
Fig. 8–4.	Downloading the System.log File from a Multi-Media Unit.	133
Fig. 8–5.	Enabling the FAULT RELAY.	135
Fig. 8–6.	Enabling the FAULT RELAY Changes the Name of Output6.	135
Fig. 8–7.	Serial Devices Tab Showing "Internal Port–Modem" Data.	138
Fig. 8–8.	Monitor Out Tab, for a Multi-Media Unit's MONITOR OUTPUT 1.	142

Fig. 8-9.	Customer Devices can Include POS Units, such as Cash Registers.	143
Fig. 8-10.	Some Devices can Be Searched for Data such as "No Sale".	144
Fig. 8-11.	Cash Registers, Connected to a Honeywell PIT.	146
Fig. 8-12.	A NetPIT Device on PORT 3, Showing All Serial Interface Values.	146
Fig. 8-13.	Expanded NetPIT device on PORT 3, showing three POS devices.	147
Fig. 8-14.	Audio Tab.	148
Fig. 9-1.	Button for Changing User Management from Local to Central.	154
Fig. 9-2.	Adding a "Night Operator" Account.	156
Fig. 9-3.	Defaults: User Account Rights (1) and Site Access (2).	158
Fig. 10-1.	Logging on to SQL-Server Differs from the Log on to Admin.	166
Fig. 10-2.	System Password.	166
Fig. 10-3.	Securing a Unit.	167
Fig. 10-4.	After Removing a System Password.	170
Fig. 10-5.	The LVP Utility Is Used only when a Unit Replaces another at a Secured Site.	173
Fig. 10-6.	Inputting a Previous Owner's System Password into the LVP Utility.	175
Fig. 10-7.	Assigning Rights to a "Night Operator" Multi-Media Account.	178
Fig. 10-8.	Summary of a User's Rights on the Users Tab.	179
Fig. 10-9.	Account's Limit on Session Time, before Needing to Reconnect.	183
Fig. 10-10.	Limiting an Account's Use of Cameras at a Site.	184
Fig. 10-11.	Identifying a Camera that is Not Recording, in a Live Session.	185
Fig. 10-12.	Overriding a Camera that is not Recording, Using Event Recording.	186
Fig. 10-13.	Sources of Events Include the Unit itself.	187
Fig. 10-14.	Once Acknowledged, Alarms Are Entered into the Multi Db.	188
Fig. 10-15.	A Multi-Media Unit Can Log an Event without Sounding an Alarm.	189
Fig. 10-16.	Events Caused by a Multi-Media Unit or a View Operator.	192
Fig. 10-17.	Search for Events Window.	193
Fig. 10-18.	A Multi-Media Unit Can Be Set to Send Alarms to Specific PCs.	195
Fig. 10-19.	Denying Access (1) and Updating Security for each Site in the Account (2).	198
Fig. 11-1.	A Multi-Media Unit Can Send Alarms to a Specific PC.	201
Fig. 11-2.	Over a Network, Alarm's Are Sent to an Alarm Station's IP Address.	205
Fig. 11-3.	Receiving Alarms from a Multi-Media Unit, over a WAN or the Internet.	206
Fig. 11-4.	Connecting through a WAN to a Multi-Media Alarm Station on a LAN.	207
Fig. 11-5.	To Report an Alarm, a Multi-Media Unit Can Call an Alarm Station.	208
Fig. 11-6.	Area Code Input Is Needed to Reach a Multi-Media Alarm Station.	209
Fig. 11-7.	Connection for an Alarm Station (1) Is Shown also in a Site's Definition (2).	210
Fig. 11-8.	Irregular Use of Area Codes when Units Are Calling an Alarm Station.	211
Fig. 11-9.	Customizing the Dial-up to an Alarm Station in the Site's Definition.	212
Fig. 11-10.	International Prefixes for Use of Rapid Eye Software in North America.	214
Fig. 11-11.	International Prefixes for Use of Dial-up in Rapid Eye Software.	215
Fig. 11-12.	A Multi-Media Unit Can Send Alarms through a RAS Server.	216
Fig. 11-13.	RAS Configuration.	216
Fig. 12-1 .	Adding a Tour Name.	222
Fig. 12-2.	The Default Amount of Time for a Tour of each Unit.	223
Fig. 12-3.	Customizing the Amount of Time that a Multi-Media Unit Is Toured.	224
Fig. 13-1.	Alarm Log	227
Fig. 13-2.	Possible Result of Sorting when Using "Month, Day, Year".	228
Fig. 13-3.	Filtering the Alarm Log.	229
Fig. 14-1.	Data Flow from Admin to View.	231

Fig. 14-2.	Admin Icon on the Windows Desktop.	232
Fig. 14-3.	Specifying the Multi Db.	234
Fig. 14-4.	The Admin Logon Window.	235
Fig. 14-5.	Copying Multi Db Data to another Multi Db.	239
Fig. 14-6.	Options for Generating a MinAdmin Multi Db Template.	241
Fig. 14-7.	The Log On to View.	243

## Tables

Table 1-1	Customer Information: Checklist	22
Table 3-1	Possible Connections to a Rapid Eye Unit	29
Table 3-2	Multiple Dial-up Connections: Decision Chart	34
Table 3-3	IP defaults used by Multi-Media units	36
Table 3-4	Network Address Translation (NAT) Example	38
Table 3-5	Router Mappings: Example for Operation of Multi-Media Units	40
Table 3-6	Automatic Connection Names for a Rapid Eye Site	48
Table 3-7	Default Transmission Control Protocol (TCP) Ports	49
Table 4-1	Effect of Time Zone Setting on Display and Clips	57
Table 4-2	Maintenance Reference Topics	62
Table 4-1	When to Accomplish Maintenance Tasks	63
Table 4-2	Messages from a Unit, During a Maintenance Session	64
Table 5-1	Frame Rate Values (Approximate ips) for Multi-Media DSP Units	70
Table 5-2	Event Recording: Duty Cycle Cutoffs	72
Table 5-3	Recording Resolutions for Multi-Media DSP (pixel × pixel): NTSC and PAL	81
Table 5-4	Recording Resolutions for Multi-Media LT (pixel × pixel): NTSC and PAL	81
Table 5-5	Display Properties for Optimal Rapid Eye Video at Higher Resolutions	82
Table 6-1	PTZ drivers for controllers and domes	88
Table 6-2	Position after Close of Session, for PTZ Cameras	94
Table 6-3	Communications for the Intellibus Device, and for each ACUIX Dome Camera	99
Table 7-1	Contrasting Motion Detection and Motion Search	120
Table 7-2	Number of Cameras: Effect on the Video Archive*	124
Table 7-3	Scheduling of Cameras: Effect on Storage	125
Table 7-4	Frame Rate: Effect on Storage	125
Table 7-5	Impact of Quality Setting on a Unit's Video Archive	126
Table 7-6	Recording Resolution: Effect on the Video Archive	126
Table 7-7	Available Storage: Comparing with One Camera to Nine	127
Table 7-8	Storage Statistics for a Multi-Media Unit	128
Table 8-1	Default Network Communications Settings	136
Table 8-2	System Tab: Default Values	137
Table 8-3	Default Modem and Dial-up Communications Settings	139
Table 8-4	Names of Temporary TCP/IP Addresses, for PPP	139
Table 8-5	Inputs for External Control of MONITOR OUTPUT 1	142
Table 8-6	Special Characters Available for a Search Rule	145
Table 8-7	Stream Availability	149



Table 8-8	Maximum Simultaneous Sessions	150
Table 10-1	Security Priorities	162
Table 10-2	System Password: Status	169
Table 10-3	Maintenance Tasks and Rights of a User Account	181
Table 10-4	Security Happenstance	185
Table 10-5	Event Reference, by Source and Tab	190
Table 10-6	Event: Default Settings for Log and Alarm	191
Table 11-1	Defining a Connection to an Alarm Station	203
Table 11-2	Connection Information Needed for a Rapid Eye site to an Alarm Station	204
Table 11-3	Router Mappings: Example for Unit Callback to Alarm Stations	208
Table 11-4	Area Code Matching, for Site and Alarm Station	211
Table 13-1	Logged Data	230
Table 14-1	A First Log On to Admin: Default Data for MS-Access	233

## Table of Contents

# The Administration of a Rapid Eye System

## Start Here

### Means of Configuring a Rapid Eye Unit

You have the option of configuring a Multi-Media DSP unit for CCTV use:

- **Without using a personal computer (PC).** Using *LocalView*, an interface that runs on the Multi-Media DSP unit, to configure and operate a unit.
- **Using a PC.** Run Honeywell Rapid Eye *Admin software* for the administration of the Rapid Eye system, and *Rapid Eye View software*, to operate Rapid Eye units.
- **Using either.**

### Designated personnel: a Multi SA from your organization

To carry out the setup and supervision of Honeywell Rapid Eye™ Multi-Media DSP units, your organization can designate a System Administrator (Multi SA) for your Rapid Eye CCTV system.

## About Using a PC to Operate Rapid Eye Units

### Using one Rapid Eye unit, or many at once

*Admin software* is used to manage a central database (Multi db) of Rapid Eye Multi-Media DSP units. Older Rapid Eye units (Multi-Media and Multi models) are supported.

*View software* is used to further configure each of the Multi-Media DSP units for: video, audio, POS devices and so on. *View software* can connect to many Rapid Eye units at once, for configuration and for video, live and recorded, alarm sessions and so on.

The information in this guide (publication number K14392) deals almost exclusively with the use of a PC to configure Rapid Eye units. For PC requirements, see the *Please Read this First!*, K14393.

## About Using LocalView Onsite

### Interface for operating one Rapid Eye unit

Configuration made using LocalView applies only to the unit on which it is running. To find out how to use LocalView, the interface offers a context-sensitive Help system.

### Network connection

If a unit is inserted in a common network, LocalView may be needed by installers to enter the unit's IP address. To do so, a Quick Install wizard is available when using LocalView. See the *Multi-Media DSP Unit: Quick Install* broadsheet, K14355.

### Watching your back

If Multi-Media DSP units are only operated remotely, from PCs, you have the option of preventing the unauthorized use of LocalView by locking the interface, using passwords for LocalView.

## Using a PC: Installing Rapid Eye Software

### For Unit Operators: View Software Only

Personnel who operate Multi-Media DSP units—to monitor video, respond to alarms, make video clips—only need View software on their PCs. Use the **View** CD-ROM to install View software only.

Figure 1-1. To Install View Software, Run the Multi-Media View CD-ROM.



### For the Multi SA Only: Admin and View Software

The system administrator of your Rapid Eye system (Multi SA) needs *Admin software* and View software. Use the **Admin** CD-ROM that came with your unit to install both. If security is important to your organization, Honeywell recommends that the **Admin** CD-ROM be used only on the PC of your organization's Multi SA.

Fig. 1-2. To Install Admin Software, Run the Multi-Media Admin CD-ROM.



## First Use: Running Admin Software

The purpose of *Admin software* is to manage information in a Multi db. On first use, starting *Admin software* is as simple as:

1. Double-click the *Admin* icon, shown in figure 1–3. The *Rapid Eye Multi-Media Admin - Logon* window appears.
2. If “Administrator” is not in the **User ID** box, type it.
3. Click **OK** .

**Fig. 1–3. Desktop Icon for Admin software.**



### Rapid Eye central database

A Rapid Eye central database (Multi db) contains information about:

- **Each Rapid Eye site.** Network and dial-up communication settings for each Multi-Media DSP unit. See Multi-Media Site: Connection Configuration, p. 29.
- **Operator accounts.** For Users of *View* software and *Admin software*, including passwords to user accounts, see p. 151.
- **Rapid Eye alarm stations.** PCs that receive alarms from Rapid Eye units. See Multi-Media Alarm Stations, p. 201.
- **Site tours.** Setup of lists of sites and time spent at each. Site tours work only if your organization has two Multi-Media DSP units, or more. See Touring Many Sites, p. 221.

*And so on.*

## Customizing a Unit: View Software

### Using View software for site maintenance

After units are installed and a Multi db is created, *View* software is used to run a Maintenance Session. During a Maintenance Session, a unit's settings can be changed:

- **Unit's Time Zone and Clock.** To identify recorded video, it is important to set a unit's time zone and clock. See page 56.
- **Video.** The resolution of *recorded video* can be set and the monitor settings of Microsoft Windows can be adjusted. See Video Feed Setup, p. 65.
- **Site hardware.** *View* is used for unit and hardware settings. See Configuring Other Hardware, p. 129.

*And so on.*

## For Questions

### In-depth reference

Most systems require *only a few pages of this guide* to make everything work. Use the table of contents and index to locate the information that you need. This guide is also available in Adobe *Portable document format* (PDF) while running *Admin software*, and can be searched using Adobe *Acrobat Viewer*.

### Configuration malfunctions

For problems with camera position, wiring, connections to other hardware, see the Unit Installation Instructions , K14390 or please contact the installer of your Multi system.



**In the figures: the names of places and people, the internet protocol (IP) addresses, and other data are for illustration only and should only be a guide when running a Multi system.**

### Calling Honeywell

Call Multi technical support for help with training or general problems. If you do call, please have on hand the information listed in table 1-1. In North America the Multi technical support number is 1 (800) 796-2288. For other locations of Honeywell Video Systems, see the back cover of this publication.

### Table 1-1 Customer Information: Checklist

---

#### Information About Your Rapid Eye Multi System

---

The version of Windows used to run Admin on the PC, such as: Windows XP-Pro.

Connection type. If you are using a dial-up connection to the unit, a list of communication tools used on the PC running Multi software: fax, AOL, CompuServe, and so on, the type of modem, and the telephone number used. For a LAN connection, the Multi-Media unit's IP address, and so on. See Types of Connection, starting on p. 29.

The database used for your Multi db: SQL or Access; see Obtaining a Multi db, p. 232

If you found information about the problem in the user guides.

Is a system password in use? See System Password, p. 166.

---

## Multi-Media Site: Name

### Preparations

#### Road map

A Multi-Media site refers to one Multi-Media unit. Even when there are many units at a “company site”, each unit is considered as one Rapid Eye site. Before setting-up Rapid Eye sites for use by View operators, your Multi System Administrator (Multi SA) should check if:

- Hardware at the Multi site is installed.
- Admin and View software are installed. See Right to Use Admin on p. 180.
- Multi central database is available. Obtained using Admin. See Multi Database, p. 231.
- If the Time zone, Clock, the IP address of the unit may have been already set, onsite, using LocalView. See the *Multi-Media DSP Unit: Quick Install* broadsheet, K14355.

#### Cameras

The **Cameras...** button is useful after you run a Maintenance Session for the site. It lists the names assigned to each camera during the Maintenance Session.

#### Last valid password

Use of the LVP button is explained fully at Last Valid Password, on p. 174.



**Uninformed use of the LVP utility can make a unit unusable and deny access to the unit for all users, including a Multi SA. When adding a new Multi site to your Rapid Eye system, do not use the “LVP” (last valid password) utility, even if you have set a system password on other units.**

The LVP utility is for dealing with replacement Multi-Media units, or mistakenly deleted sites; see Last Valid Password, on p. 174.

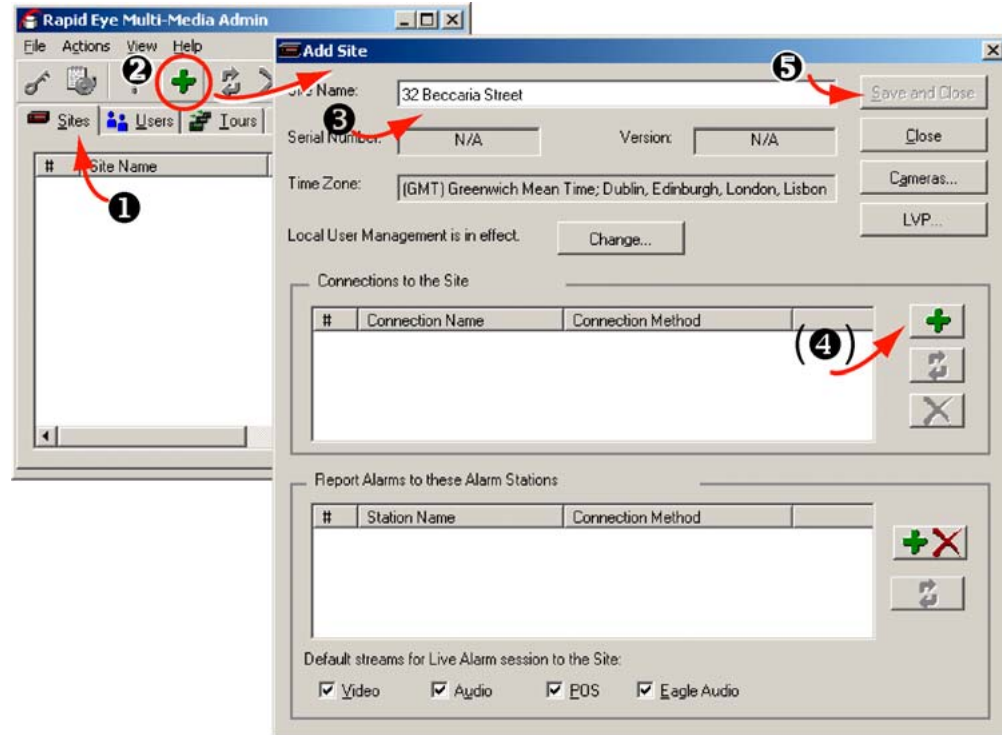
## Site Setup: Checklist




### Four items

- Name the site. See Naming / Renaming a Site.
- Identify the type of connections to the site and add them to the site definition. See Types of Connection.
- Using View, start a Maintenance Session. See p. 53.
- Make the site operational by updating time zone, time and security, as explained in Making a Site Operational, p. 55.

## Naming / Renaming a Site

Fig. 2-1. Where to Click when Adding a Site.



1. Use Admin to display the Sites tab.
2. Display the Add Site dialog box. Click the pane on the right-hand side of the Sites tab, then click . You can also do any one of the following:
  - Click the down-arrow between  and  on the toolbar. On the menu that appears, click **Add Site**.
  - Click the pane on the right-hand side of the Sites tab; then click **Add** on the Actions menu.
  - Click the pane on the right-hand side of the Sites tab; press the Ctrl+Insert keys.
  - Right-click in the pane on the right-hand side of the Sites tab; then click **Add** on the menu that appears.



3. Type a name in the Site Name box. The Multi-Media unit can be referred to by name.
4. Add a connection to the unit.
5. Click **Save and Close**.

## Site Naming Tips

Try to use descriptive names: the address, area in the building, use of the facility and so on. The goal is to avoid confusion in an emergency.

- Beware of placing an address next to a site number. Some addresses can lead to confusion.

For example:

“Site 26, 2607 Blue Jay Way” and

“Site 27, 2609 Blue Jay Way”.

A better alternative could be:

“site 26, corner house at 2607 Blue Jay Way”

“site 27, east parking lot, 2609 Blue Jay Way” or

“corner house at 2605 Blue Jay Way (site 26)”

“east parking lot, 2609 Blue Jay Way (site 27)”.

- Beware of long names that differ only at the end.  
For example, avoid “parallel phrasing” to identify sites by building, floor, area and target can lead to operator error due to a small difference only, located at the end of the identifier:  
“Rosde building, 1st floor, mezzanine east, lobby entrance” and  
“Rosde building, 1st floor, mezzanine east, lobby desk”  
Better use of parallel phrasing could be:  
“lobby, Rosde, mezzanine east” and  
“front desk, Rosde, mezzanine east”.

## After Dealing with a Site

You have the option of using Admin to:

- Create users. The sites that a user can access are listed in a user's account. See Granting Rights, on p. 158.
- Make the sites part of a site tour. After setting up a tour, View displays the sequence of video feeds from different sites. See Touring Many Sites.
- Alarm station. You can designate which alarm station(s) receives alarm reports. See Cascading Alarm Stations. For procedures to connect Rapid Eye units to an alarm station, see Multi-Media Alarm Stations, starting on p. 201.
- Groups of sites. See Grouping Sites.
- System password. Use of a system password is highly recommended by Honeywell. After a system password is set using Admin, update the security on each unit in your Rapid Eye system. See System Password, p. 166.

## Grouping Sites

### Flexibility

Grouping sites is optional and applies only to organization's with two or more Multi-Media units.



### Folders for grouping sites

As in a filing system, Multi-Media sites and Multi sites can be grouped, by assigning their names to a folder. A site cannot be duplicated or copied to another folder.

## To Create a Folder

1. Using Admin, click the Sites tab.
2. The many ways of creating a folder are for your convenience. Use any one. Either:
  - Click the pane on the left-hand side of the Sites tab; then click **Add** on the Actions menu.
  - Click the pane on the left-hand side of the Sites tab; then press the Ctrl+Ins keys.

- or -


  - Right-click in the pane on the right-hand side of the Sites tab; then click **Add** on the menu that appears.
3. Click the arrow in between the  and  on the toolbar; then click **Add Folder** on the menu that appears.
4. Type a name in the box next to the folder icon.
5. Save the name by either: pressing the Enter key or click outside of the box holding the name.

## To Assign a Site to a Folder


Do any of the following:

- Using the mouse, click and drag a site; drop it on a folder. When the mouse button is released, the folder into which the site was dropped is opened.
- A site can be assigned from a folder back to the root of the database in the same way: by clicking and dragging the site from the folder.
- One or many sites can be assigned to a folder at the same time. Press the Ctrl key while selecting sites that are not sequential in a list; then drag the lot to another folder or the root. Holding the Shift key while clicking sites selects those sites and all sites in between.

## To Rename a Folder

1. Using Admin, click the Sites tab.
2. Select a folder; then, either:
  - Click the folder's name again, once.
  - Click  , on the toolbar
  - or -
  - Right-click the folder's name; then click **Update** on the menu that appears.
3. Save the folder's name. Either:
  - Press the Enter key
  - Click elsewhere in the View window
  - or -
  - Switch to another Windows application.

## To Delete a Folder

1. Using Admin, click the Sites tab.
2. Click a folder.
3. Either:
  - Press the Delete key on the keyboard,
  - Click **Delete** on the Actions menu, or click  on the toolbar.
  - Right-click the site name; then click **Delete** on the menu that appears.
4. If the folder you are deleting contains a site or a folder and so on, the folder's contents are listed. To confirm that you want to delete the folder, click **Yes**.

## Grouping Folders

Folders can be assigned to other folders or back to the root of the database. The same name can be used for two folders that are not in the same branch.

### To assign a folder to a folder

- Using the mouse, click and drag a folder; drop it on another folder. When the mouse button is released, the folder into which the folder was dropped is opened.
- Assigning a folder to another, or the to the database root, also assigns its contents, including sites and sub-folders.

### To collapse or expand sub-folders

Either double-click a folder or click + or - on the folder's left. These + and - act as a toggle: alternately expanding and collapsing a set of sub-folders.

## Removing a Site


Honeywell recommends that before deleting a site definition, you remove the system password from that Multi-Media unit. See Removing a System Password, on p. 169. You do not need to remove the system password from all sites; only on the unit being deleted from your Multi db.



**If the site password is not removed from the unit, you will need to remember it when you create another site definition for that Multi-Media unit. The system password is also needed if you delete a site definition by mistake.**

## To Delete a Site

Deleting a site in the Multi central database has no effect on the Multi-Media unit at that site. The unit continues to record video, send alarms and so on, even once the local databases of users are refreshed. The unit's system password remains in force.

1. You have the option of going to the Rapid Eye Site to physically disconnect the Multi-Media unit from its means of communications.
2. Check if a system password is in use. If so, you have the option of removing the system password from the Multi-Media unit. If you do not need to protect the video and other recorded data from access, it is strongly recommended that you remove the system password from the unit. See Removing a System Password, on p. 169.
3. Using Admin, select a site name, listed on the Sites tab.
4. Remove the site by either:
  - Press the Delete key on the keyboard,
  - Click **Delete** on the Actions menu, or click  on the toolbar.
  - Right-click the site name; then click **Delete** on the menu that appears.
5. The site's dependencies are listed. Confirm that you want to delete the site.

## Mistakenly Deleting a Secured Site Definition

When a system password is in use and a site is deleted by mistake, you need a few extra steps to re-enter the site definition. The system password is left in use on the unit, by default. For the procedure to re-enter information about a mistakenly deleted site that is protected by a system password, see Last Valid Password, on p. 174. You can read about how to add a site in Naming / Renaming a Site, on p. 24.

## Multi-Media Site: Connection Configuration

### Types of Connection

Connections can be: dial-up or network. Alternatively, a direct connection between a PC and a unit can also be used. A connection is not needed to use LocalView. A checklist of the information needed for each type of connection is listed in table 3-1.

**Table 3-1 Possible Connections to a Rapid Eye Unit**

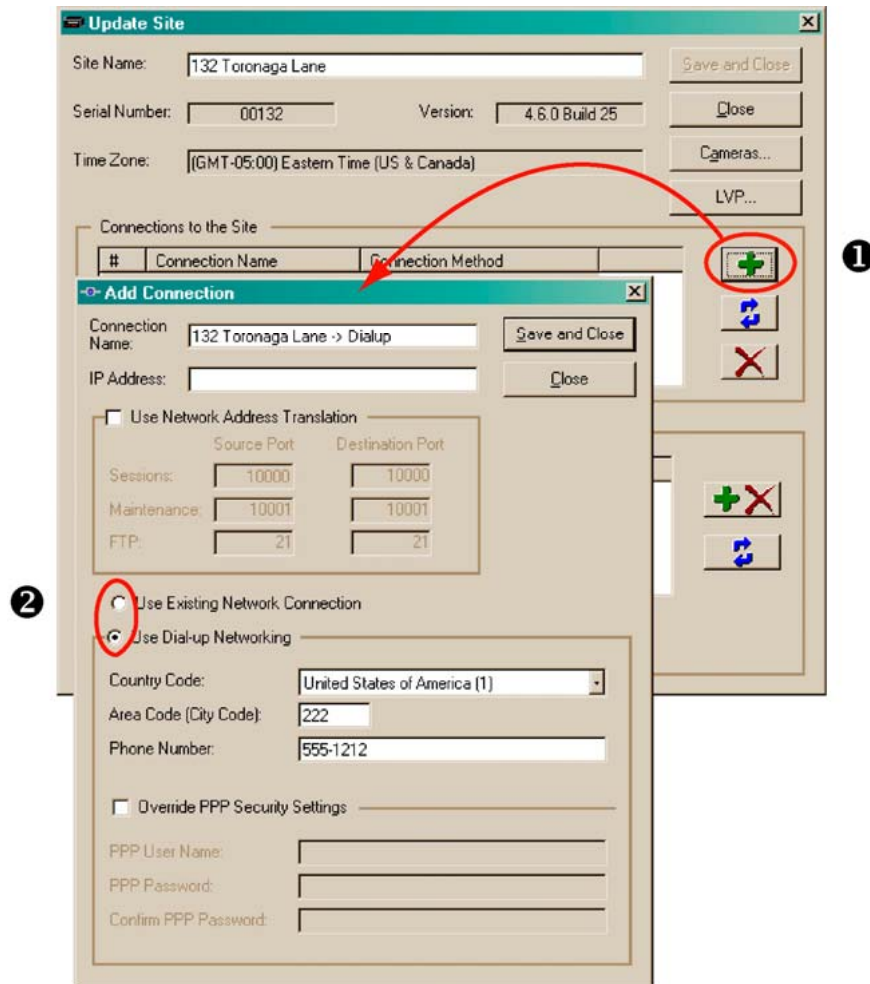
<b>For a Connection Using ...</b>	<b>A Multi SA Needs ...</b>
dial-up to a remote Multi-Media unit	- telephone number to reach unit, p. 30
dial-up making irregular use of an area code.	- telephone number to reach unit, p. 30 - to customize a dial-up connection, p. 32
network access	- standalone PC with network card, p. 36 - IP address of the unit, p. 34, or DHCP available on the network, p. 41 - open port in firewall, p. 49
a combination of dial-up or network access	- IP address of the unit, p. 43 - port in firewall, p. 49 - telephone number to reach unit, p. 30
including a remote access service (RAS) server in a connection to a Multi-Media unit. Requires overriding point-to-point protocol (PPP).	- RAS server account, p. 44 - its PPP password, p. 196 - telephone number to reach RAS - IP address of Multi-Media unit(s), p. 47 - port in firewall, p. 49
dial-up to a RAS server, before accessing one or many Multi-Media units at once, on the same remote network	- IP address of Multi-Media unit, p. 47 - PPP password, p. 196 - telephone number to reach RAS - port in firewall, p. 49 - PC operator: needs RAS account, p.44

#### **Naming and viewing a connection**

Connections are named automatically, but they can be renamed. See The Automatic Naming of Connections, p. 48, and Changing the Automatic Suffix in a Connection's Name, p. 48.

The primary connection of a site is displayed on the Sites tab; See figure 3-6, p. 35.

**Fig. 3-1. Selecting a Network or Dial-up Connection.**

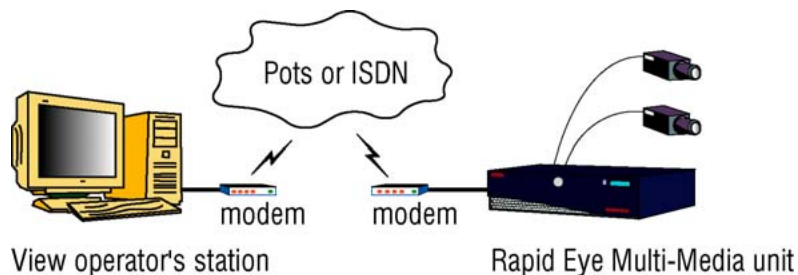


## Dial-up Connection: to a Unit

Using a modem (i.e., dial-up), an operator can connect to a Multi-Media unit. The modems can be internal or external.

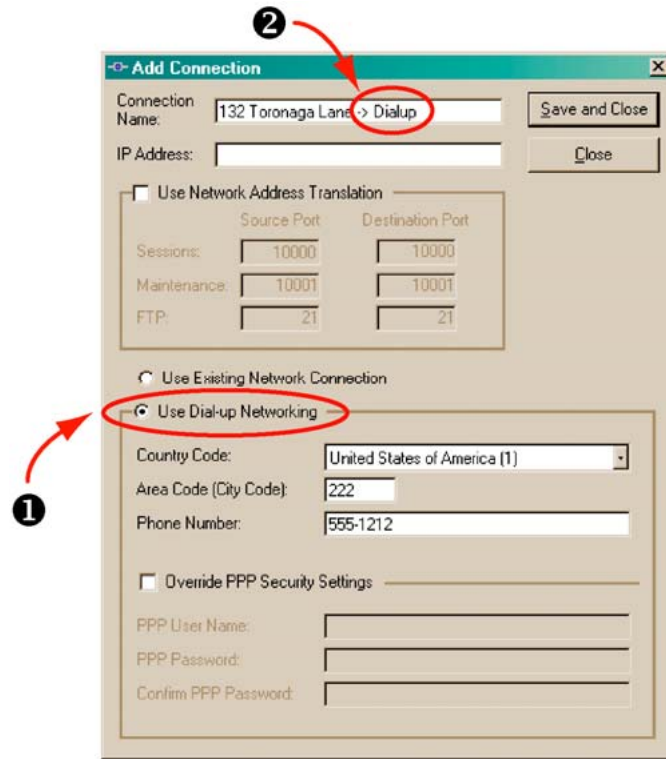
A dial-up connection is optional. For other means of connecting to a Multi-Media unit, see table 3-1 on p. 29.


**Fig. 3-2. Dial-up Connection.**



## Setting a Dial-Up Connection

Fig. 3–3. Automatic Tag Added to a Connection's Name.

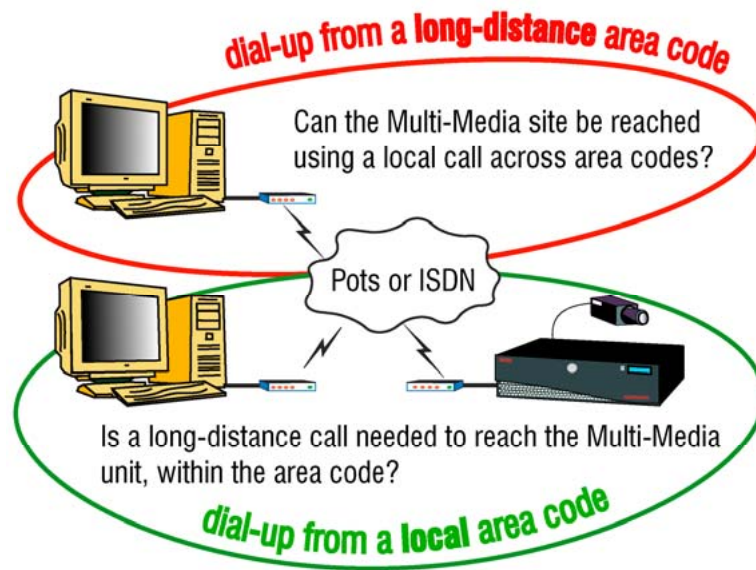


1. While adding a site (as in Naming / Renaming a Site, above) or updating one, click  in the “Connections to the Site” pane. The Add Connection dialog box is displayed. Leave the IP Address box empty for a dial-up connection to a Multi-Media unit.
2. Click **Use Dial-up Networking**. See figure 3–3, above. Admin automatically names the connection in the Connection Name box from “-> Network” to “-> Dialup”. See fig. 3–3. You have the option of keeping the name or of typing another.
3. Leave the Country Code to “(dialing same country)”, unless the Multi-Media unit is in a different country than the View operator planning to use the site.
4. Type the unit’s Area Code (City Code) and Phone Number obtained from your network administrator (this is mentioned in section Preparations, on p. 23). If a prefix number is needed to access an outside line, set the prefix—the extra telephone keystroke such as a “9” or an “8”—in Window’s Telephony program.
5. Click **Save and Close**. An “Add Site / Update Site” window is displayed.
6. Click **Close**. The Sites tab appears. In the tab’s Primary Connection column, the first letter of “dial-up” appears in parentheses: (d), followed by the telephone number used to connect to the Multi-Media unit.

Should you plan to add alarm stations, dial-up connections from a Multi-Media unit to an alarm station are explained in section Dial-up Connection to an Alarm Station, on p. 208.

## Area Code: Irregular Use

Fig. 3-4. Irregular Use of Area Codes.





Irregular use of area codes occurs when making:

- A long distance call within one area code.
- A local call to another area code.



You can easily deal with these scenarios (see figure 3-4, above) by using Admin to modify or add another dial-up connection. If a prefix number is needed to access an outside line, set the prefix—the extra telephone keystroke such as a “9” or an “8”—in Window's Telephony program.

## To Force a Long-distance Dial-up Using a Local Area Code

1. In the “Connections to the Site” pane of the Add Site / Update Site dialog box (as in Naming / Renaming a Site), click either:  
 to add a connection. The Add Connection dialog box appears.  
- or -  
 to update a connection. The Update Connection dialog box appears.
2. Click **Use Dial-up Networking** as needed.
3. In the Connection Name box, you have the option of appending a few words such as “force long distance call”. It makes sense to do so, to avoid confusing operators of View.
4. In the Phone Number box, type the telephone number needed to reach the unit, including country and long distance codes.
5. Leave the Country Code and Area Code (City Code) boxes empty. Steps 4 and 5 fool Windows' Dial-up Networking into making a local call across different area codes. Click **Save and Close**. An “Add Site / Update Site” window is displayed.
6. Click **Close**. The Sites tab appears. In the tab's Primary Connection column, the first letter of “dial-up” appears in parentheses: (d), followed by the telephone number used to connect to the Multi-Media unit.



## Forcing a Local Dial-up Across Area Codes

1. In the Add Site/Update Site dialog box (as in Naming / Renaming a Site), in the "Connections to the Site" pane, click either:
  -  to add a connection. The Add Connection dialog box appears.
  - or -
  -  to update a connection. The Update Connection dialog box appears.
2. Click **Use Dial-up Networking**.
3. In the Connection Name box, append a suggestive name such as "force local call".
4. In the Phone Number box, type only the telephone number needed to reach the unit.
5. Leave the Country Code and Area Code (City Code) boxes empty. Steps 4 and 5 fool Windows' Dial-up Networking into making a local call across different area codes.
6. An "Add Site / Update Site" window is displayed.
7. Click **Close**. The Sites tab appears. In the tab's Primary Connection column, the first letter of "dial-up" appears in parentheses: (d), followed by the telephone number used to connect to the Multi-Media unit.

## Dial-up Technical Note

### PPP

During a dial-up connection, temporary TCP/IP network communications are established between the Multi-Media unit and the PC. These default point-to-point protocol (PPP) Internet Protocol (IP) settings can be changed, should they conflict with other network devices (printers, scanners and so on). See Serial Device: Modem, on p. 138.

### Should you plan to add an alarm station

Should you plan to add one or more alarm stations using dial-up connections, Honeywell recommends that area codes be included in all telephone numbers. Dial-up connections between a Multi-Media unit and an alarm station running View are explained in Dial-up Connection to an Alarm Station, on p. 208.

## Offering Many Dial-Up Connections to the Same Unit

More than one dial-up connection to the same Multi-Media unit may be needed. Table 3–2 lists configurations, and the number of connections for best results. For example, Windows Dial-Up Networking can give unwanted results when some View operators are inside the Multi-Media unit's local calling area and others are outside. Telephone companies can also force a Multi SA to setup an irregular local call—a local call across area codes.

**Table 3–2 Multiple Dial-up Connections: Decision Chart**

Operator's PC (location)	Call to Unit (type)	Procedure (name, page)	Connections (number of)
in unit's calling area	local	Dial-up Connection: to a Unit, p. 30	1
	irregular long distance: same area code	Area Code: Irregular Use, p. 32	1
	irregular long distance: local call	Dial-up Connection: to a Unit, p. 30 & Area Code: Irregular Use, p. 32	2
outside unit's calling area	long distance	Dial-up Connection: to a Unit, p. 30	1
	irregular local call: not requiring area code	Area Code: Irregular Use, p. 32	1
some in, some out of unit's calling area	permutations of all of the above	Dial-up Connection: to a Unit, p. 30 & Area Code: Irregular Use, p. 32	from 2 to 4
in another country	international long distance	Dial-up Connection: to a Unit, p. 30	1
some out of site's country	all permutations	Dial-up Connection: to a Unit, p. 30 & Area Code: Irregular Use, p. 32	from 2 to 5

## Using Network Access


**Fig. 3–5. Operating a Multi-Media Unit Over a Network.**



### Flexibility

A network connection is optional. For other means of connecting to a Multi-Media unit, see table 3–1 on p. 29.

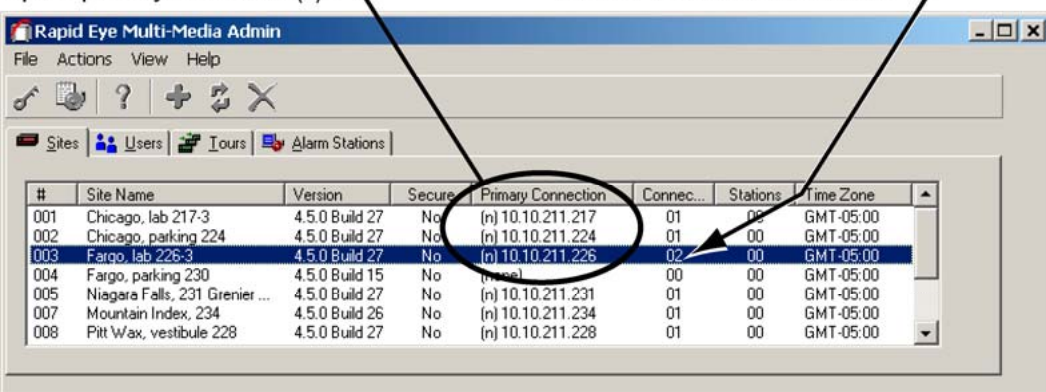
## To Set a Network Connection

- In the Add Site/Update Site dialog box, click  in the “Connections to the Site” pane. The Add Connection dialog box appears. In the Connection Name box, a stylized arrow and “Network” are appended to the site’s name.
- Before typing into the IP Address box, find out whether you are dealing with a:
  - Common network, without DHCP (or with DHCP disabled) - type a static IP address, obtained from the unit’s installer or network administrator, as mentioned in section Naming / Renaming a Site. Continue this procedure.
  - Standalone unit (unit not on a network and the PC that runs Admin software has a network card) - type a static IP address. You can match the network settings of Microsoft Windows running on the PC to either the unit’s default, listed in table 3–3 on p. 36. See Standalone Unit and a PC that Has a Network Card.
  - One IP for many destinations - type the static IP address of an internet router. Network address translation (NAT) and port address translation (PAT) values are obtained from the network administrator; see Network Address Translation, p. 37.
  - Network using DNS and a DHCP server - Obtain the site serial number, printed on a sticker affixed to the unit, for use in the computer name for the Multi-Media unit. The format for the name is: “REM[hyphen][site serial number (without the leading zeroes)]”. For example: REM-7654321. Type this computer name in the Connection Name box. See also Dynamic Host Configuration Protocol.
  - DHCP server, without DNS - type the IP address reserved by DHCP for the unit. Contact the administrator of your network, to obtain a reserved IP address; otherwise the address will change, compromising attempts to connect to the unit. See Dynamic Host Configuration Protocol.
- Name the connection, either by:
  - Leaving the name set by Admin in the Connection Name box.
  - Typing another name in the Connection Name box.
- Click **Save and Close**. The “Add Connection” window remains open.
- Click **Close**. The Sites tab appears. In the tab’s Primary Connection column, the first letter of “network” appears in parentheses: (n), followed by the IP address used to connect to the Multi-Media unit. See figure 3–6.

**Fig. 3–6. Site Tab’s Report of Primary Connections.**

report: primary connection(s) →

number of connections to site →

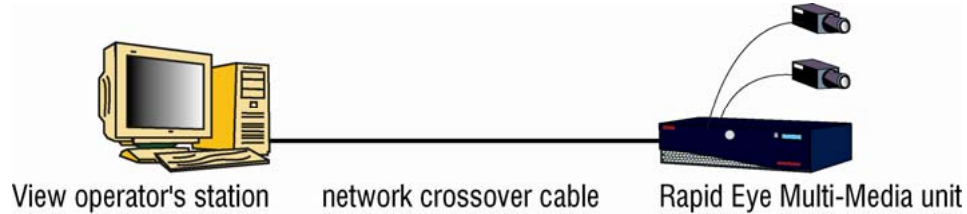


#	Site Name	Version	Secure	Primary Connection	Connec...	Stations	Time Zone
001	Chicago, lab 217-3	4.5.0 Build 27	No	(n) 10.10.211.217	01	00	GMT-05:00
002	Chicago, parking 224	4.5.0 Build 27	No	(n) 10.10.211.224	01	00	GMT-05:00
003	Fargo, lab 226-3	4.5.0 Build 27	No	(n) 10.10.211.226	02	00	GMT-05:00
004	Fargo, parking 230	4.5.0 Build 15	No	(n) 10.10.211.230	00	00	GMT-05:00
005	Niagara Falls, 231 Grenier ...	4.5.0 Build 27	No	(n) 10.10.211.231	01	00	GMT-05:00
007	Mountain Index, 234	4.5.0 Build 26	No	(n) 10.10.211.234	01	00	GMT-05:00
008	Pitt Wax, vestibule 228	4.5.0 Build 27	No	(n) 10.10.211.228	01	00	GMT-05:00

## Standalone Unit and a PC that Has a Network Card

To use a direct connection to a Multi-Media unit, you need a network crossover cable.

**Fig. 3-7. Using a Direct Connection to Operate a Multi-Media Unit.**



### Tip

For other means of connecting to a Multi-Media unit, see table 3-1 on p. 29.

#### LocalView

For a single Multi-Media unit or Multi-Media LT unit, onsite operators have the option of using LocalView instead of a PC. See About Using LocalView Onsite, on p. 20.

#### Network-like connection

For standalone PCs connected directly to a unit, using a network crossover cable, use a network connection. Match the network settings of Microsoft Windows running on the PC to the default address, subnet mask and gateway of the Multi-Media unit. The defaults are listed in table 3-3, below.

#### Static network settings, default for Multi-Media unit

The defaults in table 3-3 can be changed using:

- View, to run a Maintenance Session. See System Tab in a Maintenance Session, on p. 134.
- LocalView, onsite.

**Table 3-3 IP defaults used by Multi-Media units**

Point	Address
IP Address	172.25.2.1
Subnet Mask	255.255.0.0
Gateway	172.25.100.4

# Network Address Translation

## In a nutshell

A connection to one or many Multi-Media units, using one IP address, can be made by using network address translation (NAT) also called port address translation (PAT). This is useful to connect to Multi-Media units through: a WAN, the Internet or to another segment of the same LAN. The key is to configure a router to translate and map the Sessions source IP port.

## IP Addresses

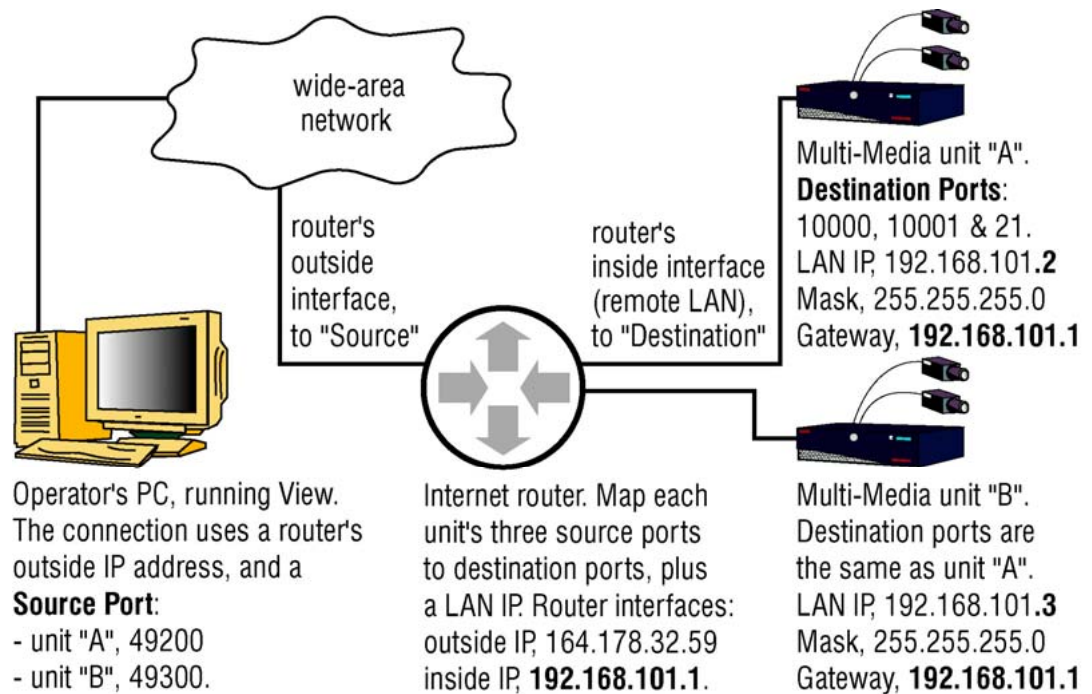
The Network Administrator of the destination's LAN can supply a Multi SA with:

- the Inside IP address and Outside IP address of the internet router
- the LAN IP addresses that are assigned to each unit. See the example in table 3-4, below.

## IP Port

For each Multi-Media unit on a remote LAN, set a different router Sessions value, under Source Ports, in the Add Connection/Update Connection dialog box of Admin software. Figure 3-10, shown further below, shows where to enter this value. The router uses the value to route commands to the proper unit, on the remote LAN.

**Fig. 3-8. NAT Configuration for Operating a Multi-Media Unit Over a WAN.**



**Table 3–4 Network Address Translation (NAT) Example**

Item	Data Field	IP Address/Port	Data Source/Comment
router		router's software	
	WAN / Outside IP*	164.178.32.59	Used also in Admin for the connection definition.
	LAN / Inside IP* Port(s)	192.168.101.1 For port mappings, see table 3–5, p. 40.	Is also unit's IP gateway map source to destination
Multi-Media	Connection dialog box	in Admin software	
unit "A"	IP Address	164.178.32.59	router: Outside IP address
	Session Source Port	49,200	Multi SA
	System tab	in View software	
	(Inside) IP Address	192.168.101.2	Network Admin
	Subnet Mask	255.255.255.0	Network Admin
	Gateway	192.168.101.1	router: Inside IP address
unit "B"	Connection dialog box	in Admin software	
	IP Address	164.178.32.59	router: Outside IP address
	Session Source Port	49,300	Multi SA
	System tab	in View software	
	(Inside) IP Address	192.168.101.3	Network Admin
	Subnet Mask	255.255.255.0	Network Admin
	Gateway	192.168.101.1	router: Inside IP address

\* The name of the data field may vary. See the router's documentation.

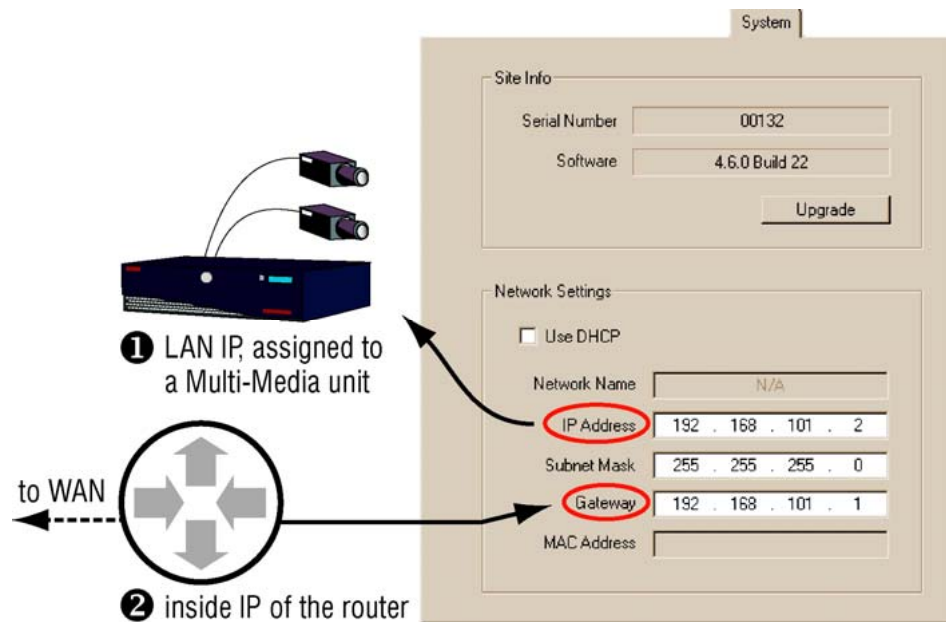
Four procedures are needed to setup a connection to use NAT:

- Adjusting a Unit's IP Settings for NAT
- Setting a Router's Mappings
- Updating a Unit's Connection and
- Refreshing the Multi-Media Local Db.

For each Multi-Media unit on the destination LAN, use these procedures.

## Adjusting a Unit's IP Settings for NAT

Fig. 3-9. NAT Configuration: Changing the IP Address of a Multi-Media Unit.



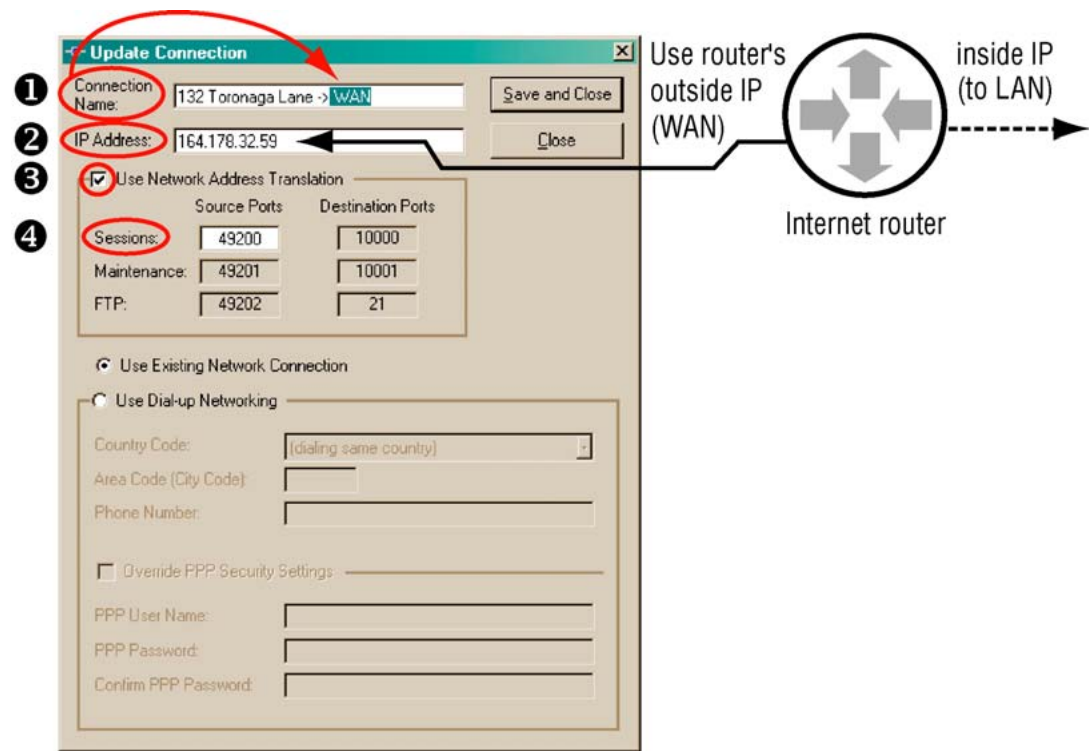
1. Ask the network administrator of the remote LAN for the unit's:
  - IP Address
  - Subnet Mask
  - Gateway. The Gateway on the unit matches the router's Inside IP address; for example, in figure 3-9, it is set to 192.168.101.1.
2. Enter the values obtained in step 1 using either:
  - LocalView software, onsite. Click the Setup tab and then click the System tab. Use the buttons in the Network Settings box.

- or -

  - A PC that runs View and that can connect to the Multi-Media units. Run a Maintenance Session to the unit. The values are entered on the System tab. See figure 3-9. This locks out View operators from further use of the unit until the router and Multi db are updated. See Setting a Router's Mappings and Updating a Unit's Connection. Operators using LocalView are not locked out.

## Setting a Router's Mappings

Fig. 3-10. NAT Configuration: Router Settings.



Supply the three destination ports for Multi-Media unit to the network administrator of the router. Indicate that they need to be mapped to the Outside IP Source Ports on the router, and to the unit's LAN IP Address. See table 3-5, below, or figures 3-8 and 3-10.

Table 3-5 Router Mappings: Example for Operation of Multi-Media Units

Admin settings to: destination		Network device: mappings	
NAT Port (to network device)	Device's Outside IP (constant)	Physical Port (firewall & unit)	Inside IP (unit's address)
unit "A"			
Session: 49,200*	164.178.32.59	>	10,000 192.168.101.2
Maintenance: 49,201	as above	>	10,001 map as above
FTP: 49,202	as above	>	21 map as above
unit "B"			
Base: 49,300*	same IP as above	>	10,000 192.168.101.3
Maintenance: 49,301	as above	>	10,001 map as above
FTP: 49,302	as above	>	21 map as above

\* Values are arbitrary. Consult the network administrator for appropriate NAT port values.



## Updating a Unit's Connection

1. Using Admin software, add (or update) a connection to a site. You have the option of renaming the suffix in the connection name to "WAN", "Internet" or other useful reminder of what type of connection is being set up. See figure 3–10.
2. Assign the router's outside IP address to the IP Address box.
3. Enable Use Network Address Translation.
4. Assign a value to the NAT Sessions Source Port. In figure 3–10, for example, the value of Sessions has been changed from 10,000 (the default) to 49,200. A value greater than 65,533 cannot be used.
5. Click **Save and Close**. To access the unit using View software, see Refreshing the Multi-Media Local Db.

## Refreshing the Multi-Media Local Db

Operators connected to the Multi Central database can either:

- If View is running, click **Refresh**.
- If View is not running, run View.

For operators that are not connected to the Multi Central database, your organization's Multi SA needs to supply each of them with an updated Local database. See Producing a Local Database, on p. 242.

## Dynamic Host Configuration Protocol

### Flexibility

Multi-Media units support the Dynamic Host Configuration Protocol (DHCP). By default, Multi-Media units are not clients of DHCP.

### Network administrator needs for using DHCP with DNS

The DNS registration of DHCP leases is made with the DNS specified by the DHCP server, network card properties. Contact your organization's Network administrator to obtain the proper primary DNS entry for your local client if the name is not resolved.

## To Configure DHCP Using Microsoft's Server2000 (or 2003)

1. Using the DHCP MMC, open the local DHCP Server Properties window.
2. On the DNS (Dynamic Network Service) tab, select Always update DNS.
3. Add a checkmark to the box next to Enable updates for DNS clients that do not support dynamic update.
4. Restart the DHCP service.

## Choosing the Computer Name or a Static IP

### In the IP Address box

With DHCP, your network administrator has the option of assigning either a dynamic IP address or static IP address to a Multi-Media unit. See the procedure: To Set a Network Connection, on p. 35.

Either a dynamic IP address or computer name. For units on a DHCP-enabled network, registration of DHCP leases is made with the DNS specified on the Properties of the network card in the DHCP server. If the name is not resolved, contact the Network administrator to obtain the proper primary DNS entry for your local client. When performing procedure To Set a Network Connection, on p. 35, a Multi SA types a computer name in the IP Address box of a Multi site's definition (instead of an IP address). A computer name for a Multi-Media unit is:

"REM[hyphen][site serial number (without leading zeroes)]";

for example: REM-7654321.

The unit's serial number is printed on a sticker affixed to the unit and may contain leading zeroes.

Static IP address. Within DHCP, your network administrator has the option of reserving an IP address after it has been assigned to a Multi-Media unit. The Multi SA types this address in the IP Address box of a Multi site's definition, instead of a unit's computer name. If for some reasons it is not practical to match the DNS entries, it is then preferable to use the local hosts or lmhosts file to match a reserved DHCP loaned IP with a multi NetBIOS name. The IP needs to be reserved in the DHCP server by the network administrator for using the hosts or lmhosts file.



**Within DHCP without DNS, an assigned IP address needs to be reserved or it will change. Let the network's administrator as well as the Multi SA know of the unit's installation; as a unit is reset, a new DHCP address is assigned to it and communication to the unit could be hampered if configured incorrectly.**

### Network without DHCP

If DHCP is unavailable on your network, a unit's request for DHCP services times-out after two minutes.

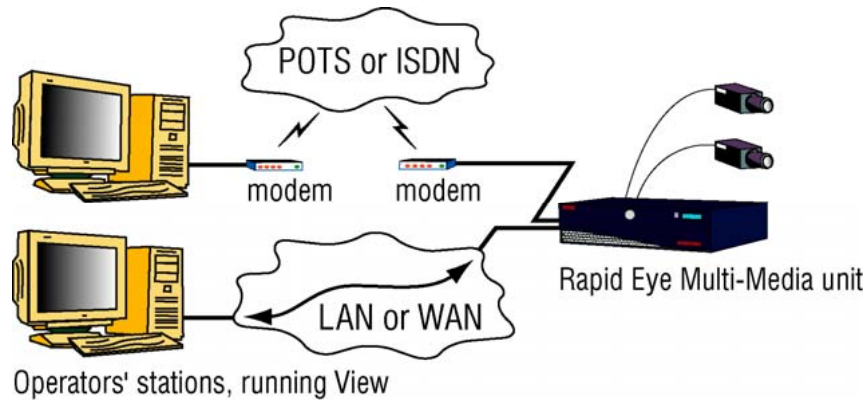
### More about DHCP

Further discussion of DHCP is beyond the scope of this *System Administrator's Guide*. Consult IT personnel for information about DHCP.

## Many Connections to a Unit

Depending on your organization's needs, you can have one or many types of connections. There can be a mix of network and dial-up connections. A dial-up connection can be simultaneous with many network connections.

**Fig. 3-11. Operating a Unit through Many Connections.**



### Tip

**Setting up many connections is optional.**

For other means of connecting to a Multi-Media unit, see table 3-1 on p. 29.

## To Specify Dial-up and Network Connections

Using the "Update Site" dialog box (or "Add site" dialog box), you can set as many connections as needed.

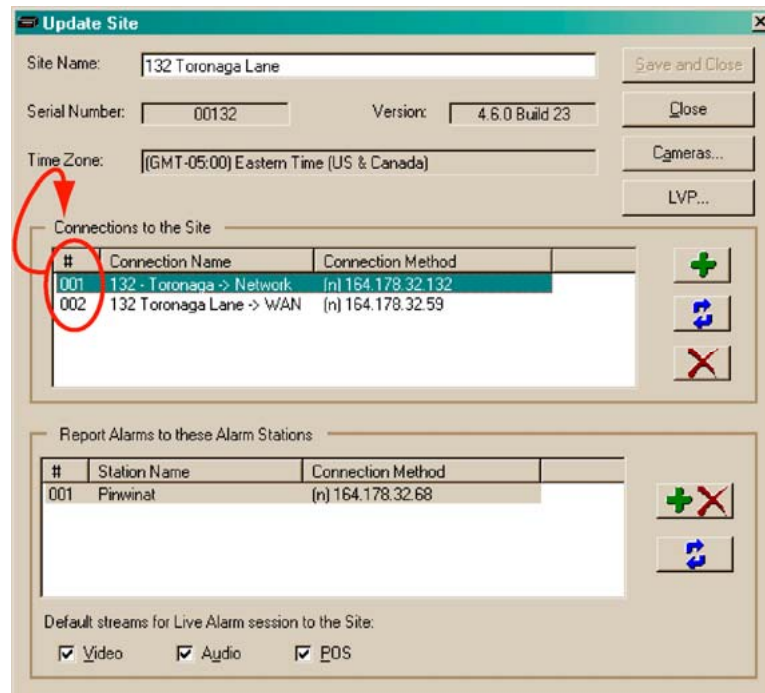
- For a dial-up connection, see p. 30.
- For a network connection, see p. 34.

The connections are listed in the Update Site dialog box. See figure 3-12, on p. 44.

### The primary connection

You can change the order by dragging an item to a different place in the list. The connection that you list first, is the primary connection. The primary connection can be either network or dial-up.

Fig. 3-12. Listing of Connections (Two) to a Site.



## RAS Server

There are two ways of connecting to Multi-Media units when using a Remote Access Service (RAS) server.

- Only one RAS-dependent unit at a time. A RAS server can be transparent to users of View by adding RAS server information to the site definition. This is ideal when there is only one Multi-Media unit on the network using the RAS server. See figure 3-13.
- Many units at once. Users dial-up the RAS server before using View. This is discussed later in Using a RAS Server before Connecting to a Unit on p. 47.

For both cases, a RAS is set up on a server that can access networked Rapid Eye Multi-Media units.

### Tip

**A RAS connection is optional. For other means of connecting to a Multi-Media unit, see table 3-1 on p. 29.**

## Planning to Connect to One Unit at a Time

You can use View to automatically connect to the site. A user has to end sessions with the unit before using another unit on that same network. From a security point of view, the View operator does not need to know the RAS username and password.

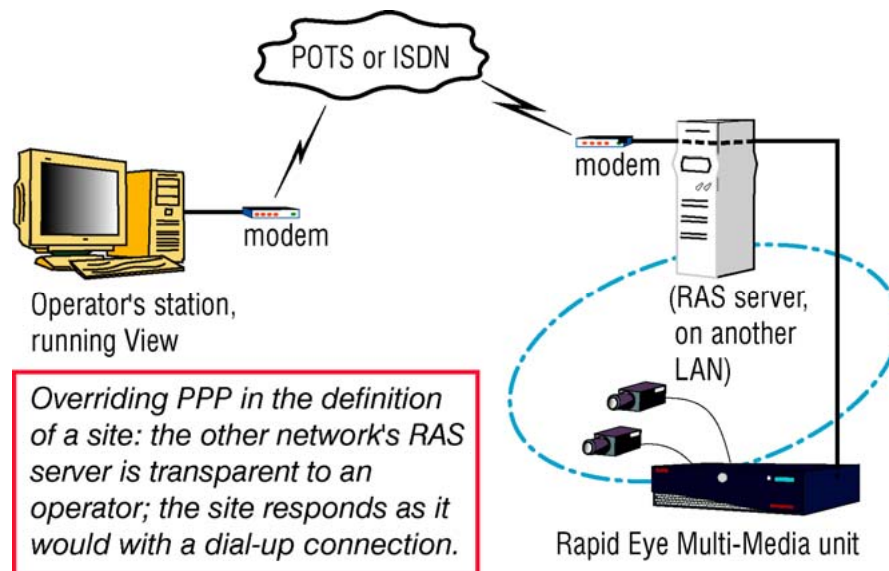
### A connection that behaves like dial-up

A session request behaves just as if you had reached the site's Multi-Media unit by connecting directly to it, by dial-up. Such a connection behaves as if it were a simple dial-up; two dial-up sites cannot be used at the same time with one modem. Sessions to a dial-up site have to be closed before using another dial-up site.


### What your network administrator needs

Multi sessions (live, retrieval and alarm) are sent to port 10,000. This port should be left open in your organization's firewall, for the sockets used by Multi.

**Fig. 3-13. Connecting to a Rapid Eye Site through a RAS Server, Transparently.**



## To Set a Connection to a RAS

1. In the Add Site/Update Site dialog box, click  in the "Connections to the Site" pane. The Add Connection dialog box appears; see figure 3-14. When adding a connection, the Connection Name box appends a stylized arrow and "Network" suffix to the site's name; this suffix may change as the next steps are carried out. Note that the suffix is not changed when updating a connection.
2. In the IP Address box, type the Multi-Media unit's IP address, obtained from your network administrator, as mentioned in section Naming / Renaming a Site.
3. Click **Use Dial-up Networking**. The connection's suffix changes to "dial-up".
4. As needed, change or leave the Country Code used to reach the RAS server by telephone.
5. Type the RAS server's Area Code (City Code) and Phone Number obtained from your network administrator (also mentioned in Naming / Renaming a Site).

### Tip

**If your telephone exchange needs a prefix number (an extra telephone key stroke such as a "9" or an "8") to access an outside line: Set this in the Window's Telephony program used by the PC. For local calls that span area codes or long distance calls within one area code, see Area Code: Irregular Use, above.**

6. Select the **Override PPP Settings** checkbox. See figure 3–14. If a connection is being added, a “PPP” is appended to the connection name. You have the option of either:
  - Typing another name in the Connection Name box, such as adding “RAS”.
  - or -
  - Leaving the connection name in the Connection Name box as it was automatically set by Admin.
7. Enter the PPP user name and password; these are obtained from the network administrator responsible for the network’s RAS server.
8. Type the PPP password a second time.
9. Click **Save and Close**. The “Add/Update Connection” window appears.
10. Click **Close**. The Sites tab appears. In the tab’s Primary Connection column, the first letter of PPP appears in parentheses: (p), followed by the telephone number to connect to a RAS server; then by (n) and the IP address used to connect to the Multi-Media unit. See also figure 3–6, p. 35.

**Fig. 3–14. RAS Server's Telephone Number and PPP Information.**

## Tip

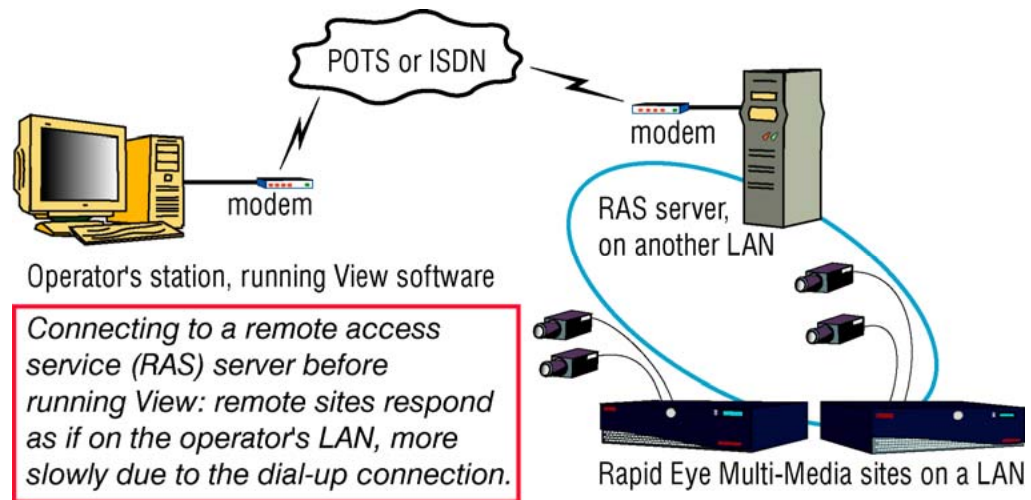
A Multi-Media unit’s own dial-up PPP username and password is used by default. Entering a PPP username and password in a site’s definition makes View use your entries for PPP instead of the Multi-Media unit’s during a dial-up connection.



**Technical warning for PPP:** Changing the “Rapid Eye Multi” phone book entry in a dial-up program is ineffective. The phonebook entry is overwritten by data in the Multi database every time an automatic connection to a RAS server is attempted.

## Using a RAS Server before Connecting to a Unit

Fig. 3-15. Connecting to a RAS Server, Before Running View to Operate Units.



### Tip

**A RAS server may not be needed by your organization.**

For other connections, see table 3-1 on p. 29.

The two ways of using dial-up to connect to a Remote Access Service (RAS) server are:

- Many units at once. A View operator, using a dial-up program of his/her choice, dials-up the RAS server before using View. The definitions of Rapid Eye sites do not contain RAS or PPP information. The sites are meant to behave as if they were on a View operator's LAN. See figure 3-15.
- Only one RAS-dependent unit at a time. See RAS Server, p. 44.

In both cases, a RAS server has been set up on a server that accesses Rapid Eye Multi-Media unit(s) on a network.

### Planning to connect to many units

For access to a RAS server "in front of" Rapid Eye sites on a network, the RAS server's information is not recorded in the Multi-Media sites' definitions. The RAS information must be known by the user of the PC and recorded in a Microsoft dial-up application. The user must use the dial-up utility to connect to the RAS server before starting a session at the site, using View.

### Preparation

Use the information in section Using Network Access, on p. 34 to define the sites as network units, using Admin. You can then use a modem to connect to these sites using the Microsoft dial-up application to connect to the RAS server.

### Use of an outside line requiring a prefix number


A prefix is an extra telephone keystroke such as a "9" or an "8" that you should be set in the Window's Telephony program, running on the PC.

### What your network administrator needs

Multi sessions (live, retrieval and alarm) are sent to port 10,000. This port should be left open in your organization's firewall, for the sockets used by Multi.

## Connections: Report and Customization

A site's connections are listed on the "Update Site" window. To view connections in the "Update Site" window:

1. Using Admin, click the Sites tab.
2. On the list of sites, do one of the following:
  - Double-click the site name you want to view.
  - Right-click a site name and click **Update** on the menu that appears.
  - Click a site name; then either: click  on the toolbar, click **Update** on the Actions menu or press the F12 key.

### Connection codes

The codes used to identify connections are listed in table 3–6, in the "Site Tab's Report" column.

**Table 3–6 Automatic Connection Names for a Rapid Eye Site**

Site Tab's Report	Automatic Name	Connection
(n) IP address	Garage -> Network	network
(d) telephone number	Garage -> Dial-up	dial-up
(p) telephone number (n) IP address	Garage -> PPP	dial-up to RAS
(d) telephone number	Garage -> Dial-up 2	second dial-up


## The Automatic Naming of Connections

### About Admin's naming convention for connections

Only when adding a site does Admin automatically name a connection in the Connection Name box. Admin uses the site's name, appends a stylized arrow and adds the connection type. See the "Garage" example used in table 3–6.

## Changing the Automatic Suffix in a Connection's Name

You can always rename a connection in full or partially, by typing in the Connection Name box.

1. While adding a site (as in Naming / Renaming a Site, above) or updating one, click  in the "Connections to the Site" pane. The Add Connection dialog box appears. The Connection Name box appends a stylized arrow and "Network" to the site's name.
2. Admin automatically names the connection in the Connection Name box. You have the option of keeping the name or of typing another.
3. An "Add Site / Update Site" window is displayed.
4. Click **Close**. The Sites tab appears.

### Tip

**When updating a connection, its name is not changed. You have the option of changing it.**



## Firewall: Technical Note

Multi sessions (live, retrieval and alarm) are sent to port 10 000, by default.

**Table 3–7 Default Transmission Control Protocol (TCP) Ports**

Port*	Name	Use	Needed at ...
10 000 <sup>†</sup>	Base	live, retrieval and alarm sessions	Multi-Media unit operator station
10 001	Maintenance	Maintenance Session for configuration, security, and sending/receiving system files	Multi-Media unit administrator's station
21	FTP	file transfer during upgrades and to obtain a unit's log	Multi-Media unit administrator's station
10 003	Alarm	alarm server for callbacks	alarm station Multi-Media unit

\* These port settings are listed in the Add Connection/Update Connection dialog boxes.

<sup>†</sup> The base port can be changed by using Admin software. For an example, see Network Address Translation.



**The TCP ports listed in table 3–7 should be left open in your organization's firewall.**

## Cascading Alarm Stations

### Flexibility in security

Prioritizing alarm stations is optional and applies only if many Multi alarm stations were created by your organization's Multi SA.

### Purpose: cascading and priority

Your Multi system can have one or many alarm stations. With many, cascading is automatic and customizable. You can specify which alarm stations your Multi-Media units tries to reach first.

### Cascade sequence

To insure against alarm station unavailability, you can:

- Assign more than one alarm station to a unit
- Set the order in which alarm stations are called.

### Preparations

Before you prioritize alarm stations:

- Create Alarm stations using the Alarm Station tab. See Adding an Alarm Station: Name and Reports, p. 203.
- Set events to trigger alarms. An alarm station is ineffective until events are set to trigger alarms. See Events Defined, on p. 187.


## To Sequence a Site's Alarm Stations

1. While Naming / Renaming a Site, p. 24, the alarm station(s) that the site can call are listed. The list is in the Report Alarms to these Alarm Stations pane of the "Add Site" or "Update Site" window.
2. To change the order of an alarm station, drag its name to the position that you want it to have in the list.
3. End the edit of the site definition. To do so, click **Save and Close**. The Admin window reappears, listing your system's sites on the Site tab.
4. Use View to update security for the Multi-Media unit. See Updating Security on a Multi-Media Unit, on p. 131.

## Quickly Assigning a Site to Many Alarm Stations

### Using the Update Site windows

The Update Site window can be used as a shortcut to add a site to many alarm stations. Alternatively, each Multi Alarm Station can be opened and a site added to each, as explained in Adding an Alarm Station: Name and Reports, on p. 203.

1. Using Admin, click the Sites tab.
2. While Naming / Renaming a Site, p. 24, click  in the "Report Alarms to these Alarms Stations" pane. The Add/Delete Stations to Call in Case of Alarms dialog box appears, displaying a list of alarm stations created on the Alarm Station tab. Stations already assigned to the site that you are editing are listed the Report Alarms to column.
3. Select one or many station names in the Alarm Stations available column.
4. To move the station names to the Report Alarms to column, either:
  - Click the right-arrow, or
  - Double-click the ones that you want to move.
5. Click **Save and Close**. The Add Site/Update Site dialog box reappears, listing the names of the alarm stations in the Report Alarms... pane. The site is also added to the site list of each alarm station that you have assigned.
6. You have the option of ending the site edit. To do so, click **Save and Close**. The Admin window reappears, listing your system's sites on the Site tab.
7. You need to use View to update security for the Multi-Media unit. See Updating Security on a Multi-Media Unit, on p. 131

## Setting a Site to Not Report Alarms to a Specific Station

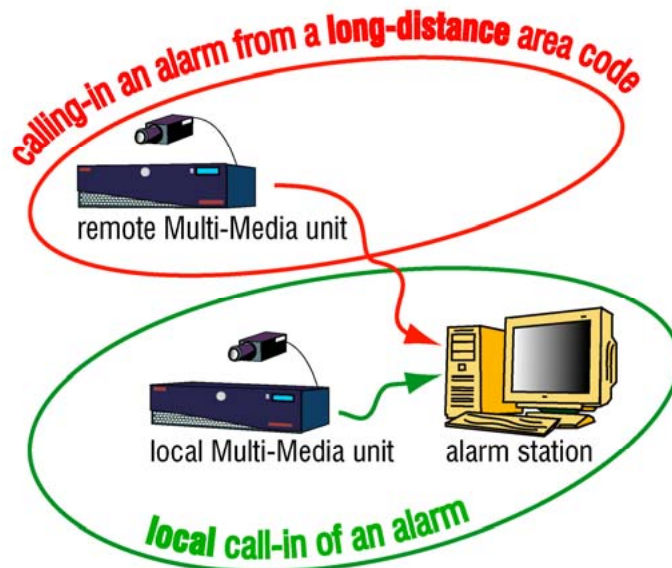
1. Using Admin, click the Sites tab.
2. While Naming / Renaming a Site, p. 24, click  in the "Report Alarms to these Alarms Stations" pane. The Add/Delete Stations to Call in Case of Alarms dialog box appears, displaying a list of alarm stations. Stations already assigned to the site are listed the Report Alarms to column.

3. To move alarm station names to the Alarm Stations available column, either:
  - Select one or many station names in the Report Alarms to column; then click the left-arrow, or
  - Double-click the ones that you want to move.
4. Click **Save and Close**. The Add Site/Update Site dialog box reappears, listing the alarm stations in the Report Alarms... pane.
5. You have the option of ending the site edit. To do so, click **Save and Close**. The Admin window reappears, listing your system's sites on the Site tab.
6. You need to use View to update security for the Multi-Media unit. See Updating Security on a Multi-Media Unit, on p. 131

## Customizing a Dial-Up Connection to an Alarm Station

The Multi SA may need to customize the telephone number used to reach a Multi-Media Alarm Station.

**Fig. 3-16. For Local Calls that Need an Area Code, Customize Dial-up.**

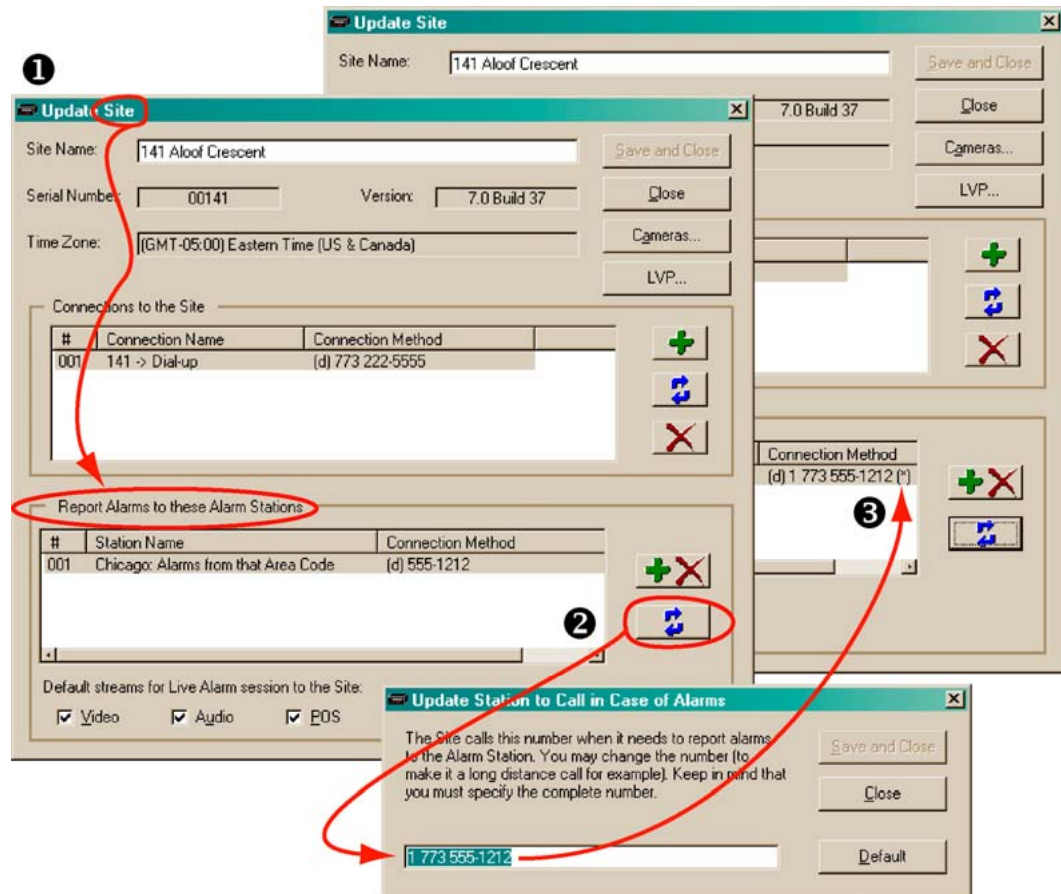



### Preparation

An alarm station's telephone number in the site definition is a copy of the number in the alarm station definition. Before customizing a dial-up connection, consider if the alarm station definition is correct, as explained in Dial-up Connection to an Alarm Station on p. 208, and Customizing a Dial-Up Connection to an Alarm Station, p. 211.


## To Customize the Dial-up Connection to an Alarm Station

Fig. 3–17. Customizing an Alarm Station's Telephone Number.



1. While creating or updating a site, select an alarm station.
2. In the Report Alarms to these Alarm Stations pane, click . See fig. 3–17. The Update Station to Call in Case of Alarms dialog box appears.
3. Modify the telephone number so that it is as one would dial it. You have the option of:
  - Removing/adding long distance country and area codes, or
  - Typing a prefix and commas, as needed to dial-out of a site's exchange.
4. Click **Save and Close**. The modified telephone number appears in the Connection Method column in the Report Alarms to these Alarm Stations pane. An asterisk is added in parenthesis (\*) to the entry's display, to indicate customization.
5. Update security for the unit; see Updating Security on a Multi-Media Unit, p. 131.

## To Cancel the Customization of a Telephone Number

1. While creating or updating a site, an alarm station with a customized telephone number shows an asterisk (\*) in the entry's display.
2. In the Report Alarms to these Alarm Stations pane, click . The Update Station to Call in Case of Alarms dialog box appears. See fig. 3–17.
3. Click **Default** in the Update Station to Call in Case of Alarms dialog box. The telephone number returns to the one entered in the Alarm Station definition.
4. Update security for the unit; see Updating Security on a Multi-Media Unit, on p. 131.

## Unit Configuration: Basics

### Maintenance Session

#### Using View

View software is used to run a Maintenance Session on a Rapid Eye Multi-Media unit, not Admin software. The Maintenance Session is discussed in this *System Administrator's Guide* because the session is designed to be used by the system administrator (the Multi SA) designated by your organization, to maintain and supervise your Rapid Eye System.

#### Using a Maintenance Session

The Maintenance Session is used to configure:

- **System hardware.** Cameras, Multi Audio, motion detection, scheduling, and other hardware connected to the unit.
- **Security.** Events Defined that trigger alarms and other security settings. See also Updating Security on a Multi-Media Unit, on p. 131.

#### Scope of a Maintenance Session

A Maintenance Session involves only the unit on which it runs. You can use View software to open a Maintenance Session on more than one unit at a time. Two operators cannot each run a Maintenance Session on the same unit. While a Maintenance Session runs, the unit's LocalView interface continues to display video but is unavailable for unit operation.

A Maintenance Session is also used to:

- **Make a site operational.** Running a Maintenance Session is needed before operators can start using a Multi-Media site; see Making a Site Operational, p. 55.
- **Obtain a unit's statistics.** See Hardware Report, p. 140 and To Obtain a Unit's Statistics, p. 128.

## To Start a Maintenance Session

1. Log on to View, using a central database.
2. Using View, select a site on the Sites list, for which maintenance must be performed.
3. To start a Maintenance Session, either:
  - Right-click on the site name to select [Maintenance] from the shortcut menu.
  - Select the site; then click the Maintenance command on the Actions menu.
4. If the Connections dialog box appears, choose the network/dial-up connection that you need and click **OK**. The maintenance tabs appear.
5. Wait for the "System Operational" message in the Feedback box.



### Site feedback

During maintenance, messages about the session appear in the Feedback box. For a list of the messages, see Feedback Box Reference, on p. 64.

### Reboot button in Maintenance window

The Reboot button reboots the Multi-Media unit, not your PC.

### Technical note for network administrators

For connections over a network, Multi Maintenance Sessions are sent to port 10,001. Leave this port open in your organization's firewall, for sockets used by Multi. For other ports used by Multi on a network, see table 3-7 on p. 49, in System Tab in a Maintenance Session.

## Support for Older Models of Units

### Setup and Maintenance

Older-model, Rapid Eye units are supported. If an older unit lacks a newer feature, the feature is not shown in a Maintenance Session. The interface appears as it did in the last-available upgrade for older units. For example, a Recording tab does not appear when running a Maintenance Session on an older-model unit; instead, the Video tab is used for the settings of recorded video.

### Using older documentation

For the setup and operation of older-model units, Honeywell recommends referring to the user guides that came with those units, as needed. Adobe PDF files of these older guides are available from Honeywell, on its website at [www.honeywellvideo.com](http://www.honeywellvideo.com).

## Making a Site Operational

A Multi-Media unit is “working” within minutes of being turned on. There are a few crucial steps needed to make your Rapid Eye site an outstanding security tool.

### The first Maintenance Session

You run the first Maintenance Session at a site after:

- Adding that site to a Multi central database. See Naming / Renaming a Site on p. 24
- Upgrading a Multi unit.

### Site registration

When the first Maintenance Session runs, the validity of the communication data to the site can be checked. If correct, the site is registered automatically, making it available to View operators who have the right to use it.

Fig. 4-1. Multi-Media Unit Serial Number and Version of Unit Software.

Result of registering a site

The screenshot shows a 'System' tab with the following sections:

- Site Info:** Serial Number: 00228, Software: 4.5.0 Build 27. An 'Upgrade' button is located below these fields.
- Signal Format:** Radio buttons for NTSC (selected) and PAL.
- System Monitor:** Checkboxes for 'Enable Status Pulse' (checked) and 'Monitor Alarm Reporting' (unchecked).
- Maximum Network Data Rate:** A checkbox for 'Regulate Data Rate' (unchecked). Below it, fields for 'Send no more than' (1000 bytes), 'every' (15), and '1/60 second', and 'Apply only to blocks larger than' (250 bytes).
- Network Settings:** A checkbox for 'Use DHCP' (unchecked). Fields for Network Name (N/A), IP Address (10 . 10 . 211 . 228), Subnet Mask (255 . 255 . 255 . 0), Gateway (10 . 10 . 211 . 1), and MAC Address (00:07:e9:3d:b:aef).

The Multi-Media unit has a serial number and software version. These numbers are displayed on the System tab, as illustrated in fig. 4-1, and on the Hardware tab.

### Tip

**Someone has to run a Maintenance Session on a unit before he or any other View operator can run Live Sessions.**

One Maintenance Session is enough to register a site for all users of that site.



**Honeywell recommends setting a unit to the correct time zone, time and date before using the unit in your organization's operations.**

### Security considerations

A Multi-Media unit is “working” within minutes of being turned on, however there are crucial steps to make your Rapid Eye site a useful security tool:

- Set the time zone and time. See Unit’s Time Zone and Clock, on p. 56. Incorrect time stamps can make the identification of video impossible.
- Check the camera configuration. See Cameras, on p. 65. Cameras are detected automatically; you need to specify drivers for cameras that pan, tilt or zoom (PTZ).
- Test the alarms. For events set to trigger alarms, test if these events give you the anticipated results. See Events Defined, on p. 187.
- Honeywell recommends using a system password. Without a system password, your Rapid Eye sites can be accessed by Admin users in other organizations. To avoid this situation, see Securing a Site, below.

### Scheduling options

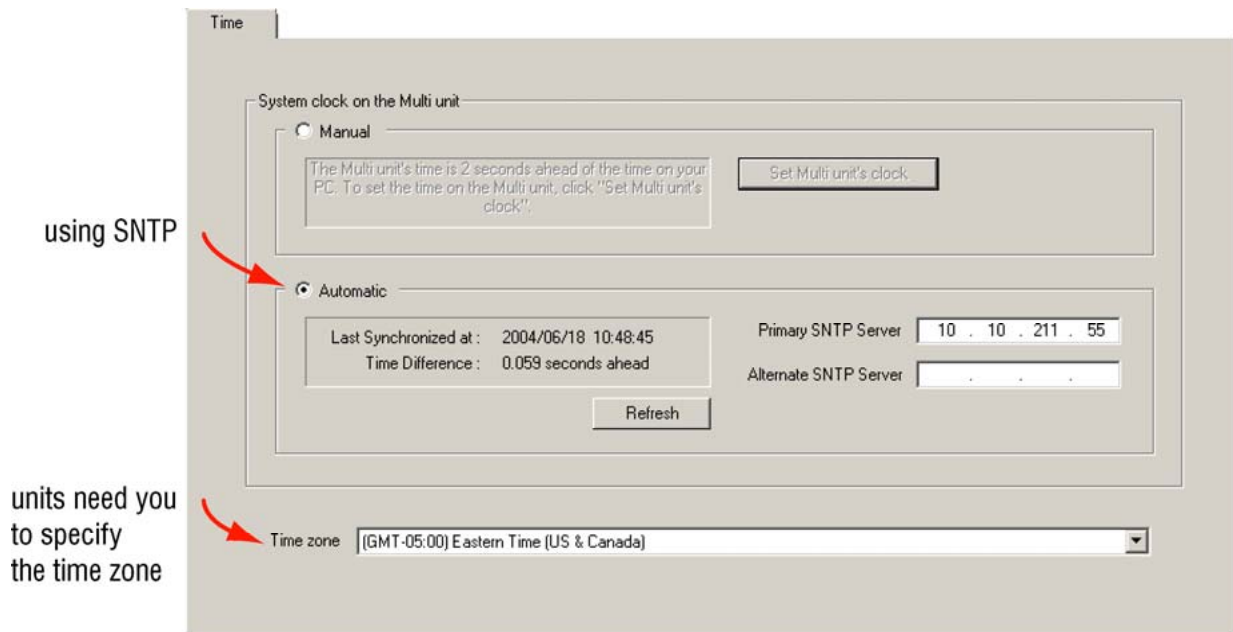
By default, video is recorded all the time and alarms can be triggered at any time. You have the option of having cameras and alarms disabled on days and at times of your choice. To do so, see: Scheduling: Configuration, p. 105.

## Unit’s Time Zone and Clock

### Crucial settings for reporting on video of events

Setting the Time Zone and System Clock on Multi-Media units is crucial to the correct identification of video. These settings also govern the scheduled recording and scheduled alarm features. Please set them with care.

Fig. 4-2. Unit Time Using SNTP as a Reference.





## Time zone

Your Multi SA needs to indicate in which time zone each Multi-Media unit is installed. Make this setting whether a Multi-Media unit's clock is set manually or automatically.



**The Time Zone of a unit is crucial for correctly reporting on the video of events.**

## To Indicate the Time Zone of a Multi-Media Unit

1. Using View, select a unit whose time zone needs to be set.
2. Start a Maintenance Session.
3. Click the Time tab. See figure 4-2.
4. If the zone indicated in the Time Zone box is incorrect, click the arrow in the box. A list of all time zones appears.
5. Scroll the list as needed to find a match for the time zone in which the unit is installed. The time zone is set right away; there is no need to reboot the unit.

### Tip

**The time zone is set on a unit-by-unit basis. Repeat this procedure for every unit in your system.**

**Table 4-1 Effect of Time Zone Setting on Display and Clips**

Operator's PC*	Unit's Time Zone <sup>†</sup>	Time Shown <sup>‡</sup> : Sessions & Clips
showing: 4 PM Eastern Time	Eastern Time UTC – 05:00	show unit's time and recorded video as 4 PM
showing: 4 PM Eastern Time	Pacific Time UTC – 08:00	show unit's time and recorded video as 1 PM

\* To set the time zone on an operator's PC, use the Control Panel in Microsoft Windows. See also the *Rapid Eye View Software Operator Guide: Selecting a Time Reference*.

<sup>†</sup> Set using View, while running a Maintenance Session.

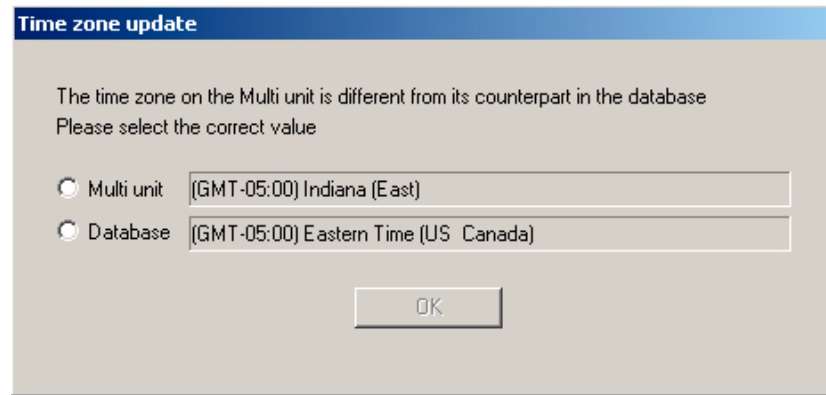
<sup>‡</sup> Display can be changed for a session's duration to LTZ (the local time zone set on your PC), RTZ (a camera's remote time zone) or to UTC (universal time zone). See the *Rapid Eye View Software Operator Guide*.

## Conflicting Time Zones

A Multi-Media unit's time zone can be changed without the knowledge of a View operator. It can be done at the unit, using LocalView, or through another Multi-Media database (Multi db). The View operator's next attempt to access the site is interrupted by a message, shown in figure 4-3.

The message also appears for areas within a time zone that have different rules for daylight savings time. For example: "Indiana (East)" in the Eastern time zone (GMT-5:00) differs from "Eastern Time (US Canada)", also GMT-5:00. To respond to a notification of conflicting time zones, select the time zone that indicates where the Multi-Media unit is installed and then click **OK**.

**Fig. 4-3. Different Rules May Apply for Daylight Savings Time in one Time Zone.**



## SNTP: Setting the Clock Automatically

See your IT Administrator to find out if a Simple Network Time Protocol (SNTP) server is in use. Multi-Media units on a LAN can benefit from the automatic setting. It is accurate to within a fraction of a second.

1. Obtain the IP address of an SNTP server. You have the option of also obtaining the address of an alternate server.
2. Using View, select a unit whose clock needs to be set.
3. Start a Maintenance Session.
4. Click the Time tab.
5. If Automatic is not selected, click it. The Time tab appears as in figure 4-2.
6. Click the Primary SNTP Server box and type the IP address of an SNTP server obtained in step 1. You have the option of indicating an alternate in the Alternate SNTP Server box.
7. Click **Refresh**. The Multi-Media unit contacts the SNTP server and synchronizes the Multi clock to the SNTP time.
8. You have the option of ending the maintenance; see Ending Maintenance, p. 62.

### Auto-synch statistics

The statistics appear are for Multi technical support, if they make a service call to your site. The Auto-synch statistics do not apply to a clock set to Manual.

Last Synchronized at. Latest time that the SNTP server was used. Synchronization to SNTP occurs at least every 24 hours.

Time Difference. Accuracy of synchronization.

## System Clock: Manual Setting

A Multi SA can synchronize the clock of a Rapid Eye Multi-Media unit using a PC's clock as reference. This is more useful for units connected only by dial-up, but can also be used for units on a LAN.

### Tip

Check/set the clock on an operator's PC, before setting a unit's clock manually.

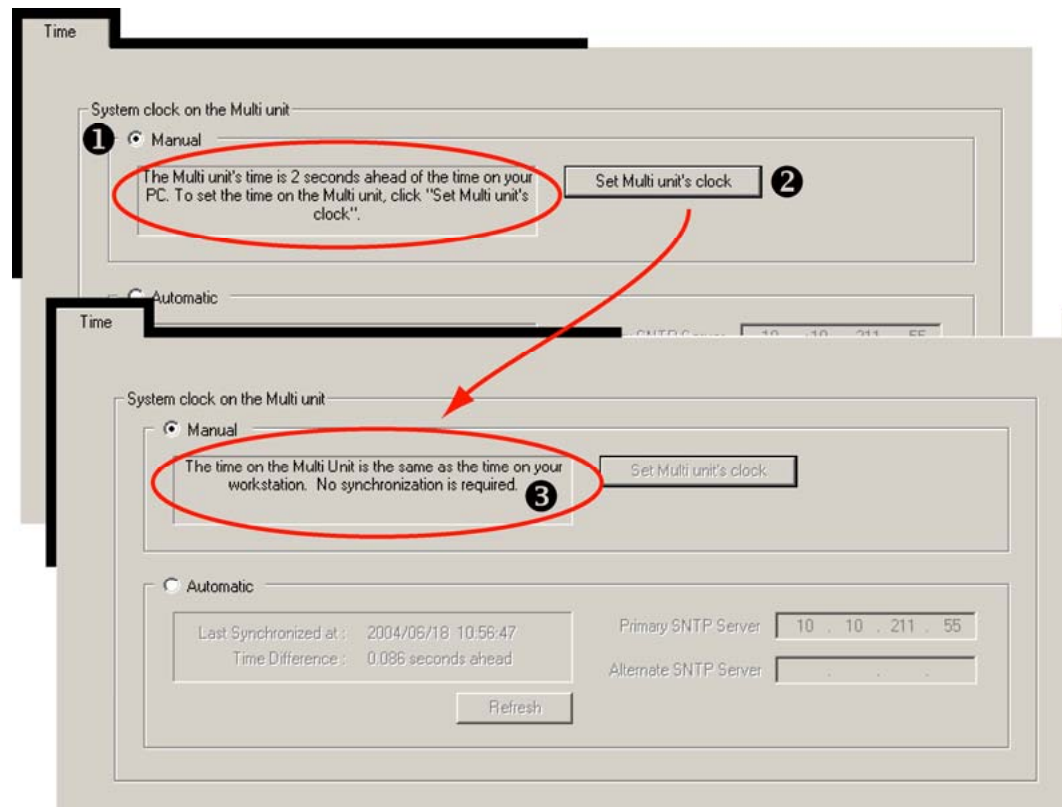
## Adjusting the Clock on a PC Running Rapid Eye Software

To adjust a PC's time, date and time zone, click **Start** followed by Settings, Control Panel and Date/Time. Check the accuracy of the time and the time zone on the PC and adjust it as needed.

## Using a PC's Clock to Set a Unit's Clock Manually

1. Using View software, select a Multi-Media unit whose clock needs to be set.
2. Start a Maintenance Session.
3. Click the Time tab. If Manual is not selected, click it. The Time tab appears as in figure 4-4.
4. Click **Set Multi-Media Unit's Clock**.

Fig. 4-4. Setting a Multi-Media Unit's Clock Manually.



### Synchronizing time over dial-up

Due to the nature of dial-up connections, the Multi-Media unit's time may still be off by a few seconds after synchronizing time.

## Adjusting the Time on an Operational Unit



**If a unit's clock is set incorrectly (more than +/- a few seconds), Honeywell recommends setting a unit to the correct time (and date) as soon as possible.**

### Human error or unauthorized use

Leaving the clock set to an incorrect time (more than +/- a few seconds) for a long length of time (an hour or more) on an operational unit, can create problems for operators who need to retrieve video when the clock is set correctly.

During the 'span of incorrect time', video is not erased and continues to be recorded; however, two instances of video can be created at the same timestamps. Using the Seek or Jump controls shows the video of the first instance only. The second instance of video can only be played through or fast-forwarded.

## Correcting the Clock

### Whole hours: time reference

Check the "Time Reference" setting. If the clock of a unit in another time zone shows a time that is off by whole hours, the clock could be set to the correct time, but using an optional display (GMT, operator's time zone, unit's time zone). See the *Rapid Eye View Software Operator Guide: Selecting a Time Reference*.

### Whole hours: time zone

Check the "Time Zone" setting. If the clock of a unit in another time zone shows a time that is off by whole hours, the clock could be set to the correct time, but set to an incorrect time zone. See *Unit's Time Zone and Clock*, p. 56.

### Setting the clock to the correct time

A short span of incorrect time. If a unit's clock shows the wrong time (more than +/- a few seconds), for a short while (a few seconds, a few minutes, up to an hour, or so):

- Set the clock correctly; either automatically or manually.

### A follow-up may be needed: clearing storage

A long span of incorrect time. If the clock remains set to an incorrect time (more than +/- a few seconds) for a considerable length of time (many hours, days or weeks) it can become inconvenient and confusing for an operator who needs to play through that recorded video. For such an error:

- Set the clock correctly; either automatically or manually.
- Consider Clearing Storage. See p. 129.

## Securing a Site

### Securing the Multi system

After Making a Site Operational (see p. 55), Honeywell recommends that you secure your Rapid Eye site by adding:

- A system password. Use Admin to set a system password to protect your sites from unauthorized accounts. See System Password, on p. 166.
- and -
- A password for the "Administrator" account. To help prevent: (a) an uncontrolled configuration of Multi-Media units; (b) the accidental clearing of a unit's storage or (c) unwanted removal of the system password. See Administrator Password, on p. 176

Then update security, as explained in Updating Security on a Multi-Media Unit, on p. 131.

## Rebooting a Unit

1. Start a Maintenance Session for the Rapid Eye site. Please wait until the "System operational" message appears.
2. Click **Reboot**.

### Lack of reasons to reboot a Multi-Media unit

Use of the Reboot button does not damage the unit. It does however interrupt the recording of video for a few moments and should best be left alone, unless Multi technical support instructs an operator to click it. A reboot can be traced to the operator who performed it. See Tracing Events on p. 191.



**The button is for rebooting a Multi-Media unit. Do not mistakenly reboot your PC when called to "click the Reboot button in the Maintenance window".**

### Automatic reboot of Multi-Media unit

A Multi-Media unit reboots by itself when:

- Changes to a modem serial device are applied. Modem settings are explained in section Serial Device: Modem, on p. 138
- System files are upgraded; as explained in System Files, p. 132.
- and -
- Power to the unit is interrupted and restored.

## Maintenance Reference

### Ending Maintenance

To end a Maintenance Session, close the Maintenance window.

Other actions can also close sessions:

- Click  Disconnect
- Click **Disconnect** on the Actions menu
- Close View.

### Using Apply

The Apply button is used after changes have been made to the: IP address and other network settings (including DHCP), motion mask, or response rules. If the Apply button is active and you click another tab, the button remains active.

## Maintenance Topics

**Table 4-2 Maintenance Reference Topics**

Topic (alphabetically)	Important for ...	Action	See... (page)
Cameras	video	configuration	65
Clearing Storage	video archive	action	129
Customer Data and Customer-Device Events	log/alarms	configuration	143
Dial-up Connection: to a Unit	dial-up	action	30
Events Defined	alarms	action	187 & 149
Feedback Box Reference	system files	report	64
Hardware Report	Honeywell	report	140
Public Display Monitor: Using Monitor Output 1	public display	configuration	141
Motion Detection	motion search	configuration / action	116
Multi Audio	audio	configuration	147
Pan, Tilt, and Zoom (PTZ) Setup	video-PTZ	configuration	85
Serial Device: Modem	dial-up connection	configuration	138
To Obtain a Unit's Statistics	Honeywell	report	128
System Tab in a Maintenance Session	LAN/WAN	configuration	134
System Files	upgrades	action	132
Unit's Time Zone and Clock	all units	action	56

## Maintenance Tasks

The tasks in table 4-1 are carried out as you see fit. Suggestions are indicated in the Accomplish column.

**Table 4-1 When to Accomplish Maintenance Tasks**

Crucial ...	Tab and Task	Accomplish ...	See... (page)
to all units	Time	after creating sites or if time on a Multi-Media unit is grossly wrong	56
for video	Video - Picture	after creating sites and when adding/removing camera(s) at a site	65
for motion	Video - Motion	at user discretion; to prepare video for motion search and alarms.	116
to restrict access	Security	after changing the system password, modifying user profiles or adding alarm stations	62
LAN/WAN	System	after creating sites or when enabling FAULT RELAY at a site	134
for PTZ	Serial Devices and Video - PTZ	To select a driver for cameras that pan, tilt and zoom (PTZ) and to enable PTZ-type camera(s) at a site	85
Multi audio	Audio	at user discretion	147
alarms	Events	at user discretion; to setup logs or alarms	187
n/a	Serial Devices - Data recording	at user discretion; to setup logs or alarms triggered by events	143
Honeywell technicians	Statistics	at user discretion; for troubleshooting	128
n/a	Clearing data	when permanently closing a site	129
upgrades	System files	when upgrading a Multi-Media unit	132
n/a	Eagle Audio	Enable Eagle hardware.	149

## Feedback Box Reference

**Table 4–2 Messages from a Unit, During a Maintenance Session**

<b>Message</b>	<b>Following ...</b>	<b>See... (page)</b>
Activate System Failure	Apply or Multi-Media unit reboot	61
Activated System	Apply or Multi-Media unit reboot	61
Activating remote unit...	Multi-Media unit Reboot	61
Activating System	Multi-Media unit Reboot	61
Clearing Storage	Use of Statistics tab	128
Clearing storage, n % completed.	Use of Statistics tab	128
Connecting to Remote Unit...	Start of Maintenance Session	53
Getting statistics from Remote Unit...	Use of Statistics tab	128
Opening media storage with full repair check, please wait...		
Promoted temporary files	Use of System Files tab	132
Reboot System Failure	Apply or Multi-Media unit reboot	61
Recovering storage, n % completed	Use of Statistics tab	128
Recovering Storage.	Use of Statistics tab	128
Requesting file transfer permission from the Remote Site	Download of system file	132
Reset System	Apply or Multi-Media unit reboot	62 & 61
Resetting remote unit...	Multi-Media unit Reboot	61
Resetting System	Multi-Media unit Reboot	61
Restarting System	Multi-Media unit Reboot	61
Runtime System Failure	Apply or Multi-Media unit reboot	61
Starting remote unit...	Start of Maintenance Session	53
Starting System	Multi-Media unit Reboot	61
Statistics received	Use of Statistics tab	128
Synchronizing Time	Use of Time tab	56
System Operational	Apply or Multi-Media unit reboot	61
Time zone updated on unit and in central and local databases	User makes a change to the unit's time zone data	56
Time zone updated on unit	Resolution of time zone conflict	56
Time zone updated in central and local databases	Resolution of time zone conflict	56
Transfer successful	Use of System Files tab	132
Transferring file...	Use of System Files tab	132
Updating security	Use of Security tab	62



## Video Feed Setup

### Cameras

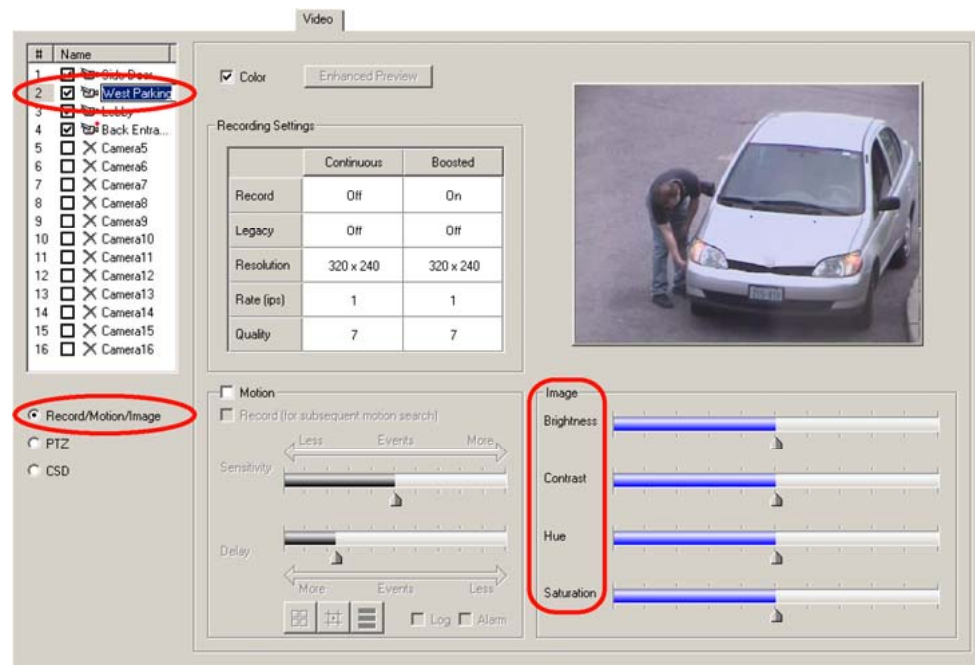
#### Automatic detection

A Multi-Media unit detects cameras that are powered and connected to it, when the unit is powered or rebooted.

#### Using a Maintenance Session

To setup a video feed, continue or start a Maintenance Session for the Rapid Eye site; how to do so is explained on p. 53.

Fig. 5-1. The Video Tab: Camera Names and Image Settings.



### Renaming a Camera

1. Continue or start a Maintenance Session.
2. On the Video tab, select the name of a camera in the Name column. Cameras have default names of "Camera1", "Camera2", and so on.
3. Click the name of the camera once more; a box appears around the name.
4. Type a new name. See figure 5-1.

## Adjusting a Video Feed

1. Continue or start a Maintenance Session.
2. On the Video tab, select the name of a camera in the Name column.
3. Adjust Brightness, Hue, Contrast and Saturation, as needed. You can monitor changes on the video feed displayed on the tab: your changes are saved on-the-fly.



**Video feed adjustments cannot correct cameras that are badly-angled, out of focus, in the dark, and so on. If corrections are needed beyond adjustment, see Environmental Interference for Video Feeds, on p. 84.**

## To Re-enable One Camera's Feed

- In the Name column, click the box next to the camera icon, next to the camera name. The camera is enabled when a checkmark appears in the box. If no video appears, consider that the camera may be turned off, disconnected from the unit, not powered or damaged. See also Environmental Interference for Video Feeds.

## To Re-enable All Newly Connected, Powered Cameras

You have the option of either:

- Enabling the new cameras one-by-one.
- Cycle the unit's power, so that cameras are auto-detected.

## To Adjust All Cameras at Once

Press and hold a Ctrl key on the PC's keyboard, while changing a setting with the mouse.

## To Disable a Camera

1. Continue or start a Maintenance Session.
2. On the Video tab, select a camera in the Name column.
3. Clear the box next to the camera's name.



**Disabling a camera resets the recording settings and other configurations to default settings. The defaults are used when the camera is re-enabled.**

## Resolution of Live Video in View Software

### Automatic optimization of resolution for Live video sessions

View software optimizes the resolution of live video. The size of a camera window determines which resolution is used. As an operator makes a camera window larger (or smaller), the

resolution of images is automatically adjusted for an optimal view of the video feed. See the *Rapid Eye View Software Operator Guide*, for more procedures and tips about live video.

## Tip

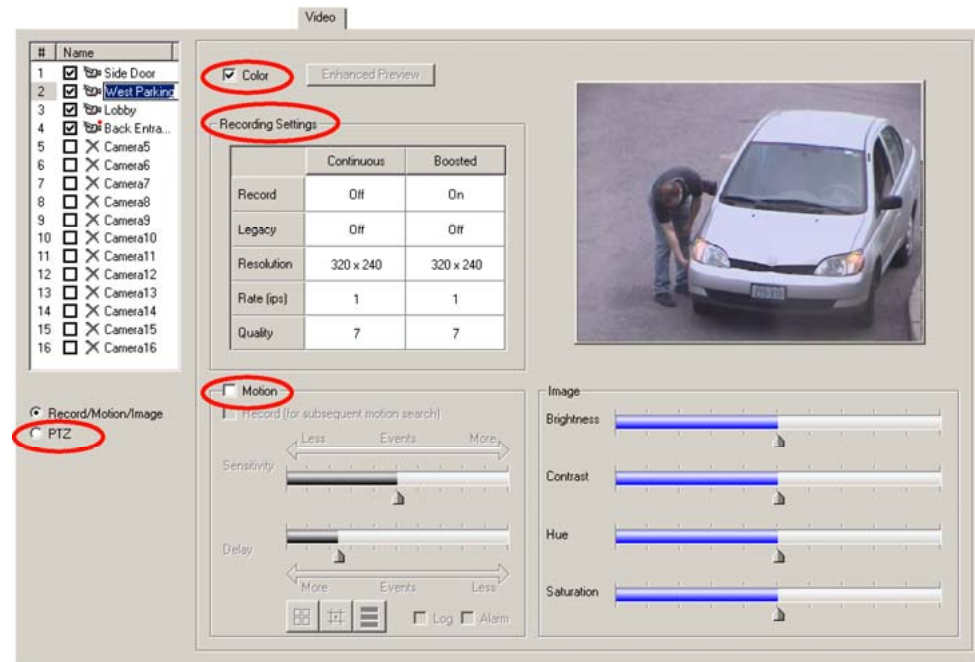
The resolution of recorded video is setup in a Maintenance Session and does not change when View software automatically optimizes the resolution of live video.

### Smoothing video

Video smoothing is an option of View, set by the View operator. It adds a load to the operator's CPU and can slow busy systems. The result of video smoothing is not recorded; it can be toggled OFF/ON while watching recorded video or while monitoring Live video. In a Maintenance Session, video smoothing can be seen in the Enhanced Preview window. See The Enhanced Preview of Resolution, p. 74. See also the *Rapid Eye View Software Operator Guide*.

## Other Video Settings

Fig. 5-2. The Video Tab: Color, Recording Settings, Motion and PTZ.



### Color

You have the option of specifying if a color video feed is viewed in color or in black and white (b&w). Removing the checkmark from the Color box on the Video tab shows the video feed in b&w. See figure 5-1, above. Color continues to be recorded and can be toggled in/out, as needed.

### Recording settings

Use the Recording tab to setup the Continuous video recording settings. The values are reported on the Video tab. See Recording Video: Continuous Recording Settings, p. 68.

### Motion

For Motion Detection, see p. 116.

**PTZ**

See Pan, Tilt, and Zoom (PTZ) Setup on p. 85 and Using a PTZ Camera, p. 88.

**Screen area: size of camera windows on a PC monitor**

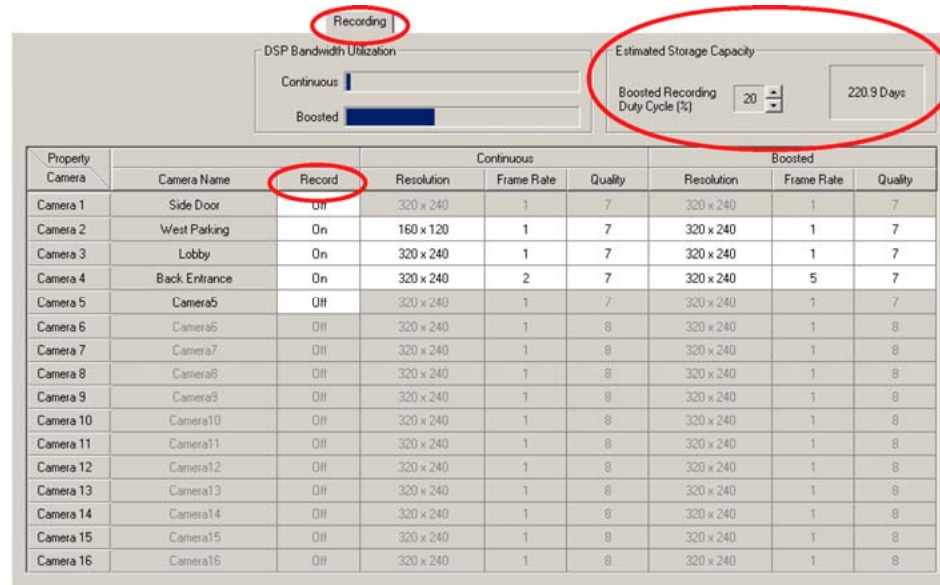
If the resolution settings for a Multi-Media unit take-up too much or too little of the PC monitor's area, adjusting Microsoft Windows' Display Properties for a PC monitor can have a positive effect. See Customizing Windows for a PC Monitor's Settings, on p. 82.

## Recording Video: Continuous Recording Settings

**Making use of a Maintenance Session**

To setup a video feed, continue or start a Maintenance Session for the Rapid Eye site; how to do so is shown on p. 53.

**Fig. 5-3. The Recording Tab, Showing that Three Cameras Are Recording.**



### To Enable the Recording of a Video Feed

1. Continue or start a Maintenance Session.
2. On the Recording tab, illustrated in figure 5-3, note that in the Record column, recording is "OFF" by default, for all cameras, when the unit is new. Cells that are unavailable indicate that that camera port is not connected to a camera, or that the camera is disabled.
3. Click the cell in the camera's Record column. A menu appears. Select "ON". The settings for **Continuous** and **Event** Recording become available.

**Feedback on the Video tab**

On the Video tab, note that a red dot has appeared, between the camera's icon and its name in the Name column. The dot means that the unit is recording that video feed.

Fig. 5-4. A Red Dot Is Added to the Icon of a Camera that Is Recording.



### Turning recording OFF

A camera's settings are retained when recording is turned OFF.



**Disabling a camera resets the recording settings and other configurations to default settings. The defaults are used when the camera is re-enabled.**

## Customizing Settings for Recorded Video

### Flexibility

Use the Recording tab to customize a Resolution, Frame Rate and Quality for each camera's continuous recording and for event recording. The recording settings can be the same for all cameras or customized, camera-by-camera.

### Making settings

Values for **Event Recording** cannot be lower than settings for **Continuous** recording.

### Forecasting results

For Computing the Length of the Video Archive, see p. 122.

To compare resolution settings, see Comparing the Resolutions of Recorded Video, p.76.

## Resolution Setting

On the Recording tab, click a cell in the Resolution column. Select a value (of pixels × pixels) from the list that appears. For comments about the values, see Optimizing Recorded Video, p. 72, and Resolution Reference: Recorded Video, starting on p. 81. The default values are, for NTSC: 320 × 240; for PAL: 384 × 288.

### Tip

**Honeywell recommends optimizing the resolution of recorded video using the Automatic DSP Performance Maximization.**



**Honeywell does not recommended gauging the resolution of recorded video based on live video. Live video is always shown at an optimal resolutions that can differ from the resolution for recording.**

## Frame Rate Setting

On the Recording tab, click a cell in the Frame Rate column. Select a value (of images per second (ips)) from the list that appears. The default value is: 1 ips.

**Table 5-1 Frame Rate Values (Approximate ips) for Multi-Media DSP Units**

<b>NTSC</b>	1	2	3	4	5	6	7.5	10	15	30
<b>PAL</b>	1	2	3	4	5	6	8	12.5	25	

### Using lower frame rates

Frame rate and resolution. Units can record up to 30 ips from each NTSC camera (up to 25 ips for PAL), at the default resolution. Setting a higher resolution may require lowering the frame-rate.

Slower fast-forward or rewind. More ips take more time to process. If recording rates of one or two images per second are satisfactory; then use them.

Security video and commercial video. The movement of persons recorded at higher rates appear smoother; however, consult your security personnel about what they need from video surveillance. Two or three frames per second may be wholly adequate for some security needs.

## Quality Setting

On the Recording tab, click a cell in the Quality column. Select a value (a compression factor) from the list that appears. The values range from: 6 to 10. The default value is: 7.

Quality and the storage of video. Lower values take less storage and can display block-like artifacts in the video. The highest setting can double the use of storage.

## To Duplicate Settings

### Using one camera as a template for others

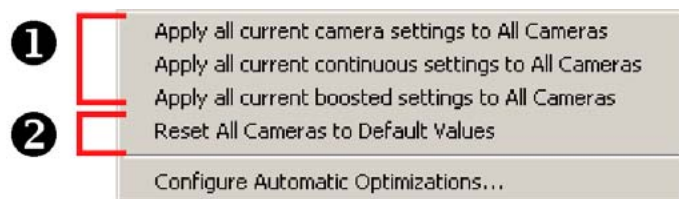
For convenience, recording settings can be copied to all cameras. To do so:

- Right-click in the row that you want to use as a model for the others. A menu appears for duplicating all settings, or only the settings for continuous recording, or event recording. See fig. 5-5.

### Restoring defaults

- Right-click on the Recording tab. A menu appears. Click "Reset all cameras to default values". See fig. 5-5.

**Fig. 5-5. The Menu for Duplicating Recording Settings (1) or for Restoring Defaults (2).**



## Continuous Recording and Event Recording

To use event recording, set different values for the Resolution, Frame Rate and Quality of from those for continuous recording.

### Authority

The settings for recording video are made by your organization's Multi System Administrator (Multi SA) or by a user with the Modify Configuration right in her account.

A Multi SA can consult View operators, security personnel and IT managers, to find out if:

- The recorded video is satisfactory for the needs of your organization.
- The settings do not shorten the video archive to the point of making it unusable.

### Report

The values selected on the Recording tab are also shown on the Video tab.

### See also

Event Recording: Configuration, p. 103.

## Estimating Storage Capacity

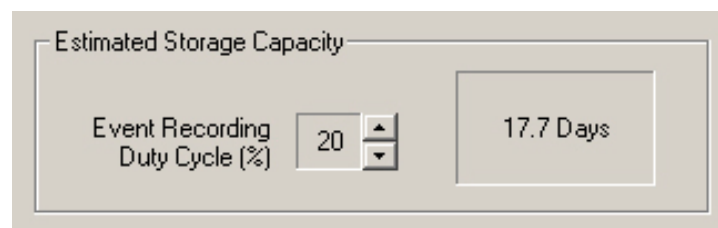
### A unit's video archive

As higher values for Rate, Resolution and Quality are set, the time that video, audio and data can be stored in a unit—the video archive—, shortens. The Estimated Storage Capacity reports a useful forecast (in days) of the length of the video archive. See fig. 5-6.

### Length of a unit's video archive

The **Event Recording Duty Cycle** can give more precision to the estimate of the unit's video archive. Base the duty cycle on how often events and operators will be using the **Event Recording** settings (% of recording time). The estimated length of the video archive is shown next to the **Event Recording Duty Cycle**.

**Fig. 5-6. Estimating a Unit's Video Archive.**



**Table 5–2 Event Recording: Duty Cycle Cutoffs**

<b>Duty Cycle (% of recording time)</b>	<b>Estimate for...</b>
0	continuous recording only
10, 20, 30, 40, 50, 60, 70, 80, 90	mostly continuous recording (10), to mostly event recording (90)
100	event recording only

**Rapid Eye Storage Estimator**

To make storage estimates using more parameters (scheduling, audio, motion and so on), Honeywell’s Rapid Eye Storage Estimator is installed with Rapid Eye software. See p. 123.

## Optimizing Recorded Video

**Flexibility**

To optimize the many setup options quickly, use the Automatic Maximization of DSP Performance. Performance maximization can be performed using View software or LocalView. The Quality settings are not affected by it. The result of maximizing performance is shown on the Recording tab and on the Video tab.

**Preparation: contiguous connections**

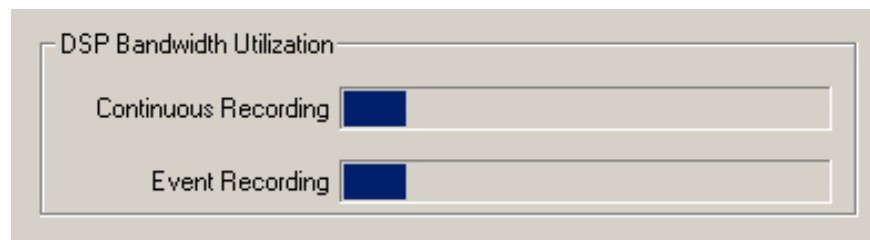
For optimization the digital signal processing (DSP) of video and its storage, an installer needs to make camera connections contiguous, on the back of a unit. Connections are said to be contiguous if they start at camera VIDEO INPUT 1 and continue sequentially. For example: Connecting three cameras to inputs: #1, #2 and #3 is contiguous; connecting the cameras to inputs: #1, #3 and #4 would not; nor would using inputs: #2, #3 and #4.

## Automatic Maximization of DSP Performance

**Gauging the processing load**

The load on DSP is reported on the gauges for DSP Bandwidth Utilization, as you use the Recording tab to customize the settings of recorded video. See fig. 5–7.

**Fig. 5–7. Load on DSP Resources.**

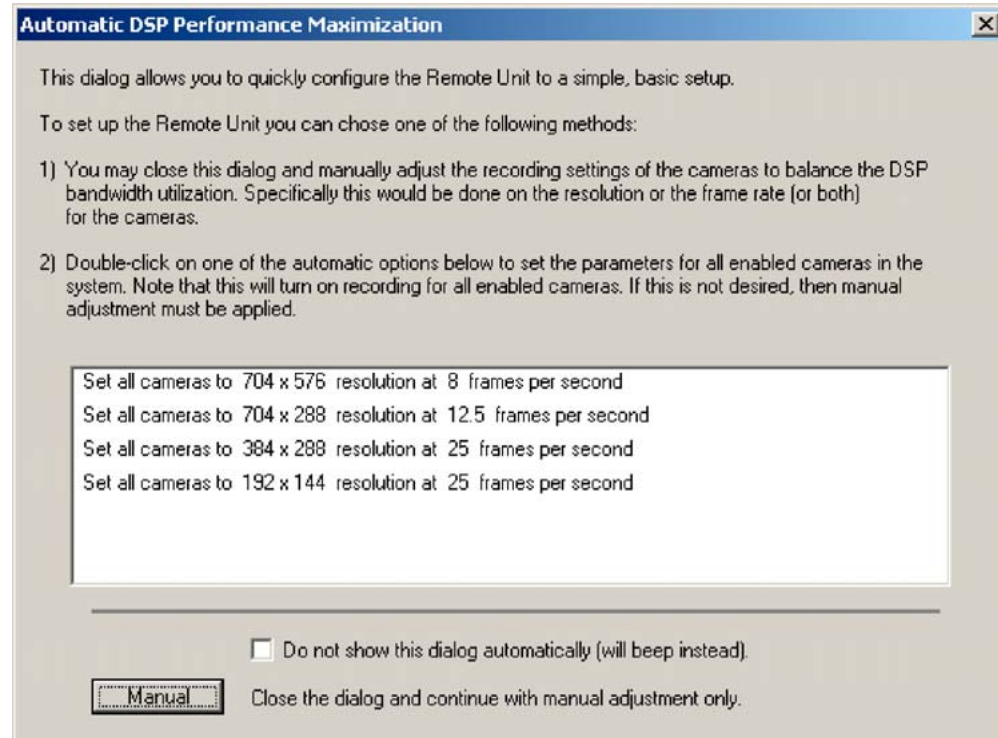




### Automatic display of Maximization tool

If settings are too high, the "DSP Bandwidth Utilization", the Automatic DSP Performance Maximization window is displayed. See figure 5–8.

**Fig. 5–8. The Automatic DSP Performance Maximization Window.**



### Optimization options

The list of options changes depending on:

- The use of NTSC or PAL
- The number of cameras connected to the unit. Optimization cannot be used if the cameras are not connected contiguously. See Optimizing Recorded Video, p. 72.

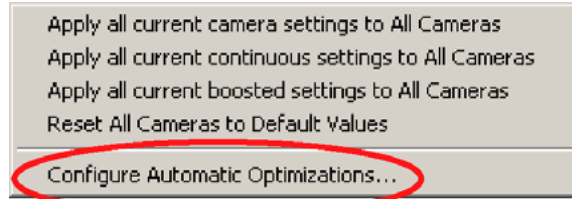
## Making Optimized Resolution and Frame Rate Settings

In the Automatic DSP Performance Maximization window (see fig. 5–8), double-click an "automatic option".

### Manual display of Maximization window

To display the Automatic DSP Performance Maximization window, click the "Configure Automatic Optimizations" command, after right-clicking on the Recording tab. See fig. 5–9.

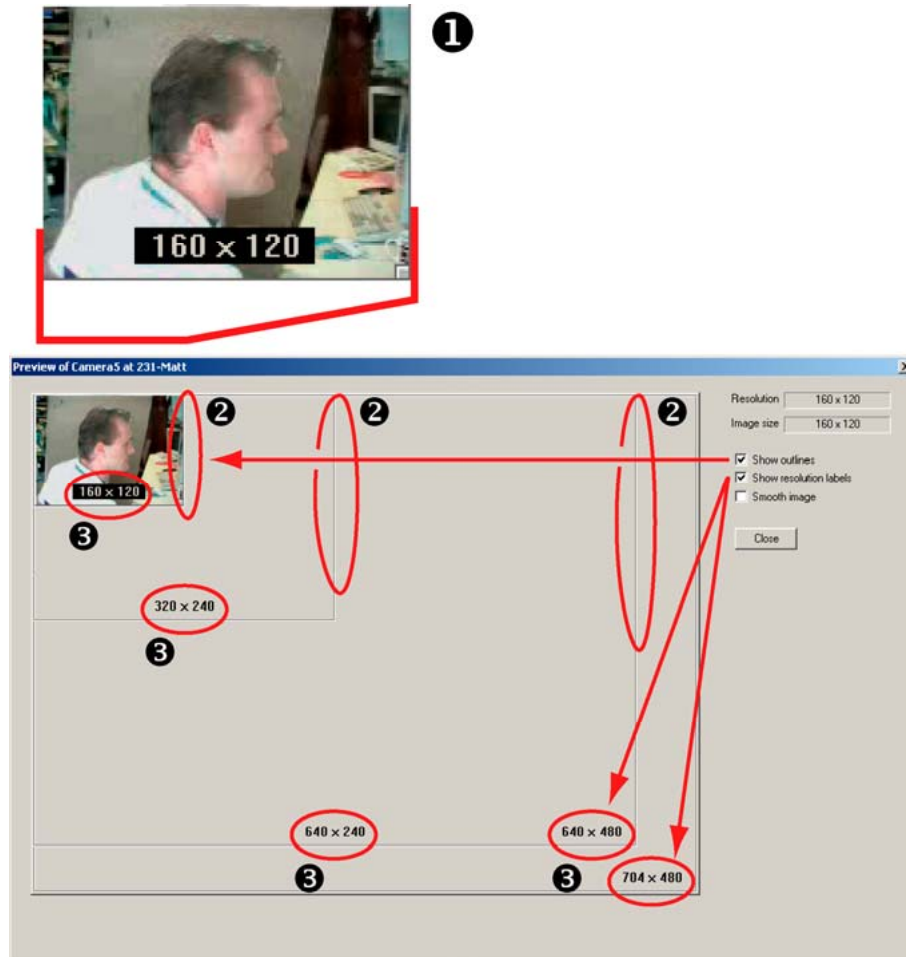
Fig. 5–9. The Configure Automatic Optimizations Command.



## The Enhanced Preview of Resolution

1. Continue or start a Maintenance Session for the Rapid Eye site.
2. On the Video tab, select a camera name in the Name column. The Enhanced Preview button is available if the camera is recording. A camera that is recording is identified by a red dot, between its icon and name.
3. Click **Enhanced Preview**. In figure 5–10, below, the detail (1) shows a feed recorded at a low resolution of 160 x 120, at the size that it would appear on a monitor. The outlines (2) show the optimal size of a video feed on the PC's monitor for that resolution. The many circled resolution labels (3) can be used to display another recording resolution.
4. You have the option of experimenting with:
  - Viewing the video feed at optimal size for a resolution. Click on the resolution labels, within a resolution outline or use the Resolution setting on the Recording tab.
  - Stretching the video image. To compare resolutions at other "image sizes", drag the lower-right corner of the video image. The Image Size box reports the size of the stretched image.
  - Displaying or hiding outlines and labels on the video preview. Select Show outlines and Show resolution labels as needed.

Fig. 5-10. The Enhanced Preview Window.



## Resolution Tips

The following tips prolong your unit's archive of video through lowering the resolution of recorded video.

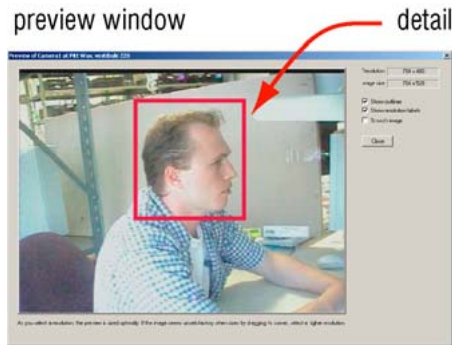
### Do you need to establish an individual's "presence" or a person's identify?

- Presence may be sufficient. For tasks that only involve establishing if "someone has entered the building", or counting cars in a parking lot, and so on, low resolution may be "good enough" to establish presence, helping to guarantee a longer video archive; see figure 5-13. How many cars? Objects can be effectively counted at low resolution make using high resolution unneeded.
- Identification is needed. Unknown vehicles, a person's facial traits and so on, camera position and higher-resolution may be needed. Identification may not be as crucial when subjects are known: employees, uniformed personnel, and so on.
- You have the option of adjusting Microsoft Windows' Display Properties for your PC monitor. See Customizing Windows for a PC Monitor's Settings.

## Comparing the Resolutions of Recorded Video

Fig. 5-11. Using High or Moderate Resolution, 320 × 240 (NTSC), to Identify a Subject.

Detail of recorded video, previewed at a resolution of **704 x 480**; captured while sized optimally. Printed life-size: at size that it would appear on a PC's monitor. The full image would extend beyond the edges of this page.



Detail of recorded video, previewed at a resolution of **320 x 240**; captured while stretched larger than optimal, to compare with higher resolution. Printed at stretched size.



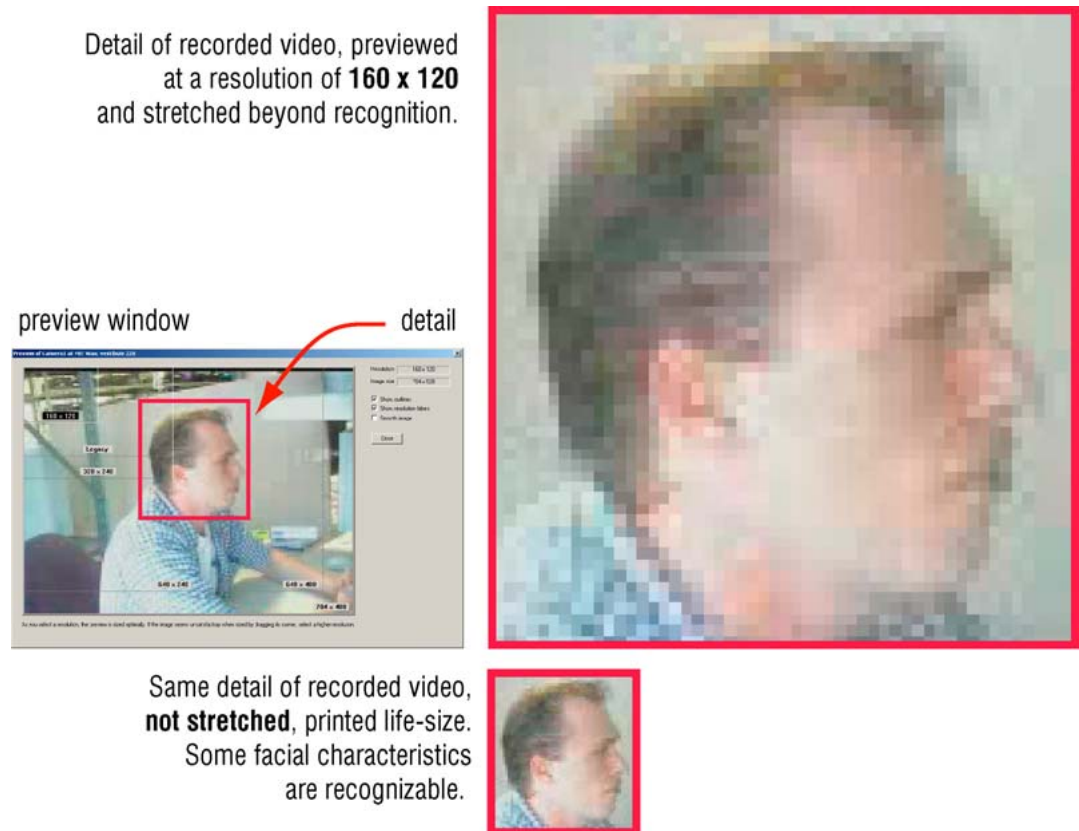
## Security and Presence

Before critical events occur, it is worthwhile to compare video recorded at **Continuous** values with video recorded using **Event** values. You can establish if the resolution is high enough for your organization's security needs. Consult your security personnel to find out whether you need to:

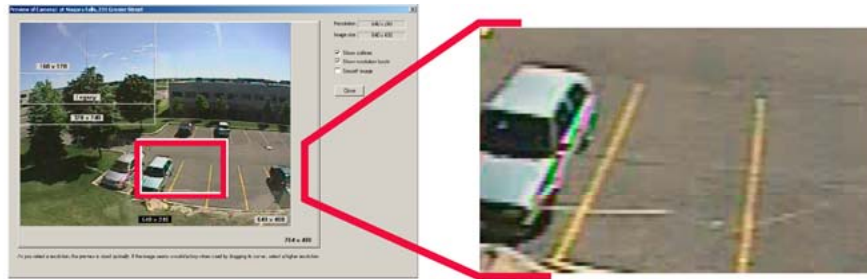
- Establish the presence of known individuals. Lower resolutions are usually adequate and take less storage. Some samples of low-resolution and high-resolution video images are shown in Comparing the Resolutions of Recorded Video, p. 76.

Video images are bitmaps. When a camera window is dragged to a larger size, the pixels of the video feed are also enlarged. The image's sharpness is not preserved; more stretching can degrade the subject of an image beyond recognition. Compare figures 5-11 and 5-12. A high resolution of 704 × 480 (NTSC) shows recognizable facial characteristics and very few artifacts—such as “pixelation”, color variance and so on. If storage time is an issue, recordings at a more modest resolution of 320 × 240 shows almost as much detail. Applications to establish presence or absence of personnel can use even lower resolutions. At 160 x 120 (NTSC) many facial characteristics of a known person are still recognizable even when the imaged is stretched, as in fig. 5-12.

**Fig. 5-12. Using Low Resolution, 160 x 120 (NTSC) to Show Presence.**



**Fig. 5-13. To Establish Presence, Lower-Resolutions May Suffice.**



preview window

Detail of preview, printed at actual size.

Detail of recorded video, previewed at a resolution of **704 x 480**. Printed at actual size.

Detail of recorded video, previewed at a resolution of **640 x 240**; stretched larger than optimal, to compare with higher resolution. Printed at stretched size.



**Retouching stills with software**

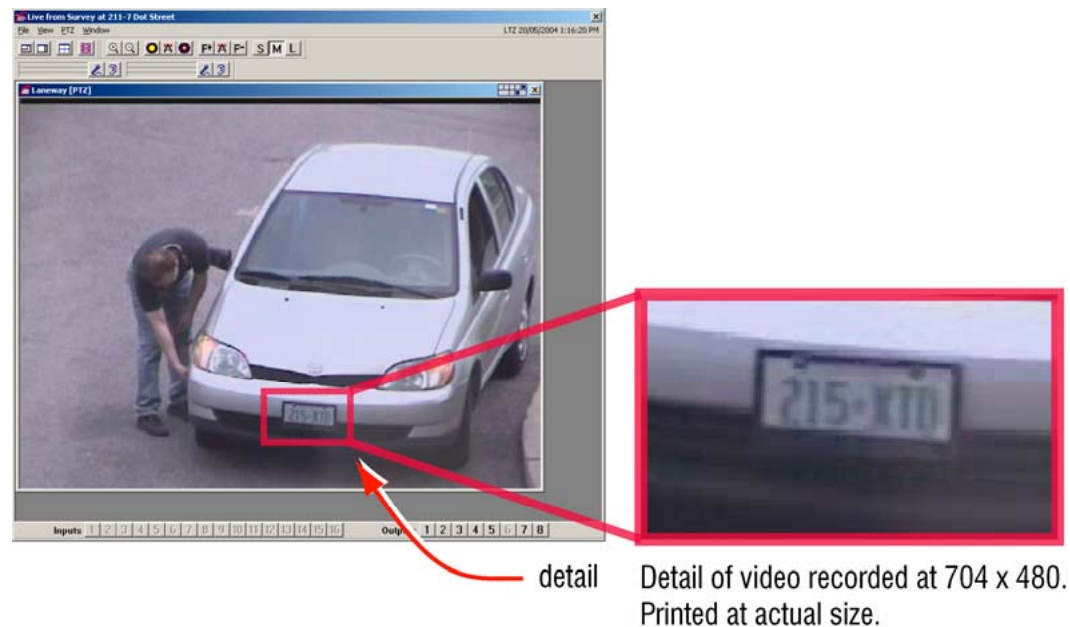
Bitmap editing tools and imaging software can be used to enhance video stills or screen captures. Though retouching may void the admissibility of the video as evidence in a court of law, it can be of use to highlight a detail or trait. Commercial software for retouching bitmaps includes: Paint-Shop Pro, Corel Photopaint, Adobe Photoshop, and others. For screen captures, use Microsoft Windows, TechSmith's SnagIt, and so on.

**Screen area: size of camera windows on a PC monitor**

Adjusting Microsoft Windows' Display Properties for a PC monitor can have an effect on how resolution is perceived. See Customizing Windows for a PC Monitor's Settings, p. 82.

## Camera Tips for Identification: Quality and Resolution

Fig. 5-14. Camera Distance Can Be more Important than High Resolutions.



Camera placement can be a crucial factor when troubleshooting resolution issues. If higher Quality and Resolution values are insufficient for your video needs, consider consulting your system installers about:

- Monitoring small or faraway objects. For license plates, facial traits, and so on, the closeness of a camera to its subject and the ability to zoom can matter as much as, or even more than, higher resolutions and higher quality.
- Using a gauntlet strategy. To identify vehicles by their license plate, install a camera at an entry or exit point, at ground level. Close camera shots coupled with high resolution give the best detail.
- Covering an area with a duo of cameras. One camera at a payment counter can be zoomed to identify facial characteristics, while another can be installed a little farther away to survey more of the scene.
- Using higher Quality and lower Resolution. The results can be better, with less impact on the video archive.

## Resolution Gauge for Retrieval Session

The resolution gauge appears when running View software. The resolution gauge for recorded video differs from the gauge for live video. The gauge for live video is shown and explained in the *Rapid Eye View Software Operator Guide*.

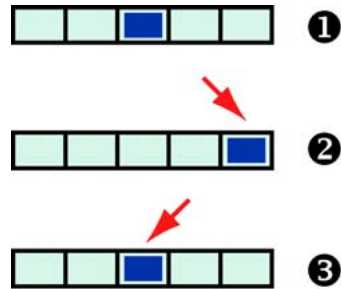
### A gauge that indicates the resolution at which the recording was made

When an operator runs a retrieval session, a resolution gauge is displayed on each camera window indicating the resolution at which the video was recorded.

### NTSC gauge

The NTSC gauge is shown in figure 5–15. (1) shows a dot that indicates the resolution of video. The dot changes position when recording settings switch to and from **Continuous Recording** settings to **Event Recording** settings. Here, 640 x 240 continuous, is shown for NTSC. While **Event Recording** occurs (2), the dot moves to the right. When the **Event Recording** stops (3), the resolution gauge again shows the resolution setting for continuous recording.

**Fig. 5–15. Resolution Gauge for Recordings Made with NTSC Cameras.**



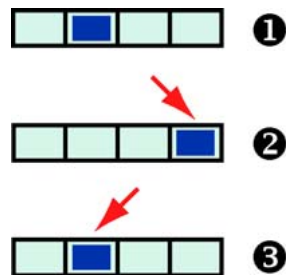
The dots movement depends on the settings made by your organization's Multi SA for **Continuous Recording** and **Event Recording**.

### PAL gauge

The gauge for PAL is shown in figure 5–16. (1) shows a dot that indicates the resolution of video. The dot changes position when recording settings switch to and from **Continuous Recording** settings to **Event Recording** settings. Here, 384 x 288 continuous, is shown for PAL. While **Event Recording** occurs (2), the dot moves to the right. When the **Event Recording** stops (3), the resolution gauge again shows the resolution setting for continuous recording.

The dots movement depends on the settings made by your organization's Multi SA for **Continuous Recording** and **Event Recording**.

**Fig. 5–16. Resolution Gauge for Recordings Made with PAL Cameras.**





## Resolution Reference: Recorded Video

**Table 5-3 Recording Resolutions for Multi-Media DSP (pixel × pixel): NTSC and PAL**

NTSC						
<b>Resolution</b>	160 × 120	legacy <sup>†</sup>	320 × 240	640 × 240	640 × 480	704 × 480
<b>Comment</b>	lowest resolution	320×192; default for upgrades from NTSC, set at legacy	default when new unit set for NTSC	also called "half"	also called "full"; highest setting for Multi-Media LT	highest NTSC setting
<b>Gauge in a Retrieval Session‡</b>		n/a				
PAL						
<b>Resolution</b>	192 × 144	384 × 288	704 × 288	704 × 576		
<b>Comment</b>	lowest resolution	Honeywell's default for PAL, including upgrades	Highest setting for Multi-Media LT	highest PAL setting		
<b>Gauge in a Retrieval Session‡</b>						

<sup>†</sup> "Legacy", used by older Multi units, is included for compatibility. There is no gauge for the NTSC legacy setting. The Legacy resolution is not shown in the Enhanced Preview.  
<sup>‡</sup> Gauges are explained at the start of Resolution Reference: Recorded Video.

**Table 5-4 Recording Resolutions for Multi-Media LT (pixel × pixel): NTSC and PAL**

NTSC			PAL			
<b>Resolution</b>	160 × 120	320 × 240	640 × 240	192 × 144	384 × 288	704 × 288
<b>Comment</b>	lowest NTSC resolution	default setting for NTSC on a new unit.	highest NTSC setting	lowest PAL resolution	default setting for PAL, including upgrades	highest PAL setting
<b>Gauge During Retrieval*</b>						

\* Gauges are explained at the start of Resolution Reference: Recorded Video.

## Customizing Windows for a PC Monitor's Settings

### Using Microsoft Windows

Honeywell recommends that if operators plan to use View's higher resolution settings:

- The Screen area (for the monitor) be set to "1280 by 1024 pixels" or higher to run View. Microsoft Windows is used to set this value, not View software. Recommended values are listed in table 5-5. The PC monitor's refresh rate can also be changed. See Larger Monitors and Microsoft Windows, p. 83.

Honeywell also recommends that if you plan to display ten or more cameras at once on a PC screen that you consider:

- Using two PC monitors at the same time. See Microsoft Dual View and Rapid Eye View Software, p. 82.

**Table 5-5 Display Properties for Optimal Rapid Eye Video at Higher Resolutions**

Screen area (pixels)	For Multi-Media DSP	For Multi-Media, Multi-Media LT and over dial-up connections**
1600 by 1200	yes	yes
1280 by 1024	yes	yes
1280 by 960	yes	yes
1152 by 864	no *	yes
1024 by 768	no	yes
800 by 600	no	no*

\* Video is visible and workable even when using smaller screen area settings; see figure 5-17.

\*\* Dial-up connections using few cameras are faster, as is retrieval of video recorded at lower resolutions. Lower settings for Screen area may be sufficient for such use.

## PC Monitor's Refresh Rate

Higher refresh rates can alleviate eye fatigue when monitoring video over time. You can change the Refresh Frequency, and the refresh rate (Hertz), as needed.

Not all monitors and video cards support the resolutions indicated in the preceding sections, nor do all offer various refresh rates. Consult the documentation supplied with Microsoft Windows, your monitor and the video card.

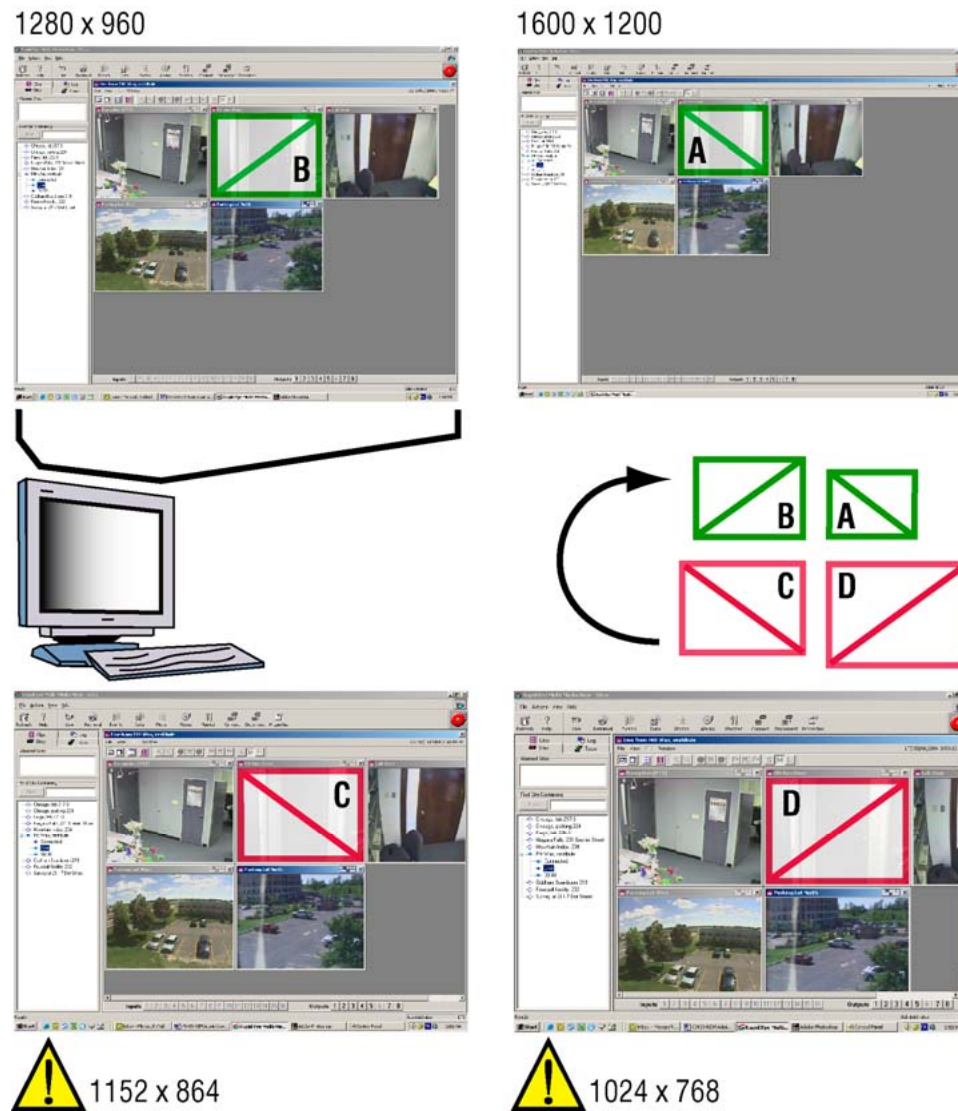
## Microsoft Dual View and Rapid Eye View Software

### Using two monitors and running View software

Two monitors can be effectively used with Multi-Media View to display more camera feeds at once. To set up a Dual View system, see your Microsoft documentation. Hardware note: a second video card is needed on the View operator's PC for Microsoft's Dual View setup.

## Larger Monitors and Microsoft Windows

Fig. 5-17. Microsoft Windows' Screen Area Settings.



### Setting Microsoft Windows

Larger computer monitors and better video cards are assets when setting Microsoft Windows for high Screen area settings. Note how in figure 5-17, the change in size of the camera windows, as the screen area changes—a camera window is highlighted for comparison. More cameras can be seen at once, and at higher resolutions (here five cameras at 320×240 resolution) when a recommended setting is used, as in A or B. Even at settings that are not recommended, video can still be viewed, though: some camera windows can appear to extend beyond the monitor's surface. At any setting, camera windows can be dragged as needed and the player window scrolled.

## Environmental Interference for Video Feeds

### Preventive measures

Checking one's installation for hard-to-predict situations includes spot-checking:

- Live video. Run a Live Session on a regular basis. Such spot checks offer confirmation that sites have not been vandalized, rendered ineffective by the environment or tampered with by an operator. See "physical compromise", below.
- Recorded video. After a day or two, run a retrieval session to look for artifacts in recorded video, at every half-hour or so, over a 24 hour period. The darkness of night or bright sunlight may indicate the need for changes in camera position or lighting. For outdoor cameras, it can be worthwhile to run such spot checks seasonally. See "physical compromise", further down.
- After use of PTZ. A camera with the ability to pan-tilt and zoom can be set to respond in a variety of ways after use and should be spot-checked. Run a retrieval to do so. See Behavior of PTZ After a Session Closes, on p. 93.
- Scheduling. The video archive can be spot-checked for recorded video when cameras are scheduled to record it. For scheduling, see Scheduling: Configuration, p. 105.

## Physical Compromise

Even when cameras are set as recommended, changing environmental factors can compromise video at the source. Obvious factors include:

- Direct sunlight at short times during the day. Daybreak can interfere with recording for cameras aimed East, as can sundown for cameras pointing West.
- Dew, frost or kitchen grease. Check camera lenses, or windows between the camera and the subject for transparency and cleanliness.
- Darkness. Without lighting or infrared cameras, indoor rooms and nighttime can make cameras ineffective.
- Cameras at an outside window, in a room that remains lit during evenings. Reflection from the window can hamper or block visibility outside.
- Opaque objects. Even small objects can obstruct a camera when near and hamper an operator's view of a site. Large mobile objects, such as a truck also can be used to compromise video of an event. See also "vandalism", below.
- Power outage. Even when plugged into a UPS, prolonged power outages can compromise the recording of video.
- Vandalism. Tampering with cameras, Multi-Media units or other hardware. This can be done by damaging hardware directly or indirectly interfering (by spraying paint, fog or moving objects in the way), or even through reconfiguration, using View software.

## Pan, Tilt, and Zoom (PTZ) Setup

### Flexibility

Use of panning-tilting and zooming (PTZ) is optional, even with cameras that have the capability to pan, tilt and zoom. Not all cameras have PTZ features. Check with your installer if you are unsure.

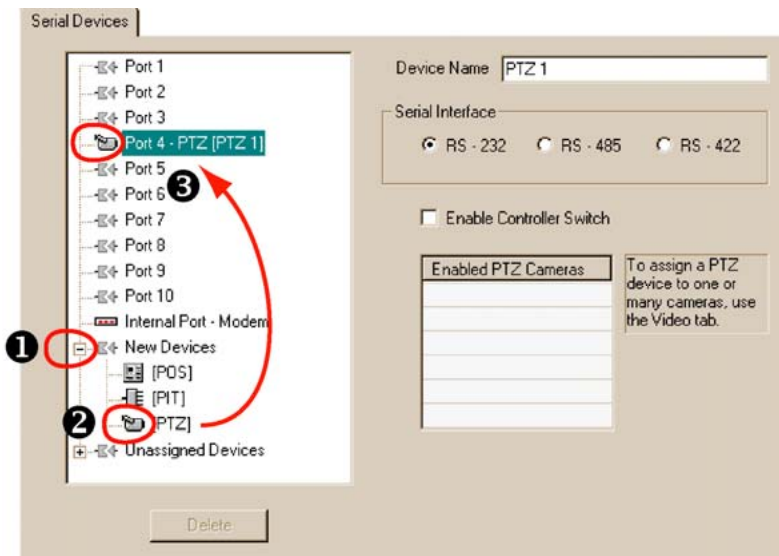
### Preparations

To prepare a Multi-Media unit to use cameras with PTZ capability, a Multi SA needs to setup a:

- **Serial device for PTZ.** A Multi SA can consult the installer to find out which serial ports of the unit are connected to the serial communications line of PTZ domes / PTZ cameras. For setting a PTZ device, see the procedure: To Assign and Set a New PTZ Device, below.
- On Multi-Media units with three or more serial ports, use any port for PTZ. For units that have only two serial ports, Honeywell recommends that PTZ domes be connected to port 2; other serial devices might be assignable only to port 1.
- Many domes, daisy-chained can be connected to the Multi-Media unit if they use the same Communications settings for PTZ. For the address set on each camera, consult the installer. Other dome communications settings can be found in the dome-manufacturer's documentation.

## Serial Device Settings for PTZ

Fig. 6-1. Assigning a PTZ Driver to a Port on the Multi-Media Unit.



## To Assign and Set a New PTZ Device

1. Find out to which serial port on the Multi-Media unit is connected to the PTZ dome(s). The installers connected the **Data In** port of domes (an RS-485 connector) to either:
  - One of the serial ports on a Rapid Eye unit. The port number for a dome can differ from that of another dome.
  - A bus, connected to one of the serial ports on a Rapid Eye unit. The port number is the same for the domes on that bus.
2. Continue or start a Maintenance Session.
3. Click the Serial Devices tab.
4. Expand the New Devices group.
5. Drag the PTZ icon to the Port that matches the unit's serial port identified in step 1. If you drop the icon on a port that is already assigned to another device, the PTZ device displaces it; the displaced device is sent to the Unassigned Devices group.
6. You have the option of renaming the device. Click the Device Name box and type. A maximum of thirty-two characters and numbers are allowed, including spaces.
7. Select the serial interface protocol: RS-232, RS-485, or RS-422.
8. You have the option of:
  - Selecting the Enable Controller Switch. A checkmark sets the Multi-Media unit's OUTPUT 1 to send a signal whenever a PTZ camera is selected during a Live session. Installers can connect OUTPUT 1 to the external controller so that the signal disables the controller while a Multi-Media operator uses a PTZ camera. When a PTZ camera is not selected, the signal from output 1 stops so that control of the PTZ serial bus is returned to the external controller.
  - Assigning another PTZ device to another Port (or to the Unassigned Devices group). To do so, repeat steps 4 to 7.

### ACUIX dome camera domes

For ACUIX dome camera domes, you have the option of using the Intellibus PTZ driver. See ACUIX Dome Camera, on p. 99.

## Video Tab Settings for PTZ

### Preparations

Assign a PTZ serial device, as explained in procedure *To Assign and Set a New PTZ Device*, above. The device can be assigned to either:

- One of the ports on the Multi-Media unit.
- The Unassigned Devices group.

### Tip

**The signal format for all cameras (NTSC, PAL) is set on the System tab. See System Tab in a Maintenance Session, p. 134.**

### Using many PTZ domes/cameras on one serial communications line

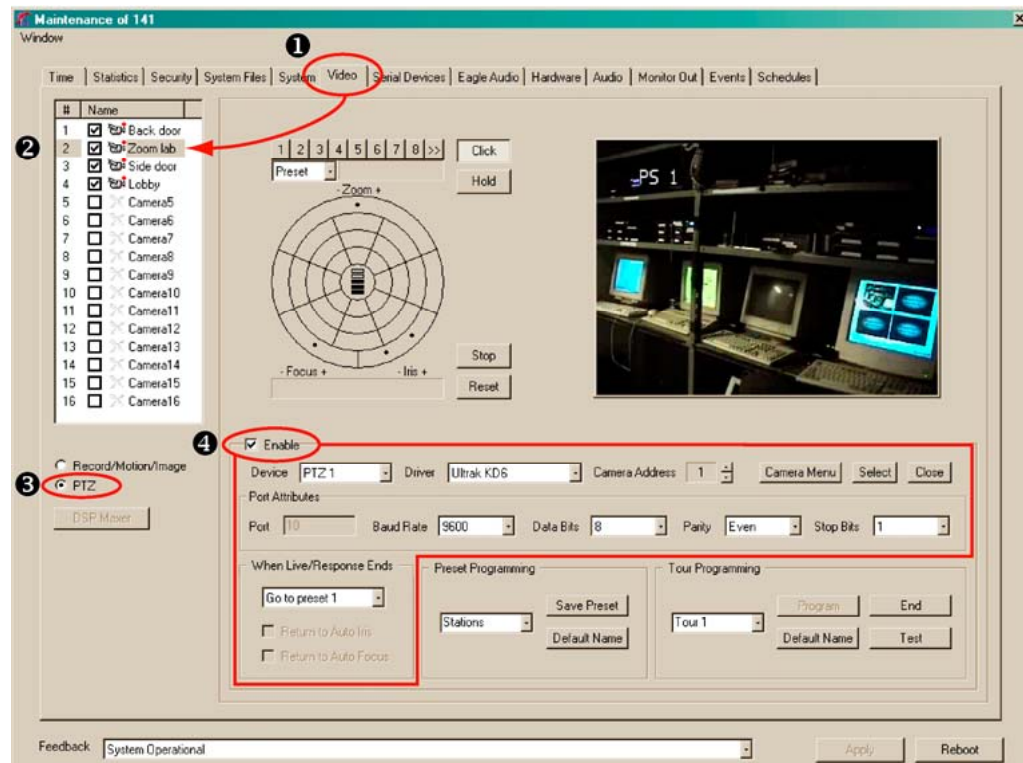
If more than one PTZ camera share the same serial communications line. If so, make a note of:

- The address set on each camera.
- The driver needed for the make and model of dome; if the domes require different drivers, they cannot share the same port/serial communications line.

## To Enable a PTZ Camera

1. Continue or start a Maintenance Session for the Rapid Eye site.
2. Click the Video tab.
3. Click **PTZ**. See figure 6–2.
4. Select the Enable box. The PTZ boxes and the PTZ controller become available. Note: the Enable box is not available if a PTZ serial device is not assigned. To assign a PTZ device, see the procedure: To Assign and Set a New PTZ Device, above.
5. Select a driver that matches a PTZ camera. Drivers are listed in table 6–1.
6. If more than one PTZ camera is sharing the device, select a Camera Address that matches the address set on the dome hardware.
7. Select the port attributes of the PTZ dome: Data bits, Stop Bit, Baud Rate and Parity Bit.
8. Select the position that a PTZ camera takes after a View operator closes a Live Session. Consult your security officer before changing the value in the When Live Closes box. See Behavior of PTZ After a Session Closes and table 6–2, on p. 94.
9. Cameras that have a command menu can be set using the Camera Menu button. Use the dartboard control or the rubber band control to choose a command; use the Select button to change a value. The PTZ controls are explained next, in section Using a PTZ Camera.

Fig. 6–2. Configuration Settings (4) for a PTZ (3) Camera (2), on the Video Tab (1).



**Table 6–1 PTZ drivers for controllers and domes**

<b>Driver (name)*</b>	<b>Baud (rate)</b>	<b>Support for (dome/controller/PIT device)</b>
Bossware	19200	PIT device, to which domes are connected.
Honeywell Fixed Camera	9600	Honeywell HCU484
Intellibus	38400	ACUIX dome camera
Javelin 308	9600	Javelin 308 Controller
Kalatel	9600 or 2400	Kalatel KTD 312 Cyberdome
Pelco D	4800, 9600, or 2400	Pelco D
Pelco P	2400	Pelco P
Rapid Dome/Orbiter	9600	RapidDome or Orbiter
SensorMatic RS422	4800	SensorMatic RS422: Delta and Speed
Ultrak (using VCL)	2400	Ultrak (configured as VCL)
Ultrak KD6	9600	KD6, HD6, HD6i

\* The drivers are not listed alphabetically in the software. A driver can be used with domes other than those listed. For other domes, controllers or PIT devices, consult their documentation.


## Using a PTZ Camera

Three PTZ controls are available to make PTZ commands: a dartboard-like control, a rubber band control and a Zonal Mode control.

Either is available while running a Live session or while using LocalView. The right to use a PTZ camera is granted in the operator's Multi-Media account; see Granting Rights, p. 158.

## To Display the PTZ Dartboard Control

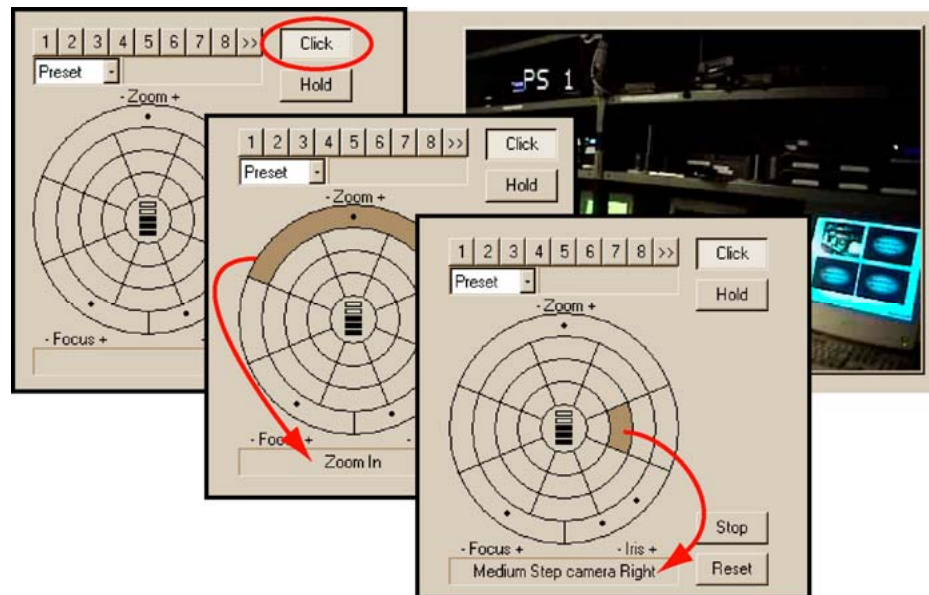
The PTZ dartboard control can be obtained in three situations:

- During a Maintenance Session, when PTZ is selected, the PTZ control is displayed on the video tab. See the first steps of procedure To Enable a PTZ Camera, above.
- During a Live session, select or add a video stream from a PTZ camera. Click , the "Enable PTZ Control" button.
- In LocalView, a "PTZ" button is shown when a Live tab is selected. It is available when a PTZ camera is selected.



## Using the Dartboard Control

Fig. 6-3. Dartboard Control for PTZ camera, Showing Command Feedback.



1. On the PTZ Control, click either **Click** or **Hold**.
2. Move the mouse pointer over the dartboard-like control to highlight areas of the dartboard. Each area on the dartboard offers textual feedback in the box, below the control. See figure 6-3.
3. Click when the command that you need is highlighted. If you are using the Hold option, the mouse button can be held pressed to make the command last as needed.

## Toggling between Zonal Mode and Pull Mode

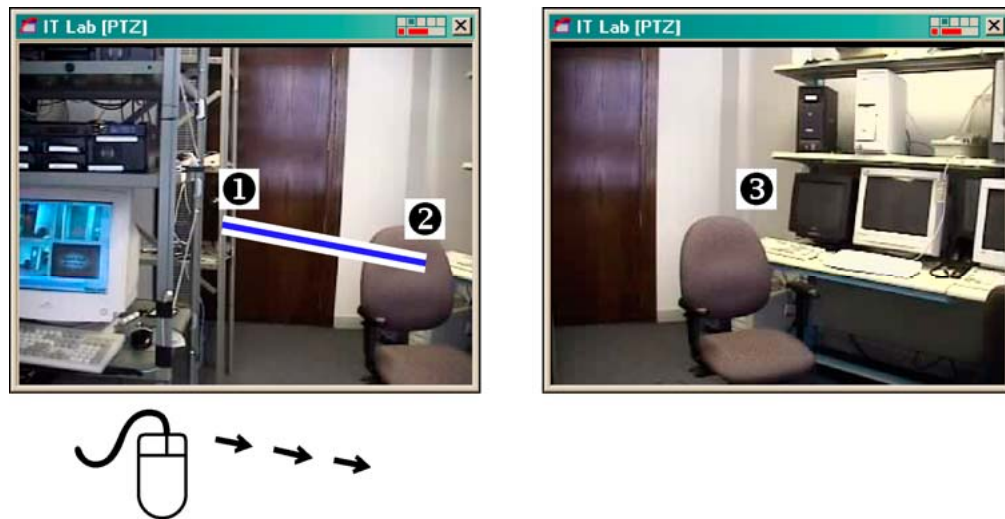
1. In a Live player, select a PTZ camera.
2. In the View menu, select Options.
3. Click **Zonal PTZ Control Mode**.
  - If there is no checkmark next to the command, Zonal mode is enabled and replaces the Rubber-Band-like control (Pull Mode).
  - If there is a checkmark next to the **Zonal PTZ Control Mode** command, Zonal mode is replaced by the Rubber-Band control.

### Tip

The rubber-band control cannot be used at the same time as the zonal mode control, and vice-versa.

## Pulling the Rubber-Band

Fig. 6-4. Dragging the Mouse Pointer in a PTZ Camera Window.

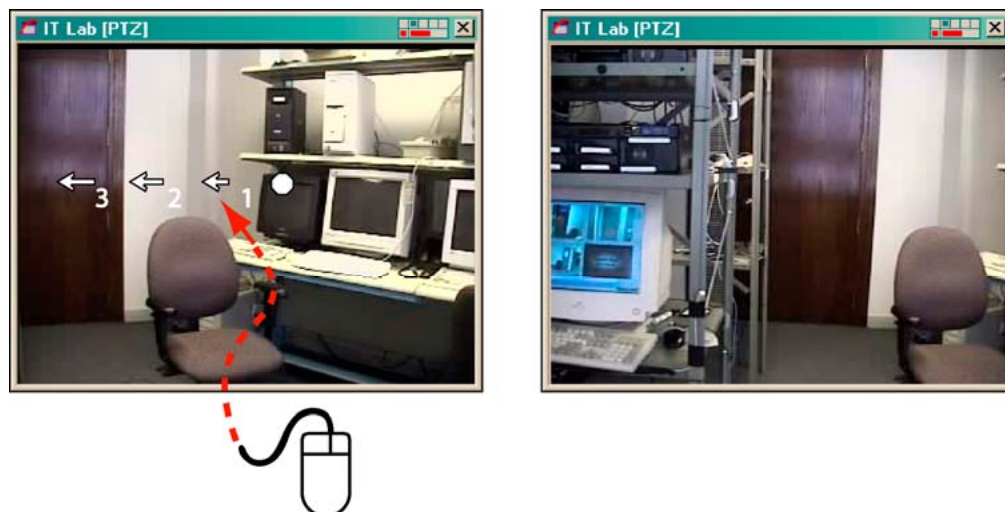


On the video image, click and drag the mouse. A line is overlaid on the video. Lengthening the line speeds-up the PTZ camera's panning or tilting. See figure 6-4.

- **Pan.** To pan right and to tilt down, slightly, drag the pointer from (1) to the right (2). In View, the band has a single color; here, it is highlighted for illustration.
- **Zoom.** Use the wheel on the mouse. If the mouse does not have a wheel, see Using the Dartboard Control, above.
- **Presets and other commands.** In a Live session and in LocalView, right-click on a PTZ camera's video to obtain a menu of PTZ commands and video resolution commands. In a Maintenance Session, use the commands on the dartboard.

## Using Zonal Mode

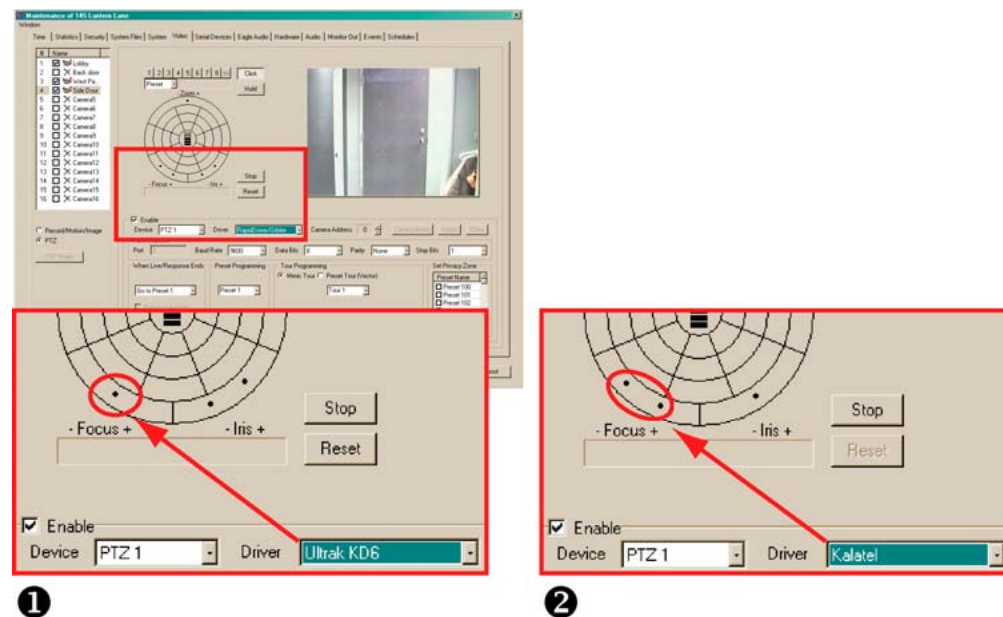
Fig. 6-5. Using PTZ Zonal Mode.



- To pan or tilt, move the mouse through the PTZ camera's window until the pointer changes to a numbered arrow. Click. Figure 6–5 shows the Zonal Mode for panning left. For continuous panning or tilting, click the arrow furthest from the center.
- To stop continuous panning or tilting, move the mouse through the PTZ camera's window until the pointer changes to an octagon. Click.
- To zoom, use the wheel on the mouse. If the mouse does not have a wheel, see Using the Dartboard Control, above

## Programming a PTZ Dome Camera

Fig. 6–6. PTZ Dome Camera without Auto-focus (1) or with, Between the Dots (2).



### PTZ preset

Presets are set during a Maintenance Session. A PTZ camera can be set to return to the first preset when use of the camera ceases, when a Live session ends.

### Auto-focus

View supports an auto-focus control when two dots appear in the “– Focus +” arc of the PTZ controller. Click between the dots to toggle auto-focus ON/OFF. See figure 6–6.

### Auto-iris

View supports an auto-iris control when two dots appear in the “– Iris +” arc of the PTZ controller. Click between the dots to toggle auto-iris ON/OFF.

## To Configure a Preset on a PTZ Camera

1. Continue or start a Maintenance Session.
2. Click the Video tab.
3. Click **PTZ**.
4. Select a camera whose PTZ preset you need to set.

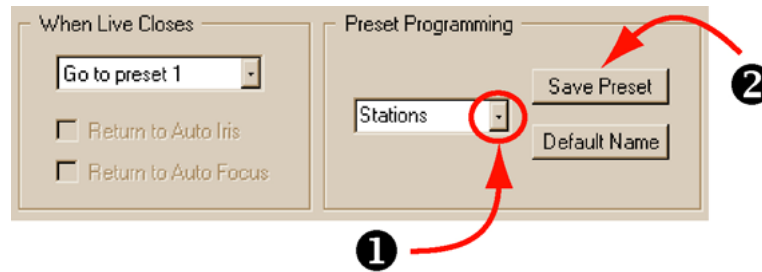
5. In the Preset Programming area, click the arrow button; see figure 6–7, below. A list appears; by default, it contains “Preset 1”, “Preset 2”, “Preset 3” and so on; in all: 127.

**Tip**

**Preset 1 may have been already set by an installer, to be used after close of session. See Behavior of PTZ After a Session Closes, p. 93. Consult your site’s installer or security officer before changing the first preset of a PTZ camera.**

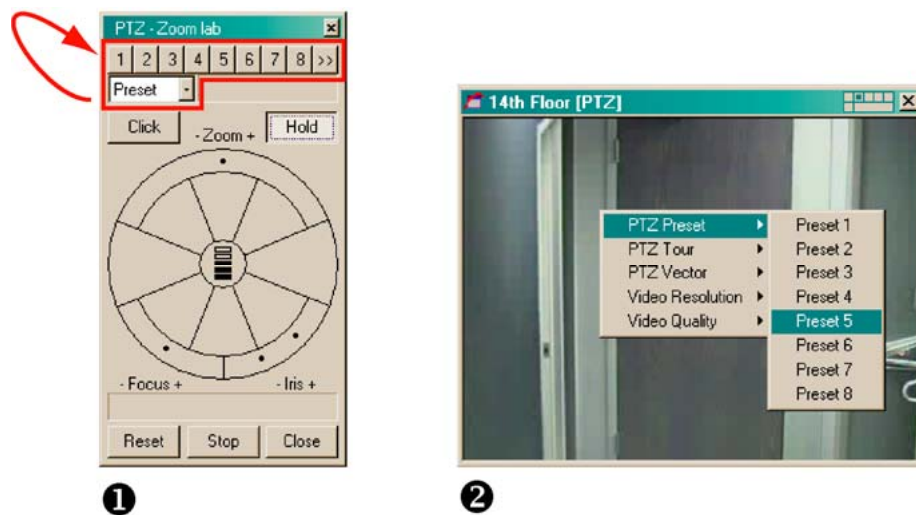
6. Click an item in the Preset Programming list.
7. You have the option of renaming the preset by typing into the box.
8. Set the camera’s pan position, tilt angle and zoom amount, as explained in Using the Dashboard Control, p. 89. Continuous panning can also be selected.
9. Click **Save Preset**. The camera’s pan position, tilt angle and zoom amount are saved.
10. You have the option of immediately:
  - Setting another preset. Repeat steps 4 to 9, using another preset in step 6.
  - Testing the preset. See the next procedure.
  - Setting presets for another PTZ camera at that site.


**Fig. 6–7. Programming a PTZ Preset.**



**To Test a Preset**

**Fig. 6–8. Testing Presets on a PTZ Camera.**



1. You have the option of running either:
  - **A Maintenance Session.** Click the Video tab, select a PTZ camera whose presets are to be tested, and click **PTZ**; the PTZ dartboard controller is displayed.
  - **A Live Session.** select or add a video stream from a PTZ camera. Click  the "Enable PTZ Control" button. The dartboard controller is displayed.
2. On the dartboard control, leave or set the drop-down arrow box to "Preset". See figure 6–8.
3. Click the numbered buttons above the Preset box. The PTZ camera moves to the preset position. If the camera does not move, check your configuration. Either:
  - A preset has not been set for that number.
  - The preset duplicates the settings of the one used previously.
  - The camera is indicated as being PTZ but is not.

**PTZ and motion detection**

When an alarm based on motion detection is enabled on a PTZ camera, use of PTZ functions will most likely trigger that alarm. You can limit the number of alarms triggered by using the Delay slider in the motion detection controls. The alarm schedule can also be changed to stop alarms at certain times when PTZ use is anticipated. See Motion Detection, on p. 116 and Events Defined, on p. 187.

**Ultrak KD6i domes**

auto-iris. Before an aperture setting can be changed manually on an Ultrak KD6i dome, the operator needs to turn OFF the auto-aperture. Auto-aperture is also known as "auto-iris" on the PTZ controller.

return to auto-focus. This command has no effect on Ultrak KD6i domes.

**Kalatel domes**

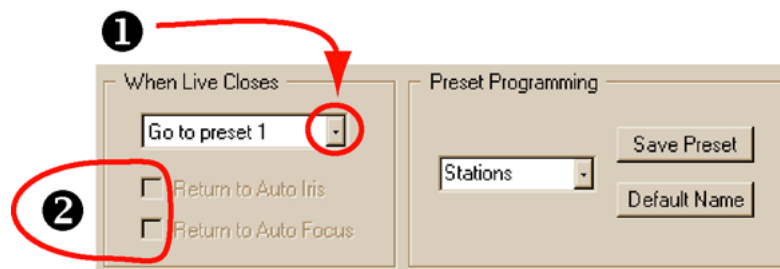
On Kalatel domes, the iris controls in View toggles coarse brighter/darker settings, not a gradual open or close. Auto-iris has no effect.

## Behavior of PTZ After a Session Closes

**Position of PTZ camera after close of session**

When a Live Session ends, a security officer may need a PTZ camera to return to a set direction and zoom, while the camera is not being monitored by a View operator.

**Fig. 6–9. PTZ Camera: Behavior after Use.**



1. Using View, continue or start a Maintenance Session at a site where camera(s) featuring pan, tilt and zoom (PTZ) need their post-session behavior set.
2. Click the Video tab.
3. Click **PTZ**. Check if the Enable box shows a checkmark. Post-session behavior cannot be set unless PTZ is enabled.
4. Click the arrow of the When Live Closes box; select a post-session behavior; they are listed in table 6–2.

**Table 6–2 Position after Close of Session, for PTZ Cameras**

<b>At Session End</b>	<b>Comment / Behavior</b>
Stay put	The camera remains in the last position used by the operator. If it is panning, it keeps on panning; if it is not moving, it stays that way, and so on. The “stay put” behavior makes available the Return to Auto-iris and Return to Auto-focus options.
Go to preset 1	The camera returns to “preset 1” configured using Multi. See the procedure: To Configure a Preset on a PTZ Camera, on p. 91 for configuring the first preset of a PTZ camera.
Start tour 1*	Some camera models can be programmed to move independently when not in use by an operator. For information on how to program a PTZ tour, see the documentation that came with the domes connected to the Multi-Media unit.

\* A “PTZ tour” differs from: (a) site tours (see Touring Many Sites) and (b) local camera tours using a monitor at the Multi-Media site.

#### **PTZ and motion search**

Video recorded while a PTZ dome or camera can be searched for motion. When the camera is fixed, results are as expected; see Motion Search, on p. 120. However, motion search is ineffective on video recorded as a PTZ camera is panning, tilting or zooming. If you plan to use motion search on a PTZ camera, use “Stay put” or a preset after close of session. See table 6–2.

Motion search can also be used to find out when a PTZ camera was moved, if that camera should be staying put.

#### **Constant panning and video archive**

Recording a video feed from a camera that pans constantly requires much more storage. If the duration of your video archive is a concern, see Quality, p. 125.

#### **Ultrak KD6i dome: restriction**

Return to auto-focus. Has no effect on the Ultrak KD6i dome.

**Do not use the “Return To Auto-Iris” on Ultrak KD6i domes.**

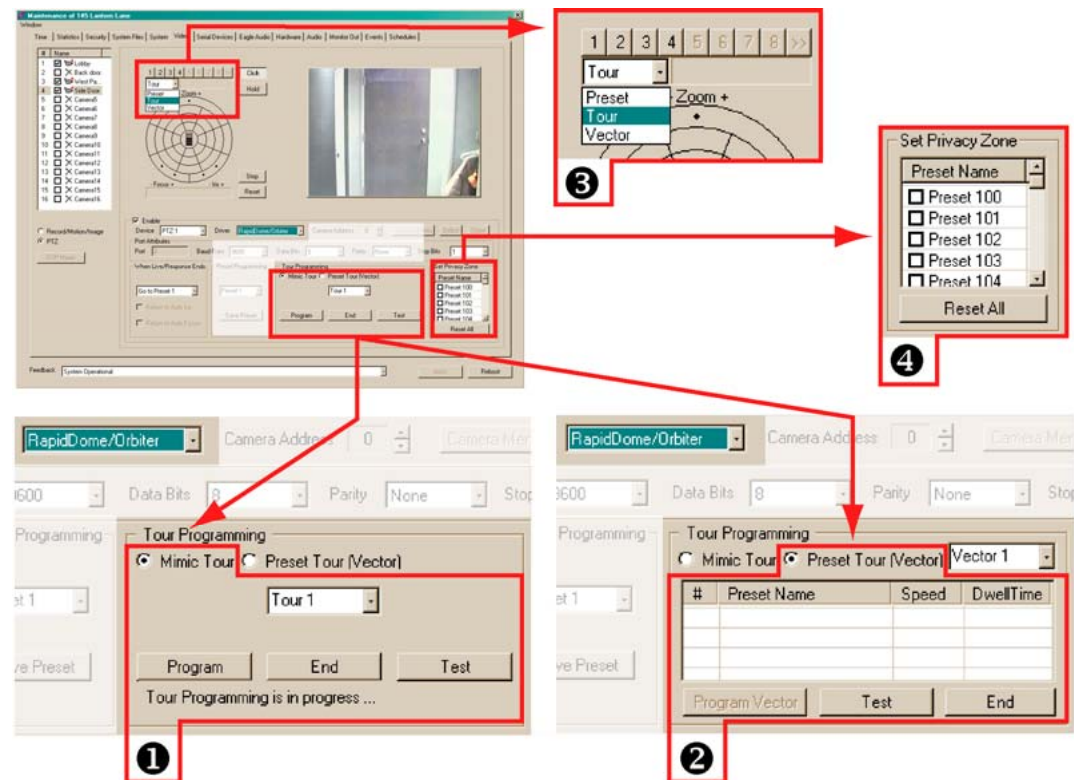


## Support for RapidDome PTZ Features

A Multi SA can preset a RapidDome PTZ dome, using View software, for:

- Mimic tours. A mimic tour recalls the commands to pan, tilt and zoom, that were sent to a RapidDome camera. Mimic tours are also known as path tours.
- Preset tours. A “preset tour” recalls a list of PTZ presets. Before setting up a preset tour, someone is needed to setup presets.
- Privacy zones. Use presets 100 to 127. The video feed is not displayed when a dome is positioned at these presets.

Fig. 6–10. Detail of PTZ Setup for the RapidDome Driver.



Detail of PTZ setup for the RapidDome Driver, on the Video tab, during a Maintenance Session. Details show controls for the mimic tour (1), preset tour (2) and privacy zone (4). The selection of presets and tours is made using the list (3) above the PTZ controller. In the list, “Vector” is used to select a preset tour.

## RapidDome PTZ Tours

1. In the PTZ controller, click the arrow in the box under the row of numbered button to display a list, showing: “Preset”, “Tour” and “Vector”. See figure 6–10–(3), on page 95.
2. Do one of the following:
  - For mimic tours, select “Tour”.
  - For preset tours, select “Vector”.
3. Click a button in the row of numbered buttons, above the box that shows the list.

## RapidDome Mimic Tour

1. While using View, select a site that has one or more RapidDome PTZ cameras.
2. Run a Maintenance Session; click the Video tab.
3. Select a dome camera.
4. Click **PTZ**. Check if the Driver is "RapidDome/Orbiter". If not, this procedure cannot be used. In the "Tour Programming" section, the Mimic Tour is selected by default. See figure 6–10, above. You have the option of selecting which of the four mimic tours you plan to setup. To do so, click the arrow button above the End button. A list appears, showing "Tour 1, Tour 2, Tour 3 ..." by default. Click an item in the list.
5. Click **Program**. A message appears below the buttons in the Tour Programming section: "Tour Programming in progress ..." See figure 6–10, above.
6. Pan, tilt and zoom the camera, as needed.
7. Click **End**.
  - You have the option of testing the mimic tour by clicking Test.
  - You have the option of renaming the mimic tour. Click inside the box in the Tour Programming section. Type a name. Save the name by clicking the mouse.
8. You have the option of programming another mimic tour for the dome camera; repeat steps 5 to 7 as needed.

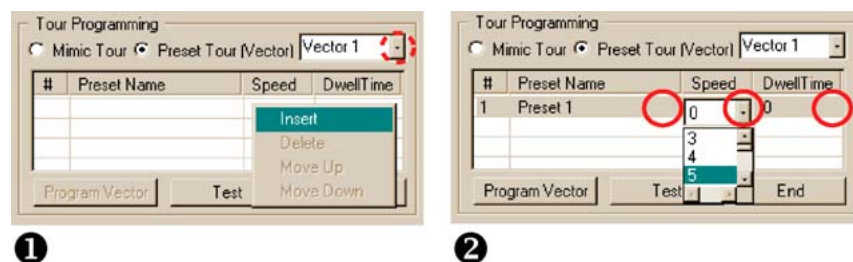
## To Test a Mimic Tour on a RapidDome Camera

1. While using View, select the site at which you have programmed a mimic tour on a RapidDome camera, as shown in procedure RapidDome Mimic Tour.
2. Run a Maintenance Session; on the Video tab, select the dome camera that is programmed with a mimic tour.
3. Click **PTZ**. Check if the Driver is "RapidDome/Orbiter". If not, the wrong camera or site may have been selected and this procedure cannot be used.
4. In the "Tour Programming" section, select a mimic tour, using the arrow button above the End button. By default, they are named "Tour 1, Tour 2, Tour 3 ..."
5. Click **Test**.

## RapidDome Preset Tour

Before setting up a preset tour, set some presets. See To Configure a Preset on a PTZ Camera, p. 91.

**Fig. 6–11. Right-clicking in the Tour Programming table reveals the Insert command.**

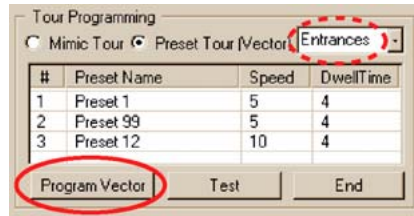




## To Setup a Tour of Presets on a RapidDome Camera

1. While using View, select a site that has RapidDome PTZ cameras.
2. Run a Maintenance Session; click the Video tab.
3. Select a dome camera.
4. Click **PTZ**. Check if the Driver is "RapidDome/Orbiter". If not, the remaining steps in this procedure cannot be used. In the "Tour Programming" section, click **Preset Tour** (Vector). While a preset tour is being programmed, the RapidDome dome does not move. You have the option of selecting which of the four preset tours you plan to setup. To do so, click the arrow button above Dwell Time. See figure 6-11 (2). A list appears, showing "Vector 1, Vector 2, Vector 3 ..." by default. Click the name that you need.
5. To add a preset to the preset tour, right-click in the table in Tour Programming. A menu appears, showing an Insert command, as in figure 6-11 (1).
6. Click the Insert command. A preset is added to the list.
  - **Speed.** You have the option of setting the time (in seconds) that the dome will take to reach the preset, by clicking the cell in the Speed column, on the line of the preset. An arrow appears. Click the arrow and select a value. Click the arrow and select a value, from "0" to "127". See figure 6-11 (2).
  - **Dwell.** You have the option of setting the time (in seconds) during which the dome will stay in the preset position, by clicking the cell in the Dwell column, on the line of the preset. An arrow appears. Click the arrow and select a value, from "0" to "255".
  - **Preset Name.** You have the option of replacing the preset with another, by clicking the cell in the Preset Name column, on the line of the preset. An arrow appears. Click the arrow and select a value, from "1" to "127". Note: preset 100 to 127 can be designated as privacy zones.
7. Repeat step 6, above, as needed. While adding more presets, you also have the option of using these commands:
  - **Move Up/Down.** You have the option of moving a preset up or down in the list, including its Speed and Dwell times. Right-click in the # column, on the line of the preset; a menu appears. Click **Move Up** or **Move Down**, as needed.
  - **Delete.** You have the option of deleting one preset or many from the list, by right-clicking in the # column, on the line of the preset. On the menu that appears, click **Delete**. To select many presets, press and hold the Ctrl key on the PC's keyboard while clicking on different lines in the # column.
  - **Test.** You have the option of testing the preset tour by clicking Test. To stop the testing of a preset tour, click **End**.
  - **Rename tour.** You have the option of renaming the preset tour. Click inside the box next to Preset Tour (Vector). Type a name. The name is saved when you next click the mouse. See figure 6-12, below: "Entrances" has replaced the default name of "Vector 1".
8. Click **Program Vector** to send the tour of presets to the camera. You have the option of programming another tour of presets for the dome camera; repeat steps 5 to 7 as needed.

Fig. 6-12. Location of the Program Vector Button.

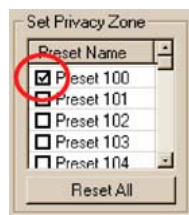


## Testing a Preset Tour on a RapidDome Camera

1. While using View, select the site at which you have programmed a Preset Tour on a RapidDome camera, as shown in procedure To Setup a Tour of Presets on a RapidDome Camera.
2. Run a Maintenance Session; click the Video tab.
3. Select the dome camera that is programmed with a Preset Tour.
4. Click **PTZ**. Check if the Driver is “RapidDome/Orbiter”. If not, the wrong camera or site may have been selected in step 1 and the remaining steps in this procedure cannot be used.
5. In the “Tour Programming” section, click **Preset Tour (Vector)**.
6. Select the preset tour that you plan to test. To do so, click the arrow button above Dwell Time. A list appears, showing “Vector 1, Vector 2, Vector 3 ...” by default. Click the name that you need.
7. Click **Test**.

## Privacy Zones for RapidDome

Fig. 6-13. Setting Up a Privacy Zone on a RapidDome PTZ Camera.



PTZ preset 100 to 127 can be toggled to not display or to display the video feed coming from the RapidDome, when the dome is in the preset’s angle and zoom.

- **Reset All.** To cancel the privacy applied to presets, click **Reset All**. A confirmation dialog box appears. Click **Yes**.

## To Set a Privacy Zone

Select the box next to the preset name so that it shows a check-mark. See figure 6-13, above, and figure 6-10-(4), on page 95. Remove the checkmark to enable Live and recoded video from that PTZ preset.

## ACUIX Dome Camera

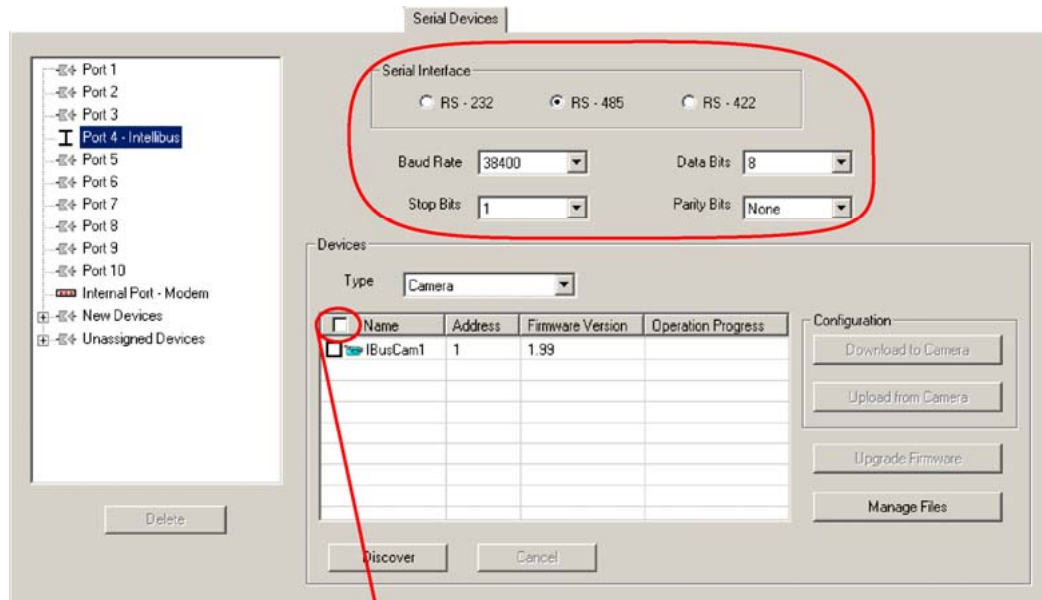
An ACUIX™ PTZ dome camera with Intellibus™ can be used and configured using Rapid Eye View software. In preparation, installers have:

- Set each ACUIX dome camera to their Intellibus mode (IBus).
- Set DIP switch 5–8 to ON, on each ACUIX dome camera. The **Camera Address** can then be set using rotary switches (SW1 to SW4) on the PCB at the base of the dome.
- Connected the ACUIX dome cameras to a port on the Rapid Eye unit.
- Notified the Multi SA of the number of the port used on the Rapid Eye unit and the **Camera Address** used for each ACUIX dome camera.

## Configuring the Intellibus Device for a Rapid Eye Unit

1. Assign the Intellibus device to the port used by the installers, by dragging its icon from the **Unassigned Devices** to a "Port n". Figure 6–14 shows the result when Port 4 is used.
  - **Port "3" through "10"**. Select **RS-485** on the Serial Devices tab.
  - **Port "1" or "2"**. Select **RS-232**. Use a hardware converter for RS-232/RS-485 on these ports to translate communications to and from the ACUIX dome cameras.
2. On the Serial Devices tab, select the values shown in table 6–3. See also figure 6–14.

Fig. 6–14. Communication Settings for Intellibus on the Serial Devices Tab.



Shortcut for selecting all of the items listed in the table.

Table 6–3 Communications for the Intellibus Device, and for each ACUIX Dome Camera

Communications	Value
Baud Rate	38400
Stop Bits	1
Data Bits	8
Parity Bits	none

## To Configure an ACUIX Dome Camera for PTZ Use

1. Run a Maintenance Session.
2. Click the **Video** tab.
3. Click PTZ. For information about enabling and configuring a PTZ dome, see *Video Tab Settings for PTZ*, on p. 86.
4. Select an ACUIX dome camera.
5. In Port Attributes, enter values for **Baud Rate**, **Stop Bits**, **Data Bits** and **Parity Bits**, using those shown in table 6–3.
6. For **Camera Address**, do not use the same value for two ACUIX cameras that share the same port.
7. Repeat steps 4 to 6 for each ACUIX dome camera.

## Discovery of ACUIX Dome Cameras

You have the option of running the discovery routine if domes were added or if the list of cameras seems incomplete.

1. Run a Maintenance Session.
2. On the Serial Devices tab, click the port to which an *Intellibus device* is assigned.
3. Click **Discover** to update the table of ACUIX dome cameras.

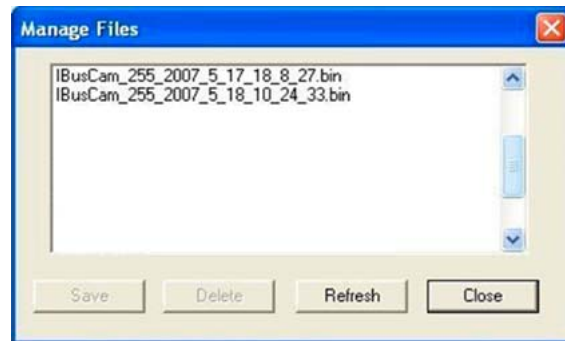
## Backing Up an ACUIX Configuration File to a PC

1. Run a Maintenance Session.
2. On the **Serial Devices** tab, click the port to which the *Intellibus device* is assigned.
3. Click **Discover** to update the table of ACUIX dome cameras.
4. Select one ACUIX dome camera or many. There is a shortcut to select all of the items in the table: click the checkbox in the **Name** column; see figure 6–14.
5. Click **Upload from Camera**. The configuration file from each of the selected ACUIX dome cameras is copied to the Multi-Media DSP unit. A configuration file for an ACUIX dome camera includes: PTZ tours, PTZ presets, vectors and all other camera settings.
6. Click **Manage Files**. The *Manage Files* dialog box appears, showing the ACUIX dome camera configuration files (\*.bin). See figure 6–15. The naming convention of configuration files is:  
camera name\_camera address\_year\_month\_day\_hour\_minute\_second.bin; for example: "Lobby\_4\_2007\_06\_16\_8\_0\_0.bin". Firmware files may also be listed and can be ignored for this procedure; their extension is (\*.ngd).
7. Select a file.
8. Click **Save**. A standard Windows dialog appears, showing the drives and folders available on the operator's PC. After selecting a drive, folder and filename, click **OK**.
9. In the *Manage Files* dialog box, click **Close**.

### Commands in the Manage Files dialog box

This *Manage Files* dialog box shows only the files which are related to ACUIX dome cameras, from among the files stored on the Rapid Eye unit. If there are no \*.bin or \*.ngd files, the Manage Files dialog box displays an empty list.

Fig. 6-15. The Manage Files Dialog Box.



**Save.** Copies a file from the Rapid Eye unit to the operator's PC. See Backing Up an ACUIX Configuration File to a PC, step 8, above.

**Delete.** Select a file and click. A confirmation dialog box appears. Click **Yes** to remove the file from the Rapid Eye unit.. This does not remove the information from an ACUIX dome camera.

**Refresh.** Updates the report in the Manage Files dialog box.

**Close.** Closes the Manage Files dialog box.

### Using LocalView

A configuration file for an ACUIX dome camera can also be saved to a Rapid Eye unit, using LocalView. See the context-sensitive Help for LocalView.

## Downloading a Configuration File to an ACUIX Dome Camera

After Backing Up an ACUIX Configuration File to a PC, p. 100, you can copy that configuration to another ACUIX camera of the same make and model.

1. Run a Maintenance Session.
2. On the Serial tab, select the port to which the *Intellibus device* was assigned.
3. Click **Discover** to update the table of ACUIX dome cameras.
4. Select one ACUIX camera or many. There is a shortcut to select all of the cameras listed: click the checkbox in the **Name** column; see figure 6-14.
5. Click **Download to Camera**. A standard Windows dialog appears, showing the drives and folders available on the operator's PC.
6. Select a configuration file (\*.bin) for the ACUIX dome camera.
7. Click **Open**. The configuration file is downloaded to the ACUIX dome camera.



**Honeywell does not recommend uploading an ACUIX configuration file from one model of ACUIX dome camera to another. For example, the configuration from an ACUIX dome camera with a FCB-EX480C camera should not be uploaded to an ACUIX dome camera with a VK-S654 camera. To identify a camera, see the procedure for Identifying the Model of the Camera, next.**

## Identifying the Model of the Camera

Honeywell recommends identifying the model of the camera in ACUIX dome cameras, to avoid uploading an ACUIX configuration file from one model of ACUIX camera to another.

1. Run a Maintenance Session.
2. Click the **Video** tab.
3. Click PTZ.
4. Select a camera that is an ACUIX dome camera.
5. Click **Camera Menu**. The model of the camera is listed.

## Upgrading the Firmware of an ACUIX Dome Camera

1. Run a Maintenance Session.
2. On the Serial Devices tab, click the port to which the *Intellibus device* is assigned.
3. Click **Discover** to update the table of ACUIX dome cameras.
4. Do one of the following:
  - Select all of the ACUIX dome cameras, by clicking the checkbox in the **Name** column. See figure 6–14.
  - Select some of the ACUIX dome cameras. If not all of the ACUIX dome cameras are selected, the cameras are upgraded one by one; see step 9 of this procedure.
5. Click **Firmware Upgrade**. A standard, Windows dialog appears, showing the drives and folders available on the operator's PC.
6. Select a drive, folder and a firmware file for the ACUIX dome camera. These files should have a \*.ngd file extension.
7. Click **Open**.
8. A *Maintenance Message* dialog box appears, to confirm the operator's selection. To proceed, click **Yes**.
9. If there are many ACUIX dome cameras connected to the unit, and all were selected in step 4 of this procedure, a *Sequence for Upgrading Cameras* dialog box appears. Select a sequence, and then click **Continue**. The upgrade of the cameras can be:
  - **Simultaneous**. Approximate time: 10 minutes.
  - **One by one**. More time consuming; about 10 minutes *for each* camera. This upgrade stops if a camera is off, or if the connection fails, and a warning appears for that camera.



**If "Simultaneous" is selected, and an ACUIX dome camera is off, or if the connection fails, the upgrade appears to continue, without warning the operator. When all of the ACUIX dome cameras are powered and the connection to them is operational, use this procedure again.**

## Enhancing Video for Security

### Event Recording: Configuration

#### Flexibility

Use of **Event Recording** is optional.

### Using Higher Settings for Video Recorded During an Event

Each camera has its own **Event Recording** values. The settings for live video are independent of settings for continuous recording and **Event Recording**.

Fig. 7-1. Continuous Recording and Event Recording, on the Recording Tab.

Property Camera	Camera Name	Record	Continuous Recording			Event Recording		
			Resolution	Frame Rate	Quality	Resolution	Frame Rate	Quality
Camera 1	Park West	On	384 x 288	1	7	704 x 288	8	9
Camera 2	Park East	On	384 x 288	1	7	704 x 288	8	9
Camera 3	Park South	On	384 x 288	1	7	704 x 288	8	9
Camera 4	Lobby East	On	384 x 288	1	7	704 x 288	8	9
Camera 5	Lobby West	On	384 x 288	1	7	704 x 288	8	9
Camera 6	Lobby Elevators	On	384 x 288	1	7	704 x 288	8	9
Camera 7	Back NE	On	384 x 288	1	7	704 x 288	8	9
Camera 8	Back NW	On	384 x 288	1	7	704 x 288	8	9
Camera 9	Walkway	On	384 x 288	1	7	704 x 288	8	9
Camera 10	Promenade	On	384 x 288	1	7	704 x 288	8	9
Camera 11	Scenic	On	384 x 288	1	7	704 x 288	8	9
Camera 12	Camera12	Off	384 x 288	1	8	384 x 288	1	8
Camera 13	Camera13	Off	384 x 288	1	8	384 x 288	1	8
Camera 14	Camera14	Off	384 x 288	1	8	384 x 288	1	8
Camera 15	Camera15	Off	384 x 288	1	8	384 x 288	1	8
Camera 16	Camera16	Off	384 x 288	1	8	384 x 288	1	8

On the Recording tab, set higher values for **Event Recording** (all settings, or some) than for Continuous Recording. Values are: **Resolution** (pixel × pixel), **Rate** (number of ips) or **Quality** (less compression). Each camera can have its own **Event Recording** values.

### Authorized Configuration

**Event Recording** can be configured by the Multi SA in your organization, or by other operators who have the right to run a Maintenance Session.



**Caution:** Using high values for **Continuous Recording** can shorten a unit's video archive to the point of making it unusable. See **Using Higher Values When Recording Video**, p. 127.

### Automatic DSP Performance Maximization

A Multi SA can optimize Event Recording settings. See **Automatic Maximization of DSP Performance**, p. 72.

### Multi-Media LT

On Multi-Media LT units, the maximum resolution for NTSC is 640×240; for PAL, 704×288; this is lower than on Multi-Media DSP units.

### Live Video

The settings for Continuous Recording and **Event Recording** are independent of those for live video.

## Setting Lower Values for Continuous Recording

The values for **Continuous Recording** need to be lower (or equal) to the values of **Event Recording**. If higher values cannot be set for **Event Recording**, check if high values are used for **Continuous Recording**.

## Event Recording on Demand, Using the Boost Button

Once **Event Recording** is set, View software operators have the option of clicking the Boost button, while monitoring Live video. See figure 7-2. For the location of the button, see the *Rapid Eye View Software Operator Guide*, K14391.

Fig. 7-2. Boost Button.



### Event Recording on demand during a Site Tour

In View software, the button for **Event Recording** is unavailable while a tour is running. To enable the button, pause the tour first.



## Automating Event Recording: Events of Interest

### Events of Interest: examples

A storage area may be of little interest until someone enters it. A Multi-Media DSP unit can be set to use Continuous recording until motion of the door to the storage area is detected *in the video* recorded by the unit. The unit then switches automatically to **Event Recording** settings.

Another example: a camera monitoring the access point of a parking lot. When a vehicle reaches the gate and idles waiting for the gate to rise, **Event Recording** can be used, to make effective use of a Rapid Eye unit's video storage.

### Use

An Outside World event or a Customer-device event can trigger **Event Recording** automatically. See Event Recording for Video: Scheduling a Response, p. 112. Continuous Recording may suffice while nothing of interest occurs.

## Scheduling: Configuration

### Flexibility

Use of scheduling is optional. A schedule can be shared by the Continuous Recording of video, the raising of Alarms and a Response Rule, or be used separately. Cameras and alarms can be scheduled before or after they are setup. Scheduling is performed unit-by-unit.

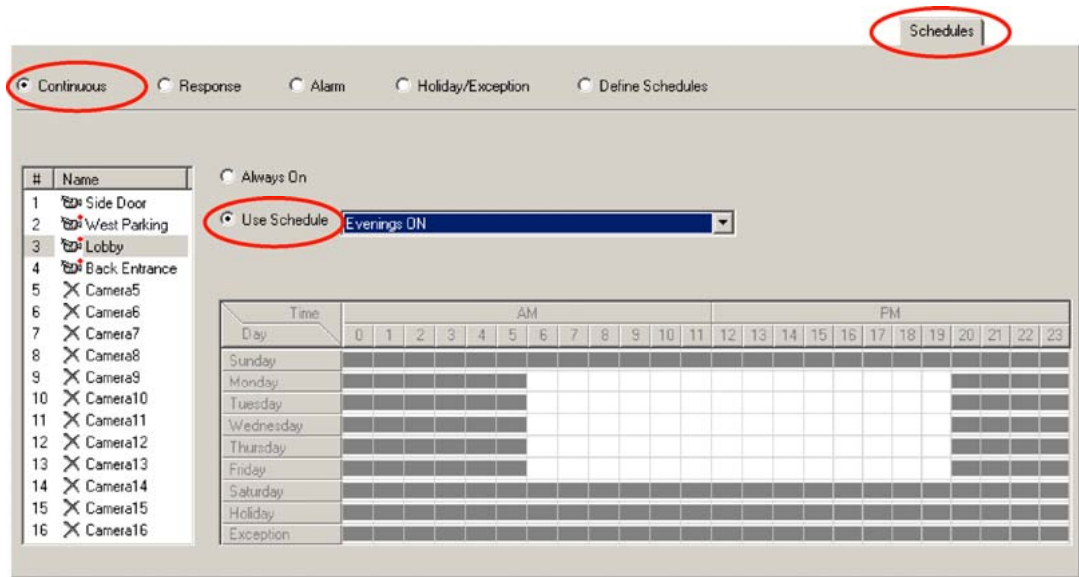
### In a nutshell

You have the option of setting a Multi-Media unit to record a video feed only at times or days that you specify. For example, your organization might need to record video of a parking lot only on holidays, or during the day, using only some cameras, and so on. You can customize schedules for specific cameras, or groups of cameras. A schedule can be prepared for use only with alarms; for example, to prevent them from ringing during business hours.

Each camera or the triggering of alarms can be scheduled to either:

- Always ON. No schedule is used. Cameras using this setting record at all times.
- Use Schedule: Default. The simplest way to simultaneously schedule all cameras and alarms is to customize the "Default" schedule; see Customizing a Schedule, p.107, and Holiday and Exception.
- Use Schedule: [defined schedule]. To schedule a camera or alarms separately, or to schedule a set of cameras as a group, see To Add a Schedule.

**Fig. 7-3. Example of a Schedule Assigned to a Camera.**



**Video archive**

A benefit of scheduling the recording of video feeds is that it spares storage on a Multi-Media unit, granting an organization a potentially longer video archive. See Computing the Length of the Video Archive, p. 122.

**Live video**

Live video is not affected by scheduling.

**Alarms**

The reporting of alarms is scheduled in the same way as Continuous video recording, using the "Default" schedule or another. See Alarms and Scheduling, p. 109.

**Motion**

If Motion is enabled on a camera, its motion events are recorded only while a camera is scheduled to record. If motion is set to trigger alarms, it will do so even if a camera is not scheduled to record, but not if alarms are scheduled not to be raised.

**Audio feeds**

Audio is recorded while enabled, no matter the recording schedules.

**Data streams**

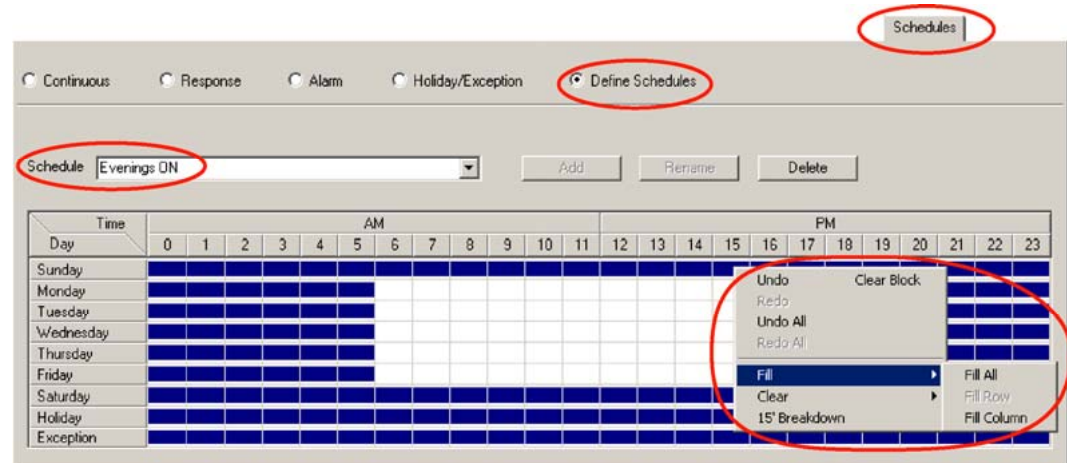
The data from POS devices is always recorded, no matter the recording schedules.

## Making Use of a Schedule

**Flexibility:** for alarms, a camera, groups of cameras or a response rule

You have the option of adding, customizing and deleting a schedule, using "Define Schedules". A schedule can then be assigned to one camera or many, to alarms or to a response.

Fig. 7-4. Customizing a Schedule.



### To Add a Schedule

1. Continue or start a Maintenance Session.
2. Click the Schedules tab.
3. Click **Define Schedules**. The tab displays the grid of the "Default" schedule. See figure 7-4.
4. Click in the Schedule box and type a name. The Add button becomes available.
5. Click **Add**.

### Customizing a Schedule

1. On the Schedules tab, during a Maintenance Session, click **Define Schedules**. The tab displays the grid of the "Default" schedule. See figure 7-4.
2. Use the Schedule box to select the schedule that you want to customize.
3. Click cells in the Time/Day grid as needed. The customization is saved automatically. The Time/Day grid can be modified in various ways, either:
  - **Cell-by-cell.** Click the cells of the Basic schedule grid as needed. Clicking the cells toggles a time from ON (dark) to OFF (light), or OFF to ON. See figure 7-4.
  - **By a block of cells.** Drag the mouse pointer over cells. When you release the mouse button, the cells within the dragged area change color and a menu appears showing Fill block and Clear block commands. Click a command, as needed.
  - **Globally.** Click the other mouse button to display a menu of commands for customizing more than one cell at once: Clear row, Clear column, and so on.

### Customizing the "Default" schedule

By default, all of a Multi-Media unit's cameras and alarms are assigned to the "Default" schedule. Customizing the "Default" schedule can be the quickest way to coordinate a unit for all cameras and alarms.

## To Assign a Schedule to a Camera, or Group of Cameras

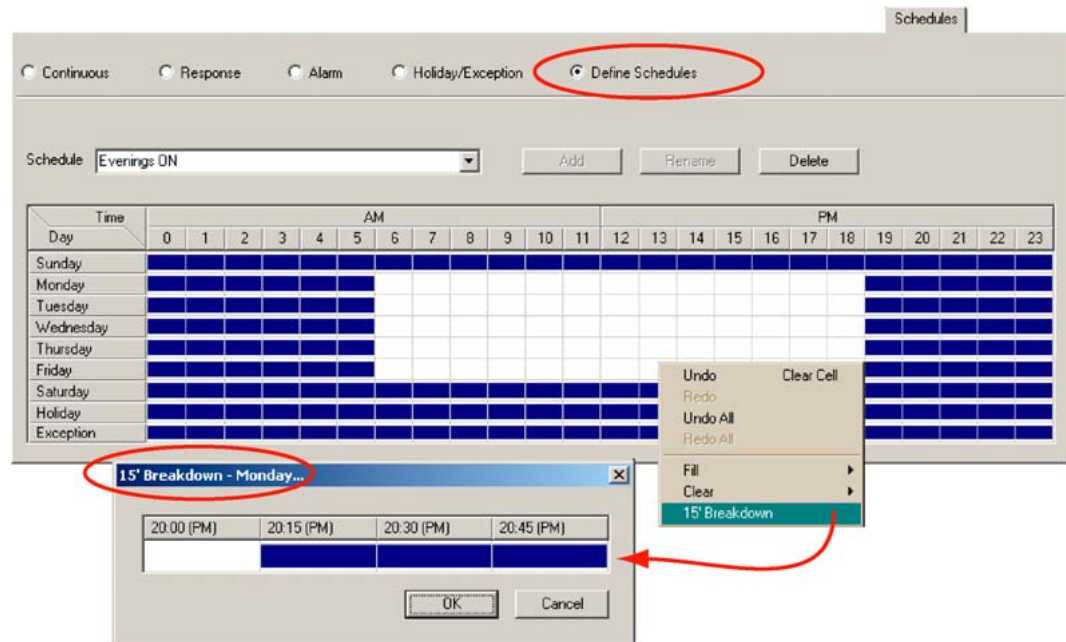
1. Continue or start a Maintenance Session.
2. Click the Schedules tab.
3. Click **Continuous**. The tab displays a list of cameras, along with a schedule grid. See figure 7-4.
4. Select a camera in the Name column. If Always On is selected, select Use Schedule.
5. Click the Use Schedule box and select a schedule for the group of cameras.
6. Repeat this procedure for the other cameras that will use the schedule selected in step 5.

### Renaming cameras

Cameras can be renamed on the Video tab. See figure 5-1 on p. 65, in Cameras.

## Using a 15-minute Increment in a Schedule

Fig. 7-5. Breakdown of a Cell into Fifteen-minute Sections.



1. In the Time/Day grid, on a day's row, right-click an hour's cell to display a menu.
2. Click the 15' Breakdown command. A 15' Breakdown window appears, showing four fifteen-minute cells for that hour, on that day. See figure 7-5.
3. Click on the cells as needed to schedule one or many of the fifteen-minute periods.
4. To save the setting, click **OK**. The 15' Breakdown window disappears.

## To Rename a Schedule

Note that the "Default" schedule cannot be renamed.

1. On the Schedules tab, during a Maintenance Session, click **Define Schedules**. The tab displays the grid of the "Default" schedule. See figure 7-4.
2. Use the Schedule box to select the customized schedule that you want to rename.
3. Type a name in the Schedule box.
4. Click **Rename**.

## To Delete a Schedule

Note that the "Default" schedule cannot be deleted.

1. On the Schedules tab, during a Maintenance Session, click **Define Schedules**. The tab displays the grid of the "Default" schedule. See figure 7-4.
2. Use the Schedule box to select the customized schedule that you want to delete.
3. Click **Delete**. If a schedule is in use, it cannot be deleted. Assign another schedule to the cameras, alarms or rules using the schedule.

## Alarms and Scheduling

### Flexibility

Use of scheduling to disarm alarms is optional. If you choose to assign a schedule to alarms, all alarms use that schedule. A schedule for the alarms can be independent from those used by cameras; for example, you can set events to trigger alarms only after business hours, while cameras keep recording. Or the opposite. See figure 7-6, below.

### Assigning a schedule to alarms

A schedule is assigned to alarms in the same way as for cameras. Alarms can be set to either:

- Always ON. No schedule is used. Cameras using this setting record at all times.
- Use Schedule: Default. The simplest way to simultaneously schedule all cameras and alarms is to customize the "Default" schedule; see Customizing a Schedule, p.107, and Holiday and Exception.
- Use Schedule: [defined schedule]. To schedule a camera or alarms separately, or to schedule a set of cameras as a group, see To Add a Schedule.

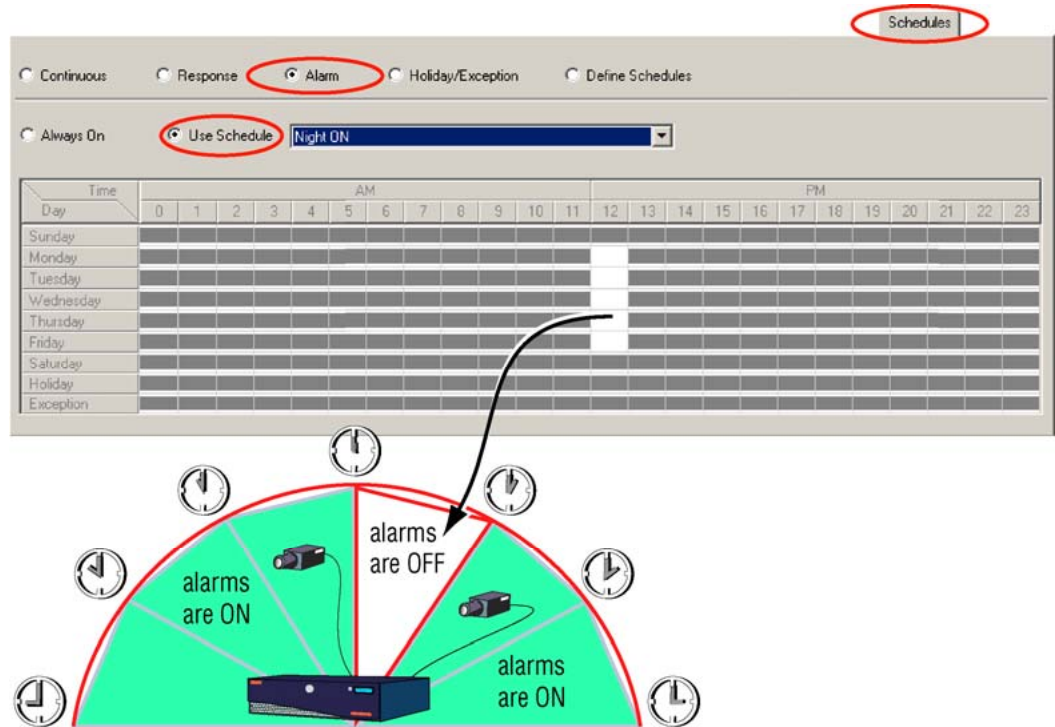
### Scheduling and Security

- Depending on your organization's security needs, it may make sense, for example, to disarm alarms or cameras set for motion detection, during working hours.
- Abuse of scheduling can have an impact on security. Please consult your organization's security officer.

### Motion detection

A useful application for scheduling alarms is to counteract false positive alarms in Motion Detection.

Fig. 7-6. Using a Schedule for Alarms.



## Tip

Settings for Holiday and Exception have higher priority than settings for days of the week. See Holiday and Exception.

### See also

How to set events to trigger alarms is explained in Setting an Event to Trigger an Alarm or to Be Logged, on p. 187.

## Holiday and Exception

### Key facts

- The dates of holidays and exceptions can be input by the Multi SA of your organization, or by operators who have the right to run a Maintenance Session.
- The dates that are added on the Holiday/Exception list become part of every schedule.
- Settings for Holiday and Exception have higher priority than settings for days of the week. For example, setting weekdays to not “trigger alarms” and the Holiday row to trigger alarms means that alarms are raised when a holiday falls on a weekday.

## Adding Holidays and Exceptions

Fig. 7-7. Specifying a Holiday for the Next Few Years.

Date	Name	Type
12/25/2006	Christmas	Holiday
2/2/2007	Groundhog Day	Exception
12/25/2007	Christmas	Holiday
2/2/2008	Groundhog Day	Exception
12/25/2008	Christmas	Holiday
2/2/2009	Groundhog Day	Exception
12/25/2009	Christmas	Holiday

1. Continue or start a Maintenance Session for the Rapid Eye site.
2. Click the Schedules tab.
3. Click **Holiday/Exception** [days]. See figure 7-7.
4. Type a name for the holiday (or exception) in the Name box.
5. Choose whether to list the day as a holiday or an exception by clicking in the Type box.
6. When entering the date, ensure that the date is in the future and that it is unused. To enter a date, either:
  - Type a date. In the Date box, click the part of the date that you want to change. Use the arrow keys on your keyboard to change the number, or type a number that you want.
  - Use the calendar utility. Display the calendar utility by clicking the arrow next to the date box. Click the date that you need in the calendar. To go to another month, click the arrow keys next to the month/year heading in the utility. The utility disappears when a date is selected.
7. Click **Add**. The date is added in the Holiday/Exception list.
8. To duplicate a holiday record for each year that you predict the system will be in use, repeat steps six and seven of this procedure, changing the year in step six as needed.

### To update a Name or a Type of holiday/exception

1. Select the faulty item in the list of holidays or exceptions; see figure 7-7.
2. Change the Type or Name, as needed.
3. Click **Update**.

### To correct a date

1. Select the faulty item in the list of holidays or exceptions; see figure 7-7.
2. Change the Date, as needed.
3. Click **Add**.
4. Select the faulty item in the list.
5. Click **Delete**.

## Event Recording for Video: Scheduling a Response

Fig. 7-8. A Rule's Trigger, Response and Schedule.

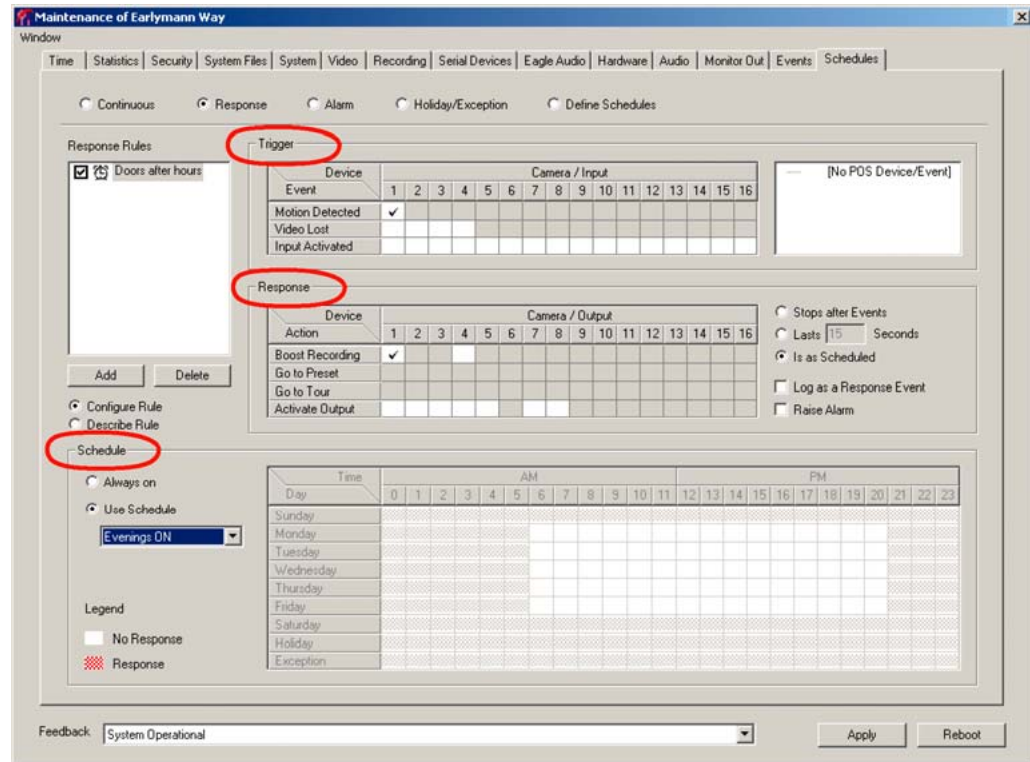


Figure 7-8 shows a rule, where:

**[Trigger:] = If a camera senses motion...**

**[Response:] = ... then a Multi-Media DSP unit responds with Event Recording. And**

**[Schedule:] = However, do not do so during business hours. When? On weekdays, during business hours between 7 am and 7 pm.**

### In a nutshell

The Response schedule is used to make simple if-then-and-when rules, to preset how a Multi-Media unit responds to events of interest.

## Trigger: an Event of Interest

An empty loading dock may become of interest when motion occurs. A **Response Rule** presets a unit to respond to Events of interest, such as:

- Motion in video.
- Lost video.
- Input, activated.
- Data from a POS device.



## Displaying the Response Panel Used for Making Rules

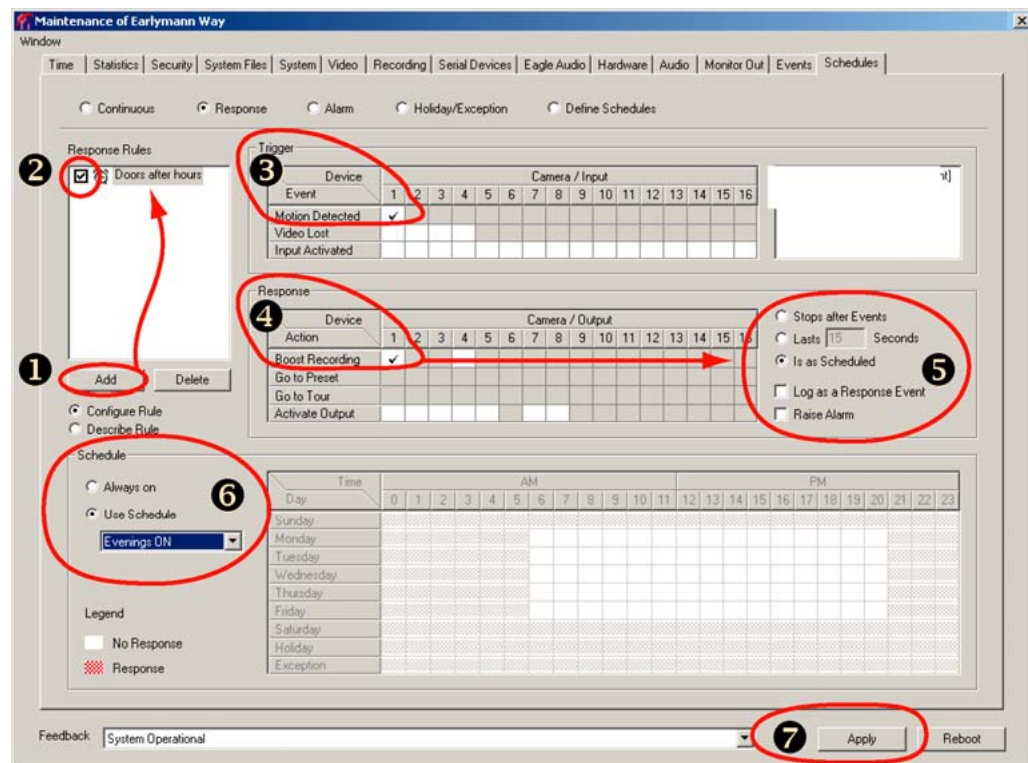
1. Continue or start a Maintenance Session for the Rapid Eye site.
2. Click the Schedules tab. See figure 7–8.
3. Click Response. The panel for making rules and customizing a response is displayed.

### Authority

Setting and customizing rules can be performed by the Multi SA in your organization, or by other operators who have the right to run a Maintenance Session.

## Checklist for Setting a Rule in the Response Schedule

Fig. 7–9. Customizing a Rule: Visual Steps.



1. **Rule creation or selection.** Click **Add** or **Select** a rule from the list in the Response Rules box. See #1 in figure 7–9. The **Describe Rule** command shows text, stating all of the rule's components—trigger, response and schedule. You have the option of Renaming a Rule.
2. **Enabling a rule for editing.** To edit and customize a rule, start by selecting the checkbox next to the name of the rule. The icon next to the checkbox changes as you customize a rule. See Rule Status: Icons, p. 114.
3. **Trigger.** Customize the rule's trigger(s), as needed, by clicking cells that are available in the Event rows.

4. **Response.** A Response can include:
  - Use **Event Recording** values to record video. For this to have an effect, settings for **Event Recording** need to be higher than those for continuous recording; see Event Recording: Configuration, p. 103.
  - Make a PTZ camera go to a PTZ preset.
  - Make a PTZ camera go to a PTZ tour.
  - Activate an Output on the Multi-Media unit.
  - Combinations of the above. If an Action cell is unavailable, the action is not setup.
5. **Log/ Alarm.** You can customize the duration of a response and if the response is Logged or Raises an Alarm. See Managing the Response to a Rule, p. 115.
6. **Schedule.** You also have the option of selecting a schedule. See Assigning a Schedule to a Response Rule, p. 115.
7. **Apply.** Sends the rule to the Multi-Media unit.

### Flexibility of checklist

After selecting a rule, you can perform steps 4 to 6 of the Checklist for Setting a Rule in the Response Schedule in any order. A rule lists the Events that Trigger a response and the Actions that are taken as a Response. Figure 7-9 shows where and how to make a rule.

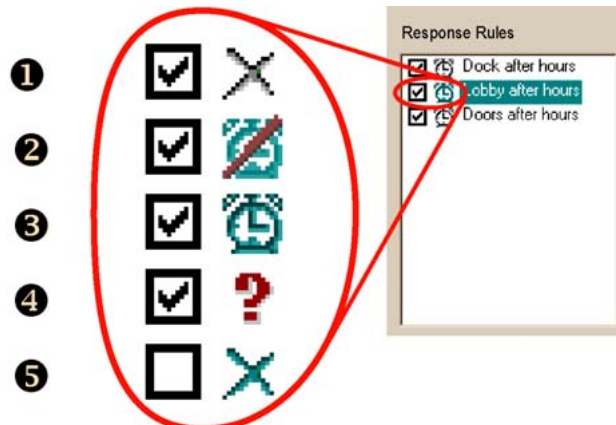
## Renaming a Rule

1. Select a rule; then click the rule's name once again.
2. Type a name. Letters and numbers can be used, as can some punctuation. The same name cannot be used for two rules.
3. Save the name. Either:
  - Press the Enter key
  - Click elsewhere in the View window
  - Switch to another Windows application.

## Rule Status: Icons

As a rule is customized, its status is reported by one of five icons; see figure 7-10.

Fig. 7-10. Status Icons for a Response Rule.



### Meaning of icons for the status of response rules

1. The rule can be edited; the operator needs to set a trigger or a response.
2. The operator has selected an empty schedule.
3. The rule is operational.
4. The rule is prevented from acting by a component that has been disabled—camera, PTZ, motion or other.
5. The rule is disabled; there is no checkmark in the box.

## Managing the Response to a Rule

Response rules offer these options:

- Stops After Events.
- Lasts for [15] Seconds. The time can be set from five seconds to 3,600 (one hour).
- Is As Scheduled.

### Alarm and Log: to report a response

A rule's response can be set to be logged silently or to raise an alarm. See Setting an Event to Trigger an Alarm or to Be Logged on p. 187.

## Assigning a Schedule to a Response Rule

A schedule is assigned to a response rule in the same way as for cameras. A rule can be either:

1. **Always ON.** No schedule is used. Cameras using this setting record at all times.
2. **Use Schedule: Default.** The simplest way to simultaneously schedule all cameras and alarms is to customize the "Default" schedule; see Customizing a Schedule, p.107, and Holiday and Exception, p. 110.
3. **Use Schedule: [defined schedule].** To schedule a camera or alarms separately, or to schedule a set of cameras as a group, see To Add a Schedule, p. 107.

## Disabling a Response Rule

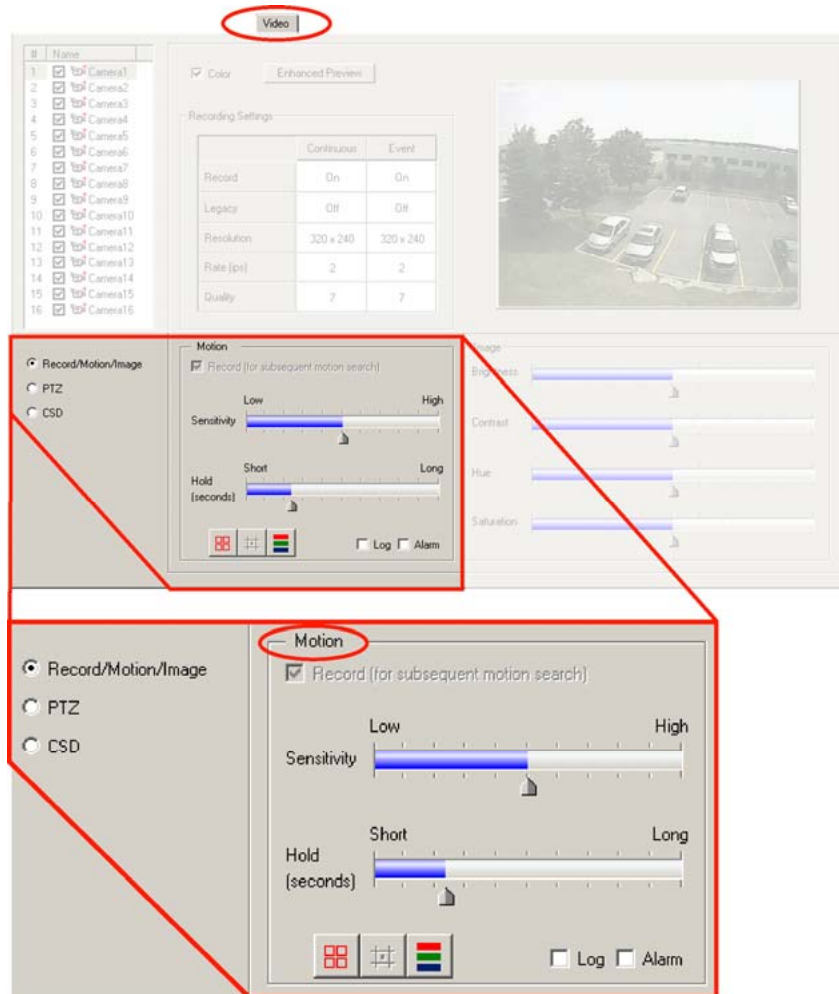
Rules can be disabled by removing the checkmark next to their name. The response of a disabled rule will not take place even if the response is scheduled to occur.

## Motion Detection

### Flexibility

Using motion detection to log or trigger alarms is optional. Live video and recorded video are not affected by motion detection settings.

Fig. 7-11. Motion Detection Configuration.



### Detection scenarios

Motion detection can trigger an Alarm or add entries in a Log, based on motion in one area, or many, of a video feed.

Motion detection can warn or log, in real-time of:

- **Unauthorized use of area.** A construction crane moving outside of a scoped area, a burglary...
- **Scheduled appointment.** Checking the arrival and departure times of: a truck at a loading dock, deliveries, and even natural phenomena such as tides...
- **Catastrophes.** Complements sensors for fire, flood, explosions...
- **Pest control.** Vermin in a storage area...

*And so on.*

## To Configure Motion Detection

1. Continue or start a Maintenance Session for the Rapid Eye site.
2. Click the Video tab. By default, Record/Motion/Image is selected.
3. For commands, you have the option of using the buttons in the Motion area or the motion commands on a menu. To use the menu, place the mouse pointer on the tab's video and right-click on the mouse. See figure 7-13.

## Customizing Detection: Masking

### Masking movement that is of no concern

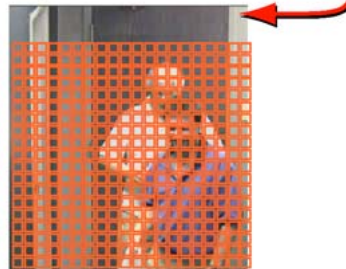
By default, motion is detected everywhere in a video feed. Some of that movement may not be of any interest, such as a roadway in a window, or people walking by a door. Areas of no concern can be masked, i.e., hidden from motion detection, so that they will not trigger an alarm.

**Fig. 7-12. Mask for Motion Detection.**

- ❶ Setting a mask at the top of the door, before using the "Invert Mask" command.



- ❷ After inverting the mask: the movement of personnel in front of the door is ignored; only door movements are detected.



## Example: Masking an Area of the Video Feed



1. Taking the image in figure 7-12 as an example: to perform surveillance on a door that many people walk by, start by setting a mask on the top corner of the door.
2. After setting the mask, place the mouse pointer on the image and click the other mouse button. A menu appears. See figure 7-13.
3. Select the Invert Mask command; the detection is now focused on an area that "moves" only when the door opens.
4. Enable Log or Alarm. The log can be used to obtain video from the time(s) when the door is opened, saving a View operator from having to "spot" video.

### Red mask and green mask

In motion detection, the mask is red and movement behind a mask is ignored.

The masking behaves opposite to that of motion search. In motion search, the parts "masked" in green act as triggers more than as a mask.

## To Mask Part of a Video Feed from Motion Detection

1. Check that Record/Motion/Image is selected, as in figure 7–11.
2. Click  the Edit motion mask command; see figure 7–11.
3. You have the option of clicking  to Show gridlines. The video image on the Video tab is overlaid with a grid.
4. Click on areas of the video feed that you need to mask. To mask more than one cell with one click, press and hold the Ctrl key on the PC's keyboard while you click. This option masks 3×3 cells at once.

## False Positives

A false positive (also known as a false alarm) is a common situation that triggers motion detection without posing a security risk. Sources of false positives can include: the sun's glare reflected on windows and cars, shadows, turning vehicle lights or building lights on and off, direct sunlight as the day progresses.

### Solutions

More than one technique can be used to reduce false-positives:

- Masking. You can mask areas of a feed where movement is of no concern.
- Scheduling. Alarms can be scheduled not to “ring” only at certain times. See Alarms and Scheduling, on p. 109.
- Camera placement. Software settings and scheduling can compensate for many camera problems but not for all; for example: direct sunlight may require moving a camera or shielding it from sunlight.
- Camera position. A camera in a building is an effective way to use motion detection, since lighting can often be controlled. However, a window or vista, which shows a roadway or pedestrians, can trigger motion detection.
- Motion search. There are cases when performing a timely search for motion is more effective than constantly testing for motion. See Motion Search on p. 120.

### Video settings and motion detection

When an alarm based on motion detection is enabled, changing picture settings (brightness and so on) can trigger that alarm. You can limit the triggering of alarms by using the Delay slider in the motion detection controls. See Cameras, on p. 65 and Events Defined, p. 187.

## Customizing Detection: Scheduling

**Scheduling alarms.** Motion is detected at all times. There may be times when movement may not be of any interest, such as during business hours. These times can be scheduled to not trigger alarms. See Alarms and Scheduling, on p. 109.

**PTZ cameras.** On a PTZ camera, motion panning, tilting or zooming triggers motion events. You have the option of scheduling alarms for times when a PTZ camera is not moving.

## Motion Detection Reference

### Commands



**Edit motion mask.** Click it to enable the “show gridlines” button, next.



**Show gridlines.** Toggles a grid that overlays the video image on the Video tab.



**Motion preview.** Click to see motion detected by Multi. Colored pixels are produced as objects move.

- **Red or green.** Indicate motion high enough to trigger an alarm or log entry, if enabled. Adjust the sensitivity until motion that needs to be reported shows up as green or red.
- **Blue.** Indicates motion that is detected but not reported.

**Hold.** The amount of time (in seconds) that motion events are ignored *after* a motion event has triggered a report. Value is displayed when the slider is clicked. Value range: 1 (Short) to 60 (Long). Default value: 30 seconds.

**Log.** You can set motion in a video image to trigger a log entry by adding a checkmark to the Log box on the Video tab.

**Alarm.** You can set motion to trigger alarms by adding a checkmark to the Alarm box on the Video tab. Motion is an Outside World event. For other events, see table 10–5: Event Reference, by Source and Tab, on page 190.

### Extra motion detection commands

The motion detection menu offers extra commands along with a few of the above. To view it, place the mouse pointer on the tab's video and right-click on the mouse.

**Fig. 7–13. Motion Detection Menu.**



**Invert mask.** Unmasks masked areas and masks unmasked areas.

**Clear mask.** Removes all masking from picture area.

**Fill mask.** Adds masking to entire picture area. Useful as a first step, when most of the image area needs masking.

**Undo.** Cancels the last click that you made.

**Undo All.** Returns the mask to its state before edits were performed.



## Motion Search

Motion search is used to search video for motion, independently of settings made for Motion detection. A motion search is performed using View software. See the *Rapid Eye View Software Operator Guide* for procedures and tips.

### Comparing Motion Detection and Motion Search

Motion search differs from motion detection. See table 7–1, below.

**Table 7–1** Contrasting Motion Detection and Motion Search

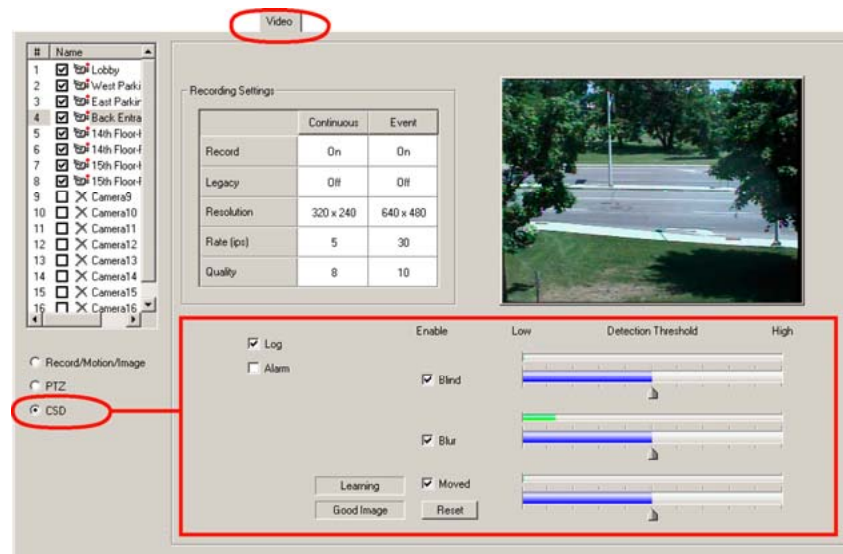
Operator (task)	Motion (tool)	Comments
<b>Detection.</b> Log motion or warn of motion during Live Sessions, in real-time.	 session, Video tab, Motion panel	<ul style="list-style-type: none"> <li>- constantly checks for motion</li> <li>- motion events can be logged or trigger alarms as they occur</li> <li>- video feed can be masked where motion is of no concern.</li> </ul>
<b>Search.</b> Search recorded video for motion.	 session	<ul style="list-style-type: none"> <li>- search for motion after the fact</li> <li>- events are all listed for retrieval of video</li> <li>- operator can select areas of video where motion is a concern.</li> </ul>

## Camera Sabotage: Detection

### Flexibility

Use of camera sabotage detection (CSD) is optional. In use, operators obtain an alarm or a log entry when a camera is blinded, blurred or moved. The settings for CSD are made on each camera, separately. Video is not affected by CSD settings.

**Fig. 7–14.** CSD Panel, on the Video Tab.





## To Configure CSD

1. Continue or start a Maintenance Session for the Rapid Eye site.
2. Click the Video tab. By default, **Record/Motion/Image** is selected.
3. Select **CSD**. A panel is displayed for configuring CSD. See figure 7–14.
4. You have the option of enabling the automatic detection of three types of sabotage: **Blind**, **Blur** or **Moved**, singly or in combination.
5. Lower or raise the threshold of detection for each type of sabotage, by horizontally dragging each **Detection Threshold** cursor, as needed. The default value is at midpoint (50), on a scale of 1 to 100. See figure 7–15.
6. Select **Alarm** or **Log** as needed; see Setting an Event to Trigger an Alarm or to Be Logged, p. 187. Each type of sabotage detection that is enabled will use the selection. If neither **Alarm** nor **Log** is selected, camera sabotage is not reported.

### Tip

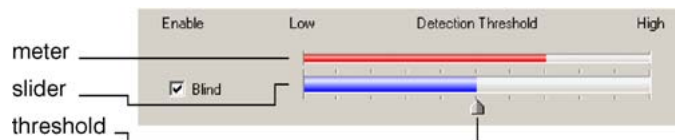


The **Blind** type of CSD can be used for fixed cameras and for PTZ cameras.

**Blur** and **Moved** are CSD types designed for fixed cameras only, not for PTZ use. Using pan, tilt or zoom triggers **Blur** and **Moved**.

## Calibration of CSD

Fig. 7–15. Calibration of Blind-type CSD.



### Detection meter

Above each slider for setting the detection threshold of **Blind**, **Blur** and **Moved**, a meter shows the CSD activity. The meter is green when activity is below the threshold, and red when the activity is above. If there is no activity, the meter is empty. See figure 7–15.

**Blind.** A camera can be blinded by too much light or too little. To calibrate, cover the camera with an opaque cloth or box, or prop a strong light in front of the camera. Blinding a camera also triggers the **Blur**-type and **Moved**-type of sabotage. Note that turning lights on/off at the scene can indirectly blind a camera. Panning a PTZ camera from a light colored scene to a darker scene (or vice versa) can also have that effect. Lowering the threshold can compensate.

**Blur.** It is not recommended to alter a camera's focus after installation. To simulate sabotage of focus, use a lens-like sheet of glass or plastic, or a transparent container of water, and prop it in front of the camera, during calibration.

**Moved.** See the next section.

### Forty-eight seconds

Activity in a scene that could be considered as sabotage drives the meter from green to red. If such activity lasts less than 48 seconds, it does not trigger an alarm or log entry. This is designed to calibrate CSD and to reduce the number of false positives. For example, a person walking by a

camera at close range and blinding the camera is not considered sabotage unless that person remains in front of the camera for more than 48 seconds.

### Event log

To search the event log, use an Event session. See Event Session: to Search the Log of Events, p. 193.

## Moved-type CSD: Learning and Rearming Alarms

### Good Image

A "Good Image" is reported, to the left of **Reset**, when a scene has enough features for the unit to detect if someone or something has moved the camera, and sabotage can be inferred. A "Bad Image" is reported when the image is indistinct, for example, if the camera is pointed at a wall of uniform color.

### From Learning to Running

When **Moved** is selected, or its threshold changed, the Multi-Media unit "learns about" the scene shown by the camera; "Learning" is reported, to the left of **Moved**, for 2 minutes to a maximum of 3 minutes. Do not blind or blur a camera while "Learning" is displayed. When learning ends, "Running" is displayed to the left of **Moved**.

### Resetting learning

**Reset** is enabled when **Moved** is selected. Clicking **Reset** starts **Learning** again, and should be used whenever the camera is moved intentionally to show another scene, or if the scene's lighting or content changes dramatically. **Reset** has no effect on **Blind** and **Blur**.

### Rows of mobile objects

Moved is sensitive to large scale changes in a scene. For example, using **Moved** for a camera that shows many chairs in a row, close by, such as in an airport or casino, may not be effective. Clicking **Reset** while people are sitting makes the unit "learn" that sitting persons are not to be considered as sabotage. When the chairs empty, the scene may have changed enough for the unit to trigger a log entry or an alarm. And if the operator makes the unit "learn" when the chairs are empty, then CSD may be triggered when people sit in the chairs. The same can be said for a row of vehicles that are frequently moved, such as in a taxi stand or truck depot.

### Alarms

After rearming an alarm produced by the Moved-type sabotage detection, move the camera back to the scene that you need to monitor, and click **Reset**.

## Computing the Length of the Video Archive

### Storage Process: Video, Audio, Data

Recordings of video, audio and data are not permanent. When a unit's storage fills, the oldest recorded video, audio and data are replaced with more recent recordings. The amount of time that recordings are available is known as the *length of the video archive*.

### What to watch out for

Adding cameras, using high rates, high-resolution and high quality settings for continuous recording, contribute to shorten the video archive on a unit. High settings in combination, on many cameras, can shorten a unit's video archive from thousands of days to a few hours. See table 7-7, p. 127. If a Rapid Eye unit's video archive becomes too short for your needs, try lowering the resolution and frame rates for continuous recording. How to do so is explained in Recording Video: Continuous Recording Settings, p. 68.

Scheduling Cameras can lengthen a video archive.

### Estimates

To make storage estimates, use Honeywell's Rapid Eye Storage Estimator that is installed with Rapid Eye software. To compare and understand the effect of factors on storage, see the tables for Number of Cameras, Audio, Scheduling Cameras, Frame Rate for Continuous Recording, Quality, and Resolution, in the next sections.

#### Estimate from a unit's statistics

If a Multi System Administrator (Multi SA) only needs to know roughly how far back in time video can be obtained, data is available when running a Maintenance Session:

- **Recording tab.** "Estimated Storage Capacity" in days, see Estimating Storage Capacity, p.71.
- **Daily Usage Rate.** Averaged over the latest 7 days of activity; see the procedure: A Multi-Media Unit's Storage Statistics, p. 127.

## Rapid Eye Storage Estimator

The Storage Estimator is installed along with Rapid Eye Software.

1. Click **Start**.
2. Point to (or click) All Programs.
3. Point to Rapid Eye Multi-Media 8.0. A menu appears.
4. Click **Storage Estimator**.

#### Finding out how long recorded video will be stored

An operator may need to know how far back in time that video, audio and data can be obtained. Honeywell provides a Storage Estimator to show the approximate length of a unit's video archive, based on a unit's settings.

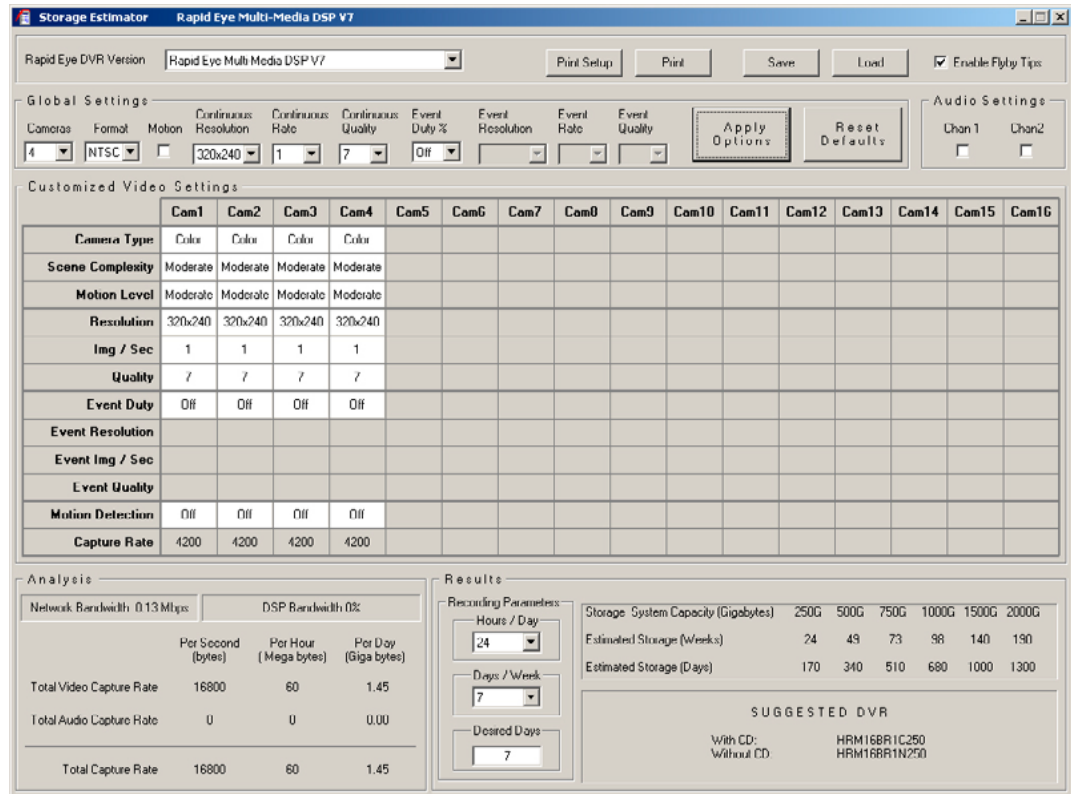


**High settings in combination, for many cameras, can shorten a unit's video archive from thousands of days to a few hours. See table 7-7, p. 127. If the archive is too short for your needs, lower the resolution and frame rate of continuous video.**

#### Storage Process: Video, Audio, Data

Recordings of video, audio and data are not permanent. When a unit's storage fills, the oldest recorded video, audio and data are replaced with more recent recordings. The amount of time that recordings are available is known as the length of the video archive. More cameras, high recording rates, high-resolution and high quality settings, all contribute to shorten the video archive on a unit. Scheduling can lengthen a video archive.

Fig. 7-16. Storage Estimator.



**Tip**

- Use the Rapid Eye Storage Estimator to forecast the length of a unit's video archive.
- Combinations of very high values be assigned only to Event Recording.

**Number of Cameras, Audio**

Doubling the number of cameras roughly halves the length of a unit's video archive.

Table 7-2 Number of Cameras: Effect on the Video Archive\*

Camera (recording)	Duration of Video Archive (estimated, camera-day)	Oldest Available Video (rounded to shortest time)
1	1153	3 years, 1 month
4	288	9 months
8	144	4 months
12	95	3 months
16	72	2 months
+ audio	57	1 month

\* Resolution = 320 × 240; Frame Rate = 1; Quality = 8; Storage = 500GB.

**Audio**

At default recording values, adding audio has roughly the same effect as adding 4 cameras. If enabled, use table 7-2, find the number of cameras connected to the unit and go the next line. At higher recording values, audio takes a smaller percentage of the archive.

## Scheduling Cameras

Scheduling can lengthen a video archive. One key application is for the recording of transactions that do not occur 24/7, as shown in table 7–3. See Scheduling: Configuration, p. 105.

**Table 7–3 Scheduling of Cameras: Effect on Storage**

Recording (hours / days)	Recording Suspended (%)	Video Archive (camera-day)	Oldest Available Video (to closest date)
24/7*	0.0	1153	3 years, 1 month
12/5 + 24/2†	35.7	1793	4 years, 11 months
12/7‡	50.0	2306	6 years, 3 months
8/5 **	76.2	4842	13 years, 3 months

\* Default value: every day, all hours, for one camera, Resolution @ 320 × 240; Frame Rate = 1; Quality = 8 and Storage = 500GB.

† Nights and weekends.

‡ Nights only; all week long.

\*\* Business hours, five days a week.

## Frame Rate for Continuous Recording

Table 7–4 shows how higher frame rates can reduce the length of a video archive. For more cameras, divide the time of the archive by the number of cameras.

**Table 7–4 Frame Rate: Effect on Storage**

Frame Rate (images per second)	Video Archive (estimated, camera-day)	Oldest Available Video* (rounded to shortest time)
1†	1153	3 years, 1 month
2	576	1 year, 6 months
6	192	6 months
15	77	2 months
30	38	1 month

\* For one camera; Resolution = 320 × 240; Quality = 8; Storage = 500GB.

† Default value

## Quality

### Video compression (“Quality”)

A higher Quality setting means less video compression and less time before your oldest video gets replaced by fresher video; see table 7–5. For example: setting Quality to “10” uses up almost twice as much storage as a setting of “6”.

### Lowering quality to spare storage

At sites where storage is at a premium, you can lower the recording quality to six (6) compression units. Table 7–5 shows that this can give you about 25% more storage—other settings unchanged.

**Pan, tilt, and zoom**

Recording a video feed from a camera that pans constantly requires much more storage. If the duration of your video archive is a concern, Honeywell recommends that you consider if constant panning is necessary to your security needs. See Behavior of PTZ After a Session Closes, p. 93.

**Table 7-5 Impact of Quality Setting on a Unit's Video Archive**

Recording Quality (compression unit)	Duration of Video Archive (Estimated, in camera-day)	Oldest Available Video* (rounded to shortest time)	(weeks)
6	1441	3 years, 11 months	200
8 <sup>†</sup>	1153	3 years, 1 month	160
10	823	2 year, 3 months	110

\* For one camera; Resolution = 320 × 240; Frame Rate = 1; Storage = 500GB.

† Default value.

## Resolution

**Using higher resolution**

Recording video at higher resolutions than default uses up more storage on a Multi-Media unit. Your organization can decide if it prefers (a) high-resolution video images that remain stored for a shorter length of time, or (b) low-resolution images that can be stored longer.

**Table 7-6 Recording Resolution: Effect on the Video Archive**

Resolution (pixels)	Video Archive* (camera-day)	Oldest Available Video (rounded to shortest time)
<b>NTSC</b>		
160 × 120	4803	13 years, 1 month
320 × 240 <sup>†</sup>	1153	3 years, 1 month
640 × 240	670	1 year, 7 months
640 × 480	320	10 months
704 × 480	274	9 months
<b>PAL<sup>‡</sup></b>		
192 × 144	3336	9 years, 1 month
384 × 288	801	2 years, 2 months
704 × 288	508	1 year, 4 months
704 × 576	254	8 months

\* For one camera; Frame Rate = 1; Quality = 8; Storage = 500 GB.

† Default Honeywell settings.

‡ PAL images are larger than NTSC and require more storage. This accounts for a shorter archive.

**See also**

For estimate tools by Honeywell, see Rapid Eye Storage Estimator, p. 123.

## Using Higher Values When Recording Video

### Effect of using a combination of higher recording values

For **Continuous Recording**, heightening Resolution, Quality and Frame Rate in combination, compounds the effect on storage. Examples are shown for one camera and for nine cameras, on a unit that has 500 GB of storage.

**Table 7-7 Available Storage: Comparing with One Camera to Nine**

Resolution	Frame Rate	Quality	1 Camera (archive)	9 Cameras (archive)	Storage (Camera-day)
<b>Lowest</b>					
160 × 120	1	6	<b>Result:</b> 15 years, 7 mo.	1 year, 8 mo.	5700
<b>Default</b>					
320 × 240	1	8	<b>Result:</b> 2 years, 11 mo.	0 year, 4 mo.	1100
<b>High, plus Quality</b>					
max: 704 × 480	1	max: 10	<b>Result:</b> 6 months	21 days	190
<b>High, plus Frames</b>					
704 × 480	10	10	<b>Result:</b> 19 days	2 days	19
	30*	10	<b>Result:</b> 6 days	0 days	6

\* A frame rate of 30 ips can be used on 1 to 4 cameras. For 9 cameras, 10 ips (max) can be used.



Honeywell recommends that high values for recording video be used only for event recording.

## A Multi-Media Unit's Storage Statistics

**Fig. 7-17. Detail of the Statistics Tab, Showing Storage Statistics.**

Time	Statistics	Security	System Files	System	Video	Serial Devices	Eagle Audio	Hardware	Audio	Monitor Out	Events	Schedules
General Info												
Storage Capacity	1,000 GB		Time Elapsed	0.0 days		Refresh						
Daily Usage Rate	0.1%		Percent Full	0.0%		Clear Storage						
Estimated Capacity	834 days		Clear Stream									

## To Obtain a Unit's Statistics

1. Continue or start a Maintenance Session for the Rapid Eye site. Please wait until a "System Operational" message appears in the **Feedback** box.
2. Click the Statistics tab. There may be a delay, based on the type of connection to the site, until the Feedback box displays "Statistics received".
3. To update the statistics, click **Refresh**.

**Table 7-8 Storage Statistics for a Multi-Media Unit**

<b>Label</b>	<b>Meaning</b>	<b>Unit</b>
Storage Capacity	The total disk space, on unit.	gigabyte (GB)
Daily Usage Rate	The portion of storage used in the last twenty-four hours. For new units, or after clearing storage, the report of <b>Daily Usage Rate</b> can be accurate within minutes. In regular use, it is averaged over the latest 7 days of activity.	percentage of storage capacity
Estimated Capacity	The amount of storage, based on past performance. The number may differ from the estimate obtained using the Rapid Eye Storage Estimator, due to fluctuations in the video signal. The estimated capacity diminishes if the <b>Continuous</b> video recording settings (resolution, quality, ips) are set to higher values and as more cameras are added.	day
Time Elapsed*	The time that has passed since the latest change to configuration or latest reboot of the Multi-Media unit. Can also be used to estimate the oldest available image*.	day, hour, minute, second
Percent Full	The portion of storage in use; at "100 %", recycling occurs.	percentage of storage capacity
Stream	device connected to a Multi-Media unit (a camera, microphone, and so on)	text
Start Time	time of earliest data	UTC (universal coordinated time)
End Time	time of latest data	UTC
Recorded	portion of storage used by a device	percentage of data
Stream ID	n/a; for Multi technical support	integer

\* Most helpful on a unit that records continuously. If a unit is off or stops recording for a while, introducing gaps in the video archive, time elapsed still reports only the oldest available video.

### Other statistics about the video archive

The Recording tab shows an "Estimated Storage Capacity" in days. See Estimating Storage Capacity, p. 71.



## Configuring Other Hardware

### Clearing Storage

#### Purpose

Clearing the storage of a Multi-Media unit or of one of its streams is a drastic measure that is irreversible and time consuming; recorded video, sound and data are permanently erased. Clearing streams or storage should be handled with care.

Clearing the storage may be needed in the rare cases where a unit is:

- Disposed of
- Moved or transferred to another organization.

**Fig. 8-1. Statistics Tab, Showing the Clear Storage Button.**

The screenshot shows a web interface for a statistics tab. At the top, there is a 'Statistics' tab. Below it, there is a 'General Info' section with several fields: Storage Capacity (240 GB), Time Elapsed (168.0 days), Daily Usage Rate (0.0%), Percent Full (18.8%), and Estimated Capacity (24,455 days). To the right of these fields are three buttons: 'Refresh', 'Clear Storage', and 'Clear Stream'. The 'Clear Storage' button is circled in red, and a black arrow points to it from the word 'Beware!' written above. Below the buttons is a table with columns: Stream, Start Time (UTC), End Time (UTC), Recorded (%), and Stream ID. The table lists various streams such as '14th Floor', 'Lobby', 'West Parking', etc., with their respective start and end times and recorded percentages.

Stream	Start Time (UTC)	End Time (UTC)	Recorded (%)	Stream ID
14th Floor	Tue Jul 26 15:20:20 2005	Tue Jan 10 12:00:00 2006	15.7	1
Lobby	Tue Jul 26 15:20:20 2005	Mon Jan 09 11:59:59 2006	8.0	3
West Parking	Tue Jul 26 15:20:20 2005	Thu Jan 05 16:17:53 2006	14.2	5
Back entrance	Tue Jul 26 15:20:20 2005	Thu Dec 22 14:18:56 2005	9.2	7
15th Floor	Tue Jul 26 15:20:20 2005	Thu Dec 22 14:18:56 2005	9.0	9
Office-15th	Tue Jul 26 15:20:19 2005	Thu Dec 22 14:18:56 2005	8.2	11
East Parking	Tue Jul 26 15:20:20 2005	Thu Dec 22 14:18:56 2005	13.9	13
16th Floor	Tue Jul 26 15:20:20 2005	Thu Dec 22 14:18:56 2005	9.2	15
17th Floor	Fri Sep 23 14:18:23 2005	Thu Dec 22 14:18:56 2005	5.3	17
18th Floor	Fri Sep 23 14:18:22 2005	Thu Dec 22 14:18:55 2005	0.7	19
19th Floor	Fri Sep 23 14:18:22 2005	Thu Dec 22 14:18:56 2005	0.7	21
20th Floor	Fri Sep 23 14:18:22 2005	Thu Dec 22 14:18:56 2005	0.7	23
21st Floor	Fri Sep 23 14:18:22 2005	Thu Dec 22 14:18:56 2005	0.7	25
22nd Floor	Fri Sep 23 14:18:22 2005	Thu Dec 22 14:18:56 2005	0.7	27



**The only safety to prevent unwarranted use of Clear Storage is setting a password to the Administrator account. The “Clear Storage” and “Clear Stream” buttons cause the permanent deletion of video and data. See fig. 8-1, in Clearing Storage, on p. 129.**

### To clear a unit's storage

1. Using View, run a Maintenance Session.
2. On the Statistics tab, click **Clear Storage**. See figure 8-1, above. A password dialog box appears.
3. Either:
  - There is a password on the Administrator account: type that password.
  - There isn't a password. Do nothing and go to the next step.
4. Click **Yes**. All video, audio, alarms and other data stored on the Multi-Media unit is erased. The time needed to clear storage is about fifteen (15) seconds for each gigabyte of storage.



#### **Clearing storage cannot be stopped or reversed, even by turning the unit off.**

Turning the Multi-Media unit off only suspends the process; storage continues to clear when the unit is powered again. It is an irreversible process.

### Clearing a stream

A stream is the information from one camera or data device. You may need to clear one or more streams, if there is ever:

- A move or transfer of a camera or unit to another location.
  - Some testing of a new camera, or training operator's in PTZ use
- And so on. -

### To change the name of a stream

Different names can be assigned to cameras on the Video tab (see Cameras, on p. 65); the name of a customer-device is assigned on the Serial Devices tab (see Customer Data and Customer-Device Events, on p. 143).

## Preventing Users from Clearing Storage

- **Add or change the password to the Administrator account.** The Administrator password acts as a safety, to prevent the error of triggering a "clear storage" by mistake. To set this password, see Administrator Password, on p. 176.
- and -
- **Right to view Statistics tab.** Your Multi SA can remove the right to use and view the statistic tab from a View operator account. See Right to Use Maintenance, on p. 180.



**Multi SAs who refuse to add a password to the Administrator account also remove a safeguard to prevent inadvertent use of the Clear storage feature.**

## To Trace the Clearing of Storage

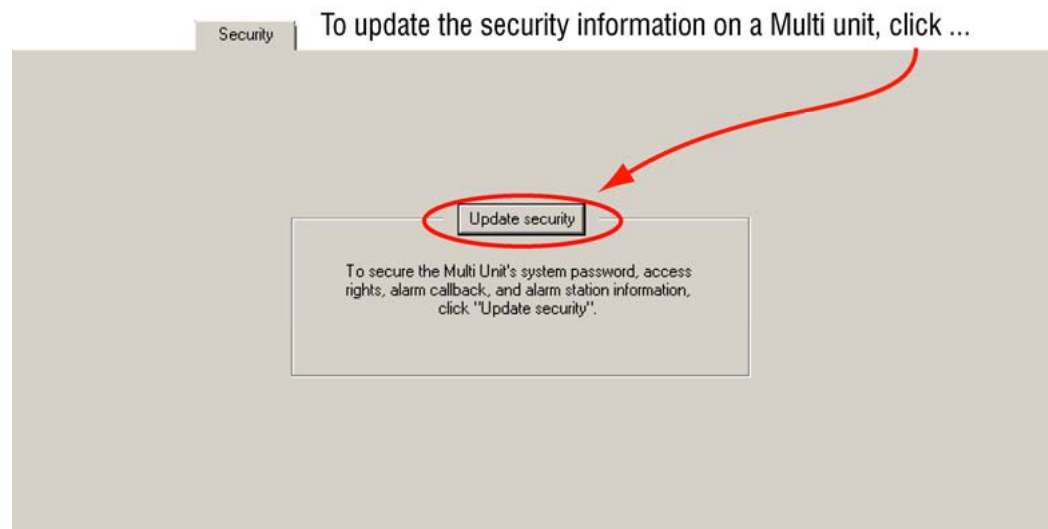
- Track the moment it happens by making this event an alarm. See Tracing Events, on p. 191, and Events Defined, on p. 187.
- Prevent future attempts by changing the Administrator account password.

### Security and unit availability considerations

Clearing of a unit's entire storage or of one of its streams can have a major impact on that site's security. All recorded video is lost. During the time that a unit is emptied a Multi-Media unit cannot record video, nor send alarms, and so on. Your Multi SA should warn View operators that use of the Clear storage and Clear stream buttons, whether planned or carried out, should be communicated to your organization's security personnel.

## Updating Security on a Multi-Media Unit

Fig. 8-2. Securing a Unit, after Changing Passwords.



1. Use View to start a Maintenance Session for the Multi-Media unit.
2. Click **Update security** on the Security tab of a Maintenance Session. See fig. 8-2, above. Information from the Multi db is copied to the Multi-Media unit. Please wait until "Updated security" appears.
3. You have the option of updating security on other units, or/and ending the Maintenance Session, as explained in Ending Maintenance on p. 62.

### Purpose

A unit's security settings need to be updated if a Multi SA adds, changes or removes:

- Alarm stations. See Adding an Alarm Station: Name and Reports, on p. 203 and Making an Alarm Station Operational, p. 218.
- The system password. See System Password, on p. 166, and Security Priorities, p. 162.
- Authorized operators of a site. See Denying Access, p. 198.
- Authorized onsite operators. See Central User Management, p. 154.

### Removing a site after updating security

After updating the security of a Multi-Media unit, care should be taken to remember the system password. The system password is needed if you need to make a new site definition for the Multi-Media unit. See Removing a Site on p. 28.

## System Files

### Purpose: System Log

Your Multi System Administrator (Multi SA) or your organization's security officer may find it useful to download a copy of a unit's System Log or other system file, as needed. Downloads of files from a Multi-Media unit are safer than uploading files; uploads should be performed by trained personnel.

Fig. 8-3. File Transfers: to a Unit or from a Unit.



### Tip

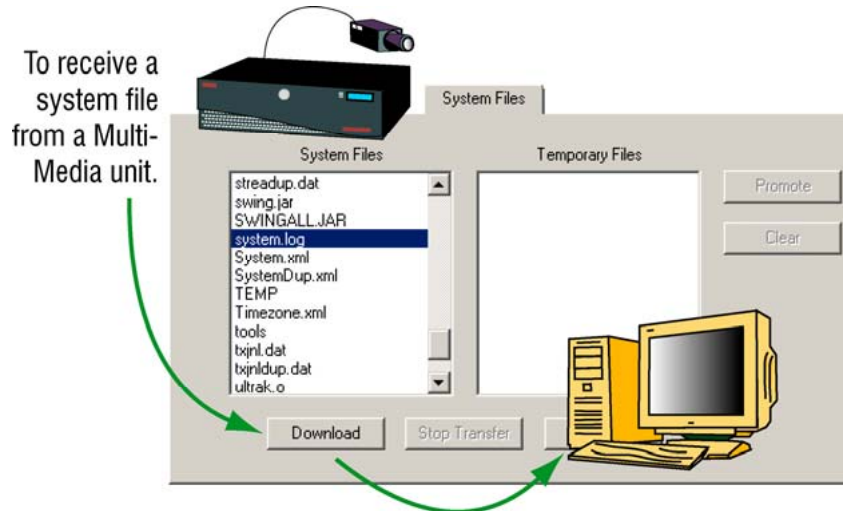
Check if the "System Operational" message appears in the Feedback box before performing the procedure To Download a File from a Multi-Media Unit, next.

## To Download a File from a Multi-Media Unit

1. Continue or start a Maintenance Session for the Rapid Eye site.
2. Click the System Files tab. See figure 8-4.
3. Select a system file in the System Files pane: "system.log", for example; see Logging System Messages, p. 134. Only one file can be selected at a time.
4. Click **Download**. A confirmation message appears; click **Yes**. The Receive file from Remote Site dialog box appears.
5. Specify the location where you want to download the file. You also have the option of renaming the file.

6. Click **OK**. A copy of the file is sent from the Multi-Media unit to the location specified in step 5.
7. Use a text editor or word processor to view the contents of the file.

**Fig. 8-4. Downloading the System.log File from a Multi-Media Unit.**



#### Uploading warning

An upgrade to a Rapid Eye Multi-Media unit, or its reconfiguration, means uploading new system files to the unit.



**Only trained View operators should perform uploads on a Rapid Eye Multi-Media unit.**

The procedure is explained here, in case you are instructed to upload a file for troubleshooting purposes by your technical support staff or Honeywell's.

#### To upload a file to a Multi-Media unit

1. Continue or start a Maintenance Session for the Rapid Eye site.
2. Before proceeding, check if the "System Operational" message appears in the Feedback box.
3. Click the System Files tab.
4. Click **Upload**. A confirmation message appears; click **Yes**. The Send file to remote site dialog box appears.
5. Specify the name of the file that you are planning to upload, and its location (PC, network).



**Double check that you are uploading the correct file.**

The file name should not be more than eight characters long. Uploading the wrong file can halt a Multi-Media unit, causing that site to become inoperable.

6. Click **OK**. A copy of the file is sent from the PC to the Multi-Media unit; its name appears in the Temporary files pane. Uploading on slow connections can take a few minutes.

7. Either:
  - Click **Promote**.

- or -

  - Abandon the upload by clicking Clear; then skip the next step.
8. You options:
  - Upload more files; repeat steps 3 to 6, as needed.
  - Empty the Temporary Files list; to do so, click **Clear**.

## System Tab in a Maintenance Session

### Road map

Each part of the System tab is discussed in turn. Default System data is listed in table 8–2, on p. 137.

### Multi-Media unit registration

During the first Multi-Media unit's Maintenance Session, the Serial Number (the site name in the site definition) and Software are obtained from the Multi-Media unit and displayed in the upper-left corner of the System tab, under Site Info.

The version of a Multi-Media unit's software may differ from the version number of Admin and View. See also Making a Site Operational, on p. 55.

## Logging System Messages

Log System Messages. The system message log is useful mostly to Multi technical support personnel. A checkmark in the Log System Messages box sets the Multi-Media unit to log all commands received in a system.log file, stored on the unit. The system.log file stores the 10,000 most recent entries. It does not get any larger over time; the older entries are replaced by the newer.

How to obtain a copy of the system.log file is explained at System Files, p. 132.

### Other Multi logs

Take care not to confuse System.log messages of commands with the logs of alarms or events. For the alarm log see Alarm Log on p. 227; for the events log, see Events Defined on p. 187.

## System Monitor

**Enable status pulse.** Enables the FAULT RELAY to trigger. Power outages and other causes can lead to a unit's failure to record video or failure to function. Failure to do either, for more than 19 minutes, triggers the FAULT RELAY located on a unit's back-panel. See the *Unit Installation Instructions*, K14390.

**Monitor alarm reporting.** Enables delays greater than 19 minutes in the reporting of alarms to trigger the fault relay. The monitoring is designed to report alarms that have not reached their designated alarm station, because of that alarm station being unavailable.

## Making the FAULT RELAY Operational

Fig. 8–5. Enabling the FAULT RELAY.

The screenshot shows the 'System' configuration page. The 'System Monitor' section is circled in red, containing the following options:

- Enable Status Pulse
- Monitor Alarm Reporting

Other visible sections include 'Site Info' (Serial Number: 00197, Software Version: 8.0 Build 25), 'Signal Format' (NTSC selected, PAL unselected), 'Network Settings' (Use DHCP unchecked, Network Name: N/A, IP Address: 164.178.32.197, Subnet Mask: 255.255.255.0, Gateway: 164.178.32.1, MAC Address: 00:02:68:03:82:2E), and 'Maximum Network Data Rate' (Regulate Data Rate unchecked, Send no more than 32 kilobits per second).

1. On the System tab, add a checkmark to: Enable Status Pulse or to it and Monitor Alarm Reporting. See figure 8–5, above.
2. On the Events tab, click the Outputs subtab.
3. The name of Output 6 has changed to “System Status Pulse”. You have the option of changing the name, by typing in the box.

Fig. 8–6. Enabling the FAULT RELAY Changes the Name of Output6.

The screenshot shows the 'Events' tab with the 'Outputs' subtab selected. The following table displays the configuration for eight outputs:

Output	Activate		Deactivate	
	Log	Alarm	Log	Alarm
1 Output1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2 Output2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3 Output3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4 Output4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5 Output5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6 System Status Pulse	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7 Output7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8 Output8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## Camera Signal Format

- NTSC / PAL. Signal type is a global setting for all cameras.

## LAN/WAN Communications

Communications settings for local- or wide-area networks (LAN/WAN) are set in the field, when the Multi-Media unit is installed. The System tab offers a convenient report of these network settings, which are seldom changed.



**Caution: communications to a unit can be temporarily disabled by setting it to invalid network data. A technician has to return to the unit to re-enable it.**

Your organization's network administrator may request changes to a unit's communication settings when:

- Change made to the network that harbors the unit.
- Moving a unit. To other network or owner; see Clearing Storage, p. 129 and Removing a System Password, p. 169.

When moving a unit to another network or network address, you have the option of changing the Multi-Media unit's addresses in the boxes for: IP Address, Subnet Mask and Gateway, before the unit is turned off. This avoids having to use the configuration shell to make changes after the move. These changes can also be made using LocalView.

## Changing a Unit's Network Settings

1. See your network administrator about the planned changes to the site.
2. Using View, continue or start a Maintenance Session for the Rapid Eye site.
3. On the System tab, type changes in the IP Address, Subnet Mask or Gateway boxes, as needed for the Multi-Media unit, and indicated by your network administrator. Default addresses are listed in table 8-1.



**Caution: the next step can make the unit unavailable until the new network connection is operational. If a mistake is made and there is a dial-up connection to the unit, you can still access the unit by modem.**

4. Click **Apply**; then confirm that you want to send the configuration data. The Maintenance Session ends by itself.

### Tip

**Changing the Internet protocol address, in the IP Address box requires Admin to change the site's connection information, as explained in Types of Connection, on p. 29.**

**Table 8-1 Default Network Communications Settings**

Box	Value*
IP Address of Multi-Media unit	172.25.2.1
Subnet Mask	255.255.0.0
Gateway	172.25.100.4

\* These values are usually changed during the installation of units connected to a network. For more information about networked Rapid Eye units, see the section on "Network Connections" in your copy of the *See the Unit Installation Instructions*, K14390.



## Changing the Maximum Network Data Rate

The operator enters only an upper bound, to Send no more than [n] kilobits per second, where "n" is a number between "10" and "200 000". Note that some numbers are not ideal to lower the data rate optimally and are automatically adjusted by the software to the closest, better value. For example: if an operator enters "33", the software will display the closest optimal value ("32"), at the next Maintenance Session.

1. Using View, continue or start a Maintenance Session for the Rapid Eye site.
2. On the System tab, enable the Regulate Data Rate box and enter a number in the sentence. The default setting is "32".

## TCP Ports

The transmission control protocol (TCP) ports are listed in table 3–7, back on p. 49. These TCP ports should be left open in a firewall for sockets used in Multi operations. For example, Multi sessions (live, retrieval and alarm) are sent to port 10,000.

## Default System Values for a Multi-Media Unit

**Table 8–2 System Tab: Default Values**

Box Group	Name of Box / Button	Default
Site Info	Serial Number	n/a*; stored on unit
	Software	n/a*; stored on unit
	Upgrade button	none
Network Settings	Use DHCP	on
	Network Name. See the sticker on the unit.	n/a*; stored on unit, for DHCP use; format: REM-serial number.
	IP Address <sup>†</sup>	172.25.2.1
	Subnet Mask <sup>†</sup>	255.255.0.0
	Gateway <sup>†</sup>	172.25.100.4
	MAC Address	n/a*; stored on unit, for DHCP use
Signal format	NTSC / PAL	NTSC
System Monitor	Enable Status Pulse	off; see System Monitor, p. 134
	Monitor alarm reporting	off
Max Network Data	Regulate Data Rate	off
	Send no more than [ ... ] kilobits per second <sup>‡</sup>	32

\* Factory settings to identify the unit's software and hardware.

† Unavailable when DHCP is enabled. On networks that are not DHCP-enabled, the DHCP default times out and set to off.

‡ Unavailable while Regulate Data Rate is not selected.

## Serial Device: Modem

### Flexibility

A dial-up connection is optional. Internal modems in Multi-Media units can remain unused. are set using the Serial Devices tab.

### Modem settings

Modems are set using the Serial Devices tab. The Serial Devices tab shows an Internal Port that lists a modem or nothing at all. If the Internal Port holds a modem, the modem cannot be deleted. The internal port cannot receive devices from the “New devices” or the “Unassigned devices” groups.

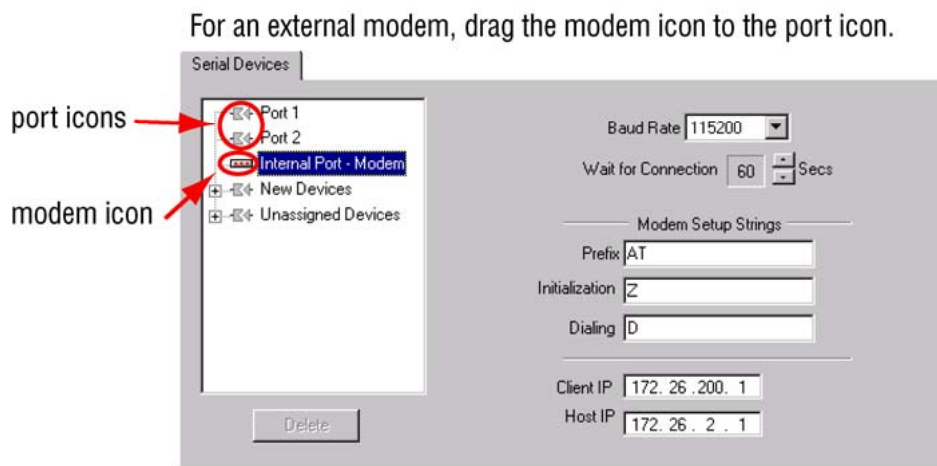


**Caution: Changing modem values in the next step can make the unit unavailable for dial-up connection. If you are unsure, see your Multi SA.**

## Viewing/Changing Modem Settings

1. Continue or start a Maintenance Session for the Rapid Eye site. Please wait until a “System Operational” message appears.
2. Click the Serial Devices tab.
3. Click the “Internal Port - Modem” icon. Boxes appear in the right half of the Serial Devices tab: Baud Rate, Wait for connection, and so on. The box’ names and their default values are listed in table 8–3, below.
4. You have the option of changing the values, as needed.

**Fig. 8–7. Serial Devices Tab Showing “Internal Port–Modem” Data.**



**Table 8–3 Default Modem and Dial-up Communications Settings**

Device	Box	Value
Modem hardware	Baud	115,200
	Wait	60
	Prefix	AT
	Initialization	Z
	Dialing	D
PPP temporary network	Client IP	172.26.200.1
	Host IP	172.26.2.1

## PPP: IP Settings Reserved for Modem Connection

During a dial-up connection, temporary network communications are established between the Rapid Eye site and the PC. A Host IP address for the Multi-Media unit is auto-detected by the Microsoft Dial-Up Networking application in Windows. Different terms are used to describe these communication points; to avoid confusion, these terms are listed in table 8–4.

**Table 8–4 Names of Temporary TCP/IP Addresses, for PPP**

Address*	Internal Port	Laymen's term	Installation shell
172.26.200.1	PPP: client IP	at operator's PC	host
172.26.2.1	PPP: host IP*	at Multi-Media unit	local

\* This is not the Multi-Media unit's network address, discussed in System Tab in a Maintenance Session.

The default, point-to-point protocol (PPP) Internet Protocol (IP) settings can be changed, in the unlikely event that they conflict with another network device (printer, scanner, and so on).

## To Set an External Modem

1. Consult the installer to find out which port on the unit is connected to the modem.
2. Continue or start a Maintenance Session for the Rapid Eye site.
3. Click the Serial Devices tab.
4. Click the "Internal Port - Modem" icon. Boxes appear in the right half of the Serial Devices tab: Baud Rate, Wait for connection and so on.
5. Change the values to those suggested by the external modem's documentation.
6. Drag the modem icon to the port icon bearing the number of the port identified in step 1.

## Serial Device: PTZ

### Flexibility

A PTZ serial device is only used to control cameras that pan-tilt and zoom (PTZ). A Multi SA obtains the port number of the Multi-Media unit that is used for PTZ from the installers of a Multi-Media system or by observing the back-panel of the Multi-Media unit.

### PTZ device settings

A PTZ device is set using a Maintenance Session, on the Serial Devices tab. It enables the PTZ settings on the Video tab. See Pan, Tilt, and Zoom (PTZ) Setup, p. 85.

## To Assign and Set a PTZ Device

1. Consult the installer to find out to which serial port of the unit the PTZ domes / cameras are connected. If more than one PTZ camera share the same serial communications line, make a note of the address set on each camera.
2. Continue or start a Maintenance Session for the Rapid Eye site.
3. Click the Serial Devices tab.
4. A PTZ device is either:
  - Assigned to a Port. Click **PTZ**. The settings are displayed and can be changed.
  - In the Unassigned Devices group. Click **PTZ**. The settings are displayed and can be changed.
  - In the New Devices group. Drag the PTZ icon and drop it either on the Unassigned Devices group or on a Port. If you drop it on a port that is already assigned to another device, the PTZ device displaces it; the displaced device is sent to the Unassigned Devices group.
5. Change the values to those suggested by the external modem's documentation.
6. Drag the modem icon to the port icon bearing the number of the port identified in step 1.

## Hardware Report

During a Maintenance Session for the Rapid Eye site, click the **Hardware** tab. The report includes a serial number of the Multi-Media unit on the Rapid Eye site, the version of software running the Multi-Media unit, date of manufacture and internal hardware used by the unit.

## Public Display Monitor: Using Monitor Output 1

A public display monitor can be set up independently of LocalView, on Multi-Media and Multi-Media LT units. There is no need for converters between the monitor and the Multi-Media unit.

1. Mount a monitor where you plan to have it display a video feed. For NTSC cameras, use an NTSC video monitor; for PAL cameras, use a PAL monitor.
2. Connect a coaxial cable to the INPUT of the video monitor.
3. Connect the other end of the coaxial cable to MONITOR OUTPUT 1, at the back of the Multi-Media unit (or Multi-Media LT unit).
4. Using View, continue or start a Maintenance Session for the Rapid Eye site.
5. Click the Monitor Out tab.
6. Select a camera that will feed the monitor in the Cameras to Choose from box. See figure 8-8.
7. Type a number in the Duration box; the number sets the amount of time (in seconds) that the video feed is displayed on the monitor. If only one camera is listed, the duration is ignored and the feed is displayed without interruption. When many cameras are listed, you have the option of changing the duration directly in the list by clicking it and typing another.
8. Click **Add**. You have the option of adding more video feeds to the public monitor; to do so, repeat steps 6, 7 and 8. A camera can be included more than once in the same tour.

### Color bars

On Multi-Media DSP units, the MONITOR OUTPUT 1 connector on the back of the Multi-Media unit cannot produce a test pattern. For these units, the Color Bars option is not available, on the Monitor Out tab of a Maintenance Session.

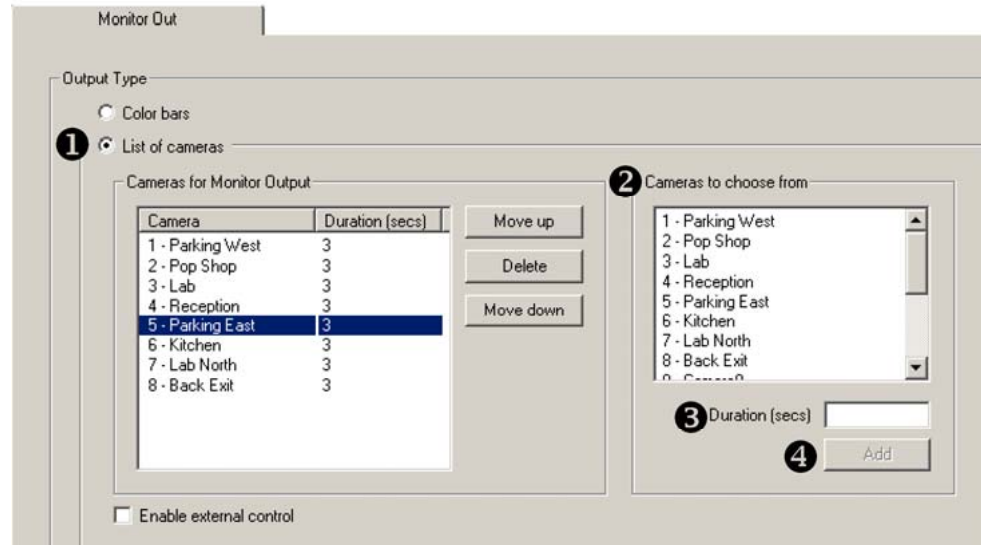
## External Hardware Control of a Public Display Monitor

You can connect a third-party hardware switch to a Multi-Media unit. The switch can freeze a public display monitor and control whether the next camera or previous camera is monitored. For wiring details, see table 8-5 and the switch documentation. To enable local hardware control of a public display monitor:

1. Using View, continue or start a Maintenance Session for the Rapid Eye site, as explained in Maintenance Session, on p. 53.
2. Click the Monitor Out tab.
3. Click the Enable external control box so that it shows a checkmark. This reserves a Multi-Media unit's General Purpose Inputs 13, 14 and 15 for switch use. You can see the box in figure 8-8.

**Fig. 8-8. Monitor Out Tab, for a Multi-Media Unit's MONITOR OUTPUT 1.**

To customize a local tour



**Table 8-5 Inputs for External Control of MONITOR OUTPUT 1**

General Purpose Input	Instructs Video Capture Card to...
13	display previous camera
14	display next camera
15	continue or pause public display monitor*

\* A selection of video feeds from one unit for use with a public display monitor is very different from: (a) site tours, involving many Rapid Eye sites (see Touring Many Sites, on p. 221) or (b) PTZ tours: preset PTZ movements (see Pan, Tilt, and Zoom (PTZ) Setup). Use of a local user interface is also unrelated to these public display monitor settings.

## Using LocalView As an Additional Public Display Monitor

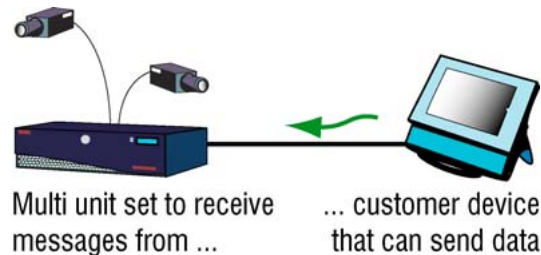
For a better public display of video, Honeywell recommends using a dedicated NTSC (or PAL) monitor, rather than the VGA output used for LocalView. Nonetheless, you have the option of using the VGA monitor displaying LocalView as a public display monitor or as a second public display monitor (in addition to a dedicated monitor). Set Local View to display the camera(s) that you need. More than one camera can be displayed simultaneously.

## Customer Data and Customer-Device Events

### Purpose

View can display messages from many non-Multi hardware devices and systems such as: cash registers, door access sensors, a guest registration system, and so on. A Multi-Media unit can record these messages.

**Fig. 8–9. Customer Devices can Include POS Units, such as Cash Registers.**



### Video from a Customer-device event

A message from a third-party device is treated as a Customer-device event by a Multi-Media unit; see, Events Defined, p. 187. You have the option of having up to 100 messages per device either logged, triggering an alarm or both. This powerful asset to surveillance technology is synchronized to recorded video.

### Preparation

Before defining customer-device events and using them as alarms, a View operator needs:

- Serial communications settings of the customer-device. These are obtained from the device's manufacturer and are required to correctly receive data from the device.
- Specific rights added to a typical View user account: (a) the Modify configuration right and (b) access to the site that is connected to the Customer-device event. See Right to Use Maintenance, p. 180.
- To know which serial port on a Multi-Media unit is used by the device, and knowing if it is already being used by another devices, such as a PTZ camera control, and so on.
- To know how rules. How "strings" of text are formatted and produced by customer-devices.

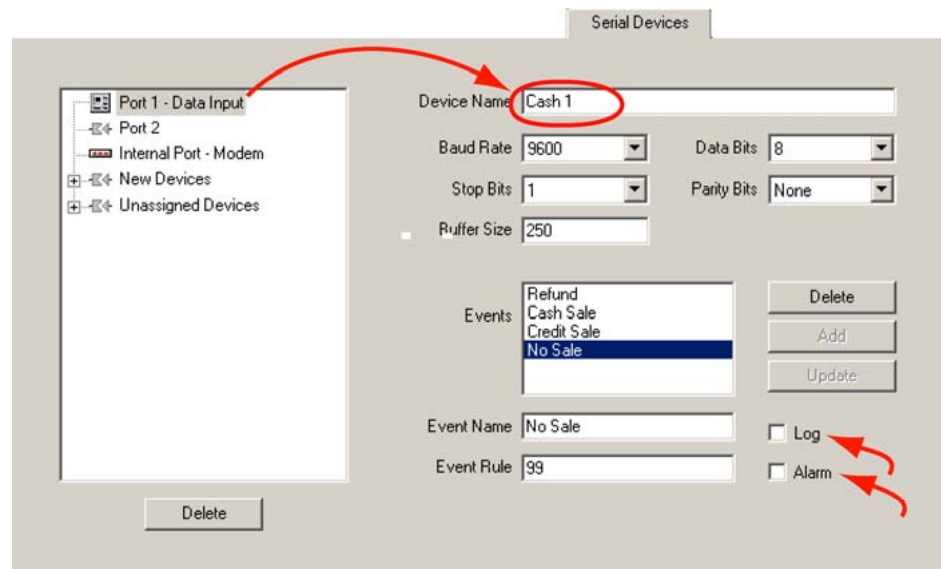
In the next procedure, let us suppose that the owner of a retail store wants video of an employee at a point of sale (POS), when goods are purchased. Assume that a cash register is connected to a Multi-Media unit and you know the cash register communication settings.

## Adding a Customer Device That Sends Data to a Unit

1. Start a Maintenance Session for the Rapid Eye site. Wait until a "System Operational" message appears.
2. Click the Serial Devices tab.
3. Expand **New Devices** (as needed) to see a Data Input icon. See figure 8–10.
4. Drag the Data Input icon to the Port 1 icon.
5. To name the interface between Multi and the cash register, click the Device Name box for the Serial device (above the Baud Rate label), and type a name, for ex. "Cash1".

6. Set the communication parameters (Baud Rate, Data Bits, Stop Bit, and Parity Bit) to values recommended by the manufacturer of the device.
7. Ignore the Buffer Size for now. This value is dealt with using procedure Adding an Event Rule for a Data-recording Device, below.
8. To add a data-recording rule(s), see the next procedure.

**Fig. 8-10. Some Devices can Be Searched for Data such as "No Sale".**



To log the "no sale" event or have it trigger an alarm

## Adding an Event Rule for a Data-recording Device

1. While or after adding a data-recording, serial device, as explained in the procedure Adding a Customer Device That Sends Data to a Unit, above, click in the Event Name box and type a name, for ex. "No Sale".
2. In the Event Rule box, type:
  - A code obtained from the manufacturer of the device. For example, a no sale message from a device is coded as one or more numbers, or text. See the documentation for the device.

– or –

  - A regular expression of your choice; see the Search Rule and Regular Expressions: Reference, next.
3. Click **Add**.
4. Compare the value in the Buffer Size box to the length of rules typed in step 2. You have the option of changing the number of bytes in the buffer so that it is greater than or equal to the longest rule added in step 2 of this procedure. Consider if any rules use wildcards (see table 8-6); you may need to use a bigger buffer. The default value of 250 bytes should be adequate for most organizations.
5. You have the option of adding more events, as many as 512 different events or regular expressions can be processed for each data-recording device.



## Search Rule and Regular Expressions: Reference

Table 8–6 lists the special characters available for use when making rules in the Rule box. Technical users who know how to use a regular expression (RE) will benefit most from using table 8–6. Also, there are examples of extended data searches in the *Rapid Eye View Software Operator Guide*.

**Table 8–6 Special Characters Available for a Search Rule**

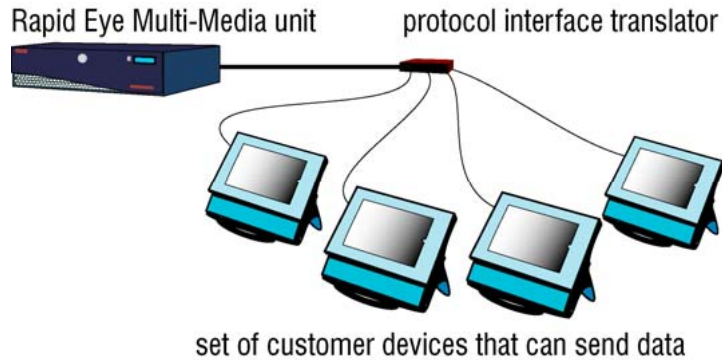
Character	Name	Searches for a Match of (...) Within the Rule
.	Period	Any one character. Ex: .ire finds “wire”, “tire”, “4ire”, and so on.
[ ]	Square brackets	Each character in the brackets, in turn. Ex: c[au]t finds “cat”, “cot” or “cut”.
^	Caret	(a) Characters that are not in brackets. Ex: r[^a] finds “rb”, “rc”, “rA”, “r1” and so on. (b) A rule at the beginning of a line. Ex: ^Hume finds “Hume” at the start of lines. (c) A control code, when used with a backslash. Ex: \^C finds the “control-C” control code.
\$	Dollar sign	A rule at the end of a line, when placed after it. Ex: Kant\$ finds only “Kant” at the end of lines.
-	Dash	A range of characters set in square brackets. Ex: [a-z] matches any lower case letter.
+	Plus sign	The character that it follows, once or more. Ex: tu+ finds “tu”, “tuu”, “tuuu”, and so on.
*	Asterisk	The character that it follows, whether absent, occurring once or more. Ex: mo*e finds “me”, “moe”, “mooe”, “moooe”, ... Ex: c[au]*t finds “ct”, “cat”, “caat”, “cut”, “cuut”, ...
?	Question mark	The character that follows the question mark, whether absent or occurring once. Ex: me?y matches either “mey” or “me”.
\	Backslash	(a) Special character, when placed before it. Ex: \? Finds “?”; (b) Control character, when placed before it. Ex: \b finds a backspace, \e an Esc (escape), \f a form feed, \n a new line, \r a carriage return, \t a tab and \x0D a hexadecimal encoded ASCII character.

## NetPIT and PIT Devices

### Support for Protocol Interface Translators

Honeywell supports Protocol Interface Translators (PITs) and a networked Protocol Interface Translator (NetPIT), for attaching many serial devices to a Multi-Media unit.

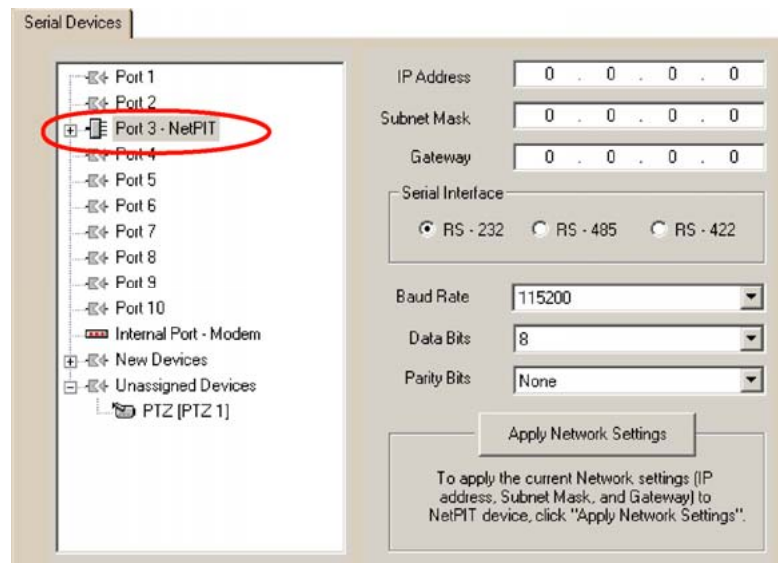
**Fig. 8-11. Cash Registers, Connected to a Honeywell PIT.**



A NetPIT device provides communications for up to 16 POS devices from one serial port. NetPIT supports applications by Retailix (RetPIT), Micros (MicPIT) and AtmPIT. A PIT can provide communications for one device (AVBPIT1) or up to four devices (AVBPIT4POS); see figure 8-11.

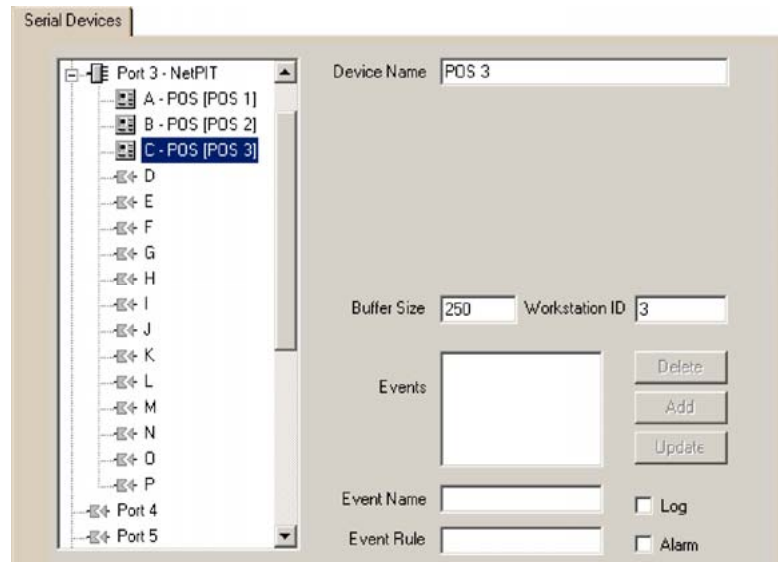
When assigned to a port on a Multi-Media unit, the configuration values of the serial interface are shown. See figure 8-12.

**Fig. 8-12. A NetPIT Device on PORT 3, Showing All Serial Interface Values.**



When expanded, a NetPIT device shows 16 virtual ports, labeled “A” to “P”; see figure 8-13. A PIT device (AVBPIT4POS) shows 4 virtual ports, labeled “A” to “D”. When a device is assigned to a virtual port, the settings of that device are shown on the Serial Devices tab. Each virtual port can be configured independently for speed, data format, and protocol. For the details of the configuration for these devices, see their documentation.

Fig. 8-13. Expanded NetPIT device on PORT 3, showing three POS devices.



#### Port restrictions

- A PIT device cannot be assigned to the virtual port of a NetPIT.
- Only one NetPIT device can be assigned to a Multi-Media port.
- If a PIT or NetPIT device is assigned to "Port 1" or "Port 2", only the RS-232 interface is available. The three serial interfaces are available on Port 3 through Port 10.
- The Internal Port cannot be used for a PIT or NetPIT (Network Protocol Interface Translation) device.

## Multi Audio

Channels can be renamed. View operators use audio "channels" to:

- **Listen.** A microphone at the Rapid Eye site.
- **Talk.** Talking on one channel, or broadcasting on both.

#### When listening...

All sound sources are mixed at a View operator's station, regardless of the number of sites being monitored at once. Each Rapid Eye site can send up to two channels of audio to a View operator.

## Audio Hardware

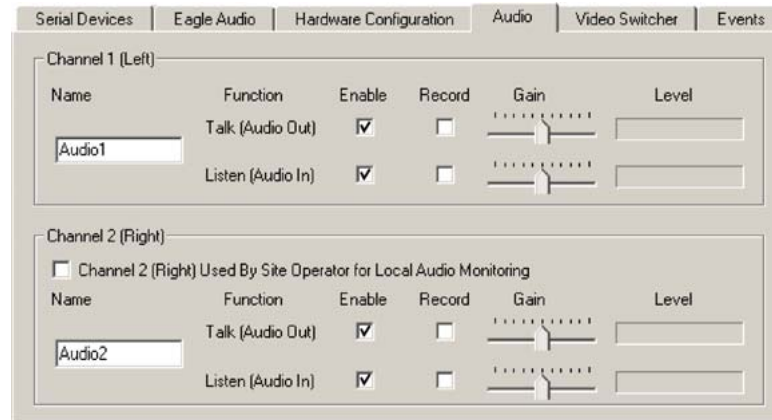
Microphones, powered speakers, and so on, need to be connected to a Multi-Media unit; the operator's PC also needs a microphone and speaker, for two-way audio, and a sound card. For more detail about audio hardware, see the *Unit Installation Instructions*, K14390. A PC running View requires a sound card to produce sound from the Rapid Eye site and to send sound to it.

## Using Multi Audio

### Monitor and record

Click the Enable boxes to enable transmission of sound from point to point and monitor it. Click the Record box to record sound along with the video from the site. You can monitor, record or do both, for each channel.

**Fig. 8-14. Audio Tab.**



### To enable “talking to” one site, or broadcasting to many

Click the monitor Talk boxes, as needed for each channel; see fig. 8-14. An operator can broadcast on either or both channels, and to as many sites at once as can be opened.

## Audio Interference

Checking one’s installation for hard-to-predict situations includes spot-checking for:

live audio. Coordinate the testing of audio with fire alarm and security alarm testing. Using View, connect to that Multi-Media unit and check audio for feedback and interference, before and during alarms.



**Loud alarms can interfere with microphones or a speaker at times when they could be needed most.**

recorded audio. After a day or two, check for background noise in recordings, using a retrieval session to spotcheck each microphone for a few seconds at every half-hour or so, during a 24 hour period. This can reveal if microphones are placed too near sources of background noise, such as a vent, that are amplified to a point where they interfere with audio. Hard to predict noise from the area’s soundscape—rush-hour traffic, passing trains and planes, crowds in a stadium, and so on—may not have been apparent during the installation of the microphones and speakers.

## Audio with LocalView

At sites where LocalView is in use, Channel 2 of audio can be reserved for use onsite. View operators using these sites can use only Channel 1. Audio can be changed by Multi System Administrators by using View to connect to the Multi-Media unit.

## To Enable Audio for Use Onsite, by LocalView

1. On the Audio Setup tab, add a checkmark to the box for Channel 2 (Right) Used by Site Operator for Local Audio Monitoring. The "channel 2" Enable, Record and name become unavailable; they are not needed for monitoring audio by a LocalView operator.
2. In the Channel 1 controls, add checkmarks to the Enable boxes for Talk, Listen or both, as needed.
3. You have the option of adding checkmarks to Record boxes for Talk, Listen or both, as needed. The Enabled box needs to be checked before its Record box can be.

## To Disable Audio for LocalView

- Using either View (or LocalView), on the Audio Setup tab, remove the checkmark in the checkbox for Channel 2 (Right) Used by ...

## Multi-Media LT Audio Resources

There is only one channel of audio on Multi-Media LT units. For audio use, see the Multi-Media LT Unit Installation Instructions.

## Eagle Audio

Eagle Audio is discussed in the *Multi and Eagle Audio Configuration Guide*, part number K9203. Please contact your Multi distributor if you need information about Eagle Audio.

### Tip

**Multi Audio differs from Eagle Audio, which is an optional, third party, audio interface.**

## Events

For Multi events, please see Events Defined, p. 187.

## Simultaneous Sessions From One Unit

Table 8–7 lists the number of streams available to operators. Table 8–8 shows how many operators can obtain the streams that are left available. For example, on one unit, two operators could both view 16 live cameras, each. If ten operators are running Live sessions on a unit, each could view three or four cameras (either the same cameras or others), for a total of 32. For live audio, the ten connected operators could each hear the two channels of audio, and each could monitor all data streams.

**Table 8–7 Stream Availability**

Session	Video	Audio	Data
Live	32	all streams × connected users*	all streams × connected users*
Retrieval	32	16	16

\* All of the unit's streams are available, to as many operators that can connect; see table 8–8.

**Table 8-8 Maximum Simultaneous Sessions**

<b>Session Type</b>	<b>View Operators in Session</b>
Live or Live-alarm	10*
Retrieval	10
Event	10
Data	10
Alarm	10
Motion	10
Maintenance	1**

\* The operators share the available streams. See table 8-7.

\*\* Other sessions are terminated if Apply or Reboot command are used.

### **Multi-Media LT**

For Multi-Media LT units, the number of simultaneous View operators may be less.

## **Simultaneous Use of Many Units by One Operator**

Up to 64 simultaneous connections to different units can be made by one operator. Note that this number can be lower due to the CPU of the PC that runs View, the PC's memory and the number of other tasks running.

### **Audio broadcast**

Audio can be broadcast to many units simultaneously, using View software. To broadcast: click **Talk** in more than one player before using the microphone at the operator's PC.

# Users

## Key Facts

### Flexibility

If one user, or very few are operating the Multi-Media unit(s) in your organization, you may not need to create user accounts. See Default User, on p. 152. However, in organizations with many Rapid Eye users or units, Honeywell recommends creating user accounts for unit operators.

### Account users operate Multi-Media units

It can be more accurate to refer to account users as “unit operators”; a Multi SA creates accounts so that personnel can operate units. Accounts created using LocalView can be used only onsite at the site that they were created. Accounts created using Admin are generally used to run View software on a PC, to connect to one or many units, over a LAN or using dial-up.

### Administrator account

To run Admin software, use the Administrator account. Use of Admin and the Administrator account should be reserved for use by your organization's Multi SA. Reasons for doing so are explained in Limiting the Use of Admin, on p. 163. The default Administrator account can also be used to run View software, to configure units, by using a Maintenance Session.

### System password

The system password is not used by users. Authorized users do not need to know and should not know the system password. It protects units from Admin and View users in other organizations. See System Password, p. 166.

### Using LocalView only

Multi SAs have the option of creating user accounts onsite, using LocalView, on a unit-by-unit basis. This is convenient when your organization has only one unit, or very few and few users. See User Management, p. 153.

## Before Creating User Accounts

### Where we are, if using Admin software

At this point, a Multi System Administrator (Multi SA) using Admin software has:

- Obtained or created a Multi Central database (Multi db). See Obtaining a Multi db, on p. 232.
  - Created at least one site. You can still create user accounts before sites; without a site, users will not be able to do much more than open View. See Naming / Renaming a Site, on p. 24.
- and -
- Added the password to the Administrator account. Highly recommended by Honeywell, though optional; see Administrator Password, on p. 176.

### Where we are, if using LocalView, onsite

At this point, a Multi SA using LocalView has:

- Added the password to the Administrator account. This is highly recommended by Honeywell, though optional; see Administrator Password, on p. 176.

### What you need from your security officer

Before adding accounts, your Multi SA may need to consult your organization's security personnel, to find out if:

- The Multi installation will be "open" or if it needs security. See Security Options, on p. 161.
- Operators are required to use passwords. See User Password, p. 176.
- Operators should have different profiles in their user accounts. See Rights of User Accounts, on p. 178.
- All operators can access Multi-Media site and operate a Multi-Media unit. See Right to Access a Site, p. 182.

## Default User

### "Administrator" accounts

Admin software and LocalView each have a default, permanent account, named: "Administrator". These accounts cannot be removed or modified; however, Honeywell recommends that you add a password to them, if they are in use. If very few users (1 or 2) are using the Multi-Media unit(s) in your organization, you may not need to create other user accounts.

### Admin software's remote "Administrator" account

The Administrator account in Admin software grants a remote operator access to every Rapid Eye unit in your organization. Users of this account can also use every function in Admin and View software. If a unit's management of accounts is "central", the Administrator account in Admin software replaces the one in LocalView.

### LocalView's local "Administrator" account

The Administrator account in LocalView grants an onsite operator access to one Rapid Eye unit in your organization. Users of this account can also use every function in LocalView software.



### Many users

If many users use the system, Honeywell recommends:

- Your Multi SA limit the use of the Administrator account and add a password to the account (see Administrator Password, on p. 176).
- That the password to the "Administrator" user account, and of any others based on that account, should be kept secure and changed regularly.

### Using Admin software

To log on to Admin software, other user accounts can be used if they have the Rights and site access are based on Administrator. Creating such accounts should be handled with care in high security environments.

### Configuring LocalView

To configure LocalView software, a user account needs the Modify Configuration right.

## User Management

### Flexibility

Switching a unit from Local User Management (the default) to Central User Management is an option.

### Setting user management

- Changing User management is performed unit-by-unit.
- Only Admin software can be used to set a unit to Central User Management.
- Only LocalView can be used to re-enable a unit to use Local User Management.

### Creating Multi-Media accounts for running View software

Whether user management is central or local, Admin can always be used to add accounts for connecting to a unit from a PC running View.

### Older units

User management is not available on older Rapid Eye models such as Multi units.

## Local User Management

### Creating accounts using either LocalView...

Local User Management enables a Multi SA to create operator accounts onsite, using LocalView, for operating that unit only. When user management is set to "Local" in LocalView, the list of accounts on that unit can be edited.

### ... or Admin software

In addition, a Multi SA can create Rapid Eye accounts using Admin software while Local User Management is in force. These "standard" Rapid Eye accounts are used to access one or many units remotely, from a PC running View software.

### Setting a centrally managed unit to Local User Management

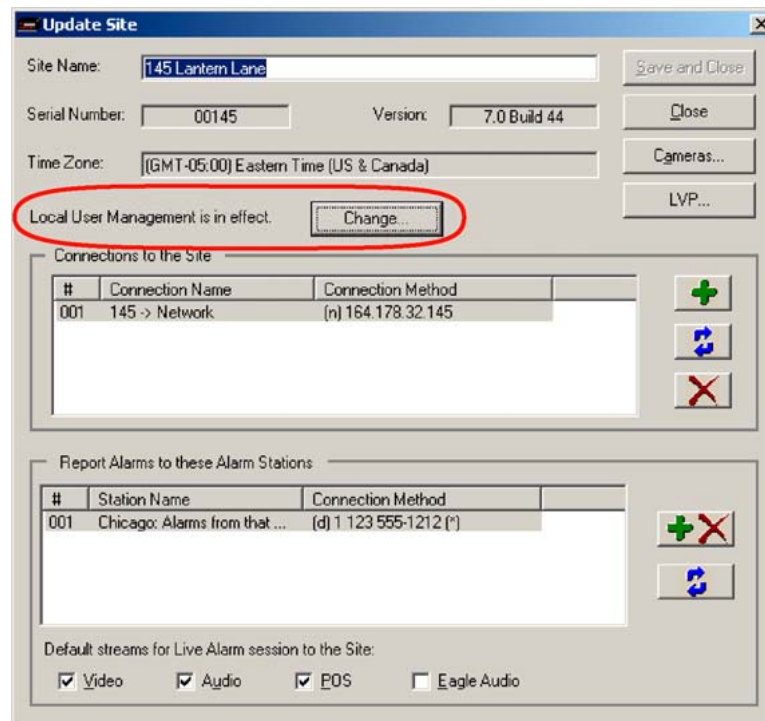
A LocalView administrator has the option of setting User Management to "Local". Accounts that were created centrally remain on the unit.

## Central User Management

### Creating accounts using Admin software

Central User Management disables only the onsite creation of operator accounts, using LocalView. If Central User Management is in effect, a Multi SA uses Admin software to create accounts. These "central" accounts can access Multi-Media units using View software or LocalView.

**Fig. 9-1. Button for Changing User Management from Local to Central.**



## Setting a Unit to "Central" User Management

1. While using Admin software to update (or create) a site's definition, click **Change...**, next to Local User Management is in effect. See figure 9–1. A dialog box appears to confirm setting the site to central user management. After clicking Yes, the message next to the button will change to "Central User Management is pending".
2. Use View to run a Maintenance Session at the site.
3. Click the Security tab.
4. Update Security. The procedure to update security is also shown in Updating Security on a Multi-Media Unit, on p. 131.

### Result

The next time that you update the site using Admin software, the label next to the Change button will read "Central User Management is in effect".

The accounts of users authorized to operate the unit are copied to the unit and replace accounts created locally. Operators with accounts that authorize operation of the unit, can access that unit either offsite using View, or locally using LocalView.


### Notification of a discrepancy between Admin software and LocalView

After a Multi SA has used Admin software to select "Central" user management and View to run a Maintenance Session, as explained above, the LocalView Administrator can select "Local" user management. The next time that the Multi SA runs a Maintenance Session, a message indicates that there is a discrepancy in the User Management settings. The Multi SA has the option of setting User Management to "Central", or of leaving it to "Local".

## Adding an Account, Using Admin and View

### Account for accessing all units

Whether user management is central or local, Admin is used to add accounts for connecting to a unit from a PC running View.

1. Using Admin, click the Users tab.
2. To display the Add User dialog box, do one of the following:
  - Click  on the toolbar.
  - Click **Add** on the Actions menu.
  - Use the Ctrl+Ins keys on the keyboard.
3. Type a name in the User Name box. See the example in figure 9–2. If the name is already used in your system, you will be asked to use another one.
4. You have the option of adding a password to the account. To do so, type a password in the Password box; type the password again, but in the Confirm Password box. Some characters cannot be used in a password, such as a double-quote ( " ). If one is typed, a warning appears.
5. You have the option of modifying the account's rights. See Granting Rights, on p. 158.
6. Click **Save and Close**.

**Fig. 9-2. Adding a "Night Operator" Account.**

The screenshot shows the 'Update User' dialog box with the following details:

- User name:** Night Operator (highlighted with a red circle)
- Password:** [Empty field]
- Confirm password:** [Empty field]
- Buttons:** Save and Close, Close
- Radio buttons:**
  - Rights and site access are based on: Administrator
  - Rights and site access are restricted to
- Restricted Access Options:**
  - Modify configuration
  - Modify security
  - Modify system settings
  - Live video
  - Retrieve video
  - Audio, listen
  - Audio, talk
  - Use PTZ
  - Use outputs
  - Process alarms
  - Time limit: 8 min
- Site Access:**
  - User can access all sites
  - User can access selected sites
- Selected Sites:**
  - Screens.mdb
  - VicGott Park
  - Gershwin Place
  - Bioc Way
- Additional Options:**
  - Automatically access sub-sites added in the future.
  - Deny this account access to sites. Important: for this to work, use View to run a maintenance session and update security at each site listed in this user account.

### Updating security for onsite use of a central account

When Central User Management is enabled, an operator account created with Admin can also be used onsite, in LocalView. To enable use of the account onsite, use View software to update security on that unit. See Updating Security on a Multi-Media Unit, p. 131.

### Extras

You have the option of:

- Basing the user-account on another. Click **Rights and site access are based on**. The box next to it lists other accounts on your Multi system that can serve as a basis for the group.
- Changing the rights of an account. You can limit access or deny access to sites and to a site's cameras, for that account; see Granting Rights on p. 158, and Denying Access, p. 198.

## Naming Restrictions

For user account names, do not use:


- The "[database name]" of the Multi db. A user account with the same name as the Multi central database causes an error when a copy of the database is made locally.
- "Self" or "(self)". Phrase used by some Multi reports.
- "Administrator". This account name is reserved.

## User Groups

To create a group of users, assign the same user-account to different users. To do so, View operators either:

- Use an account on based on another. View Operators each have their own account, but the rights, sites and so on, of the accounts are common. See Granting Rights, p. 158.
- Share the same account. Add an account as explained earlier, in section Adding an Account on p.155; then assign the same account to different staff.

## Updating an Account

1. Using Admin, click the Users tab. (There is no need to click it if the tab is already displayed.)
2. Double-click the name of the account. You can also select the user account and do one of the following:
  - Click  on the toolbar.
  - Click **Update** on the Actions menu.
  - Press the F12 key.
3. Edit the user account information.
4. Click **Save and Close**. If Central User Management is enabled and the operator account will be used to operate the unit onsite, using LocalView, use View software to update security on the unit(s) to which the account will grant access. See Updating Security on a Multi-Media Unit, p. 131.

## Adding an Account in LocalView

1. Using LocalView, click the Configuration tab.
2. Select User Management.
3. Click **Add New User**.
4. Type a name in the User Name box. If the name is already used on the unit, you will be asked to use another.
5. You have the option of adding a password to the account. To do so, type a password in the Password box; type the password again, but in the Confirm Password box. Some characters cannot be used in a password, such as a double-quote ( " ). If one is typed, nothing happens.
6. You have the option of modifying the account's rights. See Granting Rights, below.
7. Click **Save**.

### Account for accessing one unit

Accounts created using LocalView can access only the Multi-Media unit running LocalView.

### Central user management

When user management is central, accounts cannot be created using LocalView.

## Updating an Account in LocalView

1. Using LocalView, click the Configuration tab.
2. Select User Management.
3. Select a user.
4. You have the option of modifying the account's password and user name. To modify rights, see Granting Rights, below.
5. Click **Save**.

## Granting Rights

Rights can be selected when either: adding a user account or updating a user. You can:

- Customize the rights of an account.
- Base the rights on those of another account.

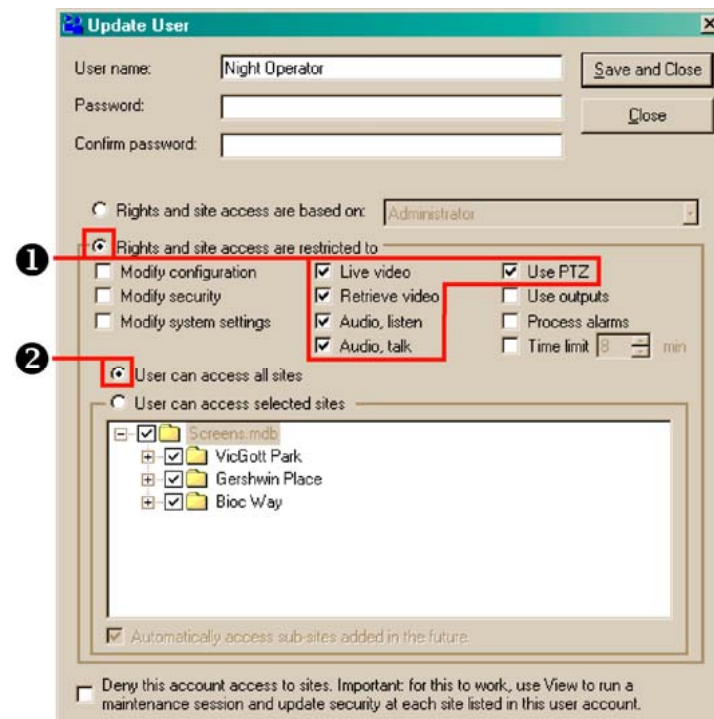
For security guidelines on assigning rights see Rights of User Accounts and its sub-sections, starting on p. 178.

**LocalView.** Using LocalView to grant rights in a user account makes those rights available only for that unit, when running LocalView.

**Admin.** Use of Admin to grant rights to a user account makes those rights available on many units.

## To Customize the Rights in an Account

Fig. 9-3. Defaults: User Account Rights (1) and Site Access (2).



1. While adding or updating an account, click a box next to a right. See figure 9-3. Adding a checkmark adds the right to the account; remove the checkmark to remove the right.
2. To limit camera access, see To Limit Use of Cameras: Camera Partitioning on p. 183.
3. After modifying rights, users of Admin need to click **Save and Close**. Users of LocalView do not. If Central Management is enabled and the operator account will be used to operate the unit using View software and LocalView, then use View software to update security on the unit(s) to which the account will grant access. See Updating Security on a Multi-Media Unit, p. 131.

## To Base Rights On Those of Another User

This feature is available in Admin only; not in LocalView.

1. Using Admin, click the User tab.
2. While updating or adding the account, click **Rights and site access are based on**.
3. Choose a user account from the list.
4. Click **Save and Close**.

## User Rights and Security

### In organizations with high security requirements

Your Multi SA can use Admin to provide operator accounts that:

1. limit the sites that a user can access. By default, access to all sites is granted. See Right to Access a Site on p. 182. You can set accounts to access only some sites.
2. limit the amount of time for use of a site. See Right to Access a Site, on p. 182.

### LocalView

When using LocalView, there is no time limit to operating a unit.

## To Deny Access

Denying access to sites is a security measure that is used against an operator who must be stopped from using Multi-Media units as soon as possible. The account data is preserved. For less severe cases, removing an account may be sufficient; see Removing a User's Account, p. 160.

### Denying access to all Multi-Media units: Admin


1. Using Admin, click the Users tab.
2. Double-click the name of the account in the User Name column.
3. Click the box next to Deny this account access to sites [...] so that it shows a checkmark.
4. Click **Save and Close**.
5. Update security at each site listed in the "User can access selected sites" list. The procedure to update security is in section Updating Security on a Multi-Media Unit, on p. 131.

### Denying access to LocalView, onsite.

1. Using LocalView, click the Configuration tab.
2. Click the Users tab.
3. Select the account.
4. Click the box next to Deny Access so that it shows a checkmark.

## Removing a User's Account

### For Accounts created using Admin software, whether user management is local or central:

1. Using Admin, click the Users tab.
2. Select the user that you want to delete.
3. Do one of the following:
  - Click  on the toolbar
  - Click **Delete** on the Actions menu.
  - Press the Delete key on the keyboard.
4. When you are warned that the user is about to be deleted, click **Yes** to continue or **No** to cancel. If other accounts are based on the account, a message warns of the fact, offering the option to proceed with, or cancel, the deletion of the account.

## To Delete an Account Used Onsite, to Access LocalView

### Local User Management

For accounts created using LocalView:

1. Using LocalView, click the Configuration tab.
2. Select User Management.
3. Select the user that you want to delete.
4. Click **Delete**.
5. When you are warned that the user is about to be deleted, click **Yes** to continue or **No** to cancel.

### Central User Management

When Admin is used to set a unit to Central User Management, LocalView cannot be used to delete user accounts. After using the procedure for Accounts created using Admin software, on p. 160, use View software to run a Maintenance Session and then Update Security on the Multi-Media unit. You also have the option of running a Maintenance Session on other units to which the operator had access, to Update Security on those as well.



# Security for a Multi-Media System

## Security Options

### Flexibility in security

These guidelines are suggestions to complement your organization's security policies and procedures. Most are optional in low-security environments.

### Security outlook

The security features of Multi can be applied to very different areas of security:

- Securing the Multi system. Includes passwords, designating as few Multi SAs as possible, and so on. Use of Multi for this type of security starts in Securing the Multi System.
- Using a Multi system as a security device. Includes setting up alarms that are triggered by an Outside World event. See Events Defined, p. 187.
- Hybrid use. Multi can be used as a security device to supervise users. See Tracing Events, p. 191 and Denying Access, p. 196.

## Securing the Multi System

### What level of security is needed?

Multi can be used effectively in high and low security situations. Use of security features is optional, making the system a flexible tool in many security environments. Officers in your organization can help define how open or secure the Multi system should be.



**Even in minimal security environments, using passwords for the system and for the default "Administrator" account are highly recommended by Honeywell. See System Password, on p. 166, and Administrator Password, on p. 176.**

## Security Priorities

### From minimal security to maximum security

Table 10–1 suggests an order for implementing a secure Multi system.

### Additional security for some installations

This additional security may not apply to your installation. If you are unsure, see the network administrator.

- LocalView. Multi SAs can use Central User Management to control user accounts. See User Management, p. 153.
- Multi databases on a network. Network system administrators or database administrators can protect a Multi Central database from deletion. See Multi Database Security, on p. 165.
- Remote access service. Multi SAs may need to obtain PPP connectivity passwords. See PPP Connectivity, on p. 196.

**Table 10–1 Security Priorities**

Priority	Action	Page
	limit installation of Admin to Multi SA PCs	163
	limit access to the <i>System Administrator's Guide</i>	163
*	use a system password	166
	add a password to the "Administrator" account	176
	designate specific PCs as Multi alarm stations	195
	assign passwords to user accounts	176
	limit the rights of user accounts	178
*	trace critical system events	191
	know how to deny access to a user	196
	backup and safeguard your Multi central database	165

\* Optional priorities for dealing with external security, or tampering that originates outside of your organization.

### Minimal security

Minimal security can be appropriate when a Multi system is used by only one person. At the very least, Honeywell recommends that you add a system password (see System Password, p. 166).

## Limiting the Use of Admin

### Flexibility in security

Like most Multi-Media security features, limiting the installation and use of Admin to the PCs of Multi SAs is optional.

## To Limit Access to Admin Documentation

- Use only the View CD to install Multi software on a View operator's PC.

### Features

For secure installations, the Security Officer(s) in your organization should:

- Designate as few Multi SAs as possible
- Limit the installation of Admin software to the PC(s) of Multi SAs, especially in open systems.

### Tip

**For secure installations, Honeywell recommends that only Multi SAs receive copies of Admin software.**

View operators should only receive copies of View.

- and -

- Limit the distribution of Admin documentation.

### Tip

**As a security measure, only the Admin disc can be used to install the Admin user documents.**

When you use the View CD, only a *Rapid Eye View Software Operator Guide* is copied to the PC hard drive. The guide is in Adobe Portable Document format (PDF). As an added security measure, no one can run Admin or View documentation from the Rapid Eye Multi CDs; one needs to install Multi software before the documentation is available.

## Password Guidelines

### Flexibility in security

Like most Multi-Media security features, use of passwords is optional. Honeywell does recommend using and changing the system password and the password of the default "Administrator" account, even in minimal security environments. See System Password, on p. 166, and Administrator Password, on p. 176.

Access to the Multi system is obtained through user accounts. The Administrator account is the "super user" or "linchpin" account. Password use counters the unauthorized access to Multi-Media units.

## Passwords

- **System password.** A global password for all of the units in your organization. The system password is not used by users; it counters access of units by unauthorized users, such as those part of another Multi-Media system. Please make a record of the System password in case Multi technical support is needed for a Multi-Media unit. Honeywell recommends that your Multi SA use a system password (see System Password, on p. 166).
- **Administrator account password.** Users of the Administrator account can use every function in Admin and View. They can access every Rapid Eye site in your system. To control this account, add a password to it, as explained in Administrator Password, on p. 176. The password to the Administrator account also protects Multi-Media units from unauthorized clearing of storage; see Preventing Users from Clearing Storage, p. 130. This password, and of any others based on the Administrator account, should be kept secure and changed regularly.
- **User account password.** A user's password can be unique or the same as another user's, as required by your security policy.

Passwords can be:

- **Of variable length.** composed of up to 50 alphanumeric characters. Double-quotes (") cannot be used.
- **Repeated.** Your Multi System Administrator (Multi SA) has the option of assigning the same password or differing passwords to users.
- **Deleted (i.e., emptied).** This is equivalent to not assigning a password. There is no "reset" function. Your Multi SA does not need to know a user account password to set it; a Multi SA should only remember/log the user account password to the "Administrator" account.
- **Set only by a Multi SA.** A View operator cannot set a user account password; only the Multi SA can.

### Using text securely in Multi password boxes

- To prevent onlookers from obtaining a password, asterisks appear as you type in these boxes.
- To prevent use of the Windows Clipboard to obtain passwords, Multi software prevents the copying or cutting of passwords from password boxes.
- To help guarantee against typing error when a password is entered, you type the password again, in the next box.
- To further guarantee against typing error when setting passwords, you can paste text from another file, into a password box.

### Password Tip

- Some passwords hamper dictionary-style attacks. Insert numbers in common words. For example, a password such as typography is made more secure as typog2691raphy. Such passwords are easier to remember than randomly generated passwords; though both types do hamper this style of attack.

## Multi Database Security

### Flexibility in security

Like most Multi-Media security features, using network means to protect a Multi database is optional. If the Multi db is protected, Multi-Media unit operators need read/write permissions to a Multi db.

### Protecting the database from deletion

The Multi db can be protected using server file system capabilities. As a preventive measure against the accidental deletion of a Multi db, back it up and use network settings (such as NTFS security). See also Deleting a Database on p. 245.

### Password security

Passwords are encrypted in Multi db files (\*.mdb and \*.mdf).

### Protecting the database from copying

It is important to protect your Multi db from copying, if only to avoid its use by external unauthorized users, who could also be licensed Multi software users.

## SQL-Server Option

### Security option for SQL-Server

To add security to a Multi database, your SQL database administrator can setup a SQL login just for Multi users. By default, Multi software connects to a server running SQL-Server by using 'sa' as a logon account, with no password.

## SQL-server Type Logon, Reserved for Multi Operators

1. Run SQL Server Enterprise Manager.
2. Add a new log on.
3. The "public" and "db\_owner" database roles need to be assigned to the log on, so that a user can connect to the Multi db, update it and—if Multi SAs are to use Admin to create a Multi db—create a new SQL-based Multi db.

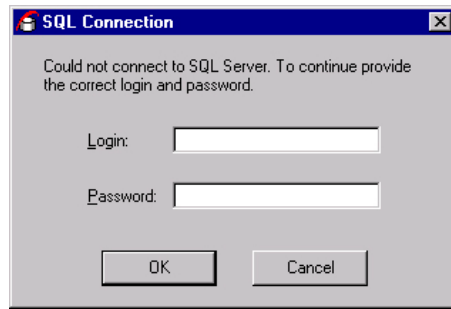
### Tip

**Creating a SQL-server type logon is a procedure for a SQL-Server administrator, not for Admin users or View operators.**

### Result

When these changes are made to SQL-Server security, a "log on to SQL" window appears, as in figure 10-1. The Login and Password of SQL can differ from the User ID and Password of a Multi account.

**Fig. 10-1. Logging on to SQL-Server Differs from the Log on to Admin.**



**The following runs of Multi software**

The next time that you use Admin or View, the same SQL logon and password are used, without the SQL Connection window appearing.

## System Password

**Flexibility in security**

Honeywell recommends you use a system password for units that use a dial-up connection or are on a public network.

On a private network, its use may be unnecessary. To find out about the security protocols in your organization, see your security personnel.

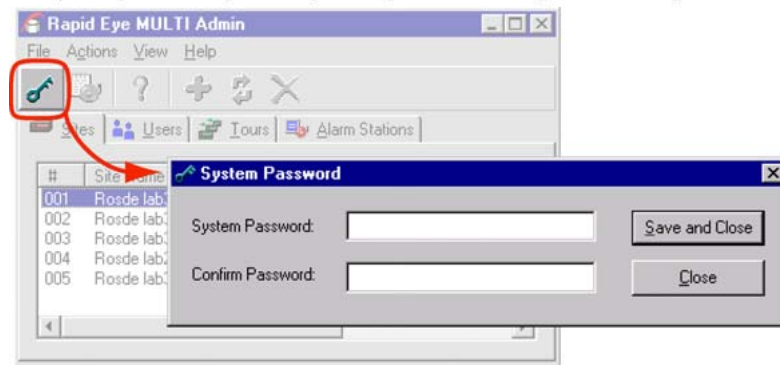
**In a nutshell: keeping unauthorized users out**

A system password blocks access to all (or optionally, some) of your sites from unauthorized users, external to your organization, who may have found out the dial-up number or IP address of a site, and who have access to Multi Admin and View software.

Authorized Operators do not have to remember the system password to use a Multi-Media unit. Only the Multi System Administrator needs to keep a record of it in case a unit is added or removed from your Multi system.

**Fig. 10-2. System Password.**

Preparing to change the system password of your Multi system...

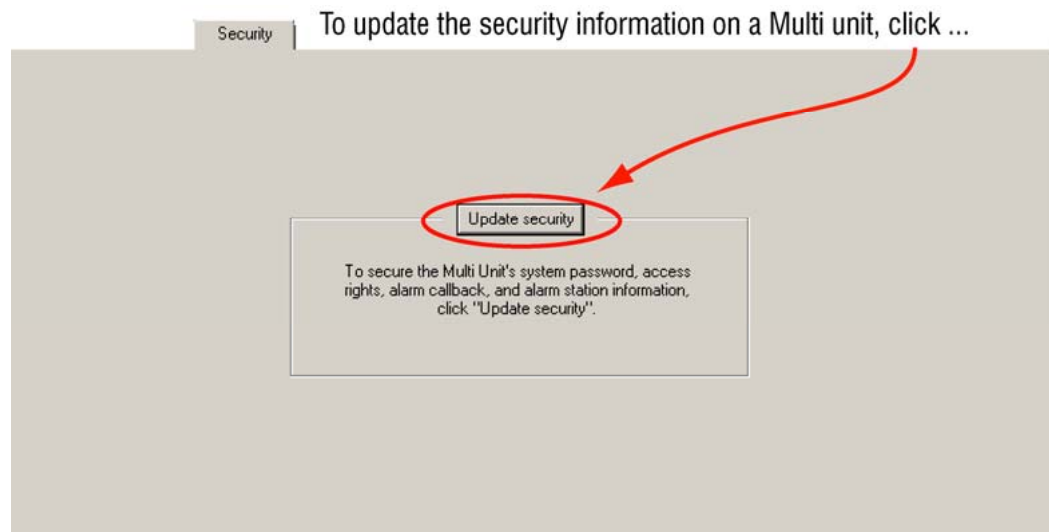


## Road Map to Setting the System Password

Setting (or changing) the system password requires four procedures:

- Use Admin to set a system password in the Multi Central database.
- Use View to run a Maintenance Session to a Multi-Media unit and click **Update security** on the Security tab. This copies the system password to the unit. See figure 10-3, below. Repeat this for each unit.
- The password is copied to the local database of View operators as they log on, when they are connected to the Multi Central database. On systems in session 24/7, or for operators who run View on standalone PCs, communicate that a system password has been added, so that View operators can refresh their local database. See Refreshing a Local Database, p. 244.

**Fig. 10-3. Securing a Unit.**



### After setting the system password...

Even Multi technical support cannot access Multi-Media units from a LAN once your system password has been changed.



### Do not use multiple Multi databases.

Using multiple Multi Dbs with different system passwords on the same Multi system is confusing and prone to operator error. A forgotten system password can prevent access to a unit even by Multi technical support. Please manage your Multi system password with care. For Admin's report on the status of your system password, see Status Report, p. 169.

### Always update security on all units

When the system password is changed, perform a Maintenance Session to update the security on each of the units in your Rapid Eye system. This prevents confusion and access problems. For example: when Touring Many Sites, the sites with a system password that differs from the current system password will be skipped over.



### Do not leave older system passwords on some of the Rapid Eye sites in your CCTV system.

### Extra steps in some system password scenarios

After your system is secured with a system password, a Multi SA may need to perform a few extra steps when faced with these tasks:


- Mistakenly deleting a site definition. To re-enter it, see Last Valid Password, on p. 174.
- Adding a used Multi-Media unit. If you obtain a unit from another organization, and it is protected by that organization's system password. See Last Valid Password.
- Removing a system password from a single Multi-Media unit. This is useful when disposing of a unit. See Removing a System Password, on p. 169.
- Replacing a Multi-Media unit. Should you need to replace a unit with a factory-issued unit. See Replacing a Unit, p. 172.




**When adding a brand new Multi site to your Rapid Eye system, do not use the "LVP" (last valid password) utility, even if you have set a system password.**

The LVP utility is for dealing with used or replacement Multi-Media units, and for mistakenly deleted site definitions, as explained in Last Valid Password, on p. 174.

## Changing the System Password, Part 1 (of 3): Using Admin

1. Run Admin to access the System Password box. Either:
  - Click  on the Admin toolbar.
  - Click the System Password command on the File menu.
  - or -
  - Press the F8 key.
2. Type a password in the System Password box, as shown in figure 10-2. A double-quote (") character cannot be used.
3. Retype the password in the Confirm Password box.
4. Click **Save and Close** to set the system password.

## Changing System Password, Part 2: Multi-Media Units

1. Using View, start a Maintenance Session for a site that is designated for a system password change. Either:
  - Right-click the site name (on the Site tab) to select [Maintenance] from the shortcut menu.
  - Select the site; then click the Maintenance command on the Actions menu.
  - Select the site; then click  on the toolbar.
2. Click the Security tab in the Maintenance window.
3. To update the site's security with the Multi Central database, click **Update security** on the Security tab. You have the option of checking the status of the site's system password, reported in Admin. See table 10-2 on p. 169.



4. You have the option of ending the Maintenance Session, as explained in Ending Maintenance on p. 62.
5. Repeat steps 1 to 4 for each Multi-Media unit in your system.

## Changing System Password, Part 3: Updating Users

The Multi SA needs to tell View operators who are logged on, to refresh their copy of the Multi db, or they will not be able to connect to Rapid Eye sites. See Refreshing a Local Database, on p. 244. Note that only users logged on 24/7 to View need to be warned of this. The refresh is automatic as users log on to View.

## Status Report

### System password and security status

After changing the System password and synchronizing security at your sites, the Admin Sites tab reports a "yes" in the Secure column of each site's line. For other values, see table 10–2.

**Table 10–2 System Password: Status**

Value	Action	Meaning and Recommended Action Details
No	needed	The worst report in a high security environment. The site is not secure from unauthorized users. Honeywell recommends that you assign a system password immediately and update security on the unit. See System Password, on p. 166.
No; set	needed	The site is not secure from unauthorized users. A system password has been set, using Admin but security at the site has not been updated. Run a Maintenance Session at the site and update security.
Yes; set	needed	The site is secure, but with another, older System password. "Yes" it is protected with an old password however you should "set" the site to the new password. Run a Maintenance Session and update security.
Yes	none needed	The optimal report. The site is secure from unauthorized users. The latest System password is in effect.

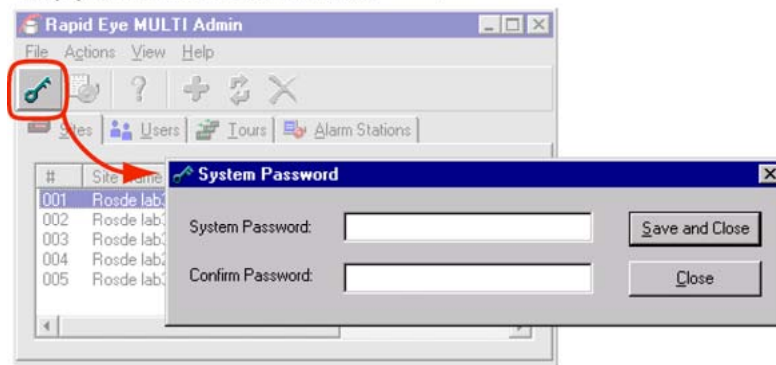
## Removing a System Password

You can remove a system password from either:



- All of your units globally. If your Rapid Eye system consists of a single Multi-Media unit, you can use this procedure too.
- Only one of many units. To remove a system password from a unit that needs servicing, while leaving it on other units in your system, see Removing a System Password, on p. 169.

**Fig. 10-4. After Removing a System Password.**

To start the removal of the system password on the Multi-Media units, empty the boxes of all asterisks " \* ".



## Remove From All Units

1. Run Admin to access the System Password window. Either:
  - Click  on the Admin toolbar.
  - Click the System Password command on the File menu.
  - Press the F8 key.
2. Remove the password in the System Password box.
3. Remove the password in the Confirm Password box; the System Password window should look like fig. 10-4, above.
4. Click **Save and Close**.
5. Using View, start a Maintenance Session for a site. Either:
  - Right-click the site name (on the Site tab); select Maintenance from the menu.
  - Select the site; then click the Maintenance command on the Actions menu.
6. Select the site; then click  on the toolbar.
7. Click the Security tab in the Maintenance window.
8. Click **Update security** on the Security tab. You have the option of Ending Maintenance; see p. 62.
9. Repeat steps 5 to 7 for each Multi-Media unit in your system.
10. The Multi SA needs to tell users who use the sites whose System password has been changed, to refresh their copy of the Multi db, the next time that they use View. See Refreshing a Local Database, on p. 244.

## Remove on One of Many Units



You may need to remove a system password from only one unit in your system, when:

- Selling the unit to another organization
- Sending the unit to Honeywell for repair

This procedure is one of the longest in this *System Administrator's Guide*. Please proceed with caution.

### Tip

**If there is only one Multi-Media unit used by your organization, do not use the following procedure. Please use the procedure in section Removing a System Password, p. 169.**

1. Check your Multi SA's password records to find out what is the current system password on your Multi-Media system. If the password is unknown, use procedure Remove From All Units first (p. 170), to change the system password on all units first.
2. Run Admin, to access the System Password window. Either:
  - Click  on the Admin toolbar.
  - Click the System Password command on the File menu.
  - Press the F8 key.
3. Remove the asterisks in the System Password box.
4. Remove the asterisks in the Confirm Password box; the two boxes in the System Password window should be empty; see fig. 10-4, above.
5. Click **Save and Close**.
6. Using View, start a Maintenance Session for site(s) from which you want to remove the system password. Either:
  - Right-click the site name (on the Site tab) to select Maintenance from the shortcut menu.
  - Select the site; click the Maintenance command on the Actions menu.
  - Select the site; then click  on the toolbar.
7. Click the Security tab in the Maintenance window.
8. Click **Update security** on the Security tab.
9. End the Maintenance Session; see Ending Maintenance, p. 62.
10. You have the option of powering down the Multi-Media unit and disconnecting it from your network or its telephone line.
11. Run Admin to access the System Password window.
12. Type the system password used earlier in the System Password box (the password that was removed in step 1 of this procedure).
13. Retype the password in the Confirm Password box.
14. Click **Save and Close**.
15. To follow-up:
  - The Multi SA may need to tell some users that they need to refresh their copy of the Multi db. See Refreshing a Local Database, on p. 244.
  - You have the option of deleting the site in the site list, as explained at Removing a Site, on p. 28.

## System Password Extras

### Older system password

If you do not know the system password at a site, you will run into some difficulty using the procedure "Remove on One of Many Units" in Removing a System Password, on p. 169. Table 10-2 on p. 169, shows that reports of "Yes; set." or "No; set." indicate that the system password on the unit is not current.

If a unit reports "Yes; set." or "No; set.", run a Maintenance Session to update security on the unit, as explained in Updating Security on a Multi-Media Unit, on p. 131; or in part 3 of Changing the System Password, Part 1 (of 3): Using Admin, on p. 168.

### When there are many Multi-Media units in a Rapid Eye system

What you want to avoid when there are many Multi-Media units in your Rapid Eye system, is to avoid changing the system password then updating security on only a few units. Doing so repeatedly, to different unit subsets, serves no security purpose and can lead to unnecessary confusion, should repair or sale of units occur. Changing a system password means you need to update the security on every unit in your Multi db.

### Using another Multi central database

Using other Multi dbs to run your system can be considered only for:

- Troubleshooting new installations before a system password is added
- Databases using identical system passwords.

After a system becomes established and a system password is added to your system, Honeywell does not recommend using many Multi databases.



**Honeywell cannot recommend using many databases for the same unit(s) if the Multi dbs use different system passwords. System passwords should match on all Multi dbs.**

### What to avoid

The warning above means that using the LVP utility to connect to units protected by the system password of in another Multi database is an abuse of system function and could jeopardize your organization's ability to respond to alarms and to requests for video clips/stills. See also High-Security Considerations, on p. 184.

## Replacing a Unit

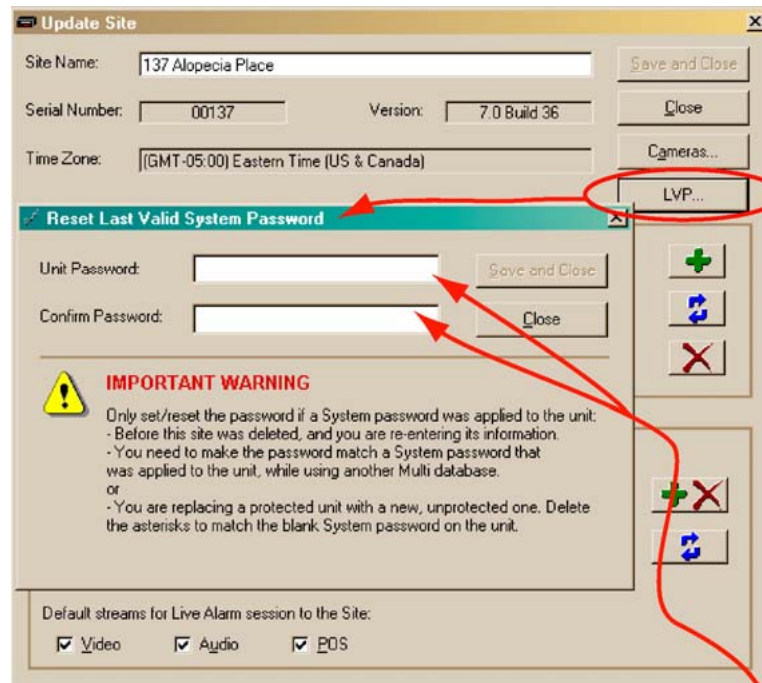
### New unit

When you replace a Multi-Media unit at a site with a fresh, factory unit, the factory unit's "last valid password" (LVP) is blank.

### When a system password is in use: LVP

If you replace a Multi-Media unit and your Multi database is set to a system password (see System Password), you need to use the LVP utility to match the site definition to the blank password on the unit.

Fig. 10-5. The LVP Utility Is Used only when a Unit Replaces another at a Secured Site.



Replacing a unit at a secured site means using the LVP utility. Use the utility to delete the asterisks that represent the system password used at that site.

## To Replace a Unit when a System Password Is in Force

### Tip

This procedure to replace a unit applies only to replacing a unit at a site that has been defined and is operational.

The procedure does not apply to adding a new site to your Multi system. To simply add a site to your system, see Naming / Renaming a Site on p. 24.

1. Check that the Multi-Media unit is powered-up at the site.
2. Using Admin, update the site's definition.
3. Click **LVP** (last valid password). A Match the Password at Unit dialog box appears. Note the asterisks in the Password and Confirm Password boxes.
4. Remove the asterisks from the Confirm Password and Password boxes. See figure 10-5, above. This does not remove your system password from other units.
5. Click **Save and Close**.
6. Using View, start a Maintenance Session for the site.
7. To set the unit to your system password, click the Security tab and update security.
8. Tell any logged on View Operators that they need to refresh the Multi db to use the new site. See Refreshing a Local Database, on p. 244. Occasional users need not worry; their local database is automatically refreshed the next time that they log on to View.

### If the site cannot be accessed

You may have left asterisks behind in the Password and Confirm Password boxes.

## Last Valid Password

### Tip

The scenarios described below are exceptional; they only apply when dealing with re-entry of information in a site definition for used units.

#### Last valid system password

When your Multi-Media system administrator (Multi SA) adds a site definition, the “last valid password” (LVP) entry for that site remains blank in your Multi central database (Multi db). When a system password is added, this database entry is updated along with the unit. There are situations where a discrepancy can occur between the system password held by a unit and the system password entry in the Multi db. An LVP utility is available to resolve the discrepancy.

The LVP utility may need to be used if you:

- Obtain a “used” unit, from another organization’s Multi system. A Multi-Media unit may still be protected by a system password. You may need to contact the other organization’s Multi SA.  
- or -
- Delete a site definition, by mistake. The Multi-Media unit of a mistakenly deleted site definition is (usually) protected by a system password. Please note that, if a site definition is deleted by mistake, but no system password has been set, you can disregard using the LVP when re-entering the site.

The LVP utility enters the last valid password (the password protecting the unit) in the Multi db.

#### Entering a site definition for an “other” unit

If you have obtained a unit from another user and you suspect that the system password on that unit was not removed, use the next procedure.

## If A Used Unit Comes from Another Multi System

1. Create a site definition (see Naming / Renaming a Site on p. 24).
2. Use View to run a Maintenance Session. If an error message is produced, contact the previous owner to obtain the unit’s system password on the previous owner’s system.
3. Having obtained that password, use Admin to update your site definition.
4. Click **LVP** (last valid password). A Match the Password at Unit dialog box appears. See figure 10–6, below.
5. Type the password obtained from the previous owner. For clarity, figure 10–6 shows a one-character password; Honeywell does not recommend using one-character passwords.
6. Confirm the password.
7. Click **Save and Close**.
8. Using View, start a Maintenance Session, to register the site.

#### Failure to run a Maintenance Session

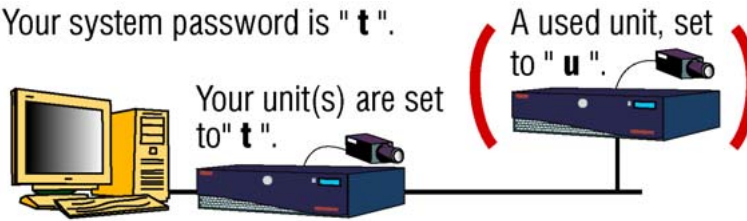
If the site cannot be accessed, you have either:

- Obtained an incorrect system password from the unit’s previous Multi SA/owner.
- Incorrectly typed the password in the LVP utility.
- A Maintenance Session is being run by another user. Try to run a Live Session instead.

If the site is still inaccessible, contact Multi technical support, as explained in For Questions, on p. 22.

**Fig. 10-6. Inputting a Previous Owner's System Password into the LVP Utility.**

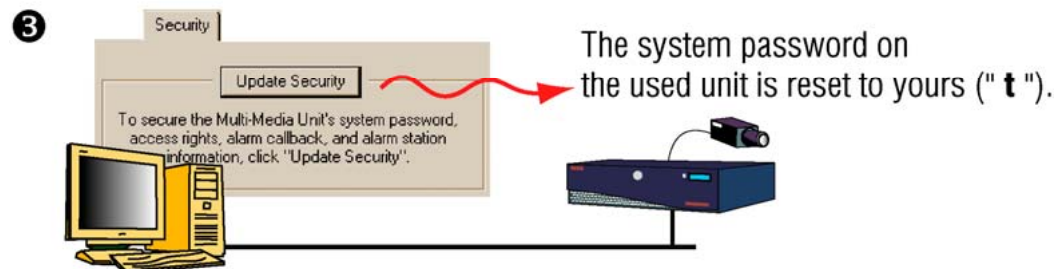
- ① Your system password is "t".



You can introduce a used unit into your organization if you know its system password ("u").



For the **used** unit, use the LVP utility to input the **used** unit's password ("u").



Update the security of the **used** unit, to reset its system password.

## To Re-enter a Site Definition for a Unit with a System Password

### Tip

When a system password is in use and a site is deleted by mistake, you need a few extra steps to re-enter the site definition.

1. While adding a site (see Naming / Renaming a Site on p. 24), click **LVP**. A Match the Password at Unit dialog box appears.
2. Type the system password that was securing the unit.
3. Confirm the password.
4. Click **Save and Close**.

## To Check if the Correct System Password Was Typed

- Use View to start a session. If the site cannot be accessed, you may have mistyped the password in the previous procedure.

## User Password

1. Using Admin, click the Users tab to view the list of users.
2. To update a user's account, double-click the "user name" in the User Name column. The Update User dialog box appears.
3. Type the password in the Password box. A double-quote (") character cannot be used in a password.
4. Retype the password in the Confirm Password box.
5. Click either:
  - **Save and Close.** Updates the user's password.
  - **Close.** Cancels the update. You will be asked to confirm that the changes are to be ignored. Click **OK** on the message.
6. Communicate the password to the user.

### Results

After the Multi SA assigns a password to a Multi-Media unit operator:

- The Password column shows "set" at that user's line.
- A password must be typed at every logon. Typing an illegitimate user ID/password combination produces a message.
- At the first log on to View, a local copy of the Multi Central database is made to the PC running View.
- A user cannot change the password using View. Only users of Admin can change a password.

### User password technical note

A user account password is encrypted in the Multi db. It is a combination of the User ID and password. This ensures a password always exists, even if the Password box is left empty. Thus: accessible, third-party tools such as MS-Access cannot be used to remove the Administrator's password, simply by loading a Multi db. Your system is protected against such elementary database tampering. Defense against criminal techniques, such as social engineering, operator negligence when managing passwords, and so on, are the operator's responsibility.

## Administrator Password

The procedure for adding/changing the Administrator account password is similar to the one for adding/changing another user account's password.

### Tip

**After a successful Multi installation, Honeywell recommends that the Multi SA add/change the "Administrator" user account password.**



### Basic security

Changing the password to the "Administrator" account is an essential security precaution. It should be carefully guarded against loss and changed regularly.

The password protects against:

- The most basic hacking of Admin by unauthorized users
- Adds an important safeguard to prevent inadvertent use of the clear storage feature. For information about this feature, see Clearing Storage, on p. 129.

### Password independence

Accounts that are based on the "Administrator" account are not affected by changes to the "Administrator" user's password (see Default User, on p. 152). Such accounts have their own passwords. Accounts based on the Administrator account can still change the Administrator password (or any other).

## To Set the Administrator Account's Password

1. Using Admin, click the Users tab to view the list of users in the User Name column. You can ignore user names in the Settings Based On column.
2. Double-click "Administrator" in the User Name column. The Update User dialog box appears. Only the password can be changed in the "Administrator" account. The name of the account and its rights cannot be modified.
3. Type the password in the Password box. A double-quote (") character cannot be used in a password.
4. Retype the password in the Confirm Password box.
5. Click either:
  - **Save and Close.** To update the "Administrator" password.
  - **Close.** To cancel the update. You are asked to confirm that the changes are to be ignored. Click **OK**, on the message.

### Results

After the Multi SA assigns a password to the "Administrator" account:

- The Password column shows "set" at the "Administrator" line.
- The password must be typed every time that a user using that account logs on. If that user types a user ID/password combination that is not valid, the user is warned with a message and returned to the logon dialog box.
- The first time that the Administrator account is used to log on to View, a local copy of the Multi Central database is made to the PC running View.

### Sharing the "Administrator" account

When an organization's security needs are limited and Multi software is used by very few people (one or two), you may elect to simply change the password of the "Administrator" account and create no other accounts.

### What you want to avoid

The locking out of authorized, legitimate users from the Multi-Media units on your Rapid Eye system is a worst-case scenario that requires many crucial steps, one of which is: knowing the password to the Administrator account. For others, see High-Security Considerations, on p. 184.

## Rights of User Accounts

### Flexibility in security

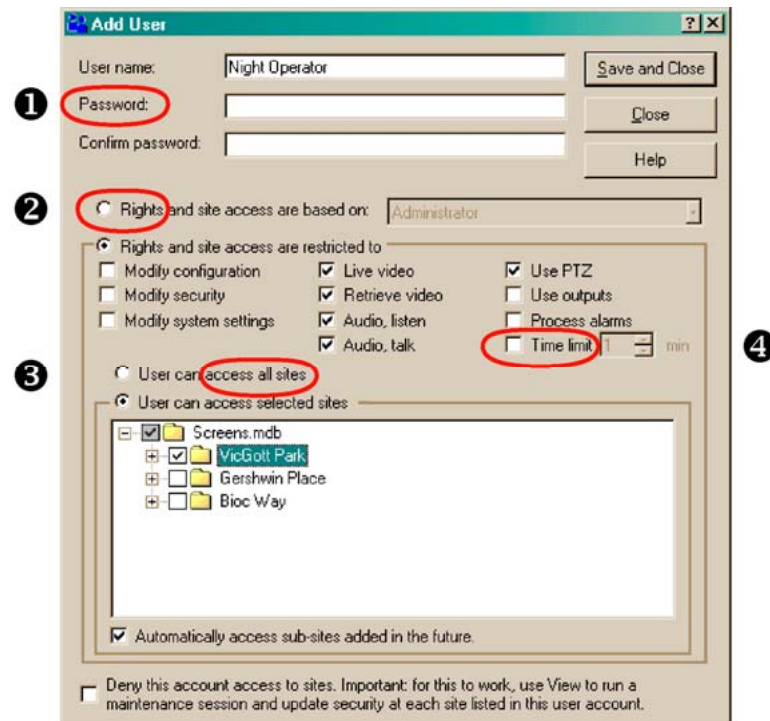
Like most Multi-Media security features, limiting user rights or access to sites is optional.

Admin software is used to set the rights of all user accounts. These rights apply to:

- Admin
- Maintenance
- View

Your Multi system administrator also defines the sites that a user is authorized to use including the amount of time that can be spent using sites.

Fig. 10-7. Assigning Rights to a “Night Operator” Multi-Media Account.



## Guidelines

A Multi account can have as few or as many rights, as needed.

## To View the Rights of a User and the Sites He may Access

1. Using Admin, click the User tab.
2. Double-click a user's line. The Update User dialog box appears, showing the rights defined by the account.

### Assigning rights when adding / updating accounts

The rights are assigned in a single location: when adding or updating a user account (see Adding an Account, on p. 155). By default, new accounts do not have the "Modify..." rights. The list of rights appears as in figure 10-7.

### Denying access to some sites

By default, a user account can access every site in your system. You can limit the user's access to a subset of the sites.

### Rights of users based on others

Optionally, you can base other user accounts on any other. The rights of all such users can then be modified.

Alternatively, a user account can be based on the "Administrator" account. This grants all rights to that user, including use of Admin.

### Removing rights

When a right is denied, the Multi function associated to it is unavailable. The user may log on to View, but commands will be unavailable or disabled. Rights apply only to sites that a user has been authorized to use.

Fig. 10-8. Summary of a User's Rights on the Users Tab.

#	User Name	Password	Rights	All Sites	Settings Based On
001	Administrator	(set)	yyy yyy yyy	Yes	(self)
008	security chief	(set)	yy yyy yyy	Yes	Administrator
003	security consultant	(not set)	rn yynn nnn	Yes	(self)
002	weekday shift operator	(not set)	nnn yyy yyy	Yes	(self)
004	weeknight supervisor	(not set)	yny yyy yyy	Yes	(self)
005	weeknight shift operator	(not set)	nnn yyy yyy	Yes	(self)
006	weekend supervisor	(set)	yny yyy yyy	Yes	weeknight supervisor
007	weekend operator - night or day	(not set)	nnn yyy yyy	Yes	(self)

### Sharing accounts

When an organization's security needs are limited and Multi software is used by a very small number of people, your Multi SA may elect to create one account and share it among users.

## Right to Use Admin

To use Admin, your account must be the “Administrator” account, or an account based on it.

### Tip

**The set of rights in an account based on the “Administrator” account cannot be modified; only the password can.**

## To Grant Access to Admin

1. View the rights of a user’s account.
2. Click **Rights and site access are based on:**.
3. In the box next to Rights and site access are based on:, select “Administrator”.
4. Click **Save and Close**.

### Tip

**Why limit the use of Admin?**

- (a) The “Administrator” account has all user rights to all functions of View, and to every site identified in your Multi db. With such an account, a malevolent user can quickly disable your system or cover up unwarranted or illicit actions, such as deleting items in the alarm log.
- (b) The Admin disc is used to install the user documents for Admin and the Multi-Media unit. This information may exceed an operator’s need to know about your Multi system.
- (c) Users of the “Administrator” account can remove an important safeguard to prevent inadvertent use of the Clear storage feature. See Clearing Storage, on p.129.

## Right to Use Maintenance

Each of these rights are sensitive for security. Each of these rights gives access only to portions of a Maintenance Session; see table 10–3. You can start a Maintenance Session in View with any one of these three rights; which tabs appear differ.

- **Modify configuration.** Gives access to the tabs for making hardware configuration settings. These rights can be sensitive in a Multi system. A user can turn recording off or set an NTSC system to “PAL”, jeopardizing the unit’s ability to record video.
- **Modify security.** Gives access to the Security tab. User has the right to click **Update security**.
- **Modify system settings.** Gives access to the Statistics and System tabs. These rights can be sensitive in a Multi system. A user can destroy all of the video and audio stored in a Multi-Media unit by clicking **Clear Storage** on the Statistics tab; see Clearing Storage, on p. 129. It also controls the rebooting of Multi-Media units and upgrading files to a Multi-Media unit.



**Your security officer and Multi SA must exercise vigilance if operators have accounts with enough rights to jeopardize the operation of a Rapid Eye unit.**

Table 10–3 Maintenance Tasks and Rights of a User Account

Right† Needed	Task	See...	Page
Modify configuration	Time	Unit's Time Zone and Clock	56
	System configuration	System Tab in a Maintenance Session	134
	Video; includes: picture, motion, PTZ and AGC	Cameras	65
	Serial devices	Customer Data and Customer-Device Events	143
	Eagle Audio	Eagle Audio	149
	Hardware	Hardware Report	140
	Audio	Multi Audio	147
	Public display monitor	Public Display Monitor: Using Monitor Output 1	141
	Events	Events Defined	187
	Recording Schedule	Scheduling: Configuration	105
Alarm Schedule	Alarms and Scheduling	109	
Modify security	Security	Maintenance Reference	62
Modify system settings	Statistics	A Multi-Media Unit's Storage Statistics	127
	Clearing storage	Clearing Storage	129
	System files	System Files	132

† The Administrator account has all rights, including these three.

## Tip

### Why limit the use of maintenance?

Operator error. Misuse of a Maintenance Session can lead to a complete loss of recorded video, the compromise of the system's ability to record video by disabling cameras, or the turning off of alarm reporting. See the sections listed in table 10–3: Maintenance Tasks, above.

## Right to Use View

Each function of View (excluding Maintenance) is subject to one of five rights. The most sensitive rights for security are marked with an asterisk (\*).

- Live video. Right to obtain a live video feed from cameras at a site. This is a Multi system's fundamental purpose. All Multi user accounts usually have this right. The amount of cameras that a user can access may be limited. See To Limit Use of Cameras: Camera Partitioning.
- Retrieve video. Right to obtain a video feed of recorded video. Also grants use of the "search for Events" feature.
- Audio, listen. Right to hear through a site's sound hardware.
- Audio, talk. Right to broadcast through a site's sound hardware.
- Use PTZ. Right to operate the pan, tilt and zoom (PTZ) commands, on cameras that have this capability, during a Live Session. Use of this right depends on the right to View Live Video.

- \* Use outputs. Right to operate outputs (for controlling gates, lights and other facilities), during a Live Session. Use of this right depends on the right to View Live Video.
- \* Process alarms. Right to respond to alarms: using an alarm session to acknowledge and to reset alarms.
- Time limit. Right to make use of sites for a limited amount of time.

## Tip


### Why limit the use of View?

This depends on your organization's security protocols. Should perhaps an operator only be allowed to monitor live video and not to view recorded video? Should use of an output to open a gate need to be monitored/controlled?

## Right to Access a Site

A user account grants site access to either all sites or a subset of the sites in your Rapid Eye Multi system. Rights to access sites are modified while adding or updating an account, as explained in the next procedure. See also Adding an Account, p. 155.

## To Define an Account's Access to Certain Sites

1. Using Admin, click the Users tab.
2. To display the Update User dialog box, do one of the following:
  - Double-click the name of the user account that you want to update.
  - or -
  - Select the user account that you want to update; then: click either:  on the toolbar, **Update** on the Actions menu, or press the F12 key.
3. In the Update User dialog box, either:
  - Click User has restricted access.
  - or -
  - Leave User can access all sites; then skip to step 6.
4. In the tree of sites below User has restricted access, select one or many sites by clicking the boxes next to names of sites, so that a checkmark appears. The checkmark means that access to the site is granted to the user of the account.
5. Click **Save and Close**.
6. Update security at each site listed in the Denied from accessing list. The procedure to update security is in section Updating Security on a Multi-Media Unit, on p. 131.

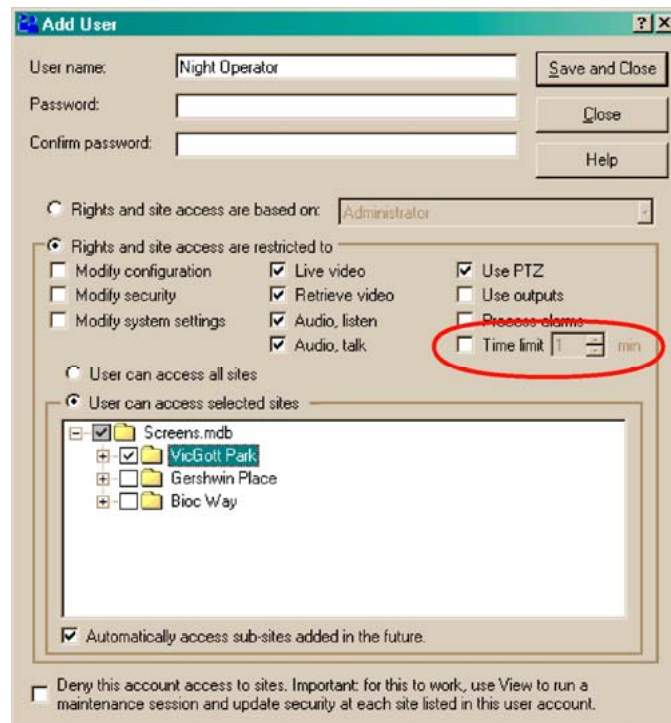
## Tip

### Why deny or limit access to a site?

This depends on your organization's security protocols. An operator might be allowed to monitor only some sites, and so on.

## Limiting the Time that a Unit Can Be Used

Fig. 10–9. Account's Limit on Session Time, before Needing to Reconnect.



Limiting time can be used to prevent users from monopolizing a Rapid Eye site's maintenance. See figure 10–9, above.


## To Limit Use of Cameras: Camera Partitioning

You can disallow access to some or all cameras at a site. By default, a user account can use every camera at a site.

### Tip

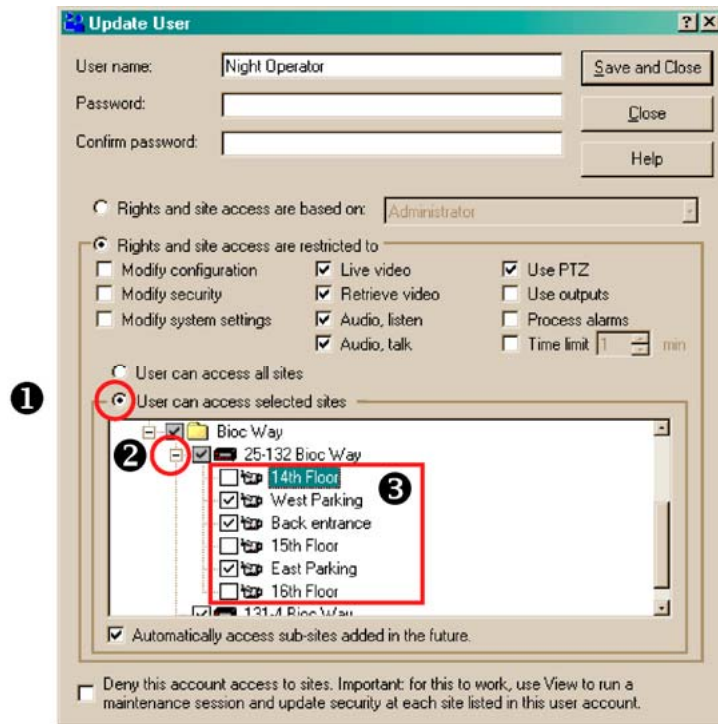
**Why deny access to a camera? This depends on your organization's security protocols. Perhaps an operator should monitor some cameras and not others.**

You need to have configured cameras at a site before you can limit their use in a user's account. To configure cameras, see Cameras, on p. 65.

1. Using Admin, click the Users tab.
2. Display the Update User dialog box by either:
  - Double-clicking the name of the user account that you want to update.
  - or -
  - Selecting the user account that you want to update; then: click either:  on the toolbar, **Update** on the Actions menu, or press the F12 key.
3. In the Update User dialog box, click **User has restricted access**. See figure 10–10, (1).
4. In the tree of sites below User has restricted access, select a site by clicking the box next to name of the site, so that a checkmark appears. The checkmark means that access to the site is granted to the user of the account.

5. Expand the site, as in figure 10–10, (2). In the branch of cameras below the name of a site, select one or many cameras. A checkmark means that access to the camera is granted to the user of the account. See figure 10–10 (3).
6. Click **Save and Close**.

**Fig. 10–10. Limiting an Account’s Use of Cameras at a Site.**



## High-Security Considerations

### Preventive measures: a short checklist

A Multi-Media unit can be set so that performance or security are compromised. To reduce the probability of this, Honeywell recommends that your Multi SA and your security officer check for situations such as the ones in table 10–4.

### Physical compromise

As obvious as such acts may seem, they include:

- Vandalism to Multi-Media units or other hardware. See also Camera Sabotage: Detection, p. 120.
- Power outages beyond the range of a UPS.
- Placing cameras where direct sunlight, dew, frost or reflections can hamper visibility.
- Placing cameras at an outside window, in a room that remains lit during evenings. Reflection from the window can hamper visibility outside.
- Placing objects to obstruct a camera’s view. See also Camera Sabotage: Detection, p. 120.



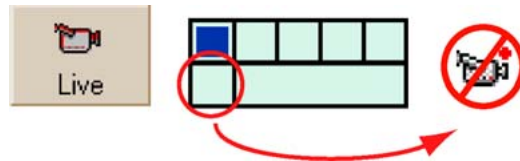
Table 10–4 Security Happenstance

Situation	Preventive and / or Last Resort Measures
vandalism	<ul style="list-style-type: none"> <li>- schedule onsite equipment inspections</li> <li>- use access control to access Multi-Media units at sites</li> </ul>
vandalism or operator error	<ul style="list-style-type: none"> <li>- schedule regular connections to each Multi-Media unit in your security system</li> </ul>
using many Multi databases	<ul style="list-style-type: none"> <li>- through training, discourage the use of many Multi dbs; using more than one db, using different system passwords, is beyond the product's design and deemed unsafe.</li> <li>- as a last resort, use the last valid password utility, as explained in Last Valid Password on p. 174.</li> </ul>
breach of trust	<ul style="list-style-type: none"> <li>- refrain from communicating a system password to a Multi SA running another Rapid Eye system</li> <li>- ask security personnel to exercise vigilance if operators have accounts with enough rights to jeopardize the data on a Multi-Media unit</li> <li>- as a last resort, contact Multi technical support for help, as explained in For Questions on p. 22.</li> </ul>

### Compromising video recording

**Setting the Recording of a camera to OFF.** Video is not recorded when Recording is turned OFF. This is easy to detect: each camera shows a recording meter during a Live Session. See figure 10–11.

Fig. 10–11. Identifying a Camera that is Not Recording, in a Live Session.



If a corrupt operator turns Recording to OFF, Live would still work but no recording would be available. Such abuse can be traced, as explained in Tracing Events, below. See also Cameras, on p. 65.

**Camera brightness.** Video may be compromised when the brightness setting on a camera is set too high or too low. Your PTZ cameras may be installed in a way that they can be turned away from the sun. See the *Rapid Eye View Software Operator Guide*.

**Resetting the time/date.** It can become complicated to analyze video “footage” after the time and date of a Rapid Eye unit is changed recklessly. Recordings with incorrect time and date stamps could be of no use to a court of law. You can trace events leading to such abuse, as explained below, in Tracing Events. See also Unit's Time Zone and Clock, on p. 56.

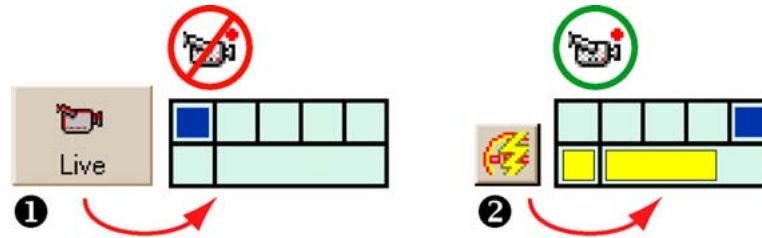
**Scheduling cameras to not record.** See Scheduling: Configuration, p. 105. This feature is designed to spare storage. It can be abused to defeat security. Use of the Boost button overrides a turned OFF recording setting for video. See figure 10–12.

### Countermeasures

.An effective countermeasure strategy includes Camera Sabotage: Detection and scheduling short Retrieval sessions on all cameras to spotcheck that Rapid Eye sites are recording as expected. One can also check if the environment has diminished the effectiveness of a site. Verification can

supplement tracing of events, as explained in Tracing Events, below. Boosted recording can override a unit to record a video feed from a camera with recording turned OFF. See figure 10–12.

**Fig. 10–12. Overriding a Camera that is not Recording, Using Event Recording.**



**Destruction of recorded video and denial of service: clearing storage**

Clearing a unit’s storage or one of its streams destroys all recorded video and, during the time that a unit is emptied (up to a few hours; see Clearing Storage, on p. 129), a Multi-Media unit cannot show live video, record video, nor send alarms, and so on. To do so requires use of the password to the Administrator account.



**Please train operators of accounts that include the right to use “Clear Storage” or “Clear Stream” buttons.**

**Compromising response to an alarm**

**Scheduling alarms to not trigger.** See Alarms and Scheduling, p. 109. This feature is designed to control some obvious false alarms. It can be abused to defeat security.

**Using more than one Multi db.** Using a database “A” set to “system password A” with the LVP utility, to create a site definition for units protected by “system password B”, can lead to much confusion if that user were to update security on the unit. The LVP utility does not change the system password on the unit; updating security does. Updating security with another “A” system password locks out all other View Operators who attempt to log on (using their usual “B” database), thus jeopardizing their ability to respond to alarms and to requests for video clips/stills.



**Honeywell does not recommend using many databases even if they are set to the same system passwords.**

**Compromising and locking-out a Multi SA**

The locking out of authorized, legitimate users from the Multi-Media units on your Rapid Eye system, including the Multi SA, is a worst-case scenario for high-security organizations. Many steps are needed by an instigator: obtaining copies of Admin and View software, creating another database, having knowledge of your system password. Even access to your Multi Central database, knowledge of Admin and of the Administrator account’s password could allow a malevolent user to change passwords to the Administrator’s account, to the system; then update security on units, locking everyone out. “Need to know” and access control are your best assets.

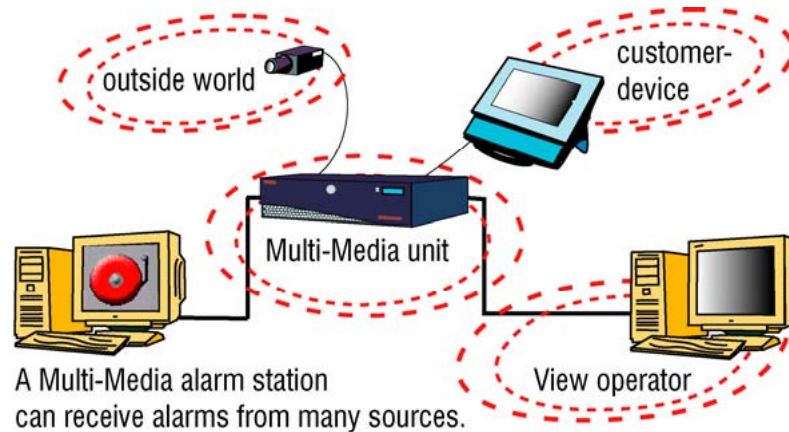
**Countermeasures.** If ever such a breach of trust occurs, contact Multi technical support for help, as explained in For Questions on p. 22.

**LocalView**

Another case of breach-of-trust can occur through LocalView, which can be used to change a unit’s LAN communication settings.

## Events Defined

Fig. 10-13. Sources of Events Include the Unit itself.



Multi-Media units provide notification of events. Events can be produced from four sources:

- *Outside World* event. Rapid Eye's Motion Detection in video, p. 116, and Camera Sabotage: Detection, p. 120. can trigger alarms. Connecting a unit to sensors for fire, water and so on, can also manage such events.
- *Customer-device* event. Messages from a cash register, card swipe and so on, that can be sent to a Multi-Media unit. See Customer Data and Customer-Device Events. p. 143.
- *Multi-Media Unit* event. For notification a Multi SA of events at the unit or from some events from to the IT environment. Extended power outages can also be monitored by connecting a Multi-Media unit to an alarm panel. See Tracing Events, on p. 191.
- *View Operator* event. An administrator can trace events caused by View operators, such as use of a site, and so on. Notification of such events usually matters more than video. See Tracing Events, on p. 191.

## Setting an Event to Trigger an Alarm or to Be Logged

### Preferences

When events occur, they can be acted upon in the following ways:

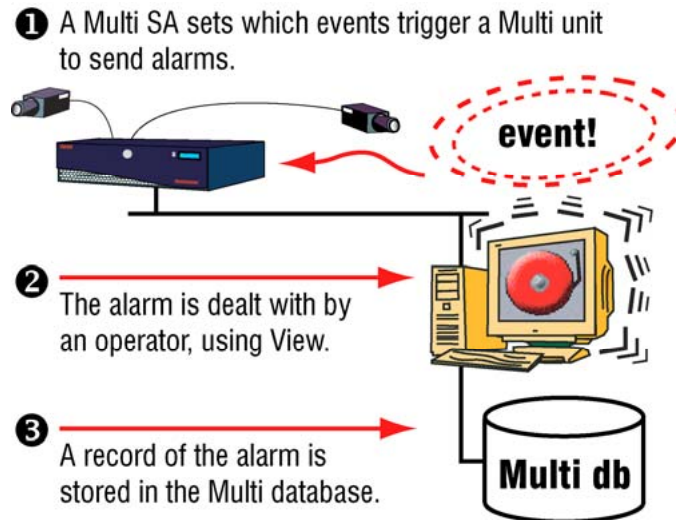
- **Logged.** The Multi-Media unit logs the time of the event. These events are not listed in an alarm session. See fig. 10-15.
- **Sound an alarm in View.** Alarms reach View operators either through an alarm station or during an alarm session. They are stored in the Multi db. See figure 10-14.
- **Do both.** An event can sound an alarm and be logged.
- **Have no effect.** This is the default setting for most events. For the events that are logged by default, see table 10-6, p. 191. Even when alarm hardware is connected to a Multi-Media unit, an event is ignored until View is used to set it to trigger an alarm, to be logged or both.

## Setting an Alarm

### Default

By default, events are not set to trigger alarms. Setting events to trigger alarms is an option. Alternatively, events can be silently logged, for administrative purposes.

**Fig. 10-14. Once Acknowledged, Alarms Are Entered into the Multi Db.**



## To Set an Event to Report an Alarm

1. Start a Maintenance Session for the Rapid Eye site. Please wait until the "System Operational" message appears.
2. Depending on the type of event that you want to set, either:
  - Click the Events tab. More tabs appear. Select a smaller tab (Session, System, and so on) that lists the event that is to be set as an alarm.
  - Click the Serial Devices tab. Select a device and one of its events.
  - Click the Video tab. For Motion detection settings, see Motion Detection, p. 116.
3. To set the event to trigger an alarm, click the Alarm checkbox next to the event, so that it shows a checkmark. For a Customer-device event, on the Serial Devices tab, click **Update** after clicking an Alarm or Log checkbox.
4. You have the option of having the event also entered into the log. To do so, click the Log checkbox so that it shows a checkmark.

### Who can set alarms?

## Tip

**To set alarms, two items must be part of the user's account:**

the "Modify configuration" right and access to the site.

To arm/disarm alarms, or that an event should be logged or ignored, a View operator needs user account with: the Modify configuration right and access to the site(s).

The Modify configuration right enables the operator to start a Maintenance Session and use a site's:

- Event tab
- Serial Devices tab
- Video tab, for Motion

#### Who can receive alarms?

A different right is needed to use an Alarm session. A View operator needs a Multi SA to:

- Add the Process alarms right to the operator's user account. This enables a View operator to: receive, view, acknowledge and rearm alarms. See Right to Use Maintenance, on p. 180.
- Grant access to site(s) to operator(s).

## Logging an Event

Fig. 10–15. A Multi-Media Unit Can Log an Event without Sounding an Alarm.

- ➊ After you set an event to be "logged", a log entry is made *on the Multi unit*, each time that the event occurs.



- ➋ To list the log's entries, use View's "Event Search".

1. Start a Maintenance Session for the Rapid Eye site. Please wait until the "System Operational" message appears.
2. Depending on the type of event that you want to set, either:
  - Click the Events tab. More tabs appear; see table 10–5: Event Reference, by Source and Tab, p. 190. Select the smaller tab (Session, System, and so on) that lists the event that is to be set as an alarm.
  - Click the Serial Devices tab. Select a device and one of its events.
  - Click the Video tab; then Motion. For Motion detection settings, see Motion Detection, on p. 116.
3. To set the event to enter an item in the event log, click the Log checkbox next to the event, so that it shows a checkmark.
  - Inputs can be additionally configured as either NO, NC or EOL.
  - For a Customer-device event, you must also click **Update** after clicking the Log checkbox.

## Event Reference

**Table 10–5 Event Reference, by Source and Tab**

Source	Event in Maintenance, Except Where Noted	Cause: an Alarm or Log Entry Could Indicate ...
<i>Outside World event</i>	System: no video recording*	a cut cable, dead camera, power outage
	Inputs: activate, input ports 1 to 16	security sensor has been triggered or the Multi-Media unit is booting
	Inputs: deactivate, input ports 1 to 16	security sensor has been reset or the unit is booting
	Video: signal unlock, cameras 1 to 16	cut cable, hardware failure in a Rapid Eye Multi Multi-Media unit, faulty camera... Can be momentary.
	Video: lock <sup>†</sup> , cameras 1 to 16	a buggy camera; time since video unlock helps troubleshooting
	Motion: On the Video tab (not on the Event tab).	intruder, a change in lighting, fire, an explosion, vermin, and so on.
	Camera Sabotage Detection: On the Video tab (not on the Event tab).	tampering with a camera.
<i>Customer-device event</i>	user defined: Not on Event tab; on Serial Devices tab.	transaction made using hardware at a customer's facility
<i>View Operator event</i>	Session: connect, reject and disconnect	use/misuse of View to connect to or disconnect from a site.
	Maintenance: changes to configuration, security, time, storage and so on... <sup>‡</sup>	use/misuse of Clear storage or Synchronize time by operator or Multi SA
	Outputs: activate, output ports 1 to 8	use/misuse of an onsite device by a View operator ex.: locking a gate at a site, by remote control
	Outputs: deactivate, output ports 1 to 8	use/misuse of an onsite device by a View operator. ex.: unlocking a gate at a site, by remote control
	System: no video recording*	camera disabled by View operator
<i>Multi-Media Unit event</i>	System: reboot	use/misuse of Reboot command
	System: failure, self-restart, reboot <sup>†</sup>	power failure or catastrophic failure of unit
	System: No video recording*	failure of unit's video hardware
	System: time server, no synch, clock drift...	failure of network or network's time server
	System: disk failure	warning of imminent failure of storage

\* Some events are repeated in the table: their source can vary. For example: an alarm triggered by an "Outside World event" can also be triggered by rebooting a unit.

† A Multi SA can set a Video lock event to be only logged rather than trigger an alarm.

‡ Some configuration settings can be changed onsite, using LocalView. These changes are not logged nor do they trigger an alarm when the configuration event is set to do so.

Table 10–6 Event: Default Settings for Log and Alarm

Source	Event	Log	Alarm
<i>View Operator</i> event	Session: connect, reject and disconnect	off	off
	Maintenance: configuration, security, system files, synchronize time, clear storage, clear stream	All are logged; logging cannot be disabled.	"
	Outputs: activate, deactivate*	off	"
<i>Multi-Media Unit</i> event	System: run-time failure, self-restart, reboot, no video recording, time server unusable, no synchronization in 24 hours, excessive system clock drift, SMART disk failure	All are logged; logging cannot be disabled.	"
<i>Outside World</i> event	Inputs: activate, deactivate	off	"
	Video: signal unlock, signal unlock	"	"
	Motion: Not on Event tab; on the Video tab.	"	"
	Camera Sabotage Detection: On the Video tab (not on the Event tab).	"	"
<i>Customer-device</i> event	user defined: Not on Event tab; on the Serial Devices tab.	"	"

\* Control Output 6 is unavailable as an event, due to its use by the Fault Relay. On a Multi-Media LT unit, the Fault Relay does not make use of a control output.

## Tracing Events

### Flexibility in security

Like most of the Multi-Media security features, tracing events caused by a View Operator event or by your Multi-Media Unit event is optional. You can set a site to produce an alarm if these occur. Alarms can be sent to specific PCs. See Multi-Media Alarm Stations, on p. 201. Tracing these events is performed on a site-by-site basis.

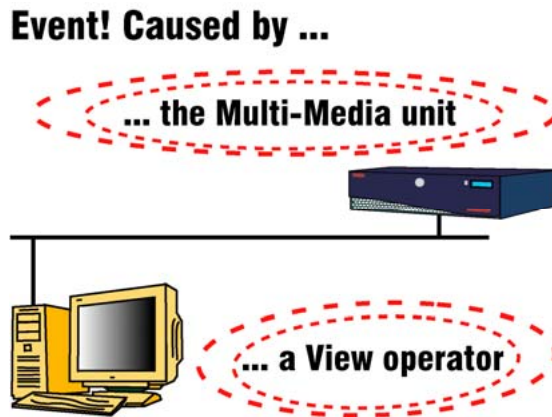
### Why trace events by View Operator events or the Multi-Media Unit event?

When you suspect that: natural causes, operator error or misuse of your Multi system may be compromising the effectiveness of a Rapid Eye site, you can trace a View Operator event or a Multi-Media Unit event.

Use tracing to monitor:

- **Power outages.** A site that regularly reboots, or that has long gaps in its recorded video archive can be monitored.
- **A breach to site security.** You can be warned about some damage, vandalism or destruction to a Rapid Eye site, due to hurricanes, fire or criminal activity.
- **Operator error.** Tracking critical operator actions that result in missing video images, can help when unidentified problems start occurring and you suspect operator error.

Fig. 10-16. Events Caused by a Multi-Media Unit or a View Operator.



#### Who can trace a Multi-Media Unit event or a View Operator event?

By using the "Administrator" account or an account based on it, your Multi SA automatically has the Modify configuration right, to record or report these or other events.

To authorize other users to do so, the Multi SA can add the Modify configuration right to their user account. With this right, you can:

- Start a Maintenance Session at a site
- Set events: to be logged, trigger alarms or be ignored, as needed
- Arm/disarm alarms.

#### Common sense

Your security officer can advise you on checking first for a technical alibi: a user account may not have the right to cause an event.

#### Event log

A Multi-Media Unit event is always logged, to easily troubleshoot your system, as needed. Use an Event Search session to search the event log.

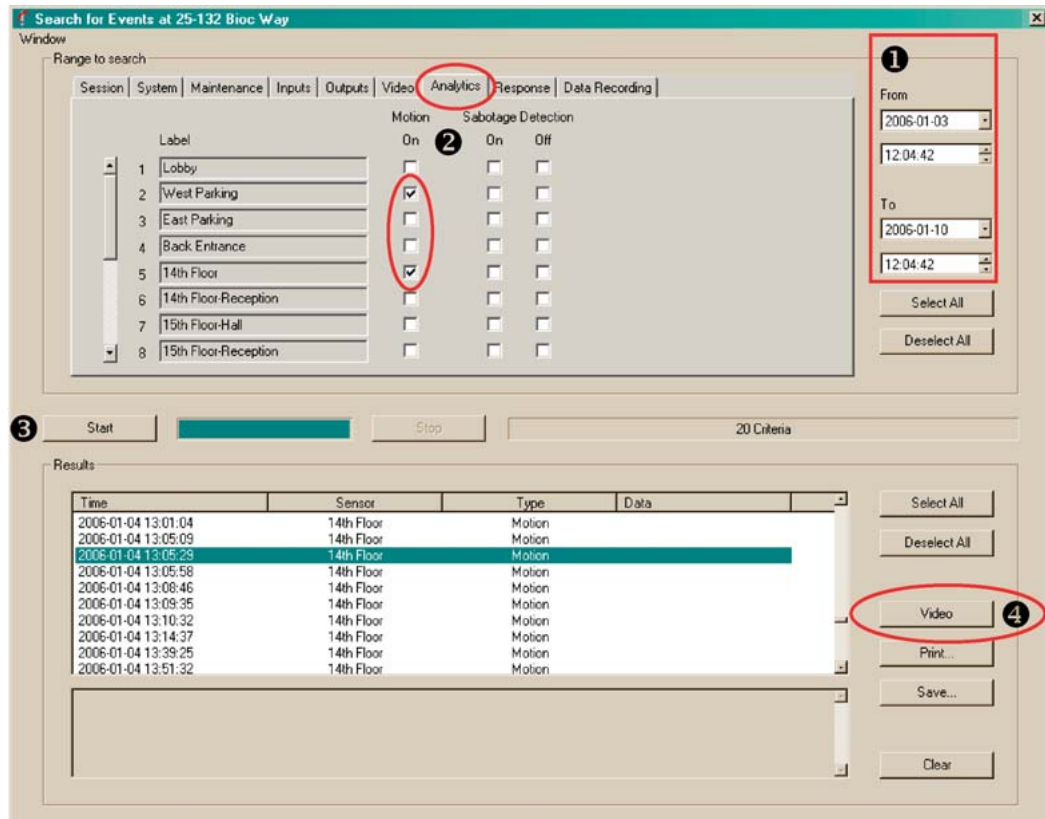



## Event Session: to Search the Log of Events

### Preparation

By default, some events are not logged; no events are set to trigger alarms. To obtain positive results from an Event session, your organization's Multi SA needs to set events to be logged or to trigger an alarm. See Logging an Event, p. 189.

Fig. 10–17. Search for Events Window.



1. Select a site in the Sites tab.
2. Display the Events window by clicking  on the Toolbar.
3. Select events that you want to search for by: clicking an event tab (see figure 10–17; “Motion” is selected) and selecting events.
4. Enter a date and time in the **From** and **To** boxes. Use of these boxes is explained in the next procedures.
5. Click **Start** to search.
6. In the Results pane, select an item.
7. To obtain video from the time of the item, click **Video**. For context, video starts five-seconds before the time of the event.



**The Start Search button is unavailable until dates and times differ in From or To.**

## To Input Times and Dates

Click on the part of the time or date that you want to change and either:

- Press cursor keys on the keyboard. The → ← keys move the cursor to the next field, and the ↑ ↓ keys increase/decrease a value.
- or -
- Type a value, as needed.

## To Set the Date of a Retrieval Using the Calendar Utility

1. In the Stream List dialog box, display the calendar utility by clicking the arrow next to the date box.
2. Click a date in the calendar. To go to another month, click the arrow keys next to the month/year heading in the utility.

**You cannot go beyond the limits of the log**

Attempting to input or select dates or times beyond the limits of the log sets the input to that limit.

## Results

You can use the search results to:

- View video from the time of events located by a search.
- Print the log entry of an event
- Make a copy of the log entry in a \*.txt file.

## To Print a Log Entry

1. After locating records of events, as explained above, in Event Session: to Search the Log of Events, select a record. The Print button becomes available.
2. Click **Print**.
3. Click **OK**. A Font dialog box appears. Select a font. Click **OK**.

## System Failure

A Multi-Media unit can be monitored for:

- Failure to function
- Failure to record video.

You can set the FAULT RELAY to trigger when these failures last nineteen minutes. An alarm panel or other external device can be preset to warn your organization, if failure occurs. A power failure also triggers the relay, but does so immediately.

A system failure is not a Multi event but it can trigger Multi events; see System Monitor on p. 134.

## A Multi-Media Alarm Station

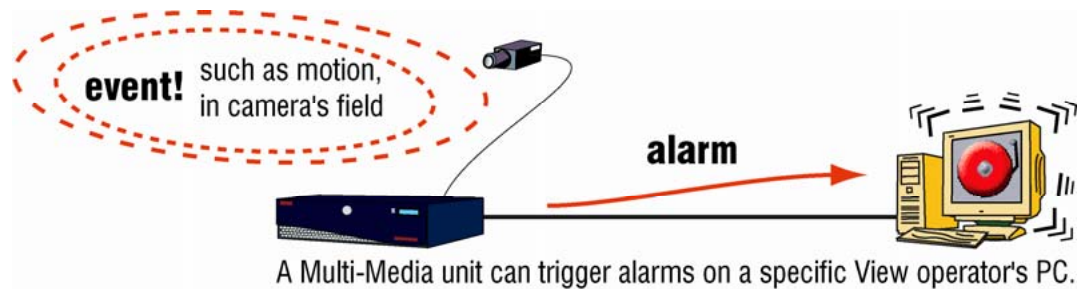
### Flexibility in security

Like most Multi-Media security features, use of an alarm station is optional.

### Purpose

An alarm station is a PC that is designated to receive alarms first, from one or more Multi-Media units. View software needs to run on PCs designated as alarm stations. Their setup is discussed in Multi-Media Alarm Stations, on p. 201. In setting up an alarm station, you might need to obtain some point-to-point connectivity information.

**Fig. 10-18. A Multi-Media Unit Can Be Set to Send Alarms to Specific PCs.**



## Alarm Notification: Response Priority

After making an alarm station operational (see Making an Alarm Station Operational on p. 218), notification of an event's occurrence can be:

- Immediate. When either: (a) Multi-Media units are networked to an alarm station, or (b) by happenstance, you are running an alarm session at the site when and where the alarm occurs, or (c) your PC is setup for Live-alarm sessions and you happen to be connected to the site where the alarm is triggered.
- Within the minute. Your Multi Administrator has set a dial-up Multi-Media unit to "call" an alarm station running View, as soon as possible after an alarm. Should the alarm station be unavailable, an attempt to call it back is made every minute until a connection to the alarm station is established.
- Deferred. When a Multi-Media unit is not assigned to call an alarm station, the unit "holds" alarms until you start an alarm session for the site. If deferral meets your organization's needs, logging the events rather than having them trigger alarms could be a good strategy, too.
- Indirect. A FAULT-RELAY on a Multi-Media unit can warn a Multi SA or Multi alarm-station through an alarm-panel. See System Monitor on p. 134.

## PPP Connectivity

### Tip

**Only in some dial-up connections are Point-to-Point Protocol (PPP) user names and passwords used.**

This procedure might not apply to your Multi system.

### Purpose

PPP (Point-to-Point Protocol) Dial-up Networking user names and passwords are used for some dial-up connections. The PPP username and password for an alarm station usually differs from the PPP username and password needed to access a RAS server.

- Multi SA includes RAS server in connection definition.
  - See RAS Server, p. 44.
  - See also Dial-up Technical Note, p. 33.
- Operator to RAS server “in front ” of one or more Multi-Media units. Use of connection accessing a RAS server, before using View is illustrated in sections:
  - Using a RAS Server before Connecting to a Unit, on p. 47.
  - See also Dial-up Technical Note, p. 33.
- Unit connecting by dial-up to alarm station’s modem. To automate the process of a Rapid Eye Multi-Media unit sending alarms to View over telephone lines, use Admin to enter the PPP user name and password for a PC, in the definition of an alarm station. Dial-up Connection to an Alarm Station on p. 208.
- Unit connecting by dial-up to RAS server “in front” of a Multi-Media alarm station. Use of an alarm callback that includes a RAS server is illustrated in:  
RAS Connection to an Alarm Station, p. 216.

## Denying Access

### Rogue user scenarios

There may be situations when a specific account user must be quickly denied access to a Rapid Eye site (for disciplinary reasons, termination, and so on). If your Multi system is accessed using a laptop, or by many PCs on your network, it could be inconvenient to physically prevent a rogue user from using Multi software.

### Best solution

The best solution is to “Deny access to sites...” in the account, as explained in Denying Access. This is quicker than deleting the rogue account and more effective than changing the account’s password.

### Stopping a user in session

On networked units, you can end a rogue user's use of sessions (maintenance, live video, and so on) by using Admin and View in combination. See the next section, To Stop a Session on a Networked Multi-Media Unit

### Stopping sessions on units that use modems

Multi sessions on a Multi-Media unit that is solely accessible by dial-up, cannot be interrupted other than by physically intervening. You must either apprehend the user or unplug the phone line connected to the Multi-Media unit's modem. For high security needs, a remotely controlled, telephone-line switch can be used.

### Dealing with an open Maintenance Session

These solutions require running a Maintenance Session. If the user has left a Maintenance Session open on a station, a Multi SA's efforts to rectify the situation are hampered. When creating accounts, you can plan to limit the amount of time that sites can be used by a user account. See Right to Access a Site, p. 182.

### Outside hackers

To prevent someone who has a copy of Multi software outside of your organization, from accessing your Rapid Eye sites: change your system password, as explained in System Password, on p. 166.

## To Stop a Session on a Networked Multi-Media Unit

### Purpose

When unauthorized use of a Rapid Eye site is identified, you may need to stop a user in session.

1. Using Admin, click the User tab.
2. Double-click the name of the user who must be stopped. The Update user dialog box appears.
3. Either:
  - Click the Deny access to sites... box so that it displays a checkmark.
  - or -
  - Remove the account's rights by clicking the checkbox of each right until each checkmark is removed.
4. Click **Save and Close**.
5. Using View, start a Maintenance Session at the site where access must be stopped.
6. On the Security tab, click **Update security**.

### Unauthorized Clips

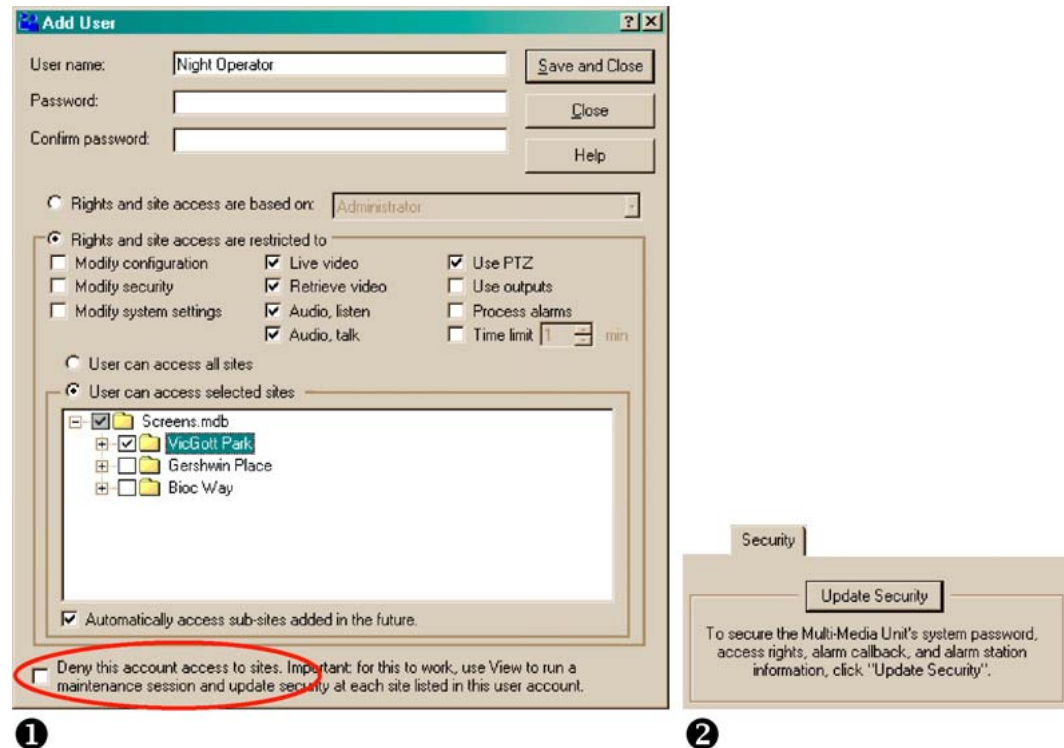
After stopping a session, you may need to check the user's PC for clips that may have been made during unauthorized access.

## Denying Access



Honeywell recommends the following procedure as the only expedient way to deny access to a user.

Fig. 10-19. Denying Access (1) and Updating Security for each Site in the Account (2).



## To Deny Access to a User of Your Multi System

1. Using Admin, click the User tab.
2. Double-click the name of the user who must be denied access to your site(s). The Update user dialog box appears.
3. Click the Deny access to sites... box so that it displays a checkmark; then click **Save and Close**.
4. Using View, start a Maintenance Session at a site where access must be denied.
5. On the Security tab, click **Update security**. See also Updating Security on a Multi-Media Unit, p. 131.
6. Repeat steps 4 and 5 for each site at which the user must be denied access.
7. There is no harm in leaving the account in the database, for archival purposes. You have the option of deleting the user's account, using Admin.



To deny access, you need to update security only at the sites the user must not access. On large systems, this can save the trouble of running many Maintenance Sessions. See Updating Security on a Multi-Media Unit, p. 131.

### Ineffective strategies for an unwanted user



Honeywell does not recommend the following strategies. They are misguided! They are explained so that they are not mistakenly used or produce a false sense of security. For a correct strategy, see the procedure:: **To Deny Access to a User of Your Multi System**, above.

- Changing the user's password. For this to work, the unwanted user would have to first refresh the Local database or quit using View, both optional acts. This is an ineffective strategy.
- Deleting a user's account (before denying access). This involves more steps than in the procedure at the beginning of this section. After deleting the account, you would still have to change the system password. As a result (see System Password, on p. 166), you then need to update security at the sites that this user must not access, and communicate with your entire user base, so that each refresh their local database. This is not good strategy.

## Removing Multi-Media Software

To remove Multi software, a Microsoft Windows procedure is used.

1. On the Windows desktop, click **Start**.
2. Click **Control Panel**.
3. Double-click **Add/Remove Programs**.
4. On the Install/Uninstall tab, use the scroll bar to help locate the Multi program. Select either:
  - Rapid Eye Multi Admin and View [version number].
  - or -
  - Rapid Eye Multi View (version number may vary).
5. Click **Add/Remove**. An InstallShield utility removes Multi software from the PC.

### Using Windows Explorer to delete Multi files

It is not recommended that you use Windows Explorer to delete Multi executable files. Multi software uses registry keys that may also need to be removed. Please use the above procedure to do so.





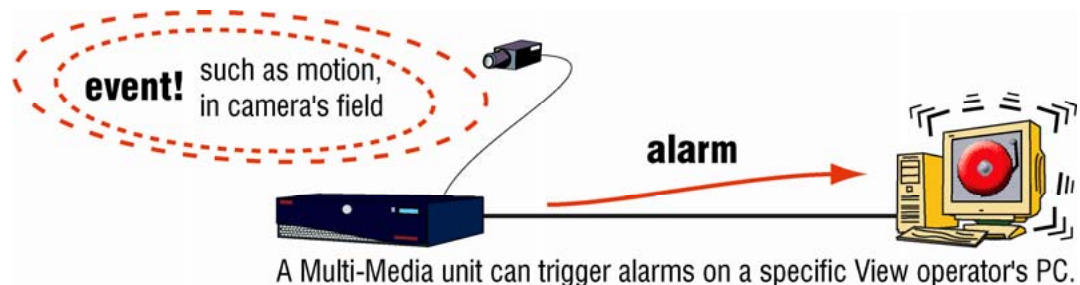
## Multi-Media Alarm Stations

### Overview

#### Flexibility in security

Like most Multi-Media security features, use of alarm stations is optional. A Multi-Media alarm station can receive alarms from one Multi-Media unit or many.

**Fig. 11-1. A Multi-Media Unit Can Send Alarms to a Specific PC.**



#### Customizing a PC to be an alarm station

Admin is used to designate a PC as an alarm station. A Multi-Media unit that is set to trigger alarms (see Events Defined, on p. 187), can be directed by your Multi-Media System Administrator (Multi SA) to send its alarms to a designated PC.

#### Where we are

Your Multi SA may prefer to add an alarm station after adding:

- **User accounts.** Without users, only the Multi SA can use alarm stations. See Adding an Account, on p. 155.
- **At least one site.** Though a Multi SA can create alarm stations before sites, without a site an alarm station cannot do much. See Naming / Renaming a Site, p. 24.

## Checklist to Configure a Multi-Media Alarm Station

1. Adding an Alarm Station: Name and Reports, p. 203.
2. Identifying and Defining a Connection. An Alarm station can be reached over either:
  - Network Connection to an Alarm Station, p. 205, or
  - Dial-up Connection to an Alarm Station, p. 208.
3. Making an Alarm Station Operational, p. 202.

## Operator Needs

### What alarm station operators need from their Multi SA

View operators who deal with alarm stations can ask their Multi SA if their user account(s) have the right to:

- **Process alarms.** See Granting Rights, on p. 158, and Right to Use View, on p. 181.
- **Access the sites set to call the alarm station.** See Right to Access a Site, p. 182.

## Multi SA Needs

### What a Multi SA needs from your organization

Before your Multi SA designates an alarm station, he or she needs:

- **Telephone number.** The number that Multi-Media units dial to reach a modem on an alarm station.  
- or -
- **IP address.** The address of an alarm station on the same network as Multi-Media units. See figure 11-2, below.  
- or -
- **Both.** For connecting to the modem of a remote access service (RAS) server, your Multi SA needs the RAS server's telephone number and IP address of the networked PC used as an alarm station.



**Honeywell recommends that Multi SAs check if their organization allows the type of connection they plan to use.**

For example, your organization may not allow connecting by modem to a PC on its network if this bypasses a firewall.


## System Administrator Needs



**Let your network administrator know that alarms are sent to port 10,003.**

This port should be left open in your organization's firewall, for the sockets used by Multi alarms. For other ports used by Multi, see table 3-7 on p. 49, in section System Tab in a Maintenance Session.

## Adding an Alarm Station: Name and Reports

1. Using Admin, click the Alarm stations tab.
2. To start adding an alarm station, display the Add Alarm station dialog box. Either:
  - Click  on the toolbar.
  - Click **Add** on the Actions menu.
3. Type a name in the Station Name box.
4. Select the name of one site or many in the Sites Available column.
5. Click the right-arrow to move the names to the **Sites that report to this Station** column.
6. You are now ready to define a connection (p. 203) and make the alarm station operational (p. 218).

### To reduce complexity: add alarm station definitions

For View operators using sites in many different areas, you have the option of creating two (or more) alarm station records to shuttle alarms to the same (!) PC. Duplication can reduce complexity, especially where customized dial-up connections are needed. For example, you could have one definition for local sites, another for sites in other cities.

### To reduce complexity further

To avoid complexity, use descriptive names such as: “[locality name] units”, “[city name] units”, such as “Chicago sites” or “Fargo sites”.

## Identifying and Defining a Connection

Enter either: dial-up information, an IP address or both, as listed in table 11–1. Connection data is compulsory when adding an alarm station.

**Table 11–1 Defining a Connection to an Alarm Station**

For a Connection to ...	Dial-Up	IP Address	See ...
alarm station modem	✓	n/a	p. 208
alarm station modem using an irregular area code, and so on	✓	n/a	p. 211 & p. 51
networked alarm station	n/a	✓	p. 205
server modem, with alarm station networked to it	✓	✓	p. 216
network address translation	n/a	✓	p. 206

**Table 11-2 Connection Information Needed for a Rapid Eye site to an Alarm Station**

<b>To Setup Alarm Station Using ...</b>	<b>A Multi SA Needs ...</b>
identical dial-up calls to alarm station's modem from Multi-Media units reporting to it	The alarm station's: - telephone number - PPP user name and password
various local, long distance or international dial-up calls, to the same alarm station's modem	The alarm station's: - telephone number - PPP user name and password Multi SA has to adjust alarm station's telephone number in site definition
network access	The alarm station's IP address
dial-up to RAS server, to access alarm station on server's (remote) network	(1) The Multi alarm station's: - IP address (2) The RAS server's: - telephone number - PPP user name and password.
Network address translation	(1) The Multi alarm station's: - IP address (2) The internet router's: - IP address.

## The PPP Fields in an Alarm Station's Definition

### Scope

This feature is for use in complex systems involving many Multi-Media, Multi-Media LT and older Multi units using modems and a RAS server to connect to a number of alarm stations.

### General case

For simple systems involving only a few units, Honeywell recommends that static PPP User Names and Passwords be typed in an alarm station's definition.

### PPP fields can be left blank

When adding or updating a Multi-Media alarm station, you have the option of leaving the PPP fields blank. The sites that report to that alarm station will use their site's name for PPP fields that are left blank.

### Updating unit Security and network routers

For this feature to take effect, your organization's Multi System Administrator (Multi SA) needs to update security on each unit that plans to use alarm stations where PPP fields were left blank. Use of the feature involves reconfiguring network routers to allow the unit names or passwords through for further processing.

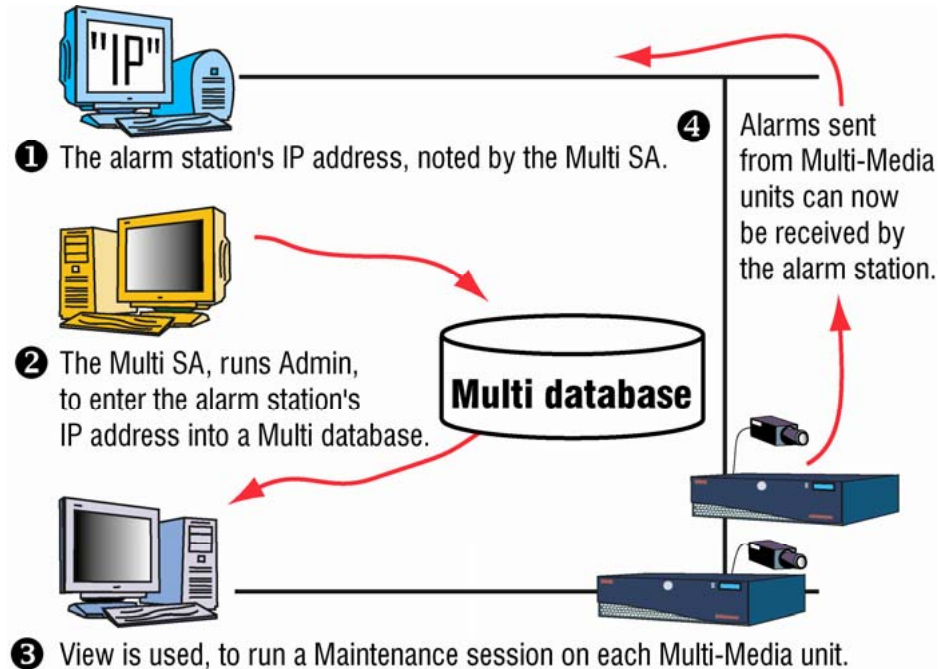
## Network Connection to an Alarm Station

### Tip

Your Rapid Eye site might not need this type of connection to an alarm station.

For other means of connecting to an alarm station, see table 11-2 on p. 204.

Fig. 11-2. Over a Network, Alarm's Are Sent to an Alarm Station's IP Address.



## To Setup a Network Connection to an Alarm Station

1. While adding or updating an alarm station definition in the Add Alarm Station/Update Alarm Station dialog box, select **Use Existing Network Connection**.
2. In the **IP Address** box, type the alarm station's address. An IP Address is mandatory for a network connection.
3. Click **Save and Close**. The Alarm Stations tab appears. In the tab's Connection Method column, the first letter of "network" appears in parentheses: "(n)", followed by the IP address used to connect to the alarm station.
4. The next step is Making an Alarm Station Operational; see p. 218.

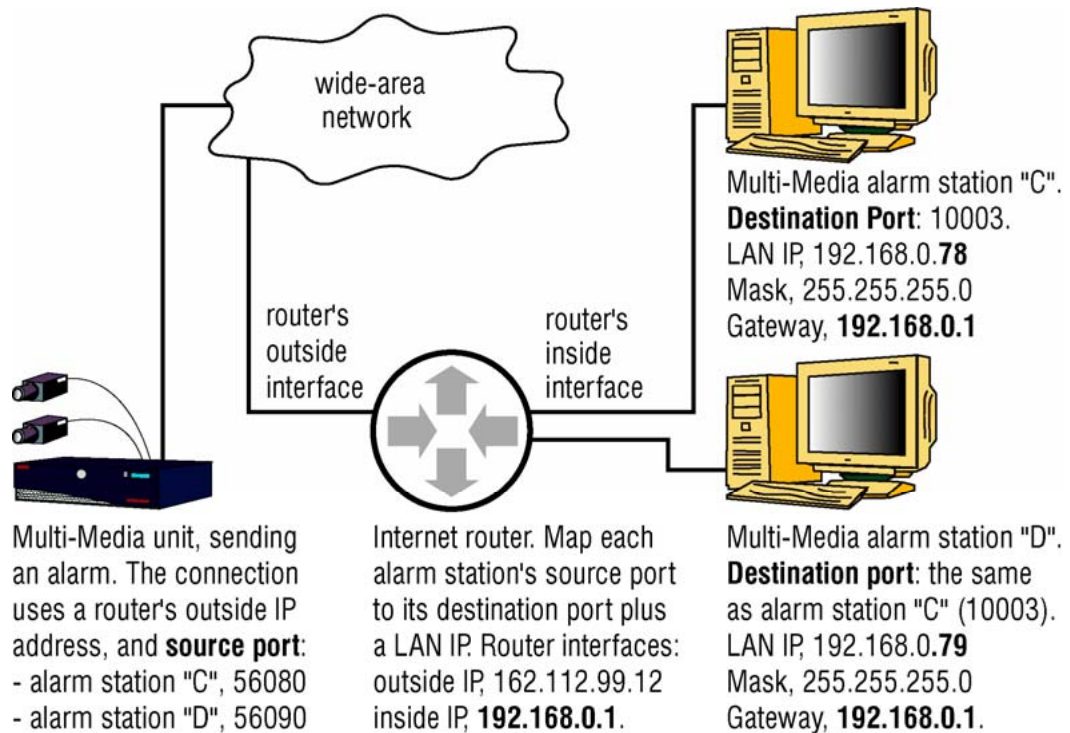
## Network Address Translation for Alarm Stations

### In a nutshell

A connection to one or many Multi-Media alarm stations, using one IP address, can be made by using network address translation (NAT) and port address translation (PAT)—a one-to-many address translation. This is useful to connect to alarm stations through:

- A WAN
- The Internet
- To another segment of the same LAN.

**Fig. 11-3. Receiving Alarms from a Multi-Media Unit, over a WAN or the Internet.**



### IP Addresses

The key is to configure a router to translate and map the Callbacks source IP port. The Network Administrator of the destination's LAN can supply a Multi SA with the "Outside" IP address of the internet router.

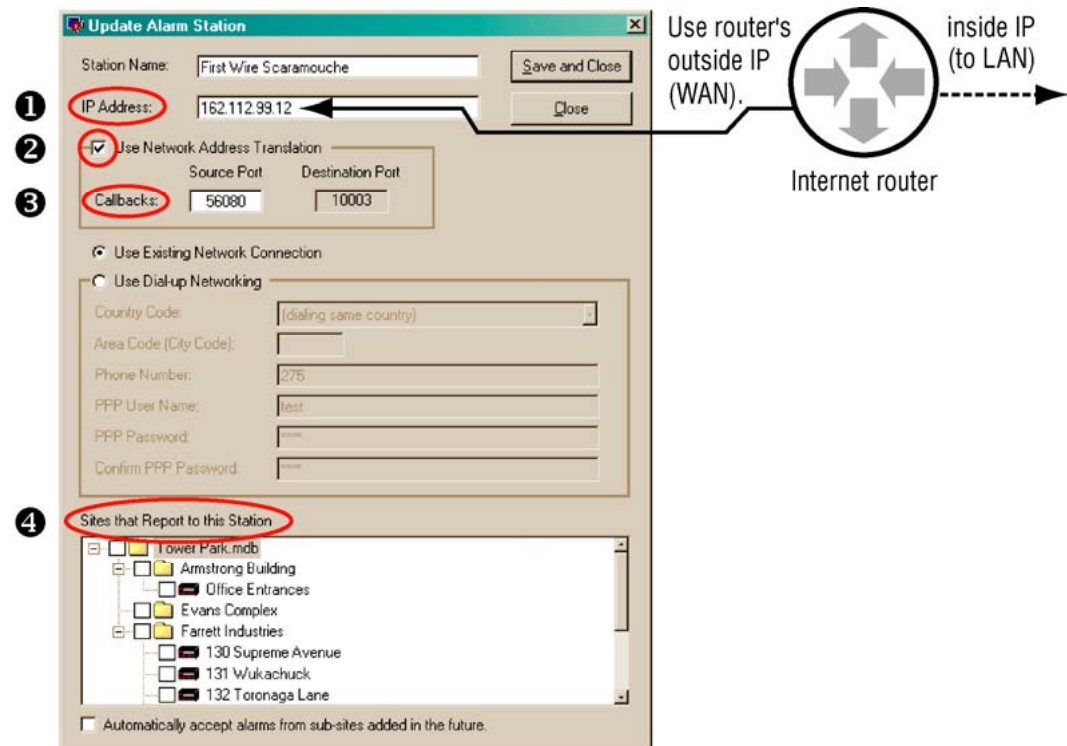
### IP Port

Callbacks to alarm stations on a remote LAN are identified by the value of the Callback Source IP Port box, in the Add Alarm Station /Update Alarm Station dialog boxes of Admin software, shown in figure 11-4. Each alarm station on a remote LAN needs to have a different Callback value.

### Mapping IP port in network's router

For each Multi-Media alarm station, one port mapping is needed when translating a network address.

Fig. 11–4. Connecting through a WAN to a Multi-Media Alarm Station on a LAN.



## To Prepare a Multi-Media Unit for NAT, Using Admin

1. Using Admin software, configure the connection to an Alarm Station. Assign the router's outside IP address to the **NAT Source Port Callbacks** box. See figure 11–4.
2. Enable **Use Network Address Translation**.
3. Assign a value to the **NAT Callbacks Source Port**. In figure 11–4, for example, the value of Callbacks has been changed from 10,003 (the default) to 56,080. A value greater than 65,532 cannot be used.
4. Select the Multi-Media sites that report alarms to the alarm station.
5. Click **Save and Close**. The Alarm Stations tab appears. In the tab's Connection Method column, a "(d)" appears, standing for "dial-up", followed by the telephone number that calls the RAS server; then an (n), standing for "network", followed by the IP address of the Multi alarm station.
6. Repeat steps 1 to 3 for other alarm stations on the same LAN.
7. Use the router's software to map each alarm station's source port to the corresponding destination port, plus the alarm station's LAN IP. See table 11–3, below, or figure 11–3, at the start of this section.

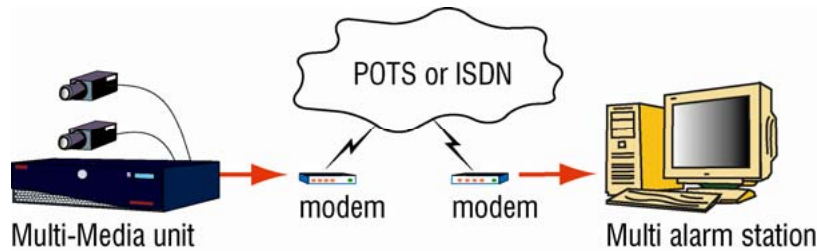
**Table 11-3 Router Mappings: Example for Unit Callback to Alarm Stations**

Admin setting to: destination		Network device: mappings	
NAT Port (to network router)	Router's Outside IP (network constant)	Physical Port (unit & firewall)	Inside IP (alarm station)
alarm station "C"			
Callback Port: 56,080	164.178.32.59	>	10,003* 10.1.0.78
alarm station "D"			
Callback Port: 56,090	map as above	>	10,003* 10.1.0.79

\* Alarms are sent to port 10,003. For other ports used by Multi, see table 3-7 on p. 49, in section System Tab in a Maintenance Session.

## Dial-up Connection to an Alarm Station

**Fig. 11-5. To Report an Alarm, a Multi-Media Unit Can Call an Alarm Station.**



## Preparing a Dial-up Connection to an Alarm Station

### Modem

Multi-Media units can use a telephone line, either: "plain old telephone system" (POTS), or higher speed "integrated services digital network" (ISDN) to connect to the modem of an alarm station, or its RAS server. You also need to know the telephone number to reach that modem.

### Microsoft Windows

To send alarms over a dial-up connection, you will need to obtain a point-to-point (PPP) protocol username and password, for the PC used as an alarm station, or for its RAS server, from their Microsoft Windows operating system. See The PPP Fields in an Alarm Station's Definition, p. 204.



## To Setup a Dial-up Connection to an Alarm Station

Fig. 11-6. Area Code Input Is Needed to Reach a Multi-Media Alarm Station.

1. While running Admin software to add or update an alarm station definition (as explained in Adding an Alarm Station: Name and Reports, p. 203), you will see either of the Add Alarm Station/Update Alarm Station dialog boxes, illustrated in figure 11-6. The IP Address box is left empty for a dial-up connection to an alarm station, except if a remote access service (RAS) server, apart from the alarm station, is part of the connection. For RAS servers, see RAS Connection to an Alarm Station, on p. 216.
2. Click **Use Dial-up Networking**.
3. Leave the Country Code to “(dialing same country)”, unless the Multi-Media unit is in a different country than the alarm station.



**Use “(dialing same country)”. Only use a country’s name (such as “United States of America (1)”) when the alarm station is in a different country from the Multi-Media unit.**

4. Type the alarm station’s area code in the Area Code (City Code) box.
5. Type the alarm station’s telephone number in the Phone number box.
6. Type the alarm station’s PPP user name and PPP password in their boxes. These can be obtained from your network administrator, as indicated in section Overview.
7. Type the PPP password a second time, in the Confirm PPP Password box.
8. Click **Save and Close**. The Alarm Stations tab appears. In the tab’s Connection Method column, a “(d)” appears, standing for “dial-up”, followed by the telephone number that calls the Multi alarm station.
9. The next step is Making an Alarm Station Operational; see p. 218.

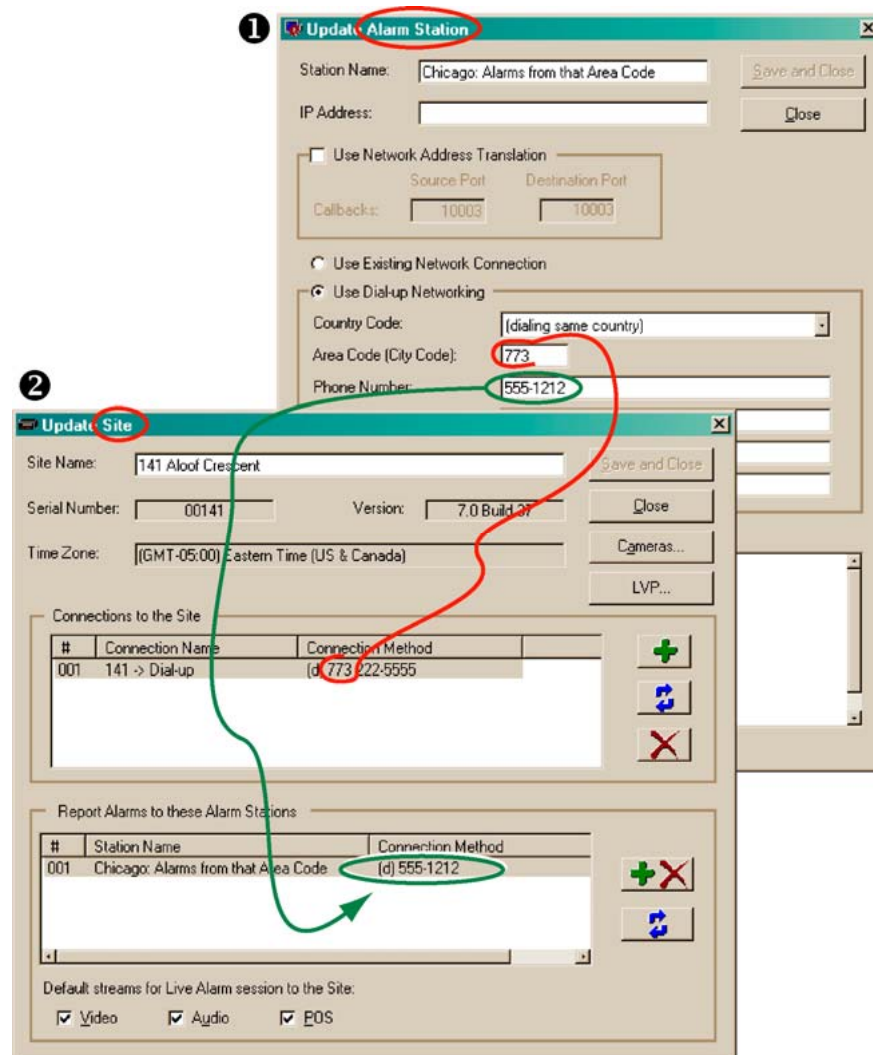
## Entering Area Codes in Site and Alarm Station Definitions

When the country and area codes of an alarm station match those of the sites reporting to it, calls to the alarm station are considered local. If they do not match, Multi uses a long distance code ("1" by default + an area code) to make the call. The rule is illustrated in figure 11-7.

### Tip

**Long distance or local, Honeywell recommends that you enter long distance codes for alarm stations and for Rapid Eye sites. The software can compare the phone numbers more easily that way, suppress their display automatically as needed, and avoid processing an error.**

**Fig. 11-7. Connection for an Alarm Station (1) Is Shown also in a Site's Definition (2).**



### Dial-up to another area code

An example is shown in table 11-4, using an alarm station in Chicago, Illinois, and Multi-Media units in Chicago and Fargo, North Dakota. Note that comparing telephone numbers without area codes can produce a local call when a long-distance call is needed.

**Table 11–4 Area Code Matching, for Site and Alarm Station**

Multi-Media Unit	Alarm Station (Chicago*)	Match	Result
enter: 773 (Chicago)	enter 773 (Chicago)	yes	OK: 555-1212
enter: 773 (Chicago)	code not entered	no	OK, local: 555-1212
enter: 701 (Fargo)	enter: 773 (Chicago)	no	OK: 1 773 555-1212
(Fargo) code not entered	(Chicago) code not entered	yes (?)	<b>error</b> ; a long distance call is needed.

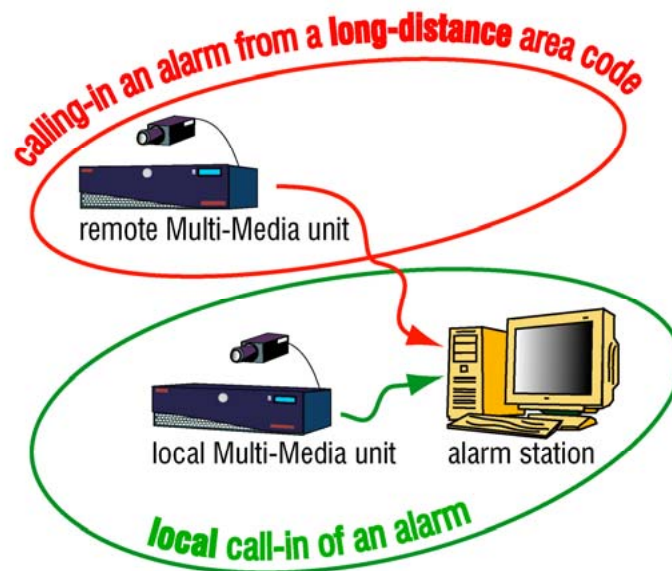
\* One of the area codes for Chicago is: 773.

## Customizing a Dial-Up Connection to an Alarm Station

### Preparation

Before customizing a dial-up connection, check your alarm station definition, as explained in Dial-up Connection to an Alarm Station.

**Fig. 11–8. Irregular Use of Area Codes when Units Are Calling an Alarm Station.**



### No need to customize... most times

You do not need to customize a long distance code when a Multi-Media unit uses regular long distance. One or many such sites can call-in alarms to the same alarm station without concern.

By default, Multi makes local calls when long distance codes match. You can add a long distance or toll-free code, site-by-site as needed, in the Update Station to Call in Case of Alarms box. See figure 11–9, below and section Customizing a Dial-Up Connection to an Alarm Station, p. 51.

### Irregular area code use

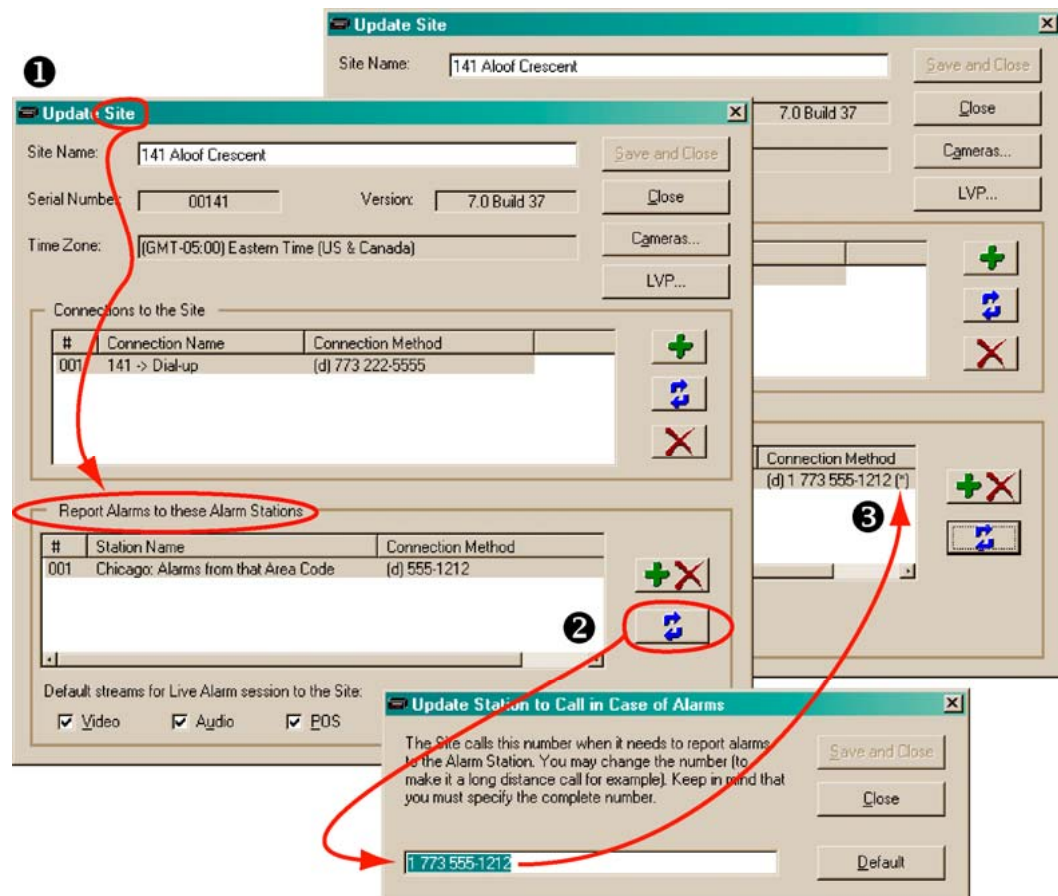
Why customize? When a unit is not in the same area code as its alarm station, sometimes a local call can be used when the alarm station is close by. Figure 11–8 illustrates this possibility and others.

You can customize an alarm station's:

- Long distance codes, for irregular and toll-free uses
- Dialing speed, by using a delay code
- or -
- Telephone exchange, at the Rapid Eye site or at the alarm station.

A copy of the telephone number in the alarm station definition is available for customization at each site definition, in its Report Alarms to these Alarm Stations pane. For example, in figure 11–9, long distance and Chicago area codes "1 773" were added to the local number, for a site that requires an irregular long distance call within one area code. A customized number is not shared with other sites. The customization is shown by an asterisk, at (3).

**Fig. 11–9. Customizing the Dial-up to an Alarm Station in the Site's Definition.**



## Tip

The alarm station telephone number in the site definition is the one that is actually used to dial to an alarm station.

See also: Customizing a Dial-Up Connection to an Alarm Station, p. 51.

## To View “Update Station to Call in Case of Alarms”

- Update the alarm station listed on the Sites tab.

## To Use a Local Call Across Area Codes

- Customization is needed when your telephone company does not require a long-distance call for a call to another area code. You can remove the long-distance code for a “remote Multi-Media unit”, site-by-site as needed, in the Update Station to Call in Case of Alarms box, obtained by updating the alarm station listed on the Sites tab. This is illustrated in figure 11–9, p. 212, and in section Customizing a Dial-Up Connection to an Alarm Station, p. 51.

## Toll-Free Numbers

- Customization is needed when toll-free numbers match and dial-up is used to: reach units or call in alarms.

## To Use a Long Distance Call in One Area Code

- Customization is needed when your telephone company requires a long-distance call within an area code. You can add the area code for a “local Multi-Media unit”, site-by-site as needed, in the Update Station to Call in Case of Alarms box, obtained by updating the alarm station listed on the Sites tab. See figure 11–9, p. 212, and section Customizing a Dial-Up Connection to an Alarm Station, p. 51.

### Regular mixed area code use

You do not need to customize Multi-Media units that use regular long distance when in different area codes. The units can call-in alarms to the same alarm station without concern.

## To Delay the Speed of Dialing

- You can add one or more commas to a telephone number to delay further dialing by one-second increments.  
For example: 9,,, 555-1212  
dials a “nine” followed by a three-second pause (the three commas mean three seconds) before the rest of the number is dialed.

### Telephone exchange

A telephone exchange might be a component in the connection chain between a Rapid Eye site and an alarm station. Find out if your system has an exchange at the Rapid Eye site, at the alarm station, or at both ends.

Telephone exchange at alarm station. In the alarm station definition, add an extension suffix in the Phone Number box, after the telephone number, in the alarm station definition. Such a delay might be needed to give the alarm station's exchange time to answer, before any exchange commands or the extension are dialed.

## To Delay the Extension Suffix

- To delay the dialing to the extension as needed, type commas in the box. Each comma adds a one-second delay. For example: 9,,, 555-1212,,,,,,226 introduces an eight second delay (eight commas would produce eight seconds of delay) before dialing the final “226”. See also the previous section, Dial-up Connection to an Alarm Station.

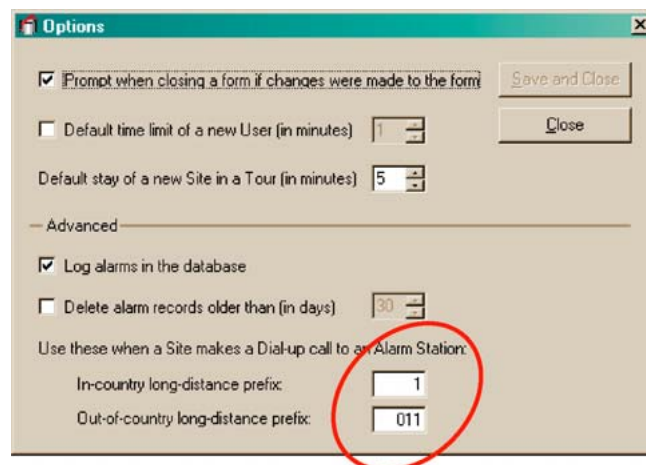
### Telephone exchange at a Rapid Eye site.

There are two cases for a prefix number—that extra telephone keystroke such as a “9” or an “8” that needs to be dialed before an alarm station’s number. For Multi-Media units using the same alarm station, either:

- The exchange is shared.** In the alarm station definition, add a prefix in the Phone Number box, before the telephone number. You can use commas as needed to delay the dialing of the extension until the alarm station’s exchange answers. See Dial-up Connection to an Alarm Station, above.  
- or -
- The exchange is not shared.** You will have to add the prefix before the telephone number, site-by-site as needed, in the Update Station to Call in Case of Alarms box, obtained by updating the alarm station listed on the Sites tab. This is illustrated in figure 11–9, on p. 212 and in section Customizing a Dial-Up Connection to an Alarm Station, p. 51.

## International Dial-up

Fig. 11–10. International Prefixes for Use of Rapid Eye Software in North America.



The prefixes are used for units that dial-up to alarm stations. Your Rapid Eye site might not need this type of customization to its dial-up connection to an alarm station. For other means of connecting to an alarm station, see table 11–2, p. 204.

### Planning for a few international units

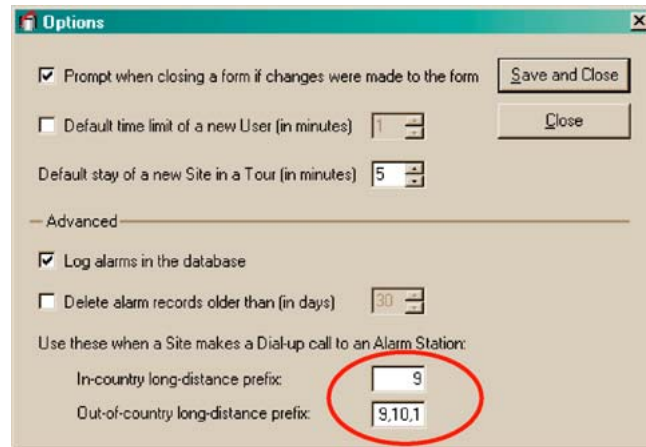
If only a few units reporting to an alarm station are outside of the alarm station’s country, it is more effective to add the prefixes, site-by-site as needed, in the Update Station to Call in Case of Alarms box, obtained by updating the alarm station listed on the Sites tab. See Customizing a Dial-Up Connection to an Alarm Station, p. 51.

### Alarm station for many international units

If there are many international units reporting to an alarm station and they are all in the same country, you have the option of changing the long distance prefixes for out-of-country and in-country dialing. Figure 11–10 shows the default prefix values.

## To Change Long-distance Prefixes

Fig. 11–11. International Prefixes for Use of Dial-up in Rapid Eye Software.



Long distance prefixes affect only connections from units to alarm stations. Connections from View to units are not.

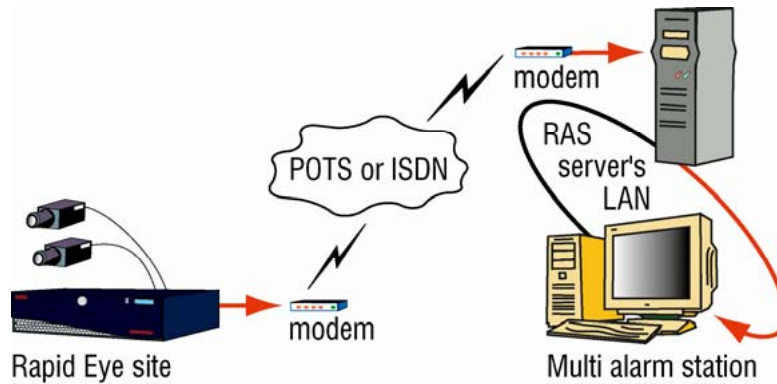
1. Click "Options" on the View menu in Admin.
2. As needed, type an in-country long-distance prefix or an out-of-country long-distance prefix in their boxes. For example, figure 11–11, above, shows the prefix for the city of Kiev, in the Ukraine. Foreign prefixes for alarm station dial-up vary depending on the country. Note also that commas can be used to introduce a delay in the dial-up.

### Creating extra alarm station definitions

The simplest solution when many international sites need customization is to create two (or more) alarm station records that shuttle alarms to the same PC. For example: one record for international sites in country "a", another for sites in country "b", as needed. You can then add whichever alarm station is most appropriate for a site, on a site-by-site basis. To create alarm station records, see Adding an Alarm Station: Name and Reports, on p. 203. When most units are outside the operator's country, it is best to change the country code in the alarm station definition.

## RAS Connection to an Alarm Station

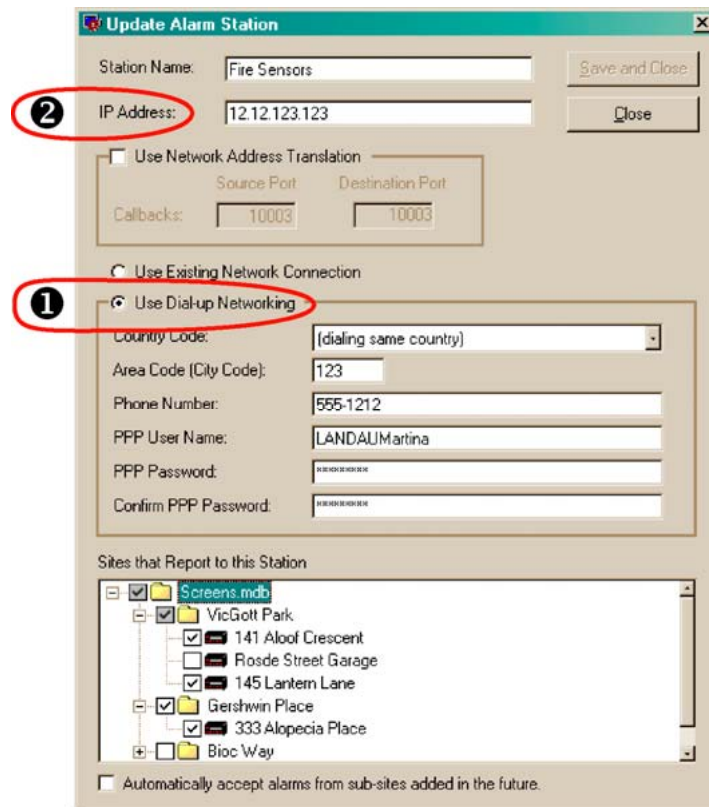
Fig. 11–12. A Multi-Media Unit Can Send Alarms through a RAS Server.



### In a nutshell

A Rapid Eye site may need to connect to a remote access service (RAS) server to reach a Multi alarm station. Figure 11–13 shows a telephone number to a server's modem. The number is dialed first (1); PPP authentication occurs. Alarms can then reach the alarm station using the unit's IP address (2).

Fig. 11–13. RAS Configuration.



### What your network administrator needs to know

Alarms are sent to port 10,003. This port should be left open in your organization's firewall, for the sockets used by Multi alarms.



**Tip**

**Your Rapid Eye site might not need this type of connection to an alarm station.**

For other means of connecting to an alarm station, see table 11–2, p. 204.

## To Setup a Connection to a RAS Server

1. While adding or updating an alarm station definition (as explained in Adding an Alarm Station: Name and Reports, p. 203), you will see either of the Add Alarm Station or Update Alarm Station dialog boxes. Type the alarm station's IP address in the IP Address box. See figure 11–13.
2. Click **Use Dial-up Networking**.
3. Leave the Country Code to "(dialing same country)", unless the Multi-Media unit is in a different country than the RAS server.



**Honeywell recommends using "(dialing same country)".**

Do not use your country's name, such as "United States of America (1)", unless the alarm station is in a different country from the Multi-Media unit.

4. In the Phone number box, type the telephone number for the RAS server's modem.
5. Type the area code for the RAS server in the Area Code box, as in figure 11–13.
6. Obtain the PPP User Name and PPP Password of Multi Alarm Stations that use a modem. This information is either held by your network administrator or set by the user of the workstation in the Windows Dial-up Networking program. Type one of the RAS server's PPP user name and its PPP password in their boxes; this authorization is obtained from the network administrator responsible for the RAS server's network, as indicated in section Overview.
7. Type the PPP password a second time in the Confirm PPP Password box.
8. Click **Save and Close**. The Alarm Stations tab appears. In the tab's Connection Method column, a "(d)" appears, standing for "dial-up", followed by the telephone number that calls the RAS server; then an (n), standing for "network", followed by the IP address of the Multi alarm station.
9. The next step is Making an Alarm Station Operational, p. 218.

### Tech note: process of a dial-up callback

When a Rapid Eye Multi-Media unit uses telephone lines to communicate with a Multi alarm station, the unit needs to use the alarm station's PPP user name and password for dial-up networking. After answering its modem, the alarm station must recognize the PPP user name and password before the Multi-Media unit can access View software.

### Creating extra alarm station definitions

You have the option of creating two (or more) alarm station records to shuttle alarms to the same PC: for example, one for local sites, and another for remote sites. To avoid complexity, use descriptive names such as: "local sensors" and "remote sensors". To create alarm station records, see Adding an Alarm Station: Name and Reports, on p. 203.

### Customizing a RAS dial-up

To customize a RAS dial-up (irregular or toll-free use of long distance codes, and so on), use the same procedures and suggestions as indicated in sections Customizing a Dial-Up Connection to an Alarm Station and International Dial-up, above.

## Making an Alarm Station Operational

### What a Multi SA needs to do

After adding an alarm station, p. 203, and defining how a Multi-Media unit connects to it, p. 203:

- You need to update security for each Multi-Media unit involved. See *Updating Security on a Multi-Media Unit*, on p. 131
- An alarm station is of little use if you have not set any events to trigger alarms. See *Events Defined*, on p. 187.
- Use View software, the Sites tab, to prioritize alarm stations. See *Cascading Alarm Stations*, on p. 49.
- Operators of PCs not designated as alarm stations can also receive alarms sent by a Multi-Media unit, by running an Alarm session using View. To find out how to run an Alarm session, see the *Rapid Eye View Software Operator Guide*.

## Using More than one Alarm Station

If enough sites need customization, you could create two (or more) alarm station records to shuttle alarms to one PC: one for long distance sites, another for local sites, i.e., within the same calling area. To avoid confusion, use descriptive names, such as: "Fire sensors – local calls" or "Fire sensors – long distance", and so on. You can then add the alarm station most appropriate for a site, on a site-by-site basis. How to create alarm station records is explained in *Adding an Alarm Station: Name and Reports*, on p. 203.

### See also

*Cascading Alarm Stations*, p. 49

*Quickly Assigning a Site to Many Alarm Stations*, p. 50

## Creating Extra Alarm Station Definitions for the same PC

A Multi SA has the option of creating two (or more) alarm station records to shuttle alarms to the same PC: for example, one for local sites, and another for remote sites. To avoid complexity, use descriptive names such as: "local sensors" and "remote sensors". To create alarm station records, see *Adding an Alarm Station: Name and Reports*, on p. 203.

## Disconnection Note


### When alarms are in progress

Closing View or disconnecting a session after a successful alarm callback voids that callback. This can occur due to: power failure, user action and so on. You can still view the alarms in an alarm session.

## To List Successful Alarm Callbacks after an Interruption

- Run View and start an alarm session.

## Removing an Alarm Station

1. Using Admin, click the Alarm station tab.
2. Select the alarm station that you want to delete.
3. To remove an Alarm Station, do one of the following:
  - Click  on the toolbar
  - Click **Delete** on the Actions menu.
  - Press the Delete key.
4. When the alarm station is to be deleted, click **Yes** to continue or **No** to cancel.

## Disabling/Enabling Dial-up Server

For some mission critical applications, your IT personnel may wish to disallow access to the Microsoft Windows procedure to disable and enable a RAS server on a PC.

## Alarms from a De-listed or Unregistered Unit

### Situations

View operators are warned with a message when a call about an alarm is from a Multi-Media unit that has been:

- Removed from a Multi-Media database (Multi db). Your Multi-Media system administrator (Multi SA) can remove a Multi-Media unit from a Multi db. However, that 'de-listed' unit may still be operating at a customer site, set to call a PC designated as a Multi-Media alarm station.
- Added without registration to a Multi-Media database. To register a Multi-Media unit, a View operator invokes a 'first' Maintenance Session on the unit. Even users without the right to use the commands of a Maintenance Session can start a Maintenance Session to register a unit.

In both situations, the following message appears. When the operator receives the message, calls about the alarm have stopped.

## To Trace the Unit Sending the Alarm


Either:

- A View operator can make a note of the unit's serial number and IP address indicated in the message.
- A Multi SA can consult the alarm log.

### Precaution

Before de-listing a Multi-Media unit or Multi unit from a Multi-Media database, Honeywell recommends that your Multi SA use Admin software to remove Alarm Stations listed in a site definition. See the procedure:: To Set a Site to Not Report to a Specific Alarm Station, next.

## To Set a Site to Not Report to a Specific Alarm Station

1. Using Admin, click the Sites tab.
2. Double-click the name of the site that you plan to remove. An Update Site window is displayed.
3. Click  in the "Report Alarms to these Alarms Stations" pane. The Add/Delete Stations to Call in Case of Alarms dialog box appears, displaying a list of alarm stations. Stations already assigned to the site are listed the Report Alarms to column.
4. To move alarm station names to the Alarm Stations available column, either:
  - Select one or many station names in the Report Alarms to column, then click the left-arrow, or
  - Double-click the ones that you want to move.
5. Click **Save and Close**. The Add Site/Update Site dialog box reappears, listing the alarm stations in the Report Alarms... pane.
6. You have the option of ending the site edit. To do so, click **Save and Close**. The Admin window reappears, listing your system's sites on the Site tab.
7. Use View to start a Maintenance Session for the Multi-Media unit that you plan to remove.
8. Click **Update security** on the Security tab of the Maintenance Session. Information from the Multi db is copied to the Multi-Media unit. Please wait until "Updated security" appears in the Feedback box.
9. Close the Maintenance Session.
10. Using Admin, remove the site.
11. Using View, click **Refresh**.

## Touring Many Sites

### Purpose

A Rapid Eye Multi system can be set to show all of the video and data from a series of sites, one site at a time, automatically. This a common use of a CCTV security system. Admin is used to setup one or more tours. View is used to run site tours.

### See also

A site tour, involving many Rapid Eye sites is very different from other types of tours, such as:

- **PTZ tour.** One camera; one site. See Pan, Tilt, and Zoom (PTZ) Setup to see how to set a PTZ-camera to a preset position.
- **LocalView tour.** Using LocalView to tour many cameras at one site. See the LocalView online help.
- **Public display monitor.** Many cameras at one site. Using a monitor connected to one Multi-Media unit. See Public Display Monitor: Using Monitor Output 1, p. 141.

## Preliminary Checklist

### Before defining a site tour

Your Multi System Administrator (Multi SA) needs at least two sites to define a tour. See Naming / Renaming a Site, on p. 24. For systems using one site only, a Live session is as effective as a Site tour. See the *Rapid Eye View Software Operator Guide*.

### Tip

**A site tour is not listed in View until more than one site is assigned to it.**

Design a site tour using two or more Rapid Eye units.

### System password

The System Password should be the same for the Rapid Eye sites selected for a site tour. See p. 166.

## Adding a Site Tour



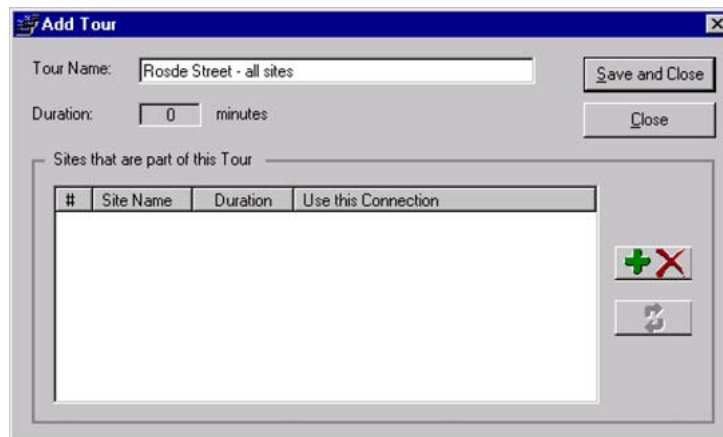
1. Using Admin, click the Tours tab.
2. To display the Add Tours dialog box, either:
  - Click  on the toolbar.
  - or -
  - Click **Add** on the Actions menu.
3. Type a name in the Tour Name box (see figure 12-1).
4. In the *Add Tour/Update Tour* dialog box, click  in the “Sites that are part of this Tour” pane. The Add/Delete Sites in Tour dialog box appears. The tour’s name must be typed before adding sites to the tour definition, when creating a tour.
5. Select one or many site names in the Available Sites column.
6. To move them to the Sites that are part of the Tour column, click the right-arrow. To move an item from one column to the other, you can also double-click it.
7. Click **Save and Close**. The Add Tour/Update Tour dialog box reappears, listing the names of the sites in the Sites that are part of this Tour pane.

Fig. 12-1 . Adding a Tour Name.



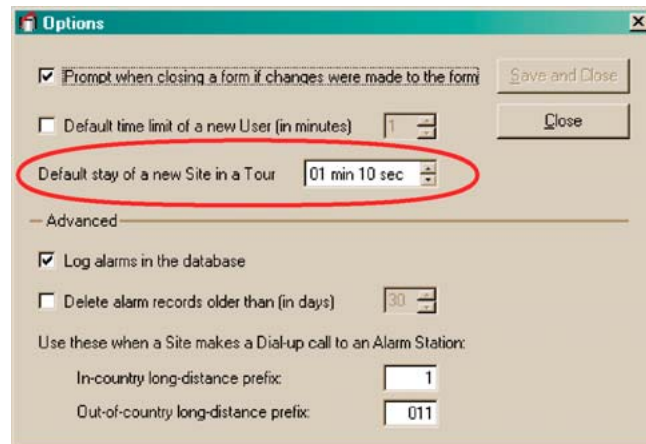
### Note on the word “tour” for PTZ cameras

The meaning of “tour” can be different for some cameras that pan, tilt and zoom (PTZ). PTZ cameras can be programmed to move independently when not in use by an operator. For information about PTZ camera configuration, see Pan, Tilt, and Zoom (PTZ) Setup on p. 85.

## Default Amount of Time to Display a Unit During a Site Tour

1. While running Admin software, select the Options command in the View menu.
2. Adjust the minutes or seconds, as needed, in the “Default stay of a new Site in a Tour” option. See figure 12-2.
3. Click **Save and Close**.

Fig. 12-2. The Default Amount of Time for a Tour of each Unit.




## Customizing a Tour

### Purpose

For each tour, you have the option of specifying:

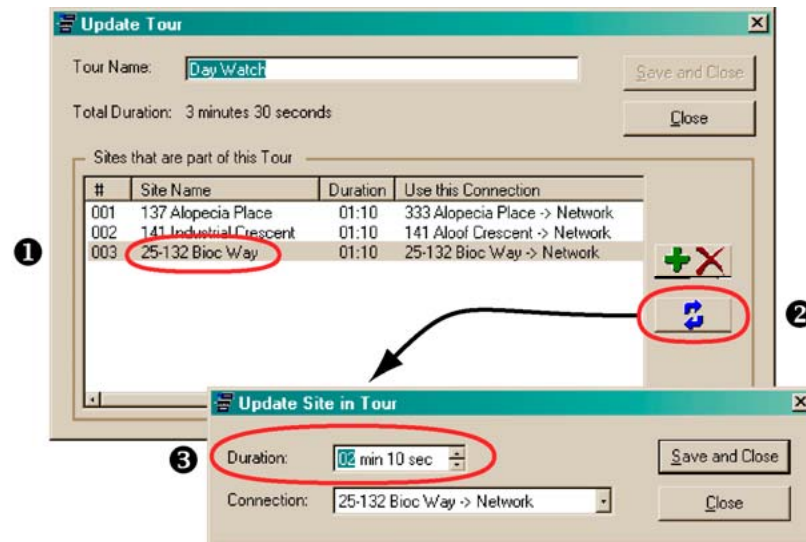
- The order in which sites are toured
- The time spent at each site
- and -
- The connection to be used to reach the site. By default, the first connection in the site's definition is used.

## To Change the Order of Sites in a Tour

1. Using Admin, click the Tours tab. There is no need to click it if already displayed.
2. To display the Update Tour dialog box, do one of the following:
  - Double-click the name of the tour that you want to customize.
  - or -
  - Select the tour that you want to customize; then: either click  on the toolbar, Update on the Actions menu, or press the F12 key.
3. In the Update Tour dialog box, drag and drop a site name to a new position in the list.
4. You can click **Save and Close** or change the time spent at the sites, as explained next.



## To Change the Time Spent at a Site, During a Tour

Fig. 12-3. Customizing the Amount of Time that a Multi-Media Unit Is Toured.



### Tip

If you are already in the Update Tour dialog box (from the previous procedure), skip to step 3.

1. Using Admin, click the Tours tab. There is no need to click it if already displayed.
2. To display the Update Tour dialog box, do one of the following:
  - Double-click the name of the tour that you want to customize.
  - or -
  - Select the tour that you want to customize; then: either click  on the toolbar, Update on the Actions menu, or press the F12 key.
3. In the Update Tour dialog box, do one of the following:
  - Select a site; then click .
  - or -
  - Double-click the name of a site.
4. A Duration box, appears in which you can adjust minutes or seconds as needed.
5. Click **Save and Close**.

### Tip



Should you plan to view a site for long periods, say thirty minutes or more, consider using a Live Session, rather than changing the durations of time spent at each site.




## To Select Another Connection to a Site, During a Tour

### Tip

If you are already in the Update Tour dialog box (from the previous procedure), skip to step 3.

1. Using Admin, click the Tours tab.
2. To display the Update Tour dialog box, do one of the following:
  - Double-click the name of the tour you need to customize.
  - or -
  - Select the tour that you want to customize; then: either click  on the toolbar, Update on the Actions menu, or press the F12 key.
3. In the Update Tour dialog box, do one of the following:
  - Select a site; then click .
  - or -
  - Double-click the name of a site.
4. Click the arrow next to the Connection box. There may only be one connection to select. Connections are defined while adding or updating a site. See Types of Connection, on p. 29.
5. Select a connection to the site used during the site tour.
6. You have options:
  - Click **Save and Close** and going to step 7.
  - Change the amount of time the site will be part of the site tour. See the previous procedure.
7. In the Update Tour dialog box, click **Save and Close**.

## Removing a Tour

1. Using Admin, click the Tour tab. There is no need to click it if already displayed.
2. Select the tour that you want to delete.
3. Do one of the following:
  - Click  on the toolbar
  - Click **Delete** on the Actions menu.
  - or -
  - Press the Delete key.
4. When you are warned that the tour is about to be deleted, click **Yes** to continue or **No** to cancel.

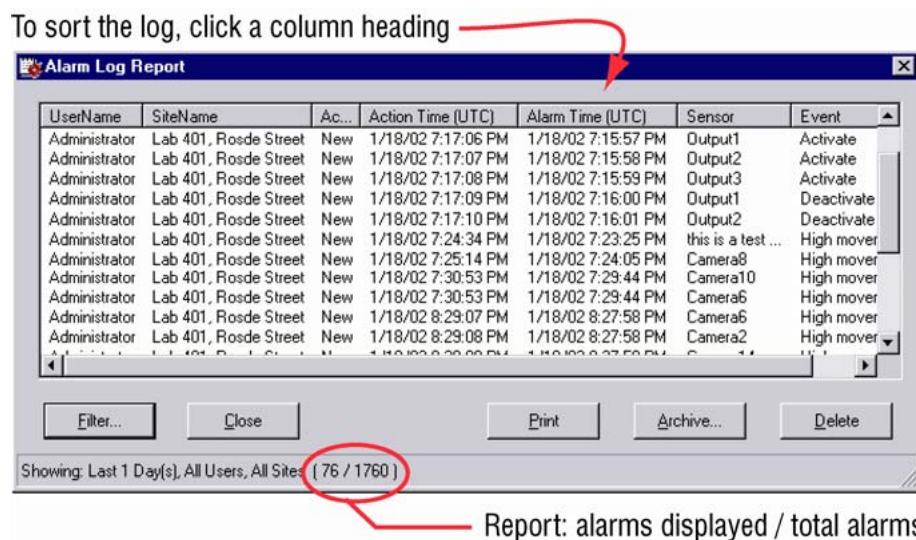


## Alarm Log

During an alarm session, a record of the event that caused the alarm is entered in the Alarm Log of the Multi central database (Multi db).

## Viewing the Log


Fig. 13-1. Alarm Log



The alarms produced in the last 24 hours are listed when the log is opened. The log can appear to be empty. Earlier alarms can be viewed by filtering (as in Filtering the Log, below).

## To view the log

Do one of the following:

- Click  on the Admin toolbar
- Click "Alarm Log" on the Actions Menu
- Press the F11 key.
- Using LocalView, click **View Log** on the Setup tab.

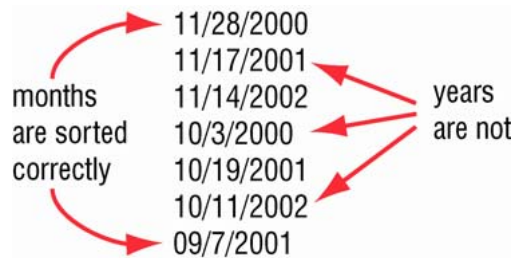
## Sorting the Log

To sort the log, click the column headings. See figure 13-1.

### A note on sorting

Items are sorted by their textual appearance. For example, if your Microsoft Windows is set to display dates as “month-day-year”, one obtains a listing such as in figure 13-2, below. This may not be what you want. You can use the simple workaround in the next procedure to obtain a chronological list.

**Fig. 13-2. Possible Result of Sorting when Using “Month, Day, Year”.**



Sorting the Action Time column might not list items in the chronological order that you expect. Log



**Honeywell recommends that the Short Date Style in Microsoft Windows be set to “yyyy/mm/dd” or similar date input (such as “yy-mm-dd”). What matters most is that a sequence of “year, month, day” be used in the format, and that months be expressed in numbers, not text. The double “m” and “d” ensure that single digits are padded with zeroes. For example, June 7, 2009 should be expressed as 2009/06/07.**

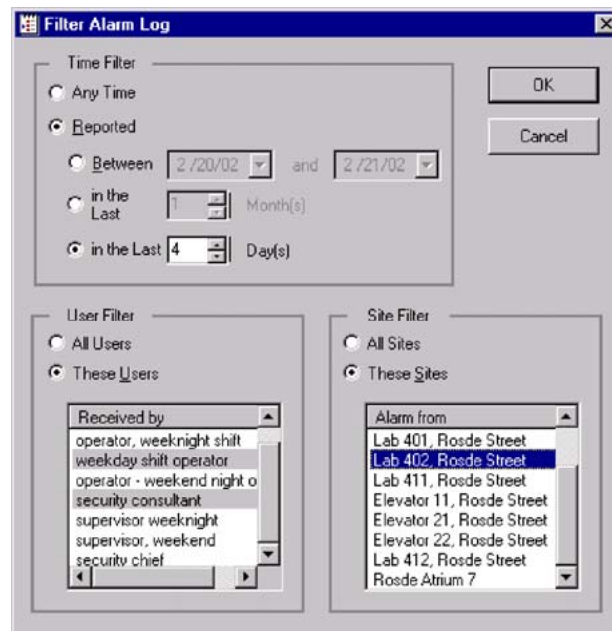
## Selecting Log Items

Use Windows’ mouse and keyboard techniques to select/deselect log items. For example:

- To select more than one user or site, press the Ctrl or Shift keys while clicking the names in the lists.
- To select all the alarms in the list, press the Ctrl+a keys. You can also right-click the list to click “Select All”, or you can select the first alarm in the list, press the Shift key; then click the last alarm in the list.

## Filtering the Log

Fig. 13-3. Filtering the Alarm Log.



Only alarms produced in the last 24 hours are listed when the log is opened. The log can appear to be empty. Earlier alarms can be viewed by filtering.

## Printing the Log

Before printing one or more of the alarms listed in the log, you have to select them.

### To Print a List of Alarms

1. While viewing the log as in Viewing the Log, above, select alarms that you want to print. To select more than one alarm, press the Ctrl or Shift keys while clicking the names in the lists.
2. Click **Print**. The print dialog box appears.
3. Click **OK**.

## Archiving the Log

You can copy a selection of alarms to a text file. The archived list of alarms is not removed from the log.

## To Archive Alarms

1. While viewing the log (as in Viewing the Log, above), select the alarms that you want to print.
2. Click **Archive...** . The “Save As” dialog box appears.
3. Type a name in the File name box.
4. Click **Save**.

### Technical note on the Alarm log

Alarm log entries accumulate over time. Each alarm takes approximately 530 bytes. There can be many entries; as many as your database engine allows. See your organization’s database administrator for rules on managing the size of the database.

## Removing Log Items

### To Delete Alarms

1. While viewing the log (as in Viewing the Log, above), select the alarms that you want to delete. You can select more than one alarm by pressing the Ctrl or Shift keys while clicking on alarms in the list.
2. Click **Delete** or press the Delete key. You are warned that the deletion is permanent.
3. To delete the items, click **Yes**.



**An Access-type Multi db filling with alarms, can become inoperable.**

## Alarm Log Data Reference

For the type of data found in the alarm log, see table 13–1.

**Table 13–1 Logged Data**

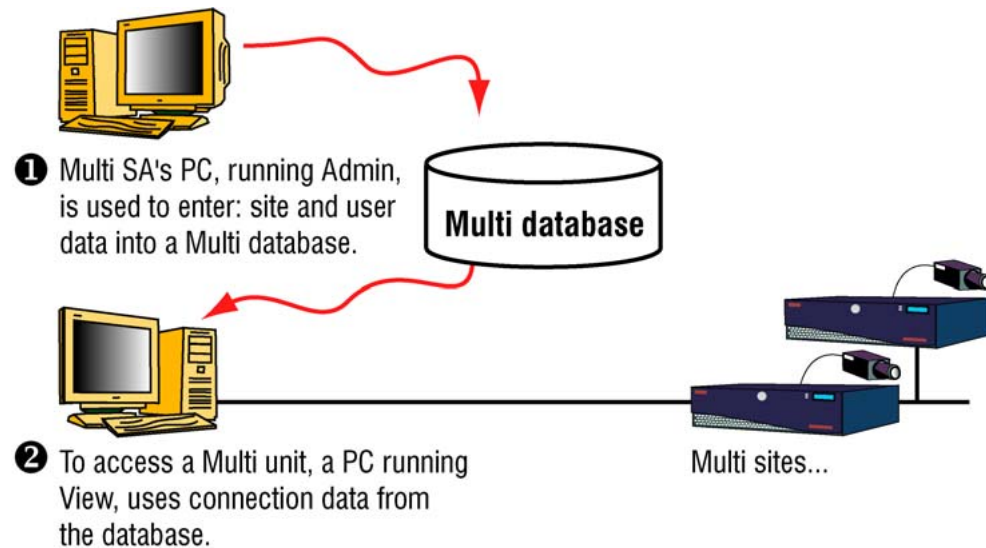
Column	Value	Section Reference
User Name	... of user logged on to alarm station or using alarm session	Adding an Account, p. 155
Site Name	... as specified in site definition	Naming / Renaming a Site, p. 24
Action	New, Ack, Rearm	Right to Use View, p. 181
Action Time	Date and universal coordinated time (UTC) at which action was taken	n/a
Alarm Time	Date and UTC of the alarm	n/a
Sensor	Multi input name for an Outside World event	Events Defined, p. 187
Event	... name of Multi event that triggered the alarm, or event from a customer-device	Events Defined, p. 187
Description	... if triggered by a rule, shows the rule's description. Otherwise, the field is empty.	Checklist for Setting a Rule in the Response Schedule, p. 113

## Multi Database

### In a nutshell

A Multi central database (Multi db, for short) is needed to run Admin. Information about: sites, users, alarm stations and site tours, is contained in a Multi db. You need only one Multi db for many sites.

**Fig. 14-1. Data Flow from Admin to View.**



When a unit operator logs on to View, a local copy of data about the operator and the sites he may access, is made from the Multi db to the PC.

### Database creation

Creating a database is a rare event that may be needed as little as once or twice during the life of your Multi-Media system. Honeywell supports two Microsoft database engines: Access and SQL-Server.

### MinAdmin

Your Multi SA has the option of supplying a Multi db that offers a limited Administrator account to run MinAdmin software.

## Starting Admin

Fig. 14-2. Admin Icon on the Windows Desktop.



## To Start Admin

1. On your desktop, either:
  - Click Start, point or click to: Programs, and then Rapid Eye Multi. Click Rapid Eye Multi Admin.
  - Double-click the desktop icon for Admin.
2. Then, either:
  - See Obtaining a Multi db, p. 232.
  - Use a Multi db that is already available. Skip to p. 243 for section Logging On.

## Obtaining a Multi db

### Alternatives

To obtain a Multi db after starting Admin, you have the option of:

- Using the default, empty, Multi db. An empty Multi db comes with the software. It is used to access a unit, out of the box. This is a simple way to get started.
- Switching to another Multi db. If you are given a Multi db prepared during the installation or at some other time, see Using Another Db: Converting, on p. 234.
- Creating an empty Multi db. See Creating a Multi Db, below.
- Copying a Multi db. You can base a new MS-Access Multi db on an MS-SQL or MSDE, and vice versa. See Db Based On Another.
- Upgrading a Multi db. Multi SAs can use a Multi db from their older Multi system; see Upgrading a Multi db on p. 241



## Using the Default Multi Db

### The first time that you log on

The file name of the default, central Multi central database is: "REMCentral.mdb". You can locate it by browsing through the folder holding the Multi software.

### The next time that you log on

The next time that you use Admin, the same Multi db is used. A Multi db can be renamed; see Renaming a Multi Db, p. 240.

**Table 14-1 A First Log On to Admin: Default Data for MS-Access**

Item	Value
User ID	Administrator
Password	none
Microsoft Access	selected
database path	to installation folder; by default it is C:\Rapid Eye Multi [version number]
database name	REMCentral.mdb, a Multi database file in the folder where Admin was installed.

## Contrasting Db Engines

### Quick contrast of database templates

Microsoft Access. You do not need to have Microsoft Access installed on your system to use the default Multi Central db immediately. The only limitation is for larger installations; an MS-Access db may not be able to hold the number of database records.

SQL Server or MSDE. These database engines require preparation and database expertise. They may involve converting a Multi Central db. These db engines are also designed to hold a larger number of records. A database administrator or network administrator installs a database server on your network. To create a db, you may need to know the database password. If use of this password is restricted, let the database administrator either create the new Multi database from your machine, or run Admin on the Multi SA's PC to create the database from there.

### Consulting MIS personnel

The Multi SA may need a database administrator to advise on or decide upon the database (db) engine used in your Multi system.

## Tip

**Multi SAs are not required to have database expertise, nor train for it.**

## Using Another Db: Converting

There may be other databases...

Your Multi SA may have created more than one Multi db. Operators have the option of switching to another Multi db.

### To Use Another Multi Db

1. Start Admin (or View). The Logon window appears.
2. In the Central Database section, leave or switch the database (Access or SQL-Server) by clicking its button.
3. Type the name of the Multi db that you need.
4. In the User ID box, type an account name that is in the Multi db selected in the previous step.
5. In the Password box, type the password to the account input in step 4.
6. Click **OK**.

Fig. 14-3. Specifying the Multi Db.

To switch to another Multi db, change the central database (Multi db) name.



**Take care when typing the name of a database in the Admin logon window.**

Typing a name of a non-existent database starts the Admin database tool. See Creating a Multi Db, below.

#### Default

Once you have set Admin to use a Multi central database (Multi db), the same Multi db is used every time that you log on.

#### Converting a Multi database from SQL to Access

A SQL Server database can hold many more alarms than an MS-Access database. To convert a SQL database to an Access format, Honeywell recommends removing alarm data from the SQL database beforehand.

## Impact on View

- View can be set to a different Multi db while Admin is running, and vice versa.
- When switching to another Multi db for use with View, a fresh local Multi db overwrites the local db used at the previous log on.
- Typing the name of a non-existent database in the View logon window is of little consequence. Acknowledge the error message and type the name again.

## Creating a Multi Db

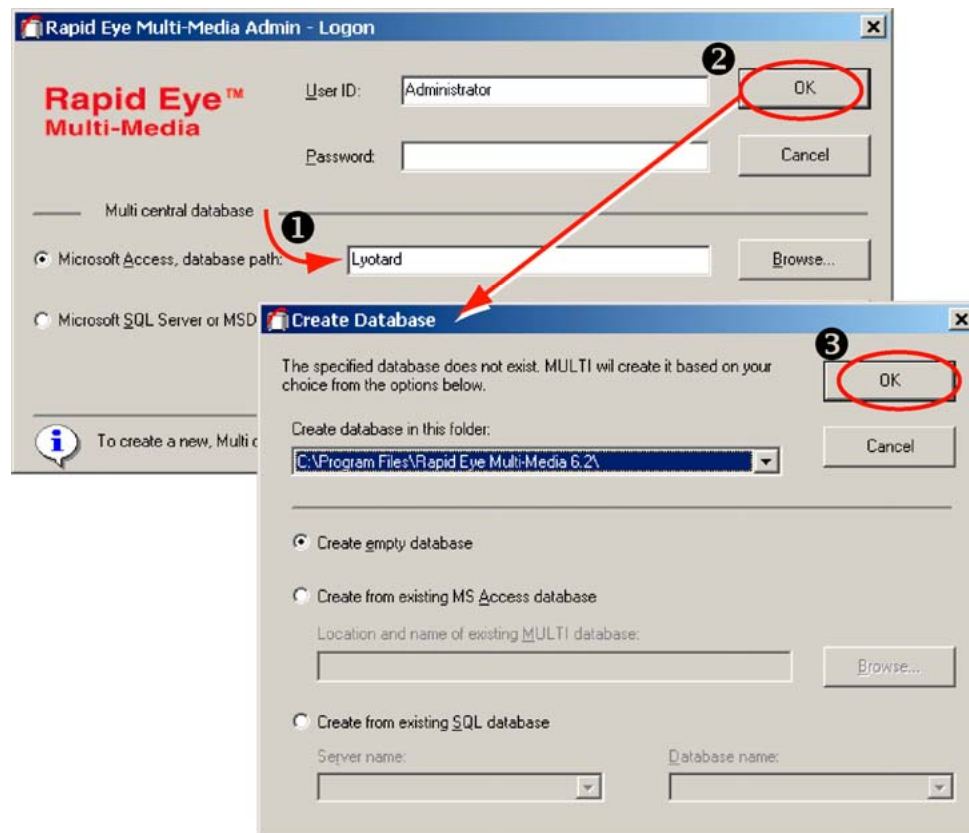
### Tip

Creating a Multi db is a rare occurrence. Only one Multi db is needed for all of the Rapid Eye sites in your system. Honeywell recommends using the default REMCentral.mdb if you plan to use only one Multi database. The installers of your system may have already created a Multi db to test the installation.

### Using the Admin - Logon window to create a database

If the installers did not supply you with their Multi db, you can use Admin to create an empty Multi db instead of logging on.

Fig. 14-4. The Admin Logon Window.



To obtain an empty Multi central database, either:

- For an MS-Access compatible format, see To Create an Empty, MS-Access-Compatible Multi Db, below
- For a SQL-Server compatible format, see SQL-Server Template, p. 237.

#### Following log on to Admin

The next time that you use Admin, the same Multi db is used.

#### And what about the Local Db?

When users run View, a partial copy of the Multi db (Local db) is made to that PC's hard drive.

## Tip

### Creating a Multi db is a rare occurrence.

Though you can create another Multi db at any Admin log on, there is no need to do so. The Multi db name is usually left unchanged during regular use of Admin. Only one Multi db is needed for all of the Rapid Eye sites in your system.

## Naming Restriction

### Multi db naming restriction

When choosing a name for your Multi db, there are restrictions. Do not use:

- A user name. Names that you will need for a user of the Multi db. A Multi db with the same name as a user account causes an error when View is started.
- "Administrator". It is the name of the default user in any Multi db.

### User naming restriction

When adding users to the database, do not use the "[database name]" as a user name. A user account with the same name as the database causes an error if a copy of the database is made locally. For other Naming Restrictions, see p. 156.

## To Create an Empty, MS-Access-Compatible Multi Db

You do not need a copy of Microsoft Access to use this procedure. Everything is included with your copy of Rapid Eye Multi software.

1. Start Admin. The procedure to do so is on p. 232, in the Starting Admin section.
2. In the Admin Logon window, leave or type "Administrator" in the User ID box.
3. Leave the Password box empty. An empty database lists one default user: "Administrator". By default, this user has no password. There is more information about the default user in section Administrator Password on p. 176.
4. Leave the Multi Central database to "Microsoft Access".
5. First-time logons can proceed as is. Either:
  - First run. You have the option of naming the database and selecting its path.
  - Subsequent runs. Change the name of the database file. This instructs the database tool to create an empty database bearing the name that you typed.

6. Click **OK**. The Create Database window appears; see fig. 14-4, above. Note that "Create empty database" is selected.
7. Click **OK**. The Admin window appears. A default site is listed on the Sites tab. There is an "Administrator" user listed on the User tab.

#### Database naming: restrictions

Do not use: (a) a name that you will need for a user of that Multi db; or (b) "Administrator". It is the name of the default user in any Multi db. A Multi db with the same name as a user account causes an error when View is started.

## SQL-Server Template

#### Asking your SQL database administrator for help

An Admin user may find it useful to ask a SQL-Server database administrator for help when creating a SQL-Server compatible Multi db. SQL-Server may have been configured using customized folder names. This can hamper creating an empty Multi db remotely, without the help of a database administrator. Admin can even be installed on the database administrator's PC.

#### Security option

By default, Multi software connects to a SQL server using the "sa" login, with no password. To add security, your SQL administrator can setup a SQL login just for Admin users. See Multi Database Security, on p. 165.

#### Intended users

Of the two procedures in this section, the next one is for your SQL-Server database administrator; the last one can be used by an Admin user, with the help of a SQL database administrator.

#### Security consideration

On some installations, the Multi db may need to be protected from copy and deletion (see Multi Database Security on p. 165).

## An Empty Multi Database Using Microsoft SQL-Server

This procedure is for a SQL-database administrator, not an Admin user.

1. Copy two files to the SQL-Server database folder:
  - REMTemplateV3-1.mdf
  - REMTemplateV3-1.ldf
2. The default, SQL folder name and path are: "C:\MSSQL7\Data\". The number in the file name is not related to the version of the software or hardware used. Rename the files to a name of your choice, for the Multi db, such as "Multi.mdf" and "Multi.ldf". Renaming is necessary to not restrict use of the template files, to create another Multi db at some future time.
3. Run Query Analyzer, an MS SQL-Server tool. This tool is not supplied with Multi; it is a standard SQL-Server tool.
4. Connect to the SQL-Server server.

5. Type this code, including the commas:  
`sp_attach_db 'Multi',  
'C:\MSSQL7\Data\Multi.mdf',  
'C:\MSSQL7\Data\Multi.ldf'`
6. Execute the code by pressing F5, or using the "Execute" command.

## Using Admin to Create a SQL-compatible Multi Database

1. Before using Admin to connect to a SQL-Server server, your SQL database administrator provides you with:
  - A SQL account and password. The SQL Administrator logon is "sa" by default, but it and its password may have been changed.
  - The SQL-Server server name
  - Share name of the folder that will hold the Multi db.
2. Ensure that a SQL-Server client is installed on the PC used to connect to a SQL-Server server.
3. Start Admin. The Admin Logon window appears.
4. In the Admin Logon window, leave or type "Administrator" in the User ID box.
5. Leave the Password box empty. An empty database lists only one user: "Administrator". By default, this account has no password. See the information about the default user in Administrator Password on p.176.
6. Click "Microsoft SQL". Your next step depends on which Windows operating system is running your PC.
  - Users of Microsoft Windows 2000 or XP. You have the option of clicking Scan, to locate SQL-Server servers in your network neighborhood. The scan takes some time to perform on shared drives. If the scan is ineffective at locating the server you need, you can try the next option, even if it is designed for other versions of Windows.

- or -

  - Users of Win98se; or if a scan was ineffective. Type the name of a SQL server in the Server name box. Your organization's database administrator can help you find this name.
7. Click the arrow in the Database Name box to see the database names that are in use. To create a database type a name that is not in use in Database Name.
8. Click **OK**.
  - If the name was typed in, a scan is performed, regardless of the Windows operating system on your PC.
  - If SQL-Server security has been changed, a SQL log on window appears, as discussed in section SQL-Server Option on p. 165. Type in a Login and Password obtained from your database administrator; then click **OK**. The Create Database window appears (see fig. 14-4). Note that Create empty database is selected.
9. Click **OK**. In the Admin window, a site is listed on the Sites tab; an "Administrator" user listed on the User tab.

## Db Based On Another

### Similarities

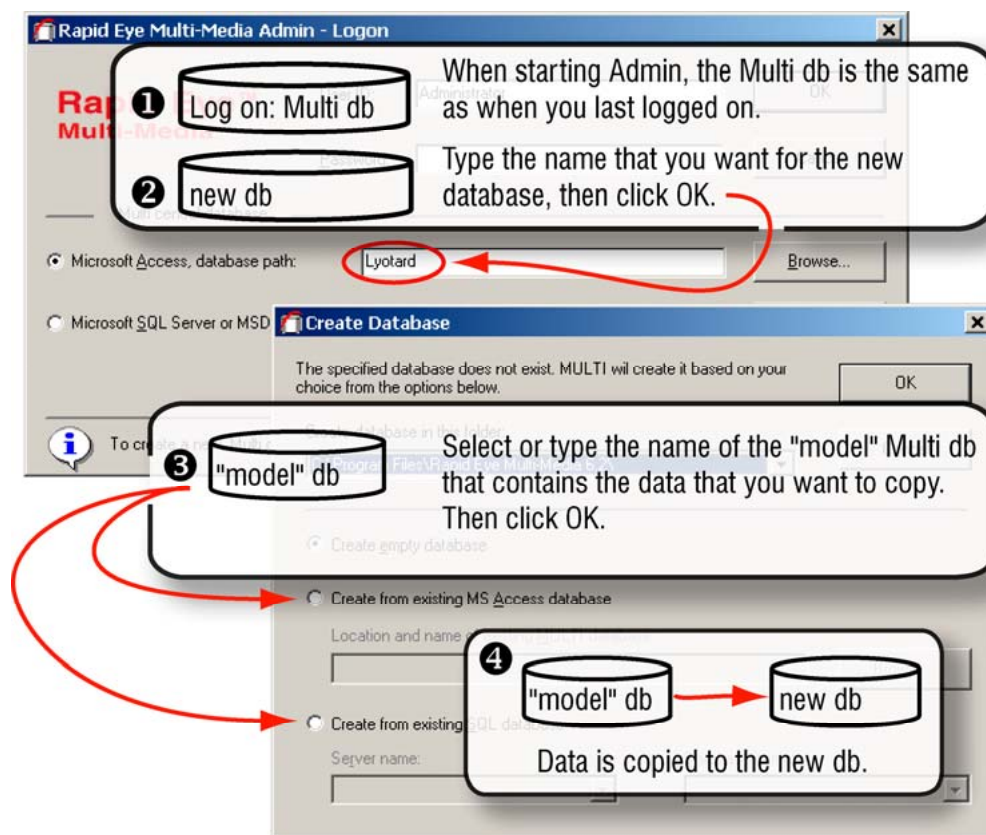
To copy a Multi db, use the Admin - Logon window as a database tool. The procedure is similar to creating an empty Multi db.

The Create Database window is used to select a "model" Multi db (see step 3 in fig. 14-5, below). You need an account and password to the model database to log on to the copy of the Multi db.

### SQL-Server

When making a copy of a SQL database, a network scan is made. This can be time consuming. If you know the name of the server and database, it is quicker to type them.

Fig. 14-5. Copying Multi Db Data to another Multi Db.



## To Make a Copy of a Multi Db

1. Start Admin.
2. Leave or type the name of an account that has the right to use Admin, in the database that you plan to copy.

## Tip

### Step 2 for making a copy of a db is not obvious.

Your usual account may not work in the database that you plan to copy. If you use the database's "Administrator" account, the password may differ from the "Administrator" account in the Multi db that you usually use.

3. Leave or type that account's password.
4. Select the database engine that will read the Multi db that you plan to create.
5. Replace the name of the database with a new name. You can also change the path, folder and server name, as needed.

## Tip

### For Windows 98 users using MS-SQL Server or MSDE, a database server name must be typed.

The database server(s) cannot be automatically identified and listed at log on.

6. Click **OK**. The Create Database window appears. See fig. 14-5, above.
7. Select either:
  - Create from existing MS-Access database. Type or browse for the location and name of a \*.mdb file.
  - or -
  - Create from existing SQL database. Select a server and type a database name of a \*.mdb file.
8. Click **OK**. The new database is created based on the data in the model db; the Admin window appears. The information that you see is a copy of the model database.

## Renaming a Multi Db

You can rename a Multi db using standard Windows techniques. For example, use Windows Explorer to locate a \*.mdb file and rename the file as you would any other.

### Multi db naming restriction

## Tip

### The file name of a local db is "<userid>.mdb".

This is why the [name of a Multi db] should not be the same as one of its users.

When adding users to the database, do not use the "[database name]" as a user name. A user account with the same name as the database causes an error when a copy of the database is made locally.

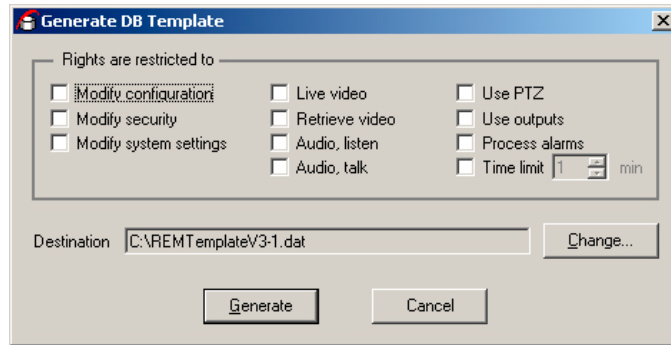
## Multi Db: MinAdmin

### Template

For Administrators of client MinAdmin software, there is a Generate Template command in the File menu. The command is used to provide central databases for MinAdmin software. The template imposes restrictions on: rights of MinAdmin's Administrator account, administration of system password and access to the Multi db used to create the template.



Fig. 14–6. Options for Generating a MinAdmin Multi Db Template.



You can produce \*.DAT files for MinAdmin users. Use of the .DAT file and the template is discussed in the *MinAdmin User Guide*.

## Upgrading a Multi db

### Upgrades from v4 to v5 are automatic

You don't have to know what version of Multi software you are upgrading, only that a message appears for upgrades from earlier versions of v2 or v3 software, as explained in the next procedure.

**Tip** Downgrading a Multi db is not supported.

## Upgrading a Local Database

### Purpose of a local database

When View runs, it uses a partial copy of the Multi db. The copy is stored on the PC's drive. The local database can be updated (refreshed) if the PC running View is connected to the Multi db.

**Tip** A local database is upgraded automatically when the user of View has an open connection to the Multi db. If the connection is not available (laptop PCs, temporary setups and so on), use the information in this section.

### Mobile users

You can upgrade View's local db without connecting to the Multi db.

## To Upgrade a Local Database, without a Connection to the Multi Db

1. Before upgrading View, use Windows Explorer to locate the [user].mdb file(s) on the PC. For example, if a user account called "night operator" is used to log on to View, look for a "nightwatch.mdb" file. These files need to be moved after the Multi software upgrade.
2. After installing the upgrade to View, move every [user].mdb file (that you located in step 1) to the latest installation folder.
3. Start View. As each user logs on for the first time to the upgraded View, a dialog box appears stating that the local database needs an upgrade.
4. Click Yes. The [user].mdb file is upgraded, after being backed up to [user].bak.

### Tip

On PCs used by many accounts, there is a [user].mdb file for each account.

## Producing a Local Database

### Obtaining a local database, not connected to Multi db

Your Multi SA can deliberately make it impossible for operators to connect to a Multi db when using MinAdmin. Your Multi SA may then elect to provide View Operators with a computer file of the local database. The next procedure indicates how to make a local database from a command line.

### Tip

Before using a command line to create a local multi database, please run Admin once before doing so. If not, an error results.

## To Make a Local Database

1. Check if View has run on the PC you are using; if you are unsure, run View and exit.
2. Using Windows, run a command line utility and type: remadmin.exe "[name of user account]". The double-quotes are needed only for spaces or non-alpha-numeric characters, such as an apostrophe. This produces a [name of user account].mdb file.
3. Distribute the \*.mdb file to the View Operator. The user needs to copy the file to the folder holding the View.exe file. See the examples, below.

### Examples

acceptable

```
d:> remadmin.exe "O'Donnell #4"
```

```
d:> remadmin.exe ODonnell4
```

error

```
d:> remadmin.exe O'Donnell #4 // double-quotes are needed.
```

## Logging On

### For routine use of Admin

After specifying a database, Admin and View will continue to use it, each time that you log on. Logging on to Admin is a simple matter of starting Admin (as explained in Starting Admin on p. 232) and clicking **OK**.

### Tip

To log on to Admin, use either:

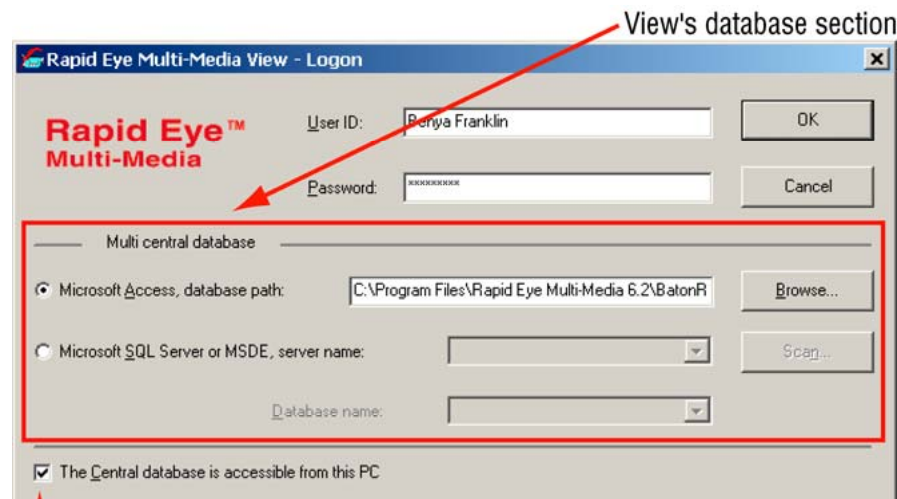
- (a) the Administrator account, or
- (b) an account with the "Use settings from Administrator" property.

### The "first use" exception

On first use, you are offered an empty, default Multi database. To obtain a Multi central database, see Obtaining a Multi db on p. 232.

## View: Setting the Db

Fig. 14-7. The Log On to View.



↑ on a mobile PC, leave this box empty

### The first time that you use View...

The View operator needs to set View to use a Multi central database (Multi db).

### Tip

**For mobile PCs that will not have access to the Multi db, have the multi SA connect the PC at least once to the Multi db and have that user log on.**

When a different Multi db is used at View's logon, the local db is overwritten with contents from the most recent Multi db.

## To Set a Multi Db for View

1. Start View.
2. Set the database. Either:
  - The PC can only run View. Select the database engine and type or browse for the name of the database file. For SQL Server or MSDE databases, indicate the server and database.
  - The PC can run Admin or View. View's Log On window automatically displays the database selected to run Admin.
3. Leave a checkmark in the checkbox next to The Central database is accessible from this PC. You should uncheck this box after one successful logon only if a PC is stand alone or mobile. Leave or type your user account name in the User ID box.
4. Type your password in the Password box.
5. Click **OK**.

### For routine use of View

Unless another Multi db is set, View continues to use the same Multi db, every time that someone logs on.

## Tip

**For PCs running Admin and View, View's Log On window automatically displays the database selected using Admin.**

The User ID and Password are authenticated once in the Multi db; afterwards, the local database is used.

### Local Multi database

The local db contains a subset of the Central db data: the information for sites that the user is authorized to use.

## Refreshing a Local Database

### Purpose

If changes are made to the Central Multi database, and it is accessible from the PC running View, the local database is refreshed automatically when you login to View. Security and site information is updated.


The local database can be refreshed by View Operators, at the request of a Multi SA, for:

- PCs that run View 24/7
- or -
- PCs that are stand-alone and only occasionally connected to a Multi Central database.

## To Refresh a Local Database while Running View

1. Run View. At the Logon, check if there is a checkmark in the checkbox next to The Central database is accessible from this PC.
  - If so, proceed with the logon.
  - If not, check with your Multi SA if the PC used to run View can connect to the PC or server holding the Multi Central database. In the affirmative, check the checkbox next to The Central database is accessible from this PC.
2. While View is running, operators can either:



- Click  on the View toolbar.
- or -
- Click the Refresh command on the View menu.

If procedure To Refresh a Local Database while Running View fails, see your Multi SA.

## Deleting a Database

You can delete a Central database at any point. Note that after deleting a Central database, users can still connect to sites, using their local database. Attempting to refresh the local db causes an error after the Central db is deleted.

### Protecting the Multi db

On some installations, the Multi central database (Multi db) may need to be protected from copy and deletion. See Multi Database Security on p. 165.

## “Cannot Open Db”

Can be the result of:

- Deleting a Multi central database (Multi db)
- Unavailability of a network connection to the Multi db.

### Tip

**Check the network's status. When using Admin, this error has the side effect of creating a new, central database that has the same name as the regular database.**



# Index

## A

Access. See Multi db, Microsoft Access

access point. See password, access point

account for user. See user account

ACUIX dome camera: camera identification, 102; configuration, 100; discovery, 100

ACUIX PTZ driver. See Intellibus PTZ driver

ADEMCO PTZ driver. See Javelin 308

Admin (software): before installing, 163; documentation, 163; for low security use, 162; granting access to, 180; in open installation, 162; limiting use to Multi SA, 163; security options, 161; starting, 232; use in secure environment, 163; used to create Multi db, 235

Administrator account, 151; after password is set, 177; changing password, 177; Honeywell recommends, 152; password, 152, 177, 235; password and Multi SA, 164; password as clearing storage safeguard, 131; password optional, but recommended, 61, 164; security precaution, 177; setting password, 177; to create Multi db, 235; user based on, 177

Administrator, used as account name, 156

alarm. See event

alarm callback: connection. See connection (to alarm station) and alarm station; dial-up customization, 211; dial-up through an exchange, 213; listing after interruption, 219; using RAS, 216

alarm log. See event log

alarm panel, 194

alarm port, 137, 202, 216

alarm station: customizing dial-up, 213; default telephone number, 52; dial-up connection, 203; dial-up connection using RAS, 216; dial-up to RAS server, 217; local call across area codes, 213; long distance call in an area code, 213; modifying phone number of..., 52; multiple, 218; notification speed, 195; port. See alarm port; preparations, 201, 202; prioritizing, 49; priority for callback, 50; removing, 219; right to use, 202; specifying not to use, 51, 220; when first adding, 209

area code: status, alarm station (table), 211

asterisk: customized telephone number for alarm station, 52; password box, 164; search rule, 145

audio: disabling for LocalView, 149; Eagle audio, 149; LocalView, 148; sound card, 147

## B

B&B Smart Switch. See PIT

bag image, for camera sabotage detection, 122

base port, 45, 47, 49, 137

blinding a camera. See camera sabotage detection

blurring a camera. See camera sabotage detection

Boost button, 104

boosting values for recording video. See event recording

Bossware PIT driver, 88

breach of trust. See security risk

## C

callback(s). See alarm callback

camera: adjust all, 66; adjust video feed, 66; brightness, as security risk. See security risk and camera sabotage detection; detection, automatic, 65; disable, 66; duo of, 79; groups of, scheduling, 107; obstructing. See security risk and camera sabotage detection; rename, 83; scheduling, 108; spot check live, 84; spot check recorded video, 84

camera address: PTZ, 86

camera sabotage detection, 184; alarms, 122; calibration, 122; optional, 120; setup, 121

camera-day (unit), 128

categories: of events, 187

central user management. See user management, central

character: in regular expression, 145; password length, 164

Clear Storage button: security risk, 131, 180; where found, 129

clearing storage: Administrator account password, 131; safeguard, 131, 177; security risk, 180; tracing start of, 131

## Index

client IP, 139

clock: clearing storage, 60; Multi-Media unit, 56; on a PC, 59; Refresh button, SNTP server, 58; setting automatically, 58; setting manually, 59; setting to automatic, 57; setting to correct time, 55; synchronizing over dial-up, 59; troubleshooting, 60

comma: delay in dial-up connection, 215

communications settings: to change, 136

computer name, Multi-Media unit. *See* DHCP

connection (to alarm station): defining (table), 203; information needed (table), 204; using RAS, 216

connection (to Rapid Eye site): auto-naming example (table), 48; auto-naming of, 48; compulsory when adding site, 29; dial-up consistency, 33; dial-up customization, 51; naming, 29; network and dial-up alternative, 43; network default (table), 36; primary connection, 44; RAS and dial-up, 44, 47; renaming, 48; to view connections, 48; various connections (table), 29

continuous recording: resolution preview, 74; set to OFF. *See* security risk

Continuous video recording: enabling, 68; no video recording message, 190

CONTROL OUTPUT: external PTZ controller, 86; FAULT RELAY, 134

crane, 116

CSD. *See* camera sabotage detection

customer-device: adding one..., 143; defining, 143; messages, 143; recording data, 143; regular expression, 145; rules, 143; to add a rule..., 144

Customer-device: event. *See* event, Customer-device

cutting password to Clipboard, 164

Cyberdome, Kalatel. *See* Kalatel

**D**

darkness. *See* security risk *and* camera sabotage detection

dartboard control, PTZ, 88

data device. *See* customer-device

[database name], used as account name. *See* user account, restricted names

database administrator, 165, 237

date, security risk. *See* security risk

default: logon to Admin (table), 233; user account, 152, 177, 235

delay: motion detection, 118

delay dial speed. *See* dial-up connection, delay...

deny access: to all sites, 159

Describe Rule command, 113

detecting sabotage. *See* camera sabotage detection

dew and frost. *See* security risk

DHCP (dynamic host configuration protocol), 42; computer name, 42; DNS and DHCP server, 35; dynamic IP Address, 42; Microsoft Server 2000 (or 2003), 41; OFF by default, 41; serial number, 35; server without DNS, 35; static IP Address, 42

dial-up connection (to Rapid Eye site): area code challenge, 32; delay dial speed, 213, 214; fooling Microsoft, 32; multiple lines, 34; network connection, combining with, 43; number needed (table), 34; to force local call, 33; to force long distance call, 32; to specify..., 31

direct sunlight. *See* security risk *and* camera sabotage detection

documentation, limiting distribution, 163

double-quote, in password, 164

download: file from Multi-Media unit, 132

duty cycle: event recording, 71

dynamic host configuration protocol. *See* DHCP

## E

Eagle audio, 149

employee timesheet, motion detection, 116

environment interfering with video, 84

Estimated Storage Capacity, 71

event: alarm, deferred report, 195; alarm, immediate report, 195; archiving alarms, 230; by category (table), 119, 189, 190; Customer-device, 105, 143, 187, 188, 189, 190, 191; disarming alarm using alarm schedule, 109; four categories of, 187; has no effect, 187, 191; *Multi-Media Unit*, 187, 190, 191, 192; *Outside World*, 105, 119, 161, 187, 190, 191, 230; printing list of alarms, 229; record an. *See* event, set to be logged; report an. *See* event, set to trigger alarm; set to be ignored, by operator, 191; set to be logged, 187; set to trigger alarm, 187, 188; system. *See* event, Multi system; tracing, 191; *View Operator*, 187, 190, 191, 192

event log: deleting items in, 230



event recording: Boost button, 104; during a Site tour, 104; duty cycle, 71; enabling, 68; optional, 103; response duration, 115; rule, 112; rule description, 113; schedule, 115; trigger, 112

explosion, motion detection, 116

external controller, PTZ, 86

external modem: to set..., 139

## F

FAULT RELAY, 63, 134, 194, 195

file: downloading from Multi-Media unit, 132; uploading to Multi-Media unit, 133

fire, motion detection, 116

firewall ports, 45, 47, 49, 54, 137, 202, 216

first preset, PTZ, 92, 93, 94

folder (Rapid Eye): assign site to, 26; create, 26; delete, 27

## G

gauntlet strategy, 79

general purpose output. *See* CONTROL OUTPUT

good image, for camera sabotage detection, 122

GPO. *See* CONTROL OUTPUT

group of sites, 26

## H

hardware: to control public display monitor, 141

HCU484, Honeywell dome. *See* Honeywell Fixed Camera PTZ driver

high security, 163

higher mask, 117

holidays: priority in scheduling, 110

Honeywell: database engine, support for, 231; guideline or recommendation, 33, 169; system password, and, 167; unit of compression, 126

Honeywell Fixed Camera PTZ driver, 88

Honeywell recommends: Administrator account, 152; area codes be included in telephone numbers, 33; changing the system password, 162; dialing same country setting, 209; entering long distance codes, 210; how to deny access, 198; tips to prevent jeopardizing performance, 184; to secure a site..., 61

host IP, 139

human resources officer, 161

## I

image quality (compression): Rapid Eye unit, 126

images per second (ips), 70

individual, identifying. *See* security, presence or identification

installing: before, 163; Multi db, used for, 232; software, Admin, 20

Intellibus: ACUIX camera, 99; PTZ driver, 88

interfering with video, environment, 84

internal modem, 138

IP address: Multi-Media unit, 136; networked alarm station, 202

IP Port, 37, 206

ips. *See* images per second

## J

Javelin 308/ADEMCO PTZ driver, 88

jeopardized performance. *See* security risk

## K

Kalatel domes, 93

Kalatel PTZ driver/Cyberdome, 88

KD6. *See* Ultrak PTZ driver

KD6i dome. *See* PTZ:Ultrak KD6i

key personnel: database administrator, 165, 237; human resources officer, 161; network administrator, 35, 45, 47, 54, 136; security officer, 87, 152, 161; when creating a site, 24

kitchen grease. *See* security risk *and* camera sabotage detection

KTD 312. *See* Kalatel

## L

LAN, 136

LAN IP, 37

last valid password. *See* system password, LVP

learning, for camera sabotage detection, 122

## Index

limiting access: Admin documentation, 163

lit room at night. *See* security risk

local database: update, 169

local user management. *See* user management, local

LocalView: audio, 148; breach of trust, 186; setup, 23

log: viewing and sorting, 227

Log System Messages. *See* Multi-Media unit, system log

log, system. *See* Multi-Media unit, system log

logging an event. *See* event, set to be logged

long distance prefix: changing default, 215

low security. *See* open installations

LVP. *See* system password, LVP

## M

maintenance: messages (table), 64, 120

maintenance port, 54, 137

maintenance session: for system password, 168; how to start..., 54; right, modify configuration, 180; right, security, 180; right, system settings, 180; scheduling tasks (table), 63; security risk, 197; tasks (table), 181, 185; user account rights (table), 181, 185

maintenance tabs: Monitor Out (figure), 142; Serial Devices, 138; Statistics, 128; System Configuration, 134; System Files, 132

manufacturer password, 167

masking: higher area, 117

Microsoft Access. *See* Multi db, Microsoft Access

Microsoft SQL-Server. *See* Multi db, Microsoft SQL-Server

Microsoft Windows: Clipboard, 164; screen area, 82

MinAdmin Multi db template, 240

modem: external, 139; internal, 138; internal, default settings (table), 139; PPP networking settings (table), 139

monitor, 82

Monitor Out tab: figure, 142

MONITOR OUTPUT 1: public display monitor, 142

monitor, for high resolution, 82

monitoring: operator error, 191; power outage, 191

motion detection: burglary, 116; crane, 116; delay, 118; masking, 117, 118; optional, 116; PTZ, 93, 94; sensors and, 116; setup, 117

moving a camera. *See* camera sabotage detection

moving a Multi-Media unit: changing settings, 136; clearing storage, 129; clearing stream, 130

MSDE. *See* Multi db, MSDE

Multi: alarm station. *See* alarm station; Customer-device. *See* event, Customer-device; Multi-Media Unit event. *See* event, Multi-Media Unit; Outside World event. *See* event, Outside World; security. *See* security; sockets, 137

Multi db (central database): and local Multi database, 28, 235; creating at log on, 235; creating empty SQL-Server..., 165, 238; creating MS-Access..., 236; creating SQL-Server..., 237; empty (figure), 235; for installation, 232; making a copy, 240; Microsoft Access engine, 233, 236; Microsoft SQL-Server engine, 165, 233, 237, 238; MSDE engine, 233; providing MinAdmin template, 240; refreshing local db, 245; reuse of, 243; security of, 165, 245; setting for View, 244; switching to another, 234; upgrading local without central, 242

Multi SA (system administrator): account. *See* Administrator account; alarm session user, defining, 189; alarm station, preparations, 201, 202; as sole user of Admin, 163; defining a Customer-device event, 143; downloading Multi-Media unit system log, 132; network administrator, and, 202; other SAs, limiting number of, 163; PPP information need, 162; rights of, 192; scheduling Maintenance (table), 63; security deployment, 161; security officer, and, 152; setting time zone on Multi-Media unit, 57; site connection overview (table), 29; synchronizing clock on Multi-Media unit, 56, 59; tasks (table) for Maintenance, 181, 185; users, before adding accounts, 152; View operators, and, 189, 202

Multi-Media LT: resolution gauge, 81

Multi-Media unit: adding, when system password in use, 172, 174; clock. *See* clock, on Multi-Media unit; computer name. *See* DHCP; downloading file from,, 132; identification, 134; moving, 129, 130, 136; removal, and removing system password, 171; removing system password, 171; removing system password from all, 170; serial number, 134; serial port, 143; site connection overview (table), 29; system log, 132, 134; uploading file to, 133; version number, 134

Multi-Media unit operator: account and PPP, 196;  
 account limiting access to sites, 182; account  
 password. *See* user password; account, denying  
 access to, 131, 196; account, restricted names, 156;  
 account, to delete..., 160; Administrator account,  
 151; alarm, 187, 195; alarm station, 202, 203; as user,  
 151; clear storage, 131; customer device, 143; in  
 many dial-up areas, 34; lengthy spotting video, 117;  
 LocalView, 151; Modify Configuration right, 188;  
 obtaining an account, 155; password to user account,  
 164; PTZ use, 87; RAS, 47; RAS password and  
 username, 44; rights. *See* user account rights; rogue,  
 131, 196; security, 159; sound at PC, 147; time zone  
 conflict, 57; unauthorized, 131, 196; uploading file to  
 unit, 133; View-only user, 163

## N

name: stream, to change, 130

NAT (network address translation): IP Port, 37, 206;  
 LAN IP, 37, 206

netBIOS name. *See* DHCP

network administrator, 35, 45, 47, 54, 136

network connection: alarm station, to..., 205; dial-up  
 connection, combining with, 43; Rapid Eye site,  
 default (table), 36; Rapid Eye site, to..., 136

network name. *See* DHCP

new device. *See* serial device

noise: background, 148; loud alarm, 148; rush-hour,  
 148; stadium crowd, 148

NTSC: incompatible with PAL, 180; Multi-Media LT, 81;  
 setting, 135

## O

object, identifying. *See* security, presence or  
 identification

open installations: Admin, 162

Orbiter dome, 88

Outside World event. *See* event, Outside World

## P

PAL: incompatible with NTSC, 180; Multi-Media LT, 81;  
 setting, 135; video archive shorter than NTSC, 126

pan. *See* PTZ

panning: PTZ and video archive, 94

parallel phrasing for naming sites, 25

parameters: system password, 169

password: access point, 163, 195, 201; access point,  
 features, 163, 195, 201; Administrator. *See*  
 Administrator account; box, 164; copying or cutting to  
 Clipboard, 164; deleting, 164; features, 164; file, 164;  
 for group, 164; length, 164; optional, 164;  
 parameters, 164; pasting, 164; PPP, 196; removing.  
*See* deleting, and resetting; repeated use, 164;  
 resetting, 164; setting, 164; system. *See* system  
 password; typing twice, 164; unique, 164; user. *See*  
 user password; using text securely in, 164

passwords, 164

pasting a password, 164

Pelco P/D PTZ driver/dome, 88

PIT (Protocol Interface Translator), 146

Point to Point Protocol. *See* PPP

port 6. *See* FAULT RELAY

power outage. *See* security risk

PPP: password precedence, 44; temporary network, 139

presence of individual or object. *See* security,  
 presence or identification, *See* security, presence  
 or identification

preset 1, PTZ. *See* PTZ, first preset

prevent access. *See* limiting access

primary connection: to make a connection a..., 43

priority: security (table), 162

Protocol Interface Translator. *See* PIT

PTZ: at close of session, 93; auto-focus, 94; auto-iris,  
 94; camera address, 86; CONTROL OUTPUT, 86;  
 dartboard control, 88; driver, 63; end of session  
 behavior (table), 94; external controller, 86; first  
 preset, 92, 93, 94; motion detection, 93; preset  
 tour, 94; rubber-band control, 90; security officer,  
 87; serial device, 86; Ultrak KD6i restriction, 93, 94;  
 When Live Closes, 87; zonal mode, 89, 91

public display monitor: hardware control of., 141;  
 MONITOR OUTPUT 1, 142

## R

RapidDome, 88

RAS server: in connection definition, 45; need to use, 47;  
 to connect to alarm station, 216

recording video. *See* continuous recording and event  
 recording

Refresh button, SNTP server, 58

regular expression, 145

resetting password, 164

resolution: gauge, 79, 81; preview for recording, 75; preview recorded video, 74; selection tips, 75

resolution best, 79

restricted names, user account, 156

retrieval: slow rewind, 70

rogue session: ending. on network, 197

rubber band control, PTZ, 90

rule: event recording, 113

rules: customer-device, 143; data-recording, 144

running, for camera sabotage detection, 122

rush-hour, 148

## S

sabotage. *See* camera sabotage detection

scheduling: camera, 108; customizing for a camera, 107; groups of cameras, 107; optional, 105, 109

screen area, monitor, 82

secure site, 169

security: additional, 162; Administrator password, 177; alarm log (table), 230; alarm notification, 195; alarm use, 189; basic, 177; before adding users, 152; central database. *See* security, Multi db; denying access, 131, 196; event. *See* event; event, by type (table), 119, 189, 190; events, by type (table), 119, 189, 190, 191; limit use of Admin, 163; low, 162; Maintenance and, 53; maintenance tab, 131, 220; maximum, 162; Multi central database, 162; Multi db, protecting, 165, 245; Multi SA and, 152, 161; optional, 49, 161, 163, 165, 166, 178, 191, 195, 201; password features, 164; password, point-of access, 163, 195, 201; presence or identification, 75, 77; priorities (table), 162; PTZ dome and, 87; RAS server, 162, 196; rights, 178; rogue user, 131; setting an alarm, 187; site tour, 221; suggestions, 161; system files, 132; system status (table), 28, 169; tracing events, 191; Update security, 131, 220; user password, 176; your organization's, 161

security officer, 161, 163; account rights, 185; Multi-Media unit system log, 132

security risk: breach of trust, 185; camera brightness, 185; camera recording set to OFF, 185, 186; camera spot check, recorded video, 84; camera, spot check live, 84; checklist, 184; Clear Storage button, 131, 180, 186; countermeasure, 185; darkness, 84; dew and frost, 84; direct sunlight, 84, 184; environmental interference, video, 84; jeopardizing performance, 184; kitchen grease, 84; lit room, at night, 84, 184; maintenance session, 197; many Multi databases, 185, 186; obstructing a camera, 84, 184; preventive measures, 184; system password, 197; time/date, 185; to alarms, 186; UPS/power outage, 84, 184; vandalism, 84, 184, 185

security,risk. *See* security risk

self, used as account name. *See* user account, restricted names

SensorMatic dome, 88

serial communications: customer-device, 143

serial device: new, 86; PTZ, 86

serial devices: maintenance tab, 138; PTZ, 140

serial number, Multi-Media unit, 42, 55

setting: database to recognize a used unit's (other) system password, 175, 176; password, 164

site, 24

site (Rapid Eye): delete, 27, 28; denying access, 179; follow-up, 25; key personnel, 24; limit access, using user account, 182; naming, 24; not protected, 169; prioritizing an alarm station, 50; protected, 169; road map, 23; that an alarm station not be used, 51, 220; to name..., 27

site tour: changing duration of, 224; changing site order, in a tour, 223; configuration, 221; preparations, 221; security, and, 221; selecting connections for, 225; two or more units needed, 221, 224, 225

Smart Switch, B&B. *See* PIT

SNTP Server. *See* clock

socket, Multi. *See* firewall, ports

sockets, Multi and firewall, 137

software version: unit, 55

sound card, 147

soundscape, 148

spot check: video, 84

spot checking: audio, 148

SQL-Server. See Multi db, Microsoft SQL-Server

stadium crowd, 148

star. See asterisk

statistics: maintenance tab, 128; storage, to view..., 128

status: system password (table), 169

storage: cleared, to trace..., 131; clearing, 129; prevent clearing of, 130; statistics, to view..., 128; stream, 129

stream: changing name of, 130

synchronizing unit time to PC, 57, 59

system: FAULT RELAY, 134; LAN/WAN, 136; NTSC/PAL, 135; pulse. See FAULT RELAY

system configuration: maintenance tab, 134

system files: maintenance tab, 132

system monitoring. See FAULT RELAY

system password, 169; and new Multi-Media unit, 172; deleting a site by mistake, after, 175, 176; effect, 169; LVP (last valid password), 174, 185; Multi SA's responsibility, 164; Multi technical support, 167; old, 169; optional but recommended, 61, 166; optional, but recommended, 164; removing from all units, 170; removing from one unit, 171; security risk, 197; setting, 167; status (table), 169; step 2 of 3, copying to Multi-Media unit, 168; step 3 of 3, updating users, 169; to limit user access, 151; used Multi-Media unit, and, 174; using other Multi db, 172

## T

table: area code status, alarm station connection, 211; connection to alarm station, Multi SA, 204

TCP ports: alarm, 137, 202, 216; base, 45, 47, 49, 137; maintenance, 54, 137

technical support. See Multi, technical support, See Multi, technical support

technical support, Multi-Media, 22, 58, 61, 128, 133, 134, 164, 167, 175, 185, 186

Template, Generate for MinAdmin, 240

test pattern, 141

tilt. See PTZ

time zone: Multi-Media unit, 57

time zone conflict, 57

time, security risk. See security risk

timesheet, motion detection, 116

toll-free numbers, to customize, 213

tour. See site tour, public display monitor and PTZ preset tour

triggering an alarm. See event, set to trigger alarm

## U

Ultrak PTZ driver, 88

unit: serial number, 55

unit operator: LocalView account, 157

units: camera-day, 128; compression, Honeywell, 126

unwanted user, 131, 198

upload: file from Multi-Media unit, 133

UPS. See security risk

user account name, restriction, 156

user account rights: Admin, for using, 180; assigning, 179; based on other, 159, 179; denying, 179; denying access to all sights, 159; denying site, 179; guidelines, 179; Maintenance, for using, 180; optional, 178; removing, 179; site access, for using, 182; View, for using, 181; viewing, 179

user management: Admin software, 153; central, 154; central and LocalView, 155; local, 154; older units, 153

user password, 164, 176; after assigning to user, 176; after setting, 176; changing, 176; optional, 164; setting, 176

user rights. See user account rights

## V

vandalism. See security risk *and also* camera sabotage detection

vermin, 116

video archive: 24/7, 125; audio, 124; frame rate, 125; higher recording values, 127; PTZ, 126; Quality setting, 125; recycling, 122, 123; resolution, 126; scheduling, 125; scheduling camera, 106; Storage Estimator, 123; too short, 123

video capture card: public display monitor, for, 142

video recording. See continuous recording and event recording; set to OFF. See security risk

View: use in secure environment, 163

View Operator event. See event, View Operator

**W**

WAN, 136

WAN IP, 37, 206

watch dog. See FAULT RELAY

When Live Closes, PTZ, 87

Win 98, 240

Windows: dial-up networking, 33

**Z**

zonal mode, PTZ, 89, 91

zoom. See PTZ













Honeywell Video Systems (Head Office)  
2700 Blankenbaker Pkwy, Suite 150  
Louisville, KY 40299, USA  
[www.honeywellvideo.com](http://www.honeywellvideo.com)  
☎ 1.800.796.2288

Honeywell Security Australia Pty Ltd.  
Unit 5, Riverside Centre, 24–28 River Road West  
Parramatta, NSW 2150, Australia  
[www.ademco.com.au](http://www.ademco.com.au)  
☎ +61.2.8837.9300

Honeywell Security Asia Pacific Ltd.  
33/F, Tower A, City Center, 100 Zun Yi Road  
Shanghai 200051, China  
[www.security.honeywell.com/cn](http://www.security.honeywell.com/cn)  
☎ +86 21.2527.4568

Honeywell Security Asia  
Flat A, 16/F, CDW Building, 388 Castle Peak Road  
Tsuen Wan, N.T., Hong Kong  
[www.security.honeywell.com.hk](http://www.security.honeywell.com.hk)  
☎ +852.2405.2323

Honeywell Security France  
Parc Gutenberg, 8, Voie La Cardon  
91120, Palaiseau, France  
[www.honeywell.com/security/fr](http://www.honeywell.com/security/fr)  
☎ +33.01.64.53.80.40

Honeywell Security Italia SpA  
Via Treviso 2 / 4  
31020 San Vendemiano  
Treviso, Italy  
[www.honeywell.com/security/it](http://www.honeywell.com/security/it)  
☎ +39.04.38.36.51

Honeywell Security España  
Mijancas 1.3a Planta  
P.Ind Las Mercedes  
28022 Madrid, Spain  
[www.security.honeywell.com/es](http://www.security.honeywell.com/es)  
☎ +34.902. 667.800

Honeywell Video Systems Northern Europe  
Network 121  
1446 WV Purmerend, The Netherlands  
[www.SecurityHouse.nl](http://www.SecurityHouse.nl)  
☎ +31.299.410.200

Honeywell Video Systems UK Ltd.  
Aston Fields Road, Whitehouse Ind Est  
Runcorn, Cheshire, WA7 3DL, UK  
[www.honeywellvideo.com](http://www.honeywellvideo.com)  
☎ +0844 8000 235

Honeywell Security South Africa  
Unit 6 Galaxy Park, 17 Galaxy Avenue,  
Linbro Park, P.O. Box 59904  
2100 Kengray, Johannesburg, South Africa  
[www.honeywell.co.za](http://www.honeywell.co.za)  
☎ +27.11.574.2500

Honeywell Security Deutschland  
Johannes-Mauthe-Straße 14  
D-72458 Albstadt, Germany  
[www.honeywell.com/security/de](http://www.honeywell.com/security/de)  
☎ +49.74 31.8 01.0

Honeywell Security Poland  
Chmielewskiego 22a, 70–028  
Szczecin, Polska  
[www.ultrak.pl](http://www.ultrak.pl)  
☎ +48.91.485.40.60

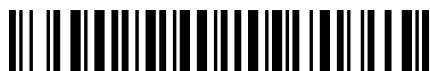
Honeywell Security Czech Republic  
Havránkova 33, Brno  
Dolní Heršpice, 619 00, Czech Republic  
[www.olympo.cz](http://www.olympo.cz)  
☎ +420.543.558.111

Honeywell Security Slovakia Republic  
Vajnorská 142, 83104 Bratislava  
Slovakia  
[www.olympo.sk](http://www.olympo.sk)  
☎ +421.2.444.54.660

# Honeywell

[www.honeywellvideo.com](http://www.honeywellvideo.com)  
+ 1.800.796.CCTV (North America only)  
[HVSsupport@honeywell.com](mailto:HVSsupport@honeywell.com)

© 2005–2007 Honeywell International Inc. All rights reserved. No part of this publication may be reproduced by any means without written permission from Honeywell Video Systems. The information in this publication is believed to be accurate in all respects. However, Honeywell Video Systems 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.



**Document K14392V1 Rev A – 07/07**

## Free Manuals Download Website

<http://myh66.com>

<http://usermanuals.us>

<http://www.somanuals.com>

<http://www.4manuals.cc>

<http://www.manual-lib.com>

<http://www.404manual.com>

<http://www.luxmanual.com>

<http://aubethermostatmanual.com>

Golf course search by state

<http://golfingnear.com>

Email search by domain

<http://emailbydomain.com>

Auto manuals search

<http://auto.somanuals.com>

TV manuals search

<http://tv.somanuals.com>