CathexisVision 2022.1

Setup Manual

005-20220419-396 13 June 2022

Contents

1. Installation 11
1.1 Getting started with CathexisVision 12
1.1.1 CathexisVision 2022.1 Release Notice 12
1.1.2 Product interoperability and support 13
1.2 Requirements and Restrictions 14
1.2.1 Supported Operating Systems 14
1.2.2 Windows Update Requirements 15
1.2.3 Hardware Requirements 15
1.2.4 Routing/Port Requirements 16
1.3 Anti-virus Exclusions 18
1.3.1 Folders to exclude from CathexisVision 2018 and later 18
1.3.2 Complete list of folders to exclude 18
1.3.3 Third-party Anti-virus real time scanning on CathexisVision clients 19
1.4 Installation 20
1.4.1 Follow the Installation Wizard 20
1.4.2 Cathexis Windows Performance Wizard 21
1.4.3 Finish Installation 23
1.4.4 Log in 23
1.5 Licensing 24
1.5.1 Trial License 24
1.5.2 Licensing from a Local Unit 24
1.5.3 Licensing from a Remote Unit 26
1.6 Create and Manage Sites 27
1.6.1 Site Explained 27
1.6.2 Open the Enterprise Manager 28
1.6.3 Create and Organise Sites into Folders 28
1.6.4 Absent Units 32
1.7 The Site List 'Edit' Menu 33
1.7.1 Make or Clear a Resources Site 33
1.7.2 Organise Sites into Folders 33
1.7.3 Highlight Level 34
2. Setup Tab: General Site Setup 35
2.1 Introduction 36
2.1.1 Setup Tab Access Rights 37
2.2 General Site Setup 38

2.2.1 Configure Archiving 39
2.2.2 A Note on Multicast 42
3. Setup Tab: Users 44
3.1 Update Notice 45
3.2 Introduction 46
3.3 Create New User 47
3.4 LDAP 48
3.4.1 LDAP Settings 48
3.5 Non-admin Users with Access Rights to Configure Users 50
4. Setup Tab: Configure Servers 51
4.1 Configure Servers 52
4.1.1 Server Options 52
4.1.2 General Tab 55
4.1.3 Email Tab 56
4.1.4 Audio Tab 57
4.1.5 Communications Tab 57
4.1.6 Gateway Tab 58
4.1.7 Configuration Backup Tab 59
4.1.8 Base-Stations Tab 60
4.1.9 User Recordings Tab 60
4.2 Cameras 62
4.2.1 Secure Camera Connection and Control 62
4.2.2 Adding Cameras 63
4.2.3 Edit Existing Camera 78
4.2.4 Right-click on a Camera 82
4.2.5 Video Analytics Button 83
4.2.6 Reference Images 83
4.3 Video Analytics 86
4.3.1 Accessing Video Analytics: two methods 86
4.3.2 Copy-Paste Analytics 87
4.3.3 Configure New Analytics 88
4.3.4 Analytics Configuration Interface Guide 91
4.3.5 Basic VMD 97
4.3.6 Smart VMD 101
4.3.7 Basic, Intermediate, and Advanced Analytics 103
4.3.8 Basic Object Classifier 117

4.3.9 Queue Length Analytics 125
4.3.10 Still Object 126
4.3.11 Mask detector 129
4.3.12 Basic people proximity 132
4.3.13 Thermal face temperature 133
4.3.14 Counting Analytics 137
4.3.15 Motion Database (tab) 143
4.3.16 Licenses (tab) 145
4.4 Databases 146
4.4.1 Add a Database 146
4.4.2 Edit an Existing Database 148
4.4.3 Alerts 151
4.4.4 Manage Storage 152
4.4.5 Import a Database 153
4.4.6 Video Ageing 154
4.5 Schedules 158
4.5.1 Add / Edit a Schedule 158
4.5.2 Set Schedule Recording Times 158
4.6 Network I/O 159
4.6.1 Analogue 159
4.6.2 Network 160
4.7 Scheduled Recordings 162
4.7.1 Add / Edit a Scheduled Recording 162
4.7.2 Right-click Menu 163
4.7.3 Copy Paste 163
4.8 Motion Recordings 164
4.8.1 Locate Motion Recording 164
4.8.2 New Motion Recording 164
4.8.3 Events 166
4.9 Scheduled Archives 167
4.9.1 Archive Video Manually 167
4.9.2 Description 167
4.9.3 New Scheduled Archive Window 167
4.10 Events 170
4.10.1 CathexisVision Events Metadatabase 170
4.10.2 CathexisVision System Events Window 178

4.10.3 New Events Window Interface 179
4.10.4 General Settings Tab 180
4.10.5 Triggers Tab 180
4.10.6 Actions Tab 188
4.10.7 Resources Tab 194
4.11 Monitors 196
4.11.1 General Settings 196
4.11.2 Monitors Tab on a Base Station 196
4.11.3 Adding a Monitor 197
4.11.4 Access 198
4.12 Access Rights 199
4.12.1 Tabs 199
4.13 Technical Alarms 203
4.13.1 General Settings 203
4.13.2 Add / Edit a Technical Alarm 204
4.14 Virtual Inputs 207
4.14.1 Add a Virtual Input 207
4.15 Keyboards 208
4.15.1 Recording Server 208
4.15.2 Base Station 208
4.16 Integration Devices General Settings 209
4.16.1 Integration Database 209
4.16.2 The Integration Devices Panel 211
4.16.3 Important Considerations 213
4.17 Analogue Matrix 215
4.17.1 Add / Edit an Analogue Matrix 215
5. Setup Tab: Resources 216
5.1 Resource Panel Configuration 217
5.1.1 Resource Panel Setup 217
6. Setup Tab: Site Actions 219
6.1 Site Actions 220
6.1.1 Creating a Site Action 220
6.1.2 Site Action Types 220
6.1.3 Adding a Site Action to an Event 221
6.1.4 Adding a Schedule to a Site Action 221
7. Setup Tab: Reports 222

7.1 Introduction **223**
7.2 Controls **224**
7.2.1 Add, Edit or Delete 224
7.2.2 Schedule 224
7.2.3 Fetch 225
7.3 Create Report **226**
7.4 Cameras Report **227**
7.4.1 Camera Report Example 227
7.5 Database Usage Report **228**
7.5.1 Database Usage Report Example 228
7.6 Disks Report **229**
7.6.1 Disks Full Report Example 229
7.6.2 Disks Exceptions Report Example 230
7.7 Environment Report **231**
7.7.1 Environment Report Example 232
7.8 Events Report **233**
7.9 File System Report **234**
7.9.1 Hardware Report Example 234
7.10 Hardware Report **235**
7.10.1 Hardware Report Example 235
7.11 License Features Report **236**
7.11.1 License Features Report Example 236
7.12 Licenses Report **237**
7.12.1 Licenses Report Example 237
7.13 NTP Queries Report **238**
7.13.1 NTP Queries Report Example 238
7.14 Reboots Report **239**
7.14.1 Reboot Report Example 239
7.15 Recording Times Report **240**
7.15.1 Recording Times Report Example 240
7.16 Software Report **241**
7.16.1 Software Report Example 241
7.17 System Report **242**
7.17.1 System Report Example 242
7.18 System Setup Report **243**
7.18.1 System Setup: Camera Recording Setup Report Example 243

7.18.2 System Setup: Encoder Setup Report Example 243
7.19 Unit Up-Time Report 244
7.19.1 Unit Up-time Report Example 244
7.20 User-Defined Report 245
7.20.1 User Defined Report Example 245
7.21 VMX Counters Report 246
7.22 VMX Temperature Report 247
7.23 Windows Unit Report 248
8. Setup Tab: Failover Servers 249
8.1 Failover Introduction 250
8.1.1 Model 250
8.1.2 Licensing 251
8.1.3 Recommendations 252
8.1.4 Minimising Failover Loss 252
8.1.5 Limitations 252
8.1.6 Example 252
8.2 Setup 254
8.2.1 Introduction 254
8.2.2 Requirements 254
8.2.3 Configuration 254
8.3 System Restore after Failover 259
8.3.1 Restoring a Site Master Recording Server 259
8.3.2 Restoring a Site Slave Recording Server 259
9. Setup Tab: Adjacent Cameras 261
9.1 Introduction 262
9.2 Setup 263
9.2.1 Interface 263
9.2.2 Map Cameras 264
9.2.3 Page Manager 266
10. CathexisVision GUI Setup 267
10.1 Introduction 268
10.1.1 Supported Languages 268
10.1.2 Minimising the GUI 268
10.2 Command Line Options 269
10.2.1 Connect Client to Alarm Gateway 269
10.2.2 Set Number of Monitors 269

10.2.3 Add Multiple CathexisVision GUIs 269
10.2.4 View Legacy Archive Viewer 269
10.3 Send Text Message when Alarms are Received 270
10.3.1 Supported Platforms 270
10.3.2 Settings Files Location 270
10.3.3 Configure Notifying Alarms 271
10.3.4 Configure Text Message Device 274
10.4 Menu Bar 275
10.4.1 File Menu 275
10.4.2 Edit Menu 276
10.4.3 View Menu 276
10.4.4 Site Menu 277
10.4.5 Video Wall Menu 280
10.4.6 Tools Menu 283
10.4.7 Settings Menu 284
10.4.8 Help 289
10.5 Status Bar 290
10.6 Monitors Tab 291
10.6.1 Open a Site on a Screen 291
10.6.2 Sequence 292
10.6.3 Sequence Manager 292
10.6.4 Sequence Editor 293
10.6.5 Salvo 293
10.6.6 Virtual Cameras Interface 294
10.6.7 Individual Panel Settings 295
10.7 Cameras Tab 296
10.7.1 Statistics and Information 296
11. CathexisVision Forensic Tool 297
11.1 Forensic Tool 298
11.1.1 Data Values Used 299
11.1.2 Date / Time Selection 299
11.1.3 Graph Window 300
11.1.4 Selected Views 302
11.1.5 Quick View 305
11.1.6 Examples of How to Interpret the Graph and Columned Values 306
Appendices 309

Appendix A: Configure Custom CatMobile http listening Port 310

Windows 310

Ubuntu 311

Appendix B: TCP vs UDP for Video Surveillance 312

Appendix C: Configuring failover features 314

Index 315

While Cathexis has made every effort to ensure the accuracy of this document, there is no guarantee of accuracy, neither explicit nor implied. Specifications are subject to change without notice.

1. Installation

1.1 Getting started with CathexisVision

This Setup Manual guides the user through the procedure of installing and configuring the CathexisVision software. Installation of CathexisVision software requires one installation file for the NVR and one file for the Client.

The software works on a licensing format. Users can install the whole package and unlock the features by using licenses. By updating the license, users can add functionality and features, such as integration or analytics.

This chapter guides users through the initial steps of the setup process. These steps are:

- Installing CathexisVision NVR, and / or the CathexisVision Client.
- Getting **licensed**.
- Creating a site with the **Enterprise Manager**.

Note: It is necessary to install the NVR and Client software on the respective units. However, an administrator can make all relevant changes to the site from either a client or NVR unit.

A NOTE ON CAMERA CHANNELS

The CathexisVision software packages have **limits on camera channels**. A multi-sensor camera is physically a single device (camera) but it requires a camera channel for each one of the internal cameras. The same applies to an encoder: a 16-channel encoder will account for 16 camera channels on the CathexisVision software, even though it is a single device. Even when a camera or device only uses a single IP license, the camera channel limit will still apply.

1.1.1 CathexisVision 2022.1 Release Notice

The following updates were made in the CathexisVision 2022.1 software release. Please consult the ***CathexisVision 2022.1 Release Notes*** for full details):

- The Carbon user interface is supported from CathexisVision 2022 onwards.
- The new CathexisVision mobile app is supported from CathexisVision 2022 onwards.
- CatObserver support has been added for Ubuntu 20.04 in CathexisVision 2022.
- CathexisVision 2022.1 has added the following video analytics features:
    - A trigger to the still object algorithm, for when a still object moves away.
    - Option to “classify on minimum motion”.
    - Human pose models.
    - Analytics models human_pose_estimation_fp32 and yolov4_tiny. Option to show overlay with only objects appearing in the classification lists selected in the triggers.
    - Option to overlay algorithm settings on reference images.
    - Local flare suppression and local noise suppression in object tracker algorithm.
    - Framerate option in option tracking analytics and basic object classifier.
- HTTP connections and HTML stats have been added to the API server in CathexisVision 2022.1.
- Multi-language supported has been added to Archive Viewer 2.
- CathexisVision now integrates with Nedap Access Control and Titan Weighbridge.

- Dahua PTZ has been reworked, and the "Area zoom" PTZ feature has been added.
- The videowall in CathexisVision 2022.1 has implemented pre-spooling of live video for salvos and sequences to improve the time to first frame when the feeds are switched. **Note**: this is for the new accelerated videowall. Pre-spooling is already supported in the old videowall.
- CathexisVision 2022 software can only connect to sites running CathexisVision 2018 and above.
- CathexisVision 2022 is the last release to support Windows 7, Windows 8, Windows 8.1 and Windows Server 2008 R2.

1.1.2 Product interoperability and support

Cathexis Technologies releases a new major version of the CathexisVision software annually. The software releases are named according to the year that they are in use (for example, CathexisVision 2017). The major software versions are usually released at the start of the third quarter of the preceding year. (For example, CathexisVision 2017 could be released in the third quarter of 2016.)

For a complete list of currently available licenses, please contact your Cathexis representative or consult the latest pricelist. For more information on CathexisVision licensing, refer to the ***CathexisVision Software Product Description and License Document***.

Please note the following regarding product interoperability and support:

1.1.2.1 Product interoperability

- All servers on a site should have the same product version installed (for example, CathexisVision 2017). Different product versions on the same site are not supported.
- The CatSite (CathexisVision) user interface will be able to connect to and view software running any service pack of the same version.
- The intention is for the user interface to be able to connect to a product one version earlier (such as CathexisVision 2017 connecting to CathexisVision 2016) but some features may not be available.
- The user interface may be able to connect to and view earlier products (2 or more versions earlier), but there are no guarantees – some or all features may not be functional.

1.1.2.2 Product support

- A product/software version will be supported with software updates until the end of the next calendar year. For example, CathexisVision 2020 will be supported until December 2021 (in 2020 and 2021).
- Product support during the first year will include periodic software service packs, containing bug fixes, minor features, and additional integrations and camera drivers.
- Product support during the second year will include periodic service packs, containing critical bug fixes and additional integrations and camera drivers.

USEFUL LINKS

*To view **tutorial videos** on CathexisVision setup, visit https://cathexisvideo.com/resources/videos*

*Find answers to Cathexis **Frequently Asked Questions**: https://cathexis.crisp.help/en/?1557129162258*

1.2 Requirements and Restrictions

Please download **CathexisVision** software to continue with this Setup Manual.

Note: there is a **minimum requirement of 4 Gigabytes of RAM** to run this software.

1.2.1 Supported Operating Systems

Supported operating systems apply to all contents of CathexisVision software installation, including:

1. CathexisVision software,
2. Map Editor,
3. Archive Viewer.

1.2.1.1 Not Supported

- Windows XP and earlier,
- Windows Vista,
- Windows Server 2008,
- Linux Fedora 16 (supported in CathexisVision 2018 and earlier),
- NetBSD.

1.2.1.2 Supported Linux Systems

- Ubuntu 16.04 LTS Desktop (64-bit)
- Ubuntu 20.04 LTS Desktop (64-bit)

1.2.1.3 Supported Windows Systems

- Microsoft® Windows® 7 SP1
- Microsoft® Windows® 8
- Microsoft® Windows® 8.1
- Microsoft® Windows® 10
- Microsoft® Windows® Server 2008 R2 SP1
- Microsoft® Windows® Server 2012
- Microsoft® Windows® Server 2012 R2
- Microsoft® Windows® Server 2016
- Microsoft® Windows® Server 2019

Note: CathexisVision 2021 is the last release to support Windows 32-bit installations.

CathexisVision 2022 is the last release to support Windows 7, Windows 8, Windows 8.1 and Windows Server 2008 R2.

1.2.2 Windows Update Requirements

Some systems require the Universal C Runtime Update. From CathexisVision 2017 onwards, updated Windows runtime libraries are used. This means that the Windows 10 Universal C Runtime update must be run on systems prior to Windows 10 (see list below).

Note: From CathexisVision 2018.3 onwards, Windows Vista and Windows Server 2008 are no longer supported. Thus, the update for 2018.3 does not apply to those systems. Windows Server 2008 R2 is still supported.

This update requirement applies to:

- Windows Server 2012 R2
- Windows 8.1
- Windows RT 8.1
- Windows Server 2012
- Windows 8
- Windows RT
- Windows Server 2008 R2 Service Pack 1 (SP1)
- Windows 7 SP1

Windows XP and earlier is not supported. Windows updates can be run, or the specific update KB2999226 may be run. The Windows 10 Universal C Runtime update can be downloaded from: https://support.microsoft.com/en-us/kb/2999226.

Running the KB2999226 update has prerequisites, and the user may first need to install:

- Windows Vista Service Pack 2 (download from https://support.microsoft.com/en-us/kb/935791)
- Windows 7 Service Pack 1 (download from http://windows.microsoft.com/installwindows7sp1)
- Windows Server 2008 Service Pack 2 (download from https://support.microsoft.com/en-us/kb/968849)
- Windows Server 2008 R2 Service Pack 1 (download from http://go.microsoft.com/fwlink/?LinkID=199583)
- Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 update
  - KB2919442 (download from https://support.microsoft.com/en-us/kb/2919442)
  - then KB2919355 (download from https://support.microsoft.com/en-us/kb/2919355)

1.2.3 Hardware Requirements

The **CathexisVision** software architecture is designed to efficiently use the various hardware system components. When choosing hardware, there are many system issues to consider. Some examples are:

- Camera resolution.
- **Camera bitrates** for recording.
- **Camera Frame rates** and resolution for “live” viewing.
- **Video Analytics**: is the I.P camera, or the **Cathexis** software used to perform Video analytics.
- Whether viewing cameras “**live**” from the same server on which recording is taking place.
- Whether “**multicast**” video streams are being streamed from the camera.
- **Storage** methodology (on-board, Network Storage etc).

1.2.3.1 Hardware Selection Guidelines

The table below provides guidelines to assist in choosing hardware for the application. The figures in the table were generated using the CathexisVision Design Tool.

Note: the following parameters were used to determine these guidelines:

1. These are conservative figures for recording servers only.
2. Live viewing not included in these numbers.
3. 3MP cameras with 3MP/24fps recording stream.
4. CIF/12fps analytics stream running Smart VMD.
5. External storage on a 1/10 Gbps network.

Note: These guidelines are not exhaustive. For assistance with the design, contact a distributor or a **Cathexis** regional office. Alternatively, navigate to cathexisvideo.com and use the Design Tool.

Processor	RAM (GB)	Server Storage throughput Mbps	No. of 3MP cameras per server
i7-7700k 4.20GHz	16	600	152
Xeon E3-1290 V2 3.70GHz	16	500	122
Xeon E5-1680 V4 3.40GHz	32	700	187
Xeon E5-2640 V2 2.40GHz	32	650	164
Xeon E5-2695 V3 2.30GHz	32	900	223
Xeon E5-2699 V3 2.30GHZ	32	1000	253

1.2.4 Routing/Port Requirements

The following router ports need to be opened on the network firewall / router / anti-virus. These ports are important in allowing several **Cathexis** services to run correctly.

1.2.4.1 Ports to Open

Operational Ports	Protocol	Application	Description
80	TCP	Default CatMobile Access	Port required to allow CatMobile client connection to server.
30010-30100	TCP	CathexisVision Software	Required ports for access to the CathexisVision software and associated configuration, live, and recorded view, etc.
30014	TCP	API (CathexisVision 2016 and previous versions) *	Required port to allow API connection to server when using software versions CathexisVision 2016 and previous.

			Note: Video also needs to be streamed from the server using TCP port 30010.
33104	TCP	API (CathexisVision 2017 and later versions) *	Required port to allow API connection to server when using software versions CathexisVision 2017 and later. **Note:** Video also needs to be streamed from the server using RTSP on TCP port 554.
*** For full list of API ports, please consult API help guide or contact support@cat.co.za**			

Maintenance Ports	Protocol	Application	Description
22	TCP	Secure Shell (SSH) - Linux	Port required to enable remote access to Linux server using Secure Shell network protocol.
3389	TCP	Remote Desktop – Windows	Port required to enable remote access to Windows server using Remote Desktop application.
NA	NA	TeamViewer or AnyDesk	Application for allowing remote access to a Windows server. No port required.

1.2.4.2 Remote Support

Please download and install one of the following programs relevant to the operating system to ensure remote support is available (see port requirements above).

Linux: Secure Shell (SSH - TCP port 22); **Windows:** TeamViewer AnyDesk, or Remote Desktop.

1.3 Anti-virus Exclusions

If running an anti-virus with active or real-time protection scanning enabled, certain CathexisVision folders need to be excluded from anti-virus scanning in order for CathexisVision to run correctly. The folders which need to be excluded are:

- CathexisVision **Server** installation folder.
- CathexisVision **Client** installation folder.
- Any folders, drivers, and volumes where **database**/s reside.

Note: All folders and paths referred to below are default installation folders – if the default folder option was not selected during installation, then locate and exclude installation folder/s from anti-virus scanning. The sections below indicate the default installation folders and paths which need to be excluded from scanning.

1.3.1 Folders to exclude from CathexisVision 2018 and later

For sites running CathexisVision 2018 and later, please exclude the following from anti-virus scanning:

CathexisVision Server	**Folders to Exclude**	
	32-bit	c:\program files (x86)\CathexisVision Server
	64-bit	c:\program files\CathexisVision Server
CathexisVision Client	32-bit	c:\program files\CathexisVision Client
Database folders/drives/volumes	Please locate and exclude.	

1.3.2 Complete list of folders to exclude

If the system uses a **global anti-virus** (meaning anti-virus protection is applied globally and not to individual units) and the different units in the site may have different installation folders, or if the **installation is prior to CathexisVision 2015**, then simply exclude **all** the default installation folders to avoid hassle.

Note: All folders and paths referred to below are default installation folders. If the default folder option was not selected during installation, then locate and exclude installation folder/s from anti-virus scanning.

CathexisVision Server	**Folders to Exclude**
	c:\program files\Cathexis CathexisVision Suite NVR
	c:\program files (x86)\Cathexis CathexisVision Suite NVR
	c:\program files\CathexisVision Server
	c:\program files (x86)\CathexisVision Server
CathexisVision Client	c:\dvs

	c:\program files\Cathexis CathexisVision Suite WRV
	c:\program files (x86)\Cathexis CathexisVision Suite WRV
	c:\program files\CathexisVision Client
	c:\program files (x86)\CathexisVision Client
Database folders/drives/volumes	Please locate and exclude.

1.3.3 Third-party Anti-virus real time scanning on CathexisVision clients

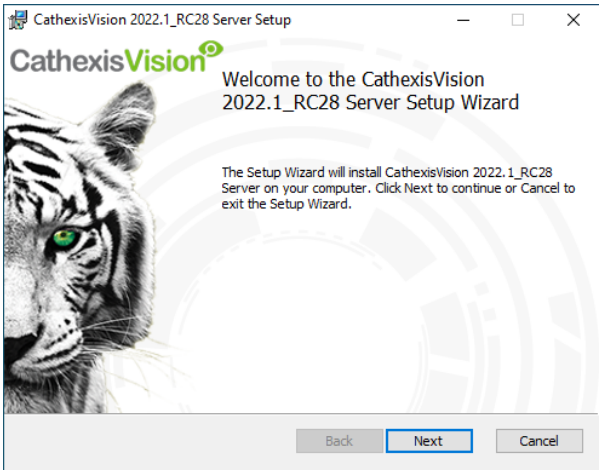
On a CathexisVision Client unit, the CathexisVision Server folder needs to be manually excluded from scanning by Windows Defender or other third-party anti-virus real time scanning components.

1.4 Installation

Installation is simple and intuitive. Double-click the installation file (.msi) to run the Installation Wizard.

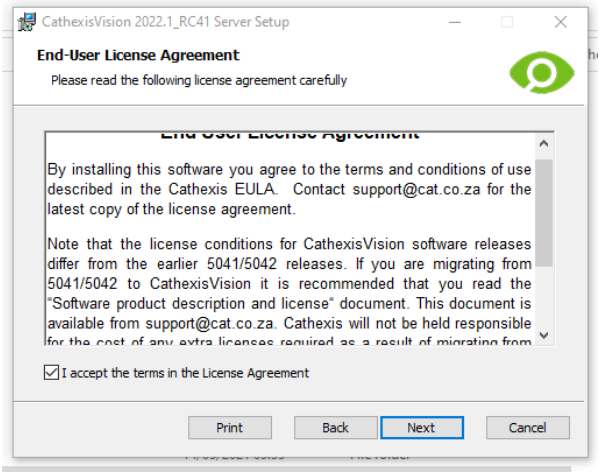
1.4.1 Follow the Installation Wizard

1



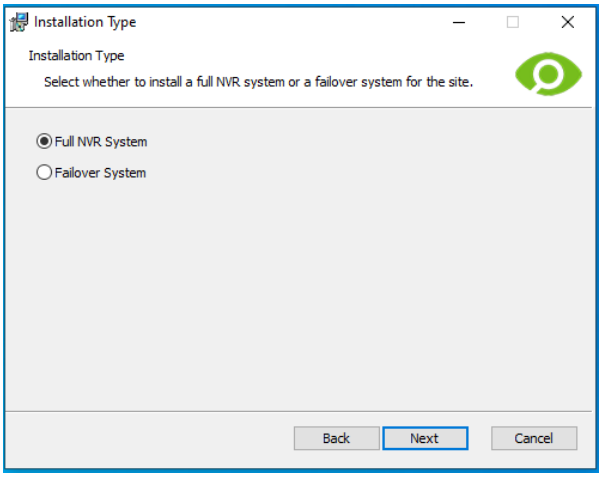
Click **Next**.

2



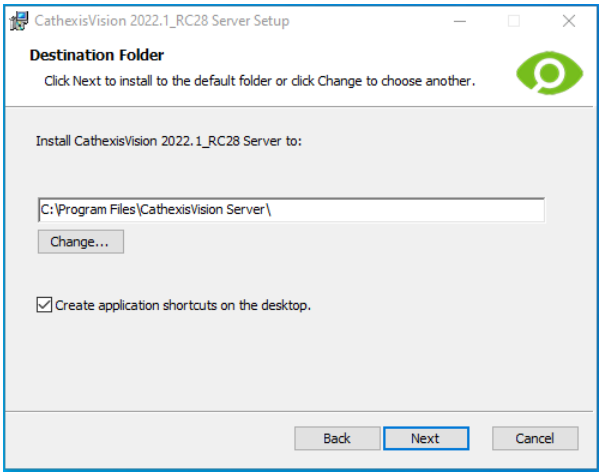
Accept the End User License Agreement.

3



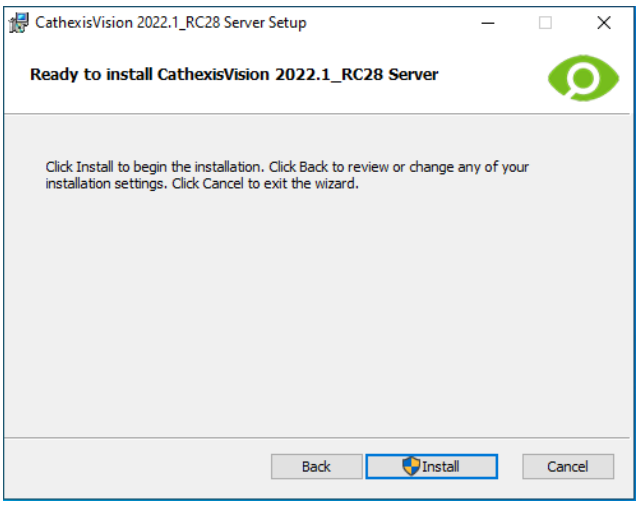
The user will be prompted to choose between a **Full NVR System** and a **Failover System** installation.

4



Choose the installation folder (this is best left as per the default section).

5



Click **Install**.

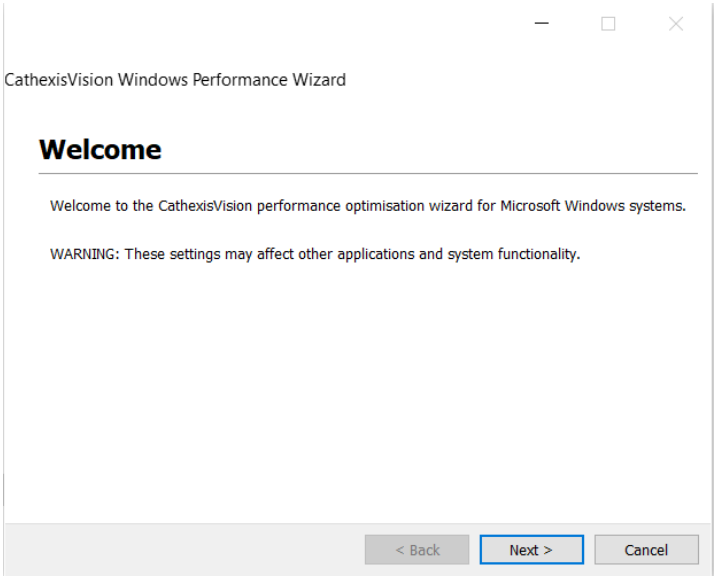
When the installation is complete, click **Finish**.

1.4.1.1 Failover Installation

If choosing the Failover installation, attempting to run CathexisVision (by double-clicking on the CathexisVision icon) will bring up the dialogue box:

Note: there is detailed information about Failover in the Setup section of this manual.

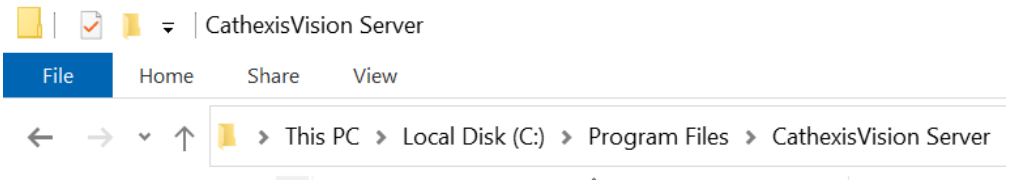
1.4.2 Cathexis Windows Performance Wizard

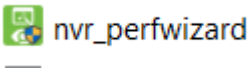


Leave the **Launch Performance Wizard** box selected. The Performance Wizard optimizes several Windows system settings for the use of **CathexisVision** software.

It should be run immediately, but it may be run any time after installation.

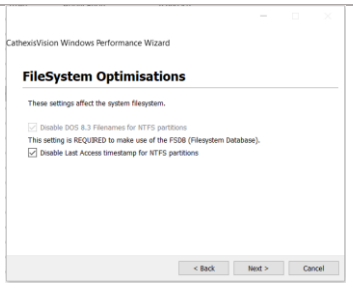
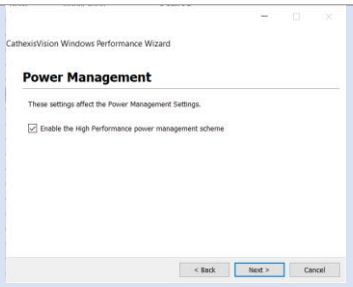
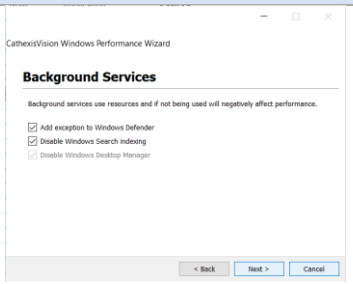
Note: If the Performance Wizard needs to be run again, the operator will need to navigate to the folder in which CathexisVision is installed. The image below shows the default location of the CathexisVision server installation.





In that folder, double-click on the file named **nvr_perfwizard.exe**. This will open the Cathexis Windows Performance Wizard.

The installer will show the current state of each setting. It presents the following options:

Category		Setting	Explanation	Action
Filesystem Optimisations		**Disable DOS 8.3 Filenames on NTFS partitions.**	This is a required setting for using the database engine.	Required
		Disable Last Access Timestamp for NTFS partitions	By default, when a file is accessed, NTFS writes information to record when the file is last accessed. To improve NTFS disk performance, disable the NTFS last-accessed timestamp.	Recommended
Power Management		**Enable the High-Performance power management scheme**	Adjusts Windows power scheme settings to ensure uninterrupted recording and live viewing.	Recommended
Background Services		**Add exceptions to the Windows Defender**	This will provide a performance gain for the caching and writing of video to the underlying software and database folder locations.	Recommended
		Disable the Windows Search Indexing	This provides a significant performance gain by preventing background indexing of the file system.	Recommended

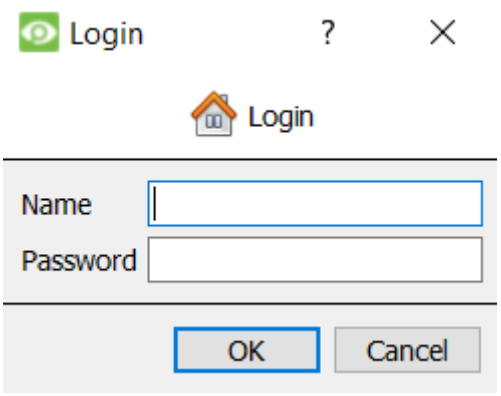
1.4.3 Finish Installation

Once finished with the Performance Wizard, click **Finish**. Installation is complete.

If there are any client stations, the user can install the **CathexisVision Client** software on them.

1.4.4 Log in

After installing, open the software and log in with the default login details.



Default login details

Username: admin

Password: admin

1.5 Licensing

The mode of licensing will depend on whether the license task is being performed on the local unit (the unit currently being worked on), or a remote unit (this being a viewing unit onto which a copy of the software has been installed). This section provides a guide for each situation.

For details on the licensing structure of CathexisVision, please consult the Software Product Description and License Document, or contact support@cat.co.za.

1.5.1 Trial License

Once CathexisVision is installed, a trial license is automatically applied to the system. To license the system further, consult the relevant licensing sub-section. Features of the trial license include:

- Two IP camera licenses.
- Maximum recording review time of two days.
- Standard CathexisVision basic analytics.

Trial licenses to unlock additional features may be requested by emailing support@cat.co.za.

1.5.1.1 Recording Review Time

With a trial license applied, only two days (48-hours) of recordings may be reviewed at a time. The camera will continue to record to a database (provided there is space, and the cameras have the requisite bitrates, etc.), but review of the recordings will be restricted to two days (48-hours) from the point of review. Apply the relevant IP camera licenses to unlock the database and review all recordings for as far back as the database has recorded.

1.5.2 Licensing from a Local Unit

The following instructions describe the process for licensing the unit that is **currently being worked on**. To license a **remote unit**, see the next section (Licensing from a Remote Unit).

1.5.2.1 Internet Connection: Product Key

If there is internet access and the vendor supplied a product key, enter the product key. The system will connect to the online licensing system and complete the process.

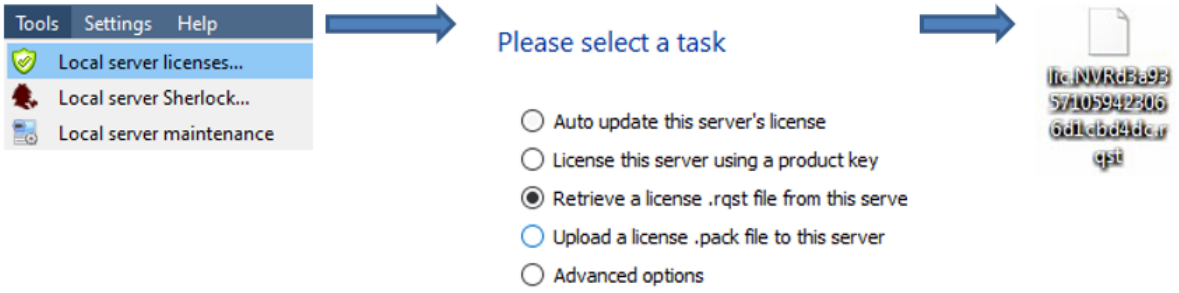
1.5.2.2 No Internet Connection: Pack File

If there is no internet access on the unit, a **.pack** file will need to be uploaded. A pack file is a file that contains all the licensing information for a unit. Send a **.rqst** file to Cathexis support at support@cat.co.za, who will then return a **.pack** file.

To receive the **.pack** file, please follow the instructions below.

1.5.2.2.1 License Request File

A .rqst file must be retrieved from the unit that needs to be licensed.



Email this .rqst file to Support, along with the information relevant to the licenses to be added to this unit.

1.5.2.2.2 Upload .pack file

The site should now be licensed. For further assistance, contact support@cat.co.za

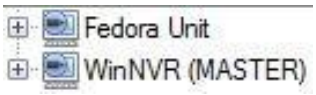
1.5.3 Licensing from a Remote Unit

When licensing from a remote unit (i.e. licensing a unit that is not the unit being worked on), the procedure is different. This is because clicking **Tools / Licensing** will license the unit currently logged in. To license remotely, do the following:

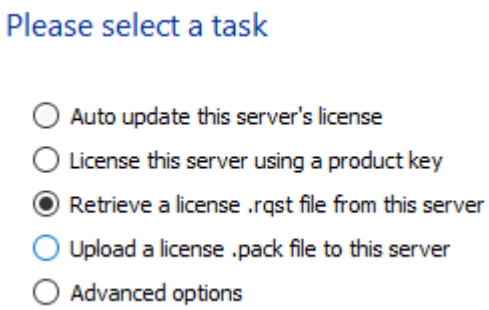
1.5.3.1 Open Configure Servers

To open **Configure Servers,** of the site currently logged into, follow this path from the menu bar: **Site / Open Tab / Setup.**

Once in the Setup tab, click on the **Configure Servers** icon.



Once **Configure Servers** is open, right-click on the individual unit that needs to be licensed and select **Licensing** from the drop-down menu.



After this, the licensing procedure is the same as following **Tools / Licensing** in the GUI of the local machine.

The options on the left will be presented.

This unit may be **Auto-updated** if it has already been licensed, or use a **Product Key** if one was provided.

To request a license, follow the procedure detailed above in the No Internet Connection section.

Note: Save the **.rqst** files, and upload **.pack** files to the storage media attached to the unit processing the license, not the one that is being licensed.

1.6 Create and Manage Sites

1.6.1 Site Explained

A **Site** brings multiple NVRs under a single software space, with one unit acting as a **Master,** and the rest considered **Slaves.** Connection to a site is via a site Master unit; this is the address to enter in the **Enterprise Manager** of the GUI.

Note:

- A server may not be a member of more than one site.
- When the CathexisVision server software is installed, the unit is automatically added to its own site.
- Therefore, when a site is located on a single, local unit, a new site does not have to be added.
- Units are added to a site. Cameras and Integrated Devices are added to the NVRs.

1.6.1.1 What does it mean to add a site?

It is important to understand that adding a site in the Enterprise Manager (dealt with below) is simply **adding a connection to an already existing site**.

This means that the only information that is contained in the **Enterprise Manager** is the name of the site, and the information the software needs to connect to that site.

Note: All edits to the site (addition of units, editing of individual NVRs, etc.) take place in **Site Menu / Open Tab / Setup / Servers.**

1.6.1.2 What is a Master Unit?

The first unit added to a new site will be considered the site **Master**. The master unit is the resource database for the site. It contains all the information relevant to the resources of that site.

Any server that forms part of the site can become a **Master** by assigning it the same IP address as the **Master**. This is because an exact copy of the site resource information gets stored on each server. This will help with failover **if** the Master unit goes down.

To make another unit the site master, change the IP addresses of the units (i.e. change the new master's IP address to that of the old master unit).

1.6.2 Open the Enterprise Manager

CathexisVision site management collects multiple units together as a Site. Sites are created and managed from the Enterprise Manager. Only administrators have access to the Enterprise Manager. Open CathexisVision and login when prompted. To open the Enterprise Manager:

Follow the path **File / Enterprise Manager**.

This will open a tab entitled **Site** List. This is the tab where sites are added and managed.

1.6.3 Create and Organise Sites into Folders

The Site list is in the panel on the left in the above image. When clicking on a site, the sites connection details are displayed in the panel on the right. **There are three steps** when adding a new connection to a new site:

1. Add a Site Name.
2. Add a connection to that site.
3. Fetch the ID of that site.

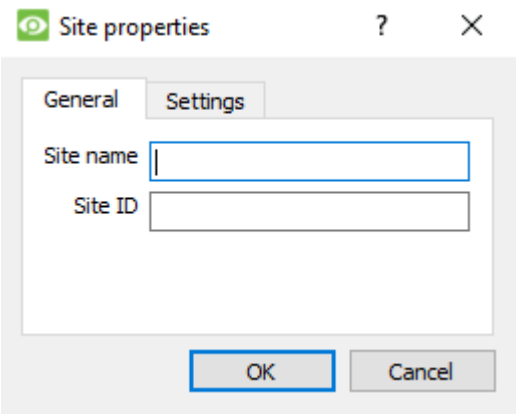
1.6.3.1 Add a Site Name

Here, the name of the site is added to the Site List. There are two ways to add a new site:

- Right-click on any white space in the **Site** list panel, and click **New Site**.

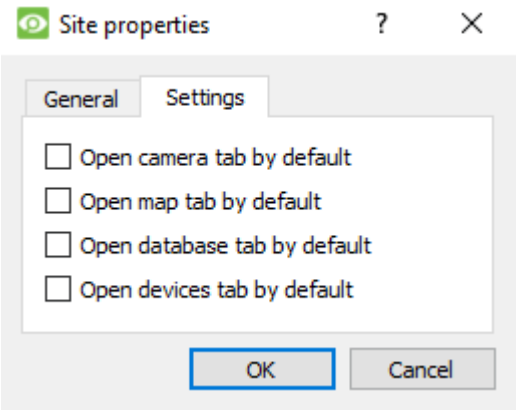
- Click on New Site in the Edit Menu.

This will bring up the **Site Properties** menu.



Under **General**, give the site a descriptive name.

Leave Site **ID blank** for now; this will be Fetched after adding a site connection.



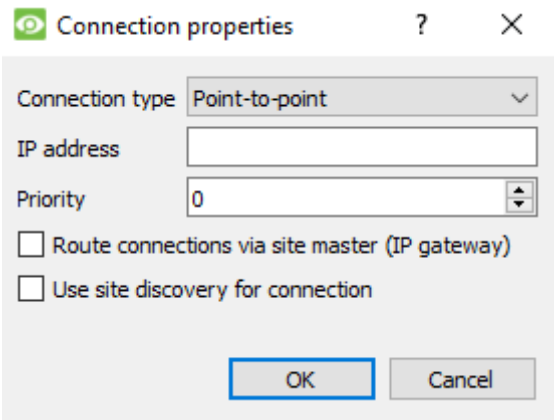
Under **Settings**, choose which tabs open when a site is opened (Cameras, Maps, Database etc.).

If the site is connected to a Gateway, there will be an Access tab. Here, specify Gateway User Levels.

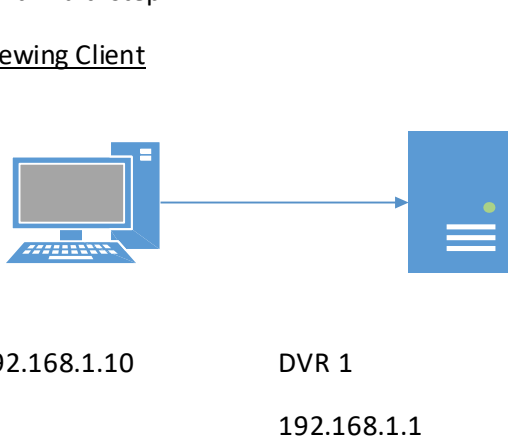
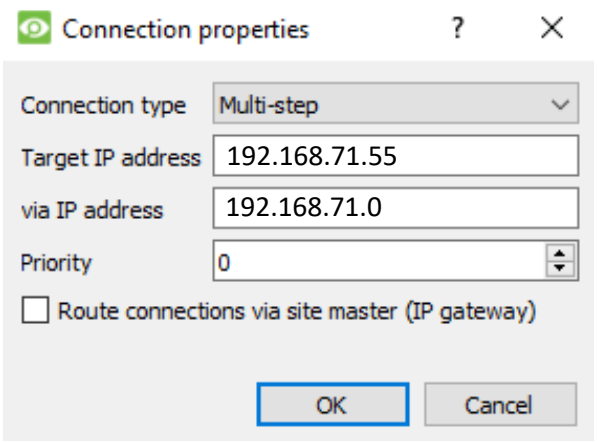
1.6.3.1.1 Add a Connection to the Site

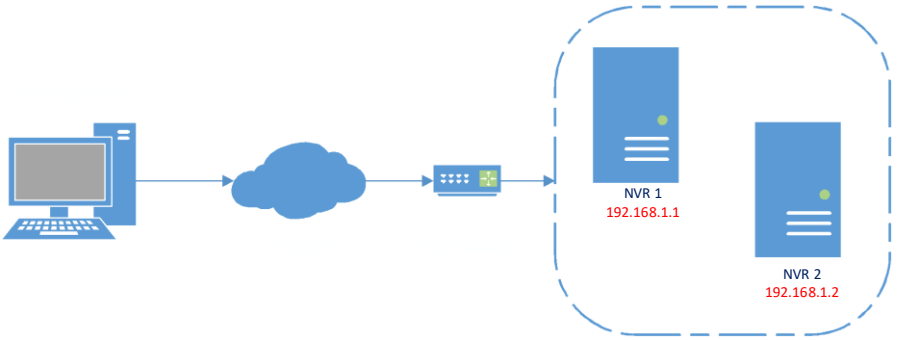
Add the information needed to connect the client to the Master unit of the site. Select the Site, then right-click in the right-hand panel, where there will be a column entitled **Connection Type**.

Click on **New connection**. This will bring up the **Connection Properties** menu:



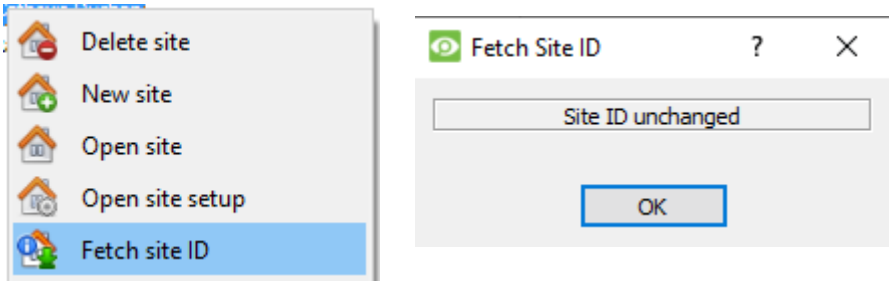
Note: One is **not** creating or editing a site here. The connection is being added to the Master unit of an **already existing site**.

Connection Type	These are the connections methods used to connect the site. There are two connection types: Point to Point and Multi-step. **Point to point** refers to a direct network connection, where the viewing station has a direct connection to the recording unit/s or site. **Note**: for clarity, the switches have been left out of the images.   **Multi-step** is when a recording unit is used to forward incoming network traffic to other recording units. The recording units would normally form part of a dedicated surveillance network. The capture station gateway unit normally has two network interface cards, or one network interface card for the local CCTV network and a dialup or WAN connection. In the screen capture above, the client is connecting to the 192.168.71.55 unit, via the 192.168.71.0 unit. In other words, the target is the reached, and the via unit is the entry-point to the site network.
IP Address	This is simply the IP address of the master unit.
Priority	When there are multiple possible methods to access a site, add these methods as separate individual connections. A connection can have 2 addresses: a Local address (192…) and also with a dyndns address. These both direct the client to the same site. The 192… address is accessible only via the LAN, and the dyndns gives access from outside of the LAN (over the internet, for instance). Connection type | Target | Route | Priority | Route connections via site master Ethernet | 192.168.XX.XX | - | 1 | No Ethernet | YourSitesName.dyndns.org | - | 0 | Yes

	The Priority determines the order that the client will attempt to make a connection via. **The higher the number the higher the priority**. (The connection with a priority of 1 will be tried before the connection with a 0 priority.) This way, queue up connection methods without having to select them each time connection takes place, and be assured that the higher quality connection will always be prioritised.
Route Connections via site master (IP Gateway)	Enable this tick box to make a connection to Site A from outside the local Network. The router also needs to be configured to route the inbound client connection to the Site Master DVR unit. This is to ensure that the client software makes a direct site master connection via the Internet or ADSL IP address. 
Use site discovery for connection	This is a mechanism which enables the client viewer to discover the IP address of the site master. This means that if the IP address of the site master changes, the client will be able to rediscover the IP address and not lose its connection. **Important Note:** If there is a failover system setup (see the Failover section of this manual), this option must be checked, in order to be able to access the site via the client in the event that the **site master** is failed over.

Connection Type	Gateway	Information required
Ethernet	Point-to-Point	○ Target unit IP Address ○ IP gateway connection mechanism (if necessary – refer to IT dept). ○ Priority ○ Route Connection via site master (IP Gateway) ○ Use Site discovery for connection.
	Multi-step	○ Target unit IP Address ○ Target via unit IP Address ○ IP gateway connection mechanism (if necessary – refer to IT dept.) ○ Via IP address ○ Priority ○ Route Connection via site master (IP Gateway)

1.6.3.1.2 Fetch Site ID



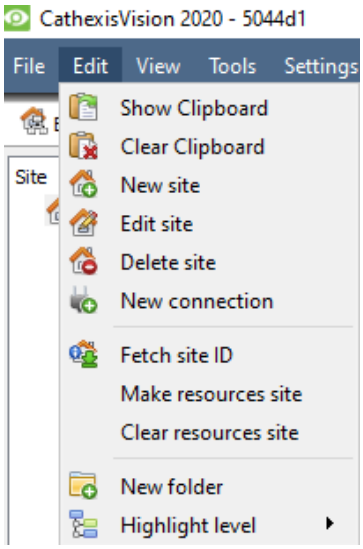
Right-click on **Site Name**, and click **Fetch Site ID**.

This tests the connection and retrieves important information about the site from the master unit of that site. Once this is done, connect to the site via **File / Site / Your_Site_Name.** Each site should have a unique site ID. The site ID is generated automatically when loading the NVR software.

1.6.4 Absent Units

A unit will be marked absent within a site if it does not connect for four or more weeks. This is important to note as any licenses that are tied to the unit will not be available to the site once that unit is marked absent. This may cause problems if other units rely on the absent unit/s for licenses.

1.7 The Site List 'Edit' Menu



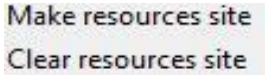
While in the Enterprise Manager tab, the Edit menu option will appear in the menu bar, as shown in the image the left.

Achieve everything covered so far via the **Edit menu**, as opposed to using the right-click options.

There are a few options that have not been examined in the initial addition stages, and which present changes that can be made to the site at a later stage. These are briefly discussed below.

1.7.1 Make or Clear a Resources Site

If there is a Video Wall attached to this site, it may be desirable for the Control Room operators to have control over what the Video Wall screens display. On the units that will be controlling the Video Wall, make the site a resources site.

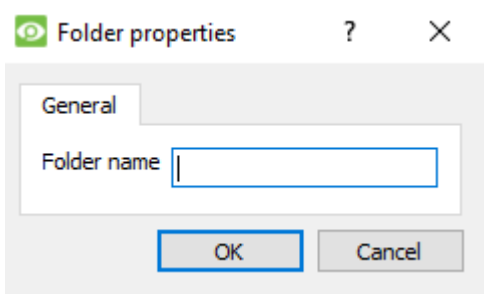


To give control, select the relevant site and click on **Make Resources Site**; to remove, CTRL- click on **Clear Resources Site**.

Note: Control of the Video Wall will be via a Monitors Setup Tab that will appear in the **CathexisVision** GUI when the site is open. For more information about this, consult the Monitors section of the Configure Servers document.

1.7.2 Organise Sites into Folders

Organise sites into folders by either right-clicking in the site list area, or **Edit / New Folder**. This will bring up the following box.



Enter a relevant name for the folder and click OK.

Once this is done, click-and-drag individual sites in/out of the folder.

Now, under **File / Open Site** there will be a folder containing the sites:

1.7.3 Highlight Level

Highlight Level is relevant to a site that has its **Alarms** sent via an **Alarm Management Gateway.** It will have an access property where only users with certain access rights are allowed to respond to certain sites. This feature allows users to highlight only those sites that are accessible to certain levels.

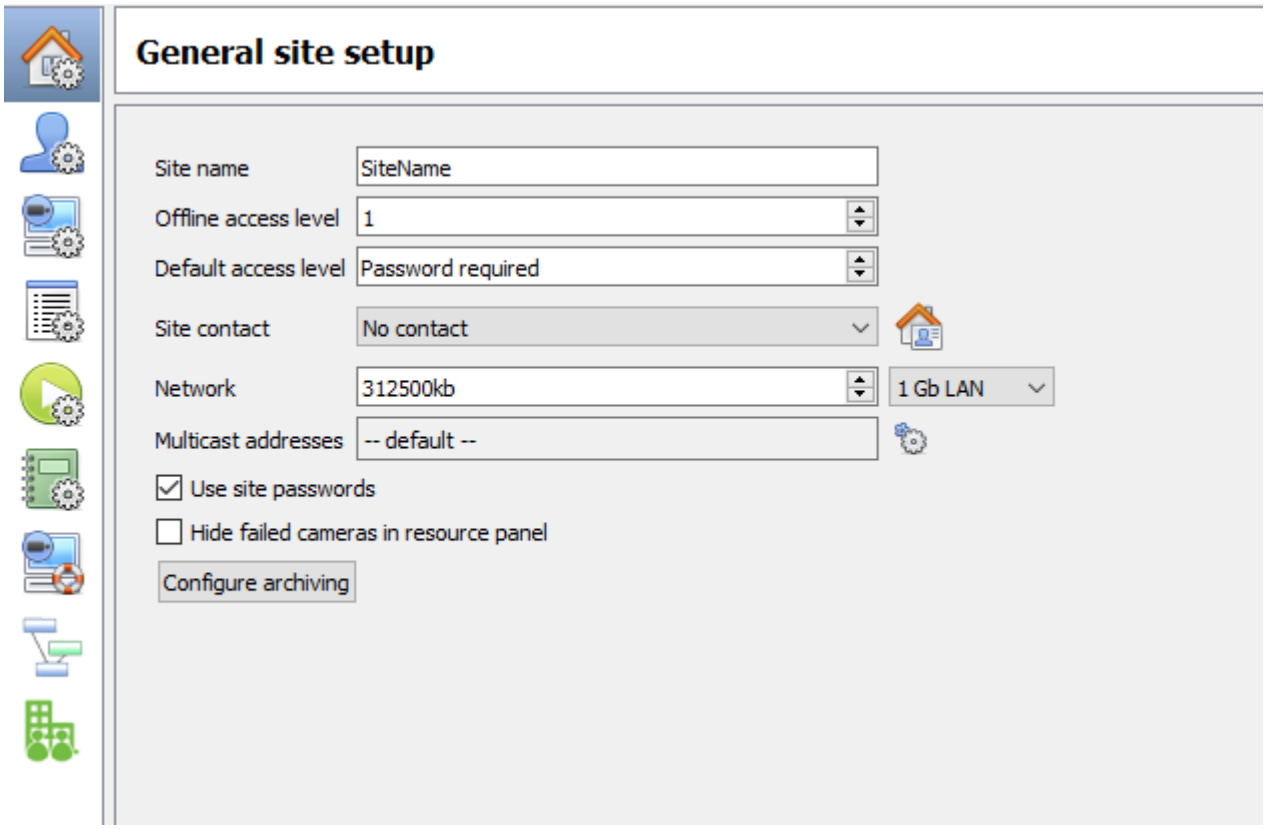
Note: This will only highlight the sites in the Site List within the Enterprise Manager.

2. Setup Tab: General Site Setup

2.1 Introduction

All server setups in the **CathexisVision** software are centralised under the **Setup Tab**. When a site is open, the **Setup Tab** is accessed via **Site** / **Open Tab** / **Setup**.

In the Setup tab, there is a list of setup option icons on the left. On the right is the setup panel of the icon selected. In the image below, the icon highlighted in blue (**General Setup**) has been selected, and all related settings are shown in the panel on the right.

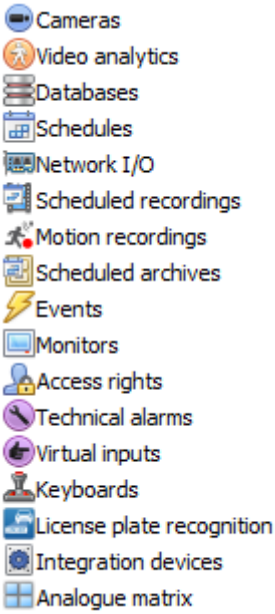


General Site Setup: contains information that is general to the entire site, such as the **Network Speed, Default access level, and Site contact.**

Users: where users are created and maintained (including login level and remote access). This can be done on a server-by-server basis, or be controlled as a site.

Configure Servers: where changes are made to the individual units that comprise the site. Anything that happens on a unit via CathexisVision can be changed here, from any access point on the site.

Note: Since sites are made up of individual units, which have their own resources, this is a very important section and the bulk of Site editions will happen here.



Resources Panel. Here, control which resources are visible to operators, in the resources panel that occupies the right-hand side of the **Cameras Tab**. Organise resources into folders, and repeat resources across folders. The following are all set on a unit-by-unit basis.

Site Actions are actions that apply to the site as a whole. **Events, and Event Actions relate to resources on individual units.** Site Actions are actions that can be applied on any unit on the site.

Reports. CathexisVision can draw complex reports on the state of the hardware and software resources of the site. These reports can be based on user created templates, and can be run on a schedule.

Failover. CathexisVision offers the ability to install failover servers, which can be managed from this section.

Adjacent Camera Mapping. The adjacent cameras feature allows the spatial relationship between cameras on a site to be defined and used as a means of swiftly navigating between cameras based on a camera's physical position.

Enterprise. This is where the enterprise manager is configured.

2.1.1 Setup Tab Access Rights

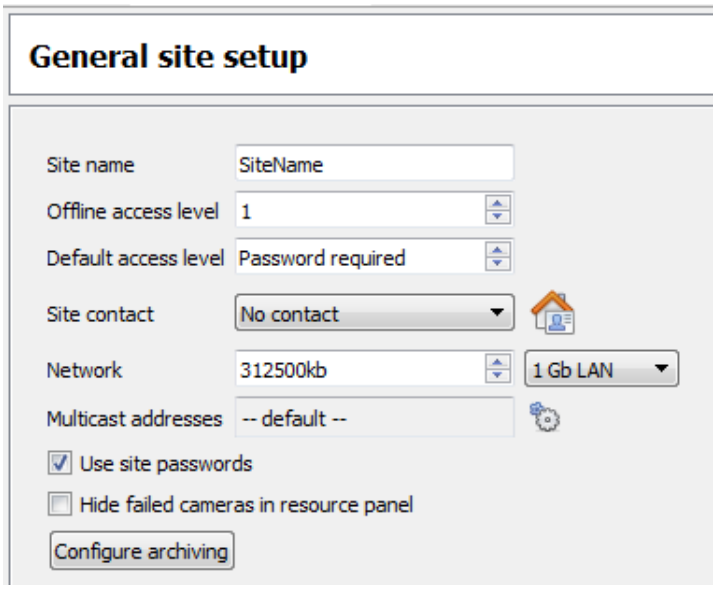
Only administrator users have the ability to open the Setup Tab (and thus access server setups such as user configuration, events, and video analytics). All other user logins, regardless of access rights or level, are unable to access this tab. This prevents any operator from being able to change site configurations.

Note: An exception is made for non-admin users who have been given the right to configure other non-admin users. These users will only be able to enter the Configure Users section of the Setup tab. No other part of the system setup will be available or visible to them.

2.2 General Site Setup

General Site Setup deals with information retrieved from the site, not from the local unit being worked on. The site information will be stored on the unit called the site **Master**. **Note**: In previous versions of the software, General Site Setup was called Global Resources.

An exact copy of the site resource information gets stored, and updated on each unit that forms part of the Site. This will help with failover if the Master Unit goes down. Any unit that forms part of the Site can become a temporary Master by assigning a "Slave" Unit the same IP address as the failed Master. Contact support for more details.



Site name	The name of the Site as a whole, held in the site database. **Note**: this is not the same as the site name given in the local systems site list.
Offline Access Level	Defines what someone, who has connected to the site, can see of the site in its OFFLINE state. Although this user cannot interact with the resources themselves, this defines what resources the user can see in the Resources panel. Options are “No access”, and levels 1 to 30.
Default Access Level	Applies to what a person can see and do on a site in its ONLINE state. If set to password required, then the user will have to enter a username and password, and the access level will be whatever level has been assigned to that user. **Note**: If the level is set at anything from 1 to 30, when the site is opened, it will default to this level without a password required. This also means that the session will not be logged as a specific user. To have audit trails for every session, set this to password required.
Site contact	This is the default site contact. This is especially important for monitoring, where an external viewer needs to contact a local responsible person. To set a site contact, click on the icon on the right. Then select an existing contact, or create a new one.
Network	Network settings are those settings specific to the LAN.

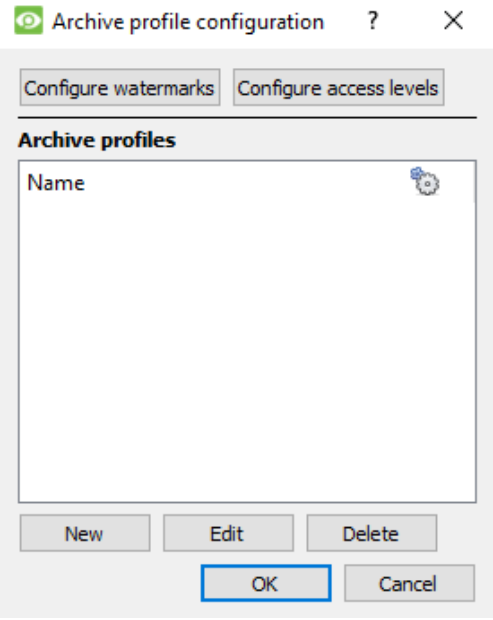
Multicast	This will define the multicast settings for the site as a whole. This is discussed in more depth below.
Site passwords	If **Use Site Passwords is checked**, it will propagate all users on the Site Master Unit to all units on the site. This centralises control of users to the master unit. **This is the recommended setting**. If left unchecked, users will be defined on a unit-by-unit basis. It is best to **enable this only after** all relevant users are set up on the Master Unit, and there aren't any users needed to be stored on other units. This is because **setting site passwords will delete all users on non-Master units** and replace them with the user list on the Site Master computer.
Hide Failed Cameras in Resource Panel	This will remove cameras that have failed from the Resources list until they are running again.

2.2.1 Configure Archiving

This section describes how to create archive profiles, set user levels, password protection, and assign watermarks. **Note** the following security enhancements made to the archiving process:

- Overall archive signature is retained.
- Critical portions of video / audio are now also independently signed and can be explicitly linked to the source NVR.
- Added extra audit logging regarding an archiving client on each NVR sourcing data for an archive.
- Provide more detailed breakdown in the archive viewer of the verification result.

2.2.1.1 Overview



The process for creating archive profiles is:

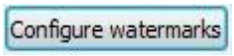
1. Configure watermarks.

2. Click **New** to create profiles and assign the watermarks to profiles.

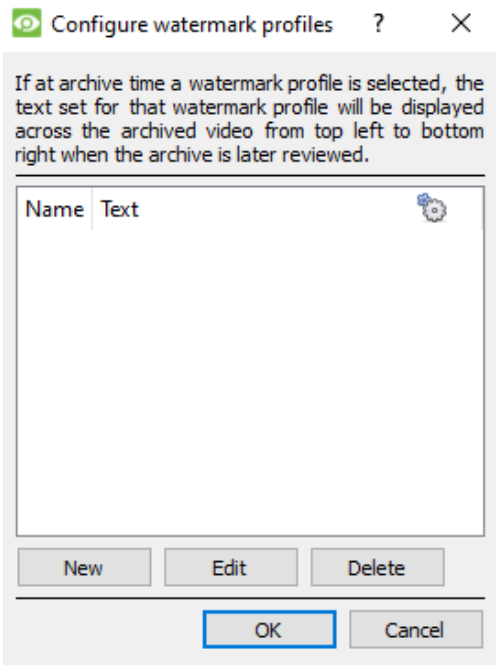
3. **Configure access levels** for each profile, including the ability to archive, set password requirement, and default watermarks.

4. Click **OK** to save.

2.2.1.2 Configure Watermarks



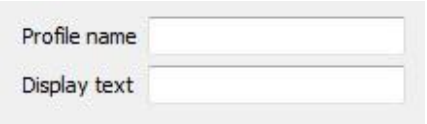
Click the **Configure watermarks** button to bring up the window.



Once watermark profiles are created, they will appear in this list.

Click the **gear icon** to customise which columns are seen in this window.

Click **New** to create a new watermark profile.



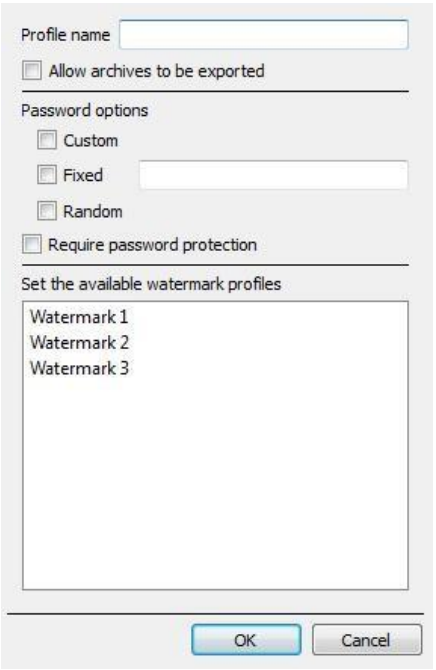
Name the profile. Type the watermark text.

To edit an existing watermark profile, select it from the list and click **Edit** to bring up the same window as above.

When done with creating all profiles, click **OK**.

2.2.1.2.1 Creating New Archiving Profiles

In the **Archive profile configuration**, click **New** to create a new profile.



Give the archiving profile a **Name**.

Ticking **Allow archives to be exported** will allow archived footage to be exported in different file formats from within the archive viewer.

Set **Password options**: Allow profiles the ability to add password requirements when creating archives. Please see below for an explanation.

Ticking **Require password protection** will force a user to set at least one of the password options allocated to them. If it is unticked, the user will be presented with the additional option of **not adding a password to the archive**.

Set the available **watermark profiles**:

If watermark profiles are created already, they will be available here. Highlight the watermark/s to attach to this profile. If multiple watermarks are selected for a profile, the operator will be able to choose between them when archiving.

2.2.1.2.2 Password Options

Site administrators may give operators the ability to add password requirements to archives when creating archives; these password requirements will have to be met by all users wishing to review the archive in the archive viewer.

Custom: The operator will be able to create a custom password by typing it into the space.

Fixed: The operator must add a Preset password to the archive. Create this password by typing it into the white box next to the **Fixed** option.

Random: A random password will be generated by the system in the archive window. The operator will need to make note of it.

2.2.1.2.3 Single / Multiple Password Options

One may assign multiple password options to archive profiles. At the time of archive, the operator will select from a drop-down menu the single/multiple password options that have been constrained in this section. If no password options have been set, the drop-down menu will offer 'None' as a password option.

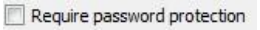
Ticking **Require password protection** when creating an archive will force a user to set at least one of the password options allocated to them. If it is unticked, the user will be presented with the additional option of **not adding a password to the archive**.

These password options will be displayed to the user in the archive window. Please note that the examples below both have multiple password options set.

Require password protection.

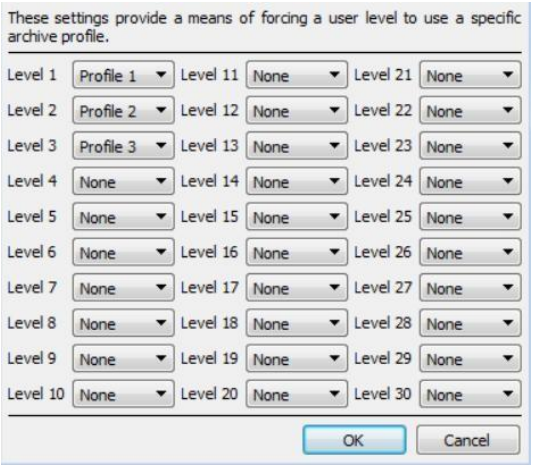
The operator **must** set a password requirement from the options set by the administrator.

Does not require password protection



The operator has the added option of **not adding a password**.

2.2.1.2.4 Configure Access Levels



These settings assign user levels to specific archive profiles. This means that whatever settings applied to archive profiles above, will be applied to the assigned user level when the user archives footage.

Simply select the desired archive profile from the drop-down menu next to each user level.

One may only assign one profile to each level.

2.2.2 A Note on Multicast

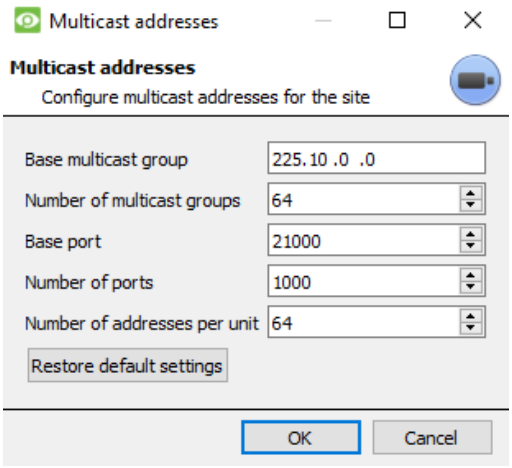
CathexisVision has the ability to automatically assign multicast addresses to cameras. When a camera is added to a unit, select to have multicast 'disabled', 'automatic', or 'enabled'. The multicast settings that are in **General Site Setup** define the parameters of the 'automatic' settings.

A **Multicast Address** consists of two components:

1. The **multicast group** is the IP address that the camera will send multicast packets to.
2. The **Port Number** is the port number associated with the multicast group.

Users/ units inform the network that they want to receive packets from this Address (this is called joining the group). The multicast switch / router will then forward packets sent to this Address to those units who join the group.

Address #	Multicast Group IP	Base Port	The address must be unique, not the individual components.
1	255.10.0.0	21000	
2	255.10.0.0	21002	



Base Multicast Group: This is the first IP address in the multicast range.

Number of Multicast Groups: This is the number of group IPs available.

Base Port: This is the first port in the range of ports that will be used for multicast addresses.

Number of Ports: This is the number of ports that will be used.

Number of Addresses per Unit: This is the number of unique Multicast Addresses that each individual unit may use/assign multicast sources.

Note:

1. In most cases the default settings will work. The only person who should be changing such settings should be someone with the relevant networking expertise. These settings **can be changed and this is desirable if**:
    a) There are multiple sites on the same network (one would need to make sure that the ranges do not overlap at all. i.e. the same address: port pair may not exist in both the ranges), or
    b) There are other devices which conflict with either the addresses or ports in the range.
2. Changing these settings will require every unit in the site to be re-started because the device multicast settings are reserved once they have been used.

3. Setup Tab: Users

3.1 Update Notice

From version 2017, CathexisVision has a new user management system, which replaces that found in earlier versions of the software. Previously, there were 2 modes of operation:

- Server-based users where every server had its own set of users, and
- Site-based users.

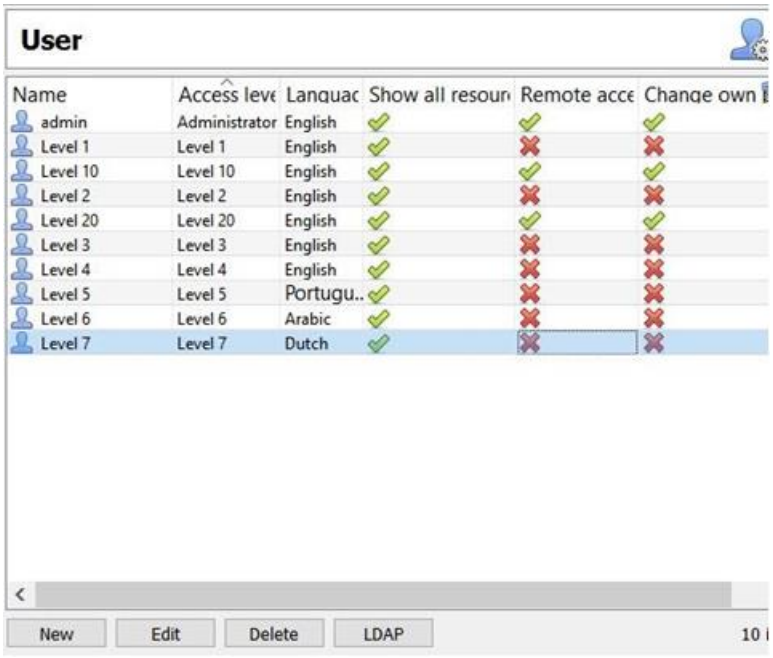
Now, all users are site-based, which means that the configured users and their access rights will be applied to all servers on the site. The old user database will automatically be converted to the new format.

Please note the following regarding the conversion process:

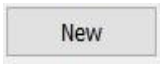
- For old systems using server-based users, the users on the master will become the new site users.
- The concept of unit groups has been deprecated and is no longer presented for CathexisVision 2017 systems. This feature will still be supported for sites running connections to earlier software versions.
- When connecting to older systems, the original user management interface will still be used.

3.2 Introduction

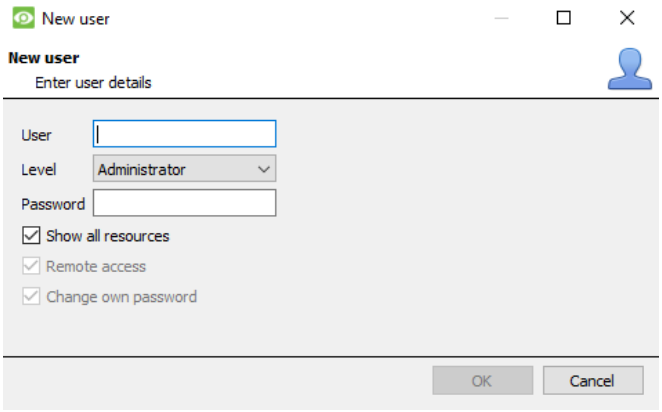
To configure users, click the icon in the **Setup tab**.



3.3 Create New User



To create a new user, click **New** at the bottom of the screen, or right-click anywhere in the **Users** area and select **New…**

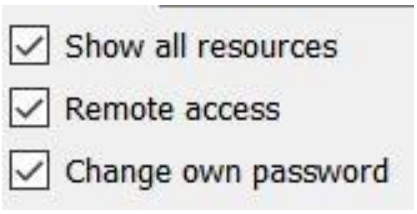


Give the new user a **User name**.

Select the user **Level** from the drop-down menu.

Set the user **password**.

Note: The user will have to enter the **username** and **password** set here to enter the CathexisVision software.



Un-check these options to determine whether it is possible to:

See all site resources.

Remotely access sites.

Change own password.

Note:

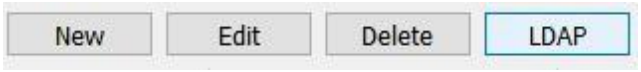
1. In order for users and their access levels to be effective, the relevant **access level settings** need to have been set. Go to **Setup tab** / **Configure Servers** / **Access rights**. (For more information about this, refer to the Configure Servers chapter of this Setup Manual.)
2. Once a user has been created, the username cannot be edited. However, all other fields can be edited.
3. The administrator has default access to **Remote access** and **Change own password**. All the options for Level 1 to Level 30 can be manipulated.

3.4 LDAP

CathexisVision now supports the importing of users from LDAP into CathexisVision. LDAP (Lightweight Directory Access Protocol) is a protocol used to communicate with user management systems, such as Microsoft's Active Directory.

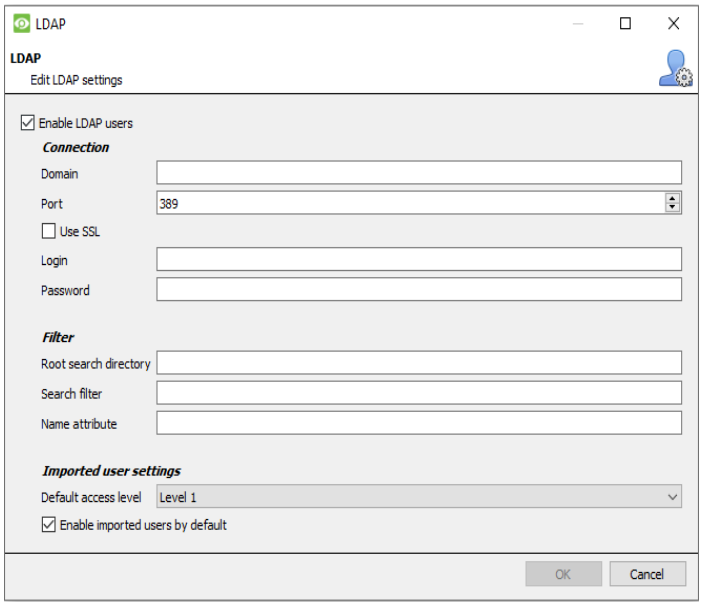
Note:

1. LDAP is only available on Pro and Premium sites.
2. LDAP users cannot use mobile I/O.
3. LDAP users cannot use the API.



To configure LDAP settings, click the **LDAP button** at the bottom of the **Configure Users** screen.

3.4.1 LDAP Settings



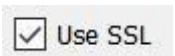
Check **Enable LDAP users** to enable LDAP import.

Enter the **Domain name** of the LDAP server.

Note: The NVR must be able to resolve the IP address of the LDAP server.

- It may be necessary to edit the /etc/hosts file on Linux to ensure that the hostname can be resolved.
- On Windows, edit the file **%SystemRoot%\System32\drivers\etc\hosts**

Enter the Port number of the LDAP server.



Check **Use SSL** to use transport layer security.

3.4.1.1 Valid SSL Certificate

SSL will not work if a valid SSL certificate is not installed. This certificate should be imported as a trusted certificate on the NVR.

3.4.1.1.1 Windows

Import certificates using the Microsoft Management Console certificate plugin. Enter mmc in command prompt to open application. Windows requires the certificate in **.crt** format.

3.4.1.1.2 Ubuntu

- Copy the certificate to /usr/share/ca-certificates/ldap.
- To trust the certificate, use: Sudo dpkg-reconfigure ca-certificates.

3.4.1.1.3 Fedora

SSL on Fedora requires a certificate in **.pem** format.

- Copy the certificate to /etc/ssl/cert
- Run /usr/nvr/3rdparty/libopenssl/bin/c_rehash /etc/ssl/certs

Enter the **Root search directory** location in which users will be searched for. The **Search filter** must be carefully constructed to ensure the correct users are imported.

To import users: (&(objectCategory=person) (objectClass=user))

To import only enabled users from Active Directory (this will only work in Active Directory):

(&(objectCategory=person)(objectClass=user)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))

Enter the **Name attribute** as unique values in order for users to be identified in the NVR. It is recommended to use:

- **sAMAccountName** for active directory
- **uid** for openldap slapd.

Set the **Default access level** which will be assigned to all users imported through LDAP. This can be changed later.

Enter the **Login** and **Password** details of the user with access rights to search the directory.

3.5 Non-admin Users with Access Rights to Configure Users

Non-admin users may create and modify other non-admin users if their user level is equipped with this access right.

This access right is configured per user level in **Setup Tab / Configure Servers / Access Rights / General Tab / Configure Users.** Please see the Access Rights section of the Configure Servers chapter in this document for details on configuring this access right.

Users with this ability **will be able to**:

- Enter the Setup tab to configure Users, however no other setup will be available or visible to that user.
- Create and modify other non-admin users.
- Change their own password.

They **will not be able to**:

- Access any part of the system setup other than the user configuration section.
- Delete themselves.
- Create admin users.
- Import LDAP users.

4. Setup Tab: Configure Servers

4.1 Configure Servers

Configure Servers: all server-based settings are configured in this section.

A **CathexisVision site** is a collection of one or more individual units. These units are consolidated in the software as a single site. The user can add and remove units from sites, and change settings on a unit-by-unit basis.

In the **Configure Servers** panel, there is a list of all servers. Under each server, there is a list of setting options available on that server.

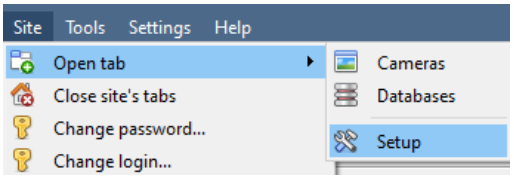
The options include:

- Cameras
- Video Analytics
- Databases
- Schedules
- Network I/O
- Scheduled Recordings
- Scheduled Archives
- Events
- Monitors
- Access Rights
- Technical Alarms
- Virtual Inputs
- Keyboards
- Integration Devices, and
- Analogue Matrix.

4.1.1 Server Options

4.1.1.1 Open Configure Servers

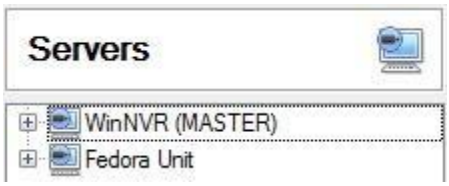
To open the Configure Servers setup, follow the instructions below.



Log in to the site. Click on **Site** / **Open Tab** / **Setup**.

In the Setup tab, click on the Configure Servers icon.

Note: Right-click on the tab of any open site to bring up the same menu as the one accessed via the method above.



The servers list will be shown to the right.

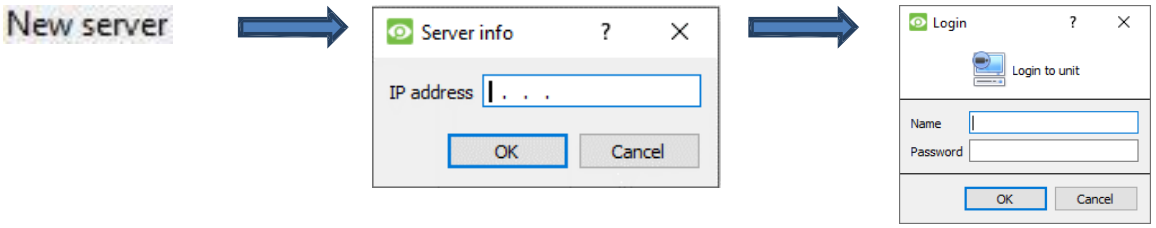
The panel to the right of that list contains the options for the current selection.

4.1.1.2 Add / Detach / Delete / Replace a Unit

4.1.1.2.1 Add a Unit

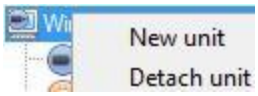
To add a new unit to a site, right-click on any white space in the **servers list** panel. The user may also click on an existing server.

Click on **New server**. Enter the IP address of the server. There will be a prompt to enter an administrative username and password.

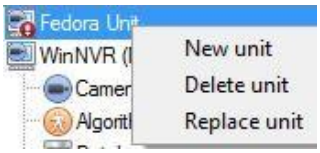


Note: The server must already be running as a **CathexisVision NVR**. However, one may add an unlicensed unit, as all servers may be licensed from the Configure Servers panel.

4.1.1.2.2 Detach, Delete, Replace a Unit



To **Detach** a unit, **right-click on the unit** in the Servers list.
Click on **Detach Server.** There will be a prompt to enter an administrative username and password.



A Detached unit will still appear in the servers list. To fully delete the unit, right-click on the detached unit. Select **Delete Unit**.

To **Replace a** detached unit with another unit, right-click on the detached unit. Click on **Replace Unit**. The next steps to take are the same as adding a unit.

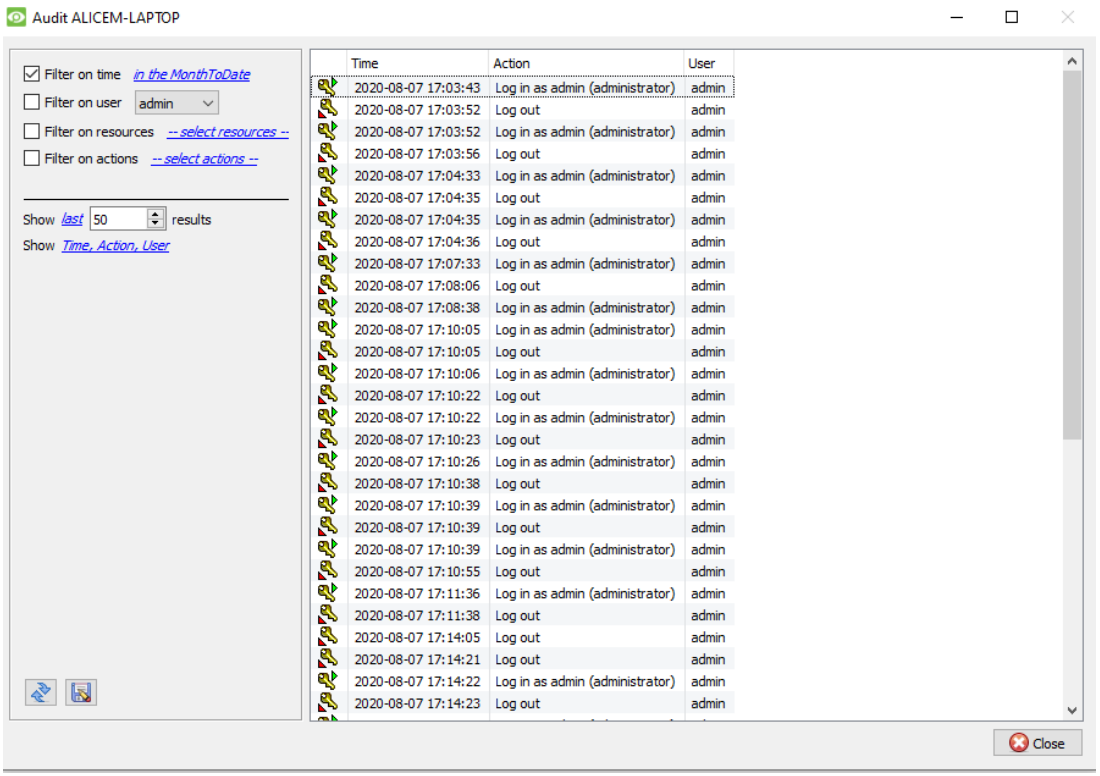
Note: Only replace units that have been detached, or that cannot be reached on the network due to a hardware failure.

4.1.1.3 Right-click on a Unit

The user can right-click on a unit to perform several important actions. The following list of options will appear.

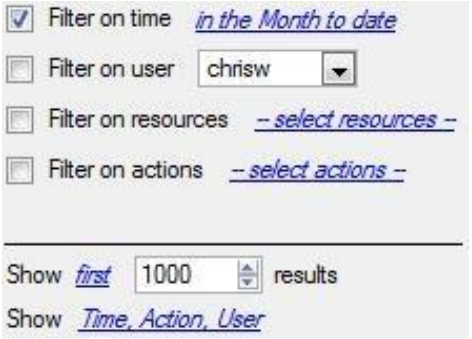
New Server: this is dealt with in the **Add a Unit** section, above.
Licensing: this relates to licensing an individual recording server. This is dealt with in the installation section.
Audit Server: allows auditing the specific unit. Auditing is explained below.
Fetch Sherlocks: this allows the Sherlocks for this device to be fetched. See below.

4.1.1.3.1 Audit Server



Various processes leave historical “footprints”. These footprints are called **audit trails**. Audit trails are mainly used as diagnostic tools – they help the user to identify exactly what happened in the system.

Each audit trail is formatted as a textual list of historical actions.



Filter: Time, Users, Resources, and Actions.
There are many options for filtering the audits, because audit logs can have a lot of information. The blue hyperlinks open up a full list of options.

Show first / last: this option limits how many results are shown.
Show time, action, user: this option lists the selected variables and allows the user to add and remove audit report columns.

Print, Save, Refresh

The report is not live. Click on the **Refresh icon** to update the information.

For a digital copy of the Report, click on the **disk icon**.

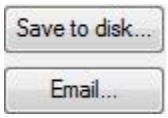
4.1.1.3.2 Fetch Sherlocks

Sherlock files are a diagnostic tool used by the Support Desk.

The standard procedure is for the user to email the Support Desk (support@cat.co.za), attaching the Sherlock file and a description of the problem. The user can also save the Sherlock file to a disk.

Right-click on the unit to get the Sherlock files. Then left-click on **Fetch Sherlocks…**

This will generate the Sherlock pack. Either **save** them to disk, or **email** the Sherlocks to the Support Desk.

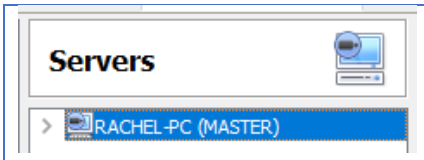
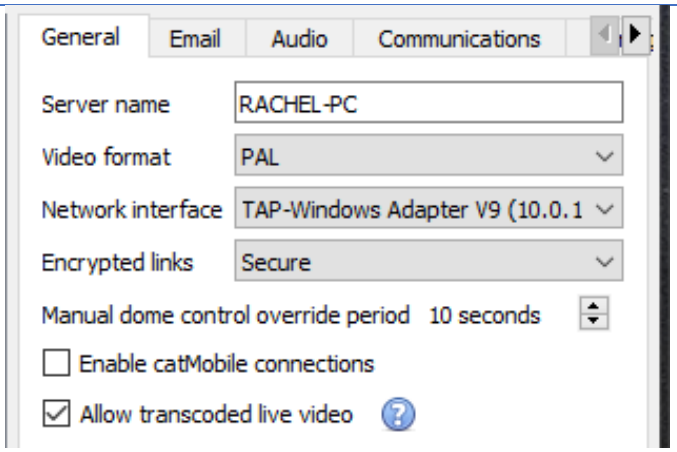


Save to Disk: allows the Sherlock files to be saved to any storage attached to the workstation.
Note: Click on **Email to recipients** to open the Operating Systems default email client.

4.1.2 General Tab

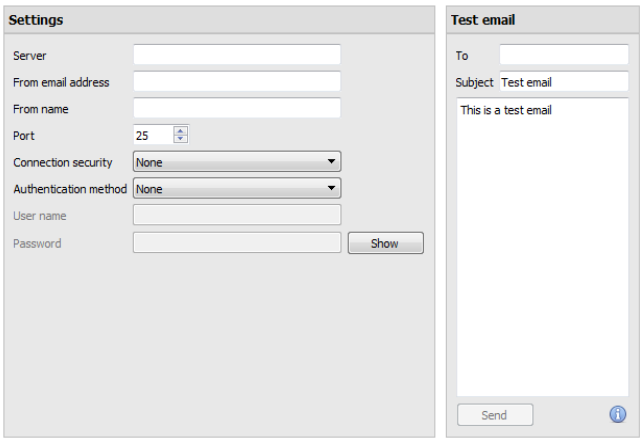
If the user clicks on the **server's name**, the panel on the right will fill with the General Setup options for that server.

Clicking on the **plus icon** (+) will expand the options.

	
Server Name	The **Server Name** identifies the unit in the GUI. It is the descriptive name given to the individual unit.
Video Format	Choose between PAL and NTSC. **Note**: It is not advisable to mix formats across units on the same site.
Network Interface	This lists the Network Interfaces on this unit and their current IP Addresses.
Encrypted links	Set the level of encryption for external site connections: • Disabled, • Minimal: only critical connections are encrypted,

	• Secure (default): all connections except those with high volume video are encrypted, • All: all connections are encrypted (including high volume video links). The encryption engine uses openssl (SHA512 hashes, ephemeral DH-RSA with forward secrecy (DH 2048 bit), and AES-GCM 128-bit symmetric ciphers) equivalent to TLS 1.3.
Manual Dome Control Override Period	This is the period of time the controller must be inactive on a PTZ camera before it resumes its automatic responses. (For example, tours, pre-sets, etc.)
Enable CatMobile Connections.	CatMobile connections are connections to the unit via a web browser, or **the iPhone/Android** Apps that are available online. **Note**: although the various CathexisVision packages have limits on the number of simultaneous client connections, the Cathexis mobile app does **not** count towards the client connection limit. **Note**: The mobile connections are made on a unit-by-unit basis, with no site knowledge. Enable this on each unit that needs to be available via the mobile interface. The listen Port can be customised. See Appendix A.
Allow Transcoded Live Video	This is currently only available on Windows units. It uses software encoding to add another stream (lower quality MPEG) to send to the Cameras Tab. This is useful for remote viewing, but will put extra strain on the processor of the unit.

4.1.3 Email Tab



Emailing is an option for notifying a Site Contact. It is also an **Action** associated with an **Event**.
For example, a possible Event Action would be to send an email to a particular email address when there is movement on a camera.

The settings are standard email settings, associated with the user's email account.

Note: these are all standard email settings. The Port number is the user's SMTP port. Make sure that the NVR unit can reach the mail server by configuring the correct network settings, IP, Default Gateway, and dns server.

4.1.3.1 Test settings

The **Test Email** box is opposite **Settings**.

A test email can be sent from the Test Email box to another email account, just as if it were from a normal email client.

Note: before attempting to send a test email, click **Apply**.

4.1.4 Audio Tab

A full list of all available audio devices is available in the respective drop-down menus. The device selected from the menu will become the device used if this unit is used as a Viewing Station as well as an NVR.

Local System Audio: is the name given to the on-board audio device located on this server.

My audio devices: is a list of the audio devices available on this server. The device selected here will determine the audio devices which are used as calling/listening devices, if this server is ever used as a Viewing Station.

This will change the name of the device as reflected in the **Resources Panel.**

4.1.4.1 Audio and Video Synchronisation

Assuming the source audio and video are synchronised on the camera, CathexisVision will maintain this synchronisation to less than 500 milliseconds.

4.1.5 Communications Tab

A Heartbeat is a signal sent from the capture unit (recording server) to an Alarm Management Gateway unit. A heartbeat tells the Gateway that the server is still active.

If the message fails to come through, the Gateway will generate an alarm. This will generate an alarm if the server goes down, or if the communications medium goes down.

Note: This needs to be set up on both the capture station and the Alarm Management Gateway.

4.1.5.1 Enable Heartbeat

To enable sending the heartbeat on the unit, check the **Send gateway heartbeat** tick box.

4.1.5.2 Select a Base-Station

The base-station referred to is the Alarm Management Gateway unit the heartbeat message is being sent to.

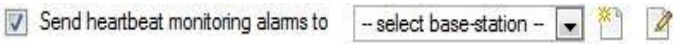
4.1.5.3 Select an interval for the heartbeat

This will define how often the unit will send a heartbeat to the Gateway.

4.1.6 Gateway Tab

This section deals with the Alarm Gateway. This option will only be seen if the selected server is set up as a gateway.

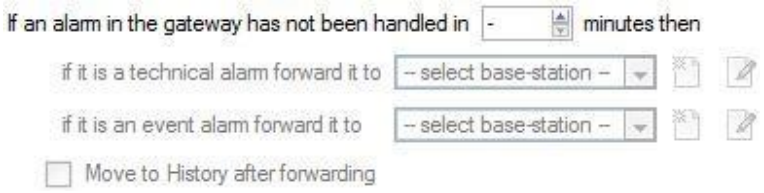
4.1.6.1 Send heartbeat monitoring alarms



If a heartbeat alarm is triggered, the gateway needs to take an action (send an alarm). In general, this alarm should go to the gateway itself. Simply select the gateway from the drop-down menu. For the heartbeat alarms to go to some other unit, select / add that unit.

Note: If this is not checked, these heartbeat alarms will not be sent anywhere.

4.1.6.2 If an alarm is not handled

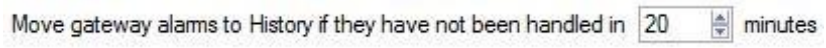


If alarms have not been handled for some time, the user might choose to send unhandled alarms to other gateways or base stations.
Choose the time frame, and the location that specific types of alarms will be sent to.

Note: when an alarm is sent to another gateway, this alarm will appear in the incoming queue of both gateways. If one is handled, the other will remain in the incoming list.

To avoid confusion, check the **Move history after forwarding** box. This will move the alarm to the history queue of the forwarding unit.

4.1.6.3 Move to history



The number of alarms can build up very fast, especially on large sites. If dealing with a site where alarms are only relevant for a short period of time, have them automatically moved to the history queue.

4.1.7 Configuration Backup Tab

This will back up all of this unit's **CathexisVision settings**, except for the database settings. The databases will remain on the drives chosen, but will have to be re-imported manually.

Note: One will only be able to **set default path,** and **Enable auto backup** from a Base-Station. To **create a manual backup**, and to **restore an existing backup,** be on the NVR unit itself. This is one of the very few things that cannot be done from anywhere else on the site.

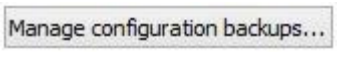
4.1.7.1 Configure Backup

Note: Choose to back up all units to a central location, such as a network drive.

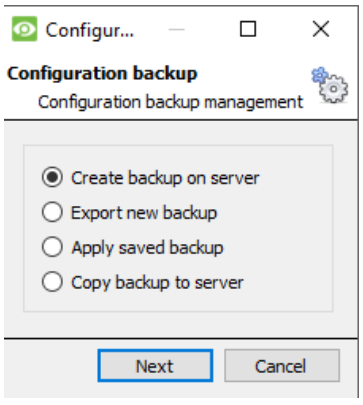
4.1.7.2 Automatic Backup

With **Enable auto backup** checked, the unit will update the Configuration Backup **every day at 2 a.m.** local time. Set the location for the automatic backup by entering the path (or browsing to it). Click on **Set default path**.

4.1.7.3 Manage Configuration Backups



Clicking on **Manage configuration backups…** will open a dialogue box.



Create backup on server: will create a backup on the server, in the default path that was set above.
Export a new backup: will allow choosing the destination of the new backup.
Apply saved backup: (formerly restore existing backup) will allow applying a saved backup.
Copy backup to server: create a restore point backup of the system's current state. This can be done straight after making new changes to the system.

4.1.8 Base-Stations Tab

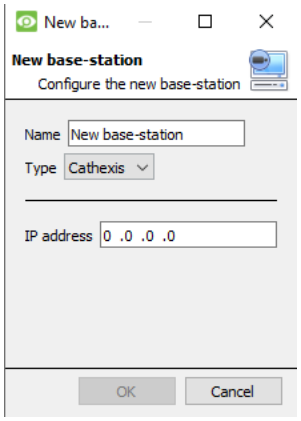
These Base-stations are the stations to which Alarms will be sent, when one is triggered by an Event. These alarms can be sent either to individual viewing stations in a control room, or to an Alarm Management Gateway.

If sending an alarm to an Alarm Management Gateway, it will appear in the alarm queue. If sending the alarm to an individual Viewing Station, it will appear as a pop-up window.

The window on the left is an example of such an alarm on a Viewing Station.

4.1.8.1 Add a New Base Station

To add a New Base Station, click **New**.



Name: Give the Base Station a descriptive name.

Type: Gives the type of the Base Station, either Cathexis or API.

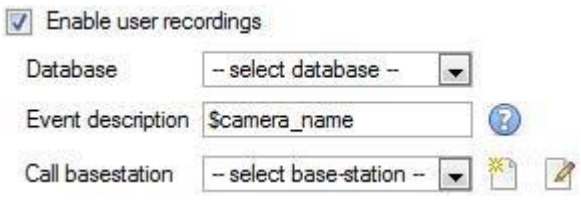
IP Address: IP address of the specific Base Station.

4.1.8.2 Send Test Alarm

Click on **Send test alarm** to test the settings. This sends a test alarm to the selected Base Station.

4.1.9 User Recordings Tab

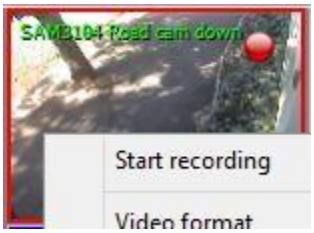
The user recordings facility allows a user to manually trigger a recording if viewing footage live in the Cameras Tab. This is useful as a recording might not have been triggered otherwise.



Database will define which database User Recordings are saved to. (Tip: Create a User Recordings database.)
Event Description is the name that will be given to the User Recording entry in the Database.
Call basestation will send an alarm to a Base Station whenever a User Recording is triggered.

4.1.9.1 Trigger a User Recording

4.1.9.1.1 Start the Recording



Middle-click on a camera in the Cameras Tab. **Start Recording** should appear as an option in the drop-down menu.

Click this to start the recording. If the recording has started, there will be a flashing icon in the top right-hand corner of the camera panel:

4.1.9.1.2 Stop the Recording

To stop the recording, middle-click on the camera panel. In the drop-down menu, click on **Stop Recording**.

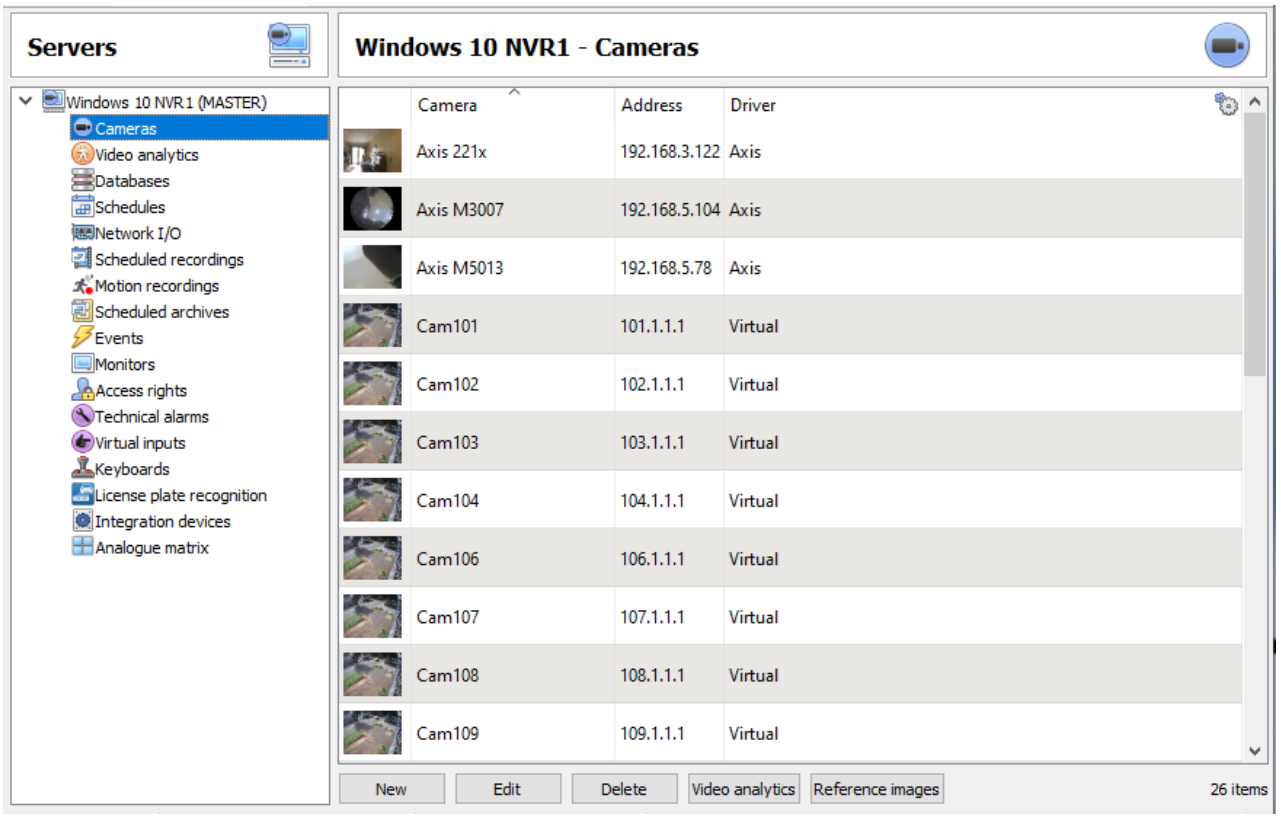
Note:

1. Only one camera can be triggered at a time.

2. It is advisable to create a separate database just for User Recordings.

4.2 Cameras

This section explains configuring and adding network cameras to the server and creating camera reference images. These create a saved image of the camera orientation, allowing for comparison between older and newer reference points.



4.2.1 Secure Camera Connection and Control

CathexisVision supports secure camera connection and control, where supported by the manufacturer. Currently supported camera drivers in CathexisVision are:

- Axis
- Mobotix
- Mobotix V2.

Note:

1. Consult the camera manufacturer for support camera models and configurations.
2. See the **Camera Connection** section of **Camera Addition Wizard** section for configuring CathexisVision for secure camera connection and control.
3. Refer to the **CathexisVision Cyber Security Overview** document for more information on security measures.

4.2.1.1 Camera configuration

1. HTTP: hypertext protocol,
2. Encrypted ssl/tls,
3. Supported by CURL (client-side URL transfer library).

4.2.1.2 Camera control

1. RTSP: real-time streaming protocol.
2. HTTPS encrypted camera connection control (where supported by the manufacturer).

4.2.1.3 Video Streaming

1. RTP – Real time transport protocol.
2. Encrypted video streaming (where supported by the manufacturer).

4.2.2 Adding Cameras

There are two ways to add a camera in CathexisVision:

1. The camera Wizard.
2. The Copy / Paste function.

This section of the manual will detail these two addition methods, examine the Camera Editing options, and provide extra information on the right-click menu.

4.2.2.1 Camera Addition Wizard

The camera addition Wizard explains all the steps needed to **add a camera**, as well as **allowing the creation of databases, schedules, and events** along the way.

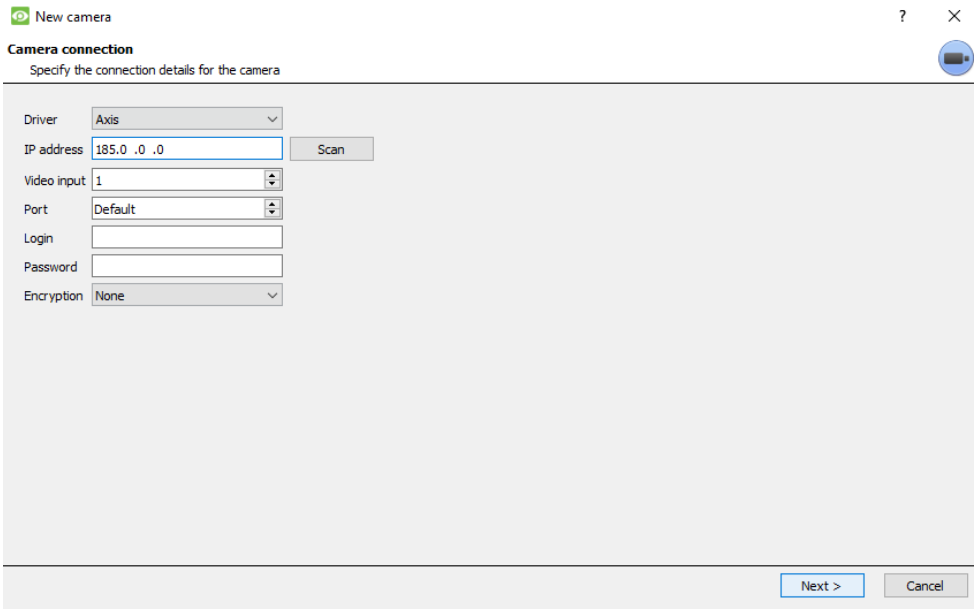
There are two phases in the addition Wizard:

1. The addition of the camera.
2. Setting up the system to record from that camera (either via a VMD Event, or via a scheduled recording).

To start the camera addition Wizard, click on the **New** button at the bottom of the cameras panel.

4.2.2.1.1 Camera Connection

The first step in the Wizard is the **Camera Connection** step. Here, set up all the connection details of the camera. The user needs to choose between adding a new, separate camera, and adding a camera that is a new video input for an existing camera. The options below will change on a camera-by-camera basis.



Driver: Select the relevant camera driver.

IP Address: Set the IP address of the camera to add.

Scan: Scan the network for available cameras. Click on a camera and driver and an IP address will be automatically set. (Under Scan will be the option to list cameras that are already linked to other servers. Check **Show devices used by servers**.

Video input will be used if connecting to an encoder that has multiple analogue inputs. If not, leave it on 1.

Port has a default setting, but can be configured to connect through desired port.

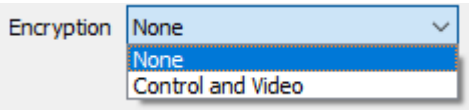
Login and **password** are the camera's current login details.

Encryption: Encrypted connection and control is supported on certain camera models (where supported by the manufacturer). See the **Secure Camera Connection and Control** section.

Configuration is required on camera side and in CathexisVision:

Camera configuration: Please consult camera manufacturer for supported camera models and relevant camera configurations.

CathexisVision: When adding or editing a camera, select the desired level of encryption in the camera connection window.



Currently supported camera drivers are Axis, Mobotix, and Mobotix V2.

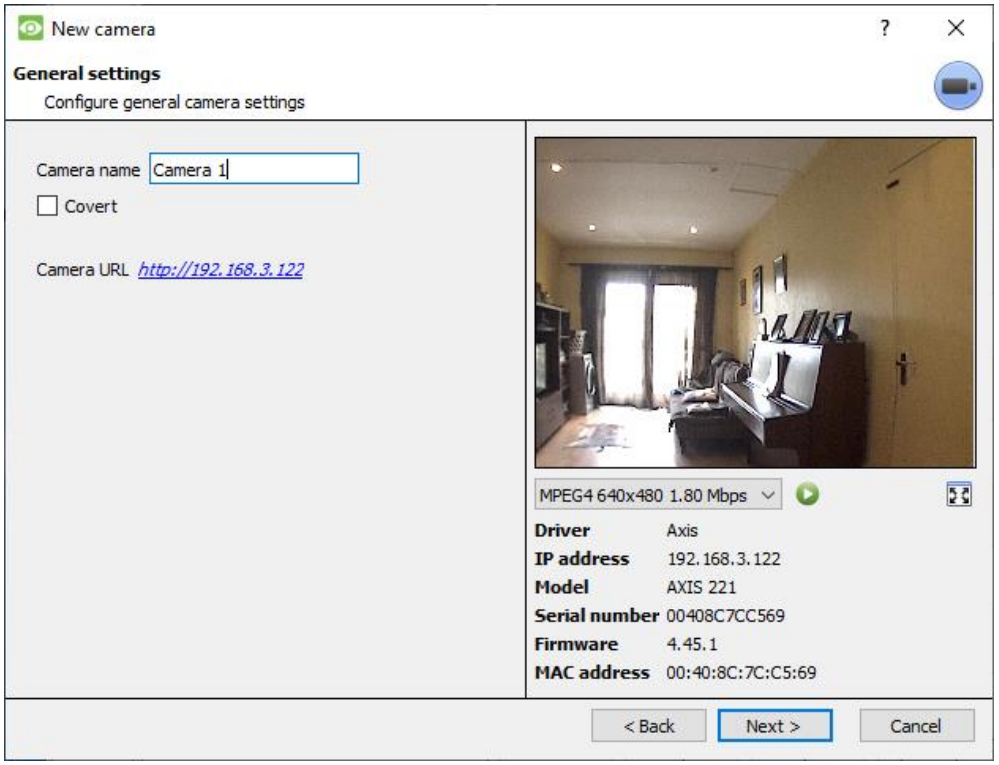
Notes on adding a new video input:

1. When adding a new video input to an existing camera, the user will be unable to change the IP address of that camera.
2. This option is not available when connecting a **CathexisVision 2015** site to a later site, as this option is exclusive to later versions.

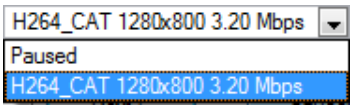
Notes on scanning:

1. Some Cameras do not support automatic location requests, and will not be found using **Scan.**
2. Universal Plug and Play (**UPnP**) will have to be enabled on the cameras that do support location requests.

4.2.2.1.2 General Settings

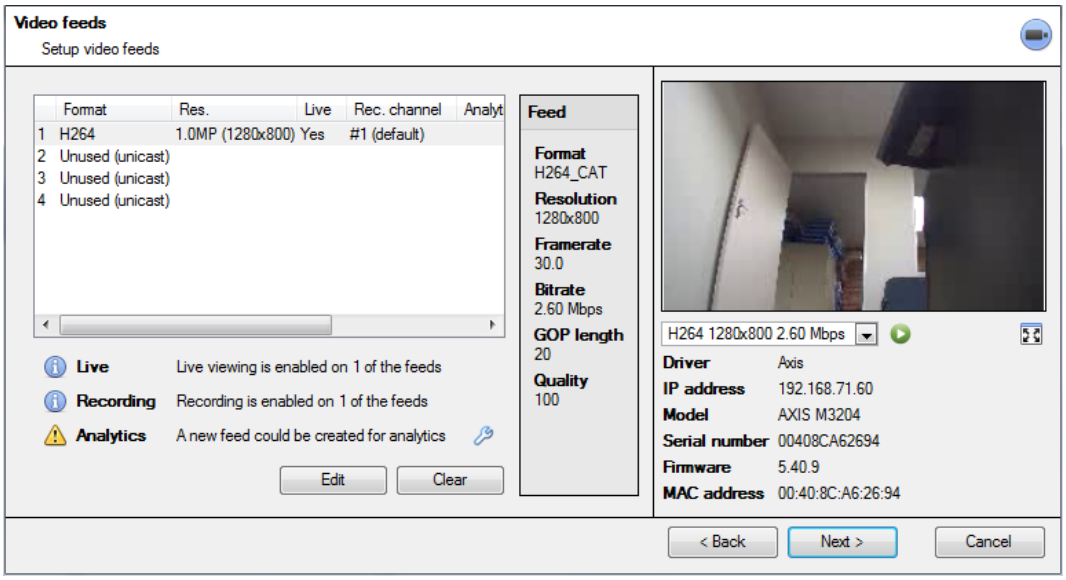


Name	Give the camera a descriptive name, to make it easily identifiable in a list.
Covert	**CathexisVision** gives the option to create a covert camera. There is a difference between a camera being covert, and a user not having access to it. **Covert**: Camera will only be present in the Resources List of an Administrator, or an access level that has been granted access to this camera. **Access Level Defined**: Camera will still appear in the Resources List of lower login levels, but these levels will not be able to view the feed.
Device Information	This will be a list of all the relevant information, pertaining to the device itself. It can be seen underneath the image preview.

Live Preview		The image displayed is a frame grab from the chosen video feed. To play the live preview, click on this icon. To enlarge the image, click on this icon.

Note: The image in the preview does not reflect the true quality of the feed, because it is transcoded when viewed in the camera addition wizard.

4.2.2.1.3 Video Feeds

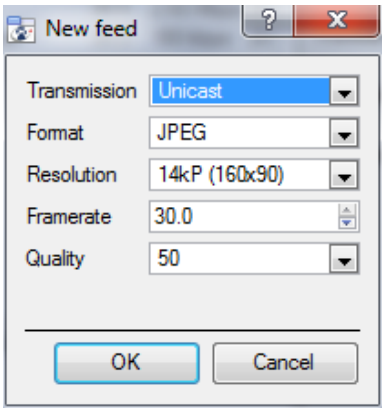


Add / Edit a Video Feed

To add / edit a video feed, click on one of the available feeds in the list. Click on the **Edit** button.

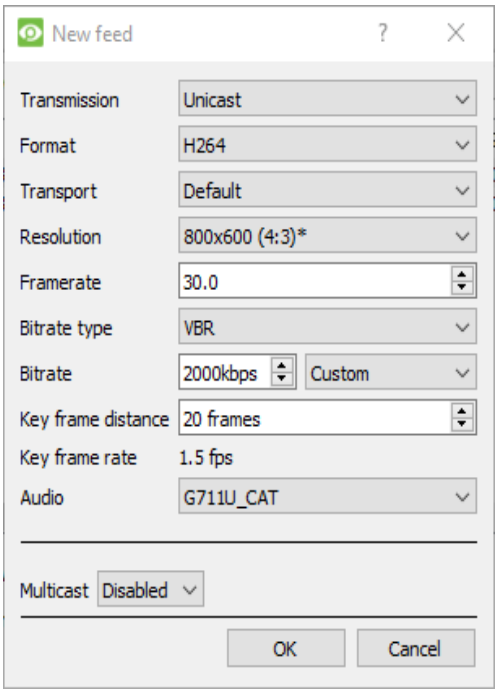
This will bring up a feed dialogue with the available video feeds, and the options that apply to them. The two most common IP feeds are JPEG and H.264 (MPEG4).

JPEG



Transmission will show the transmission type.
Format is the compression format used by this stream. Click the drop-down menu to choose the one desired.
Resolution is the number of pixels in the image.
Framerate is the number of frames recorded per second.
Quality defines how lossy the compression of the image is. At 100, the image will have the best quality. At 50, it will have the lowest quality.

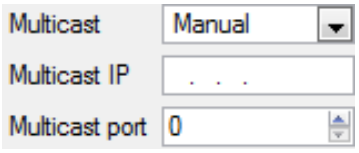
H.264



Transmission: the transmission type.
Format: the compression format used by this stream. Choose the format from the drop-down menu.
Transport: Select the transport protocol. The default option is Cathexis UDP streaming. Other options are RTP streaming using Live555, either over UDP or TCP.
Note: refer to Appendix B for more information about the differences between UDP and TCP.
Resolution: the number of pixels in the image.
Framerate: the number of frames recorded per second.
Bitrate Type: the way that the bitrate is handled. A constant bitrate will be more predictable, but will lose more information the more the image changes. Variable bitrate is less predictable, but will have better images when the picture has more motion.
Bitrate: the amount of information, in bits, that the feed will send per second. (**Quality** defines how lossy the compression of the image is.)
Key Frame Distance (GOP Length): the number of frames between each I-Frame (Key Frame).

MULTICAST

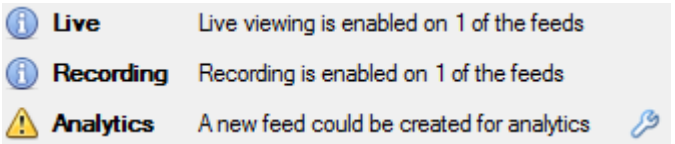
Set up Multicast on feeds by selecting the relevant option from the feed dialogue. There are 3 options: **disabled**, **auto**, and **manual**. **Note**: to not use Multicast, leave it disabled.



With **Manual** selected, enter the Multicast IP, and Multicast Port.

On **Auto**, the Multicast address will automatically be assigned. The core settings can be found in the General Site Setup section of the Setup Tab.

Feed Notifications



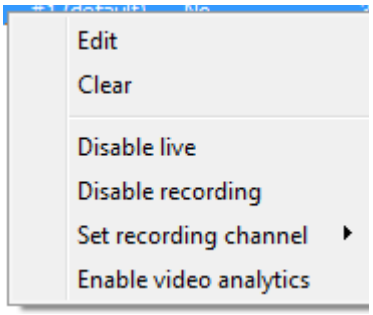
This area will show the status of the feeds created – whether **Recording**, **Live Viewing**, or **Analytics** is enabled.

Note: click on any of the icons to display detailed information about the feed / problem.

Automatic Configuration: If there is a **spanner** icon at the end of the feed notification, this means that there is a potential problem with the feed setup. Click on the icon to automatically fix the problem.

4.2.2.1.4 Right-click Menu (Live, Recording, and Recording Channel Settings)

Right-clicking on a feed after it is set it up will bring up the menu shown below. These settings can only be accomplished after the feed has been set up.



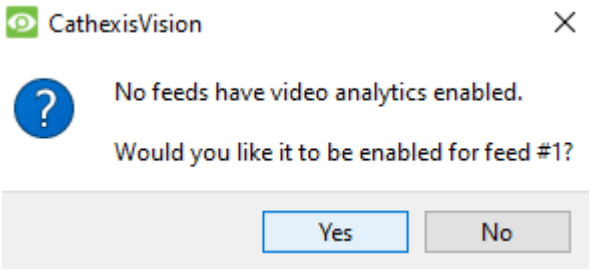
Edit	Add/edit a feed.
Clear	Clears the feed.
Disable Live	viewing of the feed.
Disable Recording	of the feed.
Set Recording Channel	Define which channel number will represent this feed.
Enable Analytics	Enable Video Analytics.

Analytics

Create a second feed in order to enable analytics on a unit. Right-click feed / **Enable Analytics**.

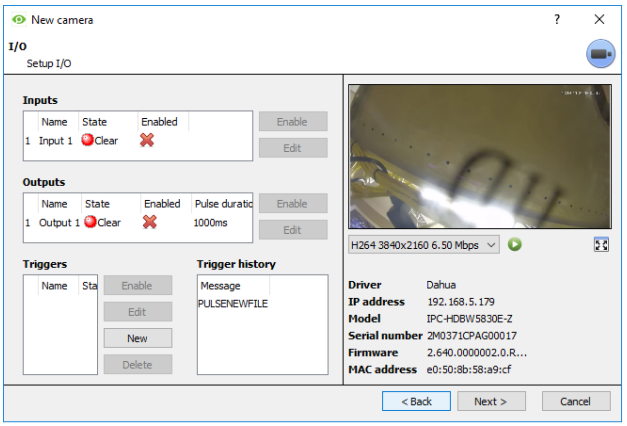
There are a few rules relating to enabling analytics:

1. If an analytics-enabled channel is not set up, there will not be a prompt to add a Video Motion Detection (VMD) later in this wizard. Nor can one add VMD using this feed later.
2. Only feeds that are QVGA resolution and lower will give the option to enable analytics.
3. If there is a spanner icon at the end of the Analytics feed notification, the feed is not enabled for analytics. Clicking on the spanner icon will automatically enable one.
4. **Note**: if the user chooses to proceed without enabling analytics, a prompt will appear. One can also enable video analytics by this route.



4.2.2.1.5 I/O

The next step in the addition is the I/O setup. The I/O values represented in the GUI will depend on the I/Os provided by the encoder.



Inputs are used to trigger an event; **Outputs** are used to give a desired output as a result of a triggered event.

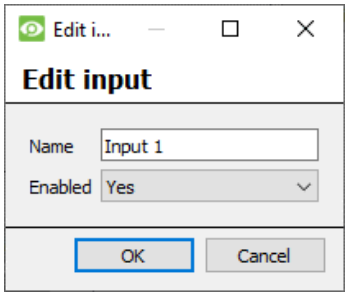
Renaming

Click on the I/O name to rename it.

Enabling

Click on the red cross or click the enable button. Once enabled, it may be used to trigger an event.

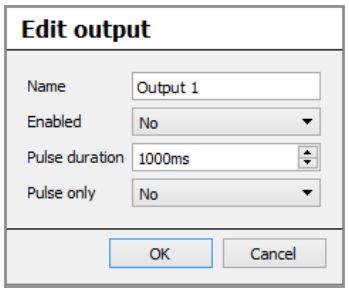
Edit an Input



Name: Give the input a descriptive name.

Enabled: Will indicate whether the output is disabled / enabled.

Edit an Output



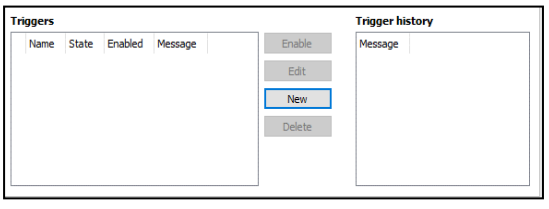
Name: Give the output a descriptive name.

Enabled: Will indicate whether the output is disabled / enabled.

Pulse duration: Will set the amount of time (in milliseconds) that the output will pulse for, if it is set to pulse.

Pulse only: If set to Yes, the output will not allow itself to be permanently Set.

Triggers



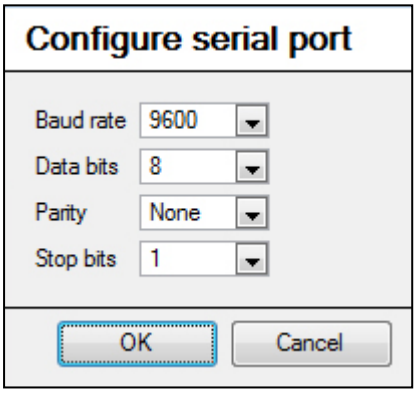
Most cameras have their own event or edge triggers. Encoders will often have I/O options.

Select **New** to either choose from a list of supported camera triggers, or define a custom text message (Axis cameras) as configured on the camera.

Note:

1. Clicking on any of the column values (Clear / Set; Enabled / Disabled) of an I/O will toggle the value. For example, clicking on a Clear state will change the state to Set. These options are available via the Right-click menu.
2. Give the I/Os descriptive names. Otherwise, they will not be identifiable.

Serial Ports

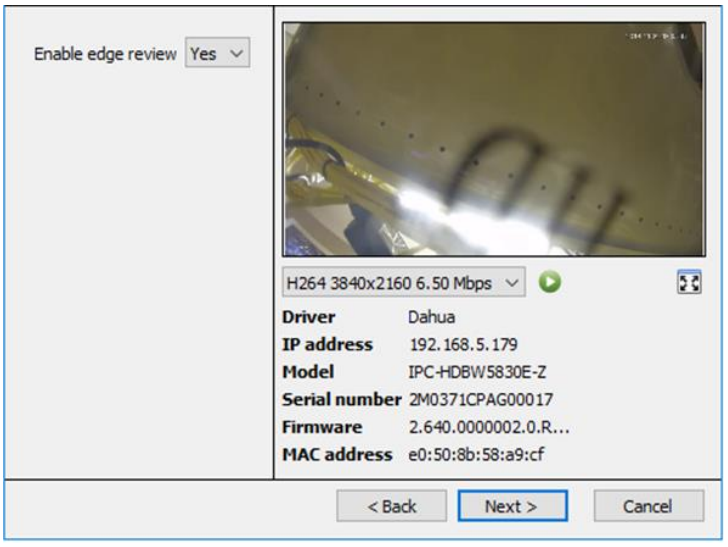


Highlight the serial port to configure. Then click the **Configure** button.

This will give the option to change the **Baud rate**, **Data bits**, **Parity**, **Stop bits**, and other camera-dependent settings.

Note: This option will only be available if the camera has serial ports.

4.2.2.1.6 Edge Review Setup



Cameras which support Edge recordings will have an additional tab in the camera wizard. This enables viewing of the camera's onboard Edge database within CathexisVision.

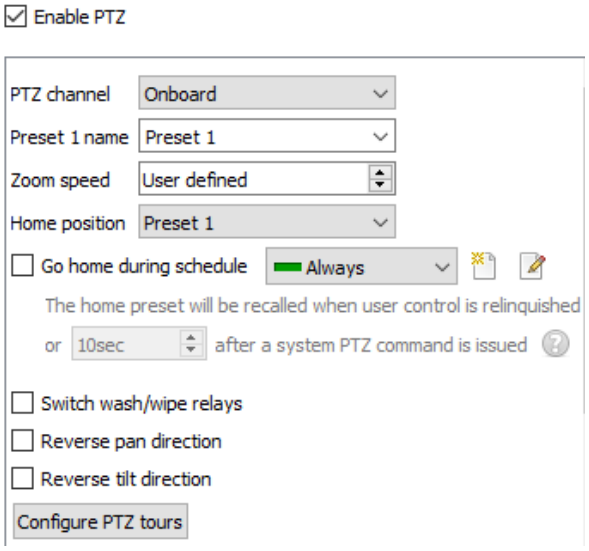
Select **Yes** from the drop-down menu to enable the database.

When this is enabled, the camera's Edge database will be available for selection in camera review, as with other CathexisVision system databases. If this is disabled, the database will not be available for selection.

4.2.2.1.7 PTZ

Check the **Enable PTZ** box if adding a PTZ camera. After this, all the available PTZ options will appear in the Wizard interface.

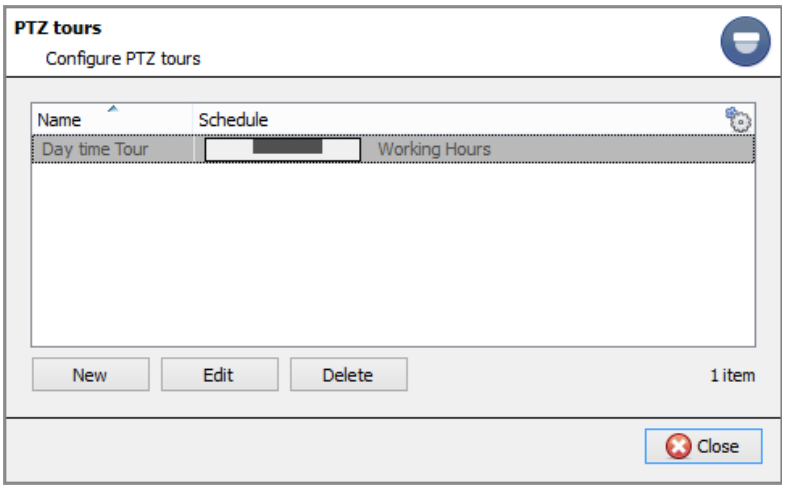
General Settings



Note: These options may vary on a camera-by-camera basis. PTZ channels can be added in 2 ways: either Onboard or Serial Port.

Preset Name	Give Presets descriptive names (such as 'front door' etc.)
Zoom Speed	This defines how fast the camera will zoom in when using the PTZ controls. **Note**: Test zoom speed by clicking **Zoom** on the PTZ control wheel of the live view panel to the right.
Home Position	A home position is a pre-set position to which the camera will return after a set period of inactivity. Automatic Return to Home: Set a **schedule** during which the camera will return to its home position. When the schedule is inactive (see Schedules), the camera will remain in the last position that it was left. If there is no schedule set, the camera will never automatically return to its home position. To have it always return home after a certain period, simply enable the Every Day schedule.
Switch Wash and Wipe Relays	In the case that the Wash and Wipe relays are incorrectly attributed, this will swap them over to the correct order.
Configure PTZ tours	A PTZ tour will run through a sequence of pre-set positions. (See section immediately below.)
Reverse Pan Direction	Will swap the pan direction. Left is right, and right is left.
Reverse tilt direction	Will reverse or swap the tilt direction. Up is down, down is up.

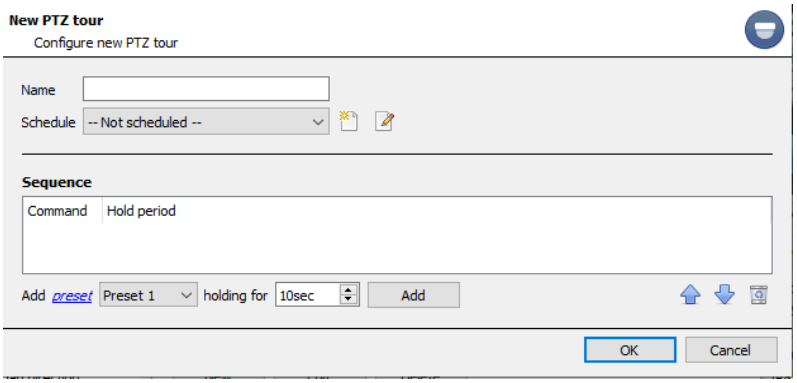
Configure PTZ Tours



Multiple tours may be configured.

To add/edit a tour, click on **New/Edit**.

This will open up the PTZ tour configuration dialogue.

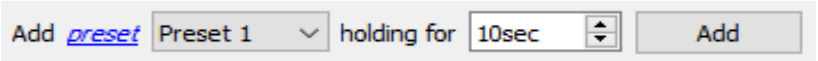


Name: Give the tour a descriptive name.

Schedule: If necessary, give the tour a schedule. (Refer to Schedules section.)

Sequence: this is the sequence in which the Presets will run.

Add Preset, Multiple Presets, or a Pattern to the Tour



Select the **Preset**. Set how long the camera should linger at this Preset.

Multiple presets:

- Starting at: Select the first Preset to add.
- Add: this is the number of Presets to add.

In the example above, Presets 4 to 6 will be added.

Select the **Pattern** to add.

PTZ Procedures

With a Pan-Tilt-Zoom (PTZ) camera an operator can manipulate the camera's direction, Zoom, focal distance (Focus) and amount of light (Iris). The operator can also control pre-configured camera views called “Presets”.

A Dome Control Panel becomes available when a Live PTZ camera is selected in the **CathexisVision** interface.

Click the panel’s drop-down menu and select **PTZ.**

The software joystick displays the options below.

Note: Remember to select / play a live feed.

Using the PTZ Control Panel

Pan Left/Right: Drag joystick left / right**.**	**Tilt Up/Down:** Drag joystick up / down
Move Camera Faster: Distance determines speed - drag joystick out, in required direction.	**Move Camera Slower**: Distance determines speed - drag joystick closer in, in required direction.
Zoom In/Out: Watch the live camera w**hile** pressi**ng** the Zoom in and Zoom out button.	**Focus Further/Closer**: Watch the live camera while pressing the Focus near and Focus far button.
Go to Preset: 1. Select the Preset from the drop-down menu, and then click GO. 2. The camera view will change to the Preset. 3. To relinquish manual control of the dome/PTZ camera from the PTZ panel, click Auto. 4. If t**he** system runs remote tours automatically, or switches displays based on events, these automated responses will take over.	**Gain Control of Dome/PTZ**: (Applies if system runs remote tours automatically, or switches display based on events.) Either click manual, or simply move the software joystick.
Lighten/Darken Live Camera View: Press the iris open or iris closed button. The image **will** lighten or darken.	**Define a Preset**: 1. Select the Preset number, from the drop-down menu. 2. Use the joystick controls to establish the Camera View, Zoom, Focus, and Light (Iris). 3. Click SET. 4. Go to this Preset to check it.

PTZ Priority Control

Control of a PTZ camera works on a priority system to determine who gets control of the camera, should more than one user at a time attempt to control the camera. Administrators get the highest priority. After administrators, the priority hierarchy runs from User Level 30 down to User Level 1.

For example, should a Level 10 user and a Level 1 user attempt to control the PTZ camera, the Level 10 user will get priority control. An administrator would get priority over both.

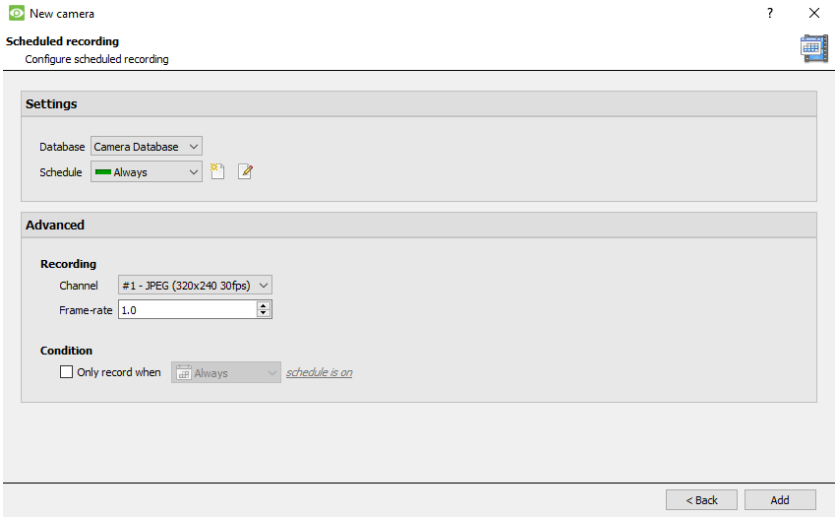
Note:

1. If two users of the same user level attempt to control the camera, then the first user gets priority. The second user will have to wait until the 'Dome override' period has elapsed.
2. Manual control of the camera takes priority over event-initiated / auto control of the dome.

4.2.2.1.8 Configure Camera

The operator can now add motion recordings and configure camera access rights.

Enable scheduled recording



Navigate to motion recording by visiting

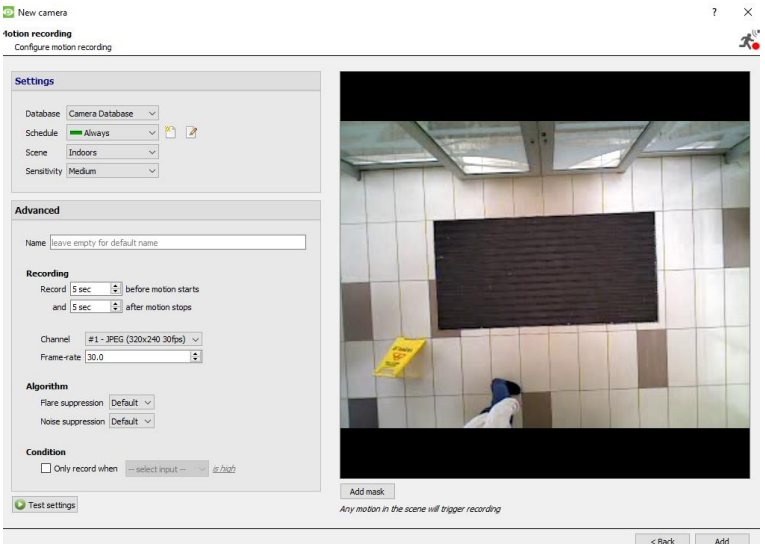
Setup / Configure Servers / Expand the server / Motion recording.

Scheduled recording can be enabled in the Camera addition wizard.

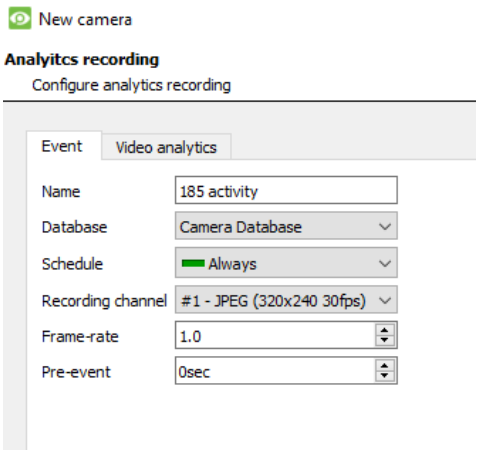
Here, set Database, Schedule, Channel, Frame-rate, and Condition.

Enable motion recording

Motion recording can be enabled. here, the user can set Database, Schedule, Scene, Sensitivity, Recording time before and after motion, Channel, Frame-rate, Flare Suppression, Noise Suppression, and Condition. One can also Add mask and Test settings.

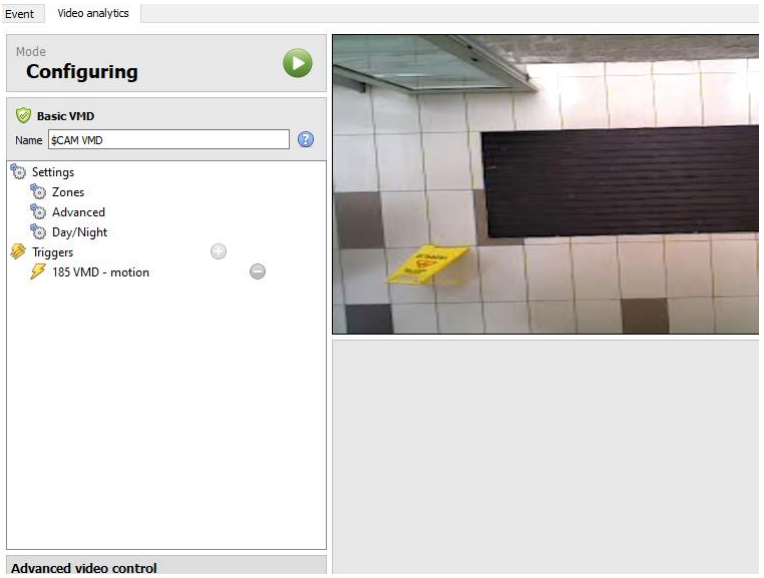


Enable analytics recording



When configuring analytics, under the Event tab, set:

Name, Database, Schedule, Recording channel, Frame-rate, and Pre-event.

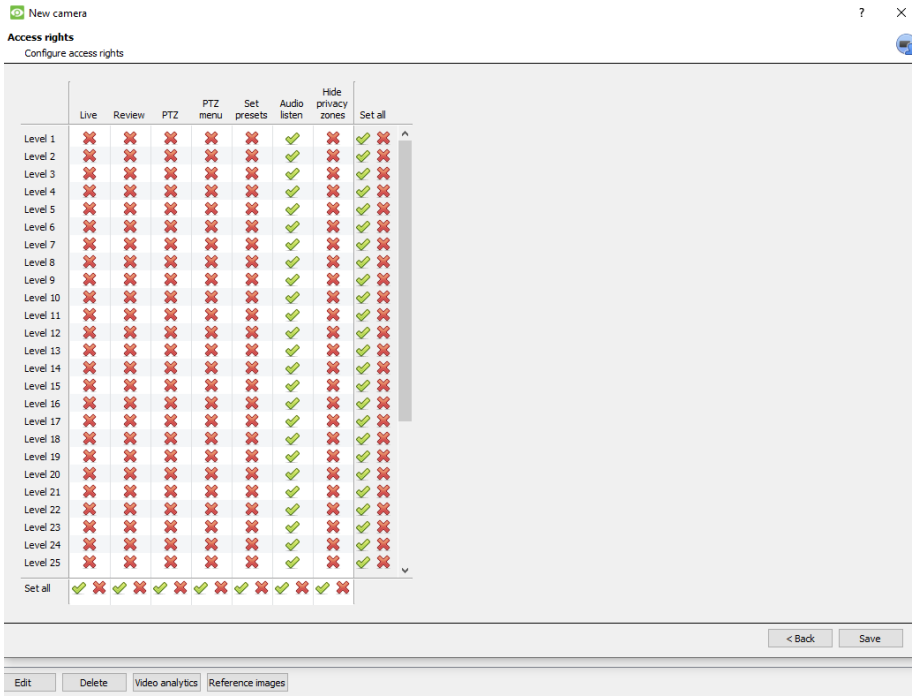


When configuring analytics under the Event tab, set Zones, Advanced options, Day/Night settings, and Triggers.

Advanced video control may also be used.

Configure access rights

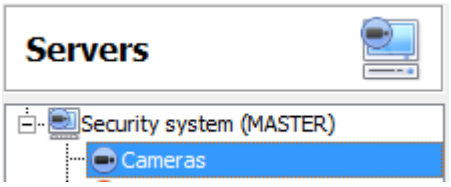
Configure relevant Access rights by clicking the **Configure access rights** button.



4.2.2.2 Camera Addition Method 2: Copy / Paste Cameras

The second method of adding a camera is by Copy / Paste. This is accessed by right-clicking on an existing camera.

If adding more than one camera that operates on the same driver, CathexisVision offers an easy solution. Copy and paste new cameras, retaining the information of the camera selected for copying.

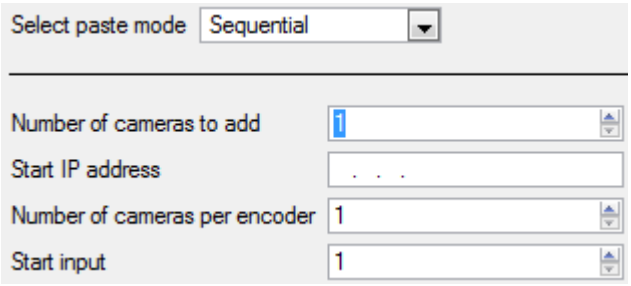


To Copy/Paste new cameras, navigate to the cameras panel of the desired unit, right-click on the previously added camera and click on **Copy**.
Then right-click anywhere in the Cameras Panel and click on **Paste new…**

There are two ways to paste cameras: Sequential, and Discovered. These are discussed below.

4.2.2.2.1 Paste mode: Sequential

The paste mode sequential window provides the option to add the new cameras as a direct copy of the camera that copied.

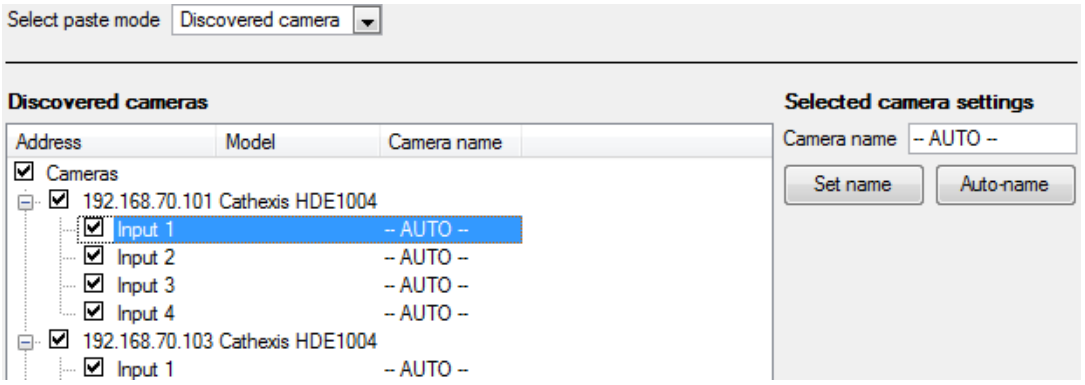


Start IP Address will determine the IP address of the first new camera being added. The IP addresses will be incremented from here. (So, make sure an IP address in this range has not been used.)

Total channels on encoder must be the full number of channels available on this encoder.

Start Input is the actual physical channel the first camera should be added to.

4.2.2.2.2 Paste mode: Discovered



Note: This will copy the video settings from the copied camera onto the discovered cameras selected.

4.2.2.2.3 Copy / Paste Video Settings

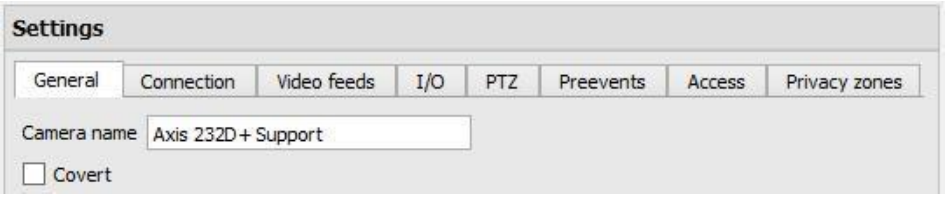
If a number of cameras with the same drivers have already been added, to simply transfer the Video Settings of each camera across, right-click and select **Copy**. Then right-click on the camera to add the video settings to, and select **Paste video settings**.

Note:

1. This is just the Video Feed settings. It will not add Video Motion Detection analytics.
2. Only copy onto cameras that have the same driver as the camera that has been copied.

4.2.3 Edit Existing Camera

Note: If making any changes to the setup of a camera that is currently multicasting, restart the streams. This simply entails removing and reselecting the cameras in the Cameras tab, after settings have been saved.



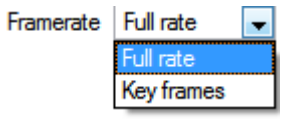
Edit an already added camera by selecting it and clicking on **Edit**.

4.2.3.1 Repeated vs Additional Options

The camera setup options of General, Connection, Video Feeds, I/O, and PTZ are all dealt with in the Camera Addition Wizard section. Three options are added in the Editing Tabs: Pre-events, Access Levels, and Privacy Zones. These options will be dealt with below.

Note: The Wizard covers the process of setting up a Database, Scheduled Recordings, and Video Motion Algorithm triggered recordings. The Tab Edition only changes camera settings, and therefore does not have these extra options. Databases, Scheduled Recordings, Algorithms, and Events all have their own panels under Configure Servers.

4.2.3.2 Pre-events tab



Pre-events were setup under the Activity Recording Section of the Wizard.

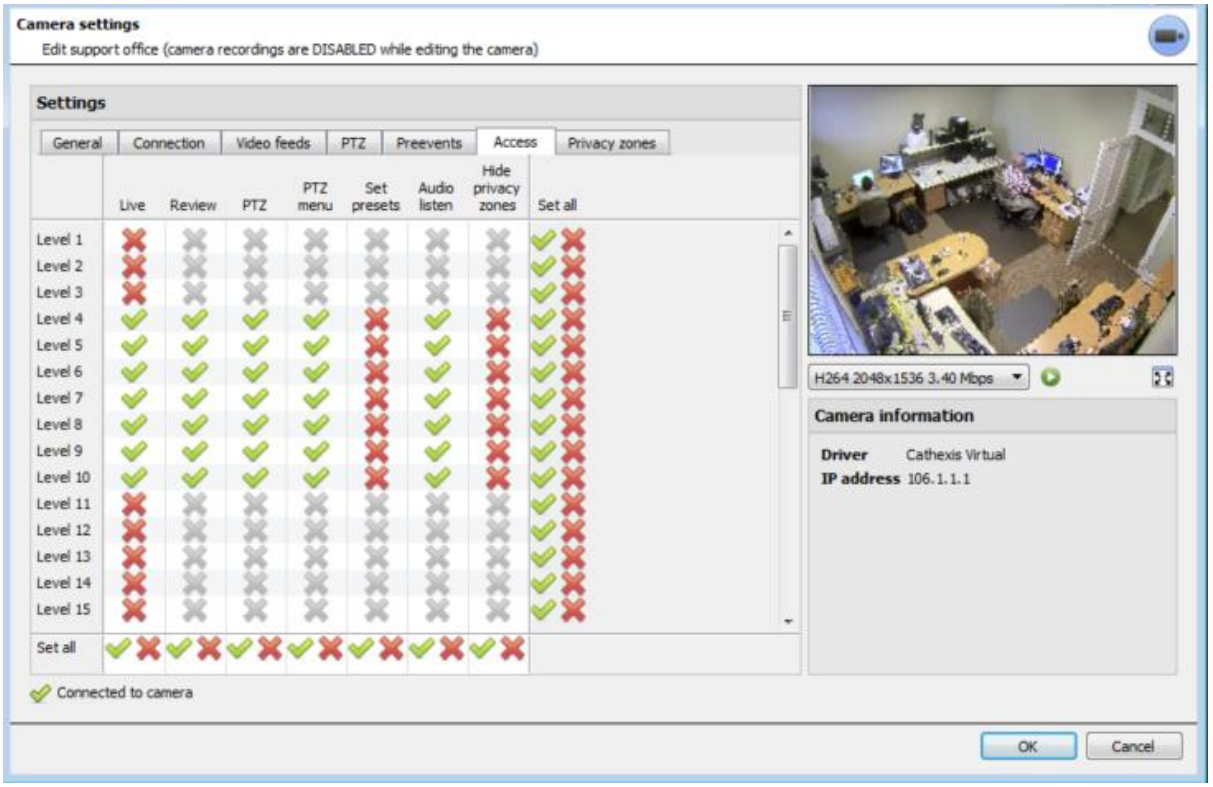
The number of pre-events cannot be defined here, but one may define the frame rate of the pre-events in this tab.

Note: JPEG is recorded in Key Frames, so only the option of **Frames per Second** will be provided when setting the pre-events on a MJPEG stream.

4.2.3.3 Access tab

Under the **Access tab**, setup which user levels have control of the different facets of the camera.

In the **Cameras** section, under **Your_Server_Name**, select the camera, click **Edit** and select the **Access** tab.



A tick means that this level has access.

A cross means that right to access has been denied to this level. Left-click on the tick / cross to change its designation.

A greyed-out cross means that this right requires another right to be set in order for it to be enabled. For example, one cannot give a user rights to Review, or use PTZ unless Live Viewing is enabled. Disabling Live Viewing will automatically disable the rest of the user rights.

The administrator should therefore be careful to enable the Live Viewing access right for the user levels, which will need to view and manage the video stream.

Important Note on Access Rights:

1. All access levels on this unit are managed in the Access Rights Panel of the Server. (**Site / Open Tab / Setup / Configure Servers / Expand the Server / Access Rights**)
2. Access rights pertain to the access levels assigned to specific users. If a user is given Level 1 access, and this camera is only assigned to other levels, that user will not see this camera (users are managed in the **Site / Open Tab / Setup / Users**).
3. Non-admin users may be given the right to configure other non-admin users. See the section 3.5 for more information on this.

Live	This controls which Access Levels can view the camera's live feed. If this option is disabled, the user will not be able to view the camera at all, and all the following rights will be automatically denied.
Review	This controls which Access Levels can review recorded footage from this camera.
PTZ	This controls which Access Levels can control PTZ movement.
PTZ Menu	This controls which Access Levels have the ability to alter the PTZ menu.
Set Presets	This controls which Access Levels can change PTZ Preset positions.
Audio Listen	This controls which Access Levels can listen to the audio associated with the camera.
Hide Privacy Zones	This controls which Access Levels can remove the privacy zones added to the camera.
Set All	Selecting the tick will give this level access to all settings; selecting the cross will give this level access to none.

4.2.3.3.1 Audio Listen Access Right

The table below details situations in which the Audio Listen access rights settings, configured by the user, do and do not apply.

Audio Listen access right settings do apply to:	**Audio Listen access right settings do not apply to:**
Live viewing. Reviewing from the camera tab. Reviewing from the database tab (both video and integration databases). Viewing video when handling an alarm in the Alarm Management Gateway.	Independent audio channels. Archived video. Connecting to a 2016.2 server using a 2015/2016.1 viewer. Connecting to a 2016.1 server using a 2016.2 viewer.

4.2.3.4 Privacy Zones Tab

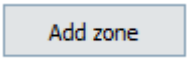
Note: Adding/editing **Privacy zones** is not a part of the camera addition Wizard, and can only be completed by editing a camera after it has been added.

Adding a **Privacy zone** will hide an area(s) of the camera image. The **Privacy zones** can be hidden or shown by an administrator, or user levels which have been assigned the access rights to do so. The **CathexisVision** system will record the footage behind the privacy zone, but only users with access rights will be able to view it.

This feature is useful, as some areas of the video stream may contain sensitive information, which require certain clearance levels to view. For example, a camera operator in a bank might not be privy to footage in which money is being counted, but if there is a dispute surrounding the money then a user with the correct access level will be able to hide the **Privacy zone** and review the dispute.

4.2.3.4.1 Add a Privacy Zone

Once the Wizard is complete, open the camera for editing again. Navigate to the Privacy Zones tab.

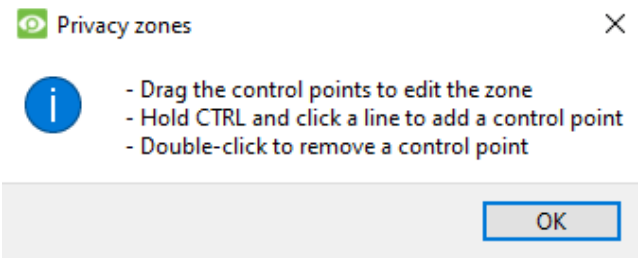


Add a new privacy zone to the camera image.

Clear all privacy zones from the camera image.

Clear only the selected zone from the camera image.

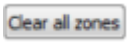
Clicking this shows instructions on defining the shape of a privacy zone:



Reshape a Privacy zone

- Click and drag the control points at the corner of the box. (Select a Privacy Zone to bring up control points.)
- CTRL-click on a line to add a new control point.
- Double-click an existing control point to remove it.

Remove a Privacy zone

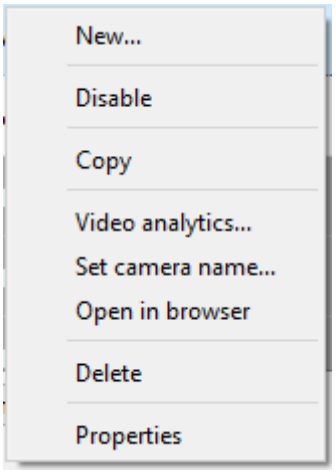
- To remove all, click **Clear all zones**. 

- To remove specific zones, select and click **Clear selected zone**.

Once done, click **OK** to save.

Note: refer to the ***CathexisVision Operator's Manual*** for instructions on hiding or showing privacy zones in the Cameras Tab.

4.2.4 Right-click on a Camera

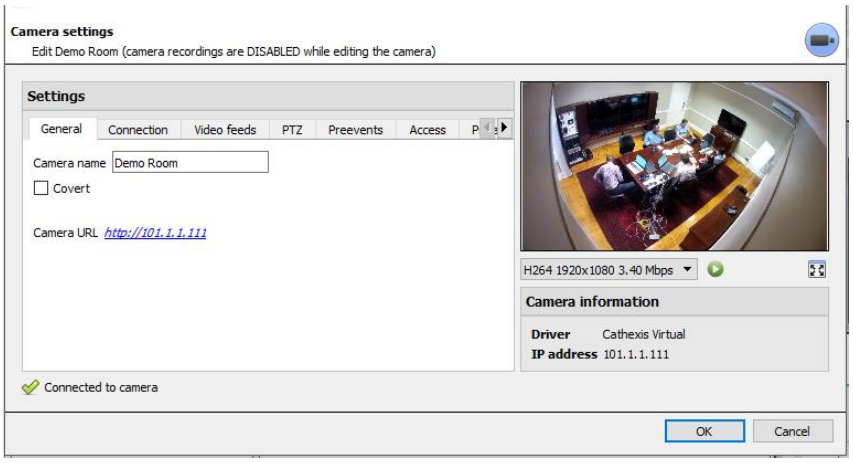


New…	Add a new camera.
Disable	Disables the current camera (but does not delete it).
Copy	Copies camera settings and enables them to be pasted onto a new camera or existing camera.
Video analytics…	Opens Edit Video Analytics window.
Set camera name	Edit the camera name without having to open the edit window.
Open in browser	Opens camera URL in web browser.
Delete	Removes camera from site.
Properties	Opens properties window (below), and enables editing the camera.

Note: **New**, **Paste New**, **Copy**, and **Paste Video Settings** are all dealt with under Copy Paste Cameras.

4.2.4.1 Camera Properties

Right-click camera and select **Properties**.

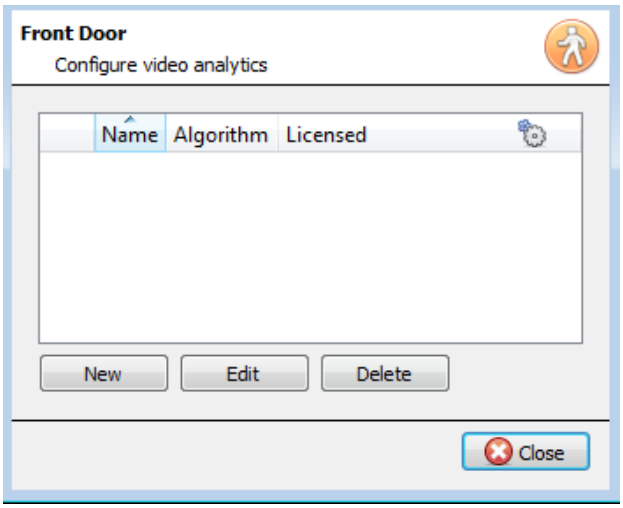


All camera settings configured during the Camera Addition Wizard can be edited by selecting the various tabs.

The Camera URL of the specific camera is listed automatically when the camera is added.

4.2.5 Video Analytics Button

Select a camera from the list. Click the **Video Analytics** button at the bottom of the cameras to add / edit video analytics. This can also be accomplished by following **Setup Tab / Configure Servers / Video Analytics**.



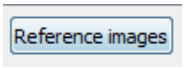
The window will open (shown on the left here).
If any video analytics have been set up, they will appear here.

Click **New** to add new analytics to the camera, or click **Edit** to edit existing algorithms.

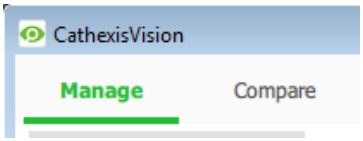
For more information on video analytics, refer to the Video Analytics section.

4.2.6 Reference Images

Creating a reference image will capture the orientation of all system cameras and save images for reference later on. These reference images can then be compared to older reference images, as well as the current orientation of cameras, in order to determine possible differences. Reference images can also be exported for review.

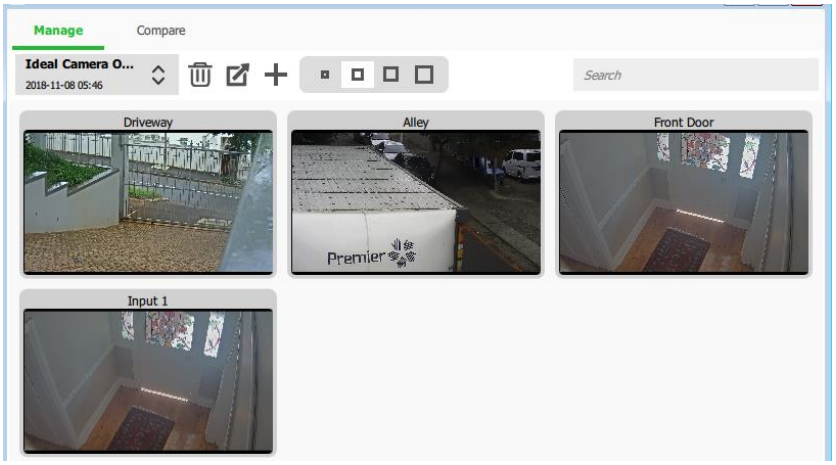


Click the **Reference images** button to open the reference image management interface.



The Reference Image management interface has two tabs: **Manage** and **Compare**. These are dealt with below.

4.2.6.1 Manage Tab

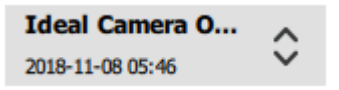


Here, reference images can be created, deleted, exported, searched, and reviewed.

If reference images have already been created, the most recent one will display its capture cards (reference images for system cameras).

See below for interface guide.

4.2.6.1.1 Select and View Existing Reference Image

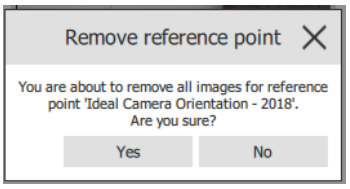


Select between existing reference images using the drop-down menu. Click on any capture card to expand.

4.2.6.1.2 Manage Reference Images

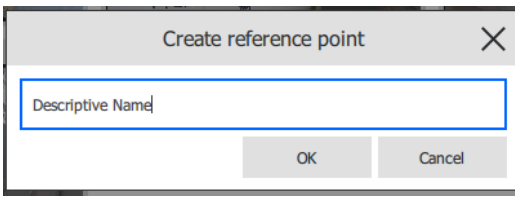
Select a reference image from the drop-down menu. Click this icon to delete it.

A prompt window will open, asking:



Select a reference image from the drop-down menu and click this icon to export it. A window will open which requires the selection of an export destination. Reference images for all cameras are saved as individual JPEG files to the selected destination.

Click to create a new reference image, which will capture images of the current orientation of all system cameras. A window will open.



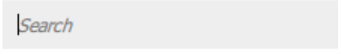
Give the reference image a name, making it easier to identify and compare later on.

Click **OK** when done.

4.2.6.1.3 Capture Card Size

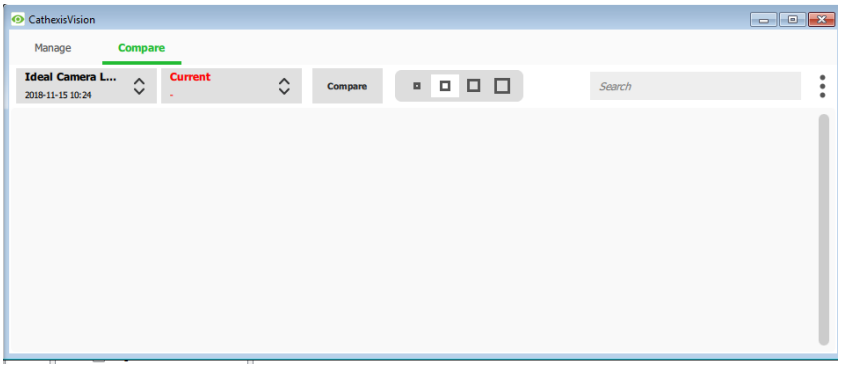
Select the desired display size of the reference image capture cards.

4.2.6.1.4 Search



Search for camera names to view capture cards. This is useful in sites with more cameras, because manually searching may be too time-consuming.

4.2.6.2 Compare Tab

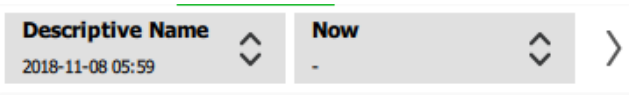


In this tab, comparisons take place between reference images.

When a comparison has been done, capture card results are displayed in the blank space.

See interface guide below.

4.2.6.2.1 New Comparison

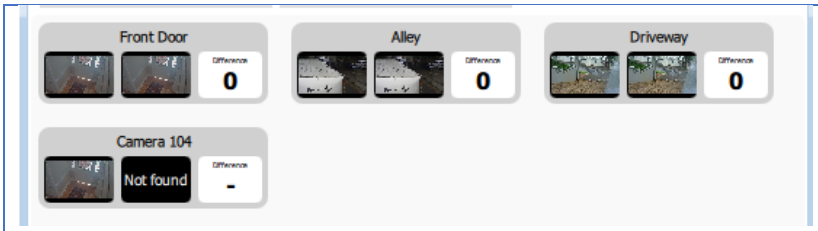


To perform a new comparison, select two reference images (or 'Now') from the drop-down list.

Click the arrow button on the right. ›

Comparisons can be performed between two existing reference images, or between a reference image and 'Now' – this being the orientation of the cameras as they are at this point in time (not a reference image).

4.2.6.2.2 View Comparison Results



The results will display the capture cards for each camera side-by-side while the number of differences found between them is shown on the right.

Click on the capture cards to expand and view the differences.

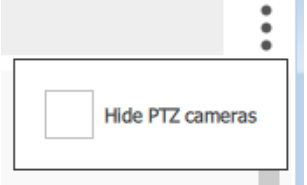
Note: If cameras are removed from the system between the creation of reference images, the results will display a 'Not found' capture card for the reference image that is missing the camera.

Select the desired display size of the reference image capture cards.

Perform a search for camera names to view comparison result capture cards for that camera.

Click to open the Options menu.

Currently the only option is:



4.3 Video Analytics

This is a guide to the Video Analytics setup process, provided to give users a deeper understanding of the algorithms and enable them to make informed decisions. The setup process requires tweaking in order to get right. Video analytics need to be adjusted on a situation-by-situation basis.

Note:

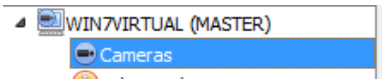
1. Algorithm names changed in CathexisVision 2017.2:

Previous name	New name
Analytics I	Basic Analytics
Analytics II	Intermediate Analytics
Analytics III	Advanced Analytics

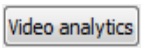
2. Advanced Analytics contain the Basic and Intermediate Analytics. Therefore, if a camera is licensed with Analytics III, the user does not need to add licenses for I and II. They will already be included.
3. The new **CathexisVision** video analytics algorithms (which were added in **CathexisVision** 2015 and licensed using Analytics I, II, and III) are only available on Linux and Windows NVRs.
4. Units running CathexisVision 2016 cannot connect forwards to units running CathexisVision 2017.2. If the user attempts this, a message will appear to update the GUI interface.
5. The Top-down head tracker algorithm (in the *Analytics type* analytics) and the Top-down head counter (std) algorithm (in the *Counting type* analytics) are not available in CathexisVision 2016. Therefore, if the user connects from a 2017.2 unit backwards to a 2016 unit, these two algorithms will not be available.

4.3.1 Accessing Video Analytics: two methods

4.3.1.1 Option 1: Via the Cameras Panel



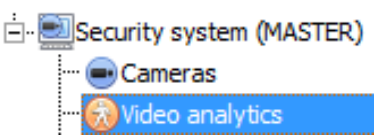
Setup Tab / Configure Servers / Cameras / Select camera / Right-Click or click button at the bottom of the tab.



Note: When adding algorithms in this window, the algorithm will only be associated with the selected camera.

Note: this is a quick setup method for a camera that has been previously licensed for video analytics. However, this method does **not** give the user the ability to associate an analytics license to a new camera.

4.3.1.2 Option 2: Via the Video Analytics Panel



This lists all Algorithms that are related to cameras on this server.

There are two ways to add analytics to a camera: **copy-paste** function (4.3.2) or **configure new analytics** (4.3.3).

4.3.2 Copy-Paste Analytics

Existing Algorithm settings may be copy-pasted to overwrite algorithms on other cameras. Or algorithm settings can be pasted onto cameras with no existing algorithms applied.

4.3.2.1 Copy / Paste an Algorithm

Copy / paste Algorithm settings either from one algorithm to another, or from one algorithm to a new camera. These settings may be copied across servers or across sites (as long as both sites are running the same version of CathexisVision).

4.3.2.2 Copy algorithm settings from one algorithm to another

Right-click on an existing algorithm, and then click on Copy. Then right-click on the algorithm to be overwritten and click Paste.

4.3.2.3 Copy algorithm settings as a new algorithm

Copy the algorithm settings onto a camera: right-click and copy the existing algorithm. Then right-click anywhere and select **Paste new…**

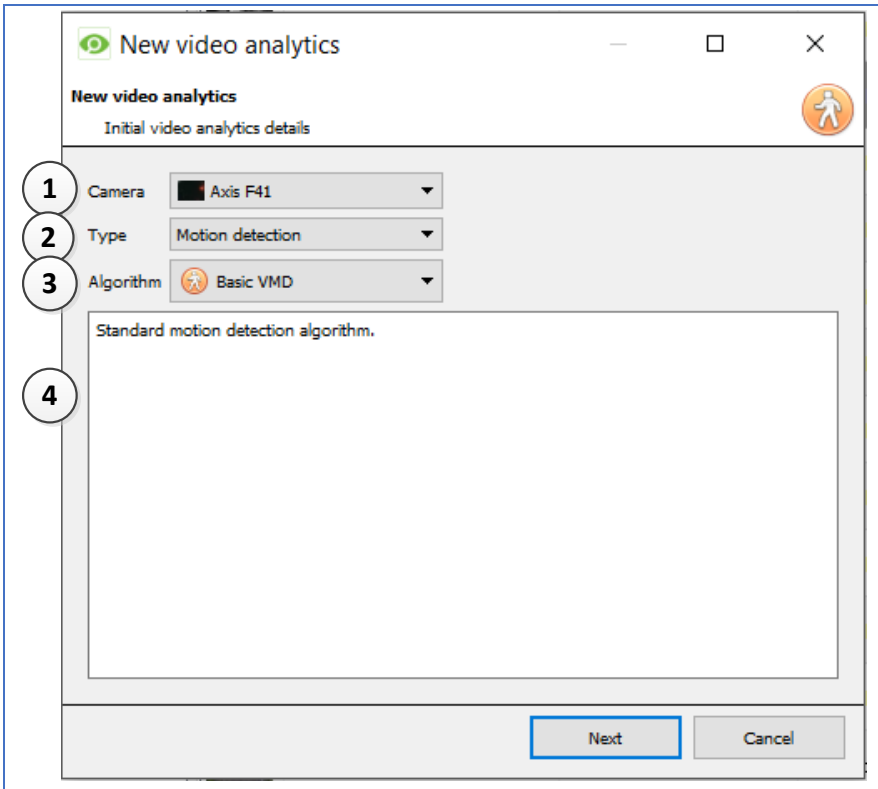
This will bring up a list of cameras that are attached to this unit (for example, Analog One).

Select to paste the algorithm onto any number of cameras. Click OK.

4.3.3 Configure New Analytics

To configure new analytics for a camera: Right-click and select **New,** or click the **New** button.

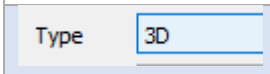
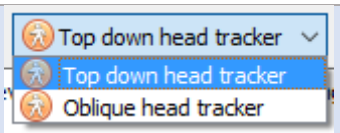
4.3.3.1 New Video Analytics Selection Interface Guide

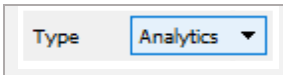


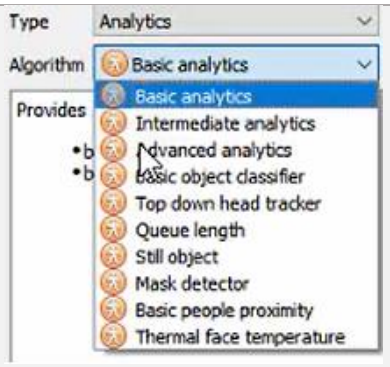
Area	Description
1	Select the **Camera** that analytics will be added to.
2	Select the broader video analytics **Type**.
3	Select the **Algorithm** to apply. Algorithm options differ according to analytics **Type** selected (above).
4	The **description field** describes the features of the algorithm.

4.3.3.2 Select the Algorithm

The table below explains the Analytics Types and Algorithm options.

Analytics Type	Algorithm Options	Description
		**<u>Top-down head tracker</u>** - Trigger events when heads cross a line using a 3D camera looking straight down. **<u>Oblique head tracker</u>** - Trigger events when heads cross a line using a 3D camera mounted at an angle (not looking straight down). For configuration, consult the ***CathexisVision 3D Headcounter App-note (Discontinued)***.





Basic analytics

Trigger events using:
- basic line crossing triggers
- basic presence triggers.

Intermediate analytics

Trigger events using:
- advanced line crossing triggers and
- advanced presence triggers.

Advanced analytics

Trigger events using:
- advanced line crossing triggers,
- advanced presence triggers,
- speed detection, and
- size and direction filters.

Basic object classifier

Detect the presence of classified objects.

Top-down head tracker

Trigger events when heads cross a line, using a standard colour camera looking straight down.

Queue length

Trigger events when a queue exceeds a certain length.

Still Object Analytics

Trigger events when an object has been left for a period of time.

Mask detector

Trigger events when people are detected to not be wearing masks.

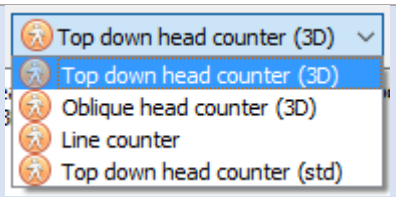
Basic people proximity

Trigger events when people are detected in closer proximity than a set distance.

Thermal face temperature

Trigger events when face temperatures are detected higher than a set value.

Note:
None of the algorithms in the *Counting type* analytics can trigger events.
To trigger events, refer to each algorithm type with the correct alternative.



Top-down head counter (3D)
- Count heads crossing a line, using a 3D camera looking straight down.

Note: To trigger events with head counts, use the Line Counter or Top-down head tracker algorithms.

For help with 3D camera analytics configurations, refer to the ***CathexisVision 3D Headcounter App-note (Discontinued)***.

Oblique head counter (3D)
- Count heads crossing a line using a 3D camera mounted at an angle.

Note: To trigger events with head counts, use the Line Counter or Top-down head tracker algorithms.

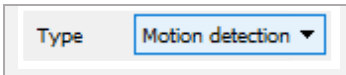
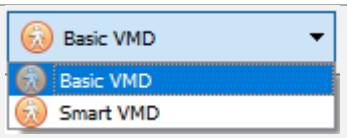
For help with 3D camera analytics configurations, consult the ***CathexisVision 3D Headcounter App-note (Discontinued)***.

Line counter
- Count objects crossing a line using a normal camera.

Note: To trigger events when objects cross a line, use the Basic, Intermediate, or Advanced algorithm options within the *Analytics type*.

Top-down head counter (standard)
- Count heads crossing a line using a standard colour camera looking straight down.

Note: To trigger events with top-down head counts on a standard camera, use the Top-down head tracker algorithm within the *Analytics type*.

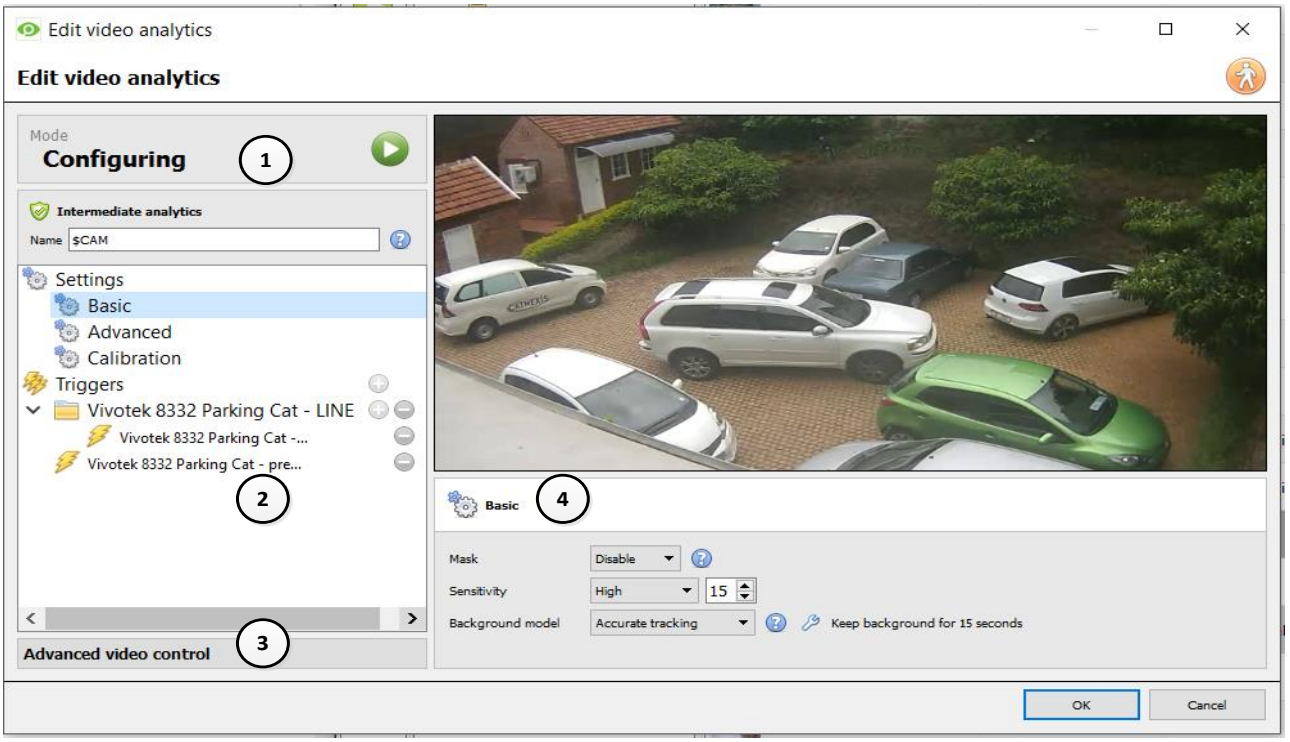
		**Basic VMD** - Standard motion detection algorithm. **Smart VMD** - Advanced motion detection algorithm designed for outdoor scenes. - Can filter out repetitive motion, such as trees or grass moving.

Once the analytics type is chosen, click **Next** to move onto configuring the analytics.

4.3.4 Analytics Configuration Interface Guide

There are two modes in the setup of Analytics: **Configuration** (4.3.4.1) and **Running** (4.3.4.2).

4.3.4.1 Configuration Interface

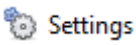


1	The header shows the current mode of the interface. There is an **arrow icon** in the top right of this panel. Click this to switch to the Running interface.

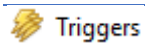
2 This area is the **configuration panel**.

The top of the panel shows the algorithm and its current licensing state (relative to the camera it has been assigned to).

It also lists the **name** of the algorithm. The "$CAM" at the beginning of the algorithm name refers to the name of the camera it has been assigned to. This is useful to export and import algorithm names that immediately assume the name of the camera that it has been imported into.



The **Settings** area lists the settings that exist for this algorithm.
The sets of algorithms will present different sets of settings options.
Analytics I, II, and III share the same settings options, but the rest all have their settings.

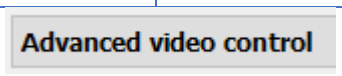


The **Triggers** area is where the user adds the analytics triggers for the sele algorithm.

To add a new trigger, click on the **plus** icon.

To remove a trigger, click on the **minus** icon.

(Triggers may be used to trigger events. Refer to the Events Setup section.)

3 

Advanced Video Controls are available in both the Configuring and Running interfaces. By default, it will be minimised.

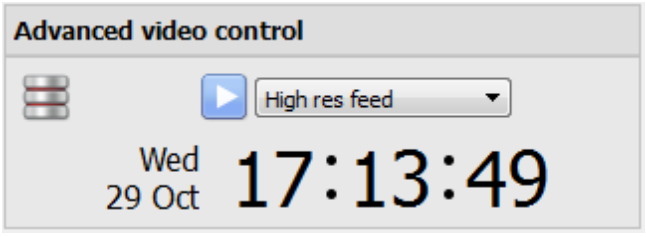
To expand this player, hover the mouse over the text of this section.

The text will turn blue. An arrow icon will appear to the right. Click on this icon to expand it.

There are two ways of viewing video with this tool: **Live Video** or **Recorded Video**.

Live Video

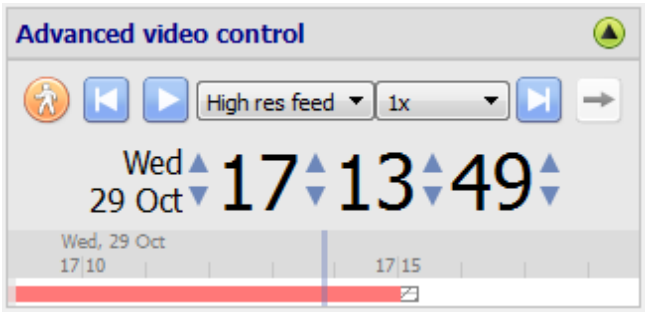
The default (in the above image) is live.



Click on the **arrow icon** to start streaming live video from the camera in the Camera panel.
There is the option to view the high-resolution feed and the low-resolution feed based on recorded footage. The actual analytics feed can be viewed, if it has been recorded, but this situation is rare.

Recorded Video

Click the **database** icon to navigate to the recorded video for this camera.



On the timestamp, use the wheel arrows to change the date of the footage being viewed.
OR: left-click and drag on the timeline at the bottom of the player.
Click on the **figure icon** to return to the live player.

This player has the ability to loop video selections. This is useful for testing algorithm settings. The user can check if a setting changes the efficacy of the algorithm. To do this, hold down **SHIFT** and left-click-drag out a selection on the timeline.

Once the portion of timeline is selected, click on the arrow.

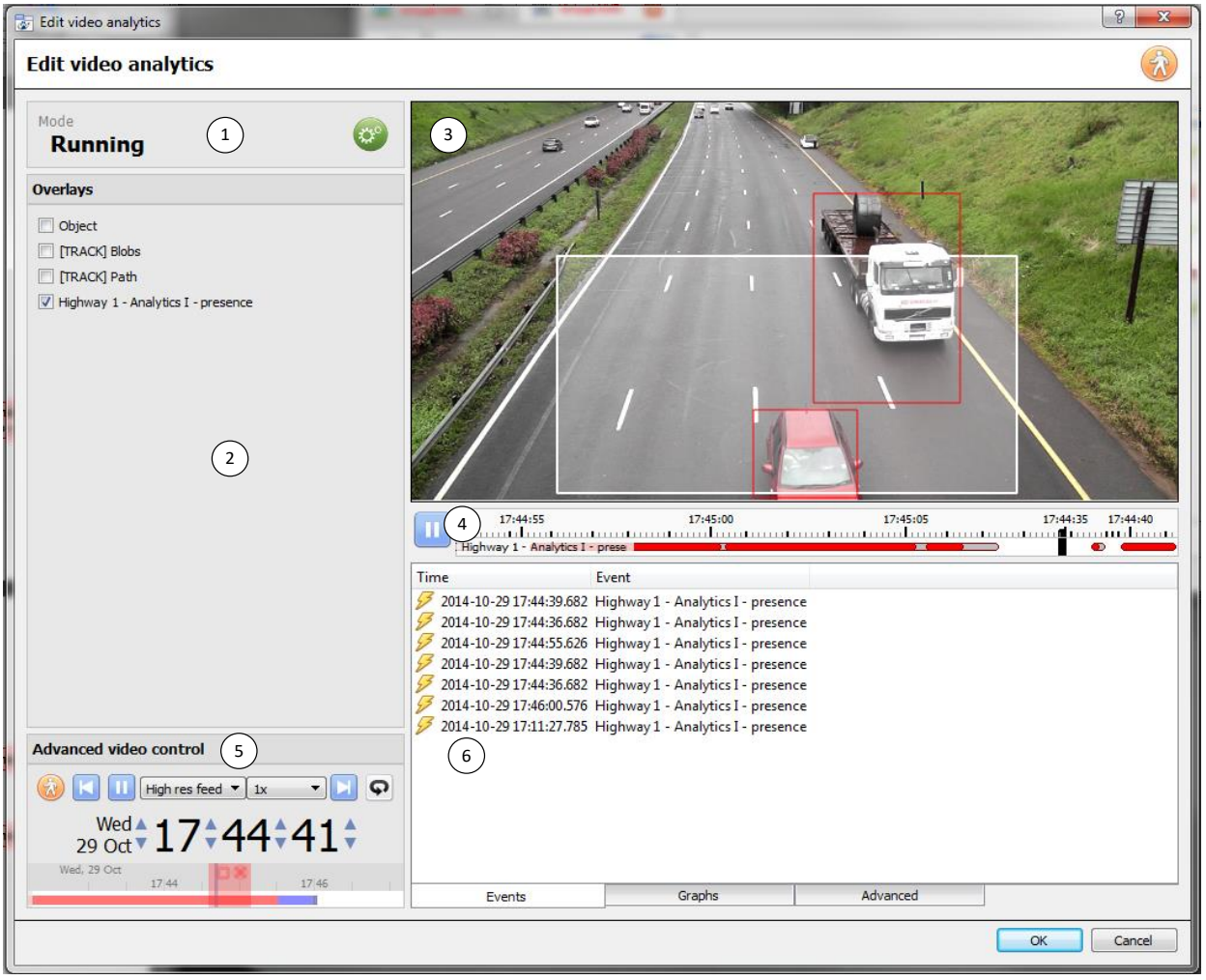
It will change from a straight arrow into a curved arrow icon.
Instead of playing continuously, it will now loop over the selected section of video.

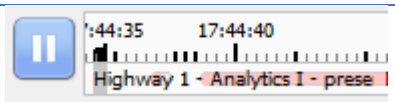
Note: This selection will transfer across from the Configuration to Running interface, and vice versa.

4 The **Context Area** displays the contextual information for what is selected in the Configuration Panel.

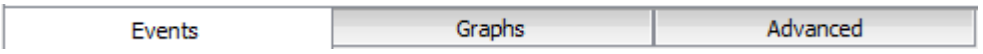
4.3.4.2 Running Interface

The **Running interface** allows users to test the settings that were defined in the **Configuration interface**. The Running interface uses live video, or a selection of recorded video, to show the configured algorithm in action.



1	The shows the current mode of the interface. The gear icon is in the top right of this panel. Click on this icon to switch back to the configuration interface.
2	In the **Overlays** panel, there are overlays that are contextually relevant to the configured algorithm. To select an overlay, check the box next to its name.
3	The footage panel displays the footage selected to view, and shows the overlays which were selected in the Overlays panel.
4	 The timeline displays recent video which has been processed by the algorithm. **Red** indicates triggers, **grey** indicates debounced triggers, and **white** means no trigger. When the video is paused, click on the timeline to allow recent frames and overlays to be viewed.

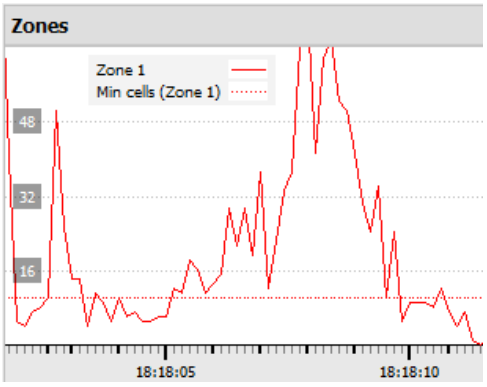
5	The **Advanced Video controls** are the same as those in the **Configuration** section.
6	The **Feedback Panel** shows live progression of the triggers as they appear. There are three ways to view the events as they come in: **Events**, **Graphs**, and **Advanced**. This is shown in the tabs at the bottom of the events panel:



EVENTS

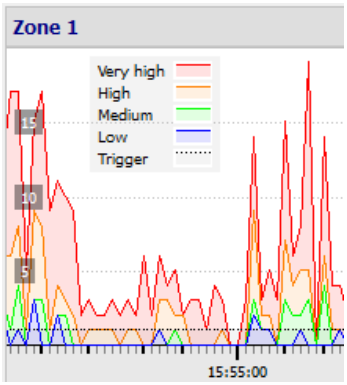
The **Events option** shows a list of triggers as they occur. For the purpose of this display, an entry is added when a new trigger appears on the recent timeline above (in other words, goes from white to red).

GRAPHS



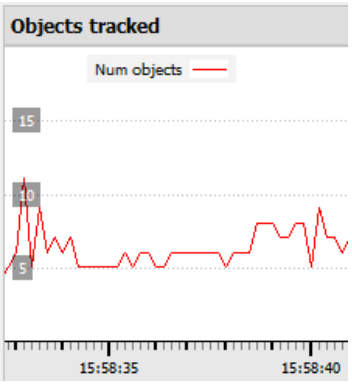
The **Graphs** option graphs the event activity occurring in the image.
For example, when using **Basic VMD**, the user can graph the zones in the algorithm. This is a visual representation of how far the triggers are above or below the minimum cells trigger line.

There will be different graphs for the Basic VMD, Smart VMD, Still Object, and Queue Length algorithms.

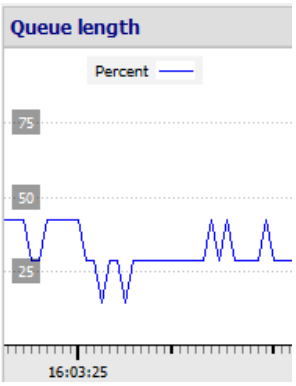


The **Smart VMD** shows the different trigger levels that occur based on specific profiles. This can be seen against the dotted line of the actual event trigger.

Use this to define how sensitive the algorithm should be, based on an objective visualisation of how it is reacting to the environment.



The **Still Object** graph simply graphs the number of objects currently being tracked.

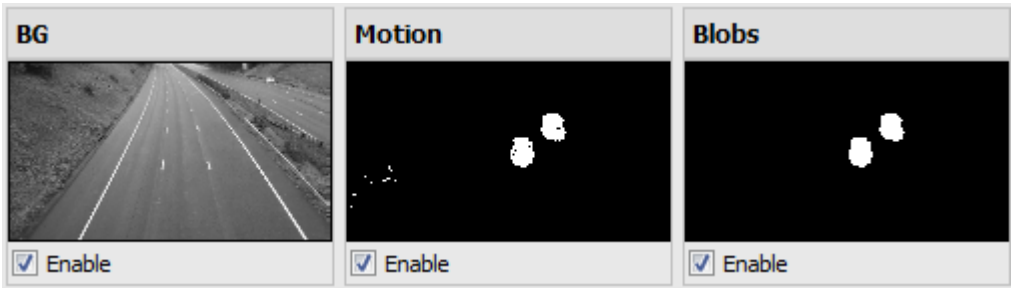


The **Queue length** graph in the **Basic Queue Length** algorithm displays the percentage of the queue's current length over time.

Use this to determine the percentage at which the trigger should be set off, or how sensitive the algorithm should be.

ADVANCED

Note: The images provided in the advanced tab will differ from algorithm to algorithm.



The Advanced tab shows the user what the algorithm is seeing.

BG	This is the **background image** that the algorithm is working with. The algorithm uses this to determine the changes that signify movement.
Motion	This shows the user all motion occurring in the video.
Blobs	This highlights all motion the algorithm has determined to be significant.

4.3.5 Basic VMD

Setup Tab / Configure Servers / Video Analytics / New / Motion Detection type / Basic VMD.

Basic VMD is designed to trigger when there is motion in an area. It works by breaking up the image into small cells. (The size of a single cell can be seen by drawing a tracking area with the brush set to the smallest size).

VMD algorithms observe changes in the light intensity of individual pixels and use this to set off triggers. Therefore, any changes in the image (such as clouds moving or a light flashing), can cause a false trigger.

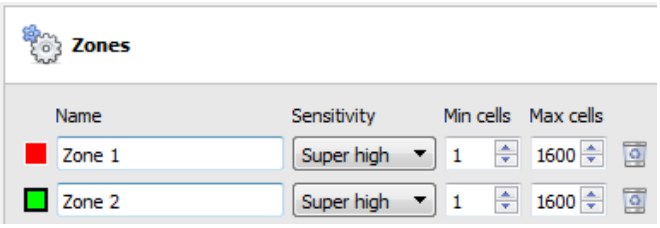
If there is motion in a certain percentage of the cell, it is considered to have triggered. The percentage is controlled by the **sensitivity**. To trigger, a high sensitivity will require a lower percentage. A lower sensitivity will require a higher percentage.

Motion is determined by comparing the incoming image with a background image, which is built up as the algorithm runs. Differences between the background and foreground images constitute *motion*.

There are several options available for modelling how the background image is created: **Historical, Travelling average, Accurate,** and **Long term**.

If any background model changes are made, users are advised to use the "Advanced" tab in the Feedback panel to check how the background tracks the foreground.

4.3.5.1 Zones



In the configuration panel of the "**Edit Video Analytics**" window, zones can be found under the Settings options.

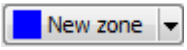
When the user selects **Zones**, the information (see image on the left) is displayed in the Context Area.

Create multiple zones, each with their own sensitivity, and minimum or maximum cell settings.

Min cells: this the smallest number of VMD cells needed to change for the algorithm to trigger.

An example of why zones are necessary is a boundary fence. The perspective of the receding fence means that a human 200m away from the camera will take up far less pixel space than a human 10m away. It is useful to set up different zones with increasing or decreasing sensitivity, and to set up both a minimum and maximum cell value for triggers.

4.3.5.1.1 Drawing Zones



To create a new zone, click on **New zone** at the bottom of the Context Area.

Select the new zone by clicking on the name of the zone.

To draw a new zone into the image, use the **Zone Drawing Tools** at the top of the Camera Panel.

Will paint the entire image with the zone.

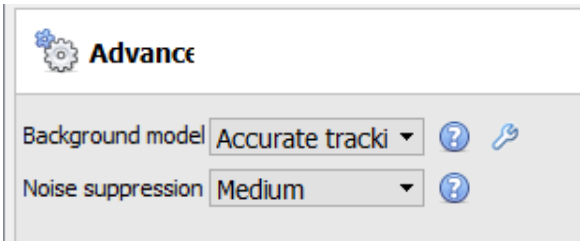
Will scrub the zone from the image.

Will drop-down a menu with a number of zone brush size options.

Paintings are done by holding left-click while dragging out the desired shape of the zone.

4.3.5.2 Advanced

4.3.5.2.1 Background Model



In the configuration panel of the "**Edit video analytics**" window, **Advanced** can be found under the Settings option.
Select **Advanced** to display the information shown in the image to the left, within the Context Area.

Accurate tracking (default): This operates similarly to the **traveling average** method. However, if there is a big change in the area, it retains the original background until such time as the foreground stabilises.

By clicking on the **spanner icon**, the settings of accurate tracking can be controlled. 'Background memory' sets how long it remembers the background. 'Background threshold' sets the region within which it smoothly adjusts the background.

Fixed Lighting: Builds up a background by looking at snapshots of the scene over an extended period. This can only be used if the lighting remains constant (for example, a controlled indoor environment). The frequency and number of snapshots used can be changed by clicking on the **spanner icon**.

Travelling average: This smoothly adjusts the background image towards the foreground.

Legacy: This method is used in **CathexisVision** 2014 and earlier.

Click on the **question mark** icon to display information about the selected options.

Click on the **spanner icon** to configure Advanced Background Model settings.

Note: Adaptive noise suppression is configured in the Advanced Background Model Settings window.

4.3.5.2.2 Noise Suppression

Noise suppression controls how sensitive a pixel is to being triggered. Increasing the noise suppression reduces sensitivity.

Adaptive Noise Suppression

The **Adaptive noise suppression** is designed to help eliminate repetitive motion such as waving trees or the waves on water.

To configure adaptive noise suppression, click the Advanced Background Model Settings icon.

Adaptive noise suppression splits the image into noise zones and evaluates each noise zone individually. The options are to split it into 1, 2x2, 3x3,4x4, and 5x5 noise zones.

Setting adaptive noise suppression to 5x5 zones will treat the noise more independently throughout the image.

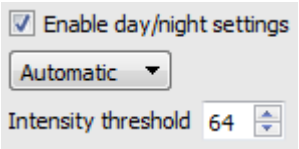
4.3.5.3 Day / Night

In the configuration panel of the "**Edit video analytics**" window, Day/Night can be found under the Settings option.

Lighting conditions change depending on the time of day. These changes can be disruptive to the motion detection algorithms. Therefore, **CathexisVision** provides alternate settings for day and night.

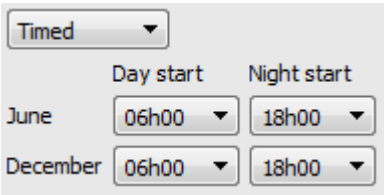
If day/night is enabled, then the settings can be set to different values for day and night.

4.3.5.3.1 Automatic



The intensity threshold is a number from 0 to 255, which represents the variable brightness level of what a pixel can achieve. This determines the brightness level at which the settings switch from day to night mode.

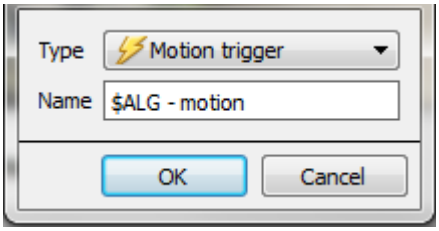
4.3.5.3.2 Timed



It is easiest to set up **Timed** Day/Night settings.

There are two periods of the year to set.

4.3.5.4 Triggers



Triggers can be found in the configuration panel of the "**Edit video analytics**" window. There is only one trigger option under Basic VMD: "Motion trigger".

Name: this is the name that was given to the algorithm. It is this name which will be databased when this algorithm triggers an event.

Once the trigger has been added, left-click on the trigger to see the Context Area options:

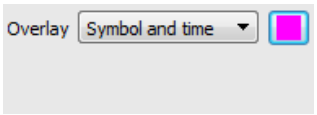
Use advanced settings If this option is not checked, there will be nothing here.

4.3.5.4.1 Zone Settings

Click on the hyperlinks to see the options for each setting.

Note: A trigger of 'no motion' can also take into account zone selection.

4.3.5.4.2 Trigger Overlay



The overlay will appear on the camera panel in the configuration interface as a small square, in the colour selected.

Reposition it by left-click dragging it.

The overlay appears when the algorithm is running. It will show the symbol for the event, and the amount of time in seconds that the event has been running.

4.3.6 Smart VMD

Setup Tab / Configure Servers / Video Analytics / New / Motion Detection type / Smart VMD.

4.3.6.1 Differences between Smart and Standard VMD

Smart VMD is designed to work in more dynamic environments than Standard VMD. It uses several methods to learn environmental noise patterns, and filters them to avoid false alarms.

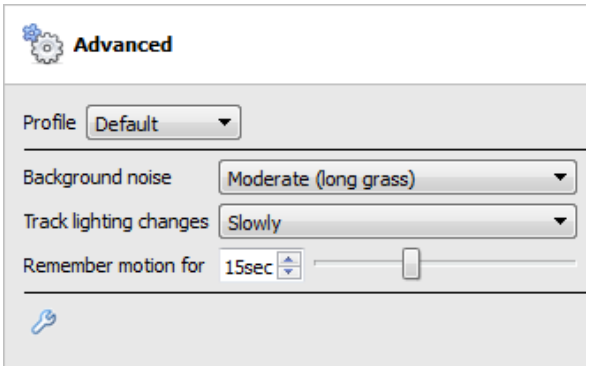
The major differences between **Smart VMD** and **Basic VMD** are:

1. The way in which the background is learned. **Smart VMD** uses its own unique background model.
2. The way the trigger threshold is calculated for a pixel in the image. **Basic VMD** uses a fixed threshold, which is modified by the noise suppression. Smart VMD uses a dynamic threshold which learns from repetitive motion in the environment to offer better noise rejection characteristics.

4.3.6.1 Zones

The zone settings for Smart VMD are identical to those described above, for Basic VMD.

4.3.6.2 Advanced Settings



Profile	Selecting a profile automatically configures the parameters, which can then be manually altered.
Tracking Light Changes	This configures how the background model responds to incremental changes in the lighting in the scene. The faster the setting, the less sensitive the algorithm will become.
Background noise	Noise refers to the fluctuations in intensity cause by things such as grass moving, or noise from the camera sensor. Background noise indicates how much background noise to expect in a scene. The less noise there is, the more responsive the algorithm can be to changes. Most scenes will do well with this set to low or moderate background noise.
Remember Motion	Once there has been motion in an area, it won't re-trigger until this period of time has passed. Making this period of time long will reduce the overall sensitivity of the algorithm. However, it also allows the algorithm to more easily mask out things like trees blowing in the wind.

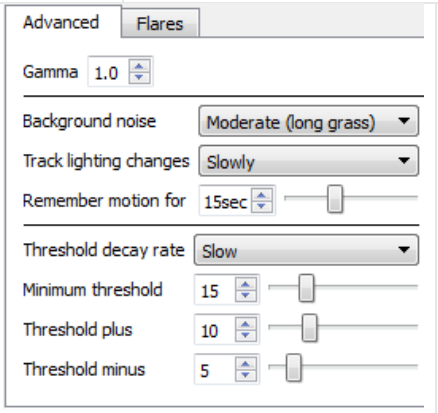
4.3.6.2.1 Profile Comparison

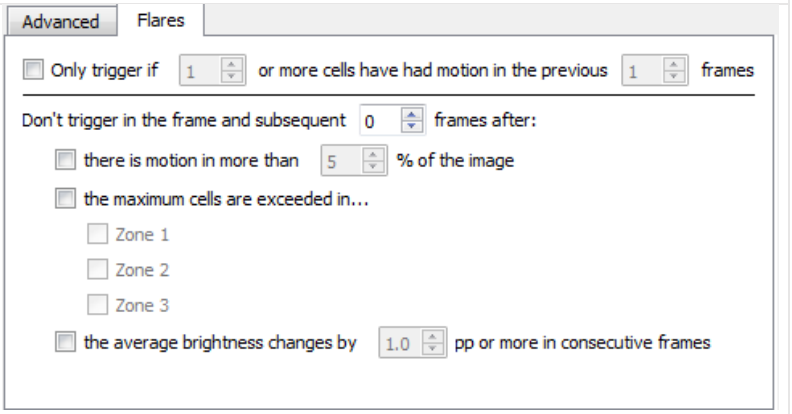
	Default	Short Grass	Long Grass
Flare	20% pp change of 2*	5% pp change of 2	5% pp change of 2
Noise Filter (First option in the Flares Tab)	NA	1 or more cells in previous 5 frames	1 or more cells in previous 5 frames
Background noise / Min Threshold	Moderate [long grass]	Low [Short Grass]	Moderate [Long Grass]
Track Light Changes	Slowly [1]	Fast [Clouds] [2]	Fast [Clouds] [3]
Motion Memory [Max Decay Countdown]	40 seconds/ 255 frames	3 seconds	5 seconds

*Note: "pp" stands for percentage points.

4.3.6.3 Advanced Settings Continued

Click on the **spanner icon** to open the advanced options of the Advanced Settings.





Gamma	**Gamma** is a brightening tool that works on a gradient. This means that it brightens the dark parts the most, and the lightest parts the least. This causes an image that is evenly brightened.
Threshold Decay Rate	**Threshold Decay Rate** sets the speed at which the threshold drops back to ambient levels, or, to the Minimum Threshold setting.
Minimum Threshold **Threshold Plus** **Threshold Minus**	These advanced settings are only for use in conjunction with **CathexisVision** support. For more information, contact support@cat.co.za.
Flares	**Only trigger if x or more...:** this is a noise filter. It requires a set amount of motion in a set number of previous frames [minimum] to trigger an alarm.

	Don't trigger…: this prevents the flare frame (and frames immediately after) from triggering an event. **Average Brightness:** in this setting, "pp" stands for percentage points. This setting measures the average change in brightness between two consecutive frames. The maximum setting is 10 percentage points. At this setting, if there is a total change in brightness of over 10%, then the change will be considered a flare. **Note**: the 10% maximum is a large average change for any image. 2% to 3% may be considered a substantial lighting change.

4.3.6.4 Day / Night

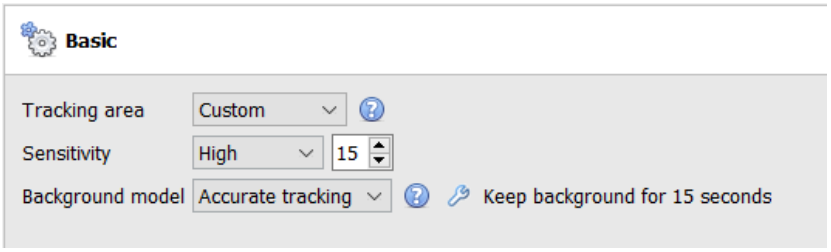
The Day/Night settings for Smart VMD are identical to the Day/Night settings for Basic VMD.

4.3.7 Basic, Intermediate, and Advanced Analytics

Setup Tab / Configure Servers / Video Analytics / New / Analytics type / Basic/Intermediate/Advanced.

The three Analytics suites share the same options for Basic, Advanced, and Calibration Settings.

4.3.7.1 Basic

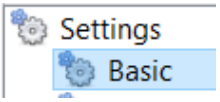


Tracking area	The **tracking area** defines the areas of the camera image to which the algorithm will be applied. To prevent false triggers, it could be useful to hide busy areas from the algorithm. "Entire scene" is selected by default. Ensure the tracking area surrounds the triggers. **Edit Tracking Area** **Move control point**: Click and drag. **Add new control point**: CTRL-click on a line, or double-click the white plus in the middle of a line. **Remove control point**: Double-click control point. **Move tracking area**: Left-click and drag (not on a control point).
Sensitivity	**Sensitivity** defines the algorithm's response to changes in the image. Select a pre-defined sensitivity level or set a custom level (maximum 50).
Background model	The **background model** is the pre-defined "normal" state of the image. For the algorithm to detect changes in the image, it needs to work with a pre-defined "normal". The **background model** defines how this is calculated. **Note**: Background model settings are only available within the *Analytics type,* in the Basic, Intermediate and Advanced algorithms.

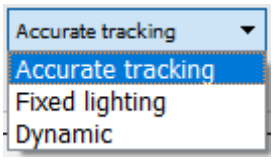
4.3.7.1.1 Background Model

If Basic, Intermediate, or Advanced algorithms within the *Analytics type* analytics are chosen, the user will be able to select a background model.

Under **Settings**, on the left of the window, select the **Basic** settings option.



Select the Background Model:

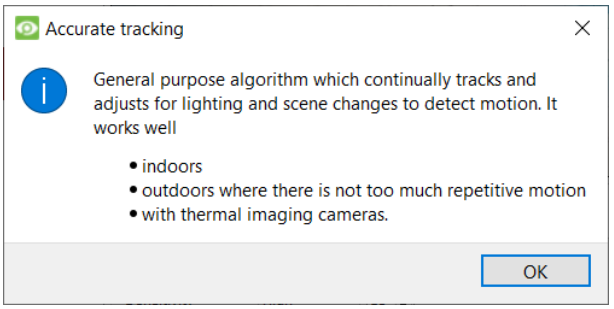


Click the question mark icon to display **information** about the selected background model. This information can help the user choose a suitable background model.

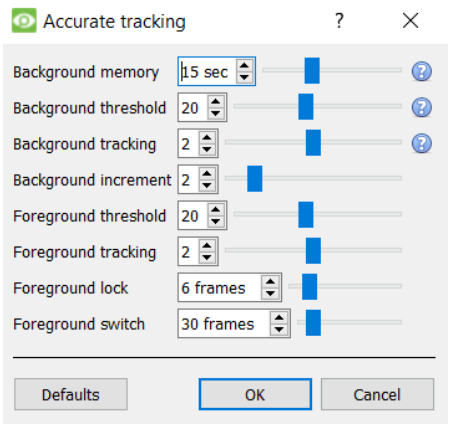
Click the spanner icon to further configure either the **Accurate Tracking** or **Fixed Lighting** background models.

Accurate Tracking Settings

Click the **question mark icon** to display information about accurate tracking.



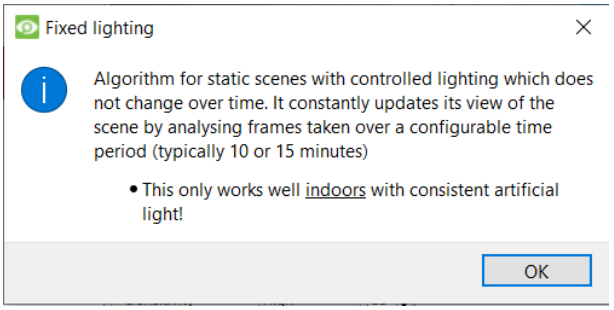
Click the **spanner icon** to configure accurate tracking.



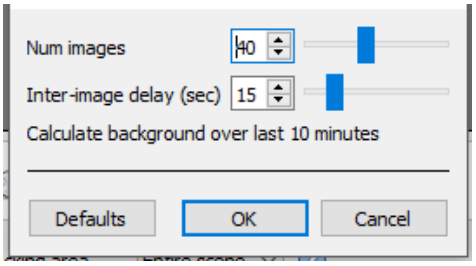
Note: These are advanced settings. It is recommended that users leave these as default.
Contact support@cat.co.za for additional help.

Fixed lighting settings

Click the **question mark icon** to display information about fixed lighting.



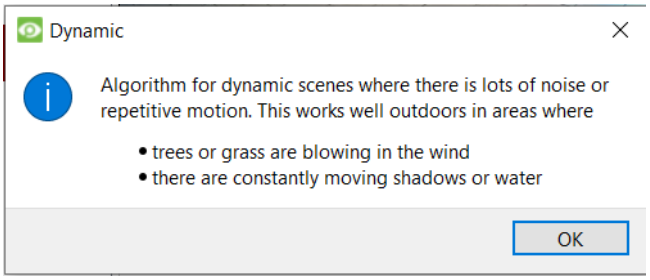
Click the **spanner icon** to configure fixed lighting.



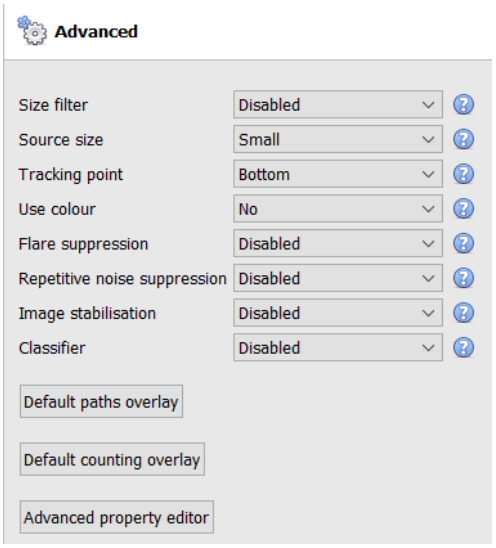
Note: These are advanced settings. It is recommended that users leave these as default.
Contact support@cat.co.za for additional help.

Dynamic

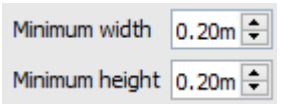
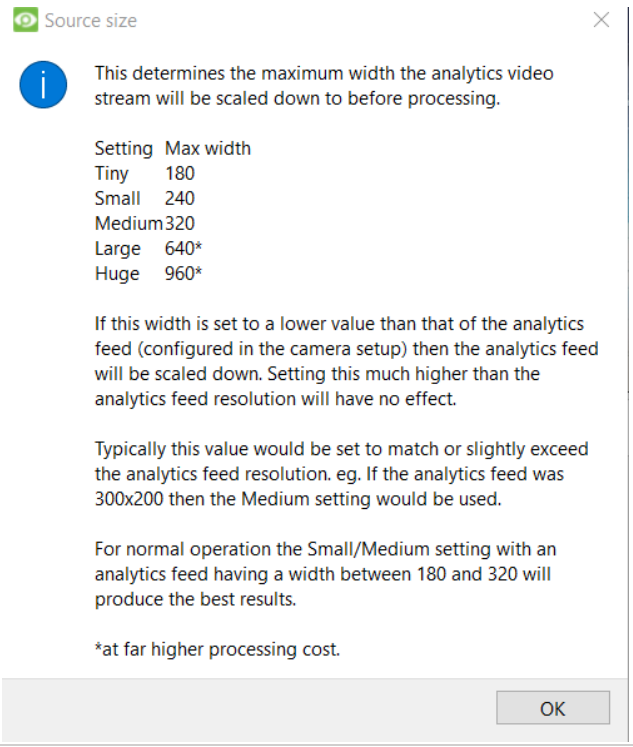
Click on the **question mark** icon to display information about the Dynamic background model.



4.3.7.2 Advanced



Note: Click the **question mark** next to any of the settings to display information about it.

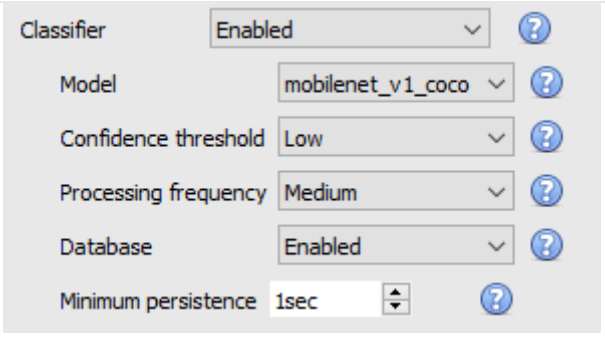
Size Filter	Filter out objects smaller than the minimum size.  When the size filter is enabled, the minimum width height options will be added to the interface. **Note:** in order for an object to be filtered out, the object width has to be less than the filter width, AND the object height has to be less than the filter height. **Note:** This is only implemented in **CathexisVision** 2016 and later. This option will not work when connecting to an older software version.
Source size	The source size determines how the video stream is scaled before processing. Small or Medium are sensible selections. Larger images substantially increase the processing load on the system, usually for marginal benefits.  (Increasing the source size increases the minimum object size the algorithm is capable of detecting. However, it also increases sensitivity to noise, which can lead to false positives.)

Tracking point	This sets where on the bounding box objects are tracked. By default, they are tracked at the bottom of the bounding box, as this corresponds to the feet of a person or the wheels of a car.
Use colour	This enables the algorithm to use colour for: • Tracking objects within the image. • Suppressing shadows.
Flare Suppression	Enabling flare suppression discards false motion as a result of intense changes in brightness levels. There are two settings: **Enabled** or **Disabled**. One discards frames when there are intense changes in brightness levels over large portions of the scene, and the other tries to silently filter out false motion caused by less intense brightness changes.
Image stabilisation	This option stabilises images in cases where camera shake is a problem. **Note**: This should not be enabled by default, because it places a heavy load on the computer's processor.
Classifier	Enable this option to classify tracked objects. Object classifications can also be databased. See section 4.3.7.2.1 for more information. **Note**: This places a heavy load on the processor.
Default paths overlay	Choose between a default object path overlay, and a user-defined one.
Default counting overlay	Choose between a default counting overlay, and a user-defined one.
Advanced Property Editor	This technical section is included in the software for support purposes only. Generally, **if the user does not understand the option presented, the user should not perform editing.**

4.3.7.2.1 Object Classifier

CathexisVision offers object classification and databasing. To enable object classification, select **Enable** from the drop-down menu. Then define the following parameters. **Note**:

- To review classifier information, recordings must be enabled on the camera to which video analytics are being applied.
- For classifications to be databased, an object classification database must be created and enabled.



- Select the **classification model:** the pre-trained deep neural network model used to classify objects.
- Select the **confidence threshold:** the confidence that an object has been classified correctly. Objects with a confidence level lower than the configured threshold will not be databased (but will still be classified and displayed in overlays, if enabled). **Note**: this threshold does not affect triggering.

- Select the **processing frequency:** the frequency at which the algorithm attempts to classify objects. **Note**: increasing processing frequency will increase the load on the processer.

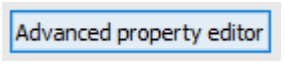
- Enable or disable the **databasing** of object classifications. **Note**: A specific database must be created for object classifications. See below.
- Set the **minimum persistence** (in seconds): This is the minimum time that an object must be on the scene in order to be considered for databasing.

Overlay Information

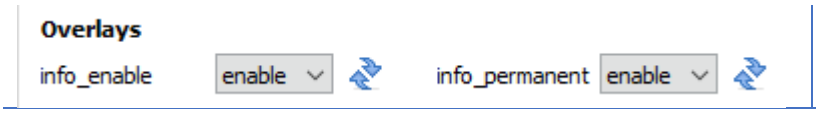
An object classifier overlay may be enabled, in addition to the object tracker overlays.

Enabling this information overlay will provide the following details related to the classified object:

- Object ID
- Object width and height
- Speed of the object
- Object classification with corresponding confidence rating from 0 to 1 (depending on what is enabled)
- Estimated object colour.



To enable an additional classifier information overlay, click the **Advanced property editor** button.



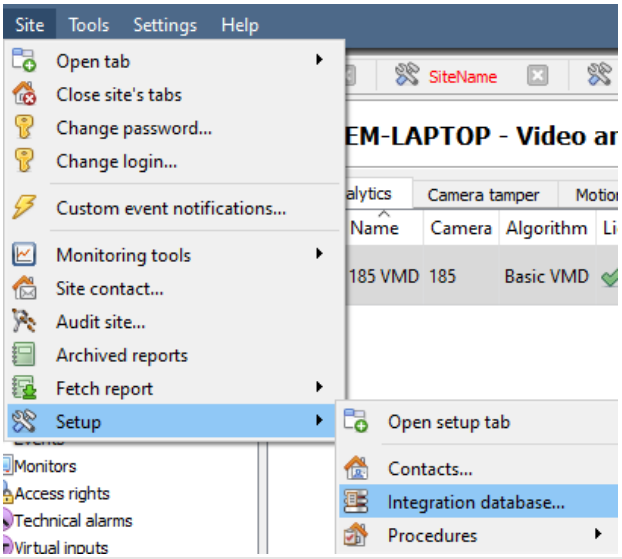
Enable both **info_enable** and **info_permanent**.

Click **OK** to close.

Create Object Classification Database

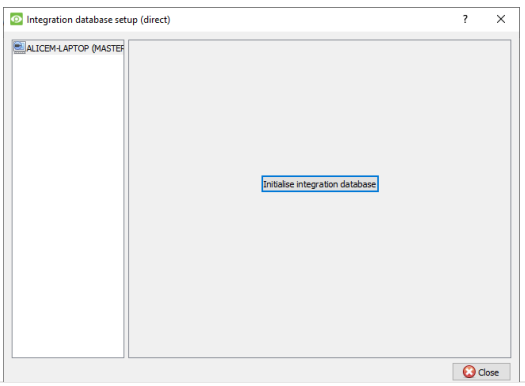
A database is necessary if object classifications need to be stored.

Note: If using the object classification database, make sure that **Database is enabled**.

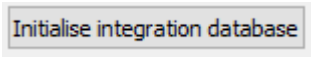


To create the database, follow:
Site Menu / Setup / Integration database.

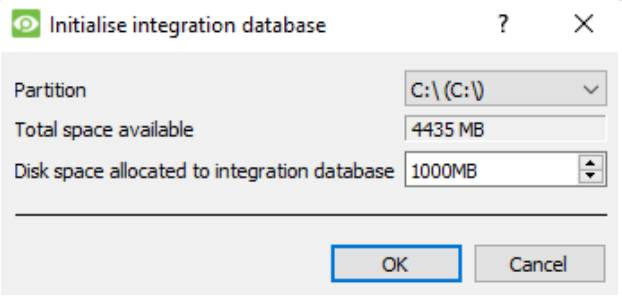
The following window will open:



If no integration databases have been created, the integration database will need to be initialised.



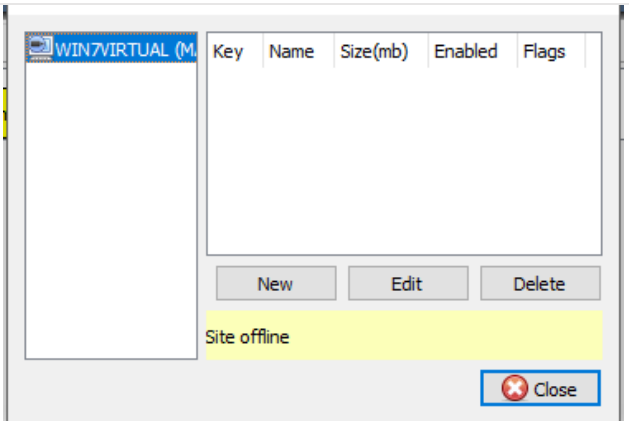
Click **Initialise integration database**.



In the initialisation window, select the partition and size of the integration database.

Click **OK** when done.

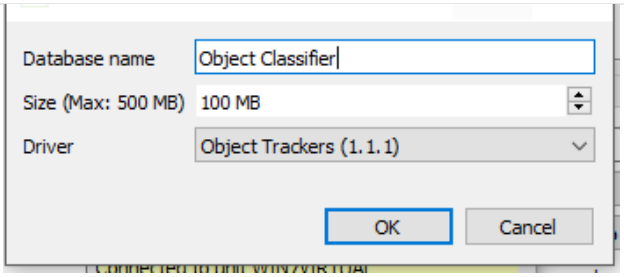
The database will initialise. The CathexisVision server will restart itself for the change to take effect.



The window will change immediately.

Now the object classifier database must be created.

Click **New**.

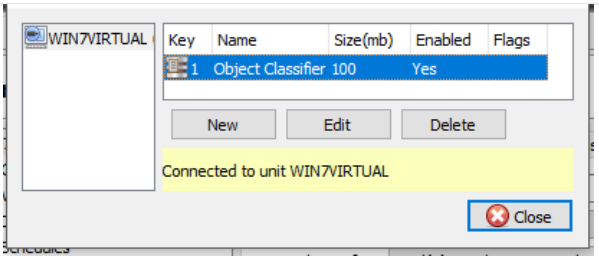


In the window that opens, set the following:

- Give the object classifier database a **descriptive name**.
- Set the **size of the database**.
- Select the **Object Trackers (1.1.1) driver** or **Object Trackers (2.2.2)** from the drop-down list.

Note: Object Trackers (2.2.2) includes a category column that the user can filter, corresponding to the trigger label rather than the classification label (for example: 'vehicle' rather than 'car','bus', etc).

- Click **OK** when done.



The database is now listed.

Click **Close**.

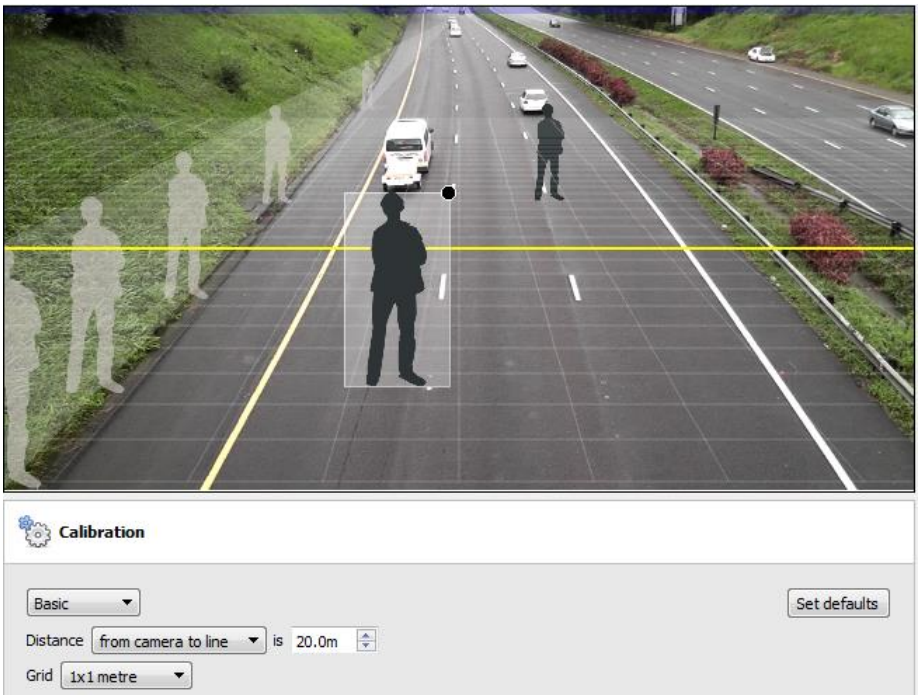
Once video analytics have been configured, the object classifier has been enabled, and the database has been set up, camera recordings with associated **object classification information may be reviewed** in the integration database. The object classification database operates like the general integration database.

To open the object classification database, follow one of the following paths:

1. **Site Menu / Open Tab / Databases**, or
2. **Right-click site tab / open tab / Databases**.

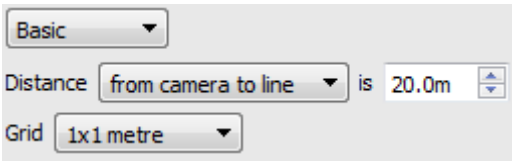
For operational information, refer to the ***CathexisVision Operator's Manual***.

4.3.7.3 Calibration



Calibration helps to determine the size of objects in the image. It uses several parameters.

4.3.7.3.1 Basic Calibration

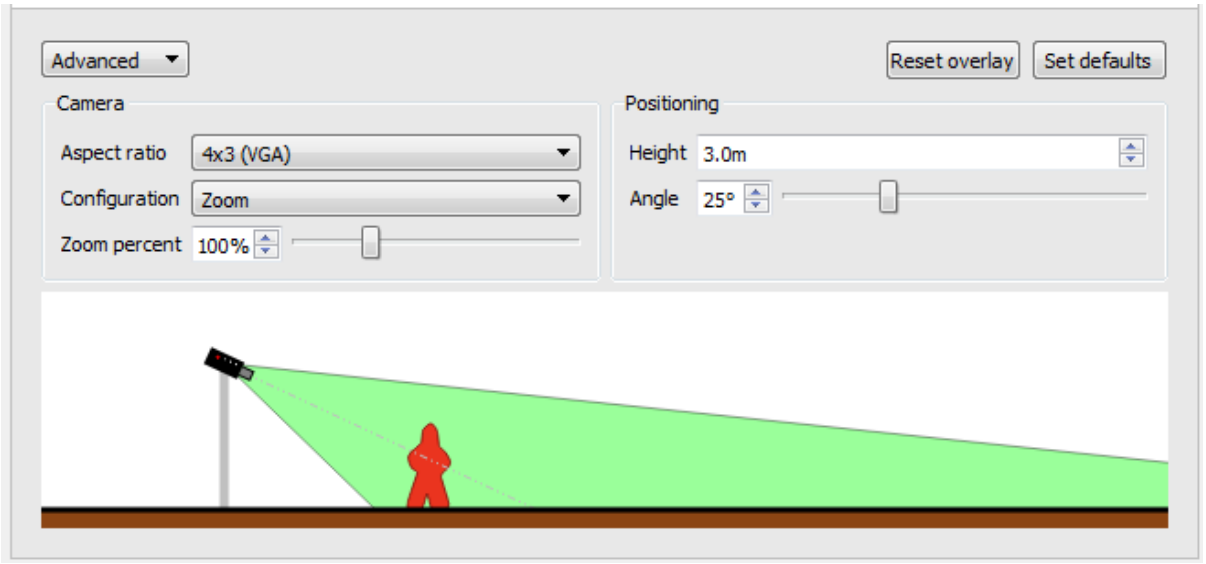


Distance	**From camera to line** Set the actual distance between the position of the camera and the yellow line in the image. The line can be moved (by clicking on it and dragging it). **Between lines** Estimate the distance between the two lines that appear in the camera image.
Grid	The grid is a visual overlay to help place the image of a shaded person on the screen.

To adjust the depth of field of the image: drag the human shapes to 2 different locations (near and far). Re-size them appropriately.

4.3.7.3.2 Advanced Calibration

Note: users are advised to only use advanced calibration settings when they require very accurate data about settings.



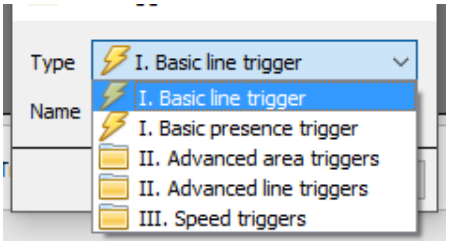
Aspect ratio	This refers to the shape of the camera image. The image below represents the aspect ratio being viewed. The camera itself also describes the aspect ratio: 16:9 3:2 4:3 5:4
Configuration	This is where the viewing angle is defined. It is defined by a **zoom percentage**, a literal **viewing angle**, or a combination of **sensor size** and **focal length.**
Height	The height of the camera off of the ground.
Angle	The angle of the camera to the ground, with 0 degrees as the level point.

4.3.7.4 Triggers

Basic, Intermediate, and Advanced Analytics are differentiated by their trigger options. Basic analytics have only basic triggers, and Advanced allows more advanced triggers.

Trigger options will depend on the analytics type selected.

To add a trigger, click the **plus** icon next to the Triggers section. Select the desired trigger from the drop-down menu.

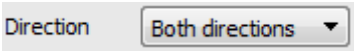


Some trigger types will need to be further defined by adding additional triggers. See below.

4.3.7.4.1 Basic Line Trigger

Available with Basic, Intermediate and Advanced Analytics.

This will trigger an event when an object crosses over the line in one or both directions. After adding the trigger, the Direction option will appear in the Context Area:



Click on the drop-down menu to change the direction options. The arrows, on the camera image, will change accordingly.

Placing the Trigger

To place the trigger, left-click on one of the control points at the end of the line. Lengthen, and pivot, the line against the control point at the other end of the line.

4.3.7.4.2 Basic Presence Trigger

Available with Basic, Intermediate, and Advanced Analytics.

The **basic presence** algorithm will trigger while an object is within the defined tracking area. The only changeable setting on this trigger is the tracking area.

Editing the tracking area

ACTION	METHOD
Move the corners of the tracking area	Click on the control points and drag them.
Add a new control point	Hold **CTRL** and click a point on one of the lines.
Remove a control point	Double-click on the control point.
Move the whole tracking area without changing its shape	Left-click and hold anywhere on the mask that is **not** a control point. Move the mouse.

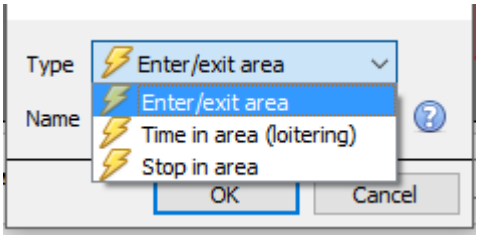
Note: the part of the image covered in the tracking area is the part where the algorithm is active.

4.3.7.4.3 Advanced Area Triggers

Available with Intermediate and Advanced Analytics.

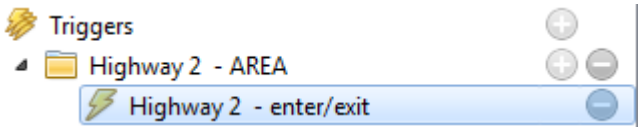
Adding an "Advanced Area Triggers" group lets the user define an area which can be used by one or more triggers. This is useful because the area is only drawn once. Once this trigger is added, it needs to be defined by adding further triggers.

To add triggers to the Advanced Area Trigger, click the **plus** icon next to the Advanced Area trigger.

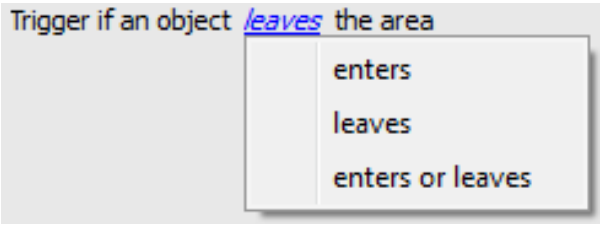


Select the desired trigger type from the drop-down menu.

Enter / Exit Trigger



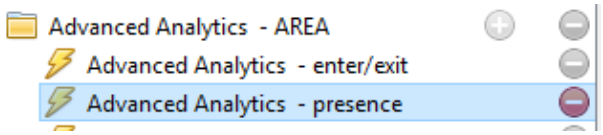
This will trigger when an object enters or leaves the area (or a combination of both). This is defined beneath the tracking area.



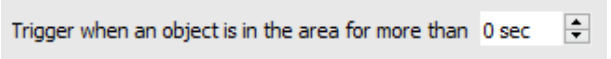
Choose between triggering the event when an object enters the area, exits the area, or both. The trigger occurs at the point when the object crosses the boundary.

Note: the algorithm is active in the part of the image covered in the tracking area. To edit tracking area, see section above.

Time in Area (Loitering)

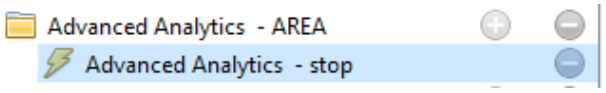


This triggers when an object has remained within the area for a prescribed period of time.

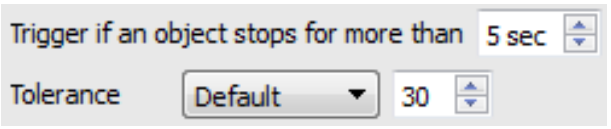


In the area beneath the mask, define the period of time an object should remain in the area.

Stop in Area



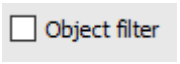
This triggers when an object has remained within the area for a prescribed period of time.



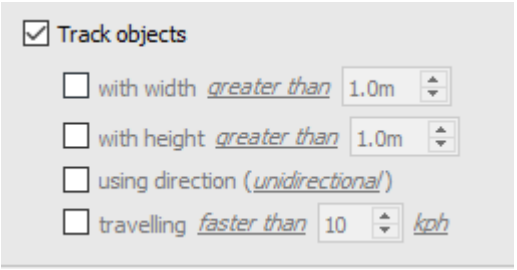
Set how long an object must be stationary for, before it triggers. **Tolerance** is measured in pixels. Tolerance refers to how far the object is allowed to move, while still considered to be stopped.

Object Filter

The Advanced Area Trigger allows for **object filtering** on triggers which are added to the area. Objects that are configured to trigger can be filtered, so that only those objects of certain heights, widths, directions or speeds will set off a trigger.



Select the triggers in the settings panel. Then tick **Object filter** in the Context Area.



Once Object filter is ticked, the Track objects options will appear.

Select the filters to apply to trigger objects. Specify each according to requirements.

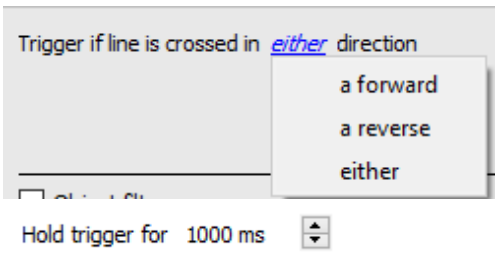
4.3.7.4.4 Advanced Line Triggers

Available with Intermediate and Advanced Analytics.

Triggers placed in the **Advanced Line Triggers** group can share the same line.

- To add a control point to the Advanced Line Trigger: hold down CTRL and click anywhere on the line.
- To move a control point: left-click on the point, and hold while moving the mouse.

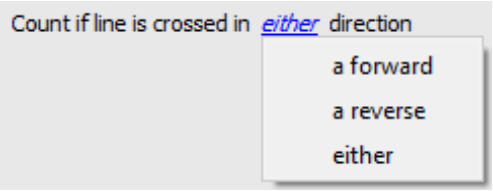
Line Trigger



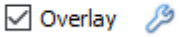
Define which direction will trigger the line.

Define how long to hold the trigger (in ms).

Line Counter

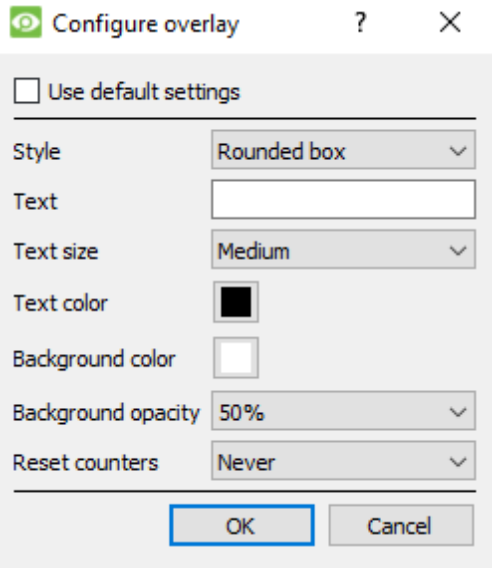


Define which direction will trigger the count.



Check to enable counting overlay. Click the **spanner icon** to configure overlays.

Configure Counting Overlays



Check box to use default overlay settings. Uncheck to edit.

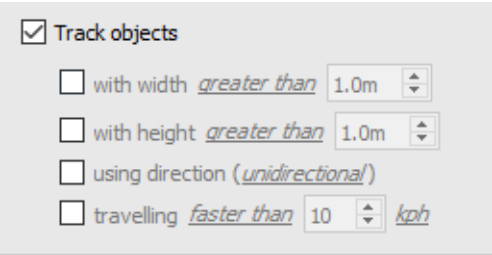
Define the Style of the counting overlay.
Enter Text which will precede the count in the overlay.
Define the Text Size.
Define the Text Colour.
Define the background colour of the counting overlay.
Define the Background opacity of the counting overlay (0 is transparent and 100 is completely opaque).
Define when to reset the count (never / hourly / daily).

Object Filter

As with Advanced Area Triggers, the Advanced Line Trigger allows for object filtering on both line counters and triggers.

Objects which will trigger when they cross the line can be filtered to only trigger on objects of certain heights / widths / directions / speed.

Select the line/counter triggers in the settings panel.
Then tick **Object filter** in the Context Area.



Once Object filter is ticked, the Track objects options will appear.

Select the filters to apply to trigger objects. Specify each according to requirements.

4.3.7.4.5 Speed Triggers

Available with Advanced Analytics.

Click the **plus icon** to add a new trigger.

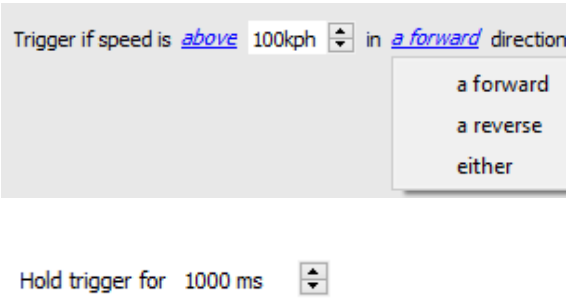
Select the Speed trigger from the drop-down menu.

Configure the general speed trigger settings. Then add a further speed range trigger to the speed trigger:

General Speed Trigger Settings

This distance is the distance between the two lines seen on the camera image.
Note: for this setting to work well, the distance between the lines needs to be accurate.

Speed Range Trigger Settings



Configure the trigger so that it will trigger if the speed is within a certain range, in a particular direction.

Click the blue hyperlinks to change the parameters.
Define how long to hold the trigger (in ms).

4.3.8 Basic Object Classifier

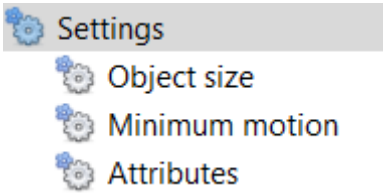
Available with Advanced Analytics (License III)

Setup Tab / Configure Servers / Video Analytics / New / Analytics type / Basic object classifier

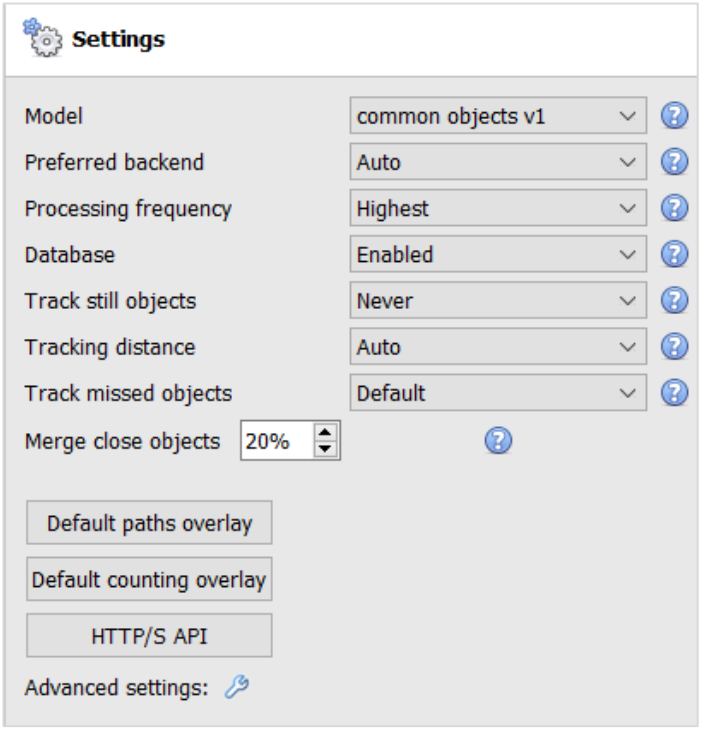
This algorithm detects the presence of classified objects. To use this option, the user will need a high-resolution feed, because this algorithm uses an AI model to detect and classify objects. The algorithm will downscale the resolution internally as necessary, but it needs a high resolution to classify accurately.

By default, it is not possible to add an analytics feed with a width above 720 pixels. **Note**: even if the system.ini is edited to circumvent this, internally, the analytics feed will be scaled to not exceed a width of 960 pixels.

4.3.8.1 Settings



To configure the **Basic object classifier** settings, click on **Settings** in the left side of the New video analytics window. The following options will appear on the right.

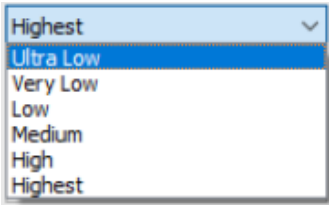


Model: the pre-trained deep neural network model used to classify objects. (**Note**: refer to the table below for more information on the models/preferred backends of object classification algorithms.)*

Preferred backend: select the preferred backend used to by the model to classify the objects. The selected model determines the backend options that are displayed. Depending on the model used, the preferred backend could be CPU, GPU_Intel, GPU_CUDA_FP32 or Auto.

Note: when the user selects the preferred backend on which to run the model, the system will attempt to use it. If GPU_Intel is selected, and the unit does not have an onboard Intel GPU, the system will attempt to run the model on the CPU. If GPU_CUDA_FP32 is selected and there is no supported Nvidia card, the algorithm will not run the classifier.

Processing frequency: select the processing frequency from the options of Ultra Low, Very Low, Low, Medium, High, or Highest.



Increasing the processing frequency will increase the number of attempts to classify objects, and thus increase the load on the processor.

Database: when enabled, classified objects are databased.

Track still objects: Usually, objects are discarded as they become part of the background. For occupancy triggers, it may be useful to keep track of still objects.

Tracking distance: Selecting Auto means that tracking distance is determined internally. Choosing Custom allows the user to set a maximum tracking distance.

Track missed objects: Attempt to locate and track objects missed by classifier. Hold recovered objects for a given time.

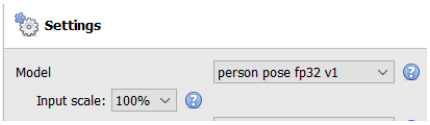
Merge close objects: The lower the value, the closer the object bounding boxes have to be in order to get merged as the same bounding box.

Custom minimum motion: Only run the object classifier when custom minimum motion is exceeded.

Default paths overlay: when the user clicks on this, the **Configure overlay** window will appear.

Default counting overlay: when the user clicks on this, the **Configure overlay** window will appear.

HTTP/S API: clicking on this will give the user the option to enable the sending of thumbnails or occupancy data.



The person pose models have the option to set the Input scale. Increasing the input scale allows the detection of smaller objects and increased accuracy, but at a higher computational cost.

4.3.8.1.1 Basic Object Classifier models

Name	Description	NVR hardware requirements
common objects v1	Low accuracy detection model that classifies 182 common objects at relatively low computational cost.	Only runs on Intel hardware: mAP@[0.5:0.05:0.95] = 23.3% on coco dataset at 2.494 GFLOPs.
common objects short v1	Low accuracy detection model that classifies 20 common objects at relatively low computational cost.	Runs on Intel hardware and NVIDIA GPU: mAP@[0.5:0.05:0.95] = 21.98% on coco dataset at 1.290 GFLOPs.
person vehicle bike v1	Accurate detection model that classifies person, vehicle, bike at medium high computational cost.	Only runs on Intel hardware: mAP = 64.48% on custom dataset at 3.964 GFLOPs.
common objects short v2	Accurate detection model that classifies 20 common objects at a very high computational cost.	Only runs on the NVIDIA GPU: mAP@0.5 = 82.2% on VOC2012 dataset at 180.6 GFLOPs.

faces v1	Accurate detection model that classifies faces at low computational cost.	Only runs on Intel hardware: mAP(head height>32px) = 84.4% on Wider Face dataset at 1.053 GFLOPs. Min head size: 90x90 pixels on 1080p.
faces v2	Accurate detection model that classifies faces at low computational cost.	Only runs on NVIDIA GPU. Comparable to faces_v1.
person pose v1	Accurate human pose detection model at medium computational cost.	Only runs on Intel hardware: mAP = 42.8% on COCO validation subset at 15.4 GFLOPs.
person retail v1	Relatively accurate detection model that classifies people in retail environment at medium computational cost.	Only runs on Intel hardware: mAP = 88.62% on custom dataset at 2.3 GFLOPs. Min person height: 100 pixels on 1080p. Pose coverage: Standing upright, parallel to image plane. Occlusion coverage: <50%.
person pose fp32 v1	Accurate human pose detection model at medium computational cost.	Runs on Intel hardware and Nvidia GPU: mAP-42.8% on COCO validation subset at 15.4 GFLOPs.
common objects v3	Accurate detection model that classifies 182 common objects at medium computational cost.	Runs on Intel hardware and Nvidia GPU: mAP@[0.5] = 46.3% on COCO dataset at 6.9 GLOPs.

Terms

mAP: mean average precision – metric used to measure the performance of models doing object detection tasks.

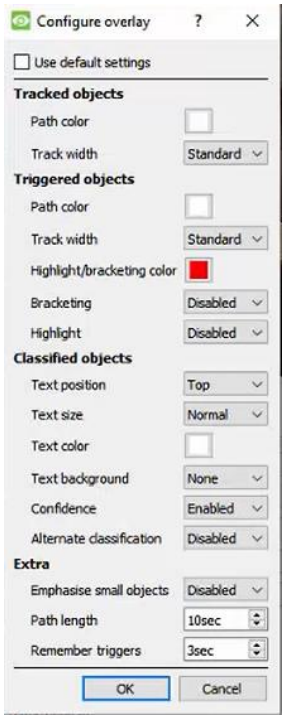
FLOPs: floating point operations – measures how many operations are needed to run the network model (rough idea of speed/cost).

*Objects

Model	Objects
common objects v1	airplane, apple, backpack, banner, baseball bat, baseball glove, bear, bed, bench, bicycle, bird, blanket, blender, boat, book, bottle, bowl, branch, bridge, broccoli, building-other, bus, bush, cabinet, cage, cake, car, cardboard, carpet, carrot, cat, ceiling-other, ceiling-tile, cell phone, chair, clock, cloth, clothes, clouds, cow, couch, counter, cup, cupboard, curtain, desk, desk-stuff, dining table, dirt, dog, donut, door, door-stuff, elephant, eye glasses, fence, floor-marble, floor-other, floor-stone, floor-tile, floor-wood, flower, fog, food-other, fork, frisbee, fruit, furniture-other, giraffe, grass, gravel, ground-other, hair brush, hair drier, handbag, hardware/appliance, hat, hill, horse, hot dog, house, keyboard, kite, knife, laptop, leaves, light, light reflecting, mat, metal, mirror, mirror-stuff, monitor/tv, moss, motorcycle, mountain, mouse, mud, napkin, net, orange, oven, paper, parking meter, pavement, person, pillow, pizza, plant-other, plastic, plate, platform, playingfield, potted plant, railing, railroad, refrigerator, remote, river, road, rock, roof, rug, salad, sand, sandwich, scissors, sea, sheep, shelf, shoe, sink, skateboard, skis, sky-other, skyscraper, snow, snowboard, solid-other, spoon, sports ball, stairs, stone, stop sign, straw, street sign, structural-other,

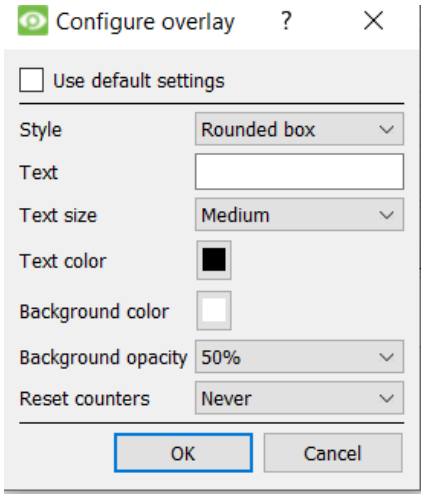
	suitcase, surfboard, table, teddy bear, tennis racket, tent, textile-other, tie, toaster, toilet, toothbrush, towel, train, tree, truck, umbrella, vase, vegetable, vegetation, wall-brick, wall-concrete, wall-other, wall-panel, wall-stone, wall-tile, wall-wood, water-other, waterdrops, window, window-blind, window-other, wine glasses, wood, zebra
	Trigger group: Person – person
	Trigger group: Vehicle - bicycle, car, motorcycle, airplane, bus, train, truck, boat
	Trigger group: Animal - bird, cat, dog, horse, sheep, cow, elephant, bear, zebra, giraffe
common objects short v1	aeroplane, bicycle, bird, boat, bottle, bus, car, cat, chair, cow, dog, dining table, horse, motorbike, person, pottedplant, sheep, sofa, train, tvmonitor
	Trigger group: Person - person
	Trigger group: Vehicle - airplane, boat, bicycle, bus, car, motorcycle, train, truck
	Trigger group: Animal - bird, cat, cow, dog, horse, sheep
common objects short v2	aeroplane, bicycle, bird, boat, bottle, bus, car, cat, chair, cow, dog, dining table, horse, motorbike, person, pottedplant, sheep, sofa, train, tvmonitor
	Trigger group: Person - person
	Trigger group: Vehicle - aeroplane, bicycle, boat, bus, car, motorbike, train
	Trigger group: Animal - bird, cat, cow, dog, horse, sheep
common objects v3	airplane, apple, backpack, banner, baseball bat, baseball glove, bear, bed, bench, bicycle, bird, blanket, blender, boat, book, bottle, bowl, branch, bridge, broccoli, building-other, bus, bush, cabinet, cage, cake, car, cardboard, carpet, carrot, cat, ceiling-other, ceiling-tile, cell phone, chair, clock, cloth, clothes, clouds, cow, couch, counter, cup, cupboard, curtain, desk, desk-stuff, dining table, dirt, dog, donut, door, door-stuff, elephant, eye glasses, fence, floor-marble, floor-other, floor-stone, floor-tile, floor-wood, flower, fog, food-other, fork, frisbee, fruit, furniture-other, giraffe, grass, gravel, ground-other, hair brush, hair drier, handbag, hardware/appliance, hat, hill, horse, hot dog, house, keyboard, kite, knife, laptop, leaves, light, light reflecting, mat, metal, mirror, mirror-stuff, monitor/tv, moss, motorcycle, mountain, mouse, mud, napkin, net, orange, oven, paper, parking meter, pavement, person, pillow, pizza, plant-other, plastic, plate, platform, playingfield, potted plant, railing, railroad, refrigerator, remote, river, road, rock, roof, rug, salad, sand, sandwich, scissors, sea, sheep, shelf, shoe, sink, skateboard, skis, sky-other, skyscraper, snow, snowboard, solid-other, spoon, sports ball, stairs, stone, stop sign, straw, street sign, structural-other, suitcase, surfboard, table, teddy bear, tennis racket, tent, textile-other, tie, toaster, toilet, toothbrush, towel, train, tree, truck, umbrella, vase, vegetable, vegetation, wall-brick, wall-concrete, wall-other, wall-panel, wall-stone, wall-tile, wall-wood, water-other, waterdrops, window, window-blind, window-other, wine glasses, wood, zebra
	Trigger group: Person - person
	Trigger group: Vehicle - airplane, boat, bicycle, bus, car, motorcycle, train, truck
	Trigger group: Animal - bird, cat, dog, horse, sheep, cow, elephant, bear, zebra, giraffe

4.3.8.1.2 Default paths overlay



Edit the overlay options as needed.

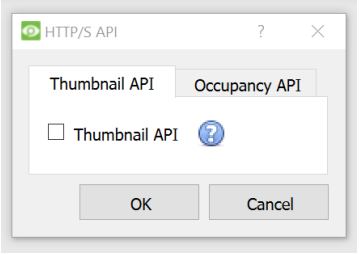
4.3.8.1.3 Default counting overlay



Either select **Use default settings,** or edit the overlay options as needed.

4.3.8.1.4 HTTP/S API

Click on the **HTTP/S API** button.



In the window that opens, click on the relevant tab.

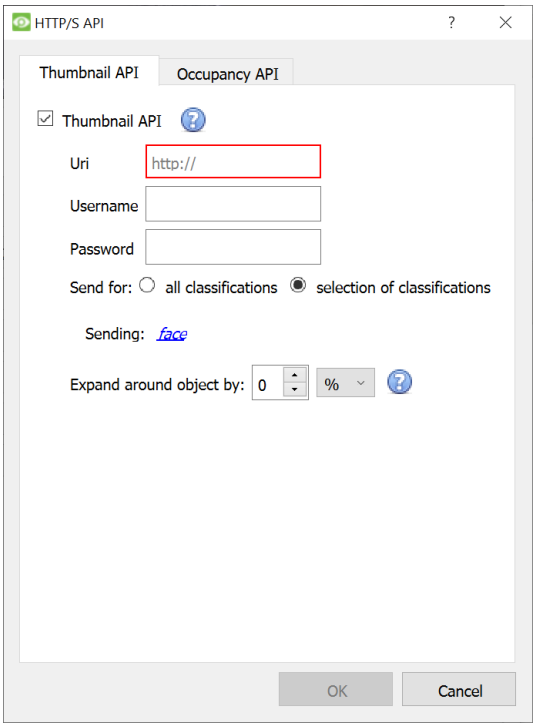
In the **Thumbnail API tab**, check the box to enable the sending of Thumbnail data to HTTP/S server.

In the **Occupancy API tab**, check the box to enable the sending of occupancy data to HTTP/S server.

The configuration options will appear below.

Thumbnail API

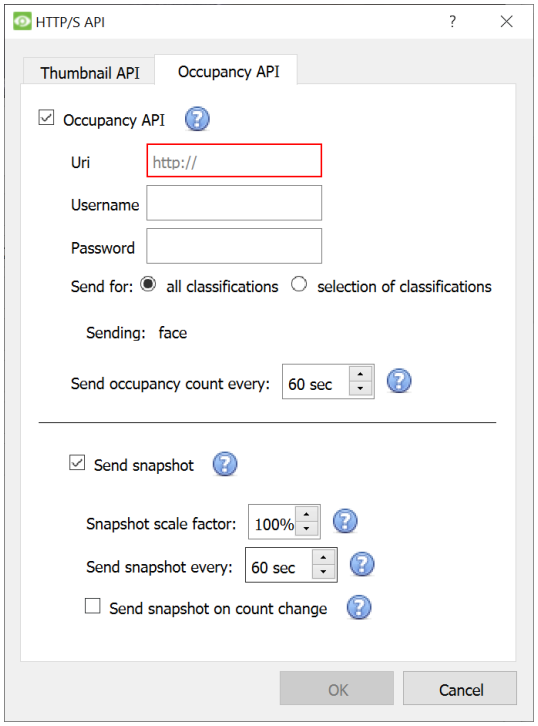
Note: The purpose of the Thumbnails API is to send thumbnails of detected objects to a remote HTTP receiver as configured. For more information, refer to the ***CathexisVision API Implementation Guide***, which is available on request and released under an NDA.



Enter the information to configure this setting.

Occupancy API

Note: The purpose of the Occupancy API is to send occupancy data to a remote HTTP receiver as configured. For more information, refer to the ***CathexisVision API Implementation Guide***, which is available on request and released under an NDA.



Enter the information to configure this setting.

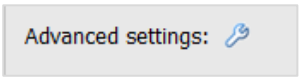
Choose the **rate** at which occupancy count should be sent to the HTTP/S server.

Select **send snapshot** to include a snapshot with occupancy count.

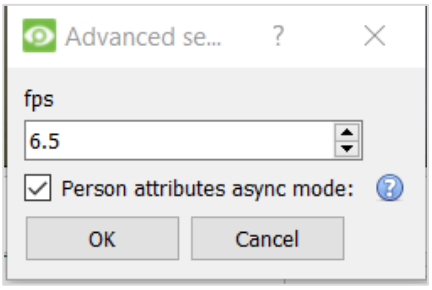
Choose the **rate** at which a snapshot should be sent to the HTTP/S server.

Select whether to **send snapshot on count change**. (**Note**: enabling this feature could take up a lot of resources if the occupancy count changes often.)

4.3.8.1.5 Advanced Settings



Click on the spanner icon in the Settings panel to configure **Advanced settings**.



Choose the **frames per second**. **Note**: this should only be configured by operators with knowledge of the software's advanced settings.

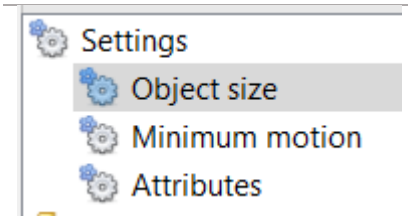
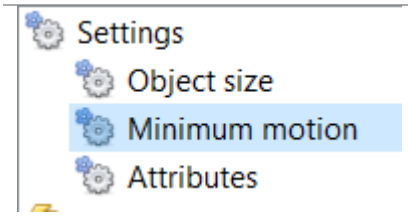
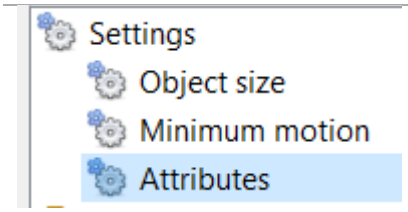
If the algorithm requests a lower frame rate, potentially more algorithms can be added to the server before it starts dropping frames. If multiple algorithms are running on the same camera, they should all run at the same frame rate.

For help with this advanced setting, contact Cathexis support: support@cat.co.za

Select to enable or disable **async mode**. If async mode is disabled, person attributes detection will block the frame until results have returned.

4.3.8.2 Other settings

Click on the icons below the main Settings icon to configure other settings.

	**Object size**: Select to exclude objects bigger than the maximum or smaller than the minimum size. The min/max object overlays may be dragged over an object in the scene for convenience.
	**Set minimum motion**: Only run the object classifier when custom minimum motion is exceeded. The overlays may be dragged in the scene for convenience. **Set motion area**: Only run the object classifier when custom minimum motion is exceeded in motion area of interest.
	**Attributes**: Enable to detect person attributes. Select the person attributes model, and preferred backend. **Note**: Attributes are currently informational, and will only be displayed as an overlay. The attributes that can be detected are: male, female, bag, hat, long sleeves, short sleeves, long trousers, short trousers, dress, long hair, short hair, coat jacket.

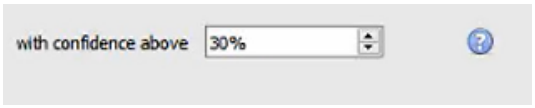
4.3.8.3 Triggers

Click the **plus icon** to add a new trigger. Select the **basic presence trigger** from the drop-down menu.

The trigger will be displayed in the panel on the right.

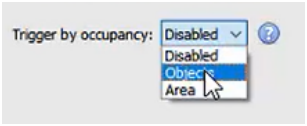
In the panel on the right:

Select or disable the type or types of classified object to be detected: **person**, **vehicle**, or **animal**. (**Note**: these types depend on the selected model.)



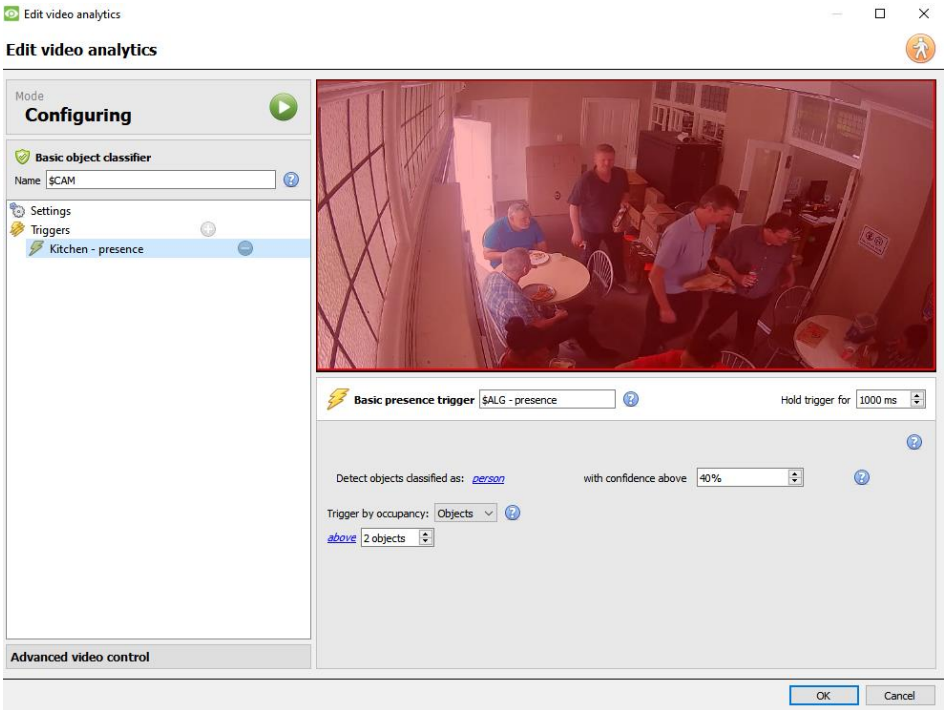
Select the **confidence** of classification (as a percentage) from which the algorithm will trigger. For example, if the algorithm is 30% confident that the detected object is the selected type of classified object, it will trigger.

4.3.8.3.1 Occupancy triggers



In the panel on the right, select the occupancy trigger (either by **objects** or **area)**.

Objects



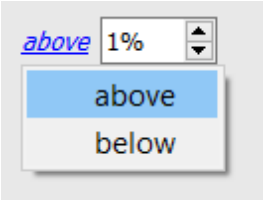
MaxObjects: trigger if number of classified objects is above or below a certain limit.

Click on the **blue hyperlink** to select whether the algorithm will trigger **above** or **below** a certain number of objects.

Select the **number** of objects.

Area

MaxArea: trigger if area occupied by classified objects is above/below a certain percentage of the total trigger area.



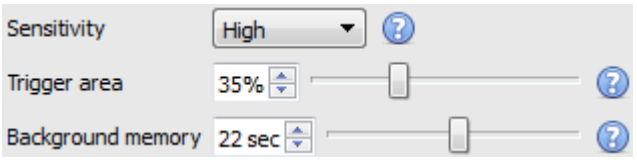
Click on the **blue hyperlink** to select whether the algorithm will trigger **above** or **below** a certain percentage of the selected area.

Select the **percentage**.

4.3.9 Queue Length Analytics

Setup Tab / Configure Servers / Video Analytics / New / Analytics type / Queue Length.

This algorithm can be set to monitor the length of a queue and trigger an event when a queue reaches a certain length. For example, this would be useful to alert a store manager that they need more staff working at the tills.



The image on the left is shown in the Context Area when selecting the settings.
Sensitivity sets how responsive the algorithm is to movement in the image.

Trigger area is the percentage of pixels that need to trigger (within the 4-by-4 pixel blocks that the algorithm uses) in order for the algorithm to also trigger.

Memory is how long the algorithm remembers the background.

4.3.9.1 Adding / Editing a Zone

By default, three zones comprise the queue area. **To add a zone**, double-click inside the area of one of the zones. This will split it in half. To merge two zones together, double-click on the line dividing the two zones.

4.3.9.1.1 Front and Back Zones

The green zone must always be set at the beginning of the queue. The red zone must be set at the end of the queue.

Note: The green and red zones cannot be divided.

4.3.9.2 Triggers

In the Context Area: after adding a trigger, set both the percentage and time for which the queue needs to be full, before a trigger is engaged.

4.3.10 Still Object

Setup Tab / Configure Servers / Video Analytics / New / Analytics type / Still object algorithm.

Still Object Detection monitors stationary objects which are introduced or removed.

This algorithm can be used in several situations, such as airports, parking, or stock areas. An object that was stationary in the image will trigger the Still Object Detection (SOD) algorithm when it is *removed*. An object that is *introduced* into the camera view will also trigger the Still Object Detection algorithm. For example, a car that parks in a restricted parking zone.

The **Still Object Detection** algorithm measures the change in an individual pixel's light intensity level over time. It identifies "blobs" of changes in intensity. If a blob is big enough and still enough, the algorithm will begin a countdown to determine whether the blob is stationary. Once this countdown stops, the algorithm will trigger. This trigger can be linked to events.

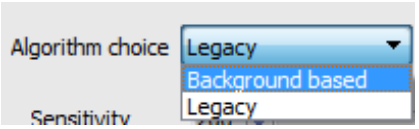
The setup process for this algorithm (and all video motion algorithms) is iterative. The user needs to adjust the algorithm to suit the environment and the objects being tracked. These guidelines do not provide generic settings, but provide definitions and explanations of how the algorithm works so that users can make informed adjustments.

4.3.10.1 Settings Panel

Select **Settings** on the left of the window. Configure the settings options which appear.

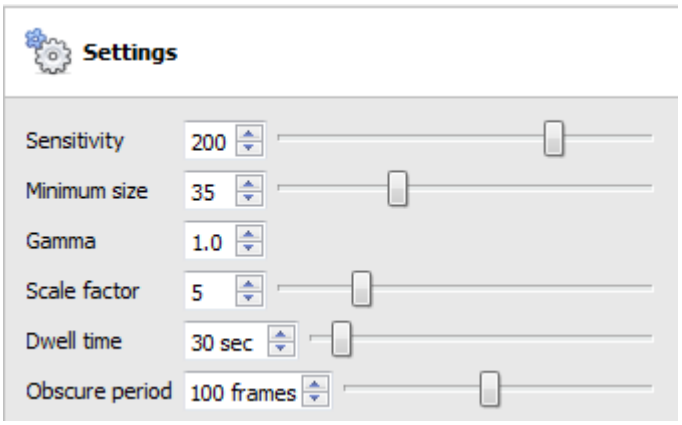
4.3.10.1.1 Choose Algorithm Type

The settings options will differ according to the algorithm type. Choose between these algorithm types:



- (updated) Background-based
- Legacy.

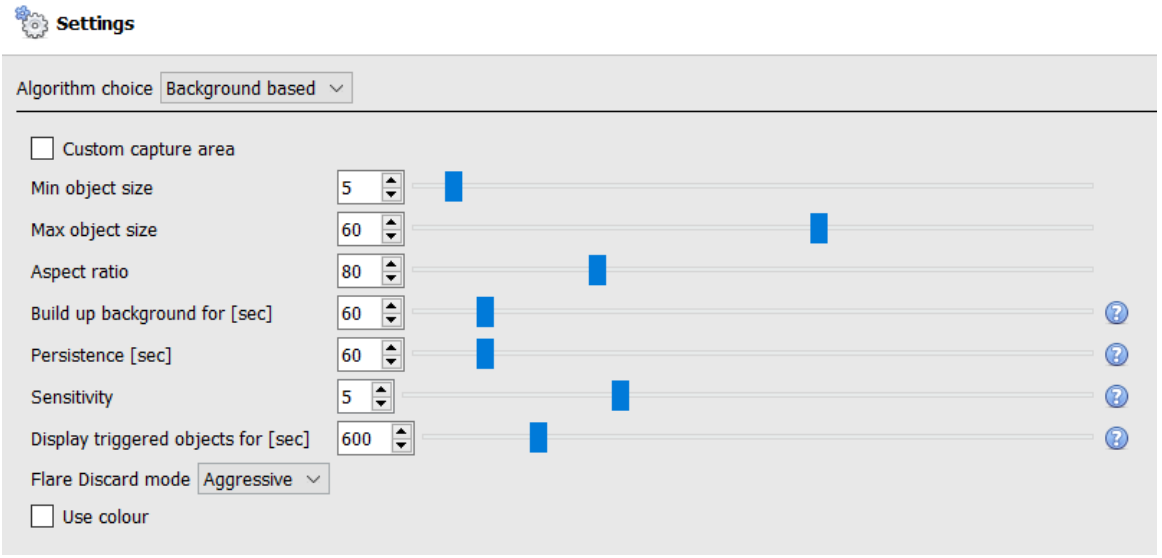
Legacy Settings



Sensitivity	The **sensitivity setting** reflects the light intensity changes on the pixel. Each pixel can produce light of 256 different levels of intensity. The sensitivity setting measures the change from the historical image to the current image. The change in intensity will be reflected as a value between 1 and 256. 50 is considered the smallest significant change in object detection, and 250 is the highest likely change that would occur. **Note**: this is not the actual intensity of the pixel. It is the *change* in intensity. Therefore, if the pixel was at 50 and then jumped to 110, the change would be 60. If sensitivity is set to 50, this change would be considered significant.
Minimum size	**Minimum size** is the smallest size an object can be, to be considered when triggering an alarm. Move the slider to view an image approximating the minimum size.
Gamma	**Gamma** changes the brightness and contrast of an image. Gamma changes these settings on a curve. *Increasing* gamma brightens darker areas, but has little effect on areas that are already bright. This allows the elimination of shadows. If objects being tracked are generally a similar colour to the background, then there should be a higher gamma setting (>10). *Decreasing* gamma will darken lighter areas and has little effect on darker regions of the image. If the objects being tracked are generally lighter than the background, it is often useful to darken the gamma.
Scale Factor	The **Scale Factor** relates to gamma and to sensitivity. It multiplies the difference between foreground and background. The default scale factor is 5. The range is 1 to 20. *Increasing* the scale factor makes the algorithm *more* sensitive to changes between foreground and background. If objects are not being tracked, the user can try to increase the scale factor. *Decreasing* the scale factor makes the algorithm *less* sensitive to changes between foreground and background. If parts of the background are being tracked, the user can try to decrease the scale factor.
Dwell time	**Dwell time** is the time that it takes for the algorithm to trigger an alarm, after a still object is placed in, or removed from, an image. This time is important, as it rules out objects that are momentarily placed, as well as momentary compression issues.

Obscure period	This setting lets the user set the time that an object is "remembered" after something has obscured it. In busy environments a still object will frequently be covered and uncovered by people passing by. The **obscure period** is measured in frames. Frames are the individual images captured by the camera, and can range from 10 to 500. This goes on the **frame rate** of the analytics channel, which usually runs at about 6 frames per second. At 6 frames per second, 500 frames will take roughly 83 seconds to pass by. The busier the environment, the longer the time objects should be remembered. The user needs to set a good balance between the **obscure period** setting and the **object dwell time** setting.

Background based Settings



Custom capture area: Check **Custom capture area** to apply an algorithm capture area. (**Note**: Adjust the capture area by clicking on it and dragging nodes.)
Min object size: Set the minimum object size to be monitored.
Max object size: Set the maximum object size to be monitored.
Aspect ratio: Adjust the aspect ratio.
Build up background model: Select the number of seconds for which to build up the background model.
Persistence: Set the number of seconds the trigger must persist in order to trigger.
Sensitivity: set the Sensitivity of the algorithm. (**Note**: The lower the sensitivity, the easier the objects will be picked up.)
Display triggered objects for: Set the number of seconds for which the triggered objects will be displayed.
Flare Discard mode: choose Passive, Aggressive, or None.
Use colour: select this to use colour for triggered objects.

4.3.10.2 Zones

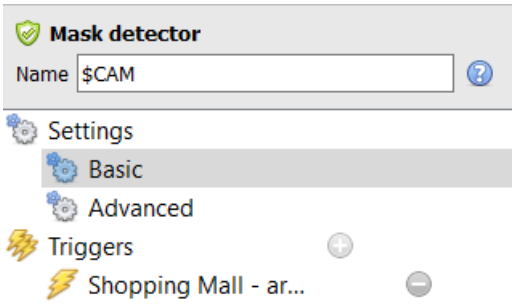
Painting zones follows the same procedure described in Basic / Smart VMD.

4.3.11 Mask detector

Available with Analytics Licenses I, II or III

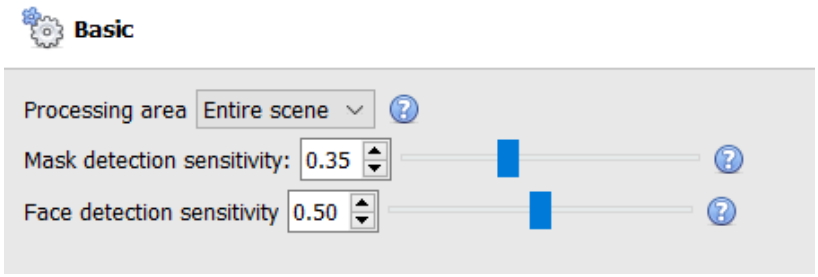
Setup Tab / Configure Servers / Video Analytics / New / Analytics type / Mask detector

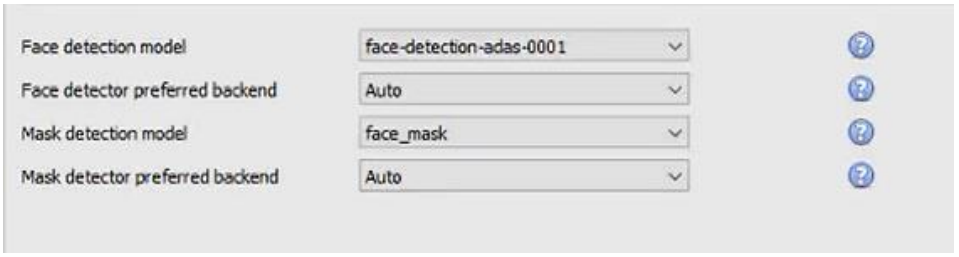
This algorithm detects face masks.



On the left of the **New video analytics** window, the user can configure settings and triggers.

4.3.11.1 Settings





Processing area: Set to custom to only process an area of the image. Make sure that the processing area surrounds the triggers. Drag the control points to change the processing area. The processing area may be adjusted by algorithm if too small.

Mask detection sensitivity: the sensitivity of mask detection. The higher the sensitivity, the more detections (accomplished by accepting masks at a lower confidence). The smaller the mask, the higher the sensitivity required to detect it. For example, if the camera range is long, it is recommended to use high sensitivity. For a camera setup that is closer to detected objects, lower sensitivity can be used.

Face detection sensitivity: decrease sensitivity to eliminated false detections. The higher the sensitivity, the more detections (accomplished by accepting faces at a lower confidence).

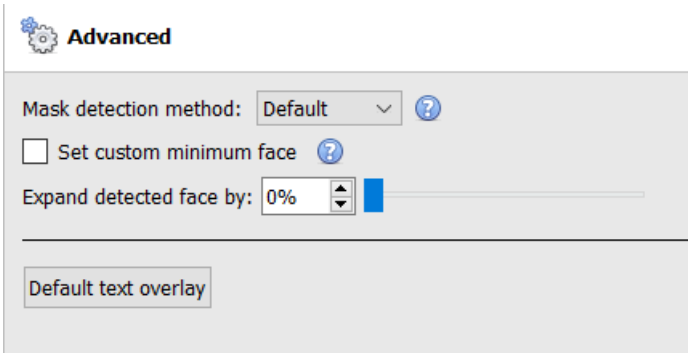
Face detection model: select a face detection model (the pre-trained deep neural network model used to detect faces).

Face detector preferred backend: select the preferred backend used by the model to detect faces. The selected model determines the backend options that are displayed. Depending on the model used, the preferred backend could be CPU, GPU_Intel, GPU_CUDA_FP32, or Auto.

Mask detection model: select the mask detection model (there is only one available, face_mask).

Mask detector preferred backend: select the preferred backend used by the model to detect masks. The selected model determines the backend options that are displayed. Depending on the model used, the preferred backend could be CPU, GPU_Intel, GPU_CUDA_FP32 or Auto.

4.3.11.1.1 Advanced settings

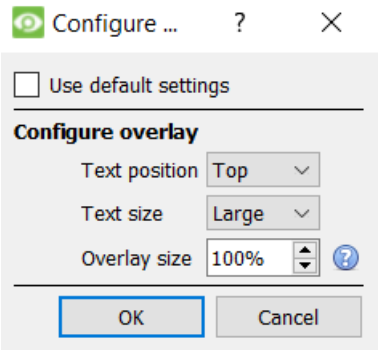


Mask detection method: the available options are Default, Immediate or Smart. *Immediate*: triggers on first occurrence of a mask/no mask. *Smart*: uses detection history to determine mask/no mask.

Set custom minimum face: the mask detector needs a reasonably-sized face to accurately determine the existence of a mask. Enable this option to set a custom minimum face size, above which to start analysing for masks.

Expand detected face by: select the percentage.

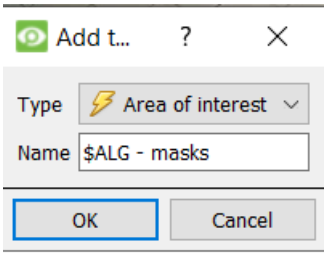
Default text overlay: click this button to configure overlays. The following window will appear:



Configure the overlay as required.

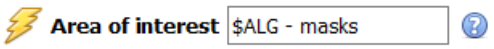
4.3.11.2 Triggers

Click the **plus icon** to add a new trigger.

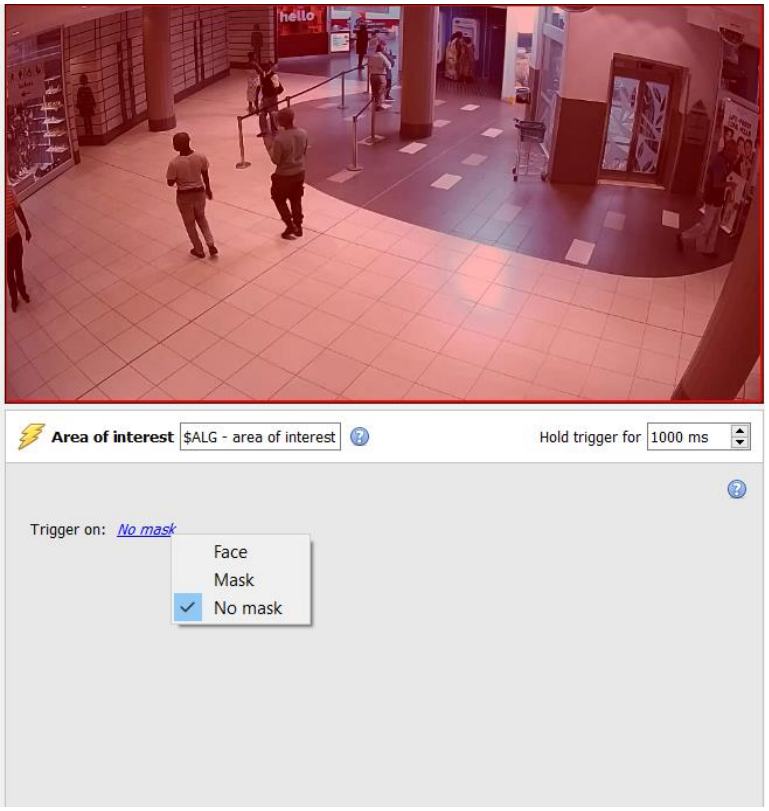


Select the **area of interest trigger** from the drop-down menu.

Give the trigger a name.



The trigger will be displayed in the panel on the right.



Configure the area.

Select whether the trigger will be prompted by **Face**, **Mask**, or **No mask**.

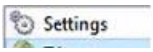
4.3.12 Basic people proximity

Available with Analytics I, II, or III

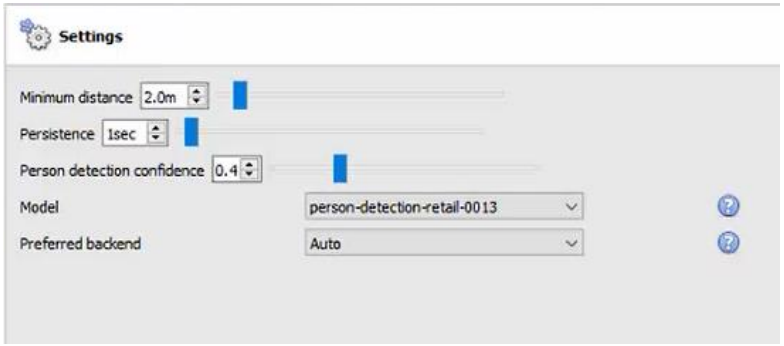
Setup Tab / Configure Servers / Video Analytics / New / Analytics type / Basic people proximity

Basic people proximity enables the detection of physical distancing violations.

4.3.12.1 Settings panel



To configure the **Basic people proximity** settings, click on **Settings** in the left side of the **New video analytics** window. The following options will appear on the right:



Minimum distance: select the minimum distance.

Persistence: set the persistence (in seconds).

Person detection confidence: select the person detection confidence. The lower the selected confidence, the lower the detection of people.

Model: the model used to detect people (the pre-trained deep neural network model used to classify objects).

Preferred backend: select the preferred backend used by the model to run the algorithm. Depending on the model used, the preferred backend could be CPU, GPU_Intel, GPU_CUDA_FP32 or Auto.

4.3.12.2 Triggers

Click the **plus icon** to add a new trigger.

Select the **basic people proximity** trigger from the drop-down menu.

Give the trigger a name.

The trigger name will be displayed in the panel on the right.

The user can select to **show occupancy**.

4.3.13 Thermal face temperature

Requires Analytics III license

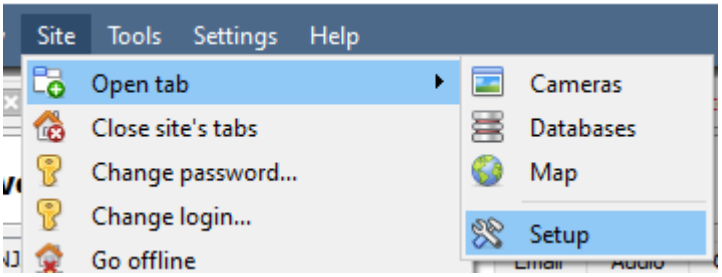
Setup Tab / Configure Servers / Video Analytics / New / Analytics type / Thermal face temperature

This algorithm is used to detect face temperatures above a certain threshold.

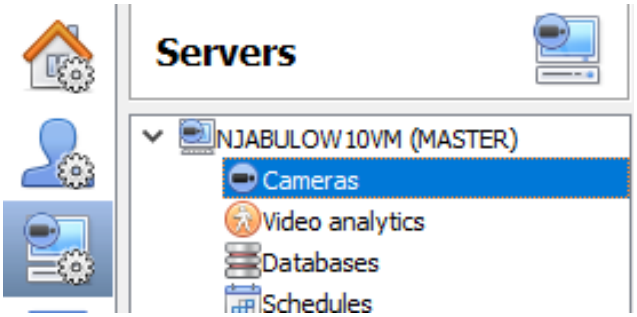
Note: this algorithm only works with Mobotix thermal cameras. For more information, please refer to the ***Mobotix Thermal Camera Integration App-note***, available on the Cathexis website.

4.3.13.1 Add camera

First, make sure that a thermal camera (integrated with CathexisVision) has been configured.



Go to **Site / Open tab / Setup**



Go to **Server / Server name / Cameras**

Click **New** to add a new camera.

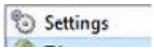
Choose the **thermal camera** and enter connection details.

Give the camera a descriptive **name**. Click **Next**.

Configure the camera streams (live/main recorded stream, analytics stream, and thermal stream).

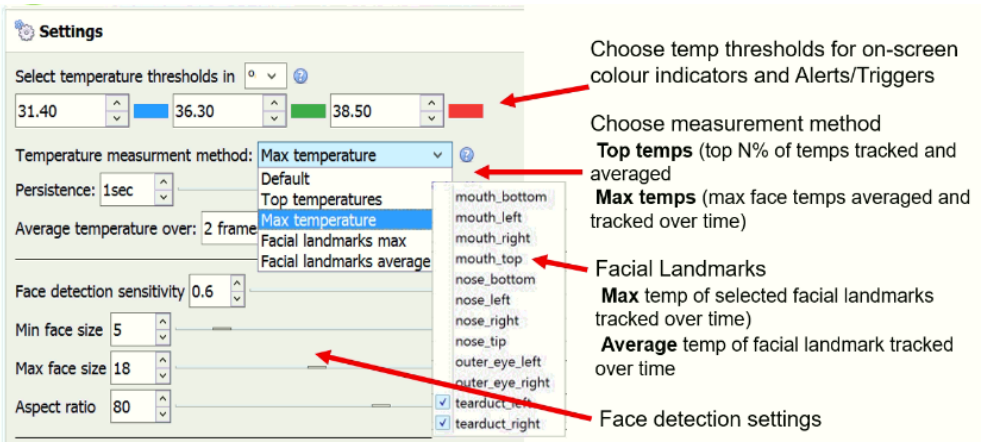
Enable video analytics in the analytics stream by right-clicking and selecting **enable video analytics**.

4.3.13.2 Settings panel



To configure the **Thermal face temperature** settings, click on **Settings** in the left side of the **New video analytics** window. The following options will appear on the right:

The annotated diagram below describes the options for settings:

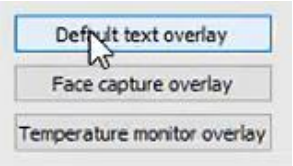


Select temperature thresholds in: temperatures can be read in Celcius (°C), Fahrenheit (°F) or Kelvin (K). **Note**: the minimum temperature read is 30 degrees Celsius. Anything lower than this value is considered an invalid reading and will not trigger.

Note:

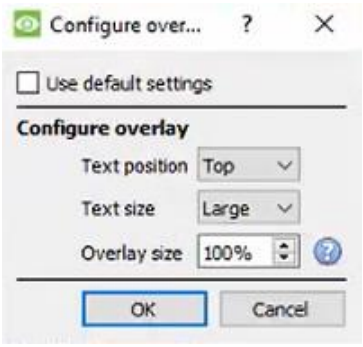
1. Facial landmarks should only be used when:
   - A black body is deployed.
   - The person being read is stationary on a precise spot marked on the floor for at least 2 seconds.
   - The parallax has been set accurately.
2. However, if Top or Max temperature are used and applied over the area of a rectangle, the exact overlap of the thermal and visual is less urgent.
3. The head size to position the person: very small head size could mean that a person can be detected from far away, and far away from the point of convergence. Face detection should be as close as possible to the point of convergence for higher accuracy and consistent results.

4.3.13.2.1 Overlays



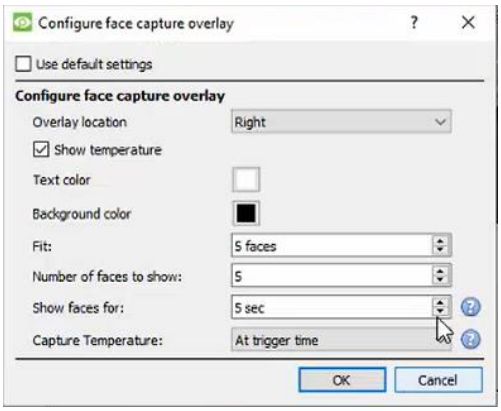
There are options to configure the **Default text overlay**, **Face capture overlay**, and **Temperature monitor overlay**.

Default text overlay



Configure the default text overlay as required.

Face capture overlay



Configure the face capture overlay as required.

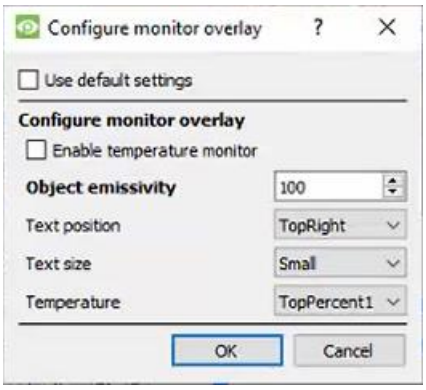
There are 2 options to **capture the temperature**: at the trigger time, or at the time of maximum temperature.

At trigger time: the temperature is stored in the database at the time of the trigger. The face will be displayed at the time of the trigger.

Time of maximum temperature: the temperature of the object/person will be monitored until the person leaves the scene. At that point, the maximum temperature and the time it was measured will be stored in the database. The face will be captured and displayed in the chosen position at the time of the highest reading.

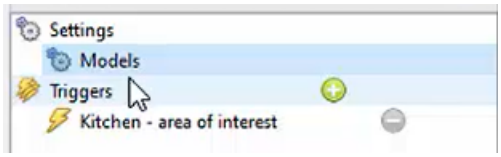
Note: the best option depends on the camera position.

Temperature monitor overlay



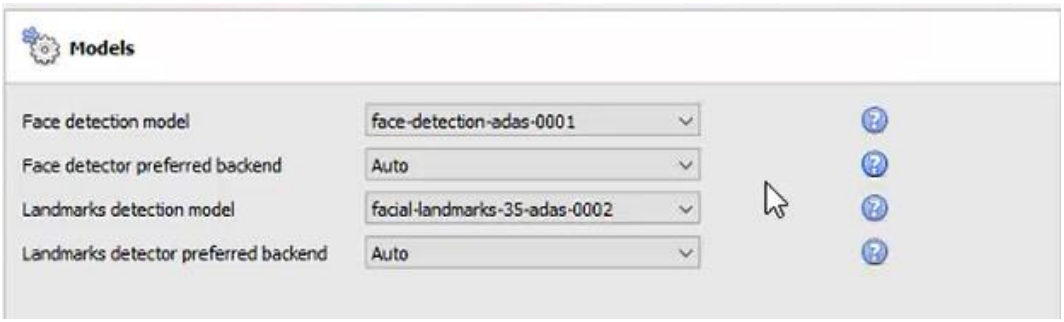
Configure the temperature monitor overlay as required.

4.3.13.3 Models



Click on **Models** in the left side of the New video analytics window.

The following options will display on the right panel:



Face detection model: the pre-trained deep neural network model used to detect faces.

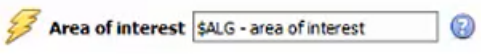
Face detector preferred backend: select the preferred backend used by the model to detect faces.

Landmarks detection model: the pre-trained deep neural network model used to detect landmarks.

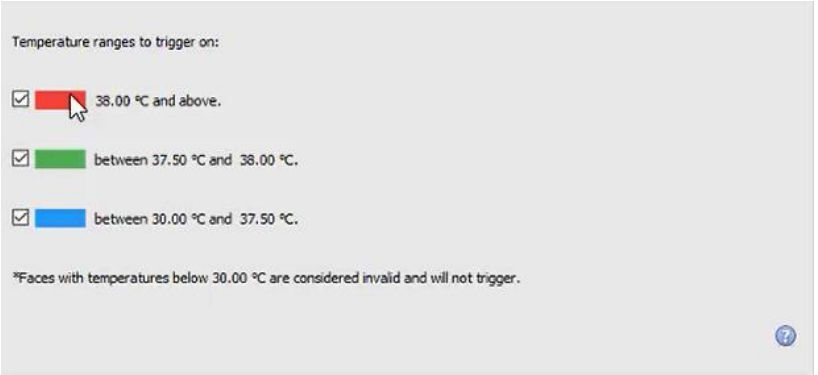
Landmarks detector preferred backend: select the preferred backend used by the model to detect landmarks.

4.3.13.4 Triggers

Click the **plus icon** to add a new trigger. Select the **area of interest trigger** from the drop-down menu.



The trigger will be displayed in the panel on the right.



Select the temperature ranges which will prompt a trigger.

4.3.14 Counting Analytics

Counting analytics allow for object counting using the **Line Counter** algorithm, and head counting using the **Top-down Head tracker** algorithm.

4.3.14.1 Line Counter

This algorithm only offers object counting. To trigger events when objects cross a line, use Basic, Intermediate, or Advanced analytics. For reports on object counting, contact support@cat.co.za.

For a guide to configuring the Line Counter algorithm, consult the Basic, Intermediate, and Advanced Analytics section as the calibrations are identical.

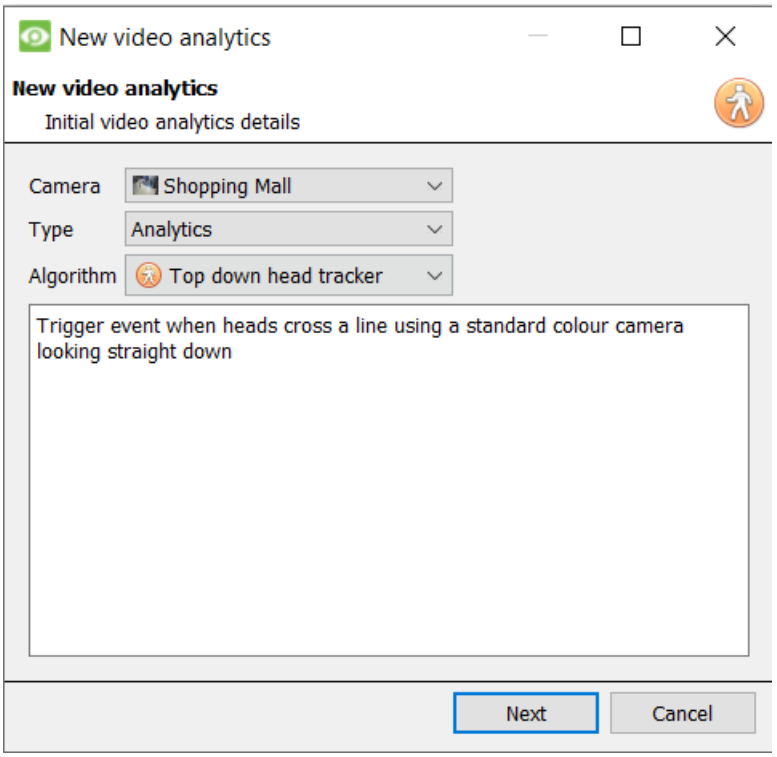
4.3.14.2 Top-Down Head Tracker

Available with Analytics III license.

Top-Down Head Tracker Analytics

Setup Tab / Configure Servers / Video Analytics / New / Analytics type / Top-Down Head Tracker

The Top-Down Head Tracker is designed to trigger when there is line crossing in an area. It offers event triggering when heads cross a line. It is used by a standard colour camera that is looking straight down.

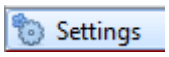


To use the top-down head tracker:

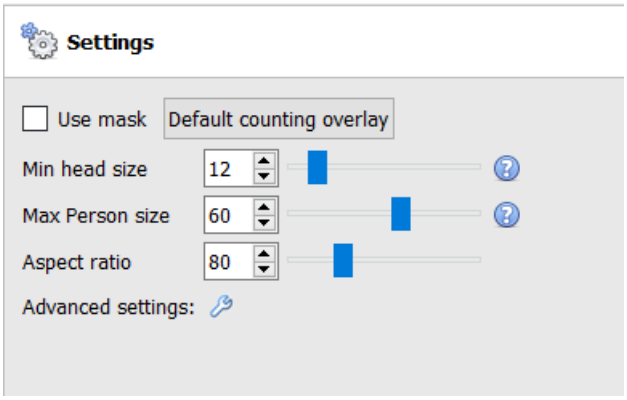
1. Visit New Video Analytics.
2. Select a camera.
3. Choose Analytics as the *type*.
4. Choose Top-Down Head Tracker as the Algorithm.
5. Click **Next**.

4.3.14.2.1 Configuring Top-Down Head Tracker Analytics

Settings Panel



In the left panel of the configuring video analytics window, select **Settings**. This will bring up the following options.

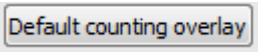


Use mask: This can be checked to capture the area of the image where the algorithm works.

Min head size: the algorithm will filter out any moving object smaller than the minimum head size.

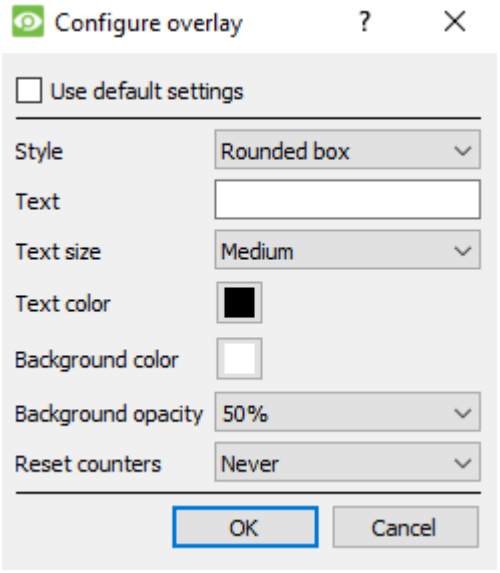
Max Person size: Moving objects larger than the "Maximum person size" will be split into a smaller object.

Aspect ratio: Change this setting to better fit the "Min head size" and "Max Person size" overlays to the moving objects.



Default Counting Overlay: Click to allow the visual display of tracking on the live and recorded data. This is useful to identify whether a head crossed a line, and how many times this occurred. These counts are also overlaid on the recorded footage. This setup allows re-setting the head counter on an hourly or daily basis.

Click on the **default counting overlay** button to adjust the following settings:



Check box to **Use default settings**.

Choose the **Style** of the count overlay.

Set **Text** to appear before the count number.

Select **Text size** and **colour**.

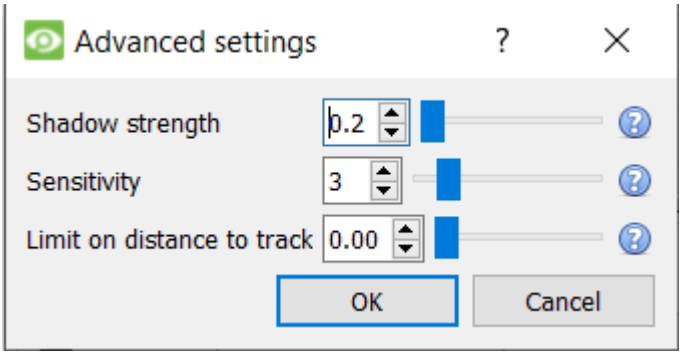
Select **Background colour** of the overlay.

Set the **Opacity** of the background colour.

Decide when to **Re-set counters**.

Advanced

Advanced settings: Click on the spanner icon to display Advanced settings.



In the Advanced tab, click on the help button to see an explanation of each option.

Shadow strength: Shadows will be multiplied by this value, making them weaker or stronger.

Sensitivity: The lower the sensitivity, the easier objects are detected.

Limit on distance to track: Maximum distance to track between heads. When '0' algorithm determines max distance.

4.3.14.2.2 Triggers Panel

Once the user has configured the algorithm, this indicates than an initial attempt has been made at the correct configuration of the system.

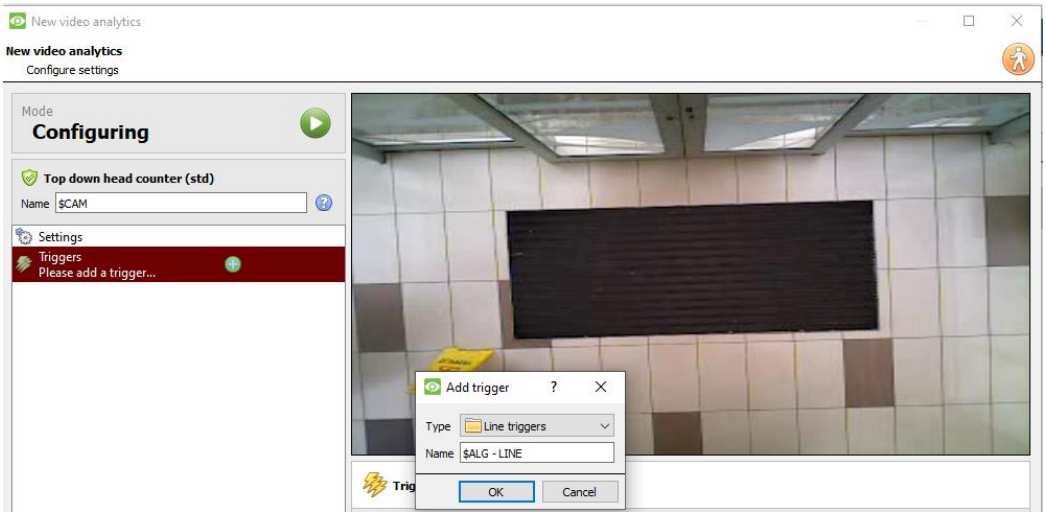
Now, the triggers need to be configured. These are rules that use the algorithm and result in decisions being made (for example, someone is tracked). Once the configuration process is complete, the configuration can be tested.

Triggers can be found in the configuration panel of the "new video analytics" window.

Add a Counting Line

Add a counting line that people need to cross in order to be tracked.

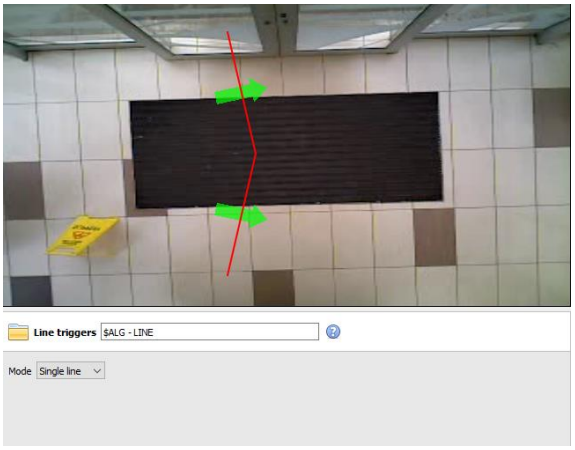
Click on the **plus sign** next to 'Triggers'.

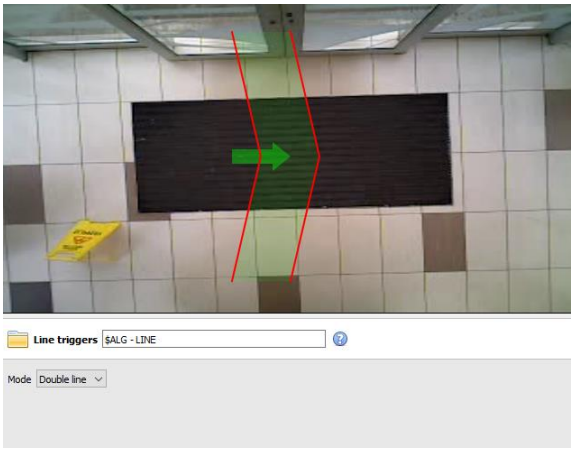


Click **OK**.

Choose Line Mode

Next, choose **single line** or **double line.**





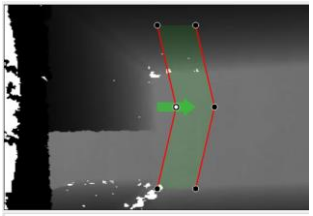
If a single line has been configured, the person needs to cross one line in order to be tracked.

If a double line has been configured, the person needs to cross both lines in order to be tracked. In this case, if the person dwells on the one line and then crosses back across the same line, that person will not be counted.

Tip: Add a double line to eliminate false counts which may occur when a person remains within a confined space around a line.

Define the Tracking Line

Note: This section details the definition of a **Double line**. The same principles apply to a **Single line**.



Define the line so that it covers the area where people will be counted as they cross.

Add nodes: Ctrl + click the red line.

Remove nodes: Double-click on the node to be removed.

Move the Line: Click anywhere on the red line to drag the counting line around.

Angle the Line: Click on a node and drag it to the desired position.

Add a Trigger

Click on the plus sign next to the camera name to add a trigger. Click **OK**.

Adding a trigger to the line enables the setup of CathexisVision events, which will trigger when the line is crossed.

If a trigger is configured, this trigger will be made available as a valid trigger in the event configuration. This trigger may be used to generate recordings, switch cameras to displays, or send alarms to a central monitoring station.

Click **OK**. Select **Line trigger.**

Note: Multiple triggers may be added to a line.

Define Direction of Trigger

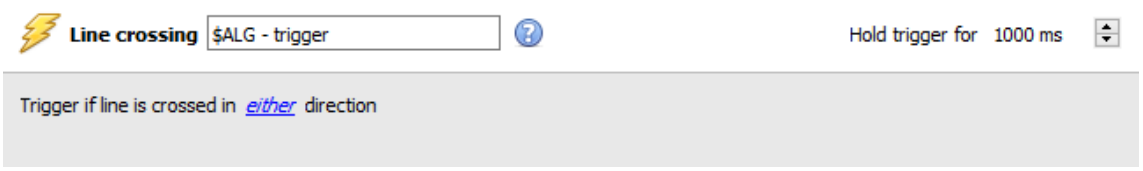
Once a trigger has been added, define which directions will trigger a count.

The default direction is set to Either. Select the trigger in the left panel. Options will appear underneath the camera image.

Note: A CNRP-1001 license is required for each direction being counted. If the default direction setting of **either** is being used, two CNRP-1001 licenses are required.

Click the blue hyperlink for options:

Either: will trigger events if people cross in either direction.



Forward: will trigger events if people cross the line in the same direction of the arrow.

Reverse: will trigger events if people cross the line in the opposite direction of the arrow.

Set the **Hold trigger** time to extend the event by this amount after the trigger has terminated.

Note: If multiple triggers have been added, define the trigger directions for each trigger.

4.3.14.2.3 Testing the Configuration

Once the initial configuration has been done, the performance of the head tracking system should be evaluated. This is done using the algorithm test mode.

Press the play button to enter the test mode.

Check the overlay tick boxes to enable the overlays. These overlays provide debug information that enable the algorithm to be tuned, by altering the settings discussed in the above **Settings Panel section.**

These overlays are also available in the live video feed and on the recorded video in the Cathexis Vision system. The recorded video may be used to evaluate the performance of the system. The user may turn some (or all) of these overlays on when required.

For further information on the Head Tracker, email support@cat.co.za.

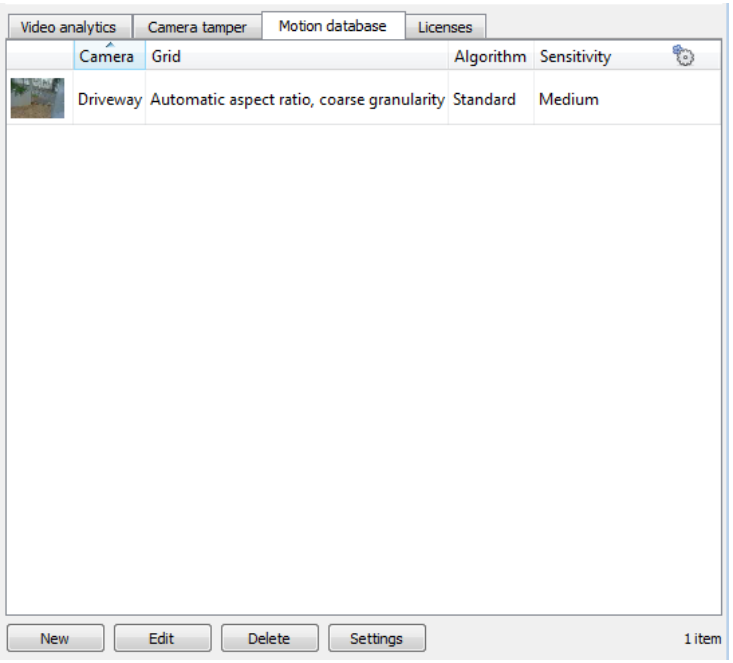
4.3.15 Motion Database (tab)

Motion database storage needs to be enabled for cameras which require motion data analytics. Motion data analytics (analytics which use data stored in this motion database) include:

- Heatmaps,
- Activity Trails,
- Motion Area Search.

Cameras on which these features are going to be enabled must then be added as motion database cameras. To add motion database cameras and configure the motion database, follow the instructions below.

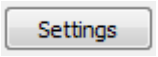
Note: For information regarding the operation of motion data analytics, please consult the ***CathexisVision Operator's Manual***.



Add a new motion database camera.

Edit an existing motion database camera.

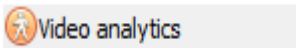
Delete a motion database camera.



Configure size and path of the Motion Database. See below.

Note: Only one motion database may be configured.

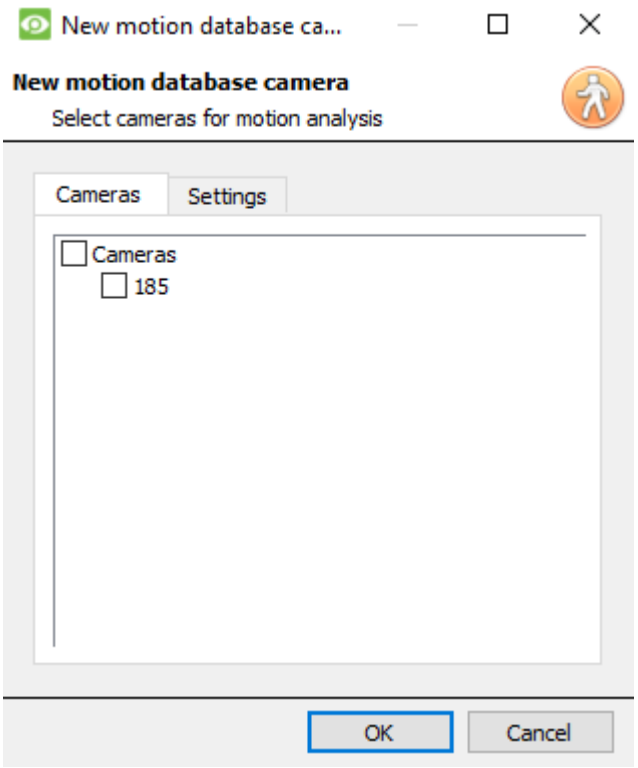
4.3.15.1 New Motion Database Cameras



Visit **Video Analytics**. Navigate to the **Motion database** tab to open the motion database.

Click New or right-click and select New to open the motion search camera window, to select which cameras motion data will be retrieved from. There are two tabs in this window; the Cameras Tab and the Settings tab.

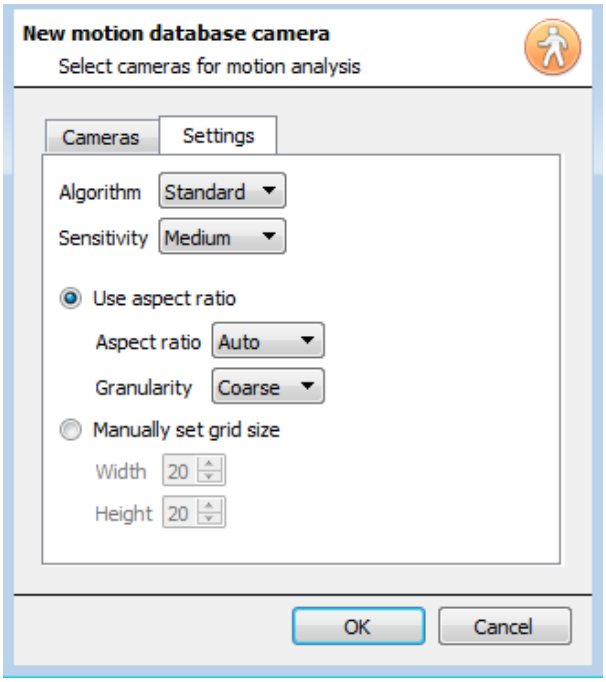
4.3.15.1.1 Cameras Tab



Select the cameras that motion search will be enabled on.

Note: Check **Cameras** before checking the desired cameras.

4.3.15.1.2 Settings Tab



Select the **Algorithm** type. Currently the only option is Standard.

Select the **Sensitivity**. The higher the sensitivity, the more finely motion is tracked.

Use either the automatic grid size settings by selecting **Use aspect ratio**, or **Manually set grid size**.

If choosing Use aspect ratio;

Select the **Aspect ratio**.
Select the **Granularity** of the overlay grid. See below for an explanation on Granularity.

To manually set grid size, select the **Width** and **Height** of the grid.

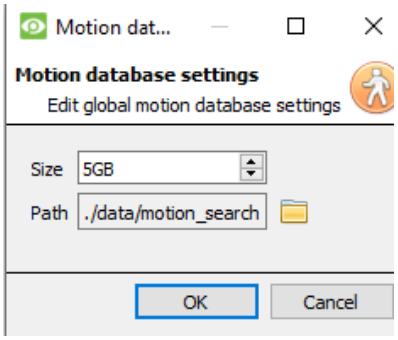
Click **OK** when done.

Granularity

The algorithm works by dividing the scene up into cells. The finer the granularity the smaller the cells, which means that motion can be detected in smaller areas of the image. The default settings are perfect for most camera configurations, the only reason to change this would be in the case of a high-resolution camera with a broad field of view, where the motion search results are not fine grained enough. There is a non-trivial cost in terms of processing and disk requirements associated with changing this. **Note**: changing the granularity on an existing motion database will invalidate the existing motion database.

4.3.15.2 Motion Database Settings

To configure the size and path of the Motion Database, click the **Settings** button.

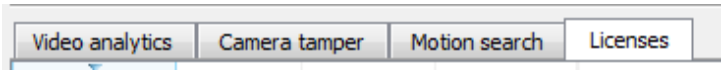


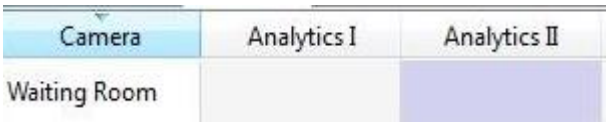
Motion Data is saved in its own database.

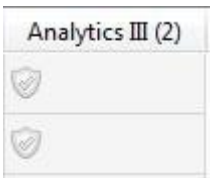
Set the **size** of the database.

Click the **folder icon** to set the **path** of the database.

4.3.16 Licenses (tab)

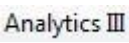






All analytics (other than Basic and Smart VMD) require licensing on a per-camera basis. Designate licenses to specific cameras in the Licenses tab, of the Video Analytics panel.

In the tab, there is a list of all cameras on this server, with a column for each Analytics type (from I to III).

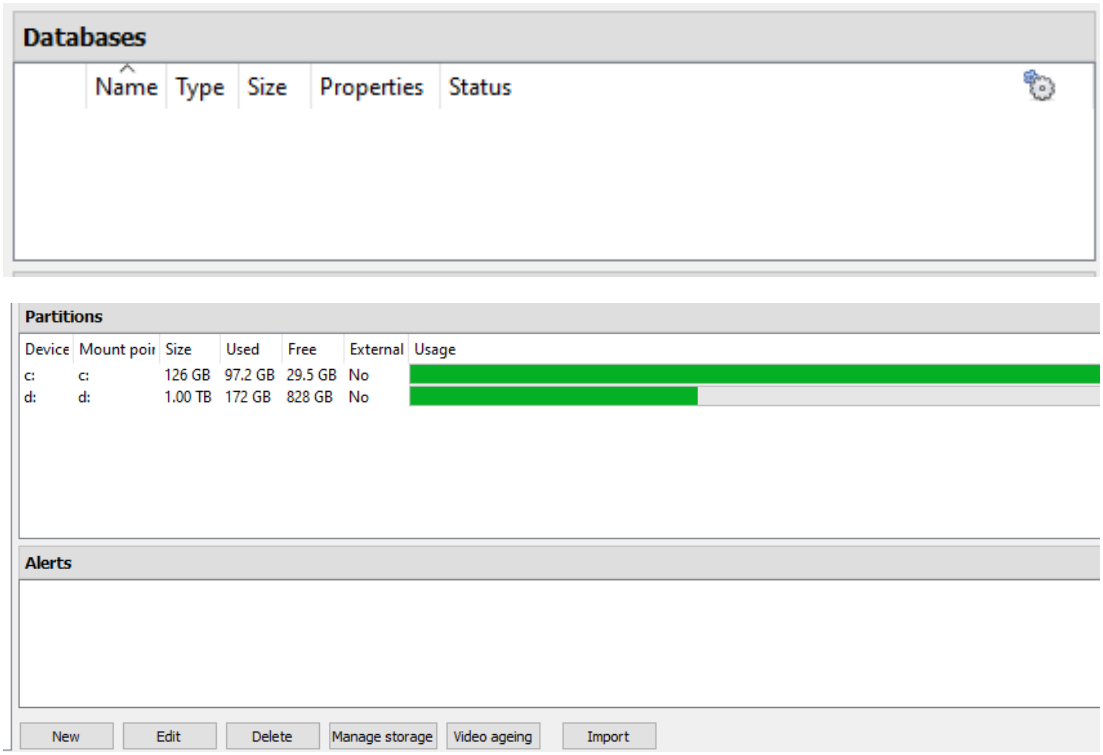
Spare Analytics licenses will be listed in parentheses next to the column header for that type. For example, Analytics III has 2 spare licenses here: 

. There will also be greyed **CathexisVision** license icons in that column.

Note: Analytics III will contain the analytics for I and II. So, if a camera is licensed with Analytics III, it is not necessary to add licenses for I and II, as they will already be included.

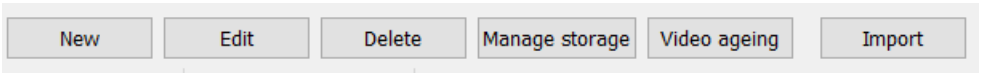
4.4 Databases

Databases are added on a Server-by-Server basis. Each server under **Configure Servers** will have a Databases section where that server's databases are managed.

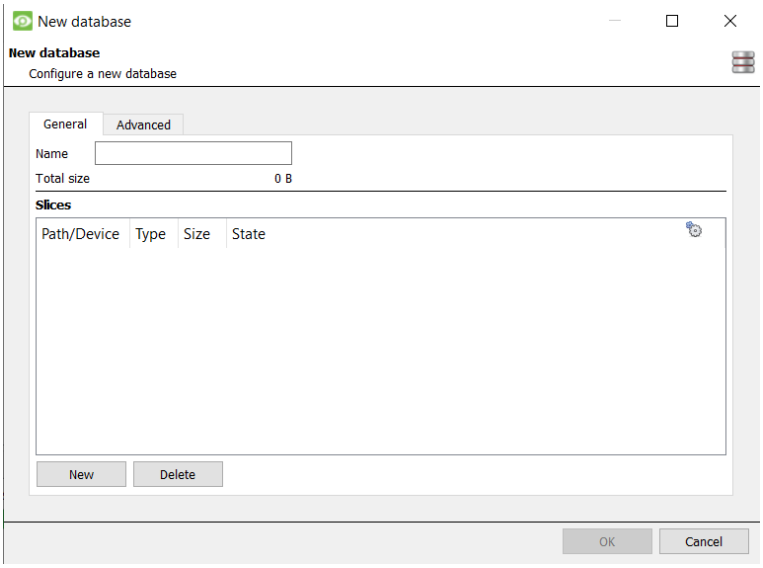


4.4.1 Add a Database

To create a new database, click on the **New** button in the **Databases** panel.



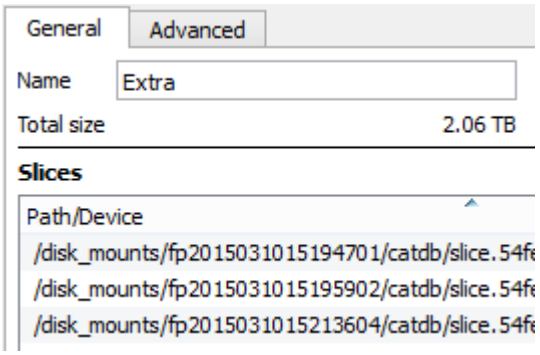
The **New Database** window will open:



Note:

1. If Adding/Importing a database to an NVR from another unit, or via a Client, the **Browse** option will not exist. In this instance, the file path should be entered manually.
2. The Basic Database option has been removed from **CathexisVision** 2015, and onwards. As such, all databases created with **CathexisVision** onwards will be Advanced Databases.
3. **Important**: When using network storage with NFS/CIFS file sharing, the NVR requires **exclusive use of the file share**. This is because, for performance reasons, the database is initialised on network storage with sparse files. This means the disk space, which is configured to be used by a database is not pre-allocated. Any other device using space on the file share could result in a failure where the database runs out of disk space.

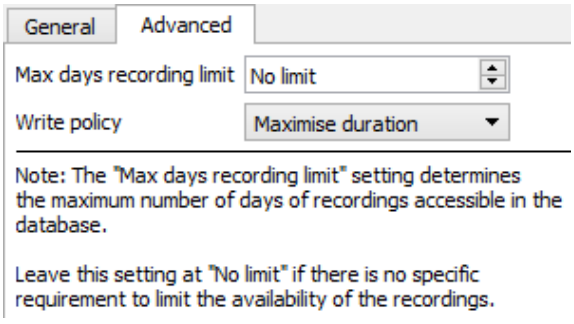
4.4.1.1 General



Give the database a descriptive **name**.

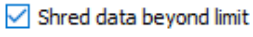
(An explanation of what slices are, and how to add them follows below.)

4.4.1.2 Advanced



The **Max days recording** setting will define how many days the database will record for. With **no limit** set, it will simply wait until the database is full to begin overwriting old data.

Document Database Shredding enables data older than the "max days recording limit" to be permanently deleted.



The data shredding option only appears when a “Max days recording limit” is set.

Write policy provides the option of maximising the duration of the recording, or the performance speeds of the database.

- With **maximise duration**, the database will pick the oldest video present when overwriting old data to add new data.
- With **maximise performance**, the database will split the cameras across all the disk slices in a manner that ensures the most even load across the disks. To do this, sometimes the database has to delete data that may not be the oldest data for a particular camera.

4.4.1.3 Adding a Slice

The database comprises a number of slices, which are sections of hard drive partitions.

To Add a Slice:

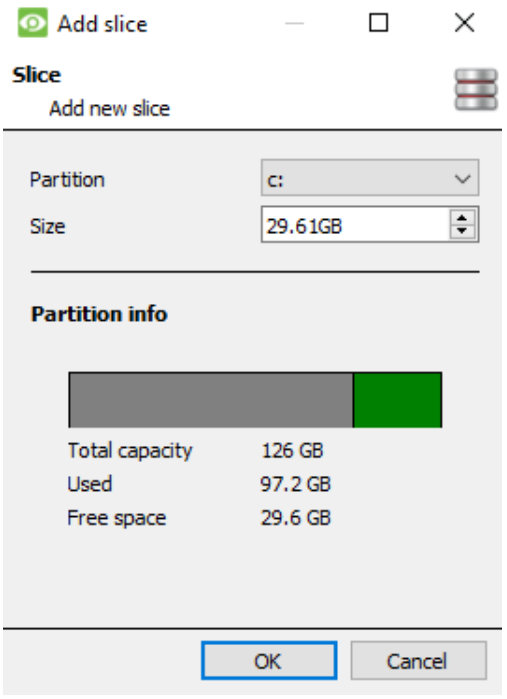
Click on **New** / Select the relevant partition / define the size of the slice / click **OK**.

Newly added slices will appear in the Slices section of the New Database window:

Slices

Path/Device	Type	Size	State
c:	file	399 GB	New
e:	file	594 GB	New

Once slices are added, click on **OK** to create an Advanced Database.



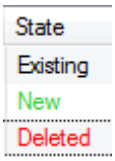
4.4.1.4 Important Recommendations

1. Ideally the database should be in its **own partition**, on its **own Hard Drive.**
2. If the database must share a drive with other information, then put it in its **own partition**.
3. It is recommended to **not** create a database in the Primary Windows Partition, however, if this is necessary:
    a. Do not create it within the **CathexisVisionNVR** installation folder.
    b. Do not make the database size unlimited. Leave between 50 and 100GB of disk space free when setting the size.

4.4.2 Edit an Existing Database

There are two ways to edit an existing database: Either:

1. Select the database / Click on the **Edit** button.
2. Double-click on the Database to edit.



When editing a database, editions to the slices will appear in the State column within the **Slices** textbox.

4.4.2.1 Edge insertion

For certain cameras, edge insertion can be enabled per database. Edge insertion will be added to newly integrated cameras as they are tested. Users are advised to contact Cathexis support (support@cat.co.za) to check which camera manufacturers are supported for edge insertion.

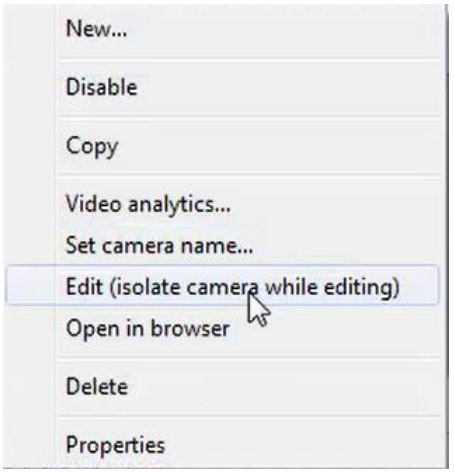
For supported camera manufacturers, follow the procedure outlined below to enable edge insertion.

1. The camera being used must support a form of **external storage**, such as SSD, SD card or HDD.
2. Make sure that the camera is set to record to the **database that is enabled** for missed footage.
3. From the camera's web interface, configure the camera to **record continuously** to the external storage. There will be options to either: overwrite footage when the SD card is full, or stop recording when the SD card is full. See note (c) below.

   Note: if the user wishes to record **audio**, make sure that audio recording to external storage is enabled on the camera's web interface.
4. **Confirm** that the recordings can be viewed from the web interface.
5. **Important note**: make sure that the camera and the Cathexis NVR are in **time sync**.

4.4.2.1.1 Enable edge in CathexisVision

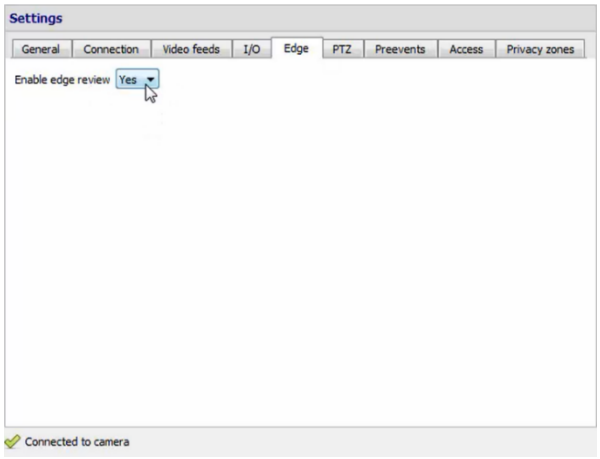
1. Go to **CathexisVision / Site / Open tab / Setup / Cameras**
2. If the camera has already been added, right-click on it.



From the menu that appears, select **Edit**.

The **Camera Settings** window will open.

3. Select the **Edge** tab.
4. Enable edge review.



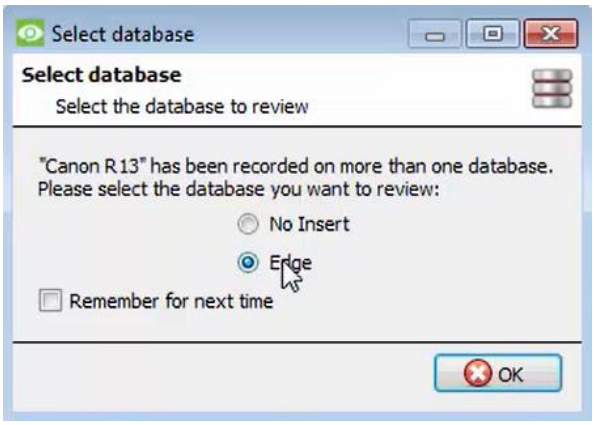
Click **OK**.

5. It is advisable for the user to check if the footage can be seen from the edge database.

   Go to **Site / Open tab / Cameras**

   Click on the camera to be viewed.

   Click on the **Review** button.

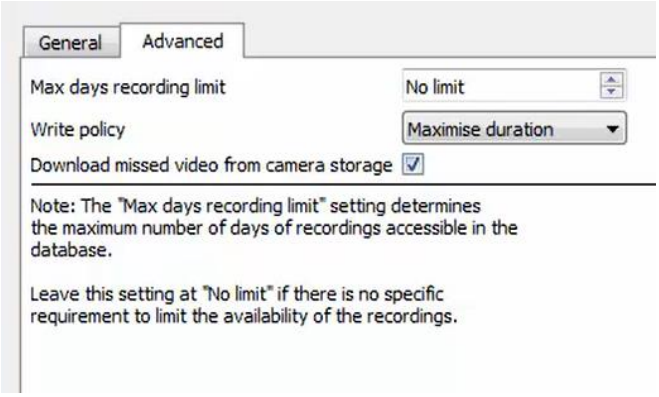
   

   In the window that opens, select the Edge database to be reviewed. Click **OK**.

   Then review the footage.

6. If the user has confirmed that the footage **can** be viewed from the Edge database, go to **CathexisVision / Site / Open tab / Setup / Databases / New** or **Edit** (depending on whether or not the database has already been created)

4.4.2.1.2 Download missed video



In the Advanced tab, tick the box that says "Download missed video from camera storage".

Click OK to save this setting.

When the network connection between the camera and CathexisVision NVR fails and is then restored, the missed data/footage will be inserted.

Note:

a. depending on the length of the footage, the insertion might take some time.

b. Only the footage from a single camera will be inserted at a time.

c. If the camera is set to **stop recording** when the SD card or external storage is full, CathexisVision will not receive data from the camera. If this setting is enabled, the user must make sure that the SD card does not get full. If the user has selected to **overwrite footage**, CathexisVision will receive footage even if the SD card is full, because the data will be overwritten.

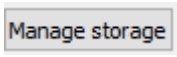
d. HikVision cameras are **not** supported for edge insertion.

4.4.3 Alerts

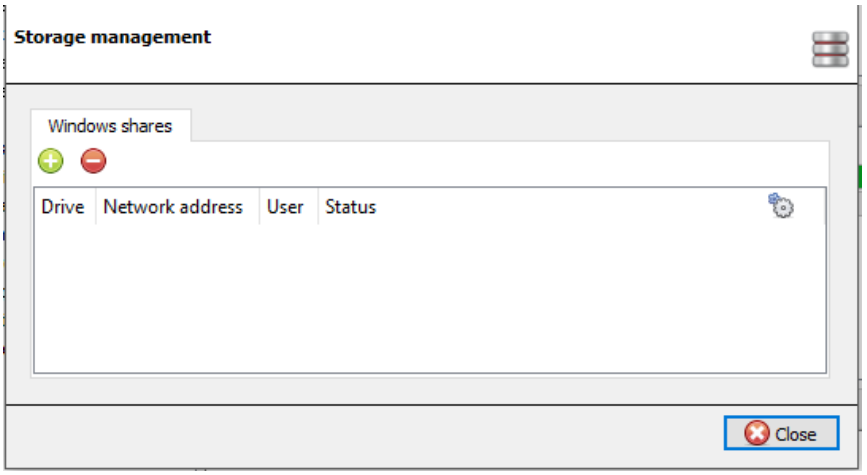
The alerts are specific to the currently selected database, and will show the **individual slice status**, if a slice in that database is not in a ready state.

For example, if the slice in a database is busy initialising, or if there is an error, an alert will be shown (with the slice ID) if that database is selected.

4.4.4 Manage Storage



Windows network shares can be managed by clicking on the **Manage storage** button.

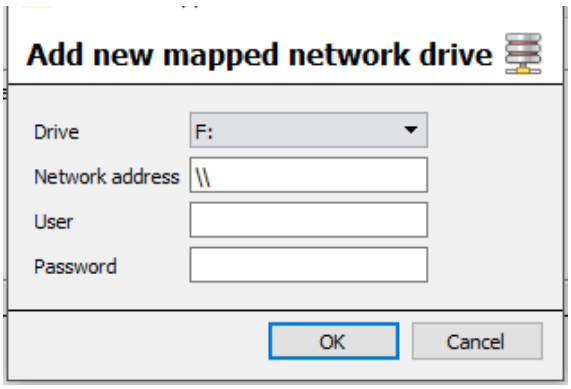


To add or remove network shares, use the **plus** or **minus** buttons.

Details of the network shares will appear in this area.

See below for adding a new network drive.

4.4.4.1 Add New Network Drive



Select the **Drive**.

Enter the Network Address.

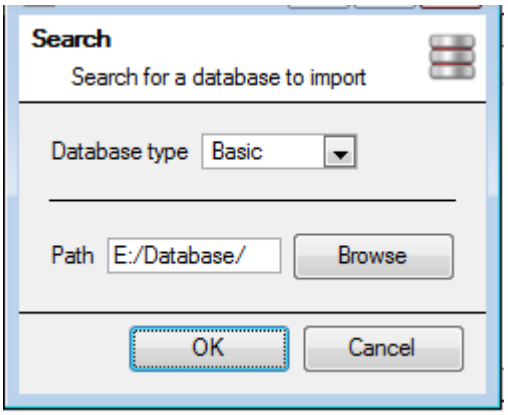
Enter the **User** and **Password** details.

Once added, the drive status should change to 'Pending' after about ten seconds. If this does not happen, check the drive settings by removing it and adding it again (there is no edit function).

4.4.5 Import a Database

Import Import an already existing database. To import a database, click on **Import**. There are two steps in importing a database.

4.4.5.1 Navigate to the Database Folder



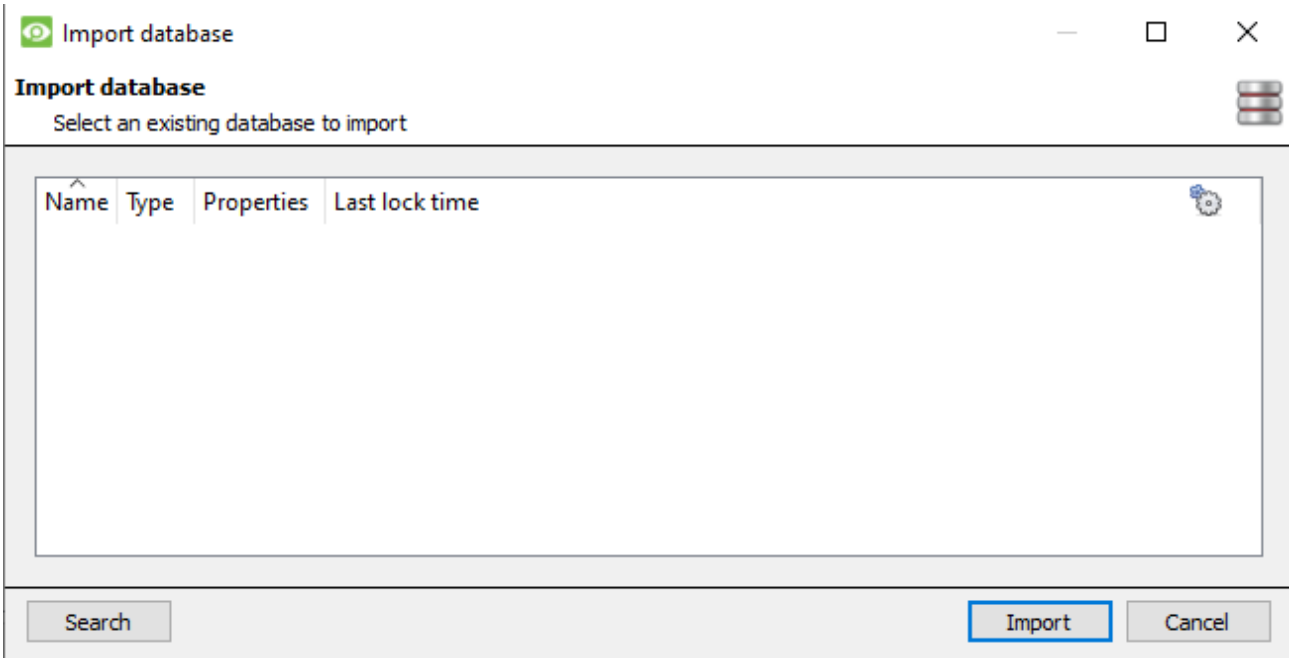
There may be multiple databases stored in one folder, and a database isn't represented as a single file. For this reason, when importing a database, only navigate into the folder that contains the database to import.

Select the Database Type.
Also, define whether or not a Basic, or an Advanced, database is being imported.

Note: If importing a database to an NVR from another unit, or a Client, there will not be the **Browse** option. Know the file path and enter it in manually.

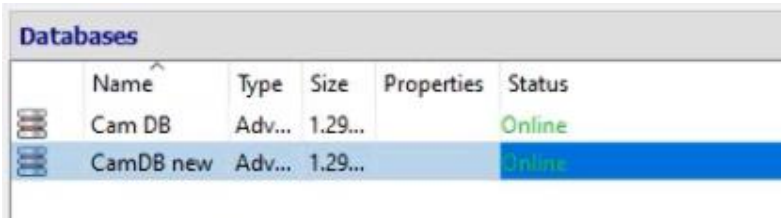
4.4.5.2 Select Database

CathexisVision will populate the database list with all databases found in this folder. Select the database to add from the list of databases.



4.4.6 Video Ageing

The video ageing setup is located at **Setup / Databases**. Video ageing requires two databases:



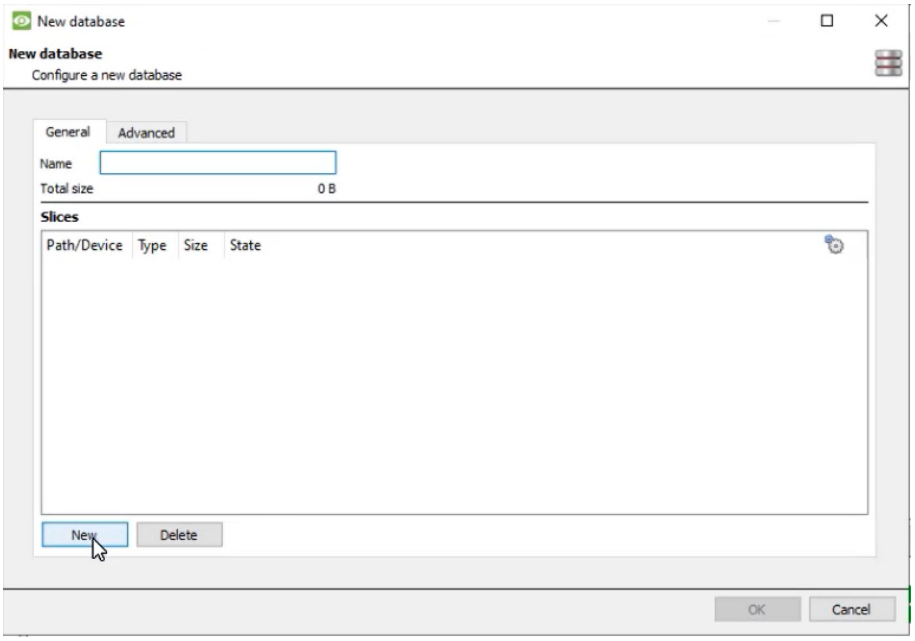
Video ageing takes the footage stored in one database and then writes it to another database. Video ageing also copies the overlays, audio and metadata of the source footage. The goal is for the video recordings to remain accessible for longer in the destination database, as they take up less space.

Note:

- The video in the destination database will likely be at a much lower FPS (frames per second) than the original footage.
- Video is only aged if it is older than 24 hours.

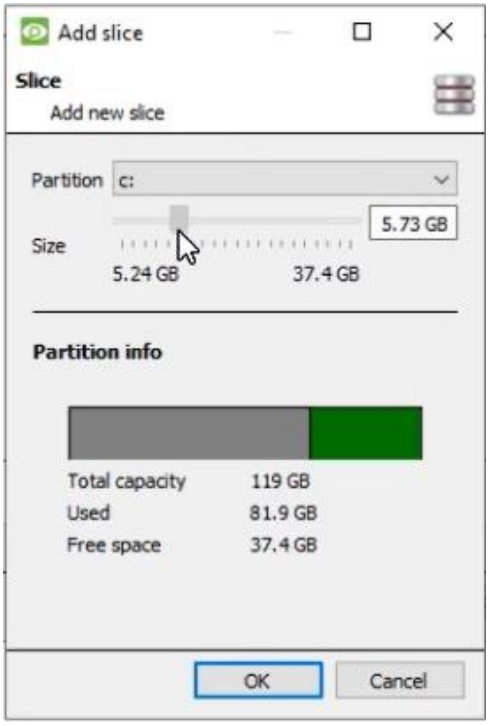
4.4.6.1 Create second database

In Databases, right-click and select **New…** . The **New database** window will appear.



Give the database a **name**.

In the bottom-left corner, click **New**. The **Add slice** window will appear.

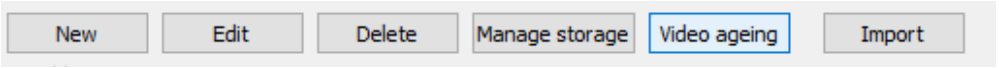


Select the partition and size.

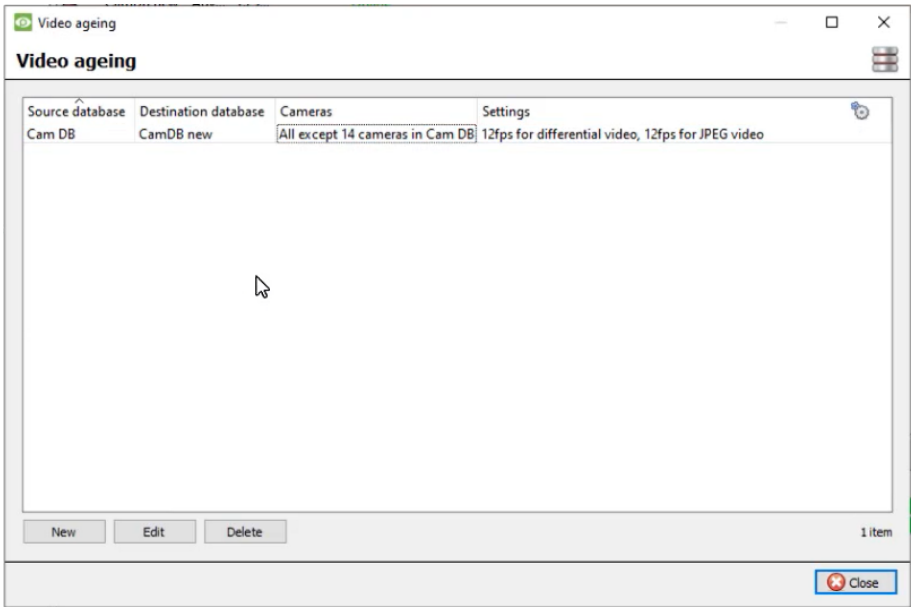
Click **OK**.

4.4.6.2 New video ageing

Click on the video ageing button at the bottom of the screen:



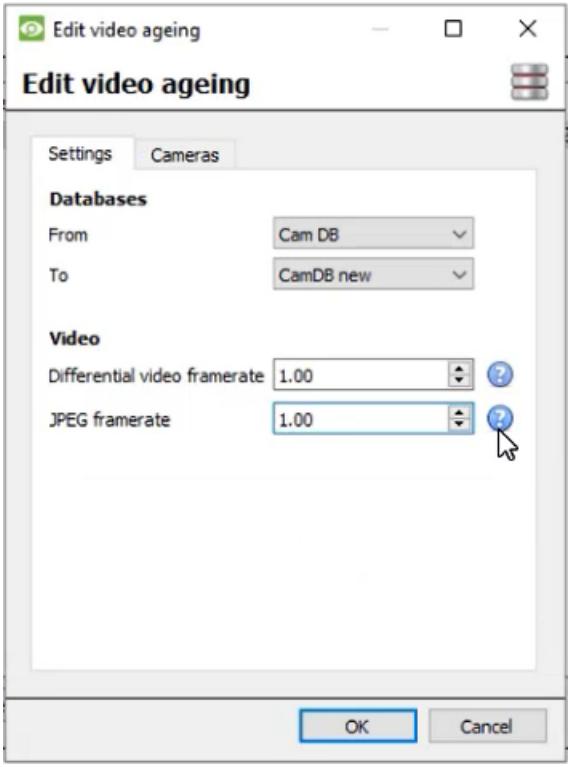
The video ageing window will appear, showing the source database and the destination database:



Click on the **New** button in the bottom-left corner.

4.4.6.2.1 Settings

After clicking **New**, the **New video ageing** box will appear. In the Settings tab:



Select the **From** and **To Databases** (source and destination database).

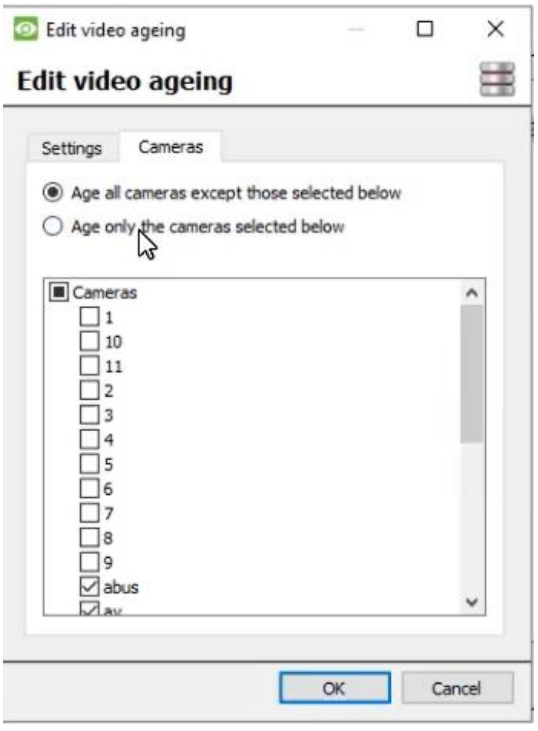
Under **Video,** adjust:

Differential video framerate: Differential video (H264, H26 etc) will be aged by storing i-frames to match the specified rate as closely as possible.

JPEG framerate: Single frame video (JPEG etc) will be aged by dropping frames to match the specified rate as closely as possible.

4.4.6.2.2 Cameras

Under the Cameras tab, decide which cameras to age.



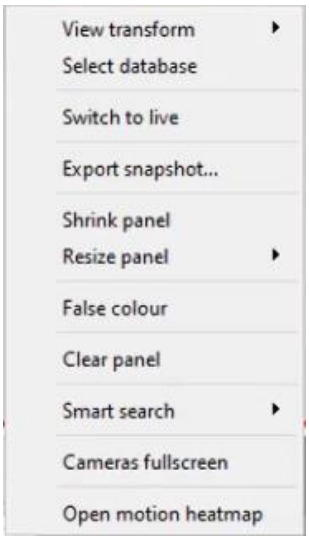
Note:

A database can only be configured as a destination once.

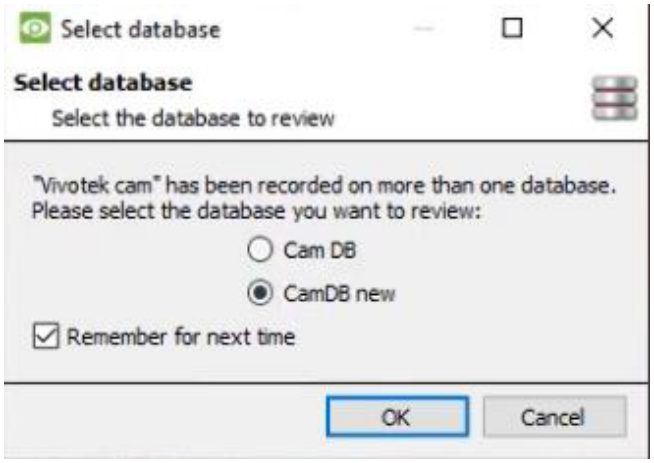
After a setting is changed, the video that is already in the destination database will not be overwritten. The settings will only affect the next video to be written.

4.4.6.3 View aged video

4.4.6.3.1 Live video feed



Right-click and choose **Select database**.



In the window that appears, select the destination database to view.

Click **OK**.

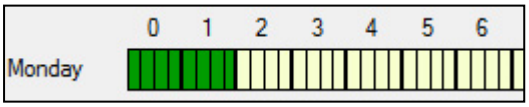
4.5 Schedules

Schedules All unit schedules for recording, and events, will be maintained under **Schedules** in the Configure Servers options.

4.5.1 Add / Edit a Schedule

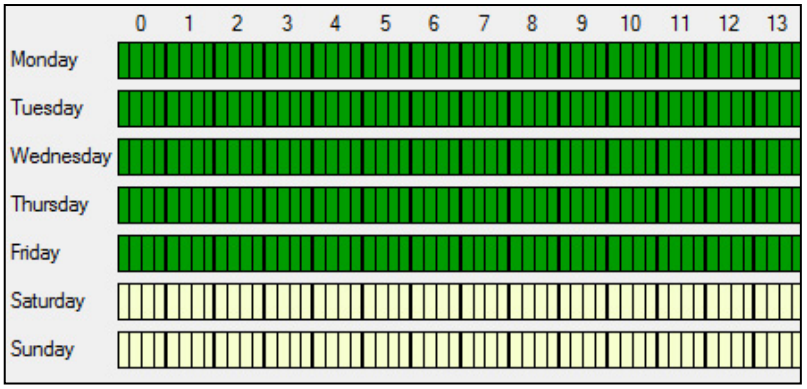
To add/edit a schedule, click on the relevant button and follow the instructions below. Give the schedule a descriptive name, and then define recording times (as shown below).

4.5.2 Set Schedule Recording Times



Left-click to select recording time – the green bars.
Right-click to unselect recording time – the yellow bars.

To **select multiple cells,** hold the left mouse button down and drag it across the desired time-frame.



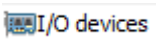
Recording week days only.
To record only week days, set the schedule as seen on the left.

Cross-section selecting.
To select, or deselect, areas in more than one day at a time: hold the mouse button and drag it across the days.

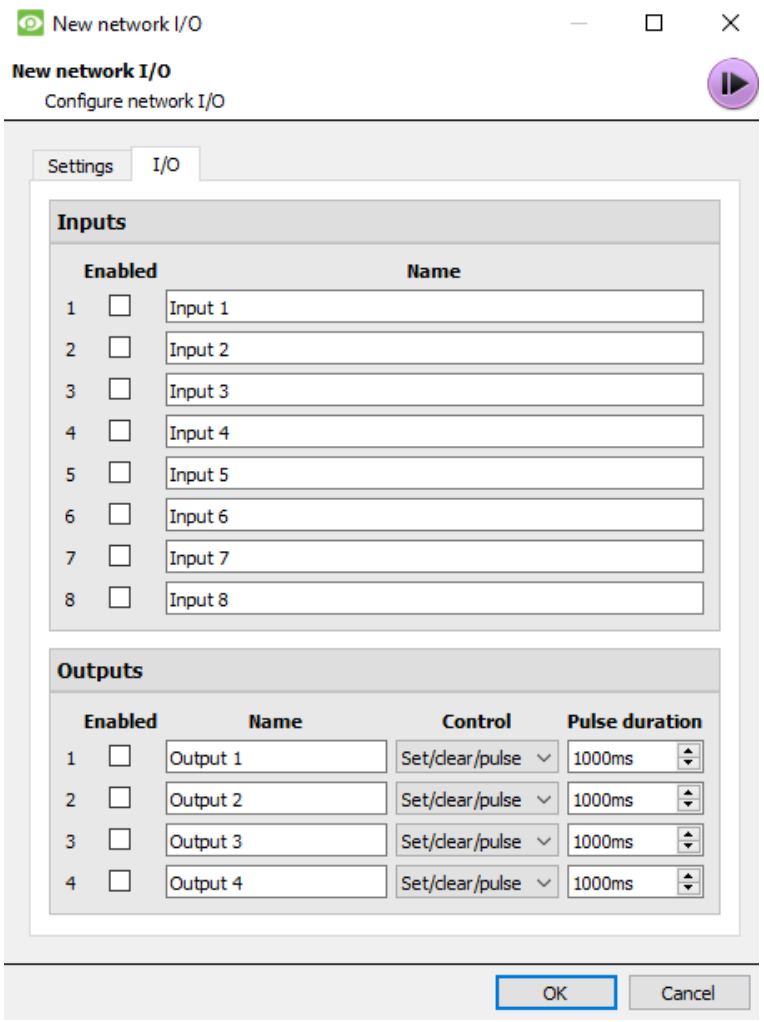
Click OK, and the schedule has been created. This schedule may now be used for recording, and events on this unit.

4.6 Network I/O

CathexisVision is capable of taking in relay inputs, and sending out relay outputs, via both analogue and digital channels. These relays may then be incorporated into the **CathexisVision** Events, and used as native triggers, and actions in the **CathexisVision** software.



Network I/O will be maintained under **I/O Devices** within the **Configure Servers** options.



4.6.1 Analogue

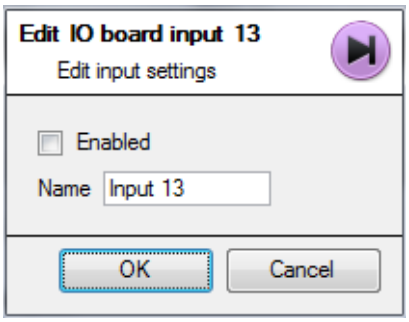
Note: this is supported on DVR units.

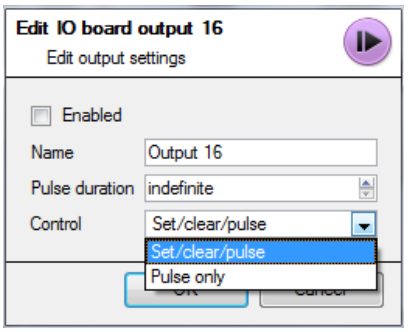
Relay connection on an analogue unit will be via the IO Board, on the back of the unit. This is connected to a PIA-mod card that comes standard on all analogue units.

The IO panel allows for 16 inputs, and 16 outputs.

4.6.1.1 Edit Input / Output

IOs are edited by selecting an input/output and clicking **Edit input**, or **Edit output**.





Enable
To enable an input, check the box titled Enabled.

Name
Give input a descriptive name.

4.6.1.2 Output Specific

Pulse Duration: Set the duration of the output pulse, in milliseconds.

Control: Also set how the Relay is controlled. Give Set, Clear, and Pulse control; or set it to Pulse exclusively.

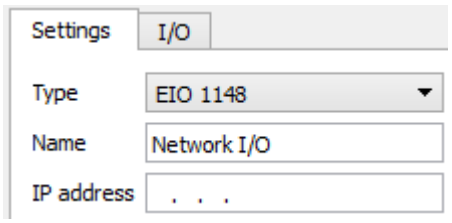
4.6.2 Network

Network Based IOs are handled by the EIO-1148, or EIO-3148, Network Base IO Expander.

This device enables comprehensive access, and control of remote in/output relays over an Ethernet network. Through the **CathexisVision** software control, opening and closing of integrated relay contacts can be incorporated into any response of a critical event.

4.6.2.1 Settings Tab

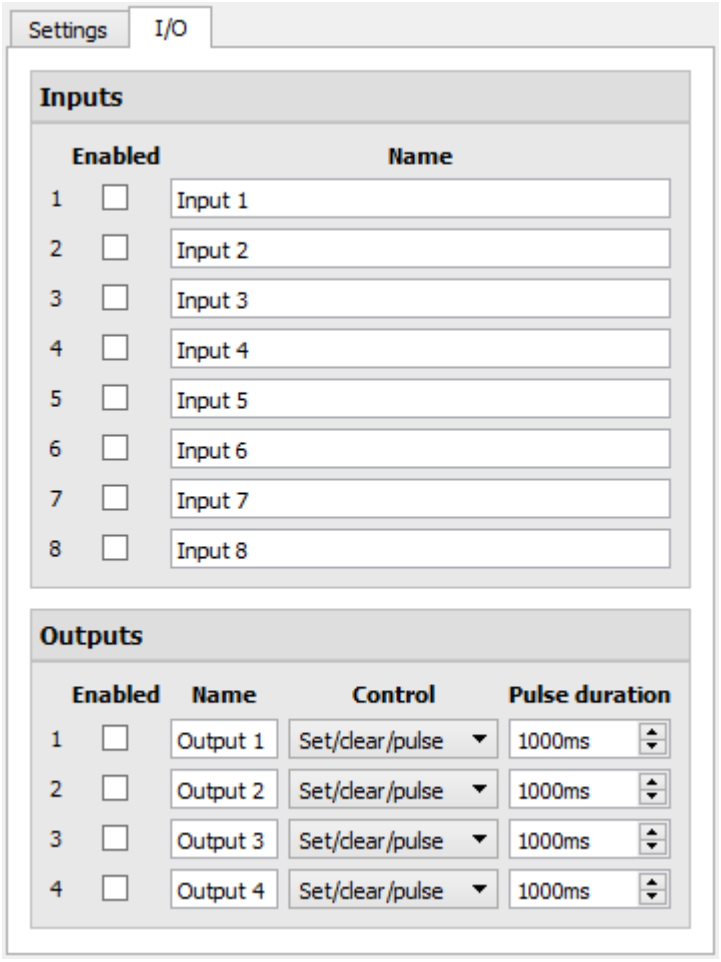
Clicking on the Network I/O tab, within the I/O devices option, followed by selecting **New**, gives the following options.



Name
Give device a descriptive name.
IP Address
This is the IP address of the IO unit.

Note: if the IP address of the EIO unit being added is unknown, find the unit using the **Cathexis Encoder Setup** tool, which is installed with the **CathexisVision** software. Find it in the **CathexisVision** install folder, or under: **Start / Cathexis / CathexisVision Encoder Setup**. On start-up this will bring up a full list of available devices.

4.6.2.2 IO Tab

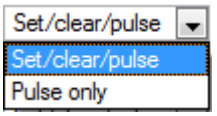


General:
Give the input a descriptive name.

To enable an input, check the box in the column titled Enabled.

Output Specific:

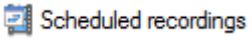
Set the way the relay is controlled using the drop-down menu in the Control column.



Pulse Duration:
Set the pulse duration of the relay, in milliseconds.

Note: make sure that these inputs have descriptive names.

4.7 Scheduled Recordings



Set cameras to record on a fixed schedule. This is done in Scheduled Recordings under **Configure Servers**.

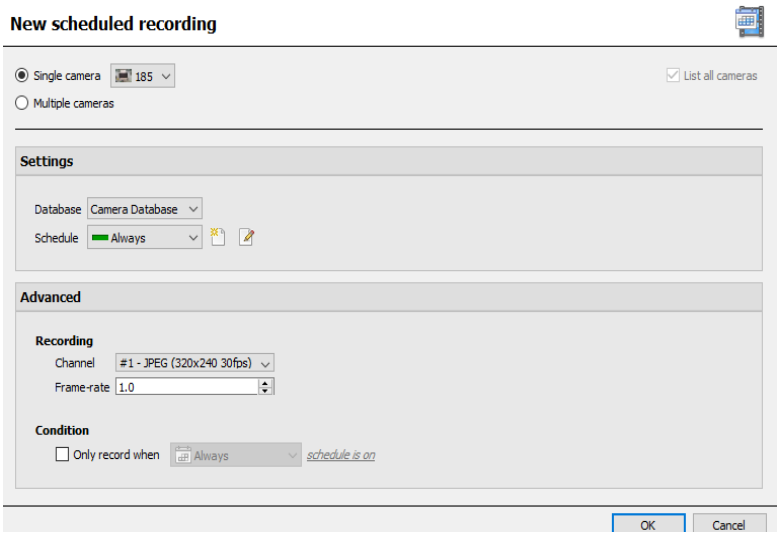
4.7.1 Add / Edit a Scheduled Recording

Either:

1. Click on **New** or **Edit**. Or
2. Right-click
   a. White-space and **New** (for a new Schedule)
   b. On an existing schedule and select **Properties** (to edit this existing schedule)

Note: Multiple scheduled recordings can be added using the "New" button in the scheduled recording setup.

This will bring up the Scheduled recording dialogue:



Camera — Select the camera to record. Choose single or multiple cameras.

Database and Schedule — The database to record to and the particular schedule to assign to this Scheduled Recording.

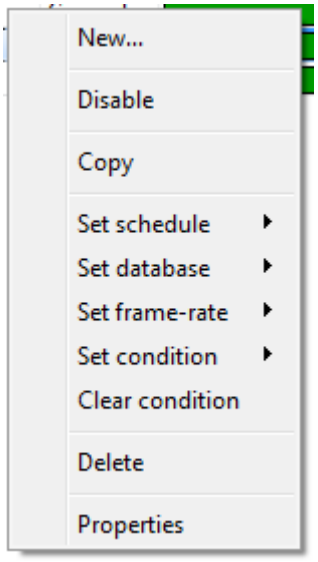
Recording Channel — The video channel to record from the camera.

Frame Rate — The frame rate at which to record.

Condition — Check the box to **only record when… . T**hen select an input from the drop-down menu. Modify the condition requirement of that input by clicking on the blue hyperlink next to the menu. This sets the scheduled recording to record based on the condition of an input. Inputs include existing schedules, virtual inputs, analytics algorithms, etc.
This condition will be indicated in the list of scheduled recordings in the 'Condition' column.
Note: Depending on the schedule selected for the recording, unless an input condition is enabled, the recording will be continuous.

Note: The schedules that are available are the schedules that are maintained on each server. Also create/edit these schedules here, using the options.

4.7.2 Right-click Menu



Right-clicking on an existing scheduled recording offers quick-adjustment options. These are the same options that are available when creating or editing a scheduled recording.

Note: To change the recording Channel, edit the schedule via **Right-Click / Properties**; or by selecting the Schedule and clicking **Edit**.

4.7.3 Copy Paste

Copy/paste schedule settings either from one schedule to another, or from one schedule to a new camera.

4.7.3.1 Copy Settings Between Schedules

Right-click on an existing scheduled recording / Copy / right-click on another scheduled recording / Paste.

4.7.3.2 Copy Schedule Settings to a New Schedule

Copy the schedule settings onto a new scheduled recording:

1. Right-click existing scheduled recording / Copy / Right-click anywhere / Paste New.

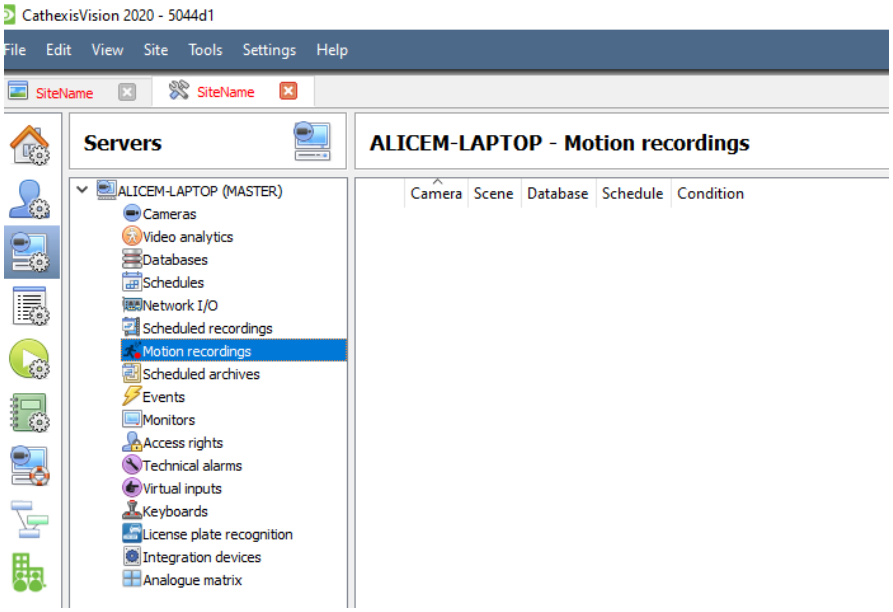
   This will bring up a list of cameras that are attached to this unit (for example: ☑ Analog One).
2. Select any number of cameras to paste the schedule onto, and click OK.

4.8 Motion Recordings

4.8.1 Locate Motion Recording

The motion recording system simplifies the process of configuring motion recording. It is analogous to scheduled recording, except the recording is triggered by VMD rather than a schedule.

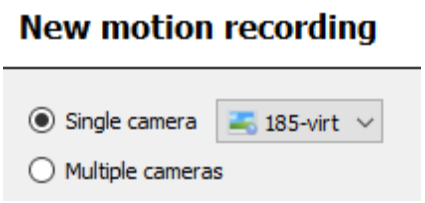
The Motion recording configuration is in the server setup, below Scheduled Recordings:



4.8.2 New Motion Recording

4.8.2.1 Cameras

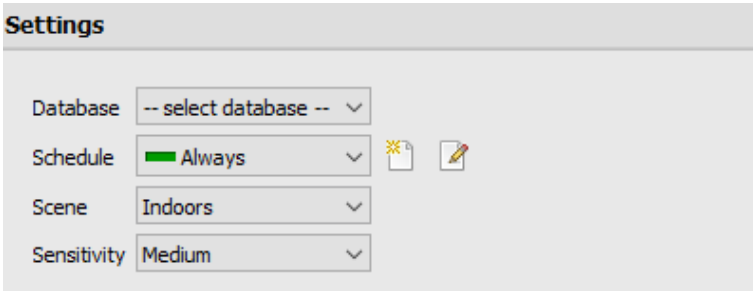
Click the **New** button at the bottom-left of the Motion recordings tab. Motion Recording can be set for multiple or single cameras:



Note:

- The same camera can be used in multiple motion recordings. For example, using a different schedule.
- When a camera is deleted, its motion recordings are also deleted.
- When a camera is deleted, its input is also deleted.

4.8.2.2 Settings



From here:

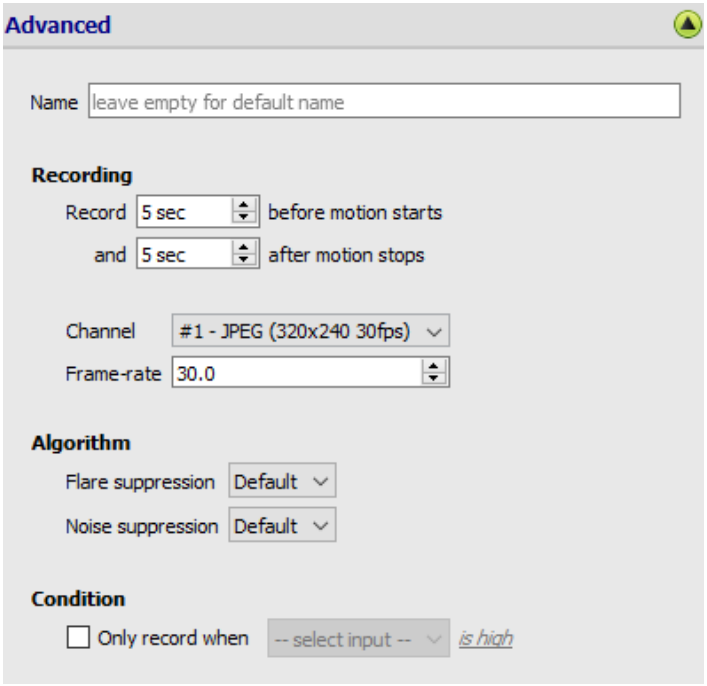
Select database.

Set **Schedule.**

Set **Scene** as Indoors, Outdoors (busy), Outdoors (sterile).

Set **Sensitivity** as low, medium, or high.

4.8.2.3 Advanced Settings



Under **Advanced Settings:**

Choose a **Name.**

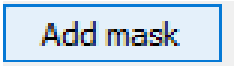
Set **Recording,** channel, and framerate.

In terms of **Algorithm,** the options for Flare suppression and Noise suppression are Default, Yes, and No.

Set **Condition** to only record when selected input is high or low.

4.8.2.4 Mask

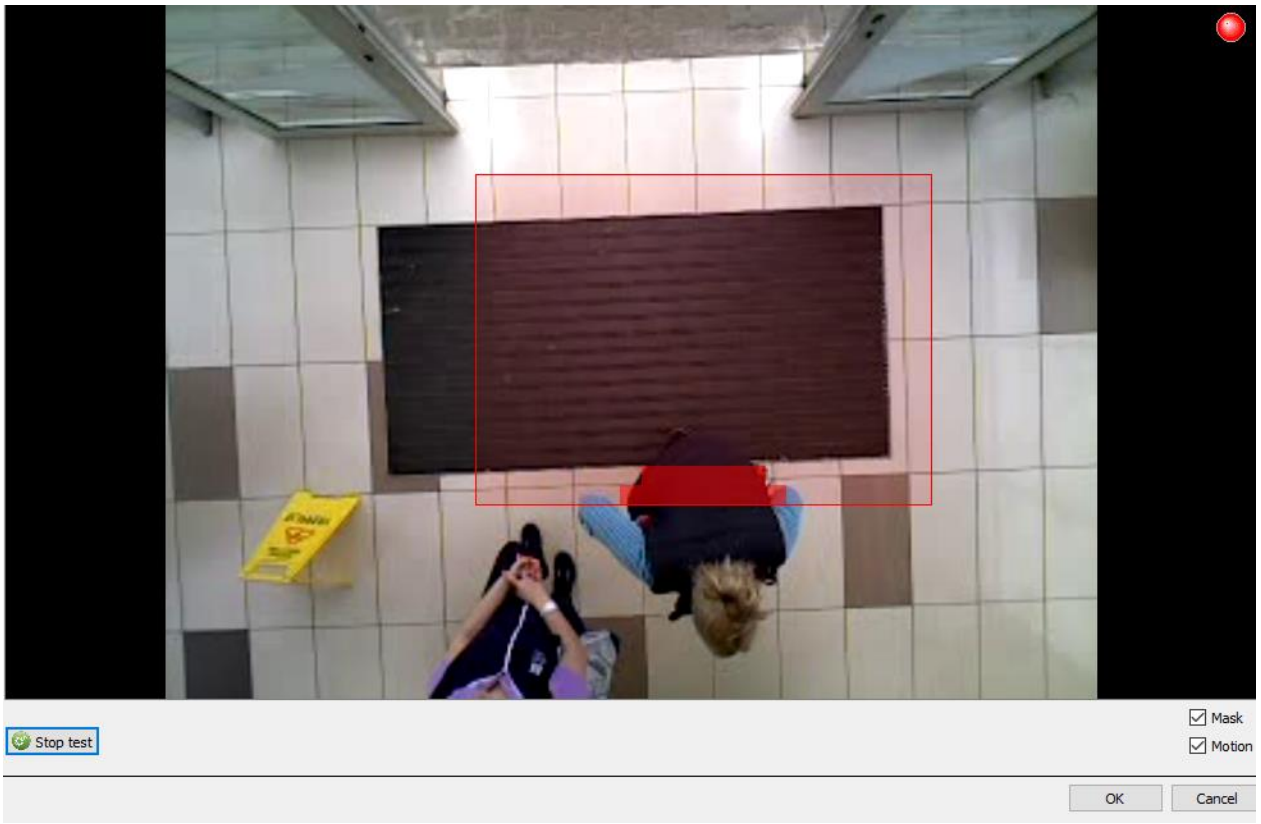
To add a mask, click **Add mask**.



Only motion in the masked area will trigger recording.

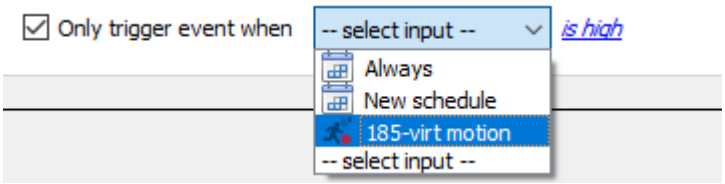
4.8.2.5 Test Settings

Click **Test settings** to display the mask, motion, and when it is triggered.



4.8.3 Events

Motion input can be used as an event trigger.



4.9 Scheduled Archives

4.9.1 Archive Video Manually

For instructions on the process of archiving video manually, please consult the ***CathexisVision Operator's Manual***.

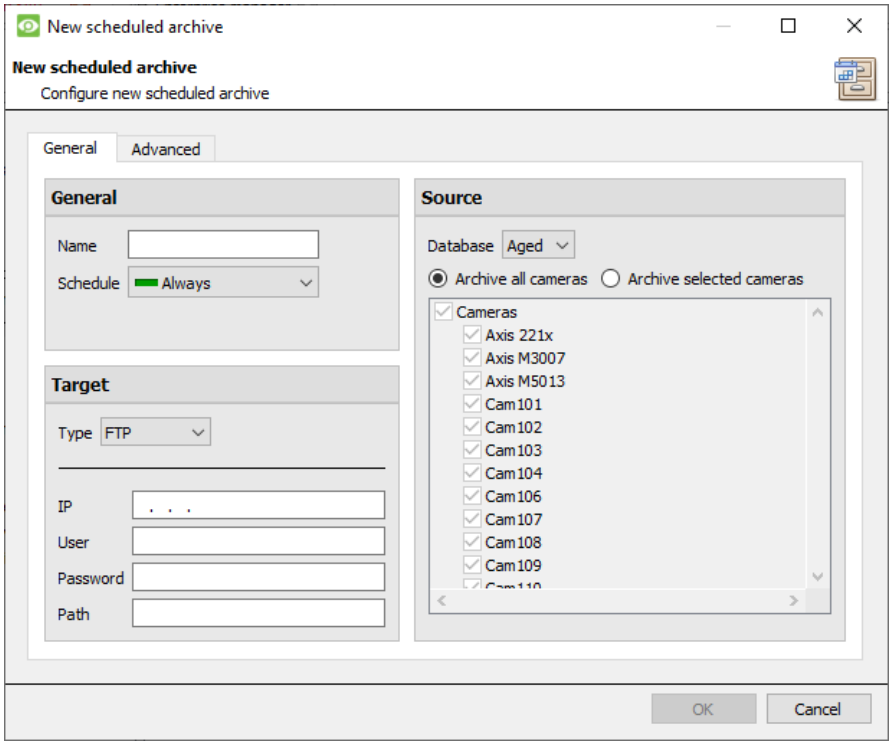
4.9.2 Description

Archiving is a facility to enable copying and selecting recordings (from specific databases) to an archiving media, such as a Local disk, or an FTP server. Unlike normal recordings, archived recordings retain their authenticity, and can be verified as authentic (unaltered) on replay, making them suitable for use in courts of law.

The Scheduled Archive feature allows periodically archiving selected cameras, from selected databases, on a schedule. This is useful for a number of reasons. An important function is to create an archive of important cameras. As databases fill up, they start to write over the oldest recordings. To keep some camera's recordings for extended periods of time, it is important to archive them.

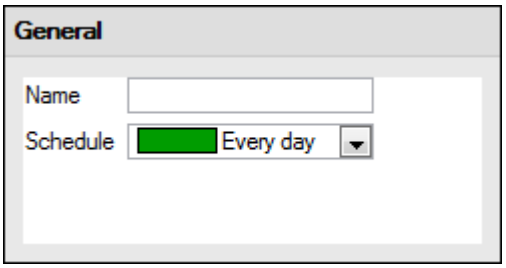
Note: When this is first enabled, it will start from the beginning of the database, subsequent archives will pick up from where it left off the previous time.

4.9.3 New Scheduled Archive Window



4.9.3.1 General Tab

4.9.3.1.1 General Panel

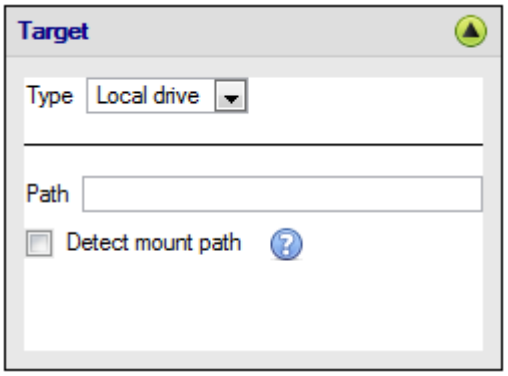


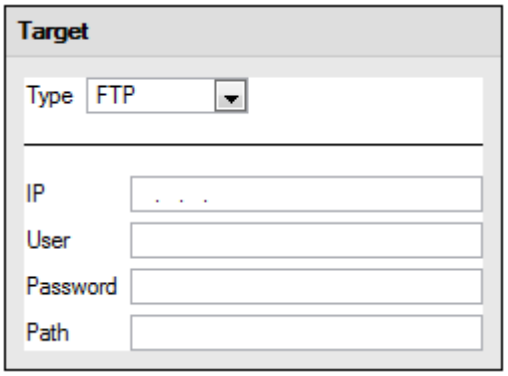
General settings consist of assigning this archive a name, and a schedule.

Note: the schedules available are the same schedules set under **Configure Servers / Schedules**.

4.9.3.1.2 Target Panel

Under Target, define where the archives are going to be recorded to. Select the relevant option from the **Type** drop-down menu.



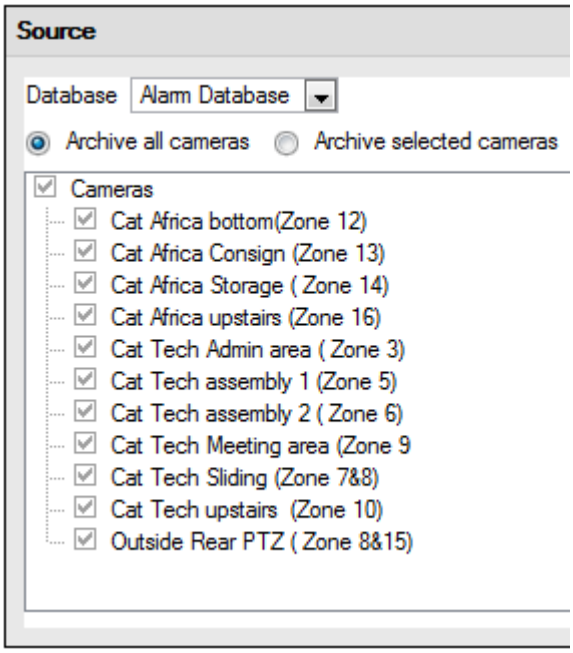


Local Drive This will write to a selected path on the local hard drive, of the recording unit.

FTP This option allows for network archiving to any accessible FTP server. This is incredibly useful, as FTP servers may be accessed across LANs, and WANs.

4.9.3.1.3 Source

Source: defines which cameras are to be archived, and the database from which to draw the cameras' recordings.

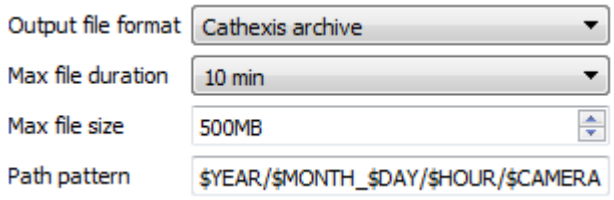


Database
There may be multiple databases for groups of cameras. Or send camera recordings from different triggers, to different databases (for example, VMD input, Access Control, Alarm Panels).

The database drop-down menu will provide a list of all available databases.

Cameras
Check the Archive all Cameras option, or Archive Selected Cameras.

4.9.3.2 Advanced Tab



Note: By default, these settings are set to maximum.

Output File Format. The only available format is the Cathexis archive format.
Max File Duration Is the maximum time length of an individual archive file.
Max File Size Is the maximum size on an individual archive file.
Path Pattern is the file naming convention used for the Archive files. There are written instructions in this window, in the GUI, detailing how to modify the Path Pattern.

4.10 Events

One of the most powerful features of the **CathexisVision** suite is the flexibility of the events system. These events can take multiple inputs, and perform multiple actions based on them. A common example of such an event, would be triggering the recording of a camera stream, based on input from Video Motion Detection.

See below for information on creating the Cathexis Events metadatabase, before proceeding with creating CathexisVision system events.

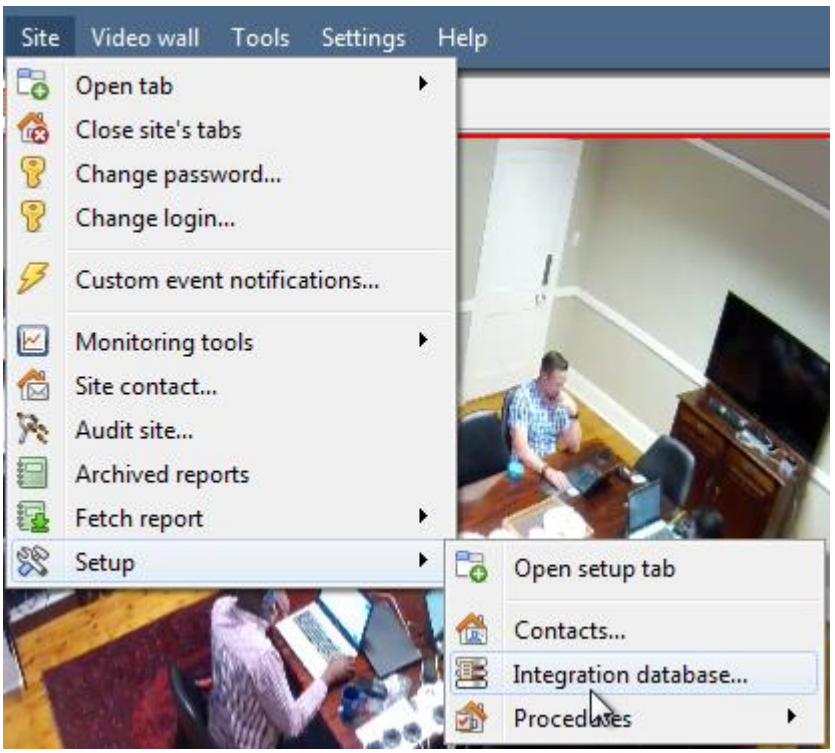
4.10.1 CathexisVision Events Metadatabase

A Cathexis Events metadatabase, once created by the user, will automatically store all site events generated by the CathexisVision system – even if there is no recording associated with the event. No other setup is required besides simply creating the metadatabase.

It might be useful to create this metadatabase before proceeding with creating the events.

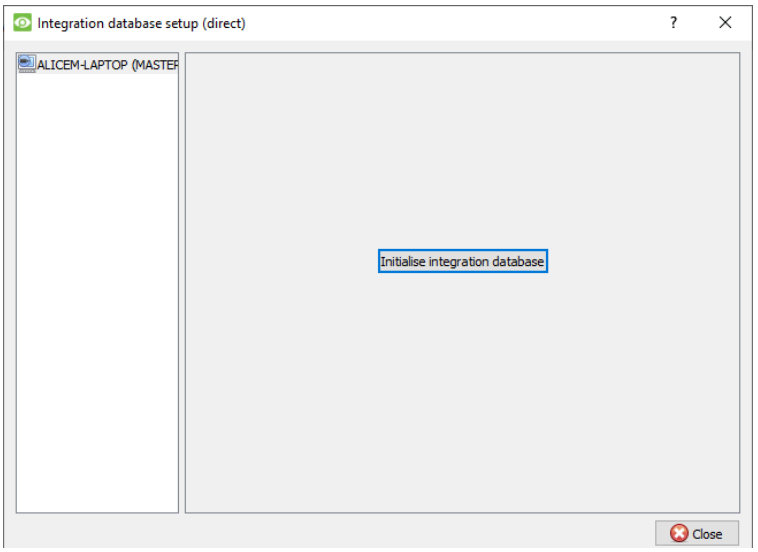
4.10.1.1 Open Integration Database Window

Site Menu / Setup / Integration Database…

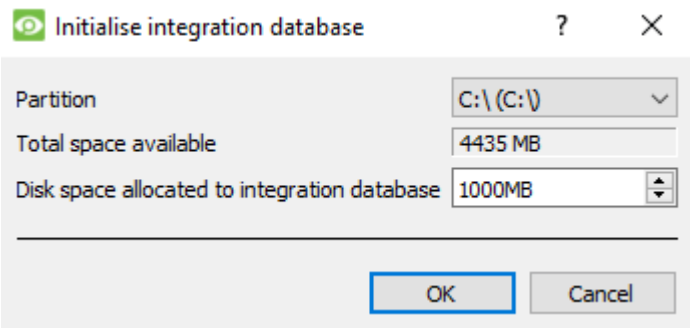


4.10.1.1.1 Initialise Integration Database

If integrations are not yet added to the system, this may be the first time initialising the integration database, also called the metadatabase.



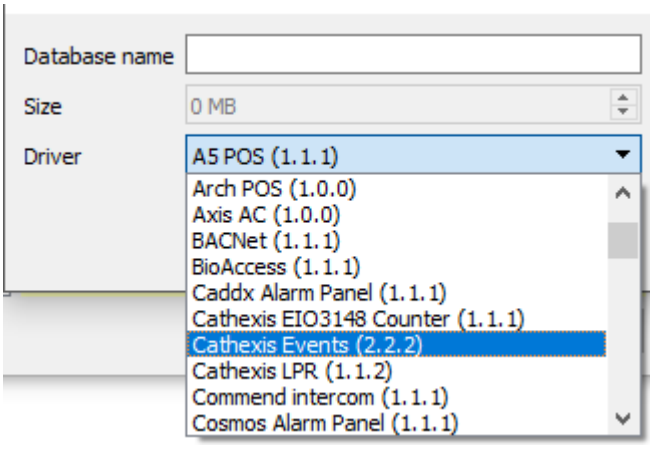
Click to **Initialise integration database**.



Then, select the size and partition of the database.

4.10.1.2 Create Cathexis Events Metadatabase

Once the integration database has been initialised (if required), create the events metadatabase by right-clicking in the white space and selecting **New**.



Give the metadatabase a **descriptive name**. A good name would be “CathexisVision Events”.

Select the **size** of the database.

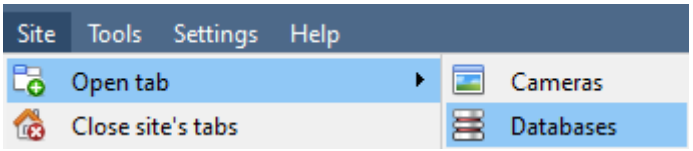
Select the **Cathexis Events** driver from the list.

Click **OK** when done.

4.10.1.3 Navigate to Database Tab

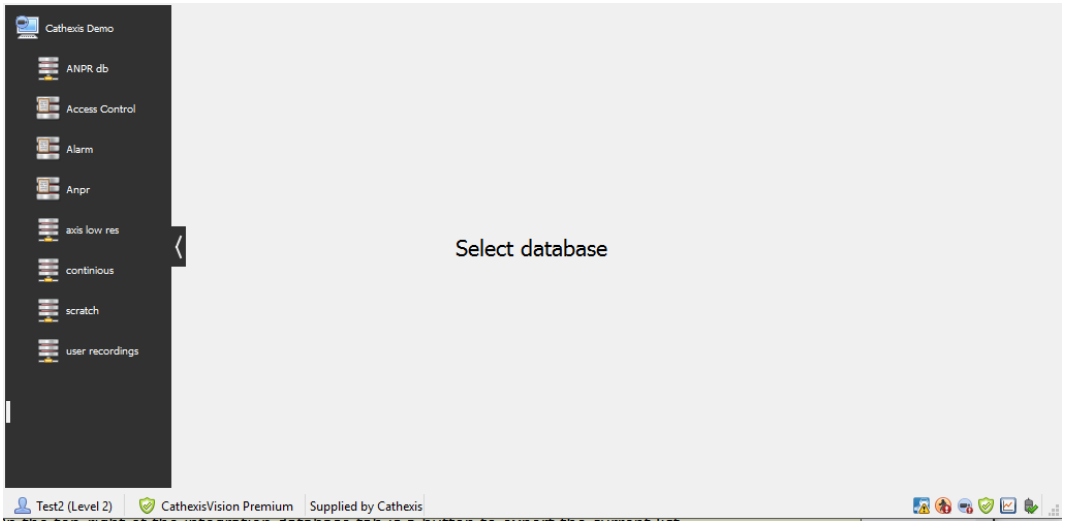
In the database tab, both the general databases and the integration/metadatabases may be viewed.

Note: Only users with correct access rights will be able to view database entries.



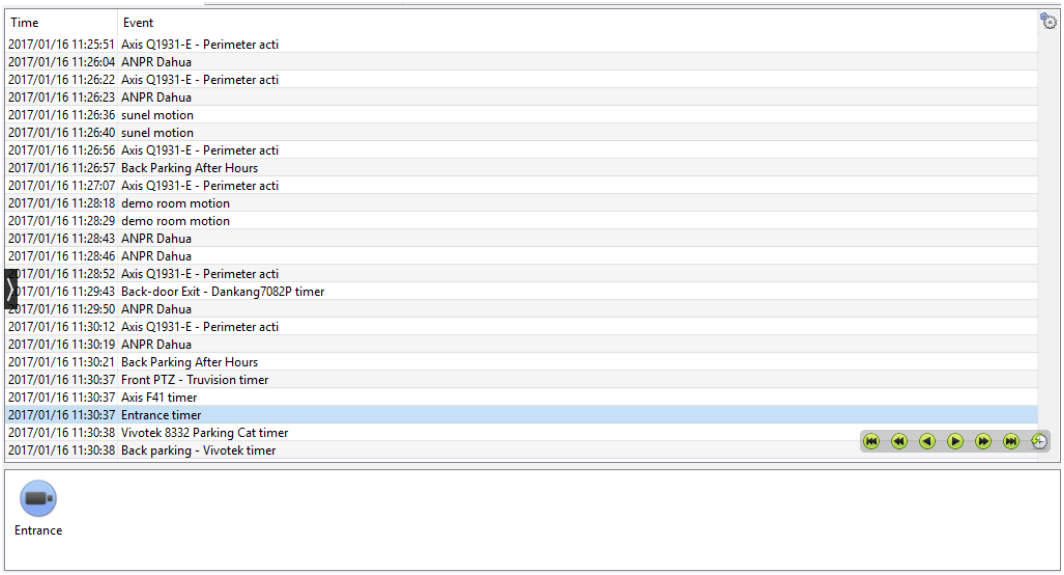
To open the CathexisVision Database Tab select **Site / Open Tab / Databases**

Once the tab is open, select a database to view.

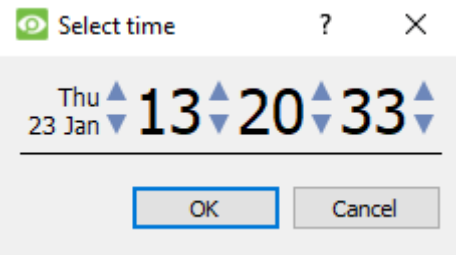


4.10.1.4 General Database

Select one of the general databases to view entries. If a Cathexis Events Database has been created, it will have the same interface as below.



4.10.1.5 Locate an Entry



In the Database Tab, click on the **clock icon**, located in the bottom right-hand corner.

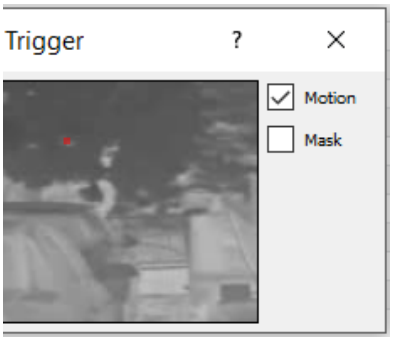
Select the date and time.

The list of database entries will have been pared down to the beginning, with the event closest to the time selected, and a few subsequent entries.

4.10.1.6 Replay an Associated Recording

CathexisVision is capable of associating video footage and other data with database entries. When reviewing associated footage there are two options. The user may review the video clip associated, or they may view the video frame at the point that the event was triggered.

4.10.1.6.1 Review Trigger Frame



To review the trigger frame, left-click on an entry.

If this icon is present in the panel below, double-click on it. This will bring up the dialogue to the left.

Motion will show where the motion occurred in the image.

Mask will show what areas of the image are covered by the algorithm which triggered the database entry.

4.10.1.6.2 Review Event Video

To review the video associated with a database entry, double-click on that entry.

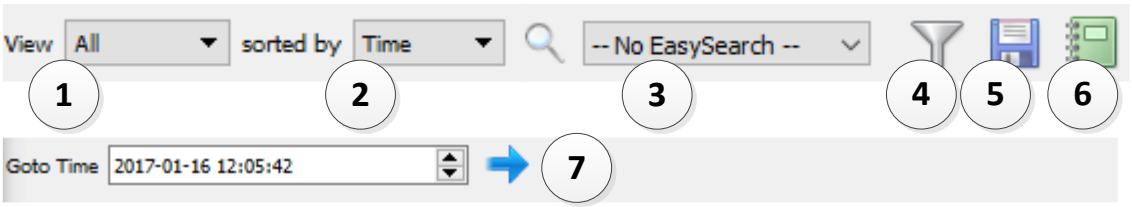
Alternatively, click on the **video icon** in the entry's details.

4.10.1.6.3 CathexisVision Controls

CathexisVision database review uses the same control schema as the timeline review used in the **Cameras Tab / Review Controls section.**

4.10.1.7 Integration / Metadatabase

Select the relevant integration/ metadatabase.



1 **View**	The user may change the way that the database is presented. Some integration databases have multiple view options.
2 **Sorted By**	Events can only be sorted by certain perameters.
3 **Easy Search**	The easy search option lets the user quickly search the database.
4 **Filter**	Filter offers a more advanced manner of sorting information in the Integration Database table. Once the filters dialogue is open, the following filter options are available: 1. To **enable** filters check this box: Enable filters 2. To **add** a new filter click on . 3. To **delete** an added filter click on . It is possible to filter the same perameters more than once. To change a filter, click on the blue hyperlinked text. Timestamp For example, click on **Timestamp.** A list of options will appear. Change the filter from Timestamp to any of the other available options. **Note**: 1. Multiple filters may be run simultaneously. 2. The filter icon will change when filters are active.
5 **Export**	Generate metadatabase reports in PDF or CSV format. See below.
6 **Scheduled Reports**	Click this to create and manage scheduled metadatabase reports. See below.
7 **Go to Time**	This navigates to a point in time, down to the second. To navigate to a timestamp, set the time using the time and date boxes. Then click on the **arrow icon**.

4.10.1.8 Scheduled Metadatabase Reports

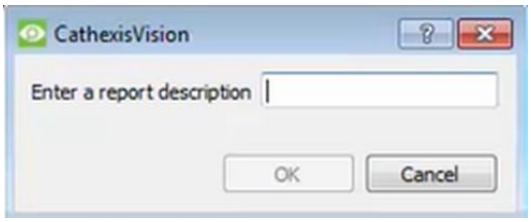
Click on this icon to open the schedule report window.

All created reports will be listed here.

First, click **Add** to create a report. Then **edit** to define the reporting schedule. See below for more detail.

To create, edit, or delete a report, select the entry and click on the corresponding button.

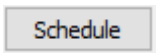
4.10.1.8.1 New Scheduled Report



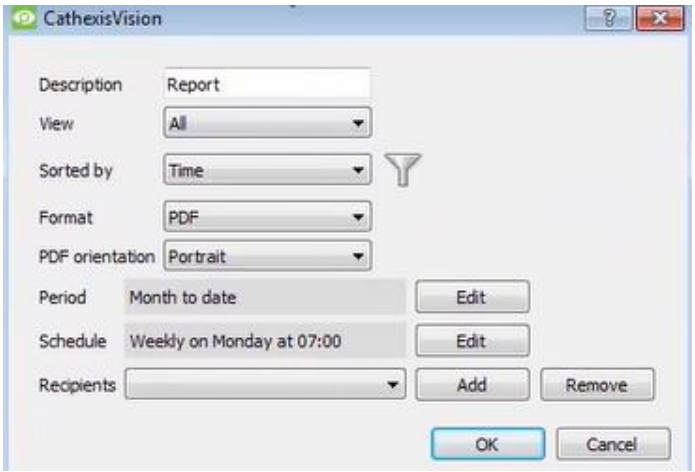
Click **Add**.

Give the report a description. Click **OK** when done.

Once the new report is listed with the other reports, select it for editing to define the reporting schedule.



Right-click the entry, and select schedule.
OR: select the entry and click the schedule button at the bottom of the screen.



Edit the **description** if needed.

Edit **Viewing** options.

Select the **Sorted by** option.

Select the **Format**.

Select the **orientation** of the Format.

Select the **period** to be reported on.

Define the **Schedule** for the report.

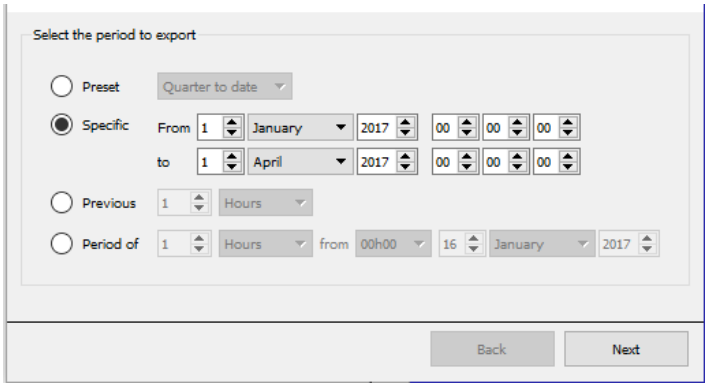
Add/remove recipients to whom reports will be sent:

Add recipient: Click **Add** and enter the email address of the recipient. Multiple recipients may be added. All will receive emails.

Remove recipient: Select the recipient from the dropdown menu and click **Remove**.

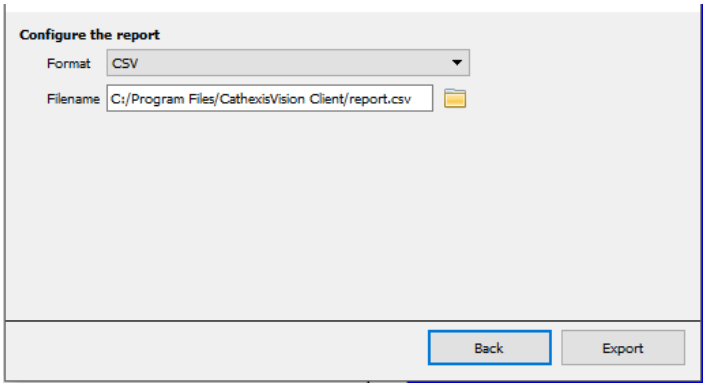
4.10.1.8.2 Generate Metadatabase Reports

Click this icon to open the Export window.



Select the **Period** to export, and enter the required details.

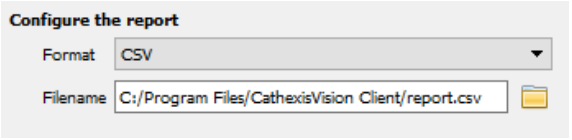
Click **Next**.



Select the **Format** in which to export the report: either CSV or PDF.

See below for the two options.

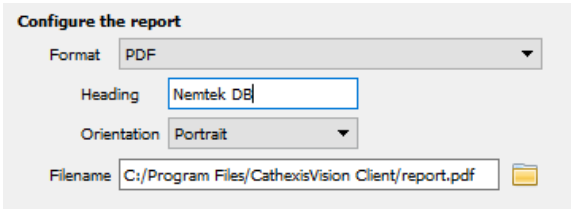
Export CSV



Select CSV **Format**.

Edit the **Filename** by either entering it straight into text field (replacing **report.csv)**, or click the **folder icon** to choose a new save folder and filename.

Export PDF



Select PDF **Format**.

Give the PDF a **Heading**.

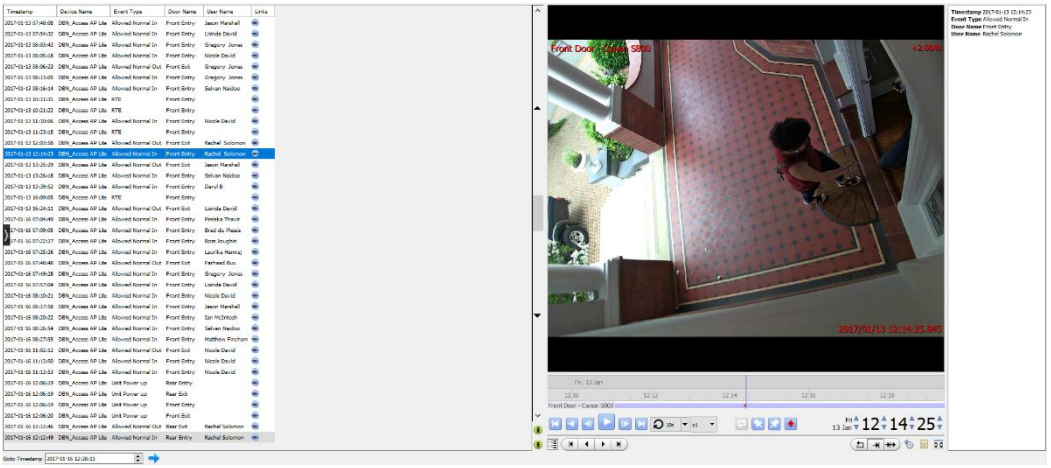
Select the **Orientation** of the PDF: either Landscape or Portrait.

To edit the **Filename**, either enter it straight into text field (replacing **report.csv)**, or click the **folder icon** to choose a new save folder and filename.

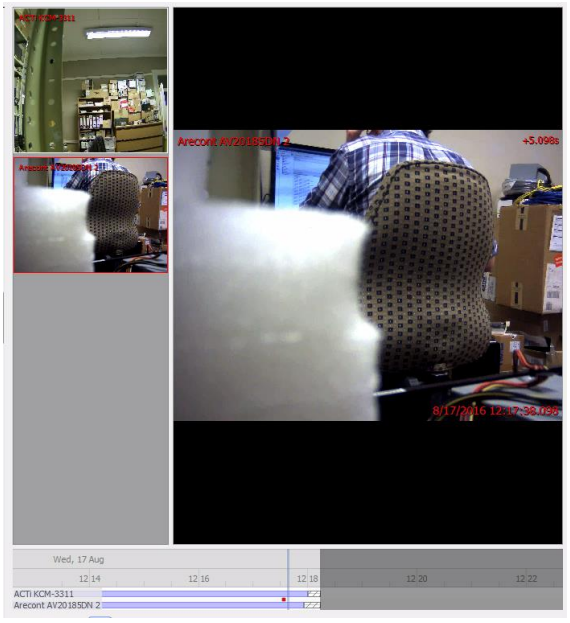
4.10.1.9 Viewing an Entry's Associated Recording

Integrations use the new video option, where the video player is embedded in the database view. This player uses the same timeline features as the CathexisVision Cameras Tab.

To view an associated recording, simply left-click on a database entry which has the **recorder icon** in the **Links** column. Then click **play** in the video player.



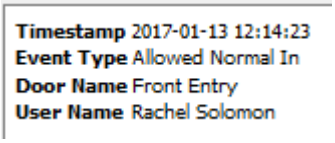
4.10.1.10 Reviewing Multiple Cameras



If multiple cameras were added to the recorded object during the integration setup, these are displayed on the left of the video player screen as thumbnails.

Select a camera thumbnail to review it.

4.10.1.11 Device Event Metadata



When an integration database entry is selected, its event information will be displayed on the right of the video player.

4.10.1.12 Archive Selected Database Recordings

Archiving video from the database follows the same process described above, in the **Archiving** section of this document. However, not that when in the database tab, the archive button icon changes: .

Note: When archiving a video feed that has **Privacy Zones** enabled, the privacy zones will appear/not appear in the archived video, depending on whether they are enabled in the feed at the time of archiving. (They may be enabled/disabled by right-clicking on the feed of video being reviewed via the database tab).

4.10.2 CathexisVision System Events Window

Navigate to the events window via the Setup Tab. The path to follow is **Site / Setup** / **Configure Servers** / **Events**.

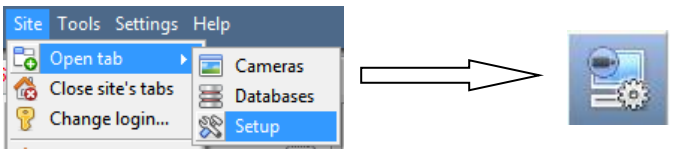
4.10.2.1 Important Note

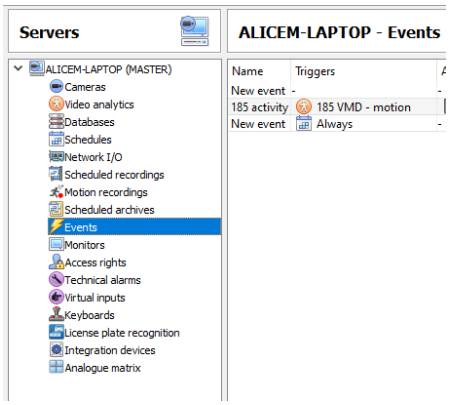
Note: Events depend on triggers that are predefined. This means that before getting to the events window, these inputs and outputs should be ready. An example [which will be discussed later] is recording based on motion. In order to set up an event based on motion detection, several things are needed:

1. A camera that has been successfully added to the system [to provide the images].
2. A Video Motion Detection algorithm needs to have been set up [to trigger the event].
3. A database needs to be set up [as a point where the action of recording takes place].

It is easy to forget this, and head straight to the Events window to create an event, before there are all the resources to do so.

4.10.2.2 Site / Open Tab / Setup / Configure Servers





Select **Events** from the Servers menu.

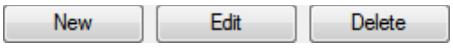
4.10.3 New Events Window Interface

Events can be complex, with multiple trigger and actions. However, all events have the same three core aspects.

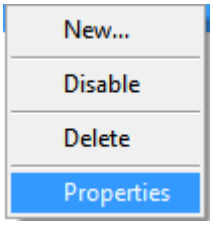
General Settings	Name, Schedule
Trigger	Initiates the event
Actions	The action taken by **CathexisVision** (as a result of the trigger).

The general events window interface is discussed below, as well as the four individual sections to edit when creating an event (General Settings, Triggers, Actions, and Resources). These are visible as tabs in the above screen capture of the Events Window.

4.10.3.1 General Interface

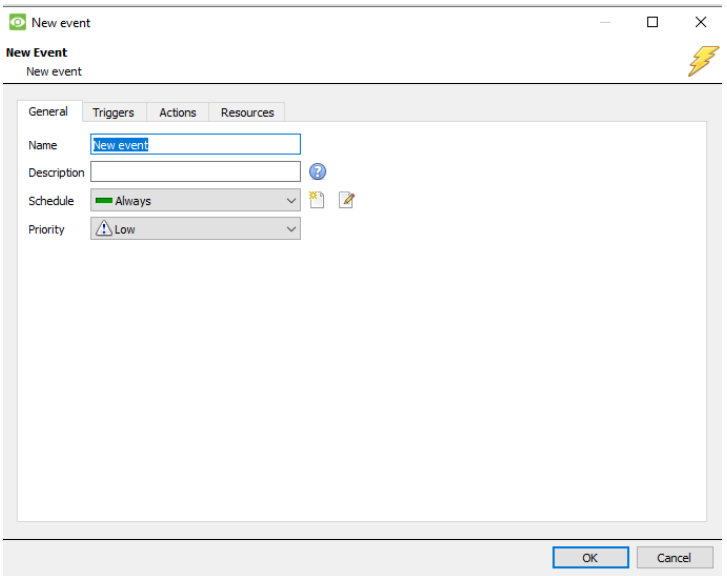


The Events panel will appear on the right. To add, edit, or remove Events in the list, use on of the buttons at the bottom of the panel.

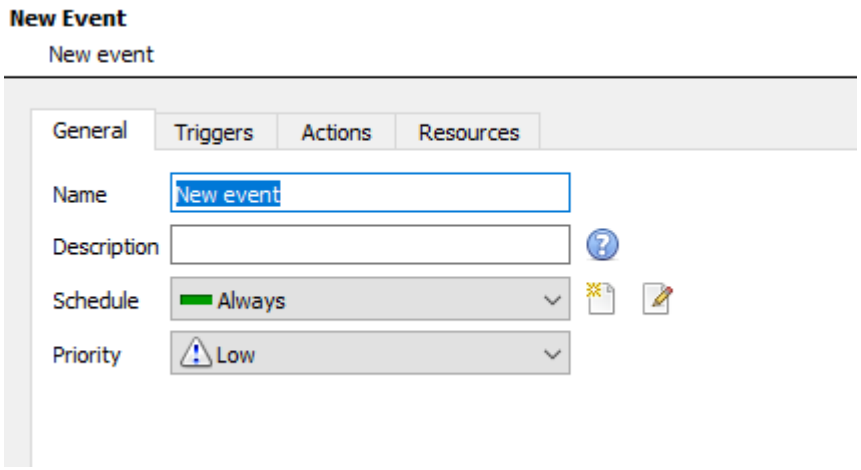


To enter the events window, either click on **New** or **Edit**, as described above. Or use the right-click menu in the Events Panel.
Clicking on white space will give the option to create a new Event. Right-clicking on an existing event will provide a drop-down menu, with the options shown in the image on the left.

The Events Addition window:

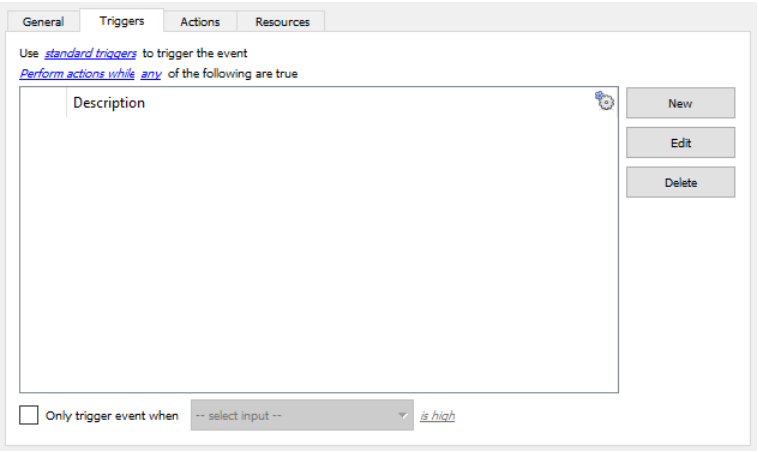


4.10.4 General Settings Tab



Name	This is a descriptive name given to the event, to make it identifiable later on.
Description	This is the name the event is given when databased, or sent as an alarm. If this field is left empty, the Event Name is used. Clicking on the **question mark icon** will provide a list of available description variables. **Note**: 1. The options available here will change, depending on the triggers chosen in the Triggers Tab, so set this parameter **after** triggers are set. 2. The format for adding the variable is: Descriptive_Name: $Variable_Name. 3. Add multiple variables.
Schedule	This will define the times during which the Event will be active
Priority	This relates to the alarm that will be set under **Call Base Station** (this will be discussed below).

4.10.5 Triggers Tab



As discussed above, a trigger is what initiates an event. There are three types of triggers:

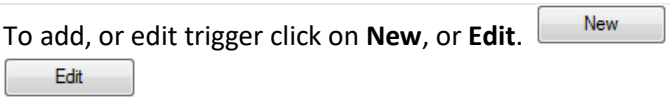
1. Standard triggers
2. Trigger templates
3. Integrated device triggers

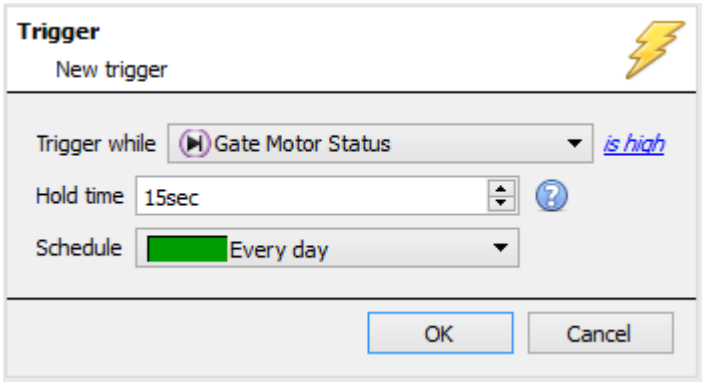
Choose between these options by clicking on the blue hyperlinked text.

4.10.5.1 Standard Triggers

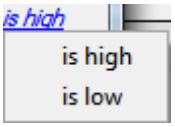
Standard triggers come in the form of **Video Motion Detection** triggers, **Relay I/Os**, **Schedules**, and **Virtual Inputs**.

To add, or edit trigger click on **New**, or **Edit**.





Trigger While is the drop-down menu from which the relevant triggers are selected.



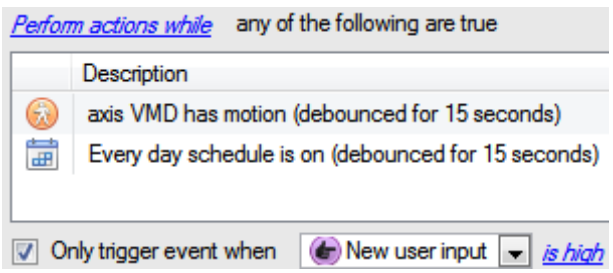
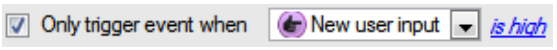
The hyperlink to the right of the trigger will give all the state options of this trigger. Click on it to access its options.

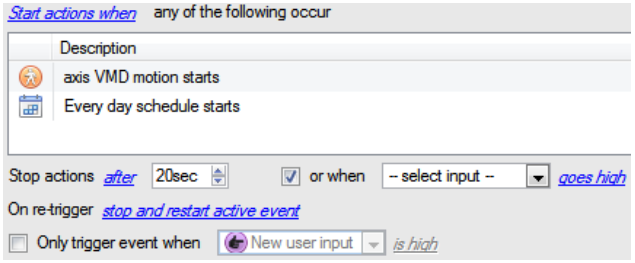
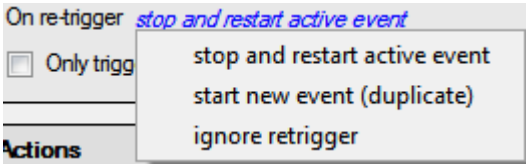
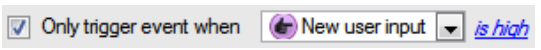
Hold Time will extend the event for this duration after the trigger has terminated.

Schedule defines when this specific Trigger is active within this specific Event.

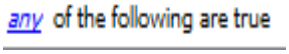
4.10.5.1.1 When and While

Standard Triggers can either trigger ***when*** or ***while*** a specific variable is true. ***When*** events are more complex, as it is necessary to specify when the event will end; ***While*** events are simpler because they automatically end when the trigger variable ends.

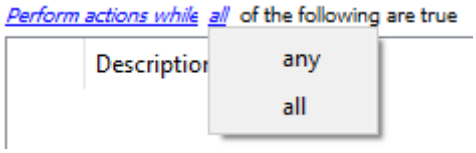
Perform Actions While	
Perform actions while is a simpler trigger setting. Where an action will be performed while certain triggers are active. 	The user can set an absolute parameter, so the event will not trigger unless this parameter is true; even if all the other event triggers have been set off.  This also comes with multiple input options, which depends only on how many triggers have been set up.

Start Actions When	
Start actions when A user can define multiple conditions that must be met for an event to trigger. This is useful if the user does not want an event to end when the initial trigger for that event changes state again. 	Stop Actions After If *Stop Actions After* are selected, choose to stop an event after a certain amount of time. Also check the *or When* checkbox. This defines a further trigger that may stop the event before the timer has run down. Stop Actions When If a timer is not desired, but the user still wants an input that will terminate the event then select *Stop Actions When* On Retrigger If one of the event's triggers is set off, while an event is already occurring, there are three options.  Only Trigger an Event When This defines an absolute parameter, without this trigger the event will not occur. 

4.10.5.1.2 Any and All



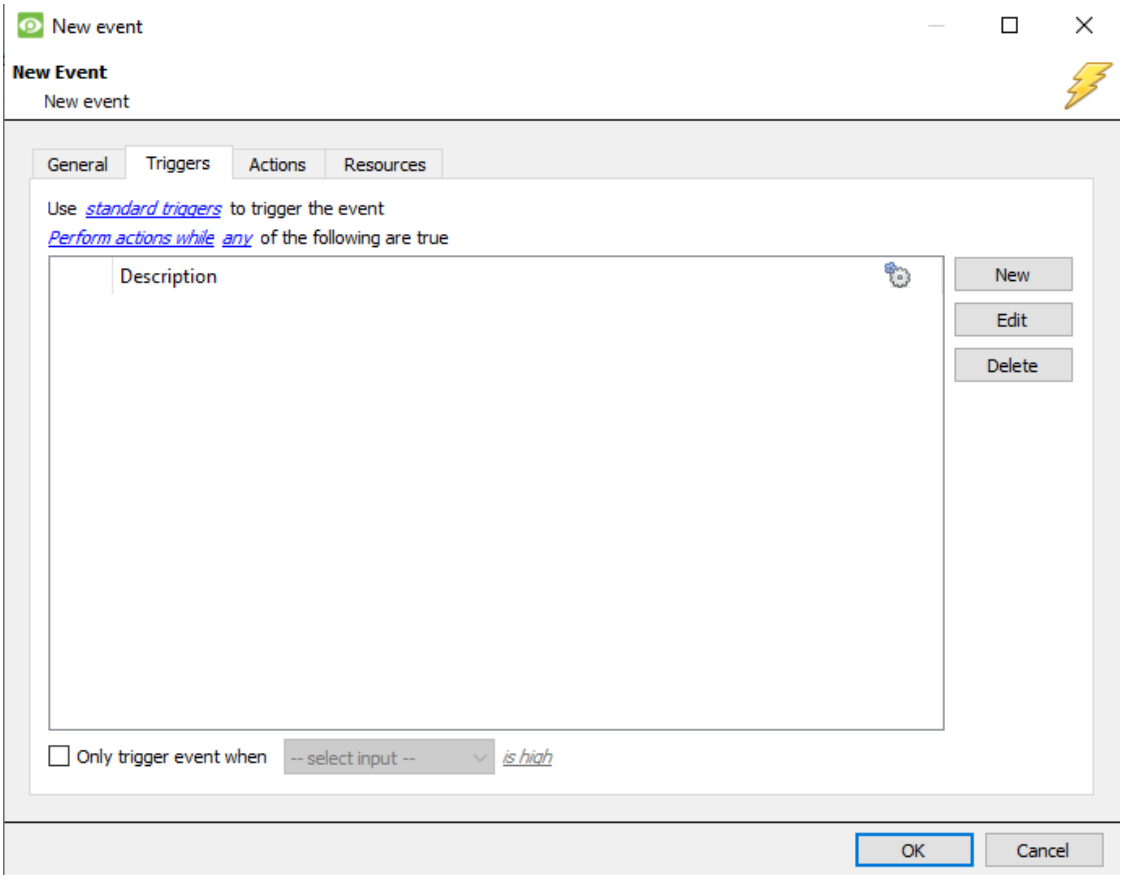
Clicking on the blue hyperlink allows the choice between ***any*** and ***all***.

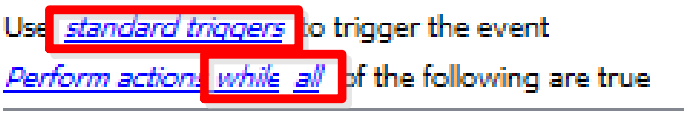


This determines whether an event will be triggered if **any** of the selected constraints are triggered (i.e., only 1 is required to trigger the event), or if **all** the selected constraints are triggered (i.e., all constraints must be triggered in order to trigger the event).

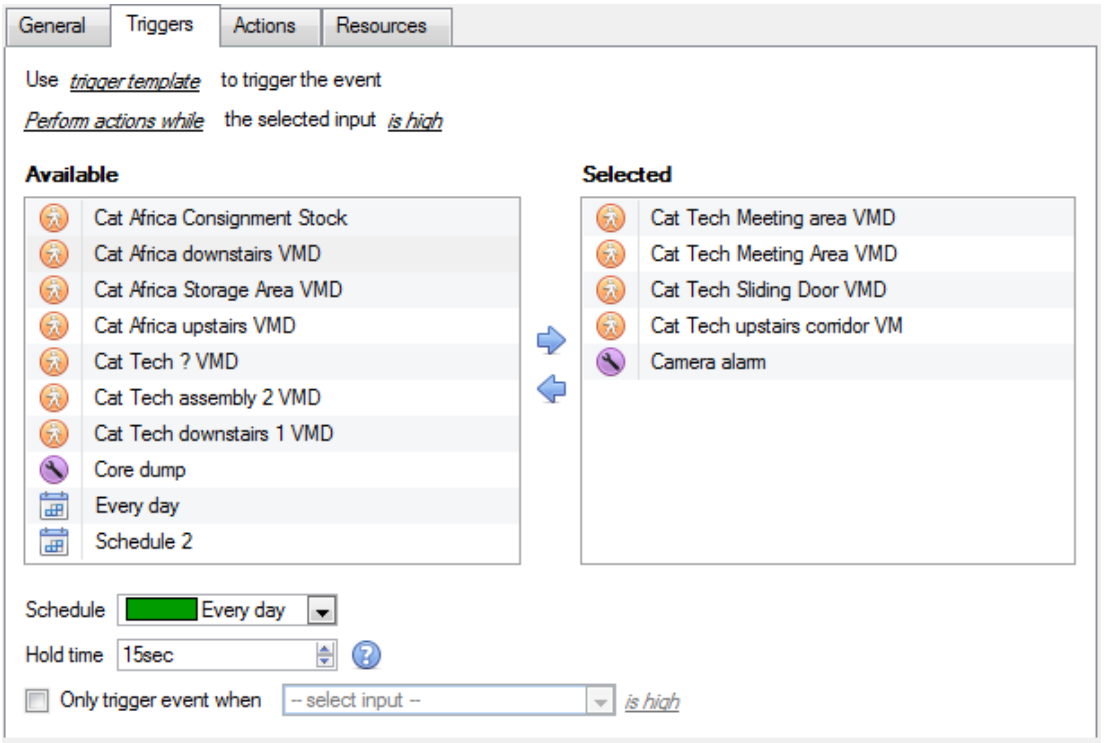
4.10.5.1.3 Filter Period

Set a filter period to only trigger an event when inputs are set for a certain time. This means that triggers which last for a shorter period of time than the filter period has been set to, will be rejected. Filter period only applies when certain parameters are set, see the image below for these.



1	Set the event to use **Standard triggers**. Set the event to Perform actions **while all** of the following are true.	
2	Set the filter period. Click the **question mark icon** for a description of the filter period.	

4.10.5.2 Trigger Template



A trigger template allows adding multiple triggers simultaneously to a single event. All **available** triggers will be displayed in the left-hand column, and all triggers that will be used in the event in the right-hand column.

To move triggers back and forth, select the desired triggers and click on the **arrow icon** that represents the direction to send the trigger.

Note: there are two important things to remember when using a trigger template:

1. This is useful in relation to the **Record Trigger Cameras** option (dealt with in the Actions section).
2. Set the database entry for this event to either take on the name of the event every time, or the name of the trigger. (This is defined above.)

4.10.5.3 Integrated Device Triggers

Note: This is general information on setting up an event with an integrated device. Each integration gets its own document, as these options change from integration to integration.

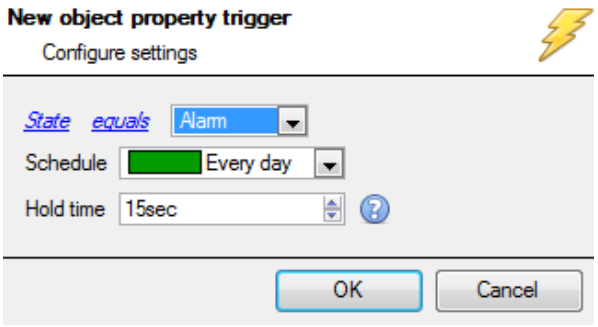
4.10.5.3.1 Select a Device

Integrated devices are also viable Event Triggers. This means that any integrated device may be used to trigger a **CathexisVision** Event. Select a specific integrated device. In the image to the left, there is an alarm panel, which can be used to trigger an event.

4.10.5.3.2 Select a Device Parameter

Clicking on this will provide a full list of the integrated device's own objects to use as trigger bases.

Once selected, one may add a new trigger by clicking on **New**.



Clicking new will give all the options that the Object provides as triggers.

For example:

If selecting *State equals* **Alarm,** and **any partition** above:

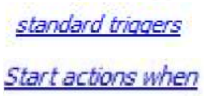
The event will trigger when any of the Zones alarm.

4.10.5.4 Triggering Events with Camera Tamper

If camera tamper detection is added to one/multiple cameras, one may want to create events which will be triggered by a camera tamper. **Note:** Tamper detection must be added to cameras in order to trigger events using tamper.

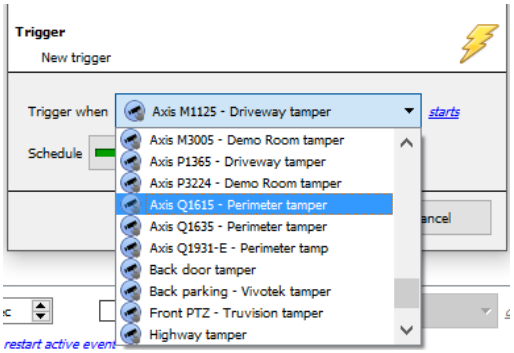
4.10.5.4.1 Trigger Event from a Single Camera Tamper

To trigger events using a tamper from a single camera, create a standard CathexisVision event which starts when the tamper trigger starts, and stops 20 second after the tamper trigger stops.



To do this, use **Standard triggers** and **Start actions when.**
Then add at least one trigger to the event.

Set Camera Tamper to Trigger an Event



From the drop-down menu, **select the camera** that, if tampered with, will trigger an event.

Select the **schedule** during which the tamper will trigger an event.

Hint: It is useful to create a tamper schedule so that false tampers will not trigger an event; such as routine maintenance checks, etc.

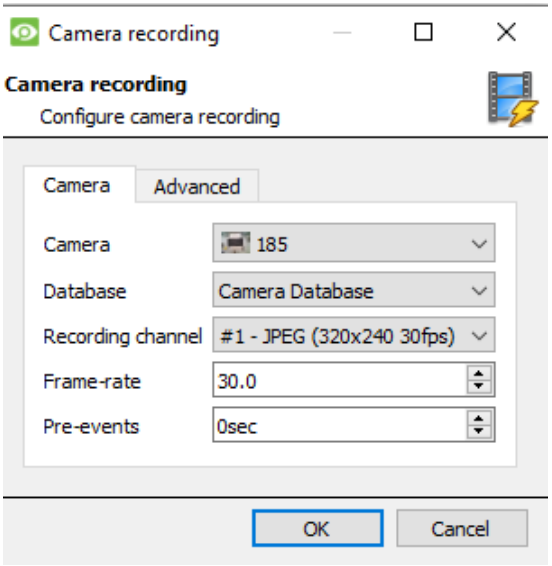
Click **OK**.

Stop Event after 20 Seconds

Once back in the New Event window, set the event to stop after 20 seconds.

Record Camera

To record any tamper events, in the **Actions** tab, select **Record Camera**.



Select the tamper camera to record.

Select the database to which tamper recordings will be archived.
Hint: Create a specific database for tamper recordings if other triggered recordings are set up.

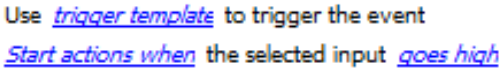
Select the Recording Channel.

Select the frame-rate.

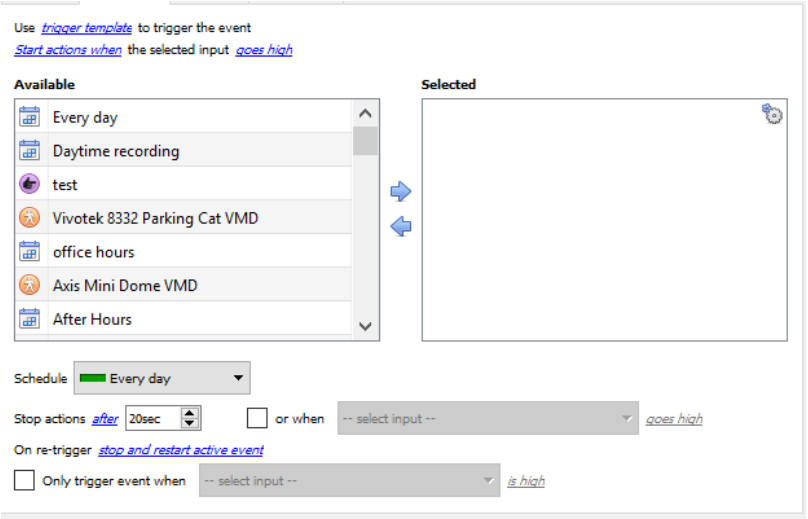
Set the pre-event to 40 seconds in order to capture events leading up to the tamper.

4.10.5.4.2 Trigger Event from Multiple Camera Tampers

To trigger an event using camera tamper from multiple cameras, create an event using the following parameters:



Select Camera Tampers to Trigger Event

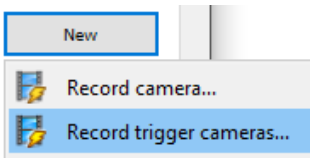


From the list of available cameras, select all **cameras** that, when tampered with, will trigger the event. Then click:

Set the **Schedule**.

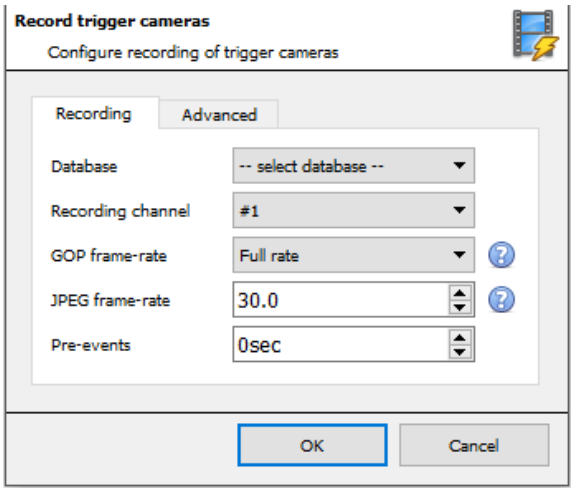
Set the event to stop after 20 seconds.

Record Trigger Camera



In the Action tab, click New and select Record trigger cameras to record the cameras, which were selected for the trigger template in Step 1., above.

Note: This option will only appear once trigger cameras have been added to the template.



In the Record trigger cameras window that opens, select the **Database** to which tamper recordings will be archived.

Hint: Create a specific database for tamper recordings if other triggered recordings are set up.

Select the Recording Channel.

Select the GOP frame-rate.

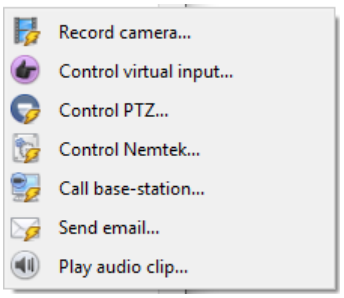
Select the JPEG frame-rate.

Set the pre-event to 40 seconds in order to capture events leading up to the tamper.

Note:

1. Keep the pre-event recording size small. For example, do not select 2MP JPEG images at 25fps.
2. Set a recording on the analytics channel to keep the database footprint to a minimum.

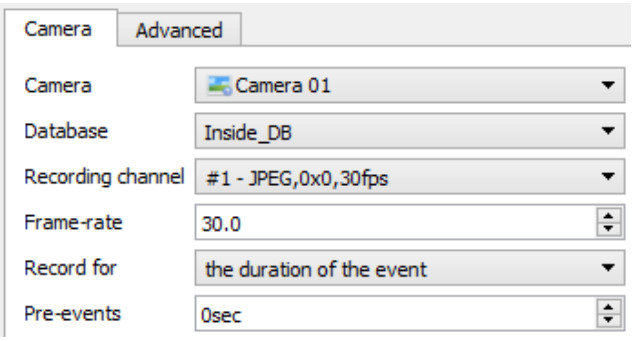
4.10.6 Actions Tab

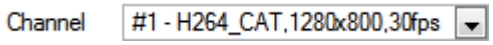
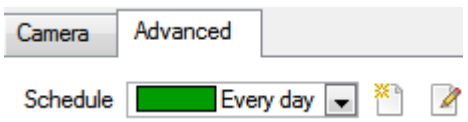


To add an action, click on the **New** button, to edit an action click on **Edit**.

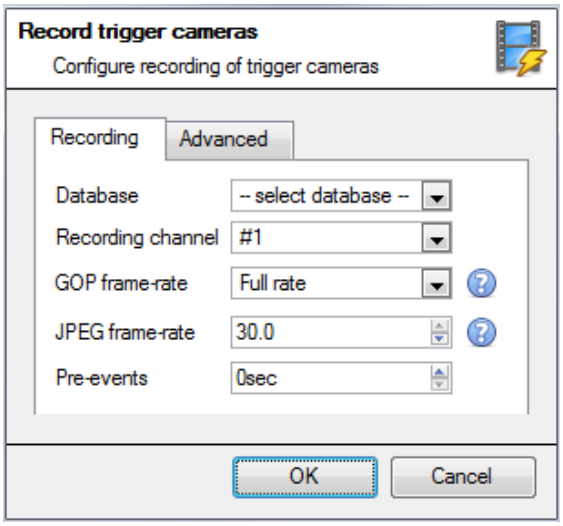
At present, the actions seen to the left are the available actions. They will be dealt with below.

4.10.6.1 Record Camera



	Select a preconfigured database on which to record the camera. One can select multiple databases to record the same event to, on multiple servers.
	Select a preconfigured camera to record to the specified database. The drop-down menu will contain all cameras on the system.
	If there is more than one video feed coming from the camera (perhaps one for recording and one for Video Analytics), then select the relevant feed for recording.
	Select the required frame rate for the video to be recorded at.
	Setting a pre-events timeframe will set the recording to start a few seconds before the event actually triggered. **Note:** It is necessary to have set up pre-events in the camera addition process, under the pre-events tab.
	The **Advanced Tab**, when setting up recording, offers the option to schedule when this recording setup should be active **within** this event. This schedule does not impact on anything beyond this specific setting.

4.10.6.2 Record Trigger Cameras



If choosing integrated device or a trigger template, in the Triggers Tab, select the option to record **trigger cameras**. This means that the action will record any of the cameras associated with triggers in the triggers tab.

Database is the database the cameras will record to.

Recording Channel is the default channel that will be recorded from the camera. Make sure that all selected trigger cameras have the same channel set for recording.

GOP Frame-rate is the frame rate to record GOP based video compression streams, such as MPEG4, or H.264.

JPEG frame-rate is the frame rate to record single frame-based compression streams, such as MJPEG.

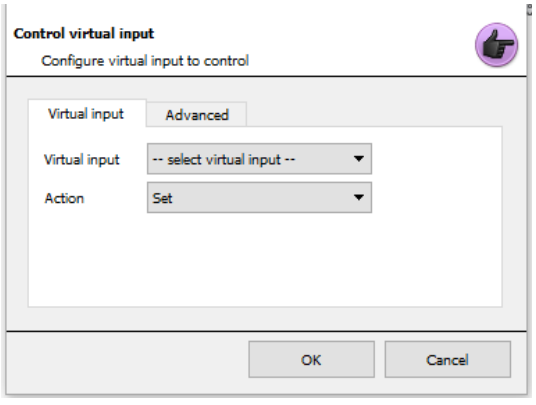
Pre-events are the number of seconds of footage that are recorded from before the event was triggered.

Tip: by adding a second Record Database action, and assigning a second database, this event is effectively cloned to another database. This is useful to clone an event to, for example, a Network Attached Storage.

4.10.6.3 Control Virtual Input

If virtual inputs have been configured, one may set an event action to control the input. This is useful as the triggering of one event can be used to trigger another.

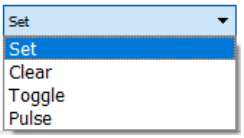
4.10.6.3.1 Virtual Input Tab



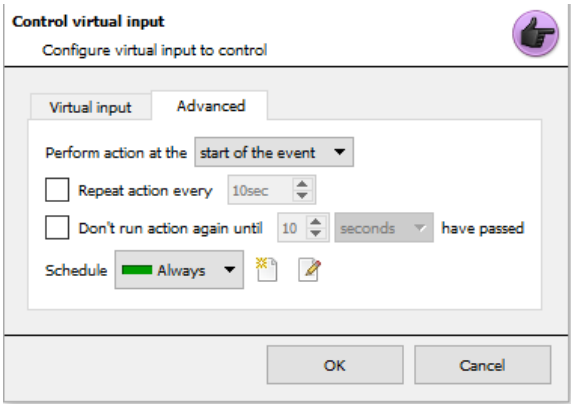
Select the Virtual input to be controlled as the event action.

Note: Virtual inputs are configured in **Setup Tab / Configure Servers / Virtual inputs.**

Select which **Action** with which to control the virtual input. Inputs may be:



4.10.6.3.2 Advanced Tab



Select whether to **Perform action at the** beginning, or the end of the event.

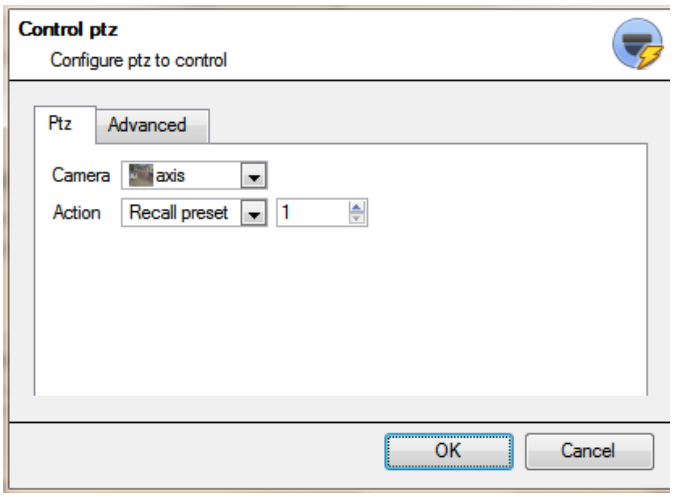
Repeat Action Every: Check this box to define how often the action occurs during an event.

Note: This action is not available under **Perform action at the end of the event.**

Don't run action again… provides the ability to define how long the software must wait after the action has run, before repeating it.

Schedule creates a schedule under which this output will be controllable by this event.

4.10.6.4 Control PTZ



Camera is the camera whose PTZ the action will control.

Action

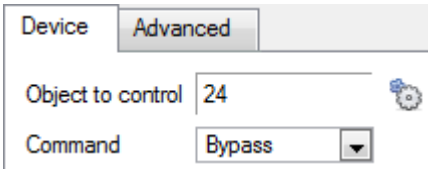
Recall preset will send the PTZ to a preconfigured position.

Run pattern will cycle through a number of preconfigured positions, that have been grouped into a **Pattern.**

Advanced Tab

The advanced options are identical to those discussed under Control Output below.

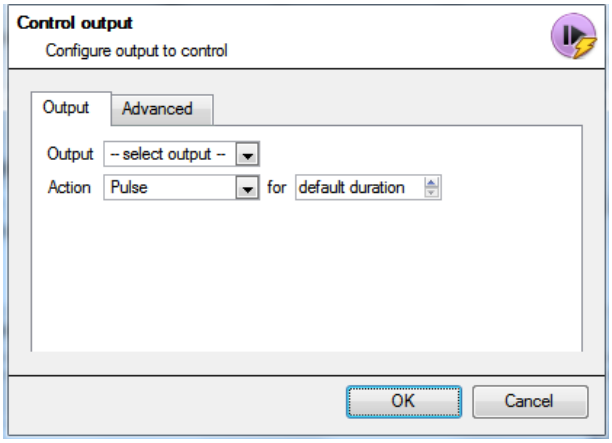
4.10.6.5 Control Integrated Device



One may take an action on an integrated device's Objects in the action of an event. The options presented will differ based on the device being controlled (e.g. set an alarm, or open a door…).

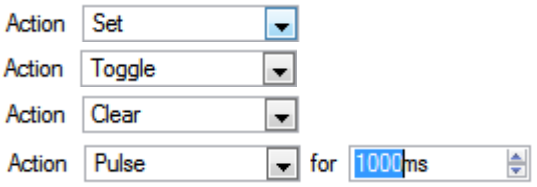
For Advance tab information, see Control Output below.

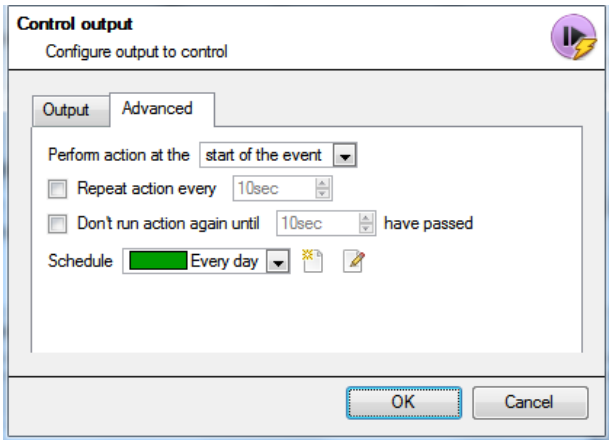
4.10.6.6 Control Output



Output will provide a list of pre-configured outputs to control as part of this action.

There are 4 **Actions** available:





There is the option to **Perform action at the** beginning, or the end of the event.

Repeat action every

Check this box to define how often the action occurs during an event.

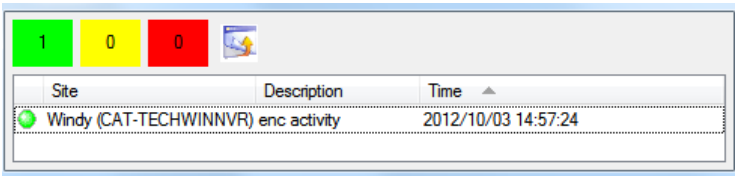
Note: This action, logically, is not available under **Perform action at the end of the event.**

Don't run action again… provides the ability to define how long the software must wait after the action has run, before repeating it.

Schedule creates a schedule under which this output will be controllable by this event.

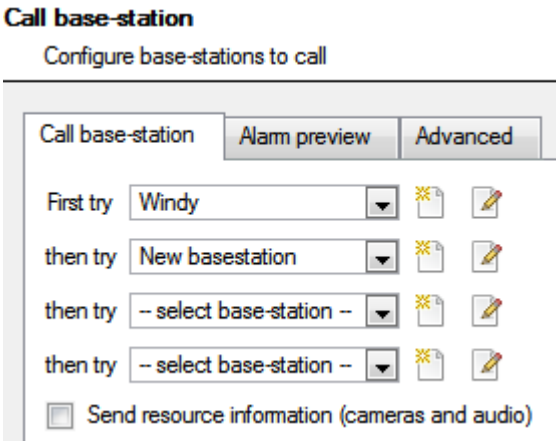
4.10.6.7 Call a Base Station

This will define which Base Station is 'called' when an event triggers. It will send an alarm pop-up box to the chosen base station:



- The three colours – Green, Yellow, and Red – indicate the priority of the alarm. They relate to low, medium, and high respectively.
- The number within the coloured block indicates how many unattended alarms of that severity the base station has received.

4.10.6.7.1 Call Base Station Tab

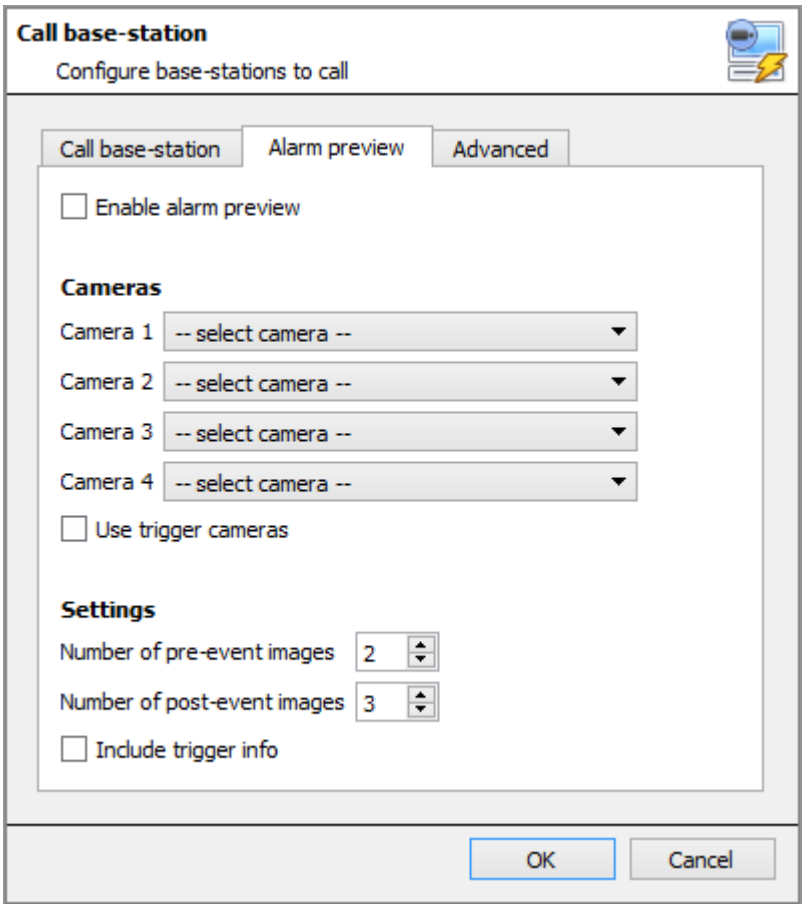


First Try: Select, from the drop-down menu, the primary base station an alarm should be sent to.

Then Try: If the connection to the first base station fails then the base station selected here will be the one that the alarm is sent to next.

Send resource information (cameras and audio): If the base station has an alarm management gateway, this will send extra information about the cameras and audio that were involved in the event.

4.10.6.7.2 Alarm Preview Tab



This applies to the Alarm Management Gateway. It will send information in the form of snapshots of the selected cameras along with the alarm.

Enable alarm preview

Checking "enable alarm preview" enables the alarm preview.

Cameras

Under Cameras, choose predefined cameras to send with the alarm preview.

Settings

Under Settings, define the number of pre-, and post-, event images to send along with the alarm.

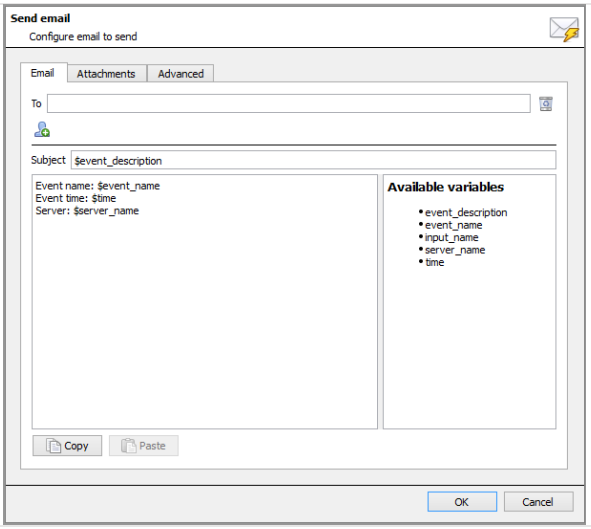
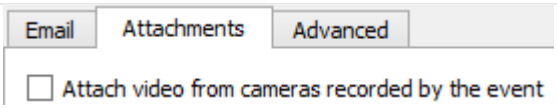
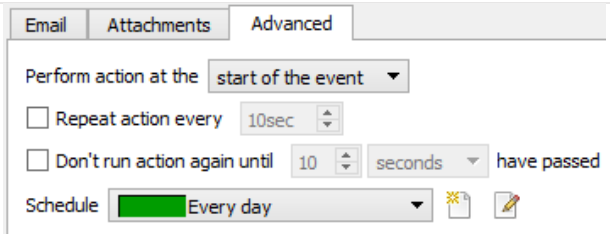
Include trigger info

Checking "Include trigger info" will include trigger information if using a third-party system as an event trigger.

Advanced Tab

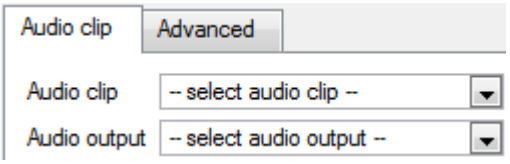
The advanced options are identical to those discussed under Control Output.

4.10.6.8 Send Email

The initial email setup must be done under **Setup Tab / Configure Servers / General Site Setup / Email tab**. However, the options of recipient and the information that will be sent in the email are set here.	
Set the Recipient	Add an email address in the **To** field. To add another recipient, click on this icon. It will add another **To** field.
Set the Variable	There is a list of Available Variables in the Send Email window. These define what information is sent in the email. To add variable, add the Variable name in the text box to the left of the Available Variables list. The format for adding the variable is: Descriptive_Name: $Variable_Name
Copy/Paste	Copy/past variable settings from one Technical Alarm to another. This is very handy for doing a batch of Technical alarms, across multiple servers.
	The Attachments tab allows the user to have video from the event attached to the email.
	The Advanced tab allows the user to define when the email action takes place, once the event has started. A schedule for the event may also be set.

4.10.6.9 Play Audio Clip

4.10.6.9.1 Audio Clip Tab



Audio Clip is the actual audio file played as an action. The sounds are stored in the installation folder under \sounds.
Audio Output is the audio device that will output the sound.

4.10.6.9.2 Advanced Tab

The advanced options are identical to those discussed under Control Output.

4.10.6.9.3 Audio Specifications

Supported format: WAV

Supported sampling rates
• 8kHz • 11kHz (actually 11025Hz) • 16kHz • 22kHz (actually 22050Hz) • 24kHz • 32kHz • 44kHz (actually (44100Hz) • 48kHz

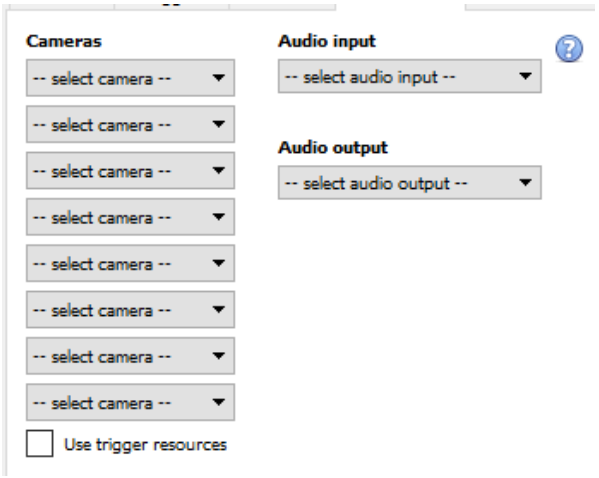
4.10.7 Resources Tab

There are two scenarios in which the resources set here will be sent.

1. **Gateway**: When a user responds to an alarm in a gateway, the system will show the cameras and start the audio listed in the resources.
2. **Camera tab**: When a camera tab is unlocked, and the event triggers, the display will switch to show the cameras listed in the resources.

Note: to view this information in the software, click on the **question mark icon**.

4.10.7.1 Resources Tab



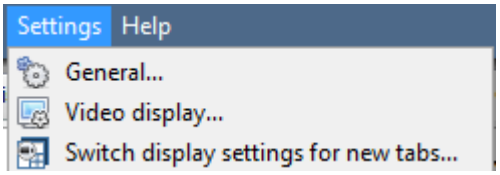
Send up to 8 cameras, an audio output, and an audio input.

This will be broadcast to all operators viewing this site, details on this are explained below.

Use trigger resources will automatically send resources that have been associated with the trigger.

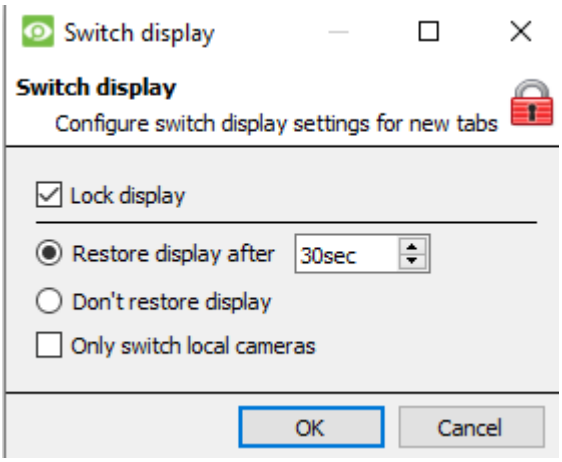
Click the **question mark icon** for more information regarding when the resources set here will be sent.

4.10.7.2 Default Switch Display Settings



If deciding to send Resources, define whether or not the Operator's cameras tab should change when these resources arrive. These settings are made outside of the Setup Tab, under **Settings Menu / Switch display settings for new tabs…**

Note: The settings here will apply to any new Cameras Tabs, opened after the settings are changed.



Lock Display
Will prevent the Cameras Tab from displaying any video feeds sent to it by the Event.

Restore display after
Will define how long after switching to the Event Cameras the Cameras Tab will return to the original display settings.

Don't restore display
Will leave the Cameras Tab on the Event Cameras until an operator, or administrator, resets the display.

Only Switch Local Cameras
Will only switch to Event cameras originating from a local site.

Note: Lock, or unlock , the currently opened Cameras Tab by clicking on the little lock located at the end of the Timeline on the Review Controls.

4.11 Monitors

The Monitors option provides the ability to send video from a server to a Video Wall. This is usually a selection of screens that are dedicated to showing video feeds.

4.11.1 General Settings

4.11.1.1 Licensing

Each monitor running on a Video Wall server needs to be licensed with a VGA license. The license is necessary on the Server sending out video, not on the Client. (Remember: "The license needs to be on the server the monitor is being added to".)

4.11.1.2 Video Wall Software

The **CathexisVision Video Wall** software is installed along with the **CathexisVision Suite**. It is called **cat_vgaserver.exe**, in the installation folder. In the Start Menu, under **Cathexis**, find it under the name **CathexisVision Video Wall.**

When running the Video Wall, software will show in the icon tray as this icon.

4.11.1.3 Run on Startup

If this unit is going to be a permanent Video Wall it is advisable to have the software run on startup. To do so, add the exe to the Startup Folder:

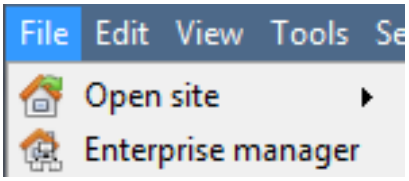
- C:\Users\User_Name\AppData\Roaming\Microsoft\Windows\StartMenu\Programs\Startup . (Replace Username with the name of the user profile that the software will be running on).
- Navigate straight to the Startup folder of the currently logged in Windows User by copy-pasting the following into the Windows Explorer Navigation bar: %appdata%\Microsoft\Windows\Start Menu\Programs\Startup.

4.11.2 Monitors Tab on a Base Station

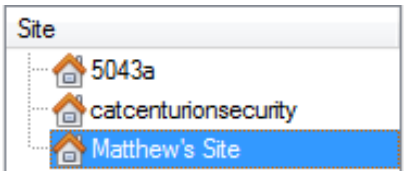
The Monitors Tab will automatically be present in **CathexisVision** on the Server which monitors are added to. For the Monitors Tab to be on a Base Station, make the relevant site a Resources Site. This must be done in the Enterprise Manager of the Base Station the Monitors Tab is being added to.

4.11.2.1 Create a Resources Site

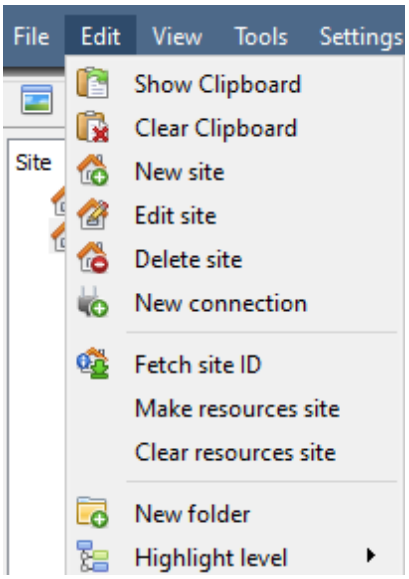
Note: this needs to be done on the Base Station the Monitors Tab is on.



Open the **Enterprise Manager**.



Select the site to edit.
Here, the site edited is called Matthew's Site.



Select Edit from the Menu Bar.
With the site still selected click on **Edit / Make Resources Site**.

To remove the Site's status as a resources site, follow the same procedure, but click on **Clear Resource Site**.

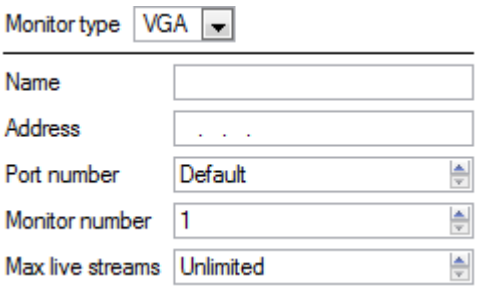
4.11.3 Adding a Monitor

4.11.3.1 Monitor type

There are two types of monitor that may be added to the system: a VGA monitor and an XP switcher monitor.

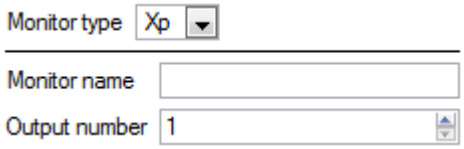
4.11.3.1.1 VGA

This will work via a VGA Server computer, with the **CathexisVision Video Wall** software running on it.



Address This is the address of the unit the video is being sent to (or the address of the router the information is being sent to, if the Video Wall is on another network).
Port Number. Leave this at default. Unless the video wall is on another network to the recording server, and it is necessary to forward specific ports.
Monitor Number corresponds to the physical monitory on the wall.
Max Live Streams will limit the quantity of live streams this monitor will support. (Set based on the monitor unit's streaming capacity.)

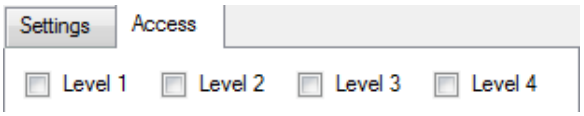
4.11.3.1.2 XP



XP monitors, attached to the unit via a rear-panel cross-point switcher (This will be added to a Linux based system, most probably Fedora).
Monitor name is a descriptive name given to the monitor.
Output Number is the number on the XP switch attached to the screen.

Note: This is available if the server unit has a VMX cross-point switcher, which is found on a Linux based server.

4.11.4 Access



Under the Access Tab, define which user Access Levels have rights to make changes to this Monitor, via the Monitors Tab (discussed below).

4.12 Access Rights

Setup tab / Configure Servers / expand Your_Server_Name / Access Rights.

Under **Access Rights**, setup which Site Resources are available to specific access levels. Each user was assigned an access level when added. This user level corresponds to the Levels assigned to Site Resources here in **Access Rights**.

Besides resources in the Cameras tab, access rights will also be carried through to the Alarm Management Gateway, the Database, Archiving, etc. Access rights will apply to any area of the software that involves the site resources, which have had permissions set here.

Note: Users can be added and managed in **Setup tab** / **Configure Users.**

4.12.1 Tabs

Select the resource from the list on the left, and check the level that will have access to this resource.

The tabs (**Cameras**, **Outputs**, **Monitors**, **General**) represent classes of resources whose access level may be controlled. The one selected will have all the resources that fall into this class displayed in the left-hand panel. In the examples below, the **Cameras** tab is selected and the settings refer to camera resources. However, the process is identical when editing **Outputs**, **Inputs**, **Monitors,** and **General.**

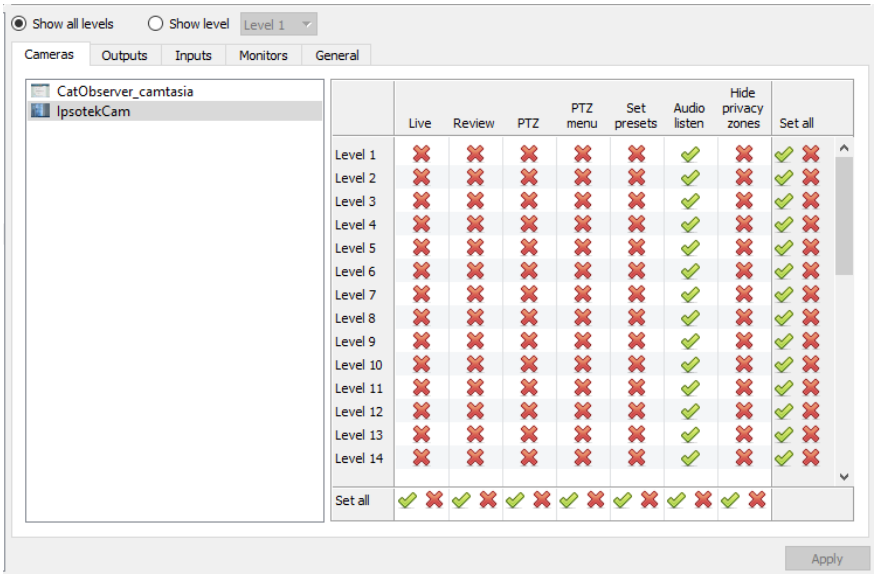
4.12.1.1 Cameras Tab

The cameras tab involves setting access rights for user levels for specific cameras.

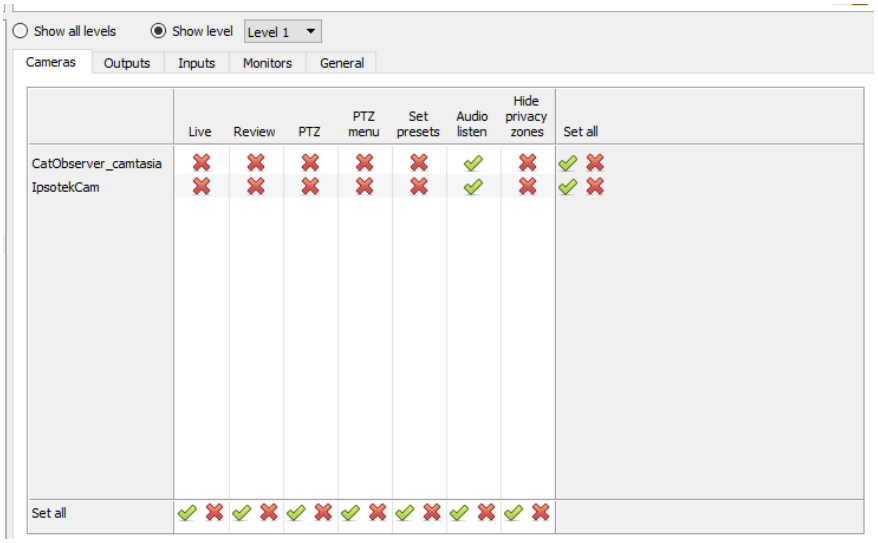
Select the relevant cameras on the left and then set the desired access right by clicking to toggle between the **tick icon** and the **cross icon**.

There are two options when editing **Access Rights:**

1. **Show all levels** will show every Level setting according to each resource.
2. **Show level** shows only the settings for the selected user level according to each resource.



Selecting **Show all levels** and then selecting a resource (in this example **Camera 1**) will display the settings for all user levels according to the particular resource. I.e., the User level settings may be different for **Camera 2**.



Show level is selected, and thus allows for the selection of a user level from a drop-down menu.
Here, **Level 1** is selected, and thus only the **Level 1** settings for each resource are displayed.
(Should there be additional resources, these would also be displayed here.)

4.12.1.1.1 Access Right Definitions

Live	This controls which Access Levels can view the camera's live feed. If this option is disabled, the user will not be able to view the camera at all, and all the following rights will be automatically denied.
Review	This controls which Access Levels can review recorded footage from this camera.
PTZ	This controls which Access Levels can control PTZ movement.
PTZ Menu	This controls which Access Levels have the ability to alter the PTZ menu.
Set Presets	This controls which Access Levels can change PTZ Preset positions.
Audio Listen	This controls which Access Levels can listen to the audio (provided the camera has an on-board mic).
Hide Privacy Zones	This controls which Access Levels can remove the privacy zones added to the camera.
Set All	Selecting the **tick icon** will give this level access to all settings. Selecting the **cross icon** will give this level access to none.

Note: A **tick** means that this level has access; a **cross** means that this right has been denied to this level. Left-click on the tick/cross to change its designation.

4.12.1.1.2 Audio Listen Access Right

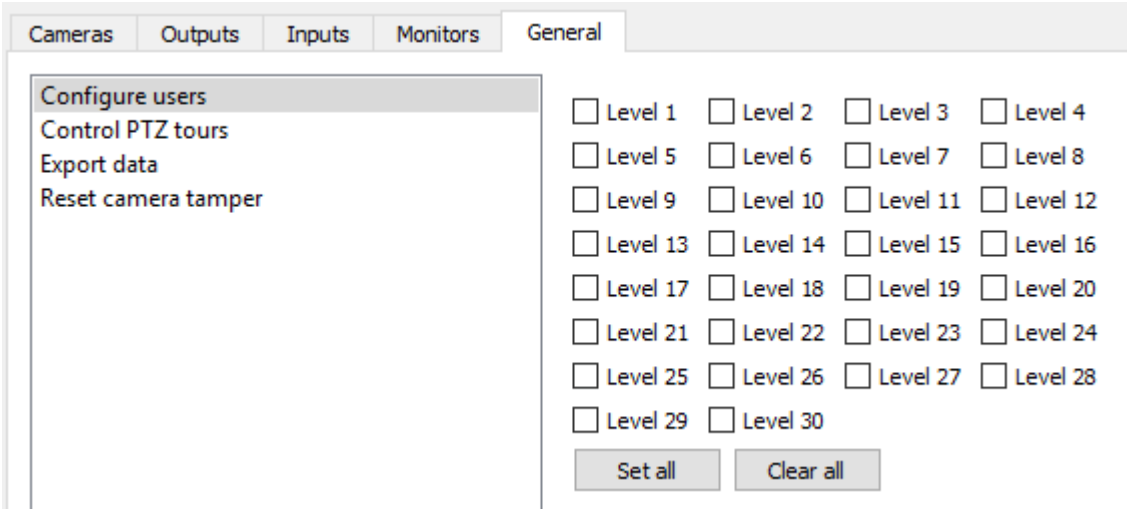
The table below details situations in which the Audio Listen access rights settings configured by the user do and do not apply.

Audio Listen access right settings **do apply** to:	Audio Listen access right settings **do not apply** to:
Live viewing. Reviewing from the camera tab. Reviewing from the database tab (both video and integration databases). Viewing video when handling an alarm in the Alarm Management Gateway.	Independent audio channels. Archived video. Connecting to a 2016.2 server using a 2015/2016.1 viewer. Connecting to a 2016.1 server using a 2016.2 viewer.

4.12.2 Inputs, Outputs and Monitors

Select the relevant tab and enable rights for user levels to access selected inputs, outputs, or monitors configured on the server.

4.12.3 General Tab

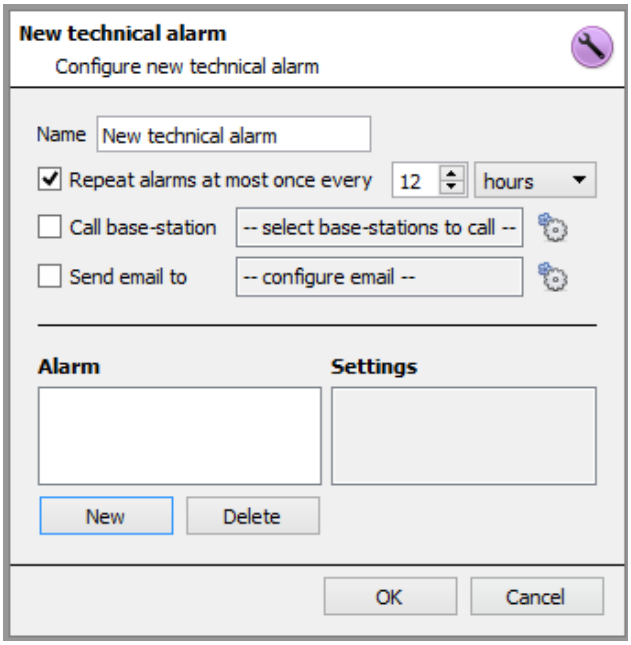


In the General tab, assign user level access rights to general site abilities that are not specific to a camera. The table below explains the four access rights (shown in the image above).

Configure Users	This gives non-admin users the ability to create and modify other non-admin users. Users with this ability **will be able to**: • Enter the Setup tab to configure Users, however no other setup will be available or visible to that user. • Create and modify other non-admin users. • Change their own password.

	They **will not be able to**: • Access any part of the system setup other than the user configuration section. • Will not be able to delete themselves. • Will not be able to create admin users. • Will not be able to import LDAP users.
Control PTZ Tours	Users with this ability will be able to control PTZ tours.
Export Data	Users with this ability will be able to export data (e.g., archives, PDF and CSV files from the database – provided they have database rights).
Reset Camera Tamper	If/when a camera tamper alert is presented on the system, users with this ability will be able to reset it.

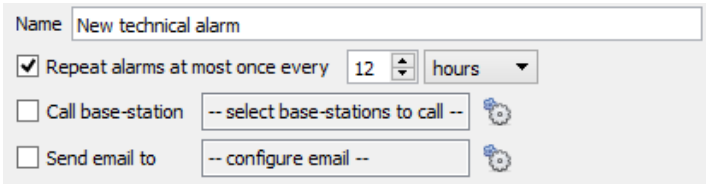
4.13 Technical Alarms



This is a facility to set up alarm conditions in the event of a technical problem. A single **Technical Alarm** can send on multiple different alarms, in this way set up an alarm to send only information regarding hardware, or software, or cameras.

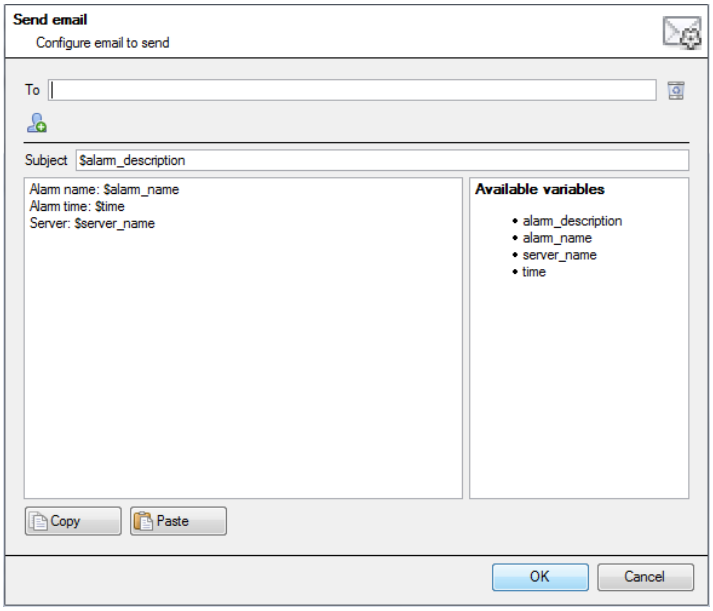
Technical Alarms are set on a server-by-server basis, and as such are located in the **configure servers** settings under **Site / Setup / Configure Servers / Technical Alarms**.

4.13.1 General Settings



Give Alarm a descriptive **name.**
The user mat set a global maximum amount of alarm repeats.
Select whether the alarms should be sent via email or go to a Base-Station.

4.13.1.1 Email Configuration



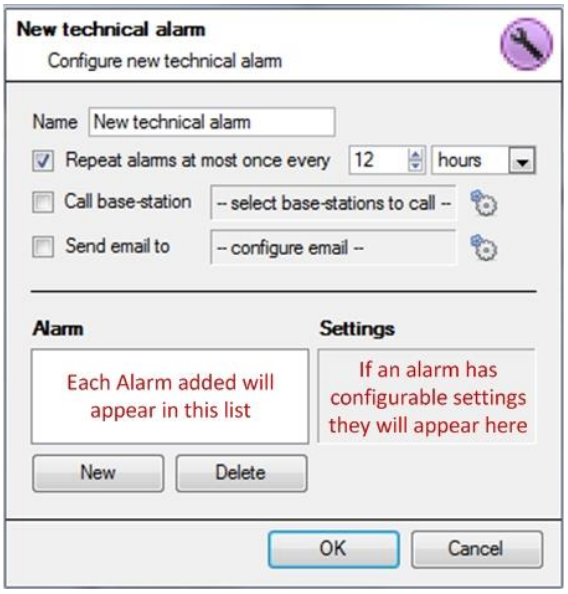
The initial email setup must be completed (see email configuration tab in the Servers configuration menu).

However, the options of recipient, and the information that will be sent in the email, are set here.

Set the Recipient	Add an email address in the **To** field. To add another recipient, click on this icon. This will add another **To** field.
Set the Variable	There is a list of **Available Variables** in the Send Email window. These define what information is sent in the email. To add a variable, add the Variable name in the text box to the left of the Available Variables list. The format for adding the variable is: Descriptive_Name: $Variable_Name.
Copy/Paste	The user may copy/paste variable settings from one Technical Alarm to another. This is very handy if dealing with a batch of Technical alarms, across multiple servers.

4.13.2 Add / Edit a Technical Alarm

New To add a technical alarm, click on **New** in the Technical Alarms panel. The following dialogue will appear:



Name: give technical alarm a descriptive name.

Repeat alarm at most… : This setting sets a 'global' repeat setting, which defines how often individual alarms may repeat.

Call Base Station

For alarms to be sent to a Base Station.

Click on the gear icon to set the Base Station/s.

Base Station setup is covered in section Call Basestation Tab.

Send Email to: there is also the option to send an email in the event of an alarm. To setup a new email, click on .

Email Setup is dealt with under the Send Email tab. See Setup Tab: Configure Servers section.

4.13.2.1 Available Alarms

Click **New** in the New Technical Alarm dialogue. This will initiate a drop-down menu with the following options.

Base-Station Alarms	Trigger when a base-station is configured to send alarms via a capture station. The base-station can generate alarms such as software failures.
Camera Faults (Configurable)	Will trigger based on cameras being up for a certain percent of the time, or cameras failing a certain number of times in a given period (configurable). The camera faults alarm has been updated to optionally check for stalled feeds.

	Configure: Here, set whether alarms trigger from one, or both options listed above. Also select to have alerts from all cameras, or from selected cameras.
Database	Triggers when the database encounters an error, such as failing to write data to the database.
Disk	Triggers when disk errors occur.
Environment	Triggers off environment warnings, such as high CPU temperature, fans running at low RPM (only).
Failover	The site master can be configured to generate a technical alarm if any of the failover servers are down.
Frame-Grabber	Triggers when a frame-grabber has a problem, such as frame-grabber reboot, card stalled.
Gateway alarm	Only applies to gateway systems, and triggers when the gateway experiences a problem, such as an error connecting to the alarm database.
Integration Database	Triggers when the integration database is down.
Network I/O	Will trigger when an EIO is down.
Network Connectivity	Triggers when target/s in a list of configured IP addresses does not reply when pinged.
Reboots	Triggers when a unit reboots frequently, or has a watchdog, or hard-reboots.
Recording failure	Triggers when a recording *should* be taking place, but is not. Enabling this alarm will periodically check recordings for failure. **Configure:** All that needs to be set here is the cameras not desired to trigger this alarm.
Recording Period	Will trigger when a database stops recording before its predefined period is complete. For example, if a database is set to record for 30 days, but it only records for 25.
Scheduled Archive	Triggers when a scheduled archive encounters a problem, such as the archive destination not being accessible.
Server Monitoring	This is a technical alarm that is generated when a unit on the site goes down.
Software Failure	Triggers when a software module fails.
Test	Triggers an alarm at a set frequency. This can test the system, to see if it will receive alarms.

4.13.2.2 Important Note on Operating Systems

Technical alarms have different levels of integration with the different Operating Systems.

Technical Alarm Type	Windows	Fedora	Ubuntu
Base-stations Alarms	X	X	X
Cameras	X	X	X
Database	X	X	X
Disk	X	X	X
Environment*			
Failover	X	X	X
Frame Grabber		X	X
Gateway	X	X	X

Meta-db	X	X	X
Network I/O	X	X	X
Network Connectivity	X	X	X
Reboot	X	X	X
Recording Failure	X	X	X
Scheduled Archive	X	X	X
Software Failure	X	X	X

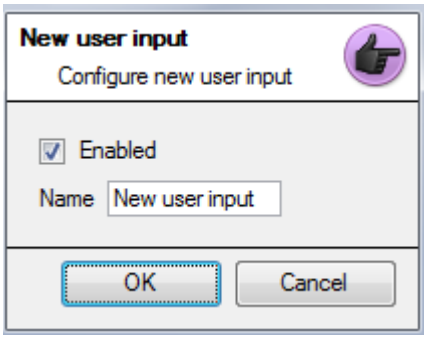
*Environment alarm only available on supported Cathexis hardware.

4.14 Virtual Inputs

Virtual Inputs are user-initiated triggers. They may be added to events, and used as manual triggers. This takes the place of a physical button (which is why the icon for Virtual Inputs is a finger).

For instance, a virtual input may be created, and added to an event that starts a camera recording. The Virtual Input would then function as a record button for that camera.

4.14.1 Add a Virtual Input



To add the Virtual Input, click **New**.

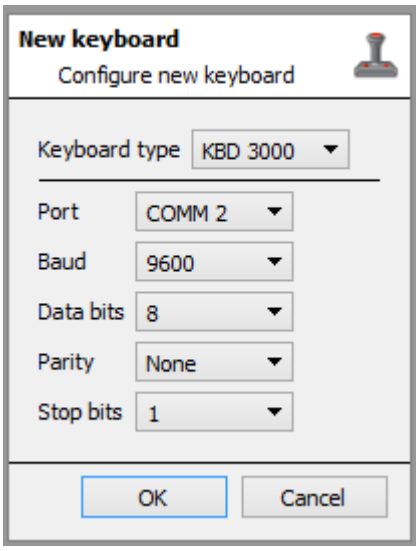
Give the input a descriptive **name.**

This Input works the same way as other triggers in an event, look to Events for more information.

4.15 Keyboards

When adding a Keyboard to a unit there are two possible situations: adding it to a **Recording Server**, via the **Site Menu / Open Tab / Setup Tab**, or to a **Base/Viewing Station** via the **CathexisVision** Menu Bar.

4.15.1 Recording Server

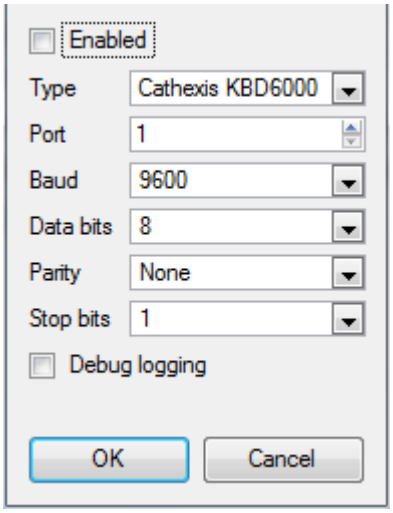


Adding a Keyboard to a Recording server is done on the server. Access **Site / Setup Tab / Configure Servers / Keyboard**.

Simply choose the Keyboard type and enter the port number that corresponds to the port that the keyboard is plugged into.

4.15.2 Base Station

If adding a keyboard to a base station, it is necessary to be on that specific base station.



Enable

Check the box titled Enabled to enable the added keyboard.

KBD3000

The only setting to change for the KDB3000 is the port number. (In fact, other changes will be ignored.)

KBD6000

The correct settings for the KBD6000 are as follows:

Baud	19200
Data Bits	8
Parity	None
Stop Bits	1

Again, these should be the default settings, and probably won't need to be changed.

4.16 Integration Devices General Settings

A major benefit of the Integration Devices panel is that it centralises all integrations to a single interface in which the addition, edition, and management of all integrations added to a server/site is done.

As there are many different integrated devices, and each device will have different options, this General Setup section is designed to introduce the user to the Integration Panel, and the features that are common to all integrations. For more specific instructions and information on a particular integration, please consult the relevant integration guide and/or integration white paper, which can be found at

https://integrations.cathexisvideo.com/manuals/.

For help with a particular integration, please contact support@cat.co.za.

4.16.1 Integration Database

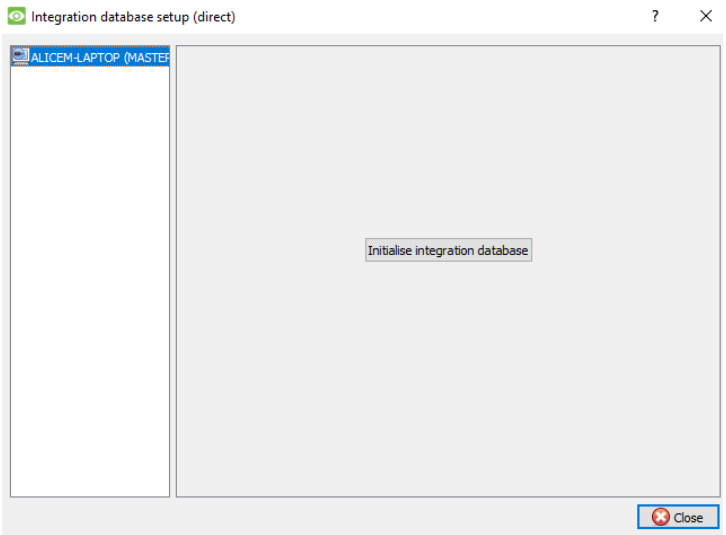
Each integration requires its own, dedicated database. This can be done from two places in the software, but the process is the same for both. The navigation options are explained below.

1. **Site menu / Setup / Integration database….**
2. **Setup tab / Configure Servers / Integration Devices Panel / General tab / Configure integration database.**

For both options, follow the steps below.

4.16.1.1 Initialise the Integration Database

Integrated device databases are added to a broader, integration database. If it hasn't been already, the integration database needs to be initialised. If it has, proceed straight on to creating a new database.



The first time an integration database is added, initialise this feature on the unit.

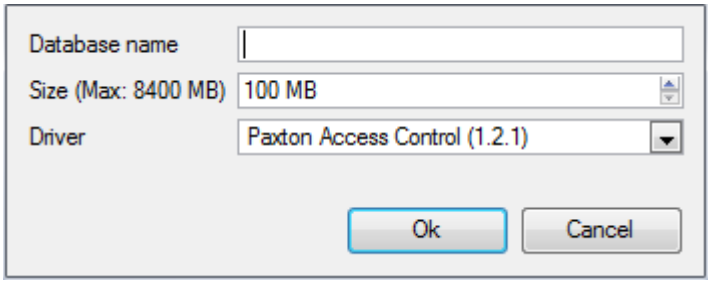
From the list on the left, select the unit to add the database to. Click **Initialise integration database**.

Choose which partition the database will be formed on. Select how much space it will take up.

4.16.1.2 Add a New Devices Database

Right-click on the white space that was occupied by **Initialise integration database** before initialising the database.

Click on **New**.



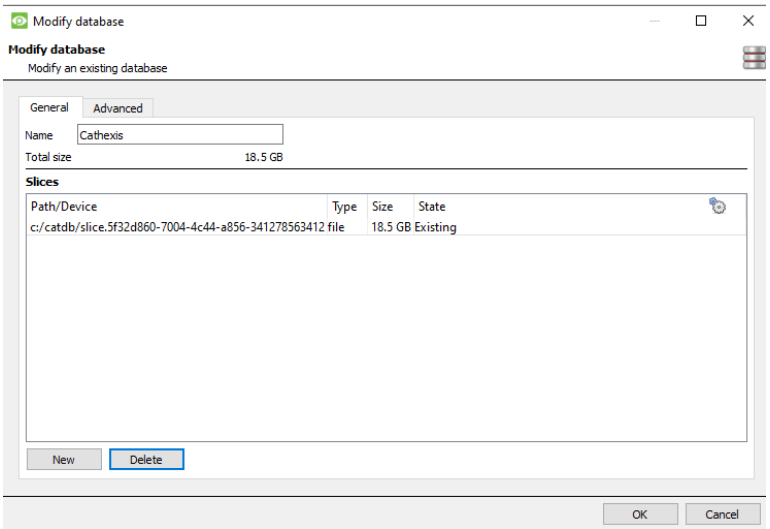
Give the database a descriptive **Database Name**.

Allocate a **Size** to the new device database.

Then choose the device **Driver** the device will be using.

4.16.1.2 Integration Database Procedures

Once at least one database is added, the following procedures will be present. Right click on a database to view:

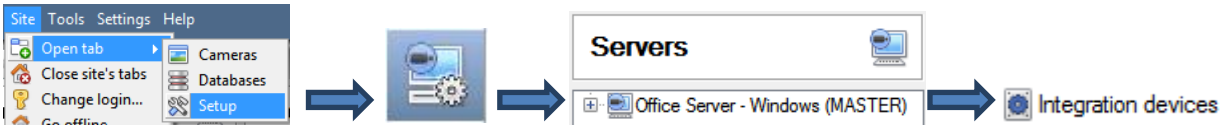


Delete will delete the database selected.
Resize allows resizing this database. There will be Min and Max options, which will either fill the database to the maximum, or the smallest, sizes allowed.
Name will simply allow renaming the Database.
New will open the New Database Dialogue.

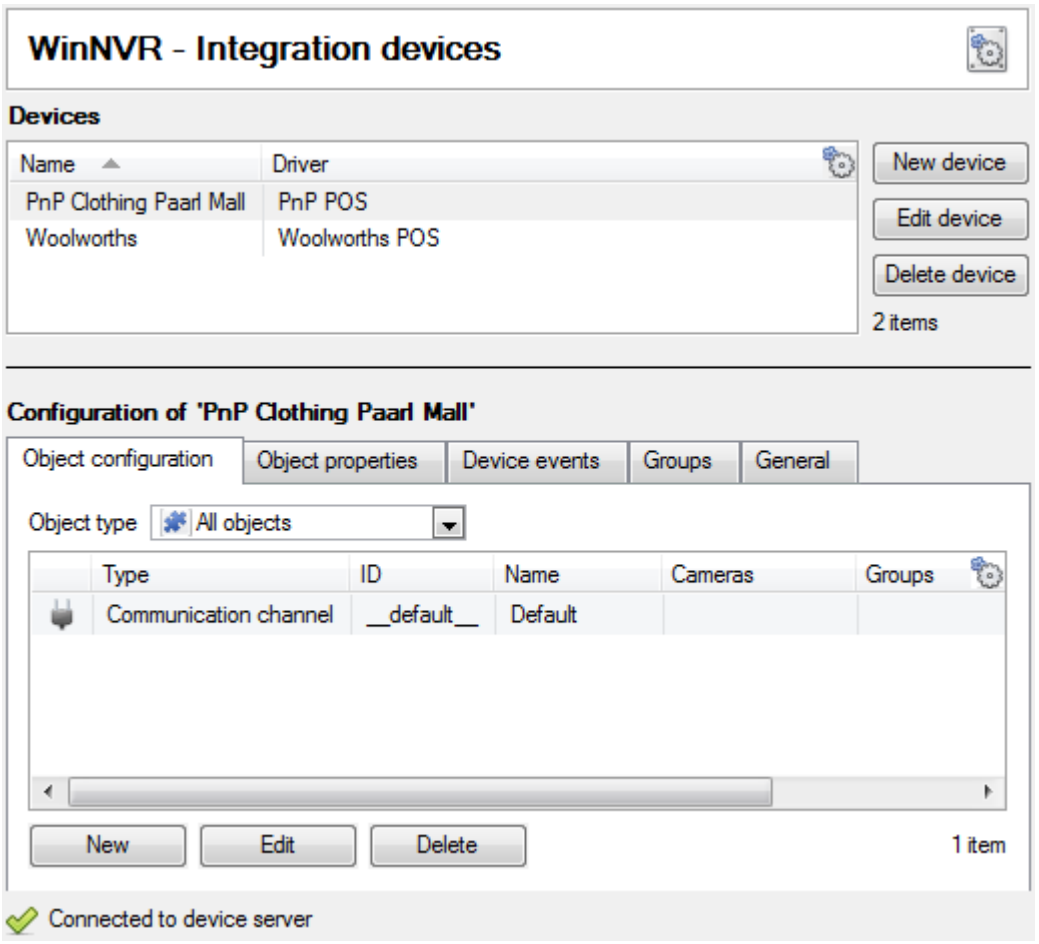
4.16.2 The Integration Devices Panel

4.16.2.1 Open the Integration Setup Panel

Setup Tab / Configure Servers / Integration Devices

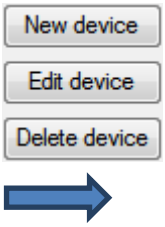


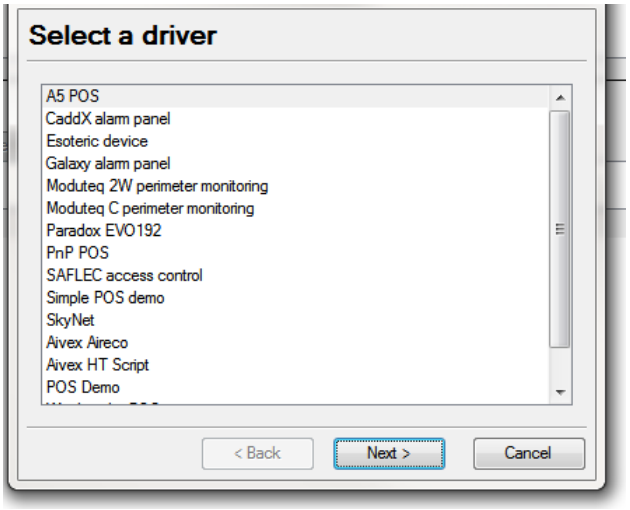
This will bring up the Integration Devices Panel on the right. This is the central point at which integrations are managed.

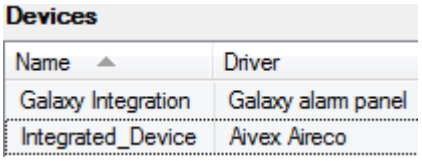


4.16.2.2 Adding an Integrated Device

Click **New device.**
Select the drivers for the device added.

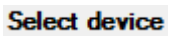






Once the device is added, it will show up in the **Devices** panel. Left-click on a specific device to access its Configuration Settings.

4.16.2.3 Configuration Tabs

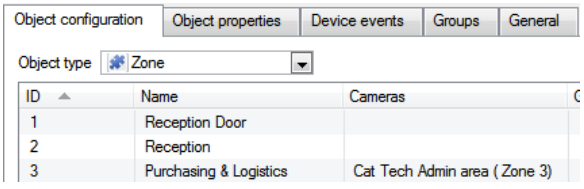


Initially, the configuration panel will be titled **Select device**.

Once an integration is added, the title will become **Configuration of Device_Name**. This is the area where one views the device's objects, and changes settings.

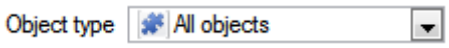
The Configuration section will be automatically populated with the information received from the device.

4.16.2.3.1 Object Configuration Tab



Individual units attached to a specific device are called **objects**. For example, on a Point-of-Sale integration, individual tills are objects. Or in access control integrations, the individual access nodes are objects.

Objects can have cameras assigned to them, so that camera recordings can be linked to the till via a metadatabase.



Each integration will obviously offer different objects.

4.16.2.3.2 Object Properties Tab

Object properties are the specific information about each object. For instance, the different names that have been given to an access control node, its armed status etc.

4.16.2.3.3 Device Events Tab

This gives a live stream of all device events as they occur. For POS this would be sales, for Access Control this would be access events, and so on.

4.16.2.3.4 Object Group Tab

Create groups of the same type of object. When creating a group, select the object type to include in the group, once the group is created the available objects panel will fill up with all available objects of that type. From this list, choose which objects to use in the Group.

This is incredibly useful in setting up Events an entire group can be used as an Event Trigger.

4.16.2.3.5 General Tab

Offers general information, such as the metadatabase that the integration is attached to.

Access the Integration Database dialogue from here from the General Tab by clicking on **Configure integration database**.

4.16.3 Important Considerations

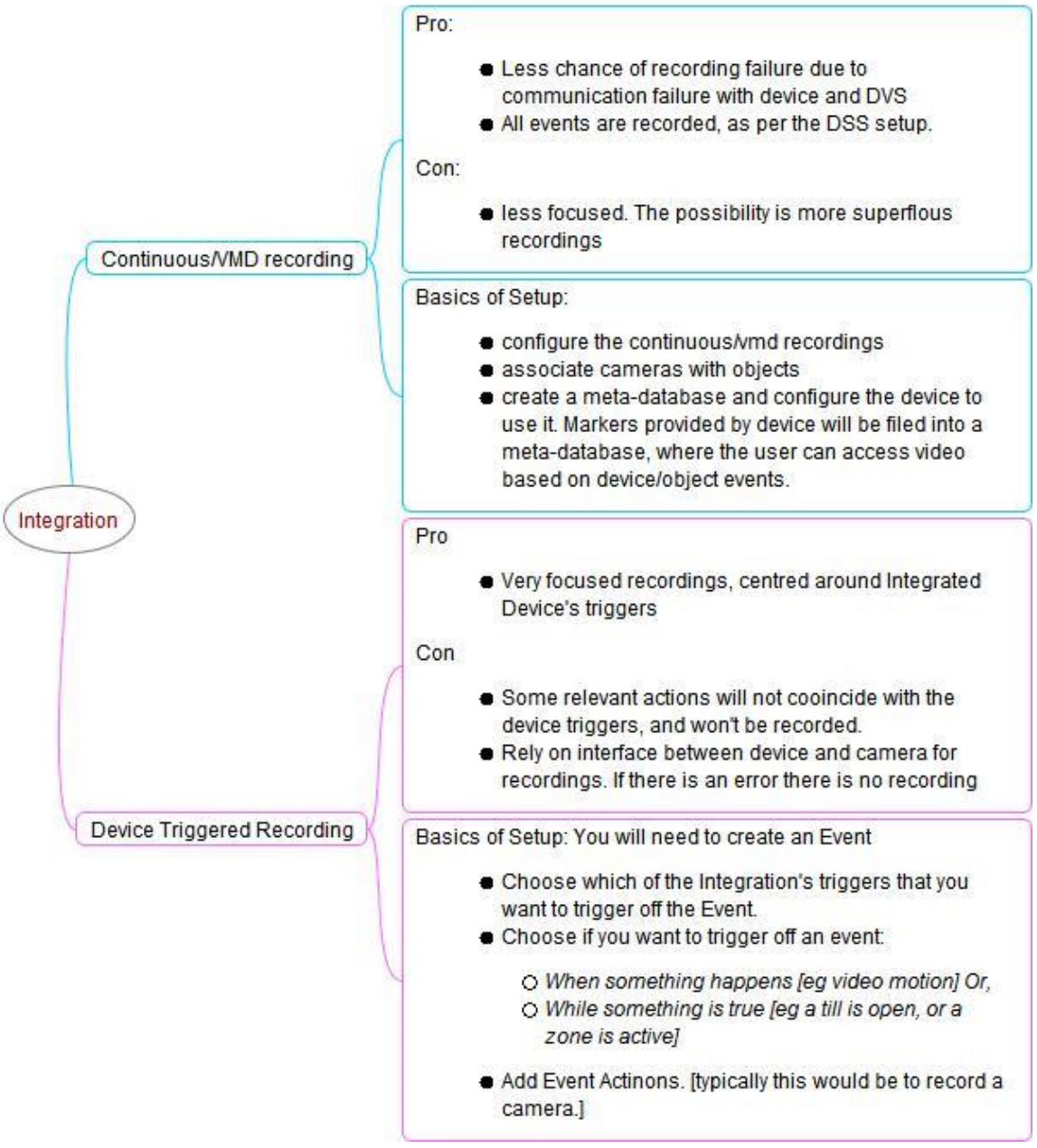
When adding an integrated device, there are some important considerations.

4.16.3.1 Device Triggered Recordings or Continuous Recording with Device Provided Markers

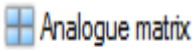
One of the first considerations when using an integrated device is how it should interact with the Surveillance System.

- Should the device set itself to trigger recordings? Or,
- Should there be continuous recording, with the integration creating time markers on this recording?

There are pros and cons to both. These, along with basic setup designs are provided in the mind-map below:



4.17 Analogue Matrix

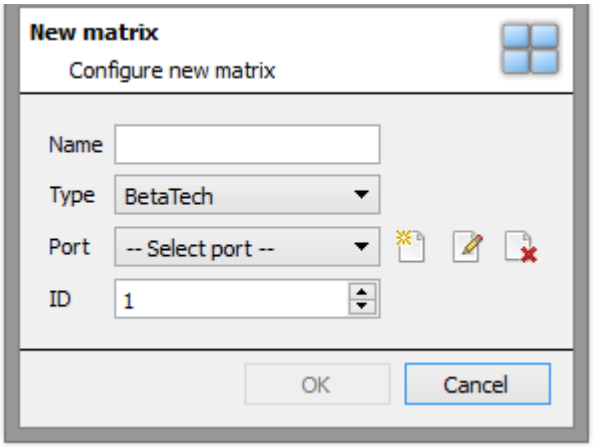


CathexisVision has the ability to support an analogue matrix. Click on **Analogue matrix** to access the setup. This feature allows for a true hybrid solution between IP and analogue based security installations.

Note: An Analogue matrix would be used on existing analogue based sites. So there would be an old analogue matrix controlling or switching analogue camera video feeds onto analogue monitors. The ability to control older matices is useful to switch a specific camera to a monitor based on a **CathexisVision** event action.

4.17.1 Add / Edit an Analogue Matrix

4.17.1.1 New Matrix Dialogue



After clicking on **New**, the dialogue box will appear.

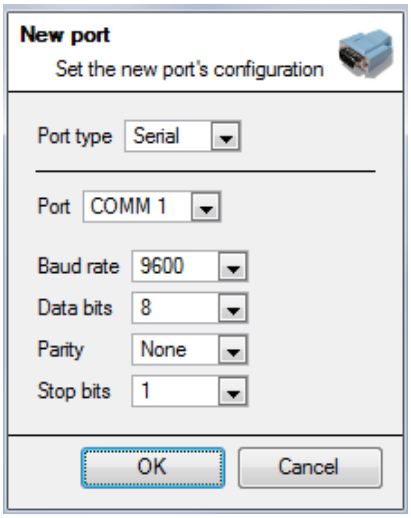
Give the matrix a descriptive **name**.

Select the **type** of matrix that will be used.

Select/Configure a **port** (dealt with below).

Set the **ID** of the matrix.

4.17.1.2 Port Editing Dialogue



To add/edit a port, this menu will be visible.

To add a new port, click on this icon.

To edit a port, click on this icon.

To delete the currently chosen port, click on this icon.

Select the **port type** that will be used.

The **port** option relates to the physical port on the unit.

Select the relevant **Baud Rate**, **Data Bits, Parity, and Stop Bits** for the specific matrix that will be used.

5. Setup Tab: Resources

5.1 Resource Panel Configuration

The Resource Panel is to the right of the Cameras Panel, in the Cameras Tab. The Resources Panel is a customisable panel of resources. It gives users quick access to the resources that are open to them. To configure the location of the Resource Panel in the Cameras Tab, refer to CathexisVision GUI Setup section.

Use the Resource Panel Setup to configure the resources that users will see in the Resources Panel. The Resource Panel should display a site's resources in a way that is useful to operators on the site. For example, list cameras under a folder together, or create one folder per operator.

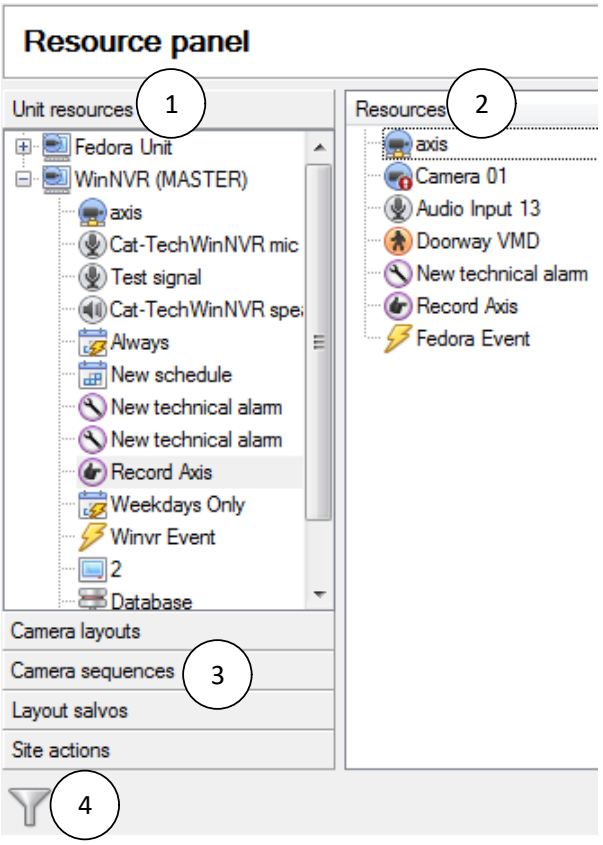
TIPS:

• **Set up the resources** in a way that will **meet the requirements** of all the users. The Resource Panel is the only point of access most users have to the resources.

• **Resources can be repeated in different folders**. For example, folders can be defined by user names, and resources can be repeated across all of these user folders.

• To reduce interface clutter, **remove unused resources** from the tab.

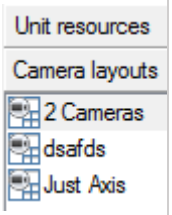
5.1.1 Resource Panel Setup



1. This list is the list of servers on the site, and the resources each server has.

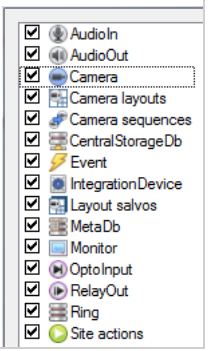
2. This is the list of resources that will appear in the Resources Panel.

3. Clicking on any of these toolboxes will bring up the named resource. This is seen in the example of Camera Layouts, to the right.



4. This is the filter feature. Use this to remove some resources from the list, to simplify the screen.

The available filters are represented in the image to the right.

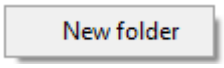


5.1.1.1 Add a Resource to the Resources List

To add a resource to the list that will appear on the panel, select one or more resources. Left-click and drag the resource horizontally into the Resources area.

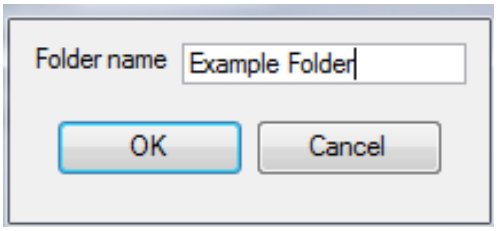
5.1.1.2 Create a folder

Organise resources further by creating a folder.
To do so, right-click on any white-space in the resources area (where the included resources are).



Click on New Folder.

Give the folder a name.



To add items to the folder, click-and-drag them into the folder (in the same way resources were added to the list).

5.1.1.3 Delete / Rename folders and Resources

To remove items from the Resources Panel list, right-click on the item. Click **Delete.**

To Rename a folder, right-click on the folder. Click **Properties**.

6. Setup Tab: Site Actions

6.1 Site Actions

Site actions are setup in the **Site Actions** section in the Setup Window. From Configure Servers.

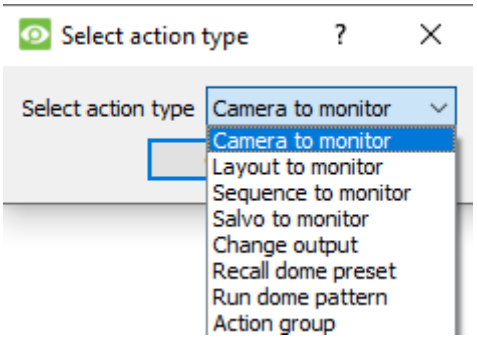
Click on this **icon** to get there.

The reason for having site actions outside of the Events Setup Window in Configure Servers, is because of the fact that Events are edited on a server-by-server basis. [A good way to think of Site Actions is as **Universal Actions**.] Therefore, the reason for creating a site action is to create one action that can be applied to multiple events, across multiple servers.

6.1.1 Creating a Site Action

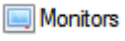
To add a new action simply right-click on any white space in the Actions Panel, and select **New action**.

The drop-down menu will contain a list of all possible site actions. Select the relevant action and set it up. The menu will change depending on the action created.



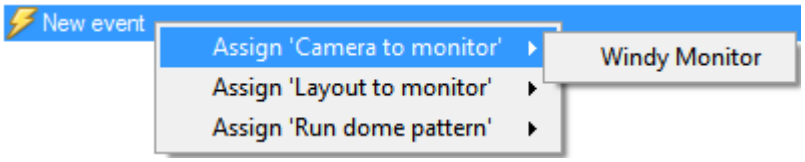
6.1.2 Site Action Types

Camera To Monitor	This will send a preconfigured camera to a **CathexisVision Video Wall**.
Layout to Monitor	This will set the view on a Video Wall to a predefined Layout.
Sequence to Monitor	This will run a predefined Sequence of individual cameras in the Monitor.
Salvo to Monitor	Will run a predefined Salvo of Layouts on a Video Wall.
Change Output	Changes an Output state.
Recall Dome Preset	Sends a PTZ camera to a Preset position.
Run Dome Pattern	Cycles a PTZ through a pattern (a sequence of Preset positions).
Action Group	An action group is a group of site actions.

Note: As with the other events, the resources used by the relevant Site Actions need to have been created and be available for use before an action can be created. For instance, the **Camera to Monitor** Site Action uses a monitor that was created under **Monitors** in Configure Servers. 

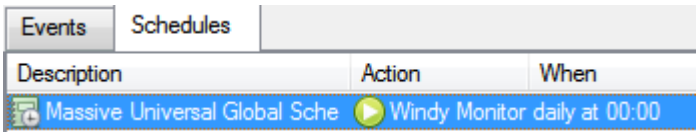
6.1.3 Adding a Site Action to an Event

For a site action to trigger when an Event triggers, attaching a Site Action to an existing Event is very simple. In the Events tab in the right-hand panel, right-click on one of the events. This provides a list of Action Types that have been added. Under each type is a list of all Actions of that type created.

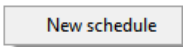


Finally, select the Action to assign to this event.

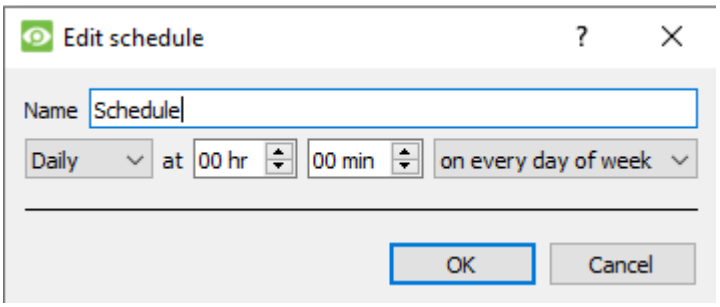
6.1.4 Adding a Schedule to a Site Action



If no schedules are created, right-click any white space under the schedules tab, and select **New Schedule**.



This will bring up the **Edit Schedule** window, as seen below.



To add the schedule, select the exact times when the Site Action will be triggered.

[i.e. It is not an active during schedule, it is a trigger when schedule.]

Use the drop-down menus to further specify times.

Note: The schedules created here only apply to Site Actions, and cannot be applied elsewhere.

7. Setup Tab: Reports

7.1 Introduction

CathexisVision offers extensive reporting on the Hardware and Software that comprise the Site.

Users can create **Report Templates**. These are pre-defined sets of reports that will pull the same information each time. Report Templates give users the ability to retrieve reports on a schedule.

Reports can be found under **Site Menu / Open Tab / Setup /**

Note: If scheduled metadatabase reports are required, these must be configured individually within the particular metadatabase. Consult the ***CathexisVision Operator's Manual*** for more information.

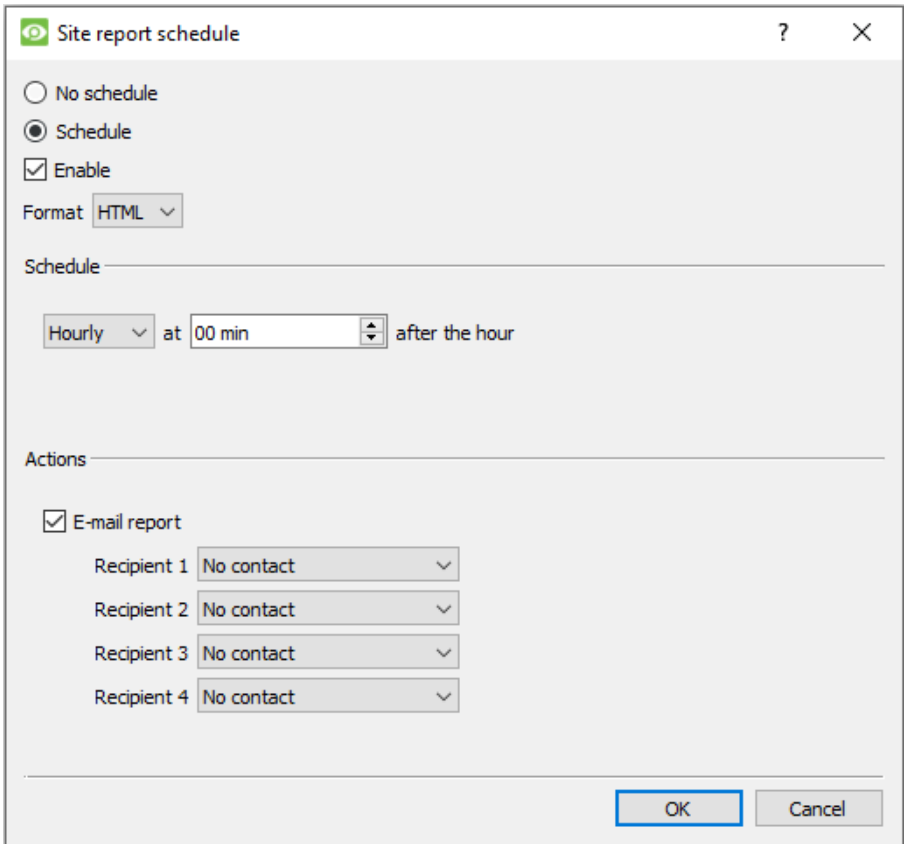
7.2 Controls

7.2.1 Add, Edit or Delete

New Click **New** to create a report.
Edit Click **Edit** to edit a new report.

Refer to the Report Window section.

7.2.2 Schedule



To add a Schedule to a report: Select a report from the Reports list and click on the **Schedule** button.

Format: Emailed reports are sent in HTML format.

Schedule: The schedule may be generated of a variety of time frames, from hourly to monthly.

Actions: If email is set up on the site and some Site Contacts are set up, then the user may email the reports when they are generated.

7.2.3 Fetch

This will pull the report for the Template Chosen.

There are four options at the bottom of the **Fetch** window.

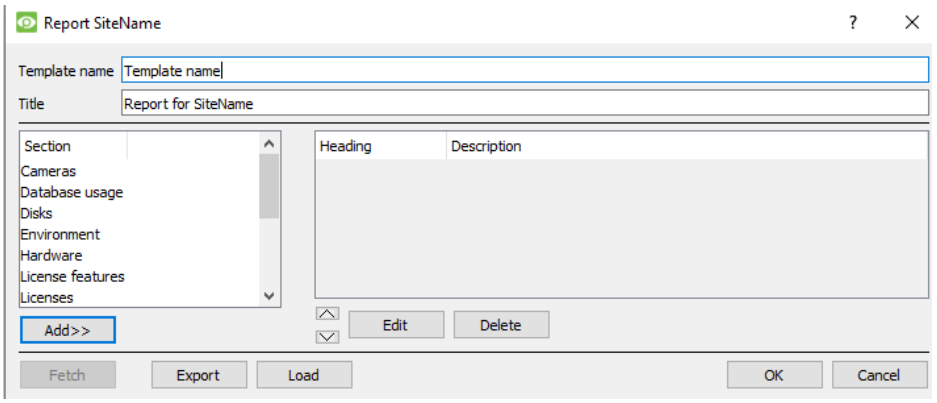
1. **Print** the report.
2. **Export** the report as an HTML file for later use.
3. **Email** the report.
4. **Archive** the report.
   a. The archived reports are filed under Install_Path\sitedb\reports.
   For example: C:\Program Files (x86)\Cathexis CathexisVision Suite WRV\sitedb\reports.

7.3 Create Report

To create a new report, or edit an existing one, select the relevant button or double-click the report.

The **Report window** will open. In the Report window, parameters for the report must be configured (such as the types of reports to be included).

There are two columns in the **Report Template Editing window**. The column on the **left** is populated with all the available Report Variables. The column on the **right** is filled with the variables that can be used by the Report Template. Each **Section** will be explained below.



Template Name: Give the template a name.

Title: Give this report a title (to be displayed on fetched report).

See below for the process of adding report types to this report, and for description of the report types selected.

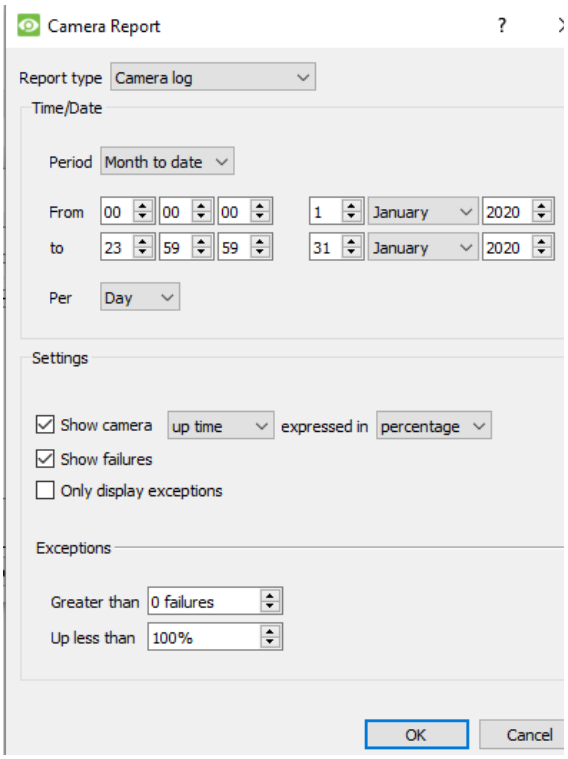
1. Select a report variable from the Sections list on the left. Click **Add** to add the variable to the report template. Report template components will be shown in the list on the right.
   a. Multiple report types from the Sections list may be added.
   b. **Note**: Report types will appear in the fetched report in the order that they are added.

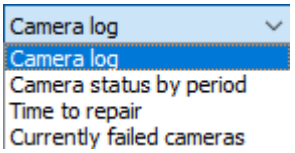
2. When adding a report variable to the current report template, a configuration window will open. The parameters for that specific report variable must be defined before it is added to the current report template. See below for the full list of report types and configuration options.

Add>>	Select a report type. Click to add to the current report template.
Edit	Select report type from current report template components. Click to Edit parameters.
Delete	Select report type from current report template components. Click to remove.
Fetch	Click to generate the current report template.
Export	Click to export the template as a local file on the NVR.
Load	Click to load the local file of an exported template.

7.4 Cameras Report

The **Cameras Report**: this reports the uptime or downtime of cameras on a site for a defined period. There are options to define the report type.





Choose one of the Report Types.

Show failures: this tells the report to show the number of failures for a camera over the given period. (A failure is when the camera stops working.)

Only display exceptions: this tells the reports to only show cameras that meet the exception criteria (which the user specifies on that same page).

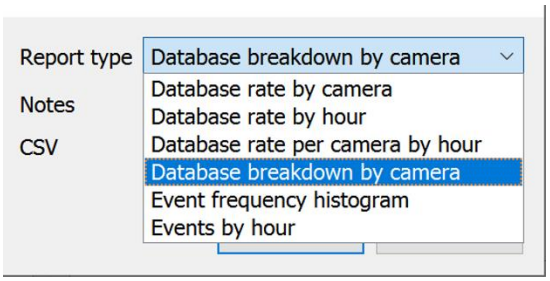
This is useful if the user wishes to only see the problem cameras.

7.4.1 Camera Report Example

		1/4		2/4		3/4		4/4		5/4		6/4		7/4	
Unit	Camera	Up	#Fail	Up	#Fail	Up	#Fail	Up	#Fail	Up	#Fail	Up	#Fail	Up	#Fail
Cathexis Demo	Back Parking - Vivotek (4)	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0	99%	1
	Back Parking - Vivotek (3)	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0
	Demo Room - Axis P3224 (8)	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0
	Spar - POS Till (26)	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0
	Demo Room - Axis M3005 (7)	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0
	Front PTZ - Truvision (19)	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0
	Driveway ANPR - Axis (14)	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0
	Road ANPR - Axis P1365 (24)	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0
	Highway SPEED DETECTION (20)	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0
	Perimeter - Axis Q1615 (23)	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0
	Thermal Road - Line Crossing (27)	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0
	Holdens ANPR - Dahua (21)	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0
	Back Door Exit IMPRO (2)	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0
	Front Door Exit IMPRO (18)	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0
	Back Door Entrance IMPRO (1)	100%	0	99%	1	100%	0	100%	0	100%	0	100%	0	100%	0
	Driveway ANPR- Hik (15)	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0
	Driveway - Axis 6000e(A) (9)	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0
	Driveway PTZ - Axis (16)	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0
	Driveway - Axis 6000e(C) (11)	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0
	Driveway - Axis 6000e(B) (10)	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0
	Driveway - Axis 6000e(D) (12)	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0
	Canoe - Dynamic Background (6)	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0
	School - Object Detection (25)	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0
	Driveway - Dahua (13)	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0
	CATOBSERVER Demo Server (5)	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0
	Perimeter - Axis	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0	100%	0
	Front Door - Entrance(31)	100%	0	99%	1	100%	0	100%	0	100%	0	100%	0	100%	0
	Kitchen Door - Hikvision	0%	0	0%	0	37%	0	60%	1	0%	0	0%	0	0%	0
	Driveway - Dahua PTZ (33)	100%	0	100%	0	100%	0	100%	0	99%	1	100%	0	100%	0

7.5 Database Usage Report

The **Database Usage Report** reports the database usage. There are options to customise how the usage report is delineated, and to export the report in CSV.



Report Type: Choose from one of the Database Report Types.

Notes: Add notes about the report, or describe why it is being fetched.

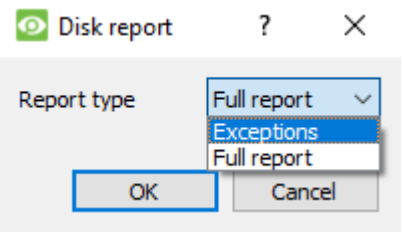
CSV: This will generate the information in Comma Separated Values, instead of a table. This is a standard representation of data and can be moved into a spread-sheet, if necessary.

7.5.1 Database Usage Report Example

Cathexis Demo				
CONTINUOUS RECDB				
Camera	**Size (MB)**	**Retention (days)**	**Rate (kbps)**	**Span**
Driveway - Dahua PTZ (33)	1058000	93.1	1077	2019/01/05 to 2019/04/08
Perimeter - Axis	596000	93.8	602	2019/01/04 to 2019/04/08
CATOBSERVER Demo Server (5)	2000	76.2	2	2019/01/22 to 2019/03/15
Driveway - Dahua (13)	2387000	93.1	2432	2019/01/05 to 2019/04/08
School - Object Detection (25)	420000	93.8	424	2019/01/04 to 2019/04/08
Canoe - Dynamic Background (6)	919000	93.8	929	2019/01/04 to 2019/04/08
Driveway - Axis 6000e(C) (11)	469000	93.0	477	2019/01/05 to 2019/04/08
Front PTZ - Truvision (19)	601000	93.1	612	2019/01/05 to 2019/04/08
Back Door Exit IMPRO (2)	256000	93.8	258	2019/01/04 to 2019/04/05
Driveway - Axis 6000e(A) (9)	358000	93.1	364	2019/01/05 to 2019/04/08
Front Door Exit IMPRO (18)	2000	25.9	7	2019/03/13 to 2019/03/29
Demo Room - Axis P3224 (8)	396000	93.8	400	2019/01/04 to 2019/04/08
Perimeter - Axis Q1615 (23)	979000	93.8	989	2019/01/04 to 2019/04/08
Back Parking - Vivotek (3)	2362000	93.0	2407	2019/01/05 to 2019/04/08
Highway SPEED DETECTION (20)	1654000	93.8	1672	2019/01/04 to 2019/04/08
Driveway PTZ - Axis (16)	1049000	93.0	1068	2019/01/05 to 2019/04/08
Driveway - Axis 6000e(B) (10)	545000	93.1	555	2019/01/05 to 2019/04/08

7.6 Disks Report

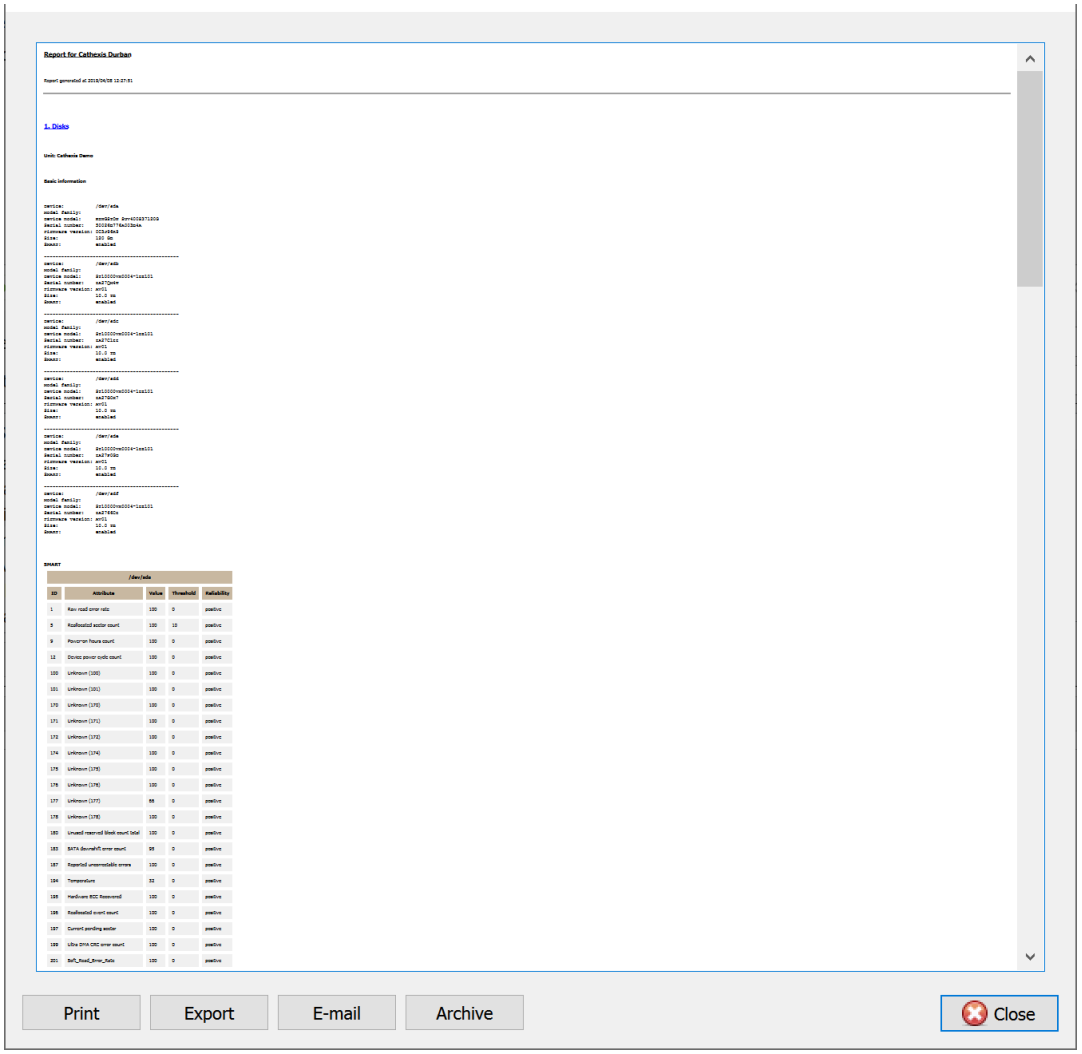
The **Disks Report** generates a report on the disks, depending on the report type that is chosen.



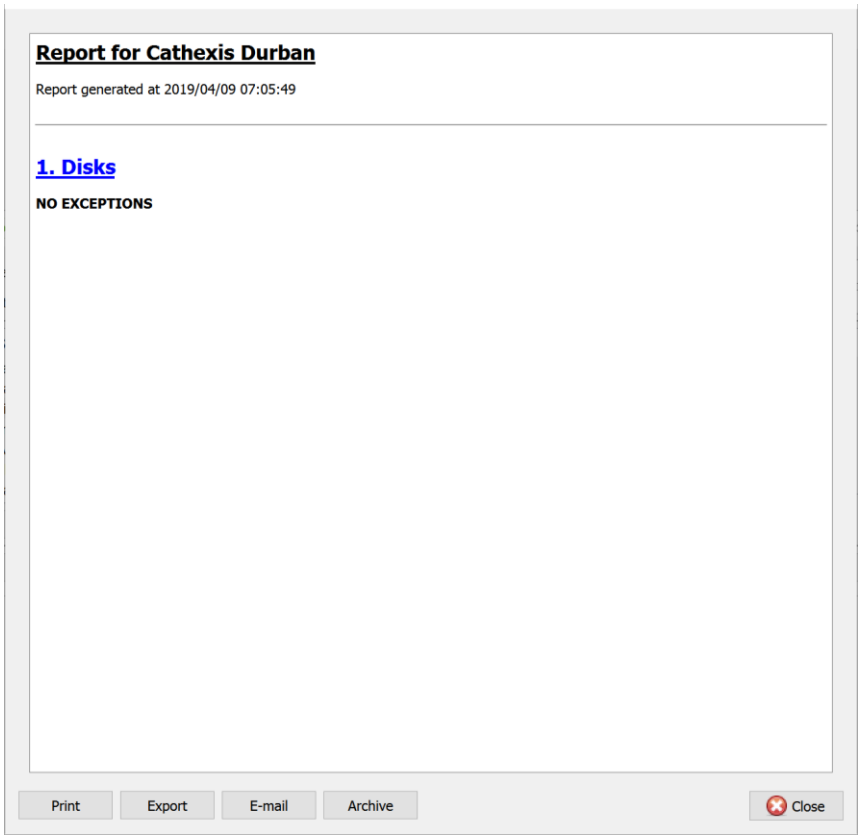
Full Report: This will contain all available information on all disks, including temperature and Raw Read Error Rates.

Exceptions: This will only display information regarding problematic drives.

7.6.1 Disks Full Report Example



7.6.2 Disks Exceptions Report Example



7.7 Environment Report

The **Environment Report** generates a report on the hardware components (such as fan speed, voltages, and CPU temperatures).

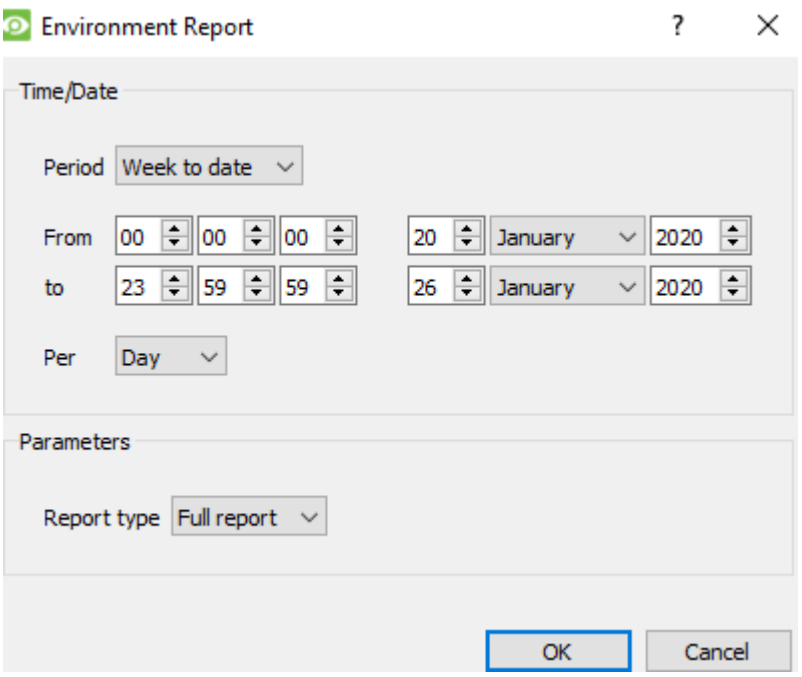
Note: Environment report is only available on supported Cathexis hardware.

Currently supported:

- DFI SB300
- DFI SB600

Supported from CathexisVision 2020.2 and later:

- DFI SB300
- DFI SB600
- DFI SD331

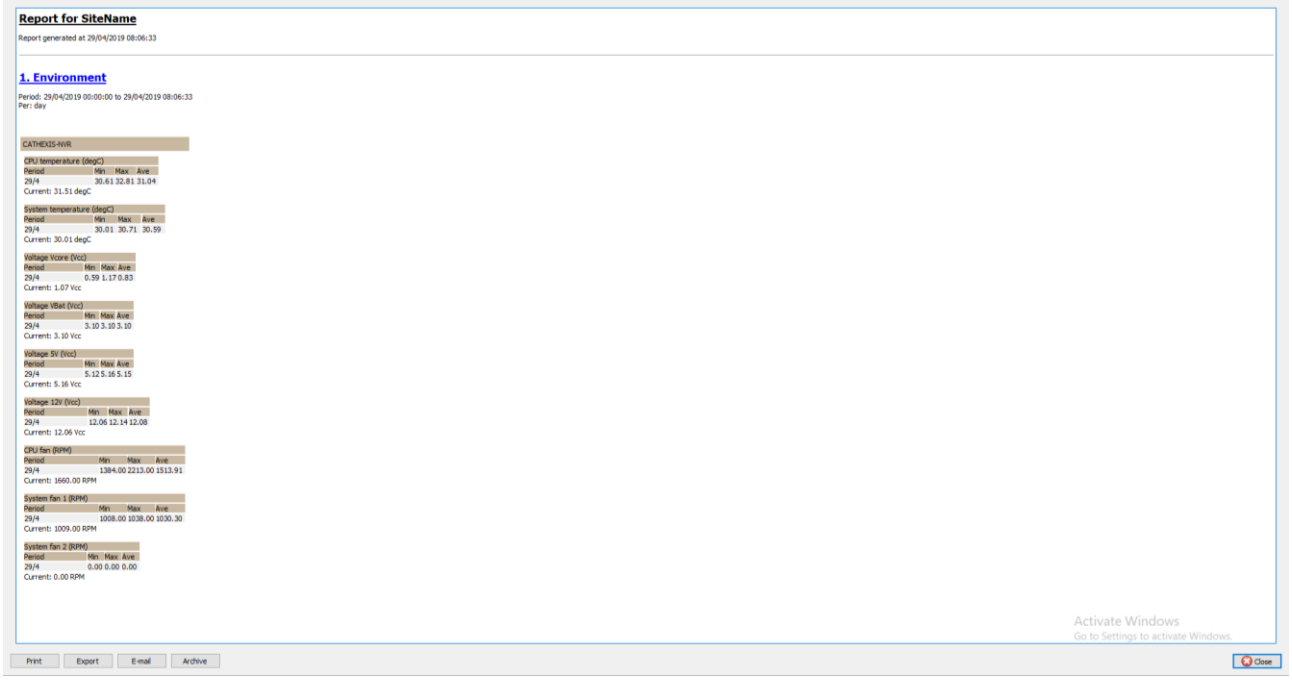


Select the report period. Then define the report type.

Full Report: This report shows details for all supported hardware components.

Exceptions: This report shows only the problem components.

7.7.1 Environment Report Example



Report for SiteName

Report generated at 29/04/2019 08:06:33

1. Environment

Period: 29/04/2019 00:00:00 to 29/04/2019 08:06:33
Per: day

CATHEXIS-NVR

CPU temperature (degC)

Period	Min	Max	Ave
29/4	30.61	32.81	31.04

Current: 31.51 degC

System temperature (degC)

Period	Min	Max	Ave
29/4	30.01	30.71	30.59

Current: 30.01 degC

Voltage Vcore (Vcc)

Period	Min	Max	Ave
29/4	0.59	1.17	0.83

Current: 1.07 Vcc

Voltage VBat (Vcc)

Period	Min	Max	Ave
29/4	3.10	3.10	3.10

Current: 3.10 Vcc

Voltage 5V (Vcc)

Period	Min	Max	Ave
29/4	5.12	5.16	5.15

Current: 5.16 Vcc

Voltage 12V (Vcc)

Period	Min	Max	Ave
29/4	12.06	12.14	12.08

Current: 12.06 Vcc

CPU fan (RPM)

Period	Min	Max	Ave
29/4	1384.00	2213.00	1513.91

Current: 1660.00 RPM

System fan 1 (RPM)

Period	Min	Max	Ave
29/4	1008.00	1038.00	1030.30

Current: 1009.00 RPM

System fan 2 (RPM)

Period	Min	Max	Ave
29/4	0.00	0.00	0.00

Current: 0.00 RPM

Activate Windows
Go to Settings to activate Windows.

Print | Export | E-mail | Archive | Close

7.8 Events Report

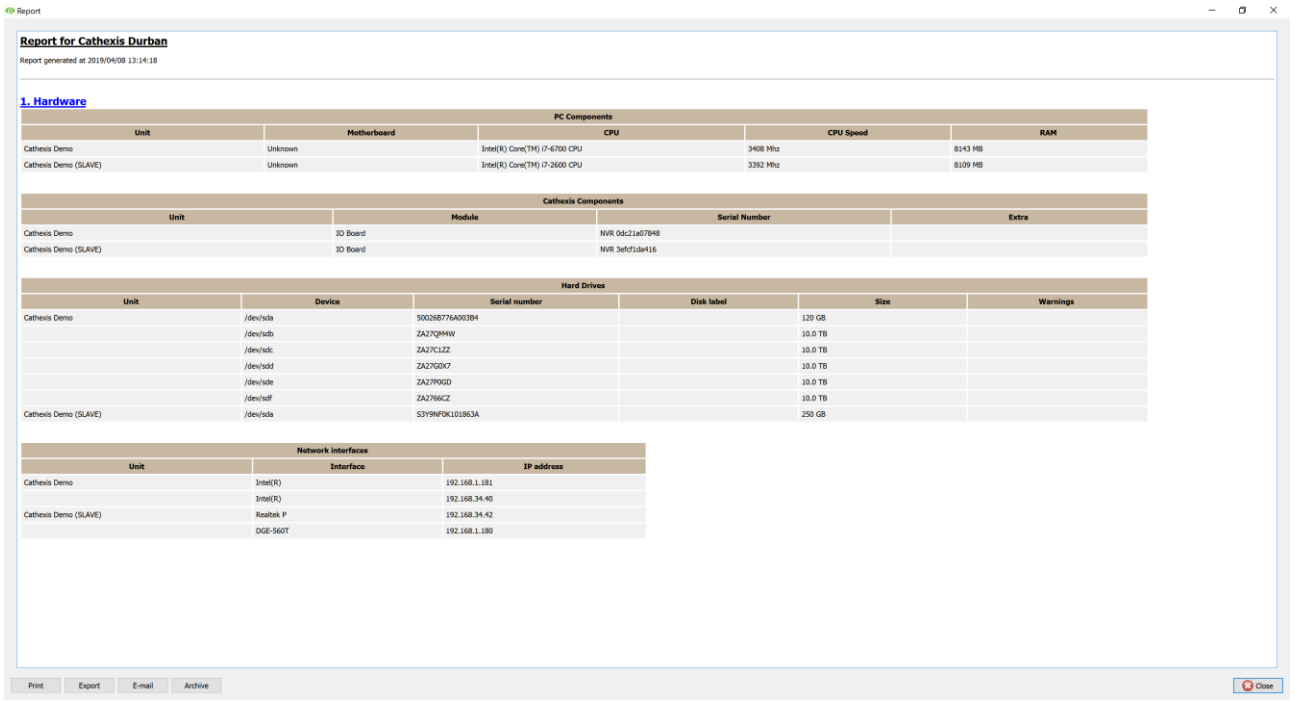
Events reports are only supported on NetBSD DVR Systems.

For event reports on all other supported systems, please consult the **Forensic Tool** section.

7.9 File System Report

The **File System Report** will fetch a full list of the relevant hardware components inside the servers. (This includes PC hardware and **Cathexis**-specific hardware). This report type is not configurable and is added straight to the template.

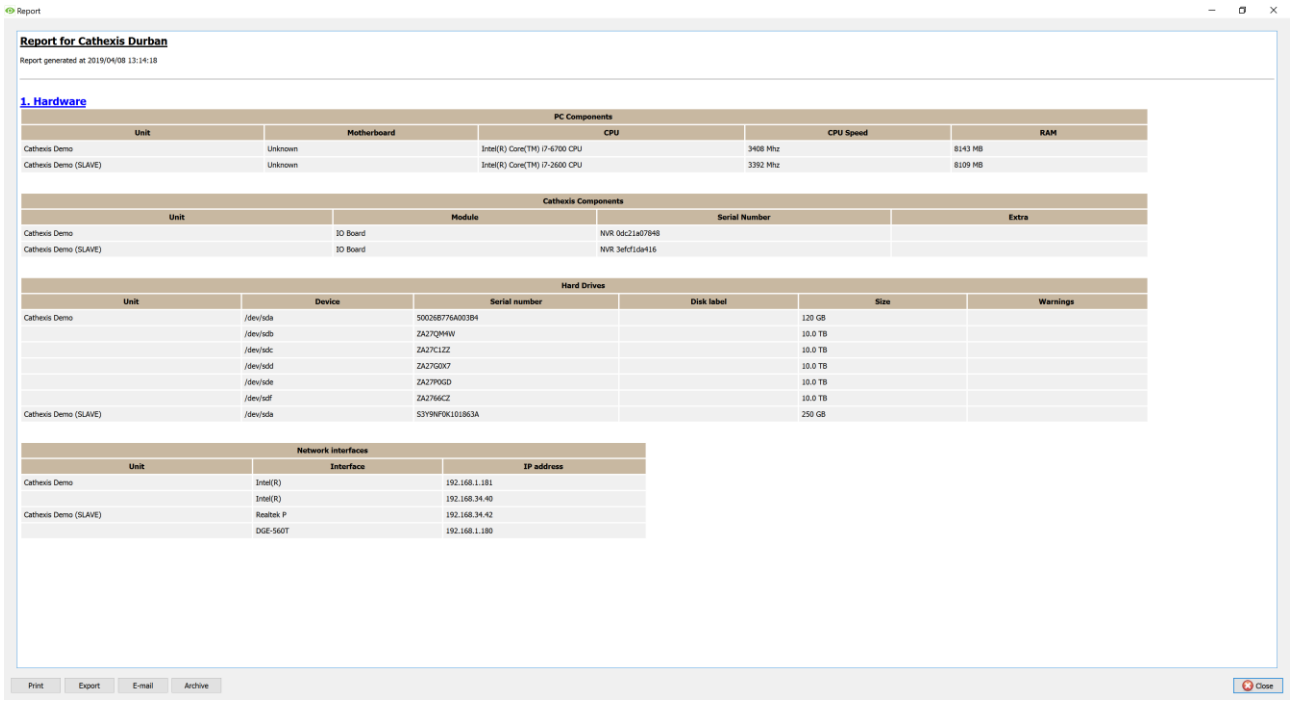
7.9.1 Hardware Report Example



7.10 Hardware Report

The **Hardware Report** fetches a full list of the relevant hardware components inside the servers. (This includes PC hardware and **Cathexis**-specific hardware). This report type is not configurable and is added straight to the template.

7.10.1 Hardware Report Example



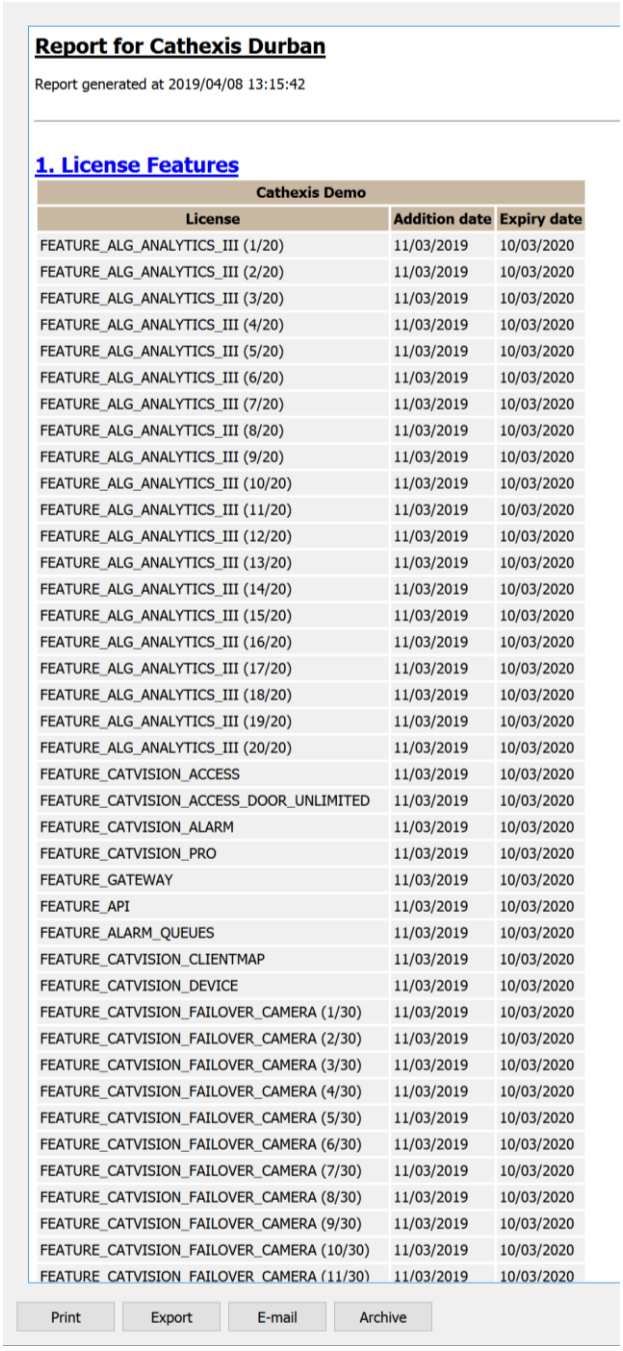
7.11 License Features Report

The **License Features Reports** generates a report for the site's license features.

Note: this report has been replaced by the updated 7.12 Licenses report, but is retained in the software in case users have previously configured and use this report.

This report is not configurable and is added straight to the template.

7.11.1 License Features Report Example



Report for Cathexis Durban

Report generated at 2019/04/08 13:15:42

1. License Features

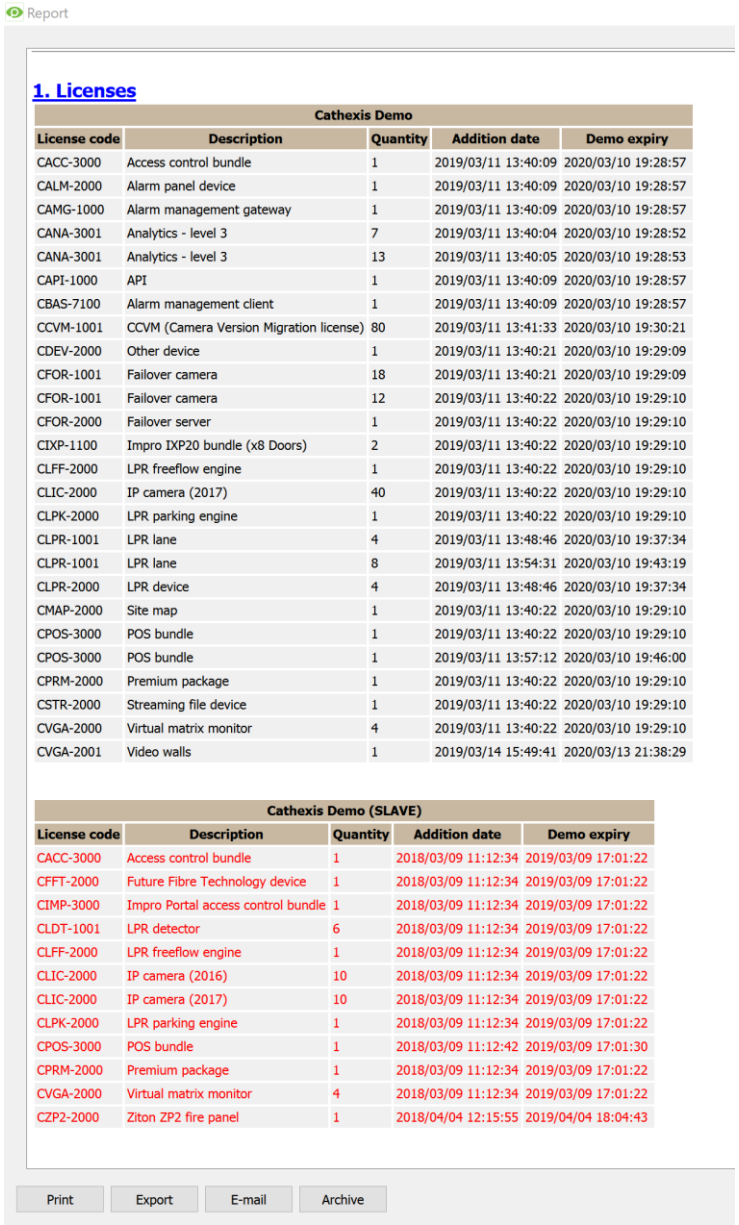
Cathexis Demo		
License	**Addition date**	**Expiry date**
FEATURE_ALG_ANALYTICS_III (1/20)	11/03/2019	10/03/2020
FEATURE_ALG_ANALYTICS_III (2/20)	11/03/2019	10/03/2020
FEATURE_ALG_ANALYTICS_III (3/20)	11/03/2019	10/03/2020
FEATURE_ALG_ANALYTICS_III (4/20)	11/03/2019	10/03/2020
FEATURE_ALG_ANALYTICS_III (5/20)	11/03/2019	10/03/2020
FEATURE_ALG_ANALYTICS_III (6/20)	11/03/2019	10/03/2020
FEATURE_ALG_ANALYTICS_III (7/20)	11/03/2019	10/03/2020
FEATURE_ALG_ANALYTICS_III (8/20)	11/03/2019	10/03/2020
FEATURE_ALG_ANALYTICS_III (9/20)	11/03/2019	10/03/2020
FEATURE_ALG_ANALYTICS_III (10/20)	11/03/2019	10/03/2020
FEATURE_ALG_ANALYTICS_III (11/20)	11/03/2019	10/03/2020
FEATURE_ALG_ANALYTICS_III (12/20)	11/03/2019	10/03/2020
FEATURE_ALG_ANALYTICS_III (13/20)	11/03/2019	10/03/2020
FEATURE_ALG_ANALYTICS_III (14/20)	11/03/2019	10/03/2020
FEATURE_ALG_ANALYTICS_III (15/20)	11/03/2019	10/03/2020
FEATURE_ALG_ANALYTICS_III (16/20)	11/03/2019	10/03/2020
FEATURE_ALG_ANALYTICS_III (17/20)	11/03/2019	10/03/2020
FEATURE_ALG_ANALYTICS_III (18/20)	11/03/2019	10/03/2020
FEATURE_ALG_ANALYTICS_III (19/20)	11/03/2019	10/03/2020
FEATURE_ALG_ANALYTICS_III (20/20)	11/03/2019	10/03/2020
FEATURE_CATVISION_ACCESS	11/03/2019	10/03/2020
FEATURE_CATVISION_ACCESS_DOOR_UNLIMITED	11/03/2019	10/03/2020
FEATURE_CATVISION_ALARM	11/03/2019	10/03/2020
FEATURE_CATVISION_PRO	11/03/2019	10/03/2020
FEATURE_GATEWAY	11/03/2019	10/03/2020
FEATURE_API	11/03/2019	10/03/2020
FEATURE_ALARM_QUEUES	11/03/2019	10/03/2020
FEATURE_CATVISION_CLIENTMAP	11/03/2019	10/03/2020
FEATURE_CATVISION_DEVICE	11/03/2019	10/03/2020
FEATURE_CATVISION_FAILOVER_CAMERA (1/30)	11/03/2019	10/03/2020
FEATURE_CATVISION_FAILOVER_CAMERA (2/30)	11/03/2019	10/03/2020
FEATURE_CATVISION_FAILOVER_CAMERA (3/30)	11/03/2019	10/03/2020
FEATURE_CATVISION_FAILOVER_CAMERA (4/30)	11/03/2019	10/03/2020
FEATURE_CATVISION_FAILOVER_CAMERA (5/30)	11/03/2019	10/03/2020
FEATURE_CATVISION_FAILOVER_CAMERA (6/30)	11/03/2019	10/03/2020
FEATURE_CATVISION_FAILOVER_CAMERA (7/30)	11/03/2019	10/03/2020
FEATURE_CATVISION_FAILOVER_CAMERA (8/30)	11/03/2019	10/03/2020
FEATURE_CATVISION_FAILOVER_CAMERA (9/30)	11/03/2019	10/03/2020
FEATURE_CATVISION_FAILOVER_CAMERA (10/30)	11/03/2019	10/03/2020
FEATURE_CATVISION_FAILOVER_CAMERA (11/30)	11/03/2019	10/03/2020

Print Export E-mail Archive

7.12 Licenses Report

The **Licenses Report** fetches a report on all the of all the licenses and their descriptions, on all of the units attached to the site. (This excludes the Base Stations.) This report is an update to the older License Features Report (7.11).

7.12.1 Licenses Report Example


Report

1. Licenses

Cathexis Demo				
License code	Description	Quantity	Addition date	Demo expiry
CACC-3000	Access control bundle	1	2019/03/11 13:40:09	2020/03/10 19:28:57
CALM-2000	Alarm panel device	1	2019/03/11 13:40:09	2020/03/10 19:28:57
CAMG-1000	Alarm management gateway	1	2019/03/11 13:40:09	2020/03/10 19:28:57
CANA-3001	Analytics - level 3	7	2019/03/11 13:40:04	2020/03/10 19:28:52
CANA-3001	Analytics - level 3	13	2019/03/11 13:40:05	2020/03/10 19:28:53
CAPI-1000	API	1	2019/03/11 13:40:09	2020/03/10 19:28:57
CBAS-7100	Alarm management client	1	2019/03/11 13:40:09	2020/03/10 19:28:57
CCVM-1001	CCVM (Camera Version Migration license)	80	2019/03/11 13:41:33	2020/03/10 19:30:21
CDEV-2000	Other device	1	2019/03/11 13:40:21	2020/03/10 19:29:09
CFOR-1001	Failover camera	18	2019/03/11 13:40:21	2020/03/10 19:29:09
CFOR-1001	Failover camera	12	2019/03/11 13:40:22	2020/03/10 19:29:10
CFOR-2000	Failover server	1	2019/03/11 13:40:22	2020/03/10 19:29:10
CIXP-1100	Impro IXP20 bundle (x8 Doors)	2	2019/03/11 13:40:22	2020/03/10 19:29:10
CLFF-2000	LPR freeflow engine	1	2019/03/11 13:40:22	2020/03/10 19:29:10
CLIC-2000	IP camera (2017)	40	2019/03/11 13:40:22	2020/03/10 19:29:10
CLPK-2000	LPR parking engine	1	2019/03/11 13:40:22	2020/03/10 19:29:10
CLPR-1001	LPR lane	4	2019/03/11 13:48:46	2020/03/10 19:37:34
CLPR-1001	LPR lane	8	2019/03/11 13:54:31	2020/03/10 19:43:19
CLPR-2000	LPR device	4	2019/03/11 13:48:46	2020/03/10 19:37:34
CMAP-2000	Site map	1	2019/03/11 13:40:22	2020/03/10 19:29:10
CPOS-3000	POS bundle	1	2019/03/11 13:40:22	2020/03/10 19:29:10
CPOS-3000	POS bundle	1	2019/03/11 13:57:12	2020/03/10 19:46:00
CPRM-2000	Premium package	1	2019/03/11 13:40:22	2020/03/10 19:29:10
CSTR-2000	Streaming file device	1	2019/03/11 13:40:22	2020/03/10 19:29:10
CVGA-2000	Virtual matrix monitor	4	2019/03/11 13:40:22	2020/03/10 19:29:10
CVGA-2001	Video walls	1	2019/03/14 15:49:41	2020/03/13 21:38:29

Cathexis Demo (SLAVE)				
License code	Description	Quantity	Addition date	Demo expiry
CACC-3000	Access control bundle	1	2018/03/09 11:12:34	2019/03/09 17:01:22
CFFT-2000	Future Fibre Technology device	1	2018/03/09 11:12:34	2019/03/09 17:01:22
CIMP-3000	Impro Portal access control bundle	1	2018/03/09 11:12:34	2019/03/09 17:01:22
CLDT-1001	LPR detector	6	2018/03/09 11:12:34	2019/03/09 17:01:22
CLFF-2000	LPR freeflow engine	1	2018/03/09 11:12:34	2019/03/09 17:01:22
CLIC-2000	IP camera (2016)	10	2018/03/09 11:12:34	2019/03/09 17:01:22
CLIC-2000	IP camera (2017)	10	2018/03/09 11:12:34	2019/03/09 17:01:22
CLPK-2000	LPR parking engine	1	2018/03/09 11:12:34	2019/03/09 17:01:22
CPOS-3000	POS bundle	1	2018/03/09 11:12:42	2019/03/09 17:01:30
CPRM-2000	Premium package	1	2018/03/09 11:12:34	2019/03/09 17:01:22
CVGA-2000	Virtual matrix monitor	4	2018/03/09 11:12:34	2019/03/09 17:01:22
CZP2-2000	Ziton ZP2 fire panel	1	2018/04/04 12:15:55	2019/04/04 18:04:43

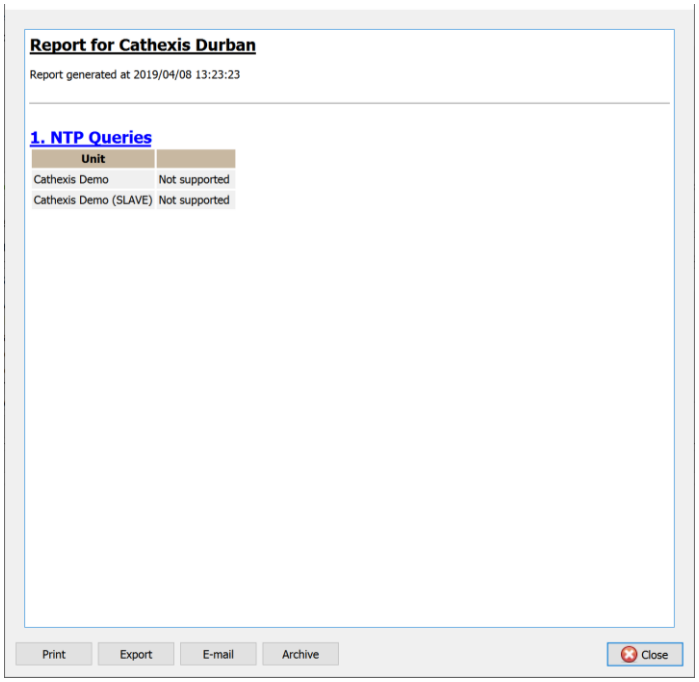
Print Export E-mail Archive

7.13 NTP Queries Report

If NTP has been setup, the **NTP Queries Report** generates a report for the NTP Queries for the site.

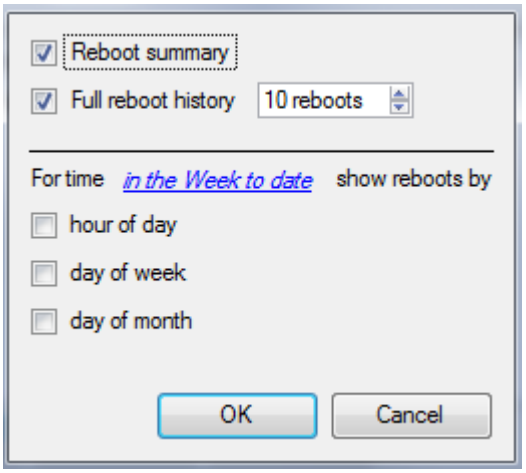
Note: this report is only applicable to NetBSD DVR systems.

7.13.1 NTP Queries Report Example



7.14 Reboots Report

The **Reboots Report** generates a report of the system reboots. It is important to monitor system reboots.



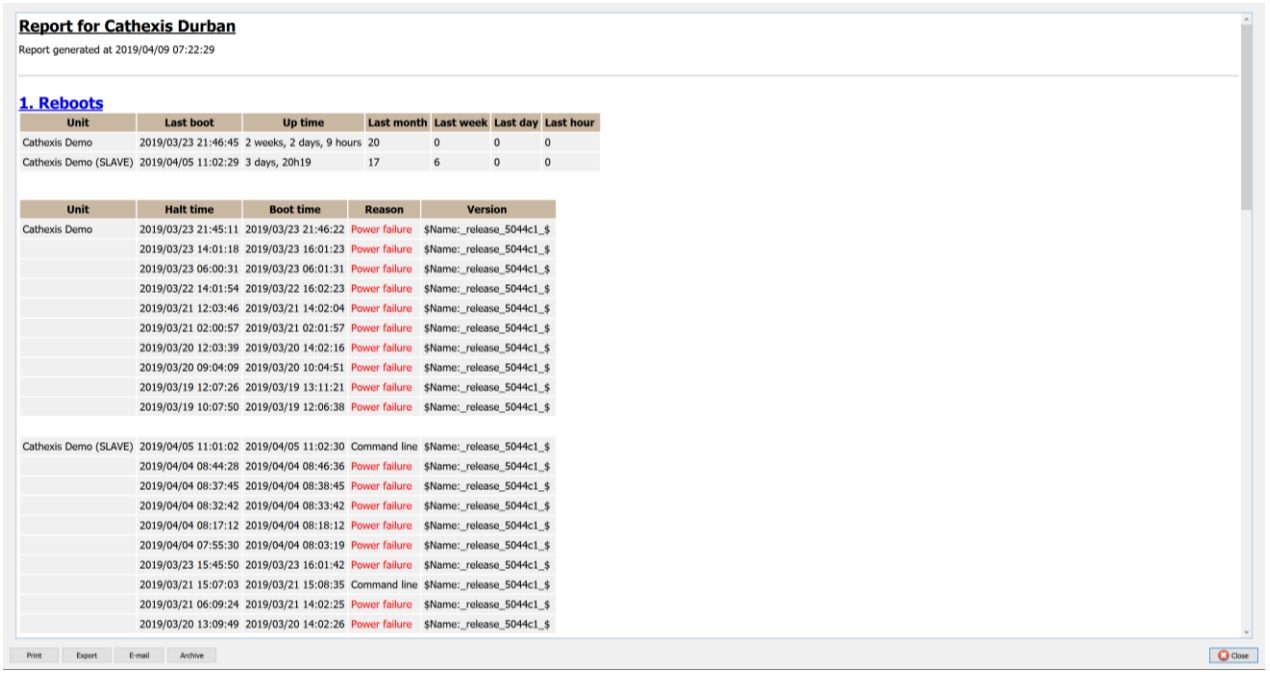
Reboot summary: Select to enable a Reboot Summary in the report,
Full reboot history: Select to enable a full reboot history. Specify the number of reboots to display in the report.

To change report period, click on the blue hyperlink: *in the Week to date*

This will open the calendar settings:

- **From-To** period (for example, from one date-and-time to another).
- From the **previous** X hours, or
- Over a **period** of time, starting at a set time, on a set day.

7.14.1 Reboot Report Example



Report for Cathexis Durban

Report generated at 2019/04/09 07:22:29

1. Reboots

Unit	Last boot	Up time	Last month	Last week	Last day	Last hour
Cathexis Demo	2019/03/23 21:46:45	2 weeks, 2 days, 9 hours	20	0	0	0
Cathexis Demo (SLAVE)	2019/04/05 11:02:29	3 days, 20h19	17	6	0	0

Unit	Halt time	Boot time	Reason	Version
Cathexis Demo	2019/03/23 21:45:11	2019/03/23 21:46:22	Power failure	$Name:_release_5044c1_$
	2019/03/23 14:01:18	2019/03/23 16:01:23	Power failure	$Name:_release_5044c1_$
	2019/03/23 06:00:31	2019/03/23 06:01:31	Power failure	$Name:_release_5044c1_$
	2019/03/22 14:01:54	2019/03/22 16:02:23	Power failure	$Name:_release_5044c1_$
	2019/03/21 12:03:46	2019/03/21 14:02:04	Power failure	$Name:_release_5044c1_$
	2019/03/21 02:00:57	2019/03/21 02:01:57	Power failure	$Name:_release_5044c1_$
	2019/03/20 12:03:39	2019/03/20 14:02:16	Power failure	$Name:_release_5044c1_$
	2019/03/20 09:04:09	2019/03/20 10:04:51	Power failure	$Name:_release_5044c1_$
	2019/03/19 12:07:26	2019/03/19 13:11:21	Power failure	$Name:_release_5044c1_$
	2019/03/19 10:07:50	2019/03/19 12:06:38	Power failure	$Name:_release_5044c1_$
Cathexis Demo (SLAVE)	2019/04/05 11:01:02	2019/04/05 11:02:30	Command line	$Name:_release_5044c1_$
	2019/04/04 08:44:28	2019/04/04 08:46:36	Power failure	$Name:_release_5044c1_$
	2019/04/04 08:37:45	2019/04/04 08:38:45	Power failure	$Name:_release_5044c1_$
	2019/04/04 08:32:42	2019/04/04 08:33:42	Power failure	$Name:_release_5044c1_$
	2019/04/04 08:17:12	2019/04/04 08:18:12	Power failure	$Name:_release_5044c1_$
	2019/04/04 07:55:30	2019/04/04 08:03:19	Power failure	$Name:_release_5044c1_$
	2019/03/23 15:45:50	2019/03/23 16:01:42	Power failure	$Name:_release_5044c1_$
	2019/03/21 15:07:03	2019/03/21 15:08:35	Command line	$Name:_release_5044c1_$
	2019/03/21 06:09:24	2019/03/21 14:02:25	Power failure	$Name:_release_5044c1_$
	2019/03/20 13:09:49	2019/03/20 14:02:26	Power failure	$Name:_release_5044c1_$

Print Export E-mail Archive Close

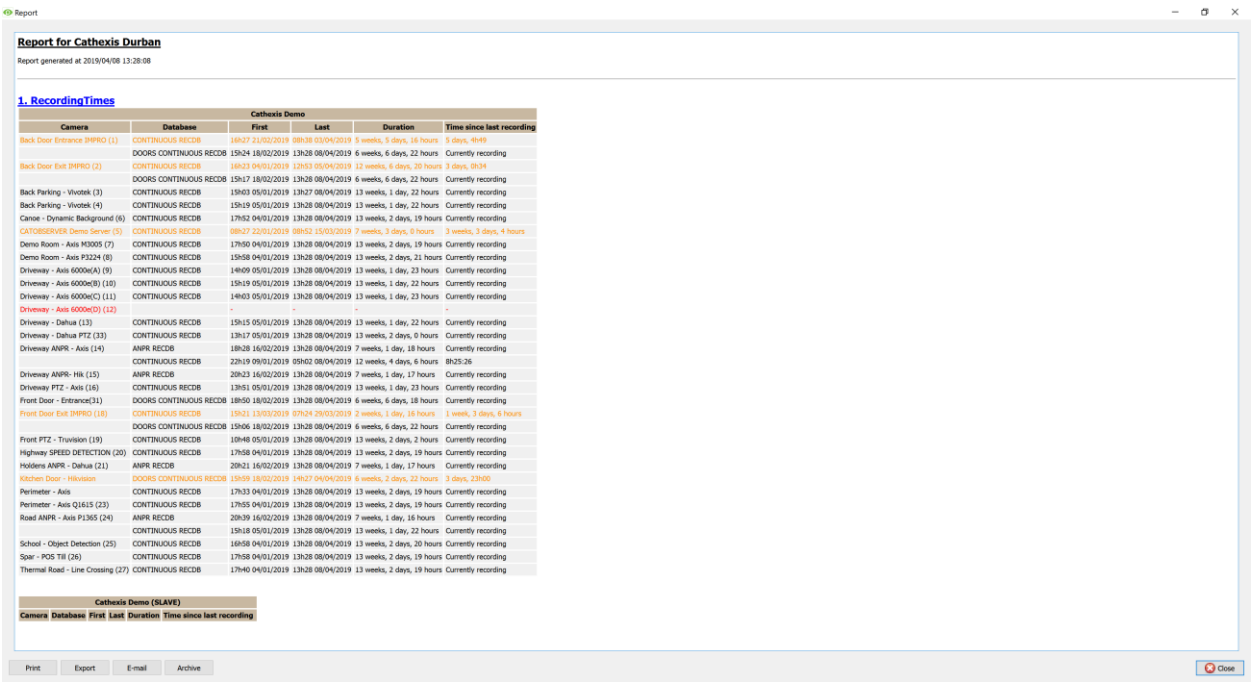
7.15 Recording Times Report

The **Recording Times Report** generates a report on the amount of time each camera, on each server, has spent recording. This report is not configurable and is added straight to the template.

Note:

1. Cameras that did not record are included and highlighted in red.
2. Cameras that have not recorded in the last day are highlighted in orange.
3. Cameras are listed alphabetically.

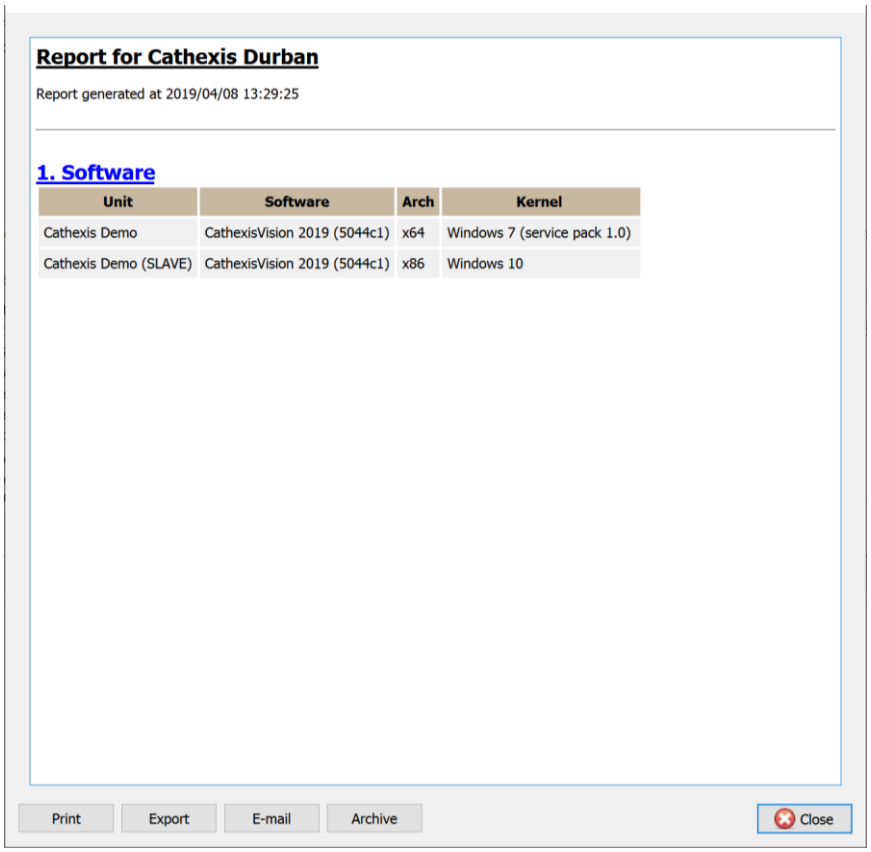
7.15.1 Recording Times Report Example



7.16 Software Report

The **Software Report** lists the version of **CathexisVision** running on each server. This report is not configurable and is added straight to the template.

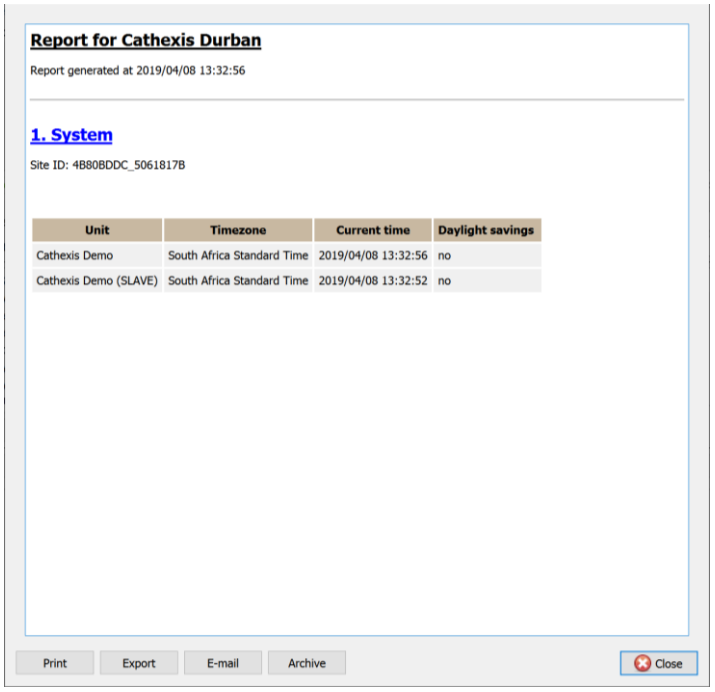
7.16.1 Software Report Example



7.17 System Report

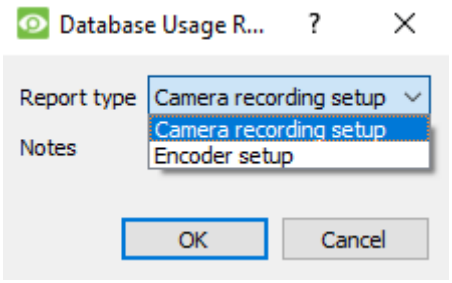
The **System Report** lists the information relating to the Time Zone (Time, Time Zone, Daylight Savings). This report is not configurable and is added straight to the template.

7.17.1 System Report Example



7.18 System Setup Report

The **System Setup Report** relates to the cameras and encoders attached to the system, and how they are set up. There are two options a **Camera Recording Setup** report, and an **Encoder Setup** report.



Camera Recording Setup — This retrieves all the information related to the actual recording of images, such as the frame-rate of recording, the pre-event recording time, and the post-event recording time.

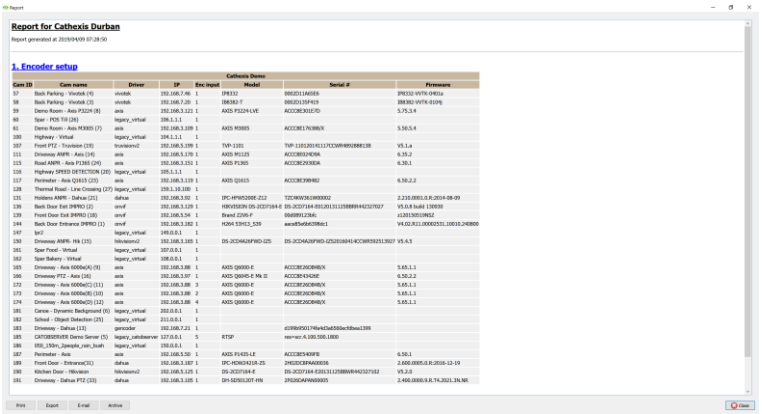
Encoder Setup — This retrieves all the information related to the setup of the encoders, such as the type of encoder, the IP address of the encoder, the name of the camera, which input it represents (physical input on the encoder), and the firmware.

7.18.1 System Setup: Camera Recording Setup Report Example

Report for Cathexis Durban

1. Camera recording setup

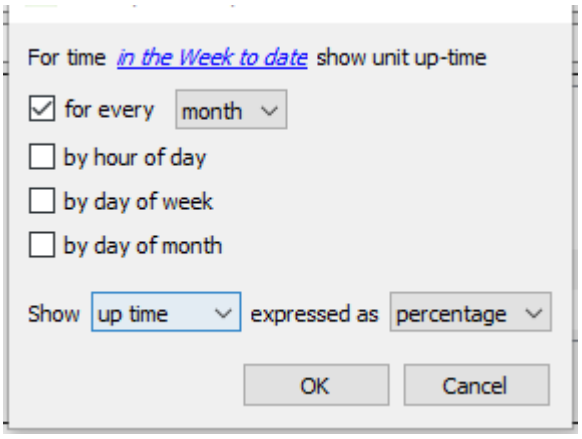
7.18.2 System Setup: Encoder Setup Report Example


Report for Cathexis Durban

1. Encoder setup

7.19 Unit Up-Time Report

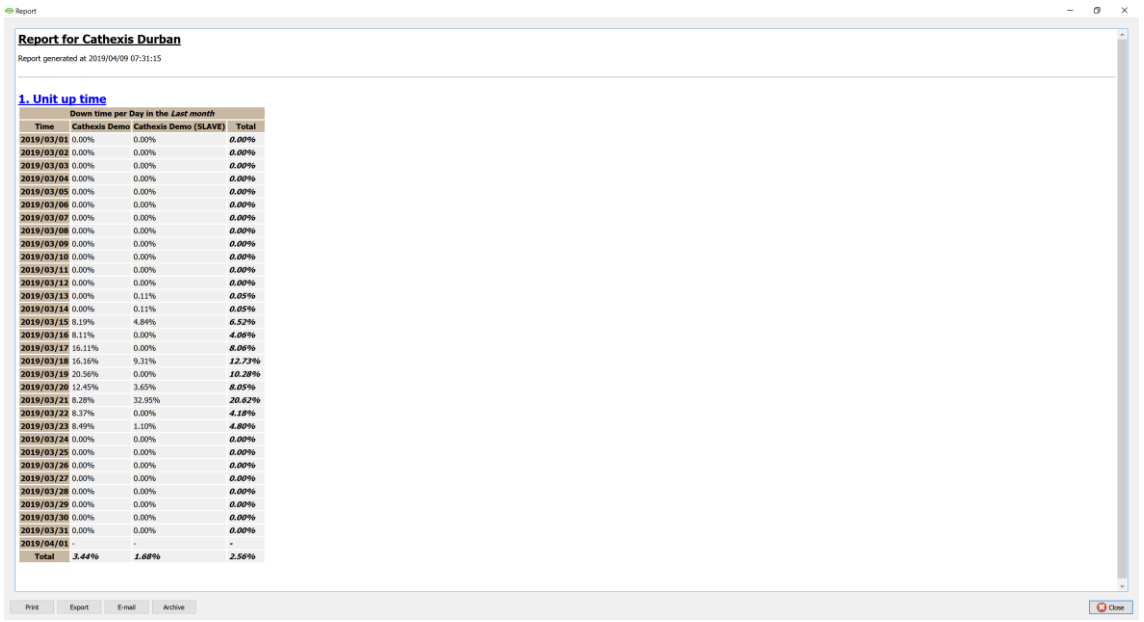
Up-Time is the amount of time that the unit stays on between reboots or failures. It is similarly important to Reboots.



Click on the blue hyperlink to define the report period. Define the rest of the settings.

Select whether to report on **Up-time** or **Down-time**. Choose whether to express the results in time or in percentage.

7.19.1 Unit Up-time Report Example



Report for Cathexis Durban

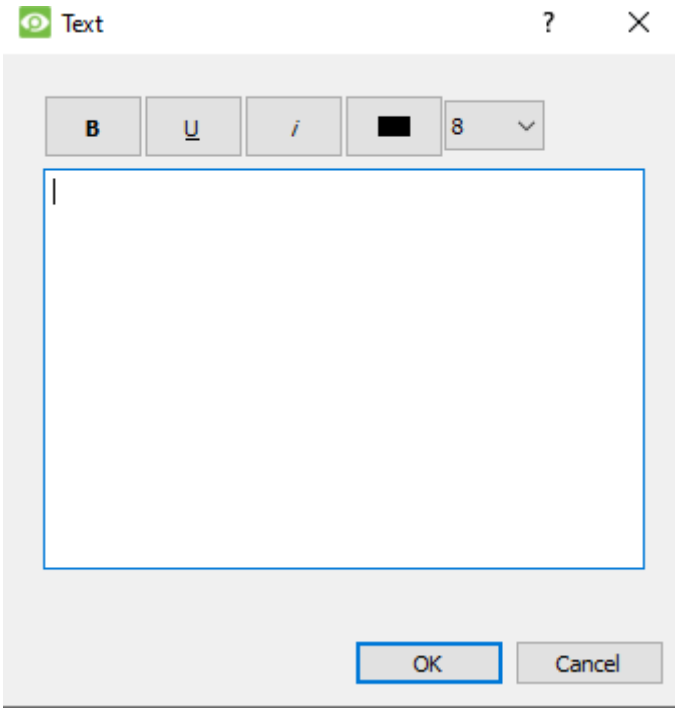
Report generated at 2019/04/09 07:31:15

1. Unit up time

Down time per Day in the *Last month*			
Time	Cathexis Demo	Cathexis Demo (SLAVE)	Total
2019/03/01	0.00%	0.00%	*0.00%*
2019/03/02	0.00%	0.00%	*0.00%*
2019/03/03	0.00%	0.00%	*0.00%*
2019/03/04	0.00%	0.00%	*0.00%*
2019/03/05	0.00%	0.00%	*0.00%*
2019/03/06	0.00%	0.00%	*0.00%*
2019/03/07	0.00%	0.00%	*0.00%*
2019/03/08	0.00%	0.00%	*0.00%*
2019/03/09	0.00%	0.00%	*0.00%*
2019/03/10	0.00%	0.00%	*0.00%*
2019/03/11	0.00%	0.00%	*0.00%*
2019/03/12	0.00%	0.00%	*0.00%*
2019/03/13	0.00%	0.11%	*0.05%*
2019/03/14	0.00%	0.11%	*0.05%*
2019/03/15	8.19%	4.84%	*6.52%*
2019/03/16	8.11%	0.00%	*4.06%*
2019/03/17	16.11%	0.00%	*8.06%*
2019/03/18	16.16%	9.31%	*12.73%*
2019/03/19	20.56%	0.00%	*10.28%*
2019/03/20	12.45%	3.65%	*8.05%*
2019/03/21	8.28%	32.95%	*20.62%*
2019/03/22	8.37%	0.00%	*4.18%*
2019/03/23	8.49%	1.10%	*4.80%*
2019/03/24	0.00%	0.00%	*0.00%*
2019/03/25	0.00%	0.00%	*0.00%*
2019/03/26	0.00%	0.00%	*0.00%*
2019/03/27	0.00%	0.00%	*0.00%*
2019/03/28	0.00%	0.00%	*0.00%*
2019/03/29	0.00%	0.00%	*0.00%*
2019/03/30	0.00%	0.00%	*0.00%*
2019/03/31	0.00%	0.00%	*0.00%*
2019/04/01	-	-	-
Total	*3.44%*	*1.68%*	*2.56%*

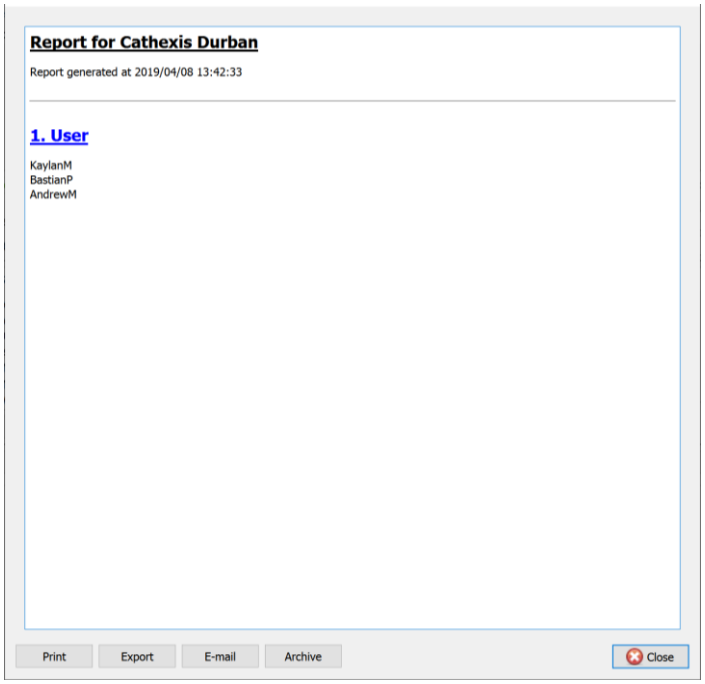
Print Export E-mail Archive Close

7.20 User-Defined Report

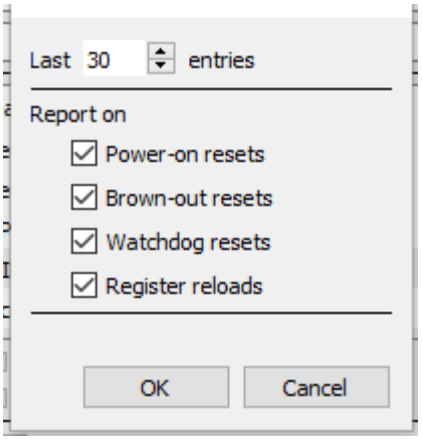


The **User-Defined Report** allows the user to enter custom text that will be added as a text section in the report.
This is useful when adding general notes or information to the report.

7.20.1 User Defined Report Example



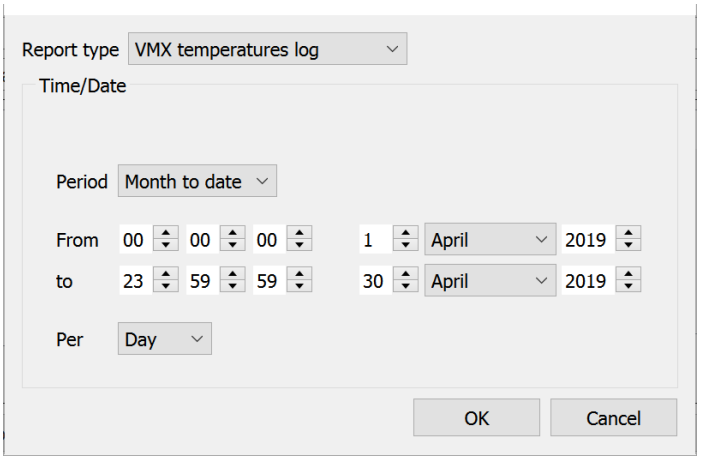
7.21 VMX Counters Report



The **VMX Counters Report** generates a report on the Video Matrix (VMX) Counters on the unit.

Note: this is only used for troubleshooting statistics for DVRs with an installed Cathexis Video Matrix.

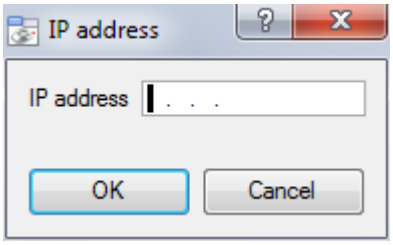
7.22 VMX Temperature Report



The **VMX Temperature Report** generates a report for the Video Matrix (VMX) Temperature on the unit, according to the configured options.

Note: this only applies to DVRs with an installed Cathexis Video Matrix.

7.23 Windows Unit Report



The **Windows Unit Report** pulls information for Windows Base Stations that use the site.

This includes hardware and software information about the Base Station, as well as the **CathexisVision** applications that it has been using.

8. Setup Tab: Failover Servers

8.1 Failover Introduction

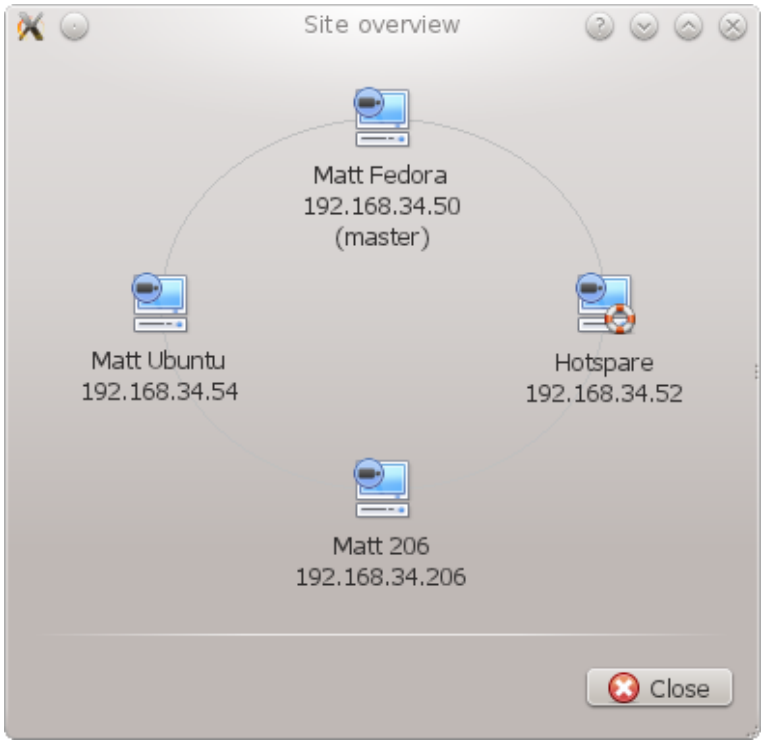
8.1.1 Model

Cathexis uses a **hotspare model** for failover. In this model, failover servers monitor the recording servers. When a recording server is down, one of the failover servers takes over the functions of the failed recording server.

In failover mode, the failover server operates exactly like the failed recording server. The site continues to function as if the recording server had not failed. Video is buffered on the failover server, and re-inserted into the original recording server's database when it restarts.

It is possible to have multiple failover servers monitoring a site. More failover servers mean less risk of downtime.

Note: One failover server can only take over the function of a single recording server at a time.



The image above shows a site in **normal configuration**. The Hotspare is available to take over the functions of a Recording Server.

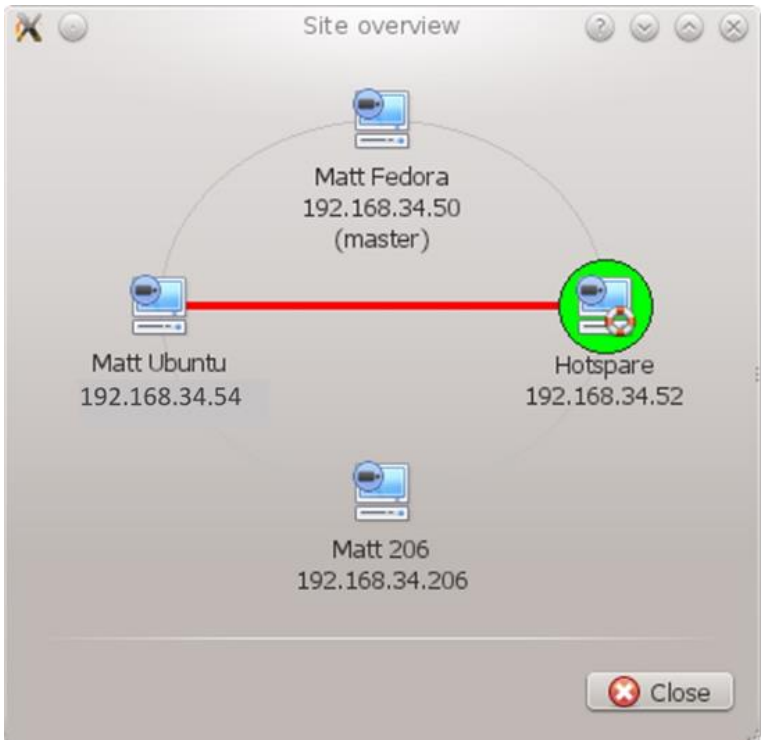
Note: there are different IP addresses for the Recording and Hotspare servers.

The failover unit is represented by the unit icon to the left.
It is distinguished from regular units by the lifebuoy image.

***Note**: if necessary, a hotspare can:

- search for recording servers at specific IP addresses. This is required when broadcast/multicast packets are not received due to the network layout.
- be configured to only monitor a subset of recording servers on the site.

***For instructions on configuring these features, refer to Appendix C.**



The image above shows a site in **failover configuration**. The Hotspare Server has now assumed the functions of the failed Recording Server 192.168.34.54. The Hotspare Server could assume the functions of either of the Recording Servers.

8.1.2 Licensing

Each failover server requires a failover server license (using **CFOR-2000**), and an adequate number of failover camera licenses (**CFOR-10xx**).

Note: The failover servers and camera licenses are all loaded onto the site master server.

1. The number of failover camera licenses must be equal to, or greater than, the number of cameras on the recording server that is to be failed over. (In other words, if a recording server has more cameras than there are failover camera licenses, it will not get failed over.)
2. If there are multiple failover servers, the failover camera licenses will be distributed evenly between them. (For example, with 3 failover servers and 90 failover camera licenses, each failover server will get 30 camera licenses).
3. All Cathexis SAM encoders require failover licenses. Licenses are required per channel.

Note: Before the failover server is licensed, the status bar license warning will be red. If it is expanded, the description should be that the failover server is unlicensed. By adding the required number of failover camera licenses, the status bar license warning should disappear.

8.1.3 Recommendations

When configuring a site with failover, do the following to maximise system up-time:

1. Have a highly reliable site master. This is important for two reasons:
   a. External viewers connect to the site using the IP address of the site master. If the site master fails, the external connections fail.
   b. The site master disseminates the information of the site to the slaves on the site. When the site master is down, this dissemination does not happen and the site operates sub-optimally.
2. Do not attach any cameras to the site master. Disable failing over of the site master. (Therefore, if the site master does fail, it does not use one of the failover servers that could be used for a recording server.)
3. Configure VGA monitors on the site master.
4. Storage space: there needs to be enough recording storage on the failover server to serve for the maximum expected downtime of the most active unit being failed over. (If it is expected to have a maximum of one day's downtime, there must be sufficient storage to serve for this period.)

8.1.4 Minimising Failover Loss

Failover loss is less than 30 seconds, during the switch from one server to the next.

To ensure that there is **zero failover loss**: ensure that relevant cameras have been configured for continuous recording to an SD card on the camera.

If continuous recording to an SD card on the camera is configured, the footage is also accessible from the user interface. This covers the loss of 30 seconds (or less) during the server switchover.

8.1.5 Limitations

- Servers with frame-grabber cards (AVM/VOM) cannot be failed over.
- The recording server needs to use the 'Advanced' database for reinsertion. This is standard for CathexisVision 2015 and onwards.

8.1.6 Example

Single site with the following:

2x NVRs with 64 cameras on each (one is the site master NVR)

1x NVR with 50 cameras

1x NVR with Gateway

Single server Failover setup:

1x Failover NVR with 64 Failover Camera licenses (assuming provision for only a single server failure at any one time).

Multiple server failover setup:

To have failover on all 4 site NVRs simultaneously, 4 failover servers with 256 Failover Camera Licenses (4 x 64) are required. The camera licenses are shared across all failover servers. Since the maximum number on a single server is 64, all servers must have access to 64 camera licenses.

The Gateway WIN7 machine, if part of the site, will be failed over. However, the Gateway functionality will not be functional due to the IP address change. There is therefore no advantage in having Failover on this unit for its Gateway functionality. If the Gateway PC was excluded from the site then only 3 x Failover Servers and 192 x Failover Camera Licenses (3 x 64) would be required.

8.2 Setup

8.2.1 Introduction

The failover configuration has two levels:

1. The failover server software needs to be installed on the failover NVR or NVRs.
2. The site needs to be configured to have access to the available failover server or servers.

8.2.2 Requirements

Ensure that the failover and recording server (NVR) times are synchronised.

It is essential to synchronise the times, so that the database items recorded to the failover server can be correctly re-inserted into the recording server's database.

8.2.3 Configuration

8.2.3.1 Failover NVR Configuration

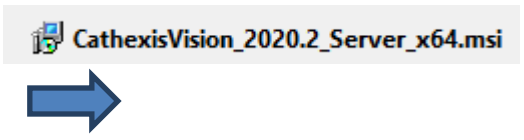
A CathexisVision failover server is installed with the regular CathexisVision installer. After installation, when the GUI is running, a message should pop up that states: "This server is running as a hotspare".

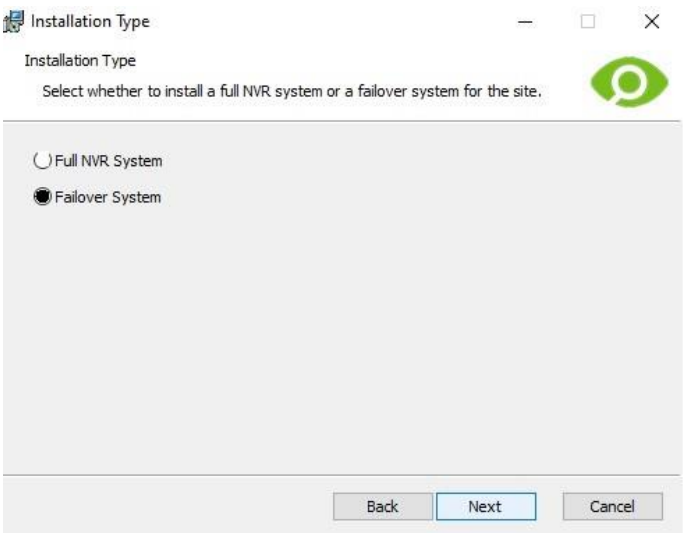
8.2.3.1.1 Install the CathexisVision Software

The CathexisVision software will need to be installed on the failover server.

During the installation process, there will be a prompt to choose between a **Full NVR System** and a **Failover System.**

For this installation, choose the **Failover System**.





8.2.3.1.2 Check Installation

After a successful installation, the user can check the installation by attempting to run CathexisVision.

When the user double-clicks on the CathexisVision icon, the dialogue box shown on the right will appear:

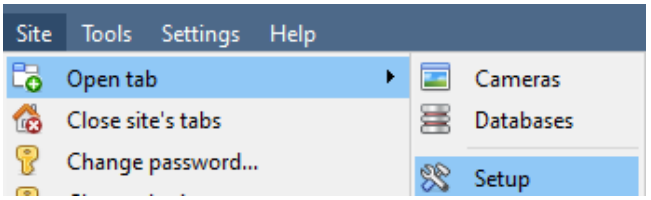
8.2.3.1.3 Site Failover Configuration

Each unit failed over will need to be configured. All failover servers are added to the site on the site master.

It is not required to configure individual master/slave recording servers for failover setup.

8.2.3.1.4 Open the Failover Panel

To open the Failover setup, follow the instructions below.

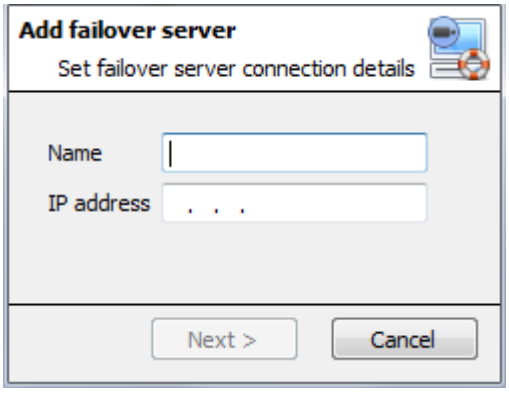


After logging into the site, open the Configure Server by clicking on **Site / Open Tab / Setup.**

In the Setup Tab, click on the Configure Failover Servers icon.

Note: Right-click on the tab of any open site to bring up the same menu as the one accessed via the method above.

8.2.3.1.5 Add a Failover Server



Click on **New** to open the dialogue to add a new failover server.

Add a descriptive **name** for the failover unit.

Enter the **IP address** of the failover unit.

Click **Next** to proceed to adding the failover database.

8.2.3.1.6 Configure Failover Network Interface

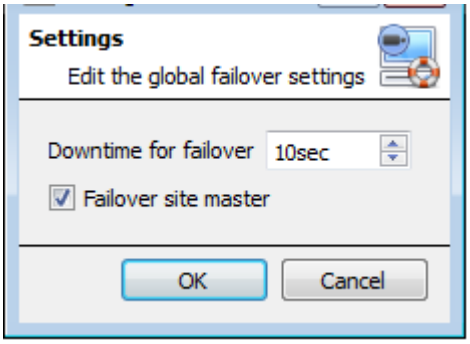
When a failover server has multiple network interfaces, it can be configured to use one of them when registering itself in the site.

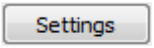
Click on the **Edit** button. Click on the **Network Interfaces** tab.

From the drop-down menu, select the required network adaptor.

Note: If left on **Auto**, the system will try to match the failover server's network card to one of the available network adaptors. This can cause problems: if the network card or adaptor is not correctly labelled, the incorrect adaptor could be selected. **To prevent this,** the user is advised to select the correct network adaptor.

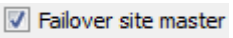
8.2.3.1.7 Define the Global Failover Settings





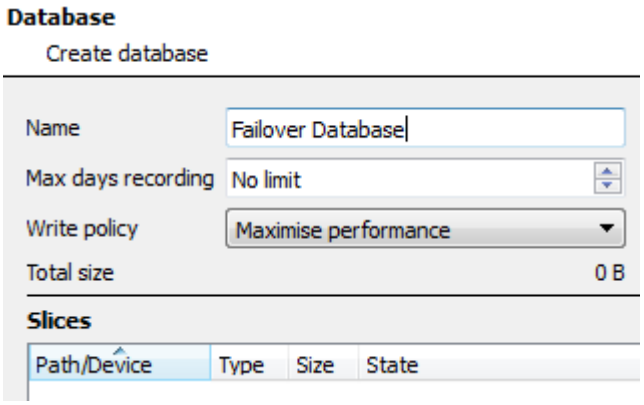
In the Failover panel, click on **Settings**.

Define the duration of **downtime** that is required for the failover server to take over.



Select **Failover site master** to failover the site master unit. (**Note:** outside connectivity will be lost when the site master is in failover.)

8.2.3.1.8 Database

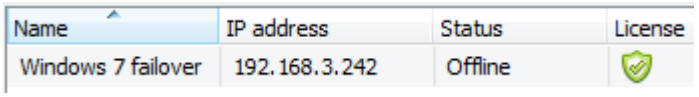


This database resides on the failover server.

The larger the database, the more recording it can do in its capacity as a failed over unit.

Note: This dialogue will only appear when editing a newly-created failover server.

8.2.3.1.9 Check that server is online



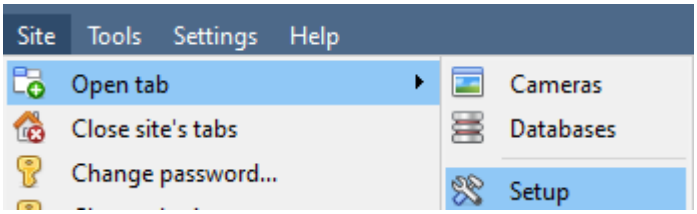
Once the server has been added, its status and licensing can be seen in the Failover panel.

8.2.3.1.10 Failover Insert Database

When the failed over server comes back online, the recordings that were stored on the Failover NVR will be moved back to the server. Many servers will have multiple active databases. Select which database these recordings get inserted into.

The time taken for inserting the video from the NVR into the database is dependent on the current load on the recording server. As this is a lower priority process, it may be delayed by current, higher priority tasks.

Navigate to the Databases Panel

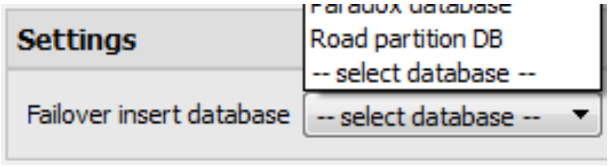


After logging into the site, to open Configure Server simply click on **Site / Open Tab / Setup.**

In the Setup Tab, click on the Configure Servers icon.

Expand the server.
Left-click on **Databases**:

Select the Insert Database



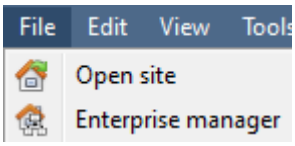
At the bottom of the databases panel, the Failover settings section will be visible.

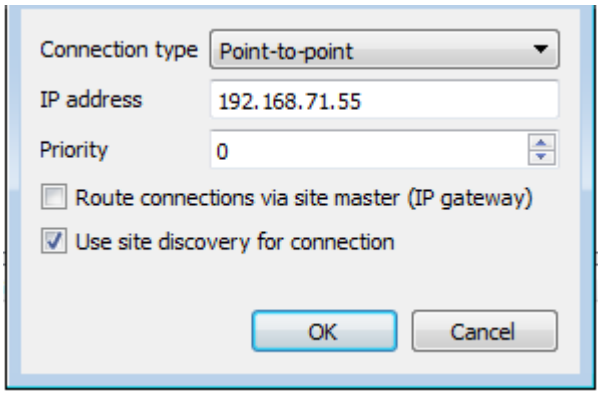
Click on “Select database” and select the database to reinsert the failed over recordings into.

8.2.3.1.11 Client Viewer Settings

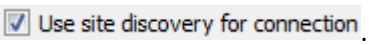
If the failover is set up so that the site master will also be failed over, the **Use site discovery for connection** option must be checked. This is important because, when a unit is failed over, its IP address will change. If this option is not enabled, and the site master gets failed over, the client will have the wrong target address for the master unit. If this happens, the client will not be able to access the site.

To do this:





1. Open the **Enterprise manager,** via the File menu.
2. Select site from the Site panel.
3. Right-click on the target IP address, and click on **Properties**.
4. In the connection properties dialogue check the option titled **Use site discovery for connection**



8.2.3.1.12 Site Master Settings

Set up the Site Master to generate a Technical Alarm, if any of the failover servers are down. For more information on this, please refer to the Technical Alarms section of **Configure Servers** (4.13 **Technical Alarms)**.

8.3 System Restore after Failover

Note: it is vital that system restore points are correctly managed for each and every site recording server for the effective configuration restore of failed recording servers. Offsite backup of restore files is strongly recommended.

The **Configuration Backup** settings are found on the **Site** / **Setup** / **Configure servers** / **Server (Master).** After clicking on the master server, click on the **Configuration Backup tab**. Database settings are not automatically backed up and restored, and will need to be manually reconfigured.

8.3.1 Restoring a Site Master Recording Server

If a full repair of the Site Master Server was required, then after reloading all the original software, do a system restore from the server itself to the most recent restore point.

If the motherboard of the server required replacement, then new licenses will need to be issued from support@cat.co.za linked to the new MAC address of the master server. The databases will need to be reconfigured from the Site Setup menu.

Once the repaired Site Master Recording Server is running, and reconnected **with its original IP address**, the failover server will stop failing over the old site master server and dump the recordings made during the failover process onto the new site master. The failover server will revert back to monitoring all the servers on the site.

Note:

- Ensure that the new unit's IP address is the same as the previous master unit.
- Install the correct software version (new installation, without config).
- Apply a restore point from the old site master.
- License the new unit, contact support.
- At this point, the site should be back online and the hot spare should no longer be failing over the old master unit.
- Create new databases.
- Select a database to insert failover recordings into.
- Ensure that all events and recordings point to the new database.

8.3.2 Restoring a Site Slave Recording Server

If a full repair of a Site Slave Server was required, then after reloading all the original software, do a system restore from the slave server itself to the most recent restore point. The databases will need to be manually reconfigured from the Site Setup menu on the slave server.

On the site master server under **SETUP / SERVERS**, right-click on the old slave server and select “Replace Server” which will insert the new slave server into the site as the failed server replacement. Once the new slave server is registered and running, the failover server will relinquish control and dump the recordings from the failover operation onto the new slave server. The failover server will revert back to monitoring all the servers on the site.

Note:

- Ensure that the new slave unit has appropriate IP settings for the network.
- Ensure the correct software version installed, and no previous configuration.
- Apply a restore point from the original slave unit onto the replacement unit.
- The Failover server needs to be taken offline before the slave unit can be replaced.
- Bring the failover back online after the unit has been replaced.
- The Slave unit will need to be re-licensed; clients will have to contact support. **Licensing** / **Advanced** / **Repair this unit's license.**
- Create new databases.
- Recordings need to be edited to point to the new DATABASE.

9. Setup Tab: Adjacent Cameras

9.1 Introduction

The adjacent cameras feature allows the spatial relationship between cameras on a site to be defined and used as a means of swiftly navigating between cameras based on a camera's physical position.

Consider an example in which a site operator observes a suspicious person wandering around the rooms in an office building. If the operator wants to follow the person on the camera monitors, they will be able to click on red arrows in the live (or review) camera view, which will then move to cameras physically related (North/South/East/West etc.) to the current camera.

Operators can change the way that adjacent cameras are displayed in the resources panel by selecting the Adjacent cameras option from the drop-down resources list.

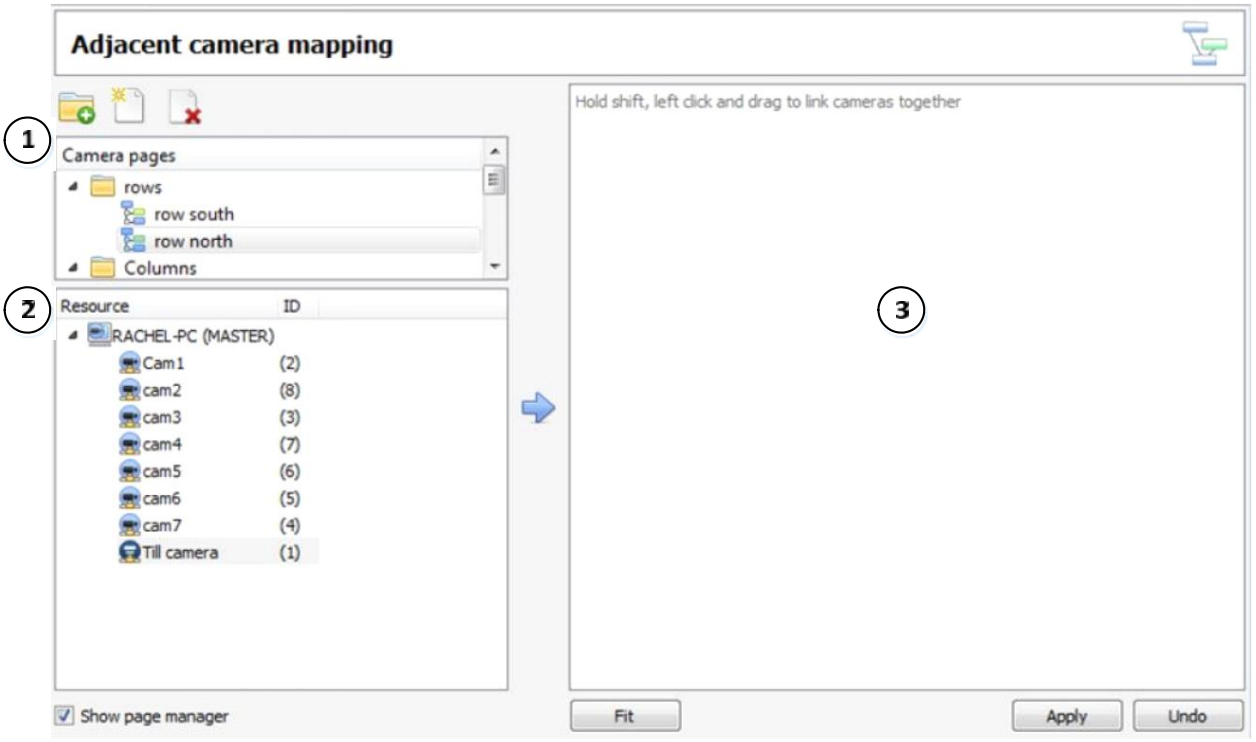
There is also a shortcut to Adjacent Camera Mapping on the left-hand side of the GUI.

If selected, adjacent cameras will be displayed with live/review thumbnails, which the operator can then select to navigate to.

9.2 Setup

Click on the **Adjacent camera mapping** icon in the left panel of the Setup tab. The screen below will be presented.

9.2.1 Interface



	Area	Description
1	**Page Manager**	Show page manager Check **Show page manager** to display this panel. From this zone, create folders and pages into which adjacent cameras can be grouped. Add a new folder Add a new page Delete selected page
2	**Resource List**	All camera resources which have been added to the system are available for mapping here.
3	**Camera Mapping Area**	Highlight desired cameras and click the arrow to add them to this area to be mapped.
	Fit	Clicking this will scale the mapped cameras to **fit** in the screen.
	Apply	**Apply** all changes made.
	Undo	**Undo** all changes. Click this before applying changes in order for them to take effect.

9.2.2 Map Cameras

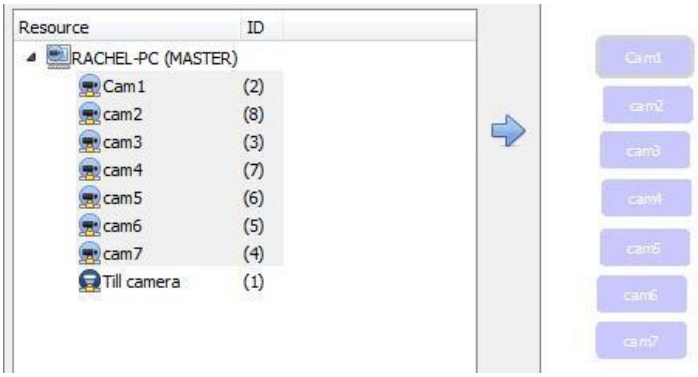
In order to map the adjacent cameras, **add the cameras** to the blank area, **link the cameras** and then **edit the camera relationships.**

9.2.2.1 Add Cameras

In the Resource list, select the cameras to map.

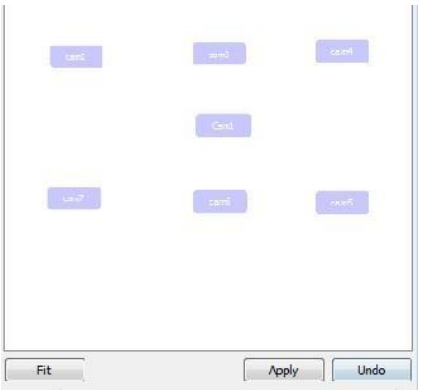
Click the **arrow** icon to add the cameras to the mapping area.

The cameras will then appear in the area in the order in which they appear in the resources list. Organise the cameras according to their physical locations.



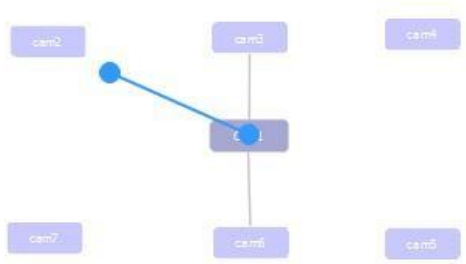
9.2.2.2 Organise Cameras

To organise the cameras, simply click on the camera name and drag it to the desired position. See below for an example:



9.2.2.3 Link Cameras

Next, link the adjacent cameras. To do so, click on the first camera while holding shift, and then drag to the second camera.



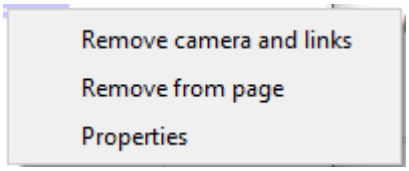
A blue line appears when linking cameras.

Cameras that have already been linked are connected by a grey line.

The directional relationships between linked cameras need to be configured. Right-click on the camera and select **Properties**.

9.2.2.4 Camera Right-Click Options

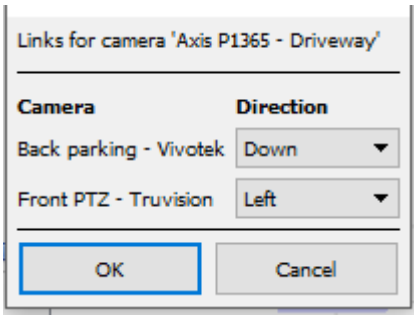
Right-clicking on a camera will offer the following options:



Remove camera and links will delete the selected camera and all its links (but not linked cameras).
Remove from page will simply remove the selected camera from the page but will not delete it from the map.
Properties will open the Edit camera relationships window. See below.

9.2.2.4.1 Properties: Edit Camera Relationships

In order to get the shortcut navigation arrows on the camera view, configure the directional relationship between each linked camera.



The linked cameras are displayed in the **Camera** column.

From the drop-down menu, select the direction of the relationship between cameras.

Once finished, click **Apply** to save or **Undo** to reset.

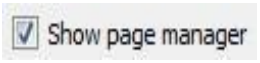
9.2.2.5 Variable Zoom Control

Click **control-mouse wheel scroll** for variable zoom control.

For more extensive camera organisation, see the next section on the **Page Manager**.

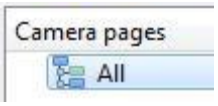
9.2.3 Page Manager

In Page Manager, it is possible to organise linked cameras into groups, which are user-defined.



Check **Show page manager** to display the Page Manager panel.

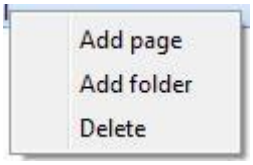
The default page is **All**, in which all cameras are grouped by the system. Selecting this page will display all cameras and their links in the mapping area.



9.2.3.1 Organise Cameras into Folders / Pages

One may extensively organise cameras into pages, which can then be grouped in folders and sub-folders.

9.2.3.1.1 Edit Pages and Folders

	Button	Right-click
Add Page		
Add Folder		
Delete (page/folder)		

9.2.3.1.2 Add Cameras to Pages

Cameras must be added to a page which is then added to a folder.

Select the newly created page.

Then, in the Resources list, select the desired cameras and click the **arrow icon** to add them to the blank mapping area.

If links and relationships are already configured, they will be retained here.

Lastly, cameras must be spatially organised in order to reflect their directional relationships. As before, click and drag the cameras to the desired positions.

10. CathexisVision GUI Setup

10.1 Introduction

This section deals with performing setups within the CathexisVision graphical user interface, as well as some other special setups which affect the way the system and/or GUI function.

If information is not available in this document, it may be information that relates to the operation of the **CathexisVision** GUI. This information is in the ***CathexisVision Operator's Manual***.

10.1.1 Supported Languages

The CathexisVision GUI supports the following languages:

- Arabic,
- Croatian,
- German,
- English,
- French,
- Hungarian,
- Italian,
- Portuguese,
- Russian,
- Spanish.

To change the language of the GUI, follow **Settings Menu / General** / **Language**, and consult the General Settings (10.4.7.1) section for more a more detailed description of this menu.

10.1.2 Minimising the GUI

It is not recommended to minimise the CathexisVision GUI in Windows. If the application is minimised, and an event occurs, a notification will popup only if there is no other active application running. The taskbar will flash indicating there is a message in CathexisVision, but the popup will not appear on top of other open applications.

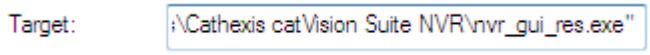
This is because Microsoft Windows does not allow applications to interrupt the user's current task. If the flashing taskbar is not sufficient, a Windows registry entry (**HKCU \ Control Panel \ Desktop \ ForegroundLockTimeout**) can be changed in order to get the window to become active if an event notification occurs.

10.2 Command Line Options

There are a number of options in **CathexisVision,** which need to be enabled/started via additional command line options. These can be added to the target paths of the shortcuts used to open the **CathexisVision** GUI.

To edit the shortcut, do the following:

Right-click on the **CathexisVision** icon, and click on **Properties** in the context menu.
In the Shortcut options tab that is opened, see the following entry:



Add the extra commands after the **"at** the end of the shortcut. Remember to leave a space between commands added to the target.

Note: Add multiple options to the end of the target by leaving a space between each option.

10.2.1 Connect Client to Alarm Gateway

Connecting to the alarm gateway can be done by following **Settings Menu / General / Connect to alarm gateway**. See the Menu Bar section under GUI Setup for more information. Enabling the gateway using this method will override settings configured in CathexisVision.

Simply add an IP address to connect to the Alarm gateway.

10.2.2 Set Number of Monitors

The default number of simultaneously reviewable cameras in **CathexisVision** is 6. For the most part this is sufficient, but to increase this limit, do so by entering the following into the target:

forms x

Here "x" represents the number of monitors **CathexisVision** will occupy when it starts up.

Note: This option will override the settings configured in the CathexisVision software under **Settings / General / Number of forms**.

10.2.3 Add Multiple CathexisVision GUIs

Add the following to the target path to have multiple **CathexisVision** GUIs open simultaneously:

user1, user2, userX

10.2.4 View Legacy Archive Viewer

By default, the legacy archive viewer will not be present from 2016 onwards. In order to see it in the GUI, the user will have to add the following command line argument:

legacy_archive_viewer

10.3 Send Text Message when Alarms are Received

The system may be configured to send a text message (SMS) when it receives an alarm. This would typically be applied to a system running as a gateway, which receives alarms for a site. However, an NVR could also be configured as a local base-station which receives site alarms (see Configure Servers for information on base-stations). The system sends text messages using a modem, or similar SMS device.

Configuration of the system to send text messages upon receipt of alarms is done by editing certain settings files in the CathexisVision installation folder. This section describes the processes of editing these settings files to configure the system to send text messages.

10.3.1 Supported Platforms

10.3.1.1 Supported Platforms

Windows and Linux.

10.3.1.2 Supported Software

CathexisVision 2014.4 and later.

10.3.1.3 Supported Modems

For supported / tested modems, consult this page: https://integrations.cathexisvideo.com/supported-integrations/modem/

10.3.2 Settings Files Location

Unless a different installation folder was selected during the install process, the default path is:

C:\Program Files\CathexisVision Server

Currently, only the GSM modem (connected to a serial port) is supported.

10.3.3 Configure Notifying Alarms

The settings file must be edited in order to configure which alarms will generate SMS notifications, and to whom they will be sent. Changes made to the settings file will reflect immediately. The CathexisVision software does not need to be restarted for these changes to take effect.

Please rename the file below in order for it to become active in CathexisVision. See instruction below.

Required File	alarm_rx_sms.txt.example This file needs to be renamed in order to become active in CathexisVision. Rename it as below.	
Rename:	alarm_rx_sms.txt	
Default Location	C:\Program Files\CathexisVision Server\settings	
Structure	# comment recipient xxxx [alarm type] [alarm type] [alarm type] # comment recipient yyyy [alarm type] [alarm type]	
File Configuration Guide		
# comment	Add a comment about the particular alarm configuration in the settings file. E.g., the name or position of the recipient. Any text following the hash (#) symbol will only be read as comment in the file and will not be included in the SMS notification.	
Recipient xxxx	Replace [xxxx] with the cell phone number to which SMS notifications should be sent. Multiple recipients receiving the same or separate alarms may be added. See 10.3.3.1.3 Example 3, below.	
[alarm type]	Replace [alarm type] with the parameters required to cause an SMS to be sent. Multiple parameters may be set. Options are:	
	tech	Enter this to specify that technical alarms will send SMS notifications.
	event low/medium/high	Enter [event low/event medium/event high] (either one, all, or a combination) to specify that event alarms with corresponding priority levels will send SMS notifications. **Note**: Event priority levels are set up when configuring events. See the Events section of this manual.

	event all	Enter [event all] to specify that all event alarms (regardless of whether a priority level has been configured) will send notifications.
	pattern abc	Enter [pattern abc], where [abc] is the event description. This is used to further refine which alarms will send notifications. **Note**: 1. Event descriptions are setup when configuring events. See the Events section of this manual. 2. The pattern uses regular expression to match the pattern to the event description. 3. Regular expressions are case sensitive. Ensure the pattern case matches that of the event description.

10.3.3.1 Examples

Below are examples of possible file configurations.

10.3.3.1.1 Example 1: Specified Alarms

Structure	Description
recipient 062123456 tech	The specified recipient will receive SMS notifications for all technical alarms.
recipient 064987654 event low event high	The specified recipient will receive SMS notifications for all events marked as 'low priority' and 'high priority' in CathexisVision.

10.3.3.1.2 Example 2: Alarm Description Pattern

Structure	Description
recipient 0837654321 tech event all pattern beware	The specified recipient/s will receive SMS notifications for all event and technical alarms, but only if the alarm description/s start with "beware."

10.3.3.1.3 Example 3: Multiple Recipients

Multiple recipients can be entered into the settings file. Recipients (and alarm parameters) must be listed individually in the file, even for multiple recipients receiving the same alarms:

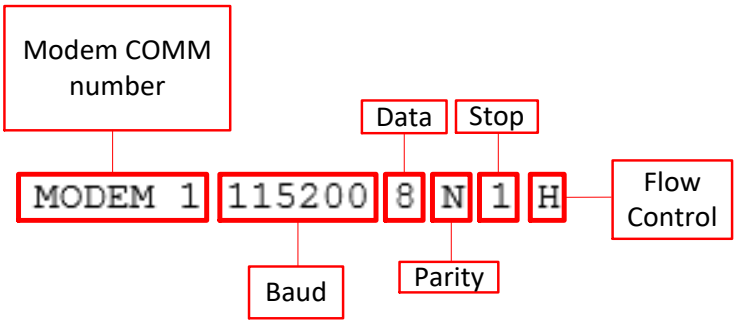
Structure	Description
recipient 0837654321 tech event all pattern beware recipient 08664537865 tech event all pattern beware recipient 0728078654 tech event all pattern beware recipient 0843928080 event medium recipient 0617654387 event high	In this example, many recipients are listed. The first three recipients will all receive SMS notifications for the same alarms, while the fourth and fifth will receive an SMS notification for a different alarm.

10.3.3.1.4 Example 4: Comment

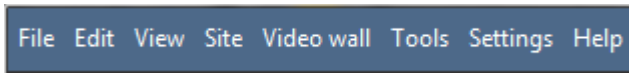
Structure	Description
# Daryl Smith – Line Manager recipient 0837654321 tech event all	The text following the hash (#) symbol is a comment in the file (and not included in the SMS). In this example, the recipient will receive an SMS notification for all technical alarms and all events. The comment in the file indicates the recipient's name and position in the company, and is useful for internal reference.

10.3.4 Configure Text Message Device

The text messaging (SMS) device needs to be configured to send text messages. This is done by editing the settings file. Changes made to the settings file will reflect immediately. The CathexisVision software does not need to be restarted for these changes to take effect.

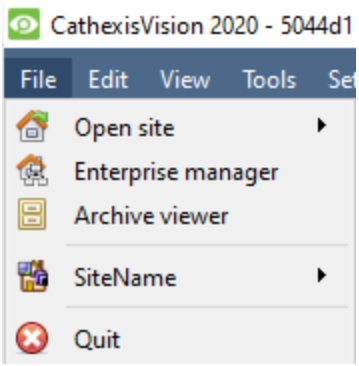
Required File	**sms_device.txt.example** This file needs to be renamed in order to become active in CathexisVision. Rename it as below.
Rename:	**sms_device.txt** (Remove the 'example' from the original file name.)
Default Location	C:\Program Files\CathexisVision Server\settings
Structure	---------- # Format for specifying a modem: # MODEM COMM BAUD DATA PARITY STOP FLOW_CONTROL # PARITY=(N)one/ (O)dd / (E)ven # FLOW_CONTROL= (H)ardware / (S)oftware / (N)one # eg MODEM 1 115200 8 N 1 H = COMM 1 at 115200 baud 8N1 with hardware flow control MODEM 1 115200 8 N 1 H ----------
Description	This settings file should indicate the Modem Comm, Baud, Data, Parity, Stop bit, and Flow Control for the relevant modem. Once the file is edited with the appropriate details, the file should only contain a single line indicating these settings. Taking the example above, delete everything in the file except for the last line: [MODEM 1 115200 8 N 1 H] Edit this line with the relevant modem details. See below for a breakdown. 

10.4 Menu Bar



This will detail the different options available to the user through the menu bar of the **CathexisVision** GUI.

10.4.1 File Menu



10.4.1.1 Open Site

The menu attached to this tag will be a list of the Sites that have been added to this unit.

10.4.1.2 Enterprise Manager

The enterprise manager is where all Site management occurs. Add/edit/remove sites, as well as create site folders.

The assignation of Resource Sites occurs in the Enterprise Manager as well.

10.4.1.3 Archive Viewer

This will open up the Archive Tab. Any archived video can be viewed here.

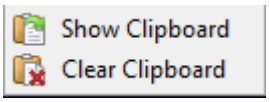
10.4.1.4 Open Site List

The names under Archive Viewer and above Quit represent the Sites that currently have connection tabs open in the GUI.

10.4.2 Edit Menu

The edit menu, in general only displays the Show Clipboard, Clear Clipboard options. When the Enterprise Manager is open, there will be a range of different options.

10.4.2.1 General Edit Menu



The only information contained on the clipboard in question will be when a screen grab is captured from one of the cameras in the Cameras Tab.

10.4.2.2 Enterprise Manager Edit Menu

Show/ Clear Clipboard will show or clear the clipboard

New/Edit/Delete Site will add a new Site; edit an existing Site, or delete an existing Site.

New Connection will add a unit connection to the selected Site.

Fetch Site ID gives a created site an ID, which is essential for a site to run. Perform this after creating the site, and adding unit connections to it.

Make Resources Site will make a site a Resources Site for this unit. This allows the unit to display a Video Wall, Alarm Management Gateway, and Maps Tab for this site.

Clear Resources site will clear resources site for this unit.

New Folder. Organise Sites in the Site List into folders.

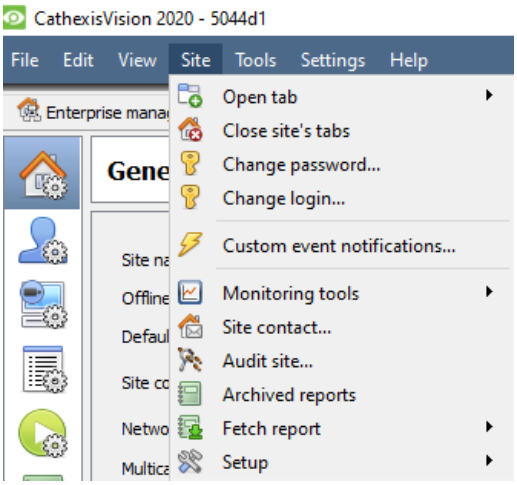
Highlight Level will highlight all Sites where X level is authorised.

10.4.3 View Menu

The only option available here is the option to change the GUI view to Full-screen.

10.4.4 Site Menu

The site menu will relate to the site whose tab is currently being viewed. To open a new Site, follow **File / Open Site/ Site Name.** Get this same menu, from a list of all currently open sites under the **File Menu**.



Open Tab will open any available tabs (Cameras, Database, Map).
Close Site's Tabs will close all open tabs for this Site.
Change password…will change the password.
Change Login will change the user who is logged in.
Custom Event Notifications: see 10.4.4.1 below.
Monitoring tools: opens Forensic tool, Stats, and Site Overview.
Site contact: will show the name and details of the Contact person for the site.
Audit Site: see 10.4.4.2 below.
Archived Reports will display a list of previously archived reports.
Fetch Report: see 10.4.4.4 below.
Setup: see 10.4.4.5 below.

10.4.4.1 Custom Event Notifications

Note: This is the main setup section for the Event Notifications feature.

Event Notifications are GUI based notifications, which will appear to an operator when there is a Cameras Tab open. There are three types of notifications.

Audio Notification	A sound clip that gets played when the event triggers.
Message Notification	A message that gets displayed in the notification area of the resource panel. It is meant as an unobtrusive feed of events. Click this icon at the bottom of the resource panel and the notification area will get shown. This can be resized. If an event has camera resources associated with it, then the notification can be double-clicked and the cameras will be shown in the camera view.
Popup Notification	A popup message box that is shown when the event triggers.

10.4.4.1.1 Event Notification Setup

There are 4 levels at which these notifications can be configured (one global, and three tiers of Site based settings).

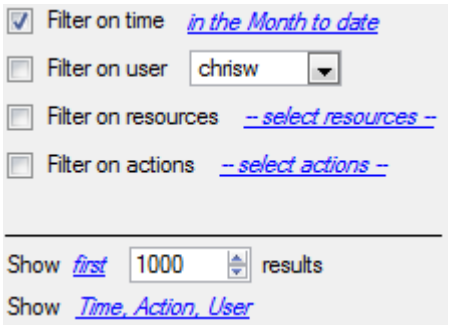
Global Level (all events for all sites)	The notifications can be configured per event priority. This is done in **Settings Menu / Default Event Notifications.**

Site Level	The event notifications can be overridden for a particular site**. Site menu / Custom Event Notifications / Site Tab.** Then click on **Use custom settings**.
Server Level	The event notifications can be specified for a particular server on the site. **Site / Custom Event Notifications / Servers Tab.** Then click on **Use custom settings**.
Event Level	The event notifications can be specified for a particular event**. Site Menu / Custom Event Notifications / Events Tab.** Then click on **Use custom settings**.

Note: These settings reside on the viewing station. So, each viewing station can be configured as each operator wants it to be. For instance, operator A may want the system to respond in one way to certain events, while operator B might opt for alternative options on a different viewing system.

10.4.4.2 Audit Site

Audit trails are the historical "footprints" left by various processes. They are used primarily as diagnostic tools to identify exactly what happened in the system. Each audit trail is in the form of a textual list of historical actions.



There are multiple options for filtering the audits, as there can be an overwhelming amount of information in the audit logs. All the hyperlinks open up a full list of options to filter.

Filter Time, Users, Resources, and Actions.

The **Show first/last** option limits how many of the results are brought up.
Show time/action/user option allows adding/removing columns to the audit report, and will list the selected variables.

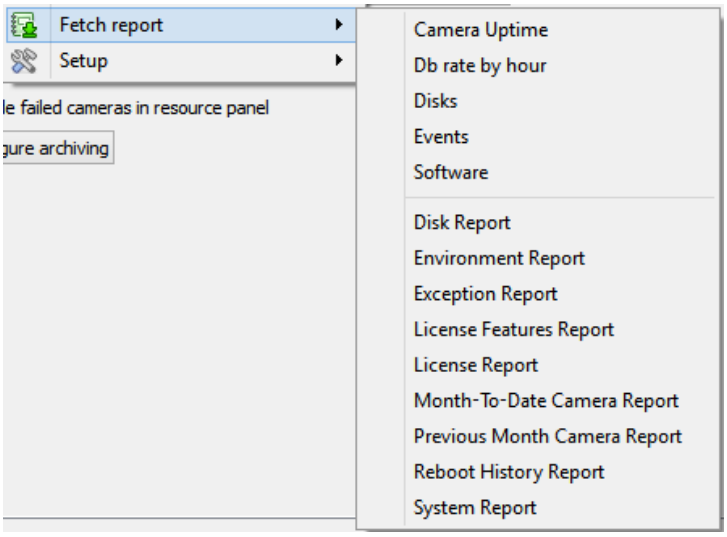
10.4.4.3 Print, Save, Refresh

The report is not live. To update the information, click on **Refresh**.

To print the Report for reference, click on the **printer** icon.

To save a digital copy of the Report, click on the **disk** icon.

10.4.4.4 Fetch Report



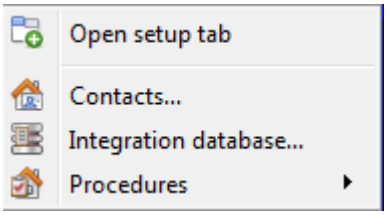
This menu allows the user to pull a full report for the entire Site.

Select to pull a **Template**, or pull up a quick report based on the list of variables below the border line.

Note: For individual unit reports, and a full description on the nature and details of reports, see the **Setup Guide / Configure Servers / Setup Tab: Reports** section of the manual.

10.4.4.5 Setup

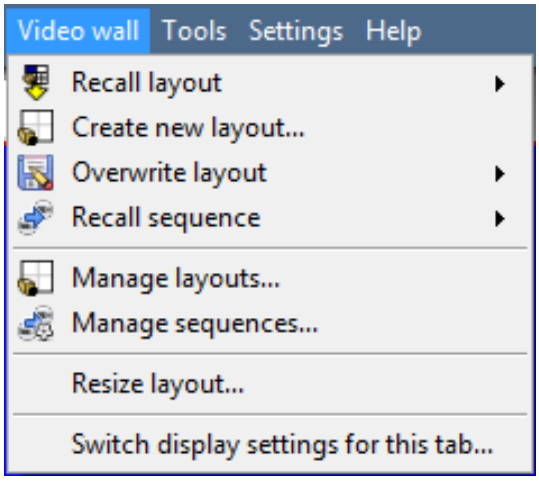
When selecting **Site** / **Setup**, the menu shown in the image opens up.



Open Setup Tab This will open the main Setup Tab for the Site.
Contacts Here, add and edit Site Contacts.
Integration Database A metadatabase (used for integrations), may be added or edited here. (The documentation for this is in the Integration section of Configure Servers, in this manual.)
Procedures is a procedure for an operator to follow in a particular event, this may include up to 6 contact people, and written instructions.

10.4.5 Video Wall Menu

In pre-**CathexisVision** 2014 software, this menu was titled the Layout Menu, and only contained setup information for Layouts.



A **Layout** defines how the cameras appear on the screen, in the Cameras Tab. Including which cameras are shown, and how much space they take up on the screen.

A **Sequence** is a cycle of individual cameras that will run, on a timer, in a single viewing panel, in the Cameras Tab.

The **Switch Display Settings for this tab** will define the behaviour of the currently open Cameras Tab, when video information is sent to the Client Station with an alarm.

Note: this menu option will only be present when viewing a Cameras Tab.

10.4.5.1 Layout

A **Layout** defines how the cameras appear on the screen, in the Cameras Tab. Including which cameras are shown, and how much space they take up on the screen.

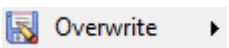
10.4.5.2 Create New Layout

To create a layout, organise cameras on the screen as desired (double-left-click to expand; single-right-click to reduce). Then click on **Layouts / New**. Give the Layout a name, and click OK. (Use Layouts created in the Cameras Tab in the Monitors Tab, and Vice Versa.)

10.4.5.3 Recall a Layout

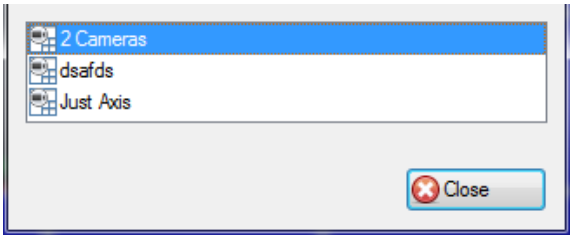
To bring up a list of existing Layouts, click on **Recall** and select the layout name desired.

10.4.5.4 Overwrite Layout



Clicking on **Overwrite** and selecting one of the Layouts in the list, will overwrite that Layout with the current panel organisation.

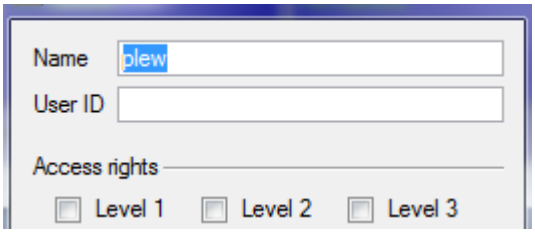
10.4.5.5 Manage Layouts



Clicking on **Manage** will bring up the list of existing Layouts to manage.

From the management list, either delete the Layout or enter the Layout Properties window.

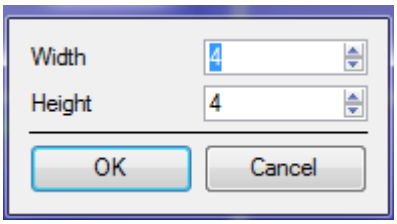
These are both done by right-clicking on the Layout in the list.

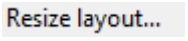


In the **Layout Properties** window, it is possible to change the Name, and User ID of the Layout, as well as the User Access Level required to view, or edit, the layout.

Note: with limited access rights, these settings cannot be changed.

10.4.5.6 Resize Layout





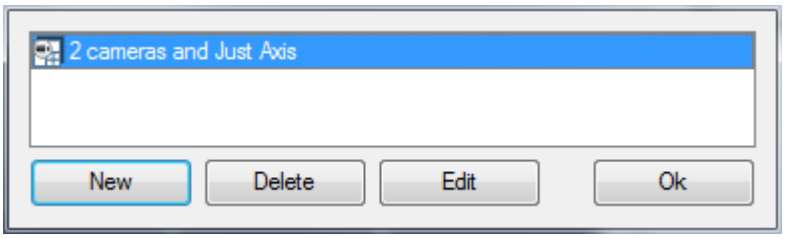
Clicking on **Resize layout** will provide the ability to change how many cameras are arranged on the screen. Define how many cameras there are per row, and per column.

The maximum number of cameras allowed per screen will be an 8*8 matrix. This provides a Layout with 64 cameras. (This would require an incredibly large screen to be practical though.)

10.4.5.7 Sequence

A **Sequence** is a cycle of individual cameras that will run, on a timer, in a single viewing panel.

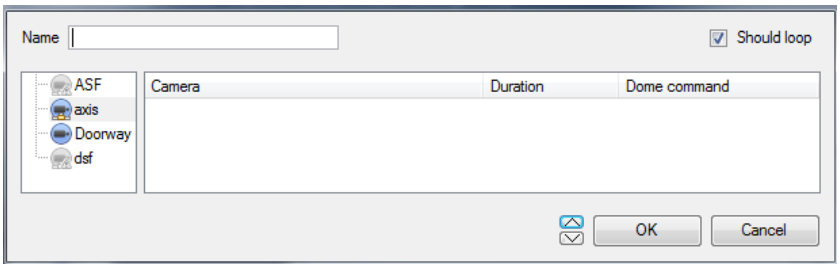
10.4.5.8 Sequence Manager



Clicking on this icon will bring up the Sequence Manager.
To **edit** a Sequence, select the existing Sequence and click Edit. To create a **new** Sequence, click on New. This will bring up the **Sequence Editor**.

10.4.5.9 Sequence Editor

Access the Sequence Editor, to create and edit sequences, via the Sequence Manager.



Name the Sequence.

The left-hand panel will hold a list of available cameras.

The right-hand panel will hold a list of cameras that are included in the Sequence.

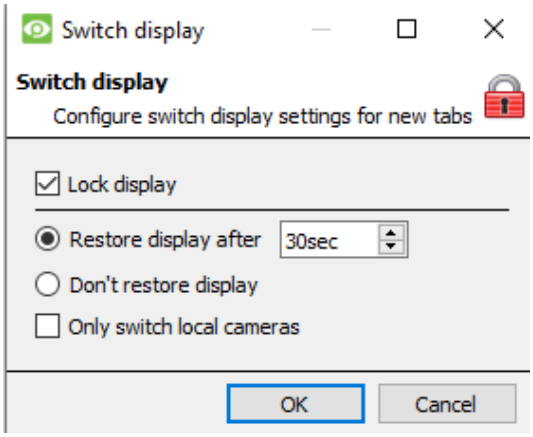
Sequence Editor Procedures	
Add a camera to a Sequence	-Double-click on a camera in the list of available cameras. -Or click-drag one, or multiple cameras, across into the Sequence list.
Remove a camera	Right-click on the camera and select Delete.
Set the duration of a camera for each loop of the Sequence	-Right-click, and select Set Duration. -Enter the duration in seconds, and click OK.
Looping	Should loop If the **Should loop** option is checked the Sequence will run indefinitely, if it is unchecked the Sequence will run once.
Change the order	Select a camera and use the arrows to move that camera up or down the order.

10.4.5.10 Recall Sequence

Recall sequence To recall an existing sequence, click on **Recall sequence** to bring up a list of all existing sequences. Click on the sequence to run.

10.4.5.11 Switch Display Settings for this Tab

Note: The Switch Display Settings set here are for the currently open tab only. To define the default Switch Display Settings for all tabs that are opened, navigate to **Settings Menu / Switch Display settings for new tabs…**



Lock Display

Will prevent the Cameras Tab from displaying any video feeds sent to it by the Event.

Restore display after

Will define how long after switching to the Event Cameras the Cameras Tab will return to the original display settings.

Don't restore display

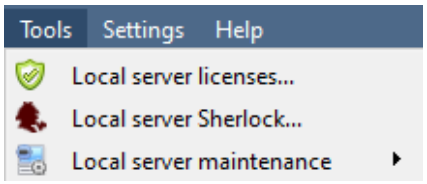
Will leave the Cameras Tab on the Event Cameras until an operator, or administrator, resets the display.

Only Switch Local Cameras

Will only switch to Event cameras originating from a local site.

Note: Lock or unlock the currently opened Cameras Tab by clicking on the little lock located at the bottom of the resource panel in the camera tab (Only appears when the mouse hovers over it.)

10.4.6 Tools Menu

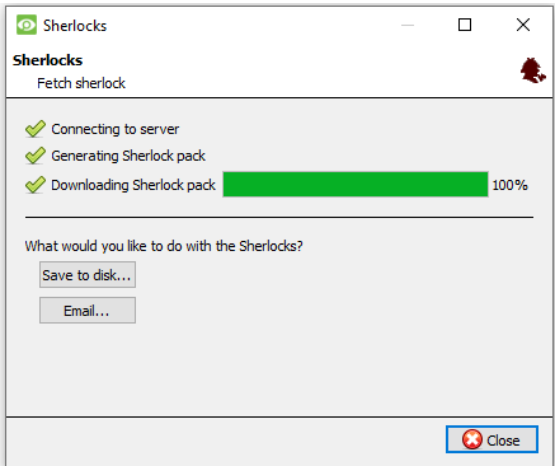


If on a client PC, it will say **Viewing Station licenses**. If on the server, it will say "**Local server licenses**". Also retrieve the server licenses from site, or units, by entering the **Setup** / **Configure Servers** / and right-clicking on the unit.

10.4.6.1 Licenses

This will allow adding a license to the Base Station being worked on, not to any of the Recording Servers on the Site.

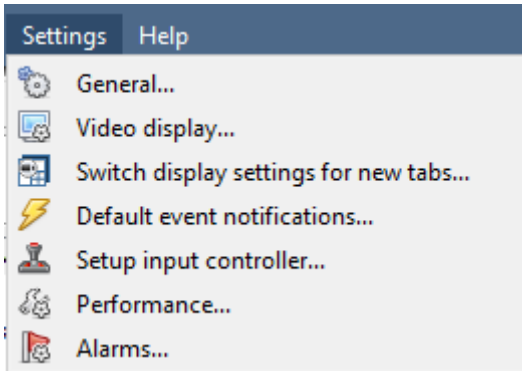
10.4.6.2 Sherlocks



Sherlock files are a diagnostic tool, used by the Support Desk. The normal procedure is to email the Sherlock file to the Support Desk, with a description of the problem, but it can also be saved to disk.

Note: clicking on Email to Recipients, will open up the Operating Systems default email client. Save to Disk will allow saving the Sherlock files to any storage attached to a workstation.

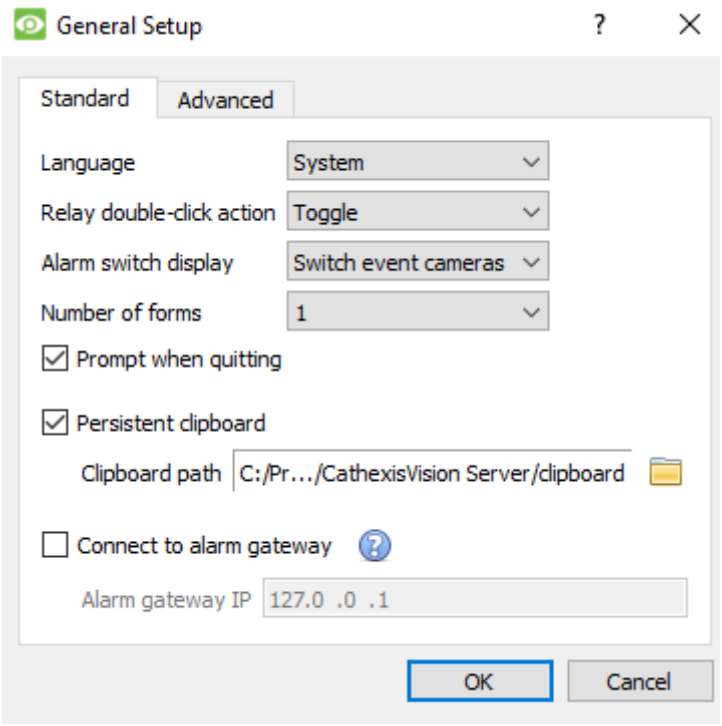
10.4.7 Settings Menu



This section deals with the General **Settings Menu**.

10.4.7.1 General

10.4.7.1.1 Standard Tab



Language: Select the language of the GUI from the drop-down menu.

Relay Double Click Action will set whether or not a relay in the Resources Panel, will be changed from its current state, or set to pulse.

Alarm Switch Display defines the GUI behaviour for when a user is handling an Event Alarm. It defines whether or not the display will switch to show the cameras attached to that Alarm.

Number of Forms

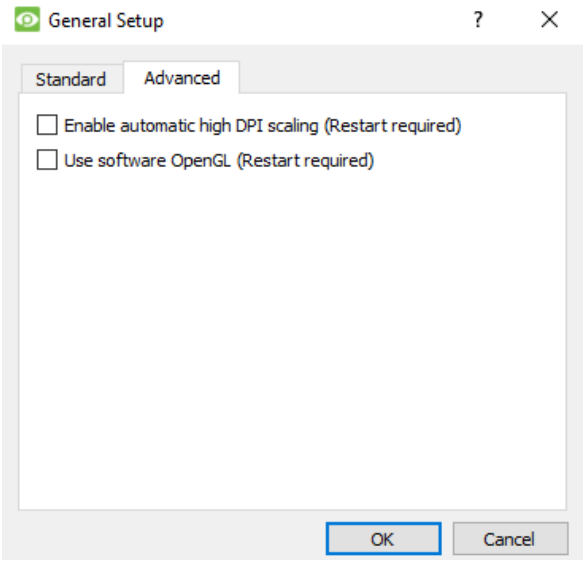
Select the default number of monitors to be displayed. The default maximum is 6, but this option can be overridden by editing the command line. See the Command Line Options section.

Prompt When Quitting will prompt the user every time CathexisVision is quit, regarding whether or not the current tabs should be reopened when the program is next started**.**

Persistent clipboard will persist after closing CathexisVision.

Connect to alarm gateway: Check to enable connection to the alarm gateway. Enter the gateway unit's IP address. Click the **?** icon to display license information.

10.4.7.1.2 Advanced Tab



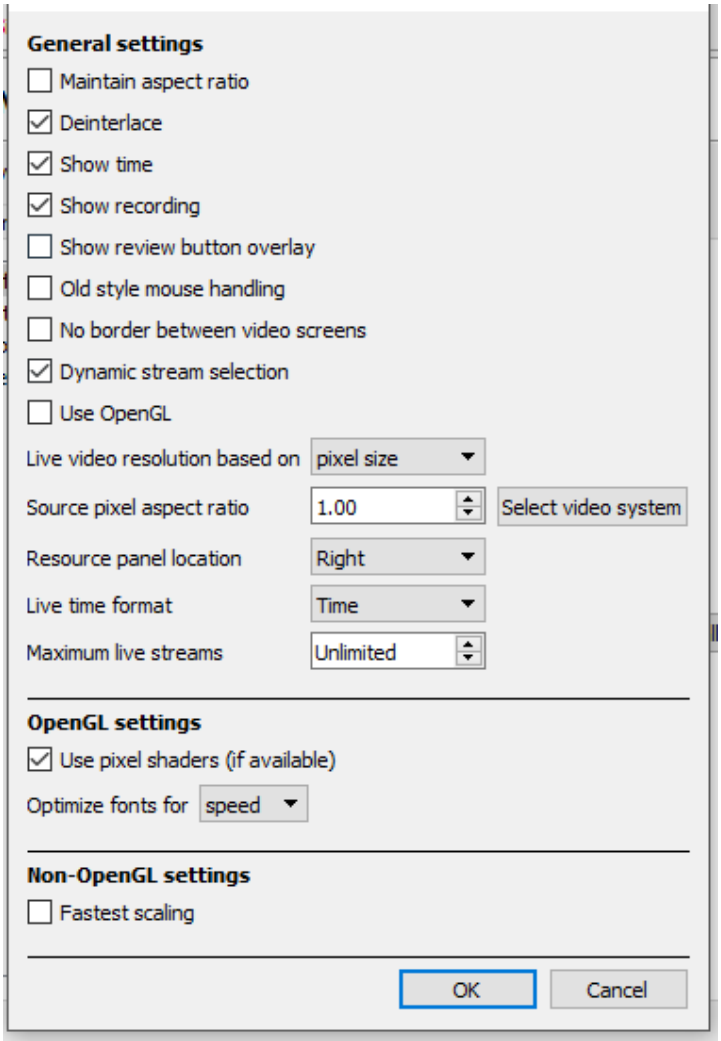
This tab deals with slightly more advanced settings for the GUI.

Check to **enable automatic high DPI scaling of the GUI**.

Check to **enable use of OpenGL software**.

Note: Restart required for both settings.

10.4.7.2 Video Display



Maintain aspect ratio: The ratio between the width and the length will be kept constant as the video size changes.

Deinterlacing: A process of converting interlaced video (like analogue) to a non-interlaced form.

Show time: Shows the time on the video.

Show recording: indicates when, with a red dot, the video feed in a panel is currently being recorded.

Show review button overlay: will overlay buttons for review, on mouse-over, on a camera panel when its video feed is being reviewed.

Old style mouse handling: Use pre-2017.2 mouse handling.

No border between video screens: Check to remove borders between video screens.

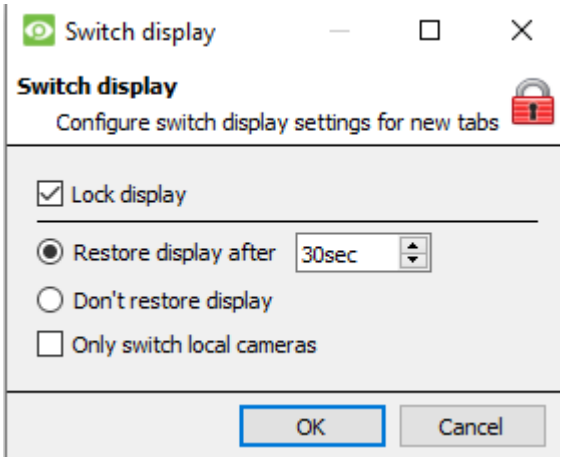
Dynamic stream selection is enabled by default. This will dynamically select the stream based on the display resolution.

OpenGL: A Graphics library...a cross-platform API for writing applications for 2D and 3D graphics. The graphics card utilises the OpenGL, and thus the load will be passed on to the GPU, freeing the load on the CPU.
Pixel shaders: Similar to OpenGL.
Fastest scaling: When the CPU has to be utilised to handle the load, this option helps optimise the instructions for the CPU.

Use OpenGL: Check to use. See below for info.
Live video resolution: Based on either panel size or pixel size.
Source pixel aspect ratio: Will conform the video source's correct aspect ratio, making the object look more real-world. For example, when a video of a perfect circle appears oval on the screen, it is an indication that the aspect ratio might be different from the original source.
Resource Panel Location: Resource Panel can be configured for left or right of video screen.
Live Time Format: Select from drop-down menu whether to display only time or date and time in live video.
Maximum Live Streams: An option to limit the number of live video streams in the CathexisVision camera tab. The limit is a global limit and applies across all screens. (On an NVR/DVR this setting is only accessible to an administrator.)

10.4.7.3 Switch Display Settings for New Tabs

This will define how the cameras tab responds when there is an event on the site that sends video and information to the Cameras Tab of the viewing client. **Note**: The settings here will apply to any new Cameras Tabs, opened after settings are changed.



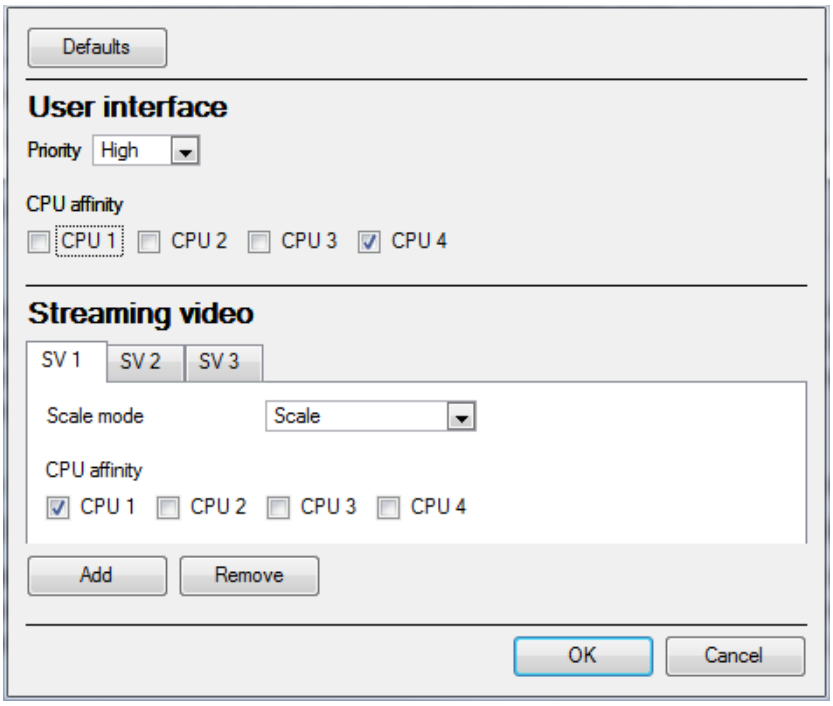
Lock Display
Will prevent the Cameras Tab from displaying any video feeds sent to it by the Event.
Restore display after
Will define how long after switching to the Event Cameras the Cameras Tab will return to the original display settings.
Don't restore display
Will leave the Cameras Tab on the Event Cameras until an operator, or administrator, resets the display.
Only Switch Local Cameras
Will only switch to Event cameras originating from a local site.

Note: Lock or unlock the currently opened Cameras Tab by clicking on the little lock located at the end of the Timeline on the Review Controls.

10.4.7.4 Default Event Notifications

Here, set the default/global Event Notifications for this Viewing Station. For more information about Event Notifications, and their Setup, see the Custom Event Notifications section (above).

10.4.7.5 Performance



Note: the system will calculate defaults that should be optimised already.

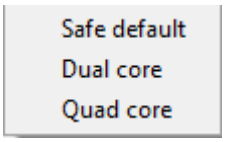
Unless the user has an understanding of this technology, and an explicit reason for changing these settings, do not change them.

(1) **Defaults**:

The system calculates default performance settings based on available CPUs, enabling optimisation of resources even before settings have been manually configured.

Once the performance settings are explicitly configured, the defaults fall away. However, recall the defaults by clicking the **Defaults** button > **OK** (customised settings will then be lost).

Default Options:



When clicking on default, there is the option to choose the default that b suits the system being worked on.
Choose safe default if unsure as to what system is being worked on.

(2) **User Interface**:

What the user sees.

Priority:

The priority setting affects what the user sees as the interface. For example, the speed and responsiveness of the interface is influenced by the Priority setting.

CPU affinity with the user interface:

The CPU affinity dictates which CPU core will be responsible for what streaming server. This enables multiple streaming servers without exceeding the processing power of the CPU.

(3) **Streaming video**:

Here, add or delete Streaming Video Servers (SVs) to match the available CPUs. A streaming video is responsible for the decompression of the compressed video from camera sources (video is compressed for transporting purposes).

Scale mode:

"Scaling" is the re-sizing of images. For example, the scaling of MPEG images from their default 4CIF down to QCIF display size. Scaling requires processing effort. One of the big advantages of multiple CPU processing is that this effort can be split across the CPUs. Each Streaming Video Server (SV) must be assigned a "Scale Mode" setting, which is the type of scaling to be performed by the SV.
Options are:

No scaling: The SV does not scale. Presumably, scaling would be assigned to another SV.

Scaling: The SV scales. If scaling is assigned to every SV, the system will attempt to spread the load.

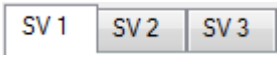
Streaming Video Server (SV):

By default, the system only has one Streaming Video (SV) server. Manually create more SVs for further CPUs, so that ultimately there are as many SVs as there are CPUs:

Dual core: SV1, SV2

Quad core: SV1, SV2, SV3, SV4

For example, for a quad processor:



CPU affinity with the streaming video:

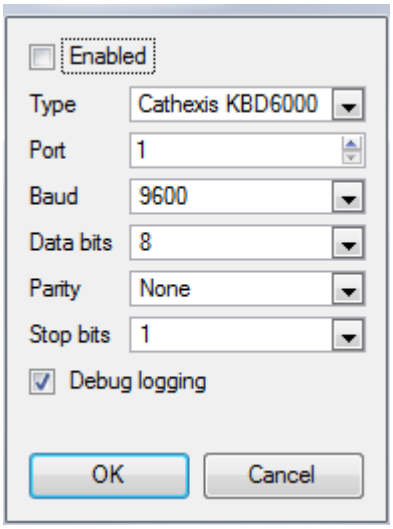
Whereas SVs are numbered SV1, SV2, etc, CPUs are numbered CPU0, CPU1, CPU2, etc

The "CPU affinity" maps CPU to SV. For example:

Dual core: SV1 (CPU0), SV2 (CPU1)

Quad core: SV1 (CPU0), SV2 (CPU1), SV3 (CPU2), SV4 (CPU3)

10.4.7.6 Keyboard



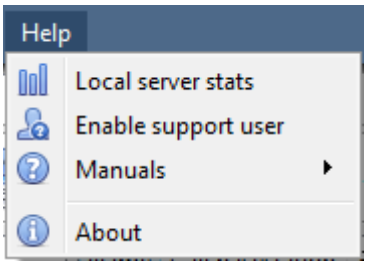
This option is for adding a keyboard to a Base Station. If adding a Keyboard to a Recording Server, do so via **Site / Open Tab / Setup / Configure Servers / Keyboard**.

Enter in the details relevant to the keyboard.

10.4.7.7 Alarms

Enter an IP address for a technical alarm server, or gateway, for the viewing software to send alarms to.

10.4.8 Help



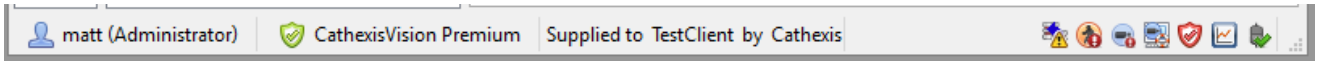
Local server stats/Viewing station stats: Shows the statistics for the local server if it is an NVR, or for the Viewing Station. (This depends on the unit on which one is on.)

Enable Support User: This will enable/disable a special user added for support purposes, when installing **CathexisVision** NVR.
Note: this will only appear on NVR units.

Manuals: The Setup, Operator's, Quickstart, and Archiving manuals are accessible within the software.

About: Provides information about the License, the Release version, and the email address for Support.

10.5 Status Bar



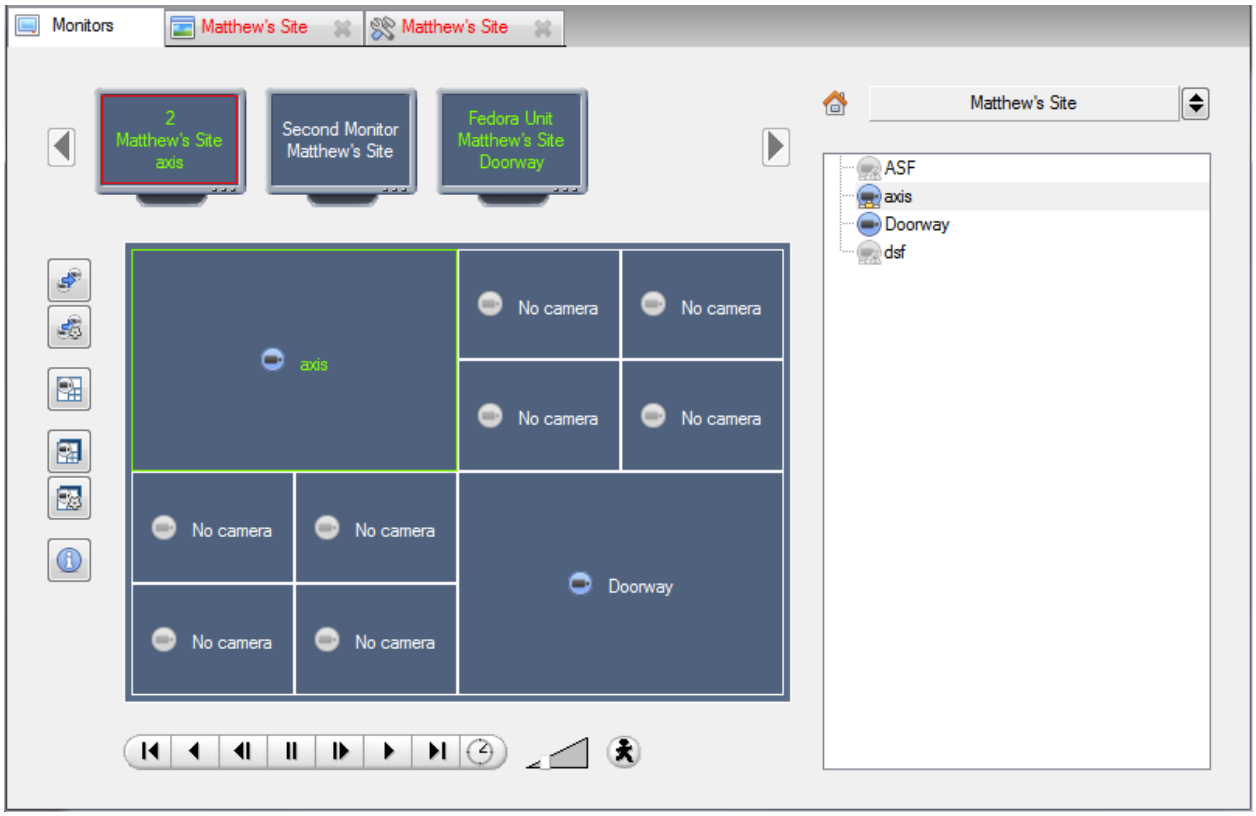
The status bar runs along the bottom of the interface. On the bottom right of the bar are a useful set of notifications. For further details, in the GUI, left-click on a specific icon.

Notification Icon	Notification Description
dvs (Administrator)	The **username**, and their access level.
CathexisVision Premium	This represents the main **license** of the unit.
Supplied to Documentation by Cathexis Internal	The distributor of the license.
	The **cameras notification** will only appear to alert the user when cameras are down. Clicking on it allows one to see which cameras these are.
Admin	The **licensing notification** will be permanently present, but will change colour depending on licensing status. Green indicates a healthy licensing status. Orange indicates that there are demo licenses due to expire. Red means either missing or expired licenses.
	The **performance monitor notification** is permanently present, and will allow viewing of performance statistics. See the Appendix of this document for a full explanation.
	The **connection status** icon is permanently present, and indicates the status of the connection to the current Site.
	Video Analytics notification. Warns the user when an error has occurred which involves one or more of the video feeds on a Site.
	Failover notification will provide information about the status of existing failover servers.
	Database volume/slice or performance notification. It can also indicate when cameras have been configured to record without being assigned a database
	Failover database synchronization notification. The failover server is transferring recorded footage back to the main server after recovery.
	LPR notification. It will show an error when there are LPR license/dongle problems.
	A health alert notificatuin. Check the tooltip to see the health status. If the primary disk is "full" the health alert will be triggered
	Tamper detection alarm. It will indicate the cameras where a tamper has been detected.
	A gateway notification. It is shown if the gateway database couldn't be started

10.6 Monitors Tab

The monitors tab is a tab that gives full control over the Video Wall. Here, the user can change the layout, and define camera Sequences, and salvos.

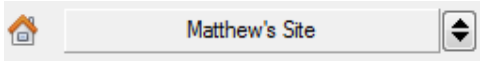
There will not be any video playing on the interface. The names of cameras where they are placed on the layout will be visible.



10.6.1 Open a Site on a Screen

The list of monitors will be representative of the number of monitors that have been added to servers on the site.

To Open a monitor from a site, select one of the available Monitors. Then click the Sites list:



Then select the site.

The Monitor with a red border will be the Monitor whose camera Layout is displayed below it.

10.6.1.1 Layout

A layout defines how the cameras appear on the screen. This includes which cameras are present and how much of the screen an individual camera takes up.

10.6.1.1.1 Create a Layout

To create a layout, organise cameras on the screen as desired (double-left-click to expand; single-right-click to reduce). Then click on **Layouts / New**. Give the Layout a name, and click OK. (use Layouts created in the Cameras Tab in the Monitors Tab, and Vice Versa.)

10.6.1.1.2 Edit an Existing Layout

Setup the cameras as desired (double-left-click to expand; single-right-click to reduce). Then click **Layouts / Save As**. Then select the Layout to overwrite, and click ok.

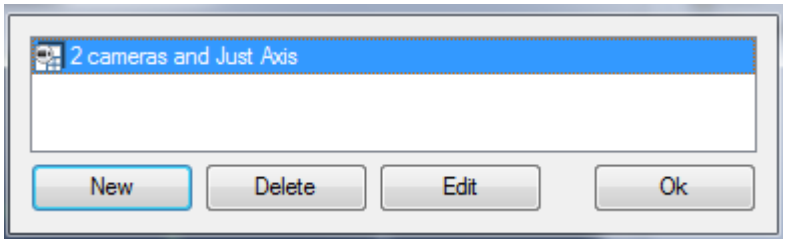
10.6.1.1.2 Recall a Layout

To bring up a particular layout on a screen, click on this icon, and select a layout name of choice.

10.6.2 Sequence

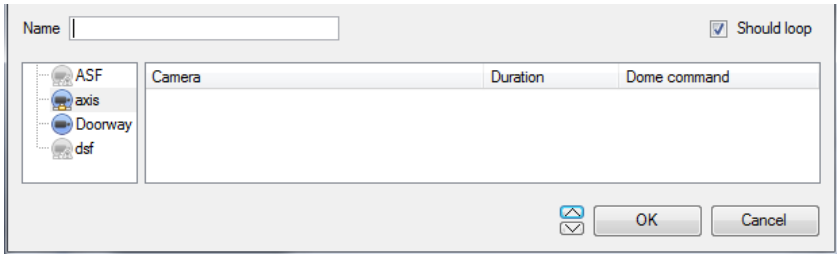
A Sequence will run a set of cameras in a single camera panel.

10.6.3 Sequence Manager



Clicking on this icon will bring up the Sequence Manager.
To **edit** a Sequence, select the existing Sequence and click **Edit**. To create a **new** Sequence, click on **New**. This will bring up the **Sequence Editor**.

10.6.4 Sequence Editor



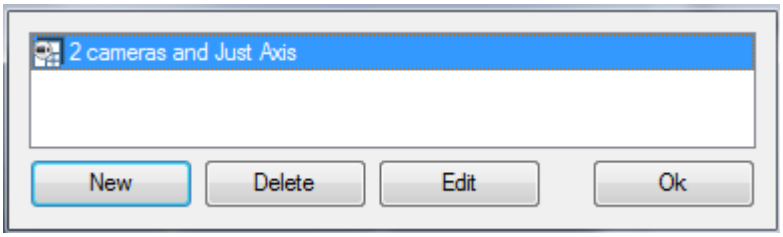
Name the Sequence.
The left-hand panel will hold a list of available cameras.
The right-hand panel will hold a list of cameras that are included in the Sequence.

Sequence Editor Procedures	
Add a camera to a Sequence	-Double-click on a camera in the list of available cameras. -Or click-drag one, or multiple cameras, across into the Sequence list.
Remove a camera	Right-click on the camera and select Delete.
Set the duration of a camera for each loop of the Sequence	-Right-click, and select Set Duration. -Enter the duration in seconds, and click OK.
Looping	Should loop If the **Should loop** option is checked, the Sequence will run indefinitely, if it is unchecked the Sequence will run once.
Change the order	Select a camera and use the arrows to move that camera up or down the order.
Run a Sequence	- Click on a camera panel. - Click on - Select the relevent Sequence from the drop-down menu.

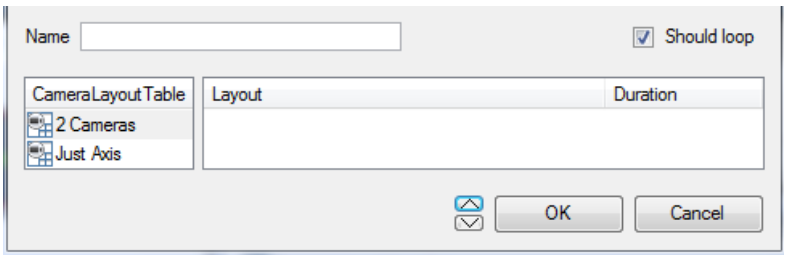
10.6.5 Salvo

A Salvo is a set of Layouts. This means that the Layout of cameras on the monitor will change, running through a set order, using the pre-defined Layouts.

10.6.5.1 Salvo Manager



Click on this icon. This will bring up the Salvo Manager.
To **edit** a Salvo, select the existing Salvo and click edit.
To create a **new** Salvo, click on **New**. This will bring up the Salvo Editor.



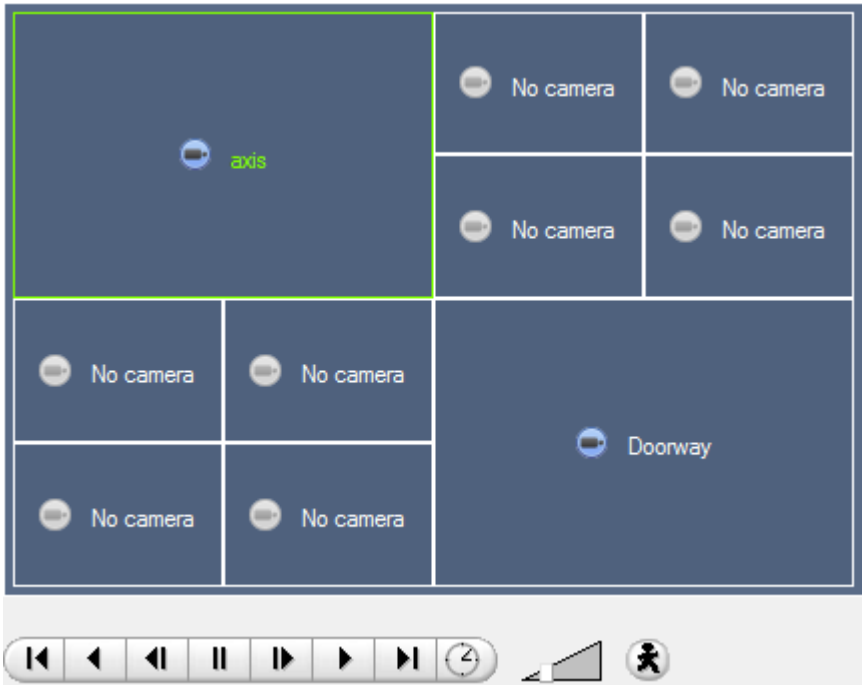
Name the Salvo appropriately.

The left-hand panel will hold a list of available Layouts.

The right-hand panel will hold a list of Layouts that are included in the Salvo.

Salvo Procedures	
Add a Layout to a Salvo	-Double-click on a Layout in the list of available Layouts. -Or click-drag one, or multiple Layouts, across into the Salvo list.
Remove a Layout	Right-click on the Layout and select Delete.
Set the duration of a Layout for each loop of the Salvo	-Right-click, and select Set Duration. -Enter the duration in seconds, and click OK.
Looping	Should loop If the **Should loop** option is checked the Salvo will run indefinitely, if it is unchecked the Salvo will run once.
Change the order	Select a Layout. Use the arrows to move that Layout up or down the order.
Run a Salvo	- Click on a Layout panel. - Click on this icon. - Select the relevent Salvo from the drop-down menu.

10.6.6 Virtual Cameras Interface



The virtual cameras interface is the interface where one can:

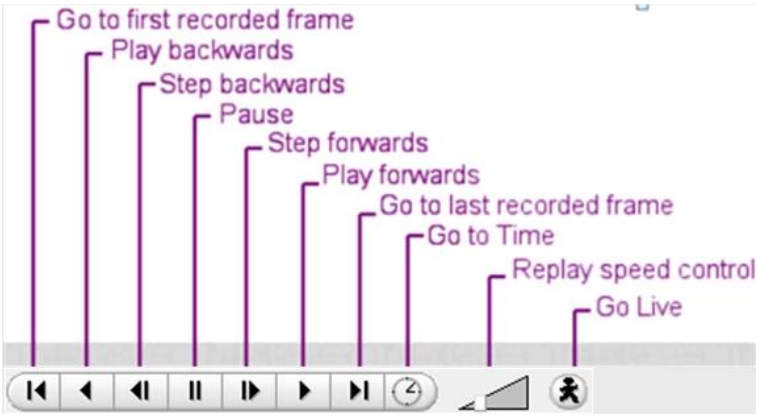
- See the Layout that the cameras will take on the Monitor selected.
- See what cameras are in which panels.
- Control the overlays on each camera.
- Use the Playback controls to review video on the Monitor.

10.6.7 Individual Panel Settings

To change the settings of an individual panel, middle-click on the panel. This will bring up the following menu:

Set no camera	**Set No Camera** will make this panel blank.
Review camera	This will bring up the recordings of the selected camera. For information on reviewing the camera, see the section below on Review Controls.
Next video format	This will cycle through the available video feeds that are available on the selected camera.

10.6.7.1 Review controls



Note: When a camera has been selected, its border and camera name will become Green.

10.7 Cameras Tab

CathexisVision offers the installer two useful tools for retrieving visual information about cameras, as they are streaming information. These steps are carried out in the Cameras Tab, viewing video.

10.7.1 Statistics and Information

10.7.1.1 Resolution and Bitrate

Pressing CTRL-R will bring up the Bit Rate, and Resolution information of the feeds. This is seen in the yellow text in the image to the left.

On the top right is the **resolution** of the feed currently being viewed

On the bottom left, are two numbers. The number in brackets is the **bitrate;** to the left of this number is the **Frames Per Second Rate**.

10.7.1.2 General Camera Information

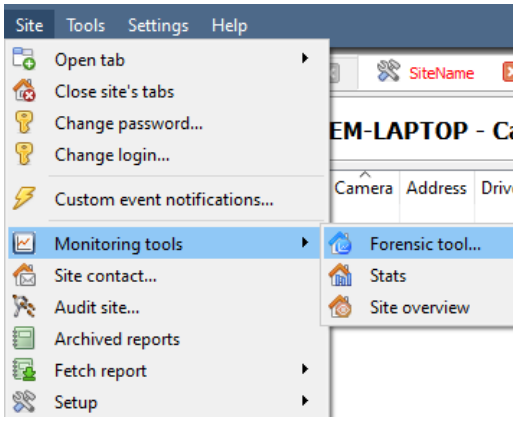
Pressing CTRL-I brings up the general camera information overlay.
Unit is the unit this camera has been added to**.**
Camera is the cameras name.
Index is a number given by the NVR to identify this camera.
Format this is the format the video is streaming in.
Type this is the type of device the camera is.
Contact this is the address of the server the camera is attached to.
Stream Profile this is the streaming profile of the video feed.

11. CathexisVision Forensic Tool

11.1 Forensic Tool

The Forensic Tool is used to troubleshoot and obtain historical network, storage, event, camera streaming, people counting, and other valuable data.

Note: The Forensic Tool is only available in CathexisVision 2014.2 (Service Pack 2) and onwards.



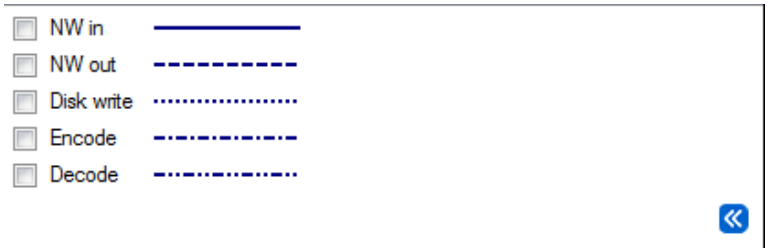
Once a connection is made to the intended camera site or NVR unit, open the forensic tool by selecting the "**Site**" menu option.
Scroll down to "**Performance tools**" and select the "**Forensic tool**..." option.

Note: to access the Forensic Tool, the user must be logged in with administrative rights.

Figure 1: Main Forensic Window

The sections below will explain the interface shown in Figure 1, and how to use this tool.

11.1.1 Data Values Used



NW in	Network In (Mbps). This would be the video, streaming in from IP cameras.
NW out	Network out (Mbps). Video going out. Remote viewing Client PCs.
Disk write	Disk writing speed in Mbps. The rate writing captured video stream to local/network storage.
Encode	Encoded pixel rate. VOM1512/MPEG4 compression for recording/streaming. **Note**: This is NOT the transcoded live streaming.
Decode	Decoded pixel rate. For analytics the compressed video is decoded into raw data.

11.1.2 Date / Time Selection

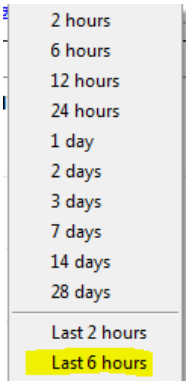
There are two ways to select the graphing period: **Time Bar selection** or **Time Frame selection**.

11.1.2.1 Time Bar Selection

Choose a date, and time, as the starting point for the graph.

Then select to fetch data **6 hours** from the selected date/time.

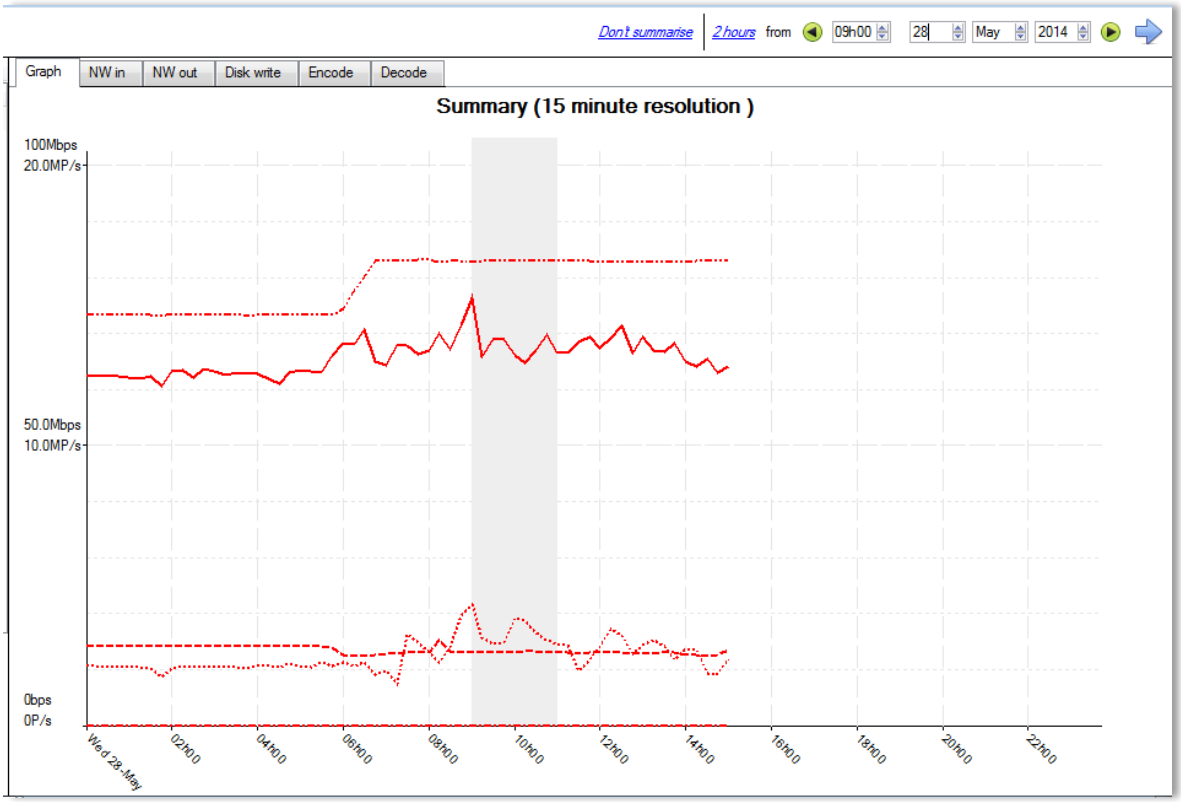
11.1.2.2 Time Frame Selection



Select to graph the “Last 6 hours”, “Last 14 days”, etc.

This will automatically move the date/time to the required position to reflect the selected period.

11.1.3 Graph Window



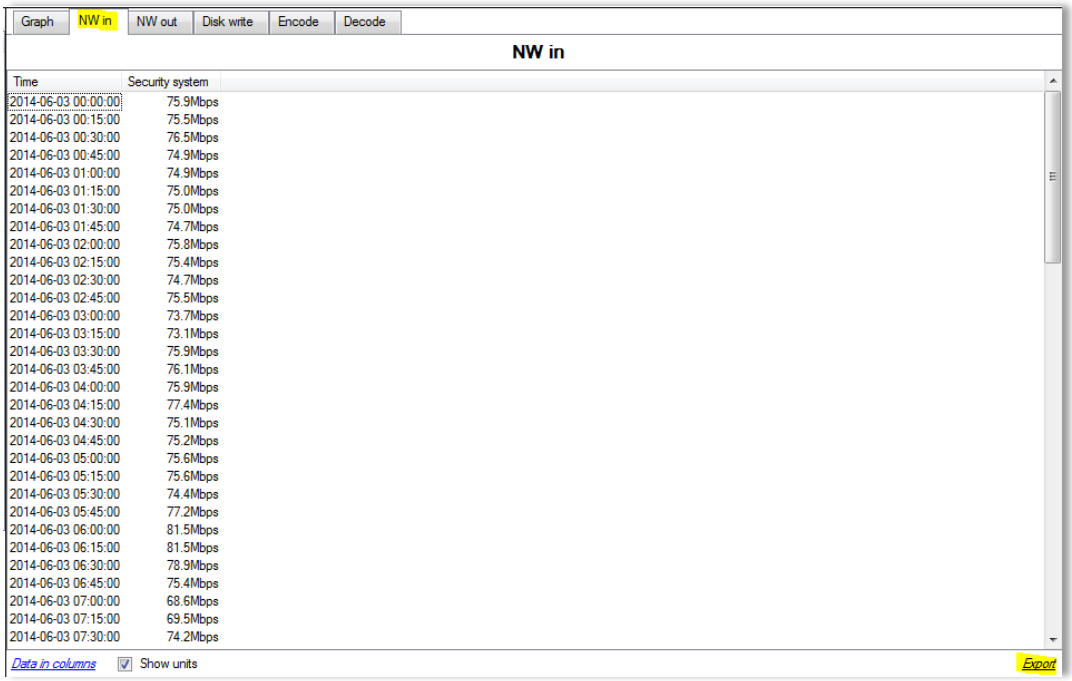
11.1.3.1 Zoom in on a Period

To zoom in on a desired period, hold down the left mouse button at the starting or ending point, and move the mouse right or left. The selected area's colour will become grey.

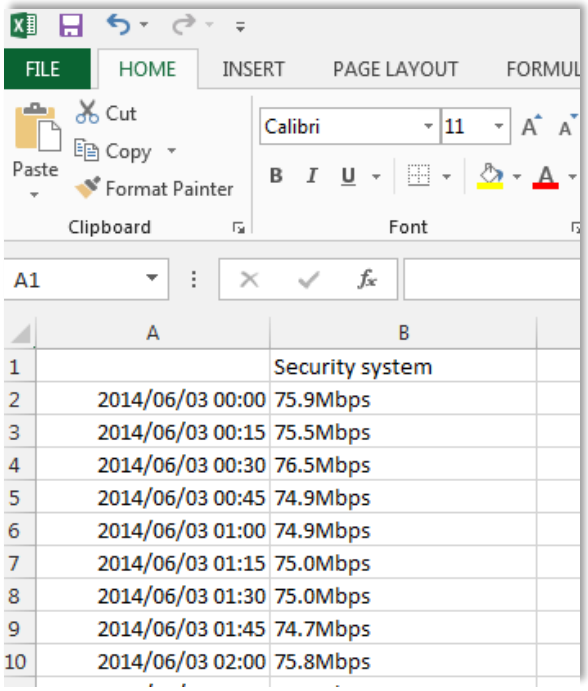
To zoom in on the selected area, select the blue arrow. This will give a detailed view of the zoomed-in time period.

11.1.3.2 See the Data Values

Get to the data values for the various data sets by selecting the “NW in” column. This is shown in the example below:



11.1.3.3 Export as a Comma Separated Values (CSV) file



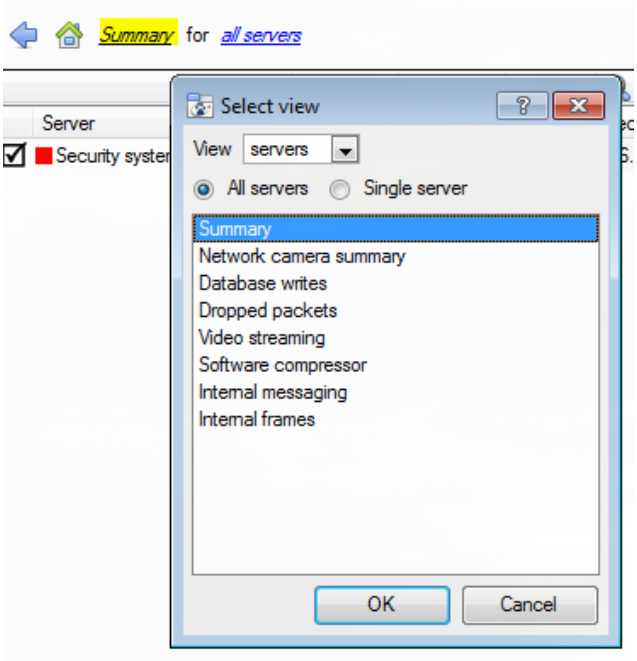
The user can also export the data to a CSV file. See bottom right “Export” shortcut highlighted in yellow.

Choose to disable the “Show units” option below if only needing to import the actual data into Excel.

See the image for the exported CSV file opened in Excel.

11.1.4 Selected Views

11.1.4.1 Summary View of Servers



The default view when opening the forensic tool is the “All servers” summary view.

Change this view by selecting the available options for the Servers view below, for example “Summary”, “Network camera summary”, etc.

As already indicated, the “Servers” view has a list of data sets, which one can choose from. The “X axis” or data sets available for the viewing options will be discussed. Select to view data for all servers, part of the site, or a single server.

11.1.4.2 Network Camera Summary

This provides the **total network throughput**, the **drop ratio**, and a count of **camera stalls** detected for all IP cameras connected to the unit/s.

Variable	Unit	Descriptions
Bitrate	Mbps	Total bitrate of all IP cameras for selected unit/s.
Drop ratio	1:200000	Means 1 dropped packet for every 200000 packets received.
Stalls	Number	A stall is when cameras are not reachable for more than 5 seconds.

11.1.4.3 Database Writes

The recording process receives video data from the cameras. The video data gets cached to local memory (Shared memory – SHM), and from there the data gets read and written to storage. Bottlenecks could be caused by slow or faulty storage/equipment.

Variable	Unit	Descriptions
Write bitrate	Mbps	Rate of writing video footage to storage.
Write Drops	1:200000	Disk writing drops. 1 data item dropped for 200000 written to disk.
SHM Drops	1:100000	Items dropped because the shared memory wrapped - the writes couldn't keep up with the data arriving. 1 item dropped for 100000 items written out of memory.

11.1.4.4 Dropped Packets

Variable	Unit	Descriptions
Network	Number	Packets dropped on the external network (i.e. from cameras to the Recorder).
Internal	Number	Internal UDP packets dropped between servers (internal software messaging).
Frames	Number	Video frames dropped internally, when being passed from process to process.

Note: For the "Number" or X axis value, 200k would indicate 200 000 packets.

11.1.4.5 Video Streaming

Variable	Unit	Descriptions
Sent	Mbps	Video streaming data sent out from the unit (for live viewing).
Received	Mbps	Video streaming data received into the unit (for live viewing).
Decoded	P/s	Pixels per second decoded for live viewing.

Note: MP/s indicates 1000 000 Pixels per second.

11.1.4.6 Software Compressor

Variable	Unit	Descriptions
Encoded	P/s	Encoded pixel rate. VOM1512/MPEG4 compression for recording/streaming **Note**: It is NOT the transcoded live streaming.
Decoded	P/s	Decoded pixel rate. For analytics, the compressed video is decoded into raw data.
Encode efficiency	%	% of frames encoded, ideally 100%. (Less means frames have been dropped).
Decode efficiency	%	% of frames decoded, ideally 100%.

Note: The encoding done by the HTML server is not accounted for at present.

11.1.4.7 Internal Messaging

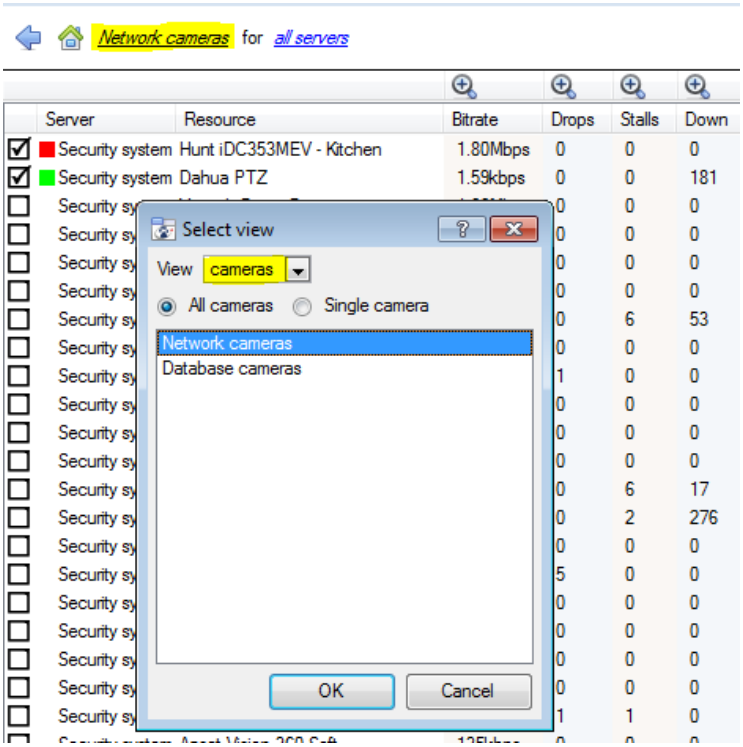
Variable	Unit	Descriptions
Missed	Number	How many UDP packets between processes have been dropped, hopefully 0.
Received	Number	How many UDP packets have been sent between processes
Logs	Number/min	How many logs have been sent to the logger per minute

Internal Frames

Internal frames passed between internal processes.

Variable	Unit	Descriptions
Missed	Number	Video frames dropped.
Received	fps	Received video frames

11.1.4.8 Network Camera View of Cameras



Change the Servers view to "Network cameras" by first selecting the "Cameras" View option as shown below. This will provide camera-specific values.

The "cameras" view has a list of data sets to choose from. The "X axis", or data sets available, for the "cameras" view will be discussed. Select to display "All cameras", or a "Single camera".

11.1.4.9 Network Cameras

Variable	Unit	Descriptions
Bitrate	Mbps	Total bitrate for selected cameras.
Drops	Number	The number of dropped packets, for each camera for selected time period.
Stalls	Number	When cameras are not reachable for more than 5 seconds.
Down	Number	The number of seconds the cameras have been down in a time bucket. So, if the bucket is 15 minutes, expect it to be around 900 if it was down for the whole time.

11.1.4.10 Database Cameras

Variable	Unit	Descriptions
Bitrate	Mbps	Total bitrate of selected cameras.
Bytes to disk	Bytes	Bytes written do disk.
Down	Number	The number of seconds the selected cameras have been down in a time bucket. So, if the bucket is 15 minutes, expect it to be around 900 if it was down for the whole time.

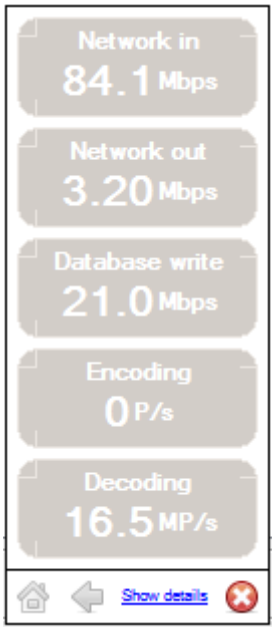
11.1.4.11 Events View of Cameras

Variable	Unit	Descriptions
Event Count	Number	Number of events per camera for the selected period.

11.1.5 Quick View

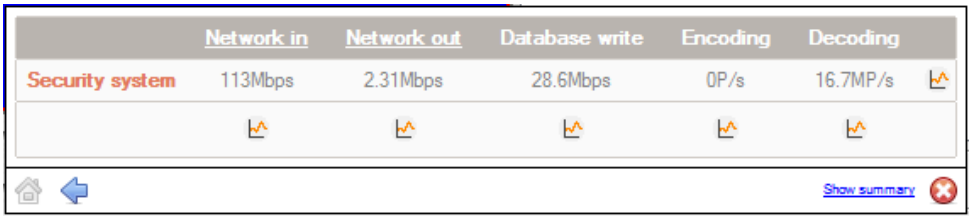
Quickly access performance information from the **CathexisVision** interface.

Left-click on this icon, which is in the bottom right-hand corner.

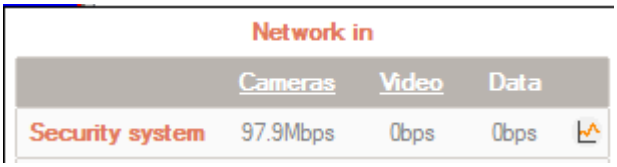


Clicking on this icon will cause the image to the left to appear. This shows live information about the system.

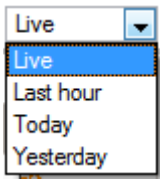
Show details Click on this and it will become the image below. The **show details info** can be seen in more detail by clicking on the information that is hyperlinked. In the below image, these are **Network in** and **Network out**. Following these links will navigate to further information regarding the cause of the network traffic.



For example, clicking on **Network in** reveals the following:



11.1.5.1 Live or Historic



Once the graph window has popped up, select between viewing the live data, or historic data.

This is done by clicking on the drop-down menu, found on the bottom right of the graph window.

11.1.5.2 Multiple Graphs

View multiple graphs by disconnecting the current graph.

This is done by clicking on this icon, which is found at the top right of the graph window.

11.1.6 Examples of How to Interpret the Graph and Columned Values

11.1.6.1 Example 1: Investigate Disk Writing Throughput

One can choose to only display the disk writing graph. Check the “Disk write” checkbox, on the bottom left-hand corner, and deselect the rest. This allows plotting the disk writing graph, exclusively, on the right-hand side. Also select the period “Today” (highlighted in yellow) for the disk writing throughput.

By moving the mouse to the left plane, away from the graph, the columned values on the left would be the **average disk writing throughput** for the selected period. Also expand the “Disk write” column, to get the minimum and maximum values for the selected period. They are also highlighted on the graph in Figure 2.

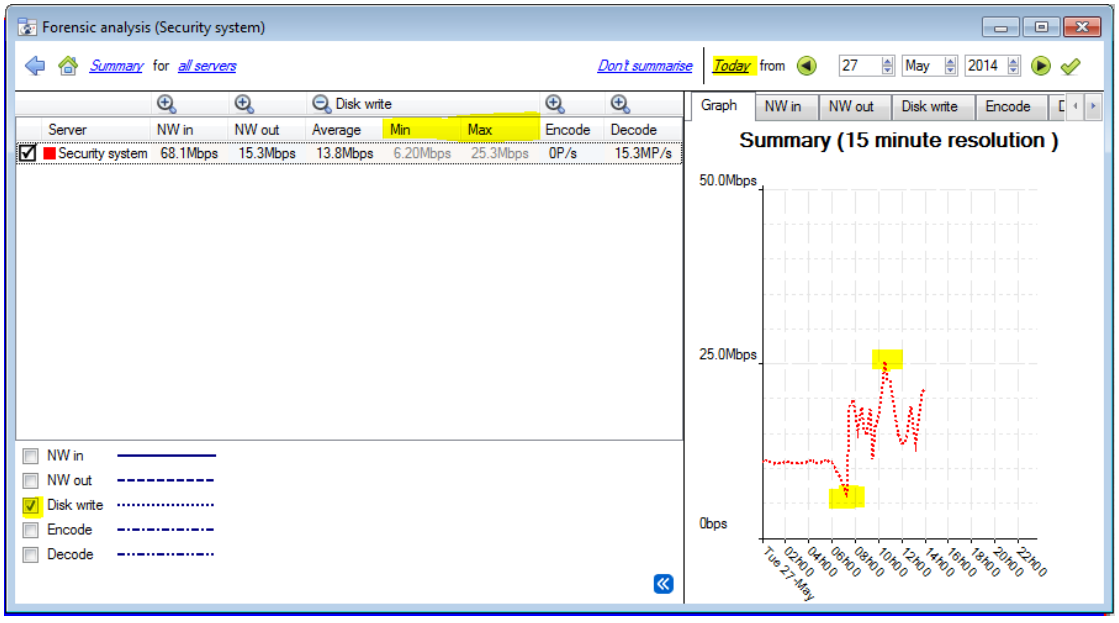


Figure 2

Note: These 2 examples illustrate the process used to filter out required information. Other system data can be retrieved in a similar fashion.

11.1.6.2 Example 2: Investigate Network Loss Issues on Selected Cameras

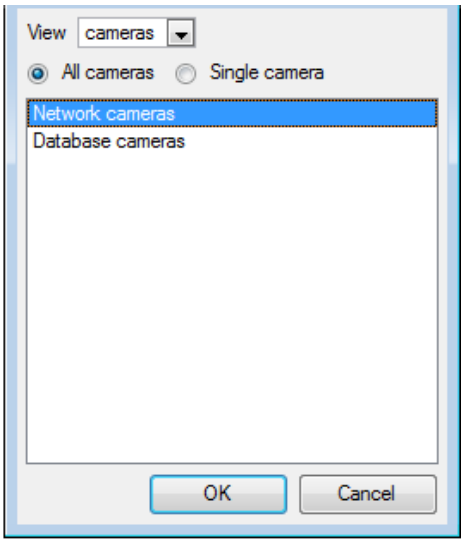
11.1.6.2.1 Scenario

The client has indicated that the live camera views on selected cameras are tearing and there are recording gaps. The camera resources on the right-hand side of the **CathexisVision** indicates low, moderate, and high packet loss. The forensic tool can help highlight the times when the packets failed, and also the magnitude.

The Forensic tool is **only one** of the possible tools with which to measure network loss. Other tools could be network switches, with port statistics; or packet analysing software: tcpdump for Linux and Wireshark for Windows - to capture and analyse RTP (RTSP) traffic loss. Refer to the "**stats**" page for network information. It will give real time packet loss statistics and more detailed video streaming parameters.

Packet loss, on selected cameras, could point to one segment of the network. For example: a segment over a wireless link. It is advisable to create a detailed network layout diagram, of the site, with all the segments and connected IP devices visible on the map. This will help isolate network issues faster. Packet loss on specific camera models could also present itself, when old camera firmware is used. Update the camera firmware to eliminate, or rule this out.

11.1.6.2.2 Method

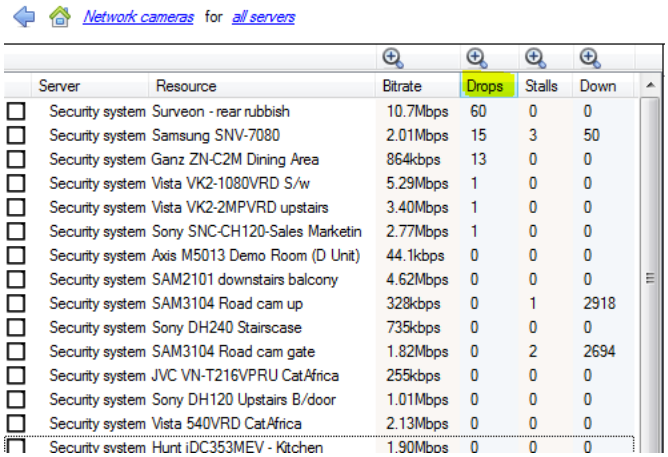


1. Change the view to "cameras".

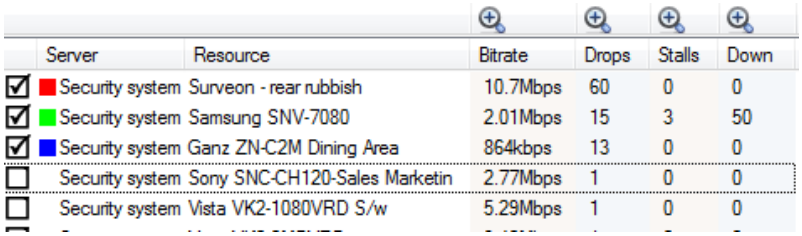
Then select "Network Cameras" from the list.

2. To inspect packet loss on all the cameras for the last day, change the period selector to display "Yesterday".

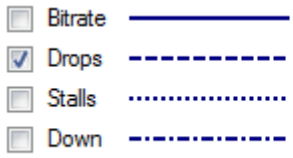
3. Sort the dropped packets on the left-hand column view, by clicking on the “Drops” column header, as indicated below in yellow.



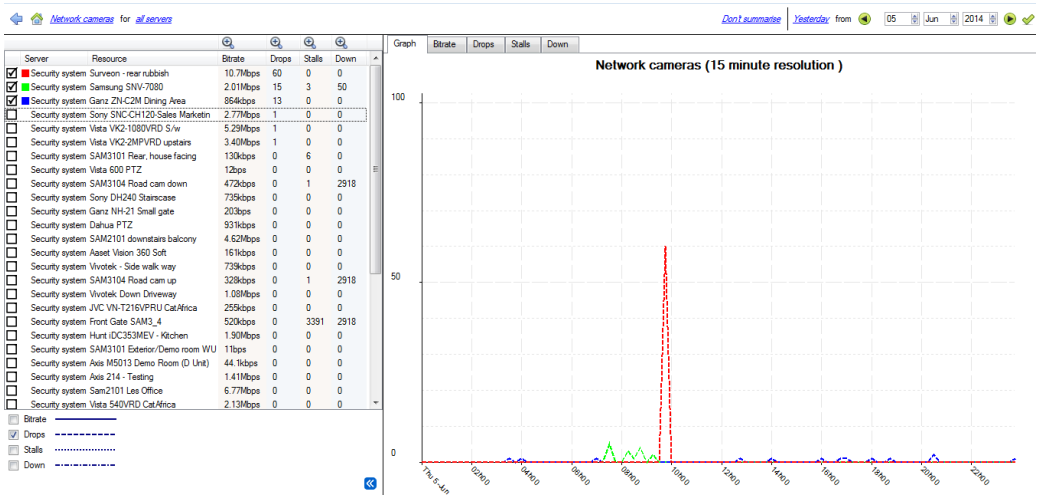
4. In order to graph the cameras, select them on the top left-hand side. Here, the first 3 cameras are examined.



5. One only needs to view the network “Drops”, on the selected cameras. Hide the Bitrate, Stalls and Down time:



The figure below shows packet loss on the “Security System Surveon” camera. It indicates 60 packets being dropped at around 10 am:



Appendices

Appendix A: Configure Custom CatMobile http listening Port

This section explains how to define the custom http listening port for each NVR unit. It lists the procedures to change the default listening port for http or https connections to the NVR unit/s. This should be done on each NVR unit that needs to be reached from outside the company network.

This change could be required if the default HTTP port (TCP PORT 80) has already been assigned to another company webserver. This change could also be required if there is more than one NVR unit on site, and the router at site is not able to port forward the incoming custom http port to the default http port 80 for each NVR unit.

Supported Software version: CathexisVision 2020.2 and later. Please contact support to update the listening port for older CarthexisVision software revisions.

Windows

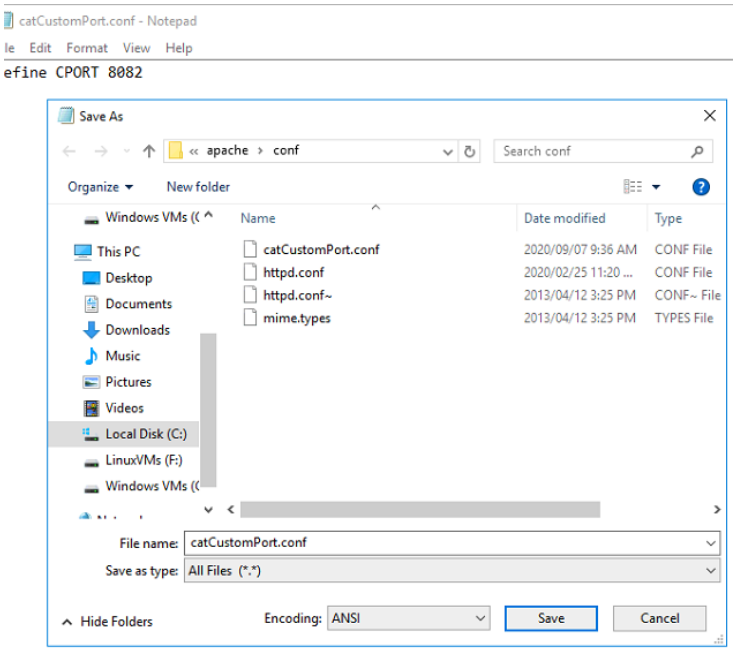
Create a file called “catCustomPort.conf” containing only “Define CPORT Port_number” where Port_number is the port desired for use.

Windows x64 path:
c:\Program Files\CathexisVision Server\apache\conf\catCustomPort.conf

Open Notepad and define the custom port as per the example below:

Note:

- When saving the file in notepad, change the “Save as Type” to “All files (*.*)” so no text extension is created for the saved file.
- Do not use TCP port 8080 as this is internally used by the CathexisVision mobile service.



Restart the recording server for the http port change to be updated.
Alternatively, restart the CathexisVision HTML server manually by opening the web browser.

- visit http://127.0.0.1:33101/control
- login with CathexisVision admin credentials (default is admin admin)
- stop and start nvr_htmlserver

Ubuntu

Create a file called “catCustomPort.conf” containing only “Define CPORT Port_number” where Port_number is the port desired for use.

Ubuntu path: /etc/apache2/catCustomPort.conf

Note: Create the file using an Ubuntu text editor like vi or Emacs.

Restart the recording server for the http port change to be updated.

Alternatively, restart the apache service:

- Open a terminal window in Ubuntu
- Type “sudo apache2ctl restart”

Appendix B: TCP vs UDP for Video Surveillance

Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are widely used network protocols. Video is sent using either RTP over UDP or RTP over TCP as part of the underlying transmission protocol.

- Both TCP and UDP are part of the IP4 protocol stack.
- Both break down data into frames and packets for transmission via ethernet.
- Most IP cameras support both TCP and UDP but generally it is not user controllable.
- VMSes vary significantly in what configuration or control they support for TCP or UDP.
- There are minimal latency differences between TCP and UDP on a dedicated network.
- In IP video, TCP and UDP may perform similarly in dedicated surveillance networks, as error correction and its associated overhead are less likely to come into play.

There are differences between TCP and UDP which make each more or less suitable to certain purposes. Some key differences are outlined below.

	TCP	**UDP**
When bandwidth is insufficient for video stream needs	Data throughput is significantly delayed and eventually the link is closed.	Tends to smear images. May provide lower latency streaming.
Live video streaming over congested networks	If fine movements are to be observed and greater time between the event and detection can be tolerated, the delays possible in TCP may be preferred, to more likely ensure all frames are seen.	Tends to be smoother. UDP's lower overhead is useful in live viewing applications, because it is important that operators receive timely notification of events. Network glitches may cause dropped frames, but events generally span more than a handful of frames, allowing the operator to determine what has occurred regardless of missing video.
Recorded video	Tends to have fewer errors. When recording a camera via a low bandwidth connection, such as cable or DSL, TCP is preferred. This helps to ensure that all frames of video are received and recorded in order.	As per the live video streaming.
Connection	TCP requires a connection be set up between the two communicating devices, performed via a handshake process, before data may be sent.	UDP does not require a connection be created prior to transmitting.
Error checking/delivery of packets	Acknowledgments are sent by the receiving device after every transmission, confirmed as received before the next set is sent. If the acknowledgement is not sent to the sending side within a certain time, the packet is re-sent, until all data is properly sent. *Advantage*: this normally guarantees delivery (assuming there is no fundamental problem with the network).	Packets are simply sent to the recipient without confirming their reception. Because of this, packet loss and errors are more common in UDP. The sender does not wait or check to see if the recipient has received all packets in one set, it simply continues sending the next set. *Advantage:* the overhead of the protocol is lower than TCP because there is no management of the acknowledgement process.

	Disadvantage: the network is loaded with additional traffic, and a delay is introduced in the total data transfer since a failed packet has to be retransmitted.	*Disadvantage: t*here is no guarantee that the packets will arrive at the receiving device in order. The application software needs to deal with this potential ordering problem.
Lost packets	Retransmitting the packets might temporarily resolve lost packets, but does not deal with the underlying issue of network load or partially functioning devices.	The video streams with lost packets may be damaged, with missing frames or frames that are damaged. This results in a video stream with artifacts such that objects or people in the video may not be identifiable.
Conclusion	Using TCP will deal with temporary problems in transmission on a network by retransmitting and hiding the problem. This is acceptable when problems are minor or uncommon. When the problem is constant and the packet loss heavy, the installer needs to deal with the fundamental problems which would cause the system to run sub-optimally in the longer run.	Using UDP as a transmission mechanism is preferable, and it indicates that the network architecture will support the data load and is functioning correctly. If the packet loss indicator is shown in the Cathexis interface it is an indication of a problem either with the camera, or network infrastructure, that should be properly resolved.

Appendix C: Configuring failover features

A hotspare can:

- search for recording servers at specific IP addresses. This is required when broadcast/multicast packets are not received due to the network layout.
- be configured to only monitor a subset of recording servers on the site.

Both of these features are configured in an ini file on the hotspare. The following can go in the `failover/data/control/failover.ini` file:

```
[monitor]
addresses=192.168.0.108,192.168.0.109
servers=1,5
```

`addresses` is a comma-separated list of IP addresses to search for recording servers.

`servers` is a comma-separated list of IDs of recording servers. This ID can be found in the tool-tip of the server in “Server setup”.

Note: For these settings to take effect, the hotspare software needs to be restarted.

Index

access rights
- audio listen
- cameras
- camera tamper
- configure camera
- configuration
- control PTZ tours
- general site
- database
- definitions
- inputs, outputs and monitors
- LDAP
- non-admin users
- privacy zones
- setup tab
- users

adjacent camera mapping
- page manager
  - organise cameras into folders/pages
- map cameras
  - add cameras
  - link cameras
  - organise cameras
  - right-click options
  - variable zoom control
- setup interface
- setup

analogue matrix

analytics
- accessing
- basic, intermediate and advanced
  - advanced settings
    - object classifier
    - property editor
    - default counting overlay
    - default paths overlay
    - flare suppression
    - image stabilisation
    - size filter
    - source size
    - tracking point
    - use colour
  - basic settings
    - background model
    - tracking area
    - sensitivity
  - calibration
    - basic
    - advanced
  - triggers
    - basic line triggers
    - basic presence trigger
    - advanced area triggers
    - advanced line triggers
    - speed triggers
- running interface
- basic object classifier
  - settings
  - triggers
- basic people proximity
  - settings
  - triggers
- basic VMD
  - adaptive noise suppression
  - background model
  - day/night settings
  - noise suppression
  - triggers
  - zones
- configure new analytics
- configuration interface
- copy-paste an algorithm
- interface guide
- licenses
- mask detector
  - settings
  - trigger
- smart VMD
  - advanced settings
  - background noise
  - flares
  - profiles
  - threshold
  - day/night settings
- counting analytics
  - line counter
- motion database
  - new cameras
  - settings
- queue length analytics
  - triggers
  - zones
- still object analytics
  - algorithms
  - zones
- top-down head tracker

triggers
testing
thermal face temperature
add camera
settings
models
triggers
archiving
archive video manually
archiving profile
scheduled archives
cameras
adding cameras
activity recording
add/edit a video feed
H264
JPEG
multicast
camera connection
copy/paste new camera
discovered mode
sequential mode
covert camera
edge recordings, review setup
enable analytics feed
encryption. See secure camera connection and control
general settings
I/O setup
PTZ, configure settings
scheduled recording
serial ports, configure
video feeds
configuration
edit camera
access rights
pre-events tab
privacy zones
reference images
secure camera connection and control
video analytics button
configure servers
open configure servers
server setup
audio
backup
base-stations
email setup
gateway
general
server heartbeat
user recordings
create and manage sites
databases
add database
alerts
edit
edge insertion
import
manage storage
network drive
max recording limit
slice
write policy
diagnostics
audit server
audit site
forensic tool
server/client statistics
sherlocks
events
metadatabase
archive database recordings
create events metadatabase
device event metadata
general database
integration database
integration/metadatabase
locate entry
navigate to
replay associated recording
review multiple cameras
scheduled reports
viewing entry's associated recording
system events
navigate to system events
actions
call base station
control integrated device
control output
control PTZ
control virtual input
play audio clip
record camera
record trigger cameras
send email

- general setup
- new events window
- resources
  - default switch display settings
- triggers tab
  - camera tamper trigger
    - single camera tampers
    - multiple camera tampers
  - integrated device triggers
    - device parameter
  - standard triggers
    - any and all
    - filter period
    - when and while
  - trigger template

failover

- example
- model
- setup
  - add failover server to the site
  - client settings
  - configure failover network interface
  - database
  - define global failover settings
  - failover insert database
  - install failover server software
  - introduction
  - requirements
  - site master settings
- licensing
- limitations
- minimise failover loss
- recommendations
- system restore

forensic tool

- date/time selection
- data values
- interpreting the graph data
- quick view
  - live/historic
  - multiple graphs
- selected views
- summary view of servers
- network camera summary view
  - database writes view
  - dropped packets view
- video streaming view
- software compressor view
- internal messaging view
- network camera view of cameras
- network cameras view
- database cameras view
- events view of cameras
- graph window
  - zoom in on a period
  - data values
  - export as CSV

GUI

- cameras tab
- command line options
  - add multiple GUIs
  - connect client to alarm gateway
  - set max number of reviewable cameras
  - set numbers of monitors
  - view legacy archive viewer
- menu bar guide
  - edit menu
    - enterprise manager edit menu
    - general edit menu
  - file menu
    - archive viewer
    - enterprise manager
    - open site
    - open site list
  - help menu
    - access manuals
    - enable support user
    - server/client statistics
  - settings menu
    - connect to alarm gateway
    - DPI scaling
    - language settings
    - number of forms
    - openGL
    - relay double click action
    - switch alarm display
    - video display
      - alarms
      - aspect ratio
      - default event notifications
      - deinterlacing
      - fastest scaling
      - live time format
      - live video resolution
      - maximum live streams
      - old-style mouse handling

performance
pixel shaders
resource panel location
show recording
show review button
show time
source pixel aspect ratio
switch display settings for new tabs
site menu
audit
custom event notifications
fetch report
setup
tools menu
sherlocks
video wall menu
layout
create new
manage
overwrite
recall
resize
sequences
recall sequence
sequence editor
sequence manager
switch display settings for this tab
view menu
minimise GUI
monitors tab
send text message when alarms are received
status bar
supported GUI languages
inputs/outputs
analogue
network
installation
antivirus
hardware requirements
installation wizard
performance wizard
requirements/restrictions
routing/port requirements
supported operating systems
integration devices
important considerations
recording
integration database
database procedures
initialise database
new integration database
integration devices panel
configuration tabs
device events
general
object configuration
object groups
object properties
new device
keyboards
add to base station
add to recording server
licensing
licensing from a local unit
pack file
product key
licensing from a remote unit
trial license
master unit
monitors
access rights
add a monitor
VGA monitor
XP monitor
licensing
monitors tab on a base station
run on startup
video wall software
multicast
PTZ
general settings
home position
priority control
procedures
PTZ tours
zoom speed
reports
add schedule
create new
fetch report
cameras report
database usage report
disks report
environment report
events report
file system report

- hardware report
- license features report
- licenses report
- NTP queries report
- Reboots report
- recording times report
- software report
- system report
- system setup report
- unit up-time report
- user defined report
- VMX counters report
- VMX temperature report
- Windows unit report

resource panel
- setup
- add a resource
- create a folder
- delete folders and resources

scheduled recording

schedules
- create schedule

site actions
- action types
- add to event
- add to schedule
- create new

site setup
- configure archiving
  - overview
  - create new profiles
  - configure watermarks
  - password options
  - access levels
- multicast

sites
- enterprise manager
- master unit

TCP
- Compared to UDP

technical alarms
- alarm types
- general settings
- operating system support

users
- create new user
- LDAP
- non-administrative users
- site resource access rights

virtual inputs