CathexisVision 2018.4 Setup Manual

Contents

Installation Chapter

1 Getting started with CathexisVision

Installation of any **CathexisVision** software is straightforward. It requires one installation file for the NVR and one file for the Client. This is because the software works on a licensing format, so one installs the whole package, and unlocks the features using licenses.

This makes for a very dynamic environment where one can add abilities (such as integrations) by simply updating the license.

The purpose of this chapter is to provide guidance through the initial steps of the setup process. These are:

- Installing CathexisVision NVR or the CathexisVision Client.
- Getting **licensed**.
- Creating the Site with the **Enterprise Manager**.

Note: While one needs to install the NVR and Client software on one's respective units, an administrator can make all relevant changes via either software installation, i.e. changes can be made to the Site from a Client or NVR. The Client unit can be local or remote to the site. It is advisable to install the same versions of both the CathexisVision NVR and Client software on the same site.

2 Requirements/Restrictions

The latest CathexisVision Software can be downloaded from the Cathexis website: www.cathexisvideo.com
Note that there is a **minimum requirement of 4 Gigabytes of RAM** to run the CathexisVision software.

a. Supported Operating Systems

Listed below are the supported operating systems.

Note: Supported systems apply to all contents of the CathexisVision software install, including:

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

Not Supported

The following systems are **not supported**:

- Windows XP and earlier,
- Windows Vista,
- Windows Server 2008,
- NetBSD.

Linux

Fedora 16 (32-bit)

- Ubuntu 12.04 LTS Desktop (32-bit)
- Ubuntu 16.04 LTS Desktop (64-bit)

Windows

- 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

b. Windows Update Requirements

The Universal C Runtime Update is required for certain systems.

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 2018.4 onwards, Windows Vista and Windows Server 2008 are no longer supported. Thus, the update for 2018.4 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 one 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)

c. Hardware Requirements

The **CathexisVision** software architecture is designed to utilise the various hardware system components with maximum efficiency.

When choosing hardware, there are many system setup configurations to be taken into consideration. Some examples are:

- **Camera resolution, Frame rate and bitrates** for recording
- **Camera resolution, Frame rates and bitrates** for "live" viewing
- **Video Analytics**: Edge based (IP camera) or Server based (**Cathexis** software) processing?
- Whether cameras are being viewed "**live**" from the recording or a separate video wall server
- Whether "**multicast**" video streams are being streamed from the camera
- **Video Storage** methodology (local server, Network Storage etc.)

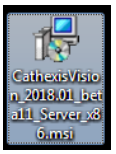
Below are some guidelines to assist in choosing the right hardware for an application. There are system Design Tools available on the CathexisVision website. For further assistance with a design contact a distributor, or a **Cathexis** regional office.

CathexisVision System Requirements Guidelines:

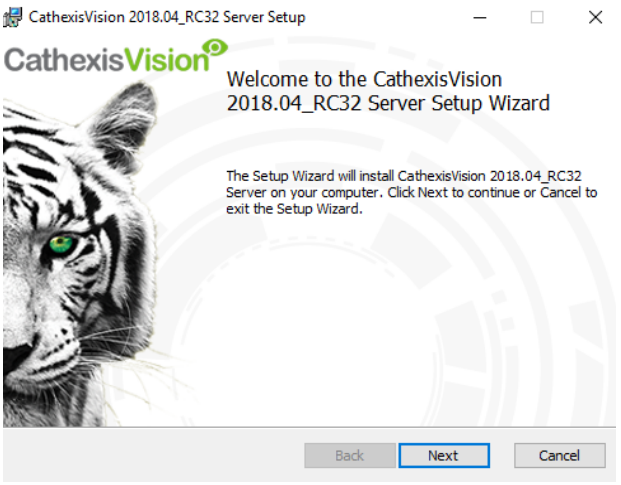
Processor	RAM	Operating system	Recording camera bitrate (Mb/s)	Live View Megapixels/sec
Core i3	4GB	Windows 7-64bit	Less than 100Mb/s	< 100 MP/s
Core i5	8GB	Windows 7-64bit	Less than 150Mb/s	< 300 MP/s
Core i7	8GB	Windows 7-64bit	Less than 600Mb/s	< 600 MP/s

3 Installation

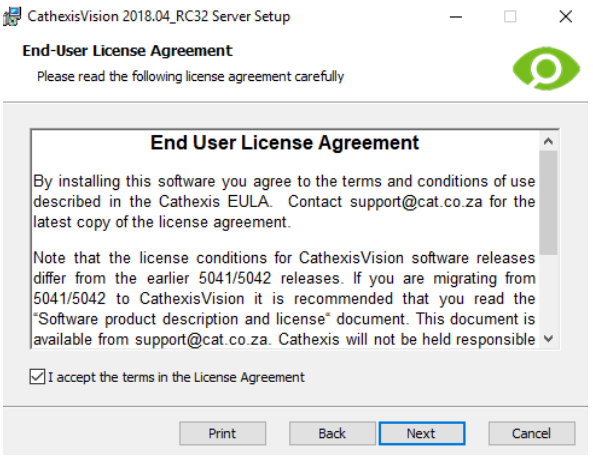
Installation is straightforward, and intuitive. Double click the installation file (.msi) to run the setup wizard.



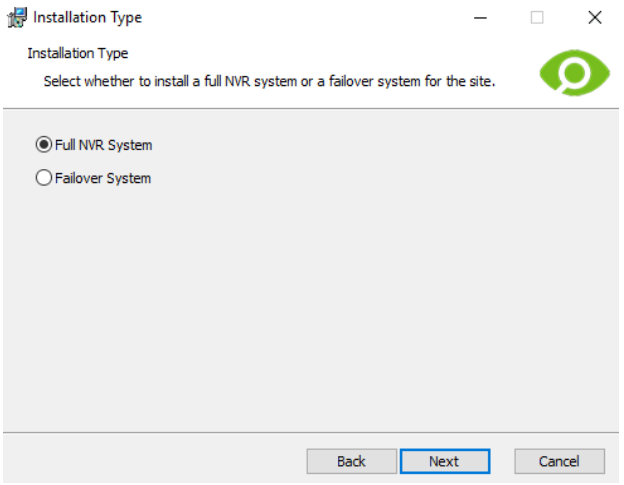
a. Follow the Installation Wizard

1. 

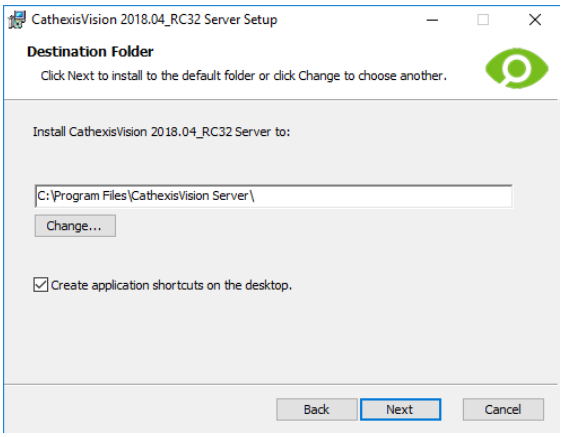
Click **Next**.

2. 

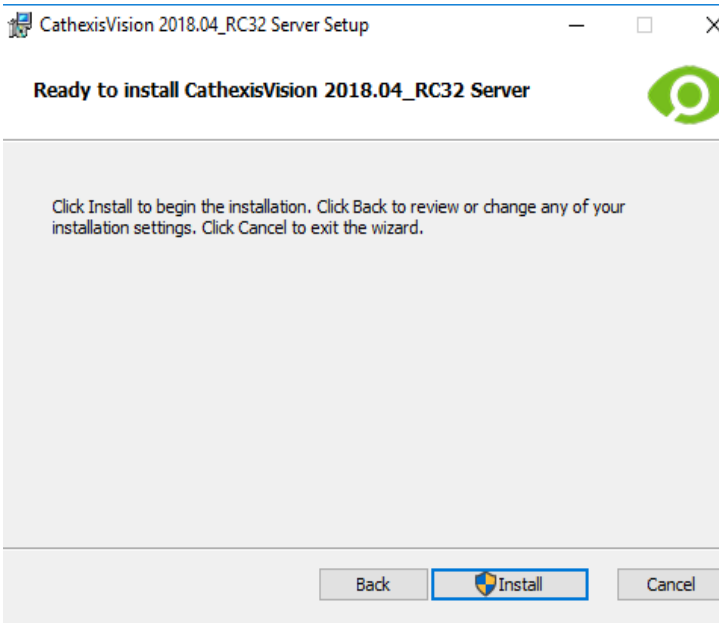
Accept the End User License Agreement.

3. 

Choose between a **Full NVR System** and a **Failover System** installation.

4. 

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

5. 

Click **Install**, and when the installation is complete, click **Finish**.

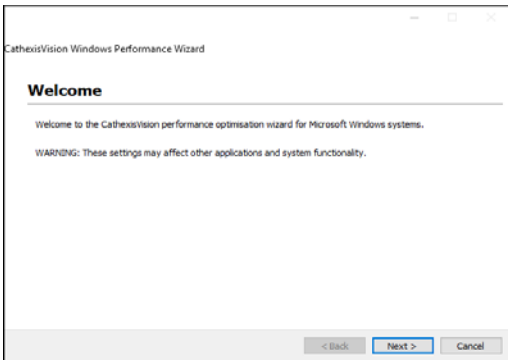
- ***Failover Installation***

If the Failover installation is chosen, attempting to run **CathexisVision** (by double clicking on the **CathexisVision** icon) will bring up the dialogue box to the right:

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

b. Cathexis Windows Performance Wizard

Leave the **Launch Performance Wizard** box ticked. The Performance Wizard optimises several Windows system settings for the use of **CathexisVision** software. While it should be run immediately, it may be run any time after installation.



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

Disable DOS 8.3 filenames on NTFS partitions. This is a required setting for using the database engine.	Required
Disable the Last Access timestamp on NTFS partitions. This provides a small performance gain when accessing large volumes of files.	Recommended
Enable the High Performance power management scheme. This adjusts power settings to allow the best performance of the system.	Recommended
Disable the Windows Defender service. This isn't required but it provides a small performance gain over a secured system however integrations ports may be blocked.	Optional
Disable the Windows Search Indexing service. Provides a significant performance gain by preventing background indexing of the file system.	Recommended

Disable the Windows Desktop Manager Service. Will disable the Aero desktop and appearance enhancements to reduce graphics system load.	Optional

c. Routing/Port Requirements

The following information regards the router ports that need to be opened on the network firewall/router/anti-virus. These ports are important in allowing a number of **Cathexis** services to run correctly.

Please ensure that these ports are also opened on the anti-virus (if running one).

- ***Ports to Open***

Operational Ports	Protocol	Application
80	TCP	Default CatMobile Access
30010-30100	TCP	CathexisVision Software
Maintenance Ports	**Protocol**	**Application**
22	TCP	Secure Shell (SSH) - Linux
3389	TCP	Windows Remote Desktop
NA	NA	TeamViewer Access

- ***Remote Support***

Please download and install one of the following programs relevant to the operating system to ensure remote support is available.

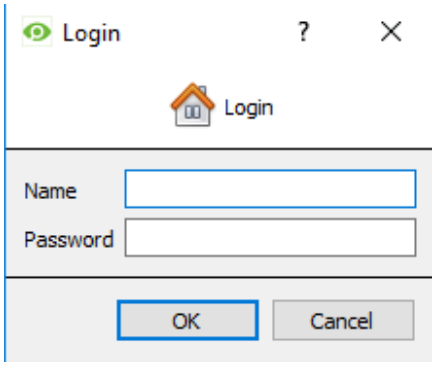
Linux: Secure Shell (SSH - TCP port 22).
Windows: Teamviewer, or Remote Desktop.

d. Finish Installation

Once the Performance Wizard is finished, installation is completed. One may wish to install the **CathexisVision Client** software on client servers.

e. Log in

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



Default Login Details

Username: admin
Password: admin

NetBSD servers and all pre-CathexisVision 2014 systems:
Username: dvs
Password: dvs

4 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.

a. 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 permanent 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.

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 database (provided there is space, 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 licenses to unlock the database and review all recordings for as far back as the database has recorded.

b. 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 (4b Licensing from a Remote Unit).

Internet Connection: Product Key

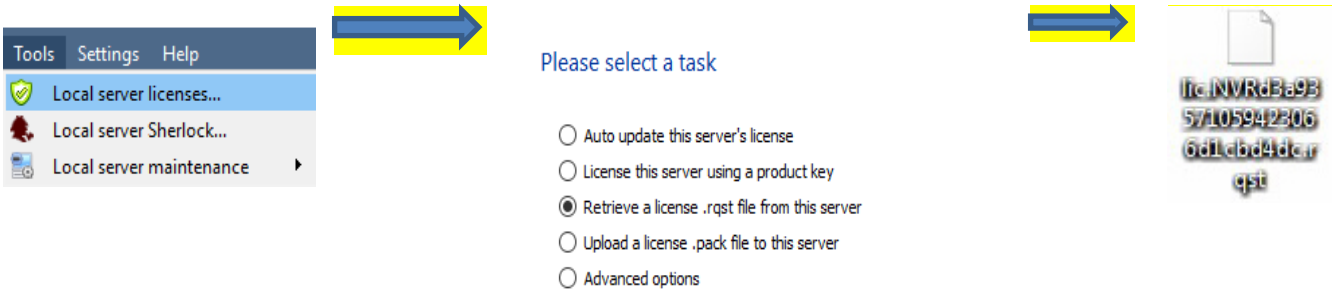
If there is internet access and the vendor supplied a product key, enter the product key. The system will connect to the online licensing system and complete the process.

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 support@cat.co.za, who will then return a **.pack** file. To receive the **.pack** file, please follow the instructions below:

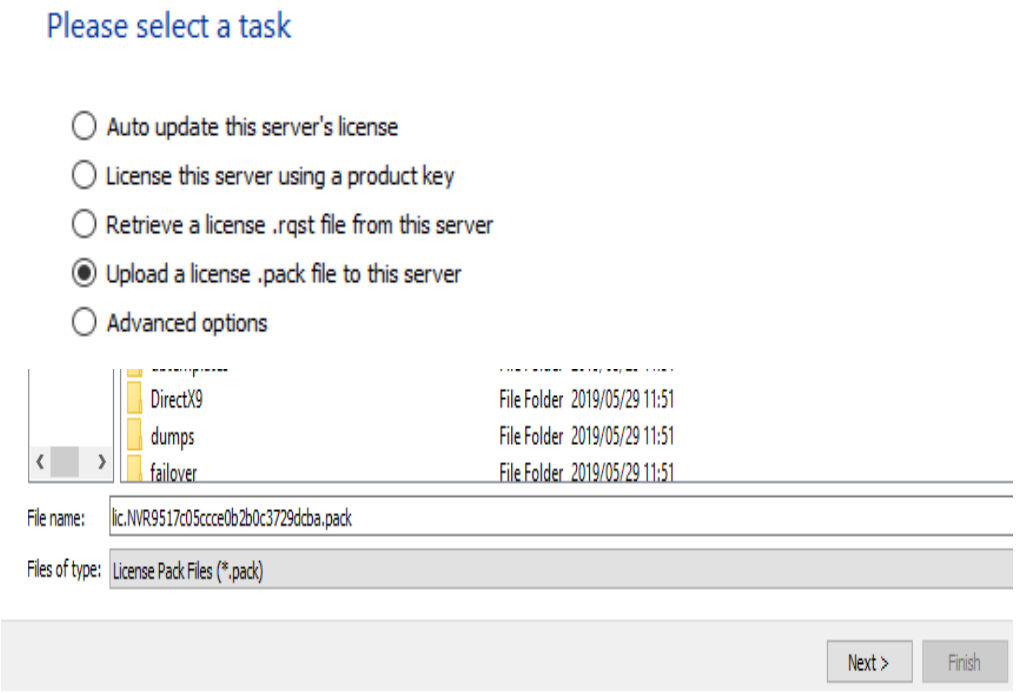
- ***License Request File***

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.

- ***Upload .pack File***



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

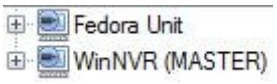
c. Licensing from a Remote Unit

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:

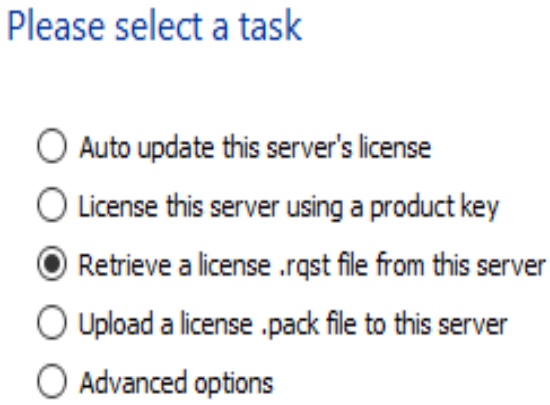
Open Configure Servers

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.

5 Create and Manage Sites

a. 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 entered 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, it is not necessary to add a new Site.
- Units are added to a Site. Cameras and Integrated Devices are added to the NVRs.

What does it mean to add a Site?

It is important to understand that when adding a Site in the Enterprise Manager (dealt with below), one is not creating, or even editing a Site. One 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.**

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 masters IP address to that of the old master unit).

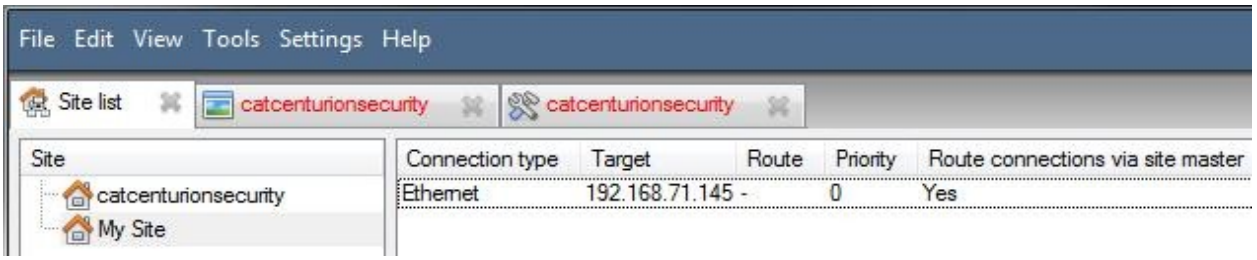
b. Open the Enterprise Manager

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. On this tab add and manage Sites.

c. Create and Organise Sites into Folders



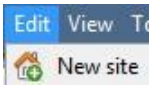
The Site list is in the panel on the left, in the above image. Click on a Site to see the Site's connection details displayed in the panel on the right. There are **three steps when adding a connection to a new Site:**

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

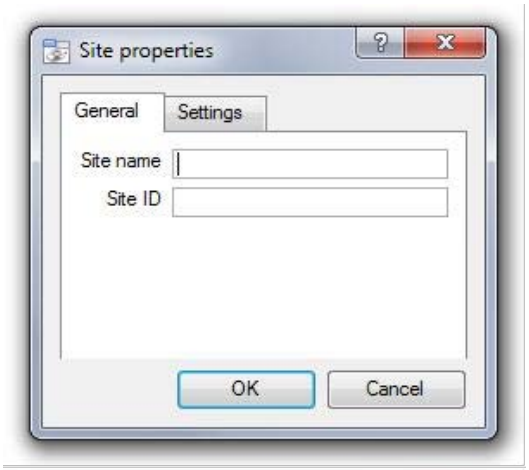
Add a Site Name

This entails adding the name of the Site to the Site List. There are two ways to add a new Site:

- Right-click on any whitespace in the **Site** list panel, and click 

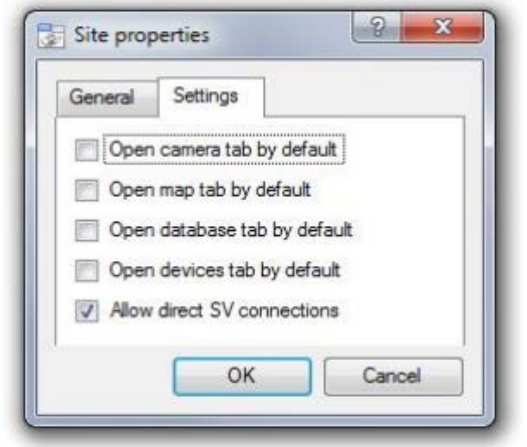
. Or,
- In the Menu Bar, click on **Edit → New Site**. 

Both of these options will bring up the *Site Properties* menu.



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

Leave the Site **ID blank** for now; this will be fetched after a Site connection is added.



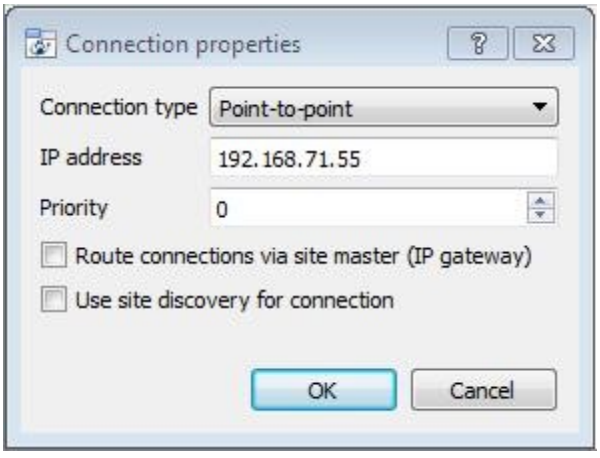
Under **Settings**, choose which tabs open when a Site is opened (Cameras, Maps, Database etc.) and whether or not to enable Direct SV connections. Direct SV connections relates to streaming video to Video Wall.

If the Site is connected to a Gateway, the **Access tab** will be displayed. Here, specify Gateway User Levels.

- ***Add a Connection to Site***

Here, one is adding 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 

. This will bring up the Connection Properties menu:

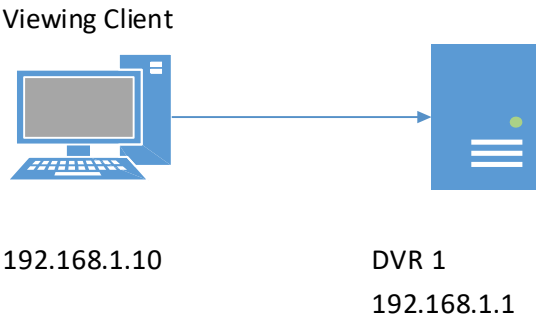


Note: This is not creating or editing a Site. One is adding the connection to the Master unit of an **already existing Site**.

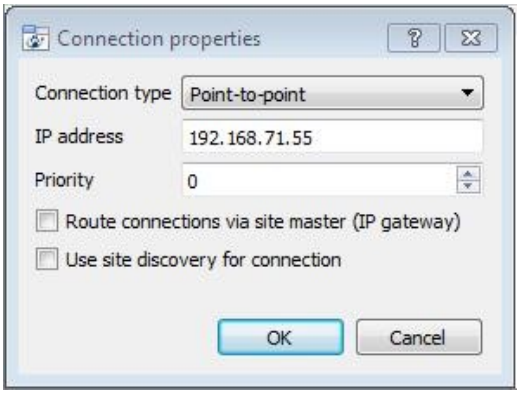
Connection Type

Connection methods are used to connect the Site. There are two connection types. **Point to Point**, and **Multi-step**. They will be described below.

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: the switches have been left out of the images for simplicities sake.



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 unit one wishes to reach, 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, one can add these methods as separate individual connections. In the image, there are two connections. A connection with a Local address (192…), and another one with a dyndns address.

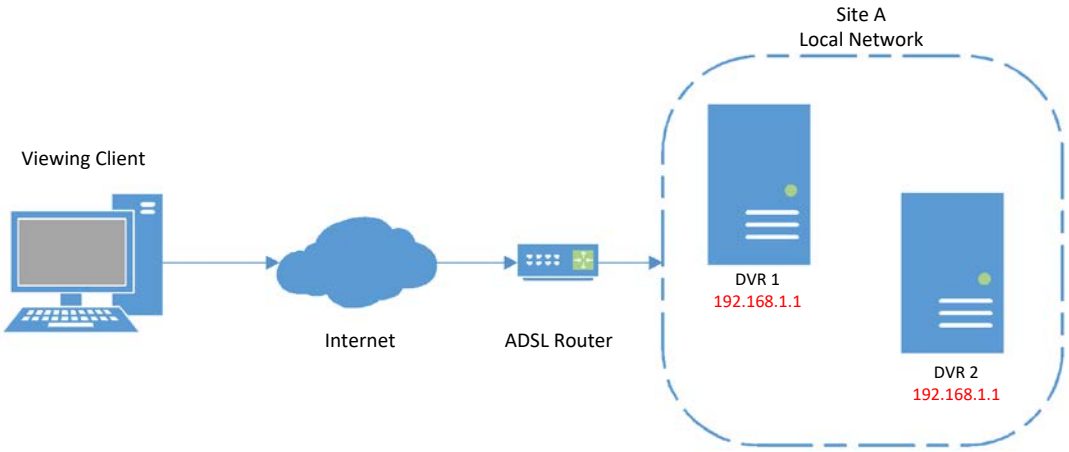
These both direct the client to the same Site. The 192… address is accessible only via the LAN, and the dnydns gives access from outside of the LAN (over the internet, for instance).

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 -----7the 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 for each connection, 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.



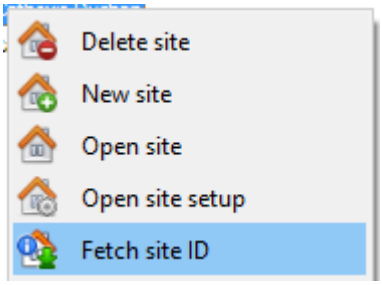
Use Site discovery for connection

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.

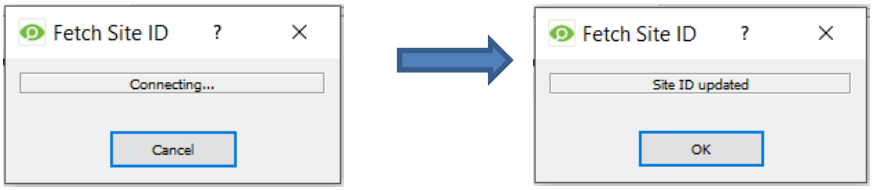
Important Note: If there is a failover system setup (see the Failover section of this manual), this option must be checked. This is if one wishes to access the Site via the client in the event that the **Site master** is failed over.

Connection Type	Gateway	Information required
Ethernet	Point-to-Point	o Target unit IP Address o Ethernet specs (is it Internet, WAN, 10MB LAN, 100MB LAN, or 1GB LAN?) o IP gateway connection mechanism (if necessary – refer to IT dept.)
	Multi-step	o Target unit IP Address o Target via unit IP Address o Ethernet specs (is it Internet, WAN, 10MB LAN, 100MB LAN, or 1GB LAN?) o IP gateway connection mechanism (if necessary – refer to IT dept.)

- ***Fetch Site ID***



Right-click on Site Name, and click Fetch Site ID:



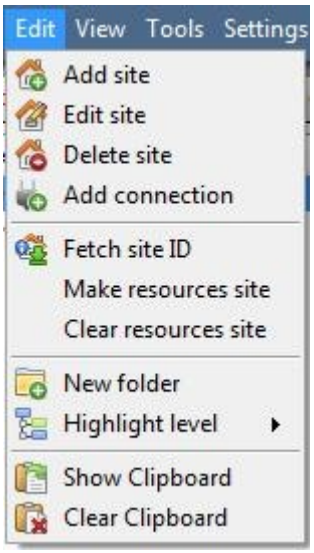
This will serve to test the connection, and retrieve important information about the Site from the master unit of that Site. Once this is done, connect to the Site via **File → Site → Your_Site_Name.** Each Site should have a unique Site ID. The Site ID is generated automatically when loading the NVR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

d. 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.

Important Note: The maximum number of per process sockets on Windows has been increased so that a VMS client can make more than 64 simultaneous Site connections.

6 The Site List 'Edit' Menu



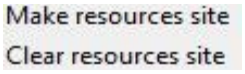
While in the **Enterprise Manager tab**, the '**Edit**' menu option will appear in the menu bar, in the form displayed to the left.

Use the **Edit menu**, as opposed to using the right-click options, to complete all steps mentioned thus far.

There are a few options in the initial addition stages that allow one to make changes to the Site at a later stage. These are examined below.

- ***Make or Clear a Resources Site***

One may have a Video Wall attached to this Site, and want 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.



For 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, consult the Monitors section of the Configure Servers document.

- ***New Folder***

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 has been done, individual Sites can be clicked and dragged in/out of the folder.

Now, under **File** → **Open Site** there will be a folder, containing the Sites:

- ***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.

7 Anti-Virus Exclusions

When 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 the installation folder/s from anti-virus scanning.

The sections below indicate the default installation folders and paths which need to be excluded from scanning.

a. Folders to Exclude in CathexisVision 2018+

For Sites running CathexisVision 2018, 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.	

b. 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 the installation folder/s from anti-virus scanning.

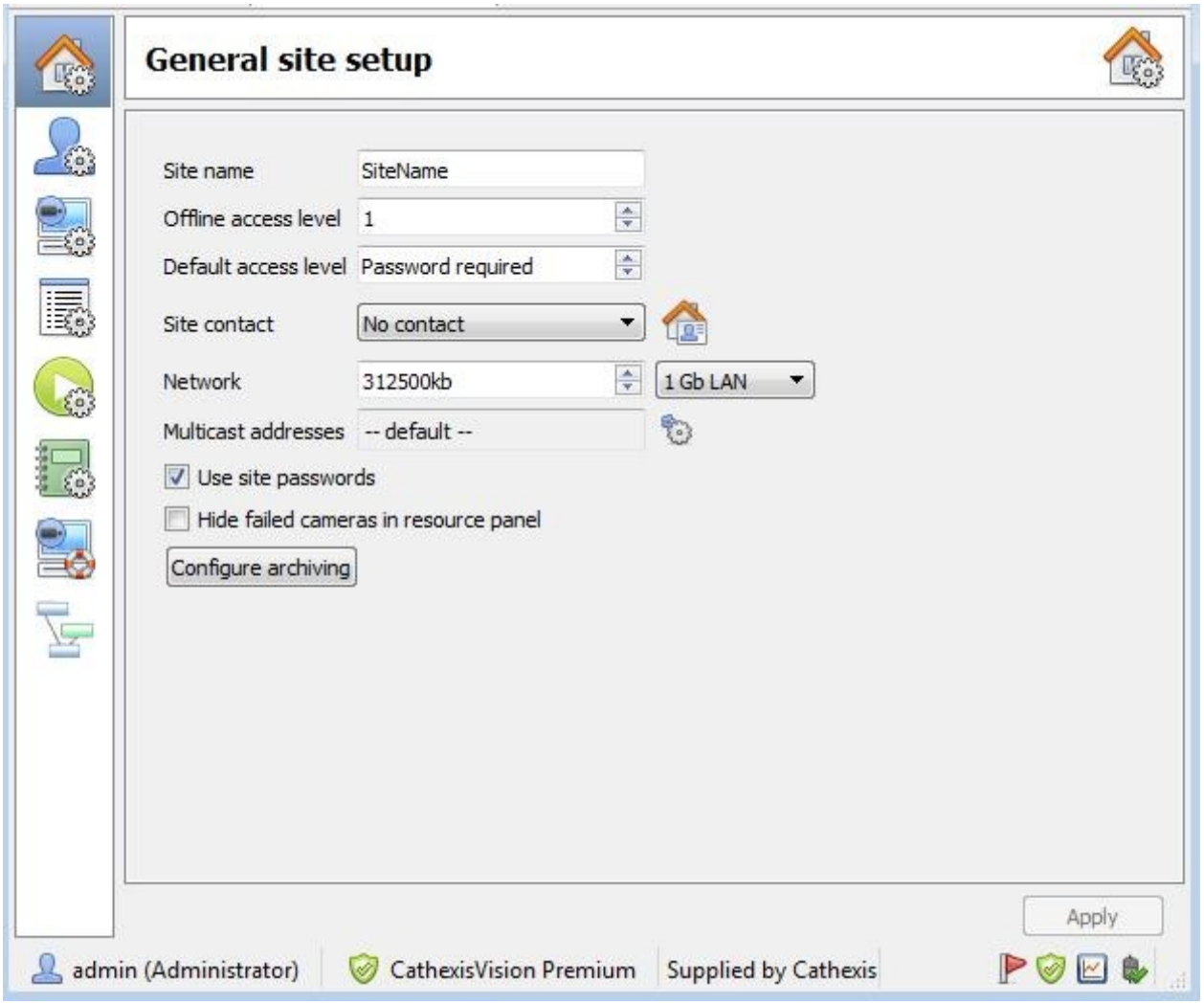
CathexisVision Server	**Folders to Exclude**
	c:\program files\Cathexis CathexisVision Suite NVR
	c:\program files (x86)\Cathexis CathexisVision Suite NVR

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

Setup Tab: General Site Setup

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



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

Users is where users are created and maintained. This includes Login Level, Remote Access, etc., and can be done on a server by server basis, or be controlled as a Site.

Configure Servers is 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 additions 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 location.

a. Setup Tab Access

The ability to open the Setup Tab (and thus access server setups such as user configuration, events, video analytics etc.) is restricted to administrator users only. All other user logins, regardless of access rights or level, are unable to access this tab, thus preventing any operator from being able to change Site configurations.

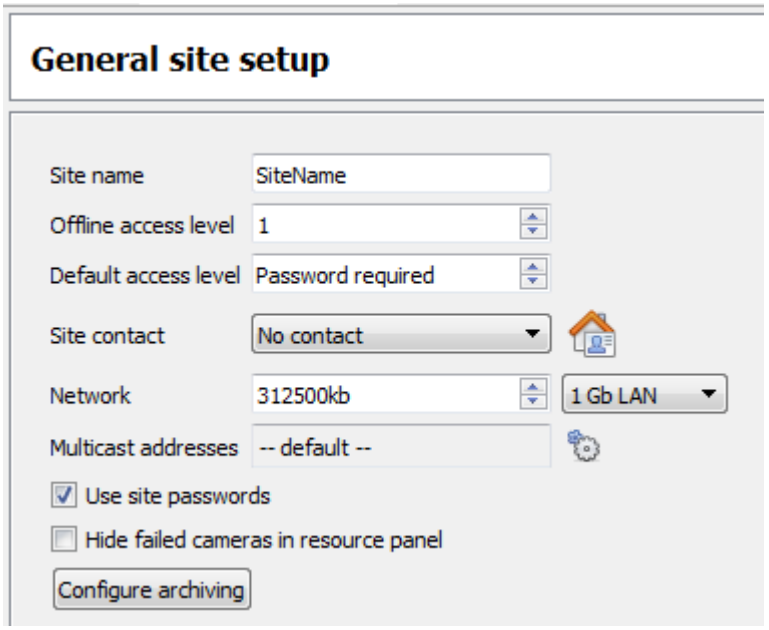
Note: An exception is made for non-admin users who have been given the right to configure other non-admin users. These users will only be able to enter the Configure Users section of the Setup tab and will not have any other part of the system setup available or visible to them.

2 General Site Setup[1]

This is information retrieved from the Site, and not from the unit one is on. The Site information will be stored on the unit called the Site.

Master.

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 is the name of the Site as a whole, held in the Site database.

Note: that 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, this defines what resources he/she can see in the Resource panel.

Options are “No view”, 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.

[1] This was called Global Resources in previous versions of the software.

Note: If the level is set to anything from 1- 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. In order to get audit trails for every session, then set this to *password required*.

Site Contact 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 the  icon. Then select an existing contact, or create a new one.

Network settings are those settings specific to an individual LAN.

Multicast. This will define the multicast settings for the Site as a whole (this is discussed in more depth below this table).

Site Passwords, if checked, 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 setup on the Master Unit, and there aren't any users that one needs 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 will remove cameras that have failed from the Resources list, until they are running again.

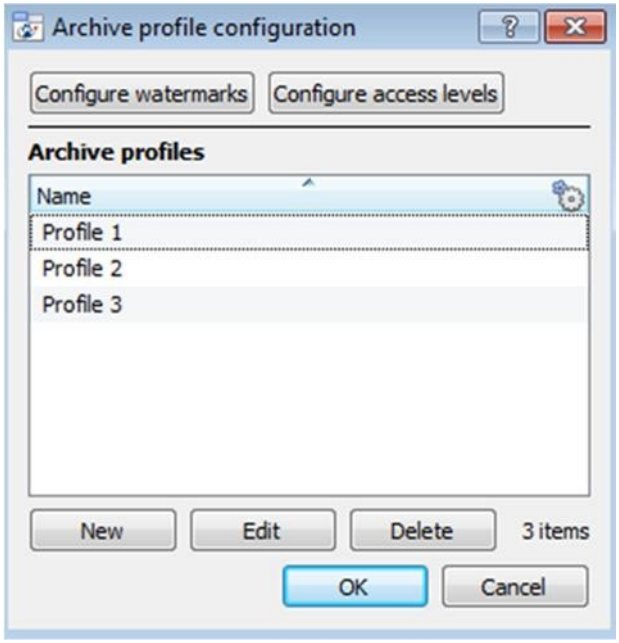
a. Configure Archiving

This section will explain how to create archive profiles, to which one may assign user levels, password protection, and watermarks.

Please 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.

Overview



The process for creating archive profiles is:

1. Configure watermarks.

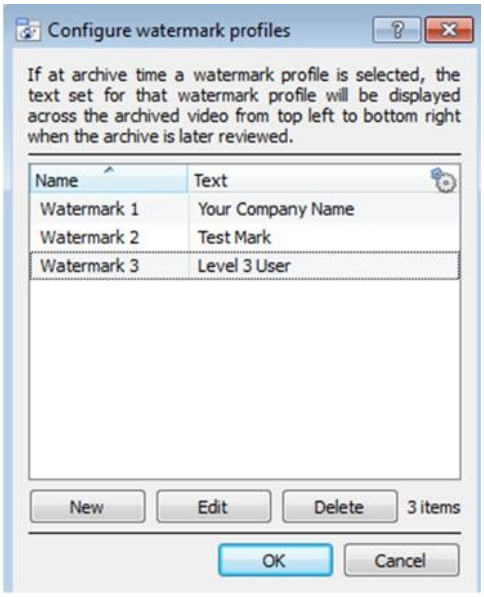
2. Click **New** to create profiles and assign the desired watermark/s to the desired profile/s.

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

4. Click **OK** to save.

Configure watermarks

Click Configure watermarks to bring up the window below.



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

Click  to customise which columns to see in this window.

Click New to create a new watermark profile

Name the profile.

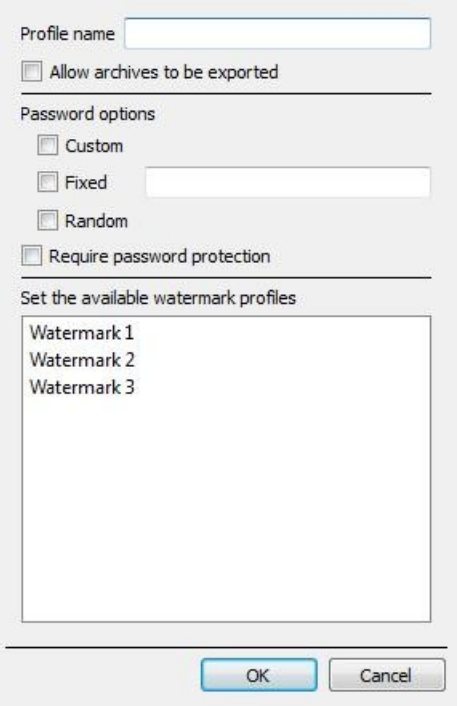
Type the watermark text.

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

When creating all profiles is complete, click **Ok**.

- ***Create new Archiving Profiles***

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

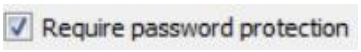


Give the archiving profile a **Name**.

Ticking 

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 

will force a user to set at least one of the password options allocated him/her. 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.

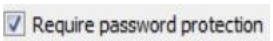
- ***Password Options***

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 now 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.

Single/Multiple Password Options:
One may assign multiple password options to:

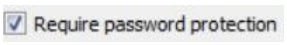
Archive profiles. At the time of archive, the operator will select from a dropdown menu the single/multiple password options that have been constrained in this section. If no password options have been set, the dropdown menu will offer 'None' as a password option.

Ticking 

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

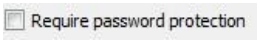
These password options will be displayed to the user in the archive window. Please note that the examples below both have multiple password options set.

Require password protection



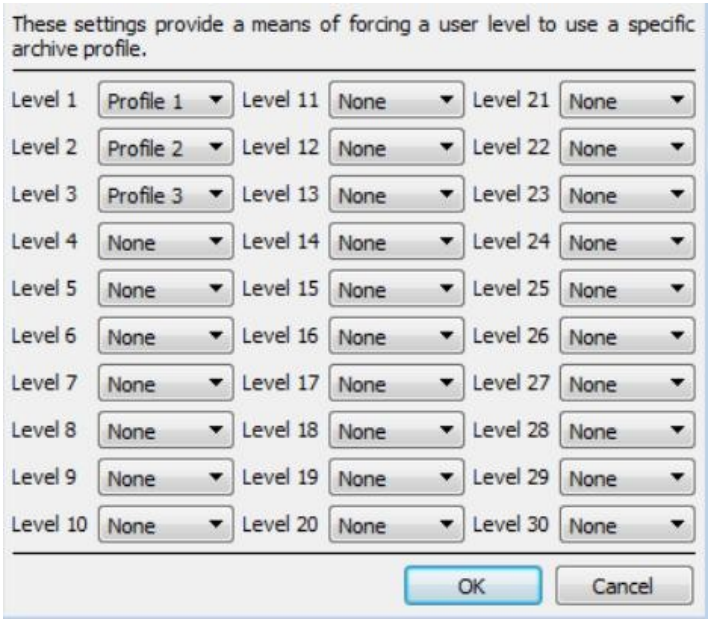
The operator **must set** a password requirement from the options set by the administrator.

Does not require password protection



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

- ***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 dropdown menu next to each user level.

Only one profile can be assigned to each level.

b. A Note on Multicast

CathexisVision has the ability to automatically assign multicast addresses to cameras. When a camera is added to a unit, one may select to have multicast 'disabled', 'automatic', or 'enabled'.

The multicast settings that are in the **General Site Setup** define the parameters of the 'automatic' settings.

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

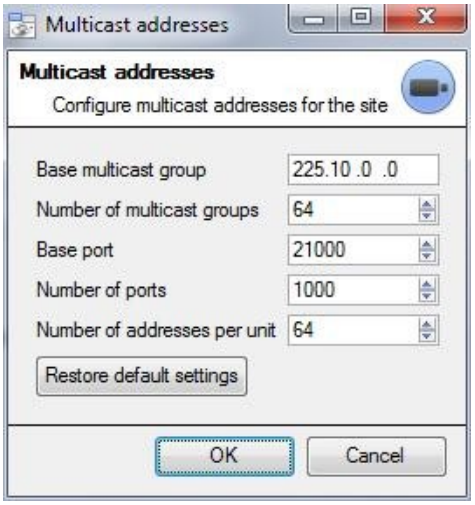
1. The **multicast group** is the IP address that the camera will send multicast packets to.
2. The **Port Number** is the port number associated with the multicast group.

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. Nevertheless, **one may want to change these settings if**:
    a. There are multiple Sites on the same network (one would need to make sure that the ranges don't overlap at all, i.e. the same address: port pair may not exist in both the ranges).
    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 restarted because the device multicast settings are reserved once they have been used.

Setup Tab: Users

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:

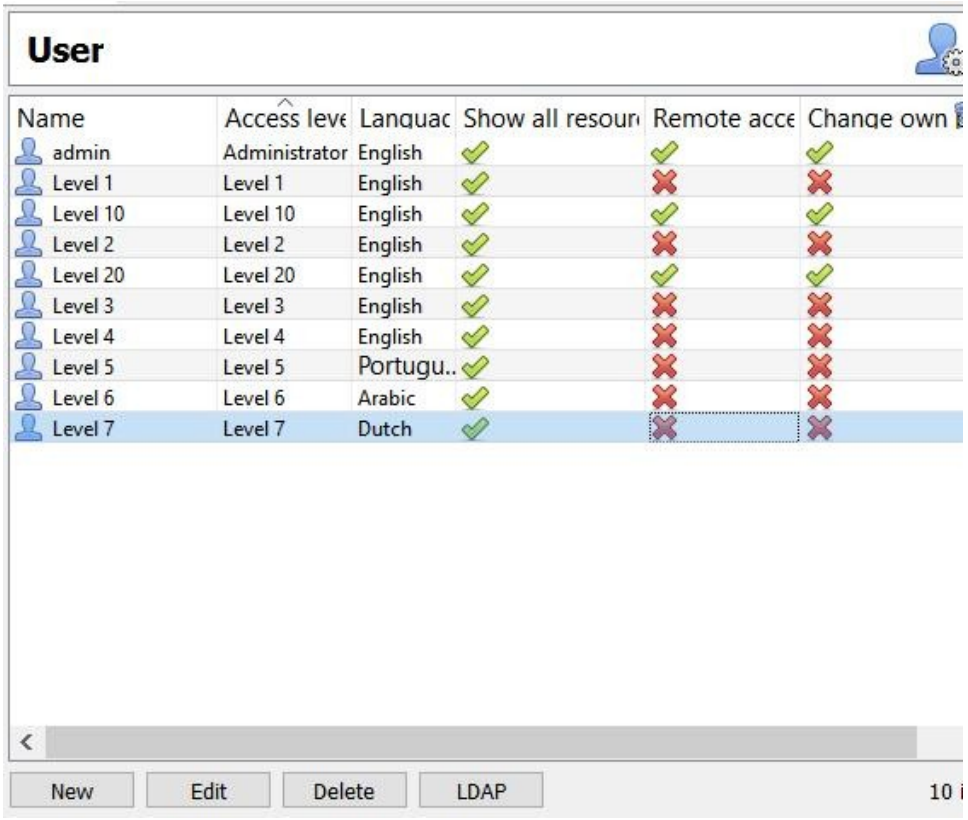
- **Server-based users** where every server had its own set of users.
- **Site-based users.**

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.

1 Introduction

Configure Users can be accessed by clicking on the icon in the **Setup Tab**.



a. Create New User

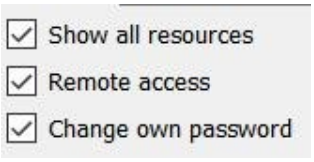
To create a new user, click 

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 dropdown menu.
Select the user's **Language** from the dropdown menu.
Set the user **password**.

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

Uncheck these options to determine whether the following options can be used:



See all Site resources.
Remotely access Sites.
Change his/**her** own **password**.

Note:

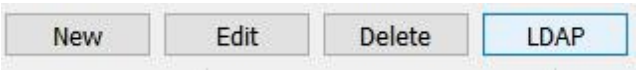
1. In order for Users, and their access levels to be effective the relevant **access level settings** need to have been set under **Setup Tab → Configure Servers → Access rights**. (For more information on this, see **Configure Servers**.)
2. One cannot edit a user's name once that user has been created, but one can edit all other fields.

b. LDAP

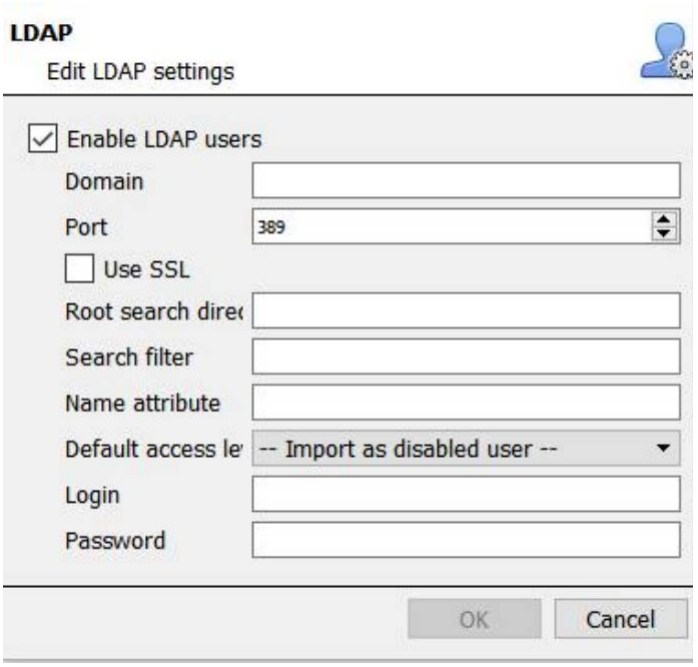
CathexisVision now supports the importing of users from LDAP into CathexisVision. LDAP (Lightweight Directory Access Protocol) is a protocol used to communicate with user management systems like Microsoft's Active Directory.

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



See below for LDAP settings.



Check 

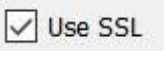
to enable LDAP import.

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, one may edit the file **%SystemRoot%\System32\drivers\etc\hosts**

Enter the Port number of the LDAP server.

Check 

to use transport layer security.

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

- Windows

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

- Ubuntu

1. It may be necessary to copy the certificate to **/usr/share/ca-certificates/ldap**
2. To trust the certificate use:

Sudo dpkg-reconfigure ca-certificates

- Fedora

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

1. Copy the certificate to /etc/ssl/cert
2. 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.

c. 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.
- Will not be able to delete themselves.
- Will not be able to create admin users.
- Import LDAP users

Setup Tab: Configure Servers

1 Configure Servers

Configure Servers is where all server-based settings take place. A **CathexisVision** Site is a collection of one or more individual units which are consolidated in the software as an individual Site. This means that one can add and remove units from Sites, as well as change settings on a unit-by-unit basis.

In the **Configure Servers panel**, one can see a list of all servers, and under each server a list of setting options available on that server:

These 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.

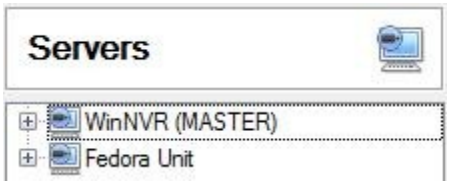
a. Server Options

Open Configure Servers

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

After logging into the Site, to open Configure Server simply click on **Site → Open Tab → Setup.** Once in the Setup Tab click on the Configure Servers icon:

Note: Right-clicking on the tab of any open Site will bring up the same menu as the one accessed via the method above.

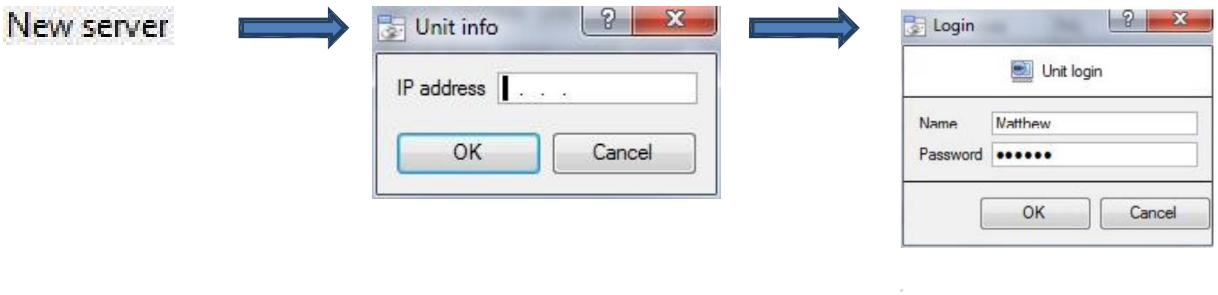


The servers list will be to the right, and the panel to the right of that will contain the options for the current selection.

Add/Detach/Delete/Replace a Unit

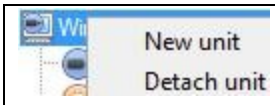
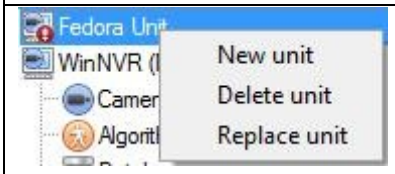
- ***Add a Unit***

To add a new unit to the Site, right-click on any white-space in the servers list panel (one may even click on an existing server), and click on New server. Then 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 **CathexisVision NVR**. One may, however, add an unlicensed unit, as one **may license all servers from the Configure Servers panel**.

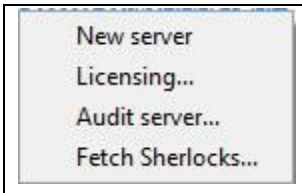
- ***Detach, Delete, Replace a Unit***

	To **Detach** a unit, **right-click on the unit** in the Servers list, and **click on Detach Unit**. 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, and select **Delete** Unit. To **Replace a** detached unit with another unit, right-click on the detached unit and click on Replace Unit. The steps after this are the same as adding a unit.

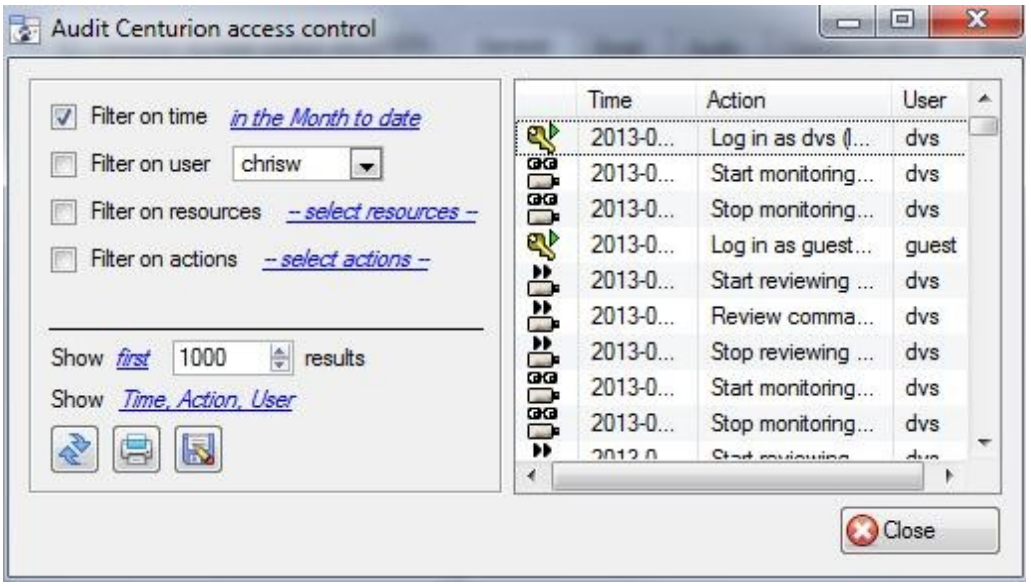
Note: One may only replace units that have been detached, or that cannot be reached on the network due to a hardware failure.

Right-Click on a Unit

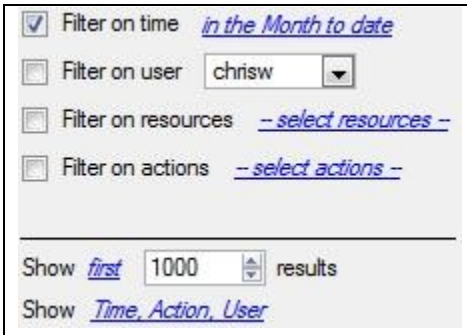
Right-clicking on a unit allows one to perform a number of vital actions.

	**New Server** is dealt with in Add a Unit (1.a) above. **Licensing** is how an individual recording server is licensed, and is dealt with in the installation section of the manual. **Audit Server** allows one to audit the specific unit. Auditing is explained below. It is also dealt within the GUI Document. **Fetch Sherlocks** allows one to fetch the Sherlocks for this device. See below.

- ***Audit Server***



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. The filters are **Time, Users, Resources, and Actions.** The **Show first/last** option limits how many of the results are brought up. The **Show time/action/user** option allows one to add/remove columns to the audit report, and lists the selected variables.

- ***Print, Save, Refresh***

	The report is not live, so to update the information, click on Refresh.
	To print the Report for reference, click on the printer icon.
	For a digital copy of the Report, click on the disk icon.

- ***Sherlocks***

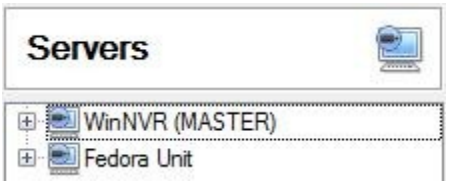
Sherlock files are a diagnostic tool used by the Support Desk. The normal procedure is to email the Sherlock file to the Support Desk (support@cat.co.za), with a description of the problem, but there is also the option to save it to disk.

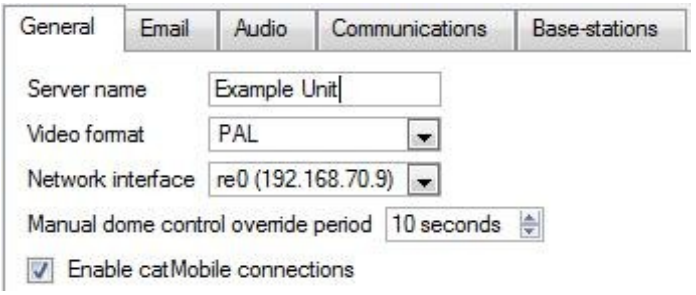
To get the Sherlock files, right-click on that unit, then left-click on Fetch Sherlocks, this will generate the Sherlock pack. Then either **Save them to** disk or **Email** the Sherlocks.

Save to disk... Email...	**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 the workstation.

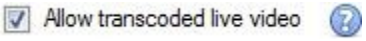
b. General Tab

When clicking on the actual server name (not the ⊞ used to expand the options), the right-hand panel will fill with the General Setup options for that server.



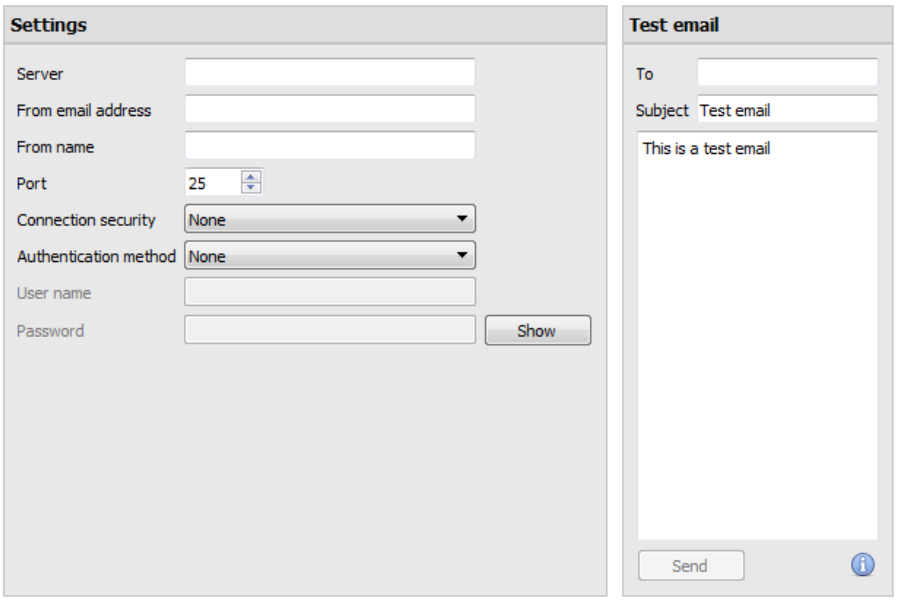


Server Name	The descriptive name given to the individual unit. That identifies the unit in the GUI.
Video Format	Choose between PAL and NTSC. **Note**: It is not advisable to mix formats across units on the same Site.
Network Interface	Will list the Network Interfaces on this unit, and their current IP Addresses.
Manual Dome Control Override Period	The period of time the controller must be inactive on a particular PTZ camera before it resumes its automatic responses. (E.g. 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**: The mobile connections are made on a unit-by-unit basis, with no Site knowledge. This means each unit needs to be enabled for it to be available via our mobile interface.



This is currently only available on Windows units. It uses software encoding to add another, lower quality MPEG, stream to send to the cameras tab. This is useful for remote viewing, but will put extra strain on the processor of the unit.

c. Email Tab



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

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

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

- ***Test Settings***

Opposite **Settings** is the **Test Email** box, from which one can send a test email to another email account, just as one would from a normal email client.

Note: Before attempting to send a test email, remember to click 

.

d. 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**

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.

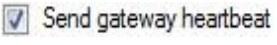
e. Communications Tab

A Heartbeat is a signal sent from the capture unit (recording server) to an Alarm Management Gateway unit, which 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 setup on both the capture station and the Alarm Management Gateway.

- ***Enable Heartbeat***

To enable sending the heartbeat on the unit: check the 

tick box.

- ***Select a Base-Station***

The base station referred to here is the Alarm Management Gateway unit the heartbeat message will be sent to.

- ***Select an interval for the Heartbeat***

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

f. Gateway Tab

This section deals with the Alarm Gateway, as such this option will only be visible if the selected server is setup as a gateway.

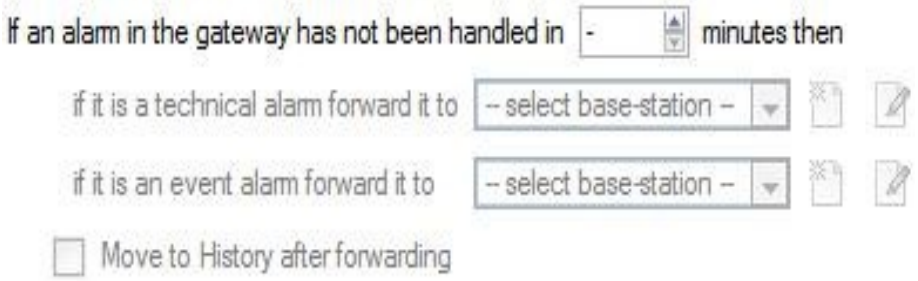
- ***Send heartbeat monitoring alarms***

If a heartbeat alarm is triggered, the gateway needs to take an action (send an alarm).

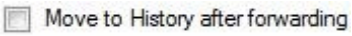
In general, this alarm should go to the gateway itself. So simply select the gateway from the dropdown menu. For the heartbeat alarms to go to some other unit, select/add that unit.

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

- ***If an alarm is not handled***

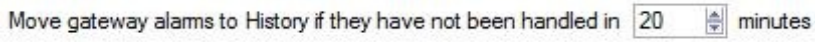
<table>
<tr>
<td> 
</td>
<td>If they have not been handled for a while, one may want to send unhandled alarms to other gateways, or base stations.

Decide on the time frame, as well as where specific types of alarms are sent.</td>
</tr>
</table>

Note: If 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 

box, which will move the alarm to the history queue of the forwarding unit.

- ***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, one may have them automatically moved to the history queue.

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

- ***Configure Backup***

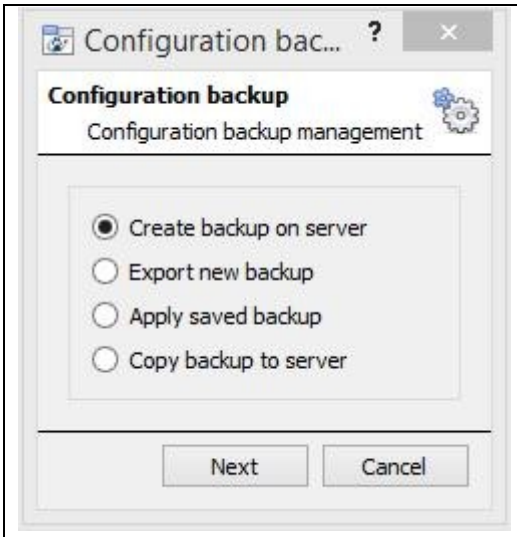
Note: One may choose to back-up all units to a central location, such as a network drive.

- ***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), and clicking on 

.

- ***Manage configuration backups***



Clicking on Manage configuration backups... will open the dialogue to the left.

Create backup on server will create a backup on the server, in the default path that was set above.

Export a new backup allows one to choose the destination of the new backup.

Apply saved backup (formerly *restore existing backup*) will allow one to apply a saved backup.

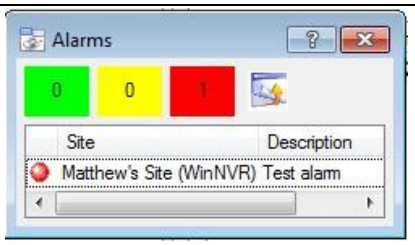
Copy backup to server allows the user to create a restore point backup of the system's current state. So, this can be done straight after making new changes to the system.

h. Base-stations Tab

The Base-stations set here 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 an alarm is sent to an Alarm Management Gateway, it will appear in the alarm queue; if an alarm is sent to an individual Viewing Station it will appear as a pop-up window.

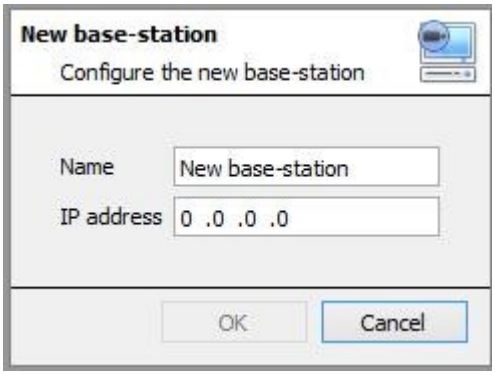
The window to the right is an example of such an alarm, on a Viewing Station.



- ***Add a New Base Station***

To add a New Base Station, click 

Name: Give the Base-station a descriptive name.
IP address: IP address of the specific Base-station.



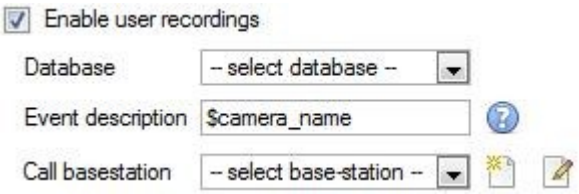
- ***Send Test Alarm***

Test Base Station settings by clicking on Send test alarm This will send a test alarm to the selected Base-station.

i. User Recordings Tab

The user recordings facility allows a user to manually trigger a recording if he/she sees something live in the Cameras Tab. This is useful as it may not be something that would have triggered a recording 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 into the Database.
Call basestation will send an alarm to a Base Station whenever a User Recording is triggered.



- ***Trigger a User Recording***

Start the Recording

Middle-click on a camera in the **Cameras Tab** and Start recording should appear as an option in the dropdown menu. Click this to start the recording. If the recording has started, there will be a flashing  in the top right-hand corner of the camera panel.

Stop the Recording

To stop the recording, middle-click on the camera panel and click on Stop recording , in the drop-down menu.

Note:

1. Only one camera may be triggered at a time.
2. It is advisable to create a separate database just for User Recordings.

2 Cameras

a. Introduction

There are two ways to add a camera in **CathexisVision**:

1. The camera Addition Wizard.
2. The Copy/Paste Function.

This section of the manual will detail these two addition methods, followed by an examination of the Camera Editing options, and some extra information on the right-click menu.

b. Camera Addition Wizard

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

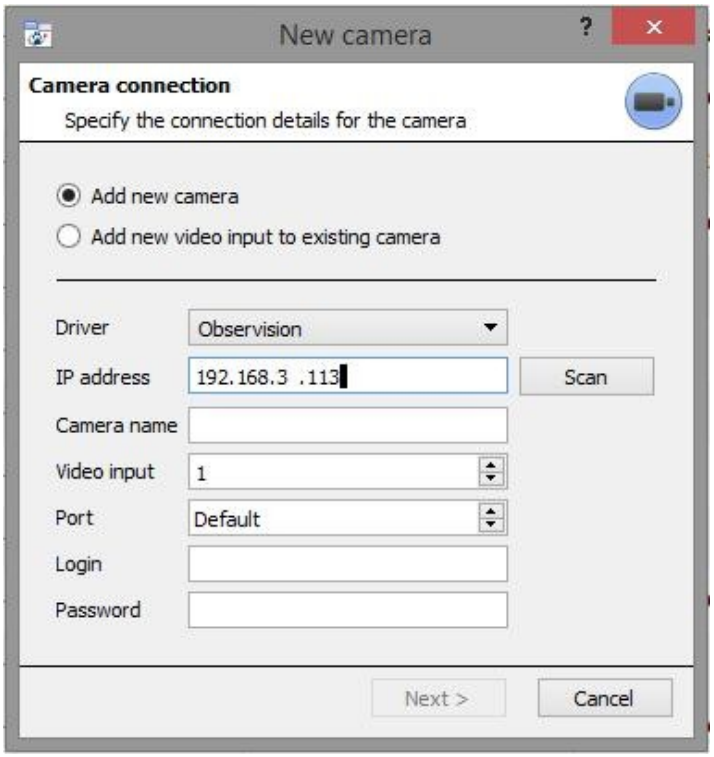
There are two phases in the addition Wizard:

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. The following explains each step in the Wizard.

- ***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 driver for the camera.

IP Address: Set the IP address of the Camera being added.

Scan will scan the network for cameras that have been setup to make themselves available. Click on a camera and it will automatically have its driver and IP address set. (Under there is the option to list cameras that are already linked to other servers. To do this: check the Show devices used by servers box.) **Camera name** is a descriptive name given to the camera.

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

Port will have a default setting, but to connect through a specific port, set it to the port of choice.

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

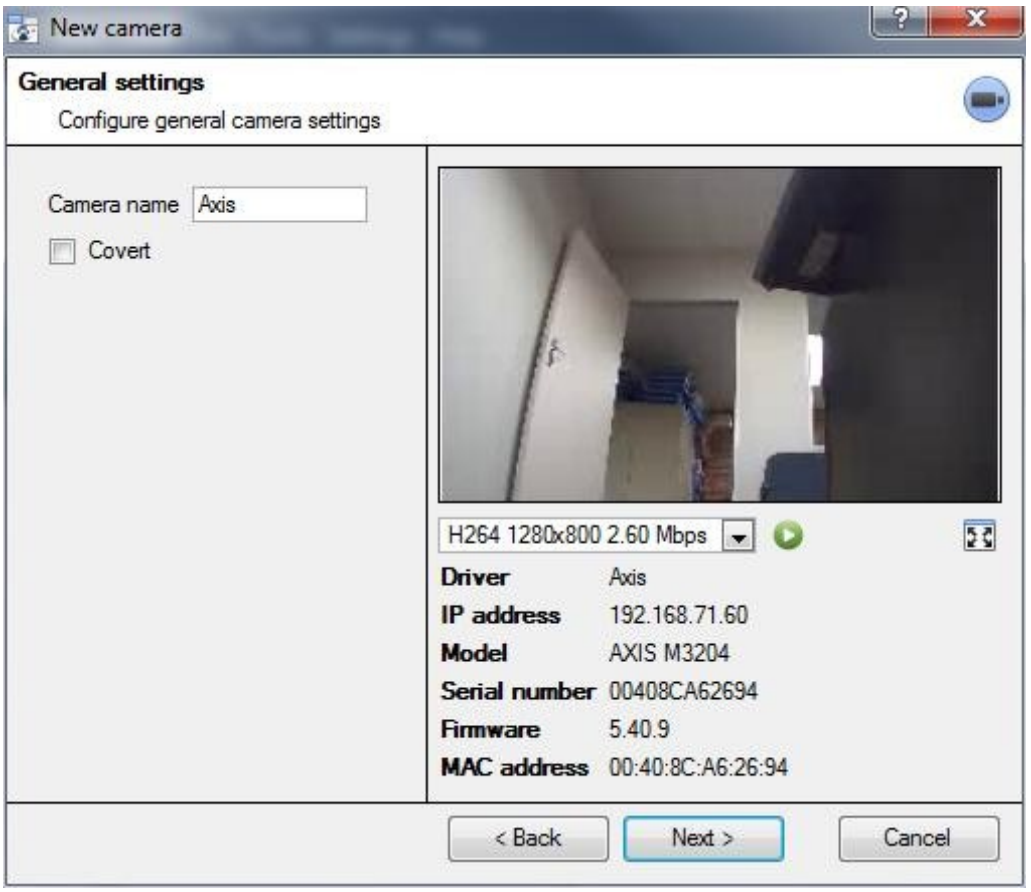
Notes on adding a new video input:

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.

General Settings



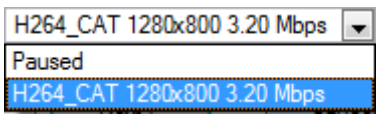
Name Give the camera a descriptive name. So as to make it easily identifiable in a list.

Covert **CathexisVision** provides 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	**Access Level Defined**
Camera will only be present in the Resources List of an Administrator, or an access level that has been granted access to this camera	Camera will still appear in the Resources List of lower login levels, but they 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. View it underneath the image preview.

Live Preview



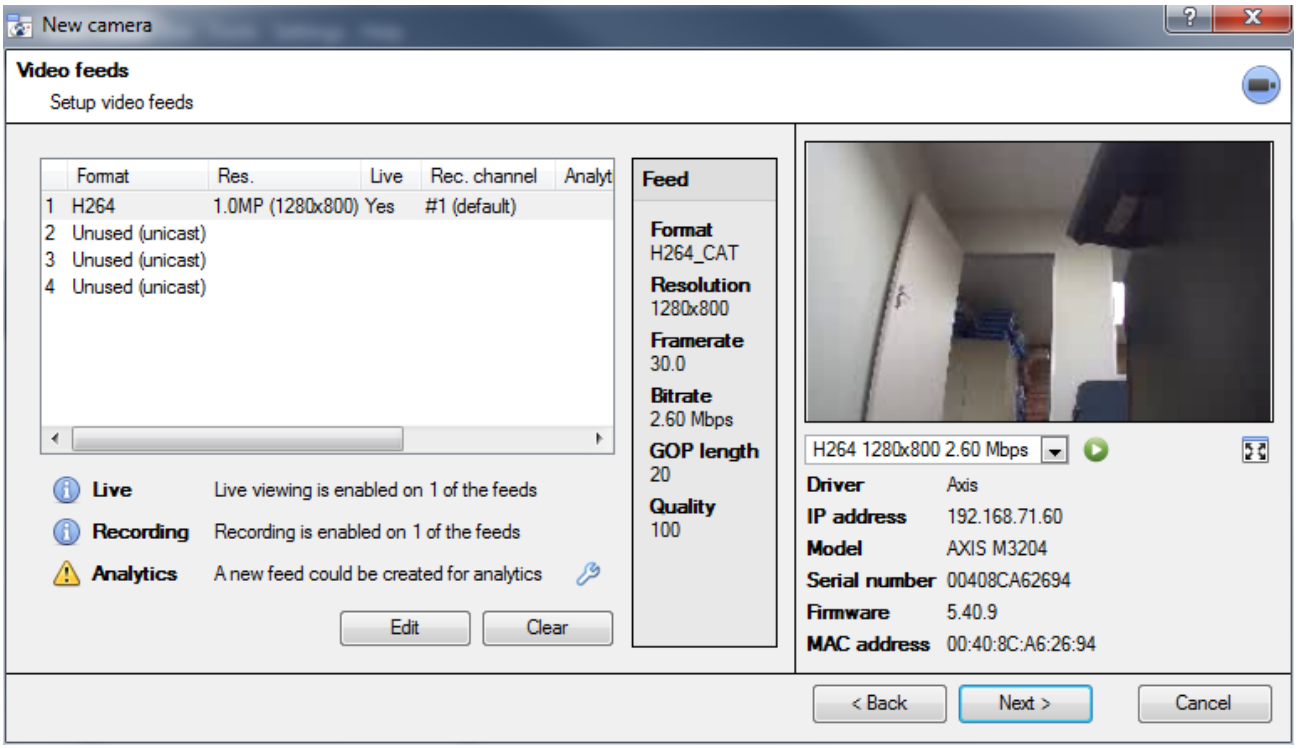
The image seen is a frame grab from the video feed chosen

To play the live preview click on:

To enlarge the image, click on:

Note: The image in the preview will not reflect the actual quality of the feed, as it is transcoded when viewed in the camera addition wizard.

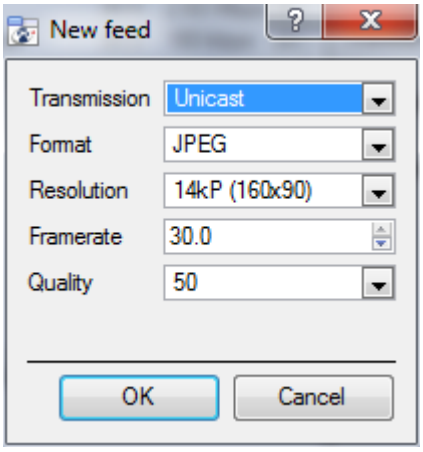
- ***Video Feeds***



- ***Add/Edit a Video Feed***

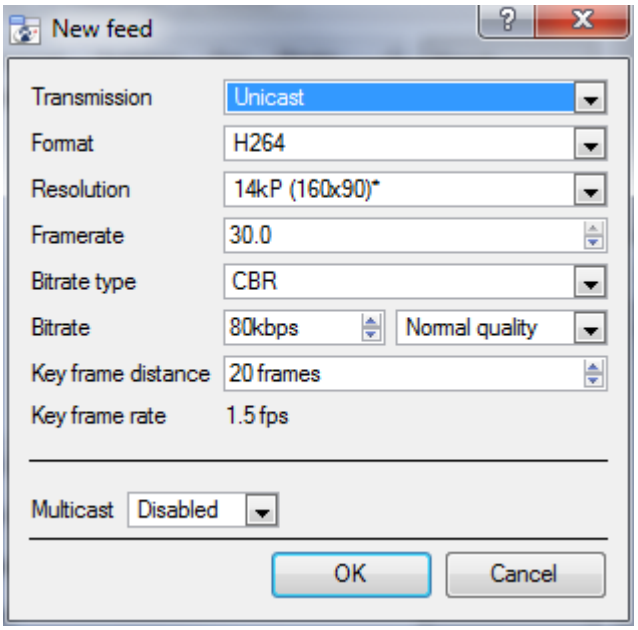
To add/edit a video feed click on one of the available feeds in the list, and click on the **Edit** button. This will bring up a feed dialogue with the available video feeds, and the options that pertain to them. The two most common IP feeds are JPEG and H.264 (MPEG4).

JPEG



Transmission will show the transmission type.
Format is the compression format used by this stream. Click the dropdown 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



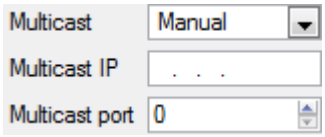
Transmission will show the transmission type.
Format is the compression format used by this stream. Click the dropdown menu to choose the one desired.
Resolution is the number of pixels in the image.
Framerate is the number of frames recorded per second
Bitrate Type this is the way that the bitrate is handled. A constant bitrate will be more predictable, but will lose more information the more the image changes. Variable bit-rate is less predictable, but will have better images when the picture has more motion.
Bitrate is 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) is the number of frames between each I-Frame (Key Frame).

Multicast

Setup Multicast on feeds by selecting the relevant option from the feed dialogue. There are three options; **disabled, auto,** and **manual**.

Note*:* Leave disabled if multicast is not desired.

Manual

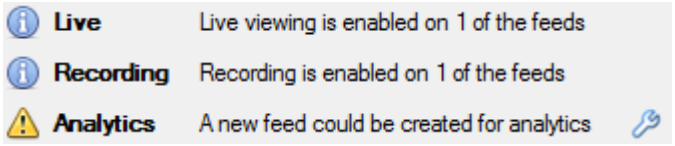


With manual selected, enter a specific Multicast IP, and Multicast Port.

Auto

On auto, the Multicast address will be automatically assigned. The core settings for this may be found in the document on the **General Site Setup** section of the **Setup Tab**.

- ***Feed Notifications***



This area will display the status of the feeds created: **Recording**, **Live Viewing**, or **Analytics**.

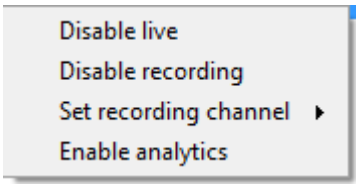
Note: Click on any of the icons to display detailed information about the feed/problem.

Automatic Configuration

If there is an icon at the end of the feed notification, this means that there is a potential problem with the feed setup. Clicking this will automatically fix the problem.

- ***Right-Click Menu (Live, Recording, and Recording Channel Settings)***

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



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

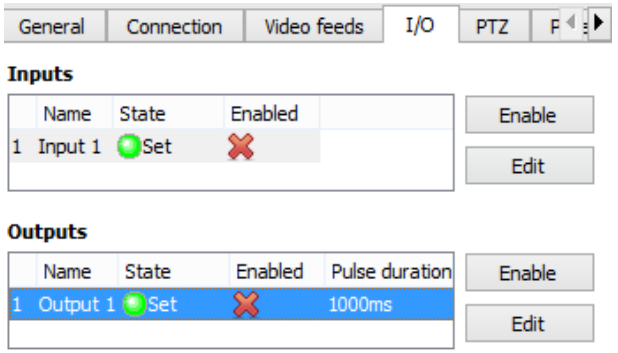
Analytics

In order to enable analytics on a unit, setup a second feed, right-click on that feed, and click **Enable Analytics**. There are a few rules when it comes to enabling analytics:

1. If an analytics-enabled channel is not setup here, there will not be a prompt to add Video Motion Detection (VMD) later in this wizard, nor can VMD be added, using this feed later.
2. Only feeds that are QVGA resolution, and lower, will provide the option to enable analytics.
3. If there is a at the end of the Analytics feed notification, there is no feed enabled for analytics. Clicking on the will automatically enable one.

- ***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.



I/O

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

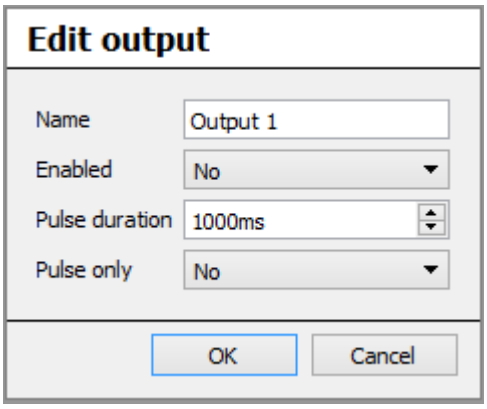
Renaming

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



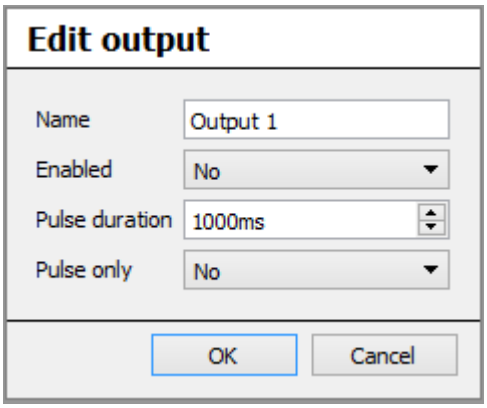
Name: Give the output a descriptive name.

Enabled: Will display 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.

Edit an Output



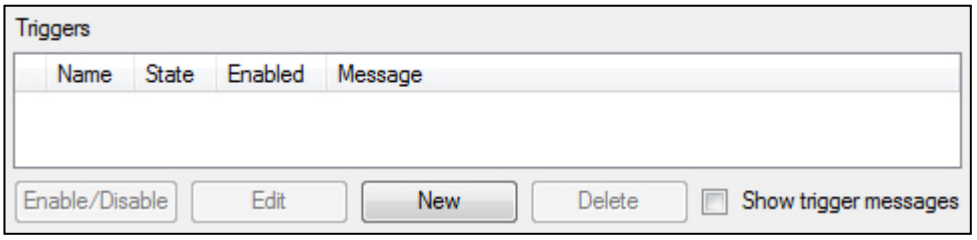
Name: Give *the* output a descriptive name.

Enabled: Will display 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

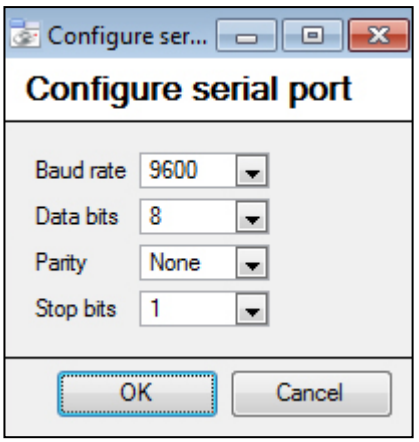


Certain cameras will have their own event triggers, and encoders will often have **I/O** options.

Note:

1. Clicking on any of the column values (**Clear**/**Set**; **Enabled**/**Disabled**) of an I/O will toggle the value. E.g. Clicking on a Clear state will change the state to Set. (These options are also 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 

button.

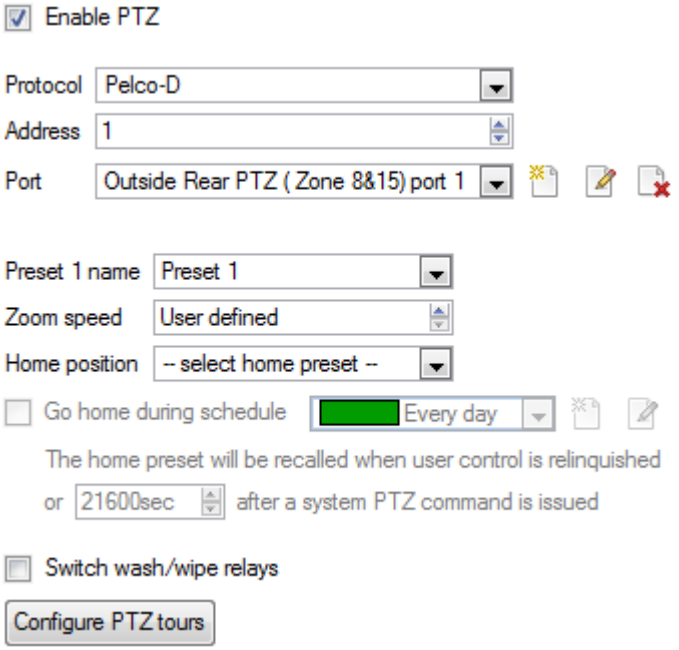
This will present the option to change the **Baud rate**, **Data bits**, **Parity,** and **Stop bits**, and other camera dependent settings.

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

- ***PTZ***

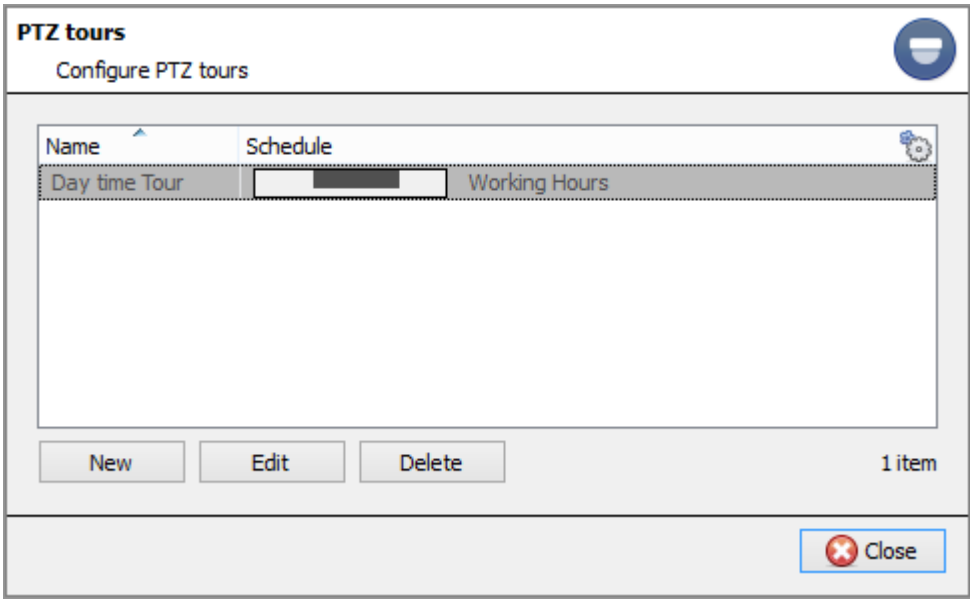
Check the Enable PTZ box if adding a PTZ camera. After this, all the available PTZ options will appear in the Wizard interface:

- General Settings



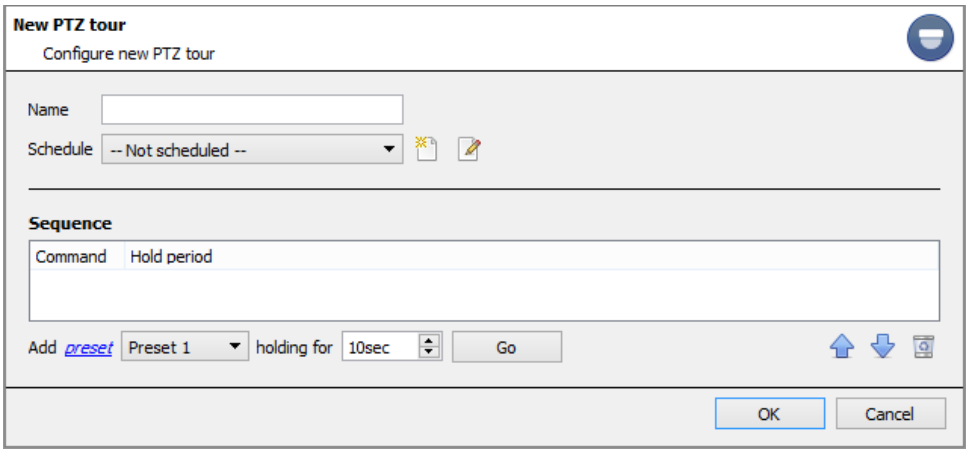
Note: These options can vary on a camera-by-camera basis.

Preset Name	One may 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 on 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 to after a set period of inactivity.
Automatic Return to Home	One may set a **schedule** during which the camera will return to its home position. When the schedule (see: 5. Schedules) is inactive, the camera will remain in the last position that it was left in. If there is no schedule set, the camera will never return automatically to its home position. To have it always return home after a 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.)



One may configure multiple tours. To add/edit a tour click on **New/Edit**.

This will open up the PTZ tour configuration dialogue below.



Give the tour a descriptive name, and, if desired, a schedule (see: 5 Schedules)

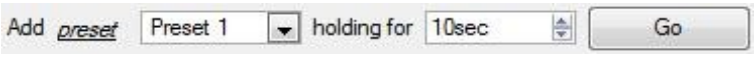
Sequence

This is the sequence that the Presets will run in.

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

Preset

Select the preset, set how long the camera should linger at this preset.



Multiple Presets

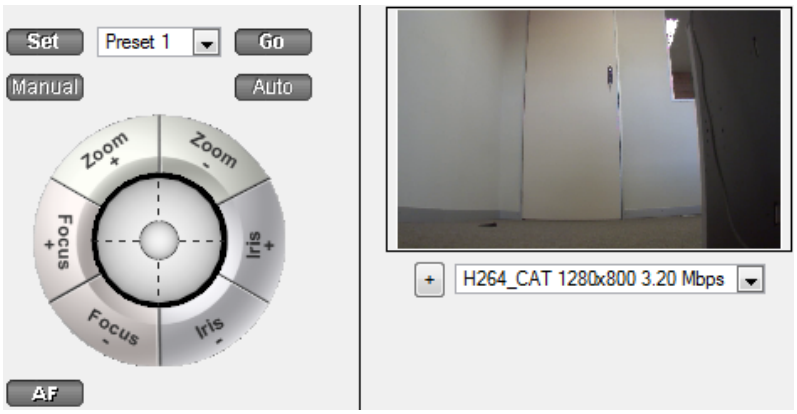
- **Starting at**: Select the first preset to add.
- **Add**: This is the number of presets to add.

In the example below, one adds presets 4 to 6.

Pattern

Select the pattern to add.

- **PTZ Procedures**



Note: Don't forget to select/play a live feed.

With a Pan-Tilt-Zoom (PTZ) camera, an operator can manipulate the camera's direction, Zoom, focal distance (Focus) and amount of light (Iris). He / she 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 dropdown menu and select **PTZ** (see below). The software joystick displays:

Using the PTZ Control Panel

To pan left / right from the PTZ panel  Drag joystick left / right To move the camera faster from the PTZ panel.  Distance determines speed - drag joystick out, in required direction. To zoom in / out from the PTZ panel, watch the live camera while pressing the Zoom + and Zoom – button. To go to a preset from the PTZ panel, select the preset from the dropdown, and then click GO > The camera view will change to the preset. To relinquish manual control of the dome / PTZ camera from the PTZ panel Click Auto. > If the system runs remote tours automatically, or switches display based on events, these automated responses will take over. To allow more or less light in the image (lighten and darken the live camera view) from the PTZ panel, watch the live camera through pressing the iris+, or iris – button. The image will lighten or darken.	To tilt up / down from the PTZ panel,  drag joystick up / down. To move the camera slower from the PTZ panel:  distance determines speed - drag joystick closer in, in required direction. To focus further / closer from the PTZ panel, watch the live camera through pressing the Focus + and Focus – button. To gain manual control of the dome / PTZ camera from the PTZ panel (this applies if the system runs remote tours automatically, or switches display based on events), either click **manual**, or simply move the software joystick Define a Preset (To set a preset from the PTZ panel) 1. Select the preset number, from the dropdown 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 which 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 and 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.

- Database

All cameras need to record to a database. If a database is not yet created, the user will be directed to the database setup, after the PTZ setup. If a database is already created, one can proceed straight to the **Scheduled Recordings/Video Motion Detection setup** and use the current database.

Create a new database for this camera by checking the 

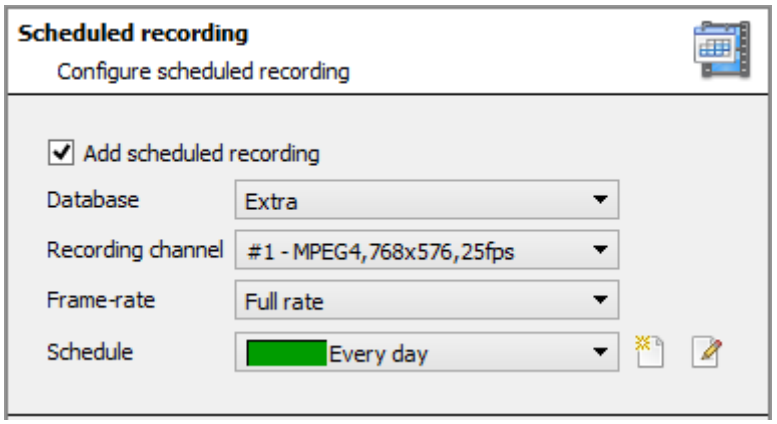
option in the bottom left-hand corner of the screen.

Note: this will setup the database on the recording server that the camera is added to, and not the unit being worked on (if using a client, or other remote unit). This means there will be no file system knowledge of the remote unit, and the path must be entered manually. (There will not be the 

option on a remote unit.)

For further information on setting up a database, please consult the  section, below.

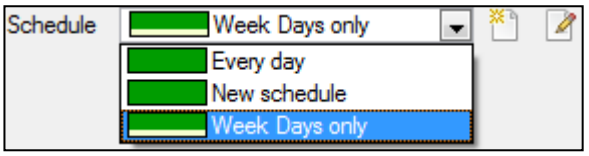
- Schedule



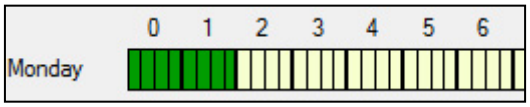
Schedule recording
Set the camera to only record at certain times, to increase efficiency and save disk space.

Select the **database**, **channel,** and **frame-rate** to apply a schedule to.

- Set Up a Schedule



Select the schedule from the drop-down menu. Create a new schedule by clicking on the  icon. To change an existing schedule, click on the  button.

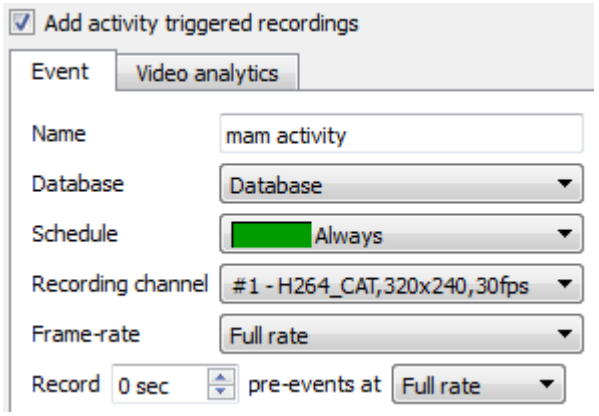


Select/Deselect time cells
Left-click to **select recording time** – the green bars.
Right-click to **unselect recording time** – the yellow bars.
Monday will be recording from 00:00 – 02:00 in the morning.

- Activity Recording (VMD Event).

Note: This does a number of things. This will add Video Motion Detection, pre-event recordings, and add an Event to the system.

- Recording



The recording option allows one to setup the recording settings.

Database is the database this event will record to.

Schedule defines when this event will be active.

Recording channel defines which video channel will be recorded.

Frame rate defines the frame-rate that recordings will take place in.

Pre-events define a time that will be buffered, and recorded, from before the initial trigger.

- Activity

The default algorithm here is the **Basic Video Motion detection**.

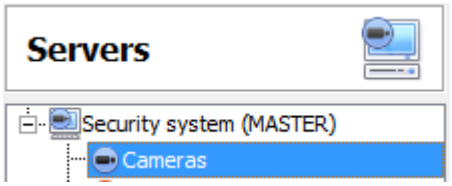
The settings for Video Motion Detection are too detailed to go into under this section, for a full description see the Video analytics section of this document.

c. 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**.

- Copy/Paste a camera

If adding more than one camera that operates on the same driver, **CathexisVision** offers a very easy solution. The user may copy and paste new cameras, retaining the information of the camera selected for copying.



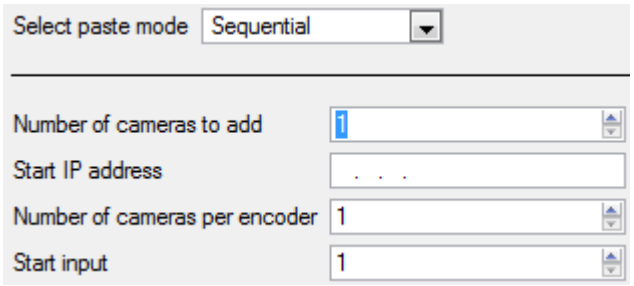
To Copy/Paste new cameras, first ensure that one is in the cameras panel of the desired unit, right-click on the previously added camera and click on Copy.

Then right-click anywhere in the Cameras Panel and click on Paste new... .

There are two ways to past cameras **Sequential**, and **Discovered**. These will be discussed, below.

- Paste Mode: Sequential

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

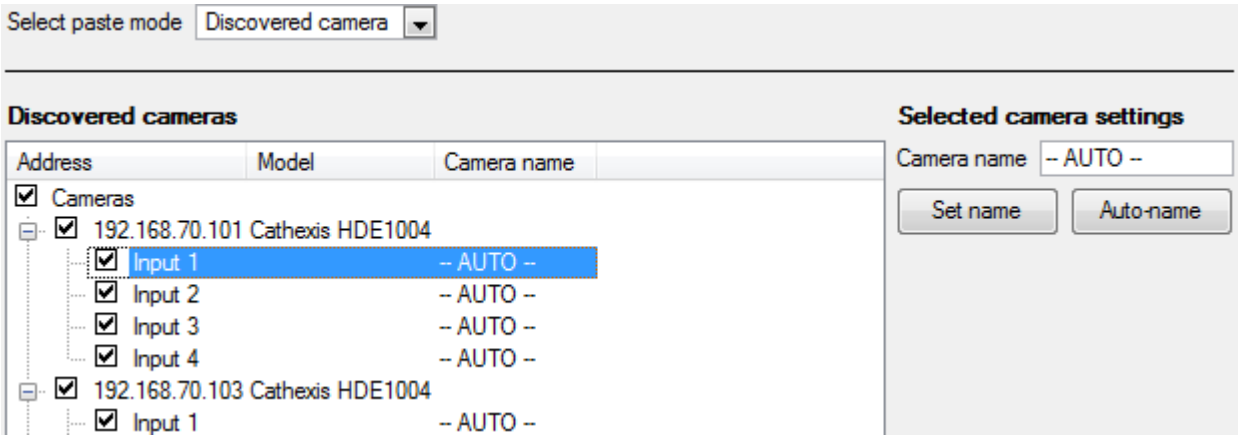


Start IP Address will determine the IP address of the first new camera being added. The IP addresses will be incremented from here. (So, make sure IP addresses in this range have not been used.)

Number of cameras per encoder must be the full number of channels available on this encoder

Start Input is the actual physical channel to add the first camera to.

- Paste Mode: Discovered



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

- Copy/Paste Video Settings

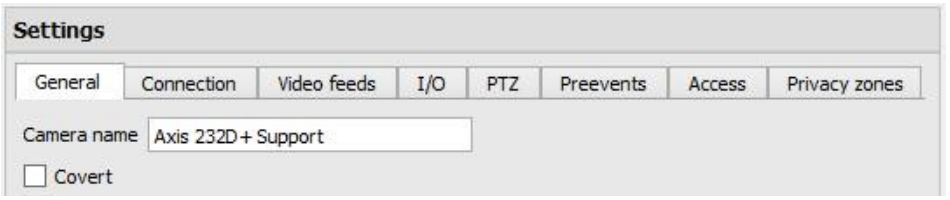
If a number of cameras with the same drivers are already added and one simply wishes to transfer the Video Settings of each camera across, then right-click and select Copy. Then right-click on the camera to add the video settings to and select Paste video settings.

Note:

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

a. Edit Existing Camera

Note: If any changes are made 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 are saved.



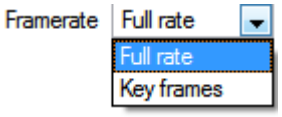
Edit an already added camera by selecting it and clicking on Edit.

- ***Repeated vs Additional Options***

The camera setup options of *General*, *Connection*, *Video Feeds*, *I/O*, and *PTZ* are all dealt with verbatim, in section b. Camera Addition Wizard (above), they will not be repeated here. Three options are added in the Editing Tabs: **Pre-events, Privacy Zones,** and **Access Levels**. These options will be dealt with here.

Note:
In the Wizard, the user may have gone through 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.)

- Pre-events tab



Pre-events were setup under the Activity Recording Section of the Wizard. One cannot define the number of pre-events here, but the frame rate of the pre-events in this tab may be defined.

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

- Access tab

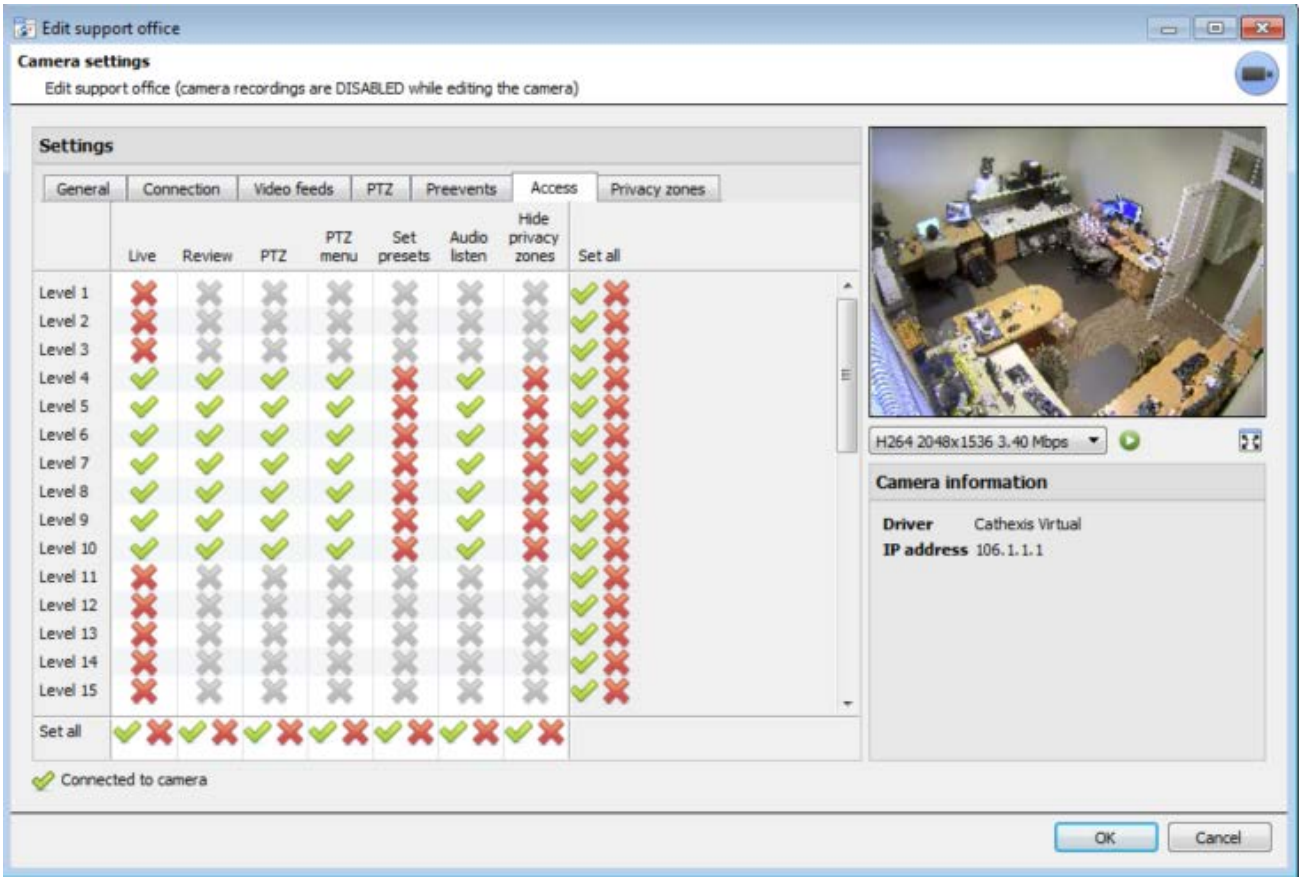
Under the **Access tab,** one can setup which user levels have control of the different facets of the camera.

From within the **Cameras** section under **Your_Server_Name**, select the camera, click 

and select the **Access** tab.

From within the **Cameras** section under **Your_Server_Name**, select the camera, click 

and select the **Access** tab.



A  means that this level has access; a  means that this right 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 instance, 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. Thus, the administrator should be careful to enable the **Live Viewing** access right for the user levels which will need to view and manage the video stream.

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 form 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 will give this level access to all settings; selecting will give this level access to none.

In the above example, user levels 1, 2, and 3 have been denied access to **Live** view of the streams, and are consequently denied the other access rights. However, users 4-10 have been given access to **Live** viewing of the stream, and thus have been granted access to **Review** viewing of the stream, control of the **PTZ** camera movements and **Audio Listen**, but have been denied the ability to **Set Presets** and **Hide privacy zones**.

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.	Independent audio channels.
Reviewing from the camera tab.	Archived video.
Reviewing from the database tab (both video and integration databases).	Connecting to a 2016.2 server using a 2015/2016.1 viewer.
Viewing video when handling an alarm in the Alarm Management Gateway.	Connecting to a 2016.1 server using a 2016.2 viewer.

Note:

1. **Users** can be added and managed in **Setup** tab → **Configure Users** .
2. **Access Rights** may also be configured by following **Setup** tab → **Configure servers** → Access rights .

- Privacy Zones tab

Adding a **Privacy zone** will hide an area(s) of the camera image. The **Privacy zones** can be hidden/shown by an administrator or user levels which have been assigned the access right to do so – this is covered in the previous section and in section **11 Access Rights.** As such, the **CathexisVision** system will record the footage behind the privacy zone, but only users with access rights will be able to view it.

This is a useful feature, 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.

Adding Privacy Zones:

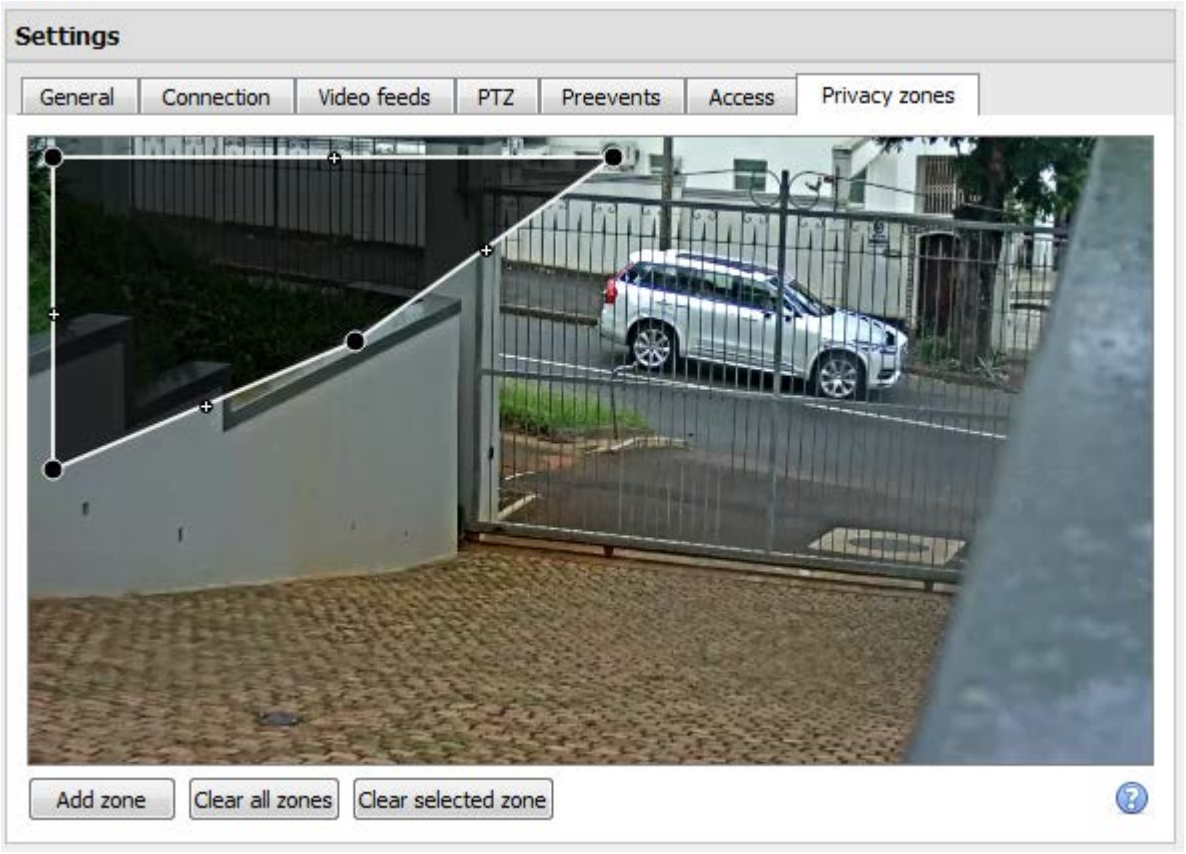
Adding/editing **Privacy zones** is not a part of the camera addition Wizard, and can only be completed by editing a camera after it has been added.

1. **Setup tab → Configure Servers** → expand options under **Your_Site_Name** → Cameras

2. The list of Site cameras will be presented, for which one can add/edit privacy zones individually. Select the relevant camera, clicking Edit at the bottom of the screen.

3. Click on the **Privacy zones** tab.

4. Click Add zone and a black box will appear on the image; add as many **Privacy zones** as desired by clicking on the same button.



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.

When finished, click OK to save.

Hiding/Showing Privacy Zones in the Camera Tab:

Privacy zones will be shown by default, with the option to hide them in the **context menu** of the camera in the **Cameras Tab**. Users with **Access rights** may hide/show **Privacy zones** in both **Live** and **Review** mode, and from within the **Video** and **Integration Database Reviews**.

Middle-click on the camera image to open the **Context Menu**. If the user has the access rights, the option to hide or show privacy zones will be presented.

If hidden, the black shapes will be removed to reveal the underlying images.

NOTE:

1. One **cannot hide/show privacy zones in archived footage**: Privacy zones will be hidden/shown depending on whether the privacy zones are hidden/shown during archiving.
2. Privacy zones will be **hidden/shown in a printed/saved snapshot** depending on whether they are hidden/shown when the snapshot is taken.
3. **Privacy zones are stationary**: Only areas of the camera image can be hidden and objects which move out of the privacy zones will be seen.
4. When **privacy zones** are added to a panamorphic camera the CathexisVision image transformations are disabled.

b. Analogue Cameras

This section will deal with the details that are specific to the Analogue Capture Cards. **Cathexis** provides two analogue-to-digital capture cards that work on its **non-Windows systems**.

Analogue cards offer 6 editable options:

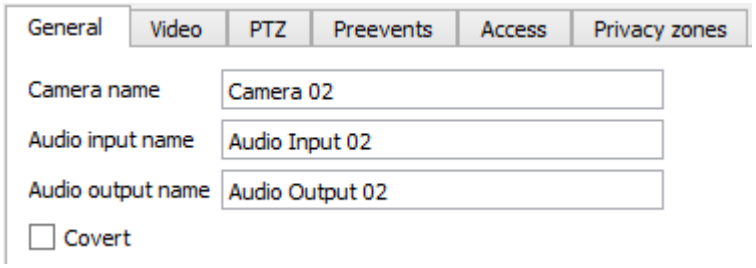
1. General settings
2. Video settings
3. PTZ settings
4. Access settings
5. Pre-events
6. Privacy zones

Aside from the video settings, and the settings under General, all of these settings are identical to the settings encountered in the IP setups above. This section will deal with those aspects of camera setup not dealt with above.

AVM Capture Card

AVM cards convert the analogue input into H.264 video. They also have the ability to synchronise audio, via on-board audio inputs.

- General



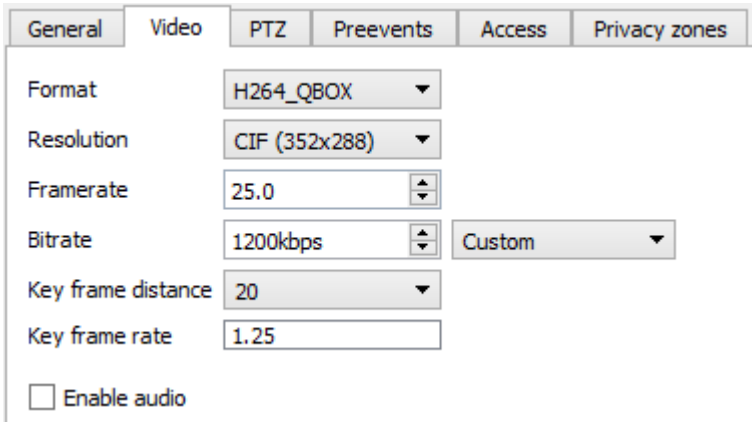
Camera name is a descriptive name given to the camera.

Audio Input Name is the audio input associated with this camera.

Audio Output Name is the name of the audio output associated with this camera.

Covert cameras will only be visible to administrators, and those people whose user accounts have a relevant access level.

- Video



Format is the compression format used by this stream.

Resolution is the quantity of pixels in the image.

Framerate is the number of frames recorded per second.

Bitrate is 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 is the number of frames between each I-Frame (Key Frame).

Key frame rate is the rate of key frames, per second.

Enable Audio will enable recording synchronised audio, using the audio channel on the AVM card.

- **PTZ**

See the **Error! Reference source not found.** section in under Wizard Addition, **Error! Reference source not found.**.

- **Access**

See the Access section, under Editing of an Added Camera, above.

- **Pre-events**

This will determine the frame-rate that pre-events will be recorded at. (These pre-events are added in the events setup.)

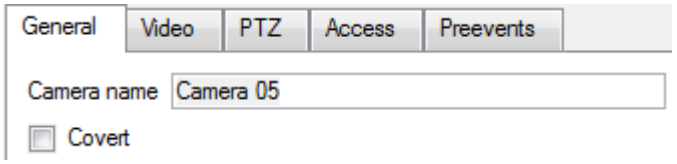
- **Privacy Zones**

See the Privacy Zone section, above.

VOM 1400/1500/1512 Capture Card

VOM capture cards convert the analogue video input to either MJPEG video, or MPEG-4 video. They have the ability to record synchronised audio, but only when using an MPEG-4 profile.

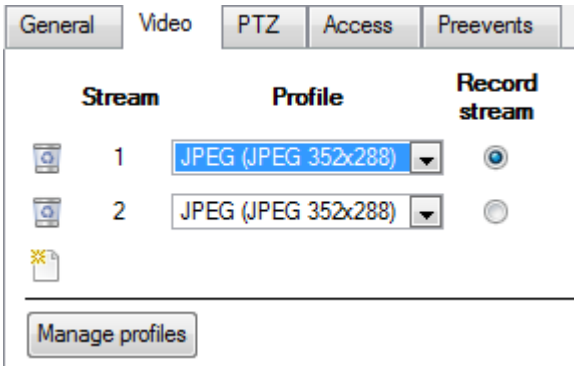
- General



Give the camera a descriptive **name**.

Covert cameras will only be visible to, administrators, and those people whose user accounts have a relevant access level.

- Video



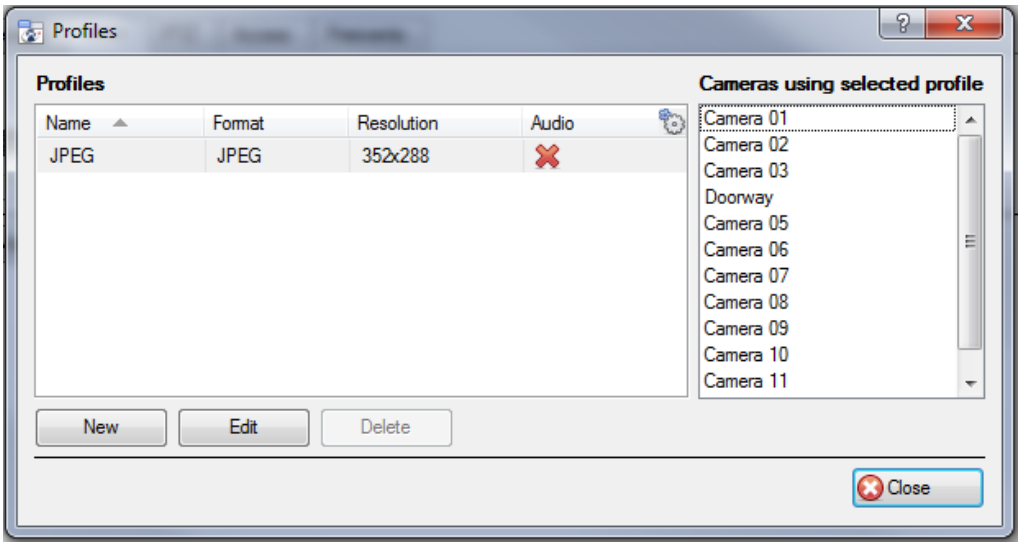
There may be a maximum of 4 streams on any VOM camera.

Stream The stream numbers are for the specific camera being configured.

Profile is a drop-down menu. Choose from any of the configured profiles. These are user configured stream profiles. (See Manage Profiles, below.)

Record Stream checked, indicates that the stream is recordable.

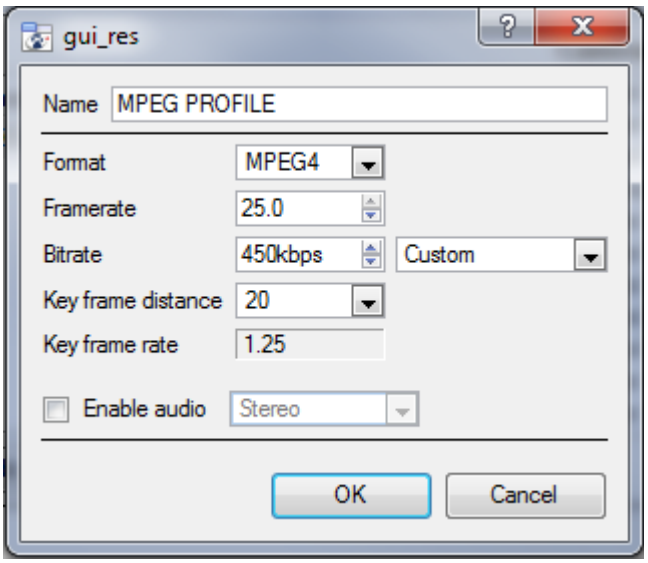
1. Manage profiles



Clicking the "Manage profiles" button presents the **Profiles** dialogue box, which provides information about the currently existing profiles.

The "**Cameras using selected profile"** lists all cameras currently using the selected profile.

- MPEG4



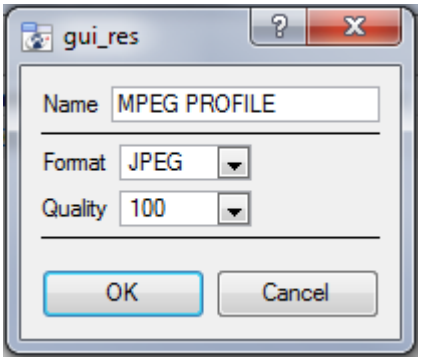
Profiles can be created/edited to use either MPEG4 or JPEG format. The image to the left is the MPEG4 creation dialogue.

Enable Audio allows synchronisation of audio on any camera attached to the VOM card. This audio will be synced with the audio input on the motherboard of the DVR.

Note:

- Only use one physical input on the motherboard at a time. When there are mic and line options available: only use the mic input **OR** the line input. The mic and line inputs **cannot** be used simultaneously.

- JPEG

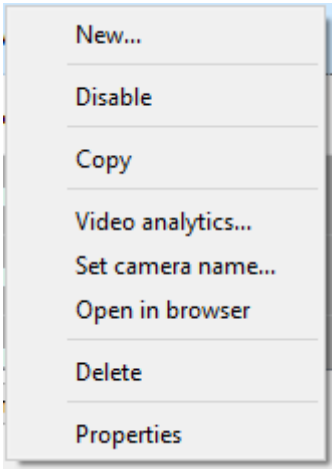


Profiles can be created/edited to use either MPEG4 or JPEG format. The image to the left is the JPEG creation dialogue.

The JPEG setup is very simple, simply choose the **format** (JPEG), and set the quality desired.

The **quality** number is a representation of the image quality. (E.g. 100 is the highest, and will give the best image quality.)

c. Right-click on a Camera

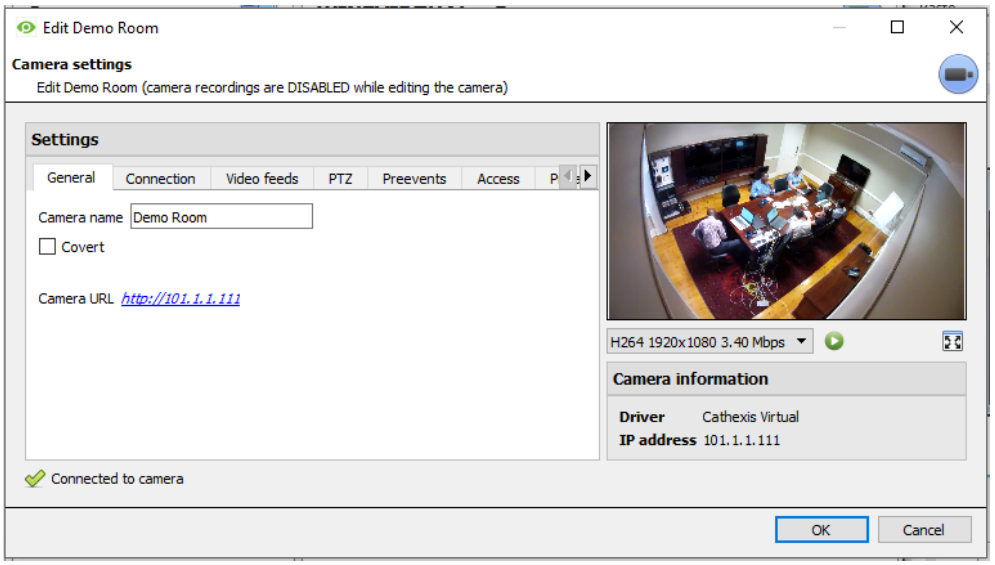


New…	Add a new camera.
Disable	Disables the current camera (but does not delete it).
Copy	Copies camera settings and enables them to be pasted onto a new camera or existing camera.
Video analytics…	Opens Edit Video Analytics window.
Set camera name	Edit the camera name without having to open the edit 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 above, under Copy Paste Cameras.

Camera Properties

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



Here, 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.

3 Video Analytics

This is a guide to the Video Motion Detection setup process. In order to give a deeper understanding of the algorithm, and facilitate informed setup decisions, the individual parameters which are available to the user will be dealt with in detail here.

It is important to remember that the setup process will be iterative, and require 'tweaking' in order to get right. This is because VMD algorithms do not work in the same way as the human eye/brain combination. Rather they observe changes in light intensity at the level of the individual pixel and use this to set off triggers. As a result, any changes in the image, such as clouds rushing over a field, or a flashing light, can cause a false trigger. These need to be adjusted on a case by case basis. In other words, there is no one-size-fits-all solution to video analytics setups.

Note:

I. Algorithm names have changed in CathexisVision 2017.2:
   a. Analytics I → Basic Analytics
   b. Analytics II → Intermediate Analytics
   c. Analytics III → Advanced Analytics

II. Advanced Analytics will contain the Basic and Intermediate Analytics. So, if a camera is licensed with Analytics III, the user need not add licenses for I and II, as they will already be included.

III. The new **CathexisVision** video analytics algorithms, which were added in **CathexisVision** 2015, (licensed using Analytics I, II and III) are only available on Linux and Windows NVRs.

IV. Units running CathexisVision 2016 cannot connect forwards to units running CathexisVision 2017.2. Should this be attempted, a message will appear to update the GUI interface.

V. When connecting from a 2017.2 unit backwards to a 2016 unit, the Top down head tracker algorithm (in the Analytics type analytics) and the Top down head counter (std) algorithm (in the Counting type analytics) will not be available as these two algorithms are not available in CathexisVision 2016.

a. Basic Video Analytics Options

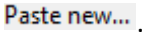
Copy/Paste an Algorithm

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

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 overwrite and click Paste.

Copy Algorithm settings as a new algorithm

Here, copy the algorithm settings onto a camera by right-clicking and copying the existing algorithm. Then right-click anywhere and select 

. This will bring up a list of cameras that are attached to this unit (e.g. 

).

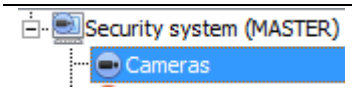
Select any number of cameras to paste the algorithm onto, and click OK.

b. Adding Analytics

Access Algorithm Settings/Setup

There are two ways to access the Algorithms, from within **Setup Tab → Configure Servers**.

- ***Option 1: Via the Cameras Panel***



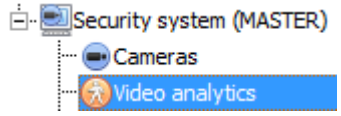
Access the Algorithms associated with a particular camera by clicking on that camera, and then clicking on the Video analytics button on the bottom of the tab. (One may also right-click a camera and select Video analytics...).

This will bring up a dialogue box with a list of algorithms associated with this camera. In the box, select algorithms to edit them, or create new algorithms.

In the window that opens, click New to add an algorithm.

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

- ***Option 2: Via the Video analytics Panel***



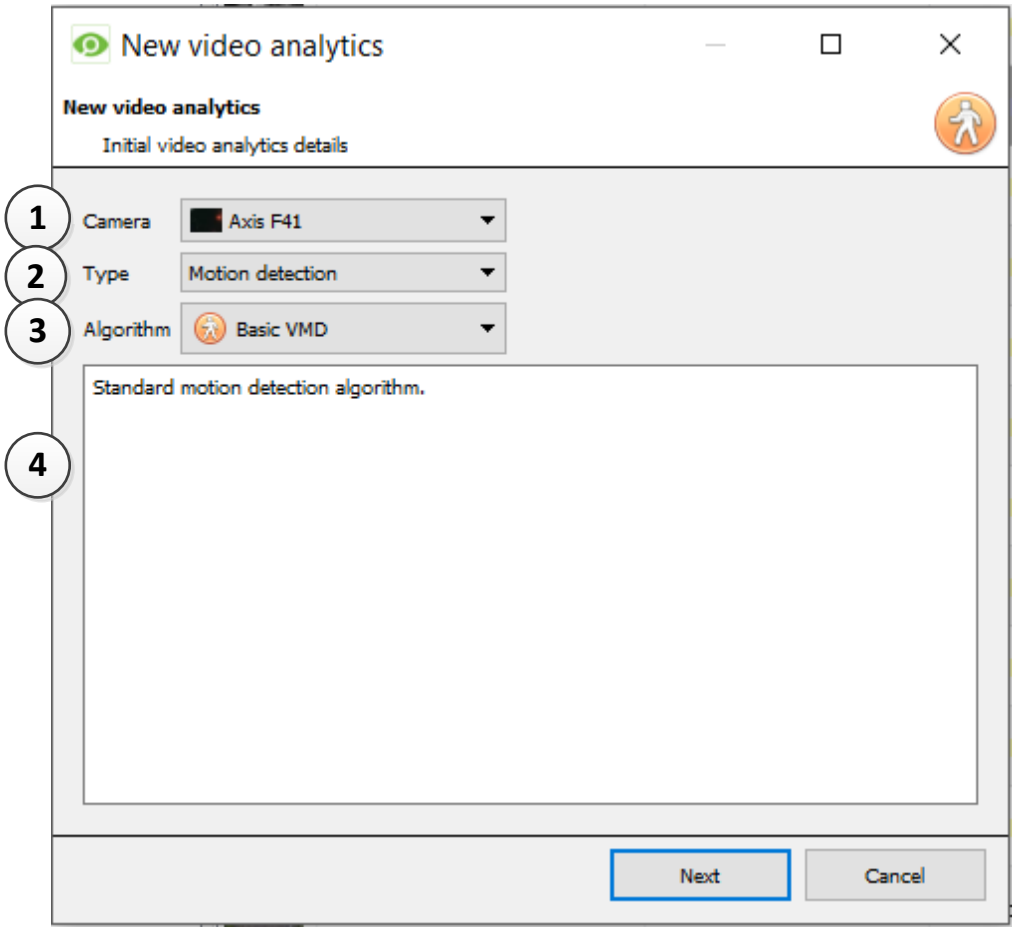
This will list all Algorithms that are related to cameras on this Server.

In this window, click New to add an algorithm.

Both options will open the same window where one chooses the type of algorithm to add.

New Video Analytics Window

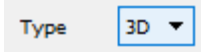
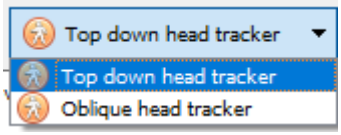
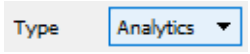
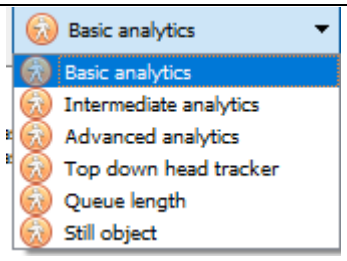
See the table below for an explanation of the New video analytics window.



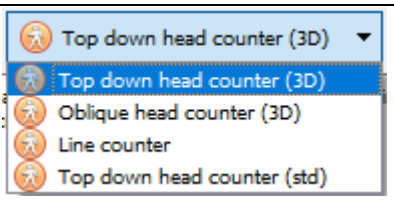
Area	Description
1	Select the **Camera** that video analytics are being added to.
2	Select the broader video analytics **Type**. Type options will differ according to which analytics level has been applied.
3	Within the video analytics type, select the specific **Algorithm** to apply algorithm types.
4	A basic description of the features of the algorithm is provided in the **description field**.

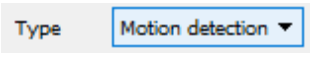
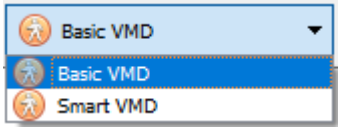
- ***Select the Algorithm***

See the table below for an explanation of the Analytics Types and Algorithm options.

Analytics Type	Algorithm Options	Description
 Note: This option only available if camera is 3D.		Top down head tracker: Offers event triggering when: - heads cross a line using a 3D camera looking straight down. Oblique head tracker: Offers event triggering when: - heads cross a line using a 3D camera mounted at an angle.
		Basic analytics: Offers event triggering using: - basic line crossing triggers and - basic presence triggers.
		Intermediate analytics: Offers event triggering using: - advanced line crossing triggers and - advanced presence triggers.
		Advanced analytics: Offer event triggering using: - advanced line crossing triggers, - advanced presence triggers, - speed detection, and - size and direction filters.
		Top down head tracker: Offers event triggering when: - heads cross a line using a standard colour camera looking straight down.
		Queue length: Offer event triggering when: - a queue exceeds a certain length.
		Still object: Offers event triggering when: - An object has been left for a period of time.
		Top down head counter (3D): - Count heads crossing a line using a 3D camera looking straight down.

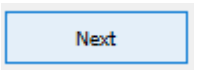
<table>
<tr>
<td rowspan="3">Note:

None of the algorithms within this analytics type can trigger events. See each algorithm type with the correct alternative to trigger events.</td>
<td rowspan="3"> 
</td>
<td>Note: This option does not trigger events, it only counts heads. To trigger events with head counts, use the Top down head tracker algorithm under the 3D analytics type, above.</td>
</tr>
<tr>
<td>Oblique head counter (3D):
- Count heads crossing a line using a 3D camera mounted at an angle.
Note: To trigger events with oblique view head counts, use the Oblique head tracker algorithm under the 3D analytics type, above.</td>
</tr>
<tr>
<td>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, above.

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, above.</td>
</tr>
<tr>
<td> 
</td>
<td> 
</td>
<td>Basic VMD:
- Standard motion detection algorithm.

Smart VMD:
- Advanced motion detection algorithm designed for outdoor scenes.
- Can filter out repetitive motion like tress or grass moving.</td>
</tr>
</table>

- ***Configure the Analytics***

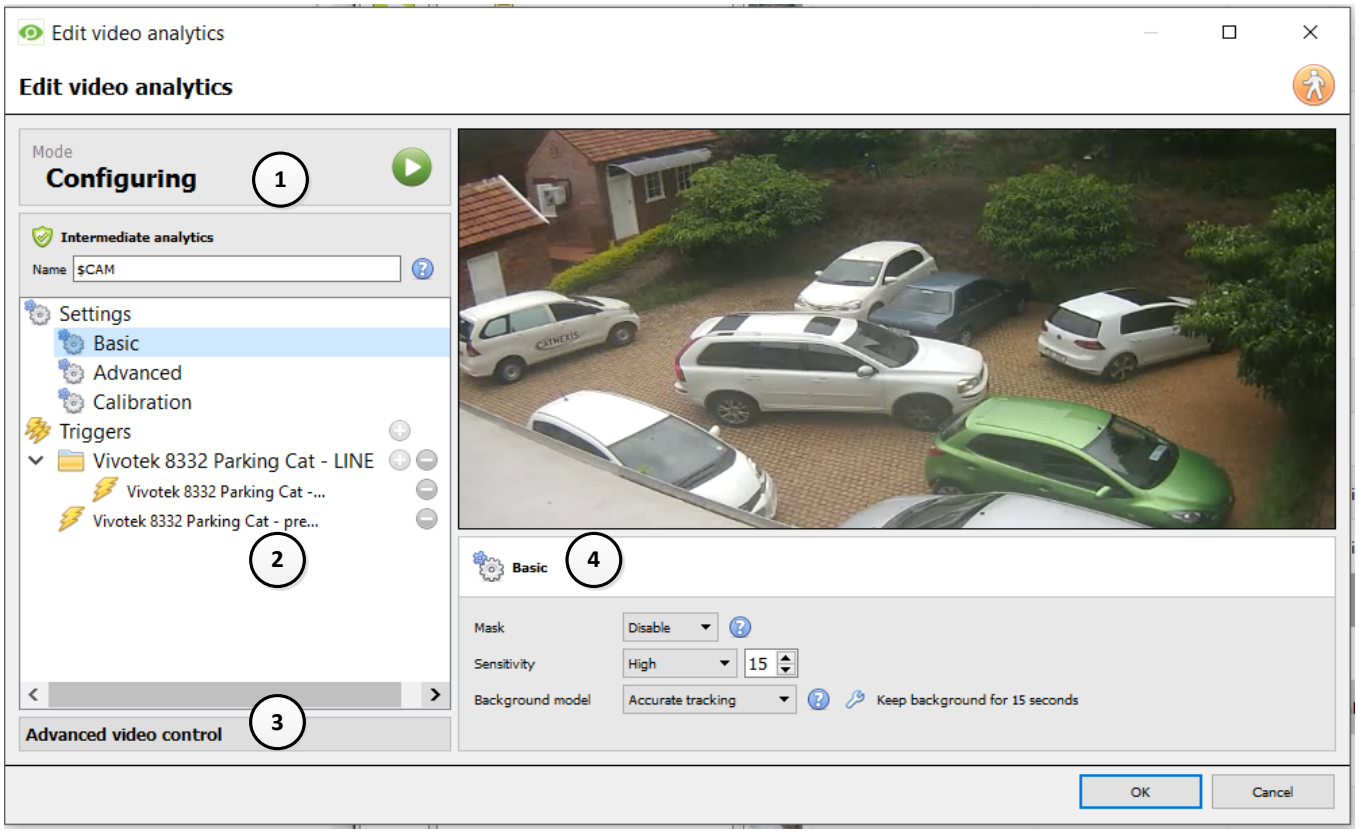
Once the analytics type is chosen, click 

to move onto configuring the analytics. See **Section b.** below.

c. Video Analytics Interface

Video analytics can be edited by clicking **Setup Tab → Configure servers → Video Analytics Panel → Video analytics tab → select camera/algorithm →Edit.** There are two modes/interfaces in the setup of the Analytics; **Configuration**, and **Running**. These will be explained below, before the specifics of each Algorithm are discussed.

Configuration Interface



1	The current mode of the interface is indicated in the header. In the top right of this panel, there will be the  icon. Click this to switch to the Running interface.
2	This area will be called the **configuration panel**. At the top of the panel will be the name of the algorithm and its current licensing state (relative to the camera it has been assigned to). It will also list the **name** of the algorithm. The "$CAM" at the beginning of the algorithm name will place the name of the camera it has been assigned to at the beginning of its name. This is useful

because to export and import algorithm names that immediately assume the name of the camera that it has been imported into.

The Settings area will list the settings that exist for this algorithm. The different algorithm sets will present with different sets of settings options. While Analytics I, II, and III share the same settings options, the rest all have their own set of settings.

Triggers is where the user adds the actual analytics triggers for the selected algorithm, after choosing which algorithm being used. To add a new trigger, click on the icon, to remove a trigger click on the icon. (Triggers may be used to trigger events. For more information see the Events Setup section.)

3

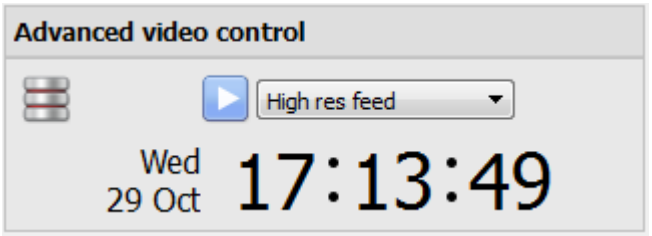
The Advanced Video Controls are available in both the Configuring and Running interfaces. By default, it will be minimised.

To expand this player, hover the mouse over the text of this section. The text will turn blue, and an icon will appear to the right of the text. Click on this to expand it.

There are two ways of viewing video with this tool. Either live, or recorded video.

Live Video:

The default (in the above image) is live.

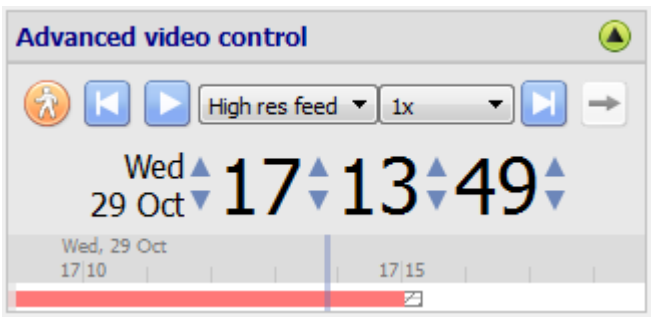


will start streaming live video from the camera in the Camera panel.

There is the option of viewing the high-resolution feed, or the one used for video analytics.

Recorded Video:

Clicking on the (database) icon will direct one to the recorded video for this camera.



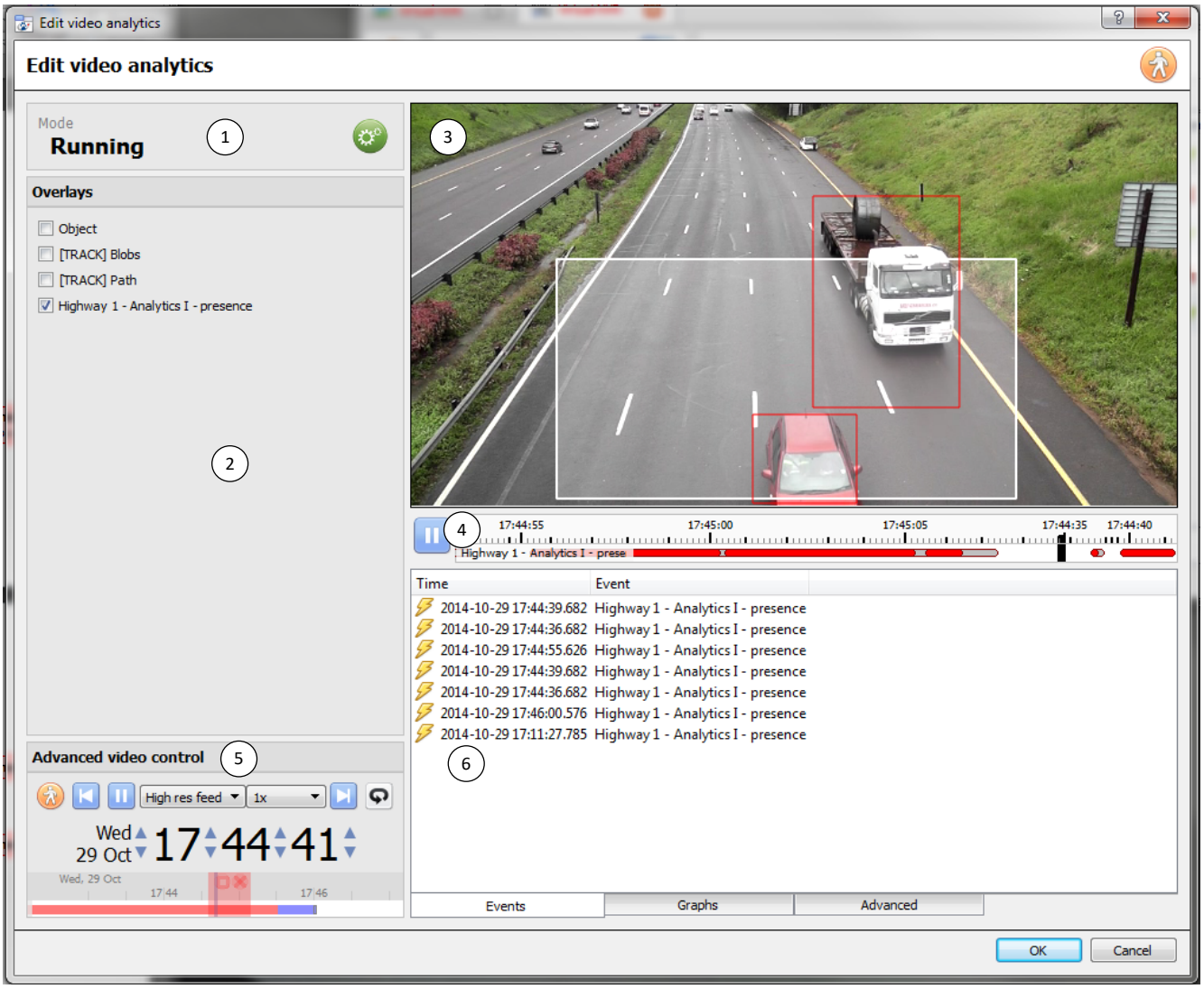
Use the wheel arrows on the timestamp to change the date of the footage being viewed.

Or left-click and drag on the timeline at the bottom of the player.

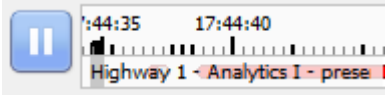
Clicking will return to the live player.

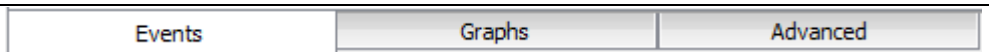
	Looping video selections is a useful ability of this player, especially when testing algorithm settings; it enables the user to objectively see if a setting changes the efficacy of the algorithm. This is achieved by holding down shift while left-clicking-dragging out a selection on the timeline. Once this portion of the timeline has been selected, click on  , it will turn into an  icon. It will now loop over the selected section of video, instead of playing continuously. **Note**: This selection will transfer across from the Configuration to Running interfaces, and vice versa.
(4)	The **Context Area** will display the contextual information/options for whatever has been selected in the Configuration Panel.

Running Interface



The running interface is used to test the settings already defined, in the Configuration interface. It will allow one to see the algorithm, as it has been programmed, in action. Either using live video, or a selection of recorded video.

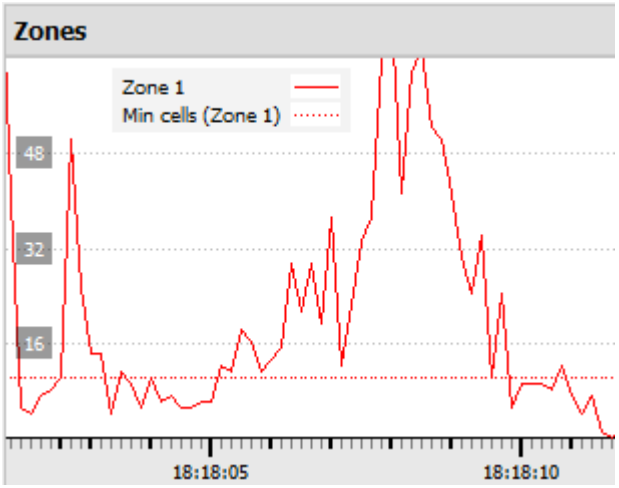
①	The current mode of the interface is indicated in the header. The  icon will be In the top right of this panel. Click this to switch back to the configuration interface.
②	In the **Overlays** panel are displayed the overlays contextually relevant to the algorithm configured. To select an overlay, check the  box next to its name.
③	The footage panel will display the footage selected to view, showing the overlays which were selected in the Overlays panel.
④	 The timeline is a display of 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, clicking on the timeline will allow recent frames and overlays to be viewed.
⑤	The **Advanced Video controls** are identical to those in the Configuration section, which was detailed above.
⑥	The **Feedback Panel** will show a live progression of the triggers, as they appear. There are three ways to view the events as they roll in. This is shown in the tabs at the bottom of the events panel:



Events

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. (i.e. goes from white to red.)

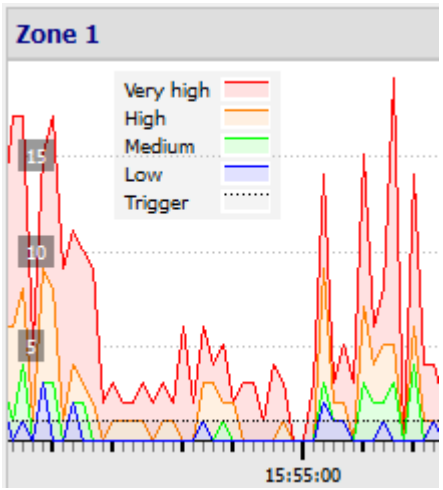
Graphs



The **graphs** option will graph the event activity occurring in the image.

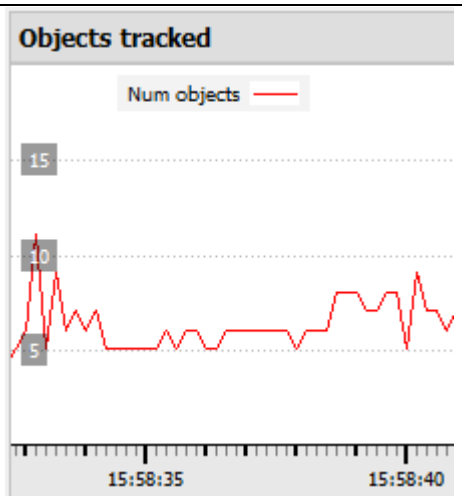
For instance, when using **Basic VMD** one may graph the zones in the algorithm. This is useful for displaying a visual representation of how far the triggers are above/below the Min cells trigger line.

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

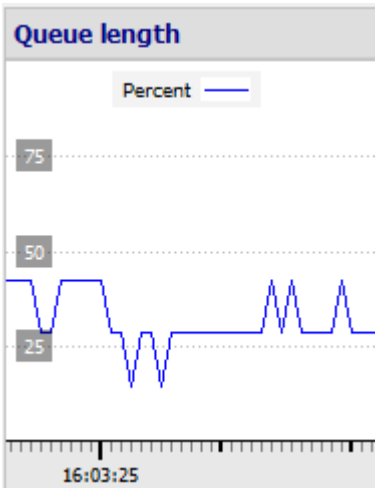


The **Smart VMD** graph will show the different triggers levels that would occur based on different profiles.

This can be seen against the dotted line of the actual event trigger. One can 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 will simply graph the number of objects currently being tracked.

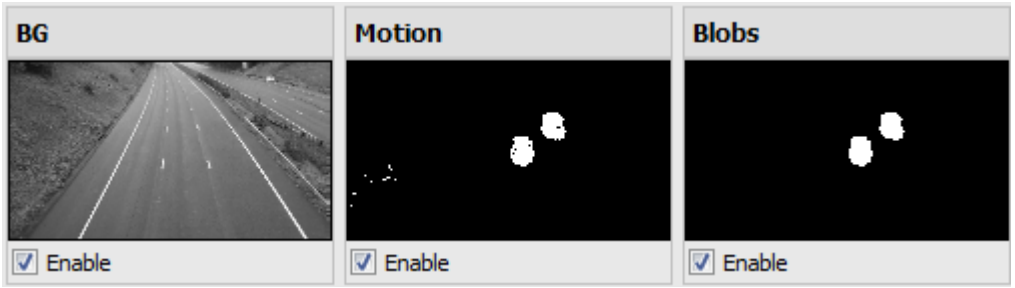


The Queue length graph in the **Basic Queue Length** algorithm is useful as it displays the percentage of the queue's current length over time.

Use this to help determine at what percentage 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 will show the user what the algorithm is seeing.

BG	This is the background image that the algorithm is working with. This is used to determine the changes that signify movement.
Motion	This will show the user all motion occurring in the video.
Blobs	This will highlight all motion that has been determined significant by the algorithm.

d. Analytics Setups

Now that the basic interface has been covered, it's necessary to look at the setup options that are available under the different algorithms.

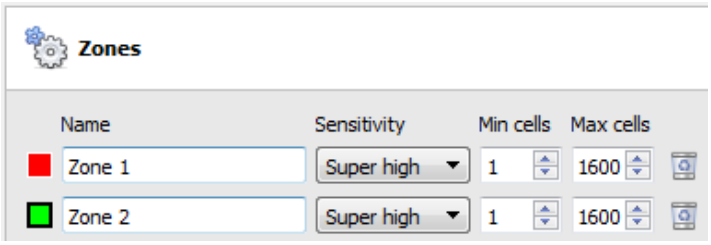
Basic VMD

Basic VMD is designed to trigger when there is motion in an area. It works by breaking the image up into small cells (the size of a single cell can be seen by drawing a mask with the brush set to the smallest size). If there is motion in a certain percentage of the cell, it is considered to have triggered. The percentage is controlled by the **sensitivity** - a high sensitivity will require a lower percentage of the cell to trigger, compared with a lower sensitivity.

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 a number of options available for modelling how the background image is created:
Historical, Travelling average, Accurate, and **Long term** (these will be dealt with in more detail, below).

If any background model changes are made it is recommended that the "Advanced" tab in the Feedback panel be used to understand how the background tracks the foreground.

- Zones

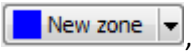


In the configuration panel of the "Edit video analytics" window, Zones can be found under the Settings option. Selecting this provides the information shown in the image to the left, within the Context Area. The user may create multiple zones, each with their own sensitivity, and min/max cell settings.

Min cells is the smallest number of VMD cells needed to have changed for the algorithm to trigger.

A good example of why zones are necessary is a border 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. This means that being able to set up different zones with increasing/decreasing sensitivity is very valuable.
In this same example, being able to set up both a minimum cell value, and a maximum cell value, for triggers is also invaluable.

Drawing Zones

To **create a new zone,** click on 

, 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.

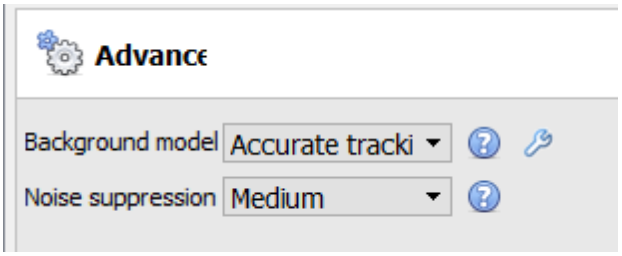
 Will scrub the zone from the image.

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

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

- Advanced

Background Model



In the configuration panel of the “Edit video analytics” window, Advanced can be found under the Settings option. Selecting this provides the information shown in the image to the left, within the Context Area.

Accurate tracking (default). This operates much like the traveling average method except that if there is a big change in an area it retains the original background until such time as the foreground stabilises. How it does this can be controlled by clicking the wrench icon below. 'Background memory' sets how long it remembers the background, and '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 (e.g. controlled indoor environment). The frequency, and number of snapshots used, can be changed by clicking on the wrench below.

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

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

Click  to display information about the selected options.

Click  to configure Advanced Background Model settings.

Note: Adaptive noise suppression is configured in the Advanced Background Model Settings window. Information is provided below on adaptive noise suppression.

Noise Suppression:

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

Adaptive Noise Suppression

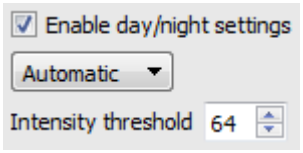
The *Adaptive noise suppression* is designed to help eliminate repetitive motion such as waving trees or the waves on water. To configure adaptive noise suppression, click the Advanced Background Model Settings icon  .

The adaptive noise suppression splits the image into noise zones and evaluates each noise zone individually. The image can be split it into 1, 2x2, 3x3,4x4, and 5x5 noise zones. Setting it to 5x5 zones will have the noise treated more independently throughout the image.

- Day/night

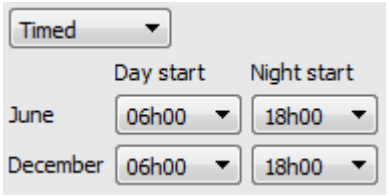
In the configuration panel of the "Edit video analytics" window, Day/Night can be found under the Settings option. Lighting conditions will obviously change depending on what time of day it is. These changes can be disruptive to the motion detection algorithms, which is why **CathexisVision** provides alternate settings for day and night. If day/night is enabled, then the settings can be set to different values for day and night.

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 of the settings as they switch from day to night mode.

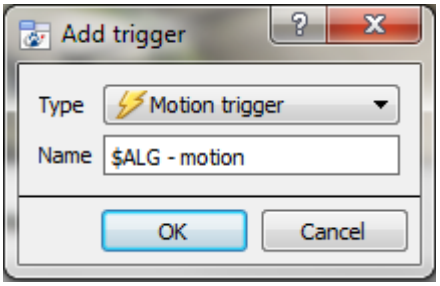
Timed



Timed Day/Night settings will be the easiest to set up.

There are two periods of the year to set.

- Triggers



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

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

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

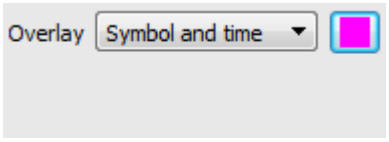
Unless the **Use advanced settings** option is checked, there will be nothing here.

Zone Settings

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

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

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 will appear, 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.

Smart VMD

Differences between Smart and Standard VMD.

Smart VMD is specifically designed to work in more dynamic environments than Standard VMD. It uses a number of methods to learn environmental noise patterns, and filter them, to avoid false alarms. The following guide will explain how Smart VMD does this, and in the process, how to set it up.

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

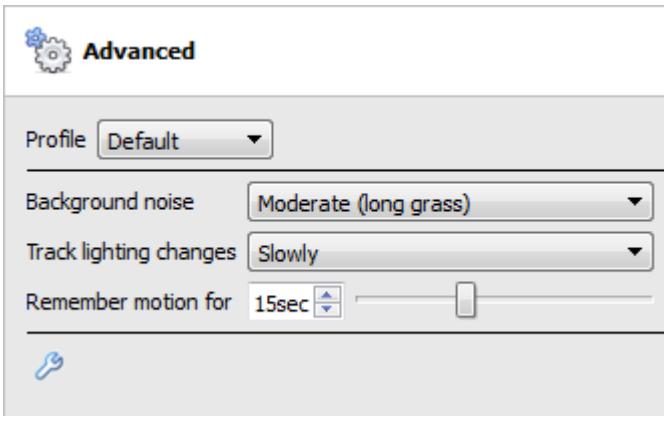
1. The way in which the background is learned. **Smart VMD** uses its own unique background model.

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 substantially better noise rejection characteristics.

- Zones

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

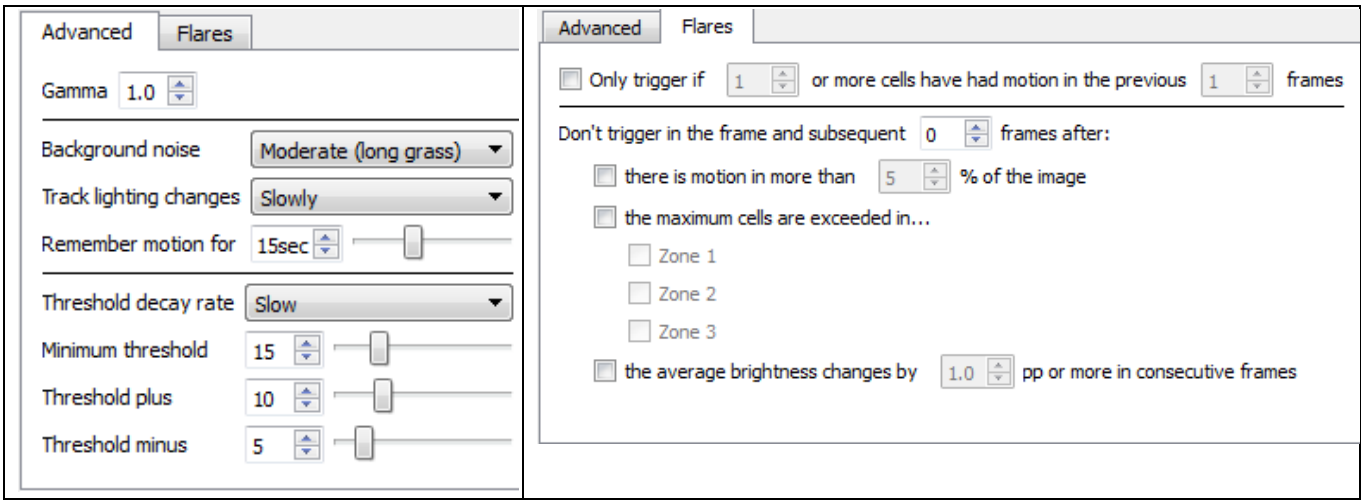
- Advanced



Profile	Find here a selection of pre-defined settings with descriptive names.
Tracking Light Changes	This configures how the background model responds to incremental changes in the lighting in the scene caused by things like clouds moving overhead. The faster the setting, the less sensitive the algorithm will become.
Background noise	This indicates how much background noise to expect in the scene (noise being defined as fluctuations in intensity caused by things like grass moving or possibly noise from the camera sensor). 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 retrigger until this period of time has passed. Setting this to a long time will reduce the overall sensitivity of the algorithm, but also allows it to more easily mask sounds like trees blowing in the wind.

- Advanced Settings Continued

Clicking on the will open the advanced options, of the Advanced Settings.



Gamma	Gamma is a brightening tool that works on a gradient. In other words, it brightens the dark parts the most, and the lightest parts the least. This causes an evenly brightened image with no overexposed areas, and no dark patches.
Threshold Decay Rate	This sets the speed at which the threshold drops back to ambient levels, or, to the Minimum Threshold setting.
Minimum Threshold	These advanced settings are only for use in conjunction with **CathexisVision** support. For more information contact support@cat.co.za.
Threshold Plus	
Threshold Minus	
Flares	The first option, **Only trigger if x or more…** is really a noise filter. It requires a set amount of motion in a set number of previous frames [minimum] to set off an alarm.

	Don't trigger… will prevent the flare frame, and frames immediately after from triggering an event. In the **Average Brightness** 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% max may seem small, but it is in fact a large average change for any image. 2 to 3% may be considered a substantial lighting change.

Comparison of default profiles

The table below is a comparison of the default profile settings.

	Standard	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

- Day/Night

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

Still Object

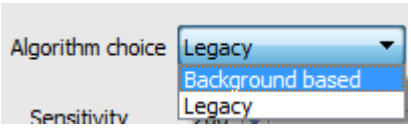
Still Object Detection is used to monitor introduced, or removed, stationary objects. This means that an object that was stationary in the image, such as a painting, will trigger the Still Object Detection (SOD) when removed. An object that is introduced into the camera view will also trigger the Still Object Detection, such as a car that parks in a handicapped parking zone. It can be used in any number of situations. For example: airports to monitor busy areas where people might leave a bomb, handicapped parking, stock areas etc.

As with other algorithms, the Still Object Detection does not detect objects in the same way that a human eye/brain does; instead it measures the change in the light intensity level of an individual pixel over time. In doing this, it identifies 'blobs' of intensity change. If a blob is big enough and still enough, the algorithm will begin a countdown to determine whether it is stationary. Once this countdown stops, the algorithm will trigger. This trigger can be linked to any one of the events mentioned above.

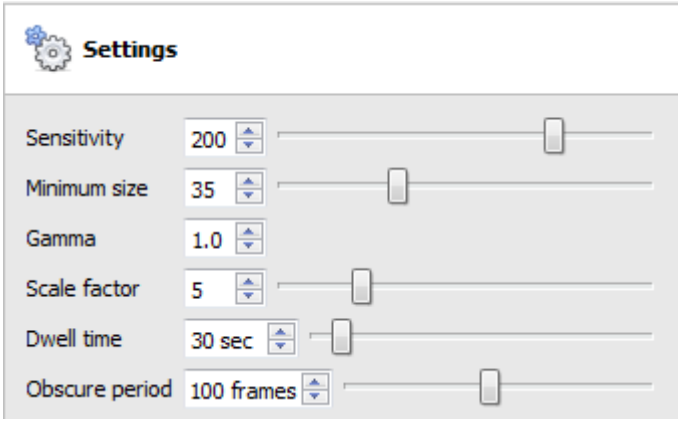
It is important to note that, as with all of the Video Motion algorithms, the setup process will be iterative. Adjust them to suit the environment, and the objects that being tracked. For this reason, the following guide will not provide a list of generic settings. It will, however, provide the meanings of the different terms, and explain how the algorithm works, so as to enable understanding and make intelligent and informed adjustments.

Choose Algorithm Type

Choose between the (updated) Background based Still Object algorithm, and the Legacy algorithm. The settings options will differ according to the algorithm chosen.



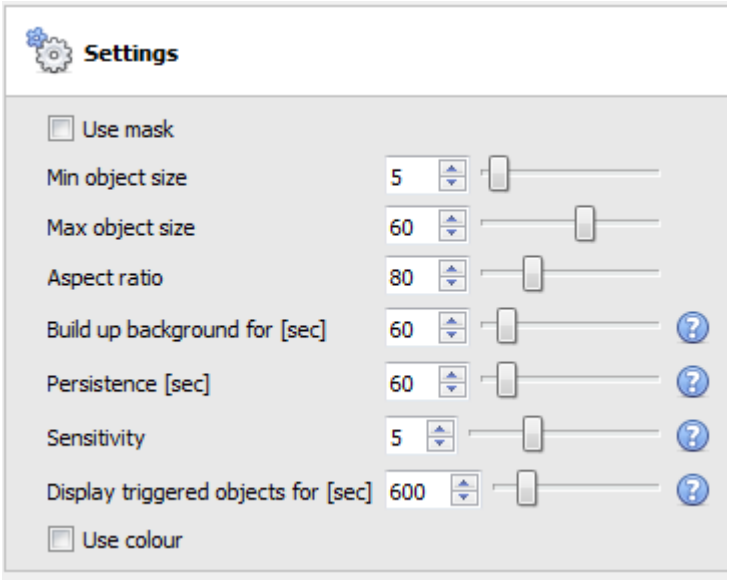
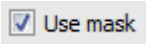
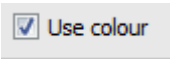
Legacy Settings



Sensitivity	This setting (between 50-250) reflects the actual light intensity changes on the pixel. Each pixel is capable of producing light of 256 different levels of intensity. The sensitivity setting will measure the change from this 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. Remember this is not the actual intensity of the pixel; it is the amount of change in intensity. So, if the pixel was at 50, and then jumped to 110 the change would be 60. If sensitivity was set to 50, this change would be considered significant.
Minimum size	This reflects the smallest an object can be, to be considered when triggering an alarm. As the slider is moved, an image will appear on the screen approximating the area needed to be taken up by the object.
Gamma	Gamma changes the brightness and contrast of an image. The important way that gamma changes these settings is that it changes them on a curve. Increasing the gamma will brighten darker areas, but have little effect on already bright areas. This will allow the

	elimination of shadows. If the objects already being tracked are generally a similar colour to the background they are set in, then there should be a higher gamma setting (>10). Decreasing gamma will darken lighter areas and have 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 the sensitivity. It multiplies the difference between foreground and background. Increasing the scale factor will make the algorithm more sensitive to slight changes between foreground and background. If objects are not being tracked, try increasing the scale factor. Decreasing the scale factor will make the algorithm less sensitive to slight changes between foreground and background. If parts of the background are being tracked, try decreasing the scale factor. Default scale factor is 5. The range is 1-20.
Dwell time	**Dwell time** is the time period that it takes for the algorithm to trigger an alarm, after a still object is either placed in, or removed from, an image. This time is important, as it will rule out objects that are momentarily placed, as well as momentary compression issues, and bugs on the screen etc.
Obscure period	In busier environments, such as train stations, a Still Object will constantly be covered and uncovered by people passing by. This setting allows the user to set the time period that an object is 'remembered' after something has obscured it. It is measured in frames, which are the individual images captured by the camera, and can go from 10-500 frames. 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 one will want to remember objects. There is a balance however as a busy environment will have many objects constantly being left and then taken away. Set a good balance between this setting and the **object dwell time** setting.

Background based Settings

	Check  to apply an algorithm **mask** to the area. **Note**: Adjust area of mask by clicking on it and dragging nodes. Set the **Min object size** to be monitored. Set the **Max object size** to be monitored. Adjust the **aspect ratio**. Select the number of seconds **to Build up background model** for. Set the number of seconds the **trigger must Persis**t in order to trigger. Set the **Sensitivity** of the algorithm. Note: The lower the sensitivity, the easier the objects will be picked up. Set the number of seconds that the triggered objects will be displayed for. Check  to use **colour** for triggered objects.

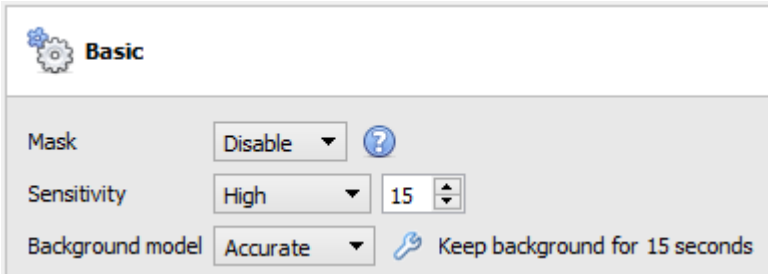
- Zones

Painting zones follows the same procedure described in Basic VMD, above.

Analytics I, II and III Basic, Advanced, and Calibration Settings

The three Analytics Channels all share the same options for Basic, Advanced, and Calibration Settings

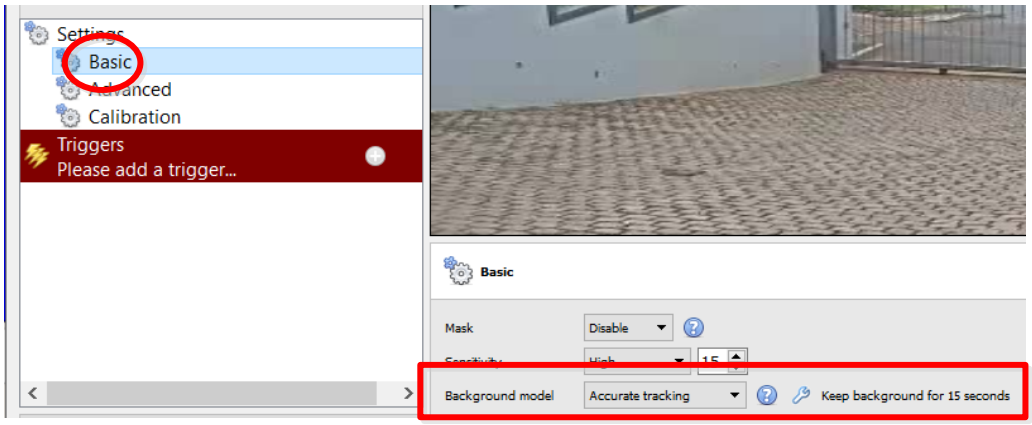
- Basic



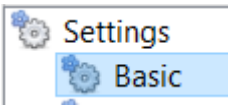
Mask	The mask defines which areas of the camera image have the algorithm applied to them. The user may wish to hide certain, busy, areas from the algorithm to prevent false triggers. By default, it is disabled, which means that the algorithm will apply to the entire image. Editing the mask: • Once enabled, manipulate the mask by clicking on the control points, and dragging them to move the corners of the mask. • Holding CTRL and clicking a point on one of the lines, will add a new control point. • Double clicking on a control point will remove it. • To move the whole mask, without changing its shape, left-click and hold anywhere on the mask that **isn't** a control point, and move the mouse. **Note**: the part of the image covered in the mask will be the part where the algorithm is active.
Sensitivity	This will define the algorithms response to changes in the image.
Background model	For the algorithm to know that something has changed in the image, it needs to have a predefined "normal" to work with. This is the background. The background model will define how long this is calculated. **Note**: Background model settings are only available in the Basic, Intermediate, and Advanced algorithms (within the Analytics type of analytics).

Background Model

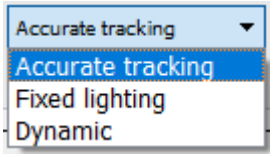
If either Basic, Intermediate, or Advanced algorithms within the Analytics type analytics are chosen, the user will be able to select a background model.



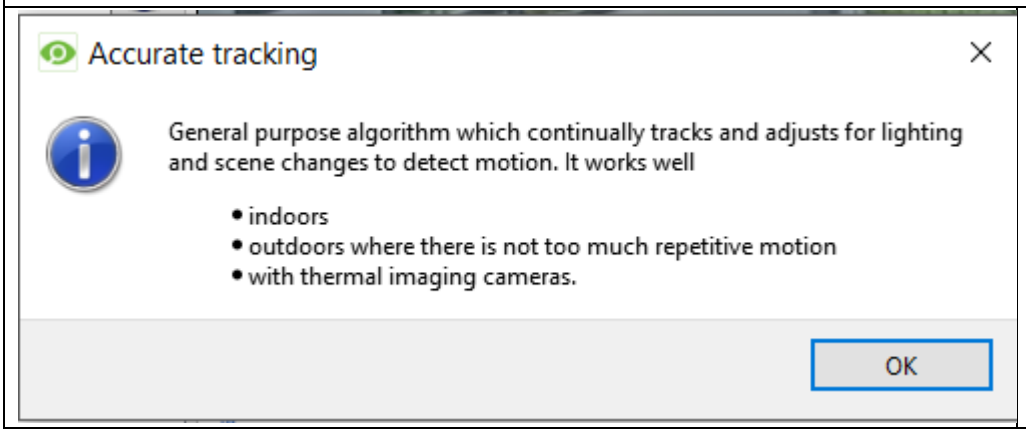
Under **Settings**, on the left of the window, select the **Basic** settings option.



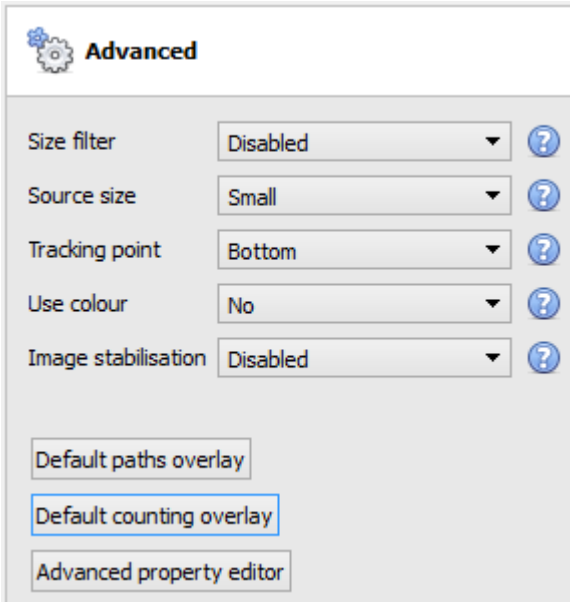
Select the Background Model:

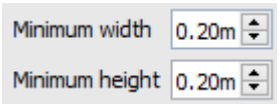


Click the  to display information about the selected background model. This information is useful in deciding which model will be best suited to which conext. For example, when Accurate tracking is selected, the information displayed is:



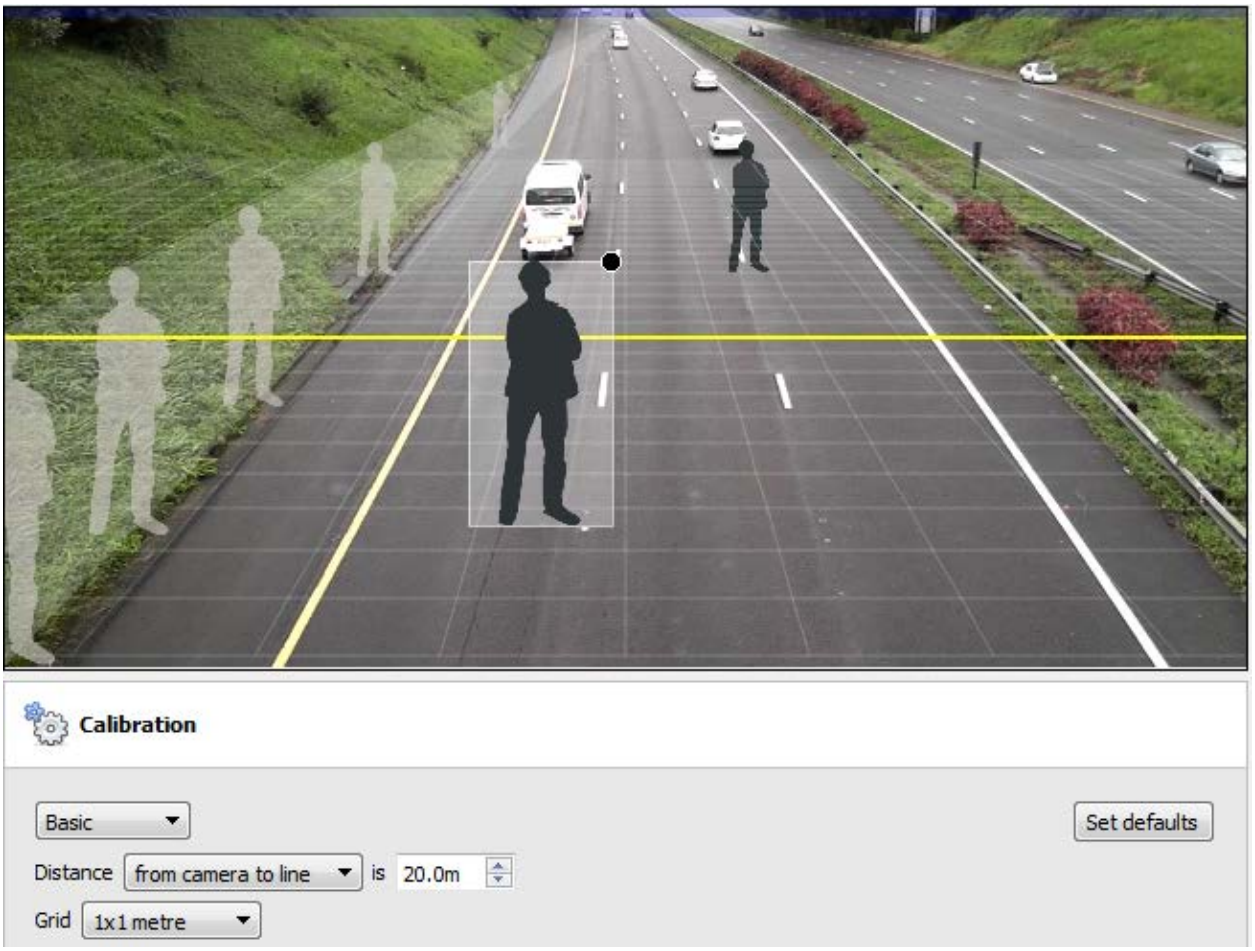
- Advanced



Size Filter	Filter out objects smaller than the minimum size.  When enabled, the minimum width and height options will be added to the interface. **Note:** This is only implemented in **CathexisVision** 2016 and later; when connecting to an older software version this option will be present, but ineffective.
Source size	This 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.
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.
Image stabilisation	This enables image stabilisation for cases where camera shake is a problem. **Important note**: This should not be enabled by default, because it places a heavy load on the processor of the computer.
Default paths overlay	Allows the user to choose between a default object path overlay, and a user defined one.
Default counting overlay	Allows the user to choose between a default object path overlay, and a user defined one.

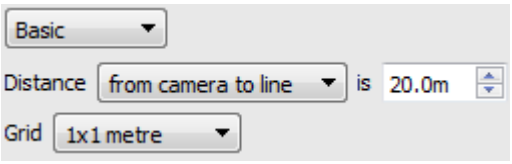
Advanced Property Editor	This section is included in the software for support purposes only, and is very technical. As a rule of thumb, **if the user does not understand the option presented, do not edit them.**

- Calibration



The calibration is used to help determine the size of objects in the image. It uses a number of parameters to do so.

Basic Calibration



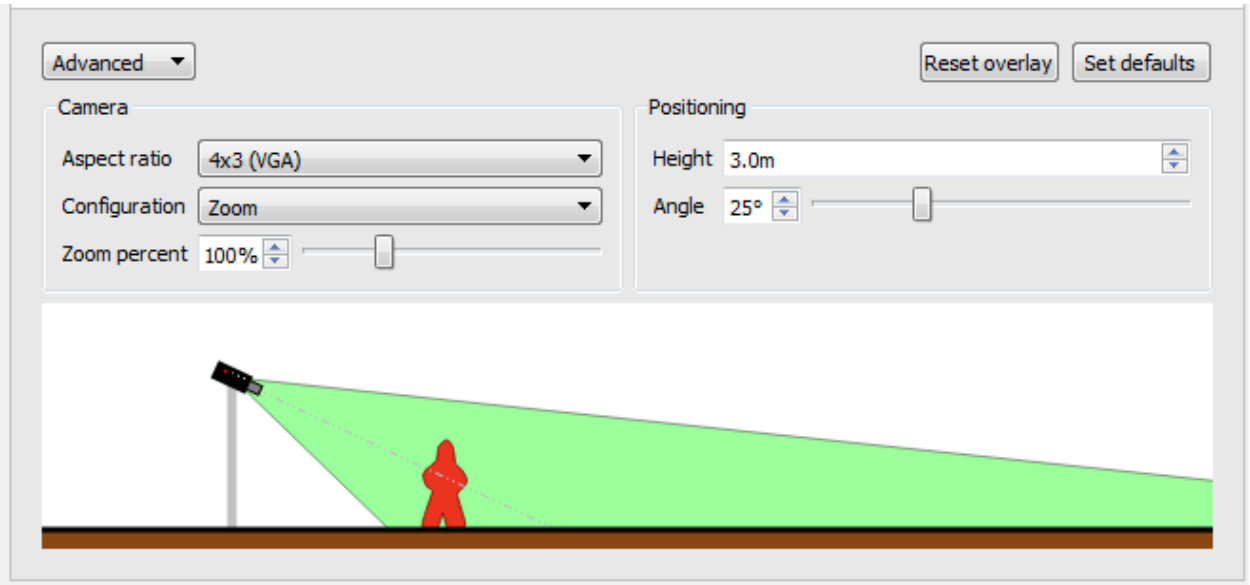
Distance	**From camera to line** Here, set the actual distance between the position of the camera and the yellow line in the image. The line can be moved, by clicking on it, and dragging it. **Between lines** Here, estimate the distance between the two lines that appear in the camera image.
Grid	The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

Adjusting the depth of field of the image

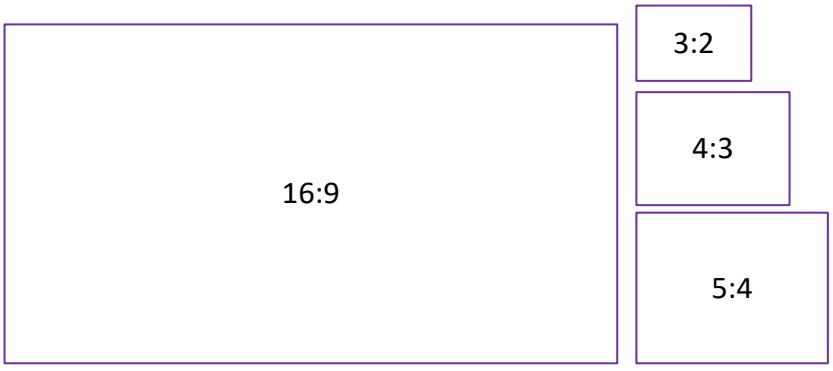
This is done by dragging the human shapes to 2 different locations (near and far) and resizing them appropriately.

Advanced Calibration

Note: it is suggested to only use the advanced calibration settings when very accurate data regarding the settings is required.

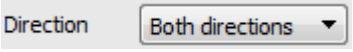


Advanced Calibration adds a number of options.

Aspect ratio	This refers to the shape of the camera image. The below image should provide an idea of the aspect ratio being looked a. One should know from the camera itself what the aspect ratio is: 
Configuration	This is where the viewing angle is defined. Either 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, 0 degrees as the level point.

- Basic Line Trigger

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. The user will be able to lengthen, and pivot, the line against the control point at the other end of the line.

- Basic Presence Trigger

This basic algorithm will trigger while an object is within the defined mask. The only changeable setting on this trigger is the mask.

Editing the mask:

- Once enabled, manipulate the mask either by clicking on the control points, and dragging them to move the corners of the mask.
- Holding CTRL and clicking a point on one of the lines, will add a new control point.
- Double clicking on a control point will remove it.
- To move the whole mask, without changing its shape, left-click and hold anywhere on the mask that **isn't** a control point, and move the mouse.

Note: the part of the image covered in the mask will be the part where the algorithm is active.

- Advanced Area Triggers

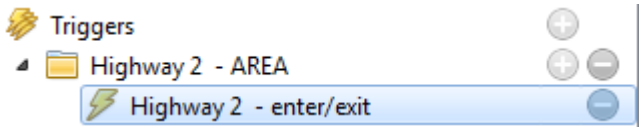
Adding an "Advanced Area Triggers" group allows the user to define an area which can be used by one or more triggers. This is useful because the area is only drawn once.

Editing the mask:

- Once enabled, manipulate the mask by clicking on the control points, and dragging them to move the corners of the mask.
- Holding CTRL and clicking a point on one of the lines, will add a new control point.
- Double clicking on a control point will remove it.
- To move the whole mask, without changing its shape, left-click and hold anywhere on the mask that **isn't** a control point, and move the mouse.

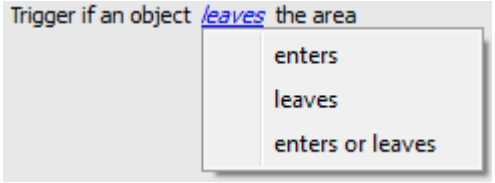
Note: the park of the image covered in the mask will be the part where the algorithm is active.

- Enter/Exit Trigger



Note: the mask editing procedure is identical to the one above, in Basic Presence Trigger.

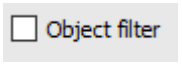
When to Trigger



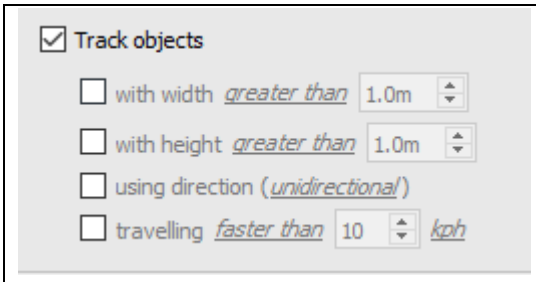
Choose between triggering the event when an object enters the area, exits the area, or both. The trigger occurs at the point when the object crosses the boundary.

Object Filter

The Advanced Area Trigger allows for object filtering on triggers which are added to the area. This means that the objects which will trigger in the area can be filtered to only trigger on objects of certain heights/widths/directions/speed.

Select the triggers in the settings panel, and then tick 

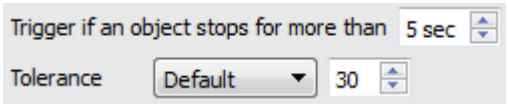
in the Context Area.

	Once Object filter is ticked, the Track objects options will appear. Select the filters to apply to trigger objects, and specify each according to requirements.

- Time in Area (loitering) Trigger

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

- Stop in Area Trigger

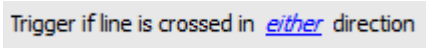


Set how long an object must be stationary for, before it triggers. **Tolerance** is how far/much the object is allowed to move, while still considered to be stopped. It is measured in Pixels.

- Advanced Line Triggers

Like the Advanced Area Trigger, this is a group under which triggers can be placed, sharing the same line.

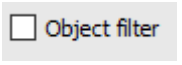
- To add a control point to the Advanced Line Trigger, hold down CTRL while clicking anywhere on the line.
- To move a control point, hold down left-click on that point, while moving the mouse.



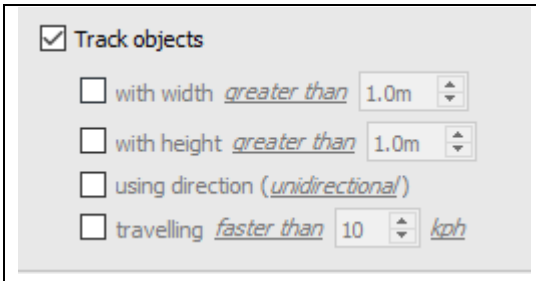
This image appears in the context area when adding a trigger. Also define the **direction** which will trigger the line.

Object Filter

The Advanced Line Trigger allows for object filtering on both line counters and triggers which are added to the Line. This means that the 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, and then tick 

in the Context Area.

	Once Object filter is ticked, the Track objects options will appear. Select the filters to apply to trigger objects, and specify each according to requirements.

- Speed Triggers

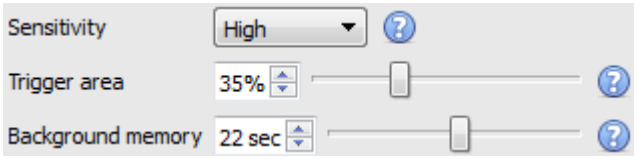
The distance here is the distance between the two lines seen on the camera image.

Note: How well this works will depend on how accurate the distance between the lines is.

- Basic 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. This would be useful, for example, in a shopping centre, to alert a manager that they need more cashiers working the tills.

- Settings



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*4 pixel blocks that the algorithm uses) in order for the algorithm to also trigger.

Memory is how long it remembers the background.

Adding/Editing a Zone

By default, there are three zones which 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.

Front and Back Zones

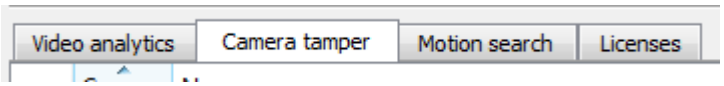
The green zone must always be set at the beginning of the queue, and the red zone must be set at the end of the queue.

Note: One cannot divide the green and red zones.

- Triggers

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

e. Camera Tamper Detection (tab)



Enabling camera tamper on one/multiple cameras means there will be an alert if any of those cameras have been tampered with, or if any conditions concerning the camera impede its video feed. Also add CathexisVision standard events, which are triggered by a tamper.

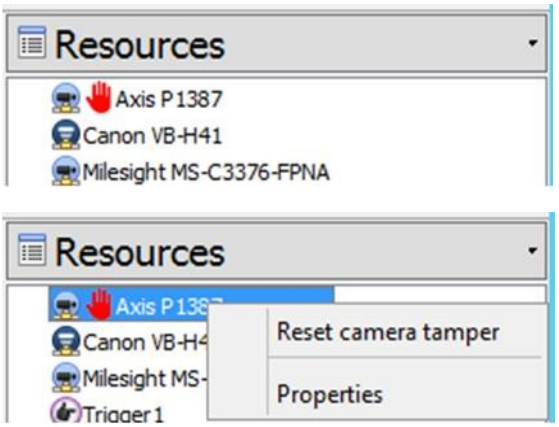
A camera is considered to have been tampered with if any of the following occur:

Tamper	Explanation
Camera moves position	This might be the natural sliding of the camera if it has not been secured properly, or if someone intentionally moves it, such as a maintenance worker, or potential intruder.
Camera becomes defocused	This might be a natural defocus of the camera itself, or someone might have defocused it intentionally, such as a maintenance worker, or a potential intruder.
Camera is covered	The camera may be covered by an object (such as a hand, cloth, paint, etc.).
Extreme lighting changes	This might be a torch light or any other extreme lighting changes which are not considered 'natural.'

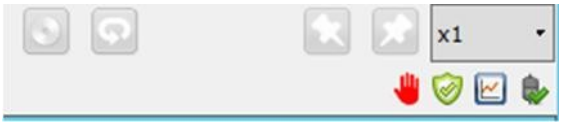
Note: To add camera tamper, the desired camera must have a video analytics enabled feed.

When a Camera is Tampered

When a camera is tampered with, a few things will happen:

	Event	Description	
1.	Tamper icon appears in Resources List.	A red hand icon will appear in front of the tampered camera in the Resources List of the Cameras tab. If access rights have been assigned to do so, operators may reset the tamper from here by right- clicking on the camera.	

2. Tamper icon appears at the bottom of the GUI. Clicking on the icon will display a list of tampered cameras. If access rights are assigned to do so, operators may reset the tamper from here.

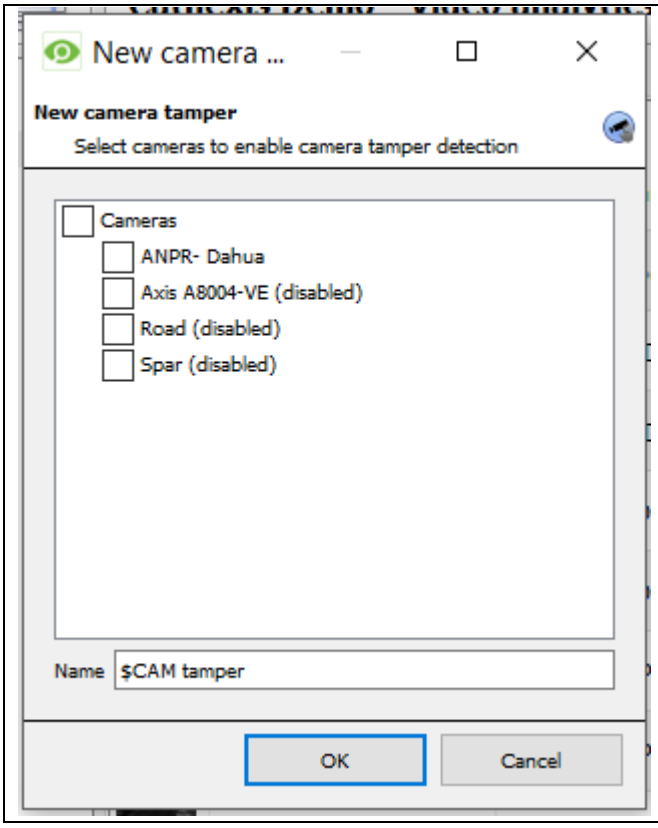


3. Event Triggered (possibly) If an event is setup with a tamper trigger, then this event and its actions will be set off.

Add Camera Tamper Detection

In the Video Analytics section of Configure Servers, navigate to the **Camera tamper tab**.

Select New to enable existing cameras with camera tamper detection in the dialogue box that opens.



Only cameras which have had video analytics enabled will be available to add camera tamper detection.

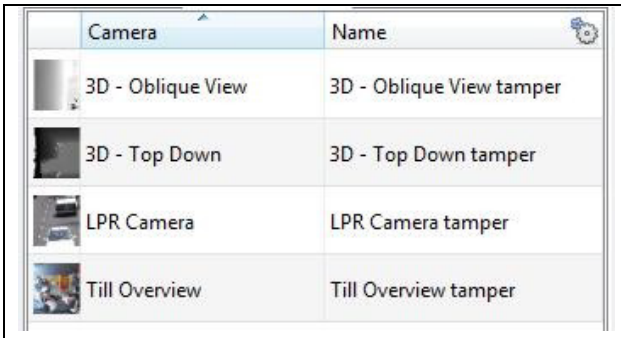
To add camera tamper detection to all cameras, select 

.

To only add camera tamper detection to selected cameras, check the desired cameras.

Click **OK** when done.

Once camera tamper detection has been added, the relevant cameras will appear in a list, like below.

	**Camera** indicates the camera to which tamper detection has been applied. **Name** is the default name of the tamper detection algorithm applied to the camera: It is the camera name + tamper. To change the name of the tamper algorithm, right-click and select **Properties**, or click the **Edit** button.

Note:

1. To add camera tamper detection, cameras must have already been added to the system, and they must have video analytics enabled.
2. It is a good idea to setup a database specifically for camera tamper if there are other triggered recordings set up.

Triggering Events with a Tamper

Please see the **Events Section** for information on creating events triggered by a camera tamper.

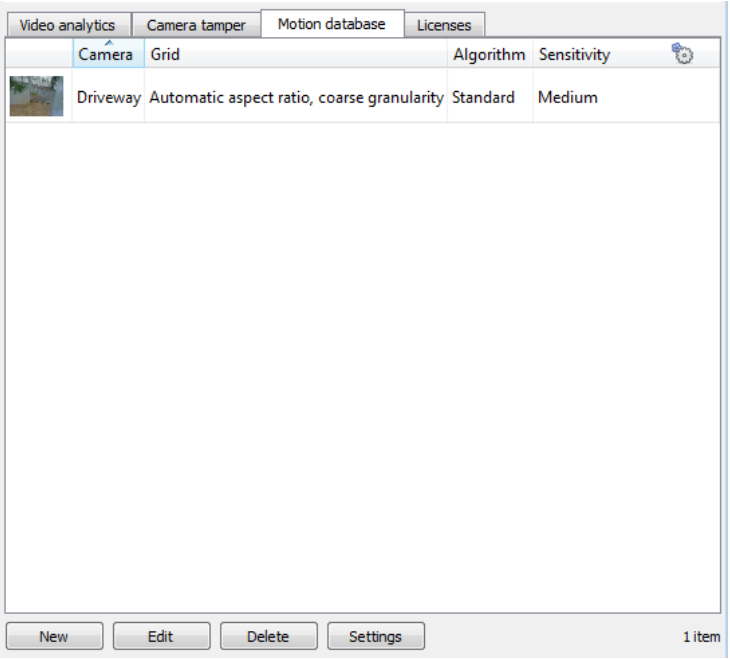
Reset Tamper Access Rights

Please see the **Access Rights Section** for information on granting access rights for user access levels to reset camera tamper.

f. Motion Database (tab)

A Motion Database is required to use the Activity Trails and Motion Area Search analytics. 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.



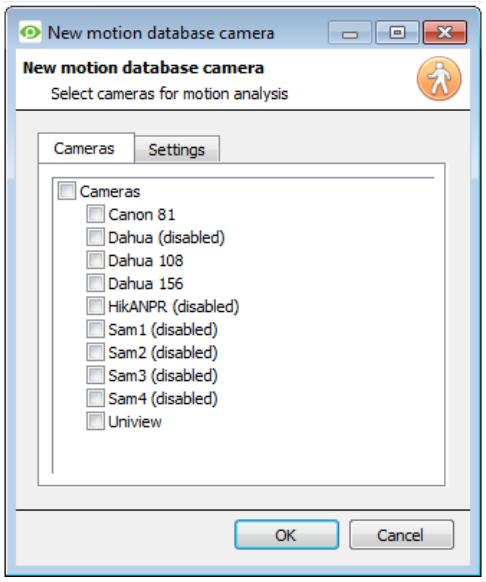
New	Add a new motion database camera.
Edit	Edit an existing motion database camera.
Delete	Delete a motion database camera.
Settings	Configure size and path of Motion Database. See below.

Note: Only one motion database may be configured.

New 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.

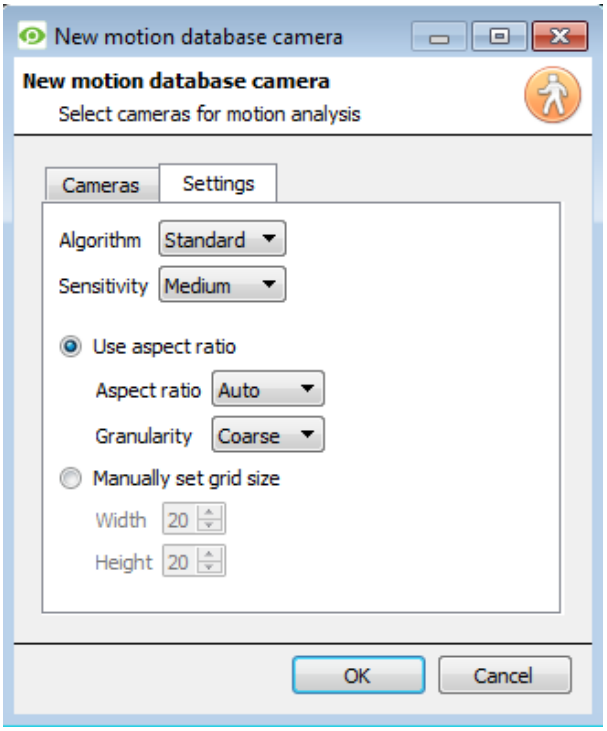
- ***Cameras Tab***



Select the cameras that motion search will be enabled on.

Note: **Cameras** must be checked before checking the desired cameras.

- ***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 aspect ratio is used;

Select the **Aspect ratio**.

Select the **Granularity** of the overlay grid. See below for an explanation on Granularity.

If grid size is manually set, select the **Width** and **Height** of the grid.

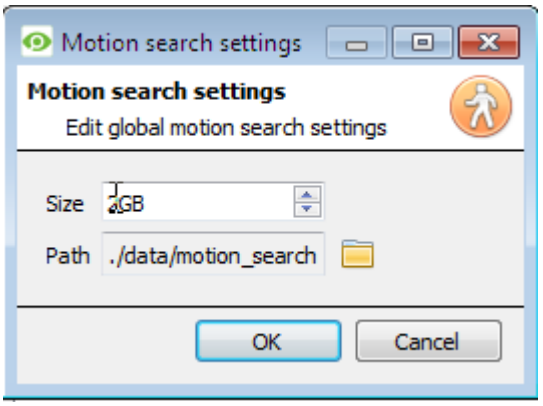
Click **OK** when done.

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.

Motion Database Settings

To configure the size and path of the Motion Database, click the Settings button.

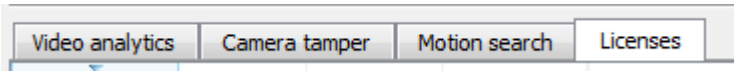


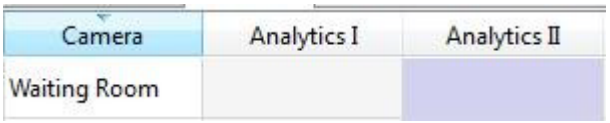
Motion Data is saved in its own database.

Set the **size** of the database.

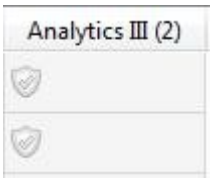
Click to set the **path** of the database.

g. 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.

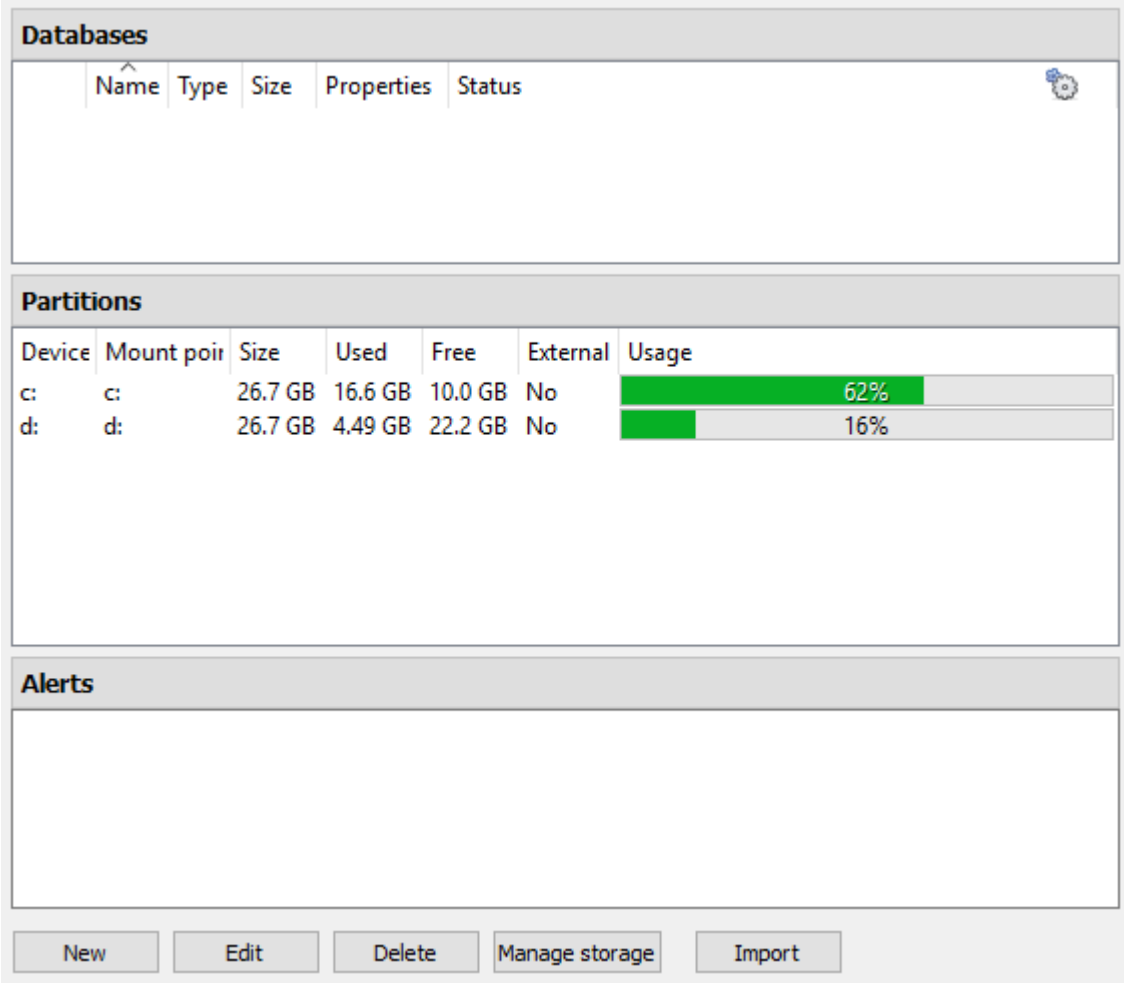


In the tab, there is a list of all cameras on this server, with a column for each Analytics type (from I to III). Spare Analytics licenses will be listed in parentheses next to the column header for that type. E.g. Analytics III has 2 spare licenses here: Analytics III (2) . There will also be greyed **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 Databases

Databases are added on a Server-by-Server basis. As such, each server under **Configure Servers** will have a Databases section where that server's databases are managed.



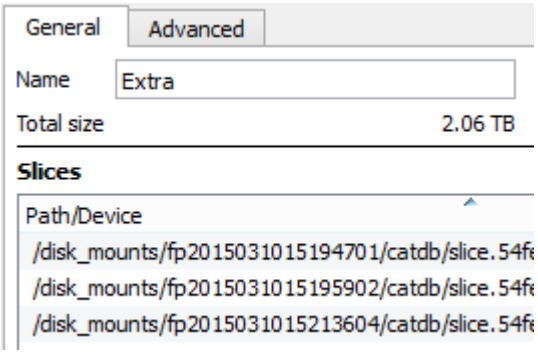
a. Add a Database

To create a new database, click on the **New** button in the **Databases** panel.

Note:

1. For Adding/Importing a database to an NVR from another unit, or via a Client, there will not be the **Browse** option. Know the file path and enter it in 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.

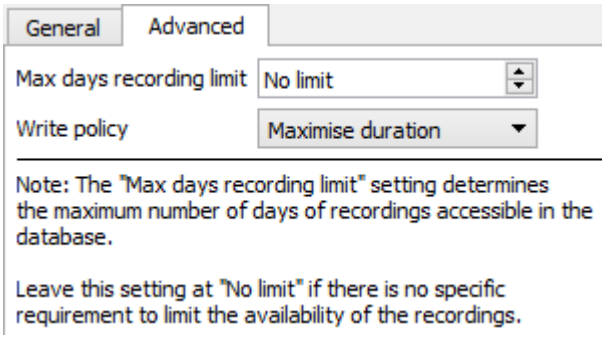
- General



Give the database a descriptive **name**.

An explanation of what slices are, and how to add them follows below.

- Advanced



The **Max days recording** setting will define how many days the database will record for, before overwriting the oldest recordings. With **no limit** set, it will simply wait until the database is full to begin overwriting old data.

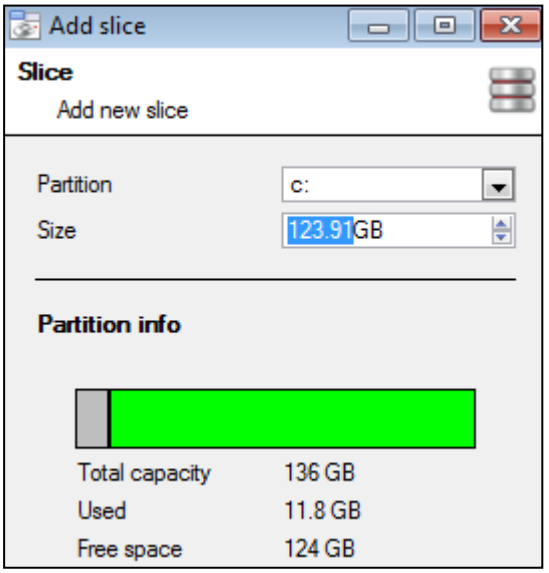
Write policy will provide the option of maximising the duration of recording, or the performance speeds of the database.

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.

- Adding a Slice

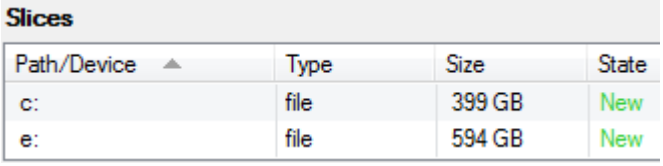
The database is comprised of a number of slices, which are sections of hard drive partitions. To Add a Slice:



Click on 

—> 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:



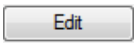
Once slices are added, click on OK to create an Advanced Database.

- Important Recommendations

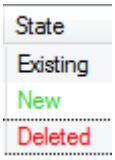
1. Ideally, the database should be in its **own partition**, on its **own Hard Drive.**
2. If the database must share a drive with other information, then put it in its **own partition**.
3. It is recommended to not create a database in the Primary Windows Partition, however, if the user wants to do so:
    a. Do not create it within the **CathexisVision NVR** installation folder.
    b. Do not make the database size unlimited. Leave between 50 and 100GB of disk space free when setting the size.

b. Edit an Existing Database

There are two ways to edit an existing database, either:

1. Select the database —> Click on the 

button.
2. Double-click on the Database to edit



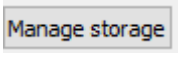
When editing a database, editions to the slices will appear in the State column within the **Slices** textbox.

c. Alerts

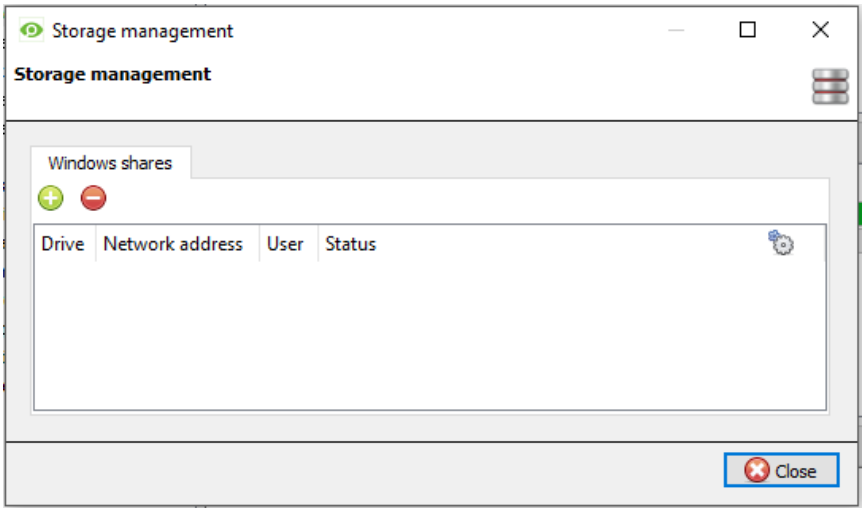
The alerts are specific to the currently selected database, and will show the *individual slice status*, if a slice in that database is not in a ready state.

For example, if the slice in a database is busy initialising, or if there is an error, there will be an alert (with the slice ID) if that database is selected:

d. Manage Storage

Windows network shares can be managed by clicking on the 

button.

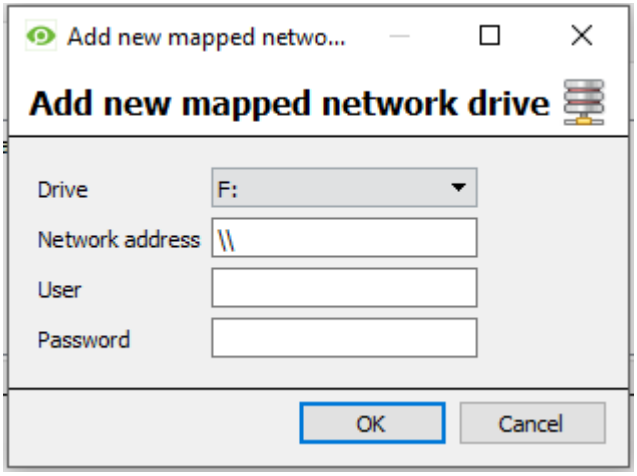


To add or remove network shares, use the buttons.

Details of the network shares will appear in this area.

See below for adding a new network drive.

Add New Network Drive



Select the **Drive**.

Enter the Network Address.

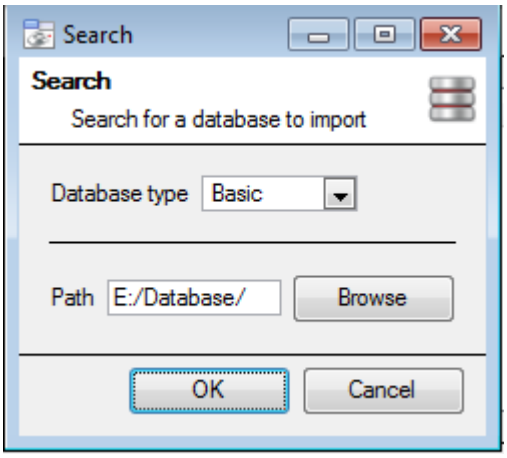
Enter the **User** and **Password** details.

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).

e. Import a Database

To import an existing database, click on Import. There are two steps in importing a database:

- Navigate to the Database Folder



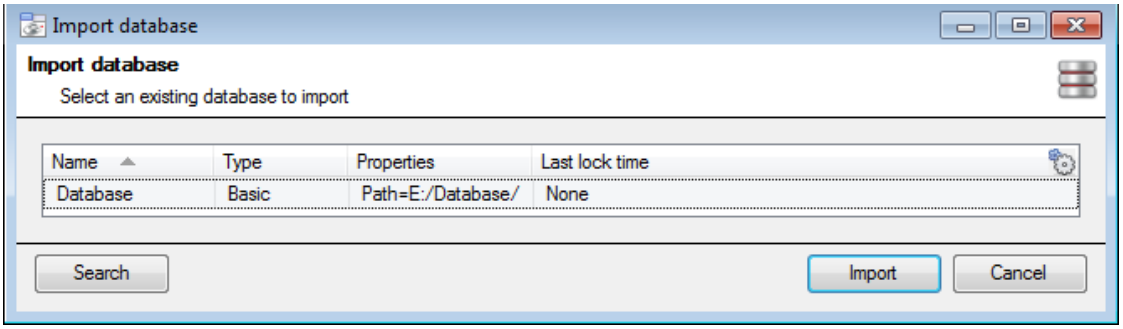
There may be multiple databases stored in one folder, and a database isn't represented as a single file. For this reason, when importing a database, one only needs to navigate into the folder that contains the database to import.

Select the Database Type
Define whether 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.

- Select the Database

CathexisVision will populate the database list, with all databases found in this folder. Select the database to add from the list of databases.



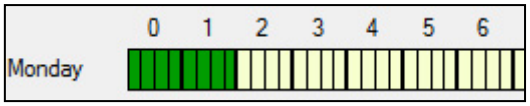
5 Schedules

All the unit's schedules for recording, and events, will be maintained under Schedules in the configure servers options.

- ***Add/Edit a Schedule***

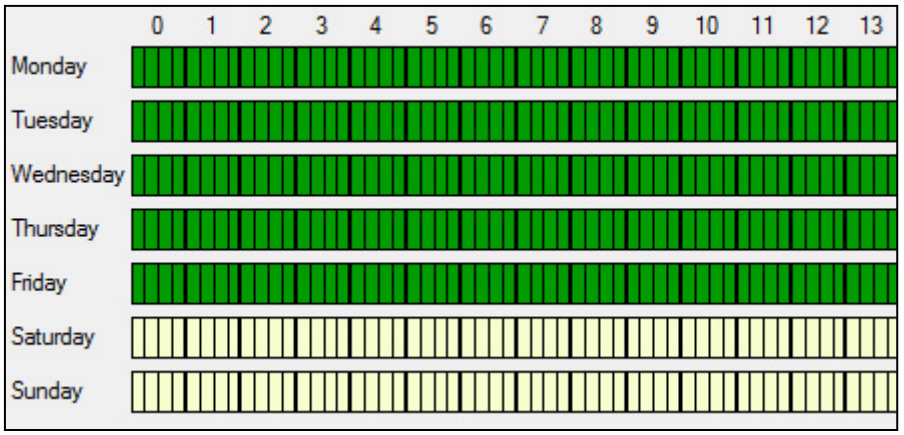
To add/edit a schedule, click on the relevant button and follow the instructions below. Give the schedule a descriptive name, and then define the recording times (as shown below).

- ***Set Recording up, and down-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.



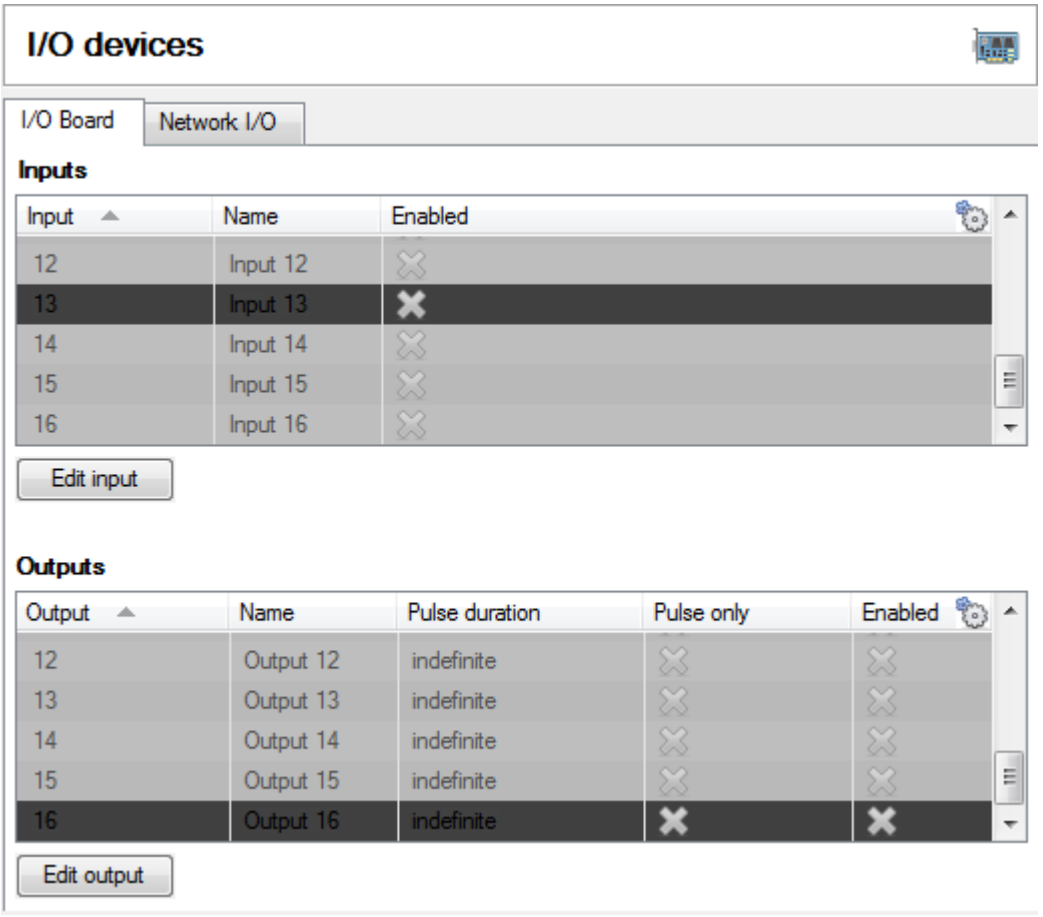
Recording week days only
To record only week days, set the schedule as seen on the left.

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.

It is as simple as that. Click OK, and the schedule has been created. This schedule may now be used for recording, and events on this unit.

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.



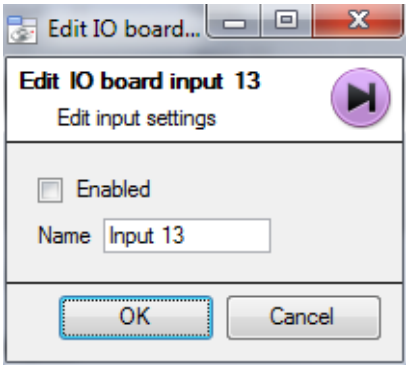
a. Analogue

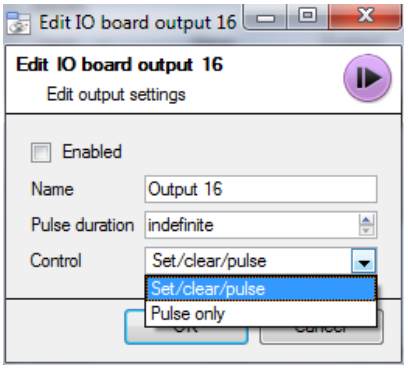
Relay connection on an analogue unit will be via the IO Board, on the back of the unit. This is connected to a PIA-mod card that comes standard on all CathexisVision analogue units.

The IO panel allows for 16 inputs, and 16 outputs

- 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 the input a descriptive name.

- Output Specific

Pulse Duration
One may set the duration of the output pulse, in milliseconds.

Control
One may also set how the Relay is controlled. Give Set, Clear, and Pulse control; or set it to Pulse exclusively.

b. Network

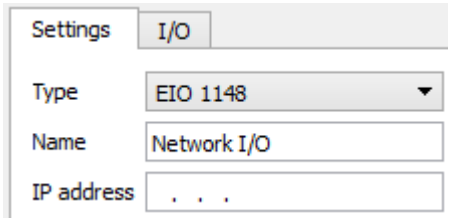
Network Based IOs are handled by the EIO-1148, or EIO-3148, Network Base IO Expander.

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.

- Settings Tab

Clicking on the Network I/O tab, within the I/O devices option, followed by selecting 

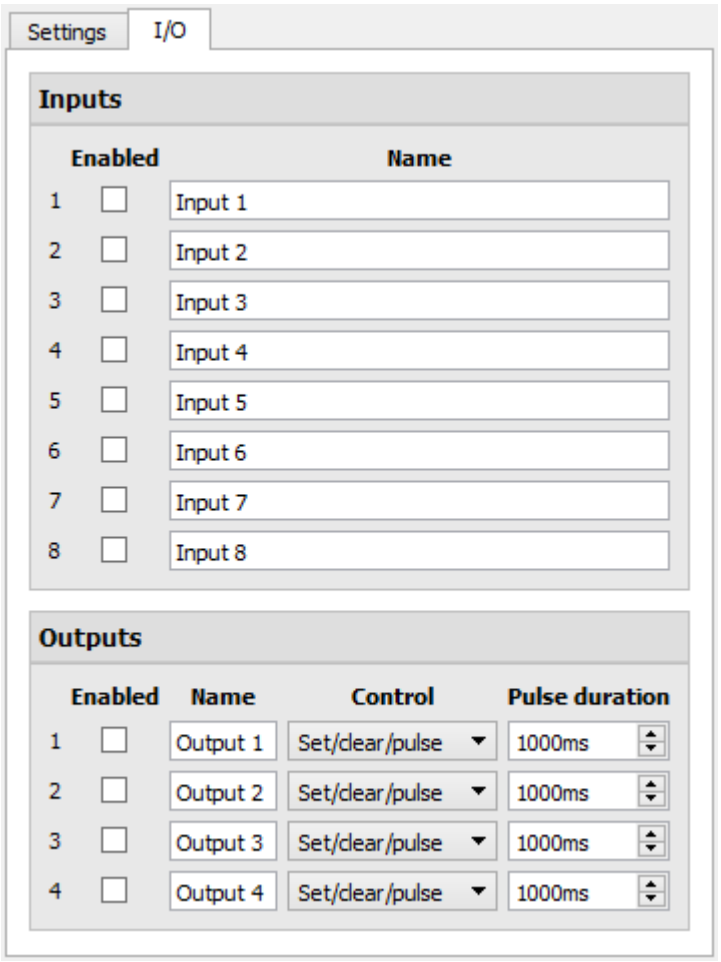
, gives the following options.



Name
Give the 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 **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.

- IO Tab



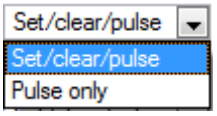
General:

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 dropdown menu in the Control column.



Pulse Duration:

Set the pulse duration of the relay, in milliseconds.

Note: make sure to give these inputs descriptive names.

7 Scheduled Recordings

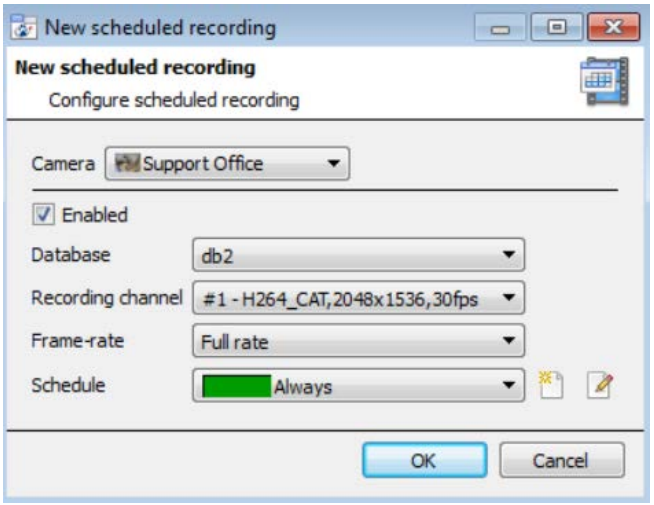
One may set cameras to record on a fixed schedule. This is done in Scheduled recordings under **Configure Servers**.

- Add/Edit a Scheduled Recording

Either:

1. Click on New or Edit. Or
2. Right-click
   a. white-space and clicking on **New** (for a new Schedule)
   b. on an existing schedule and selecting P**roperties** (to edit this existing schedule)

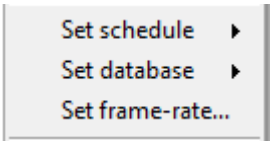
This will bring up the Scheduled recording dialogue:



Camera	Select the camera to record.
Enabled	To enable the schedule, check the box, to disable the schedule uncheck the box.
Database	The database to record to.
Recording Channel	The video channel to record from the camera.
Frame Rate	The frame rate at which to record.
Schedule	The particular schedule to assign to this Scheduled Recording.

Note: The schedules that are available are the schedules that are maintained under Schedules on each server. Create/edit these schedules here, using the options.

- Right-click Menu



Make a quick adjustment to a schedule by right-clicking on it.

To change the recording Channel, edit the schedule via **Right-Click → Properties**; or by selecting the Schedule and clicking Edit.

- Copy Paste

Copy/paste schedule settings either from one schedule to another, or from one schedule to a new camera.

Copy schedule settings from one schedule to another
Right-click on an existing algorithm, and then click on Copy. Then right-click on the algorithm to overwrite and click Paste.

Copy schedule settings to a new schedule

Here, copy the schedule settings onto a camera, so right-click and Copy the existing schedule. Then right-click anywhere and select Paste new... this will bring up a list of cameras that are attached to this unit (e.g. ☑ Analog One).

Select any number of cameras to paste the schedule onto, and click OK.

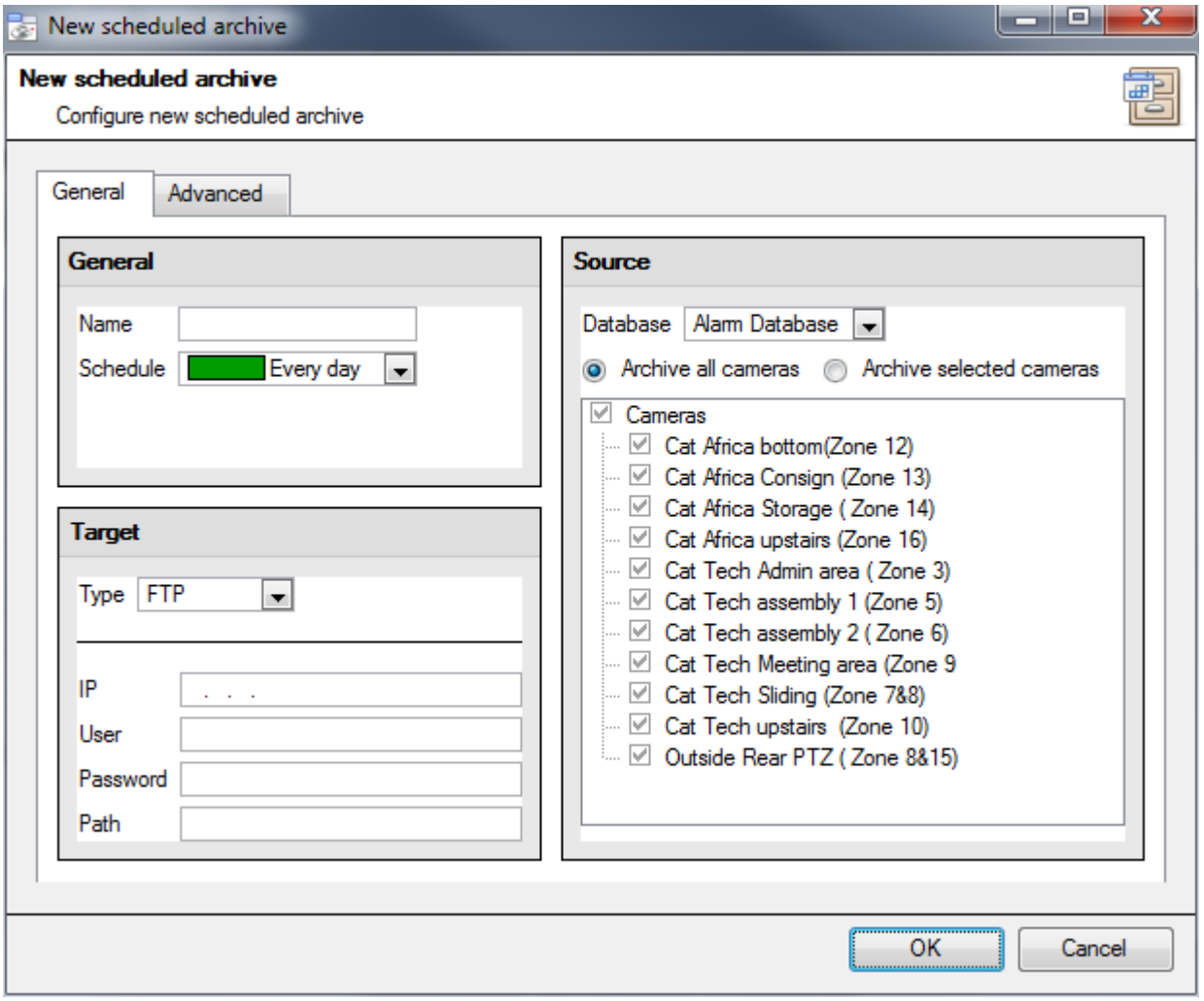
8 Scheduled Archives

Archiving is a facility to enable copying selected 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.

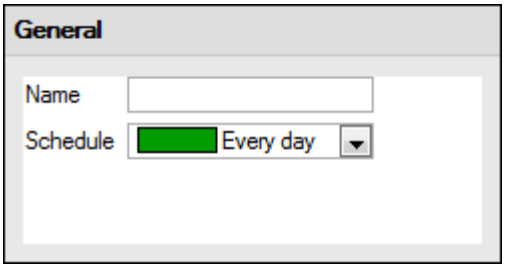
This is useful for a number of reasons. An important function, is to create an archive of important cameras. As databases fill up, they start to write over the oldest recordings. In order to keep some camera's recordings for extended periods of time, it is important to archive them.

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.



a. General

- General

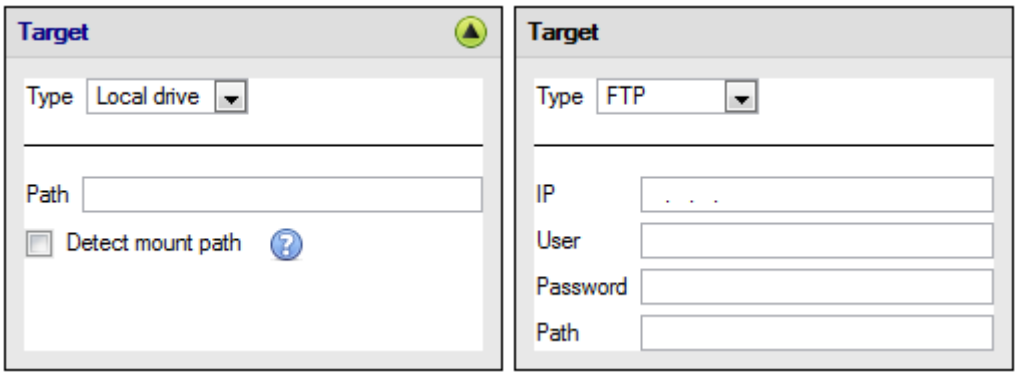


General settings consist of assigning this archive a name, and a schedule.

Note: the schedules available are the same schedules set under **Configure Servers —> Schedules**.

- Target

Under Target, define where the archives are going to be recorded to. Select the relevant option from the **Type** dropdown menu.



Local drive

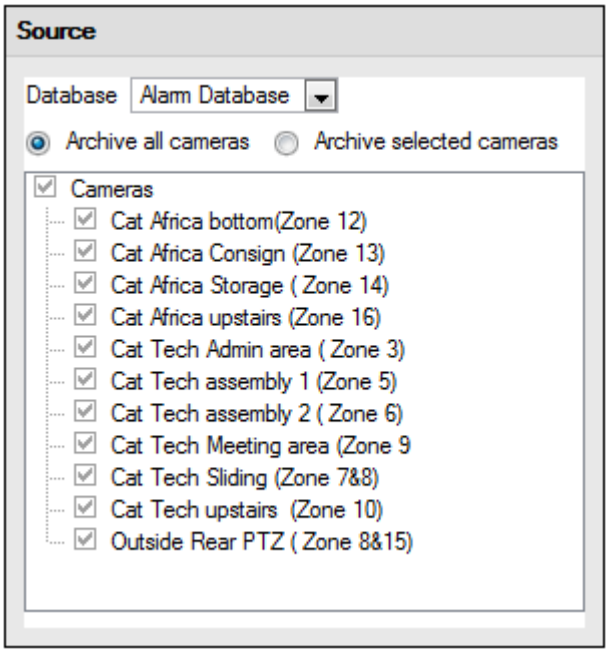
This will write to a selected path on the local hard drive, of the recording unit.

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.

- Source

Source will define which cameras are to be archived, and which database to draw the cameras' recordings from.



Database

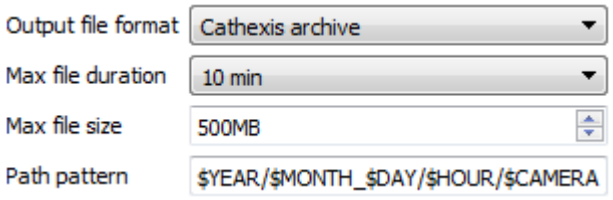
One may have multiple databases for groups of cameras. Or one may be sending camera recordings from different triggers, to different databases (e.g. VMD input, Access Control, Alarm Panels).

The database drop-down menu will provide a list of all available databases.

Cameras

Check the Archive all Cameras option, or Archive Selected Cameras.

b. Advanced



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

9 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.

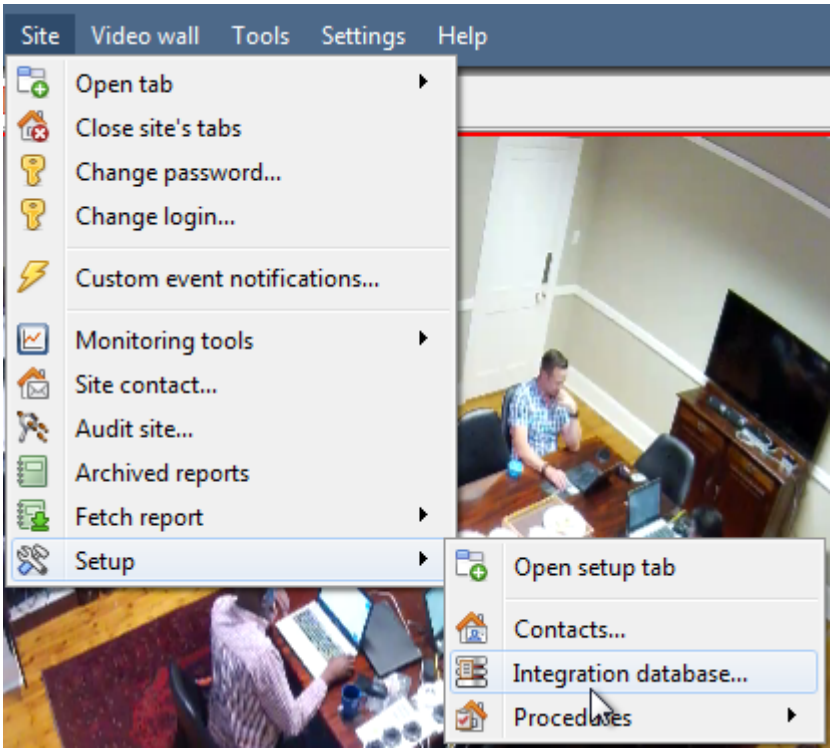
See below for information on creating the Cathexis Events meta-database, before proceeding with creating CathexisVision system events.

a. Cathexis Events Meta-Database

A Cathexis Events meta-database, 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 meta-database.

It might be useful to create this meta-database before proceeding with creating the events.

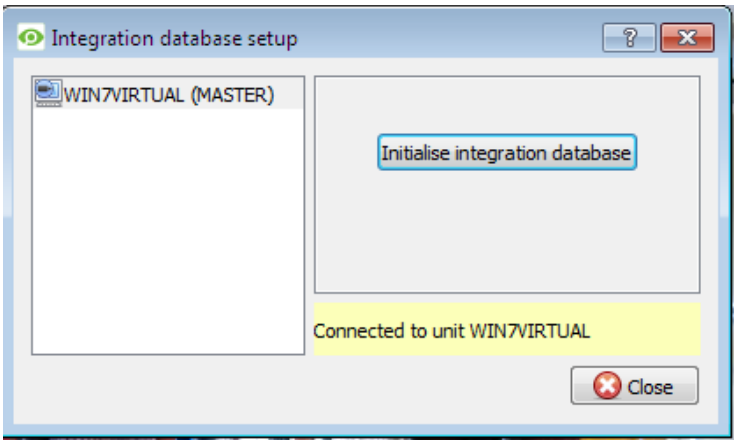
Open Integration Database Window



Site Menu → Setup → Integration database…

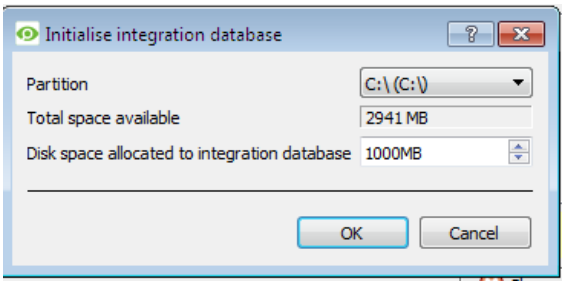
- ***Initialise Integration Database***

If integrations are not added to the system, this may be the first time it is necessary to initialise the integration database, also called the meta-database.



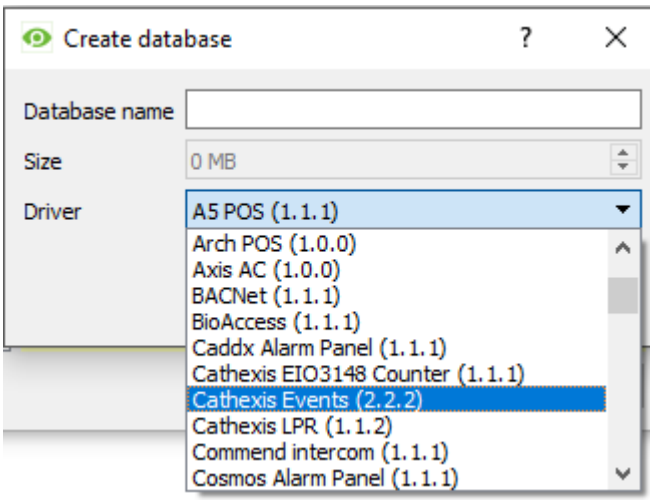
Click to Initialise Integration Database.

Then, select the size and partition of the data-base:



Create Cathexis Events Meta-Database

Once the integration database has been initialised (if required), one may create the events meta-database by right-clicking in the white space and selecting **New**.



Give the meta-database 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.

That's it. No other setup is required in order to get the events data-base working. Should information on the operation of the meta-database be required, then please consult the Operator's Manual.

b. Navigate to the Events Window

Navigate to the events window via the Setup Tab. The path to follow is ***Site →Setup →Configure Servers →Events***:

Important Note

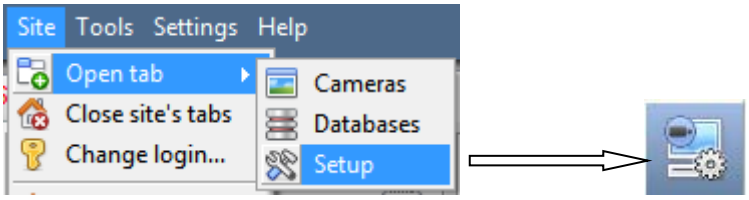
It is important to remember that Events depend on triggers that are predefined. This means that before reaching the events window, these inputs and outputs should be ready. An example [which will be discussed

later] is recording based on motion. In order to set up an event based on motion detection, a number of things are necessary:

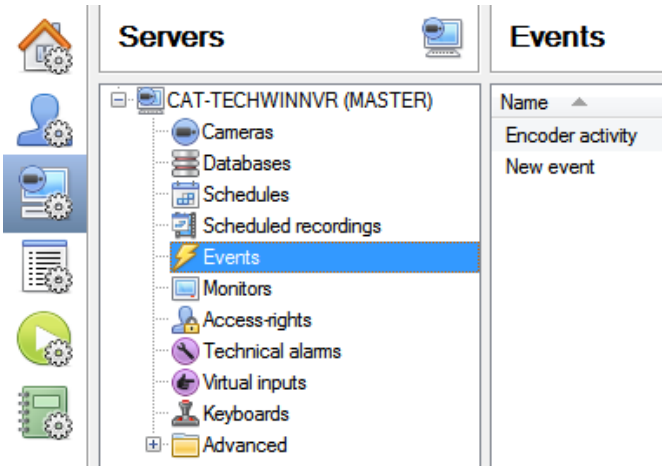
1. A camera that has been successfully added to the system [to provide the images]
2. A Video Motion Detection algorithm needs to have been set up [to *trigger* the event]
3. A database needs to be set up [as a point where the *action* of recording takes place]

It is easy to forget this, and head straight to the Events window to create an event, before one has all the resources to do so.

Site → Open Tab → Setup → Configure Servers



- Select the Events from the Servers menu.



c. New Events Window Interface

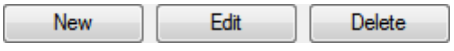
Introduction

Events can be very complex things, with multiple triggers and actions; but they all 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).

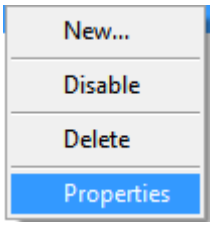
Below, the general events window interface is examined, as well as the four individual sections to edit when creating an event (General Settings, Triggers, Actions, and Resources). These are visible as tabs in the above screen capture of the Events Window.

General Interface.

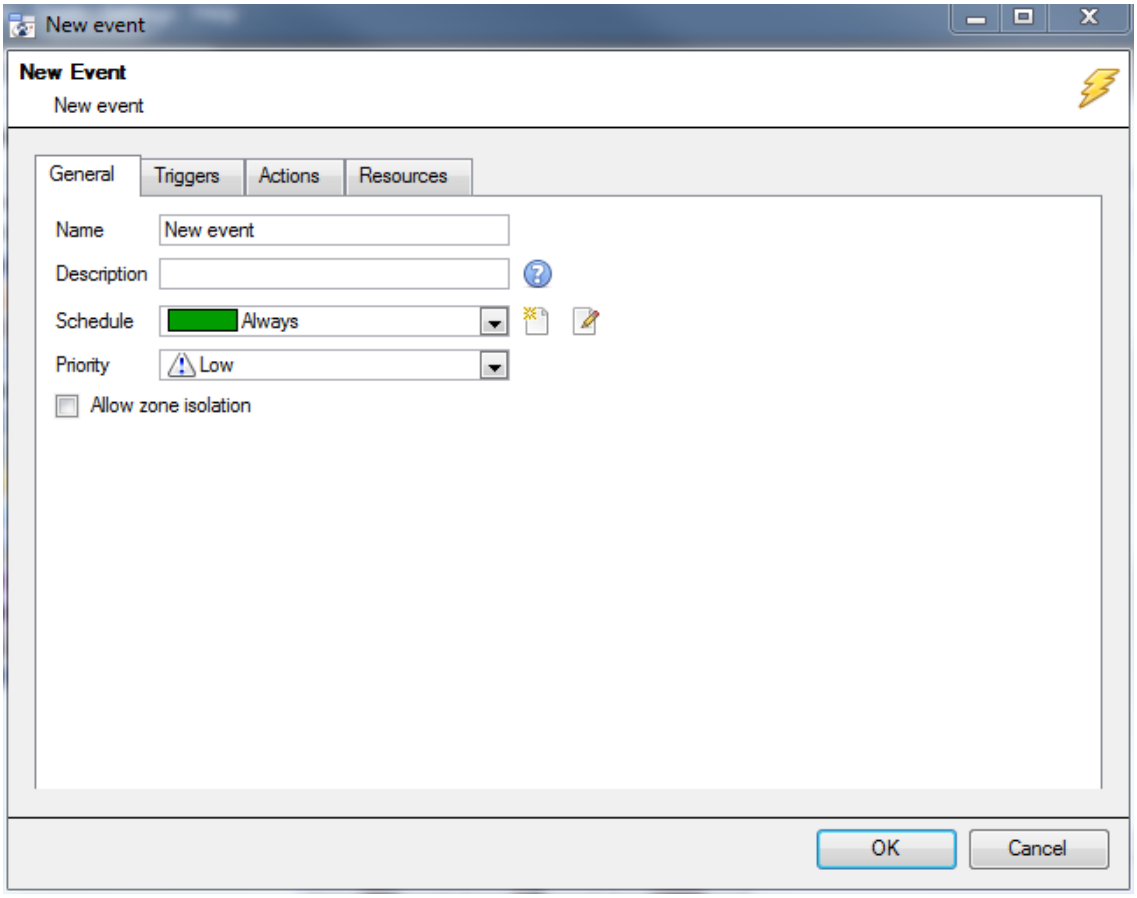
The Events panel will appear on the right. To add, edit, or remove Events in the list use one of the 

buttons at the bottom of the panel.

- The Events Window

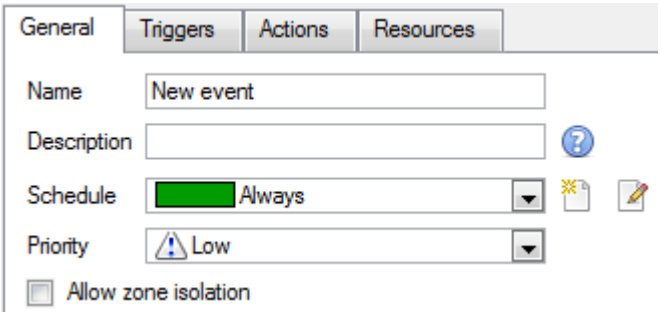


To enter the events window either click on ***New*** or ***Edit***, as described above. Or use the right-click menu in the Events Panel. Clicking on white space will give the option to create a new Event. Right-clicking on an existing event will present a dropdown menu, with the options shown in the image on the left.



The Events Addition Window

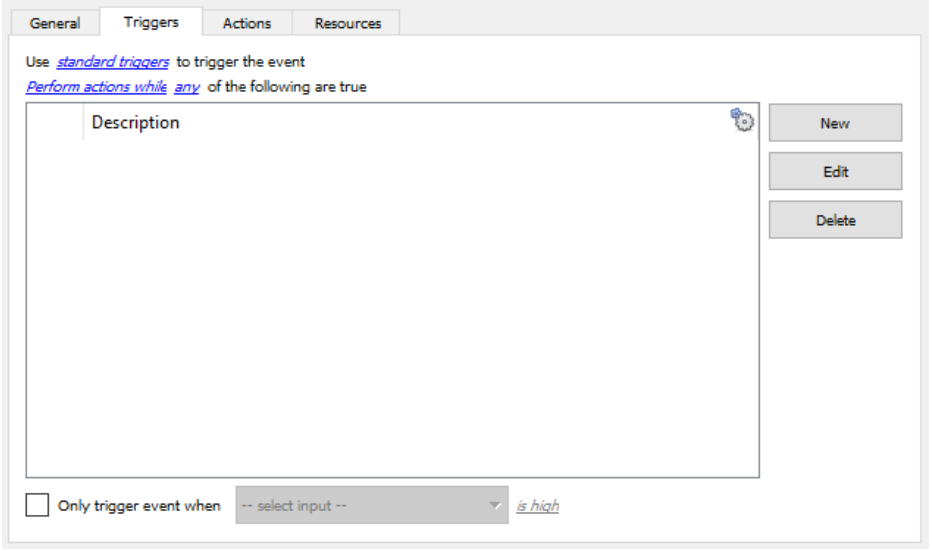
d. General Settings Tab



Name	This is a descriptive name for the event, which makes 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 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** the triggers are set. 2. The format for adding the variable is: `Descriptive Name: $Variable_Name` 3. Multiple variables may be added.
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).
Allow Zone Isolation	Check this to give the operator the option to disable this event alarm for a short period. This is useful in cases where there are repeat false alarms. This doesn't disable the event. It prevents the alarm from popping up on the operator's workstation, or alarm queue.

e. Triggers Tab



As discussed above, a trigger is what initiates an event. There are three types of triggers:

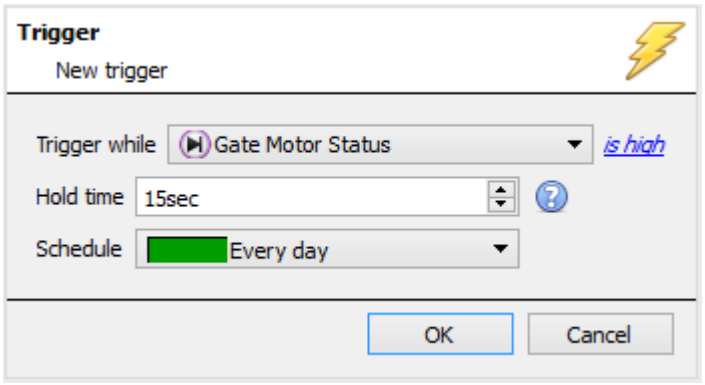
1. Standard triggers.
2. Trigger templates.
3. Integrated device triggers.

Choose between these options by clicking on the blue hyperlinked text.

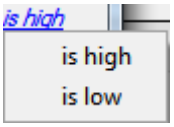
Standard Triggers

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 dropdown menu from which to select the relevant triggers.



The hyperlink to the right of the trigger, will provide 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. (See table directly below, for a graphic representation).

Schedule defines when this specific Trigger is active within this specific Event.

Hold Time

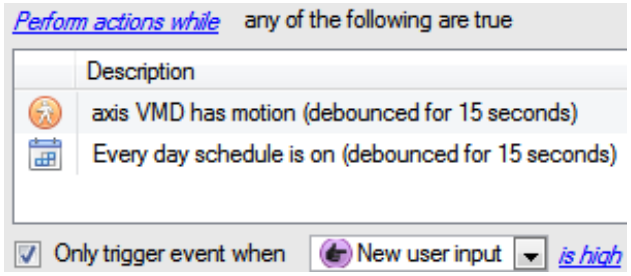
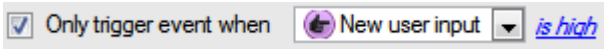
VMD level: _____| _____|____| |_____

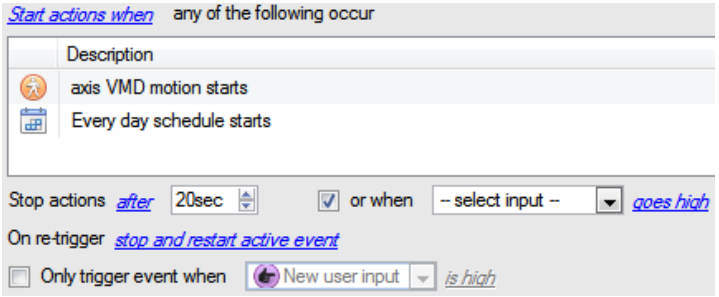
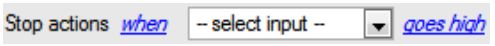
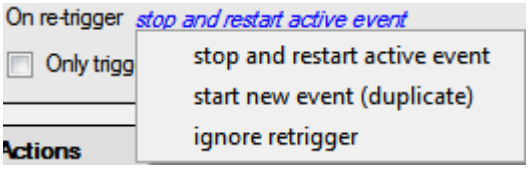
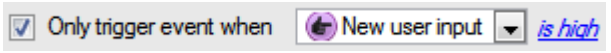
Event: _____| xxxxxx|_____

xxxxxx is the hold time.
One can see how the little dip (where the trigger is inactive) in the middle is filtered out by the hold time. This creates a continuous event.

When and While

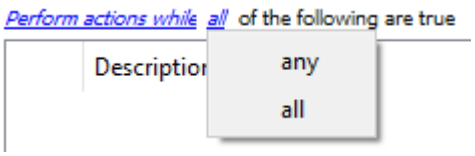
Standard Triggers can either trigger ***when*** or ***while*** a specific variable is true. ***When*** events are more complex, as they need to specify when the event will end; ***While*** events are simpler because they automatically end when the trigger variable ends.

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 setup.

Start Actions When	
Under *Start actions when* a user can define multiple conditions that must be met for an event to trigger. This is useful to prevent an event from ending 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. One may 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 one does not wish to have a timer, but still want 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, one has three options.  • Only Trigger an Event When This defines an absolute parameter, without this trigger the event will not occur. 

Any and All

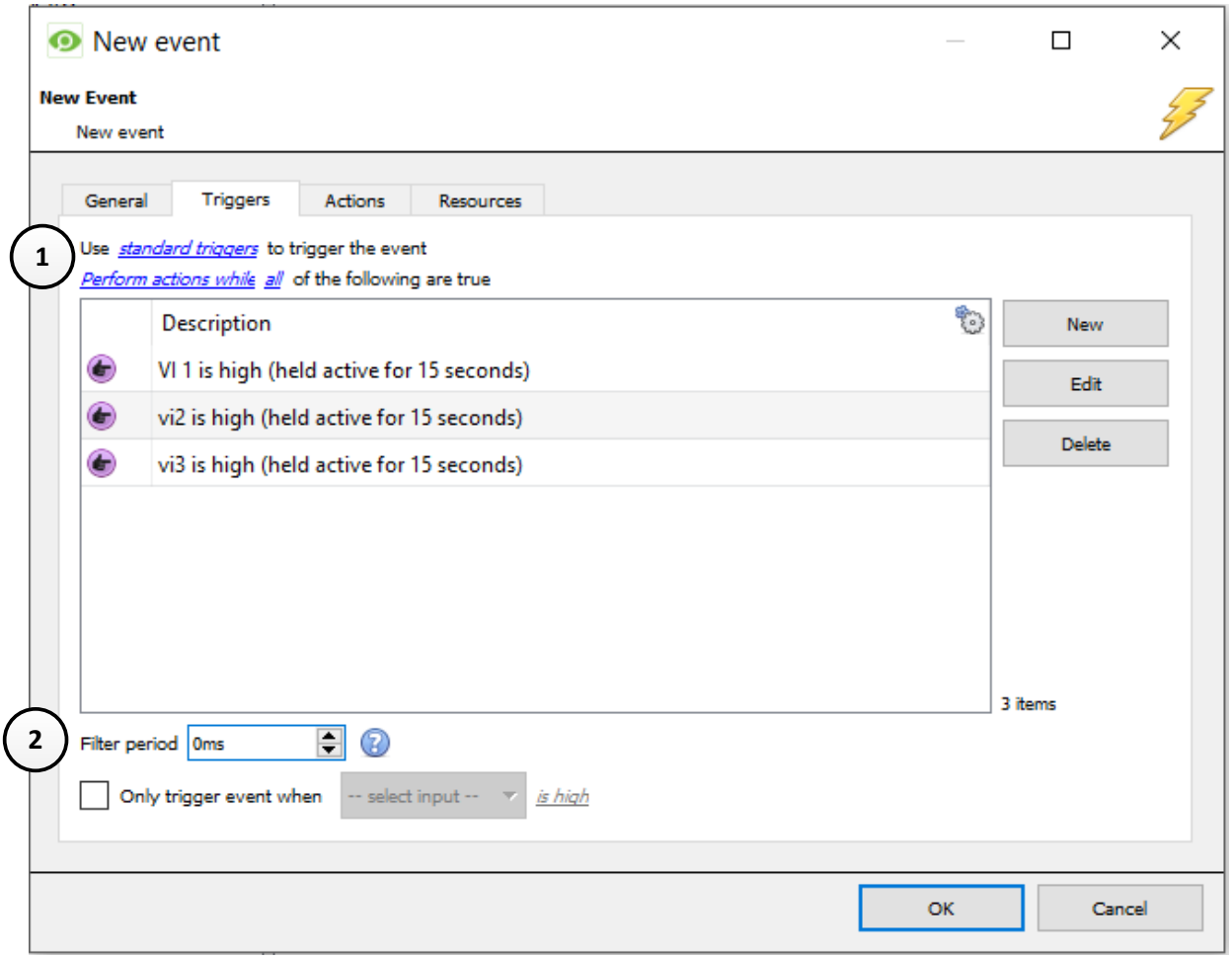
Clicking on the blue hyperlink *any* of the following are true, lets one choose between ***any*** and ***all***.



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).

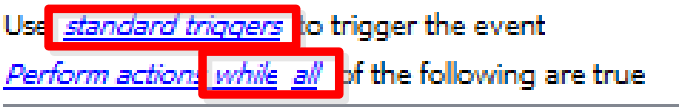
Filter Period

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.



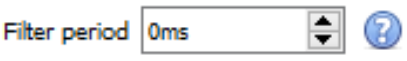
1

- Set the event to use **Standard triggers**.
- Set the event to Perform actions **while all** of the following are true.

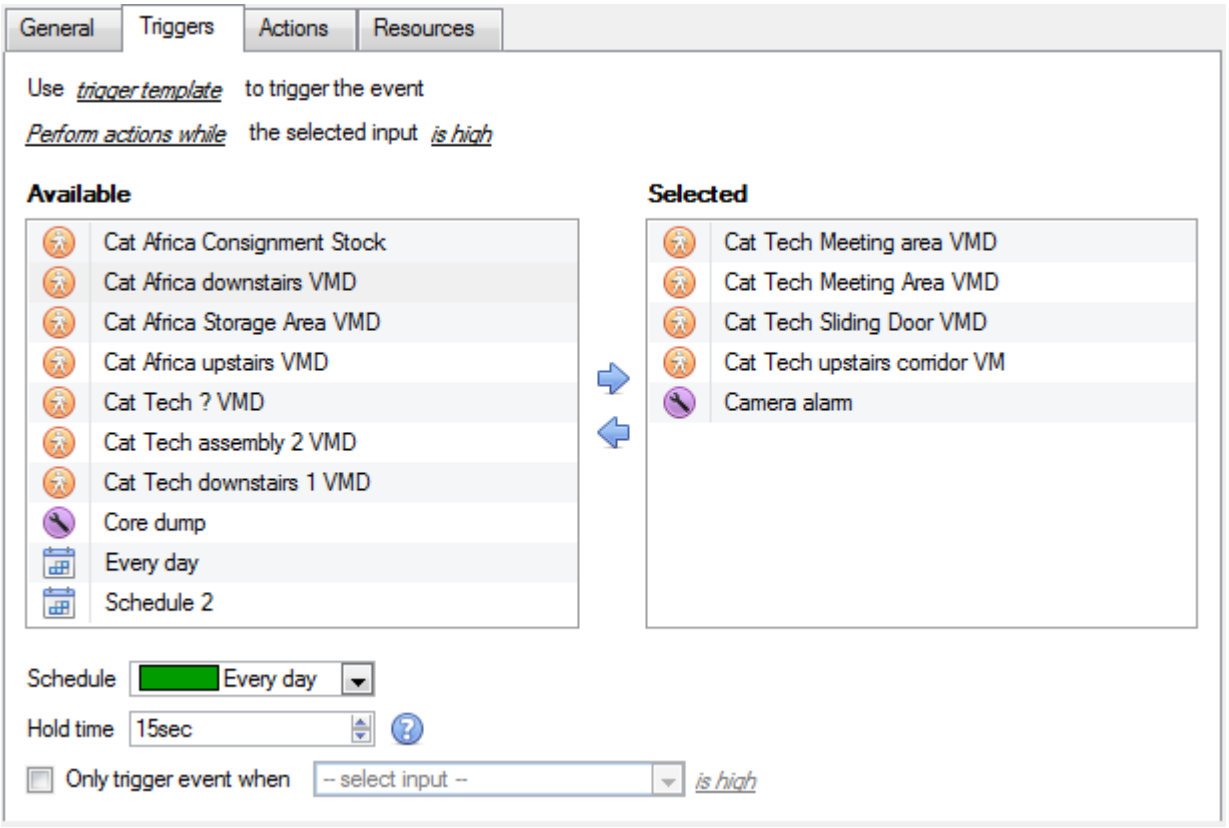


2

- Set the filter period.
- Click the  a description of the filter period.



- Trigger Template



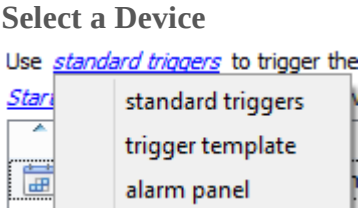
A trigger template allows one to add multiple triggers simultaneously to a single event. All **available** triggers will be in the left-hand column, and all triggers that will be used in the event in the right-hand column. To move triggers back and forth select the desired triggers and click on the  icon that represents the direction to send the trigger.

Note: There are two important things to remember when using a trigger template.

1. It is useful in relation to the **Record Trigger Cameras** option (dealt with in the Actions section, Actions).
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 in the **Error! Reference source not found.**, dealt with above.)

- 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.

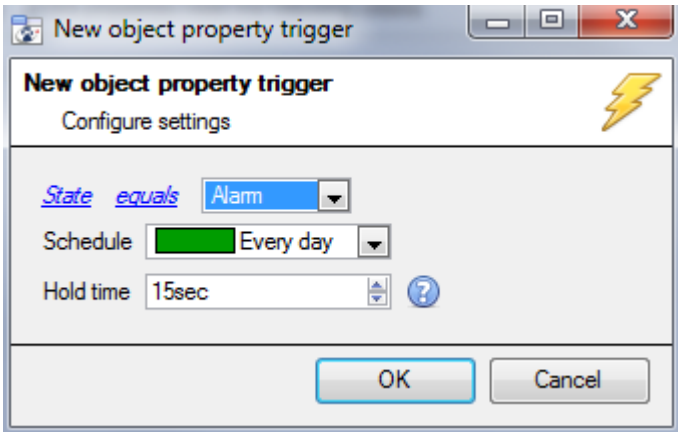


Integrated devices are also viable Event Triggers. This means that any integrated device may be used to trigger a **CathexisVision** Event.

Select a specific integrated device. In the image to the left, there is an alarm panel, which can be used to trigger an event.

Select a Device Parameter

Clicking on Trigger using *any device event* will provide a full list of the integrated devices own objects that one may use as trigger bases. Once one is selected, add a new trigger, by clicking on New.

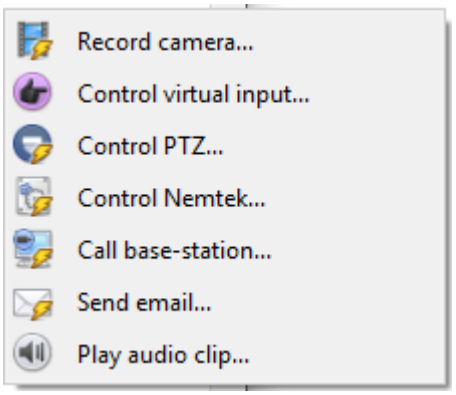


Clicking new will display all the options that the Object provides as triggers.

For example:
If State equals **Alarm** is selected**,** and any partition above is selected:

The event will trigger when any of the Caddx Zones alarm.

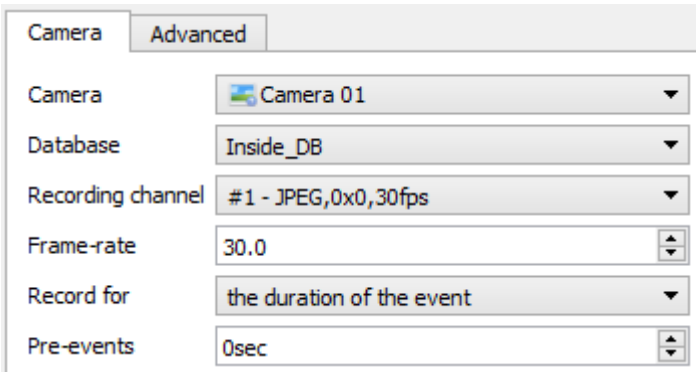
f. Actions Tab

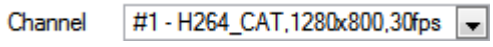
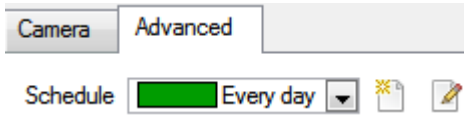


To add an action, click on the New button, to edit an action click on Edit.

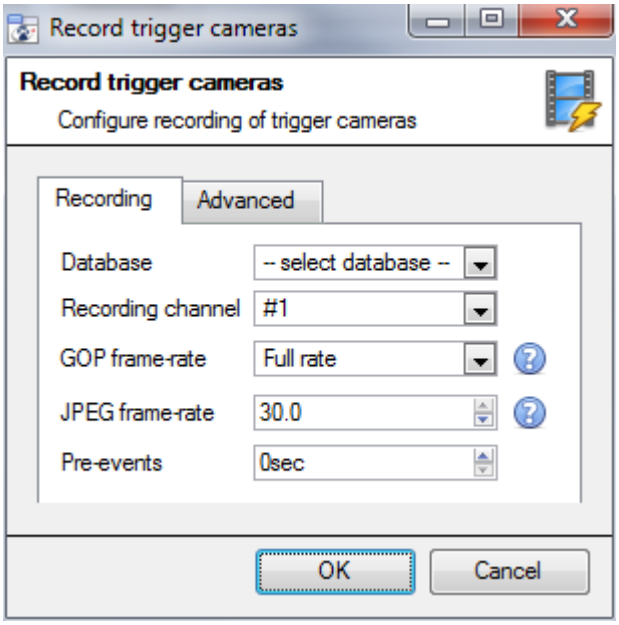
At present, the actions seen to the left are the available actions, and they will be dealt with below.

Record Camera



	Select a preconfigured database to 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 frame rate required 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: For this, setup 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 will be active **within** this event. This schedule does not impact on anything beyond this specific setting.

- Record Trigger Cameras



If *integrated device* or a *trigger template* is chosen, in the Triggers Tab (above) one may 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.

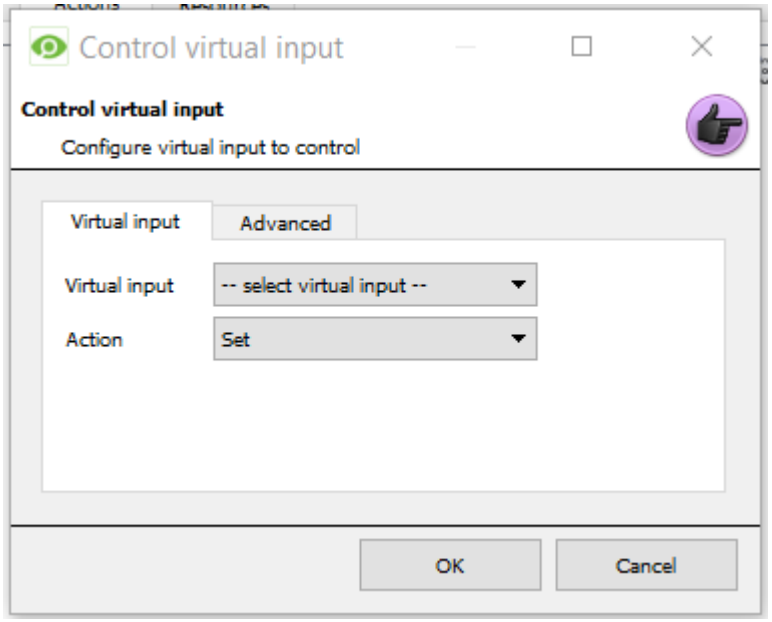
Database is the database the cameras will record to.
Recording Channel is the default channel that will be recorded from the camera. (make sure that all selected trigger cameras have the same channel set for recording.)
GOP Frame-rate is the frame rate to record GOP based video compression streams, such 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, one will effectively clone this event to another database. This is useful, to clone an event to, say, a Network Attached Storage.

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.

- ***Virtual Input tab***

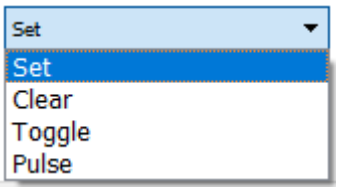


Select the Virtual input to be controlled as the event action.

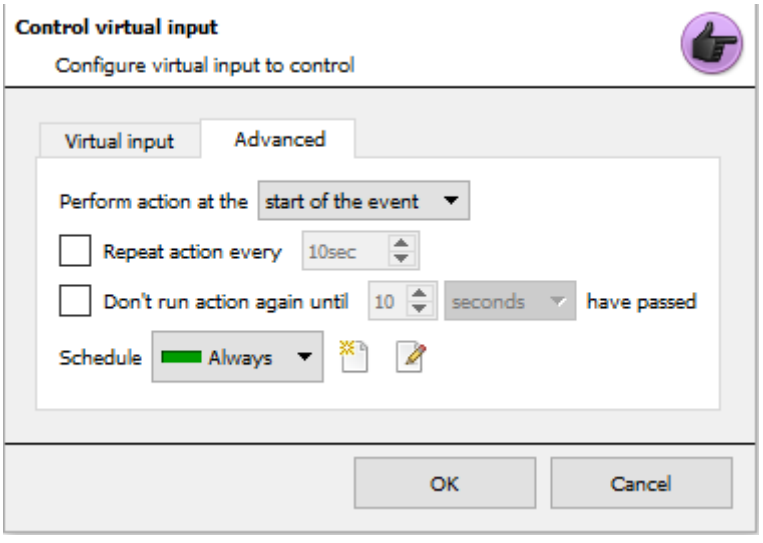
Note: Virtual inputs are configured in **Setup Tab → Configure Servers → Virtual inputs.**

Select which **Action** to control the virtual input with.

Inputs may be:



- ***Advanced Tab***



Select whether to **Perform action at the** beginning, or the end of the event.

Repeat Action Every

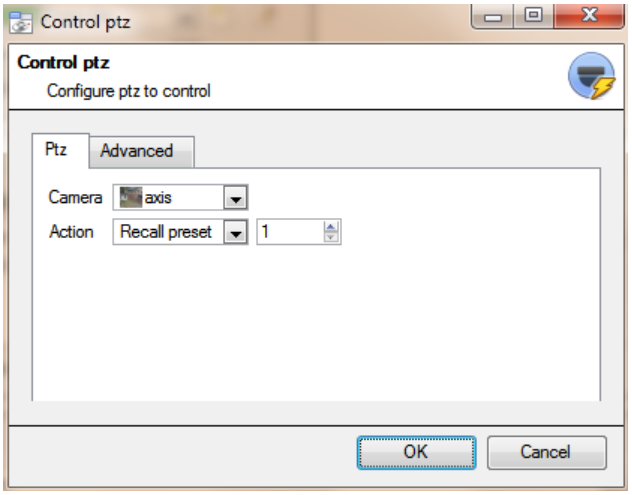
Check this box to define how often the action should occur during an event.

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.

Control PTZ



Camera is the camera whose PTZ the action will control.

Action

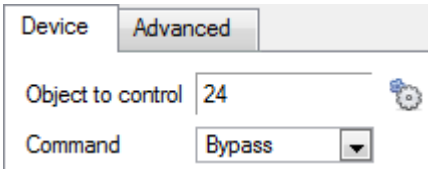
Recall preset will send the PTZ to a preconfigured position.

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.

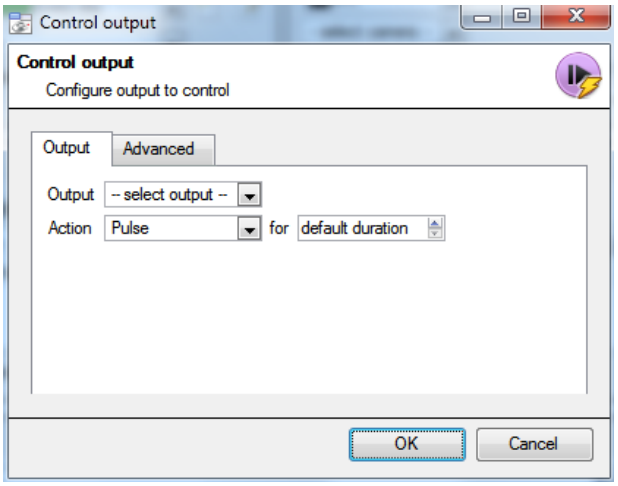
Control Integrated Device



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…).

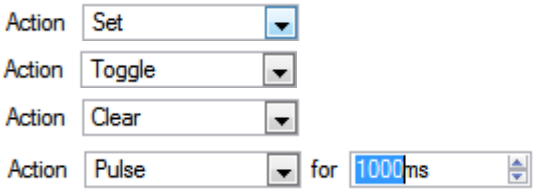
For Advance tab information see the Control Output, below.

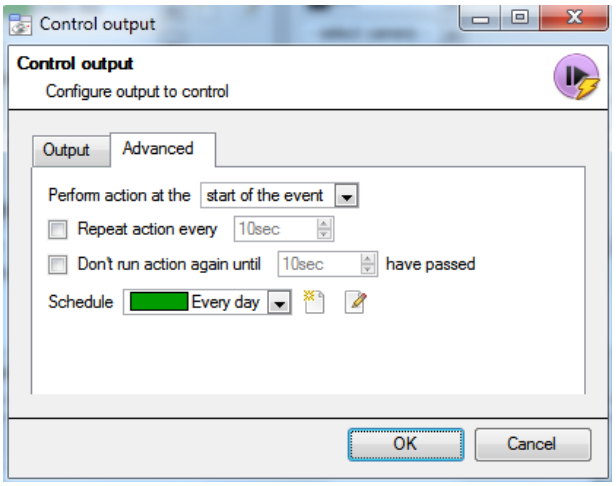
Control Output



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 should occur during an event

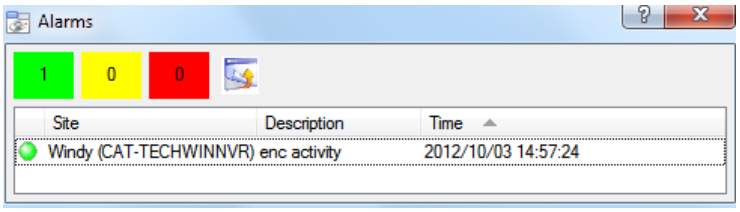
Note: This action, logically, is not available under *Perform action at the end of the event*

Don't run action again… offers 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.

Call a Base Station

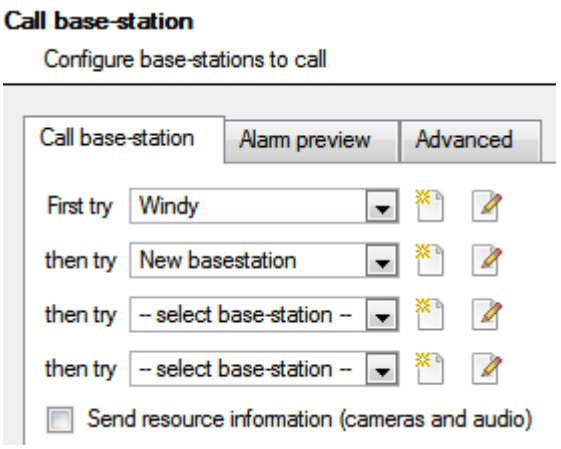
This will define which Base Station is 'called' when an event triggers. It will send an alarm pop-up box like this:



to the base station chosen.

- 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.

- ***Call Base Station Tab***

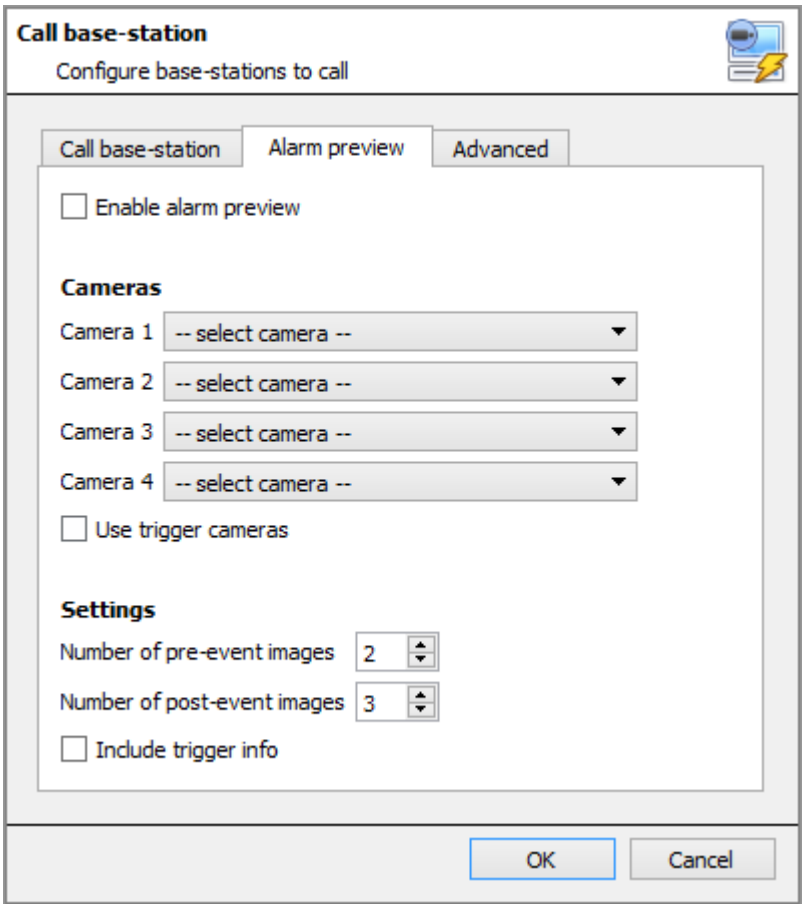


First Try: Select, from the drop-down menu, the primary base station to send an alarm to.

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

- ***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 enables the alarm preview

Under **Cameras** choose predefined cameras to send with the alarm preview.

Under **Settings** define the number of pre-, and post-, event images to send along with the alarm

Include trigger info will include trigger information if using a third party system as an event trigger

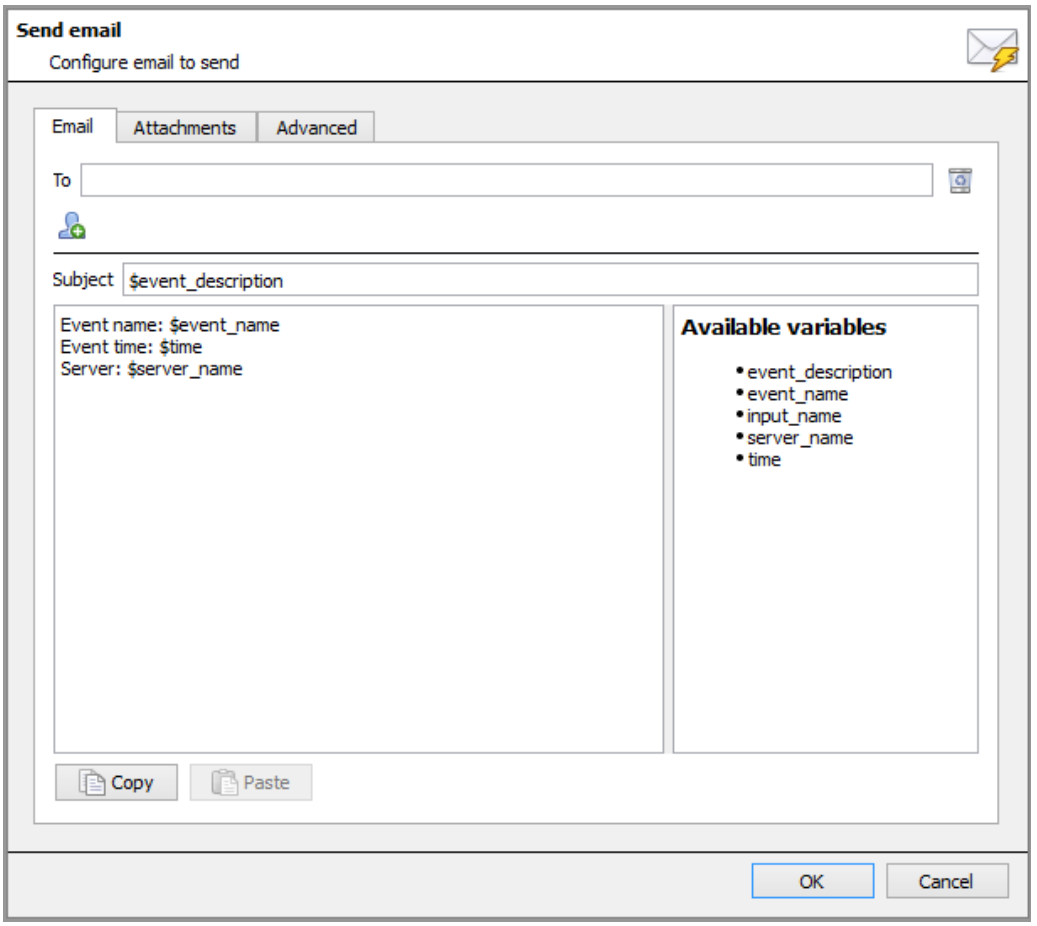
Advanced Tab

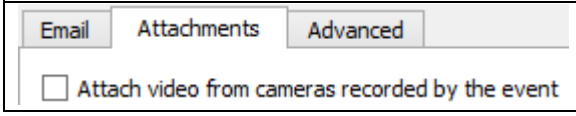
The advanced options are identical to those discussed under Control Output.

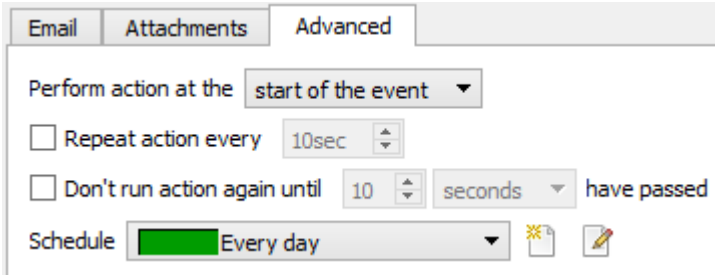
Send Email

The initial email setup must be done under **Setup Tab → Configure Servers → General Site Setup → Email tab**.

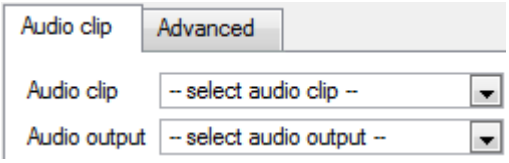
However, the options of recipient, and the information that will be sent in the email, are set here.



Set the Recipient	Add an email address in the *To* field. To add another recipient, click on the  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 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 and the email action takes place, once the event has started. A schedule for the event may also be set.

Play Audio Clip



Audio Clip is the actual audio file one may play as an action. The sounds are stored in the installation folder under \sounds.
Audio Output is the audio device that will output the sound.

Advanced Tab
The advanced options are identical to those discussed under Control Output.

g. Resources Tab

There are two scenarios in which the resources set here will be sent:

1. Gateway

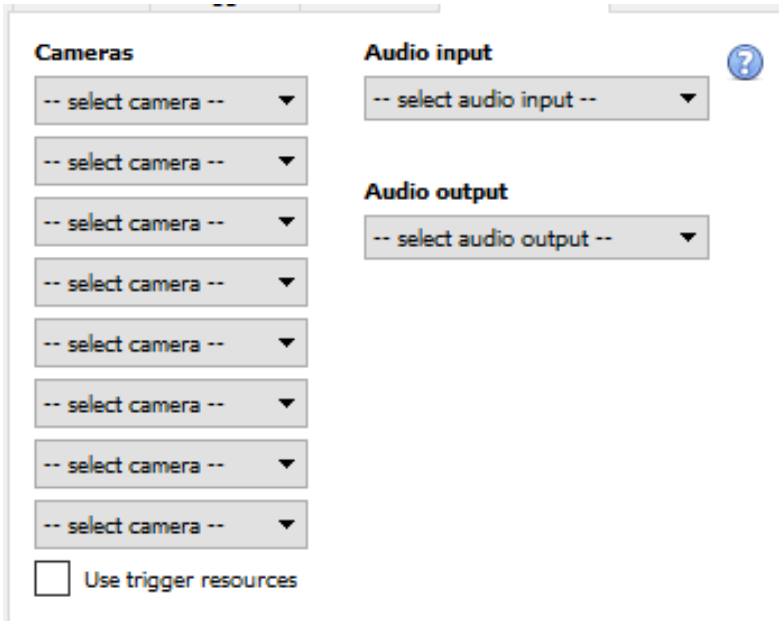
When a user responds to an alarm in a gateway the system will show the cameras and start the audio listed in the resources.

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 .

Resources Tab



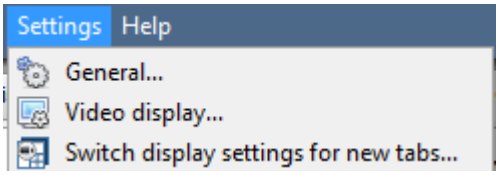
The user can send up to 8 cameras, an audio output, and an audio input.

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.

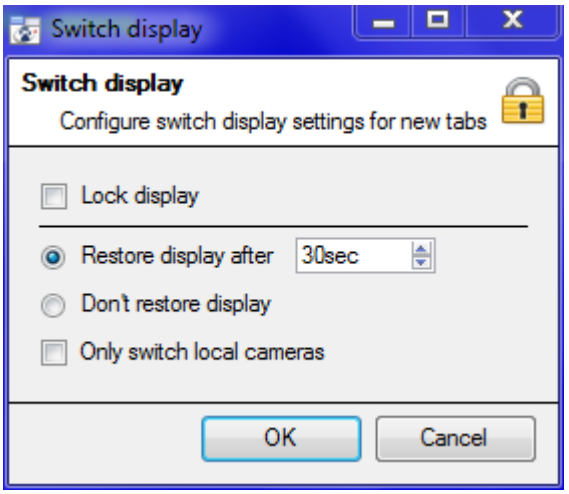
Click for more information on when the resources set here will be sent.

- Default Switch Display Settings



When sending Resources, define whether or the Operator's cameras tab will 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 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.

Triggering Events with Camera Tamper

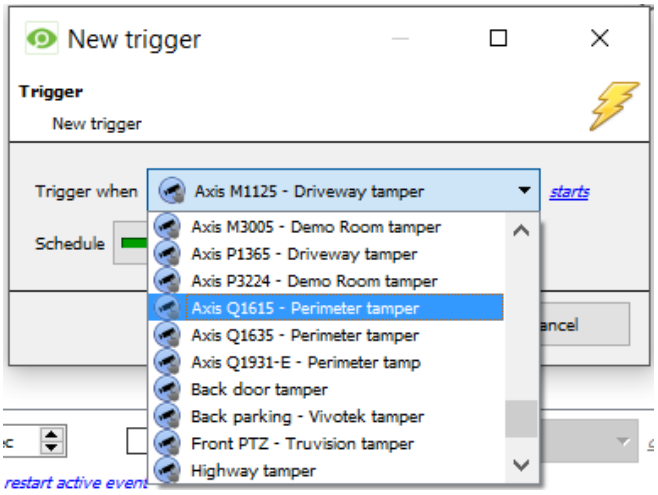
If camera tamper detection is added to one/multiple cameras, one may want to create events which will be triggered by a camera tamper.

Note: One must have already added tamper detection to cameras in order to trigger events using tamper.

- ***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*, and then add at least one trigger to the event.

1. 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.

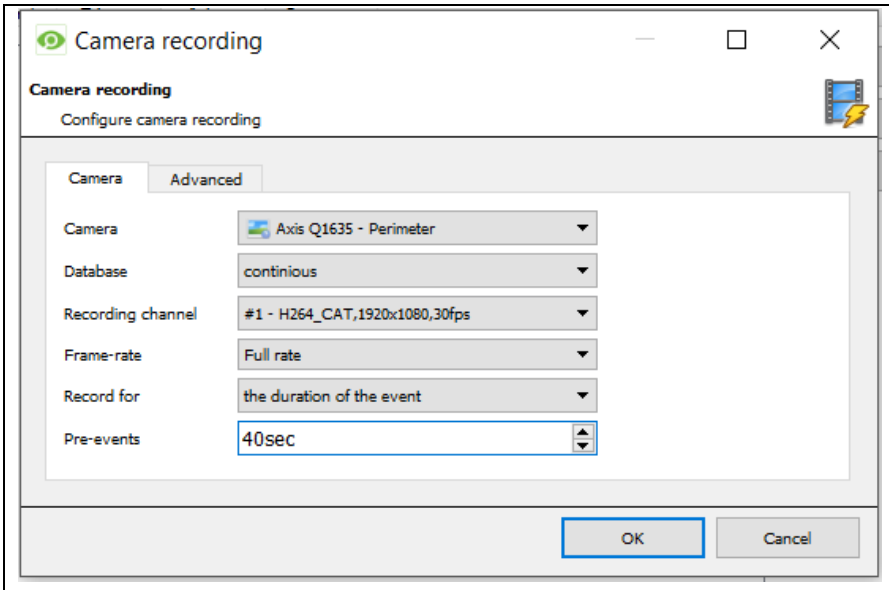
Click **OK**.

2. Stop Event after 20 Seconds

Stop actions *after* 20sec	Once back in the New Event window, set the event to stop after 20 seconds.

3. Record Camera

Recording tamper events is a priority. 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 Record for the duration of the event.

Set the pre-event to 40sec in order to capture events leading up to the tamper.

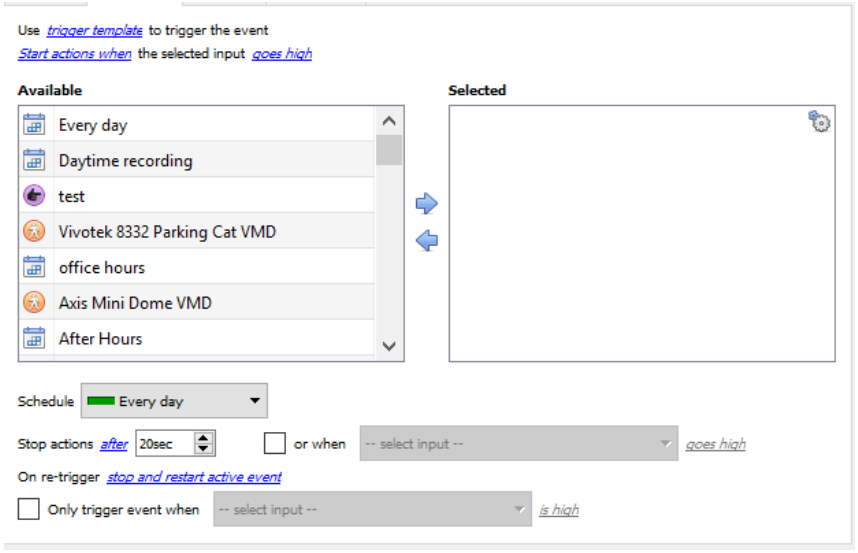
- ***Trigger Event from Multiple Camera Tampers***

To trigger an event using camera tampers from multiple cameras, then create an event using the following parameters:

Use *trigger template* to trigger the event
Start actions when the selected input *goes high*

Then add a trigger.

1. Select Camera Tampers to Trigger Event

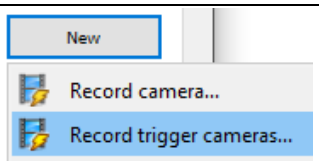


From the list of available cameras, select all **cameras** that, when tampered with, will trigger the event. Then click the

Set the **Schedule**.

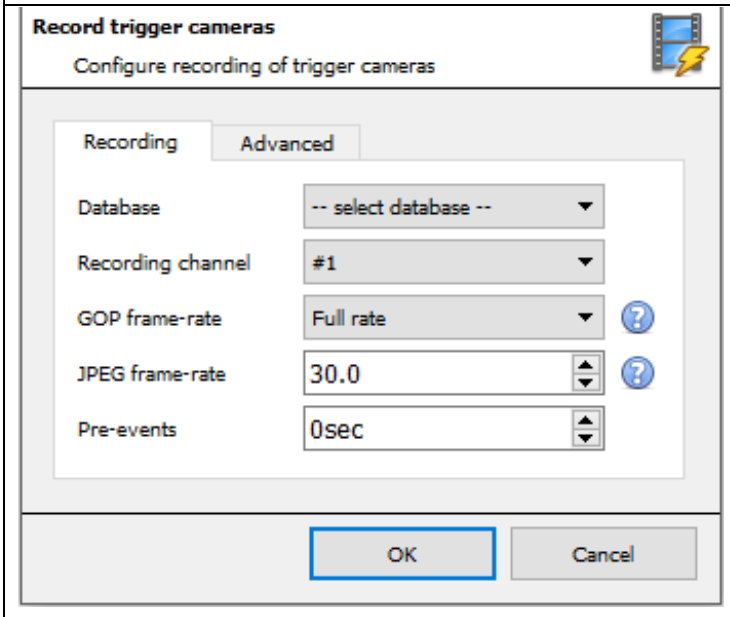
Set the event to stop after 20sec.

2. 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 40sec 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.

10 Monitors

The Monitors option will provide 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.

a. General Settings

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. (This is easy to remember. Just think: "The license needs to be on the server the monitor is being added to".)

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 the icon.

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:

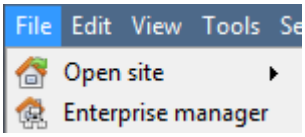
- C:\Users\User_Name\AppData\Roaming\Microsoft\Windows\StartMenu\Programs\Startup . (Replace Username with the name of the user profile that the software will be running on.)
- One may also navigate straight to the Startup folder of the currently logged in Windows User by copy-pasting the following into the Windows Explorer Navigation bar: %appdata%\Microsoft\Windows\Start Menu\Programs\Startup

- Resources Site

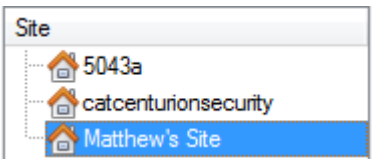
The Monitors Tab will be automatically present in **CathexisVision** on the Server which monitors have been added to. To have the Monitors Tab on a Base Station, make the relevant Site a Resources Site. This must be done in the Enterprise Manager of the Base Station the Monitors Tab is being added to.

- Create a Resources Site

Note: this needs to be done on the Base Station which the Monitors Tab is on.

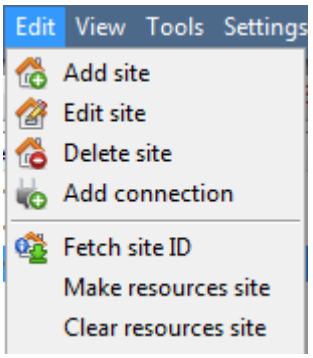


Open the Enterprise Manager.



Select the Site to edit.

Here, the Site being 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 **resource site**, follow the same procedure, but click on **Clear Resource Site**.

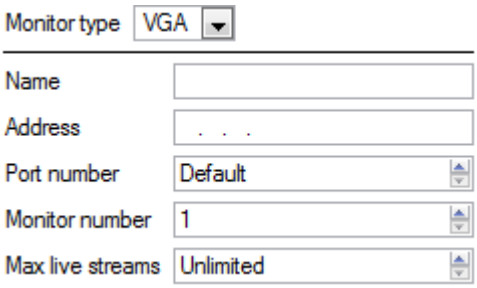
b. Adding a Monitor

- Monitor type

There are two types of Monitor that may be added to a system. A VGA monitor and an XP switcher monitor.

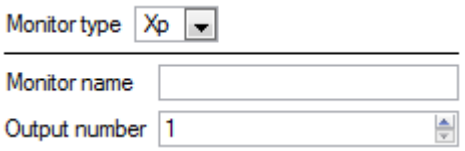
- VGA

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's necessary to forward specific ports.
Monitor Number corresponds to the physical monitor 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.)

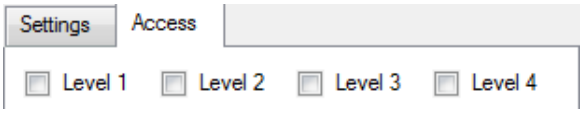
- XP



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.

c. Access



Under the Access Tab, define which user Access Levels have rights to make changes to this Monitor, via the Monitors Tab. (Discussed Below.)

11 Access Rights

Setup tab → Configure Servers → expand Your_Server_Name → Access Rights.
Under **Access Rights**, setup which Site Resources are available to which access levels. Each user was assigned an access level, when he/she was 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** .

Tabs

Select the resource from the list on the left, and check the level one wishes to have access to this resource.

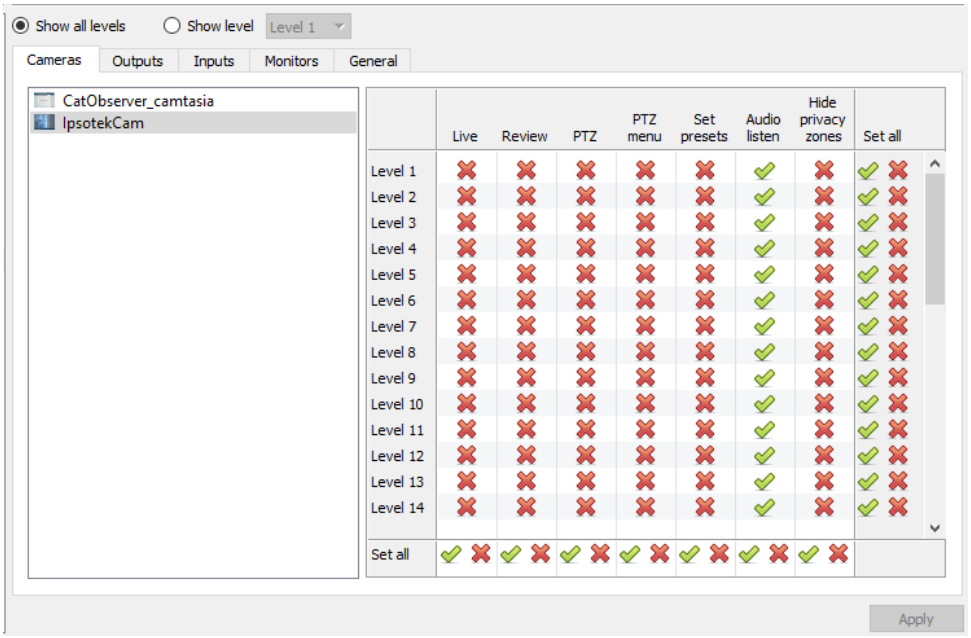
The tabs (**Cameras**, **Outputs**, **Monitors**, **General**) represent classes of resource whose access level may be controlled. The one selected, will have all the resources that fall into this class displayed in the left-hand panel. In the examples below, the **Cameras** tab is selected and the settings refer to camera resources. However, the process is identical when editing **Outputs**, **Inputs**, **Monitors,** and **General.**

- ***Cameras Tab***

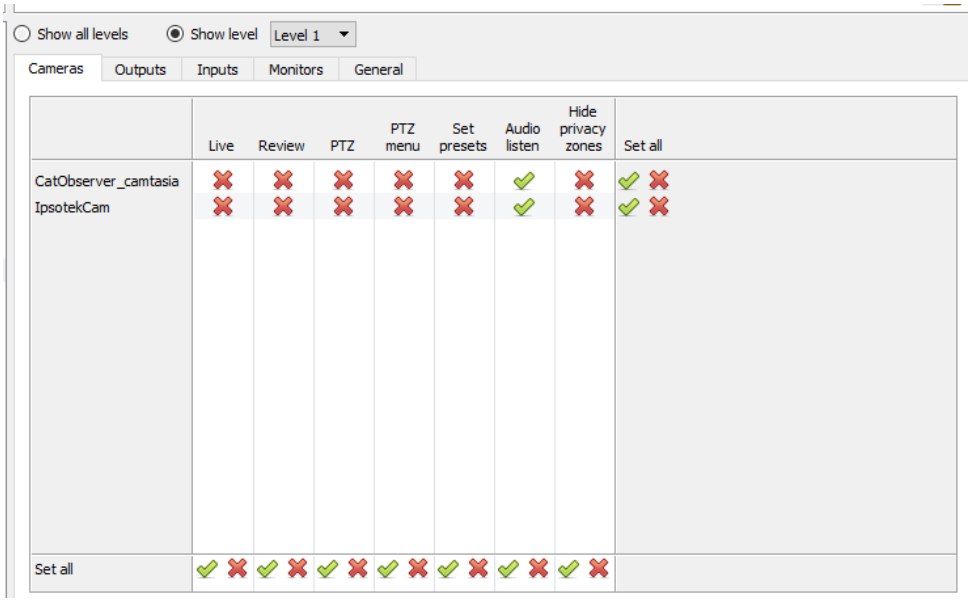
The cameras tab involves setting access rights for user levels for specific cameras. Select the relevant cameras on the left and then set the desired access right on the right by clicking to toggle between and .

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 dropdown 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.)

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 will give this level access to all settings; selecting will give this level access to none.

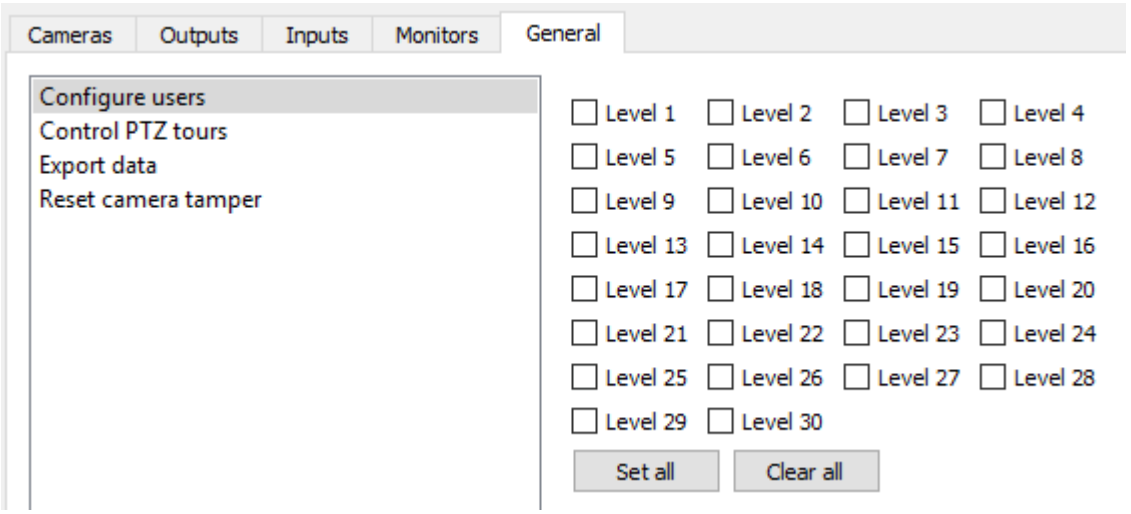
Note: A means that this level has access; a means that this right has been denied to this level. Left-click on the tick/cross to change its designation.

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.	Independent audio channels.
Reviewing from the camera tab.	Archived video.
Reviewing from the database tab (both video and integration databases).	Connecting to a 2016.2 server using a 2015/2016.1 viewer.
Viewing video when handling an alarm in the Alarm Management Gateway.	Connecting to a 2016.1 server using a 2016.2 viewer.

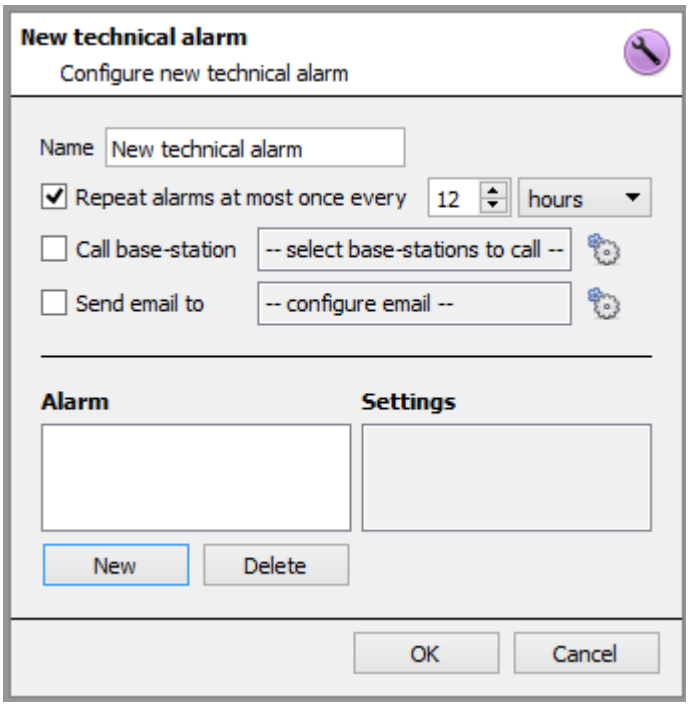
- ***General Tab***



In the General tab, one may 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.

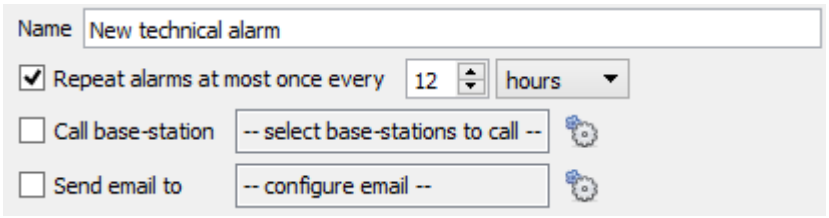
12 Technical Alarms



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 one may setup 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**.

a. General Settings



Give the Alarm a descriptive **name.**

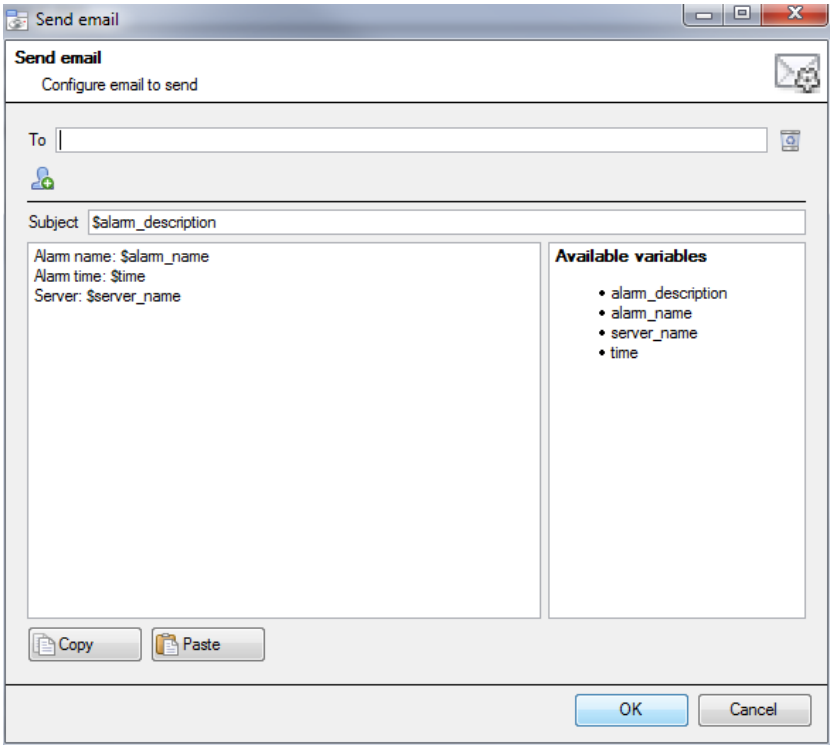
Set a global maximum amount of alarm repeats.

Select whether the alarms should be sent via email or to a Base-Station.

- Email Configuration

The initial email setup.

However, the options of recipient, and the information that will be sent in the email, are set here.

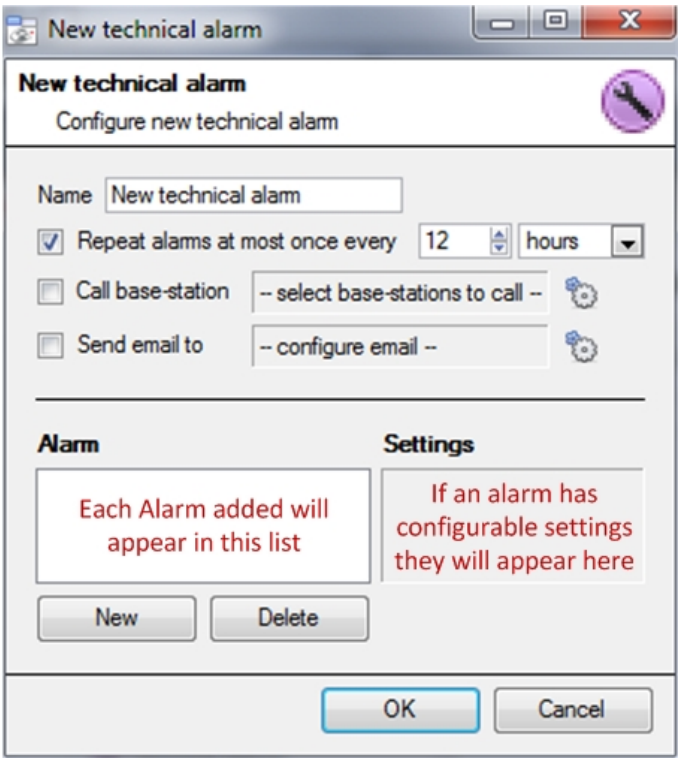


Set the Recipient	Add an email address in the ***To*** field. To add another recipient, click on the  icon, this will add another *To* field.
Set the Variable	There is a list of **Available Variables** in the Send Email window. These define what information is sent in the email. To add a variable, add 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	Copy/paste variable settings from one Technical Alarm to another. This is very handy when one is doing a batch of Technical alarms, across multiple servers.

b. Add/Edit a Technical Alarm

To add a technical alarm, click on 

, in the Technical Alarms panel. This will bring up the following dialogue:



Name

Give the Technical alarm a descriptive name.

Repeat alarm at most…

This setting sets a 'global' repeat setting, which will define how often individual alarms may repeat.

Call Base Station

This is if the alarms should be sent to a Base Station. Click on  to set the Base Station/s.

Base Station setup is dealt with under section **Error! Reference source not found. Error! Reference source not found.**.

Send Email

There is 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 section **Error! Reference source not found. Error! Reference source not found.**.

- Available Alarms

Clicking **New**, in the New Technical Alarm dialogue, will initiate a drop-down menu with the following possible 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) Configure: Here, set whether alarms trigger from one, or both options listed above. One may 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.[2]

[2] 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.
Meta-Database	Triggers when the meta-database (typically used in integrations) encounters a problem, such as running out of disk space.
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 for some reason isn't. Enabling this alarm will periodically check recordings for failure. Configure: All that needs to be set here is the cameras that are not required to trigger this alarm.
Recording Period	Will trigger when a database stops recording before its predefined period is complete. E.g. 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 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 is intended to test the system, to see if it will receive alarms.

- Important Note on Operating Systems

The technical alarms have different levels of integration with the different Operating Systems. The following is a table indicating the Operating Systems, and the technical alarms that are supported.

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[3]			

[3] Environment alarm only available on supported Cathexis hardware.

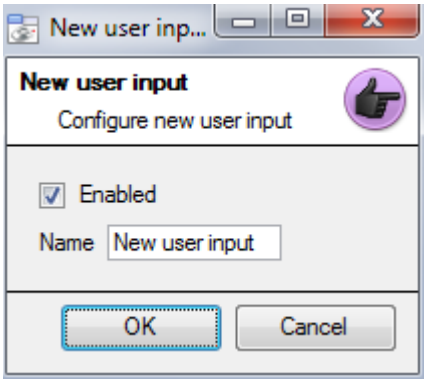
Failover	X	X	X
Frame Grabber		X	X
Gateway	X	X	X
Meta-db	X	X	X
Network I/O	X	X	X
Network Connectivity	X	X	X
Reboot	X	X	X
Recording Failure	X	X	X
Scheduled Archive	X	X	X
Software Failure	X	X	X

13 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.

a. Add a Virtual Input



To add the Virtual Input click New.

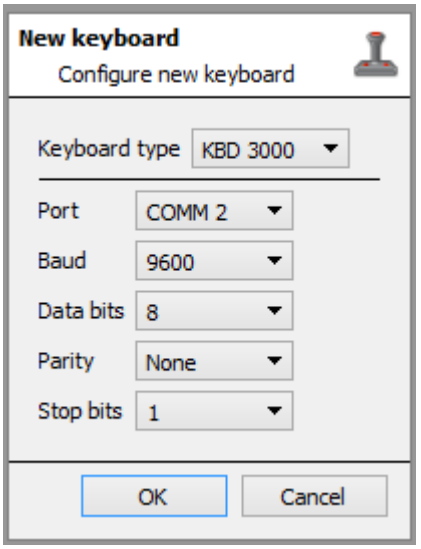
Give the input a descriptive **name.**

This Input works the same way as other triggers in an event, look to 9 Events for more information.

14 Keyboards

When adding a Keyboard to a unit there are two possible situations. One may either be 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.

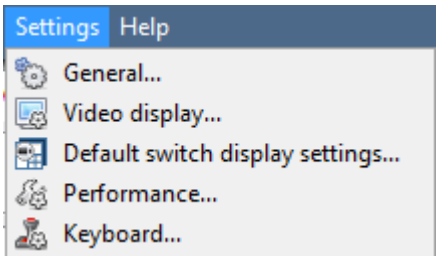
a. Recording Server



Adding a Keyboard to a Recording server is done on the server, and as such, access **Site→ Setup Tab → Configure Servers → Keyboard**.

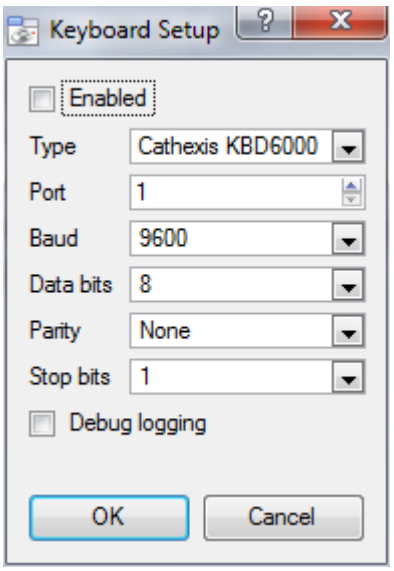
Simply choose the Keyboard type and enter the port number that corresponds to the port that the keyboard is plugged into.

b. Base Station



If adding a Keyboard to a base-station, be on that specific base station.

Go to the menu bar and select **Settings—>Keyboard**.



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.

Integration Devices General Settings

a. General Setup

Because there are many different integrated devices, and each device will have different options, this General Setup section is designed to introduce the Integration Panel, and the features that are common to all integrations.

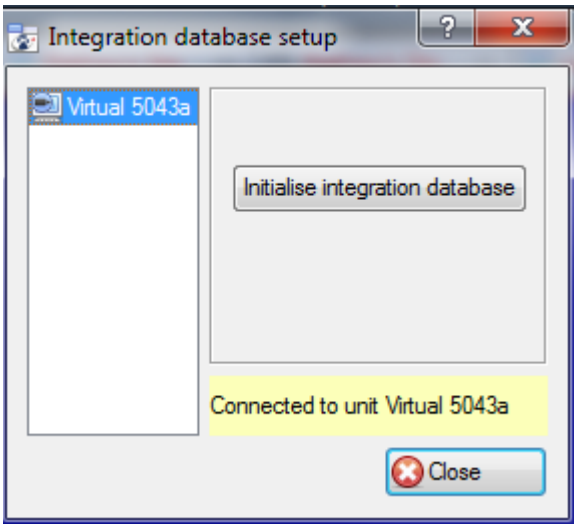
One major benefit of the Integration Devices panel is that it ***centralises all integrations to one point***. The addition, edition, and management of all integrations added to a server/Site is done from this one point.

- Integration Database Management

This is done outside of the **Setup Tab→ Configure Servers**. This is because integration databases are not specific to servers, but should be considered as Site resources. For this reason, add/edit integration databases via the Site Menu: Once logged into the Site, navigate to the Integration Database Manager via **Site—>Integration Database…**

- Initialise the Integration Database

This will add a broad database, within which all integrated device's databases will be added.

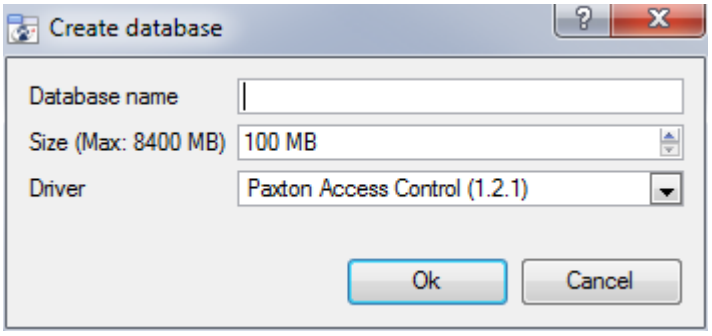


The first time an integration database is added, initialise this feature on the unit.

Select the unit to add the database to, from the list on the left, and click Initialise integration database. Choose which partition the database will be formed on, and select how much space it will take up.

- Add a New Devices Database

Right-click on the white space that was occupied by Initialise integration database before the database was initialised, and click on New.



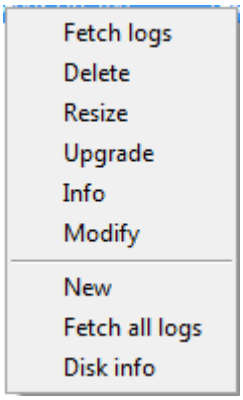
Give the database a descriptive **Database Name**.

Allocate a **Size** to the new device database.

Then choose the device **Driver** that the device will be using.

- Integration Database Procedures

Once at least one database has been added, one will see the following procedures through right-clicking on a database:

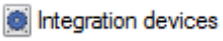


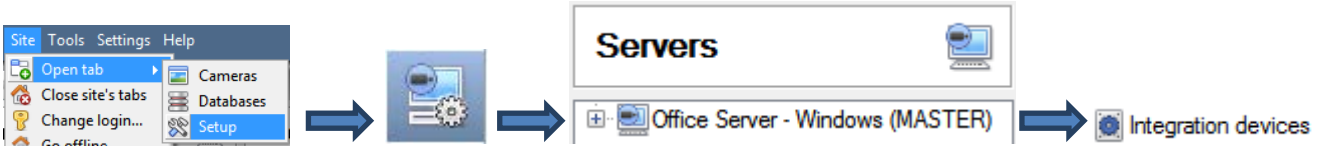
Fetch Logs will fetch the logs for the unit right-clicked on.
Delete will delete the database selected.
Resize allows resizing this database. There will be Min and Max options, which will either fill the database to the maximum, or the smallest, sizes allowed.
Upgrade upgrades the metadatabase.
Info provides a full list of all available information on the database.
Modify will simply allow renaming of the Database.
New will open the New Database Dialogue.
Fetch All Logs will pull a consolidated log for all integrations databases on this unit.
Disk Info will provide detailed information about the hard drive the database is on, as well as the Databases on it.

- Open the Integration Setup Panel

First, navigate to the Integration Setup Panel.

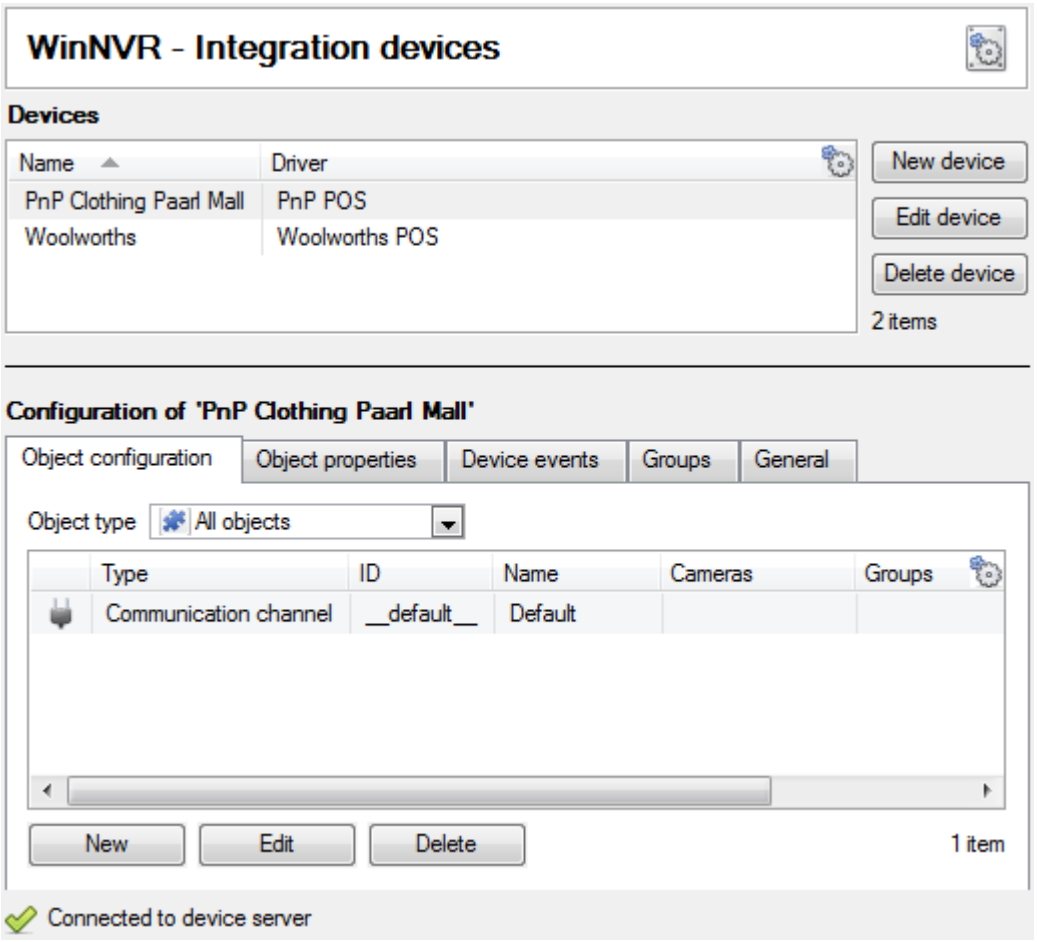
- Enter Configure Servers

Once in Configure servers, left-click on 



This will bring up the Integration Devices Panel on the right. This is the central point at which integrations are managed.

- The Integration Devices Panel

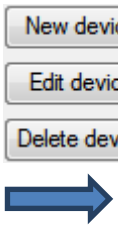


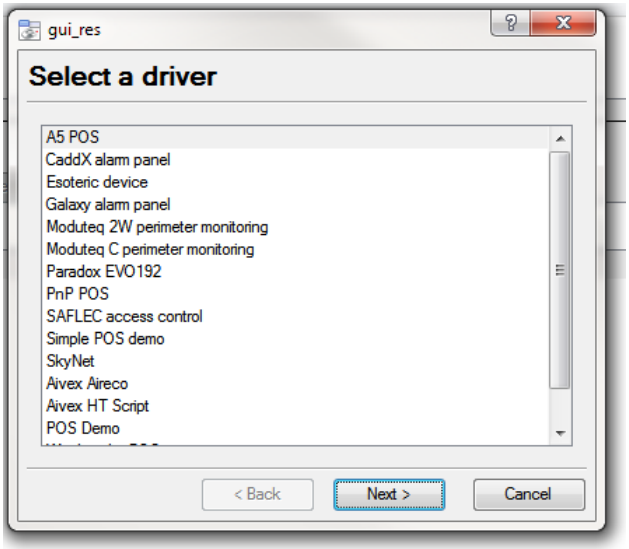
- Adding an Integrated Device

Adding an integrated device is incredibly simple.

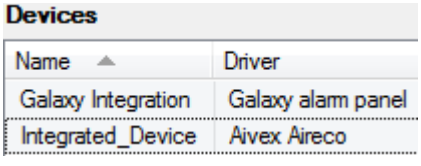
- Add the device

Click *New device*, and select the drivers for the device one wishes to add.





- Devices



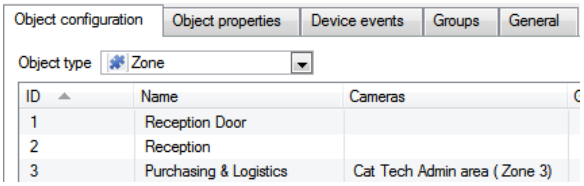
Once the device is added, it will show up in the **Devices** panel. Left-click on a specific device to access its Configuration Settings.

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 will be able to view the device's objects, and change settings.

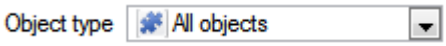
The Configuration section will be automatically populated with the information received from the device.

- ***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.

- ***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.

- ***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.

- ***Groups Tab***

Create groups of the same type of object. When creating a group, select the object type to be 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 useful in setting up Events as one can use an entire group as an Event Trigger.

- ***General Tab***

Offers general information, such as the meta-database that the integration is attached to.

One may also access the Integration Database Management dialogue from here, by clicking on

b. Important Considerations

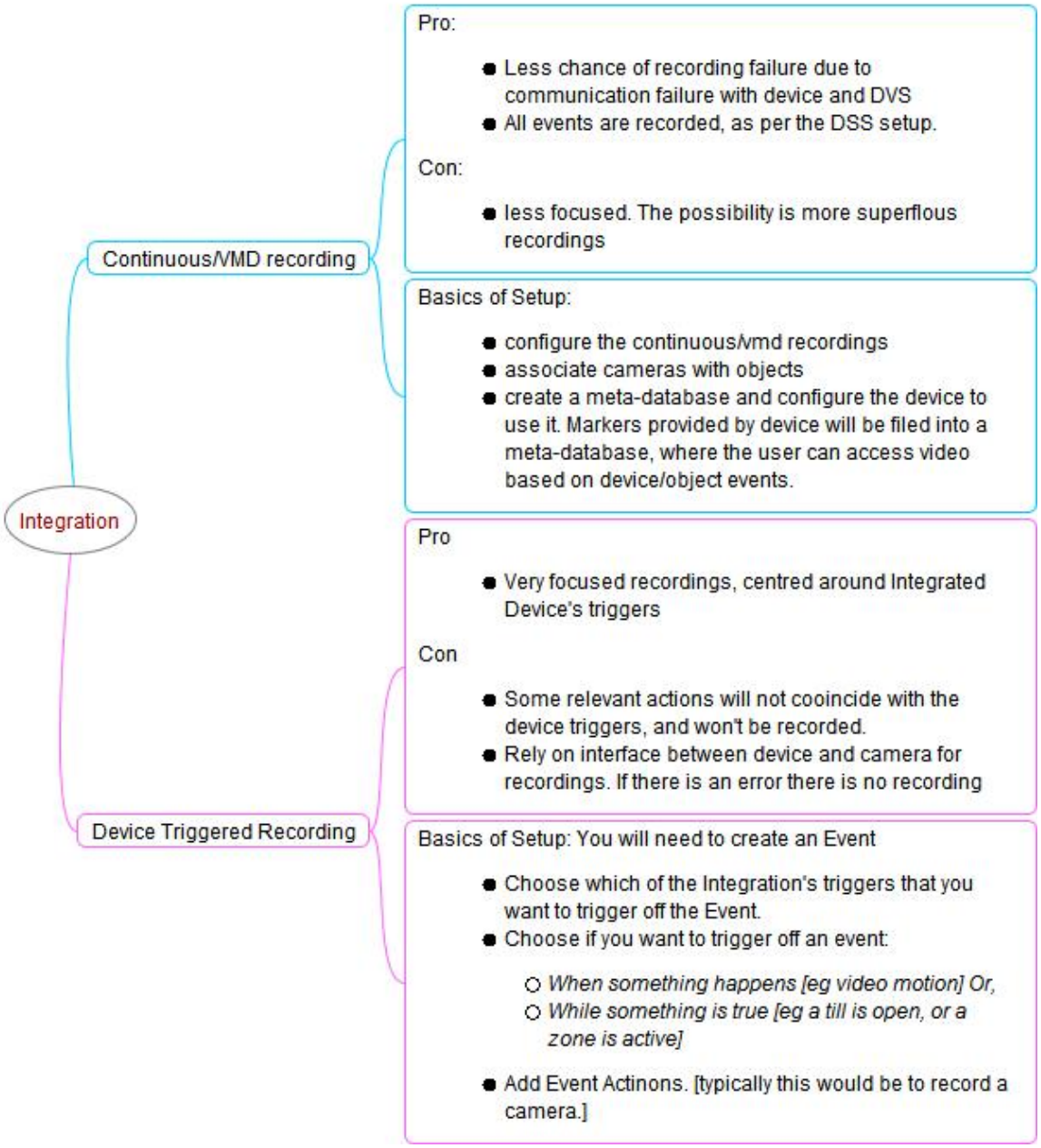
There are some things that need to take into consideration when adding an integrated device.

- Device Triggered Recordings; or Continuous Recording with Device Provided Markers

One of the first things to take into consideration when using an integrated device is how it will interact with the Surveillance System.

- Should the device itself 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:



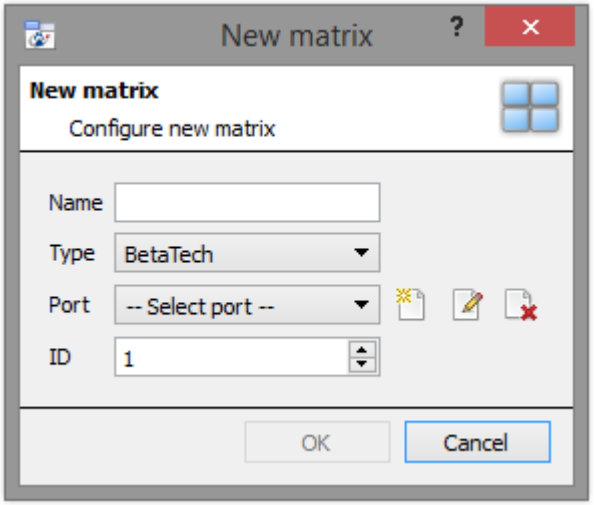
15 Analogue Matrix

CathexisVision has the ability to support an analogue matrix. Click on Analogue matrix to access the setup. This feature allows for hybrid solution between IP and analogue based security installations.

Note: An Analogue matrix would be used on existing analogue based Sites. So, an old analogue matrix controls or switches 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.

a. Add/Edit an Analogue Matrix

- New Matrix Dialogue



After clicking on NEW, the dialogue box will appear.

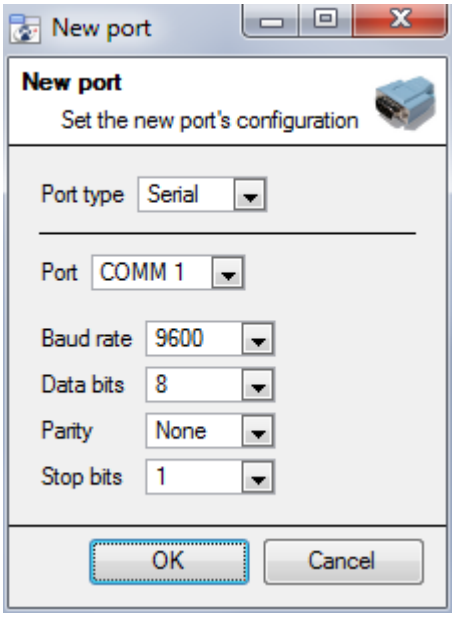
Give the matrix a descriptive **name**.

Select the **type** of matrix that will be used.

Select/Configure a **port** (dealt with below).

Set the **ID** of the matrix.

- Port Editing Dialogue



To add/edit a port, this menu will appear. To add a new port, click on the icon, to edit one click on the icon, and to delete the currently chosen one click on the 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.

Setup Tab: Resources

1 Resource Panel Configuration

The Resources Panel is the panel on the right-hand side of the Cameras Panel, in the Cameras Tab. It is a customisable panel of resources, which gives the user quick access to the resources available. The Resources Panel Setup is the means to configure the resources that users will see in the Resources Panel.

The Resources Panel should present all of a Site's resources in a manner that is suitable for operators on the Site. For example: List all cameras for the 1st floor of a building under a folder called "1st Floor cameras", or list all doorway cameras under their own folder, or create a folder per operator, and list resources relevant per operator.

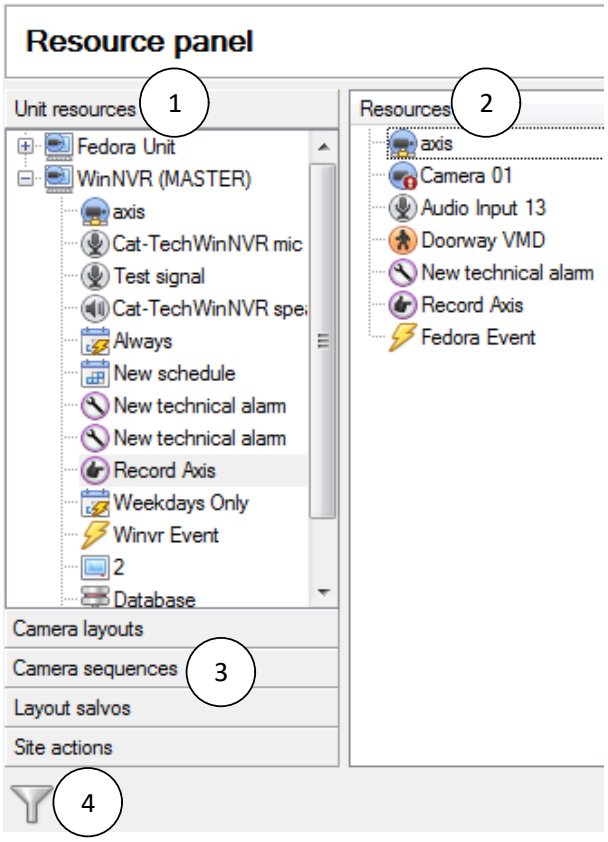
TIPS:

• ***Ensure that all of the resources are setup*** as required by the complete spectrum of users, because for most users this is the only point of access to the resources.

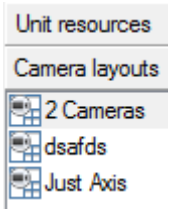
• ***Resources can be repeated in different folders***, so, for example, one could have folders defined by user names, and certain resources repeating across all of these user folders.

• Remove unused resources from the tab to reduce interface clutter.

a. Resource Panel Setup

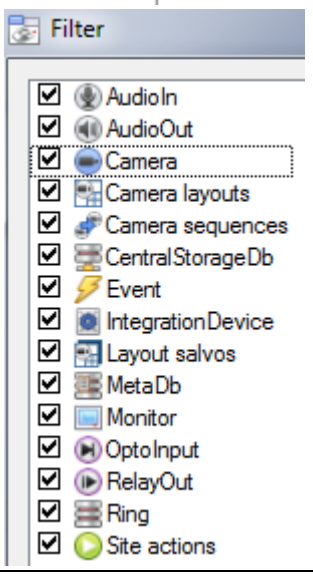


1. This list is the list of servers on the Site, and the resources each server has.
2. This is the list of resources that will appear in the Resources Panel.
3. Clicking on any of these toolboxes will bring up the named resource. This is evident in the example of Camera Layouts, to the right.



4. This is the filter feature. It may be used to remove some resources from the list, in order to simplify the screen.

The available filters are represented in the image to the right.

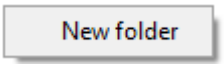


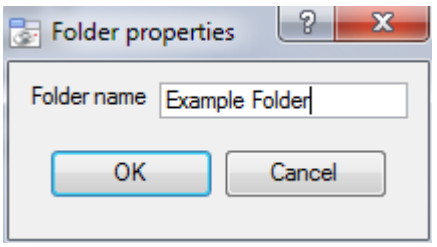
- Add a Resource to the Resources List

To add a resource to the list that will appear on the panel, simply select one or more resources, by left-clicking on them, then click-drag them horizontally into the Resources area.

- Create a folder

Organise the resources further by creating a folder. To do so, right-click on any white-space in the resources area (Where the included resources are), and click on New Folder. Give the folder a name.





To add items to the folder, simply drag-click them into the folder, in the same way resources are added to the list.

- Delete/Rename folders and Resources

To remove items from the Resources Panel list, right-click on the item and click **Delete.**
To Rename a folder, right-click on the folder, and click **Properties**.

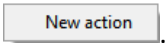
Setup Tab: Site Actions

1 Site Actions

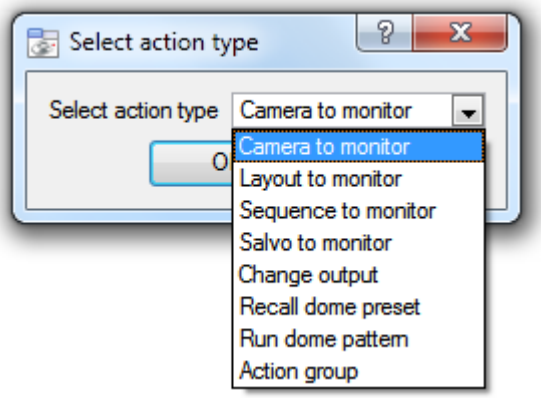
Site actions are setup in the **Site Actions** section in the Setup Window. From Configure Servers, click on the following icon to get there:

The reason for having Site actions outside of the Events Setup Window in Configure Servers, is because of the fact that, when Events are edited, this is done so 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.

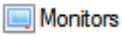
a. Creating a Site Action

To add a new action, simply right-click on any white space in the Actions Panel, and select 

. 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.



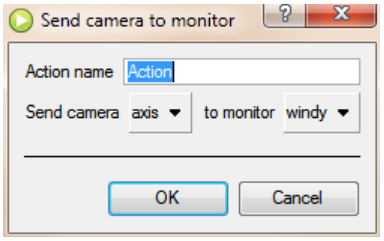
Camera To Monitor	This will send a preconfigured camera to a **CathexisVision Video Wall**.
Layout to Monitor	This will set the view on a Video Wall to a predefined Layout.
Sequence to Monitor	This will run a predefined Sequence of individual cameras in panel.
Salvo to Monitor	Will run a predefined Salvo 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, all the actions under Site Actions need to have already been created before an action can be created using them. [For instanced the *Camera to Monitor* Site Action uses a monitor that was created under 

in Configure Servers.]

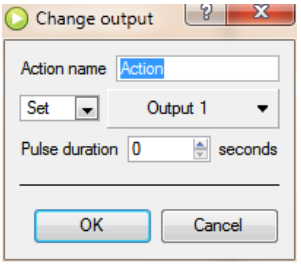
b. Four Action Types

Monitor related actions



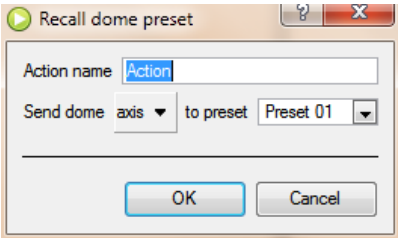
Will send a specific Site resource to a predefined Monitor.

Output related actions



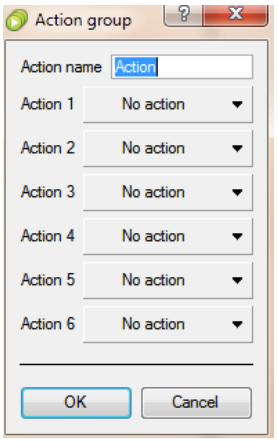
Will change the state of a predefined Output.

Dome related actions



Will affect a PTZ camera. I.e. **Run Dome Pattern**, or **Recall Dome Preset.**

Group actions

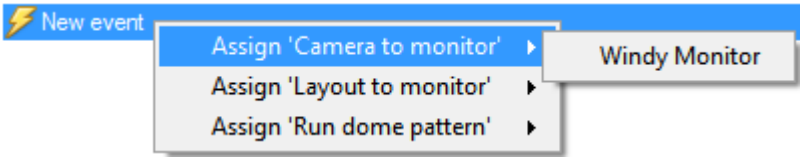


An Action Group is a single Site Action that contains multiple Site Actions.

Use this option to have more than one Site Action on an event.

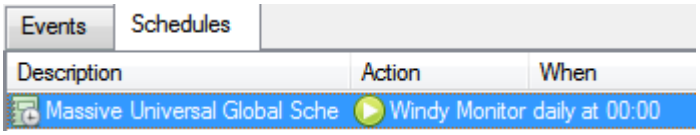
c. Adding a Site Action to an Event

For a Site action to trigger when an Event triggers, attaching a Site Action to an existing Event is very simple. Right-click on one of the events. This will provide a list of Action Types that have been added. Under each type is a list of all Actions of that type that have been created.

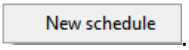


To complete, select the Action to assign to this event.

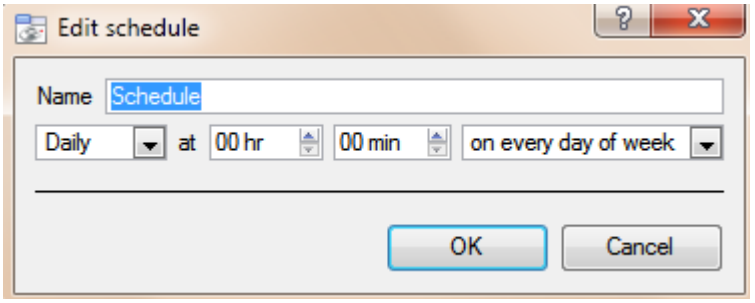
d. Adding a Schedule to a Site Action



If there aren't any schedules created, right-click any white space under the schedules tab, and select



. 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.

Setup Tab: Reports

1 Reports

a. Introduction

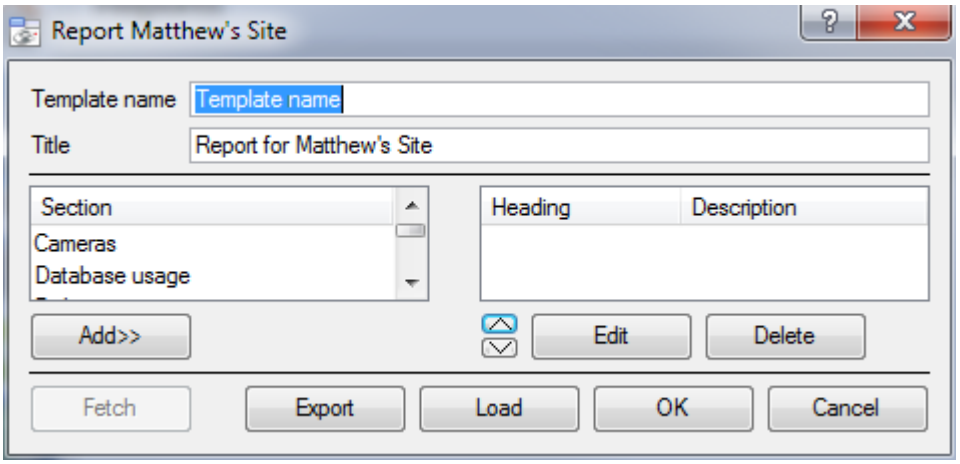
CathexisVision offers extensive reporting on both the Hardware, and Software, that comprise the Site. A very practical feature of Reports is the ability to create **Report Templates**. These are pre-defined sets of reports that will pull the same information each time. One of the real benefits of the Templates is the ability to retrieve the reports on a schedule.

Reports is under **Site Menu→Open Tab→Setup→**

b. Controls

- Add, Edit or Delete

To Create a Report, or edit a new one, click on either New or Edit. In the Report Template Editing window below, there are two columns. The column on the left is populated with all the available Report Variables. The column on the right is filled with the variables that the current Report Template will use. Each available **Section** will be explained in detail, below.



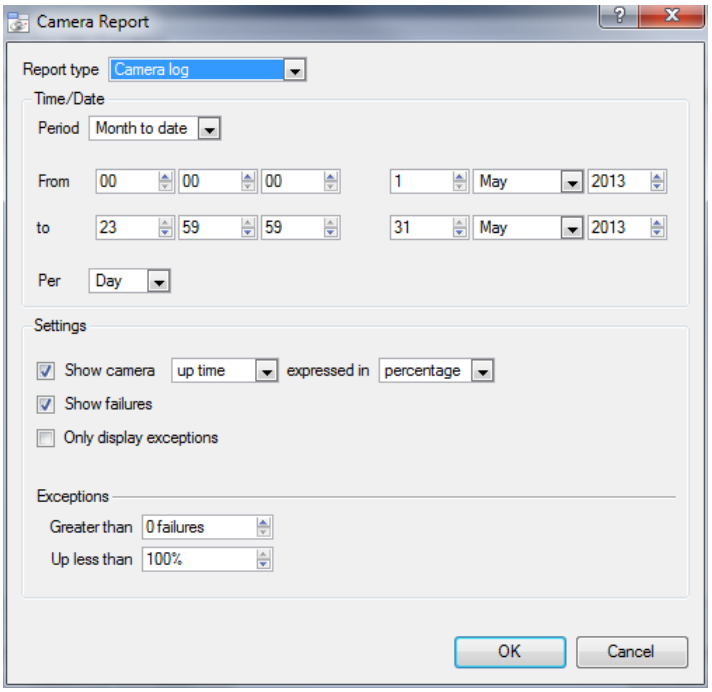
Fetch will generate the Report setup, based on the variables that are currently populating the active variables list.

Template Name is the name of the Template.
Title will be the title of Report that is produced.
Add will add the selected section to the Report's list of active variables.
Edit will edit a variable selected from the active list.
Export will export the Template as a local file on the Master NVR, which can then be imported to another Site using the **Load** button.

Note:

- Many of the report variables will require some setup.
- The reports will appear wherever the variable appears in the list. So, add them in the order desired for them to appear in the report.

- Cameras Section



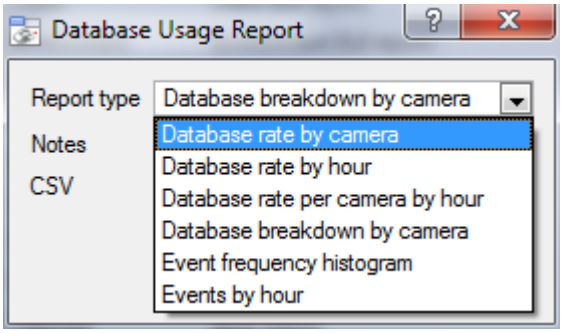
Report Type

Choose one of the descriptive Report Types.

Show failures tells the report to show the number of failures for a camera over the given period (a failure is when the camera goes from working to not working i.e. it fails)

Only display exceptions tells the reports to only show cameras that meet the exception criteria, which the user specifies on that same page. This is useful to only see the problem cameras.

- Database Usage Section

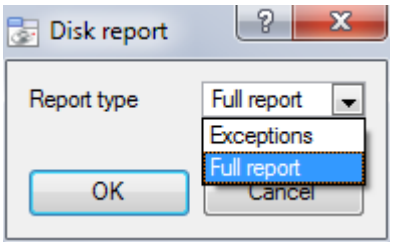


Report Type. Choose from one of the descriptively titled Database Report Types.

Notes. Here, add some notes about the report, or 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.

- Disks Section



Report Type.
A Full Report will contain all available information on the Disks, including temperature, and Raw Read Error Rates.

An Exception Report will contain only information on Exceptions that have occurred.

- Environment Section[4]

Environment will fetch information about the environment inside the servers. Such as voltages, CPU temperatures, and fan speeds.

- Events Section

The "Events" reports listed the frequency of events occurring over a period.
Note: from 2016 onwards, this option will not work.

[4] Only available on supported Cathexis hardware.

- Hardware Section

This will fetch a full list of the relevant hardware components inside the servers. (Includes pc hardware, and **Cathexis** specific hardware)

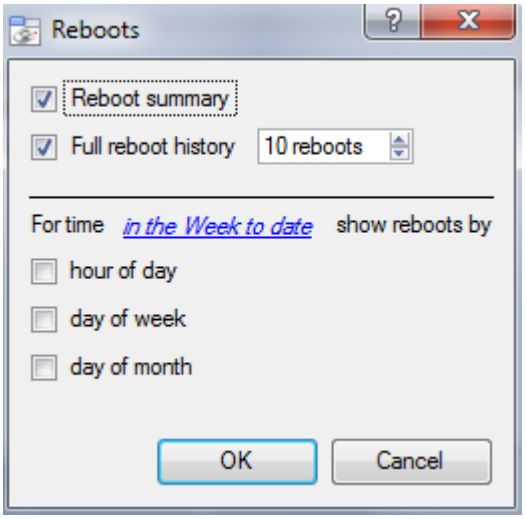
- Licenses Section

This will fetch a list of all the licenses, and their descriptions, on all of the units attached to the Site. (This will exclude the Base Stations.)

- Network Time Protocol Queries Section

If NTP is setup, this report will pull all NTP query related information.

- Reboots Section



Reboots are an important problem to monitor.

To fetch reboot reports for a period other than *in the Week to date*, click on the hyperlink.

This will navigate to the calendar settings, where one may set the report to pull information from a

- **From-To** period. (E.g. from X date-and-time, to Y date-and-time).
- From the **previous** X hours, or
- Over a **period** of time, starting at a set time, on a set day.

- Recording Times Section

The amount of time each camera, on each server, has spent recording.

Note:

- Cameras that didn't record will be included and highlighted in red.
- Cameras that haven't recorded in the last day will be highlighted in orange.
- Cameras are listed alphabetically.

- Software Section

This will list the version of **CathexisVision** running on each server.

- System Section

This will list the Time Zone related information. (Time, Time Zone, Daylight Savings.)

- System Setup Section

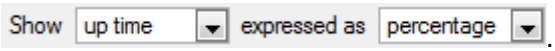
This relates to the cameras/encoders attached to the system, and how they are setup. There are two options a **Camera Recording Setup** report, and an **Encoder Setup** report.

Camera Recording Setup	This will pull 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 will pull 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 (physical input on the Encoder) it represents, the Firmware etc.

- Unit Up-Time Section

Up-Time is the amount of time that the unit stays on between reboots, or failures. It is of similar importance to Reboots.

And an important setting is 

. Here, either show Up-Time, or Down-Time. One may also express the Up/Down-time as a percentage, or in time units.

- User Defined Section

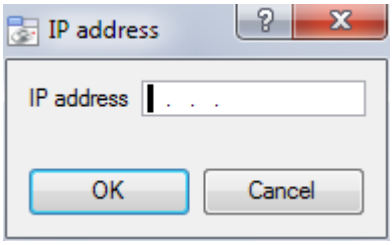
When adding a User Defined variable, one will be presented with an empty text editor box.

The text added here will simply be added as a section in the report. One may use this to add any general notes, or information needed to appear in the report.

- VMX Counters and VMX Temperatures Section

Each brings up a different set of information about VMXs attached to the servers.

- Windows Unit Section

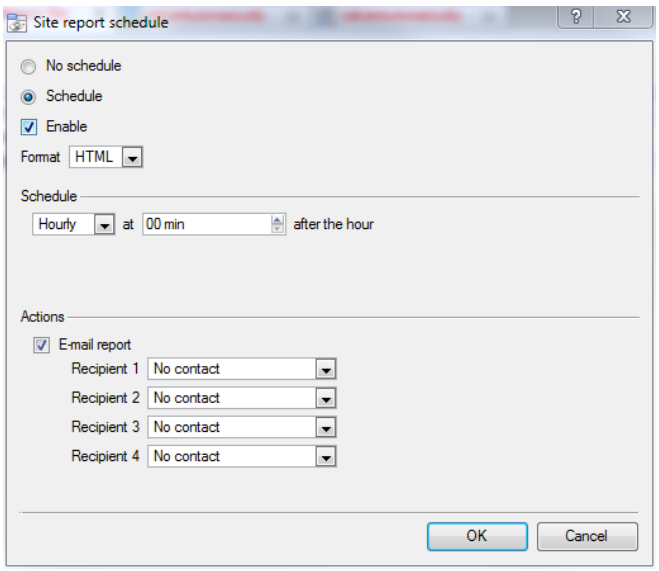


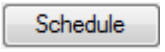
When adding a Windows Unit, the user will be prompted to enter an IP address.

This report will pull information for Windows Base Stations that use the Site.

This will include hardware, and software information about the Base Station, as well as the **CathexisVision** applications that it has been using.

- Schedule



To add a Schedule to a report: Select a report from the Reports list, and click on the 

button.

Format
Emailed reports are sent in HTML format.

Schedule
The actual schedule may be generated of a variety of time frames, from hourly to monthly.

Actions
If the Site has setup emailing, and setup some Site Contacts, then one may email reports when they are generated.

- Fetch

This will pull the report for the Template chosen.

At the bottom of the fetch window, there are four options.

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.

E.g. C:\Program Files (x86)\Cathexis CathexisVision Suite WRV\Sitedb\reports.

Setup Tab: Configure Failover Servers

1 Failover Introduction

a. Model

Cathexis uses a Hot-spare model for failover. In this model, failover servers monitor the recording servers. When a recording server is down, one of the failover servers assumes the functions of the failed recording server.

In failover mode, the failover server operates exactly like the failed recording server, and 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 assume the function of a single recording server at a time.

Image Above: A Site, in normal configuration with the Hot-spare Server, available to assume the functions of a Recording Server. Note that there are different IP addresses for the Recording and Hot-spare servers.

The failover unit is represented with the unit icon to the left.
It is distinguished from regular units by the lifebuoy/lifesaver image.

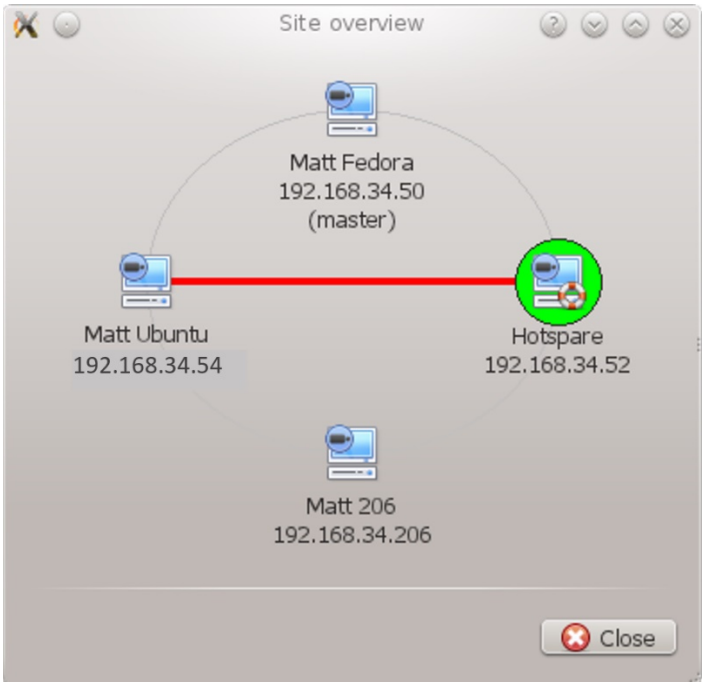


Image Above: A site, in Failover configuration, with the Hot-spare Server 192.168.34.52 having now assumed the functions of the failed Recording Server 192.168.34.54. The Hot-spare Server could assume either of the Recording Servers functions. **Note:** The IP address of the recording server has changed to the IP address of the failover server, and will remain as such until the recording server is back online.

b. 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 the total number of cameras on the site that is to be failed over. (I.e. if a site has more cameras than there are failover camera licenses it will not get failed over.)
2. All Cathexis SAM encoders require failover licenses. Licenses are required per channel.

Note: Before the failover site is licensed, the status bar license warning will be red, and if it is expanded, the description should be that the failover site is unlicensed. By adding the required number of failover camera licenses, the status bar license warning should disappear.

c. Recommendations

When configuring a Site with failover, there a few things the designer can do to maximise system up-time:

1. Have a highly reliable Site master. This is important for two reasons:
    i. External viewers connect to the Site using the IP address of the Site master. If the Site master fails, the external connections fail.

ii. 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. Don't attach any cameras to the Site master, and disable failing over of the Site master (this is so that 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 must be enough recording storage on the failover server to serve for the maximum expected downtime, of most active units being failed over. Expect to have a maximum of one day's downtime, and have enough storage for this period.

d. 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 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, this ensures that the footage is also accessible from the user interface and covers the loss of 30 seconds (or less) during the server switchover.

e. 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 onwards.

f. Example

Single Site with the following:
2x NVR's 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 NVR's simultaneously, it requires 4 failover servers with 256 Failover Camera Licenses (4 x 64). The camera licenses are shared across all failover servers and since the maximum number on a single server is 64, then all servers must have access to 64 camera licenses.

The Gateway WIN7 machine, if part of the Site, will be failed over but 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 3x Failover Servers and 192x Failover Camera Licenses (3 x 64) would be required.

2 Setup

a. Introduction

The failover configuration has two levels:

1. The failover server software needs to be installed on the failover NVR/s.
2. The Site needs to be configured to have access to the available failover server/s.

b. Requirements

Ensure that the failover and recording server (NVR) times are synchronised. This is a critical requirement for the database items recorded to the failover server to be correctly re-inserted into the recording server's database.

c. Configuration

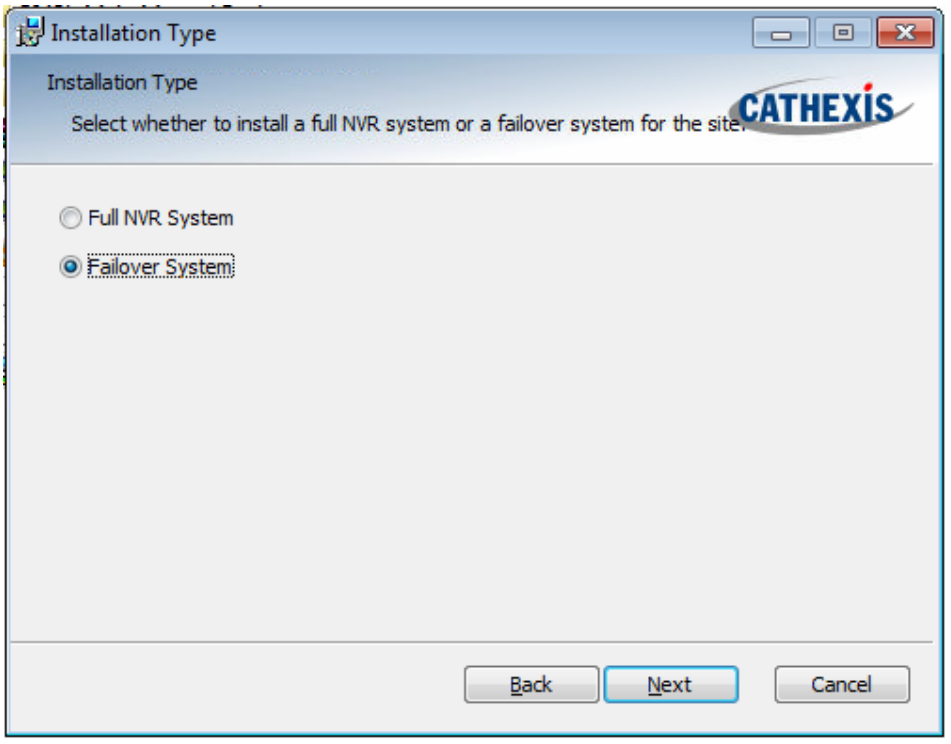
Failover NVR Configuration

A **CathexisVision** failover server is installed with the regular **CathexisVision** installer. After installation, if the GUI is run, it should popup a message saying "This server is running as a hot spare".

- ***Install the CathexisVision Software***

The failover server will need the **CathexisVision** Software installed on it.

During the installation process, one will be prompted to choose between a **Full NVR System** and a **Failover System**. For this installation, choose the **Failover System**.



- ***Check installation***

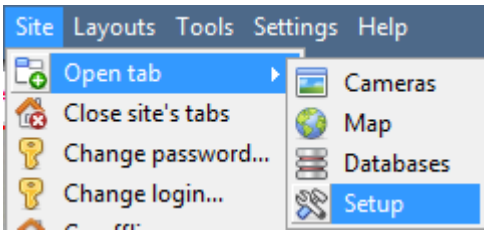
After a successful installation, if one attempts to run **CathexisVision**, by double clicking on the **CathexisVision** icon, there will be the dialogue box to the right:

- ***Site Failover Configuration***

Each unit failed over will need to be setup to do so. All failover servers are added to the Site on the Site master. There is not individual master/slave recording server configuration required for failover setup.

- ***Open the Failover Panel***

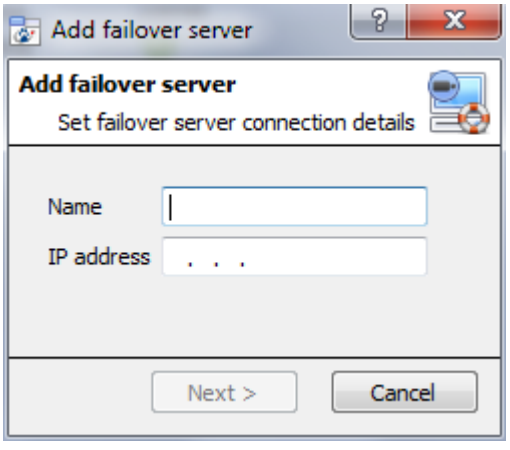
To open the failover setup, follow the instructions below.



After logging into the Site, to open Configure Server simply click on **Site → Open Tab → Setup.** Once in the Setup Tab click on the Configure Failover Servers icon: 

Note: Right-Clicking on the tab of any open Site will bring up the same menu as the one accessed via the method above.

- ***Add a Failover Server***



Clicking on 

will open the dialogue to add a new failover server.

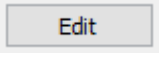
Add a descriptive **name** for the failover unit.

Enter the **IP address** of the failover unit.

Click **Next** to proceed to adding the failover database.

- ***Configure Failover Network Interface***

When a failover server has multiple network interfaces, it can be configured specifically to use one of them when registering itself in the Site.

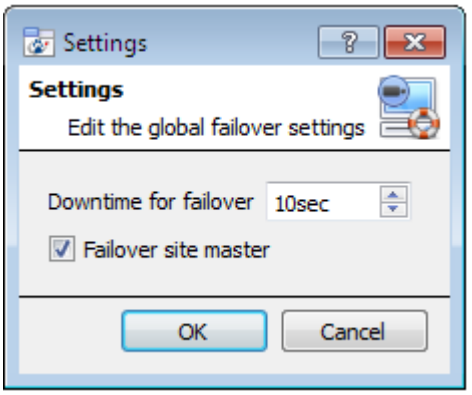
Click on the 

button and click on the Network Interfaces tab.

From the dropdown 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, resulting in the incorrect adaptor being selected. It is recommended to simply select the correct network adaptor to prevent this from happening.

- ***Define the Global Failover Settings***

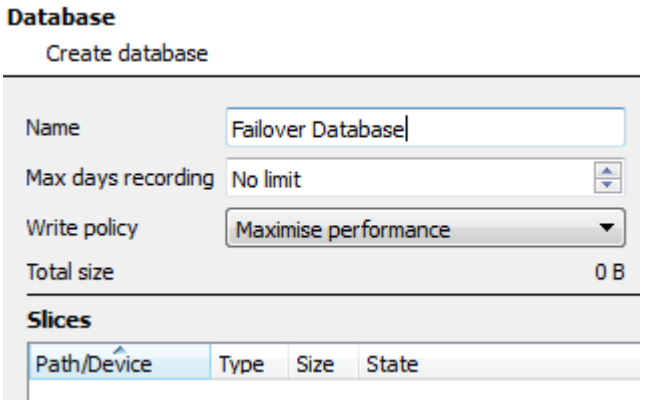


Click on Settings, inside the Failover panel.

Here, define the duration of **downtime** that is required for the failover server to take over.

Check Failover site master to failover the Site master unit. (**Note:** outside connectivity will be lost when the Site master is in failover.)

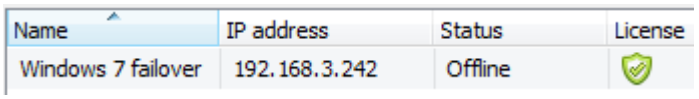
Database



This is the database which resides on the failover server itself. 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.

- ***Check the server is online***



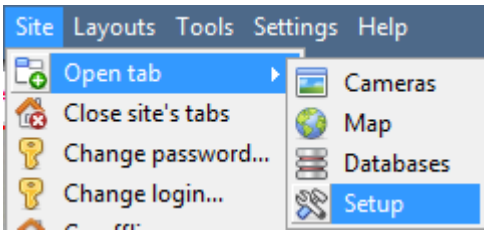
Once the server has been added, see its status and licensing in the Failover panel.

- ***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 it. Many servers will have multiple active databases; as such select which database these recordings get inserted into.

The reinsertion time for the video is dependent on the current recording server load onto which the databases are being updated due to the lower priority level of this process.

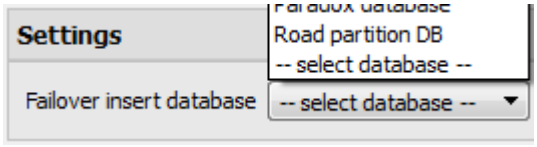
Navigate to the Databases Panel



After logging into the Site, to open Configure Server simply click on **Site —> Open Tab —> Setup.** Once in the Setup Tab, click on the Configure Servers icon: 

Expand the server, and left-click on Databases:

Select the Insert Database

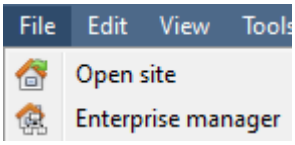


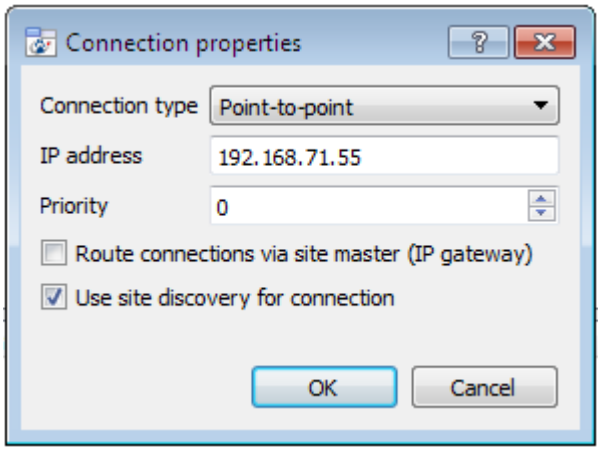
At the bottom of the databases panel, the Failover settings section will be visible. Click on "Select database" and select the database to reinsert the failed over recordings into.

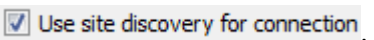
- ***Client Viewer Settings***

If the failover is setup so that the Site master will also be failed over, have **Use Site discovery for connection** option 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 

.

- ***Site Master Settings***

Setup 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**, which is dealt with in **Section 4.12 Technical Alarms**.

3 System Restore after Failover

Note that it is vitally important 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.

a. 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.

Important Notes:

- Ensure that the new unit's IP address is the same as the previous master unit.
- Install the correct software version (new installation, without configuration).
- 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.

b. 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.

Important Notes:

- 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.

Setup Tab: Adjacent Camera Mapping

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, he/she 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.

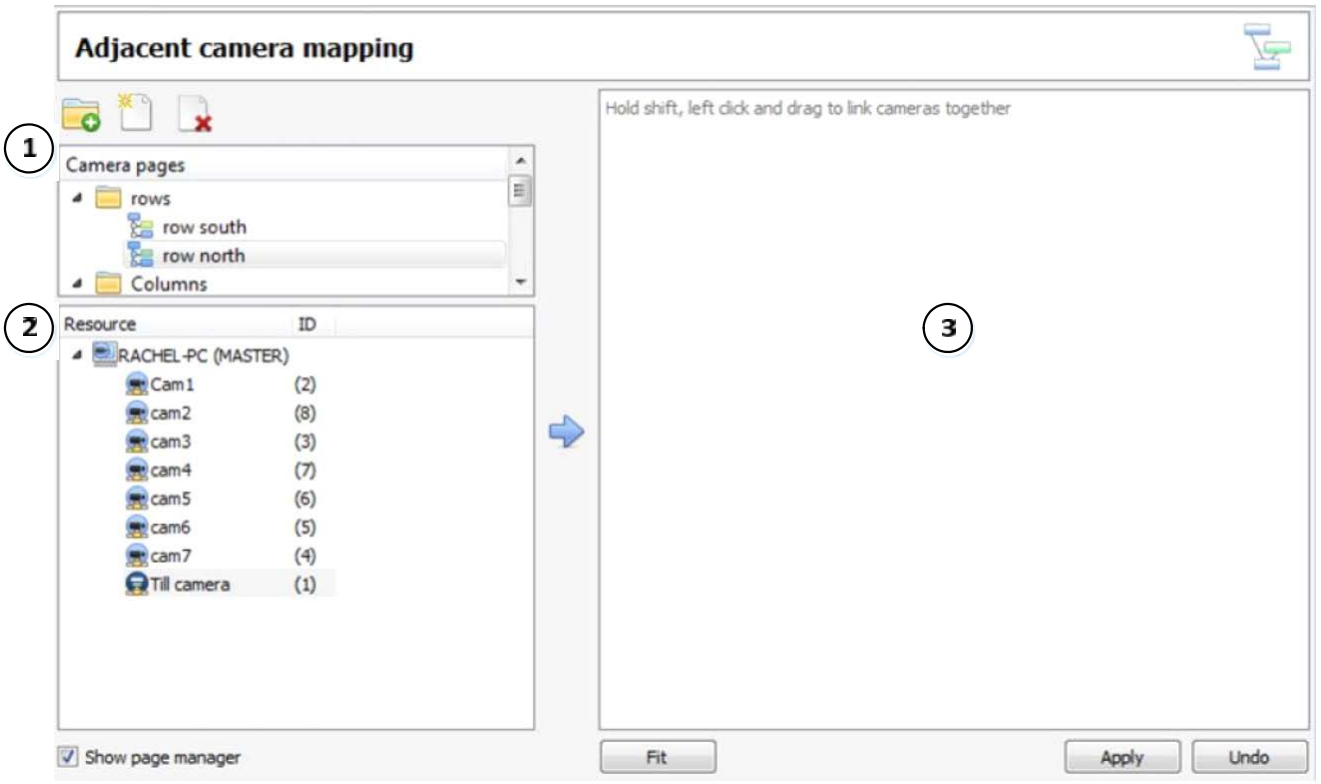
Operators can change the way that adjacent cameras are displayed in the resources panel by selecting the Adjacent cameras option from the drop-down resources list.

If selected, adjacent cameras will be displayed with live/review thumbnails which the operator can then select to navigate to.

2 Setup

Click on the **Adjacent camera mapping** icon in the left panel of the Setup tab. It will present the screen below.

a. Basic Interface



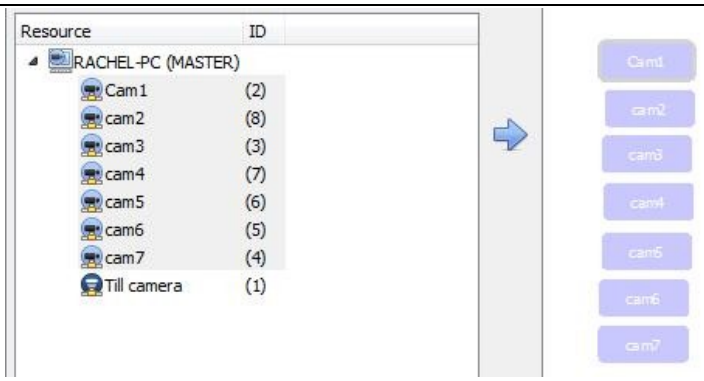
	Area	Description
1	Page Manager	Check Show page manager to display this panel. From this zone, one may create folders and pages into which adjacent cameras can be grouped. Add a new folder Add a new page Delete selected page
2	Resource List	All camera resources which have been added to the system are available for mapping here.

3	Camera Mapping Area	Highlight desired cameras and click the arrow to add them to this area to be mapped.
		Clicking this will scale the mapped cameras to fit in the screen.
		Apply all changes made.
		Undo all changes. Click this before applying changes in order to take effect.

b. Map the Cameras

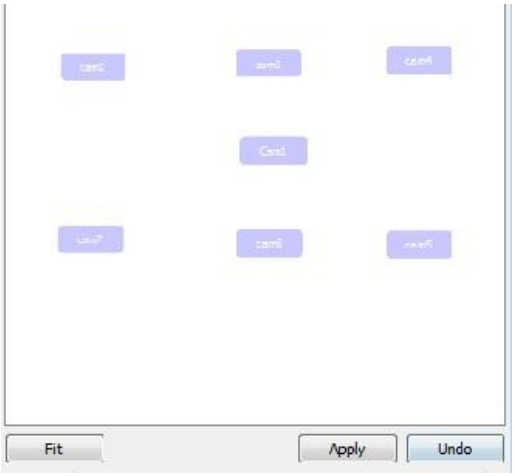
In order to map the adjacent cameras, **add the cameras** to the blank area, **link the cameras** and then **edit the camera relationships.**

Add Cameras

In the Resource list, select the cameras to map. Click the  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. Then organise the cameras according to their physical locations.	

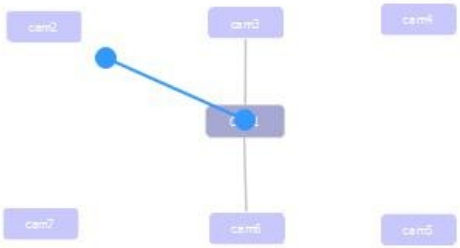
Organise Cameras

To organise cameras, simply click on the camera name and drag it to the desire position. See below for an example:



Link Cameras

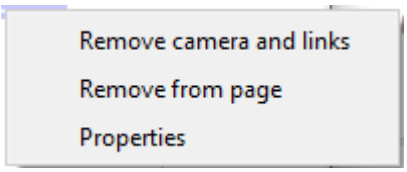
Next, link the adjacent cameras. To do so, click on the first camera while holding shift, and then drag to the second camera.

	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**.

Camera Right-Click Options

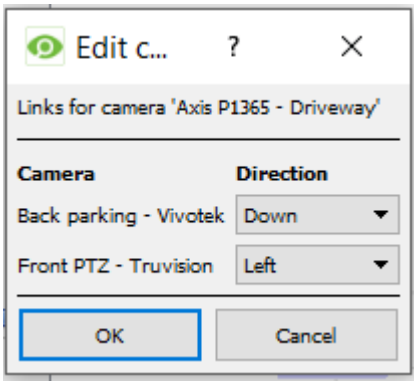
Right-clicking on a camera will offer the following options:



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.

- ***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 

to save or 

to reset.

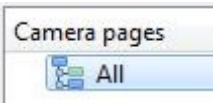
For more extensive camera organisation, see the next section on the **Page Manager**.

c. Page Manager

In the Page Manager, it is possible to organise linked cameras into groups which are user-defined. Check 

to display the Page Manager panel.

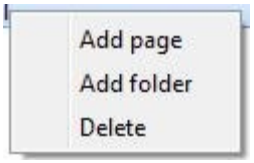
The default page is **All**, in which all cameras are grouped by the system. Selecting this page will display all cameras and their links in the mapping area.



Organise Cameras into Folders/Pages

One may extensively organise cameras into pages which can then be grouped in folders and sub-folders.

- ***Edit Pages and Folders***

	Button	Right-click
Add Page		
Add Folder		
Delete (page/folder)		

- ***Add Cameras to Pages***

Cameras must be added to a page which is then added to a folder.

Select the newly created page and then, in the Resources list, select the desired cameras and click the  icon to add them 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.

CathexisVision GUI Setup

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.

Note: For information that relates to the ***operation*** of the **CathexisVision** GUI, consult **Operators Manual**.

a. Minimising the GUI in Windows

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 what the user is currently doing. 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.

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, there will be the following entry:

Target: :\Cathexis catVision Suite NVR\nvr_gui_res.exe"

Add the extra commands after the quotation mark 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.

a. 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.

To review a **CathexisVision** Alarm Management Gateway, add the following:

gw xxx.xxx.xxx.xxx

The "x's" here represent the IP address of the gateway unit the user wants to connect to. For example,

Target: n Suite NVR\nvr_gui_res.exe" gw 192.168.42.43

b. 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, enter the following into the target:

forms x

Here "x" represents the number of monitors for **CathexisVision** to occupy when it starts up.

Please note: This option will override the settings configured in the CathexisVision software under Settings → General → Number of forms.

c. Set Max Number of Reviewable Cameras

The default number of simultaneously reviewable camera in **CathexisVision** is 8. For the most part this is sufficient. But to increase this limit, enter the following into the target:

max_reviews x

Here “x” represents the number of cameras set as the maximum review amount.

Note:

1. This is for reviewing recorded footage, not the viewing of live cameras.
2. The default number is a conservative amount, and is set to prevent **CathexisVision** from consuming too much of the systems RAM to function.

d. Add Multiple CathexisVision GUIs

Add the following to the target path to have multiple **CathexisVision** GUIs open simultaneously:

user1, user2, userX

e. View Legacy Archive Viewer

The legacy archive viewer will not be present from 2016 onwards, by default. In order to see it in the GUI, the user will have to add the following command line argument:

legacy_archive_viewer.

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. Unless a different installation folder was selected during the install process, the default path is:

C:\Program Files\CathexisVision Server

This section describes the processes of editing these settings files to configure the system to send text messages.

Supported Platforms

Windows and Linux.

Supported Software

CathexisVision 2014.4 and later.

Supported Modems

For supported/tested modems, consult this page:
https://integrations.cathexisvideo.com/supported-integrations/modem/

Currently, only the GSM modem (connected to a serial port) is supported.

a. Configure Notifying Alarms

Here, the alarms which will send text message notifications will be configured. 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 the CathexisVision software. 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	
	recipient cell number tech # SMS's should be sent for technical alarms event low # send SMS for low priority event alarms event medium # send SMS for medium priority event alarms event high # send SMS for high priority event alarms event all # send SMS for all event alarms pattern # specified a regular expression, used on the alarm description, to filter alarms	
Description		
	recipient cell number	Replace [cell-number] with the cell phone number of the person/people to send SMS notification to. Multiple recipients may be added.
	#	All text preceded by a # symbol is simply a comment in the file and will be ignored by the software.
	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	Enter [pattern abc], where [abc] is the event description. This is used to further refine which alarms will send notifications. **Note**: Event descriptions are setup when configuring events. See the Events section of this manual.

Example

Below are examples of possible file configurations.

- ***Example 1: Specified Alarms***

Structure	**Description**
========== recipient 062123456 tech recipient 062123456 recipient 064987654 event high ==========	Technical alarms will be sent to the recipient listed above 'tech.' Events alarms with a high priority will also be sent to multiple recipients listed above 'event high.'

- ***Example 2: No Alarm Filter***

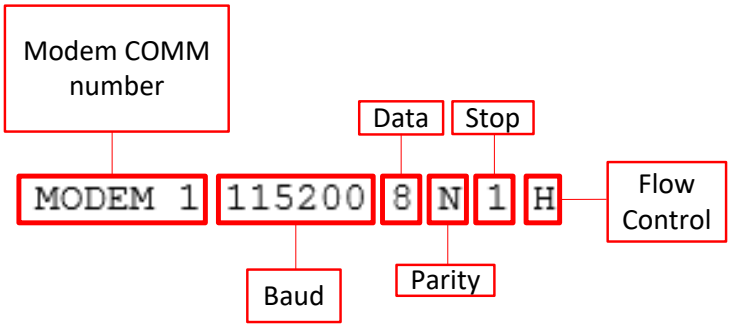
Structure	**Description**
========== recipient 062123456 ==========	All alarms received will be texted to the recipient as there are no alarm filters.

- ***Example 3: Alarm Description Pattern***

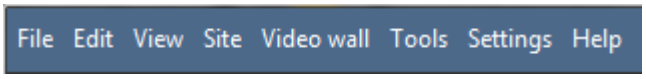
Structure	**Description**
========== recipient 0837654321 tech event all pattern ^Beware.* ==========	The listed recipient/s will receive all event and technical alarms, but only if the alarm description/s start with "Beware".

b. 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.

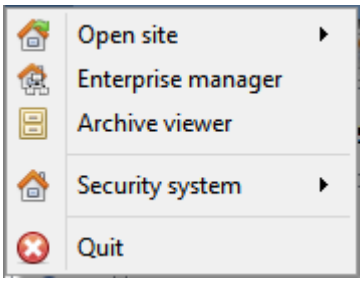
Required File	**sms_device.txt.example** This file needs to be renamed in order to become active in CathexisVision. Rename it as below.
Rename:	**sms_device.txt** (Remove the 'example' from the original file name.)
Default Location	C:\Program Files\CathexisVision Server\settings
Structure	---------- # 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.
	

4 Menu Bar



This will detail the different options available to the user through the menu bar of the **CathexisVision** GUI.

a. File Menu



Open Site

The menu attached to this tag will be a list of the Sites that have been added to this unit.

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.

Archive Viewer

This will open up the Archive Tab. If there is any archived video, it can be viewed here.

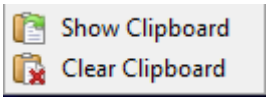
Open Site List

The names under Archive Viewer and above Quit represent the Sites that currently have connection tabs open in the GUI.

b. Edit Menu

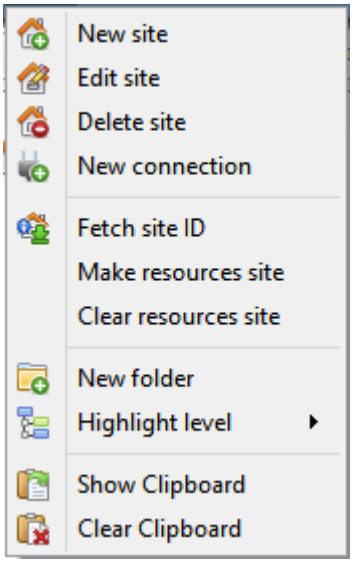
The edit menu, in general only displays the Show Clipboard, Clear Clipboard options. When the Enterprise Manager is open, there will be a range of different options.

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.

Enterprise Manager Edit Menu



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.

New Folder. One may organise Sites in the Site List into folders.

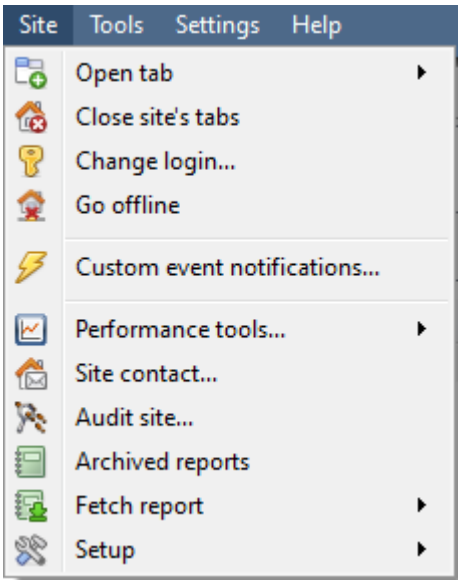
Highlight Level will highlight all Sites where X level is authorised.

c. View Menu

The only option available here is the option to change the GUI view to Full-screen.

d. Site Menu

The Site menu will relate to the Site whose tab is being viewed. To open a new Site, follow **File→ Open Site→ Site Name.** One may 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 Sites Tabs will close all open tabs for this Site.
Change Login will change the user who is logged in.
Go Offline will terminate the connection to the Site.
Custom Event Notifications below.
Performance tools Please see the Appendix to this document.
Site contact will show the name and details of the Contact person for the Site.
Audit Site below.
Archived Reports will display a list of previously archived reports.
Fetch Report below.
Setup below.

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 he/she has a Cameras Tab open. There are three types of notification.

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's meant as an unobtrusive feed of events (click the  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.

Event Notification Setup

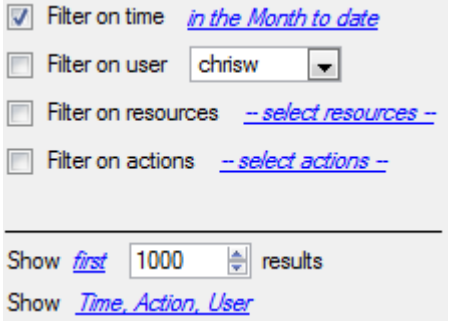
There are 4 levels at which these notifications can be configured (one global, and three tiers of Site based settings).

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. The idea being that operator A may want his system to respond in one way to certain events that is different from operator B on a different viewing system.

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 on.

Filter Time, Users, Resources, and Actions.

The **Show first/last** option allows one to limit how many of the results are brought up.

Show time/action/user option allows one to add/remove columns to the audit report, and will list the selected variables.

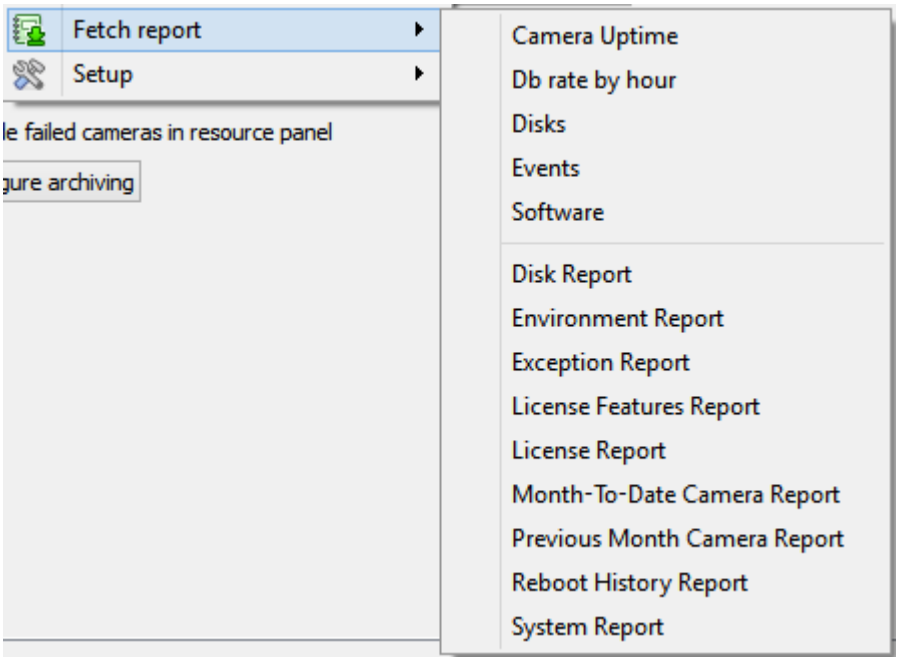
Print, Save, Refresh

 The report is not live, so 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.

Fetch Report



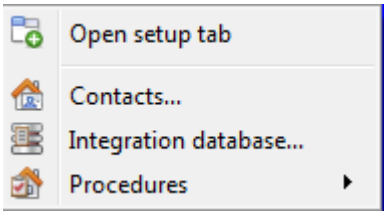
This menu allows a full report to be pulled for the entire Site.

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.

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.

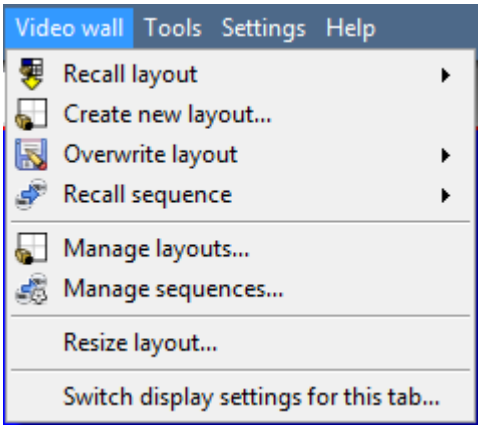
Contacts Here, add and edit Site Contacts.

Integration Database If the user needs, or has, a metadatabase (used for integrations), add or edit them here.[5]

Procedures is a procedure for an operator to follow in a particular event, this may include up to 6 contact people, and written instructions.

[5] The documentation for this is currently in the Integration Section of Configure servers.

e. 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 pane, 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.

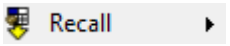
Layout

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.

Create new Layout

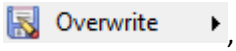
To create a layout, organise cameras on the screen as desired (double-left-click to expand; single-right-click to reduce). Then click on Layouts**—>New**. Give the Layout a name, and click OK. (one can use Layouts created in the Cameras Tab in the Monitors Tab, and Vice Versa.)

Recall a Layout

To bring up a list of existing Layouts, click on 

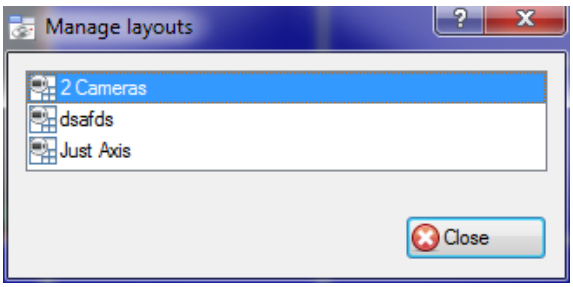
and select the layout name desired.

Overwrite Layout

Clicking on 

, and selecting one of the Layouts in the list, will overwrite that Layout with the current panel organisation.

Manage Layouts

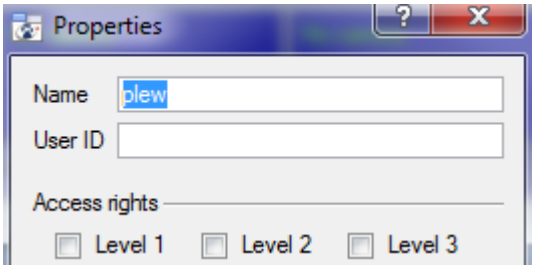


Clicking on 

will bring up the list of existing Layouts to manage.

From the management list, either delete the Layout or enter the Layout Properties window.

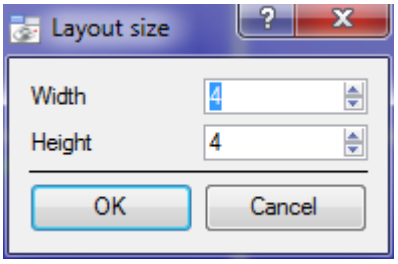
These are both done by right-clicking on the Layout in the list.



In the **Layout Properties** window, 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, it isn't possible to change these settings.

Resize Layout



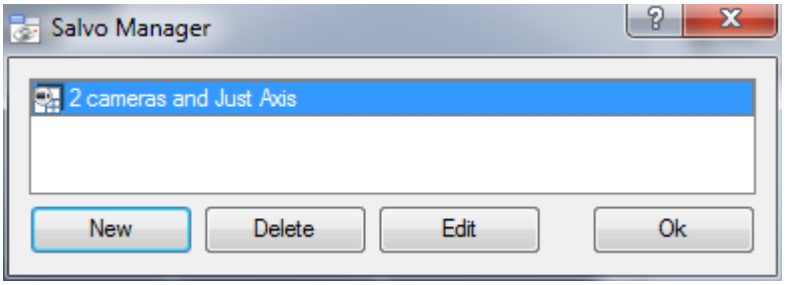
Clicking on Resize layout... provides the ability to change how many cameras are arranged on the screen. Define how many cameras there are per row, and per column.

The maximum amount of cameras per screen will be an 8*8 matrix. This is a Layout with 64 cameras. (This would require an incredibly large screen to be practical though).

Sequence

A **Sequence** is a cycle of individual cameras that will run, on a timer, in a single viewing pane.

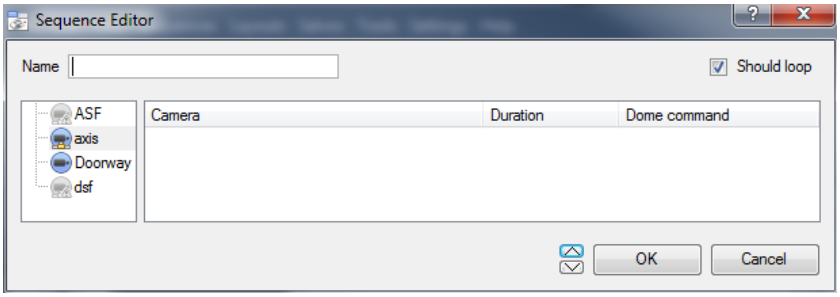
Sequence Manager



Clicking on the  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**.

Sequence Editor

Access the Sequence Editor, to create and edit sequences, via the Sequence Manager.



Name the Sequence appropriately.

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.

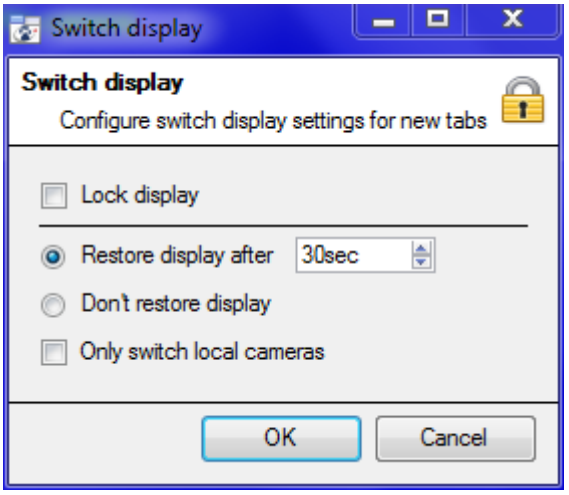
Remove a camera	Right-click on the camera and select Delete.
Set the duration of a camera for each loop of the Sequence.	-Right-click, and select Set Duration. -Enter the duration in seconds, and click OK.
Looping.	If the Should loop option is checked the Sequence will run indefinitely, if it is unchecked the Sequence will run once.
Change the order.	Select a camera and use the arrows to move that camera up or down the order.

Recall Sequence

To recall an existing sequence, click on Recall sequence to bring up a list of all existing sequences. Click on a sequence to run it.

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.

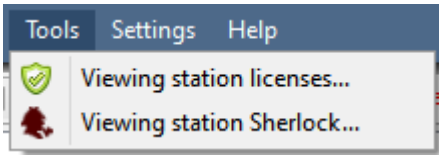
Restore display after
Will define how long after switching to the Event Cameras the Cameras Tab will return to the original display settings.

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 (which only appears when mouse hovers over it).

f. Tools Menu

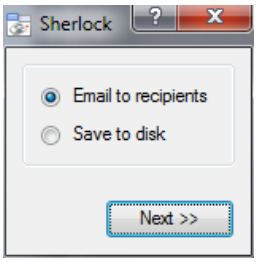


On a client PC it will say **Viewing Station licenses**. On the server, it will say "**Local server licenses**". Retrieve the server licenses from Site, or units, by entering the **Setup → Configure Servers→** and right-clicking on the unit.

Licenses

This will allow one to add a license to the Base Station being worked on, not to any of the Recording Servers on the Site.

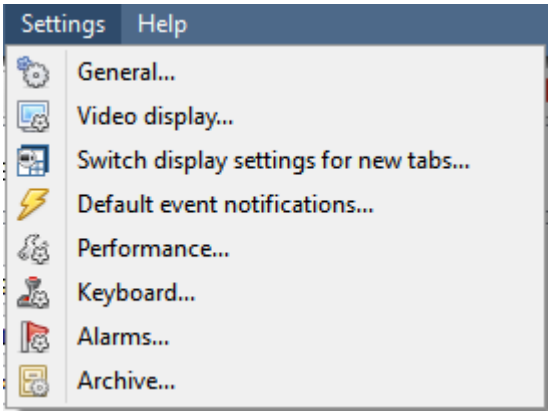
Sherlocks



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.

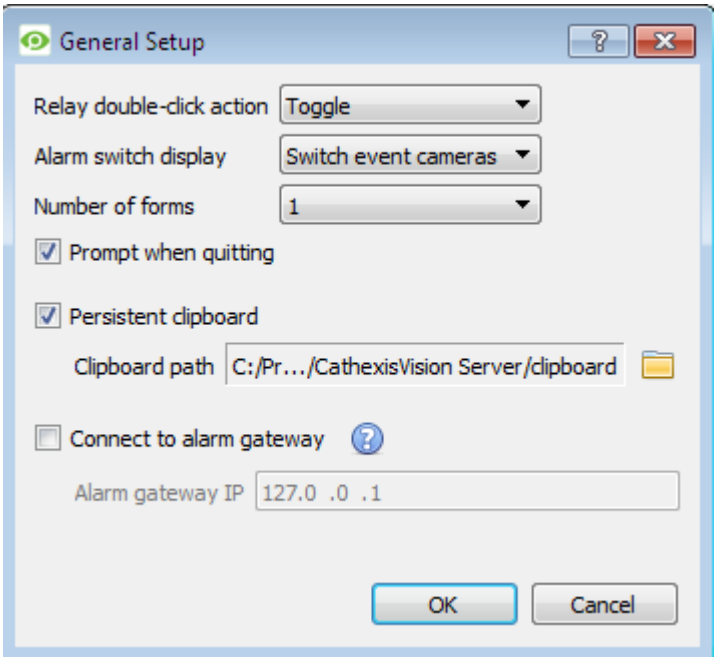
Note: clicking on **Email to Recipients**, will open up the Operating Systems default email client. **Save to Disk** will allow one to save the Sherlock files to any storage attached to the workstation.

g. Settings Menu



This section deals with the General **Settings Menu**.

General



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

This 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

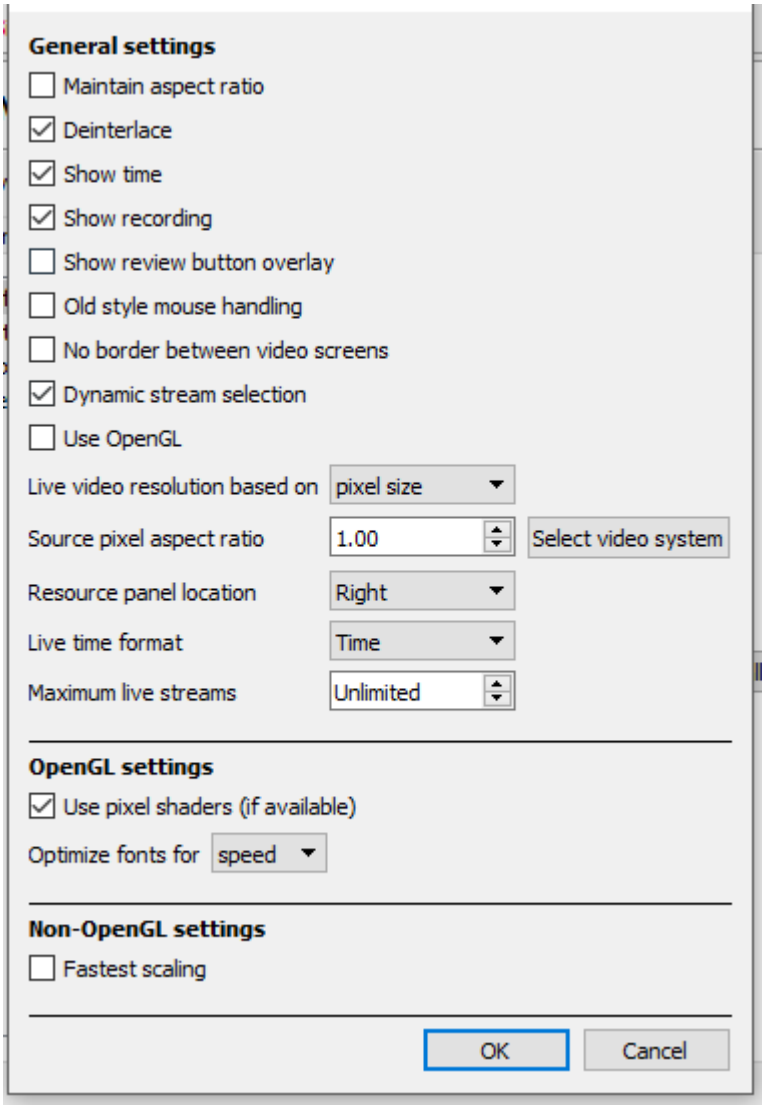
Select the default number of monitors to be displayed. The default maximum is 6, but this option can be overridden by editing the command line. See the Command Line Options section.

Prompt When Quitting will prompt the user every time he/she quits **CathexisVision** 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. These settings can also be configured by editing the command line. See the Command Line Options section below. Note that editing the command line will override these settings.

Video Display



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.

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, when 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.

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.

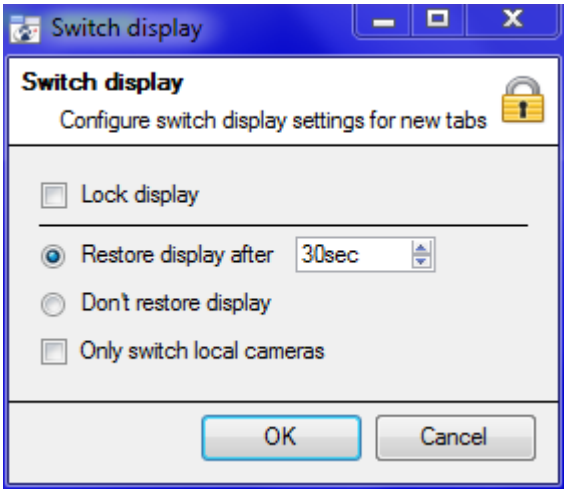
Live Time Format: Select from drop-down menu whether to display only time or date and time in live video.

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).

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.

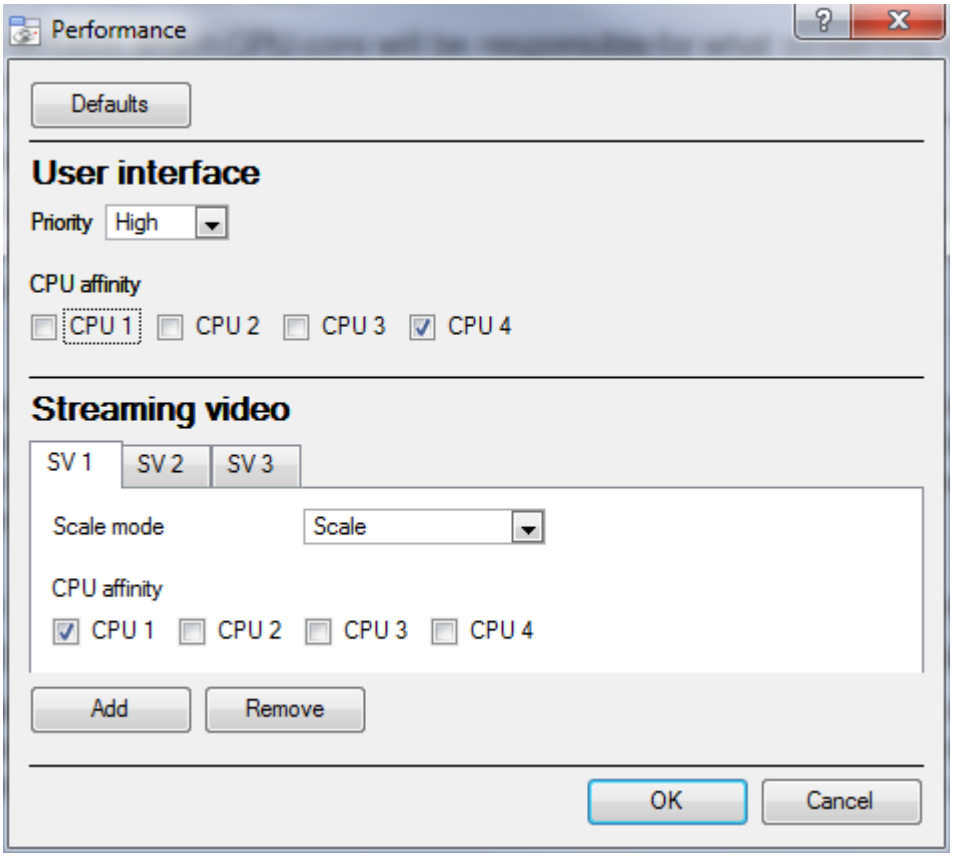
Note: Lock, or unlock, the currently opened Cameras Tab by clicking on the little lock located at the end of the Timeline on the Review Controls.

Default Event Notifications

Here, set what will be the default/global Event Notifications for this Viewing Station.

For more information about Event Notifications, and their Setup, see the section entitled 2.d. Custom Event Notifications (above).

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, don't 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.** Recall the defaults by clicking the **Defaults** button > **OK** (customised settings will then be lost). Default Options: Safe default Dual core Quad core Click on default to choose the default that best suits the system being worked on. Choose safe default if the system is unknown.
(2)	User Interface: What the user sees.
	Priority: The priority setting affects what the user sees as 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).

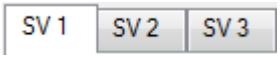
Streaming Video Server (SV):

By default, the system only has one Streaming Video (SV) server. Manually create further 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:

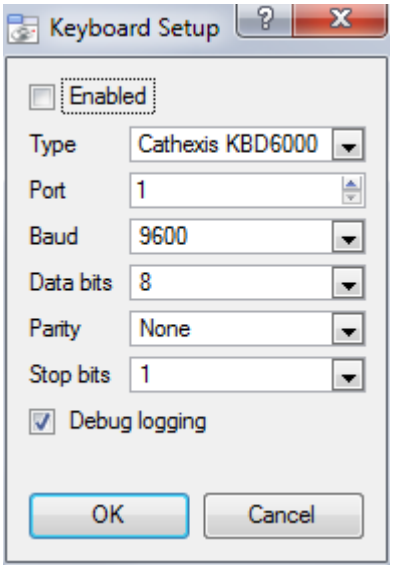
Whereas SVs are numbered SV1, SV2, etc, CPUs are numbered CPU0, CPU1, CPU2, etc

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)

Keyboard



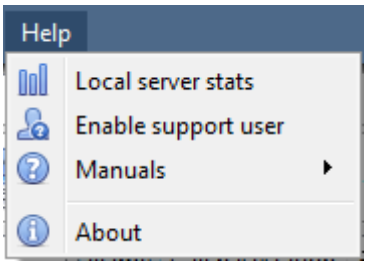
This option is for adding a keyboard to a Base Station. If adding a Keyboard to a Recording Server, do so via **Site—>Open Tab—>Setup—>Configure Servers—>Keyboard**.

Enter in the details relevant to the keyboard.

Alarms

Enter an IP address for a technical alarm server, or gateway, for the viewing software to send alarms to.

h. Help



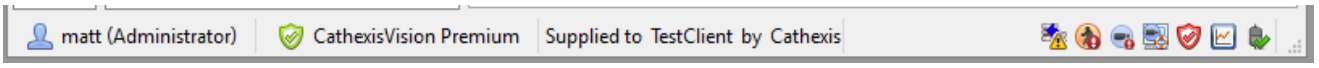
Local server stats"/"Viewing station stats: Shows the statistics for the local server if it's an NVR, or for the Viewing Station. Depending on which unit is being worked on.

Enable Support User: This will enable/disable a special user added for support purposes, when **CathexisVision** NVR is installed.
Note: this will only appear on NVR units.

Manuals: The Setup, Operator's, QuickStart, and Archiving manuals are accessible within the software.

About: Will inform one about the License, the Release version, and the email address for Support.

5 Status Bar



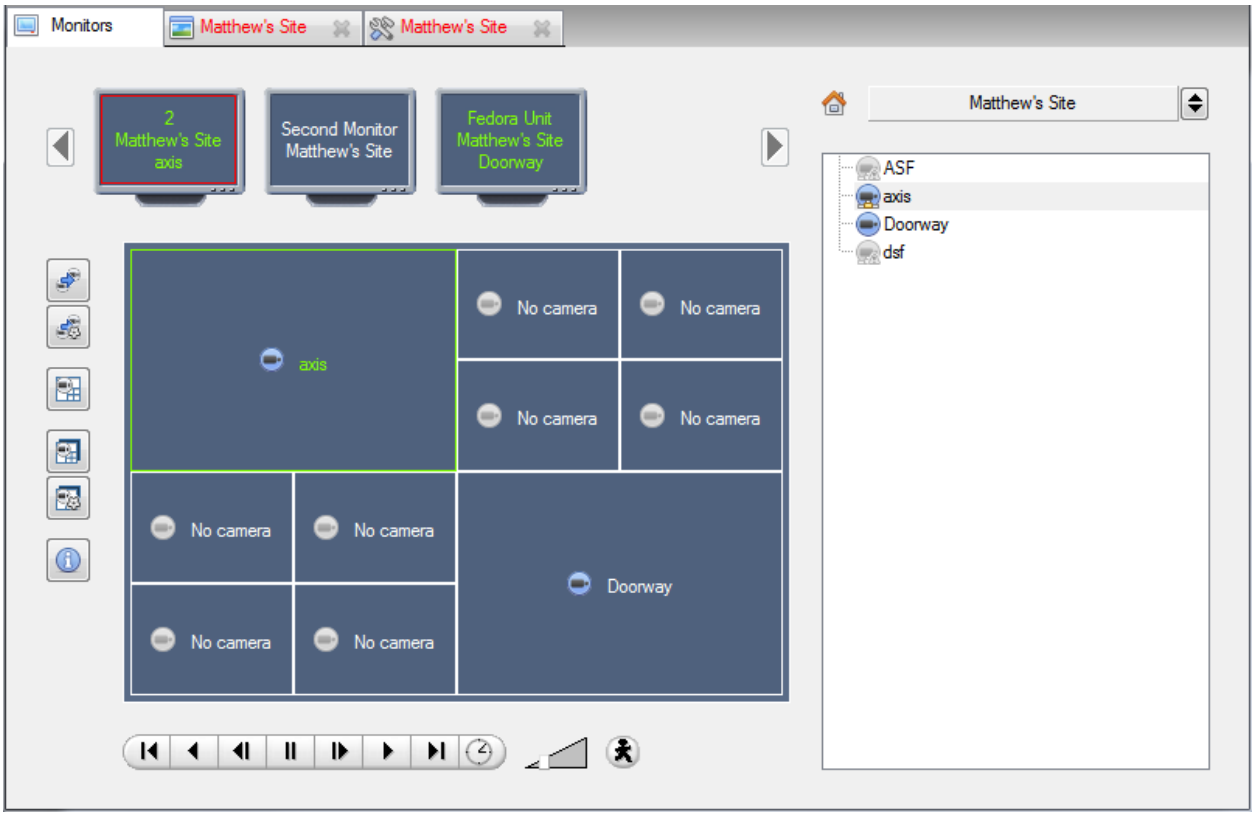
The status bar runs along the bottom of the interface. On the bottom right of the bar are a useful set of notifications. For further details, in the GUI, left-click on a specific icon.

Notification Icon	Notification Description
dvs (Administrator)	The currently logged in **user**, and their access level.
CathexisVision Premium	This represents the **Site License**.
Supplied to Documentation by Cathexis Internal	The **distributor** of the license.
	The **cameras notification** will only appear when cameras are down. Clicking on it will allow one to see which cameras these are.
	The **licensing notification** will be permanently present. Click to display information about Site 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.
	**Failover data merge** icon will provide details about current data merge operations.

6 Monitors Tab

The monitors tab is a tab that provides full control over the Video Wall. Here, change the layout, and define camera Sequences, and salvos.

There will not be any video playing on the interface. Rather, the names of cameras, where they are placed on the layout, will be displayed.



a. 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.

Layout

A layout defines how the cameras appear on the screen. This includes which cameras are present, to how much of the screen an individual camera takes up.

- ***Create a Layout***

To create a layout, organise the 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.)

- ***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.

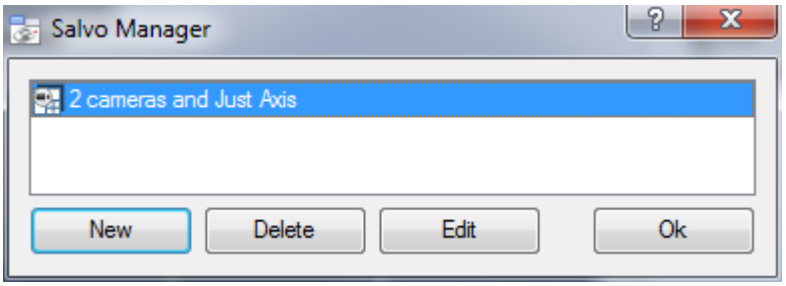
- ***Recall a Layout***

To bring up a particular layout on a screen, click on the  icon, and select the layout name desired.

b. Sequence

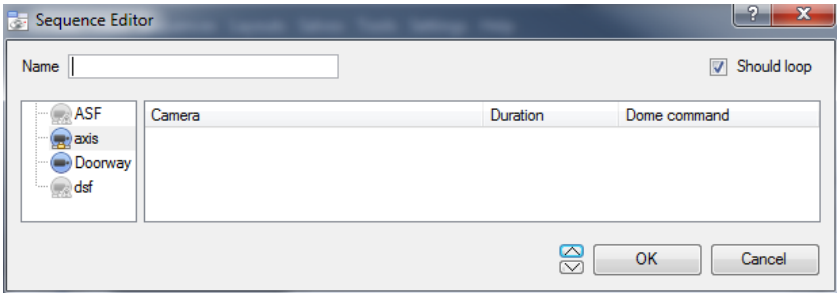
A Sequence will run a set of cameras, in a single camera panel.

c. Sequence Manager



Clicking on the  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**.

d. Sequence Editor



Name the Sequence appropriately.

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.

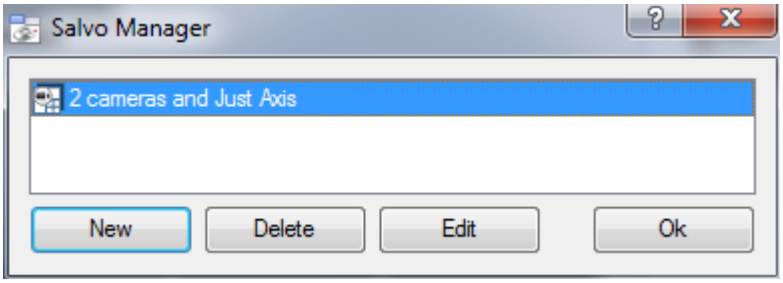
Sequence Editor Procedures	
Add a camera to a Sequence	-Double-click on a camera in the list of available cameras. -Or click-drag one, or multiple cameras, across into the Sequence list.
Remove a camera	Right-click on the camera and select Delete.
Set the duration of a camera for each loop of the Sequence	-Right-click, and select Set Duration. -Enter the duration in seconds, and click OK.
Looping	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.

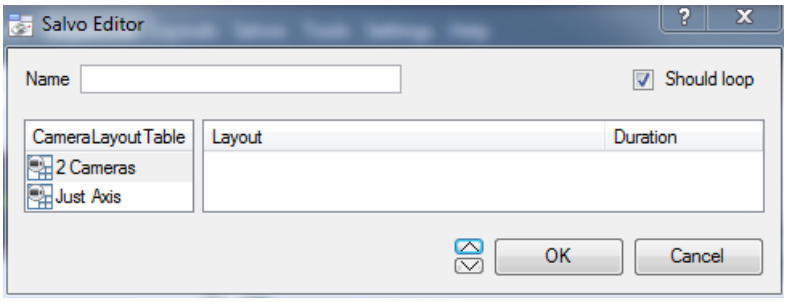
e. Salvo

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.

Salvo Manager



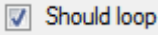
Click on the  icon. This will bring up the Salvo Manager. To **edit** a Salvo, select the existing Salvo and click edit. To create a **new** Salvo, click on New. This will bring up the Salvo Editor.



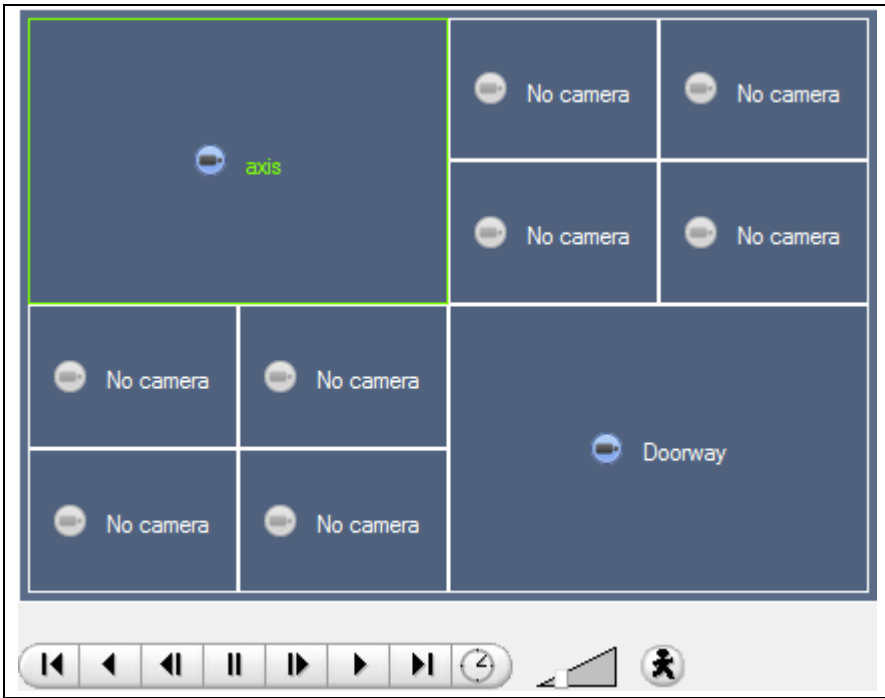
Name the Salvo appropriately.

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	If the  option is checked the Salvo will run indefinitely, if it is unchecked the Salvo will run once.
Change the order	Select a Layout and use the  arrows to move that Layout up or down the order.
Run a Salvo	- Click on a Layout panel. - Click on  - Select the relevent Salvo from the drop-down menu.

f. Virtual Cameras interface



The virtual cameras interface allows one to:

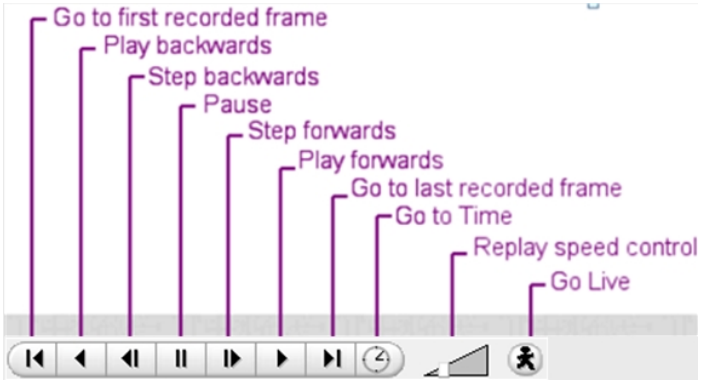
- See the Layout that the cameras will take on the Monitor selected.
- See what cameras are in which panels.
- Control the overlays on each camera.
- Use the Playback controls to review video on the Monitor.

g. 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.

- Review Controls



Note: When a camera has been selected, its border, and camera name, will become Green:

7 Cameras Tab

CathexisVision offers the installer two useful tools for retrieving visual information about cameras, as they are streaming information.

One needs to be in the Cameras Tab, viewing video, to carry out these steps.

a. Statistics and Information

Resolution and Bitrate

By pressing CTRL-R, 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 one can view the **resolution** of the feed currently being viewed

On the bottom left, there will be two numbers. The number in brackets is the **bitrate;** to the left of this number is the F**rames Per Second Rate**.

General Camera Information

By pressing CTRL-I the general camera information overlay will be brought up.

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 the 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.

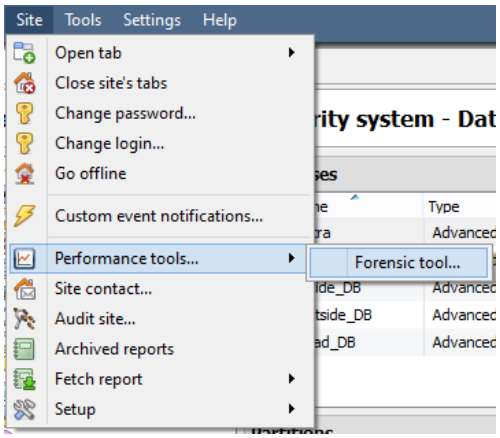
CathexisVision Forensic Tool

1 Forensic Tool

a. Introduction

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 will only be available in **CathexisVision** 2014.2 (Service Pack 2) and onwards.



Once a connection to the intended camera Site or NVR unit is made, open the forensic tool by selecting the "**Site**" menu option, scrolling down to the "**Performance tools**", and selecting the "**Forensic tool**..." option.

Note: One needs to be logged in with administrative rights to gain access to the Forensic Tool.

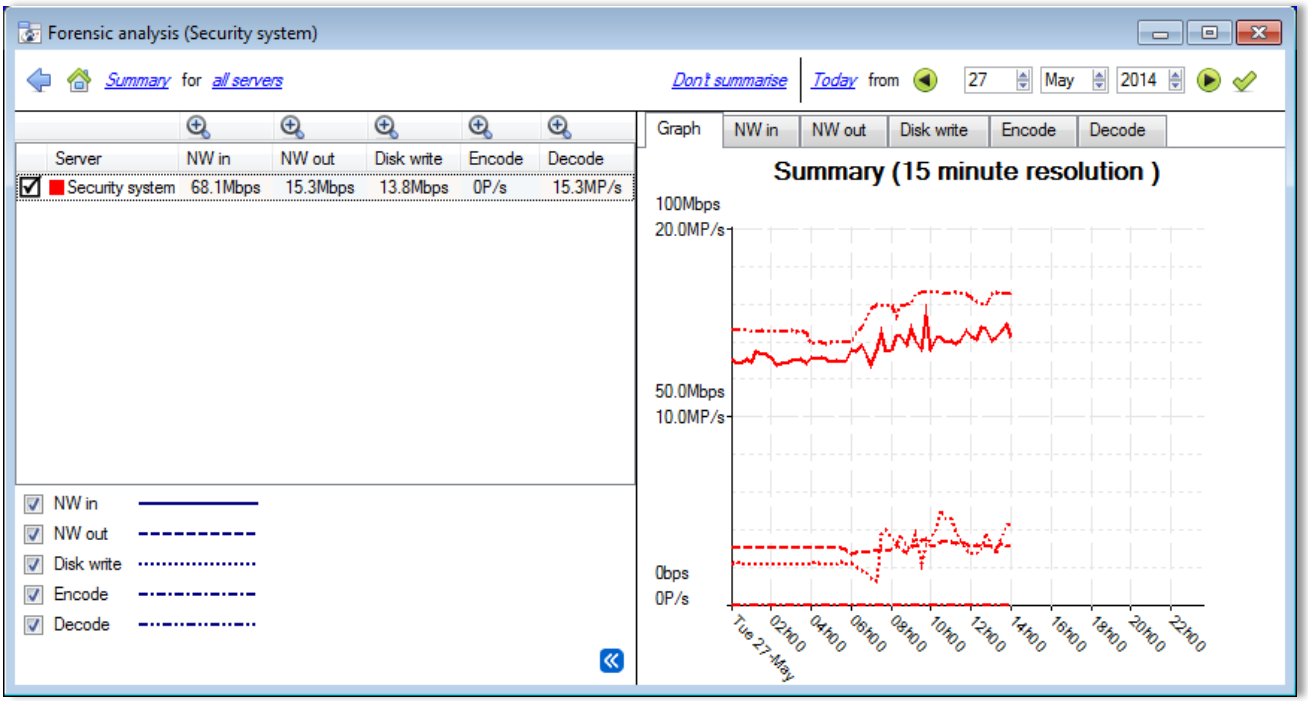
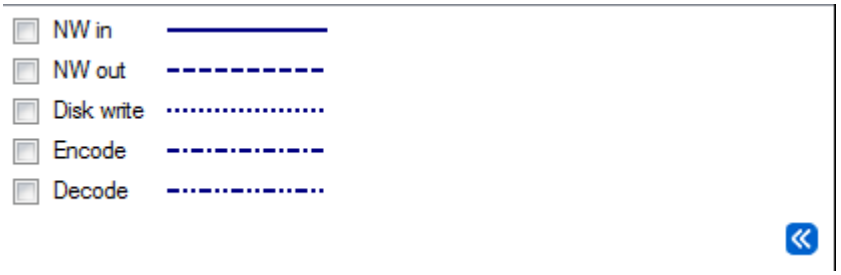


Figure 1 Main Forensic Window

The below sections explain the interface in Figure 1, and how to go about using this tool.

b. Data Values Used

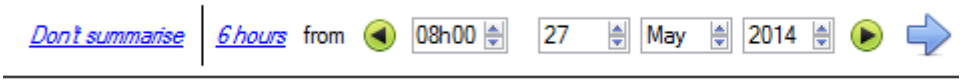


NW in	Network In (Mbps). This would be the video, streaming in from IP cameras.
NW out	Network out (Mbps). Video going out. Remote viewing Client PCs.
Disk write	Disk writing speed in Mbps. The rate writing captured video stream to local/network storage.
Encode	Encoded pixel rate. VOM1512/MPEG4 compression for recording/streaming. **Note**: This is NOT the transcoded live streaming.
Decode	Decoded pixel rate. For analytics the compressed video is decoded.

c. Date/Time Selection

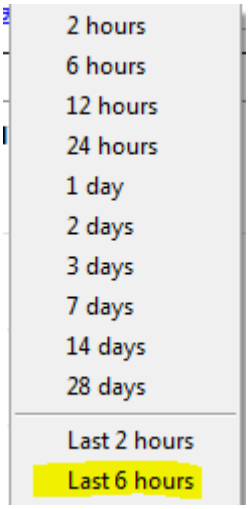
There are two ways to select the graphing period:

- Time Bar Selection



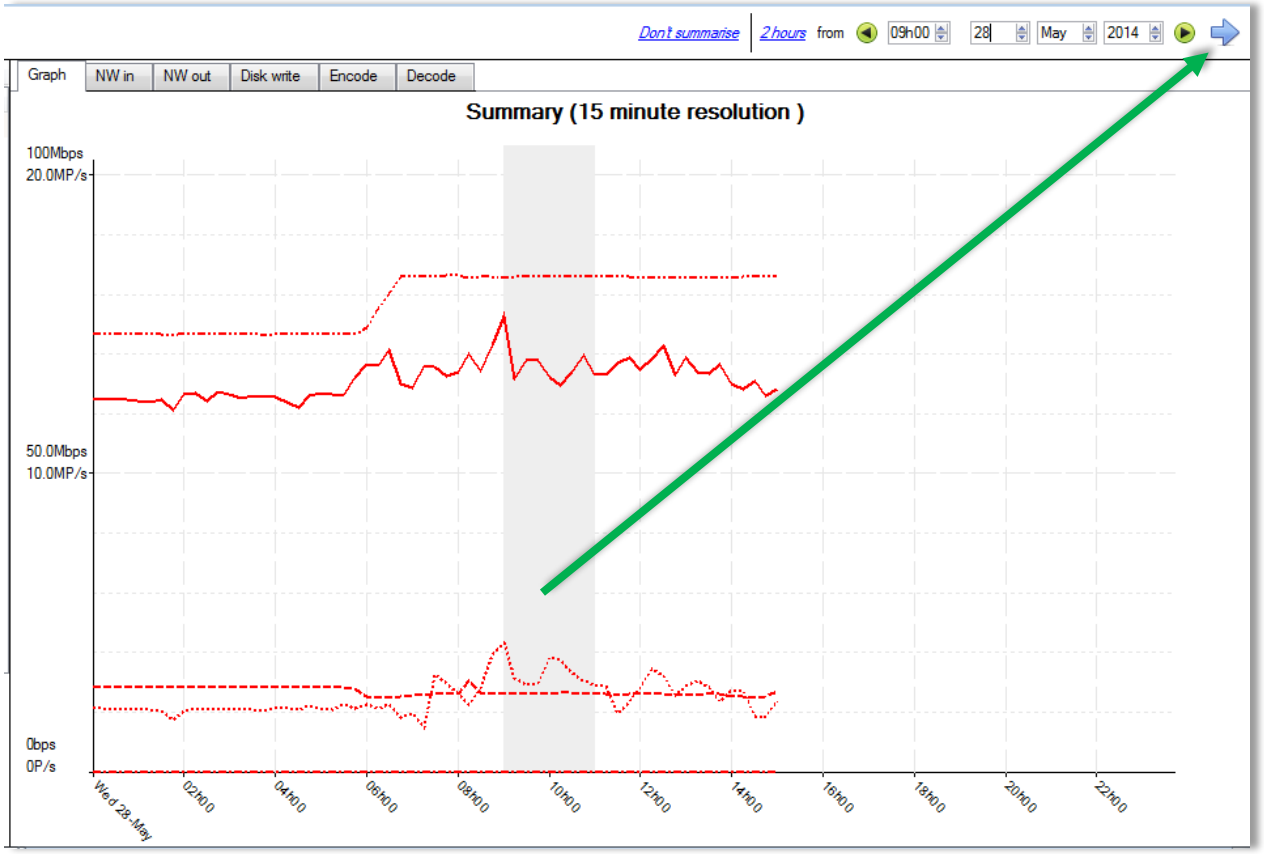
Choose a date, and time, as the starting point for the graph. Then select to fetch data *6 hours* from the selected date/time.

- Time Frame Selection



Or 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.

d. Graph Window

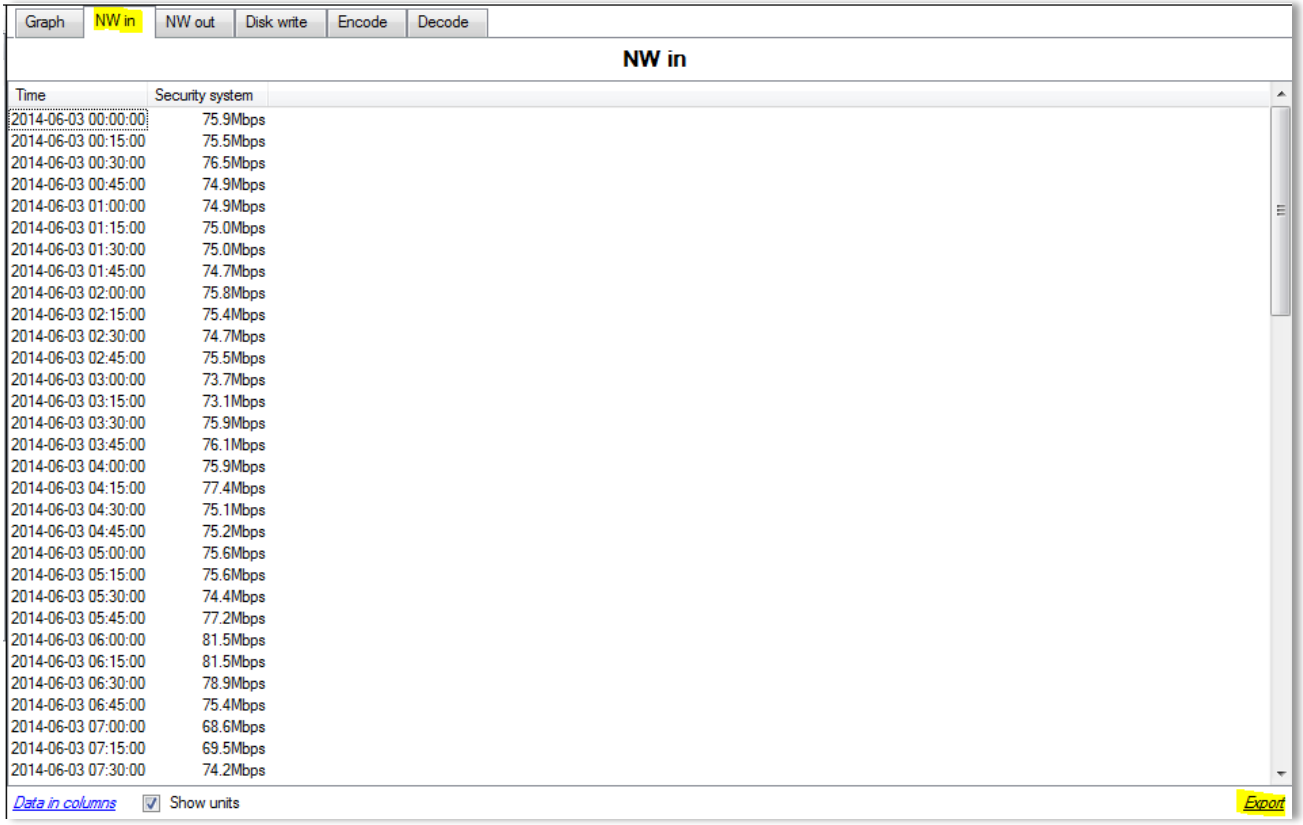


- Zoom in on a Period

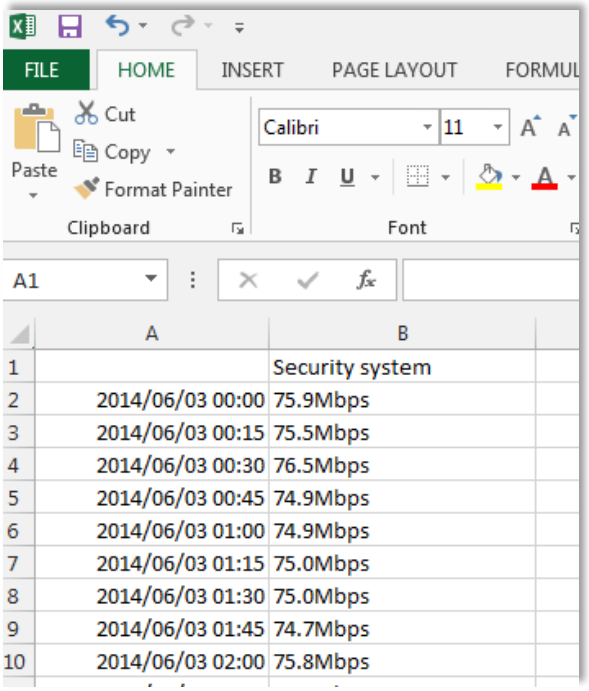
Zoom in on a desired period by holding down the left mouse button, at the starting or ending point, and move the mouse right or left. The selected areas colour will become grey. One can zoom in on the selected area by selecting the blue arrow ( ). This will give a detailed view of the zoomed-in time period:

- See the Data Values

One can get to the actual data values for the various data sets by selecting the “NW in” column as shown in the example below:



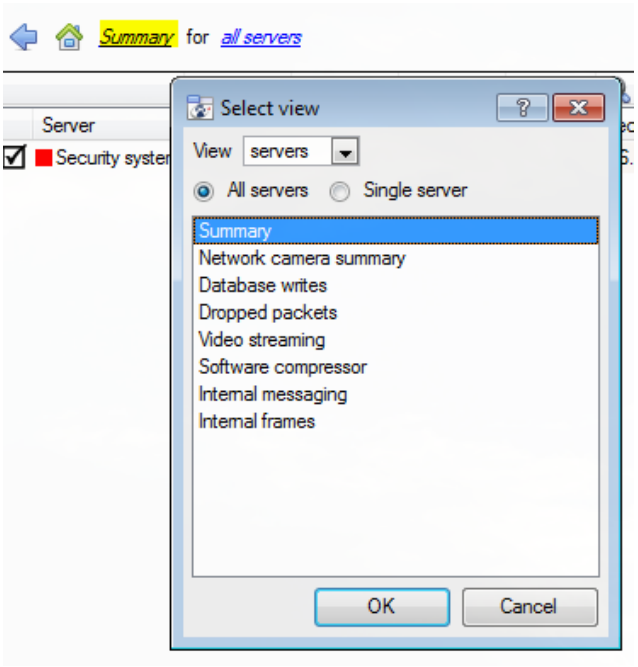
- Export as a Comma Separated Values (CVS) file



One can also export the data to a CVS file. See bottom right “Export” shortcut highlighted in yellow. Also choose to disable the “Show units” option below if one only needs to import the actual data into Excel. See below the exported CVS file opened in Excel.

e. Selected Views

- 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, to choose from. The “X axis” or data sets available for the viewing options is discussed. Select to view data for all servers, part of the Site, or a single server.

- 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.

- 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.

- 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.

- 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.

- 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.
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.

- Internal Messaging

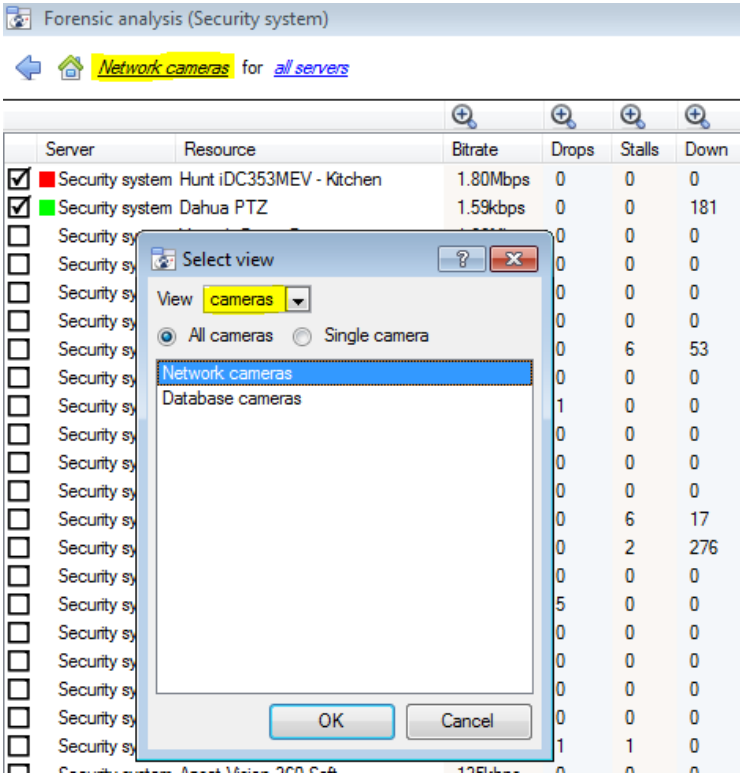
Variable	Unit	Descriptions
Missed	Number	How many UDP packets between processes have been dropped, hopefully 0.
Received	Number	How many UDP packets have been sent between processes.
Logs	Number/min	How many logs have been sent to the logger per minute.

- Internal Frames

Internal frames passed between internal processes.

Variable	Unit	Descriptions.
Missed	Number	Video frames dropped.
Received	fps	Received video frames.

- Network Camera View, of Cameras



Change the Servers view to “Network cameras” by first selecting the “Cameras” View option as shown below. This will present 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”.

- 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.

- Database Cameras

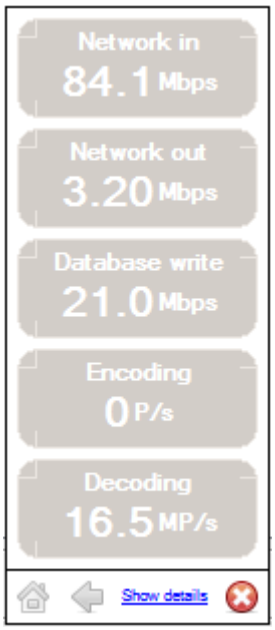
Variable	Unit	Descriptions
Bitrate	Mbps	Total bitrate of selected cameras.
Bytes to disk	Bytes	Bytes written do disk.
Down	Number	The number of seconds the selected cameras have been down in a time bucket. So, if the bucket is 15 minutes, expect it to be around 900 if it was down for the whole time.

- Events View, of Cameras

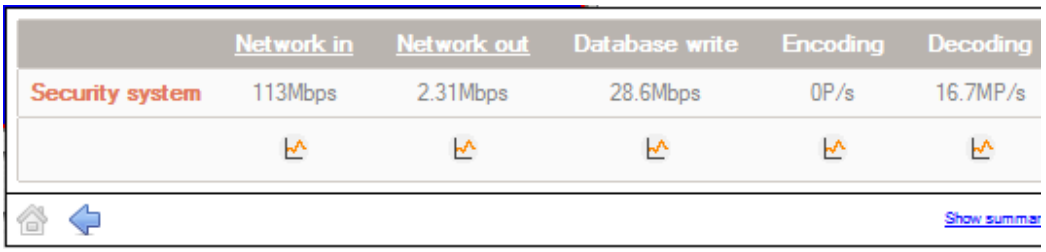
Variable	Unit	Descriptions
Event Count	Number	Number of events per camera for the selected period.

f. Quick View

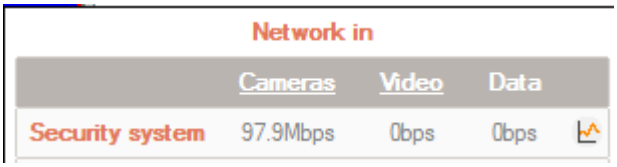
Quickly access performance information from the **CathexisVision** interface. In the bottom right-hand corner there will be the icon. Left-click on this icon.



Clicking on the icon will cause the image to the left will appear. This shows live information about the system. Click on Show details and it will become the image below. Detailed information can be looked further into 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 pertaining to network traffic.



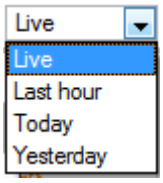
For example, clicking on **Network in** reveals the following:



- Graphing the Quick View Data.

Graph any of the information in this quick view by clicking on the relevant icon. During viewing, the graph the icon will change to .

- 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.

- Multiple Graphs

View multiple graphs by disconnecting the current graph. This is done by clicking on the  icon, found at the top right of the graph window.

g. Examples of How to Interpret the Graph and Columned Values

- 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 will allow plotting the disk writing graph, exclusively, on the right-hand side. Select the period “Today” (highlighted in yellow) for the disk writing throughput.

Move the mouse to the left plane, away from the graph, and the columned values on the left would be the **average disk writing throughput** for the selected period. 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 (below).

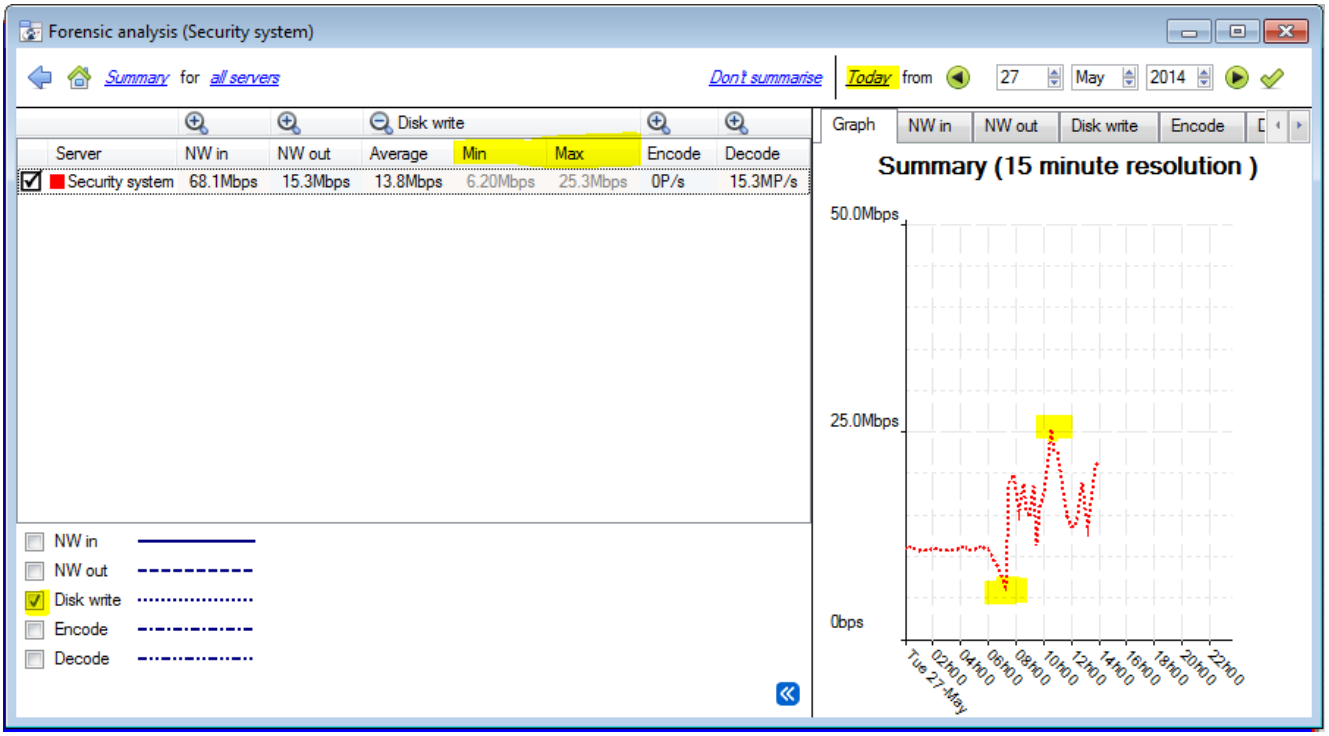


Figure 2

Note: These 2 examples are just the process to filter out required information. Other system data can be retrieved in a similar fashion.

- Example 2: Investigate Network Loss Issues on Selected Cameras
- Scenario

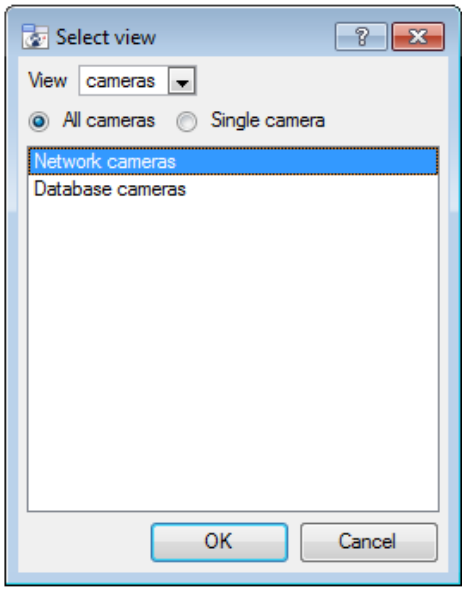
The client has indicated that the live camera views on selected cameras are tearing and there are recording gaps. The camera resources on the right-hand side of the **CathexisVision** indicates low, moderate and high packet loss. The forensic tool can help highlight the times when the packets failed, and also the magnitude.

The Forensic tool is **only one** of the possible tools used 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. Also 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. Make sure the camera firmware is eliminated, or rule this out.

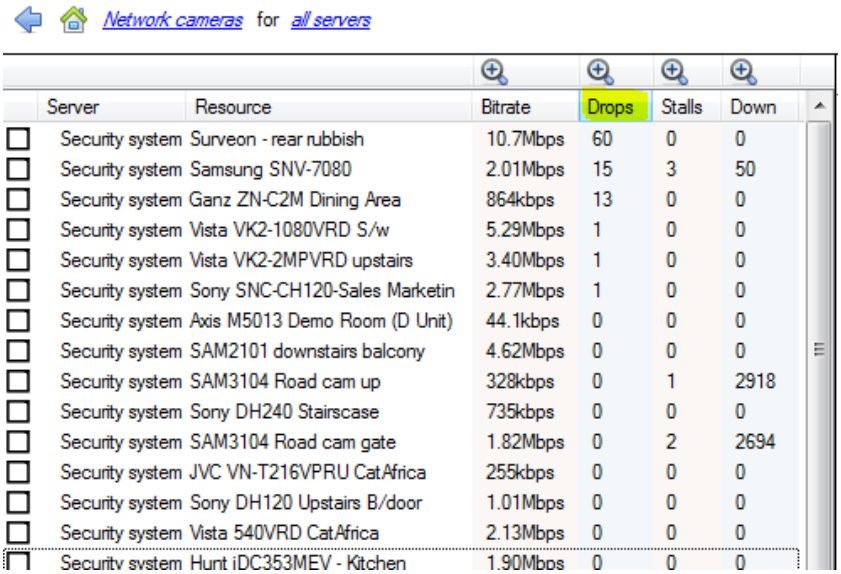
- Method

1.) Change the view to "**cameras**", and then select "**Network cameras**" from the list:

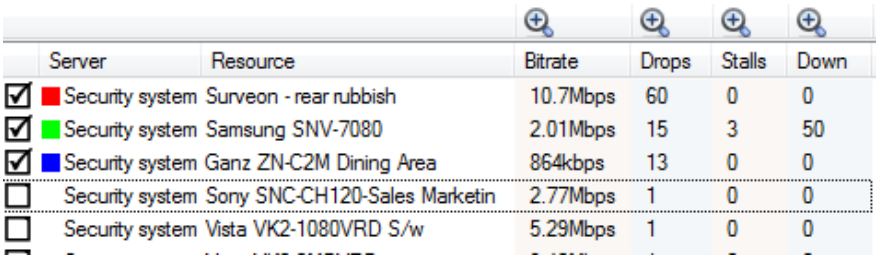


2.) To inspect packet loss on all the cameras for the last day, change the period selector to display "**Yesterday**":

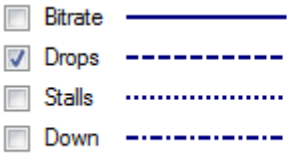
3.) Sort the dropped packets on the left-hand column view, by clicking on the "**Drops**" column header, as indicated below in yellow:



4.) In order to graph the cameras, select them on the top left-hand side. Here, look at the first 3 cameras:



5.) One only needs to view the network “**Drops**”, on the selected cameras. So, 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: