Wavestore

Video Management Software

User Manual

Version 6.46

Wavestore Global Limited
Waterside House
Riverside Way
Uxbridge, UB8 2YF – UK

For Technical Support
P: +44 (0)1895 527 127
E: support@wavestore.com
W: www.wavestore.com

Contents

1 Introduction

1.1 About This Document

This document is about the Wavestore suite of software. It doesn't cover the hardware on which the software may be running. Separate documentation is provided for the various hardware ranges available.

The first part of the document explains the basics of the Wavestore system and how to get started.

The next part focusses on the main user interface and how to use an already configured system. This covers the Main Screen, the Find Screen, making and playing back exports, etc.

Next there is a reference section about the Setup Screens. This covers each Setup Screen and explains what each item on each screen does.

Then there is a section for "Common Setup Tasks and Concepts". Since some common tasks require several steps of configuration across multiple screens, this section consists of walkthroughs for those common tasks, along with some sections which explain important concepts in the Wavestore system.

1.2 About Wavestore

The Wavestore Video Management Software (VMS) provides the perfect hybrid digital video recording solution for users who may wish to deploy a combination of analogue, IP, megapixel, HD, HD-SDI, thermal, panoramic and 360 degree cameras. Robust and reliable, the Wavestore VMS is able to meet the requirements of virtually any video surveillance project, including airport, casino, bank, retail, commercial, industrial, homeland security and government applications.

Wavestore VMS is ONVIF Profile S certified, ensuring compatibility and compliance with this industry standard as it evolves, and enabling industry consultants, systems integrators, installers and end-users to select conformant cameras with the knowledge that compatibility is assured.

High performance and flexible recording

Easy to install and operate, the Wavestore VMS software is able to simultaneously record up to 254 channels with a combination of H.265, H.264, MPEG-4, MJPEG, JPEG2000 or MxPEG compression formats. Up to 8 HD-SDI cameras can be specified at the time of the order. Up to 255 servers per location are supported, and options to support unlimited sites and unlimited users are available.

The Wavestore open architecture design enables straightforward integration of video analytics and third party technologies, including Command and Control, PSIM, Perimeter Intrusion Detection (PID), Building Management System (BMS), Access Control, People Counting, retail analytics, licence plate recogni-

tion, Electronic Point of Sales (EPOS) and Scanning systems. Biometric Facial Recognition systems are also available, delivering high integrity solutions to assist in identifying various individuals; whether VIPs, regular customers, staff or black–listed persons.

Easy to use

Wavestore remote viewer client software (WaveView) allows users to securely monitor real–time live images or retrieve recorded video over the network, whilst multiple recorders can be configured into a server group to support large and distributed video surveillance applications. Image authentication and encryption are also available.

Simple drag and drop functionality enables each user to create unique multiple display preferences, whilst the Wavestore VMS software delivers an extremely fast search facility to allow users to quickly review recorded images of any occurred event.

Ultra reliable

The Wavestore Linux based server design delivers a high integrity and resilient recording platform, whilst the uncomplicated viewer client software (WaveView) can be operated from Windows (8.1 and later, or Server 2012 or later) and Linux operating systems. A mobile client is also available for Android and iOS platforms.

Wavestore servers have single, dual or triple redundant power supplies options and are provided with up to three year full return to base warranty.

Server and Client configuration

Installed in about 10 minutes on the server system drive, the Wavestore VMS software manages the video, audio and metadata information that is sent from the cameras and devices connected to the server and records onto the storage hard drives.

The Wavestore viewer client software (WaveView) is pre–installed onto the server and provides a wealth of tools for accessing cameras and devices, streaming video and managing events. It can operate on multiple operating systems and is multithreaded to allow maximum performance on multiple CPU cores when displaying video streams.

WaveView can also be installed onto a PC to connect to a Wavestore server over a TCP/IP network and many of the server configuration tasks (e.g. user administration) can be performed remotely, with only a small number required to be carried out on the server itself. If multiple Wavestore servers are configured together as a server group, the operator can easily access via WaveView all cameras and devices from any of the servers within the server group (See figure 1.1).

If multiple Wavestore servers are configured together as a server group, the operator can easily access via WaveView all cameras and devices from any of the servers within the server group.

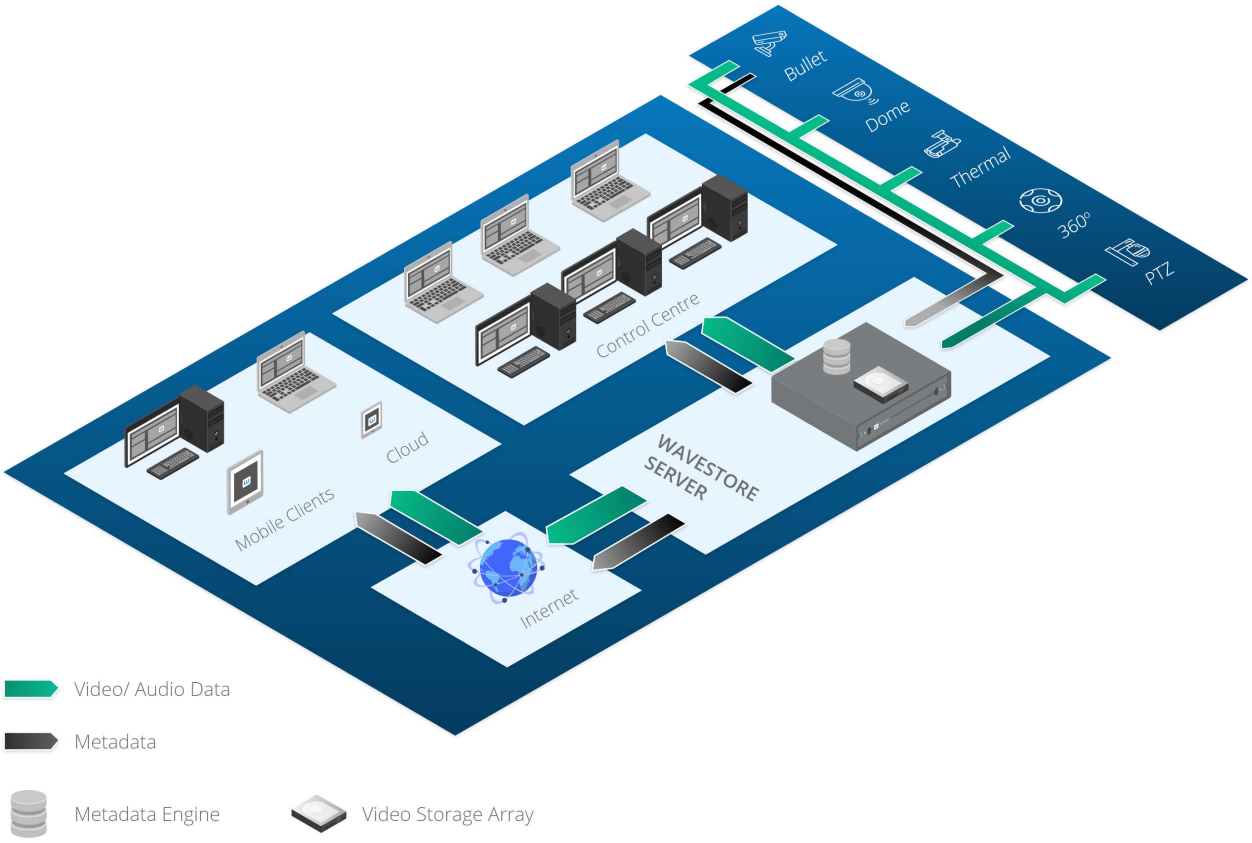


Figure 1.1: Typical System Configuration

Key Features

Video Management Software (VMS)

Video standards NTSC, PAL, HD-SDI and IP

Video resolution QCIF, CIF, 2CIF, DCIF, D1, 720p, 1080p, VGA, megapixel, multi-megapixel, custom Analogue rate at D1 Up to 25/30 fps (PAL or NTSC) per input; up to 1600/1920 fps per recorder IP and HD rates: high image rate streams supported, camera dependent

Still image BMP/JPEG/PNG formats

Record type Continuous, schedule, motion, alarm, event and digital input trigger

Recording tracks 3 independent video tracks assignable to different HDDs, each with independent settings plus a Metadata track

Overwrite modes Configurable auto deletion and overwrite function by time or disk allocation

Privacy Mask Configurable mask to avoid viewing sensitive areas within a camera view

Time zone regional setting available

Languages multiple languages supported

Operating system embedded Linux platform

Client Software (WaveView)

Remote users 2 to unlimited concurrent users

Operating Systems Windows (8.1 and later, or Server 2012 or later) and Linux (Red Hat and Debian based systems)

Mobile client support for Android and iOS devices

Find and display instantaneous and simultaneous display of live and recorded images

Video displays user configurable by image size, aspect ratio and position

Video displays layouts standard and customisable layouts with saving option per user

Playback, Search and Export

Playback options linear and logarithmic search options with variable speed sliders

Playback speed up to 8192 times the normal view rate

Playback mode multi-way (play, rewind, jump, fast-forward and frame-step multiple cameras simultaneously)

Playback display synchronise and replay all camera images

Slow motion playback available

Search options date, time, annotations, motion, alarm, events

Search mode full speed, full frame search

Export mode export multiple cameras simultaneously, including linked audio

Live video export available

Export devices CD, DVD, USB, HDD

Advanced exports ability to transcode video and audio data to large number of alternative formats (i.e. AVI, WMV, MPEG, MP4)

Security

Password profile multiple protection levels

Cameras and displays accessible on a per-user basis

Configuration files save and restore capability for any recorder in the group

Digital watermarking image authentication with real time checking

Encryption up to 4096 bit encryption

Diagnostics remote and secure diagnostics, repair functionality available – Optional

Remote administration remote control via TCP/IP network, including restart and rebooting

Automatic system restart after power loss (when power resumes)

Monitoring full system monitoring, including SMART disk health monitoring – Optional

Failover ability to switch to a standby recorder upon the abnormal termination of another recorder in the same system – Optional

Watchdog function auto-reboot of system in case of system failure

Redundant recording NAS, SAN and RAID options

Events and alarms

Advanced events shows a real time stream of incoming events and alarms on the main window

Event detection any third party technologies events and alarms, video loss, darkening, motion within image, camera movement, camera tamper, digital input, login succeeded, login denied, fault, warning

Event management customisable display and sound, definable search, and instant response options

Event actions record on event, text overlay, boost recording rate, trigger output, spot monitor, PTZ camera on preset, notify client, run script, emails, flashing light, sound alerts

Event notification via WaveView, email or TCP/IP message

Other features event logging, enable and disable on schedule

Motion Mask/Areas of interest configurable areas to target analogue analytics

Licensable Features

De-warping for any 360 degree cameras provides customisable linear views of live and archived images and the ability to recall a total field of view and follow subjects as if tracking with a PTZ camera, creating ad hoc video clips around the occurred events

Interactive Maps configurable map screen for finding and interacting with cameras and devices

HTTP proxy server enables direct interface with cameras when on a different network

Optional modules

Third party integration ability to translate any third party events and trigger a wide range of definable actions based on customisable rules

Facial recognition ability to interface with biometric facial recognition systems to dynamically compare images of individuals from incoming video streams against specific databases and immediately send alerts when a positive match occurs

Intelligent Video Analytics (IVA) ability to integrate with any video analytics allowing specific types of events and activities to be recognised automatically and promptly alarming the operator directly within the user interface when an event occurs

People counting delivers accurate metrics to monitor people flow, people tracking and queue management, efficiently improving customer service and sales performance

Point of Sales (POS) ability to display text from POS devices alongside associated video images providing transactions search options

Automatic Number Plate Recognition (ANPR/LPR) ability to register the arrival time of service vehicles and permit access to authorised vehicles to restricted areas

2 Getting Started

2.1 Basic System Configuration

The Wavestore system consists of two main components:

- Wavestore server software, responsible for managing and recording streams from input devices (audio and video)
- WaveView client software; provides a user interface to the Wavestore server software, for functions such as Live View/Search/Playback, and also server configuration

A Wavestore server usually runs both the Wavestore server software, and the WaveView client software, although in some circumstances, a textual client is offered instead of WaveView.

WaveView can also be installed on Linux and Windows PCs, and used to access networked Wavestore servers. WaveView running on the Wavestore server box can also be used to access other Wavestore servers in the same manner.

Servers are shipped with both the Wavestore server and WaveView client programs pre-installed, with only minimal configuration required before the server is ready for use.

Certain server configuration tasks can only be undertaken when working on the server box itself (client connects to the local host), but the majority of configuration tasks can be carried out on either the server box or a client software PC.

When installing a remote client, it is recommended to use the same base version of WaveView client as the server, or higher. By "base version" we mean the first two numbers in the version, for example the base version of "6.14.51" is "6.14". So for example if the server is running version 6.16, the WaveView client version should be 6.16 or higher.

2.2 Login Screen

Following the menu path File → Connect calls up the Login Dialog Box, which allows the operator to log in to a Wavestore Server or Server Group as follows:

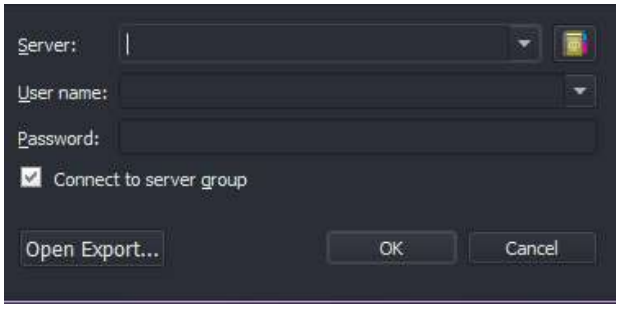


Figure 2.1: WaveView Login Dialog

- in the server field
  - if you are working directly on the Wavestore server box, enter 'localhost'
  - if you are working remotely from a client PC, enter the IP address or hostname of the server
- in the user field, enter a valid user name (for example 'install')
- in the password field, enter the corresponding password for your selected user. The default password for the install user is 'a'.
- if you are connecting to a server that is part of a server group (section 6.8 – Server Group), leave the 'connect to server group' option checked; your client will connect to all of the servers within the server group

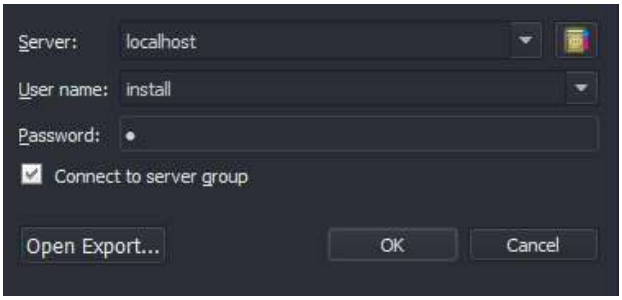


Figure 2.2: Entering data in WaveView login screen

A user will become locked if the password was entered incorrectly 5 times in a row. In this case the username will be locked for 30 minutes, and all attempts to log in will be rejected with "Locked" error message. Either wait for 30 minutes or log in using another username.

In the event that the configured IP address on the server clashes with the IP address of another device on the network, you will not be able to login on the server box using the server name 'localhost'. In the 'Server' field, replace 'localhost' with the IP address 127.0.0.1, and login as above.

Upon first login for any given user, that user may be forced to change their password. If the user does not do so and attempts to cancel the password change, the WaveView application will exit.

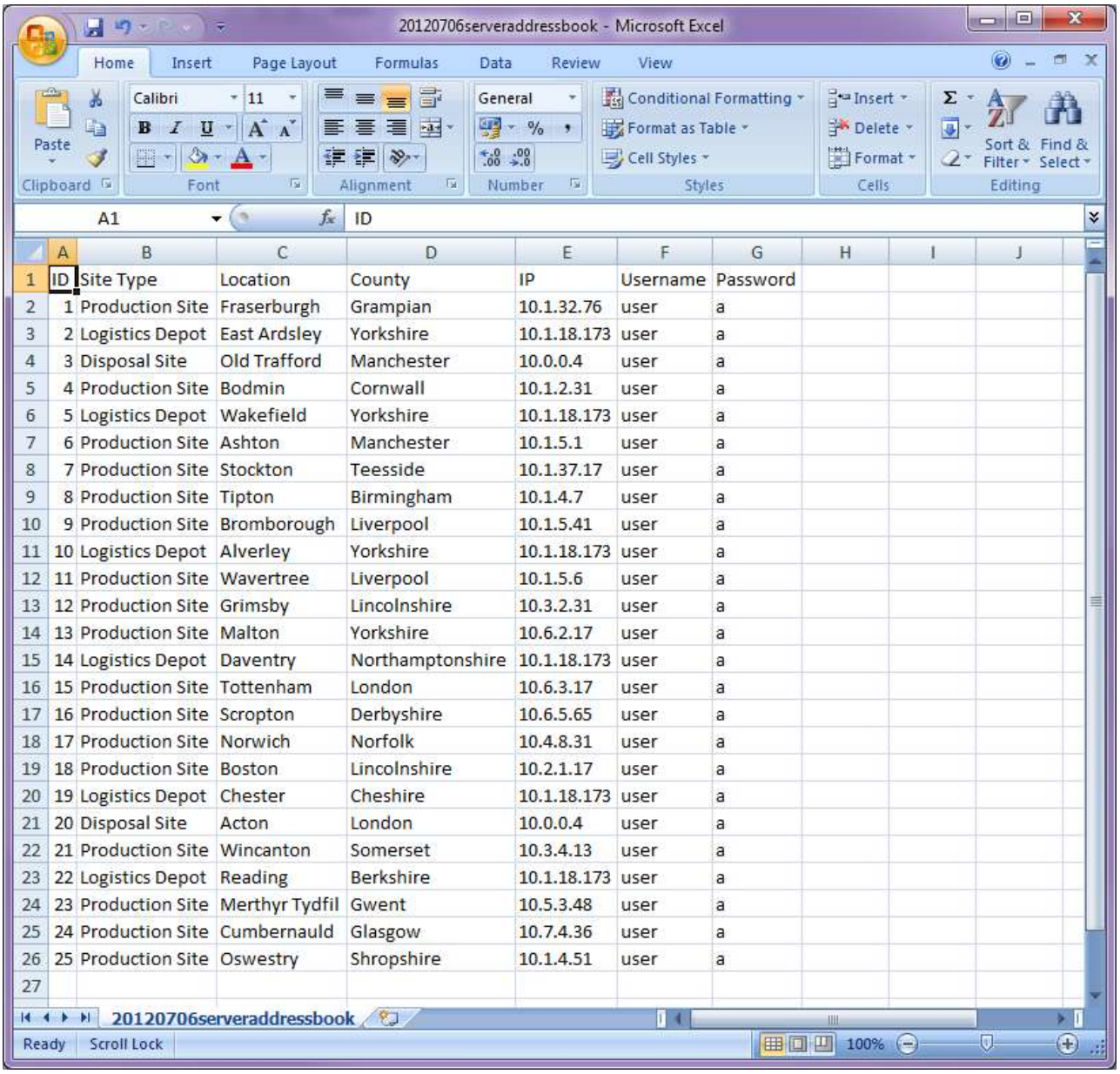
Section 6.2.2 – Network describes how to reconfigure the server IP address in the Network menu, if required.

The 'Open Export' button is used to open a locally saved export file for playback, as described in section 5.1 – Playing Back Exported Files on a PC from DVD/USB device.

For a WaveView installation on Windows PC, the Login Dialog box can be associated with a CSV file (on a local PC or networked resource) that can act as a server 'address book'. This file can contain user configured details such as site location, IP address, and optionally login details such as user name and password.

This feature can be useful for a client installation that is used to connect to Wavestore servers at multiple sites.

A CSV file can be created using Microsoft Excel; an example is shown below:



	A	B	C	D	E	F	G	H	I	J
1	ID	Site Type	Location	County	IP	Username	Password			
2	1	Production Site	Fraserburgh	Grampian	10.1.32.76	user	a			
3	2	Logistics Depot	East Ardsley	Yorkshire	10.1.18.173	user	a			
4	3	Disposal Site	Old Trafford	Manchester	10.0.0.4	user	a			
5	4	Production Site	Bodmin	Cornwall	10.1.2.31	user	a			
6	5	Logistics Depot	Wakefield	Yorkshire	10.1.18.173	user	a			
7	6	Production Site	Ashton	Manchester	10.1.5.1	user	a			
8	7	Production Site	Stockton	Teesside	10.1.37.17	user	a			
9	8	Production Site	Tipton	Birmingham	10.1.4.7	user	a			
10	9	Production Site	Bromborough	Liverpool	10.1.5.41	user	a			
11	10	Logistics Depot	Alverley	Yorkshire	10.1.18.173	user	a			
12	11	Production Site	Wavertree	Liverpool	10.1.5.6	user	a			
13	12	Production Site	Grimsby	Lincolnshire	10.3.2.31	user	a			
14	13	Production Site	Malton	Yorkshire	10.6.2.17	user	a			
15	14	Logistics Depot	Daventry	Northamptonshire	10.1.18.173	user	a			
16	15	Production Site	Tottenham	London	10.6.3.17	user	a			
17	16	Production Site	Scropton	Derbyshire	10.6.5.65	user	a			
18	17	Production Site	Norwich	Norfolk	10.4.8.31	user	a			
19	18	Production Site	Boston	Lincolnshire	10.2.1.17	user	a			
20	19	Logistics Depot	Chester	Cheshire	10.1.18.173	user	a			
21	20	Disposal Site	Acton	London	10.0.0.4	user	a			
22	21	Production Site	Wincanton	Somerset	10.3.4.13	user	a			
23	22	Logistics Depot	Reading	Berkshire	10.1.18.173	user	a			
24	23	Production Site	Merthyr Tydfil	Gwent	10.5.3.48	user	a			
25	24	Production Site	Cumbernauld	Glasgow	10.7.4.36	user	a			
26	25	Production Site	Oswestry	Shropshire	10.1.4.51	user	a			
27										

Figure 2.3: Example CSV file

Once associated with the CSV file, WaveView will use the data on Line 1 as column headings in the Server Search screen, as shown below.

To associate the CSV file with WaveView, click on 'Search' on the Login Dialog screen, and in the Server

Search screen that appears, click 'Browse', and locate your saved CSV file:

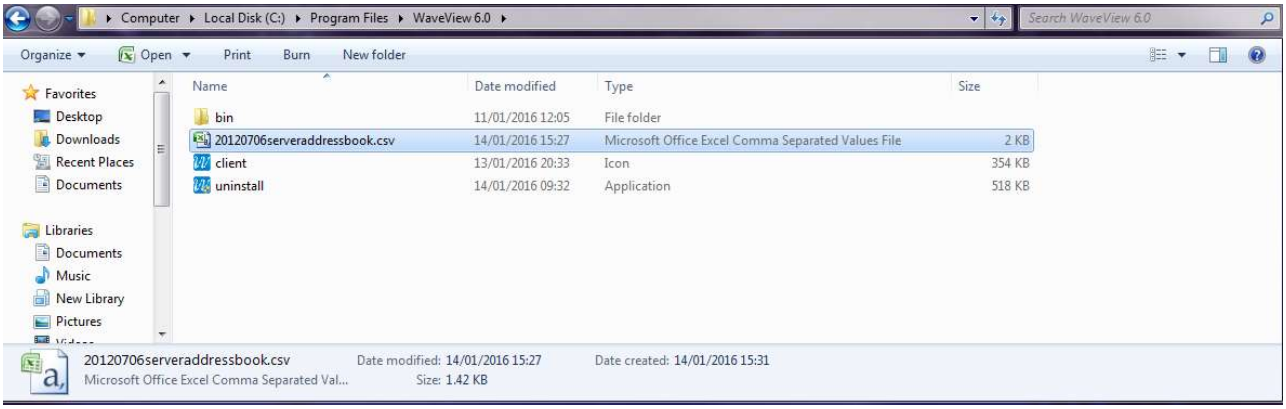


Figure 2.4: Browsing to locate CSV file

The contents of the CSV file will now be loaded by WaveView:

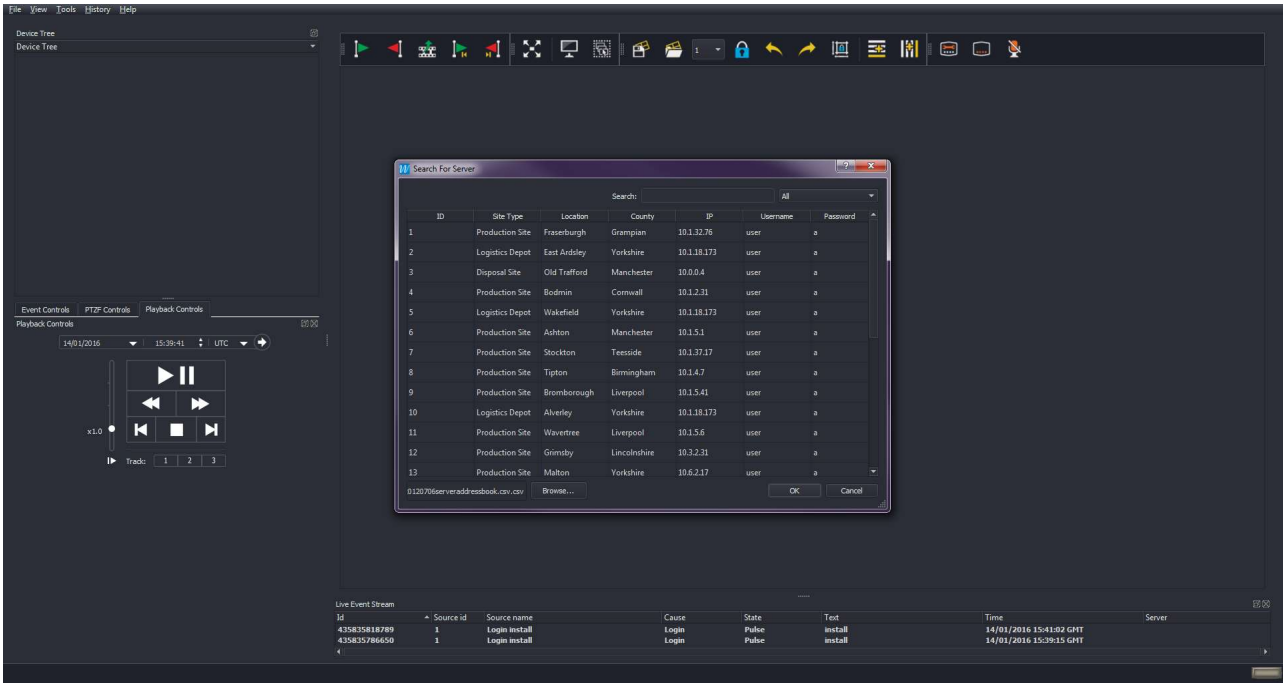


Figure 2.5: CSV File loaded into WaveView as 'address book'

You can search the list manually to select a server by using the side slider bar, or by entering text into the 'Search' field:

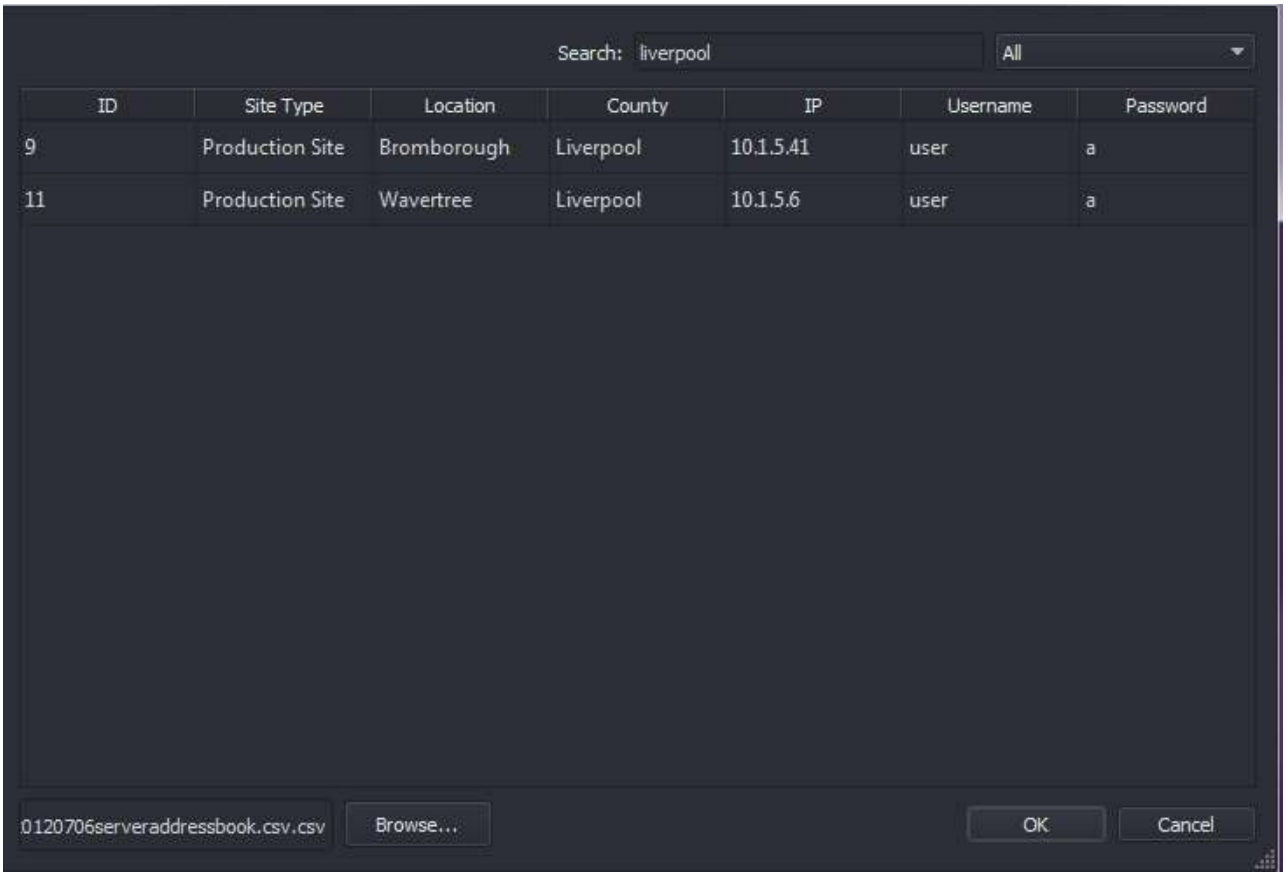


Figure 2.6: Searching address book for text 'liverpool'

You can also click on the category headings to sort the listed sites according to the data in the selected column:

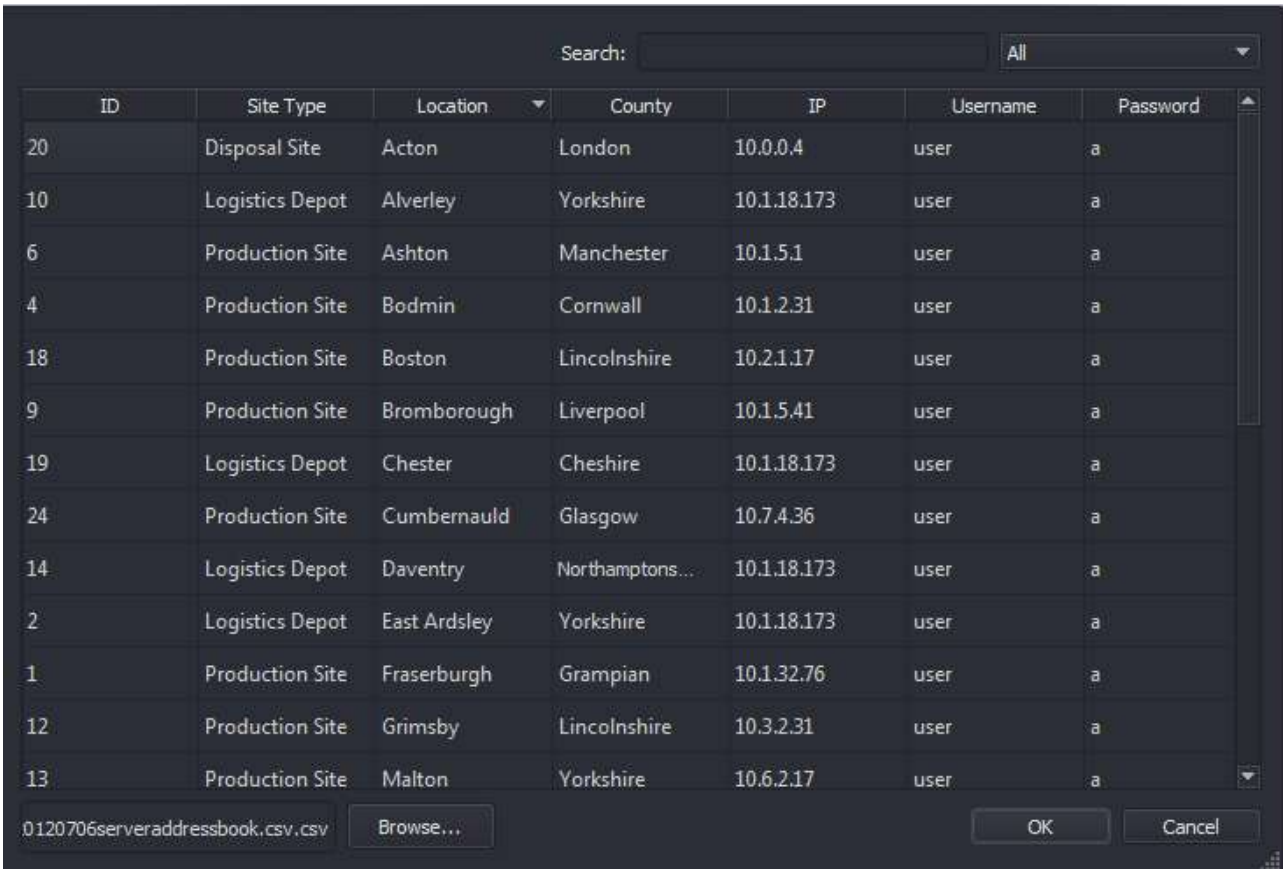


Figure 2.7: Sorting address book using 'Location' data

Once you have located the server that you require, double click on the server entry in the list, and the fields in the Login Dialog box (including User Name and Password if this data is contained within the CSV file) will be auto populated.

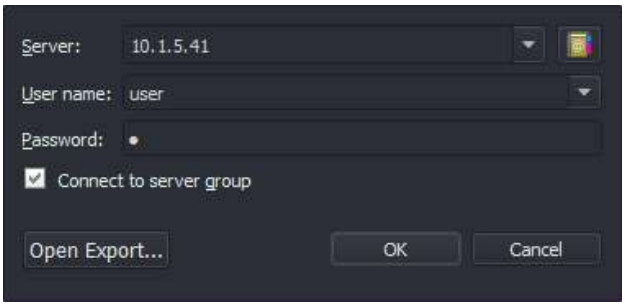


Figure 2.8: Auto population of Login Dialog

Click on ***OK*** to connect to the server.

Once the Client has connected to the server(s), the Device Tree will appear showing a representation of the connected Wavestore server(s), with any active audio/video channels that the user has permission to access.

If you are connecting to a new server, no audio/video channels will be displayed in the Device Tree until

these channels have been configured and enabled (see section 9.3 – Configuring Analogue Cameras, or section 9.1 – Configuring IP Cameras).

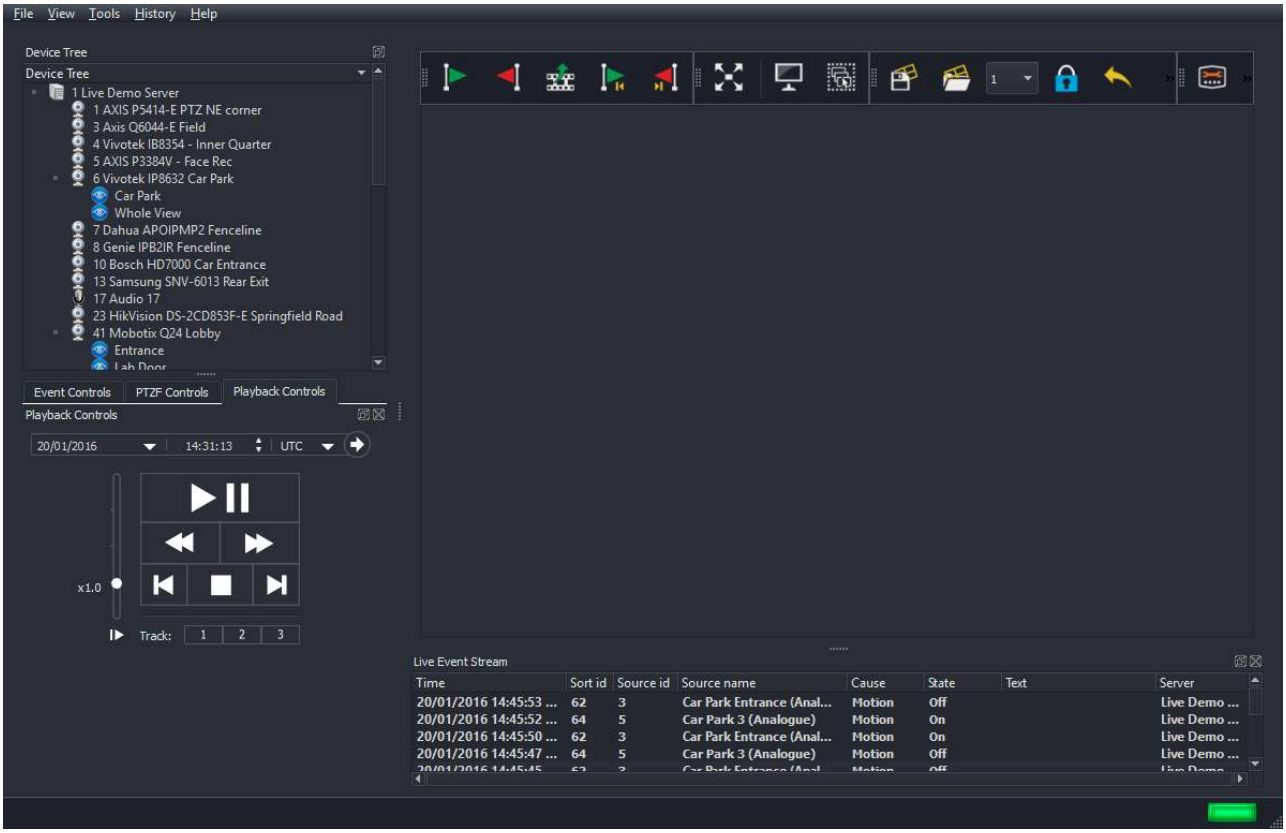


Figure 2.9: Main operating screen showing Device Tree

2.3 Shutting down the Server

To shut down the Wavestore server, follow the menu path View → Setup → Server → Shutdown System:

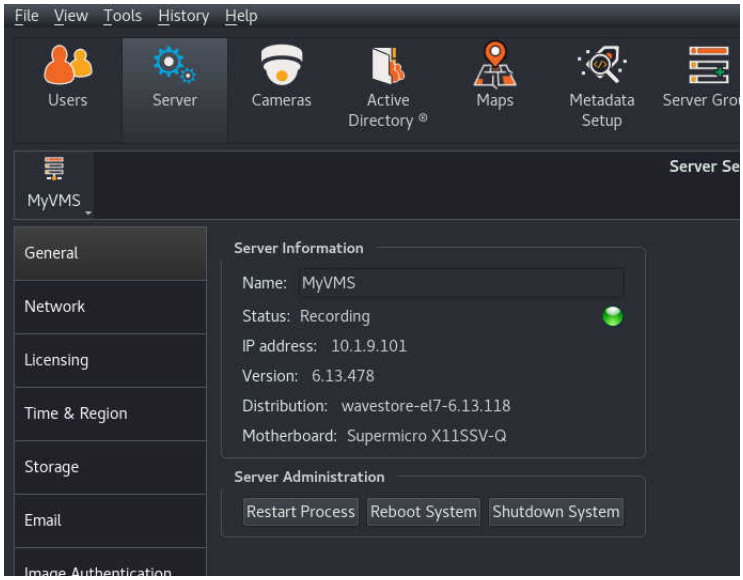


Figure 2.10: Shutting down the server from WaveView

It is acceptable to shut down the Wavestore server (either in an emergency or for routine maintenance) by switching the server off using the switch on the rear of the chassis, by removing the power lead or by switching the mains supply off at the power outlet.

The Wavestore software is designed to be robust when power fails unexpectedly, and no data is lost (other than the last second or two which might not have been flushed to disk). The Wavestore server will recover and fully check its storage in less than a second when power is reapplied. There is no need for external UPS devices.

If your Wavestore server is connected to an external RAID device, then other shutdown rules might apply to this RAID device. Many RAID boxes do require UPS protection, and must be powered down in an orderly fashion.

3 Main Screen

The Main Screen (menu path View → Main) is shown below:

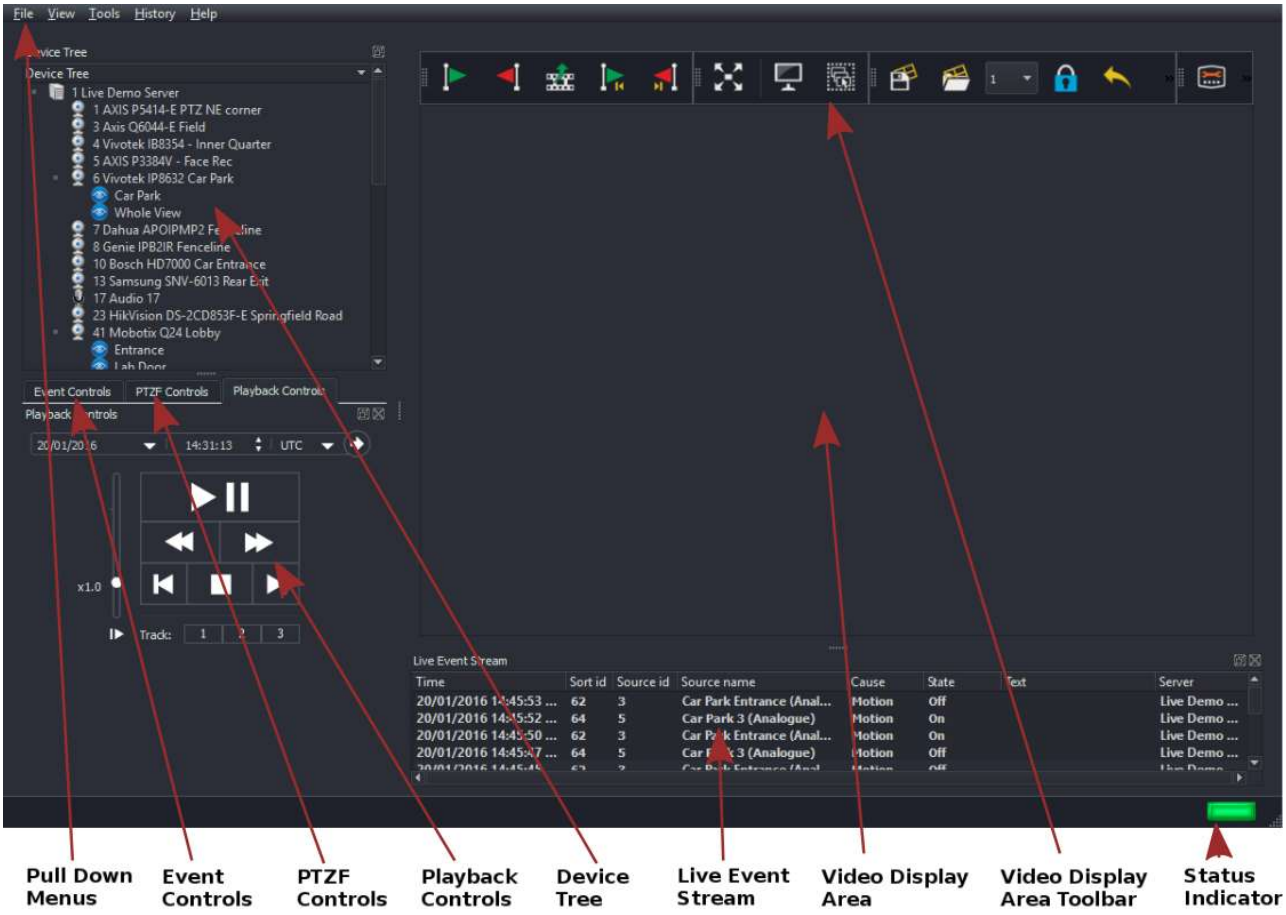


Figure 3.1: WaveView Live Screen

Pull Down Menus File/View/Tools/Help. See section 3.1 – Pull Down Menus.

Device Tree Displays a list of the connected Wavestore servers, with active audio/video channels. See section 3.8 – Device Tree.

Event Controls Start/Stop operation of configured Event Rules. See section 6.12 – Event Rules.

Playback Controls Used to control playback of Video Displays. See section 3.10 – Playback Controls.

PTZF Controls Used for control of Pan/Tilt/Zoom cameras. See section 3.12 – PTZF Controls.

Live Event Stream (Licensed upgrade) Licensed upgrade; displays events from connected devices. See section 3.18 – Live Event Stream (Optional Licensed Upgrade).

Display Area Video Displays from system cameras can be added here. See section 3.2 – Display Area.

Display Area Toolbar Used for controlling individual Video Displays. See section 3.3 – Display Area Toolbar.

Status Indicator Normally displays Green, changes to Red when a connected server has reported a fault – clicking on this icon will causes a new window to open displaying the System Log (See section 3.21.1 – System Log)

The main screen contains "dockable" panels which can be dragged from their dock positions to become floating panels. These panels can also be closed if not used.

If any or all of the panels "Event Control", "PTZF Controls", "Playback Controls" are closed, they can be reopened by right–clicking on the "Device Tree" heading.

If the "Live Event Stream" panel is closed, it can be reopened by clicking the dots at the bottom of the Video Display Area and dragging upwards, then right–clicking on the space below.

Once Video Displays have been added to the Display Area, the Main screen will typically appear as below.

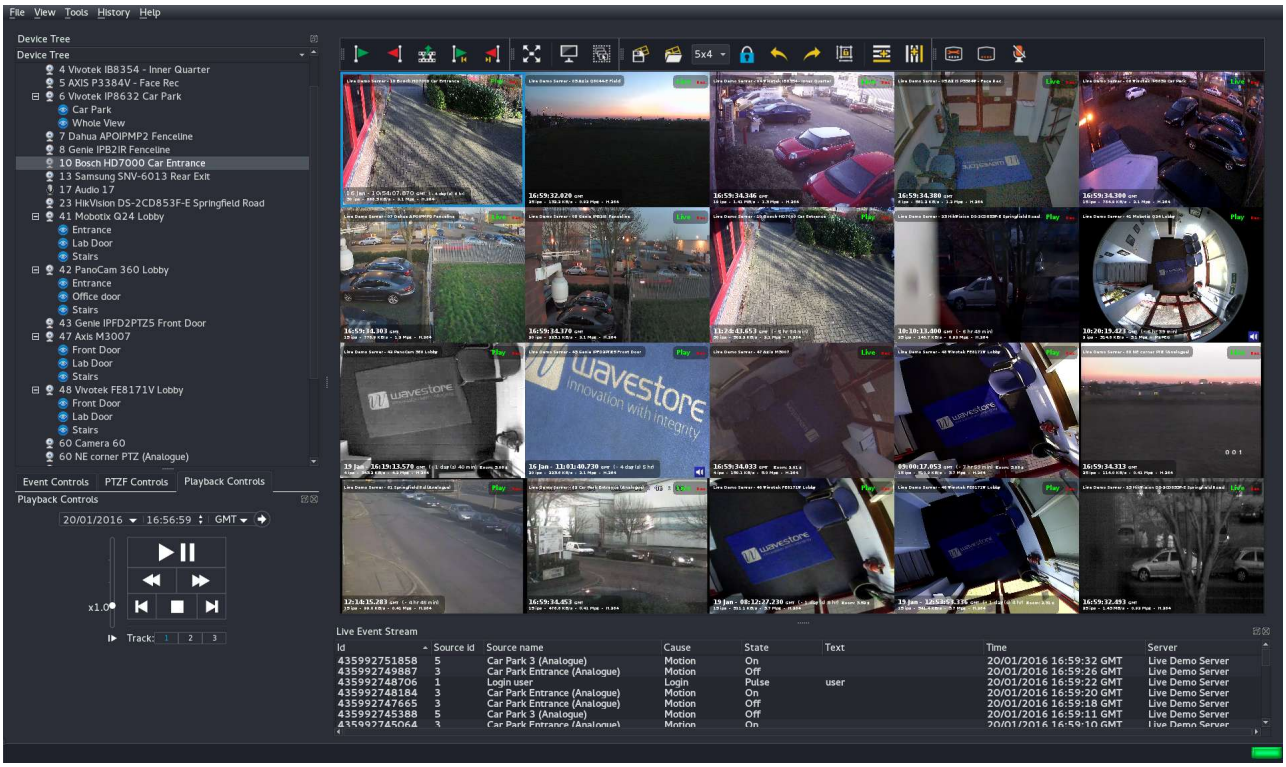


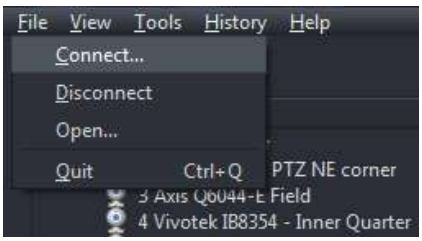
Figure 3.2: WaveView Main Screen with Video Displays Added

The Display Area can be freely configured, with a mixture of Live and Playback camera views if desired. Multiple instances of the same camera can be displayed, showing playback from different dates/times simultaneously.

3.1 Pull Down Menus

The pull down menus contain the following items:

3.1.1 File Menu



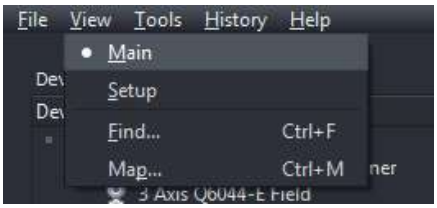
Connect Open the Login Window in order to establish a new connection to a Wavestore.

Disconnect Disconnect from the currently connected Wavestore Server, Server Group, or Export File.

Open Open an Export File.

Quit Exit the WaveView clientSoftware

3.1.2 View Menu



Main The Main Screen containing the Display Area

Setup For configuring the Wavestore Server or Server Group, including...

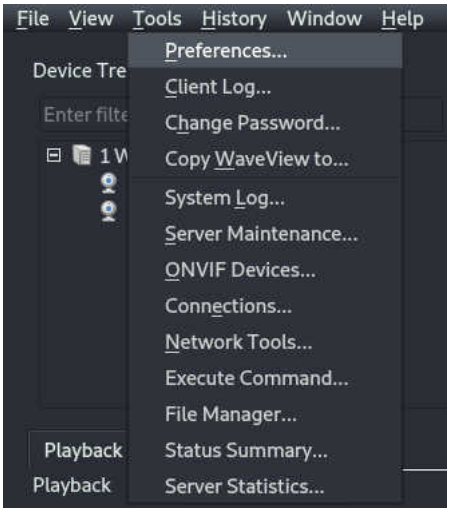
- Administration of User Logon ID/password
- Recording settings for Audio and Video Devices
- Spot Monitor output from Server for analogue cameras
- Server Time/Date and Time Zone
- Server IP settings
- Email of event notifications
- Schedules (can be attached to User logons/Camera Recording)
- Custom Channel Tree Groups of cameras
- Upgrade of server software
- Event Rules associating input devices/events with output devices/events

- I/O Devices (digital inputs, relay outputs etc.)
- Notification Targets for messages sent by the server
- Configuration of Video Storage Hard Drives

Find Search and Export Recorded Footage

Map View Camera Maps Configured on the Server (Licensed Option)

3.1.3 Tools Menu



Preferences Configuration Options relating to the client PC. See section 3.22 – Preferences.

Client Log Log of Events within the WaveView client. See section 3.21.3 – Client Log.

Change Password Allows password of the current user to be changed.

Copy WaveView to Creates a separate copy of the program in a user nominated folder (for playback of exported files). See section 3.24 – Copy WaveView.

System Log Log of Events on the connected Server(s). See section 3.21.1 – System Log.

Server Maintenance For advanced configuration use as directed by Wavestore staff. See section 3.25 – Server Maintenance.

Connections List of Clients currently connected to the servers (User ID and IP Address). See section 3.23 – Connection List.

Network Tools Allows network connectivity to other devices to be checked. See section 3.20 – Network Tools.

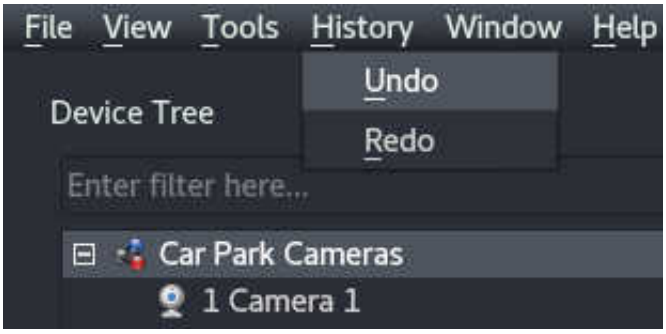
Execute Command Used for Advanced Functions under direction of Wavestore staff

File Manager Allows uploading, downloading, and deletion of files to and from the servers in the server group. See section 3.26 – File Manager.

Status Summary Provides a summary, including thumbnails, of all cameras in the server group. See section 3.27 – Status Summary.

Server Statistics Provides visual representation of statistical data relating to server performance, such as network throughput and disk activity. See section 3.28 – Server Statistics.

3.1.4 History Menu

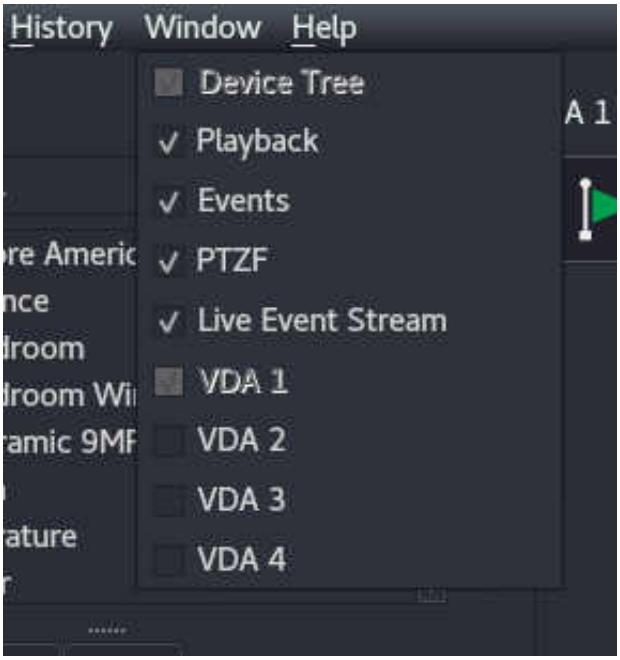


Undo Reverts the last change to the layout in the currently selected Video Display Area

Redo Re–applies the last "undone" change to the layout in the currently selected Video Display Area

Note that the layout history is limited to 50 layout change operations.

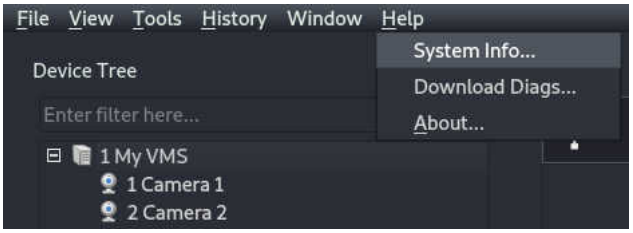
3.1.5 Window Menu



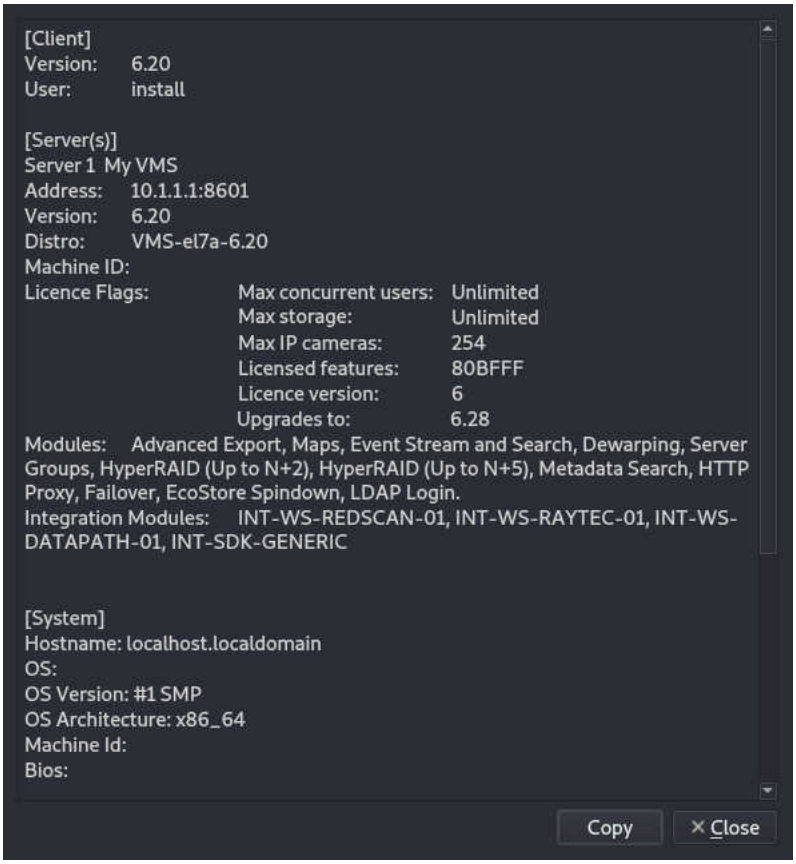
Each entry in this menu corresponds to an element in the UI which can be shown or hidden. For example the "Live Event Stream" can be hidden to make more space for the main Video Display Area.

Also it allows multiple Video Display Areas to be enabled or disabled.

3.1.6 Help Menu

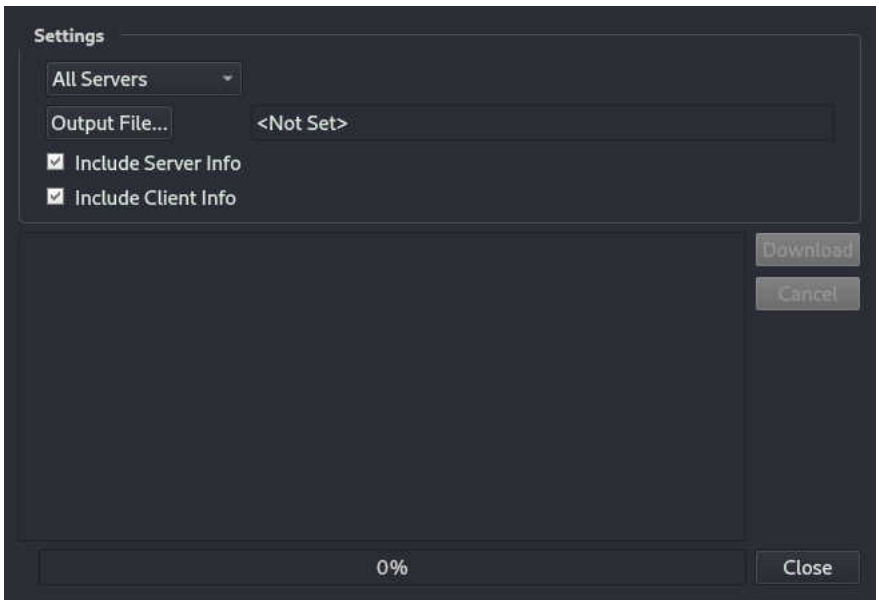


System Info...



The 'System Info' window gives information about the client PC and the connected servers and their licences.

Download Diags...



This window provides an easy way of obtaining lots of information about the current Client PC and all connected servers. It allows downloading all the information into a single zip file which can be passed to our technical support team.

It is possible to select "All Servers" (the default) or just a single server. Click "Output file..." to select a destination path for the zip file which will be written. Click "Download" to start downloading the files for the server.

This may take some time depending on the bandwidth available between client and server(s). The client diagnostic information should be very fast since it is only copied locally.

About...

This window provides information about the WaveView client application and its licence, as well as any third party libraries used to build the product.

3.2 Display Area

Right-clicking the Display Area calls up the context menu, containing the following options:

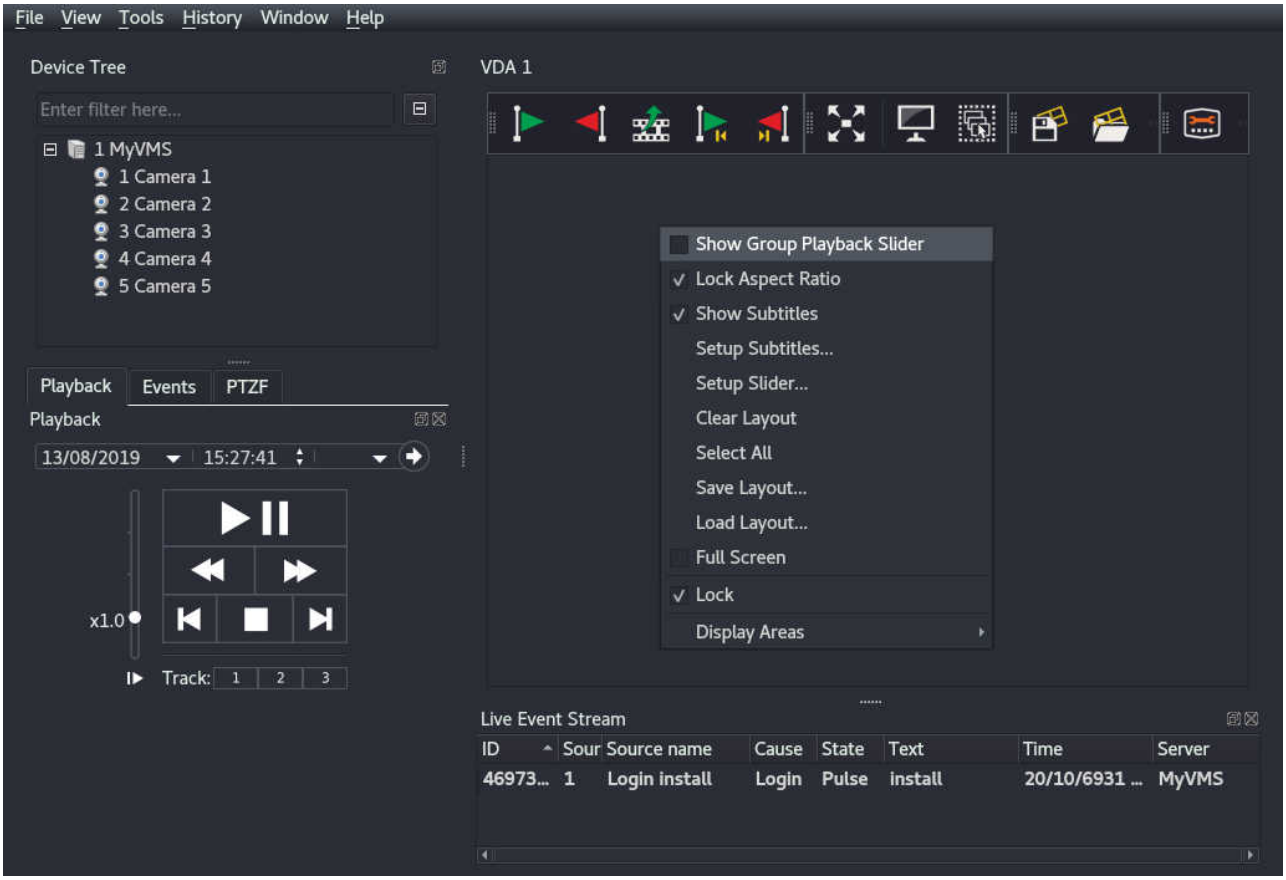


Figure 3.3: Context Menu

Show Group Playback Slider – as described in section 3.15 – Quick Search Controls using Time Slider.

Lock Aspect Ratio – Causes all Video Displays to be fixed to their true aspect ratios (width and height)

Show Subtitles – Video Displays subtitles toggle option (on/off)

Setup Subtitles – Opens the Setup Subtitles screen

Setup Slider – allows configuration of the actions and appearance of the Time Slider used for quick search at the lower edge of each Video Display

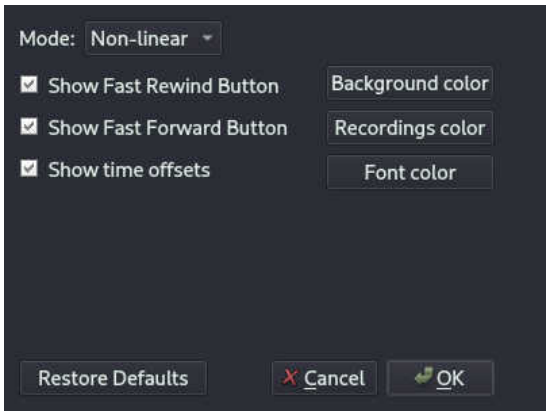


Figure 3.4: Slider Settings Box

Clear Layout – Removes all Video Displays from the Display Area.

Select All – Selects all Video Displays within the Display Area.

Save Layout – Saves the current camera layout under a specified name. See section 3.7.1 – Saving and Loading Layouts.

Load Layout – Allows a previously saved camera layout to be loaded. See section 3.7.1 – Saving and Loading Layouts.

Full Screen – Expands the Display Area to full screen display (to exit from full screen display, right click to call up the Context Menu once again, and toggle the Full Screen option OFF, or click the "Exit Full Screen" button at the top which is visible when the mouse is moved)

Lock – Controls the size of the Video Displays

Display Areas – Allows new Video Display Areas to be added and removed

Restore Toolbars – Useful if all toolbars have been hidden, makes them all visible again

Many of these functions can also be carried out from the Display Area Toolbar (details in section 3.3 – Display Area Toolbar below).

3.3 Display Area Toolbar

Figure 3.5: Display Area Toolbar

The Display Area toolbars are split in three sections, each of which can be displayed or hidden (right click on the Toolbar to configure).

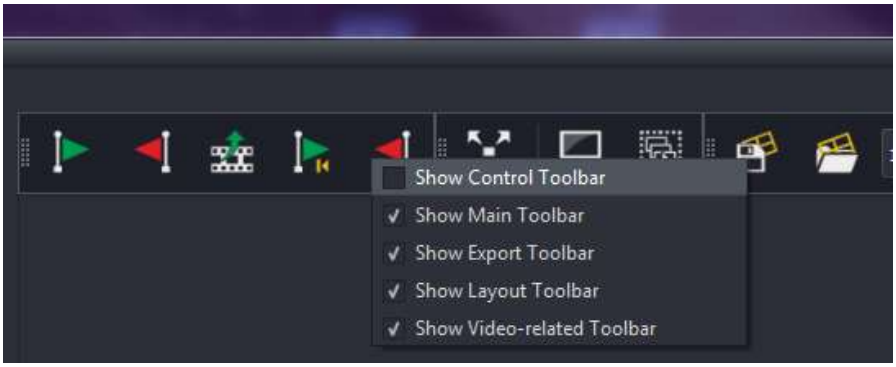


Figure 3.6: Display Area Toolbar display menu

The toolbar icons are as follows:

Export Toolbar

-  Mark 'Start Time' for Export icon – selects the start time for a quick export from the Main screen
-  Mark 'End Time' for Export icon – selects the end time for a quick export from the Main screen
-  Export icon – calls up Export Window
-  Go to 'Start Time' icon – moves the current playback position to the selected 'Start Time'
-  Go to 'End Time' icon – moves the current playback position to the selected 'End Time'

Main Toolbar

-  Full Screen Display icon – Clicking on this icon removes all menus and toolbars from the screen, and expands the camera view(s) to fill the entire screen.
-  Clear Layout icon – The Clear Layout icon removes all cameras from the Display Area.
-  Select All icon – selects all Video Displays
-  Save Layout icon – Clicking on the Save Layout icon allows you to save a configured layout of camera displays with a friendly name (e.g. Car Park Cameras) for quick recall. Note that layouts cannot be saved if the configuration is locked – i.e. an installer or administrator is currently editing the system settings. In this case an error will be displayed.
-  Load Layout icon – loads a previously saved Layout of cameras
- 

Display Configuration icon – Clicking on this icon allows you to select the configuration of the camera display from the following selections:
  - Free – Switches the Display Area to freely configurable mode
  - 1, 2x2, 3x3, 4x4, 3x2, 4x3, 5x4, 5x3 – Switches to a fixed, preset layout of displays
  - Custom Layout – Switches to a previously saved custom layout
-  Lock Layout – Toggle option to lock/unlock the current positions of the video displays. When the 'unlock' option is selected, you can click and drag a video display to an empty position in the dis–

play grid (if a fixed Display Configuration e.g. 2x2 has been selected). If the Display Configuration setting is configured as 'Free', the video display can be moved to any position.

The same action can be carried out even if the Lock layout option is in the 'Lock' state, by holding down the CTRL key while you click and drag the display.

-  Undo Layout – returns to the previous layout
-  Redo Layout – re–applies a layout after an undo operation
-  Toggle option to lock/unlock the aspect ratio of the currently selected video display.
-  Adds a horizontal row of video displays to the current layout
-  Adds a vertical column of video displays to the current layout

Video Toolbar

-  Setup Subtitles icon – The Setup Subtitles screen allows configuration of the subtitles within all Video Displays of the current Display Area.

  When clicked, a new window appears showing the subtitle template with a variety of 'tags' ar–ranged to reflect the current subtitle settings (e.g. Server/Camera name, time stamp, frame rate etc.). These can then be amended as required.

-  Subtitles icon – Clicking on this icon allows you to toggle the video display subtitles on/off.
-  Talkback status icon – displays the status of the Talkback channel from a microphone on the client device, to a speaker on the server or camera. Talkback for any channel is switched on/off by clicking on the Microphone icon on the Video Toolbox (section 3.6.2 – Video Display Toolbox). When talkback is active on any channel, the status will show as Red.

  This icon can also be used as a global on/off toggle switch for the Talkback feature, to activate talk–back for any configured camera channels.

3.4 Working with Video Displays

3.4.1 Video Displays from Standard Cameras

To add a camera view to the Display Area, firstly select which Camera View type you want to use (Free/Custom/1/2x2/
by right clicking on the Display Area to call up the Context Menu (Figure 5.1), and then left clicking on your desired selection (e.g. '2x2' in this example). You can also do this by click the drop down box on the Video Display Toolbar.

You can also click on the 'Add Column to Grid Layout' or 'Add Row to Grid Layout' button on the Video Display Toolbar (see section 3.3 – Display Area Toolbar above) To create a Video Display, double click on the Camera Name in the Device Tree and it will appear in the next free space in the Display Area.

Alternatively, click and drag the camera name from the Device Tree to the position that you want on the Display Area (e.g. Camera 3):

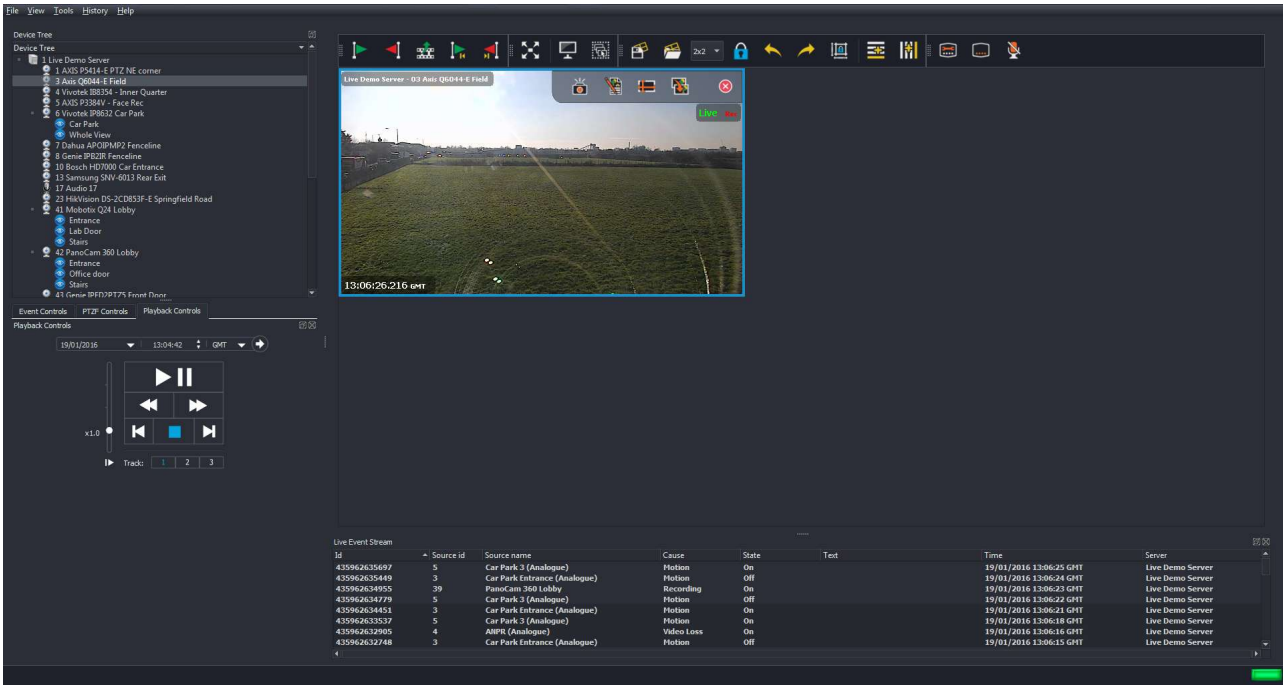


Figure 3.7: Dragging Camera 2 from Device Tree on Display Area

Repeat for any other cameras that you require:

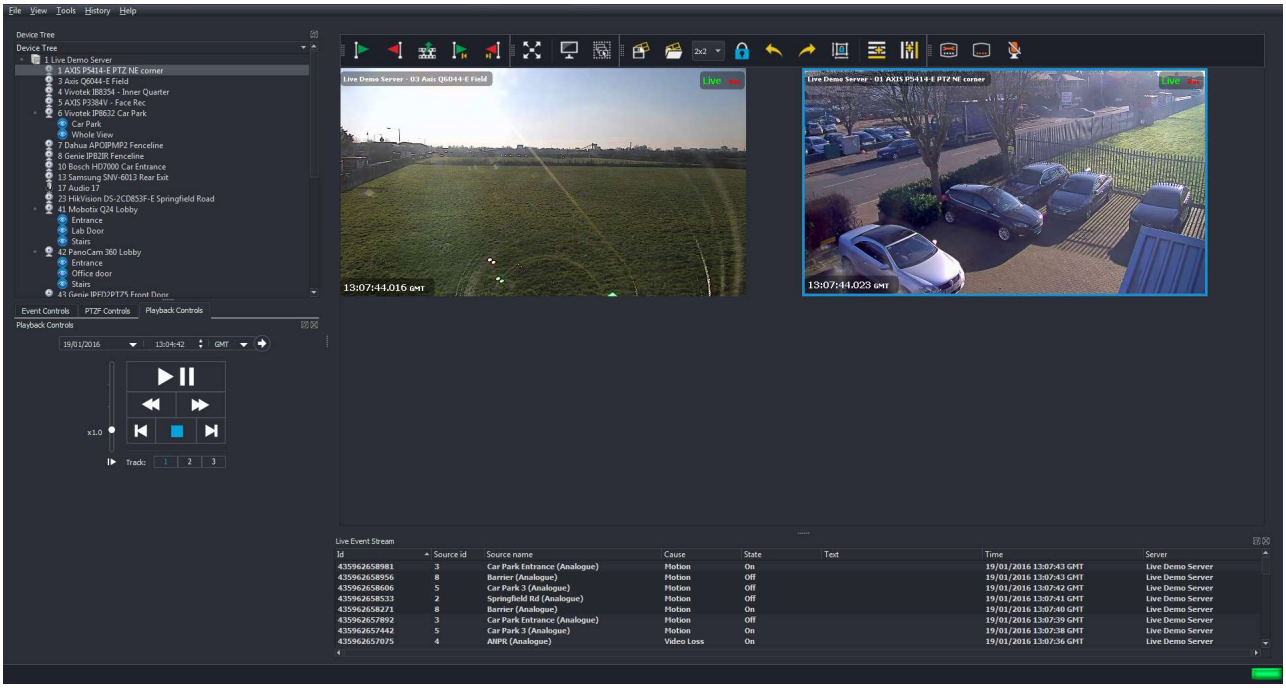


Figure 3.8: Camera 4 added from Device Tree to Display Area

To select a Video Display for user control (for PTZ control/playback etc.), click on that camera view so that the camera view frame is highlighted blue, as shown in Figure 5.7 (the top left camera is active in this case).

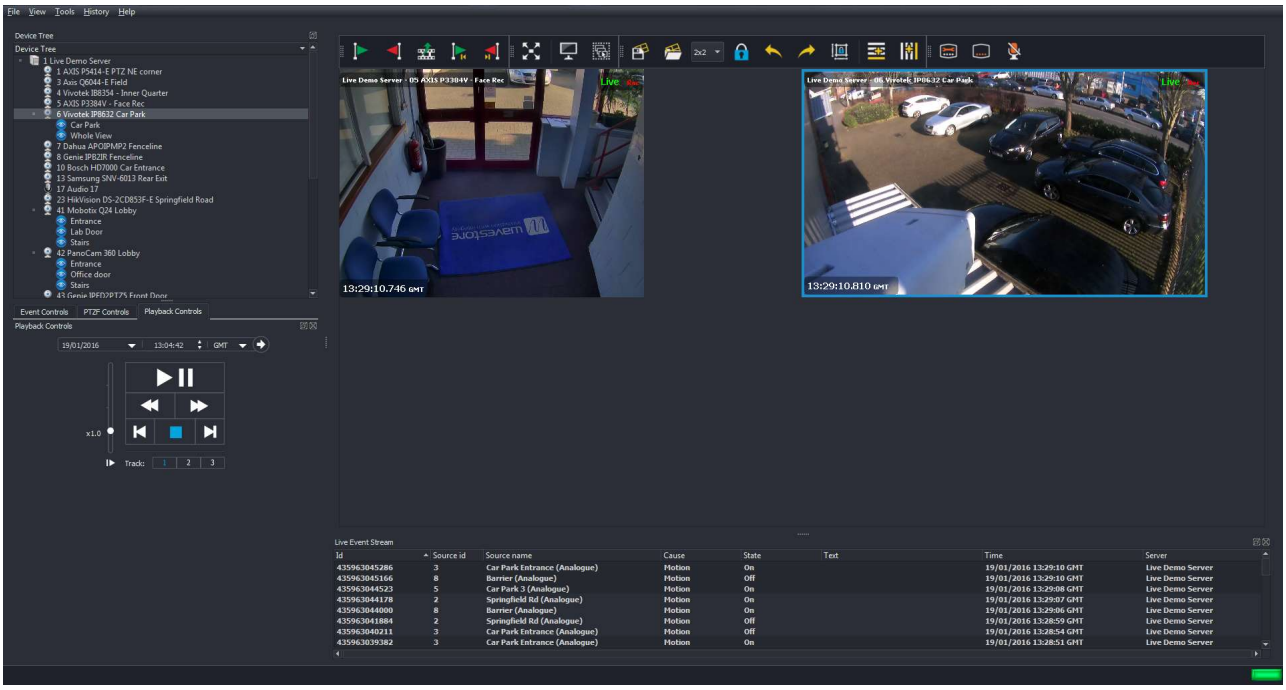


Figure 3.9: Camera 2 active for PTZ control/playback

You can now use the Playback controls to pause the Live stream, and search the recorded footage for

this camera:

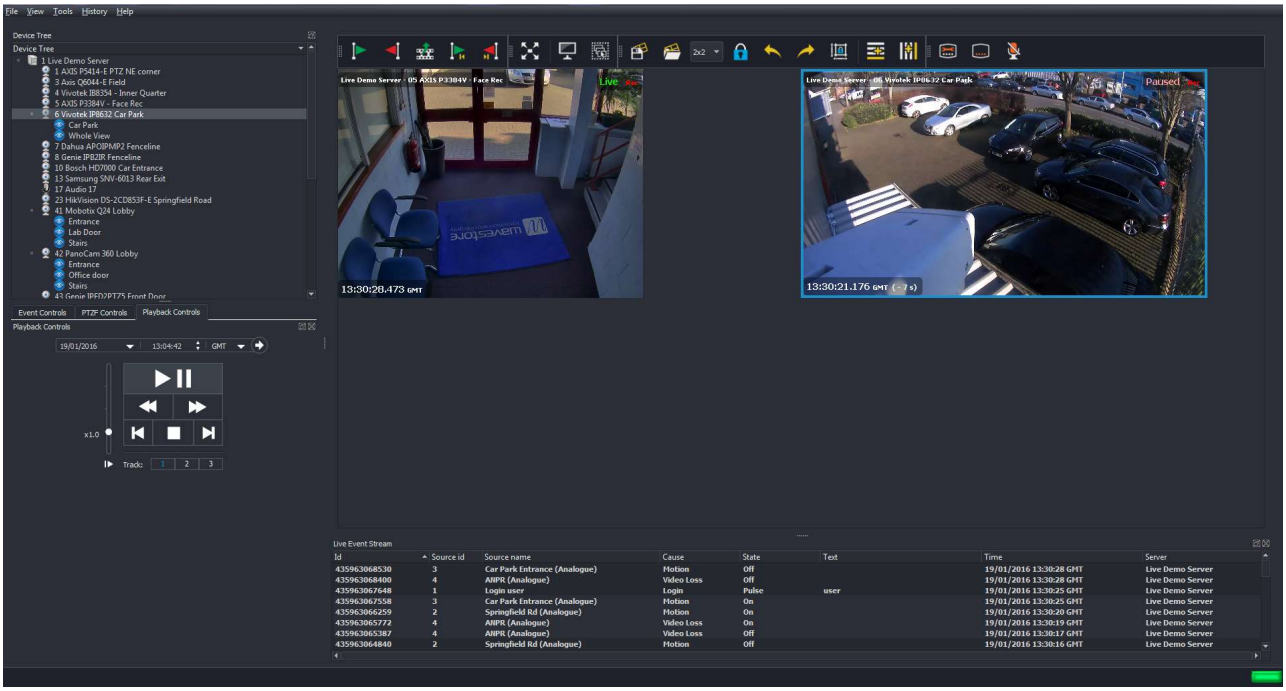


Figure 3.10: Camera 2 paused

When adding Video Displays for other cameras, they will inherit the playback state of any selected Video Displays. For example, if you have a Video Display playing back recordings and it is selected, if you drag and drop or double–click a different camera in the Device Tree, the new Video Display will begin playing back from the same time point (as long as there are recordings for that period).

To "solo", or enlarge, an individual Video Display (e.g. Camera 3), double click on the Video Display; the display will now fill the entire Display Area.

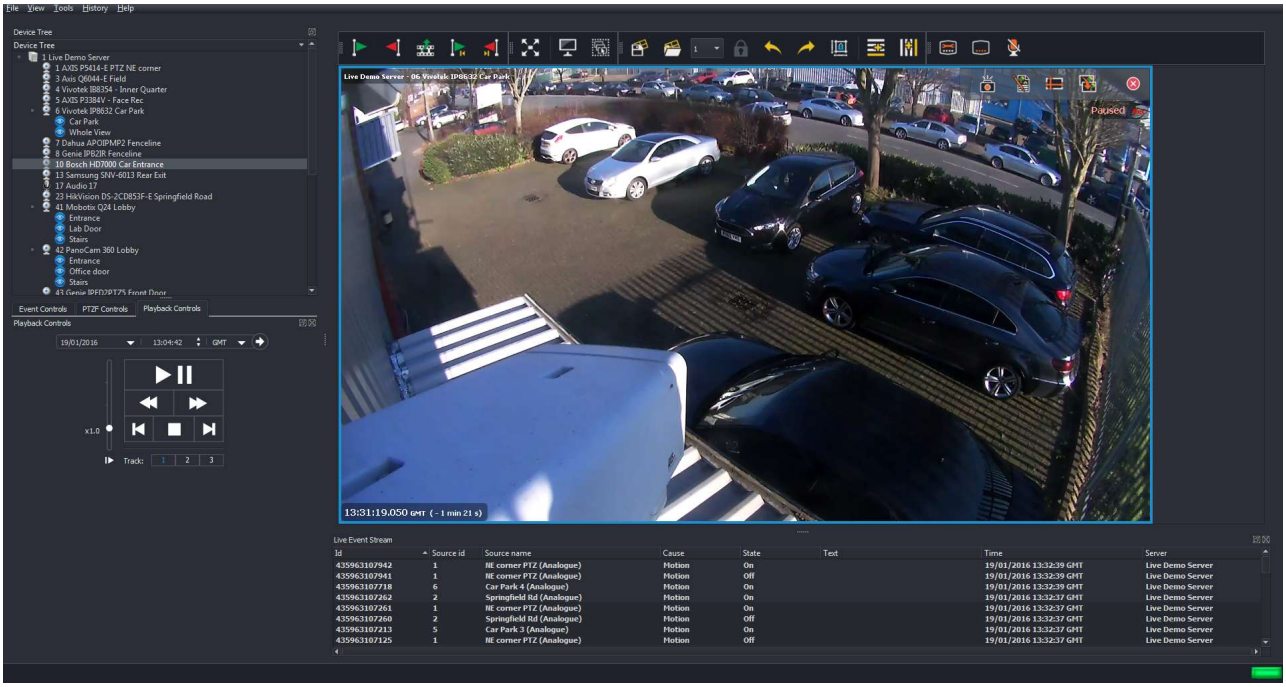


Figure 3.11: Camera 3 view enlarged

To "unsolo", or return to the previous layout, double click on the Camera Display again.

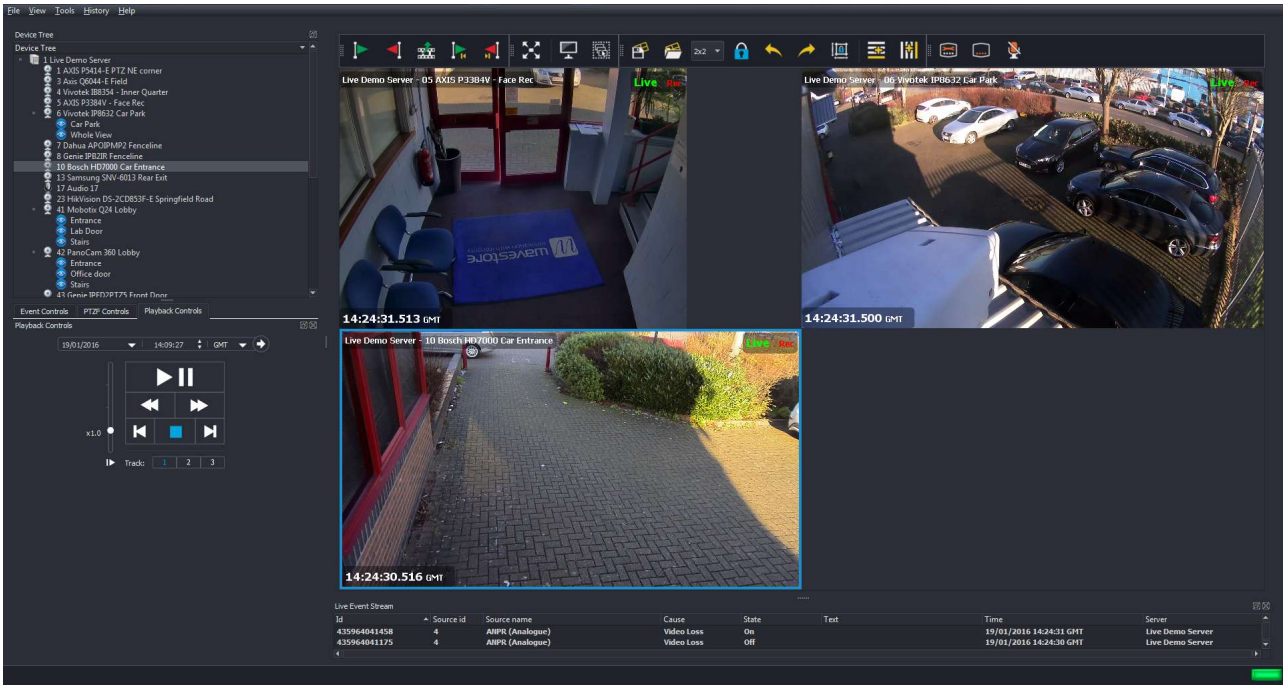


Figure 3.12: Exiting Full Screen View

3.4.2 Dewarped Video Displays from Hemispheric Cameras

This section explains how to interact with fisheye lens cameras and assumes that the cameras have already been suitably configured by the system administrator.

We will walk through "cloning a display" and dewarping the cloned display, although the cloning step isn't actually necessary. The benefit of cloning displays is that only one video stream is transmitted over the network and decoded, yet it can be viewed several times with different dewarping settings. This also means that playback control will affect all the cloned displays.

Double–clicking the name of the hemispheric camera in the Device Tree will create a new Video Display of the raw warped stream from that camera in the Display Area...

Figure 3.13: Calling up Video Display from 360° Camera

Click on the 'Add Column to Grid' button layout to change the display configuration. This will make space in the Display Area for another Video Display.

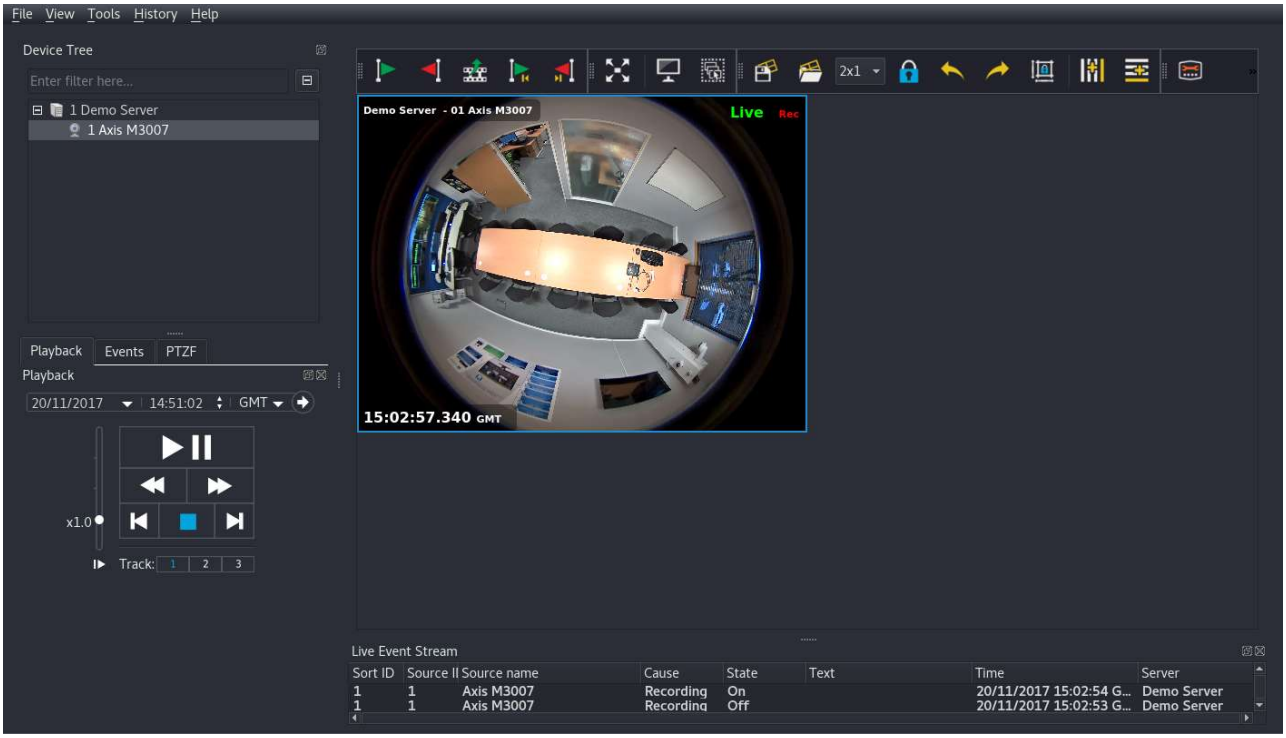


Figure 3.14: Adding Column to display grid layout

Hover your mouse over the top of the Video Display, so that the Video Display Toolbox appears.

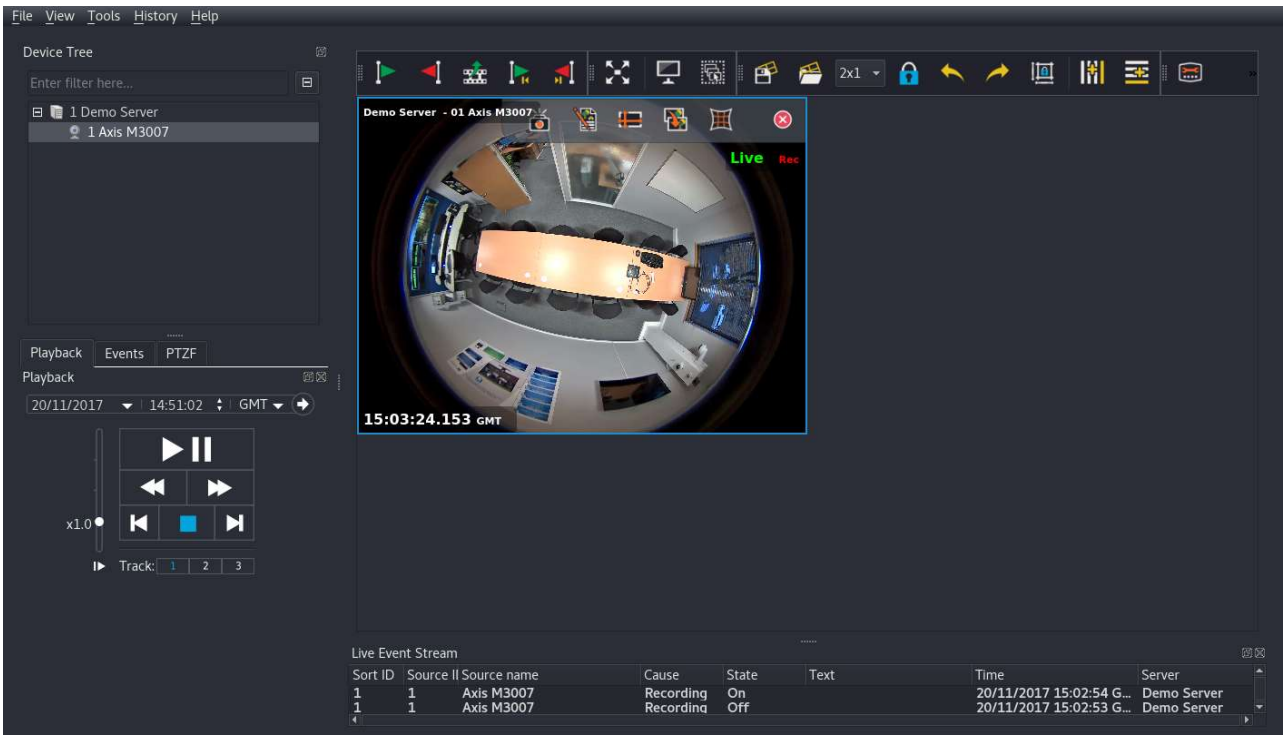


Figure 3.15: Calling up the Video Display Toolbox

Click on the Clone button on the Video Display toolbox to create a clone of the original Video Display.

Figure 3.16: Clone button

These two displays both display the same video stream, and are time synchronised. Any playback commands (Pause/Rewind/Fast Forward) will affect both displays.

Figure 3.17: Creating Cloned Video Display

On the cloned Video Display, position your mouse in the top right of the display to call up the Video Display Toolbox.

Figure 3.18: Video Display Toolbox

Figure 3.19: Dewarping button

Click on the Dewarping button and choose "Default".

The dewarped image can be manipulated by clicking and dragging the mouse to perform Pan and Tilt operations, and scrolling the mouse wheel for a Zoom operation. Note that this requires the layout to be locked, otherwise clicking and dragging the Video Display will move it within the layout. The layout can be locked with the padlock icon in the Display Area Toolbar, or temporarily toggled by holding the CTRL key.

It can sometimes be useful to see an indication of the dewarping operation. Clicking the 'Contours and Tracking' icon in the Display Area Toolbar will enable a mode whereby the dewarped areas of the original image are highlighted in red, as shown below...

Figure 3.20: Contours and Tracking button

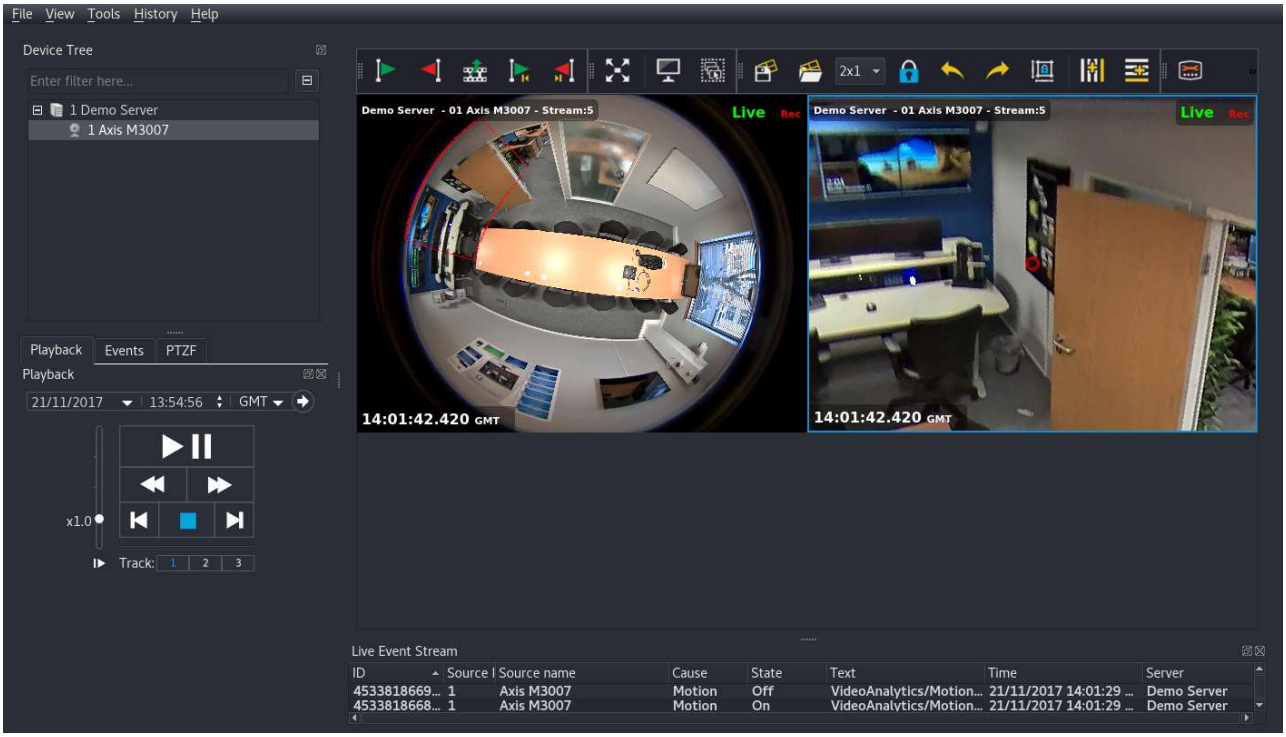


Figure 3.21: The Contours and Tracking Feature

You can create a virtual PTZ tour in a dewarped virtual camera view, by clicking in the centre of that view, and then then dragging the mouse pointer outside that camera view. The view will pan in the same manner as a physical PTZ camera.

3.4.3 Panoramic Video Displays from Hemispheric Cameras

Creating a Panoramic view is very similar to normal dewarping, with a couple of key differences. Primarily the use of free layouts, and selecting 'Panoramic' instead of 'PTZ.

In this section we'll walk through an example of how you might want to set up a layout with a panoramic camera.

Start with an empty 2x2 layout and double–click on the name of the hemispheric camera in the Device Tree to add it to the Display Area.

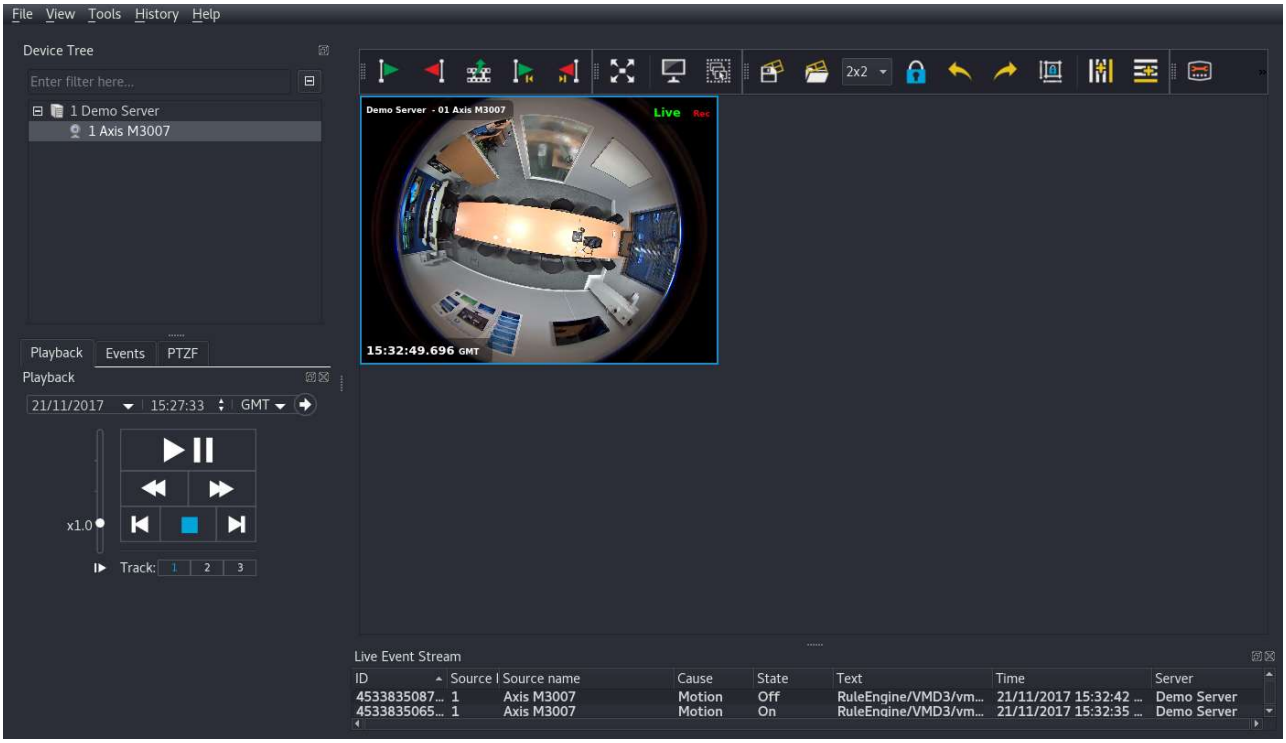


Figure 3.22: Video Display of raw warped stream from 360° camera

Position your mouse over the top of the Video Display of your camera, so that the Video Display Toolbar appears. Then click the Clone icon to create a clone of the original Video Display.

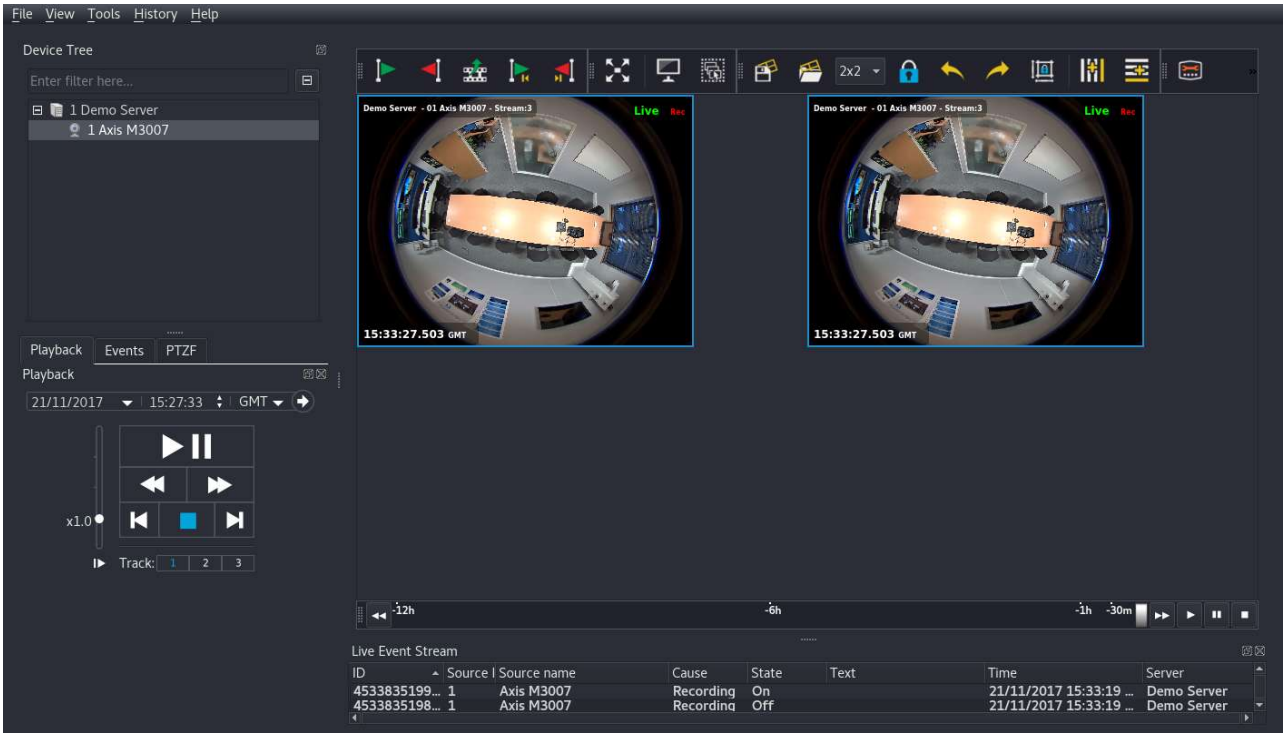


Figure 3.23: Creating Cloned Video Display

Now change the layout from '2x2' to 'Free' and drag the cloned Video Display to the bottom left position.

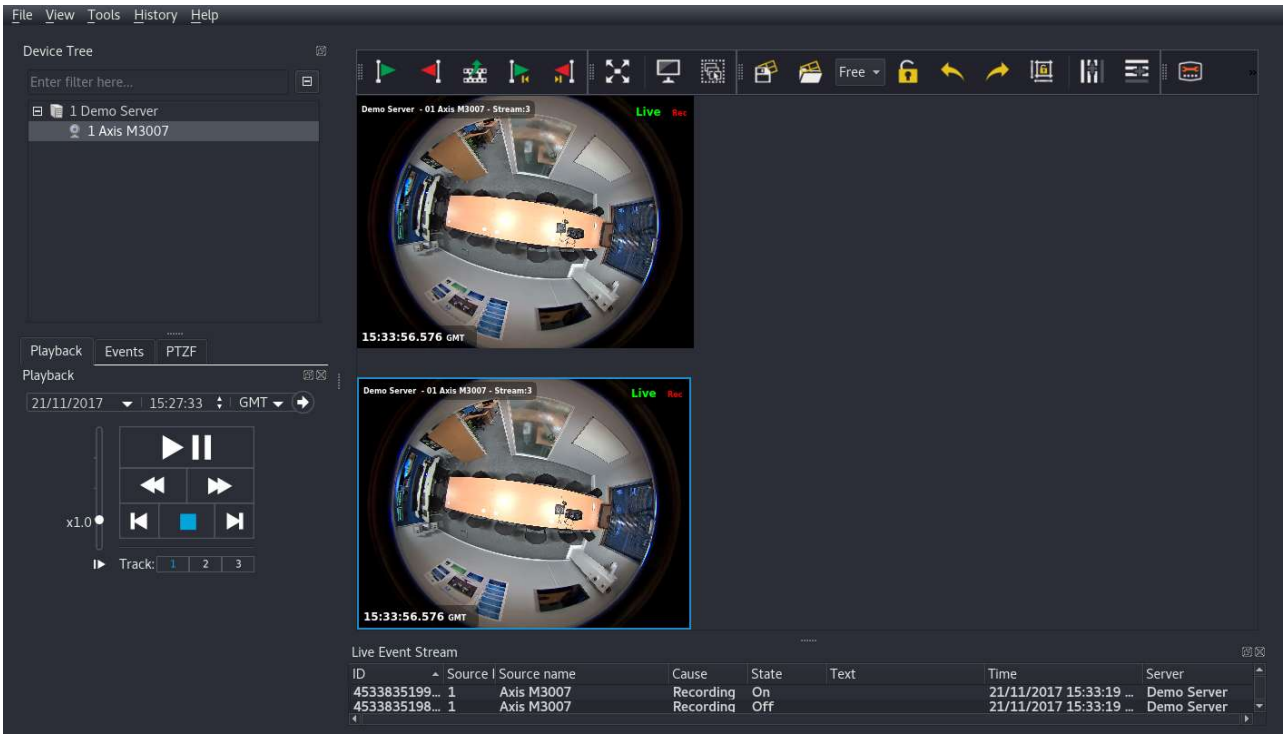


Figure 3.24: Positioning displays in a free layout

On the cloned Video Display, click the Dewarping icon and select "Panoramic". The cloned video display will now display a panoramic section of the original raw image.

Resize the bottom Video Display so that it takes up the width of the Video Display Area.

It's also useful sometimes to enable the 'Contours and Tracking' feature from the Display Area Toolbar.

Figure 3.25: Contours and Tracking button

The panoramic area will now be shown on the original warped image. The panoramic image can be adjusted by clicking and dragging with the mouse and using the mouse wheel to zoom.

Figure 3.26: Panoramic Display with Contours and Tracking

Clicking on the 'Contours and Tracking' button again will remove the green setup graphics.

3.4.4 Keyboard Shortcuts

Opening many cameras with an appropriate layout size

Holding ***Shift*** whilst double-clicking either a server name, or a ***Channel Group*** name, will cause the layout grid dimensions to change to a "best fit" size, and open all the cameras on that server or within that ***Channel Group***. For example, if you have a ***Channel Group*** containing 9 cameras, a 3x3 grid layout will be opened containing all 9 cameras. The same happens when dragging and dropping the server name or ***Channel Group*** name with ***Shift*** held.

Opening cameras with the keyboard

Hold *Ctrl* and press the forward slash numpad key / to open the camera selection overlay. Keeping the *Ctrl* pressed, enter the desired camera number, then press *Enter*.

Opening saved layouts with the keyboard

Hold *Ctrl* and press the asterisk numpad key * to open the layout selection overlay. Keeping the *Ctrl* pressed, enter the desired layout number, then press *Enter*.

Next and previous camera

Holding *Ctrl* and pressing + or – will switch to the next or previous camera.

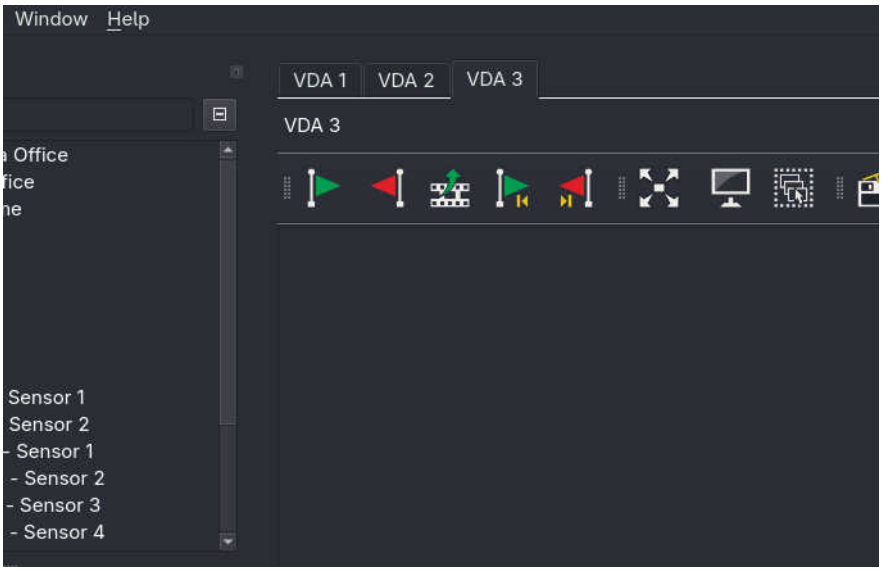
Locking and unlocking the layout

Pressing *Ctrl* will temporarily toggle the layout lock/unlock button. This is particularly useful for modifying grid layouts. For example if a dewarped camera is in a layout and the layout is locked, clicking and dragging in the video display will operate dewarping PTZ on that camera. If, however, you want to move the camera to a different slot in the grid, holding *Ctrl* will temporarily unlock the layout and allowing clicking and dragging to move the display.

3.4.5 Using Multiple Video Display Areas

WaveView supports the use of up to 4 Video Display Areas simultaneously. The default VDA is known as VDA1. VDAs 2, 3, and 4 can be opened using the *Window* menu.

By default, newly opened VDAs are arranged as tabs above VDA1, but they can be detached and moved to the desired location, such as a separate monitor.



By default, double-clicking items in the Device Tree causes those items (e.g. cameras or audio channels) to open in VDA1, however they can be dragged and dropped to any VDA. Also, it is possible to choose a different default VDA for double-click opening in the *System Settings* preferences (see section 3.22.1 – System Settings). Similarly, double-clicking an event in the Live Event Stream opens that event on VDA1 by default, but the desired default VDA can be configured in the same preferences.

There is also per-user configuration option for automatically opening a layout on each of the VDAs. This has to be configured for the desired user by an install-level or admin-level user. See section 6.1 – Users.

Video Displays can even be dragged and dropped between VDAs as long as neither VDA is locked.

3.5 Setup Subtitles Menu

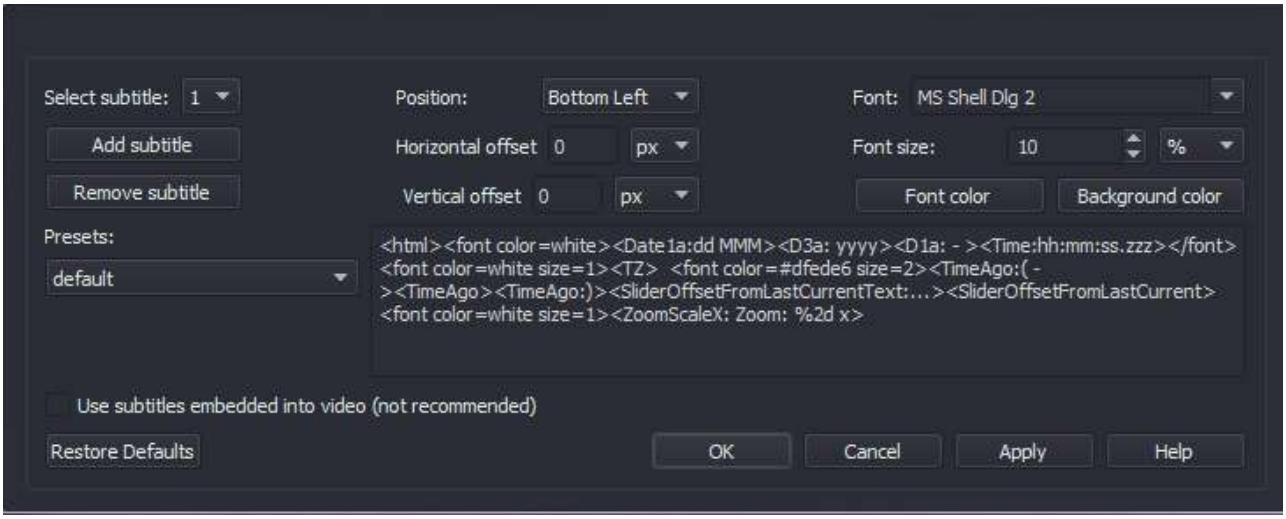


Figure 3.27: Subtitle Setup submenu

The Setup Subtitles menu allows the default subtitles that appear on individual Video Displays to be re-configured or removed.

This menu contains individual configuration for each of the subtitle positions on the display, such as position, font, size and displayed text.

The Presets section allows you to select from a list of commonly used configurations.

If you wish to configure a custom subtitle configuration for that position, click in the text box (light grey section), and you can add/remove the sections that you require.

The Help button opens a window showing the list of available tags, along with a description of each. You can copy and paste from this window into the text box for each position.

The functions of the remaining menu buttons are as follows:

- The Restore Defaults button sets the subtitles to the default settings
- The OK button accepts the current setting and closes the Setup Subtitles window
- The Cancel button cancels all changes and closes the Setup Subtitles window
- The Apply button saves the current setting but keeps the Setup Subtitles window open
- The Help button gives a full list of the Subtitle options available
- The Use Subtitles embedded into video option can improve the clarity of the displayed subtitles, if the client PC has a low quality graphics card

3.6 Video Displays

A single Video Display shows a single video stream and plays any associated audio stream. When the mouse is hovered over the top right corner of the Video Display, the Video Display Toolbox is shown which provides access to various tools and settings for that Video Display. The Video Display contains a subtitles area, along with Video Status Icons which indicate the current state of the video stream.

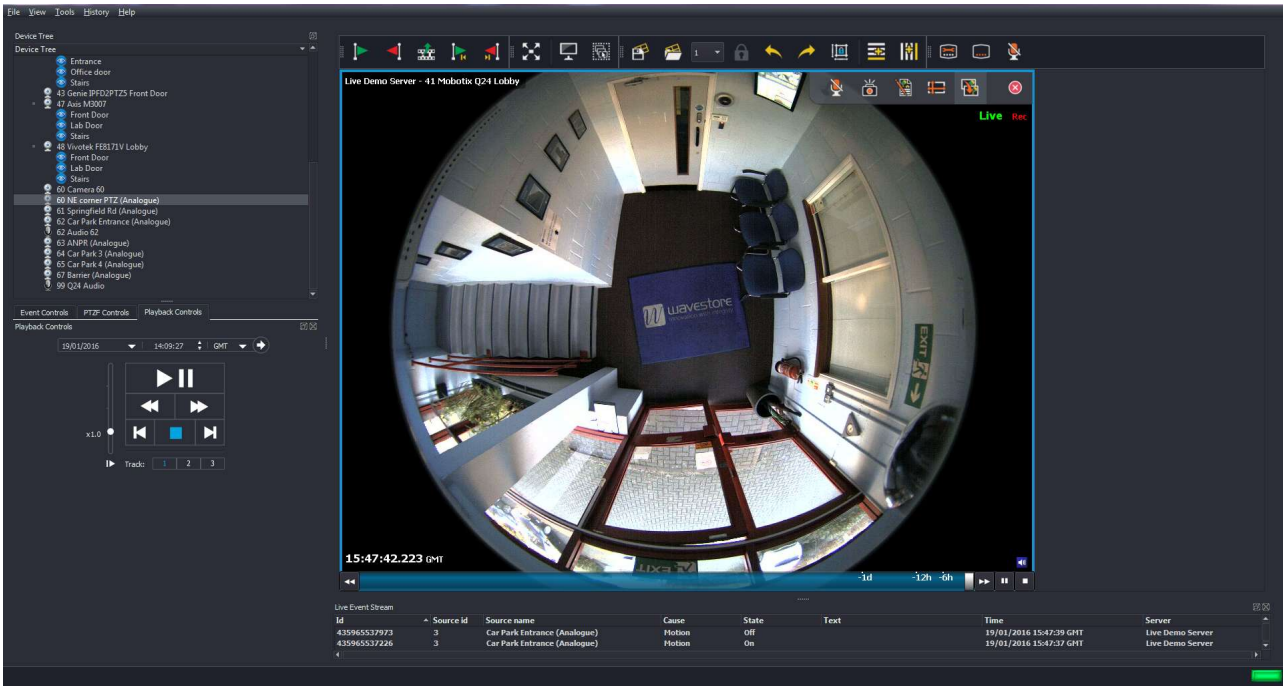
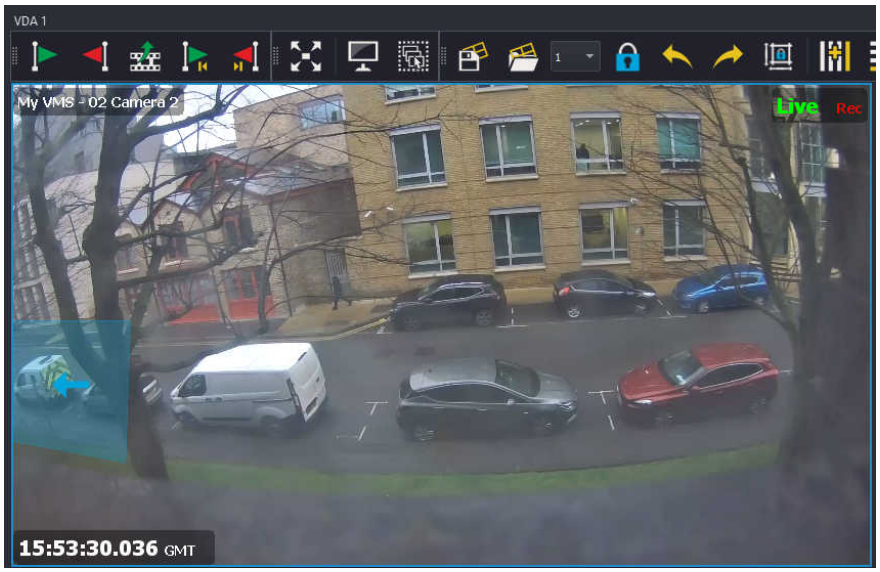


Figure 3.28: Video Display

3.6.1 Hot-Spots

If configured, Hot-Spots associated with a Video Display will be shown when the mouse is over that Display.



Each Hot-Spot will highlight when the mouse is hovered over that Hot-Spot. A tooltip will show the name of the Hot-Spot if the mouse is stationary over the Hot-Spot.

Left-clicking the mouse activates the action associated with the Hot-Spot.

For details of configuring Hot-Spots, see section 6.5 – Hot-Spots.

3.6.2 Video Display Toolbox

Figure 3.29: Video Display Toolbox

The Video Display Toolbox appears when the mouse pointer is placed in the top right hand corner of the Video Display, and shows a number of icons used for performing operations on the currently selected Video Display(s) (highlighted with a Blue frame).

- 

  Snapshot captures the currently displayed image and displays it in a new window, allowing editing, export and printout.

- 

  Video Resolution allows you to change the current 'requested' viewing resolution (Low/Medium/High) to improve the image rate on a slow network connection.

- 

  Create Annotation – A section of Video Footage can be marked with annotations, so that it can be easily located at a future date.

- 

  Dewarping – Enables dewarping of fisheye and panoramic cameras. Only present if configured for the current camera.

- 

  Clone Video Display – a new Video Display, time synchronised to the original display, will open in the Display Area, a useful feature when viewing different saved views from a hemispheric camera. Only supported for hemispheric cameras.

- 

Metadata Display – opens a new window displaying Metadata associated with this camera channel (if configured)

- 

  Talkback – click to toggle on/off (if Talkback has been configured for this channel). The icon colour changes to Red when Talkback is active. Note that this controls capture of audio from the microphone and transmission to the target device. When playing back recordings, the talkback audio will always be played if recording for that Talkback track has been enabled.

- 

  Mouse PTZ – click to toggle on/off (if PTZ has been configured for this camera). See section 3.6.3 – Mouse PTZ Control.

- 

  Close – closes the Video Display

3.6.2.1 Snapshot Window

When the Snapshot button is clicked, the currently displayed image is captured and displayed in a new window, allowing the user to:

- Edit the image using the following commands (click and drag on the image to select an area, then select your desired command from either the pull down menus or the toolbar)
  - Crop
  - Sharpen
  - Blur
  - Mosaic
  - Desaturate
  - Invert
  - Equalize
  - Brightness +/–
  - Contrast +/–
  - Gamma +/–
- Resize the image
- Save a copy of the still image (if permitted) in BMP, JPG or PNG format
- Print the image

Note that the "Export" user permission controls whether the current user is permitted to save the snapshot.

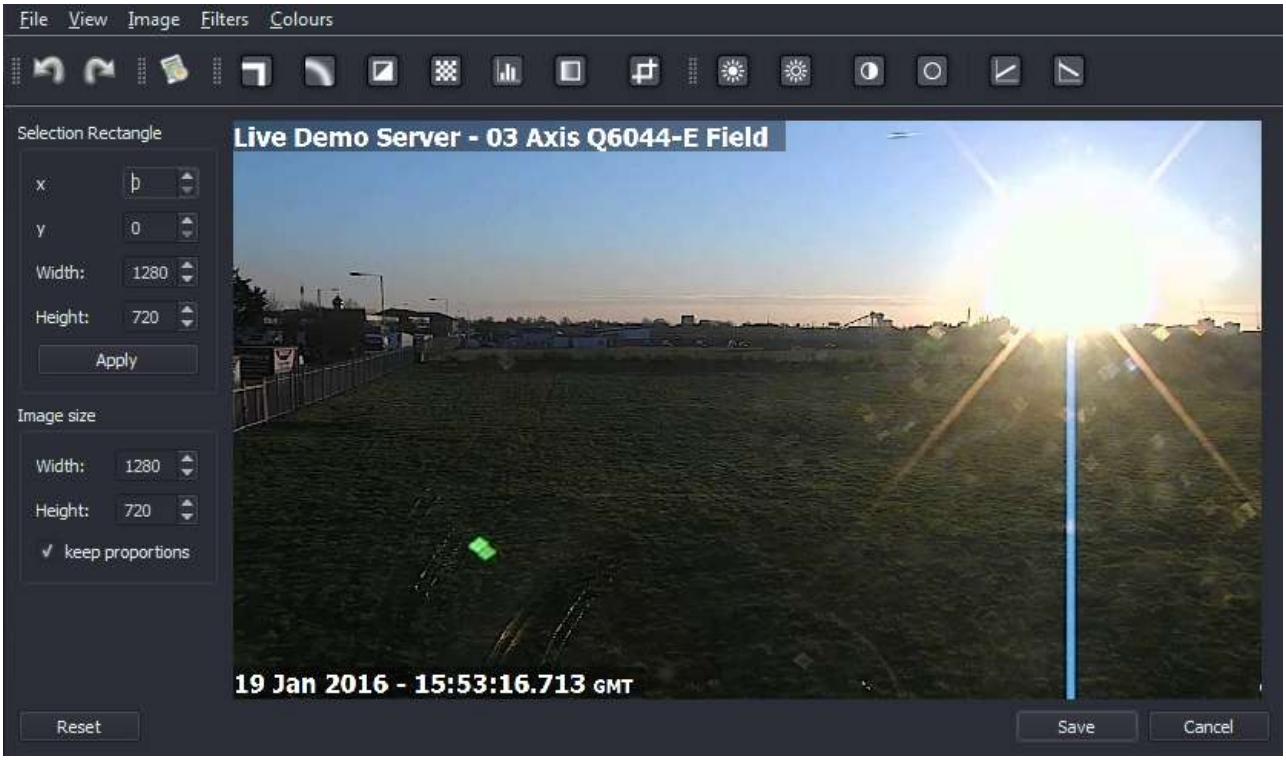


Figure 3.30: Snapshot Screen

Following the menu path Image → Subtitles Setup allows you to configure the appearance and position of the subtitles on the image.

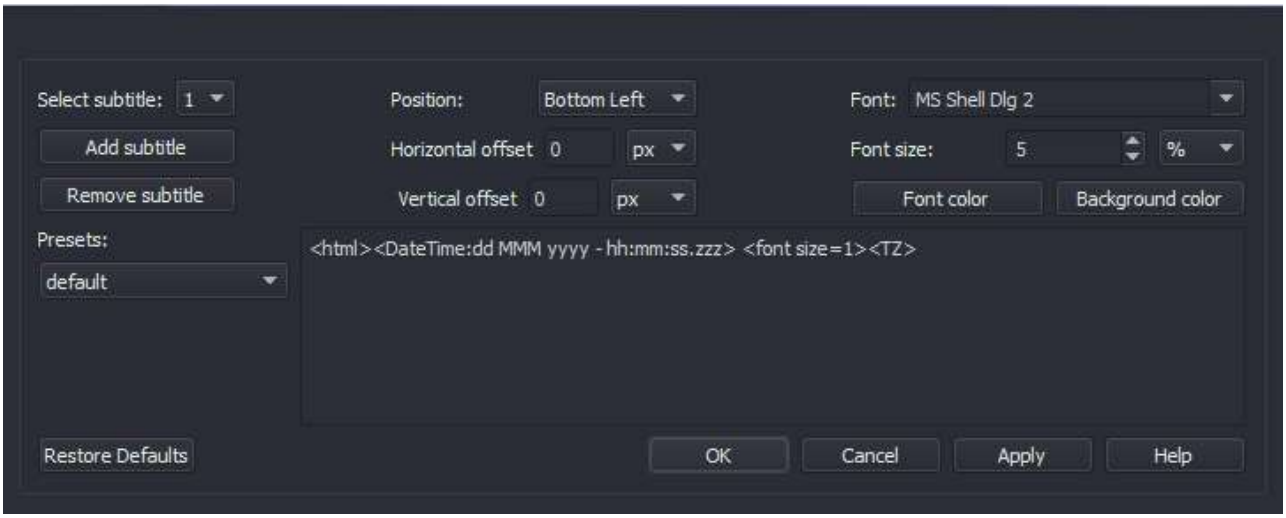


Figure 3.31: Snapshot Screen – Setup Subtitles submenu

The setup subtitles menu allows you to configure, reposition or remove the subtitles from the selected position on the image.

3.6.2.2 Create Annotation Window

Clicking on the 'Create Annotation' icon calls up the Annotation window; a user can add notes of interest to a bookmark a section of footage. To carry this out, enter the start and end times of the required footage, and any annotation that you require.

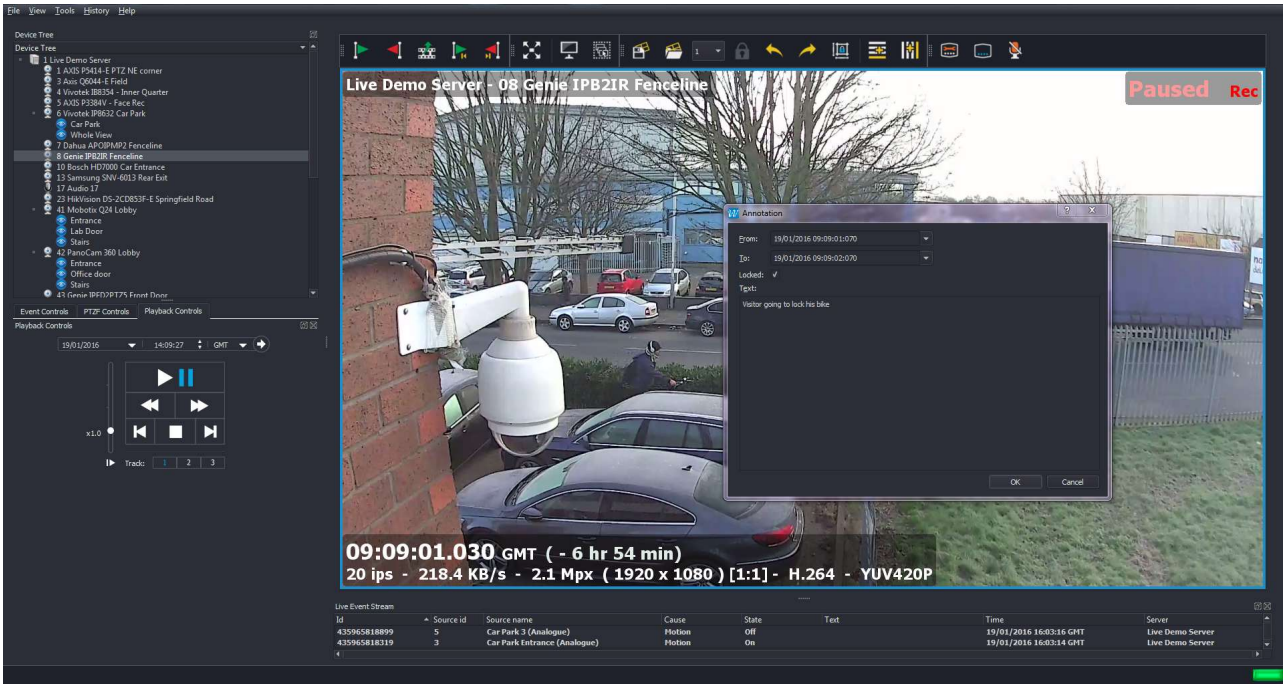
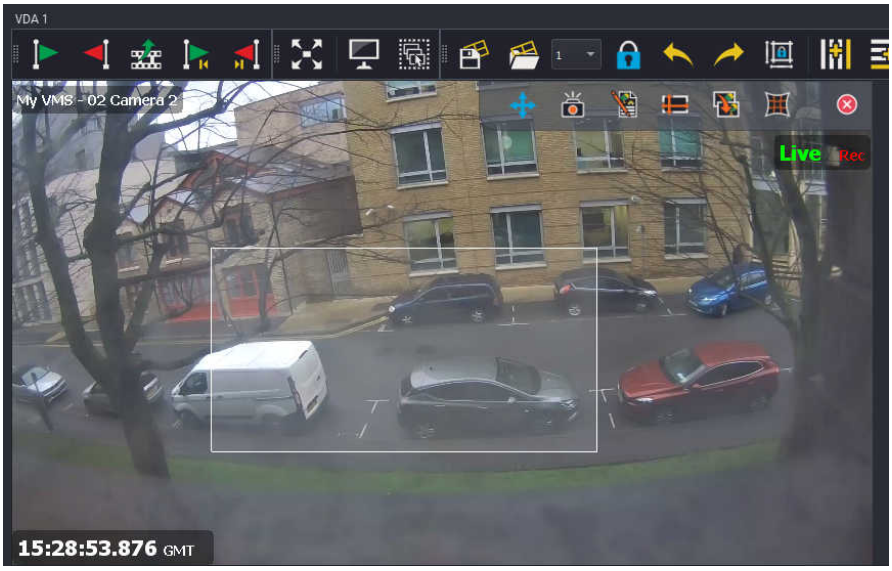


Figure 3.32: Annotation Setup

3.6.3 Mouse PTZ Control

When this mode is enabled, PTZ cameras can be controlled using the mouse. Left click and drag to pan and tilt the camera, use the mouse wheel to zoom.

Some cameras also support drawing a box on screen to move the camera and zoom to the desired region. This is performed by clicking the middle mouse button and dragging a box to highlight the desired area.



3.6.4 Video Status Icons

The Video Status Icons (lower right of Video Display) indicate the state or features of the current video stream, as follows:

3.6.4.1 Audio Icons

- 

  Audio Available Icon – If this icon is present, an audio channel is associated with this video channel. The audio can be heard if this Video Display is set to Audio Master.

  Hovering your mouse pointer over the Audio Available Icon will cause additional icons to display as follows:

- 

  Audio Mute This icon mutes the audio from this channel

- 

  Audio Enable This icon enables the audio from this channel.

- 

  Solo Audio Clicking this icon instructs WaveView that it should only plays the audio associated with this Video Display. This will mute any audio streams from Video Displays already playing.

3.6.4.2 Authentication State icons

If Image Authentication has been activated on the server (see section 6.2.7 – Image Authentication), the Authentication State Icon shows the Image Authentication status of the current stream in the lower right corner of the Video Display. The available states are:

- 

Authentication checked and OK

- 

  Authentication not checked. This can happen if playing back close to the current time, e.g. 1 second from live. This is because the authentication data is only recorded every few seconds. It can also happen if signature stream recording was not enabled at time of recording the video.

- 

  Authentication checked and failed

If Image Authentication has not been enabled for the server, no Authentication State icon will be visible.

3.6.4.3 Encryption State icons

The server can be configured to encrypt one or more of its video channels. The Encryption State Icon shows whether encryption is currently enabled for this camera.

The available states are:

- 

  Encrypted

- 

  Unencrypted

If you connect to a channel for which encryption has been configured on the server, you may see the following message, if a Private Key to decrypt the channel has not been loaded:

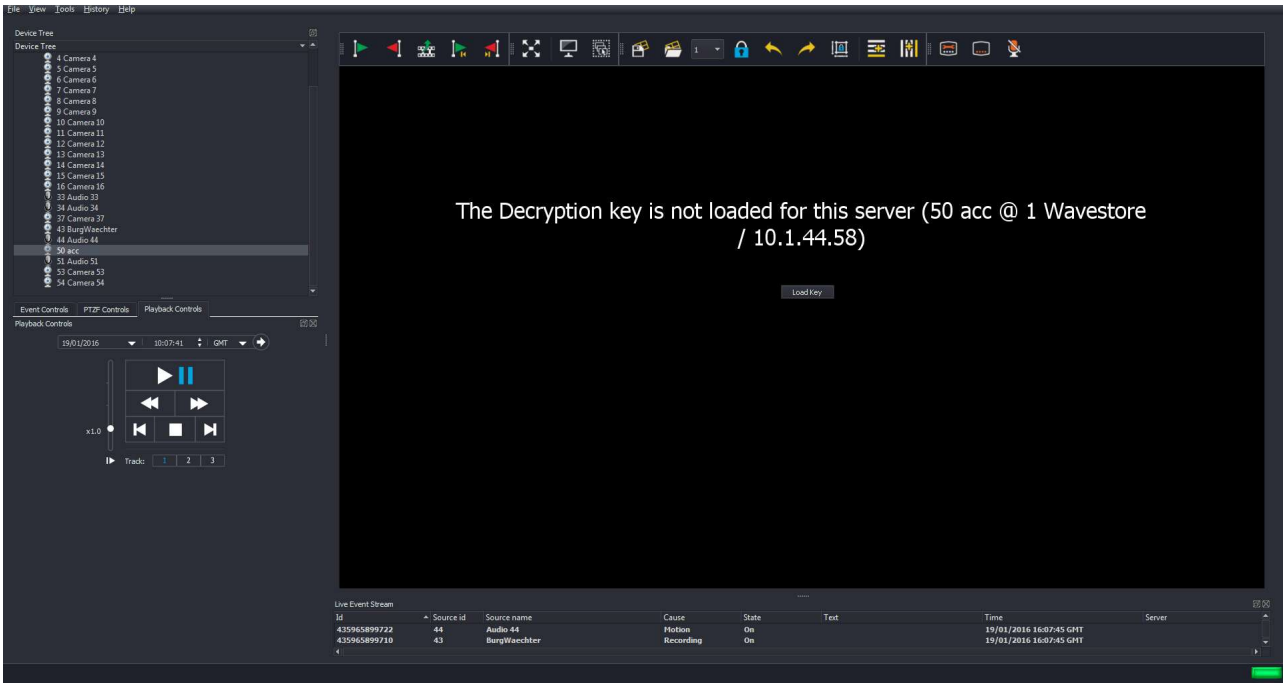


Figure 3.33: Encryption Key prompt

To load your Private Key in order to decrypt the stream, click on 'Load Key'.

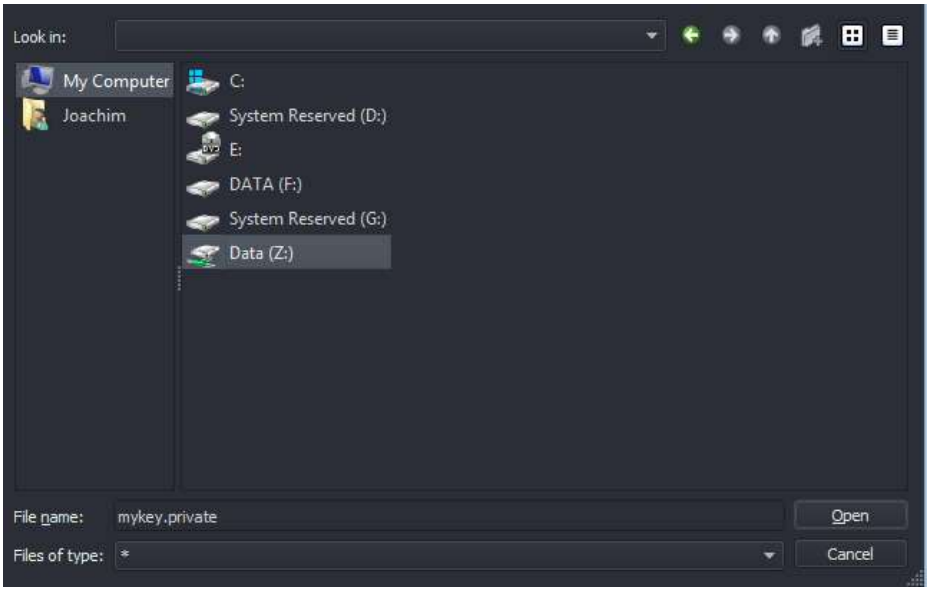


Figure 3.34: Loading Private Key

Other Text Information is displayed in the Video Display such as Server Name, Camera Name, Time Stamp, Time Zone, frame rate and file size of the image. The Subtitle Settings control which of these text items are displayed.

3.7 Layouts

A Layout consists of various cameras in various positions in the Video Display Area, along with various properties for each of those cameras.

It is possile to save Layouts with a name so that they can be easily recalled later. It is also possible to create sequences of layouts to create a cycled display.

Layouts are, by default, private to the user who created them. However they can also be marked as "shared" so that other users can see them.

It is also possible to configure auto-loading of a particular Layout or Layout Sequence for each user upon login. However note that this has to be configured by an "admin" or "install" level user for "user" level users. See section ?? – ??.

The following properties are saved with a layout:

- The layout name
- Whether aspect ratio should be preserved for the cameras in the layout
- Whether subtitles should be shown for the cameras in the layout
- The cameras to display and their positions
- The resolution (high or low) for each of the cameras
- The digital zoom level and position for each of the cameras

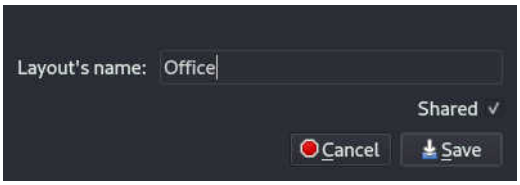
- The fisheye dewarping position for each of the cameras – if applicable
- Whether the dewarping "contours and tracking" feature should be enabled or disabled
- Whether a particular camera is a clone of another
- Audio mode (for audio channels only), e.g. mute, solo, or enabled

In server groups, the layouts are saved to all servers. When loading, they are read from the first connected server. Any level of user can save a layout.

3.7.1 Saving and Loading Layouts

Layouts can be saved by right–clicking the Display Area and choosing "Save Layout...", or by clicking the Save Layout button in the Display Area Toolbar...

The Layout can be given a name and optionally marked as "Shared" so that other users can see this Layout. Saving, overwriting, or deleting shared layouts is only possible for users who have been granted this permission.

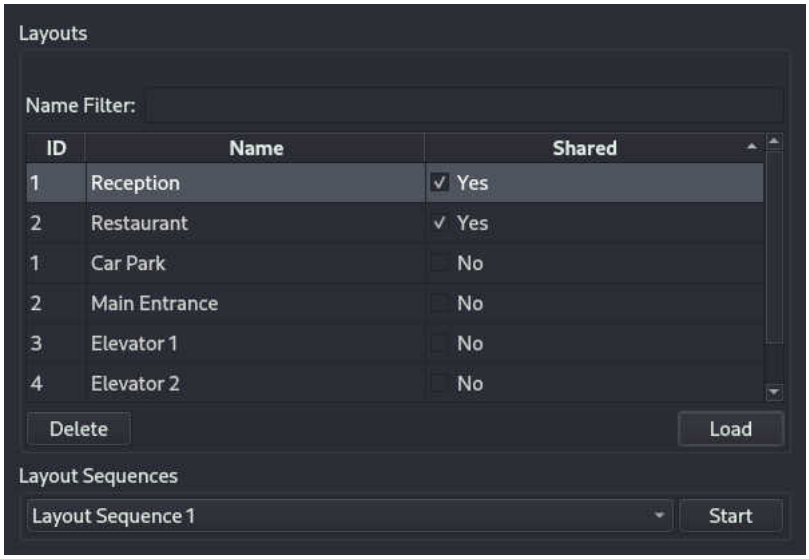


Layouts can be loaded by right–clicking the Display Area and choosing "Load Layout...", or by clicking the Load Layout button in the Display Area Toolbar...

A list of saved layouts is presented, with the Shared Layouts shown first. Note that shared layouts and personal layouts each have their own list of IDs, so it's possible to see multiple layouts with the same ID, where one is shared and the other isn't.

The "Name Filter" box at the top allows layouts to be searched. Simply start typing to filter the list to only layouts containing that text.

Layouts can also be deleted from here.



To load the Layout, either double–click it's entry in the table, or click once and click Load.

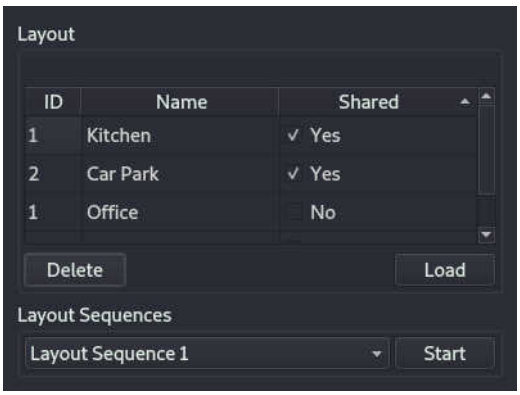
When layouts are loaded, they will inherit the playback state of any selected display in the Video Display Area. For example, if an existing display is currently playing back from 10 minutes ago, the newly displayed layout will load at that time point and continue playing.

3.7.2 Triggering Layout Sequences

Layout Sequences allow layouts to be automatically loaded consecutively with configurable durations for each one. They are configured in the Setup Screens by an "install" or "admin" level user.

Layout sequences are triggered from the Load Layout dialog, which can be accessed either by right–clicking the Display Area and choosing "Load Layout...", or by clicking the Load Layout button in the Display Area Toolbar...

At the bottom of the Load Layout dialog, a drop–down list of configured Layout Sequences is presented. To start a Layout Sequence, choose the desired sequence and click Start.



Once the Layout Sequence has started many of the facilities relating to the Display Area are unavailable until the sequence is stopped. The Display Area Toolbar has a new Stop button which will be present if a Layout Sequence is running.

3.8 Device Tree

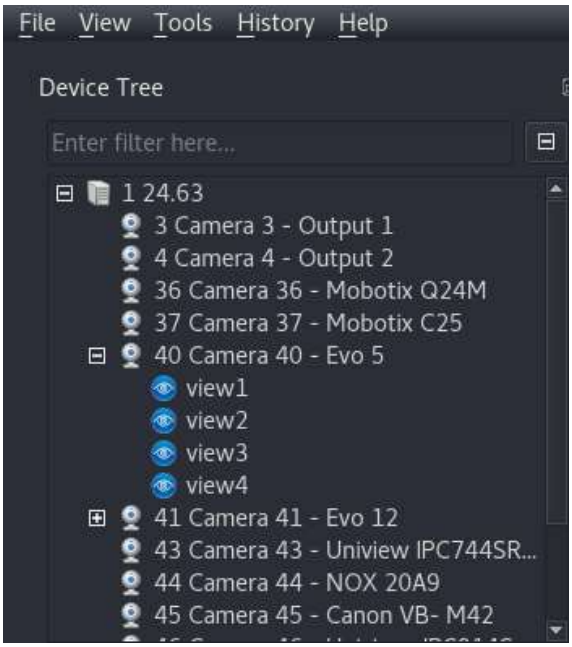


Figure 3.35: Device Tree

The Device Tree displays the currently connected Wavestore Servers, with enabled Audio and Video Channels listed beneath.

The Filter box at the top allows the user to start typing the name of a server, channel, or view, and only items matching that text will be shown.

The icon to the right of the filter box allows expanding or collapsing all the items in the tree.

Right clicking on the Device Tree text allows you to view the select various display options for the Device Tree:

- Display either Channel Tree (all channels) or Camera Group Tree (if this option has been configured)
- Show Channel IDs
- Show Disabled Channels

- Show Servers
- Show Servers IDs
- Show Views (saved 'virtual camera' dewarped or panoramic views from panoramic cameras are shown)

These settings are automatically saved so they are preserved when WaveView is restarted.

When "Show Servers" is disabled, only the cameras and views are displayed. If using a server group it is sensible to give cameras unique "sort IDs" across the group, otherwise the ordering of cameras may not be as expected. See section 9.21 – Sort IDs for more information.

Double-clicking on a Channel Name on the Device Tree, causes the video from that Channel to be displayed in the Video Display Area. Alternatively,

Multiple-cameras can be selected and then dragged onto the Video Display Area. Holding CTRL and left-clicking selects individual cameras, whereas holding SHIFT selects a range.

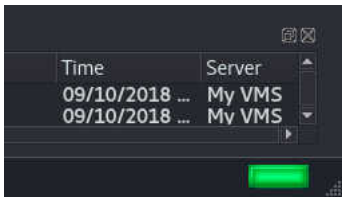
If the Video Display Area is currently viewing one Video Display only, the Video Display is switched to the newly selected channel. Otherwise a new Video Display (containing the new Channel) is added to the Video Displays that are already displayed within the Video Display Area.

Double-clicking on a Channel Group name on the Device Tree, causes the video from the cameras in that Channel Group to be displayed in the Video Display Area.

3.9 Status Indicator

The Status Indicator provides a quick summary of the status of all servers in the group. It changes colour to show the worst status of all servers in the group. For example if all servers are OK except one has a Fault status, it will show red for the fault status.

The Status Indicator can be clicked to jump to the System Log to inspect more details of any issue with the servers in the group.



The possible statuses are as follows:

Recording

The system has no detected issues and is recording from at least one camera.
Shows a green Status Indicator and transparent background for the server name in the Device Tree.

Unlicensed

The server doesn't currently have a valid licence and therefore is not recording.
Shows an amber Status Indicator and amber background for the server name in the Device Tree.

Server awaiting restart

The server currently requires a restart to apply recently made configuration changes.
Shows an amber Status Indicator and amber background for the server name in the Device Tree.

Recording not enabled

The server is functioning correctly but no recording is occurring.
Shows an amber Status Indicator and amber background for the server name in the Device Tree.

Standby

Used as part of the Failover mechanism, this server is acting as a Standby server.
Shows an amber Status Indicator and amber background for the server name in the Device Tree.

Starting

The system is starting up.
Shows an amber Status Indicator and amber background for the server name in the Device Tree.

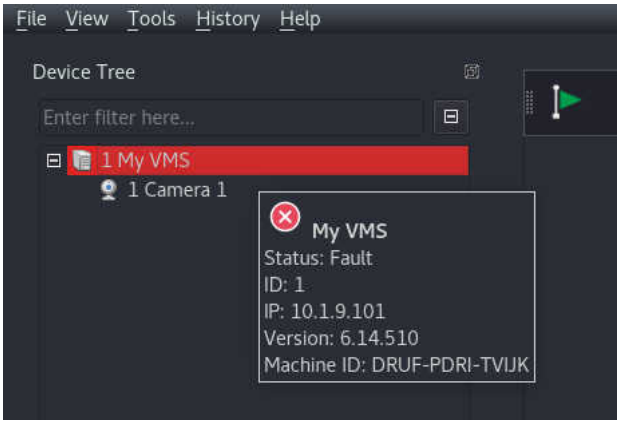
Fault

This server has a problem. Inspect the System Log to find out details of the problem.
Shows a red Status Indicator and red background for the server name in the Device Tree.

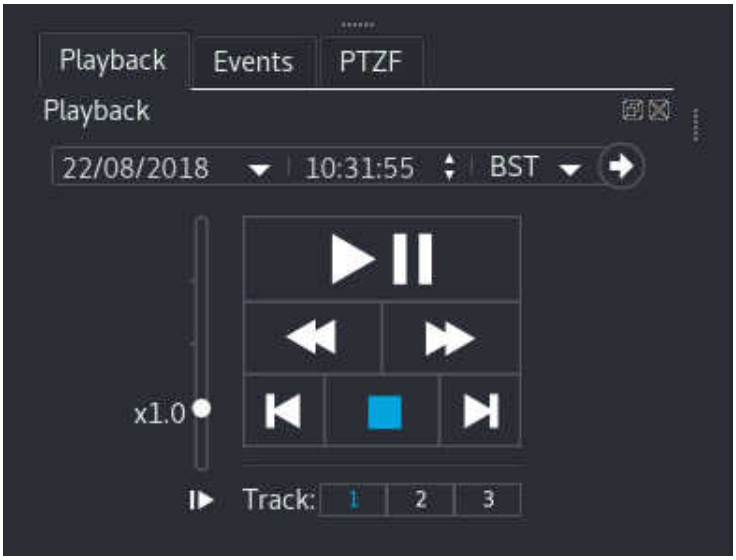
Failed

This status is shown when a Force Failover event occurs. This means that an event rule has put this server into a "Failed" state, and caused failover to occur.
Shows a red Status Indicator and red background for the server name in the Device Tree.

The server status is also indicated in the Device Tree as the background colour for the server name. Hovering the mouse over the server name also provides details of the status, as shown below.



3.10 Playback Controls



The playback controls affect any currently selected Video Display (highlighted with blue frame) in the Display Area, and operate as follows:

Play/Pause Starts/pauses playback of the stream

Rewind/Frame Step Back A single left–click steps back a single frame. Holding the left mouse button starts Rewind; the speed of Rewind increases the longer the mouse button is depressed.

Fast Fwd/Frame Step Fwd A single left–click steps back a single frame. Holding the left mouse button starts Fast Forward. The speed of Fast Forward increases the longer the mouse button is de–pressed.

Beginning of Archive Jumps to the oldest recording on the currently selected Channel and Track

Stop Exits playback to return to Live View

End of Archive Jumps to the latest recording on the currently selected Channel and Track

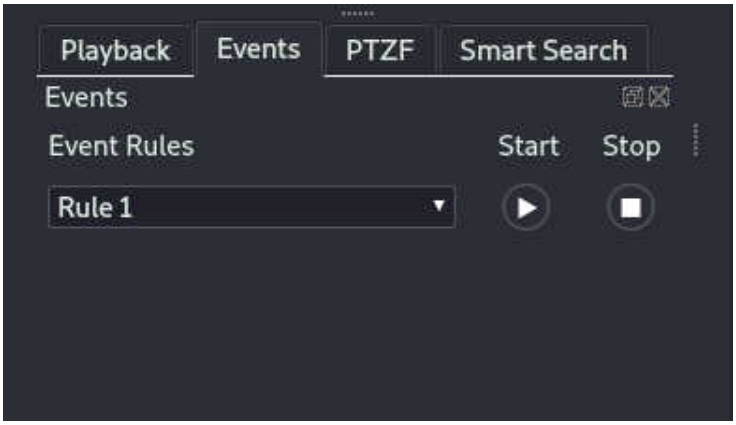
Go to field Allows you to access a specific point in time by directly entering Date and Time

Playback Speed slidebar Click and drag the slide bar to choose playback between 0.1x – 4.0x real time. Note that the maximum is configurable, see section 3.22.5 – Playback. Also note that fast playback requires a powerful PC and the video may jump if the system is not powerful enough. This mech–anism is not a substitute for the Fast Forward operation.

Track Selection buttons 1/2/3 Allows you to select a recording track for the selected video displays.

After selecting a track (either 1, 2 or 3), all playback operations described above will affect this track only. The text display in the top right hand corner of the Video Display indicates whether the status of the video stream being viewed (Live/Play/Paused).

3.11 Events Control



The Events control allows Event Rules to be started or stopped (in the case of an "On/Off" type of Manual Trigger), or triggered (in the case of a "Pulse" type Manual Trigger).

The drop-down list consists of the names of all Event Rules where the Causes contain a Manual Trigger. When a rule is selected, if the Manual Trigger in the rule is an "On/Off" type, then On and Off buttons are presented, which can be used to activate and deactivate the Manual Trigger within the event rule. If it is a "Pulse" type (in other words "instantaneous"), then a single "Pulse" button is provided to allow the Manual Trigger to be triggered.

See section 6.12 – Event Rules for more details on configuring such rules.

3.12 PTZF Controls

Figure 3.36: PTZ Controls

The PTZF Controls Panel allows control of configured Pan/Tilt/Zoom cameras. These controls will be disabled if:

- The active camera is not a PTZ camera
- The current user does not have permission to control PTZ actions on this camera

Available controls are:

- Pan left/right
- Tilt up/down
- Zoom in/out
- Focus in/out
- Iris open/close
- Movement Speed Control slider
- Shift left/right – for rail mounted cameras
- Wash
- Wipe
- Lamp toggle

- Go to/Setup a Preset Position (see section 3.12.1 – Setting PTZ Preset positions)
- Start/Setup a Tour (see section 3.12.2 – Setting PTZ Tours)

3.12.1 Setting PTZ Preset positions

Access the Live Screen by following the menu path View → Main, and open a Video Display for the PTZ camera by.

Using the PTZF controls, move the camera to the desired position.

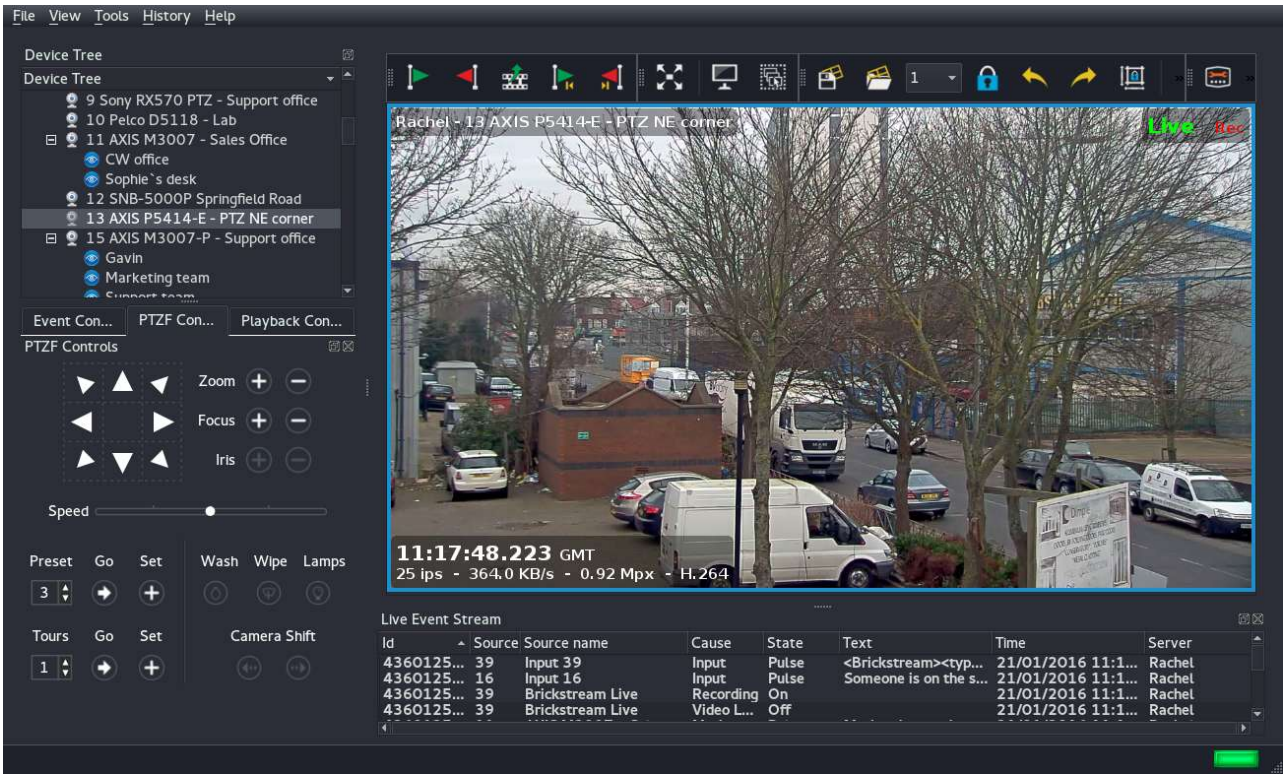


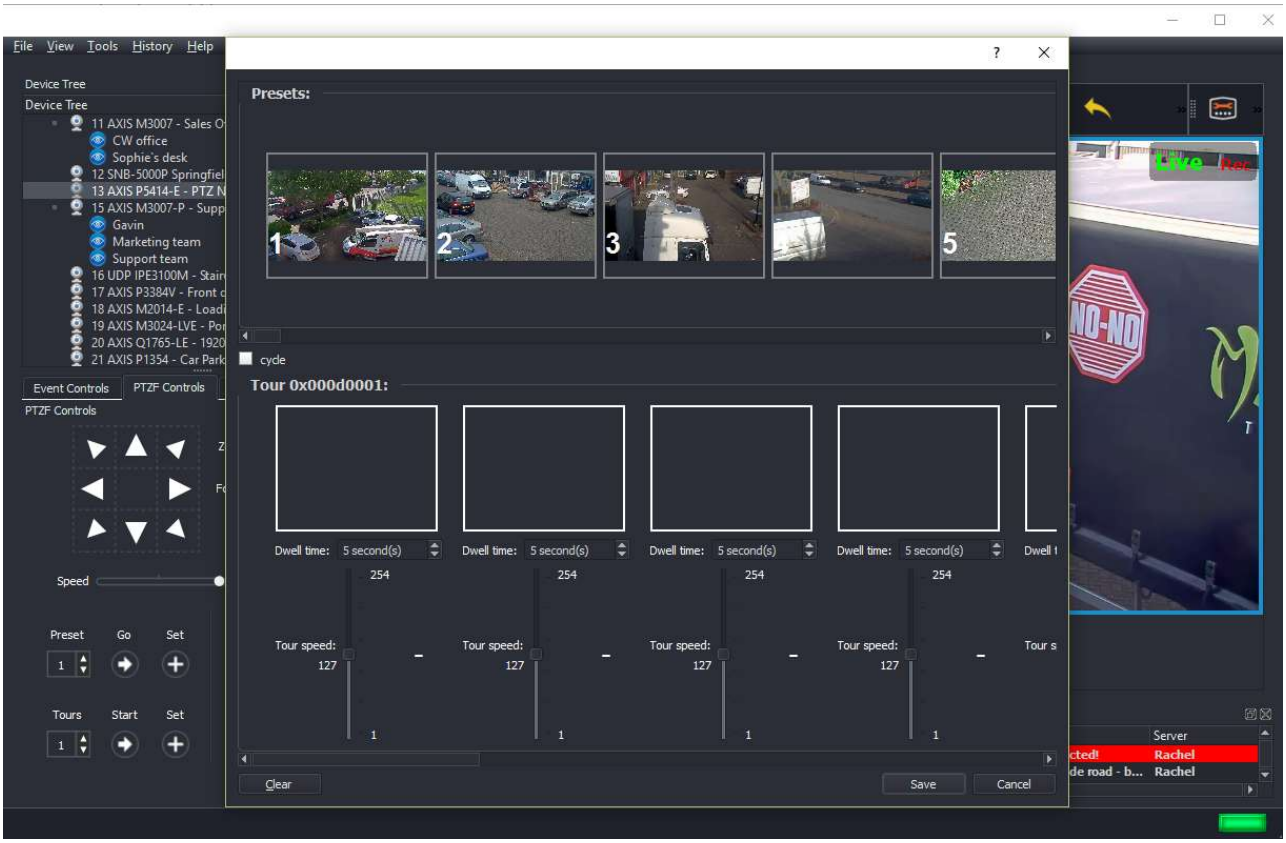
Figure 3.37: Live View screen showing PTZ controls

In the Preset section, use the arrow keys to call up the Preset number that you want to assign, and then click 'Set'.

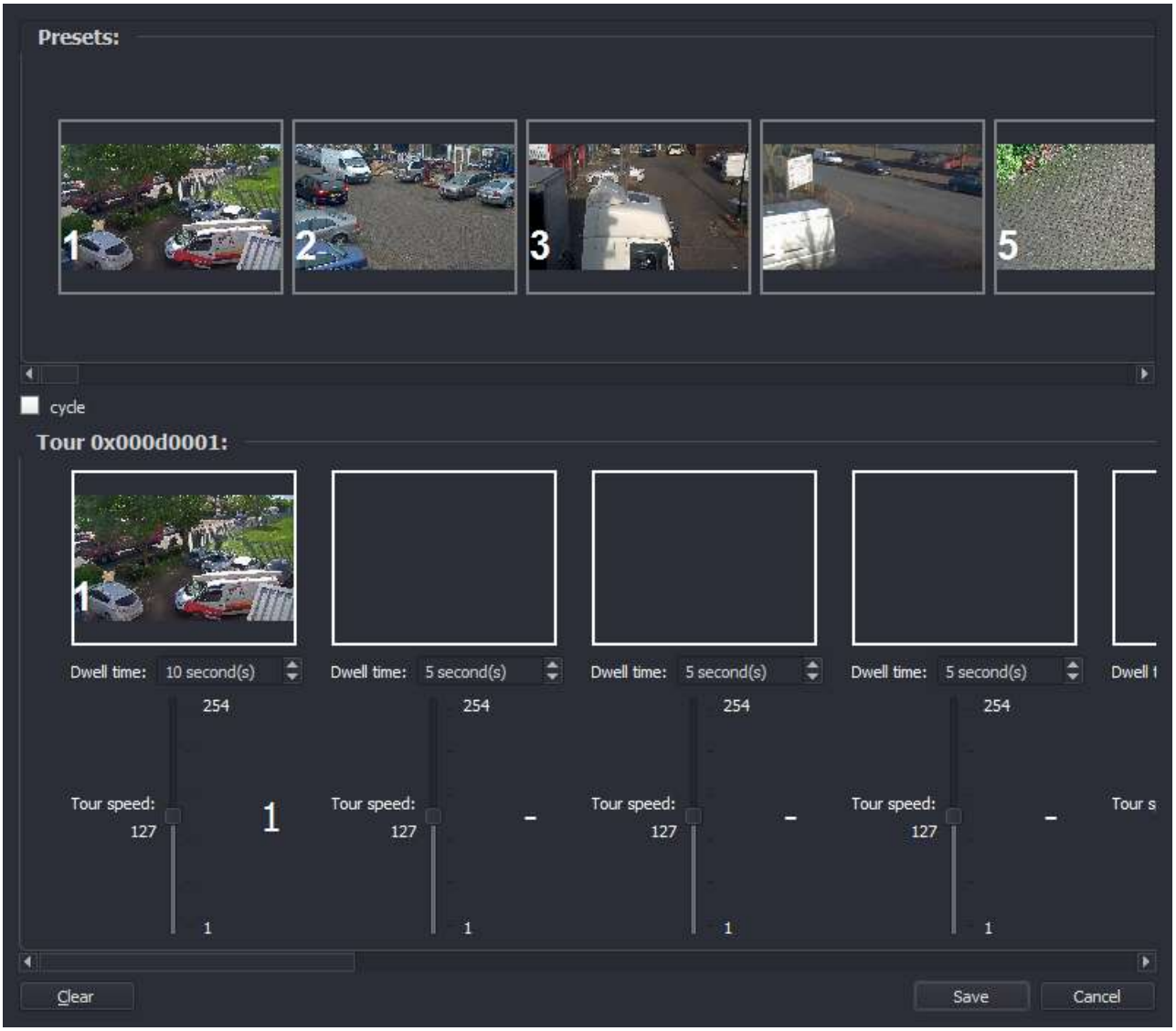
If you want to check the position of saved Preset, move the camera to another position, use the arrow keys to call up your desired preset position, and then click 'Go'.

3.12.2 Setting PTZ Tours

Use the arrow keys to call up the Tour number that you want to assign, and then click 'Set'. The Tour configuration window will now appear, showing preset views currently configured on the server.

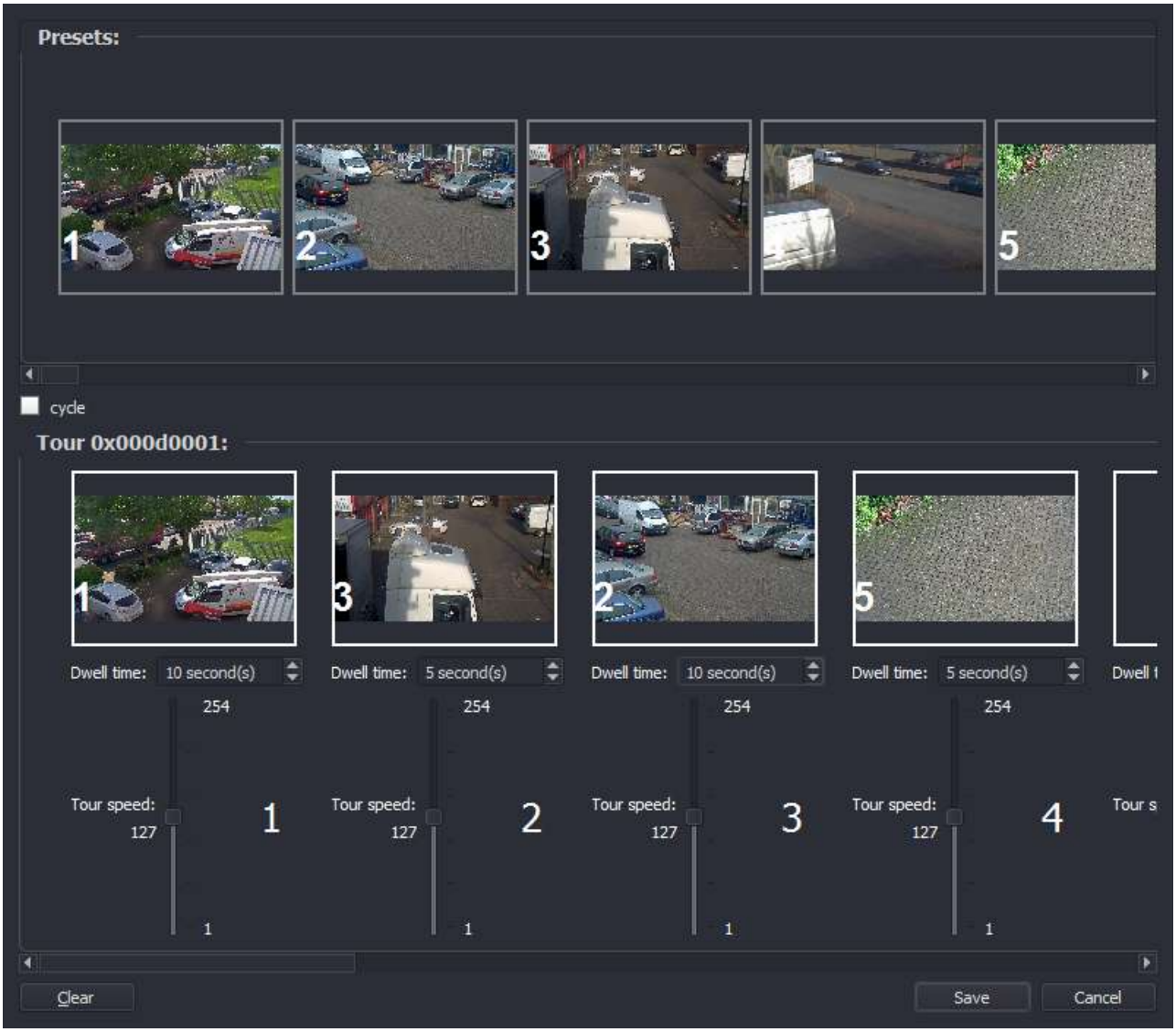


To configure the first position on the tour, drag and drop the one of the Preset views into the first window in the Tour section.



Use the Dwell Time and Tour Speed settings, to configure how long the camera should remain at that preset position, and the speed at which it will move to the next Preset position. Note that the Speed setting is only supported on a limited number of cameras.

Repeat the above steps for the remaining preset positions that you wish to add to the tour.



If you want the tour to operate continuously (cycling from the last Preset position back to the first), select the 'Cycle' option.

Finally click on 'Save' to return the Live View screen.

To start the tour operating from the Live View screen, use the arrow keys to call up the number of your desired tour, and then click 'Start'.

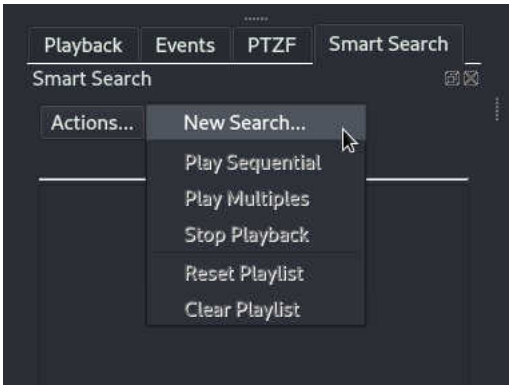
3.13 Smart Search Control

The Smart Search control allows a post–recording search of a period of recordings based upon motion or video analytics data. This section documents how to perform the Smart Search, assuming the cameras have been appropriately configured. See section 9.8 – Configuring Smart Search for information on how to configure cameras for Smart Search.

Note that Smart Search is also available in the Find screen, however the Main screen implementation supports the Multiple playback mode, whereas the Find screen does not. This is because the Find screen

is intended to show all cameras at the same point in time, but the Multiple playback mode requires showing the cameras at different points in time. Also, analytics searches are only currently supported in the Main screen.

The *Actions...* menu can be used to perform the various relevant operations.



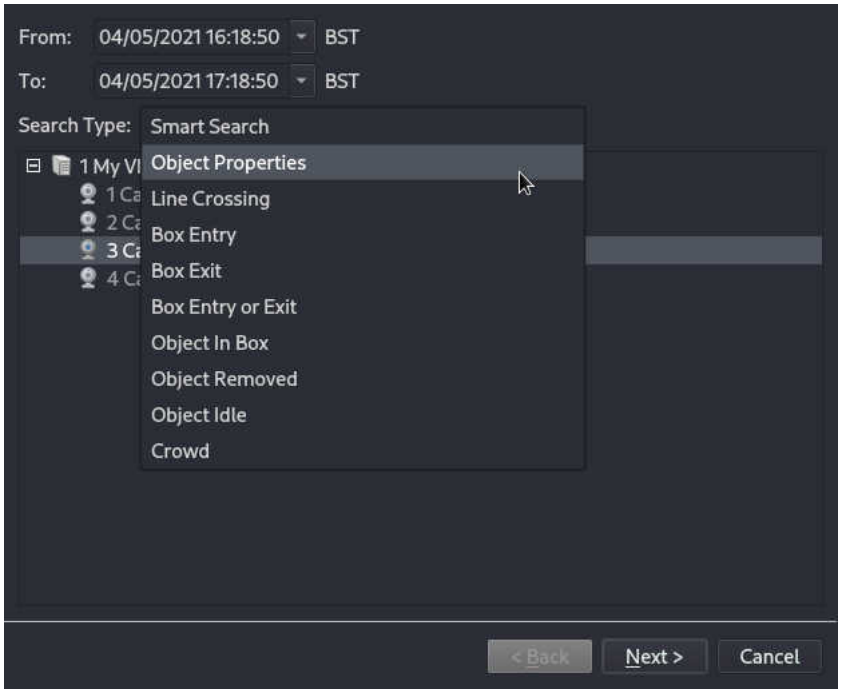
The *New Search...* option opens a wizard to build a search query. The remaining options are used to control playback of the results.

3.13.1 Performing a Smart Search

The first page allows the following to be selected:

- The time range for the search
- The type of search
- The camera(s) to be searched

The *Search Type* selector will only contain search types available for the currently selected camera. If no cameras are selected, it will show the aggregate of all search types available for all cameras. For any camera which is currently unavailable for selection for the current search type, a tooltip is available explaining why, visible by hovering the mouse over the camera name.



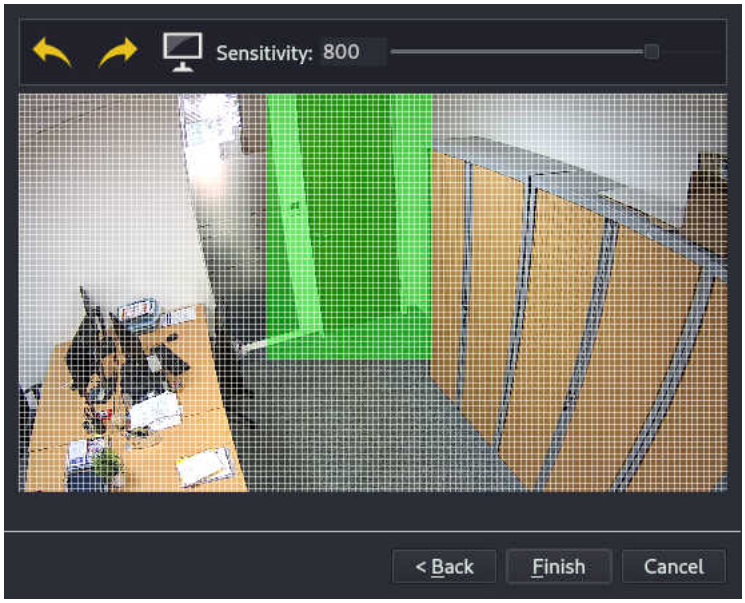
Once the desired parameters for the search have been set, clicking ***Next >*** will advance to the next page in the search wizard.

The options available for each search type are discussed below.

Motion Search

Motion Search performs a historical search based on the motion within the scene.

A mask, or area of interest, and a sensitivity can be specified for the search. The default sensitivity is often appropriate. The last sensitivity and mask is recalled on a per-camera basis to help make repeated searches easier.

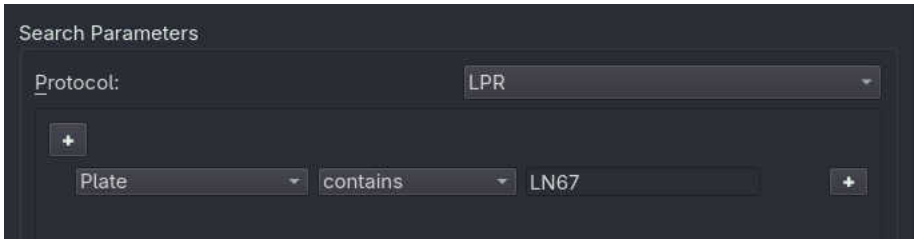


When the mask and sensitivity have been set and the ***Finish*** button is clicked, the search will be performed.

The search is performed on 4 second blocks of recordings and so the results will always have durations which are multiples of 4 seconds. This means that, when playing back the results, the lead-in before the actual motion occurs could be 0 to 4 seconds.

Metadata Search

This search type allows searching metadata. This metadata is normally configured when installing purchased integration modules and instructions for setup are included with the integration module.

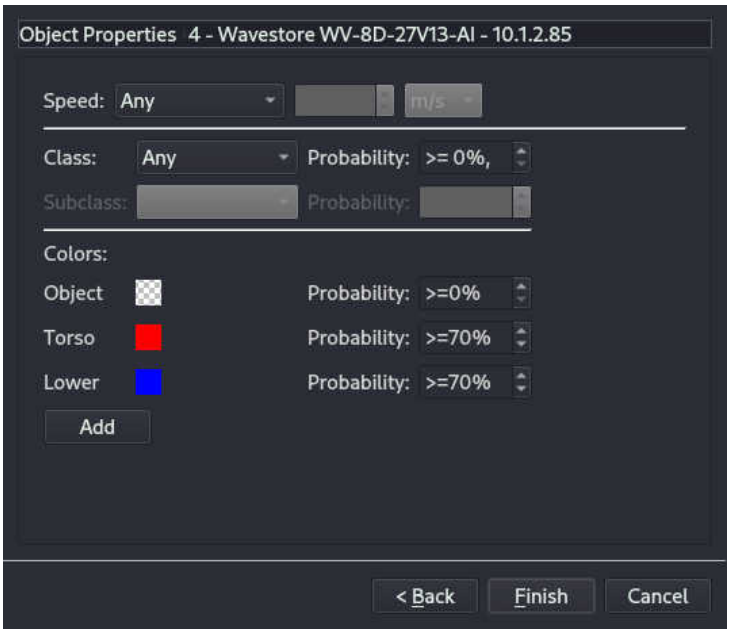


When performing a search, firstly the Protocol should be selected. This will be something like Point-of-Sale or License Plate Recognition. Next, the desired field type should be selected. This might be "Price" for Point-of-Sale, or "Plate" for LPR. Next, the query type should be selected. For text fields this might be something like "Contains" or "is equal to". For numerical fields, queries such as "is greater than" or "is less than" are available. Finally, the search data should be entered.

Multiple conditions can be specified by clicking the "+" button to add another query. The search will return results that match all queries.

Object Properties

This analytics search allows searching of analytics object data to match various properties of the objects.



It is possible to search on the object speed, being greater than or less than the specified value. The units can be ***m/s (metres per second)***, ***mph (miles per hour)***, or ***kph (kilometres per hour)***. Alternatively, if 'Any' is selected, the speed is not checked in the search.

It is also possible to search on the object class and, optionally, subclass. The availability of the subclass option is dependent on the source of the analytics data for the current camera.

For the class and subclass matching, it is possible to provide a minimum probability for the object matching that class.

If supported by the selected camera, it is also possible to search by ***Segment Colour***. A segment is a part of the object, e.g. Torso, Lower. Either select a colour, or select the checkerboard to indicate no colour. For each segment, a probability of that colour can be specified.

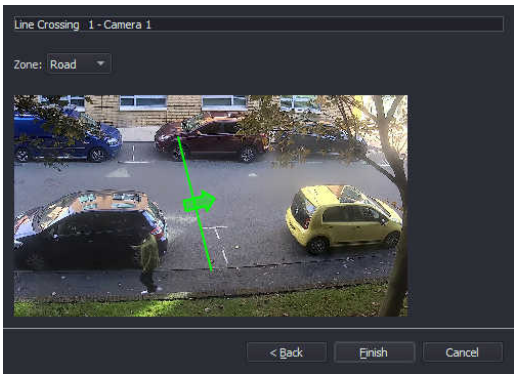
Once the desired parameters have been chosen, clicking ***Next >*** will perform the search.

Line Crossing

This search allows detecting objects crossing a line, in either direction or both. The object properties can also be matched.

The first page presented is the same as the ***Object Properties*** search type. To search for any object, just click the ***Next >*** button.

The second page allows configuration of the line.



Lines which have been previously configured can be selected from the drop-down list, but not edited. Alternatively, "Custom" can be selected and then the line can be edited as follows:

- Click and drag a circular end-point of the line to move that point
- Click and drag on the line to move the whole line
- Double click the arrow to change the direction of the arrow.

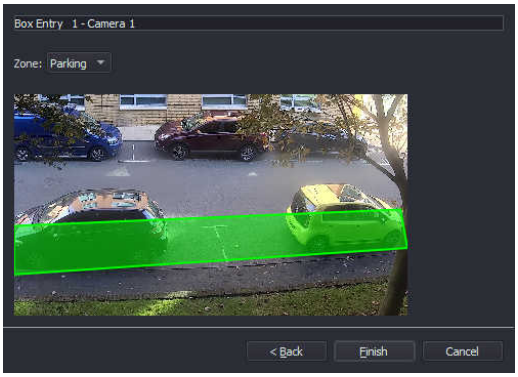
Once the desired line has been configured, clicking ***Next >*** will perform the search.

Box Entry

This search allows detecting objects entering a region. The object properties can also be matched.

The first page presented is the same as the ***Object Properties*** search type. To search for any object, just click the ***Next >*** button.

The second page allows configuration of the box.



Boxes which have been previously configured can be selected from the drop–down list, but not edited. Alternatively, "Custom" can be selected and then the box can be edited as follows:

- Click and drag a circular end–point of the line to move that point
- Double–click on an edge of the box to add another point
- Double–click a circular end–point to remove it
- Click within the box and drag to move the whole box

Once the desired line has been configured, clicking ***Next >*** will perform the search.

Box Exit

This search is the same as ***Box Entry*** except it detects objects leaving the region instead of entering.

Box Entry or Exit

This search is the same as ***Box Entry*** except it detects objects leaving the region as well as entering.

Object In Box

This search is the same as ***Box Entry*** except it returns results for the duration that the objects were inside the the region.

Object Removed

This search allows detection of objects being removed from the scene. For this search type, the 'zone' is optional.

The first page presented is the same as the ***Object Properties*** search type. To search for any object, just click the ***Next >*** button.

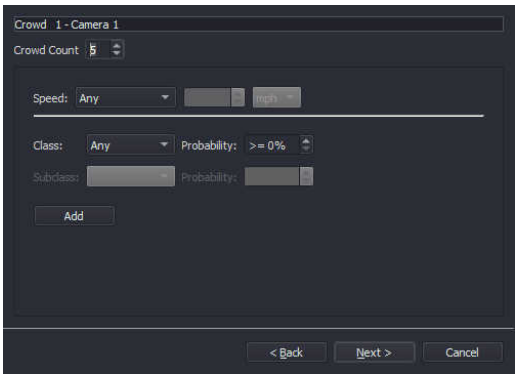
The next page is used to configure the zone. Only objects removed from within the zone will be matched. The zone configuration page is the same as described in ***Box Entry***.

Object Idle

This search is the same as ***Object Removed*** except it returns results for when an object becomes idle, i.e. not moving, instead of when the object is removed.

Crowd

This search allows detecting when a certain number of objects are within a certain zone.



The first page presented is similar to the ***Object Properties*** search type. To search for any object, leave the settings as default.

This page also allows choosing the ***Crowd Count***, which is the minimum number of objects within the zone to trigger a match.

There is also a checkbox for 'Use Entire Scene'. If checked, the page to configure the zone is skipped. Otherwise, the next page allows configuring a zone, in the same way as described for ***Box Entry***.

3.13.2 Reviewing Smart Search Results

When the search has completed, the results are shown in the playlist. The way the results are presented can vary depending on the type of search performed. Also, the playlist can be undocked and will provide extra columns, giving extra detail about the results of the search.

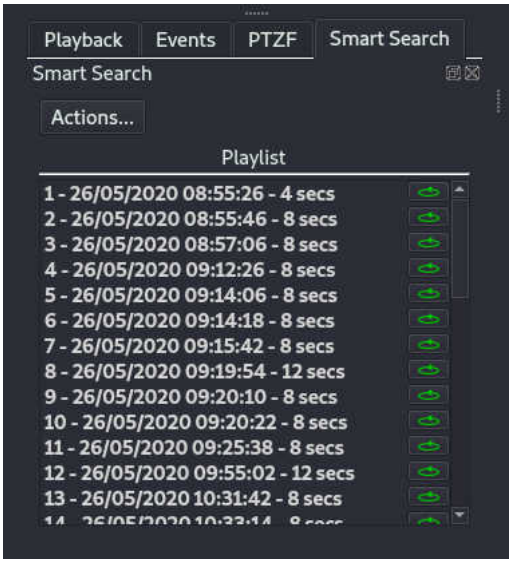
All searches give:

- A start time
- A duration
- A "loop" control

Many analytics searches will present the results in a tree–like structure grouped by the Object ID. This is because there may be many matches for the same object and the playlist entry represents the time duration for the matches for that object.

A ***Crowd*** search will show the crowd count for the results. Again these will be in a tree–like structure grouped together if the crowd count is the same and the result is within a few seconds of the last result. Note that small changes in the crowd count are ignored. For example if there are many results with a crowd count of 4, with one result of 3 in the middle, the 3 will be grouped in with the results for 4. This is to prevent brief miscounts of the crowd resulting in separate playlist items.

Each item in the playlist has a button to control whether the item playback should be looped.



Now that there are results in the playlist, the ***Actions...*** button allows more operations to be performed. These are described below:

Play Sequential
: This sets the Display Area layout to "1", for a single camera. It then plays the items in the playlist one by one. They are not set to loop so when each one finishes it will play the next.

Play Multiples
: This fills the current layout with cameras from the playlist and automatically adds new ones each time one is closed. It defaults to a 2x2 grid, but if there is already a grid selected (e.g. 4x4) it will use that. The cameras are looped by default so they will repeat until closed.

Stop Playback
: This stops the playback of the playlist.

Reset Playlist
: This sets all the items in the playlist back to the "unplayed" state.

Clear Playlist
: This removes all items from the playlist.

During playback, unplayed items are shown with bold text, items being played are highlighted in blue, and played items are shown in normal text with no highlighting.

As well as the Sequential and Multiples playback modes described above, it is also possible to simply double–click an item to open it from the playlist.

3.14 Layouts Control

The Layouts control provides convenient access to the layout load dialog. See section 3.7 – Layouts for details on its use.

3.15 Quick Search Controls using Time Slider

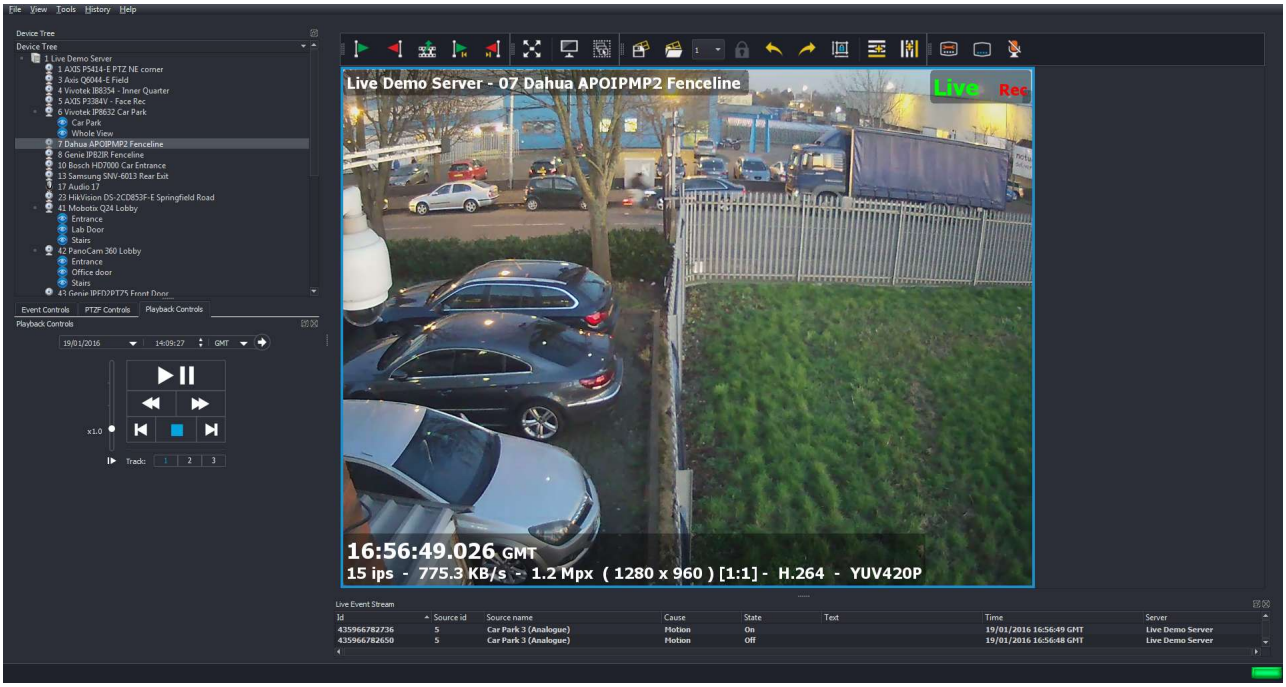


Figure 3.38: Video Display showing Live View from Camera 3

If you move the mouse pointer over the lower edge of an individual camera view, a quick search time slider with playback controls appears as shown below.

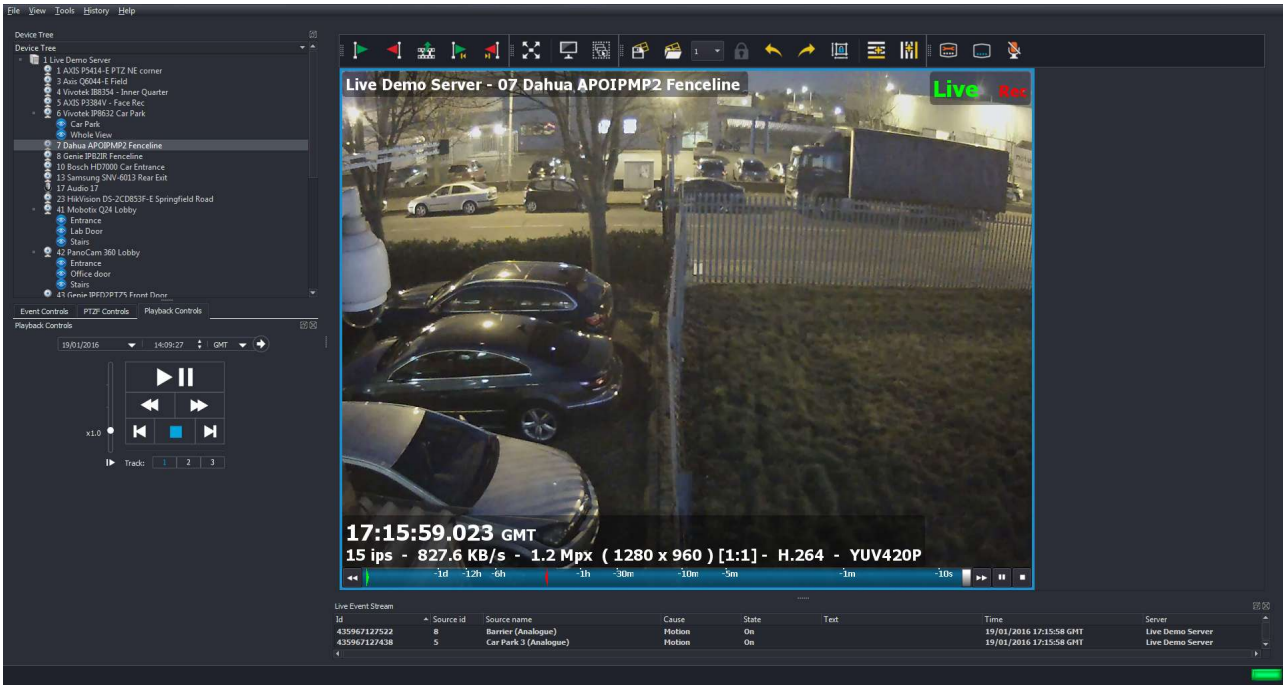


Figure 3.39: Video Display showing Live View from Camera 3 with time slider bars

The dark grey bar represents the footage on the selected recording track for this camera (oldest footage at the left, most recent footage on the right). The grey bar will contain gaps for any periods when the channel was not recorded by the server (e.g. a channel configured for Motion Detect recording).

The light grey slider shows displays the current position on the recorded track The quick search play–back control buttons (either end of the time slider) allow you to pause or resume playback, frame step forward/backward (quick click), and also fast forward and rewind (click and hold).

Clicking and dragging on the light grey slider gives the user control of the current playback position on the recorded track.

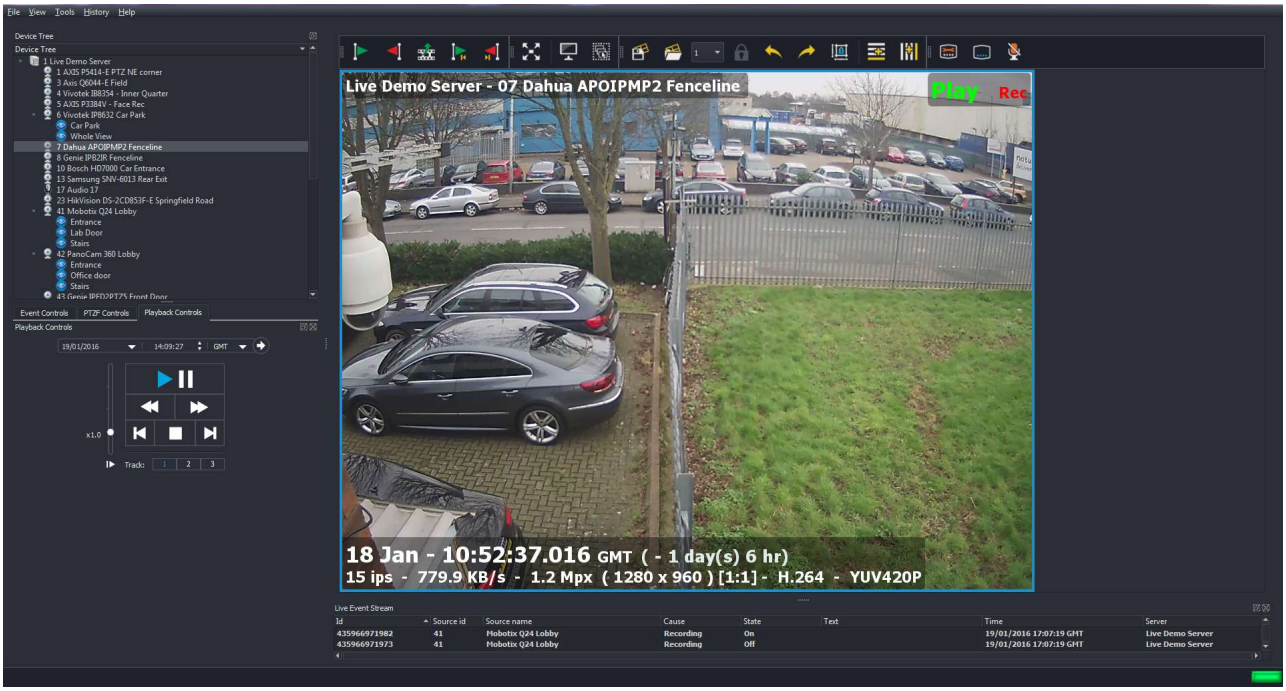


Figure 3.40: Searching using Grey Time Slider bar

To carry out a more detailed search, hover your mouse pointer over the blue time slider, and roll the mouse wheel forward.

Rolling the mouse wheel forward/backward will zoom in/out on the time period; as you do this, the scale of the time increments will change, as below:

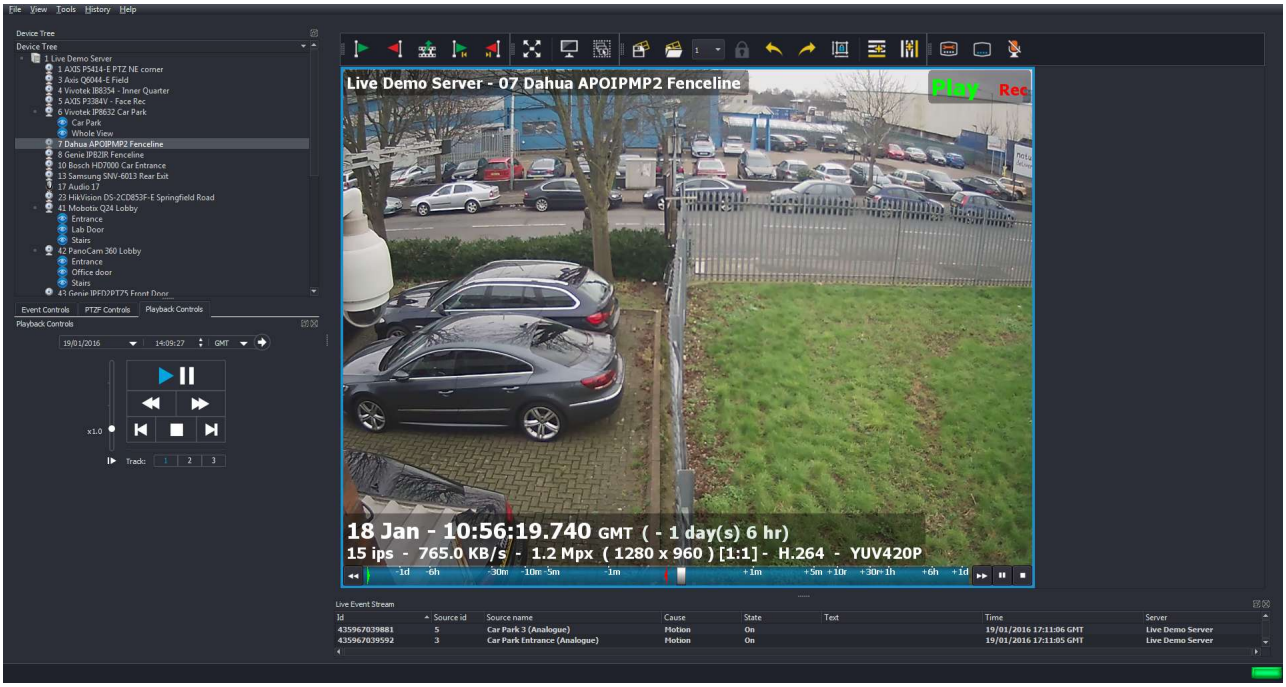


Figure 3.41: Time Increments on Blue Time Slider bar changed by rolling mouse

Wheel Clicking on a point on the either side of the grey slider moves the current playback position to that point in time.

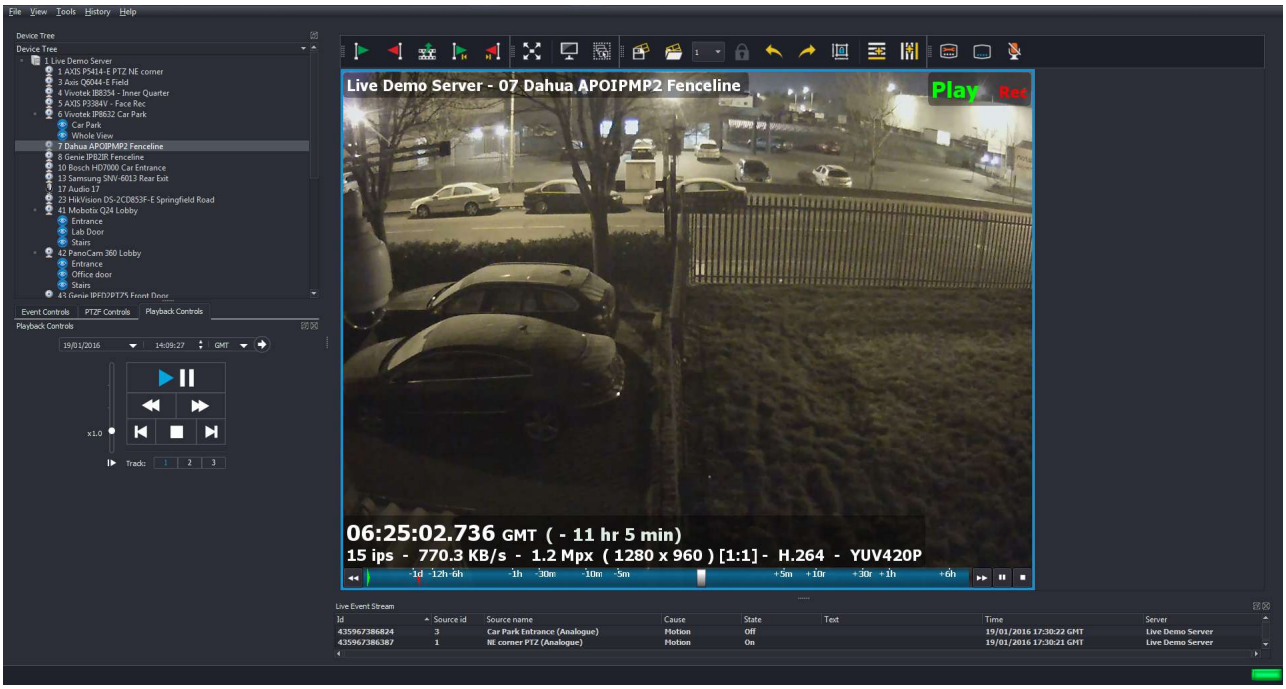


Figure 3.42: Time of display moved forward four minutes by clicking on Time Slider bar

If you wish to look at footage from another camera at the same point in time, you may need to first re-configure your display type (e.g. from a single camera display).

You can do this by using the drop down menu on the Display Area Toolbar:

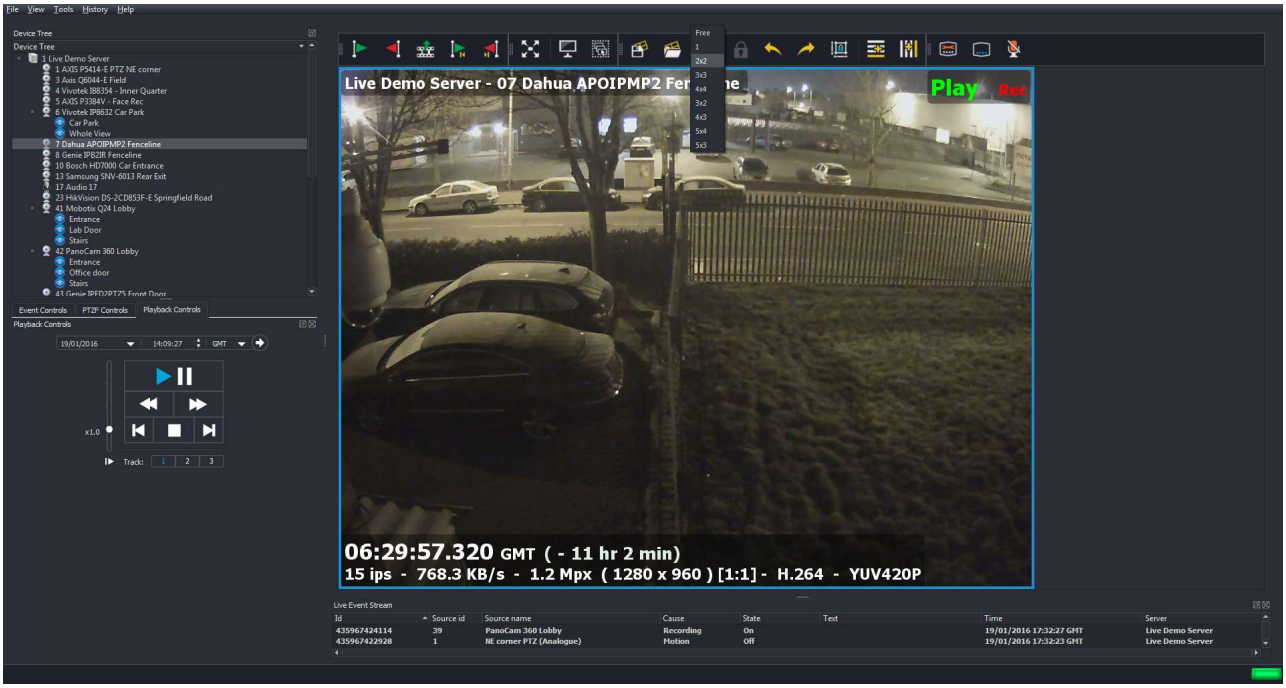


Figure 3.43: Changing display configuration using drop down list

Alternatively you can click on either the 'Add Row to Grid layout' or 'Add Column to Grid Layout' buttons on the Video Display Toolbar:

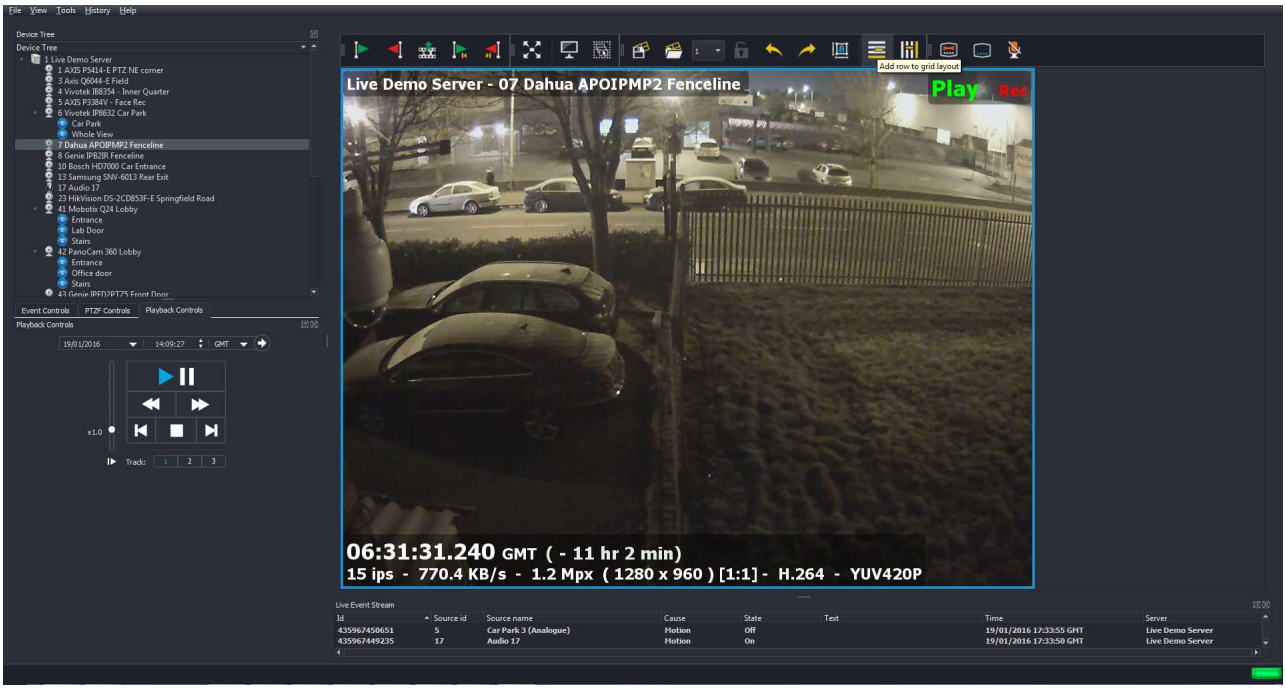


Figure 3.44: Changing display configuration using 'Add Row to Grid Layout' button

The Video Display configuration will now change:

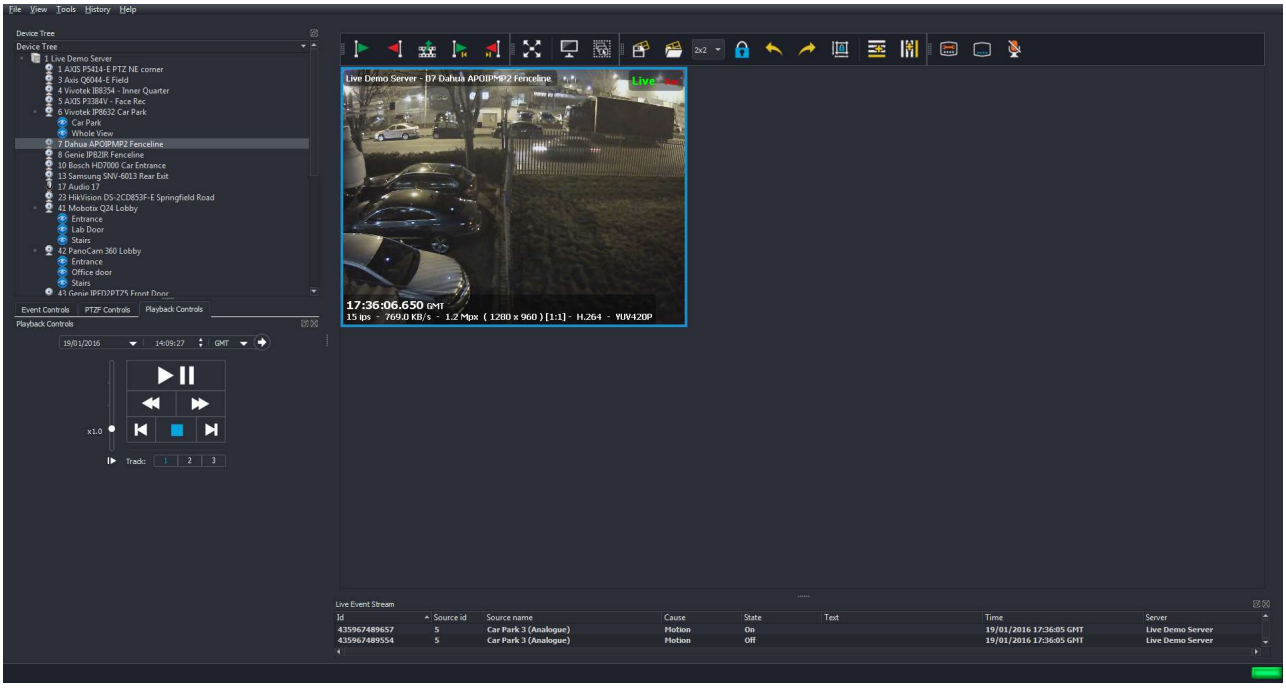


Figure 3.45: New Display Configuration

To add the video, first check that the current Video Display is selected so that the frame is highlighted blue (click within the Video Display if not), and pause playback.

Next, double–click on the name of the camera in the Device Tree that you want to add to the display.

The new camera will now be added to the display:

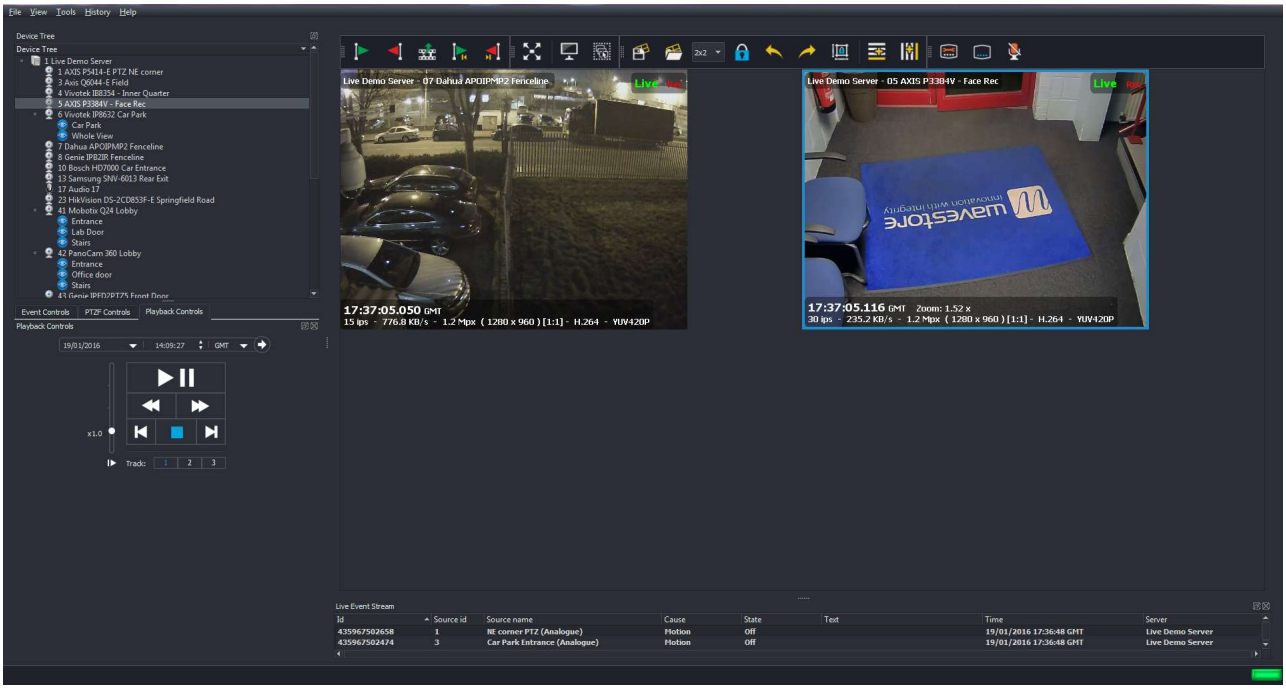


Figure 3.46: Camera 7 added to display (in Playback Mode), paused at same time as Camera 3

To return a Video Display to Live View, just click on the Stop icon within that display.

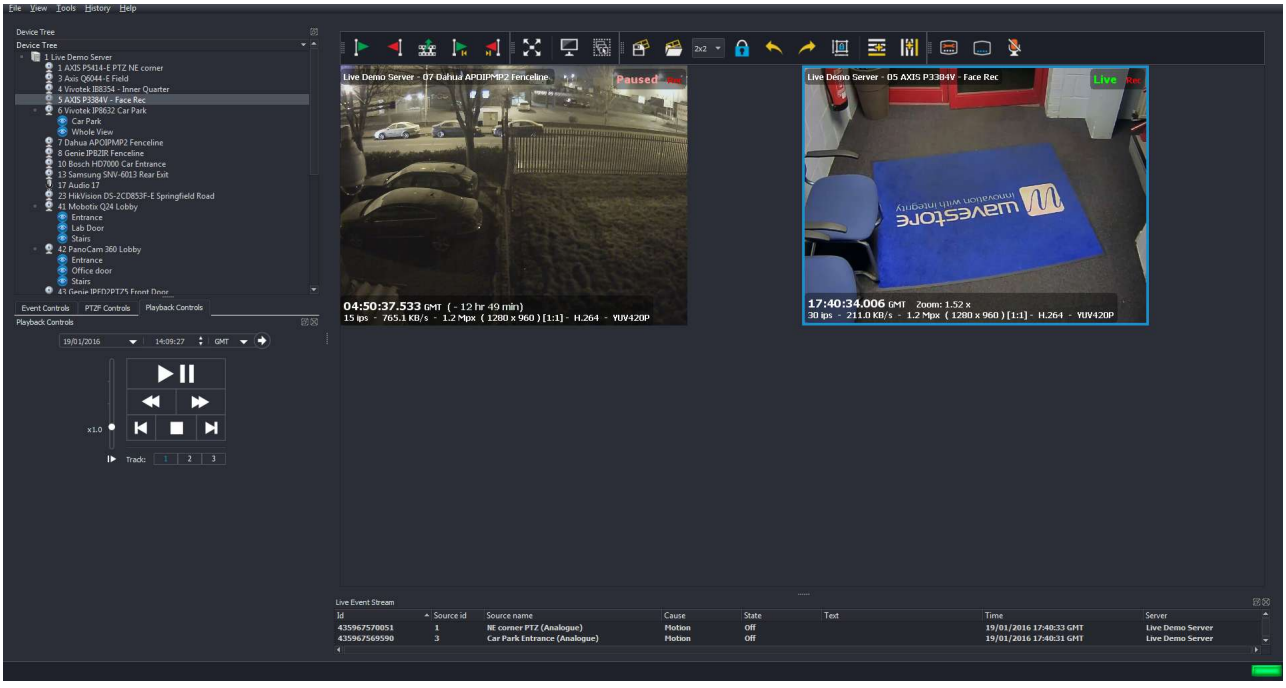


Figure 3.47: Camera 3 paused in Playback mode, Camera 7 in Live View mode

3.16 Quick Export for Single Camera Channel

If the Video Display that you are working with is a dewarped view from a hemispheric camera (see Appendix B), you can pan/tilt/zoom within the Video Display during playback to track a person or object, and these movements will be shown in the export file once created, if you select any export format other than the Wavestore Native format (WSB), for example AVI or WMV.

A WSB format export will contain the full warped video stream for that camera, and any dewarped views that have been saved for that camera.

Please note that the permissions of the user making the export may conditionally limit the functionality of the exported data. For example, if the current user does not have permission to make transcoded exports (e.g. converting to AVI), any WSB export made by that user will contain that permission setting, meaning that the resulting WSB export cannot be subsequently converted to another format. This design is intentional, to prevent a possible workaround where a user could make an AVI by first creating a WSB export then opening the export and converting it to AVI.

If there is a critical need to override these settings, staff at Wavestore Limited can do so, but it is not trivial and a fee may be charged.

3.16.1 Quick Export for Standard Camera

Once we have identified required footage using the Search function, we can carry out an export for a single camera from the Live Screen as follows:

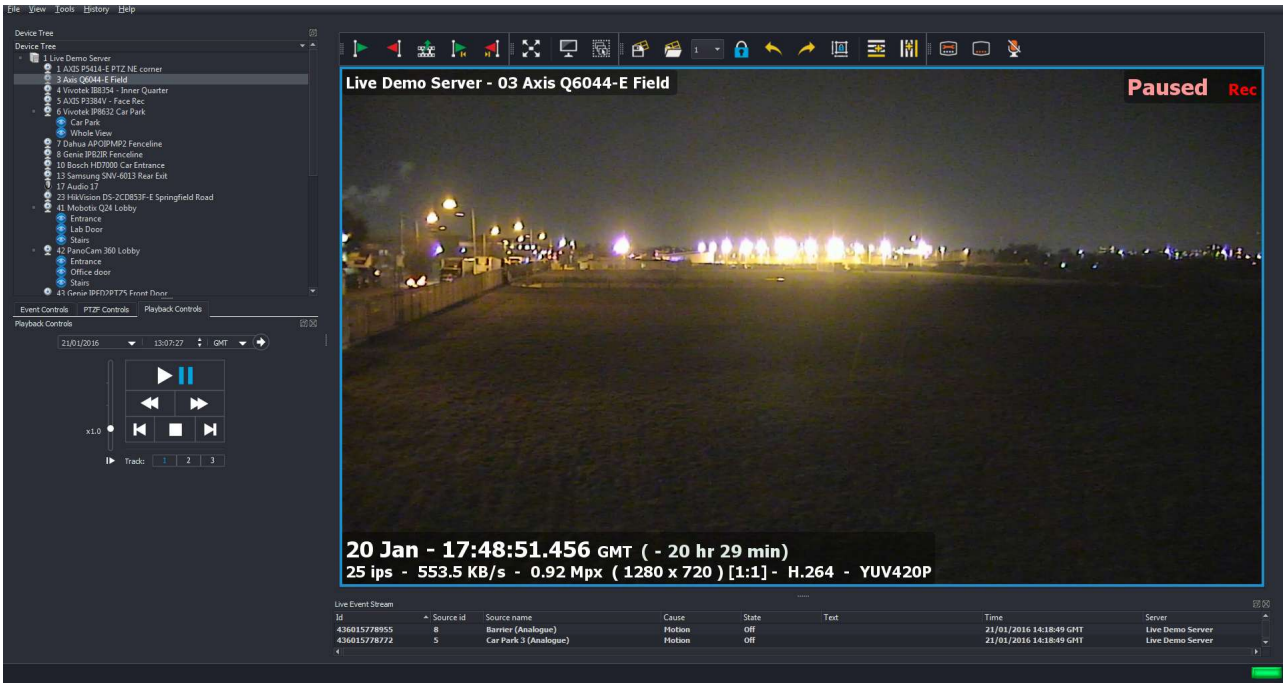


Figure 3.48: Quick Export – Playback paused at the start of required footage

Click on the 'Mark Time for Start of Export' button (green flag icon) on the Video Toolbar when you have reached the start point of the footage that you require (use the Pause function if necessary).

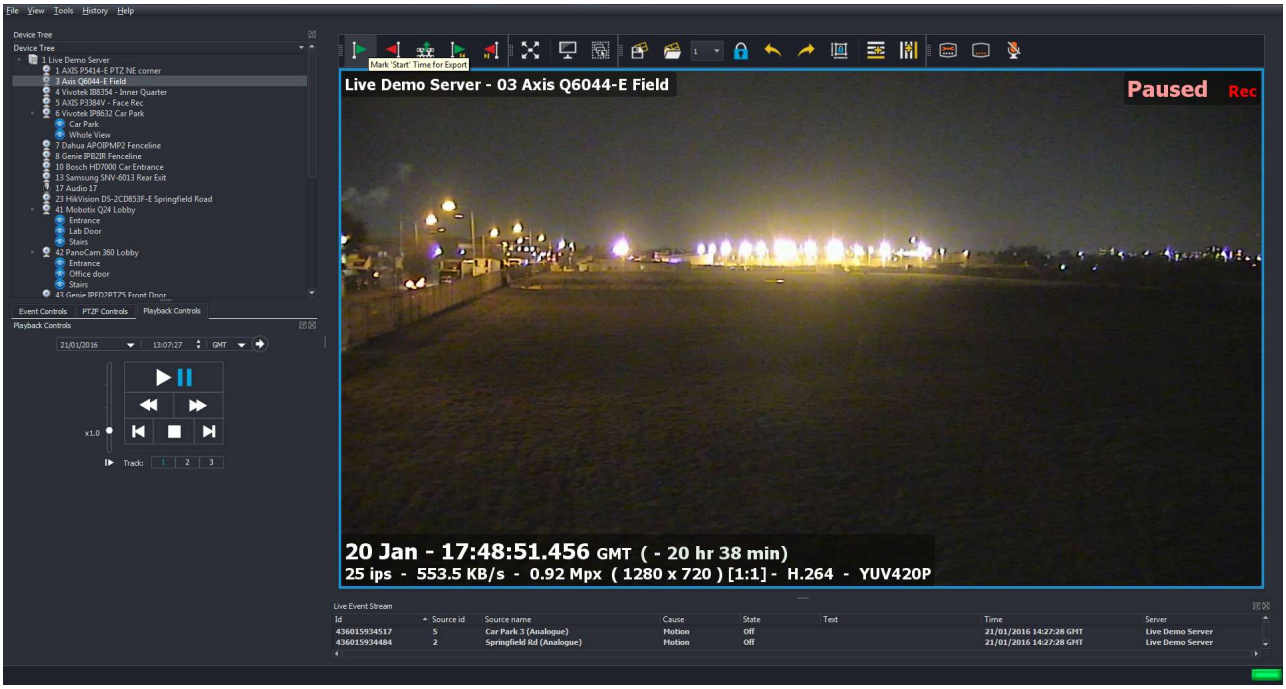


Figure 3.49: Quick Export – Mark 'Start Time' for export

If you move the mouse pointer over the lower edge of an individual camera view, you can see that a green arrow is now shown on the time slider, showing the Start Time for the export.

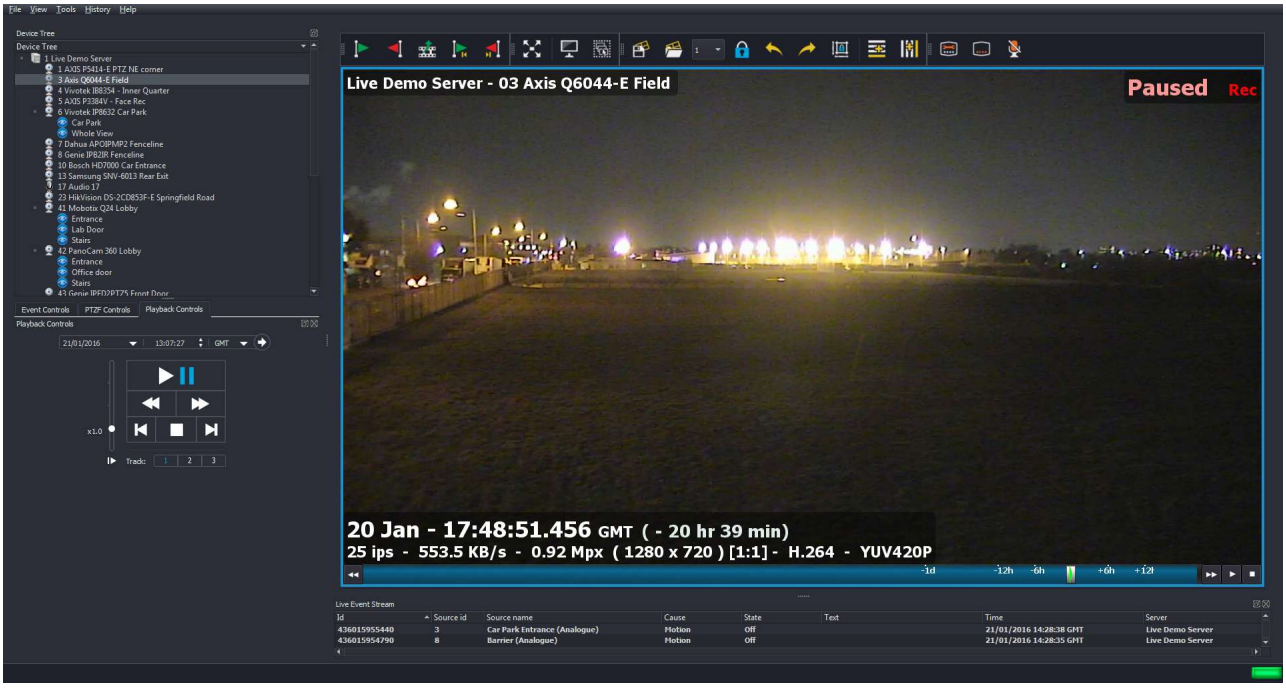


Figure 3.50: Quick Export – Green 'Start Time' marker on time slider

You can now resume playback of the footage until the desired end point of the Export is reached. Click on the Red Flag on the Video Display Toolbar.

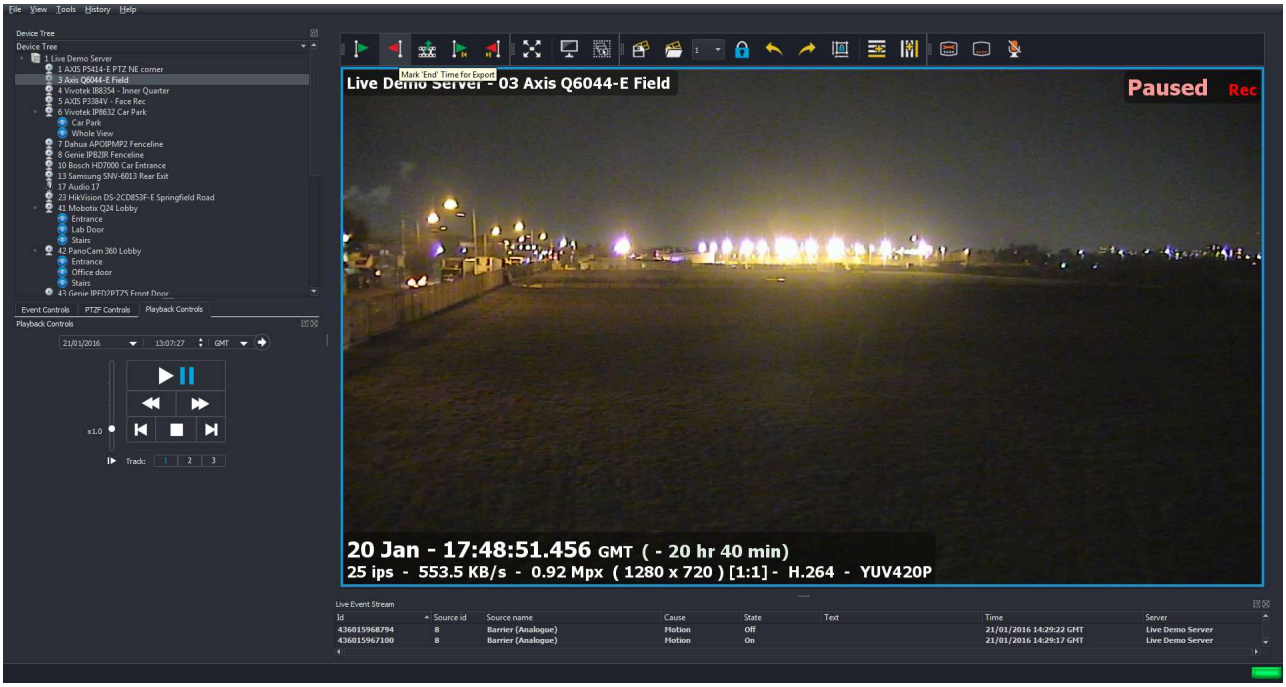


Figure 3.51: Quick Export – Mark 'End Time' for export

If you move the mouse pointer over the lower edge of an individual camera view, you can see that a red arrow is now shown on the time slider, showing the End Time for the export.

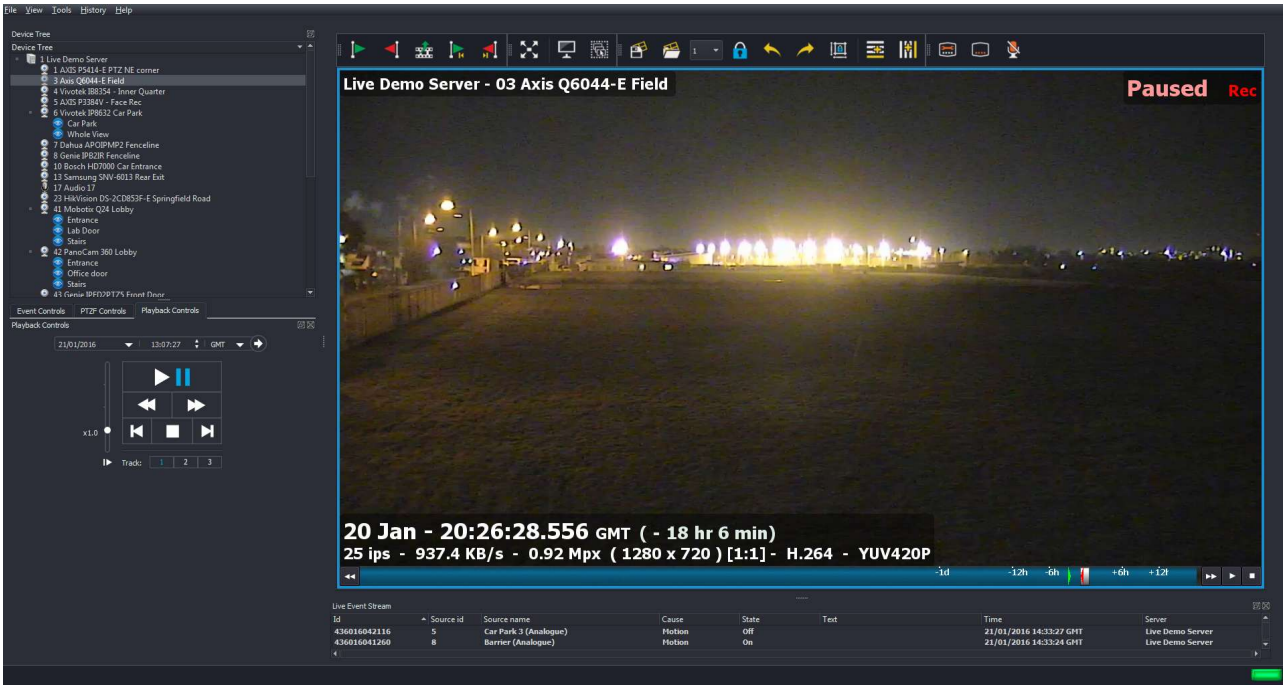


Figure 3.52: Quick Export – Red 'End Time' marker on time slider

Click on the Export button on the Video Toolbar (filmstrip icon) to call up the Export Window:

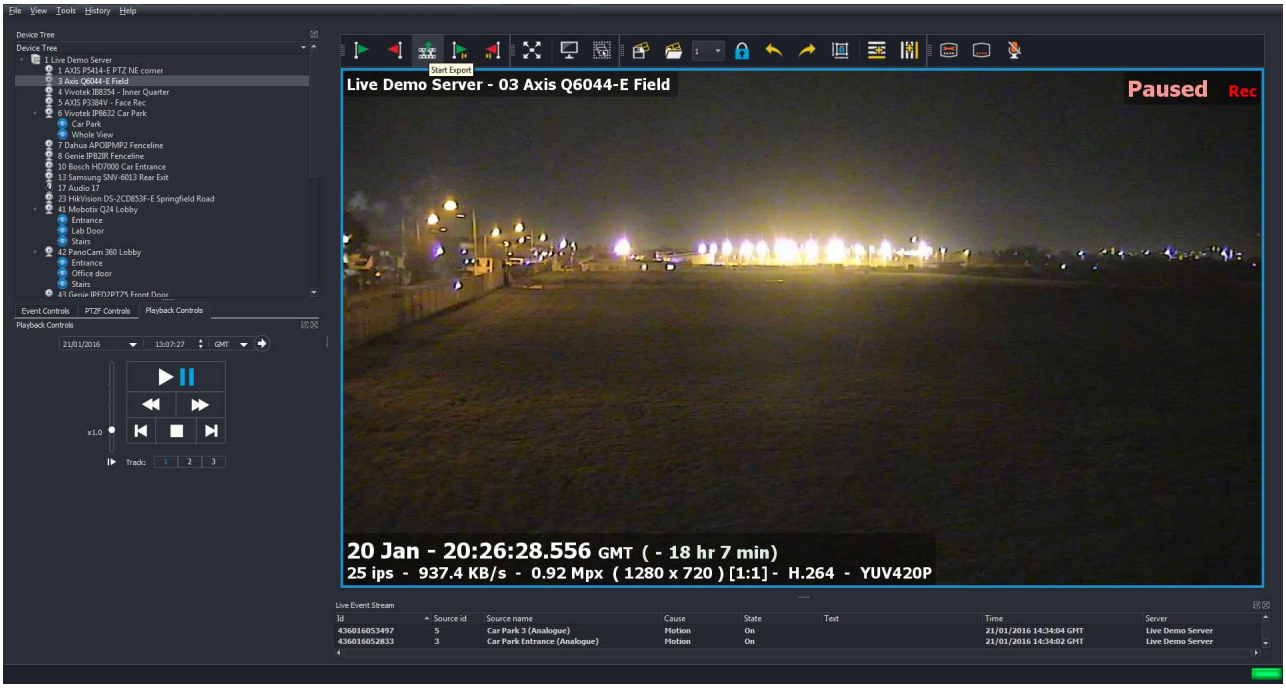


Figure 3.53: Quick Export – Export button

The Export Window will now appear:

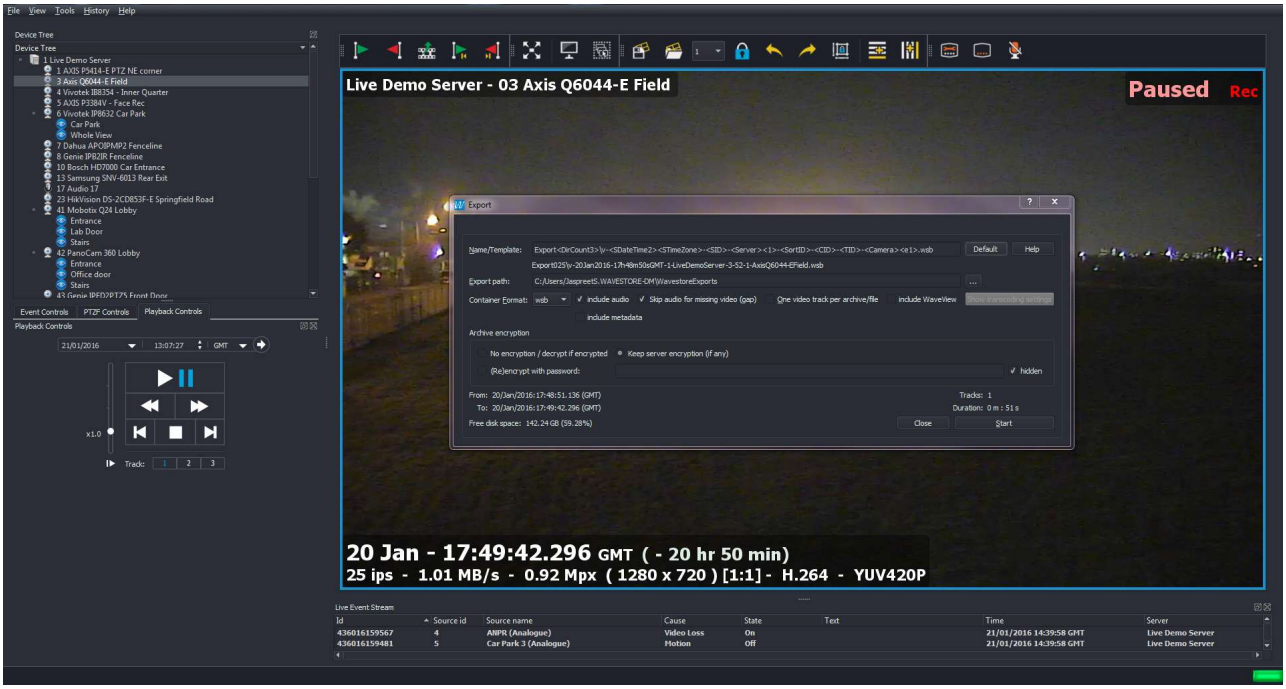


Figure 3.54: Quick Export – Export menu

Browse to your desired Export Path by clicking on the '...' button, and then select your desired Container Format (full details of the export procedure are described in section 4.9 – Exports). The Wavestore WSB format will be selected by default.

Finally click Start; the progress bar will fill during the export, with an acknowledgement message displayed once the export is completed.

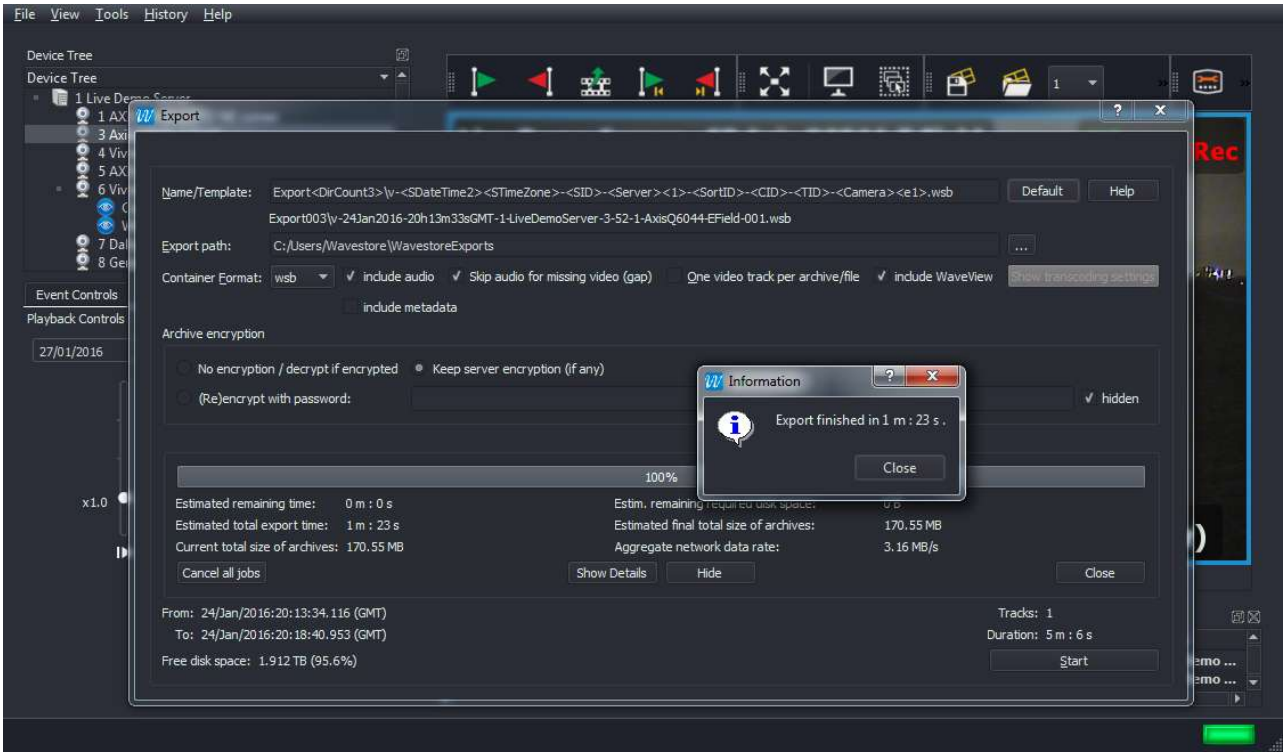


Figure 3.55: Quick Export – Export completion message

Once you have completed the export, you will be prompted to add a copy of the WaveView software to the export folder. This software can be used to playback the export file from the media. It is not necessary to first install the software onto the PC being used to play the export file.

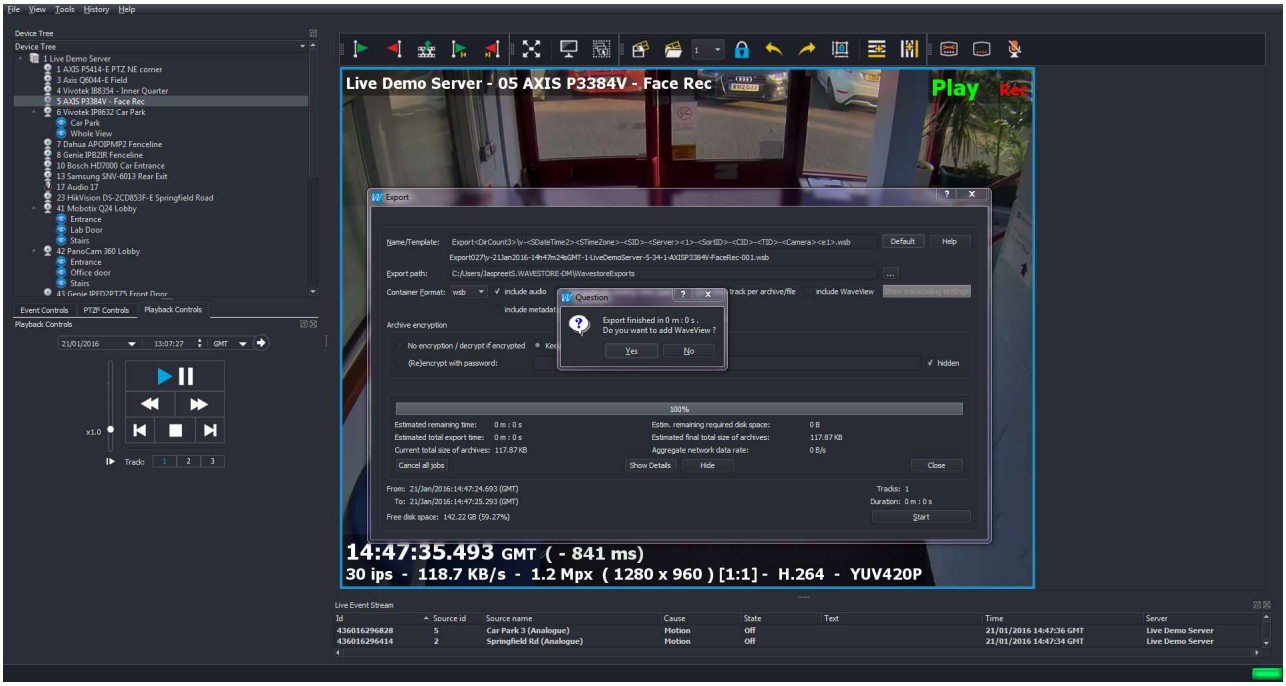


Figure 3.56: Quick Export – prompt to add WaveView

To add a copy of the WaveView software, click on 'Yes' You will now be prompted to confirm the folder where WaveView will be saved.

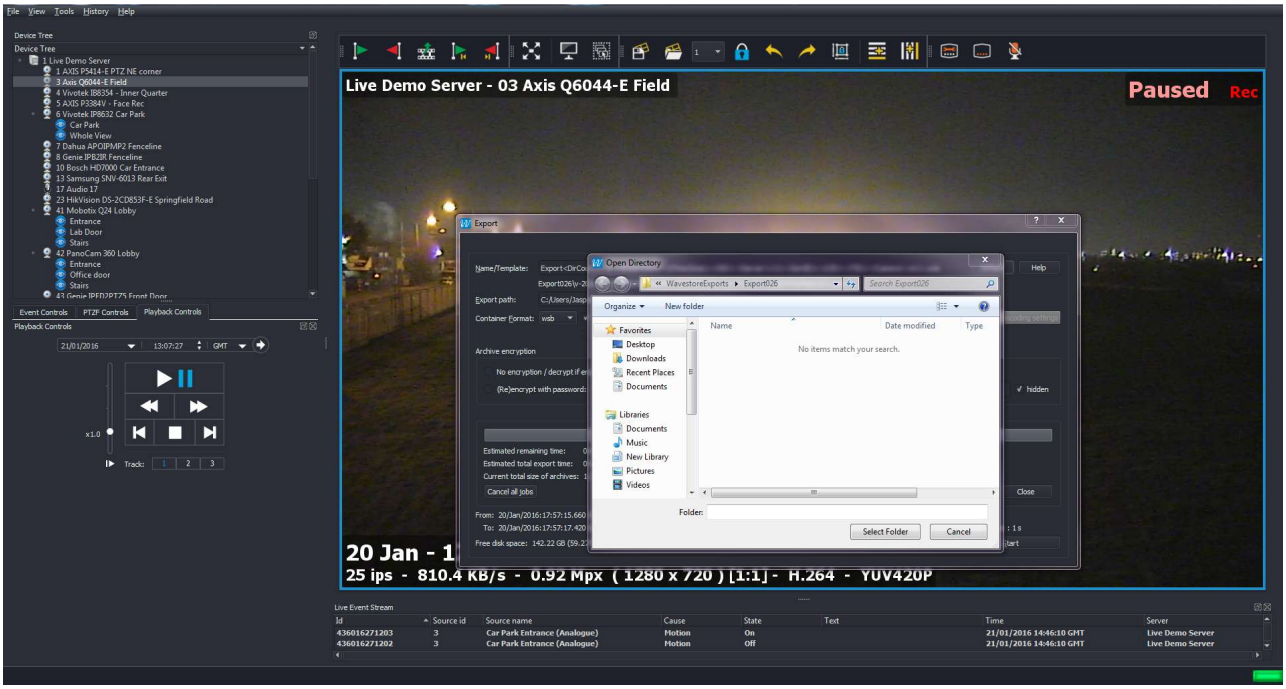


Figure 3.57: Quick Export – selecting destination folder for WaveView

Browse to your desired folder, and then click 'Select Folder'. A progress bar will now fill from left to right and a confirmation message will appear once complete.

3.16.2 Creating a Quick Export tracking a Person/Object in a Dewarped Camera View

If the Video Display that you are working with is a dewarped view from a hemispheric camera, you can pan/tilt/zoom within the Video Display during playback to track a person or object, and create a transcoded export file (e.g. WMV) showing your tracking movements (pan/tilt/zoom).

Once you have reached the desired start time for your export, pause Playback first.

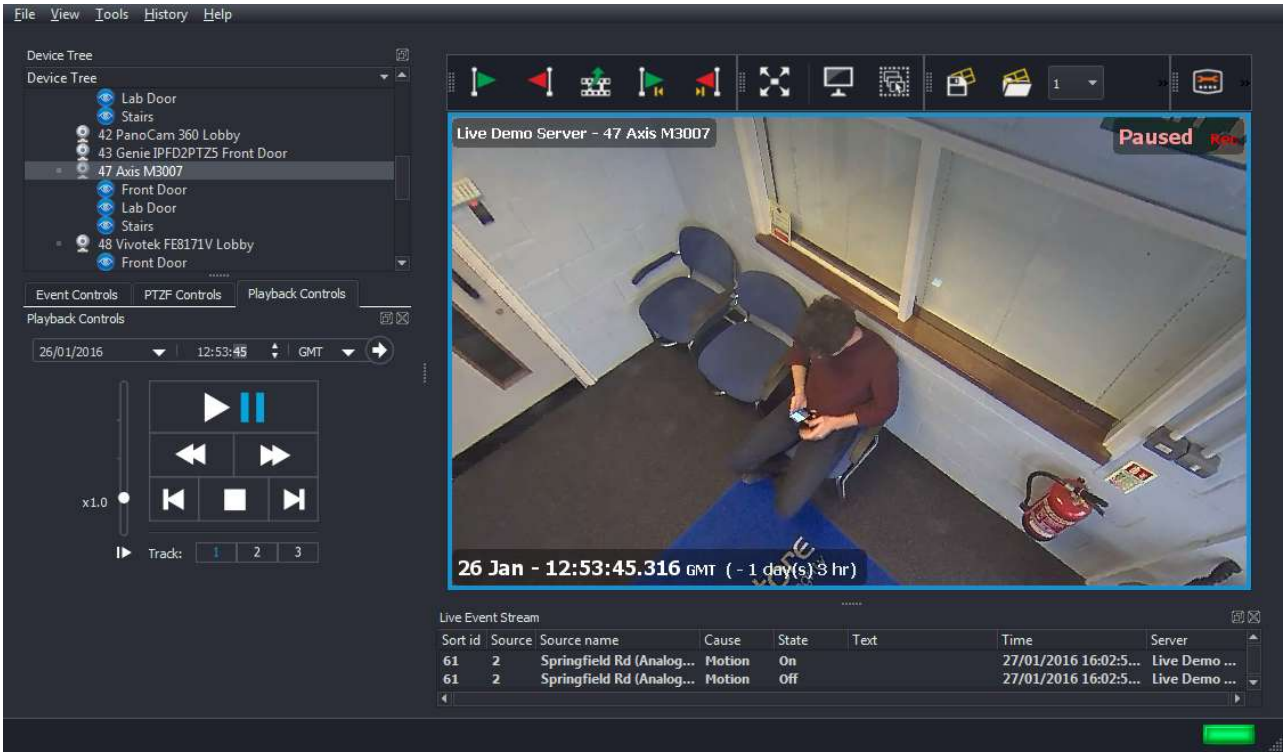


Figure 3.58: Quick Export from dewarped camera view– Playback paused at the start of required footage

Click on the 'Mark Time for Start of Export' button (green flag icon) on the Video Toolbar when you have reached the start point of the footage that you require (use the Pause function if necessary).

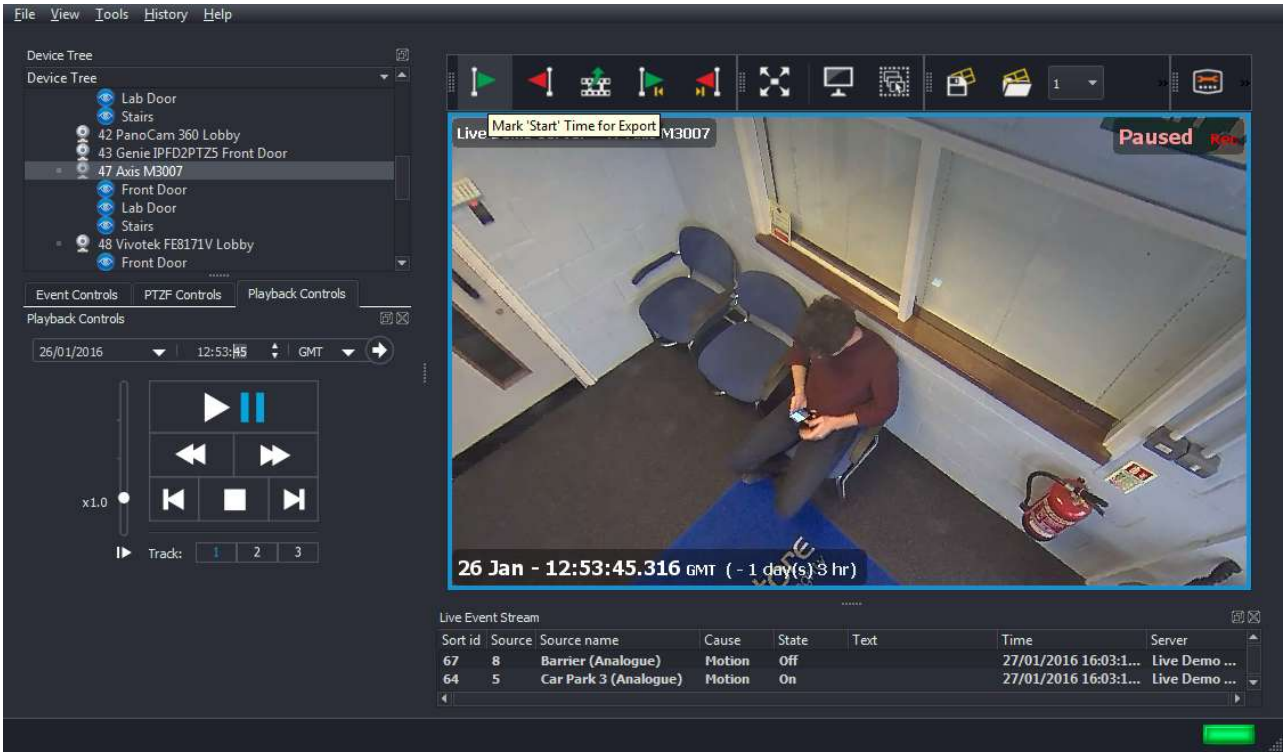


Figure 3.59: Quick Export from dewarped camera view – Mark 'Start Time' for export

If you move the mouse pointer over the lower edge of an individual camera view, you can see that a green arrow is now shown on the time slider, showing the Start Time for the export.

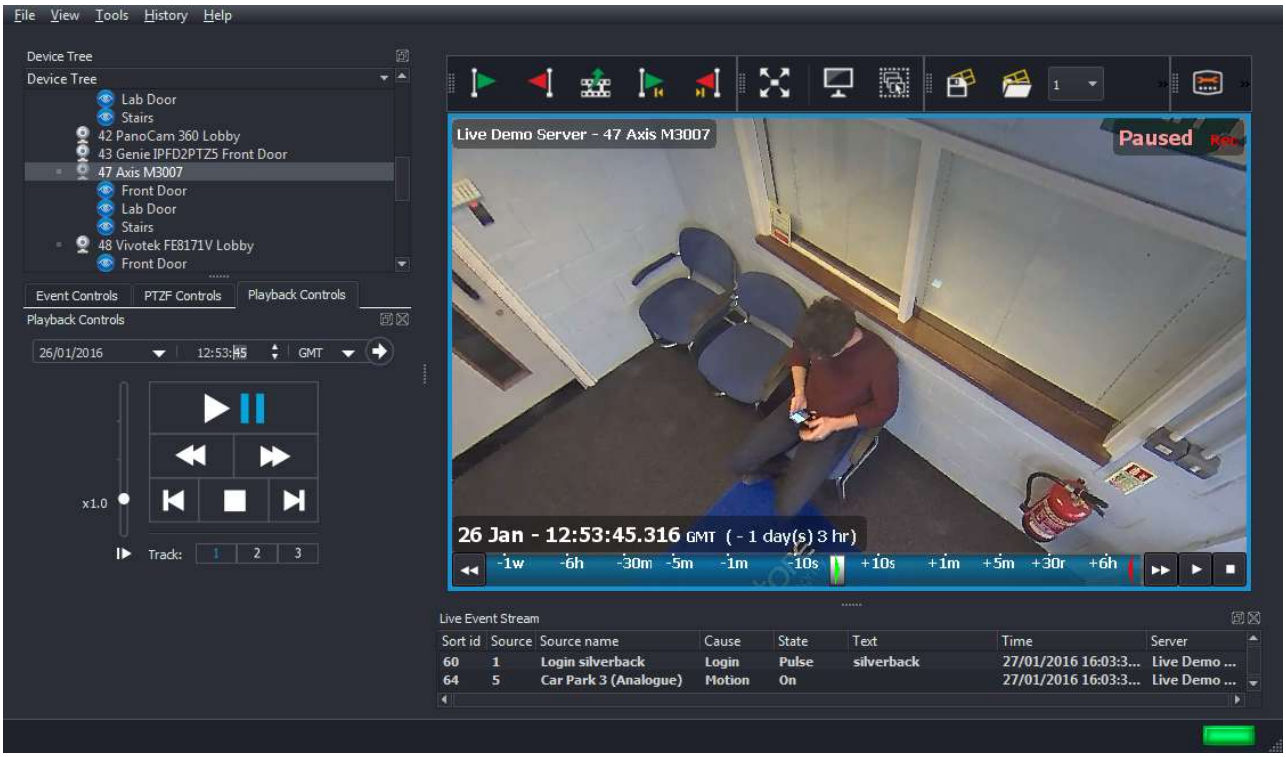


Figure 3.60: Quick Export from dewarped camera view – Green 'From Time' marker on time slider

If you move the mouse pointer over the lower edge of an individual camera view, you can see that a green arrow is now shown on the time slider, showing the Start Time for the export. You can now resume playback of the footage, clicking and dragging using the mouse to track the target person/object:

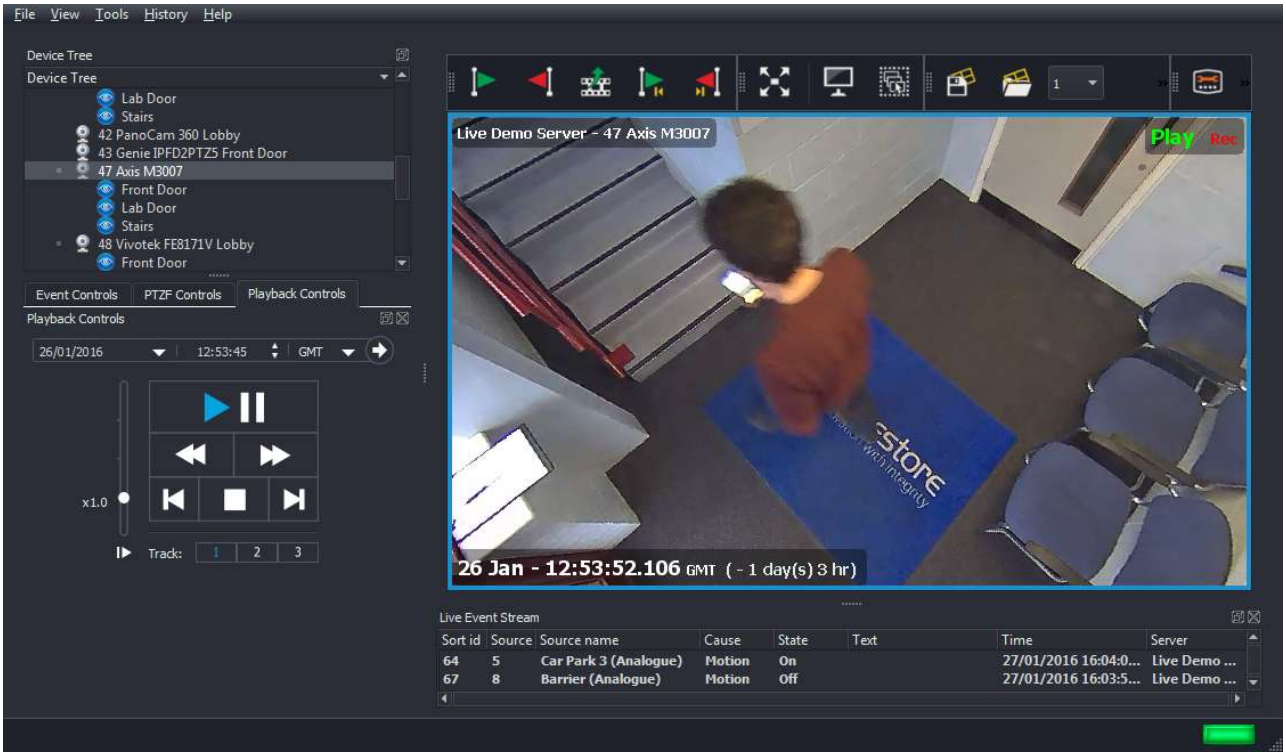


Figure 3.61: Quick Export from dewarped camera view – tracking target person/object

You can use the mouse wheel to zoom in/out on the target during playback:

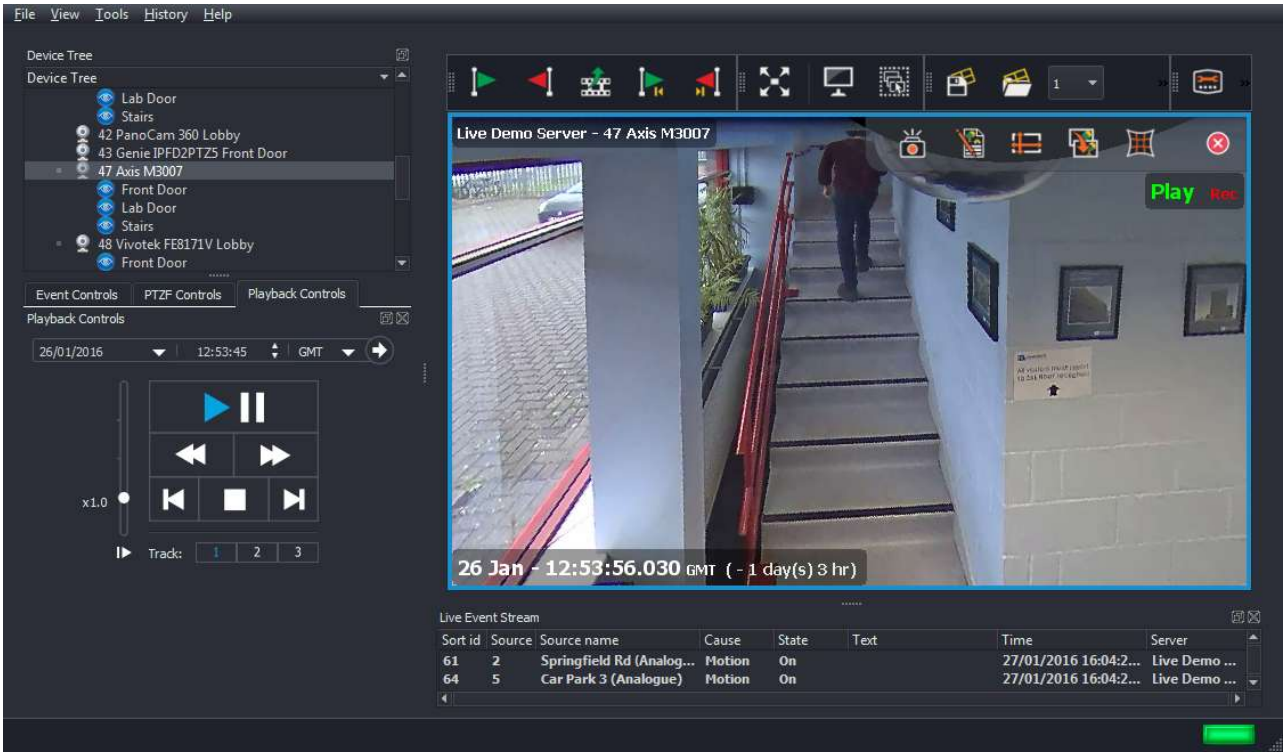


Figure 3.62: Quick Export from dewarped camera view – tracking target person/object

You can now resume playback of the footage until the desired end point of the Export is reached. Click on the Red Flag on the Video Display Toolbar.

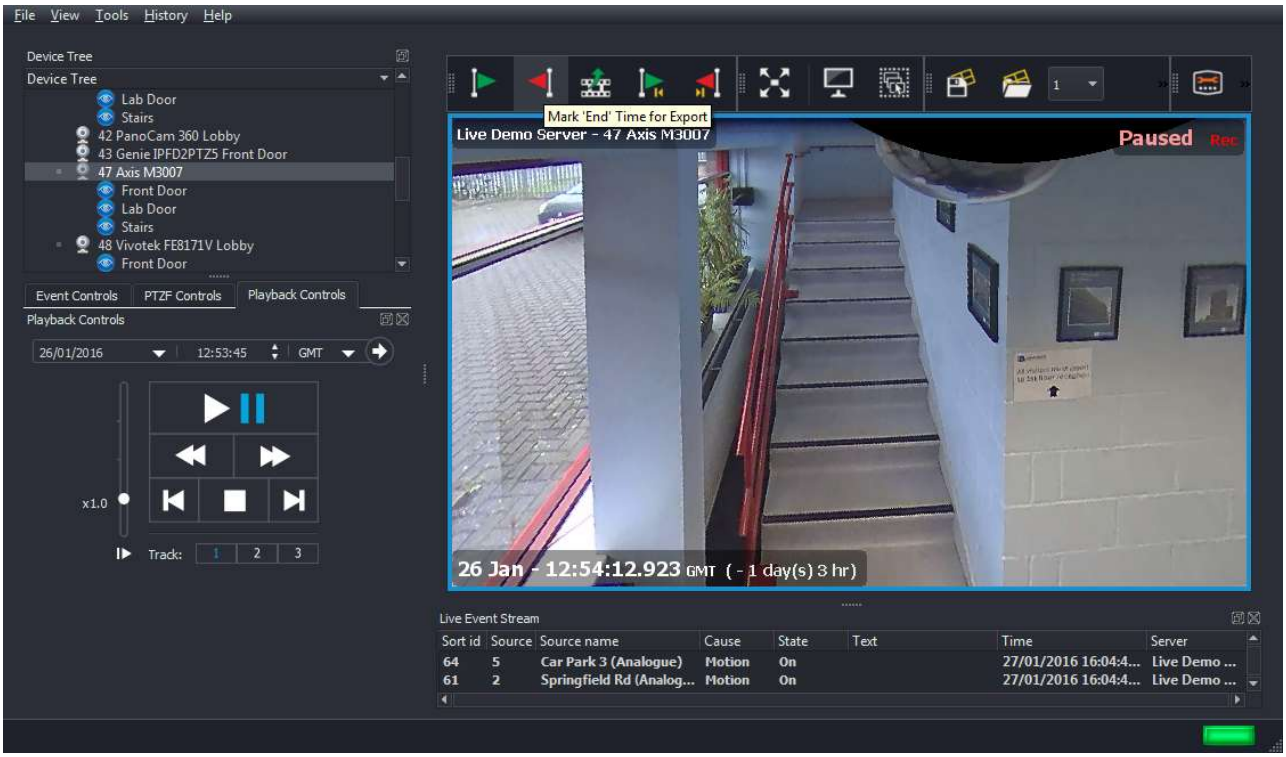


Figure 3.63: Quick Export from dewarped camera view – marking end time of export

If you move the mouse pointer over the lower edge of the camera view, you can see that a red arrow is now shown on the time slider, showing the End Time for the export.

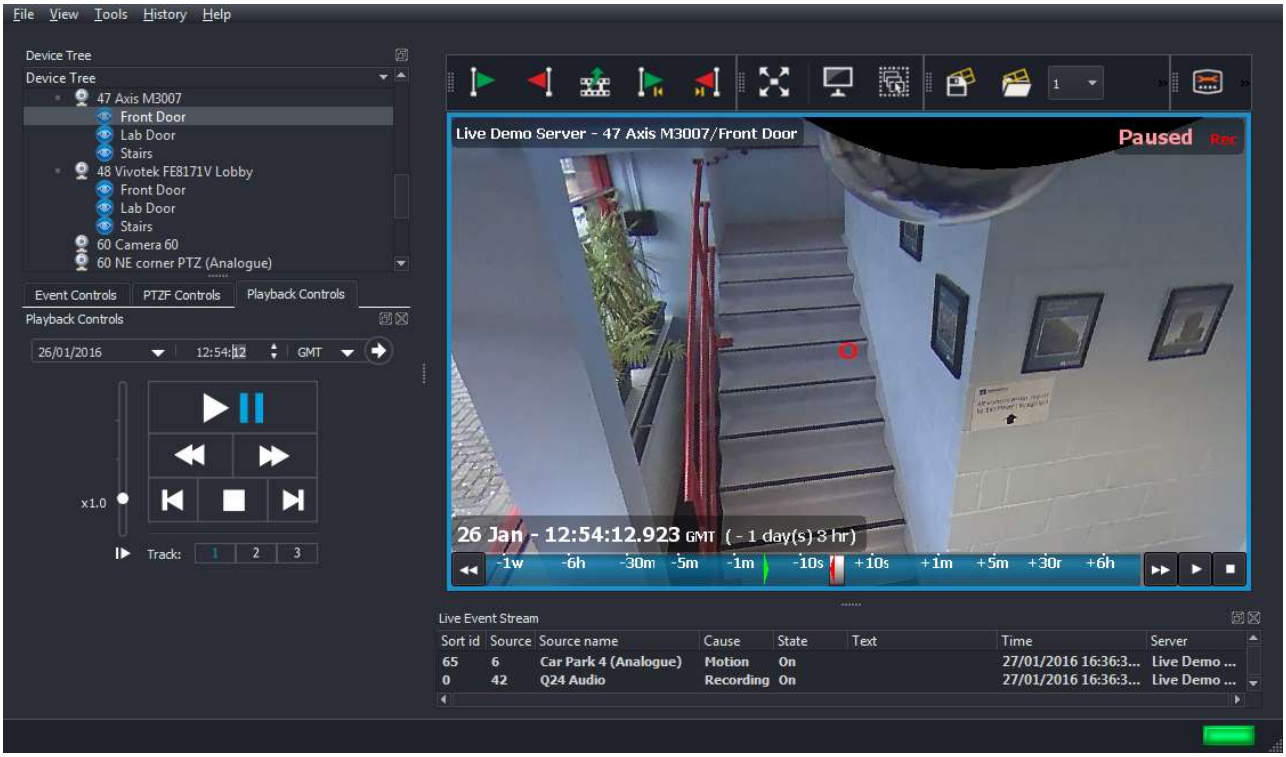


Figure 3.64: Quick Export from dewarped camera view – Red 'End Time' marker on time slider

Click on the Export button on the Video Toolbar (filmstrip icon) to call up the Export menu:

The Export menu will now appear:

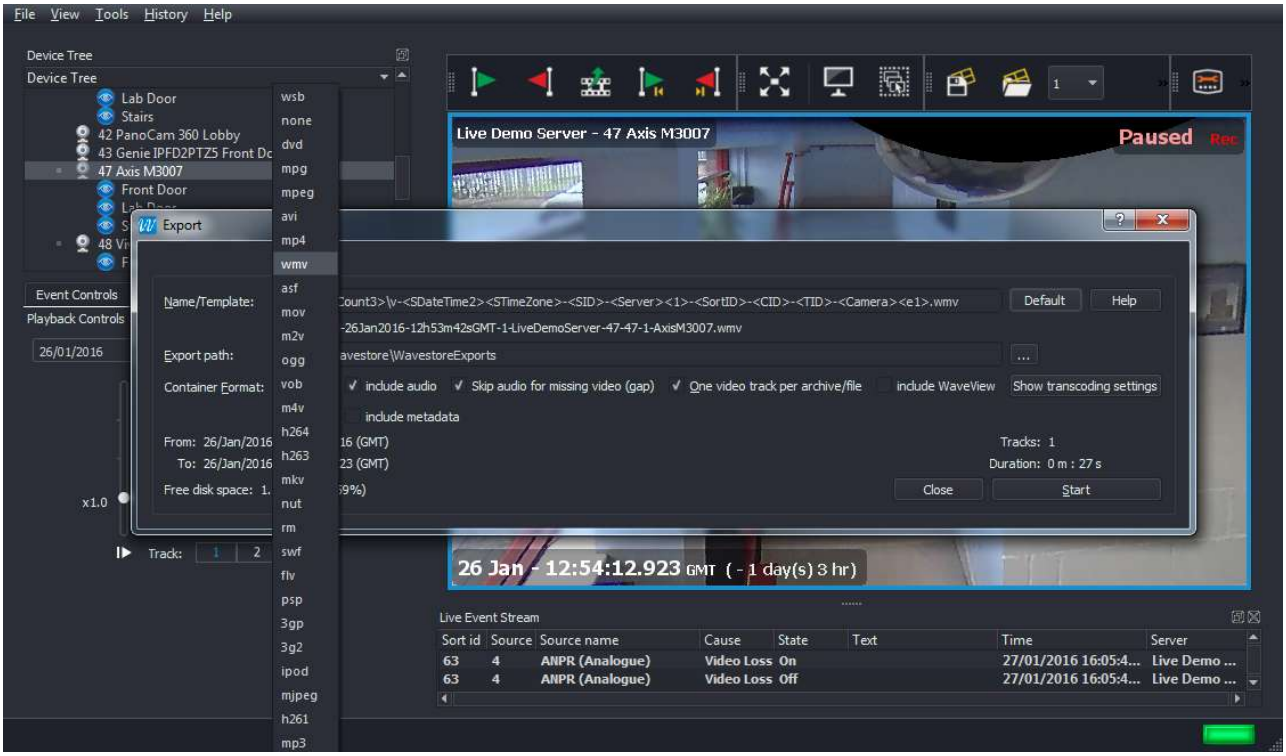


Figure 3.65: Quick Export – Export menu

Browse to your desired Export Path by clicking on the '...' button, and then select your desired Container Format (full details of the export procedure are described in section 4.9 – Exports). The Wavestore WSB format will be selected by default, change this to AVI or WMV.

Finally click Start; the progress bar will fill during the export, with an acknowledgement message displayed once the export is completed.

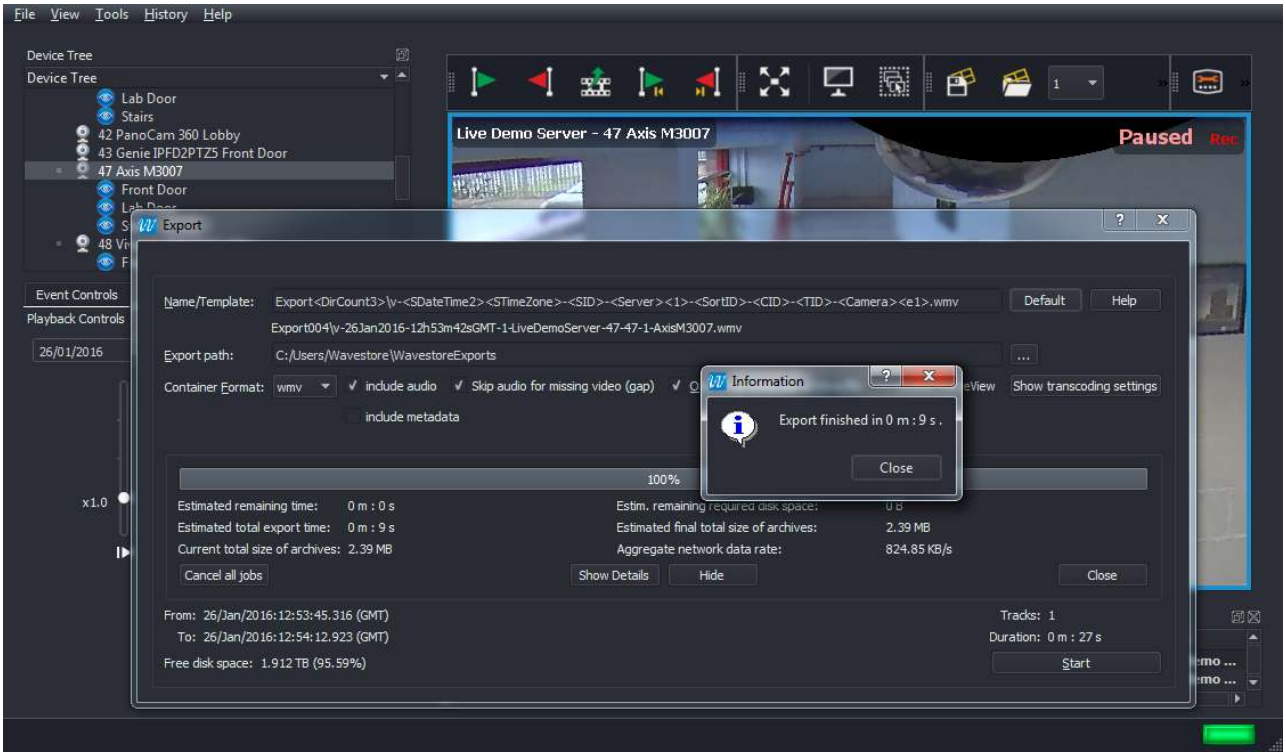


Figure 3.66: Quick Export – Export completion message

Once you have completed the export, you can playback the export using a suitable media player e.g. Windows Media Player/VLC.

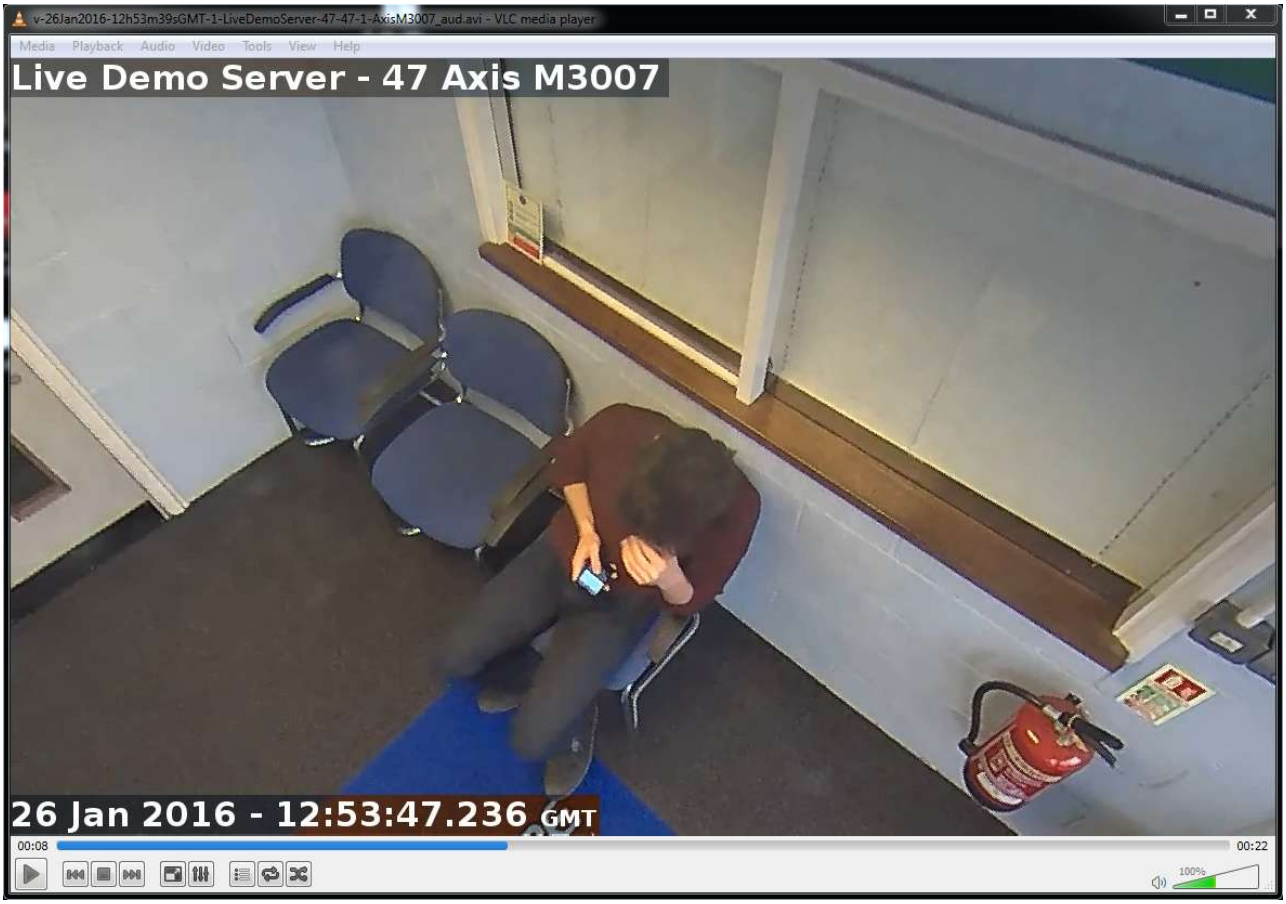


Figure 3.67: Playback of Tracking Export using Windows Media Player

The export file will show the exact tracking movements that you made, whilst viewing the camera before carrying out the export.

Figure 3.68: Playback of Tracking Export using Windows Media Player

This export option is only applicable when using AVI or WMV formats. A WSB export will contain the entire warped image, along with any dewarped views that have been previously saved for that camera.

Figure 3.69: Playback of Tracking Export using Windows Media Player

3.17 Quick Export for Multiple Camera Channels

Once we have identified required footage using the Search function, we can carry out a export from the Live Screen of multiple camera channels as follows: Configure the display so that it contains that camera channels that you require.

Select the cameras that you wish to export by clicking to making their displays active so their frame is highlighted 'Blue' (either by clicking 'Select All' on the video display toolbar, or by holding down CTRL on your keyboard and clicking on the individual displays that you require).

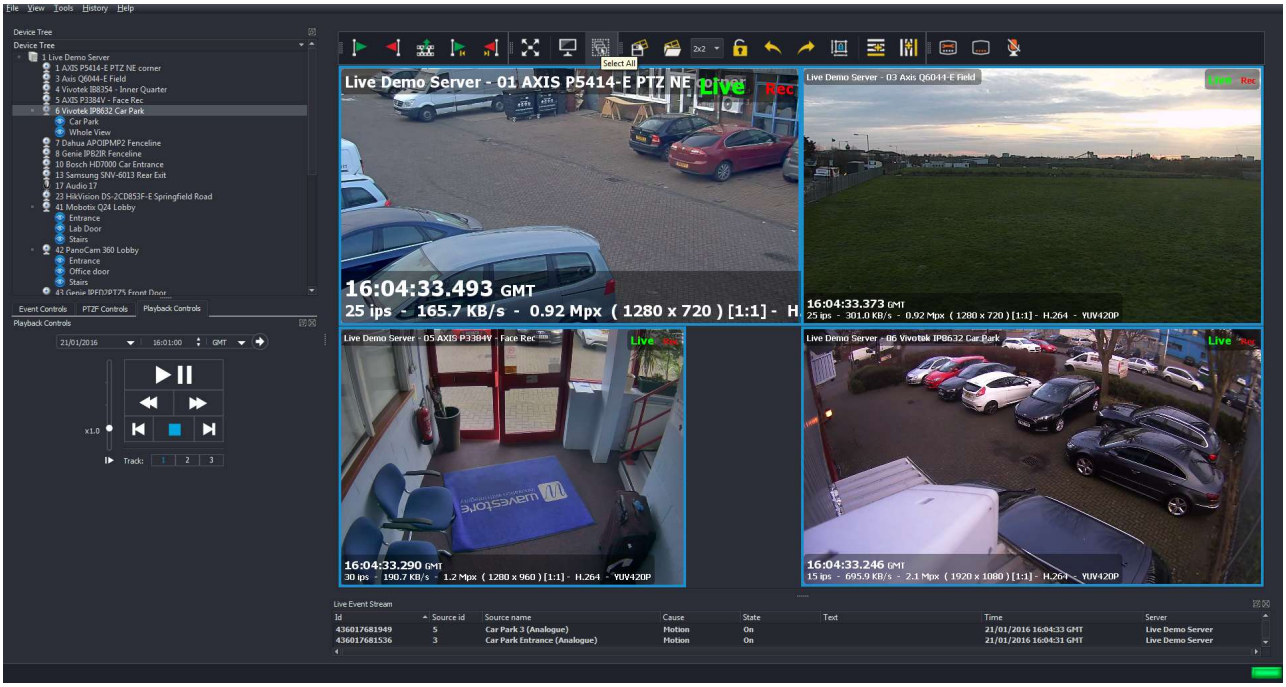


Figure 3.70: Quick Export – 'Select All' option for Video Displays

Right click to call up on the Display Area to call up the Context menu, and left click to select the 'Show Control Toolbar'.

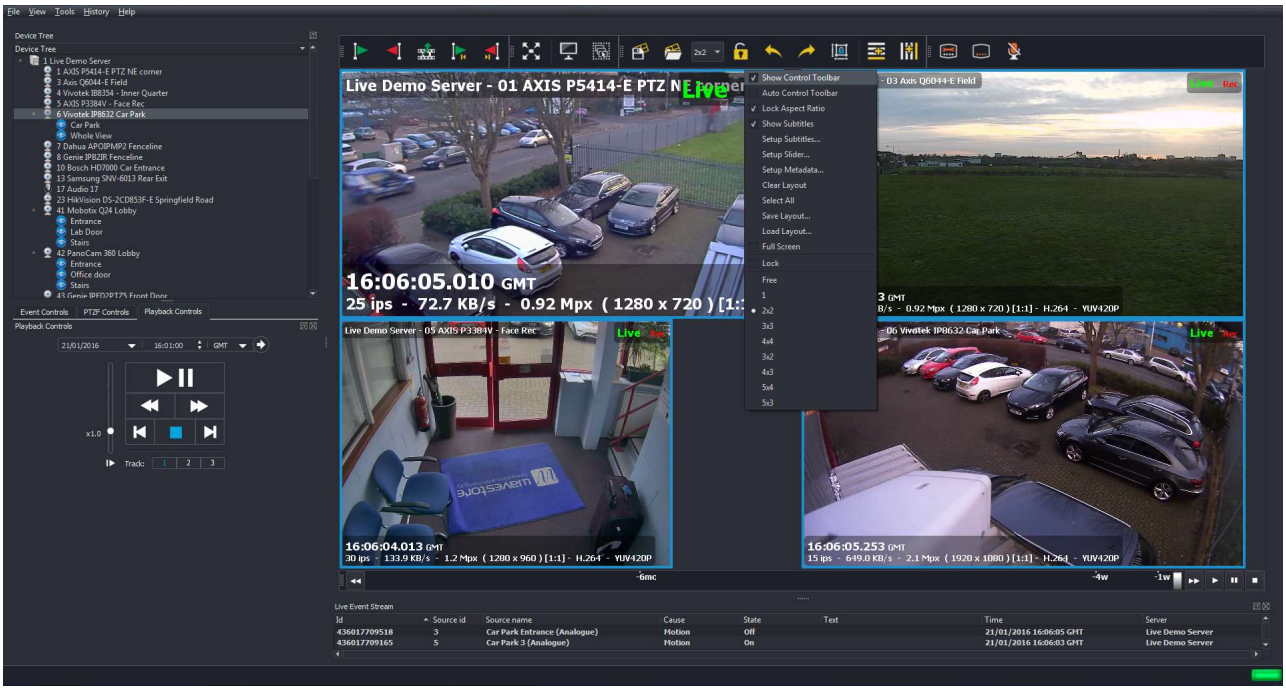


Figure 3.71: Quick Export – 'Show Control Toolbar' enabled on Context Menu

A Control Time Slider Toolbar will now appear at the lower edge of the screen. Use the mouse to control the playback of the video displays using the Control Time Slider Toolbar as described in section 3.15

– Quick Search Controls using Time Slider. You should see that all selected displays are synchronised.

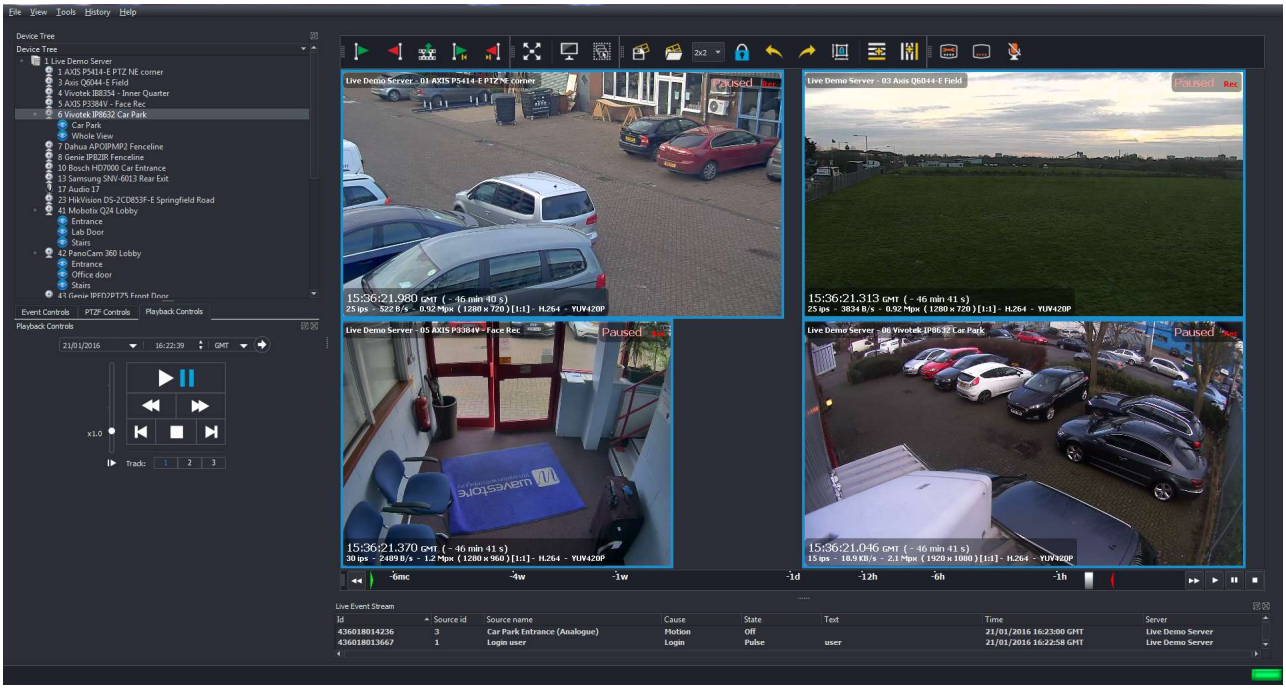


Figure 3.72: Quick Export – Control of Video Displays using Control Time Slider Toolbar

Click on the 'Mark Time for Start of Export' button (green flag icon) on the Video Toolbar when you have reached the start point of the footage that you require (use the Pause function if necessary).

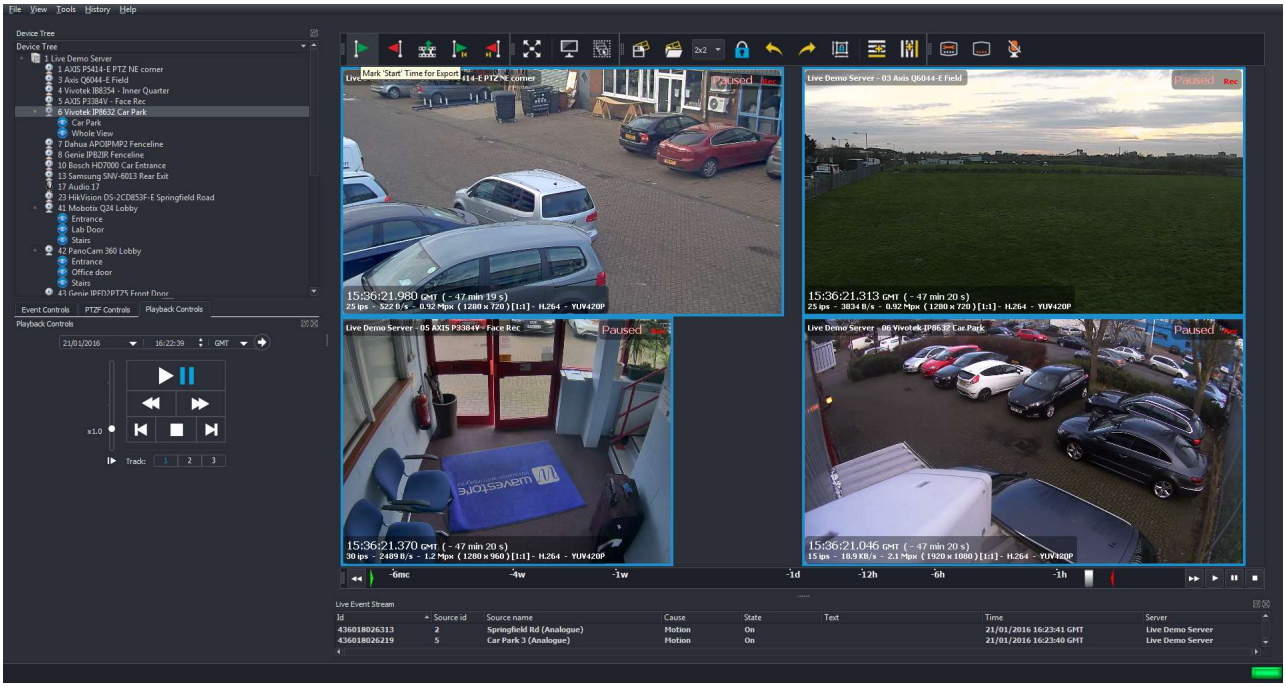


Figure 3.73: Quick Export – Selecting Start Time for Export

Once you have reached the desired end time for your export, click on the 'End Time for Export' button (Red Flag icon on Video Toolbar). You may wish to pause Playback first.

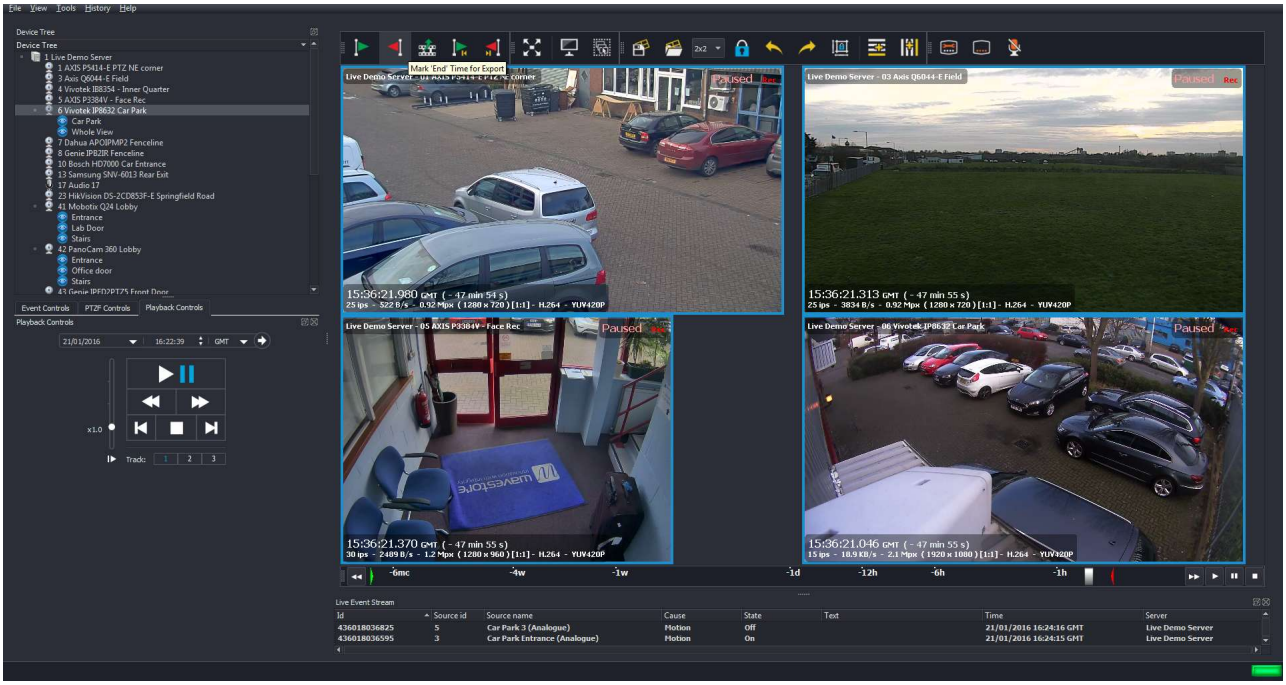


Figure 3.74: Quick Export – Mark 'End Time' for export

Click on the Export Dialog button on the Video Toolbar (filmstrip icon) to call up the Export dialog menu:

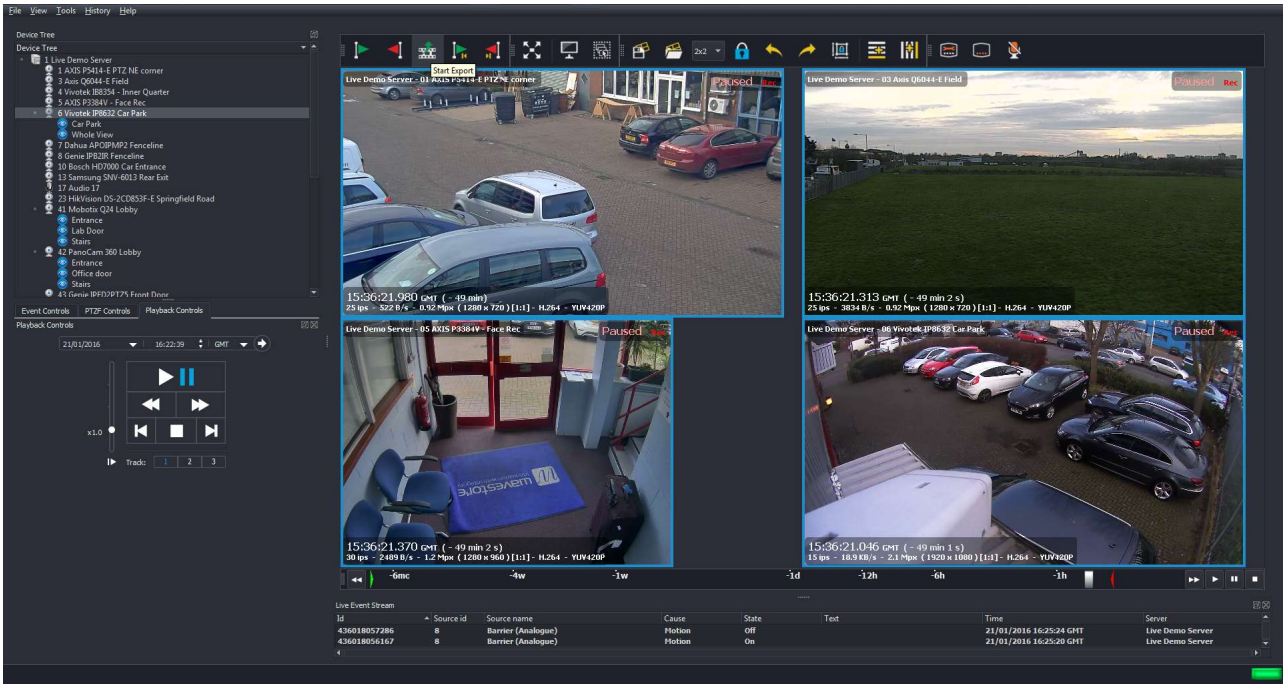


Figure 3.75: Quick Export – Export button

The Export menu will now appear:

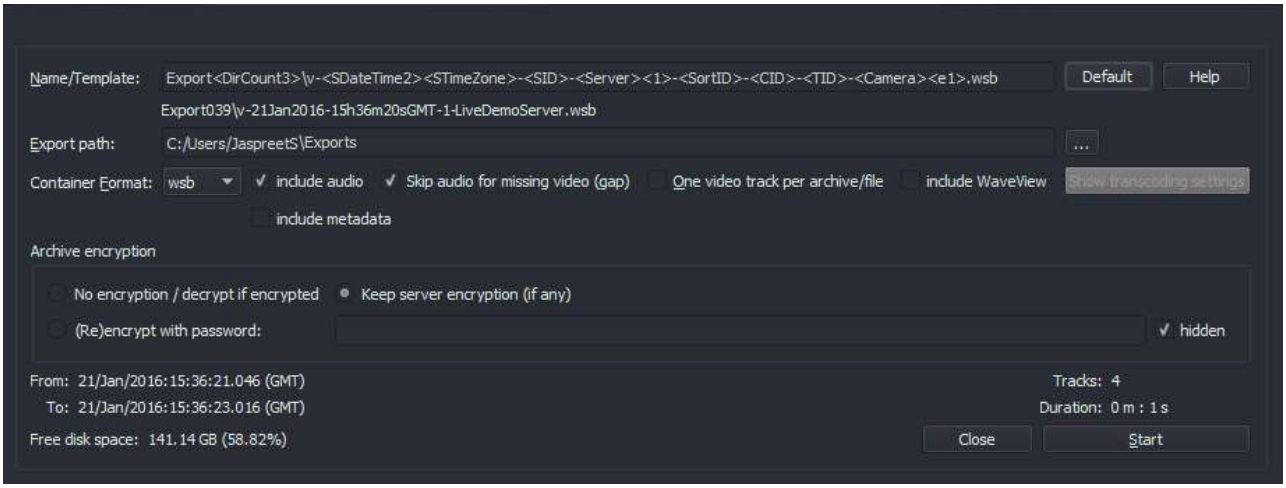


Figure 3.76: Quick Export – Export menu

Browse to your desired Export Path by clicking on the '...' button, and then select your desired Container Format (full details of the export procedure are described in section 4.9 – Exports). The Wavestore WSB format will be selected by default.

Finally click Start; the progress bar will fill during the export, with an acknowledgement message displayed once the export is completed.

Once you have completed the export, you will be prompted to add a copy of the WaveView software to the export folder.

This software can be used to playback the export file from the media. It is not necessary to install the software onto the PC that is being used to play the export file.

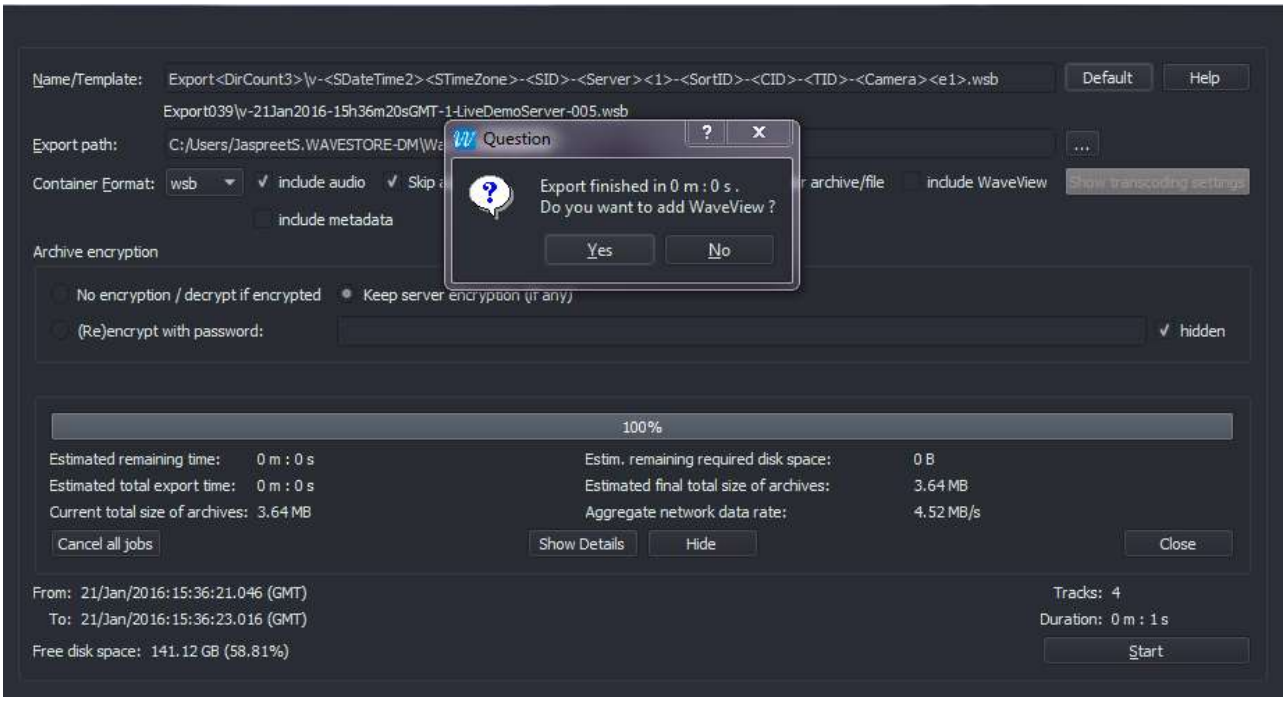


Figure 3.77: Quick Export – prompt to add WaveView

To add a copy of the WaveView software, click on 'Yes' You will now be prompted to confirm the location where WaveView will be saved.

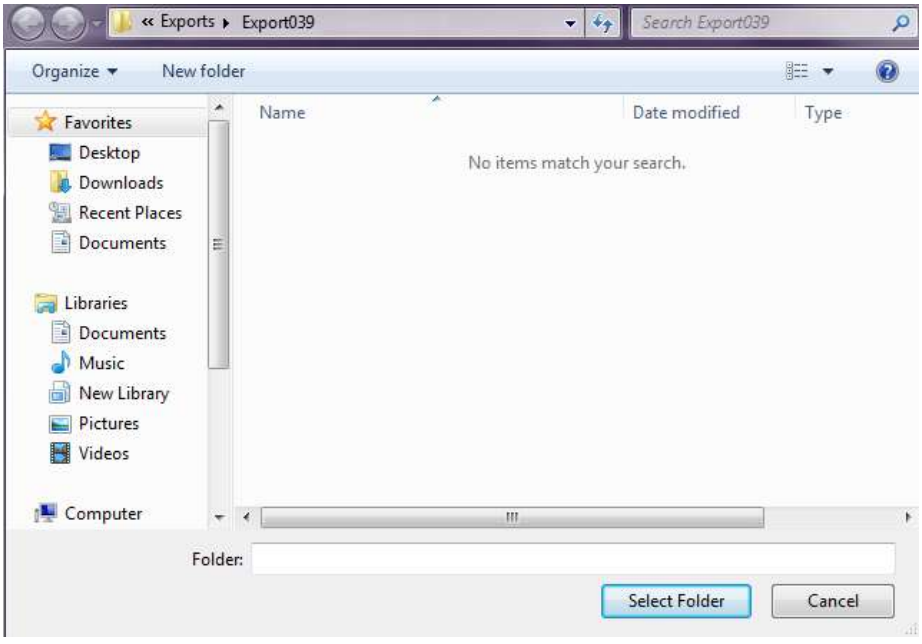


Figure 3.78: Quick Export – selecting destination folder for WaveView

Browse to your desired folder, and then click 'Select Folder'. A progress bar will now fill from left to right and a confirmation message will appear once complete.

Section 5 – Playing Back Exported Files gives details on how to play back .WSB export files using a PC.

3.18 Live Event Stream (Optional Licensed Upgrade)

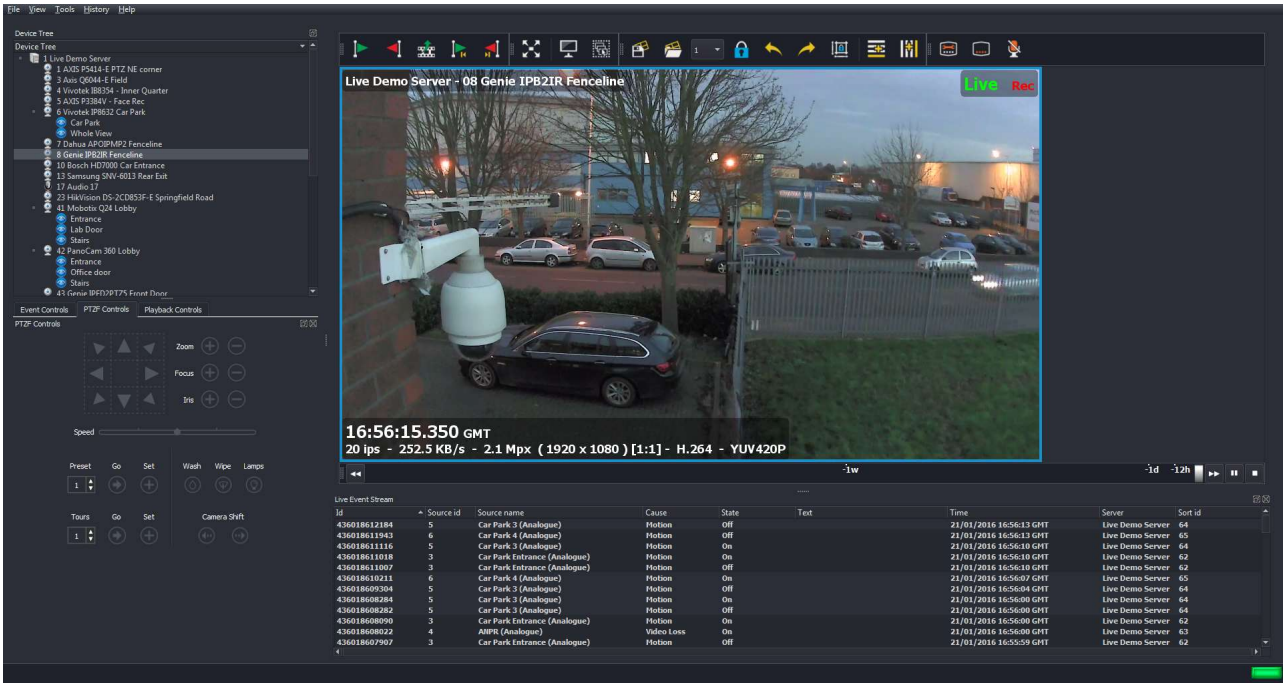


Figure 3.79: WaveView Live View Screen showing Live Event Stream

The Live Event Stream provides a list of incoming events (updated in real time). The Event types that are displayed can be filtered, and their properties (colour of text and/or background, sound notification) can be edited; section 3.22 – Preferences gives full details on how to configure.

It should be noted that the events are not saved locally (on the PC running WaveView); they are stored on the Wavestore server itself.

The Live Event Stream panel can be minimized and maximized by clicking the ↓ arrow icon. When maximized, it shows a table with the following columns:

Time
: Shows the date and time of the event

Id
: Shows a unique ID corresponding to this event

Status
: Can be 'On', 'Off', or 'Pulse'

Text
: Any associated text for this event

Cause
: The cause of the event being triggered, e.g. Motion, Login, Darkening, Video Loss, Input

Source
: An associated parameter for the event; for motion this could be a camera number, for digital inputs this could be the input number

Server

Server that is the source of the event

Right clicking on the column headings in the Live Event Stream displays a menu with toggle options that controls the columns displayed.

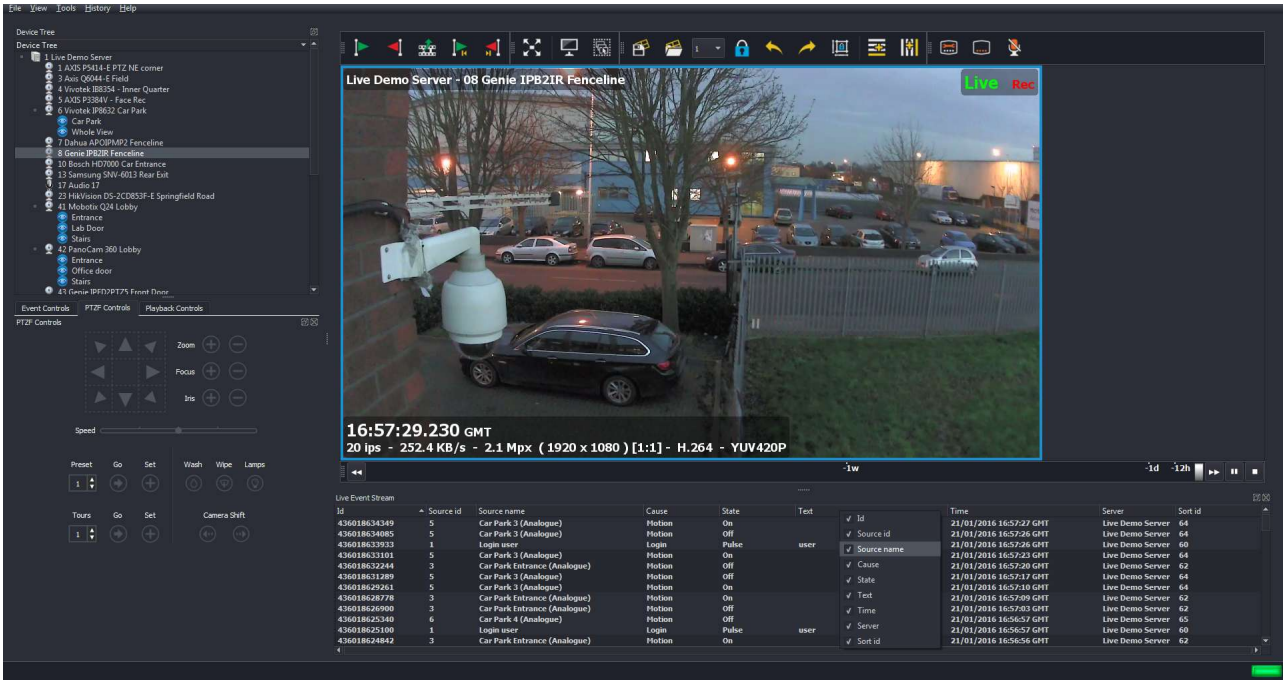


Figure 3.80: WaveView Live View Screen, Column Selection Menu

Clicking and dragging on the column headings allows you to change the order that they are displayed in.

The Events themselves that are displayed can be filtered, and their properties (colour of text and/or background, sound notification) can be edited; section 3.22 – Preferences gives full details on how to configure.

It should be noted that the events are not saved locally (on the PC running WaveView); they are stored on the Wavestore server itself.

We can playback or export associated with an event by right clicking on an event in the list, and then selecting the desired option from the menu that appears as below:

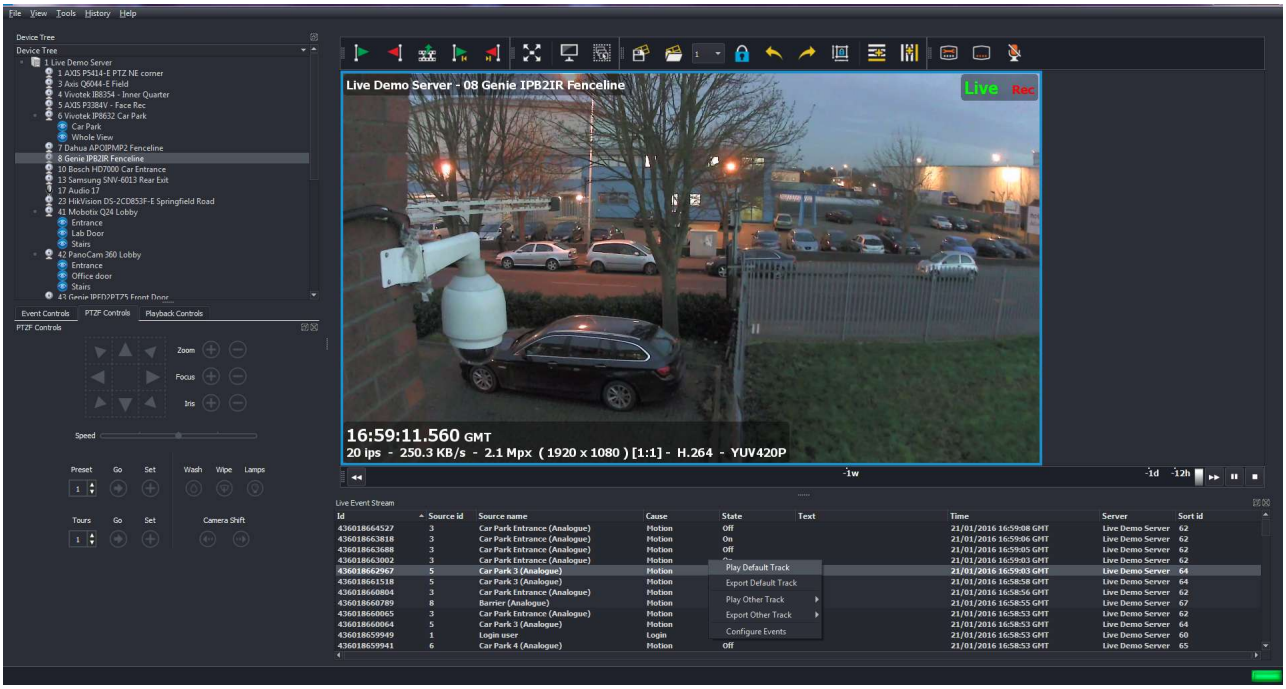


Figure 3.81: WaveView Live View Screen, Column Selection Menu

Selecting 'Play Video Clip' will close any Video Displays currently shown, and open a new single Video Display playing footage associated with the event you have chosen.

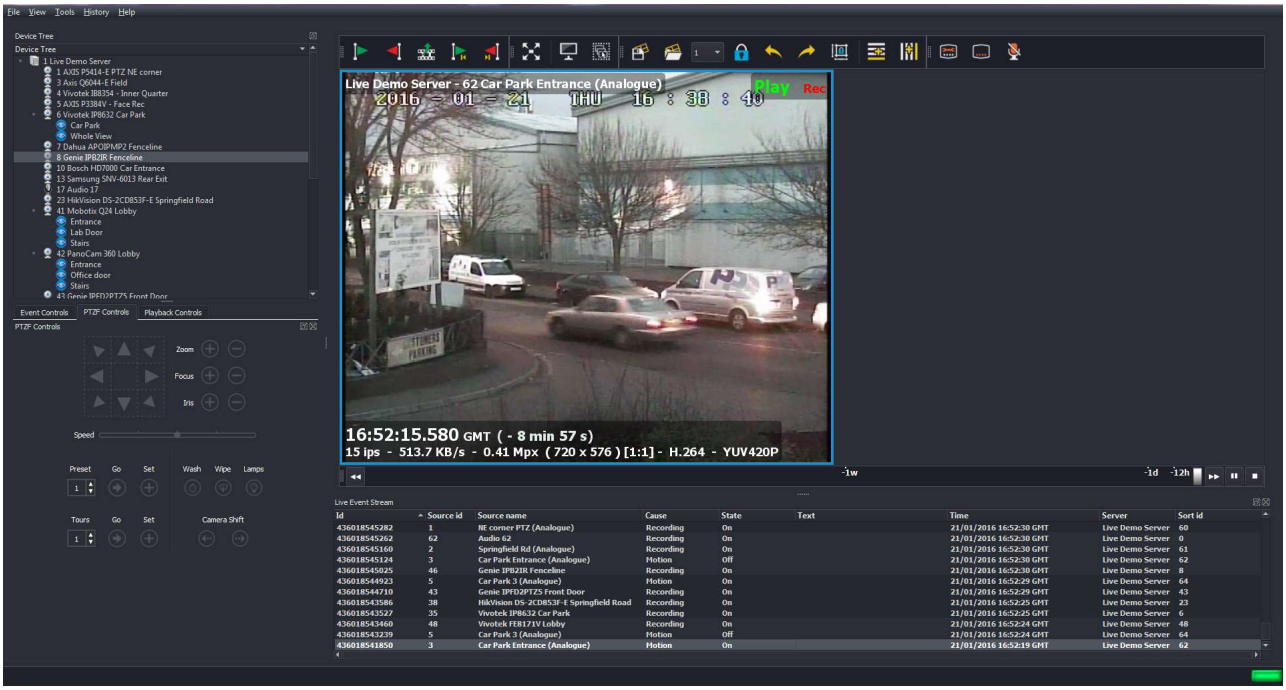


Figure 3.82: WaveViewLive View Screen, Playing Back Video Clip from Event List

If you select the 'Export Video Clip' option, the video clip will be saved to: C:\Users \[username] \Wave–storeExports \EventClips Events on the list can be acknowledged by clicking them. These Events will

no longer show up in the summary when the Live Event Stream panel is minimized.

When minimized, a summary is displayed which shows:

- The number of unviewed events
- The date and time of the last event
- The type (cause) of the last event

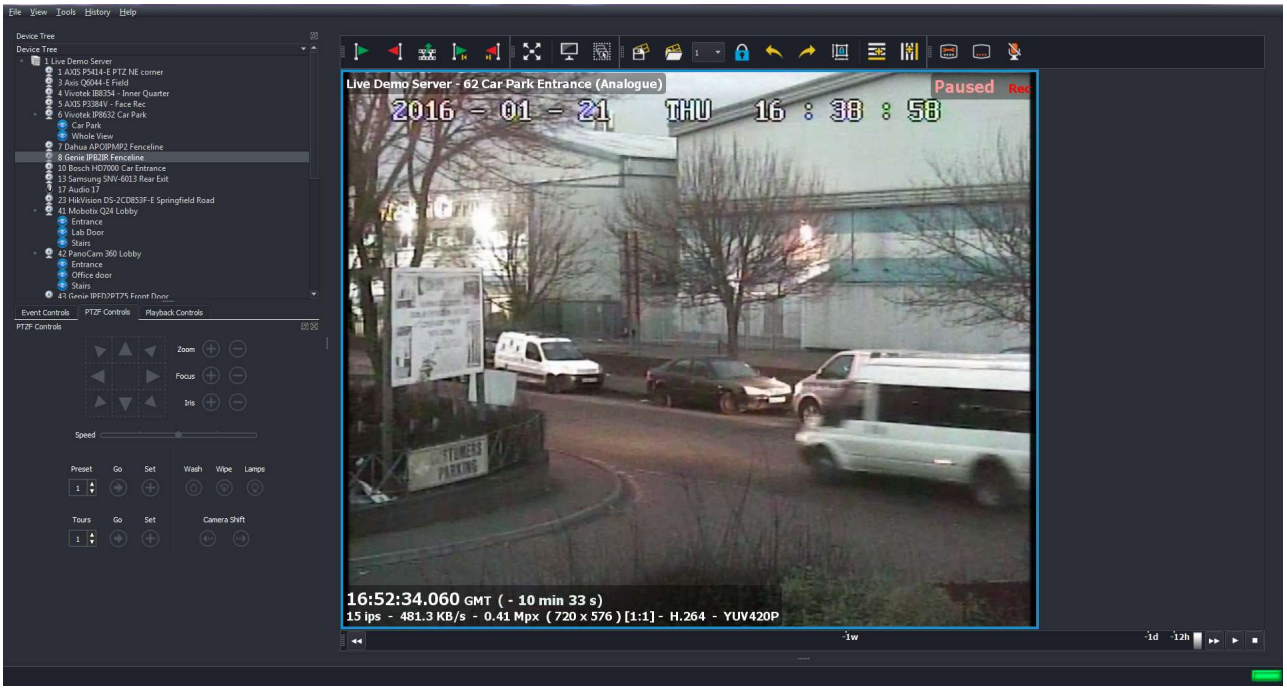


Figure 3.83: WaveViewLive View Screen, Event List minimised

We can also search for Individual Events by following the Individual Events by following the menu path View → Find → Search → Events

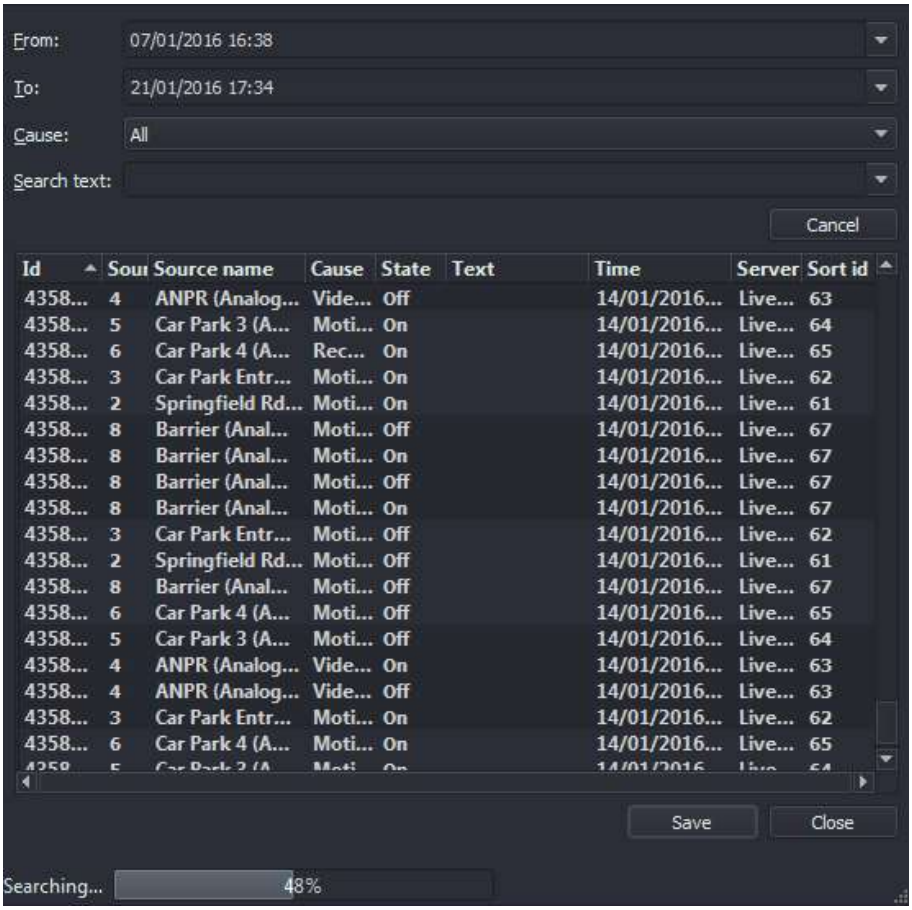


Figure 3.84: Event Search Dialog screen

3.19 Maps

WaveView provides map functionality to allow cameras and alarm devices to be visualised on one or more interlinked images. The Maps are configured if the Map Setup screen and viewed via the "View → Map" menu.

If no map data exists, the Map Viewer will display an explanatory message. It is not possible to create map content from within the map display window.

In the Map Viewer there are fewer controls and slightly different mouse interactions to the Map Setup screen. Essentially, controls relating to editing the map are not present.

The controls that are present are:

Current Area Dropdown

This dropdown list shows the current area and allows the selection of other areas.

Toggle Rubber Band

When enabled, left-clicking the mouse and dragging draws a rectangular area. When the left mouse button is released, any cameras within the rectangular area will be shown on the Video Display Area. When disabled, left-clicking the mouse and dragging can be used to pan around the map area when zoomed in.

ToolTips Enabled
: When enabled, hovering over item shows additional information about that item. Hovering over a camera will show a live stream from the camera.

Note that cameras which are open in the Video Display Area are highlighted on the map.

Left Double click on a camera to view that camera in the WaveView Display Area.

Cameras also show their status by changing colour to orange or red depending on the status. Hover over a camera to view details of the status.

3.20 Network Tools

The Network Tools menu (menu path Tools → Network Tools) contains the following items:

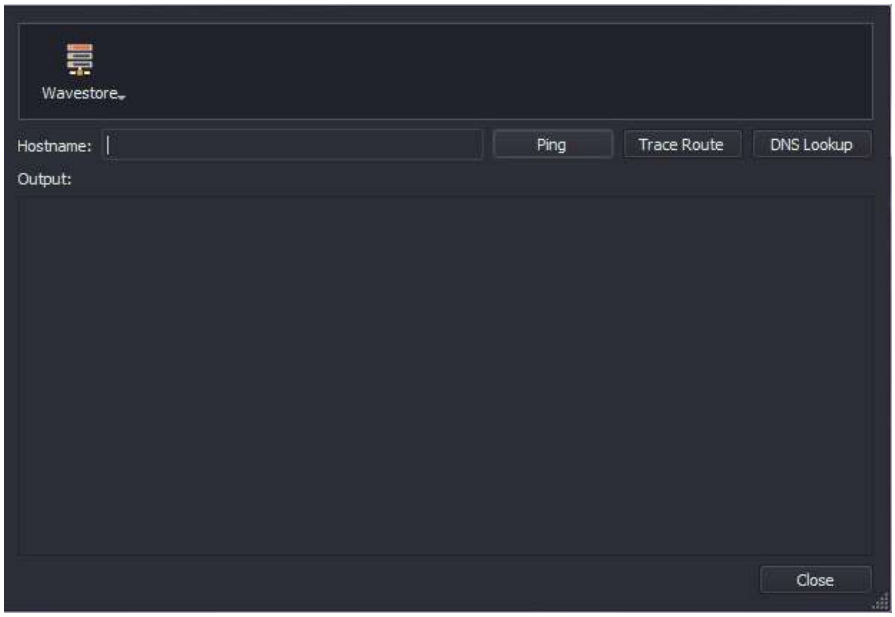


Figure 3.85: Network Tools menu

- Ping
- Trace Route
- DNS Lookup

These commands can be used to test/troubleshoot connectivity to networked devices, such as IP cameras and NTP servers.

Enter the IP address or host name, and then click 'on the function that you wish to use.

Information will be displayed in the Output window below.

3.21 Log Files

The Wavestore has a number of log files. Since it is a client–server architecture, there are separate log files for the server and client. Since most client messages appear on the screen, it's rare you need to look

at the information in the client log. However, most things the server reports have nowhere to go other than the system log, and so this is the principle log of the system.

Historically a lot of information was in the system log, and this has been broken out into a number of alternative log files. There's now a separate log for each disk or disk array, for each camera or capture device, and for a number of other special items. These alternative logs are available in the "Extra Logs" tab of the System Log screen.

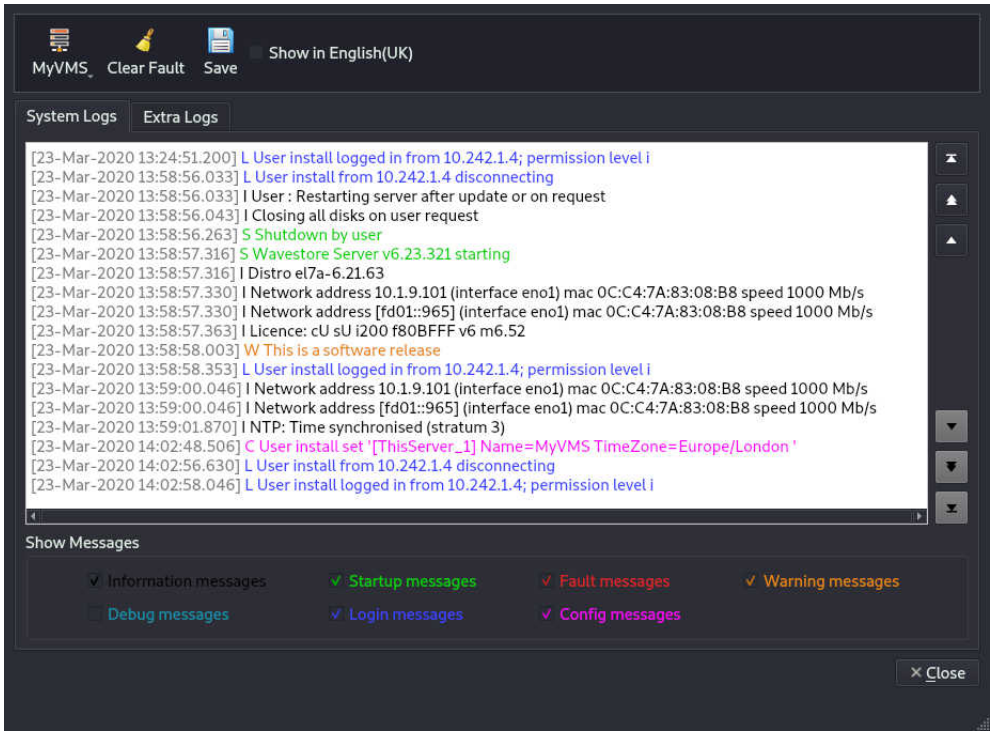
3.21.1 System Log

The server System Log can be accessed by the menu path Tools → System Log, or by clicking on the Server status indicator (see section 3 – Main Screen), and can give valuable diagnostic information regarding the status of the server.

This log file can be saved to a USB device from the server, or to a local drive on a connected client.

In the case of a server group installation, the System Log for any of the Server within the group can be accessed by clicking on the grey server icon (server name is beneath this icon – default setting is 'Wavestore') in the top left corner of the System Log window, and selecting from the drop down menu.

The server name can be changed by following the menu path View → Setup → Server → Name (see section 6.2.1 – General).



System Log Messages are colour coded and start with a letter according to their type:

Information: 'I' Black

Start-up: 'S' Green

Fault: 'F' Red

Warning: 'W' Orange

Login: 'L' Dark Blue

Configuration: 'C' Pink

Debug: 'D' Light Blue

Users can filter certain types of message by checking/unchecking the relevant box.

Messages other than debug messages are intended to be readable by a typical user and will be translated into the selected language.

Debug messages might contain less readable internal states. See also the 'Alternative log' files section below.

The Server Log can be backed up to a USB device/local drive by clicking Save, and browsing to the desired location.

Common system log messages include:

- S Wavestore server starting – shown at startup with the server software version.
- S Shutdown – shows when the system shut down. If it shut down unexpectedly, this message will be produced when it restarts with the correct time of shutdown.
- I IP Address – gives the address of the principle network interface in the system.
- I Licence: – shows the licence loaded with the abbreviated licence flags.
- I NTP: Time synchronised (stratum 4) – shows that time synchronisation has occurred. The stratum shows how many machines are in the chain between this device and the time source.
- I Authentication disabled – this refers to video watermarking authentication not being enabled.
- L User install logged in from – shows who logged in and from which IP address.
- L User install from ... disconnecting – shows when that user disconnects.
- C User install set ... – shows configuation parameters which have been changed, format is the same as the advanced configuration screen.
- C User install reset – shows configuation parameters which have been removed.

3.21.2 Extra Logs

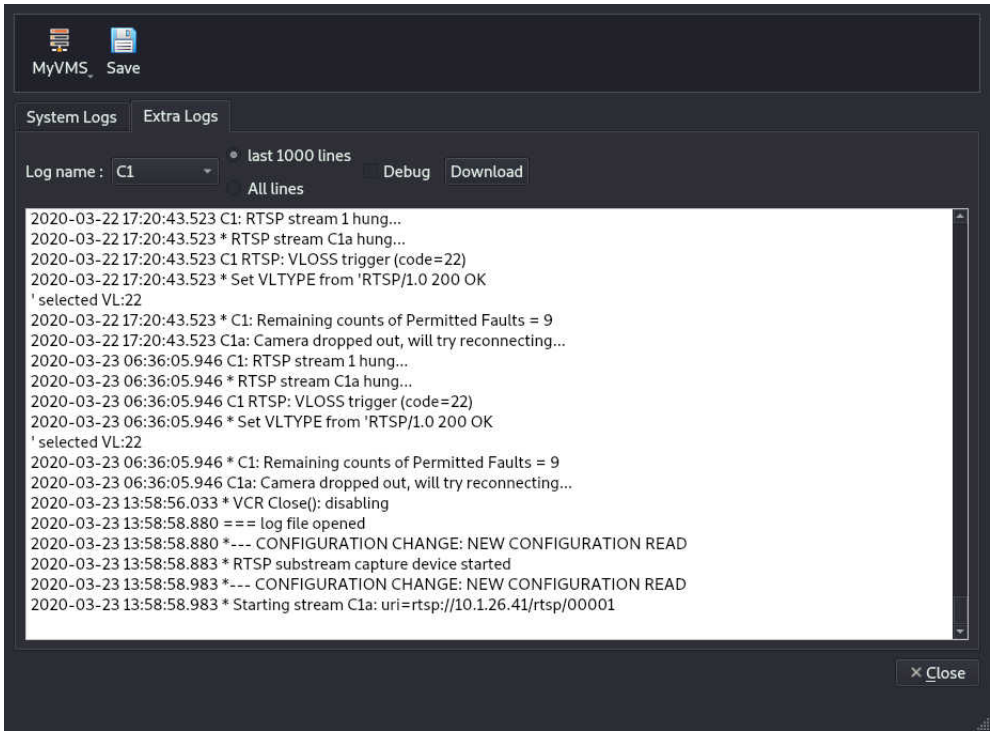
For detailed debugging of problems, there are now separate logs for each disk or disk array, for each camera or capture device, and for a number of other special items. These items used to be in the main system log when 'debug' option was selected, but now have been moved out into their own log files.

These alternative logs are accessed using the "Extra Logs" tab of the System Log window.

It's important to have detailed logs when things go wrong: it's clear that the camera isn't streaming video, but why? By looking in the log file for the specific camera we can find all the infomration we want (and rather a lot we don't want). By having a separate log for each capture device (and each disk) then issues related to one device do not get confused with another.

Serious information like fault messages when a camera isn't streaming are still reported to the main system log as before, but the full debugging information is in the alternative log file.

To access an alternative log file, go to *Tools → System Log...* then click the *Extra Logs* tab.



Log files for cameras configured by the new setup screen (not using any legacy methods) are called `C` followed by the camera number, so `C2` is the log file for camera 2. If there are multiple streams for camera 2, they have lettered suffixes, so there might be files called `C2b` `C2c` for second and third streams. Auto–configuration of ONVIF cameras from version 6.14 onwards have suffix `auto`, eg, `C2auto`. Talkback devices have suffix `tb` in V6.14, eg `C2tb`.

Legacy camera capture devices (configured by version 6.12 or before) such as ONVIF capture devices are named after the capture device (not the camera) using the same convention used in the system log or the Cameras setup screen, for example the third capture device which is an ONVIF type is called `ONVIF3`.

Log files for disks or disk arrays are named after the disk letter, eg, DiskD for Disk or Disk Array D.

To view a specific log file, select it from the drop–down list and click Download. By default, the last 1000 lines of the log file are downloaded, showing commands sent and replies without the detail of every byte sent over the network. For the detailed debug information including all the network data, check the "Debug" checkbox and click Download.

Again this is only the last 1000 lines. This detailed version includes network data transmission in lines beginning **>** for data sent and **<** for data recieved. Only textual data is shown; not every byte of binary data is listed but a summary of the number of binary packets is shown.

To obtain the full log (not just the last 1000 lines), select the "All line" radio button.

These might be lengthy and take a while to download (tens of seconds or a few minutes). If you are submitting one of these logs to our technical support team, please obtain the full log with Debug included unless otherwise asked.

3.21.3 Client Log

The Client Log can be accessed by the menu path Windows Client Log Client Log, and give information regarding the user activities on the WaveView client software.

This log file can be saved to a USB device from the client PC.

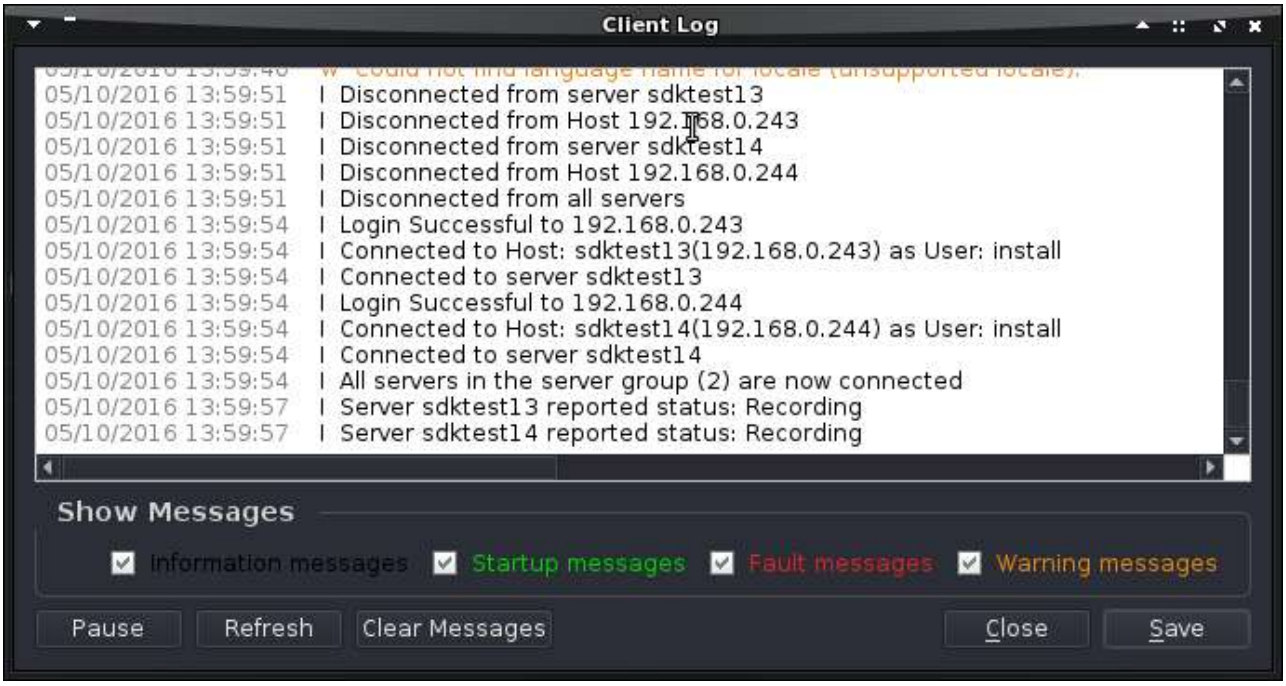


Figure 3.86: Windows Menu, Client Log screen

Log Messages are colour coded according to their type:

Warning: Orange

Information: Green

Fault: Red

Users can filter certain types of message by checking/unchecking the relevant box.

The log can be backed up to a USB device/local drive by clicking 'Save', and browsing to the desired location.

Note that the Client Log is not translated into non–English languages and is only intended for diagnostics by Wavestore Global Limitedtechnical staff.

3.22 Preferences

The WaveView client software screen can be personalised using the Preferences screen (menu path Tools → Preferences).

This screen allows the following preferences to be set for the local Client software installation (not the server itself):

The screen has various submenus as follows:

3.22.1 System Settings

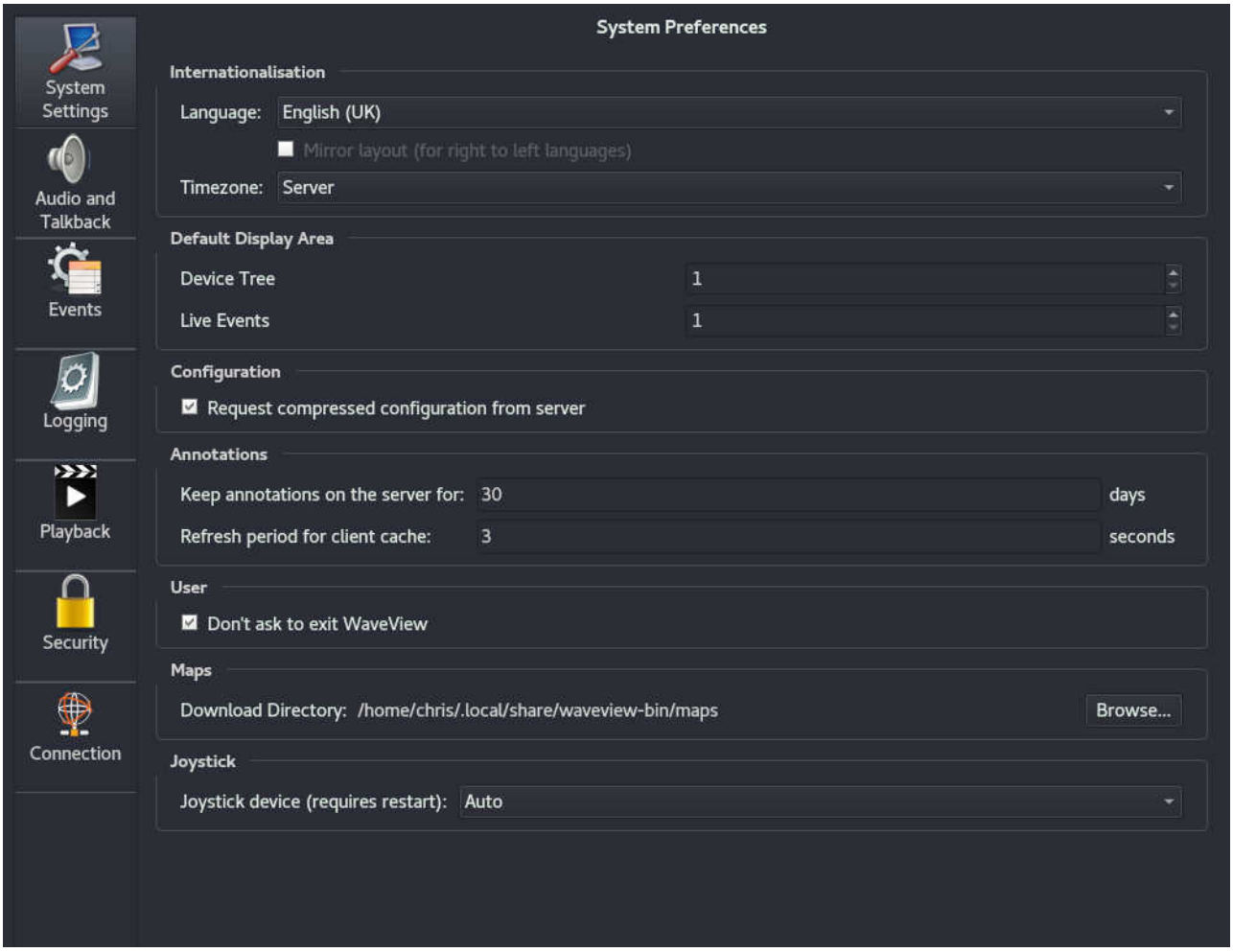


Figure 3.87: Preferences Menu, System submenu

Language — The language to use for the user interface. By default, WaveView will attempt to detect the language automatically from the operating system. Note that it is advisable to restart WaveView after applying this setting.

Mirror layout — This it not editable, but shows whether the user interface will be switched from left-to-right to right-to-left.

Timezone — This setting determines whether the user interface will show timestamps in the server's timezone, the client's timezone, or UTC. When set to "Server", the client will use the timezone of the first connected server.

Default Display Area	Allows choosing which Display Area (VDA) to use when double-clicking to open cameras in either the Device Tree or Live Events window. If the requested VDA is not open when the operations are performed, any other VDA will be used.
Request compressed configuration from server	By default, the server's configuration is transmitted in compressed form.
Keep annotations on the server for	Defines how long annotations should be preserved.
Refresh period for client cache	Determines how frequently the client checks for annotations. If there are lots of annotations and they are requested frequently, this could cause performance issues.
Don't ask to exit WaveView	Determines whether WaveViewshould ask "Are you sure you want to exit?" when closing.
Maps – Download Directory	Specifies the location of the temporary maps download directory for storing map images. Note that this should be set to a dedicated temporary path, and not a directory containing other user files as existing data may be overwritten. See section 6.7.7 – for more information.
Joystick device	Allows manual selection of a specific joystick. The default setting will automatically detect a joystick device and choose the first one found.

3.22.2 Audio and Talkback

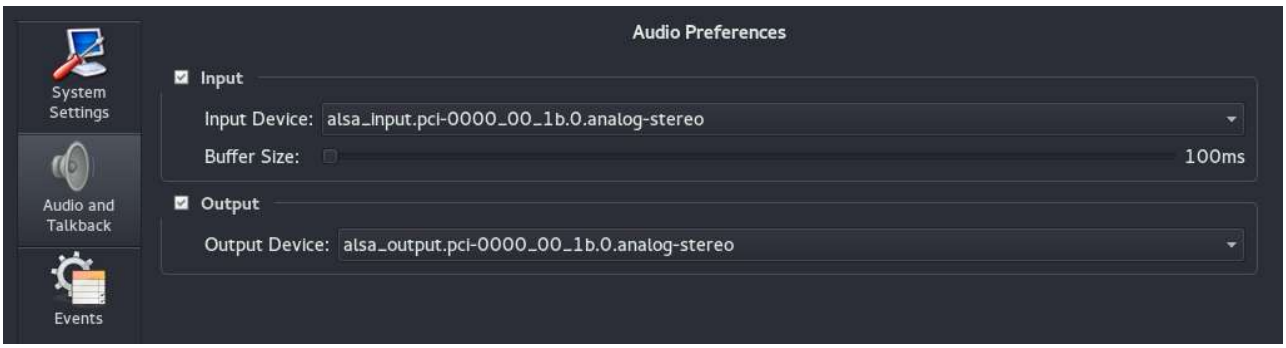


Figure 3.88: Preferences Menu, Audio submenu

This screen allows selection of the audio input and output devices. Audio input devices are used for the Talkback functionality and audio output devices are for playing audio.

3.22.3 Events

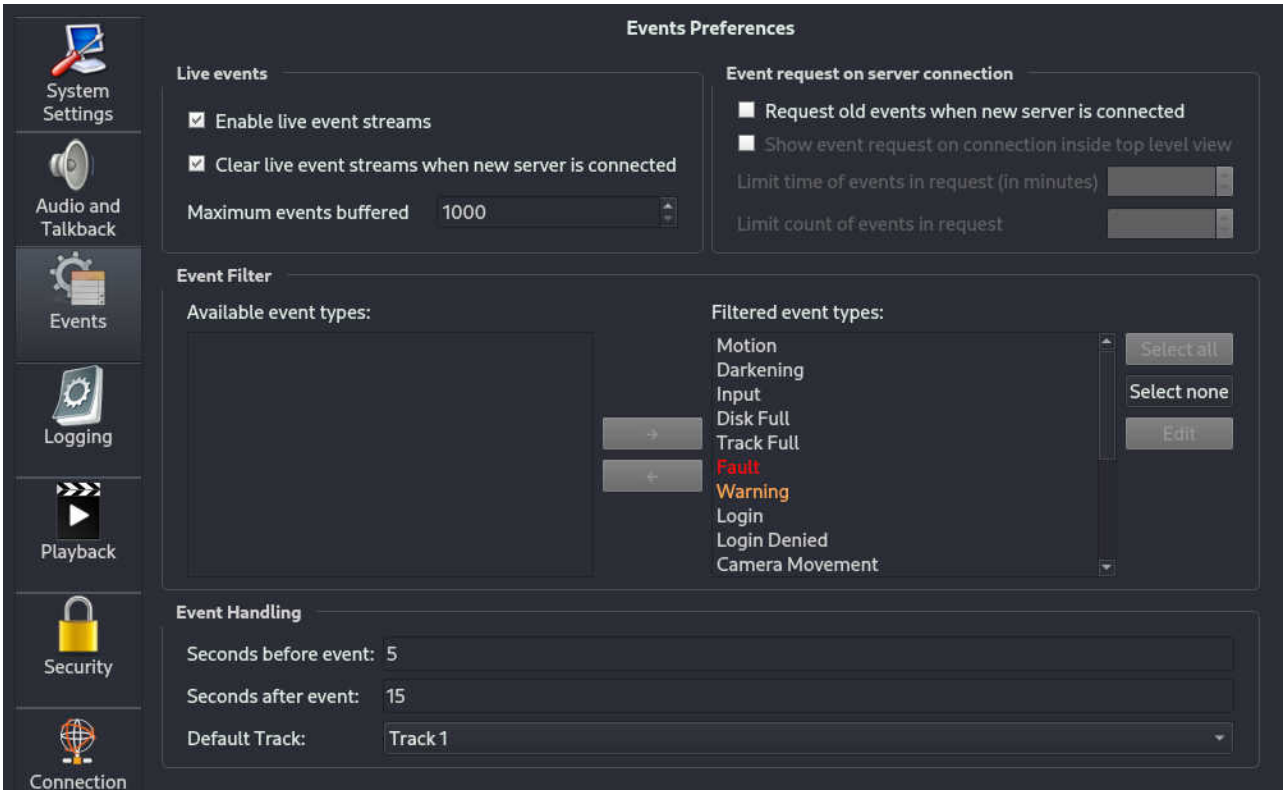


Figure 3.89: Preferences Menu, Events submenu

This screen provides a wealth of options relating to event handling. Note that the live event stream is licence controlled and so these options are only relevant if using a suitably licensed system. The options are described below:

Live Events

Enable live event streams	If enabled, WaveView will pull a stream of events from each connected server for display in the Live Event Stream on the main screen.
Clear live event streams when new server is connected	When disconnecting from a Wavestore server and then connecting to a new one, it is often desirable to clear the old events. That will happen if this option is enabled.
Maximum events buffered	This sets the maximum number of events to be stored in memory. Increasing this number increases the memory usage of WaveView.

Event request on server connection

Request old events when new server is connected	When WaveView disconnects from a server, it makes a record of the last event seen. If this option is enabled, when WaveView re-connects to that same server it will request all events since that previous connection.
Show event request on connection inside top level view	This is a diagnostic tool used when examining issues with requesting events. Generally not needed in everyday use.
Limit time of events in request (in minutes)	When requesting old events, only request those which are not older than the number of minutes specified here. The limit is 2880 minutes which is 48 hours.
Limit count of events in request	When requesting old events, only request a maximum of this number.

Event Filter

This area allows detailed configuration of the types of events that will be shown in the Live Event View. It is described in more detail below.

Properties associated with each event type can be edited to change the appearance (text/background colour in the Live Event Stream), and also assign a notification sound for that event type.

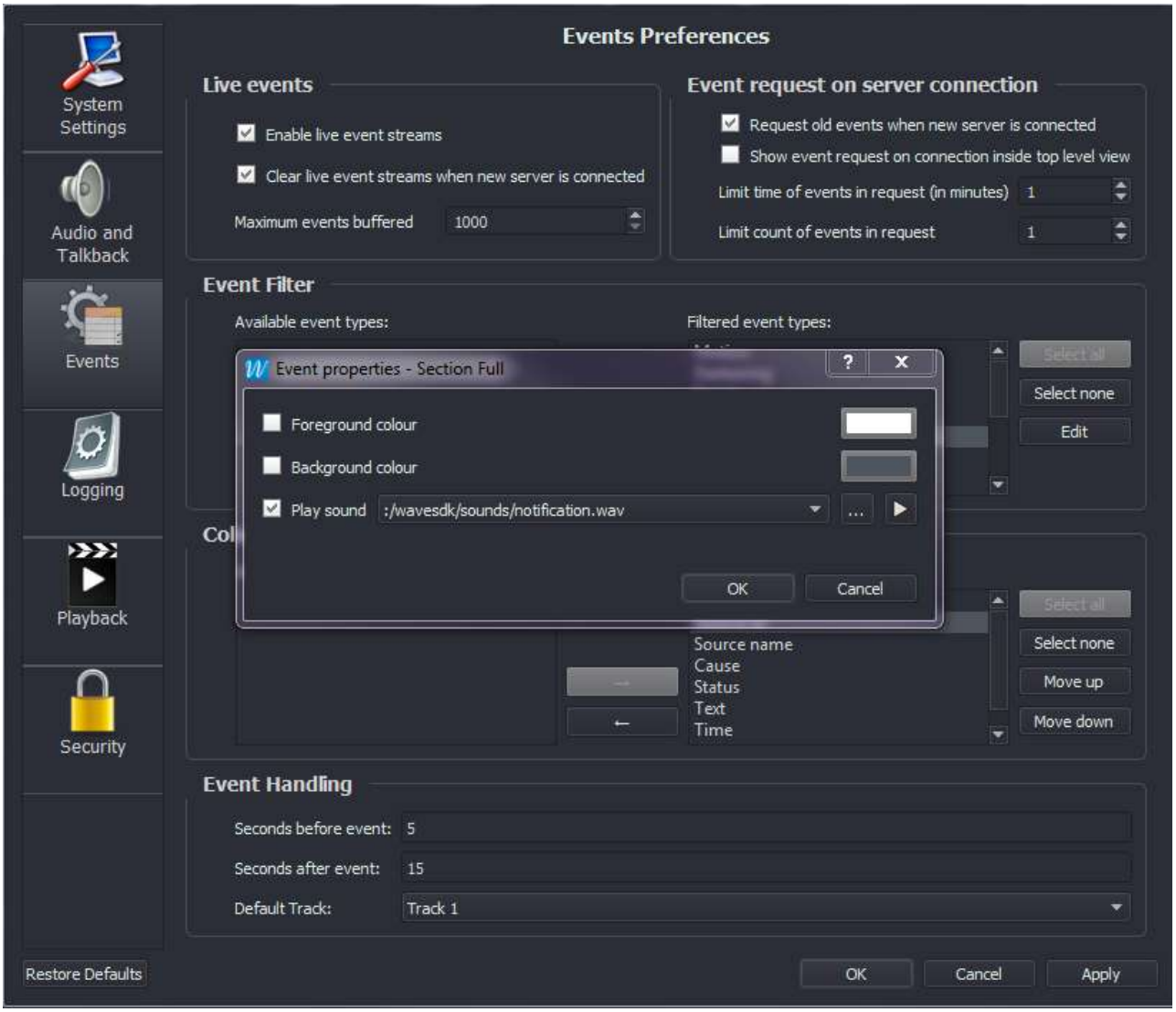


Figure 3.90: Preferences Menu, Events submenu, configuring Properties for Event

To add a new Event to this list, click on your desired Event in the Available Event Types list (the event name will highlight Dark Grey), then click on '–>' arrow key; the event name will now appear in the Filtered Event Types box. To add remove an Event from the Filtered Events Types list, click on your desired Event, then click on *LEFT ARROW* key.

Event Handling

If the system has the "Live Events Stream" licence feature activated, a user can manually export footage for an event (e.g. Digital Input) by right clicking on that event in the Live Event Stream window (see section 3.18 – Live Event Stream (Optional Licensed Upgrade)).

Exports are created in the native Wavestore "WSB" format, and can then be played back using the WaveView software. The exports are saved to `C:/Users/username/WavestoreExports`.

The 'Event Handling' options determine how these exports are made:

Seconds before event	When creating an export from an event in the Live Event View, this specifies the length of time before the event that the export should start.
Seconds after event	When creating an export from an event in the Live Event View, this specifies the length of time after the event that the export should end.
Default track	When creating an export from an event in the Live Event View, this specifies the default recording track to use.

3.22.4 Logging

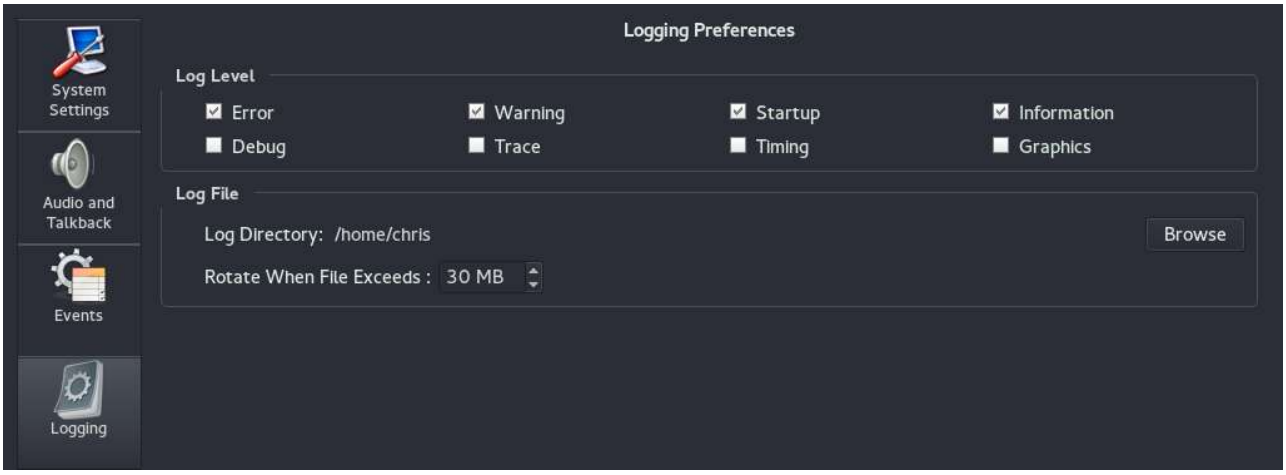


Figure 3.91: Preferences Menu, Logging submenu

The Logging submenu controls which message types are written to the Client Log (Debug/Error/Information/Warnin

We can also configure which folder on the local PC the log messages are written to, and the size of the folder that will be allocated to these messages.

3.22.5 Playback

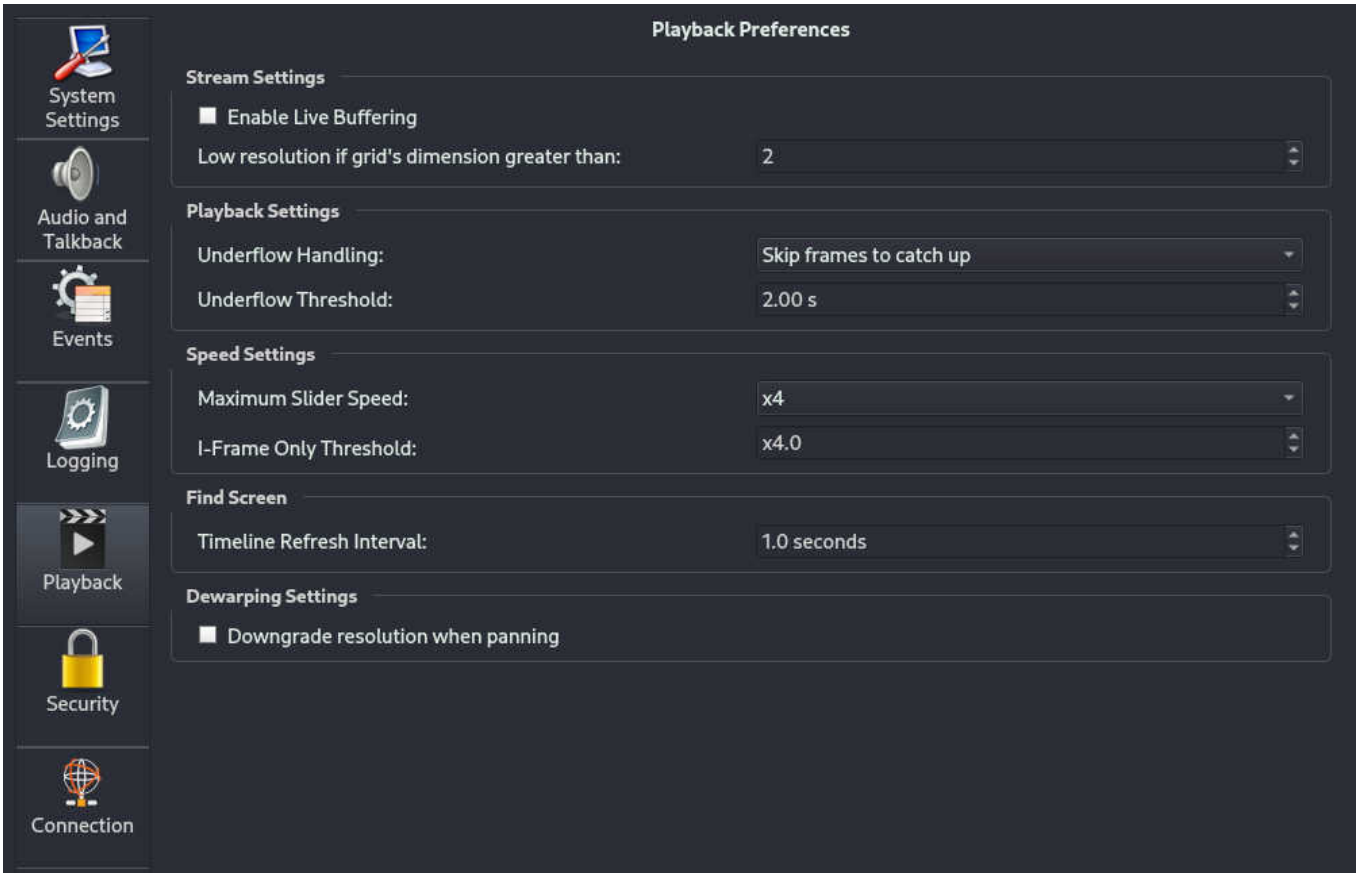


Figure 3.92: Preferences Menu, Playback submenu

The Playback Preferences menu has the following settings:

Enable Live Buffering — When this option is disabled, live images are shown as soon as possible. This means that latency is kept to a minimum, but can mean that live viewing isn't very smooth. Enabling the option introduces some latency but smooths the live streaming. It is generally advisable to disable this when using PTZ cameras as latency can make them hard to control.

Low resolution if grid's dimension greater than — WaveView will request a low resolution stream for each camera when a grid layout has a dimension greater than this number. This only applies for certain camera types and when dual-streaming has been set up.

Underflow Handling — This determines what the client should do when it is struggling to keep up with the video. For example if the CPU can't decode the video fast enough, or if the network can't deliver images fast enough.

Underflow Threshold — This setting determines when the playback mechanism will jump forward to the expected time if it is

	struggling to keep up with playback.
Maximum Speed Slider	The Main Screen has a slider for fast playback. The default maximum speed for this is x4.0. This setting allows the maximum speed to be changed. Note that fast playback requires a powerful PC and the video may jump if the system is not powerful enough. This mechanism is not a substitute for the Fast Forward operation.
I-Frame Only Threshold	When doing fast-playback on the Main Screen using the fast-playback slider, high playback speeds may result in jerky playback. To remedy this the software will switch to only playing i-frames once the playback speed exceeds this threshold.
Timeline Refresh Interval	Dictates how frequently the timeline in the Find Screen is refreshed. On particularly highly loaded systems, this might be useful to reduce the amount of data being sent across the network.
Downgrade resolution when panning	This feature, when enabled, improves the performance of panning a dewarped camera by temporarily reducing the display resolution. This allows for smoother panning.

3.22.6 Security

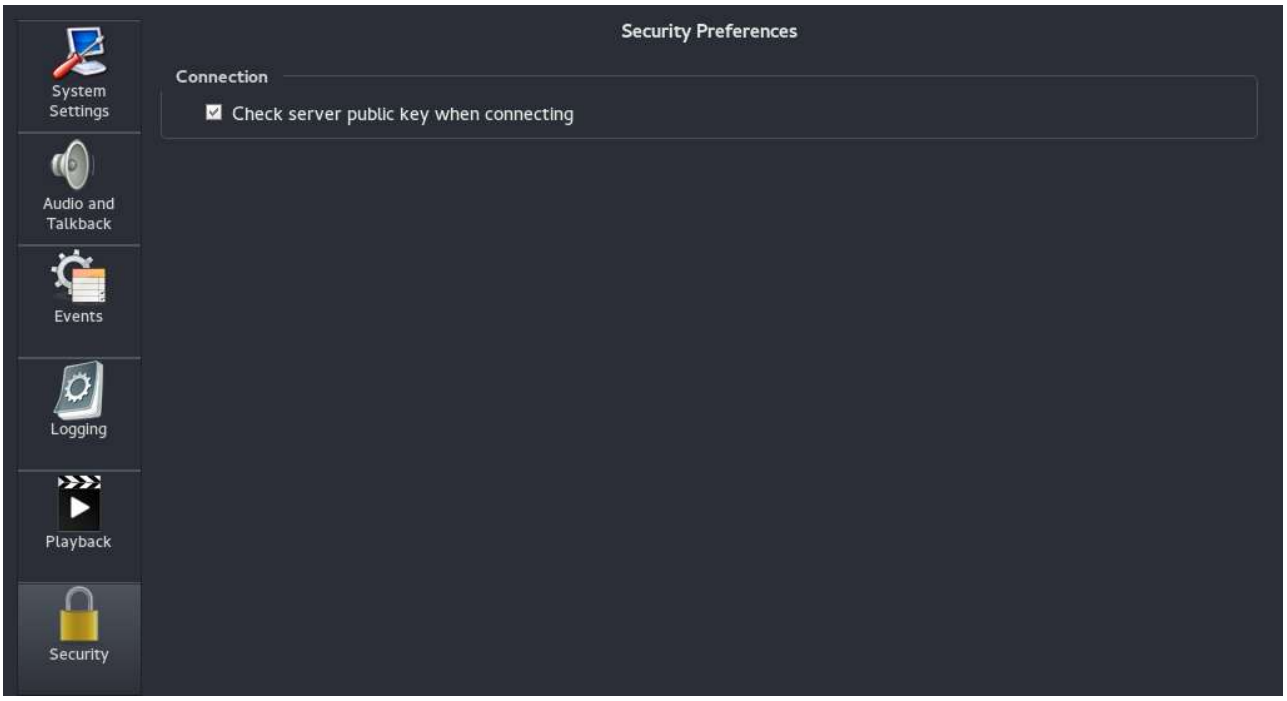


Figure 3.93: Preferences Menu, Security submenu

This screen currently has one option; "Check server public key when connecting". This is a security measure designed to protect against "Man in the middle" attacks. Each Wavestore server has a unique key which is generated when the software is installed. When WaveView connects to a server for the first time, it stores that key. If the same server is connected to at a later time and the key is different, this suggests either that the Wavestore software has been re-installed, or that somebody is attempting to intercept the communications, in which case it is inadvisable to continue the connection.

Note that older servers (prior to version 5.52) had an issue where the key would change when the server is restarted, therefore a warning message will appear on every connection between server restarts. It is advisable to upgrade those older servers, but this preference option can also be disabled to prevent WaveView from performing the check.

3.22.7 Connection

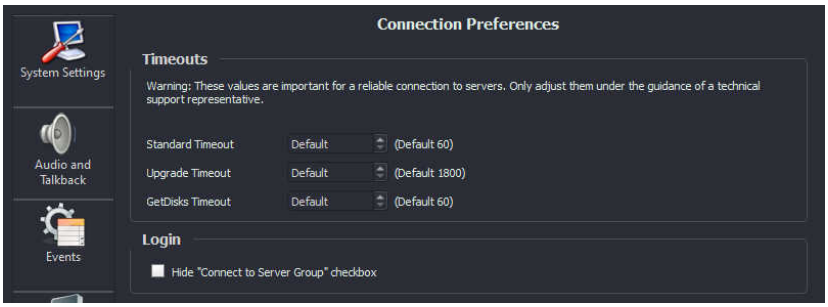


Figure 3.94: Preferences Menu, Connection submenu

This screen contains advanced options relating to the connections between WaveView and each connected Wavestore server.

Timeouts

As described in the warning message, it is strongly discouraged to modify the timeout values unless under the guidance of an official technical support representative. The default values are carefully chosen to work well in the vast majority of cases.

Login

This section has one option – Hide "Connect to Server Group" checkbox. If enabled, the checkbox on the Login Dialog to allow connection to a server group, rather than an individual server, will be hidden. This is useful if certain clients should only be allowed to connect to one server at a time.

3.23 Connection List

Once a WaveView client has established a connection to a Wavestore server, we can view a list of all active client connections to that server by following the menu path Tools → Connections

Click to select the server that you wish to interrogate in the column on the left; information on all connected users (Client IP address, and user logon ID) will then be displayed:

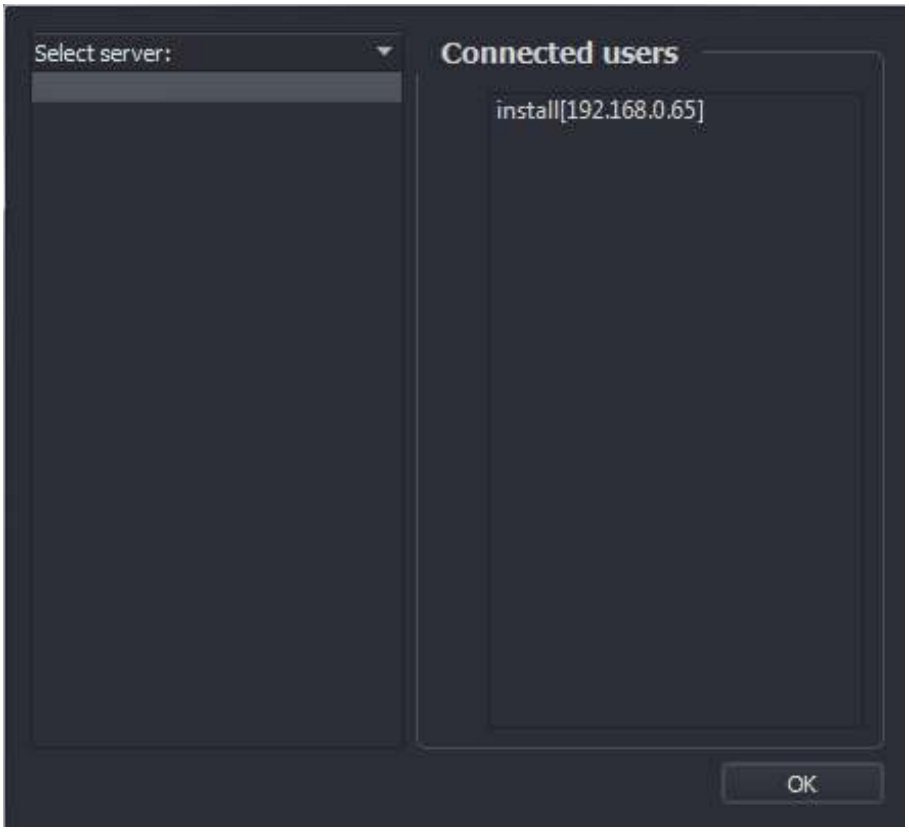


Figure 3.95: Tools Menu, Connection list

3.24 Copy WaveView

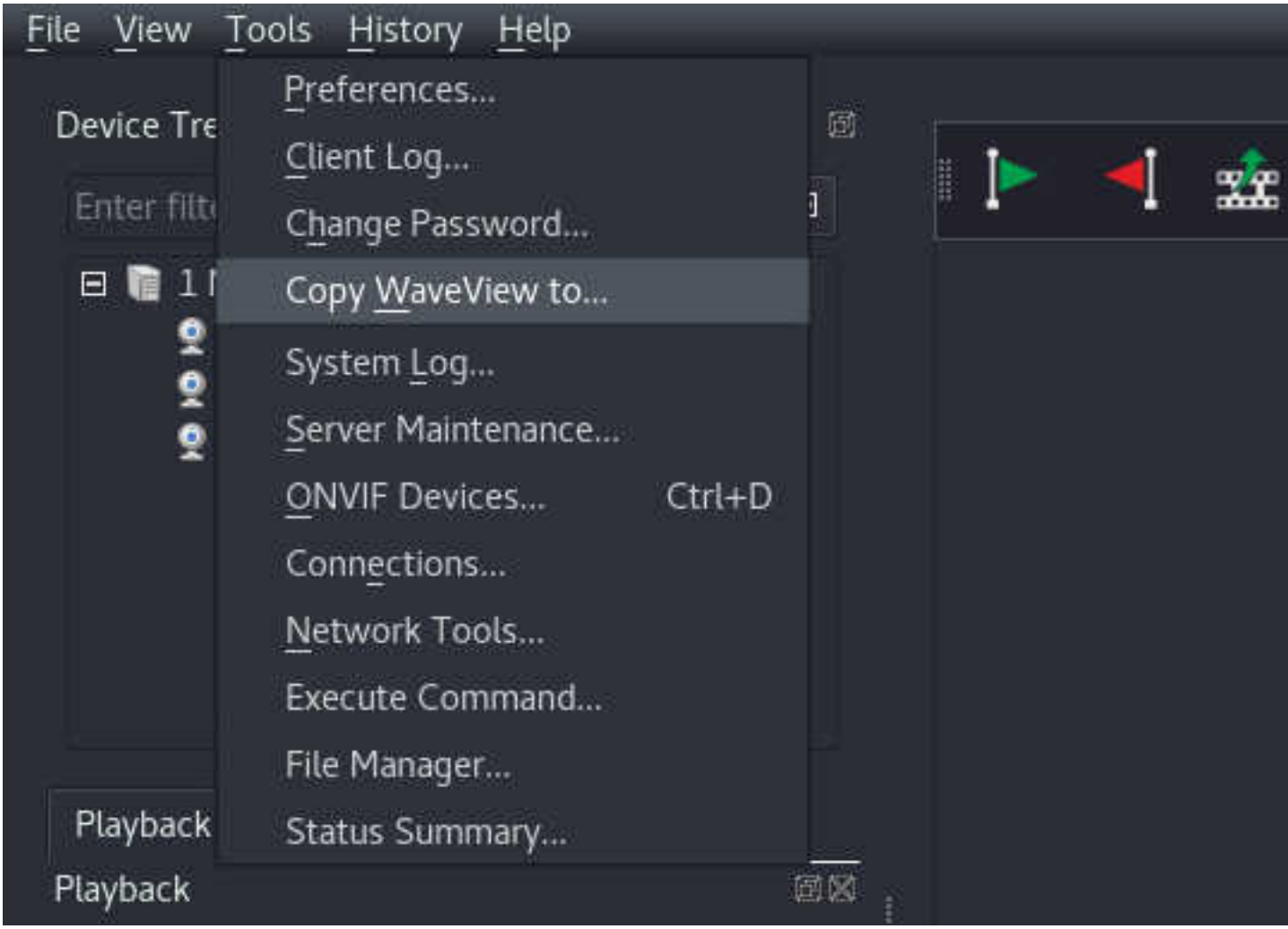


Figure 3.96: Tools Menu, Copy WaveView

Selecting this option will send a copy of the WaveView program files to a selected folder on your PC. This feature is useful if you have exported a WSB export file which you wish to play back on another PC that does not have WaveView installed.

Simply browse to your desired destination folder, and then click 'Select Folder' to start the copy process.

Note that the files are copied from your local WaveView installation. They are not transferred from the server.

3.25 Server Maintenance

The Server Maintenance menu is used to set up various systems and services on the Wavestore server.

Menu entries can be selected by double-clicking the entry, or single-clicking the entry to select it then clicking OK. Clicking ***Close*** will return to the previous menu.

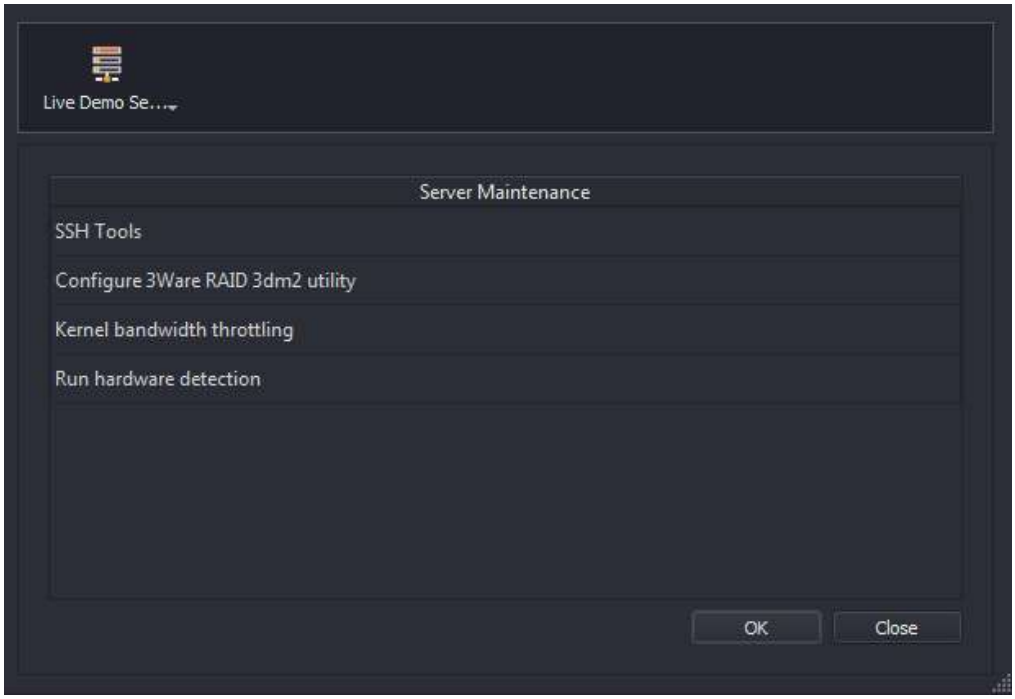


Figure 3.97: Tools Menu, Server Maintenance submenu

SSH Tools Note: This option will only function if you have installed the 'wavestore-ssh-tools' software package. This package is not normally distributed due to export laws, however you can obtain it by contacting your support representative.

The SSH Tools allows configuration of the Secure SHell service which is used for remote support by Wavestore support representatives. In normal usage these options should be left as the defaults, however a Wavestore support representative may ask for some settings to be changed for the purposes of remote diagnosis and investigation.

The menus allow:

- Enabling and disabling the service
- Switching between secure mode and password mode

Secure mode requires a special key to log in, and only Wavestore support representatives have this key. Therefore this is the preferred setting. Password mode is less secure and should therefore only be enabled under guidance from a Wavestore support representative.

Configure 3Ware RAID 3dm2 utility

When a Wavestore is supplied with RAID (Redundant Array of Independent Disks), it is usually provided by a 3Ware RAID card – this is a physical device in the Wavestore server. In order to manage the RAID system there is a web interface which is disabled by default.

This menu option allows enabling and disabling of the 3Ware RAID service. When enabled, the RAID utility can be accessed from a web browser (either from the server itself, or a PC) using the following URL: https://[serverIPaddress]:888

Default login details for the 3ware GUI are ID: Administrator, Password: 3ware

An example of typical RAID setting to use on a Wavestore server is shown below:

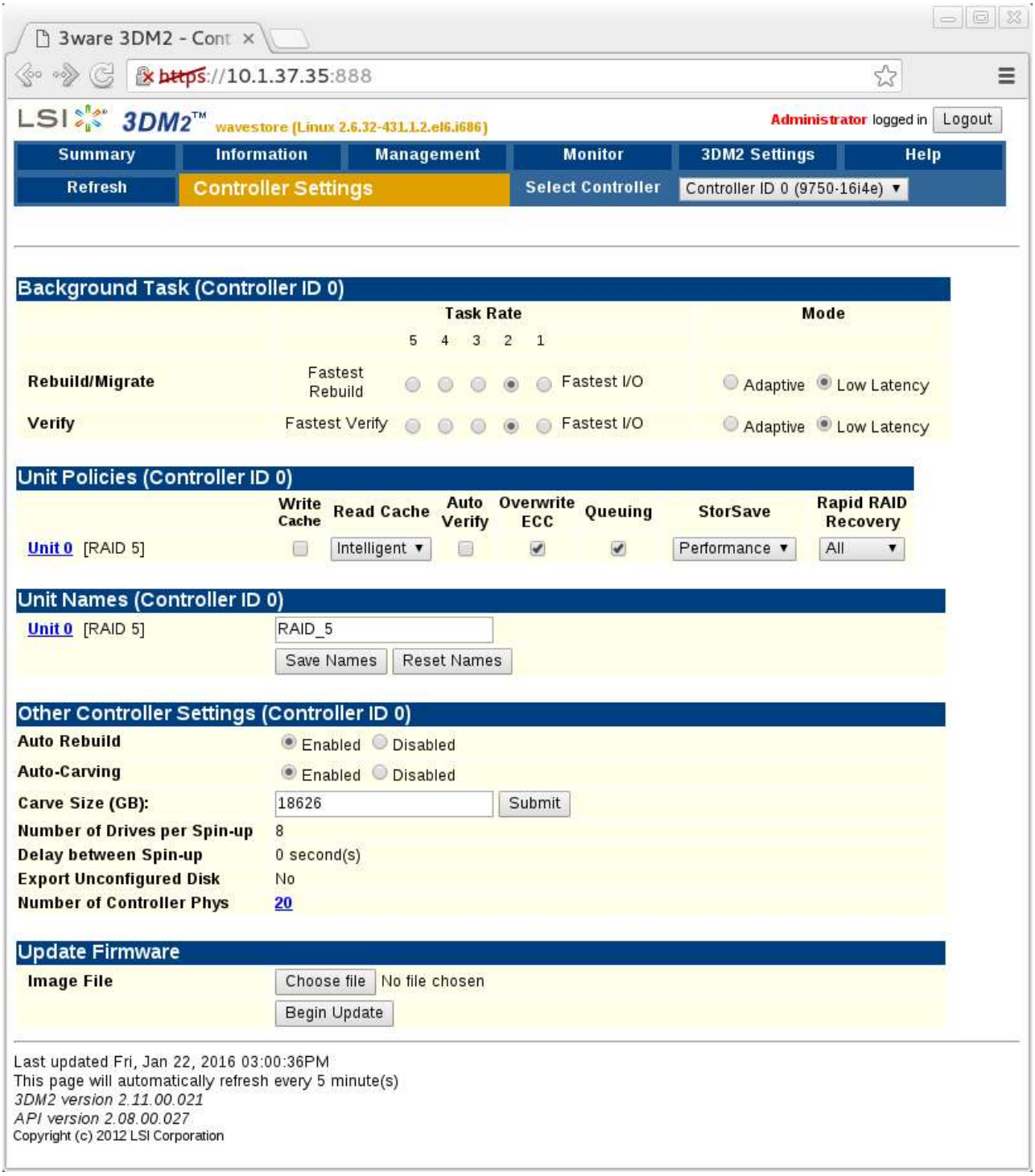


Figure 3.98: 3ware RAID array – example configuration

Run Hardware Detection When a Wavestore has new capture hardware installed, e.g. an analogue capture card or audio card, it will automatically detect that new hardware is present and run its 'hardware detection' process. This modifies the server configuration to ensure that the appropriate number of video and audio channels are available for configuration in the Cameras setup screen.

In rare circumstances it may be necessary to force the detection process to run and this menu option

provides that facility.

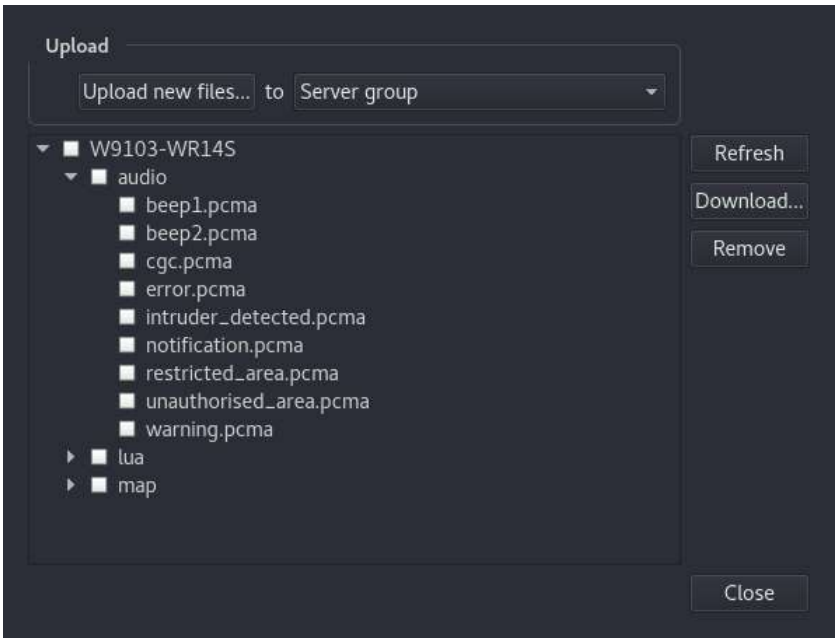
Configure server graphics drivers The default graphics drivers on any Wavestore should normally perform well out–of–the–box. However sometimes, for either performance or compatibility reasons, it may be desirable to install the proprietary graphics drivers from the appropriate manufacturer, either NVIDIA or AMD (formerly ATI).

This menu option allows the proprietary graphics drivers to be installed or uninstalled remotely. This can be useful when doing remote upgrades or maintenance, although it's advisable to have someone available to check that the graphical interface is working after any change. A reboot is required after installing or removing proprietary drivers. Removing the proprietary drivers causes the system to fall back to the default drivers.

3.26 File Manager

Overview

The File Manager is used to upload and download files to or from individual Wavestore servers or a server group. An "install" level user is required to perform all the operations, although other user–levels can view the files.



Currently there are 3 types of files shown:

Audio These files are used when creating Event Rules used to trigger a sound to be played by the server – either via an audio output or by transmitting to a network camera with audio output. Any audio file uploaded should be raw PCMA (8kHz PCM A–law) with a '.pcma' suffix.

Lua These are scripts which are used by integration modules – used to integrate Wavestore with 3rd party devices.

Map These are image files used by the Map system. It's not normally required to upload or downlod them from here, it's performed automatically when setting up maps using the Map Setup Screen.

However they are shown here for diagnostic purposes.

Usage

The available files are represented as a "tree" where the top level consists of the servers in the server group. The second level is the file type, and the third level is the files of each type.

To download a file, simply select it and click "Download...". This will ask the user where the file should be saved.

Similar, to remove a file, simply select it and click "Remove".

When uploading a file, it is necessary to prepare a zip file containing the file or files to be uploaded. There are restrictions on the valid file names and types as follows:

- The file name may only contain characters 'a–z', '0–9', '–', '_', and '.'
- The file name must end in one of: '.lua', '.pcma', '.jpeg', '.jpg', '.png', '.svg', '.bmp', '.gif', '.wsb', '.conf', '.pdf', '.txt', '.devdb'
- The file must be 2 Gigabytes or smaller in size

To upload the zip file, first decide if the file should be uploaded to an individual server or the whole server group. By default "Server group" is selected. Clicking the "Server group" drop–down list allows selecting an individual server.

The next step is to click "Upload new files...", then to select the zip file prepared earlier. Upon receving the zip file, the Wavestore will analyse the contents and move the contained files to the appropriate location. e.g. audio files of the correct type will be moved to the "audio" directory, and image files of the correct type will be moved to the "map" directory.

3.27 Status Summary

Overview

The status summary screen provides quick access to server group devices. It will show a list view of all devices connected to all servers in a group and status information for each device.

To open the screen, select Status Summary from the application Tools Menu. The screen will open in a separate window so that it is possible to continue working in the main application.

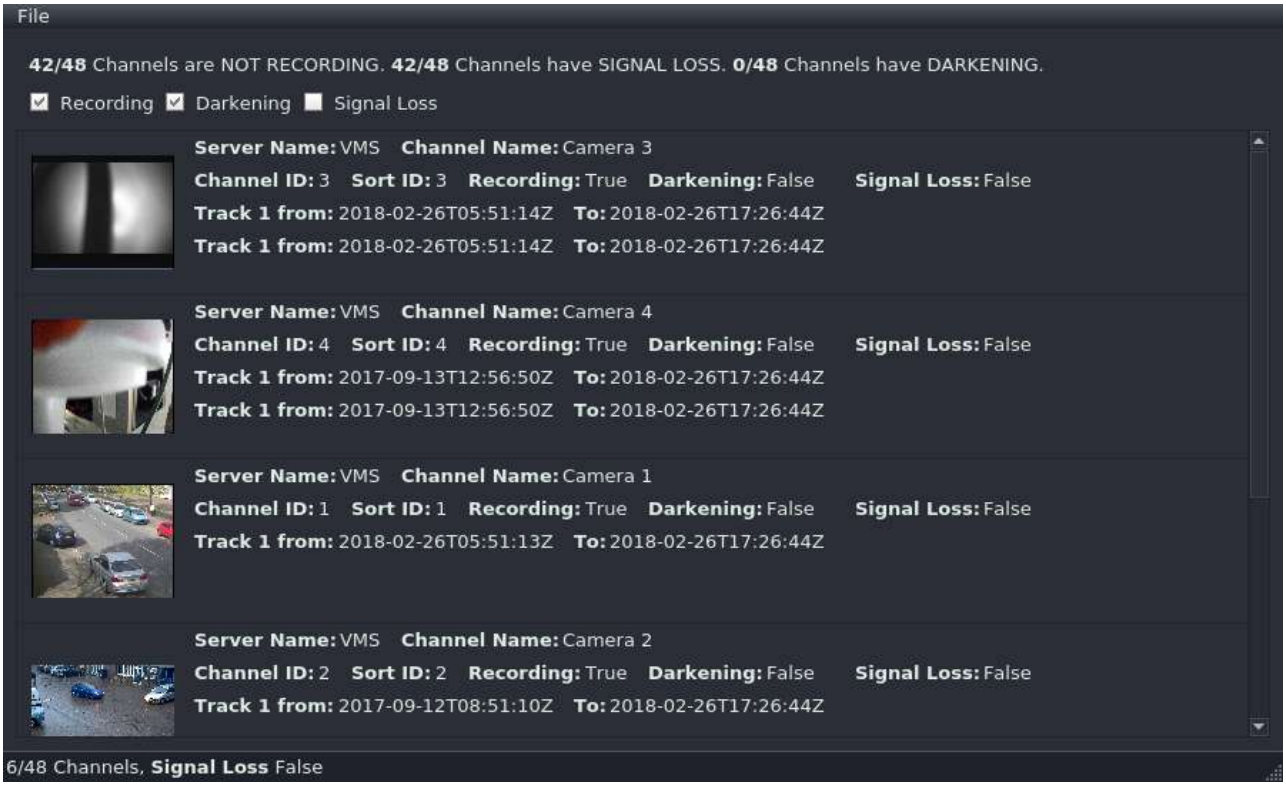


Figure 3.99: Status Summary Screen

Channel Status Fields

The status of each channel is shown in the table. Possible states are True and False and a description of each status field is given below:

Recording Whether recording is active for this channel on any recording track.

Darkening The image from the camera is unusually dark and might indicate tampering.

Signal Loss There is a problem receiving data from this channel.

Channel Types

If the device is a camera and is functioning correctly, then a thumbnail capture from the camera will be shown in the status summary table. Otherwise, one of the following icons indicates the channel type and status:

- Audio Channel
- Audio Channel with Signal Loss
- Talkback Channel
- Talkback Channel with Signal Loss
- Camera Channel (Loading)

-  Camera Channel with Signal Loss

Channel Information Fields

Server Name The name of the server in the group to which the device is connected.

Channel Name The name of the channel associated with the device.

Channel ID Numeric code identifying the channel on the server.

Sort ID This is the custom number assigned to a channel (used to allow custom numbering schemes).

IP The IP address of the camera, if applicable.

Track List

Active tracks will be listed below the state fields with the start and end timestamps for the recording duration. If a track has a custom name, it will be shown instead of the track number. Disabled tracks will not be shown.

Filtering

It is possible to apply a filter to the table, and see only those channels with a particular status by toggling the state of the check-boxes at the top of the window. Filtering is disabled by default and all channels will be shown in the table.

The filter value of each field is show in the status bar of the window, along with the number of channels which pass the filter and appear in the table.

The possible states of the check-boxes are shown below:

Tick The field does not participate in the filter.

Mark Only channels with the field marked as True will be shown.

Blank Only channels with the field marked as False will be shown.

Table Export

The contents of the table can be exported to a CSV (comma-separated-values) file to be viewed with external software. The entire contents of the table will be exported and will include all channels from all servers in the group, even when filtering has been applied to the view. There is some extra information in the exported CSV file such as the duration of recording for each track.

To export the table to a file:

- Select Export from the File menu in the Status Summary window.
- Browse to the save path.

- Press save.

3.28 Server Statistics

Overview

The server statistics screen displays graphs of statistics, to allow the client to monitor hardware performance and other server information.

To open the screen, select Server Statistics from the application Tools Menu. The screen will open in a separate window so that it is possible to continue working in the main application.

Operation

The server statistics screen can display one or more graphs.

If using a server group containing more than one server, the server for which to display statistics can be selected on the top button bar.

The + and – buttons at the bottom of the screen can be used to insert new graphs or remove existing ones.

The chart drop-down list is used to select which statistics are displayed on the graph. One graph is always displayed. When the screen is opened the graph defaults to the first entry in the chart drop-down list.

The ***filter*** text box can be used to filter which statistics are shown in the drop-down list.

Statistics in the list have data points usually sampled every 15 minutes. The time range for all graphs can be set by adjusting the date and time and selecting a duration.

Hovering over the graph line displays a tooltip giving the value of that data point and the time it occurred. If the data is numeric then the range of values contained in the statistics is also displayed.

4 Search/Playback/Export using Find Screen

The Find screen (menu path View → Find) allows you to search and play back footage stored on the server.

This screen displays a searchable timeline of recorded audio/video, for all recording tracks for each channel.

If the client software is connected to a number of Wavestore servers that have been configured as a Server Group, we can search footage on any of the servers in the group.

The Find screen allows easy navigation within the archived video, exporting of video in multiple formats, an annotation facility for sections of video footage, and searching using filters such annotation and events. The screen is similar to the main screen Display Area, the main difference being that all of the Find Screen Video Displays are time synchronized with each other; playback of a single Video Display cannot be controlled independently.

The time displayed in all of the Find Screen Video Displays is based on the position of the current time marker (black vertical marker) on the purple timeline bars. This time is also displayed on the Current Time Indicator.

The Find screen contains the following items:

- Display Area
- Horizontal Timeline Bars (marked in purple)
- Pull Down Menu Bars
- Archive Range section
- Selection Range section
- Current Time Indicator
- Playback Controls
- Video Display Toolbar

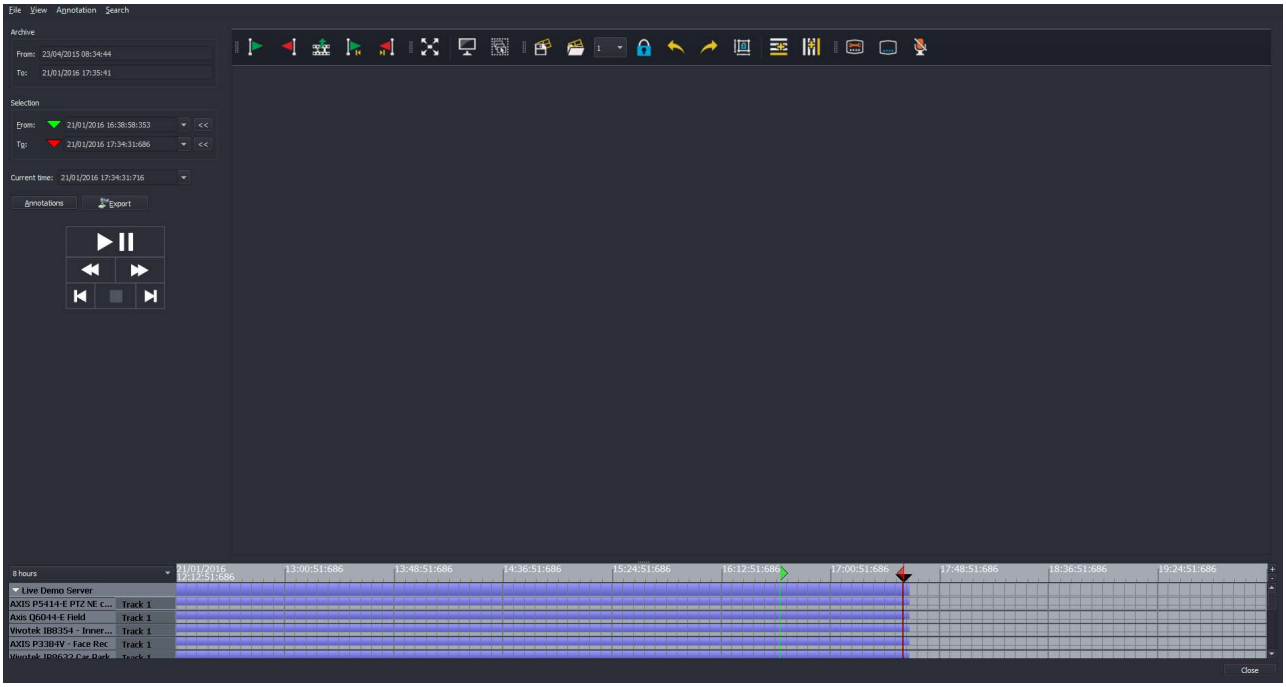


Figure 4.1: Find Display Area

4.1 Pull Down Menus

The Find screen pull down menus contains the following items:

File Menu

Close Closes the Find Screen

View Menu

Track 1 Toggle option to display recorded footage from Track 1 in the time line (default – On)

Track 2 Toggle option to display recorded footage from Track 2 in the time line (default – Off)

Track 3 Toggle option to display recorded footage from Track 3 in the time line (default – Off)

Show Time Grid Toggle option to display a grid is shown under the time line (default – On)

Show Annotations Toggle option to display any annotations marked into indicator beneath each camera channel timeline

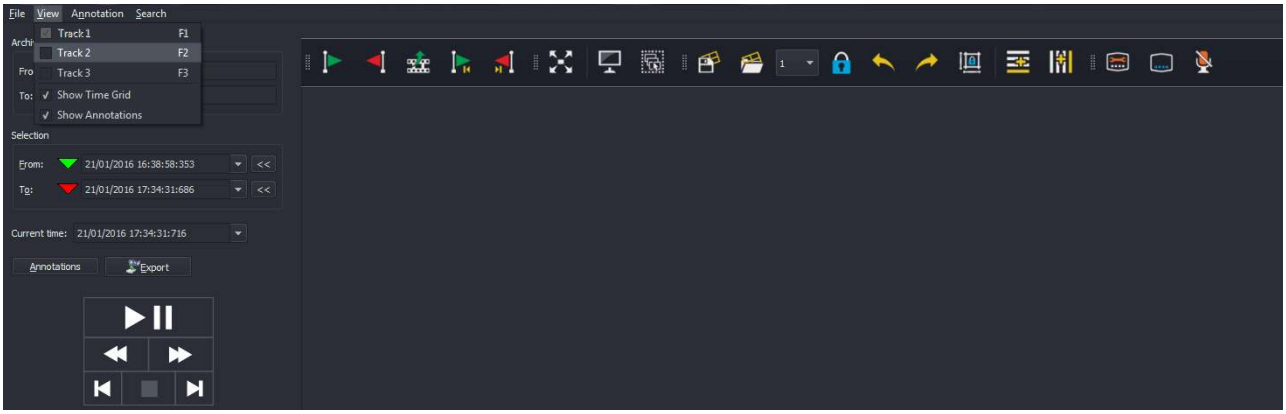


Figure 4.2: Find Screen – View Menu

Annotation Menu

New Opens the Create Annotation window

Edit Opens the Annotation Edit window

Search Menu

Events Opens the Event Search window (optional licensed upgrade module)

Metadata Opens the Metadata Search window (optional licensed upgrade module)

4.2 Time/Date Displays

4.2.1 Archive Range

The archive range displays the time and date range of the recorded footage currently stored on the server.

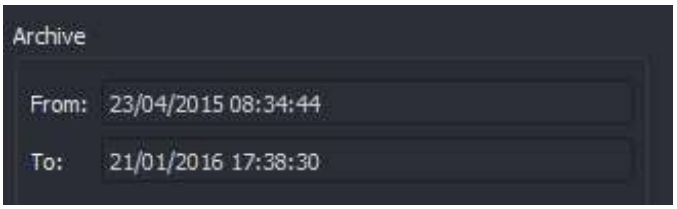


Figure 4.3: Archive Range

4.2.2 Selection Range

The selection range displays the section of footage selected for export.

The data in these fields can be configured by highlighting with the mouse, and entering the required data with the keyboard.

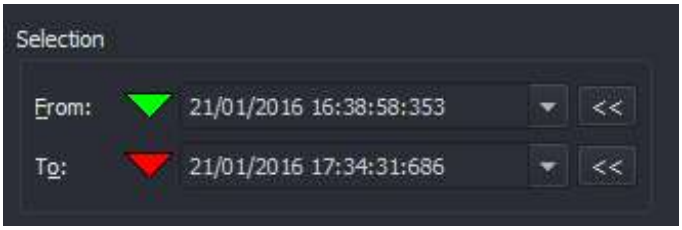


Figure 4.4: Selection Range

Alternatively we can click and drag on the timeline bars to select the required ***From*** time, then click the ***Double left arrow*** icon, and repeat for the ***To*** time (click on ***Double right arrow*** icon).

The final method that can be used is to configure the Selection Range is to click and drag the Green and Red markers on the Time Line, to set the ***From*** and ***to*** times.

4.2.3 Current Time Indicator

The current time indicator displays the current master time for all individual Video Displays in the Display Area.

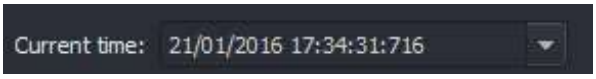


Figure 4.5: Current Time Indicator

When a new time is entered in this box, all Video Displays in the Display Area will display footage from the new time that has been entered.

4.3 Play Controls

The Play Controls in the Find screen behave in the same way as on the main Live View screen (see section 3.10 – Playback Controls); the only differences being that they control all of the individual Video Displays, and that live view is not available.

4.4 Search/Playback

When the Find screen is first opened, the Display Area has no camera views configured, as shown in Fig 6.1. To select a display configuration or a custom view, right click on the Display Area to call up the Context Menu:

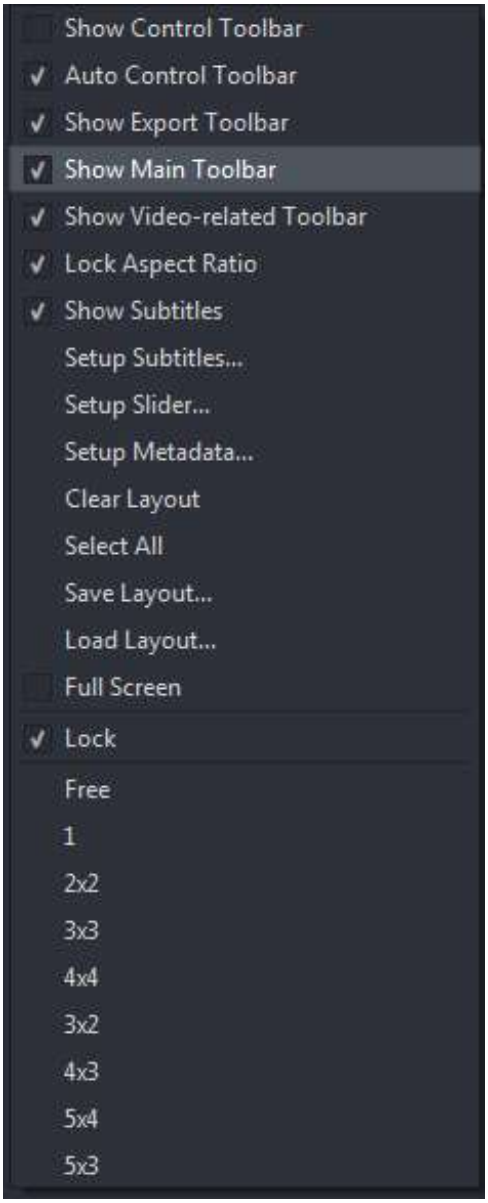


Figure 4.6: Context Menu

The Context Menu offers the following options:

Camera View Configuration

Show Control Toolbar Quick Search Toolbar described in section 3.15 – Quick Search Controls using Time Slider

Show Audio Toolbar described in section 3.3 – Display Area Toolbar

Lock Aspect Ratio Causes all Video Displays to be fixed to their true aspect ratios (width and height)

Show Subtitles Video Displays subtitles toggle option (on/off)

Setup Subtitles Opens the Setup Subtitles screen

Setup Slider allows configuration of Time Slider used for quick search at the lower edge of each Video

Display

Clear Layout Removes all Video Displays from the Display Area

Select All Selects all Video Displays within the Display Area

Save Layout Saves the current layout – see section 3.7.1 – Saving and Loading Layouts

Load Layout Switches to a previously saved layout – see section 3.7.1 – Saving and Loading Layouts

Full Screen Expands the Display Area to full screen display (to exit from full screen display, right click to call up the Context Menu once again, and toggle the Full Screen option OFF, or click the "Exit Full Screen" button at the top which is visible when the mouse is moved)

Camera View Selection

Free You may add views from as many cameras as you wish

1, 2x2, 3x3, 4x4, 3x2, 4x3, 5x4, 5x3 – Switches to a fixed, preset layout of displays

Double–clicking on the timeline of a Camera Channel will cause the associated Channel to be displayed in the Display Area, as shown below.

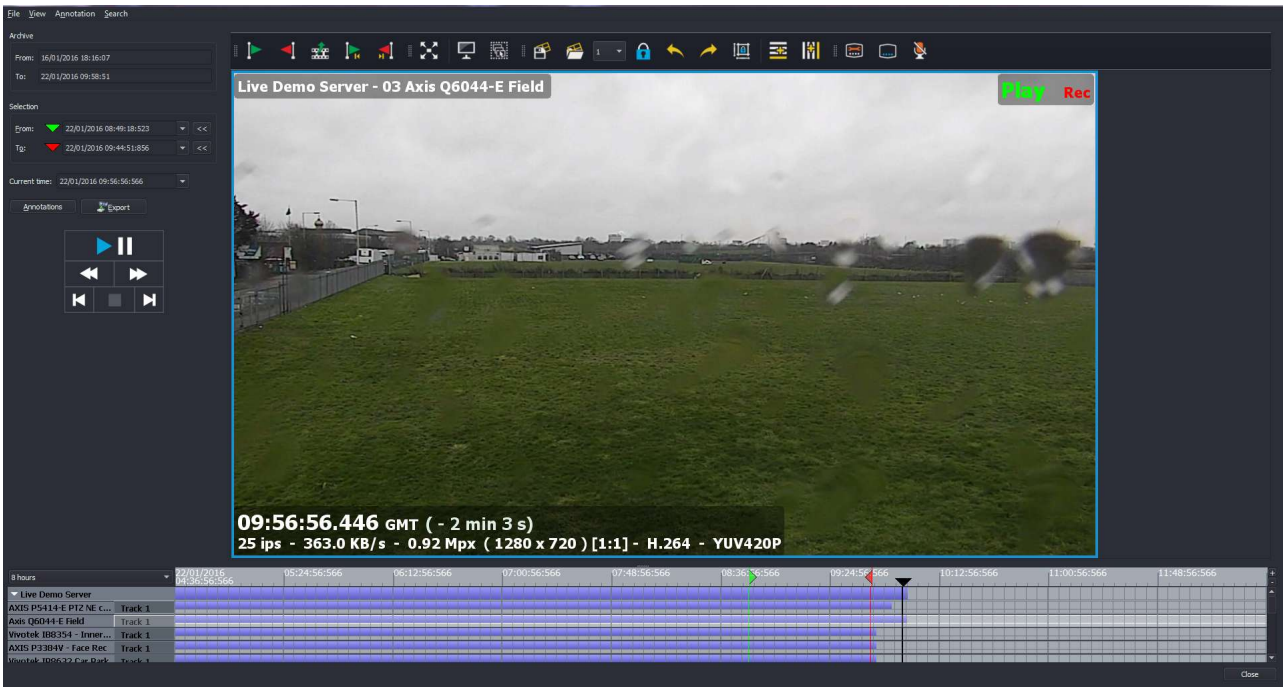


Figure 4.7: Single Camera Channel displayed in Find screen

When you click on a Camera Channel timeline, if the Video Display is currently viewing one Video Display, the Video Display is switched to the newly selected channel.

Alternatively, if you have configured a multichannel display (e.g. by selecting the 2x2 option from the Context Menu), a new Video Display containing the new Channel is added to the Video Displays already displayed within the Display Area.

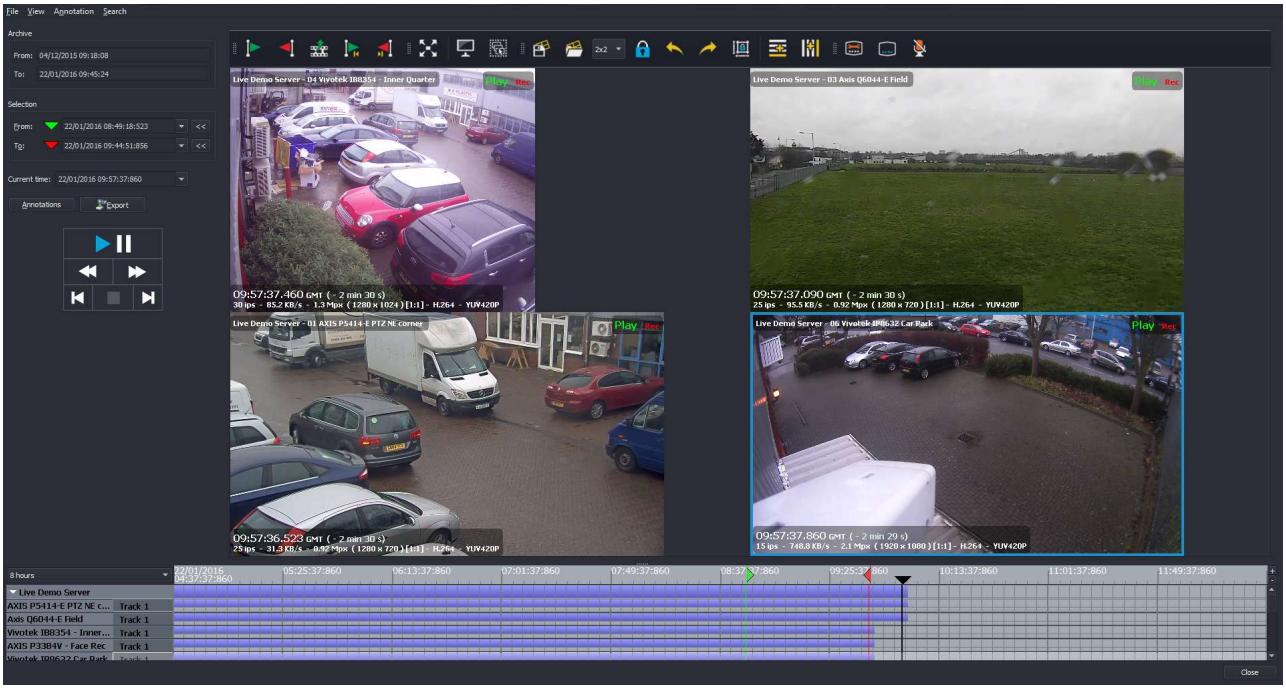
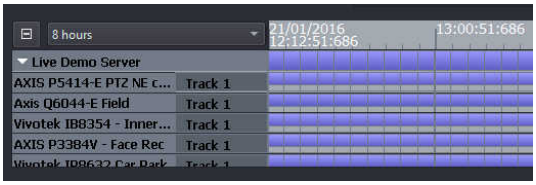


Figure 4.8: Four camera channel display in Find screen

4.4.1 Using the Time Line to Search

The time line is displayed horizontally, with oldest recordings to the left.



There is a row per server, and a row per channel on each server. Clicking the "–" button (sometimes shown as "+") toggles expanding or collapsing each server, to show or hide all the channels for that server.

The purple bars next to the server name indicate areas where recorded events exist. Underneath the server name, there is a row for each recording track, although by default only Track 1 is shown for each camera.

The black vertical marker indicates the current point in time for playback. Gaps in the time line indicate that no recordings are present for that time period (e.g. a camera channel recording on Motion Detect).

Searching on the time line can be carried out as follows:

- Left–click and drag the horizontal bars to change the current time position, and display the relevant video in the Video Displays

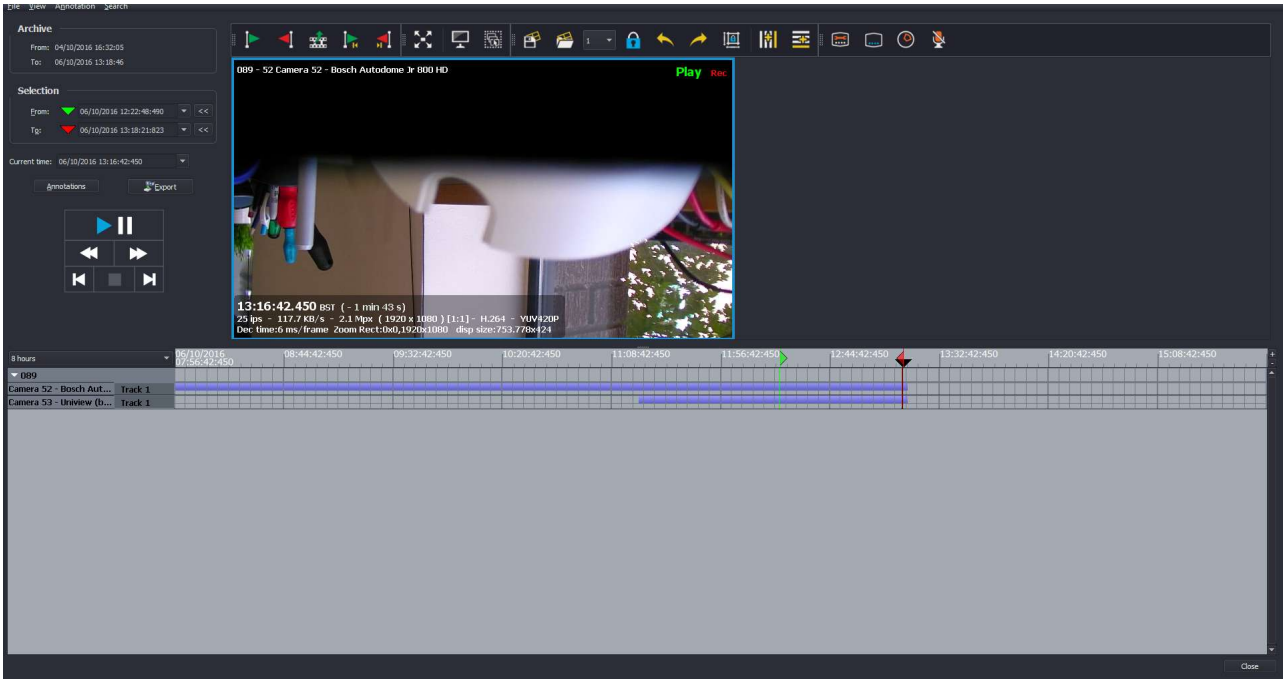


Figure 4.9: Clicking and Dragging Track on Timeline

- Double left–click the mouse on the horizontal bar associated with a track to show the associated Channel in the Display Area
- Hover the mouse over one of the horizontal bars to see the precise time at that point in the record–ings

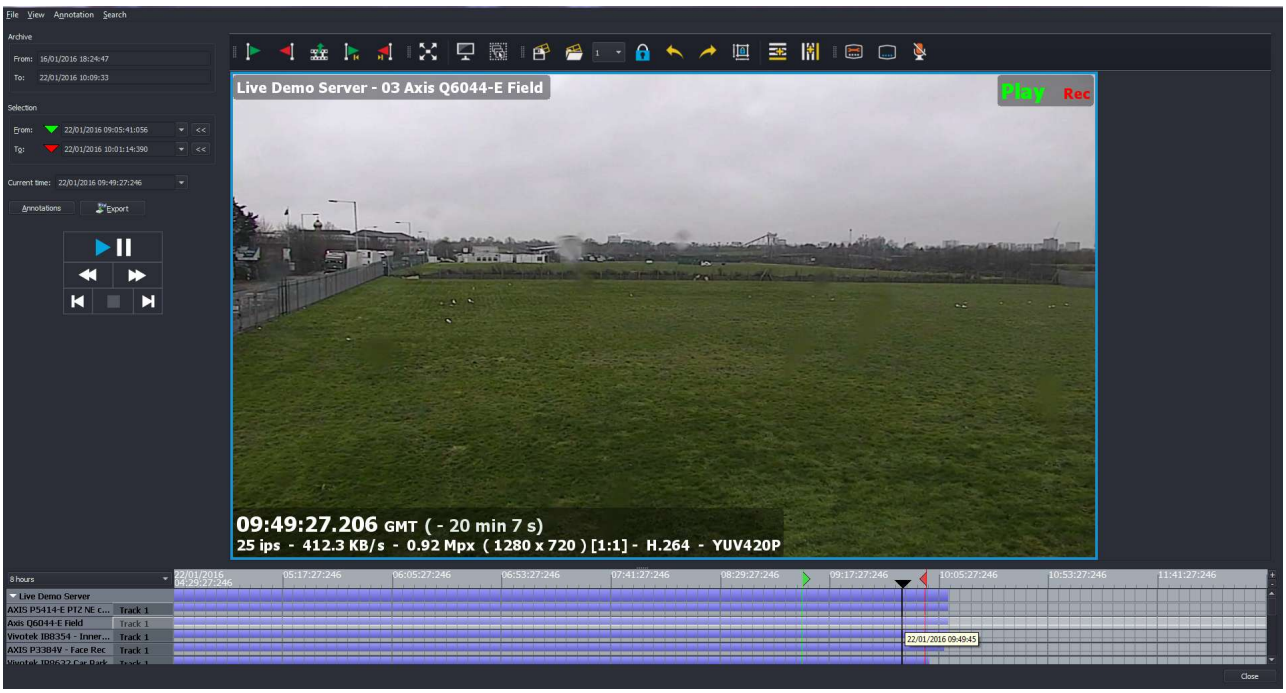


Figure 4.10: Time Display on Camera Channel Timeline

- Click the 'span' drop–down box to change the size of the timeline view; this allows a timeline of

varying durations (from 2 minutes up to 60 days) to be displayed. Alternatively, while hovered over the time ruler, use the mousewheel.

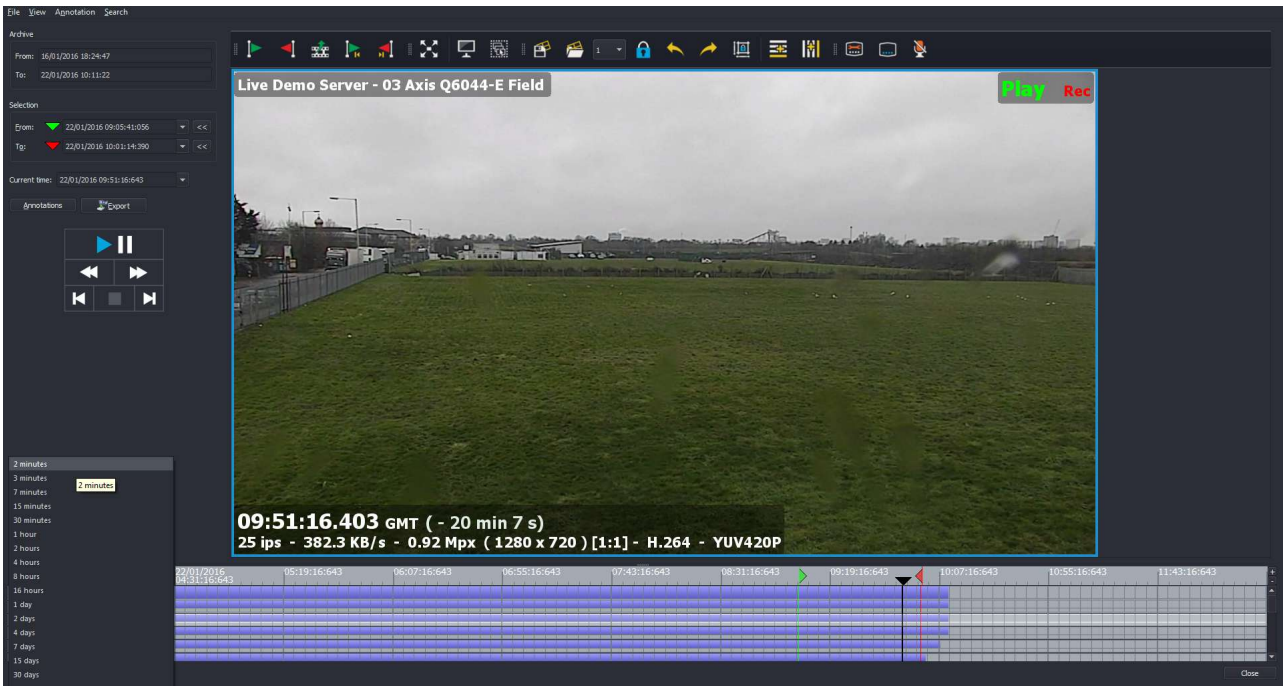


Figure 4.11: Find Screen Time Span menu

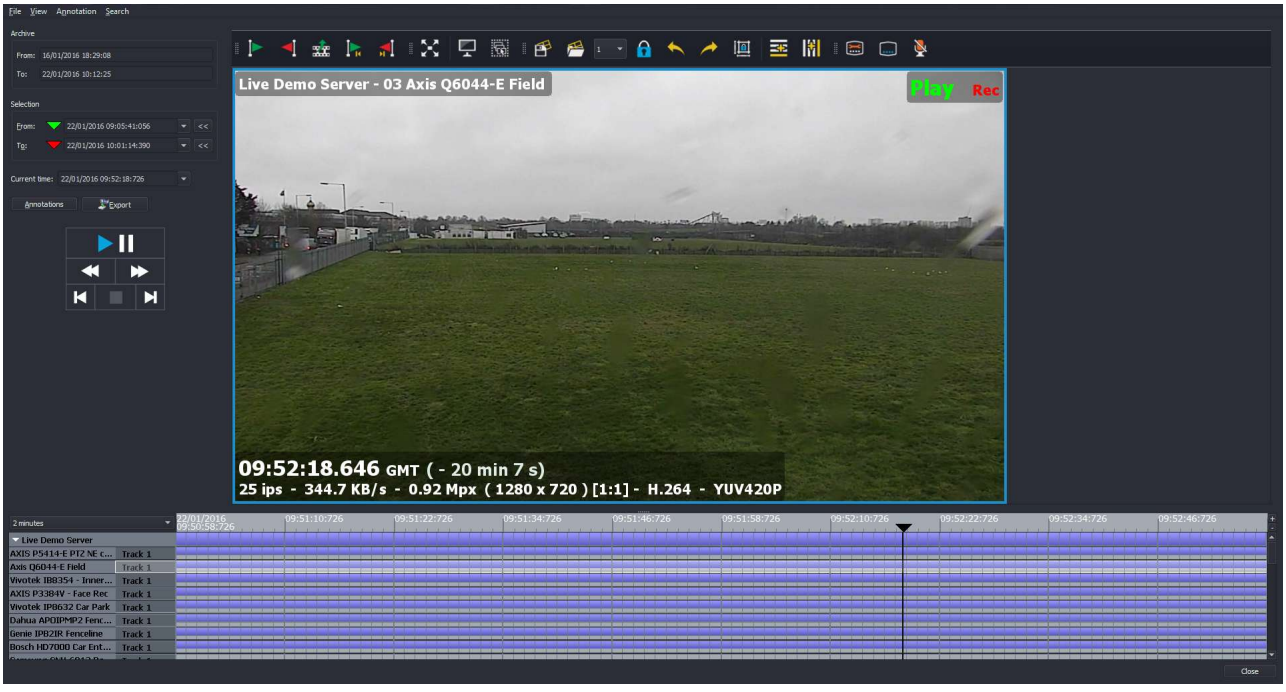


Figure 4.12: Find Screen Time Span reset to 2 minutes

4.4.2 Time Line Markers

The Find time line has 3 markers:

Figure 4.13: Time Line Markers

- 'Current position' marker (Black) – this indicates the current position in time that is being displayed on the video display; instead, click and drag the time line relative to this marker
- 'Start' and 'End' markers (Green/Red respectively) – these markers set the area of interest for creating exports, or searching the Event Track; click and drag to a required time using the mouse, or alternatively this can be set to the current time position being viewed by clicking on the « icon in the Selection submenu

4.5 Annotation

4.5.1 Creating an Annotation

The Annotation feature allows you to mark footage of interest, for quick recall at a later date.

To create Annotations for footage, or search for those previously created, first click on the 'Annotations' button to call up the Annotation Edit screen.

To create a note...

- Select the desired channel and associated record tracks
- Select the time range
- Check the 'Locked' box if you want to prevent the associated recordings from being overwritten.
- Enter some associated text
- Click 'OK'

The 'Lock' mechanism marks the associated recording region as being unavailable for overwriting. This is useful to preserve important incidents but be careful when using this feature, it means that less disk space is available for new recordings. If too many recording regions are locked, the desired recording duration may not be achieved.

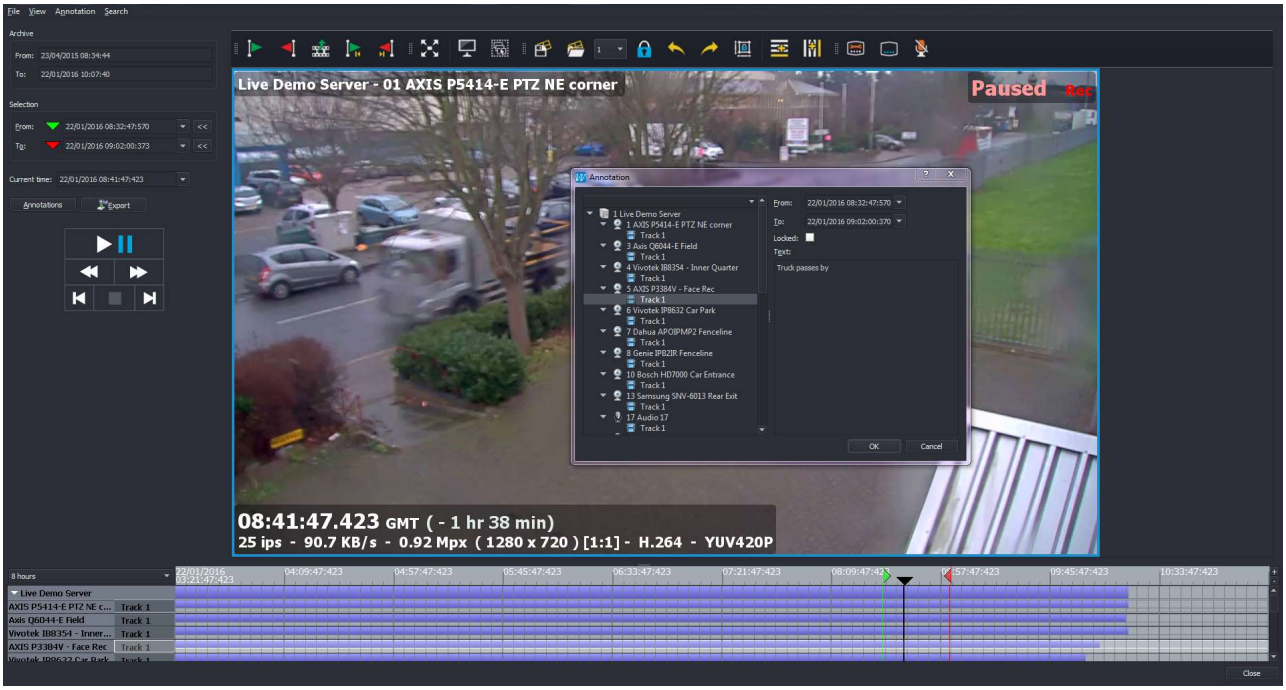


Figure 4.14: Annotation Menu

In the View menu, enable the 'Show Annotations' option, and the annotation will now be shown in yellow beneath the recording track.

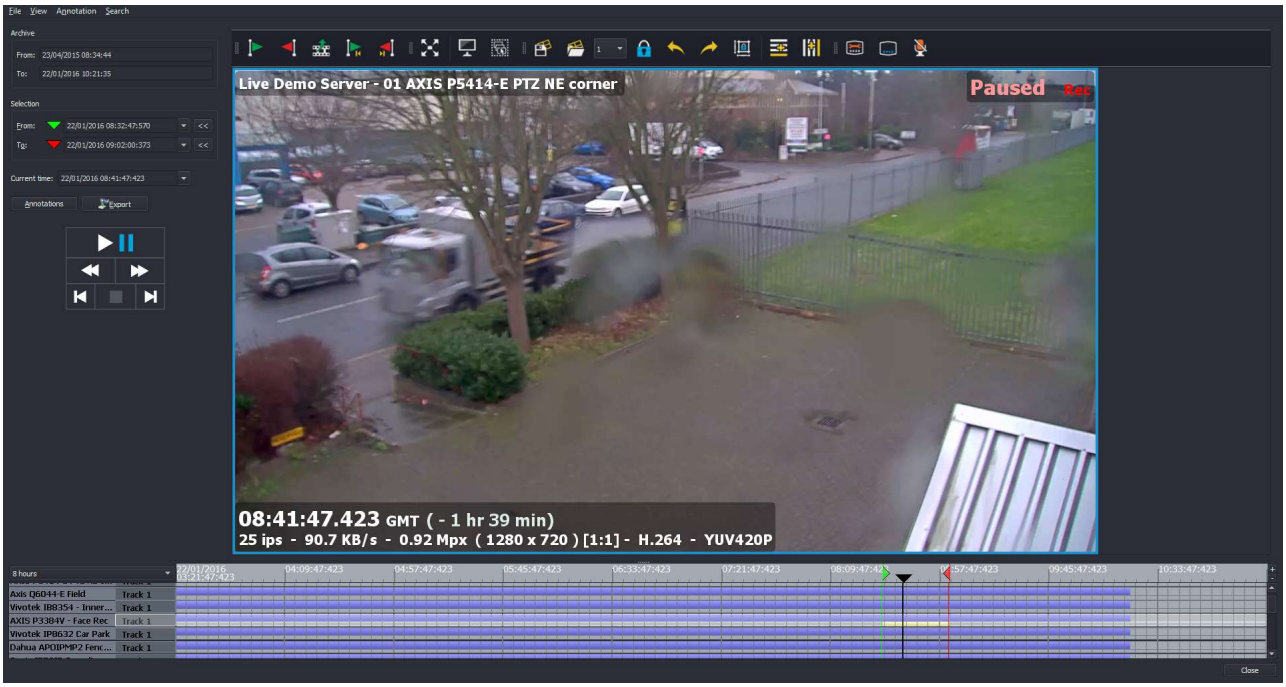


Figure 4.15: Annotation Track now visible

4.5.2 Working with Annotated footage

Follow the menu path Annotation → Edit and the Annotation Edit box will appear:

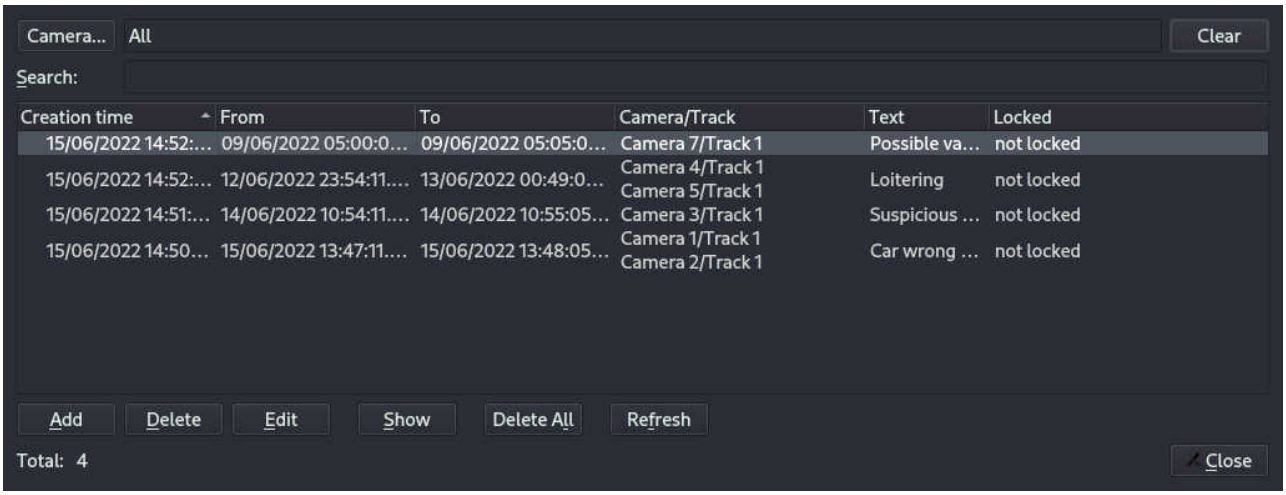


Figure 4.16: Annotation List

To edit an annotation, highlight an entry in the list and click 'Edit'. To playback annotated footage, you can highlight an entry from the list and click 'Show'.

Alternatively, we can carry out a search on the annotation text by entering '*searchterm*' in the Search field.

Click 'Enter' to generate a list of Search results:

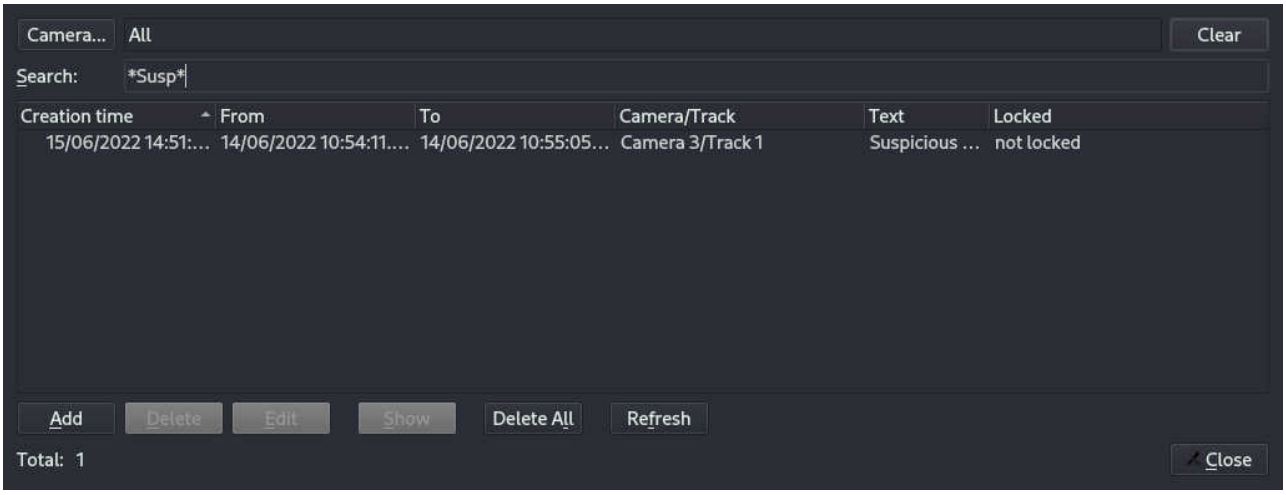


Figure 4.17: Annotation Search Results

By default, all cameras are shown and searched. It's possible to limit the search to a single camera. To do so, click the "Camera.." button and select the desired camera. To revert to searching all cameras, click the "Clear" button.

To delete an annotation, select the note of interest and click the 'Delete' button. Note that the 'locked region' associated with the annotation is automatically unlocked when the annotation is deleted.

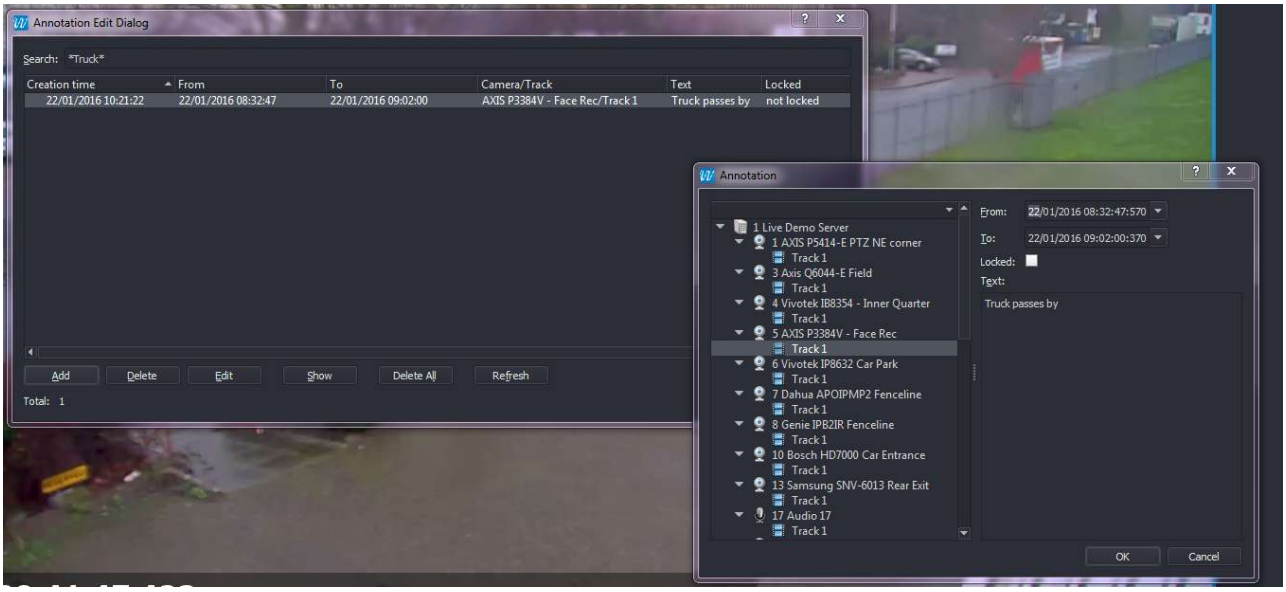


Figure 4.18: Find Screen Timeline Markers

4.6 Searching Events

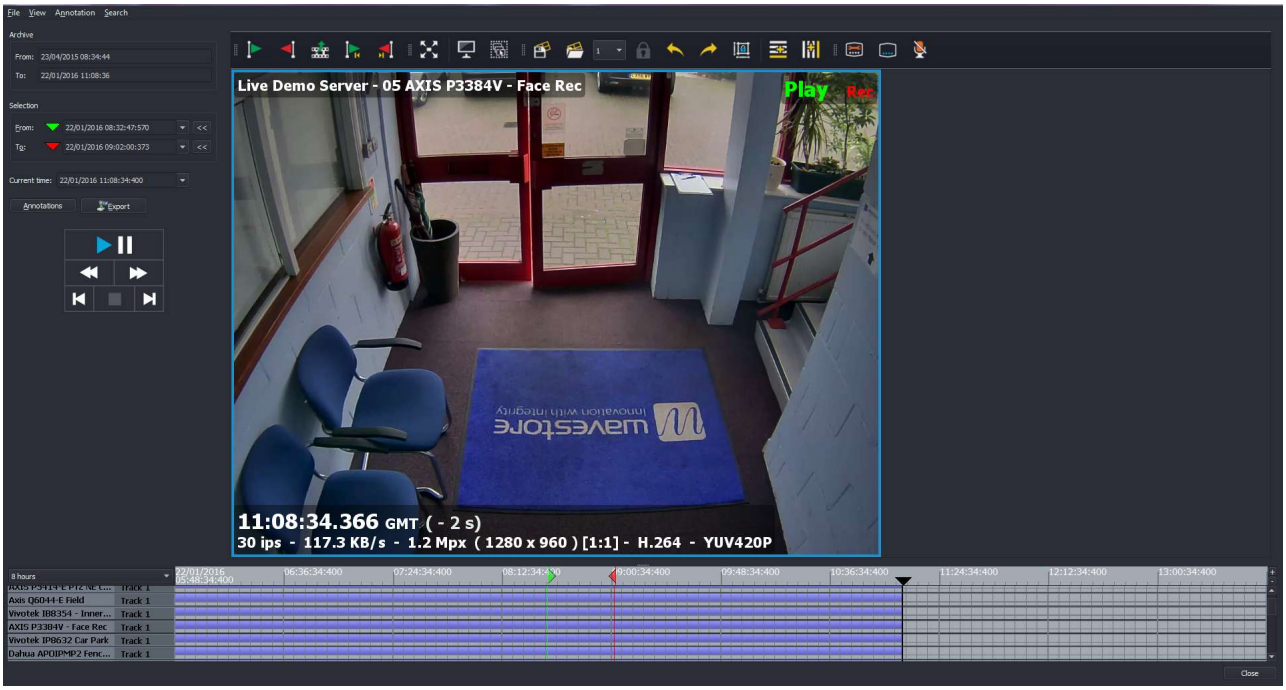


Figure 4.19: Find Screen

Follow the menu path Search → Events:

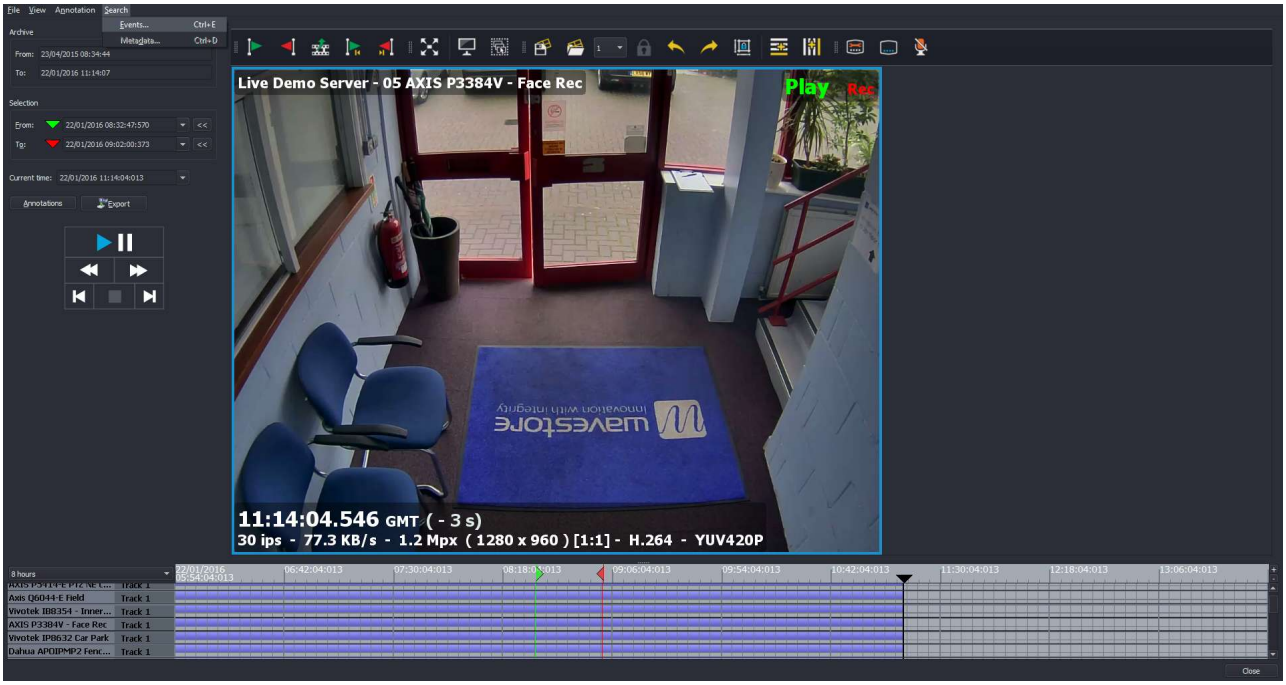


Figure 4.20: Find Screen Search Menu

The Event Search box will now appear:

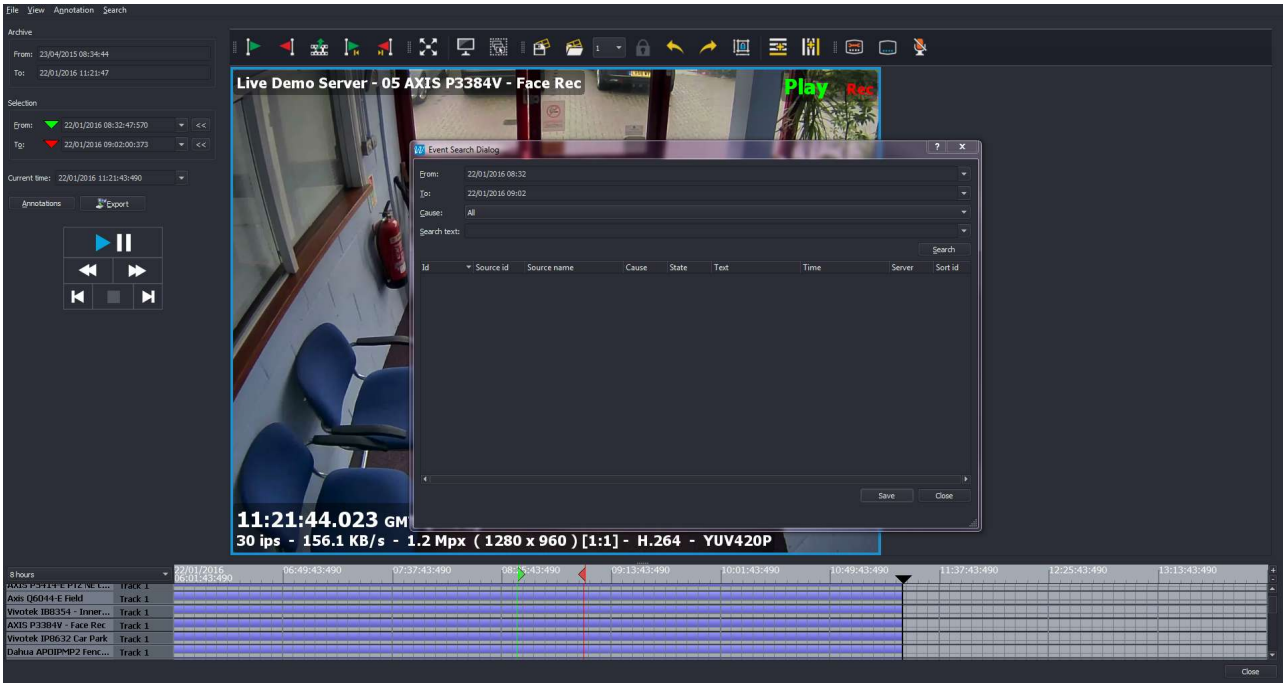


Figure 4.21: Find Screen Event Search Box

Configure the parameters for your search (Time Range/Event Type). Note that, although seconds are not shown, they are assumed to be zero, e.g. "13:00" is really "13:00:00".

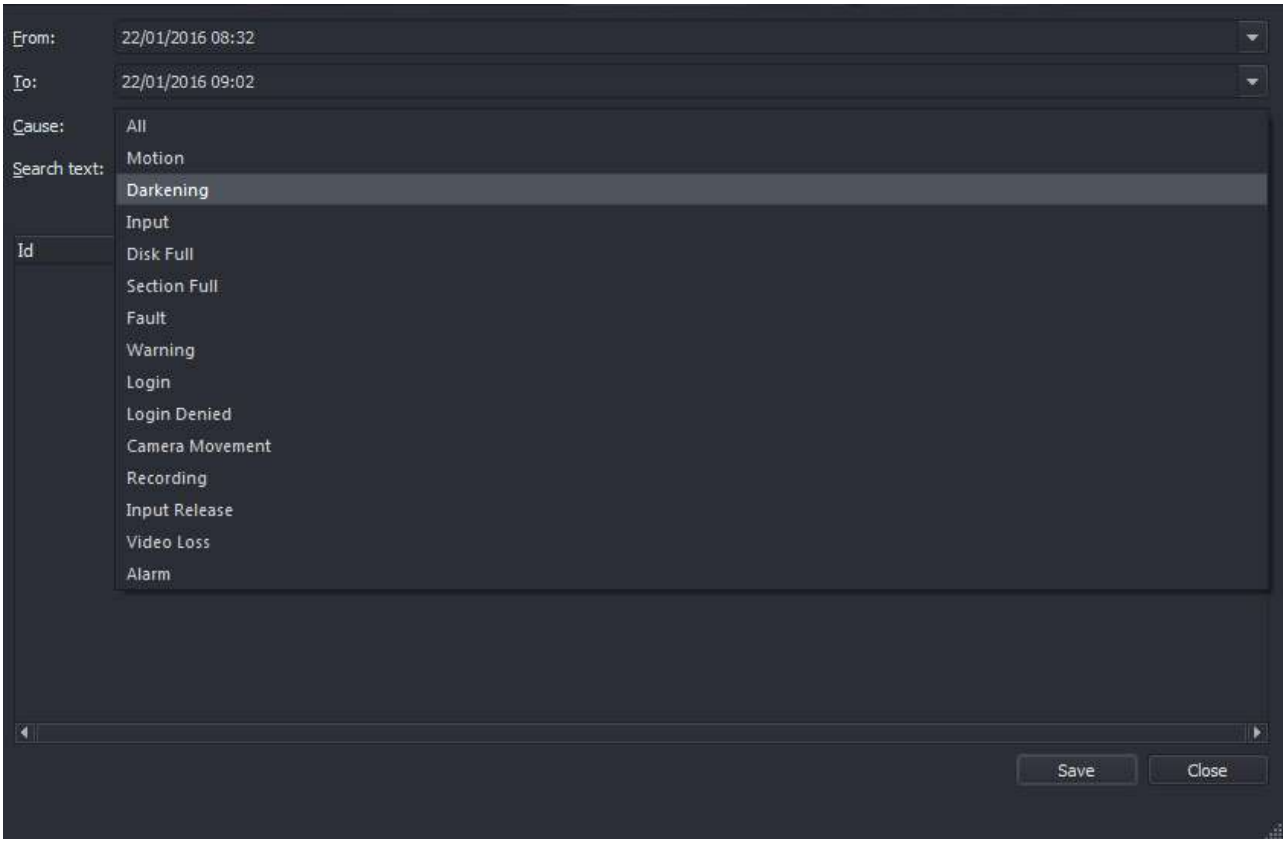


Figure 4.22: Configuring Search parameters

You can configure the Search results box to display that data that you're most interested in (right click on the column headings to display the toggle options):

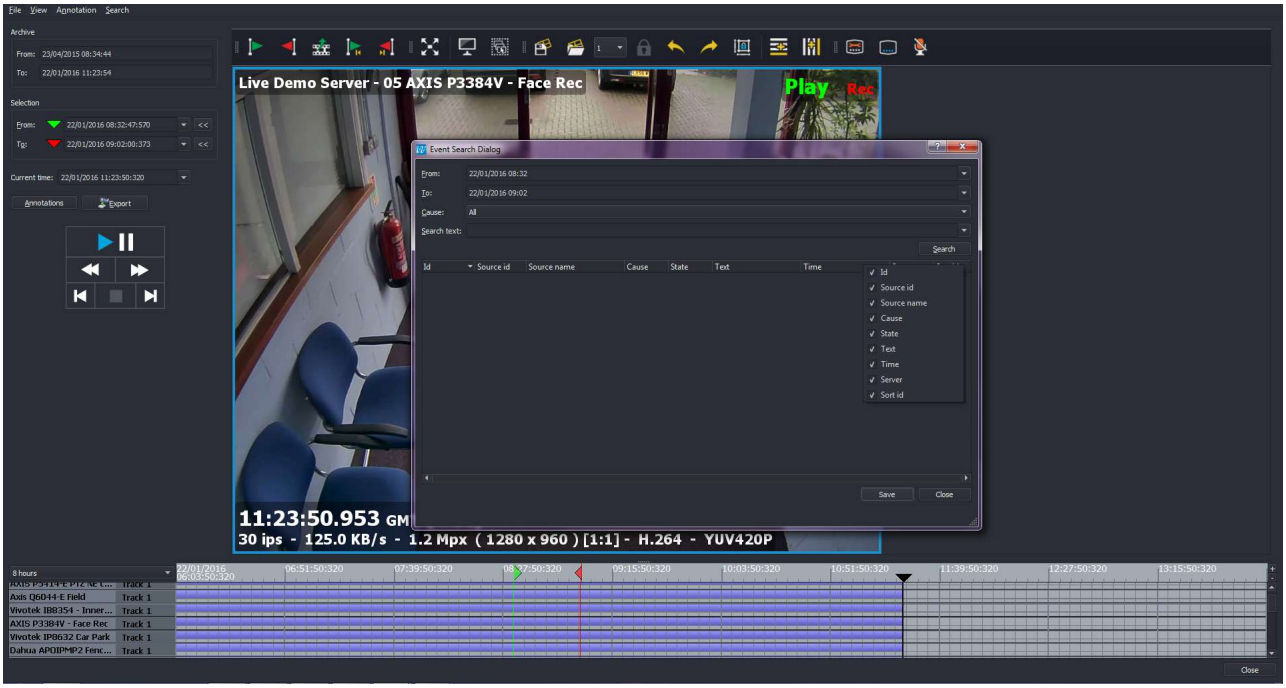


Figure 4.23: Configuring display of Search results

Click on Search and your results will be displayed.

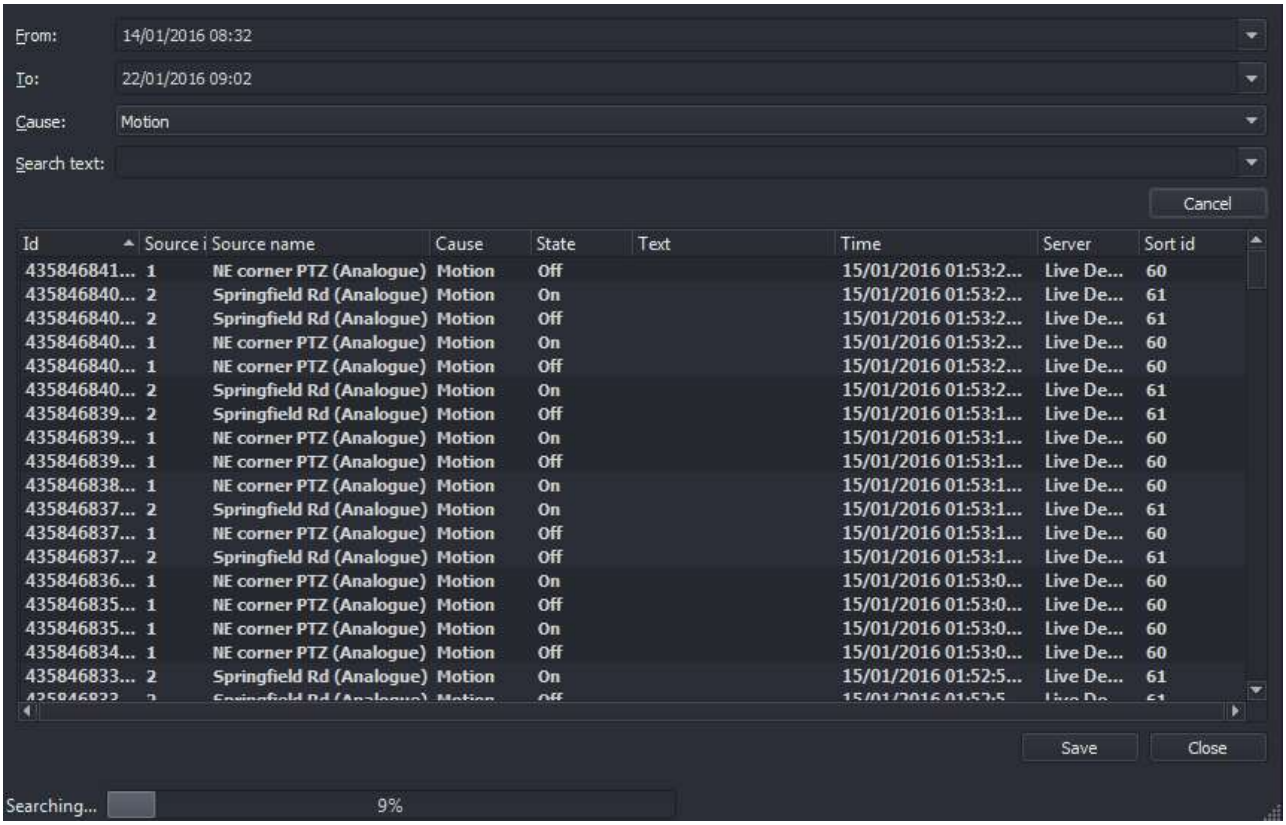


Figure 4.24: Search Results

Double click on a Search result to playback that event, or right to display other options (e.g. Export).

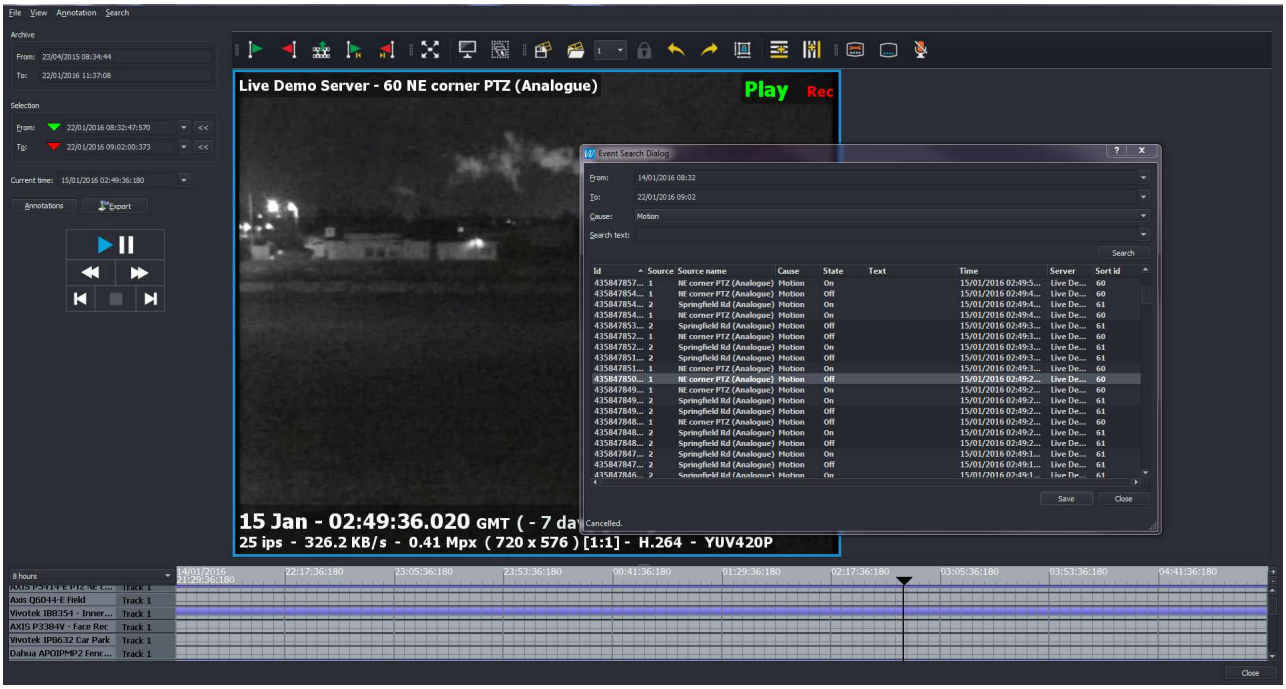


Figure 4.25: Playback of Event

4.7 Searching Metadata

Follow menu path Search → Metadata, and the Find Meta screen will open:

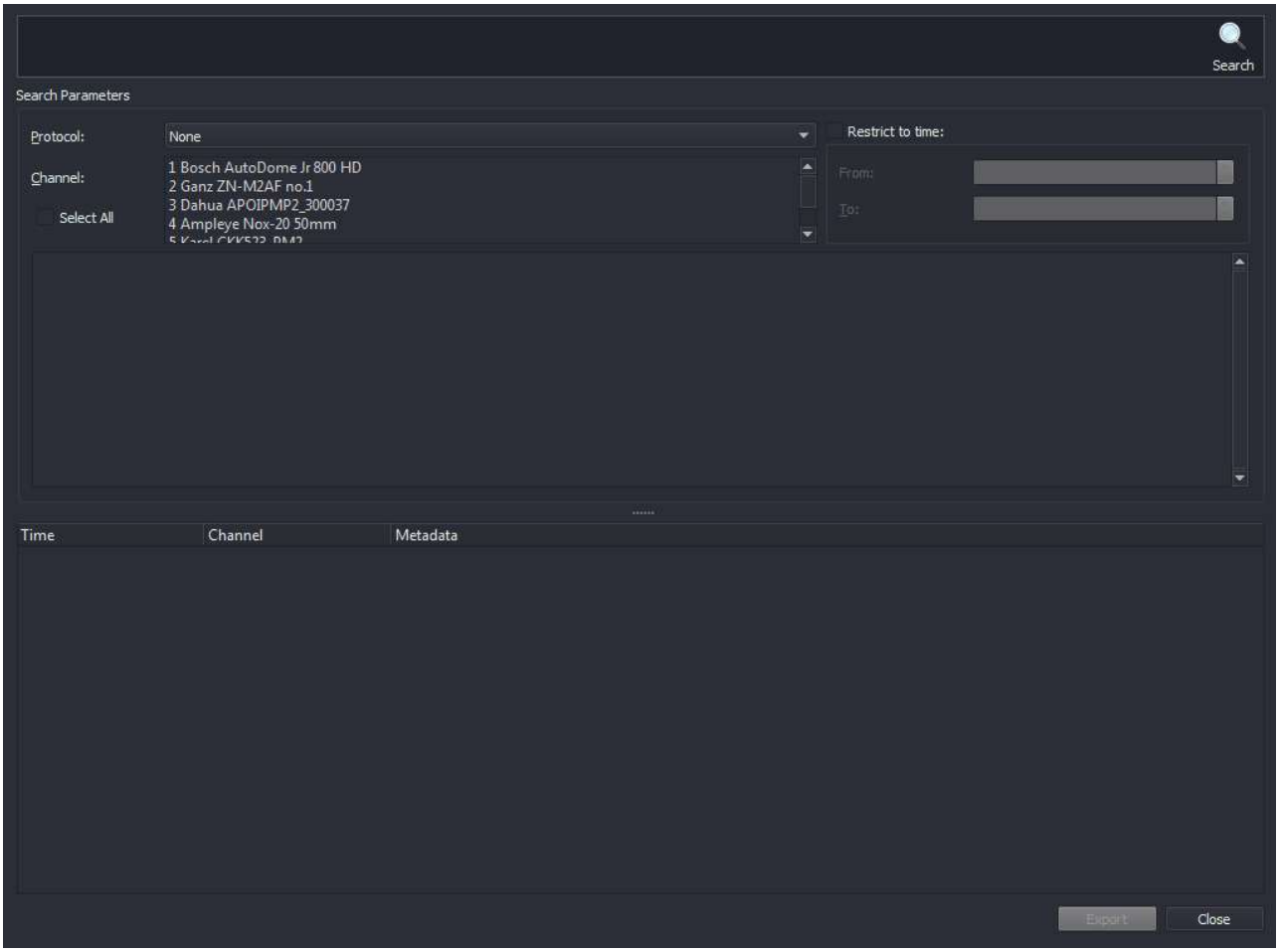


Figure 4.26: Metadata box

Enter the From and To times for your search, the text that you wish to search for, the associated channel (if applicable), and then click Search. In the example below, we'll search for POS transactions involving Crew ID '47' on the camera channel 'Checkout 2'.

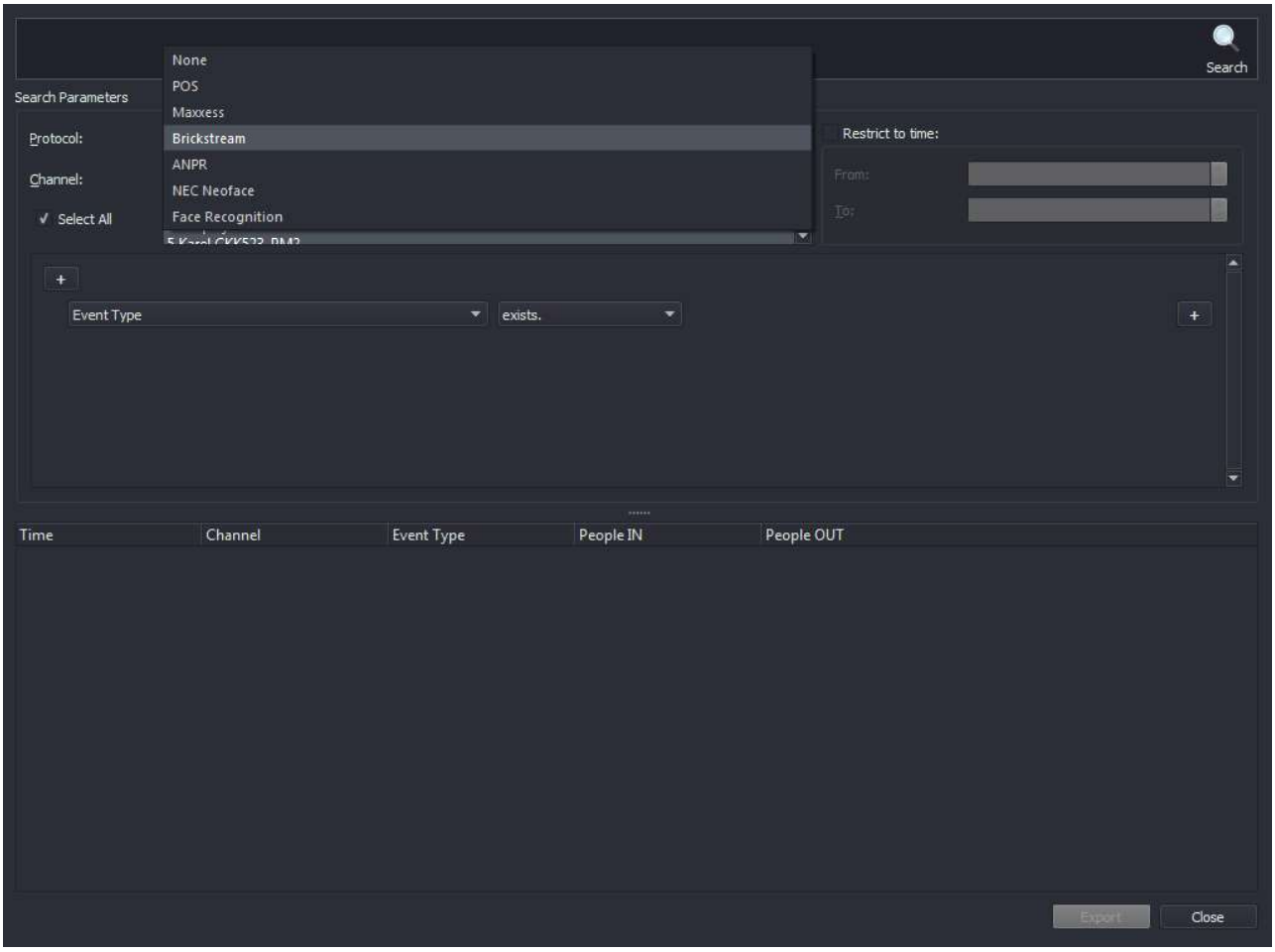


Figure 4.27: Entering Metadata search details

Click 'Search', and a list of results will now be generated:

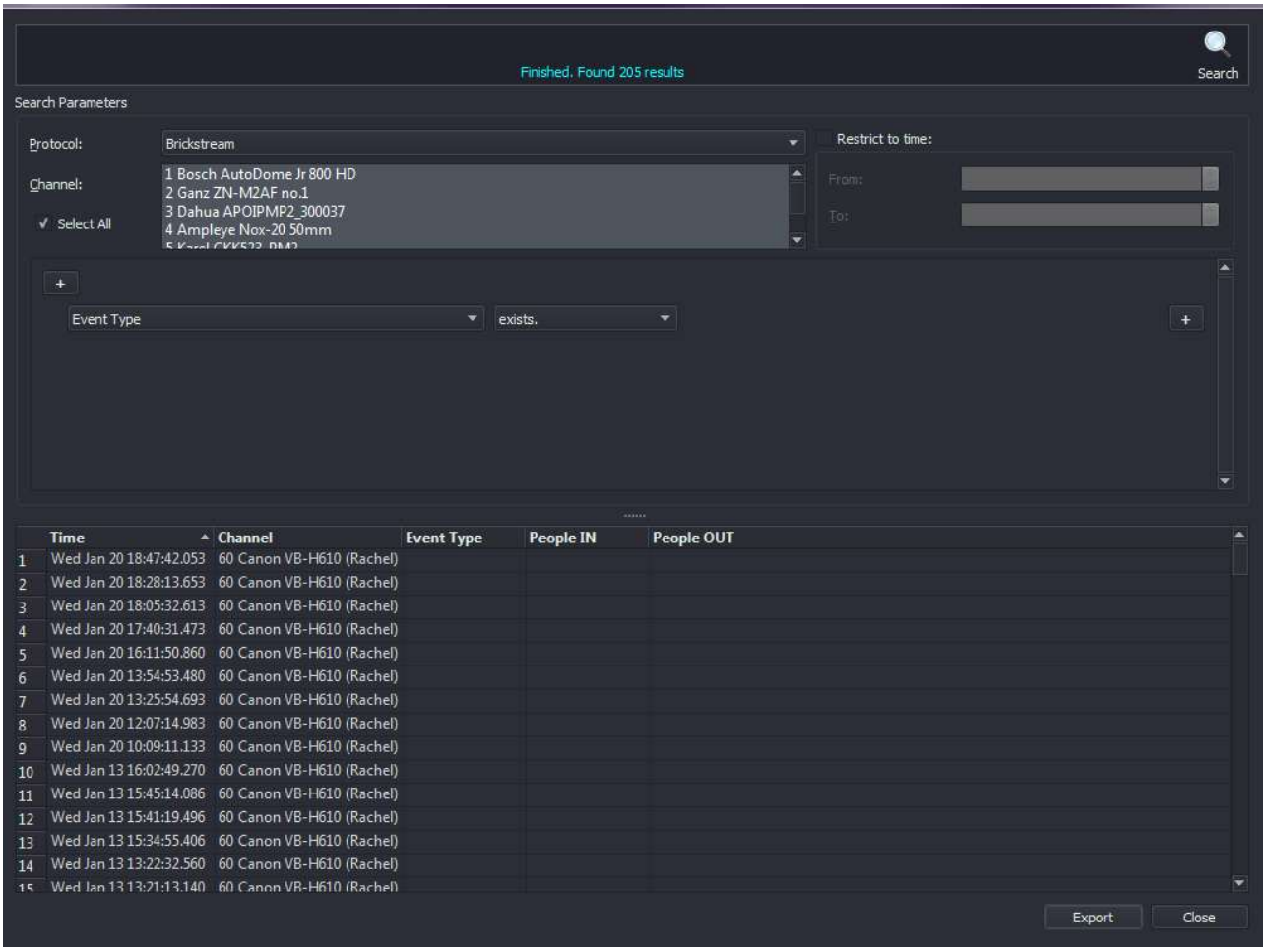


Figure 4.28: Metadata search results

This list of results can be exported as a CSV file by clicking the 'Export' button, and browsing to your desired location.

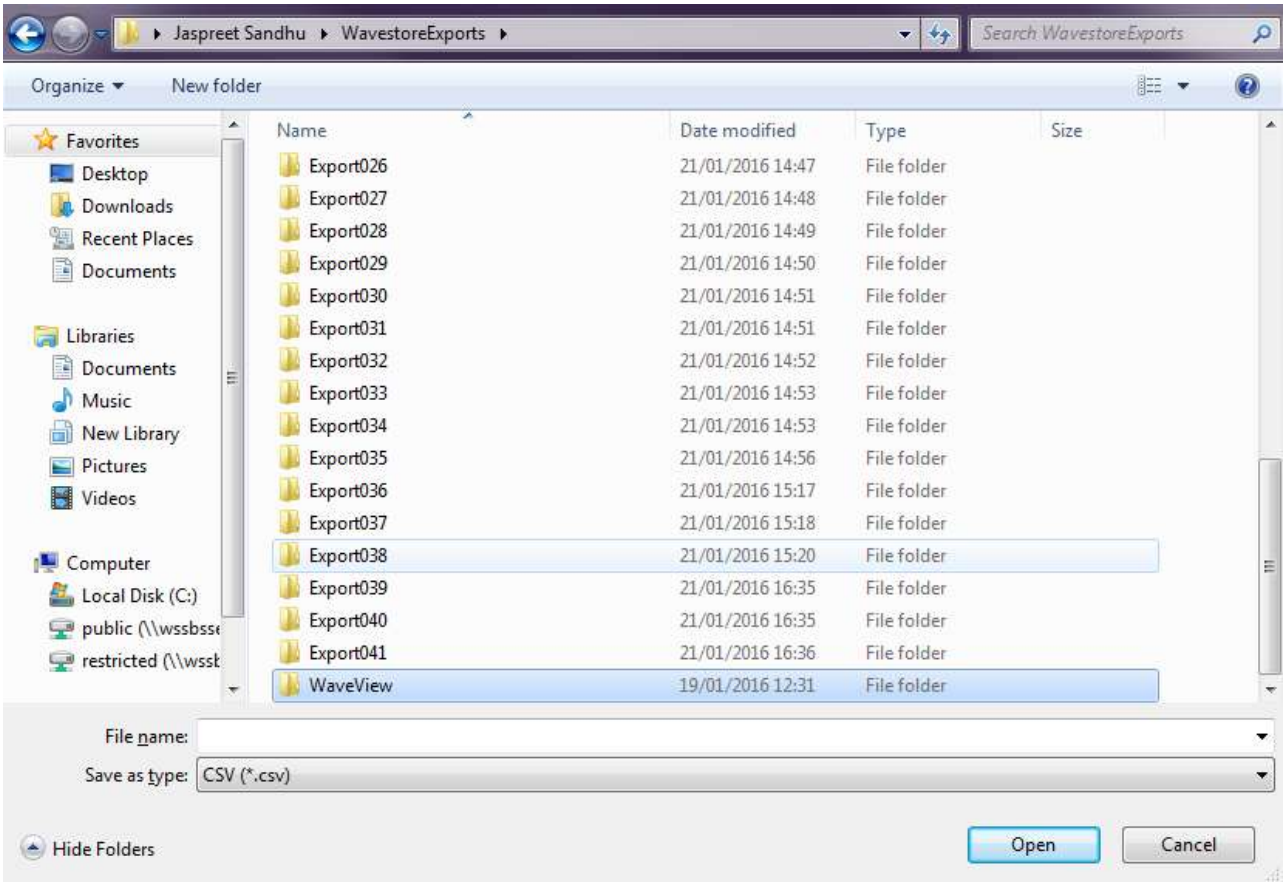


Figure 4.29: Saving Metadata search results

4.8 Smart Search

Wavestore has a facility to perform a post–recording search of a period of recordings based upon motion. See section 9.8 – Configuring Smart Search for information on how to configure cameras for Smart Search. This section documents how to perform the Smart Search, assuming the cameras have been appropriately configured.

Performing the Search

Performing the search consists of the following steps:

- Selecting the desired date/time range
- Selecting the desired cameras
- Drawing a mask (area of interest) for each selected camera
- Setting the desired search sensitivity for each selected camera

To select the desired range, either drag the red and green vertical bars on the timeline, or use the "Selection" widgets in the side–pane. This is described in more detail in section 4.2.2 – Selection Range.

To select the desired cameras, hold the CTRL key and click on the horizontal tracks in the timeline. If multiple recording tracks are enabled for each camera, only one needs to be selected.

Now click the "Smart Search" button to move to the next step.

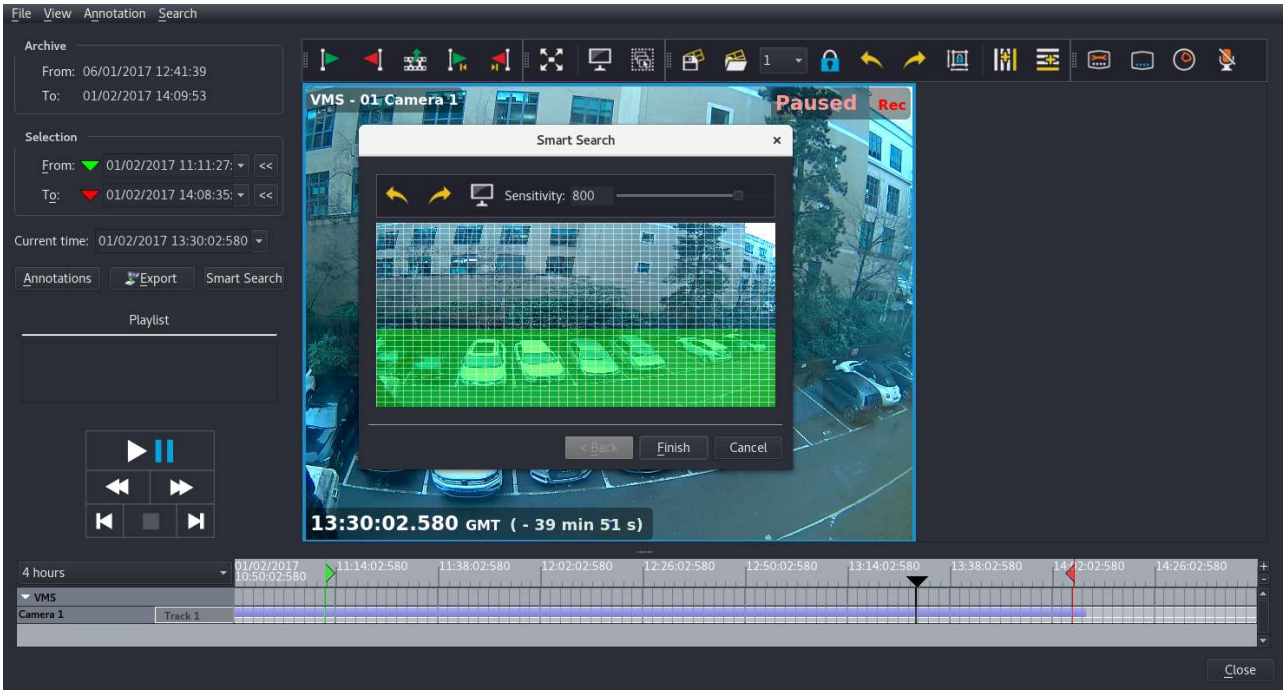


Figure 4.30: Export selection

The Smart Search window will appear with a grid displayed over a snapshot of the current camera's live image. Draw a mask on the image by clicking the left mouse button and dragging the desired area. The green highlighted area is the area which will be searched.

Use the slider to adjust the sensitivity.

If multiple cameras were selected, click Next to go to the next camera and set up another mask and sensitivity. Otherwise, the "Next" button will become a "Finish" button, which initiates the search.

Using the Search Results

Once the search is complete, the areas of motion will be highlighted in pink on the timeline, and a playlist of periods of motion will appear in the side pane.

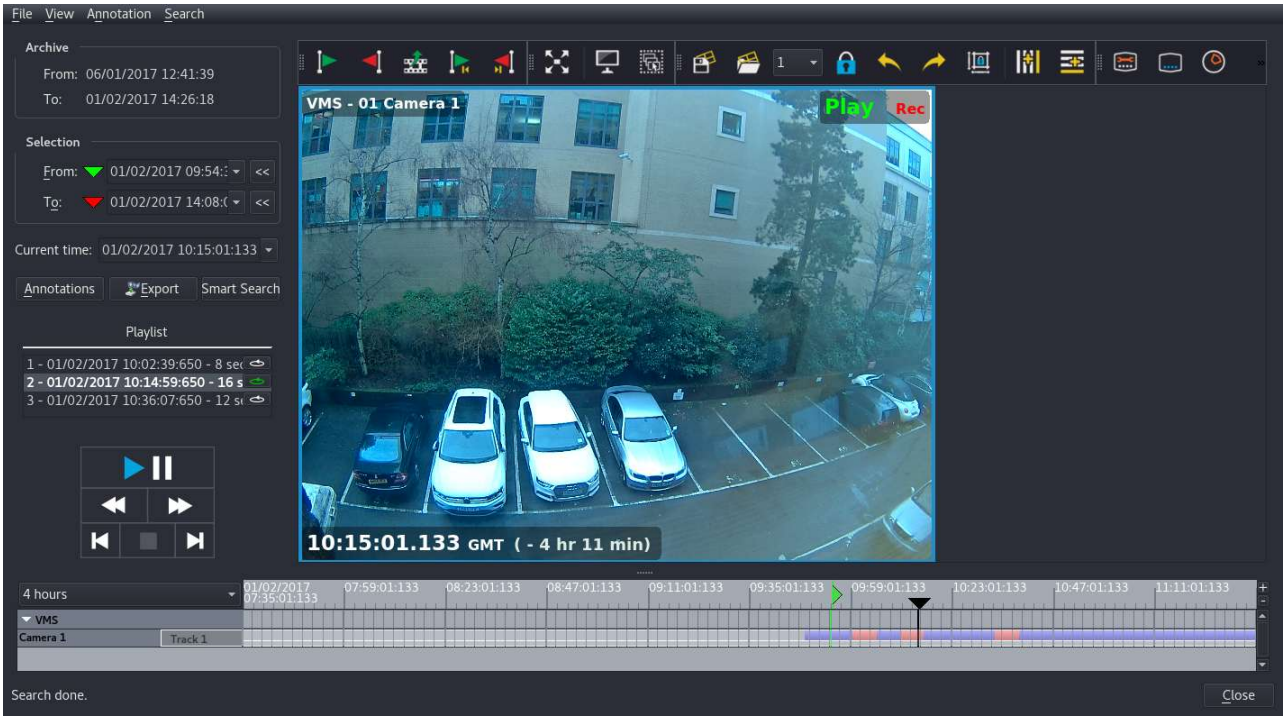


Figure 4.31: Smart Search Results

The playlist allows skipping between areas of motion, by double–clicking the desired item. Each item can be put in a loop by clicking the loop icon next to the playlist item.

Note that the camera(s) displayed are not dependent on the search results. So it is possible to perform a search on one camera, then view the periods of motion on a different camera, or several cameras.

The playlist and areas of motion are cleared either when a new search is performed, or when the Find screen is closed.

4.9 Exports

Please note that if you are saving an export to a DVD/USB device directly on the server itself, you must first 'mount' the device on the server before proceeding with the export, this process is fully described in section 4.9.3 – Exporting directly to DVD from Wavestore Server and section 9.17 – Accessing a USB disk on the Wavestore server.

Please note that the permissions of the user making the export may conditionally limit the functionality of the exported data. For example, if the current user does not have permission to make transcoded exports (e.g. converting to AVI), any WSB export made by that user will contain that permission setting, meaning that the resulting WSB export cannot be subsequently converted to another format. This design is intentional, to prevent a possible workaround where a user could make an AVI by first creating a WSB export then opening the export and converting it to AVI.

If there is a critical need to override these settings, staff at Wavestore Limited can do so, but it is not trivial and a fee may be charged.

4.9.1 Exporting footage to a Windows PC running WaveView client software

The Wavestore server can directly export footage to a DVD or USB device, or over a network connection to a PC.

Footage can be exported in a variety of formats; the Wavestore Native format (.WSB) is supported as standard, and an optional licensed upgrade offers transcoding options to other formats such as .AVI and .WMV.

Wavestore Native format is the recommended choice for exports, and provides support for both encryption and image authentication.

To create an Export, we must first select the Export start and end times.

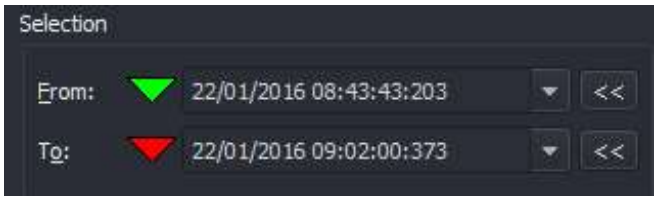


Figure 4.32: Export selection

This can be carried out either by clicking and dragging the Search timelines to set the red/green 'Start' and 'End' markers (click the '«' icon when the timeline is positioned on the desired time in each case), or by entering text in the Selection 'Start' and 'End' boxes, to set the required date and time for precisely.

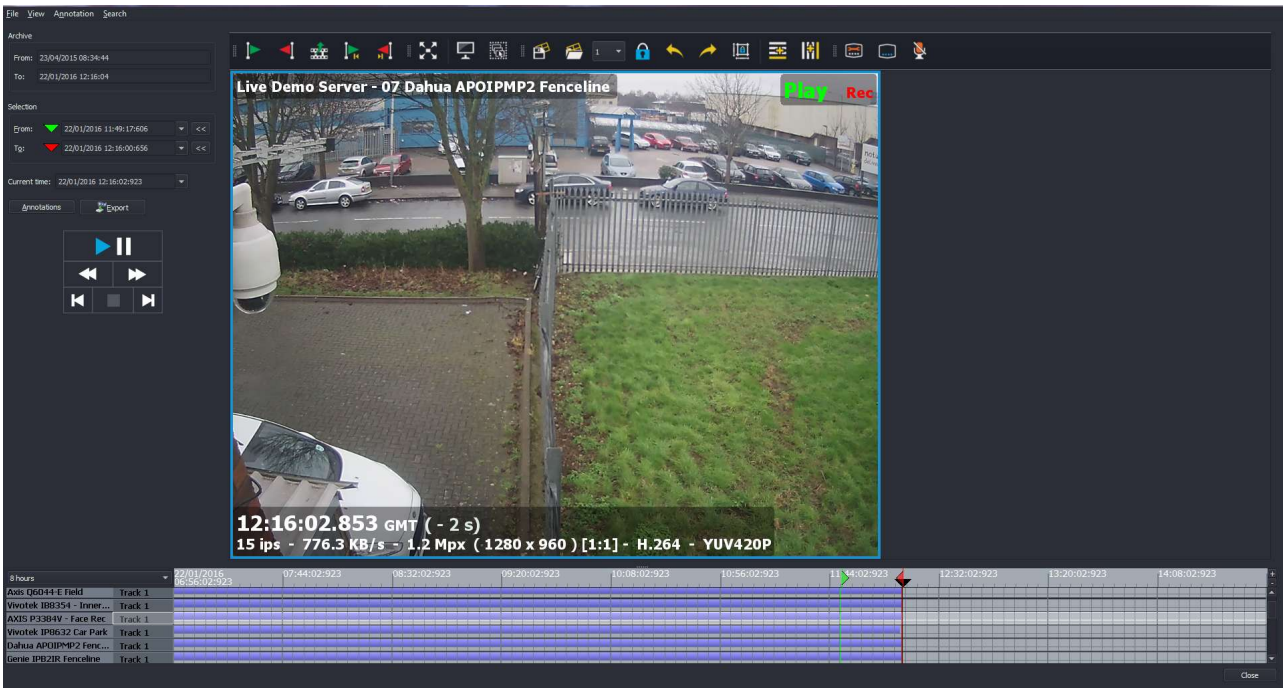


Figure 4.33: Find Screen Timeline Markers

To select an audio/video channel, left-click on the timeline bar corresponding to that device. To select

multiple cameras, hold down the 'CTRL' key and left click the required camera channels of choice to add/remove them from the current selection (selected cameras will be highlighted white).

Once the selection has been made, click the 'Export' button to open the Export Screen.

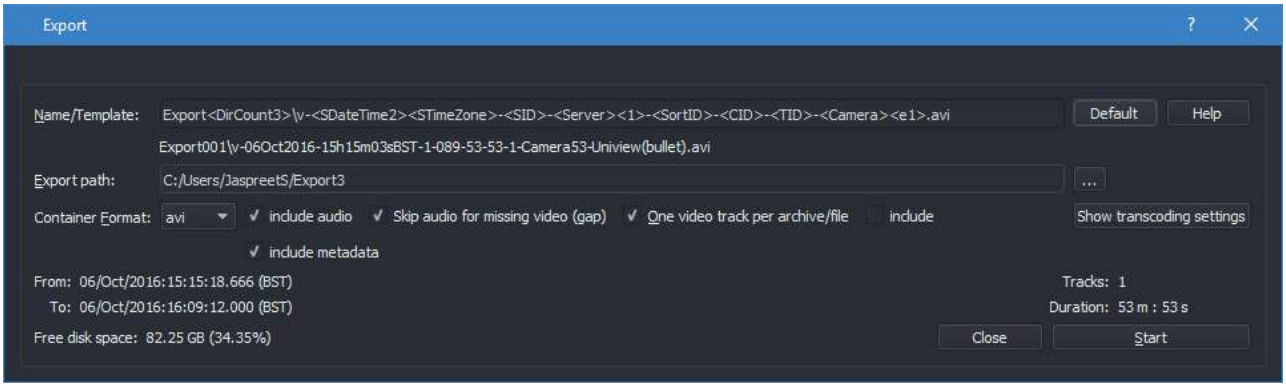


Figure 4.34: Export Screen for .WSB export

The export screen offers a number of configurable selection options:

Name/Template Allows an export name or template to be specified

Export Path The folder or directory into which the export file(s) will be saved – please note that if you are saving an export to a DVD/USB device directly on the server itself, you must first 'mount' the device on the server. Once you have saved the file, you must then 'eject' the device before it can be removed. The procedure for this is described in section 4.9.3 – Exporting directly to DVD from Wavestore Server.

Container Format format to be used for the download e.g. AVI, WMV, WSB (native Wavestore format)

Include Audio Selects whether audio should be included if any audio channel is associated with the selected video channels.

- Skip audio for missing video toggle option
- One video track per archive/file – Chooses whether tracks should be merged as a single file or exported as individual files. Note that using this option means that only one camera can be viewed at a time later.
- Include WaveView playback software toggle option
- Keep/Remove Encryption – in the event that the downloaded channel has been configured with encryption active
- (Re)encrypt with password – restricts access to the export through use of user configurable password (you'll be prompted to enter a password when this option is selected)

If your client installation is licensed with the transcoding option, you can select an alternative export format (e.g. AVI).

Once you have selected the format, select 'Show Transcoding Settings', and the screen shown below will appear allowing you to select transcoding options as you require:

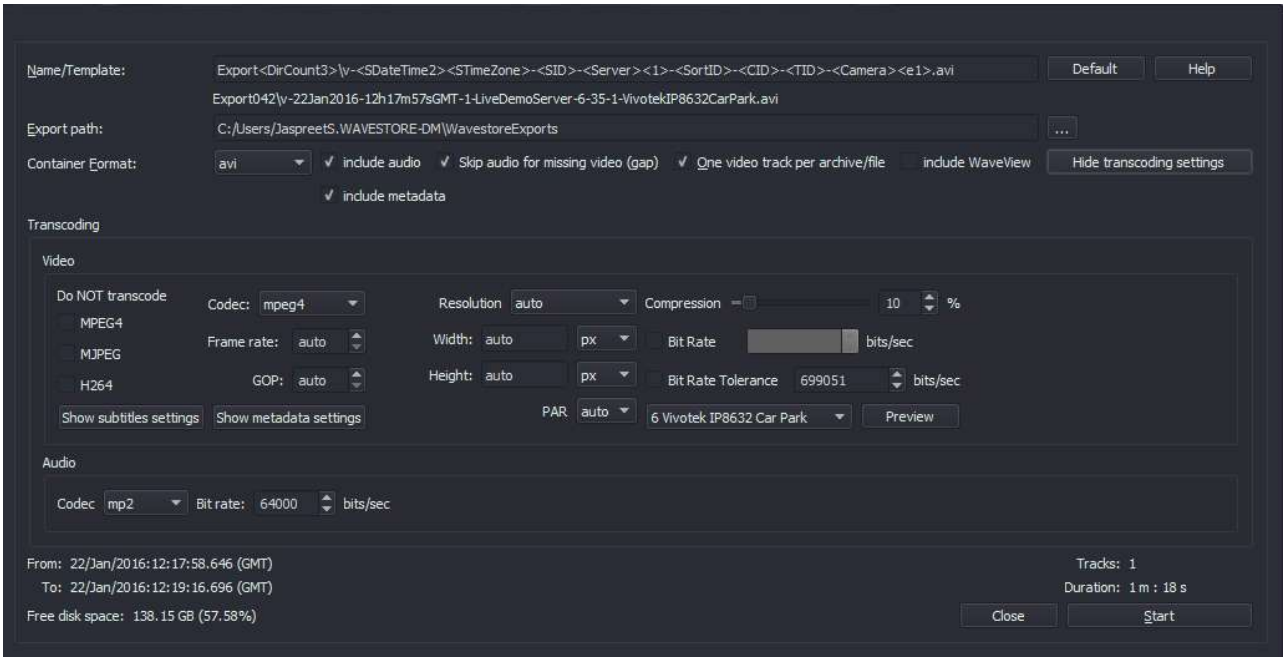


Figure 4.35: Export Screen showing options for Transcoding

Some points to note:

- When creating an export using AVI container format, selecting the 'Do NOT Transcode' option (Video submenu in Transcoding section) for the footage type(s) that you are downloading (MPEG4, MJPEG or H.264) will result in higher image quality.
- Certain codecs impose limitations on footage that has been recorded at a low frame rate; in this case you should select the WMV container
- Variable framerates are not supported so, if the source video has varying framerates, the resulting export may appear to speed up and slow down.
- Compression or Bit Rate can be set manually if required, based on the following: Bit Rate = (Compression/100) x W x H x BPP (Bits per Pixel) x Frame Rate Where BPP = YUV420 : 12 and YUV422 : 16 Bit Rate Tolerance = Bit Rate/4

Subtitles on the export can be configured as you require by clicking on 'Show Subtitles Settings', and then configuring as you need:

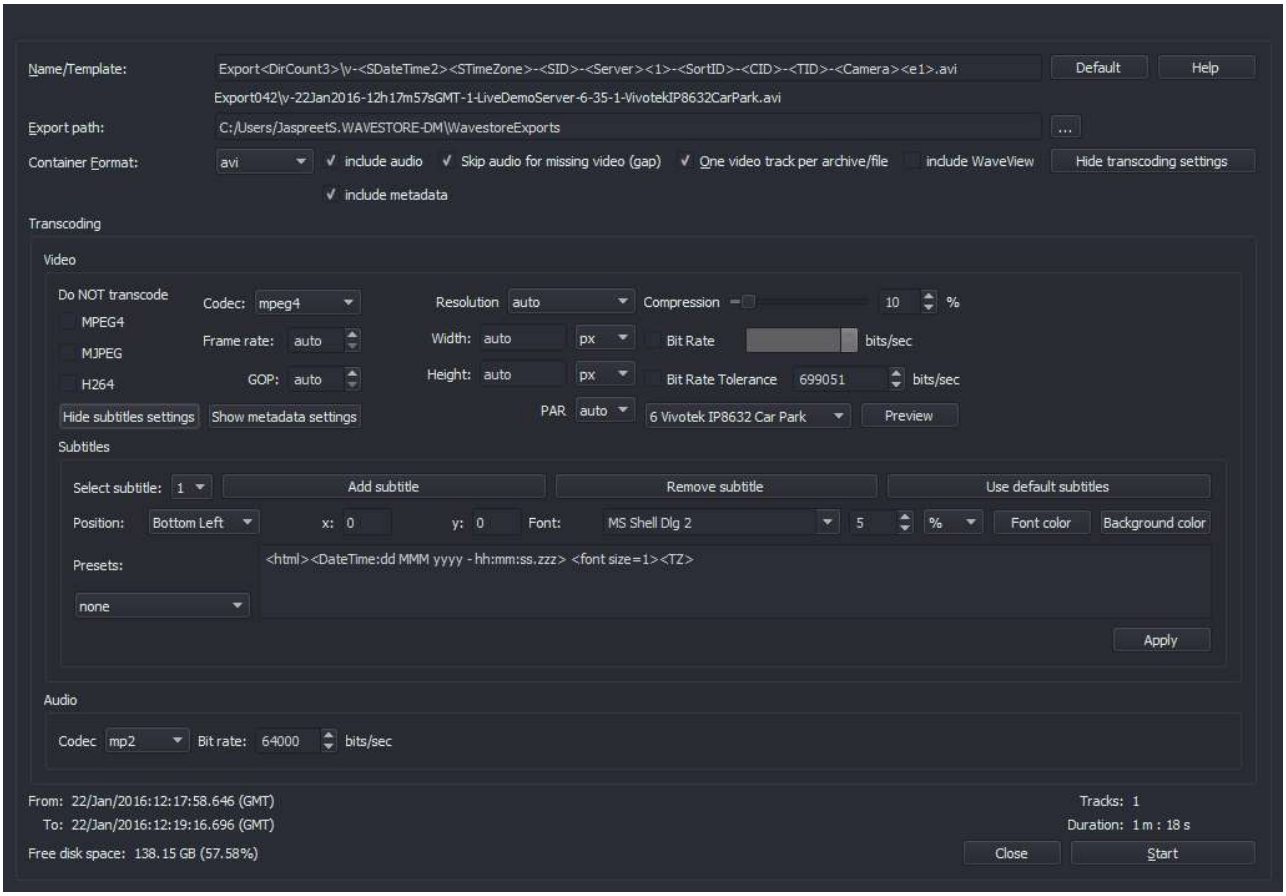


Figure 4.36: Export Screen showing Transcoding and Subtitle settings

Some experimentation may be required to optimise the size of the subtitles in the export; this can be configured in the Font Size setting (Subtitles submenu)

If the export operation is being carried out from a remote location using WaveView client software, then footage can only be saved either to the hard disk of the PC, or to a connected USB device.

It is then possible to burn the export file to CD/DVD, by using standard CD/DVD burning software (e.g. Nero/Roxio) to copy the archive directory.

Browse to your desired Export Path by clicking on the '...' button, and then select your desired Container Format.

Finally click 'Start'; the progress bar will fill during the export, with an acknowledgement message displayed once the export is completed.

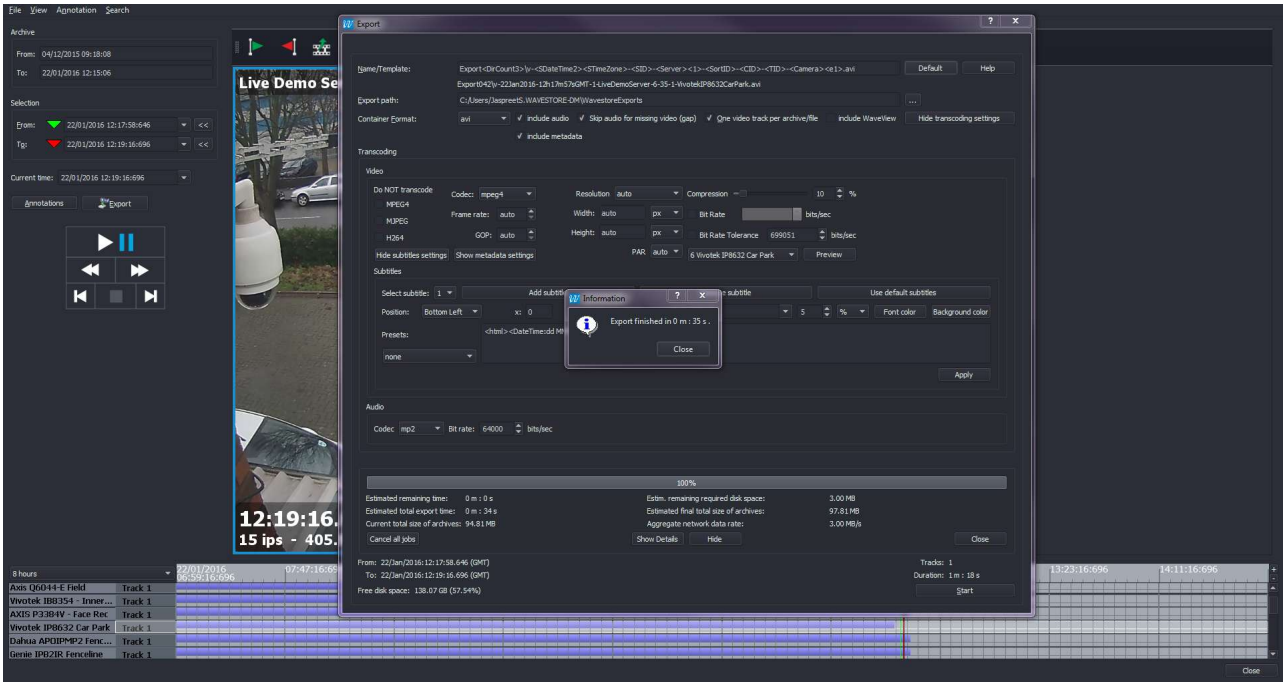


Figure 4.37: Export completion message

Section 8 gives details on how to playback exported files using a PC.

4.9.2 Exporting still images to a Windows PC running WaveView client software

Single still images can be backed up from the server as follows:

- Select your desired channel for playback by double clicking on the timeline for that channel
- Pause playback using the playback controls
- Clicking on the Snapshot button on the Video Toolbar calls up the Snapshot screen

We are able to carry out image manipulation/editing in the Snapshot screen as required (full details in section 3.6.2.1 – Snapshot Window).

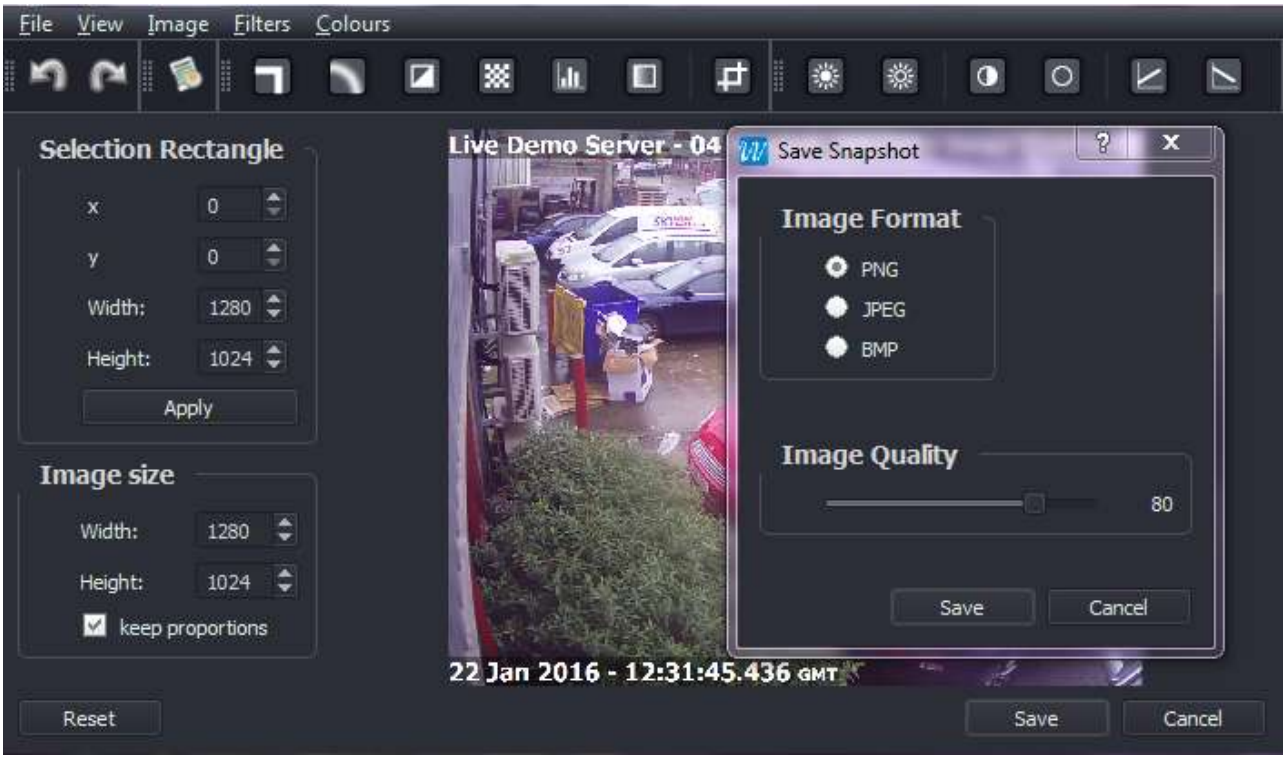


Figure 4.38: Still Image Export

Finally we can save the image to a storage device, once we have selected a save path and file name.

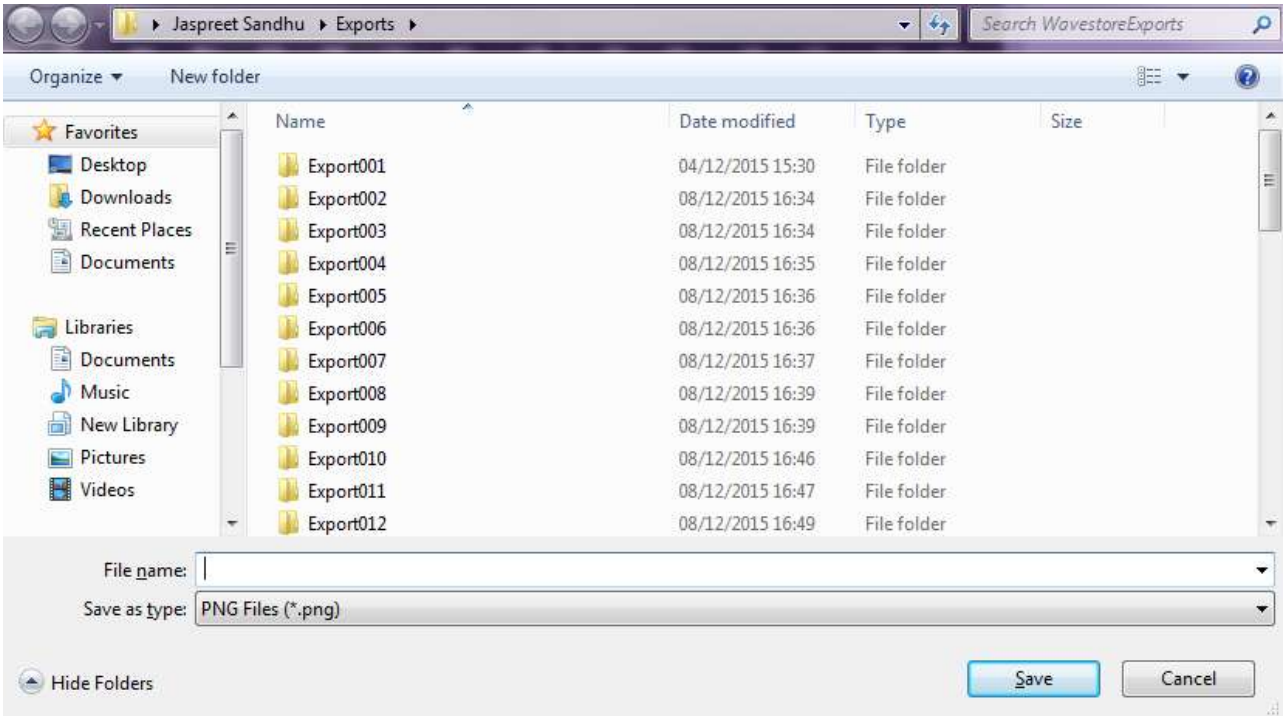


Figure 4.39: Still Image Export

4.9.3 Exporting directly to DVD from Wavestore Server

- Follow the menu path View → Find to access the Find Screen, and configure the required Camera, Start and Stop times as described in section 4.9.1 – Exporting footage to a Windows PC running WaveView client software; for Still Images refer to section 4.9.2 – Exporting still images to a Windows PC running WaveView client software.

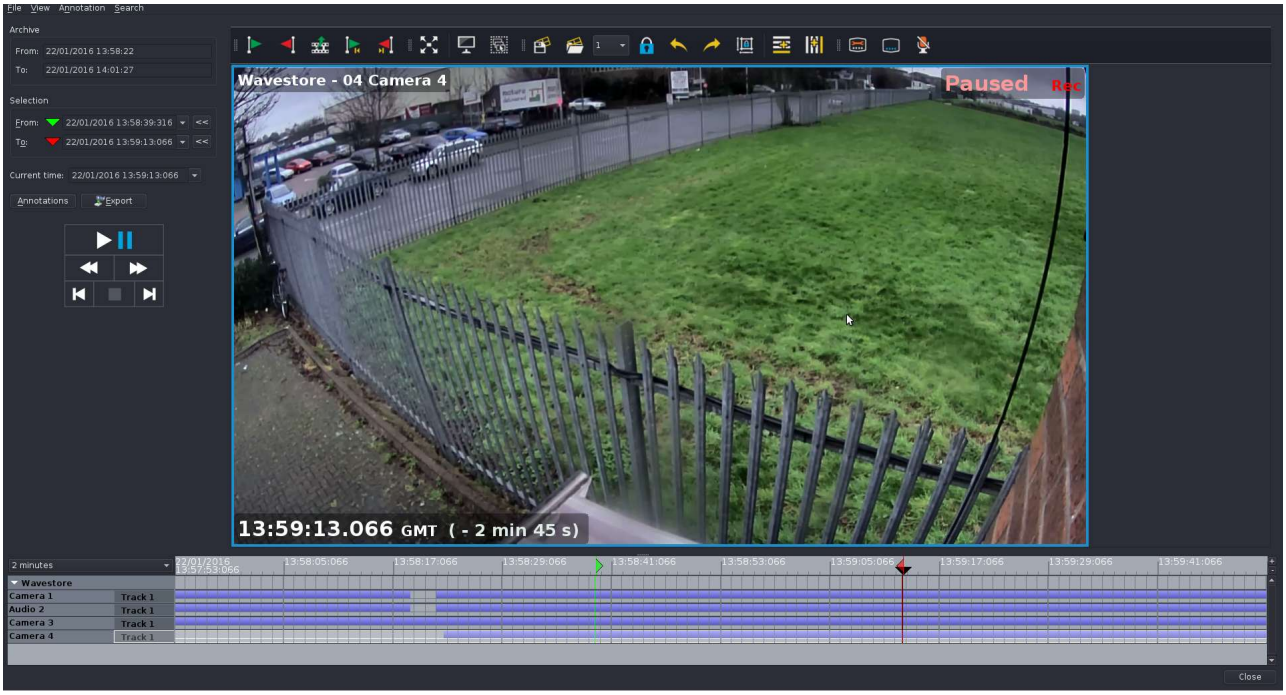


Figure 4.40: Export Camera Channel, Start and Stop times configured

- Click on the 'Export' button to call up the Export Window, configure the file name as you require, and accept the default Save Path, so that the export is saved in the WavestoreExports folder:

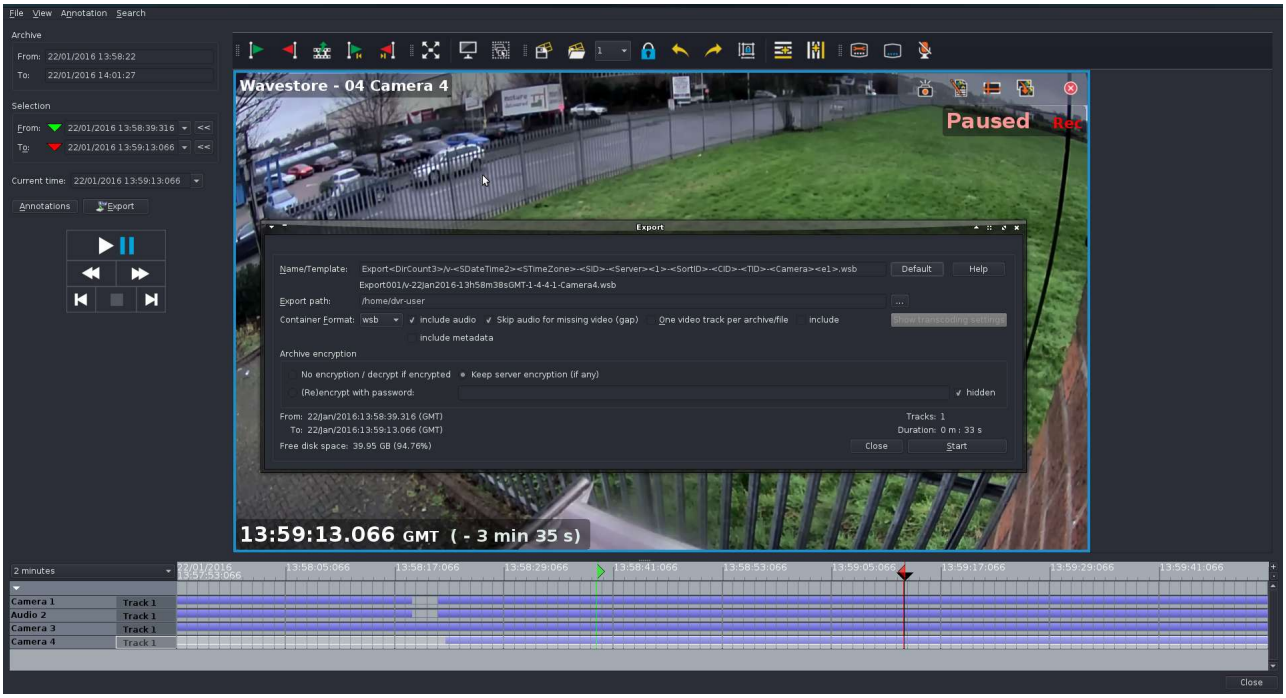


Figure 4.41: Export Screen

- Click on 'Start' to begin the Export; a progress bar will now appear, and fill as the export progresses:

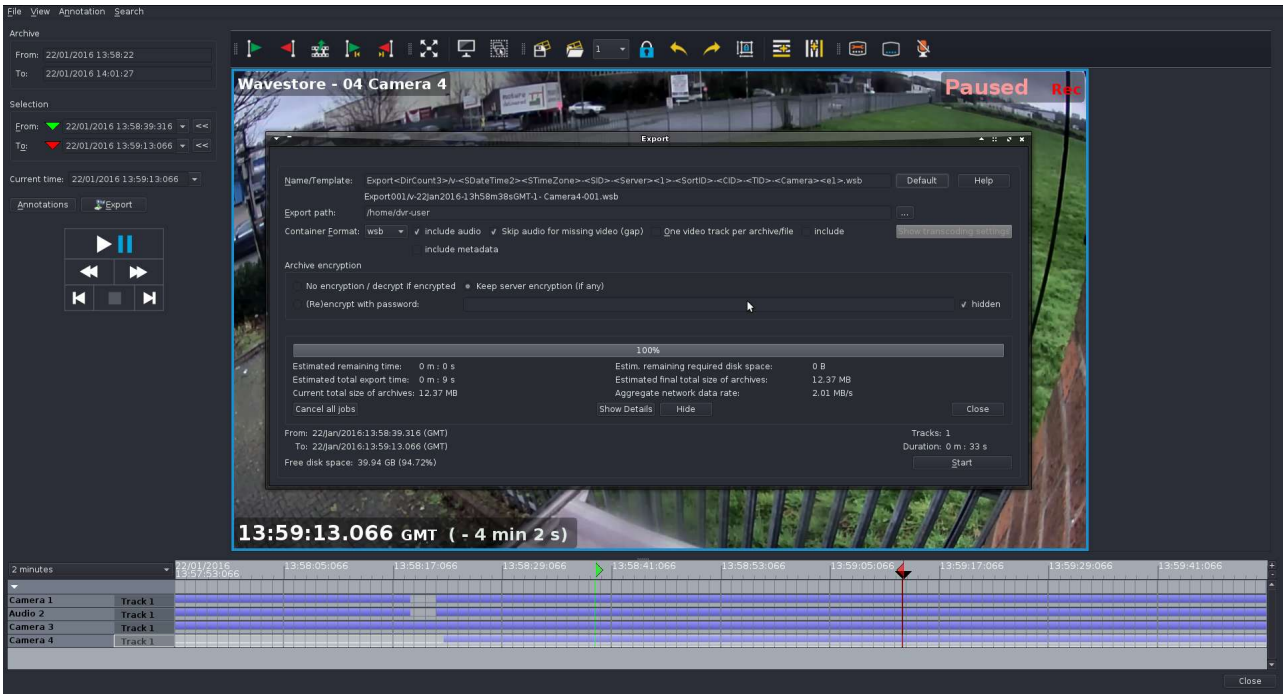


Figure 4.42: Export Completion Bar shows 100 percent

- Once the export has completed, a confirmation message will appear:

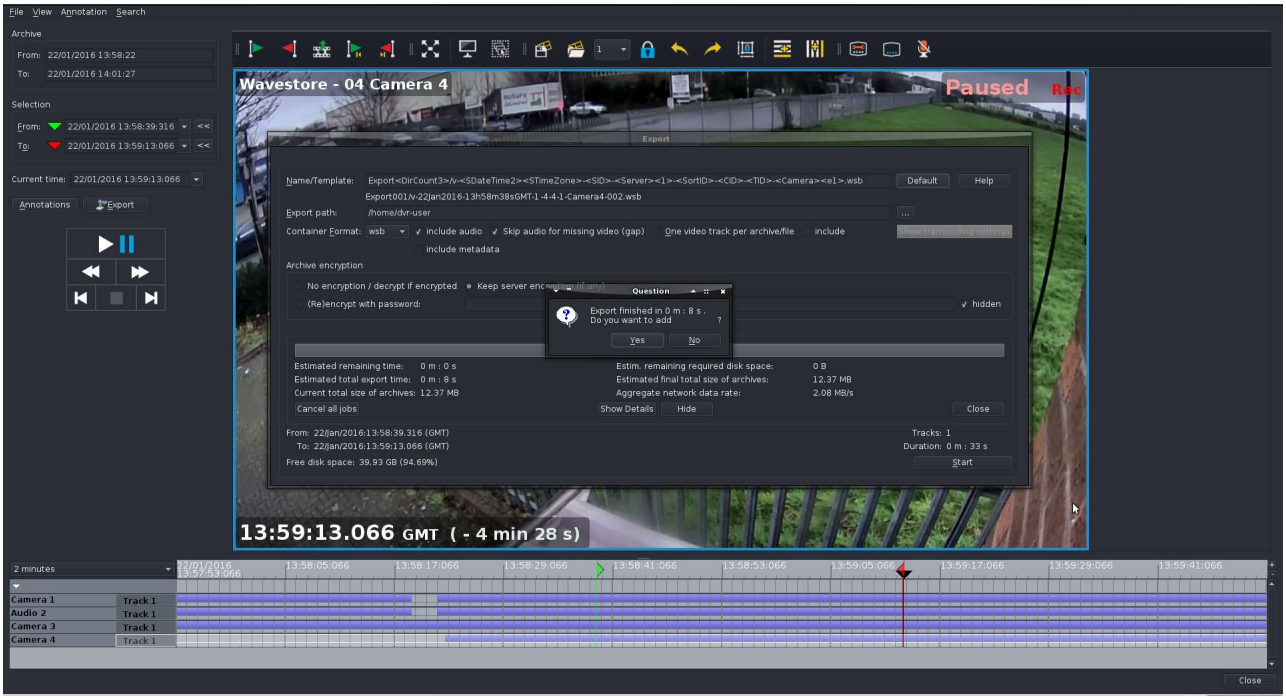


Figure 4.43: Export Completion Message

- Move the mouse pointer into the top left corner of the screen, so that the Accessories Toolbar appears:

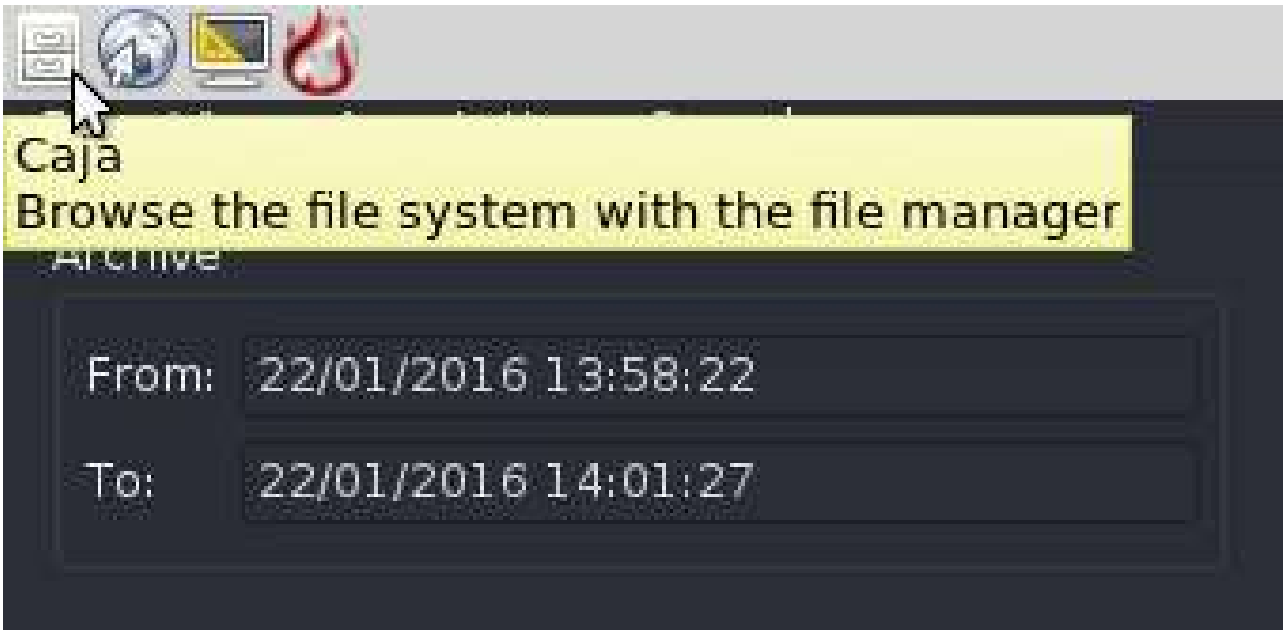


Figure 4.44: Accessories Toolbar

- Click on the CD/DVD icon to launch the K3B CD/DVD burning software:
- If asked about 'Konqueror integration' click the 'Enable Konqueror integration' option.
- Click on 'New Data DVD' project:

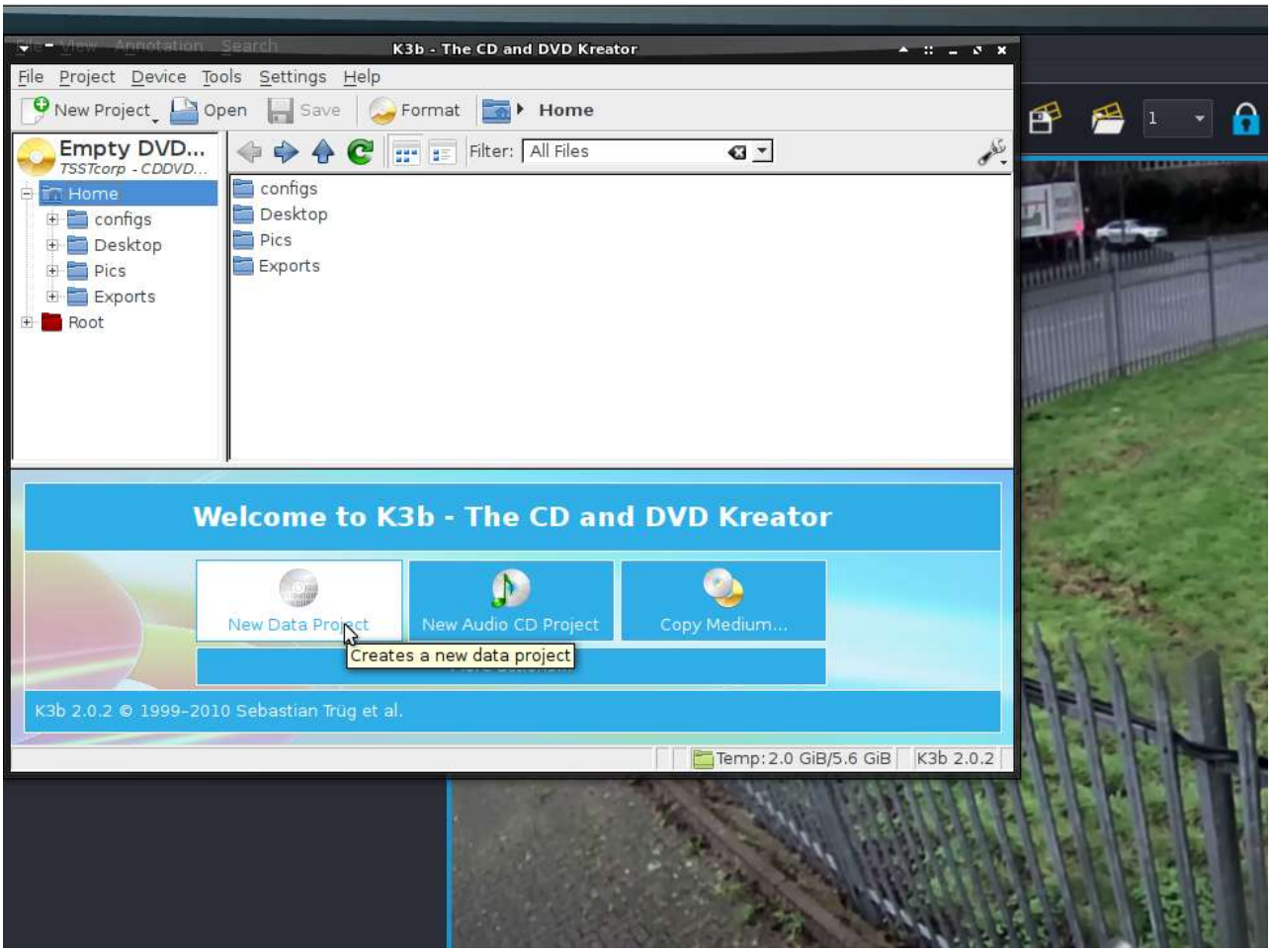


Figure 4.45: Configuring K3B Export screen

- Browse to select the file(s) that you wish to export, and click to select so the filenames appear in the 'Current Projects' window:

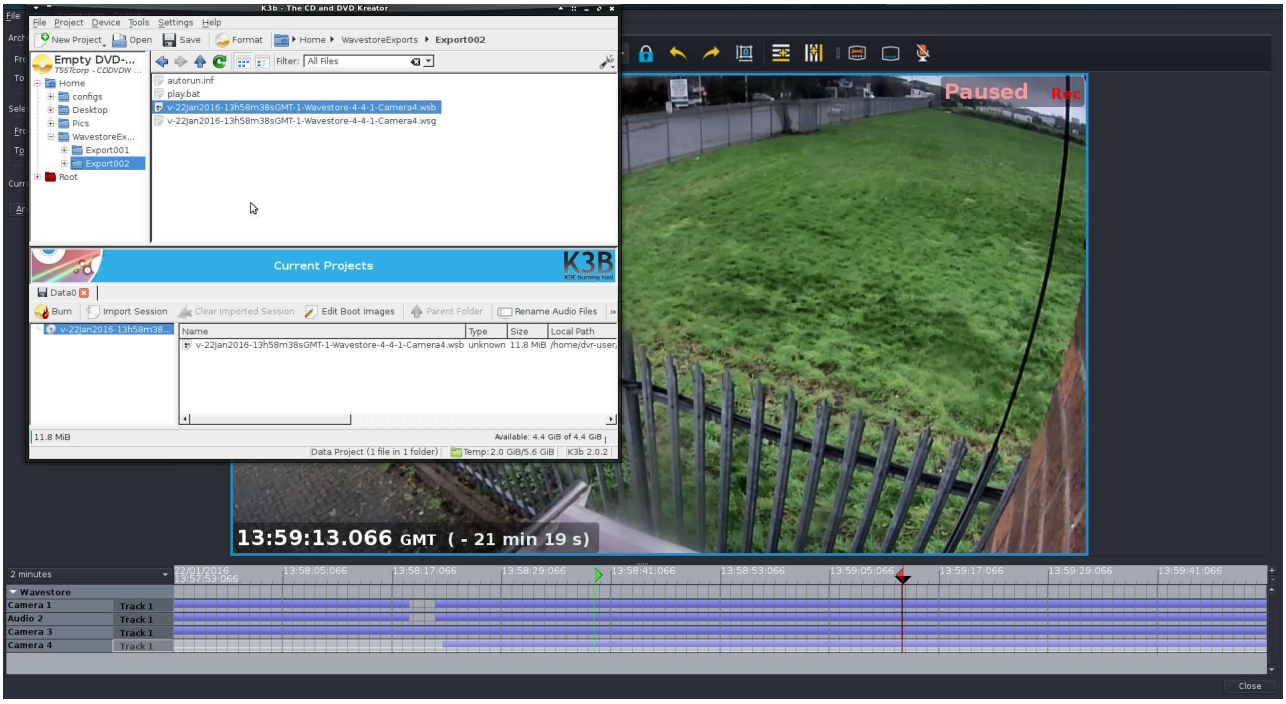


Figure 4.46: Selecting File for Export

- On the DataDVD0 tab, click on Burn, a new 'DVD Project' window will appear:

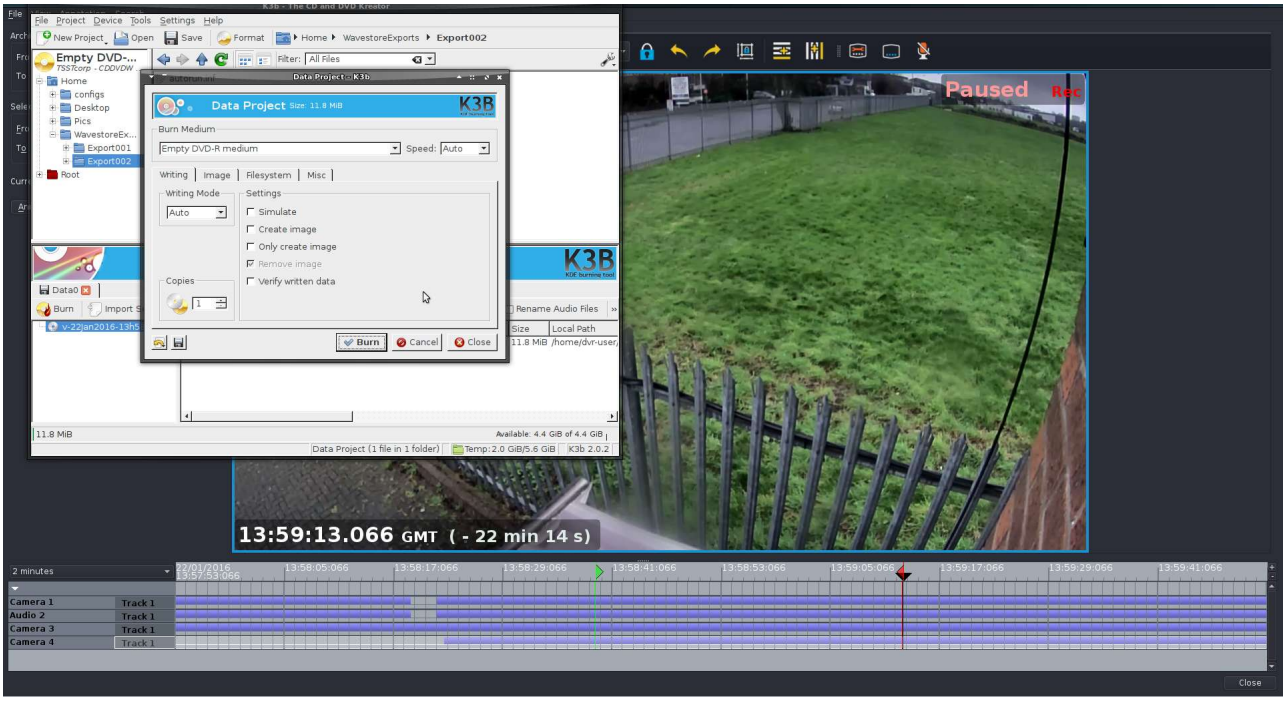


Figure 4.47: Configuring Export

- Click on 'Burn', and in the warning that appears, click on 'Cut volume descriptor in the Joliet tree':

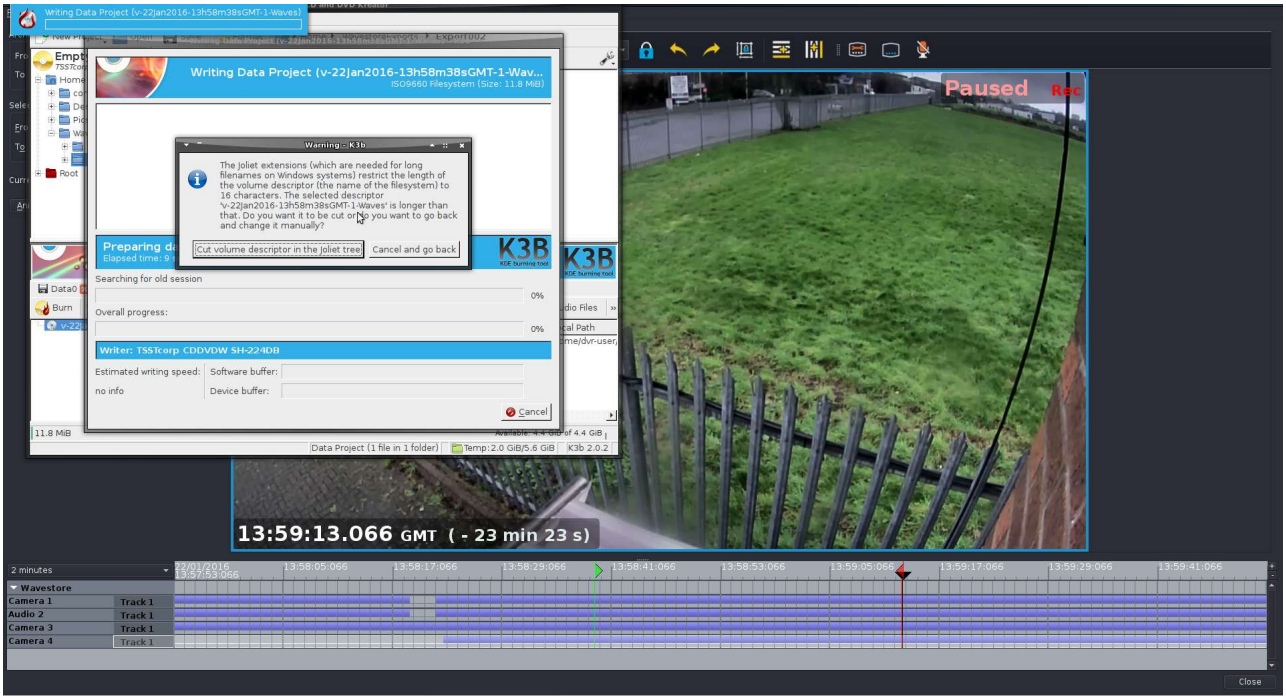


Figure 4.48: File Name length selection

- The progress bars will now fill, as the DVD is burnt:

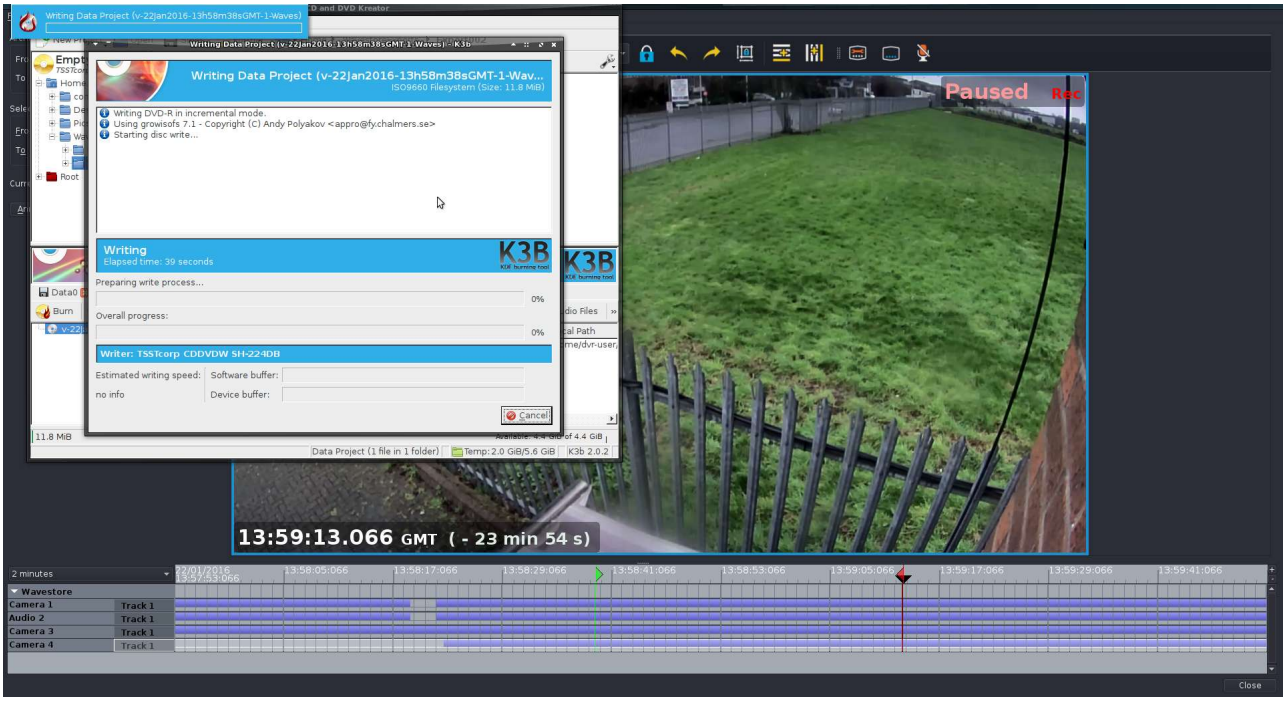


Figure 4.49: DVD burn progress bar

- Once the DVD is burnt, a completion message will display:

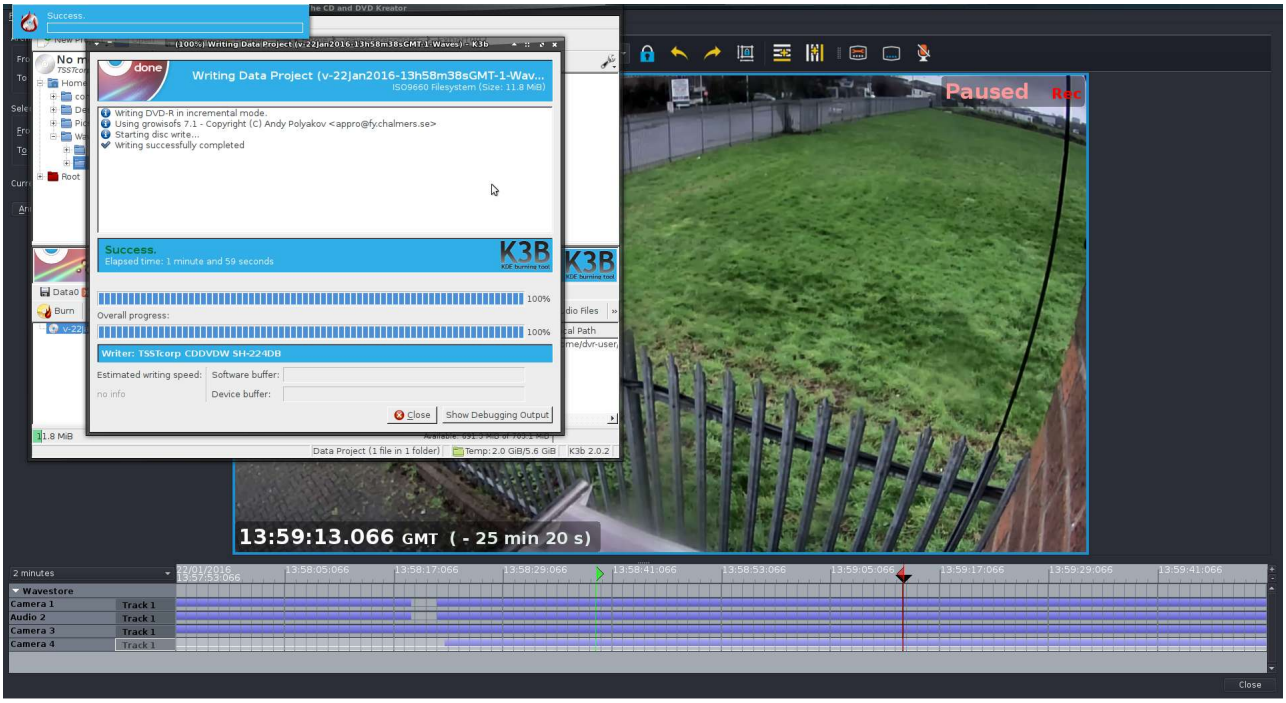


Figure 4.50: DVD Burn completion message

- Click on Close to close the window:

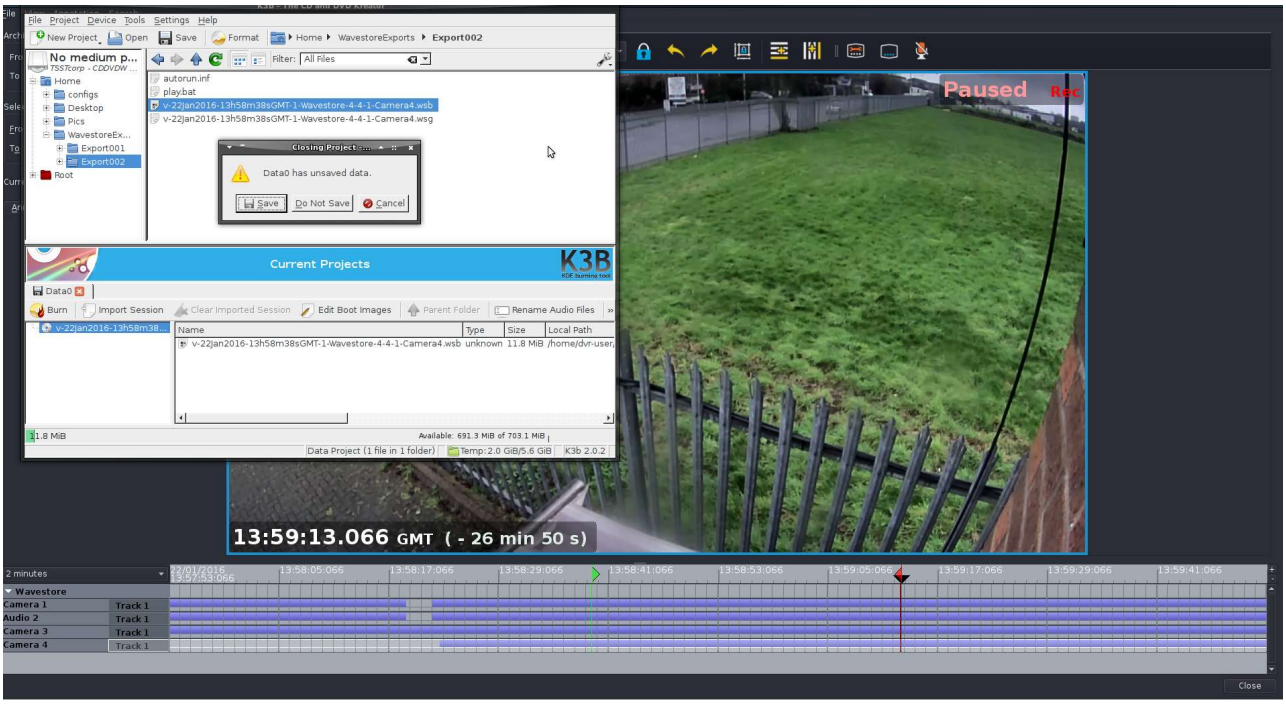


Figure 4.51: Closing K3B Project

- Click on 'Discard' to empty the temporary buffer, the K3B window will now close:

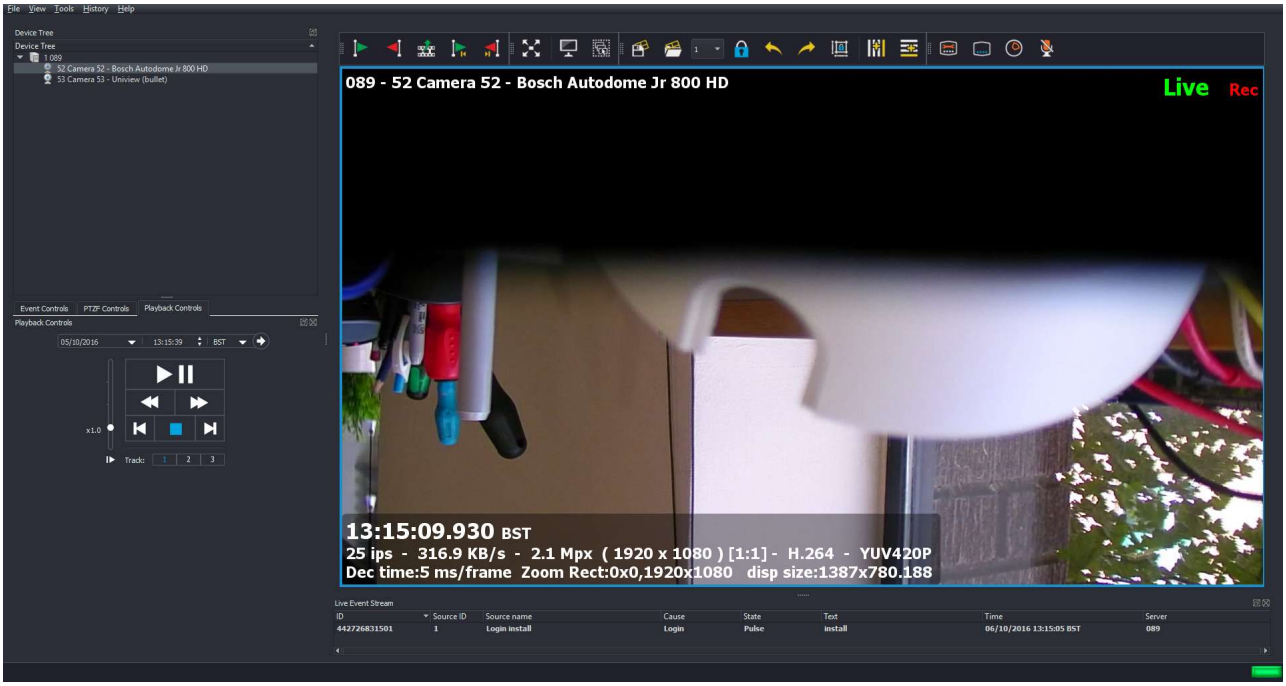


Figure 4.52: Exiting to main WaveView screen

4.9.4 Exporting to USB devices from the Wavestore Server

Before exporting to a USB device, it is necessary to "mount" the USB device. This is described in section 9.17 – Accessing a USB disk on the Wavestore server.

You can now export footage and still images from the Find screen to the USB device (menu path View → Find), the procedure for this is fully described in section 4.9.1 – Exporting footage to a Windows PC running WaveView client software; for Still Images refer to section 4.9.2 – Exporting still images to a Windows PC running WaveView client software.. Firstly select your Camera Channel, Start Time and Stop Time:

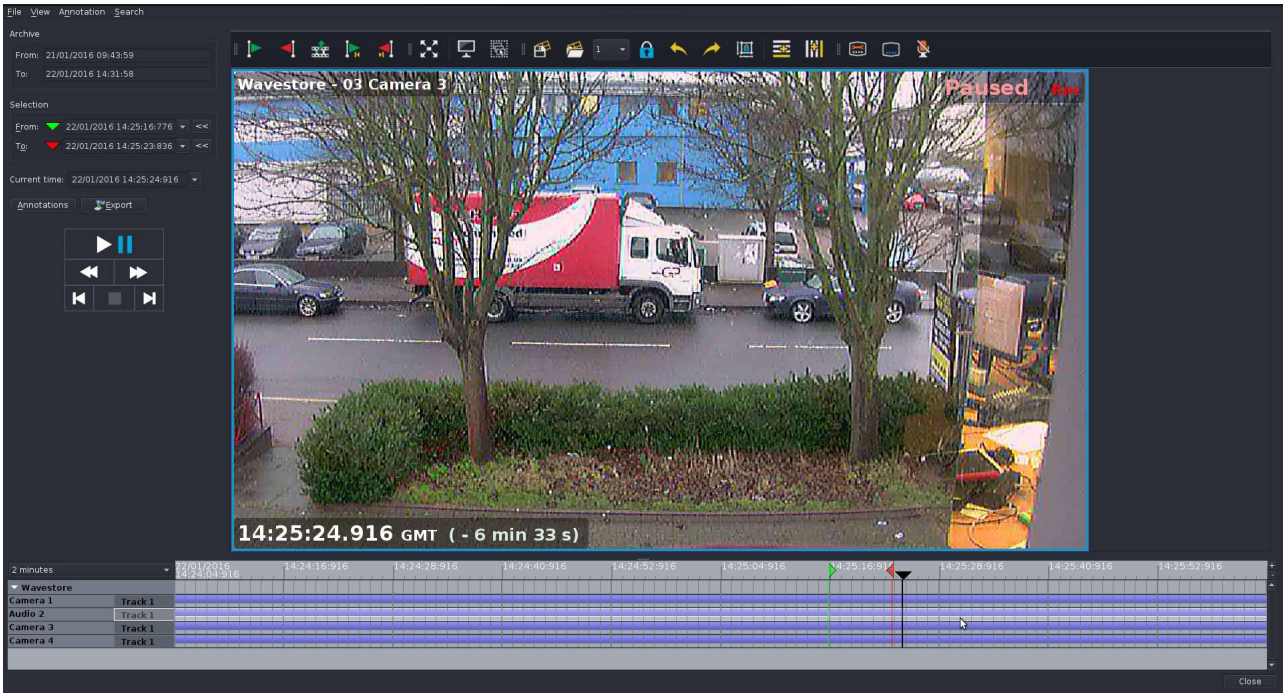


Figure 4.53: Find screen – configuring Camera Channel, Start Time and End Time

- Click on Export:

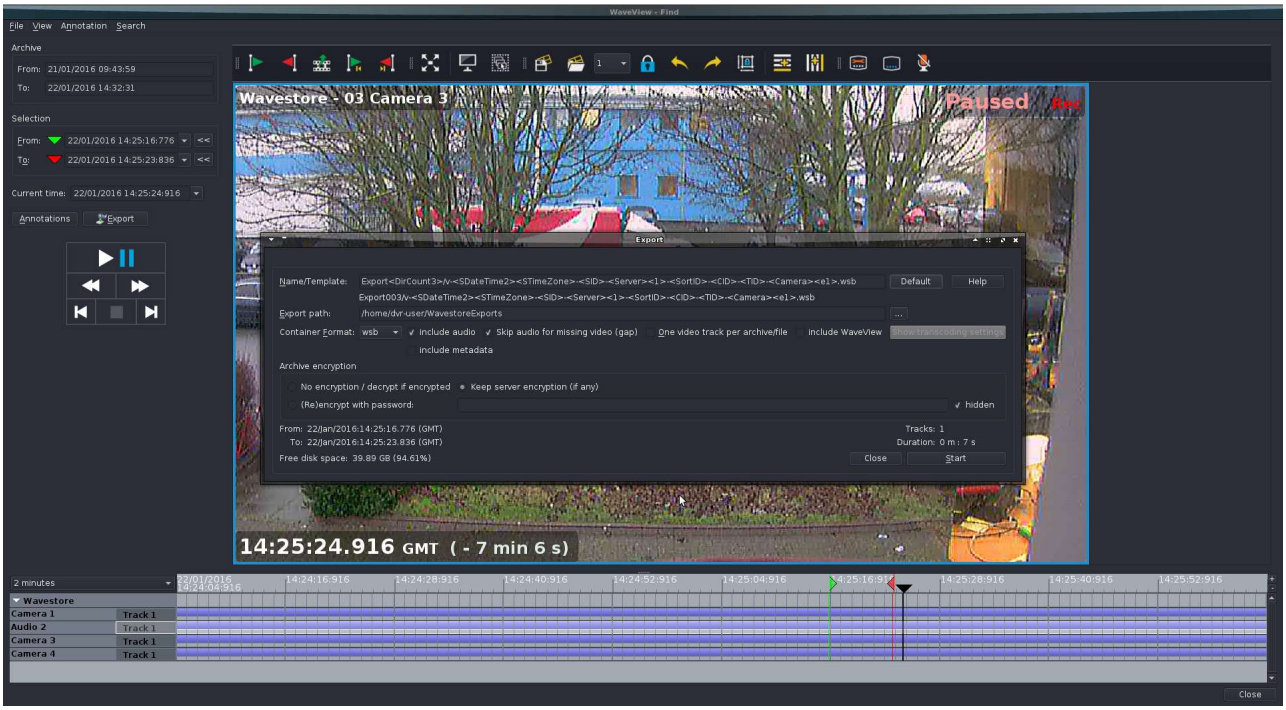


Figure 4.54: Find Screen – Export Screen

- Click on the ***Browse(...)*** button to open the File Directory for browsing:

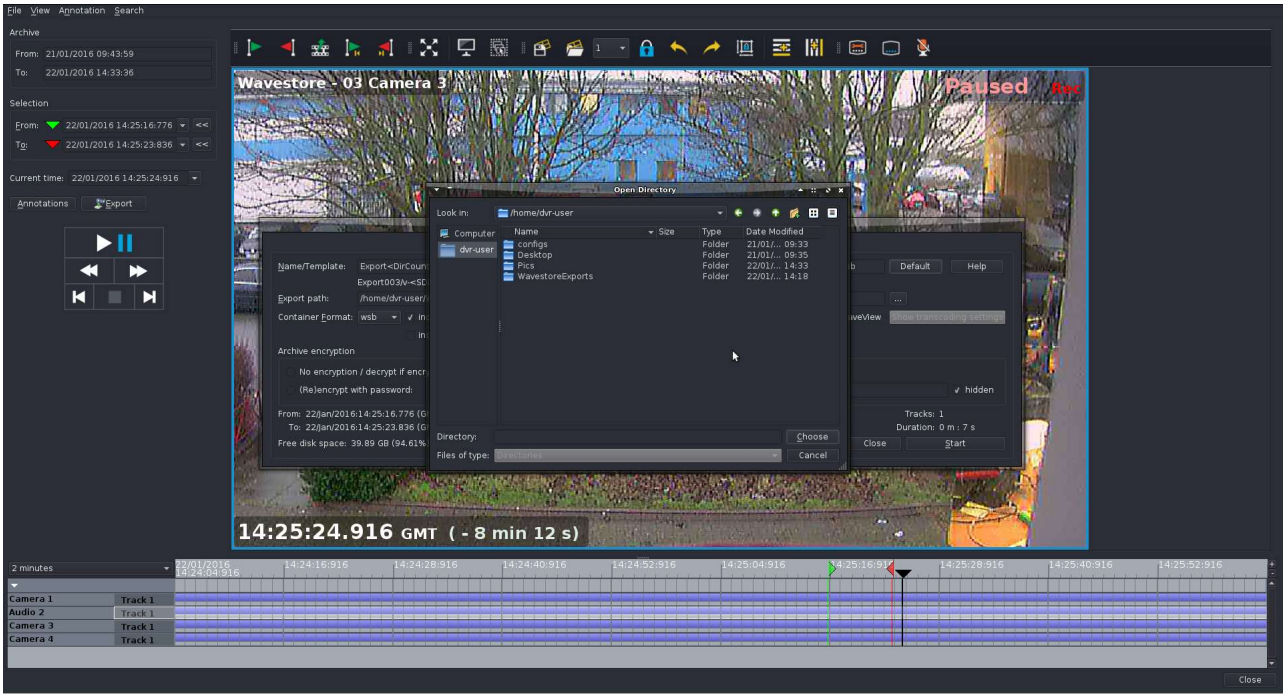


Figure 4.55: Find screen – Browsing directories to set Export path

- Click on the *UP ARROW KEY* button to browse up one level to the 'home' directory:

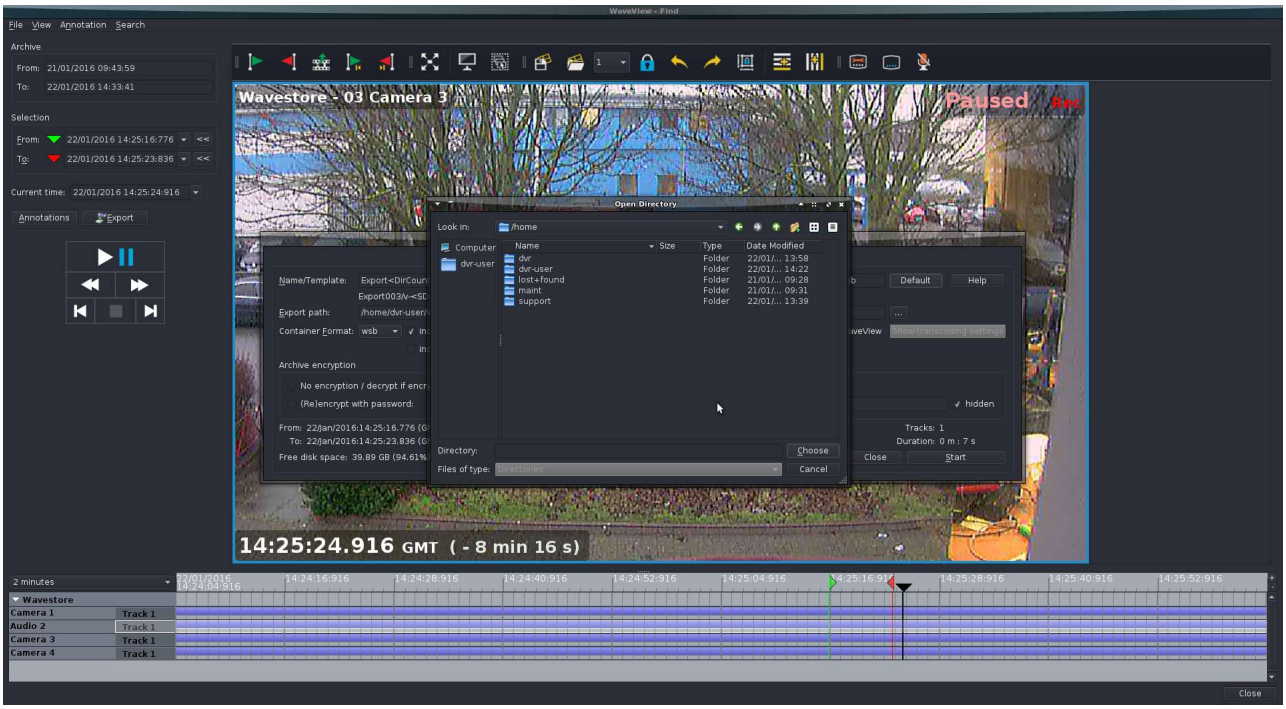


Figure 4.56: Find screen – Browsing directories to set Export path

- Click on the *UP ARROW KEY* button to browse up one level :

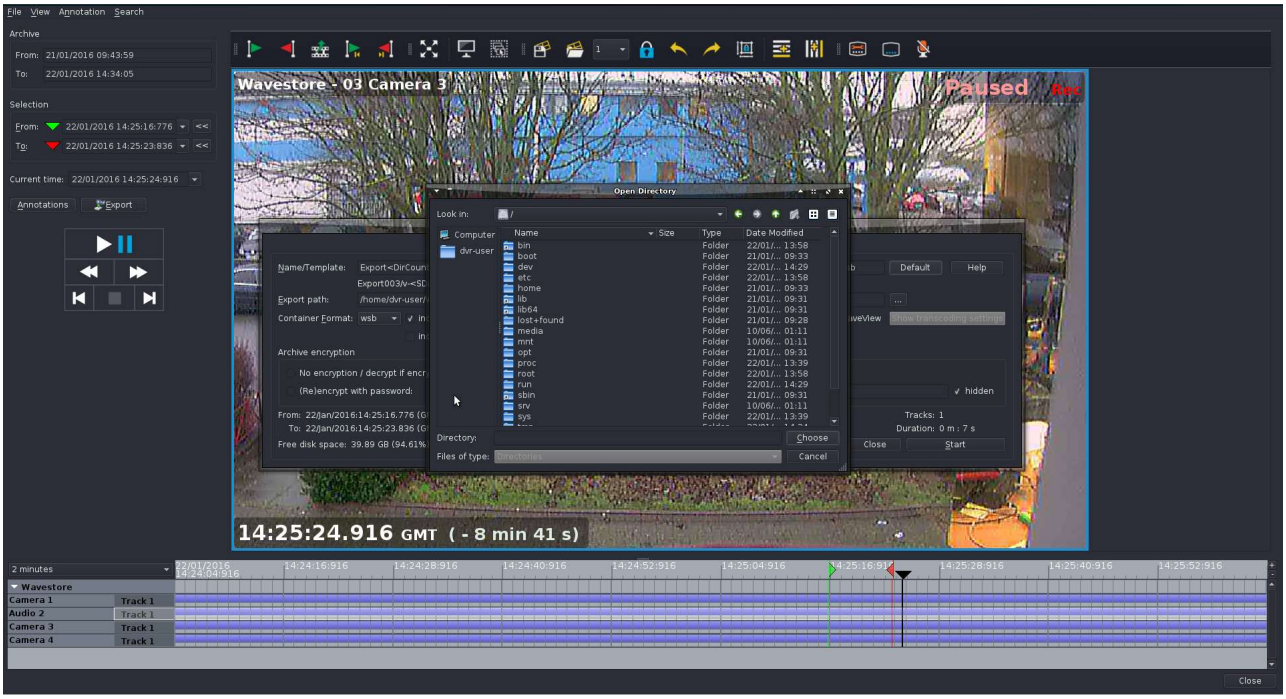


Figure 4.57: Find screen – Browsing directories to set Export path

- Click on the '↑' button to browse up one level to the 'media' directory:

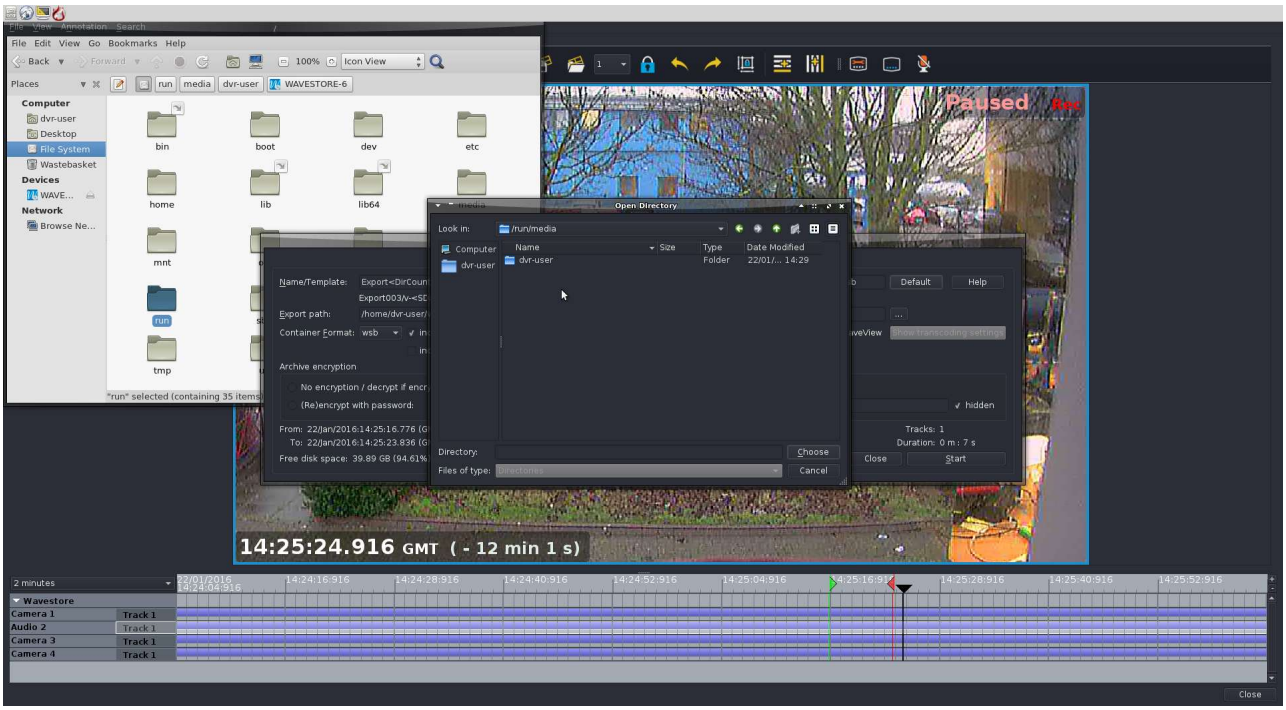


Figure 4.58: Find screen – Browsing directories to set Export path

- Click on the name of the USB media (in this case 'WAVESTORE–6'); files contained on this USB device will now be displayed:

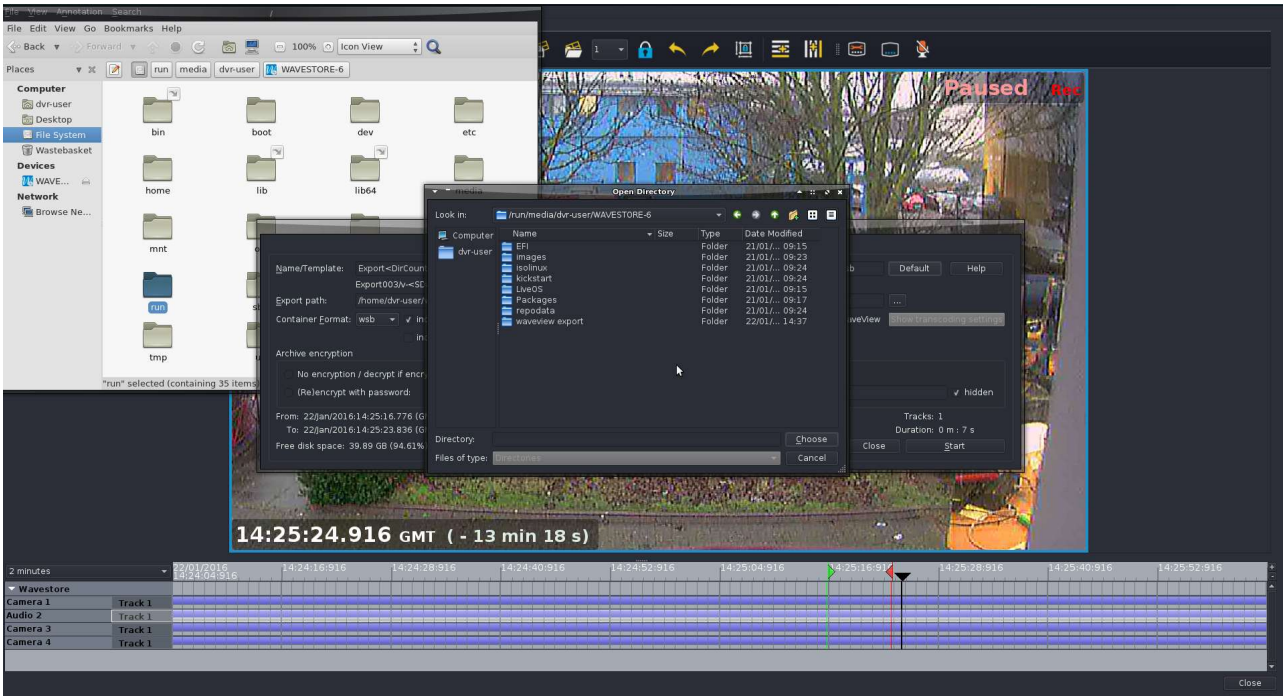


Figure 4.59: Find screen – Contents of USB device displayed

- Select the save path folder on the USB device, then click on 'Choose'.

The Open Directory window will now disappear. Configure the file name/container format etc. as required.

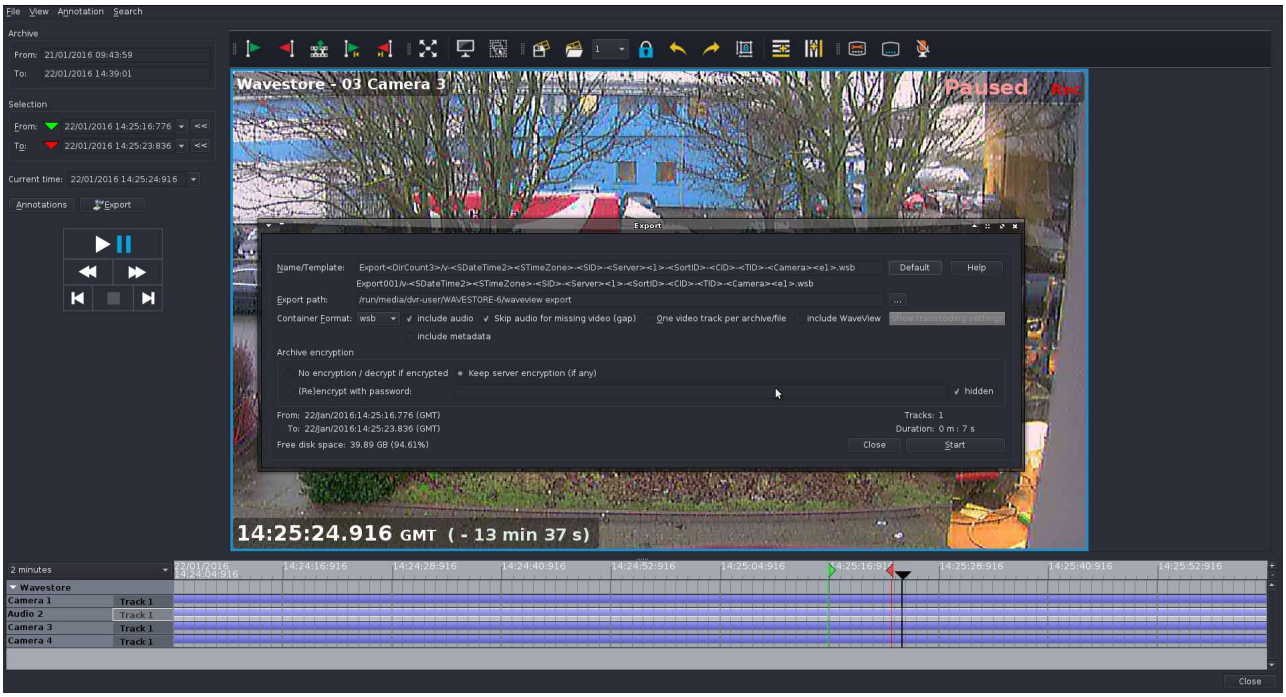


Figure 4.60: Find screen – Export Window

- Click on 'Start'; the export progress bar will now fill to 100%.

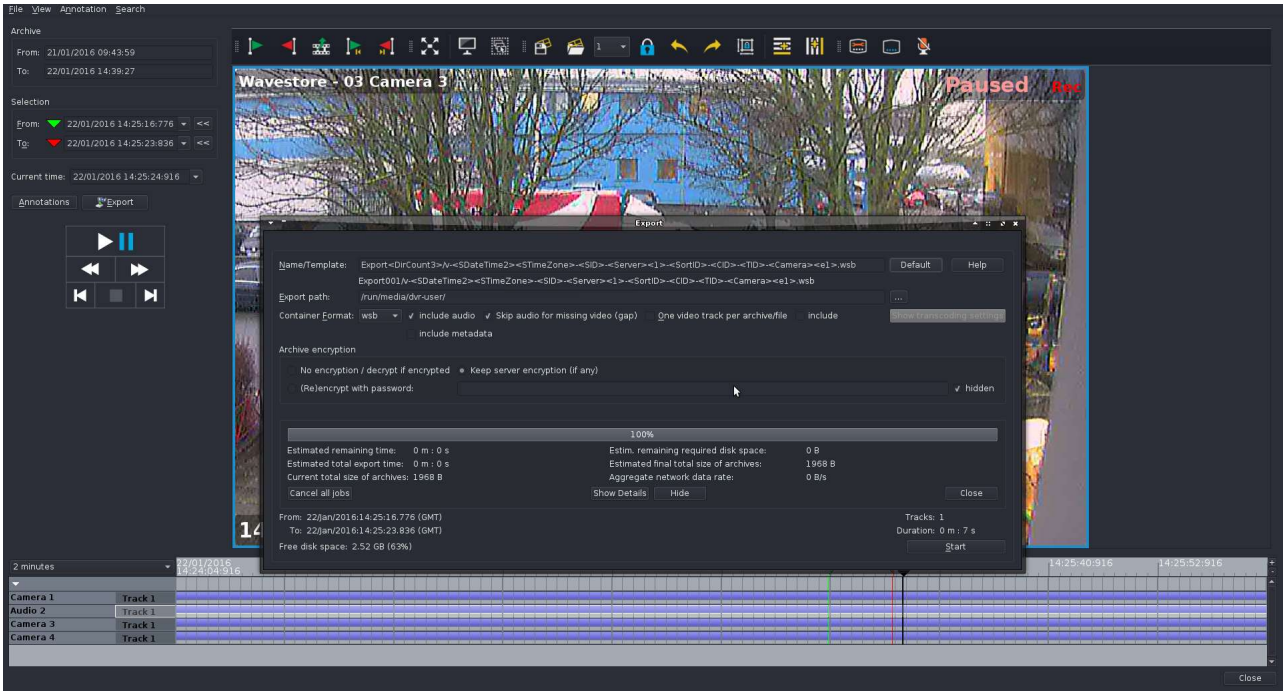


Figure 4.61: Find screen – Export completed

- Repeat for any other files that you require.
- Once completed, you must then 'eject' the device before it can be removed from the server. Close the Find screen, and on the main WaveView screen, move the mouse pointer into the very top left corner of the screen, so the Accessories Panel appears at the top left of the screen as shown below:

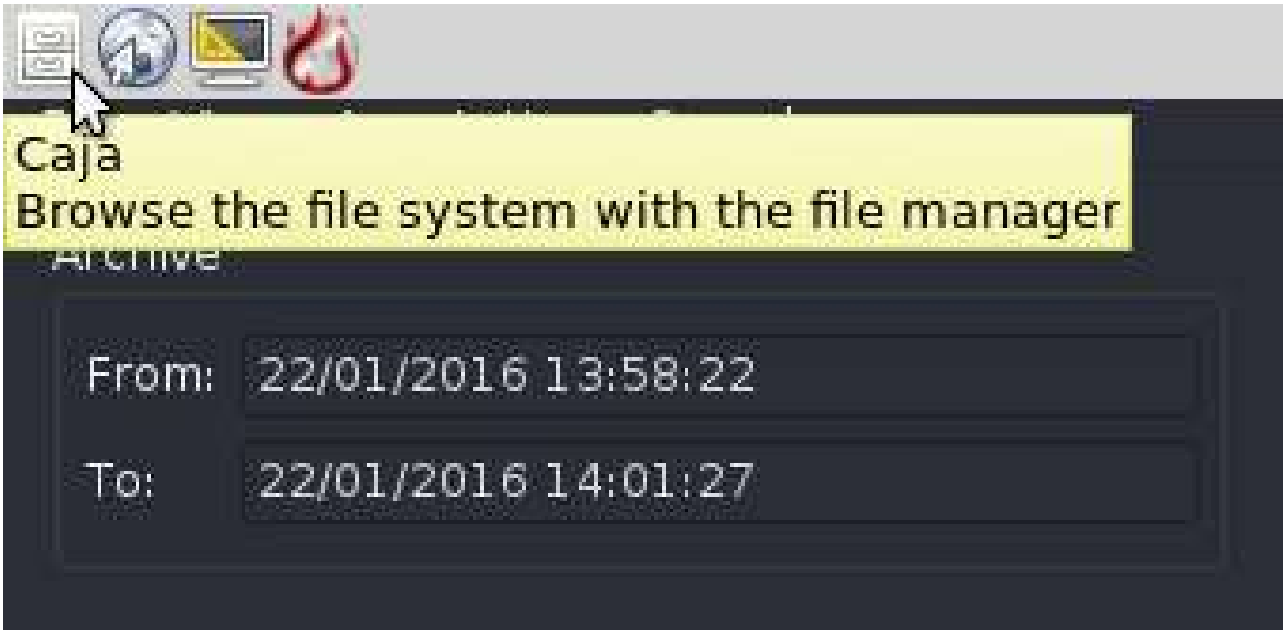


Figure 4.62: Accessories Toolbar

- Click on the File Manager Icon (third icon), and the File Manager window will open, with the left column in the window showing connected devices on the server and network, including the USB

device.

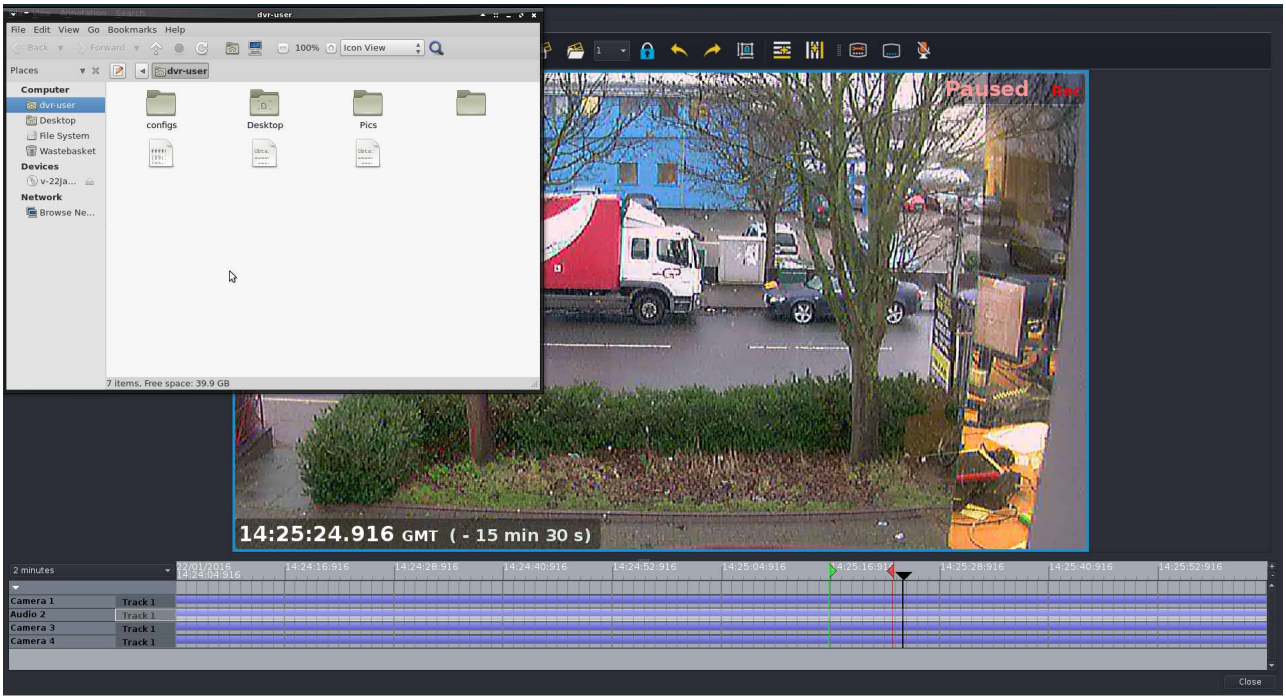


Figure 4.63: WaveView screen showing File Manager window

- On the device tree on the left, click on the USB device so it is highlighted blue:

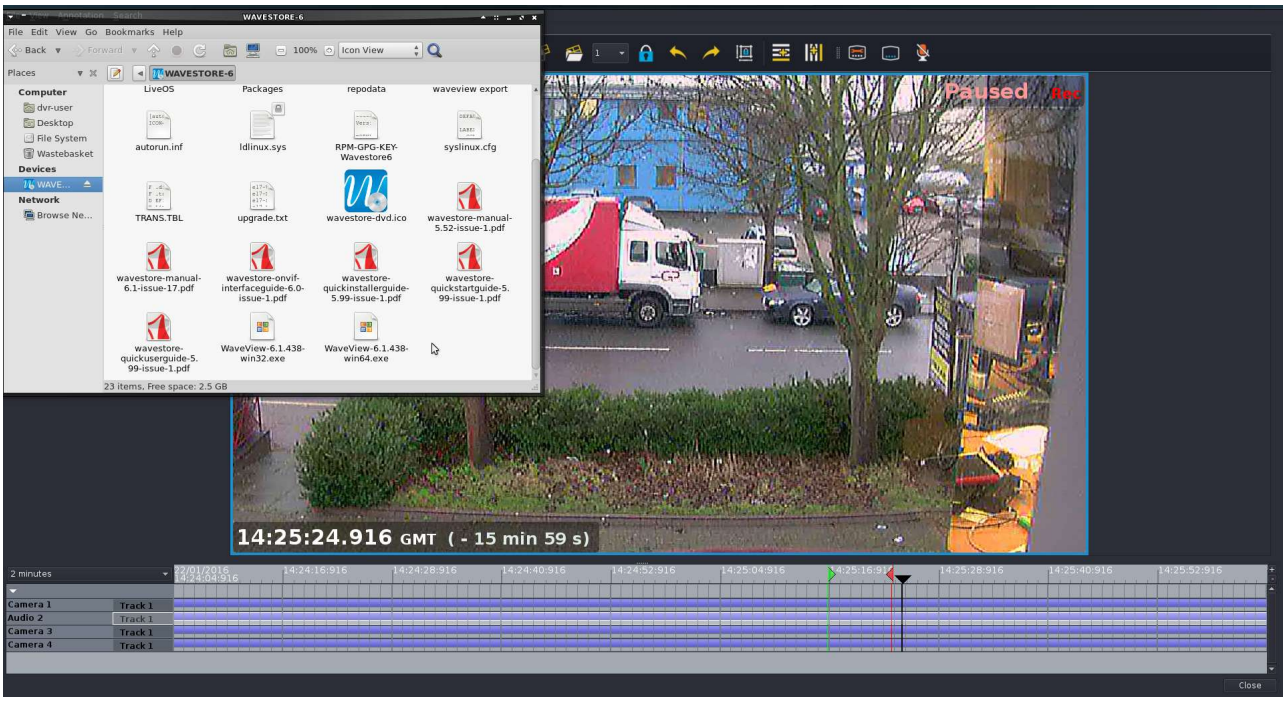


Figure 4.64: File Manager window showing contents of USB device

- Click on the 'eject' icon next to the name of the USB device to eject the device. The USB device will now disappear from the File Manager display window will now display as below:

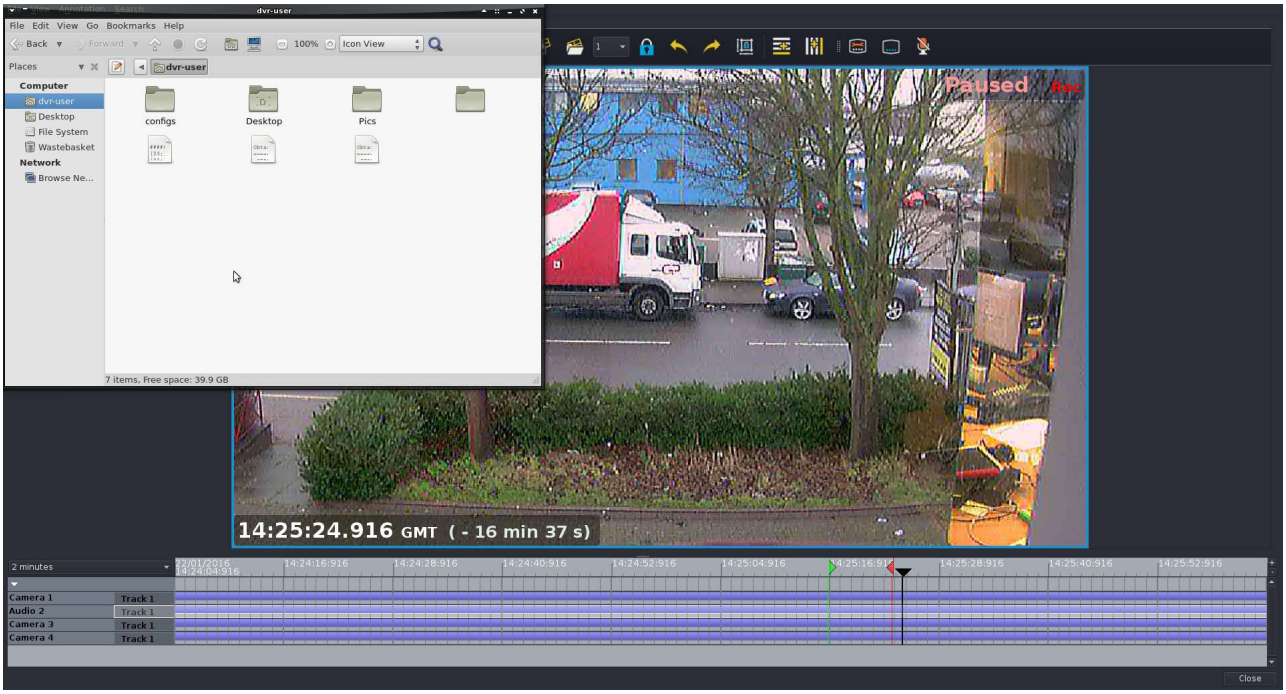


Figure 4.65: File Manager window with USB Device now removed

- You can now remove the USB device.

5 Playing Back Exported Files

5.1 Playing Back Exported Files on a PC from DVD/USB device

If the PC that you are using already has the WaveView client software installed, launch it as usual, either from the Start Menu or by double-clicking the desktop WaveView shortcut.

Alternatively, if the DVD/USB device contains a copy of WaveView, open the device on your PC:

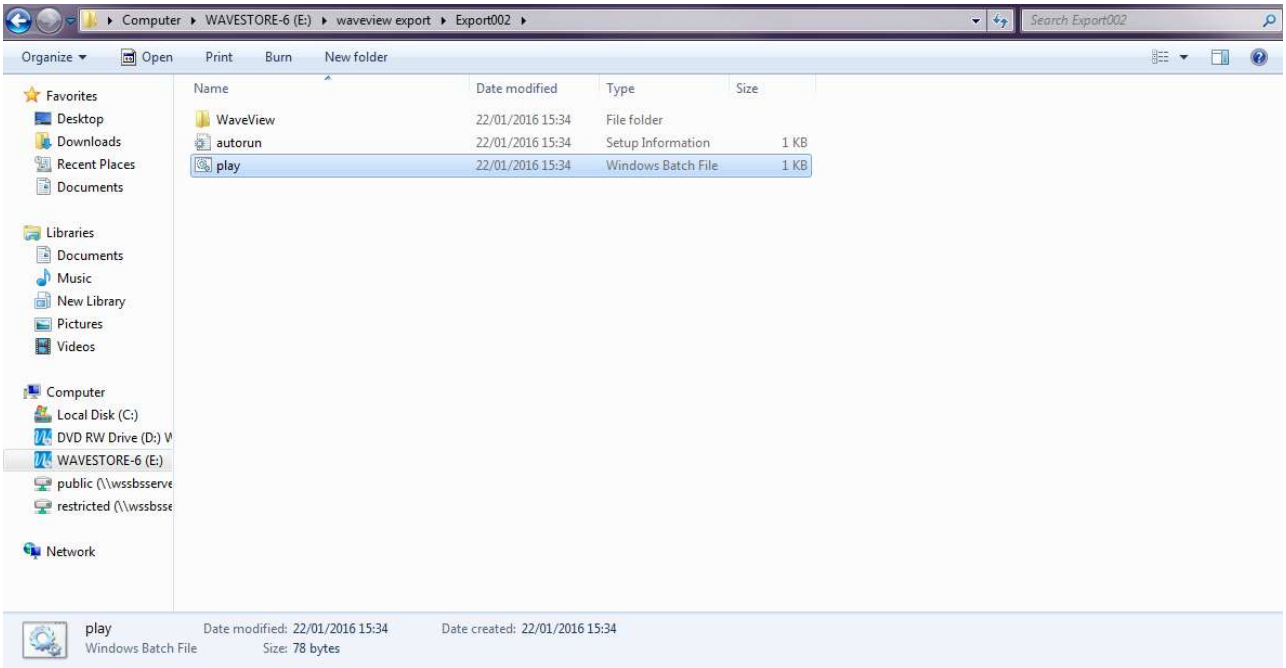


Figure 5.1: Browsing to locate export file

Double click on the file named 'play.bat'. The WaveView program will launch, and open the export file as below. You may be prompted to enter a Password, if this option was selected when the export was originally created:

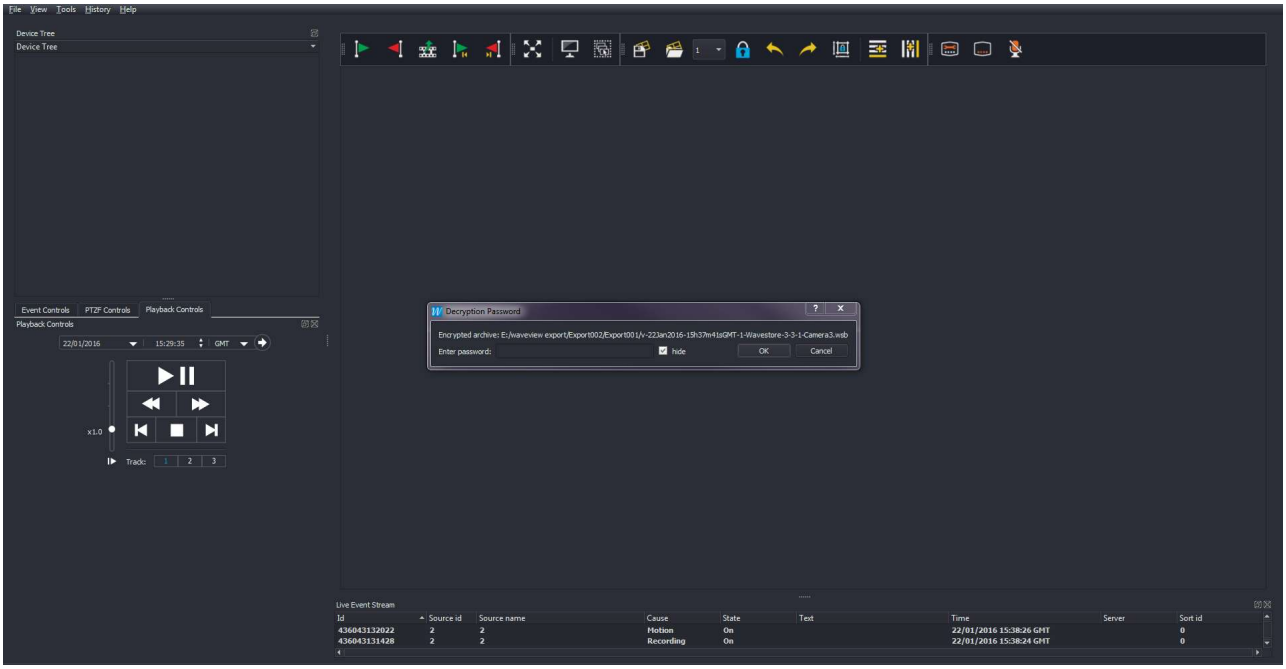


Figure 5.2: Entering Decryption Password

The configured name of the original source Wavestore server, and also details of the camera channels that are contained in the export file, will now be displayed in the Device Tree section.

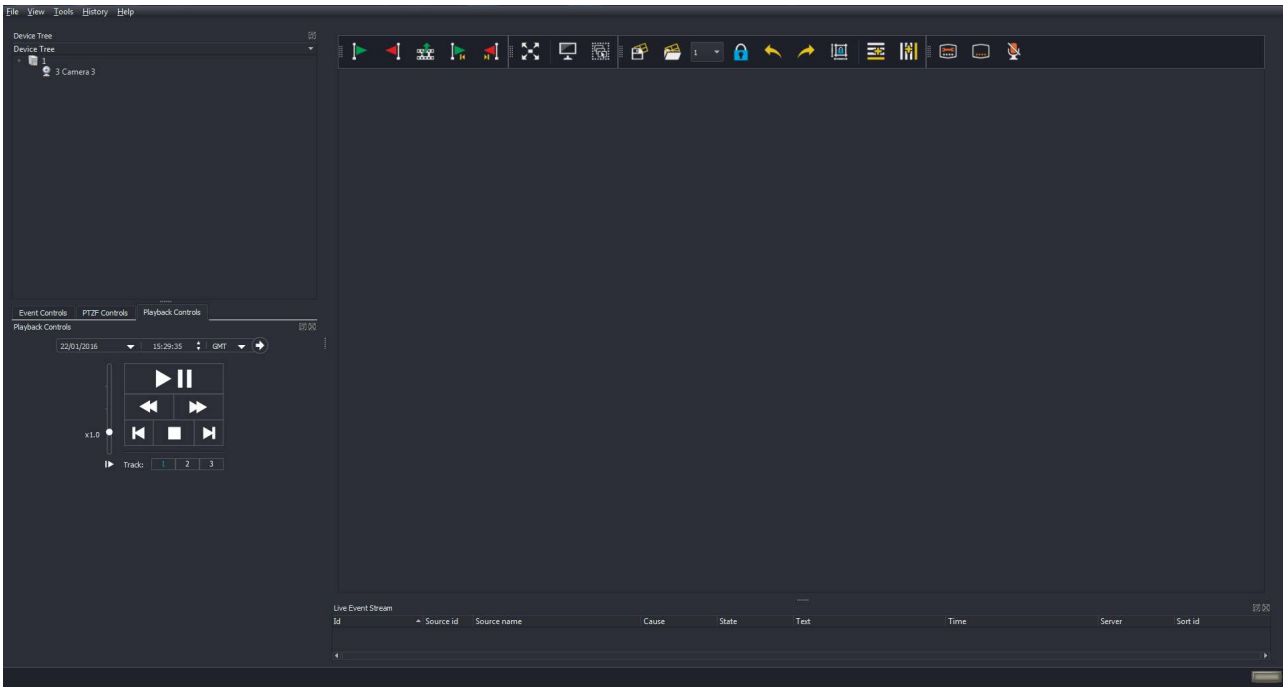


Figure 5.3: Device Tree showing camera(s) contained in export

Double click on the camera channel(s) that you require; and click on 'Play' to commence playback:

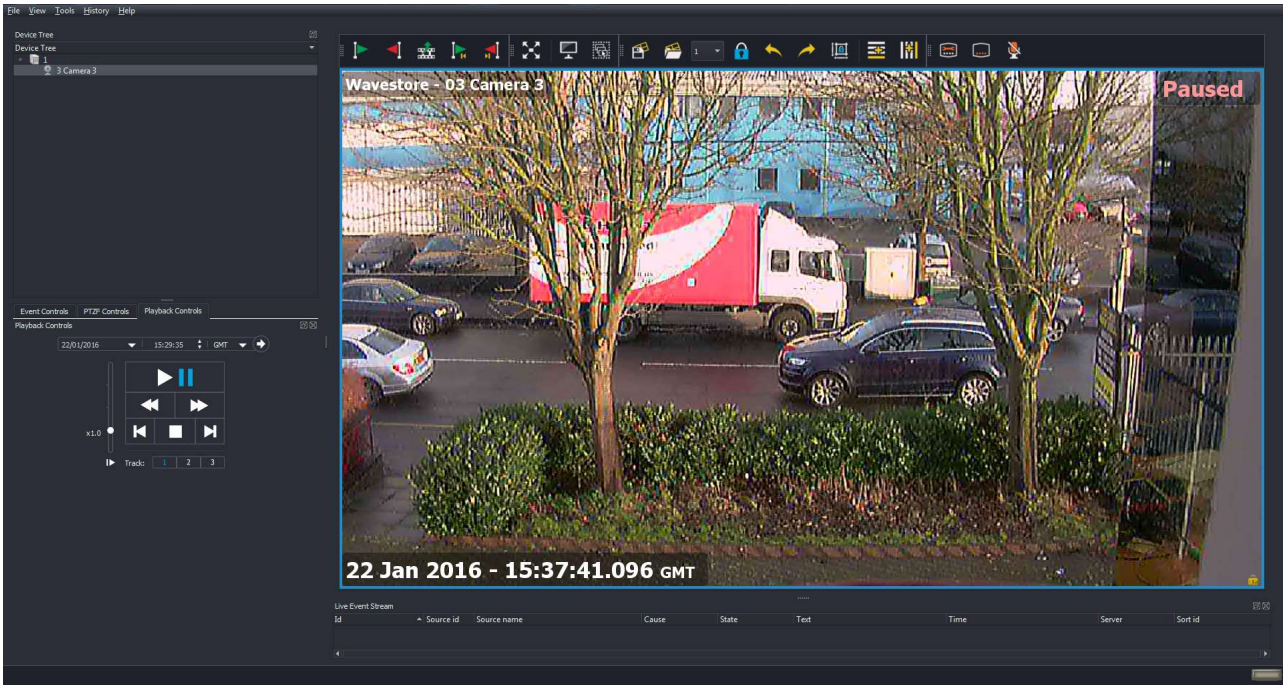


Figure 5.4: Playback of export file

The Playback controls can be used as described in section 3.10 – Playback Controls and section 4 – Search/Playback/Export using Find Screen to control playback of the footage, create further export files, and save still images.

5.2 Playing Back Exported Files on a Wavestore Server from a DVD

- Insert the DVD into the server, and move the mouse pointer into the very top left corner of the screen, so the Accessories Panel appears at the top left of the screen as shown below:

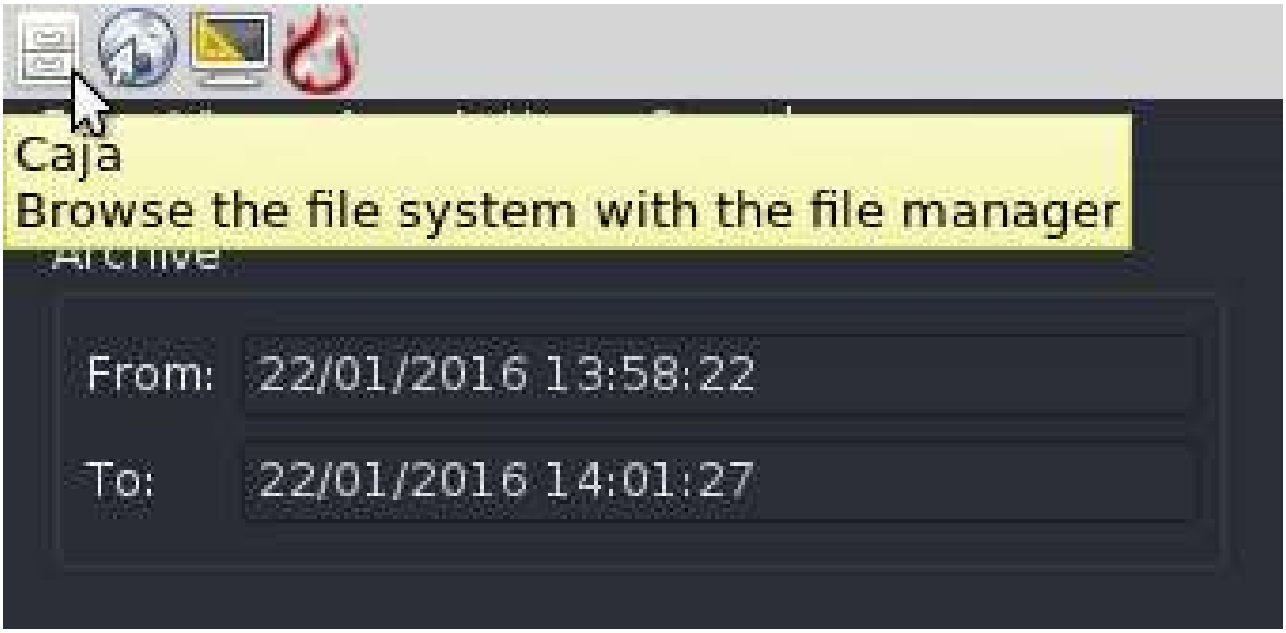


Figure 5.5: WaveView screen showing Accessories Panel

- Click on the File Manager icon (third icon across), and the File Manager window will open, with the left column in the window showing connected devices on the server and network, including the DVD. The right hand section of the window shows the files and folders contained on the selected device.

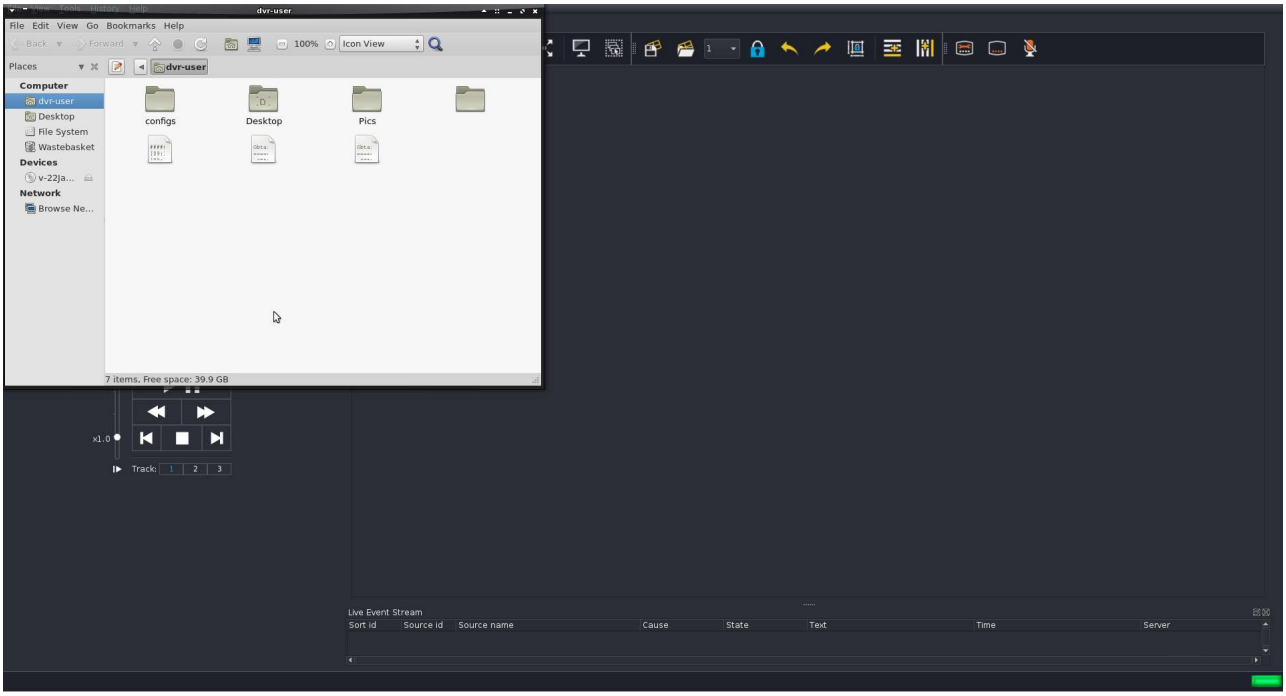


Figure 5.6: WaveView screen showing File Manager window

- On the device tree on the left, click on the DVD; files contained on the disc will now be displayed:

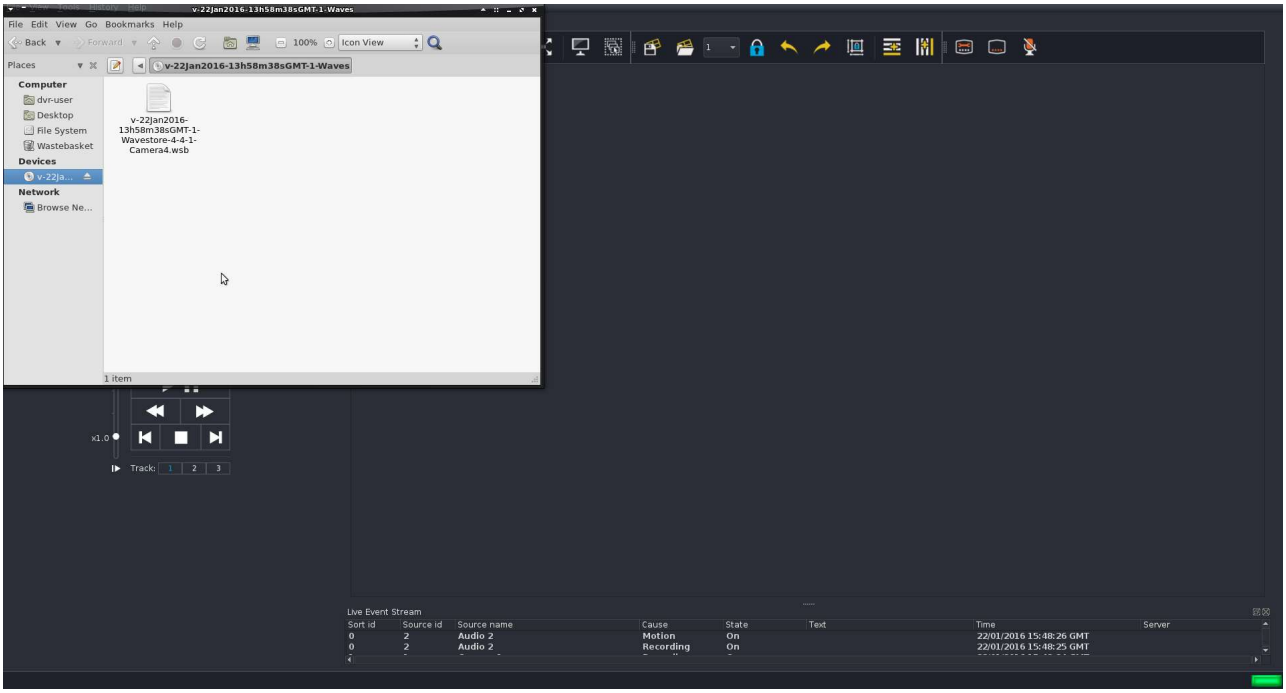


Figure 5.7: File Manager window showing contents of USB device

- The DVD is now mounted on the server. You can now playback footage files on this disc. To open a file, first disconnect from any servers that you are connected to (menu path File → Disconnect). Click on 'Open Export' in the Login Dialog box,

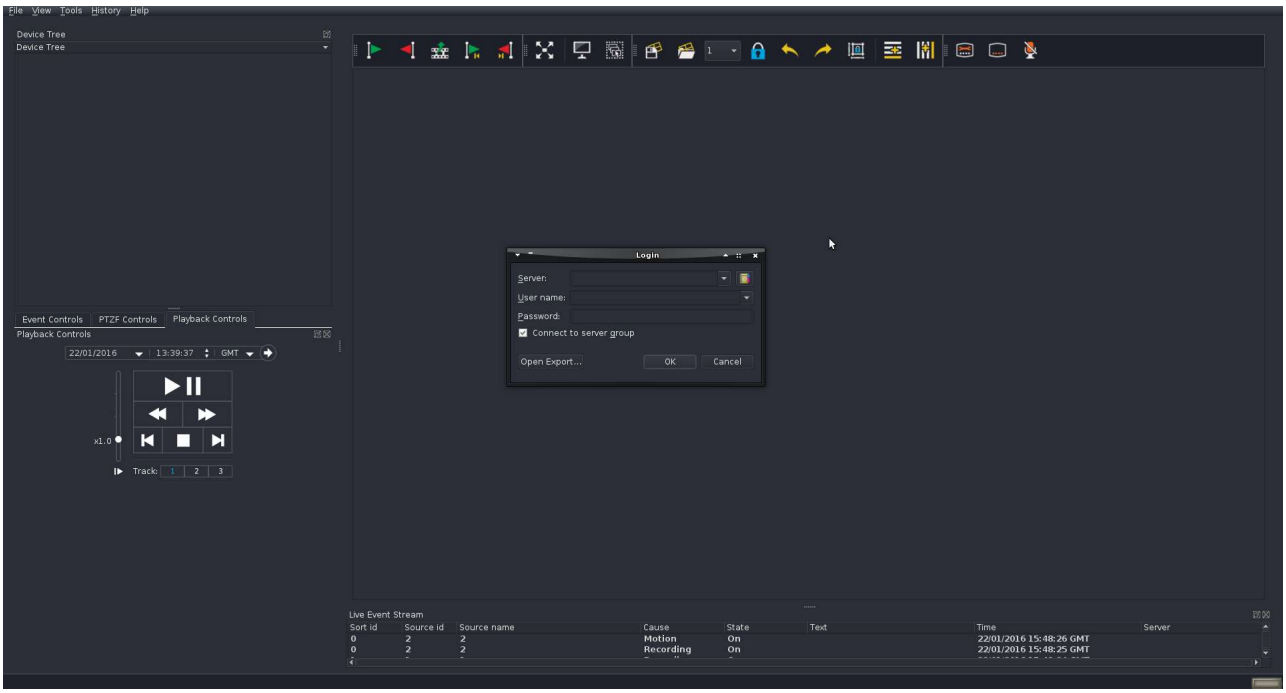


Figure 5.8: Login Dialog box

- and the Open dialog windows will appear as follows:

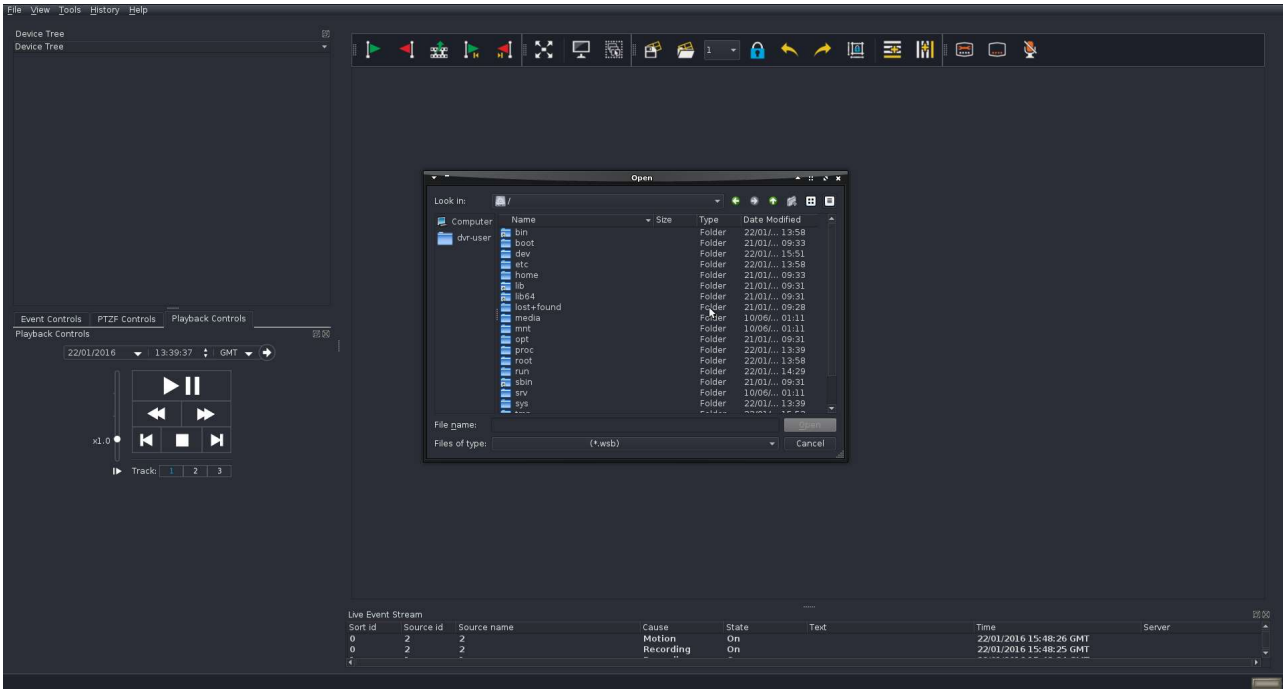


Figure 5.9: Open file dialog

- Click on the media folder:

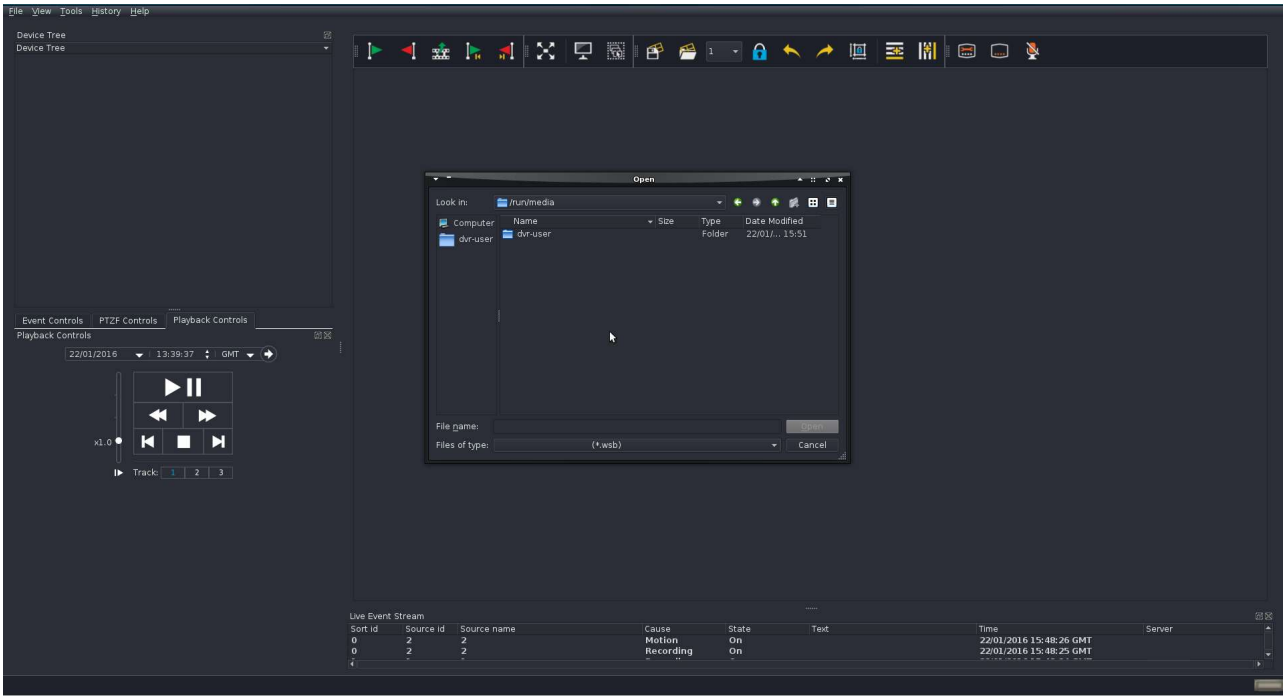


Figure 5.10: Browsing for WSB file

- Click on the name of the disc containing your footage:

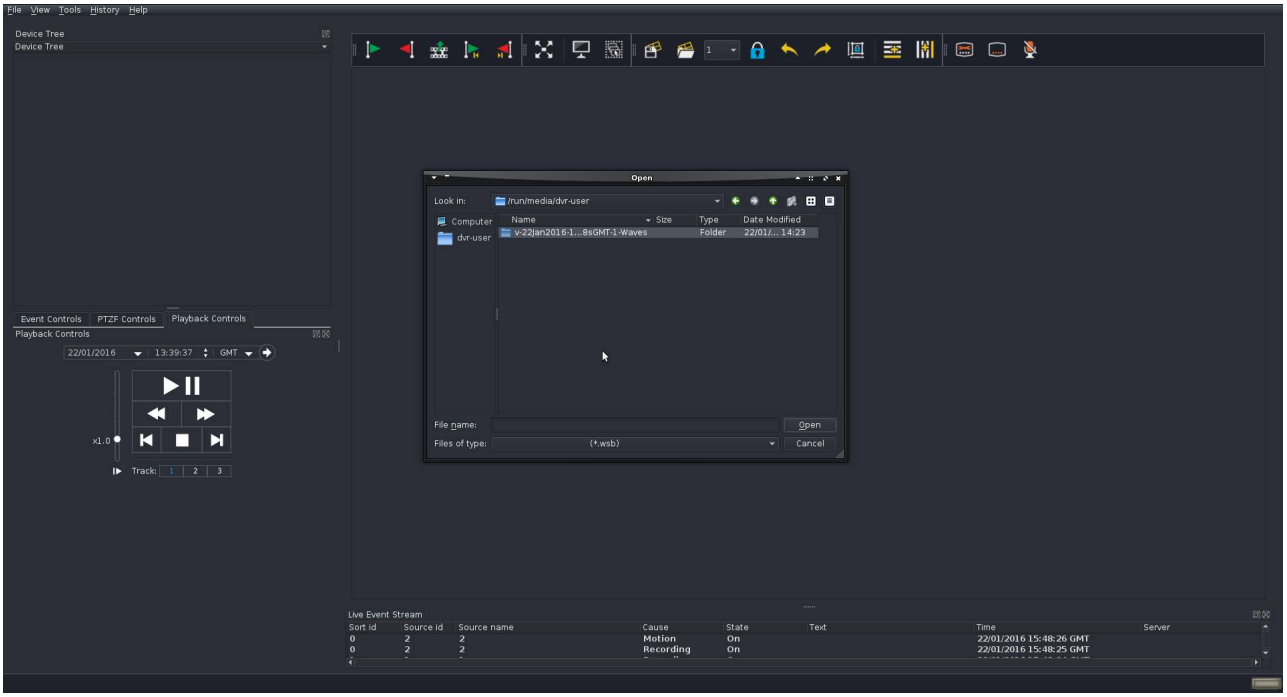


Figure 5.11: Browsing for WSB file

- Click on Open:

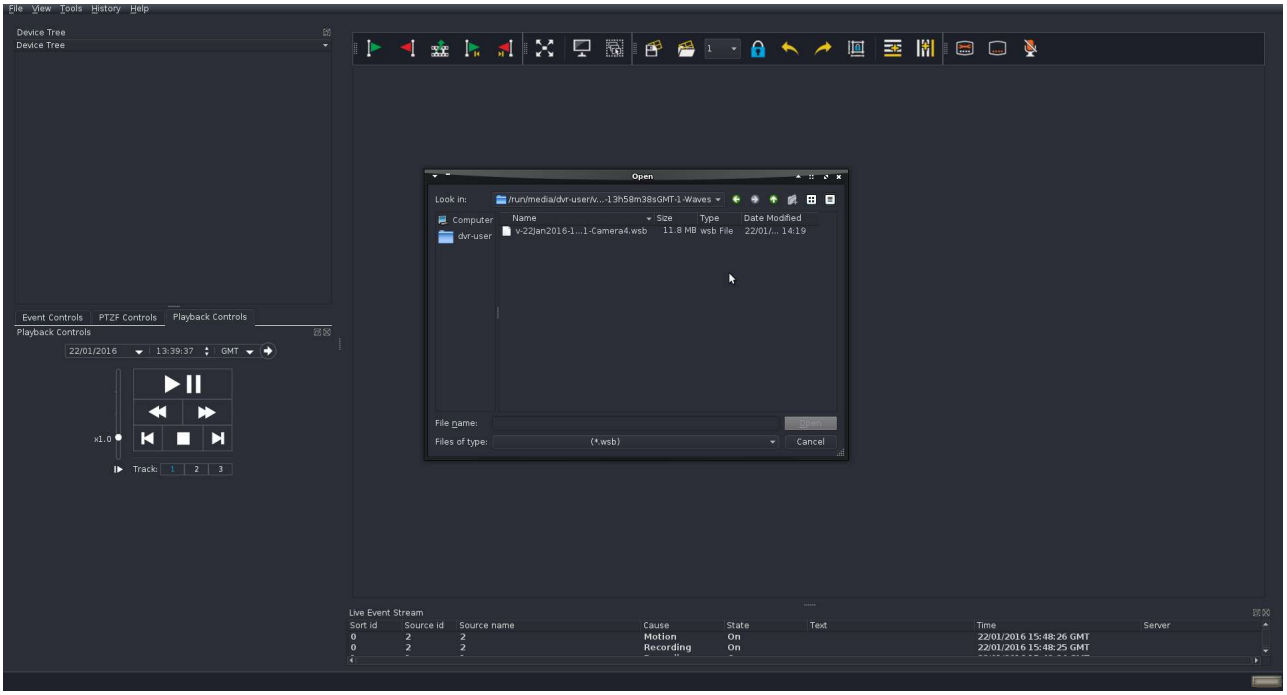


Figure 5.12: Find screen – Browsing directories to set Export path

- Click on the file name, and then click Open. The server and camera name(s) relating to the footage will now be displayed:

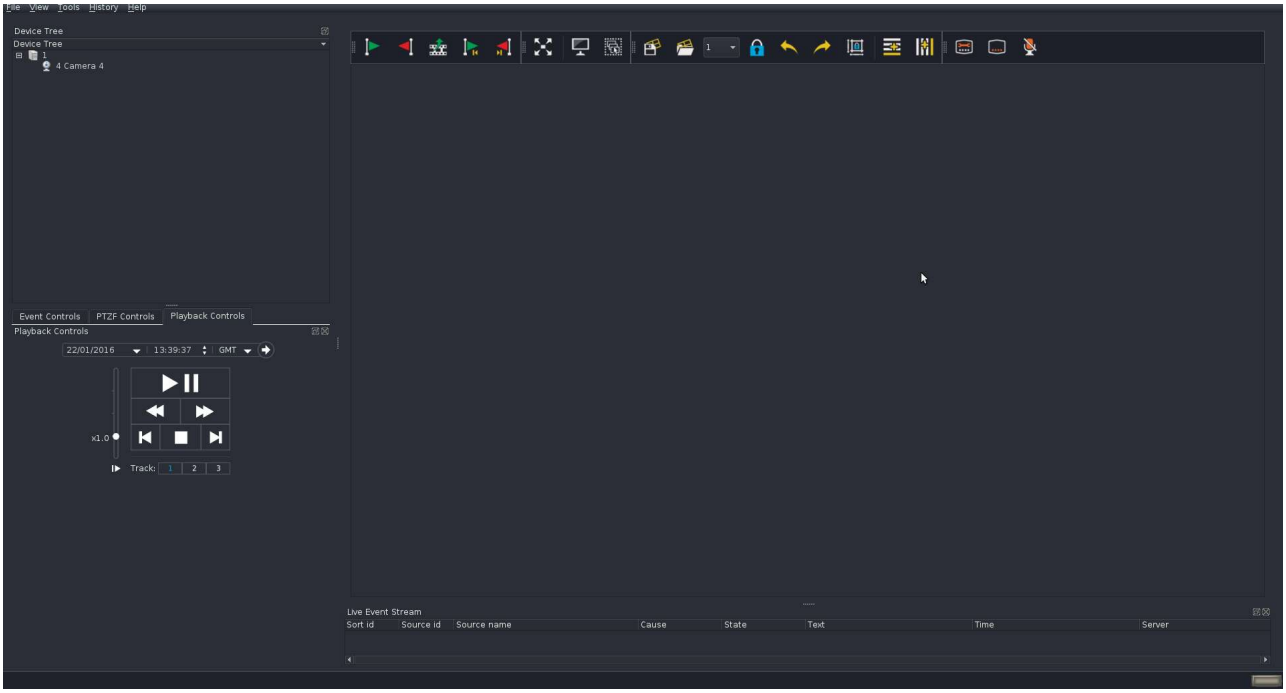


Figure 5.13: WSB file opened

- Double click on the camera name(s) that you wish to view (full details of the Playback controls are described in section 4.4 – Search/Playback):

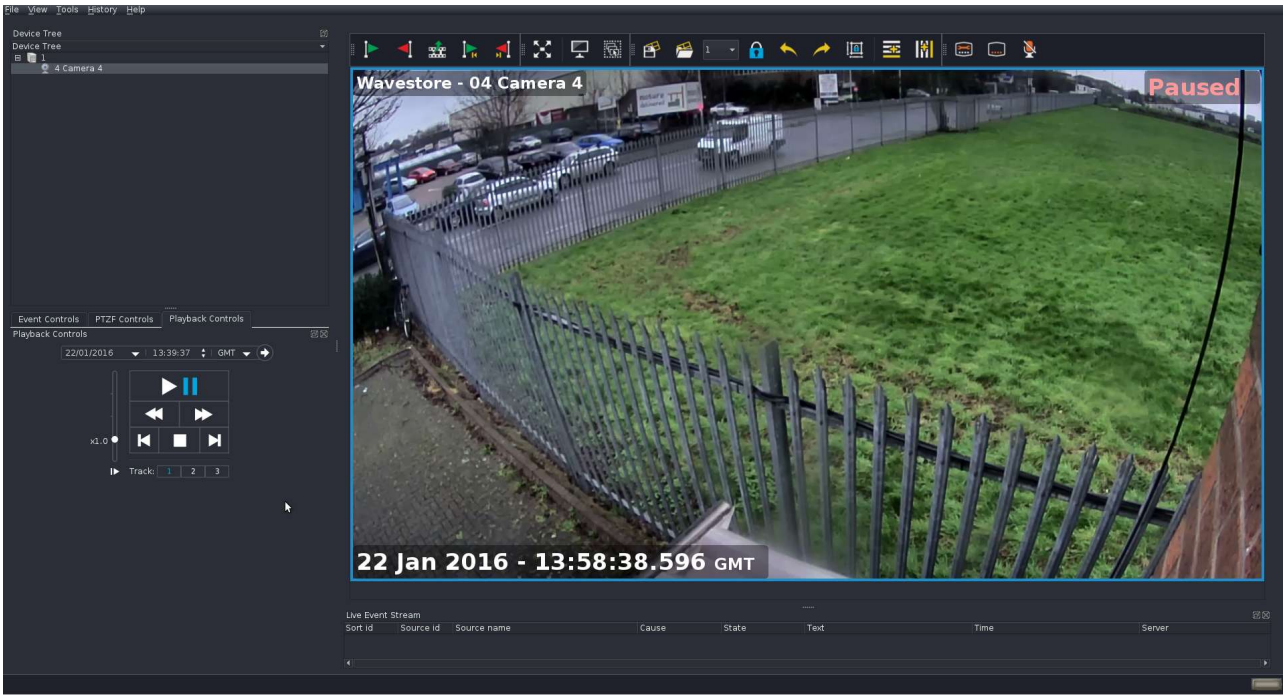


Figure 5.14: Camera opened

- Once you completed playback operations, follow the menu path File → Disconnect to close the file.

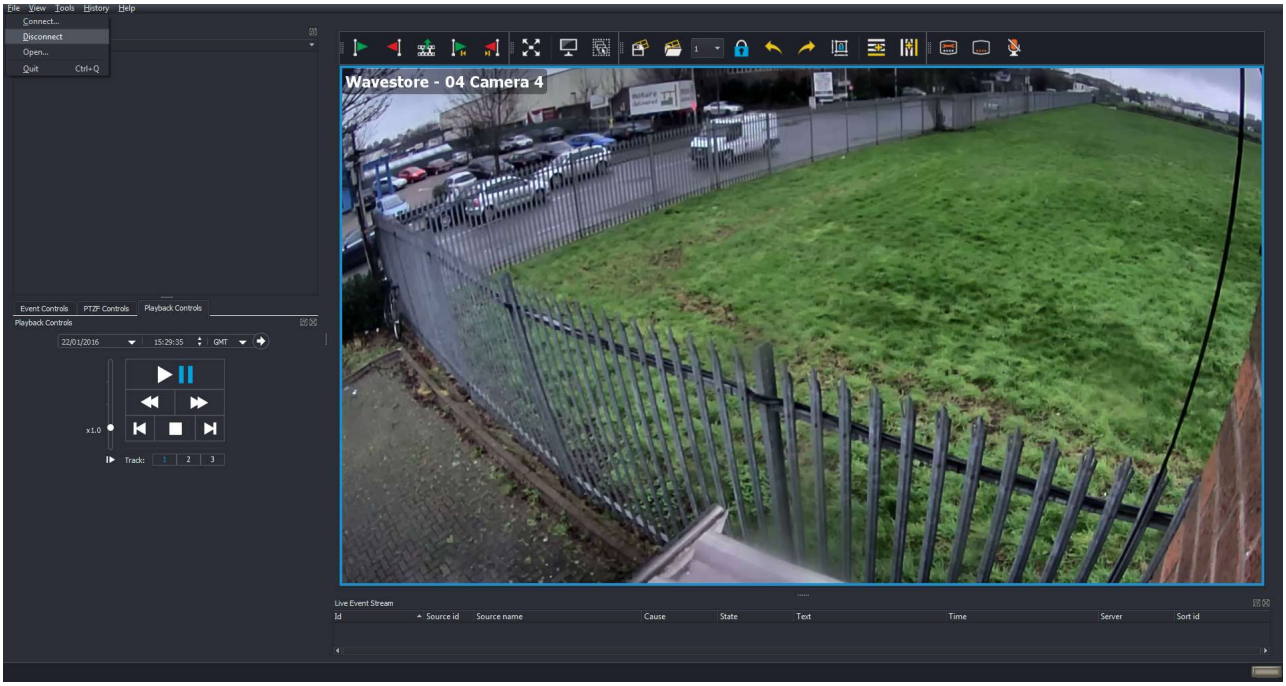


Figure 5.15: Closing WSB file

- You can now eject the DVD using the push button on the front of the DVD drive

5.3 Playing Back Exported Files on a Wavestore Server from a USB device

- Insert the USB device into the server, and move the mouse pointer into the very top left corner of the screen, so the Accessories Panel (containing the Internet, DVD burn and File Manager icons) appears at the top left of the screen as shown below:

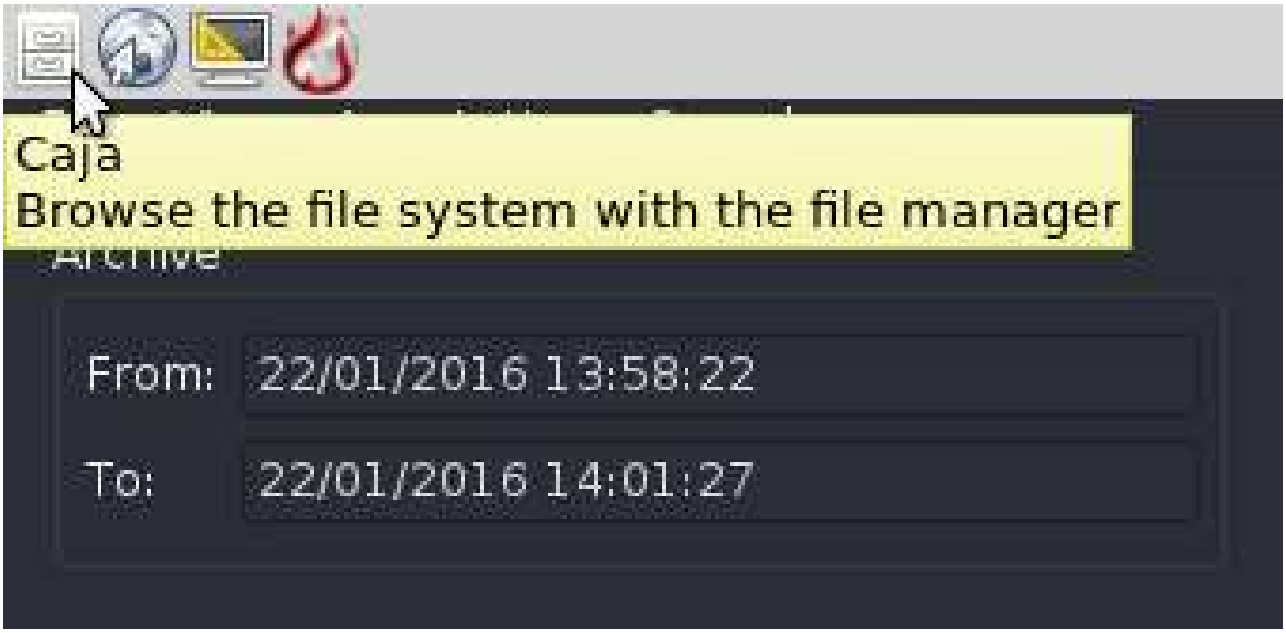


Figure 5.16: WaveView screen showing Accessories Panel

- Click on the File Manager icon (third icon across), and the File Manager window will open, with the left column in the window showing connected devices on the server and network, including your USB device. The right hand section of the window shows the files and folders contained on the selected device.

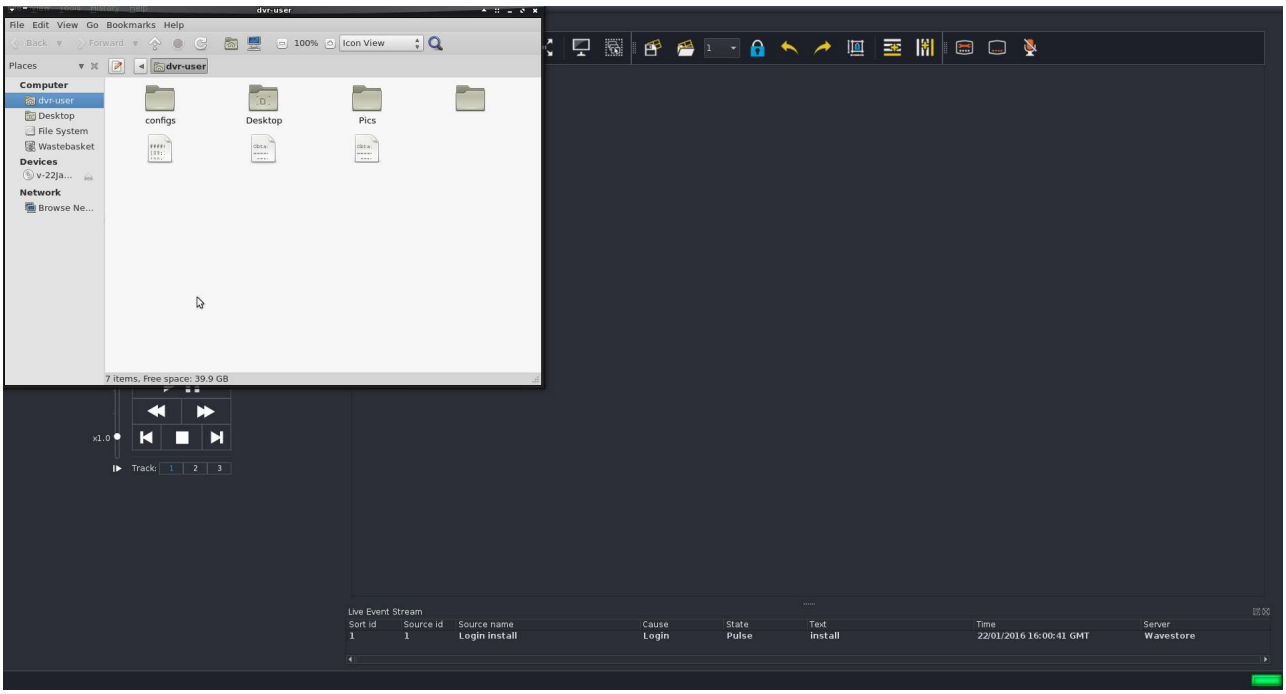


Figure 5.17: WaveView screen showing File Manager window

- On the device tree on the left, click on the USB device; files contained on the disc will now be displayed:

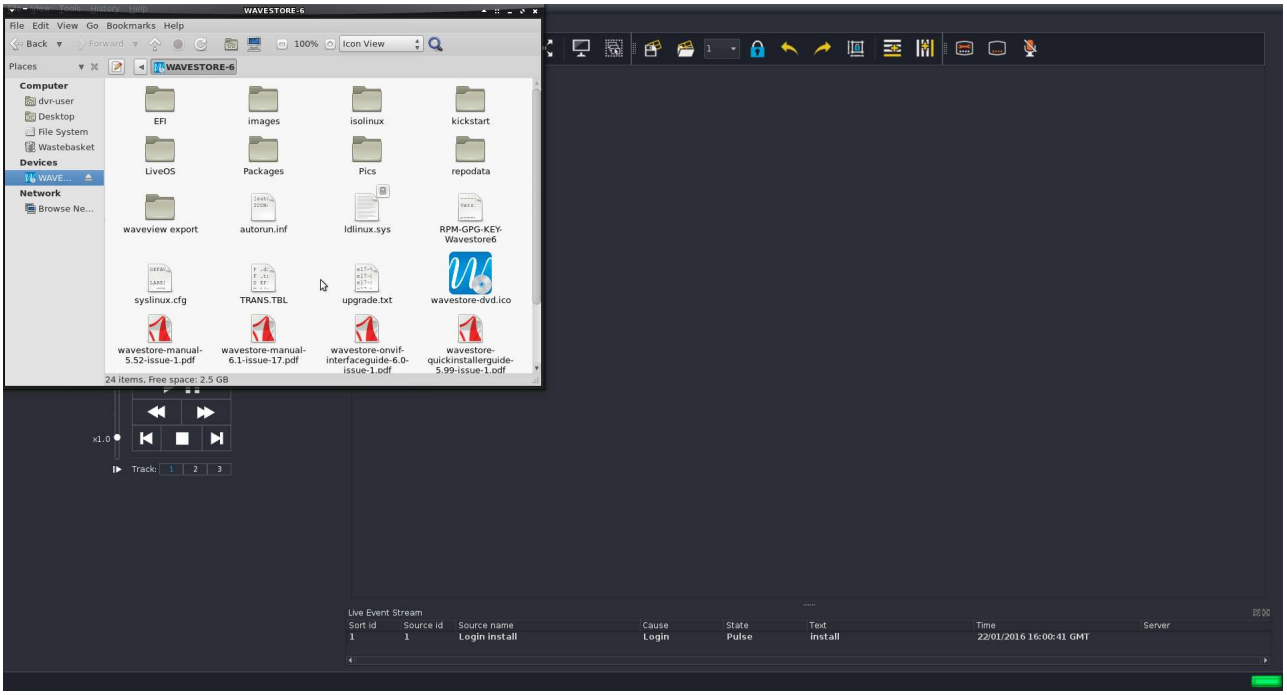


Figure 5.18: File Manager window showing contents of USB device

- The USB device is now mounted on the server, and you can now playback footage files from this device. To open a file, first disconnect from any servers that you are connected to (menu path File → Disconnect). Click on 'Open Export' in the Login Dialog box, and the Open dialog windows will appear as follows:

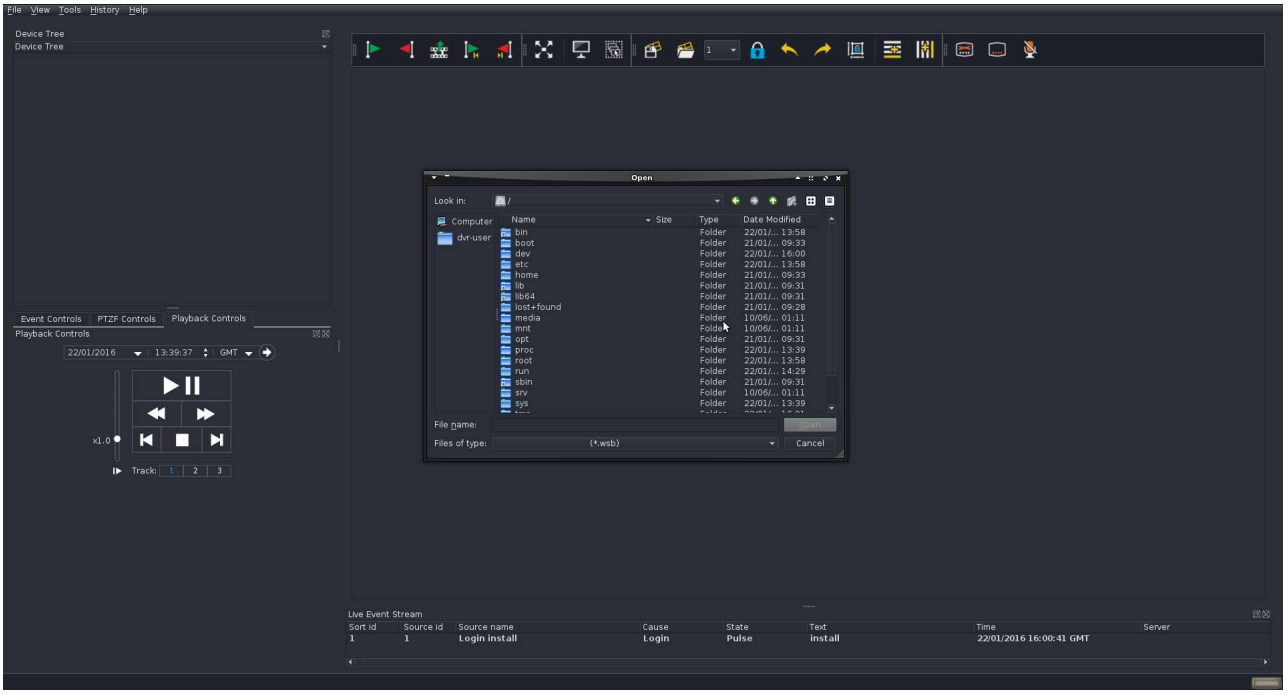


Figure 5.19: Browsing for USB device

- Click on the media folder:

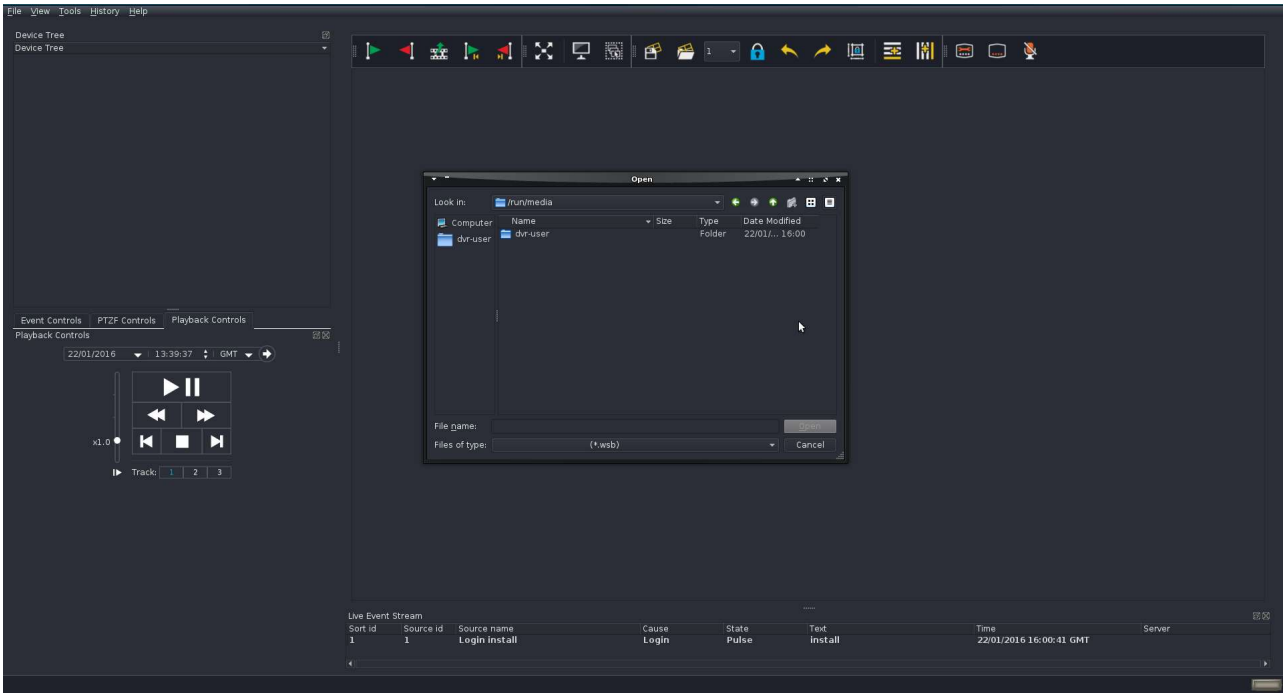


Figure 5.20: Browsing for USB device

- On the device tree on the left, click on the DVD; files contained on the disc will now be displayed:
- Click on the name of the device containing your footage:

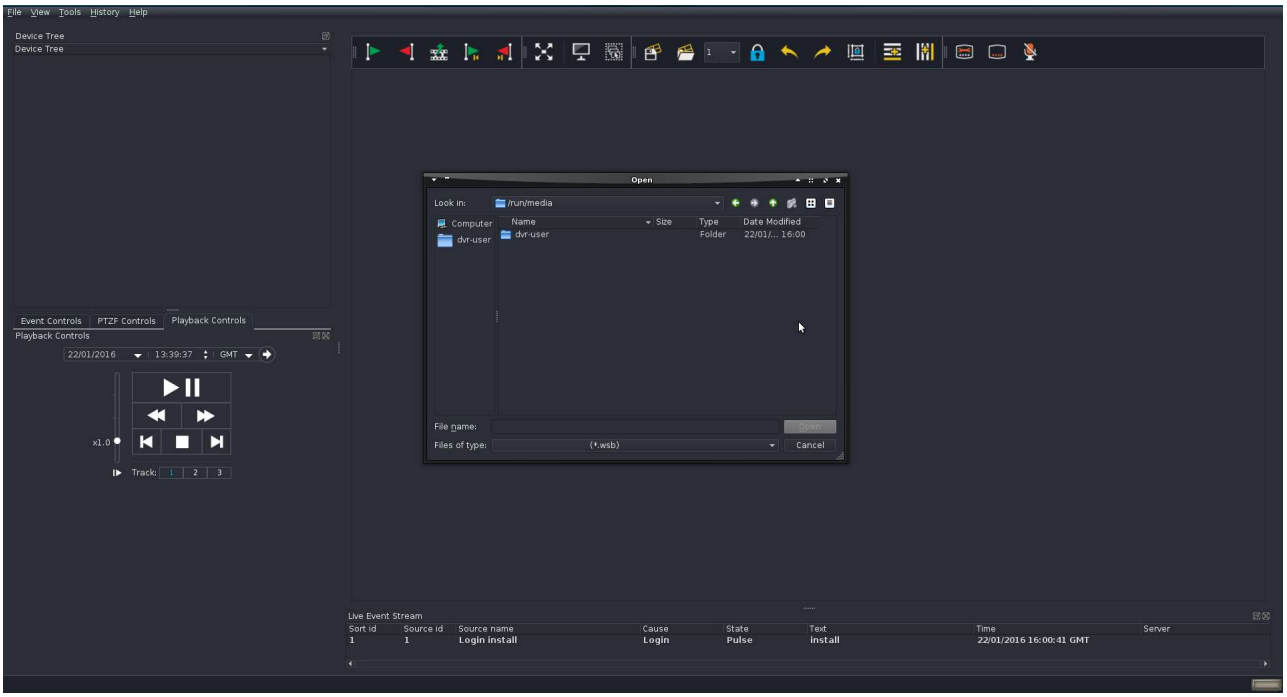


Figure 5.21: Browsing for USB device

- Click on Open:

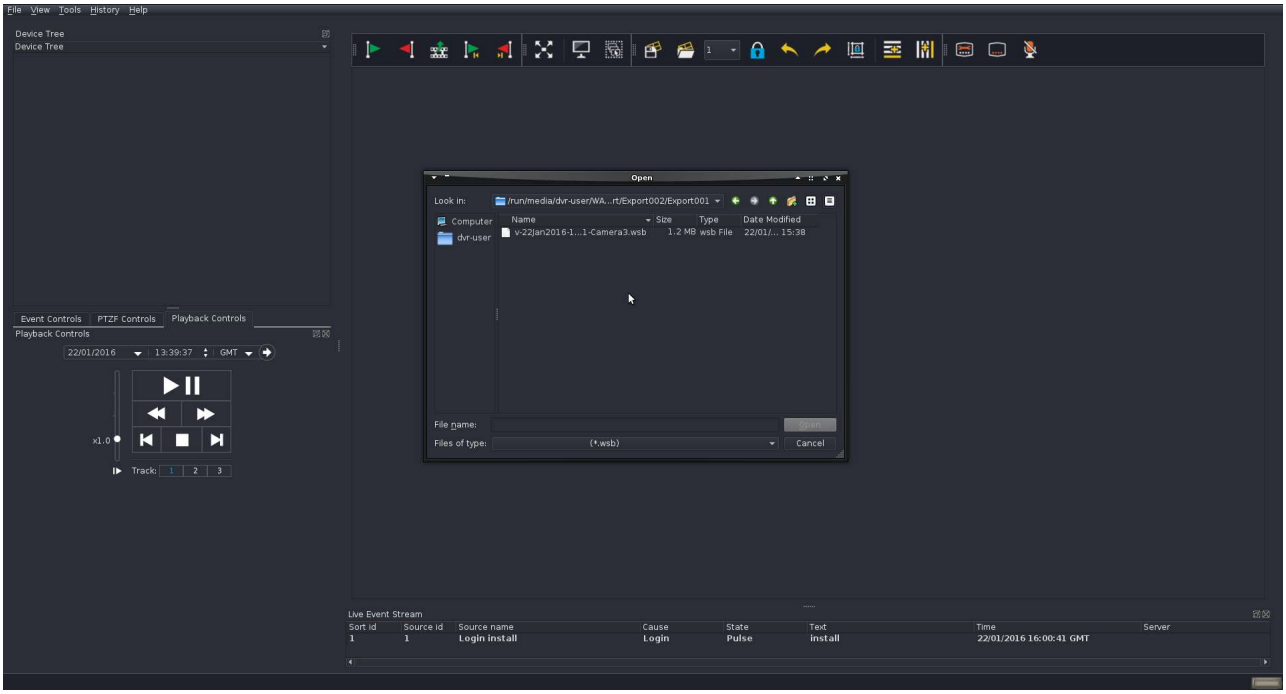


Figure 5.22: Open export directory

- Click on the file name, and then click Open. The server and camera name(s) relating to the footage will now be displayed:

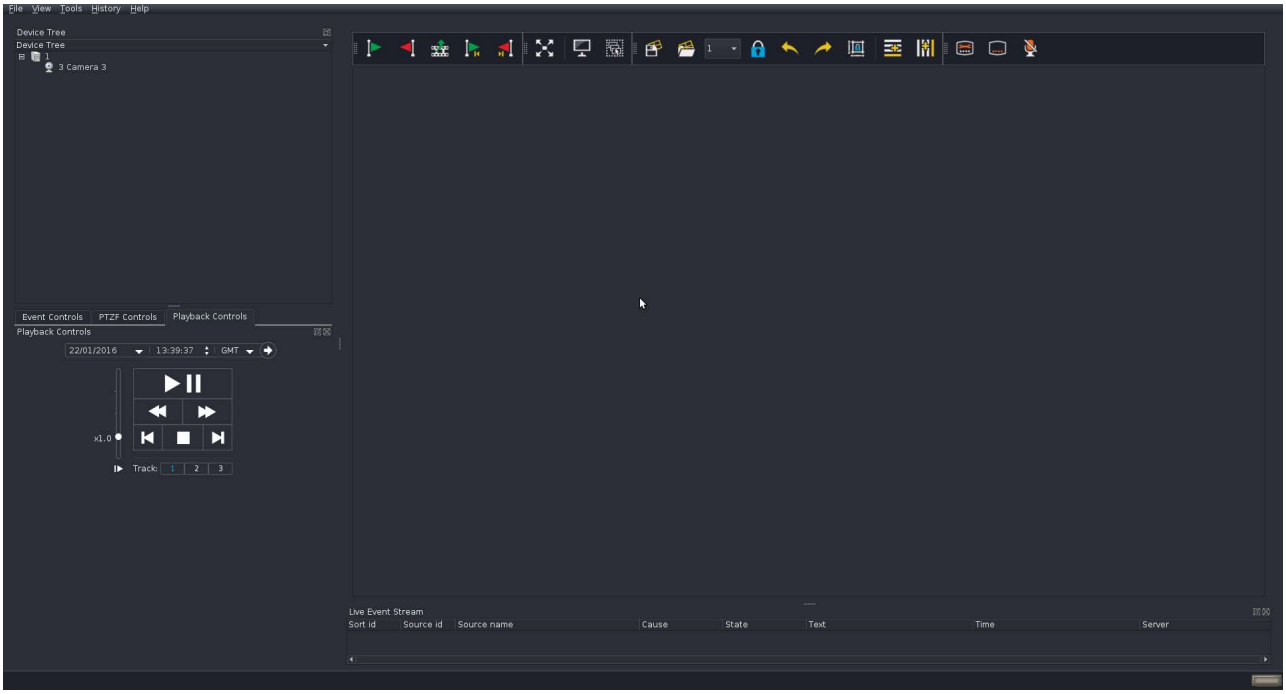


Figure 5.23: Main screen with WSB open

- Double click on the camera name(s) that you wish to view (full details of the Playback controls are described in section 3.10 – Playback Controls):

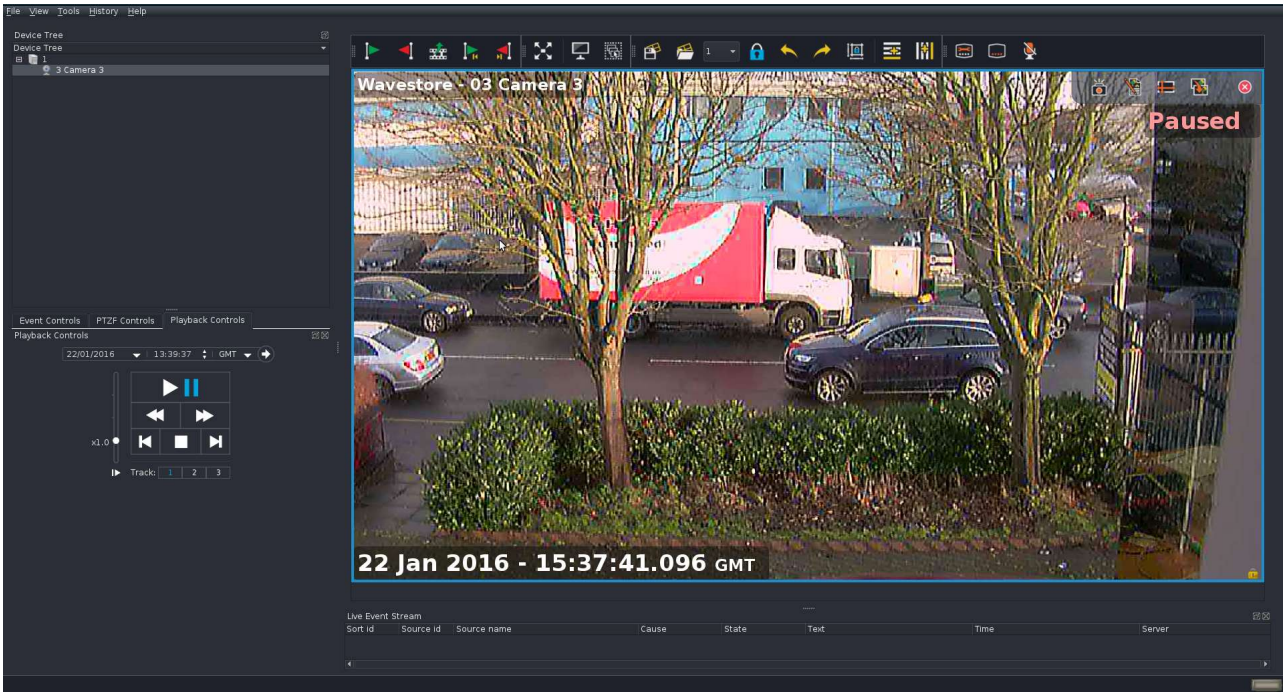


Figure 5.24: Camera opened from WSB file

- Once you completed playback operations, you must then 'unmount' the USB device before it can be removed from the server. Close the Find screen, and on the main WaveView screen, move the mouse pointer into the very top left corner of the screen, so the Accessories Panel appears at the top left of the screen as shown below:

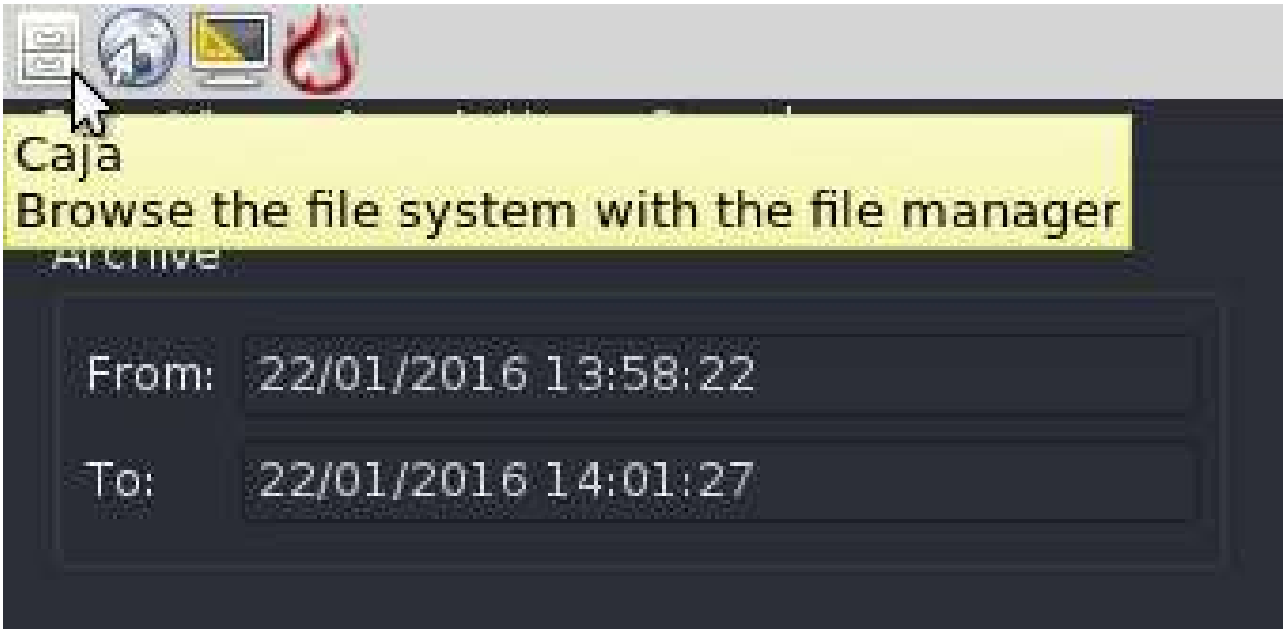


Figure 5.25: Accessories Toolbar

- Click on the File Manager Icon (third icon across), and the File Manager window will open, with the left column in the window showing connected devices on the server and network, including the

USB device.

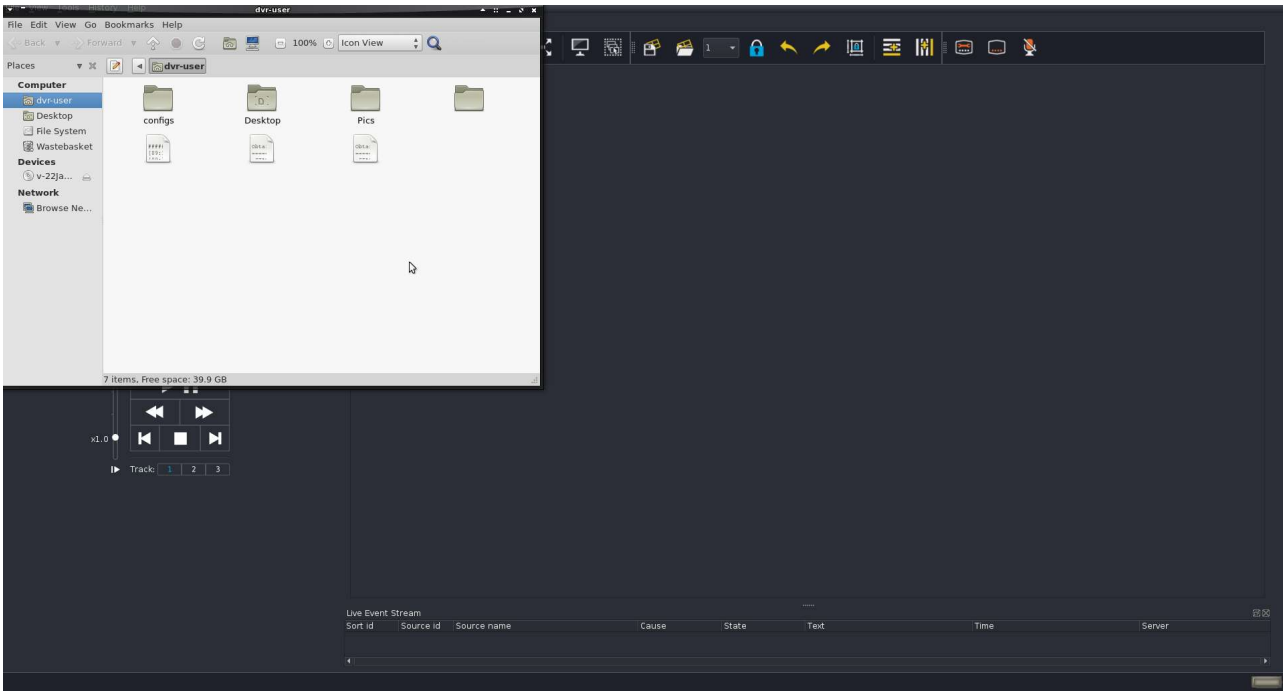


Figure 5.26: WaveView screen showing File Manager window

- On the device tree on the left, click on the USB device so it is highlighted blue:

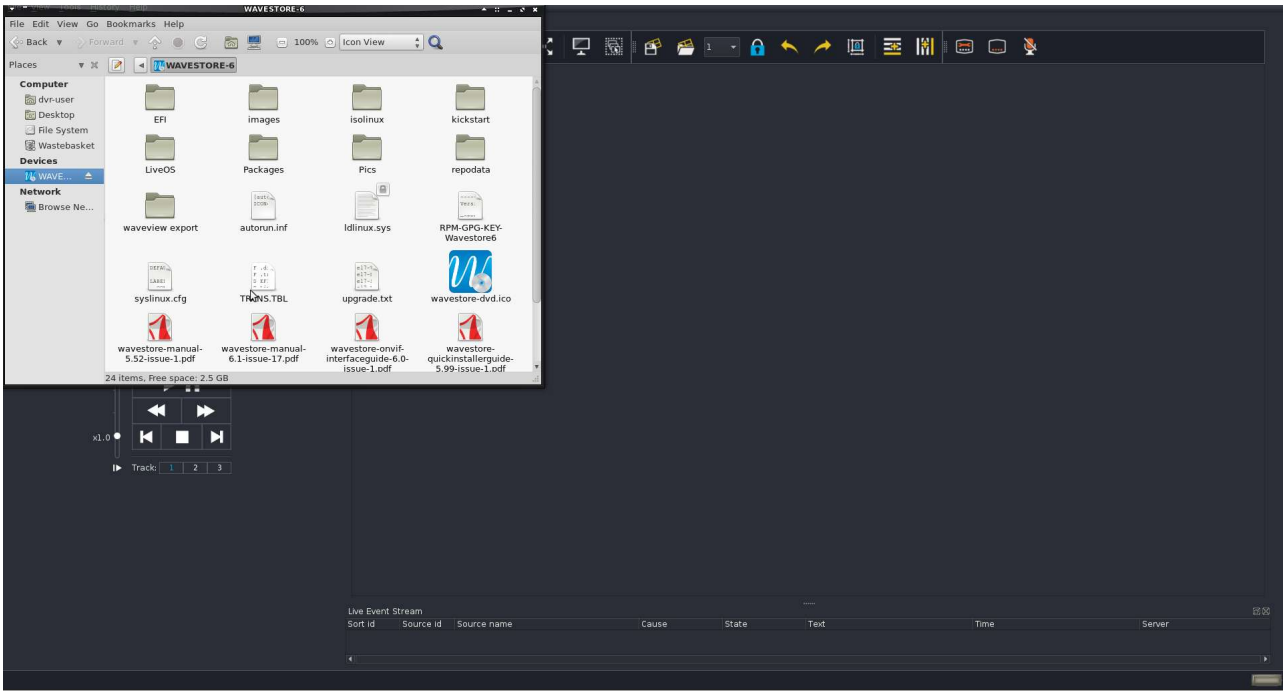


Figure 5.27: File Manager window showing contents of USB device

- Click on the 'eject' icon next to the name of the USB device to unmount the device. The USB device will now disappear from the File Manager display window will now display as below:

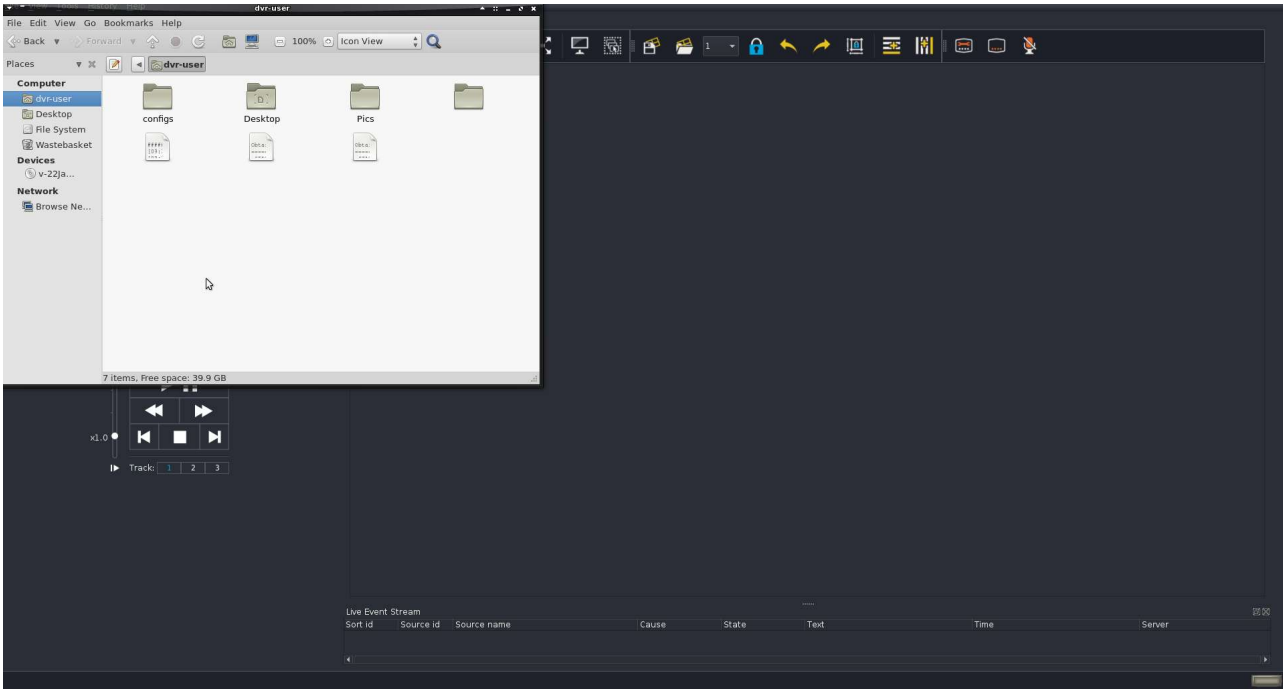


Figure 5.28: On the device tree on the left, click on the DVD; files contained on the disc will now be displayed:

- You can now remove the USB device from the server.

6 Setup Screens

The Wavestore Server is configured using the Setup Screen as shown (menu path View → Setup).

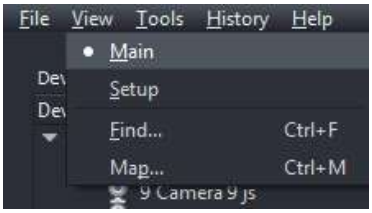


Figure 6.1: Accessing Setup Menu

The main Setup menu will now appear, displaying various submenus as shown below:

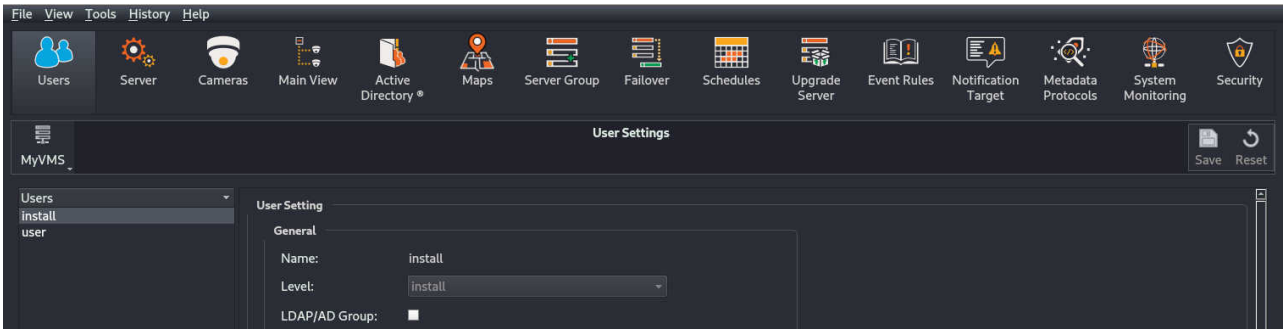


Figure 6.2: Setup Screen Sub-menus

If the horizontal size of your WaveView client window is too narrow to view all the submenu icons, you can move left/right though the icon list by positioning your mouse pointer at the left or right hand end of the list.

Click on any of the sub-menu icons to enter a menu.

To save any configuration changes you make in the Setup menus, click on the 'Save' icon (top right of screen).

If you wish to discard the changes that you have made, click on the 'Reset' icon.

If at any point you wish to exit from the Setup menu, follow the menu path View → Main.

At the top left of the main area is the Server Selector:

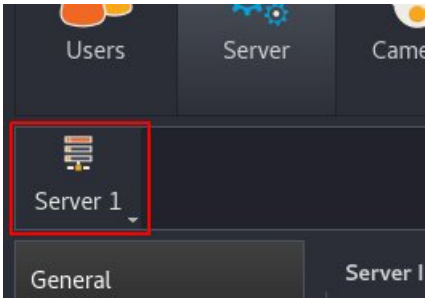


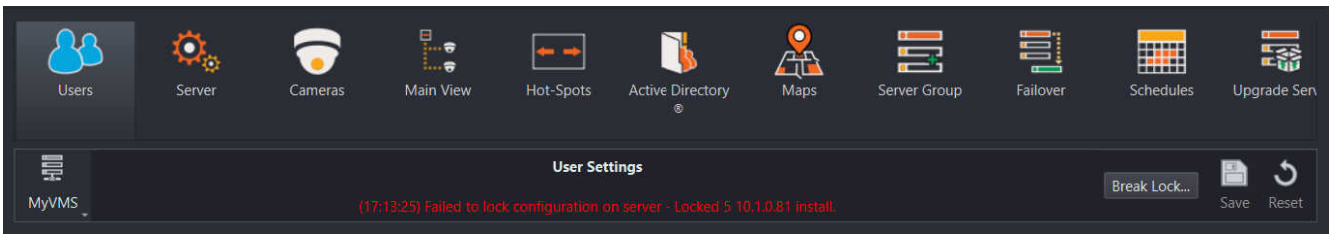
Figure 6.3: Server Selector

Clicking on this icon allows selection of a particular Wavestore server within a Server Group. If the currently selected setup page applies to the whole server group, then this icon will be disabled.

For setup screens which pertain to a server group, if there are inconsistencies between the configuration on different servers within the group, a Conflict Resolution tool will appear asking for the operator to choose the server with the correct configuration. This will then be synchronised to all the servers in the group. This is discussed in more detail in section 9.15 – Server Group Configuration Conflict Resolution.

Note: When entering a setup screen, the WaveView client will lock the configuration on the server or servers. If the setup screen in question pertains to the whole server group, all servers in the group will be locked. If the setup screen only pertains to a single server, only the selected server will be locked. This lock means that no other users can edit the configuration whilst you are editing it. The lock is released upon leaving the setup screens or by changing servers if on a setup screen that only pertains to a single server.

If the configuration is locked upon entering the setup screens, an error message will be shown which details the user and IP address of the user holding the lock.

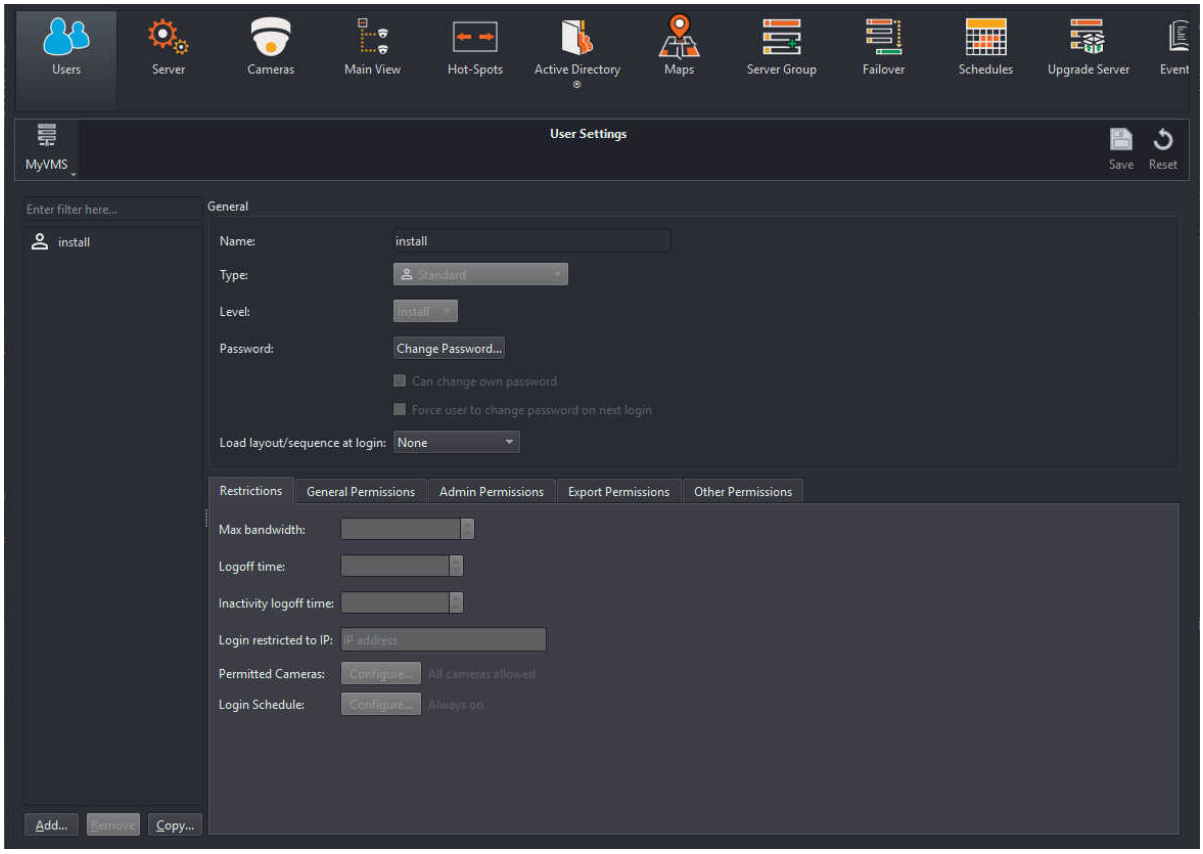


The "Break Lock" button can be used to deny the other user of the configuration lock and take it for yourself. That other user will then be unable to save their changes and likely have to redo any configuration that they were in the process of making.

6.1 Users

Click on the Users icon to enter the User Settings screen.

Note: The settings in this page apply to all servers in the server group.



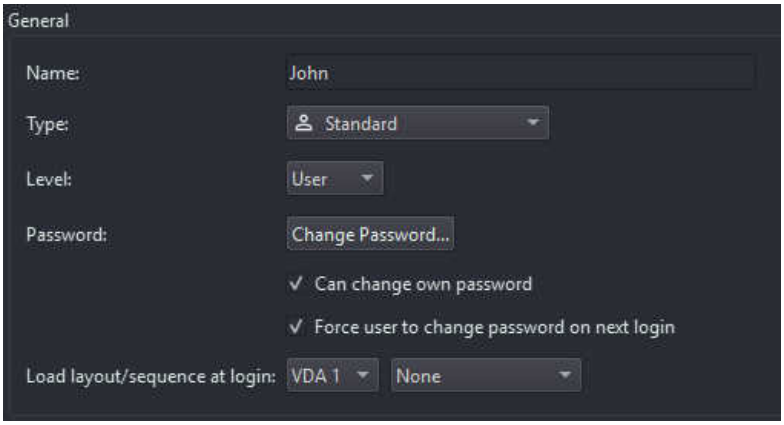
When the server is in its default state when new, the only user on the system is an "install" level user with username 'install' and password 'a'.

To add a new user ID, click 'Add', and enter the required name in the name field. Then click 'Change Password' and set a password for the user. It will not be possible to log in as that user until a password is set.

To erase a user ID, highlight the user name and click 'Remove'.

If you wish to edit the settings for a user, click on the name of that user in the Users list, and you can now edit settings for that user ID such as user level, password etc.

6.1.1 User Type, Level, and Preferences



We can configure the following options to apply to individual users:

Name The user name. Note that it is case-sensitive.

Type The type of user as described below:

User Type	Description
Standard	• The default, and recommended type of user. This user has access to all servers in the server group.
Local	• A user which only access to one server in the server group. The server is selectable.
Active Directory / LDAP	• This user is treated as a group rather than a user. You will not be able to log in as this user but the permissions set here will be inherited by any users who are a member of a group matching this user name in an Active Directory. See section 6.6 – Active Directory ® for more details.

Level The user's level. This gives some default permissions as described below:

User Level	Permissions
install	• Full access to all server functions
admin	• Configurable permissions for live view, search, playback, export • Able to create and edit admin and user level operators (but not install users) • Limited access to server configuration screens
user	• Configurable permissions for live view, search, playback, export • No access to server configuration

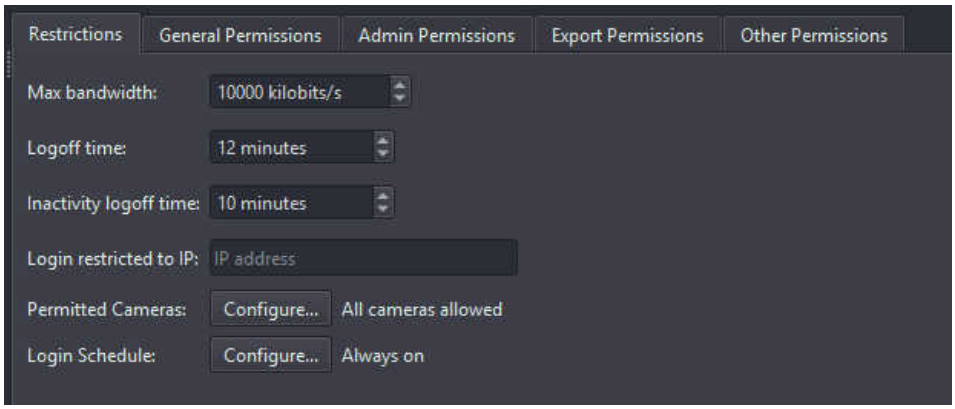
Change Password Allows changing of another user's password. This is not always permitted, for example if the selected user is of a higher level. Note that the currently logged–in user cannot change their own password here. To do so, use the *Tools → Change Password* menu.

Can change password Gives the user permission to change their own password

Force user to change password on next login The user will be forced to change password on the next login, but not on subsequent logins

Load layout/sequence at login Select to either load a previously saved Layout or Layout Sequence (see section 3.3 – Display Area Toolbar), or select 'Automatic' to reload the layout that was being viewed when the user last logged out. This can be configured on a per VDA (Video Display Area) basis.

6.1.2 Restrictions



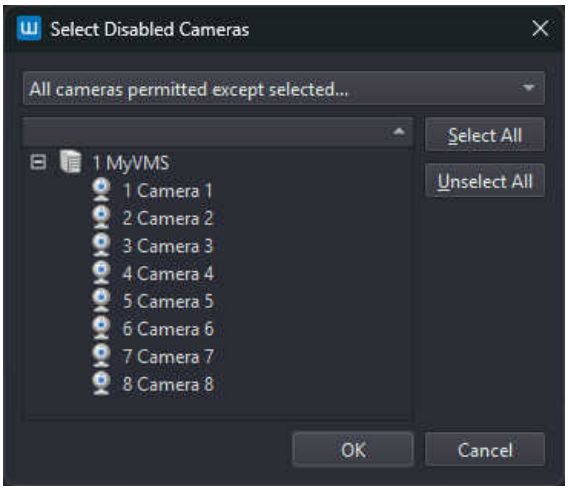
Max Bandwidth Permitted bandwidth for the user's connection

Logoff Time Sets a maximum duration for the user's logged in session

Inactivity Logoff Time Sets a maximum inactivity duration before the user is automatically logged out

Login restricted to IP This allows restricting this user's login to one or more IP addresses. Substrings can be used, for example "127. [::1]" (without the quotes) matches only local connections, or "192.168. [fd01::" matches only IP addresses starting with those values.

Permitted Cameras Controls permissions for which cameras (and other channels) this user is permitted or denied access to...

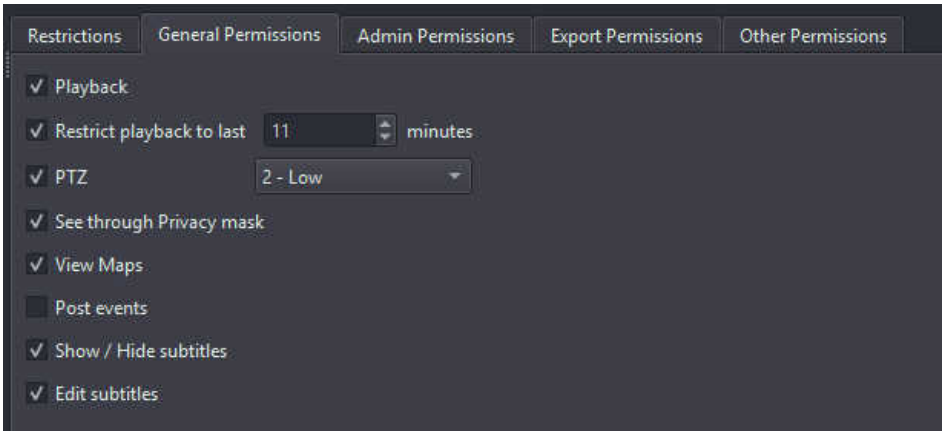


It is possible to choose either an "allow list" or "deny list" mode via the drop-down selection. These are shown as "All cameras permitted except selected..." and "All cameras denied except selected...". This selectable behaviour is useful when the system is being extended with new cameras as it affects default visibility of newly added cameras. This mode is available per-user.

The cameras selected in the user interface are either permitted or denied to the user based upon the mode selected.

Login Schedule Access to the server can be limited to times defined by a schedule (configured in the Schedules menu – see section 6.10 – Schedules)).

6.1.3 General Permissions



Playback Permission to Search and Playback recorded footage. Note that this option should always be enabled when using encrypted recordings otherwise live view will not function correctly.

Restrict playback to last N minutes If enabled, playback is restricted the last N minutes. Older recordings cannot be viewed by this user.

PTZ (and Priority) Priority level for PTZ control, if enabled. 1 is the lowest priority and 5 is the highest. If multiple users attempt to control the camera at the same time, the user with the highest priority will have control.

See through Privacy mask If enabled, privacy masks are not enforced for this user.

View Maps Permission to use the Maps functionality.

Post events External systems which send events to the Wavestore must provide a username and password. This permission controls whether a user is allowed to send events from the outside. For security reasons it is advisable to leave this disabled (the default) unless a particular mechanism for sending events is being set up.

Show/Hide subtitles Controls whether the user is allowed to show or hide the subtitles.

Edit subtitles Controls whether the user is allowed to configure subtitle settings.

6.1.4 Admin Permissions

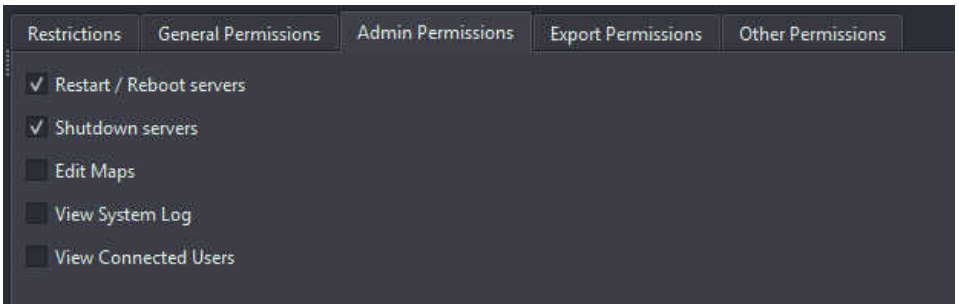


Figure 6.4: Admin Permissions

These permissions are only available for "admin"–level users. "install"–level users always have these permissions and "user"–level users can never have them.

Restart / Reboot servers Allows a Wavestore to be restarted (software restart) or rebooted.

Shutdown servers Allows a Wavestore to be shut down.

Edit Maps Allows the user to edit the system maps.

View System Log Allows access to the System Log.

View Connected Users Allows access to a list of currently connected users.

6.1.5 Export Permissions

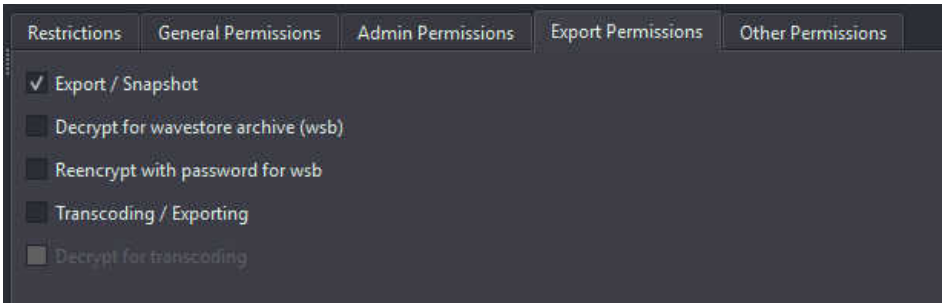


Figure 6.5: User Permissions for Export

Export Controls whether users are allowed to create exports. Either WSB format or transcoded to another format. If this option is disabled then other export permissions are not available as they are not relevant.

Decrypt for Wavestore archive (wsb) If the source video is encrypted and the user wants to decrypt the video before writing it to a WSB export file unencrypted, this permission must be granted.

Re-encrypt with password for wsb If this permission is granted, the user can create a WSB export file with password protection.

Transcoding/exporting If this permission is granted, the user can write to formats other than WSB, e.g. AVI or MOV.

Decrypt for transcoding If this permission is granted and the source video is encrypted, the user can decrypt the video before writing it in another format, e.g. AVI or MOV.

6.1.6 Other Permissions

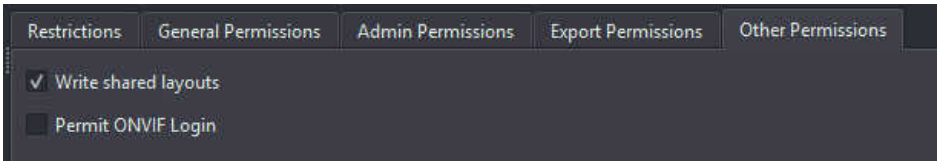


Figure 6.6: Other Permissions

Write shared layouts Determines whether the user can write, overwrite, and delete shared layouts

Permit ONVIF login Controls whether external systems should be able to login as this user using the ONVIF protocol. Note: this is less secure than the default Wavestore password system, see technical note below.

Technical note regarding ONVIF Login: ONVIF mandates either 'WS-UsernameToken' or 'HTTP Digest' login, and both of these require the device to store the passwords using reversible encryption so they can the retrieved to validate the login password. Normally the Wavestore server uses a much more secure password storage (a one-way hash with 10,000 iterations) which is not reversible and can be use for the validation of the password using the secure Wavestore protocol login, but this cannot be used for the

ONVIF–mandated login procedure because it is not reversible. Therefore, allowing ONVIF login reduces the security of the login for the associated user.

6.2 Server

The 'Server' setup screen contains a list of selectable sub–sections to configure various aspects of the currently selected server.

These are detailed in the following sections.

6.2.1 General

Server Information

The ***General*** submenu gives server information such as server name, status, IP address and server software version.

Note that the IP address shown is the address that was used to connect to the server. The server might have many IP addresses. Full details of the network configuration can be inspected in the Network Setup screen – see section 6.2.2 – Network.

A 'friendly' server name can be configured by clicking in the 'Name' field in the General panel, and replacing 'Wavestore' with the new name. It is recommended to give each server an individual 'friendly' name, to prevent confusion when viewing cameras or configuration information from different servers within a group (e.g. connected devices, system log).

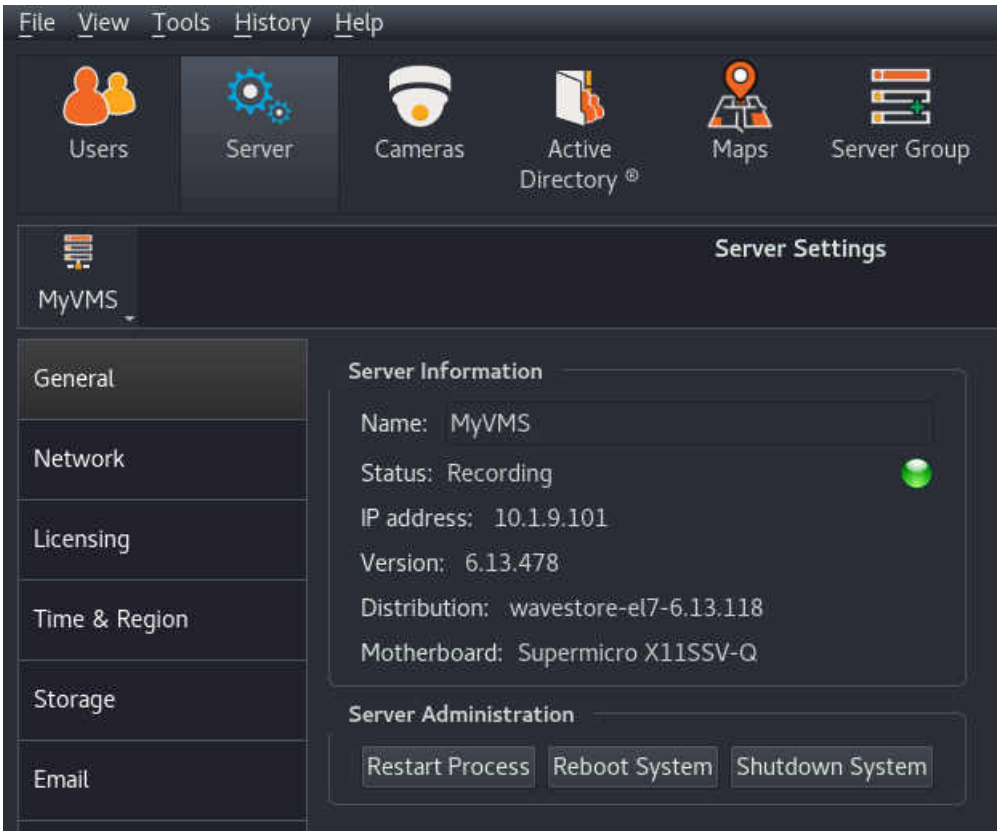


Figure 6.7: Server Setup Screen – General Page

Server Administration

The Server Administration submenu allows the server to be shutdown, the Server software program to be restarted, or the server completely rebooted. During the last operations, the client software will disconnect temporarily, and then reconnect once the server is back online.

6.2.2 Network

The Network setup page allows configuration of network interfaces as well as creating secondary and bond interfaces. This section explains how this configuration can be made.

The default configuration for all network interfaces is use DHCP (automatic IP address allocation). If a DHCP server is available, an IP address will be automatically obtained and this will be displayed in the "Current Interface Status" for the selected interface as shown below:

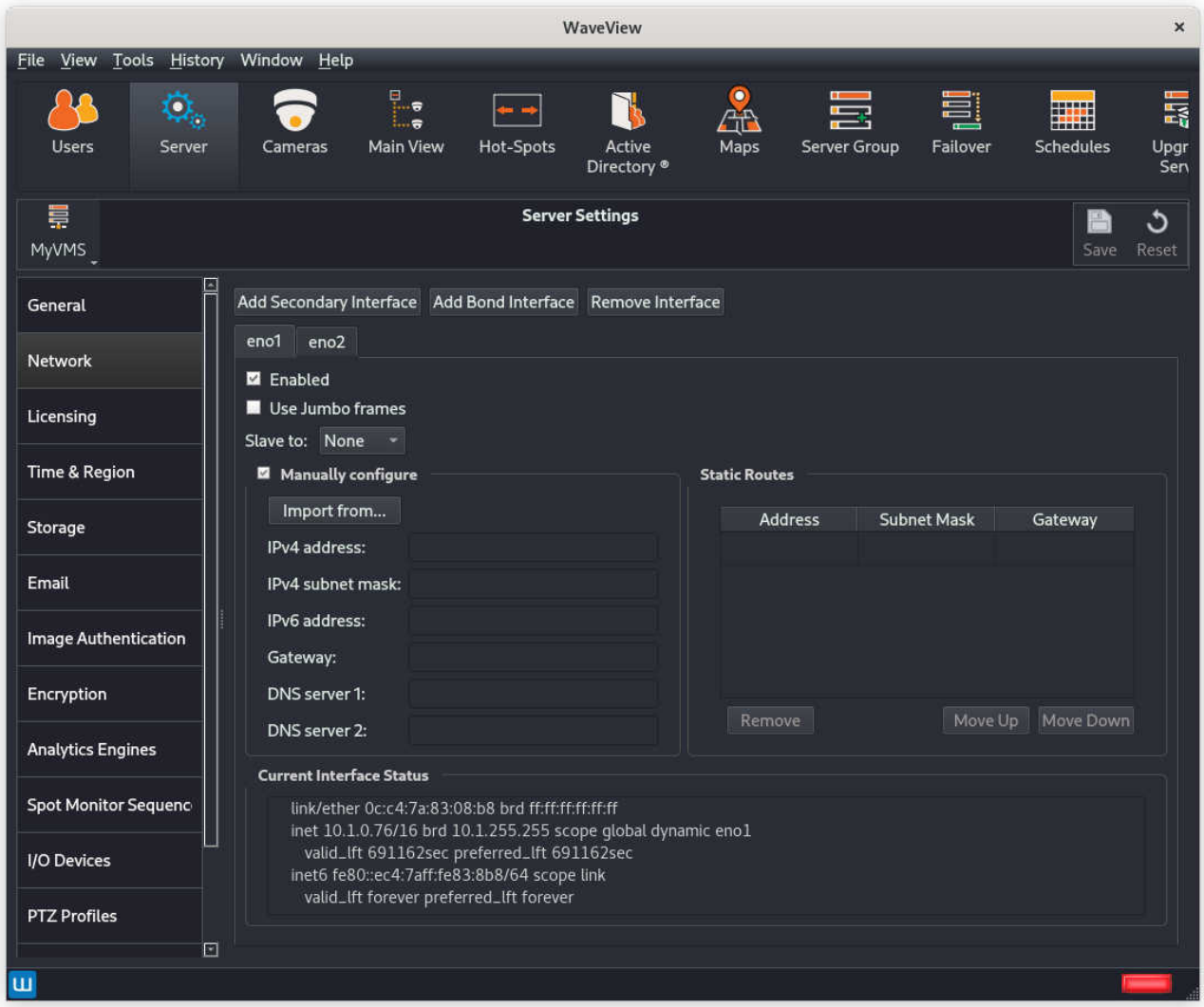


Figure 6.8: Confirming server IP address allocated by DHCP server

If the Wavestore server cannot find a DHCP server on the local network, it will have no IP address.

If you wish to manually configure the IP address for a network adaptor on the Wavestore server, click to select the adaptor you wish to set up, and select 'Manually Configure'.

A server may have multiple network adaptors, for example if the case of a server that has one adaptor connected to IP cameras, and the second adaptor connected to the site LAN/client PCs etc. Each network adaptor on your server is represented by an tab with a network name associated, eg, `enp3s0`. These names will vary depending on the hardware: see the hardware document for details of the names of the ports on the back of the machine. Select the adaptor that you wish to configure, by clicking on the tab.

The settings for this adaptor will now be displayed.

Select 'Enable' to allow the network adapter to be used, otherwise it is diabled and is not assigned an ip address and behaves as if it is not present.

The 'Use Jumbo Frames' tick box enables a larger network MTU size of 9000 bytes. Normal frame size is quite small for modern fast gigabit networks, and jumbo frames are a way of making frames larger and more efficient, but this is not fully standardised and therefore this option is not enabled by default.

The 'Slave to' box allows bonding (see section below). Leave as None for normal operation.

To set an IP address, tick the 'Manually Configure' tick box, and enter the IP address, subnet mask and gateway for your server in the relevant fields.

The 'Current Interface Status' box displays various information about the currently selected interface.

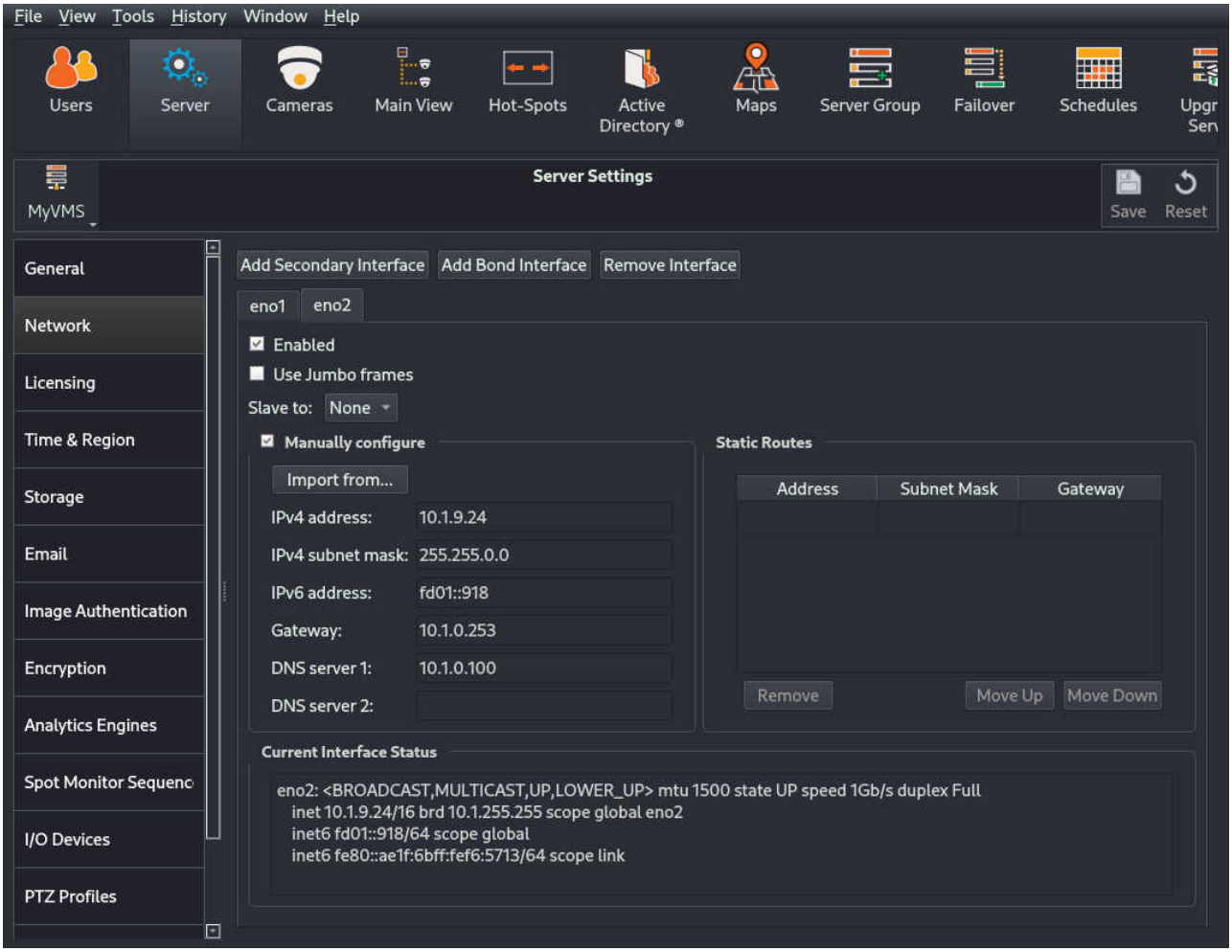


Figure 6.9: Manually configuring IP address

Note that Wavestore servers use TCP port 8601 to communicate. If it is necessary for a client outside a firewall to contact a server within a firewall, for example connecting to servers on a site over the internet, then port forwarding for port 8601 must be configured on the firewall/router at the site.

Static Routes

Static routes can be configured for each interface using the provided table. Each route should define an Address, Subnet Mask, and Gateway.

The static route is for traffic to the range defined by Address/Subnet Mask which will be initially routed to the address specified by Gateway. For example:

- Address: 192.168.1.0
- Subnet Mask: 255.255.255.0
- Gateway: 10.2.1.250

This route would define that all requests to the 192.168.1.0 network should be sent via the address 10.2.1.250.

Secondary Network Addresses

A single network interface can have more than one network address. This might be useful if it needs to connect to cameras two separate subnets, for example 192.168.x.x and 10.1.x.x. It can also be used for 'Failover' where each machine has a physical address which os fixed, and in addition has a separate logical address which moves to a new machine when when that machine fails.

To add a secondary interface address, first enable the tab for the interface adapter required and then click the 'Add secondary interface' button.

The tab for the secondary interface is displayed and can be configured. Secondary interfaces end with `:1`, for example, `enp3s0:1`. The secondary interface can be enabled and set up as if it was a normal network interface.

It is not normally required to enter DNS or Gateway settings for a secondary interface, as it will use the settings from the primary interface.

If desired to remove a secondary interface, select the appropriate tab and click 'Remove interface'.

Port Bonding

In many cases it is desirable to treat all the network interfaces on the machine as a single interface with a single IP address. If one network interface fails or the cable is broken, the others will continue to work. And if all are working, they share the data between them which increases the total network bandwidth linearly.

To set up Bonding, first add a Bond interface by clicking the 'Add bond interface' button, then click on the tab which will have a name like `bond0` to select it.

The bond interface can be enabled and set up as if it was a normal network interface and it can have an IP address assigned.

All physical interfaces which are to be bonded to `bond0` need to have their 'Slave to' set up to `bond0`. If you make a physical interface a slave to a Bond master, then you do not assign an IP address to it, it is just treated as a data path for the master bond interface.

If you have a number of network interfaces on the hardware, it's possible to set some interfaces as bonded, and keep others independant. It's also possible to set multiple Bond interfaces, depending on your network requirements.

Wavestore default bonding is "round-robin" or "Static" mode which shares the load over all the operational links in both directions. This is widely used and the network links should be configured at both ends as bonded (trunked). This is sometimes known as Static trunking or Static bonding.

More advanced information and trouble-shooting tips relating to port bonding can be found on the Wavestore knowledgebase.

6.2.3 Licensing

Each Wavestore server requires a valid licence to enable all system functionality.

There are two main ways of licensing a Wavestore server:

- By entering a valid Server Licence, which is a string of text. This method does not require an internet connection.

- By obtaining a licence subscription. This method does require an internet connection.

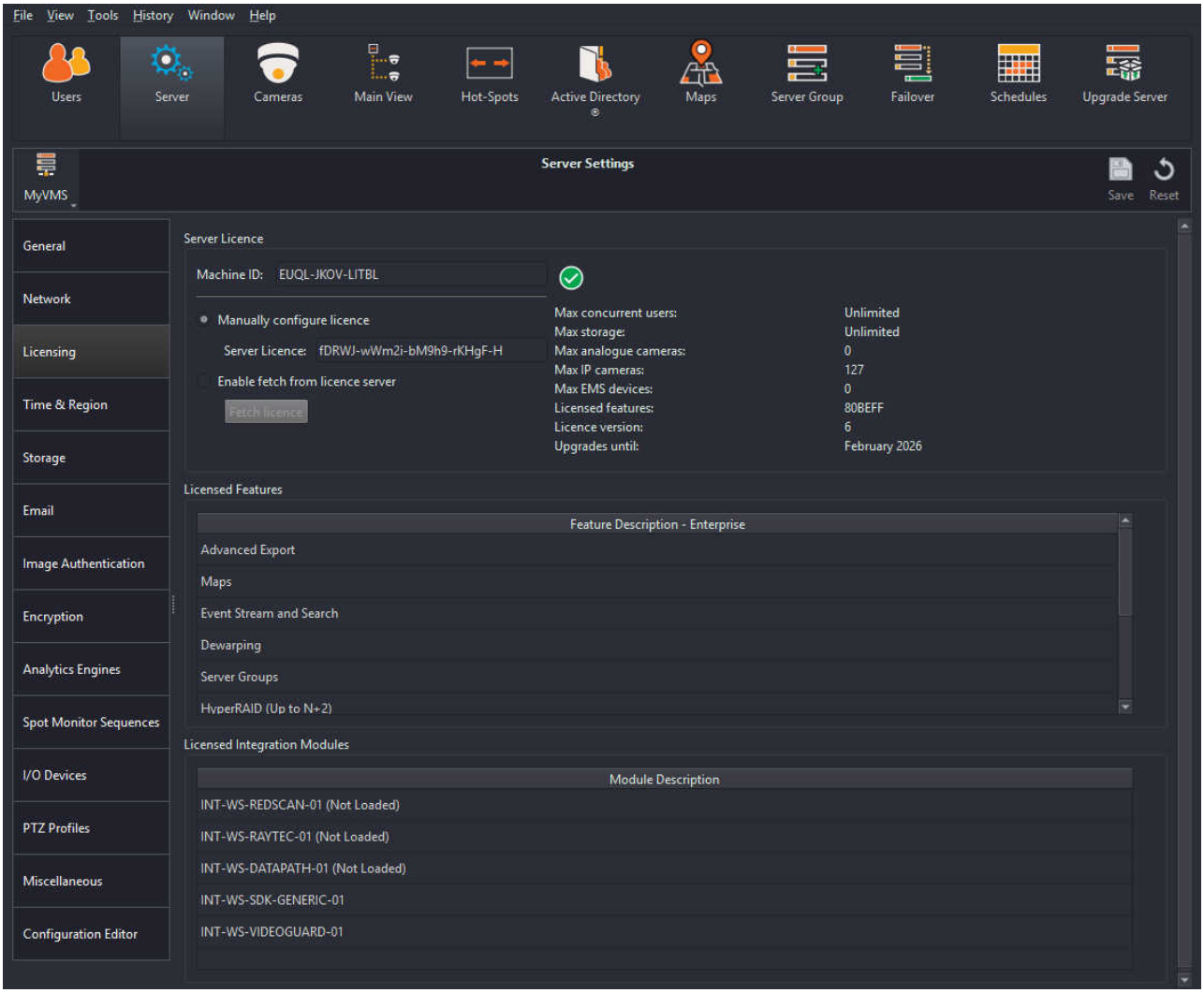


Figure 6.10: Licensing Setup Page

A licence of either type is specific to a particular Wavestore server's MachineID which is unique to each server and cannot be edited.

In the Licensing setup screen, the ***Manually configure licence*** option allows the Server Licence to be manually entered. If using Subscription Licensing, select the ***Enable fetch from licence server*** option. The Wavestore server will then automatically retrieve an up-to-date licence when required. The ***Fetch licence*** button can be clicked to force the Wavestore server to check for a new licence immediately.

When using a textual Server Licence, it is recommended to make a note of the licence in case a software reinstallation is required in future. A charge may apply for reissuing a Wavestore licence if the original licence details are is lost. If the licence is lost, please contact Wavestore Global with the following details:

- Wavestore Server Serial Number
- Machine ID

The Wavestore server must have a valid licence before the server can be configured for recording. Charge-

able licence upgrades can be requested to increase functionality of the server (e.g. increase number of IP camera channels or client software connections); in such cases the licence is field upgradeable, and the server does not have to be returned to Wavestore.

This licence controls the following settings:

- Number of simultaneous WaveView Client Software connections to the server
- Number of Analogue Camera Channels
- Number of IP Camera Channels
- Number of EMS (Encoder and Multi–Sensor) Camera Channels
- Licensed Software Functions such as Advanced Exports, Live Events Stream, Maps, Server Groups, integration modules, Metadata support etc.
- "Upgrades until" – this is the date after which it will no longer possible to upgrade the server to a later version. Note that for some older servers this may show a version number instead of a date. Licence upgrades can be purchased to extend the upgrade period of the server.

6.2.4 Time & Region

The Time and Region menu allows the configuration of the server time, time zone, and time synchronisation to another device (e.g. Wavestore server or NTP time source).

We recommend that you configure the server time and date before you start recording footage from audio/video devices. Alternatively, if you make a large change in the time/date, reformat the server hard disks after you have carried this out.

Region Settings

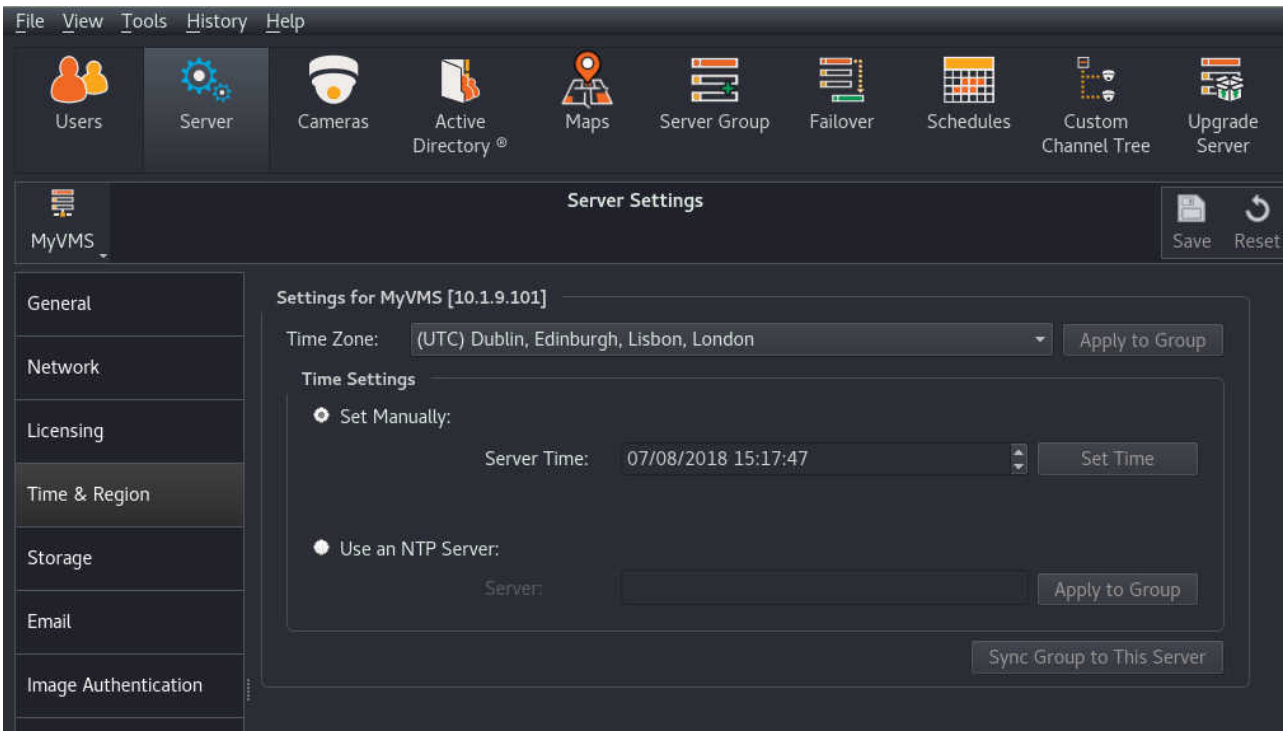


Figure 6.11: Time and Region settings

The server hardware's own internal clock is set to the UTC time zone (BIOS settings). Using the Wavestore software, we can apply an offset for the local Time Zone, including local daylight saving changes; you should carry this out prior to setting the time.

To configure, select the region that you require from the dropdown menu, then click 'Save'. You will now be prompted to restart the server.

Once the server software has restarted, confirm that the correct time is displayed in the 'Server Time' field. If not, you can adjust the time as described below.

Time Settings – Manual

Before adjusting the time, confirm that the correct Time Zone has been selected (as described in section 6.2.4 –). Enter the current time, click the 'Set Time' button, then click on 'Save'

For a small change in time (less than 29 minutes), the server time will slew slowly by approximately 1 second per minute, until the desired time is reached. This ensures the time stamp on the footage never jumps, which would be confusing, and in particular it never jumps backwards.

This behaviour occurs irrespective of the time source: it behaves the same when using NTP and when setting the time manually.

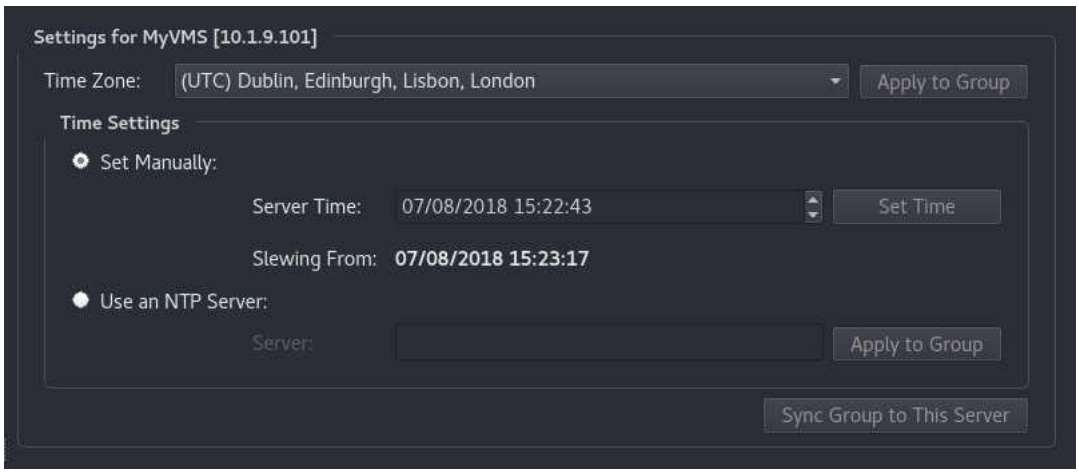


Figure 6.12: Time and Region settings – Slewing of server time after time has been set manually

For a larger time change (greater than 29 minutes), it would take too long to slew the time so a time jump will be required. It is unlikely that this will be necessary in normal operation; indeed if you need to change the time by several hours then it probably indicates you have selected an incorrect time zone.

Time Settings – Jumping time

A time jump forwards of more than 29 minutes must be handled specially, and jumping backwards by more than 29 minutes might lose footage because footage is indexed by time and that time is overwritten.

The system has protection against time jumping backwards. On restart, if time has jumped back, it will automatically jump forwards to 1 minute after the time of last recording, to prevent overwriting of video footage. This probably isn't quite the correct time, but if the jump was caused by a reboot then the time will be close and can easily be slewed to the correct time.

There is no protection against time jumping forwards over a reboot because time does that continuously (if the time appears to have jumped forwards by 1 day, perhaps the Wavestore server was simply switched off for 1 day).

Occasionally it will be necessary to deliberately jump the time backwards. This will lose footage because the footage recorded after new 'current' time will become inaccessible.

The "slewtimefast" command has been added to slew for periods longer than half an hour without losing any footage or switching off. However this does take a long time, typically 10 times the time to be slewed.

Also, commands "jumptime" (forwards) and "jumptimeback-delete" (backwards, deleting only the period being overwritten by the time change) are available.

To jump time forwards (the easy case):

- Change the hardware clock to the correct time (e.g. change by 1 hour) (Typically using WaveView Set Time; disable NTP for this).
- Execute Command: `jumptime`
- Time will change immediately, giving an apparent time gap in the footage but all footage is recorded and none lost.

- Fault will be logged in the system log because the time jump does not represent normal operation. Clear Fault to clear.
- If desired, enable NTP.

To jump time backwards immediately:

- Change the hardware clock to the correct time (e.g. change by 1 day) (Typically using WaveView Set Time; disable NTP for this).
- Execute Command: **`jumptimeback-delete`**
- Time will change immediately, overwriting the footage which had a time which is now in the future. FOOTAGE WILL BE DELETED!!
- Fault will be logged in the system log because the time jump does not represent normal operation. Clear Fault to clear.
- Restart the server if needed (it will prompt you to do this) as certain timers will be upset by this jump.
- If desired, enable NTP.

To slew the time without losing all footage:

- Change the hardware clock to the correct time (e.g. change by 1 hour) (Typically using WaveView Set Time; disable NTP for this).
- Execute Command: **`slewtimefast`**
- Do not reboot, but leave the system running. It will slew at a rate of 1:10. So a 1 hour slew will take 10 hours, and a 24 hour slew will take 10 days. Note that the desired target slew time will be reset multiple times by this mechanism. If a reboot or restart is necessary, reset the correct time and issue slewtimefast again after the restart/reboot.
- If desired, enable NTP. It is possible to do this before the slew has completed; it will be ignored until the time is almost right.

Time Settings – NTP

Network Time Protocol (NTP) can be used to synchronise the server time with a networked time source. All Wavestore servers are NTP time sources, so for example a system with 6 servers can have 5 servers set to synchronise to Server 1, and that server can synchronise to an upstream time source.

To configure NTP, check the 'Use an NTP Server' radio button, enter the IP address of the time source in the box provided, and click 'Save' to confirm your changes. Multiple IP addresses can be added separated by spaces, and they will be tried in sequence until a good one is found.

It is also possible to use a host name instead of an IP address, however it is recommended to synchonise to a local time source if possible.

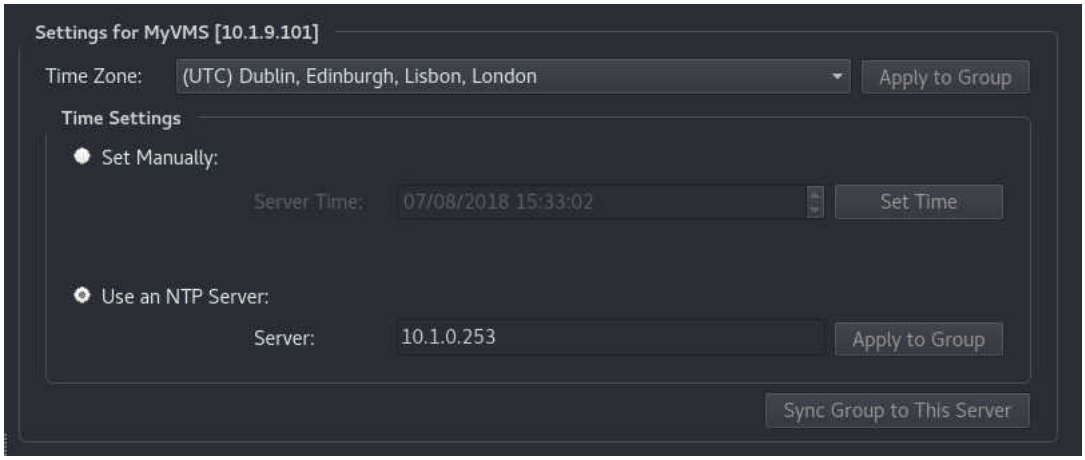


Figure 6.13: Time and Region settings – NTP Server option selected

Synchronising with GPS clock

The Wavestore server can also be synchronised with a GPS clock over a serial link, using NMEA protocols. This will normally connect to a USB port on the server, possibly via a USB–RS232 converter.

To set this up, use the IO/Devices screen and Add a new device on the appropriate serial port using Protocol NMEA.

Synchronising with IRIG–J

The Wavestore server can also be synchronised with a IRIG–J clock over a serial link.

To set this up, use the IO/Devices screen and Add a new device on the appropriate serial port using Protocol IRIG.

6.2.5 Storage

The Storage screen is used to manage hard disks and other storage devices. The screen displays various statistics about the available devices such as size, percentage used, drive model and serial number, format status and device letter. The screen also allows various operations to be performed on these devices including...

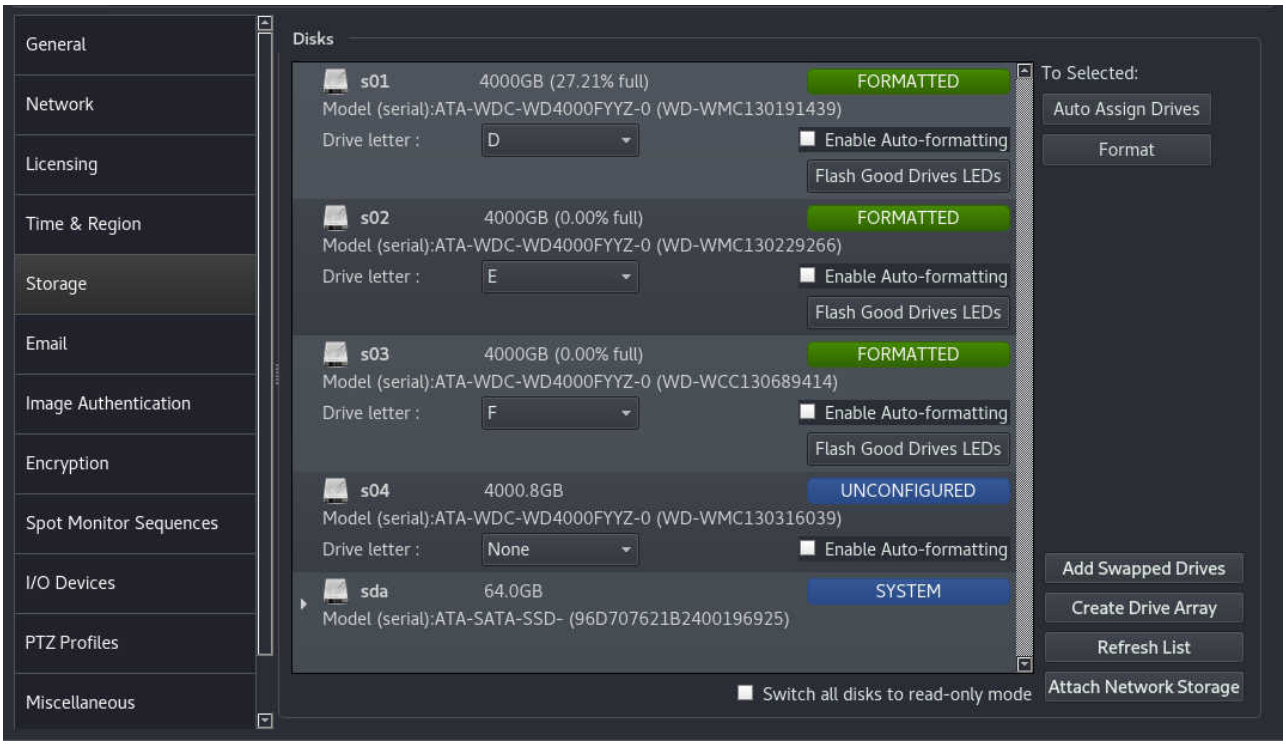
- Formatting storage devices
- Assigning "Drive letters" to storage devices
- Creating RAID arrays from individual disks
- Configuring network storage devices
- Switching all disks to read–only mode (all recording stopped) – to protect critical footage and prevent it from being overwritten

The subject of configuring storage is quite in–depth and can vary depending on the storage technology used. Therefore the section 9.13 – Configuring Storage Devices offers in–depth information for each supported storage system.

Note that admin–level users can inspect the settings, and perform the "Add Swapped Drives" operation, but cannot modify the storage configuration since this is a critical operation that can result in data loss, therefore is only available to install–level users.

The rest of this section will explain the various UI elements and buttons in the Storage setup screen, then walk through configuring simple Direct Attached Disks.

Storage Screen Buttons



Here we will explain what each of the buttons in the Storage setup screen does:

Drive Letter Selection

Each storage disk or "volume" has a drop–down menu to allow a Drive Letter to be assigned. These are used to refer that device elsewhere in the software. For example when choosing which disk a camera should record to.

Flash Good Drive LEDs

This function will cause the system to attempt to flash the disk activity on LED(s) on the disk, or disksif it is an array of disks. This helps identify faulty or missing disks as their LEDs will not be flashing.

Auto Assign Drives

This function is used to quickly assign drive letters to a large number of disks. Select the desired drives and click the button. Holding Shift or Ctrl when selecting the disks allows selecting a range.

Add Swapped Drives

This button is used when attempting to re–incorporate disks. For example if a disk was removed and re–inserted it may show as Unformatted. Similarly if a RAID array has a failed disk and it is replaced, this button will incorporate the replacement drive into the array.

Create Drive Array

This button allows RAID arrays to be created. These could be HyperRAID or MegaRAID arrays. Setting up such systems is described in section 9.13 – Configuring Storage Devices.

Refresh List

This causes the Wavestore to refresh its list of available disks. This operation is performed when first entering the Storage screen, but refreshing is useful if a disk has been physically inserted or removed, or its state has possibly changed and needs to be checked again.

Note that occasionally after a major change, the disk subsystem will not have fully restarted when the display is automatically refreshed, and some disks might be shown as "MISSING". Clicking on "Refresh List" a few seconds later will show the correct state.

Attach Network Storage

This button launches a new dialog allowing network storage devices to be searched for and connected to the Wavestore. Supported types include:

- iSCSI – see section 9.13.3 – Configuring iSCSI Storage Devices
- NFS – see section 9.13.4 – Configuring NFS Storage Devices
- AWS (Amazon Web Services) – see section 9.13.5 – Configuring AWS Storage Devices
- Microsoft Azure – see section 9.13.6 – Configuring Azure Storage Devices

Switch all disks to read-only mode

This option, when enabled, means that no recording or deletion will occur on any disk in the system. This is useful if there is a major incident and the entire system needs to be stored away for future use.

For example, if the system is set to record for no more than 31 days (using the 'Maximum' recording mode) and it were switched off and put into storage for two months, when it is switched on again it will immediately delete the footage which is older than 31 days. Enabling this option prevents such a problem from occurring.

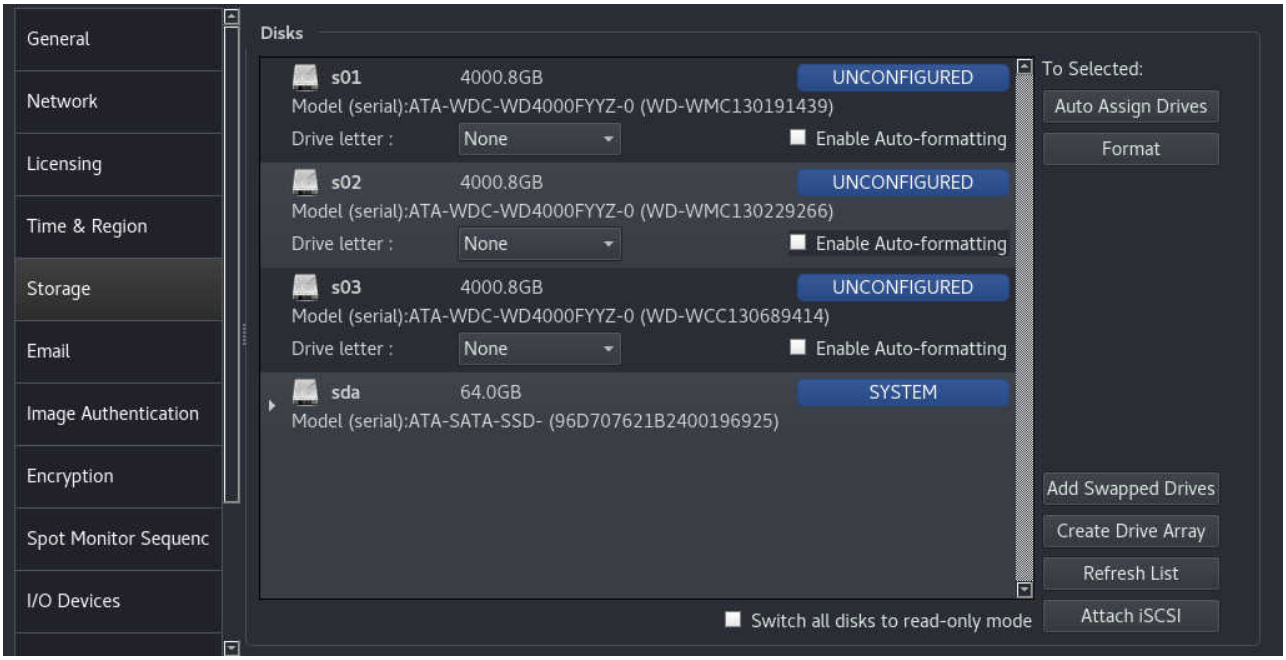
Configuring New Storage Volumes

Before a hard disk (or other storage device) can be used, the disk needs to be formatted, and a device letter allocated to it.

When Wavestore servers are supplied new, all disks are preformatted and assigned letters, but it will be necessary to reallocate the drive letters if the server software is reinstalled at a later date, or if an additional/replacement hard disk is installed in the server.

It is also necessary to carry out this procedure if a removable storage device is to be used with the server. A drive letter must be allocated to the device after it has been attached to the server, before the device can be used recording footage.

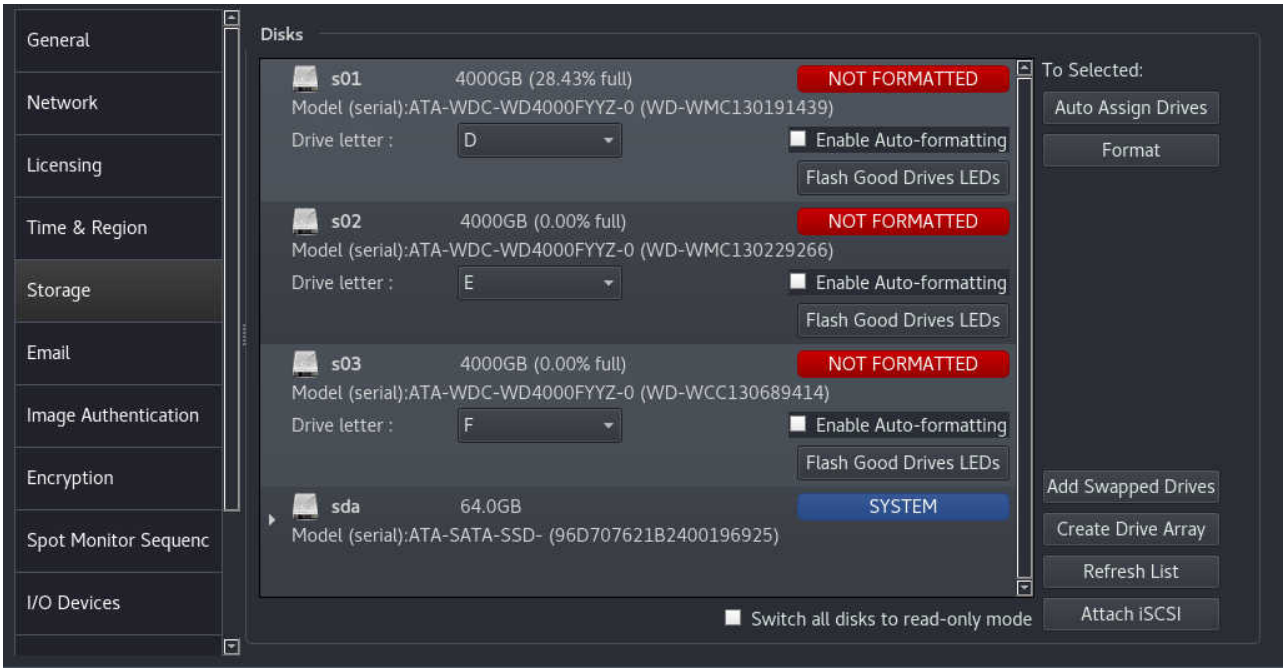
We'll look now at the steps required to configure a newly installed drive, so that it can be used for recording.



In the screenshot above we have four devices...

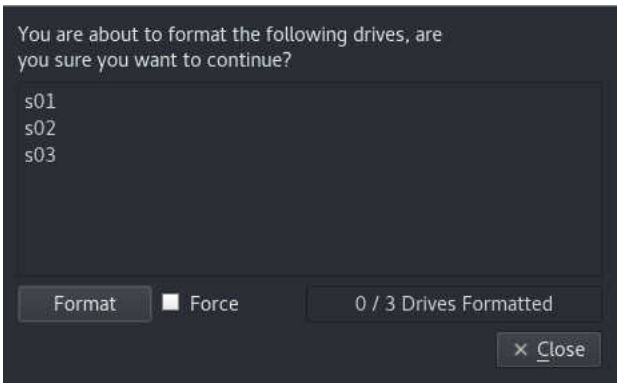
- 3 storage disks, s01 to s03, marked as Unconfigured
- 1 "System" disk. This contains the operating system and is split into partitions. The arrow to the left causes the item to expand and show the partitions. This disk is shown for completeness but we won't use this for storing video.

Firstly we need to assign some drive letters to these disks and Save the changes...



In this case we assigned D, E, and F. It's convention to start at D for historical reasons.

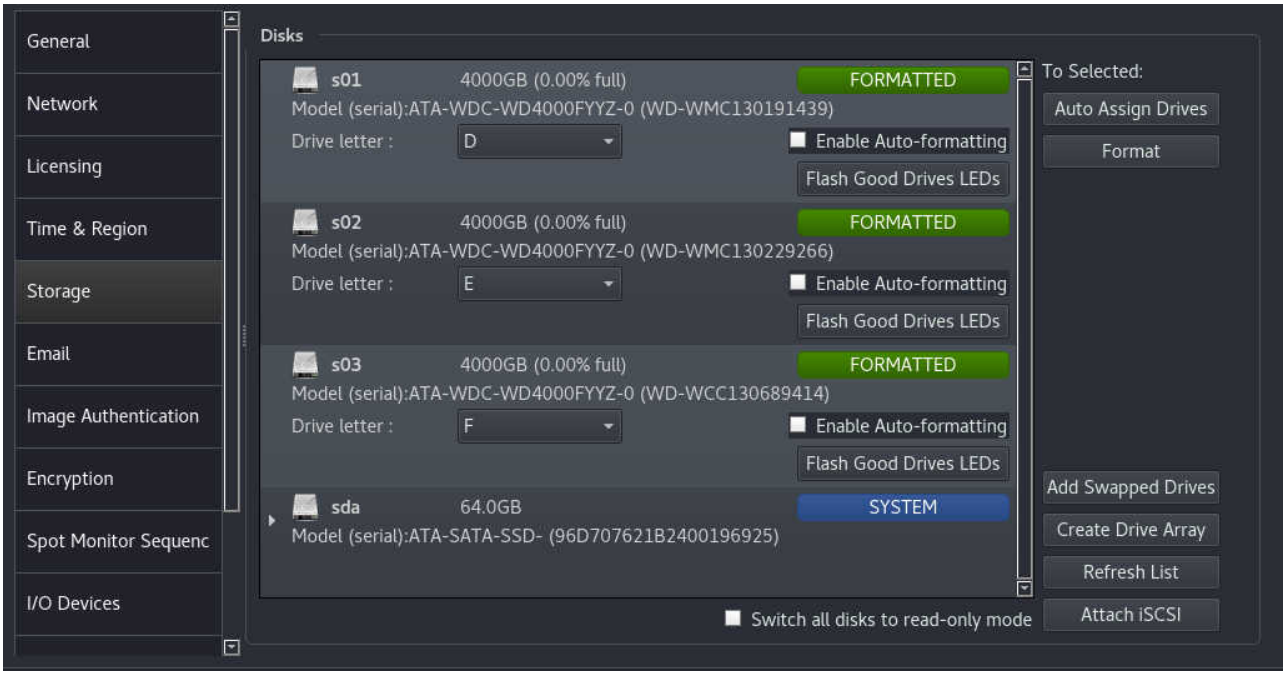
As you can see, these disks are marked as Unformatted. So we can select all 3 and click the Format button.



Check that the correct disks and listed and click Format to perform the operation.

The "Force" option can be required when formatting disks that aren't already empty or LASS formatted, for example disks that are formatted for use with Windows or Linux. This is to prevent accidental formatting of a disk which isn't meant to be LASS-formatted, for example the operating system disk.

Once the drives have been formatted, they should show as Formatted in the main UI.



The volumes are now ready for use, and can have recording tracks allocated to them.

6.2.6 Email

The Wavestore server can be configured to send an email to configured recipient(s), in the event of a configured Event (section 6.12 – Event Rules) being triggered.

The Email setup screen is accessed by the menu path (View → Setup → Email). In order to configure the Email function we need to enter the following details:

Server This is the hostname or IP address of the SMTP server. This field is required.

Port This is the port number of the SMTP server. Default is 25.

Sender This is the email address to be used as the sender. i.e. the "from" address. This field is mandatory.

User This is the username for authentication with the SMTP server. Not mandatory.

Password This is the password for authentication with the SMTP server. Not mandatory.

Use SSL Enables SSL mode if checked. Default is disabled. Normally not needed as security is auto-negotiated with the commonly used STARTTLS mechanism.

Throttle Count Provides a throttling mechanism to prevent lots of repeated emails being sent to the same sender. See below for more details. Default is 10.

Throttle Duration Duration in minutes for checking whether to throttle email sending. See below for more details. Default is 60 minutes.

Debug Will log extra information to the System Log to help diagnose issues if enabled. Default is disabled.

The throttling mechanism requires two parameters to be set – Throttle Count and Throttle Duration. Count is the number of emails and Duration is the time period for the count. So for example if Throttle Count is 10 and Throttle Duration is 60, 10 emails within an hour will be permitted, but an 11th will be discarded. Throttled emails are not counted so emails will eventually be allowed through again.

The throttling mechanism takes into account:

- The Cause of the event (e.g. Input, Motion)
- The Source parameter (which might be camera number for certain events such as Motion or Darkening, input number for Input events, etc.)
- The email Recipient

So for example if Input 1 is triggered many times and throttling occurs to prevent a recipient receiving too many emails, Input 2 may still trigger an email to that recipient since it is a different event.

For this mechanism to work, all sent emails are logged in a database. The database is trimmed when it reaches a certain size but doesn't take up much space and can easily stored a few tens of thousands of records. To force deleting the database, use the WaveView "Execute Command" tool to run "clear-tmp".

To configure email recipients, click 'Add' and enter the destination email addresses as required.

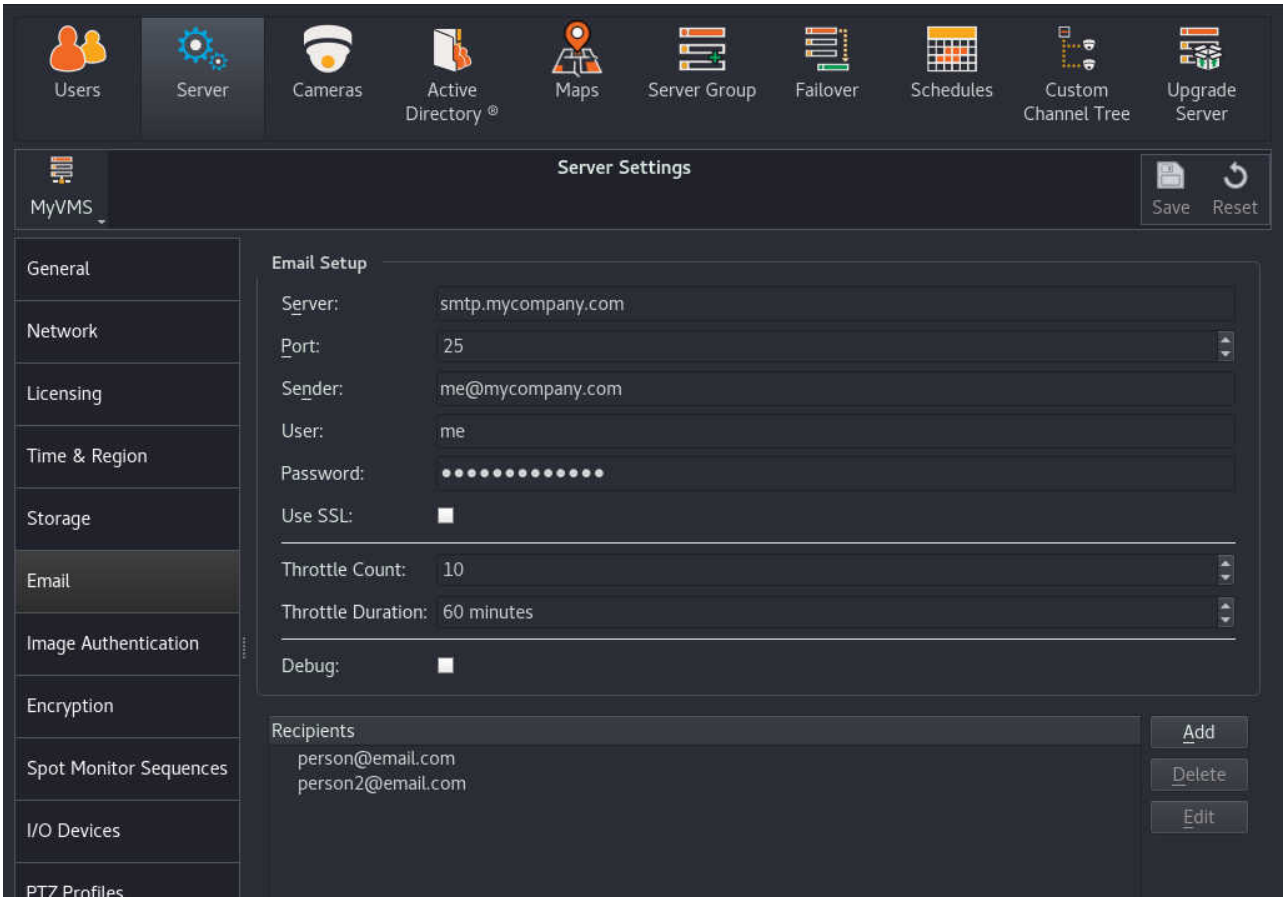


Figure 6.14: Email Configuration Menu

6.2.7 Image Authentication

The Wavestore Server offers an Image Authentication function (sometimes known as 'watermarking') that can be used to ensure that an image or set of images were originally recorded on a particular Wavestore server, and have not been subsequently tampered with.

When Authentication is enabled, the Video Display will show the authentication status of the video stream.

Authentication is only possible on recorded images, not live. There is a short delay before recorded images can be verified; in these cases, the Video Displays may show the orange 'Authentication not checked' icon.

Authentication is also possible on exported video when played through the WaveView client software.

Configuration of Image Authentication requires enabling Signature Stream Recording, and use of a Digital Certificate. There are two types of digital certificate which can be used with Wavestore...

Self-signed

Available on servers running v6.20 or later. These certificates are automatically generated when authentication is enabled and are the easiest way to get up and running. However they are considered less secure than CA-signed certificates.

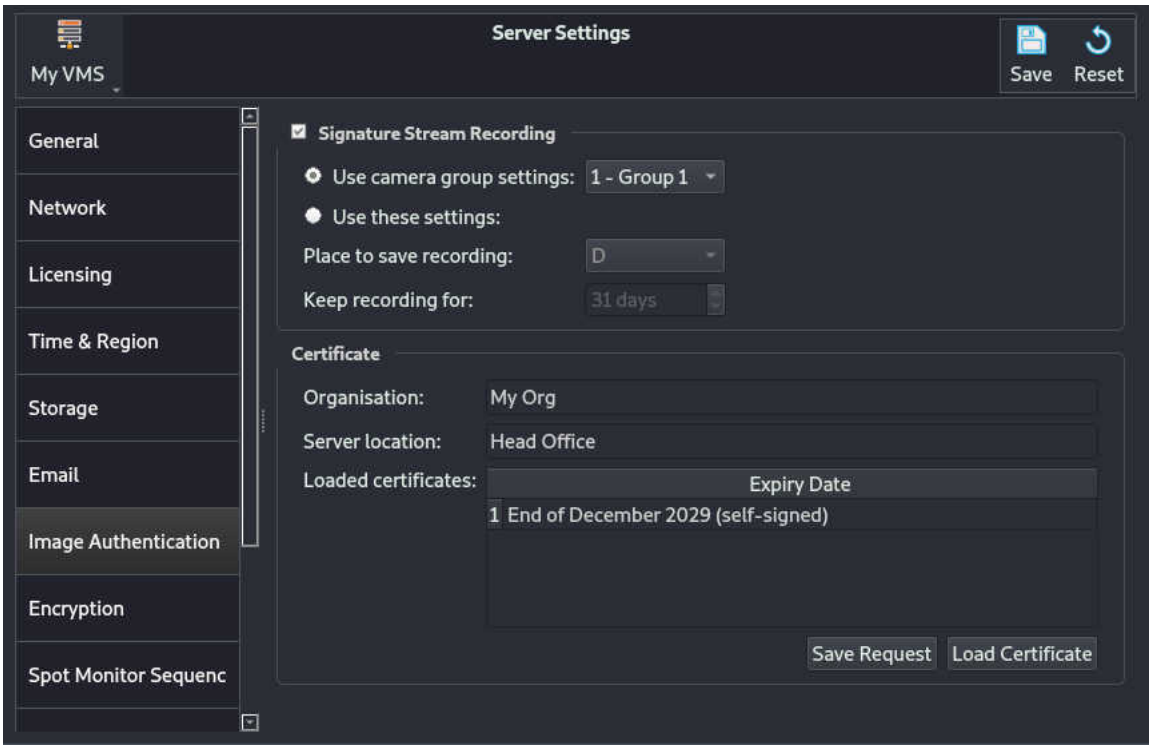
CA-signed

These certificates are generated and digitally signed by a Certificate Authority (Wavestore Global

Limited). For these certificates it is necessary to generate a "certificate request" and send it to Wavestore Global Limited to request an official digital certificate. A charge may apply. The digital certificate can then be installed.

Signature Stream Recording

Data relating to Image Authentication needs to be recorded to the Wavestore server. To enable this, enable the 'Signature Stream Recording' checkbox.

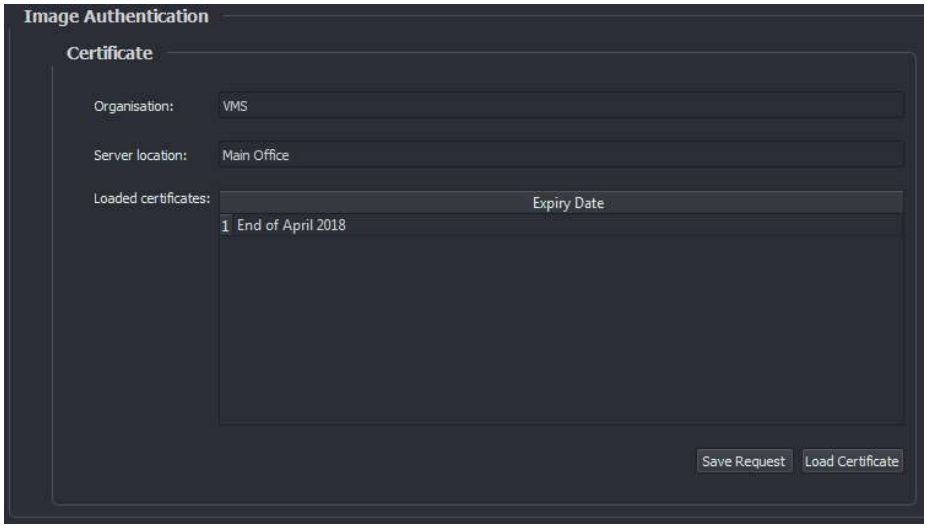


The default recording settings are to use the same settings as the first Camera Group. That is, the same target disk and recording duration. An alternative Camera Group can be chosen.

Alternatively, choose "Use these settings:" and specify the desired disk and duration to keep the recordings.

Certificate

The 'Certificate' section of the 'Image Authentication' setup page shows details of any currently installed digital certificate.



If it is a self–signed certificate then it will show "(self–signed)" after the certificate expiry date.

To switch from a self–signed certificate to a CA–signed one, the following procedure should be followed:

- Complete the 'Organisation' and 'Server location' fields.
- Save the changes.
- Click 'Save Request' to create the certificate request.
- Save the file and email it to support@wavestore.com.
- Once a reply is received containing the CA–signed certificate, choose 'Load Certificate' and select the certificate file.

Please note that once the Image Authentication Certificate has expired, a new certificate must be obtained and loaded in the same manner.

6.2.8 Encryption

The Wavestore uses encryption for three purposes:

Password protection
A one way encryption is used to protect passwords

Command protection
Sensitive commands sent over the network are encrypted

Video protection
The system can encrypt video and audio from capture until playback using end–to–end encryption

These are largely distinct methods of encryption. The one–way password encryption is performed using a secure one–way hash function and is transparent to the user.

Commands sent over the network are encrypted using RSA public key encryption for negotiation and then AES128 for content encryption, and this too is transparent to the user. It is similar to using HTTPS to access your web server.

Video and Audio can be encrypted at the point of recording. It remains encrypted on disk, when sent over the network, and when backed up to a backup device. It is decrypted only at the point of viewing on

the WaveView client. This is not transparent to the user as it requires key distribution, and it is described in the next section.

Video Encryption

The Wavestore server can encrypt recorded video and audio, such that it can only be viewed by users that hold a special 'private key'.

The configuration steps required to enable this functionality are as follows:

- Generate a key pair – creating a public key and a private key
- Load the public key onto the Wavestore server (menu path View → Setup → Server → Encryption).
- Enable Signature Stream Recording as described in section 6.2.7 – .
- Enable encryption for each individual channel that you wish to encrypt.
- Distribute the private key to any WaveView client that is required to access the video and audio.

The Encryption setup screen shows the public key so that it can be copied or checked if necessary.

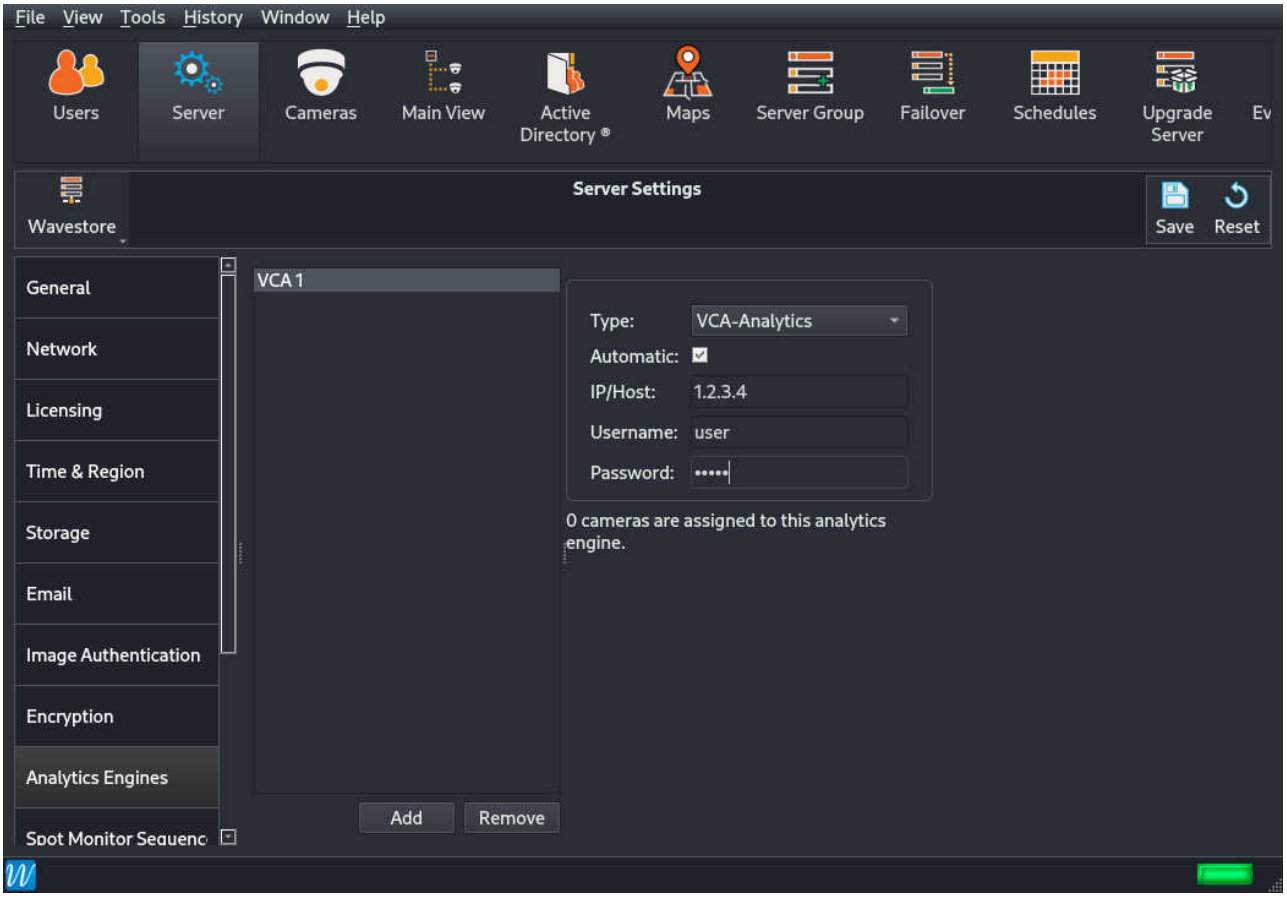
When WaveView client (running either on the server itself, or a client PC) first detects encrypted footage, the operator is prompted to load the private encryption key. If this key is valid, the video will be displayed (or audio played). Otherwise it will not be possible to view/listen to the encrypted footage.

Details of how to load the private key onto the WaveView client, in order to access encrypted audio/video streams, is contained in section 3.6.4.3 – Encryption State icons.

6.2.9 Analytics Engines

The Wavestore can interface to external Video Content Analytics engines. The Wavestore will send video to the device and retrieve analytics metadata, which can be used to monitor for events in real–time via the Wavestore event system, or do retrospective Smart Search operations.

The Analytics Engine setup screen allows an external analytics device to be configured.



Type
: Selects the type of analytics engine that will be connected to.

Automatic
: If enabled, cameras on the Wavestore will be automatically mappd to channels on the analytics engine. Otherwise, each camera on the Wavestore should have its corresponding *Analytics Channel* ID on the analytics device configured in the *Setup* → *Cameras* screen.

IP/Host
: The IP address or hostname of the analytics engine.

Username
: The username used to interface with the analytics engine.

Password
: The password used to interface with the analytics engine.

To assign Wavestore cameras to the analytics engine:

- Go to *Setup* → *Cameras* → *Camera Groups*.
- For any Camera Groups you would like to interface with the analytics engine, under *Analytics*, select the Analytics Engine by its ID, and optionally set which *Stream* should be sent to the engine.
- If not using *Automatic* mode, under *Setup* → *Cameras* → *Cameras* → *General*, set the *Analytics Channel* to the ID of the channel on the engine.

The Analytics Engines setup screen will show how many channels are assigned to each engine.

6.2.10 Spot Monitor Sequences

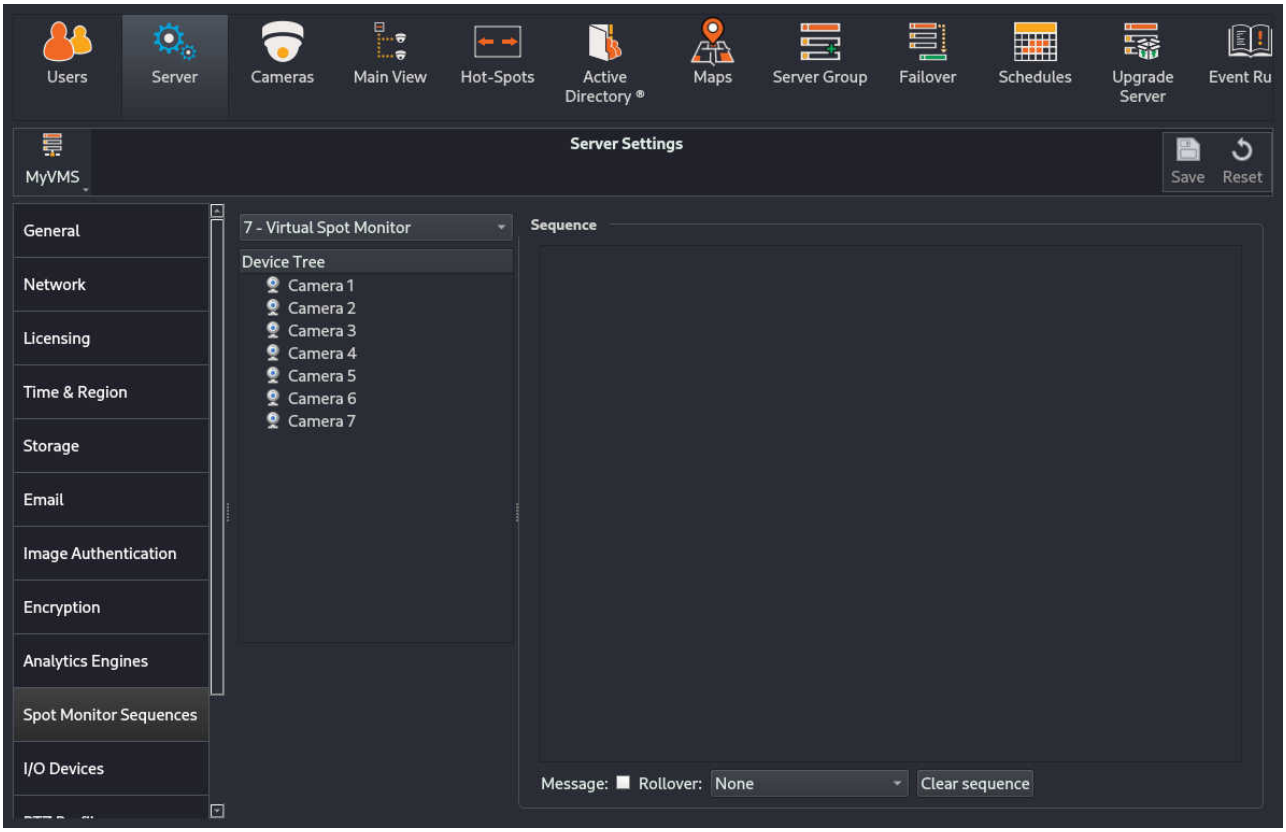
Certain analogue compression cards may have one or more spot monitor outputs. These can be configured to display different cameras in a sequence from the various video inputs on that card.

The Wavestore also supports the concept of Virtual Spot Monitors which allows switching of any camera in the system to a "virtual camera". So that camera can be displayed in WaveView and it will switch its contents to the source camera. Creating *'Virtual Spot Monitors'* is described in section 9.10 – Configuring Virtual Spot Monitors.

As an example, a sequential display of cameras can be configured viewing camera 1 for 2 seconds, camera 3 for 2 seconds, camera 5 for 5 seconds, and camera 11 for 5 seconds; then returning to the start of the sequence (camera 1) and so on. Dwell time can be configured individually for each camera selected, and cameras may be repeated with different dwell times in each instance.

The Spot Monitor output can also be configured to react to digital inputs/motion events etc.; this is carried out in the Event Rules section (see section 6.12 – Event Rules).

To create a Spot Monitor Sequence, navigate to its setup screen – *View → Setup → Server → Spot Monitor Sequences'*.



In the screenshot above we have selected the spot monitor channel 6. We can select a different spot monitor to configure if desired by using the drop-down menu.

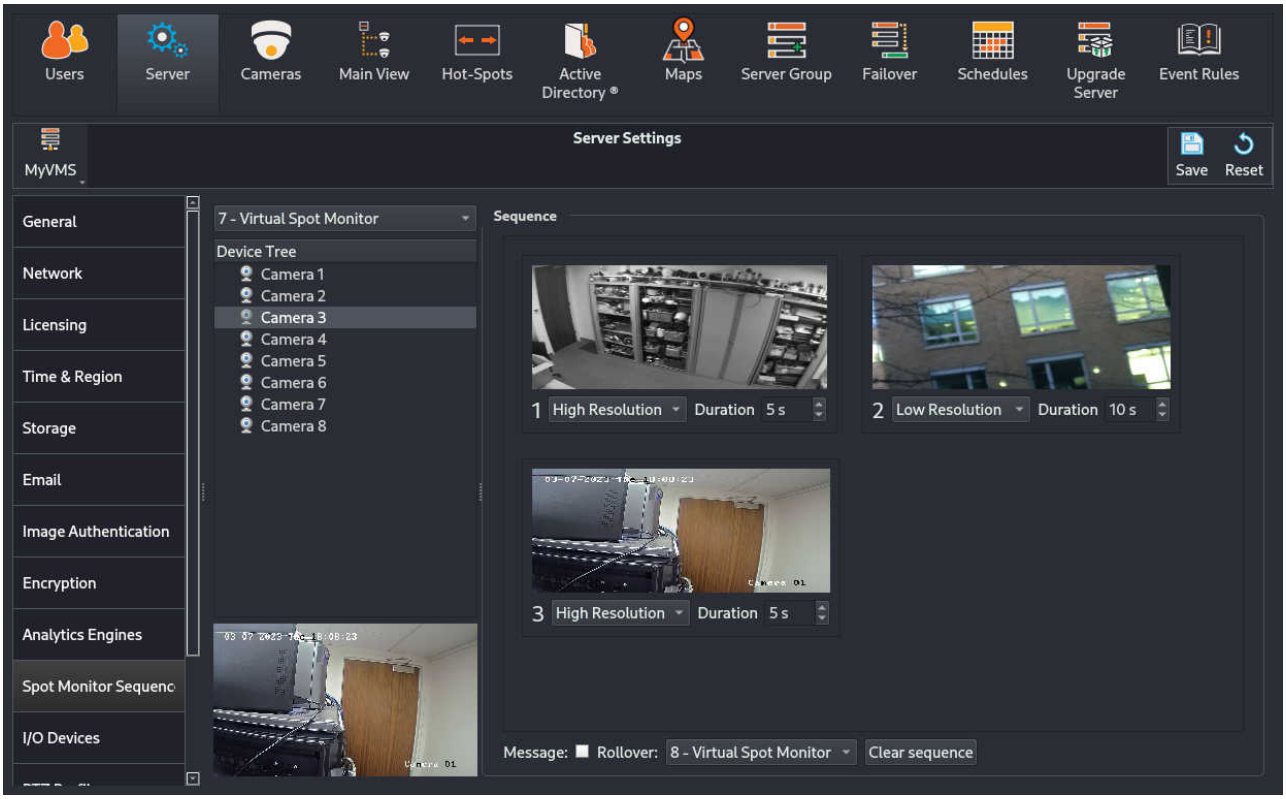
Under the spot monitor select is the list of cameras on this server. Note that we can only use cameras on the current server. For analogue spot monitor outputs we can only use analogue inputs from the same capture card.

To create a sequence we simply drag and drop cameras from the Device Tree into the Sequence area on the right. Clicking on a camera channel displays the image from that camera.

The duration that each camera channel will be displayed can be configured using the up and down arrows.

It is also possible to select either the High or Low resolution streams (corresponding to Streams 1 and 2 in the Cameras setup screen). If the selected stream is not available, the server will try to use the other one.

When using IP cameras with codecs that use I-frames and P-frames, such as H.264, the camera will only switch when an I-frame is received within dwell time. The timer is reset when the camera is switched to, meaning that these 'dwell times' are less precise the larger the interval between I-frames.



The *'Message'* checkbox defines if subtitles should appear on the spot monitor output, but only applies to analogue spot monitor outputs.

The *'Rollover'* option is used when events are triggering spot monitors to show cameras. If the current spot monitor is showing a camera due to an event and another event occurs, the event will be forwarded to the selected *'Rollover'* spot monitor. If no *'Rollover'* spot monitor is provided, the current spot monitor will show the camera associated with the new event immediately. This can be cascaded for any number of Virtual Spot Monitors.

To remove a configured sequence, click on 'Clear'.

Once the sequence has been configured, click on 'Save', and the spot monitor will display the saved sequence.

6.2.11 I/O Devices

The Wavestore Server can be interfaced with peripheral I/O devices such as:

- input/output devices that can be configured in the Event Rules menu (see section 6.12 – Event Rules) e.g. to control recording on the server, and/or activate an output.
- external control device
- NMEA devices (e.g. GPRMC clocks for time synchronisation)
- Supported IP cameras that notify Wavestore server of detected events (e.g. Motion Detected) using proprietary message formats (e.g. HTTP/CGI)
- Supported POS Devices we wish to record data (e.g. transaction details) from, for use with Metadata recording

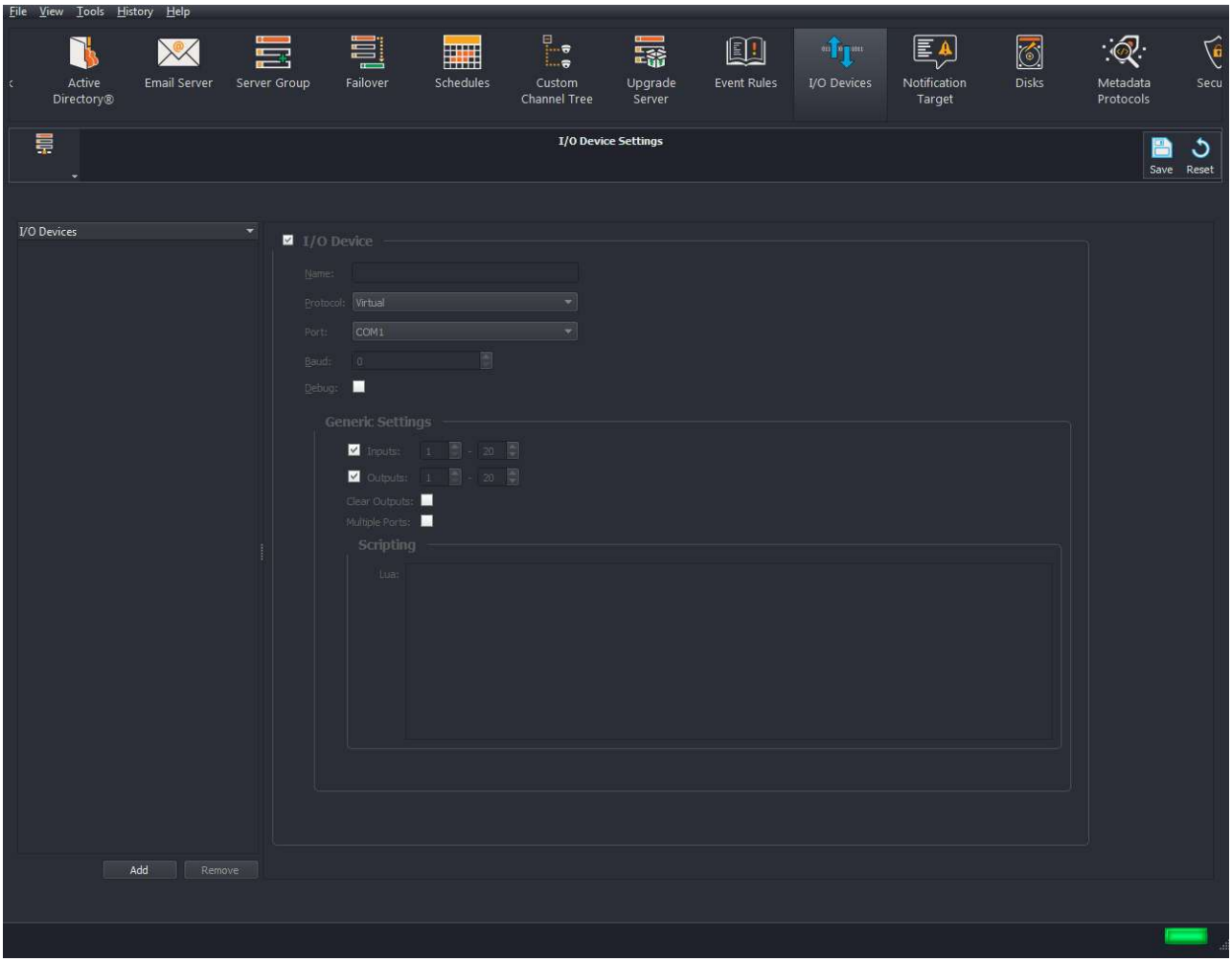


Figure 6.15: I/O Devices screen

To configure a device, click on 'Add', and then select the correct Protocol for your device.

6.2.11.1 *Configuring Stretch Alarm Boards as Input/Output devices*

If your server is fitted with a Stretch VRC7008ALM Alarm board, these devices are auto detected by the server software, and no configuration is required for them in the I/O Devices menu.

In the Event Rules menu, inputs/outputs on configured I/O devices listed in the format Device Name and ID: Input/Output Number, e.g. Stretch 1:1. Inputs/Outputs on the Stretch alarm board are automatically detected by the server and numbers assigned to each input output. If you have additional I/O devices (e.g. Wavestore USB Alarm Board), numbers need to be assigned to these inputs/outputs manually, make sure that each input/output has a unique number assigned that does not clash with any input/output.

The eight digital inputs on the VRC7008ALM board will appear in the Event Rules menu as follows:

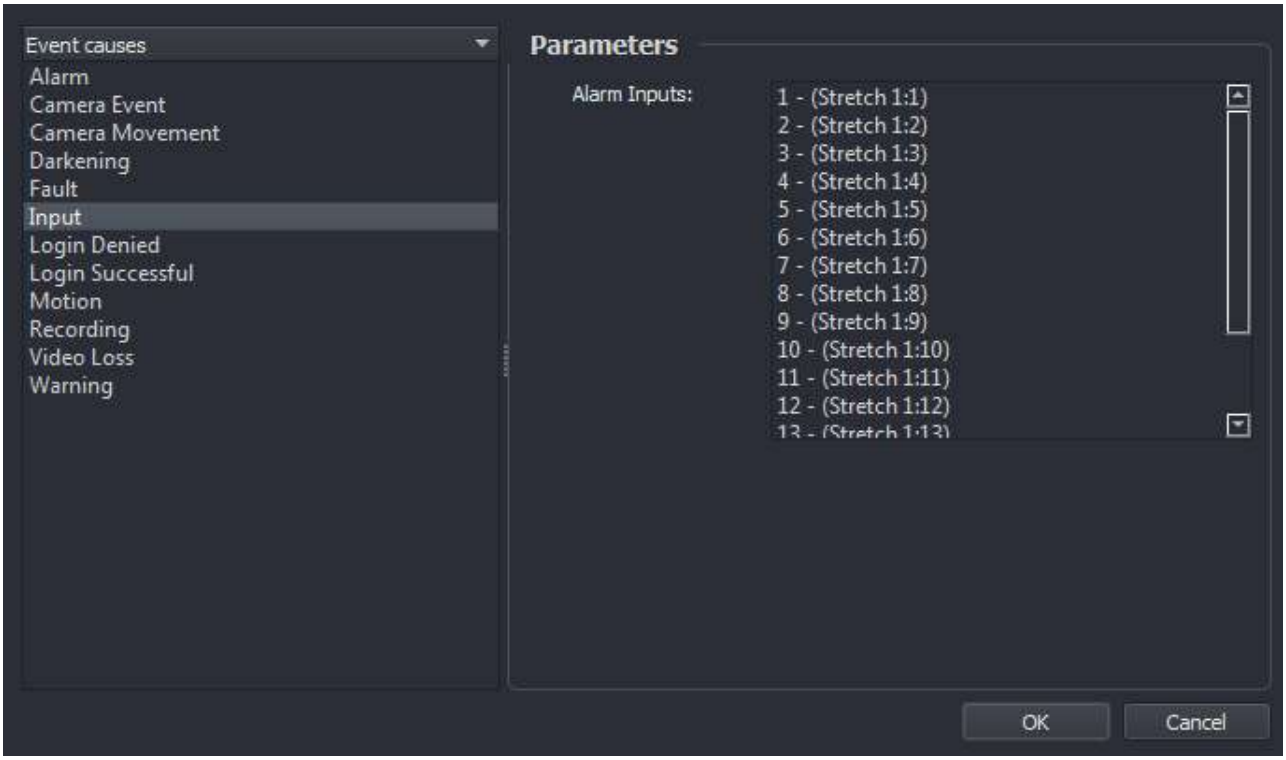


Figure 6.16: I/O Devices, Stretch Alarm Board Inputs

The eight relay outputs on the VRC6008–ALM board will appear in the Event Rules menu as follows:

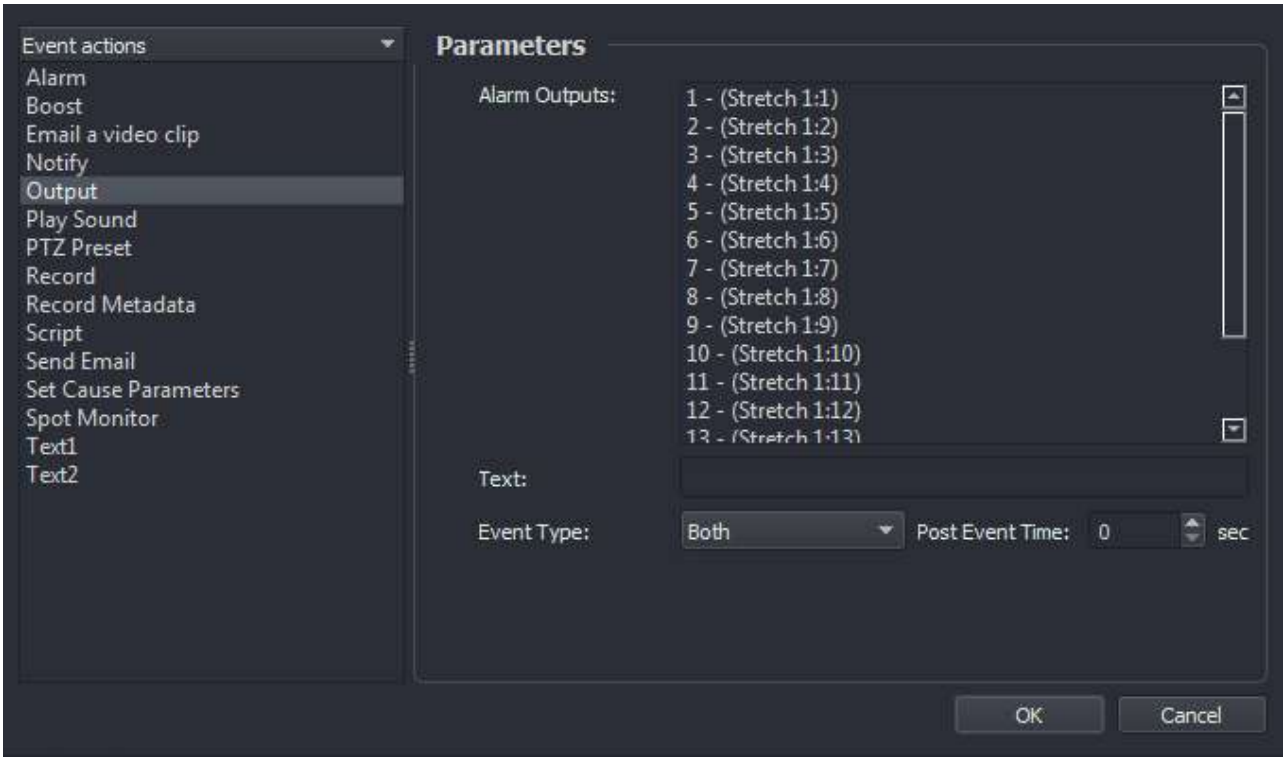


Figure 6.17: I/O Devices, Stretch Alarm Board outputs

6.2.11.2 Configuring 16 input USB Alarm Boards as an I/O device

Configuration for a USB Alarm Board is carried out as follows:

- Click on 'Add' and enter the name for your new device
- In the Protocol field, select 'WaveAlarm'
- In the Port section, select Alarm–x–y.z from the dropdown list (e.g. ALARM–2–1.5 in the example below)
- In the Baud section, select '9600'
- In the Generic settings section, assign a range of numbers to the sixteen Inputs; each USB Alarm Board must be assigned a unique range of input numbers that do not clash with any other Alarm Devices
- In the Generic settings section, assign a range of numbers to the sixteen Outputs; each USB Alarm Board must be assigned a unique range of output numbers that do not clash with any other Alarm Devices

An example configuration is shown below:

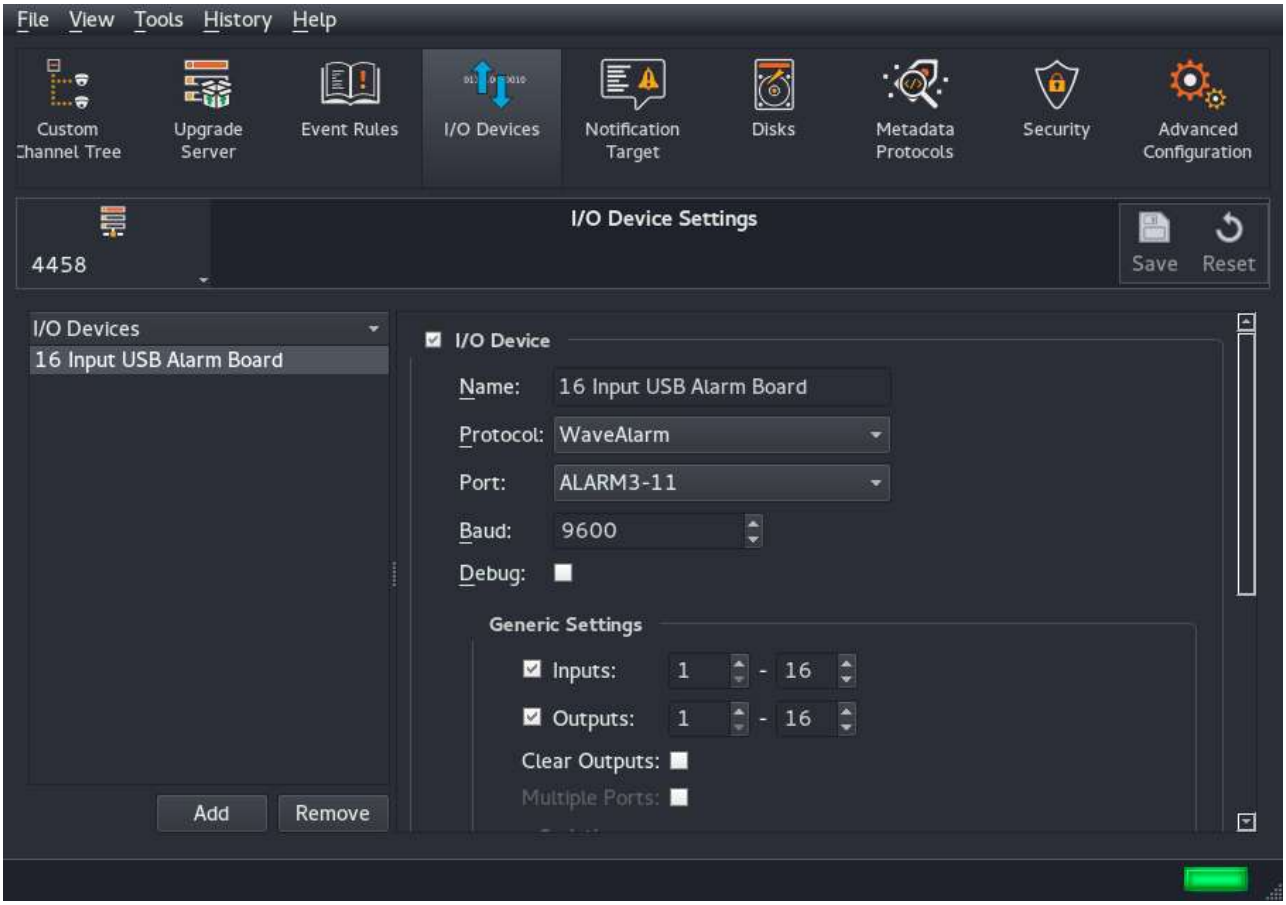


Figure 6.18: I/O Devices screen – USB Alarm Board configuration

In the Event Rules screen, the USB alarm board will appear as follows in the Event Cause sub menu:

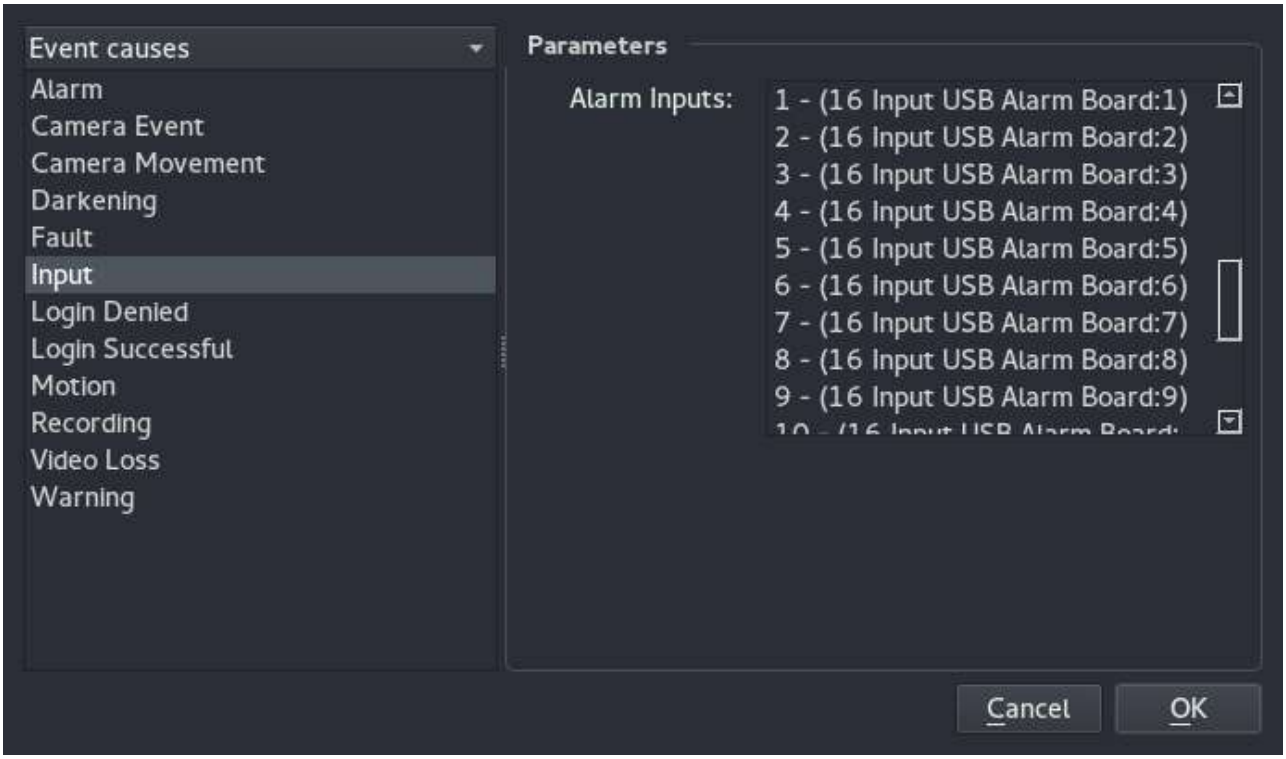


Figure 6.19: I/O Devices screen – USB Alarm Board digital inputs

In the Event Rules screen, the USB alarm board will appear as follow in the Event Action sub menu:

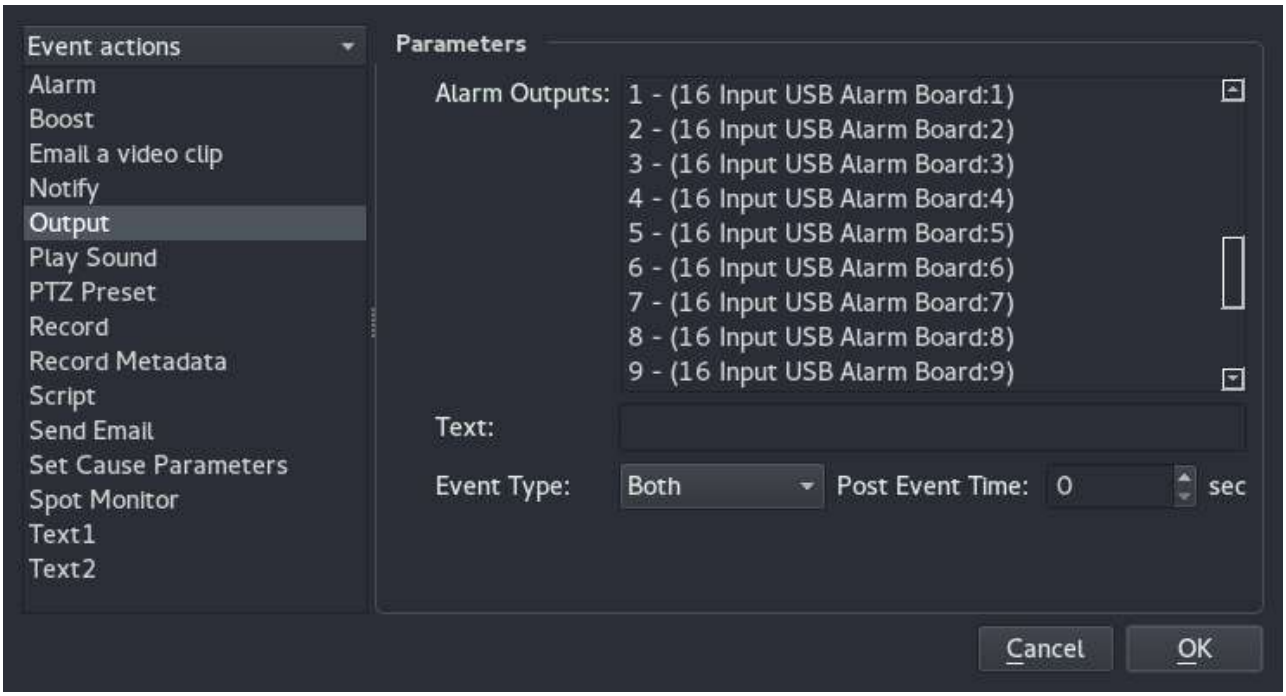


Figure 6.20: I/O Devices screen – USB Alarm Board relay outputs

6.2.11.3 Configuring 20 input USB Alarm Boards as an I/O device

Configuration for a USB Alarm Board is carried out as follows:

- Click on 'Add' and enter the name for your new device
- In the Protocol field, select 'WaveAlarm'
- In the Port section, select one of the USB ports (e.g. 'usb1'); each USB Alarm Board must be assigned a unique port number that is not being used by any other USB devices (e.g. USB Alarm Board/RS485 PTZ adaptor)
- In the Baud section, select '9600'
- In the WaveAlarm settings section, assign a range of numbers to the twenty Inputs; each USB Alarm Board must be assigned a unique range of input numbers that do not clash with any other Alarm Devices
- In the WaveAlarm settings section, assign a range of numbers to the twenty Outputs; each USB Alarm Board must be assigned a unique range of output numbers that do not clash with any other Alarm Devices

An example configuration is shown below:

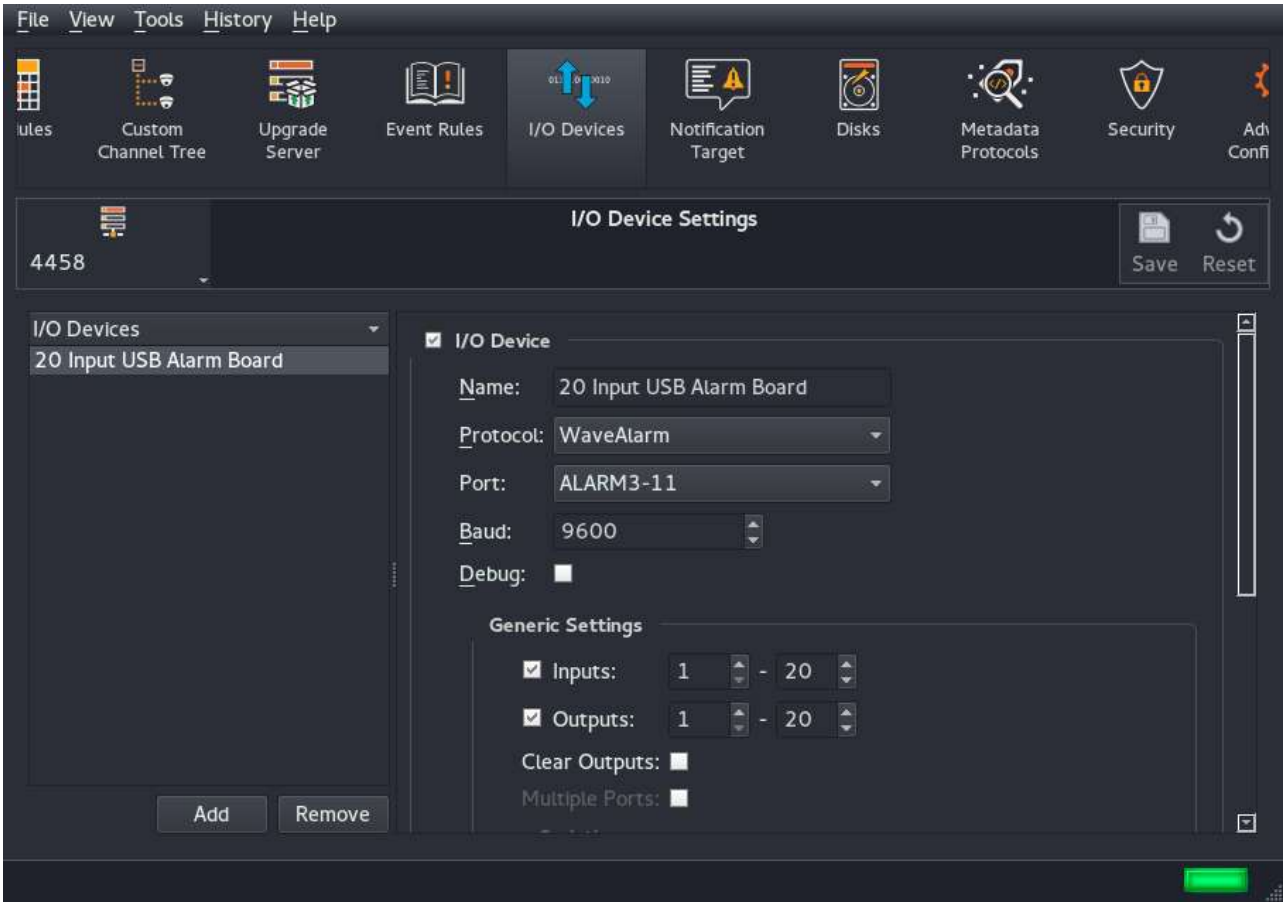


Figure 6.21: I/O Devices screen – USB Alarm Board configuration

In the Event Rules screen, the USB alarm board will appear as follows in the Event Cause sub menu:

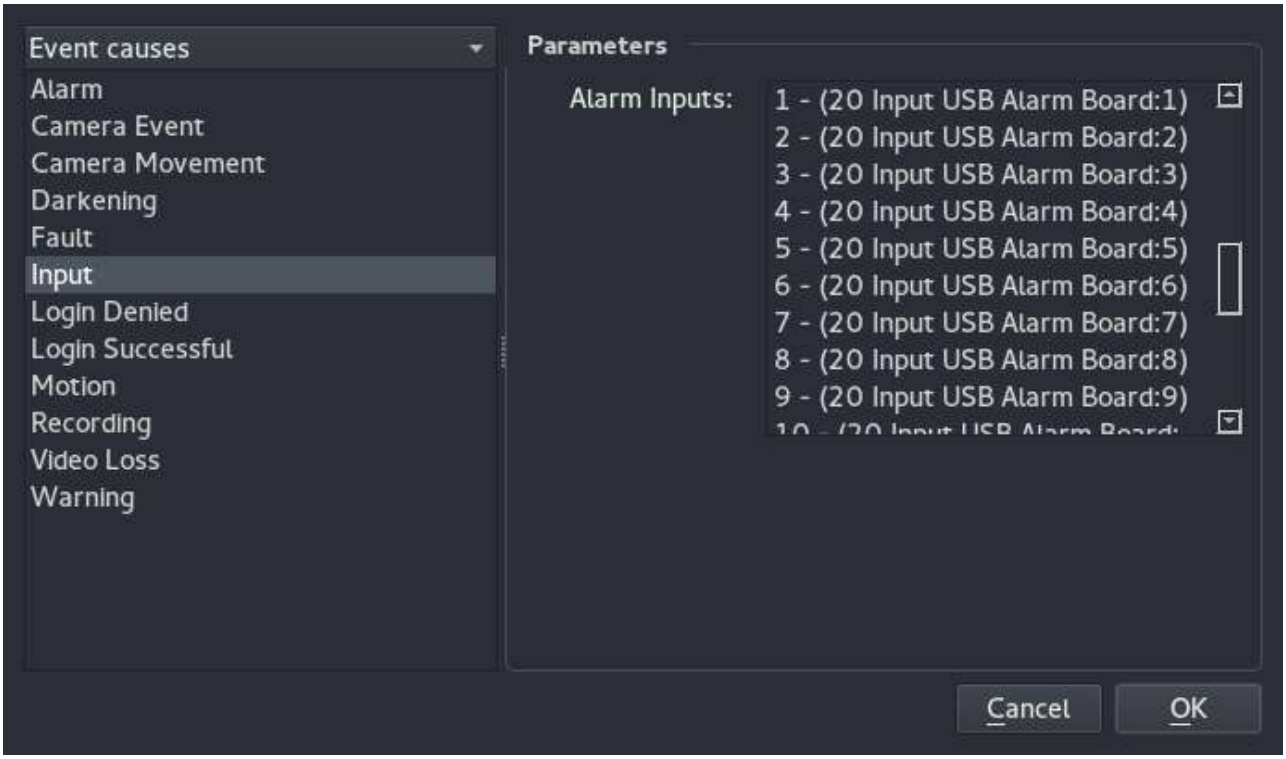


Figure 6.22: I/O Devices screen – USB Alarm Board digital inputs

In the Event Rules screen, the USB alarm board will appear as follow in the Event Action sub menu:

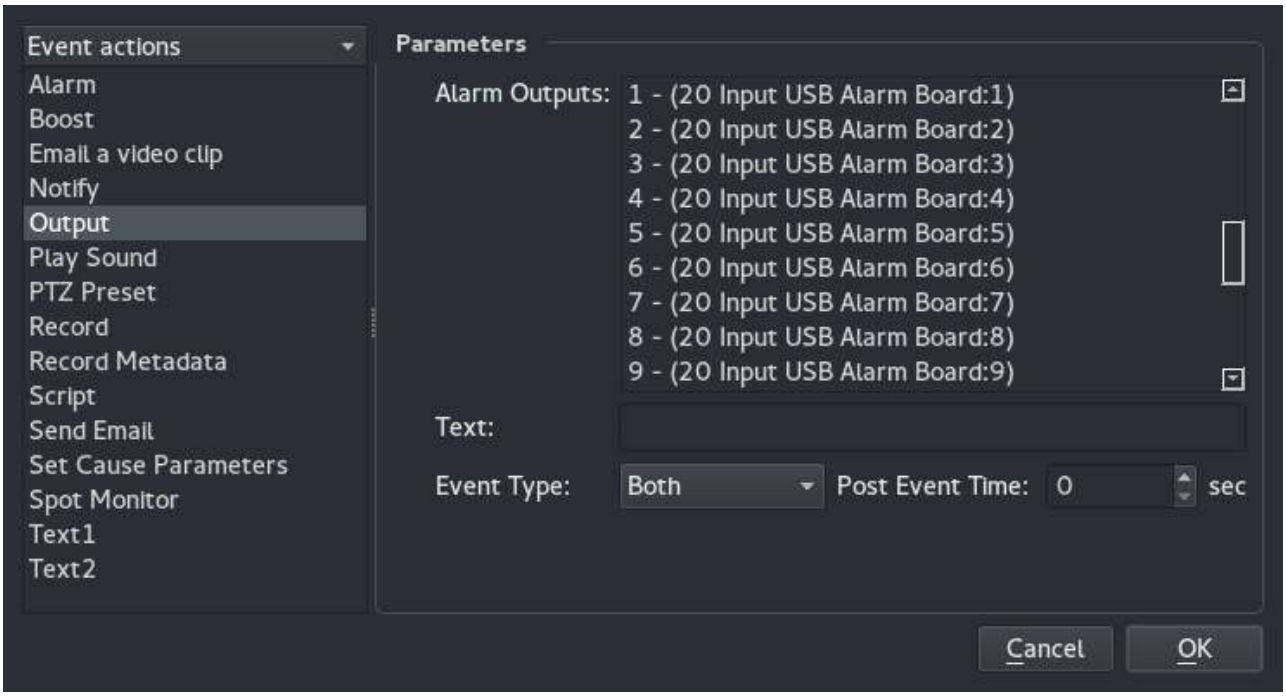


Figure 6.23: I/O Devices screen – USB Alarm Board relay outputs

6.2.11.4 Configuring an SOM Device as an I/O device

SOM protocol is used to interface the Wavestore server with the SOM1 module available from CPC. It supports 4 event outputs only.

For full details of support for SOM (Serial Output Module) protocol devices, please contact the Wavestore Support Team.

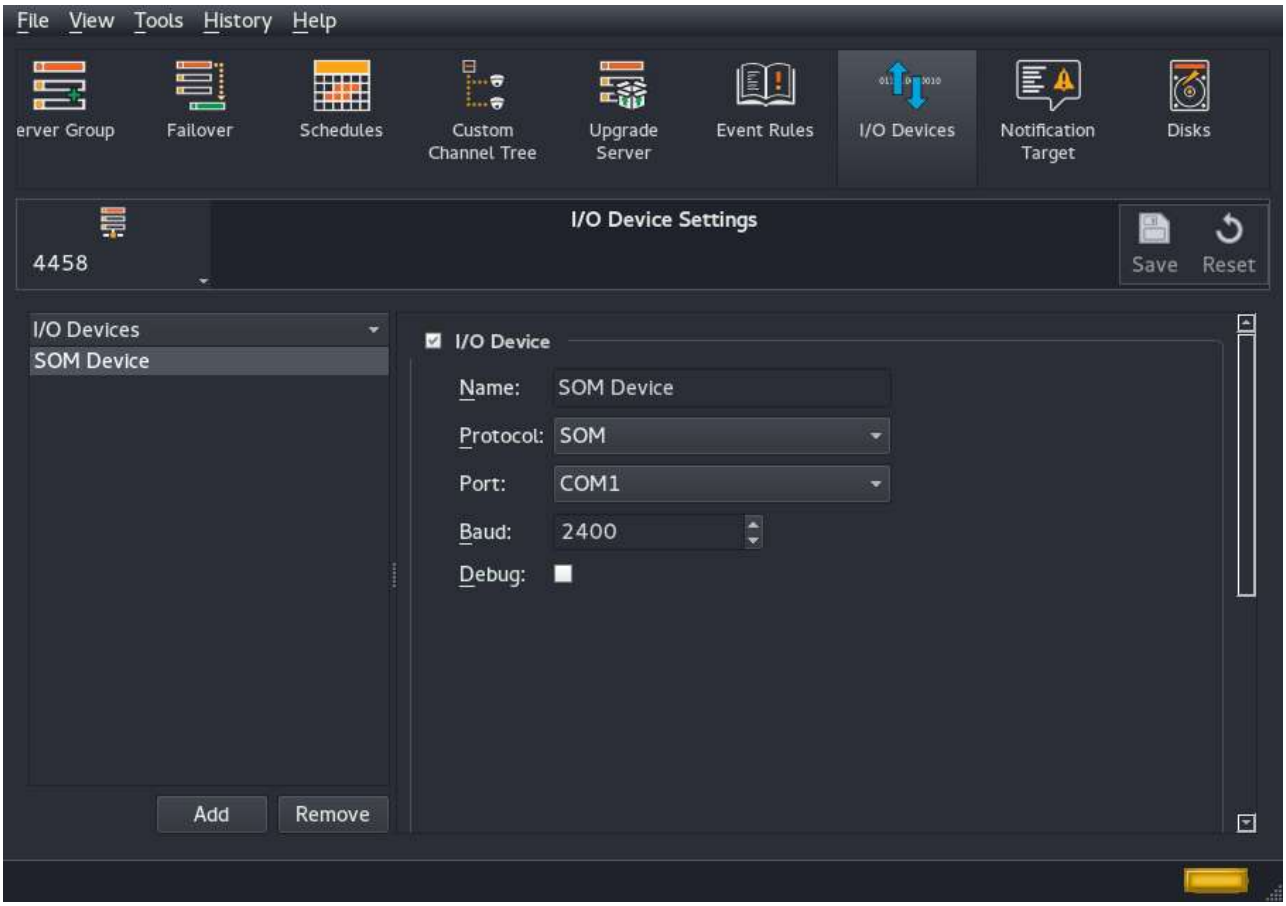


Figure 6.24: I/O Devices screen – SOM protocol device

6.2.11.5 Configuring an NMEA Device as an I/O device

NMEA protocol is used for GPS system integration. It is primarily used to set the system time from the GPS. It can also generate positional text event inputs and set the system time.

To set the time: chose which of the NMEA commands will be used to set the time. Multiple fields may be comma separated but omitted or empty ones are treated as any permitted, but non–empty fields must match. Typically an RMC command will be used: `$GPRMC`

Most GPS devices will output RMC commands. But in some cases it might be desirable to synchronise to the time or position using another command, so flexibility is provided.

An option is available to allow bad checksums for the few NMEA devices which do not provide correct checksums.

An 'Accurate after' parameter specifies number of fixes before a fix are considered accurate. Default 750. Before this, an error of 16s is assumed because of the difference between GPS and UTC timescales. This

correction is only broadcast every 12.5 minutes and therefore for the initial 750 fixes the time information might not be in UTC.

A 'delay' parameter specifies delay from timestamp to the '$' of the command being received. Default 3, which assumes the '$' is sent within a millisecond of the time being computed, and since the '$' takes 2ms to be sent at 4800 baud, the total is 3ms. This parameter can be used for fine tuning when the actual delay is known.

For location information, the same RMC command used for time can be used but it might be necessary to reject these unless the third field is an A, hence use **`$GPRMC,,A`** for this event command field if positional events are required.

First Input: the INPUT event to trigger when location information arrives.

Fields: the fields which need to go to the TEXT field of INPUT. Field 0 is command name, field 1 the one after, etc. Checksum is treated as just another field. If multiple fields are included, the comma or star separator between them will be included. To get entire line (all fields including checksum but excluding newline at end), use fields 0 to 99. If using the RMC command, use fields 3 to 6 to get the position.

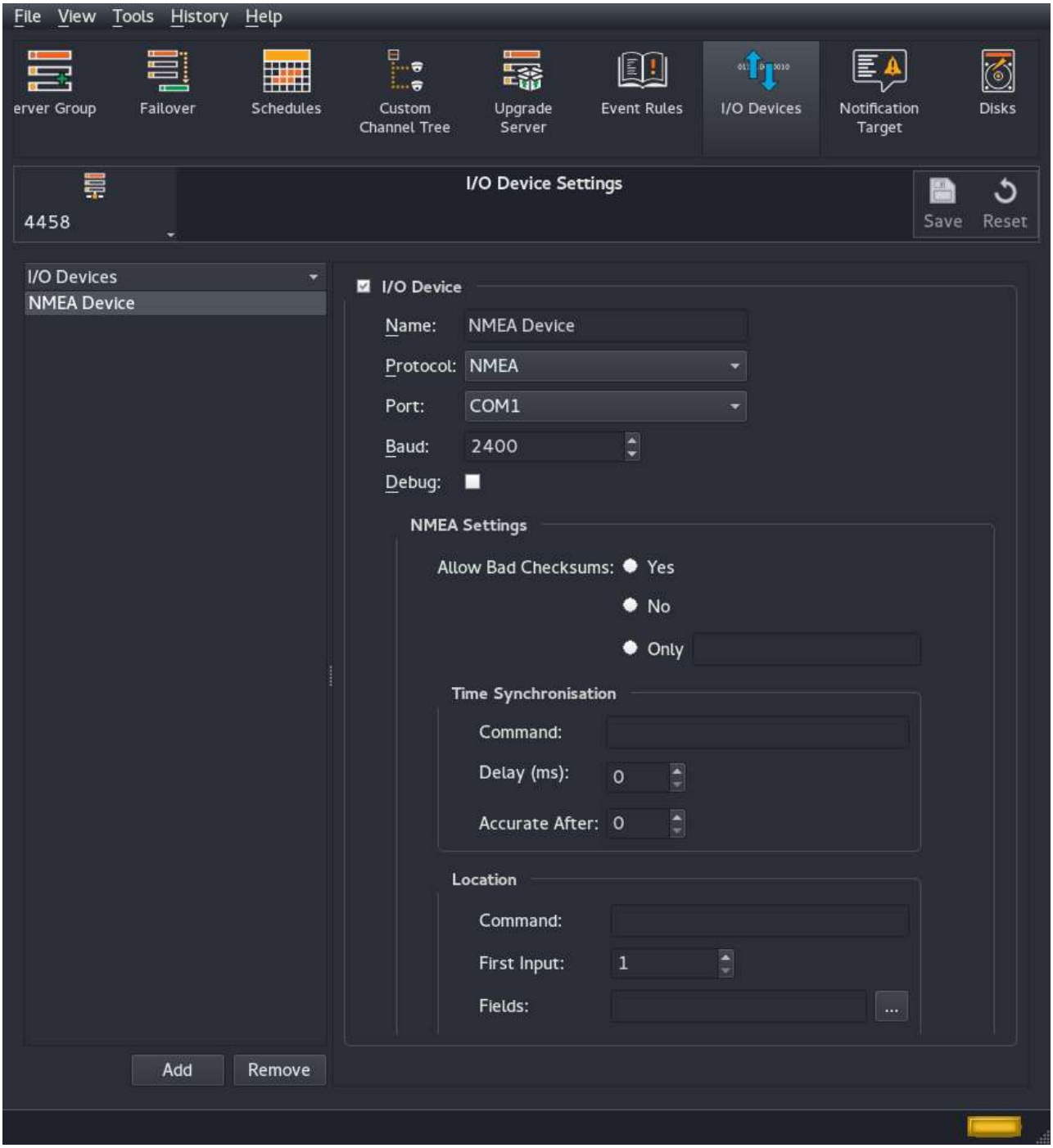


Figure 6.25: I/O Devices screen – NMEA protocol device

6.2.11.6 Configuring an IRIG Device as an I/O device

IRIG protocol is used for Time integration.

To configure an IRIG device, configure protocol as 'IRIG', with baudrate '2400'.

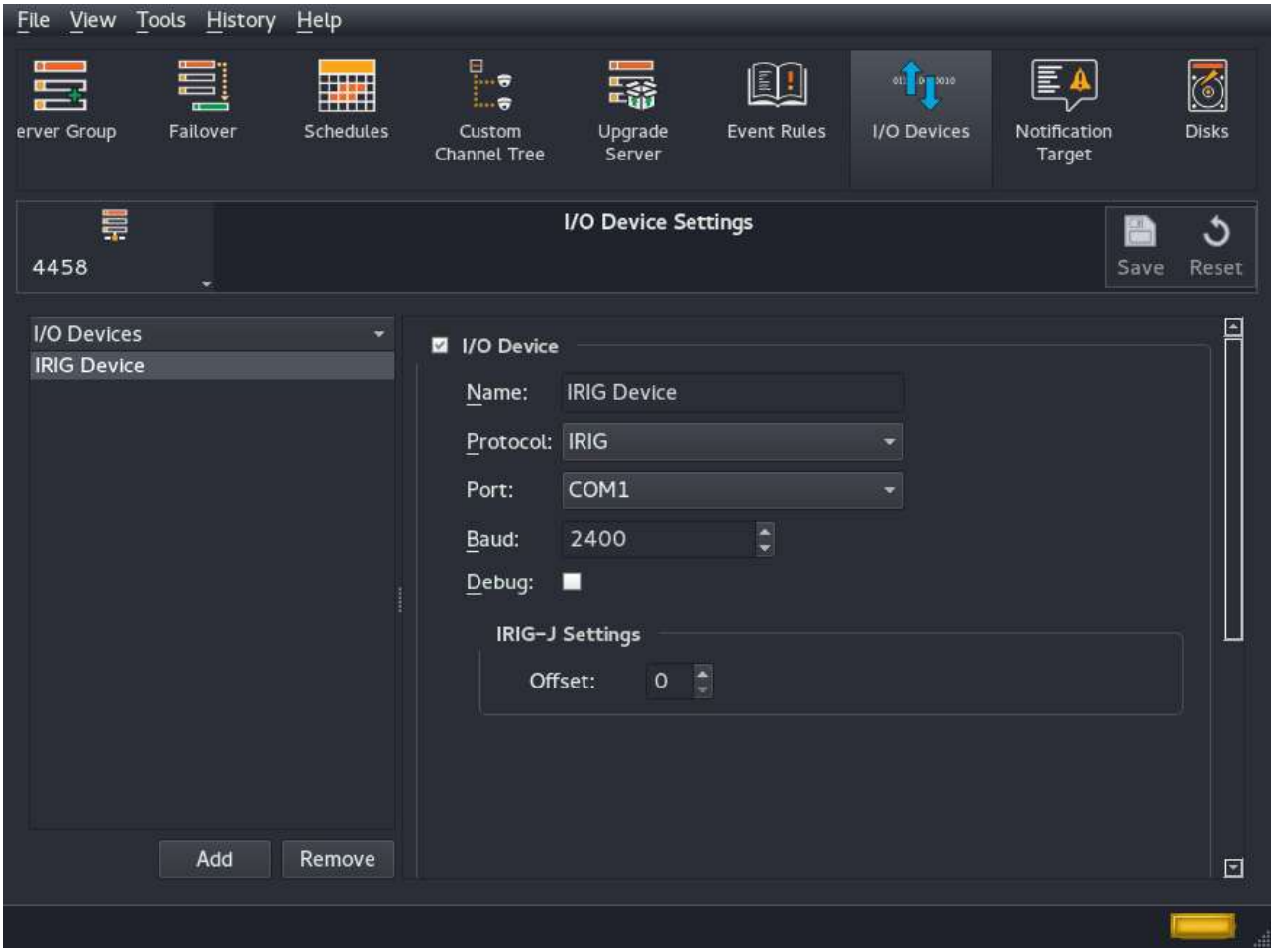


Figure 6.26: I/O Devices screen – IRIG protocol device

6.2.11.7 Configuring an IP Camera as an I/O device

An example of IP camera configuration is shown below:

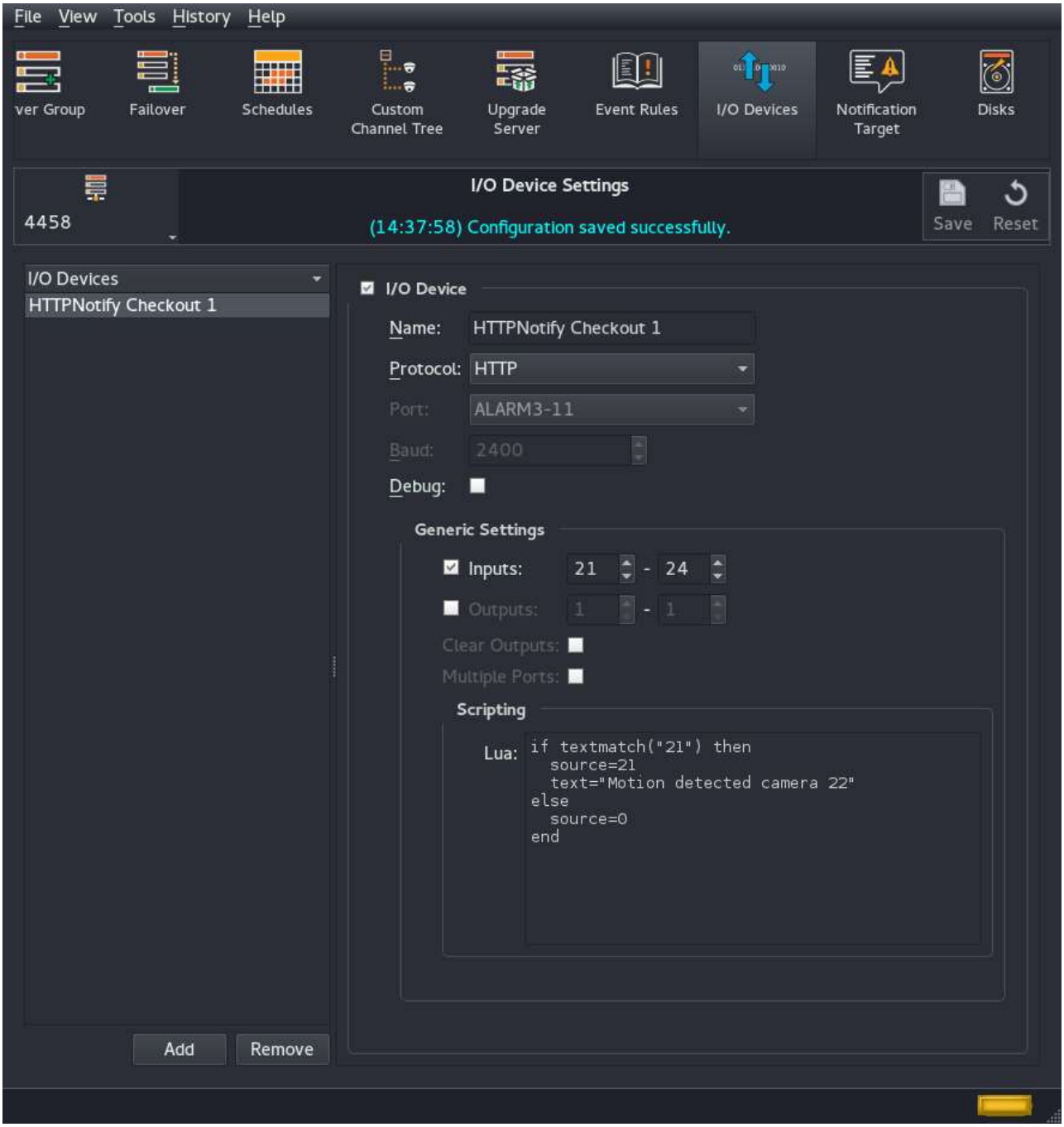


Figure 6.27: I/O Devices screen – HTTP Notification from IP camera

In this case, the IP cameras has been configured (using a Web Browser) to send HTTP Notifications of Motion Events to the Wavestore server. The Wavestore server has also been configured to record the Video Stream from the camera.

The Digital Input ID assigned to this I/O Device must match the Sort ID associated the camera channel in the Devices menu. An integration module has been entered, to enable parsing of the data from the camera.

Actions required on the Wavestore server (e.g. record video from a camera, on an enabled track for an

enabled camera channel, when an digital input is received) can be configured in the Event Rules screen (see section 6.12 – Event Rules).

In this example below, the server is configured to record video from the 'Checkout 1' camera to Track 1, when the HTTP notification is received from that camera.

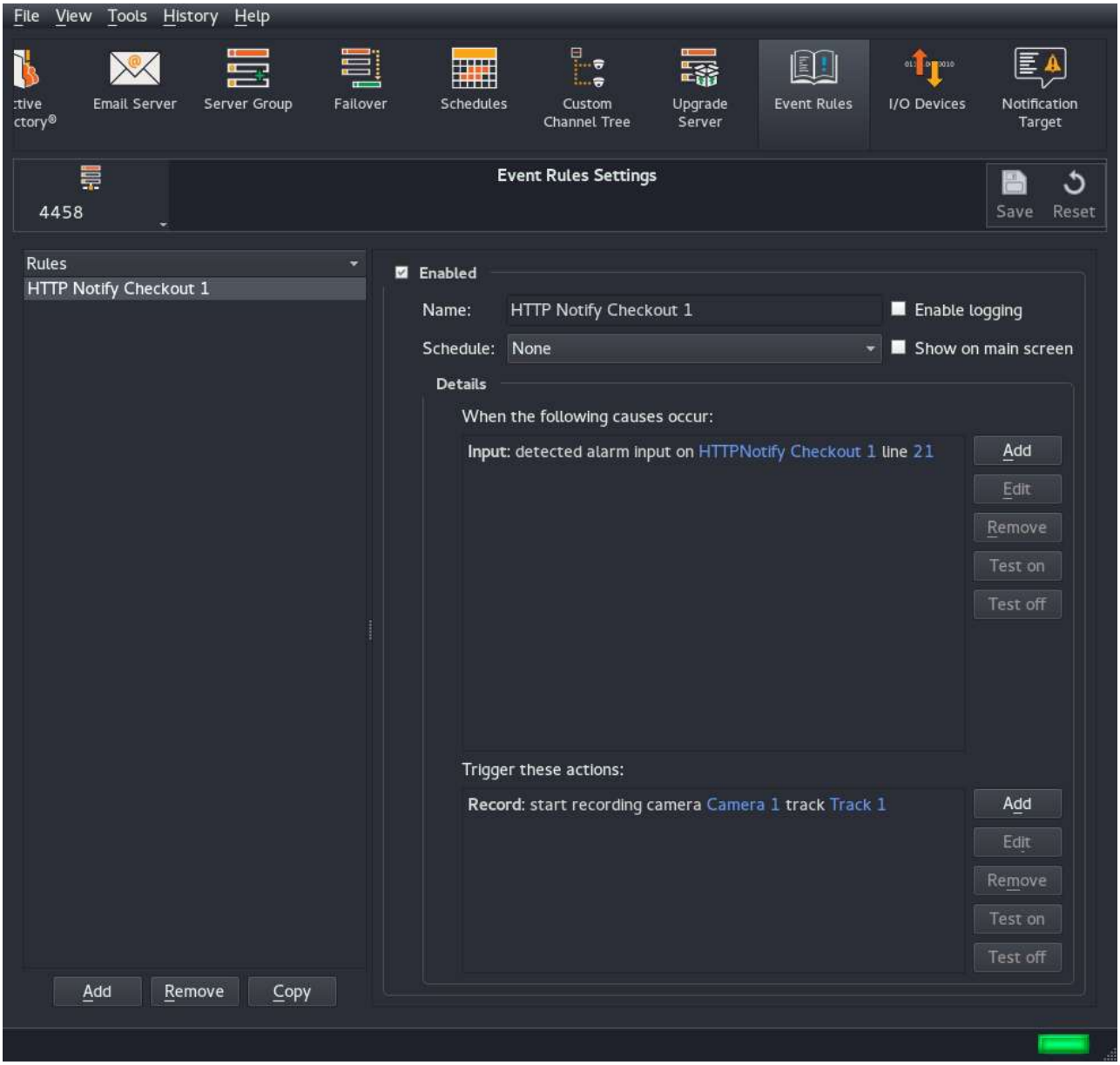


Figure 6.28: Event Rules screen – Motion Recording on HTTP Notification from IP camera

6.2.11.8 Configuring a POS Device as an I/O device

An example of POS Device configuration is shown below:

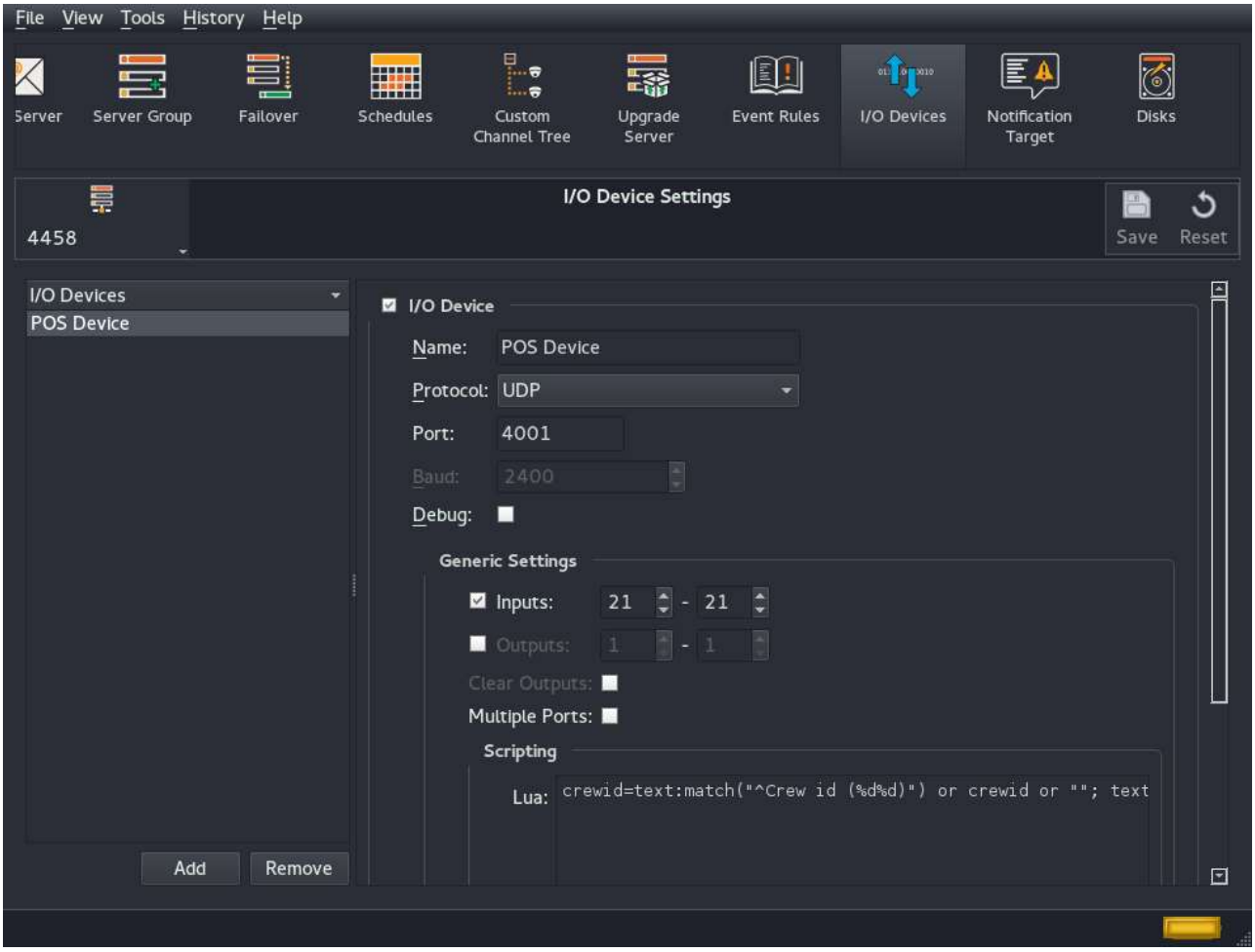


Figure 6.29: I/O Devices screen – POS device sending UDP format data

In this case, the POS terminal is sending transaction data over the UDP transmission protocol to UDP port number 4001. An integration module has been configured to enable parsing of the data from the POS Device. The data stream from the POS Device has been assigned digital input number 21.

Actions required on the Wavestore server (e.g. record metadata from an external input, on an enabled Metadata track for an enabled camera channel) can be configured in the Event Rules screen.

In this example below, the server is configured to the Record Metadata from input 21, on the Metadata track for the 'Checkout 2' camera:

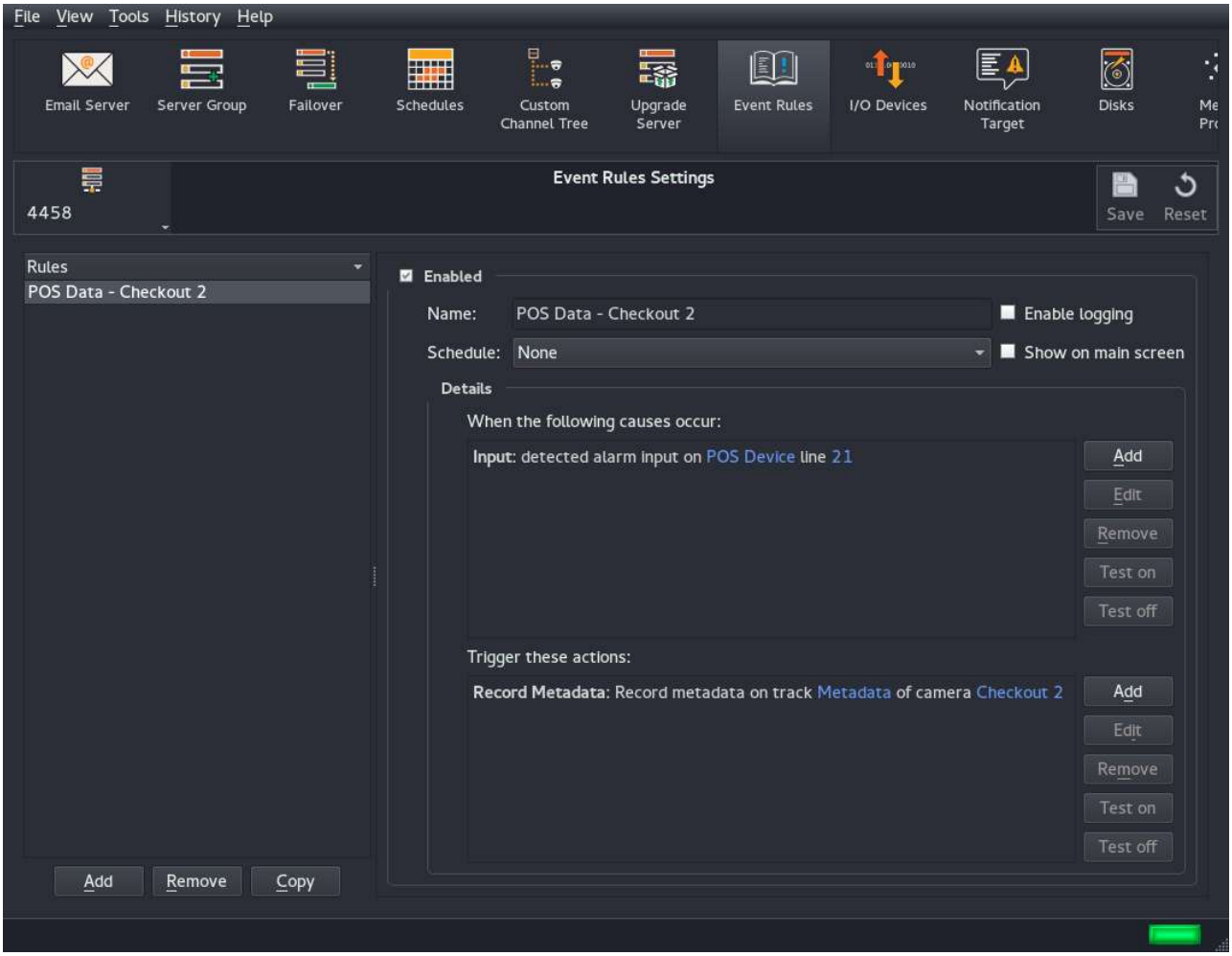


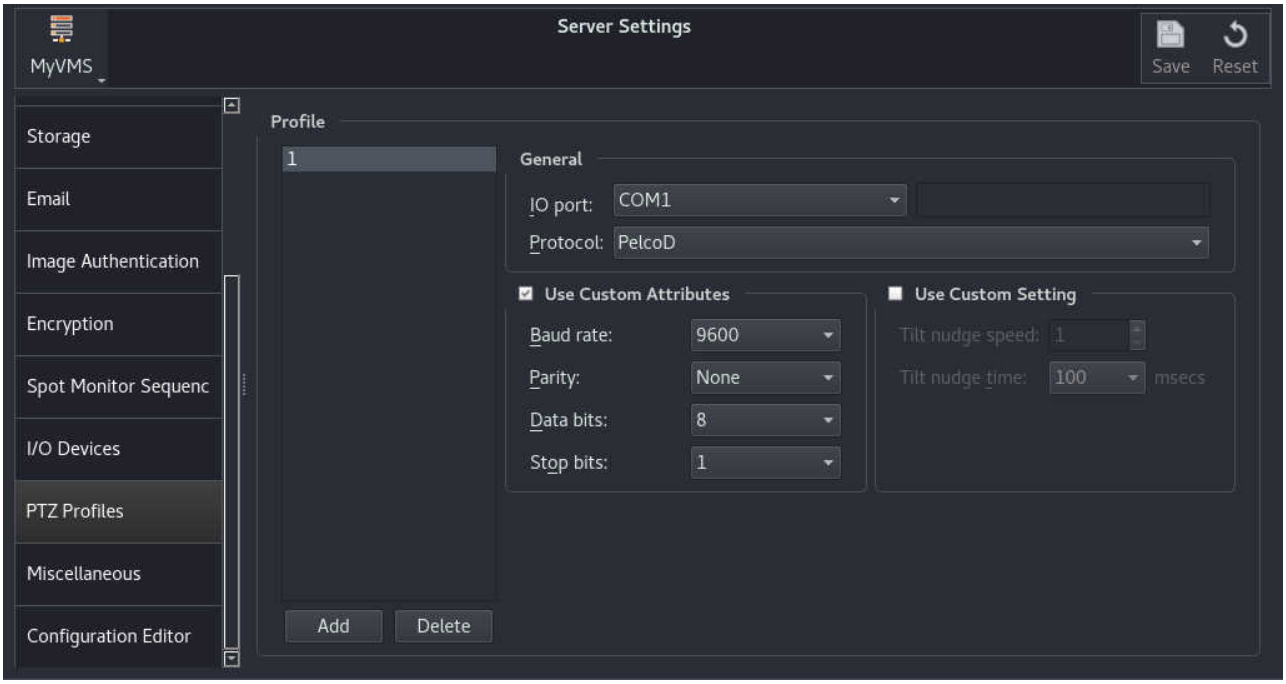
Figure 6.30: Event Rules screen – Recording Metadata from POS device

For further details, please contact the Wavestore Support Team.

6.2.12 PTZ Profiles

The 'PTZ Profiles' screen allows the configuration of collections of settings for PTZ control. Each individual camera can then be assigned a profile to use in the 'Cameras' setup screen. This often isn't necessary for IP cameras since the 'Auto' setting can handle most IP cameras without requiring manual configuration.

PTZ Profiles are always required for analogue PTZ camera configuration.



To begin, click the 'Add' button to add a new profile with default settings. Then configure the following settings as required:

IO Port
: This is the communication device to be used. It might be 'COM1' to 'COM4' for a serial port, or 'usb1' to 'usbN' for a USB serial device. For IP cameras it should be 'HTTP'.

Protocol
: This is the communications protocol to be used. The list contains a large number of IP protocols as well as some analogue serial protocols which are found at the end of the list.

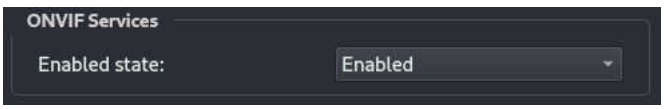
Use Custom Attributes
: These are serial settings used only for analogue PTZ communication. The required settings will depend on the cameras in use and should be supplied by the camera manufacturer.

Use Custom Setting
: These settings affect the speed and duration of PTZ nudge commands. These settings are rarely required.

Once the settings have been made and saved, the PTZ Profile will be available for selection in the 'Cameras' setup screen.

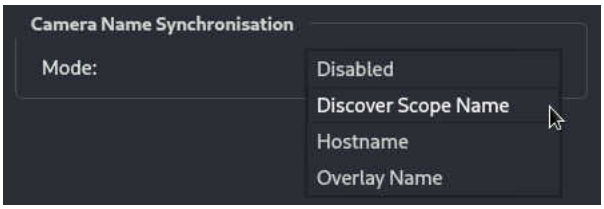
6.2.13 Miscellaneous

ONVIF Services



This option allows the server's ONVIF services to be enabled or disabled. By default on new installations they are disabled by default. Enabling them allows ONVIF functionality such as network discovery and re-streaming of video.

Camera Name Synchronisation



In the *Cameras* setup screen, it is possible to pull camera names from the cameras, or push the locally configured names to the cameras. There are multiple places where these camera names might be stored on the camera. This setting determines which location should be used when pushing or pulling camera names.

Discover Scope Name
: This is the name presented by the camera when scanning the network during a Discover operation. Some cameras may not allow this to be overwritten.

Hostname
: This is the camera's hostname and is only available after correctly adding the camera with the correct username and password. Note that hostnames may not include spaces. They will be removed automatically if pushed to the camera.

Overlay Name
: This is the camera name stored in the camera's internal settings and is only available after correctly adding the camera with the correct username and password. Support for reading and writing the Overlay Name is only available for supported cameras. Please check the camera compatibility list for details of supported cameras.

Event Stream Recording

A recording track can be configured to record events which occur on the currently selected server. Event search can only be performed if this recording track has been enabled.

To record these events, ensure the "Event Stream Recording" checkbox is checked. It is possible to either:

- Use the Disk and Recording Duration settings from a Camera Group (selectable but uses the first group by default)

- Manually specify the desired Disk and Recording Duration

Metadata Stream Recording

A recording track can be configured on the server itself (not associated with individual camera channels), for applications such as GPS data input.

To record this data it is possible to either:

- Use the Disk and Recording Duration settings from a Camera Group (selectable but uses the first group by default)
- Manually specify the desired Disk and Recording Duration

Track Names

Each of the three Recording Tracks can be given a 'friendly' name. This will be used in the UI in certain places such as the Find Screen.

To configure, click in the text field, enter the text you require, then click Save.

6.2.14 Configuration Editor

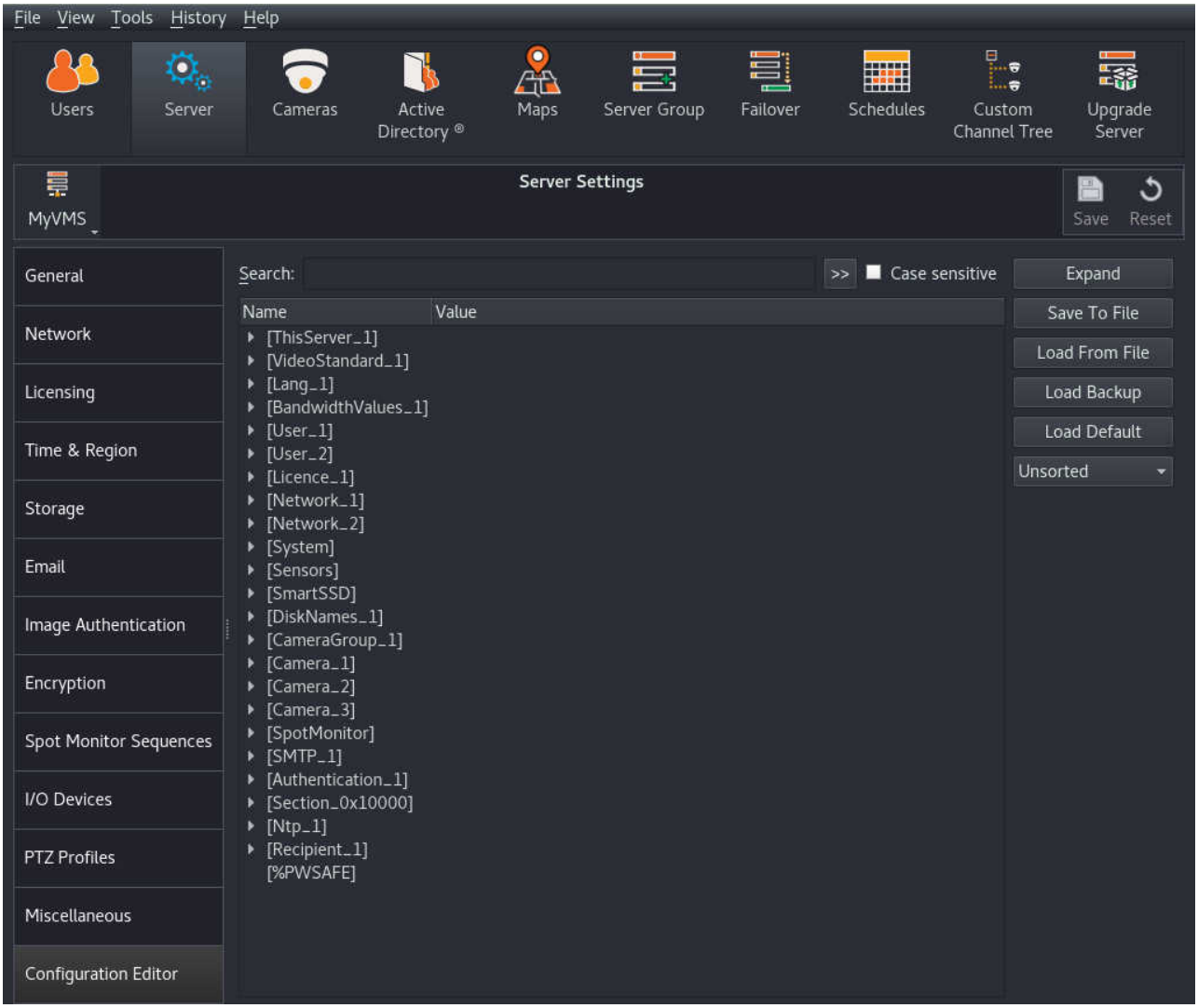


Figure 6.31: Configuration Editor

The 'Configuration Editor' menu contains a representation of the raw configuration file of the Wavestore server.

The Search dialog box allows the user to quickly find a configuration section by entering text, and then clicking on the '»' button.

The configuration file can be edited manually, saved for future use (onto removable media, or a networked WaveView PC), or overwritten by an imported file.

If required, the server configuration settings can be restored to their default state (click 'Load Default').

Saving and Loading Server Configuration File

It is good practice to back up the configuration file before making major changes to the configuration of the server (click 'Save to File').

A saved configuration file can be uploaded onto the server at a later date if required (click 'Load from File').

When loading a configuration file, several options are provided to prevent unique server settings being overwritten:

Current 'install' User Login Details

Network Settings

Licence

Disk Assignments

System Monitoring Settings (fans, temperatures, etc. usually specific to the model of hardware in use)

If attempting to load or save on the Wavestore server itself, it may be necessary to "mount" a USB device – see section 9.17 – Accessing a USB disk on the Wavestore server.

Loading a Backup Configuration File

The Wavestore automatically performs a backup of the configuration early every Monday morning. It also makes a backup whenever a configuration file is loaded and when a major version upgrade is performed. A maximum of 50 backups are stored, with the oldest being deleted once the limit is reached.

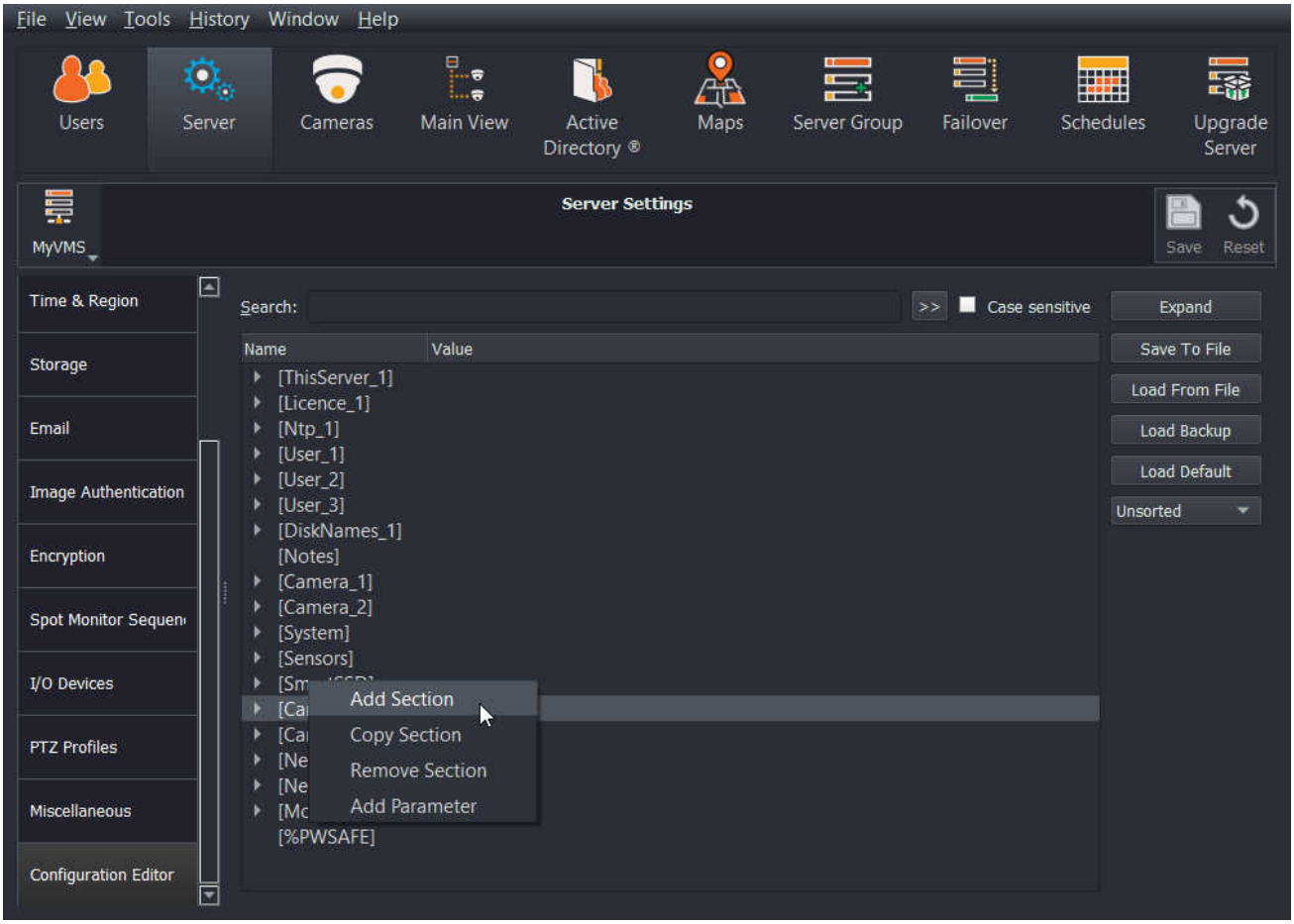
When the 'Load Backup' button is clicked, a list of all the available backups is presented. The user can then select a configuration backup to restore.

6.2.15 Configuring Wavestore server for use as proxy server

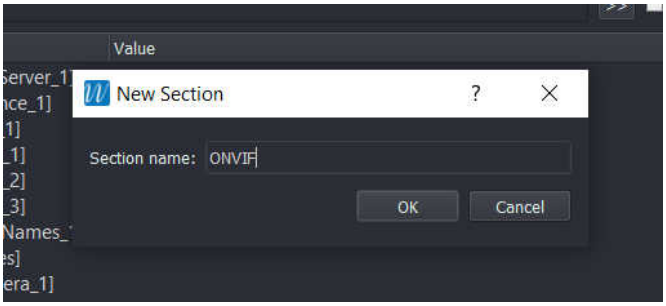
If the Wavestore server is configured with multiple network ports, it can be useful to configure the server as an HTTP proxy server, so that a networked PC (e.g. a PC connected to the 'eno1' port) can access devices (such as IP camera or iSCSI storage) that are connected to other network ports on the Wavestore server. This supports HTTP and HTTPS proxy. See the the Wavestore knowledgebase article on proxy for more information.

To enable this function, additional configuration is required in the Configuration Editor.

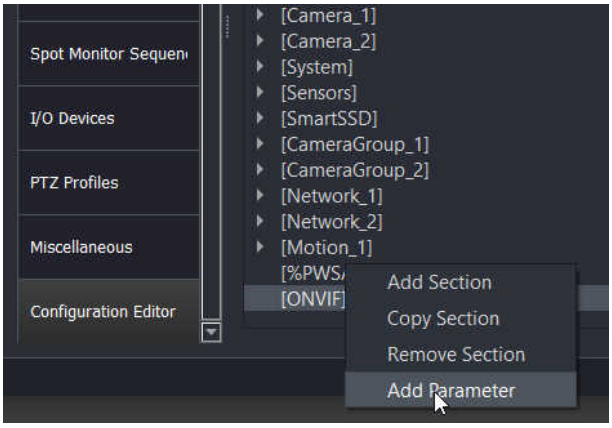
Right click on any of the existing configuration headings in square brackets, and click on 'Add Section':



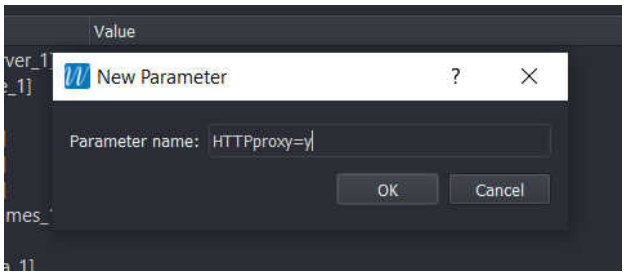
In the dialog box that appears, enter 'ONVIF' as the new section name, then click OK:



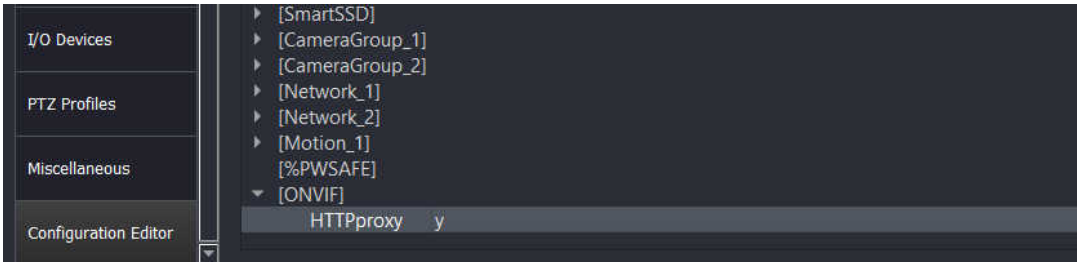
The new section will appear at the bottom, so scroll to find it if necessary. Right–click on the new Section Name that you have created, and left click on 'Add Parameter':



Enter 'HTTPproxy=y' as the new parameter, then click OK.



Click 'OK', and click 'Save' to confirm your changes.



Restart the server software (menu path View → Setup → Server → General → Restart Process)

To connect to the IP devices from your PC, using the Wavestore server as a proxy server, you'll also need to reconfigure your web browser with the IP address details of the Wavestore server Ethernet port that you connect to from the PC.

When you connect for the first time, you'll also be prompted to enter a valid Wavestore user 'install' level logon ID and password.

6.3 Cameras

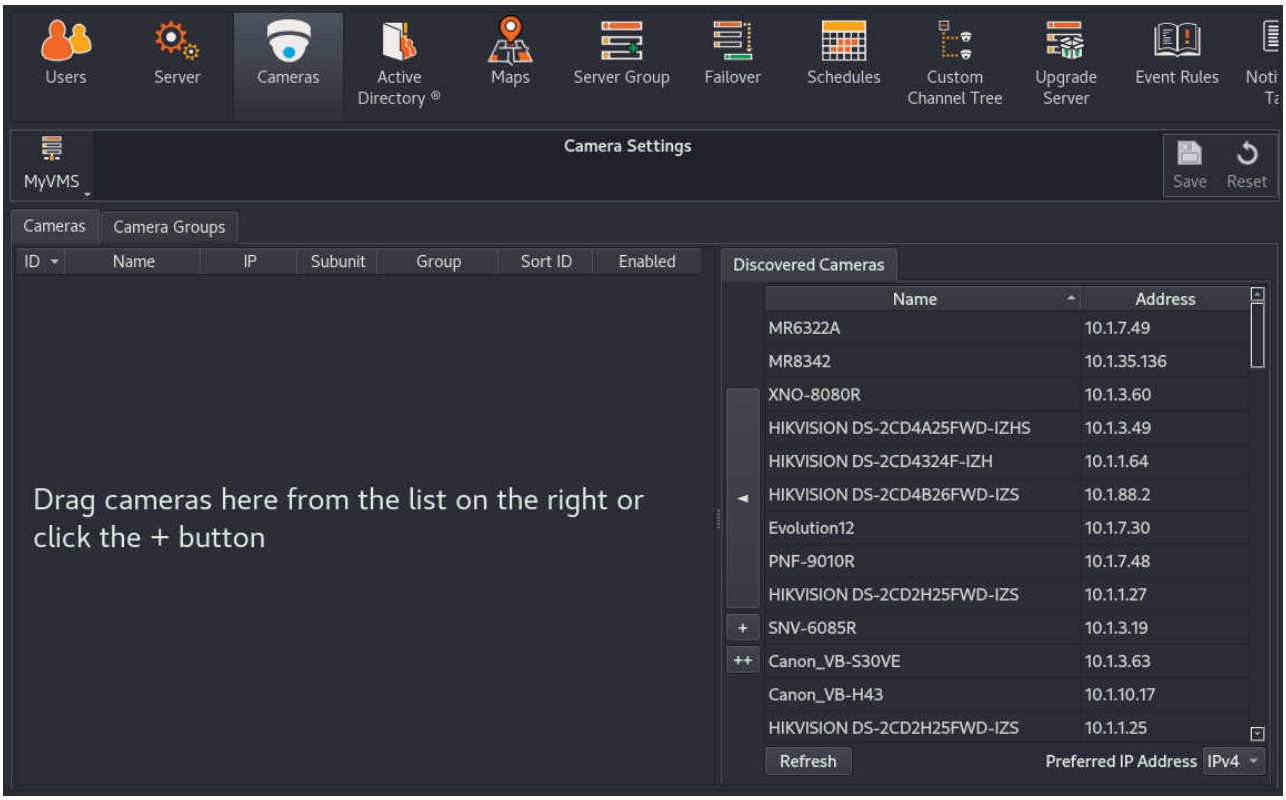
The Cameras setup screen allows for rapid discovery and configuration of cameras, audio and talkback (also known as "backchannel") devices.

Wavestore allows allocating cameras to 'Camera Groups' so that configuration changes can be easily managed for large collections of cameras, rather than having to change every camera individually.

This section describes the process of discovering and adding cameras, as well as configuring them either individually or via Camera Group settings.

6.3.1 Discovering and Adding Cameras

Upon entering the 'Cameras' screen, the Wavestore will start a process of searching the network for any available IP cameras. Once fully received this list will not be refreshed for another 30 minutes, or until WaveView is restarted, or Refresh is clicked.



The Discovered Cameras can be sorted by name or IP address to make it easier to find the desired device. The names are provided by the cameras themselves and the information available can vary by manufacturer, many will report the manufacturer and model.

The preferred default shown IP Address can be selected in the bottom-right part of the Discovery Cameras tab. Options are IPv4 or IPv6. If IPv6 is selected, the default address for a camera will show its configured IPv6 address. If a camera doesn't have an IPv6 address it will fallback to displaying its IPv4 address. By double-clicking on a camera's address field it's possible to see all the available IP addresses for the camera, including link-local addresses, and select the desired one.

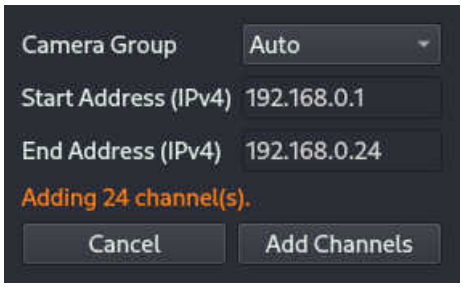
Note that IPv6 is not currently supported for multicast.

To add a camera, simply click and drag it from the right–hand pane to the left. Use Shift+click to select a range, or Ctrl+click to select multiple individual items. The left arrow button can also be used instead of dragging and dropping.

When added, cameras will be assigned to the first Camera Group automatically. If there are no existing Camera Groups, a new one will be created and the user is prompted for a username and password to be used to access the cameras. If the cameras have different usernames and passwords, these can be specified per–camera later.

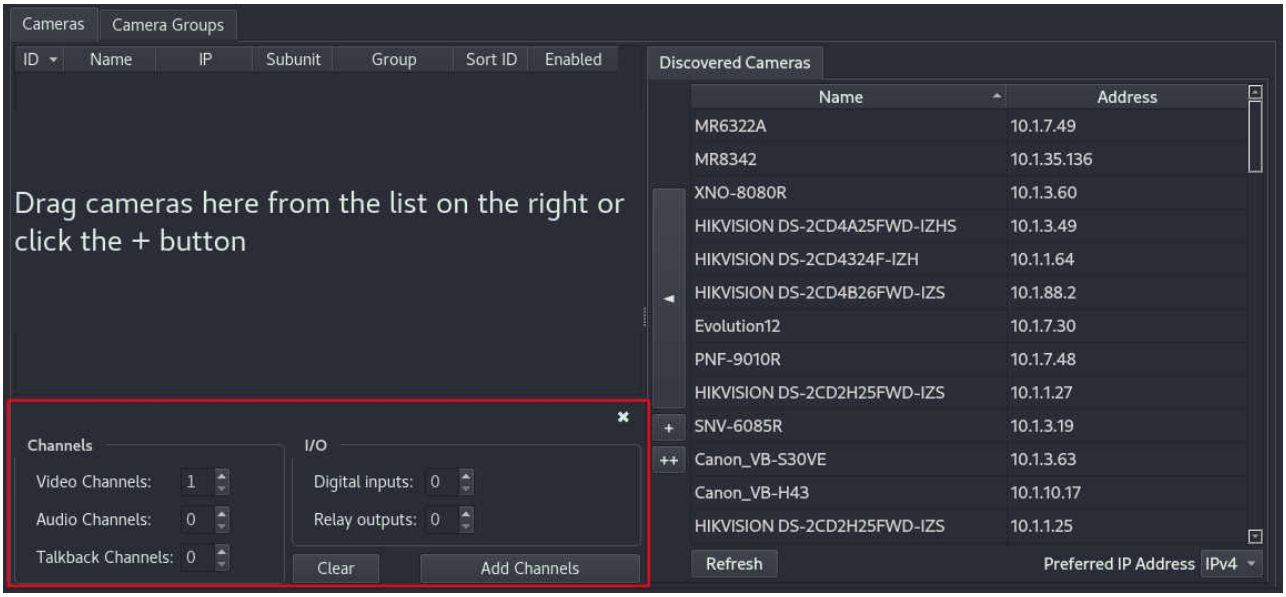
Another way of adding a camera is using the + (plus) button. This simply adds a new row to the Cameras table. The IP Address and Group can then be manually specified.

It's also possible to add multiple cameras by providing an IP address range. To do this, click the '++' button. The following dialog will appear:



It is possible to specify the Camera Group to which the cameras will be assigned, and the start and end of the IP range. If the range consists of more cameras than the server can support, or if the range appears to be invalid, the dialog will provide a suitable warning.

If it is necessary to add multiple channels for one device, or to use digital inputs/outputs from the device, hold the Shift button whilst clicking the + (plus) button. This opens a new panel which allows the extra details to be specified:



Camera details can also be imported from a spreadsheet in the CSV (Comma–Separated Values) format. See section 6.3.4 – Importing Camera Settings.

Once cameras have been added, the table on the left can be used to:

- Edit the camera name.
- Edit the IP address and port of the camera.
- Change the assigned Camera Group of the camera.
- Change the Sort ID of the camera – see section 9.21 – Sort IDs.
- Enable/Disable the camera.

To change the assigned Camera Group, either left–click the group name to select from a list of existing groups, or right–click for more options. The right–click menu has several options:

Change Camera Group – choose an existing group to re–assign the selected camera.

Change Camera Group – Create New Group – this creates a new group with default settings and prompts the user for a username and password to use for the cameras in this new group.

Change Camera Group – Clone Group – this creates a new group with the settings copied from the selected existing group. This is useful when you need to split a group into multiples with slightly different settings.

Remove Cameras – removes the currently selected camera or cameras.

Camera Setup Web Page – opens up the default browser using the currently selected camera's address. Alternatively, if the Gateway Proxy feature is enabled for the associated Camera Group, the URL used will be the appropriate one to route traffic via the Wavestore gateway proxy feature, removing the need for direct network access to the camera.

Synchronise Camera Names – allows pushing local camera names to the selected camera(s), or pulling the names from the selected camera(s). See section 6.2.13 – .

Selecting an individual camera in the camera table causes the right–hand pane to show the settings for the individual camera. This is covered in section 6.3.3 – Individual Camera Settings.

Clicking the 'Camera Groups' tab in the left–hand pane opens the 'Camera Groups' settings which are covered in the next section.

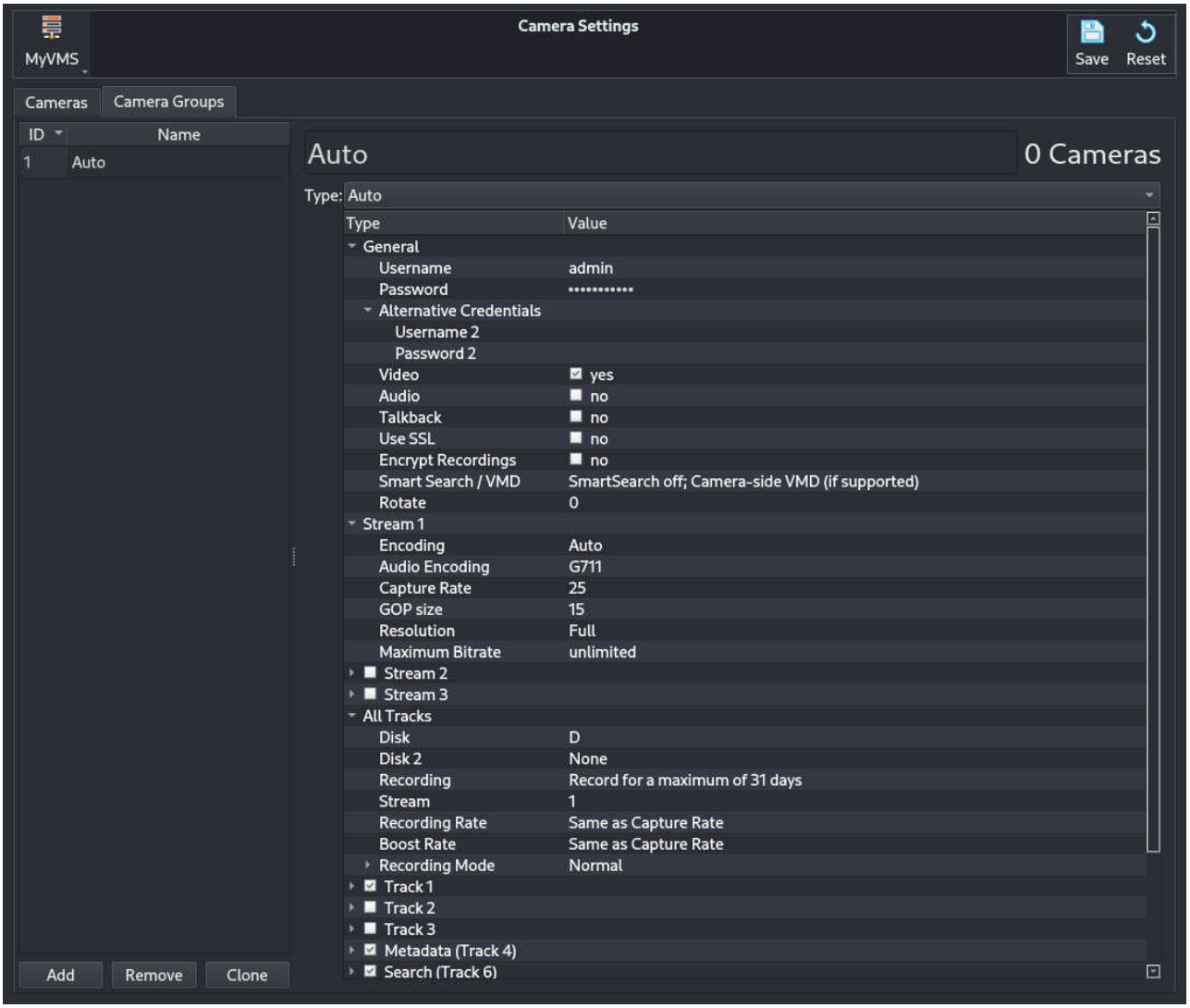
Multiple selection is possible by clicking and dragging down the camera number column. Alternatively Shift + click and Ctrl + click can be used. This allows changing camera groups for multiple cameras at a time, or removing multiple cameras. It's also possible to use the delete–key to remove the selected cameras.

The camera table can also be sorted by different properties by clicking the column header of interest.

6.3.2 Camera Group Settings

The Camera Groups screen allows editing settings for Camera Groups as well as adding and removing groups.

Note that when settings are changed for existing cameras, where possible they will continue streaming with the old settings until the new settings have been configured in a separate profile. Then streaming is switched over to the new profile with the new settings. When this happens, the subtitles will show "Reconfiguring".



The 'Add' button creates a new group with default settings. The 'Remove' button removes the currently selected groups. Multiple groups can be selected and removed at the same time either by clicking and dragging on the group number column, or by using Shift + click or Ctrl + click to do multiple selection. It's also possible to use the delete–key to remove the selected cameras.

The 'Clone' button causes a new group to be created with a copy of the settings from the most recently selected group.

The 'Remove' and 'Clone' options are also available through a context menu by right–clicking on a camera group in the table.

Change the name of the group by selecting it in either the table or in the right–hand pane.

The right–hand pane shows the amount of cameras that belongs to the selected group. In the example above, 17 cameras belong to the 'Group 1'–group.

Each Camera Group has a Type. The default Type is Auto which allows the Wavestore to try to automat–ically detect the device and use the optimal settings.

The various types are described below:

Auto

This is an IP device type where the Wavestore will try to auto-detect the best method of communication. The Wavestore will also try to configure the device with the desired video streaming settings.

Important Note: Auto-configure works well when one Wavestore configures one or more cameras, but not when a camera is shared between Wavestore systems (or other ONVIF clients) each of which will attempt to reconfigure the camera and might alter or delete profiles or encoders which another system is using. If more than one Wavestore or other ONVIF client will access the camera: select ONVIF protocol as the Camera Group type on the Wavestore and enter a manual profile, or RTSP protocol with an appropriate request string. Also, do not add the same camera with the same subunit to the same Wavestore more than once in Auto-configure mode. If a copy of a channel is required, use VirtualSpotMonitor.

ONVIF

This is an IP device type which uses the ONVIF standard for communication and setup.

ONVIF-Multicast

This is an IP device type which uses the ONVIF standard to stream from a device in Multicast mode.

RTSP

This is an IP device type which uses the RTSP communication protocol to pull data.

HTTP

This is an IP device type which uses the HTTP communication protocol to pull data.

MxPEG

This is an IP device type which communicates with Mobotix cameras, retrieving video in the MxPEG format.

Ampleye

This is an IP device type which communicates with Ampleye cameras, retrieving video in the JPEG2000 format.

VirtualSpotMonitor

This is a special capture type used for the Virtual Spot Monitor feature within Wavestore.

Audio

This capture type communicates with an analogue audio capture card. Possibly the audio inputs and outputs on the motherboard, or a PCI or USB audio interface.

Stretch

This is a capture type used to communicate with an analogue capture card, usually providing video and audio. There are various "sub-types" which correspond to the model number of the capture card.

File

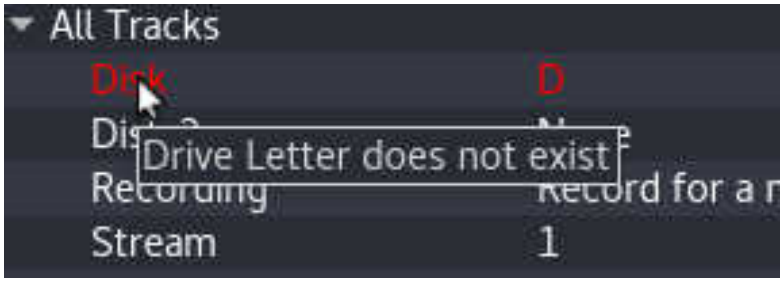
This is a capture type used to play back a video or audio file in a loop. See section 9.6 – Configuring a File Playback Camera.

Backup

This is a special capture type used for Failover servers. See section 6.9 – Failover.

All the various options are explained below. Not all options are available for all types, in which case the supported types are listed.

If there is a problem with a particular option, it will be highlighted with a red colour. The reason for the error can be found by hovering the mouse over the option. See example below where the drive letter doesn't exist. Please note that this is currently only implemented for some of the parameters.



Also note that some other options will be higlighted with a yellow colour while they are fetching for more data from the server.

General

Username

The username to be used to authenticate with the camera or device. Note that if the username is modified, it is necessary to re-enter the password. The user specified must have permissions to configure the camera if the "Auto" group type, or the "Auto-configure Camera Streams" options are to be used.

Not applicable for "VirtualSpotMonitor" and "Backup" group types.

Password

The password to be used to authenticate with the camera or device.

Not applicable for "VirtualSpotMonitor" and "Backup" group types.

Alternative Credentials

Allows other username and password combinations to be provided. These will be tried if the primary username and password fails to authenticate.

Not applicable for "VirtualSpotMonitor" and "Backup" group types.

Video

Enables streaming of video from this device. Default is On.

Only applicable for "Auto", "ONVIF", and "RTSP" group types.

Audio

Enables streaming of audio from this device.

Not applicable for "ONVIF-Multicast", "VirtualSpotMonitor", "Audio", "Stretch", and "Backup" group types.

Talkback
: Enables sending audio to this device. Sometimes alternatively called "backchannel".

Not applicable for "ONVIF-Multicast", "Ampleye", "VirtualSpotMonitor", "Audio", "Stretch", and "Backup" group types.

Talkback Type
: Allows choosing the method of sending audio to the device. The default is Auto and will work for most devices.

Only applicable for "ONVIF" and "RTSP" group types.

Request
: Note that certain group types have a Request field under the ***Stream 1/2/3*** section. The ***Request*** parameter under the General section is used to allow options to be set for the streaming. For example this might be to force "HTTP Tunneling" or transmission over UDP. The default empty setting should be used in the vast majority of cases.

Not applicable for "Auto", "RTSP", "VirtualSpotMonitor", "Audio", "Stretch", and "Backup" group types.

Use SSL
: If enabled, causes the Wavestore server to communicate with the device using Secure Sockets Layer.

Not applicable for "ONVIF-Multicast", "VirtualSpotMonitor", "Audio", "Stretch", and "Backup" group types.

Encrypt Recordings
: If checked, this channel will be encrypted during recording. This will only work if the Wavestore server has been correctly configured for encryption. See section 6.2.8 – Encryption.

Smart Search / VMD
: Enables the capture and recording of metadata relating to the amount of motion in the video. This can be used for either server-side or camera-side motion detection together with Smart Search. See section 9.8 – Configuring Smart Search for more details.

Only available for "Auto", "ONVIF" group types. For "Stretch" group types this feature is always on and so is not configurable.

Pull Point
: If enabled, the Wavestore server will "subscribe" to the event stream of the device. This means that the camera will notify the Wavestore of any events it detected such as motion or video analytics

events.

Only available for "ONVIF" group type. For "Auto" type, event streaming of some kind will be enabled if possible.

Auto-configure Camera Streams

This setting means that the Wavestore will attempt to create push stream settings to the device, for example by creating ONVIF Profiles for ONVIF devices. Rather than having video stream settings configured and stored on the camera, the settings will be made within Wavestore and pushed to the camera when necessary.

Important Note: Auto-configure works well when one Wavestore configures one or more cameras, but not when a camera is shared between Wavestore systems (or other ONVIF clients) each of which will attempt to reconfigure the camera and might alter or delete profiles or encoders which another system is using. If more than one Wavestore or other ONVIF client will access the camera: select ONVIF protocol as the Camera Group type on the Wavestore and enter a manual profile, or RTSP protocol with an appropriate request string. Also, do not add the same camera with the same subunit to the same Wavestore more than once in Auto-configure mode. If a copy of a channel is required, use VirtualSpotMonitor.

Only available for "ONVIF" group type. For "Auto" type, this is implicitly On.

Rotate

Requests the camera to rotate to the transmitted image. Default is 0, no rotation. Other allowed values are 90, 180 or 270, representing degrees clockwise.

Only available for "Auto" and "ONVIF" group types. This functionality is available on most, but not all, ONVIF-compliant cameras. If the camera doesn't support it, the "Cxauto" camera log will say "Image rotation not supported!", where "x" is the camera number. These are available under "Tools > System Log... > Extra Logs".

Input Select

Allows switching between the "line" and "microphone" inputs on the audio device.

Only available for "Audio" group type.

Volume

Set the input capture volume for the audio device. The volume starts from 0 and the maximum is 100.

Only available for "Audio" group type.

Analogue Format

This is the video standard used for capturing video. For Standard Definition devices it is usually PAL or NTSC. High Definition capture devices have more options such as 1080p60, 1080i50, 720p60. These are all standard formats for High Definition video.

Only available for "Stretch" group type.

Stream 1/2/3

Note that Stream 3 is only available for the group types RTSP, ONVIF, and Auto.

Profile

The name of the camera Profile which will be used for streaming video. This list is populated by querying the first camera in this Camera Group.

Only available for "ONVIF" and "ONVIF-Multicast" group types.

Request

Allows a specific request string to be provided for each of the 2 possible streams. This is used to make requests to the camera to retrieve video. The string can either be entered manually or a pre-set can be chosen from the drop-down selector which contains request strings for many major camera manufacturers.

Only available for "RTSP" group types.

Encoding

This is the video encoding to be used. Selectable between "Auto+", "Auto", "H264", "H265", and "JPEG". "Auto+" will favour H.265, then H.264, then JPEG. "Auto" will favour H.264 then JPEG.

Only available for "Auto" and "Stretch" group types, and "ONVIF" group type when "Auto-configure Camera Streams" is set to "Yes".

Audio Encoding

This is the audio encoding to be used. Selectable between "Auto", "AAC", and "G711". "Auto" will favour AAC, then G.711.

Only available for "Auto" and "Stretch" group types, and "ONVIF" group type when "Auto-configure Camera Streams" is set to "Yes".

Capture Rate

This is the rate, in "images per second" that will be used to encode the video stream.

Only available for "Auto" and "Stretch" group types, and "ONVIF" group type when "Auto-configure Camera Streams" is set to "Yes".

GOP Size

GOP is Group Of Pictures. In certain compression formats such as H.264 and H.265, there are "i-frames" which are full images, followed by a number of "p-frames", which are essentially contain only the differences between this frame and the previous one. The GOP size dictates how many frames there are in a group. So for example, a GOP size of 5 would suggest 1 i-frame followed by 4-pframes, and then the same repeated.

Only available for "Auto" and "Stretch" group types, and "ONVIF" group type when "Auto-configure Camera Streams" is set to "Yes".

Resolution

The resolution at which the video will be encoded. "Full" means the highest available resolution, but other available resolutions are usually specific industry standard terms. A custom resolution may be specified. If the precise resolution is not supported by the camera, Wavestore will attempt to choose the closest available match.

Only available for "Auto" and "Stretch" group types, and "ONVIF" group type when "Auto-configure Camera Streams" is set to "Yes".

Quality Mode

This dictates the type of compression available. These are explained in more detail later in this section.

Only available for "Stretch" group type.

Constant Quality — This is the default, and recommended setting for most uses. The video encoder tries to keep the video quality at the same level. This has the benefit of ensuring that no matter how much activity or detail there is in the scene, the video quality will remain. The disadvantage is that high levels of activity or detail can cause the bitrate to increase, meaning more storage and bandwidth is required.

Constant Bitrate — The video encoder attempts to keep the bitrate at a roughly constant level. The advantage of this is that it makes it easier to calculate the storage and bandwidth requirements. The disadvantage is that when there is increased activity or detail in the scene, the image quality will actually reduce in order to keep the data rate at the desired level.

Variable Bitrate — The video encoder allows the data rate to fluctuate around the "Average bitrate" setting, but when there is increased detail or activity, the data rate is allowed to increase up to the configured "Maximum bitrate" setting. Similar to Constant Quality, this setting has the disadvantage of a varying data rate meaning that the required storage and bandwidth varies depending on the scene content.

Average Bitrate

This is the average bitrate to use for the encoding (in Kilobits per second). It does not apply when the Mode is Constant Quality.

Only available for "Stretch" group type.

Maximum Bitrate

This defines the maximum bitrate to be used for encoding. When the group type is "Stretch", this setting is only applicable when the Mode is set to Variable Bitrate. Note that for ONVIF IP cameras, this feature is optional and may not have the desired effect. In that case the Quality setting can be used to reduce the bitrate per camera if desired. See the "General" settings under section 6.3.3. A per-camera Quality setting is often the better option to ensure that the video quality does not

degrade when there is lots of activity, which may happen if attempting to stay below a specified maximum bitrate.

Only available for "Stretch" and "Auto" group types, and "ONVIF" group type when "Auto-configure Camera Streams" is set to "Yes".

All Tracks / Track 1–8

Wavestore uses a system of different "recording tracks". Tracks 1 to 3 allow recording the video streams with different settings. Track 4 is for general metadata associated with the camera. Track 5 is currently unused. Track 6 is for Smart Search metadata, Track 7 is for Audio (input), and Track 8 for Talkback (audio output).

The 'All Tracks' option is a shortcut for making settings that apply to all recording tracks (1 to 8). If the individual tracks have been configured with different settings then that setting will show as "various" under "All Tracks".

The available settings are described below:

Disk

Hard disk where the recording will be stored. This is chosen from a list of disk letters which are configured in the Storage page under the Servers setup creen.

Disk 2

An optional secondary hard disk for a mirror of the recordings.

Recording

Duration, in days, that footage is to be stored. The "Mode" can be either:

- **Approximately** – once the hard drive is full, and the server is about to start overwriting older footage, server uses the value entered for 'Time Period' to determine how much of the hard drive space to allocate to each camera/recording track. As an example, let's take the example of a Hard Disk that is being used to store footage from two cameras. Camera A is configured set to record for 'Approximately 15 Days', and Camera B configured to record for 'Approximately 5 Days'. When we compare the storage duration for the two cameras, we can see that Camera A is required to store footage for three times the period of Camera B, so Camera A will be allocated three as much as space on the hard drive; so in the case Camera A will be allocated 75% of the hard drive, and Camera B will allocated the remaining 25% of the drive.
- **Maximum** – this option sets a hard limit, after which footage will be deleted; as an example, if this option is enabled, with Time Period set as '7 days', and the Wavestore server then left to record for a few days, on Day 8, the footage from Day 1 will be deleted in increments.

Stream

Selects which Stream (1 or 2) will be recorded.

Recording Rate

Selects the recording framerate. The default and recommended setting "Same as Capture Rate" means that all received frames will be recorded. For H.264, H.265, and MPEG-4 streams this setting should generally be left as the default. If it is set to a lower rate than the rate the camera is outputting then only "i-frames" – the full images – will be recorded. See section 9.12 – H.264, H.265 and Framerates for more information.

Boost Rate

Recording framerate to use when a "boost" event action occurs, as configured in the Event Rules menu (section 6.12 – Event Rules).

As with the normal recording rate setting, this option isn't always well–suited to use with H.264, H.265, and MPEG–4, due to to the presence of P–frames. See section 9.12 – H.264, H.265 and Framerates for a more detailed explanation.

Recording Mode

A variety of recording modes are available...

Normal	Normal continuous record (when schedule is on). Schedule may be set and will affect the recording. Pre Record setting is not applicable.
Event	Normally no recording but Event Rules can trigger recording. Pre Record parameter may be set if needed. Schedule may be set and will affect the recording.
Normal + Event	Continuous recording when schedule is On. Event recording if event rules triggered and schedule is Off. Schedule and/or Pre Record may be set. Schedule will not affect event recording.
Framerate Boost on Schedule	Normal recording with boosted framerate when schedule is On.
Motion	If supported by the device, motion will trigger recording. Pre Record parameter may be set if needed. Schedule may be set and will also affect the recording. Requires "Smart Search / VMD" to be enabled except for the "Stretch" group type.
Normal + Motion	Continuous recording when schedule is On. If supported by the device, motion will trigger recording when schedule is Off. Schedule and/or Pre Record parameter may be set. Schedule will not affect motion recording. If desired to have a separate schedule for motion, use Normal + Event mode. Requires "Smart Search / VMD" to be enabled except for the "Stretch" group type.

Schedule

Recording of the Track can be controlled by a configured Schedule (see section 6.10 – Schedules). This setting allows a schedule to be chosen within which recording will be enabled.

Pre Record

When using event or motion recording, this value specifies the number of seconds to record before the start of the event.

Pre Boost

When set to a value other than "Never" this setting causes the framerate of recordings before an event to be "boosted", that is increased. For example, if set to 5 seconds, when an event triggers a framerate boost, 5 seconds of recording before the event will have the increased framerate. Note that the duration specified here is only approximate.

Post Motion

When recording on Motion, this value specifies the number of seconds to record after the end of the Motion event. For Event recording, the equivalent Post time is specified in the Event Rule so that different values can be used for different event types.

PTZ Options

Enable
: Allows PTZ to be disabled for this camera group. Particularly useful when using the "Auto" group type because it's possible that PTZ functionality might be available on the camera and automatically detected, but not desired.

Profile
: Allows specifying the PTZ Profile to be used to control this camera, where a "PTZ Profile" is a collection of settings. The default "Auto" setting will generally manage to automatically set up most IP cameras. For some IP cameras, and all analogue cameras, it will be necessary to set up a PTZ Profile which can be done under Server setup screen. See section 6.2.12 – PTZ Profiles.

Pan Reverse
: Reverses Pan Left/Right commands for this camera.

Tilt Reverse
: Reverses Tilt Up/Down commands for this camera.

Warning Options

GOP Check
: It is generally recommended to use a GOP size (Group Of Pictures) of 64 or lower in order to get the best performance from Wavestore. By default, the System Log will provide warnings for any streams which exceed this recommendation. This setting allows the check to be disabled to silence those warnings.

Analytics

This section is only present if an Analytics Engine has been configured. See section 6.2.9 – Analytics Engines.

Analytics Engine
: The ID of the analytics engine to which streams from cameras in this group should be sent.

Stream
: The Stream ID to send to the analytics engine.

Advanced

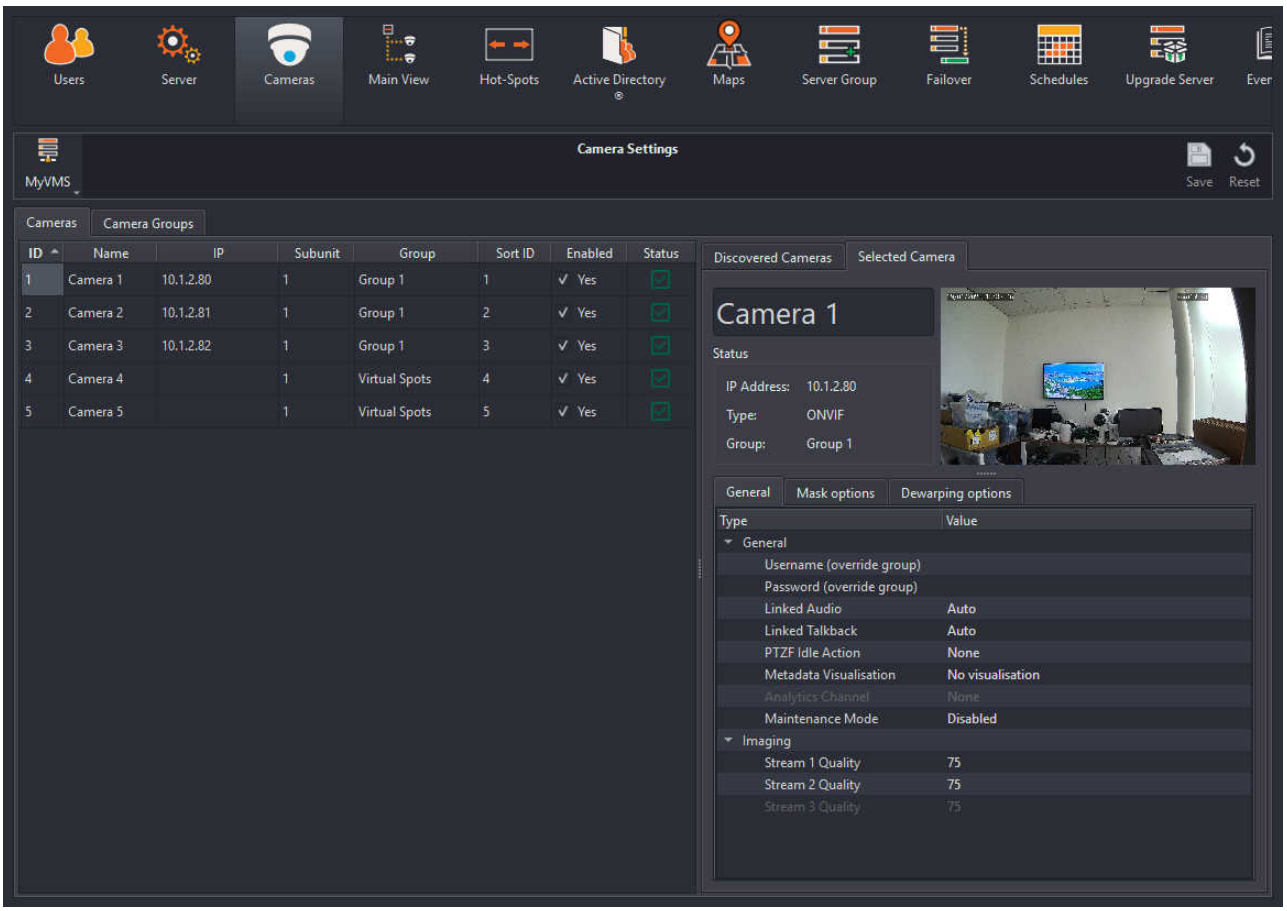
This section is only present if the contained options are relevant to the current camera group type.

EMS Licensing
: Treat cameras in this group as Encoder/Multi-Sensor devices. Normally such devices are auto-detected so this setting wouldn't be necessary, but if the device is not correctly detected as an Encoder or Multi-Sensor devices, this option forces it to be detected as such. When enabled, the Wavestore server will prefer using an EMS channel licence and allow up to 4 lenses per licence to be added.

Gateway Proxy
: Enables camera Gateway Proxy feature for cameras in this group. When enabled, the Wavestore acts as a gateway (or HTTP reverse proxy) to allow access to the camera; the camera web page can be accessed via the Wavestore IP address and port 1000+n (http) or 2000+n (https) where n

is the camera number. It can also be accessed by right-clicking the camera in the table within the "Cameras" tab of the Cameras setup screen and selecting "Camera Setup Web Page".

6.3.3 Individual Camera Settings



The camera table in the left pane has multiple columns which are detailed below:

ID (Non-editable) This shows the Channel ID of the camera on this row.

Name (Editable) This is the name of the camera.

IP (Editable) This is the IP address or hostname of the camera.

Subunit (Editable) This field should normally be left as 1, but can be changed to select a lens for a multi-lens camera, or a channel within a multi-channel encoder.

Group This is the Camera Group to which this camera is assigned.

Sort ID This ID is used to provide custom sorting within the UI, e.g. in the Device Tree on the main screen.

Enabled This determines whether the camera is enabled or disabled.

Status This shows the status of the camera. See section 15 – Appendix E – Camera Statuses for details of available statuses.

When a camera is selected in the left pane of the Cameras setup screen, the camera-specific settings (as opposed to camera group settings) become visible in the right-hand pane.

The camera name can be changed by selecting it in the right-hand pane.

There are 3 tabs available:

General
: Commonly used per-camera options.

Mask options
: For configuration of Motion Detection Masks, Privacy Masks, and sensitivities for Motion Detection, Darkening Detection, and Camera Movement detection.

Dewarping options
: For configuring dewarping settings for fisheye and panoramic cameras.

These sections are described in detail in the following sections...

General

- *General*

  Username (override group)
  : A username to use for authentication with the device. Overrides the username configured for the camera group. Note that, when making this setting, the Password setting below also needs to be provided.

  Password (override group)
  : A password to use for authentication with the device. Overrides the password configured for the camera group. Note that, when making this setting, the Username setting above also needs to be provided.

  Linked Audio
  : Allows selection of a separate audio channel to be associated with this video channel. If set to Auto then the same channel will be used for video and audio if Audio is set to "yes" for the camera group.

  Linked Talkback
  : Allows selection of a separate talkback channel (also known as "backchannel") to be associated with this video channel. If set to Auto then the same channel will be used for video and talkback if Talkback is set to "yes" for the camera group.

  PTZF Address
  : Sets the PTZ Address for this camera. Generally only ever needed when using analogue PTZ.

  PTZF Idle Action
  : Allows configuration of an action for a PTZ camera to take when nobody has controlled the camera for a period of time. Possibly actions are "Go To Preset" and "Start Tour". For example, "Go To Preset 4 After 90 Seconds".

  Metadata Visualisation
  : Allows selecting a "metadata visualisation" to be associated with this camera. Default visualisations are provided as well as any which have been configured in the Metadata Display

setup screen. Metadata Visualisations are usually used in conjuction with Integration Modules, such as a Point of Sale module. In this case, configuration instructions for the Metadata Visualisation are provided with the Integration Module.

Analytics Channel

Only available for cameras in a group with an Analytics Engine assigned. Allows selecting a channel ID on the Analytics Engine to which this camera will be mapped.

Maintenance Mode

Puts this camera into "Maintenance Mode" until the specified date. Whilst in this mode, the camera will not report faults as F faults in the system log, nor will it set FAULT on the status indicator or remote monitor. Useful if a camera is known to be problematic but an immediate fix isn't possible, to prevent leaving the whole system in Fault state.

- *Imaging*

Stream 1 Quality

Allows configuration of the image quality for stream 1. Higher values mean reduced video compression and higher image quality, but also higher data rates. Higher data rates equate to more network bandwidth usage (when using IP cameras) and also more disk space used. Often the image quality can be reduced to quite a low level before any visible artifacts become apparent so it is recommended to avoid the temptation of setting this value unnecessarily high.

Stream 2 Quality

Allows configuration of the image quality for stream 2, if enabled.

Saturation / Brightness / Contrast / Sharpness / Hue / Noise reduction / Deinterlace / Median filter

Adjusts various properties of the image.

Only available for cameras that belong to a "Stretch" group type.

Mask options

The Mask Options panel is only available for video channels. It serves several purposes:

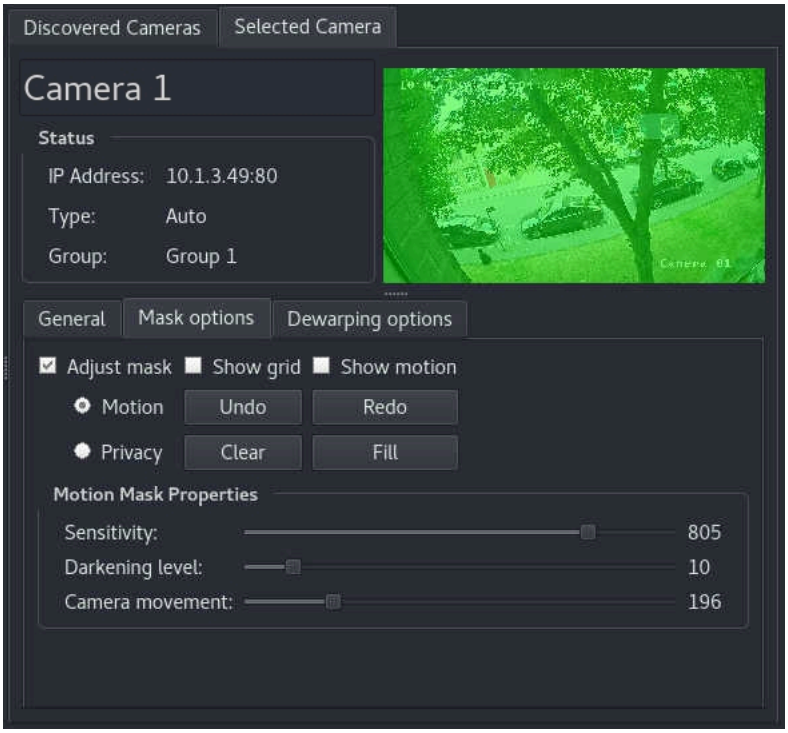
- Configuration of Motion Detection Masks
- Configuration of Privacy Masks
- Configuration of sensitivity for Motion Detection, Darkening Detection, and Camera Movement detection

Note that Privacy Masks are available for all video channels. Motion Masks will only have an effect for:

- Analogue video channels
- IP video channels with "Smart Search / VMD" enabled

Camera Movement detection (server–side) is supported for analogue video channels and IP video channels when "Smart Search / VMD" is enabled.

Darkening detection is supported for analogue cameras and for ONVIF IP cameras that have the ability to detect a darkening event and provide this via the ONVIF PullPoint mechanism.



Privacy Masks allow an area of the image to be blocked, often used for privacy reasons. The ability to ignore privacy masks is configurable on a per-user basis in the Users Setup Screen.

The Motion Mask is used to determine if the motion triggers a Motion event (see below for more detail). There are also Sensitivity settings for motion detection, darkening detection, and camera movement detection. The higher the sensitivity the more likely that each of those events will be detected, but if the sensitivity is too high then false alarms may occur.

The various settings and buttons are described in detail below:

Adjust Mask	The mask is only shown when this checkbox is enabled. Note that if the mask has not yet been configured, i.e. it is an empty mask, nothing will appear on the video image. When this setting is enabled, the mask can be drawn onto the video image by left-clicking with the mouse. Motion Masks are shown in green, Privacy Masks are shown as a dark area on the image.
Motion / Privacy	This radio button determines whether a Motion or Privacy mask is being configured. These options are only available if Adjust Mask is enabled.
Show grid	If enabled, a grid will be shown to assist with drawing the mask.
Show motion	If enabled, areas where motion is detected will be highlighted in blue on the image. This can be used to help adjust the sensitivity to the appropriate level. See notes below on motion outside the mask area.
Undo	Reverts the last mask editing operation
Redo	Re-applies a previously undone mask editing operation
Clear	Clears the entire mask
Fill	Fills the entire mask

Sensitivity	Sets the sensitity for motion detection.
Darkening level	Sets the sensitivity for "darkening" detection. "Darkening" is when the camera is obscured in some way. The Wavestore server can detect this and trigger an event.
Camera movement	Sets the sensitivity for "camera movement" detection. This is to detect when the camera has been moved to face in another direction. The Wavestore server can detect this and trigger an event.

Note that the system will detect motion over the entire image. The server saves this detected motion (if the track is enabled) for later use, for example by Smart Search.

The Motion Mask is used to determine if this motion triggers a Motion event, which might perform an action like starting recording or alerting a user to an intruder. The Motion Mask is used as the video arrives from the camera to decide if the Motion event is triggered. The mask does not affect the motion detected, and in particular it does not affect the motion stored for later processing, for example by Smart Search, where you choose a mask at the time of search.

So when you view motion on the setup screen, you will see motion detected both inside and outside the mask area. This is normal, as the motion is being shown where it is detected.

Dewarping options

The Wavestore server is compatible with a wide range of hemispheric (360°) and wide angle cameras. These cameras stream raw 'warped' images of the area surrounding the camera. The true proportions of the objects being viewed may be altered on these raw images, and straight lines of objects viewed by the cameras may appear to be curved.

The warped images are recorded by the Wavestore server, but can then be 'dewarped' by a WaveView client (either on the server box or a PC, for Live View or Playback), so that the viewed objects appear with their true proportions and straightened line edges. This mode of operation is known as 'Post Recording Dewarping', and any 360° cameras used with the Wavestore server must be configured for this mode of operation, rather than 'Pre Recording Dewarping' mode (also supported by some cameras), where the image 'dewarping' is carried out on the camera itself, before the images are streamed to the server.

Individual dewarped views can be configured and saved on the WaveView client software. The field of view and level of digital zoom for these views can be freely configured by the user, effectively creating one or more 'virtual' cameras. These views can be created to monitor Live footage, or playback raw 'warped' footage that has been previously recorded. In this way, a single 360° camera can be used to replace multiple standard cameras.

Initial setup of Hemispheric/Wide Angle camera is performed in the same way as for a standard IP camera. Note that if a camera has just been added, it is necessary to save the camera configuration before dewarping can be enabled, since the software needs to be receiving video in order to properly configure the dewarping parameters.

Some additional configuration is necessary as follows:

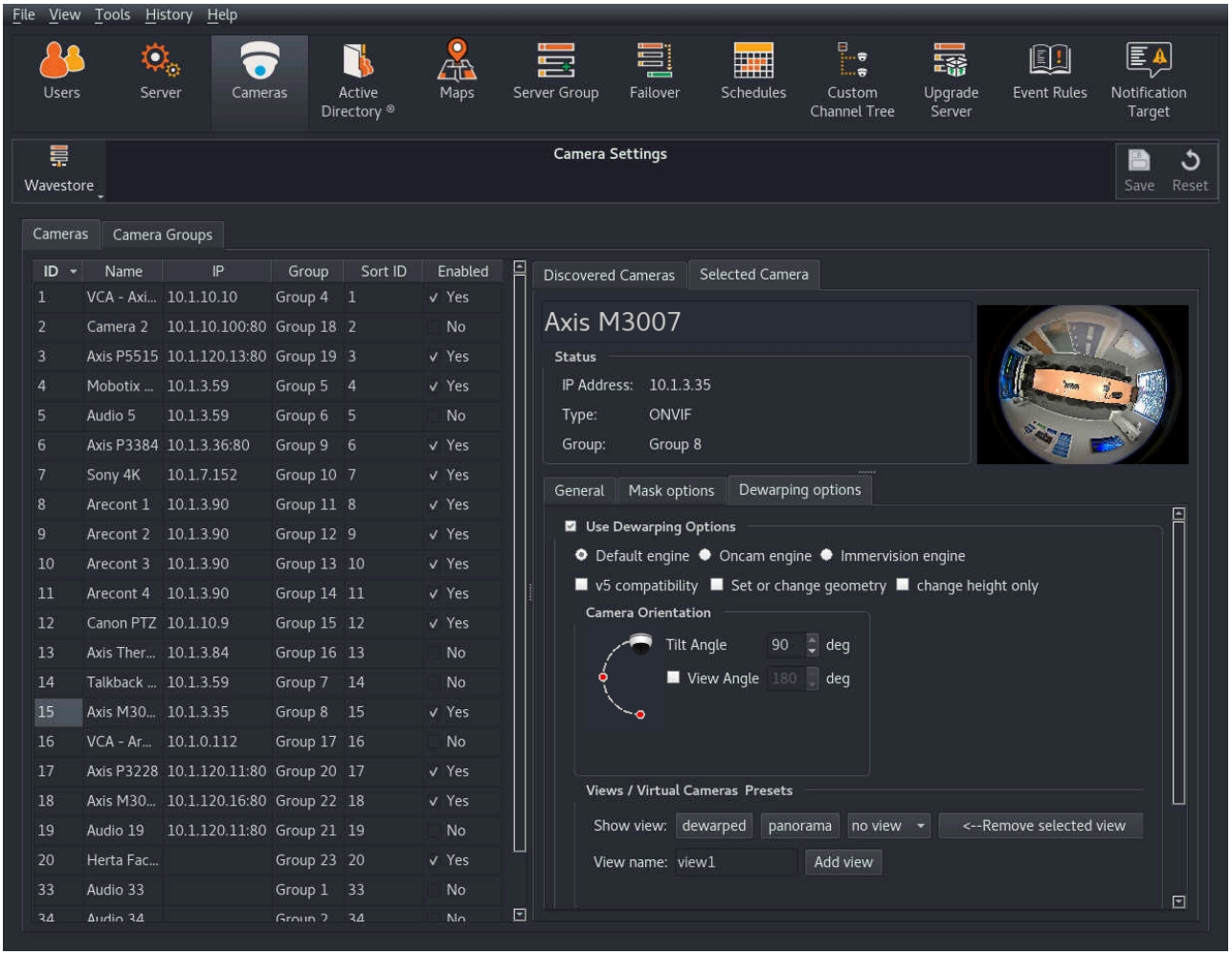


Figure 6.32: 360° camera configuration screen

In the Dewarping Settings submenu, check the 'Use Dewarping Options'.

Next, choose the appropriate dewarping engine:

Default engine

This is the Wavestore engine for dewarping and is suitable for most fisheye camera types.

Oncam engine

This engine is for use with cameras manufactured by Oncam and offers the Oncam experience within the Wavestore software.

Immersion engine

This engine is for cameras which use Immersion Panamorph lenses, which should be specified in the camera's documentation, and offers the Immersion experience within the Wavestore software.

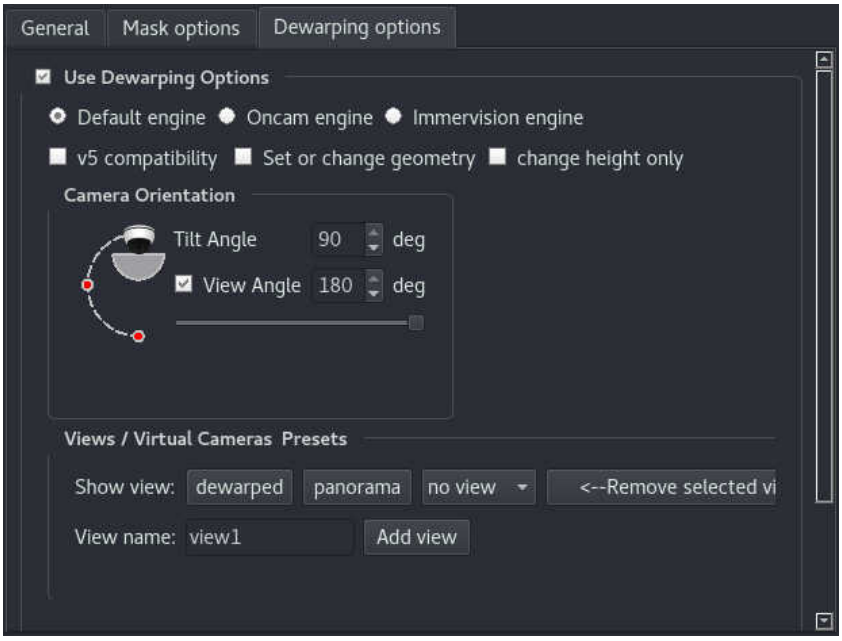
Depending on the engine chosen, different options will be presented.

Default Engine

To set up the camera for the Default Engine click the 'Set or Change Geometry' boxes. A red circular graphic will now appear on the raw warped camera image as shown below:

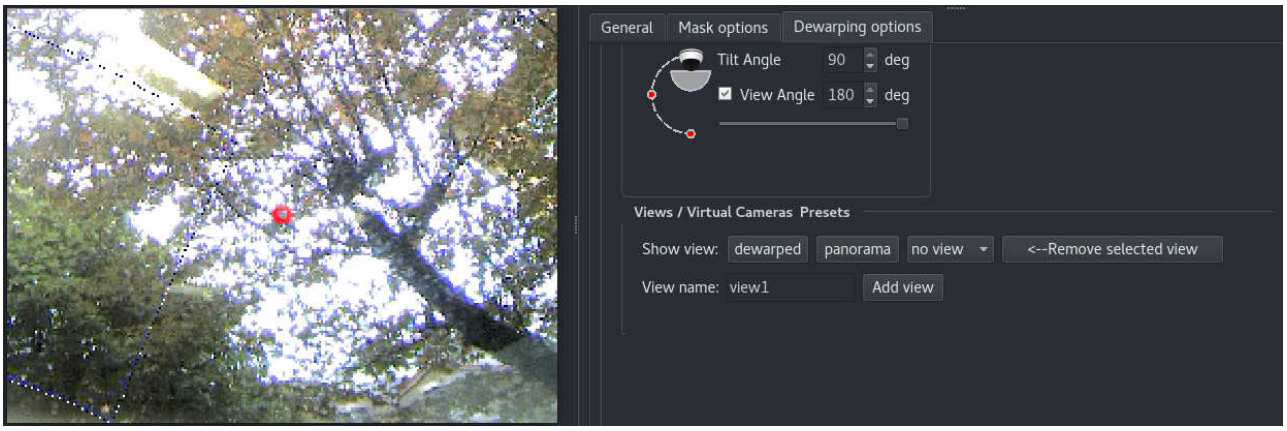
Use the mouse controls (click and drag/roll mouse wheel) to change the size and position of the circle until it neatly surrounds the non-black area of the camera image. This setting ensures that the appropriate lens correction is applied to the image and also restricts the viewing area when dewarping.

The next step is to select the orientation of the camera according to the position of the camera mount. Wavestore allows any orientation, although the most common are Ceiling (90°), Wall (0°), and Table (-90°).



The *View Angle* can also be changed if it is known to be something other that the default 180°. Simply check the "View Angle" box and set the value.

It is also possible to create saved "Dewarp Views". To do so, click either "Dewarped" or "Panorama", depending on the type of view desired. This will open a new window showing the video in dewarp or panorama mode. Use the mouse controls in the video window to pan/tilt/zoom to the desired position...



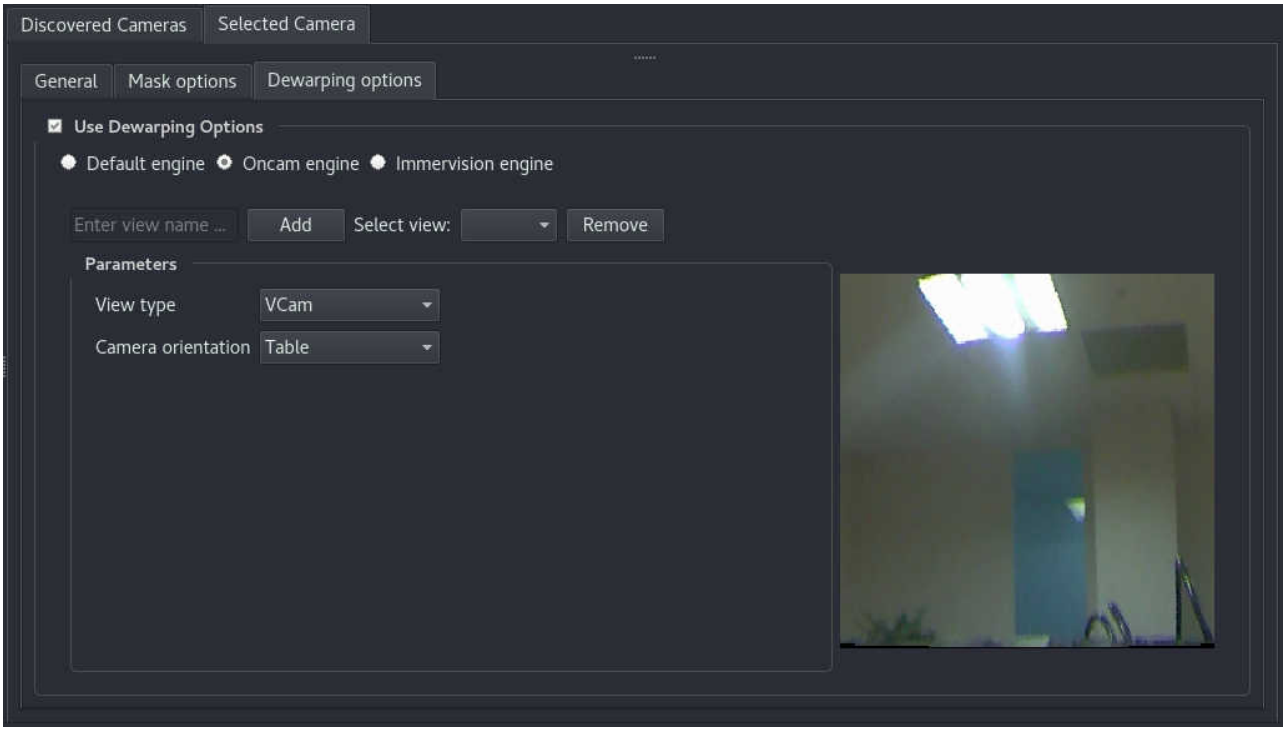
To save the View, enter a name in the "View name" box and click "Add view". To remove a saved view, click the third drop-down box, select the view, then click "Remove Selected View".

Note that only a few views can be saved. Normally this is around 4 per camera but the precise number depends on the length of view name, so short names should be preferred.

Oncam Engine

Configuring a camera to use the Oncam Engine is quite simple. Just choose a desired dewarping "View type" and select an orientation of either Ceiling, Wall or Table, then save the changes.

The camera display should should now show the dewarped view. The view can be controlled by clicking and dragging with the mouse and using the mouse-wheel to zoom.



To save a dewarped view, move the image to the desired orientation, enter the name in the "Enter view name..." box, then click Add.

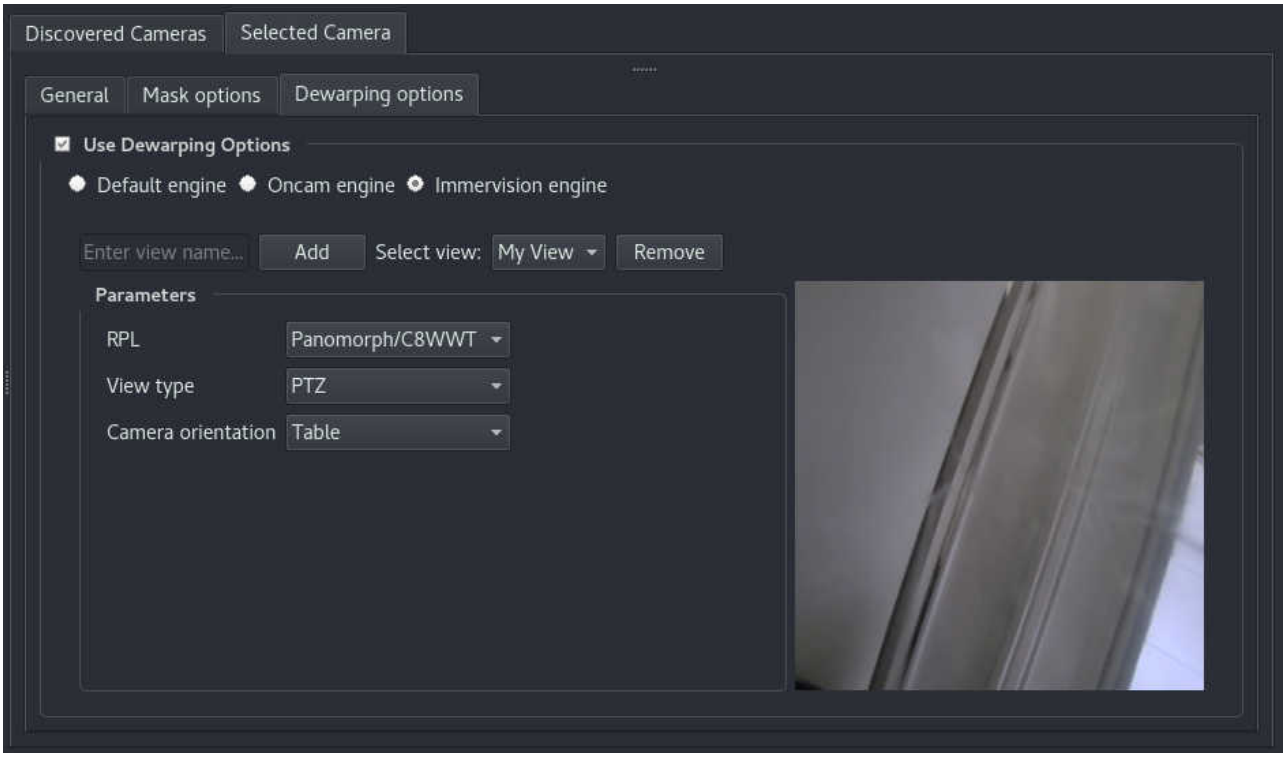
To remove a view, select it from the "Select view" drop-down menu, then click "Remove".

Immervision Engine

To configure a camera to use the Immervision Engine, it is necessary to determine the lens type. This information should be available from the camera manufacturer.

Choose the lens type from the "RPL" drop-down menu, then select an orientation of either Ceiling, Wall or Table, then save the changes.

The camera display should should now show the dewarped view. The view can be controlled by clicking and dragging with the mouse and using the mouse-wheel to zoom.



To save a dewarped view, move the image to the desired orientation, enter the name in the "Enter view name..." box, then click Add.

To remove a view, select it from the "Select view" drop-down menu, then click "Remove".

6.3.4 Importing Camera Settings

Certain camera settings can be imported from a spreadsheet to make adding large numbers of cameras convenient.

The spreadsheet should be in CSV (Comma-Separated Values) format. Most popular spreadsheet software can export in this format.

To perform the import, right-click on the Camera Table and select "Import from CSV...". Then choose your CSV file and click Open.

The import mechanism can import:

ID The channel ID

Name The channel name

IP The IP address or hostname for the channel

Subunit The Subunit for the channel (often used to select a lens for a multi-lens camera, or a channel within a multi-channel encoder)

Sort ID The Sort ID for the channel, used to display cameras in an abritrary order on the main screen.

Group The name of the Camera Group to assign

Only the ID field is mandatory.

The first row of the CSV file should be the headings. The headings are case-insensitive and multiple alternatives are permitted. Here are the permitted alternative headings:

ID "id", "no", "no.", "camera", "channel", "camera id", "channel id", "camera no.", "channel no."

Name "name", "camera name", "channel name"

IP "ip", "ip address", "host", "host name", "hostname"

Subunit "subunit", "sub unit", "sub-unit", "lens"

Sort ID "sort id", "sortid"

Group "group", "camera group", "channel group"

Here are some important notes about the behaviour of the import process:

- If no ID column is present in the CSV file, the import will be rejected.
- If there are duplicate IDs, the first one will be accepted. The rest will be rejected and an error shown detailing the duplicate IDs.
- If there are any invalid IDs, e.g. text instead of numbers, these will be rejected and an error shown detailing the rows within the CSV file which had these invalid IDs.
- If there are too many entries, the importer will add as many as possible and show an error detailing the ID of the first entry that was rejected. Subsequent entries will also have been rejected.
- If a channel with the given ID already exists, it will be overwritten with the imported settings, otherwise a new channel will be created.
- If no Name is provided, a default name is used, unless the channel already exists, in which case the Name is not changed.
- If no IP is provided, it is left blank, unless the channel already exists, in which case the IP is not changed.
- If no Subunit is provided, or the provided value is invalid, the default Subunit of `1` is used, unless the channel already exists, in which case the Subunit is not changed.
- If no Sort ID is provided, or it is invalid, the Sort ID is set to the same as the Channel ID, unless the channel already exists, in which case the Sort ID is not changed.
- If the Group Name is not found, or is missing, a default existing group is assigned, unless the channel already exists, in which case the Group Name is not changed.

Here is a brief example CSV file:

```
ID,Name,IP,Subunit,Group,Sort ID
1,Camera 1, 192.168.0.1,1,Group 1,1
2,Camera 2, 192.168.0.2,2,Group 1,2
3,Camera 3, 192.168.0.3,1,Group 2,3
4,Camera 4, 192.168.0.4,2,Group 2,4
```

If the import procedure completes and the results are unexpected, click Reset to return to the previous settings, and check the CSV file is correct.

6.4 Main View

The 'Main View' setup screen contains a list of selectable sub-sections to configure various aspects of behaviour relating to the Main View screen.

These are detailed in the following sections.

6.4.1 Channel Groups

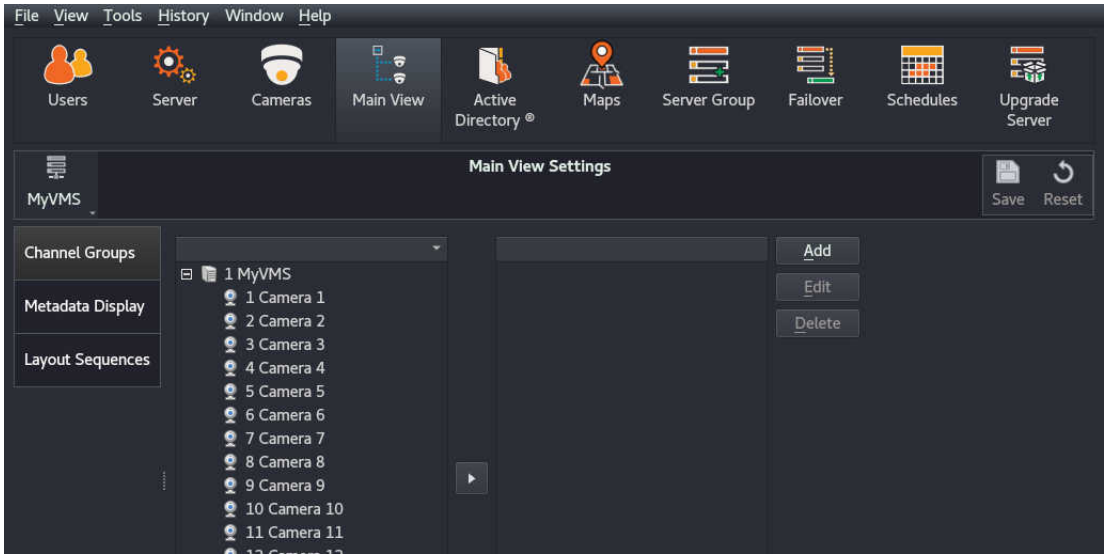
Note: The settings in this page apply to all servers in the server group.

The Custom Channel Tree allows a user to group frequently used cameras together, so that they can be quickly accessed.

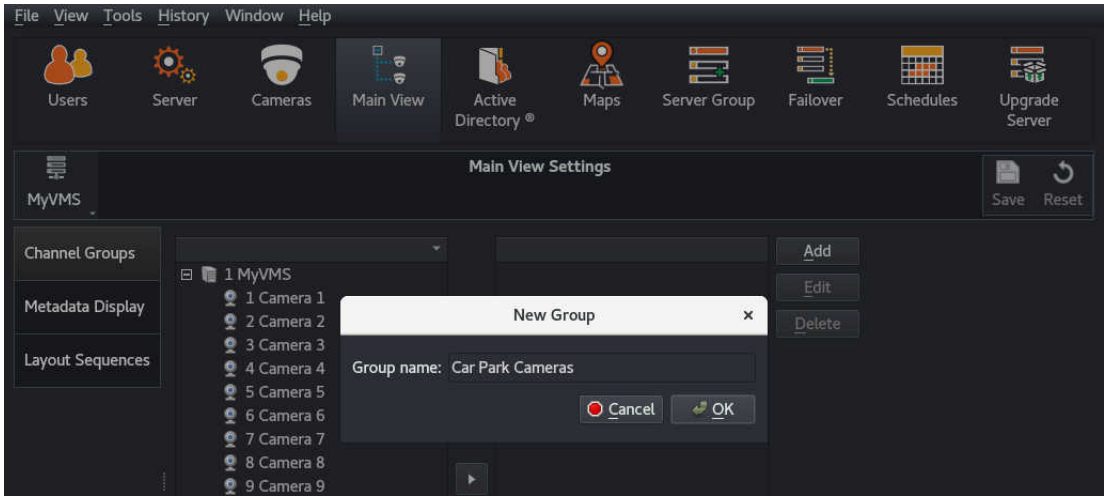
Right-clicking on the Device tree allows the user to switch between the Channel Tree View (all cameras listed) and Group Tree view (only cameras that are part of a group are listed).

We can create a camera group as follows:

- Follow menu path *View* → *Setup* → *Main View* → *Custom Channel Tree*



- Either right-click on the right-hand pane and choose 'Add Group', or click on the 'Add' button.
- Enter a name for the new camera group that you are creating, then click 'OK'.

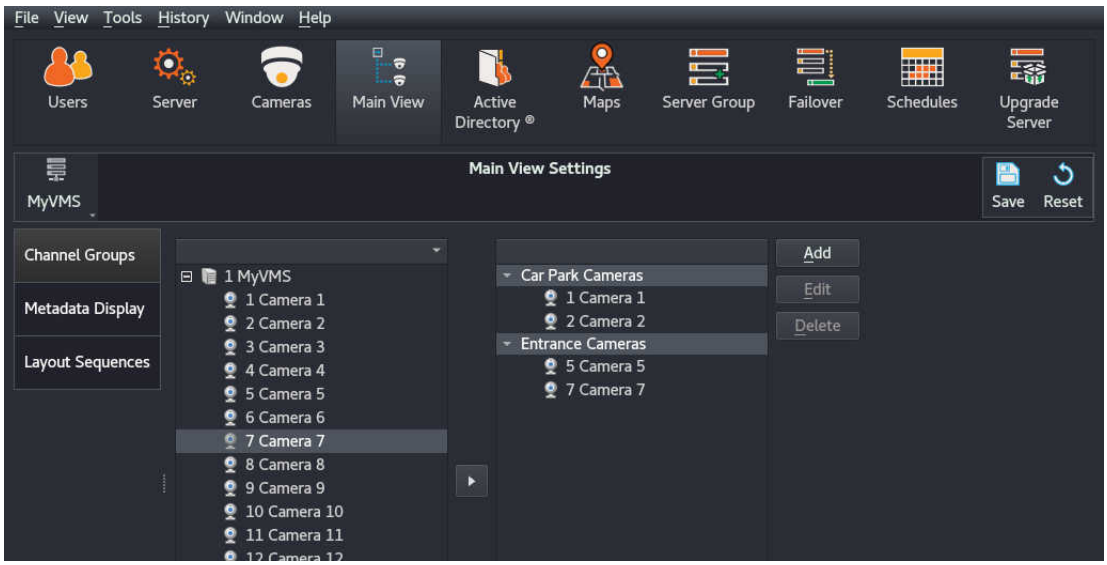


There are now two ways to add a camera to a group...

- Click on the name of the camera group in the right panel, so that it is highlighted, then click on the camera in the left panel that you wish to add to the group.
- Then click on the ***Right Arrow*** button between the two panels.

...or...

- Drag one or more camera names from the left panel onto the name of the group in the right panel. To select multiple cameras, hold CTRL and left-click to select individual cameras, or Shift to select a range.



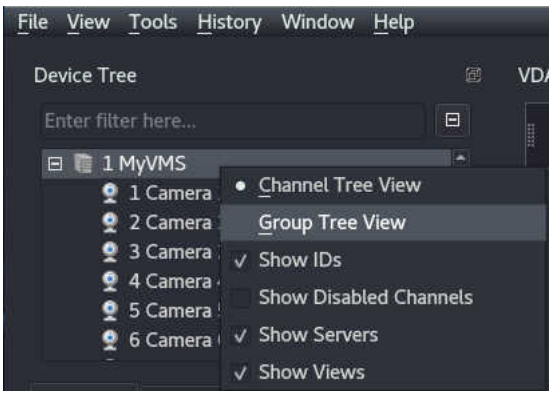
- Repeat for any other cameras/groups as required:
- Click on 'Save' to store your changes on the server.

The cameras in the Camera Group panel on the right can be dragged and dropped into new positions as desired. Above each of the two panels, there is a button to collapse all or expand all groups.

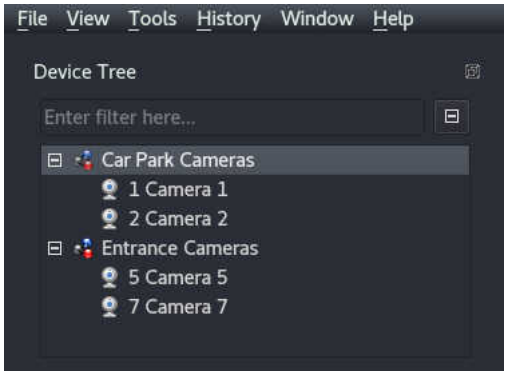
Some considerations to note:

- When an "admin"–level user is configuring Camera Groups, they may have not have permission to access all cameras. Non–permitted cameras are not shown in the existing Camera Groups but those groups can still be edited.
- Any camera within a Camera Group which exists on a server which is no longer in the server group will not be shown in the setup screen or in the main screen, but may still exist in the Camera Group configuration until that group is deleted.

Once saved, the custom groups can be accessed by any client. To display the Camera Groups in the Main screen, right click on the Device Tree:



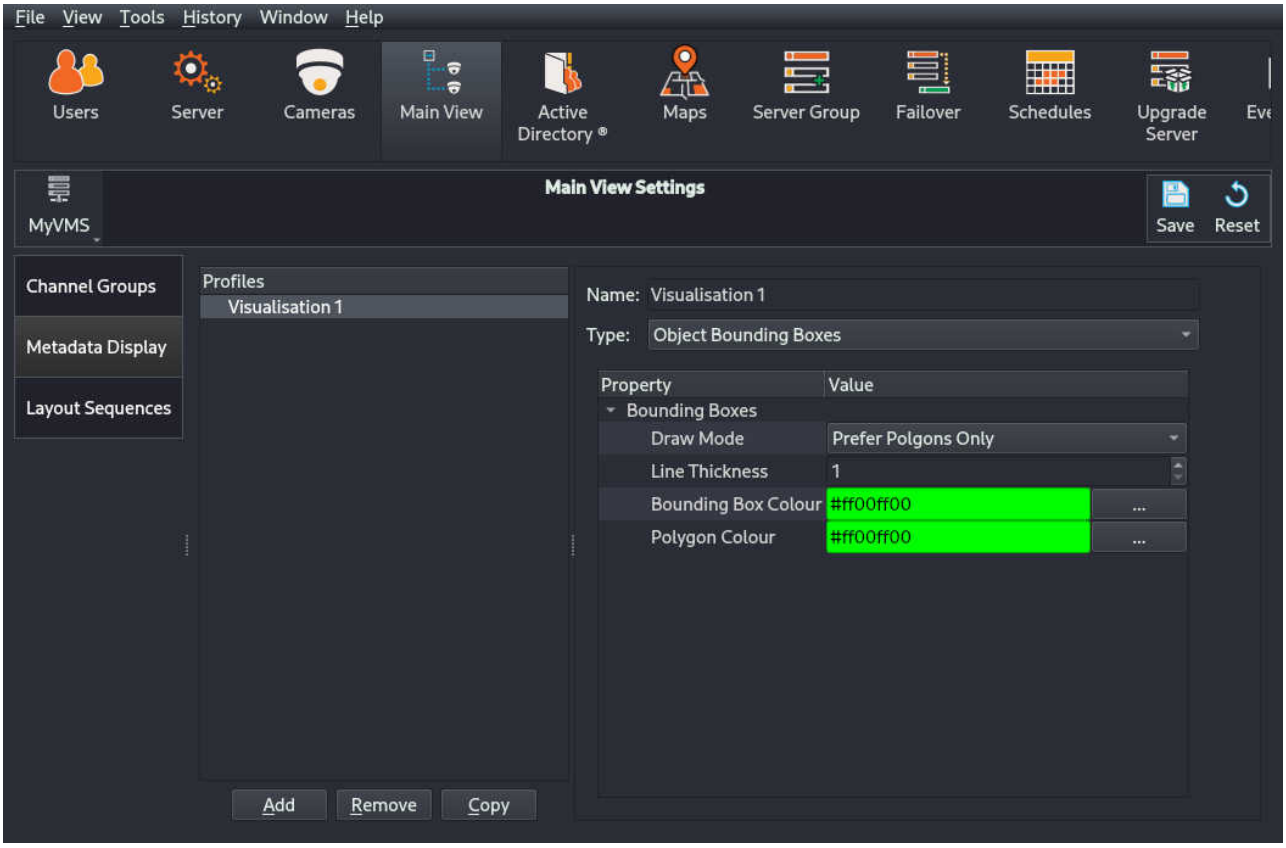
- Select the Group Tree View option:



The Device Tree preference (Channel Tree View or Group Tree View) will be remembered when Wave–View is exited and restarted. It is possible to double–click on the Group name to open all the cameras in the group in a suitably sized layout.

6.4.2 Metadata Display

This screen allows the customisation of metadata visualisations, such as video analytics bounding boxes. Visualisations are assigned to cameras in the Camera Setup screen – see section 6.3.3 – Individual Camera Settings. Normally it's sufficient to use the default settings for any given visualisation, however this screen allows a copy of the default to be created, named, and configured. Once saved, it can then be assigned to a camera.

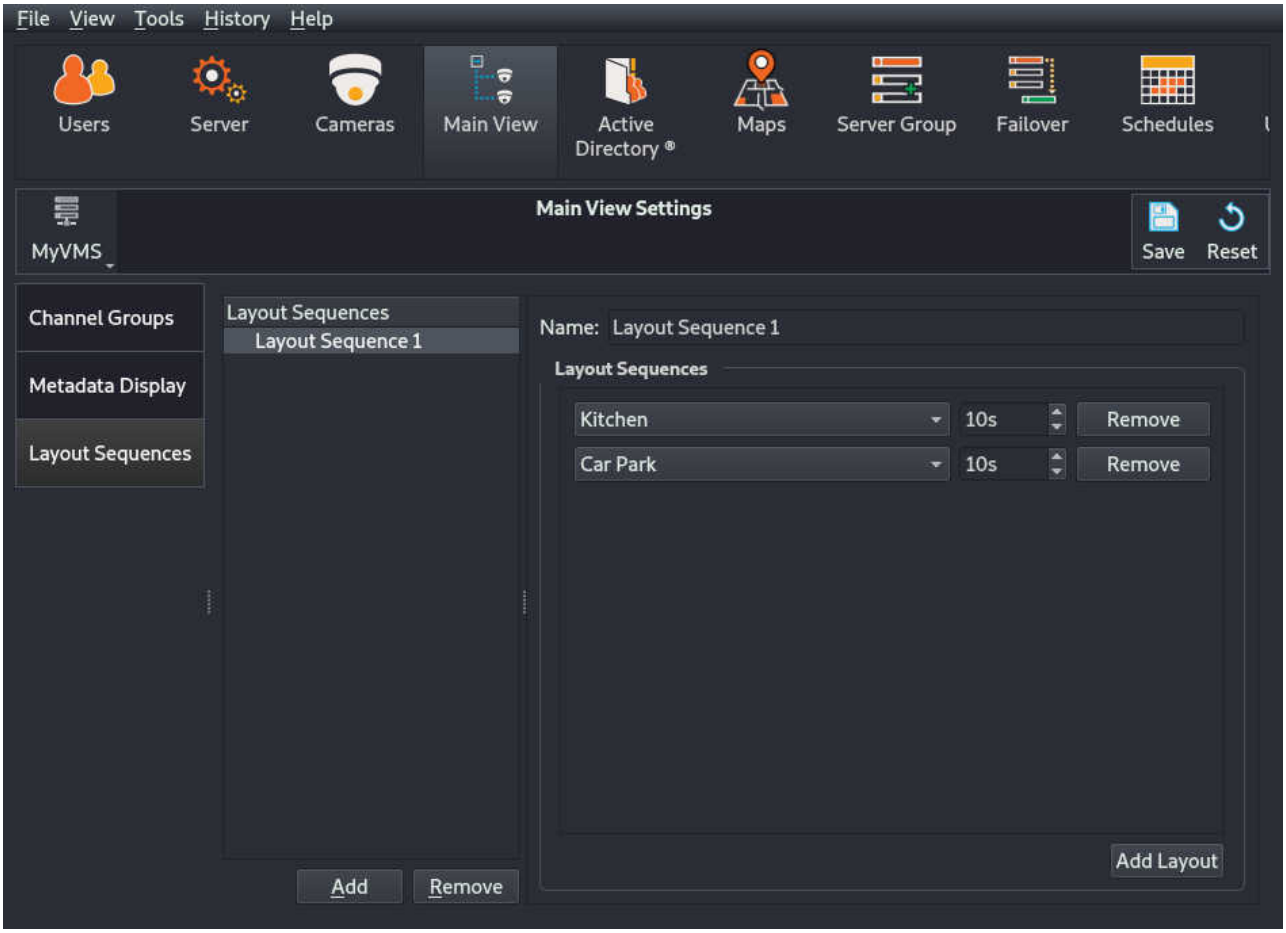


To create a new visualisation, click Add, then choose the Type and give it a name. By default, the newly created visualisation will have the default settings which should be reasonable, so the settings can be tweaked from that point as desired.

Once complete, click Save to store the visualisation settings to the server. Note that, if returning to the main screen to check how the settings look, it is necessary to reopen the camera to obtain the new settings.

6.4.3 Layout Sequences

Layout Sequences allow layouts to be automatically loaded consecutively with configurable durations for each one. They are configured in this screen. See section 3.7.2 – Triggering Layout Sequences for details about their use.



Layout Sequences can only be created from Shared Layouts, which any user can create from the Main Screen.

The Add button can be used to create a new Layout Sequence. By default it will be empty, but layouts can then be added to the sequence with the 'Add Layout' button.

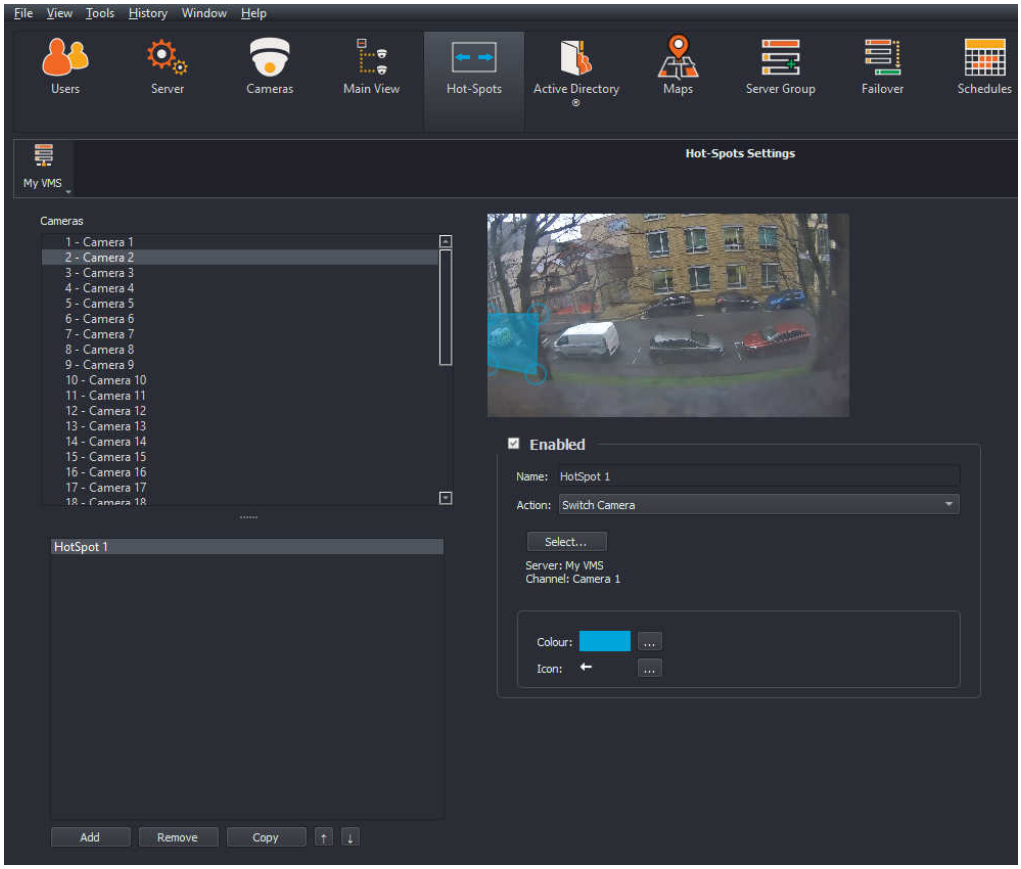
For each step in the sequence, a Layout can be selected and a duration, in seconds, specified.

Once complete, click Save to store it to the server. It will then be available for use in the Main Screen.

6.5 Hot-Spots

The Hot-Spots setup screen allows configuring regions to be overlaid on cameras which allow clicking to switch to other cameras or trigger *Event Causes*. For example, if several cameras cover a long corridor, a Hot-Spot might be configured on each camera at each side of the image to allow moving to the cameras further along the corridor in each direction. Or a Hot-Spot might be configured to trigger an event which locks and unlocks the door.

Hot-Spots are unique to each camera. Each Hot-Spot can have a configurable region, colour, icon, and action to perform when clicked.



To add a Hot-Spot, first select a camera, then click 'Add'. A new Hot-Spot will be added with a default name, region, and colour.

It is recommended to set a suitable name for the Hot-Spot as this will be shown as a tooltip when users hover their mouse over the Hot-Spot. Therefore, the name should ideally describe the action that will occur when the Hot-Spot is activated.

It is necessary to choose at least one action to perform when the Hot-Spot is clicked. The actions are *Switch Camera* and *Trigger Event Cause*, and are detailed later in this section.

It is possible to add more actions by clicking the green **+** button at the bottom of the existing actions. Actions can be removed with the red **–** button.

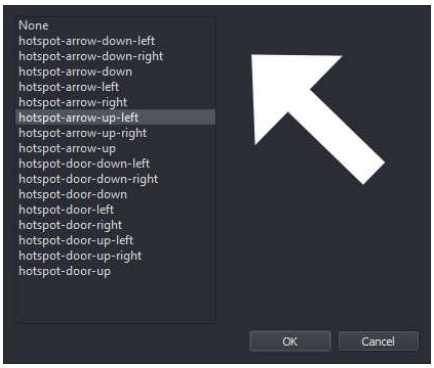
In the main screen, when viewing a camera, if the Hot-Spot has more than one action available, the desired action can be selected from a menu by right-clicking the Hot-Spot.

Once the actions are configured, it is likely to be desirable to configure the region where the Hot–Spot will be shown on the camera. The region can be edited as follows:

- Click and drag a circular end–point of the line to move that point
- Double–click on an edge of the region to add another point
- Double–click a circular end–point to remove it
- Click within the region and drag to move the whole region

The colour of the Hot–Spot region can be configured by clicking the "..." button next to the 'Colour' indicator.

An optional icon can be selected by clicking the "..." button next to the 'Icon' indicator. This will open a new dialog with a choice of icons to use. Choose 'None' if an icon is not required – although this is the default.



Note that the selected icon is not shown in the Hot–Spot region on this screen, but will be shown when the camera is viewed in the Main Screen or Find Screen. The icon is scaled automatically to a reasonable size.

At this stage, clicking 'Save' will make the Hot–Spot available.

For a given camera, it is possible to 'Add' more Hot–Spots, 'Copy' existing Hot–Spots, and then edit them, and to 'Remove' Hot–Spots. It is also possible to use the up and down arrows to change the order of the Hot–Spots. This has no effect on the behaviour in the rest of the software and is only present to help make configuration easier if configuring many Hot–Spots.

Each Hot–Spot can also be disabled by unchecking the 'Enabled' box. This allows a Hot–Spot to be disabled without having to delete it, which it might be useful if the target camera is temporarily offline.

6.5.1 Switch Camera action

For the *Switch Camera* action, it is simply necessary to select the target camera by clicking the *Select...* button and choosing the camera from the Camera Tree. Only one camera can be selected.

6.5.2 Trigger Event Cause action

The *Trigger Event Cause* allows the Hot–Spot to be configured such that it can be used to trigger a newly created *Event Cause*. This*Event Cause* can then be used to create an Event Rule, which allows one or more *Event Actions* to be triggered.

The *Trigger Event Cause* Hot–Spot action has several parameters which need to be configured. They are as follows:

Event Cause Name The name of the new *Event Cause* to be created. Details about valid cause names are provided below.

Device ID The main parameter for the *Event Cause*. Its meaning varies depending on the *Event Action* used within any *Event Rule* later configured. For example, it could be a camera number if the *Event Action* is to be "record" or "boost recording rate", door control panel number for "Door Unlock", etc.

Sub Device ID A sub parameter for the Event Cause. For example it might mean the "recording track" when configuring an *Event Rule* to record a camera.

Type Configures whether the new *Event Cause* should be of "Pulse" type, meaning it is an instaneous event, or "On/Off", meaning it has a start and an end.

Label Configures the text to show on the Hot–Spot in the main screen. For example if the new *Event Cause* has type "On/Off", you might want the text to show "Start/Stop", "Open/Close" or something else.

The following characters are allowed in Event Cause names:

- 0–9
- A–Z
- a–z
- /
- _
- Space (" ")
- Any unicode character greater than 0x80 except unicode characters 0x2423 and 0x2080 to 0x2089.

Therefore any Unicode (or ASCII) character under 0x80 which is not in the permitted list above, is not permitted. This includes certain punctuation characters such as these: !"#$%&'()*+,–{|}

6.6 Active Directory ®

Note: The settings in this page apply to all servers in the server group.

Wavestore supports Active Directory via LDAP for authenticating users, meaning that it's not necessary to create and manage users separately on the Wavestore. Users can be configured within the AD server to be a member of a Wavestore group. The Wavestore will then use the permissions for the group when that user logs in. The permissions themselves are configured on the Wavestore and there can be many groups. For example, a typical setup might be as follows:

- In the Active Directory there are 2 users, "Andy" and "Brenda".
- The Administrator creates 2 groups in Active Directory. One called "DVRUsers" and one called "DVRAdmins". (Note that the group names must start with "DVR").
- Still within AD, the Administrator makes "Andy" a member of "DVRUsers", and "Brenda" a member of "DVRAdmins".
- Now moving to the Wavestore side, the Administrator creates two new users in the Wavestore Users Setup screen (Setup → Users), one called "DVRUsers" and one called "DVRAdmins", each configured with appropriate permissions.
- The Administrator then configures the Wavestore to use the Active Directory server by setting its hostname or IP address, domain, and any other required information.
- Now, when Andy logs in, he can use his normal domain username and password and it will be checked against the AD server. If successful, Andy is logged in with the permissions of the DVRUsers group.
- If Brenda logs in, she inherits the permissions of the DVRAdmins group.
- When new employees join, the Administrator simply needs to create them in Active Directory and add them to the desired "DVR" group.

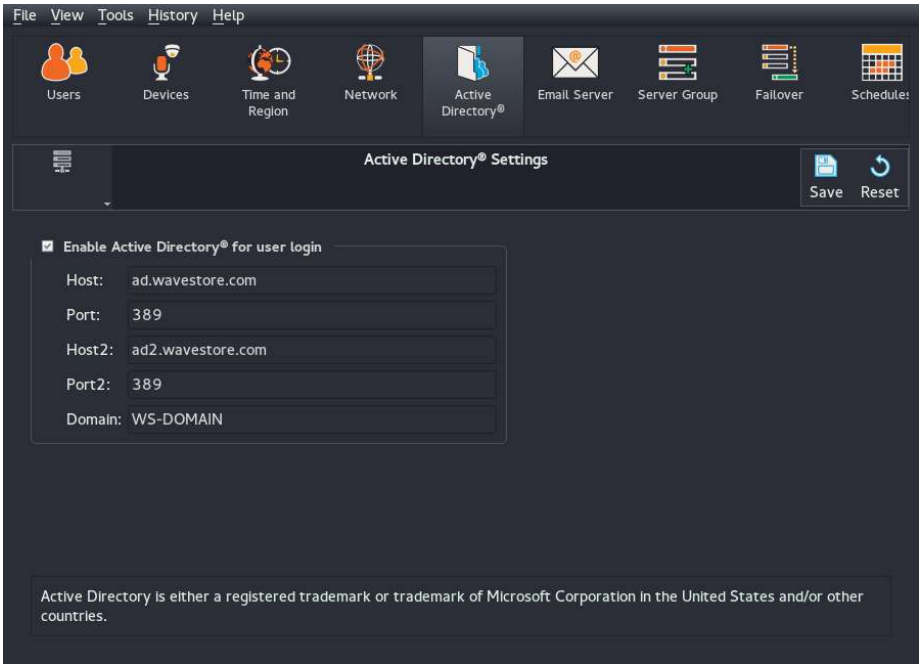


Figure 6.33: Active Directory Setup Screen

The available parameters are as follows:

Enable Active Directory for user login	This enables and disables the AD functionality.
Host	This is the IP address or hostname of the Active Directory server.
Port (optional)	This is the port number for LDAP communication, the default is provided as 389 (TCP).
Host2 (optional)	This is the IP address or hostname of a secondary AD server which will be used if the primary AD server cannot be contacted.
Port2 (optional)	The port number for the secondary AD server.
Domain	This is the Windows domain in which the AD server and users reside.

6.7 Maps

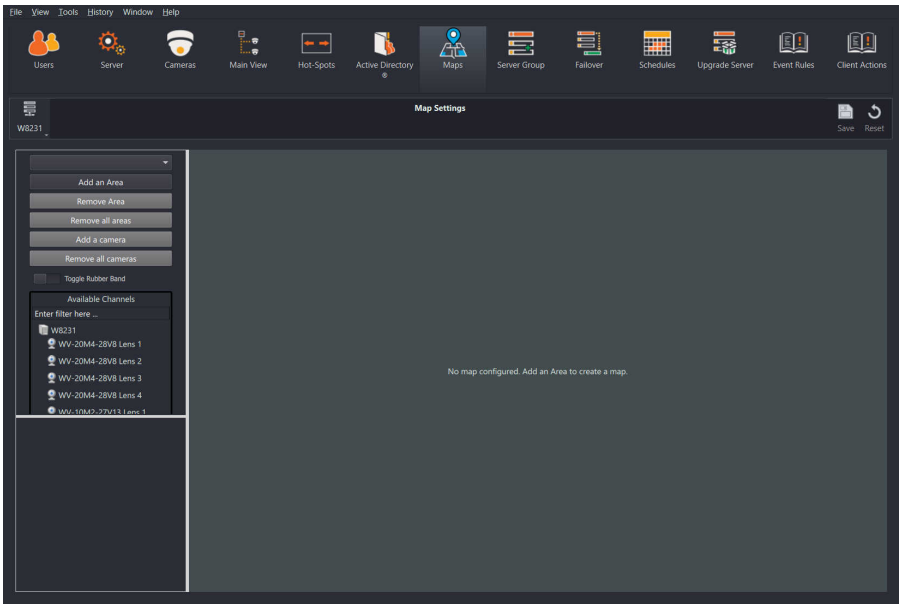
WaveView provides map functionality to allow cameras and alarm devices to be visualised on one or more interlinked images. The Maps are available to users on the main screen, and this section describes how to configure them.

The map system is designed around the concept of "Areas". Cameras, Event Items, and other devices are all added onto "Areas". A background graphic can be loaded onto an area which might be a floor plan or perhaps a photo of the front of a building.

Of course, the Areas don't have to represent physical things. They could just be used to create custom views of different cameras.

The area size is defined either by the loaded background graphic or, if none loaded, by the position of the cameras dragged onto it. The Cameras and Event Items can be scaled on a per–area basis so that they appear a sensible size.

Map Setup Controls



The rest of the controls in the top–left of the screen allow various operations for editing the maps.

The first control is a drop–down list of available Areas which allows selection of other areas, once added. This will be empty if no areas are yet configured.

Under the area selector, there is a set of push button controls. Under these buttons is the Device Tree, labelled "Available Channels". Cameras can be added to the current area by dragging them from the list onto the area.

In general a left mouse button drag is used to move objects about. A left double click on an object allows the setting of the object name or parameter. A right click brings up a context sensitive menu.

Right–clicking the map area allows adding Cameras, Event Items (icons representing events being On or Off), Alarm Zones (zones representing events, which will highlight when On), or Area Link Zones (zones which can be clicked to jump to a different Map Area).

The other controls, as follows:

Add an Area
: This creates a new Area with a default name of 'Map Area ' followed by an auto incrementing number. You must have at least one area to drop cameras onto.

Remove Area
: This deletes the current area plus all its associated objects.

Remove all Areas
: Removes all map configuration.

Add a camera
: Adds a camera to the centre of the current area. The camera can be selected and configured later.

Remove all cameras
: Removes all cameras from the current area.

ToolTips Enabled
: If enabled, when the mouse is hovered over a camera, a thumbnail view of the camera is shown along with details of the camera.

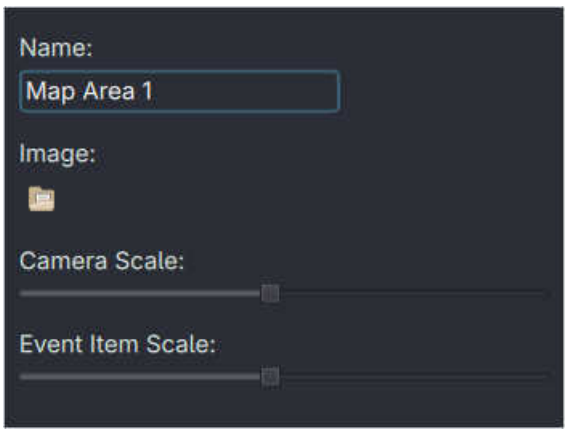
When an area is added, it is automatically selected so that its properties are visible in the bottom left panel. Similarly, selecting a Camera or Event Item on the map shows the available properties for that element in the bottom-left panel. These property panels are described below.

6.7.1 Configuring Zones

As stated above, the right-click drop-down menu allows adding various items to the map, including "Alarm Zones" and "Area Link Zones". Both of these "zone" items consist of configurable polygon shapes.

When a new zone is added, it is added as a square with four "handles". To move a handle, simply click and drag. To add a new handle, and therefore a new point in the polygon, double click on one of the edges of the polygon. To remove a handle, right-click it and choose "Remove this handle".

6.7.2 Area Properties



This panel allows editing properties relating to the area.

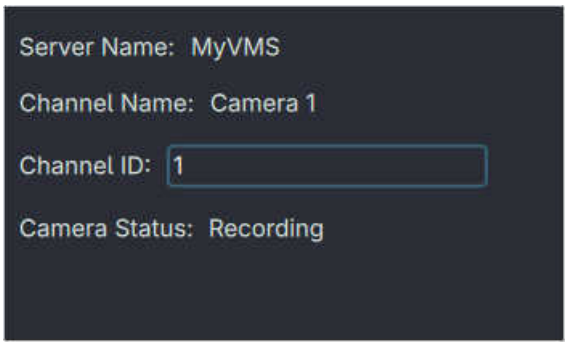
Name
: Allows editing the name of the area which will be shown in the drop-down area selector.

Image
: Clicking the icon allows the loading of an image file to become the background for the area. The SVG image format is supported which allows smooth scaling even when zooming in a long way. Non-scalable formats (png, jpg, gif and bmp) are also supported. There are currently no checks to limit the size of the loaded graphic.

Camera Scale
: Allows resizing the cameras so that they are at an appropriate scale for the area image.

Event Item Scale
: Allows resizing the event items so that they are at an appropriate scale for the area image.

6.7.3 Camera Properties



This panel shows various properties relating to the camera, although only the Channel ID is editable.

Server Name
: The name of the server on which this camera exists.

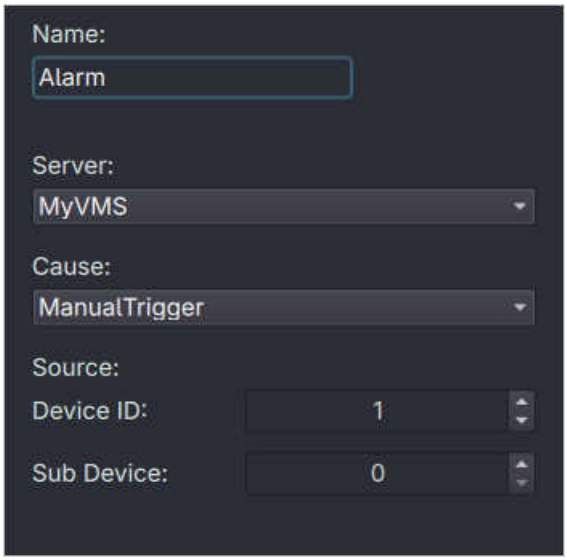
Channel Name
: The name of the camera.

Channel ID
: The ID of the camera, which can be edited.

Camera Status
: The current status of the camera.

6.7.4 Event Item Properties

An Event Item represents the state of an event. It can be assigned to any Event Cause and Event Source on any server.



Name
: The name of this item.

Server
: The server on which the event being monitored exists.

Cause
: The Event Cause with which this Event Item is associated.

Source
: The Device ID and Sub Device ID associated with the Event Item. For camera–based Event Causes, such as Motion, this is usually just a Device ID matching the camera ID. Other Causes might require a Device ID and Sub Device ID, e.g. a door controller and door number.

6.7.5 Alarm Zone Properties

Alarm Zones have the same properties as Event Items. The only difference is that they are displayed as shapes instead of icons.

6.7.6 Area Link Zone Properties

Area Link Zones only have one property: "Linked Area". This is the area that this zone will switch to when clicked.

Mouse Controls

On Areas

- Use the mouse wheel to zoom in and out.
- Left Click and drag to pan around within the area, when zoomed in. reposition areas.
- Double Left Click to rename areas.
- Right Click to bring up a context menu.

On Cameras

- Left Click on camera body to select that camera.
- Left click and hold on camera body and drag to reposition camera.
- Left click and hold on FOV (Field Of View) 'fan' (a dotted line will extend from the fan), and move mouse up and down to alter FOV angle.
- Left click on dot within FOV 'fan' and drag up and down to rotate camera.
- Right click to open the context menu.

Note, you can only do one of these at a time. As soon as you move the mouse in one axis, movement in the other will be ignored.

On Event Items

This is the same as for cameras, except that there is no FOV control.

6.7.7 Settings

The map settings are as follows:

Custom Camera Icon
: Click the folder icon to choose a different default icon for the cameras. To reset to the default icon, ensure that the 'Use Default' switch is to the right.

Notes About Image Files

The software supports loading of SVG, JPEG, JPG, and PNG image files as map area images. The files will be uploaded to the server so that they are available for other map users to view. Once they have been uploaded to the server, the original source images may be deleted and the images will still be visible in the map viewer until they are removed or changed on the server. See section of Map Local Storage.

If an image fails to load because it has been removed from the server without deleting the associated map objects, then a place–holder graphic will be displayed instead.

Map Local Storage

Map image files are stored on the server and must be downloaded to the local system in order to display them. To avoid unnecessary downloading of data from the server, map image files are stored in a local temporary directory which the software tries to automatically keep synchronised.

The location of this temporary directory can be changed by the user (see section 3.22.1 – System Set–tings). The software will overwrite and delete files in the temporary directory without warning, so it is suggested that if a non–default location is chosen it should be a directory solely for this task. The user may safely delete files stored in this directory as this will not interfere with the operation of the software.

It is possible to manually update the map image files using the software File Manager.

If many map layouts are created and modified, it may be necessary to clean the files. The map files are listed in a section in the file manager and can be deleted or replaced individually, if required.

If a file is removed from the server when it is being used by a map layout, then the software will display an error image. This can be fixed by manually changing the image associated with the area.

The contents of the local cache directory are kept synchronized with the contents of the map directory on the server.

If a server is part of a group, changes to the map layout will be copied across all servers in the group so that the same map layout is visible no matter what server the software is connected to. Image files are stored and copied to all servers in a server group.

6.8 Server Group

Note: The settings in this page apply to all servers in the server group.

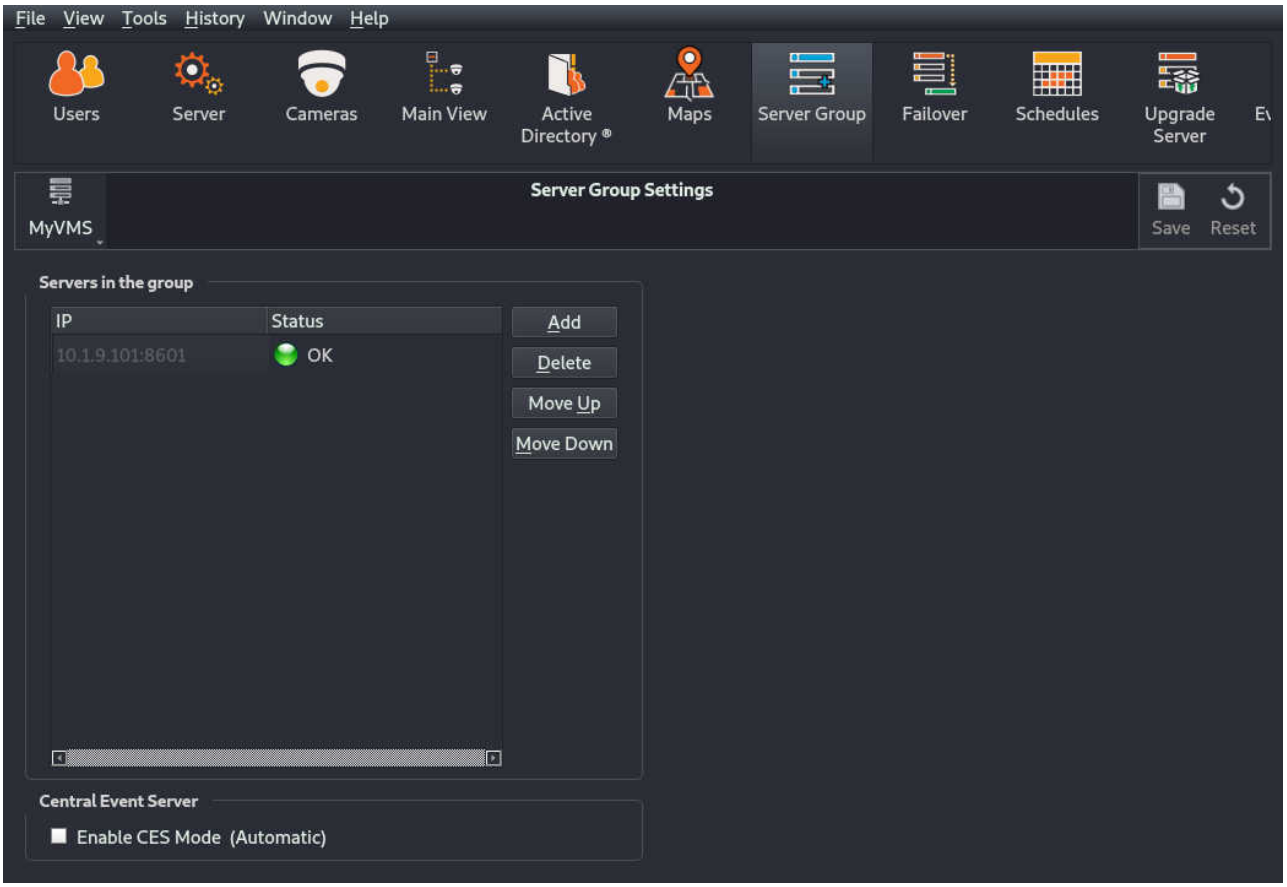
Individual Wavestore Servers can be configured as a server group, allowing users connecting using WaveView client software to access cameras connected to any of these servers. This feature is only available in certain licence levels.

Administration of any of the connected servers can also be carried out from a single Client.

All of the servers intended to be part of a Server Group must first be configured to be connected to the same LAN subnet (contact your IT administrator for assistance if necessary).

When a server group is being created the WaveView client will attempt to connect to each new server added using the login credentials used for the current connection. Those login credentials need to be an install–level user on each of the target servers.

Usually this means ensuring that each individual server has an install–level user configured with the same password, then logging in to the first server with those credentials before adding the others. It may be advisable to check that you can log in to each server before creating the group.



The procedure for creating a Server Group is as follows:

- Login to the server nominated to be the first server in the group. Ensure to use the IP address or hostname that you want to be entered in the server group configuration – this could be a Private

IP address, potentially a secondary address if the server is a Logical Server in a Failover group, or a Public IP address.

- Go to the 'Server Group' setup screen. You should see the IP address or hostname of the first server automatically entered.
- Click the 'Add' button.
- In the IP address field that appears, click the 'Enter host here' text, then enter the IP address of the next Wavestore server to be added to the group. As noted above, this could be either a Private IP address (potentially a secondary address if the server is a Logical Server in a Failover group), or a Public IP address.
- Repeat for any further servers as required.
- Click 'Save' when finished.

If any of the servers fail to be added, it's sensible to abandon the changes, log out, then attempt to log in to that server directly using the same login details. That way you are likely to get more specific error messages about why the connection failed.

You may wish to synchronise the time on all of the servers in the group to the same time source (either once of the servers, or an external NTP time source.

Central Event Server

The "Enable CES Mode" checkbox is used to enable the Central Event Server feature. This is described in more detail in section 9.18 – Central Event Server.

Note that for this feature to work, the IP addresses provided in the Server Group list must be contactable by each other. This is because the servers communicate between each other to pass events.

6.9 Failover

The Failover Setup Screen is used to configure the list of *physical servers* in a *failover group*. These concepts, as well as a full guide to configuring failover for a group of Wavestore servers, are explained in more detail in section 9.19 – Failover. This section covers this particular setup screen only, but failover requires several setup steps.

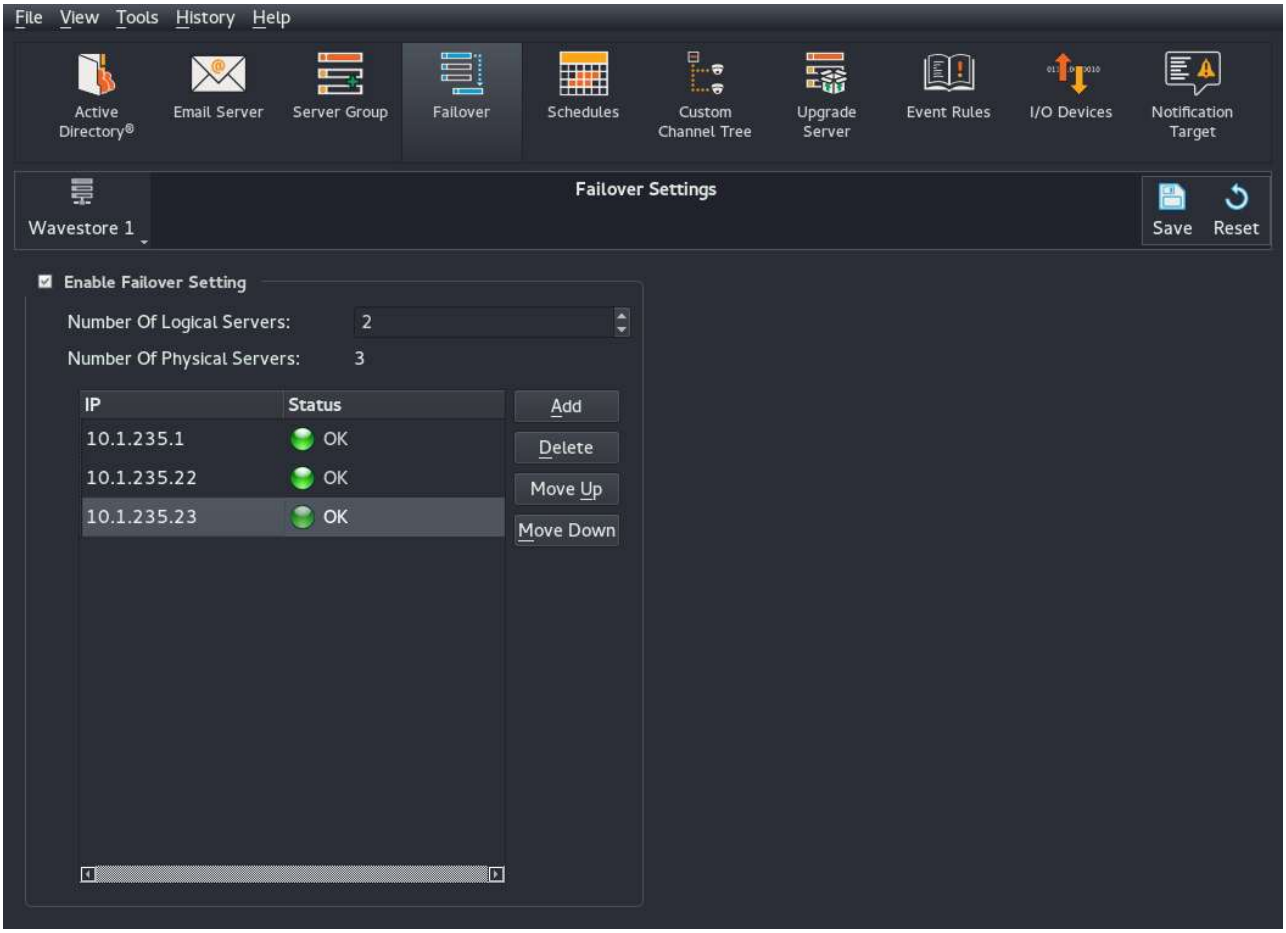


Figure 6.34: Failover Setup Screen

The list of *physical servers* is configured by using the **Add** and **Delete** buttons and entering the IP addresses in the table.

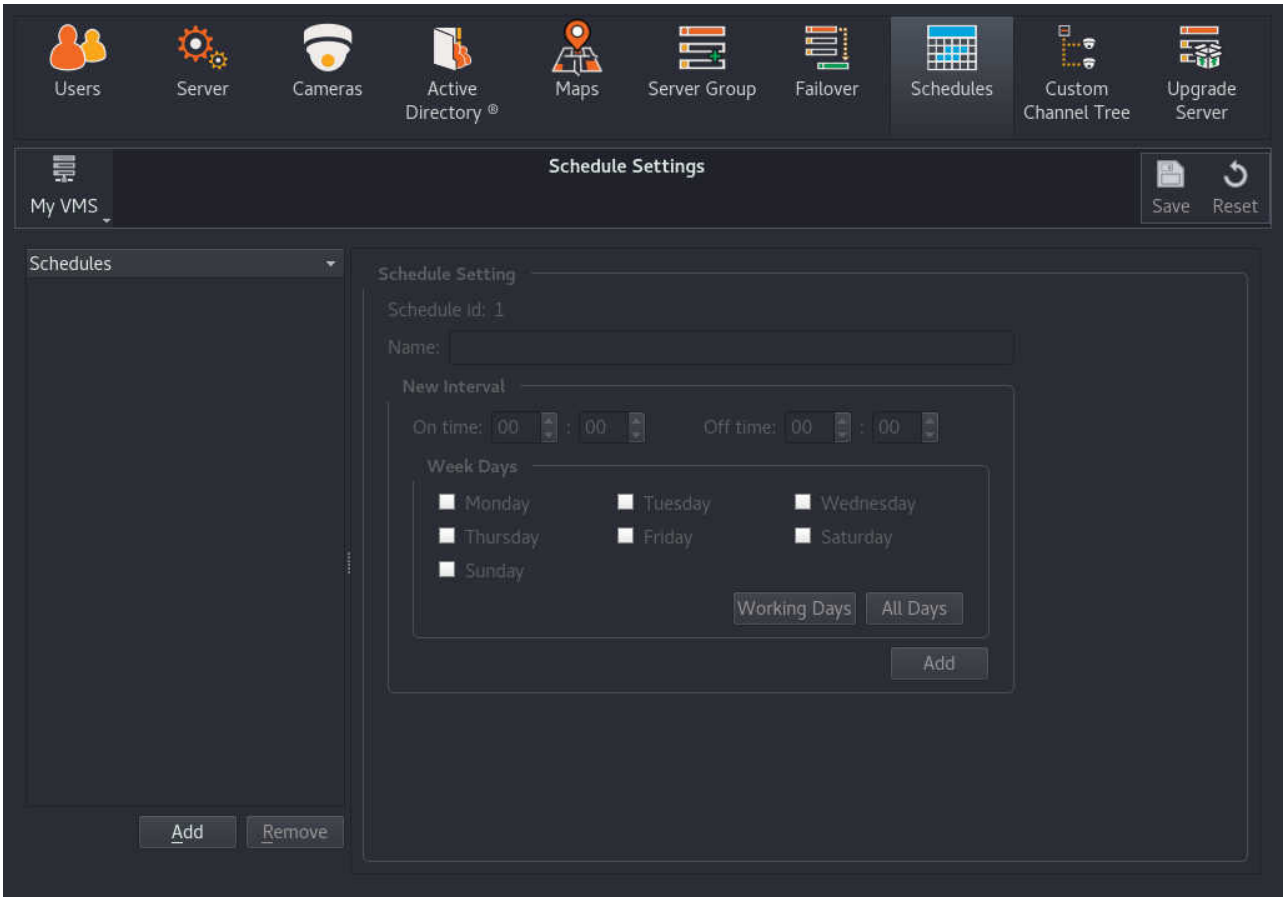
As each physical server is added, WaveView will attempt to connect to the address and, if successful, check that DHCP is not enabled for any network interfaces since this can cause problems with the failover mechanism. A warning will be shown if the connection or DHCP check fails.

6.10 Schedules

Note: The settings in this page apply to all servers in the server group.

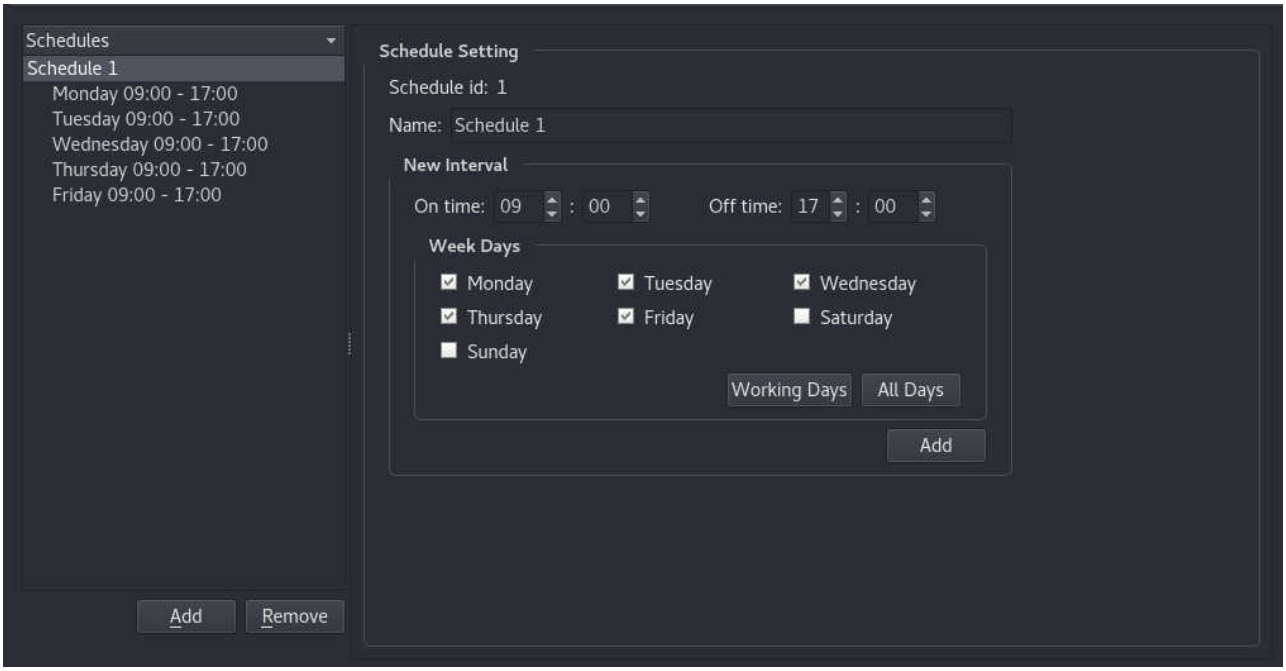
The Schedules menu allows the system administrator or installer to create schedules that can be used to control server functions, such as Recording or User Logon.

There is an "invisible" schedule numbered zero which implies "always on", therefore it is not necessary to create a schedule for this purpose. All settings, such as recording and user logon will use schedule zero by default. Schedules should only be created when it is intended that something should be disabled at a certain period of the day or week.



Once a schedule has been defined, it can be linked to multiple functions such as camera recording, event rules, and user login permissions.

To create a new schedule for a camera, follow the menu path View → Setup → Schedules. Under the Schedule List (left side of screen), click 'Add' to create a new schedule:



With the new schedule highlighted dark grey in the Schedule list, you can now configure items on the new Schedule such as Description, On/Off Times and Days etc.

Schedules can be configured with multiple On and Off times, for example, 'On' at 02:00, 'Off' at 04:00, then 'On' again at 14:00 and 'Off' again at 16:00, for Monday, Tuesday and Friday. To configure this, select the times using the On/Off Time controls, then select the required days in the Week Days panel and then click 'Add'.

The dates and times will then appear under the schedule in the schedule list.

Individual items can be removed from the schedule by selecting them in the schedule list and clicking Remove. Alternatively the complete schedule can be removed by clicking to highlight, then clicking Remove.

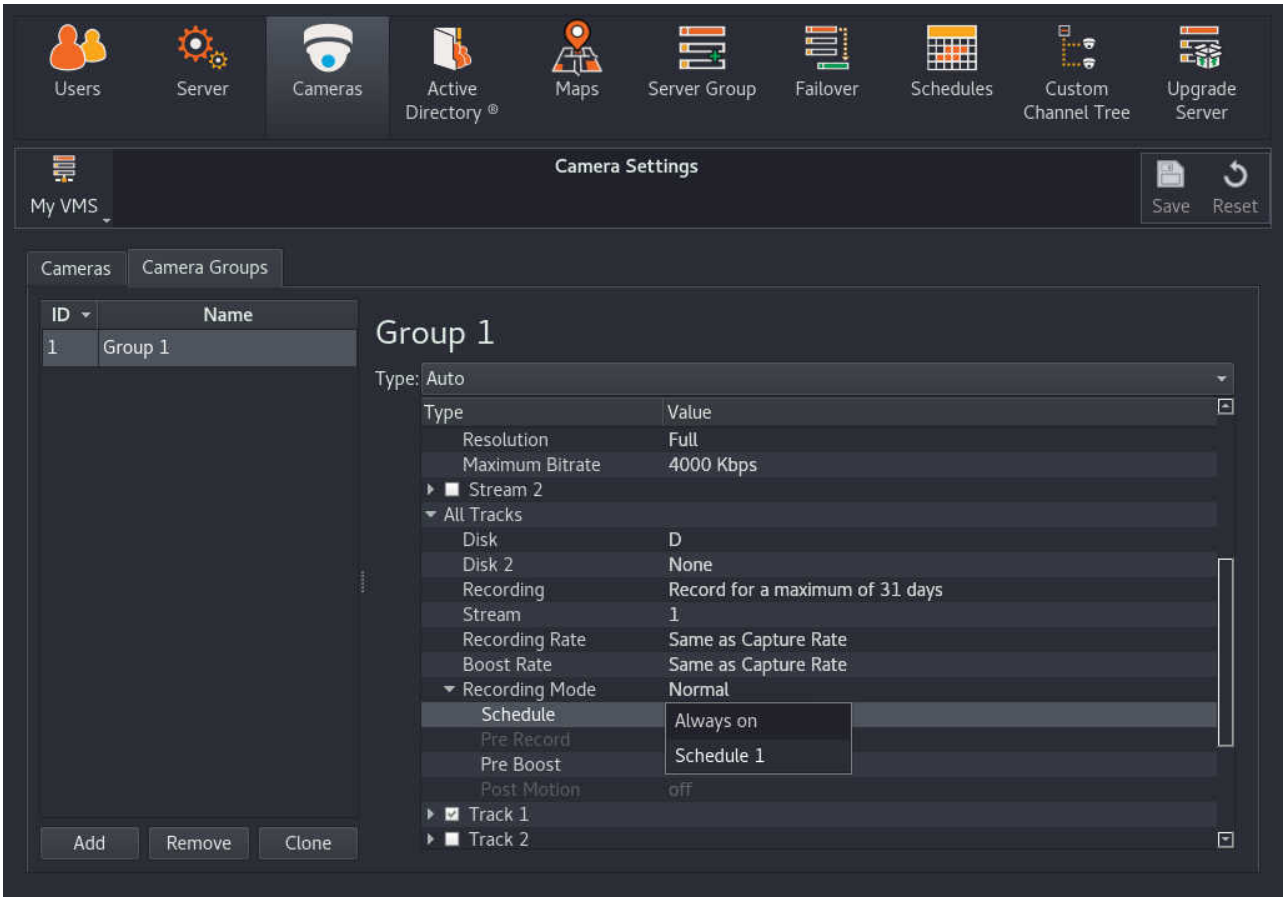
To configure a schedule which runs overnight from one day to another, these is created in two segments;

- Segment 1 is set with 'Off' time to be 24:00,
- Segment 2 is set with 'On' time to be 00:00 the following day. For example, for a schedule to run from Monday 2200hrs to Tuesday 1000hrs, configure as follows:
- Monday 22:00 → 24:00
- Tuesday 00:00 → 10:00

Repeat this process for any other required schedules and click 'Save' to save the changes.

To attach a schedule to a Camera Group for Recording, follow the menu path View → Setup → Cameras. Select the 'Camera Groups' tab and then select the Camera Group to which you want to assign the schedule.

Each Camera Group has multiple recording tracks so the schedule can be assigned to 'All Tracks' or a specific track. Under the desired track, or 'All Tracks', expand the 'Recording Mode' option and then click the menu next to 'Schedule' as shown below.



Finally click on 'Save' to confirm the changes that you have made.

6.11 Upgrade Server

Note that from version 6.10 onwards it is necessary for the Wavestore to be suitably licensed for an upgrade to the target version. The section 6.2.3 – Licensing explains how to check your "upgrade bundle" version number. From WaveView version 6.8 onwards the Upgrade screen will warn if attempting to upgrade to a version later than permitted by the licence.

The Upgrade Setup Screen (menu path *View* → *Setup* → *Upgrade*) allows the Wavestore server software to be upgraded to the latest version.

Note: Upgrades will be applied to all connected servers in the server group and can be carried out from a networked PC or laptop, or on the server itself.

If upgrading from a remote PC, it is recommended to update the WaveView software on that PC first, before upgrading the servers.

There are two methods of upgrading the system to a new version:

File Upgrade
: The system will be upgraded using an ISO file which has been downloaded. No internet connection is required.

Network Upgrade
: The system will download updates from the internet. Therefore, the Wavestore servers must be connected to the internet.

6.11.1 Performing a File Upgrade

To upgrade from an ISO file, the ISO first needs to be "mounted" or written to a USB memory stick or DVD. If the ISO is on a Windows PC, the easiest method is simply to mount the ISO. This is done by right-clicking the ISO file and choosing *"Mount"*. The ISO is then available as a separate disk (e.g. "F:"), as if a pre-written USB stick or DVD had been inserted.

If it is necessary to upgrade the Wavestore by connecting to it directly rather than from a remote client PC, it will be necessary to write the ISO file to a USB memory stick or DVD. On Windows we recommend the use of a program called Rufus. See section 14 – Appendix D – Writing an ISO with Rufus.

Before performing the upgrade, navigate to the Server setup screen (View → Setup → Server) and inspect the "Distribution" field. This is displayed on the "General" tab which is the default.

If the distribution contains "el7" rather than "el7a" it is recommended to perform the upgrade twice. The first upgrade will update the Wavestore software but not the operating system. The second will update the operating system. This is only ever necessary once. Subsequent upgrades will only need to be performed once.

If in doubt, performing the upgrade twice is sensible. If there is nothing to upgrade on the second pass it will complete very quickly.

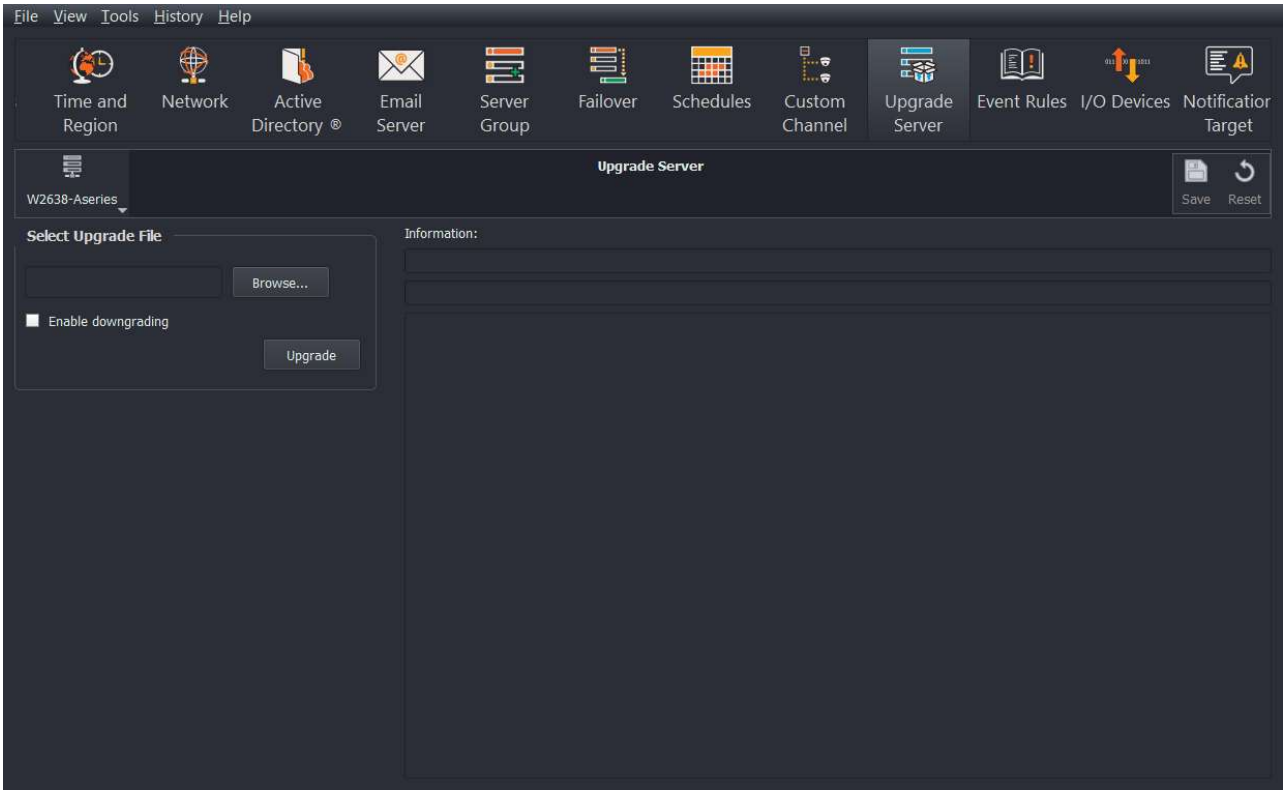


Figure 6.35: Upgrade Server Screen

To perform the upgrade, first browse to the location of the upgrade file ('upgrade.txt').

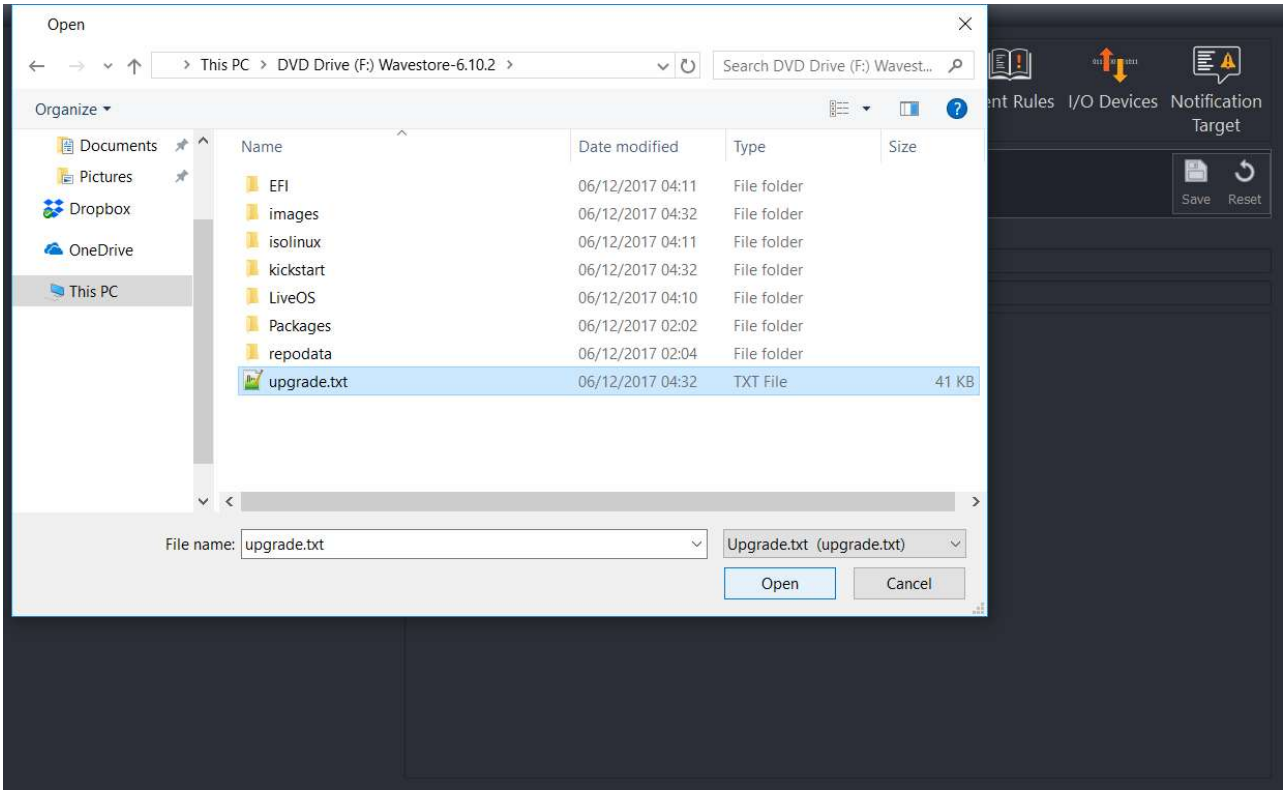


Figure 6.36: Upgrade Server screen – browsing to locate 'upgrade.txt' file

Once you have located the ***'upgrade.txt'*** file, select it then click on ***'Open'***.

The ***Select Upgrade File*** field will now show the upgrade file that you have chosen.

If performing a downgrade, ensure the "Enable downgrading" checkbox is checked. Only enable this checkbox if deliberately downgrading to an earlier version.

Click on ***'Upgrade'***, and the Information window will show progress of the upgrade, as the upgrade files are copied across to the server:

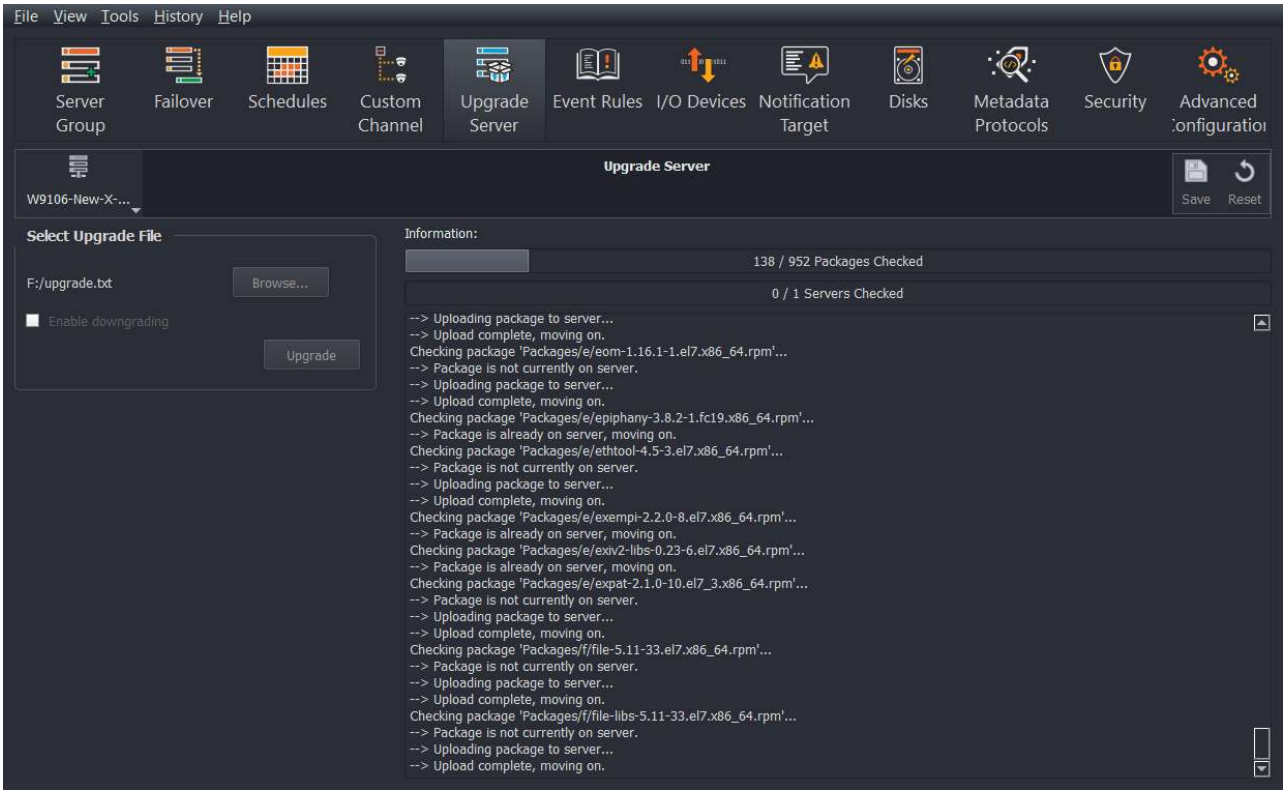


Figure 6.37: Upgrade Server screen – upgrade files being copied to the server

Once all the files have been checked and copied, the upgrade process will start. The system will tell you to wait and this may take a few minutes.

Whilst the upgrade takes place, recording continues. However once the upgrade is complete, the server will either do a software restart or a reboot, depending on what is necessary to complete the upgrade. Obviously recording is interrupted briefly at this time. Downgrades will always perform a reboot.

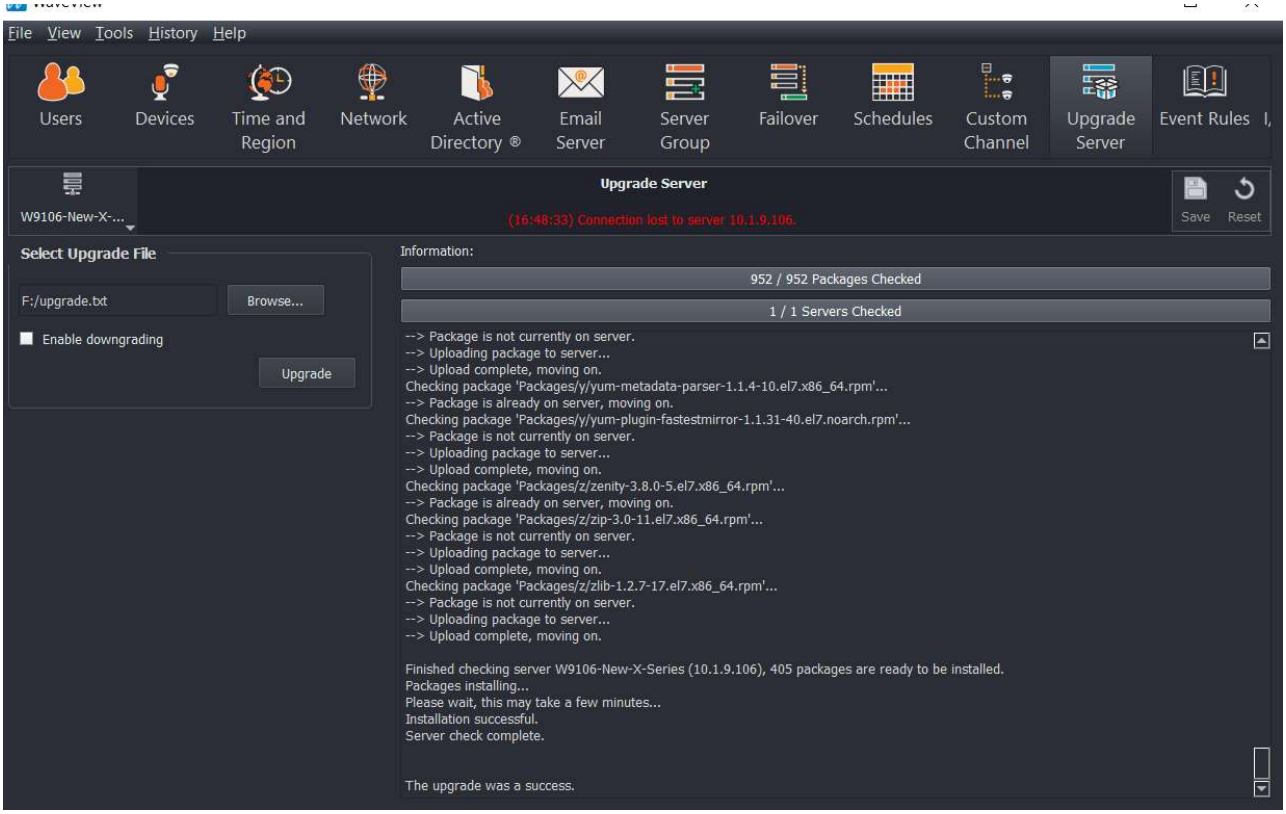
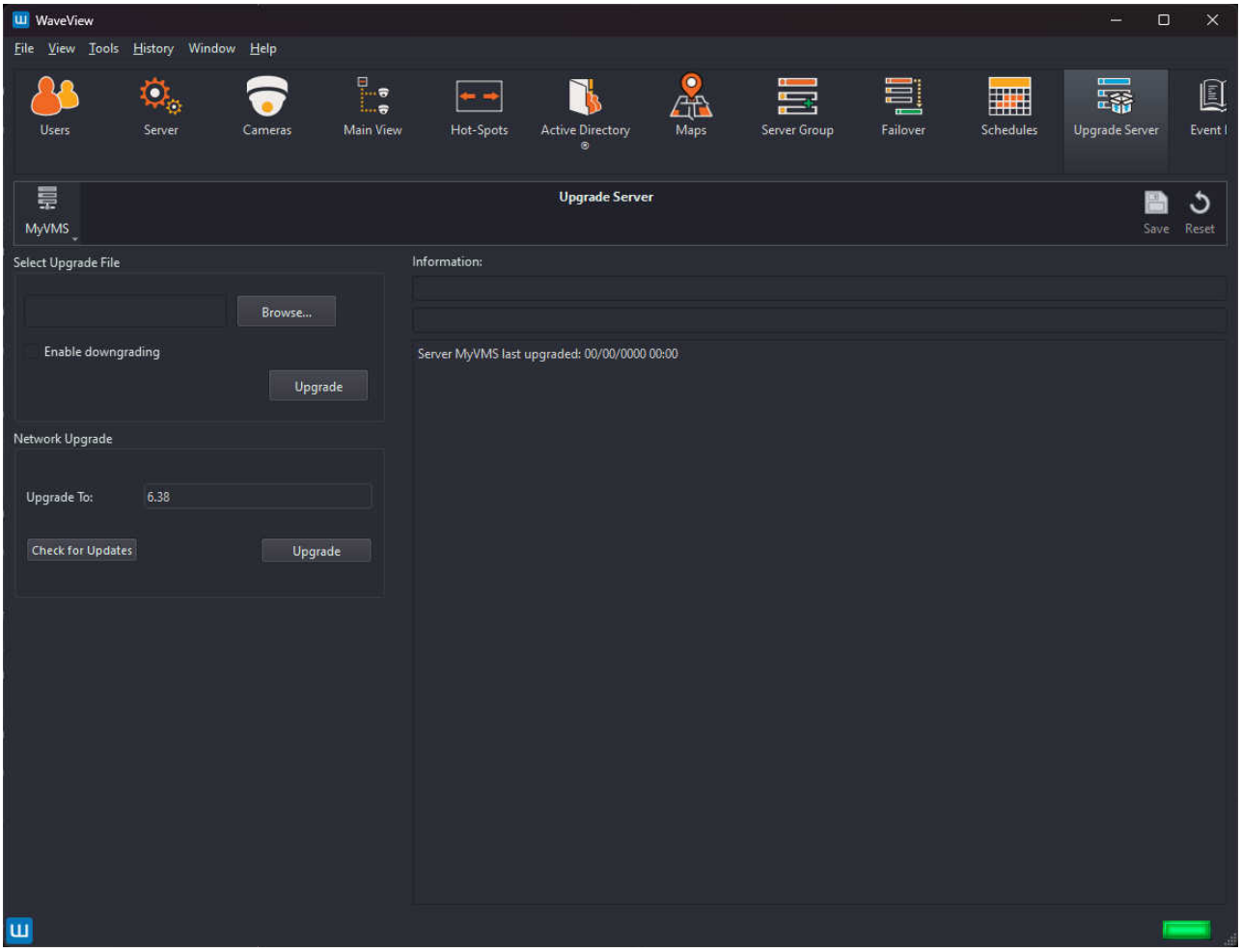


Figure 6.38: Upgrade Server screen – upgrade completed

6.11.2 Performing a Network Upgrade

Servers running version 6.38 or later can be upgraded over the internet. Each server in the server group will need to be connected to the internet.

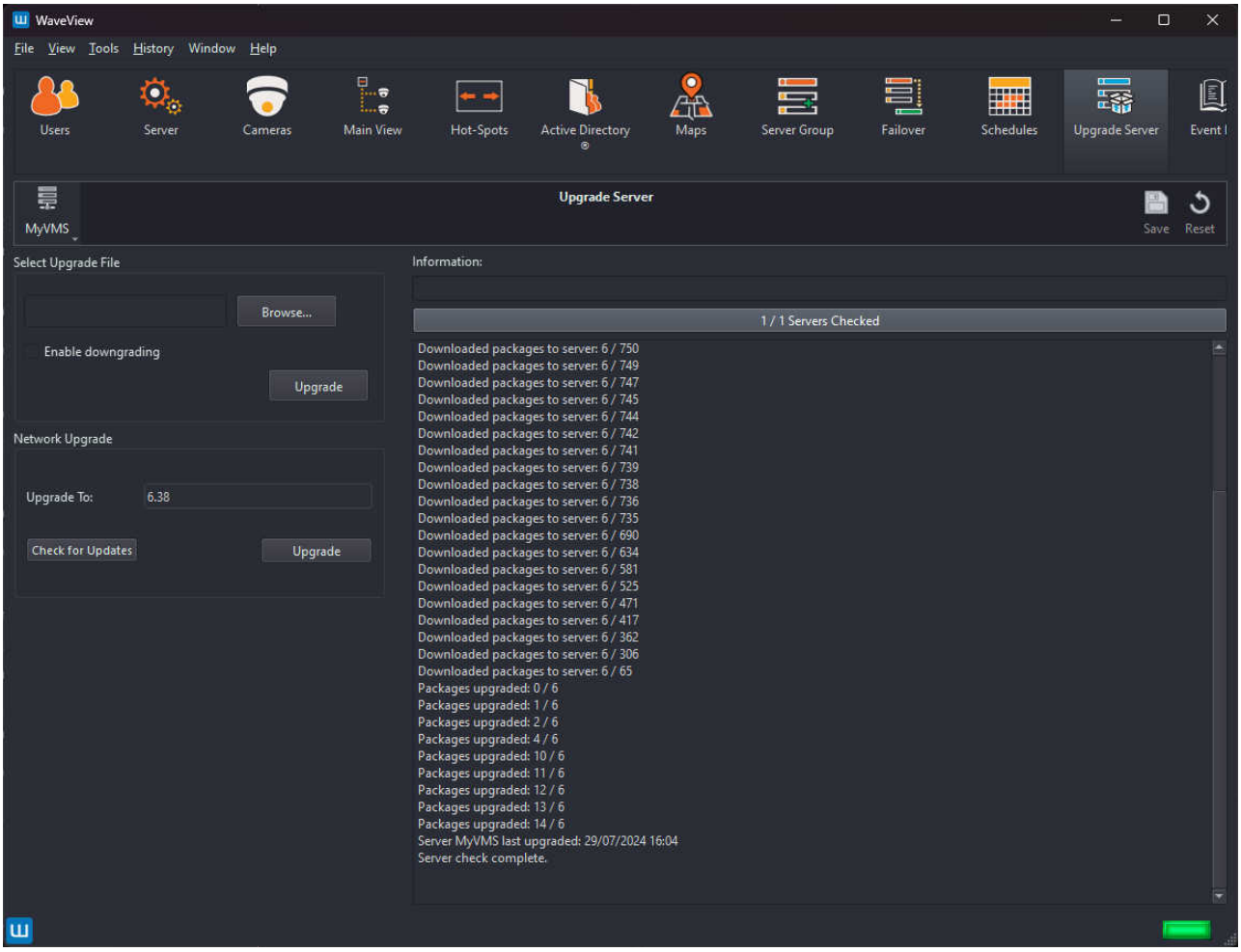
Note: If any server in the server group does not support network upgrades, network upgrades will be disabled for the whole group. In that case it will be necessary to log in to each server (which does support network upgrades), and perform the upgrade individually.



To perform a network upgrade, enter the version to which the servers should be upgraded in the *'Upgrades To'* text box, for example *'6.38'*, then click *'Upgrade'*.

The process performed by each server is:

- Check that the requested upgrade version is available
- Download the packages (i.e. components) for the upgrade
- Install the packages



The progress of the upgrade will be reported in the *'Information'* panel.

6.11.3 Potential Issues

If the upgrade fails, it will usually either show a failure message in the Upgrade screen, or a message saying "the upgrade completed without sending a status reply".

In this case, gathering more information depends on the currently running version.

For servers running version 6.24 or later, this information is available in WaveView by navigating to *Tools → System Log*, clicking the *'Extra Logs'* tab, then choosing *'Upgrade'* from the drop-down box, then clicking *'Download'*.

For servers running version 6.16 or later, a more detailed log of the upgrade is available by following this procedure:

- Select *Tools → Execute Command...*
- Run the command *alog -a Upgrade*
- Send this output to our support team for assistance

For servers running version 6.14 or earlier, the information is in the system log, available in WaveView by navigating to *Tools → System Log*.

The possible errors are listed below with an explanation of what to do:

Upgrade failed: installing package XXX needs nMB on the / filesystem

Certain upgrades such as to v6.16 require a large amount of temporary space on the operating system disk and those originally installed with an early version of Wavestore (version 6.10 or earlier) may not have enough space to complete a full upgrade.

It may be possible to free up space on the system using the file manager although this requires physical access to the server. Using the client display on the server itself, move the mouse to the top-left of the screen and a toolbar should drop down. Choose the icon which resembles a filing cabinet. If there are any large files in there, deleting them may free up enough space to complete the upgrade.

If the above steps do not work, it may not be possible to perform the operating system upgrade without a re-installation. Re-installation requires being on-site and usually takes around 20 minutes. Performing the re-installation creates a larger partition so that future upgrades do not have this issue.

SSD wearing out too fast

This message may appear in the log because some upgrades perform a large amount of writing to the operating system disk. Unless you are going to do a full system upgrade every week, this is not a concern and can be ignored, and the SSD will still last for many years.

Note that the message is a check on rate of wear, not an indication it is worn out. If you want to see how much life left (in percentage terms), in WaveView go to *Tools* → *Execute Command* and run the command *"ssd"*.

6.12 Event Rules

Note: The settings in this page are independent for each server in the server group.

The Event Rules menu can be reached by the menu path Tools → Setup → Event Rules.

This menu allows the server to be configured with Event Rule(s) to react to "event causes" (e.g. video loss, digital input, motion event), by triggering "event actions" (e.g. send email, move PTZ camera, trigger digital output).

Note that in version 6.20 a new Event Rules system was introduced. The old and new event rules engines are not compatible. When a Wavestore server is upgraded to version 6.20 and has existing event rules, the Event Rules setup screen will show "Using legacy Event Rules mode" at the top. The old system can still be used, but to enable usage of the new engine it is necessary to remove all existing event rules, then exit the Event Rules screen and re-enter it.

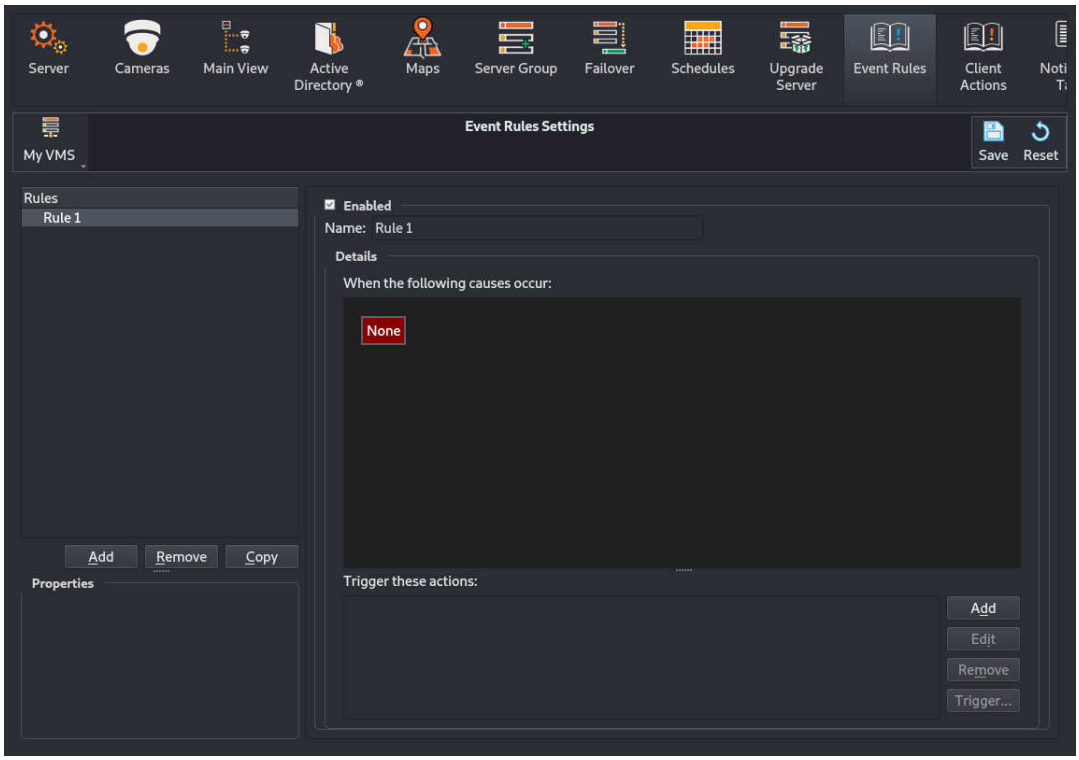
In the new event rules system, event logging occurs to a special Events log file. This can be viewed using the Extra Logs tab of the System Log window. It is listed as "Event" in the drop-down selector. See section 3.21.2 – Extra Logs.

6.12.1 Creating and Editing Event Rules

Event Rules can be added by simply clicking the Add button under the Rules list. Existing rules can be removed or copied by selecting them in the Rules list and clicking Remove or Copy.

Existing event rules can be edited simply by selecting them in the Rules list.

Newly added event rules have a single Event Cause set to "None". All rules need at least one Cause and Action.



Causes can be editing by double-clicking, or right-clicking and choosing "Edit...".

Multiple Causes can be added by adding logical operators. These logical operators can be added by right-clicking a Cause and choosing "Add Operator...".

The logical operators are:

Logical OR
: The output is True if either or both inputs are True.

Logical AND
: The output is True if both inputs are True.

Logical XOR
: The output is True if either inputs are True, but not both.

When a logical operator is added, a new "None" cause is automatically added.

Both Cause and Actions can be triggered for testing purposes. Causes can be triggered by right-clicking on them and choosing the desired type from the menu. Similarly, Actions can be triggered by selecting them and clicking the "Trigger..." menu. When triggering a Cause or Action you can select:

On
: Turn the Cause or Action to the "On" state.

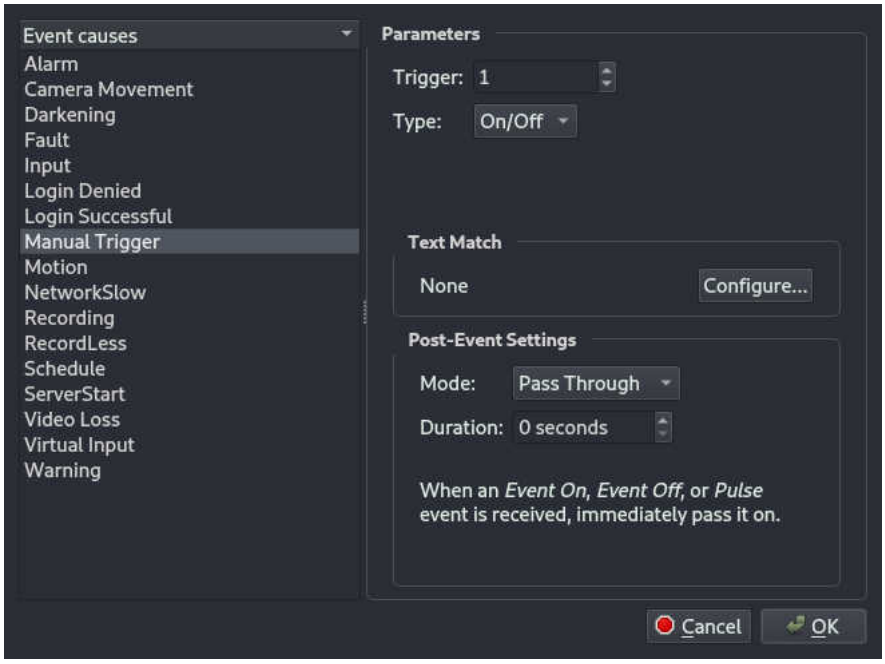
Off
: Turn the Cause or Action to the "Off" state.

Pulse
: Trigger the Cause or Action instantaneously.

Causes can be removed but logical operators cannot be directly removed. To remove a logical operator it is necessary to remove one of the 2 Causes connected to it.

Note that, when using the Central Event Server feature, and when editing Server 1, it is possible to select the Server for each Cause and Action. For example, Motion on Camera 3 of Server 2 could be used to trigger Output 1 on Server 3. See section 9.18 – Central Event Server.

6.12.2 Event Causes

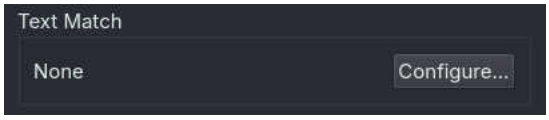


Event Causes are the conditions for a rule to be triggered. The different types of Cause are documented in this section.

Causes can be triggered as a "Pulse" – meaning they are instantaneous, or "On/Off" – meaning they have a start and an end.

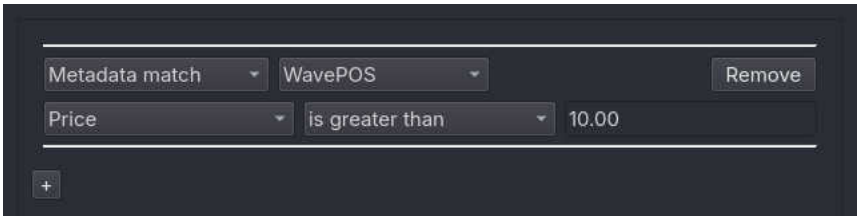
Text Match

Each Event Cause can have Text associated with it. The Wavestore event rules system can do pattern matching on this text so that Causes only trigger when those matches occur.



These matches can be simple sub-string matches to some provided text, a sub-string match within an uploaded file, or more complex matching of fields in "metadata". Metadata is usually supplied when causes are triggered by devices configured via Wavestore Integration Modules.

For sub-string matches, select "Text contains..." and provide the text to match in the text box.



For metadata matches, it is necessary to select:

The Metadata Protocol These are usually configured automatically when an Integration Module is installed. An example might be "Point of Sale".

The Metadata Tag These are also configured automatically by Integration Modules. They are fields within a particular metadata protocol. For "Point of Sale" these might be "Item" or "Price" for example.

The Condition This is the type of match to perform. It can be "exists" to check if a Metadata Tag is present. Alternatively it can be "equals", "is greater than", or "is less than" to perform a comparison. For all conditions except "exists", a value should be provided in the text box provided.

For matching against entries in a file, select "Named Table Match", then choose the desired match file.

Multiple matches can be added by clicking the plus (+) button. In this case, all the conditions must be matched for the Cause to be accepted.

Any match can be removed by clicking the "Remove" button next to it.

Post-Event Time Settings

Each Cause has "Post-Event Settings" which allow the timing to be modified in some way.

Pass Through
This is the default and simply means that any "On", "Off" or "Pulse" event is passed on immediately.

Extend End
The "On" is triggered immediately but the "Off" is delayed by the specified number of seconds. If a "Pulse" event is received it is treated like Fixed Duration (see below)

Fixed Duration
When an "On" or "Pulse" event is received, it will be considered "On" for the specified duration, then "Off".

Pulse
This turns an "On/Off" event into a pulse. When the "On" is received, it is triggered as a "Pulse", then the "Off" is ignored.

Delay Start

This mode only affects "On/Off" events. The "On" is delayed by the specified number of seconds. The "Off" is passed on immediately.

Post-Event settings are configured for the Event Cause of the Event Rule, and therefore all associated Event Actions are affected. This may not be desirable for certain kinds of Event Actions. For example, if you have two actions, one to record video and one to send an email, the Post-Event setting might make sense for the Record action but not the Send Email action, and so the behaviour might not be as expected. In this case it is sensible to create two separate rules, one for each Action.

Available Causes

Wavestore provides a built-in collection of Event Causes, but some are also conditionally added to the list. The conditionally added Event Causes can appear for the following reasons:

- An ONVIF IP camera has sent an event of a type not in the present Event Causes. The Wavestore server will record this event type and make it available as an Event Cause upon which an Event Rule can be built.
- An integration module has been installed which defines these Event Causes. These EventCauses will pertain to types of event which can come from the device the integration module relates to.

Note that some well-known ONVIF event types are already mapped to built-in Wavestore types. For example, the ONVIF event type for "Motion" is already mapped to the Wavestore "Motion" event cause.

When a non-built-in Event Cause is selected in an event rule, the only options available are a "Device ID" field and a "Sub-Device ID" field. These fields allow specifying generic parameters and their meaning will relate to the type of event cause, for Device ID 1 and Sub-Device ID 2 might mean door 2 on door controller 1.

The standard Event Cause types are listed below. The entries that do not have descriptions are some common events that can be received from different cameras. Any documentation for these events should be available either from the camera manufacturer, or in the ONVIF standard.

Alarm

This Cause occurs when an 'Alarm' Action occurs. For example, one rule might take some Cause or combination of Causes, and use it to trigger "Alarm 1". Another rule can then be created where the Cause is "Alarm 1" and some other Action is applied.

It can also be used to provide highlighting certain events in the main screen Live Event Stream. For example, if a digital input is triggered AND there is motion on a camera, you might want to trigger an Alarm with some preset text for operators to see in the Live Event Stream.

The only parameter is an arbitrary Alarm ID.

Camera Movement

This Cause is used to detect scene change. It is triggered when motion occurs around all (or most) of the edges of the image. This can be detected by the Camera (by an ONVIF GlobalSceneChange event, for example) or by the Server. See Motion (below) for details on how to configure this.

The only parameter required is the camera.

Darkening

This Cause is used to detect when the image becomes dark, presumably due to being obscured.

This can be detected by the Camera (by an ONVIF ImageTooDark event, for example), or by the Server. See Motion (below) for details on how to configure this.

The only parameter required is the camera.

Fault

This Cause is triggered when the server enters a Fault state, meaning something is wrong. It is required to choose a particular fault type.

Voltage problem

Only for supported motherboards. Check the documentation for your hardware platform.

System Over Temperature

Only for supported motherboards. Check the documentation for your hardware platf orm.

Generic fault

Any fault not otherwise classified.

Fan Problem

Only for supported motherboards. Check the documentation for your hardware platform.

Disk over Temperature

Only for direct attached storage.

Disk Failure

A direct–attached disk has failed or a member of a direct–attached RAID array has failed. For network attached storage this will only trigger if the device is not–contactable, rather than for individual drives in an array. However, for RAID arrays, it will trigger if a member disk has failed, even though the RAID array itself might still be functional due to the redundancy.

Disk SMART pre–failure

Only for direct attached storage, not including hardware RAID arrays.

Capture Card failure

For analogue capture cards.

PSU problem

Indicates a PSU fault. Not all PSUs are capable of producing this fault indication.

Input

This Cause is triggered by digital inputs. The inputs can be from:

- IP Cameras
- Configured I/O Devices (see section 6.2.11 – I/O Devices).

The parameters to select are the device (either Camera or I/O Device), and the Input number on that device.

Login Denied

Triggered when a user tries to login but is denied. No parameters are required.

Login Successful

Triggered when a user successfully logs in. No parameters are required.

Manual Trigger

Manual Triggers can be used to allow event rules or their actions to be triggered from the main

screen. The Rule name is displayed on the main screen. Ensure every manual trigger has a unique source id.

Note that Manual Triggers can be configured with a Type which can be "On/Off" or "Pulse". "Pulse" types are instantaneous whereas "On/Off" are stateful and have a start and an end.

Motion
: This Cause is triggered when motion is detected for the specified camera. Note that for IP Cameras, the means by which this is detected can vary depending on how the Camera Group is configured. It is possible to use Server-side VMD or Camera-side VMD (see section 6.3.2 – Camera Group Settings).

NetworkSlow
: This Cause is triggered when a network link from a bonded network interface goes down or a link renegotiates to a slower speed. Note that in some cases a Fault will also be triggered in this case, for example if the network cable for a non-bonded network interface is removed.

Recording
: This Cause is triggered by recording occurring on any recording track for the specified camera.

RecordLess
: This Cause is used to detect when recording is occurring for less than the configured duration on the selected camera and track. It will only trigger when overwriting is occurring on the selected track, and the recording duration is less than that configured for that track. The event cause will remain "on" until the configured recording duration is achieved.

Schedule
: This Cause can be used to trigger based on pre-configured time schedules (see section 6.10 – Schedules. The Cause is "on" when the schedule is "on" and the same for "off".

  Normally this would be used in conjunction with another Cause and the "AND" logical operator. For example you might want the rule to trigger only when motion occurs on a particular camera AND the schedule is on, to detect movement out of working hours.

ServerStart
: This Pulse-type Cause occurs when the server software process is starting. Note that this is not exactly the same as a reboot since server process restarts can occur without a reboot, although a reboot will also trigger a ServerStart.

Video Loss
: This is triggered when loss of video signal occurs. For analogue cameras, the analogue cable might be removed. For IP cameras, it would normally mean a loss of connectivity to the camera or refusal of the camera to stream.

  Note that this Cause also works for audio channels and has the same meaning, except for audio rather than video.

Virtual Input
: This Cause is like Input except it's not required for a device with an input to actually physically exist. This is useful when needing to trigger some rules over the network. For example an external program might trigger Virtual Inputs of different numbers in order to trigger some Actions. These rules can be configured with Virtual Inputs as the cause.

Warning
: This Pulse-type Cause is triggered when certain warnings are raised by the server.

Dynamic Event Cause types will depend on the presence of the camera, integration module or a specific service.

Event Causes which are enabled when a Failover group is enabled are:

Failover
: This Cause is triggered by a Standby server when failover occurs.

StandbyFail
: This Cause is triggered by one of the main servers when the Standby server in a failover group fails.

Dynamic events from cameras include the following. In the majority of cases the same name is used for events from different cameras even if the camera uses slightly different terminology. (In a few cases slight variants have crept in, notably Tamper and Tampering). The meaning of these events will be in the camera documentation.

AbandonedObject

AdaptiveMotion

AnomalyDetected

AppearDisappear

Audio

AudioDetection

CameraSabotage

Counter

DirectionViolated

Enter

Exit

FaceDetected

ImageBlurry

ImageBright

IntruderAlarm

Intrusion

LineCrossed

LineCrossedLeft

LineCrossedRight

Loitering

LoiteringDetection

LPR

Mask

MxActivitySensor

MxAnalytics

MxMotion

Object

ObjectCounter

ObjectCounting

ObjectCrosses

ObjectDisappears

ObjectEnterArea

ObjectInside

ObjectLeaveArea

ObjectNotPresent

ObjectPresent

ObjectPresentRepeated

ObjectRecognized

ObjectRemoval

ObjectsAppears

ObjectsInside

ObjectsLeaves

ObjectStops

PeopleCounting

PTZPresetAborted

PTZPresetInvoked

PTZPresetLeft

PTZPresetReached

EdgeRecording

Relay

Shock

SmartMotion

StoppedVehicle

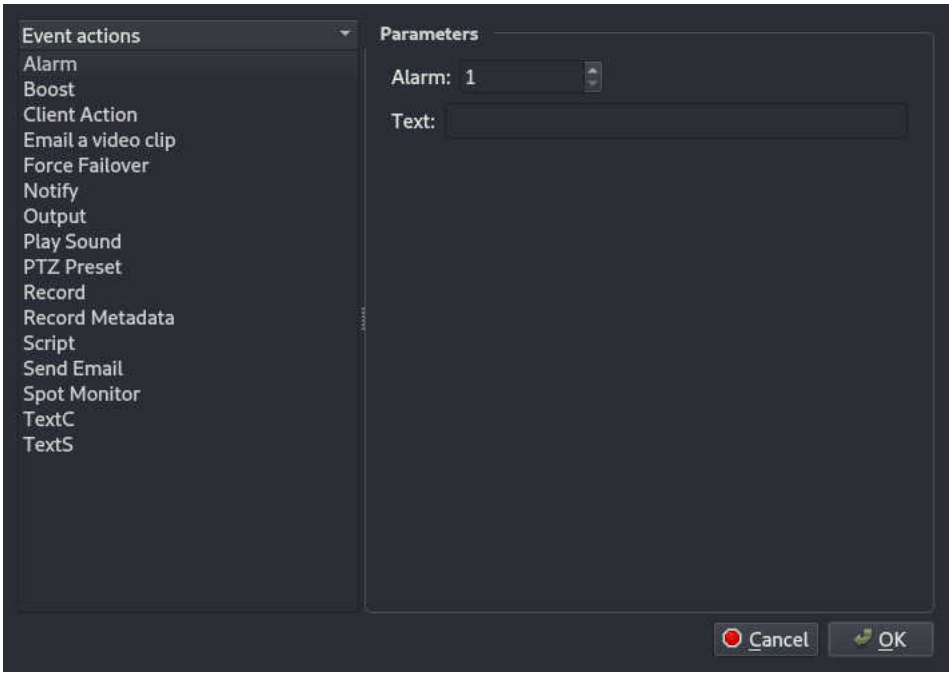
Tamper

Tampering

EdgeTrack

VirtualInput

6.12.3 Event Actions



Event Actions are the actions that the system will take when the Cause conditions are met. Multiple actions can be triggered. The different Actions are documented in this section.

As with Causes, Wavestore provides a built-in collection of Event Actions, but some are also conditionally added to the list by installed integration modules.

Available Actions

The standard Event Action types are as follows:

Alarm

This Action triggers a new Event Cause of type "Alarm" with the specified Alarm ID. This can then be used as the Cause for other Event Rules. Since the Live Event Stream uses the "source" parameter of an event as the default camera ID associated with the event, it is often sensible to choose an Alarm number that matches the ID of any relevant camera.

Boost

This Action causes the recording framerate to increase to any pre-configured Boost rate on the selected camera and recording track. These rates are configured in the Camera Groups setup screen.

Client Action

This Action allows any pre-configured Client Actions to be triggered (see section 6.13 – Client Actions). This can be used to trigger pop-up of cameras or saved layouts for example.

The Text field can be used to pass parameters to the Client Action.

[CopyTrack]

Allows a CopyTrack command to be issued, typically for backing up video on event or schedule. Place the CopyTrack parameters in the text field. See CopyTrack documentation for details.

DoorAccess

DoorLock

DoorUnlock

These are only visible if a door controller has been added to the system. They perform standard door actions, see documentation on the door controller. The Access action usually opens the door to permit access and then locks it again after it has closed.

Email a Video Clip

This Action is used to send a video clip via email. Some steps are required before this can be used:

- An SMTP server should be properly configured (see section 6.2.6 – Email).
- One or more potential recipients should be configured (see section 6.2.6 – Email).
- A user called "localbackup" should be added (see section 6.1 – Users). It is not necessary to set a password for this user, however it needs at least the following permissions: "Playback", "Export", "Transcoding/exporting".

The various fields which can be configured are:

Recipients
: The "To" address for the email.

Channel
: The Camera (or Audio channel) from which to perform the export.

Track
: The recording track from which to perform the export.

Subject
: The subject for the email.

Message
: The message for the email.

Pre–Event
: The duration in seconds from before the time of the event from which the export should start.

Post–Event
: The duration in seconds after the event for which the export should continue.

Container
: The type of video file to create.

Note that each time this Action is triggered, the software will have to perform a transcoded export. This is a fairly intensive operation so it's important not to configure the system such that it's likely to have to perform a large number of them simultaneously as it might affect server performance.

Configuring a "Post–Event" time adds a delay to the operation. For example if the "Post–Event" time is set to 30 seconds, the system will need to wait for 30 seconds after the event for the recordings

to be made, before they can be exported and attached to the email.

Email Config

This Action is used to send a copy of the system configuration file via email. Some steps are required before this can be used:

- An SMTP server should be properly configured (see section 6.2.6 – Email).
- One or more potential recipients should be configured (see section 6.2.6 – Email).

The recipients of the email can be selected and the email Subject field can be specified.

Force Failover

This Action is only available if Failover is configured. It causes the current server to be put into a "failure state" meaning that any available standby server will take over.

Notify

This Action can be used to send a message to specially configured client PCs. See section 6.15 – Notification Target.

Output

This Action triggers a digital output. The output can be on:

- IP Cameras
- Configured I/O Devices (see section 6.2.11 – I/O Devices).

The parameters to select are the device (either Camera or I/O Device), and the Output number on that device.

Play Sound

The server can play a sound file (stored on the server) through a networked audio output device that has been configured as a Talkback channel (e.g. IP camera audio output, or server motherboard audio output).

To configure, select the Talkback device that you want to use, and the audio file to play. New audio files can be uploaded using the File Manager (see section 3.26 – File Manager).

PTZ Preset

This Action moves the specified PTZ camera to the specified PTZ Preset number.

PTZ Tour

This Action starts a PTZ Tour with the tour number.

Record

This Action triggers recording on the specified Camera and Recording Track. Note that recording is normally continuous so for this event to work, the relevant camera and track should have its Recording Mode set to "Event" or "Normal + Event". See section 6.3.2 – Camera Group Settings.

Record Metadata

This is used to trigger recording of input data to the metadata track of the selected camera. Normally this is required when configuring integration modules and instructions will be provided with the integration module.

Send Email

This Action is used to send a plain text email. Some steps are required before this can be used:

- An SMTP server should be properly configured (see section 6.2.6 – Email).

- One or more potential recipients should be configured (see section 6.2.6 – Email).

The configurable parameters for this Action are:

Recipients
: The "To" address for the email.

Message
: The message for the email.

Spot Monitor
: This Action causes the specified Spot Monitor to show the specified camera. It is also possible to specify whether the High or Low resolution stream should be used, where available.

  This action can be used for Spot Monitor outputs on analogue capture cards, or Virtual Spot Monitors (see section 9.10 – Configuring Virtual Spot Monitors).

TextC
: This Action replaces the Camera Name used in the video display subtitles with the configured text.

TextS
: This Action replaces the Server Name used in the video display subtitles with the configured text.

Configuring Complex Events

As an example, imagine that a digital output is connected to a gate and it is required that an operator can open the gate manually. A Manual Trigger can be used in this case.

Also imagine that we need to allow a digital input from a camera to also trigger the gate.

So we need an OR condition: open the gate if either one OR the other is true.

In this case a rule can be configured as follows:

Rule Name Open Gate

Causes Input 1.1 (Camera 1 Input 1) OR Manual Trigger 1

Actions Output 1.1 (Camera 1 Output 1)

When configured like this the Events panel on the main screen will show an entry for "Open Gate" which will trigger the "Manual Trigger 1" Cause.

6.13 Client Actions

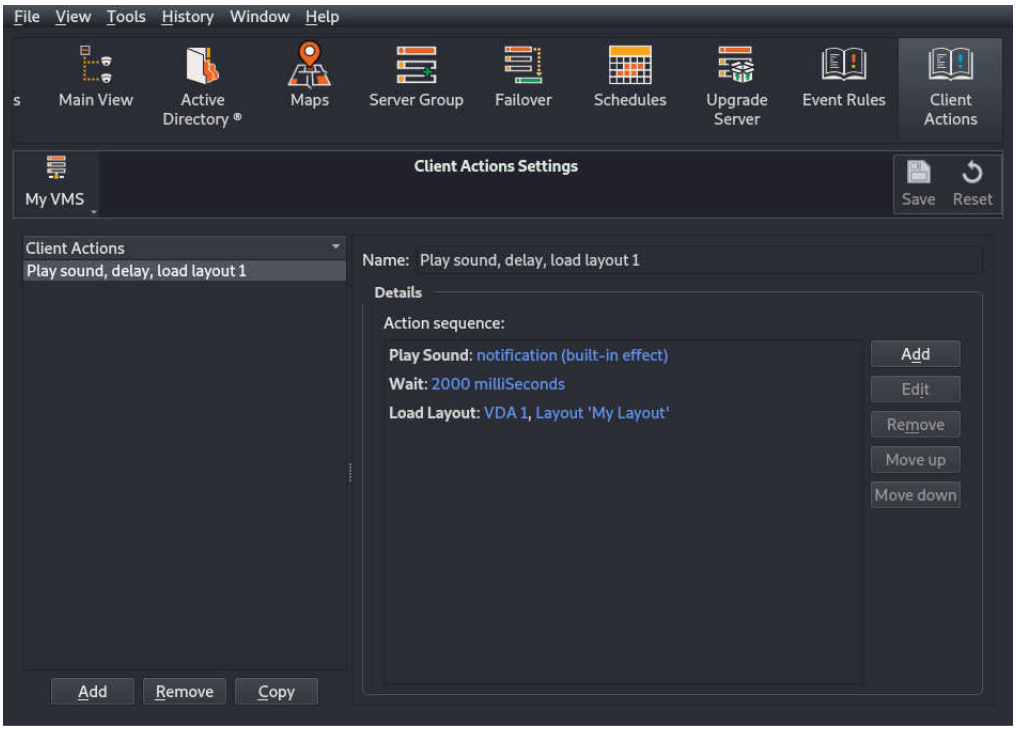
Note: The settings in this page apply to all servers in the server group.

The Client Actions menu can be reached by the menu path Tools → Setup → Client Actions.

This menu allows the configuration of automated behaviour of the WaveView software based upon server events. For example, it may be desirable for a saved layout of cameras to be displayed when a digital input is triggered. The overall rule for this is configured in the Event Rules setup screen (see section 6.12 – Event Rules), however the specific behaviour of the WaveView client software is configured in this Client Actions setup screen.

The top section of the screen allows the specifics of the ***Client Action*** to be configured.

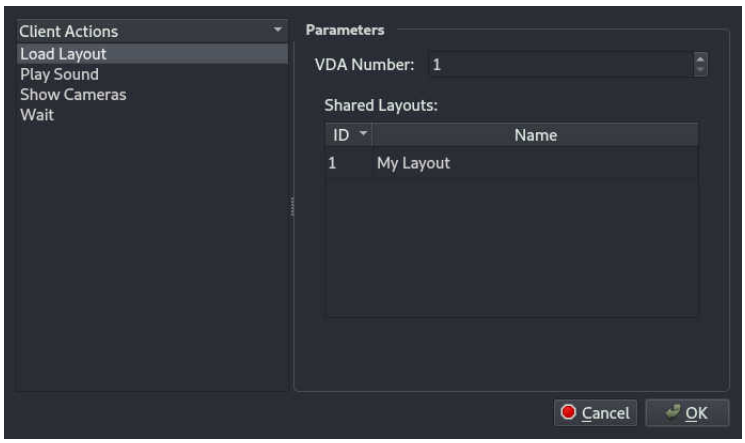
The bottom of the screen shows ***Conditions*** to which the action is limited. Currently the only condition is ***Users***. This is a comma–separated list of usernames for whom this action will be taken. If the currently logged in user is not in the list and this Client Action is triggered, it will be ignored and no action taken. For example a valid list would be "install,john,andrew". If a user called "roger" is logged in and the client action is triggered, nothing will happen.



Each Client Action is a series of steps which will be taken in sequence. A name can be associated so that it can be selected in the Event Rules screen when programming rules.

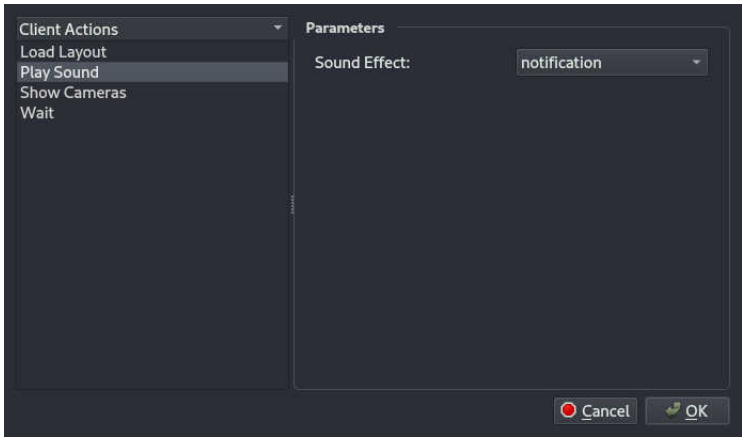
The available actions are...

Load Layout



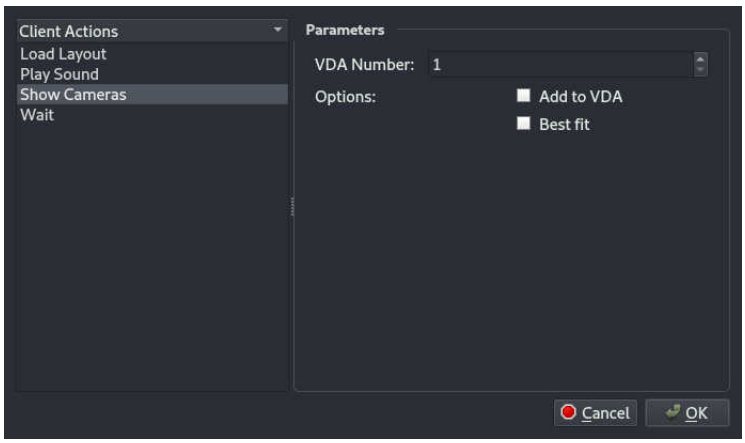
Loads a saved layout onto the selected VDA (Video Display Area). If the desired VDA is not available, it will attempt to use VDA 1. Note that only shared layouts can be selected.

Play Sound



Plays the selected sound file. The sounds listed are built-in to the WaveView software.

Show Cameras



Causes one or more associated cameras to be displayed on the selected VDA (Video Display Area). If the desired VDA is not available, it will attempt to use VDA 1.

There are 2 modes possible:

Add to VDA
: The camera(s) will be added to any free slots in the current Video Display Area.

Best fit
: Any existing cameras on the VDA are cleared, the grid is set to the optimal dimensions for the number of cameras to be shown, then the cameras are displayed.

Remove with event 'Off'
: For events that are of type 'On/Off' (as opposed to instantaneous 'Pulse' event types), the camera will be added to the VDA when the 'On' occurs, and removed when the 'Off' occurs.

There is also an option to "Remove with event 'Off'". This causes the cameras triggered for this event to be removed when the event cause switches to an 'Off' state. For example, the camera are added when Motion starts, and removed when Motion no longer occurs. For 'Pulse' type events, those that represent something instantaneous, there is no 'Off' part to the event, so the cameras will remain.

The associated camera, or cameras, can be provided in several ways. They are attempted to be used in the following priority order. If any is absent, the next is attempted...

The Text field of the Event Rule Action
: When configuring the Event Rule (in the Event Rules setup screen), the "Client Action" action has a Text field. This field can be used to specify the associated cameras.

The event's CAMERA field
: This is not user configurable. It is inserted into events which are provided by integration modules. The integration module inserts the associated cameras.

The Event Source
: The event source is the parameter associated with the Event Cause. For example if the event rule has a "cause" of "Motion on Camera 3", the event source is 3. Therefore camera 3 will be shown by this client action. This also applies when the event source is not a camera. For example if "Input 2" is triggered, the event source will be 2 and so camera 2 is shown.

As described above, it is possible to put an entry in the Text field of the event action when configuring an event rule, which determines which camera(s) to show.

The Text field should begin with a forward slash (/). Then it can have a comma–separated list of camera IDs with "modifiers" before each one.

Note that the 'Show Cameras' action can only show cameras connected to the server from which the Event Cause was received. If it is required to show cameras from multiple servers, consider using the 'Load Layout' action. The disadvantage of the 'Load Layout' action is that it does not have the playback functionality of the 'Show Cameras' action (described below). If cameras from different servers ***and*** playback functionality is required, the 'Show Cameras' action may be suitable, but the 'Best fit' option will not work. This is because each server will send an event with a list of cameras, causing the layout to be cleared each time and only the cameras from that server to be put in the layout. The 'Add to VDA' option should work well as long as the current layout is set to one with enough slots for all the cameras that might need to be displayed.

The modifiers are:

p (Default)
: Shows the camera in Playback mode using the time that the event was triggered.

l
: Shows the camera in Live mode

f
: Pauses the camera at the time of the event, searching forwards if there is a gap in recordings at the time of the event.

b
: Pauses the camera at the time of the event, searching backwards if there is a gap in recordings at the time of the event.

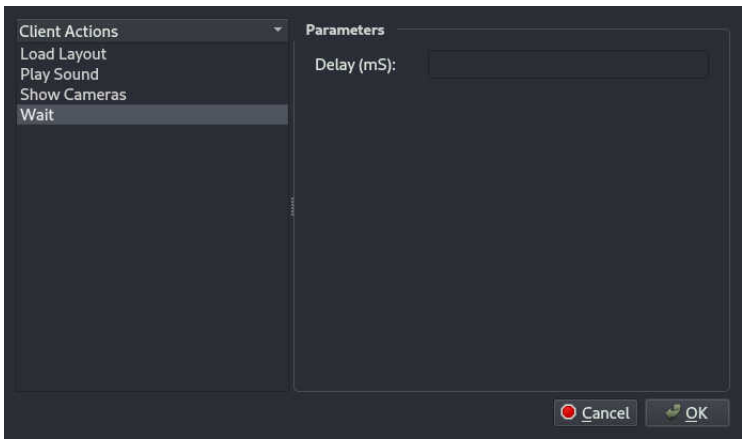
Text Field Examples:

/1,2
: Shows cameras 1 and 2. By default these will Play from the time that the event was triggered.

/l1,l2,l3
: Shows cameras 1, 2 and 3, all in Live mode.

/l3,b4,p5
: Shows camera 1 in Live mode, camera 4 paused, and camera 5 playing.

Wait



Adds a delay into the series of steps for this action. The duration is in milliseconds and can be from zero to 10 minutes (600,000 milliseconds).

6.14 Analytics

Note: The settings in this page are independent for each server in the server group.

The Analytics setup screen can be reached by the menu path *Tools* → *Setup* → *Analytics*.

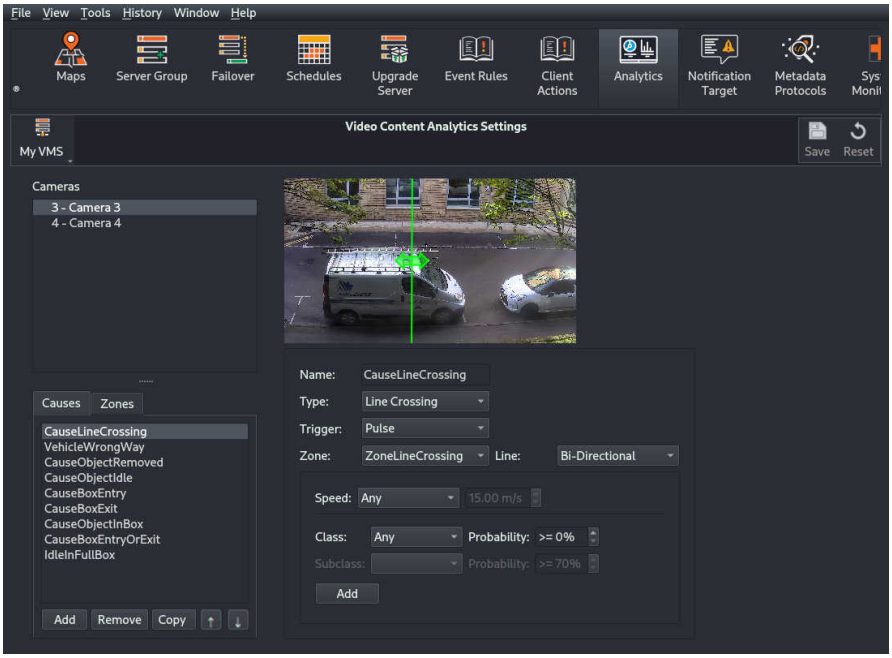
This screen allows the configuration of custom 'Event Causes' specific to video analytics. These 'Event Causes' are then visible in the live event stream when they occur, and they can be used to trigger Event Rules.

Note that this facility is only available for supported cameras and devices. This is explained in more detail in section 9.9 – Configuring Video Analytics.

The screen consists of three main areas:

- The camera selection list
- The Cause and Zone selection list
- The editing area

Configuring Causes



To begin editing, select a camera, then click the *Add* button under the Cause selection list. If the camera does not support analytics, the Add button will be disabled.

In the editing area, give the Cause a name.

The following characters are allowed in Event Cause names:

- 0–9
- A–Z
- a–z

- /
- _
- Space (" ")
- Any unicode character greater than 0x80 except unicode characters 0x2423 and 0x2080 to 0x2089.

Therefore any Unicode (or ASCII) character under 0x80 which is not in the permitted list above, is not permitted. This includes certain punctuation characters such as these: !"#$%&'()*+,–{|}

Next, choose the type of analytics event to match. The options are:

Object Properties
: Matches object properties such as object class, the probability of that object class, and the object speed.

Line Crossing
: Matches objects crossing in a line.

Box Entry
: Matches objects entering a box.

Box Exit
: Matches objects leaving a box.

Box Entry or Exit
: Matches objects entering or leaving a box.

Object In Box
: Matches for the duration of an object being in a box.

Object Removed
: Matches when an object is removed from the scene or box.

Object Idle
: Matches when an object becomes stationary within a scene or box.

Crowd
: Matches when a certain number of objects are within a scene or box.

Next, it is necessary to choose a *'Trigger'* type, either *'Pulse'* or *'On/Off'*. *'Pulse'* means the event will be considered instantaneous and is therefore best suited for *Line Crossing*, *Box Entry*, *Box Entry or Exit*, *Object Removed*, and *Object Idle*. *'On/Off'* means the event has a duration and so is best suited for *Object Properties*, *Object In Box*, and *Crowd*.

Many of the analytics types require a zone of some kind, either a box or line. If that's the case for the selected type and some zones already exist, one will be selected. Otherwise a button will be presented which allows jumping straight to the zone editing part of the screen.

Staying on the subject of creating the Event Cause, various parameters will be presented for the current analytics type. Note that *Object Properties* are available for matching their own, or as an addition to other analytics match types.

Object Properties matches allow matching on the object speed being greater than or less than the specified value. The units for speed can be selected from *m/s (metres per second)*, *mph (miles per hour)*, or *kph (kilometres per hour)*. Alternatively, if 'Any' is selected, the speed is not checked in the search.

It is also possible to match on the object 'class' and, optionally, 'subclass'. The availability of the subclass option is dependent on the source of the analytics data for the current camera. For both class and sub-class matching, it is possible to provide a minimum probability for the object matching that class.

If supported by the selected camera, it is also possible to search by ***Segment Colour***. A segment is a part of the object, e.g. Torso, Lower. Either select a colour, or select the checkerboard to indicate no colour. For each segment, a probability of that colour can be specified.

Line Crossing matches require a Line type zone to be specified, along with a direction.

Box Entry, ***Box Exit***, ***Box Entry or Exit***, and ***Object In Box*** matches require a zone of type Polygon.

Object Removed, ***Object Idle***, and ***Crowd*** matches can have a Polygon zone optionally applied, though the default is ***'Entire Scene'***.

Crowd matches have a ***'Count'*** parameter, which is the minimum number of objects within the scene or zone required to trigger the match.

Configuring Zones

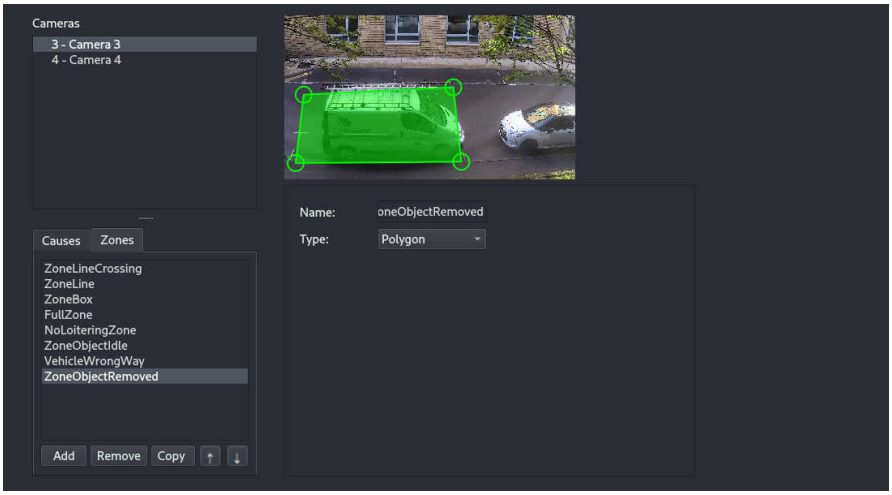
Each zone needs a name and a type. The name can contain almost any character. The type is either ***'Line'*** or ***'Polygon'***.

When editing a Line, the line itself can be edited as follows:

- Click and drag a circular end-point of the line to move that point
- Click and drag on the line to move the whole line
- Double click the arrow to change the direction of the arrow.

When editing a Polygon, the shape can be edited as follows:

- Click and drag a circular end-point of the line to move that point
- Double-click on an edge of the box to add another point
- Double-click a circular end-point to remove it
- Click within the box and drag to move the whole box



6.15 Notification Target

Note: The settings in this page are independent for each server in the server group.

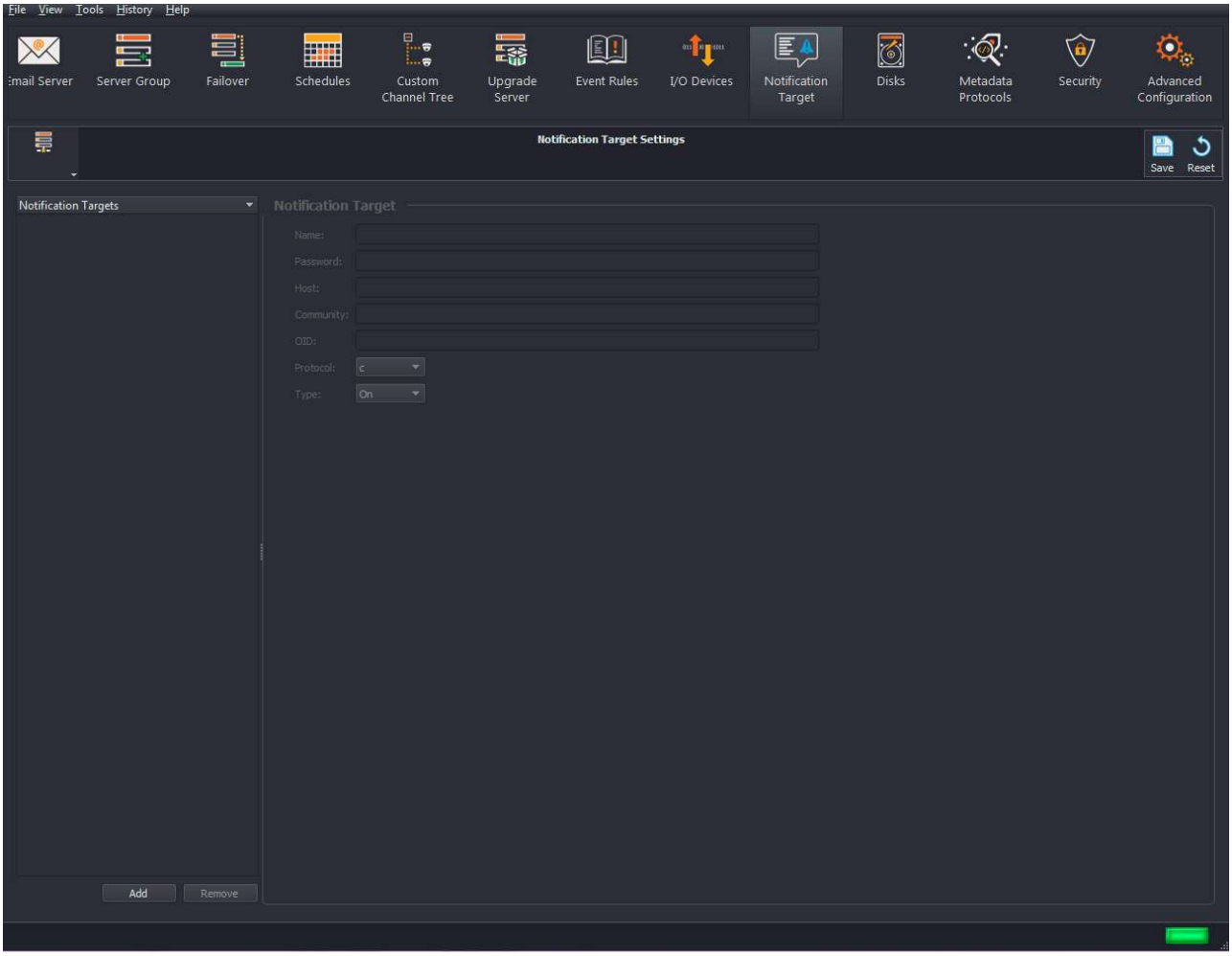


Figure 6.39: Notification Target screen

The Wavestore server can be configured to send message notifications, for events such a Video Loss, to an external devices (such as a PC running a Python script) using the Event Rules menu (see section 6.12 – Event Rules).

The details of the device(s) that are to receive notification must first be configured in the Notification Target menu.

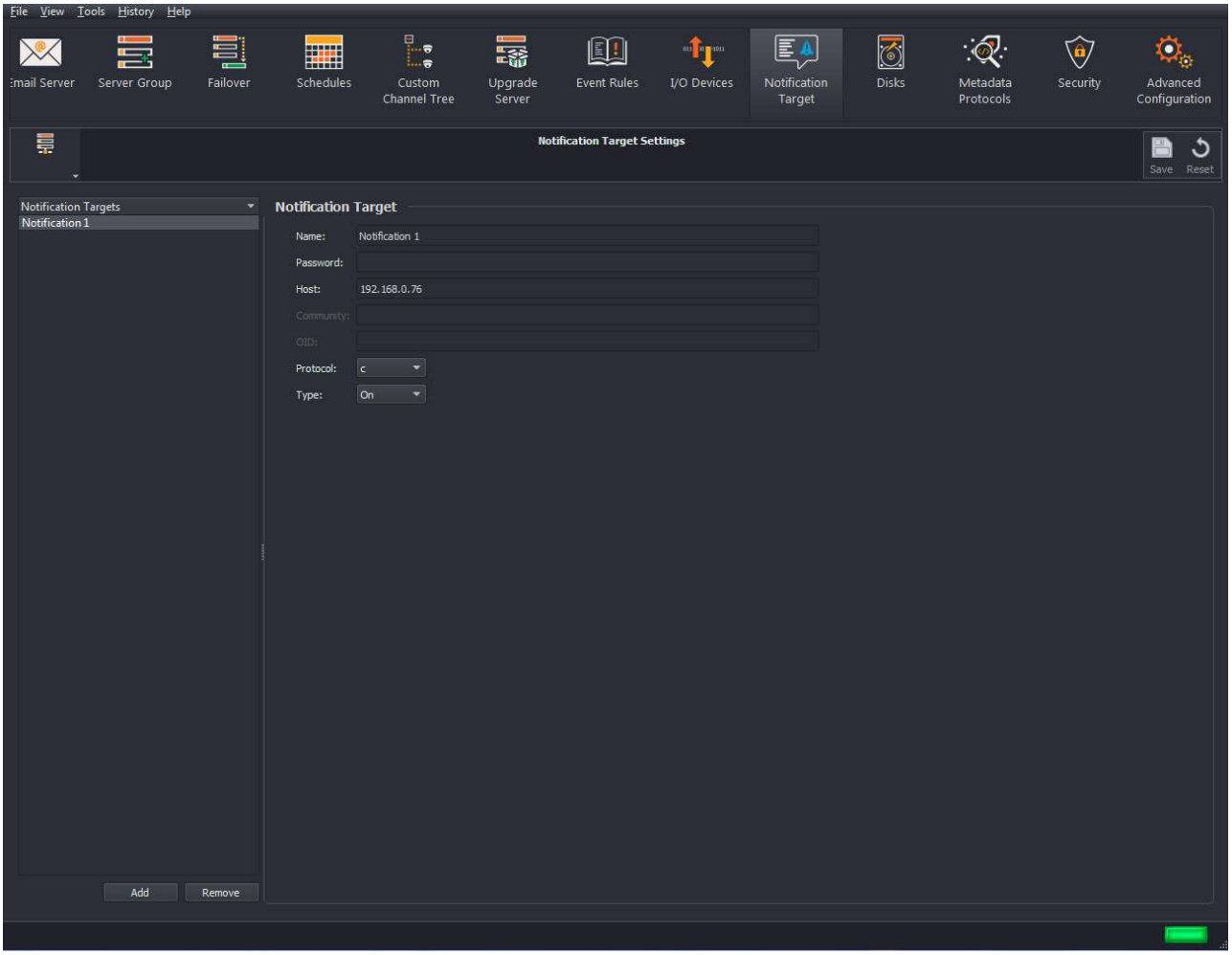


Figure 6.40: Configuration of Notification Target screen

For further information regarding message format/protocol see the knowledge base at kb.wavestore.com.

6.16 Metadata Protocols

Note: The settings in this page apply to all servers in the server group.

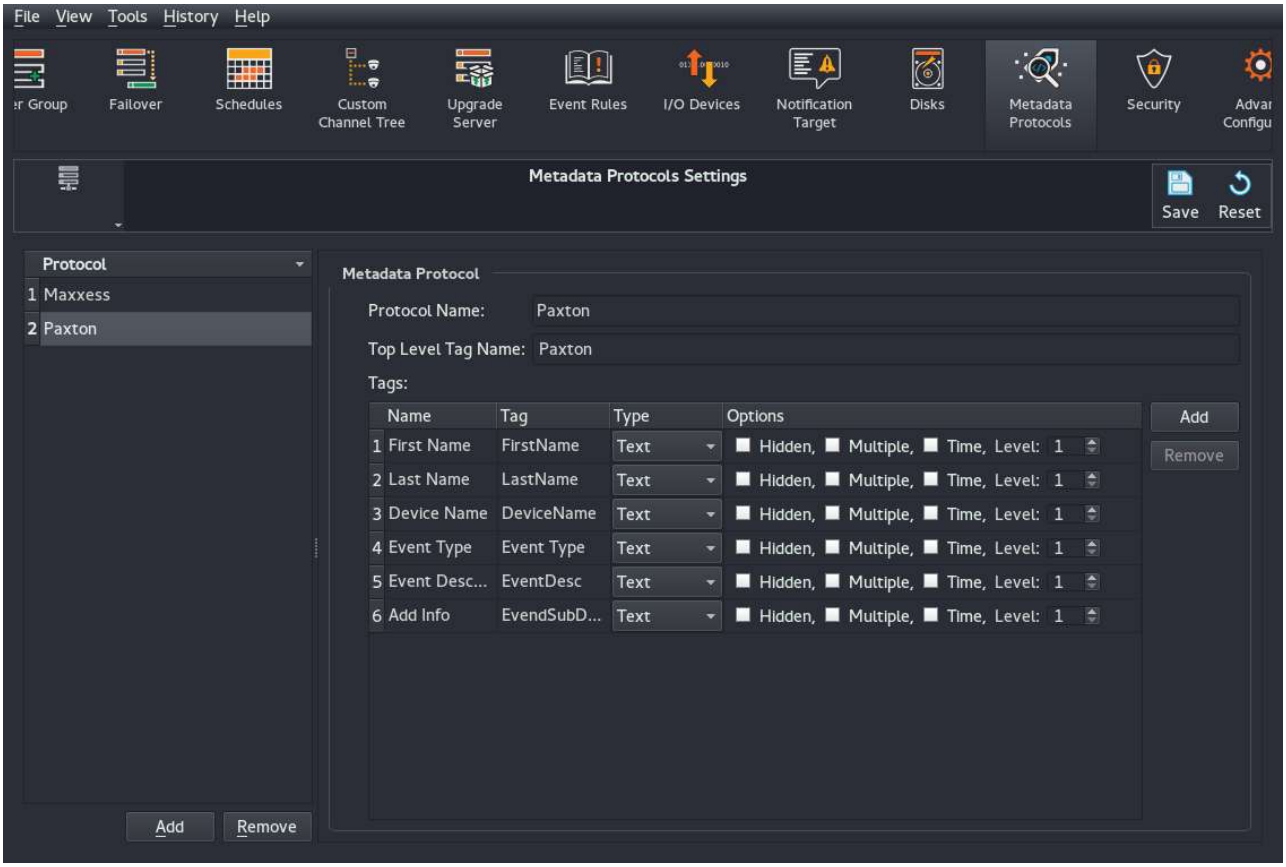


Figure 6.41: Metadata Protocols Setup Screen

The Metadata Protocols Setup Screen is used to configure information about tags which might be captured as metadata when using an integration module.

It is generally not necessary to configure anything in here directly. The settings are made automatically when an integration module is installed. For example, the screenshot above shows the setup screen after the Maxxess and Paxton integration modules have been installed.

Any changes to this configuration might cause issues with the integration modules, and so should only be performed in special cases under the guidance of Wavestore technical staff.

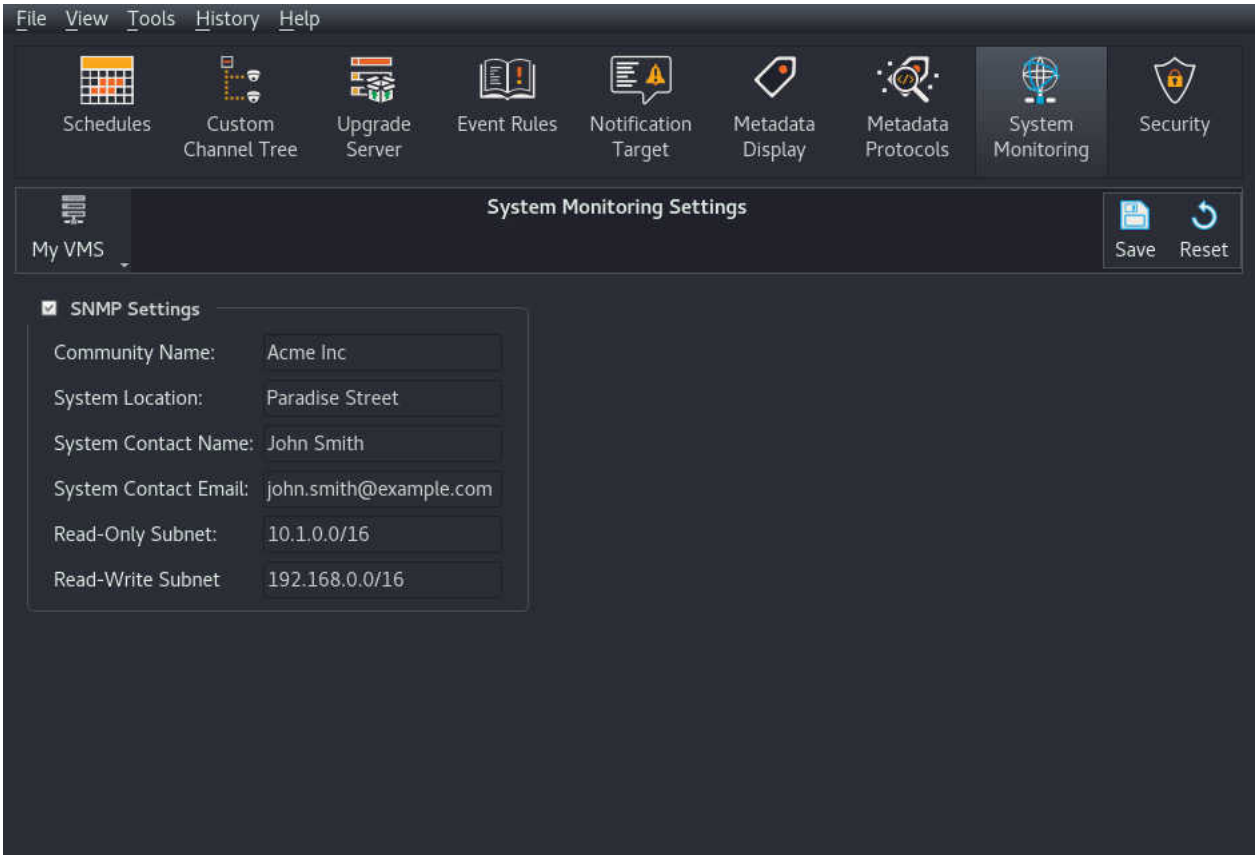
6.17 System Monitoring

Note: The settings in this page apply to all servers in the server group.

The System Monitoring page allows configuring the server group settings relating to:

- SNMP (Simple Network Management Protocol)
- Health Monitor – for cloud–based system monitoring

6.17.1 SNMP



The settings provided here are fairly standard for SNMP but an explanation is below for completeness.

Community : The "Community" string is the password use to access the information over SNMP. This is required.

System Location :

System Contact Name :

System Contact Email : These three fields are descriptive only. They can be useful to a user of the SNMP information (a network engineer, for example) to know what the machine is and where it is located.

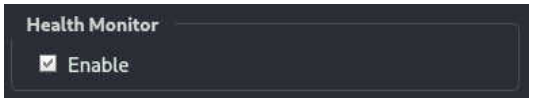
Read–Only Subnet : This field defines the network subnet from which read–only operations can be performed. The subnet is expressed in CIDR notation, e.g. "192.168.0.0/16". Restricting this to a

subnet within the company or a single management station will enhance security.

Read-Write Subnet : It is not recommended to set a Read/Write subnet as it will allow alterations to the Wavestore settings. This field can be left blank to disable this feature.

Once the settings have been made, click on 'Save' to confirm the changes that you have made.

6.17.2 Health Monitor



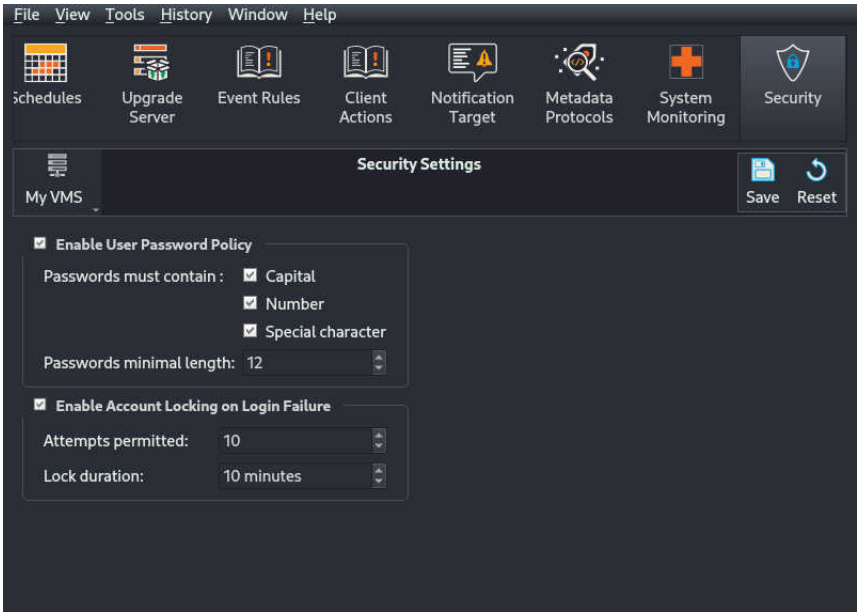
If enabled, the Wavestore will connect to a cloud service to upload system monitoring information.

The data uploaded includes information about the status of the server itself and the registered cameras. No personal information is included in the data. The data is retained for up to 3 months.

6.18 Security

Note: The settings in this page apply to all servers in the server group.

This setup screen allows configuration of various security related settings.



Enable User Password Policy

If enabled, a password policy will be enforced based on the other settings in this screen. Otherwise any password other than blank can be used.

Capital If enabled, any new password must contain at least one capital letter.

Number If enabled, any new password must contain at least one number.

Special character If enabled, any new password must contain at least one special character (not a letter or number).

Passwords minimal length The minimum length of any new password.

These settings cause a password policy to be applied for all users in the server group. Note that if a password policy is applied, it only affects subsequently changed passwords. Any users whose passwords do not conform to the new policy will not automatically be forced to change their password. However this can be done by setting the "Force user to change password on next login" for each user in the Users Setup Screen (see see section 6.1 – Users for more details).

Enable Account Locking on Login Failure

Attempts permitted This determines the number of failed logins before the user's account will be locked.

Lock duration This determines the duration, in minutes, of an account lockout when the maximum number attempts permitted has been reached.

This feature can also be disabled completely by unchecking the checkbox.

7 Maintenance Menu

The Maintenance Menu is a system on the Wavestore server which can be used to rescue or configure the system when the GUI is not available.

To access this menu, press CTRL + ALT + F2. This should present a command prompt. At the prompt, login as user "maint". You will then be prompted to "Enter Install Password". This can be the password of any install–level user.

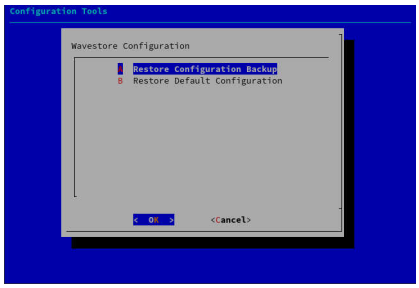
Note that to return the normal GUI, you can press CTRL + ALT + F1. In the rare occurrence that this doesn't work, try the other Fn keys in combination with CTRL + ALT.

If your login is correct you will be presented with the Maintenance Menu.

The menus are navigated using the keyboard. Normally this means the arrow keys to move Up, Down, Left and Right. The Enter key can be used to accept an option, Escape to cancel. The Tab key can be used to highlight different buttons.

Configuration Tools

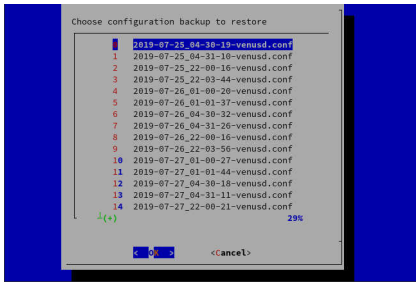
The Configuration Tools menu can be used to restore configuration backups or return to the factory default configuration.



Restore Configuration Backup

This option allows the user to restore the system to an earlier backed up configuration. Backups automatically occur weekly and also in some exceptional circumstances such as when upgrading to a newer version.

When this option is selected, a list of configuration backups is presented.



The filenames represent the dates and times of the backups, for example "2019-06-30_04-30-54-venusd.conf" is a backup from 30th June 2019 at 04:30am.

When the desired backup is selected, the user is asked for confirmation before the configuration is loaded. Upon loading the configuration the server process will automatically restart (not reboot).

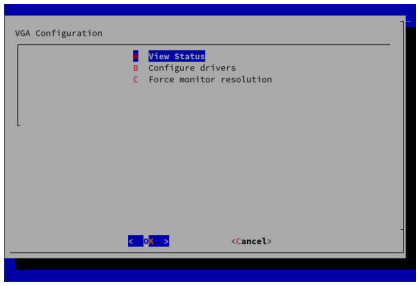
Restore Default Configuration

This allows resetting the system to its factory default. Note that when this operation is performed a backup of the existing configuration is automatically made.

When selected, the user is asked for confirmation of the operation. If confirmed, the user is asked if the existing licence should be preserved.

Once the operation is complete, the server process will automatically restart (not reboot).

VGA Configuration



This menu is used to configure the graphics drivers for the graphical display on the Wavestore server.

View Status

This option shows information about the current display adapter and the graphics driver currently in use.

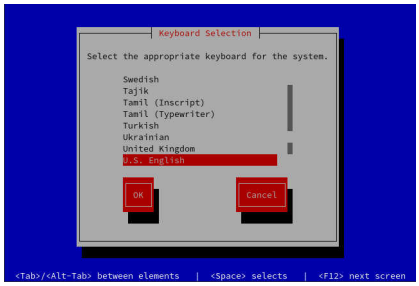
Configure drivers

This option allows a specific graphics driver to be installed or removed. It is vital to install the correct driver for the display adapter in the system. The "View Status" option can be used to check this.

Force monitor resolution

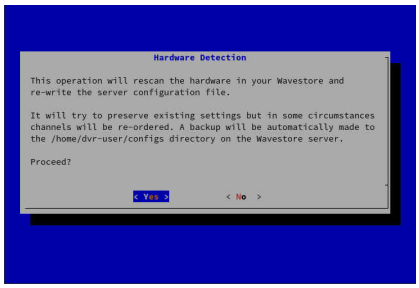
By default, the optimum display resolution is automatically detected. However this option allows a specific resolution to be set. Once set, these settings can be applied by switching back to the graphical desktop (CTRL + F1) and restarting the graphical display with CTRL + ALT + BACKSPACE.

Configure keyboard



This option allows the user to configure the keyboard layout for the keyboard connected to the Wavestore server. A reboot is required after selecting the desired keyboard layout for it to take effect.

Interactive Hardware Detection



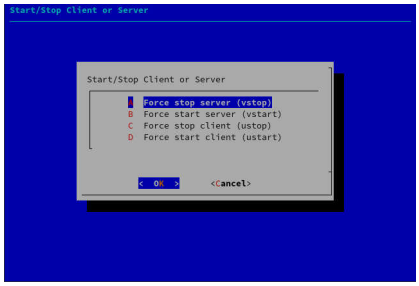
The Hardware Detection mechanism is used to detect "capture devices" available on the server and add them to the server's configuration so that they are available for use. An example of a "capture device" is an analogue capture card, or the onboard audio device of the motherboard.

Normally there is no need to run this process manually. It occurs automatically on first boot, and whenever the system detects that a relevant new piece of hardware has been connected. That would be either an audio device, or a PCI device.

One potential use of running this manually is if there are devices automatically detected which you do not want to be available for use. For example if the onboard audio device is detected, its channels will be available in the WaveView Cameras setup screen. This causes certain channel numbers to be reserved,

which may not be desired. By running this detection process you can choose to ***not*** include the device. This configuration will remain unless another relevant hardware device is added or removed, at which point the automatic detection will run on boot.

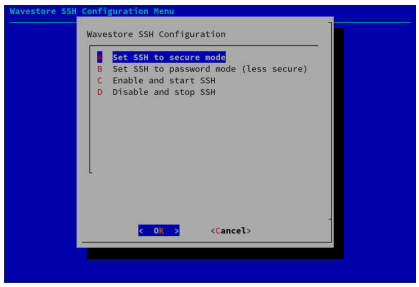
Start/Stop Client or Server



This option allows either the server or client to be stopped or started. By default both are started.

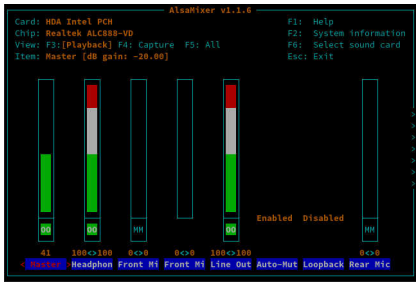
It is important to note that the process in question (server or client) will remain in the selected state upon reboot. So for example if you stop the server, it will not run on reboot until it is re-enabled in this menu. Be careful with this option because if you disable the server, you will not be able to log in remotely via WaveView.

SSH Tools



This menu allows configuring and starting/stopping the SSH service. This service can be used by Wavestore Global support staff to provide remote technical support, and will provide guidance on how to use this menu as required.

Audio Mixer

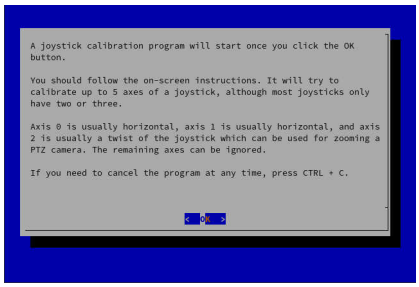


This option presents an audio mixer to allow configuring volume and mute/unmute status of audio inputs and outputs. This should not be used in normal operation, instead the options in the WaveView Cameras setup screen should be used instead. Any settings made here will potentially be lost on reboot.

Check installed software is same as DVD

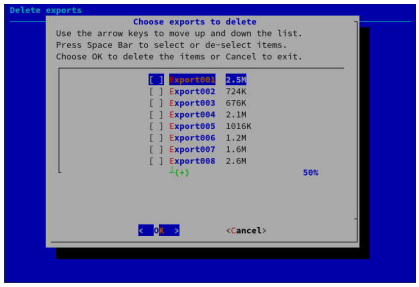
This option is used to compare if a installed system has the same files as an installation DVD. It is rare to need to use these options but it is left for legacy reasons.

Calibrate joystick



This option is used to calibrate a joystick so that its central point and extreme points correctly translate to PTZ speed. Simply follow the on-screen instructions to perform the calibration.

Delete selected exports



Since the Wavestore allows exports to be saved to the server, it is possible to completely fill the operating system disk. In some rare cases this may mean that it is not possible to start the UI, meaning that exports cannot be deleted to free up space.

This menu options presents a list of the exports on the system to allow them to be deleted, to free up disk space.

Write diagnostic disc

This option collates a variety of log files and configuration files, and allows them to be written to a USB device or directory so that they can be copied off.

By default these files are copied to the `/home/dvr-user` directory. On the Wavestore, it is possible to move the mouse to the top-left corner to open a menu which includes a file browser. This can then be used to copy the files to a USB memory stick.

IPMI Event Simulator

This menu option can be used to test alarms from servers which support IPMI (Intelligent Platform Management Interface). Simply select the sensor in question to turn it into an alarm state. Remember to turn it off again afterwards!

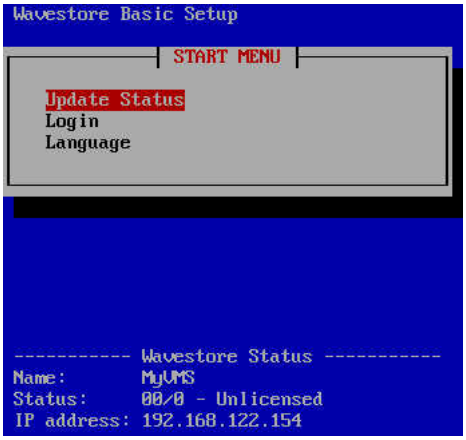
8 Other Utilities

8.1 Textual User Interface

The Wavestore text user interface (Wavestore–tui) client is a basic setup program designed for use on server machines which are not intended to run, or capable of running, the full WaveView client.

It allows basic initial setup operations (setting network address and machine name) to be performed on the Wavestore server itself, after which a WaveView client can connect in over the network and complete setup of cameras and view live and recorded footage.

The mode of operation without local WaveView but with Wavestore–tui is described as "Server Only" mode.



Choosing Wavestore–tui or WaveView during Install

When installing Wavestore using the normal menu options:

- If it's a Virtual Machine or server without appropriate graphics hardware, "Server Only" (Wavestore–tui) mode is selected automatically
- If doing an "unattended install", then WaveView is selected automatically
- Otherwise, a dialog box "Do you want to start WaveView" will appear, and Yes will run WaveView and No will run Wavestore–tui as the main setup client.

This is then permanent and will remain unchanged over reboot unless explicitly changed by a command (see "Switching to Server Only mode" below).

It is possible to switch between console windows:

- The main client, WaveView or Wavestore–tui, is available on Ctrl–Alt–F1
- The Wavestore–tui interface is always available on Ctrl–Alt–F2
- The system log is always available on Ctrl–Alt–F7

Operation

The Wavestore–tui basic setup client appears on the console (virtual console 1 or 2).

Initially it offers a Start Menu and shows some status information. Note that Status displayed is not automatically kept up to date, but any menu operation will update it.

Moving around the menus

- For choice menus, use Cursor Up and Down keys to highlight the desired option and use Enter to action it.
- For data entry forms, use Tab or Enter or cursor keys to switch fields, and the keyboard to type changes needed. Use Enter on the final field to log in. Use ESC to exit without entering data.

Start Menu

Update Status update the server status

Login offer a login screen

Language select the language to use for the this user interface

Use Cursor Up and Down keys to highlight the desired option and use Enter to action it.

Note that the status is displayed on this screen but will not update while waiting for a command. Selecting any option will cause the status to update.

Login Menu

Username username to log in, use ”install” initially

Password password to log in

Use Tab or Enter or Cursor keys to switch fields, and the keyboard to type changes needed. Use Enter on the final field to log in.

Once logged in, the Main Menu will be displayed.

Main Menu

- Logout
- Set IP address
- Set Name
- Restart
- Reboot
- Power off

Only basic operations which are needed on initial setup are offered, plus ones which you might want to do on a local console such as restart and power off.

Note that all menus (other than the Start Menu) will time out after 5 minutes and will then log out and return to the Start Menu. This prevents you accidentally leaving it logged in.

The most basic operation is to set the initial IP address. Setting the server name is also offered to allow it to be clearly identified. Additional setup operations and viewing of footage is not offered by this basic client. WaveView running on another machine (such as a desktop PC) should be used to access and continue setting up and using the Wavestore server.

Choose Network Interface

If ***Set IP address*** is selected, Wavestore-tui will prompt you to chose a network interface.

If no bond interface is available, you can set one up here, and all interfaces will automatically be set as slaves to the bond interface.

Set IP Address (bond0)

- Slave to
- IPv4 address
- IPv4 netmask
- IPv6 address
- Gateway
- DNS Server

If ***Set IP address*** is selected, after a network interface is chosen, this menu will be shown.

The ***Slave to*** setting is only applicable for interfaces which have a bond interface as slave, otherwise it is set to None.

Set IP addresses and netmask as required. Leave IPv6 address blank if using only IPv4. Set Gateway and DNS Server if desired.

As usual, Enter on the final field will save the entries. ESC will escape and leave without saving.

Set Server Name

- Name

This menu will allow initial naming of the server which might be useful to aid identification when logging in remotely. Enter a name and Enter to save. Note that this will restart the server.

Switching to Server Only mode

After install, it's possible to switch between modes.

To switch to server-only mode:

- Go to ***Tools*** → ***Execute Command*** and run "server-only".

This disables the local WaveView client and enables the local Wavestore–tui client for basic setup only.

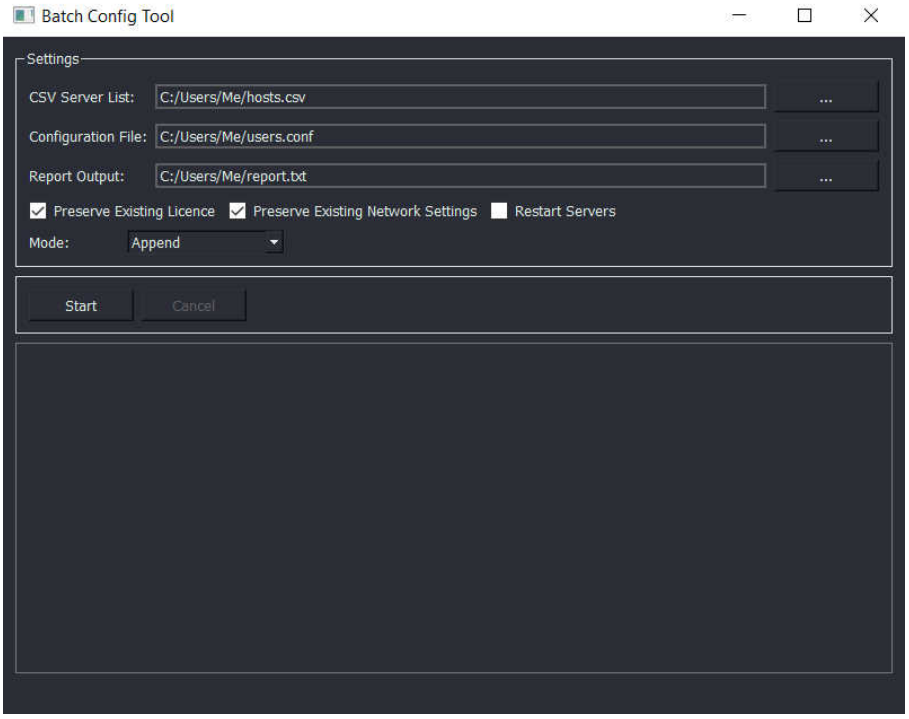
To switch to full WaveView mode:

- Go to ***Tools*** → ***Execute Command*** and run "server–and–client".

Both operations only work if the relevant packages are installed, which they are by default.

8.2 Batch Configuration Tool

Included within the WaveView installer is a tool called "Batch Configuration Tool". This tool can be used to push configuration sections or complete configuration files to a list of servers which is stored in a CSV (Comma Separated Values) file. This is useful when dealing with a large number of servers which are not in a Server Group.



The Batch Configuration Tool asks for 3 file locations, 2 of which are mandatory:

CSV Server List (required) This is the path to the csv file containing the list of servers, usernames, and passwords. The format is described in more detail below.

Configuration File (required) This is the file containing the configuration to be sent to the servers. This is described in more detail below.

Report Output This is an optional path to a file which will be written with a report of the operation. This is optional because the same report is output to the screen, but it can be useful to have the results automatically saved to a file.

There are also several more options available:

Preserve Existing Licence The Licence configured on the destination server will not be overwritten by the uploaded configuration file.

Preserve Existing Network Settings The network settings configured on the destination server will not be overwritten by the uploaded configuration file.

Restart Servers Each server will be restarted after the configuration is uploaded. Several settings require a server restart to take effect so this is often desirable.

Mode A choice of...

Append Any configuration sections uploaded will be appended to the existing configuration if they don't already exist, or they will replace the existing sections if they do. For example if you server has `[User_1]` and `[User_2]` sections, and your uploaded configuration has `[User_2]` and `[User_3]`, the `[User_2]` section on the server will be replaced and the `[User_3]` section will be appended.

Replace The entire configuration on the server will be replaced with the provided configuration.

CSV Server List format

The CSV file requires a list of headings followed by entries, one for each Wavestore server, as follows:

```
host,username,password
192.168.0.1,install,a
192.168.0.2,install,a
```

The first entry on each line is an IP address or hostname of a Wavestore server.

The second entry is a username which will be used to login. It is required that user be an "install"–level user, but it doesn't have to be the actual user named "install".

The final entry is the password to use for that server. Obviously the password is stored in the CSV file in plain text so it is important to be careful with distribution of this CSV file.

Configuration File format

The configuration file must be a plain text file with Line Feed line–endings. (Generally this means avoiding use of Notepad in Microsoft Windows, other text editors are usually fine).

In general, the configuration file of a server can be obtained using WaveView by navigating to *View > Setup > Server > Configuration*, and choosing *Save To File*.

The format of the configuration file is a lengthy and complex subject not covered by this document.

9 Common Setup Tasks And Concepts

9.1 Configuring IP Cameras

Wavestore servers are compatible with a wide range of IP cameras including but not limited to those conforming to the ONVIF Profile S standard.

It is generally recommended to use the Auto camera type to connect to cameras as this allows the greatest compatibility with various camera features and requires the least manual configuration. This should work for any ONVIF Profile S conformant device, however other mechanisms are available to stream video and perform other operations if the Auto mechanism doesn't perform as required for your device.

Configuring cameras with Auto mode is described in 9.1.1 – Configuring IP Cameras using Auto Mode.

Configuring cameras without Auto mode is described in 9.1.2 – Configuring IP Cameras without Auto Mode.

9.1.1 Configuring IP Cameras using Auto Mode

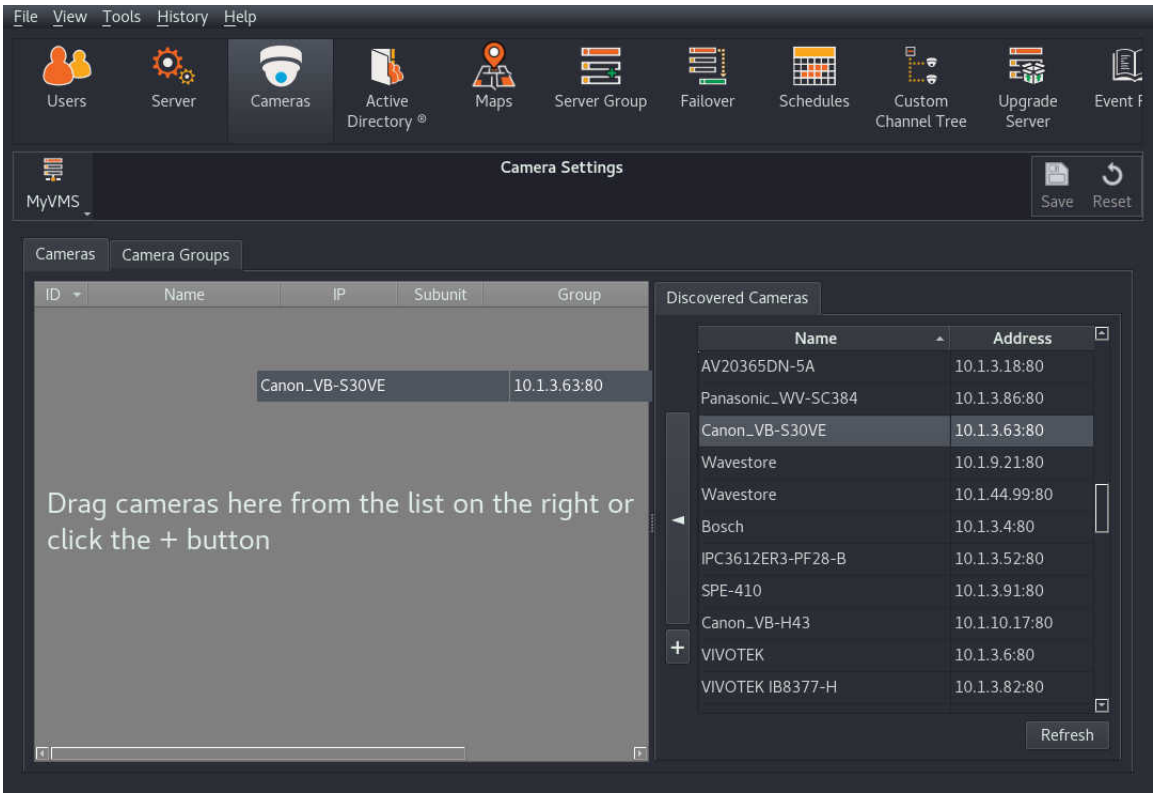
Wavestore servers are compatible with a wide range of IP cameras including but not limited to those conforming to the ONVIF Profile S standard.

It is generally recommended to use the Auto camera type to connect to cameras as this allows the greatest compatibility with various camera features and requires the least manual configuration. This should work for any ONVIF Profile S conformant device, however other mechanisms are available to stream video and perform other operations if the Auto mechanism doesn't perform as required for your device.

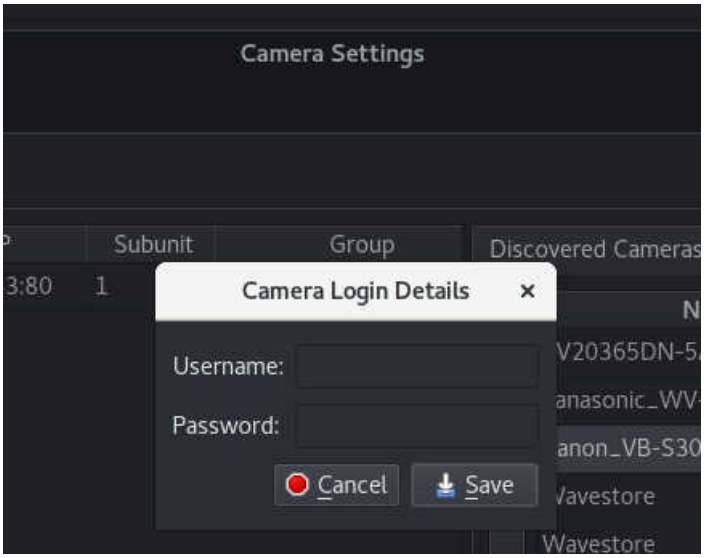
IP cameras are configured in the Cameras Setup screen which can be accessed in WaveView via the *View* → *Setup* → *Cameras* menu.

Upon entering the Cameras Setup screen, a discovery option is performed and a list of discovered cameras is provided on the right of the screen.

To add a camera, simply drag and drop it from the right to the left. If the device is not listed, click the plus button to add a new column on the left, then enter its IP address.



When a camera is added, it will either be added to an existing *Camera Group* if one exists, or a new group will be created. If a new group is created then a prompt for the camera's username and password is displayed.



Once this has been provided, for most cameras it should be sufficient to simply Save the changes. By default:

- Only the video stream is requested.
- The video stream is assigned to the default disk and set to record continuously for a maximum of 31 days (this recording duration is not guaranteed and depends on disk space available).
- The video stream is set to the optimal codec available from the device with H.265 as first preference, followed by H.264, then JPEG. If a specific codec is desired it must be manually selected under 'Encoding'.
- The audio stream, if enabled, is set to the optimal codec available from the device with AAC as first preference, followed by G.711. If a specific codec is desired it must be manually selected under 'Audio Encoding'.
- The framerate and resolution are set to the maximum available from the camera but are configurable.
- PTZ is enabled if supported by the camera.
- The maximum bitrate (bandwidth used) by the camera is set to 4000 kbps (kilobits per second).

Many different options can be enabled and these are described in detail in 6.3 – Cameras.

To enable audio input from the camera, simply tick the ***Audio*** checkbox. Similarly to enable Talkback (audio output from the camera – sometimes called "Backchannel"), simply tick the ***Talkback*** checkbox.

A secondary video stream can be enabled simply by ticking the ***Stream 2*** checkbox and specifying any desired settings.

Note that in all cases, the Wavestore will request the desired setting from the camera but if the camera cannot provide the precise setting, it will choose the closest match.

9.1.2 Configuring IP Cameras without Auto Mode

Whilst the ***Auto*** mode provided by Wavestore should work for the vast majority of modern IP cameras, there are other mechanisms available to connect to devices in case they are required.

ONVIF
: Although the ***Auto*** mode will often use ONVIF, this mode can be forced by selecting ***ONVIF*** mode. Also, ***ONVIF*** mode allows you to select a ***Profile*** (collection of settings) which has been configured on the camera rather than relying on Wavestore to push the settings to the camera.

ONVIF-Multicast
: Used to force the capture of a multicast stream from an ONVIF camera. Note that IPv6 is not supported for multicast.

RTSP
: Allows basic streaming using the RTSP protocol.

HTTP
: Allows basic streaming using the HTTP protocol.

MxPEG
: Used to pull the MxPEG video format from Mobotix cameras.

Ampleye
: Used to efficiently stream JPEG2000 video from Ampleye cameras.

9.1.2.1 Configuring IP Cameras in ONVIF Mode

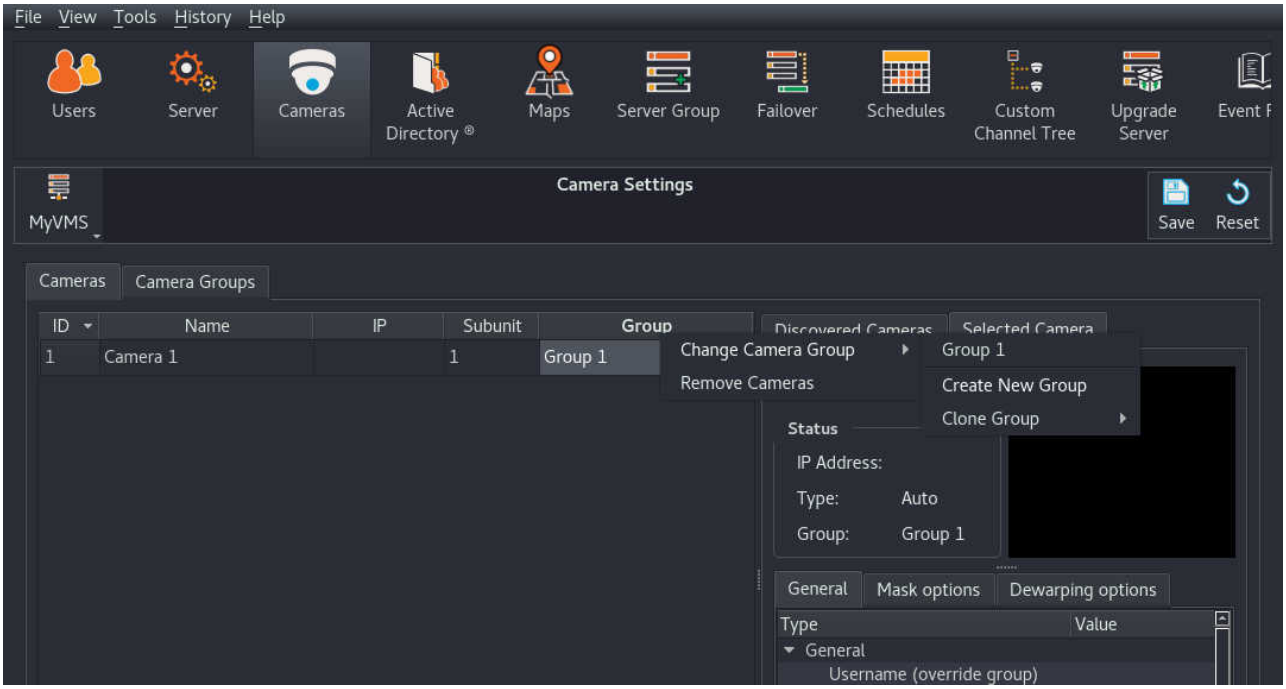
When using ONVIF cameras there are generally two modes of operation which are dictated by whether the "Auto-configure Camera Streams" option is selected.

If the option is enabled then the camera settings are made within the WaveView setup screens and the Wavestore server will push the settings to the camera. This is the recommended mode of operation.

If the option is disabled, it is necessary to use the camera's own setup facilities to configure one or more "profiles", where a "profile" is a collection of settings. The Wavestore is then configured to use a particular camera profile.

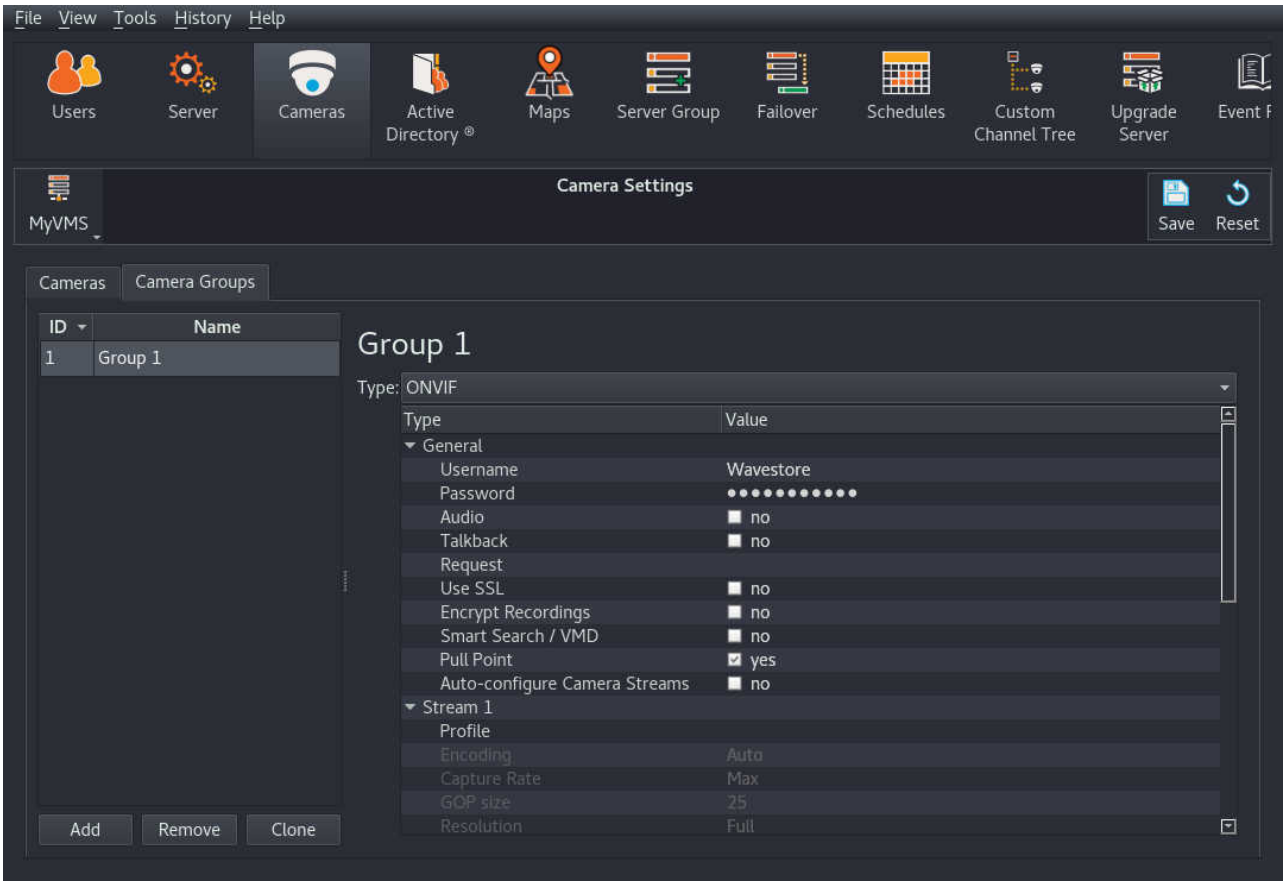
The first step of configuring an ONVIF camera is to add it to the Wavestore. This can be done by discovering the camera on the network or by adding it manually. The former is the easier and recommended way but there are some circumstances where the discovery process won't work, such as when the camera is on a different network segment.

To add the camera manually click the + button. The camera will be added to an existing ***Camera Group*** if one exists, otherwise a new group is created and a prompt for the username and password is provided. If the camera has been added to an existing group which isn't already set up for ***ONVIF*** mode, right-click the ***Group*** column for the camera and choose "Change Camera Group", then "Create New Group" as shown below...



Before we configure the group, enter the IP address of the camera in the "IP" column.

Now we can configure the group by selecting the "Camera Groups" tab and selecting the group we are working on. Change the type to "ONVIF" and we are presented with the available options for this type...



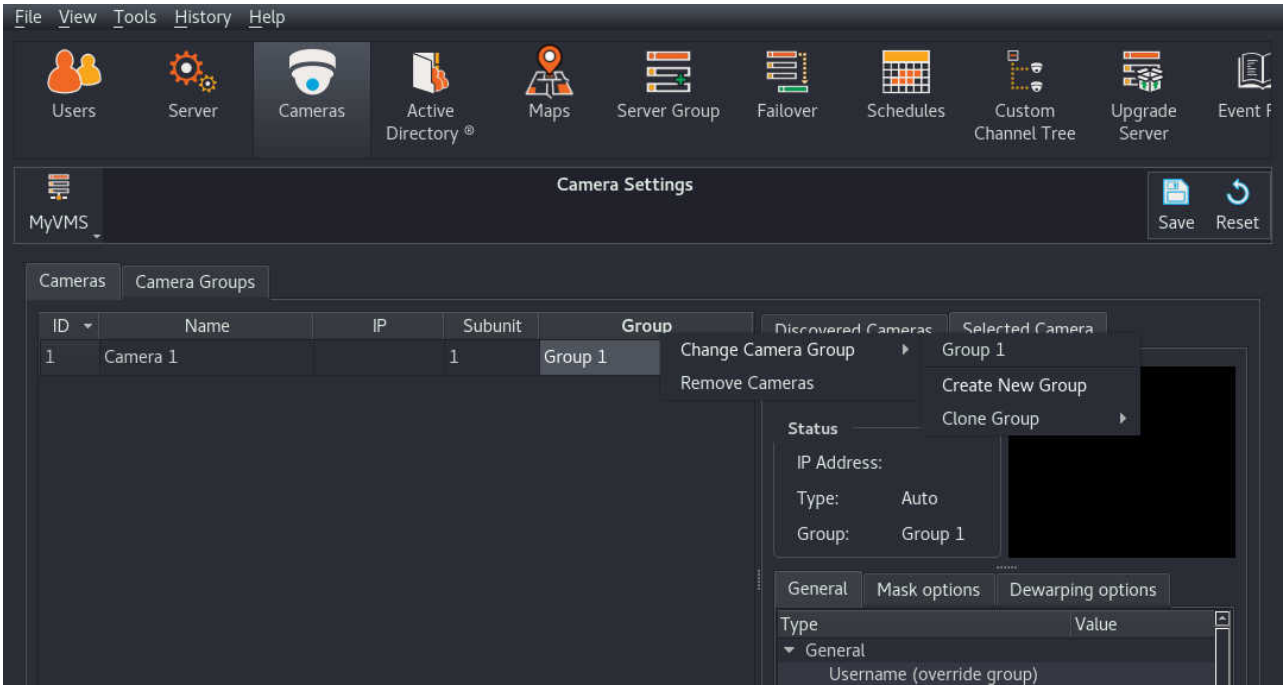
The various options presented here are described in detail in 6.3 – Cameras but the key decision, as described earlier, is whether to select Profiles configured in the camera, or allow Wavestore to push settings to the camera. This is controlled by the "Auto-configure Camera Streams" option.

If "Auto-configure Camera Streams" is disabled, a Profile can be selected for each of the two possible streams. Note that it may be necessary to save your changes to allow the Wavestore to connect to the camera before the Profile list is populated...

After saving the changes, the Wavestore will start streaming and recording the camera with default settings. More detail about available settings is in 6.3 – Cameras.

9.1.2.2 Configuring IP Cameras in ONVIF-Multicast Mode

To add an IP camera to the Wavestore server using ONVIF Multicast, in the Cameras Setup screen click on the + button. The camera will be added to an existing ***Camera Group*** if one exists, otherwise a new group is created and a prompt for the username and password is provided. If the camera has been added to an existing group which isn't already set up for ***ONVIF-Multicast***, right-click the ***Group*** column for the camera and choose "Change Camera Group", then "Create New Group" as shown below...



Before we configure the group, enter the IP address of the camera in the "IP" column.

Now we can configure the group by selecting the "Camera Groups" tab and selecting the group we are working on. Change the type to "ONVIF–Multicast" and we are presented with the available options for this type...

The two available methods for streaming multicast are RTSP and SOAP. Click the "Request" row in the table and then choose the desired from the drop–down box.

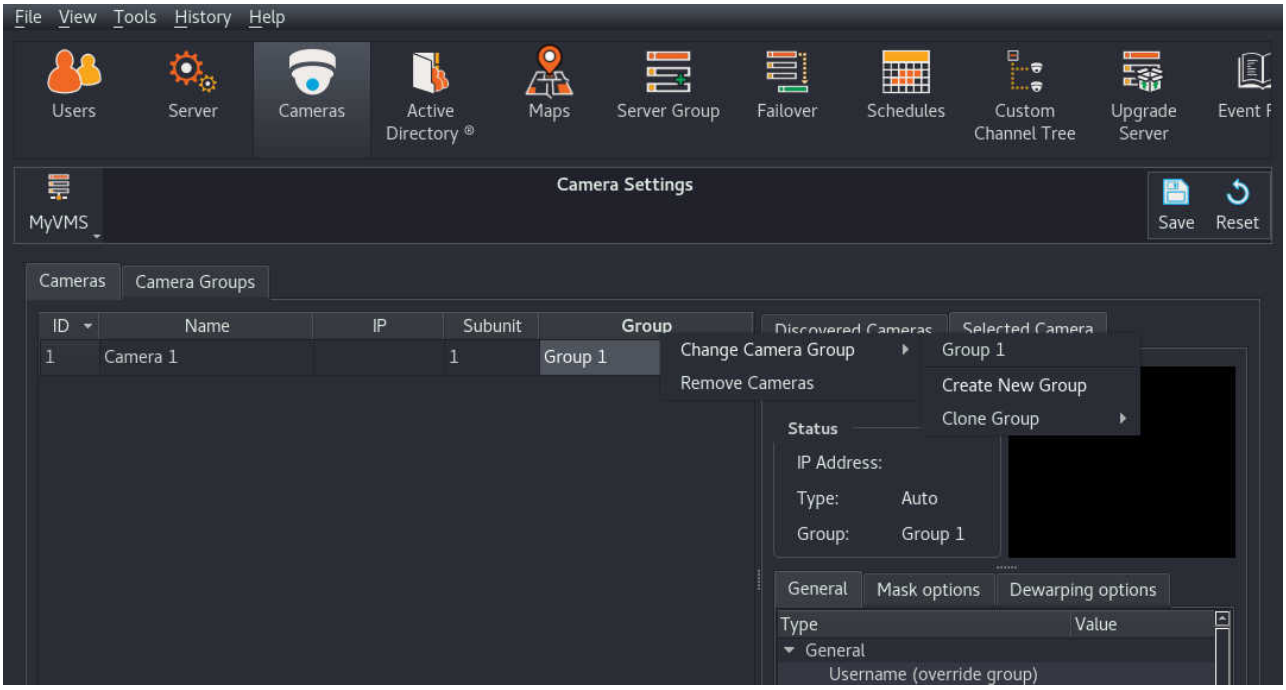
Please note that to configure settings such as the resolution of the video stream it will likely be necessary to do this in the camera's own setup screens via a web browser.

After saving the changes, the Wavestore will start streaming and recording the camera with default set–tings. More detail about available settings is in 6.3 – Cameras.

9.1.2.3 *Configuring RTSP or HTTP Cameras*

It may be necessary to refer to documentation supplied with by the camera manufacturer, to obtain information required during the IP camera setup on the Wavestore server (e.g. stream type/request string etc.).

To add an IP camera to the Wavestore server, in the Cameras Setup screen click on the + button. The camera will be added to an existing ***Camera Group*** if one exists, otherwise a new group is created and a prompt for the username and password is provided. If the camera has been added to an existing group which isn't already set up for ***RTSP*** or ***HTTP*** mode, right-click the ***Group*** column for the camera and choose "Change Camera Group", then "Create New Group" as shown below...



Before we configure the group, enter the IP address of the camera in the "IP" column.

Now we can configure the group by selecting the "Camera Groups" tab and selecting the group we are working on. Change the type to "RTSP" or "HTTP" as desired, and we are presented with the available options for this type...

The settings for HTTP and RTSP are practically identical. The "Request" option is the important part. For HTTP it is under the "General" heading as only one stream is supported. For RTSP it is under the Stream 1 and Stream 2 headings as two streams are supported.

The "Request" string is used to determine how to request video from the camera. The string can be entered manually, but there is also a drop-down list containing the request strings for well-known camera manufacturers.

The documentation from Camera manufacturers may describe how to request video in a format similar to the below:

http://<camera-ip>/video.mjpg

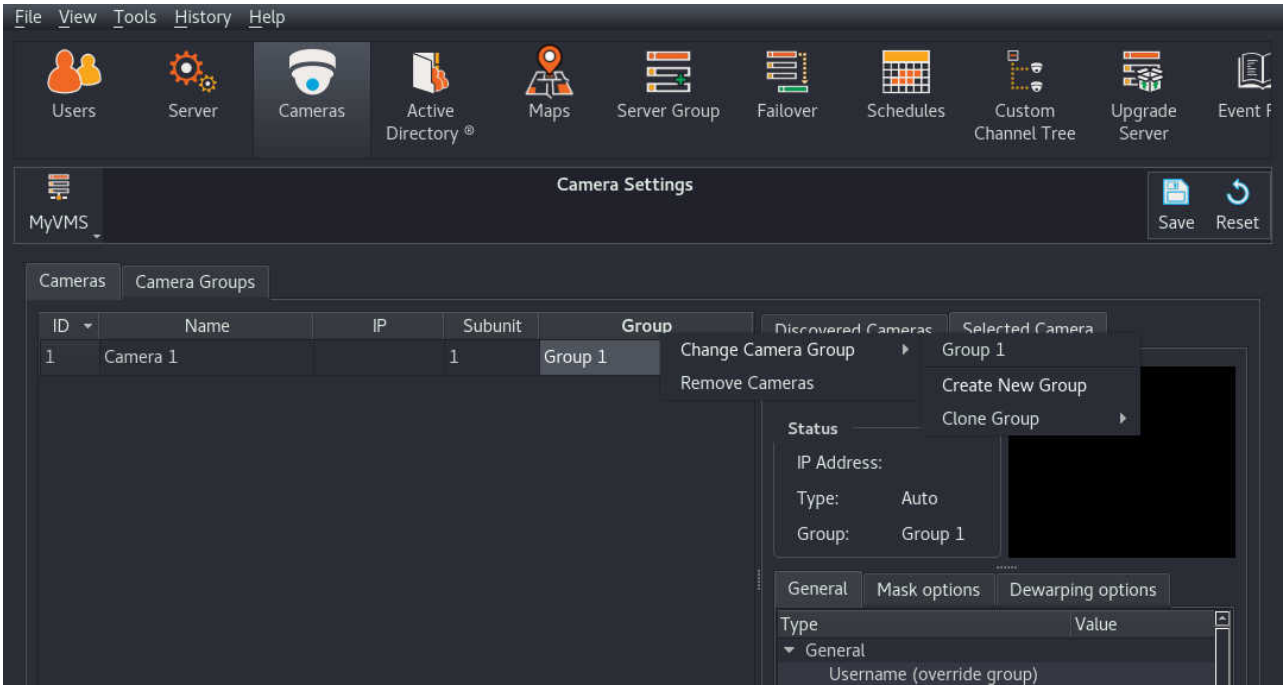
In this case, the "Request" parameter to enter would be "/video.mjpg".

Please note that to configure settings such as the resolution of the video stream it will likely be necessary to do this in the camera's own setup screens via a web browser.

After saving the changes, the Wavestore will start streaming and recording the camera with default settings. More detail about available settings is in 6.3 – Cameras.

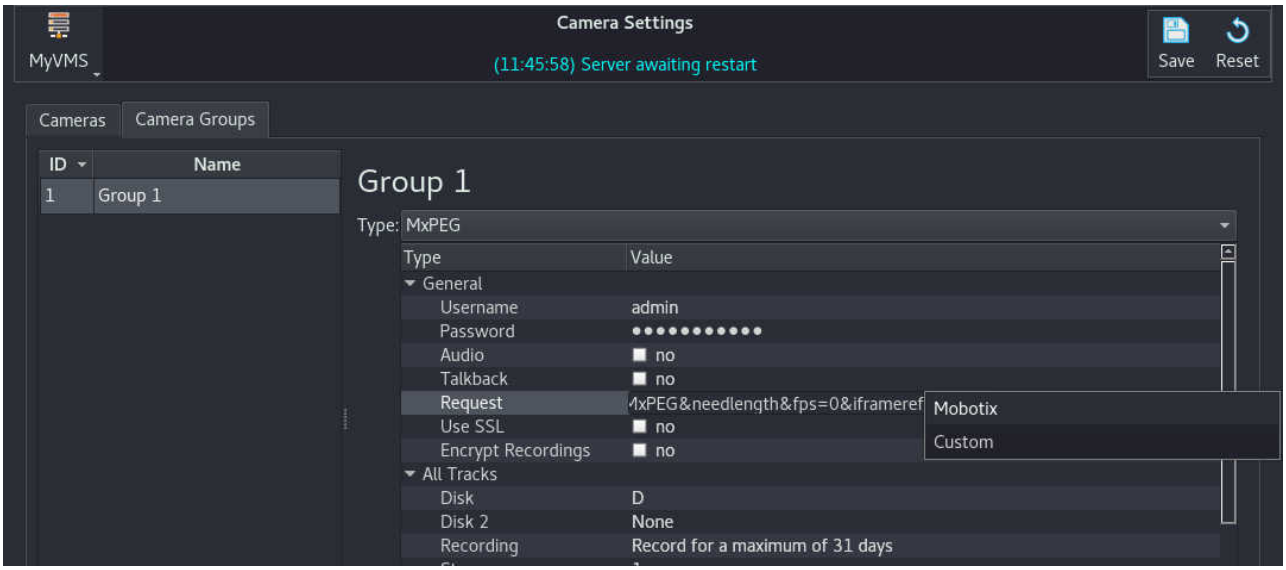
9.1.2.4 Configuring MxPEG or Ampleye Cameras

To add an MxPEG or Ampleye camera to the Wavestore server, in the Cameras Setup screen click on the + button. The camera will be added to an existing ***Camera Group*** if one exists, otherwise a new group is created and a prompt for the username and password is provided. If the camera has been added to an existing group which isn't already set up for ***MxPEG*** or ***Ampleye*** mode, right-click the ***Group*** column for the camera and choose "Change Camera Group", then "Create New Group" as shown below...



Before we configure the group, enter the IP address of the camera in the "IP" column.

Now we can configure the group by selecting the "Camera Groups" tab and selecting the group we are working on. Change the type to "MxPEG" or "Ampleye" as desired, and we are presented with the available options for this type...



The settings for MxPEG and Ampleye are practically identical. For MxPEG the "Mobotix" Request preset should be chosen and for Ampleye the "J2KOO" Request preset should be chosen. The MxPEG request string can be edited to pass different settings for the stream request if desired. Documentation for this is available from Mobotix.

Please note that to configure settings such as the resolution of the video stream it will likely be necessary to do this in the camera's own setup screens via a web browser.

After saving the changes, the Wavestore will start streaming and recording the camera with default settings. More detail about available settings is in 6.3 – Cameras.

9.2 Configuring Multi-lens IP Cameras and Encoders

There are several different ways to add multi-lens IP cameras and multi-channel encoders to Wavestore.

Using a single *Camera Group* of type *ONVIF*

This is the preferred method and should be compatible with most devices. The down side to this method is that if any non-default stream settings are required, such as framerate and resolution, these will have to be configured in the setup menus provided by the device, rather than in Wavestore. Setup for this mode is described in 9.2.1 – Configuring Multi-lens IP Cameras and Encoders in ONVIF Mode below.

Using a single *Camera Group* of type *Auto*

This method is known to work with the majority of ONVIF Profile S devices, however a small number of devices have shown issues and the startup is slower than the alternatives. This method has the benefit of allowing stream settings to be configured in the Wavestore setup screens rather than having to use the device's menus. Setup for this mode is described in 9.2.2 – Configuring Multi-lens IP Cameras and Encoders in Auto Mode below.

Create one *Camera Group* per lens or channel on the device

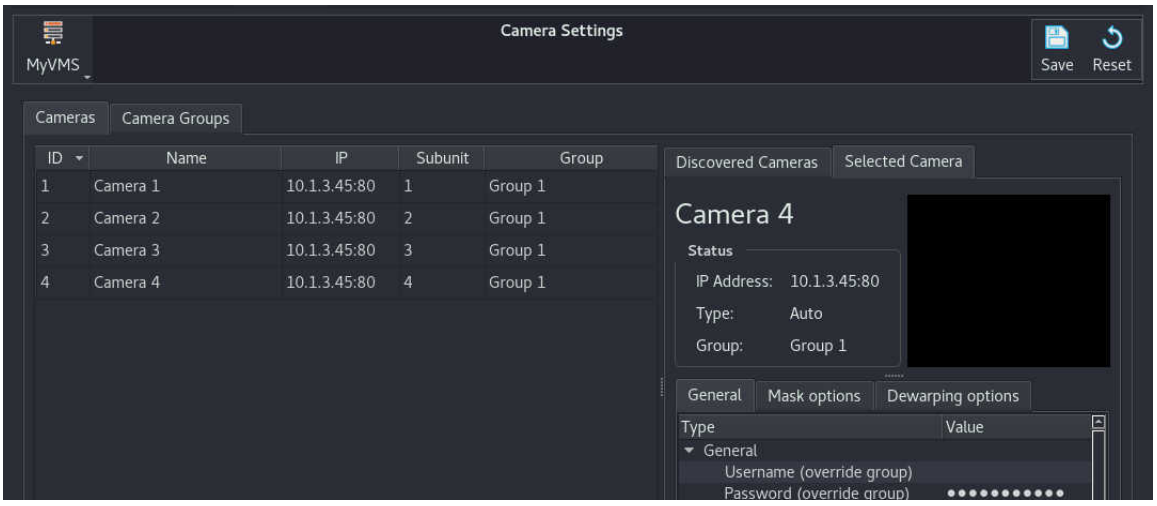
This is the most laborious method of setup as it requires configuring each channel or lens individually rather than through a group. Therefore it is not recommended, but possible if desired.

9.2.1 Configuring Multi-lens IP Cameras and Encoders in ONVIF Mode

Cameras are configured in the Cameras Setup screen which can be accessed in WaveView via the ***View*** → ***Setup*** → ***Cameras*** menu.

As an example, we will add a 4 lens multi-lens camera but the same principle applies for multi-channel encoders.

To set up such a device we simply need to add the camera 4 times and ensure that each camera has different ***Subunit***. The channels can be added by dragging and dropping from the "Discovered Cameras" panel on the right multiple times, in which case the ***Subunit*** will be automatically incremented. Alternatively the channels can be added by clicking the + icon until the desired number of channels has been added, then entering the IP address of the device for each one. In that case the ***Subunit*** field needs to be manually set to unique numbers, e.g. 1 to 4 for channels 1 to 4, as shown below:



Now that the channels have been added, switch to the "Camera Groups" tab. Change the Type to "ONVIF" and ensure that "Auto-configure Camera Streams" feature is disabled.

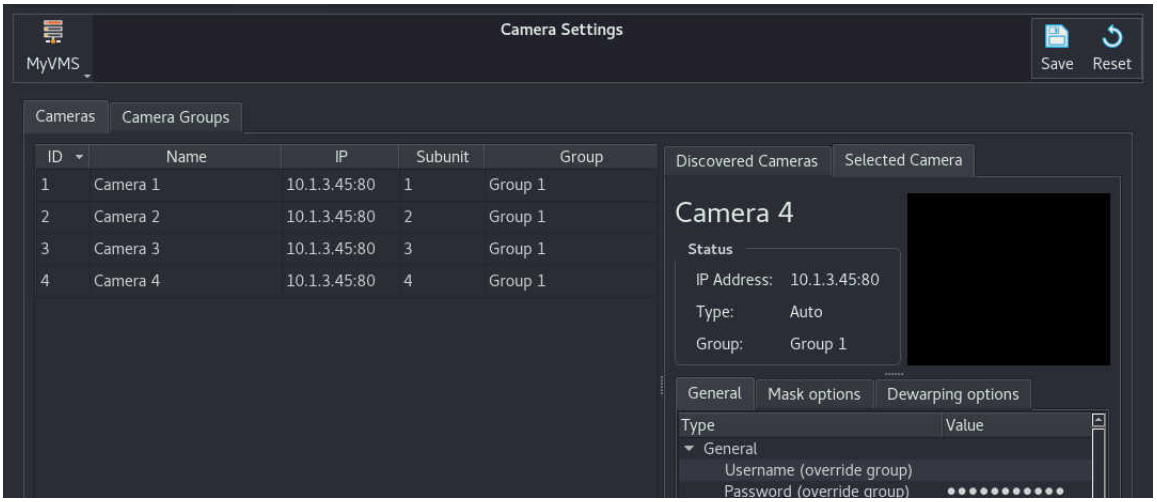
Now simply save the changes and the Wavestore will connect to the camera channels and start streaming. The channels can be further configured via the ***Camera Group*** in the same way as a normal camera. See 6.3 – Cameras for more details.

9.2.2 Configuring Multi-lens IP Cameras and Encoders in Auto Mode

Cameras are configured in the Cameras Setup screen which can be accessed in WaveView via the ***View*** → ***Setup*** → ***Cameras*** menu.

As an example, we will add a 4 lens multi-lens camera but the same principle applies for multi-channel encoders.

To set up such a device we simply need to add the camera 4 times and ensure that each camera has different ***Subunit***. The channels can be added by dragging and dropping from the "Discovered Cameras" panel on the right multiple times, in which case the ***Subunit*** will be automatically incremented. Alternatively the channels can be added by clicking the + icon until the desired number of channels has been added, then entering the IP address of the device for each one. In that case the ***Subunit*** field needs to be manually set to unique numbers, e.g. 1 to 4 for channels 1 to 4, as shown below:

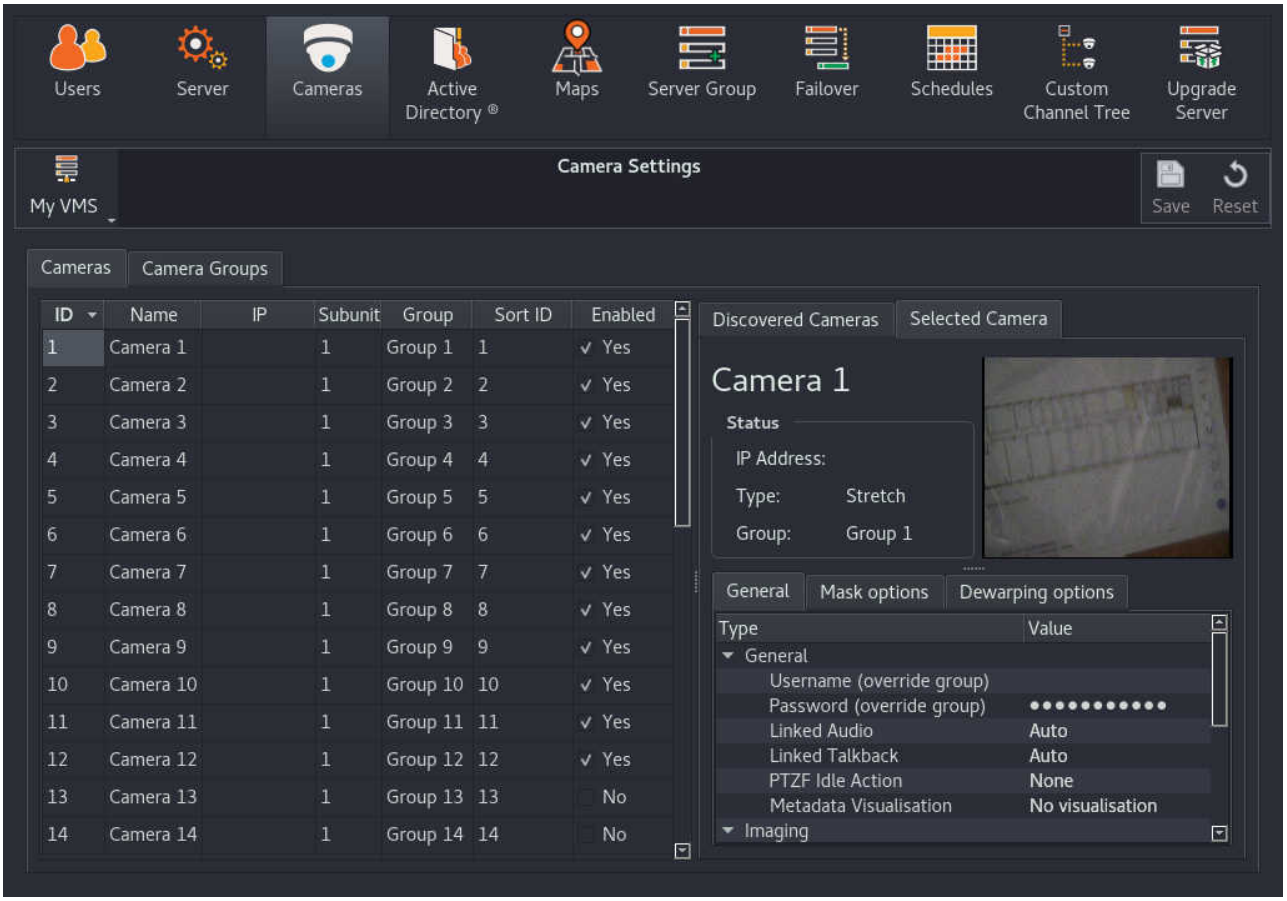


Now that the channels have been added, simply save the changes and the Wavestore will connect to the camera channels and start streaming. The channels can be further configured via the ***Camera Group*** in the same way as a normal camera. See 6.3 – Cameras for more details.

9.3 Configuring Analogue Cameras

If your Wavestore contains an analogue video capture card, the card will be automatically detected and its video and audio channels will be made available for configuration.

To configure the channels, navigate to the Cameras setup screen – *View → Setup → Cameras*.



The available inputs on the capture card are automatically listed in the Cameras screen. Simply click the 'Enabled' checkbox for any required inputs, then click 'Save' to apply the changes.

Note that for analogue channels, each one is assigned to its own *'Camera Group'*.

By default the cameras will be configured to record to disk D at the maximum framerate for 31 days. These settings can be changed as desired, the available options are described in detail in section 6.3 – Cameras.

Each video channel has Imaging settings which can be applied...

There is a Quality setting for each of the 2 available streams per channel. The higher the Quality, the better the image, but the more bandwidth used by the channel, which means more disk space required.

In the *Camera Groups* tab the options per group are generally the same as for any other type of camera, except that the analogue capture cards have some extra Encoding Modes, as follows:

Constant Quality
: This is the default, and recommended setting for most uses. The video encoder tries to keep the video quality at the same level. This has the benefit of ensuring that no matter how much activity or detail there is in the scene, the video quality will remain. The disadvantage is that high levels of activity or detail can cause the bitrate to increase, meaning more storage and bandwidth is required.

Constant Bitrate
: The video encoder attempts to keep the bitrate at a roughly constant level. The advantage of this is that it makes it easier to calculate the storage and bandwidth requirements. The disadvantage is that when there is increased activity or detail in the scene, the image quality will actually reduce in order to keep the data rate at the desired level.

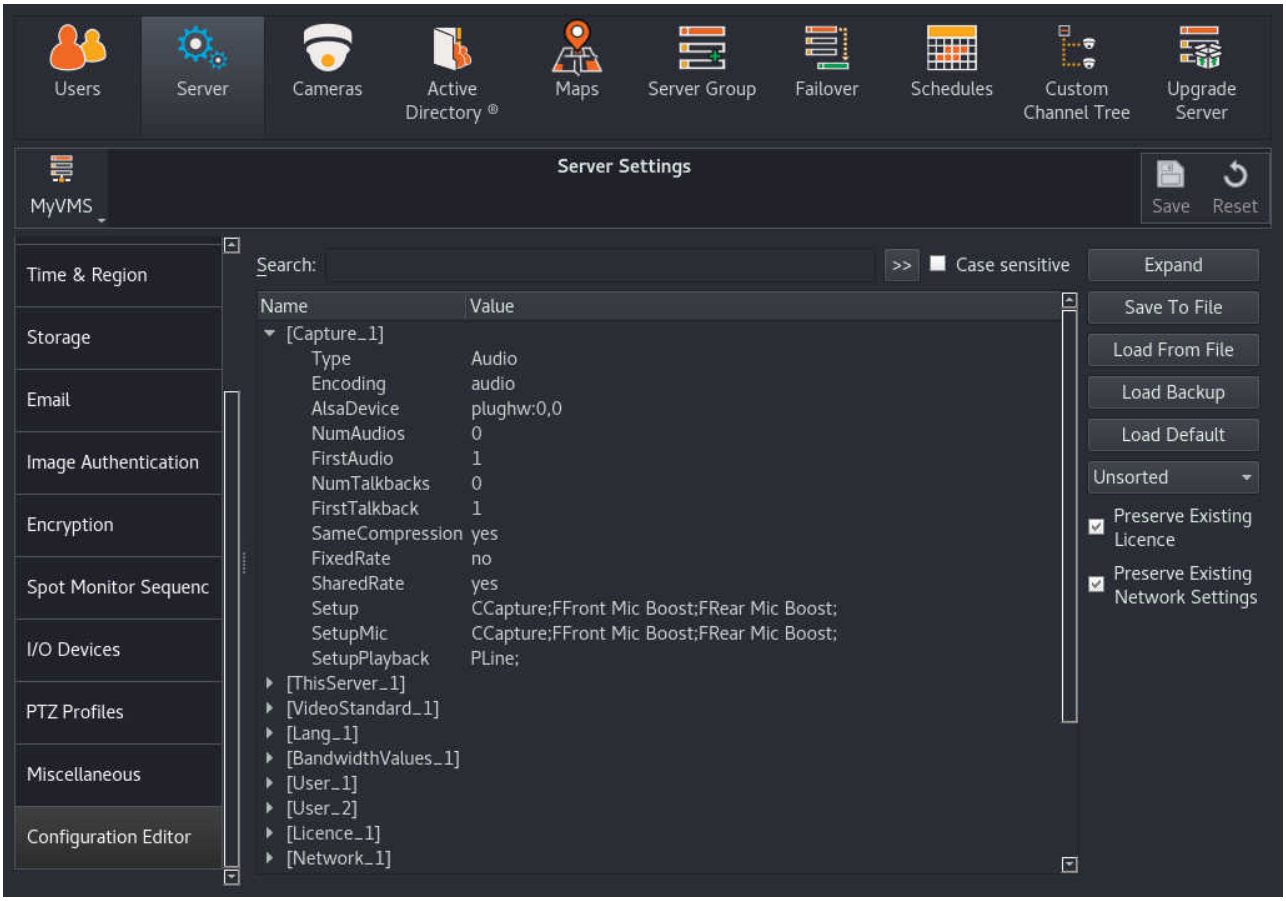
Variable Bitrate
: The video encoder allows the data rate to fluctuate around the "Average bitrate" setting, but when there is increased detail or activity, the data rate is allowed to increase up to the configured "Maximum bitrate" setting. Similar to Constant Quality, this setting has the disadvantage of a varying data rate meaning that the required storage and bandwidth varies depending on the scene content.

9.4 Configuring a Dedicated Analogue Audio Device

Some Wavestore systems may have a dedicated analogue audio device such as one built into the motherboard.

If the device is supported by Wavestore, it will be present in the configuration file as a "Capture Device". However these devices are disabled by default as they are rarely used and having their channels present in the channel list can cause undesirable confusion with camera numbering. Therefore they need to be enabled manually.

To check if an audio device is present and detected, navigate to *View → Setup → Server → Configuration Editor*. Look for a section called "[Capture_N]" where N is a number, as in the example below:



Note: if you do not see the Audio device, check if your system hardware supports it. You might need to enable it in the BIOS on some motherboards (C7P67 boards have this under *Advanced → Chipset → Southbridge*). Once enabled in the BIOS, from WaveView run *Tools → System Maintenance → Run Hardware Detection* to add it to the configuration file. It is best if no cameras or camera groups exist when Hardware Detection is run as they will need to be renumbered. Once this is run, you should see the [Capture_N] section for Audio.

The NumAudios and NumTalkbacks parameters here are set to zero, which means that no channels are available to the system. This is the default: hardware audio is disabled by default.

For onboard audio the number of channels available are always 2 Audios and 1 Talkback, so we need to edit the configuration to set the number of channels and the first channel of each type. So in our example

we set:

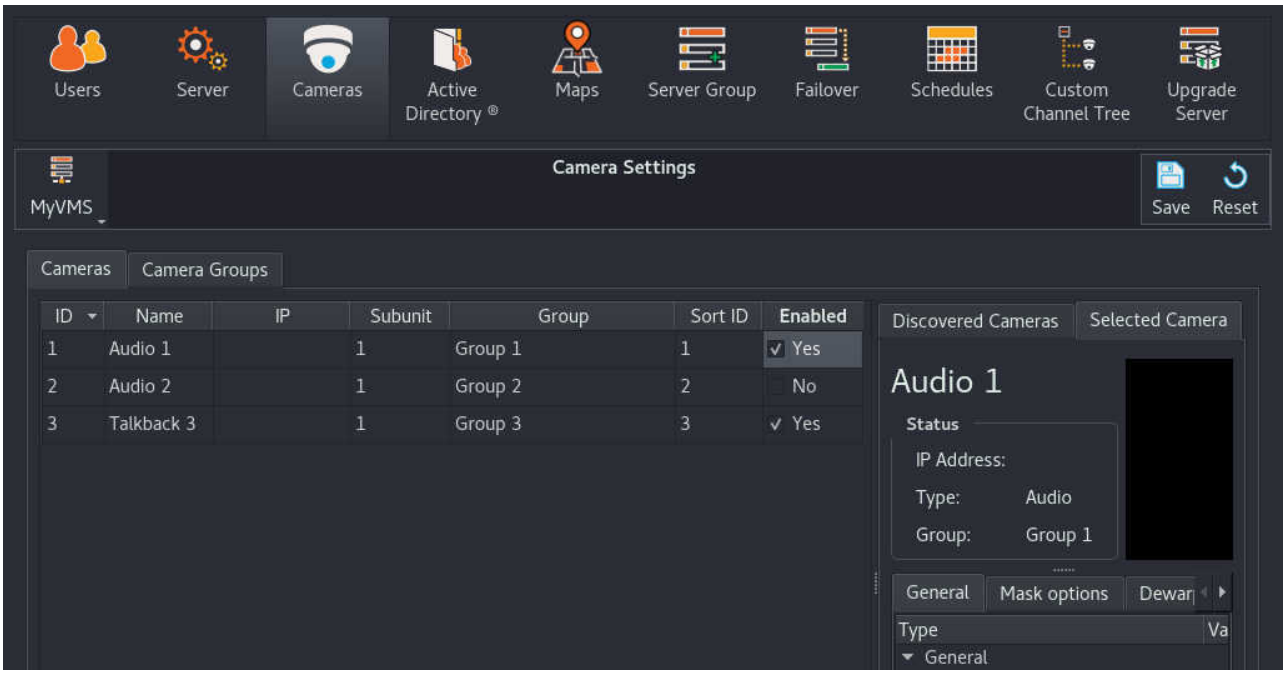
NumAudios=2
: As stated above, these devices always have 2 audio inputs.

FirstAudio=1
: In our case we want the numbering to start at channel 1. We could set it to any channel number desired, assuming there isn't already a channel with that number configured. For example we might want to call it channel number 101.

NumTalkbacks=1
: As stated above, onboard audio devices always have 1 audio output (for "talkback").

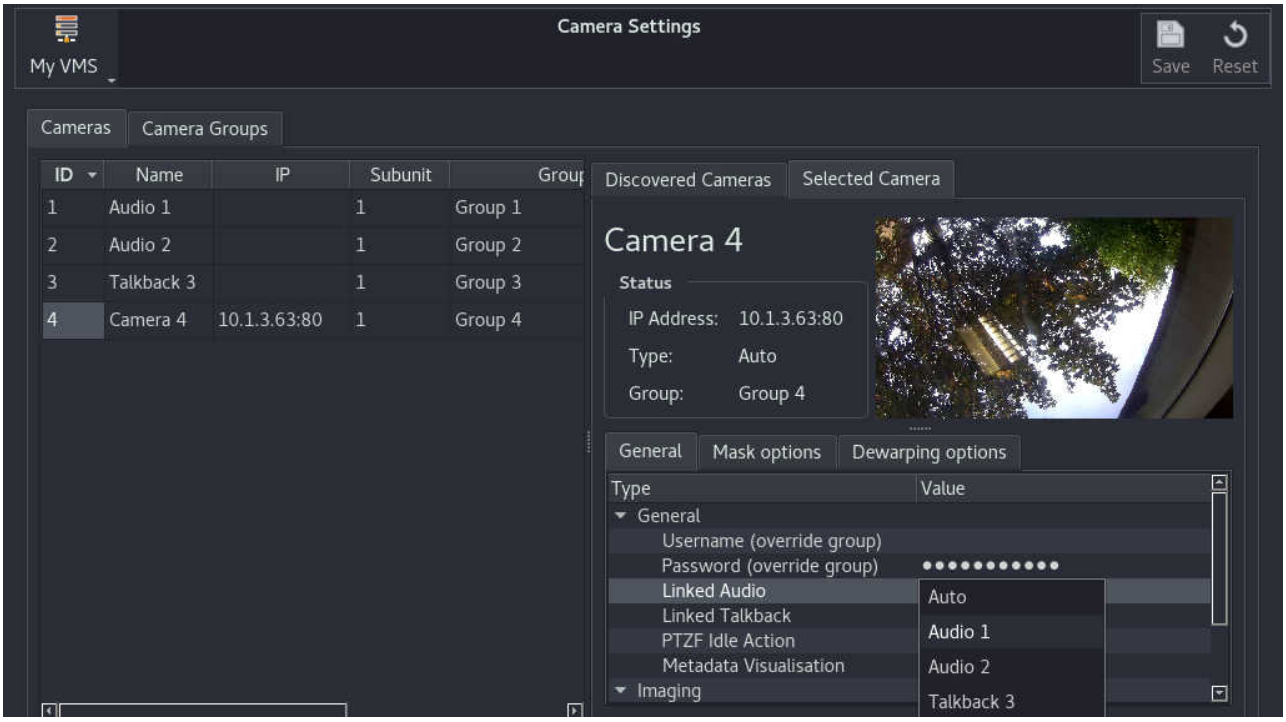
FirstTalkback=3
: In our case we want the talkback channels to start at channel 3, because channels 1 and 2 are used by the audio inputs.

After we save these changes, we can go to the Cameras setup screen to see our channels.



We can now simply enable the desired channels (as shown above for channels 1 and 3). Once the changes are saved these channels will be enabled and recording with default settings. Further settings available are described in 6.3 – Cameras.

To associate a camera with an audio channel, select the camera in the Cameras table, and select the Audio channel in the "Linked Audio" field as below.



Note that the default is "Auto" but this is designed for use with IP cameras which transmit video and audio together, so the automatic link between video and audio channels is obvious. For dedicated audio devices, as discussed in this section, the Auto mode is not applicable and so the link from camera to audio channel has to be specified.

9.5 Configuring Talkback (Client to Server Audio)

The Wavestore server can be configured to allow two way audio (Talkback) between a client device (e.g. WaveView PC) and a supported networked audio device (e.g. audio output on a supported IP camera/server motherboard audio output).

Section 3.22 – Preferences gives details of how to configure the audio input on the WaveView client PC.

Multiple camera channels can be mapped to a Talkback output (either an audio output on an IP camera/server motherboard audio output).

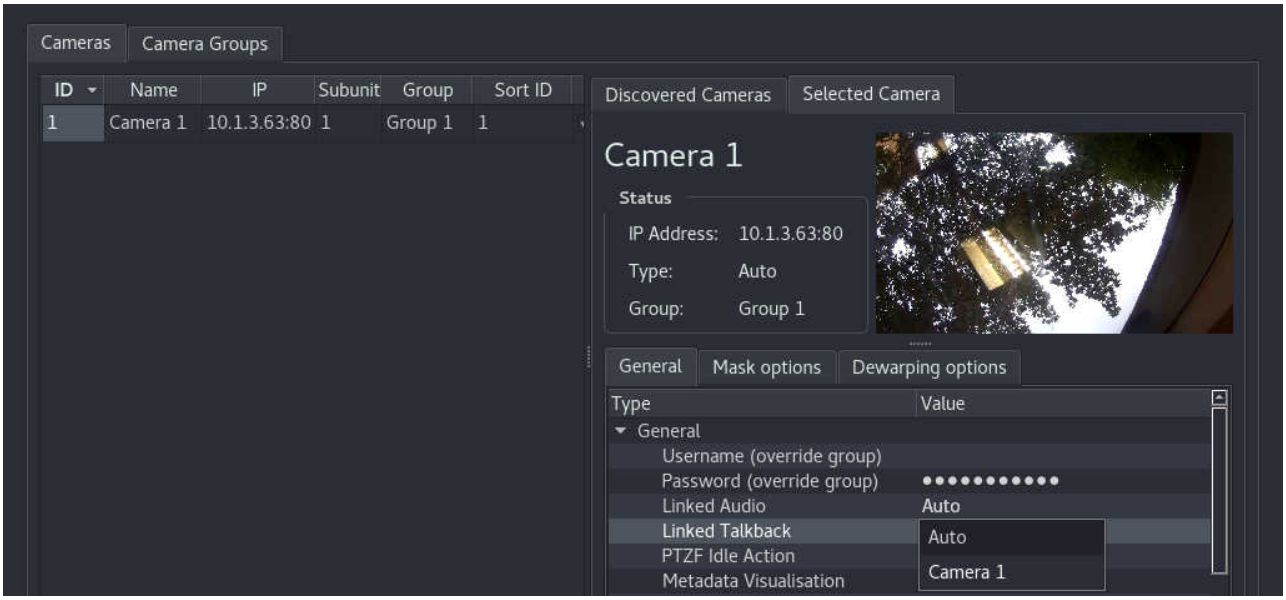
Talkback channels can also be used to play a configured sound (e.g. Warning Message/Audible Tone), configuration for this feature is carried out in the Event Rules menu (section 6.12 – Event Rules).

Note that only one audio source can be sent to a talkback device at a time. For example it is not possible for multiple clients to talk to the same target device simultaneously.

9.5.1 Configuring Talkback using supported IP Camera Audio Output

To enable Talkback for an IP camera, simply navigate to View → Setup → Cameras, select the ***Camera Group*** associated with the cameras in question, then enable the Talkback checkbox.

By default, a talkback channel on an IP camera is linked to the video channel of that camera. If it is desired to link a video channel to the talkback channel on a different camera, select the camera in the Cameras table then select the Talkback channel from the ***Linked Talkback*** dropdown list:

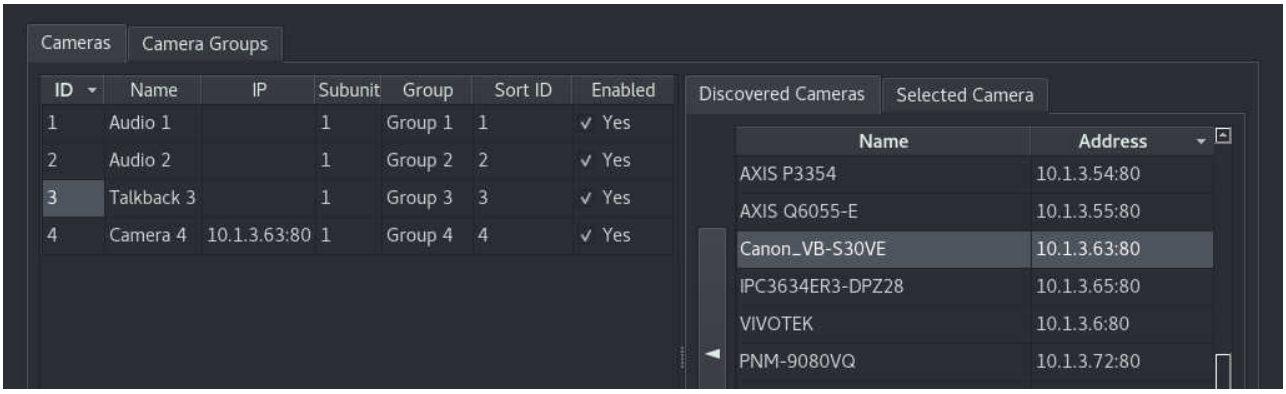


Save your changes, and the Talkback channel is ready to use.

9.5.2 Configuring Talkback using Server Motherboard Audio Output

To use the server motherboard audio port, these ports must first be enabled. See 9.4 – Configuring a Dedicated Analogue Audio Device for details on how to do this.

We can then follow the menu path View → Setup → Cameras to configure the talkback channels.

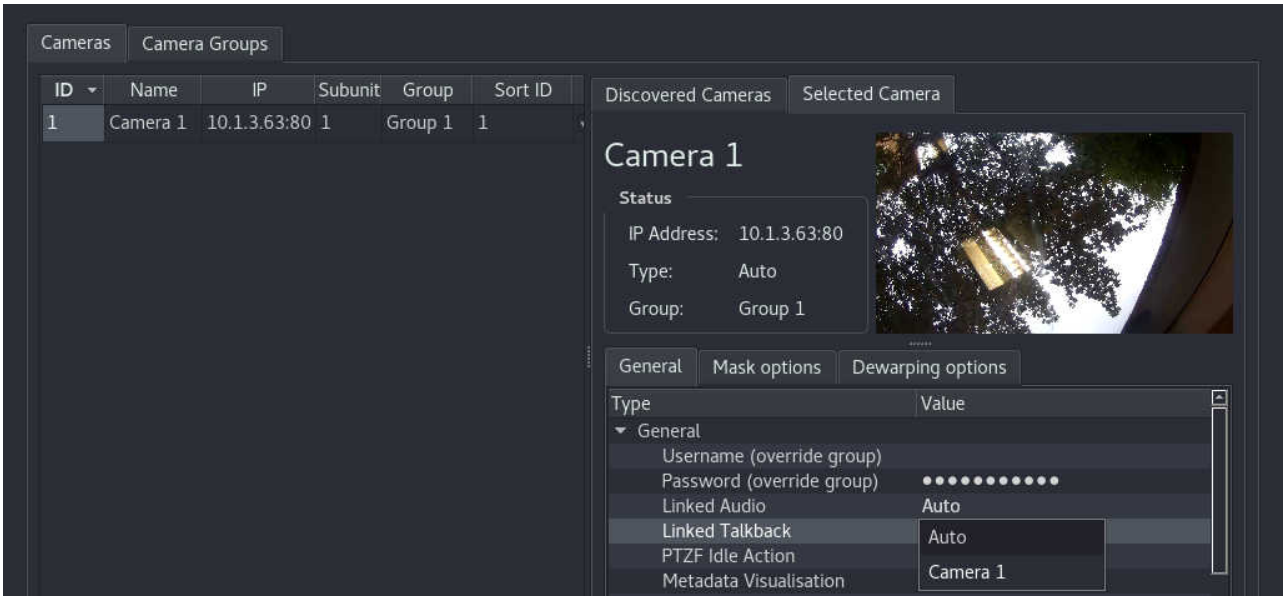


The motherboard audio channels will be displayed in the camera table with appropriate default names. In our example these are channels 1–3 with the talkback channel as channel 3.

Ensure that the channel is enabled. Then, ensure the channel is selected, switch to the Camera Group tab to see the settings for the group this channel is assigned to. In most cases the defaults are sufficient, but the channel recording settings can be modified here.

Click Save to ensure the talkback channel is enabled.

The final step is to link this talkback channel to a video channel. To do so, select the camera in the Cameras table then select the Talkback channel from the ***Linked Talkback*** dropdown list:


Cameras
Camera Groups
ID
Name
IP
Subunit
Group
Sort ID
1
Camera 1
10.1.3.63:80
1
Group 1
1
Discovered Cameras
Selected Camera
Camera 1
Status
IP Address: 10.1.3.63:80
Type: Auto
Group: Group 1
General
Mask options
Dewarping options
Type
Value
General
Username (override group)
Password (override group)
Linked Audio
Auto
Linked Talkback
PTZF Idle Action
Metadata Visualisation
Auto
Camera 1

9.6 Configuring a File Playback Camera

It is possible to configure a "camera" where the source is a file which contains video or audio. It will then be played in a loop. This can be used to display promotional or warning messages, or replay short clips. It is not suitable for playing large files as the entire file is kept in memory.

The supported types are somewhat limited at the moment but more may be added in future. The supported types are:

- WSB with a single channel
- JPEG single image
- PCMA audio

To configure a File playback "camera", first it is necessary to upload the file. This can be done using the File Manager – see section 3.26 – File Manager. Images usually appear in the "maps" or "misc" directory and audio usually appears in the "audio" directory.

Once the file is uploaded the camera can be configured.

- Go to *View > Setup > Cameras > Camera Groups*.
- Add a new group.
- Set the Type of the group to "File".
- Ensure that the Video and Audio fields are enabled or disabled as appropriate for the type of file you are playing.
- Set the Capture Rate in the camera group. For audio, Rate=8 is recommended. For a still image it's sensible to use Rate=1. For a video file, it would usually be best to set it to the rate of the source video.
- Switch to the ***Cameras*** tab in the Cameras setup screen.
- Add a camera with the + icon and assign it to the newly created group.
- In the IP field, enter the filename. Don't enter any path as the appropriate directories will be searched.
- Save the changes.

The newly added camera should now be available to view in the Main screen. If there are any errors, they will be reported in the System Log.

9.7 Configuring Motion Detect Recording

The Motion Detect Recording function allows the server to be configured to record only when Motion Activity is detected on the viewed scene.

For analogue cameras, the motion detection is always performed within the Wavestore. For IP cameras there are several ways in which this can be performed:

Motion Detection within Wavestore

The motion detection can be performed within the Wavestore for certain cameras. The requirements are the same as for Smart Search – an ONVIF Profile S compliant camera which is able to transmit a second JPEG stream of 648x648 pixels or less. The JPEG stream is a low resolution stream at 4 frames per second and so some extra bandwidth is used for this.

The advantage of this method is that it is simple to set up and can be configured in the Wavestore setup screens.

The potential disadvantage is that the in-camera motion detection facilities may be more advanced, depending on the camera. Also, if using "Auto" group type or "ONVIF" group type with "PullPoint" enabled, the camera may also send motion events which will be used to start and stop recording. In that case it is recommended to disable the in-camera motion detection system.

To enable this system, either:

- Set up the camera with the ***Auto*** camera group type and ensure the 'VMD / Smart Search' option is enabled.
- Set up the camera with the ***ONVIF*** camera group type and ensure both the 'Auto-configure Camera Streams' and 'VMD / Smart Search' options are enabled.

Motion Detection within the camera via ONVIF PullPoint

Wavestore can receive motion events from ONVIF Profile S compliant cameras and trigger recording or other actions based on that.

As described above, it is not recommended to use this method in conjunction with the Smart Search facility as it means there are two separate motion detection mechanisms in operation.

To enable this system, either:

- Set up the camera with the ***Auto*** camera group type. The events will be pulled if available.
- Set up the camera with the ***ONVIF*** camera group type and ensure that the 'Pull Point' option is enabled.

Motion Detection within the camera via TCP Notification

Wavestore offers a protocol called EVENTP whereby a camera can be configured to send a message to the Wavestore whenever motion occurs. This can be used to trigger recording appropriately.

This method has the disadvantage of being fairly time consuming to set up and it requires configuration in each camera. As with the ONVIF PullPoint method, it is not recommended to use this method in conjunction with the Smart Search facility as it means there are two separate motion detection mechanisms in operation.

Enabling this system is described in section 9.7.3 – Configuring Motion Detection Via TCP Notification.

If in doubt, Wavestore Technical Staff can provide advice on the best method to use.

9.7.1 Configuring the Camera for Motion Detection Recording

Ensure that motion detection is enabled for the camera as described in section 9.7 – Configuring Motion Detect Recording. Then navigate to the Cameras setup screen (View → Setup → Cameras), select the *Camera Group* tab, then select the relevant Camera Group.

Motion recording can either be set on All Tracks or a specific recording track. In the screenshot below we use Track 1. Set the 'Recording Mode' to Motion, then the 'Pre Record' and 'Post Motion' settings become available to allow setting recording durations for before and after the motion events.

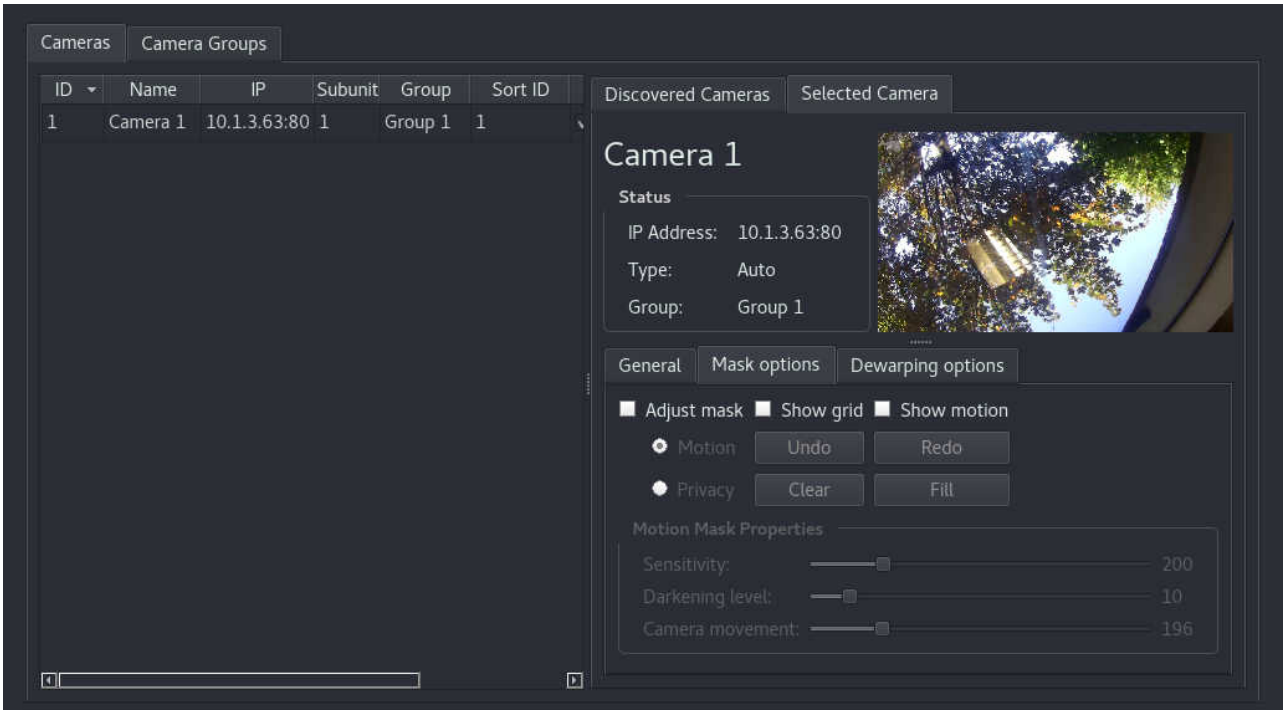
Other recording modes are available and are detailed in section 6.3.2 – Camera Group Settings.

Finally, click 'Save' to confirm your changes.

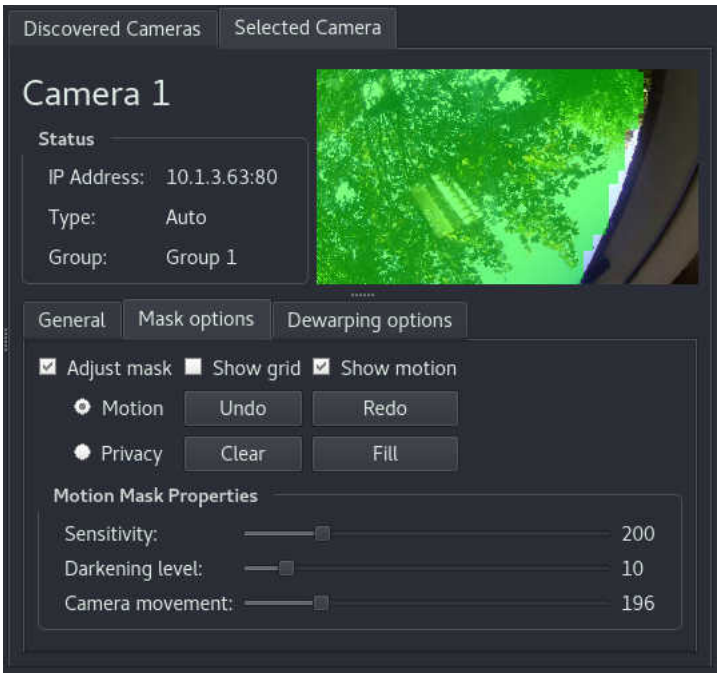
9.7.2 Configuring Settings and Masks for Motion Detection within Wavestore

When using the Motion Detection system within Wavestore, it is possible to configure masks to limit the motion detection to a region of the image, as well as sensitivity.

To configure these settings, navigate to *View* → *Setup* → *Cameras*, then select the desired camera under the *Cameras* tab. In the right hand panel, select *Mask Options*.



Check the 'Adjust Mask' and 'Show Motion' options; the camera view will now show the areas active for Motion Detection in Green, with areas where motion is currently being detected shown in Blue.



Configure the areas you wish to make active for Motion Detection by using the 'Fill' and 'Clear' buttons, or left click and drag using the mouse to add/remove areas. You may also wish to adjust the values in the 'Motion Mask Properties' section, to fine tune the Motion Sensitivity settings.

Finally, click 'Save' to confirm your changes.

9.7.3 Configuring Motion Detection Via TCP Notification

Certain cameras, such as those in the AMG Panogenics, Axis, Brickcom, Mobotix and Vivotek ranges, can be configured to send TCP messages which can be used by the Wavestore server to trigger a configured Event Rule to record, without requiring parsing to be carried out.

When Motion is detected by the camera, the camera needs to be configured to send a TCP notification message for the Motion Event to the Wavestore, in the format:

P<valid Wavestore username>;<valid password for that user name>;M<camera-channel-number><optional-event-type>;

For example:

Puser;a;M6; for a Pulse (i.e. instantaneous) Motion event

Puser;a;M6+; for Motion ON

Puser;a;M6-; for Motion OFF

where the server has a configured user ID: 'user' with password: 'a', and the camera channel is No: 6. Note that the user also needs the "Post events" permission.

9.7.4 Configuring Motion Detection Recording for other IP cameras (using non standard message notification formats)

Wavestore can integrate with many other cameras using the integration module system.

Please contact the Wavestore support team for further information.

9.8 Configuring Smart Search

Wavestore has a facility to perform a post-recording search of a period of recordings based upon motion.

Supported Camera Types

The Smart Search facility is available for:

- Analogue cameras connected via a Stretch analogue capture card
- Most ONVIF Profile S compliant cameras (specifically, ONVIF cameras which allow a second JPEG stream of 648x648 pixels or less)

For IP cameras it is necessary to ensure the "Smart Search / VMD" setting is set such that Smart Search shows as On, whether using Server-side or Camera-side VMD (Video Motion Detection). This feature is available for the "Auto" and "ONVIF" group types. For the "ONVIF" group types, it is necessary to use the "Auto-configure Camera Streams" option.

Note that for ONVIF cameras the Wavestore will request an extra low-resolution 4 fps JPEG stream from the camera. It is an ONVIF Profile S requirement that all cameras support this. However some cameras may not permit dual-streaming at the same time as taking this JPEG stream for motion analysis.

How It Works

When properly configured, the Wavestore will continually capture and record metadata relating to the amount of motion in the video. For ONVIF network cameras, the Wavestore will pull a low-resolution, low-framerate JPEG stream and perform analysis on that. For analogue cameras, the motion detection is performed in the capture card hardware.

In all cases this metadata needs to be recorded so that motion analysis can be performed at a later date. This is done by ensuring that the Search track (Track 6) is enabled and appropriately configured. This track is enabled by default and configured for 31 days recording so the default settings are usually sufficient.

See section 4.8 – Smart Search for information on how to perform the search.

9.9 Configuring Video Analytics

Wavestore has a facility to perform a post–recording search of a period of recordings based upon video analytics metadata, and to trigger events based on real–time analysis of the video analytics metadata.

The analytics metadata can from:

- An ONVIF camera which supports streaming of standard ONVIF Analytics Metadata
- A supported external analytics device

For supported ONVIF cameras, the analytics metadata stream will be started automatically if configured using the Auto camera group type. It is possible to check if this is working using the ***Execute Command*** tool (Tools → Execute Command). Just run 'streams N' where N is the camera number, for example 'streams 3'. If metadata is being received, it will be indicated as such for stream 4. For example:

```
Live Streams from camera 3:
Stream1: H264 at 30 ips
Stream4(Metadata): Data at 1 ips
VMD/SmartSearch: bitmap 32x18 from JPEG 256x144
Total bandwidth 5190 Kbit/s (all streams)
```

To perform a post–recording search of the analytics data, the data must be recorded. This can be acheived by enabling Track 4 for the appropriate camera group (see section 6.3.2 – Camera Group Settings). The data can be searched using the Main screen Smart Search facility (see section 3.13 – Smart Search Control).

To trigger events based on real–time analysis of the video analytics metadata, it is not necessary to record the data. However it is necessary to create Event Causes in the Analytics setup screen (see section 6.14 – Analytics). Once the appropriate Event Causes have been created, event rules can be programmed as usual in the Event Rules setup screen (see section 6.12 – Event Rules).

9.10 Configuring Virtual Spot Monitors

Virtual Spot Monitors are an innovation in Wavestore which allow video routing within the system between video channels.

Imagine a system with 4 IP cameras numbered 1 to 4. It is possible to create a channel 5 which is a 'Virtual Spot Monitor' and assign a sequence to that channel so that it shows cameras 1 to 4 for a few seconds each, or it could be configured to switch camera based on an event. The operator can then view that channel 5 within WaveView and see the camera switch when an event occurs or after a time period.

Virtual Spot Monitors do not take up a licensed channel meaning that many can be created if desired. They can route IP or analogue video channels.

Note that Virtual Spot Monitors do not currently support Privacy Masks.

Creating Virtual Spot Monitors is simple...

- In the Cameras setup screen (View → Setup → Cameras), click the + icon to create a new 'camera'.
- We need to assign that camera to a ***Camera Group*** of type 'VirtualSpotMonitor'. Assuming you haven't created one already, right-click the newly added camera and choose ***'Change Camera Group → Create New Group'***.
- When prompted for a username and password, just click 'Cancel' as we don't need any login details for this kind of device.
- Switch to the ***'Camera Groups'*** tab and ensure the newly created group is selected.
- Change the Group Type to ***'VirtualSpotMonitor'***.
- Save the changes.

Subsequent Virtual Spot Monitor 'Cameras' can be added to the previous Virtual Spot Monitor ***Camera Group***.

That's all that is required for a default setup although a few tweaks might be desirable such as renaming the Camera Group to something appropriate, and possibly disabling recording (by default the Virtual Spot Monitor will record, but the original cameras are probably also recording). Further settings are documented in section 6.3 – Cameras.

Once a Virtual Spot Monitor 'camera' has been created, a ***'Sequence'*** can be created for it. This is detailed in section 6.2.10 – Spot Monitor Sequences. Also, event rules can be created to switch certain cameras to spot monitors when events occur – see section 6.12 – Event Rules.

9.11 Configuring Framerate Boost

Wavestore has a facility to increase the recording framerate in certain circumstances. The potential benefit of the "boost" is to reduce storage usage, although for H.264 and H.265 video streams the streams need to be carefully configured to ensure there is benefit gained. See section 9.12 – H.264, H.265 and Framerates for a detailed explanation.

There are two main ways to use boost:

On a Schedule

The boost can be programmed to occur at different times of the week. This is quite simple to set up. Firstly create a Schedule as described in section 6.10 – Schedules. Secondly, in the Cameras setup screen, under the *'Camera Groups'* tab, set the Recording Mode to *'Framerate Boost on Schedule'*, set the normal framerate and boost framerate, then set the desired schedulet.

When an event occurs

The Wavestore Event Rules system can be programmed to trigger the boost when an event occurs. This could be from a range of *Event Causes* such as Motion, digital input, or analytics trigger from an external device.

We'll describe below how to configure boost to occur when there is motion. There are essentially 3 steps to this:

Ensure that the camera is sending required events such as motion

For cameras connected via an analogue capture card in the Wavestore, this is automatic.

For IP cameras there are several ways to do this depending on the camera capabilities. These are described at the start of section 9.7 – Configuring Motion Detect Recording but for most modern cameras configured with the *'Auto'* group type, it will just work without any settings needed to be made.

Configure an event rule to trigger boost when the desired event occurs

For the second step it is simply necessary to configure an event rule whereby the Cause is the desired event type such as "Motion" for the selected camera, and the Action is "Boost recording rate on a camera track", selecting the desired recording track. This is described in more detail in section 6.12 – Event Rules.

Configure the boost rate settings

The boost rate settings are found in the Cameras setup screen, under the *'Camera Groups'* tab. There are 3 relevant settings:

Recording Rate

This is the normal recording rate when no events are triggered.

Boost Rate

This is the recording rate when the event is triggered, until it ends.

Pre Boost

Note that this is found under the *'Recording Mode'* option group. This option sets a duration for a period before the event where the recording should also occur at the "boosted" rate. Note that generally only a few seconds are permitted here. If very large durations are requested they may not be acheived. The pre-boost recording duration is also not guaranteed to be handled precisely.

9.12 H.264, H.265 and Framerates

9.12.1 H.264 and H.265 basics

H.264 is currently the most commonly used compression format in the CCTV industry and so this section will provide a simplified explanation of how it works and the implications on various Wavestore features. The principles described here also apply to H.265 although we will generally only refer to H.264.

The H.264 compression algorithm and other similar compression formats such as MPEG-4 work on the basis of not always sending complete frames. The video stream is comprised of different frame types:

i-frames
: These are complete frames. In H.264 an i-frame is very similar to a full JPEG image. An i-frame on its own is useful in that it can be decoded and displayed without needing any other frames.

p-frames
: These are smaller frames which essentially contain only differences compared with the previous frame. Therefore they are useless on their own. In order to view a p-frame you need all previous frames in the stream back to the last i-frame.

b-frames
: These are similar to p-frames except that they are bi-directional and can refer to frames in the future. This has potential negative consequences in CCTV such as increased latency and so most cameras do not output b-frames, or at least have the option to disable them. Wavestore does not currently support b-frames.

A collection of a single i-frame followed by several p-frames is called a Group Of Pictures – or GOP.

To keep things simple we'll consider a video stream with a framerate of 5 frames per second and a GOP size of 5. This means that there is one i-frame every second, so 3 seconds of video will look like this:

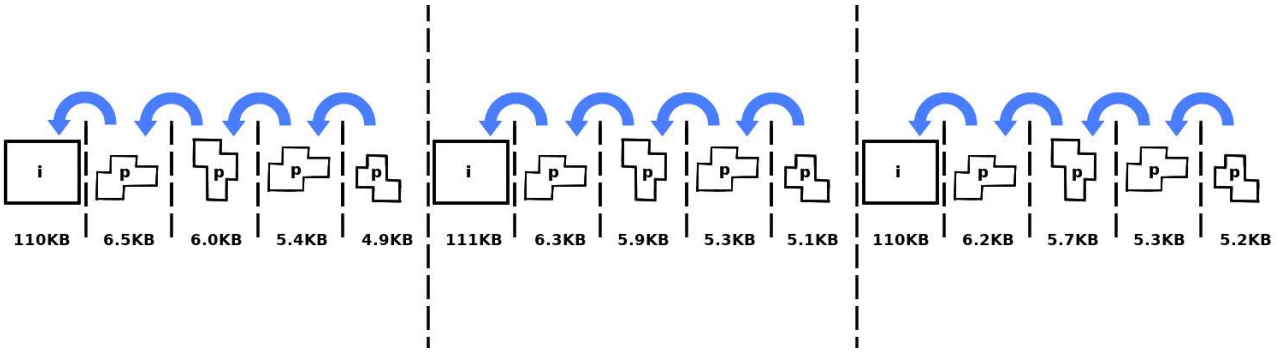


Figure 9.1: Simpified representation of H.264 stream with GOP size of 5

The frame sizes shown are from a real 2.1 megapixel camera from a well-known camera manufacturer. The camera was situated in an office with little movement.

As can be seen from the frame sizes in the diagram, the p-frames are generally very small compared to the i-frames. This can have implications on the effectiveness of using settings such as "framerate boost on motion".

9.12.2 Framerate Boost Considerations

Since each p-frame depends on the previous p-frames we can't just dispose of any of them because it would cause corruption in the stream...

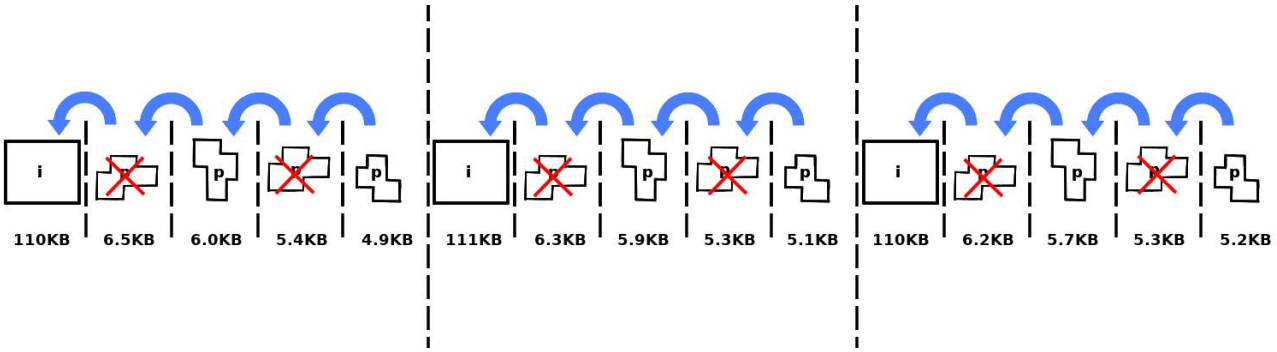


Figure 9.2: Corrupted H.264 stream due to missing p-frames

In the diagram above we've tried to reduce from 5fps to 3fps, but the stream is corrupted because the first remaining p-frame refers to the previous p-frame which is no longer present. Wavestore has a mechanism to prevent this from happening.

We could potentially get rid of just the trailing p-frames in a GOP. For example like this...

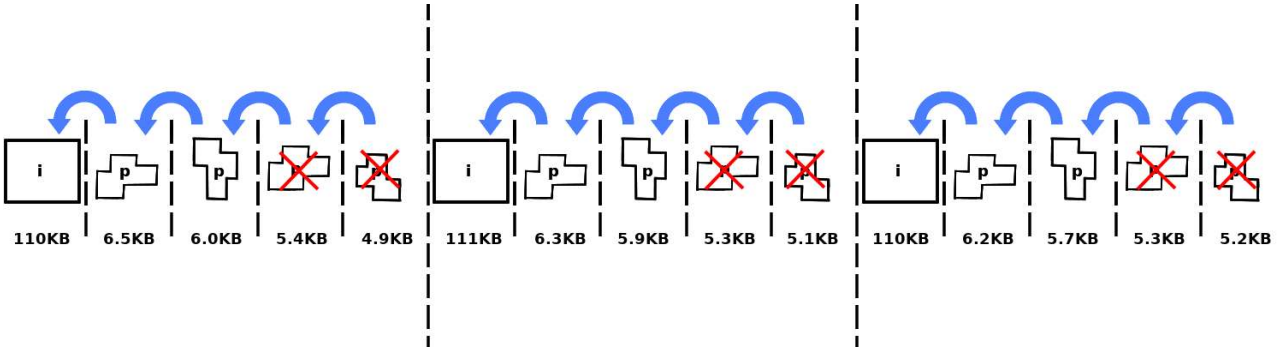


Figure 9.3: Non-corrupted H.264 stream with p-frames at start of GOP

Now this stream isn't corrupted, however all the video is squeezed into the beginning of the GOP. In this case every second there will be 3/5ths of a second video, then 2/5ths of a second of frozen video.

This is exascerbated for higher framerates and GOP sizes. For example if we have 25 frames in a GOP and 25 frames per second, if we wanted to reduce it to 5 frames per second, we'd have to keep the i-frame and 4 subsequent p-frames, then discard the next 20 p-frames. But this means that although we now have 5 frames per second, they are all crammed into the first 1/5th of every second! Not really the desired effect.

For this reason, Wavestore doesn't support doing this. Generally if you set a lower recording framerate than the stream framerate, Wavestore will tend to discard all p-frames to avoid corrupting the stream.

It's still possible and fairly useful to configure boost in this case but the frequency of i-frames needs to be considered. For example if you want to boost from 1 fps to 25 fps, ensure you have 1 i-frame every second.

9.12.3 Effectiveness of Framerate Boost with H.264

Staying with the 25fps example, how much storage space would we save by reducing the framerate from 25 to 1?

If we use the frame sizes from our test camera the 25fps stream would be approximately...

$$110KB + (24 \times 6KB) = 254KB/s$$

...whereas a 1fps stream would be...

$$110KB/s$$

Therefore going from 25fps to 1fps reduced our storage to 43% of its normal size.

What if we wanted to go from 25fps to 3fps instead? Well, as described above, you would need to configure the stream to contain 3 i-frames per second, so a GOP size of 8.

In this case the 25fps stream would be:

$$(3 \times 110KB) + (22 \times 6KB) = 462KB/s$$

...and the 3fps stream would be...

$$3 \times 110KB = 330KB/s$$

So we've had to significantly increase the data rate of our 25fps stream to enable the extra i-frames, and now our 3ips stream takes even more space than the 25fps stream with the GOP size of 25 in the previous example.

So framerate boost is a useful feature for space saving, but the required configuration needs to be considered carefully as a poor configuration can end up using even more storage space than normal continous recording.

9.13 Configuring Storage Devices

9.13.1 Configuring and Managing HyperRAID™

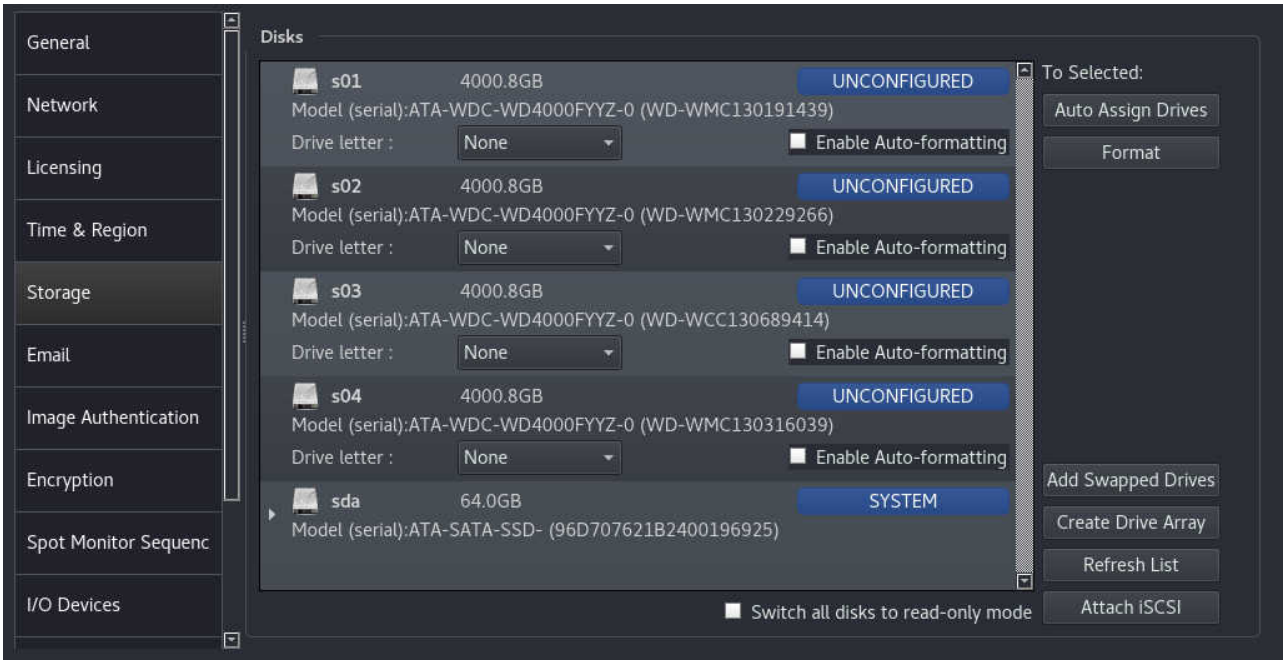
The unique HyperRAID™ architecture in Wavestore provides cost–effective redundancy in storage arrays whilst performing faster than traditional RAID without requiring a traditional hardware RAID card to operate. This technology is compatible with a wide range of Wavestore servers.

Creating a HyperRAID™ Array

Here we will describe the process of creating a HyperRAID™ array from 4 disks. There will be 3 ***data disks*** and 1 ***parity disk***.

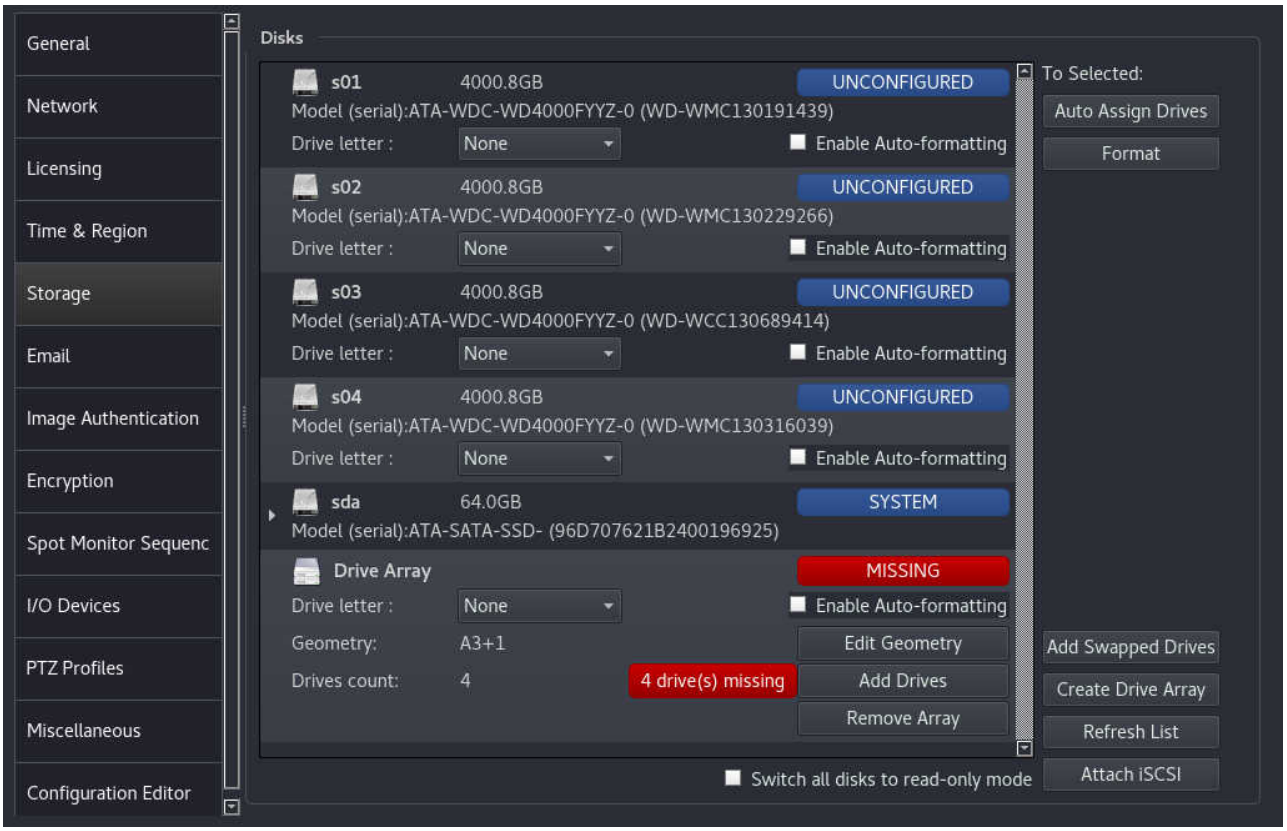
The number of parity disks defines how many disks in the array can fail without any data in the array being lost. So in this case, 1 disk can fail and no data is lost. However it's important to replace the failed disk and give the system time to rebuild the array, otherwise if another one fails before the rebuild is complete, all the data in the array is lost. The good news is that Wavestore offers up to N+5 redundancy, meaning up to 5 parity disks per array.

If we have 4 unconfigured disks, the Storage setup screen (*View* → *Setup* → *Server* → *Storage*) will show something similar to the below screenshot:



Click 'Create Drive Array' to open the 'Array Geometry Editor'. This is where you can configure the structure of the array to be created.

Click 'Add' and set the desired number of data and parity disks, then click OK.



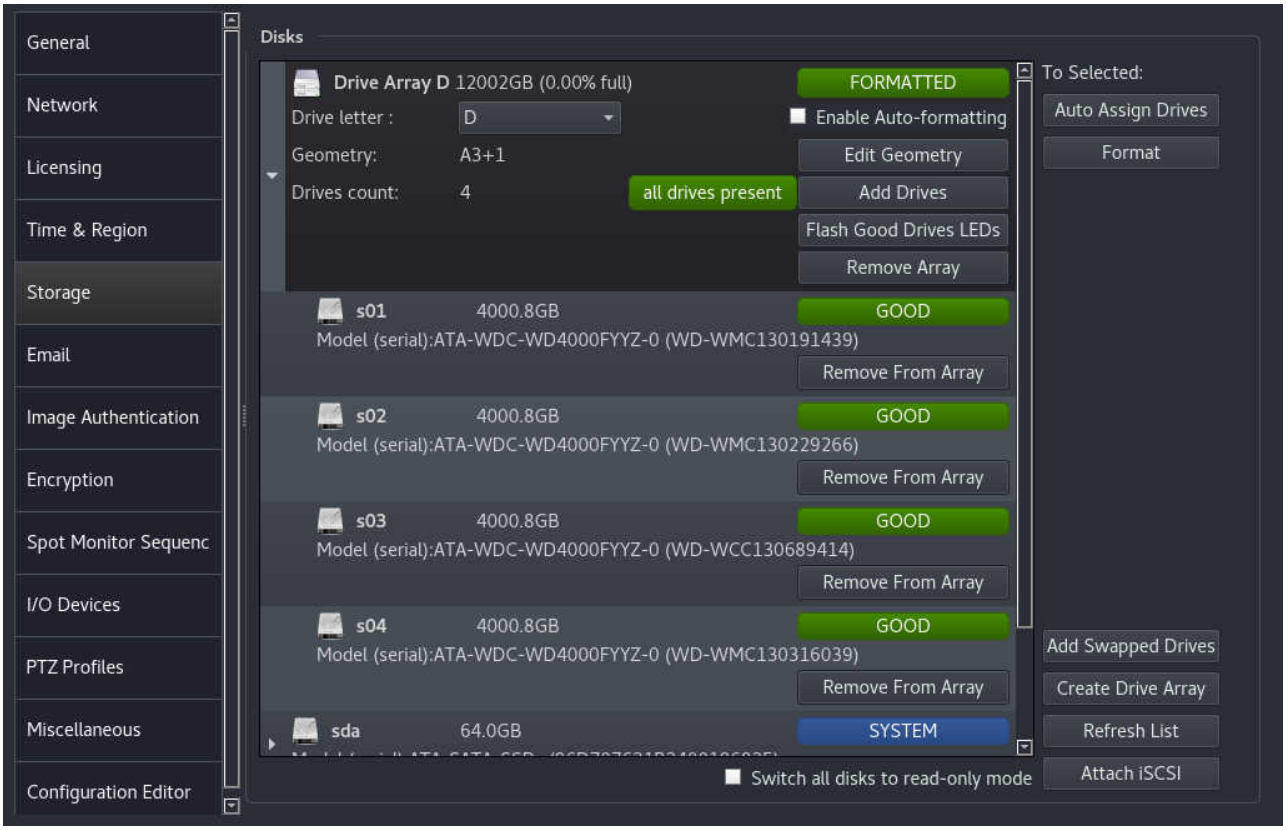
Now we have an 'empty' Drive Array. We need to chose which disks are members of this array. There are two ways of doing this:

- Drag and drop the 'Unconfigured' disks onto the array with the 'missing' drives.
- Click the 'Add Drives' button within the Drive Array and select them from the presented list.

Only local disks can be added to the drive array. You cannot build a HyperRAID array from multiple network or cloud drives.

Once the array has all the required drives assigned, we need to assign a 'Drive letter'. In this case we assign drive letter 'D' and click Save.

At this point the array has been created, but is not formatted. So the final step is to select the array and click 'Format', then confirm the request to format.



Now the setup is complete. We have a formatted array with 'all drives present'. We can click the arrow next to the array to see the members of the array and their statuses as shown in the screenshot above. We can now assign camera recording tracks to Disk D to use the array.

9.13.2 Configuring and Managing MegaRAID

If your Wavestore server has a MegaRAID® hardware RAID controller card installed, the WaveView software provides tools to configure and manage those RAID arrays.

There are two main methods of doing so:

Managed by MegaRAID® tools

In this mode, the RAID arrays are created outside of Wavestore and simply appear to Wavestore as a single disk. Wavestore provides the 'storcli' command to allow remote administration as per the manufacturer's instructions. This can be performed with the Execute Command tool (*Tools → Execute Command*).

Creating the arrays can be done in different ways and varies by system. Sometimes it can be done via the BIOS–like menus available on starting the system, or it can be done via the 'storcli' command–line tool.

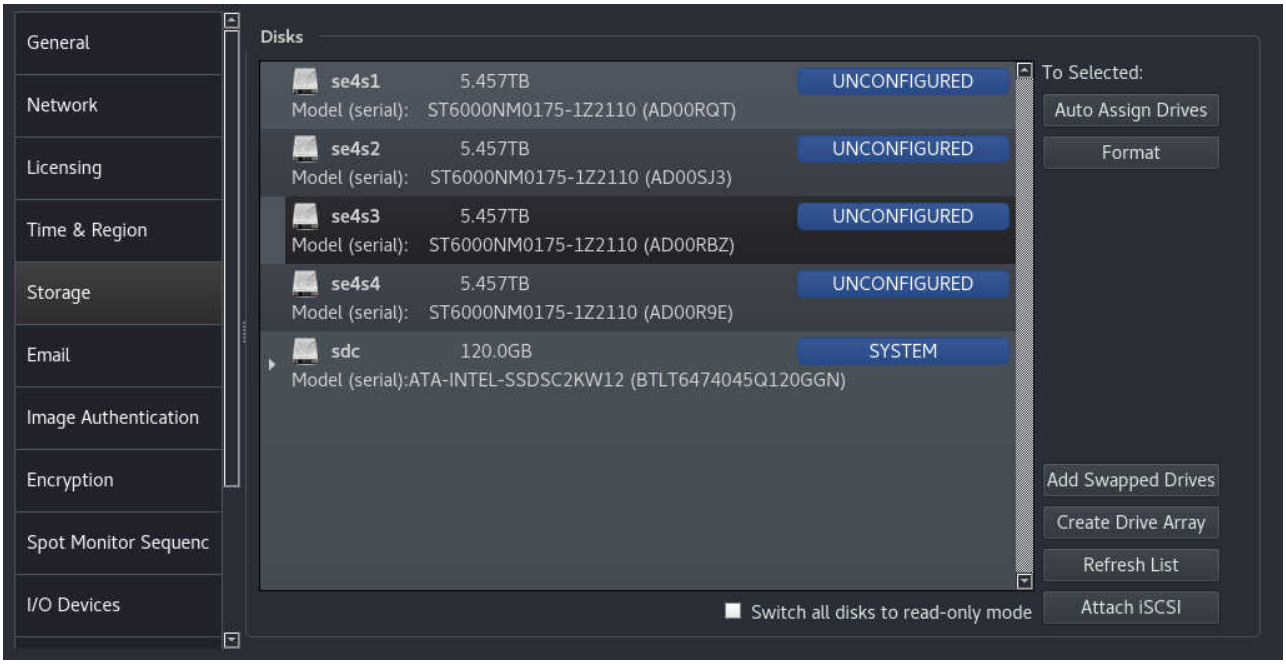
Managed by Wavestore

Wavestore can be used to manage the RAID arrays via the WaveView user interface. This will occur if the arrays are created using the WaveView user interface.

This section will focus on the case where the arrays are managed by Wavestore.

Creating a MegaRAID array

When various disks are available on the RAID controller but not set up yet, they will appear as UNCONFIGURED in the Storage setup screen.



To create a RAID array, click on the 'Create Drive Array' button. This allows one or more disk groups to be added, each of which can be a RAID array. Click 'Add' to add a disk group, and select how many data disks (N) and how many parity disks (P) are required. A single parity disk is called N+1 or by the RAID

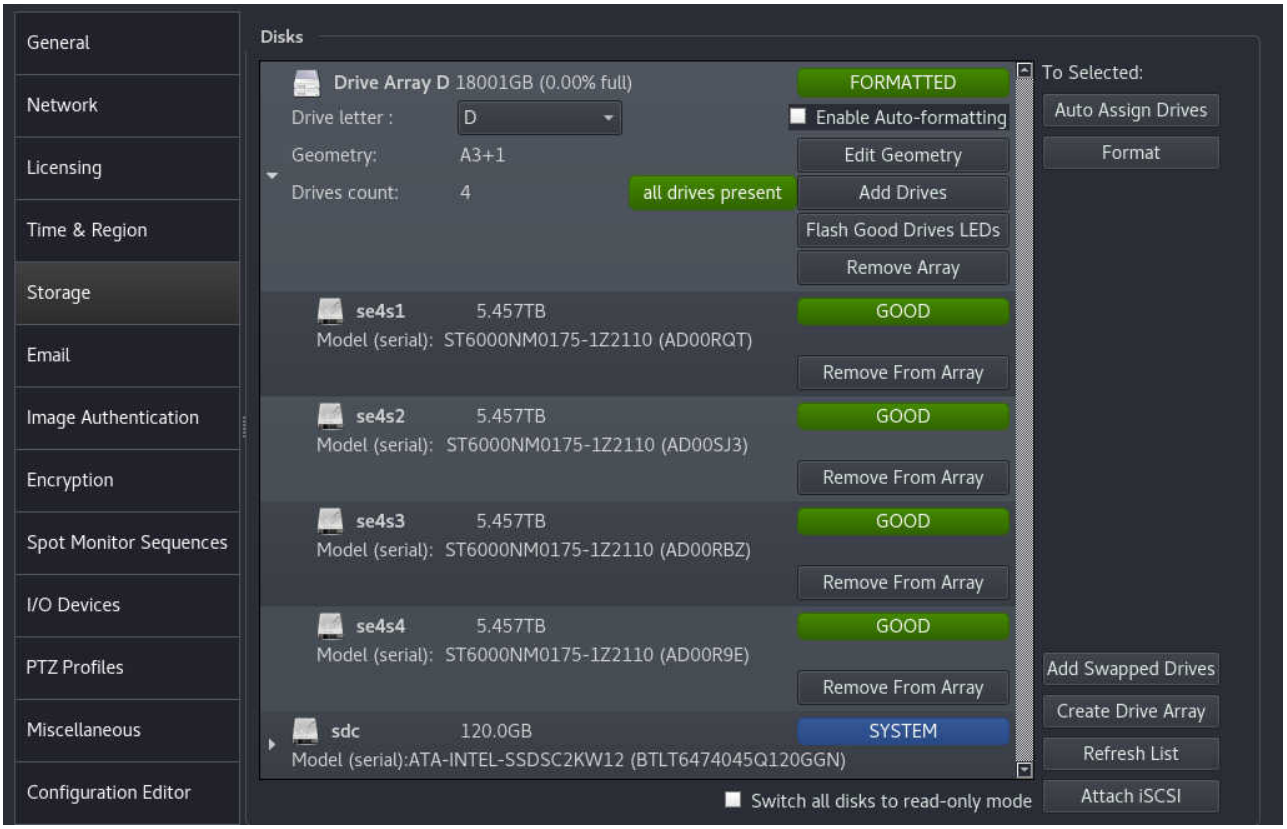
term 'RAID5', and two parity disks are called N+2 or 'RAID6'. Most hardware RAID controllers allow up to 2 parity disks.

Next, add the UNCONFIGURED disks to this RAID array. Disks can be added by dragging them onto the array, but for large numbers of disks it's easier to click on "Add Drives" and then select them from the list: click on the first drive and drag the mouse over all the others to select all, then click OK.

Give the Drive Array a Drive Letter (e.g. "D") and click Save.

When first added, the drive might be shown as MISSING. Click "Refresh List" to refresh the list and show the newly created drive array. It is necessary to format it at this point, so select it and click 'Format'.

Your drive array is now ready for use.



In current versions of the software, only two RAID arrays with different letters can be set up by this method. If it's necessary to configure the system in other ways, see the MegaRAID® Configuration Commands section below.

Note: MegaRAID is a trademark or registered trademark of LSI Corporation in the United States and/or other countries.

Deleting or Changing MegaRAID Arrays

To change the RAID type or number of drives after the arrays have been created, it is necessary to delete and recreate them. This will require reformatting and will cause a total loss of data. If you do change the RAID format, the Wavestore server will not automatically delete the old RAID array.

When using Wavestore to manage the MegaRAID arrays, if you remove the array in the Storage setup screen, the array will no longer be managed by the Wavestore, however it is not actually deleted.

To explicitly delete the array it is necessary to use the 'storcli' command-line tool. This is performed by running commands via the 'Execute Command' tool (*Tools → Execute Command*).

To delete all volumes on the RAID controller (**WARNING: doing this loses all your video footage!**), execute the following command:

```
storcli /call/vall del
```

Alternatively, it's possible to delete a specific "volume". First, determine the volume ID for the desired volume. To list all "volumes":

```
storcli /call/vall show
```

This will show something like the following:

```
---------------------------------------------------------------
DG/VD TYPE State Access Consist Cache sCC Size Name
---------------------------------------------------------------
0/0 RAID5 Optl RW No RAWBD - 16.372 TB DiskArrayD
---------------------------------------------------------------
```

In this case the number under VD is 0 which is the volume ID. So now we can delete volume 0... **WARNING: doing this loses all video footage on that volume!...**

```
storcli /call/v0 del
```

Replacing a failed disk in a MegaRAID array

When a disk within a RAID array fails, the array itself will enter a DEGRADED state, and this is indicated in the Disks Setup screen, as well as the System Log.

Usually, although dependent on the hardware, the disk caddy itself will either show a red light or no lights at all.

When the disk has been replaced with a new disk, it is necessary to tell the RAID controller to re-incorporate the disk. To do so:

- Go to *View → Setup → Server → Storage*
- Select the degraded RAID array

- Click the 'Add Swapped Drives' button

After a short period of time, refresh the disks list and the state should change to REBUILDING. If further information or inspection is required the 'storcli' tool can be used.

Note that if a disk is moved from one MegaRAID system to another it will show a status of FOREIGN. The 'Add Swapped Drives' will remove this FOREIGN status and incorporate the disk into the degraded array.

9.13.3 Configuring iSCSI Storage Devices

iSCSI devices are configured in the Storage setup screen (*View* → *Setup* → *Server* → *Storage*). The 'Attach iSCSI Devices' button opens the 'Search for iSCSI Devices' screen:

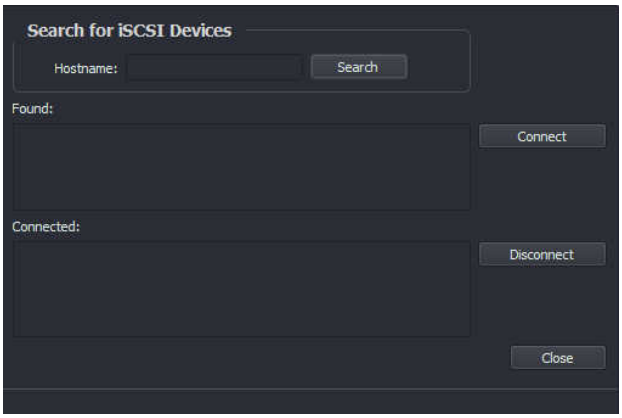


Figure 9.4: Search for iSCSI devices screen

To attach an iSCSI device, first we need to find it via its IP address. So enter the IP address of the iSCSI device, and click Search.

Figure 9.5: IP address of iSCSI device entered

If the device is successfully found, it will be listed in the 'Found' window.

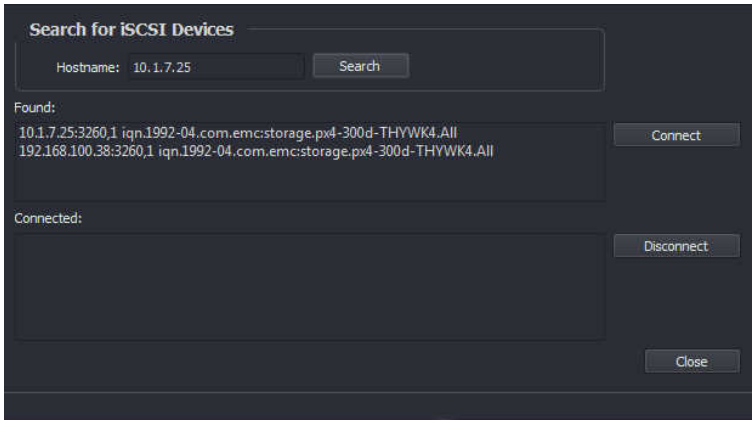


Figure 9.6: Networked iSCSI devices located

To then connect to that device, left–click to highlight it and click 'Connect':

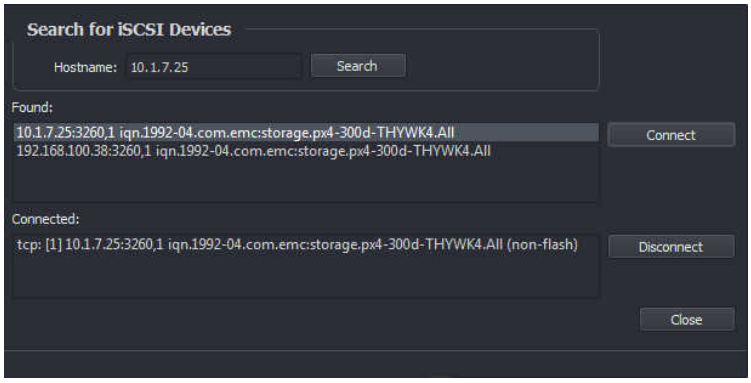


Figure 9.7: Connected to iSCSI device

If the connection is successful, the device will appear in the Connected list.

The device can then be assigned a drive letter and formatted to make it ready for use:

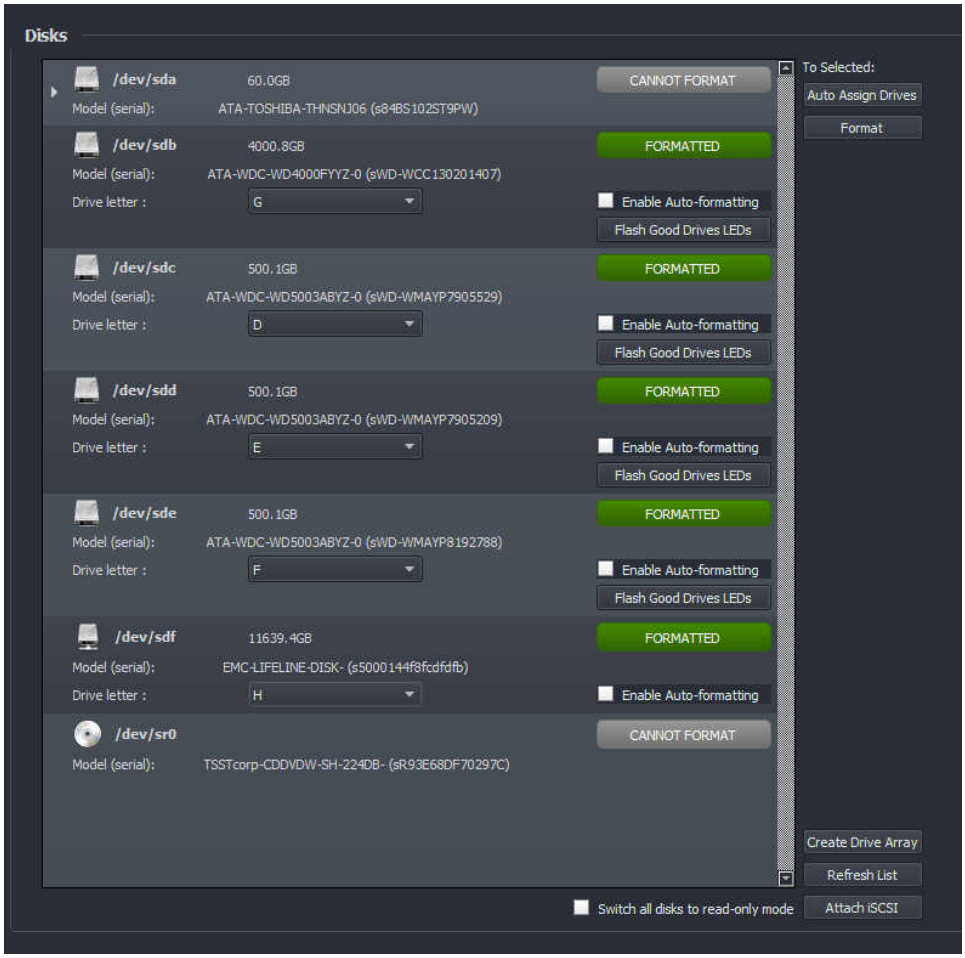


Figure 9.8: Disks screen – new iSCSI device (Drive F) shown in list of Disks

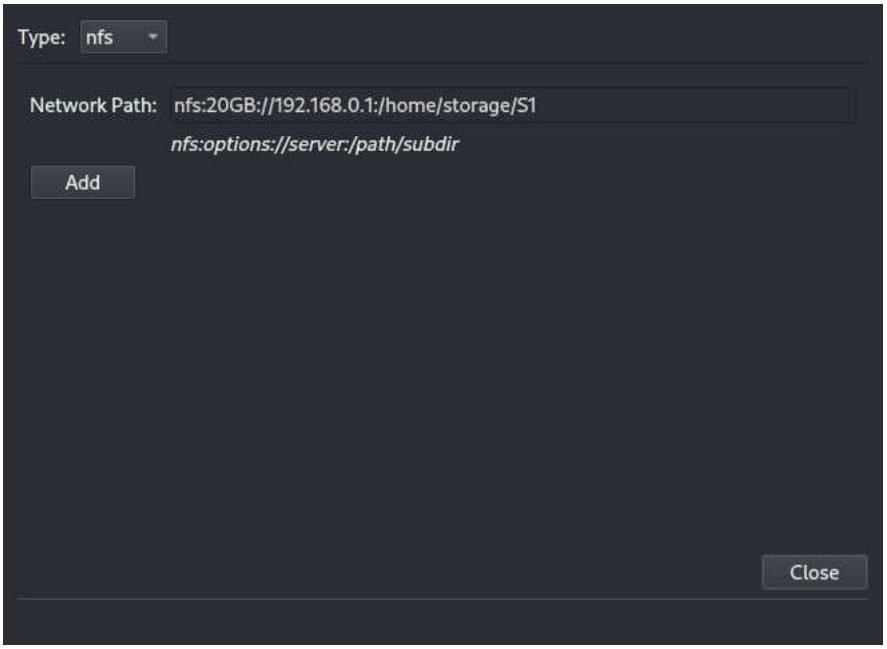
iSCSI devices should be managed using the tools provided with the device itself. Wavestore can only connect to the device, use it, and report any issues when communicating with it. The device will be treated in the same way as in individual disk.

9.13.4 Configuring NFS Storage Devices

Wavestore can store video in files on an NFS (Network File System) target.

Note the Wavestore will need to have been installed with the version 6.16 or later to get the latest OS packages which are needed for NFS; it cannot be installed with an earlier version 6 and upgraded.

To add an NFS device, go to *View > Setup > Server > Storage* and click *Attach Network Storage*. From the *Type* drop-down, select "nfs".



Enter the required details as described below, then click *Add* to attach to the device. If successfully added, assign a disk letter in the Storage screen and save the changes to make the device usable.

As described on-screen, it is necessary to add a Network Path in the format...

`nfs:<options>://<nfsserver>:/<nfspath>/<directory>`.

`<options>` can contain a size and optionally other mount options: eg, 16GB or 2TB,noac,noatime. If mount options are omitted then noac,noatime will be used and usually no special options are required. A size field is always required.

`<nfsserver>` is the server address, e.g. `192.168.0.1`

`<nfspath>` is a path on the server, e.g. `/home/storage`

`<directory>` is a directory within the NFS export so more than one server can use it. Typically it is `S` followed by `1..99`, e.g. `S1`.

For example:

`nfs:20GB://192.168.0.1:/home/storage/S1`

This will mount `192.168.0.1:/home/storage` as an NFS share, and access footage within the S1 directory, using up to 20GB of space.

Notes

Resizing

Currently once a size has been set, it cannot be changed due to the index structure.

Failover Notes

Normally each server has its own /S1 or /S2 directory. In future we will allow "/Sn" to be configured as the directory part, which will allow a Standby server to take over the correct directory replacing n by logical server number. This will only be available in Ultimate licence, and is not yet available. If this feature is not available, the standby should be configured to use its own directory, eg, /S99, and the footage will be available by redirection as normal after the main server has come back up.

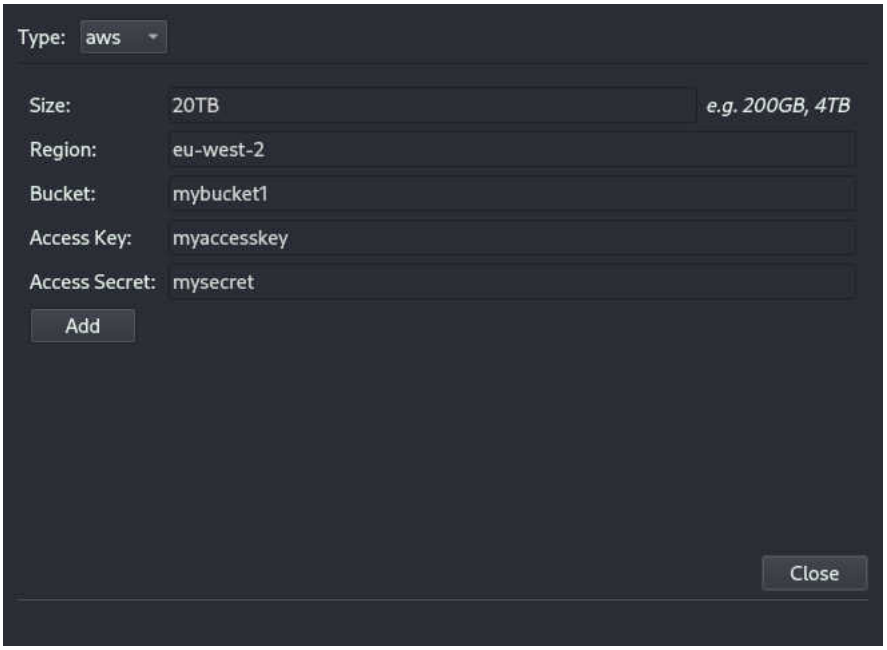
Format Button

An NFS volume is not a disk, so "Format" will not format it. The operation of adding the device prepares the device appropriately.

9.13.5 Configuring AWS Storage Devices

Wavestore can store video in files on an AWS (Amazon Web Services) target.

To add an AWS target, go to *View > Setup > Server > Storage* and click *Attach Network Storage*. From the *Type* drop-down, select "aws".



Enter the required details as described below, then click Add to attach to the device. If successfully added, assign a disk letter in the Storage screen and save the changes to make the device usable.

As described on-screen, it is necessary to add several parameters.

`Size` specifies the space reserved on this device: eg, 16GB or 2TB.

`Region` is the region as specified by your AWS account

`Bucket` is the name of the storage bucket as provided by AWS

`Access Key` is part of the authentication credentials and should be provided by AWS

`Access Secret` is part of the authentication credentials and should be provided by AWS

Notes

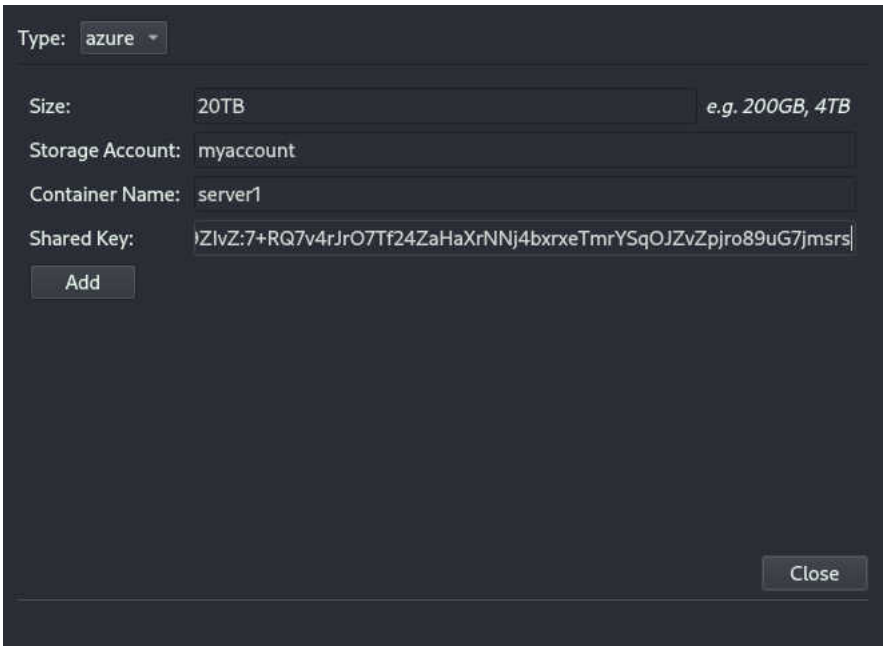
Resizing

Currently once a size has been set, it cannot be changed due to the index structure.

9.13.6 Configuring Azure Storage Devices

Wavestore can store video in files on an Azure target.

To add an Azure target, go to *View > Setup > Server > Storage* and click *Attach Network Storage*. From the *Type* drop-down, select "azure".



Enter the required details as described below, then click Add to attach to the device. If successfully added, assign a disk letter in the Storage screen and save the changes to make the device usable.

As described on-screen, it is necessary to add several parameters.

`Size` specifies the space reserved on this device: eg, 16GB or 2TB.

`Storage Account` is the account name as provided by your Azure account

`Container Name` is the name of the storage container as provided by Azure

`Shared Key` is part of the authentication credentials and should be provided by Azure

Notes

Resizing

Currently once a size has been set, it cannot be changed due to the index structure.

9.13.7 Configuring Sequential Recording and EcoStore®

The 'traditional' way of configuring recording in Wavestore is to set up either a single large recording volume, for example a RAID array, and record everything to that volume. Or, if there are 4 disks and 100 cameras for example, to record 25 cameras to each disk.

Version 6.14 introduced new functionality whereby recordings can occur to disks or groups of disks in sequence. These are known as 'Disk Groups'. When suitably licensed, Wavestore can 'spin down' these disk groups, meaning significant reduction in power consumption.

For example, if there are four disks, ***s01***, ***s02***, ***s03***, and ***s04***, the Wavestore can be configured such that it will start recording to ***s01 only***. Once ***s01*** is full, it will move to ***s02***, and so on. The disks which aren't currently in use can be spun down to save power.

If spindown is enabled and the user needs to access recordings which are on a spun-down disk, the system will automatically spin up the disk, although this can take a few seconds. The disk will then stay spun up until it has been inactive for a period of time.

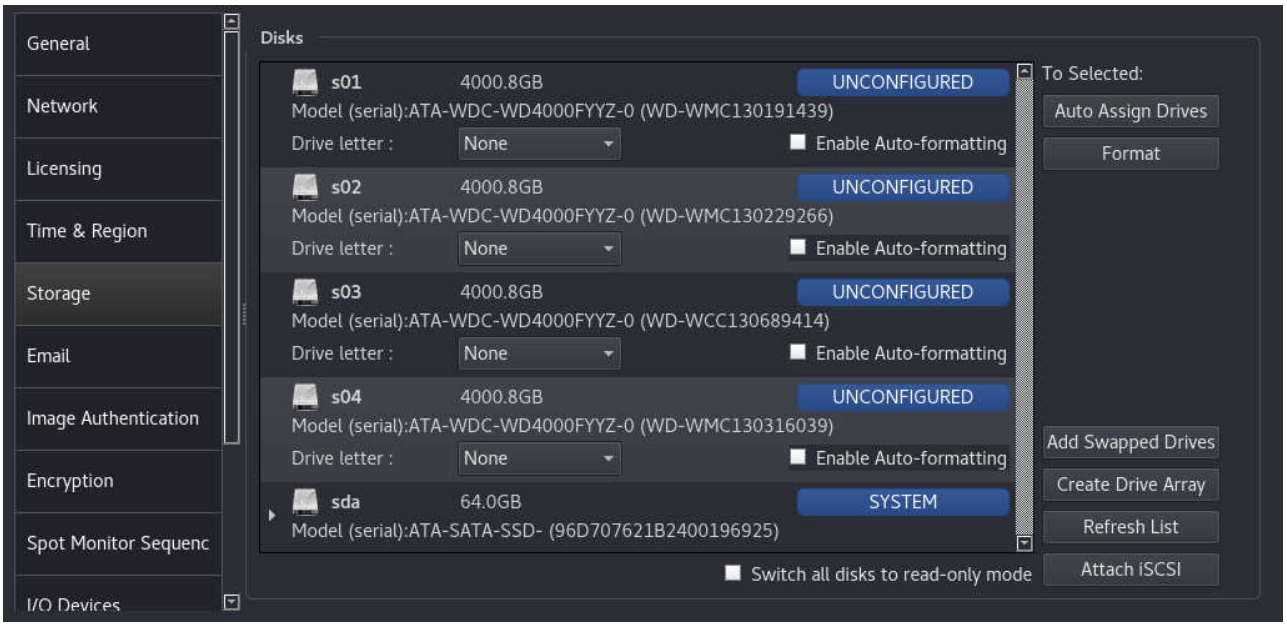
The same principle can be used in conjunction with the HyperRAID™ system. For example, each disk group could be a HyperRAID™ array and the unused arrays will be spun down.

Note that EcoStore® functionality is not compatible with MegaRAID disk controllers.

Configuring a Simple Sequential Array with EcoStore®

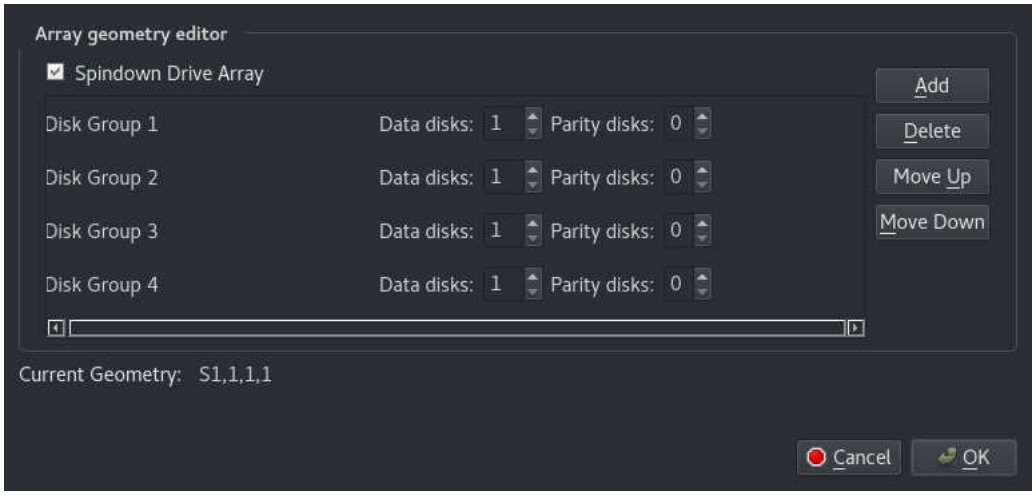
To enable sequential recording we simply need to create an array with multiple 'disk groups'. Here we will take a fresh system with 4 disks and create a single sequential array with the EcoStore® spindown mode enabled.

We start with a system that has 4 unconfigured disks...

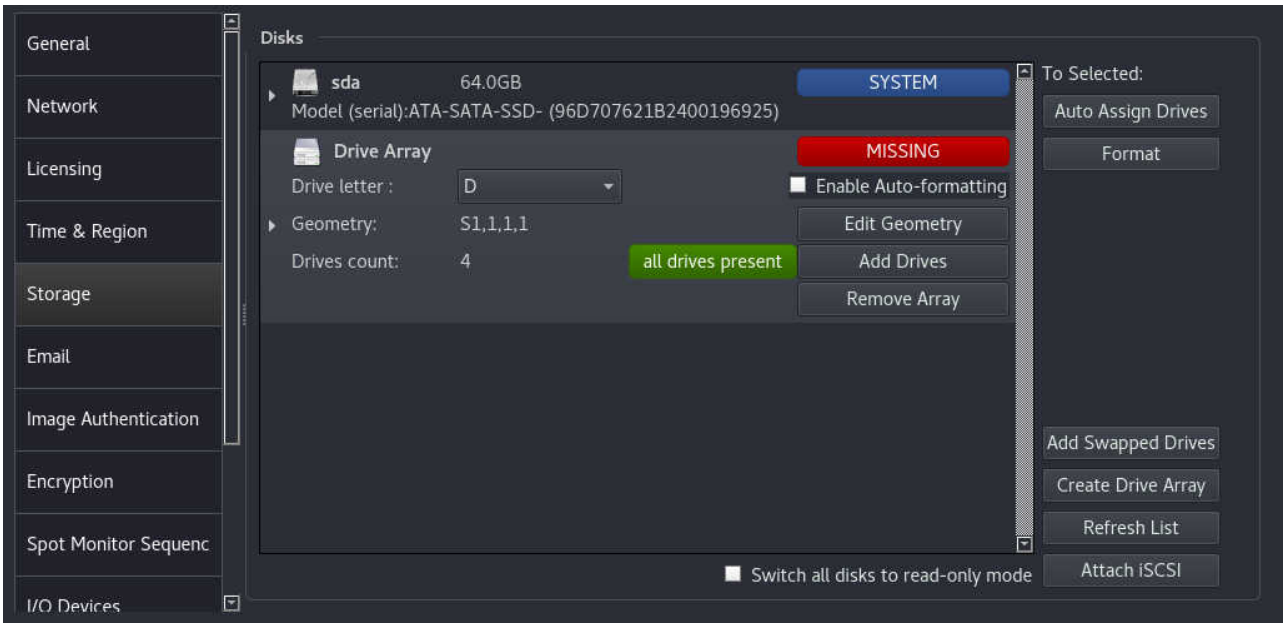


Click 'Create Drive Array' to open the 'Array Geometry Editor', then click Add four times to create four 'disk groups' each with one ***Data disk*** and zero ***Parity disks***.

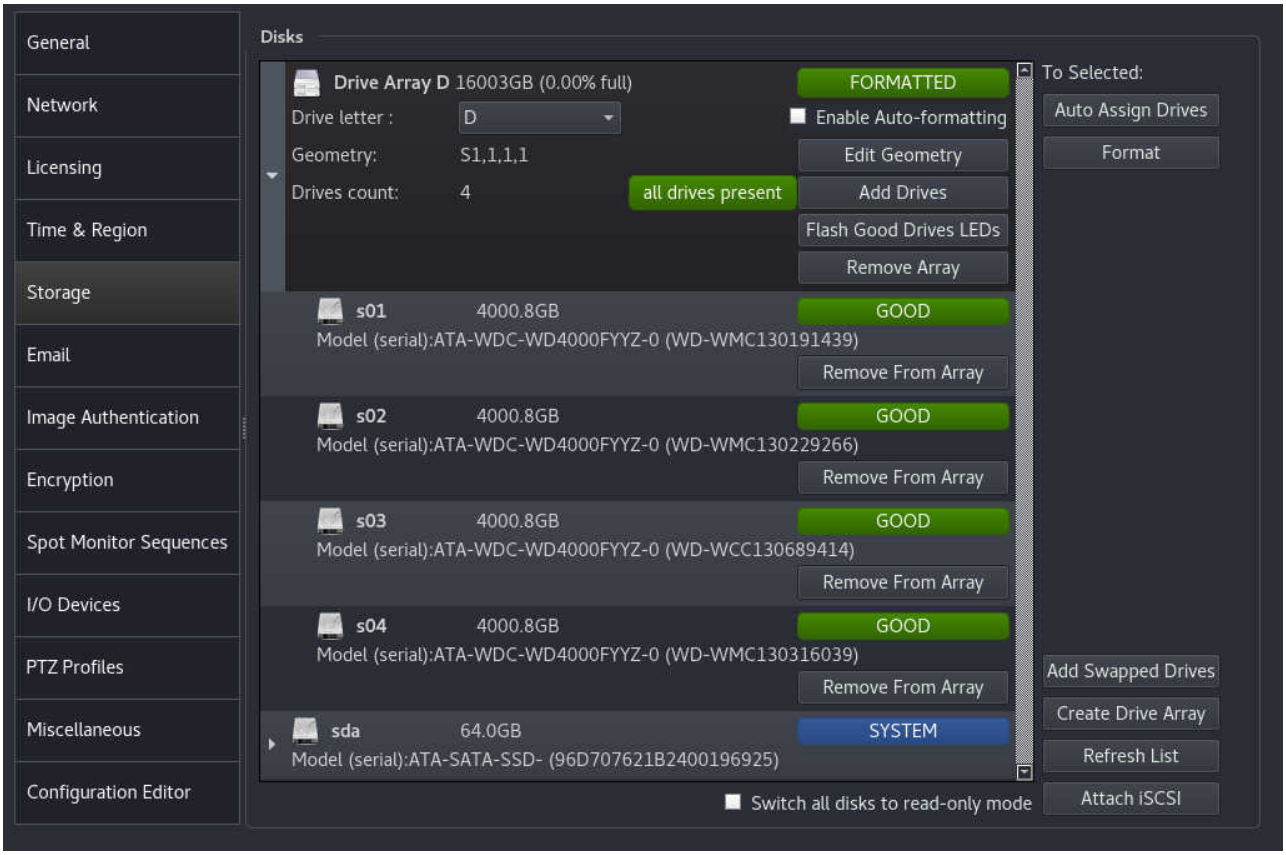
The 'Spindown Drive Array' option enables the EcoStore® function where any 'disk group' not currently in use will be switched into a low-power mode whenever possible, saving energy and heat output. This feature is only available in certain licence levels and hardware configurations.



Once the array gemoetry has been confirmed, click OK then set a Drive letter and save the changes. The array will then be created, however it may show as MISSING...



The final step is to Format the array, it should then show FORMATTED in green. Click the arrow next to the array to inspect its members and their status...



The array is now available to be used for recording.

9.13.8 How To Recover From Disk Faults or Removed Disks

If a disk has a fault or is accidentally removed, it will show as FAULT or MISSING in the Storage setup screen. Some disk faults will cause the disk to show as MISSING rather than FAULT because it has failed in such a way that it is not possible to detect the disk at all; both states are treated in a similar way by the software.

If a HyperRAID array has a disk with a disk fault, it is necessary to replace the faulty disk with a new one and click the "Add Swapped Drives" button to force the system to recognise the changed disk. After the failure the array will show as DEGRADED until this replacement occurs, and REBUILDING after the replacement (after a few seconds). After the rebuild has completed it will show as FORMATTED. It should be usable throughout this time and no data will be lost. The same applies if a disk was accidentally removed and reinserted.

If a single disk has a disk fault, data might be lost. It will usually be necessary to replace by a new disk and reformat it before it starts working again. This will result in loss of footage on the failed disk.

If a single disk was accidentally removed, and is replaced while the power is still on, it will still show as FAULT or MISSING. If the "Add Swapped Drives" button does not force it to be recognised, the recommended technique is to change the disk drive letter to another letter (eg, Z) and Save, then change it back to the desired letter (eg, D) and Save. This configuration change will cause the Disk subsystem for that disk to reset and forget it was faulty. It will probably show as UNFORMATTED at first (to encourage formatting of any newly added drive), and the "Add Swapped Drives" will then re-read it and show it as GOOD (providing there is no other fault).

If moving a disk (or entire array) from one machine to another, it will behave in a similar way. It will usually show as UNFORMATTED at first (to encourage formatting of any newly added drive), and "Add Swapped Drives" will then re-read it and show it as GOOD (providing there is no other fault).

9.14 Accessing Wavestore Server from Client PC

9.14.1 PC Requirements

Minimum

- 4th Generation Intel® Core™ i3-4170 or better
- 2 GB of RAM or better
- 80 GB hard drive for Windows OS and WaveView
- Integrated graphics card
- 100 Mbps Ethernet network interface card

Recommended

- 4th Generation Intel® Core™ i5-4670 or better
- 4 GB of RAM or better
- 64-bit operating system
- 120 GB Solid State Drive for Windows OS and WaveView
- GbE network interface card
- NVIDIA® GT 730 2GB video card

High performance (Video intensive configuration)

- 5th Generation Intel® Core™ i7-5820K or better
- 16 GB of RAM or better
- 64-bit operating system
- 120 GB Solid State Drive for Windows OS and WaveView
- GbE network interface card
- NVIDIA® GeForce® GTX 970 4 GB video card

9.14.2 WaveView Client Software installation process on a Windows PC

WaveView allows all user functions, and most installer configuration functions to be carried out from a PC.

The WaveView installer is provided on the installation DVD but is also available from our website. The installer for Windows is only provided in a 64-bit version, named 'WaveView-6.xx.xx-win64.exe', where the "xx" can vary depending on the version.

It is recommended to use the same base version of WaveView client as the server, or higher. By "base version" we mean the first two numbers, for example the base version of "6.14.51" is "6.14". So for example if the server is running version 6.16, the WaveView client version should be 6.16 or higher.

The WaveView installer is similar to those for most Windows applications with a few installation options which are detailed below:

- System Path – the WaveView installer also includes some command–line tools. If you wish to use these it is recommended to add the WaveView installation directory to the system path. This option will do so if selected, but it can also be done manually later if desired.
- Create Desktop icon for WaveView

In the 'Choose Install Location' screen, select the destination folder for the WaveView installation.

Once the installation process has completed, click on 'Finish' to close the Install Wizard.

Figure 9.9: WaveView Desktop shortcut icon

To connect to your server, click on the desktop shortcut to launch the program; the WaveView screen will appear as below.

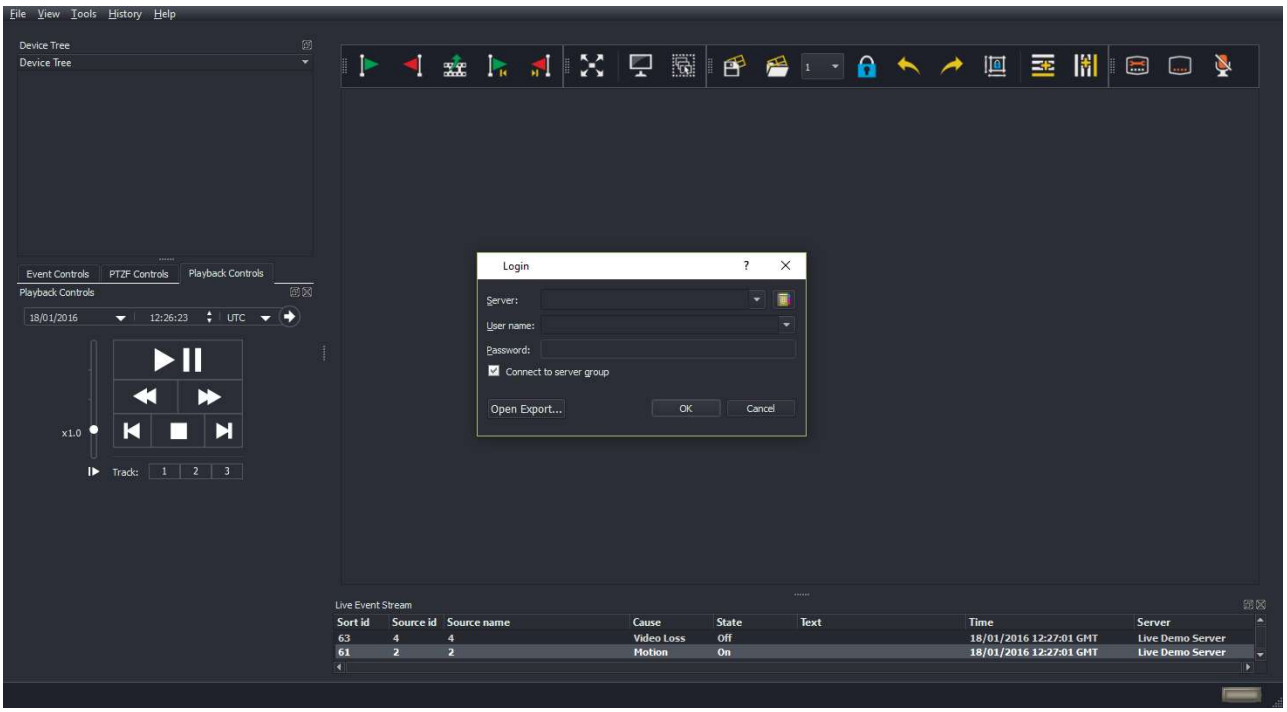


Figure 9.10: WaveView launch screen

To connect to your server, enter the following details in the login screen:

Server: IP address of server

User Name: valid user logon ID – default is 'install'

Password: valid user password – default is 'a'

9.15 Server Group Configuration Conflict Resolution

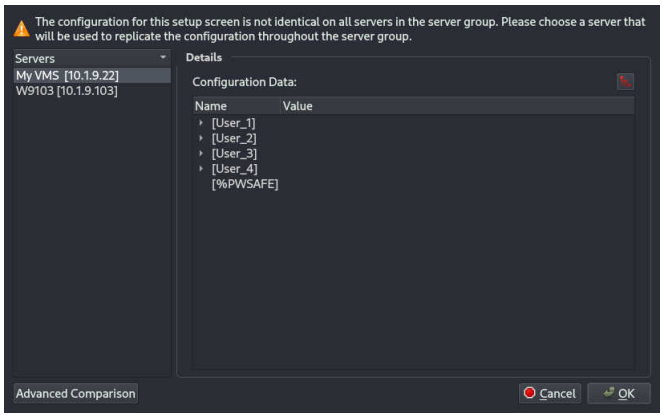
When accessing a setup screen which pertains to a server group, if there are inconsistencies between the configuration on different servers within the group, a Conflict Resolution Tool will appear asking for the operator to choose the server with the correct configuration.

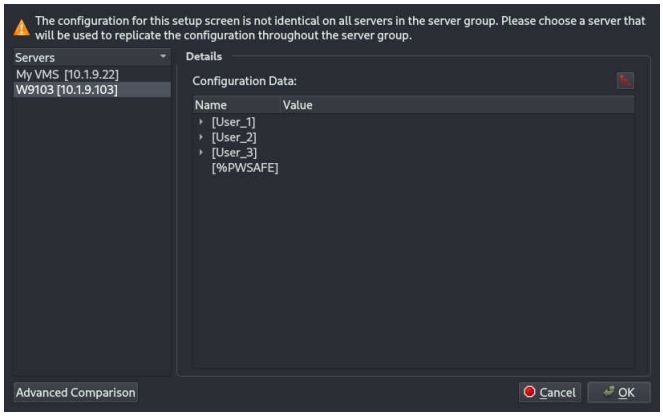
Note that this tool only pertains to the current setup screen. There may be other conflicts in other screens. If there is a conflict on one screen (e.g. *'Users'*) it is advisable to check all the other setup screens in case they also have conflicts.

To resolve the conflict, simply select the server with the correct configuration from the list on the left, then click OK. The configuration for this server will then be synchronised to the other servers in the group.

If there is uncertainty about which server is correct, or why there is an inconsistency, the Conflict Resolution Tool provides some facilities to help understand.

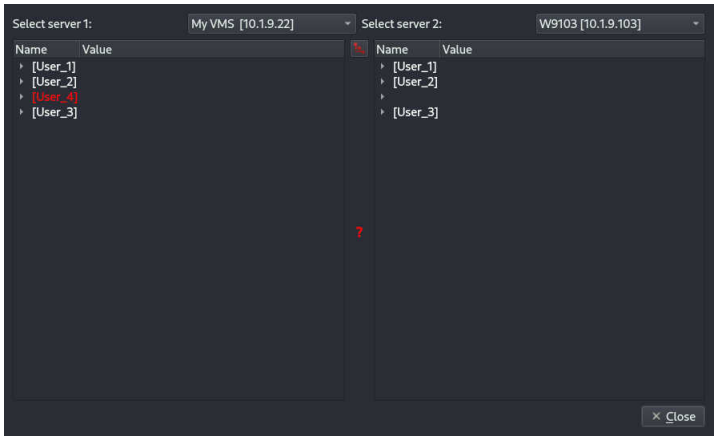
For example, in the screenshots below, we click on each of the server names and see the relevant configuration sections for each of the servers.





It's fairly apparent here that the first server has 4 users, and the second server has 3 users.

If it's still not clear what the difference is, we can click *'Advanced Comparison'* to compare the configuration in a different way. As we select different servers, the centre of the UI will either show a white equals sign ('=') if both servers have identical configuration, or a red question mark ('?') if they do not.



Here we can see clearly that the [User_4] section is present on the server on the left, but not on the server on the right, as indicated by the red question mark between the two configurations.

The drop-down menus at the top allow servers to be selected, so that any servers within the group can be compared.

Once the issue is understood, back in the main Conflict Resolution Tool window, select the server with the correct configuration, and click OK.

9.16 Reinstalling Wavestore Server Software

In the event that the Wavestore software needs to be reinstalled on the server, this can be easily carried out, either by using the Wavestore DVD supplied with each new Wavestore server, or by creating a new DVD or bootable USB memory stick.

To obtain the latest Wavestore installer, contact the Wavestore Support Team who can provide a download link for the ISO image of the software.

If choosing to do the re-installation by DVD, download the ISO image file and burn to a DVD. On modern versions of Microsoft Windows (8.1 and later) this can be performed by right-clicking the ISO file name and selecting 'Burn Disc Image'. Alternatively, DVD writer software such as Nero or Roxio can be used.

To install or upgrade Wavestore from a USB memory stick it is necessary to extract the ISO to the USB stick. The way to do this depends on the Operating System. Most commonly Microsoft Windows is used, in which case the Rufus program is recommended.

Assuming the installation ISO has already been obtained, the process is as follows:

- On Windows, download Rufus from `http://rufus.akeo.ie`
- Run Rufus.
- Plug in the USB stick. Rufus should recognise the USB and populate the "Device" box.
- On Rufus: "Format Options"/"Create a bootable disk using" and select "ISO Image".
- On Rufus: click the icon to the right of the above text and select the ISO.
- On Rufus: click [Start] to start the write to USB.
- Select "Write in ISO Image mode (recommended)" and click OK if Rufus asks about deleting files on the USB stick.
- It'll take a few minutes to create the bootable USB.

9.16.1 Reinstallation Preparation

Note: UEFI/EFI mode is not currently supported. Many motherboards use this as the default so it may be necessary to change your BIOS settings to use "Legacy" mode rather than UEFI/EFI.

In addition to the install media (DVD or bootable USB stick), you will also require a USB device with a saved copy of the current server configuration file (see section 6.2.14 –).

It is also advisable to make a note of the server Licence and Machine ID, whether you saved the configuration or not.

9.16.2 Reinstallation Procedure

Before starting the installation it is necessary to decide whether to record video to the operating system disk. This is generally discouraged, particularly if the operating system disk is an SSD.

It is usually only advisable to record to the operating system disk if there are no other disks in the system. The default installation option assumes that you will not record to the operating system disk. It is not possible to change this after installation so re-installation will be necessary to change it.

- Connect a keyboard and mouse to the server.

- Shut down the server (menu path View → Setup → Server → General → Shutdown System)
- If installing from USB, insert the USB stick and power up.
- If installing from DVD, power up the server and insert the installation disc in the DVD drive.
- The system should now boot from the DVD or USB device, and display the installation menu.

There are now several choices of installation type:

Install Wavestore from DVD This will begin a default installation from the DVD drive. No video storage partition will be created on the operating system disk so all recording will be to separate disks.

Install Wavestore from USB This will begin a default installation from the USB drive. No video storage partition will be created on the operating system disk so all recording will be to separate disks.

Advanced Options This opens another menu with further, less common, installation modes.

The Advanced Options menu presents further installation modes as described below:

Install Wavestore from DVD with data partition This will begin an installation from DVD with a video storage partition configured.

Install Wavestore from USB with data partition This will begin an installation from USB with a video storage partition configured.

Unattended Wavestore Install from DVD This will begin a default installation from the DVD drive. No video storage partition will be created on the operating system disk so all recording will be to separate disks. No warning messages will be offered before overwriting the operating system disk.

Unattended Wavestore Install from USB This will begin a default installation from the USB drive. No video storage partition will be created on the operating system disk so all recording will be to separate disks. No warning messages will be offered before overwriting the operating system disk.

Rescue installed system This is a special mode used to recover a faulty system and should only be used under guidance from Wavestore support staff.

Memory test This performs a test of the system memory to check for faults.

Once the installation procedure has completed, remove the ejected install DVD or USB stick, and select Reboot

The system will restart and examine the server hardware. During start up, you will be prompted to select the Graphics Card configuration (press Enter), and the unit will then reboot once again.

Once the server has restarted, login using the following details:

Server: localhost

Username: install

Password: a

To complete the installation, either load the previously saved configuration file as described in section 6.2.14 – , or manually enter the server licence details as described in section 6.2.3 – Licensing.

9.17 Accessing a USB disk on the Wavestore server

It is often useful to access a USB memory stick or hard disk, for example to make exports or save configuration files. Doing so is a little different on a Wavestore server when compared with a Windows PC.

Upon inserting a USB device, the file browser should open automatically with the contents shown. If not, move the mouse to the top-left corner and click the filing cabinet icon, as shown below, to launch the file browser.

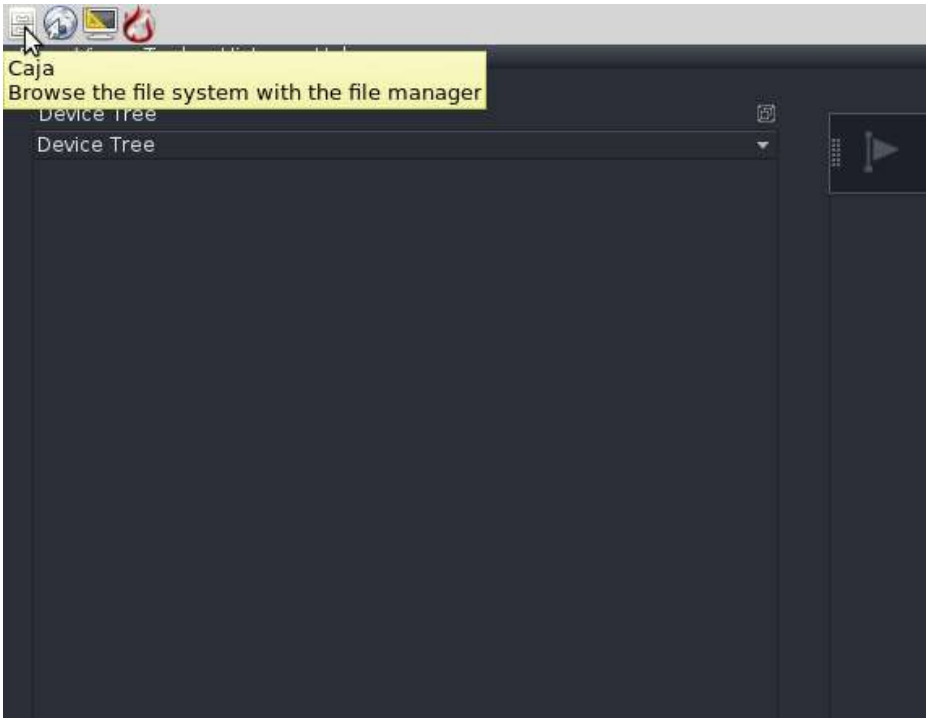


Figure 9.11: Opening the file browser

Once open, select the USB device in the left-panel to view the contents. This is known as "mounting" the USB device.

From inside the WaveView application, navigating to the USB device is as follows:

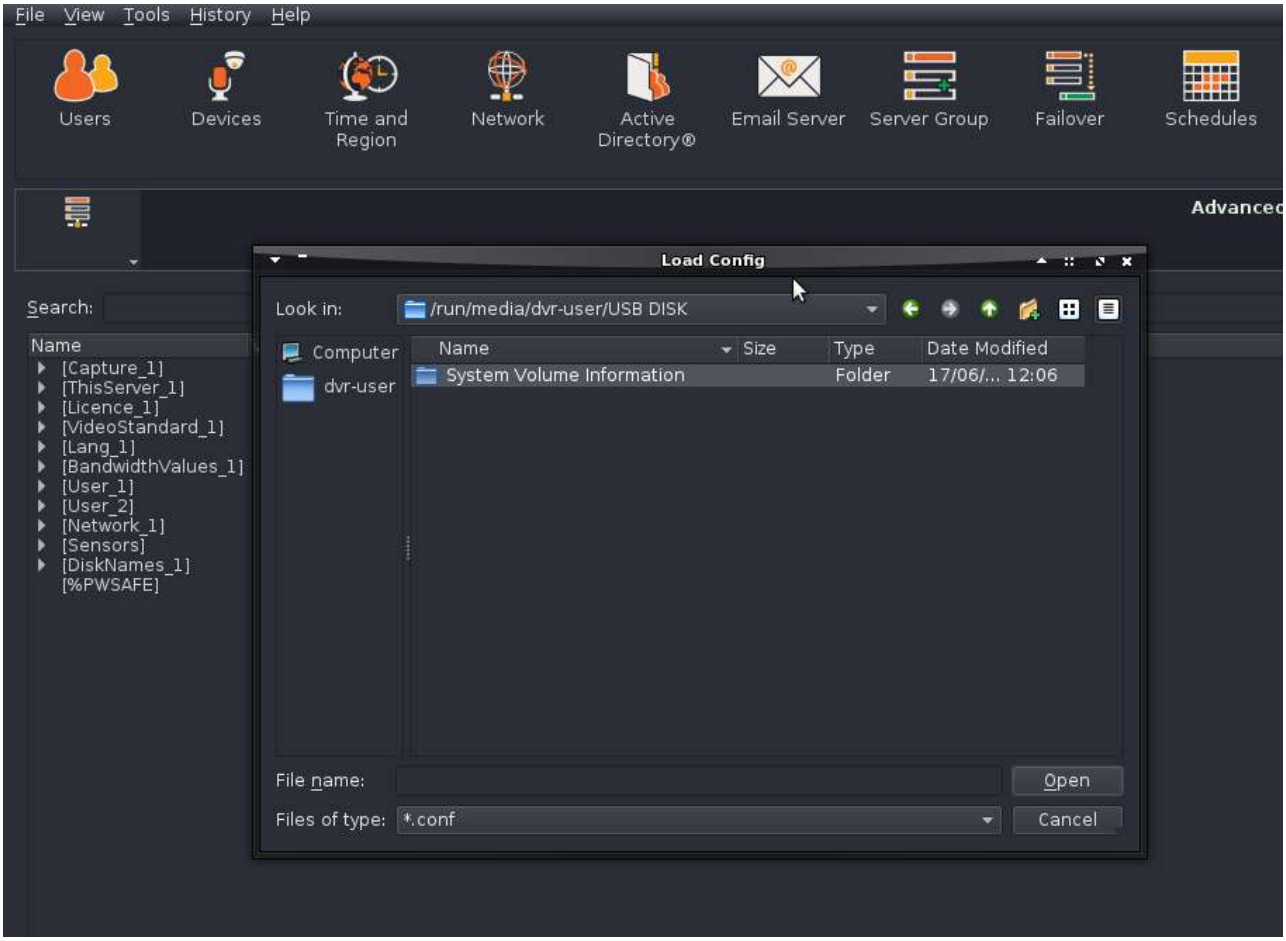


Figure 9.12: Accessing the USB device from WaveView

First, click "Computer" in the left panel. We now want to navigate to the path `/run/media/dvr-user/`. This is done as follows:

- Double-click "/"
- Double-click "run"
- Double-click "media"
- Double-click "dvr-user"

Finally you should now see the name of the USB device. Double-click it to view the files.

When finished with the USB device and prior to removal, it is strongly advised to "unmount" it. This is akin to the "safely remove" procedure on Windows.

To do so, access the Caja file browser as described before, then select the eject icon next to the USB device name in the left panel.

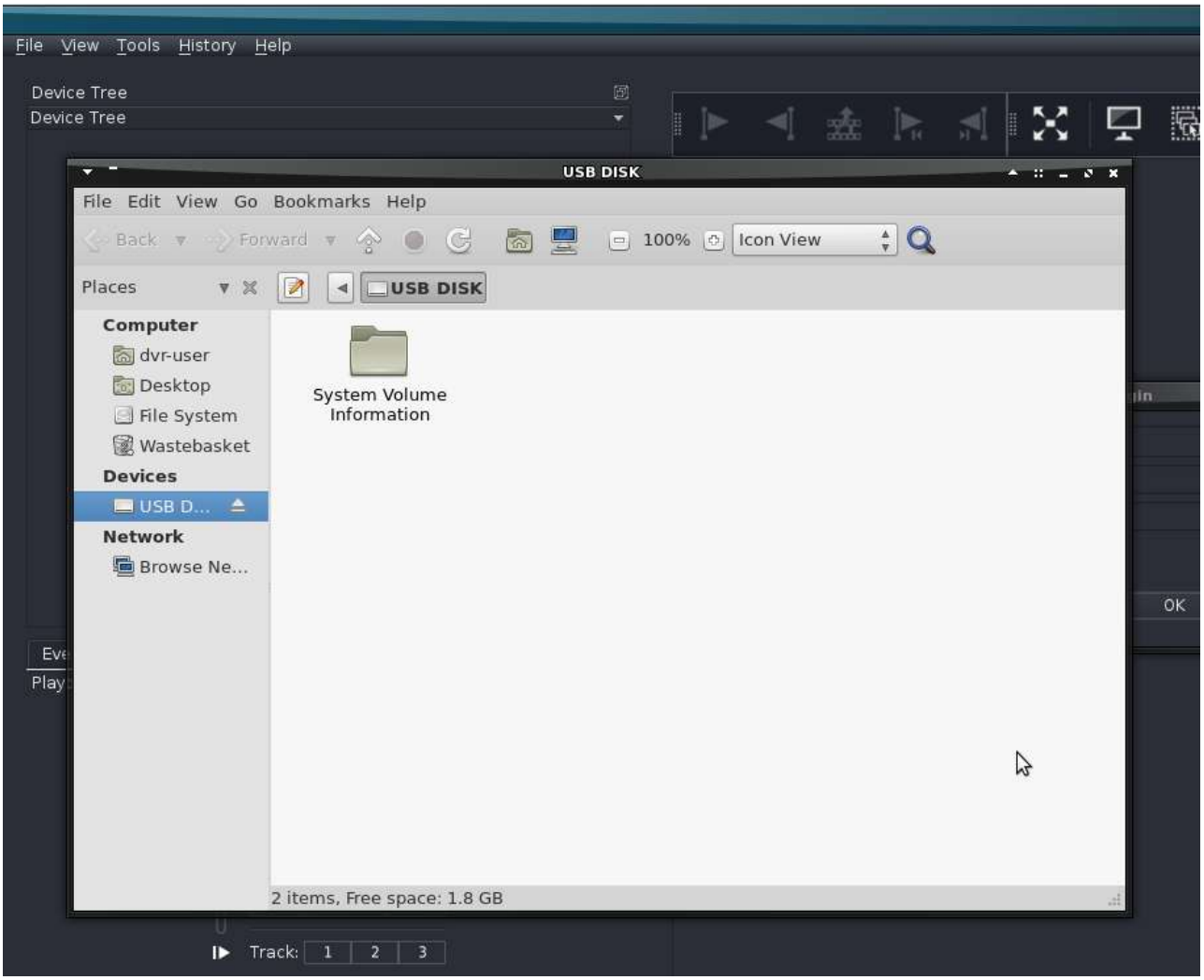


Figure 9.13: Viewing the USB device in the file browser

9.18 Central Event Server

The Central Event Server (CES) is a powerful and extensible feature of Wavestore which allows all (or some) events from the Live Event stream on a number of Wavestore servers to be forwarded to a central server which we call the "Central Event Server" or "CES", which can process the events. The feature is available from version 6.20.

The actual Central Event Server itself is just one of the Wavestore servers, it does not require any special hardware.

For example: consider a system with 5 Wavestore servers all in one Server Group. Server 1 can be set as the Central Event Server, and this will pull events from the other servers in the group automatically (providing the CES has been enabled). That server can then be programmed with Event Rules relating to all servers in the group.

This feature is disabled by default but can be enabled in the Server Group setup screen. See section 6.8 – .

When the CES feature is enabled, the first server in the group, Server 1, will be the CES, and the other servers will share their events with the CES.

Normally when configuring Event Rules, the Causes and Actions pertain only to the current server. However, when CES is enabled and Server 1 is being configured, the Event Rules screen allows the specific server to be selected for Causes and Actions. For example, Motion on Camera 3 of Server 2 could be used to trigger Output 1 on Server 3.

9.19 Failover

Wavestore systems support Failover, so if a recorder fails then another can take over.

To get a number of Wavestore servers to support Failover, we need one (or more) extra machines which will act as Standby servers. The concept is simple and is a type of virtualization: we have "logical servers" which do the recording and they are always up, and these run on "physical servers" which are the real hardware. Each physical server has its own IP address, so each physical server has a physical server IP address so we can monitor it.

In addition, each logical server usually has an IP address, and these are the ones to which the client and other devices connect to as part of the DVR operation so when it switches hardware it changes seamlessly. So when logical server 1 (LS1) is running on physical server 1 (S1) then that hardware has two IP addresses. This is optional: it is possible to have failover where you manually connect to Server 1 or to the Standby server if Server 1 is down, but adding logical addresses makes this seamless for a user who does not need to know if failover has occurred but merely wants to view the footage.

We need more physical servers than logical servers, these extras are the standby servers.

Pure virtualization techniques only virtualize the processor, but the Wavestore is primarily a storage unit. Different techniques are needed to make storage failover work efficiently from standard processor virtualization, and because Wavestore Failover has been designed for just this purpose, it is ideally suited to it.

So if we have 3 servers plus one standby, we need 4 physical servers in total, and servers 1, 2 and 3 will be configured to run as logical servers 1, 2 and 3. Server 4 will be configured as a standby.

Figure 9.14: Failover logical and physical devices

Remember we need 7 IP addresses for these 4 servers, since each logical server has a different IP address. This logical IP address is a secondary IP address on the network adapter.

When a server fails, the standby server takes over the role of the logical server:

Figure 9.15: Failover logical and physical devices after failure

The Standby server (or servers) monitor the logical servers and take over if any one fails. This leads to a brief interruption in recording, only a few seconds, and the recording while the original server is down is done on the standby server. When the original server comes back up, it takes over recording again, and the system redirects the footage recorded by the standby machine so it instantly appears onto the original server, so it's all in the same place as far as the user is concerned.

The Standby machine must be similar hardware to the machines which it will take over from, including the names of network interfaces in use, and number of disk volumes and their disk letters. Failover is not supported on machines which are not very similar, but some small variations are allowed: typically the Standby machine is a smaller version of the main servers.

Do not configure cameras or events on the Standby machines. The camera and event configurations will be copied from the logical servers and used when one of those physical servers fails. One exception to this is described below.

9.19.1 What counts as Failed?

A number of conditions are considered to be Failed for Failover purposes:

- The server loses power or stops working and vanishes from the network
- The server reboots or restarts
- If a network interface or bond group goes down. This could be because a cable has been disconnected. Note: if a single link of a bond group goes down this does not count as failed, all links of a bond group need to be down. See configuration options below.
- If a disk or disk array fails, so no data can be written to the disk or disk array. Note: if a single disk of a disk array goes down and redundant disks mean it continues to work then this does not count as failed, only if the array is no longer functional will it count as failed. See configuration options below.
- If a Failover event action is performed. This event action allows the user to configure an event which can trigger the server to be treated as failed.

- A force–failover command has been executed. This allows the user to force failover for maintenance purposes.

In the case of a reboot or restart, or network or disk failure, the server will be counted as working again once the reboot/restart/failure has been resolved. In the case of a Failover event action or force–failover command, it will be necessary to restart the server to recover from the condition.

Network Interface and Disk Array failure condition checks can be disabled by configuration options. These need to be manually applied into the configuration file if needed.

9.19.2 Identical Hardware for Failover

The server hardware should be identical in the following respects:

- all must have the same number of disk letters.
- each camera must have the same tracks recorded to the same disk letters (consistent across all servers).
- all must have the same network interface names.
- all must be running the same software version.

A number of differences are permitted:

- The Standby server can have smaller disks (or fewer disks in a disk array), but it must have the same number of disk volumes with the same disk letters. For example, the main servers might each have 24 disks in a RAID volume called Disk D. The Standby might be a smaller version of this with only 8 disks in a RAID volume called Disk D. But since both have a single volume called Disk D that would suffice as "identical".

  Network interfaces with IP addresses assigned must have identical names, but if the names of the physical network interfaces do not match, use bonding and assign the network interfaces to be slaves of the bonded interface "bond0"; assign the IP address to bond0 instead of the individual network ports. Now the interface name is identical on all machines, it's always called "bond0", the slave names are irrelevant. This can be extended to multiple bond devices if multiple IP addresses are required.

  Note that any number of normal or bonded slave network interfaces will be kept on failover, up to the first secondary network address (i.e. DEVICE with ":" in the device name). That secondary and all subsequent network interfaces will be taken from the logical server. This will work in most cases, providing bonding is set up before any secondary network addresses are added.
- The Wavestore servers may have different numbers of cameras, or different tracks configured for each camera, but when one is configured it should have the same disk letter as any other camera/track as the other Wavestore servers. And it's useful to configure all of them on the Standby server or they can't be seen later. For example a 2+1 server system might have 12 cameras on the first logical server and 11 on the second, but the standby is configured for all 12.
- The case might be a different size, and number of disks might differ, so long as the disk letters are identical. So a V–series server can be a standby for an X–series, and an X–series can be standby for a Petablok.
- During software upgrades the servers in a failover group will not all have the same version, as one server is upgraded first and another is yet to be upgraded. This will not normally cause a problem,

but for reliable operation all should be on the same version once the upgrade has been completed. It is usually best to upgrade the Standby server(s) last.

- Note that things which are not used don't need to be identical, so an additional disk which is not configured with a disk letter is not a problem.

Historical note: From V6.24 the requirement to have identical numbers of network interfaces on the two machines has been removed, and there is no longer a requirement to create dummy network interfaces. It's acceptable for either the main or standby servers to have more network interfaces so long as they are bonded as described above. These changes have been made to make it easier to replace failed hardware even when an identical replacement is no longer available.

When one or more servers in the failover group contains an analogue capture card, the channels on this card cannot be failed over since they are physically connected to the original server. Special configuration is required on the standby server to ignore the capture card when failover occurs.

9.19.3 Failover Group Size

Very large failover groups should be avoided: the monitoring overhead and network traffic increases significantly with large groups. It is recommended that a single failover group should have no more than 20 to 30 logical servers with one or more standby servers. The maximum permitted is 40 physical servers (ie, logical servers plus standby servers) per failover group.

Note that large server groups can be split into multiple failover groups, as server groups (which make viewing easier) and failover groups (which cope with server failure) can be configured independently.

9.19.4 Setting up Failover: Preparation

Connect the servers to the network, and use WaveView to configure the physical IP addresses. Do not put these servers into a server group at this time.

Add Logical network addresses as secondary addresses to the physical machines, excluding the Standby server, to allow WaveView to follow the logical server even when it fails over. Use WaveView Network Setup to do this using the "Add Secondary" button to the first network interface. This is an optional step but it makes the system very easy to use. See section 6.2.2 – for more information.

Note that it is essential that any logical (secondary) network interface or interfaces are added after all the physical (primary) network interfaces, otherwise it will not function correctly on failover. It should show as the last tab (or tabs) in the WaveView Network Setup screen.

Note that interfaces used for failover need to be configured with manually configured (static) IP addresses. Automatically obtained (DHCP) network addresses can only be used on interfaces which are not used by Failover. All the network interfaces use by Failover (primary and secondary) should use manually configured (static) IP addresses. If any interfaces are configured for DHCP, it is recommended that they are placed after the primary interfaces used for Failover. Bonding can be used to reorder them if needed, so bond0 is the Failover Primary and bond1 can use used for automatic (DHCP) addresses. Secondary addresses always go after all primary addresses.

Set all servers to synchronise time to an NTP server. It works well for all to synchronise to logical server 1, except logical server 1 itself which should get time from another NTP server or be manually configured.

Log into these machines and configure camera and audio channels as as normal. You can do this using either the physical or logical network addresses. It's a good idea to do much of the setup now, before Failover is started, but it can be done after failover has started if required.

Log into the Standby machine using the Physical address and set up camera and audio channels using a "Backup" type to create dummy channels, primarily to configure which disk is used for storage to allow access to any previously recorded footage when the Standby is in Standby mode. The number of channels configured should be such that it includes the channel numbers used by all the servers. For example if there is one server with 25 channels and another with 30, the standby server should be configured with 30 channels. Or, another example, if one server has channels 1, 2, and 4, and another has channels 3, 4, and 5, the standby server should have at least 1, 2, 3, 4 and 5. This is so that these channels can be viewed on the Standby server if needed and match the original channel numbers. It is not necessary to configure the channel names (leave them as default camera 1, 2, etc) but make sure the desired recording tracks are enabled and assigned to the same disk letter for the same length of time as the equivalent track in the logical servers.

To create the Backup camera types (which will be used when the machine is behaving as a "standby" machine):

- Go to 'Setup → Cameras'
- Choose 'Camera Group' tab
- Add a new group (name this 'Backup' to make it clear what it is for)
- Select the type 'Backup' (which is a type used to make this camera available without doing any new recording)
- Select the correct Disk, recording tracks, and recording duration
- Choose 'Cameras' tab
- Click '+' icon multiple times to add the number of desired channels, irrespective of whether audio or video, on the other servers. They should all be put in the 'Backup' group if that's the only one configured
- If the cameras are not all in the correct group, highlight them (click-drag over all those to change) and right-click and select 'Change Camera Group' and select the correct group
- Save the changes

Note that if the cameras are assigned to different disks or recording durations are required, then multiple groups should be created; the above procedure can be used to add cameras their respective groups.

If any of the physical servers are using ***Event Stream Recording***, ensure that the standby server also has ***Event Stream Recording*** enabled.

To ensure that any map images, integration modules, or custom sound files are available on the Standby server, log in to the main server group and use the File Manager to download all files. Then connect to the Standby server and upload those files. This ensures that any custom files will be available if/when the standby server takes over from a failed server. See section 3.26 – File Manager.

Note that if you are using any licensed integration modules, the standby server will also need to be suitably licensed such that it can run them if it takes over from a failed server.

It is a good idea to complete these preparation steps before adding the servers to the Failover group (see below), because you don't want failover happening while doing the initial setup.

9.19.5 Setting up Failover: Failover Group

After the preparation has been completed, it is necessary to add all the servers to the failover group.

Log into one Physical server and configure the list of Physical servers using the View → Setup → Failover screen. Add the main servers first (the ones which are already configured as logical servers) and add the standby server (or servers) last. Configure the correct number of logical servers. It is best to leave failover disabled until all servers are set up.

When adding these physical IP addresses, note the following:

- The physical IP addresses should be the first physical network interface on each machine.
- If using network bonding for all interfaces, then this should be the first bond interface, bond0. Configure bonding before configuring any failover group or secondary addresses.
- The physical IP addresses entered here need to be accessible from the client PC used to add them because WaveView needs to send the configuration to the Wavestore servers via these addresses.

Finally: enable failover and save.

Now failover is set up; the servers will automatically restart if needed and failover will be working.

If desired, add all the logical servers to a server group as described in section 6.8 – Server Group. If you use the logical (secondary) IP addressees then, when failover occurs, the client will automatically connect to the standby server.

Log into this server group to view all the servers.

Normally, make sure nothing is set to record on the Standby server (eg, no EVENT recording) when it's in standby mode. There is a special flag which allows recording and events to occur early on the Standby machine, at the cost of longer failover times (it takes a few seconds longer): in this case you will need to add Prestart=y to the Failover configuration section.

Finally:

- Restart all the servers to ensure they read the failover settings correctly
- Check in the system log that the Standby server is reporting that it is a PRIMARY STANDBY server.
- Check there are no issues in the system logs of the other servers.

When failover occurs and the standby server takes over, WaveView might report an error on login, stating "The server's identity has changed". This mechanism is used to prevent "man–in–the–middle" attacks and is warning that the real server at the IP address you used isn't the same server as last time. Of course, when failover occurs this is expected. If WaveView is connected to a server group when a server goes offline and failover occurs, WaveView may fail to automatically reconnect to the server due to this mechanism. The mechanism can be disabled in WaveView by navigating to "Tools → Preferences → Security → Check server public key when connecting".

Failover can be triggered quite quickly when a server is down, even briefly. For example, if making configuration changes to a server, it might be necessary to perform a software restart (called "Restart process" in WaveView). Failover can trigger in this case, but will revert to the original server once it is back up.

Note: Prior to V6.20, it was necessary to add a user called "failoverserver" to all DVRs. This is no longer required, and any such user is just a normal user now. On existing systems, you can keep this user if you prefer or you may delete the user if the Wavestore servers is on V6.20 or later. For new systems installed with V6.20 or later, this user is not required, which makes it quicker to set up.

9.19.6 Setting up Failover with IPv6

If only IPv6 addresses are configured for the Wavestore, then it's necessary to use them for Failover. Remember to use square brackets around the IPv6 addresses when setting up the Failover group. eg [fd01::918].

If there is a "dual stack" with both IPv4 and IPv6 addresses on the Wavestore, then it's necessary to configure the Failover group with IPv4 addresses as these will be the "primary" addresses of the Wavestore.

9.19.7 Stopping Failover

If you have a server which was part of a failover group but now isn't, especially a standby server, it's sometimes hard to disable failover because when it has failed over to the other server configuration, any edits are edits to the logical configuration, not the Standby server's configuration.

There is an command to deal with this case (see Tools → Execute Command):

- ifailover-disable

disables the failover configuration from the server even if it has currently taken over another logical server's configuration. It also deletes any resources and saved configuration files cached on this server.

Typically use this when you need to repurpose a server and remove it from the failover group, but it can also be used to disable failover on the Standby server to complete the configuration of the Standby without it taking over another server.

9.19.8 Licences for Failover

All physical servers, including the standby server, should have their own licence for the maximum number of channels on that server. Each licence should be of a sufficient level to support the Failover feature. There is also a special "standby licence" which can be used to specifically license a standby server, usually at a lower cost than a full licence. The "standby licence" allows the standby server to take over from a failed server in the group, but not to record itself independently when there is no failure in the group. Note that a standby licence is not required, a normal licence with the appropriate number of channels will also work.

For example, if there are two logical servers, normally on Server 1 and 2 with 25 and 30 channels respectively, and a standby on Server 3: then Servers 1 and 2 will need a normal licence for 25 or 30 channels respectively and Server 3 will need a licence for 30 channels so it can take over from either Server 1 or 2. Licences are specific to the physical server, not to the logical server.

9.19.9 Failover on Event

Whilst failover will occur by default when a server in the failover group fails completely, it is also possible to configure failover to occur on specific conditions, e.g. disk fault, using the Wavestore event rules system (see section 6.12 – Event Rules).

Simply configure a rule with an appropriate cause, such as "Fault > Disk failure", and set the Action to "Force Failover". Note, this only needs to be configured on the logical servers, not the standby server(s).

Note that if the rule is configured to trigger failover when a "Fault" occurs, clearing the Fault on the logical server will return the server to its "good" status, but the system will not automatically fail back. The previously failed server will need a restart to trigger that (Setup > Server > select the relevant server > Restart Process).

9.19.10 Network Failover

Network interfaces can be designed to fail over if a network interface or cable fails by grouping them together using Bonding.

In the View → Setup → Network screen, Add Bond Interface. Give this an IP address, and assign multiple physical network interfaces to be slaves of this logical device.

9.20 Licensing and Machine ID and Virtual Machines

A Wavestore is licensed to use various features with a licence string which only works on one specific machine. Each machine has a Machine ID, which looks like ABCD-EFGH-JKLM.

Most machines have a System Machine ID, which is dependant on the hardware of the system. A licence is specific to that machines. However, Virtual Machines (VMs) do not have a System Machine ID, and therefore a Hardware Dongle must be used or a Network Machine ID generated, otherwise the machine ID will appear as ?!?!.

9.20.1 Hardware Dongle

To use a Hardware Dongle, you must first obtain one of the tiny USB Dongles from your Wavestore supplier. When you insert it into the machine, the Machine ID changes to the Machine ID from the Hardware Dongle.

If you are adding the Dongle to a VM, it is usually necessary to tell the host system to connect the USB dongle to the VM. A typical procedure (this is for VMWare ESXi) looks like:

- Insert the USB Hardware dongle.
- Log into the VM console.
- Right click the Wavestore VM and select "Edit settings"
- Under the hardware tab click the "add" button
- Add the USB controller "UHCI + EHCI"
- Add the USB device "Unikey HID"

Notes:

- You can't share one Hardware Dongle with multiple Wavestore VMs on the same machine, but a single Wavestore VM can do all the work needed so there is little point in having more than one. The limitations are mostly network and disk throughput, and they won't be improved by adding VMs.
- It is, of course, possible to have other non-Wavestore VMs running on the same VM host.
- Hardware Dongles can be used on any machine, not just a VM. They can be useful if you want to move the licence from one machine to another.

Once the Hardware Dongle is inserted and connected, and the Machine ID obtained, a licence can be obtained for that Machine ID in the usual way.

9.20.2 Network Machine ID

An alternative to using a Hardware Dongle is a Network Machine ID.

To obtain a Network Machine ID (MID), the Wavestore will need to have access to the Internet and a valid DNS and gateway configured. The Wavestore should also have the clock set to a time within a few seconds of the correct time (typically with NTP). Once these conditions are met, if no other Machine ID is available, then the network Machine ID will be generated automatically. Once the system has a confirmed Network MID, it will attempt to continue with the same MID providing it's never considered to be a duplicate.

If a VM is cloned with identical parameters, the Network Machine ID will be cloned as well, and the remote servers will indicate one or other is a duplicate. There is a command "newmid" which can be used to force generation of a new Machine ID on one or other machine if needed. This is rarely needed unless the VM machines are identical.

If a machine is replaced or reinstalled, the network machine id will remain the same. This can now be determined immediately.

Once a Wavestore is given a Network Machine ID, it will attempt to use the same Machine ID forever and will poll the Network MID servers once an hour to check the validity. These checks merely ensure there are no duplicate Machine IDs to minimise any issues of downtime. In addition you get up to 5 days grace when your network goes down. The period your network can be down is increased by an hour for each hour it's been up, to a maximum of 5 days, and decreased by hour for each hour the network is down. So if it was up for 3 days, then down for 12 hours, then up for an hour, you still have 2.5 days left before the licence times out. If the Network Machine ID validity cannot be confirmed after this period then licence will time out. Fault messages will be produced to warn of this issue.

If you need a VM with a Machine ID which does not require a network, then use a USB Hardware Dongle.

9.21 Sort IDs

Sort IDs are used to give a unique number for every channel within a server group.

For example, imagine you have 2 servers in a group and each one has 50 channels. By default, the channels 1 to 50 on both servers will have Sort IDs 1 to 50.

The recommended way to set it up is to change the Sort IDs for server 2 so that they become 51 to 100.

This is useful for many reasons, one example being when using a PTZ joystick to call up cameras. With unique Sort IDs across the group, in our example group above, if you call up channel 61 you'll get channel 10 on server 2.

Another reason for Sort IDs is that in our experience, existing installations often have an existing camera numbering scheme, but technical issues mean that the channel numbers on the Wavestores can be forced. For example, if an installation has 12 analogue cameras and 4 IP cameras, a 16-channel analogue capture card is required. The system will then end up with channels 1-12 and 33-36 (because 1 to 16 are the analogue cameras and 17-32 the analogue audio channels). But the customer might prefer the cameras to just be numbered 1 to 16. Sort IDs allow this.

Note: Sort IDs are generally only used for presentation to the user in the user interface. Internally, the real "Channel IDs" are generally used. For example, if you are configuring linked audio – to link a video channel to an audio channel – the real channel number is supplied in the Cameras Setup screen.

9.22 Working With Joysticks

Wavestore provides support for a number of joystick/keyboard controller devices. The Wavestore Global Sales Team can provide advice on the currently supported products.

Usually the joystick will be automatically detected and enabled by WaveView, however this can be checked and edited in the *Tools > Preferences > System Settings* menu of WaveView. It may be necessary to restart WaveView after changing this setting.

9.22.1 Loading Layouts

The Wavestore system has the concept of per-user layouts and shared (system-wide) layouts. Each layout has an ID number, so for example you might have layout `1` for your user, and a shared layout `1`. Therefore, to open a shared layout, the layout ID should be prefixed with a zero.

For example:

- To load personal layout 5, the operator presses "Layout Selection", 5 and then OK.
- To load shared layout 5, the operator presses "Layout Selection", 0, 5 and then OK.

10 Technical Support

10.1 Introduction

The Wavestore website `http://www.wavestore.com` contains technical information and FAQ sections.

For further technical assistance, please email support@wavestore.com, or call the Wavestore Technical Support line in the UK (+44 1895 527 127, Monday–Friday 0900–1730).

Before contacting Wavestore Technical Support, please note the serial number of your Wavestore server (Wxxxx). This is normally located on a white label on the front or rear panel of the server. Please also take a note of the server software currently installed (menu path View → Setup → Server → Version).

In order to resolve certain issues, it may be necessary for Wavestore staff to log into the Wavestore servers remotely via an external internet connection.

10.2 Frequently Asked Questions

I connect and power up the Wavestore server, but nothing is displayed on the monitor.

Does the Wavestore server 'beep' shortly after it is powered up? If not then there is may be a hardware failure within the graphics card or the motherboard.

I connect my monitor to the Wavestore server and watch the server boot normally, but the final screen is not viewable i.e. either a blank or noisy picture.

Once the server has completed booting up, press CTRL + ALT + BACKSPACE to reconfigure the output resolution.

Cannot login using the WaveView client on the server box itself, using server name 'localhost'?

This can be caused by the configured IP address on the server clashing with the IP address of another device on the network. In the 'Server' field on the Login Dialog box, replace 'localhost' with the IP address 127.0.0.1, and you will now be able to login. Section 6.2.2 – Network describes how to reconfigure the server IP address if required.

Why can't I connect to my Wavestore server from a remote client Windows PC?

Firstly, trying pinging the Wavestore server from your PC (Start Menu → Command Prompt → ping [Wavestore server IP address]). You can confirm the Wavestore server IP address settings by following the menu path View → Setup → Network. If the server does not return the ping, there is likely to be network connectivity issue between the PC and the server.

To check the server, configure a fixed IP address on your PC that is in the same address range as the server, connect the PC to the server using a crossover cable, then try pinging the server once again.

If the server returns the ping, then the problem lies on the network connection between the client PC and the server.

If the server does not return the ping, the fault may lie with the server itself.

I have multiple Wavestore servers networked together and I'm viewing cameras on a remote client PC. The screen text displays 25ips, but sometimes the actual displayed rate seems to be lower than this?

This is likely to be due to network bandwidth limitations, if several remote clients are connected to the Wavestore server. As a consequence, the camera images displayed by the remote clients are refreshed less frequently. A user can select to view a lower resolution video stream for that camera, by selecting this from the Video Display Toolbox, as described in section 3.6.2– Video Display Toolbox.

In addition, each user of the system can be configured with a bandwidth limit; to set this up, follow the menu path View → Setup → Users screen, highlight the user that you wish to configure, and then re–configure the Maximum Bandwidth setting.

11 Appendix A – Technical Glossary

ADMINISTRATOR System operator who can allocate restrictions and passwords to other operators

BANDWIDTH Quantity of data which can be carried in a given time period

BNC Standard connector used to connecting a Wavestore server to coaxial cable (e.g. analogue camera)

CAPTURE DEVICE A means of capturing video and other data from a physical capture card or over the network

CLIENT A remote device connecting to the Wavestore server

COMPRESSION RATIO The level of compression to be applied

CROSSOVER CABLE A network cable with the TX pin at one end connected to the RX pin on the other end, and vice versa

DHCP Dynamic Host Configuration Protocol; enables management and automation of IP address assignment in an IP network

DIGITAL INPUT Incoming digital signal from external equipment

EVENT An occurrence which is detected by the Wavestore server

GATEWAY A network point that acts as an entrance to another network

GPU The Graphics Processor Unit component of a PC

GOP Used in H.264 and H.265 compression; Group of Pictures is the number of 'P' frames referring to an 'I' frame.

HTTP HyperText Transfer Protocol; a method of delivering data over a TCP/IP network

IMAGE CLIP Recorded activity with specific start and stop times

INSTALLER A special, high-level operator; permitted to perform maintenance tasks

IPS Images per second

IP ADDRESS Address of a PC/server on a network; the device address is unique on that network

ISDN Standard for digital transmission over telephone lines

LAN Local Area Network (normally 100Mbps)

LOCAL Activity at the Wavestore server itself

MASK A specific area of an image protected from modification

MJPEG Motion JPEG, a stream of individual JPEG images

MOTHERBOARD The main board in a computer that contains the computer's basic circuitry and components

NTSC Analogue television/CCTV video standard used in the USA, Far East and other areas

NTP Network Time Protocol; synchronizes the time of devices on a network

OPENGL A technology used by WaveView for improving graphical performance by utilising the graphics card (GPU)

OPERATOR A user, administrator or installer with associated password, permitted to use the Wavestore system

PAL Analogue television/CCTV video standard used in Europe and Australasia

PCI A type of expansion slot found on most modern motherboards

PRESET A set position which is stored in a dome camera for quick recall

PTZ Pan/Tilt/Zoom; refers to remotely controlled dome cameras

RAID Acronym for Redundant Array of Independent Disks; a standard for data storage; Wavestore uses RAID to enable high volumes of data storage

RELAY OUTPUT Outgoing digital signal to external equipment

REMOTE Activity at the client PC when networked to the Wavestore server

RESOLUTION The number of pixels in an image; higher resolution means a more detailed image

SATA Standard electronic interface between a motherboard's data paths or bus and the computer's disk storage devices

SCHEDULE A description of whether certain features should be active or inactive during a certain time period

SCSI Interface that enables communication with peripherals including disk drives

SERVER Network term for a Wavestore digital video recorder

SPOT MONITOR Analogue CCTV display, connected to a dedicated output separate from the main VGA output

STORAGE MEDIUM Device used for storage of data, e.g. CD–R, DVD–R, hard disk, USB device

SUBNET MASK Related to IP address, gives information about server locations on a network

TCP/IP Transmission Control Protocol/Internet Protocol; the basic communication language of the Internet

TOUR A series of presets and timing information, to cause a dome camera to follow a set path

USER The lowest level of operator, with limited permissions

VGA/SVGA Display resolution standards for monitors

VMD Visual Motion Detection

12 Appendix B – System Log Messages

Startup Messages

S Disk<X>: Recover successful: master index fully recovered
: Success message after a disk has been recovered and is now operating normally. The status of the disk will be shown as GOOD. Normally this message is only output after a type 3 recover operation (after a serious loss of data required specific attention to recover).

S Disk<X>: Recover successful: master index mostly recovered (<N>/<T>)
: Success message after disk recovery which had only partial success.

S Mirror: connected to mirror <M>
: The Wavestore is mirroring some of the disks to another device. This is an obsolete function.

S Power off on user request
: The Wavestore is switching itself off in response to a user request.

S Rebooting on user request
: The Wavestore is rebooting in response to a user request.

S Restart after disk shutdown
: A shutdown and restart was detected by the disk subsystem, but this was only the disk subsystem not the entire Wavestore. Typically this is because the disks have been reconfigured or formatted.

S Shutdown
: The Wavestore server shutdown by an unknown reason at this time. This message is generated on startup based on the time of last activity, so the timestamp is usually earlier than the position of the message in the log.

S Shutdown by system (<REASON>)
: The Wavestore server shutdown and restart for a system reason. There are a variety of reasons which cause automatic restarts, including Network Licencing when the licence beomes valid and Failover when it switches back to standby.

S Shutdown by user <USER>
: The Wavestore server shutdown under user request, possibly because it is rebooting after an up-grade.

S Wavestore Server v<VERSION> starting
: The Wavestore server started.

S <DEVICE>: Streaming images from '<IP>' port <PORT> rate <RATE> ips (approx)
: A camera or similar device started streaming over the network from <IP>:<PORT>. The rate is com-

puted as <RATE> images per second based on the rate the images arrive, which might not necessarily be the same as the rate which is configured: see the camera documentation for details.

Information Messages

I Applying settings to RAID card <CARD>
A configuration change is occurring to a RAID card.

I Camera <C>: Firmware upgrade succeeded: firmware version <VERSION>
The upgrade to the firmware on the camera appears to have succeeded.

I Camera <C>: User <USER> controlling PTZ
Information that a user has moved a Pan/Tilt/Zoom camera. Each camera is logged separately. Any subsequent operations within the time period (5 minutes) will be treated as the same operation unless a different user starts using the camera PTZ. After the time period has expired, any subsequent movements will be logged again.

I Closing all disks on user request
Before a disk configuration change, all disks are closed down and reopened.

I Configuration deleted
When uploading a configuration file, the old one is completely deleted first.

I Configuration edited in <APPLICATIONNAME> Configuration screen
This message indicates that the subsequent configuration change was performed in the Configuration setup screen of <APPLICATIONNAME>

I Configuration file loaded from <APPLICATIONNAME>
This message indicates that the subsequent configuration change was performed by loading a configuration file using <APPLICATIONNAME>

I DiskArray<DISK>: HyperRAID rebuild complete
In a HyperRAID array, after a failed disk has been replaced, a rebuild will start. This message is output when it completes and the disk array is no longer degraded.

I DiskArray<DISK>: HyperRAID rebuild of <DISK><N> starting
In a HyperRAID array, after a failed disk has been replaced, a rebuild will start.

I DiskArray<DISK>: HyperRAID rebuild <DISK><N> continuing
In a HyperRAID array, if a power cycle or restart occurs during a rebuild, it will restart when the Wavestore restarts.

I DiskArray<DISK> is degraded
In a HyperRAID array, if a disk has failed, the array is no longer considered "good", but is "degraded". It is still fully usable and no data is lost, but the failed disk should be replaced as soon as possible.

I Disk<DISK>: iSCSI: Target remounted and opened ok
The remote ISCSI disk was mounted and is working ok.

I Distro <DISTRO>
The version of the Wavestore operating system distribution

I Email: Email to <Recipient> sent successfully
If Email has been configured, it has been sent

I Error flag cleared by user <USER>

Once an error has been reported, the Error flag (usually a red blob on the bottom of the screen) is shown until it's explicitly cleared. This message is output when it's cleared.

I Event match table <NAME> loaded

Events can now match against a file of entries, this informs the user that such a table has been loaded. Use the file manager to load and delete these tables.

I Failover group with <N> physical servers and <M> logical servers

On startup, the size of the failover group is reported. Normally there are more physical servers than logical ones, and these extra ones are the standby servers.

I Failover: taking role of logical server <N> (<NAME>)

When a machine fails, and a standby server is available, it will take over the role of one of the logical servers. This message is output when this happens.

I Failover: this server is an AUXILIARY STANDBY machine (physical server <N> is PRIMARY STANDBY)

If there is more than one standby servers in a failover group, then we want just one to be ready to take the place of a failed machine and all the others will wait their turn. These others are called AUXILIARY STANDBY machines and one will become primary standby if the primary standby either fails or is becomes another logical server.

I Failover: this server is PRIMARY STANDBY machine

This is the main standby server in a failover group.

I File: Limited to <MAX> cameras

The File playback device is limited to <MAX> cameras.

I Finished Native Export: <USERNAME>@<IPADDRESS>, start:<STARTDATETIME>, end:<ENDDATETIME>, (<CA

A Native (WSB) export has completed.

I Finished Pass-through Export: <USERNAME>@<IPADDRESS>, start:<STARTDATETIME>, end:<ENDDATETIM

A pass-through export has completed. This is when the original video data is simply written to file.

I Finished Transcoded Export: <USERNAME>@<IPADDRESS>, start:<STARTDATETIME>, end:<ENDDATETIME

A transcoded (e.g. AVI, MP4) export has completed.

I Hard Delete of all disks complete

If you have run the hard delete command, this message will be output when it completes.

I Hard Delete of <DISK> complete

If you have run the hard delete command, this message will be output when it completes.

I Hard Delete of <DISK> starting

If you have run the hard delete command, this message will be output when it starts.

I IP address <IP>

Information about which IP addresses are available on interfaces on this Wavestore.

I Last shutdown occurred around <TIME>

The Wavestore server shutdown by an unknown reason at this time. This message is timestamped

at startup but contains a secondary timestamp of the last shutdown time.

I Licence: <FLAGS>
This log messages shows the licence flags (showing the number of channels licensed).

I Licence: unlicensed
The Wavestore is not licensed, either because it's new and you have not entered one in the Licence screen or because it had a time limited licence which has run out. If you are using a network licence then you might need to enter the "oldmid" or "newmid" commands to restore an old Machine ID or create a new one, see the network licence documentation.

I MegaRAID: Creating new RAID volume DiskArray<DISK>: <UNFO>
RAID volume creation message

I MegaRAID: DiskArray<DISK>: Deleting array
The array has been deleted by a user altering the configuration. Normally this can be recovered by recreating the array.

I MegaRAID: Disk <DISK> being reincorporated
RAID volume reincorporation message: See MegaRAID documents for details.

I Mirror: disconnecting from <M>
Mirroring message. Obsolete.

I Mirror: lost connection to mirror <M>
Mirroring message. Obsolete.

I Native Export: <USERNAME>@<IPADDRESS> – <FILEPATH>
This is a status message which is reported after an export starts or finishes, to document the file path.

I Network address <IP> (interface <IF>) mac <MAC> speed <SPEED> Mb/s
Information about the network link: this shows the IP address and MAC address for a specific interface and the current speed negotiated for this link. If it's a bond interface, the speed is the aggregate of all the slave links which are currently up.

I Network Link (<IF>): speed was <OLDSPEED> now <NEWSPEED>
Shows the network link speed changed; usually this is because a bond has lost a slave link, but it might be because a cable or connector is inadequate and a lower speed has been negotiated.

I Network slave (interface <IF>) master <MASTER> mac <MAC> speed <SPEED> Mb/s
Information about the network link for interface <IF> which is a slave interface to master <MAS–TER>. Shows the MAC and the link SPEED of this link alone.

I Notify<N>: protocol=<PROTOCOL>, type=<TYPE>, client=<CLIENT>, dialout=<DIALOUT>, password <PASSWOR

Notification setup log message.

I NTP: Changed NTP server to '<IP>'
The configuration of the NTP server used has been changed to the specified server.

I Pass–through Export: <USERNAME>@<IPADDRESS> – <FILEPATH>
This is a status message which is reported after an export starts or finishes, to document the file path.

I PTZFIdleAction=<A> unrecognised in section <SEC>
The configuration contains a corrupt parameter.

I PTZF idleTimeout increased to 5 seconds

The configuration contains an idle period which was too short and has been increased.

I Reboot required to complete configuration changes

After a major configuration change it is necessary to reboot the computer. This message is logged as information only in the case when this occurs.

I Reloading Stretch driver

The "Stretch" Analog Camera card is reloading, usually because it stopped.

I Restart required to complete configuration changes

The Wavestore sometimes requires a restart to complete a configuration change. This message is output if a restart is needed.

I <DEVICE> Camera <N> IP='<IP>'

Camera startup message.

I <DEVICE>: Capture device started ok

Camera or device startup message.

I <DEVICE>: Connected to '<IP>' port <PORT>

Camera or device connection message.

I NTP: Slewing time by <N> seconds (stratum <ST>)

It's important to have correct time on a Wavestore so images are correctly timestamped, but it's even more important to keep time ticking forwards and not have it jump forward or backward. When NTP is enabled, any time errors are slewed gradually until the time is correct. For errors of around a second, a slew rate 1:60 is used (1 second corrected each minute).

I <DEVICE>: <N> virtual spot monitors enabled

Spot monitors have been enabled on a virtual spot monitor device.

I Starting Native Export: <USERNAME>@<IPADDRESS>, start:<STARTDATETIME>, end:<ENDDATETIME>, (<CA

A native (WSB) export has started.

I Starting Pass-through Export: <USERNAME>@<IPADDRESS>, start:<STARTDATETIME>, end:<ENDDATETIM

A pass-through export has started. This is when the original video data is simply written to file.

I Starting Transcoded Export: <USERNAME>@<IPADDRESS>, start:<STARTDATETIME>, end:<ENDDATETIME>

A transcoded (e.g. AVI, MP4) export has started.

I NTP: Time synchronised (stratum <ST>)

When NTP is enabled, and there is no significant error, then the time is said to be synchronised. The clock rate is adjusted fractionally to ensure it remains correct.

I Temporary network IP disabled

This message is output when the temporary IP address (set by arp-ping) is no longer available.

I Temporary network IP <IP>

When setting up a Wavestore, a temporary IP address can be set using the arp-ping method.

I Time slew completed

NTP indicating time slew has completed. See "Slewing time" above

I Time will slew by <N> minutes
: NTP indicating a rapid time slew has started.

I Time will slew slowly by <N> milliseconds
: NTP indicating a slow time slew has started.

I Time will slew slowly by <N> seconds
: NTP indicating a normal time slew has started.

I Transcoded Export: <USERNAME>@<IPADDRESS> – <FILEPATH>
: This is a status message which is reported after an export starts or finishes, to document the file path.

I Upgrade: delete package: <PACKAGE>
: Upgraded information: a package is being deleted

I Upgraded: <PACKAGE>
: Upgraded information: a software package has been upgraded

I Upgrading NVIDIA graphics driver as previous driver was automatically removed via upgrade
: After an upgrade, if an old version of the proprietary NVIDIA driver was installed and had to be removed to complete the upgrade, the new one will be installed automatically. This log line indicates that the new installation is in progress.

I User <USER> FORMATTED Disk<DISK>(<PATH>)
: A disk or disk array has been formatted or reformatted by the specified user.

I User <USER>: Rebooting server
: The user has requested a reboot.

I User <USER>: Restarting server after update or on request
: The user has requested a restart or an upgrade has completed (which causes a restart). Occasionally this will result in a reboot as well if major changes have been made.

I User <USER>: Shutdown server
: The user has requested that the Wavestore is shut down.

I Video Authentication: Signing enabled, <N> bit key
: Video Authentication is enabled.

Fault Messages

F Analytics<DEV>: Analytics from camera <C> failed to stream
: When using an analytics device, the device will stream video from the Wavestore and the Wavestore will then stream analytics metadata from the analytics device. This indicates that the Wavestore cannot stream due to an error.

F Analytics<DEV>: failed to connect
: this indicates that the Wavestore cannot stream from an analytics device as it cannot connect to the device.

F Analytics<DEV>: please upgrade analytics to latest version
: This indicates that the Wavestore cannot stream from an analytics device because a software upgrade is required.

F Authentication: Key and Certificate do not match

An error occurred when loading a key/certificate, probably because the key was regenerated after the certificate request was generated or the wrong certificate loaded. If it cannot be resolved by loading the correct certificate, regenerate the key/certificate request pair again (exactly once) and get the new key (certificate request) signed.

F Cannot allocate buffer! Buffer pool fully used

An internal error which usually caused by too many channels in use on a machine with inadequate RAM. Contact technical support if this persists.

F Cannot downgrade OS to this version as UEFI is not supported

Indicates that the current system is using UEFI and cannot be downgraded to the requested older version, since UEFI was not supported in that version.

F Clock has jumped backwards by a large amount!

It is possible for the Wavestore battery–backed hardware clock to malfunction when it is rebooted or powered off. To prevent the loss of footage in this case a fault is raised. The correct action is to reset the clock to the correct time and then it should be ok. If it continues to show this after any power cycle, then it is likely to be a hardware issue: probably a flat battery.

F Configuration file uses X PullPoint event cause in event rules

Recommended course of action: Go to "Setup | Event Rules" and find any rules where the event cause starts with X. Delete these rules and reprogram them since they will no longer work. If the desired event cause cannot be found in the list, contact Wavestore support. Background: In version 6.8 if PullPoint was enabled for an ONVIF camera and the camera sent an event type which was unknown to Wavestore (which most were), they would be passed through by the server with an "X" prefix and would be available in the Event Rules screen for users to program rules with. For example, if a Canon camera sent "LineCrossing", the Wavestore would look it up in the device database, fail to find it, but then make it available as an Event Cause called "XLineCrossing". Users may have programmed event rules based upon this. For many cameras known event causes have now been added, so "LineCrossing" now gets passed through as "LineCrossing", or something similar. Any unknown event causes from the cameras are discarded by default from version 6.10. This is the desired behaviour, to actively add known event causes to the device database and ensure they're consistent. For example, some cameras might send "LineCrossed", so the Wavestore device database will map it to "LineCrossing", so all different cameras show up with the same terms when setting up the event rules. In v6.10 there is a new "flag" <A> for the Camera request string to force the old behaviour of letting all event causes through, with the X prefix if not known. Adding this flag is an alternative course of action if the recommended course of action above is not desirable for some reason

F CopyTrack: no matching source found for server '<SERVER>': not copying

The copytrack has failed due to the parameters being entered incorrectly.

F DiskArray<X> has failed

A disk array has failed. It is not recoverable and the data is lost.

F DiskArray<X>: Too Many Failed Disks

Too many disks in a RAID array have failed, for example if 2 disks out of an N+1 (RAID5) array both fail at the same time, then it is not possible to recover any data and a reformat is needed.

F Disk<X>: Another program is accessing the database

If the Wavestore server believes another program is accessing the same disk, it will output this

message. In very rare cases this is seen on a sudden restart. Normally it would indicate a configu–ration error.

F Disk<X>: Another program is writing to this disk; aborting
This message is produceed if two Wavestores are writing to the same disk, or if two programs are running on one Wavestore. Writes to the disk could cause corruptuon, so writes are not allowed.

F Disk<X>: Attempting to record to missing disk
This is caused by a configuration error of the removal of a disk which the system is recording to.

F Disk<X>: Authentication error
For network or cloud disk storage, this indicates authentication errors occurred when attempting to access the remote disk.

F Disk<X>: disk array DEGRADED
The disk array specified has a fault with one of the disks: the array is operating in a fully functional but degraded state. The faulty disk should be removed and replaced as soon as possible when it will enter a REBUILDING state. See also the knowledge base article: "Why do new disks fail?".

F Disk<X>: disk or disk array not present
Disk array does not appear to be present. This is typically seen when using MegaRaid or simular disk arrays, possibly which have been set up in an unexpected way by an external tool, and the re–sult is that the array does not appear to be present to Wavestore. The solution is usually to examine the disk array using the tools it was originally set up using, or delete the array and use Wavestore to set up the array.

F Disk<X>: disk <X><PATH> appears bad; not using
Disk has shown errors. Sometimes this is seen when setting up, because the disk has not yet been setting up. Sometimes this is seen when inserting a new disk, because the disk has not yet been fully inserted. In both cases the solutiion is to complete setup and/or click Add Swapped Drives.

F Disk<X>: disk <PATH><XX> is too small (<N>KB when <M>KB needed); not using
Use a bigger disk. The message will tell you how much is needed.

F Disk<X>: Error mounting nfs://<PATH> as <XX> (code <NN>; <MSG>)
Error mounting an NFS disk.

F Disk<X>: Error mounting <PATH> as <XX> (code <NN>; <MSG>)
Error mounting a disk.

F Disk<X>: Error mounting smb:<PATH> as <XX> (code <NN>; <MSG>)
Error mounting an SMB (Window share) disk

F Disk<X> is corrupt: autorecover started
Auto recovery of master indexes has started.

F Disk<X>: Last recording was in the future!
To prevent the loss of footage in this case a fault is raised if the footage appears to be in the future. See "Clock has jumped backwards by a large amount" above.

F Disk<X>: Maximum number of channels on one disk volume exceeded
The old MTable3 has a maximum number of 511 channels on one disk volume. This includes any channels which have been set up even if no images have been written, and typically 4 channels per camera are set automatically by the default camera group. Solutions is to disable the channels which are not required in the camera group, and restart the server, or distribute cameras over a

number of disk volumes. Each disk letter corresponds to a disk volume. The newer MTable4 storage system has no such limit but this is not the default storage system in this version.

F Disk<X>: Maximum number of channels on one volume exceeded
: The old MTable3 has a maximum number of 511 channels on one disk volume. This includes any channels which have been set up even if no images have been written, and typically 4 channels per camera are set automatically by the default camera group. Solutions is to disable the channels which are not required in the camera group, and restart the server, or distribute cameras over a number of disk volumes. Each disk letter corresponds to a disk volume. The newer MTable4 storage system has no such limit but this is not the default storage system in this version.

F Disk<X> not formatted or corrupt
: A disk is not used because it is not formatted or corrupt. Normally the solution is to format it.

F Disk%s: Path '%s' did not match a valid disk type
: The disk setup string is invalid and begins with an invalid prefix; this might be seen when downgrading to earlier software which does not support the feature.

F Disk<X>(<PATH>): disk failed
: A disk has failed. This should be replaced and the replacement formatted.

F Disk<X><N>(<PATH>): disk failed
: A disk has failed. If this is a unit of a disk array, then the disk array becomes "degraded" and will continue to function normally if there are still adequate redundant disks. It is recommended the disk is replaced as soon as possible. If a Hot Spare or Warm Spare is available, then the replacement will automatically occur immediately (but you might want to replace the spare).

F Disk<X><N>:(<PATH>) is about to fail and should be replaced
: A disk has failed it's SMART tests and is considered to be likely to fail.

F Disk<X><N>:(<PATH>) is too hot (<DEGREES>C)
: A disk has got very hot. The temperature reported by SMART is shown.

F Disk<X>: Transfer error
: An error was seen when transfering data from an external disk–like system.

F Email sending script failed to run correctly. Check debug log messages.
: This suggests there may be a problem with the software which sends out emails. Please capture the System Log including Debug messages and report it to the Wavestore support team.

F Encryption disabled because invalid [Encrypt_1 key]
: Please ensure that the encryption key entered into the configuruation file is valid; have you entered the wrong type of key? Until the issue with the key is resolved, the encryption has been temporarily disabled.

F Error in configuration file
: The configuration contains an unspecified error, probably because it was edited manually. If this proves to be a problem, restore an old configuration and make any required changes again.

F Failover: Could not take over server <N> because configuration file not available
: In a failover group, the Standby server collects details of all the working servers so it can take over in case of failure. If it detects a failure for a server which it has not been able to load the configuration details from, then it will not be able to take over. This will only occur on configuring the Failover group, probably because the failed server failed immediately or prior to the configuration of the Failover group.

F Failover disabled due to configuration error

If Failover is enabled but the configuration is incorrect, the entire failover system will be disabled and this error will be produced.This is preferable to it behaving in a confusingly manner because of the misconfiguration. More detail about the issue will be found in the Failover log.

F Failover: Disk FAULT: enter FAILURE state

The failure of an entire disk array or a single disk not in an array will trigger failover; this failure message is produced when this is triggered. Note that a single disk in a redundant array will not trigger failover providing the array is still usable.

F Failover: Event triggered FAILURE condition

It is possible to configure an event to trigger failover; this failure message is produced when such an event is triggered.

F Failover: physical server <N> failure while in standby

A fault message produced by a primary wavestore when a standby has failed.

F Failover: physical server <N> (<IP>) has failed

A fault message produced by a standby wavestore when a primary wavestore has failed.

F Failover: This server's IP address (<IP>) not in Failover server list

The failover system is badly configured. Refer to the manual for restrictions on IP addresses used for configuration: in short, the first interface which has an IP address on each Wavestore will be used for Failover and this should be the address configured in the Failover list.

F Failover: Time difference on servers in failover group: <SECONDS>s

Indication that the time is not synchronised between servers in a failover group. This will lead to confusing results and footage recorded at different times on different servers when failover occurs. Configure NTP to ensure all are synchronised.

F Inadequate main memory: at least <N>MB of RAM required

More RAM is required.

F Invalid Protocol string (Protocol=%s)

The Protocol= line in the configuration file is incorrect

F iSCSI: Failed to connect to iSCSI target

The system will attempt to connect to any iSCSI drives when it first starts up. This message is given if it fails. Check the iSCSI drive or drives are functional and the network connectivity to them is good.

F Jumping time immediately in this exceptional case

Normally the server will slew the time slowly if it is wrong, so no jumps occur but it's brought back to being correct as soon as possible, but it is possible to get it to jump if the gap is too great to slew and the user explicitly requests a jump. This message will be output if it jumps. It's a FAULT message to indicate normal operation did not occur at this point.

F Kernel crash dump exists in /var/crash

Indicates that a serious issue has occurred in the operating system. This is usually indicative of faulty or unsupported hardware.

F Kernel: Out of memory: restarting process

There is an issue with memory and a process has been restarted. No immediate action is needed as the system will continue to operate as normal after the restart. This is rare, but usually indicates a problem, so it should be reported to support@wavestore.com for investigation.

F Licence expired

The licence was a subscription or time limited licence and it has now expired. You will need to purchase a new licence.

F Licence: OPLP incompatible with Network Licensing

If you are using an On-premise licence proxy (OPLP), you cannot configure network licensing which requires access to the central licence server to confirm the licence. Network licensing is mandatory for virtual machines.

F Licence: This version is newer than AUD permits: upgrade licence or downgrade software

The upgrade bundles are now controlled using dates ("AUD") and you have upgraded to one which is more recent than you are permitted.

F MachineID rejected (Server returns FAIL)

A network-validated Machine ID has been rejected by the licence server. This probably indicates you have cloned a virtual machine and not reset the machine id using "newmid" command. Contact technical support if you are not on a virtual machine.

F MegaRAID: Manual action required

The old MegaRAID cards can get into states where manual action is required with storcli command: see MegaRAID documentation in the Wavestore manual.

F MegaRAID: Manual action required to delete old RAID array – THIS WILL LOSE DATA

The old MegaRAID cards can get into states where manual action is required with storcli command: see MegaRAID documentation in the Wavestore manual.

F NASDisk<DISK>(<PATH>): disk failed

A Network Disk has failed or the link to it is down.

F Network: failed: check cables connected and disable unused interfaces

The network checking code has detected a failure on one of the network interfaces. Probably this is due to an unused interface being enabled. A typical case is that a network interface is enabled and set to obtain an IP address automatically, but not connected to a network with a DHCP server, so it fails to obtain an address. The solution is to disable any unused interface or configure an IP address manually. An alternative to disabling unused interfaces is make them all slaves to a bond interface and only configure the IP address on the bond interface.

F Network Link (<IF>) Down: speed was <OLDSPEED> now <NEWSPEED>

Shows the network link has gone now down and is no longer working; usually this is because a cable has been removed.

F OPLP enabled but no [SysMonitor S1 address configured]

To use an On-premise licence proxy (OPLP), you will need to configure it's address as S1 which is the same server as the On-premise health monitoring server.

F Out of memory: Cannot allocate data buffers

This should never occur and if it does contact technical support.

F Restarting server to recover from recording problem

Very rarely the Wavestore server will encounter a problem which can best be resolved by restarting or rebooting to reset the hardware, and a restart or reboot will automatically occur to resolve the issue. This message will be produced.

F %s: Camera dropped out, check the connection

Normally if a camera drops out, the server will attempt to reconnect to it. If it reconnects promptly

and then goes on working without needing intervention, no fault is raised, but messages are logged in the camera–specific log file if this happens.

F %s: Camera dropped out several times, check the connection
: Normally if a camera drops out, the server will attempt to reconnect to it. If it reconnects promptly and then goes on working without needing intervention, no fault is raised, but messages are logged in the camera–specific log file if this happens. If the camera drops out more than would be expected, to the extent the camera or network mighr be faulty and need attention, this fault message is produced.

F %s: Camera returned Unauthorized: username or password is wrong
: The username or password used to access a network camera has been rejected by the camera.

F <DEVICE>: Camera type is incorrect (NTSC or PAL)
: On analog cameras, the type should be set to the same as the camera. Usually this is set for the entire machine.

F <DEVICE>: Cannot connect to board (<ID>)
: Hardware issue. Contact technical support.

F <DEVICE>: Cannot create channel <ID> (<INFO>)
: A channel cannot be created on a multichannel device (typically an analog camera); if this persists attempt to restart the server and if still a problem contact technical support.

F <X>: Cannot create DECODE channel <C> (chan_num <N>) (<D>)
: Decode error for an Analog Video Out device. Obsolete.

F <DEVICE>: cannot have more audio channels than video
: Usually shown by a misconfigured device. If it persists, contact technical support.

F <DEVICE>: Cannot load firmware '<FILE>' (<INFO>)
: Usually shown by a misconfigured device. If it persists, contact technical support.

F <DEVICE>: Cannot open audio OUT device <DEVICE2> (<INFO>)
: Usually shown by a misconfigured device. If it persists, contact technical support.

F <DEVICE>: Capture card failure
: Indicates a capture card is not working. If it persists, contact technical support.

F <DEVICE>: Capture card not working properly
: Indicates a capture card is not working. If it persists, contact technical support.

F %s: Could not connect to camera
: A network connection cannot be made to the camera. Check the camera is functioning and the network connectivity is good.

F <DISK>: Disk is too slow (<RATE> MB/s): data lost
: There is an issue with the disk or disk volume and data is being lost. This might be because there is too much being recorded to this disk or because the disk has become faulty. This message is only output if the disk appears to be slower than expected, and therefore the disk (or disk interface) might be the problem. See also "Too many cameras streaming to this disk" for the case where the disk seems to be ok but the data rate seems too high.

F Sensors: <X> = <Y> <Z> triggered alarm
: The Wavestore supports Sensors for temperature, voltage and fan speed on standard Wavestore

servers and enclosures. If one of the sensors indicates a problem, this alarm message will be raised. Check the hardware and replace any failed item.

F Sensors: <SENSOR> triggered <E>
: One of the system sensors triggered an issue. Usually this is a Fan, Temperature, or PSU problem.

F <DEVICE>: error enabling DECODER for channel <CHANNEL> (<INFO>)
: Unspecified error when enabling a decoder channel (usually on an analog capture device). Contact technical support if it persists.

F <DEVICE>: error enabling encoder for channel <CHANNEL> (<INFO>)
: Unspecified error when enabling an encoder channel (usually on an analog capture device). Contact technical support if it persists.

F <DEVICE>: error enabling encoder for SECONDARY channel <CHANNEL> (<INFO>)
: Unspecified error when enabling a secondary encoder channel (usually on an analog capture device). Contact technical support if it persists.

F <DEVICE>: error enabling SECONDARY channel <CHANNEL> (<INFO>)
: Unspecified error when enabling a secondary channel (usually on an analog capture device). Contact technical support if it persists.

F <DEVICE>: ERROR in configuration file: too few cameras specified, using NumCameras=1
: This might be seen in a manually edited configuration file: fix the configuration manually or restore an old working one.

F <DEVICE>: ERROR in configuration file: too many cameras plus decode channels specified (<N>) – disabling

: This might be seen in a manually edited configuration file: fix the configuration manually or restore an old working one.

F <DEVICE>: ERROR in configuration file: too many cameras specified, using NumCameras=<N>
: This might be seen in a manually edited configuration file: fix the configuration manually or restore an old working one.

F <DEVICE>: error setting parameters for channel <CHANNEL> (<INFO>)
: Unspecified error when setting parameters on a channel (usually on an analog capture device). Contact technical support if it persists.

F <DEVICE>: error setting parameters for SECONDARY channel <CHANNEL> (<INFO>)
: Unspecified error when setting parameters on a channel (usually on an analog capture device). Contact technical support if it persists.

F <DEVICE>: Failed to obtain Events from camera
: A device (typically a camera) failed to stream events. Often these are conveyed by a separate mechanism from the video stream, for example ONVIF Pullpoint, and this is the stream which has failed. Events from a camera might include Darkening and Motion.

F <DEVICE>: Failed to Pull Metadata
: Metadata (events or analytics) could not be pulled from the camera.

F <DEVICE>: Failed to stream images
: A device (typically a camera) failed to stream images. This message is only given if a connection has been established to the device and authentication has succeeded, but the stream has then failed to start for some reason. Any additional information is in the camera-specific log file.

F <DEVICE>: Multicast failed from this camera

Multicast is not working from the specified camera

F <DEVICE>: No VIDEO available from this stream

There is no VIDEO stream configured from this camera and a video stream was requested; usually this is because it is disabled in the GUI or in an ONVIF profile. If it's expected that there is no video from this device, disable the video stream in the camera group.

F <DEVICE>: Problem: Error connecting to camera '<IP>' port <PORT>

For an IP camera: the Wavestore could not connect to the camera. Ping the camera to check if it actually exists on that IP address.

F <DEVICE>: PTZ Request failed

The camera or PTZ device gave an error when a PTZ request was sent.

F <DEVICE>: PTZ Request unauthorised

The camera or PTZ device complained about the username or password when a PTZ request was sent.

F SSD: System drive about to fail

The system disk, which is an SSD, has reported that it is about to fail (via SMART parameters).

F %s: Server not licensed for this camera

The server licence typically has inadequate channels for this camera. The recommended solution is to disable excess cameras and restart the server, or obtain a licence with more channels.

F <DEVICE>: Sound device disabled due to setup errors

Sound device is not working correctly.

F <X>: Talkback is not supported by this camera

Audio talkback (audio from the User or Server to the Camera or Network Audio device) is not supported by the Camera or Network device. This might be because it uses another protocol from the one it is configured to use. It should be noted that ONVIF Profile S does not include talkback (ONVIF Profile T is required) but some cameras will support audio talkback by other means.

F NTP: Time change is unexpectedly large (<N> minutes), ignored

Small time changes will slew, but large ones are assumed to be errors and will be ignored unless manual steps are taken. It would not be approprate to slew by a large amount because it would take too long.

F <DISK>: Too many cameras streaming to this disk (<RATE> MB/s): data lost

There is an issue with too much data being written to a disk or disk volume, hence data is being lost because the disk cannot keep up. This appears to be because too many cameras are being recorded to this disk, or because the data rate from each camera is too high. This message is only output if the disk appears to have too much being recorded to it, and therefore the configuration might be a problem. See also "Disk is too slow: data lost" message for the case where the configuration seems ok but the disk seems faulty.

F <N>: To perform a large time change, disable NTP and enter time change manually

Small time changes will slew, but large ones are assumed to be errors and will be ignored unless manual steps are taken.

F Stretch: Cannot initialise Stretch SDK (<INFO>)

Hardware error. Contact technical support.

F Stretch: invalid board number (<N>)
: Hardware error. Contact technical support.

F <DEVICE>: Unrecognised file type (<TYPE>)
: A file (which was uploaded by the installer) had an unrecognised type and therefore will be ignored.

F <CAMERA>: VMD stream 'Profile3' not found or blank in the config!
: VMD has been enabled, and manual profiles selected, but there's no VMD profile (Profile3=) configured.

F System needs reboot as new graphics driver has been installed
: Graphics drivers require a reboot immediately after installation. This message is shown once a graphics driver installation has been performed.

F Time jump completed
: Information message after an exceptional time jump. This is a FAULT message because the system is not behaving normally and footage recorded will show a gap or a jump.

F Time Set: Exceptional time change encountered: please check the time and timezone
: Small time changes will slew, but large ones are assumed to be errors and will be ignored unless manual steps are taken. It is recommended you check that you've set the correct timezone before changing the time.

F Time Set: Exceptional time change rejected
: Attempt to change time by large amount has been rejected. See above.

F Time Set: Failed to change time
: Attempt to change time failed.

F Time Set: Footage will be lost if this time change is made
: If you jump the time backwards, footage "in the future" will be deleted because the footage is indexed by time and it does not allow footage after the current time. This is a warning that you are going to do something very serious.

F Time Set: To perform a large time change, use slewtimefast or jumptime commands
: Small time changes will slew, but large ones are assumed to be errors and will be ignored unless manual steps are taken. This is a summary of the commands you can use, after you have checked the timezone is correct.

F Time wrong: manual action required
: The time on the Wavestore is wrong and a licence cannot therefore be obtained automatically. The best solution is to correct the time on the Wavestore.

F Too many cameras configured for this system (<N> maximum); memory upgrade required
: Wavestore servers have minimum memory requirements for various number of cameras in order to function correctly. If more cameras than permitted for a specific memory size are installed, this fault will be logged. The solution is to reduce the number of cameras or upgrade the server memory.

F Upgrade failed
: An upgrade failed. See the Upgrade log for more details.

F Upgrade failed: package unsigned: <PACKAGE>
: An upgrade failed because a package was unsigned. Often a package appears unsigned because it was only partially uploaded and corrupted by a network dropout and another attempt will work. See the Upgrade log for more details.

F Upgrade finds <N> duplicate packages: reinstall is recommended

After upgrading a package, a consistency check is performed to ensure there are no duplicate packages which can cause issues. Sometimes these issues are caused by a network or power failure during the upgrade. A command "remove-dup" can be executed (by Execute Command on WaveView) to remove duplicates, after which it is recommended that the upgrade be attempted again to ensure the correct packages are installed. If this is unsuccessful, reinstall might be needed.

F Upgrade: previous upgrade/downgrade did not complete correctly: reinstall is recommended

After upgrading a package, a consistency check is performed to ensure there are not "broken" or half-completed upgrades (which might occur for example if you restart the Wavestore in the middle of an upgrade). This is a warning that you have an unstable system and a reinstall is needed.

Warning Messages

W Bad disk2 name '<NAME>' in config section '<SECTION>'

Corrupt configuration. Fix it or restore a working configuration file.

W Bad disk name '<NAME>' in config section '<SECTION>'

Corrupt configuration. Fix it or restore a working configuration file.

W Camera out of range in channel <N> in <SECTION>

Corrupt configuration. Fix it or restore a working configuration file.

W Camera <N>: Invalid Resolution=<RESO>

Corrupt configuration. Fix it or restore a working configuration file.

W Cannot allocate any disks

Usually this indicates that no disks are specified in the disk setup screen, or that those set up have been removed.

W Cannot open configuration: creating dummy with no cameras

If the configuration has been deleted but no other uploaded, the server will create a default configuration to ensure the system is usable. Usually the correct action in this case is to restore an old configuration file.

W C<CAMERA>: Audio encoder option AAC Not supported by this device.

The camera or device is not correctly configured.

W C<CAMERA>: Audio encoder option Not supported by this device.

The camera or device is not correctly configured.

W C<CAMERA>: GOP size too large (<N>)

Wavestore systems are specified to handle GOP sizes up to 64 frames; above that playback performance can be severly reduced. The GOP size is the size of the "Group of pictures" which start with an I-frame (initial frame) (also called IDR or IRAP frame) and then contain other frames which rely on the first frame to be decoded properly. If you start to play back some footage, or switch to view a different camera, the WaveView client will need to get all frames from the last I-frame and decode from there to the desired frame. This has been optimised for up to 64 frames. If GOP sizes are larger than this, it might become slow or jumpy. There is a way to disable this warning if you must have larger GOPs, but it is not recommended.

W Disk<DISK> is too large

Warning that a disk is too large. Obsolete, as very large disks permitted in current software.

W Disks set to READ ONLY mode: recording is turned off

Warning that the disks were set to read–only by an installer, and therefore there will be no recording. This option is found on the disk setup screen.

W Disk<DISK><N>:(<DISKPATH>) is too cold (<DEGREES>C)

Warning that the disks are rather cold; with luck they will go on working but action should be taken to ensure the server doesnot get too cold.

W Dwell out of range in Dwell=<D>

The dwell time specified is not in the valid range. This is caused by misconfiguration.

W Email: All recipients were refused and nobody got the mail

Recommended course of action: Check all settings in "Setup | Email" including the Recipient list, as they are likely to be incorrect for your email server.

W Email: Connection unexpectedly closed – possibly username and password issue

Recommended course of action: Check all settings in "Setup | Email", primarily username and password.

W Email: No suitable authentication method was found

Recommended course of action: Check the settings in "Setup | Email" as they are likely to be incorrect for your email server. Background: This warning suggests that the configured email server didn't allow us to login. Consider checking username and password. Also consider enabling or disabling the "Use SSL" option.

W Email: SSL/TLS support is not available to your Python interpreter

This shouldn't ever happen. If it does, please contact Wavestore support.

W Email: The server didn't accept the from address

Recommended course of action: Check the "Sender" setting in "Setup | Email" as the email server complained about this.

W Email: The server didn't accept the username/password combination

Recommended course of action: Check the settings in "Setup | Email" as they are likely to be incorrect for your email server.

W Email: The server didn't reply properly to the HELO greeting

Recommended course of action: Check the settings in "Setup | Email" as they are likely to be incorrect for your email server. Background: This warning suggests that the configured email server didn't respond to us properly, so most likely a problem with the email server settings.

W Email: The server does not support the STARTTLS extension

Recommended course of action: Check the settings in "Setup | Email" as they are likely to be incorrect for your email server. Background: This warning suggests that the configured email server didn't respond to us properly, so most likely a problem with the email server settings. Try enabling or disabling the "Use SSL" option.

W Email: The server replied with an unexpected error code

Recommended course of action: Check all settings in "Setup | Email". Failing that, consider talking to the administrator of your email server as it is sending unexpected responses.

W ERROR: failed to start nginx as reverse proxy to access cameras

The system uses nginx for camera gateway proxy (also known as a reverse proxy) if it is enabled in the configuration. This message indicates some error prevented it starting. Contact technical support for assistance.

W ERROR: failed to stop nginx

See previous entry. This message indicates some error prevented it stopping. Rebooting should fix this.

W Failed to send alert email. Recipients setting is missing.

Recommended course of action: Check that the "Recipients" settings in "Setup | Email" have been completed correctly. Background: This warning suggests that email alerts have been configured in the "Setup | Event Rules" screen but no potential recipients for email have been configured in "Setup | Email".

W Failed to send alert email. SMTP setting is missing.

Recommended course of action: Check that the settings in "Setup | Email" have been completed correctly. Background: This warning suggests that email alerts have been configured in the "Setup | Event Rules" screen but the email server settings have not been set up in "Setup | Email".

W Holiday: unrecognised day <DAY>

In the configuration file, a bad day was specified

W Holiday: unrecognised month <MONTH>

In the configuration file, a bad month was specified

W Invalid findmeta textual match syntax: <MATCH>

A metadata match, often in the configuration file for an event rule, has a corrupt match syntax. Probably due to a manual edit.

W Key generation failed

RSA key generation (for authentication or encryption) has failed. Contact technical support.

W Licence: <N> analogue <TYPE> configured when only <N> permitted

You have allocated more analogue cameras than permitted by your licence. Upgrade your licence.

W Licence: <N> EMS <TYPE> configured when only <N> permitted

You have allocated more EMS encoders or multisensor cameras than permitted by your licence. Upgrade your licence.

W Licence: <N> IP <TYPE> configured when only <N> permitted

You have allocated more IP cameras than permitted by your licence. Upgrade your licence.

W Licence: Storage over <N>TB not permitted on this licence; Skipping disk <DISK>

You have allocated more storage than is permitted on this licence. Upgrade your licence. Note that all V6 licences currently allow unlimited so you should not see this.

W Malformed event line in <F>:<N>

Corrupt configuration. Fix it or restore a working configuration file.

W Match file: <NAME> failed to load

An event rule match table is referenced in the configuration file but the table file does not appear to exist. Upload the table again or change the match rule.

W Mirror: failed to connect to mirror <M>

Mirroring message. Obsolete.

W Mirror: failed to login to mirror <M> as user <UU>

Mirroring message. Obsolete.

W Missing Licence – please enter licence

Please enter a licence string.

W NetworkThread: cannot bind to port, retrying

The server port is not available. Unlikely. Contact technical support.

W Notifier <N>: no such notifier

A request to notify using notifer <N> has been made in an event rule but no such notifier exists. Correct the notifier number or add the correct one.

W Notify<N>: Failed to notify event for over 2 minutes: check IP (<X>) <Y> <Z>

A notifier cannot connect to the target.

W Notify: unsupported protocol=<PROTO>

The configured protocol does not exist

W NTP: Cannot get time from server '<SERVER>'

When NTP is configured, the NTP service cannot contact the specified server and get the time from it.

W NTP: Upstream server '<SERVER>' is unsynchronized

NTP has failed to synchonize because the <SERVER> it is configured to pull the time from (the 'upstream server') is not correct ('unsynchonized'). Usually that upstream server should be synchronised to another NTP source. It is possible to synchronise time from a Wavestore where the time has been manually set, but the manual time configuration should have been performed recently, if not this message will be shown.

W Only <N> GB RAM available: performance will be reduced

Wavestore servers are generally shipped with adequate RAM for the load they are specified. However old servers which have been upgraded and other systems might not have adequate RAM and therefore buffering and other items will be reduced as needed, this warning shows that this reduction occurred.

W Prerecord buffer limited to maximum permitted (%s seconds)

A fixed maximum limit has been exceeded. Use a smaller value.

W Preset out of range in Preset=%s

<PRESET> A ptz preset number is invalid.

W <ID>: bad On/Off entry: <TEXT>

Corrupt configuration. Fix it or restore a working configuration file.

W <DEVICE>: Could not open port <PORT>

A device (typically an io device) cannot open a specific io port. Usually this is due to misconfiguation of the port.

W Section out of range in channel <N> in <SECTION>

Corrupt configuration. Fix it or restore a working configuration file.

W SerialAlarm: Baud=<BAUD> is not a recognised value

The baud rate is invalid. This is due to misconfigurtion.

W <DEVICE>: ERROR in configuration file: too many cameras specified, using NumCameras=<N>

Corrupt configuration. Fix it or restore a working configuration file.

W <FEATURE> feature not licensed

The specified <FEATURE> is not licensed. Upgrade your licence.

W %s: Limited Video Encoders, requested streams may not be possible.

The camera has limited resources. Check camera documentation and reconfigure.

W Speed out of range in Speed=<SPEED>

The configured speed for a PTZF operation is invalid. This is due to misconfiguration.

W <DEVICE>: Problem: Error connecting to camera <N> port <PORT>

W <DEVICE>: Rebooting the camera to resolve streaming issues

An attempt to reboot to camera has been made after a camera was not streaming for some time. This is only done as a last resort, usually after an hour of inactivity and multiple attempts to recover it in other ways. Note that this is just a camera reboot, not a Wavestore server reboot. The camera reboot can be controlled using various parameters in the CameraGroup configuration.

W <DEVICE>: Requested encoding <X> is not supported by this camera, choosing <Y> instead

The encoding requested by the user (eg, H265) is supported by the camera so another encoding (eg, H264) is used instead.

W SSD: System drive wearing out too fast

The Wavestore uses SSD system drives for speed and reliability. They are very reliable so long as they don't get overused. Occasionally something is accidentally configured which writes heavily to the SSD, hence the Wavestore monitors this and warns if it seems to be wearing out fast. Note that it's rate of wear which is monitored, so this warning might be issued even if the SSD has 99% of usable live left simply because it ran though the 1% faster than expected. This check means we can recify the issue before it becomes a problem.

W <SECTION>: unrecognised day <X>

A corrupt configuration file.

W <SECTION>: unrecognised hour <X>

A corrupt configuration file.

W <SECTION>: unrecognised minute <X>

A corrupt configuration file.

W System will reboot in 5 mins unless FAULT flag is cleared

Some serious problems will force a reboot unless the user deliberately stops it. This message is given in this case.

W System will reboot to recover from error

Some serious problems will force a reboot. This message is given when this occurs.

W Talkback clip '<NAME>' not found

When configuring an event to send a talkback audio clip, if the wrong audio clip name is given this message will appear.

W Talkback failure on device <X>.<Y>

Talkback (audio output from the user or server to the camera or audio device) has failed for device X.Y

W This is a beta-test software release

This message is produced when using early pre-release software. It can generally be ignored, but please do remember to upgrade to the release software when it released.

W Tour out of range in <DEV>

A tour is misconfigured.

W tw_cli is not installed – cannot make required settings to RAID card
: This is unlikely to happen and suggests an installation problem. The message suggests that the Wavestore has a 3Ware RAID card installed but the required utilities to interact with it are missing.

W type=<TYPE> unrecognised in section <SECTION>
: A corrupt configuration file.

W Unrecognised network command: <CMD>
: Usually caused by corruption on the network connection; reconecting is recommended.

W UPGRADE Early file termination (<X>) (expected <N> bytes)
: Usually caused by corruption on the network connection, try again.

W User <USER> login from <IP> failed: SECURE=y set and insecure login attempted
: A user used the old V4 client to connect and that uses a less secure mode which is no longer allowed.

W Warning: event rule matches on missing table '<NAME>'
: An event rule match table is referenced in the configuration file but the table file does not appear to exist. Upload the table again or change the match rule.

Configuration Messages

C Failover: and <N> custom sections: <DETAILS>
: Information message, the final part of a Failover changed message (only used if custom sections exist)

C Failover: configuration changed to logical server <LS> (<NAME>)
: Information message showing the Standby has taken over the logical server <LS> when they are both part of a Failover group. Usually this occurs when the physical server which had been running as logical server <LS> has failed.

C Failover: except for <N> network interfaces, disks, system and licence
: Second part of Failover changed the configuration message.

C Reset <SECTION> as maintenance mode for camera <N> has expired
: Indicates the configuration has been updated automatically to remove maintenance mode from a camera since the time period selected has now expired. Note that this message only occurs if it has expired, it can also be removed by normal configuration changes.

C System has moved <N> local users to [%PWSAFEL section]
: A configuration file upgrade occurred

C User <USER> configuration '<FILE>'
: Message indicates that a configuration file has been loaded.

C User <USER> has changed password
: Message when a user sets own password

C User <USER> reset '<CONFIG>'
: Message when a configuration section is cleared (ie, set to nothing). See 'set' below.

C User '<USER>' set a password for '<USER2>'
: Message when an administrator sets another user password

C User <USER> set '<CONFIG>'

Message when a configuration section is set. The configuration is shown in the internal format which can be viewed in the advanced configuration editor. This might continue over several lines if needed.

C User <ADMINUSER> setting password for <SECTION> user <USER>

Message when ADMINUSER sets password for another user, USER.

C User '<USER>' updated Password Safe

Message when an administrator sets multiple passwords (probably by uploading a file)

Login Messages

L Logging in using group '<GROUP>'

When LDAP/Active Directory login is configured, a login occurred with the specified <GROUP> because the user was authenticated by the LDAP/Active Directory password server and was a member of <GROUP> on that password server, and that <GROUP> exists as a user group on the Wavestore. Permissions are granted by the user <GROUP> on the Wavestore.

L Login failed because no DVR group was found on this password server

If LDAP/Active Directory login is configured, a DVR group must be present on the password server (ie, the Active Directory server) and the user must be a member of that group. DVR groups are group with names beginning DVR (eg DVRuser for normal user level login).

L User <USER> from <IP> disconnected on timeout

User whose login name is <USER> who had connected from <IP> ip address was disconnected from the server by a server timeout. This can be a disconnect on idle or because they were logged in too long or on a schedule.

L User <USER> from <IP> disconnecting

User whose login name is <USER> who had connected from <IP> ip address disconnected from the server.

L User <USER> logged in from <IP>; permission level <LEVEL>

A login occurred from username <USER> from IP address <IP> at permission level <LEVEL> (install/admin/user).

L User '<USER>' was authenticated by password server '<SERVER>'

When LDAP/Active Directory login is configured, the user <USER> was authenticated by the LDAP/Active Directory password server <SERVER>, and the authentication passed successfully.

L WARNING: multiple groups match (<GROUP1>,<GROUP2>)

When LDAP/Active Directory login is configured, the user could not log in because they were a member of more than one DVR group.

13 Appendix C – WaveView Launch Options

--autoLogin=<server>[:<port>],<user>,<password>[,sg]
: Login to the the given server automatically. <server>, <user> and <password> are required. <server> can be a hostname or IP address. <port> is optional and defaults to 8601. The last optional argument ("sg") indicates whether to connect to the server group. If not present, only the specified server will be connected to, rather than the group.

--fullscreen
: Forces the video display area to be displayed in fullscreen.

--maximize
: Forces the main window to be maximized.

--screen=<screen_number>
: Forces the main window to be displayed on the screen corresponding to <screen_number>.

--useDesktopOpenGL
: Force to use Desktop OpenGL driver, instead of auto-detecting.

--useSoftwareOpenGL
: Force to use OpenGL software rendering, instead of auto-detecting.

Examples

--autoLogin=10.1.2.3,joe,a,sg
: Logs in to server 10.1.2.3 with username "joe" and password "a". Connects to all servers in the group.

--autoLogin=10.1.2.3:8602,joe,a --maximize --screen=1
: Logs in to server 10.1.2.3 on port 8602 with username "joe" and password "a". Does not connect to all servers in the group, only server 10.1.2.3. Opens the client on screen 1 and maximizes the window.

Adding Shortcut Options on Windows®

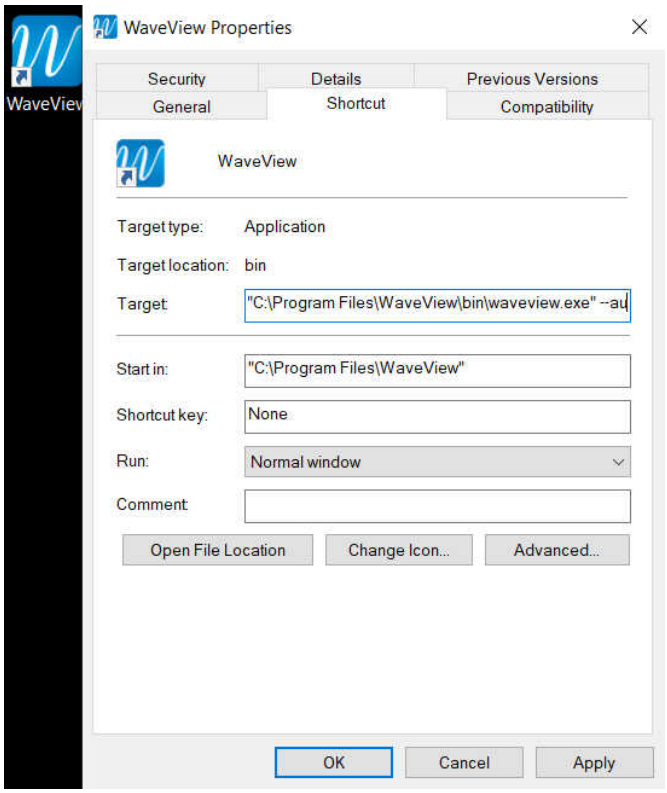
The launch options documented above can be used on Microsoft Windows®. One way is simply to run WaveView from a Command Prompt, but this isn't very convenient. The most common way is to create and edit a shortcut to WaveView with the appropriate options set.

Depending on the options chosen when installing WaveView, there might already be a shortcut on the Desktop. If not, there are several ways to create a new shortcut. One way is to use Windows Explorer

to navigate to the installation directory. By default this is `C:\Program Files\WaveView\bin`. The executable file is called waveview.exe although the ".exe" extension may be hidden.

Right-click the executable and choose "*Send to > Desktop (create shortcut)*".

Now the shortcut on the desktop can be edited by right-clicking and choosing "*Properties*".



The desired launch options can be added by adding them at the end of the *Target* field. Ensure that they go outside the quotation marks.

14 Appendix D – Writing an ISO with Rufus

To install or upgrade Wavestore from a USB memory stick it is necessary to extract the ISO to the USB stick. The way to do this depends on the Operating System. Most commonly Microsoft Windows is used, in which case the Rufus program is recommended.

Assuming the installation ISO has already been obtained, the process is as follows:

- On Windows, download Rufus from `http://rufus.akeo.ie`
- Run Rufus.
- Plug in the USB stick. Rufus should recognise the USB and populate the "Device" box.
- On Rufus: "Format Options"/"Create a bootable disk using" and select "ISO Image".
- On Rufus: click the icon to the right of the above text and select the ISO.
- On Rufus: click [Start] to start the write to USB.
- Select "Write in ISO Image mode (recommended)" and click OK if Rufus asks about deleting files on the USB stick.
- It'll take a few minutes to create the bootable USB.

15 Appendix E – Camera Statuses

There are 4 camera status categories, each represented by an icon. Within each category, there are various possible statuses which are shown within a tooltip by hovering over the icon. The statuses and status categories are described below:

Category: Unknown

Unknown The status of the camera is not yet known

Not Enabled The camera is not enabled so its status cannot be queried

Category: Ok

Not Recording The camera is not configured to record but is otherwise working correctly

Recording The camera is working correctly and recording

Category: Warning

Darkening The image from the camera is unusually dark and might indicate tampering

Camera Movement The camera has been moved from its previous position, i.e. the scene has changed

Initializing The camera is about to be set up

Configuring Settings are being pushed to the camera

Connecting The Wavestore server is connecting to the camera

Connected And Starting The Wavestore server has connected to the camera and is starting streaming

Category: Maintenance

Maintenance The camera is in maintenance mode and will not report faults as F faults into the system log nor will it set FAULT on the status indicator or remote monitor

Category: Error

Not Permitted The current user is not permitted to view this camera

Not Licensed The system is not licensed to use this camera

Video Loss No video is being received from the camera

Unauthorized The Wavestore server does not have permission to access the camera, normally indicating incorrect credentials in the camera setup

Could Not Connect The Wavestore server could not connect to the camera, normally indicating a configuration or network issue

Failed To Stream The Wavestore server connected to the camera but was unable to initialise streaming, normally indicating a configuration issue or problem with the camera

Server Awaiting Restart The Wavestore requires a software restart before full operation can continue

Check System Log Some issue occurred which is detailed in the System Log

Network Problem The Wavestore has detected a problem with network

No Live It has not been possible to perform live streaming from the camera