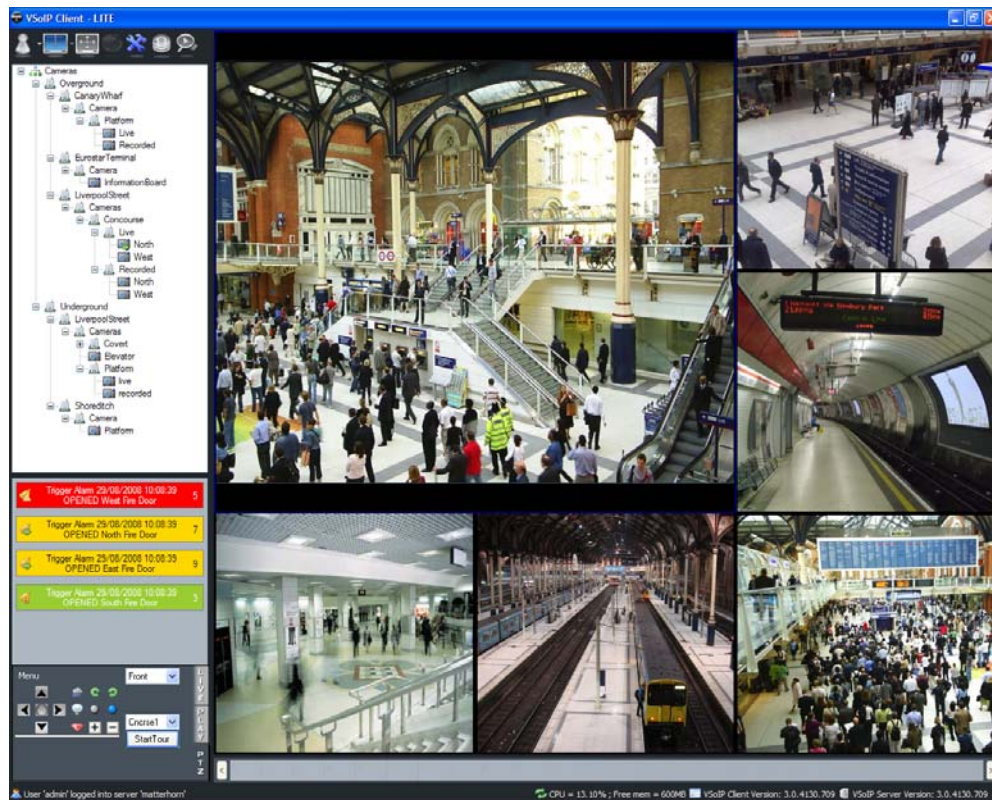


# MANAGEMENT SOFTWARE

# **VSOIP LITE**

## USER MANUAL



**QAWZ®**



# Table of Contents

|   |           |
|---|-----------|
| <b>1 System Overview .....</b>              | <b>4</b>  |
| System Components .....                     | 4         |
| Surveillance Suite Architecture .....       | 4         |
| IP Camera and DVR Compatibility .....       | 4         |
| System Environment .....                    | 4         |
| Network traffic .....                       | 4         |
| Infrastructure .....                        | 5         |
| Configuring Stream Settings .....           | 5         |
| System Software .....                       | 6         |
| Shutting Down the Computer .....            | 7         |
| <b>2 Installing VSoIP Lite.....</b>         | <b>8</b>  |
| Introduction.....                           | 8         |
| Prerequisites.....                          | 8         |
| Hardware.....                               | 8         |
| Operating System .....                      | 9         |
| Additional mandatory software .....         | 9         |
| Before Installing VSoIP Lite .....          | 9         |
| Operating System Settings .....             | 9         |
| Networking .....                            | 9         |
| Installing VSoIP Lite .....                 | 11        |
| Upgrading a License .....                   | 11        |
| <b>3 VSoIP Lite Configuration.....</b>      | <b>13</b> |
| Getting Started.....                        | 13        |
| User Configuration.....                     | 14        |
| Device Configuration .....                  | 15        |
| Adding Devices .....                        | 15        |
| Deleting Devices .....                      | 17        |
| Configuring Video Sources.....              | 18        |
| Configuring Triggers.....                   | 19        |
| Configuring Pan-Tilt-Zoom Capabilities..... | 20        |
| Working with Live Video and PTZ.....        | 21        |
| Specifying Video Pane Layout.....           | 22        |
| Starting and Stopping Live Video .....      | 23        |
| Using Digital Zoom.....                     | 24        |
| Taking a Snapshot of Live Video .....       | 24        |
| Control of Pan-Tilt-Zoom .....              | 25        |
| Working with Alarms .....                   | 27        |
| Overview of Alarm Display .....             | 27        |
| Viewing Properties of an Alarm.....         | 27        |
| Acknowledging an Alarm.....                 | 28        |
| Closing an Alarm .....                      | 29        |
| <b>4 Recording with VSoIP Lite .....</b>    | <b>30</b> |
| Recording Camera Footage .....              | 30        |

|  |               |
|--|---------------|
| Creating a Recording .....                                   | 30            |
| Playing Back Recorded Video .....                            | 31            |
| Discovering Recorded Footage.....                            | 31            |
| Playing Back Recorded Footage.....                           | 31            |
| Using Digital Zoom .....                                     | 34            |
| Taking a Snapshot of Recorded Video .....                    | 34            |
| Editing Recording Jobs .....                                 | 34            |
| Deleting/Disabling Recordings .....                          | 35            |
| Synchronising Playback of Recorded Footage .....             | 36            |
| Exporting Recorded Video.....                                | 36            |
| Exported Recordings Player .....                             | 37            |
| Prerequisites .....  | 37            |
| Before Installing Player .....                               | 38            |
| Installing the Player .....                                  | 38            |
| Using the Player .....                                       | 38            |
| <br><b>Appendix A — Maintenance Information .....</b>        | <br><b>40</b> |
| Opening a command prompt in Microsoft Windows .....          | 40            |
| Opening the Run dialog .....                                 | 40            |
| Finding out the IP Address of your computer .....            | 40            |
| Windows Events – using the Event Viewer .....                | 41            |
| Configuring Application Log to Overwrite Oldest Entries..... | 42            |
| Viewing Windows Services List .....                          | 42            |
| Checking connectivity of a networked device or computer..... | 44            |
| Troubleshooting .....  | 45            |
| Providing technical support information .....                | 45            |
| <br><b>Index.....</b>  | <br><b>47</b> |

# Chapter 1 – System Overview

This chapter contains information on the following:

- System Components
- System Environment
- Shutting Down the Computer

VSolP Lite's all-in-one architecture is based on one standard Windows PC acting as an IP video stream recording service, surveillance system manager and live video, PTZ control, play back and recorder control client for Windows.

---

**Caution:** When turning off the computer, it is **essential** to shut it down properly — incorrect shutdown could affect the recording element of VSolP Lite and risk loss of previously recorded footage, or recorder system failure. For details, see “Shutting Down the Computer” on page 7.

---

This system is a complex one with Ganz and other manufacturers supplying differing hardware with different feature sets and characteristics. In such systems the adherence to standards is the route relied on to make the overall system work.

The system architecture is based on an Internet Protocol (IP) network — all communication is performed over IP networks — and the surveillance suite software relies on Microsoft Windows technologies.

## System Components

VSolP Lite consists of a combined client/server/Networked Video Recorder (NVR). These components are installed together during installation and work seamlessly together.

## Surveillance Suite Architecture

When the system components are installed on computer hardware and interconnected via a computer network, and given access to compatible IP cameras and networked digital video recorders, the components act together to form a surveillance system.

## IP Camera and DVR Compatibility

A list of compatible devices is supplied separately. Please note that a device should be configured in the manner indicated in the list at system installation time. Device configuration support is not provided by the surveillance software suite.

## System Environment

The system makes use of Internet Protocol based computer networks. The construction of such networks is beyond the scope of this document however the network design must take into full consideration the large quantity of data transferred across networks by surveillance systems.

It is useful however to have a high level discussion of the major areas that should be addressed when designing such a network and choosing the communication parameters of the IP cameras and networked digital video recorders attached to the network.

## Network traffic

Video streamed from IP cameras and networked digital video recorders is the major configurable source of traffic on the network. The quantity of data traffic from each source accumulates as it is consumed by increasing numbers of devices.

Furthermore, since NVRs replay recorded network streams, the amount of data traffic generated is the same as that of the original recorded stream. Multiple playback sessions of the same recorded stream result in an accumulation of data traffic in line with the number of playback sessions. A transcoder/broadcaster software component also adds to network load since it must consume media streams for analysis.

It is therefore critical that IP cameras and networked digital video recorders are configured with a view to the number of potential viewing clients, Video-walls and NVRs recording them. Where there is a requirement for remote sites to view media streams over a restricted bandwidth connection, a transcoder/broadcaster software component can be used to present suitable bandwidth streams. Is this true for VSoIP Lite?

## Infrastructure

When planning system infrastructure, you should take the following into account:

- Cable connections to a typical network switch device have maximum rates of 100 or 1000 megabits per second.
- Network connections between a device and a network switch can be:
  - Half-duplex – they can either send or receive traffic at any given moment.
  - Full-duplex – they can send and receive traffic at the same time.
- A network connection might have traffic from:
  - A single IP camera or networked digital video recorder (DVR) only.
  - Many IP cameras and networked DVRs.
  - IP cameras, networked DVRs and played-back network streams (in the case of NVRs).
  - A transcoder/broadcaster. This software component receives media streams and generates them.
  - An analytics server consuming media streams.
- There may be non-surveillance network data on same network.
- Multicast traffic may help reduce bandwidth requirements. However, it may not be supported by the surveillance suite components.
- A network time server. The presence of a hardware or software based time server is a mandatory requirement. All IP cameras, encoders, networked digital video recorders, server and client computers should obtain their base time from the network time server. For evidential purposes, the central time server should synchronise itself with an external real-world time source. Where there are multiple surveillance site locations, local time servers in each location should provide time to the site. Each local time server should coordinate with the same external real-world time source.

## Configuring Stream Settings

When configuring IP camera and Networked DVR stream settings, you should consider the following:

- Generally more traffic is generated by:
  - High resolutions.
  - High bitrates.
  - High frame-rates.
  - High frame-rate MJPEG streams, which generally tend to generate more traffic than high frame-rate MPEG4 streams of the same resolution.
- More traffic is generated by MJPEG by high frame quality / low compression factor.
- More traffic is generated by MPEG4 by:
  - High I-frame quality.
  - Excessively high P-frame quality.
  - Low p-frame frequency/high I-frame frequency.

- Virtue of scene observed by camera(s): e.g. more data traffic is generated by: PTZ cameras that move through tours of presets, or are frequently moved; noisy feeds from analogue cameras; night-time viewing and automatic gain causing noise, scene subject to motion – crowd scenes, busy roads, in-vehicle safety cameras, etc.
- Using H.264/AVC (MPEG4-part10) encoded video network streams can achieve equivalent video quality to MPEG4-part2 encoded video network streams at lower bandwidth. Consider using H.264 encoding for more efficient use of bandwidth particularly when using mega-pixel video sources.
- Careful infrastructure planning will lead to an overall surveillance system that can be relied on. It is important to locate any network links that are heavily loaded by data traffic.
- It is also worth noting that when viewing live video from IP cameras and networked DVRs on a switched network, data is routed directly from the IP camera or networked DVR to the client component viewing that camera or networked DVR, i.e. it is not received by the server component and then forwarded on to the viewing clients.
- Some IP cameras allow for different streaming rates, depending on which encoder within the camera is connected. One use of such a facility is to have one encoder on the IP camera set to typical live view settings and another encoder in the same camera set to typical recorder settings.
- Mega-pixel cameras require considerable care when deployed with a surveillance system. They can generate considerable traffic, due to their high resolution when used at 25 or 30 frames per second and when using MJPEG. If the integrated VSoIP Lite NVR is used to record high-definition, mega-pixel network streams, this puts a large load on the recorder, consuming a larger percentage of the available network connection bandwidth and consuming more storage space per second than CIF and 4CIF resolution streams.
- Predicting network traffic can be difficult so it is highly recommended that a safety margin be built in to accommodate sudden bursts of higher than average data traffic caused by a faulty camera, or similar.

## System Software

The surveillance suite components are designed to run under the Microsoft Windows XP Professional and 2003 Server operating systems. It is assumed that the operating system installed on computer hardware is that as installed by the computer manufacturer or installed from a genuine copy of the Windows installation media.

---

**Caution:** Anti-virus, anti-spyware and software firewall products should not be installed on surveillance computers.

---

No additional software other than that described as prerequisites to the various surveillance system components should be installed. Adding additional software could have unforeseen impact on the satisfactory performance of the system.

It is common for IT personnel to make changes to various aspects of Microsoft Windows locking down certain features and applying various operating policies. These types of changes are not supported by the surveillance software components.

Microsoft's in-built automatic update feature should be disabled. Instead, updates to the operating system should be carried out prior to installing the surveillance software, and then during planned system maintenance. If automatic updating is enabled unexpected behaviour such as setting changes and unplanned system restarts might occur.

It is important to update all operating system device drivers, particularly for network adapters (and graphic adapters for clients), it is best to use the latest drivers available from the computer manufacturer. If you find that the computer manufacturer uses hardware from a third party, please be certain that using the third-party's driver is appropriate – often computer manufacturers obtain specially crafted variants of the third party's hardware making the usual driver from the third party less than optimal, or completely incorrect.

All surveillance suite software components use Microsoft's .Net framework. This must be installed on all computers. The setup program for the surveillance software will attempt to install the appropriate version of the .Net framework from Microsoft's web-servers if it is not detected on the computer.

The client surveillance suite components use Microsoft's Direct-X. This must be installed prior to running VSoIP Lite, and can be obtained directly from Microsoft.

Server and NVR software components use Microsoft's SQL Express 2005 database management system. This must be installed on all computers using these components. The setup program for VSoIP Lite will attempt to install the appropriate version of the .Net framework from Microsoft's web-servers if it is not detected on the computer.

---

**Caution:** It is recommended that the SQL Express 2005 database management system uses its default values. It should not be secured in a way that prevents the server or NVR from creating or accessing databases. SQL Express should only manage those databases added by the Server and NVR software.

---

Specific version information is discussed in the documentation detailing each surveillance suite software component.

## Shutting Down the Computer

There may be occasions when you need to shut down the computer whilst VSoIP Lite is recording.

---

**Caution:** Incorrectly shutting down the recorder could risk loss of previously recorded footage, or recorder system failure.

Disconnecting Storage Area Network (SAN) connections or external Direct Attached Storage (DAS) connections whilst the recorder is in operation could result in loss of current recordings and possible corruption of previously recorded footage.

---

The recorder continuously writes to storage media whilst operating. If the computer running the recorder needs to be disconnected from the utility power, or if the connection to a storage system is to be removed, the operating system **must** be shut down as follows:

- On the computer running VSoIP Lite, use the Start menu>Shutdown shortcut, OR
- Press the [CTRL], [ALT] and [DEL] keys simultaneously, then choose the Shut Down option.

**Note:** An Uninterruptable Power Supply (UPS) system must be installed to prevent system corruption due to power loss. Please see "Prerequisites" on page 8.

---

**Warning:** If you do not have the necessary privileges to shut down the computer yourself then you **MUST** refer the matter to a user with the necessary authority to do so. **DO NOT** switch off the power supply to the computer as a means of shutting it down. To do so could result in irrecoverable recordings and potentially a partially or fully corrupted system, liable to fail either immediately on restarting or at some time in the future.

---

# Chapter 2 – Installing VSoIP Lite

This chapter contains information on the following:

- Prerequisites
- Before Installing VSoIP Lite
- Installing VSoIP Lite

## Introduction

VSoIP Lite is a Microsoft .Net framework-based application for Microsoft Windows operating systems. It is designed to provide access to surveillance resources such as IP cameras and the VSoIP Lite NVR. VSoIP Lite software comprises three integrated subcomponents: the Server, the Client and VSoIP Lite NVR.

The computer running VSoIP Lite should be a server grade or high powered desktop PC.

## Prerequisites

### Hardware

- Processor: Intel Core 2 Quad Q6600 Quad Core Processor (2.4Ghz, 8MB Cache)
- Memory: 3GB
- Hard Drive/Storage - 500GB SATA II Hard Drive
- Optical Drive - DVD/RW
- 1000-Base T network card configured for full duplex
- A high performance graphic system with Direct Draw hardware acceleration and Direct 3D hardware acceleration — such as an nVIDIA® GeForce 9600GT 256MB DDR2 (or equivalent).

---

**Caution:** In some graphics systems, there is a limit to the maximum number of separate areas of video on-screen that can be supported at the same time, even if they have the two types of hardware enabled acceleration. This limitation appears to a user as if no more than a fixed number of players can show video, i.e. for those video areas that are not displayed, the application otherwise appears as if the video is being displayed. In this case stopping video which is being displayed in one player causes a player that was not showing video to display video. This is not a defect in the application, rather this is a limitation of the graphics system hardware in use.

---

- Uninterruptable Power Supply (UPS) system

To prevent system corruption due to power loss, a UPS system must be installed. This should be of a type that shuts down the operating system automatically if the utility power does not resume before the UPS power fails.

To prepare for this possibility, the computer's power-on settings, operating system, and the UPS system should be configured so that the computer is powered on and the operating system is automatically rebooted as soon as utility power is restored.



## Operating System

Windows XP Professional – service pack 2, or greater, is recommended.

---

**Caution:** In geographical regions where several calendar types are used, please ensure that your regional Date/Time setting is set to use the Gregorian calendar.

---

## Additional mandatory software

- Microsoft .Net Framework 3.5 – includes .Net frameworks 1.1, 2.0, 3.0 and 3.5 – automatically downloaded from Microsoft if not present at install time. Also available from Microsoft's web-site as a download
- Windows Installer 3.1
- Microsoft Direct-X 9.0c (March 2009)
- Microsoft SQL-Express 2005 SP 2 or above
- Microsoft Internet Explorer 7 or later.

**Note:** Microsoft frequently re-designs its websites therefore an Internet download link is not provided. Instead we recommend that you use Google or another search engine to find the download links for the mandatory software. On examining the search results, please ensure that the download source is Microsoft.

## Before Installing VSolP Lite

### Operating System Settings

The PC should have the operating system installed either by the computer manufacturer or from the operating system installation media. The computer is assumed not to be the member of any Windows network domain.

**Note:** Changes to the operating system settings, such as changing the local or global policies relating to rights and permissions, are discouraged. These notes assume that the operating system is set up in a fresh installed state.

A local user account should be added. This should be a member of the local administrator group. Software installation, .Net installation and Direct-X installation, and all maintenance should be carried out as this local user with local administrative rights.

To prevent unscheduled system restarts, switch off the automatic Windows update feature. Updates to the Windows operating system should be carried out as part of scheduled system maintenance.

### Networking

Set up the network settings for the PC and make sure that the PC network connection is enabled and connected. To do this:

- 1 Open a command prompt.
- 2 Enter the command **ipconfig**

If IP address, subnet mask and gateway for the network connection intended to be used as part of the surveillance network are listed then your connection is enabled and connected. The ipconfig command should not indicate 'media disconnected' for this connection.

---

**Caution:** The surveillance system is designed to work in systems where there is a single active network connection. Multiple network cards are not supported and there is no mechanism within the system to define to which network card the software should bind.

---

## Firewall Information

Any local software firewall should either be disabled, or carefully configured so as not to prevent VSoIP Lite from contacting IP cameras or other additional software applications. Also, any hardware firewall on the LAN should be configured to allow appropriate network access to the PC on which VSoIP Lite is executing. Some local, software-based firewalls block incoming/outgoing traffic solely on a port number basis. Others block ports to all but explicitly defined applications.

**Table 4** Firewall-related setup data

| Application   | Role                 | Default Path                     | Port Number | Note                                   |
|---------------|----------------------|----------------------------------|-------------|--|
| Setup.exe     | VSoIP Lite installer | installation media               | 80/TCP      | The bootstrap installer for VSoIP Lite |
| MSI file      | VSoIP Lite installer | installation media               | 80/TCP      | The main installer for VSoIP Lite      |
| VSoIPLite.exe | Application          | C:\Program Files\GANZ\VSoIP Lite | 7002/TCP    | VSoIP Lite application                 |

**Note:** Blocking the required ports and/or not allowing VSoIP Lite and related applications to use the network can prevent successful installation, activation or execution of VSoIP Lite.

The port information and network transport for all IP cameras and encoders that are be controlled and viewed should be added to the firewall rules.

## Additional Security Software

It is not advisable to execute the following on the PC unless the impact of their execution is considered carefully:

- Anti-virus
- Anti-spyware
- Software firewall

## .Net Framework

The installation program for VSoIP Lite will automatically download the correct version of the .Net Framework. However, if preferred, install the .Net Framework prior to installing the software. No configuration of the .Net Framework is required.

## Windows 3.1 Installer

The installation program for the .Net will automatically download Windows 3.1 Installer if required. If preferred, the Windows 3.1 Installer can be installed prior to installing the software.

## Direct-3D Hardware Support and Microsoft Direct-X 9.0c or above

To ensure maximum performance, the VSoIP Lite PC requires an excellent graphics sub-system. The minimum requirement is a graphics sub-system capable of hardware accelerated Direct 3D rendering. You should have also installed the latest released graphic drivers either from the graphics sub-system manufacturer or from the PC manufacturer.

---

**Caution:** When using MegaPixel cameras or encoders, the resolution of the rendered image might exceed the Direct -X 3D capabilities of the graphics adapter or driver. Where this occurs, the displayed image will be missing regions of the actual image being sent from the camera and can also be distorted. This is not a fault of the software but is a limitation of the graphics sub-system. Please ensure that the graphics adapter you select can render textures on a Direct-X surface equal to or greater than the resolution of the mega-pixel source.

---

**Note:** Some graphic sub-systems are modified to work in the PC manufacturer's hardware.

Use Direct-X diagnostics to determine which version of Direct-X the VSoIP Lite PC is using, and whether the graphics sub-system is able to support Direct 3D, as follows:

- 1 From the Windows Start menu, select Run.
- 2 In the Run dialog, enter **dxdiag**.
- 3 On the System tab, find the System Information entry for Direct-X version. Check this is 9.0c or a higher revision number.

On the Display tab, find the Direct 3D Acceleration entry and ensure that it is enabled. If either the version or 3D support is unsatisfactory, the system will be unable to run VSoIP Lite.

## SQL-Express

The installation program will automatically download Microsoft SQL-Express 2005 if it is not already present on the PC.

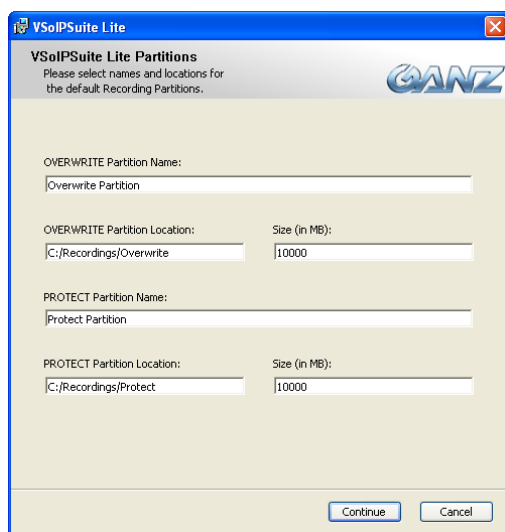
## Installing VSoIP Lite

This section explains how to install VSoIP Lite for the first time on your computer.

- 1 Log in to the computer using the user name of the local user with administrative level privileges.
- 2 Double-click the setup.exe file to start installation.

The VSoIP Lite installer program setup.exe automatically examines the local system for the .Net Framework, SQL-Express, Direct-X and Windows Installer 3.1. If these are not present, or earlier versions are installed, the installer program automatically connects to Microsoft's servers over the Internet and downloads the correct versions of the software.

- 3 After accepting the terms and conditions, you are prompted to specify the name and size of the recording partitions that will be used to store recordings. You can accept the defaults, or change the names, locations and sizes to suit your system.



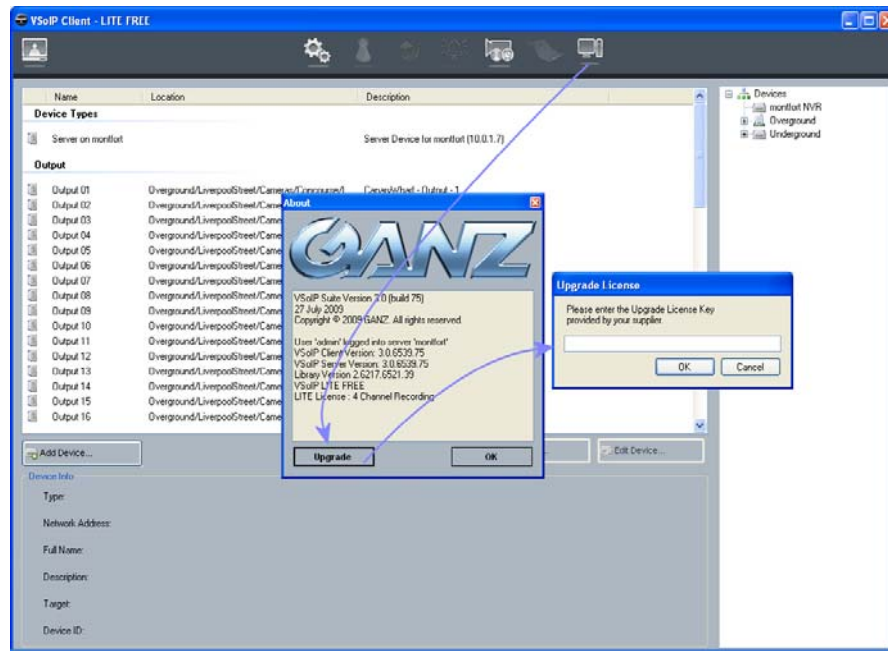
**Figure 1** Setting up recording partitions

- 4 Click Continue to finish the installation.

## Upgrading a License

If you have purchased an upgrade for your current version of VSoIP Lite, you need to activate the upgrade, as follows:

- 1 Click the System Configuration icon on the toolbar, as shown in Figure 2.



**Figure 2** Activating an upgrade of VSolP Lite

- 2 Click Upgrade, and enter the license key you have been given.
- 3 Click OK. The About box is updated to indicate the new license.

# Chapter 3 – VSoIP Lite Configuration

This chapter contains information on the following:

- Getting Started
- Adding Devices
- Deleting Devices
- Configuring Video Sources
- Configuring Pan-Tilt-Zoom Capabilities
- Working with Live Video and PTZ
- Working with Alarms
- Playing Back Recorded Video
- Exported Recordings Player

VSoIP Lite contains several configurable aspects, including collections of IP cameras and Networked DVRs.

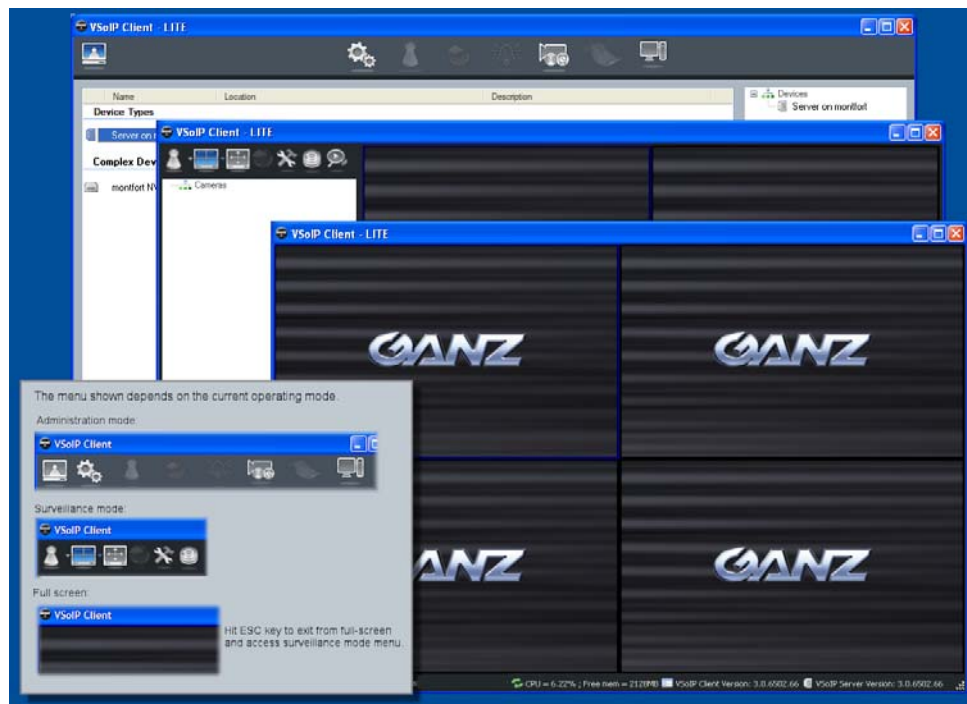
## Getting Started

We recommend that you take the following steps when configuring VSoIP Lite:

- 1 Start VSoIP Lite. To do this, select Programs>VSoIPSuite Lite from the Start menu.

**Note:** If the application does not start, this may be because another instance of the application has been detected. If the other instance is running normally, it is brought to the front. If the other instance is in the process of shutting down, it is terminated immediately and the new instance is started.

- 2 Add devices to the system.
- 3 Configure alarm triggers.



**Figure 3** Accessing VSoIP Lite's main menu

## User Configuration

VSoIP Lite is preconfigured with three users - Administrator, Manager and Operator.

- **Administrator** — has access to all functionality.
- **Manager** — has access to all functionality, with the exception of adding, editing or deleting devices and disabling recording schedules.
- **Operator** — can view live and recorded video. Supervisor authentication is required to view recordings.

## Device Configuration

A device can be one of the following:

- An IP camera.
- An IP encoder.
- A Networked DVR.

Some devices such as a Networked DVR or an IP encoder can have several analogue camera inputs. In addition, certain devices have multiple encoders for each analogue camera input.

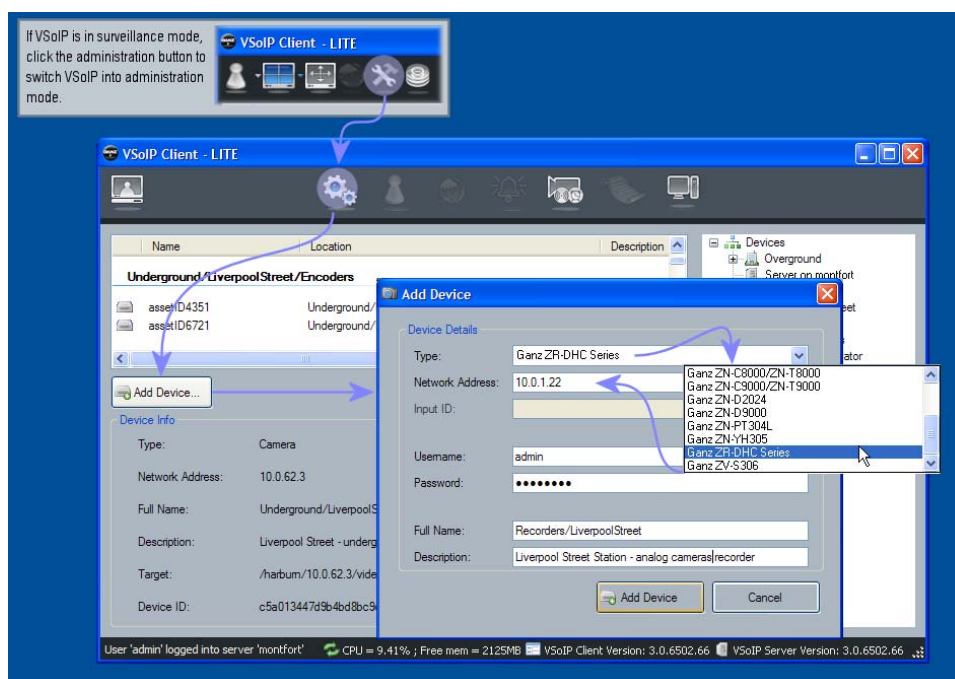
This means that a single device such as an IP camera could generate several video sources, one for each encoder built in to the camera.

Some devices support trigger inputs. These are sources that signal some event has happened. For some devices this represents a simple electrical voltage being applied to a single input pin. Other devices such as Networked DVRs the signal can be as the result of some rule set defined within the Networked DVR.

IP cameras and Networked DVRs can optionally support Pan-Tilt-Zoom (PTZ) devices. A PTZ allows the camera's field-of-view to be altered using the pan-tilt- zoom controls in the Client.

**Note:** The surveillance system is preconfigured with a number of types of Ganz IP cameras, Networked DVRs, pan-tilt-zoom control units and protocols.

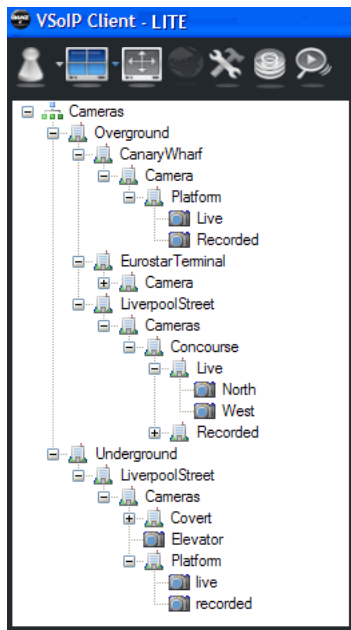
## Adding Devices



**Figure 4** Adding a device

**Note:** If you are adding a device which needs to use a particular port number, add it after the IP address, in the format 192.168.1.2:6400.

## Location Text and the slash character ('/')



**Figure 5** Device hierarchy example

Location text is used by the System to logically group devices. An example of the location text can be seen by looking at the presentation of the device hierarchy or “site” in the Client. When constructing a location string each level of the hierarchy is defined by the use of the forward slash character, e.g. ‘/’.

If the location string is left blank then the name of the device is the sole label for the device and is shown at the top level of the hierarchy. A location string entered without slashes adds the device one level down in the hierarchy with a top level entry labelled by the location string. A location string containing two labels separated with a single slash adds the device two levels down the hierarchy, with the text before the slash labelling the device at the top level, the text after the slash labelling the device at the second level and then finally the name of the device labelling the third level.

By naming different devices with common top, second, third, etc location text labels, a number of devices can share some or all of the same location text.

Some location text examples as shown in Figure 5:

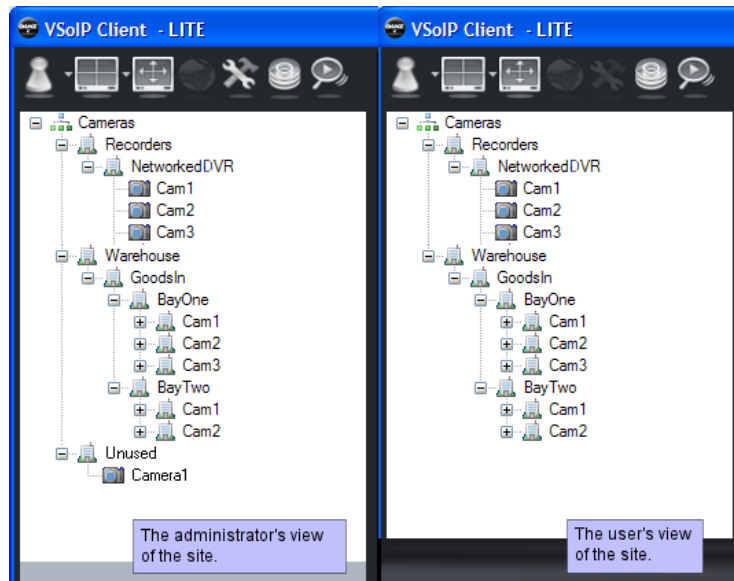
- Overground (shared with Canary Wharf, EurostarTerminal and LiverpoolStreet)
- Underground (shared with LiverpoolStreet)

### Location Text Example

Assume you have a series of video sources with views of different sections of a warehouse.

- Three IP cameras viewing bay one in goods-inward: Cam1, Cam2, and Cam3.
- Two IP cameras in bay two of goods-inward: Cam1 and Cam2.
- Three IP cameras in goods-inward: Cam1, Cam2 and Cam3.

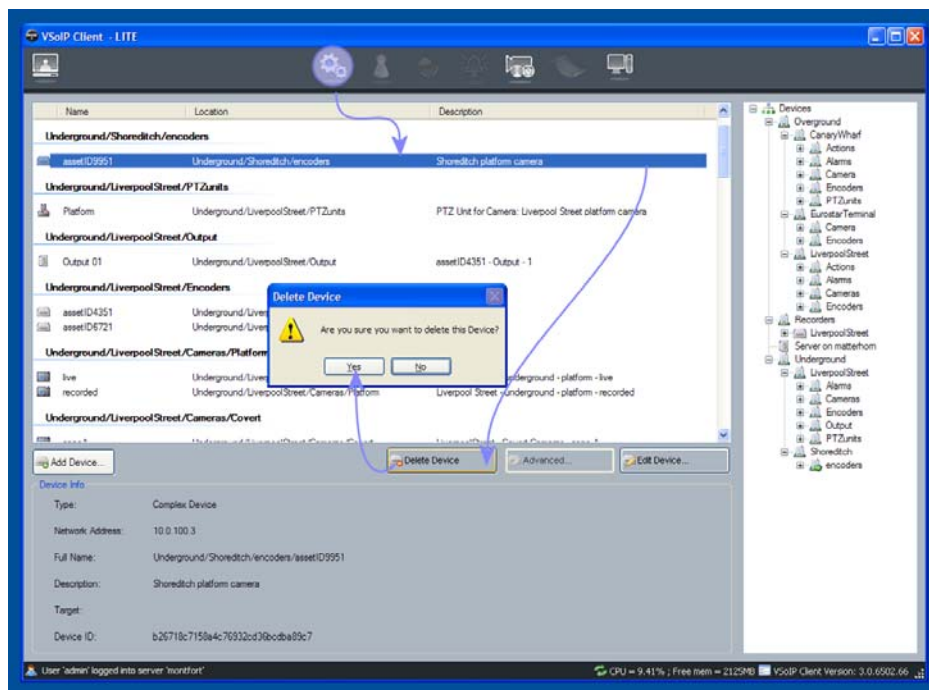




**Figure 6** Warehouse site location text example

- 1 Add three IP camera devices with names Cam1, Cam2 and Cam3 and use the same location text: Warehouse/GoodsIn/BayOne.
  - 2 Next add two more IP camera devices with names Cam1 and Cam2 and use the same location text for both: Warehouse/GoodsIn/BayTwo.
  - 3 Add a Networked DVR device named NetworkedDVR with location text Recorders.
  - 4 Next name inputs 1, 2 and 3 of the DVR Cam1, Cam2 and Cam3 respectively.
- Using the name and location text as described above will result in a site as shown in Figure 6.

## Deleting Devices



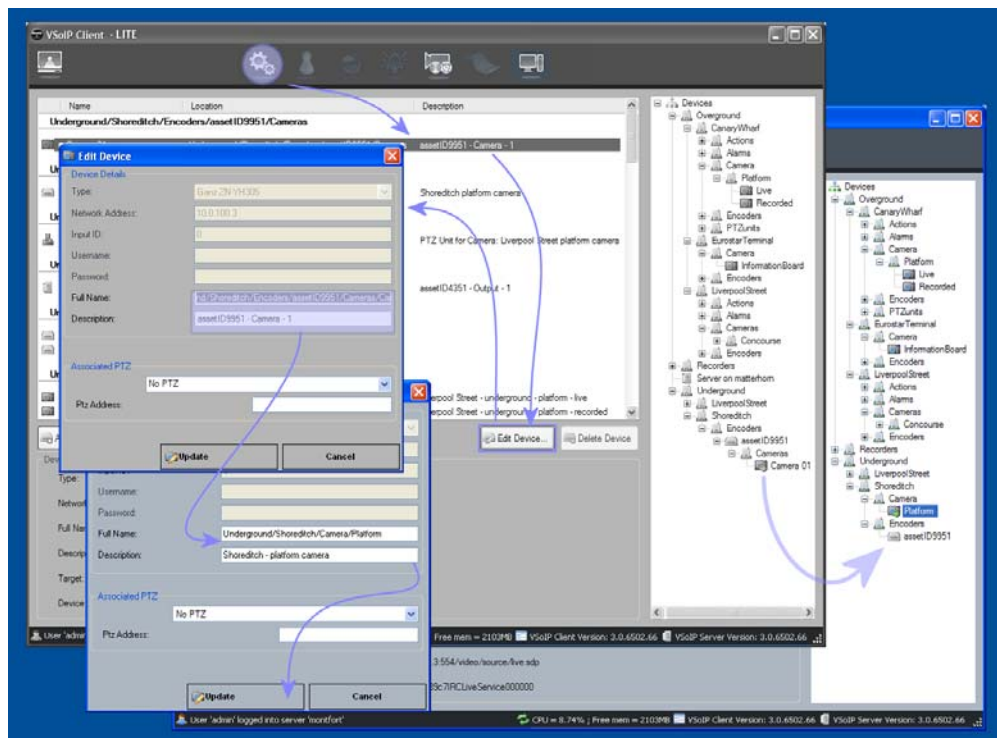
**Figure 7** Deleting a device

**Note:** When deleting a device such as an IP encoder, all associated sub-devices related to that device are also deleted, e.g. PTZ units, etc.

## Configuring Video Sources

An IP camera or Networked DVR supports one or more video sources. Each video source has a default name. When a device is initially added to the system, the various video sources are named automatically and grouped into a sub-hierarchy under the device.

The automatically assigned name and location text can be changed, allowing you to group the video sources logically.



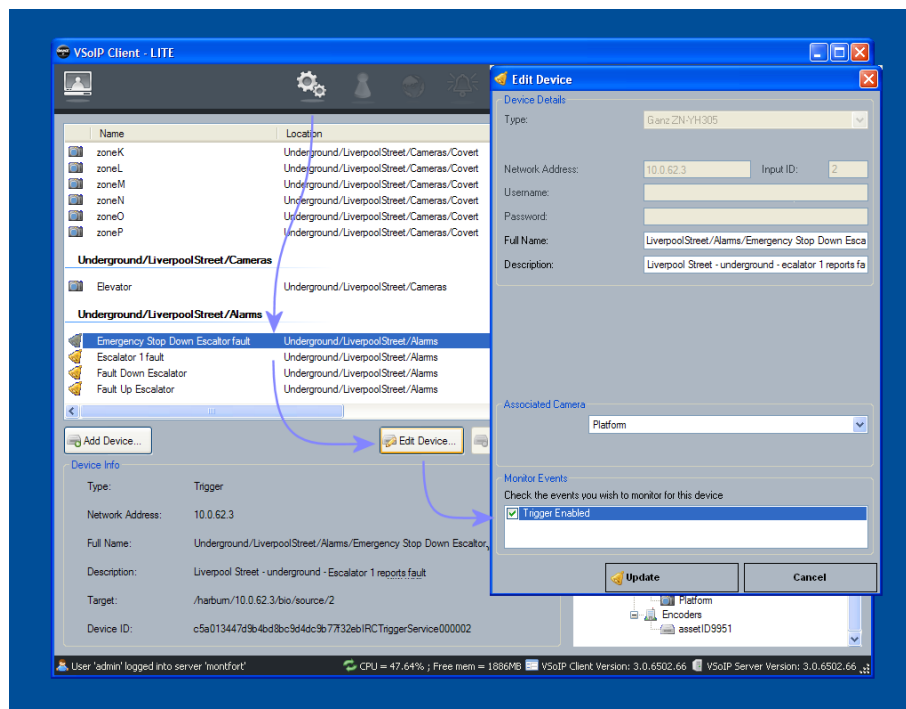
**Figure 8** Renaming/setting location for video source

**Note:** Using the location text, group all Networked DVRs together in their own logical group of recording devices. Next rename and modify the location text for the various video sources of IP cameras and Networked DVRs to allow the physical layout of the surveillance site to be readily understood from the site/device hierarchy.

## Configuring Triggers

A trigger is the source of an alarm, such as an alarm contact on an IP camera or a Networked DVR. Alternatively, it could be the result of some alarm process logic running on a Networked DVR, e.g. an alarm contact plus a video motion event and an enabling schedule on the Networked DVR resulting in an alarm from the Networked DVR.

**Note:** This is a DVR feature rather than a software feature within the surveillance suite.



**Figure 9** Activating and naming triggers

To activate a trigger:

- 1 Select the alarm you want to edit from the list and click Edit Device.
- 2 Select the camera associated with this alarm. This allows operators interacting with the alarm to easily see a related video feed.
- 3 Check Trigger Alarms. This allows VSoIP Lite to receive alarms.
- 4 Click Update.

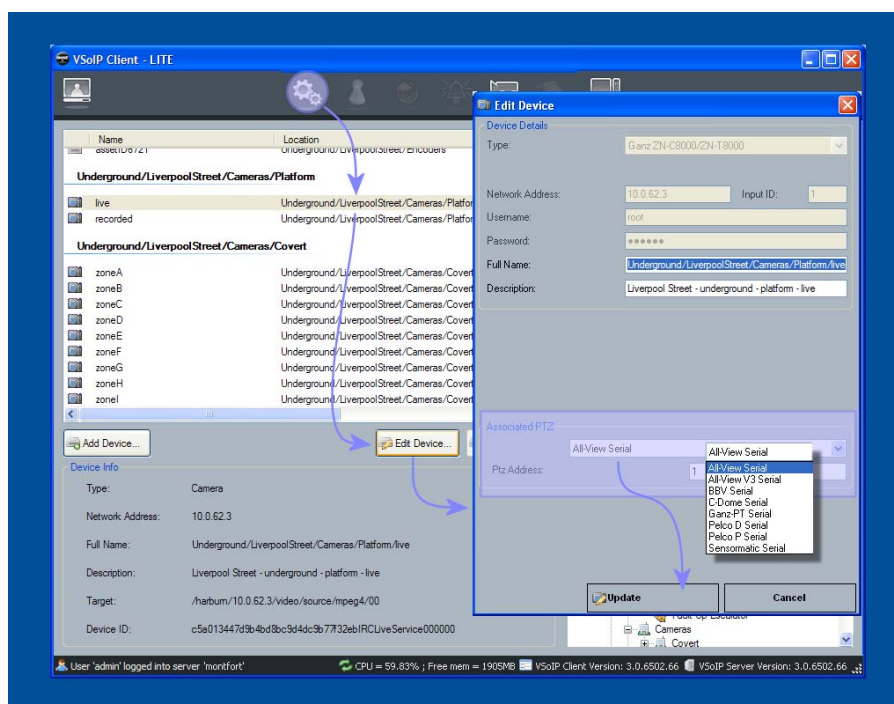
**Note:** Triggers can either be actively monitored or not. When updating a trigger make sure that you have enabled monitoring of events for that trigger.

Use the location text to logically group triggers into groups that make sense for the physical site being monitored.

You cannot delete triggers. If one or more triggers available from a device are not required, then disable monitoring of each trigger event. You can collect unused triggers together under a logical group of unused triggers keeping them separated from the triggers in use.

## Configuring Pan-Tilt-Zoom Capabilities

IP cameras and Networked DVRs can provide connections that enable one or more pan-tilt-zoom control units to be attached. In some cases the IP camera includes a built-in pan-tilt-zoom controller.



**Figure 10** Enabling PTZ capability for a video source

Some cameras, typically those attached to video encoders, might be connected to a PTZ controller unit. This is usually done using the serial port of the video encoder. E.g. ZN-T9000 connected to a C-ALLVIEW.

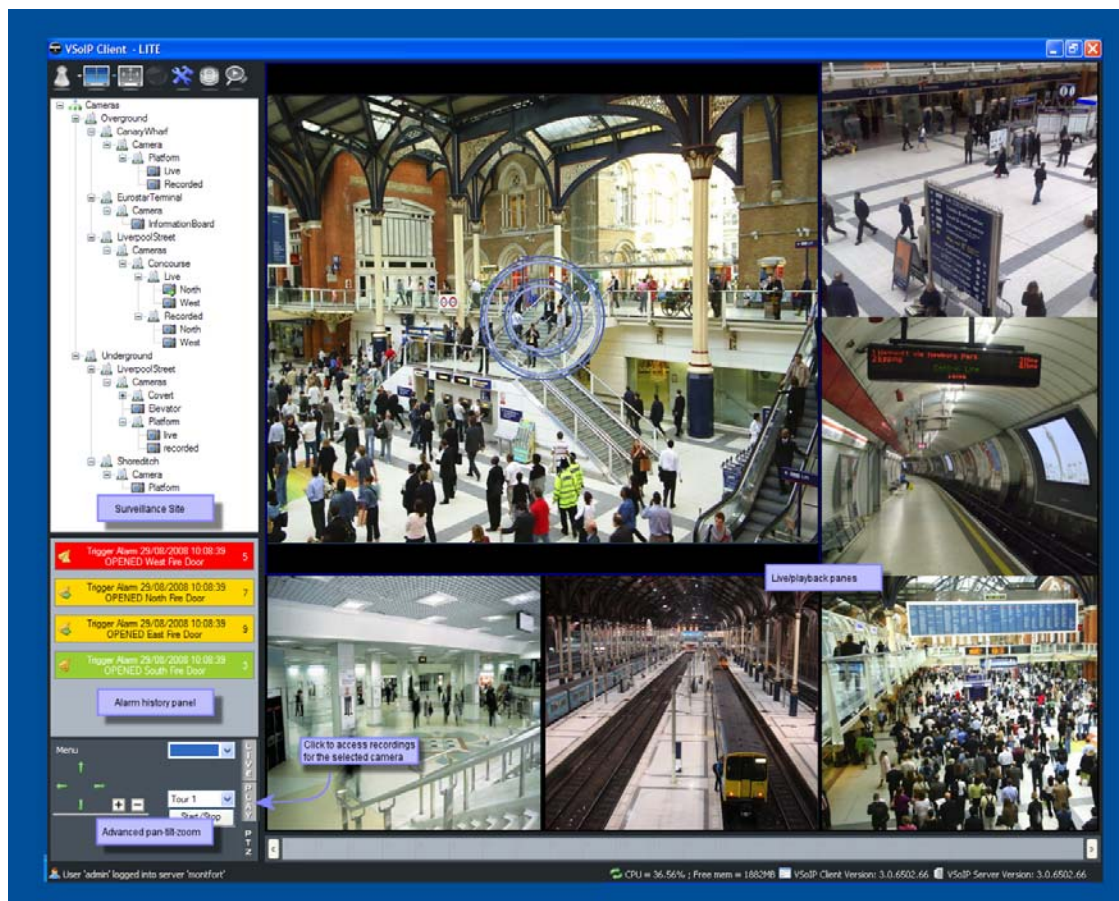
A typical arrangement with encoders is using several analogue inputs alongside several PTZ units. The CCTV installer will use different PTZ addresses when sharing a common serial port.

Under this arrangement, find out the appropriate PTZ address for the camera and PTZ unit pairing and set the appropriate PTZ address when associating a PTZ with an analogue camera.

## Working with Live Video and PTZ

VSoIP Lite allows CCTV operators to view live video from IP cameras and cameras attached to networked DVRs. It also allows the operator to move pan-tilt-zoom (PTZ) cameras, to zoom in closer to the scene displayed, and to take a snapshot of a particular moment. The video panes, or cameos, making up the operator's viewing area can be laid out in various ways as suits the operator's needs and the capabilities of the display hardware.

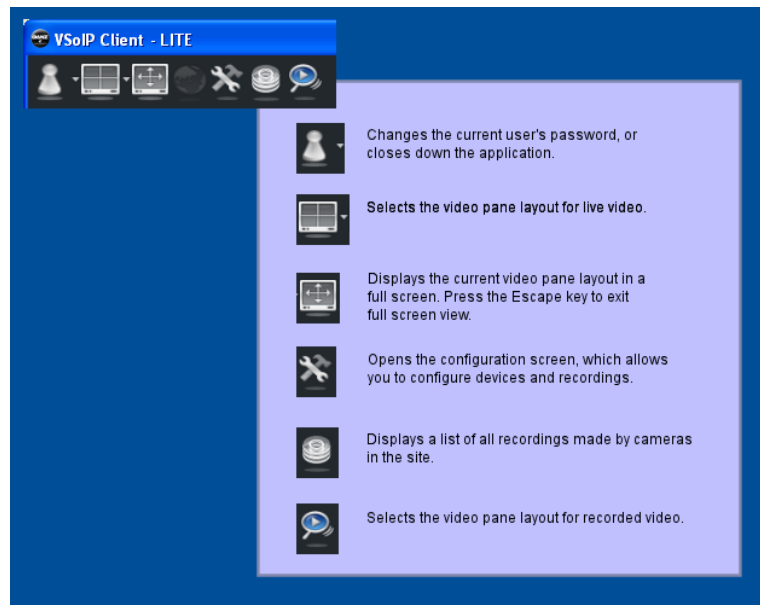
### Live View Controls



**Figure 11** Main live viewing controls


### Accessing other features

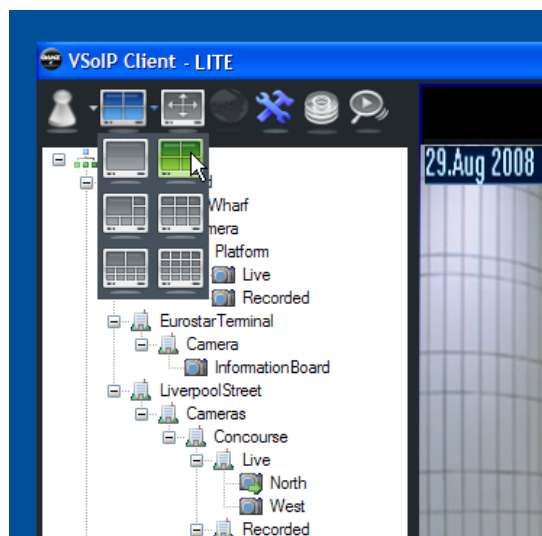
The main menu can be used to switch the Client into various surveillance modes including live viewing.



**Figure 12** Location of main menu

## Specifying Video Pane Layout

To specify a video pane layout:, click  and select the required layout from the drop down menu.



**Figure 13** Selecting a video pane layout



## Starting and Stopping Live Video

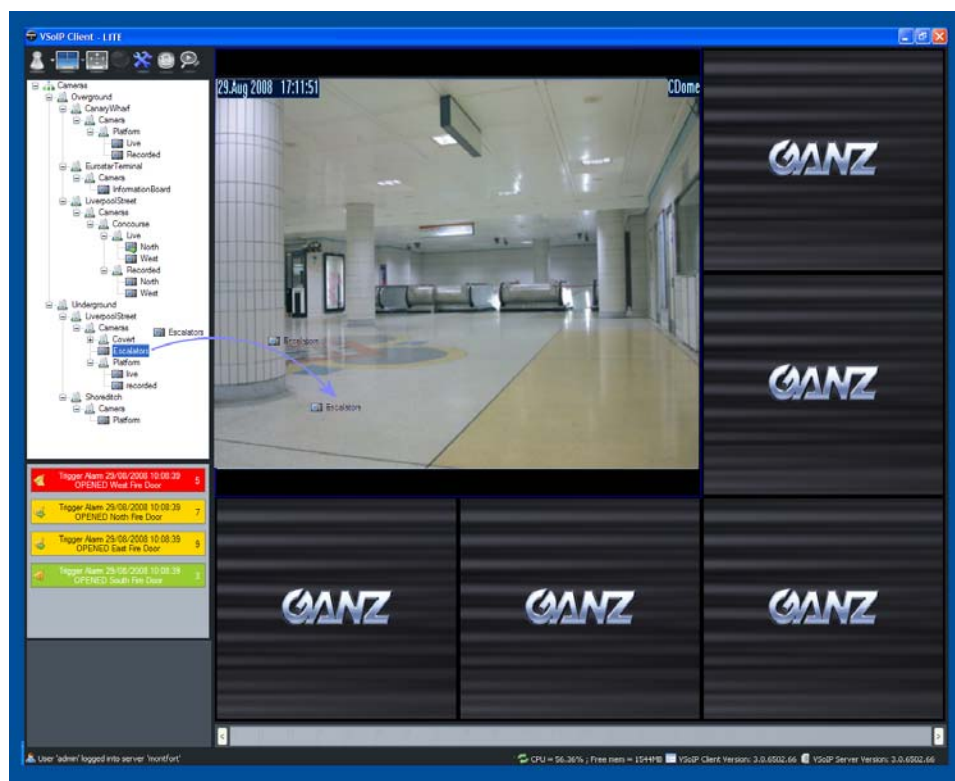


Figure 14 Starting video using mouse drag-drop

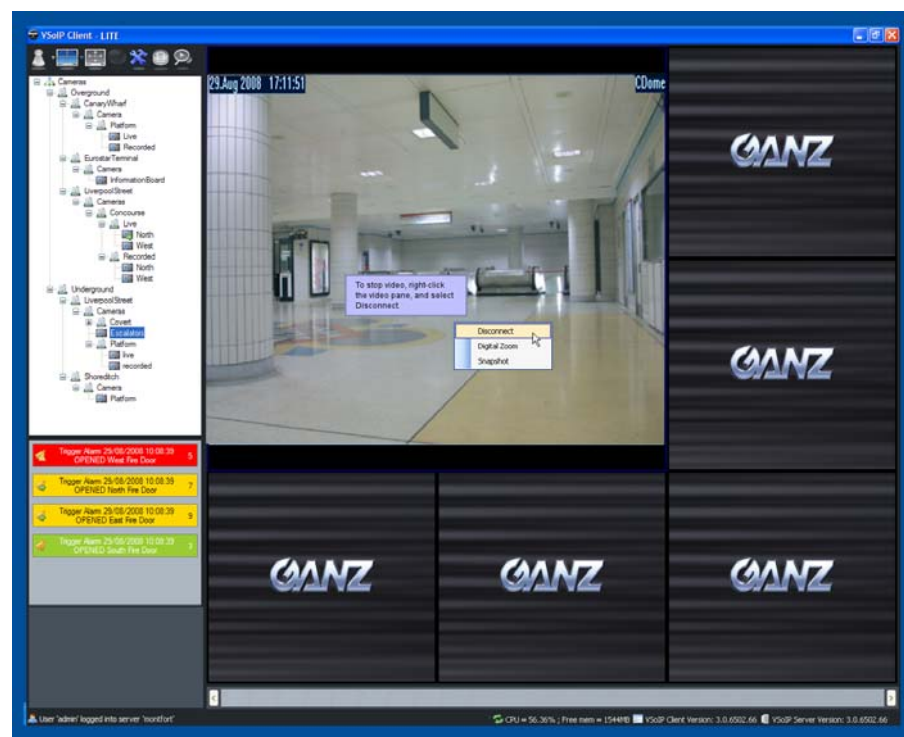
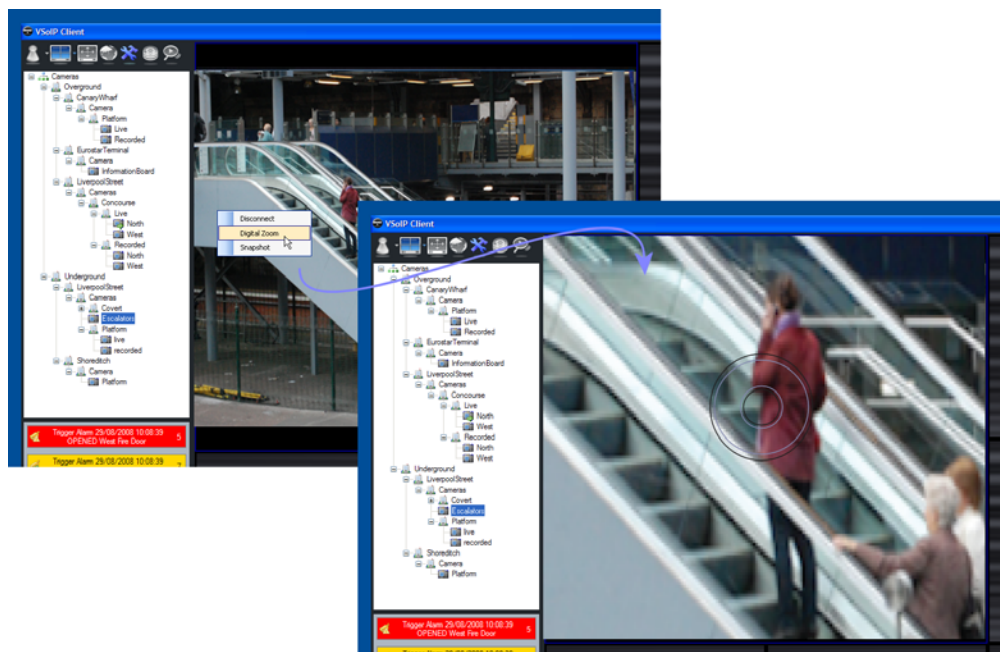


Figure 15 Stopping video

## Using Digital Zoom

VSolP Lite allows you to zoom in on and move around live video footage.

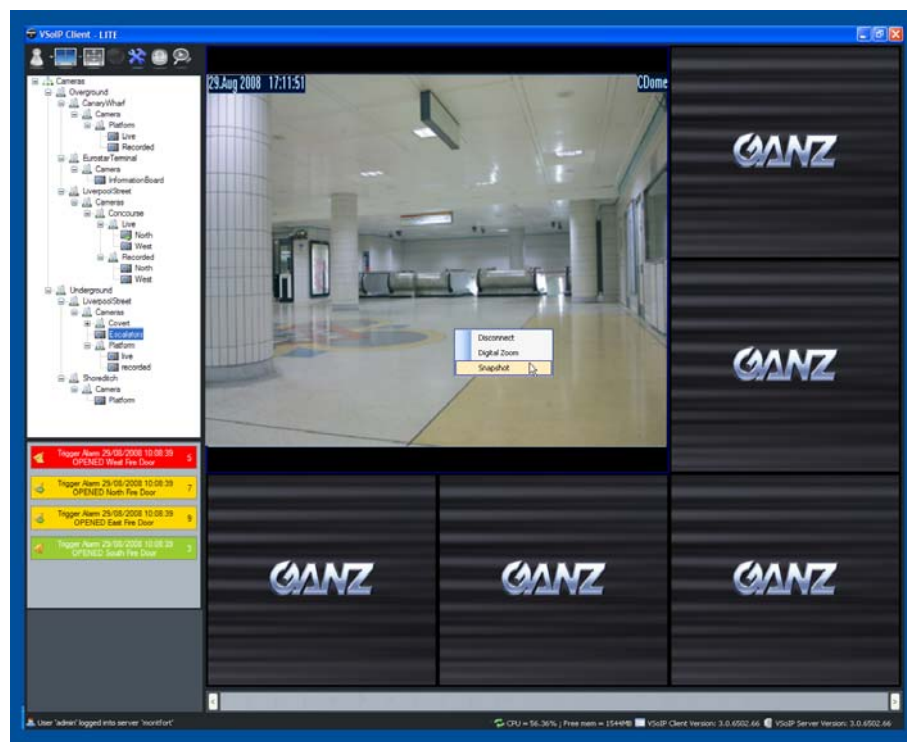


**Figure 16** Zooming into live video

Click the part of the video pane that you want to see in more detail, then use the mouse scroll button to zoom in and out as required.

## Taking a Snapshot of Live Video

VSolP Lite allows you to capture snapshots of live video playing in a video pane. By default, these are saved to \Desktop\VSolP Image Clips\FromLiveDevices, as .jpeg images. To take a snapshot, right-click in the pane displaying the video at the point you want to capture.

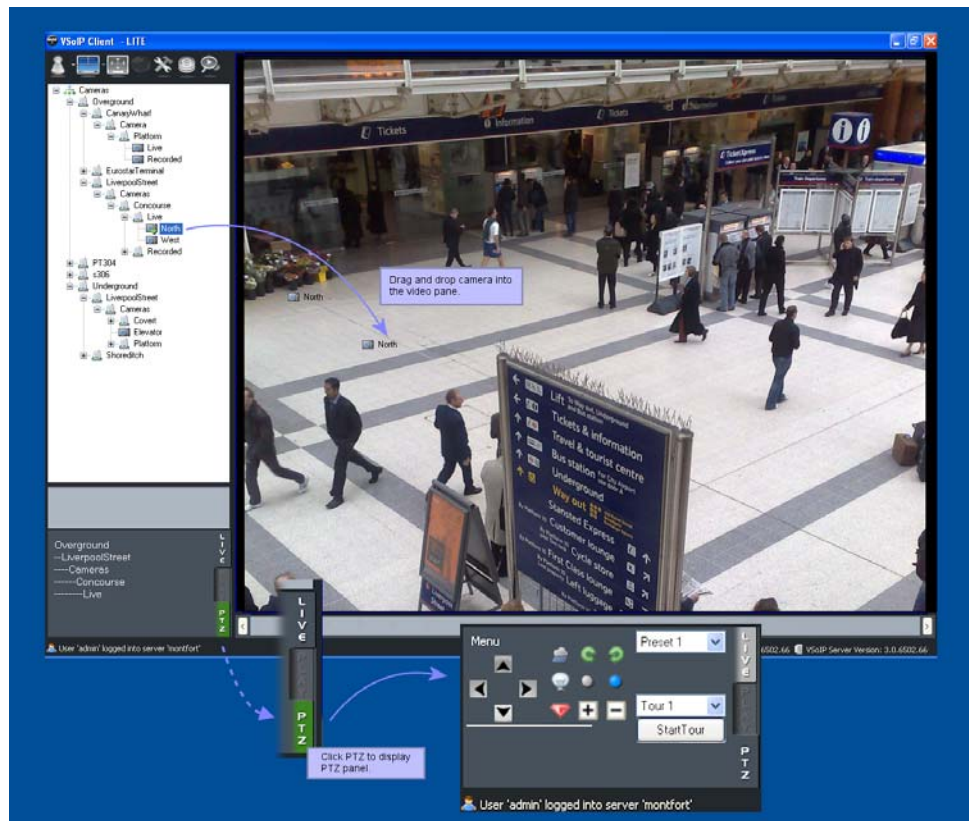


**Figure 17** Taking a snapshot of live video



## Control of Pan-Tilt-Zoom

### Activation/Deactivation



**Figure 18** Activating/deactivating PTZ support

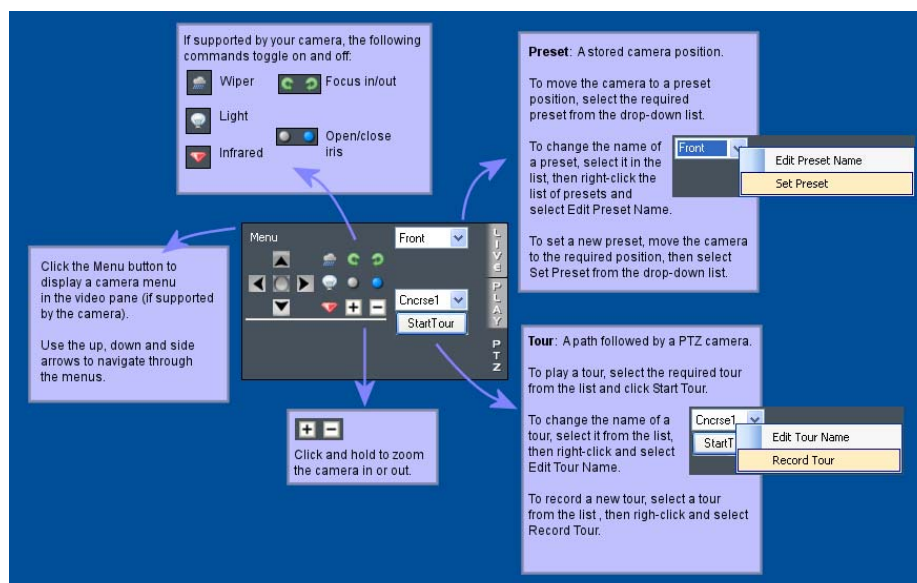
### Moving and Zooming



**Figure 19** Panning, tilting and zooming

## Extra features

Some PTZ cameras and protocols provide access to extra functionality, which allows you to carry out extra commands, such as using presets or tours. These are detailed below.



**Figure 20** Additional PTZ unit features support

**Note:** PTZs vary in functionality, so access to features depends on the chosen PTZ unit's capability.

## Working with Alarms

The alarm display presents unacknowledged, acknowledged and closed alarms.

**Note:** To enable the Client to display an alarm for a particular alarm source, e.g. contacts on a Networked DVR, the alarm type for the device associated with the alarm source must have been enabled during the setup of the surveillance site. For details, see “Configuring Triggers” on page 19.

### Overview of Alarm Display

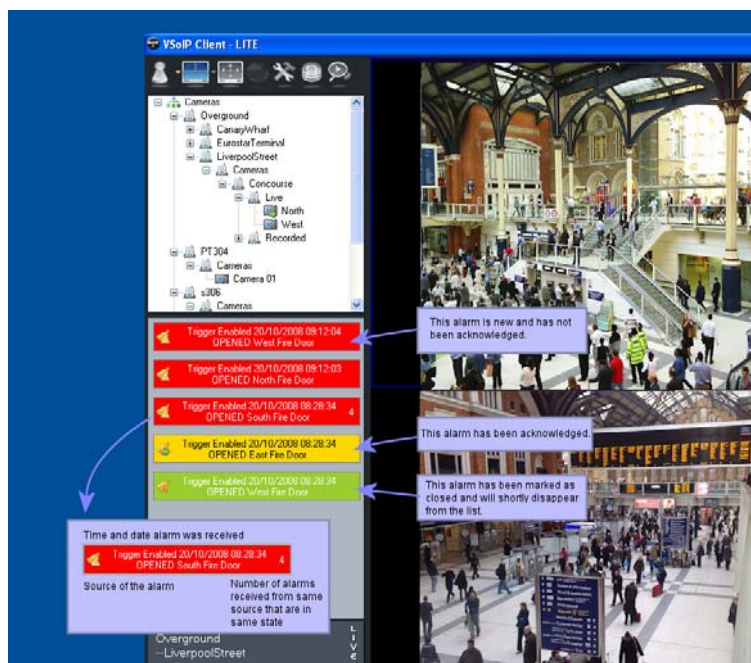


Figure 21 Overview of alarm display

### Viewing Properties of an Alarm

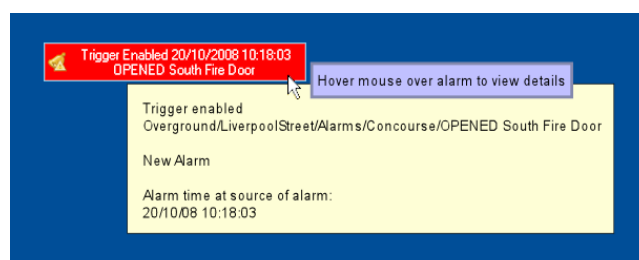
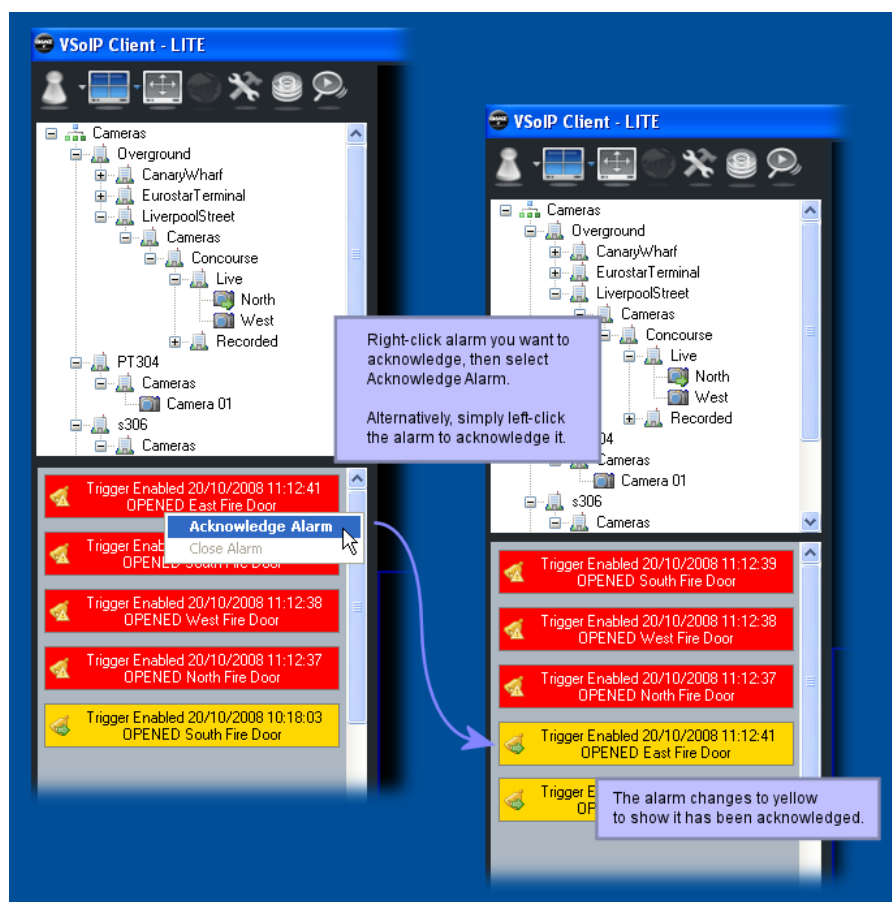


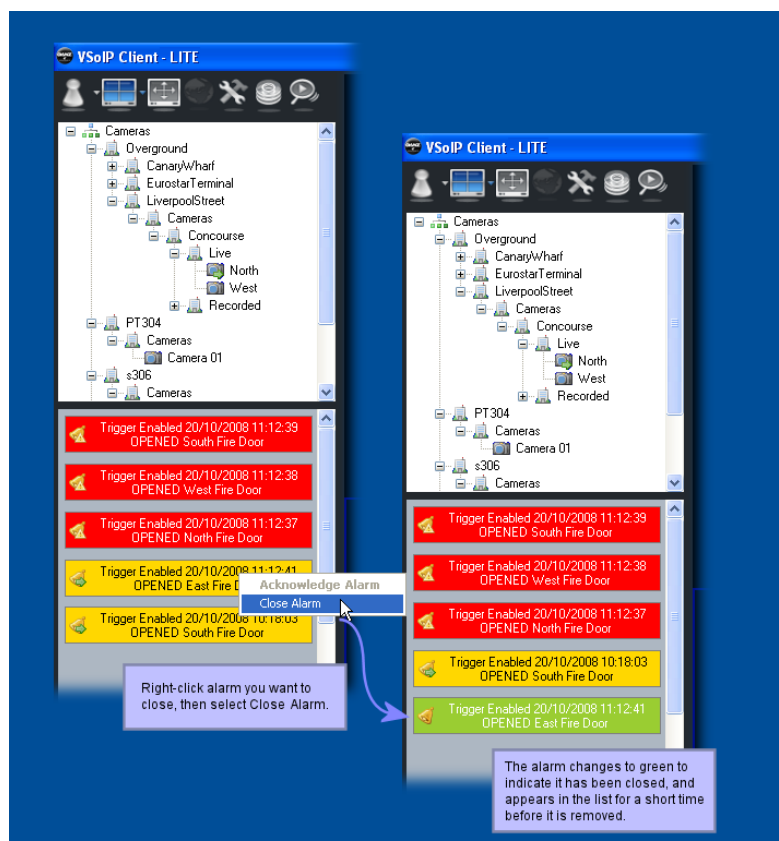
Figure 22 Alarm properties

## Acknowledging an Alarm



**Figure 23** Acknowledging an alarm

## Closing an Alarm



**Figure 24** Closing an alarm

# Chapter 4 – Recording with VSoIP Lite

This chapter contains information on the following:

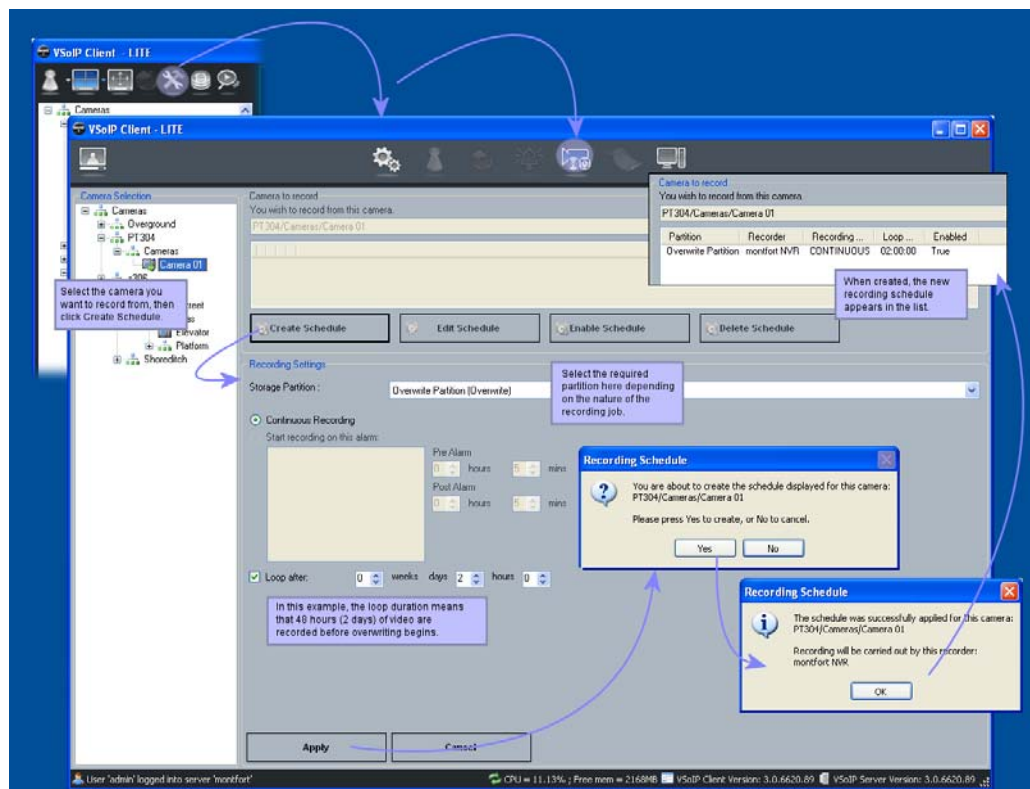
- Recording Camera Footage
- Playing Back Recorded Video

## Recording Camera Footage

VSoIP Lite allows you to record continuously from cameras in your surveillance site. You can then play back the recorded footage (see “Playing Back Recorded Footage” on page 31).

### Creating a Recording

Figure 25 indicates how to create a camera recording.



**Figure 25** Starting recording from a camera

You can specify whether the NVR should automatically remove older recordings for the job or whether this is carried out manually by a user with privileges to delete recordings.

A looped recording job deletes older recording footage automatically when that footage reaches a certain age. If you do not want recordings to be deleted automatically, deselect Loop after.



## Playing Back Recorded Video

VSoIP Lite allows users to view up to 4 recordings simultaneously. Recording footage is stored on the integrated NVR which is installed at the same time as VSoIP Lite. For information on creating recordings, see "Recording Camera Footage" on page 30.

**Note:** In this section the term *recorders* is used to mean Networked DVR or NVR.

## Discovering Recorded Footage

The screenshot displays the VSoIP Client - LITE interface. The left sidebar shows a tree view of cameras, with 'Underground' selected. The main window shows a table of recordings with columns: Camera Name, Camera Location, Start Time, End Time, Recorder Name, and Recorder Location. The table lists several recordings for 'zoneA' and 'zoneB' cameras. Below the table is an 'Event Category' and 'Event Type' list. The 'Events' pane on the right shows a list of events for the selected recording. Annotations provide instructions on how to filter recordings by camera location, how to view events for a specific recording, and how to delete recordings.

**Recordings Table:**

| Camera Name | Camera Location                           | Start Time          | End Time     | Recorder Name   | Recorder Location |
|-------------|---|---------------------|--------------|-----------------|-------------------|
| zoneA       | Underground/LiverpoolStreet/Cameras/Cover | 18/10/2008 09:22:36 | Not Finished | LiverpoolStreet | LiverpoolStreet   |
| zoneB       | Underground/LiverpoolStreet/Cameras/Cover | 18/10/2008 09:14:47 | Not Finished | LiverpoolStreet | LiverpoolStreet   |
| zoneC       | Underground/LiverpoolStreet/Cameras/Cover | 18/10/2008 09:21:24 | Not Finished | LiverpoolStreet | LiverpoolStreet   |
| zoneD       | Underground/LiverpoolStreet/Cameras/Cover | 18/10/2008 09:09:22 | Not Finished | LiverpoolStreet | LiverpoolStreet   |
| zoneE       | Underground/LiverpoolStreet/Cameras/Cover | 18/10/2008 09:08:56 | Not Finished | LiverpoolStreet | LiverpoolStreet   |
| zoneF       | Underground/LiverpoolStreet/Cameras/Cover | 18/10/2008 09:05:14 | Not Finished | LiverpoolStreet | LiverpoolStreet   |
| zoneG       | Underground/LiverpoolStreet/Cameras/Cover | 18/10/2008 09:06:57 | Not Finished | LiverpoolStreet | LiverpoolStreet   |

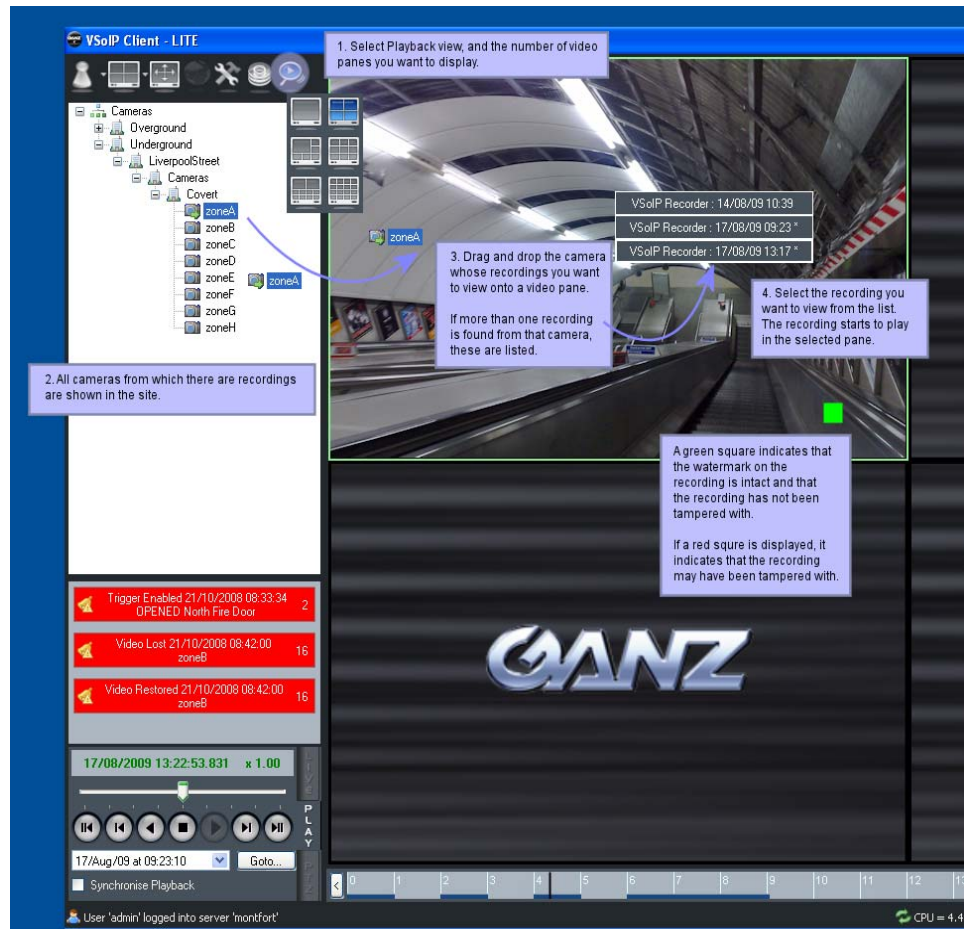
**Event Category and Event Type:**

| Event Category | Event Type          | Time                     | Username |
|----------------|---------------------|--------------------------|----------|
| Device Events  | Device Connecting   | 20 October 2008 13:42:38 | admin    |
| Device Events  | Device Connected    | 20 October 2008 13:42:38 | admin    |
| Device Events  | Device Disconnected | 20 October 2008 13:42:43 | admin    |
| Device Events  | Device Connecting   | 20 October 2008 13:42:53 | admin    |
| Device Events  | Device Connected    | 20 October 2008 13:42:53 | admin    |
| Device Events  | Device Disconnected | 20 October 2008 13:42:55 | admin    |
| Device Events  | Device Connecting   | 20 October 2008 13:42:56 | admin    |
| Device Events  | Device Connected    | 20 October 2008 13:42:56 | admin    |
| Device Events  | Device Disconnected | 20 October 2008 13:42:58 | admin    |
| Device Events  | Device Connected    | 20 October 2008 13:44:07 | admin    |
| Device Events  | Device Disconnected | 20 October 2008 13:44:20 | admin    |
| Device Events  | Device Connecting   | 20 October 2008 13:44:20 | admin    |
| Device Events  | Device Connected    | 20 October 2008 13:44:20 | admin    |
| Device Events  | Device Disconnected | 20 October 2008 13:44:36 | admin    |

**Figure 26** Recordings discovery

## Playing Back Recorded Footage

Search for the name of the IP camera or camera input on a Networked DVR to locate a recording. Choose to play back and then review the footage to locate the time of interest.



**Figure 27** Initial playback and reviewing footage

**Note:** If your mouse has a scroll button, you can zoom in and out quickly on the timeline. Position your mouse over the area of the timeline you want to view in more detail, and move the scroll button up to zoom in, and down to zoom out.



## Playback Controls

Once playback starts, various playback controls are available: rewind, fast forward, pause, resume, step-backward, step-forward. Also, the current position is indicated as a date and time.

**Note:** Not all recorders can perform every playback control, e.g. step-back. If an operation is not possible, the request to perform it is ignored.

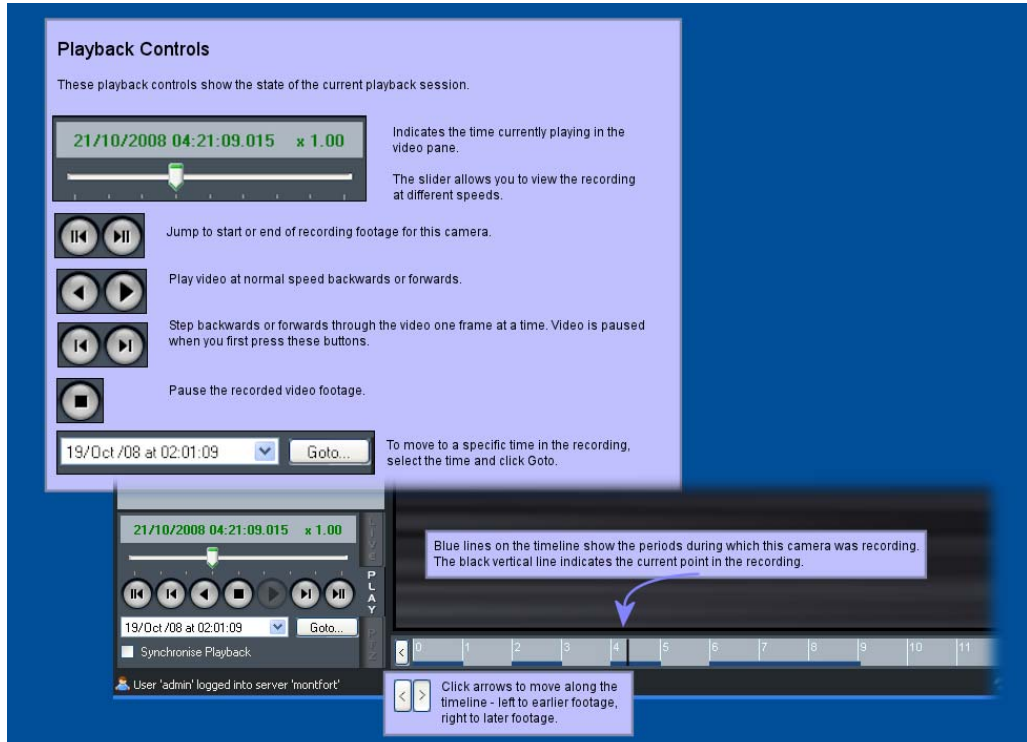
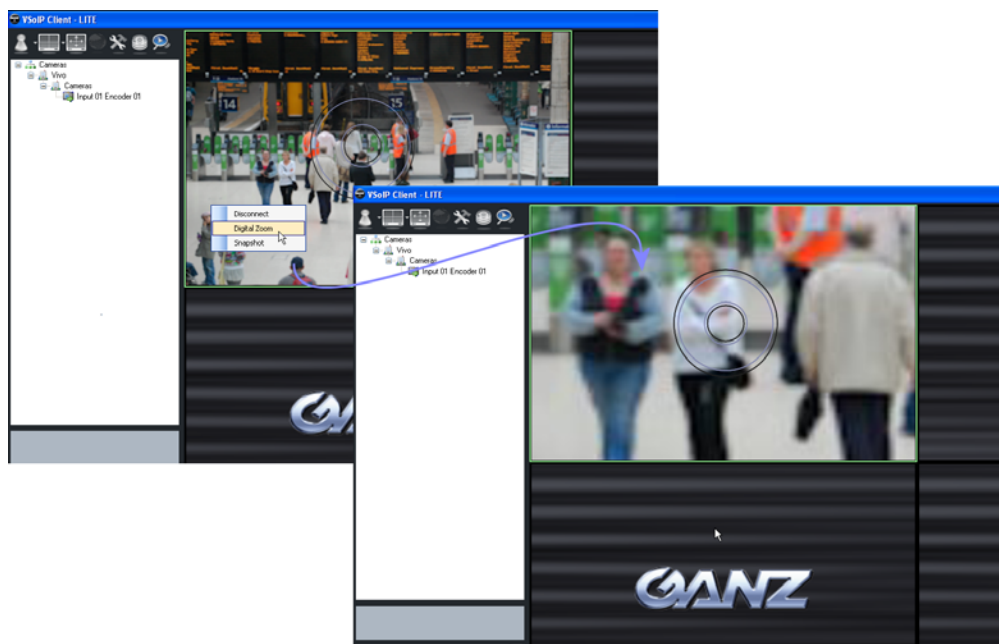


Figure 28 Controlling playback

## Using Digital Zoom

VSolP Lite allows you to zoom in on and move around recorded video footage.



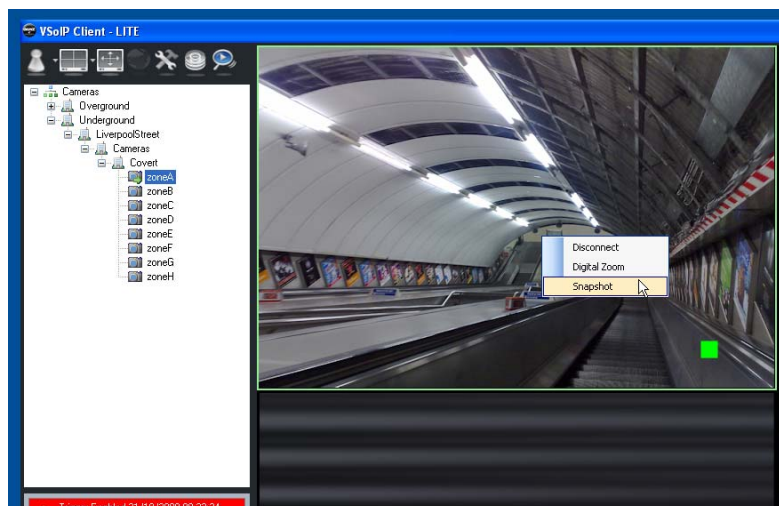
**Figure 29** Zooming into recorded video

Click the part of the video pane that you want to see in more detail, then use the mouse scroll button to zoom in and out as required.

## Taking a Snapshot of Recorded Video

VSolP Lite allows you to capture snapshots of recorded video playing in a video pane. By default, these are saved to \Desktop\VSolP Image Clips\FromRecordings, as .jpeg images. .

To take a snapshot, right-click in the pane displaying the video at the point you want to capture.



**Figure 30** Taking a snapshot of recorded video

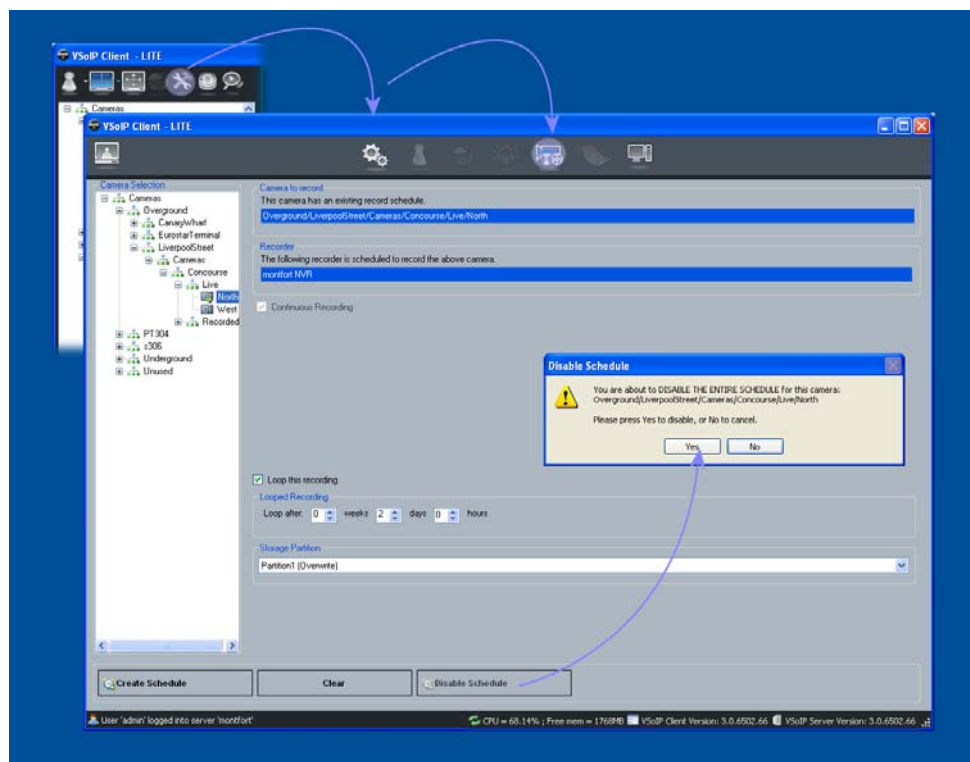
## Editing Recording Jobs

An existing recording job can be edited to use an alternative set of rules about when to record, e.g. switching on or switching off the looping functionality, or changing the loop duration. The partition on which the recording is being made can also be changed. If the recording job for that video source is no longer required then the recording job can be disabled.

**Note:** It is not possible to change the video source of a recording job.

## Deleting/Disabling Recordings

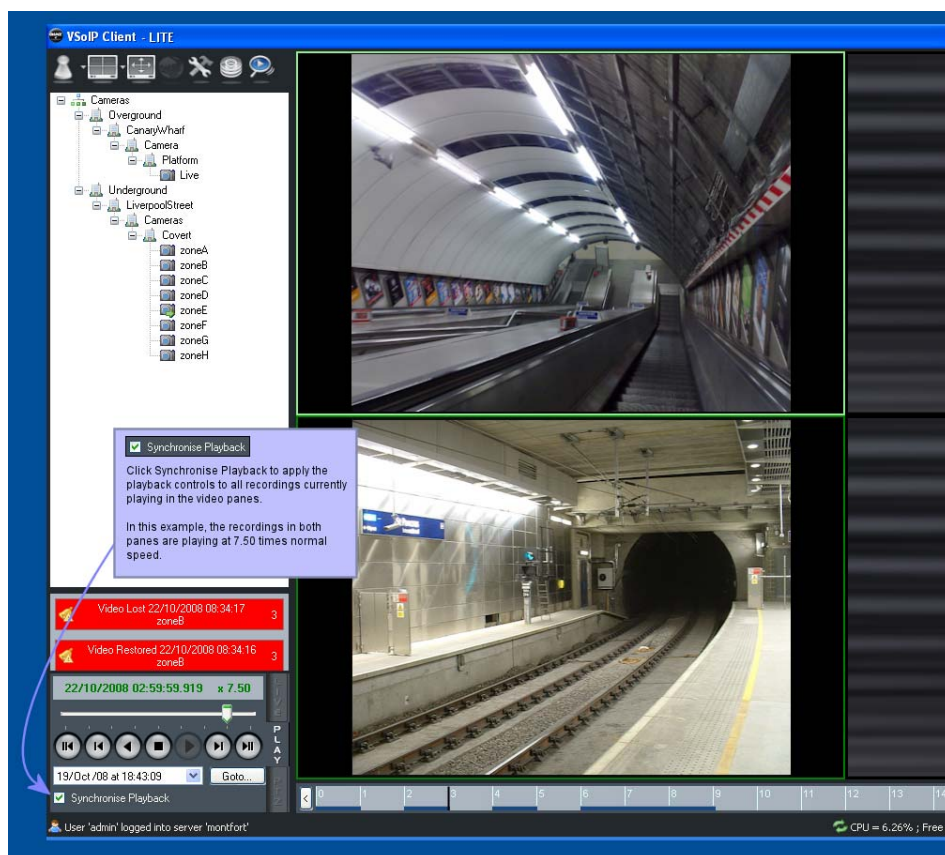
Due to the internal design of the VSoIP Lite NVR, “deleting” a job in the VSoIP Lite Client disables it on the NVR. Remember that you can edit a job to use a different recording criteria, for example, looping policy, and/or storage partition. If the recording job for a video source is no longer required then you should disable it, as shown in Figure 31.



**Figure 31** Disabling a recording job

## Synchronising Playback of Recorded Footage

To help operators review recorded footage from multiple cameras on multiple networked DVRs and/or NVRs simultaneously, it is possible to control playback using a master set of playback controls. This allows playback to be paused and wound forward or backwards at the same time saving time switching between playback sessions.



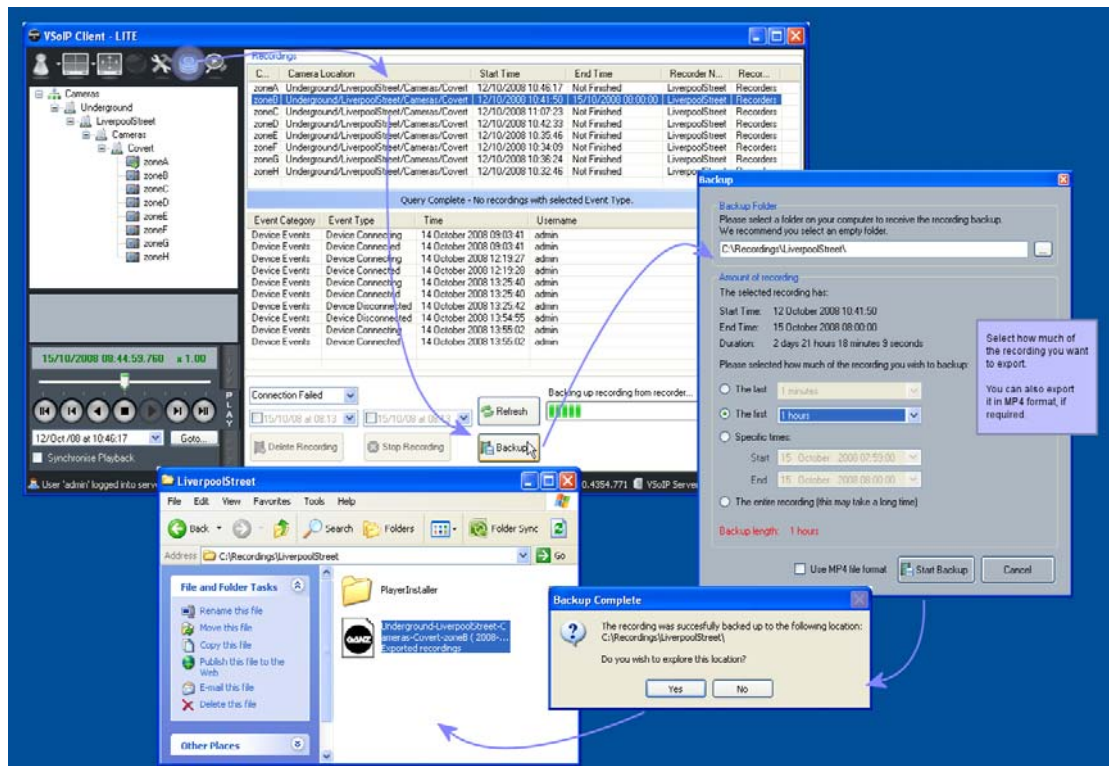
**Figure 32** Synchronised playback

**Note:** Networked DVRs can vary in their performance. Some Networked DVRs are limited to a certain number of concurrent playback sessions. The performance of the application during synchronised playback will reflect the responsiveness and performance of the poorest responding and performing element.

## Exporting Recorded Video

For evidential purposes, it is often necessary to extract a portion of recorded footage for playback in a player application. Locate your recording in the list of recordings of IP cameras and camera inputs on Networked DVRs.

Figure 33 shows the steps required to export recording footage.



**Figure 33** Exporting recording footage

## Exported Recordings Player

The Exported Recordings Player is designed to maintain the evidential integrity of the original recording by keeping the recording in its native format. Unlike other forms of export, e.g. MP4, native exporting means that the exported recording has not been transcoded or altered in any way.

When VSolP Lite is instructed to export recordings in native format, it copies the Exported Recordings Player Installer into the same folder as the exported recordings. The folder therefore contains one, or more, .REX files - one for each exported recording and the installation program for the player. The intent is to create an evidence “pack” for use by individuals without access to VSolP Lite.

**Note:** Although the computer running the Player can be considered to be a general purpose PC, it must support Microsoft Direct-X 3D rendering to a reasonable performance level.

## Prerequisites

### Hardware

- 32bit x86 architecture, single processor based personal computer.
- 1.5 GHz, or higher CPU speed.
- 0.5GB of fast memory.
- 5600 RPM hard disk drive speed.
- 50GB of hard drive space for operating system .Net Framework and Player software.
- Direct-X 3D rendering support in graphics sub-system.

### Operating System

- Windows XP Professional – service pack 2, or greater, is recommended.

### Additional mandatory software

- Microsoft .Net Framework 2.0 – automatically downloaded from Microsoft if not present at install time. Also available from Microsoft's website as a download.
- Microsoft Windows Installer 3.1.
- Microsoft Direct-X 9.0c (March 2009) redistributable.

**Note:** Microsoft frequently redesigns its websites therefore an Internet download link is not provided. Instead we recommend that you use Google or another search engine to find the download links for the mandatory software. On examining the search results, please ensure that the download source is Microsoft.

### Windows 3.1 Installer

The installation program for the .Net will automatically download Windows 3.1 Installer if required.

## Before Installing Player

### Activation and Licensing

The player does not require licensing or activation.

### Operating System Settings

Player installation, .Net installation and Direct-X components installation should be carried out as a user with local administrative rights.

### .Net Framework

The installation program for the Player automatically downloads the correct version of the .Net Framework for the Player over the Internet if there is a connection available. However if preferred, install the .Net Framework prior to installing the Player. No configuration of the .Net Framework is required.

### Windows 3.1 Installer

The installation program for the .Net will automatically download Windows 3.1 Installer if required.

## Installing the Player

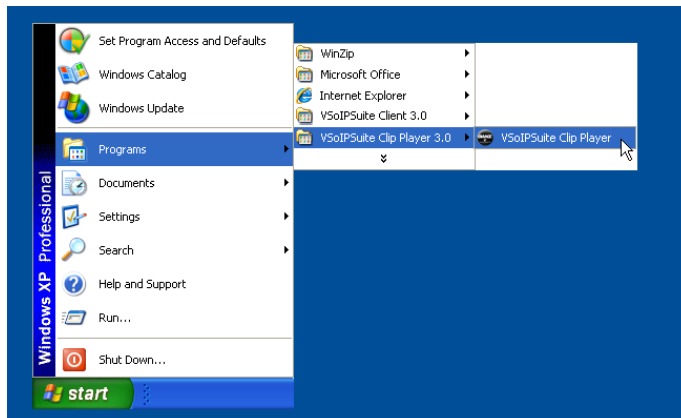
- 1 Log in to the computer with administrative level privileges — typically this is the administrator user name.
- 2 The Player installer program, setup.exe, automatically examines the local system for the .Net Framework. If this is not present, or it is an earlier version, the installer program automatically connects to Microsoft's servers over the Internet and downloads the correct version of the software,
- 3 Choose the Player's installation folder, or use the default folder suggested.
- 4 Click Next, then Next again.

## Using the Player

### Starting the Player

Open Windows Start menu and choose the Player shortcut to start the Player.

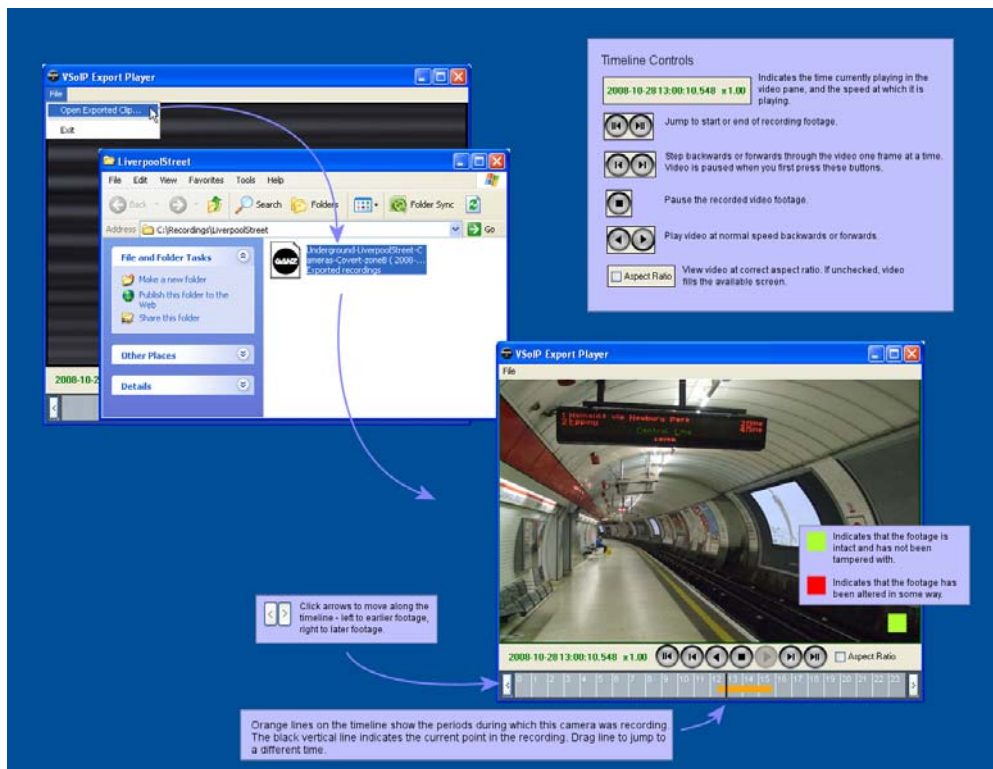




**Figure 34** Starting the Player from the Windows Start menu

Alternatively, since the installer program sets up an association between files with .REX file extension and the Exported Recordings Player, you can also start the Player automatically by opening a .REX file in Windows Explorer either by double clicking the left mouse button on a .REX file, or opening the context menu on a .REX file and choosing the Open menu option.

## Typical Operation



**Figure 35** Playback components

# Appendix A — Maintenance Information

The follow entries provide useful information regarding the general use and setup of the surveillance system.

## Opening a command prompt in Microsoft Windows

The command prompt allows certain tools that do not have a graphical user interface to execute. Often such commands require extra parts called arguments that detail what options need to be configured.

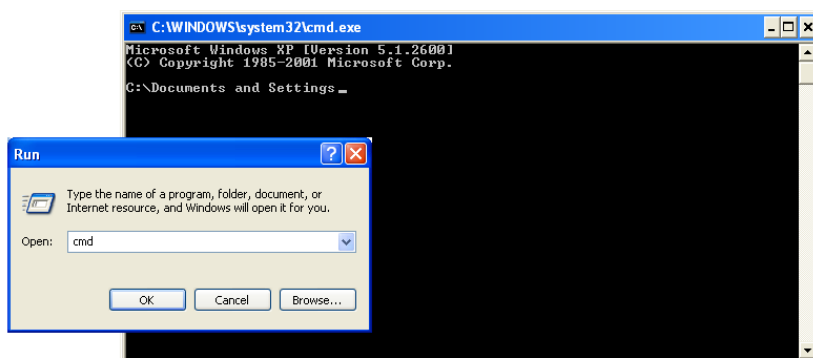
For instance, the networking command **ping** allows the network connections to another networked device to be tested. The main argument required is the IP address of the device, e.g. ping 10.11.12.13

**Note:** Often the commands run at the command prompt require certain privileges therefore it is important to use the command prompt as an administrator level user.

### Windows XP

The command prompt can be started from the Start menu, Start>All Programs>Accessories>Command Prompt. It is also often started from the Run dialog, by typing CMD and clicking OK.

In the command prompt window at the prompt after the > character enter the required command. After typing the command press the Enter (also called Return) key to perform the command.



**Figure 36** Opening a Windows command prompt

## Opening the Run dialog

The run dialog can be shown using the Windows Start menu, Start>Run or by holding the Windows key and pressing the “R” key.

**Note:** If the Start menu item Start>Run is missing you can enable it by right-clicking the Start menu button. Choose Properties, select the Start Menu tab, click Customize then select the Advanced tab. In the Start menu items list-box, locate the Run command entry and check the box against it. Click OK twice to apply the change.

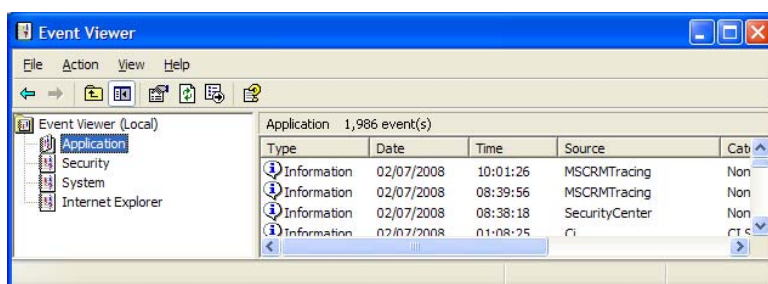
## Finding out the IP Address of your computer

There are a number of methods for doing this. One approach that can be relied on irrespective of the Windows version being used is the command IPCONFIG.

To use IPCONFIG, open a command-prompt. Enter the command **ipconfig**. On entering the command, the operating system will respond with a series of addresses, note the one labelled IP Address.



## Windows Events – using the Event Viewer



**Figure 37** Windows Event Viewer

Some services and applications running on a computer need to communicate with the user but do not have a graphical interface to do so. For these services and applications the operating system provides methods of recording the occurrence of an event. All the events in the system are logged into various event logs. The event viewer is a convenient method of examining all the events that have recently occurred, as such issues concerning the proper functioning of the system are recorded and allow problems to be solved during commissioning and maintenance cycles.

### Viewing

The Windows Event Viewer allows a user to view various different Windows logs. The log of interest to the Surveillance System is the Application Log. The application log holds a historical list of information, warning and error messages related to applications running on the local computer.

From the Start menu open the Control Panel and choose the Administrative Tools. If the control panel is in category view, choose the Performance and Maintenance category, then Administrative Tools. Open the Event Viewer. Double-click the Application log.

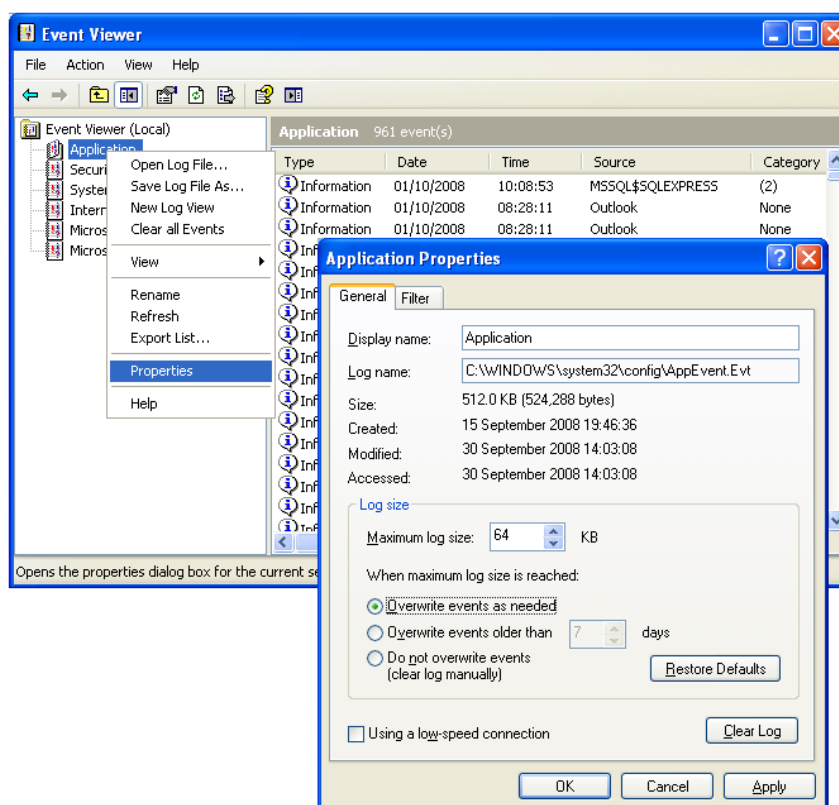
When examining the log, note the Source column. This lists the name of the application that generated the log entry. Entries can be:

- Informational, shown with an i icon.
- Warnings, shown with an exclamation mark icon.
- Severe error, shown with a stop-sign icon.

Surveillance suite software components that have warning or error log entries should be read to determine the source of the error. The system log can be useful for finding out about computer issues that might affect the surveillance suite applications indirectly, for example low disk space.

**Note:** If the control panel entry is missing you can enable by right-clicking the Start menu button. Choose Properties, select the Start Menu tab, click Customize then select the Advanced tab. In the Start menu items list-box locate the Control Panel entry and choose either Display as a link or Display as a menu. Click OK twice to apply the change.

## Configuring Application Log to Overwrite Oldest Entries



**Figure 38** Changing Windows logging behaviour

The event log can become full and prevent proper execution of the tasks running on the computer. To prevent this, change the properties of the application event log to overwrite earliest events when there is insufficient space available.

To do this, open the event viewer application as described in the section “Windows Events – using the Event Viewer”. Right-click the Application entry in the left-hand window and choose Properties. In the Application Properties choose the General tab and in the Log size group click Overwrite events as needed, and click OK.

## Viewing Windows Services List

Some parts of the surveillance system run as background tasks and do not require a user to be logged in for tasks to be run. These background tasks are known as services.

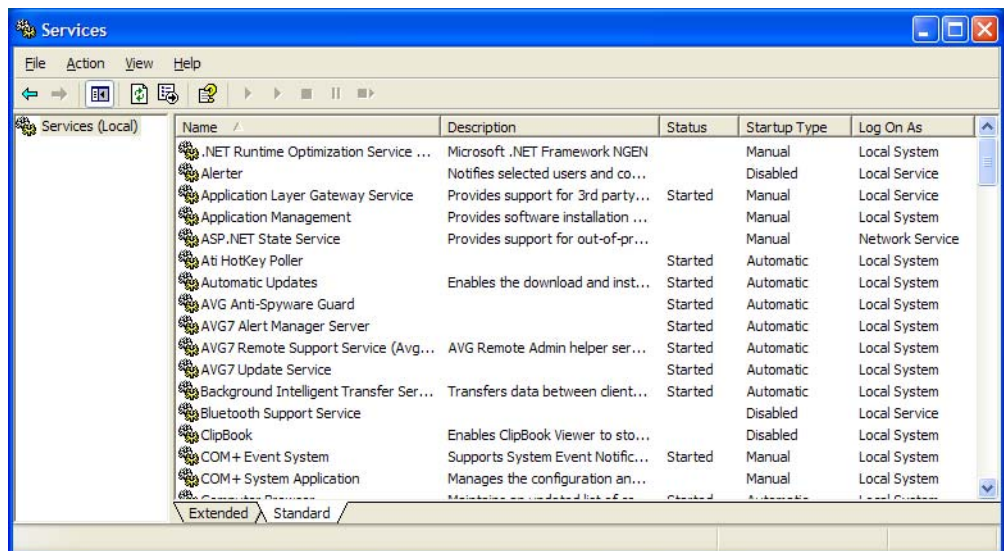
Although services run in the background, do not interact with users graphically, and do not require a user to be logged in, they are initiated and run and thus owned by a user account on the computer. Typically this account is one of the built-in accounts, usually a user called LocalService or sometimes as a user called NetworkService.

Services can be started or stopped by the operating system when it starts or shuts down - automatic. Alternatively services can be started or stopped by a logged in user with sufficient privileges to do so - manual.

When service based surveillance suite components are installed they are installed in a state that requires a logged in user with appropriate privileges to start the service.

The windows services list permits a logged in user with sufficient privileges to switch a manual service to start automatically, to switch an automatically starting service to manual or completely disable the service preventing it from being started.

To open the services list, from the Start menu open the Control Panel and choose the Administrative Tools option. If the control panel is in category view, choose the Performance and Maintenance category, then Administrative Tools. Open the Services application.



**Figure 39** Windows services application

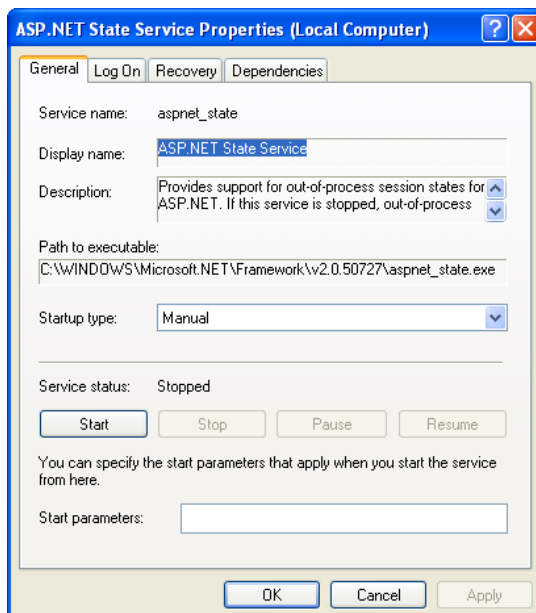
Right-click and choose Properties to display the Properties dialog for the service.

To request that Windows start a service when the operating system starts, change the Start-up type to Automatic. Note, the service will not actually start until Windows is re-started. It is possible to start the service from this dialog by using the Start button.

To change an automatic service back to one that requires a logged in user to start and stop the service, change the Start-up type to manual. Note, a started service will not stop until Windows is shut down. To stop the service before then, you can use the Stop button.

Click OK and close the Services application.

**Note:** Remember, informational messages, warnings and error events logged by services can be viewed through the Windows Event Viewer.



**Figure 40** Configuring start-up action for selected service

## Checking connectivity of a networked device or computer

During installation, commissioning and when troubleshooting an installed system, it might be necessary to confirm that a particular network device is reachable. One technique is to use a network Ping. The network ping sends a special data packet over the network that on receipt by the end party is replied to. Most networked devices, IP cameras, Networked DVRs, computers running a Server component, computers running a NVR component or computers running a Video-wall component unless configured not to will reply to incoming Ping requests.

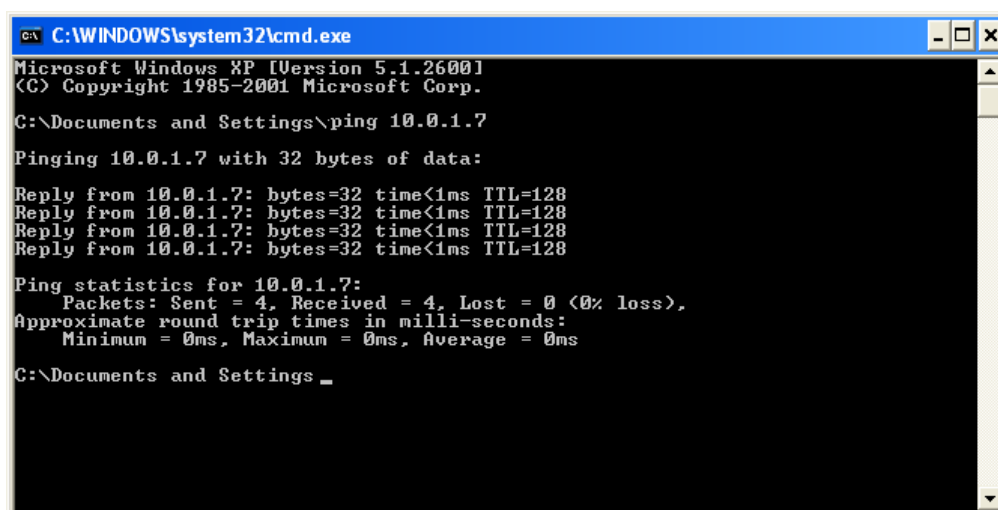
To use a ping you need to know the IP address of the network device you wish to find.

**Note:** If no response is gained from a pinged network device then first ensure you have the correct IP address for the device, if correct then confirm that you have connectivity with other network devices before assuming that the device is not reachable – it might be that the computer from which you are Pinging is not able to reach a number or all networked devices due to a configuration issue with the computer you are using, a coincidental localised or wider network-connectivity issue, or the presence of a software firewall preventing ping requests being sent or received.

### Steps

The following steps show how to determine whether a certain device with IP address 10.0.0.1 is available on the network. It also assumes that some checks have been made to ensure that the computer being used in the test is connected to the same network as the device and that other devices known to exist and connected to the network have responded.

- Open a Command prompt.
- Type at the command prompt: ping 10.0.0.1 and press the Enter (or return) key.
- If the network device (or computer running a surveillance software component) cannot be reached then the response will be at least 4 lines indicating “Request timed out”.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\ping 10.0.1.7

Pinging 10.0.1.7 with 32 bytes of data:

Reply from 10.0.1.7: bytes=32 time<1ms TTL=128
Reply from 10.0.1.7: bytes=32 time<1ms TTL=128
Reply from 10.0.1.7: bytes=32 time<1ms TTL=128
Reply from 10.0.1.7: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.1.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings _
```

**Figure 41** Successful ping reply

- If the network device was reachable then the response will contain several replies.
- If there is a mix of replies and timed out messages, this suggests that a network connection fault exists, that the network is highly congested, that the target device is too busy due to heavy workload to reply, or a mixture of all of these. In this case, this indicates that there is a system issue which could adversely affect the system's overall performance and could result in failed recordings, live or playback requests, and a general lack of system responsiveness.

The ping command is a useful troubleshooting tool that can highlight issues affecting the overall system and is one method that might indicate that the overall system is currently overdriven and is not operating as designed.

## Troubleshooting

Troubleshooting is a complex area when the components of the Surveillance Suite software, the underlying operating systems, database managers, rendering engines, the different types of hardware involved and the various issues related to networking are all taken into consideration.

This section covers some typical issues that occur when installing, running and maintaining the surveillance system. It also describes how to assist a technical support representative by providing them with useful information and run-time log files to help them determine the root of a problem. It is worth noting that by examining the information provided there will be cases where the solution might be obvious and you can implement a solution without having to contact the software vendor or other support provider.

It is important to note that a high level of technical competency is required in order to perform troubleshooting. There are a number of skills required to identify the likely cause of the issues being experienced and several attempts might be required to solve problems.

It is very important to design a system from the outset rather than to make an arbitrary system using various hardware elements and using networking infrastructure that has not been optimised for surveillance use, i.e. not high bandwidth optimised. There are discussions elsewhere about the importance of design in constructing the surveillance system.

**Note:** It is assumed that the overall system (software, hardware and networking infrastructure) is fit for purpose and has performance safety margins that allow peaks of demand to be accommodated. It is also assumed that high performance computer hardware is used: server grade for Server and Networked Video Recorder components and that all computer hardware matches or, preferably, exceeds the minimum specifications.

---

**Caution:** It is highly recommended that computer hardware is NOT used to perform non-surveillance system tasks unless the interaction between the CCTV and non-CCTV aspects of the installation can be safely accommodated within the specification of the computer and there is no shared dependency, e.g. shared database manager usage, that compromises the system.

---

## Providing technical support information

All software components have a built-in automatic log file generator. The generator is enabled whenever a special file called logging.config is detected.

### Enabling Logging

All software components have a built-in automatic log file generator. The generator is enabled whenever a special file called logging.config is detected.

- 1 Locate a suitable logging.config file and copy it into the clipboard. This will be:
  - In the installation folder of the software component and called logging.config.disabled (or some other name that distinguishes it from logging.config).
  - Or in a sub-folder of the installation folder.
  - Alternatively, you might be sent the file by a technical support representative.
- 2 Close the application you want to log
  - For clients, exit the application.
  - For servers or NVR components, stop the service controlling the application.
- 3 Paste the logging.config file into the installation folder. (If necessary, rename it so that it is called logging.config.)
- 4 Start the application to be logged.
- 5 Note that a log-roll.txt file will appear in the application's installation folder.

### Disabling Logging

- 1 Close the application currently being logged.
  - For clients, exit the application.

- For servers or NVR components, stop the service controlling the application.

**Note:** Currently the application being logged will occasionally write to the log-roll.txt file. You will not be able to delete the log-roll file(s) or the logging.config file until the application being logged is stopped.

- 2 Remove the logging.config file from the installation folder by moving to a sub-folder, to another safe location, deleting it (if you have kept a copy) or renaming it to (for example) logging.config.disabled.
- 3 Start the application.
- 4 Note that after removing any log files in the application's installation folder, no more log files are added to the folder.

## How Logging Works

---

**Caution:** The logging.config file contains the operating parameters for the generator and should not be modified unless you have been instructed to do so.

---

The log file generator automatically "rolls" the log file every hour. This means that the log-roll.txt file is renamed to a name starting with log-roll but also appends the date and hour of the day that the log started on, and a new log-roll.txt file is created containing the next hour's logging information.

This rolling behaviour has two undesirable side-effects:

- Whenever the application being logged is restarted, the log-roll.txt is deleted and a new one created. This may mean that vital error information gathered prior to the failure of the application is lost.

To overcome this and capture the last moments of an application's behaviour in the log file, locate the log-roll.txt and rename it to, for example, log-roll-showing-UAE.txt. This means when the application being logged is restarted, the log-roll.txt will not be present to be overwritten.

**Note:** If the application is still executing and you wish to capture the moment where something is happening, then wait until the required moment has passed, then stop the application. Once stopped rename the log-roll.txt file as described, and restart the application.

- If logging is enabled and the system unmaintained for an extended period, the log files may eventually consume large quantities of storage on the drive where the application is installed. This could compromise the overall performance of the computer running the application being logged.

To overcome this, you can safely move or delete log-roll files with dates and times appended to the file's name, since these are not actively being written to by the generator. Alternatively, be sure to disable logging once your logging requirements have been met.

---

**Caution:** Logging puts extra demand on any system due to the CPU load of executing surveillance software components and log generator. This could cause system overload and result in misleading log content.

---

In some cases where overall system power is limited, enabling logging can put a serious load on the system, perhaps causing the system to become overdriven. Always ensure that the computer is able to accommodate the logging overhead on top of normal system operation. If this is not done, the content of the logs may be misleading since they will reveal an overdriven system rather than the fault trying to be captured. In such situations alternative approaches to troubleshooting are required.

# Index

---

## A

acknowledging alarms 28  
adding devices 15  
alarms  
    acknowledging 28  
    closing 29  
    viewing properties 27

---

## C

camera compatibility 4  
checking connectivity 44  
closing alarms 29  
command prompt, opening 40  
compatibility  
    cameras 4  
    DVR 4  
computer's IP address, determining 40  
configuring  
    devices 15  
    PTZ 20  
    triggers 19  
    video sources 18  
controlling PTZ 25  
controls, live view 21  
creating recordings 30

---

## D

deleting  
    devices 17  
    recordings 35  
devices  
    adding 15  
    configuration 15  
    deleting 17  
disabling logging 45  
displaying  
    recording footage 31  
DVR compatibility 4

---

## E

enabling logging 45  
exported recordings player 37  
    installing 38  
    pre-installation 38  
    prerequisites 37  
extra PTZ features 26

---

## F

firewalls 10

---

## I

installation procedure 11  
installing  
    exported recordings player 38  
IP address, determining 40

---

## L

live video  
    controls 21  
    starting 23  
    stopping 23  
logging  
    disabling 45  
    enabling 45

---

## M

moving PTZ 25

---

## O

opening  
    command prompt 40  
    run dialog 40  
overview of system 4

---

## P

ping command, using 44  
player, exported recordings 37  
port numbers, specifying 15  
pre-installation  
    exported recordings player 38  
    VSoIP Lite 9  
prerequisites  
    exported recordings player 37  
    VSoIP Lite 8  
PTZ  
    configuration 20  
    control 25  
    extra features 26  
    moving and zooming 25

---

## R

recording footage  
    displaying 31  
    synchronising 36  
recordings  
    creating 30  
    deleting 35  
run dialog, opening 40

---

## S

specifying port numbers 15  
starting up live video 23  
stopping  
    live video 23  
synchronising recording footage 36  
system  
    components 4  
    overview 4

---

## T

triggers, configuring 19

---

## U

user overview 14

---

## V

video sources, configuring 18  
viewing  
    alarm properties 27

---

## W

Windows Events Viewer 41  
Windows Services 42

---

## Z

zooming PTZ 25



