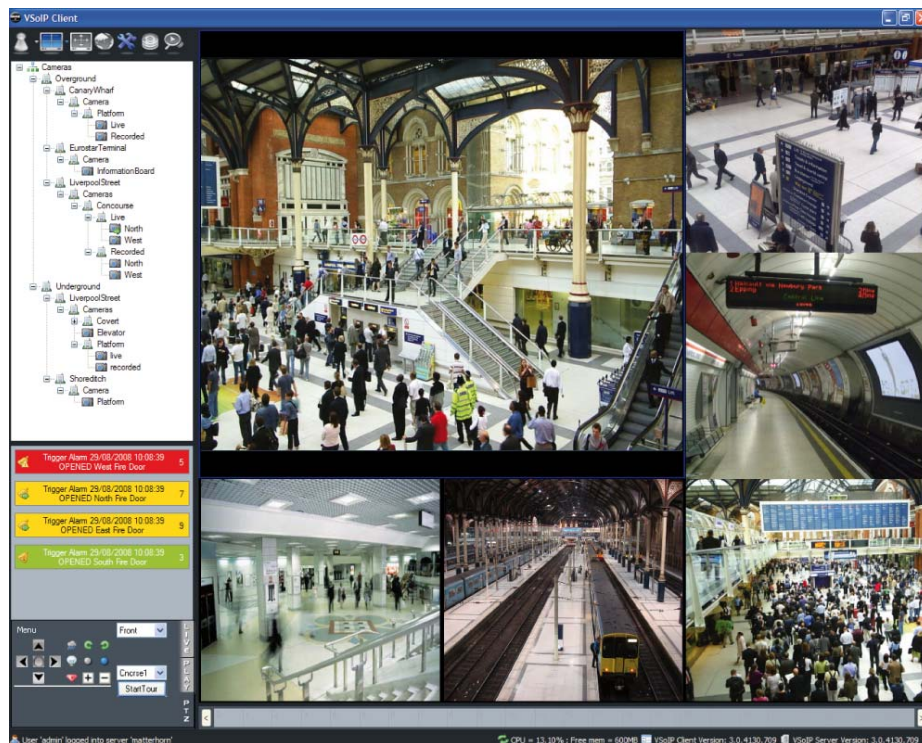


# MANAGEMENT SOFTWARE

# **VSOIP 3.0 SUITE**

## USER MANUAL



**QAWZ®**



# Table of Contents

<b>1 System Overview .....</b>	<b>6</b>
System Components.....	6
Surveillance Suite Architecture.....	7
IP Camera and DVR Compatibility .....	7
System Environment.....	7
Network traffic.....	7
Infrastructure.....	7
Configuring Stream Settings.....	8
System Hardware Considerations .....	9
System Software.....	9
System Licensing.....	10
 <b>2 The Server Component .....</b>	 <b>12</b>
VSoIP Pro Server Overview.....	12
Server Prerequisites .....	13
Additional mandatory software .....	13
Optional, useful software .....	13
Before Installing the VSoIP Pro Server.....	13
Installing the VSoIP Pro Server.....	15
Customising the Database .....	16
Using the VSoIP Pro Server .....	16
Starting the Server Manually.....	16
Starting the Server Automatically.....	16
Stopping the Server .....	17
Troubleshooting .....	17
How can I be sure the Server is running?.....	17
Network Time Server .....	17
 <b>3 The Client Component.....</b>	 <b>18</b>
VSoIP Pro Client Overview .....	18
Prerequisites .....	19
Before Installing the VSoIP Pro Client .....	20
Installing the VSoIP Pro Client.....	22
Post-installation checklist.....	22
Network Time Server .....	22
 <b>4 Client Activation and Licensing .....</b>	 <b>23</b>
Activating the VSoIP Pro Client .....	23
Client Licensing – Evaluation mode.....	24
Logging in to the VSoIP Pro Client .....	25
Starting the Client .....	25
Default Administrative User .....	25
Logging in .....	26
Logging out.....	26

<b>5 Client Configuration .....</b>	<b>27</b>
System Overview .....	27
Getting Started .....	27
User Configuration .....	28
Adding a new user .....	28
Changing user passwords .....	29
Temporarily preventing a user from logging in.....	30
Deleting an existing user .....	31
User Group Configuration .....	32
Creating a User Group.....	32
Deleting a User Group .....	33
Device Configuration.....	34
Adding Devices .....	35
Deleting Devices.....	37
Configuring Video Sources .....	38
Configuring Triggers .....	38
Configuring Pan-Tilt-Zoom Capabilities .....	39
Mapset Configuration .....	40
Adding Mapsets .....	40
Associating Map-links with Devices .....	40
Deleting Mapsets .....	41
Working with Live Video and PTZ .....	42
Specifying Video Pane Layout .....	43
Starting and Stopping Live Video.....	44
Using Digital Zoom .....	45
Taking a Snapshot of Live Video .....	45
Control of Pan-Tilt-Zoom .....	46
Working with Alarms .....	48
Overview of Alarm Display.....	48
Viewing Properties of an Alarm .....	49
Acknowledging an Alarm .....	49
Closing an Alarm .....	50
Playing Back Recorded Video.....	51
Discovering Recorded Footage .....	51
Playing Back Recorded Footage .....	51
Using Digital Zoom .....	54
Taking a Snapshot of Recorded Video .....	54
Synchronising Playback of Recorded Footage .....	55
Exporting Recorded Video .....	55
Exported Recordings Player .....	56
Prerequisites.....	56
Before Installing Player .....	57
Installing the Player .....	57
Using the Player .....	57
Audit Trail Configuration.....	59
Audit Trail Profiles.....	60
 <b>6 Mapsets.....</b>	 <b>61</b>
Mapset Overview .....	61
Designing Mapsets.....	62
Creating a Mapset without a Map Design Tool.....	62
Typical Workflow .....	63
Placeholder Map Page .....	64

Page Links - Textual .....	64
Camera Links - Graphical .....	65
Alarm Links .....	67
<b>7 NVR Component .....</b>	<b>70</b>
NVR Overview .....	70
Prerequisites .....	70
Before Installing NVR .....	71
Installing the NVR .....	73
Customising the Database .....	74
Using the NVR .....	74
Starting the NVR Manually .....	74
Starting the NVR Automatically .....	75
Stopping the NVR .....	75
Troubleshooting .....	76
Expected Performance .....	77
Network Time Server .....	77
<b>8 NVR Activation and Licensing .....</b>	<b>78</b>
Activating the NVR .....	78
<b>9 NVR Configuration .....</b>	<b>79</b>
NVR Recording Schedules .....	79
Recording Schedules .....	79
Creating a Recording Schedule .....	79
Editing Recording Schedules .....	80
Disabling/Deleting Recording Schedules .....	81
NVR Alarm-Triggered Recording .....	81
How does alarm-based recording work? .....	81
<b>10 System Administration .....</b>	<b>82</b>
Restoring Factory Defaults .....	82
Reusing Devices, Users and Groups .....	83
Exporting Devices, Users and Groups .....	83
Importing Devices, Users and User Groups .....	84
Viewing System Information .....	84
Default Settings .....	85
Changing Client Settings .....	85
Available Client Settings .....	87
<b>Appendix A — Maintenance Information .....</b>	<b>88</b>
Opening a command prompt in Microsoft Windows .....	88
Opening the Run dialog .....	88
Finding out the IP Address of your computer .....	88
Windows Events – using the Event Viewer .....	89
Configuring Application Log to Overwrite Oldest Entries .....	90
Viewing Windows Services List .....	90
Checking connectivity of a networked device or computer .....	92
Troubleshooting .....	93
Providing technical support information .....	93
<b>Appendix B — Supported Devices .....</b>	<b>95</b>

**Appendix C — NVR Partitions and Partition Groups ..... 96**  
    Default partition.....96  
    Partition Modes.....96  
    Partition Groups.....96  
    Choosing an NVR Recording Partition.....97

**Appendix D — Complex Alarm Configuration ..... 99**  
    Simple Alarms and Scheduled Alarms.....99  
        Simple Alarms.....99  
        Scheduled Alarms.....99  
    Understanding Alarm Processing.....99  
    Creating Complex Alarms .....100  
    Using the NOT Boolean Operator .....103  
    How Complex Alarms Work .....104  
    Example of Complex Alarm Processing.....105

**Index..... 107**

# Chapter 1 – System Overview

This chapter contains information on the following:

- System Components
- System Environment
- System Licensing

VSolP Pro is an entry-level surveillance suite which provides a mechanism primarily for viewing, recording and reviewing video via computer network hardware, networked cameras, networked digital video recorders (DVR), networked computers, systems software and bespoke software.

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

**Table 1** System Components

Client	A client is a software entity that presents a view of the current state of the surveillance suite. It makes requests to a server which permits certain actions to be carried out by the client. The client can also act in an administrative capacity allowing the configuration and maintenance of the whole system.
Server	The server is a software entity that acts as a central decision and control centre for the whole system. It provides a series of services to clients. It ensures that actions made by the clients, if appropriate, update the surveillance system.
Networked Video Recorder	The NVR is a software entity that stores network streams originating from IP cameras and networked digital video recorders onto a storage device and retrieves these at a later time. The “recorded” stream is not tampered with in any manner so the evidential integrity of recorded video is maintained.
Video-wall	The Video-wall is a software entity that displays video originating from IP cameras and networked digital video recorders in a matrix style layout.
Transcoder/broadcaster	A combined transcoder/broadcaster software entity converts media streams originating from network streams from IP cameras and networked digital video recorders, from folders of image files and from video files and broadcasts media streams transcoded to alternative encoding, framerate, resolution and bit-rates. These transcoded and broadcasted streams are later consumed by Clients, Video-walls or Networked Video Recorders.
Media analytics processor	A media analytics processor is a software entity that carries out stream analytics tasks using various algorithms and provide a series of alarms to subscribed Server and Networked Video Recorder entities.

**Caution:** The incorrect shutdown of the recorder could risk loss of previously recorded footage, or recorder system failure. See “Stopping the NVR” on page 75 for more information.

## Surveillance Suite Architecture

When the system components — client, server, recorder and Video-wall — 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.

Typically the surveillance system will consist of:

- At least one networked video source, either camera or recorder (but ordinarily many more).
- A single server.
- At least one client (but ordinarily several).
- A Video-wall, NVR, analytics and transcoder/broadcaster components are optional. There can be several NVR and Video-wall components within the system.

**Note:** There is only one server component within the surveillance system. There can be several surveillance systems on the same network but note that each system has a single server component at its core.

## IP Camera and DVR Compatibility

A list of compatible devices is supplied separately in the appendices. 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 clients, Video-walls and NVRs.

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.

### 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 (in the case of Video-walls).
  - 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 sever. 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.
- Storage systems for recordings should be very high speed, large capacity integrated or external Direct Attached Storage (DAS) or Storage Area Networks (SAN). On no account should Network Attached Storage (NAS) be used. Also, when configuring external DAS or SAN systems, the network delivering the video streams from the CCTV network should not be the same network used to attach the storage.

## 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 or H.264 streams of the same resolution.
  - More traffic is generated by MJPEG by high frame quality / low compression factor.
  - More traffic is generated by MPEG4 or H.264 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.
- Note:** H.264 can require more CPU power to decode than the equivalent stream encoded in MPEG4. Please consider this when interpreting PC specification requirements.
- 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 — typically these will be links to NVRs and Video-walls.



- 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. The client software component will consume more PC resources than with a CIF/SIF resolution stream and thus either the specification of the PC should be revised in light of the higher decode and rendering requirements, or the number of concurrently displayed streams should be reduced, or both. If NVRs are used to record high-definition, mega-pixel network streams, these put 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.
- The network's ability to support multicast is important – the discovery system used in the surveillance suite is based on multicast and broadcasting. If multicast support is impossible, computers running the client software component can still locate the server component if the server's IP address is known.

## System Hardware Considerations

When considering optimal hardware for the surveillance system, consider the following:

- The server and NVR software components have a serving behaviour and as such will benefit from computer hardware optimised for the role of serving.
- The client and Video-wall components have graphical display behaviour, and so benefit from computer hardware optimised for multi-media graphical display. It may be useful to add specialist display adapters that provide dual- or quad-head capability. Such display adapters must have the functional ability to perform Direct-3D rendering in hardware, i.e. not offload this work to the computer system's host processor.

## System Software

The surveillance suite components are designed to run under the Microsoft Windows XP Professional SP3 and 2003 R2 Standard Edition 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 such as locking down certain features or applying various operating system group 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 and Video-wall components), 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 the client software, 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 the server and NVR surveillance software components 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.

---

The Video-wall software component uses Microsoft's Internet Information Services. This is provided with Microsoft Windows and is an extra component that must be installed from the Windows installation media.

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

## System Licensing

Some surveillance system software components must be licensed. The process of licensing a software component is known as activation. In order to activate a software component you must have an activation ID.

Example of an activation ID: aa936b02-3615-49cf-986b-0f38df9c32ea.

An activation ID is supplied for each software component purchased that requires one. To activate a component the activation ID must be entered when requested or the appropriate licensing application for the software component must be executed.

On entering the activation ID, the software component must contact a licensing server over the Internet. The software component will collect identifying features of the computer executing the component, encrypt this information along with the activation ID and sends this to the licensing server. The licensing server decrypts this information and if the activation ID is unused, it associates the identity with the activation ID and sends an encrypted license to the computer licensing the software component.

The identifying features of the computer used include:

- The IDs of the processor(s).
- The serial number of the hard drive(s).
- The machine (MAC) address(es) of the network card(s).

There is a level of tolerance in the licensing system which allows some of the identifying features of the hardware to be changed, e.g. the hard-drive, network card could be changed without causing a license validation failure. However if too many distinguishing elements have changed then the validation of the license will fail. It will then be necessary to obtain a new activation ID from your software vendor. Your software vendor may charge you a fee to obtain a replacement activation ID, or you may have to purchase a new activation ID.

**Note:** Some computers do not have sufficient devices to accommodate a tolerance. In such cases, changing a component within the computer will require a new activation ID to be obtained.

If the license file for a software component is deleted from the computer then the original activation ID for the software component can be used to reactivate the software component. The original license file will be recreated.

---

**Caution:** A licensed software component does not need access to the Internet. It is only during activation and license file generation that an internet connection is required. Normal day-to-day running of a licensed software component does not require access to the Internet.

---

# Chapter 2 – The Server Component

This chapter contains information on the following:

- Server Prerequisites
- Before Installing the VSolP Pro Server
- Installing the VSolP Pro Server
- Customising the Database
- Using the VSolP Pro Server
- Troubleshooting
- Network Time Server

## VSolP Pro Server Overview

The VSolP Pro server software component (the “Server”) is a Microsoft .Net framework based service for Microsoft Windows operating systems. It is designed to control access by computers executing the client software component (the “Client”) to surveillance resources such as IP cameras, networked digital video recorders (DVR), computers executing the NVR software component (the “NVR”) and computers executing the Video-wall software component (the “Video-wall”).

- The Server monitors for events on various IP cameras, DVRs and NVRs, raising alarms on those Clients permitted to receive events.
- The Server is responsible for maintaining an audit trail. The audit trail is stored in a Microsoft SQL Express 2005 database either on the same computer as the Server or on another networked computer.
- The Server also coordinates access to the NVRs within the system.

Initial configuration and day-to-day operational control of the surveillance system is via Clients connected to the Server. Clients discover Servers on the network using a multicast based discovery broadcast. Clients on networks that do not have broadcasting ability must use the IP address of the computer on which the Server is executing. Communication between Clients, Servers and NVRs is via .Net remoting. Communication between Clients and Video-walls is via HTTP.

The Server runs using a local system account, either LocalService or NetworkService. These accounts are built-in accounts in Microsoft Windows and do not need to be created.

The computer used to run the Server should not be considered to be a general purpose PC and should not be used for other tasks that might starve the Server of system resources. It is possible to run a Client and/or a NVR on the same computer as the Server but this can lead to a conflict of resources and as such is discouraged in all but the smallest of systems.

# Server Prerequisites

## Hardware

- Processor: 32 bit architecture CPU (e.g Intel Quad Core Processor (or better)) 2.4Ghz.
- Memory: 4096MB.
- Hard Drive/Storage - 500GB SATA Hard Drive (or other very high performance drive).
- Optical Drive — DVDROM (for installation).
- 100 Base-T network card configured for full duplex
- 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  
-or-  
Windows Server 2003 Standard Edition – service pack 2, or greater, is recommended.

---

**Caution:** In geographical regions where different 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.
- Microsoft SQL Server 2005 Express Edition – service pack 2, or greater, automatically downloaded from Microsoft if not present at install time. Also available as a download from Microsoft's web-site.
- Windows Installer 3.1.

**Note:** Microsoft frequently re-designs its web-sites 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.

## Optional, useful software

- Microsoft SQL Server Management Studio Express – useful for changing various database settings.

## Before Installing the VSolP Pro Server

### Operating System Settings

The PC should have the operating system installed either by the computer manufacturer or from the operating system installation media. It is assumed that the computer does not belong to any Windows network domain.

**Note:** Changes to the operating system settings, such as the 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 single local user should be added. This should be a member of the local administrator group. Server installation, .Net installation and SQL installation, and all maintenance should be done as this local user with local administrative rights.

**Note:** The Server and SQL database engine run as Windows services and as such will execute irrespective of what user, if any, are logged in to the PC.

To prevent unscheduled system restarts, switch off the automatic Windows update feature. Updates of the Windows operating system should be carried out as a 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. Check this by opening a command prompt and running the IPCONFIG Windows command-line utility, see appendices.

It is worth noting the IP address of the Server – this address could be useful for Clients that cannot discover the Server using the multicast discovery system built into the software system because the network does not support multicast.

The PC must be set up so that it can browse the Internet. Following installation, the Server will need to contact a licensing server located on the Internet in order to complete the installation and activate.

## Firewall Information

For best performance, simplicity of setup and easy maintenance, it is recommended that a dedicated firewall protects the entire network rather than firewall software running on the server PC.

Any local software firewall should either be disabled, or carefully configured so as not to prevent the Server from contacting the licensing server. Also any hardware firewall on the LAN should also be configured to allow appropriate network access to the PC on which the Server 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.

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

**Table 2** Firewall-related setup data

Application	Role	Default Path	Port number	Note
Setup.exe	Server installer	installation media	80/TCP	The bootstrap installer for Server
.MSI file	Server installer	installation media	80/TCP	The main installer for the server
VSolPService	Application	C:\Program Files\GANZ\VSolPSuite Server	24752/TCP	Server service application

More details about port utilisation should be available in documentation supplied with the IP camera or encoder, on the manufacturer's website, or from their technical support contacts.

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

- Anti-virus.
- Anti-spyware.
- Software firewall.

## .Net Framework

The installation program for the Server will automatically download the correct version of the .Net Framework for the Server. However if preferred, install the .Net Framework prior to installing the Server. 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.

## SQL Server Express Edition

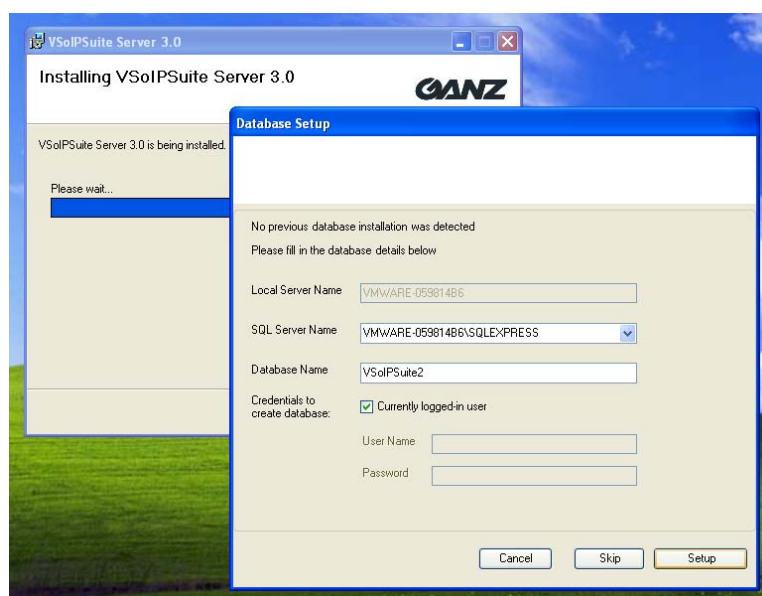
The installation program for the Server will automatically download the correct version of the SQL Server Express Edition. However if preferred, install the SQL Server prior to installing the Server.

Any desired configuration of SQL Server Express Edition should occur following the installation of the Server, and after the point where the database for the Server has been created.

## Installing the VSoIP Pro Server

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

The Server installer program setup.exe automatically examines the local system for the .Net Framework and SQL Server Express Edition. If these are not present, or they are earlier versions, the installer program will automatically connect to Microsoft's servers over the Internet and download the correct versions of the software.
- 3 Click to accept the terms of the license agreement.
- 4 Select an installation folder for the Server, or use the default folder suggested.
- 5 Click Next, then Next again.
- 6 The next step makes use of the SQL Server Express Edition database management system:



**Figure 1** Database Setup Phase

---

**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.

---

- a. Ensure that the SQL Server name includes the local server name, i.e. other SQL servers might be found on the network.
- b. Give a suitable short meaningful name for the database, or choose the one suggested.

- c. In typical installations, the credentials for the user authorised to create a database will be the currently logged-in user. Otherwise enter a user name and password that does have these privileges.

7 Click Setup to create the database.

---

**Caution:** If this step is skipped then the SQL database server is not used to store data. Instead, a file-based system is used. This should be avoided. It is suited only to demonstration systems where stored data is managed manually.

---

## Customising the Database

Following installation, the database settings can be customised if required using Microsoft's SQL Server Management Studio Express.

## Using the VSoIP Pro Server

Prior to starting the Server, confirm the following:

- Network connection is available and configured.
- .Net Framework is installed.
- SQL Server Express Edition is installed and the SQL server running.
- SQL database has been created by the Server's installer program.
- You are logged in with administrative privileges.

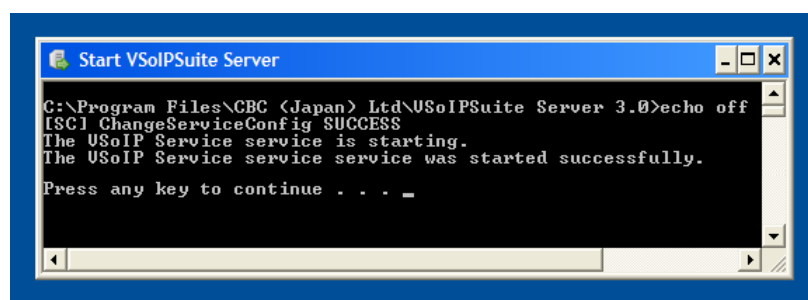
The Server runs as a Windows Service. As such it runs irrespective of whether or not a user is logged into the computer.

**Note:** Using the PC for other purposes in addition to running the Server service might impact on the performance of the Server.

The Server can be controlled in one of two ways. Either it can be started and stopped manually, or it can be started and stopped automatically when the operating system starts up and shuts down.

## Starting the Server Manually

From the Start menu locate the Server entry and choose the Start Server option. This signals to the Server that it should start up and run as a background task until the computer is shut down. When restarting the computer, the Server will not start again unless started through the start menu.



**Figure 2** Starting the server service

## Starting the Server Automatically

From the Start menu locate the Server entry and choose the Autostart option. This signals to the Server that it should start up and run as a background task until the computer is shut down. When restarting the computer, the Server will be signalled to start again and to remain running as a background task whenever the computer is running.



## Stopping the Server

From the Start menu locate the Server entry and choose the Stop Server option. This signals that the Server should stop running as soon as possible. If the start up of the Server was automatic then automatic start is switched off. The Server will now only start when Start menu Server start command is chosen.

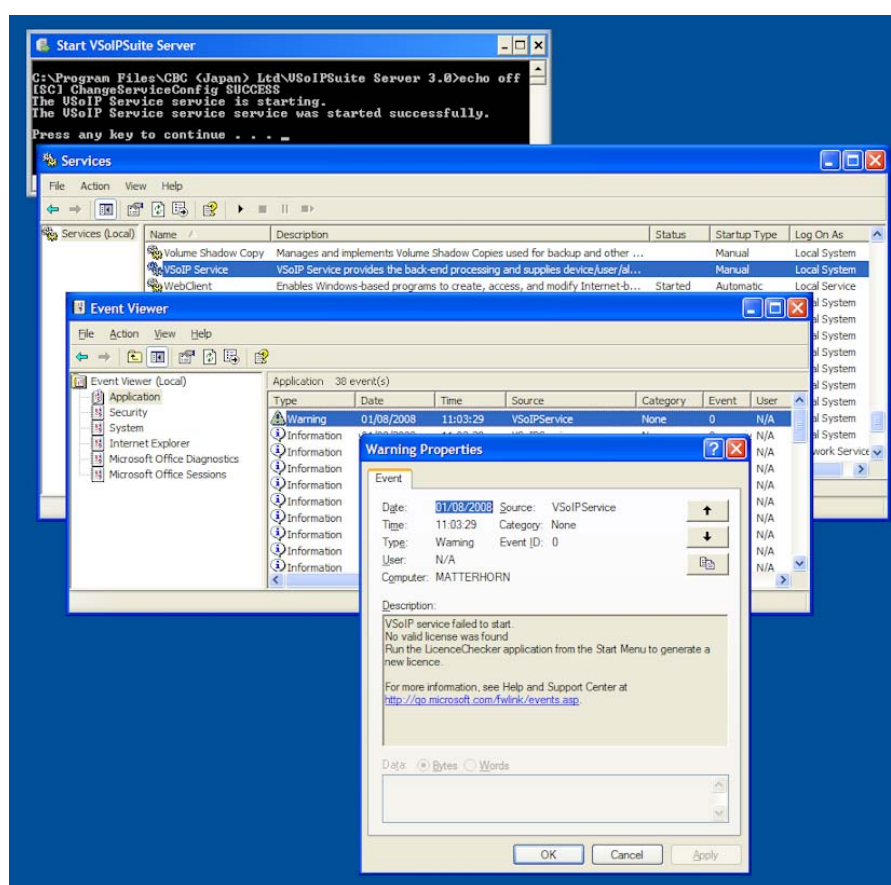
## Troubleshooting

### How can I be sure the Server is running?

The Server runs as a Windows service, see appendices for more details.

- 1 Using the Windows services listing application, check that the status of the Server service.
- 2 If the Server service is not started then check the Windows Event Viewer application to determine what errors might be preventing startup.

Figure 3 provides an example of this.



**Figure 3** Troubleshooting the Server service using Windows application

## Network Time Server

It is **extremely important** that all PCs running the Client software and other devices use a coordinated time service.

One unified time source must be used. If this coordinated time is provided by the Windows Domain server, then ensure that the source used by the Domain is the same one used for all networked video devices.

If using a Windows Domain controller as a time source, ensure that the Windows Time service is set to automatic start-up.

# Chapter 3 – The Client Component

This chapter contains information on the following:

- Prerequisites
- Before Installing the VSolP Pro Client
- Installing the VSolP Pro Client
- Post-installation checklist
- Network Time Server

## VSolP Pro Client Overview

The VSolP Pro Client software component (the “Client”) is a Microsoft .Net framework based application for Microsoft Windows operating systems. It is designed to view, play back, record and monitor alarms originating from surveillance resources such as IP cameras, networked digital video recorders (DVR), computers executing the NVR software component (the “NVR”) and computers executing the Video-wall software component (the “Video-wall”). Access to surveillance resources is controlled by the server software component (the “Server”).

The VSolP Pro Server sends events from various IP cameras, DVRs and NVRs, raising alarms on any Client permitted to receive events.

An audit trail representing a historical listing of past surveillance operations managed by the Server can be viewed on the Client.

Recording tasks such as scheduled recordings can be created and managed using Clients. Video footage originating from NVRs within the system can be played back on Clients. Access to NVR resources is managed by the Server.

The computer used to run the VSolP Pro Client should not be considered to be a general purpose PC and therefore should not be used for other tasks that might starve the Client of system resources. It is possible to run a Server and/or a NVR on the same computer as the Client but this can lead to a conflict of resources and as such is discouraged in all but the smallest of systems.

---

**Caution:** Clients discover Servers on the network using a multicast based discovery broadcast. Clients on networks that do not have broadcasting ability must use the IP address of the computer on which the Server is executing. Communication between Clients, Servers and NVRs is via .Net remoting. Communication between Clients and Video-walls is via HTTP.

---

The type of PC used should be one specially tuned for graphical display tasks and should be optimised to have very high Microsoft Direct-X 3D rendering performance. If dual-head displays are being used then it is important to confirm that the two heads each support Direct-X 3D rendering.

---

**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.

---

The network connection bandwidth should be carefully matched to the maximum number of viewing/playback sessions that are likely to be simultaneously viewed. This is the sum of the bandwidths consumed by the video feeds (live/DVR playback or from NVR playback).

## Prerequisites

### Hardware

The following hardware specification provides full frame rate video, without dropped frames, video corruption or latency, for 1 Mbps, 25fps, CIF resolution MPEG4 encoded PAL video with one I-frame every 10 seconds.

---

**Caution:** It is highly recommended that you consider the different demands of the bit-rates, resolutions, frame rates, levels of compression, codec types, of the system you are implementing when compared with this specification to ensure that your own system has the system performance that matches the demands it is likely to make. In addition, it is wise to add a safety overhead in addition to this to accommodate operating system efficiency changes over time.

---

- Processor: 32 bit architecture CPU (e.g Intel Core Quad Core Processor 2.4Ghz).
- Memory: 4096MB.
- Hard Drive/Storage - 500GB SATA Hard Drive.
- Optical Drives — DVDROM (for installation) and DVD/RW (for exporting recordings).
- 100 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:** Even on graphics systems with the two types of hardware enabled acceleration, there are some graphics systems that are limited to a maximum number of separate areas of video on-screen that can be supported at the same time. This limitation appears to a user as if no more than a fixed number of video panes 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 pane causes the expected video that was not being displayed in another pane to be displayed. This is not a defect in the surveillance client, rather this is a limitation of the graphics system hardware in use.

---

---

**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.

---

### Operating System

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

---

**Caution:** In geographical regions where different 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.
- Microsoft Windows Installer 3.1.
- Microsoft Direct-X 9.0c (March 2009).
- Microsoft Internet Explorer version 7 or later

**Note:** Microsoft frequently re-designs its web-sites 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.

## System

A Server must be available on the network for a Client to operate — if multicast is available on the network the name of the Server will be discovered by the Client, otherwise the IP address of the Server must be known.

# Before Installing the VSolP Pro Client

## 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 the changing the local or global policies relating to rights and permissions, are discouraged. These notes assume that the operating system is set-up is in a fresh installed state.

One local standard user account should be added. This should be a member of the Users group.

Client installation, .Net installation and Direct-X components 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 of the Windows operating system should be carried out as a 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. Check this by opening a command prompt and running the IPCONFIG Windows command-line utility, see Appendix A.

The PC must be set up so that it can browse the Internet. Following installation, the Client will need to contact a licensing server located on the Internet in order to complete the installation and activate.

## Firewall Information

For best performance, simplicity of setup and easy maintenance, it is recommended that a dedicated firewall protects the entire network rather than firewall software running in the client PC.

Any local software firewall should either be disabled, or carefully configured so as not to prevent the Client from contacting the licensing server. Also any hardware firewall on the LAN should also be configured to allow appropriate network access to the PC on which the Client 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 3** Firewall-related setup data

Application	Role	Default Path	Port no.r	Note
Setup.exe	Client installer	installation media	80/TCP	The bootstrap installer for Client
.MSI file	Client installer	installation media	80/TCP	The main installer for the Client
VSolPClient	Activation	C:\Program Files\GANZ\VSolPSuite Client	80/TCP	Required to enable Client
VSolPClient	Application	C:\Program Files\GANZ\VSolPSuite Client	24752/TCP	Access to Server Service application

More details about port utilisation should be available in documentation supplied with the IP camera or encoder, on the manufacturer's website, or from their technical support contacts.

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

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

To ensure maximum performance, the Client PC requires an excellent graphic 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 graphic 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 Client 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.
- 4 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 the Client.

### Additional Security Software

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

- Anti-virus.
- Anti-spyware.
- Software firewall.

### .Net Framework

The installation program for the Client will automatically download the correct version of the .Net Framework for the Client. However if preferred, install the .Net Framework prior to installing the Client. 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 VSoIP Pro Client

- 1 Log in to the computer using the user name of a user with administrative level privileges, typically this is the administrator user name.
- 2 Navigate to and double-click setup.exe to start installation.  
  
The Client 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 Click to accept the terms and conditions, then click Next.
- 4 Choose the Client's installation folder, or use the default folder suggested. Click Next.
- 5 Click Next to start the installation.

## Post-installation checklist

Prior to starting the Client, confirm the following:

- Network connection is available and configured.
- .Net Framework is installed.
- Microsoft Direct-X 9.0c (March 2009) installed.
- Client has been activated.
- Server is reachable on the network. For more information about how to check connectivity with networked components see the Appendices
- A "standard user" operating system account has been created, i.e. a member of the Users operating system group.

## Network Time Server

It is **extremely important** that all PCs running the Client software and other devices use a coordinated time service.

One unified time source must be used. If this coordinated time is provided by the Windows Domain server, then ensure that the source used by the Domain is the same one used for all networked video devices.

If using a Windows Domain controller as a time source, ensure that the Windows Time service is set to automatic start-up.

# Chapter 4 – Client Activation and Licensing

This chapter contains information on the following:

- Activating the VSoIP Pro Client
- Client Licensing – Evaluation mode
- Logging in to the VSoIP Pro Client

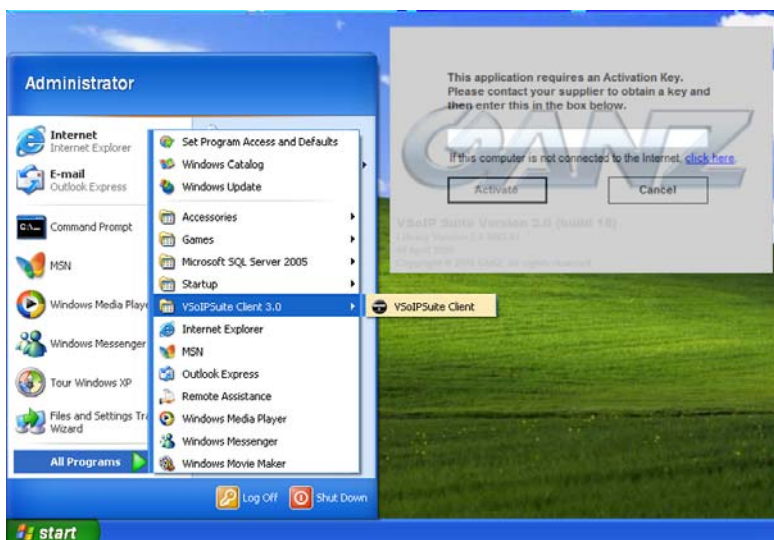
## Activating the VSoIP Pro Client

Prior to use, you must activate the VSoIP Pro Client. Activation is performed over the Internet and requires an activation ID. Activation is a one-time process. Once activated, the VSoIP Pro Client does not need reactivating.

**Note:** Activation IDs are tied to various products even though they look very similar. Please be sure that you use a Client activation ID rather than a Server or NVR activation ID.

Once an activation ID is used it is tied to the identity of the computer used to activate it. If for some reason the licence file generated by activation is lost, then the ID originally used to license the Client can be reused to re-activate the Client.

Each time the Client is started a licence check is made. This check does not require Internet access. If the Client is not licensed, then the activation dialog will be displayed.



**Figure 4** Client activation

During activation, it is essential that you are connected to the Internet. The Client needs to contact the licensing server over the Internet to validate the submitted activation ID. Ensure that an internet connection is available and that the Client application is not prevented from accessing the Internet by a local software firewall.

Enter the activation ID and click Activate. Activation can take a few seconds. Activation success, or failure, will be indicated.

If activation fails, please check the following:

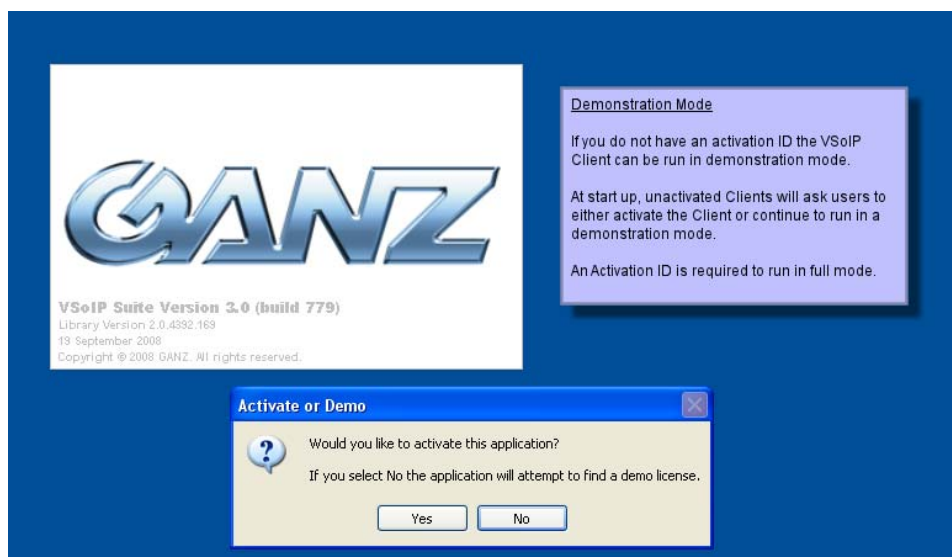
- Have you used the correct Activation ID?
- Has the Activation ID already been used by a different PC?
- Have there been too many hardware changes to the computer?

- Have you turned off the CPU ID feature of your PC or are using hardware identity masking software? If there are insufficient identifying characteristics, then the licensing server cannot license your PC.
- Are you using machine virtualisation software such as VirtualPC or VMWare? You must use native hardware rather than virtualised hardware.
- Could something be preventing an Internet connection – e.g. firewall block?
- Could the activation server be busy? Wait a while and try again.
- Do you have sufficient account rights to write licence file to local hard disk? Ensure you are attempting to license the Client using an account with administrator level privileges.
- If you are in a geographical region where several calendar types are used, have you set your regional Date/Time setting to use the Gregorian calendar?

## Client Licensing – Evaluation mode

Typically the Client must be activated in order for full use can be made of the Client. However, the Client can also be executed in a demonstration mode.

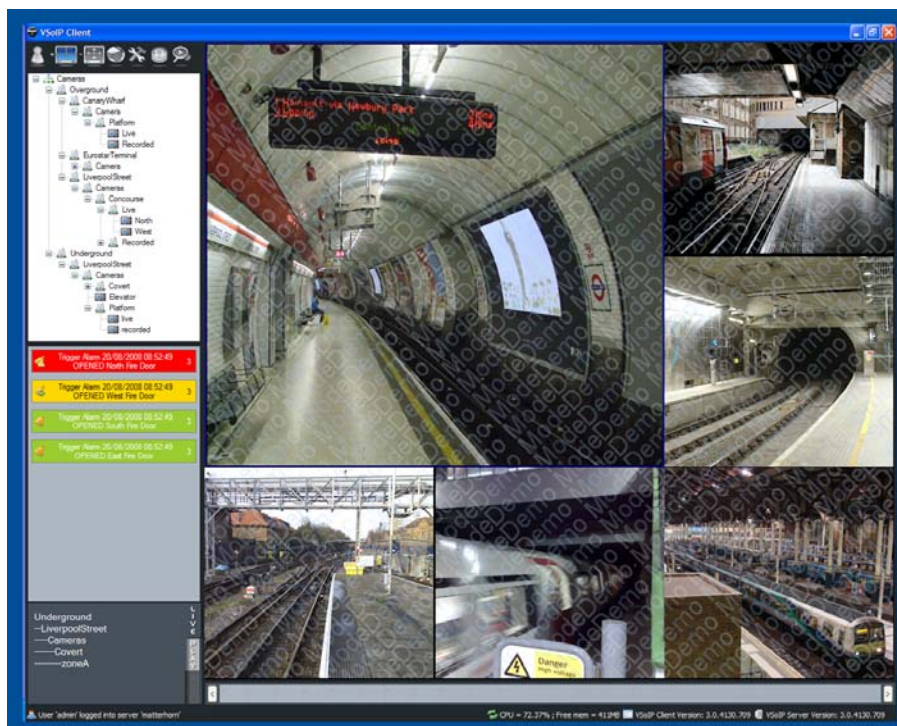
**Note:** The Client installed is the full version running in an evaluation or demonstration mode. To switch off demonstration mode a Client activation ID is required.



**Figure 5** Starting in evaluation mode

In demonstration mode, live video panes have text obscuring some of the video displayed from the Networked DVR, IP camera or encoder.





**Figure 6** Demonstration mode in action

## Logging in to the VSoIP Pro Client

In order for a Client to participate in the Surveillance system the Client programme must have been installed, activated, started and a user must have logged in.

### Starting the Client

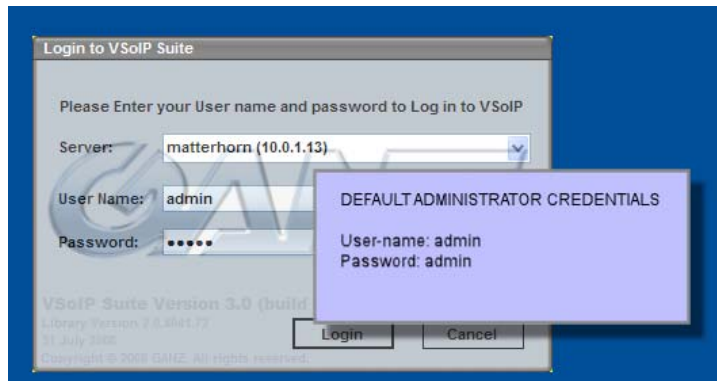
Open the Windows Start menu and choose the Client shortcut to start the Client.



**Figure 7** Starting the Client from the Windows Start menu

### Default Administrative User

The Server has a pre-loaded administrative user name and password. Use this user to initially configure your system.



**Figure 8** Logging in using the default administrative user

---

**Caution:** The default administrative password should be changed as soon as possible as it poses a security risk, should the password become known to users of the system.

---

## Logging in

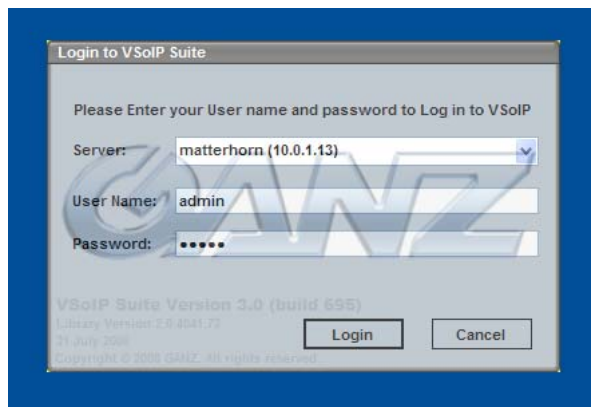
After starting the Client, you are asked to log into the Server. To log in, specify which Server you wish to log into and enter the required user name and the password associated with that user.

To be granted access to the Server you must have:

- Chosen a Server to log into.
- Used a user name known to that Server.
- Entered a password for the user which matches the one known by the Server.

If you experience problems when logging in, check that:

- The server is reachable.
- Your user name has not been disabled.



**Figure 9** Logging in to the client

Following a successful login, the Client remembers the last user name and Server used. This allows quicker login next time the Client is started. The user's password is not remembered and must be entered each time the Client is started.

**Note:** If you do not see the expected Server name in the list of Servers, you can enter the IP address of the Server manually.

## Logging out

To log out of a Server, close the Client.

# Chapter 5 – Client Configuration

This chapter contains information on the following:

- System Overview
- Getting Started
- User Configuration
- User Group Configuration
- Adding Devices
- Deleting Devices
- Configuring Video Sources
- Configuring Pan-Tilt-Zoom Capabilities
- Complex Alarm Configuration
- Mapset Configuration
- Working with Live Video and PTZ
- Working with Alarms
- Playing Back Recorded Video
- Exporting Recorded Video
- Audit Trail Configuration

## System Overview

The VSoIP Pro system contains several configurable aspects, including:

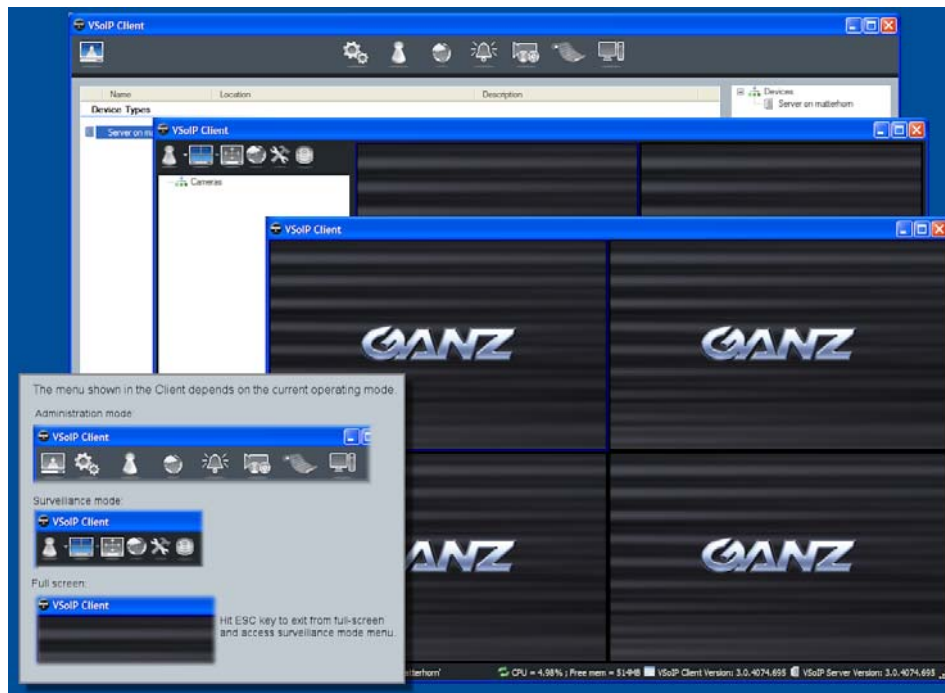
- Devices — collections of IP Cameras, Networked DVRs, Video-walls and NVRs.
- Mapsets — collections of maps.
- System users.
- User groups — groups of users with restricted access to devices, mapsets, and various operations within the system.
- Audit trail — keeps a record of actions taken on the system.

## Getting Started

We recommend that you take the following steps when configuring your VSoIP Pro client:

- 1 Log in as the default administrative user.
- 2 Add a new administrative level user.
- 3 Log out.
- 4 Log in as the new administrative level user.
- 5 Change the default administrative user's password.
- 6 Add devices to the system.
- 7 Add previously constructed mapsets (optional).
- 8 Add a non-administrative level user group.
- 9 Assign the devices, mapsets, and set rights and privileges for various actions to the non-administrative level user group.

10 Add all system users to the non-administrative level user group.



**Figure 10** Accessing the Client's main menu

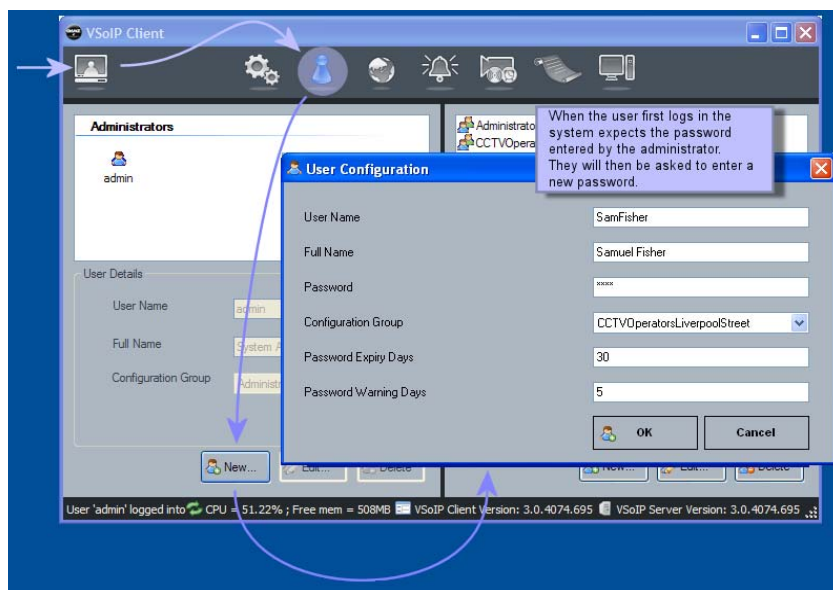
## User Configuration

The system is preconfigured with one user, the default administrative user. This is the user initially used when starting the system setup process.

**Note:** When you finish adding users, you can create a backup of these in case of data corruption. See “Reusing Devices, Users and Groups” on page 83 for details.

### Adding a new user

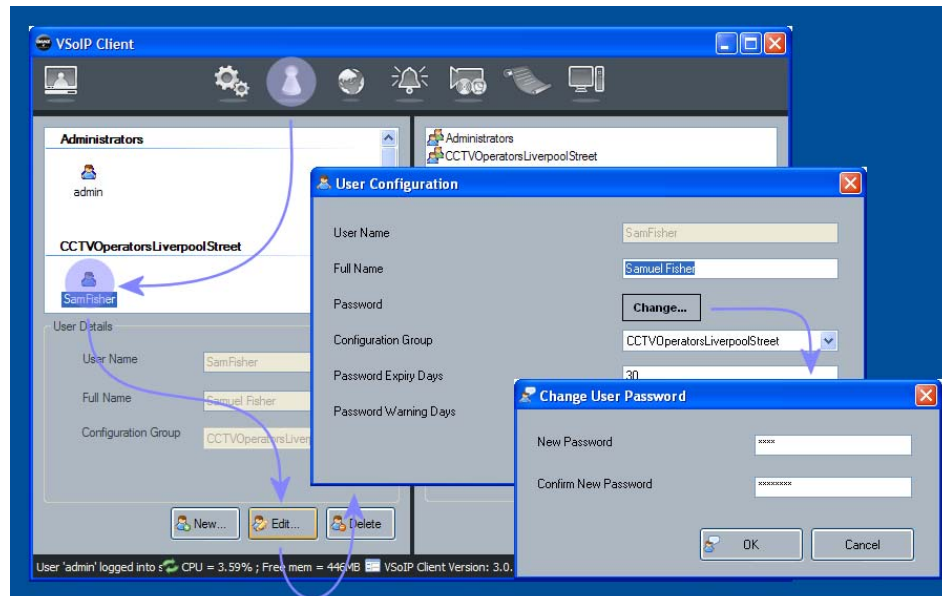
To add a new user you must be logged in as a member of the administrative user's group. When adding a new user, you must add the user to an existing group.



**Figure 11** Adding a new user

## Changing user passwords

An administrator level user can assign and change existing passwords for all users, including themselves.

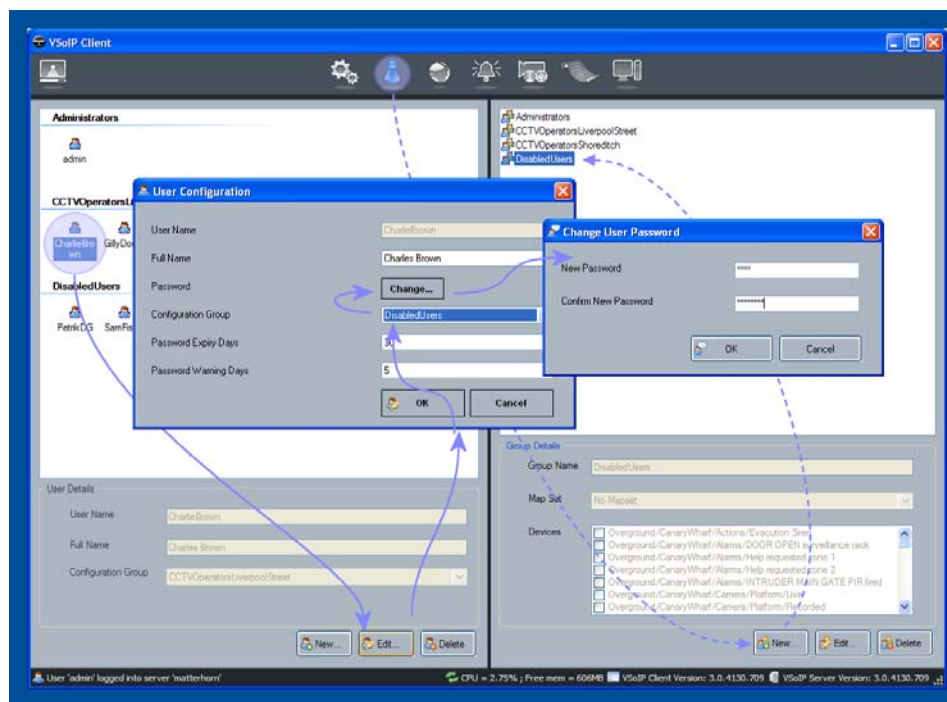


**Figure 12** Changing user password

**Note:** Any user can change their password using the top-level menu.

## Temporarily preventing a user from logging in

Rather than deleting a user to prevent them from using the system, you can disable the user's log-in privilege.



**Figure 13** Enabling/Disabling a user

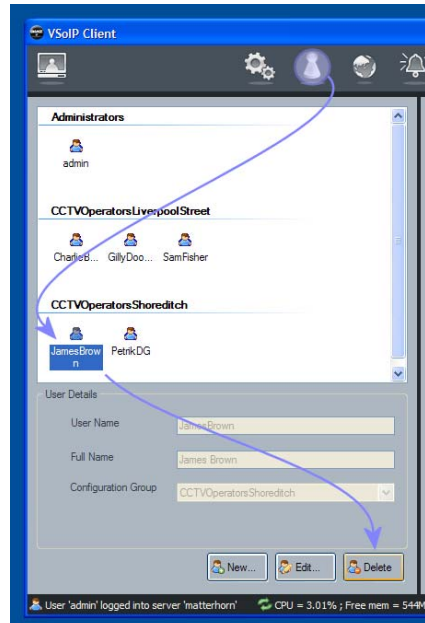
To disable a user:

- 1 Create a Disabled Users group. Members of this group should not have any administrator permissions, nor access to any devices.
- 2 Select the user to be disabled.
- 3 Click Edit.
- 4 Change the group for that user to Disabled Users.
- 5 Change the password. You now have a group containing users which have been disabled. These users cannot now log in since they are unaware of the new password. They would also not be able to access devices, etc, if they were to correctly guess the new password.

**Note:** It is not possible to disable all administrative level users, i.e. there is always one enabled administrative level user maintained within the system.

## Deleting an existing user

You cannot delete a user if you are logged in as the user being deleted. You cannot delete the only administrative user within the system.



**Figure 14** Deleting a user from the system



## User Group Configuration

VSolP Pro is preconfigured with one user group, the administrative group. This group provides unrestricted access to all system elements. Any user created in the system that is added to this group will also gain similar unrestricted access.

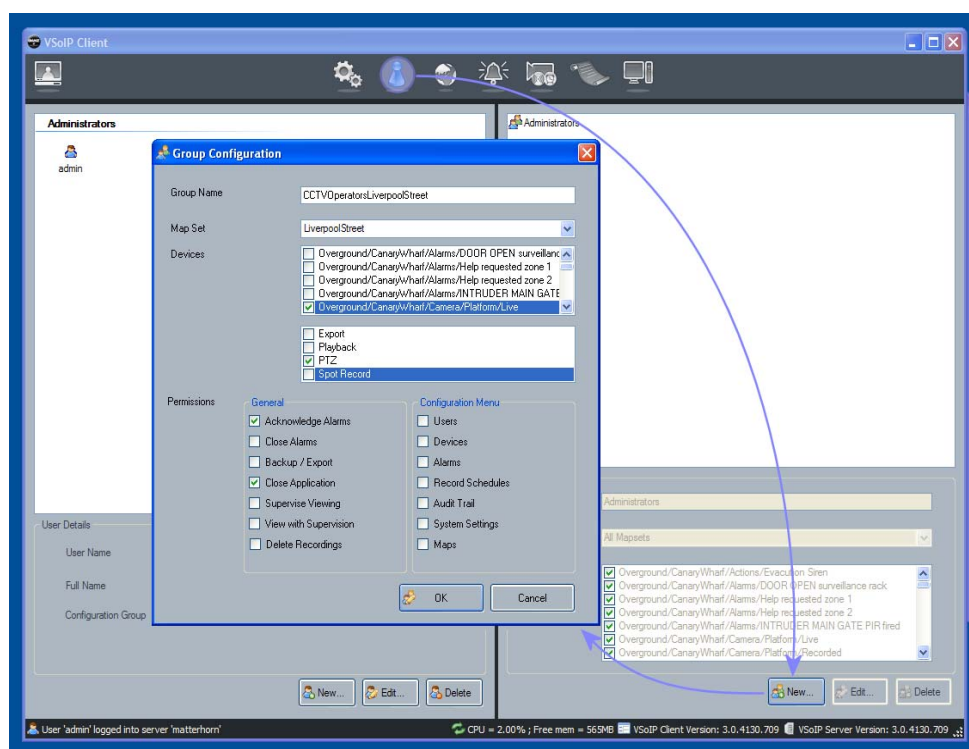
---

**Caution:** The system installs one default administrative user with a well documented user name and password. This password should be changed soon after the system is installed and prior to the completion of the system's commissioning.

---

**Note:** When you finish adding user groups, you can create a backup of these in case of data corruption. See "Reusing Devices, Users and Groups" on page 83 for details.

### Creating a User Group



**Figure 15** Adding a new user group

To create a new user group:

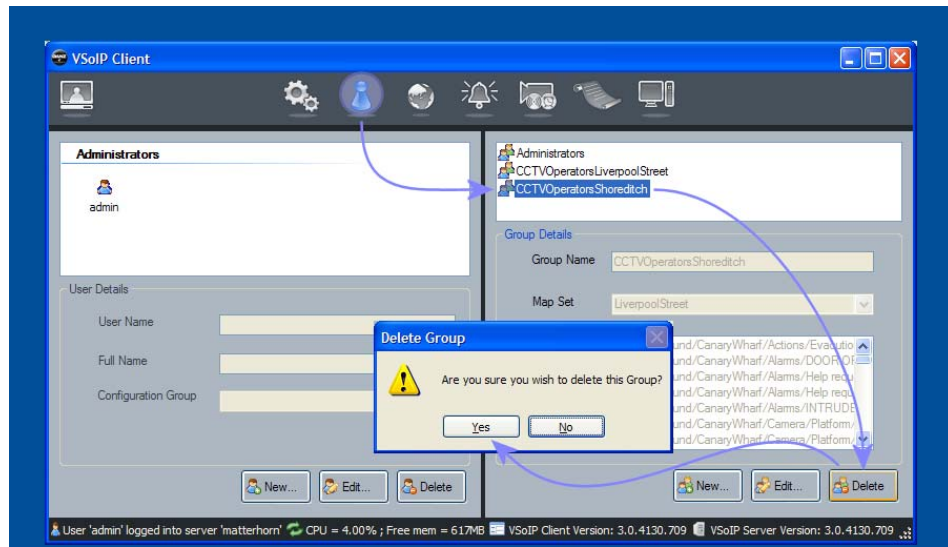
- 1 Type a name for the group
- 2 Put a check against those devices that members of this group can access.
- 3 Next, for each of the devices, choose the operations in addition to viewing live video that group members can perform, e.g. viewing recordings from that camera, controlling an attached pan-tilt-zoom control unit.
- 4 Next specify which administrative operations members can perform, e.g. examine the audit trail, add new maps, delete users, etc.
- 5 Finally choose general restrictions that apply, e.g. they are not allowed to create backups of a recording.



## Deleting a User Group

To remove members, you can delete them, or reassign them to a different user group.

**Note:** You must ensure that there are no users in a group before you delete it.



**Figure 16** Deleting a user group

---

**Caution:** You must remove all users from a group before you delete it. You can remove members by deleting users, or reassigning the users to different configuration group(s).

---

## Device Configuration

A device can be one of the following:

- An IP camera.
- An IP encoder.
- A Video-wall.
- A Transcode Server.
- An Analytic Server.
- A Networked DVR.
- A Networked Video Recorder.

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. A Networked DVR can have a number of video sources, typically one for each video input, e.g. sixteen video sources in a sixteen channel Networked DVR.

A Video-wall device is a mirror opposite of devices that act as video sources. A Video-wall displays video sources; the maximum number of video sources displayed is a fixed capability of the Video-wall device.

An NVR device records video sources and is also a video source. An NVR generates one video source for every playback session that is active.

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.

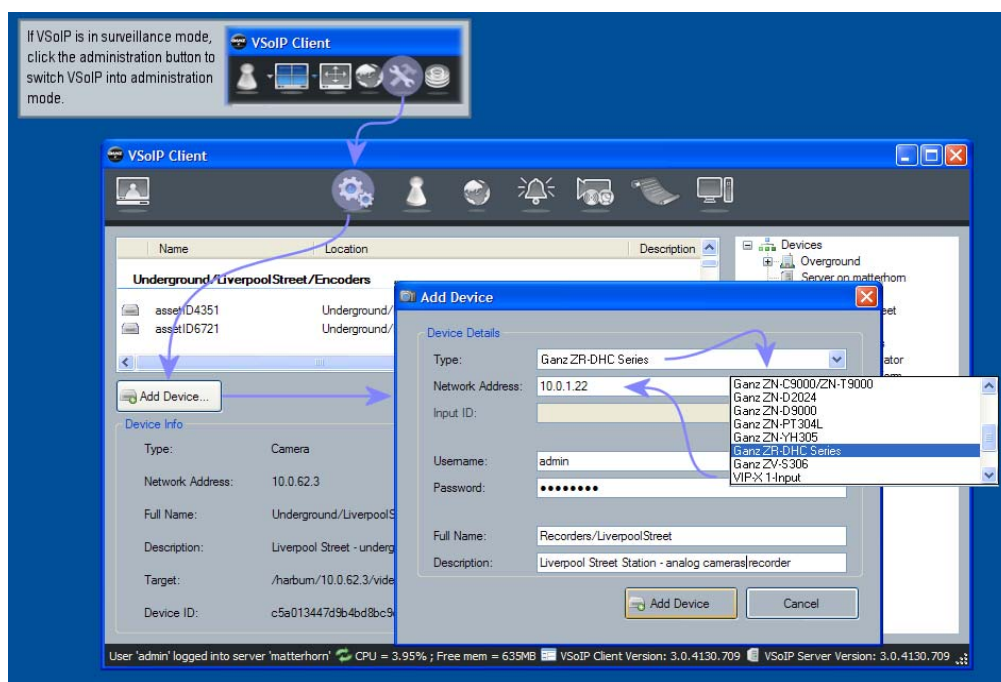
Other signals can be as a result of motion detection events generated by video analytics on the device.

NVRs and Networked DVRs can signal the occurrence of a system event such as insufficient storage space, or some other fault.

IP cameras and Networked DVRs can optionally support Pan-Tilt-Zoom (PTZ) devices. A PTZ device 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 IP cameras, Networked DVRs, pan-tilt-zoom control units and protocols, NVRs and Video-walls. When you finish adding devices, you can create a backup of these in case of data corruption. See "Reusing Devices, Users and Groups" on page 83 for details.

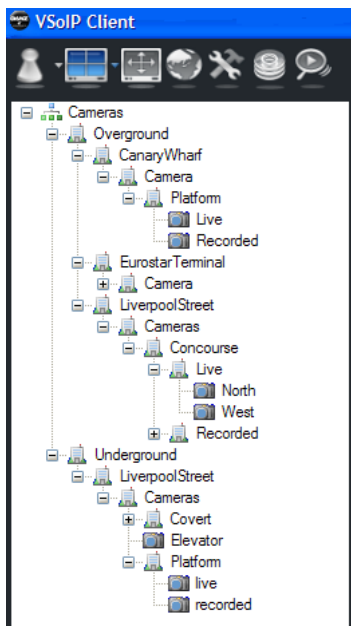
## Adding Devices



**Figure 17** 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 18** Device hierarchy example

Location text is used to logically group devices. An example of the location text can be seen by looking at the presentation of the device hierarchy or "site". 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.

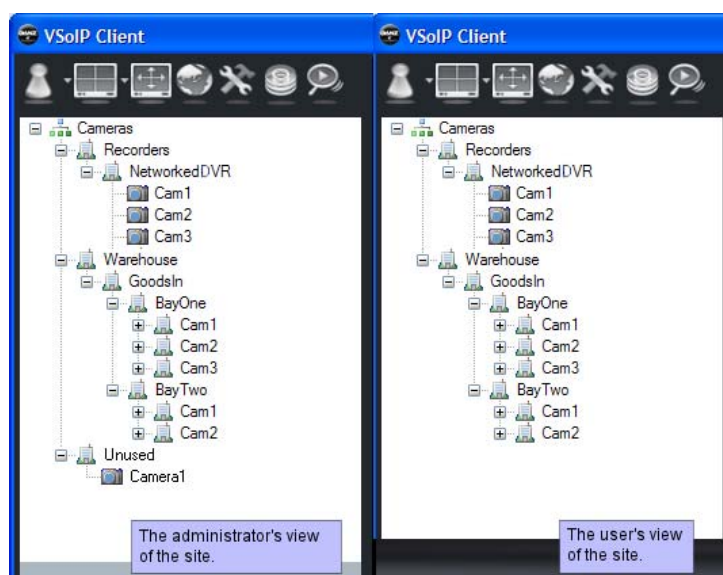
Some location text examples as shown in Figure 18:

- 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 19** 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 19.

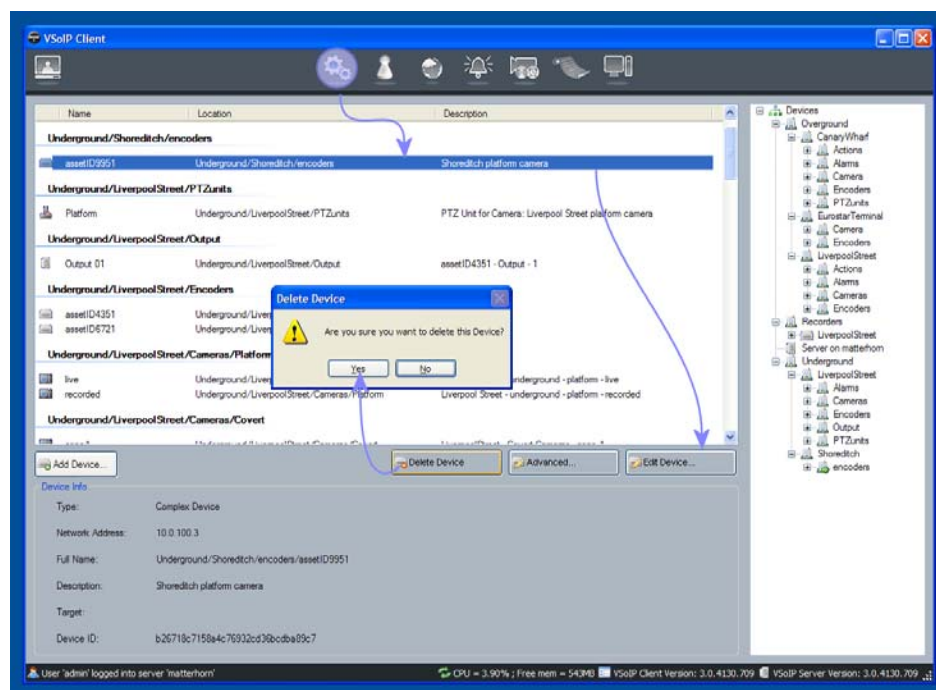
### Using the location string to hide unused devices

Because you cannot delete cameras from a device in the site, you can use the location string to “hide” cameras which are currently unused so that they cannot be seen by users.

To do this, create a location string and allocate it to unused devices, as shown in Figure 19. Here, Camera 1 has been given the location string Unused/Camera1.

You can then use the User Group Configuration dialog (see Figure 11) to specify that no users can view devices with that string.

## Deleting Devices



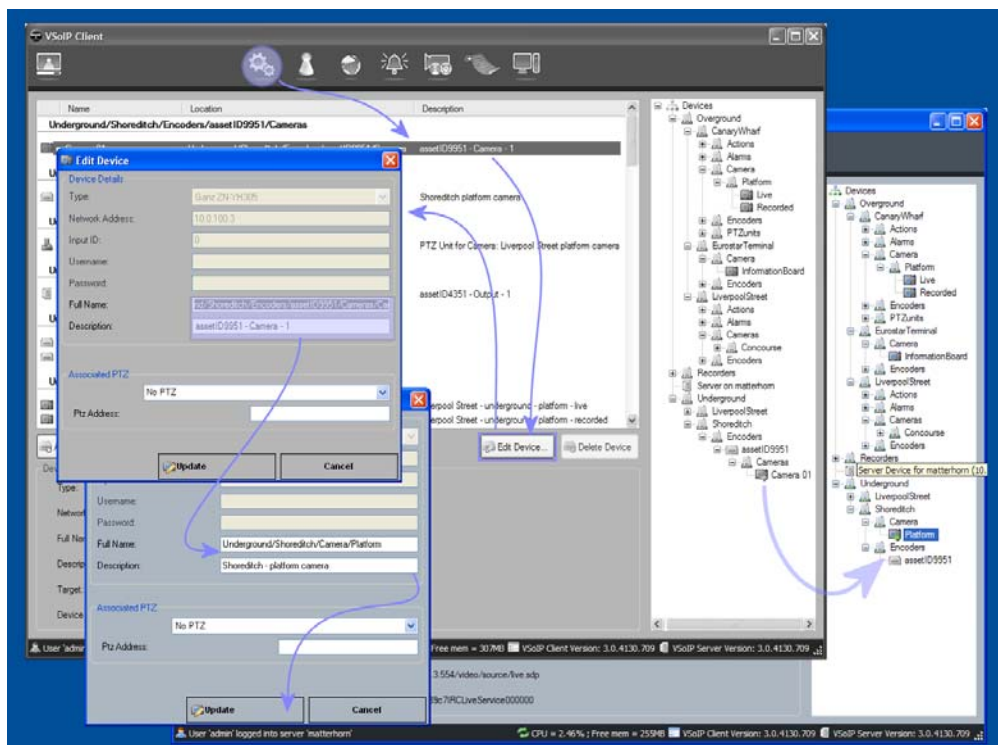
**Figure 20** Deleting a device

**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 21** 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.

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 Pro Clients 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.

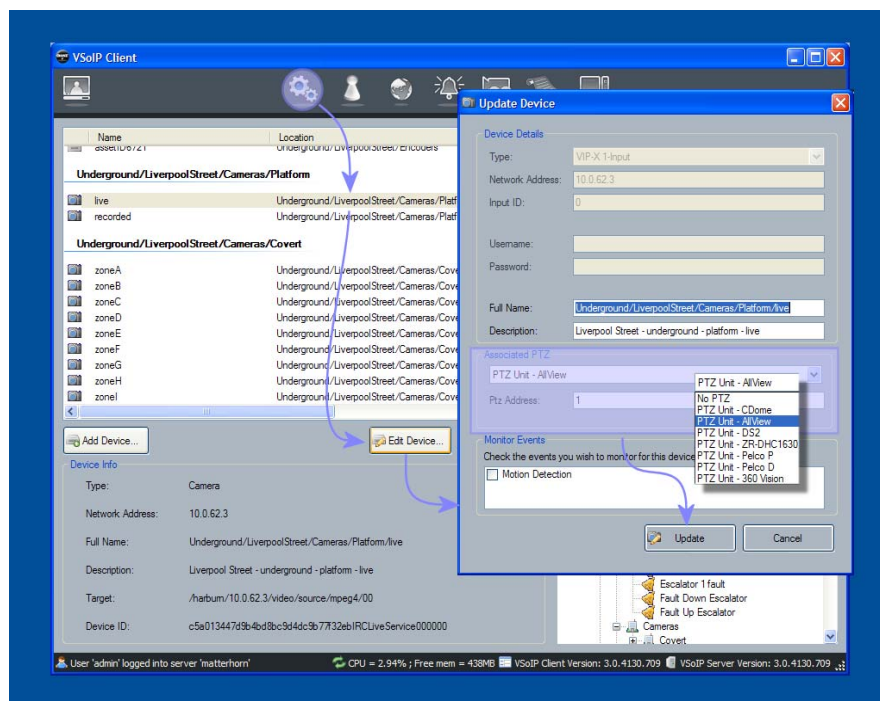
Use the location text to logically group triggers into groups that make sense for the physical site being monitored.

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.

The surveillance suite can allow the pan-tilt-zoom control to be controlled by any user within the surveillance site with permissions to do so.



**Figure 22** 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.



## Mapset Configuration

Mapsets are a collection of hypertext marked-up documents archived in a zip file format archive. See “Designing Mapsets” on page 62 for more details about mapsets and their construction.

**Note:** The following assumes that a valid mapset has been created.

### Adding Mapsets

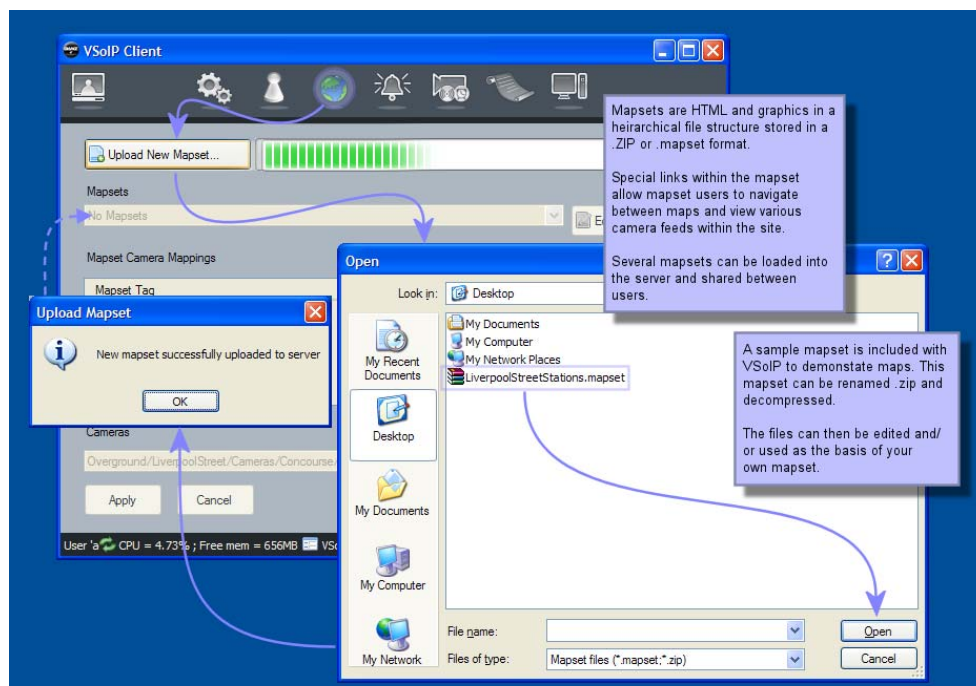


Figure 23 Uploading mapset on disk to server

### Associating Map-links with Devices

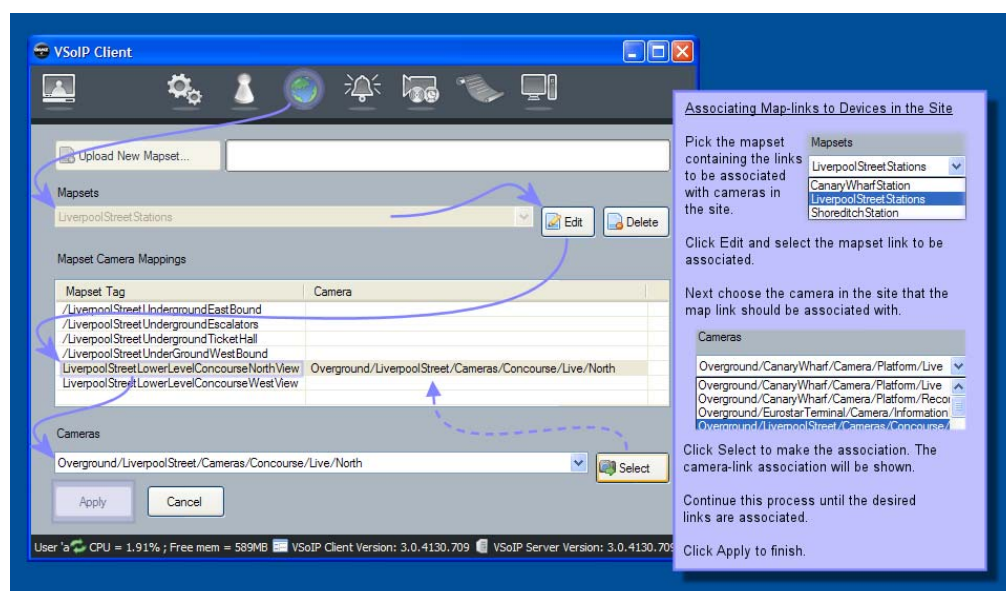
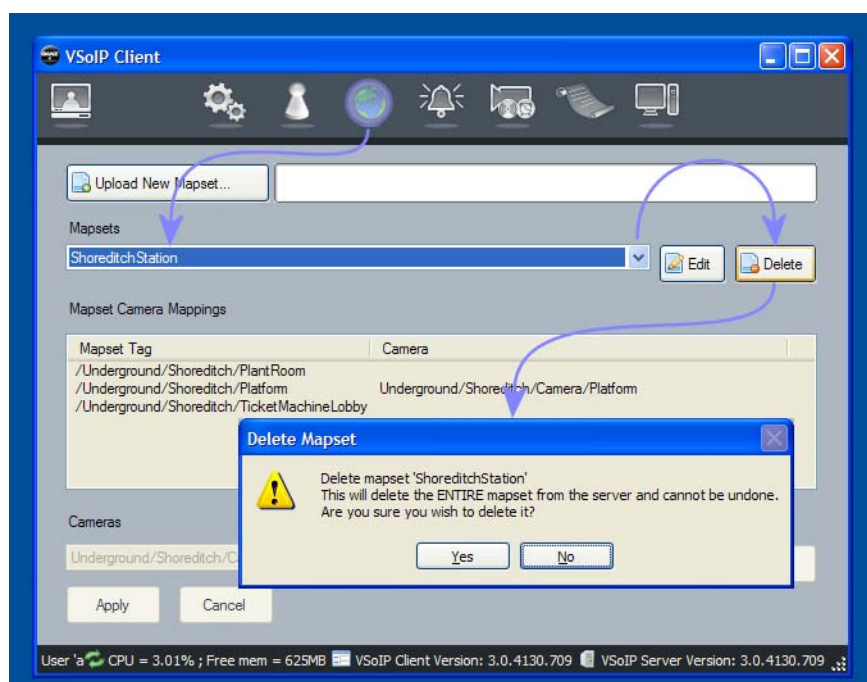


Figure 24 Assigning map-links to devices within site



## Deleting Mapsets



**Figure 25** Deleting mapsets from server

## Working with Live Video and PTZ

VSolP Pro 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.

**Note:** Permissions to view an IP camera, a camera input of a Networked DVR and control a PTZ unit associated with those cameras are managed by the Server.

### Live View Controls

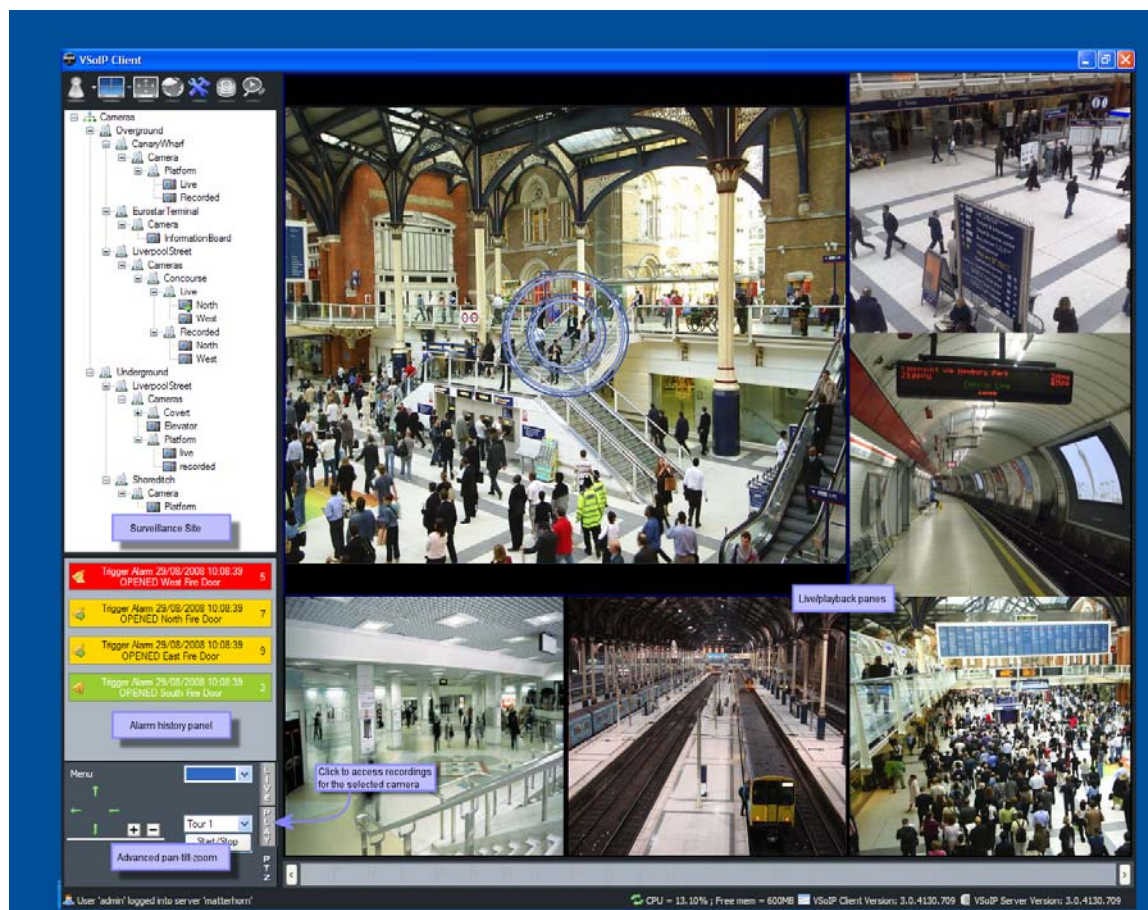
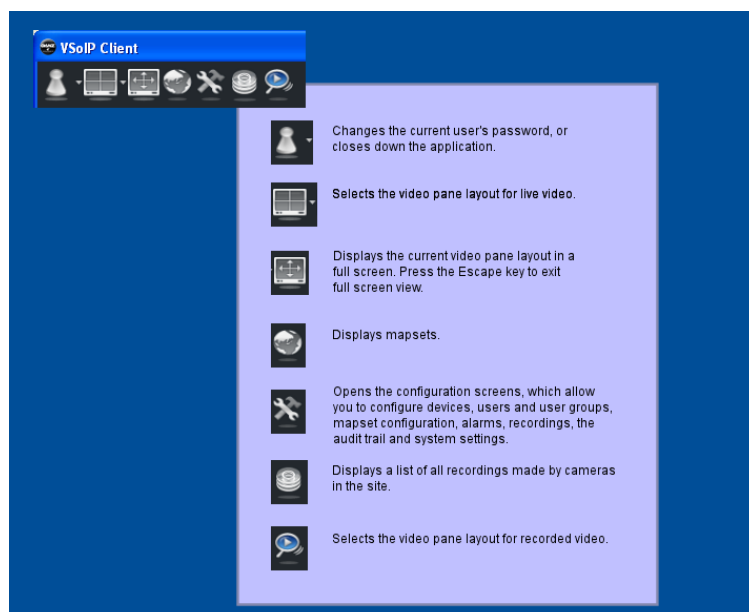


Figure 26 Main live viewing controls


## Accessing other features

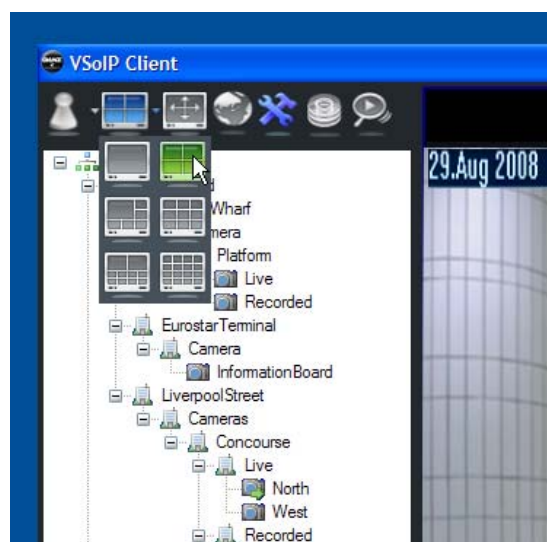
The main menu can be used to switch the Client into various surveillance modes. This menu also allows the operator to change their own password and exit the application.



**Figure 27** 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 28** Specifying a video pane layout

## Starting and Stopping Live Video

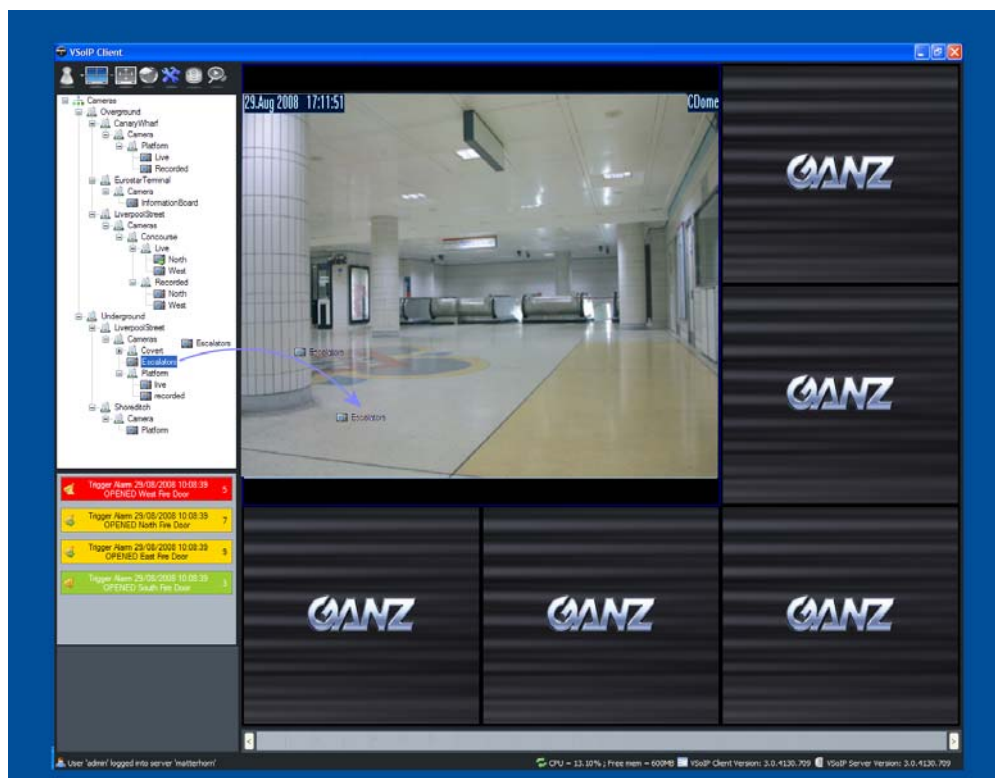


Figure 29 Starting video using mouse drag-drop

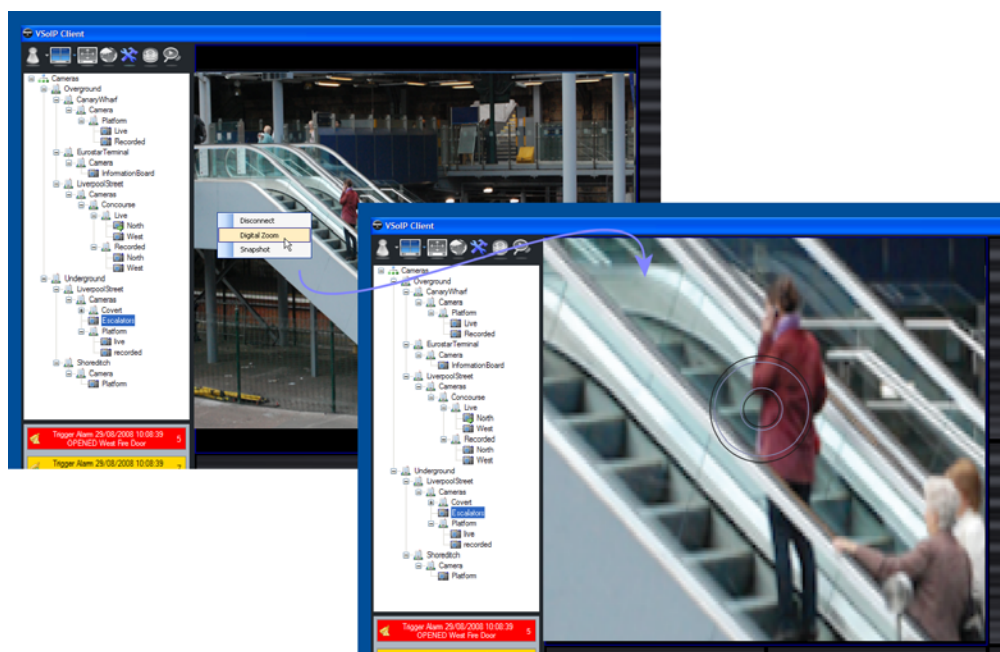


Figure 30 Stopping video or exiting from a map



## Using Digital Zoom

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

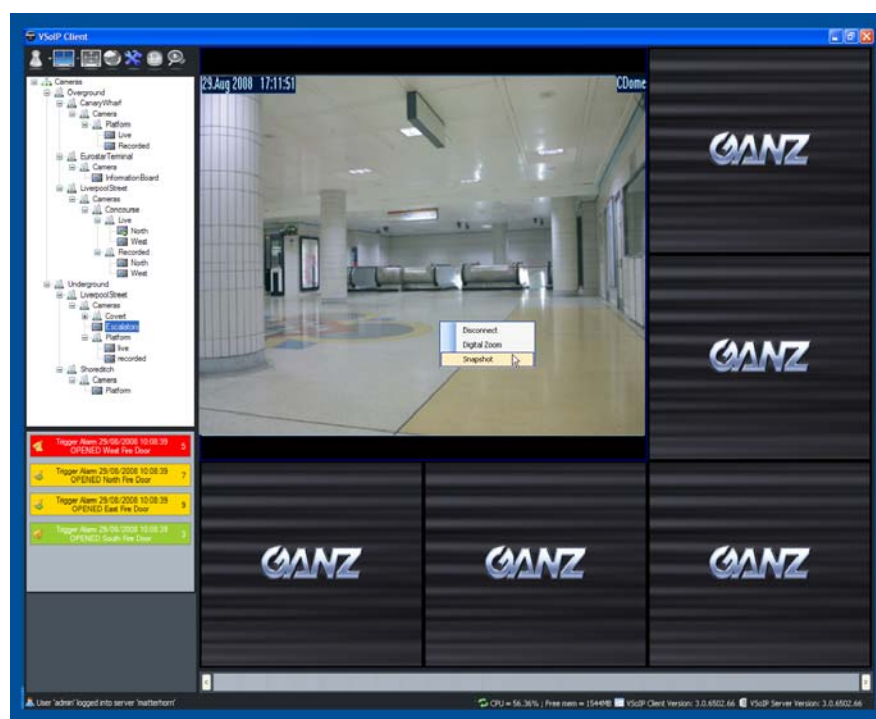


**Figure 31** Zooming into live video

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

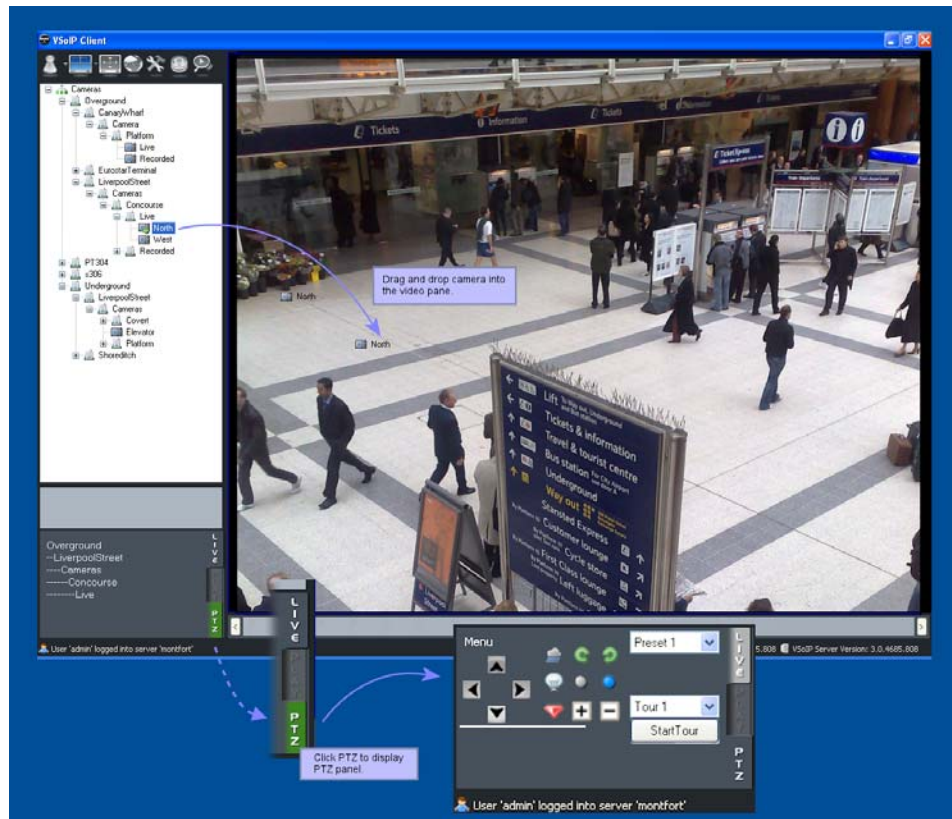
VSolP Pro allows you to capture snapshots of live video playing in a video pane. By default, these are saved to \Desktop\VSolP Image Clips\FromLiveDevices, as .jpeg images. To change this location, see “Changing Client Settings” on page 85. To take a snapshot, right-click in the pane displaying the video at the point you want to capture, and select Snapshot.



**Figure 32** Taking a snapshot of live video

## Control of Pan-Tilt-Zoom

### Activation/Deactivation



**Figure 33** Activating/deactivating PTZ support

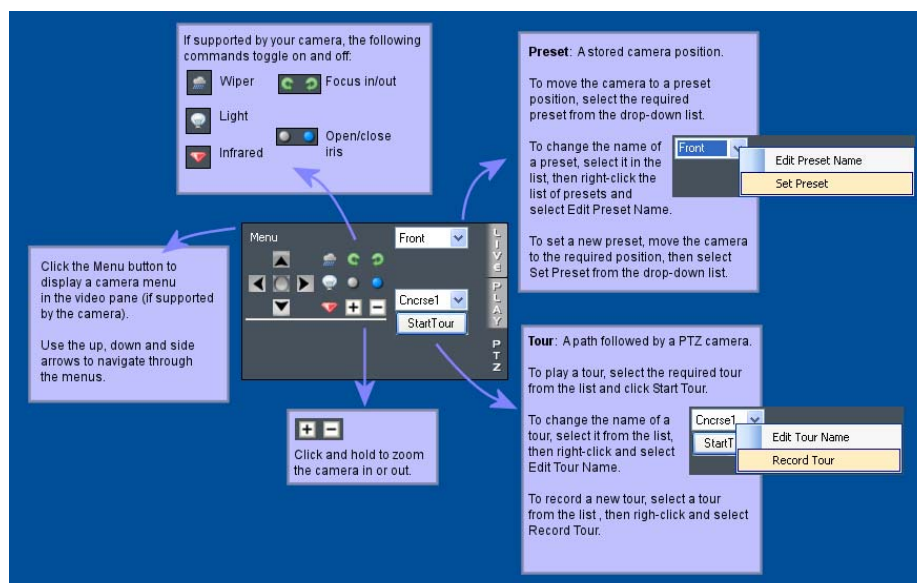
### Moving and Zooming



**Figure 34** 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 35** Additional PTZ unit features support

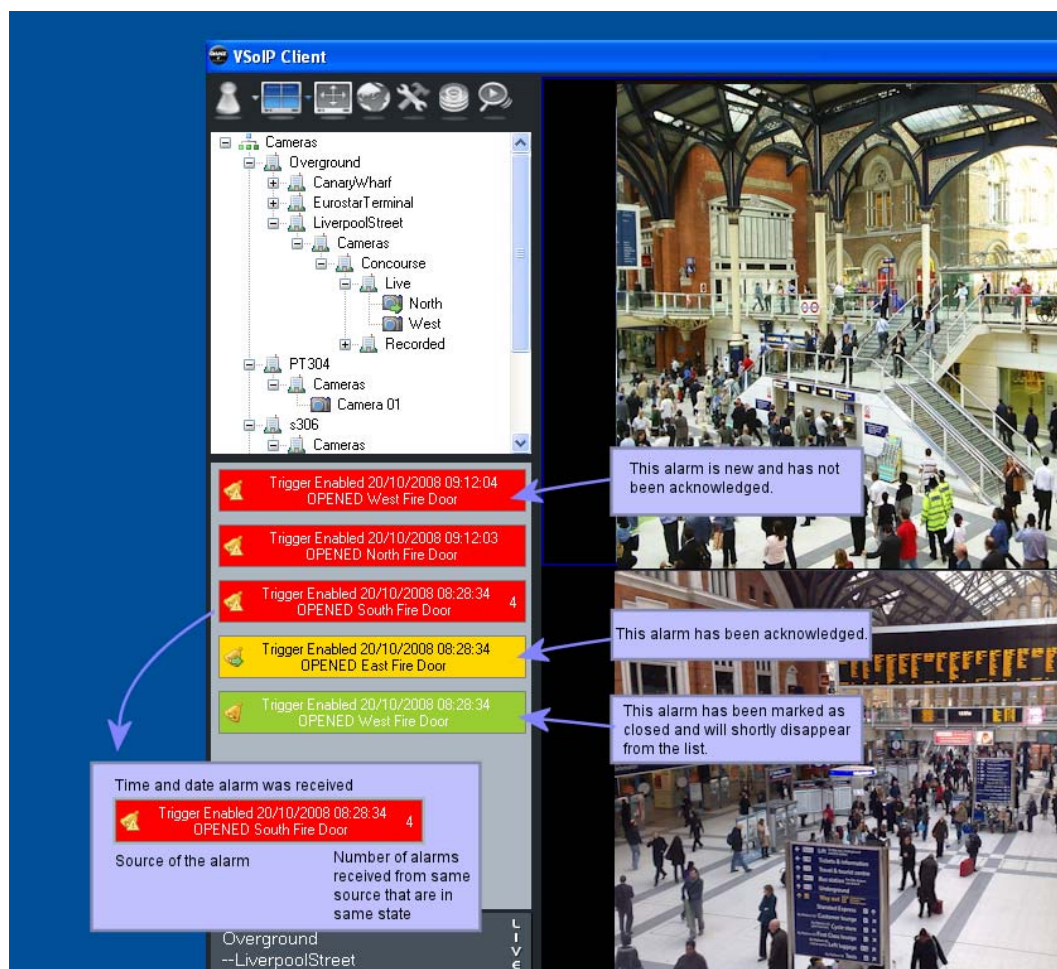
**Note:** PTZs vary in functionality, so access to features depends on the chosen PTZ unit's capability.

## 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. Access to the device associated with the alarm source must also have been enabled for the group to which the logged-in user belongs. For details, see “Configuring Triggers” on page 38.

### Overview of Alarm Display

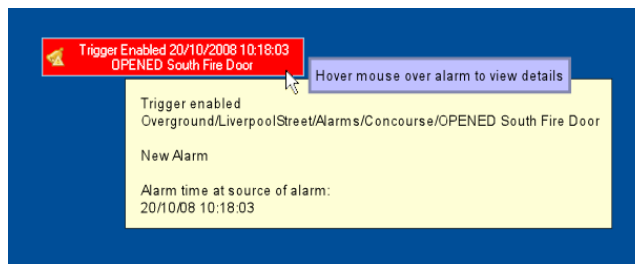


**Figure 36** Overview of alarm display

**Note:** If an alarm in the alarm stack is associated with a camera, you can drag and drop it onto a video pane to view live video from that camera. Similarly, if an alarm in the alarm stack has a recording associated with it, drag and drop it onto a video pane to start viewing that recording.

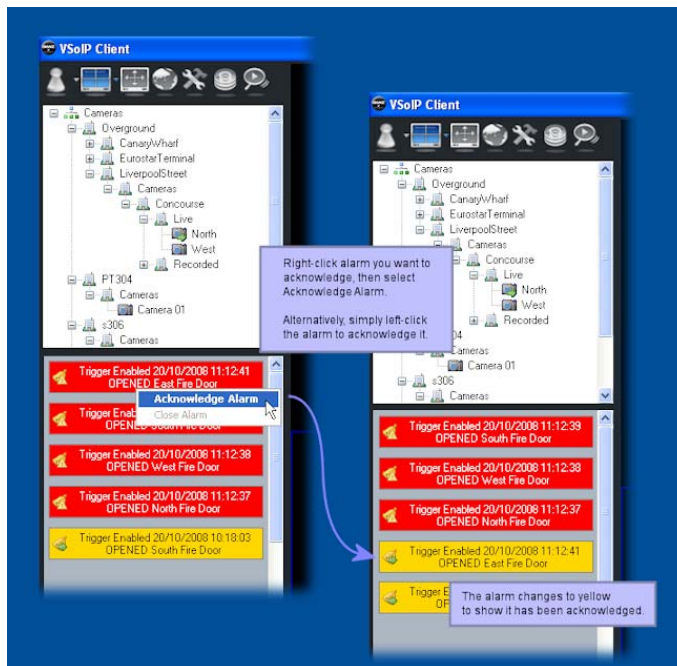


## Viewing Properties of an Alarm



**Figure 37** Alarm properties

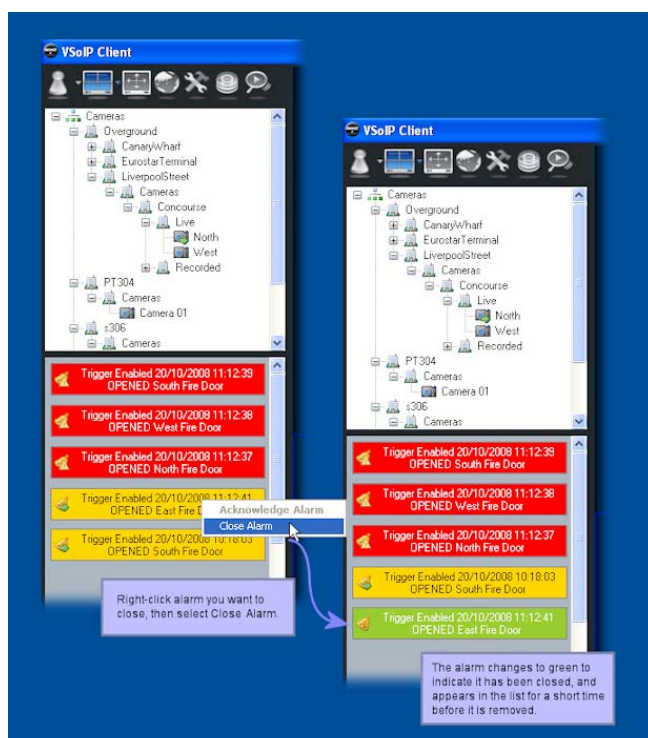
## Acknowledging an Alarm



**Figure 38** Acknowledging an alarm

When a user acknowledges an alarm, the Server notifies all connected Clients, which in turn update the alarm display to reflect the new state of the alarm.

## Closing an Alarm



**Figure 39** Closing an alarm

**Note:** When the user closes an alarm, all Clients connected to the Server remove the closed alarm from the alarm display (this may take a short time).

## Playing Back Recorded Video

The Client allows CCTV operators to view video recorded on Networked DVRs and NVRs.

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

Playback is very flexible and permits playback from more than one camera on the same recorder, cameras from different recorders, and the same camera on the same recorder at different times, or some permutation of these.

**Note:** Be aware of the load placed on various parts of the network and on the devices themselves when requesting playback sessions.

The Server manages access to recorders within the surveillance site. To play back video from recorders a user must belong to a group with appropriate privileges to view the IP camera or Networked DVR analogue input AND permitted access to the recorder.

## Discovering Recorded Footage

For a recording of a particular camera to be visible, that camera must have been recorded by at least one recorder in the surveillance site. Recordings made by a recorder that do not match any device in the surveillance site are not listed.

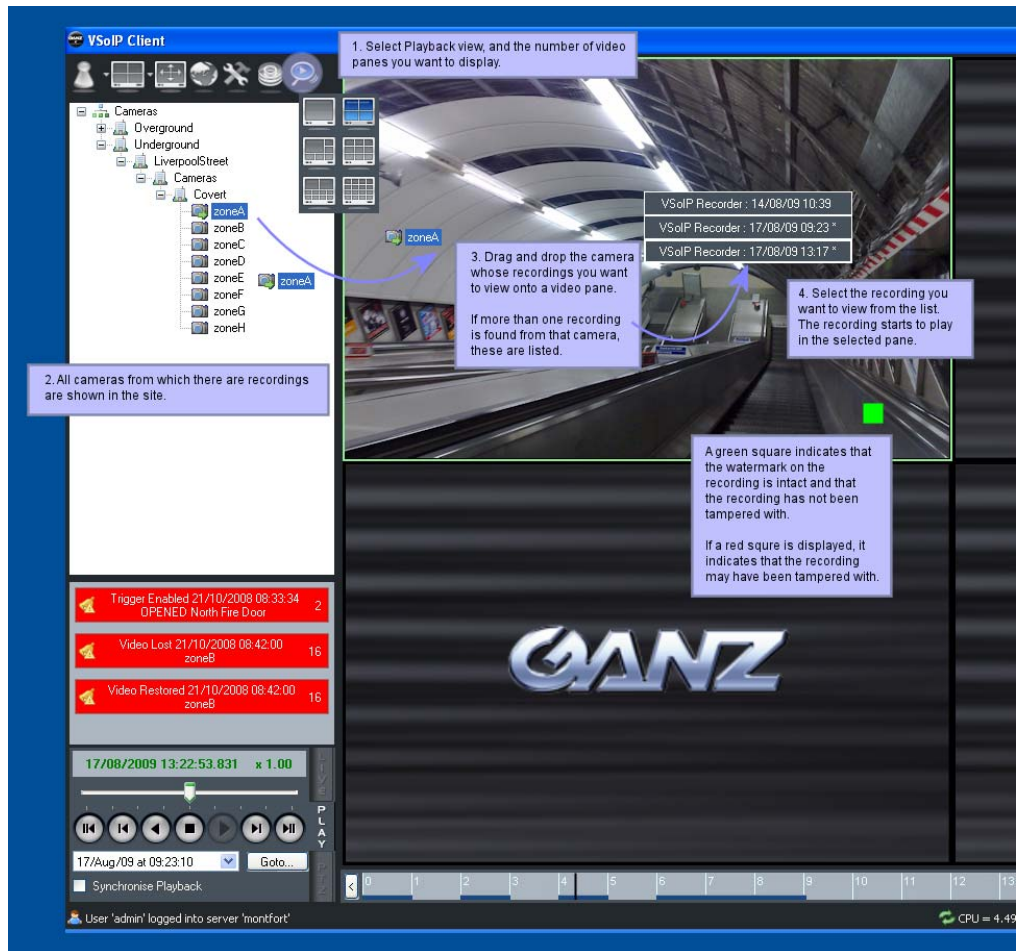
The screenshot shows the VSoIP Client interface with the following components and annotations:

- Left Tree View:** Shows a hierarchy of cameras and recorders. Annotations indicate that selecting a camera or group of cameras (e.g., "Underground") filters the recordings displayed.
- Main Table:** Displays a list of recordings with columns: Camera Name, Camera Location, Start Time, End Time, Recorder Name, and Recorder Location. A "Query Complete" status is shown at the bottom of the table.
- Events Pane:** Lists events associated with the selected recording, including Event Category, Event Type, Time, and Username. Annotations explain that this pane shows all events associated with the selected recording.
- Bottom Controls:** Includes buttons for "Delete Recording", "Stop Recording", and "Backup". Annotations explain how to delete a finished recording and how to stop a recording.

**Figure 40** 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.



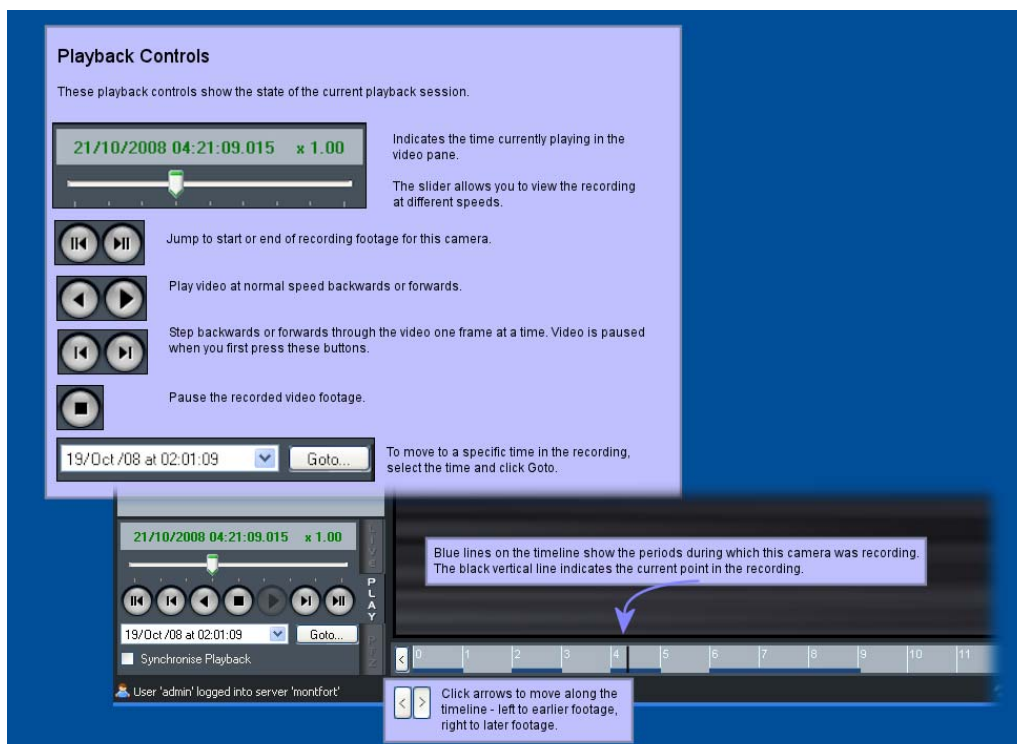
**Figure 41** Initial playback and reviewing footage

**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-forward, step-back. Also, the current position is indicated as a date and time.

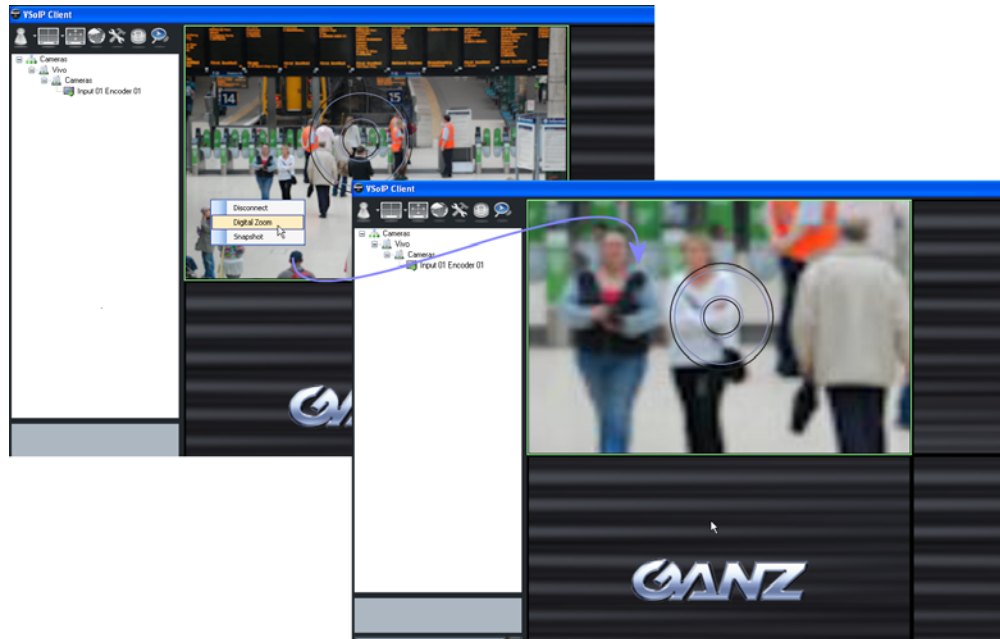
**Note:** Not all recorders can perform every playback control, e.g. step-back. If an operation is not possible, the request to perform it is ignored.



**Figure 42** Controlling playback

## Using Digital Zoom

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



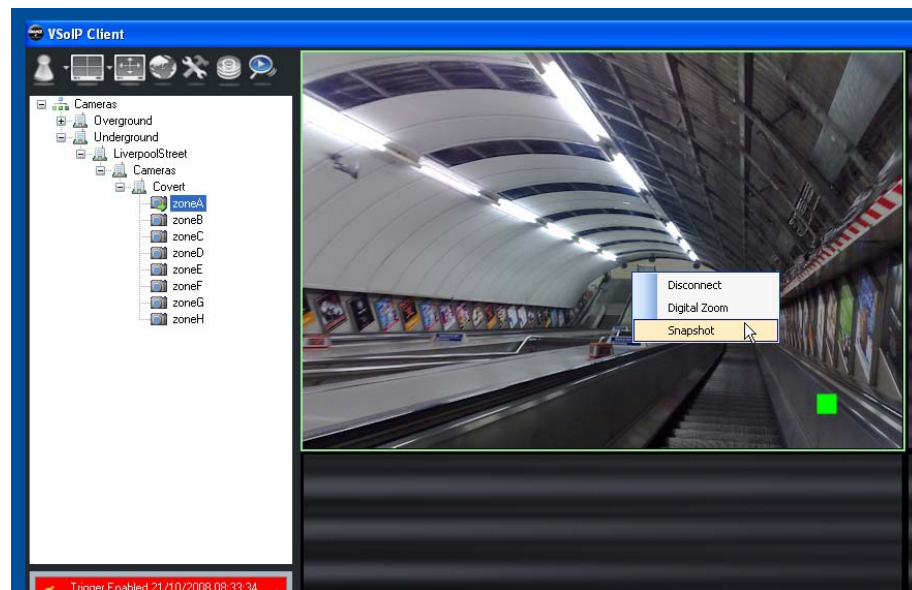
**Figure 43** Zooming into recorded video

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 Pro 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 change this location, see “Changing Client Settings” on page 85.

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

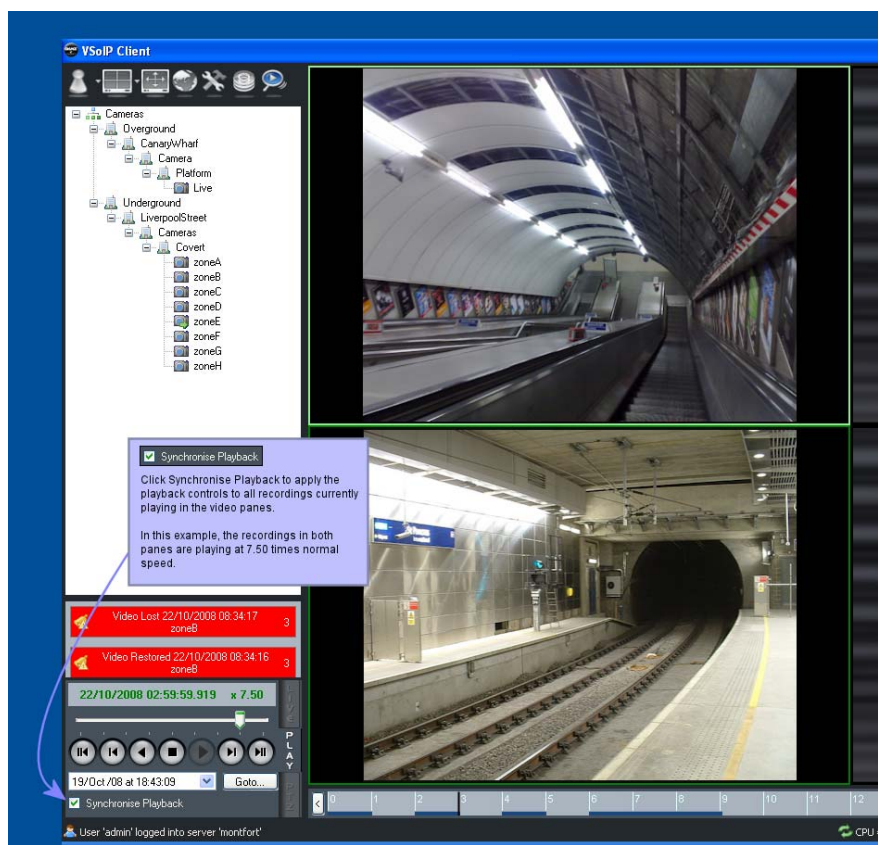


**Figure 44** Taking a snapshot of recorded video



## 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 45** Synchronised playback

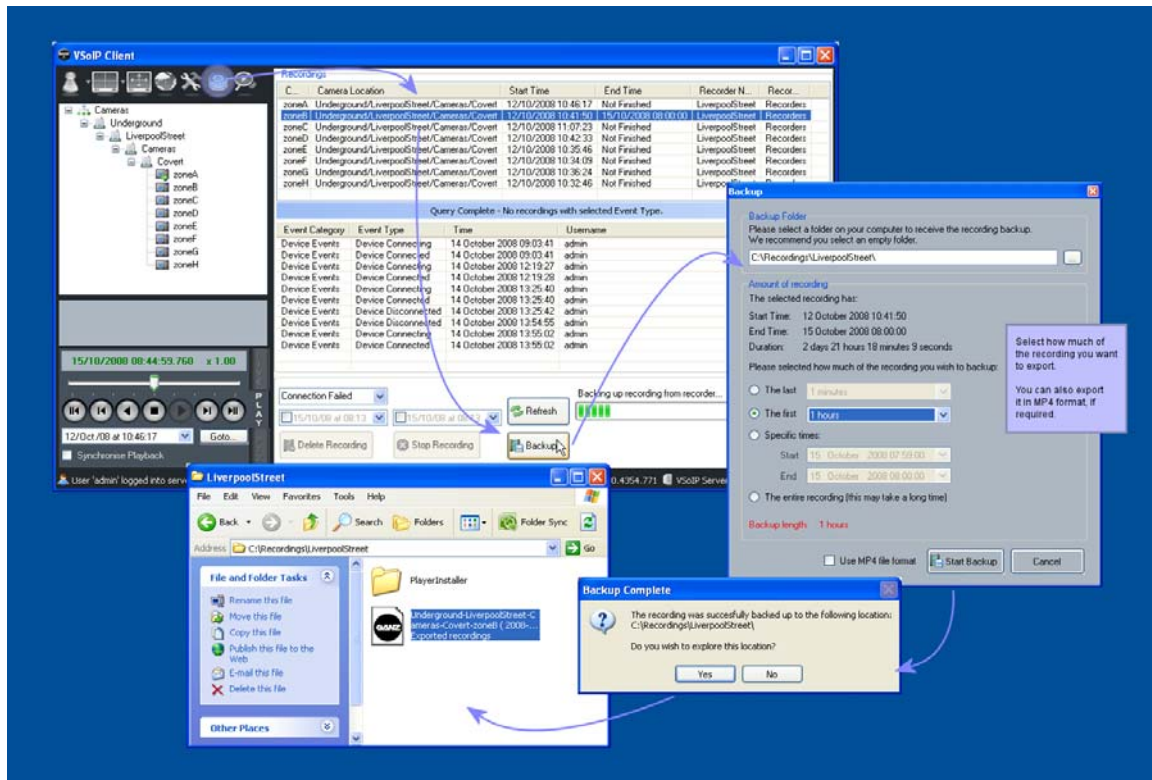
**Note:** Networked DVRs can vary in their performance. Some Networked DVRs are limited to a certain number of concurrent playback sessions. The performance of the application during synchronised playback will reflect the responsiveness and performance of the poorest responding and performing element.

## Exporting Recorded Video

For evidential purposes, it is often necessary to extract a portion of recorded footage for playback in a player application. This permits recorded footage to be viewed without requiring a Client to be connected via a Server to a recorder – instead a simpler reproduction system is used, e.g. a standalone laptop.

Locate your recording in the list of recordings of IP cameras and camera inputs on Networked DVRs.

Figure 46 shows the steps required to export recording footage.



**Figure 46** 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 the Client is instructed to export recordings in native format, the Client 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 "package" for use by individuals without access to the Clients, Server and the Networked DVRs and NVRs of the surveillance system.

**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.

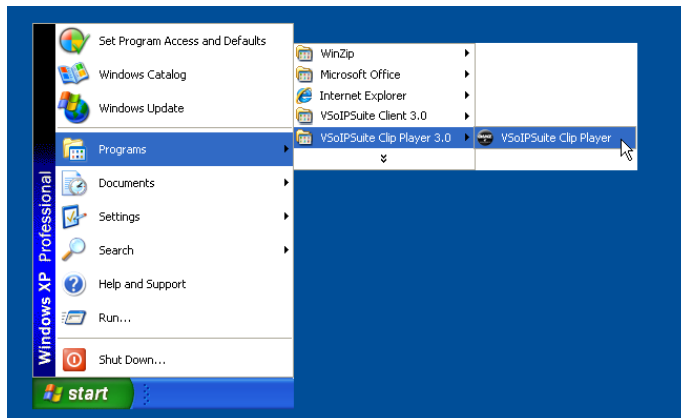
## Installing the Player

- 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

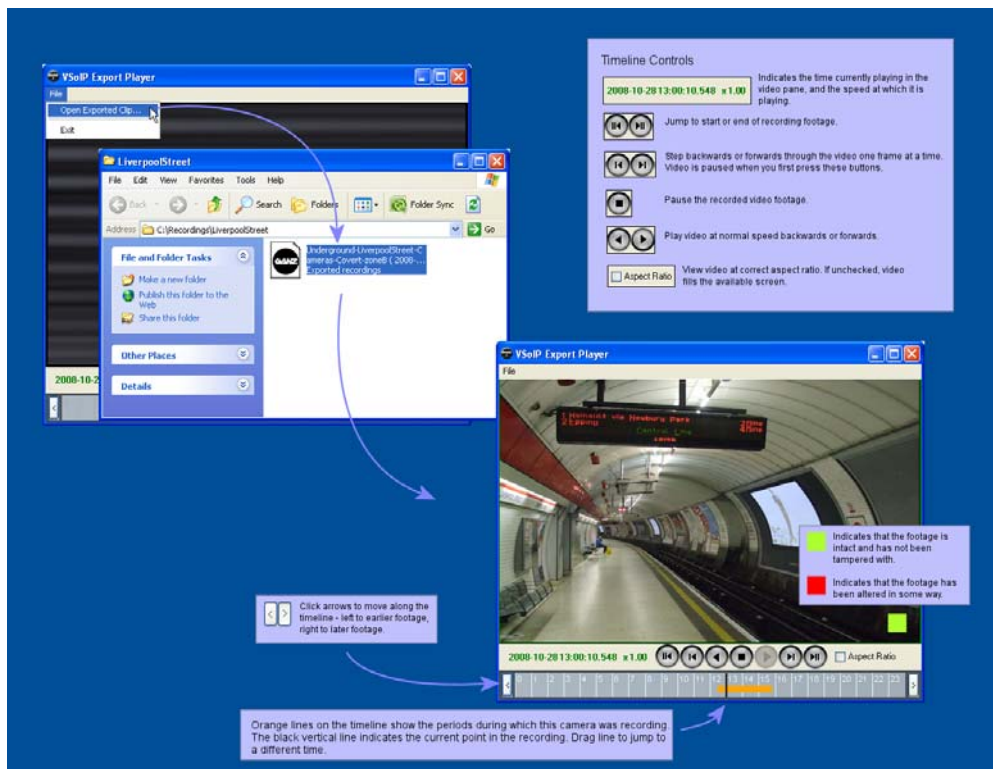
Open Windows Start menu and choose the Player shortcut to start the Player.



**Figure 47** 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 48** Playback components

## Audit Trail Configuration

The audit trail provides a comprehensive list of events that have occurred since the Server component was installed. Some examples of event information are:

- Alarms (acknowledgement, closed).
- Users (added, deleted, edited etc.).
- Devices (added, updated, deleted, disconnected etc.).
- Recording (disk space low or critical).

This list is not comprehensive – many other types of event are also monitored.

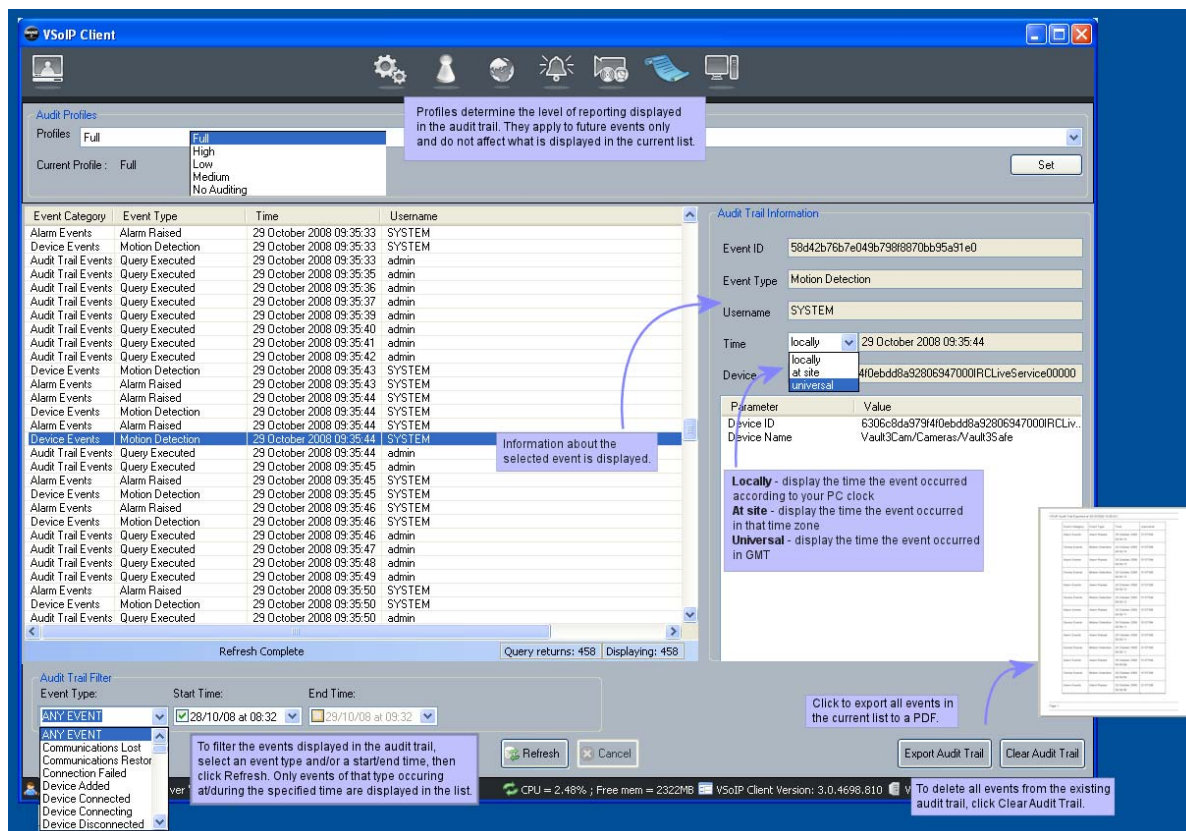


Figure 49 The audit trail

## Audit Trail Profiles

By default, the audit trail lists all events that have occurred since Server installation. Some of these events may be of more interest to you than others. *Profiles* allow you to specify which events you want to display in the audit trail.

There are five audit trail profiles — full, high, low, medium and No Auditing. The default settings are as follows:

**Table 4** Default Audit Trail settings

• Low	<ul style="list-style-type: none"><li>• Server Started</li><li>• Server Shutdown</li><li>• Service Hosted</li><li>• Service Shutdown</li><li>• User Login</li><li>• User Logout</li><li>• Security Failure</li><li>• Session Timeout</li></ul>	<ul style="list-style-type: none"><li>• Alarm Raised</li><li>• Alarm Acknowledged</li><li>• Alarm Closed</li><li>• Alarms To Raise Changed</li><li>• Device Connected</li><li>• Device Disconnected</li><li>• Video Lost</li><li>• Video Restored</li></ul>
• Medium - all of the above, plus:	<ul style="list-style-type: none"><li>• User Added</li><li>• User Deleted</li><li>• Group Added</li><li>• Group Deleted</li></ul>	<ul style="list-style-type: none"><li>• Device Added</li><li>• Device Removed</li><li>• Mapset Added</li><li>• Mapset Deleted</li></ul>
• High - all of the above, plus:	<ul style="list-style-type: none"><li>• Group Members Changed</li><li>• Group Updated</li><li>• User Updated</li></ul>	<ul style="list-style-type: none"><li>• Connection Failed</li><li>• Device Connecting</li><li>• Mapset Updated</li></ul>
• Full	All of the above	

# Chapter 6 – Mapsets

This chapter contains information on the following:

- Mapset Overview
- Designing Mapsets
- Creating a Mapset without a Map Design Tool

## Mapset Overview

A mapset is similar to a mini-website; it is a collection of interconnected pages or “maps” that contain links to various surveillance system components. Similar to the Web, mapsets can contain a mix of text and graphic parts.

Mapsets are often used as an alternative view to the hierarchical, branched tree representation of system components observed in the Client.

Mapsets are an opportunity to present the site in a manner familiar to the operators of the system. For example a member of a CCTV operator's group might have access to a mapset or a series of mapsets showing the physical layout of the site they are monitoring, i.e. it contains a graphical site-map, a site plan showing various named buildings and floor plans of the various buildings. These various parts are most likely to be shown over several interconnected pages. Links between pages could be specially marked areas over the buildings, the floor plan etc. Alternatively a mapset for an installer might be a series of system wiring diagrams allowing the engineer to troubleshoot device issues without the need to understand the physical location of a devices.

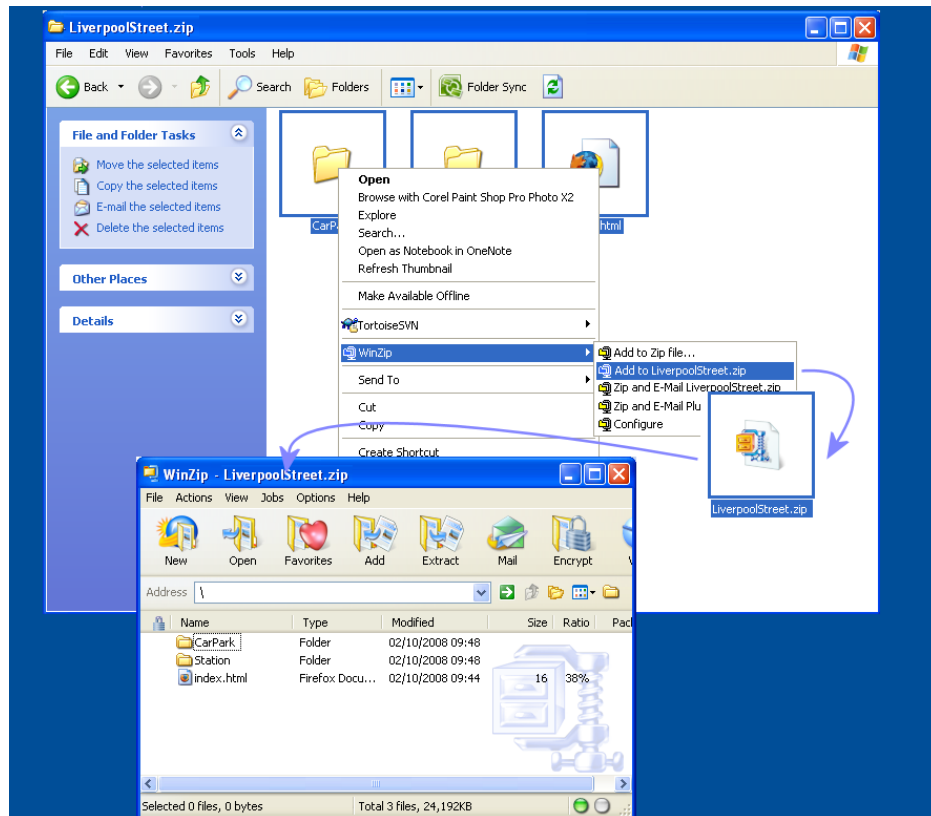
The similarity between mapsets and websites can also be seen by viewing the pages making up a mapset in a text editor, are seen as a series of pages containing textual content formatted and following the rules of XHTML as managed and publicised by the World Wide Web Consortium.

For more details and on-line tutorials about creating XHTML documents valid as Mapsets please visit the World Wide Web Consortium's website and compare the details there with the sample Mapsets installed alongside the Client in the Client's installation folder.

[World Wide Web Consortium XHTML \(http://www.w3.org/TR/xhtml1/\)](http://www.w3.org/TR/xhtml1/)

The Server requires that the individual pages that constitute a single mapset are collected together in a single file. This file is an archive generated by any archive generating tool that can produce ZIP format files.

The structure of the archived file system, e.g. the files and folders that are contained in the ZIP archive, is flexible, however each archive MUST contain a single file called index.html at the top-level of the archived folder hierarchy, as shown below.



**Figure 50** Before and after - mapset creation

## Designing Mapsets

Consider the purpose of the mapset:

- Is the mapset for CCTV operators, or for maintenance personnel? This drives the style of the content.
- Is a single page enough, or will multiple pages be required?
- Is the size of each page background image suitable for the PC display resolution in use by the Clients? Large images could be broken into smaller images and become backgrounds on interconnected pages.
- Do you have a list of the devices that should be present on the map?
- Are the images in a format suitable for inclusion on a page? Images should be in .GIF, .JPG or .PNG format.

Ideally, a mapset design tool should be used to create the mapset. However, you can also create mapsets manually using Windows Notepad, as explained below.

## Creating a Mapset without a Map Design Tool

A mapset is a set of one or more map pages that provide the user with an alternative method of using the surveillance system.

If the system installer, administrative level user, or user with mapset addition privileges plans to create a mapset and they do not have access to a map design tool for the surveillance system, they can create mapsets using:

- **Windows Notepad** — The Windows notepad application has sufficient capabilities to create and maintain map pages. This is accessed from the Start menu>All Programs>Accessories>Notepad.

- File Compression Utility — This is used to collect map pages and, optionally, graphical content, into a single archive file. This is also known as a compressed folder. A compressing application is built in to the operating system but if preferred third-party, standalone applications such as WinZIP or WinRAR can be used.
- Graphical editor (optional) — This is useful for creating the page background. Editors that show the position of the mouse relative to the upper-left corner of a loaded image are useful when calculating positions for map graphics such as camera or alarm icons.
- Internet Explorer (optional) — This is useful for accessing services such as those for Globally Unique Identifier (GUID) generation, for example <http://guidgen.com>.
- GUID generator application (optional) — Several third party GUID generator applications can be downloaded from the Internet. Since links always change none is included here - perform an Internet search to find a suitable application.

It is within the means of most engineer grade personnel to use these instructions along with some study of basic web-page construction to create powerful and useful mapsets. This section cannot however teach all that is required to create XHTML pages. This section is written as a guide to those already familiar with HTML and web page construction. It is recommended that some study of web-page design using HTML is carried out for those who are not familiar.

## Typical Workflow

The mapset creator decides on the layout of the mapset, or mapsets that will be used. A mapset itself is a collection of one, or more map pages. The user navigates a mapset entering at the home page, which has file name `index.htm`, and jumps to other map pages using anchor links added to a map page.

When designing mapsets, you should consider the following:

- Always have a page link from any page back to the home page of the mapset.
- Adding *previous* and *next* map history links can allow for quick navigation.
- You can aid navigation by adding page links to other map pages to the home page.

For example, if you have a mapset with a home page and pages called:

- floor 1
- floor 2
- roof
- basement

You may find navigation easier if you add links to floor 1, floor 2, roof, basement to the home page rather than adding links to floor 1 and basement to the home page, but links to floor 2 on the floor 1 map page, and to roof on floor 2 map page.

- Use map-page background images to add detailed content, but always size these to match the screen area (in pixels) of the map window shown by the PCs running the surveillance client used to view map pages. For example, the client PC has a 1280 x 1024 pixel monitor, but the area most likely to be used for map display on that monitor will typically be 640x480 pixels, with other video, and client application user interface taking up the remaining area. Thus, making background images 640 x 480 will mean that users will not need to scroll left and right, or up and down, to see the map content.
- Split content rich, dimensionally large backgrounds images down into several dimensionally smaller background images. Use these dimensionally smaller images as the background on several interconnected map pages with page links connecting adjacent pieces of the divided background. This is better than scaling a dimensionally large image smaller with the resultant lack of detail and clarity.
- Ensure that images are 72dpi and not higher, since higher dpi will not necessarily improve map background clarity, but will unnecessarily add to the system memory consumed on surveillance clients and possibly slow down client log-in and mapset page loading performance.

The following workflow is suggested:

- 1 Make a list of all the map pages that will be needed.
- 2 Obtain background images for each, scaling or sub-dividing as necessary.

- 3 Consider which map page will be the home page.
- 4 Obtain suitable images for camera icons and alarm icons as required.
- 5 Calculate the coordinates relative to top-left of background image where camera and alarm icons should be placed.
- 6 Using the notepad application, create a placeholder page for each map required using the standard map page content shown below, saving the map chosen as the home map as index.htm and the others with memorable names related to the custom map page content to be added. All text files saved by the Notepad application should be in the same folder and all have the file extension .htm.

## Placeholder Map Page

The placeholder map page is a text file, saved with .htm extension, containing the bare minimum content to be a valid map page. The page will not display any content if added to a mapset but contains all mandatory elements required to be uploaded to the surveillance suite server and to be displayed by surveillance suite clients.

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <title>PLACEHOLDER PAGE CHANGE ME</title>
    <meta http-equiv="content-type" content="text/html; charset=utf-8" />
  </head>
  <body style="background-color:#ffffff">
    <div style="position:absolute;height:97%;width:97%">
      <div
        style="margin-left:-320px; margin-top:-240px;position:relative;
          left:50%;top:50%;">
        
      </div>
    </div>
  </body>
</html>
```

The page placeholder assumes that a background image called VgaBackgroundImage.png has been created and placed in the same folder as this file. Notice that there are width and height style attributes that match the size of the VgaBackground.png image i.e. 640 pixels wide by 480 pixels high.

Importantly notice also immediately prior to the <img /> XHTML tag that describes the VgaBackground.png image, there is a <div> tag which has a style attribute detailing a left and top margin. This is half the size of the height and width of the background image.

When changing the background image to another image make sure that you change the value representing the background images filename src="VgaBackgroundImage.png" to the appropriate name of the background image. Also change the value of the height and width style attributes to match that of the new image. Finally change the left and top margin style attribute values to a half of the height and width of the image.

---

**Caution:** The margin-left and margin-top <div> tag's style attribute values should be negative values. Only change the number part of these values and leave the sign unchanged.

---

## Page Links - Textual

A page link causes the map page to switch to the new page described by the link. The XHTML content to do this is known as the anchor, or <a></a>, tag.

To link from a map page to the home page, the following XHTML statement can be placed within the <body></body> content of that map page.

```
<a href="index.htm">Home page</a>
```

**Note:** The anchor (or page link) tag cannot appear between <object> and </object> tags.



To link from a page to another page, the following XHTML statement can be placed using the same rules listed above.

```
<a href="floor1.htm">Go to floor ONE</a>
```

## Camera Links - Graphical

A camera link is a graphical object on a map that is used to show an alternative view of the IP cameras, DVR inputs, and encoders described in the surveillance site. A user can interact with the camera link to perform operations on the IP camera or encoder associated with the link, typically this would be to view video from the camera.

A camera link has the following attributes:

- Name (required) — A short but descriptive name for the camera. The name should not start with a number, should contain only letters or numbers and cannot include spaces.
- Description (optional) — A longer descriptive name for the camera. The name should contain only letters, numbers and spaces.
- Camera image (required) — A 256 colours, or greater, JPEG or PNG format graphic of 48x48 pixels in width and height.
- Map position (required) — The coordinates on the map background where the upper-left hand corner of the camera link image should appear.

The x-coordinate starts at 0 at the extreme left of the background and counts up one unit at time until the maximum value which is near the extreme right of the background image. This maximum is the width of the background graphic in pixels minus the width of the camera image.

The y-coordinate starts at 0 at the extreme top of the background and counts up one unit at time until the maximum value which is near the extreme bottom of the background image. This maximum is the height of the background graphic in pixels minus the height of the camera image.

- Unique element ID (required) — A precisely formatted identifier called a Globally Unique Identifier, or GUID.

The user of the map sees only the following attributes:

- Camera image.
- Position — the image appears on map at the position specified.
- Dimensions — the image is scaled to the size given.

**Note:** For a user to interact with the camera images, the user must have permissions to view the camera associated with the camera link. If the user does not have permission, they will always see the camera image irrespective of whether they are permitted to interact with that camera.

The administrator of the system sees only the camera link name attribute during mapset configuration. The administrator uses the names of IP cameras, encoders and DVR inputs and the names of the camera links to associate the cameras with the camera links.

### Defining a Graphical Camera Link

Adding a camera link to a map page is similar to the process of defining an alarm link. Camera links make use of an XHTML expression all contained within an Object tag.

```

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <title>Camera link example</title>
    <meta http-equiv="content-type" content="text/html; charset=utf-8" />
  </head>
  <body style="background-color:#ffffff">
    <div style="position:absolute;height:97%;width:97%">
      <div
        style="margin-left:-320px; margin-top:-240px;position:relative;
          left:50%;top:50%;">
        
        <object title="Upper left corner VGA sized map"
          style="left: 0px; position: absolute; top: 0px;"
          id="4300bcd547364605977dad65db231504"
          classid="RapidCCTV.MapControls.dll#RapidSDK.CCTV.MapControls.RCMapCamera"
          width="48" height="48">
          <param name="ObjectID" value="CameraUpperLeft" />
          <param name="ImageUrl" value="TopLeft.png" />
          <img
            src=""
            title="Upper left corner VGA sized map"
            alt="Upper left corner VGA sized map" />
        </object>
        <object title="Upper right corner VGA sized map"
          style="left: 599px; position: absolute; top: 0px;"
          id="bfe3c1fcabl64b2ca8e38a8165e7c6d0"
          classid="RapidCCTV.MapControls.dll#RapidSDK.CCTV.MapControls.RCMapCamera"
          width="48" height="48">
          <param name="ObjectID" value="CameraUpperRight" />
          <param name="ImageUrl" value="TopRight.png" />
          <img
            src=""
            title="Upper right corner VGA sized map"
            alt="Upper right corner VGA sized map" />
        </object>
        <object title="Lower left corner VGA sized map"
          style="left: 0px; position: absolute; top: 439px;"
          id="6d6156b22f2d4ba6b7653e1f6a8597f2"
          classid="RapidCCTV.MapControls.dll#RapidSDK.CCTV.MapControls.RCMapCamera"
          width="48" height="48">
          <param name="ObjectID" value="CameraLowerLeft" />
          <param name="ImageUrl" value="LowerLeft.png" />
          <img
            src=""
            title="Lower left corner VGA sized map"
            alt="Lower left corner VGA sized map" />
        </object>
        <object title="Lower right corner VGA sized map"
          style="left: 599px; position: absolute; top: 439px;"
          id="62781b4a4f8c40438c933b5db3566391"
          classid="RapidCCTV.MapControls.dll#RapidSDK.CCTV.MapControls.RCMapCamera"
          width="48" height="48">
          <param name="ObjectID" value="CameraLowerRight" />
          <param name="ImageUrl" value="LowerRight.png" />
          <img
            src=""
            title="Lower right corner VGA sized map"
            alt="Lower right corner VGA sized map" />
        </object>
      </div>
    </div>
  </body>
</html>

```

The content shown above is an example of a complete map page. It was created in Windows Notepad. In this example the map page is the file index.htm, The name is relevant here as index.htm is the "entry point" or home page of a mapset.

Ordinarily this file, along with other map pages and images would be held in a single zip archive file, renamed to have a .mapset filename so that it could be loaded into the surveillance suite.

Study the content shown above. The content shown outside the sections bounded by the <object> and </object> XHTML tags is common to all map pages. Typically the text between the <title> and </title> XHTML tags is changed to suit the purpose of each map page, e.g. Ground Floor, Car-park, Lobby etc.

On map pages, a pair of object tags, <object></object> surrounds each camera link. Each object has the following attributes:

- Title — A longer descriptive name for the camera. The name should contain only letters, numbers and spaces.
- Position — An offset from the left and an offset from the top of the map page in pixels.
- Width — The maximum width in pixels of the camera image.
- Height — The maximum height in pixels of the camera image.
- Id — A system wide unique GUID for this camera link as generated from a GUID generator service like <http://guidgen.com> or from a GUID generating application.

**Note:** The GUID must only contain letters and numbers. Any hyphen characters should be removed.

- classid — Must be set to  
`RapidCCTV.MapControls.dll#RapidSDK.CCTV.MapControls.RCMapCamera.`
- ObjectID — The name of the camera link: a short but descriptive name for the camera. The name should not start with a number, should contain only letters or numbers and cannot include spaces.
- ImageUrl — The filename of a .PNG or .JPG graphic representing the camera. The filename must include a file path relative to the folder containing the map file.

Notice that the textual content associated with the title attribute is repeated in the <img /> tag as values for the img tag's "title" and "alt" attributes.

**Note:** This section contains details of adding camera links to a map page. There is additional page content that is not shown in this subsection that describes page artwork and region, text and alarm links. Also, the process of adding the created page to a zip archive so it becomes a part of a mapset is not described here.

---

**Caution:** The `RapidCCTV.MapControls.dll#RapidSDK.CCTV.MapControls.RCMapCamera` classid must be used whenever an object is to be associated with a camera link.

---

## Alarm Links

An alarm link is a graphical object on a map that can be used to show the state of an alarm within the surveillance system.

An alarm link has the following attributes:

- Name (required) — a short but descriptive name for the alarm. The name should not start with a number, should contain only letters or numbers and cannot include spaces.
- Description (optional) — a longer descriptive name for the alarm. The name should contain only letters, numbers and spaces.
- Inactive image (required) — A 256 colours, or greater, JPEG or PNG format graphic of 48x48 pixels in width and height.
- Active image (required) — A 256 colours, or greater, JPEG or PNG format graphic of 48x48 pixels in width and height.
- Flash image (required) — A 256 colours, or greater, JPEG or PNG format graphic of 48x48 pixels in width and height.

- Map position (required) — The coordinates on the map background where the upper-left hand corner of the alarm link image should appear.

The x-coordinate starts at 0 at the extreme left of the background and counts up one unit at time until the maximum value which is near the extreme right of the background image. This maximum is the width of the background graphic in pixels minus the width of the alarm image.

The y-coordinate starts at 0 at the extreme top of the background and counts up one unit at time until the maximum value which is near the extreme bottom of the background image. This maximum is the height of the background graphic in pixels minus the height of the alarm image.

- Unique element ID (required) — A precisely formatted identifier called a Globally Unique Identifier, or GUID.

The user of the map sees only the following attributes:

- Inactive image — when the alarm source associated with the alarm is in the acknowledged or closed state.
- Active image — when the alarm source associated with the alarm is in the unacknowledged state - and the flash image is not currently displayed.
- Flash image — when the alarm source associated with the alarm is in the unacknowledged state - and the active image is not currently displayed.
- Position — one of the images appears on map at the position specified.
- Dimension — the images are scaled to the size given

**Note:** For a user to see the active and flash alarm images representing an alarm link, they must have permissions to view alarms for the alarm source associated with the alarm link. If the user does not have permission, they will always see the inactive image irrespective of the state of the alarm within the system.

The administrator of the system sees only the alarm link name attribute during mapset configuration. The administrator uses the names of alarm sources and the names of the alarm link to associate the alarm source to the alarm link.

## Defining an Alarm Link

Adding an alarm link to a map page is similar to the process of defining a camera link. Alarm links make use of an XHTML expression all contained within an Object tag.

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <title>Alarm link example</title>
    <meta http-equiv="content-type" content="text/html; charset=utf-8" />
  </head>
  <body style="background-color:#ffffff">
    <div style="position:absolute;height:97%;width:97%">
      <div
        style="margin-left:-320px; margin-top:-240px; position:relative;
          left:50%;top:50%;">
        <object title="Alarm link example"
          style="left: 320px; position: absolute; top: 240px;"
          id="2abd95e7-3987-4c33-8a4a-daa3a504be3b"
          classid="RapidCCTV.MapControls.dll#RapidSDK.CCTV.MapControls.RCMapAlarm"
          width="48" height="48">
          <param name="ObjectID" value="AlarmNameGoesHere" />
          <param name="ActiveImageUrl" value="alarm_active.PNG" />
          <param name="InactiveImageUrl" value="alarm_inactive.PNG" />
          <param name="ActiveFlashImageUrl" value="alarm_active_flash.PNG" />
          <img src="" title="Alarm link example" alt=" Alarm link example" />
        </object>
      </div>
    </div>
  </body>
</html>
```

The content shown above is an example of a complete map page. It was created in Windows Notepad. In this example the map page is the file index.htm. The name is relevant here as index.htm is the "entry point" or home page of a Mapset.

Ordinarily this file, along with other map pages and images would be held in a single zip archive file, renamed to have a .mapset filename so that it could be loaded into the surveillance suite.

Study the content shown above. The content shown outside of the section bounded by the <object> and </object> XHTML tags is common to all map pages. Typically the text between the <title> and </title> XHTML tags is changed to suit the purpose of each map page, e.g. Ground Floor, Car-park, Lobby etc.

On map pages, a pair of object tags, <object></object> surrounds each alarm link. Each object has the following attributes:

- Title — A longer descriptive name for the alarm. The name should contain only letters, numbers and spaces.
- Position — An offset from the left and an offset from the top of the map page in pixels.
- Width — The maximum width in pixels of the active, active flash and inactive images.
- Height — The maximum height in pixels of the active, active flash and inactive images.
- Id — A system wide unique GUID for this alarm link as generated from a GUID generator service like <http://guidgen.com> or from a GUID generating application.

**Note:** The GUID must only contain letters and numbers. Any hyphen characters should be removed.

- classid — must be set to `RapidCCTV.MapControls.dll#RapidSDK.CCTV.MapControls.RCMapAlarm`
- ObjectID — The Name of the alarm link: a short but descriptive name for the alarm. The name should not start with a number, should contain only letters or numbers and cannot include spaces.
- ActiveImageUrl — The filename of a .PNG or .JPG graphic representing an unacknowledged alarm when it is being shown in the not flashing state. The filename must include a file path relative to the folder containing the map file.
- ActiveFlashImageUrl — The filename of a .PNG or .JPG graphic representing an unacknowledged alarm when it is being shown in the flashing state. The filename must include a file path relative to the folder containing the map file.
- InactiveImageUrl — The filename of a .PNG or .JPG graphic representing an unacknowledged alarm when it is being shown in the not flashing state. The filename must include a file path relative to the folder containing the map file.

Notice that the textual content associated with the title attribute is repeated in the <img /> tag as values for the img tag's "title" and "alt" attributes.

**Note:** This section contains details of adding alarm links to a map page. There is additional page content that not shown in this subsection that describes page artwork and region, text and camera links. Also, the process of adding the created page to a zip archive so it becomes a part of a mapset is not described here.

---

**Caution:** The `RapidCCTV.MapControls.dll#RapidSDK.CCTV.MapControls.RCMapAlarm` classid must be used when an object is to be associated with an alarm link.

---

# Chapter 7 – NVR Component

This chapter contains information on the following:

- Prerequisites
- Before Installing NVR
- Installing the NVR
- Customising the Database
- Using the NVR
- Troubleshooting
- Network Time Server

## NVR Overview

The Networked Video Recorder software component (the “NVR”) is a Microsoft .Net framework based service for Microsoft Windows operating systems. It is designed to record media streams – primarily video feeds – from surveillance resources such as encoders, IP cameras and networked digital video recorders (DVR).

The recording duties of the NVR are controlled by various schedules held in an SQL database. Typically the NVR works alongside a server software component (the “Server”). The Server allows administrative access to the NVR, communicates recording schedules, signals that various events have occurred within the surveillance system and is the authentication authority for client software (Clients) requests for playback sessions, recording export, archiving and deletion.

Initial configuration of the NVR is carried out by editing an XML configuration file using the Windows Notepad application. Day-to-day operational control of the NVR system is via Clients connected to the Server. Communication between Clients and Servers is via .Net remoting. Communication between Clients and Video-walls is via web-services.

The NVR runs using a local system account, either LocalService or NetworkService. These accounts are built-in accounts in Microsoft Windows and do not need to be created.

---

**Caution:** The computer used to run the NVR should not be considered to be a general purpose PC and should not be used for other tasks that might starve the NVR of system resources. It is possible to run a Client and/or a Server on the same computer as the NVR but this can lead to a conflict of resources and as such is discouraged in all but the smallest of systems.

---

## Prerequisites

### Hardware

The following hardware specification provides full frame rate video, without dropped frames, video corruption or latency for 80Mbps throughput (combined recording and normal speed playback).

---

**Caution:** Backing up recordings can put significant load on the recorder particularly where backing up in non-native format is a frequent occurrence. In such cases a safety margin should be factored into the CPU power element of PC specification to accommodate this. Since this margin varies according to the demands of transcoding

the particular attributes of input format, accurate figures are only obtainable by making test back-ups on similar hardware to that proposed and measuring CPU load and scaling this up to the numbers of concurrent non-native back-ups likely to be made.

---

- Processor: 32 bit architecture CPU (e.g Intel Quad Core Processor (or better)) 2.4Ghz.
- Memory: 4096MB.
- Hard Drive/Storage - 500GB SATA Hard Drive (or other very high performance drive).
- Optical Drive — DVDROM (for installation).
- 100 Base-T network card configured for full duplex.
- 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.
- or-
- Windows Server 2003 Standard Edition – service pack 2, or greater, is recommended.

### 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.
- Microsoft SQL Server 2005 Express Edition – service pack 1, or greater, automatically downloaded from Microsoft if not present at install time. Also available as a download from Microsoft's web-site.
- Windows Installer 3.1.

**Note:** Microsoft frequently re-designs its web-sites 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.

### Optional, useful software

Microsoft SQL Server 2005 Management Studio Express – useful for changing various database settings.

## Before Installing NVR

### 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 single local user should be added. This should be a member of the local administrator group. NVR installation, .Net installation and SQL installation, and all maintenance should be done as this local user with local administrative rights.

**Note:** The NVR and SQL database engine run as Windows services and as such will execute irrespective of which user, if any, is logged in to the PC.

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

## Networking — General

Set up the network settings for the PC and make sure that the PC network connection is enabled and connected. Check this by opening a command prompt and running the IPCONFIG Windows command-line utility; for information on how to do this, see Appendix A.

Note the IP address of the NVR PC – in order for the system to make use of the NVR, its IP address must be known.

The PC must be set up so that it can browse the Internet (see notes). Following installation, the NVR will need to contact a licensing server located on the Internet in order to complete the installation and activate.

## Firewall Information

Any local software firewall should either be disabled or carefully configured so as not to prevent the NVR from contacting the licensing server. Also, any hardware firewall on the LAN should be configured to allow appropriate network access to the PC on which the NVR 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.

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

**Table 5** Firewall-related setup data

Application	Role	Default Path	Port number	Note
Setup.exe	NVR installer	installation media	80/TCP	The bootstrap installer for NVR
.MSI file	NVR installer	installation media	80/TCP	The main installer for the NVR
Recorder.LicensingApp.exe	Activation	C:\Program Files\Recorder Service	80/TCP	Required to enable recorder
Recorder.Service.exe	Application	C:\Program Files\Recorder Service	25775/TCP	NVR Service application

More details about port utilisation should be available in documentation supplied with the IP camera or encoder, on the manufacturer's website, or from their technical support contacts.

## Additional Security Software

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

- Anti-virus.
- Anti-spyware.
- Software firewall.

## .Net Framework

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

## Windows 3.1 Installer

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



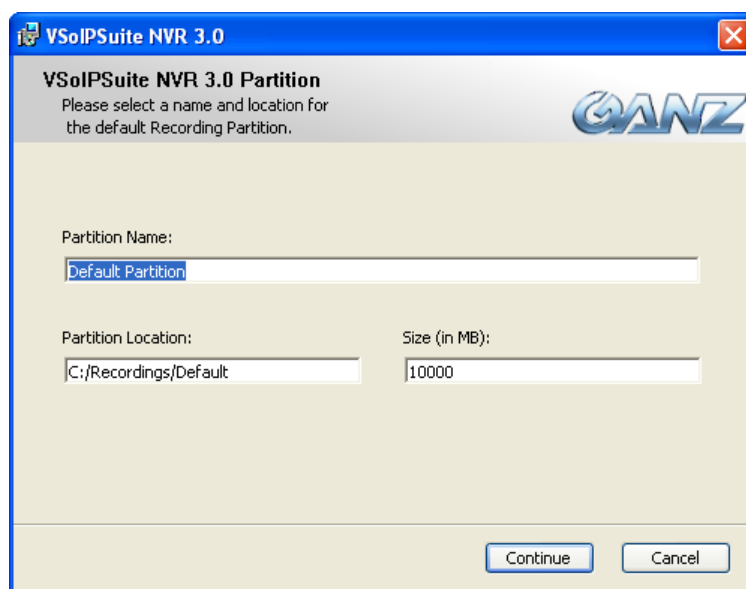
## SQL Server Express Edition

The installation program for the NVR automatically downloads the correct version of the SQL Server Express Edition. However if preferred, install the SQL Server prior to installing the NVR.

Any required configuration of SQL Server Express Edition should occur following the installation of the NVR, and after the point where the databases for the NVR have been created.

## Installing the NVR

- 1 Log in to the computer using the user name of the local user with administrative level privileges.
- 2 The NVR installer program setup.exe automatically examines the local system for the .Net Framework and SQL Server Express Edition. If these are not present, or they are earlier versions, the installer program automatically connects to Microsoft's servers over the Internet and downloads the correct versions of the software.
- 3 Choose the NVR's installation folder, or use the default folder suggested.
- 4 Click Install to begin the installation.
- 5 You are prompted to enter a name and location for the default recording partition. NVR partitions are logical areas of computer storage – reserved areas of a predefined size using an existing, pre-formatted hard-drive partition.



**Figure 51** Specifying a default recording partition

Enter a name for the partition, a location and the space you want to allocate to it.

- 6 The next step makes use of the SQL Server Express Edition database management system:

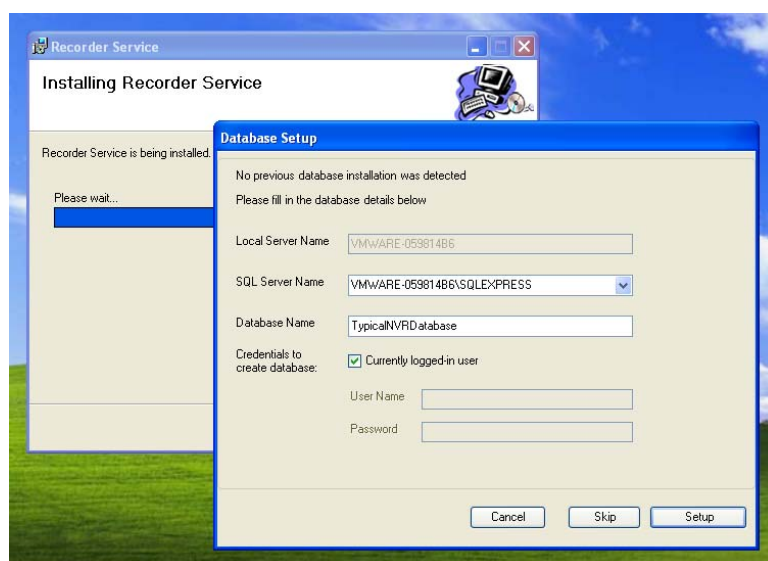
---

**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.

---

- a. Ensure that the SQL Server name includes the local server name, i.e. other SQL servers might be found on the network.
  - b. Give a suitable short meaningful name for the database, or use the one suggested.
  - c. In typical installations, the credentials for the user authorised to create a database will be the currently logged in user. If this is not the case, enter a user name and password that does have these privileges.
- 7 Click Setup to create the database.

**Note:** If this step is skipped then the SQL database server is not used to store data. Instead, a file-based system is used. This should be avoided. It is suited only to demonstration systems where stored data is managed manually.



**Figure 52** Database setup phase

## Customising the Database

Following installation, the database settings can be customised if required using Microsoft's SQL Server Management Studio Express.

## Using the NVR

Prior to using the server you must activate it. Please refer to the section on NVR activation. Before starting the NVR, confirm the following:

- Network connection is available and configured.
- .Net Framework is installed.
- SQL Server Express Edition is installed and the SQL server running.
- SQL database has been created by the Server's installer program.
- Server has been activated.

The NVR runs as a Windows Service. As such it runs irrespective of whether or not a user is logged in to the computer.

**Note:** Using the PC for purposes in addition to running the NVR service might impact on the performance of the NVR.

The NVR can be controlled in one of two ways. Either it can be started and stopped manually, or the NVR can be started and stopped automatically when the operating system starts up and shuts down.

## Starting the NVR Manually

From the Start menu, locate the Recorder Service entry and choose the Start Recorder option. This signals to the NVR that it should start up and run as a background task until the computer is shut down. When restarting the computer, the NVR will not start again unless started through the start menu, as shown in Figure 53.

## Starting the NVR Automatically

From the Start menu, locate the Recorder Service entry and choose the Autostart Recorder option. This signals to the NVR that it should start up and run as a background task until the computer is shut down. When restarting the computer, the NVR will be signalled to start again and to remain running as a background task whenever the computer is running.

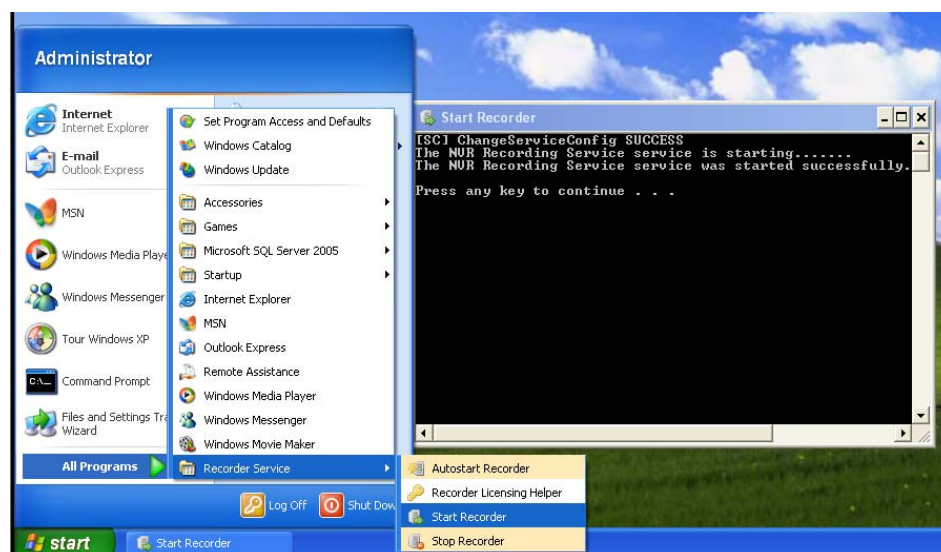


Figure 53 Starting the NVR service

## Stopping the NVR

There may be occasions when you need to shut down the computer whilst the Recording Service is running. Alternatively, you may want to stop just the recording service. The following sections explain how to do both.

### Shutting down the Computer when the Recording Service is Running

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 the storage system is to be removed, the operating system **must** be shut down as follows:

- Log into the computer running the recorder and 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. For more information, please see "Prerequisites" on page 70.

---

**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.

---

---

**Caution:** 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.

---

## Shutting Down the Recording Service

To shut down just the recording service, from the Start menu locate the Recorder Service entry and choose the Stop Recorder option. This signals that the NVR should stop running as soon as possible. If the NVR startup was automatic then automatic start is switched off. The NVR will now only start when the Start menu Start Recorder command is chosen.

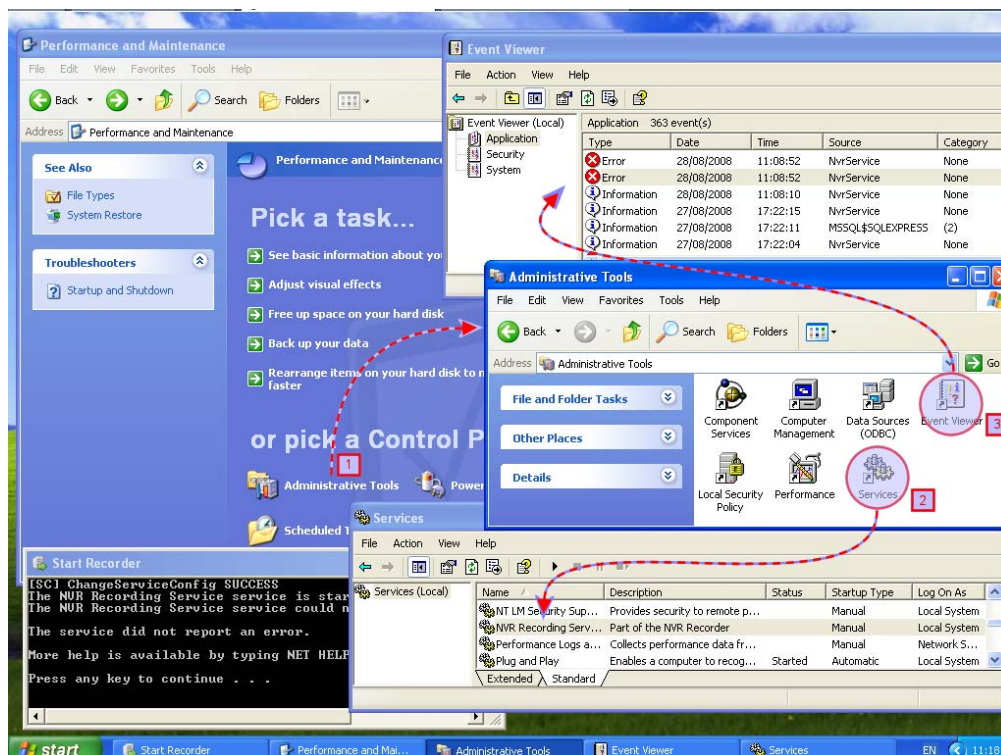
## Troubleshooting

How can I be sure the NVR is running?

The NVR runs as a Windows service — see appendices for more details.

- Using the Windows services listing application, check the status of the NVR Recording Service.
- If the NVR Recording Service is not started then check the Windows Event Viewer application to determine what errors might be preventing startup.

See Figure 54, which demonstrates a common reason for a NVR service not starting – use of an invalid or expired licence.



**Figure 54** Troubleshooting the NVR service using Windows applications

The Recording Service may not start when commanded, or appear to start but not react when a Server or Client tries to use it.

To determine whether a recorder is running:

- 1 Open the Control Panel from the Windows Start Menu, and open up Administrative Tools.
- 2 Open up Services and locate the NVR Recording service. Check that its current status is "Started".
- 3 If not listed as started, start the Event Viewer and open the Application log.
- 4 Double-click on the entries for the NvrService that have an exclamation mark or cross against them to examine the report.

## Expected Performance

### How many IP cameras can I record?

The NVR can record any number of IP cameras and analogue video sources attached to video encoders or Networked DVRs. The Server component within the system contains the list of devices and allows authorised system users to set schedules to start and stop recording.

**Note:** The NVR does not have an enforced upper limit on the number of cameras that it can record simultaneously. Instead the system should be set up so that an NVR is not recording any more than 32 video sources simultaneously.

### How many playback sessions can an NVR stream?

It is recommended that an NVR with hardware specification as given in the section “Hardware” should have no more than 32 streams playing at one time.

**Note:** The system does not enforce an upper limit of playback sessions. To ensure that this limit is enforced, it is recommended that playback rights are used at the Server level to restrict the number of users that can play back video within the system. A rule of thumb can be obtained from calculating the number of playback sessions likely per Client (i.e. the maximum number of video panes that are likely to be switched into playback mode) and multiply this by the number of logged in users with playback rights.

### What overall bandwidth can the NVR process?

There is an overall suggested maximum bandwidth of 60 Megabits per second for the host PC as described in the section “Hardware”.

**Note:** When considering bandwidth utilisation, remember that the proportion of the bandwidth used by a single playback session is the same (plus a slight overhead) as the stream originally recorded.

Fast-winding or rewinding recordings can use bandwidth several times higher than normal speed playback.

Recording export is an additional bandwidth consumer.

Always consider the recording, playback and export loads when deciding whether your system requires several NVRs to accommodate the recording and playback demands of your site.

Do not attempt to run the NVR beyond 60 megabits per second. Doing so might result in poor playback performance, late alarm triggered recording, and other unspecified performance issues.

## Network Time Server

It is **extremely important** that all PCs running the Client software and other devices use a coordinated time service.

One unified time source must be used. If this coordinated time is provided by the Windows Domain server, then ensure that the source used by the Domain is the same one used for all networked video devices.

If using a Windows Domain controller as a time source, ensure that the Windows Time service is set to automatic start-up.

# Chapter 8 – NVR Activation and Licensing

This chapter contains information on activating and licensing the NVR.

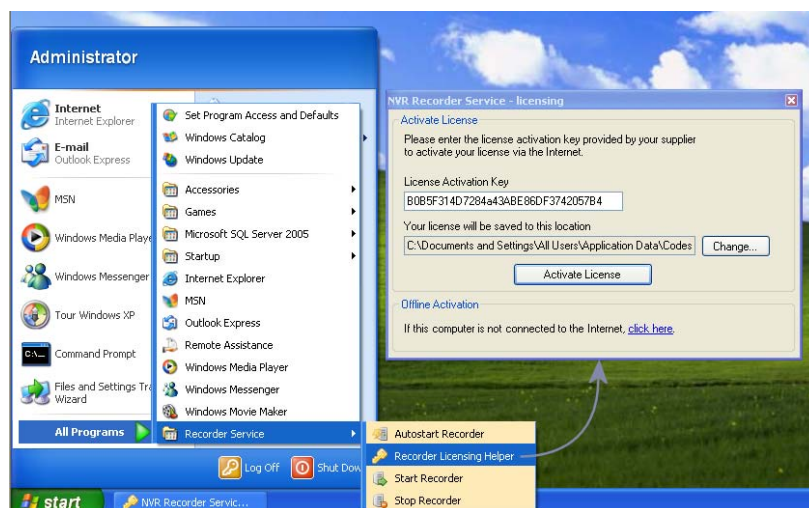
## Activating the NVR

Prior to use, the NVR must be activated. Activation is performed over the Internet and requires an activation ID. Activation is a one-time process. Once activated, a NVR does not need reactivating.

**Note:** Activation IDs are tied to various products even though they look very similar. Please be sure that you use a NVR activation ID rather than a Client or Server activation ID.

Once an activation ID is used it is tied to the identity of the computer used to activate it. If for some reason the licence file generated by activation is lost, then the ID originally used to license the NVR can be reused to re-activate the NVR.

To activate the NVR, locate the Recording Service component in the Windows Start menu, and start the licensing application. Enter the activation ID and commit this. Activation can take a few seconds. Activation success, or failure, will be indicated.



**Figure 55** First-time activation of recording service (NVR)

If activation fails, please check the following:

- Have you used the correct Activation ID?
- Has the Activation ID already been used by a different PC?
- Have there been too many hardware changes to the computer?
- Have you turned off the CPU ID feature of your PC or are using hardware identity masking software? If there are insufficient identifying characteristics, then the licensing server cannot license your PC.
- Are you using machine virtualisation software such as VirtualPC or VMWare? You must use native hardware rather than virtualised hardware.
- Could something be preventing an Internet connection – e.g. firewall block?
- Could the activation server be busy? Wait a while and try again.
- Do you have sufficient account rights to write licence file to local hard disk? Ensure you are attempting to license the Client using an account with administrator level privileges.
- If you are in a geographical region where several calendar types are used, have you set your regional Date/Time setting to use the Gregorian calendar?

# Chapter 9 – NVR Configuration

This chapter contains information on the following:

- NVR Recording Schedules
- NVR Alarm-Triggered Recording

## NVR Recording Schedules

The Networked Video Recorder records streams from IP cameras, encoders and Networked DVRs according to recording schedules created by a Server.

### Recording Schedules

A recording schedule is a set of rules which specify when footage from a video source should be recorded. A schedule may specify continuous recording (24/7), alarm-based recording, or time-scheduled recording. You set up recording schedules using your Client application. Each recording schedule within the system describes:

- One video source (IP camera, encoder or Networked DVR) to be recorded.
- When the video source should be recorded, for example, by using schedules to decide when to record.
- When older recordings made by this schedule should be removed, for example, by the type of partition used, or by looping.

Once a schedule has been created, the NVR is wholly responsible for controlling the schedule. This means that if the Server becomes unavailable on the network, the NVR still performs scheduled recordings.

**Note:** This only applies to continuous recording. If complex alarms are used then the Server must be on-line to process the complex alarm logic and command the NVR to start and stop recording.

To create a recording schedule, you must have added at least one NVR to your surveillance site. For information on how to do this, see "Adding Devices" on page 35.

### Creating a Recording Schedule

Aside from which video source to record and when, a schedule also describes whether the NVR should automatically remove older recordings or whether this is carried out manually by a user with privileges to delete recordings.

A looped recording schedule deletes older recording footage automatically when that footage reaches a certain age.

It is possible to create multiple recording schedules for the same video source, however if the schedules for these schedules overlap then there will be multiple concurrent recordings for that camera. If the overlap is large then this can be wasteful of recording storage space and for that reason is discouraged.

---

**Caution:** Recording schedules can only be created by users with appropriate privileges.

---

### Alarm Types

An NVR schedule can be configured to record the video source continuously (24/7), or when some "alarm" condition occurs.

The alarm condition that dictates when recording occurs is described by the alarm logic of one or more complex alarms.

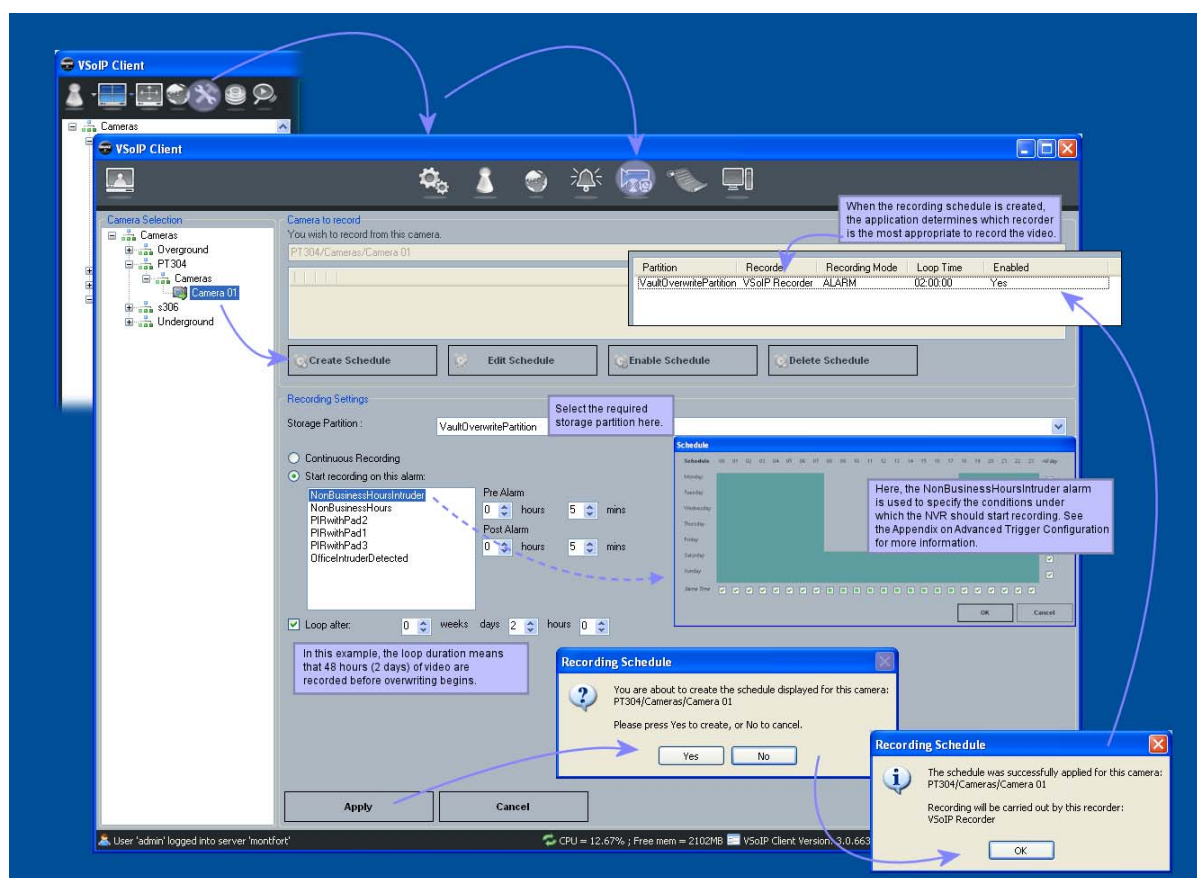


If a recording schedule is based on more than one simple alarm, then recording occurs when any of the alarm triggers are active. Under such situations a single recording is made by the NVR for the length of time any of the alarms are active.

**Note:** The same complex alarms can be used to control several recording schedules. Complex alarms allow various different simple alarms within the system to be combined along with time schedules to provide such complex alarms such as:

- Every weekend
- Mon, Tues, Thurs when motion detected from a chosen number of cameras
- Video-loss on camera 1 causes recording on cameras 2,3,9

See Appendix D for more information regarding the creation of complex alarms. See “NVR Alarm-Triggered Recording” for more details about pre- and post- alarm recording.



**Figure 56** Creating a recording schedule

## Editing Recording Schedules

An existing recording schedule can be edited to use an alternative set of rules about when to record, e.g. a different schedule, switching on or off the looping functionality, or changing the loop duration. If the recording schedule for that video source is no longer required then the recording schedule can be deleted or disabled.

It is not possible to change the partition used for a recording schedule once you have created it or to have two schedules record to the same partition — however, you can create a new recording schedule for the same video source, and select a different partition.

**Note:** It is not possible to change the video source of a recording schedule. However it is possible to have many schedules that record video from the same source.



## Disabling/Deleting Recording Schedules

You may want to temporarily disable a recording schedule, for example, if the partition onto which a schedule is recording is becoming full, and you want to manually delete some recordings to free up space. To do this, select the required schedule and click Disable Schedule. To enable it again, click Enable Schedule.

**Note:** Disabling a schedule does not affect existing recordings associated with this schedule.

You can also permanently delete a recording schedule if it is no longer required. (Remember that you can edit a schedule to use different recording criteria, for example, time schedule or looping policy.)

---

**Caution:** Deleting a recording schedule permanently deletes all recordings in the partition associated with that schedule.

---

To delete a recording schedule, select the required schedule from the list and click Delete Schedule. VSoIP Pro alerts you that all recordings in the partition associated with that schedule will be deleted too. Click OK. The recording schedule is no longer displayed.

## NVR Alarm-Triggered Recording

NVR alarm-triggered recording causes the NVR to record when one or more triggers are fired.

### How does alarm-based recording work?

#### Pre- and Post-Alarm Buffers

So that the recording of the event that caused the alarm to trigger is not missed, the recorder constantly records the video source defined in the schedule at the times given by the schedule. To manage storage overheads, the recorder makes a short looped recording. The duration of this looped recording is known as the *pre-alarm* time. This is the duration of footage that would be preserved and made available as a pre-alarm recording if the trigger fired.

If no alarm is triggered then older footage in the loop is discarded. However, when the associated trigger fires, the recorder automatically preserves the footage and records for a period known as the *post-alarm* time. The resultant footage, pre-alarm footage and post-alarm footage are then made available as event triggered footage.

If the trigger is fired again before the post-alarm duration of the initial triggering expires, then the elapsed part of the post-alarm is reset, causing the recorder to continue recording and resulting in an extended piece of event triggered footage.

**Note:** Recording footage made in this manner is not automatically deleted. The footage must be deleted by a user with appropriate privileges.

Setting up an alarm-based recording is similar to setting up a continuous recording schedule but with additional steps of specifying one or more complex alarms used to trigger recording.

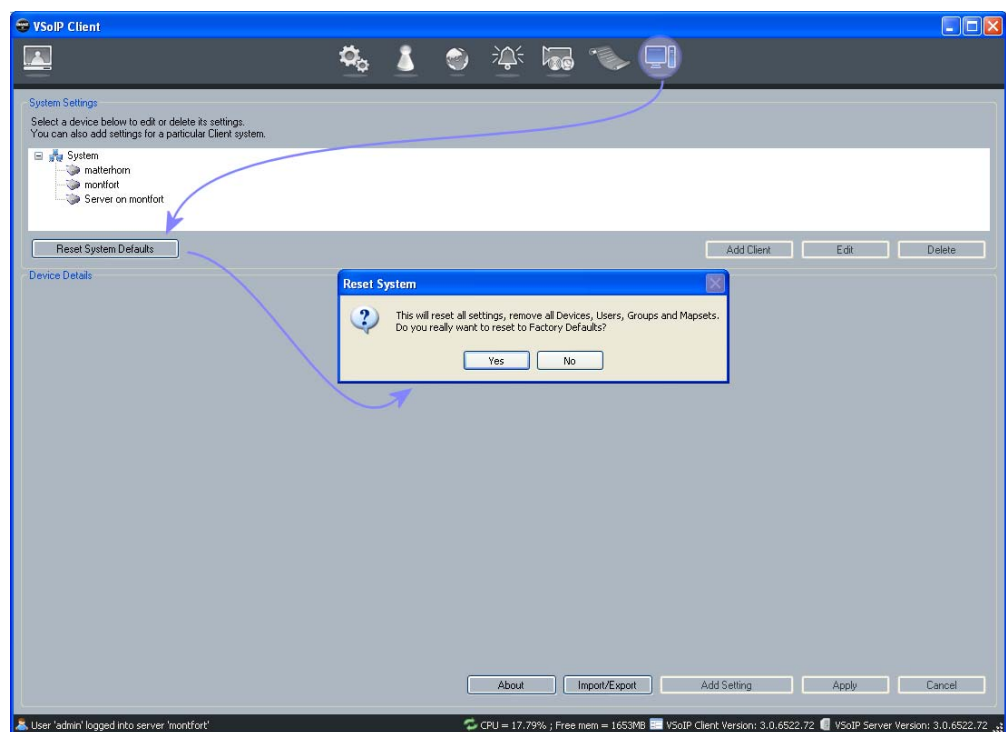
# Chapter 10 – System Administration

This chapter contains information on the following:

- Restoring Factory Defaults
- Reusing Devices, Users and Groups
- Viewing System Information
- Default Settings

## Restoring Factory Defaults

You can revert VSoIP Pro back to its factory default settings, as shown in Figure 57:



**Figure 57** Restoring factory defaults

---

**Caution:** It is not possible to undo this action, so ensure that you really want to restore all settings before proceeding.

---

**Note:** After restoring to factory defaults, you must restart the client to have access to full functionality.

## Reusing Devices, Users and Groups

You can export groups of devices, users and groups that you have set up in one version of VSoIP Pro, and use them in another. These are exported as .xml files.

**Note:** When you have finished setting up your site and all site components (devices, users etc), we recommend that you use this process to make a backup of your site, in case of data corruption.

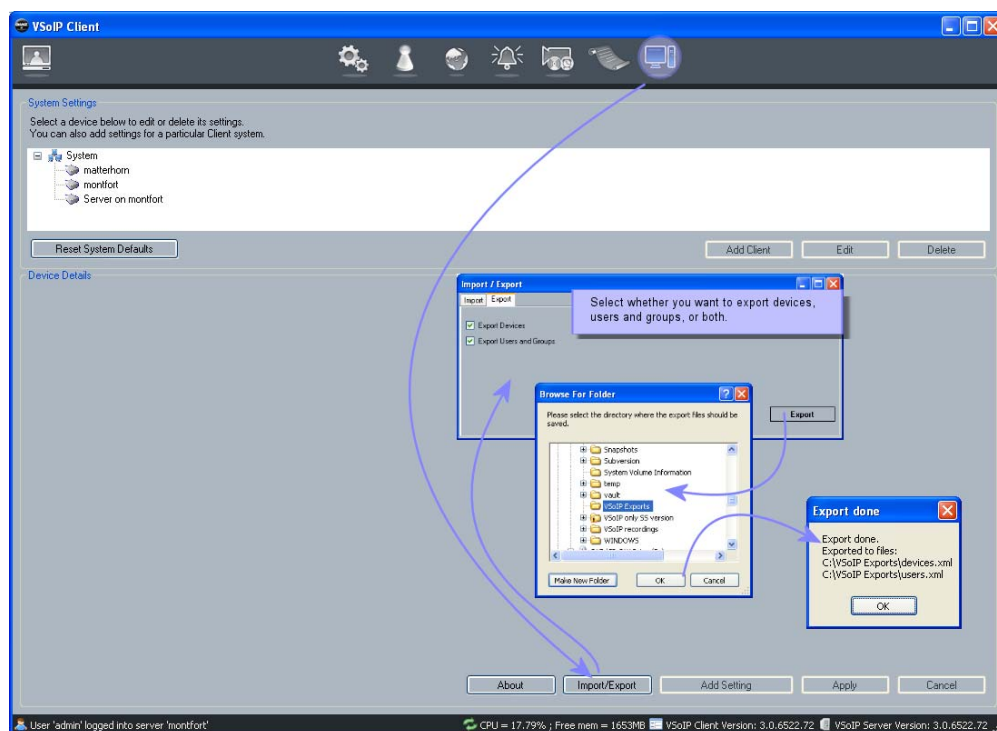
---

**Caution:** Note that client settings which override the defaults are not stored, nor are mapset details.

---

## Exporting Devices, Users and Groups

Figure 58 shows how to export from VSoIP Pro.

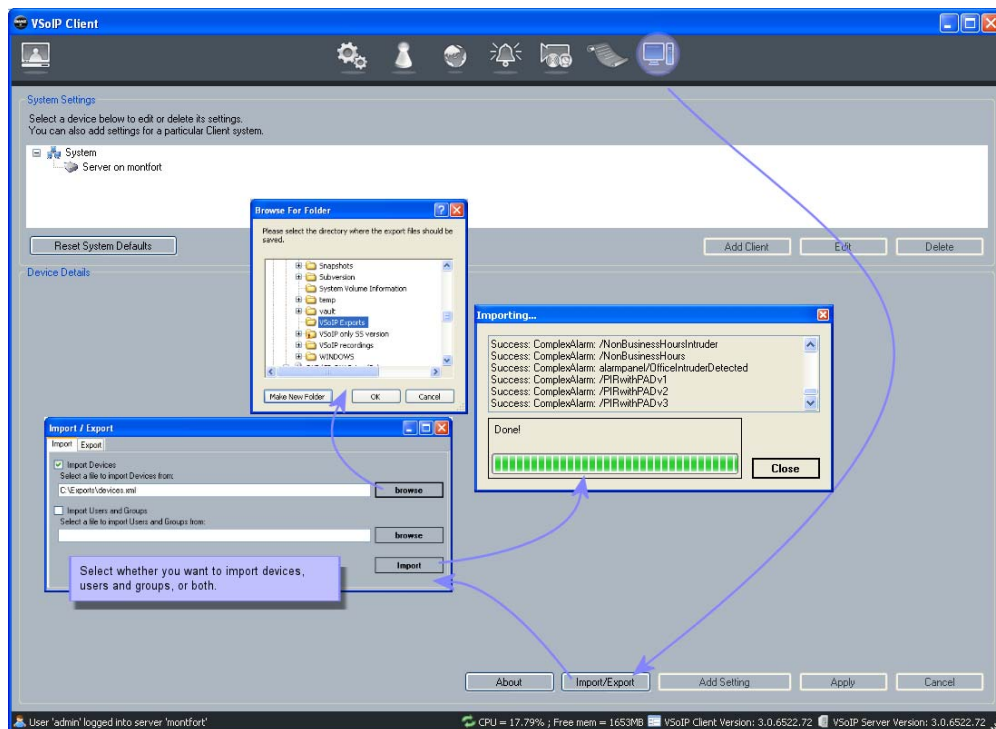


**Figure 58** Exporting from VSoIP Pro

The exported data is saved in .xml format. Device information is stored in devices.xml, and user/group information is stored in user.xml.

## Importing Devices, Users and User Groups

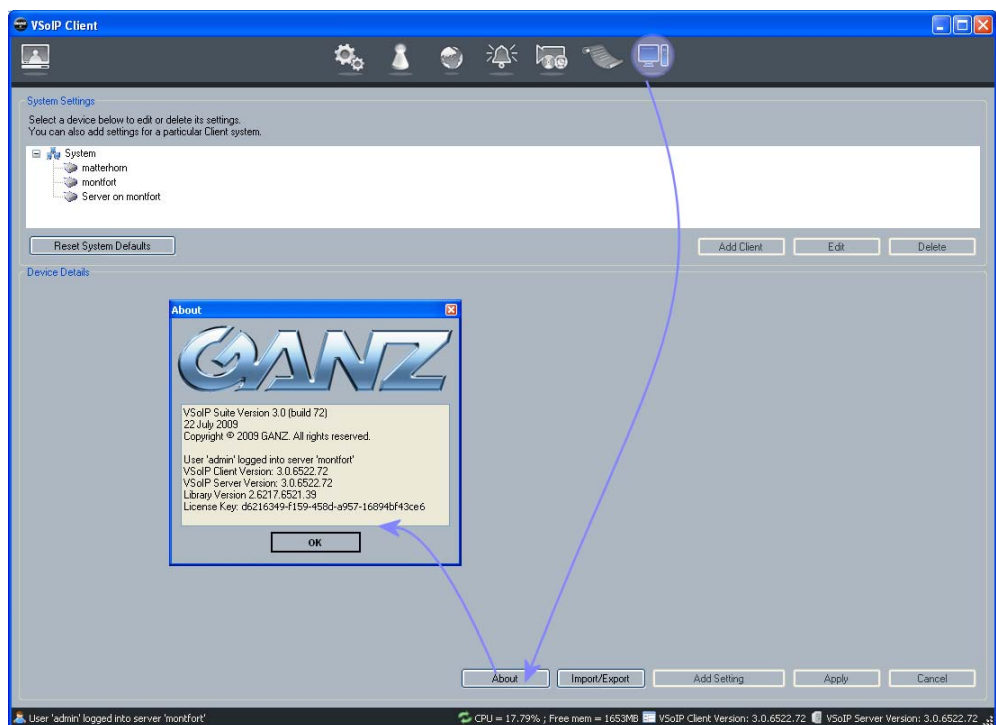
You can import device, users and user group information that you have exported from one version of VSoIP Pro, as shown in Figure 59:



**Figure 59** Importing devices into VSoIP Pro

## Viewing System Information

You can view details of the current installation of VSoIP Pro, as shown in Figure 60:



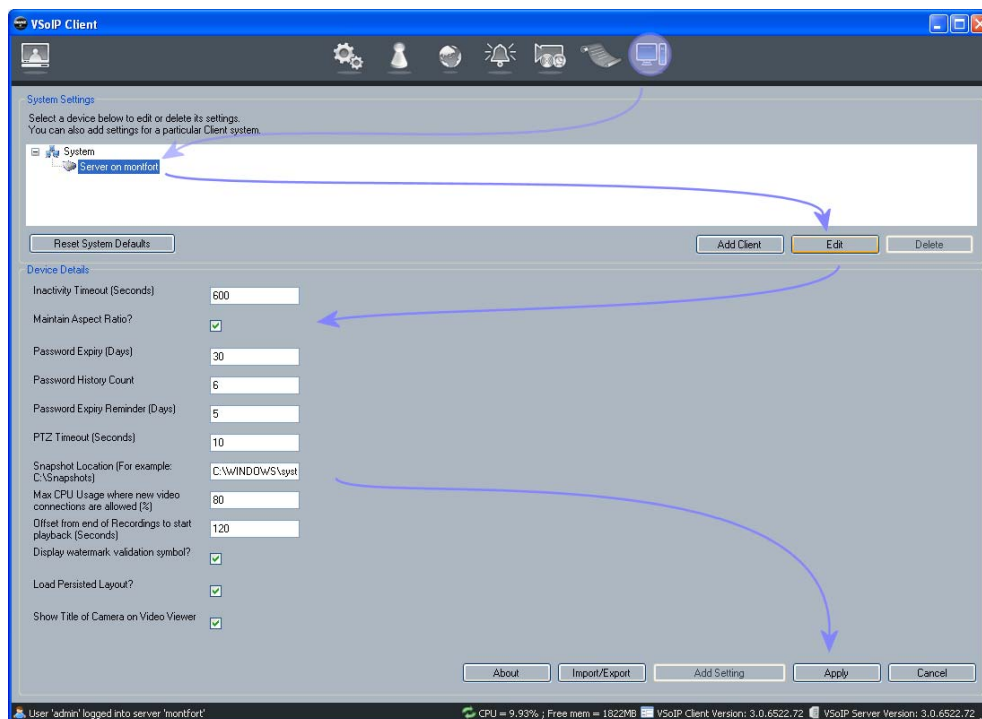
**Figure 60** Viewing installation details

## Default Settings

When you first view the System Settings window, the server is displayed in the device tree.

The server specifies default settings, such as inactivity timeout, aspect ratio, PTZ timeout etc for all clients. To change a value for a particular client, see “Changing Client Settings” on page 85.

Figure 61 shows how to view these settings, and change them if required.



**Figure 61** Viewing existing client settings

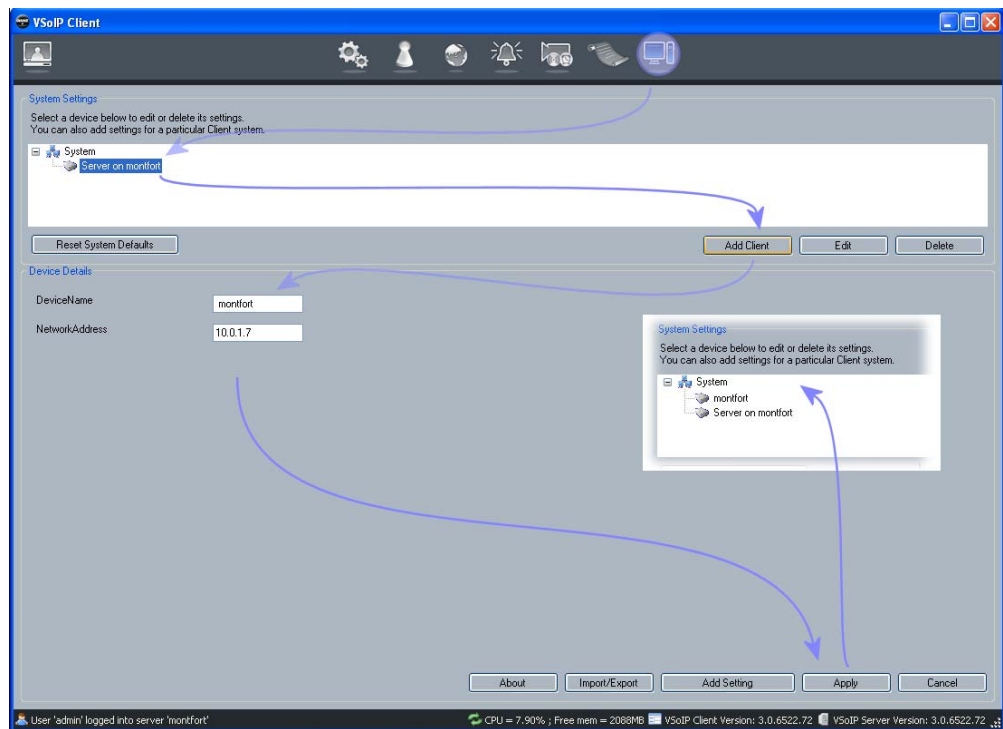
**Note:** If you change a server default value, this change automatically applies to *all* clients connected to that server.

## Changing Client Settings

By default, all clients take their system values from the server. To change values for a particular client:

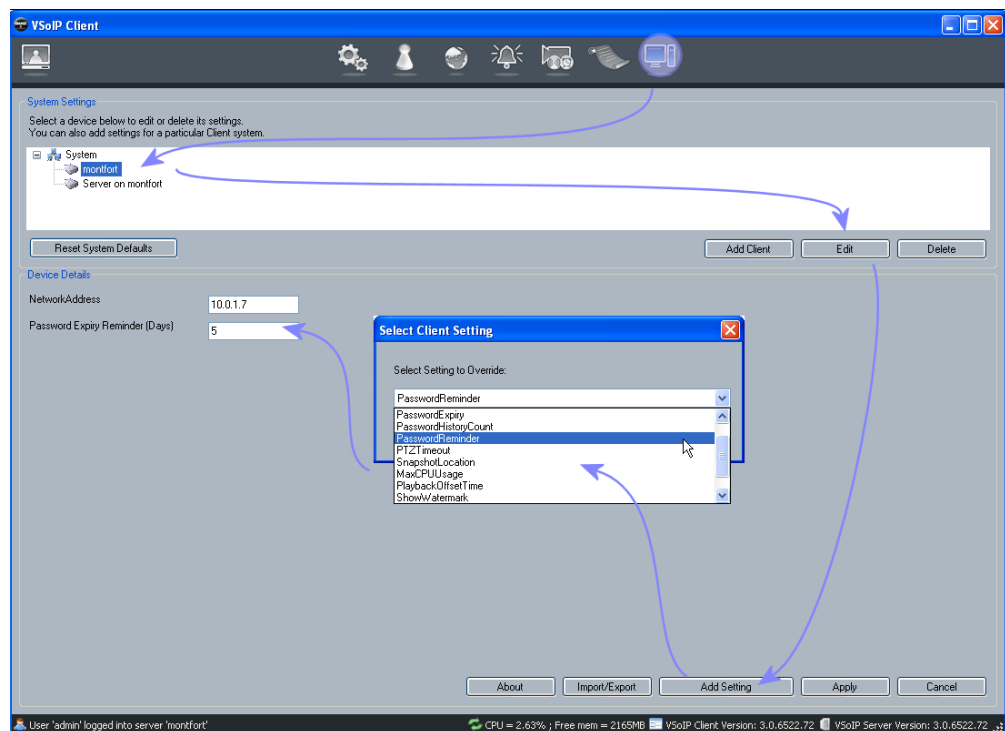
- 1 Select the server in the devices list, and click Add Client, as shown in Figure 62.
- 2 Enter the client name and IP address, and click Apply.

**Note:** The IP address must be the same IP address as the computer running the client. You can use any name but we recommend you use the name assigned to the computer under the Windows Workgroup or Domain.



**Figure 62** Adding a new client

- 3 The client appears in the device tree.
- 4 Select the client name in the device tree, and click Edit (Figure 63).



**Figure 63** Overriding default client settings

- 5 Click Add Setting, and select the setting that you want to override from the drop-down list.
- 6 Click OK, and the setting appears under Device Details, with the default value shown.
- 7 Change this value as required, then click Apply.
- 8 Repeat for each setting you want to change from the default.

## Available Client Settings

The following settings are available for clients:

**Table 6** Available client settings

Setting	Meaning	Default Value
Inactivity Timeout	Length of time that the client can be inactive before a password is required to access functionality again.	600 seconds
Keep Aspect Ratio	Maintain correct aspect ratio of video panes, even when they are resized.	On
Password Expiry	Length of time before a password expires and must be changed.	30 days
Password History Count	The number of different passwords that must be used before a password can be reused.	6
Password Reminder	The number of days before a password expires that you are reminded to change it.	5
PTZ Timeout	Length of time that a PTZ camera can be inactive in a video pane before the PTZ controls must be reactivated	10 seconds
Snapshot Location	<p>The folder where snapshots from live and recorded video are stored. VSolP Pro automatically creates separate sub-folders for live and recorded snapshots.</p> <p><b>Note:</b> This is the path on the computer running the client software component rather than a path on the computer running the server.</p>	C:\WINDOWS\system32\config\systemprofile\Desktop
Max CPU Usage	The maximum CPU usage at which new video connections are allowed. This prevents overdriving the system by preventing new connections starting when the current displayed video is consuming more than this maximum value.	80%
Playback Offset Time	When playing back a recording by dragging and dropping it onto a playback pane, this is the number of seconds before the current time at which video starts playing, for example, now, minus 120 secs.	120 seconds
Show Watermark	Specify whether a red or green square is displayed on recorded video to indicate the integrity (or not) of a recording	On
Load Persisted Layout	When opening the application, display the same cameras and layout that were in use when the application shut down.	On
Show Camera Title	Display the camera title (and path) on the top left of video panes.	On

# 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.

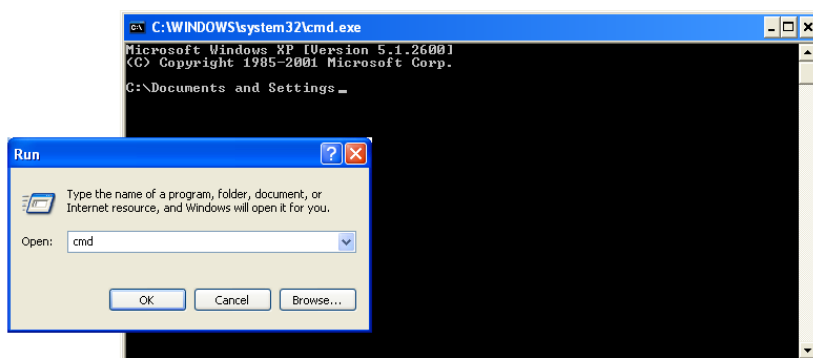
For instance, the networking command **ping** allows the network connections to another networked device to be tested. The main argument required is the IP address of the device, e.g. ping 10.11.12.13

**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 64** 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.

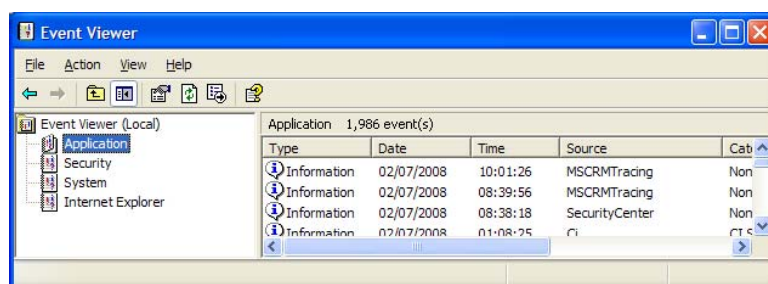
## Finding out the IP Address of your computer

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 65** 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.

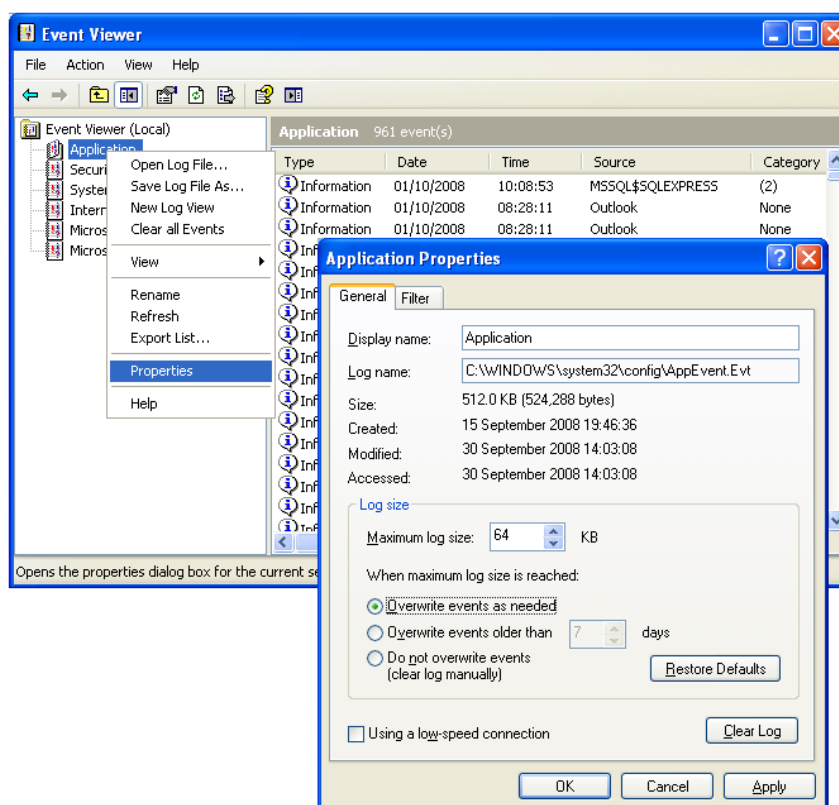
When examining the log, note the Source column. This lists the name of the application that generated the log entry. Entries can be:

- 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 66** 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.

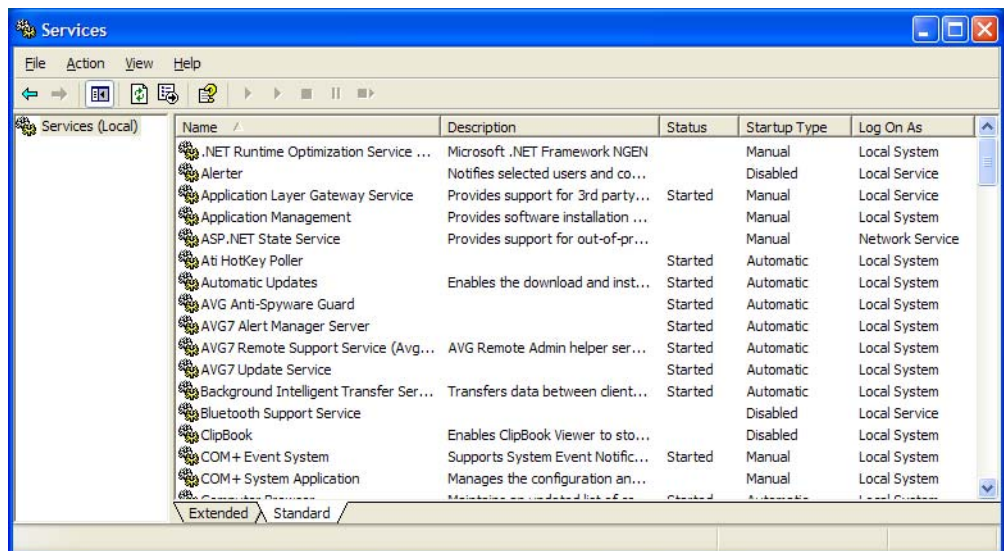
Although services run in the background, do not interact with users graphically, and do not require a user to be logged in, they are initiated and run and thus owned by a user account on the computer. Typically this account is one of the built-in accounts, usually a user called LocalService or sometimes 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 67** Windows services application

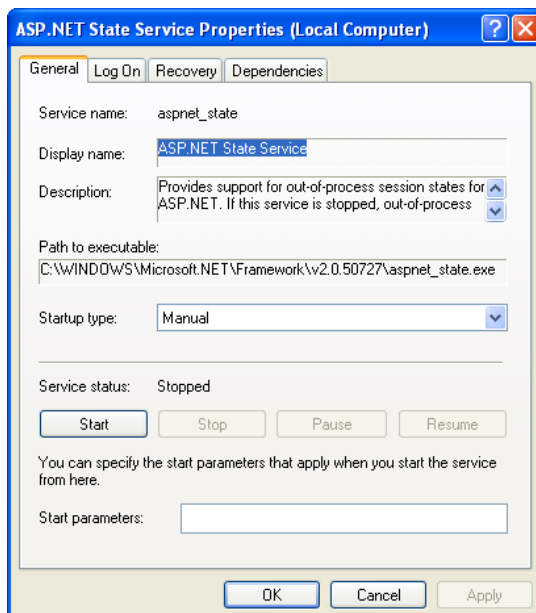
Right-click and choose Properties to display the Properties dialog for the service.

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 68** 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.

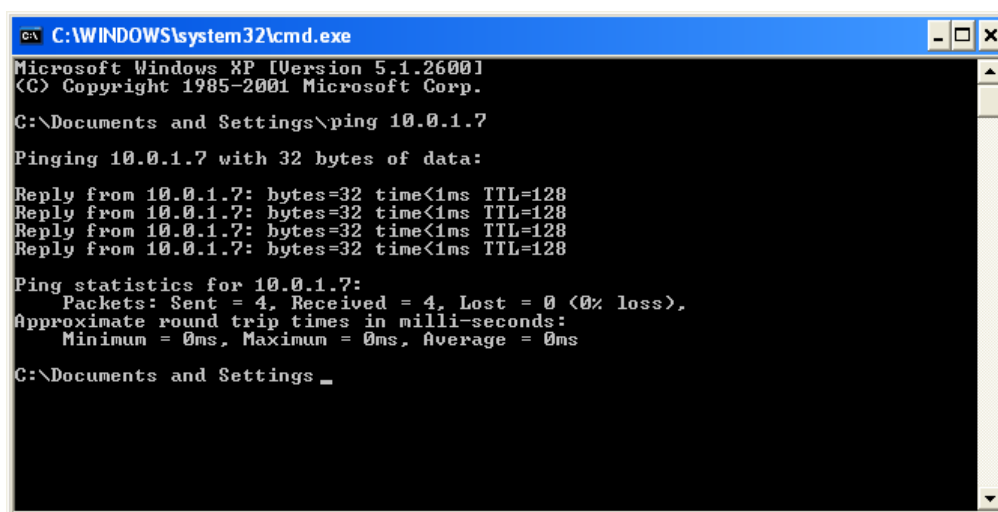
To use a ping you need to know the IP address of the network device you wish to find.

**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 69** 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.

## Appendix B — Supported Devices

This appendix provides a list of devices currently supported by VSoIP Pro.

DEVICE MODEL	Alarm Inputs	Alarm Outputs	Direct PTZ	Transparent PTZ	Motion Detector	NVR Recording	DVR Recording/ Playback	Videowall Live Display	N° Encoders	Remote Config
ZN-T9000	4x	1x	N/A	YES	YES	YES	N/A	YES	2	by I.E.
ZN-C9000	4x	1x	N/A	YES	YES	YES	N/A	YES	2	by I.E.
ZN-L9000	4x	1x	N/A	YES	YES	YES	N/A	YES	2	by I.E.
ZN-T8000	2x	1x	N/A	YES	YES	YES	N/A	YES	2	by I.E.
ZN-C8000	2x	1x	N/A	YES	YES	YES	N/A	YES	2	by I.E.
ZN-L8000	2x	1x	N/A	YES	YES	YES	N/A	YES	2	by I.E.
ZN-D9000	TBI	TBI	N/A	N/A	TBI	YES	N/A	YES	1	by I.E.
MP1AI	N/A	N/A	N/A	N/A	TBI	YES	N/A	YES	1	by I.E.
MP2AI	N/A	N/A	N/A	N/A	TBI	YES	N/A	YES	1	by I.E.
MP3AI	N/A	N/A	N/A	N/A	TBI	YES	N/A	YES	1	by I.E.
MP5AI	N/A	N/A	N/A	N/A	TBI	YES	N/A	YES	1	by I.E.
MP1DN	N/A	N/A	N/A	N/A	TBI	YES MJPEG, H264 TBI	N/A	YES MJPEG, H264 TBI	2, YES MJEG, H264 TBI	by I.E.
MP2DN	N/A	N/A	N/A	N/A	TBI	YES MJPEG, H264 TBI	N/A	YES MJPEG, H264 TBI	2, YES MJEG, H264 TBI	by I.E.
MP3DN	N/A	N/A	N/A	N/A	TBI	YES MJPEG, H264 TBI	N/A	YES MJPEG, H264 TBI	2, YES MJEG, H264 TBI	by I.E.
MP5DN	N/A	N/A	N/A	N/A	TBI	YES MJPEG, H264 TBI	N/A	YES MJPEG, H264 TBI	2, YES MJEG, H264 TBI	by I.E.
ZN-PT304WL	N/A	N/A	YES	N/A	N/A	YES	N/A	YES	1	by I.E.
ZN-D2024	1x	1x	N/A	N/A	TBI	YES	N/A	YES	2	by I.E.
ZVS306	1x	1x	YES	TBI	TBI	YES	N/A	YES	2	by I.E.
ZN-YH305	1x	1x	N/A	N/A	N/A	YES	N/A	YES	1	by I.E.
DDK1500	1x	1x	N/A	YES	YES	YES	N/A	YES	2	by I.E.
C-NV4VS	N/A	N/A	N/A	N/A	N/A	YES	N/A	YES	4	by Specific application
VIPX1	4x	1x	N/A	YES	YES	YES	N/A	YES	2	by I.E.
VIPX2	4x	1x	N/A	YES	YES	YES	N/A	YES	4	by I.E.
VIPX4	4x	1x	N/A	YES	YES	YES	N/A	YES	8	by I.E.
ZR-DHC1630NP	16x	N/A	YES	N/A	YES	YES	YES	YES	16	TBI
ZR-DHC830NP	8x	N/A	YES	N/A	YES	YES	YES	YES	8	TBI
DR4N-DVD	4x	1x	YES	N/A	TBI	YES	YES	YES	4	TBI
DR8N-DVD	8x	8x	YES	N/A	TBI	YES	YES	YES	8	TBI
DR16N-DVD	16x	16x	YES	N/A	TBI	YES	YES	YES	16	TBI
DR8NRT	8x	8x	YES	N/A	YES	YES	YES	YES	8	TBI
DR16NRT	16x	16x	YES	N/A	YES	YES	YES	YES	16	TBI
DM NetVu	16x	N/A	N/A	N/A	YES	YES	YES	YES	16	TBI
IPC3100	N/A	1x	YES	YES	YES	YES	N/A	YES	1	by I.E.
IPC3500	N/A	1x	YES	YES	YES	YES	N/A	YES	1	by I.E.
IPE110	N/A	1x	YES	YES	YES	YES	N/A	YES	2	by I.E.
NVC1000	N/A	1x	YES	YES	YES	YES	N/A	YES	2	by I.E.

\*TBI: To be implemented

Transparent PTZ protocols:

All-View Serial  
All-View V3 Serial  
BBV Serial  
C-Dome Serial  
GANZ-PT Serial

Pelco D Serial  
Pelco P Serial  
Sensormatic Serial  
Vicon Serial

All protocols implement:

Zoom, Pan, Tilt  
Presets store recall  
Presets renaming

OSD (when supported)  
Tours (when supported)

# Appendix C — NVR Partitions and Partition Groups

The computing term “partition” is a widely understood one. It is used to describe a logical area of a computer storage device typically on a computer hard-drive that stores data. Within such a partition there can be many folders and files. NVR partitions are similar – they are logical areas of computer storage – but rather than being an area taken from the raw hard-drive which is then formatted to give it structure, NVR partitions are simply reserved areas of a predefined size using an existing, pre-formatted hard-drive partition.

## Default partition

The default partition for VSoIP was specified during the installation process. It is not possible to change the location of this partition, or delete it — however, you can add and delete other partitions, as shown in Figure 70.

## Partition Modes

The NVR manages usage of each NVR partition according to the partition mode. The NVR partition modes are:

- **Overwrite** – when the content footprint in the partition reaches the size of the partition, the oldest data is automatically overwritten. Recordings scheduled as looped recordings will be forced to loop earlier than scheduled. Recordings scheduled as not looped will be looped. This mode keeps the most recent recordings.
- **Protected** – when the storage requirements of NVR data in the partition reaches the pre-defined size of the partition, then any currently recording schedules using this group are disabled and recording ends. This mode can be thought of as keep oldest recordings.
- **Archive** – this partition mode flags this position as one used to keep significant recording footage. Typically a process of maintenance has identified some recordings in an overwrite partition that need keeping, or recordings that must be deleted from a protected partition to allow the NVR to make full use of the partition. In these scenarios the recorded footage is moved into the archive partition.

## Partition Groups

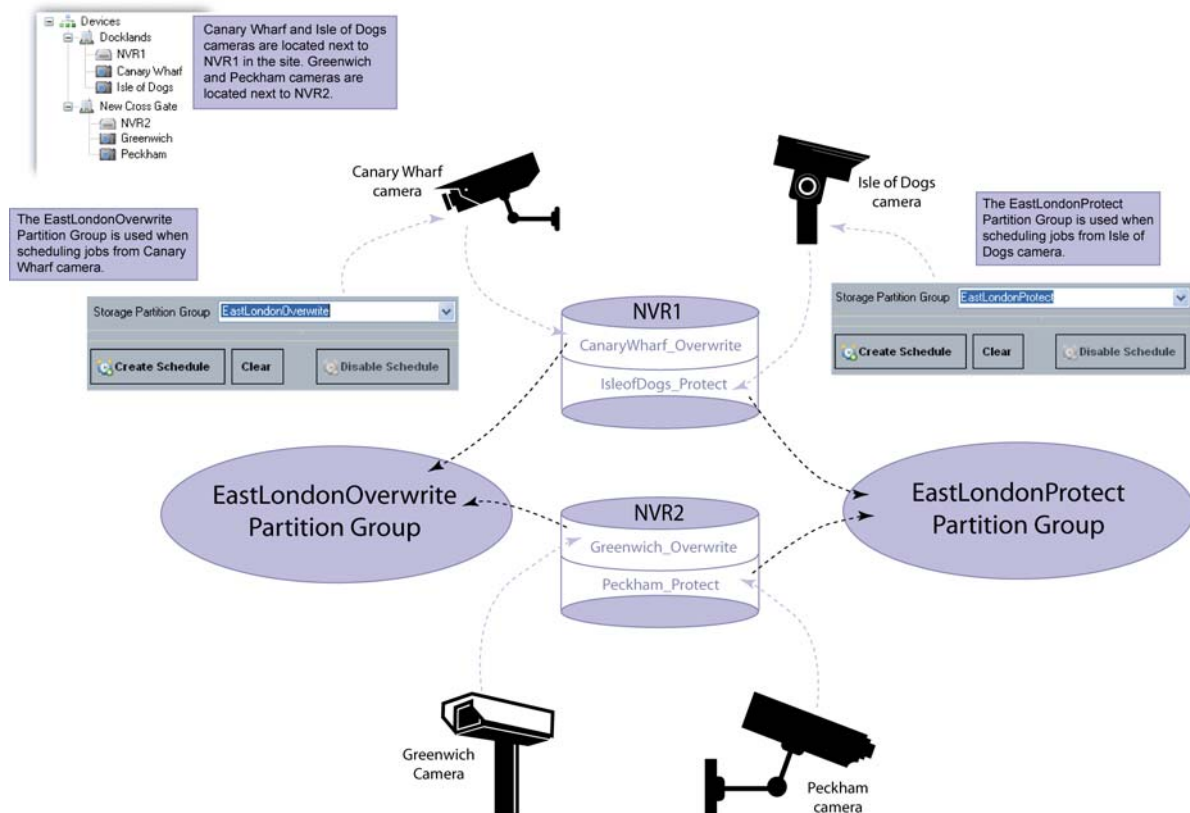
Partitions are organised into *partition groups*. These combine partitions from different NVRs into virtual groups. This means that you do not have to specify an exact partition when creating a recording schedule – the server considers which partitions belong to that group, and decides which partition is best to record to, using the following criteria:

- Available disk space on each partition
- Current recording load on each partition
- Position in the site of each NVR in relation to the camera being recorded

When creating a partition, you must specify which group it belongs to. It is strongly recommended that all partitions in a particular group are of the same type, i.e., Overwrite or Protect.







**Figure 71** Partition overview

- Footage from the Canary Wharf camera is being recorded to an Overwrite partition on NVR1, which forms part of the EastLondonOverwrite partition group.
- Footage from the Greenwich camera is being recorded to an Overwrite partition on NVR2, which is also part of the EastLondonOverwrite partition group.

When scheduling these recording jobs, the EastLondonOverwrite partition group was selected. The server used the above criteria to decide which partition was most appropriate for the recording job – in this case, the partition on NVR1 is logically closest to the two cameras.

- Footage from the Isle of Dogs camera is being recorded to a Protect partition on NVR1, which forms part of the EastLondonProtect partition group.
- Footage from the Peckham camera is being recorded to a Protect partition on NVR2, which is also part of the EastLondonProtect partition group.

When scheduling these recording jobs, the EastLondonProtect partition group was selected. The server used the above criteria to decide which partition was most appropriate for the recording job – in this case, the partition on NVR2 is logically closest to the two cameras.

# Appendix D — Complex Alarm Configuration

This appendix contains the following information:

- Simple Alarms and Scheduled Alarms
- Understanding Alarm Processing
- Creating Complex Alarms
- Using the NOT Boolean Operator
- How Complex Alarms Work
- Example of Complex Alarm Processing

## Simple Alarms and Scheduled Alarms

Complex alarms are created by combining simple alarms and scheduled alarms together to form more complex alarm processing logic. This section considers simple alarms and scheduled alarms.

### Simple Alarms

A simple alarm represents an alarm source on an IP Camera, encoder or Networked DVR within the surveillance system. Examples of such alarm sources are:

- Binary inputs.
- Motion detector alarms.
- Video loss alarms.
- Networked DVR complex alarm logic.

### Scheduled Alarms

A schedule is another type of alarm source. A server can be the source of one or more alarms based on a schedule. A schedule is a time-based alarm source that causes an alarm to be continuously output when the time and day of a week matches a marked period within the schedule. Each marked period represents one hour. Each schedule has seven days of twenty-four hour long periods available. Any number of periods can be chosen.

Examples of schedules an administrator level user might create on a server are:

- All weekend — all periods for Saturday and Sunday are selected
- Outside weekday office hours — Monday to Friday, periods representing hour long intervals after 18h00 until interval prior to 09h00, are selected
- During lunch-hour — A period of one hour after 12h00 for each weekday is selected.

## Understanding Alarm Processing

A common technique used to represent logic expressions like those described previously is a logic system called Boolean logic. The inputs and outputs of Boolean logic expressions are either true or false. These states can be thought of as voltages present (TRUE) or absent (FALSE) at an input and voltages present (TRUE) or absent (FALSE) at an output.

In Boolean logic a condition represents something which takes one or more inputs and produces a single output which is either true or false depending on the states of the input(s) and the Boolean logic condition being used. Examples of Boolean logic are explained in the following section.

## Creating Complex Alarms

To illustrate the creation of complex alarms, we shall use the following scenario:

A surveillance system has equipment monitoring three bank vaults using PIR sensors connected to IP cameras and pressure pads connected to a Networked DVR.

The aim of the system's designer is to have an alarm triggered when all of the following conditions apply:

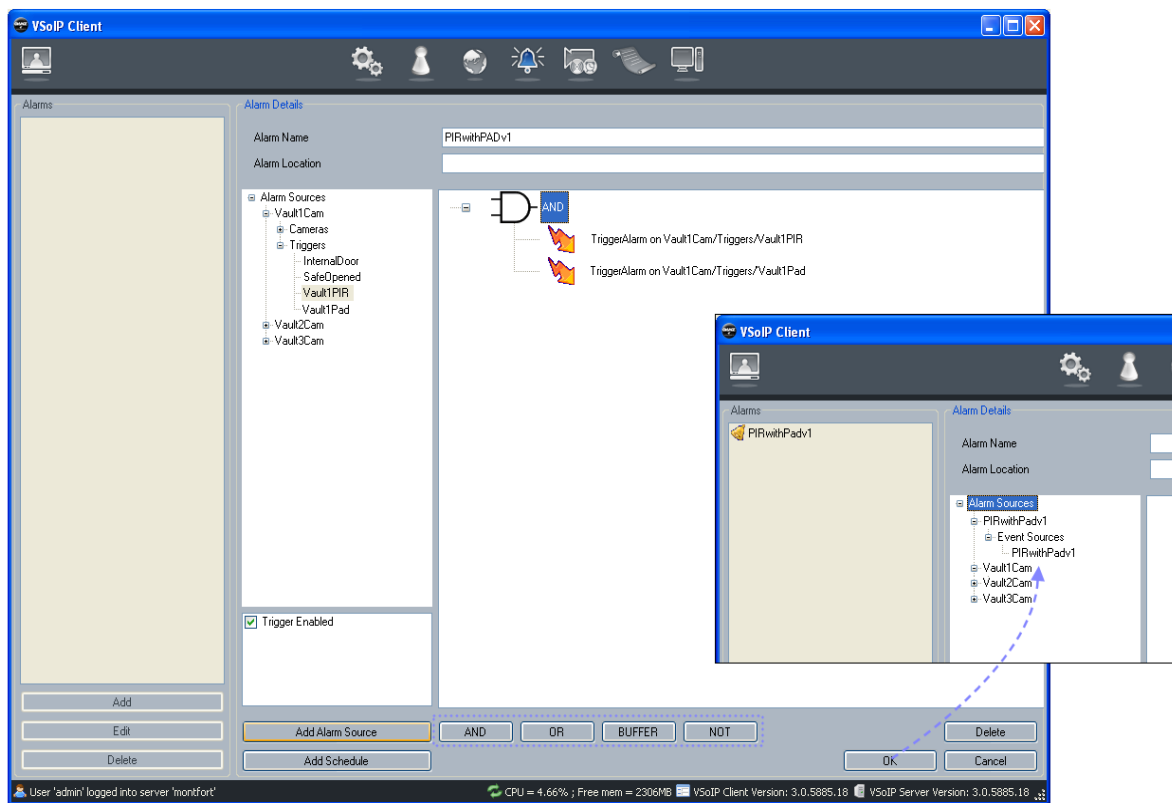
- a PIR AND a pressure pad are activated
- in ANY of three bank vaults
- during non-business hours

This can be achieved by setting up several complex alarms. This process is explained below.

**Note:** It is also possible to achieve the same end result by setting up a single complex alarm. However, a modular structure is useful because it allows individual elements to be altered separately, and reused within other complex alarms.

### Step 1

To prevent false alarms, the system's designer has specified that a vault's intruder alarm should *only* be triggered when the pressure pad AND the PIR trigger in that vault are both activated, i.e. both sensors change state from FALSE to TRUE.



**Figure 72** Creating PIRwithPADv1 complex alarm

- 1 At the bottom left of the screen click Add.
- 2 Enter a name for the alarm and (optionally) a location. In this example, the alarm is called PIRwithPADv1.
- 3 Click the Boolean logic operator button required for the part of the alarm logic you are describing; in this example it is AND (i.e. /Vault1Cam/Triggers/Vault1PIR AND /Vault1Cam/Triggers/Vault1Pad). The symbol for this operation appears in the alarm logic designer pane.

**Note:** AND is the logic condition for “all inputs must be active”. All inputs of an AND logic expression must be TRUE for the output to be TRUE.

- 4 Select the alarm source you want to use from the list. The events that that alarm source can generate are listed. Put a check against the event that should cause an alarm from the alarm source.

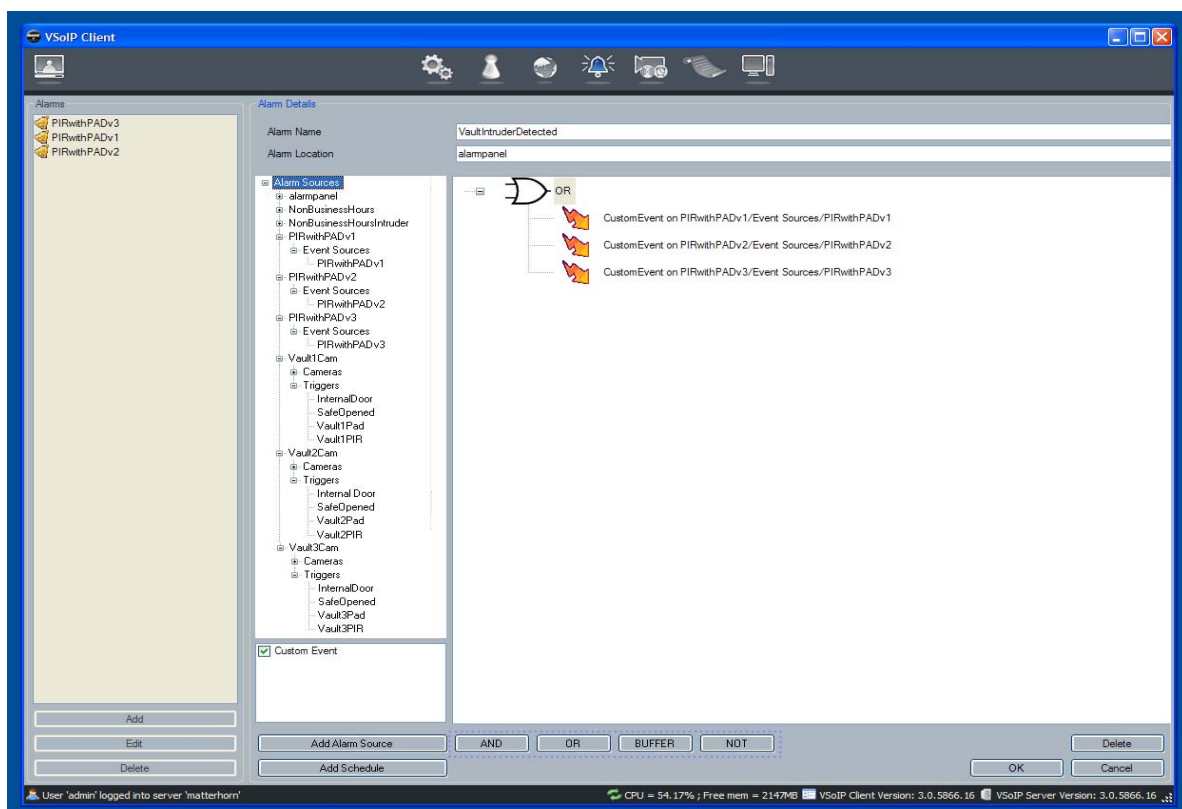
**Note:** If, for example, a video-based alarm source had been chosen, other possible events could have been checked such as video loss or video motion detected.

- 5 Click Add Alarm Source.
- 6 Repeat steps 4 and 5 until the required logic is achieved. In this example, Vault1PAD is added in the same way.
- 7 When finished, click OK. The output of this conditional expression becomes a new complex alarm, e.g. /PIRwithPADv1. When the /Vault1Cam/Triggers/Vault1PIR sensor and /Vault1Cam/Triggers/Vault1Pad sensor are both activated, then the /PIRwithPADv1 complex alarm will fire.
- 8 Click OK to complete the complex alarm.
- 9 In this example, steps 1-9 would be repeated for vaults 2 and 3.

**Note:** If you make a mistake, select the item and click Delete. We recommend that you write out your logic design on paper first, then place *only* the logic operators on the pane, then finally add in the alarm sources and schedules.

## Step 2

The system’s designer has specified that a secondary alarm must be triggered if ANY ONE of the vaults is breached, i.e. when any one of the vaults’ PIRwithPAD trigger changes state from FALSE to TRUE.



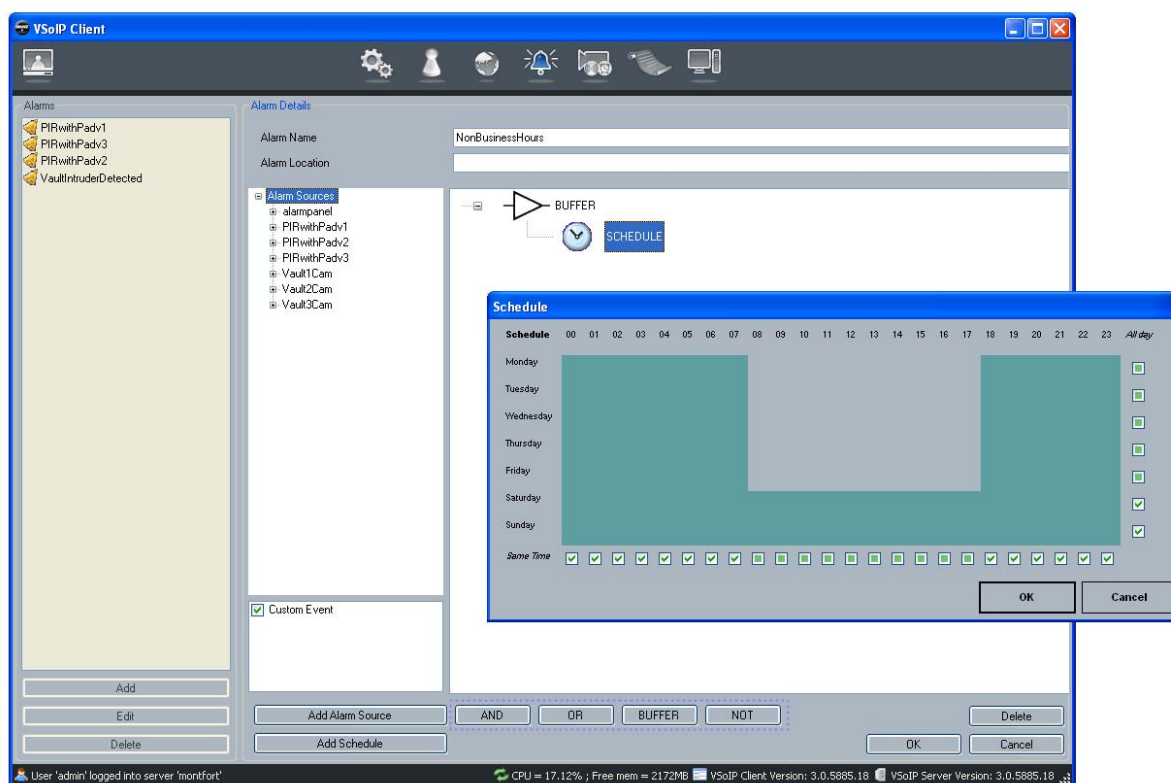
**Figure 73** Creating VaultIntruderDetected complex alarm

- 1 At the bottom left of the screen click Add.
- 2 Enter a name for the alarm and (optionally) a location. In this example, the alarm is called VaultIntruderDetected and the location is alarmpanel.

- Click the Boolean logic operator button required for the part of the alarm logic you are describing; in this example it is OR (e.g. /PIRwithPADv1 OR /PIRwithPADv2 OR /PIRwithPADv3). The symbol for this operation appears in the alarm logic designer pane.
- Note:** OR is the logic condition for “any inputs are active”. If ANY inputs of an OR logic expression are TRUE then the output will be TRUE.
- Select the alarm source you want to use from the list, remembering to choose an event available from the source, and click Add Alarm Source. In this case, the alarm source PIRwithPADv1 is the first to be added.
  - Repeat step 4 until the required logic is achieved. In this example, PIRwithPADv2 and PIRwithPADv3 are added in the same way.
  - When finished, click OK. The output of this conditional expression becomes a new complex alarm, e.g. /alarmpanel/VaultIntruderDetected. When the /PIRwithPADv1 or /PIRwithPADv2 or /PIRwithPADv3 is activated then the /alarmpanel/VaultIntruderDetected complex alarm is triggered.

### Step 3

The third alarm that the designer must create is a scheduled alarm. This is a time-based alarm source that causes an alarm to be continuously output when the time and day of a week matches a marked period within the schedule.



**Figure 74** Creating NonBusinessHours scheduled alarm

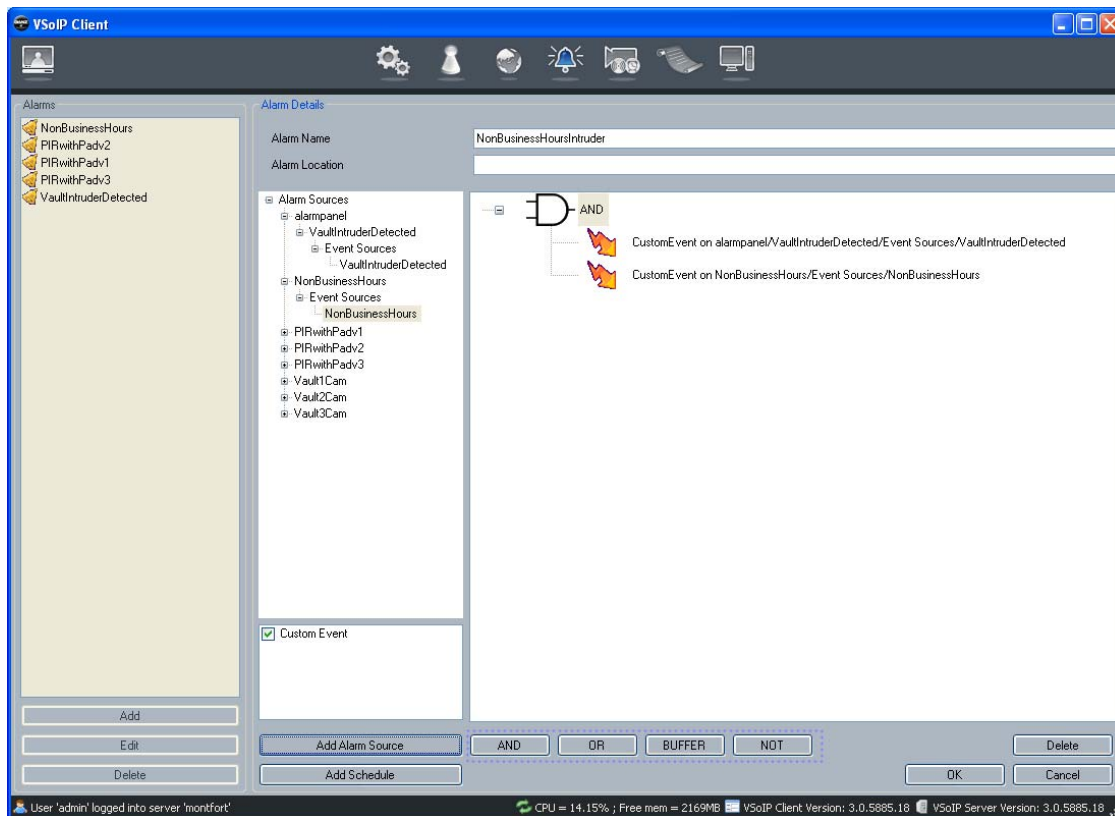
- At the bottom left of the screen click Add.
- Enter a name for the alarm and (optionally) a location. In this example, the alarm is called NonBusinessHours.
- Click the Boolean logic operator button required for the part of the alarm logic you are describing, or, if the schedule does not need to be part of a more complex alarm logic system, click BUFFER.
- Click Add Schedule. In the Schedule dialog, select the hours you want the alarm to be continuously output. In this example, the schedule is active from 18:00 every evening until 08:00 the following morning, and at weekends.

**Note:** Check the box for a row/column to select the entire row/column.

- Click OK when finished, then OK again.

#### Step 4

Finally, the designer needs to create a complex alarm that combines the alarms he has set up already. This complex alarm would be triggered when a PIR AND a pressure pad are activated in ANY of three bank vaults during non-business hours.



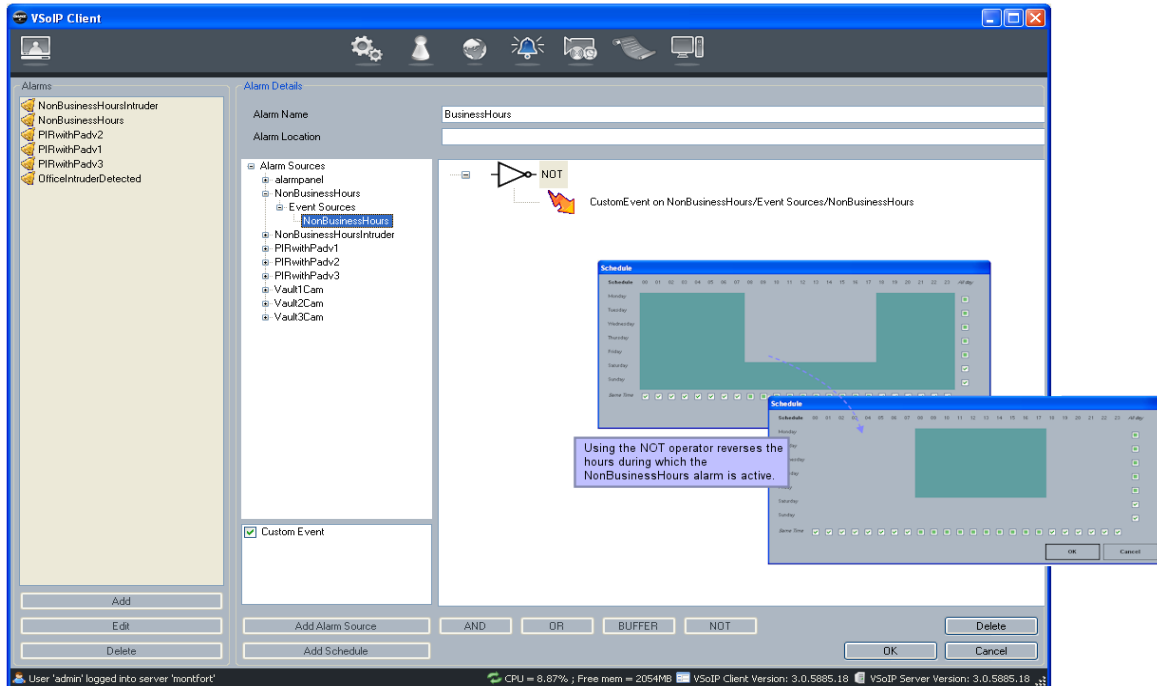
**Figure 75** Creating NonBusinessHoursIntruder Complex Alarm

- At the bottom left of the screen click Add.
- Enter a name for the alarm and (optionally) a location. In this example, the alarm is called NonBusinessHoursIntruder.
- Click the Boolean logic operator button required for the part of the alarm logic you are describing; in this example it is AND (e.g. /alarmpanel/VaultIntruderDetected AND /NonBusinessHours). The symbol for this operation appears in the alarm logic designer pane.  
  
**Note:** AND is the logic condition for “all inputs must be active”. All inputs of an AND logic expression must be TRUE for the output to be TRUE.
- Select the alarm source you want to use from the list, remembering to choose an event available from the source, and click Add Alarm Source. In this case, the alarm sources /alarmpanel/VaultIntruderDetected and /NonBusinessHours are added.
- When finished, click OK. The output of this conditional expression becomes a new complex alarm, e.g. /NonBusinessHoursIntruder. When the /alarmpanel/VaultIntruderDetected complex alarm is firing and /NonBusinessHours complex alarm is active then the /NonBusinessHoursIntruder alarm will be triggered.

## Using the NOT Boolean Operator

The above examples made use of the AND and OR Boolean operators and buffers. Another operator, NOT, could be used in conjunction with the NonBusinessHours alarm detailed above, as part of a complex alarm that operates *only during business hours*. Figure 76 illustrates how using NOT reverses the hours during which the alarm is active.





**Figure 76** Creating BusinessHours scheduled alarm using NOT Boolean operator

- 1 At the bottom left of the screen click Add.
- 2 Enter a name for the alarm and (optionally) a location. In this example, the alarm is called BusinessHours.
- 3 Click the Boolean logic operator button required for the part of the alarm logic you are describing; in this example it is NOT. The symbol for this operation appears in the alarm logic designer pane.

**Note:** The Boolean NOT condition outputs TRUE whenever a FALSE is input, or outputs FALSE whenever a TRUE is input.

- 4 Select the alarm source you want to use from the list, remembering to choose one, or more of the events available from the source, and click Add Alarm Source. In this case, the alarm source /NonBusinessHours is added.
- 5 When finished, click OK.

## How Complex Alarms Work

The server is responsible for keeping track of the state of all simple alarms, scheduled sources and complex alarms that are included within the logic of each complex alarm.

Whenever a simple alarm is triggered, the server marks this by changing the simple alarm's recorded state from FALSE to the TRUE state. The server then maintains this alarm's state as being TRUE for a period of five seconds irrespective of the actual external state of the alarm. After five seconds have elapsed, the server automatically marks the simple alarm as FALSE.

Whenever the Server changes the state of a simple alarm's marked state, the server locates all complex alarms that rely on that simple alarm and processes the trigger logic. For each simple alarm included in a complex alarm, the server looks up the last recorded state of the simple alarm and uses the recorded TRUE or FALSE value in the Boolean logic.

**Note:** When a complex alarm is evaluated by the server as being TRUE, it is marked as true for a period long enough to evaluate any other complex alarms that refer to it.

Scheduled sources remain TRUE for as long as the marked period matches the time and day of the week.



The momentary storage of the state (TRUE or FALSE) of the output of a simple alarm, buffered scheduled source or complex alarm for five seconds is automatic and is performed by the server alarm trigger logic processor.

**Caution:** For a scheduled source to be used outside of the alarm processor, a scheduled alarm source must be converted to an complex alarm. This is done whenever schedules are a part of the alarm logic for a multi-source complex alarm. If the output required is to be based solely on single scheduled source, a complex alarm containing a buffer logic processing element must be used along with the scheduled source.

## Example of Complex Alarm Processing

The following example details how the server deals with the following scenario: an intruder enters vault one and is detected first by the PIR and then a half a second later they stand on the pressure pad, activating it.

**Note:** The alarm schedule discussed in Step 3 above is not included in Table 7.

**Table 7** Complex alarm walkthrough

Stage	Elapsed (msecs)	Activity
PIR detects intruder	T+0000	Simple alarm /Vault1Cam/Triggers/Vault1PIR is received by the server.
	T+0010	The server checks to see if /Vault1Cam/Triggers/Vault1PIR participates in any complex alarms, finds one, and changes the recorded state of /Vault1Cam/Triggers/Vault1PIR from FALSE to TRUE
	T+0176	The server now evaluates all complex alarms containing /Vault1Cam/Triggers/Vault1PIR and finds /PIRwithPADv1. This is a Boolean Logic AND expression between the recorded state of simple alarm /Vault1Cam/Triggers/Vault1PIR and the recorded state of simple alarm /Vault1Cam/Triggers/Vault1Pad. This simplifies to the Boolean condition TRUE AND FALSE which results in FALSE. The complex alarm /PIRwithPADv1 is marked as FALSE.
	T+0193	The server now evaluates all complex alarms containing /PIRwithPADv1 and finds /alarmpanel/VaultIntruderDetected. This is a Boolean Logic OR expression between the recorded states of /PIRwithPADv1, /PIRwithPADv2 and /PIRwithPADv3. Since all of these complex alarms have a recorded state of FALSE, then this simplifies to the Boolean condition FALSE OR FALSE OR FALSE which results in FALSE. Complex alarm /alarmpanel/VaultIntruderDetected is marked as FALSE
	T+0213	The server now evaluates all complex alarms containing /alarmpanel/VaultIntruderDetected and does not find any. Server now considers processing complete.
	T+0500	Simple alarm /Vault1Cam/Triggers/Vault1Pad is received by the server.
	T+0508	The server checks to see if /Vault1Cam/Triggers/Vault1Pad participates in any complex alarms, finds one, and changes the recorded state of /Vault1Cam/Triggers/Vault1Pad from FALSE to TRUE
Pressure pad activated	T+0603	The server now evaluates all complex alarms containing /Vault1Cam/Triggers/Vault1Pad and finds /PIRwithPADv1. This is a Boolean Logic AND expression between the recorded state of simple alarm /Vault1Cam/Triggers/Vault1PIR and the recorded state of simple alarm /Vault1Cam/Triggers/Vault1Pad. This simplifies to TRUE AND TRUE which results in TRUE. The complex alarm /PIRwithPADv1 is marked as TRUE.
	T+0622	The server fires /PIRwithPADv1 alarm.
	T+0629	The server now evaluates all complex alarms containing /PIRwithPADv1 and finds /alarmpanel/VaultIntruderDetected. This is a Boolean Logic OR expression between the recorded states of /PIRwithPADv1, /PIRwithPADv2 and /PIRwithPADv3. These complex alarms now have a recorded state of TRUE, FALSE and FALSE respectively. This simplifies to TRUE OR FALSE OR FALSE which results in TRUE. The complex alarm /alarmpanel/VaultIntruderDetected is marked as TRUE.
	T+0645	The server fires /alarmpanel/VaultIntruderDetected alarm.  The server now evaluates all complex alarms containing /alarmpanel/VaultIntruderDetected and does not find any. It now considers processing complete.

**Table 7** Complex alarm walkthrough (Continued)

System clears PIR trigger	T+5010	The server changes the recorded state of /Vault1Cam/Triggers/Vault1PIR from TRUE to FALSE
	T+5098	The server now evaluates all complex alarms containing /Vault1Cam/Triggers/Vault1PIR and finds /PIRwithPADv1. This is a Boolean Logic AND expression between the recorded state of simple alarm /Vault1Cam/Triggers/Vault1PIR and the recorded state of simple alarm /Vault1Cam/Triggers/Vault1Pad. This simplifies to FALSE AND TRUE which results in FALSE. The complex alarm /PIRwithPADv1 is marked as FALSE.
	T+5109	The server now evaluates all complex alarms containing /PIRwithPADv1 and finds /alarmpanel/VaultIntruderDetected. This is a Boolean Logic OR expression between the recorded states of /PIRwithPADv1, /PIRwithPADv2 and /PIRwithPADv3. Since all of these complex alarms have a recorded state of FALSE, then this simplifies to FALSE OR FALSE or FALSE which results in FALSE. The complex alarm /alarmpanel/VaultIntruderDetected is marked as FALSE
	T+5142	The server now evaluates all complex alarms containing /alarmpanel/VaultIntruderDetected and does not find any. It now considers processing complete.
	T+5508	The server changes the recorded state of /Vault1Cam/Triggers/Vault1Pad from TRUE to FALSE
System clears pressure pad trigger	T+5532	The server now evaluates all complex alarms containing /Vault1Cam/Triggers/Vault1Pad and finds /PIRwithPADv1. This is a Boolean Logic AND expression between the recorded state of simple alarm /Vault1Cam/Triggers/Vault1PIR and the recorded state of alarm trigger/Vault1Cam/Triggers/Vault1Pad. This simplifies to FALSE AND FALSE which results in FALSE. The complex alarm /PIRwithPADv1 is marked as FALSE.
	T+5563	The server now evaluates all complex alarms containing /PIRwithPADv1 and finds /alarmpanel/VaultIntruderDetected. This is a Boolean Logic OR expression between the recorded states of /PIRwithPADv1, /PIRwithPADv2 and /PIRwithPADv3. Since all of these complex alarms have a recorded state of FALSE, then this simplifies to FALSE OR FALSE or FALSE which results in FALSE. The complex alarm /alarmpanel/VaultIntruderDetected is marked as FALSE
	T+5569	The server now evaluates all complex alarms containing /alarmpanel/VaultIntruderDetected and does not find any. It now considers processing complete.

**Note:** The technique of remembering the state of something, for example a simple alarm, for five seconds, is known as buffering. i.e. the TRUE state of a simple alarm is buffered as TRUE for five seconds following the firing of the simple alarm.

# Index

---

## A

- acknowledging alarms 49
- activating
  - client 23
- activating NVR 78
- activating PTZ 46
- adding
  - devices 35
  - mapsets 40
  - user groups 32
  - users 28
- alarm triggered recording 81
- alarms
  - acknowledging 49
  - closing 50
  - configuring 48
  - display 48
  - viewing properties 49
- aspect ratio, default setting 87
- audit trail 59
  - profiles 60

---

## B

- backup, site 83

---

## C

- camera compatibility 7
- camera title, displaying 87
- changing client defaults 85
- checking connectivity 92
- client
  - activating 23
  - configuration 27
  - default settings 85
  - evaluation mode 24
  - firewall information 20
  - installation 22
  - pre-installation 20
  - prerequisites 19
  - starting 25
- closing alarms 50
- command prompt, opening 88
- compatibility
  - cameras 7
  - DVR 7
- complex alarms, configuring 99
- computer's IP address, determining 88
- configuring 59
  - alarms 48
  - audit trail 59
  - client 27
  - complex alarms 99
  - devices 34
  - mapsets 40, 61
  - PTZ 39
  - stream settings 8
  - triggers 38
  - user groups 32

- users 28
- video sources 38
- configuring NVR 79
- controlling PTZ 46
- controls, live view 42
- CPU usage, maximum 87
- creating new user 28

---

## D

- default administrative user 25
- default settings, client 85
- deleting
  - devices 37
  - mapsets 41
  - user groups 33
  - users 31
- deleting recording jobs 81
- device information
  - exporting 83
  - importing 84
- devices
  - adding 35
  - configuration 34
  - deleting 37
  - specifying location 35
- disabling
  - users 30
- disabling logging 94
- disabling recording jobs 81
- displaying
  - camera title 87
  - recording footage 51
- DVR compatibility 7

---

## E

- editing recording jobs 80
- enabling logging 93
- evaluation mode, client 24
- expected performance, NVR 77
- exported recordings player 56
  - installing 57
  - pre-installation 57
  - prerequisites 56
- exporting device and user information 83
- exporting recordings 55, 56
- extra PTZ features 47

---

## F

- factory defaults, restoring 82
- firewall information
  - client 20
  - server 14

---

## I

- importing device and user information 84
- inactivity timeout, default setting 87
- installing
  - client 22
  - exported recordings player 57
  - server 15
- installing, NVR 73
- IP address, determining 88

---

## L

- layout
  - specifying 43
- licensing 10
- licensing NVR 78
- live video
  - controls 42
  - snapshots 45
  - starting 44
  - stopping 44
- location
  - text 35
- logging
  - disabling 94
  - enabling 93
- logging in to server 26

---

## M

- main menu 43
- map-links, associating with devices 40
- mapsets
  - adding 40
  - configuring 40, 61
  - deleting 41
- moving PTZ 46

---

## N

- NVR
  - activating 78
  - configuring 79
  - expected performance 77
  - installing 73
  - licensing 78
  - partition groups 96
  - partitions 96
  - pre-installation 71
  - prerequisites 70
  - starting 74
  - stopping 74
  - troubleshooting 76

---

## O

- opening
  - command prompt 88
  - run dialog 88
- overview of system 6

---

## P

- pane layout 43
- partition groups, NVR 96
- partitions
  - on NVR 96
  - selecting 97
- password
  - expiry, default 87
  - history count, default 87
  - reminder, default 87
- passwords, changing 29
- persisted layout, loading 87
- ping command, using 92
- playback offset time default 87
- player, exported recordings 56
- playing back recordings 51
- port numbers, specifying 35
- pre-installation 71
  - client 20

- exported recordings player 57
  - server 13
- prerequisites 70
  - client 19
  - exported recordings player 56
    - server 13
- previous layout, displaying 87
- profiles, audit trail 60
- PTZ
  - activating 46
  - configuration 39
  - control 46
  - extra features 47
  - moving and zooming 46
  - timeout, default 87

---

## R

- recording footage
  - displaying 51
  - synchronising 55
- recording jobs
  - deleting/disabling 81
  - editing 80
  - scheduling 79
- recording partitions 96
- recordings
  - exporting 55, 56
  - playing back 51
  - taking snapshot 54
- recordings, starting on alarm 81
- restoring factory defaults 82
- reusing devices, users and groups 83, 84
- run dialog, opening 88

---

## S

- scheduling recording jobs 79
- server
  - firewall information 14
  - installation 15
  - logging in 26
  - pre-installation 13
  - prerequisites 13
  - starting 16
- site backup 83
- snapshot, default location 87
- snapshots
  - live video 45
  - recorded video 54
- specifying
  - location 35
  - pane layout 43
- specifying port numbers 35
- starting up
  - client 25
  - server 16
- starting up live video 44
- starting up NVR 74
- stopping
  - live video 44
- stopping NVR 74
- stream settings, configuring 8
- supported devices 95
- synchronising recording footage 55

- system
  - components 6
  - information, viewing 84
  - licensing 10
  - overview 6

---

## T

- triggers, configuring 38
- troubleshooting NVR 76

---

## U

- user groups
  - adding 32
  - configuring 32
  - deleting 33
- user information
  - exporting 83
  - importing 84
- users
  - adding 28
  - changing passwords 29
  - configuration 28
  - creating new 28
  - deleting 31
  - disabling 30

---

## V

- video pane layout 43
- video sources, configuring 38
- viewing
  - system information 84
- viewing client defaults 85
- viewing, alarm properties 49

---

## W

- watermark, default 87
- Windows Events Viewer 89
- Windows Services 90

---

## Z

- zooming PTZ 46

