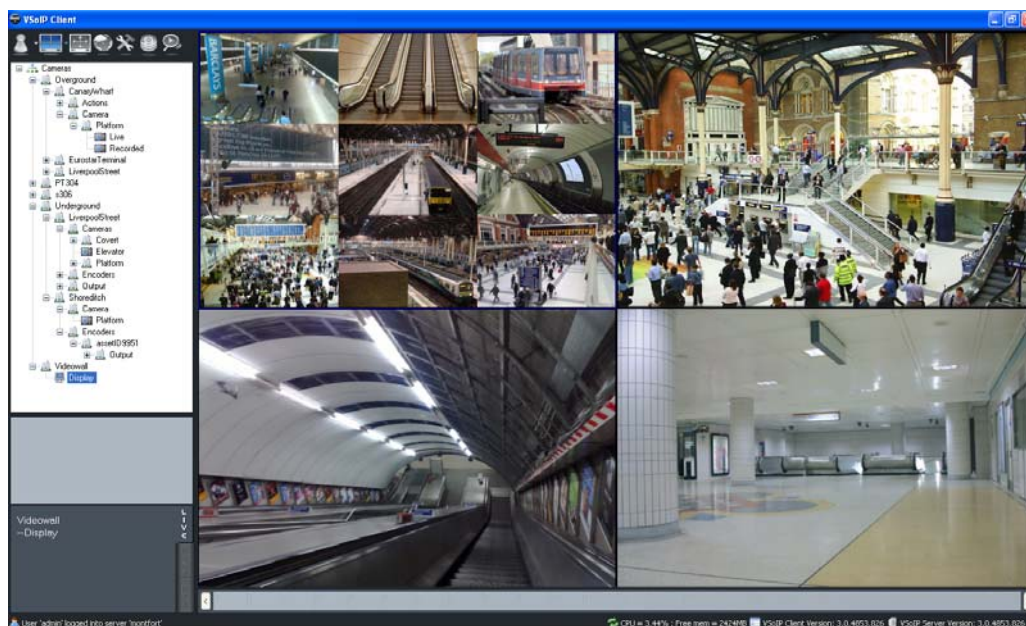


MANAGEMENT SOFTWARE

VSOIP 3.0 SUITE

VIDEO-WALL USER MANUAL



QAWZ®



Table of Contents

About This Guide	4
Safety Terms and Symbols	4
1 Installing the Video-wall	5
Video-wall Overview	5
Prerequisites	5
Preparations	6
Installing the Video-wall	11
Exiting the Video-wall	11
Offline Activation	12
Activating a Trial Version of the Video-wall	13
2 Using the Video-wall with a Web Browser	14
Prerequisites	14
Opening the Video-wall	15
Overview of the Video-wall Configuration Website	16
Adding a Device	16
Controlling Screen Layout	18
Starting Video	18
Stopping Video	19
Enabling “With Motion” Device Support	19
Advanced Features	22
Debug Mode	22
Maximum CPU Utilisation	22
Programmatic Control of Video-wall	23
3 Using the Video-wall with a Client	24
Prerequisites	24
Adding the Video-wall to your Surveillance Site	25
Connecting to the Video-wall	25
Disconnecting from the Video-wall	26
Controlling Screen Layout	26
Starting Video on a Video-wall Pane	27
Stopping Video on a Video-wall Pane	27
4 Using the Video-wall with the onscreen menu	28
Prerequisites	28
Opening the Video-wall	28
The Video-wall Menu	28
Adding a Video Source Device	28
Controlling Screen Layout	29
Starting Video	29
Stopping Video	30
Accessing Device Web Configuration Pages	32
Appendix A — Maintenance Information	33
Opening a Command Prompt in Microsoft Windows	33
Opening the Run Dialog	33

Finding out the IP Address of your Computer	33
Configuring Application Log to Overwrite Oldest Entries.....	34
Checking Connectivity of a Networked Device or Computer.....	34
Troubleshooting	35
Providing Technical Support Information.....	36
Index.....	38

About This Guide

The VSoIP Video-wall is a Windows XP Professional application designed to make a high-performance PC simultaneously display video from several different brands of video encoder sources over networks.

This document provides you with the basic information necessary to install, configure and make use of the Video-wall.

Safety Terms and Symbols

These terms may appear in this manual:

Table 1 Safety terms and symbols

Caution	Cautions identify conditions or practices that may result in damage to the equipment or other property
Warning	Warnings identify conditions or practices that could result in equipment damage or serious personal injury

Chapter 2 – Installing the Video-wall

This chapter contains the following information:

- Video-wall Overview
- Prerequisites
- Preparations
- Installing the Video-wall

Video-wall Overview

The Video-wall is software that converts a PC running a Microsoft Windows XP Professional (or later) operating system and several video displays into a dedicated Video-wall system. All of the screen area is used for surveillance – Windows taskbar, desktop, caption and borders are not shown. Video sources from different manufacturers can be displayed simultaneously, irrespective of the encoding used – MxPEG, H.264, MPEG4, M-JPEG or Wavelet.

It can be used in the following ways:

- Configuration and control using a web browser (Internet Explorer version 7 and above recommended). Video is not displayed in the web browser but in the Video-wall application itself. This web browser can either be:
 - On a second PC networked to the PC running Video-wall. This method of use is particularly suitable where the mouse and keyboard have been removed from the PC used for the Video-wall.
 - On the PC running the Video-wall. This “embedded” web browser is accessed using the onscreen menu.

For more information see the chapter entitled “Using the Video-wall with a Web Browser”.

- Configuration and control using the onscreen menu with a keyboard and mouse. This method is suitable only where mouse and keyboard are connected to the PC using the Video-wall. For more information see the chapter entitled “Using the Video-wall with the onscreen menu”.
- Configuration and control using a client. For more information see the chapter entitled “Using the Video-wall with a Client”.

Prerequisites

Hardware

The following hardware is required:

- Workstation grade, 32bit x86 architecture, single processor or multi-processor based personal computer.
- 2.4 GHz, or higher CPU speed – benchmark: Intel® Core™ 2 Quad Q6600 Quad Core Processor
- 2GB of memory.
- 5600 RPM hard disk drive speed.
- 160MB of hard drive space for operating system .Net Framework (v3.5) and Client software.
- 100-Base T network card configured for full duplex.
- A very 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 when these two types of hardware enabled acceleration are present, some graphics systems 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 adaptor 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 SP1 – 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 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.

Preparations

Dedicate a Windows XP Professional PC

The PC running the Video-wall should be specifically customised to be suitable for single purpose use; the Video-wall application runs so that it obscures the entire screen area so the PC cannot be used for another purpose whilst acting as a Video-wall. All software that does not form part of the system should be removed from the PC.

Networking – Firewall Information

The Video-wall requires an open HTTP port on any local software firewall. On starting, the service attempts to use port 80 (the standard HTTP web-page port). If this is in use, then the port serviced will be port 8000, then 8001, and so on.

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 Video-wall PC.

Any local software firewall should either be disabled, or carefully configured to allow the Video-wall to contact 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 Video-wall 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 information

Application	Role	Default path	Port number	Note
setup.exe	Server installer	Installation media	80/TCP	The main installer for the Server — required to gain access to the internet to download prerequisite Microsoft software
Videowall.Server.exe	Server	C:\Program Files\GANZ\VSolP Videowall	80/TCP, or 8000/TCP (if 80 is in use)	Access to the Video-wall application

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

Note: The firewall information details the ports that must be open to allow remote control of the Video-wall from a configuring client, e.g. web browser. However, if IP cameras or encoders are on the untrusted side of the firewall, additional ports may need to be opened: typical ports for RTSP/RTP streams using TCP are 7070 and 554, and for RTSP/RTP streams using UDP, 20000 to 21024. TCP is preferred since fewer ports require opening. 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.

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

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

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

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

Use Direct-X diagnostics to determine which version of Direct-X the PC running the Video-wall 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 (March 2009) or a higher revision number.

Caution: If the graphics hardware driver is updated, then the Direct-X installer must be run again with the updated driver. Also be sure to observe any reboot requests. Do not ignore a reboot request and then install further system or application software.

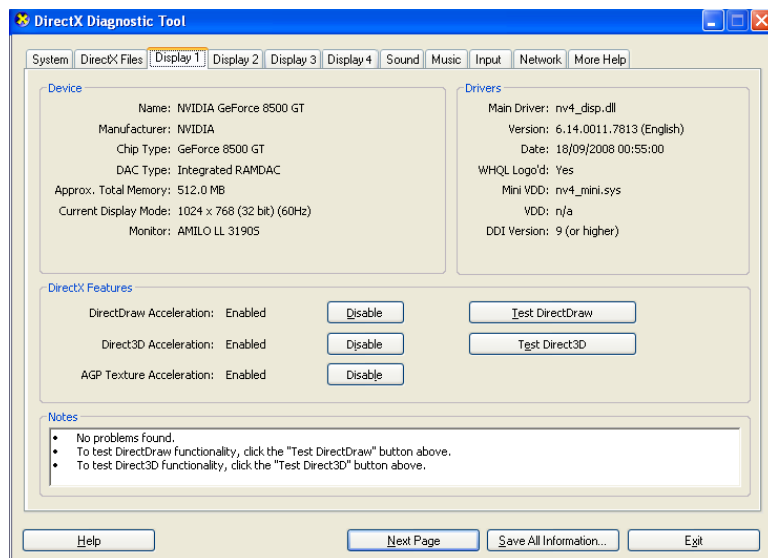


Figure 1 Using the Direct-X Diagnostic Tool

- 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 Video-wall.

Install .Net Framework

The Video-wall makes use of Microsoft's .Net framework to provide high levels of application robustness, security and efficiency. Windows XP Professional does not come with Microsoft .Net installed so when setting up the Video-wall server, Windows will obtain Microsoft's .Net framework directly from Microsoft's servers.

Rather than using the Internet, you can also install Microsoft's .Net framework from the CD before running the Video-wall's server setup program, restarting the PC as required.

Enable XP Automatic Login

The Windows XP PC used to run the Video-wall should be dedicated to that task. It must also be configured so that automatic login is used. If this is not done, manual intervention is required to log in so that the Video-wall's startup sequence can be initiated.

Please read Microsoft's Knowledge Base article 315231. This article explains how to enable XP automatic login. <http://support.microsoft.com/kb/315231/en-us>. You will have to enter various values into Windows Registry such as the administrator's login and password, and set the AutoAdminLogon value to one. You must add any missing entries (keys) to the Registry.

If you do not choose to enable automatic login, you must accept that should a system restart occur operator intervention will be required to enable the Video-wall to restart. Enabling XP automatic login is strongly advised since this assists in making the Video-wall's PC and software a turnkey device.

Alternatively you should consider uninterruptable power supply equipment to prevent the Video-wall from restarting due to power outages.

Switch off Automatic Windows Updates

Windows updates could cause issues and potentially force restarts of the Video-wall's PC. Since this might stop the Video-wall from functioning, we do not recommend automatic updates.

Operating system updates should be performed during scheduled surveillance system maintenance. This means that issues related directly to the update can be addressed immediately by maintenance personnel.

Also ensure that no software installed on the PC has an automatic updater e.g. the Java runtime, Apple QuickTime. Such updates often have a user interfaced element which could interfere with the operation of the Video-wall.

Switch off Screen Saver

Since no interaction with the keyboard or mouse occurs during normal use when the PC is used as a Video-wall, an enabled screen saver will activate and obscure the video display panes.

To prevent interference with the operation of the Video-wall, switch off the screen saver as follows:

- 1 From the Windows Start menu, select Control Panel.
- 2 Double-click the Display icon, or double-click the Appearance, Themes icon and then the Display icon.
- 3 In the Screen Saver tab, change the current screen saver to [none] and click Apply.

Note: Alternatively, you can open the Display settings by right-clicking the desktop background, choosing Properties and continuing as described above. Click OK when complete.

Switch off Power Saving

You should disable all power saving related to the monitor displays. To do this:

- 1 From the Windows Start menu, select Control Panel.
- 2 If present, open the Performance and Maintenance category, then open Power Options. Alternatively, open Power Options.
- 3 In the Power Schemes tab, locate the Turn Off Monitor and System Standby options and select Never.
- 4 Click Apply, then OK to exit.

Configure the “Soft Power” Switch to Shut Down

You may have removed the keyboard and mouse from the PC used for the Video-wall for security and tamper-proofing. Doing so prevents the PC being shut down using the normal Start menu shutdown technique. This presents the problem of how to initiate a shutdown. If your PC is fitted with a soft-power button, then the function of the power button on your PC can be set to command the PC to initiate a graceful shutdown. We recommend you configure the soft power switch as follows:

- 1 Open the Start menu, choose the Control Panel option, and then the Power Options (opening the Performance and Maintenance category as needed).
- 2 Click the Advanced tab and for the power-button option choose “Shut down”. For completeness, the sleep button option should be set to “Do nothing”.

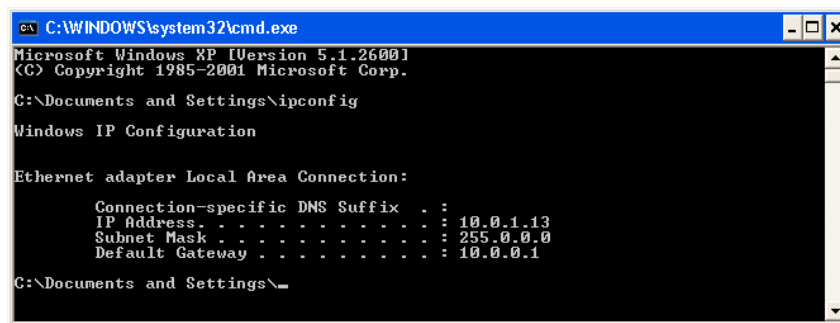
Disable/carefully Configure your Firewall

The Video-wall must be remotely configurable and must be able to obtain video streams from the required network devices. Considering these network connectivity requirements you must carefully configure any local firewall product, or completely disable the local firewall in favour of (for example) protection provided by a standalone, hardware-based firewall.

Determine the IP Address of the PC running the Video-wall

You must know the IP address of the PC running the Video-wall in order to configure the system. To determine this:

- 1 Open the Start menu and select Run. Alternatively you can press the Windows key and type r.
- 2 Enter `cmd` and click OK to open the command prompt.
- 3 Enter `ipconfig` into the command prompt and press Enter.

A screenshot of a Windows XP command prompt window. The title bar reads 'C:\WINDOWS\system32\cmd.exe'. The window content shows the following text:

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\ipconfig
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 10.0.1.13
    Subnet Mask . . . . . : 255.0.0.0
    Default Gateway . . . . . : 10.0.0.1

C:\Documents and Settings\
```

Figure 2 Running IPConfig command at Windows command prompt

The command prompt details information regarding the network settings of the PC running the Video-wall. Locate the entry IP Address and note the number shown. In Figure 2 this is 10.0.1.13.

Acquire an Activation ID

Without an activation ID, the Video-wall only runs in demonstration mode. Demonstration mode allows full operation of the Video-wall, but after a period of operation any video shown is overlaid with a semi-transparent image indicating that the software is not licensed.

If you have purchased the Video-wall then you will have been provided with an activation ID. This is a sequence of characters separated by dashes. An example of an activation ID is shown below:

ed7b5d61-f300-4c95-a981-a5e639a01efb

Ensure you have Access to the Internet During Setup

To operate the Video-wall in full rather than demonstration mode, it must be licensed. During the Video-wall setup, and every time you run a Video-wall that is currently in demonstration mode you are asked to activate the application. If you choose to not to use the Video-wall in demonstration mode, then you are asked to enter your Activation ID. The Video-wall then contacts a licensing centre over the Internet with this ID. If you have a firewall protection product installed, this must be set to allow the Video-wall access to the Internet.

Readiness Checklist

Review the following check list and check that you have:

- An Activation ID and access to the Internet, if running in full mode.
- A Windows XP PC dedicated to the Video-wall duties.
- Installed Direct 3D hardware support and Microsoft Direct-X 9.0c (March 2009) or above.
- Installed .Net framework.
- Enabled XP automatic login
- Switched off automatic Windows Updates.
- Switched off screen saver.
- Switched off power saving.
- Access to a second PC running IE 7 to be used to configure the Video-wall (if required).
- Configured "soft power" switch to shut down the Video-wall.
- Disabled or carefully configured the Video-wall's software firewall.
- The IP address of the PC running the Video-wall.

If you have satisfied the above conditions then proceed with the Video-wall software installation.

Installing the Video-wall

Caution: The Video-wall automatically starts up when users log in, i.e. it is installed as a member of the Startup applications group.

- 1 Run the setup.exe application. Check the “I accept the terms” box on the license dialog.

Note: By default, the installation folder is C:\Program Files\GANZ\VSolP VideoWall\.. To change this, click Advanced on the license dialog.

- 2 After accepting the terms and conditions, you are prompted to license the Video-wall. You can:
 - Use a trial license. Trial licenses allow access to all standard functionality, but video panes have text obscuring the video being displayed. If you later upgrade to a full version, you must activate that version; see “Activating a Trial Version of the Video-wall” on page 13.
 - Use an existing license from a previous installation.
 - License the Video-wall offline. Use this option if you are installing the Video-wall on a PC with no Internet access. See “Offline Activation” on page 12.
 - Enter a new license key to activate the Video-wall. You must obtain a license key from your vendor before continuing with the installation.
- 3 If required, enter the license key you have been given and click Check License. The system indicates whether or not the activation has been successful.

Caution: You should only enter the license key if you wish to license the software on the PC being used, as the licensing server will activate the license and lock it to the PC.

- 4 Click Next to complete the installation.

If activation fails, please check the following:

- Have you used the correct Activation ID?
- Has a trial Activation ID expired?
- Has the Activation ID already been used by a different computer?
- 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 license file to local hard disk? Ensure you are attempting to license the Video-wall using an account with administrator level privileges.
- In geographical regions where different calendar types are used, please ensure your regional Date/Time setting is set to use the Gregorian calendar.

Exiting the Video-wall

With a keyboard attached to the Video-wall's PC it is possible to exit the Video-wall application by holding the ALT key and pressing the F4 key. Stopping the Video-wall using a key-sequence is deemed a security risk; it is therefore advised that the keyboard and mouse are locked away or electronically disabled. If this is impossible, then we recommend that you run the Video-wall without a keyboard or mouse attached. To shut down the PC running the Video-wall in this case, use the soft-power key.

Offline Activation

Note: This section applies only if you selected Use Offline Activation during installation. You must have an activation ID before attempting to activate this software. Obtain this from your software vendor.

If the computer on which you are installing the Video-wall is not connected to the Internet, you can activate it from a computer which is connected, as follows:

- 1 Select Use Offline Activation during installation, then click Next.
- 2 Navigate to the folder where you want to save the license data, or accept the default and click Save License Data.

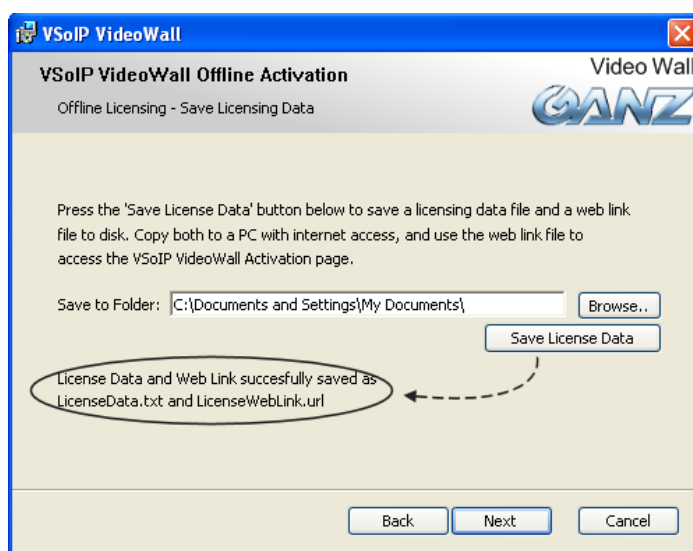


Figure 3 Offline licensing

- 3 Navigate to the LicenseWebLink.url file and open it to access the activation page:

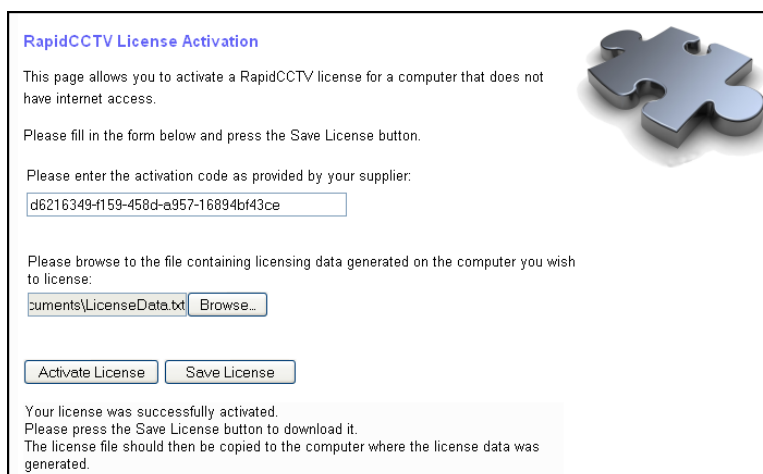


Figure 4 Activation web page

- 4 Enter the activation code you have been given, and browse to the folder where the license data was saved.
- 5 Click Activate License. The licensing data and activation key are sent to the license server. If everything is correct, text appears indicating that the license was successfully activated. Otherwise, you must contact your software vendor supplying details of the key used.
- 6 If successful, click Save License to save the license to the computer where the license data was generated.

- 7 Return to the License Activation dialog and click Next, then enter the activation code. Browse to the folder where the new license data has been saved, and click Copy Activated License.

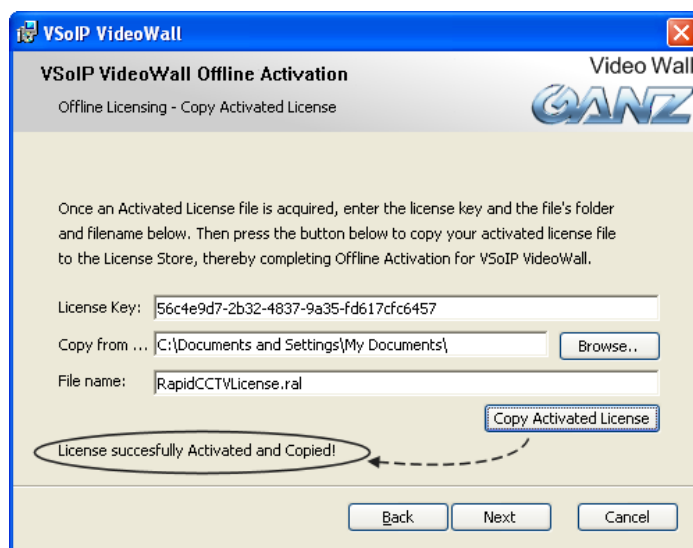


Figure 5 Offline activation

- 8 If activation has been successful, click Next to continue the installation process. If not, see "Installing the Video-wall" above for reasons why installation might have failed.

Activating a Trial Version of the Video-wall

Note: The following section applies only if you have first installed a trial version of the Video-wall.

Prior to unrestricted use, the full version of the Video-wall must be activated. Activation is typically performed over the Internet and requires an activation ID. Activation is a one-time process. Once activated, a non-trial activation ID does not need reactivating.

Note: Activation IDs are tied to various products even though they look very similar. Please be sure that you use the correct 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 license file generated by activation is lost, then the ID originally used to license the Video-wall can be reused to re-activate it.

To activate a full version of the Video-wall, locate the Video-wall Licensing Helper component in the Windows Start menu.

- If your computer can connect to the Internet, enter the License Activation Key you have been given, then click Activate License. Activation may take a few seconds. Activation success, or failure, will be indicated.
- If your computer cannot connect to the Internet, click to activate the Video-wall offline, and follow the instructions in "Offline Activation" on page 12.

If activation fails, see "Installing the Video-wall" on page 11 for possible reasons.

Chapter 3 – Using the Video-wall with a Web Browser

This chapter contains the following information:

- Prerequisites
- Opening the Video-wall
- Overview of the Video-wall Configuration Website
- Adding a Device
- Controlling Screen Layout
- Starting Video
- Stopping Video
- Enabling “With Motion” Device Support
- Advanced Features
- Programmatic Control of Video-wall

Caution: This chapter describes how to use the Video-wall with a web browser.

The Video-wall contains an “embedded” web browser which can be used to add devices and carry out other configuration. However, if you have not attached a keyboard or mouse to your Video-wall computer, then you must carry out this configuration using a second networked PC.

It is also possible to configure and use the Video-wall using Client software or with the on-screen menu. However, it is not advisable to use two methods simultaneously. It is recommended that you select one and then use it exclusively to control the Video-wall.

Although a web browser is used to configure and control video display, video is not displayed within the web browser, but rather in the Video-wall application you have installed.

Prerequisites

The following section assumes the following:

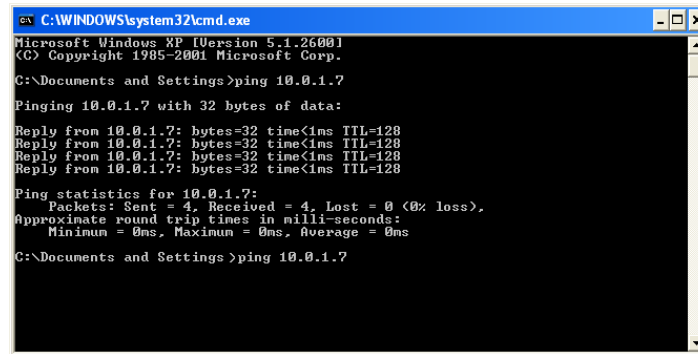
- The Video-wall server Windows application has been installed on the display PC.
- The Video-wall PC is running.
- The Video-wall PC is showing a video layout of a series of slightly tinted dark rectangles each representing a video display area.
- The IP address of the PC running the Video-wall is known.
- If there is no mouse or keyboard attached to the PC running the Video-wall, you require a second PC networked to the PC running the Video-wall (for configuration purposes only). The second PC is used throughout the configuration process. On the second PC, open Internet Explorer 7 (or above). In the address bar, type the IP address of the Video-wall, e.g. <http://10.0.1.13>. The Video-wall configuration website is displayed.

Note: If a port other than 80 is used, then specify this in the URL entered into the address bar. For example, if port 8000 is in use, then the URL to use would be <http://10.0.1.13:8000>.

Connectivity Troubleshooting

If you obtained a connection error, check that you typed the address correctly and that the Video-wall is running — the Video-wall should be showing a series of slightly tinted dark rectangles.

To check connectivity from your configuration PC to the PC running the Video-wall use the Windows ping command from the command prompt.



```
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>ping 10.0.1.7
```

Figure 6 Using the ping command

The ping command sends a message to a specified IP address and if the computer with that IP address receives the message and can respond, then it issues a reply. Ping requests and responses can be prevented by firewalls.

If you are certain that the IP address of the PC running the Video-wall used by the ping command is correct, then do the following:

- Check the network cabling between your configuration PC and the cabling for the Video-wall.
- Check for software firewalls on both PCs — ensure that they are correctly configured, or disabled.
- Confirm that you are able to view web sites from the Internet at large.

Opening the Video-wall

During installation, the Video-wall is added to the Startup menu. This means it should open automatically when you start or reboot the PC, and you should not have to start it manually.

Note: The Video-wall may take up to a minute to start. To determine if it is running, use Windows Task Manager, as follows:

- 1 Press the Ctrl, Alt and Delete keys together once.
- 2 Click Task Manager.
- 3 Click the Processes tab, and look for Videowall.Server.exe in the list of processes.

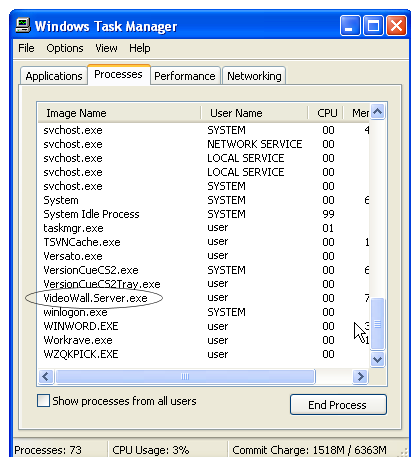


Figure 7 The Video-wall application shown in Windows Task Manager

If you have closed the Video-wall, select Programs>VSoIP Videowall>VSoIP Videowall from the Start menu to re-open the application.

Overview of the Video-wall Configuration Website

The Video-wall configuration website is available using both the embedded and remote web configuration pages, and allows you to:

- Make permanent and persistent connections to video sources at various positions on the Video-wall.
- Choose from a set of video layouts.
- Add or remove video sources.
- View version information.

The website contains a left-hand menu which provides access to various configuration options:

- Display setup.
- Screen layout.
- Device configuration.
- System configuration.

Adding a Device

To add video sources to the Video-wall:

- If using the embedded web pages, click the screen anywhere to reveal the menu, then select Settings.
 - If using a second PC for configuration, enter the IP address of the Video-wall PC into the browser and press Return.
- 1 On the web configuration pages which appear, select Device Config from the left-hand menu.

Figure 8 Adding devices

- 2 Choose the video source from the sources listed in the Platform drop-down list.
- 3 Enter at least an IP address and a memorable name for the source.

Depending on your chosen device you may need to format the IP address entry in a particular way, e.g. the video input port. IP addresses are in the usual three dots form, e.g. 10.0.62.1. If required, a network port can be added if one has been configured on the device. e.g. 10.0.62.1:554

- 4 Enter an input port, if required. For most devices, a value of 0 is acceptable.

Note: On Bosch VIP-x multi-input multi-encoder devices, the following input ports are valid:

Table 4 Port usage for multi-input multi-encoder devices

00	analogue input 0	encoder 0	20	analogue input 2	encoder 0
01	analogue input 0	encoder 1	21	analogue input 2	encoder 1
10	analogue input 1	encoder 0	30	analogue input 3	encoder 0
11	analogue input 1	encoder 1	31	analogue input 3	encoder 1

Video input port details relate to what analogue input (and encoder) the video should be sourced from. All port numbers are 0-based i.e. for Bosch platforms, on a single analogue input and single encoder unit, the input port would be 00.

- 5 If the device has username and password access protection, enter these in the username and password fields.
- 6 If you are adding a “with motion” device, enter an event duration. The Video-wall can display video from “with motion” cameras when a motion event occurs. The event duration is the length of time that video from that camera remains on screen, once the *last* motion event has been received from that camera.

Note: You must enable “with motion” device support to display video from “with motion” devices when a motion event occurs. See “Enabling “With Motion” Device Support” on page 19.

- 7 Select Add Device. The device is added to the system.

Note: The Video-wall does not contain a method of adjusting the operational settings of platforms, e.g. video quality, motion detect sensitivity, etc. To adjust a platform’s settings you should use the web-page or application as described by the platform’s manufacturer.

Controlling Screen Layout

To control how video is displayed on the Video-wall:

- If using the embedded web pages, click the screen anywhere to reveal the menu, then select Settings.
 - If using a second PC for configuration, enter the IP address of the Video-wall PC into the browser and press Return.
- 1 Select Screen Layout, then the layout that you want to use.
 - 2 You can choose from several layouts. Clicking on the layout representation immediately causes the Video-wall to switch to that layout. The current selection is highlighted in red.

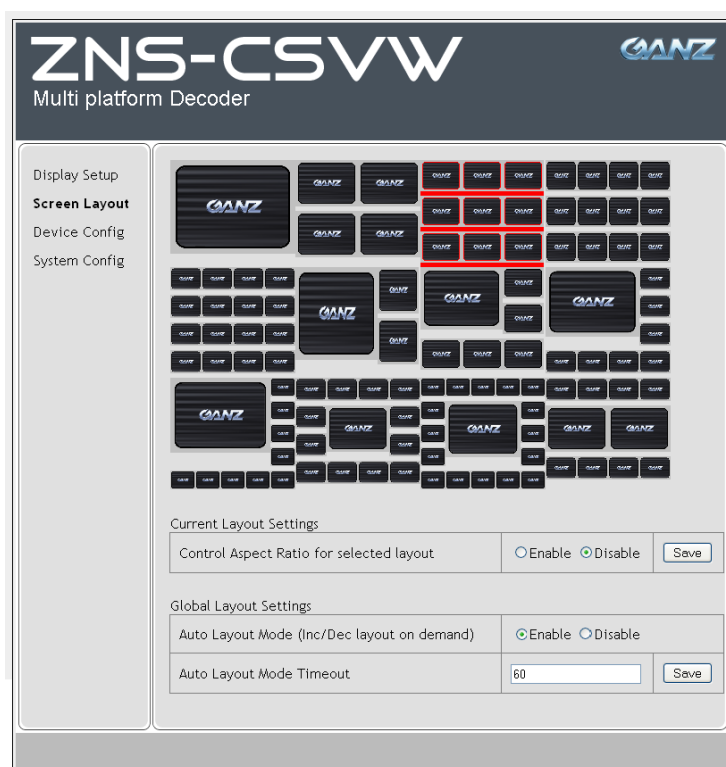


Figure 9 Video-wall layout options

Video within a video display area normally stretches to fill the full area. This can distort the proportions of the video and may not be acceptable in all circumstances. To prevent distorted video, set Control Aspect Ratio to Enabled.

Note: The current Control Aspect Ratio setting applies only to the selected layout. Once enabled for a specific layout, the setting is retained for that layout.

Global Layout Settings

These refer to settings that affect all layouts. For more information, see “Enabling “With Motion” Device Support” on page 19.

Starting Video

To display video in the Video-wall:

- If using the embedded web pages, click the screen anywhere to reveal the menu, then select Settings.
 - If using a second PC for configuration, enter the IP address of the Video-wall PC into the browser and press Return.
- 1 Select Display Setup from the left-hand menu.

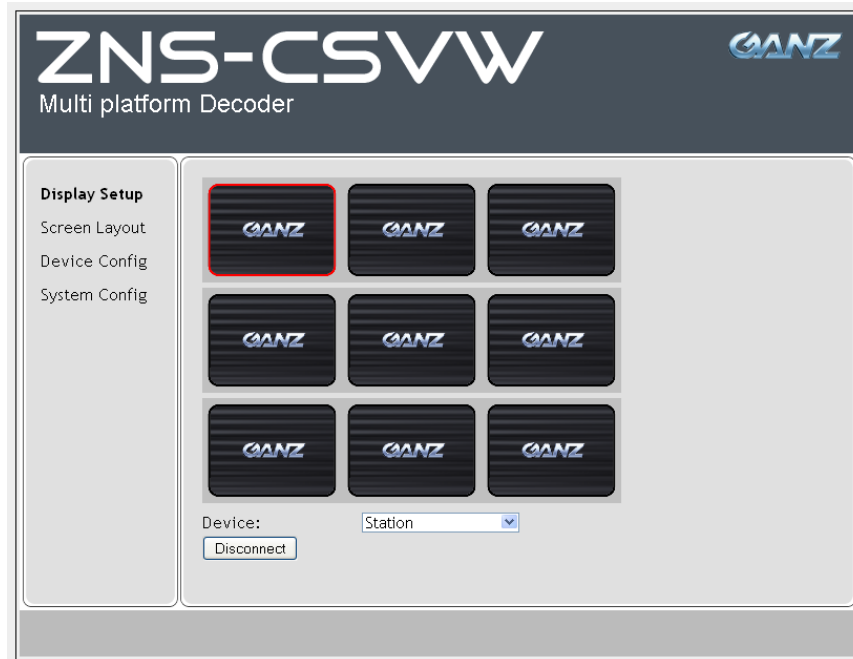


Figure 10 Displaying video

- 2 Select the video display area in which you wish to display video. The selected video display area is highlighted in red.
- 3 Open the Device drop-down list and choose the video source you want to display in this area. Video from this device is displayed on the Video-wall in the selected position.

Note: The video display area on the web-page does not show video from the camera. Note also that video display areas on the web-page do not show which panes are in use. The current state of the Video-wall is determined by observing the monitor(s) connected to the PC running the Video-wall.

Once video is started in this manner, video from the selected source is displayed in the video display area until it is stopped by a user command. If the PC running the Video-wall is shut down and restarted, video will be reconnected automatically. If a video source is no longer available, the Video-wall will repeatedly retry to connect the video feed until a connection is achieved or the user stops the connection attempt, by selecting the appropriate display area that matches the one retrying and clicking Disconnect (see Figure 10).

The text “Connecting” is displayed whenever the Video-wall has been commanded to obtain video from a device but has not yet received any video.

Stopping Video

To stop video displaying in a video pane:

- 1 Confirm the position on the Video-wall for the video to be stopped.
- 2 Select the matching position on the Display Setup web-page (Figure 10). The selected video display area is highlighted in red.
- 3 Click Disconnect to stop the video (or any repeating reconnecting attempts) in the selected area.

Enabling “With Motion” Device Support

The Video-wall can display live video from “with motion” devices when a motion event occurs. For this to happen, you must enable “with motion” device support, as follows:

- If using the embedded web pages, click the screen anywhere to reveal the menu, then select Settings.

- If using a second PC for configuration, enter the IP address of the Video-wall PC into the browser and press Return.
- 1 Select System Config from the left-hand menu.

ZNS-CSVW Multi platform Decoder	
Display Setup	Application Information:
Screen Layout	Version: 1.5.1010.46
Device Config	Version Date: 09/07/2009 16:02:00
System Config	<div>Installed System Modules</div> <div>Bosch Video Motion Event Module <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled</div>

Figure 11 System Configuration web-page

- 2 Set the Video Motion Event Module to Enabled.

This means that video from a “with motion” device is now automatically displayed on screen when a motion event occurs on that device, and automatically stops after a period of time (as specified when adding the "with motion" device, shown in Figure 12).

ZNS-CSVW Multi platform Decoder	
Display Setup	Platform: Bosch MPEG4 with Motion
Screen Layout	Parameter Value
Device Config	Address: 10.0.17.12
System Config	Input Port (00..31): 00
	Name: Door Entry
	Description:
	Username:
	Password:
	Event Duration (sec): 10
	<input type="button" value="Add Device"/>

Figure 12 Setting the Event Duration for an individual device

Note: The Video-wall interprets this duration as the length of time that video from that device remains on screen, once the *last* motion event has been received from that device.

Increasing/Reducing Video Panes

The Video-wall can increase or reduce the number of video panes shown on screen, according to motion events received from devices and the availability of vacant panes.

To enable this functionality, select Screen Layout from the left-hand menu.

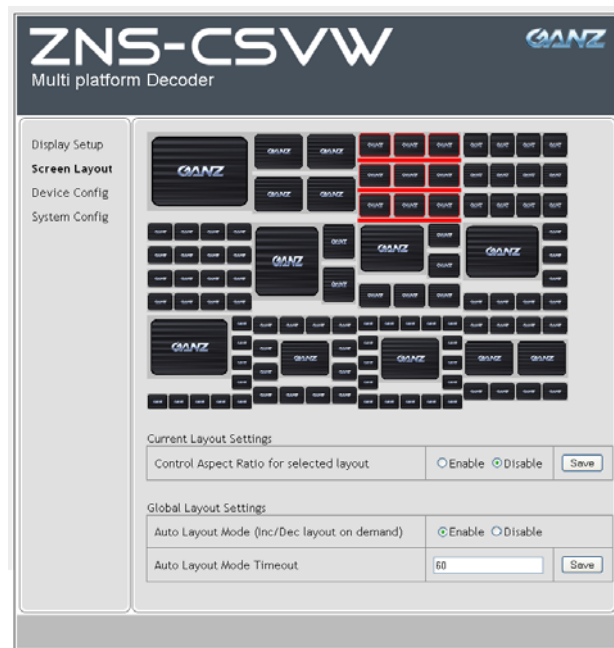


Figure 13 Video-wall layout options

- **Auto Layout Mode** — When enabled, the number of video panes shown on the Video-wall reduces or increases according to motion events received by the server and the availability of vacant panes. Only devices that have a “with motion” entry react in this manner.
- **Auto Layout Mode Timeout** — The Video-wall continuously analyses the number of video areas being used to display video. If the number of display areas used by the current layout is such that a smaller layout would make better use of the screen, **and** if no new video is displayed during the timeout period, then the layout is automatically changed to the smaller layout. The Auto Layout Mode Timeout prevents constant switching between layouts when video from a device automatically stops.

The following scenario describes a visitor entering a building with three “with motion” cameras: Door Entry, Corridor and Lift. Auto Layout Mode has been enabled on the Video-wall. The individual timeout values (set when adding the devices, see Figure 8) for the Door Entry, Corridor and Lift cameras are 10, 5 and 5 seconds respectively.

Time (secs)	Activity
T+0	Visitor approaches door entry system and triggers Door Entry camera motion sensor. Video starts displaying in a single pane.
T+5	Visitor enters building.
T+8	Visitor walks into corridor, and moves out of range of Door Entry camera. The timeout value for the Door Entry camera (10 seconds) begins when his last movement is detected.
T+8	Visitor triggers Corridor camera motion sensor. The Video-wall changes the display to 2x2 to display video from both Door Entry and Corridor cameras.
T+13	Visitor enters lift, and lift doors close. Lift camera starts displaying video. The timeout value for the Corridor camera (5 seconds) begins as there is no more movement in the corridor.
T+13	All three cameras now displaying video in a 2x2 display.
T+18	Video from Door Entry and Corridor cameras stop displaying as the timeout values have been reached. The Video-wall switches back to a single view displaying the Lift camera.
T+28	Lift reaches floor 3 and visitor exits lift, moving out of range of the Lift camera.
T+33	Lift camera's timeout value is reached and video stops displaying from this camera.

In this example, the Auto Layout Mode Timeout value is not required as the total time from start to finish is less than the 60 seconds specified in Figure 9. However, over a longer time period and with many more motion events, the display could be almost constantly switching between different layouts. The Auto Layout Mode Timeout prevents this from happening. If the Video-wall detects that the number of display areas used by the current layout is such that a smaller layout would make better use of the screen, **and** if no new video is displayed during the Auto Layout Mode Timeout period, then the layout is automatically changed to the smaller layout.

Advanced Features

There are a number of user-configurable options that are not exposed to the administrator via the web-page (or web-service) front-ends. These options are configurable from the settings.xml file located in the installation folder of the Video-wall's server application. This setting file is generated and populated with the Video-wall's basic settings when the Video-wall is run for the first time.

Note: The settings.xml is not listed in the installation folder after initial installation. The file is generated by running the Video-wall and then closing the application.

The settings.xml is read when the Video-wall application starts. Settings changes made will be used the next time the Video-wall is started.

If changes are to be made to this file, it is highly recommended that a copy of the file is made first as backup. It is also important to be sure that editing is carried out carefully since incorrect modifications could result in the Video-wall either not starting or starting with invalid settings.

Before making changes to the settings.xml file, ensure that you have shut down the Video-wall's server application. It is recommended that Windows NotePad is used to edit the settings.xml file.

Debug Mode

To prevent the Video-wall from obscuring the whole desktop and to run it within a window, change the following value from false to true.

```
<DictionaryEntry>
  <Key xsi:type="xsd:string">RunInDebugMode</Key>
  <Value xsi:type="xsd:string">true</Value>
</DictionaryEntry>
```

This is a useful mode of operation that allows a user to use a web browser to edit the Video-wall's server settings and view the results on the same PC.

Note: The window caption indicates the current system CPU and memory use — it is useful to observe system behaviour when viewing various platforms. This is useful when determining streaming and other platform settings that affect the load on the Video-wall.

Maximum CPU Utilisation

To prevent the Video-wall from being overdriven, an averaged percentage CPU utilisation by the whole system over the last few seconds is examined every time a connection is made. If the average system load is currently at or exceeding the maximum, the connection request is ignored. A value from 1 to 100 percent is valid. A maximum utilisation of 80% is the default.

```
<DictionaryEntry>
  <Key xsi:type="xsd:string">MaxCpuUtilisation</Key>
  <Value xsi:type="xsd:string">80</Value>
</DictionaryEntry>
```

The connection request can either be made via the web-page or from a motion detect event received by the Video-wall.

Programmatic Control of Video-wall

In addition to controlling the Video-wall using web-pages, it is also possible to interact with it via a web-service. Programmers interested in information about what is available can find out by entering the URL: `http://10.0.1.13/mpd.asmx`, where 10.0.1.13 is the IP address of the Video-wall. If a port number has been specified, then this should be appended to the IP address, for example the user has previously set the web serving port to port 8000, so the programmer would use the URL `http://10.0.1.13:8000/mpd.asmx`.

Note: The Video-wall must be running in order for the URL to be valid.

Chapter 4 – Using the Video-wall with a Client

This chapter contains the following information:

- Prerequisites
- Adding the Video-wall to your Surveillance Site
- Connecting to the Video-wall
- Disconnecting from the Video-wall
- Controlling Screen Layout
- Starting Video on a Video-wall Pane
- Stopping Video on a Video-wall Pane

Caution: This chapter describes how to use the Video-wall with Client software.

It is also possible to configure and use the Video-wall using a web browser, or with the onscreen menu. However, it is not advisable to use two methods simultaneously. It is recommended that you select one and then use it exclusively to control the Video-wall.

Prerequisites

The following section assumes the following:

- The Video-wall server Windows application has been installed on the display PC.
- The Video-wall PC is running.
- The Video-wall PC is showing a video layout of a series of slightly tinted dark rectangles, each representing a video display area.
- The IP address of the Video-wall is known.

To choose which video sources should be displayed on the Video-wall you must:

- 1 Add a Video-wall device to your site. The IP address of the Video-wall PC should be used.
- 2 Connect to the Video-wall.
- 3 Start displaying video in one of the Video-wall's panes.

Note: Video displayed in a pane continues to be displayed until a request is made to stop it.

Note: You can have more than one Video-wall device in your site — a client can then be used to manage several Video-walls.

The Video-wall has been designed as a stand-alone product. Once you have chosen a layout and started displaying video sources in panes, the Video-wall continues to show the chosen layout and video sources, even if the surveillance client or server is not running.

If the PC running the Video-wall is shut down and restarted, the Video-wall restarts the layout and video sources last shown.

If a video source is not reachable on the network, the Video-wall regularly checks to determine when the device returns. When it is again contactable, the Video-wall reconnects to the device during the next status check.

Adding the Video-wall to your Surveillance Site

To control the Video-wall using a client, you must add a Video-wall device to the client's surveillance site.

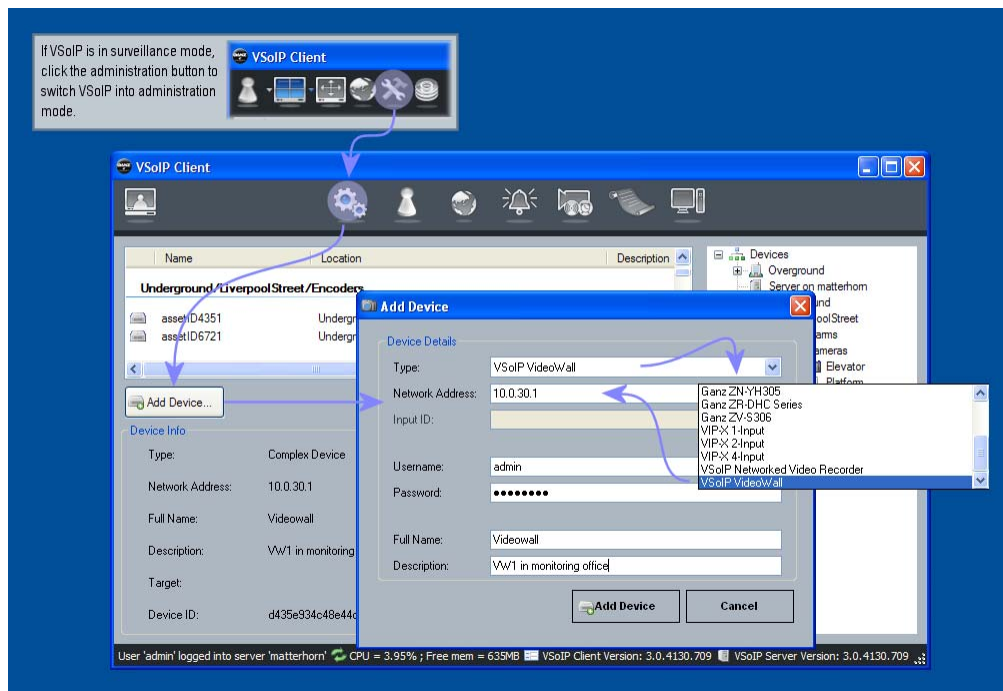


Figure 14 Adding the Video-wall to a site

Connecting to the Video-wall

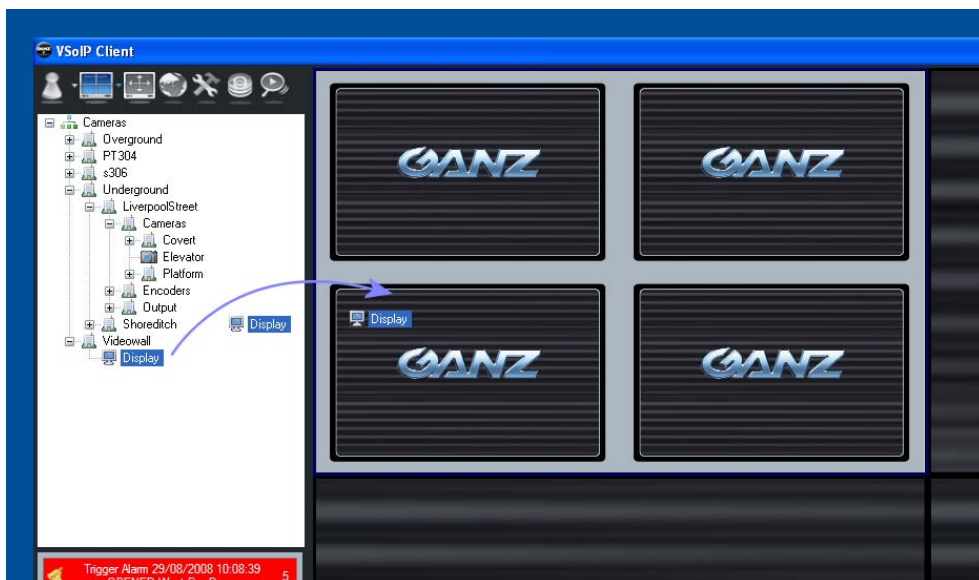


Figure 15 Connecting to the Video-wall

To connect to a Video-wall, drag the Video-wall device shown in the site onto a video pane. This establishes a direct, persistent connection between the Video-wall and the video source i.e. the video stream is not routed through the Server or any Client.

Note: The video displayed on the Video-wall PC continues irrespective of whether the Client or Server program is running and whether or not the user is viewing the Video-wall panes within the Client software.

Disconnecting from the Video-wall



Figure 16 Disconnecting from the Video-wall

To disconnect from a Video-wall, right-click any Video-wall pane and choose Disconnect Video-wall.

Controlling Screen Layout

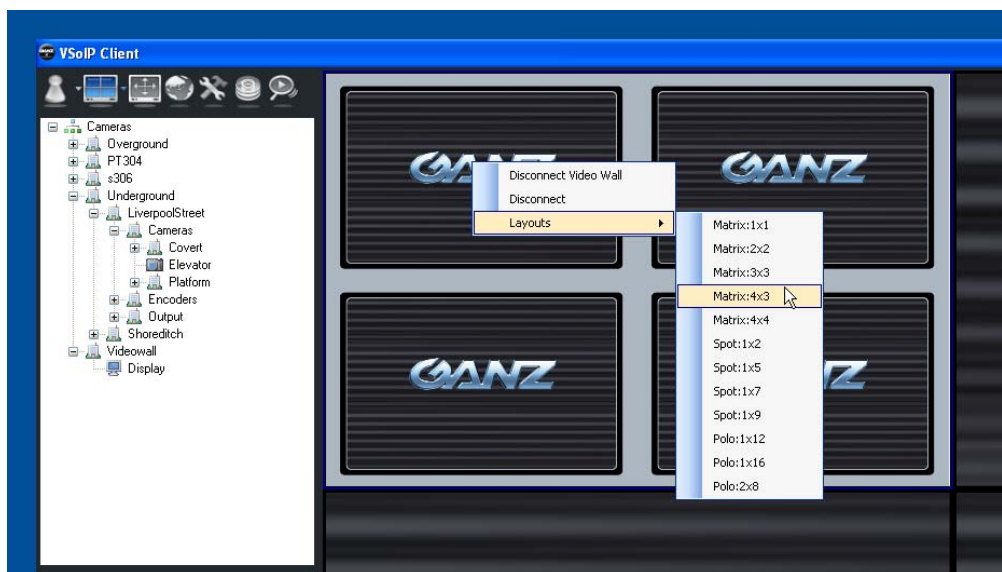


Figure 17 Changing the Video-wall layout

To change Video-wall layout, right-click any Video-wall video pane and select the required layout.

Starting Video on a Video-wall Pane

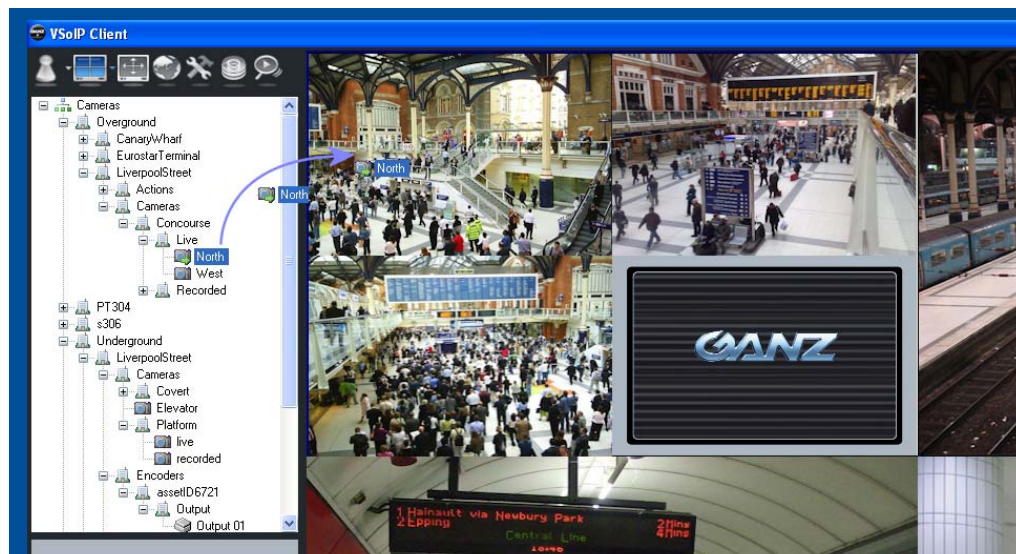


Figure 18 Starting video on the Video-wall

To start playing video on a Video-wall, drag and drop a camera onto one of the Video-wall panes. The Video-wall establishes a connection direct to the video source and displays video from it in the Video-wall pane.

Note: Other panes display single cameras as usual.

The position used corresponds to the pane that the video source was dropped on to in the Client.

Connection status and errors are shown within the video pane on the Video-wall in the Client. When successfully connected, every few seconds a snapshot of video will appear on the appropriate video pane of the Client.

Stopping Video on a Video-wall Pane

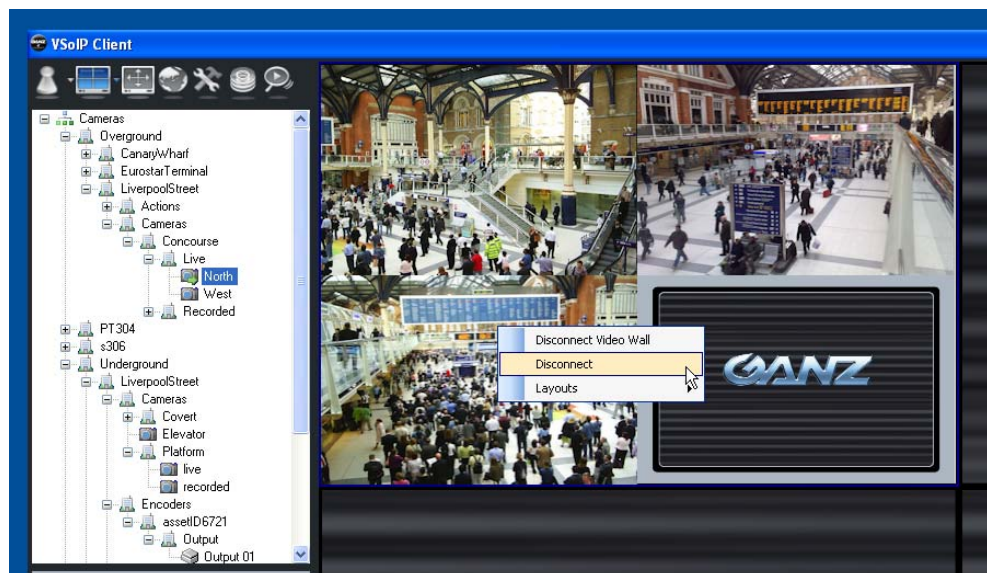


Figure 19 Stopping video on the Video-wall

Right-click the required Video-wall pane and select Disconnect to disconnect the video source for that pane. The Video-wall stops displaying video in the selected pane.

Chapter 5 – Using the Video-wall with the onscreen menu

This chapter contains the following information:

- Prerequisites
- Opening the Video-wall
- Adding a Video Source Device
- Starting Video
- Stopping Video
- Controlling Screen Layout
- Accessing Device Web Configuration Pages

Caution: This chapter describes how to use the Video-wall with a mouse and keyboard if these are available on the PC where the Video-wall is installed.

It is also possible to configure and use the Video-wall using a web browser running on a second networked PC, or with a Client. However, it is not advisable to use two methods simultaneously. It is recommended that you select one and then use it exclusively to control the Video-wall.

Prerequisites

The following sections assume the following:

- The Video-wall server Windows application has been installed on the display PC.
- The Video-wall PC is running.
- The IP address of the PC running the Video-wall is known.

Opening the Video-wall

During installation, the Video-wall is added to the Startup menu. This means it should open automatically when you start or reboot the PC, and you should not have to start it manually. To determine if the Video-wall is running, use Windows Task Manager, as described on page 15.

If you have closed the Video-wall, select Programs>VSoIP Videowall>VSoIP Videowall from the Start menu to re-open the application.

The Video-wall Menu

The Video-wall menu is hidden during normal operation. To reveal it, click the screen. Note that no mouse pointer is shown until after the initial left or right click. If no interaction is made with the menu items, the menu is automatically hidden.

The Video-wall initially opens with four video display areas known as "video panes", or just "panes". To start using the Video-wall, you must add video sources.

Adding a Video Source Device

To add a video source device (IP cameras and encoders) to the Video-wall, you must use a web browser (either "embedded" within the Video-wall or on a second PC) or a client. Please follow the instructions in the relevant chapter.

Controlling Screen Layout

To control the screen layout used by the Video-wall:

- 1 If the menu is not showing, click the screen anywhere to reveal it.
- 2 Select Layouts.



Figure 20 Controlling screen layout

- 3 Select the layout you require. The Video-wall immediately switches to that layout. Note that reducing the number of visible video panes automatically stops video playing in the hidden pane(s). If a layout is then chosen with more available panes, the video previously stopped when the number of available panes was reduced is not automatically re-started.

Note: Video within a video display area normally stretches to fill the full area. This can distort the proportions of the video and might not be acceptable in all circumstances. To maintain correct proportions, you must change the aspect ratio option using a web browser. See “Controlling Screen Layout” on page 18.

Starting Video

To display video in a Video-wall pane:

- 1 Ensure that you have added at least one video source for the Video-wall to show.
- 2 If the menu is not showing, click the screen anywhere to reveal it.
- 3 Select Cameras from the menu on the right of the screen.

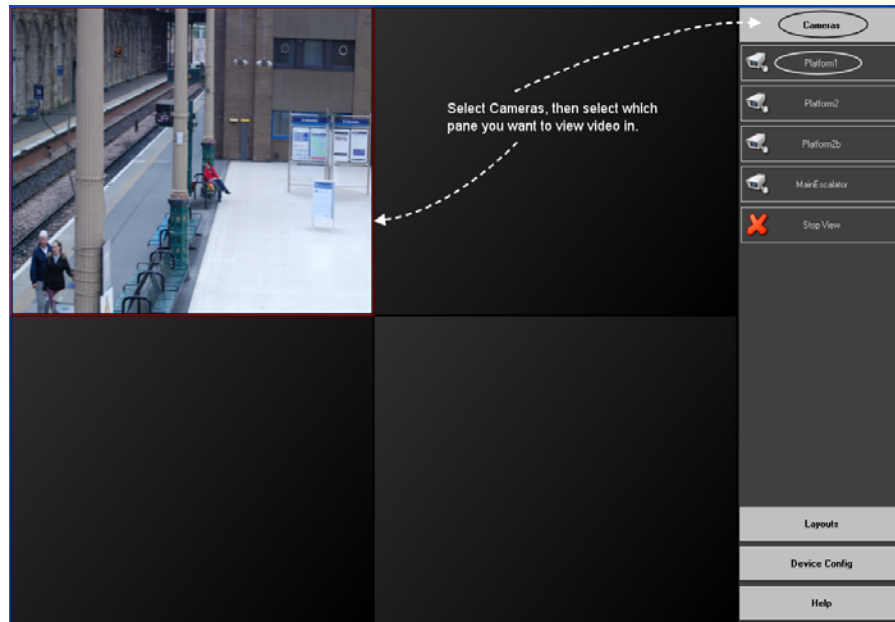


Figure 21 Displaying video in a video pane

- 4 Select the pane where you want to display video. A red border appears around that pane to indicate that it is the active pane.
- 5 Select a video source device to display video from that device in the selected pane. Video from that camera is displayed.

Note: Once video is showing, the Video-wall attempts to display the video source device at all times until video is stopped. If the video source is not available, the video pane will appear completely black. The Video-wall will occasionally attempt to reconnect to absent devices. The message "Connecting..." will be seen when the Video-wall attempts to reestablish a connection. If the Video-wall is shut down and then restarted, video source devices that were being displayed or absent at shutdown time will be automatically started.

Stopping Video

To stop video playing in a Video-wall video pane:

- 1 Select the pane displaying video you want to stop.

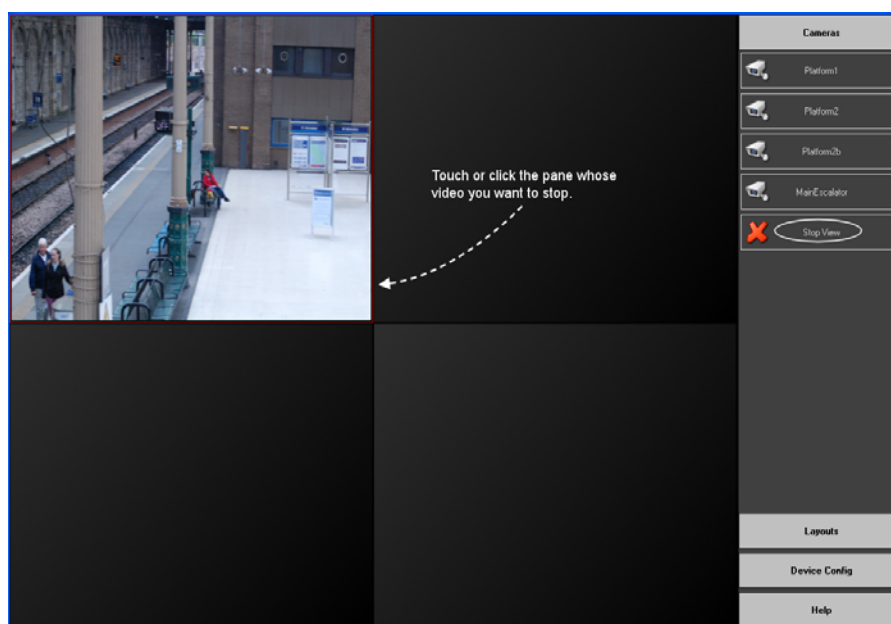


Figure 22 Stopping video in the Video-wall

2 Select Cameras, then Stop View.

Note: Once a video source device has been disconnected in this manner, the camera will not be automatically shown when the Video-wall is restarted.

Accessing Device Web Configuration Pages

The Video-wall allows you to alter a device's configuration using the device's own configuration web page (if available), as follows:

- 1 If the menu is not showing, click the screen anywhere to reveal it.
- 2 Select Device Config, then the device you want to configure.

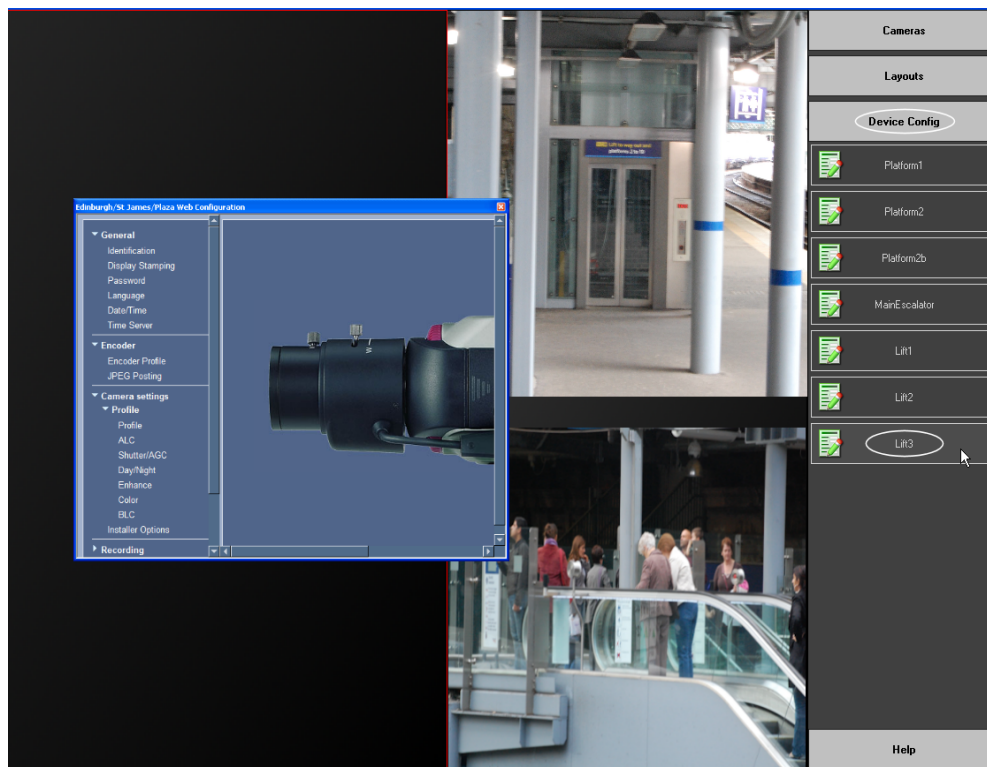


Figure 23 Accessing device web configuration pages

- 3 The device's web page appears in a new window.

Note: Only one device's configuration page can be open at any one time. You must close the web page before you can perform any other commands. Select the close button on the browser window to close the web page.

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 desired command. After typing the command hit the Enter (also called Return) key to perform the command.

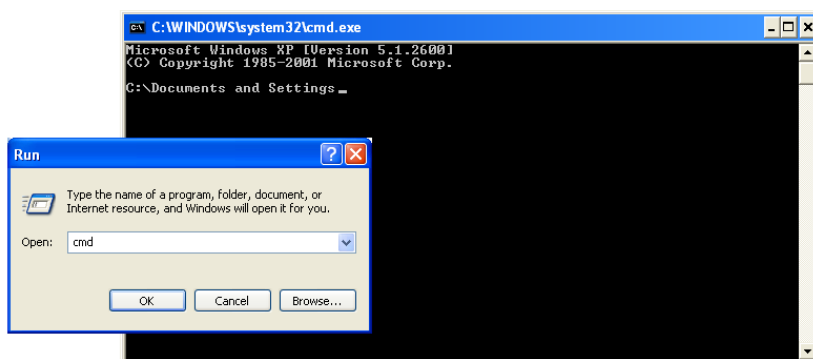


Figure 24 Opening a Windows command prompt

Opening the Run Dialog

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

Note: If the Start menu item Start>Run 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 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.

Configuring Application Log to Overwrite Oldest Entries

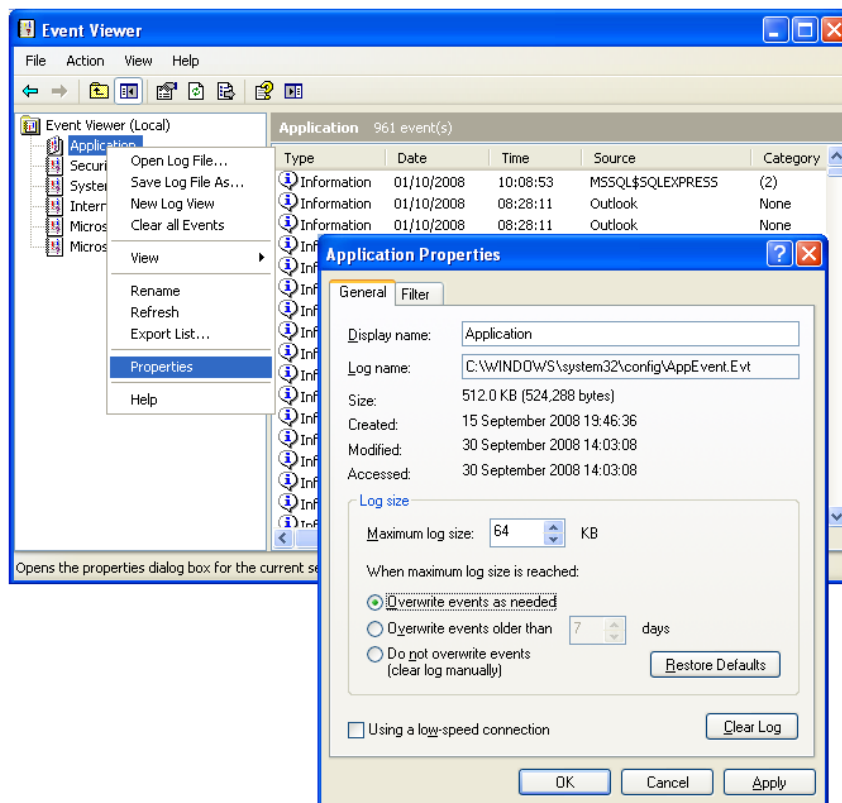


Figure 25 Changing Windows logging behaviour

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.

- 1 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.)
- 2 Open the Event Viewer.
- 3 Double-click the Application log.
- 4 Right-click the Application entry in the left-hand window and choose Properties.
- 5 In the Application Properties choose the General tab and in the Log size group click Overwrite events as needed, and click OK.

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.

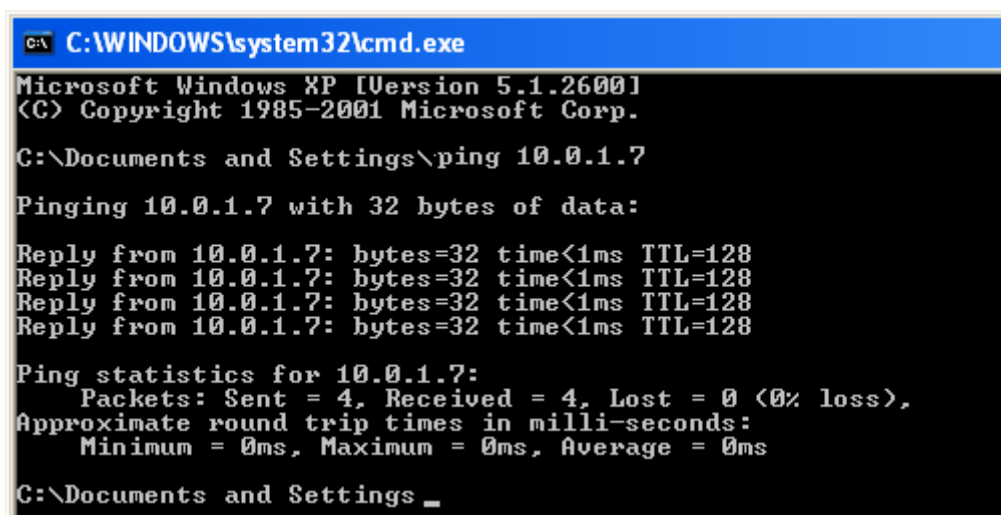
To use a ping you need to know the IP address of the network device you wish to find.

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.

Checking Connectivity Example

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.

- 1 Open a command prompt.
- 2 At the command prompt enter: **ping 10.0.0.1** and press the Enter (or return) key.
- 3 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 26 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 either:
 - In the installation folder of the software component and called `logging.config.disabled` (or some other name that distinguishes it from `logging.config`).
 - In a sub-folder of the installation folder.
 - Alternatively, you might be sent the file by a technical support representative.
- 2 Close the application you want to log.
 - For clients, exit the application.
 - For servers or NVR components, stop the service controlling the application.
- 3 Paste the `logging.config` file into the installation folder. (If necessary, rename it so that it is called `logging.config`.)
- 4 Start the application to be logged.
- 5 Note that a `log-roll.txt` file will appear in the application's installation folder.

Disabling Logging

- 1 Close the application currently being logged.
 - For clients, exit the application.
 - For servers or NVR components, stop the service controlling the application.

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

- 2 Remove the `logging.config` file from the installation folder by moving to a sub-folder, to another safe location, deleting it (if you have kept a copy) or renaming it to (for example) `logging.config.disabled`.
- 3 Start the application.

- 4 Note that after removing any log files in the application's installation folder, no more log files are added to the folder.

How Logging Works

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

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

This rolling behaviour has two undesirable side-effects:

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

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

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

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

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

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

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

Index

Symbols

.Net framework 8
"with motion" device support 19
"with motion" devices 17

A

accessing onscreen menu 28
activating
 offline 12
 trial version 13
activation failure, possible reasons 11
activation ID 10
adding devices
 using client 25
 using onscreen menu 28
 using web configuration 16
adding Video-wall to site 25
advanced features, web
 configuration 22
application
 installing 11
 opening 15, 28
auto layout 21
auto layout mode timeout, uses 21
automatic login 8
automatically adjusting video panes 20

C

changing layout
 using client 26
 using onscreen menu 29
 using web configuration 18
checking connectivity 15, 34
client
 changing layout 26
 connecting to application 25
 disconnecting from application 26
 starting video 27
 stopping video 27
closing application 11
command prompt, opening 33
computer's IP address, determining 33
configuration website, overview 16
configuring
 soft power switch 9
configuring event duration 20
connecting to Video-wall 25
connectivity
 checking 15
 troubleshooting 15
controlling screen layout
 using client 26
 using onscreen menu 29
 using web configuration 18
CPU utilisation 22

D

determining

Direct-X version 8
IP address 9
devices
 "with motion" 17, 19
 adding 16, 28
Direct-X 6, 7
 diagnostics 8
disabling
 power saving 9
 screen saver 9
 Windows updates 8
disconnecting from Video-wall 26
displaying video
 using client 27
 using onscreen menu 29
 using web configuration 18
distorted video, preventing 6, 18

E

event duration, setting 20
exiting application 11

F

firewalls
 blocking ports 7
 configuring 6, 9

G

graphics systems, limitations 6

H

hardware prerequisites 5

I

ID for activation 10
input ports, for multi-input
 multi-encoders 17
installation
 activation 10
 application 11
 preparations 6
IP address, determining 9, 33

L

layout, changing
 using client 26
 using onscreen menu 29
 using web application 18
licensing options 11
limitations, of graphics systems 6

M

MegaPixel cameras 6
menu, accessing 28
motion events 19

O

offline activation 12
onscreen menu
 accessing 28
 adding devices 28
 controlling layout 29
 starting video 29
 stopping video 30
opening

command prompt 33
run dialog 33
troubleshooting 15
Video-wall 15

P

ping command 15
ports, blocking 7
power saving, disabling 9
prerequisites, hardware 5
preventing distorted video 18
programmatic control 23

R

reasons for activation failure 11
run dialog, opening 33
running application within a window 22

S

screen layout, controlling
 using client 26
 using onscreen menu 29
 using web configuration 18
screen saver, disabling 9
site, adding Video-wall to 25
soft power switch, configuring 9
software 5
starting video
 using client 27
 using onscreen menu 29
 using web configuration 18
starting Video-wall 15
stopping video
 using client 27
 using onscreen menu 30
 using web configuration 19

T

trial version, activating 13
troubleshooting
 connectivity 15
 starting application 15

V

video distortion, preventing 18
video panes, increasing/decreasing 20
video, displaying
 using client 27
 using onscreen menu 29
 using web configuration 18
Video-wall
 adding to site 25
 connecting to 25
 disconnecting 26

W

web configuration
 accessing 32
 adding devices 16
 advanced features 22
 controlling layout 18
 overview 16
 starting video 18
 stopping video 19
Windows updates, disabling 8

