

VIDEOINSIGHT



5.5 IP Server Administrator Guide

www.Video-Insight.com

© Copyright 2014 Video Insight, Inc. The information contained herein is subject to change without notice. The only warranties for Video Insight products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Video Insight shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation. Oracle and Java are registered trademarks of Oracle and/or its affiliates.

IP Server v5.5 Administrator Guide, February 2014

Contents

INTRODUCTION	7
SYSTEM OVERVIEW.....	8
PLANNING	11
Server.....	11
FAILOVER SERVER.....	13
NETWORK.....	13
Monitor Station.....	15
Web Client	15
Health Monitor	16
CAMERAS	16
LICENSING	16
Router configuration.....	16
STORAGE CONSIDERATIONS	17
DATABASE CONSIDERATIONS	18
SOFTWARE INSTALLATION.....	19
IP SERVER.....	19
Installation without an existing SQL installation.....	19
Installation with an existing SQL installation	22
Initialization	25
Activate Using Demo Mode	31
MONITOR STATION CLIENT	33
Adding servers manually.....	35
Adding servers automatically.....	36
WEB CLIENT.....	38
Configuring IIS.....	38
Accessing the Web Client.....	38
Using the Web Client	40
Layouts toolbar	43
High Speed mode.....	44
Configuration menu	45
Viewing recordings	48
Camera toolbar	49
Creating a clip	49
HEALTH MONITOR	50
CUSTOMIZATION	51
IP SERVER.....	52
Setup and Configuration tab.....	52
Cameras tab	53
Advanced tab	54
Health Monitor tab	56
Client Tab	57

Access Configuration tab	59
Contact Information tab	60
IP SERVER MANAGER.....	60
Accessing IPSM	61
Configuring IP Server	61
IPSM: Options	63
IPSM: System Log.....	65
IPSM: Network Options	66
IPSM: Diagnostics.....	67
IPSM: No Cameras	72
IPSM: Update Activation	72
MONITOR STATION	73
Main Dashboard.....	74
Main menu toolbar	74
Facility Maps	114
Layouts.....	120
Rules Manager	127
TV decoders	130
Live View Monitor.....	132
Left navigation tree.....	133
Contextual right-click menu	137
PTZ Controls pane	147
Search pane	147
Live Audio Controls pane	148
Layouts toolbar	149
Quick Access toolbar.....	149
HEALTH MONITOR	153
SERVER CONFIGURATION	155
SECURITY.....	160
USER MANAGER	160
Adding users	160
Deleting users	161
Modifying users	162
Importing users.....	167
Adding groups.....	168
Deleting groups.....	170
Modifying groups.....	171
PTZ priority.....	176
LOGIN.....	178
ACTIVE DIRECTORY	181
Prerequisites	181
Configuring Active Directory	182
Adding users or groups	187
Removing users or groups	191
Viewing user permissions	192

LDAP (LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL)	197
CHECKSUM	197
Enabling CheckSum Watermark.....	197
Verifying a CheckSum Watermark	198
ALARM LOG	205
CAMERAS	207
ADDING CAMERAS	207
Automatically	207
REMOVING CAMERAS	209
MODIFYING CAMERA DETAILS	209
General tab	210
Record tab.....	212
Advanced tab	217
Motion Settings tab	218
Video Settings tab.....	222
Optional Controls tab.....	223
Privacy Zone tab.....	224
Contact Information tab	225
Maintenance tab.....	226
DUAL-STREAMING CAPABILITY.....	226
ACCESS CONTROLS	228
S2.....	228
RS2.....	228
DSX	229
MONITORCAST.....	230
BLACKBOARD	233
Lane Viewer	236
Access View.....	239
MEDIA PLAYER	240
LEFT NAVIGATION TREE.....	240
TOOLBAR	245
SYNCHRONIZED PLAYER CLIP OPTION	251
TROUBLESHOOTING	253
FREQUENTLY ASKED QUESTIONS	253
What types of cameras are supported?.....	253
Why am I seeing skipping in Live View?.....	253
I'm having trouble installing IP Server on my computer.....	253
I can't get Health Monitor and my IP Server to connect.	254
I just added my servers, so why does it keep asking me to reenter them? It's not saving added servers.	254
Is there a list of all the ports used by IP Server and their purpose?	254
What does 'There was a database error, or this version of the database...' mean?	254
How do I set the IP Service to restart in the event of a crash?	256

How do I backup and restore my Video Insight database?257

I'd like to migrate all of my servers to one centralized database.258

How do I completely remove Microsoft SQL without reformatting the drive?259

I'm getting errors when playing recordings in Windows Media Player and Video Insight's Media Player.261

How do I add a VP1, VP8, VP16 Encoder or an Arecont-type camera with multi channels?262

How do I disable Map Labels for the Web Client?262

My C-drive is filling up due to Temp Cache, how do I clear it?263

ONLINE RESOURCES.....265

REMOTE SUPPORT.....265

CONTACT US.....266

APPENDICES.....267

 APPENDIX A: IP SERVER PORT LIST.....268

 APPENDIX B: CURRENT CUSTOMERS EXAMPLES269

 APPENDIX C: COMMONLY USED CAMERA CREDENTIALS271

 APPENDIX D: CONFIGURING A CNB CAMERA.....273

 APPENDIX E: CONFIGURING SENTRY FS1000 AND FS2000 CAMERAS.....275

 APPENDIX F: CONFIGURING AN IQEYE CAMERA USING OPTIONAL CONTROLS276

INDEX.....278

Introduction

Video Insight is a leading developer of enterprise-class video management software. Our vision is to provide powerful, user-friendly software that will run on "off-the-shelf" hardware based on IP technology. We have developed our solution from the ground-up, making us one of the few pure-play IP video management software providers.

Video Insight's suite of products was created to protect clients by providing intelligent, easy to use IP security solutions. Our extensive effort has resulted in products that are flexible and powerful enough for any situation, yet still very cost effective. Our software boasts the largest number of camera integrations available on the market. Users can access their Video Insight surveillance systems on mobile devices, through the web and on Microsoft Windows clients over internal networks or the Internet.

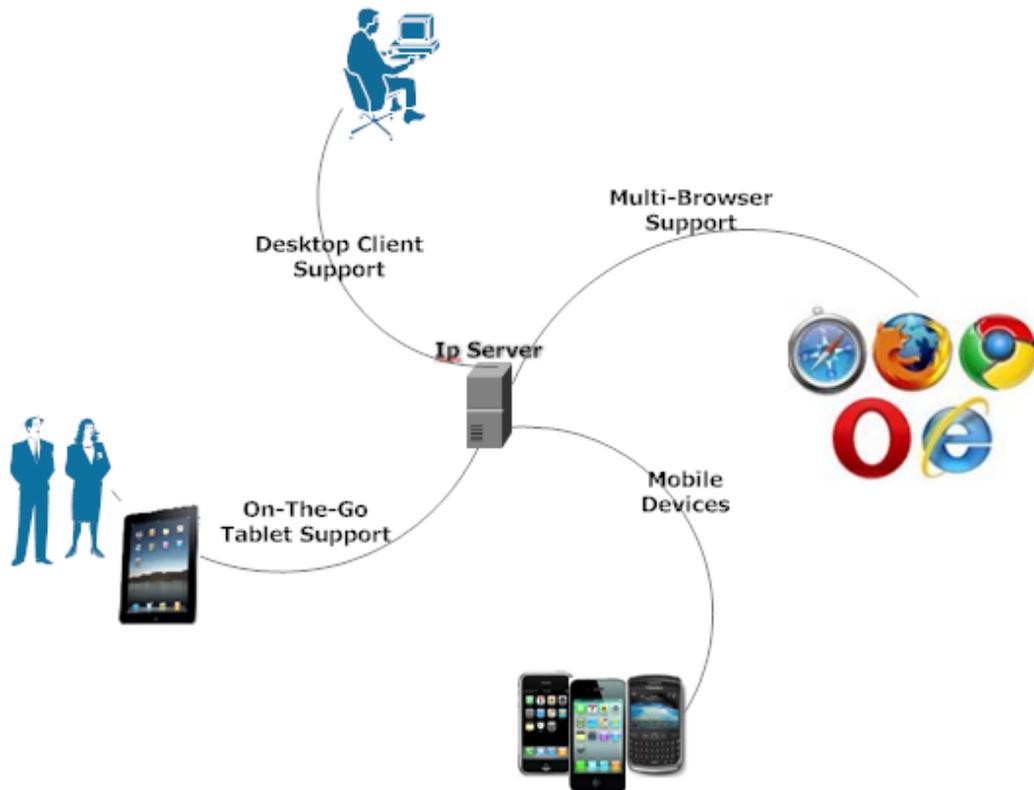
Video Insight v5.5 can intelligently and efficiently monitor security throughout your organization. Key advantages of this version are:

- Pure 64-bit server, clients and camera drivers
- Cloud-ready
- Optimized for centralization and hosting
- Panic button features
- Refresh Live Display only on Motion

The Video Insight IP Server Administrator Guide includes everything you need to install and configure IP Server with best practices and a troubleshooting guide. This document is intended for use by advanced users and system administrators.

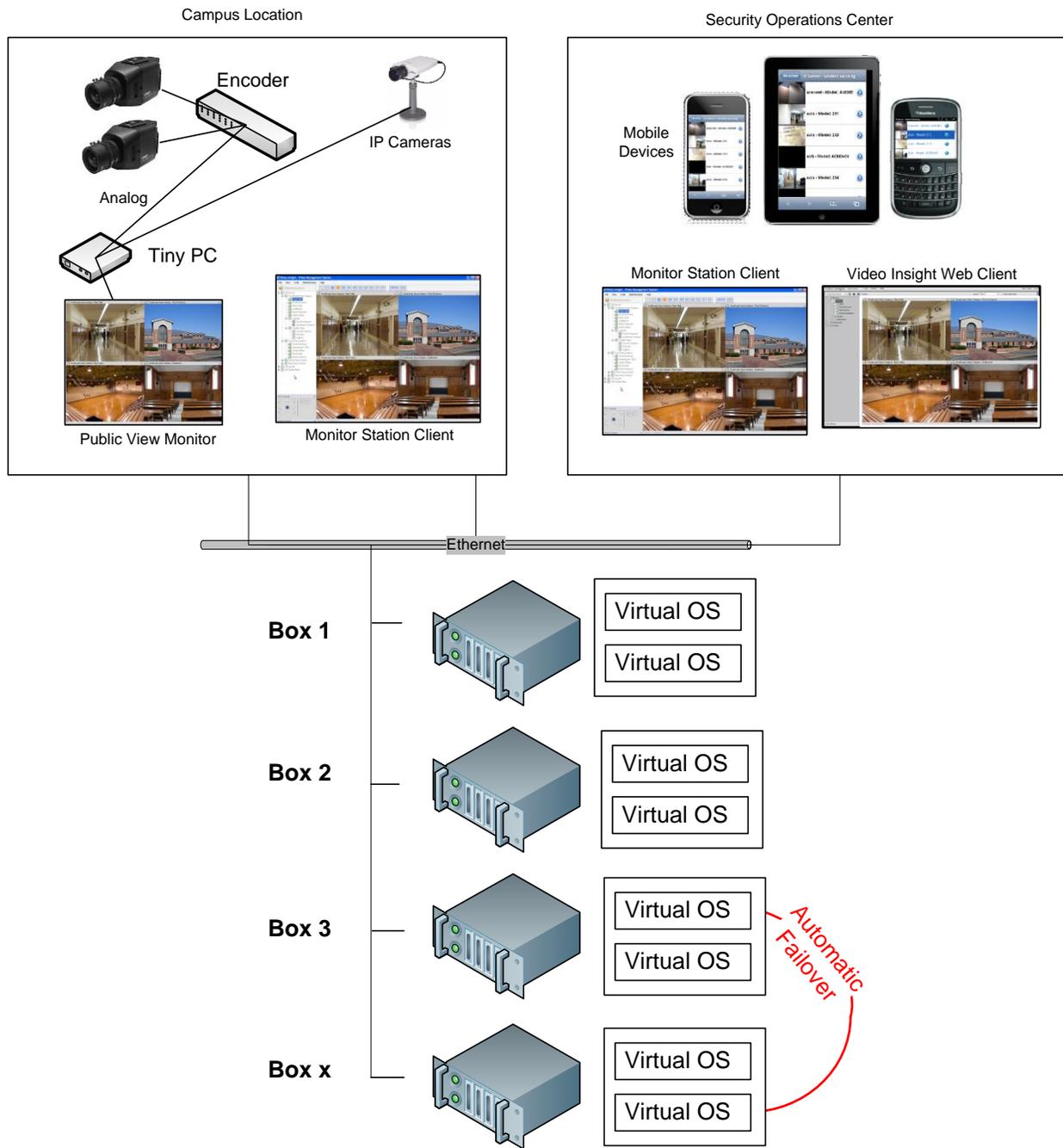
System Overview

The Video Insight application suite provides a solution for many different scenarios. You can use it for basic unattended monitoring or mobile remote viewing by patrolling security personnel. At its core is Video Insight IP Server, which powers the software platform. The figure below shows video monitoring options for users.



The Video Insight application suite runs over an Ethernet network, meaning cameras, security personnel and servers do not have to be co-located.

The figure below shows the distributed flexibility of the system extending to IP Server’s automatic failover capability.



The system is a robust software platform that has three main components that capture and view live or recorded video from anywhere: IP Server, Monitor Station and Web Client. The table below summarizes the role of hardware in the Video Insight application suite.

Table 1: Role of Client Applications, Hardware, and Software in the Video Insight application suite.

Product Suite: IP Server		
Client Applications	Monitor Station	<ul style="list-style-type: none"> ▪ Client application ▪ Live and recorded video ▪ Centralized administration ▪ Alarm notification
	Web Client	<ul style="list-style-type: none"> ▪ Live and recorded video ▪ Internet Explorer, Safari, Chrome and Opera (with optional ActiveX plug-in support for Internet Explorer)
	Smart Phone/Tablet Client	<ul style="list-style-type: none"> ▪ Live and recorded video ▪ iPhone, iPad, BlackBerry and Android support ▪ PTZ control
Hardware	IP Server	<ul style="list-style-type: none"> ▪ Records and manages video ▪ VM support ▪ Alarm processing ▪ 3rd-party, access control and analytics integration ▪ Microsoft IIS for Internet clients ▪ Active Directory, LDAP and Novell eDirectory support
	Storage	<ul style="list-style-type: none"> ▪ Direct Attached, SAN/NAS and iSCSI storage support
Software	IP Server Manager	<ul style="list-style-type: none"> ▪ Monitors the IP Server(s) and presents a visual status for each ▪ Network connection administration ▪ Diagnostics for trouble shooting and system optimization
	Health Monitor	<ul style="list-style-type: none"> ▪ Accessory application that monitors the health of all your servers and cameras from a single location ▪ Email notification on error

Planning

Getting the most out of your hardware and our software requires planning. Understanding your needs will help you size your solution. Evaluate and plan the integrations you will need to make.

Server

IP Server is at the heart of the Video Insight platform. It runs on industry-standard hardware and works with 32- and 64-bit versions of these Microsoft operating systems.

- Windows Server 2008 R2
- Windows Server 2008 Enterprise, Standard and Web editions
- Windows Server 2003 Enterprise, Standard and Web editions
- Windows 7
- Windows Vista
- Windows XP Professional

IP Server also requires Microsoft .NET Framework 3.5 and Microsoft Internet Information Services (IIS) with “static content” enabled. The operating system must be current with updates because Video Insight hardware and software integrates with the latest updates.

The hardware required for installation of IP Server is determined by a variety of factors including the number of cameras, the resolution of those cameras, the number of frames per second, as well as the number of days of required video storage. Generally, hardware requirements depend on whether 100 or more cameras will be connected. For less than 100 cameras use Table 2 as your guide.

Table 2: Video Insight IP Server hardware requirements for systems with less than 100 cameras.

Component	Minimum	Recommended
Processor	1 2.4 GHz quad-core	2+ 2.4 GHz quad-core
Memory	8 GB	16 GB
Video	X MB	Xx MB
Network	X Gb/s	Xx Gb/s
Storage		RAID 5/6

Keep in mind that you can expect higher CPU usage without Microsoft Direct Show installed. Also, the server video memory requirement depends on whether compression will be used.

Table 3 shows the hardware requirements if you plan on connecting more than 100 cameras.

Table 3: Video Insight IP Server hardware requirements for systems with more than 100 cameras.

Component	Minimum	Recommended
Processor	2 2.4 GHz quad-core	4+ 2.4 GHz quad-core
Memory	16 GB	32 GB
Video	X MB	Xx MB
Network	X Gb/s	Xx Gb/s
Storage		RAID 5/6

Network throughput is especially important when more than 100 cameras will be connected. High definition cameras will slow already busy network segments to a crawl.

Failover Server

In the event a network outage or hardware failure prevents a server from recording camera video, the IP Server Failover Server feature will enable another server to take over the recording capabilities of the offline server. When configured with a shared IP address as part of a cluster, the Failover Server feature eliminates video loss and enables continuous live streaming video.

To use the Failover Server feature you must:

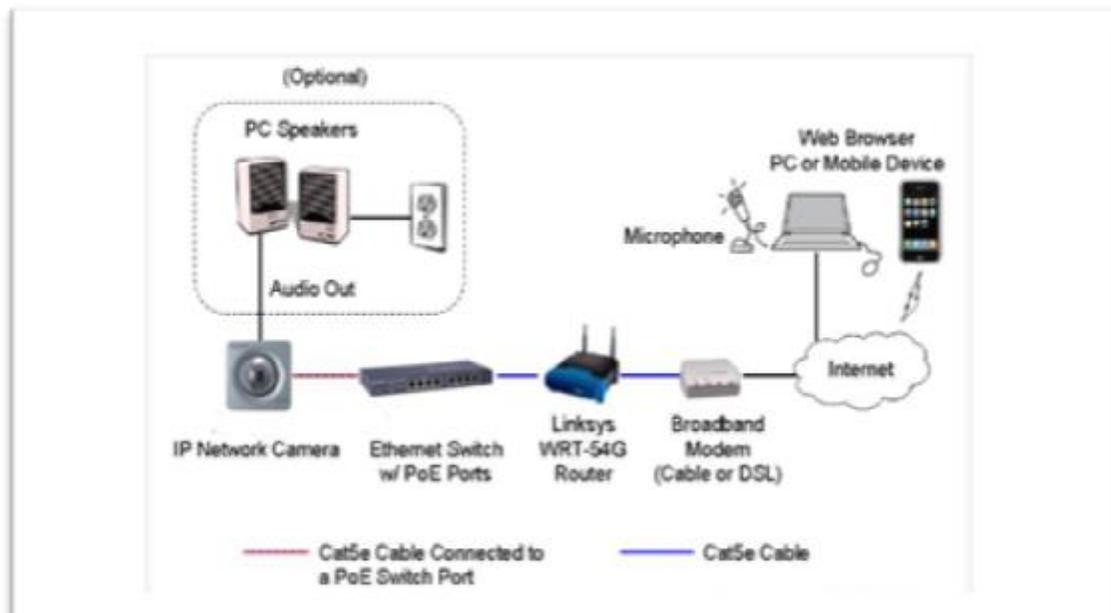
- Have at least two servers with the same hardware configuration, i.e., a cluster.
- Have a Shared Database installation; see IP Server installation with an existing SQL installation.
- Have a shared IP address.
- Have at least one license and a serial number or activation key for each server.

Network

Network configuration is extremely important when implementing an IP video solution. IP cameras use considerable bandwidth to deliver information between the camera and the server. Different cameras will require different amounts of bandwidth based on resolution and frame rate. Accessing video from Monitor Station, Web Client, mobile device client and Video Wall increases the needed bandwidth.

Figure 3 illustrates a very basic, isolated network comprising of one switch, one camera and one router.

Figure 3: Basic IP video monitoring solution with remote viewing.



Factors affecting performance

Any system is the sum of its parts. A mismatched sub-system or component can have a negative effect on the whole system. Video streaming can only be as good as the cameras and underlying network. Best practices for IP video solutions indicate cameras connected to and powered over Ethernet or separate VLANs for cameras.

Local and Wide Area Network

Video travels over a network, meaning infrastructure plays a big part in the overall performance of the Video Insight solution. A slow network can create bottlenecks that result in a slow frame rate, jittery video and packet loss. Avoid devices on your local network with a port speed of 100 Mb/s or less.

The following network issues can cause cameras to drop a connection or otherwise go offline:

- Camera is using a dynamic instead of static IP address
- Another service or device is running at the same time with the same IP address, causing a conflict
- Multiple applications pulling a stream from one camera (some cameras limit the number of streams)
- Power output of a switch is less than required by the cameras. The power output of a switch has to be greater than the sum of the power requirements of the attached cameras. Refer to the camera's manual for power requirements

You may be tempted to implement wireless local networking to connect cameras. Due to potential dead zones, transmission speed, outside interference and weather conditions you can expect subpar performance and dropped connections. We do not recommend using wireless networking to connect your cameras.

If your organization has more than one site you will likely be relying on an Internet provider for connectivity. The performance you get from the provider will depend on their network infrastructure, customer utilization of that network and what you can afford. Streaming video remotely to a desktop client requires basic broadband. Streaming to a mobile device requires 4G service.

Cameras

The following factors can affect camera imaging:

- Bit rate – a higher bit rate usually gives better picture quality
- Resolution – a higher resolution usually gives better picture quality
- Format – some picture formats incorporate better algorithms that more accurately represent the subject
- Firmware – outdated firmware can impair camera functionality
- Location – unless intended for such use, placement in dark or obstructed locations, or in places affected by adverse weather, will not result in useful pictures
- Number of cameras connected to server – the higher the number of connected cameras, the greater the load on server resources

Monitor Station

Monitor Station, the Video Insight thick client, allows users full access to all cameras and provides centralized administration for the system. It is used to watch live and recorded video.

Monitor Station runs on industry-standard hardware and works with 32- and 64-bit versions of Microsoft Windows XP or later. Microsoft Direct Show 9 or higher is required. The operating system must be current with updates because Video Insight hardware and software integrates with the latest updates.

Monitor Station requests video from the server in the camera's native format. Transferring video in the camera's native format is a file server operation that does not burden the IP Server CPU as a video decompression operation would. Because video decompression is performed on the client and not the server, the hardware requirements for Monitor Station are different from those of IP Server. Table 4 shows the hardware requirements for Monitor Station.

Table 4: Monitor Station hardware requirements.

Component	Minimum	Recommended
Processor	1 2.0 GHz single-core	1 2.4 GHz dual-core
Memory	2 GB	4 GB
Video	256 MB	512 MB
Network	100 Mb/s	1 Gb/s

Note

The video sub-system must support Microsoft Direct Show.

Monitor Station will require additional system memory, video memory and processor if more cameras are viewed and processor-intensive compression protocols are used. The greater the number of compressed images viewed at once, the greater the load on the processor.

Web Client

Web Client, the Video Insight thin client, allows users remote access to cameras. Web Client is distinct from the Video Insight mobile device application. Web Client utilizes Microsoft IIS services hosted on the same server as IP Server. To support cross platform compatibility, IP Server sends MJPEG images to clients that are unable to decompress MPEG4 or H.264 streams. These images are normally provided as a dual stream from the camera. IP Server can create a MJPEG but this increases the load on the CPU.

Web Client connects directly to the cameras to view live video, unlike Monitor Station. Table 5 shows Internet browsers supported by Web Client.

Microsoft IIS 5.1 or higher must be installed and configured prior to the installation of IP Server.

Health Monitor

Health Monitor is a separate application used to monitor the health of one or all of your servers. Health Monitor adds peace of mind with a server monitoring your video surveillance servers and cameras. You can further mitigate risk and disaster recovery issues by adding a Failover Server.

Health Monitor does not have any hardware requirements and is compatible with the same operating systems as IP Server. However, keep the following in mind when planning for Health Monitor:

1. We recommend hosting Health Monitor on its own computer to isolate it from the failure of an IP Server.
2. Health Monitor does not have to be on the same network subnet as IP Server. It can be local or remote.
3. Health Monitor requires a database. It can be local or remote. If the database will be remote you must create it before you install Health Monitor.

Cameras

Video Insight supports a vast array of cameras from a large number of manufacturers. Additional camera support is included with every software release Refer to our website for the latest list of supported cameras.

Video Insight supports the Open Network Video Interface Forum (ONVIF) standard. We support version 1.03.

Licensing

Our licensing structure is simple: one camera requires one license. Our floating licenses means there is no need to tie a licensing seat, IP address or MAC address to a particular camera. Cameras offering multiple camera views only require one license. Separate video streams from the same camera do not require a separate license. Video Insight offers encoders, such as the VP16, that allow up to 16 analog cameras with only one license. Please contact us for more information on specific licensing requirements.

Note

Some cameras include a license for use with our software.

Router configuration

We recommend using some type of router if your computer is connected to the internet. Small Office/Home Office (SOHO) routers provide a simple hardware firewall that protects your computer. SOHO routers connect to your DSL or cable modem and you connect to your server through them. The

SOHO router prevents all inbound traffic from accessing your network and computers except for the traffic that you specifically allow through.

How to configure your Video Insight server and router for remote access:

1. Assign a static IP address to IP Server. SOHO routers typically use DHCP to assign an IP address from a range of addresses to devices connected to the router. Choose an address outside of this range but within the subnet to assign to the server. For help on assigning a static IP address, review your SOHO router user guide or consult with your network administrator.
2. Configure your SOHO router to forward ports 80 and 4011 to IP Server.
 - a. For help on forwarding ports, review your router manual or consult with your network administrator.
 - b. www.portforward.com provides information on how to configure most SOHO routers. Video Insight does not endorse this information.
3. Test your configuration by trying to access the Web Client externally.
 - a. Start your Internet browser.
 - b. Enter: `http://<external IP>/videoin sight4` into the address bar of your Internet browser.
 - c. Note, many SOHO routers will not allow you to connect to your external IP address when you are behind the firewall. You will need to be outside your network.
 - d. You can use a third-party website such as canyouseeme.org to get your external IP address and to verify if the correct ports are being forwarded.

Storage considerations

The amount of storage required for recordings depends on the number of cameras, the CODEC, Frames per Second (FPS), resolution of the images and the percentage of pixel change. The Video Insight solution gives you flexibility of per camera storage options:

- Record Always – requires significantly more storage space because video is constantly recorded.
- Record On Motion Only – requires less storage space than Record Always because video is recorded only when motion occurs in the camera’s field of view.

IP Server supports the following types of storage:

- **RAID 5 and RAID 6**
- **NAS**
- **SAN**
- **Long Term Storage Application (LTS)**

You can specify which cameras to copy, how many days to keep before copying and what time of the day to execute the copy. The copied files can be viewed using Video Insight software or Microsoft Windows Media Player.

- **File Manipulation Rule**

A feature that allows users to back up their files to other locations such as standard file servers, NAS or SAN using the Rules manager. This feature takes the task of remembering to back up important video recordings on the local server and automates it. File Manipulation can also move or delete videos.

Database considerations

IP Server saves configuration settings, user names, camera information and event logs in a Microsoft SQL database. When IP Server starts, it reads its settings directly from the assigned database. When Monitor Station connects to IP Server it saves all recordings to its local hard drive so recordings are still accessible in the case of database failure.

Use Table 5 to help you determine whether you need a local or a shared database.

Table 5: Choosing a local or shared database.

Local	Shared
Small centralized organization with 1-3 servers	Large regional organizational with many servers
Use Monitor Station and built in User Manager	Use Active Directory/LDAP
Number of users is small	Number of users is large
Disaster recovery and back up for each server's database	Disaster recovery and back up for one database
Failover server functionality is not desired	Failover server functionality is desired
Servers are not on the same LAN or the communication link between the server the database is a low-speed connection	Servers are on the same LAN
Cameras will not move from one server to another	Cameras will move from one server to another
Avoid exposure SQL to the network	Exposure of SQL to the network

Software installation

Video Insight software supports both 32- and 64-bit operating systems. Choose the correct executable to begin the installation process. Review the following list prior to beginning the installation process:

1. [Storage Considerations](#)
2. [SQL Considerations](#)
3. [Network Considerations](#)
4. Online Calculator: www.video-insight.com/Support/Tools/Configuration-Calculator.aspx
5. Administrator-level access on server is required

IP Server

If Microsoft SQL Server is not already present in your environment you can choose to install the package. It includes Microsoft SQL Server 2008 R2 for both 32-bit and 64-bit OS's.

If your environment already has Microsoft SQL Server 2008 installed and you only need the Video Insight database and are not required to install SQL Server installation package.

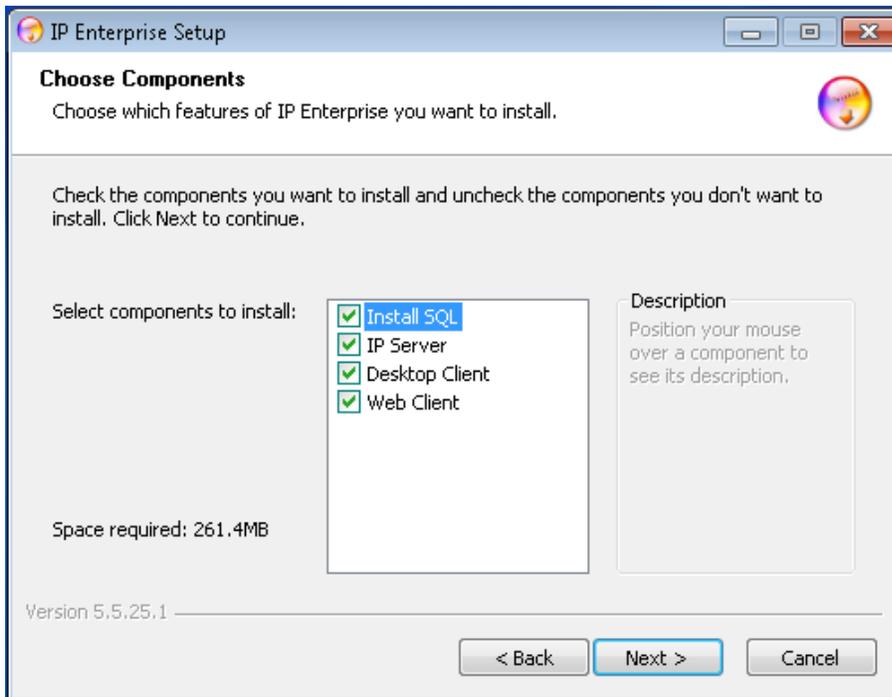
Installation without an existing SQL installation

Use the following steps to install IP Server with Microsoft SQL Server for the first time. This option will also install Monitor Station and Web Client:

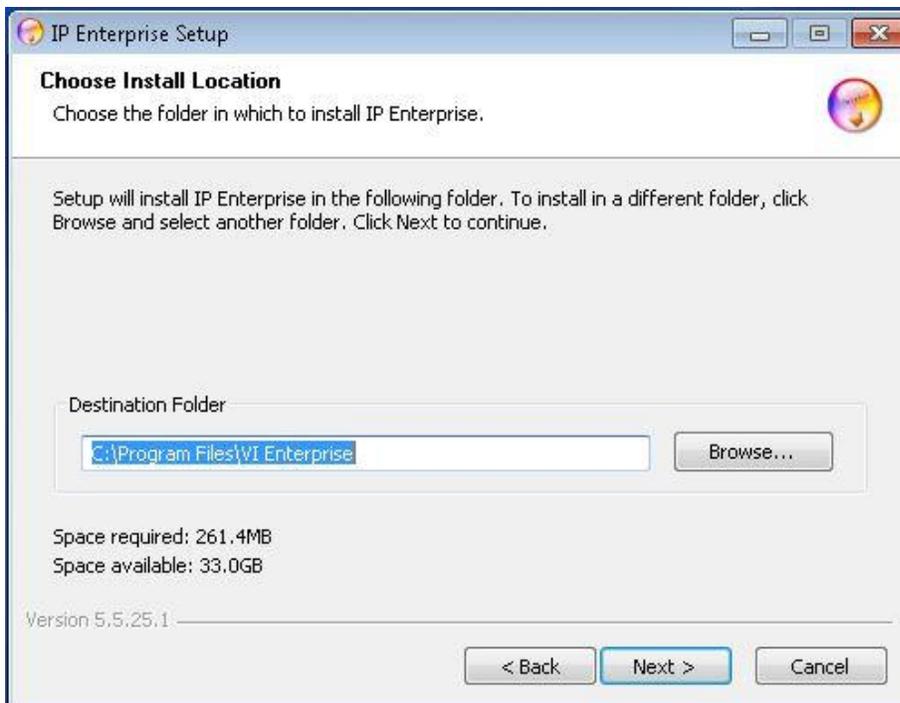
1. Launch the executable for your OS type (32-bit or 64-bit OS). Click **I Agree** to agree to the terms and continue the installation. If you do not agree or do not want to continue the installation, click **Cancel**.



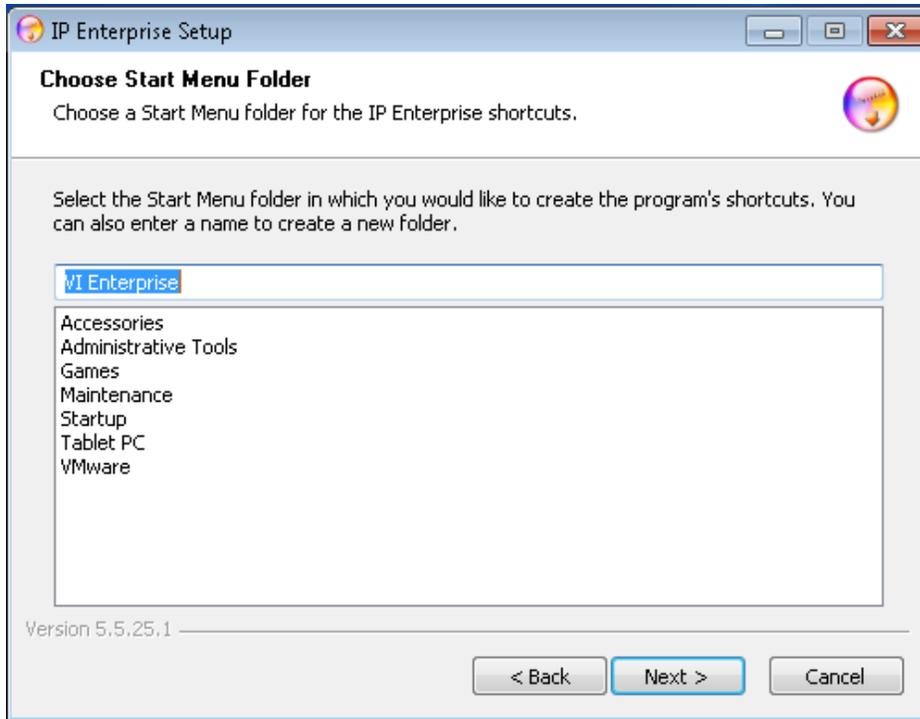
2. Select all the components that you would like to install, click **Next**.



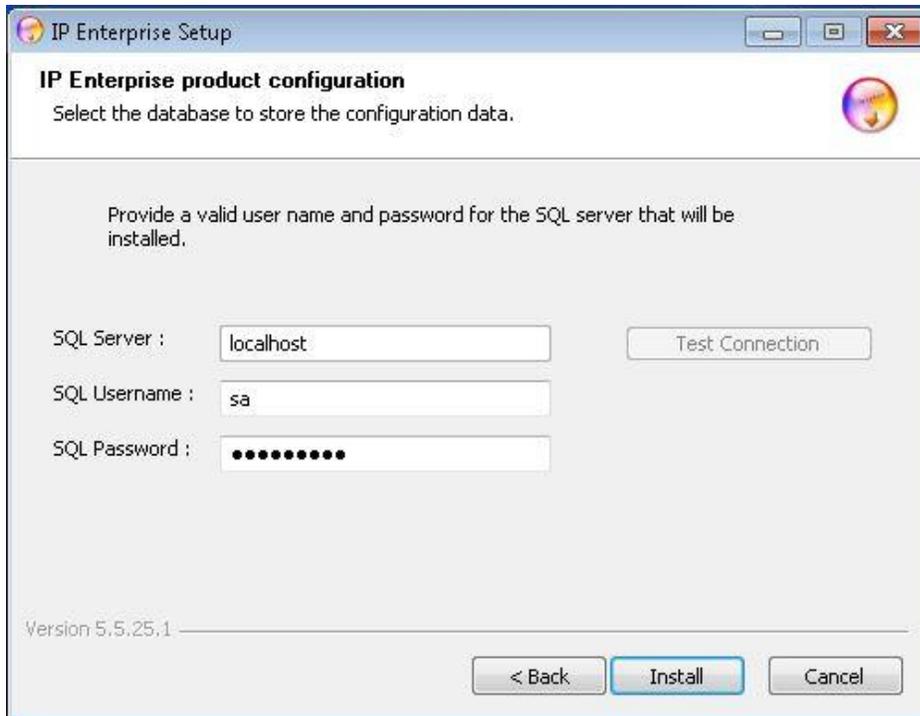
3. To accept the default destination folder, click **Install**. To choose another destination, enter the destination path or click **Browse** to search.



4. Select the start menu folder that you would like the installation to be created, click **Next**.



5. The default credentials are entered for the SQL installation, if you would like to change the credentials please enter them now and click **Install**.

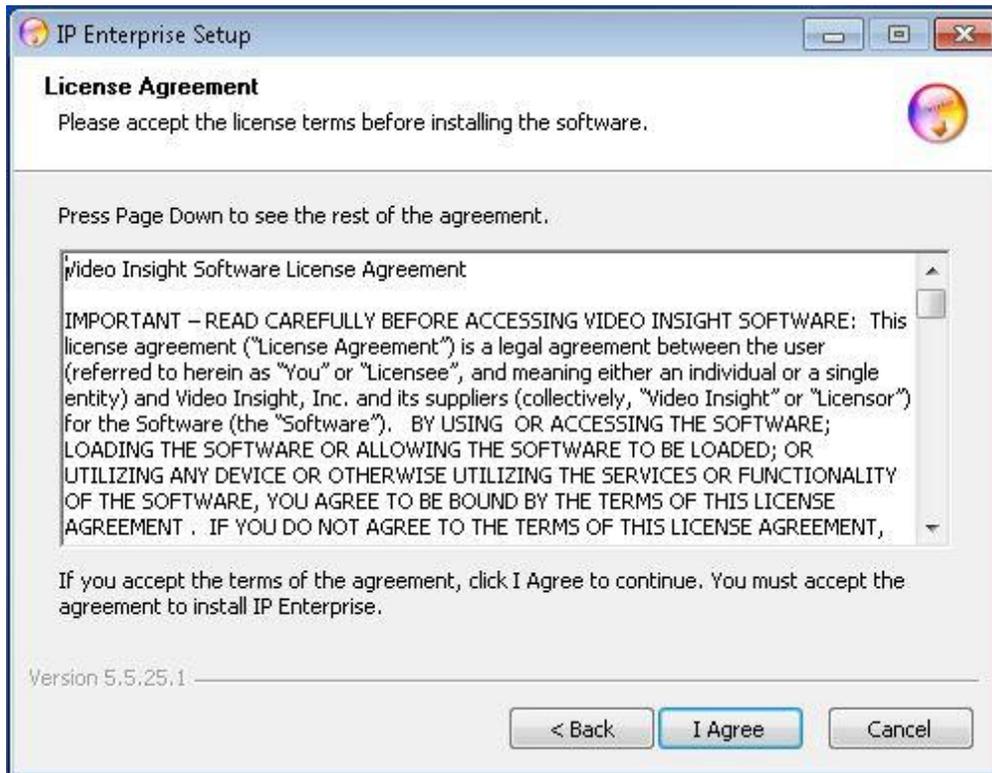


6. IP Server is installed. To initialize and configure it, see [Initialization](#).

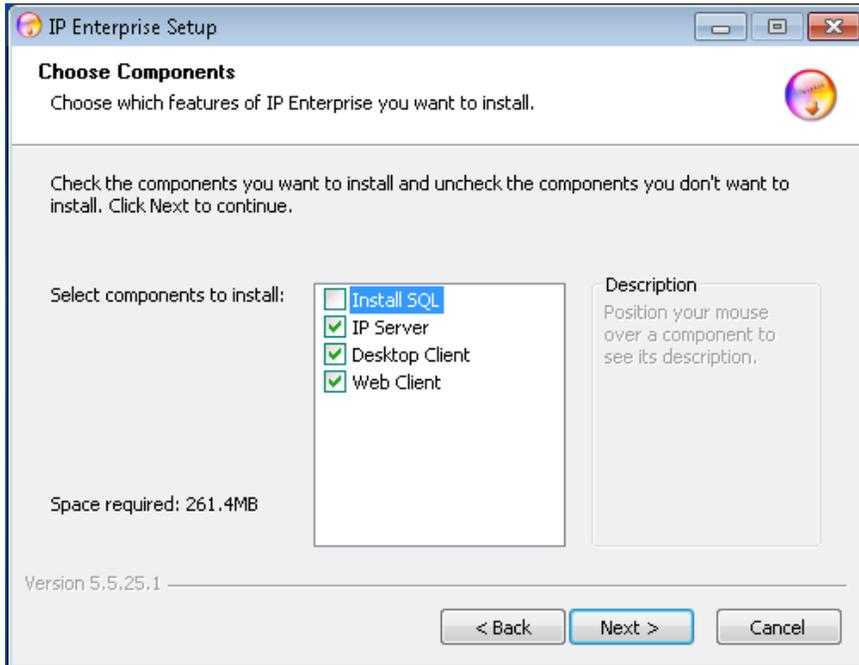
Installation with an existing SQL installation

Use the following steps to install IP Server for the first time in an environment with Microsoft SQL Server. This option will also install Monitor Station and Web Client.

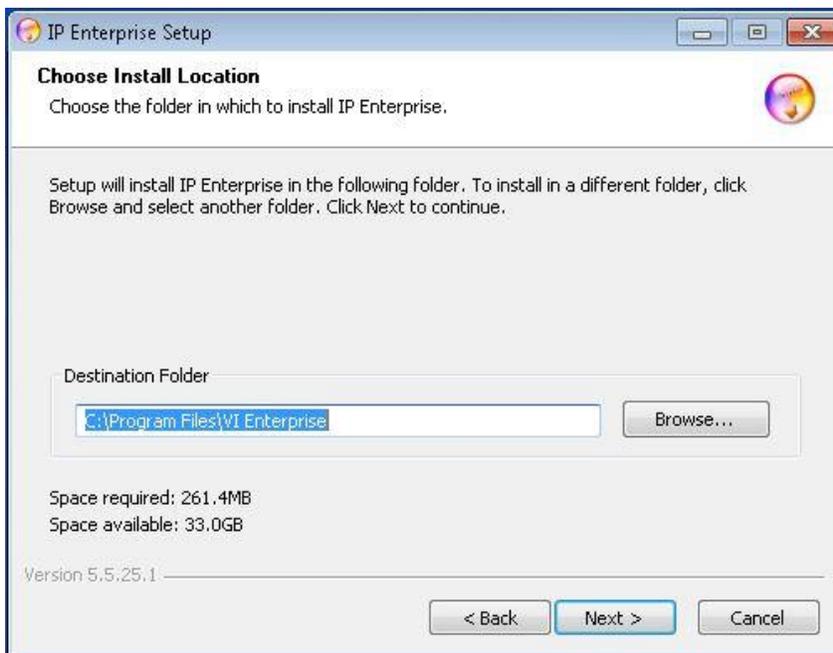
1. Launch the executable for your OS type (32-bit or 64-bit OS). Click **I Agree** to agree to the terms and continue the installation. If you do not agree or do not want to continue the installation, click **Cancel**.



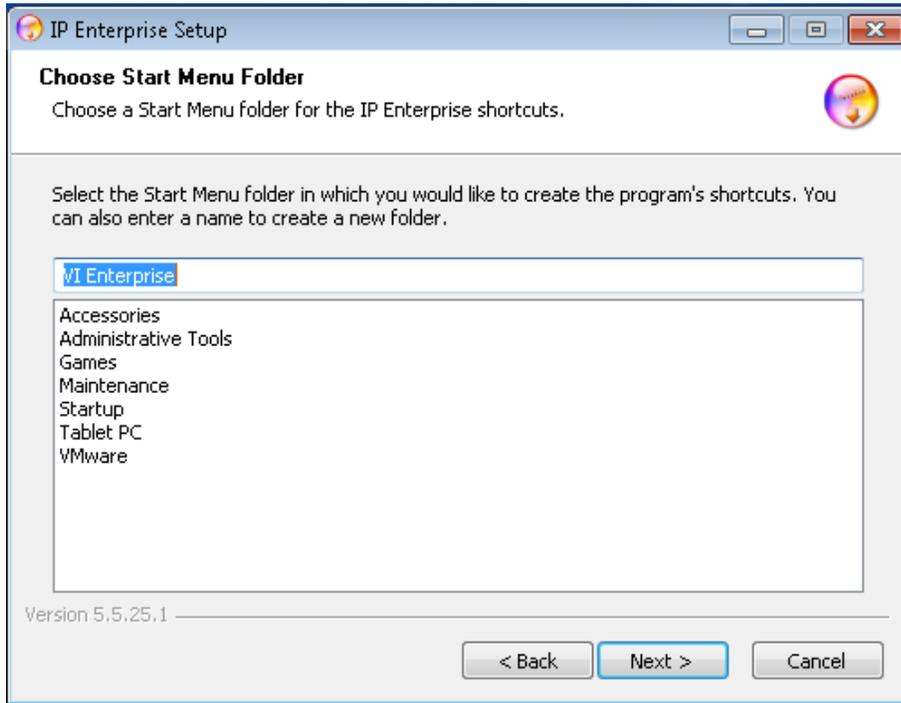
2. Select all the components that you would like to install, click **Next**.



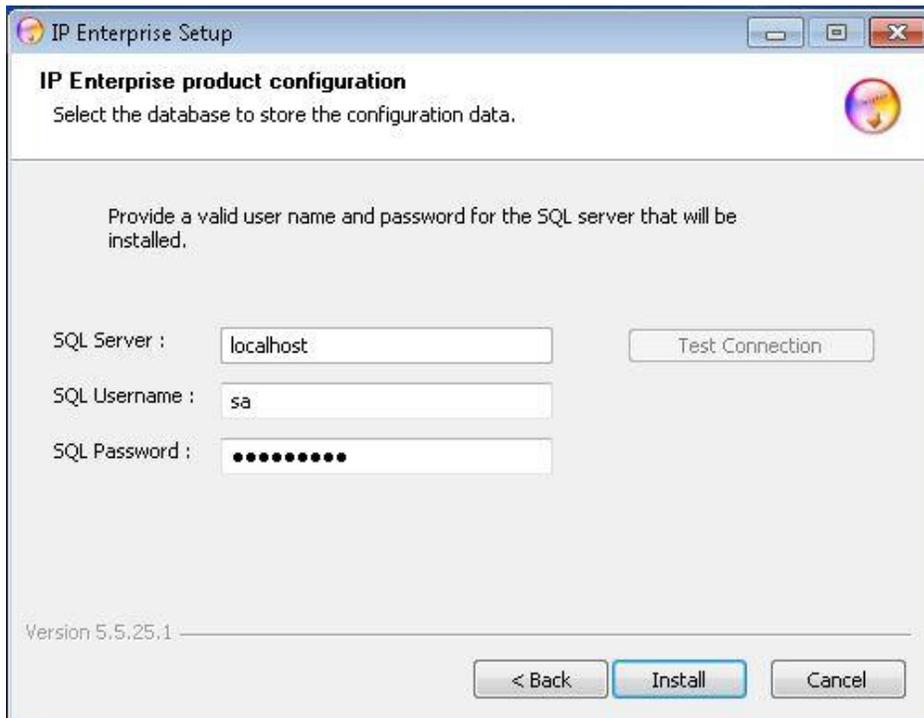
3. To accept the default destination folder, click **Install**. To choose another destination enter the destination path or click **Browse**. Click **Next** to begin the installation process.



4. Select the start menu folder that you would like the installation to be created, click Next.



5. The default credentials are entered for the SQL installation. If you would like to change the credentials, please enter them now and click **Install**.



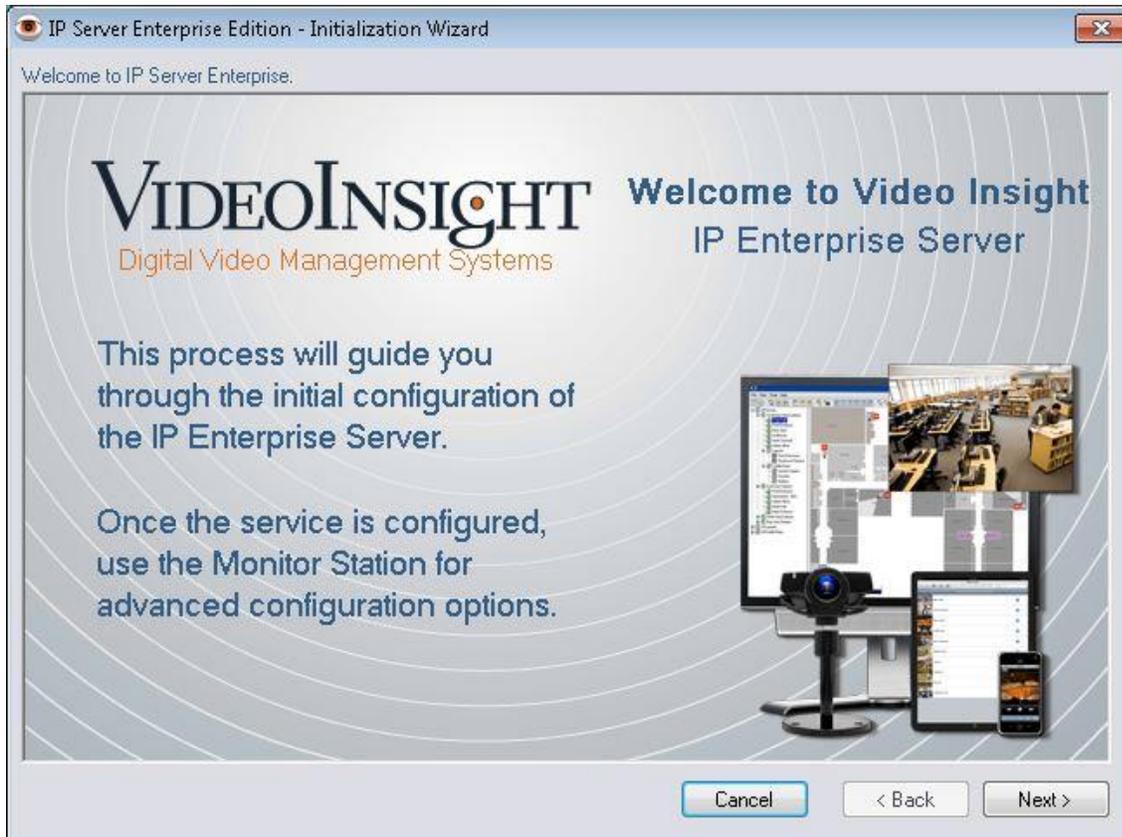
6. IP Server is installed. To initialize and configure it, see [Initialization](#).

Initialization

You must activate and initialize IP Server before you can use it.

To activate IP Server with a serial number:

1. If you are activating IP Server with a serial number, click **Next**. If you are activating by phone, click **Next** and go to page [34](#). If you are activating a demo, click **Next** and go to page [35](#).





2. Enter the five character alpha-numeric serial number provided to you at the time of purchase and then click **Next**.

Clicking **Cancel** will abort the installation and the server will not start automatically.

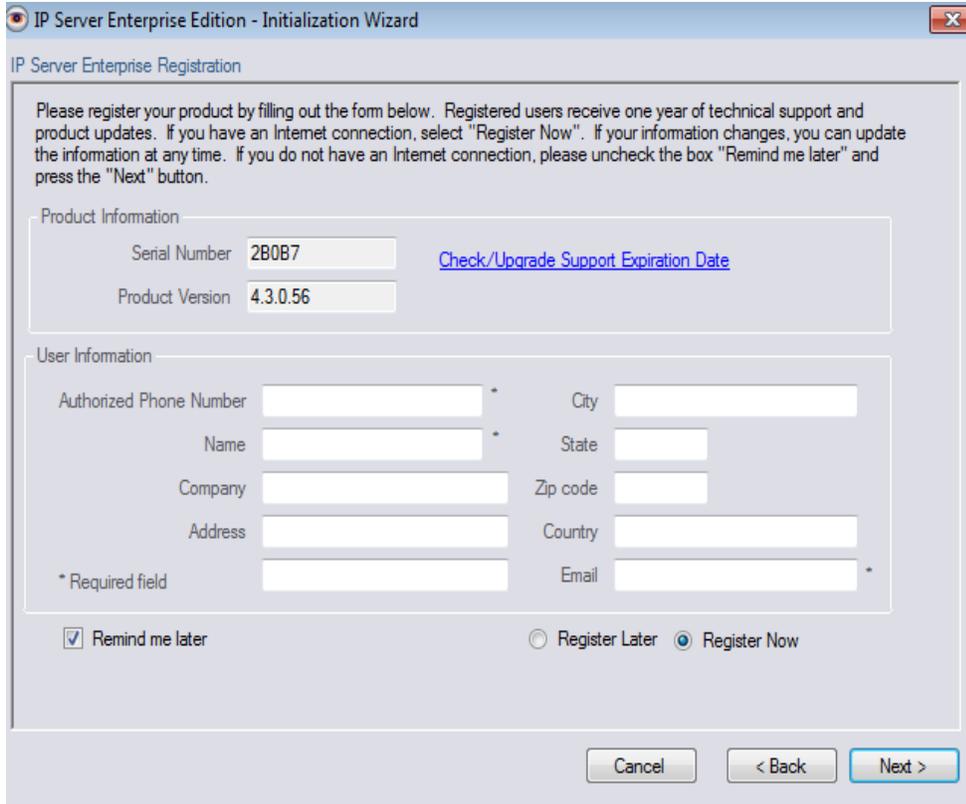
Note

Select Activate by Phone and call 713-621-9779 if you are having a problem activating the software with your serial number, or select Demo mode to start recording immediately.

Toll charges may apply.

4. Enter your user information if you would like to be notified of updates and releases, and then click **Next**.

If you would like to enter this information later, select Register Later and then click **Next**.



The screenshot shows the 'IP Server Enterprise Edition - Initialization Wizard' window. The title bar reads 'IP Server Enterprise Edition - Initialization Wizard'. The main window title is 'IP Server Enterprise Registration'. Below the title is a paragraph of instructions: 'Please register your product by filling out the form below. Registered users receive one year of technical support and product updates. If you have an Internet connection, select "Register Now". If your information changes, you can update the information at any time. If you do not have an Internet connection, please uncheck the box "Remind me later" and press the "Next" button.'

The form is divided into two sections:

- Product Information:** Contains two text boxes: 'Serial Number' with the value '2B0B7' and 'Product Version' with the value '4.3.0.56'. A blue hyperlink 'Check/Upgrade Support Expiration Date' is located to the right of the Serial Number box.
- User Information:** Contains several text boxes: 'Authorized Phone Number', 'Name', 'Company', 'Address', '* Required field', 'City', 'State', 'Zip code', 'Country', and 'Email'. Each of these boxes has an asterisk next to its label, indicating they are required fields.

At the bottom of the form, there are three radio buttons: 'Remind me later' (checked), 'Register Later', and 'Register Now'.

At the bottom of the window, there are three buttons: 'Cancel', '< Back', and 'Next >'.

IP Server automatically detects most settings for you. Verify the information or make changes, then click **Next**.

Note

Recording to a shared location requires a user with write permission to that share or recordings will not be saved.

Server Name: The default is “IP Server –“and the detected IP address of this server. You can change this to a more friendly or meaningful name. Do not use special characters.

IP Address: This is the selected server’s IP address and should not be changed.

Version: The current version of the software.

For additional settings click **Advanced**. The Default Port is 4010 and the Command Port is 4011. Do not change these values unless the ports are already in use by another program.

SQL Server Location: This is the location or IP address of the database server. ‘localhost’ indicates that the database and Microsoft SQL server are local to the host computer. An IP address in this field indicates the Microsoft SQL Server is located on another computer.

To test the connection click **Test DB**. Click **Advanced** to modify the database connection string values: Database Name, IP Address, SQL Server User ID and Password.

IP Server Enterprise Edition - Initialization Wizard

Server Configuration

Server Identification

Server Name: IP Server -10.10.1.189

IP Address: 10.10.1.189

Version: 4.3.0.56

Database Information

Sql Server Location: localhost

Test DB Advanced

Advanced

Video Storage

Video data storage path *

c:\video Browse

* Note: If using a Network Drive, use the UNC path (i.e. \\v4\share\video)

Cancel < Back Next >

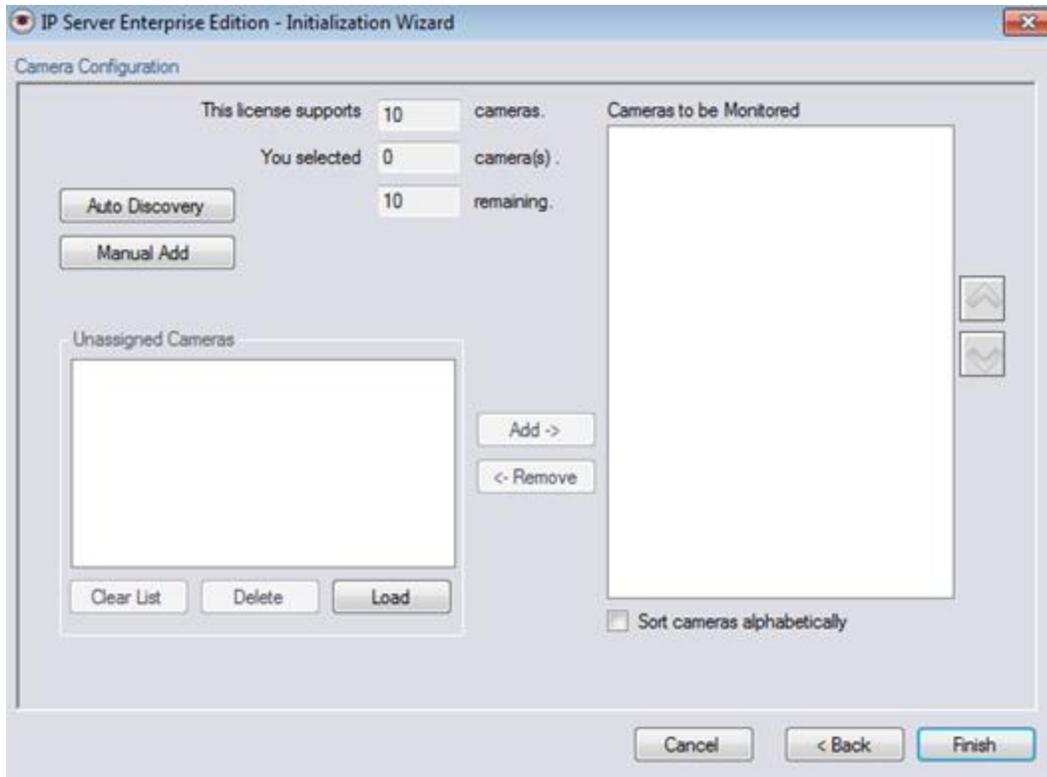
To test the connection click **Test DB**. Click **Advanced** to modify the database connection string values: Database Name, IP Address, SQL Server User ID and Password.

Video Data Storage Path: This is the location where all the recorded video will be saved. The default is the local OS drive (i.e., C). The video folder is created automatically once server configuration is completed. You can choose to save video to several different locations:

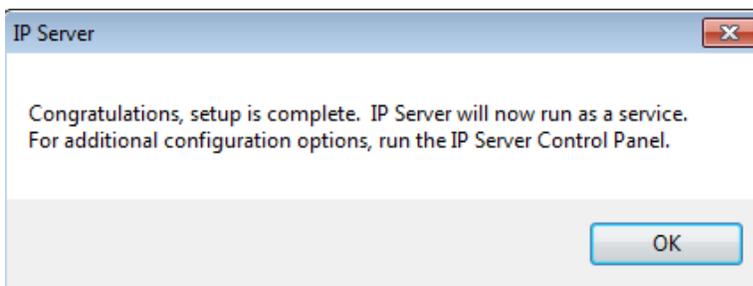
Local server drive: For example, C:\video

Alternate local drive: For example, D:\video

Shared drive: For example, \\v5\share\HHSvideo



1. Add cameras using Auto Discovery, Manual or Add Add/ Remove as needed. See Adding Cameras for more information on adding cameras. Click **Finish**.



2. Click **OK**.
3. Click **Yes** to restart the computer.

Use one of the following steps to activate IP Server.

IP Server Enterprise Edition - Initialization Wizard

IP Server Enterprise Activation

IP Server Enterprise Activation

Serial number *

Activate or upgrade your license through the Internet
On a machine with an internet connection, activate the IP Server by entering the serial number and press the Next button. This will upgrade your license to most recent amount.

Activate by phone
On a machine with no internet connection, use the 'Activate by Phone' method.
Be prepared with the following information:

Hardware Code

Call Technical support at: (713) 621-9779 Monday - Friday, 8:30AM to 6:30 PM CST

Activation Code

Demo mode
If you are unable to perform either of the two above methods, then enter the system in 'Demo Mode.' You can configure the system and activate the system at your earliest convenience.

* The serial number is found on the product package and on the sales receipt

Cancel < Back Next >

Select Activate by phone.

Call the phone number displayed. Give the representative your serial number. If you do not have one, the representative will ask you for a hardware code. If the account is in good standing you will be given a 16 digit activation code. Enter the activation code and then click **Next**.

Activate Using Demo Mode

Selecting Demo mode will allow IP Server to operate normally for up to 30 days using up to 99 cameras. Once the 30-day period has expired the software will no longer record or display live images. IP Server will fail to start until initialization is completed with a valid serial number or activation code. Reinstallation is not required.

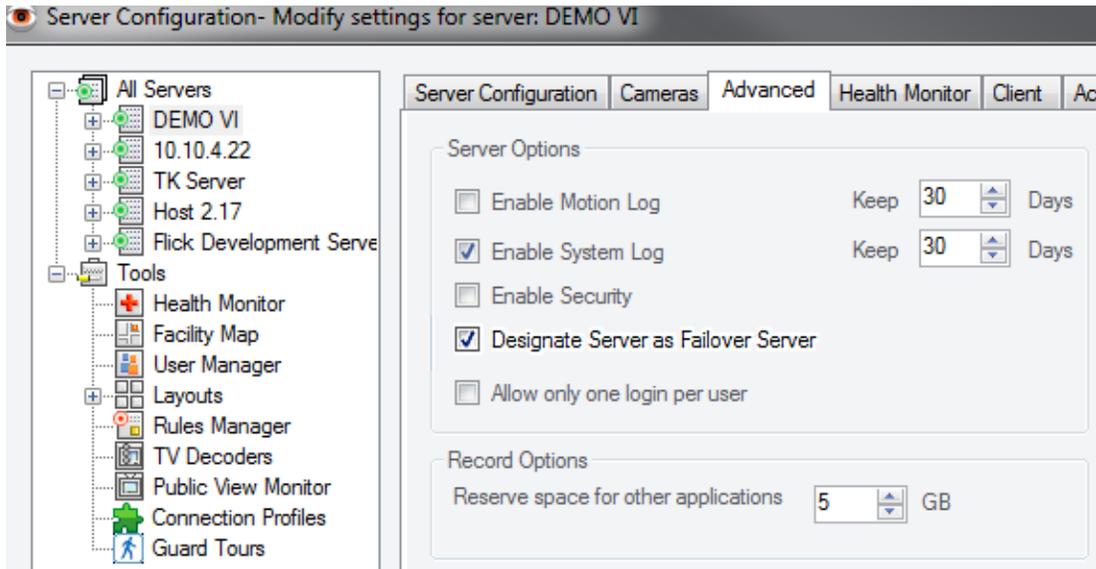
Failover Server

A fault-tolerant feature of IP Server is the ability to designate a failover server. Once designated and configured, the failover server can take over from another server that has gone offline.

To designate a server as a Failover Server:

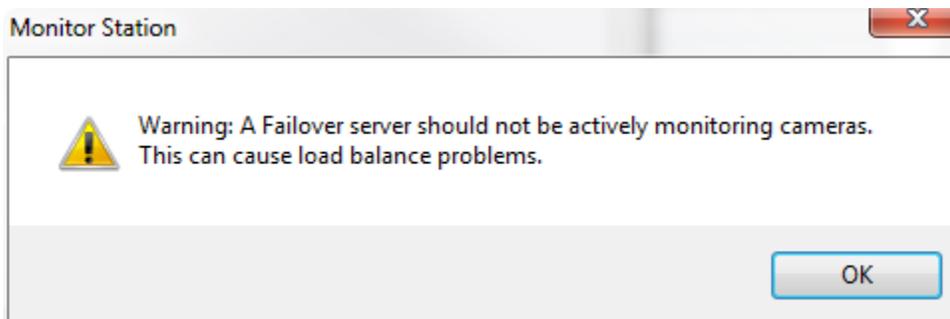
1. Click Administration -> Setup and Configuration from the main menu.
2. Select the desired failover server from the left navigation pane.
3. Select the Advanced tab.

4. Check the “Designate Server as Failover Server” box.



Avoid selecting a server that is actively monitoring cameras. Figure 4 shows the warning that appears if a server with existing cameras is selected as a Failover Server.

Figure 4: Warning generated when designating a server that is actively monitoring cameras.



If a failure occurs the transfer of the camera(s) to the Failover Server will take approximately 5-10 minutes to recover. During that time the Monitor Station on the Failover Server will show all cameras and images from the offline server and all recorded video will be recorded to the Failover Server or a previously configured shared location.

Note

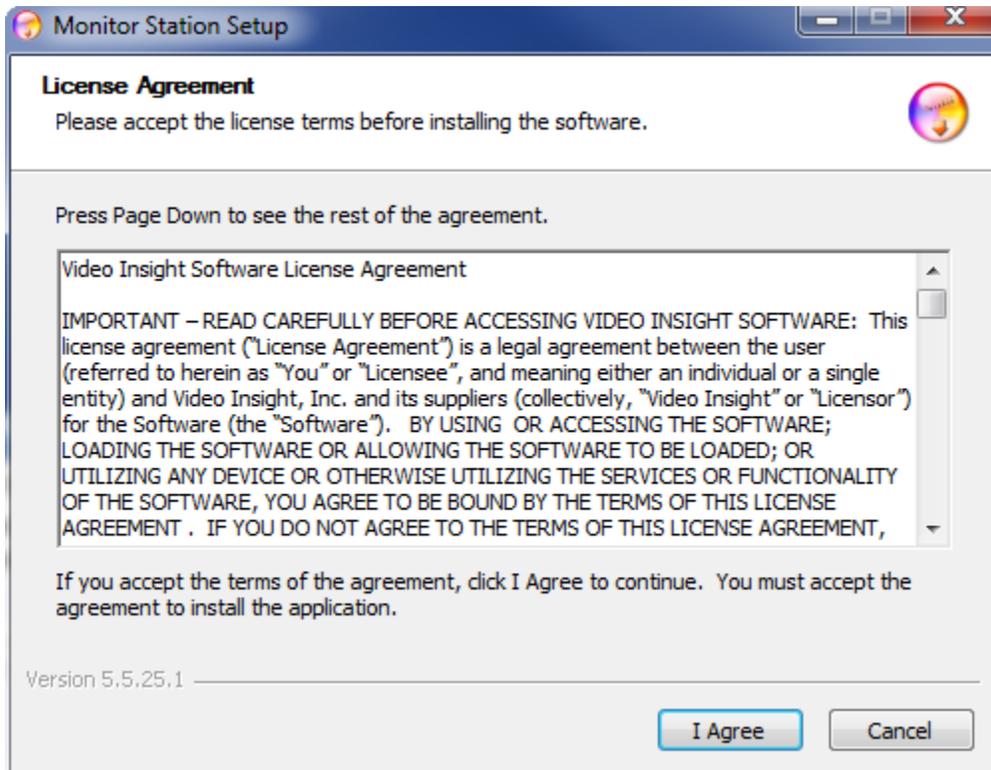
You can also access Server Properties by right-clicking the server name in the left navigation and selecting Properties, selecting the Advanced tab and then selecting Configuring a Failover Server.

Monitor Station Client

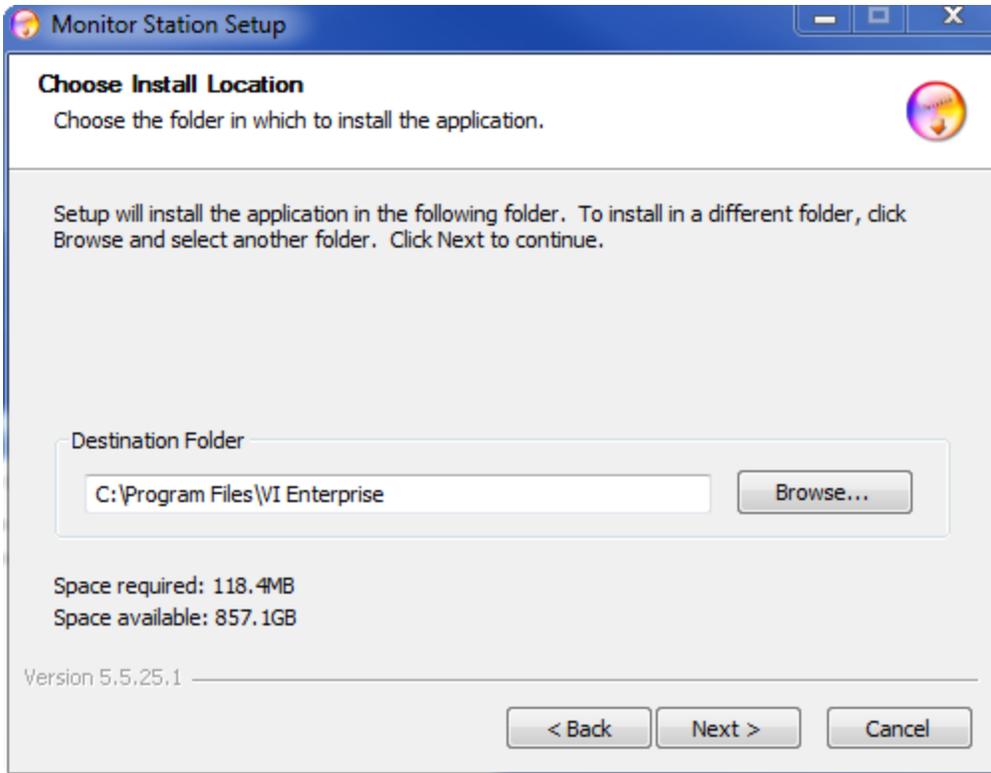
The Monitor Station client is installed automatically with either IP Server install or IP Server installation with an existing SQL installation so a client is easily accessible from the server. In some cases a client-only install is needed for active visitor monitoring personnel.

To perform a client-only installation:

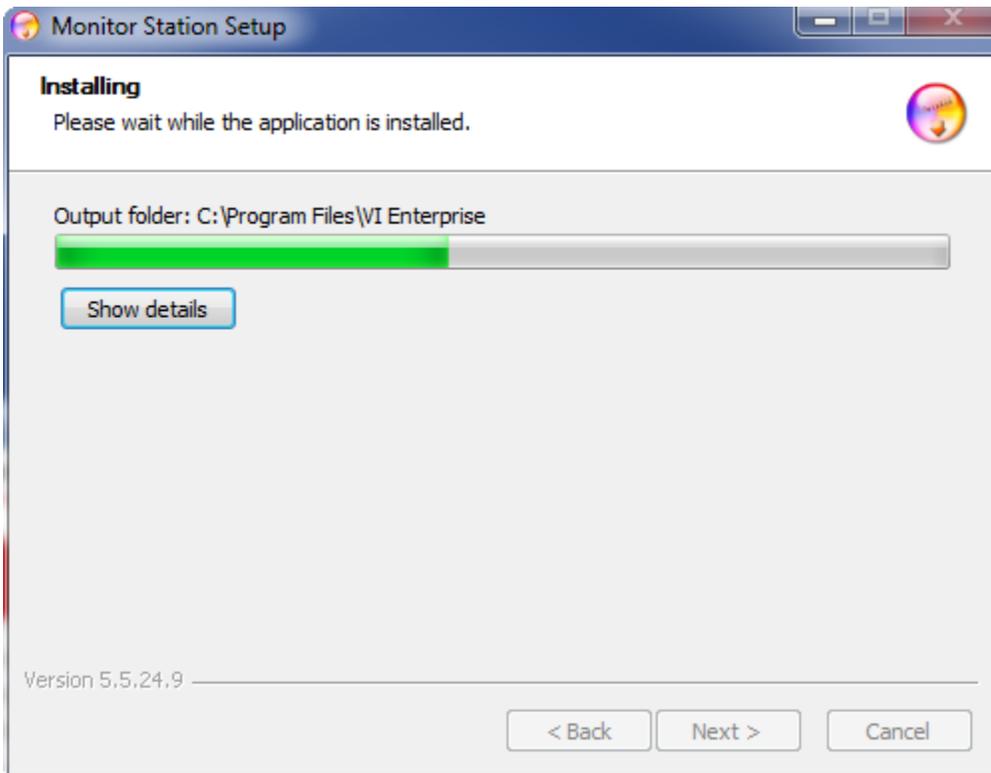
1. Double-click the Setup executable applicable to your system type: 32- or 64-bit OS.



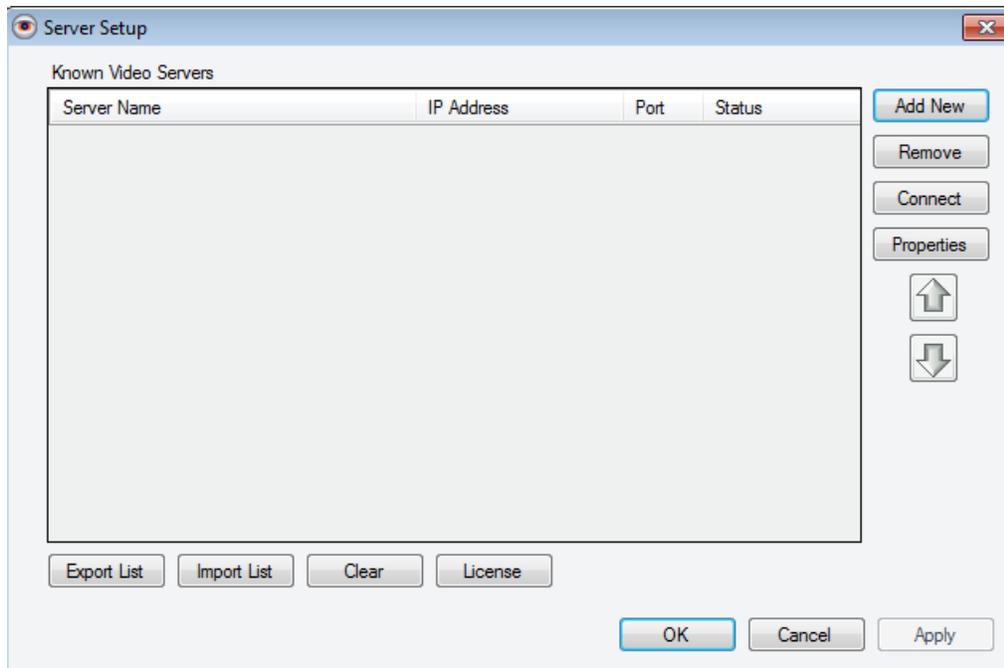
2. Click **I Agree** to accept the terms and continue the installation. If you do not agree or do not want to continue the installation, click **Cancel**. Select Monitor Station install and then click **Next**.



3. To accept the default destination folder, click **Install**. To choose another destination enter the destination path or click **Browse**, then click **Install**.



4. When installation is complete, click **Next**.
5. Click **Finish**.
6. Click **Yes** if prompted to reboot.
7. Monitor Station is now installed and ready to be initialized and configured. Double-click the Monitor Station icon on your desktop.
8. Enter login credentials or accept the default login, and click **OK** to continue.
9. At least one server must be entered into the Server Setup dialog box before the client can be used.

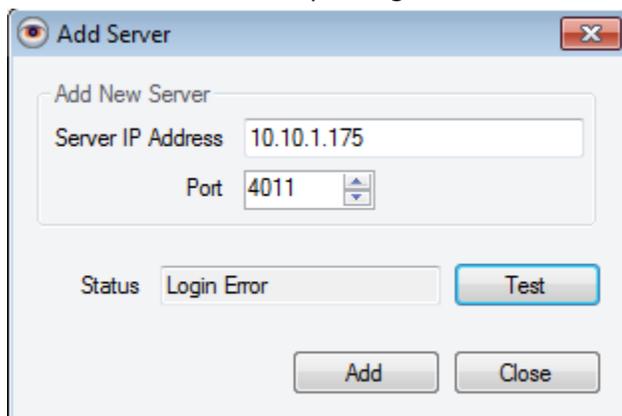


You can enter server information one server at a time or add servers automatically.

Adding servers manually

To add a server manually:

1. In the Server Setup dialog box click **Add New**.



2. Enter the IP address or name of the server to connect to, and the port if different from the default.
3. Click **Test** to initiate a connection. There are three possible outcomes:

Login Error: The server is found but security is on and the server attempted to authenticate the login with the initial credentials used to login to Monitor Station. The server default login is Administrator/*blank for the password*). You can still add the server. Then logout of Monitor Station login again with the right credentials.

No Server Found: Either the IP address, server name, server port or both are incorrect. Enter the correct values and then click **Test** again.

Server Found: The server is found and a successful connection was made using the current credentials (Administrator/blank). The server's name is displayed in the Status field.

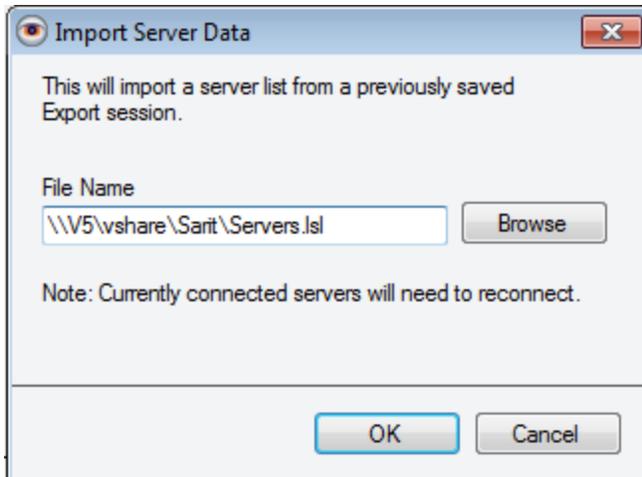
4. Click **Add**.
5. Repeat steps 1-5 for additional servers if needed.
6. Click **Apply** and then **OK**.

Adding servers automatically

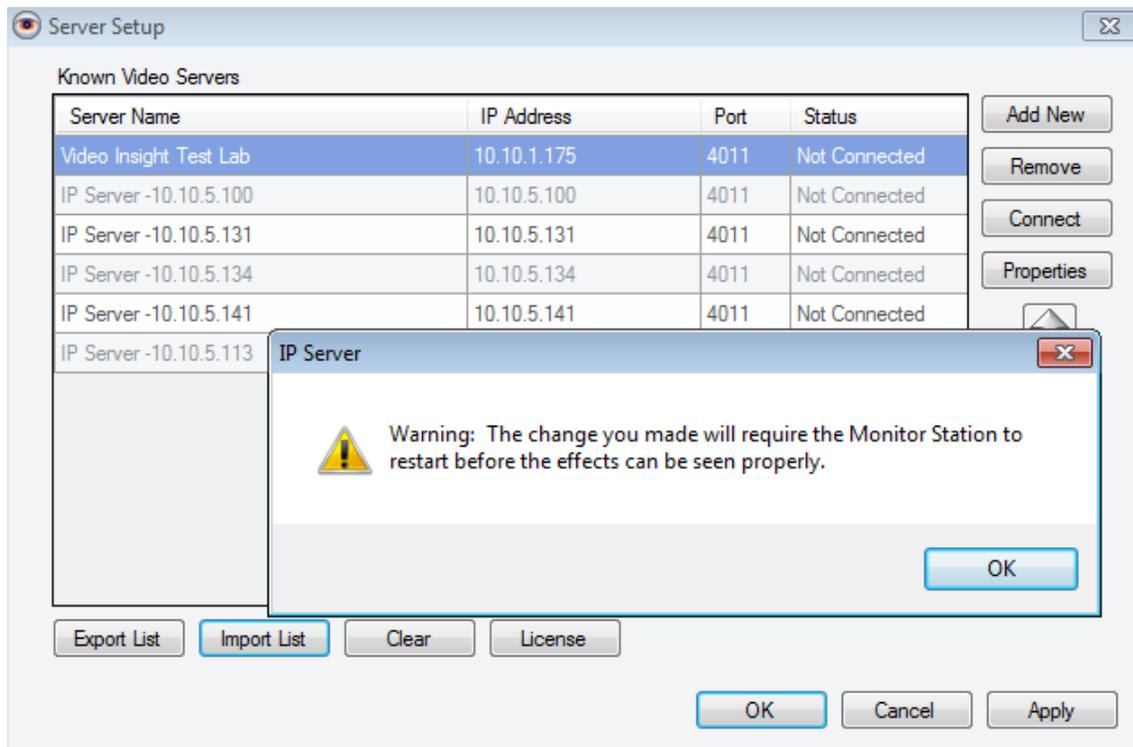
In a large organization it is possible to have upwards of 20 video surveillance servers across multiple locations. You can easily add a long list of servers at one time using the import feature.

You need an exported list of servers before you can import them using this feature. The file format is .LSL. See the [Login](#) section for instructions on how to create this file.

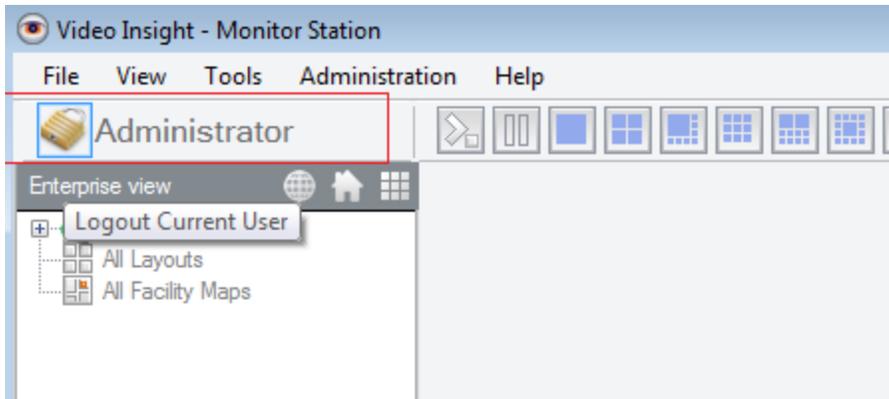
1. In the Server Setup dialog box click **Import List**.
2. Enter the file name or click **Browse** to go to the location of the saved .LSL file.



3. Click **OK**.
4. If the file is unreadable or not found an error will display. If the import is successful the full list of servers will display in the Known Video Servers grid. You will be prompted to restart Monitor Station.



5. Click **OK**.
6. Click **Apply** and then **OK**.
7. Restart Monitor Station by clicking the Lock icon on the upper left of the main dashboard.



8. Enter the credentials to login to the desired server(s) or click **OK** to bypass the Login dialog box without any credentials.

Web Client

You can use the Web Client to view live or recorded video from anywhere using a supported browser. Support browsers are:

- Microsoft Internet Explorer with optional ActiveX-plug-in
- Google Chrome
- Apple Safari

You can use the Web Client to control PTZ cameras and playback recorded video. The system supports multiple users and is tightly integrated into the Windows operating system for complete security.

The Web Client is automatically installed if Microsoft IIS is configured.

Configuring IIS

Consult your operating system manual for information on how to install and configure IIS.

Accessing the Web Client

Version 5.5 of the Web Client offers:

- Seamless playback
- Simplified navigation
- Intuitive clip creation
- Optional H.264/MPEG streaming
- Snapshot Feature
- Customization
- Advanced configuration

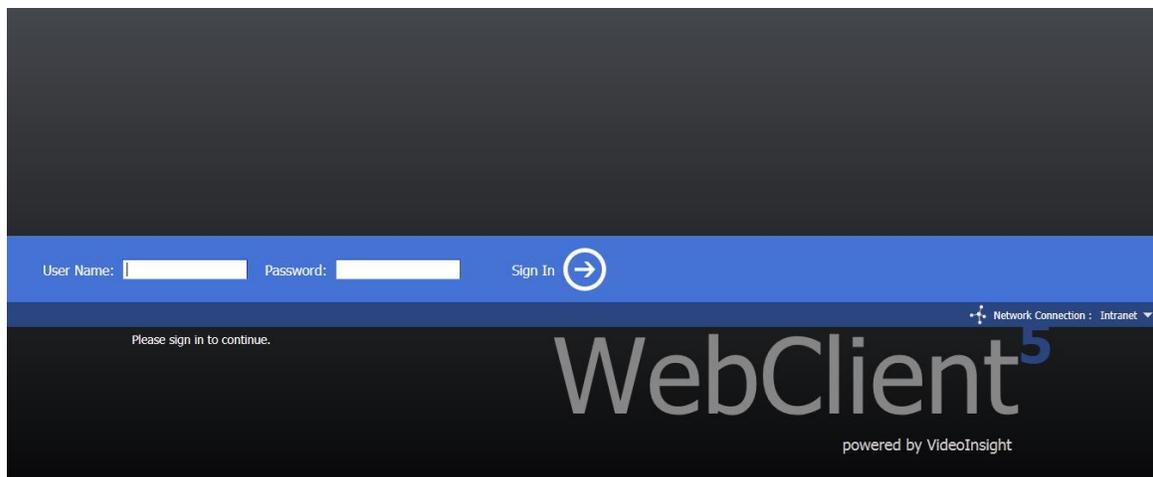
To start the Web Client:

1. Start your Internet browser.

2. Navigate to [http://\[your server's IP address\]/videoinsight/default.aspx](http://[your server's IP address]/videoinsight/default.aspx).
3. If Security is off, you will see servers and cameras ready for viewing. If Security is on a login, a prompt displays.

Note

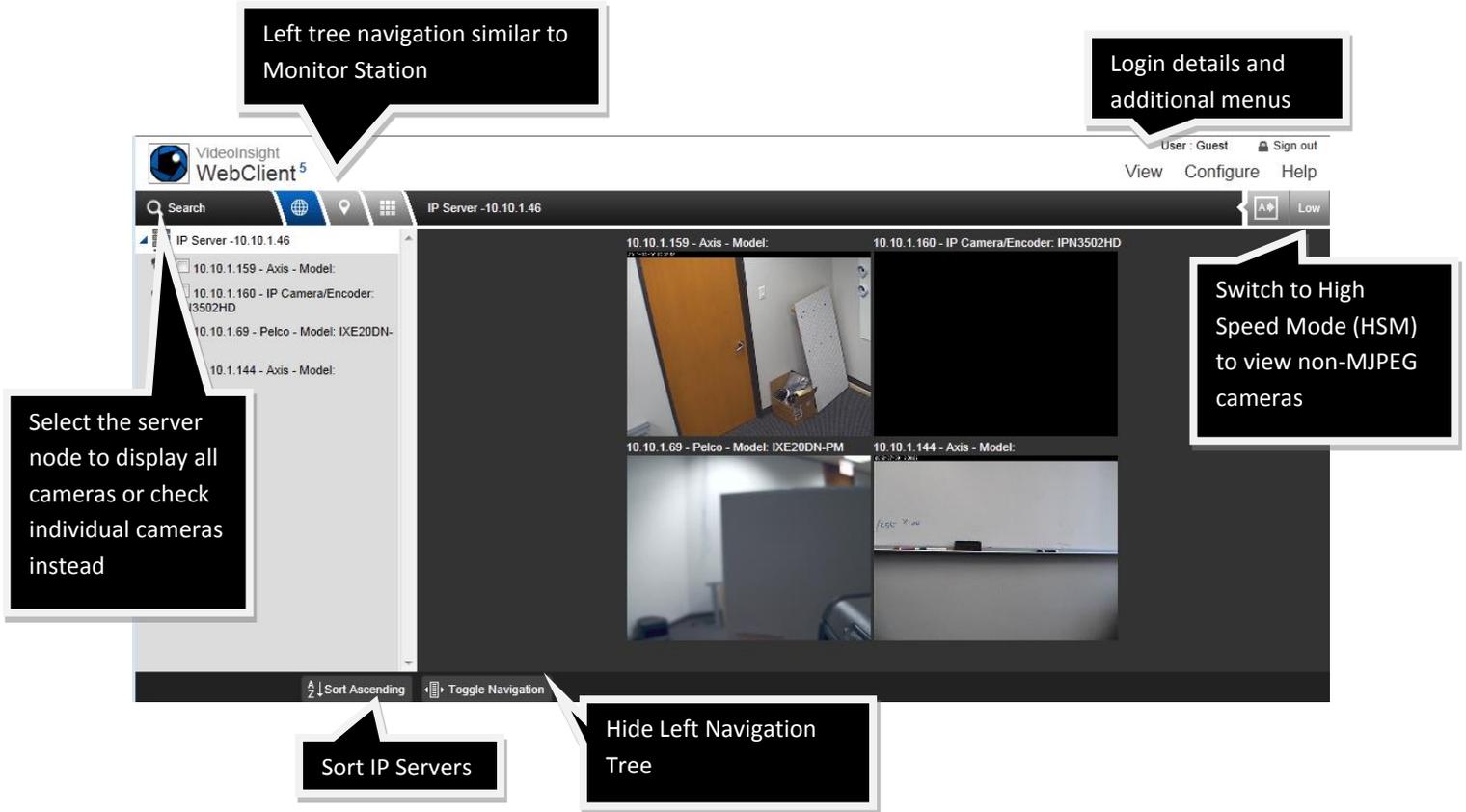
The Profile option is used primarily when you are accessing the system over the Internet or when you need to limit how much bandwidth you use for video. For example, you can have an intranet user profile that permits high-speed video over a LAN and an Internet user profile that limits video frame rates for use on slower Internet connections.



4. Enter your user name and password.
5. Select a profile from the drop-down menu.
6. Click **Sign In**.

Using the Web Client

After login the Web Client displays as shown in figure below.



Left navigation tree structure

The left navigation tree structure in the Web Client functions in much the same way as in the Monitor Station. At the top of the tree there are three options for sorting the tree:

-  Enterprise View (default)
-  Facility Map View
-  Layout View

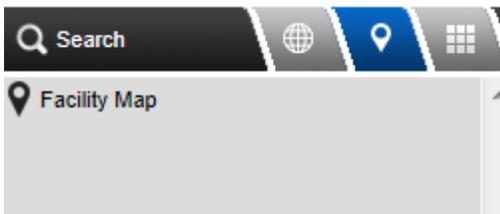
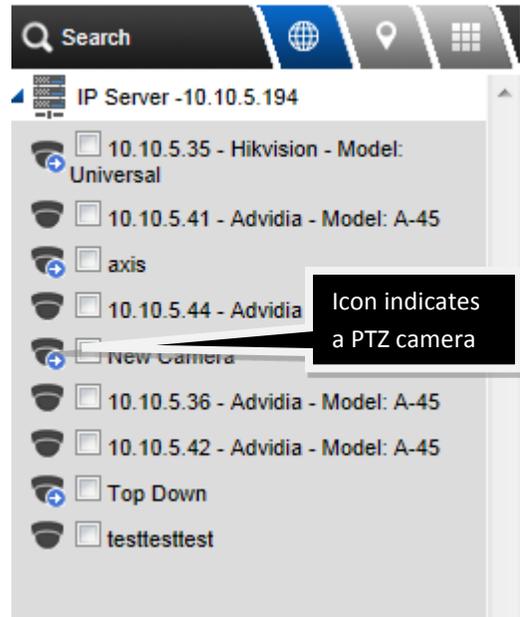
Enterprise View

Enterprise View is the default view and orders the navigation tree based on the server hierarchy. You can use this view to display cameras, layouts and facility maps for each server.

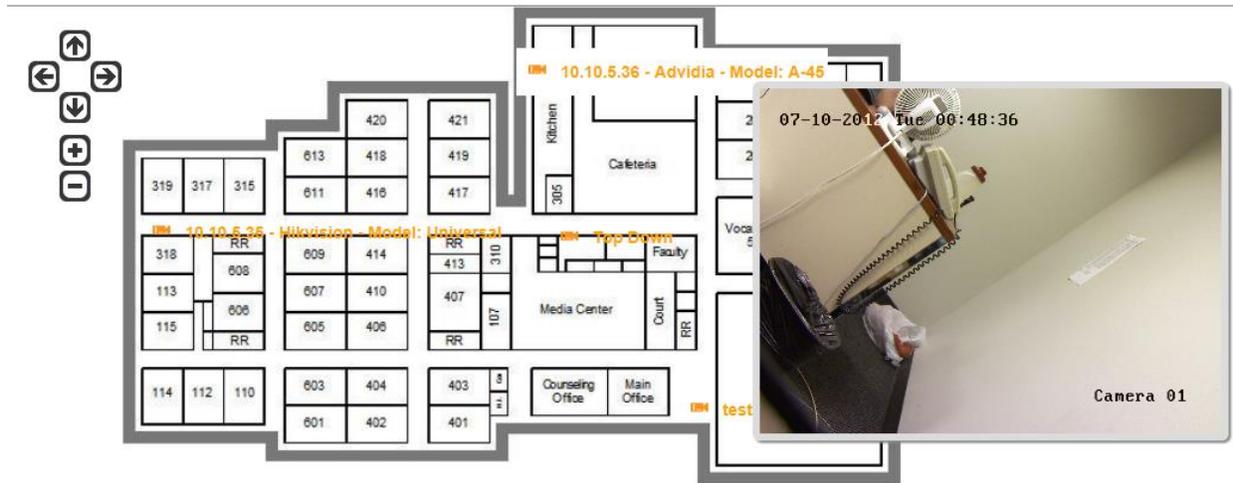
You can click the magnifying glass to search all of the Enterprise, Facility Maps and Layouts nodes.

Facility Map View

Facility Map orders the navigation tree based on the facility hierarchy. You can use this view to display cameras and layouts for each facility map.



Selecting a facility map displays it in the viewing pane. Moving the mouse over a camera icon on the map brings up a live view from that camera.

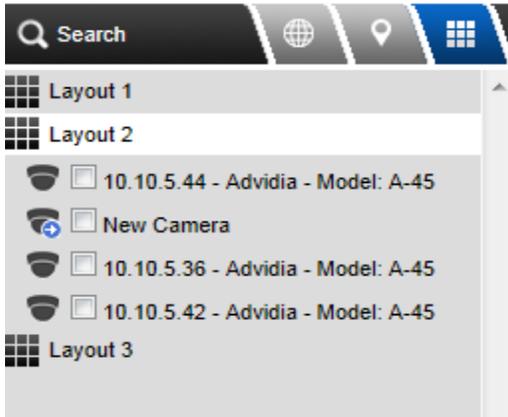


Use the arrow controls to move the Facility Map or use the plus and minus controls to zoom in or out.

Layout View

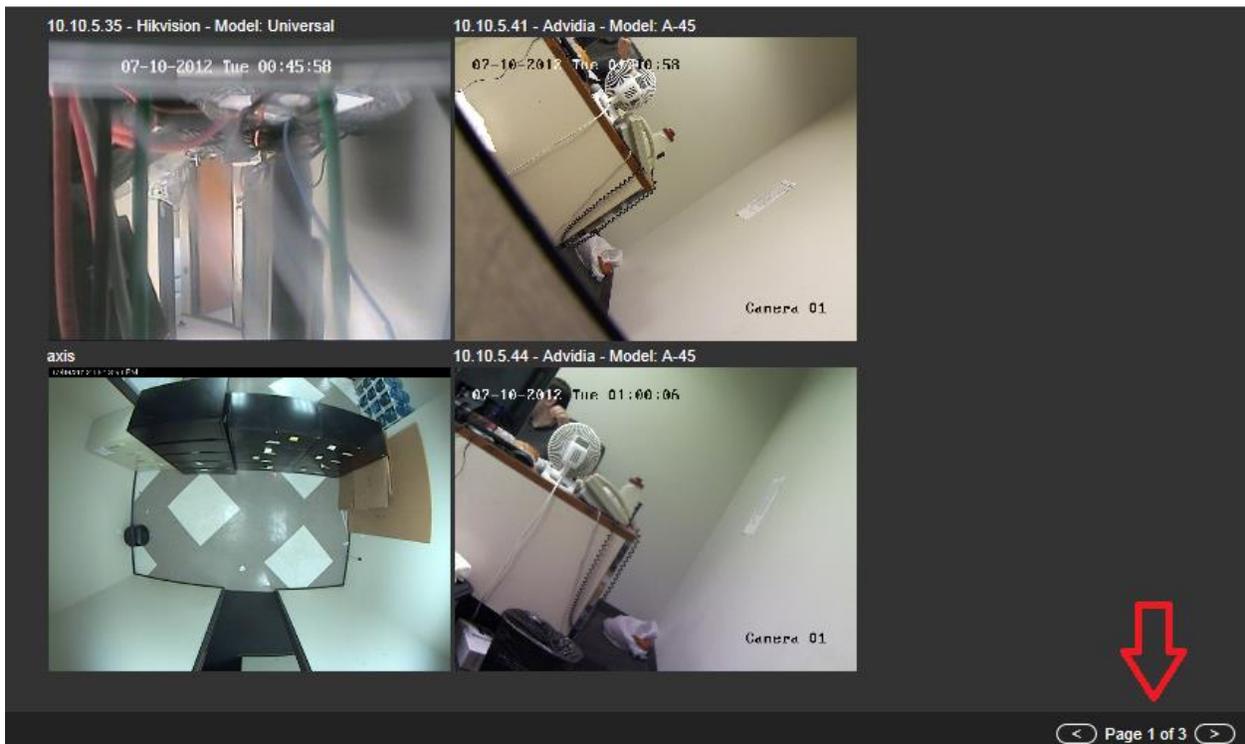
Layout View orders the navigation tree based on the layout hierarchy. You can use this view to display cameras for each layout.

Selecting the layout from the tree displays the layout on the right side of the screen. You can also select individual cameras from each layout, or mix and match multiple layouts and cameras by checking the box next to each item. Expand a layout by clicking the Layout name to view the included cameras.



Layouts toolbar

The collapsible section in the top right offers several different options for layouts. Click the desired layout to rearrange the cameras. If the number of cameras selected exceeds the number of cameras displayed by the layout view, the extra cameras are viewable on pages accessible at the bottom-right of the screen, as shown in Figure x.



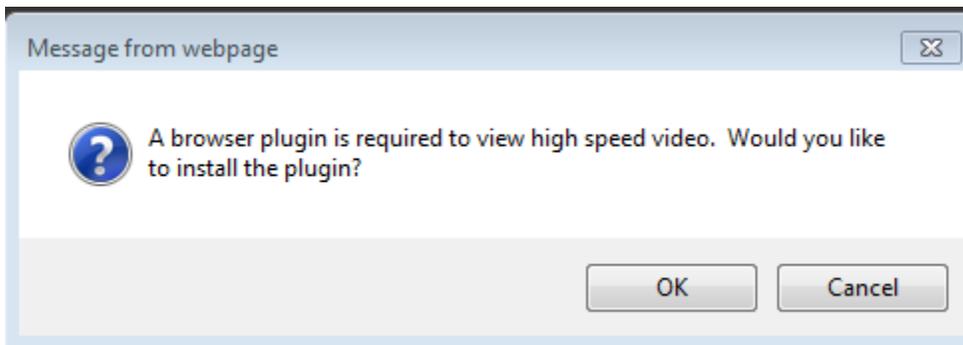
You can also have a layout automatically selected for the number of cameras checked. For example, if only one camera is currently displayed and there are four cameras checked, click the  icon and the view will automatically change to the 2x2 layout.

High Speed mode

Low Speed mode is the default streaming mode which utilizes higher bandwidth and higher processing power on the server. However, you may need a better refresh rate or you may be viewing MJPEG cameras High Speed Mode has the added benefit of lower bandwidth.

To activate High Speed mode:

1. Click the  button in the Layout toolbar to turn on high speed mode.



2. Click **OK**.

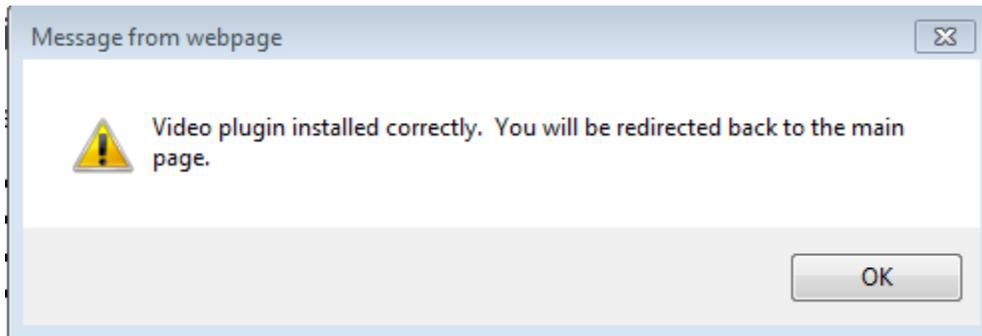
VideInsight Video Control

Installing the latest video plugin provides :

- High speed streaming video
- Support MPEG-4, H.264, & other video standards
- Lower bandwidth usage
- DirectX hardware rendering (with supported graphics cards).



3. Click **Install now**.



4. After the ActiveX plug-in successfully installs, click **OK**.

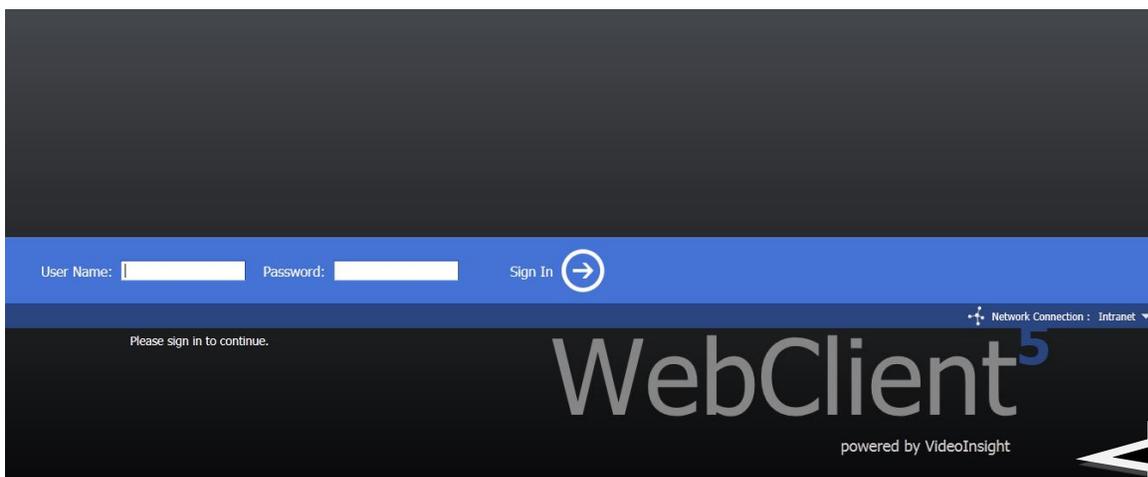
Configuration menu

The Configuration menu has several options for further customization. When you make changes to options available on this menu they affect ALL other Web Clients connected to the server.

1. Click **Configure**. The notification shown in the figure below displays even if Security is on.

You do not have permission to modify settings. Please [sign in](#) with an administrative account.

2. Click the sign in link.



3. Enter an Administrator-level user name and password and then click **Sign In**.
4. Click **Configure** again.

You can change options in four categories:

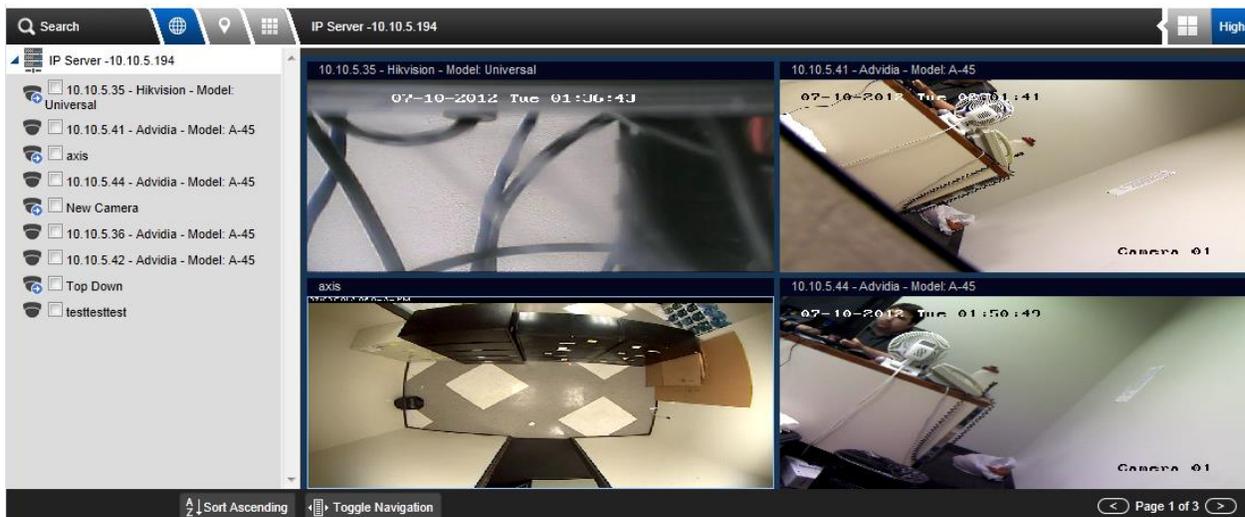
- Video
- Navigation
- Content
- Login

Video

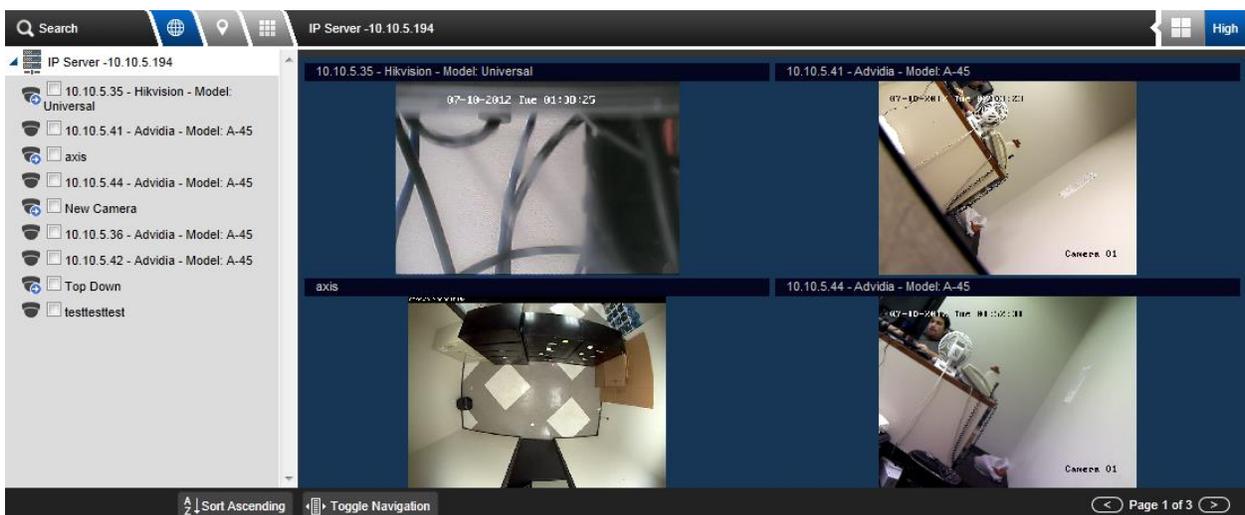
Set to high speed by default – This option applies to Internet Explorer only and prompts all subsequent Web Client connections to install the High Speed Mode ActiveX plug-in.

Preserve aspect ratio – All cameras are displayed at a 4:3 aspect ratio for layout and maximized use of the viewing area, but you can check this box if you want to display the camera's actual resolution.

The figure below shows a layout without Preserve aspect ratio checked.

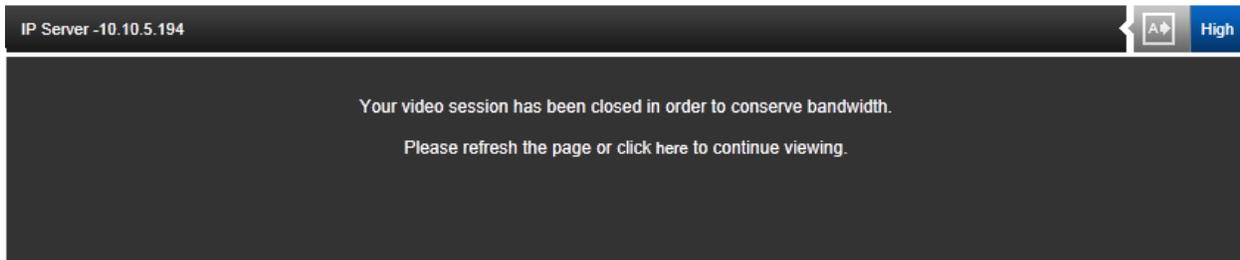


The figure below shows the same layout with Preserve aspect ratio checked.



Buffer recorded video – Every time recorded video is played back a temporary file is created in the local TEMP directory for faster viewing later. Buffering recorded video this way obviates the need to download video files over and over again. You can delete these files from the directory if local storage consumption becomes an issue.

Limit video streaming to 'X' minutes – Zero is the default value and means there is no time limit for live streaming. You can change this value if you do not want to waste bandwidth on inactive viewers. The figure below shows a video session that has timed out due to inactivity.



You can resume streaming by clicking where indicated or refresh your browser.

Navigation

Navigation

- Show navigation panel
- Show Enterprise by default
- Show Maps by default
- Show Layouts by default

You can hide the navigation panel by unchecking the box for Show navigation panel.

Content

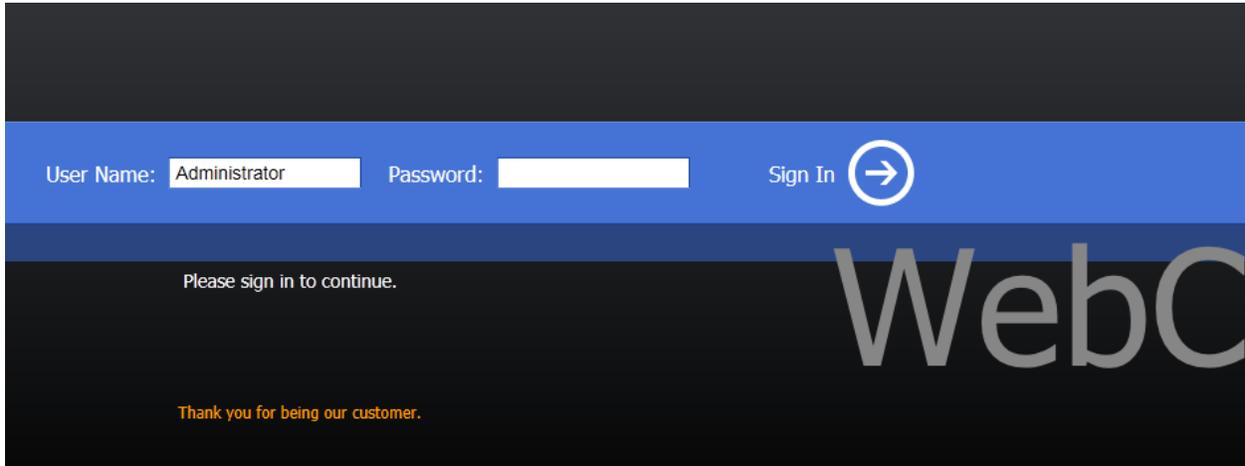
Stretch map to fit screen – This option stretches a smaller facility map to fill most of the Facility Map viewable area.

Show camera labels – This option is checked by default, but when unchecked camera names are not displayed on the facility map, just the camera icon.

Show map labels- This option is unchecked by default, but when checked the nested Facility Map name displays on the map.

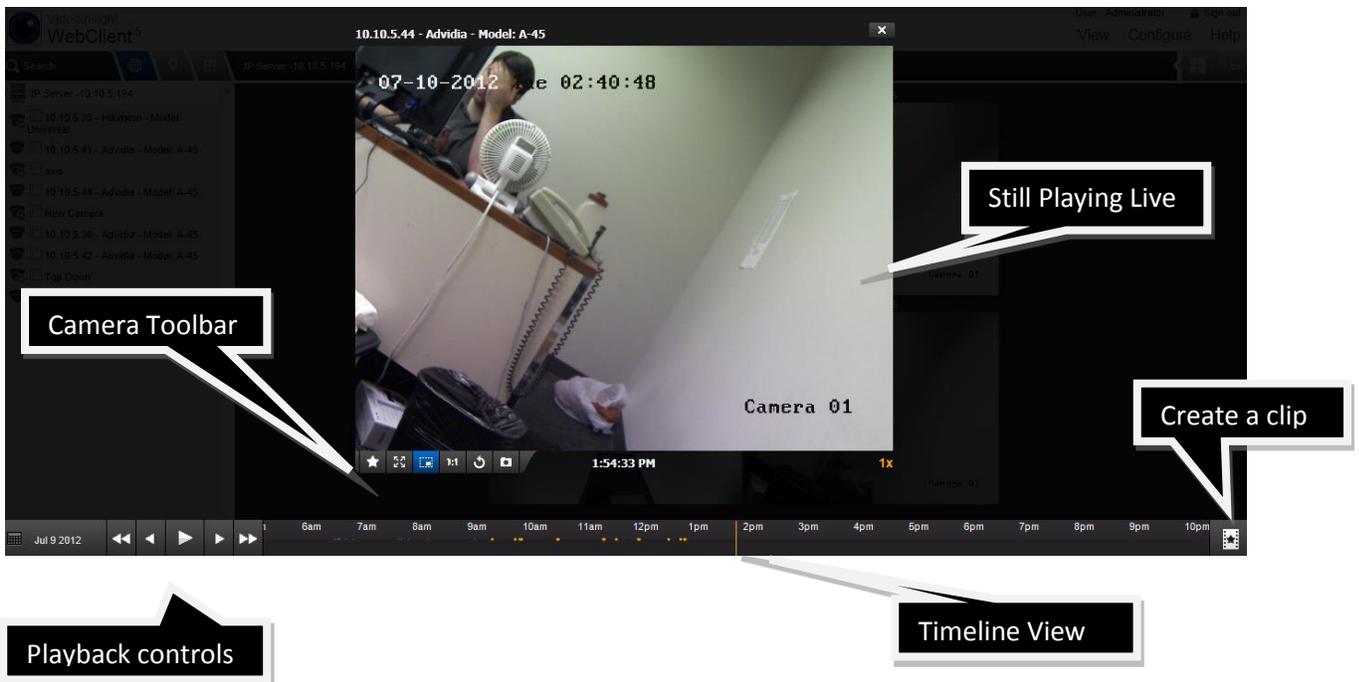
Login Message – This is an empty text field by default. You can use it to display a message up to 255 characters long to Web Client users. The message displays on the main login page when Security is on or when accessing the Configure menu.

The figure below shows a sample message.



Viewing recordings

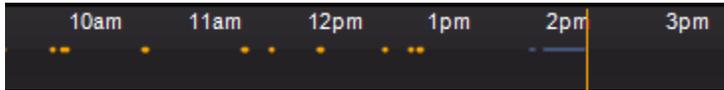
You can view a recording using the Web Client by clicking a camera from the live view. When you click a camera in the live view it is brought into focus as shown in the figure below.



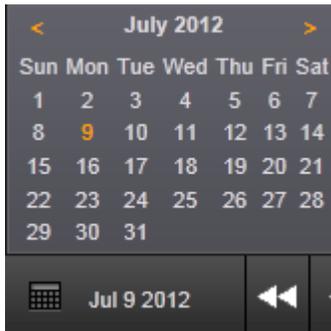
The timeline at the bottom indicates the time and type of recording. Orange dots indicate a recording of motion events only, and a solid blue line indicates a recording without motion events.

To begin playing, click and hold the time point and drag it left or right, then release it at the point desired.

The figure below shows a camera timeline where the recording type was changed from Motion-only to Record Always.

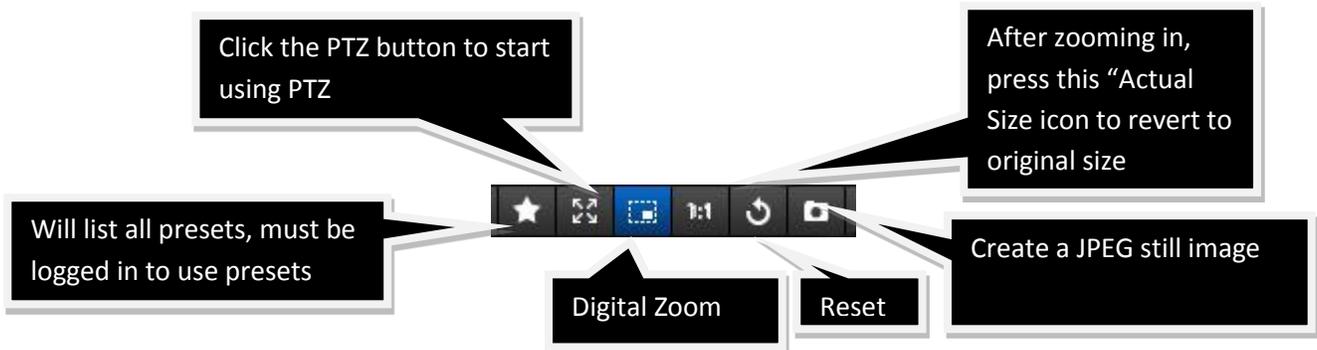


You can expand the calendar on the bottom left to see if recordings are available for a particular day. Days with recordings are indicated by orange text.



Camera toolbar

The camera toolbar at the bottom of the view has several functions:



To create a clip for later playback or distribution:

1. Click the  icon.



2. Drag and drop the time point or enter the exact time.
3. Use the blue handles to lengthen or shorten the clip time.

4. Click the  icon to begin the download.



5. When the progress bar reaches 100%, choose whether to save or open the clip.

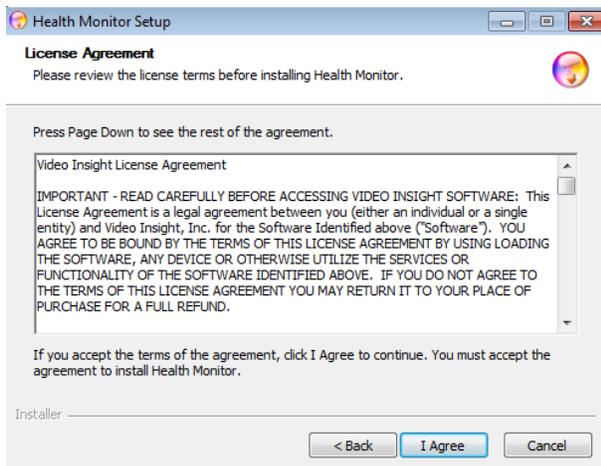
Health Monitor

To install Health Monitor:

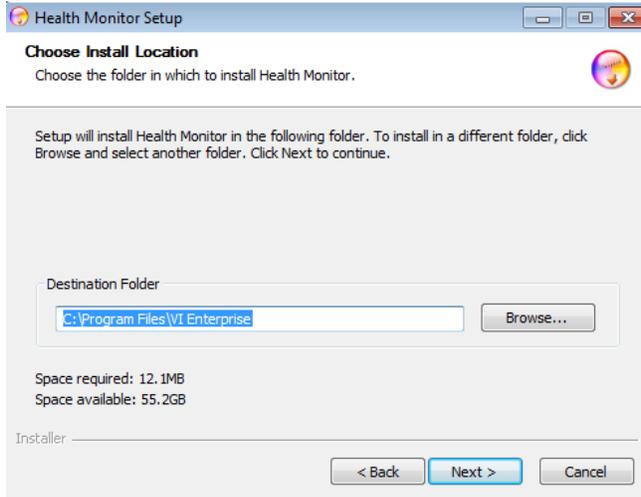
1. Double-click accsetup.exe.



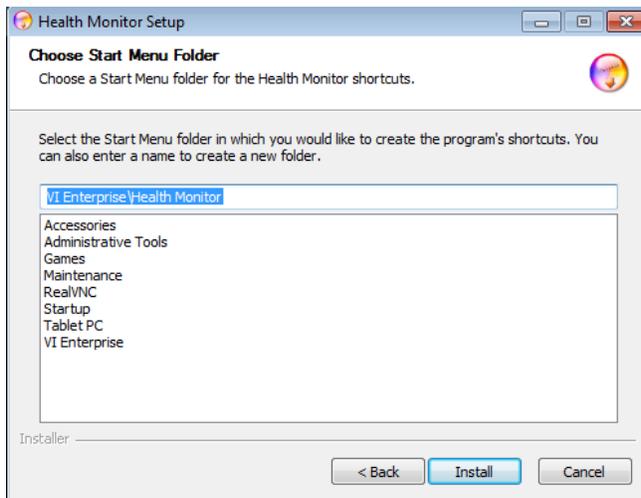
2. Click **Next**.



- Click **I Agree** to accept the License Agreement and continue, or click **Cancel** to terminate the installation.



- Accept the default destination folder or enter or browse to another location. Click **Next**.
- Click **Install**.



- Accept the default Start Menu folder or enter or select another. Click **Install**.
- Click **Finish**.

Customization

Video Insight software offers features and capabilities beyond those addressed during installation and initial configuration.

IP Server

After IP Server is installed and configured, you can use both Monitor Station and the [IP Server Manager Utility](#) to customize server settings. Administrative-level access is required to make changes.

Note

You can also access Server Properties by navigating to Administration, selecting Set up and Configuration and then selecting your server.

To customize IP Server using Monitor Station:

1. Launch Monitor Station.
2. Right click the server name in the left navigation pane and select Properties.

Setup and Configuration tab

The Server and Configuration tab displays information about the server, database and video storage path. It is the same tab that displays during IP Server initialization.

Setup and Configuration | Cameras | Advanced | Health Monitor | Client | Access Configuration | Contact Information

Server Identification

Server Name: Video Insight Test Lab

IP Address: 10.10.1.175

Version: 4.3.0.58

Database Information

Sql Server Location: localhost

Advanced

Video Storage

Video data storage path *

C:\video

* Note: If using a Network Drive, use the UNC path (i.e. \\v4\share\video)

Note

Recording to a shared location requires a user with write permission to that share or recordings will not be saved.

Server Name: The default is “IP Server –“and the detected IP address of this server. You can change this to a more friendly or meaningful name. Do not use special characters.

IP Address: This is the selected server’s IP address and should not be changed.

Version: The current version of the software.

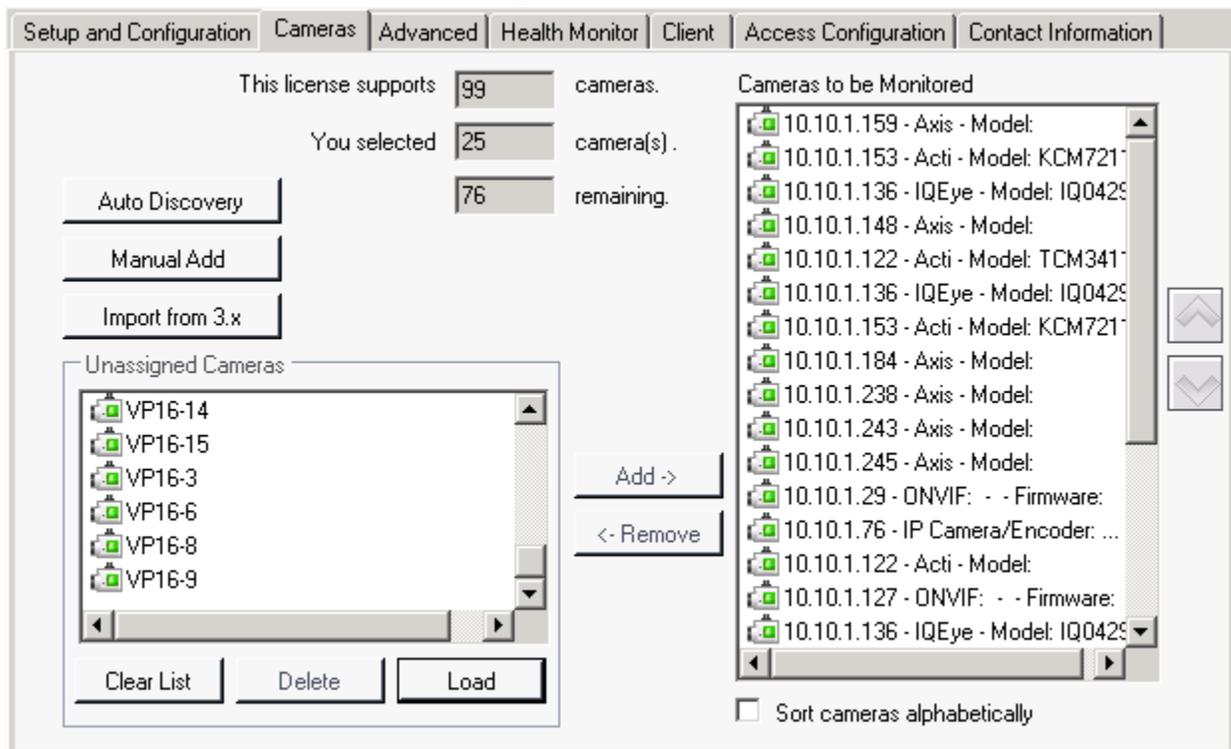
SQL Server Location: This is the location or IP address of the database server. ‘Localhost’ indicates that the database and Microsoft SQL server are local to the host computer. An IP address in this field indicates the Microsoft SQL Server is located on another computer. Click **Advanced** to modify the database connection string values: Database Name, IP Address, SQL Server User ID and Password. To change advanced SQL settings, use [IP Server Manager Utility](#).

Video Data Storage Path: This is the location where all the recorded video will be saved. The default is the local OS drive (i.e., C). The video folder is created automatically once server configuration is completed. You can choose to save video to several different locations:

- **Local server drive:** For example, C:\video
- **Alternate additional drive:** For example, D:\video
- **Shared drive:** For example, \\v5\share\HHSvideo

Cameras tab

The Cameras tab displays information about monitored cameras, unassigned cameras and camera licenses. It is a centralized location to manage cameras on a server.



This license supports: Shows the maximum number of IP cameras allocated to the serial number assigned to the server. Using a Video Insight encoder such as the VP16 will show a value of zero in this field, but all 16 channels of the encoder can be added.

The license count adjusts automatically as cameras are added to or removed from a server.

You selected: The number of cameras in the Cameras to be Monitored pane.

You can add cameras in two ways: **Auto Discovery** and **Manual Add**

Unassigned Cameras: This field shows all cameras that are not assigned to the selected server. These cameras were previously added and removed and remain in the database for reuse. If sharing a database with multiple servers you can quickly un-assign cameras from one server and re-assign them to another server using this tab. Unassigned cameras do not use a license.

Click **Clear List** to permanently delete all unassigned cameras, **Delete** to permanently delete the selected camera, and **Load button** to load cameras from the database.

Cameras to be Monitored: This field shows all cameras assigned to the selected server. Each camera in this field uses a license. You can reorder their position in the Main dashboard by selecting a camera and clicking either the up or down buttons. You can also check the box to sort them alphabetically.

Advanced tab

The Advanced tab displays information about server, view and record options.

The screenshot displays the 'Advanced' tab of the Video Insight Administrator interface. The interface is divided into several sections:

- Server Options:** Contains five checkboxes: 'Enable Motion Log' (checked), 'Enable System Log' (checked), 'Enable Security' (checked), 'Designate Server as Failover Server' (unchecked), and 'Allow only one login per user' (unchecked). There are two 'Keep' fields, each set to '30' days.
- Record Options:** Contains a 'Reserve space for other applications' field set to '5' GB.
- Live Display Options:** Contains a 'Server timeout' field set to '30' minutes (0 to turn off).
- View Options:** Contains a section for 'Optimize Video Streams' with two radio buttons: 'Low CPU \ High Bandwidth' (selected) and 'High CPU \ Low Bandwidth' (unselected).

The interface also shows a navigation bar at the top with tabs for 'Server Configuration', 'Cameras', 'Advanced', 'Health Monitor', 'Client', 'Access Configuration', and 'Contact Information'.

Enable Motion Log: The default for this field is 30 days. The maximum number is 1000. In order for the server to save the Motion Log at least one camera must be using Motion-only Recording or Record Always with the [Calculate Motion Detection](#) checkbox found on each camera's Record tab. All Motion Logs can be viewed from either the [Alarm Log](#) or Motion Events.

Enable System Log: The default for this field is 30 days. The maximum number is 1000. The System Log is a great way to track user actions, server and camera changes as well as troubleshoot issues. See [System Log](#) for more information.

Enable Security: Security is off by default. In this state any user can modify both Client and Server settings. Check the box to turn Security on. When checked, both admin and non-admin users must have valid credentials to login. See [Security](#) for more information on security.

Designate Server as Failover Server: Check this box to assign the role of Failover Server to this server. A Failover Server is used to assume responsibilities of recording and monitoring in the event that another server fails.

Server timeout sets the timeout period at which point the Monitor Station will no longer receive video streams and will pause. Server timeout is set at the server level; however, it is Monitor Stations and Web Clients that are checking for activity. Activity is defined as mouse movement. For example, a Monitor Station has an active user who is viewing several cameras while actively moving the mouse from pane to pane. Another Monitor Station has the application running and a passive user. With a Server timeout set to five minutes, the first Monitor Station will remain active while the second Monitor Station will eventually pause. The software will stop the video stream when live video is paused. This reduces bandwidth consumption.

Allow only one login per user: Check this box to restrict the number of concurrent logins permitted per non-admin users from different IP addresses. Non-admin users can still login multiple times from the same computer. Checking this box does not restrict the number of logins an Administrator can have.

Reserve space for other applications: This option sets the amount of storage that will NOT be used by the Video Insight server to record video. The default is 5 GB, regardless of the save location. As recording video is a continuous process the server determines when storage is becoming limited and approaching Reserve Space, at which point the Server Deletion Routine will initialize to delete the oldest video first to free storage for new video. The deletion process only deletes one file at a time, not whole folders, to free storage.

The Server checks the amount of free storage every 5 minutes. When it is smaller than the amount of reserved storage the deletion routine executes. If the amount of Server storage is large enough, the Server will only need to delete the oldest day folder. If Server storage is extremely small or Reserved Disk Space is set high, the deletion routine will delete the current day's video, beginning with the oldest hour recorded.

Live Display Options: This area of the application will allow you to configure the time in which the server will stop displaying live video feeds.

Note

Reserve Disk Space is not an exact number; a percentage of the server Total Disk Space is also taken into account: Reserved Disk Space = Max (8% x Total Disk Space [Reserve Disk Space]). For example, with a 2 TB disk and Reserve Disk Space set to 10 GB, IP Server will reserve 160 GB. In another example, with a 50 GB disk and Reserve Disk Space set to 10 GB, we will reserve 10 GB.

Optimize Video Streams: You can choose Low CPU\High Bandwidth or High CPU\Low Bandwidth depending on your organization's infrastructure or policies. If you choose Low CPU\High Bandwidth you will be relying heavily on your network's performance to send uncompressed images directly to the Monitor Station. If you select this option you should carefully consider the resolution size, bit rate and FPS and number of cameras you will be using.

If you select High CPU\Low Bandwidth, video and image compression occurs at the server level. The server sends a compressed MPEG4 image to the Monitor Station or Web Client. The server compresses the image, sends them and then decompresses them. It allows the system to get a much higher frame rate over slower networks.

Health Monitor tab

The Health Monitor tab displays information about the Health Monitor service and server.

Health Monitor is a separate application available in the suite of Video Insight products aimed at monitoring the health of your servers. Only one Health Monitor is needed per farm of servers. See [Health Monitor](#) for instructions on installing and configuring.

Setup and Configuration | Cameras | Advanced | Health Monitor | Client | Access Configuration | Contact Information

The Health Monitor runs as a service in the background and monitors the receipt of messages from other video servers to ensure server uptime and reporting of any issues affecting the servers or cameras. The Health Monitor can be configured to send email alerts to the appropriate individual if messages from the servers are not received within the pre-determined time frame. The video servers also send messages to the Health Monitor on camera operation and disk storage usage.

Enable Health Monitor Server Name

Information to send to the Health Monitor	Health Monitor Server
<input checked="" type="checkbox"/> Version Number	IP Address <input type="text" value="10.10.1.154"/>
<input checked="" type="checkbox"/> Lost Signal	Server Port <input type="text" value="11000"/>
<input checked="" type="checkbox"/> Camera information	Send Frequency <input type="text" value="1 Min"/>

Enable Health Monitor: Check this box to have the server send a message to Health Monitor in preparation for its configuration in Health Monitor. Health Monitor will not be aware of the server until the server's properties are added to Health Monitor.

Version Number: Check this box to send the IP server version to the Health Monitor.

Lost Signal: Check this box to have the server notify the Health Monitor should a camera lose signal or a server stops responding. Time intervals are set in Health Monitor.

Camera information: Check this box to have the server include camera information when sending camera issues to Health Monitor.

Server Name: The IP Server's name is the default. You can edit this field.

IP Address: Enter the IP address of the Health Monitor server.

Server Port: The Health Monitor server port defaults to 11000. If this port is already in use, open another port and enter it here.

Send Frequency: The default is to send an email every minute. You can select interval of one minute to 24 hours.

Client Tab

The Client tab displays information about client communications.

The screenshot displays the 'Outgoing Email' configuration window within the 'Access Configuration' tab. On the left, there are three input fields: 'Use Data Port' set to 4010, 'Command Port' set to 4011, and 'Maximum Connections' set to 64. Below these is a button labeled 'Launch Windows Group Policy Editor' with a sub-label 'Group Policy Editor'. The main configuration area is titled 'Outgoing Email' and contains several sub-sections. The 'SMTP Server' is set to 'VIC4' and the 'SMTP Port' is set to 25. Under 'SMTP Logon Information', the 'User Name' is 'swilliams' and the 'Password' is masked with asterisks. Two checkboxes are present: 'SMTP server requires authentication' is checked, and 'SMTP server requires encryption (SSL)' is unchecked. At the bottom, the 'Send Test Email' section has an 'Email to' field, a 'Send' button, and an 'Email from' field containing 'TestMessage@IpVideoServer.net'.

Use Data Port: The port the IP Server uses to send live video to the Monitor Station.

Command Port: The port the Monitor Station uses to get and set system information.

Maximum Connections: The maximum number of Monitor Stations that can be connected to the server at one time. Additional processing power is required for each remote client connected.

Launch Group Policy Editor: This is an administrator feature in environments where the organizational security policy for video monitoring personnel is extremely limited. An administrator with appropriate credentials on the Monitor Station can launch the Microsoft Windows Group Policy Editor from this tab.

SMTP Server: Enter the SMTP server's IP address or its name.

SMTP Port: The default SMTP port is 25.

SMTP Logon Information: Checking the box for SMTP server requires authentication and enter the SMTP user name and password here. Missing or invalid credentials can result in emails not being sent to the intended recipients.

If the SMTP server uses SSL encryption for incoming and outgoing messages, check the box for SMTP server requires encryption.

Send Test Email: Enter an email address to send a test email to. Leave the default From email address TestMessage@IpVideoServer.net or enter another. You can also leave it blank, but some SPAM filters may prevent the email from going through without a From address.

Click **Send** to send a test email like shown in the figure below. Two entries will also be made in the System Log.

Test Email

VITestServer@IpVideoServer.net

Sent: Thu 12/22/2011 9:05 AM

To: Sarit Williams

Test Email

Depending on the performance of your infrastructure, it may take a few minutes for the email to be routed from the Monitor Station to the IP Server, then to the SMTP server and finally to the destination inbox.

Access Configuration tab

The Access Configuration tab displays information about access control options and doors. It is used to configure various access configuration systems. See [Access Control Configuration](#) for more information on access control configuration.

Setup and Configuration | Cameras | Advanced | Health Monitor | Client | Access Configuration | Contact Information

Enable access control support Access Control Type: Blackboard

Oracle Connection String

 Test

Access Configuration Options

- Log all card events in the event motion log
- Log Alarms in the system log
- Send alarms to Monitor Station
- Send entries to Monitor Station

Imported Doors

Door/Device Name	Server	Camera
Door Contact		Not set
Door Contact		Not set
Door Contact	Video Insight Tes...	Not set
Monitor Point #5	Video Insight Tes...	Not set
Monitor Point #6	Video Insight Tes...	Not set
Monitor Point #7	Video Insight Tes...	Not set
Monitor Point #8	Viden Insight Tes	Nnt set

Import Properties Delete Door Delete All

Polling Options

Update Alarms once every second(s)

Update Events once every second(s)

See [BlackBoard](#) and [MonitorCast](#) for more information on configuring these systems.

Contact Information tab

The Contact Information tab displays contact information for the server.

Setup and Configuration	Cameras	Advanced	Health Monitor	Client	Access Configuration	Contact Information																																				
<div style="border: 1px solid gray; padding: 5px;"> <div style="border-bottom: 1px solid gray; margin-bottom: 5px;"> <p>Server Information</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; border-right: 1px solid gray; padding: 5px;"> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">Server Name</td> <td><input type="text" value="Video Insight Test Lab"/></td> </tr> <tr> <td>Building</td> <td><input type="text" value="Science"/></td> </tr> <tr> <td>Floor</td> <td><input type="text" value="4th"/></td> </tr> <tr> <td>Room</td> <td><input type="text" value="313"/></td> </tr> <tr> <td>Phone</td> <td><input type="text" value="504-555-5555"/></td> </tr> </table> </td> <td style="width: 50%; padding: 5px;"> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">Description</td> <td><input type="text" value="This server manages a total of 200 cameras installed in and around the Science building."/></td> </tr> <tr> <td>City</td> <td><input type="text" value="Houston"/></td> </tr> <tr> <td>State</td> <td><input type="text" value="Texas"/></td> </tr> <tr> <td>Country</td> <td><input type="text" value="U.S.A"/></td> </tr> </table> </td> </tr> </table> </div> <div style="border-bottom: 1px solid gray; margin-bottom: 5px;"> <p>Contact Information</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; border-right: 1px solid gray; padding: 5px;"> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">Primary Contact</td> <td><input type="text" value="Officer Bert"/></td> </tr> <tr> <td>Secondary Contact</td> <td><input type="text" value="Judge Judy"/></td> </tr> <tr> <td>Police Number</td> <td><input type="text" value="713-281-HELP"/></td> </tr> </table> </td> <td style="width: 50%; padding: 5px;"> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">Primary Phone</td> <td><input type="text" value="713-281-2563"/></td> </tr> <tr> <td>Secondary Phone</td> <td><input type="text" value="713-504-3325"/></td> </tr> </table> </td> </tr> <tr> <td colspan="2" style="padding: 5px;"> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">Notes</td> <td><input type="text" value="We do have a failover server as a backup for this location in the event of a power failure or a network outage. That server's name is: Science2"/></td> </tr> </table> </td> </tr> </table> </div> </div>							<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">Server Name</td> <td><input type="text" value="Video Insight Test Lab"/></td> </tr> <tr> <td>Building</td> <td><input type="text" value="Science"/></td> </tr> <tr> <td>Floor</td> <td><input type="text" value="4th"/></td> </tr> <tr> <td>Room</td> <td><input type="text" value="313"/></td> </tr> <tr> <td>Phone</td> <td><input type="text" value="504-555-5555"/></td> </tr> </table>	Server Name	<input type="text" value="Video Insight Test Lab"/>	Building	<input type="text" value="Science"/>	Floor	<input type="text" value="4th"/>	Room	<input type="text" value="313"/>	Phone	<input type="text" value="504-555-5555"/>	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">Description</td> <td><input type="text" value="This server manages a total of 200 cameras installed in and around the Science building."/></td> </tr> <tr> <td>City</td> <td><input type="text" value="Houston"/></td> </tr> <tr> <td>State</td> <td><input type="text" value="Texas"/></td> </tr> <tr> <td>Country</td> <td><input type="text" value="U.S.A"/></td> </tr> </table>	Description	<input type="text" value="This server manages a total of 200 cameras installed in and around the Science building."/>	City	<input type="text" value="Houston"/>	State	<input type="text" value="Texas"/>	Country	<input type="text" value="U.S.A"/>	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">Primary Contact</td> <td><input type="text" value="Officer Bert"/></td> </tr> <tr> <td>Secondary Contact</td> <td><input type="text" value="Judge Judy"/></td> </tr> <tr> <td>Police Number</td> <td><input type="text" value="713-281-HELP"/></td> </tr> </table>	Primary Contact	<input type="text" value="Officer Bert"/>	Secondary Contact	<input type="text" value="Judge Judy"/>	Police Number	<input type="text" value="713-281-HELP"/>	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">Primary Phone</td> <td><input type="text" value="713-281-2563"/></td> </tr> <tr> <td>Secondary Phone</td> <td><input type="text" value="713-504-3325"/></td> </tr> </table>	Primary Phone	<input type="text" value="713-281-2563"/>	Secondary Phone	<input type="text" value="713-504-3325"/>	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">Notes</td> <td><input type="text" value="We do have a failover server as a backup for this location in the event of a power failure or a network outage. That server's name is: Science2"/></td> </tr> </table>		Notes	<input type="text" value="We do have a failover server as a backup for this location in the event of a power failure or a network outage. That server's name is: Science2"/>
<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">Server Name</td> <td><input type="text" value="Video Insight Test Lab"/></td> </tr> <tr> <td>Building</td> <td><input type="text" value="Science"/></td> </tr> <tr> <td>Floor</td> <td><input type="text" value="4th"/></td> </tr> <tr> <td>Room</td> <td><input type="text" value="313"/></td> </tr> <tr> <td>Phone</td> <td><input type="text" value="504-555-5555"/></td> </tr> </table>	Server Name	<input type="text" value="Video Insight Test Lab"/>	Building	<input type="text" value="Science"/>	Floor	<input type="text" value="4th"/>	Room	<input type="text" value="313"/>	Phone	<input type="text" value="504-555-5555"/>	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">Description</td> <td><input type="text" value="This server manages a total of 200 cameras installed in and around the Science building."/></td> </tr> <tr> <td>City</td> <td><input type="text" value="Houston"/></td> </tr> <tr> <td>State</td> <td><input type="text" value="Texas"/></td> </tr> <tr> <td>Country</td> <td><input type="text" value="U.S.A"/></td> </tr> </table>	Description	<input type="text" value="This server manages a total of 200 cameras installed in and around the Science building."/>	City	<input type="text" value="Houston"/>	State	<input type="text" value="Texas"/>	Country	<input type="text" value="U.S.A"/>																							
Server Name	<input type="text" value="Video Insight Test Lab"/>																																									
Building	<input type="text" value="Science"/>																																									
Floor	<input type="text" value="4th"/>																																									
Room	<input type="text" value="313"/>																																									
Phone	<input type="text" value="504-555-5555"/>																																									
Description	<input type="text" value="This server manages a total of 200 cameras installed in and around the Science building."/>																																									
City	<input type="text" value="Houston"/>																																									
State	<input type="text" value="Texas"/>																																									
Country	<input type="text" value="U.S.A"/>																																									
<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">Primary Contact</td> <td><input type="text" value="Officer Bert"/></td> </tr> <tr> <td>Secondary Contact</td> <td><input type="text" value="Judge Judy"/></td> </tr> <tr> <td>Police Number</td> <td><input type="text" value="713-281-HELP"/></td> </tr> </table>	Primary Contact	<input type="text" value="Officer Bert"/>	Secondary Contact	<input type="text" value="Judge Judy"/>	Police Number	<input type="text" value="713-281-HELP"/>	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">Primary Phone</td> <td><input type="text" value="713-281-2563"/></td> </tr> <tr> <td>Secondary Phone</td> <td><input type="text" value="713-504-3325"/></td> </tr> </table>	Primary Phone	<input type="text" value="713-281-2563"/>	Secondary Phone	<input type="text" value="713-504-3325"/>																															
Primary Contact	<input type="text" value="Officer Bert"/>																																									
Secondary Contact	<input type="text" value="Judge Judy"/>																																									
Police Number	<input type="text" value="713-281-HELP"/>																																									
Primary Phone	<input type="text" value="713-281-2563"/>																																									
Secondary Phone	<input type="text" value="713-504-3325"/>																																									
<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">Notes</td> <td><input type="text" value="We do have a failover server as a backup for this location in the event of a power failure or a network outage. That server's name is: Science2"/></td> </tr> </table>		Notes	<input type="text" value="We do have a failover server as a backup for this location in the event of a power failure or a network outage. That server's name is: Science2"/>																																							
Notes	<input type="text" value="We do have a failover server as a backup for this location in the event of a power failure or a network outage. That server's name is: Science2"/>																																									

The only default value on this tab is the Server Name. An Administrator can enter server information.

IP Server Manager

The IP Server Manager (IPSM) application is used to manage and troubleshoot advanced server settings. It is installed at the same time as IP Server.

The IPSM:

- Monitors the IP Server and presents visual status cues for each servers
- Provides a Diagnostics version of the IP Server Manager for troubleshooting and system optimization
- Manages IP Server network connections
- Manages licensing and registration
- Manages Lightweight Directory Access Protocol (LDAP) and Active Directory configuration

Options available in IPSM vary slightly depending on the installation type. See [Installation](#) for more information on installation types.

Accessing IPSM

The IPSM icon resides in the Windows System Tray. It has two possible states:

= Server is functioning properly; streaming video to clients, recording video and reporting to Health Monitor, if applicable



= Server is stopped and is NOT streaming or recording video

You can configure IP Server, manage the IP Server service, exit the application and see information about Video Insight by right-clicking on the IPSM icon.



Select Server Configuration to manage the IP Server service, configure IP Server and terminate the IPSM application.

Select Start IP Server, Stop IP Server or Restart IP Server to start, stop or restart the IP Server service.

Select Exit IP Server Manager to terminate the IPSM application and remove the icon from the Windows System Tray.

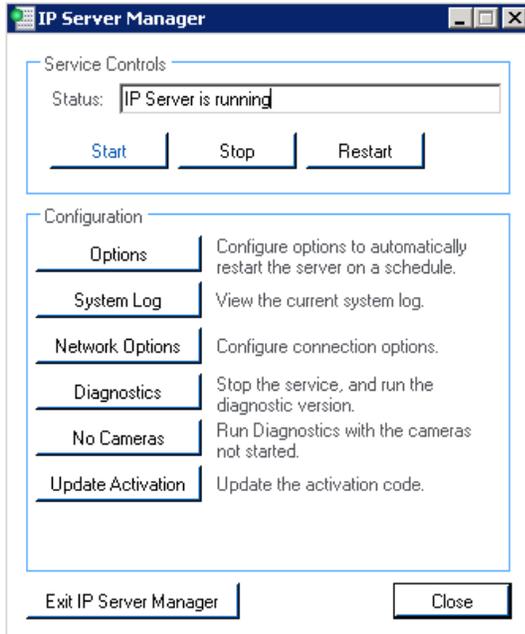
Note

Terminating the application prevents clients from remotely restarting the IP Server service.

Select About Video Insight to display version information, technical support information and legal terms.

Configuring IP Server

You can manage service controls and configure IP Server by right-clicking the IPSM icon in the Windows System Tray and selecting Server Configuration.



The Service Controls Status field displays IP Server service status. Click **Start**, **Stop** or **Restart** to start, stop or restart the IP Server service.

Clicking **Close** closes the IP Server Manager dialog box but does not exit IPSM. To exit the IPSM application, click **Exit IP Server Manager** to terminate the IPSM application and remove the icon from the Windows System Tray.

Note

Terminating the application prevents clients from remotely restarting the IP Server service.

Click a configuration button to perform other functions:

- Options – configure options to automatically restart the server on a schedule
- System Log – view the current system log
- Network Options – configure connection options
- Diagnostics – stop the IP Server service and run the diagnostic version
- No Cameras – run Diagnostics with cameras not started
- Update Activation – update the activation code

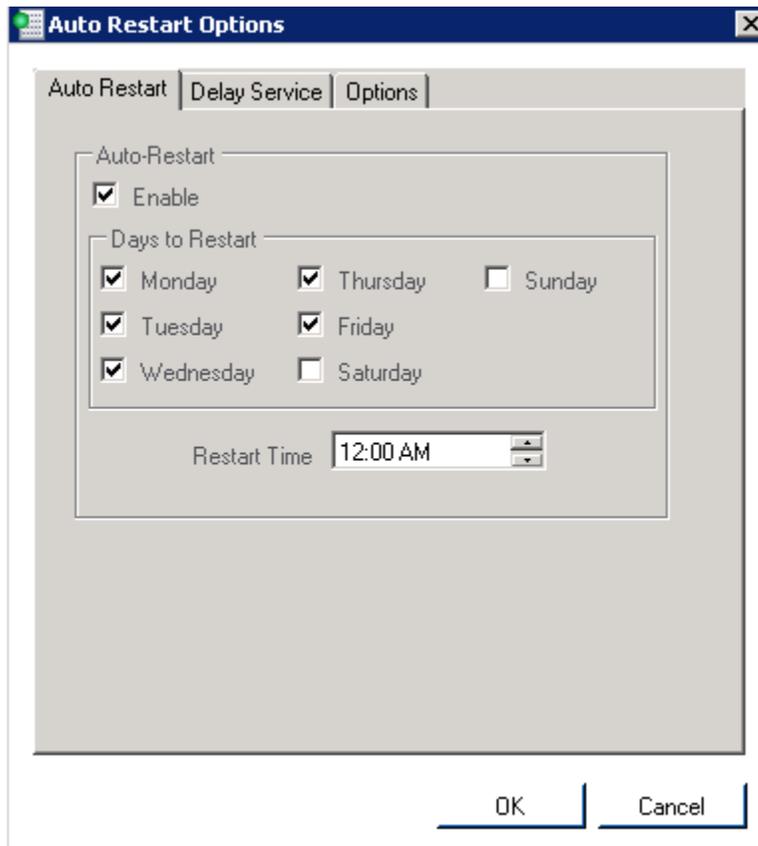
Each function is detailed below.

IPSM: Options

Clicking **Options** brings up the Auto Restart Options dialog box. This dialog box offers several settings aimed at mitigating some organizational and server environment settings that could interfere with the IP Server service.

Auto Restart

Restarting the service can refresh streaming, bandwidth and CPU performance by releasing used resources. You can choose to automatically restart the service on a specific day and time. This flexibility to restart means that you can schedule it so as to not interfere with business hours.

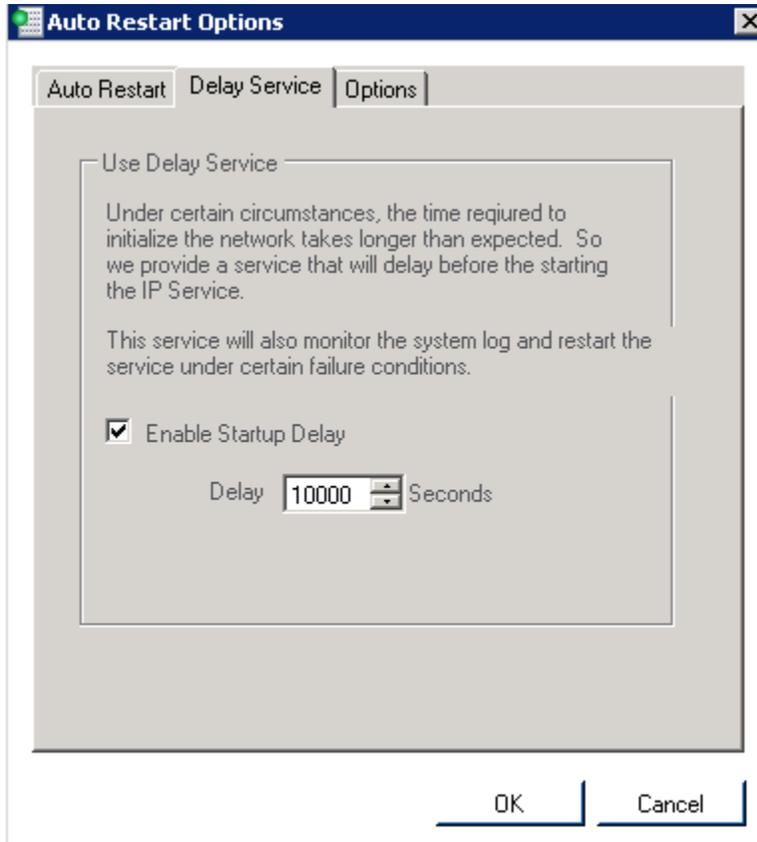


To set an auto-restart schedule:

1. Check the Enable box.
2. Select the restart day or days.
3. Select a restart time.
4. Click **OK**.

Delay Service

Delaying the IP Server service start is an option to consider if the server has many services that have to start in addition to the IP Service. The IP Server service may have trouble initializing without services such as the Microsoft SQL database service already running.

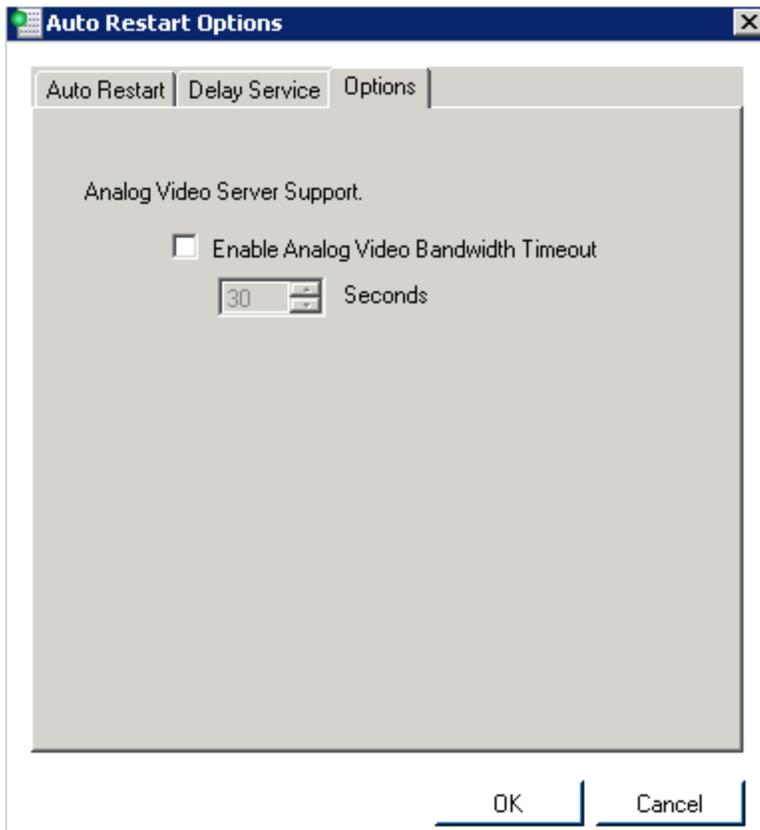


To set a startup delay:

1. Check the Enable Startup Delay box.
2. Select the startup delay time in seconds.
3. Click **OK**.

Options

In environments where both an Analog and an IP server are installed on the same server, and where bandwidth resources will likely be very highly utilized as a result, there is an option to restrict the Analog server's bandwidth consumption.



Enabling this option will terminate communication between the Analog and the IP server and no live streaming or recording will be done by the IP server when the timeout threshold has been reached.

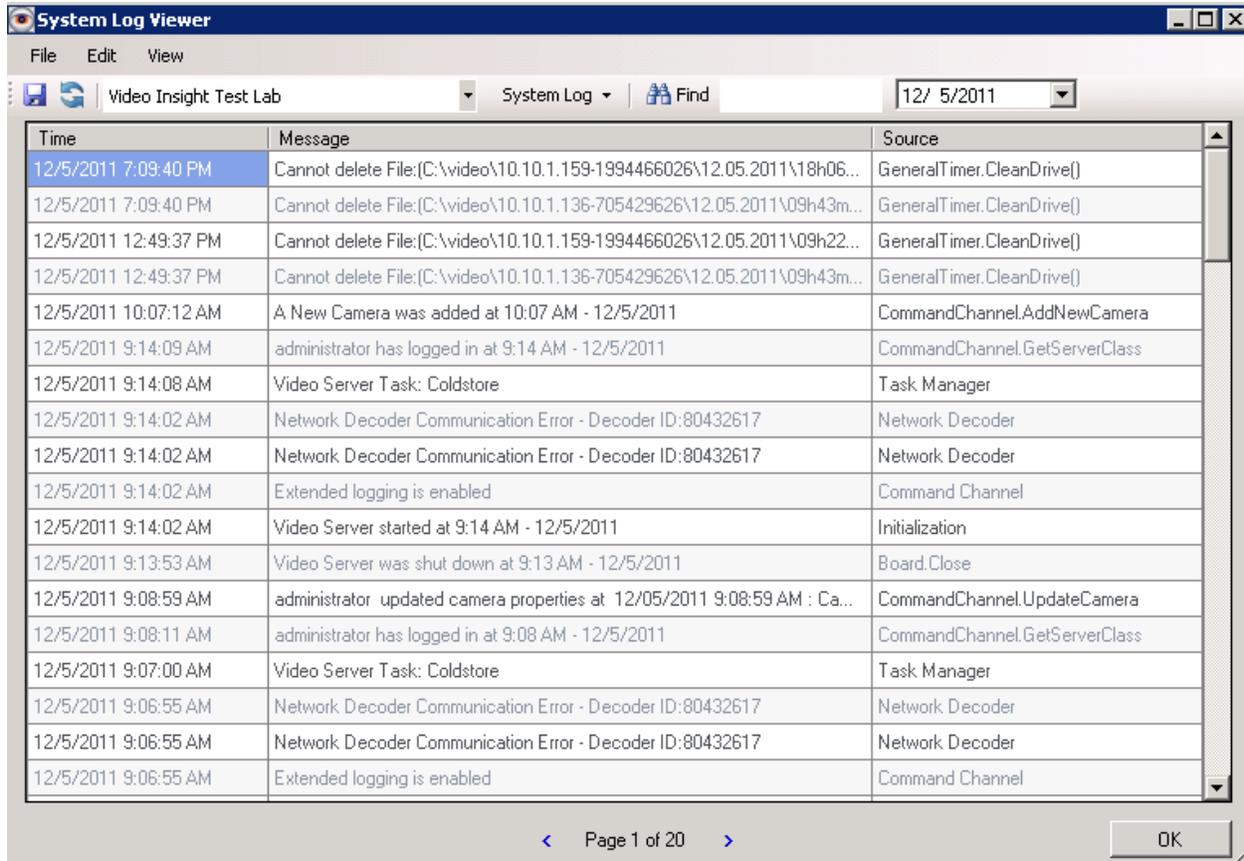
For example, in a scenario with the timeout enabled and set to 30 seconds, there is a Monitor Station layout comprised of both analog and IP camera images. For 30 seconds, both streaming and recording is managed by the IP Server. When 30 seconds have passed the analog cameras will stop streaming and recording due to this feature. Changing the layout will restart streaming and recording for all cameras until the timeout is reached again.

To set an analog video timeout:

1. Check the Enable Analog Video Bandwidth Timeout box.
2. Select the timeout in seconds.
3. Click **OK**.

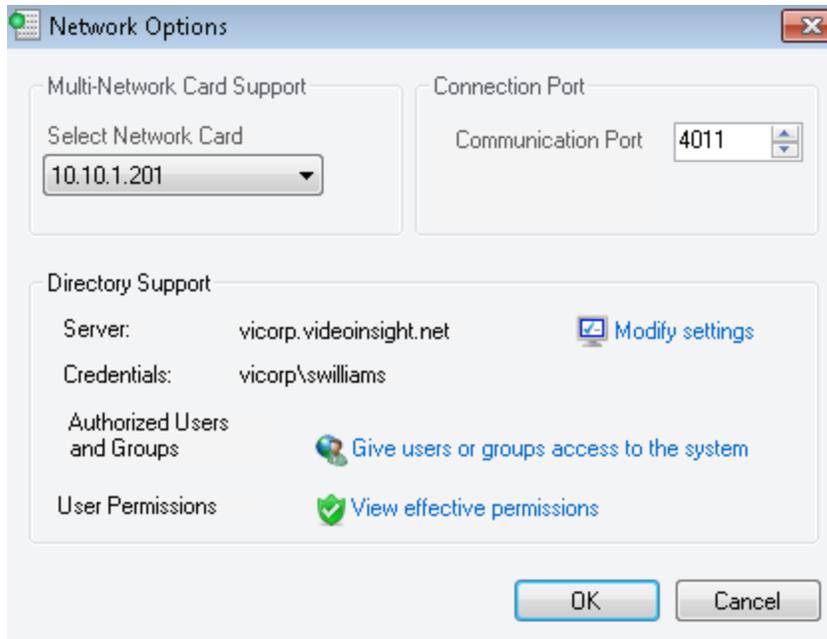
IPSM: System Log

Clicking **System Log** will bring up the System Log dialog box. The System Log documents warnings, errors, security and informational messages related to various system functions. Each message may or may not appear depending on the configuration and whether security is enabled on the server.



IPSM: Network Options

Clicking **Network Options** brings up the Network Options dialog box. This dialog box is used for selecting the network scheme when a server has dual NIC cards or changing the communication port of the server. You can also modify Active Directory and LDAP settings.



Note

If you change the Communication Port here, you must also change the command port in Server Properties.

IPSM: Diagnostics

Clicking **Diagnostics** brings up the Video Server Diagnostics interface. This interface is used for troubleshooting any service related issues. The IP Server service is stopped when Diagnostics is launched; however, recording and live streaming continue normally. The difference is that Video Server Diagnostics has a user interface and the IP Server service is a background process without a user interface.

Video Server Diagnostics

Video Server is running as an application to help trouble shoot problems with the service. This application uses the same settings as the service.

Video Insight Test Lab

- Setup and configuration
- Live view
- System Log

Vital statistics display

Server name: Video Insight Test Lab IP address: 10.10.1.175 Port: 4011

Version: 4.3.0.58 Max cameras: 99 Available: 86

Camera Name	Time of last write	Last image received
10.10.1.76 - IP Camera/Encoder:	12:00:00 AM	12:00:00 AM
10.10.1.127 - ONVIF: - - Firmware:	12:00:00 AM	12:00:00 AM
10.10.1.136 - IQEye - Model: IQ042S	12:00:00 AM	3:45:36 PM
10.10.1.148 - Axis - Model:	12:00:00 AM	12:00:00 AM
10.10.1.151 - ONVIF: - - Firmware:	12:00:00 AM	12:00:00 AM
10.10.1.153 - Acti - Model:	12:00:00 AM	12:00:00 AM
10.10.1.159 - Axis - Model:	12:00:00 AM	3:45:36 PM
10.10.1.166 - IQEye - Model:	12:00:00 AM	12:00:00 AM
10.10.1.173 - ONVIF: - - Firmware:	12:00:00 AM	12:00:00 AM

Exit

Server name: This field displays the server name previously entered. It is not editable. To change the name of the server, click **Setup** and configuration in the left pane or from Server Properties.

IP Address: This field displays the server's IP address and should not be changed.

Port: This field displays the port used by the Monitor Station to get and set system information. This port is also referred to as the Command Channel Port. See [list of ports](#) for more information on ports used by the software.

Version: This field displays the software version.

Max cameras: This field displays the maximum number of cameras allocated to the serial number assigned to the server. Using a Video Insight encoder such as the VP16 will show a value of zero in this field, but all 16 channels of the encoder can be added.

Available: This field displays the number of licenses available to add to the server.

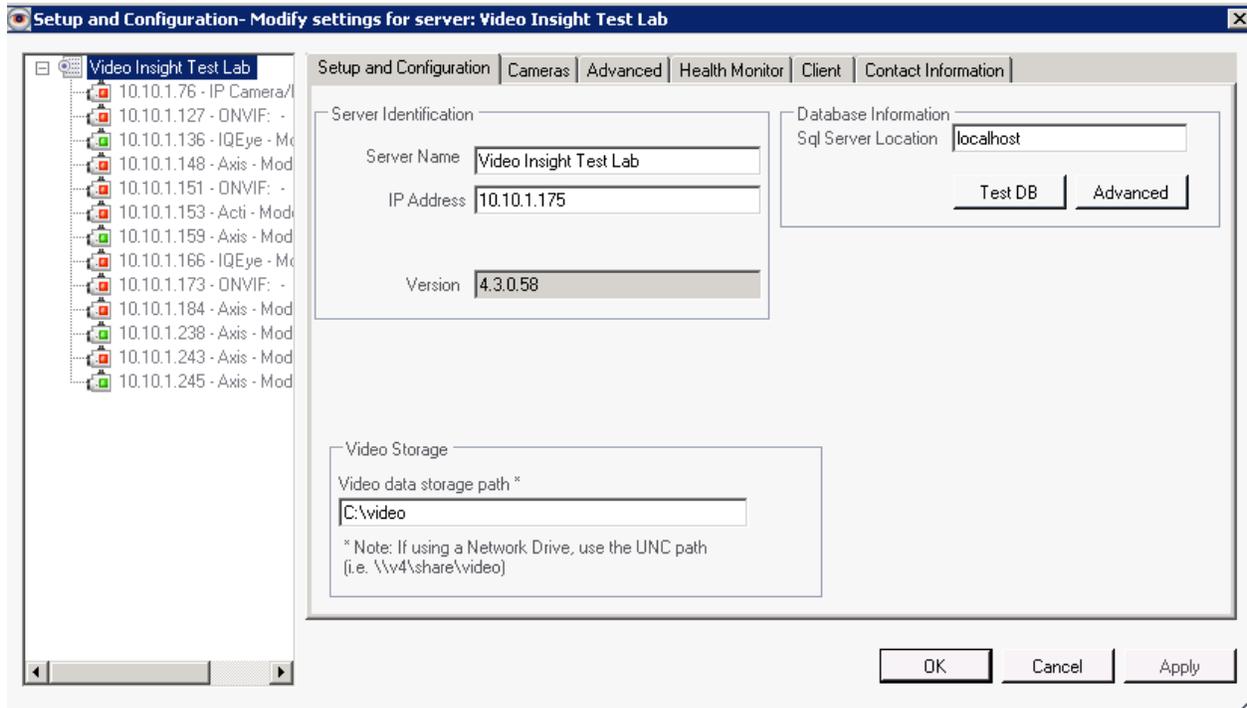
The grid area of the Diagnostics interface is read-only and displays all cameras, the last video write time, if it is recording and the time the last image was received, or the last time a live image was received from the camera.

Time of last write: This column displays the last time the camera's images were recorded to a file. A time of 12:00:00 AM is indicative of a camera that is set to Recording Off or not recording due to a Motion-Only recording type.

Last image received: This column displays the last time the camera's live images were streamed. A time of 12:00:00 AM is indicative of a camera that is offline. The camera could be offline for several reasons:

incorrect credentials, network, bandwidth or the IP Server service not running. See the [FAQ](#) section for more information on why a camera could be offline.

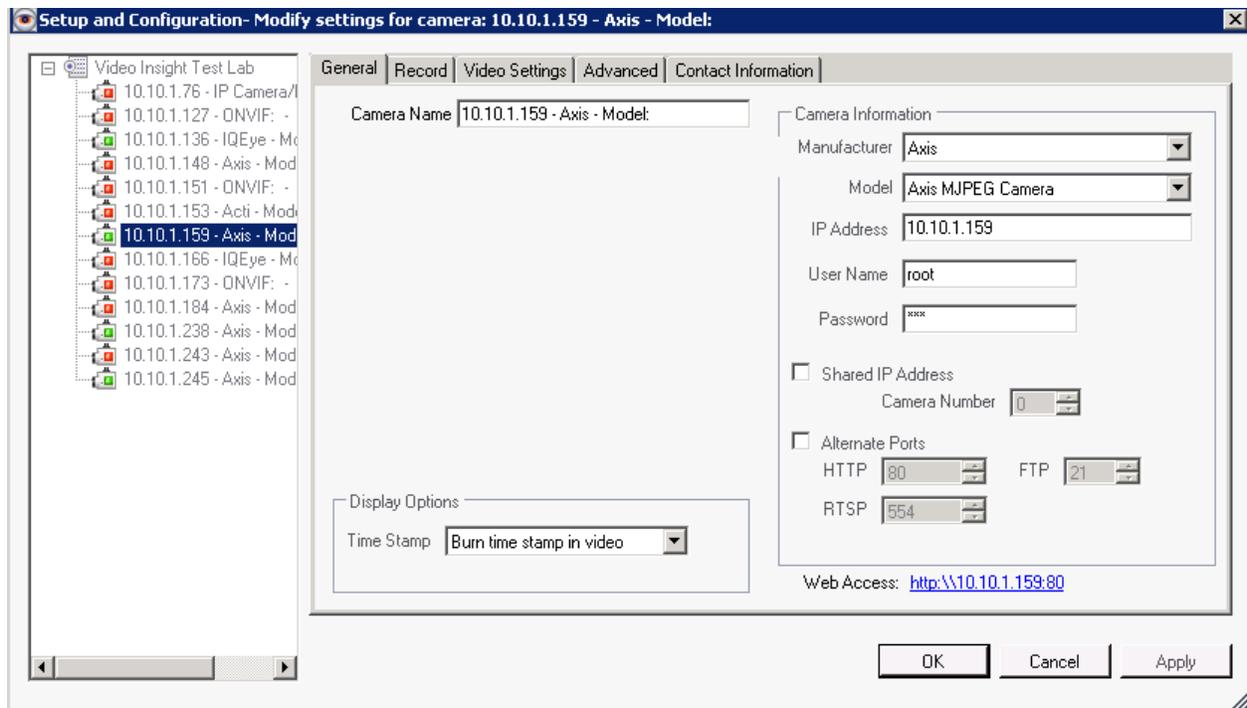
To view the Setup and Configuration section of Video Server Diagnostics click that node from the left pane.



With the exception of the [Access Configuration](#) tab available in IP Server properties the tabs in this view are the same as [Server Properties](#) accessed from the Monitor Station. The cameras listed in the left pane can be managed in this view. Click the camera on the left and the camera's properties will be displayed.

Note

Remember to start the service when exiting the Diagnostics application.



See [Modifying Camera Details](#) for more information on camera property tabs.

Two additional features for troubleshooting are available that are not available in Monitor Station, by highlighting the server node in the left pane: **Test DB** and **Advanced**.

Click **Test DB** to test connectivity to the database. The database test will pass when the server makes a successful connection to the database. If it does not, the test will display: “Error: Database version is not correct. Either the database did not respond, nor has an outdated version.” There are several reasons why the database test failed. See [FAQs](#) for possible reasons for and potential solutions to the failure.

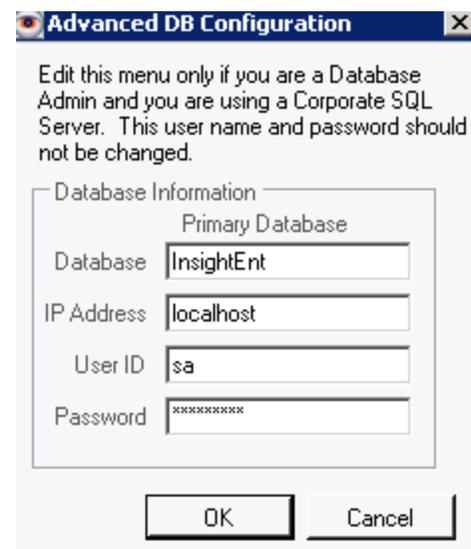
Incorrect database information may be one cause of test failure. To update or confirm the information click **Advanced**.

Database: Enter the database name. The default database name is InsightEnt.

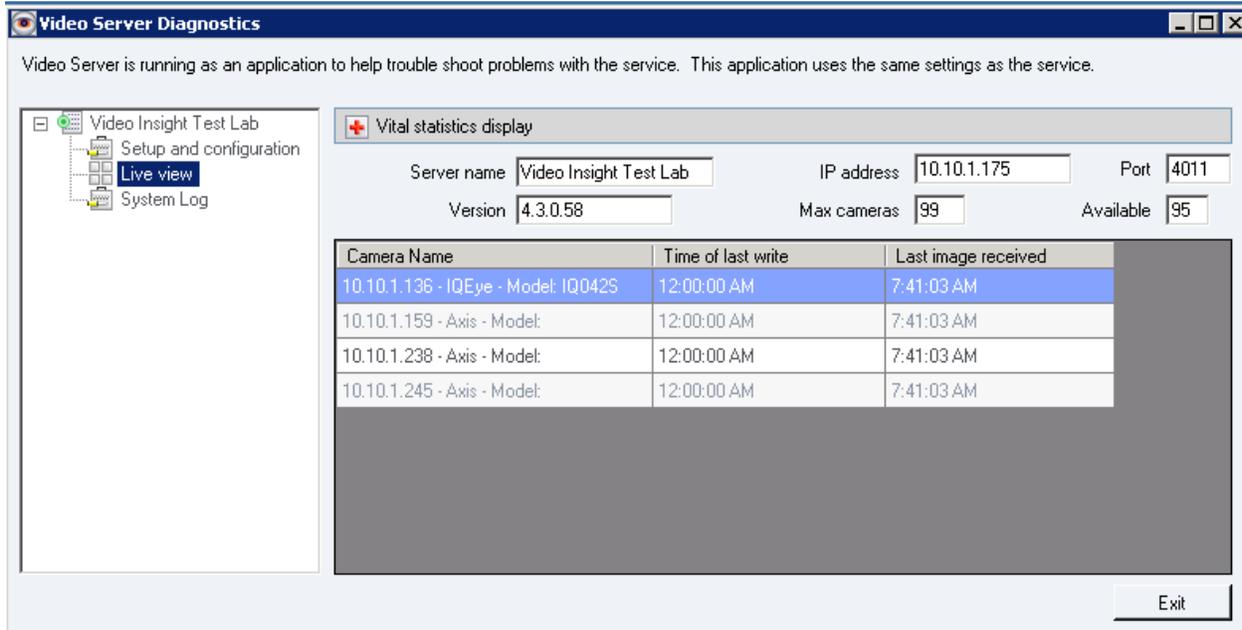
IP Address: Enter either the IP address or the hostname of the database server.

User ID: The default user ID for the InsightEnt database is sa.

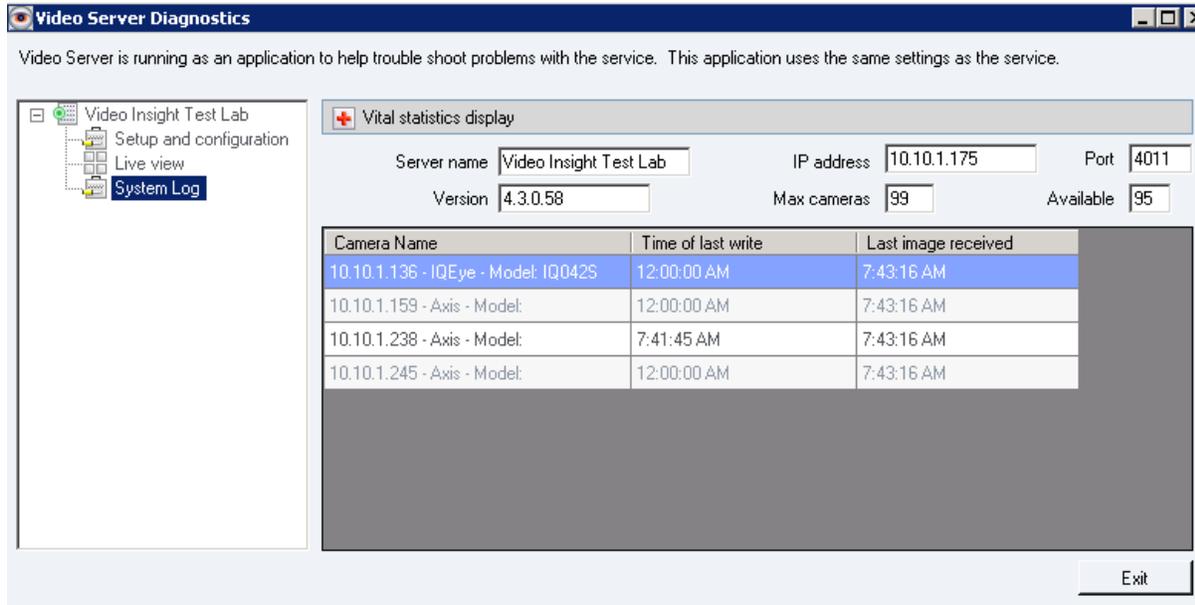
Password: The default password for the InsightEnt database is vinsight.



Video Server Diagnostics offers a live view feature. Clicking **Live View** in the left pane display a separate window with all of the cameras added to the server.



You can view the System Log by clicking the node in the left pane. See [System Log](#) for more information on the system log.



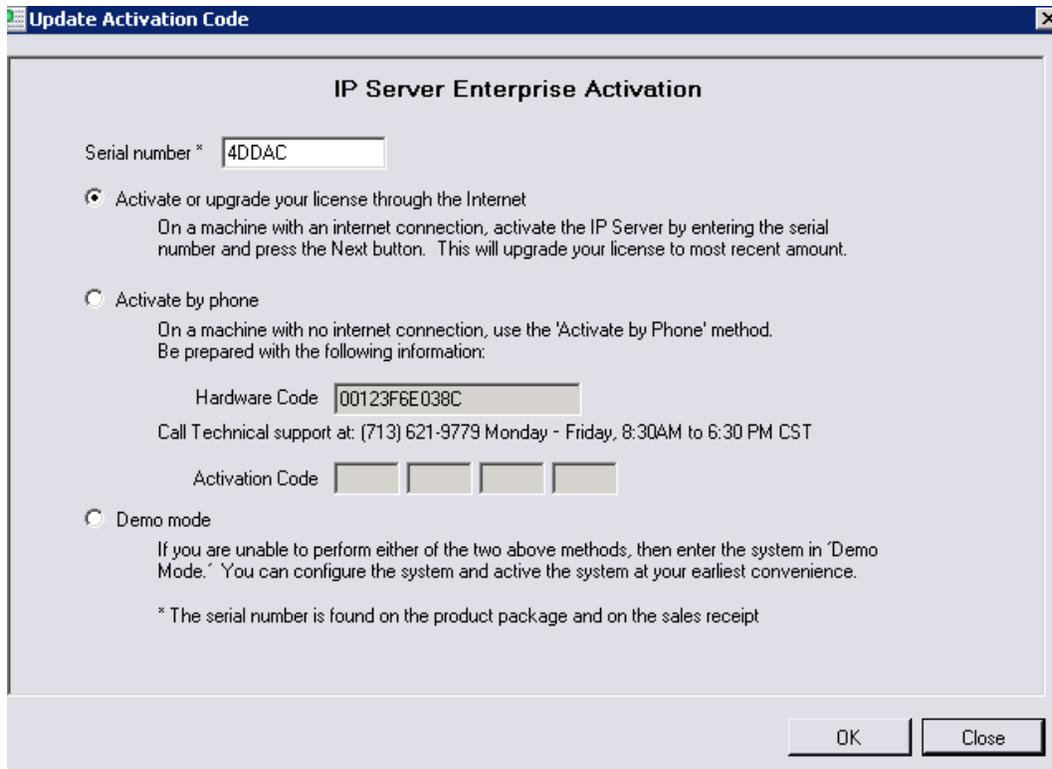
IPSM: No Cameras

Another troubleshooting option is a diagnostics version that can run the application without starting any cameras. This version does not consume any bandwidth.

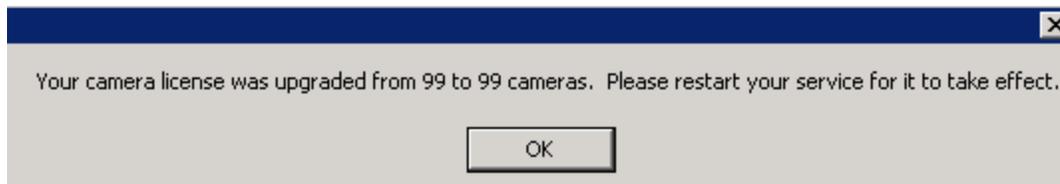
This version functions the same as the other version, with the exception that camera-related features and information such as Live View and Time of last write are not available after this diagnostics version is started. See [IPSM Diagnostics](#) for more information on running diagnostics.

IPSM: Update Activation

The Update Activation option is used to update the Activation type (e.g., transitioning from Demo to purchased licensing scheme) or when the serial number used is upgraded with additional licenses.



See [Installation](#) for more information on changing the activation type. Click **OK** to confirm the number of licenses currently available.

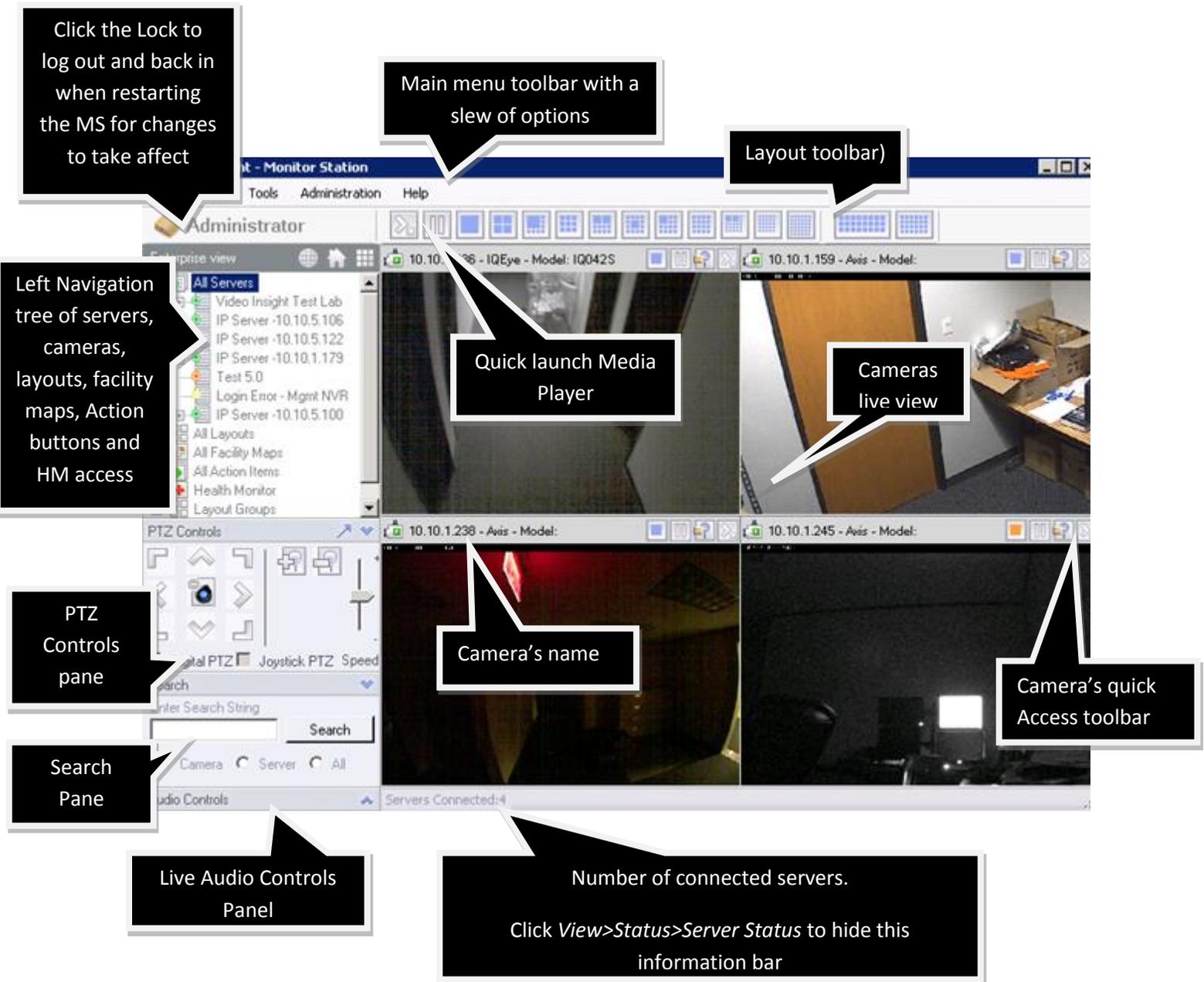


Monitor Station

Monitor Station is the primary user interface in the product suite and can be considered the hub from which all configurations and monitoring is done. Configuration changes to the Monitor Station will only affect the local host and not the server or other clients, unless Administrator-level access changes are made in Setup and Configuration.

Main Dashboard

The main dashboard has many features to make daily monitoring easy and manageable. It is the first view to appear after starting Monitor Station.



Main menu toolbar

The Monitor Station's main toolbar has several menus: Tools, Administration and Help.

File

The File menu has two selections: Media Fixer and Exit. Media Fixer is used to fix corrupted video files and Exit terminates the program.

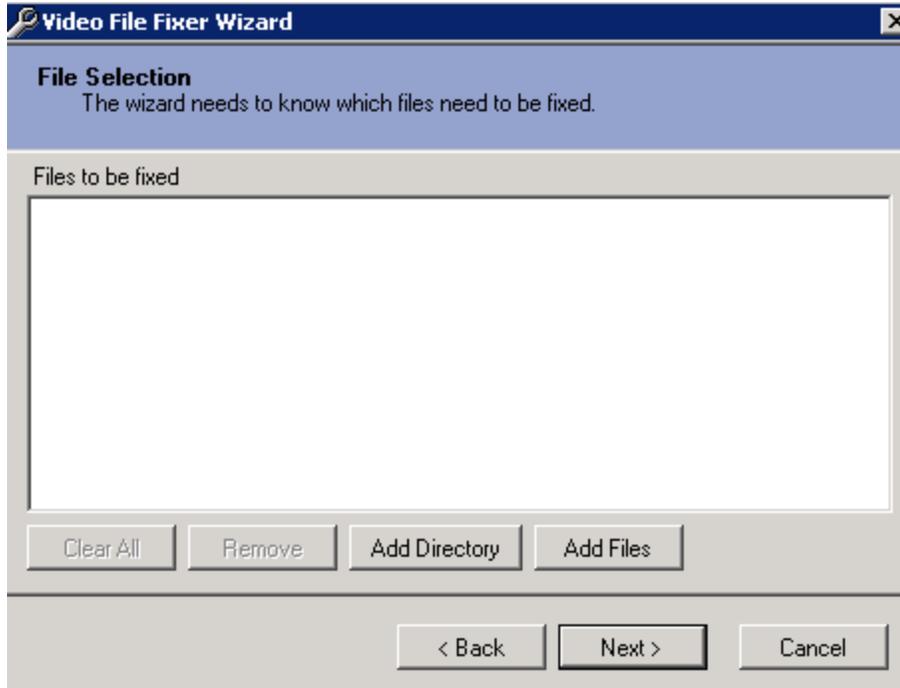
File>Media Fixer

Media Fixer helps you fix corrupted media files.

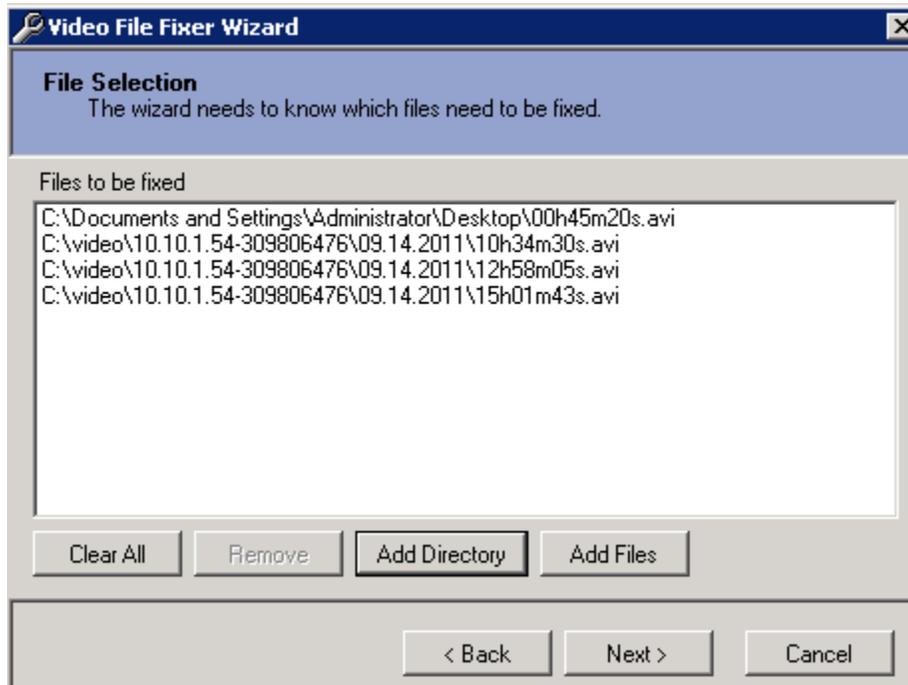
1. Click the File menu and select Media Fixer.



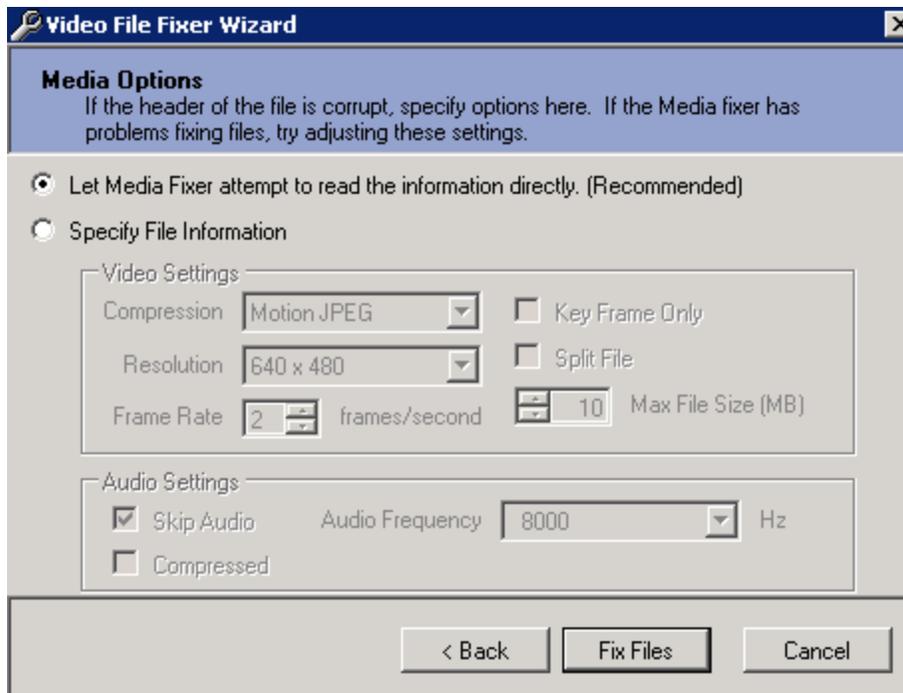
2. Click **Next**.



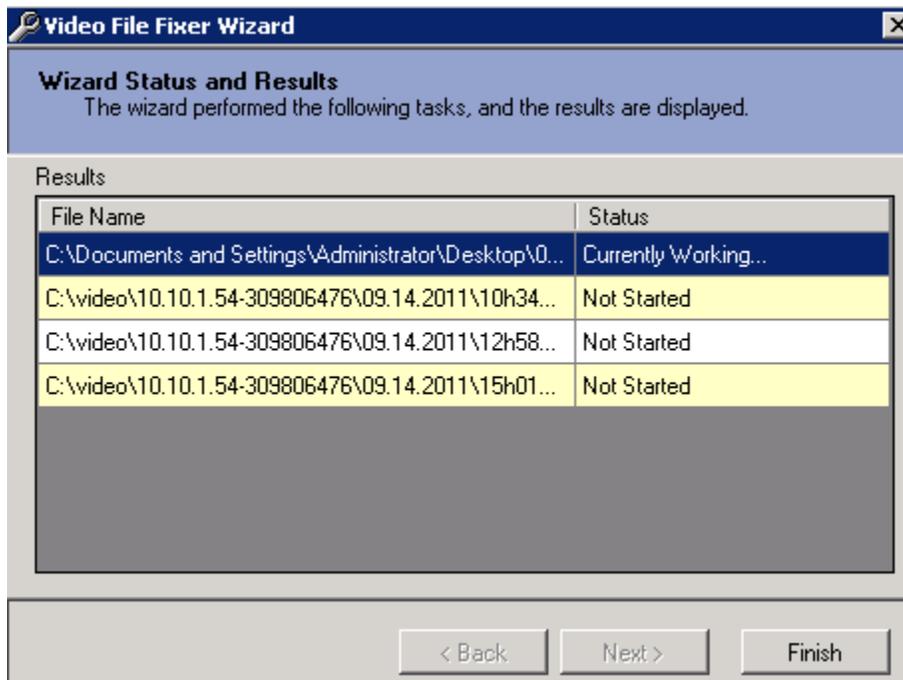
3. You can add a single video file, multiple video files or folders of video files to be fixed. The path to each file will be displayed after it is added.



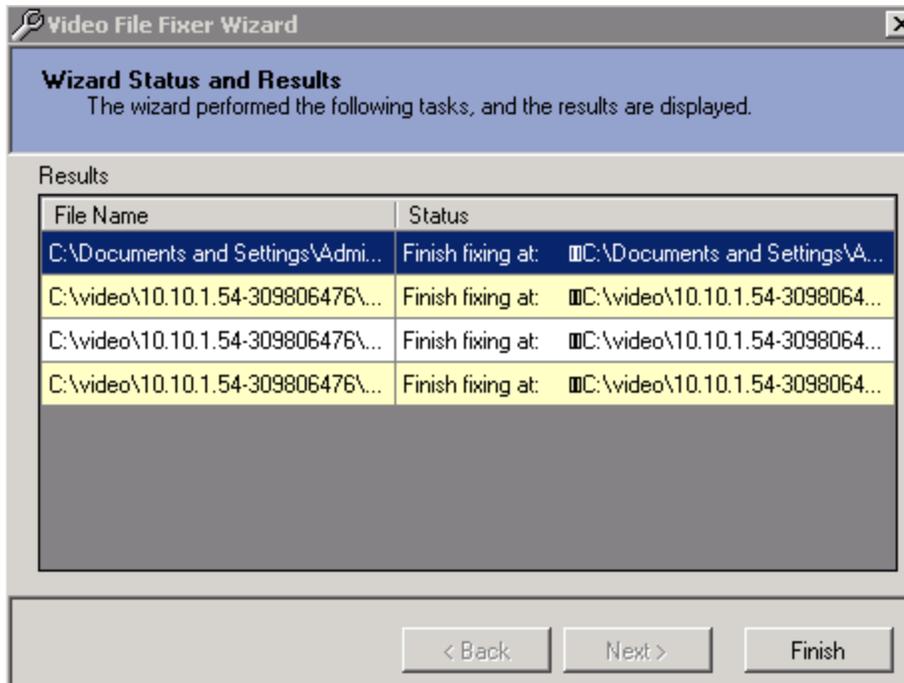
4. Click **Next**.



5. For best results let Media Fixer attempt to read the file information. If you choose to specify the file information it is crucial to provide the correct file header information. Attempting to fix it with incorrect information may render the file unusable. Click **Fix Files**.



6. The Status dialog box displays progress. When the wizard is complete it will display the path of the fixed file.



7. The fixed file will have “fixed” appended to the file name. The original file still exists and has not been altered.

Name	Size	Type	Date Modified
00h45m20s_fixed	67,043 KB	Video Clip	1/2/2012 12:02 PM

8. Click **Finish**.

File>Exit

Click the File menu and select Exit. Monitor Station will display a prompt to confirm exiting the application. This behavior is exactly as if you were to press the Lock Icon.



You can also exit the application without having to make the confirmation by unchecking the Exit confirmation checkbox on the Tools>Options>General tab.

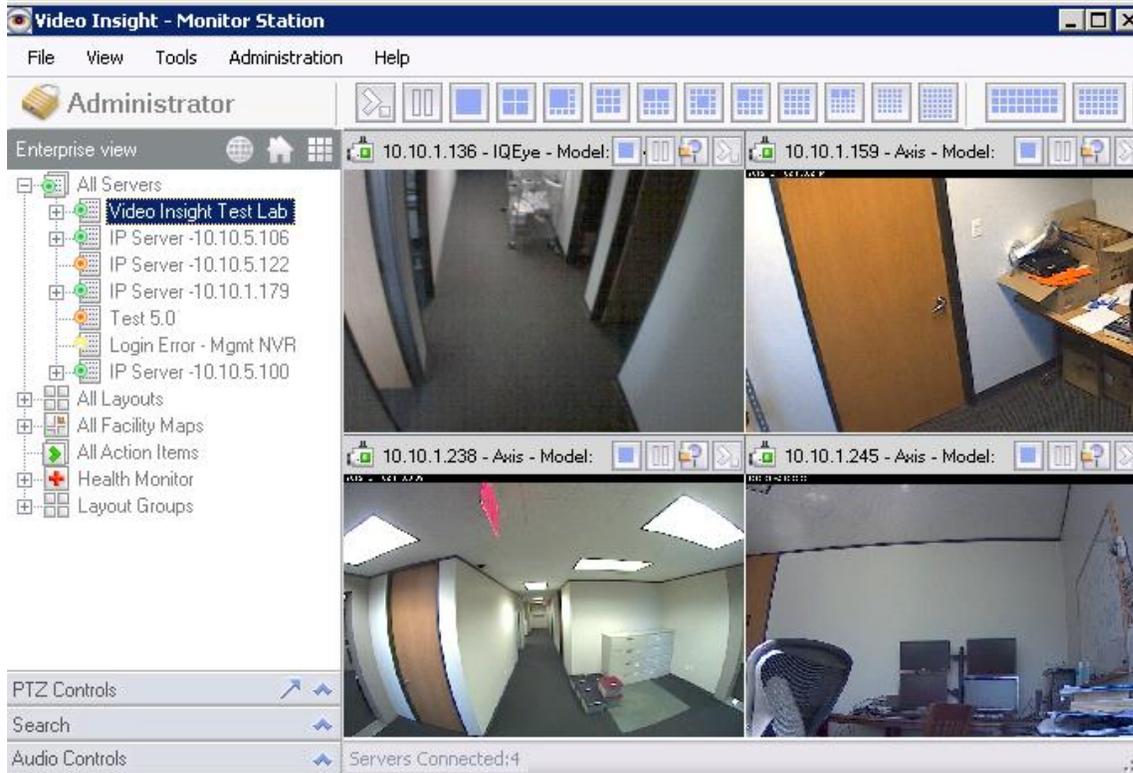
View

The View menu has six selections: Archive Tree, Full Screen, Layout, Mini Toolbars, Status and Toolbars.

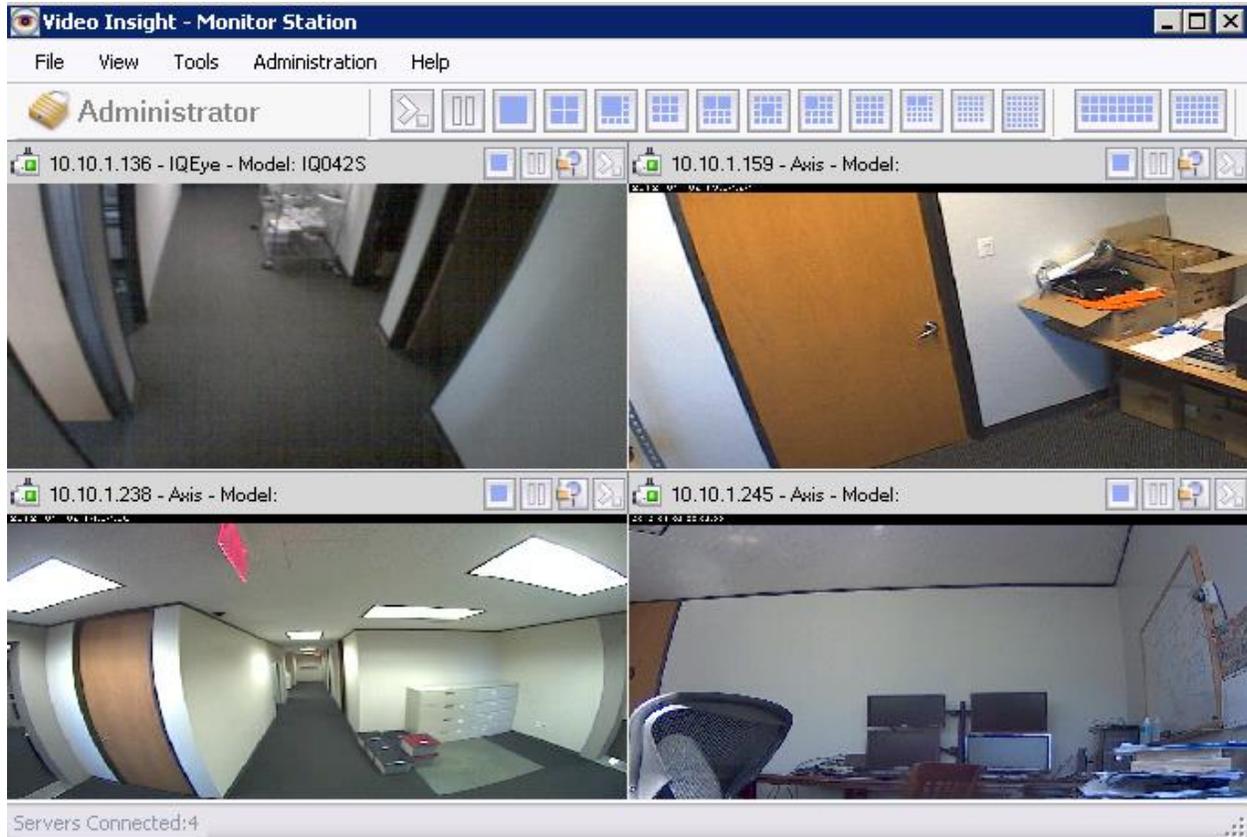
View>Archive Tree

The Archive Tree option is checked by default. If unchecked the left navigation tree will be hidden. This is useful if you want to have more space within the application for live view streaming.

The default view with Archive Tree selected is shown in the figure below:



The view with Archive Tree deselected is shown in the figure below.



View>Full Screen

Selecting Full Screen expands the main dashboard view to fill your display. Pressing the F11 key on your keyboard performs the same function.

View>Layout

Selecting Layout shows the full list of the predefined camera layouts. Selecting one of the layouts displays the selected number of cameras in the main dashboard view. Pressing the related Function key on your keyboard performs the same function.

1 Camera Layout	F1
4 Camera Layout	F2
8 Camera Layout	F3
9 Camera Layout	F4
10 Camera Layout	F5
13 Camera Layout	F6
13 Camera Layout - 2	F7
16 Camera Layout	F8
19 Camera Layout	F9
25 Camera Layout	F9
36 Camera Layout	F10

Use the shortcut keys on your keyboard to change the

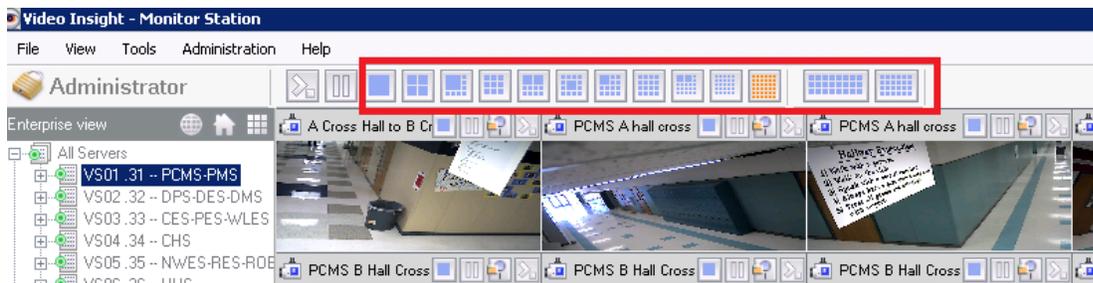
View>Mini Toolbars

Selecting Mini Toolbars creates Cycle Layouts and PTZ Controls function boxes that can be repositioned anywhere on your dashboard for easy access.

Cycle Layouts

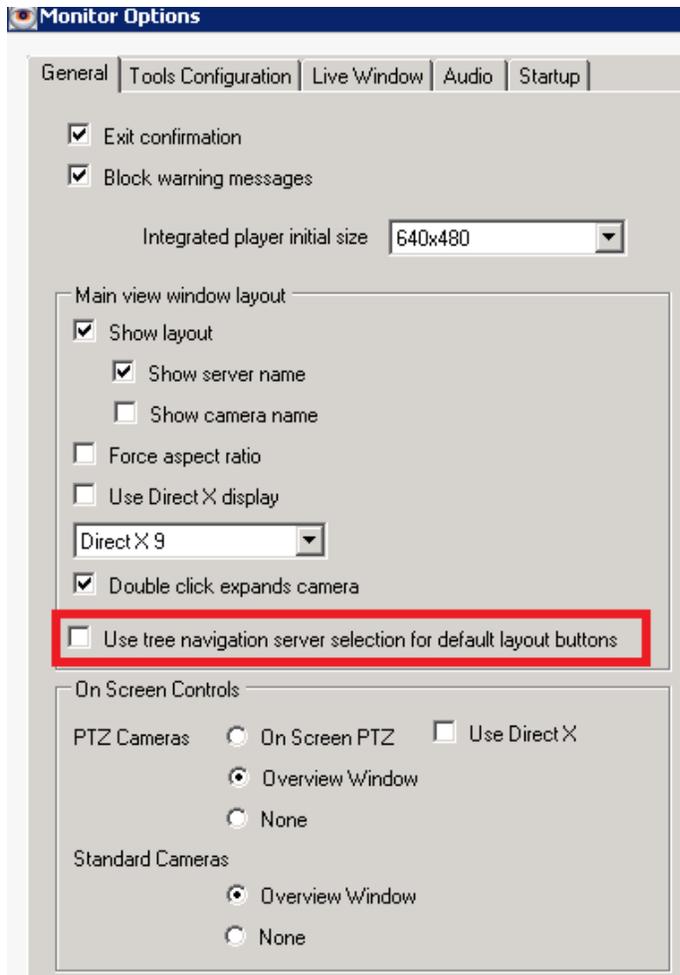
Security personnel may be assigned to a particular area and may only need to review certain locations. In practice, locations are usually grouped by server. For example, one Monitor Station may be connected to multiple sites, with one Server per site. As each site may have a different number of cameras you may have a different layout for each site. You can perform a virtual walkthrough of each site by cycling each site's layout.

You can cycle layouts two ways: manually or automatically. You can manually cycle layouts by pressing any of the predefined Layout buttons as shown in the figure below.



To configure the one server cycling for manual selection:

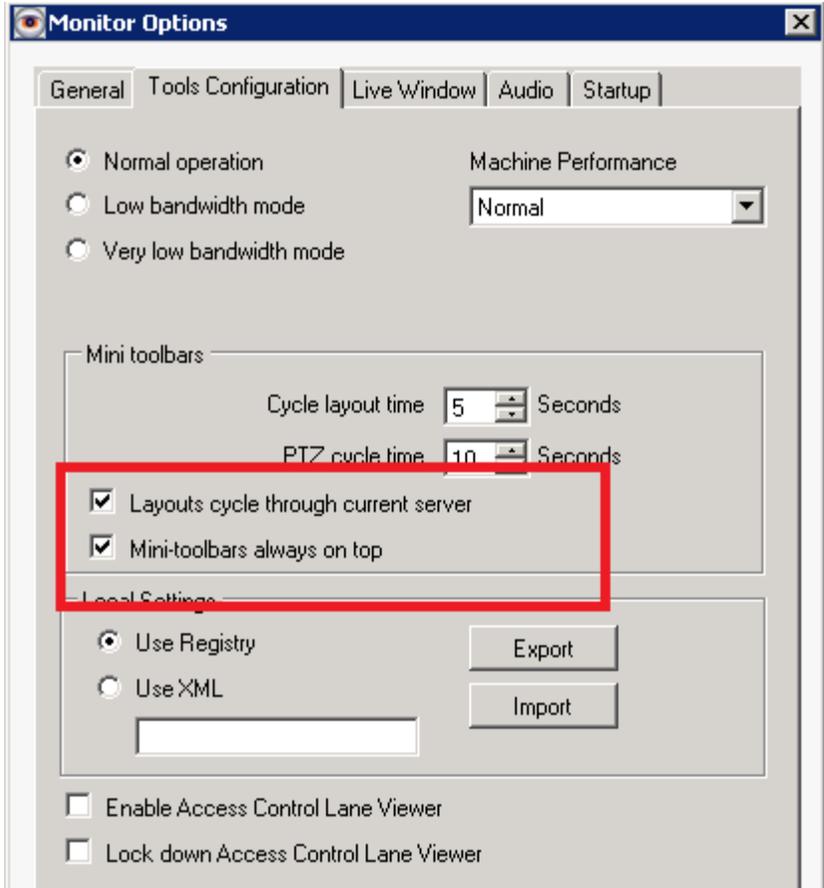
1. Click the Tools menu and then select Options.
2. On the General tab check the box for "Use tree navigation server selection for default layout buttons".



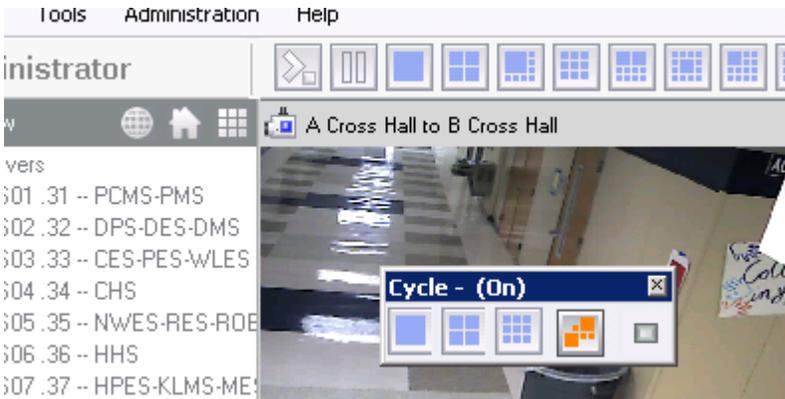
3. Log out and back in to the Monitor Station to refresh the settings.
4. Select the highlighted server from the left navigation tree.
5. Click any of the Layout buttons and notice that only the selected server's cameras will be selected for the layout view.

To configure the one server cycling for automatic selection:

1. Click the Tools menu and then select Options.
2. On the Tools Configuration tab check the box for "Layouts cycle through current server". This box is checked by default.



3. Log out and back into the Monitor Station to refresh the settings.
4. Click the View menu, select Mini Toolbars and then select Cycle Layouts.
5. Click the desired Layout scheme and click the Play icon.



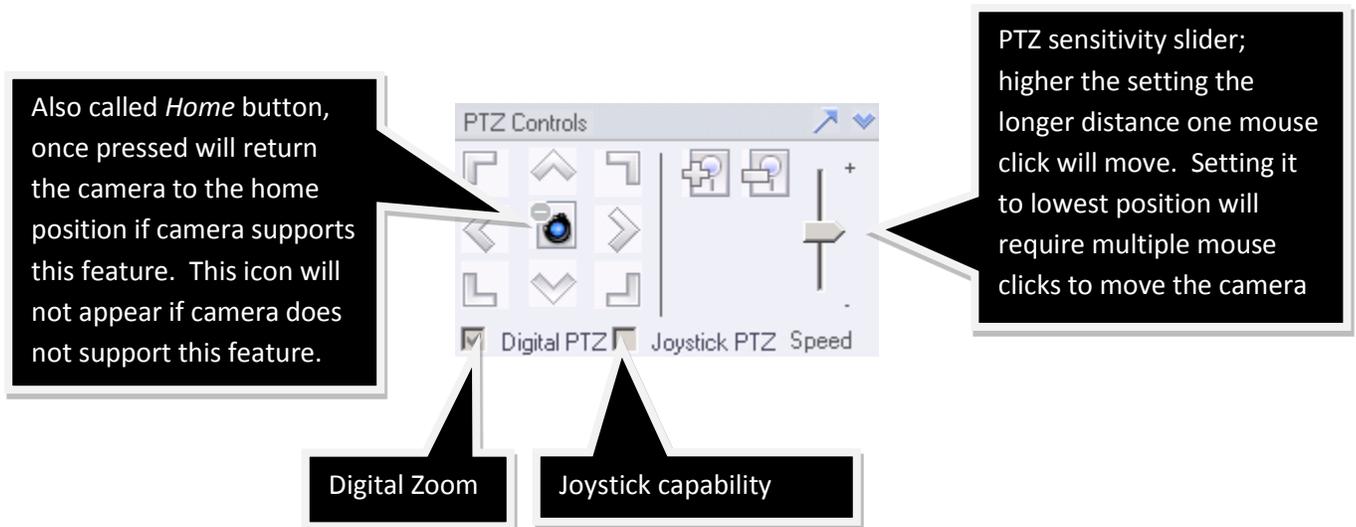
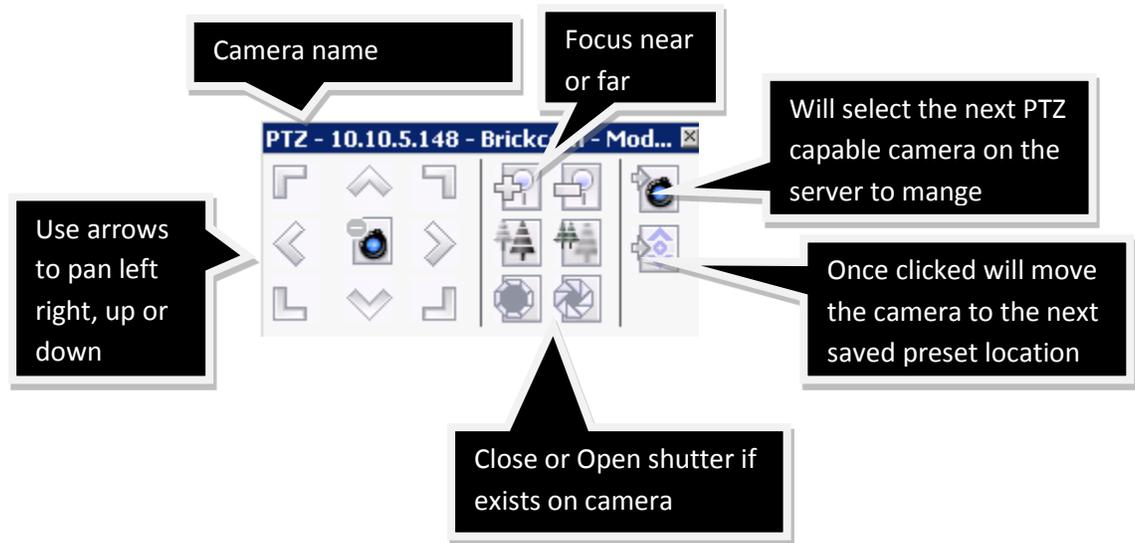
PTZ controls

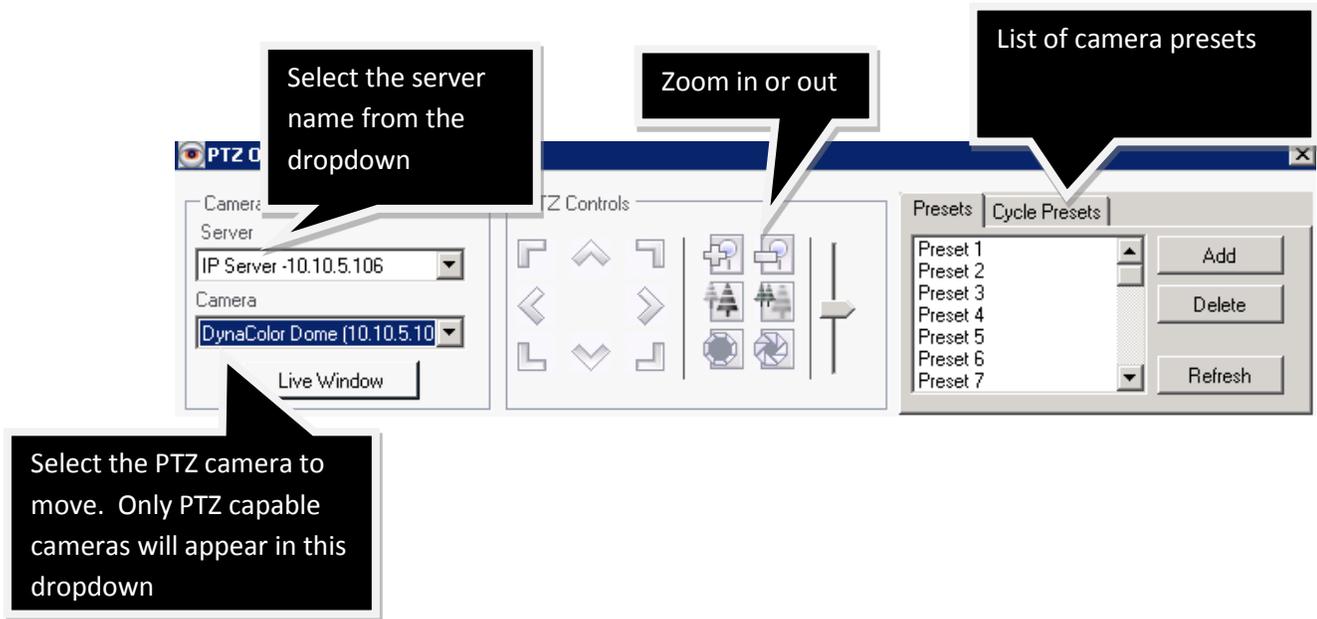
You can control PTZ operations for PTZ-capable cameras from different areas in the application. Each area offers a slight variation in capability.

Note

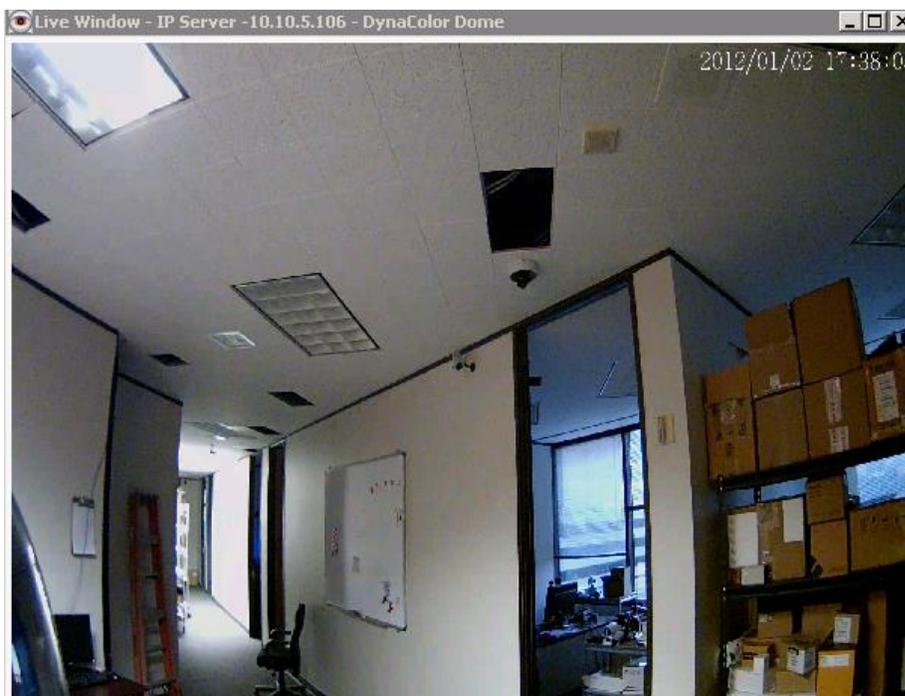
PTZ Operations can also be launched by clicking the Tools menu and selecting PTZ Operations. To start the PTZ Controls function box, click the View menu, then Mini Toolbars and then PTZ Controls. The figure below describes the different functions available.

The following figures describes the left navigation tree PTZ Controls pane





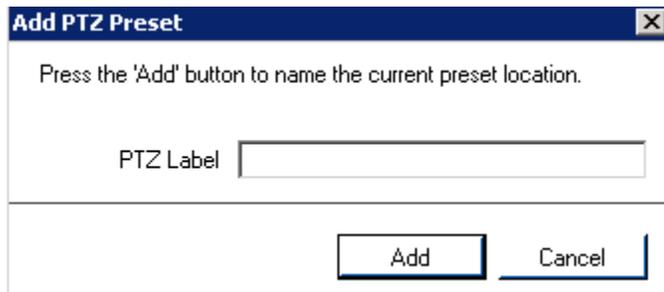
Clicking **Live Window** launches a live view of the selected camera. This window can be used to manipulate the live view using the PTZ controls.



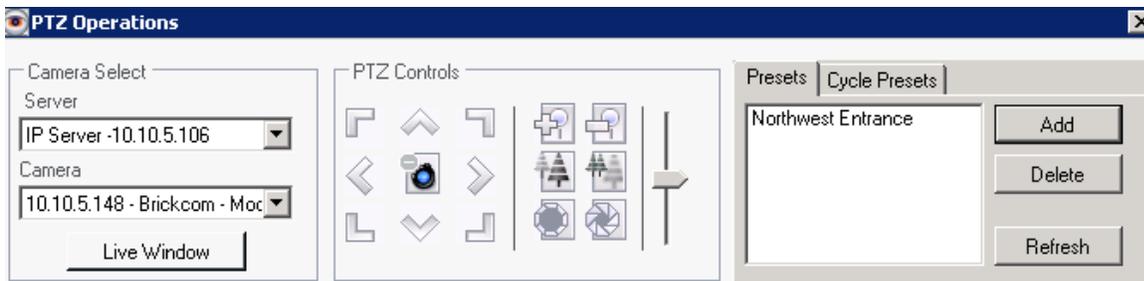
You can use the PTZ Operations pop-up with its expanded features to create and manage PTZ presets. PTZ presets are predefined views that can be used for cycling or manually going to a camera with a click of a button during live view from the main dashboard.

Creating a preset

1. Launch the PTZ Operations pop-up.
2. Select the server and camera from the drop-down menu.
3. Click **Live View** to view the camera as it is being moved.
4. In Live Window move the camera to the desired preset location.
5. Click **Add**.

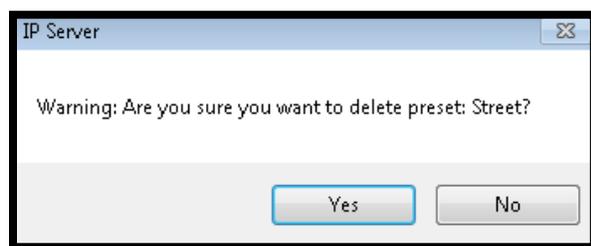


6. Enter a label for the preset.
7. Click **Add**.
8. The newly-added Preset appears in the Presets pane.



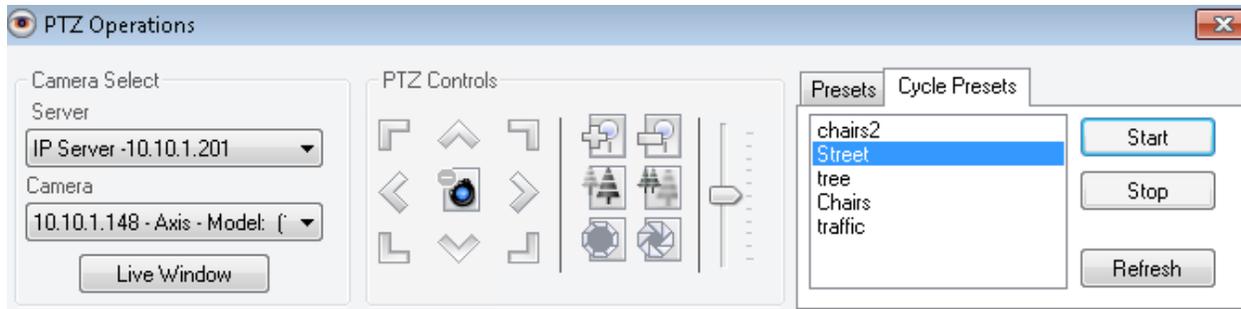
9. Continue moving the camera to the second position and repeat steps 4-7 to add as many presets as required. A maximum of 32 presets are supported depending on the camera.

To remove a Preset, select it from the Presets pane and click **Delete**.

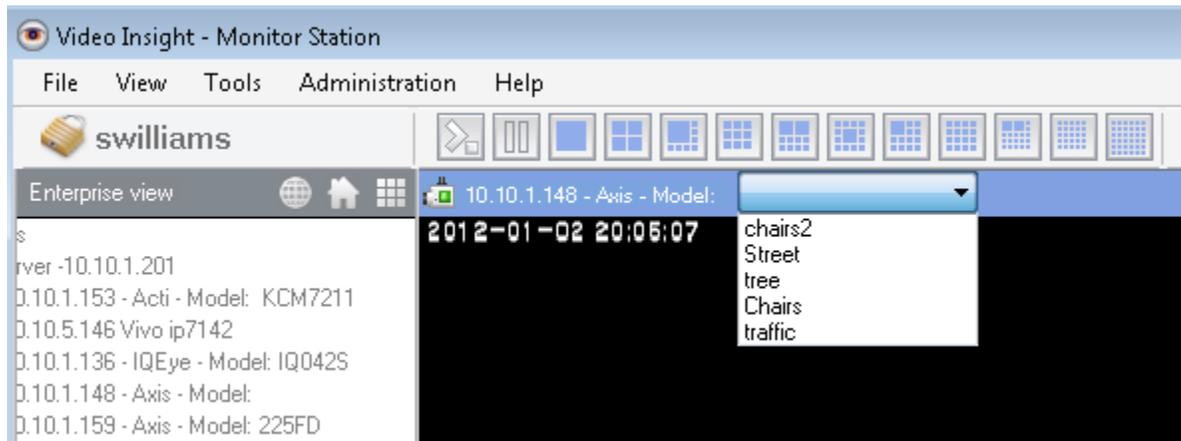


Click **Yes** to permanently remove it or **No** to cancel the operation and return to the PTZ Operations screen.

You can also cycle automatically through presets by navigating to the Cycle Presets tab and clicking **Start**.



Added Presets can also be selected from the Live view camera toolbar in the Main Dashboard as shown in the figure below.



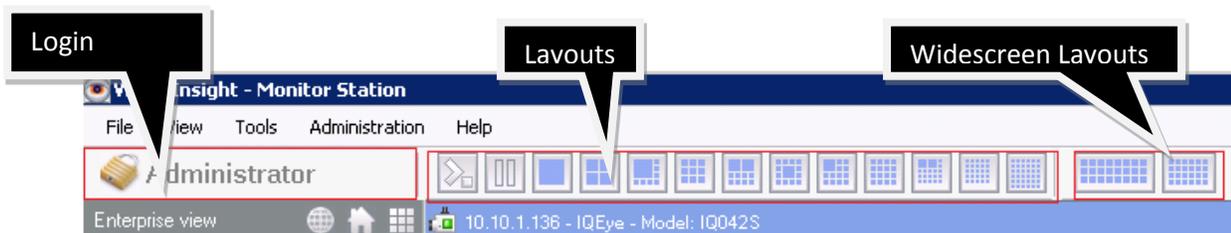
View> Toolbars

You can hide additional options displayed by default in the main dashboard by clicking the View menu and selecting Toolbars. Hiding them will add space to the live view.

1. Click the View menu and select Toolbars.



2. Three sub options are checked by default. Unchecking all three will hide the following Main Dashboard items:



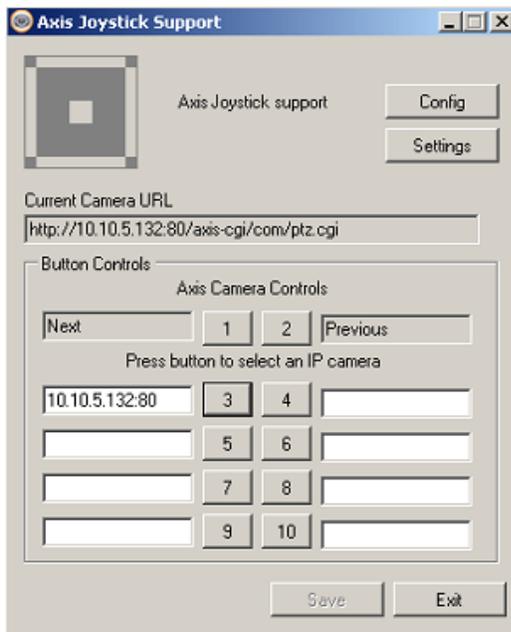
Tools>System Log

You can access the System Log from several different areas of Monitor Station and Diagnostics.

Tools>Axis Joystick Control

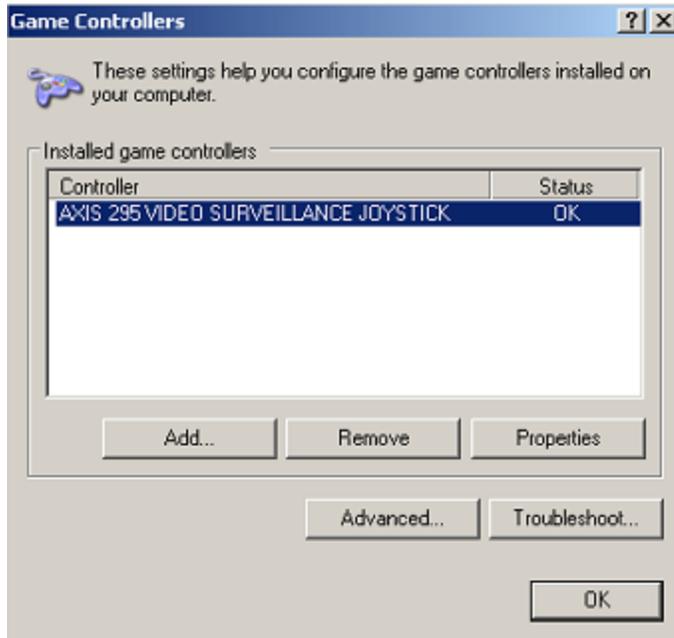
The Axis Joystick Control supports the Axis Joystick. This USB joystick replaces a mouse for control of Axis PTZ-capable cameras.

After the joystick is connected, click the Tools menu and select Axis Joystick Control.

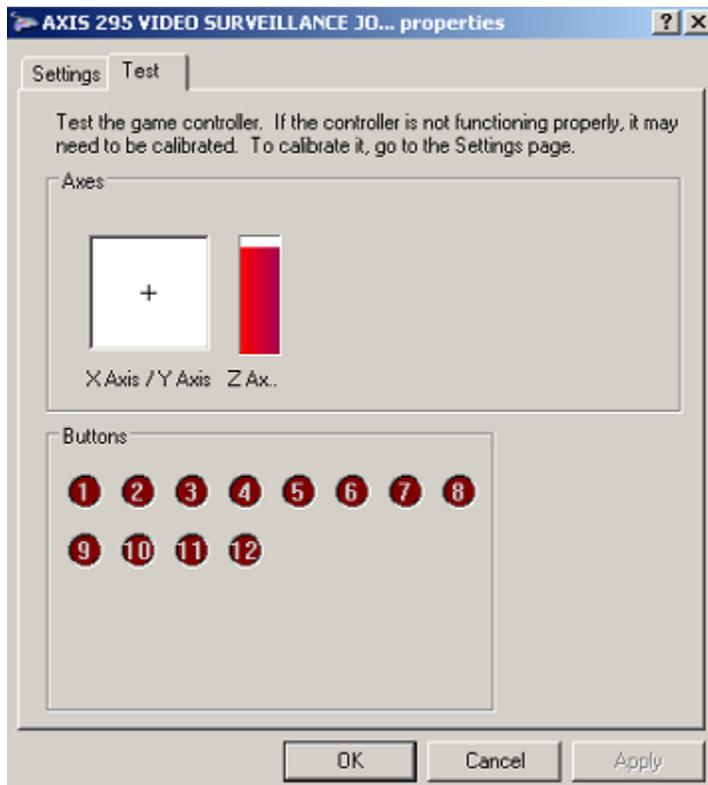


Up to 10 Axis PTZ-capable cameras added to a server in a Monitor Station will automatically populate the Axis Joystick Control, including the IP address and port.

You can manage any game controller's settings and firmware by clicking **Config**.

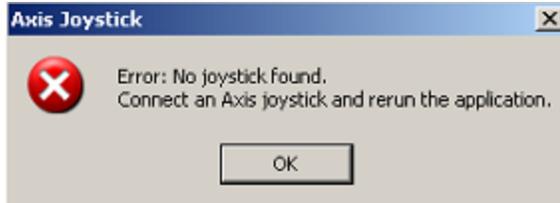


Select the controller you'd like to manage and click **Properties**.

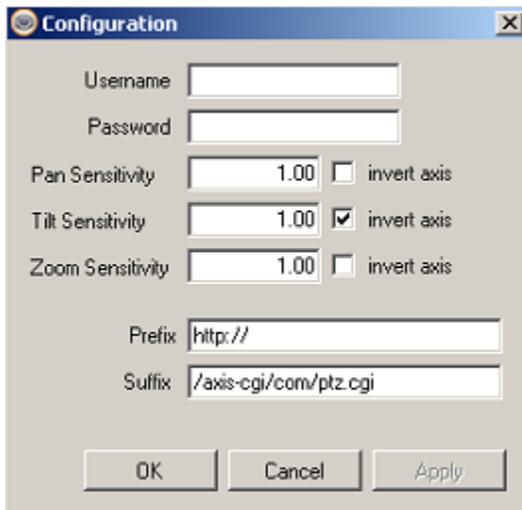


You can test and calibrate the controller's settings. Click **Apply** and then **OK**.

If you click the Tools menu and select Axis Joystick Control without having an Axis Joystick attached, an error displays.



You can customize the joystick's pan, tilt and zoom sensitivity by clicking the Settings tab.



Enter the user name and password if credentials are required to change the joystick configuration.

Note

The Layouts drop-down list will not appear if no Layouts exist.

Tools>Live Window

You can use Live Window as a free-floating single or multi camera view. It is another feature that is accessible from several different areas of the application. It also has slightly different options depending on where it is accessed.

Figure shows Live Window when launched from the main toolbar.





You can select the server name or IP address from the Server drop-down menu. The server's camera(s) becomes available for selection from the Camera drop-down menu. In addition, all Layouts for all servers in that Monitor Station become available in the Layouts drop-down menu.

The red line bordering the Live Window image signifies that motion was detected on this camera. To remove the motion indicator click the Tools menu, select Options, then select the Live Window tab and uncheck the box for Red Outline on Live Window.

Tools>Media Player

Media Player is a standalone video player created by Video Insight. It has many capabilities and is built in to Monitor Station. See [Media Player](#) for more information.

Tools>PTZ Operations

See PTZ Controls for more information on PTZ Operations.

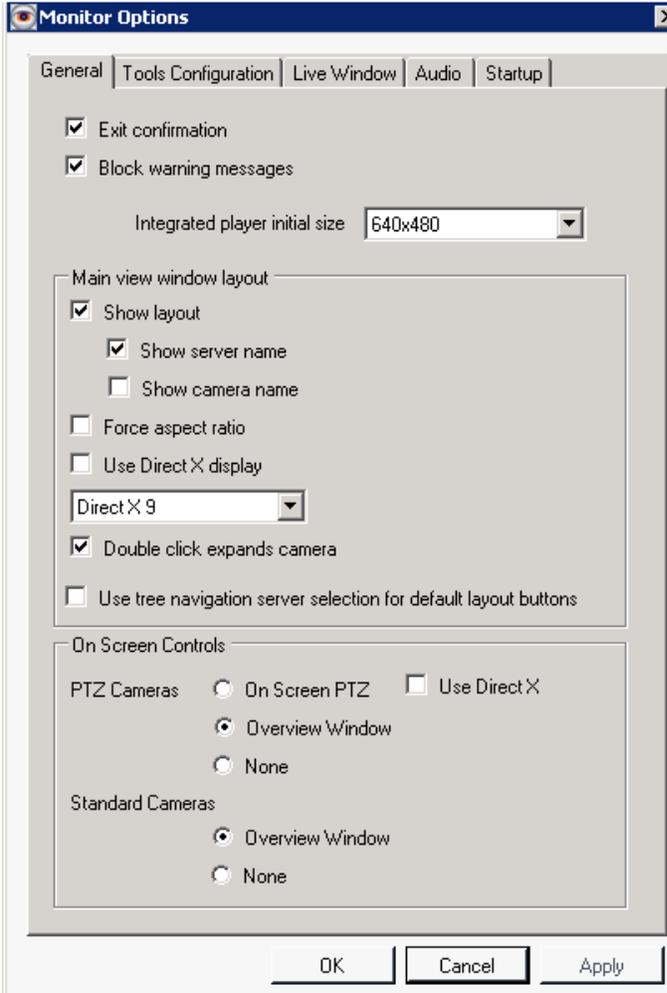
Tools>Synchronized Player

Synchronized Player allows for synchronized playing of multiple cameras. See the [Synchronized Player](#) section for more information.

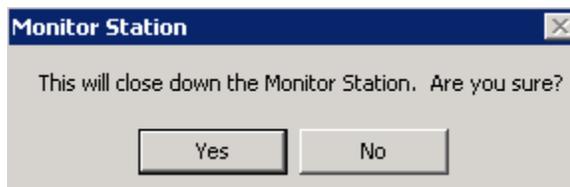
Tools>Options

You can use Options for additional configuration and personalization of your Monitor Station.

General tab



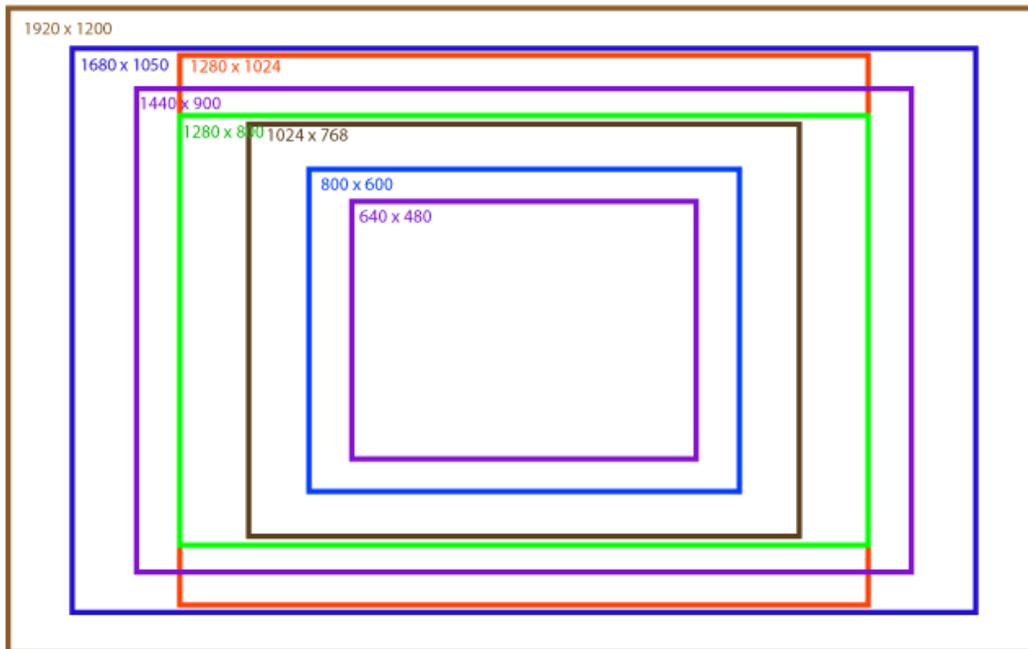
Exit confirmation: By default, closing Monitor Station displays a confirmation dialog box. To avoid this message uncheck this box.



Block warning messages: By default, Monitor Station warning messages informs you of cameras that lose connectivity, when the connection is restored and any disk write errors that occur. To avoid these warning messages check the box.

Integrated player initial size: The Integrated Player size is the size of the player when playing files from the Main Dashboard. Changes made here do not affect Media Player size. Available sizes are: 320x240,

400x300, 480x360, 560x420, 640x480, 720x540, 800x600, 960x720, 1080x810, 1280x960, 1440x1080 and 1600x1200.

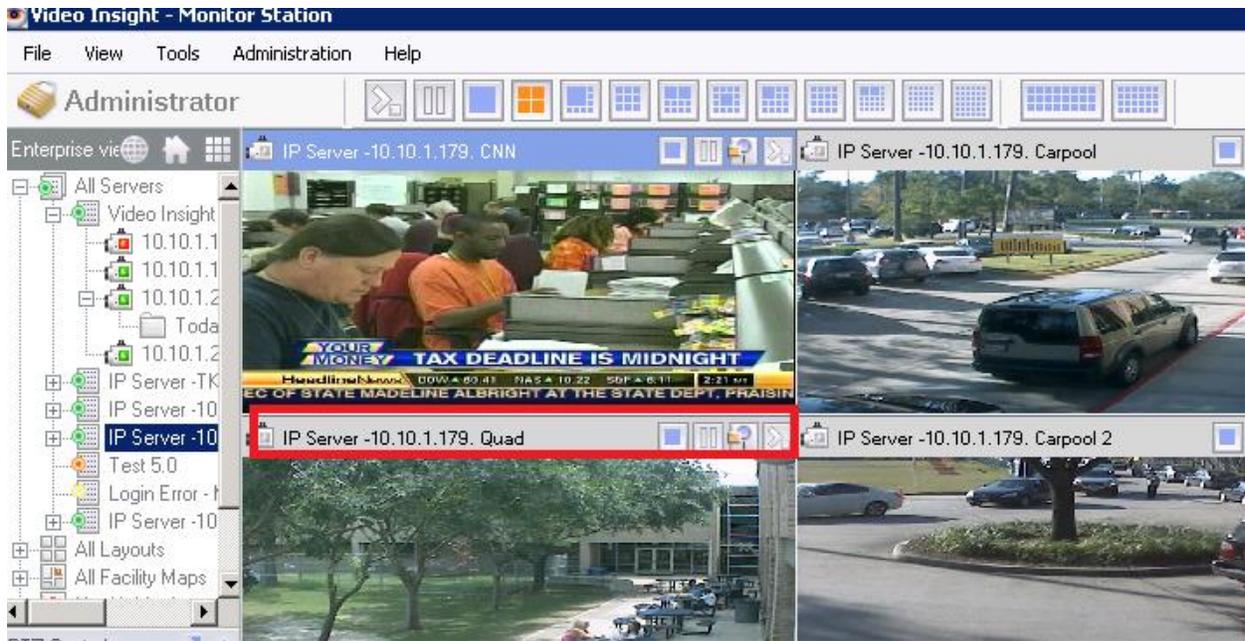


Show layout: This option determines whether the camera's toolbar in Live view will display or not. It is checked by default. When unchecked, more of the screen is used to view the live image of the camera(s) rather than displaying camera information.

When this option is checked it will display camera information as shown in the figure below.

Note

Choosing a player size mismatched to your display and resolution can prevent you from seeing the Controls bar at the bottom of the player.



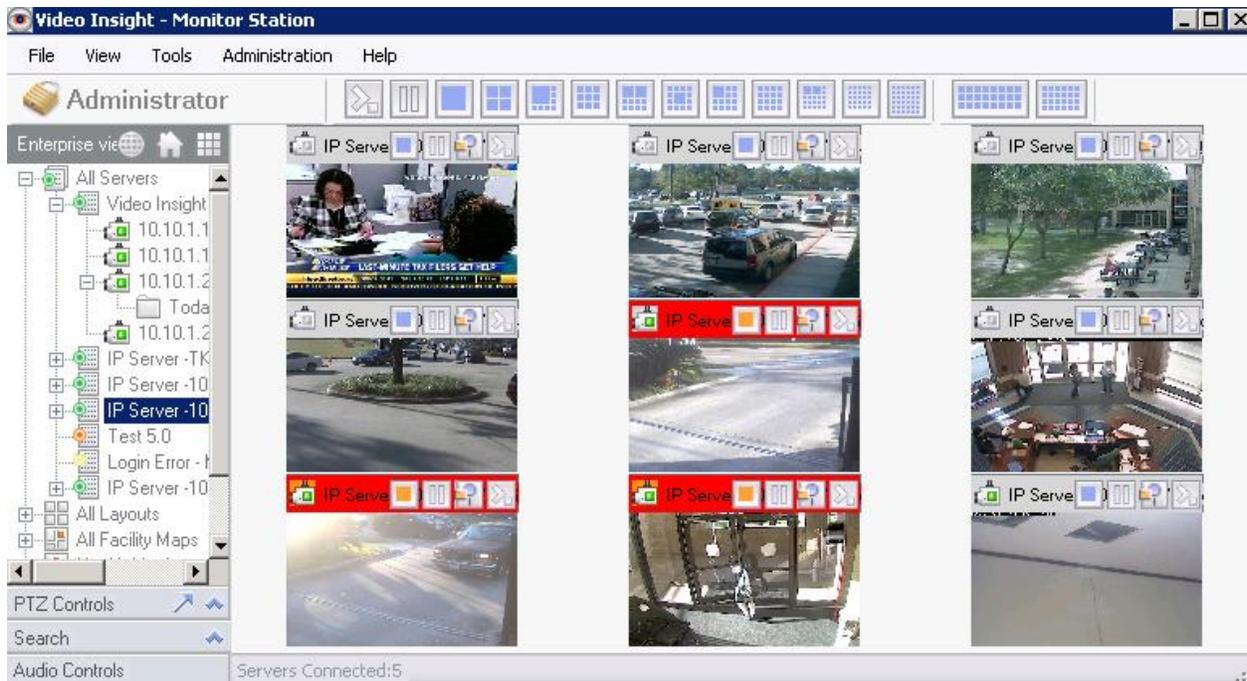
When this option is unchecked, it will not display camera header information.



Show server name: By default, this option displays the server name in the camera toolbar in the main view as well as in the server and camera Live Window pop-ups. The Show layout option must also be checked for this information to appear.

Show camera name: By default, this option displays the camera name in the camera toolbar in the main view as well as in the server and camera Live Window pop-ups. The Show layout option must also be checked for this information to appear.

Force aspect ratio: This option is another customization for achieving the best layout on your display. With Force aspect ratio checked, all live images will be forced to a 4:3 size in the main layout as shown in the figure below. This option does not affect Live Window pop-ups.



Use DirectX display: This option reduces CPU usage by attempting to use DirectX rather than the onboard or installed graphics device. If checked, you must select the correct version of DirectX installed on the computer: DirectX 9, 7 or Legacy for versions older than 7.

If the DirectX version selected is not installed on the computer, the error message “Cannot Initialize renderer (0x80040273)” displays. Select the correct version of DirectX or uncheck the option.

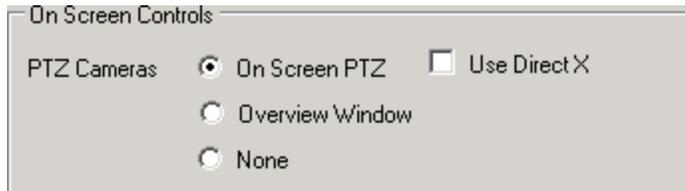
Note

This capability will affect only the first four cameras in live view and Layouts.

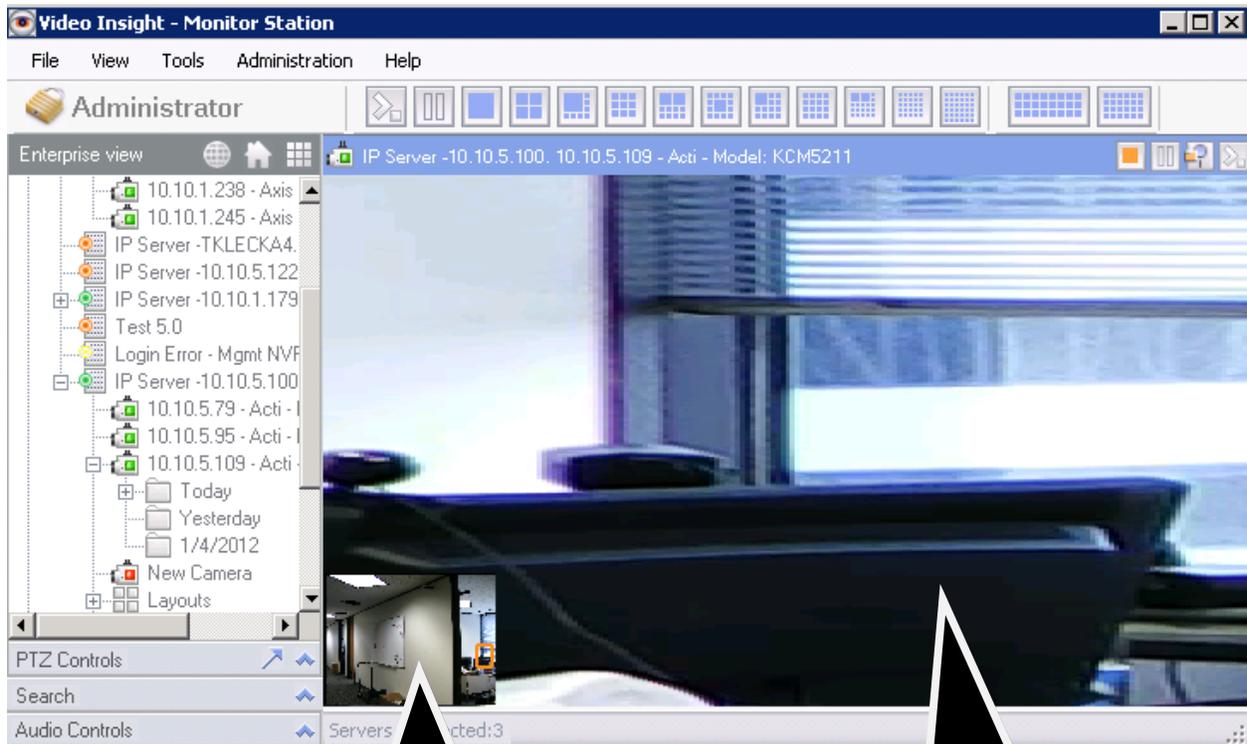
Double click expands camera: This option specifies whether a single- or double-click is required to expand the camera in the left navigation tree to show its recordings. If this option is selected a single click on the camera only displays the camera in the viewing panel.

Use tree navigation server selection for default layout buttons: This option determines which server’s layouts will be used when cycling manually or automatically. See [Cycle Layouts](#) for more information on cycling layouts.

On Screen Controls (for PTZ Cameras): The default is On Screen PTZ. It superimposes directional arrows on the view for PTZ cameras to signify a PTZ camera is selected in live view on the main dashboard.



Selecting Overview Window displays a magnifying glass as a cursor in the live view. To zoom in on an area, draw a square with the cursor. The figure below shows an example of a square drawn on the view.



Overview Window of full camera view

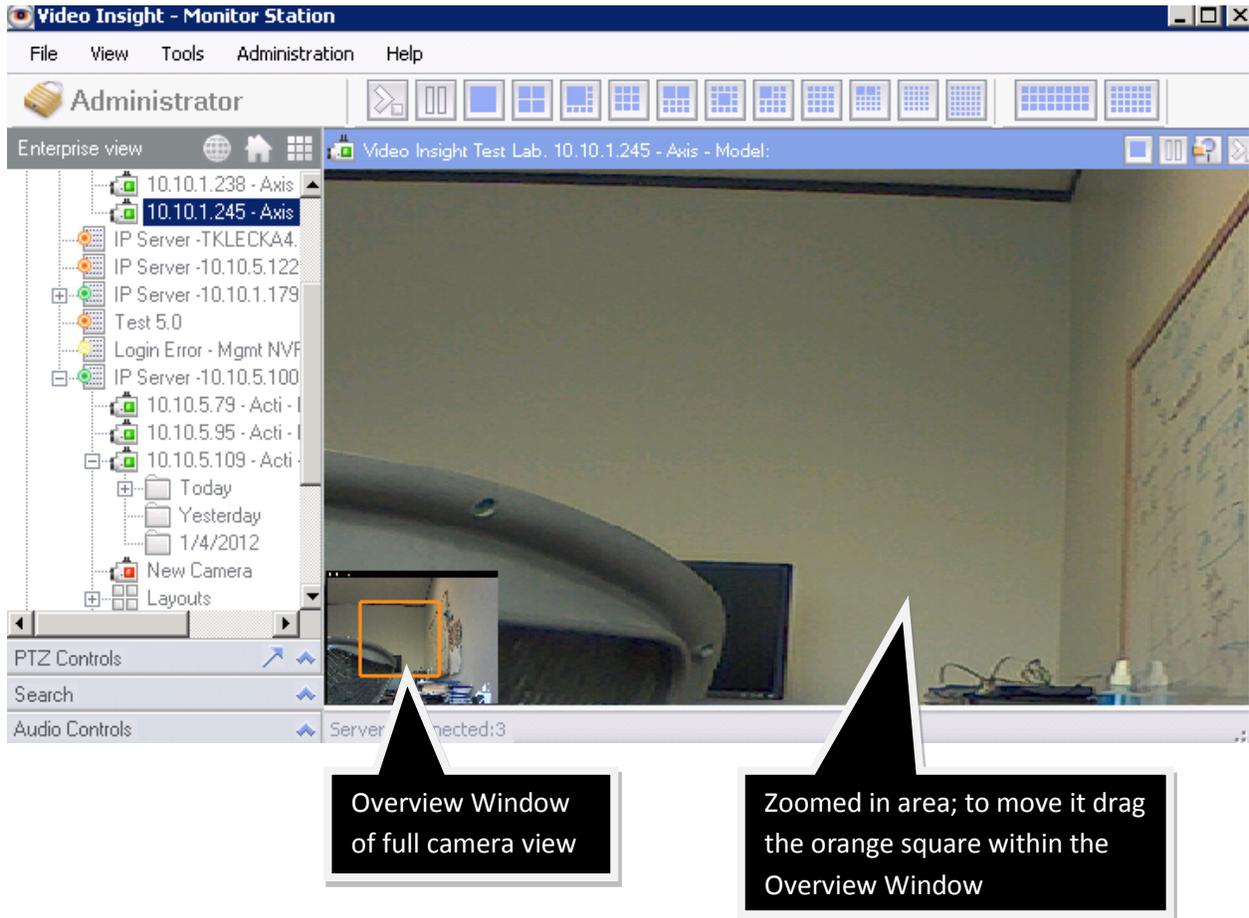
Zoomed in area; to move it drag the orange square within the Overview Window

Selecting None does not display any special cursors for PTZ cameras. Use the PTZ Controls function box found in the left navigation tree.

On Screen Controls (for Standard Cameras): The default is Overview Window. It displays a magnifying glass as a cursor in the live view.



To zoom in on an area, draw a square with the cursor. Standard cameras use a digital zoom. The figure below shows an example of a square drawn on the view.



Selecting **None** disables the ability to digitally zoom in live view for standard cameras.

Tools Configuration tab

General | **Tools Configuration** | Live Window | Audio | Startup

Normal operation Machine Performance
 Low bandwidth mode Normal
 Very low bandwidth mode

Mini toolbars

Cycle layout time 5 Seconds
PTZ cycle time 10 Seconds

Layouts cycle through current server
 Mini-toolbars always on top

Local Settings

Use Registry Export
 Use XML Import
[Empty text field]

Enable Access Control Lane Viewer
 Lock down Access Control Lane Viewer
 View Sentry 360 cameras in Quad View when in single camera mode

Creating clips

Enable Watermark
 Force Motion JPEG format

You can choose from three bandwidth-related options to optimize the live view performance in Monitor Station.

Normal operation: This option uses all available resources to display live streaming. This option is sensitive to network bottlenecks and should only be used for clients with very good connectivity. Normal streams all images as uncompressed MJPEG.

Note

If the Low Bandwidth\High CPU option is selected at the server, client options are ignored as all images are already compressed.

Low bandwidth mode: Select Low bandwidth mode if you are viewing multiple images over moderate network bandwidth. This option compresses multiple images. If you switch to a single image view it will send that image as uncompressed.

Very low bandwidth mode: In Very low bandwidth mode all images are compressed. Choose this option for clients with poor connectivity.

You can use the Machine Performance drop-down menu to choose from three options to improve live streaming when using multiple camera views. This option improves performance when viewing layouts with nine or more cameras.

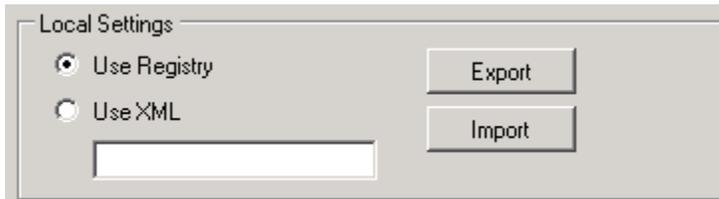
Normal: When selecting this option expect the Monitor Station to use the current capabilities of your client machine's CPU.

Workstation: The Monitor Station will use approximately the same amount of CPU as in Normal mode when viewing a four camera layout and a higher performance of live streaming. If you view a layout with nine or more cameras you will see an increase in CPU usage because more cameras are visibly streaming with better live performance.

High Performance: The Monitor Station will use the most CPU to deliver the smoothest live view with layouts of 16 cameras or more. This option should be selected only if the Monitor Station host has a powerful CPU.

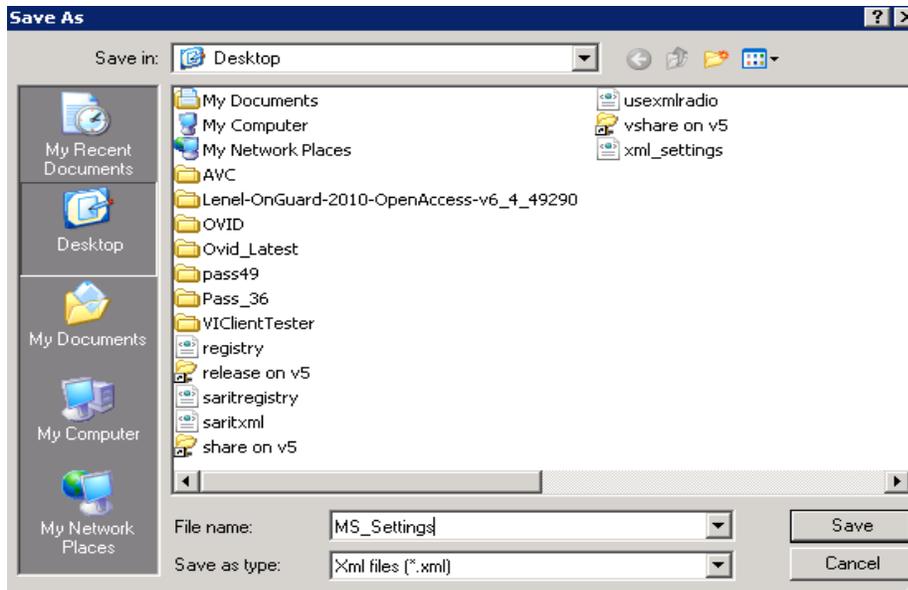
Mini Toolbars (for cycling layouts): See [Cycle Layouts](#) for more information on cycling layouts.

Local Settings: You can export your Monitor Station settings two ways.



To export your Monitor Station settings:

1. Select Use Registry or Use XML as the export method and then click **Export**.



2. Enter a name for the export file and select a save location if different from the default, then click **Save**.

Export files are saved in XML format. The figure below shows a sample export file.

```
<?xml version="1.0" standalone="yes" ?>
- <NewDataSet>
  - <Table1>
    <Key>LocalServerItem</Key>
    <Value>Zj+Mz0m4ntVS8qCxIy9l4OIM/YAM2+K2</Value>
  </Table1>
  - <Table1>
    <Key>ExitConfirm</Key>
    <Value>1</Value>
  </Table1>
  - <Table1>
    <Key>StandardSecurityLevel</Key>
    ...
  </Table1>
```

You can use this file to configure other clients. Click **Import** in the same area to import the previously exported file.

Enable Access Control Lane Viewer: This option is for [BlackBoard](#) access control integration.

Note

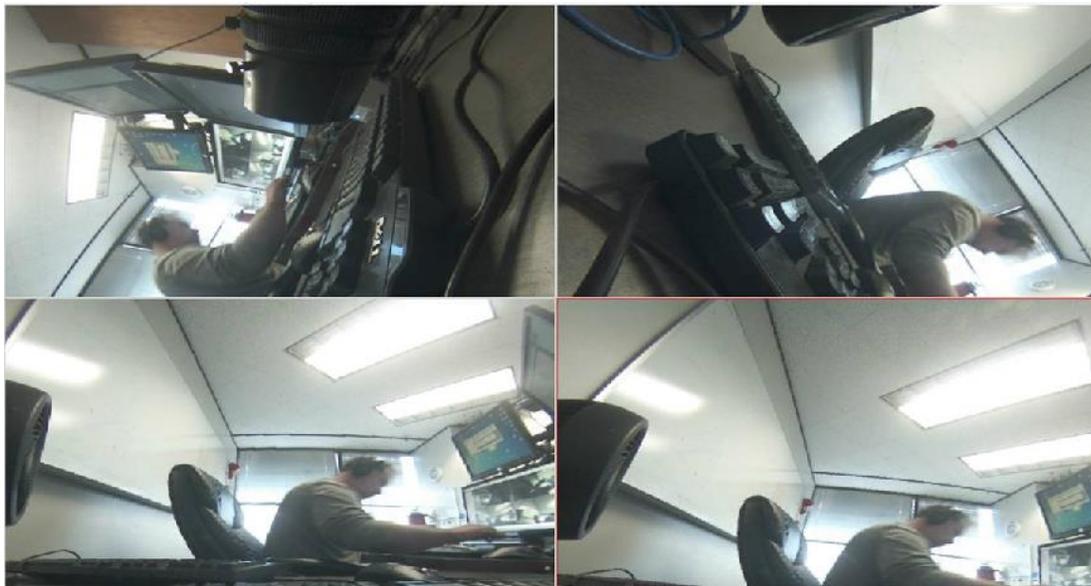
BlackBoard and other access control integrations are discussed beginning on page 241.

Lock down Access Control Lane Viewer: This option is for BlackBoard access control integration.

View Sentry 360 cameras in Quad View when in single camera mode: Left unchecked, Sentry 360 cameras offer multiple views: Full image, Quadview and Panoramic. The figure below shows an example of this view.



You can check the option and if the camera is selected from the main dashboard or the left navigation tree only the quad view displays. The figure below shows an example of this view.



Creating clips (Enable Watermark): By default, this option interlaces the Checksum security mark to detect any tampering with the created clips. See [topic] for more information on creating clips.

Creating clips (Force Motion JPEG Format for Clips): By default, this option creates all clips in Motion JPEG format. Motion JPEG is a format that can be read by most software media players.

Live Window tab

Live window configuration. The live window is used as a free floating camera view. Select these options for desired operation.

- Block live window pop-ups
- Live window always on top
- Integrated Facility Map
- Use Four Camera Facility Map display
- Force record option Keep minutes
- Red Outline on Live Window
- Pause main display when live window launches
- Include Server Name for All Facility Maps
- Include Server Name for All Layouts
- Layout tour cycle time seconds

Rules Manager Triggered Actions

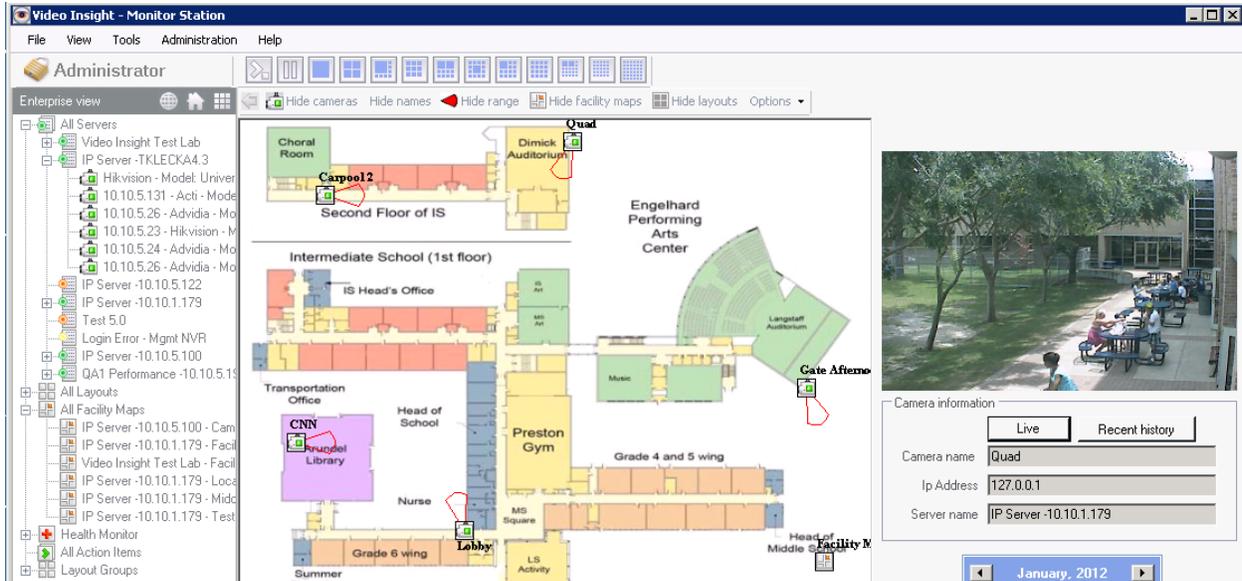
- Block rules from popping up messages/instruction
- Block rules from switching main layout
- Block rules from launching instant replay window

- Flash Red on Motion Duration
- Use Maintenance view

Block live window pop-ups: This option is unchecked by default. If checked, it suppresses all Live Windows from popping up while Monitor Station is active. Live Windows can be sent to you from other users, by rules or manual launch.

Live window always on top: This option is unchecked by default. If checked it shows all received Live Windows on top of Monitor Station.

Integrated Facility Map: Selecting this option displays a Facility Map in the main dashboard area of Monitor Station on the left side of the left navigation tree. See [Facility maps](#) for more information on creating, maintaining and using facility maps. The figure below shows an example of a facility map.



Use Four Camera Facility Map display: You can apply this option to both integrated and non-integrated maps. The four camera view is very useful when attempting to seam together a four eye camera to view a complete hallway at once, such as the Arecont 180 or 360 cameras. This view can also be used for other cameras, as shown in the figure below.

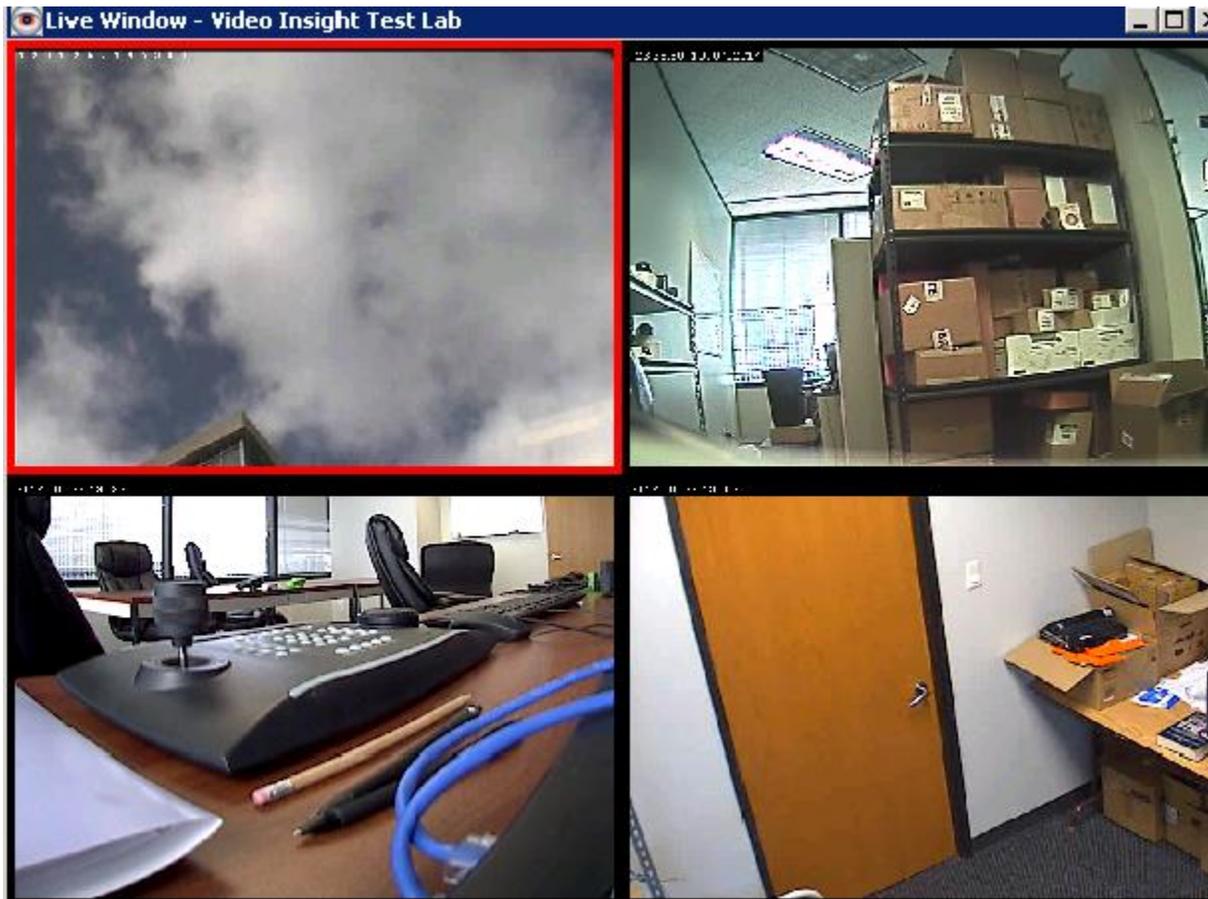


Force record option: Checking this option adds a button to the Camera Toolbar in the Main Dashboard. Clicking this button immediately records, and will continue to record, until the button is clicked again or the time set has been reached (maximum of 200 minutes).

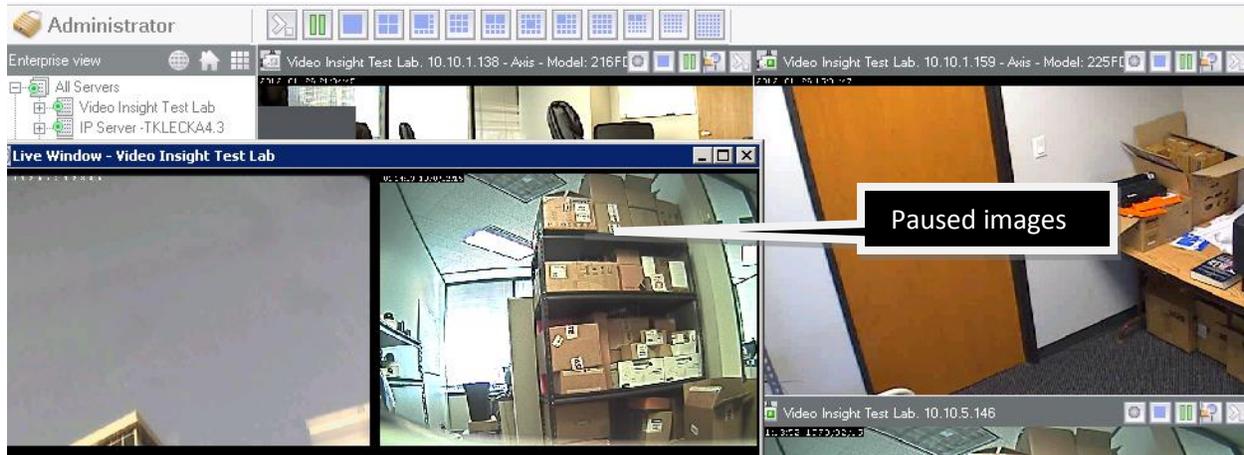


Selecting this option does not permanently change the camera's recording type. Clicking the Force Record button forces the camera to record and when complete the camera will resume its normal recording setting.

Red Outline on Live Window: You can launch Live Window by right-clicking on the server node from the left navigation tree. It displays all cameras for that server and outlines each with a red line for a few seconds when motion is detected, as shown in the figure below.

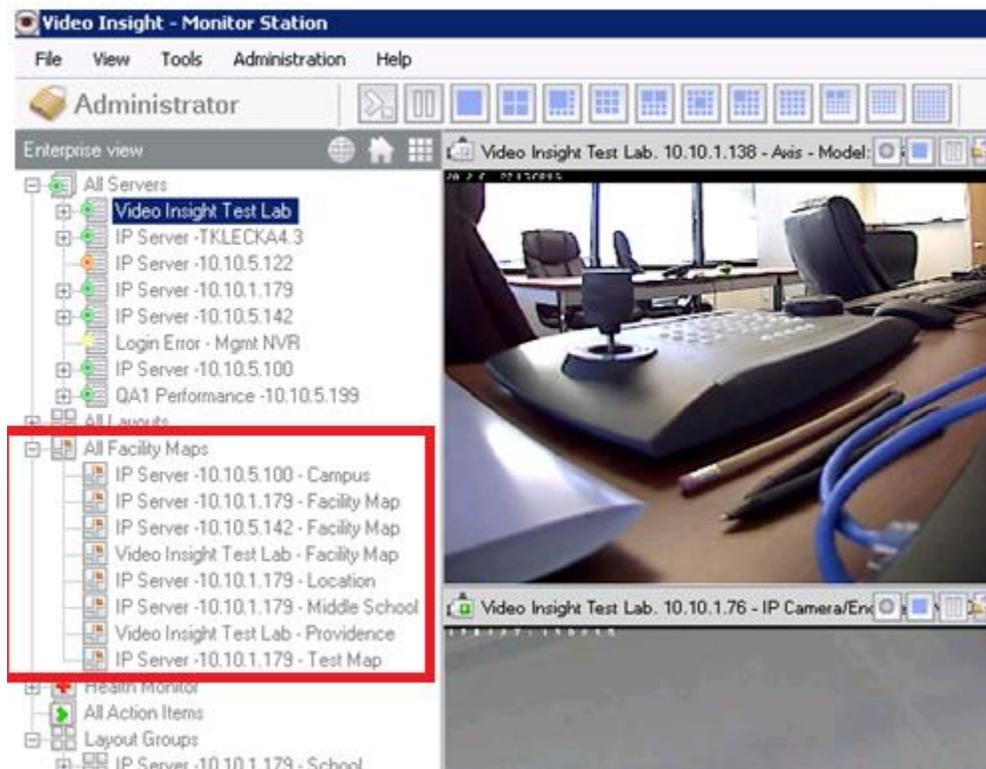


Pause main display when live window launches: If you launch Live Window from a server or from the left navigation tree or for a single camera, the main dashboard will pause all streaming to improve performance and conserve bandwidth. The paused images will appear gray after a few seconds.



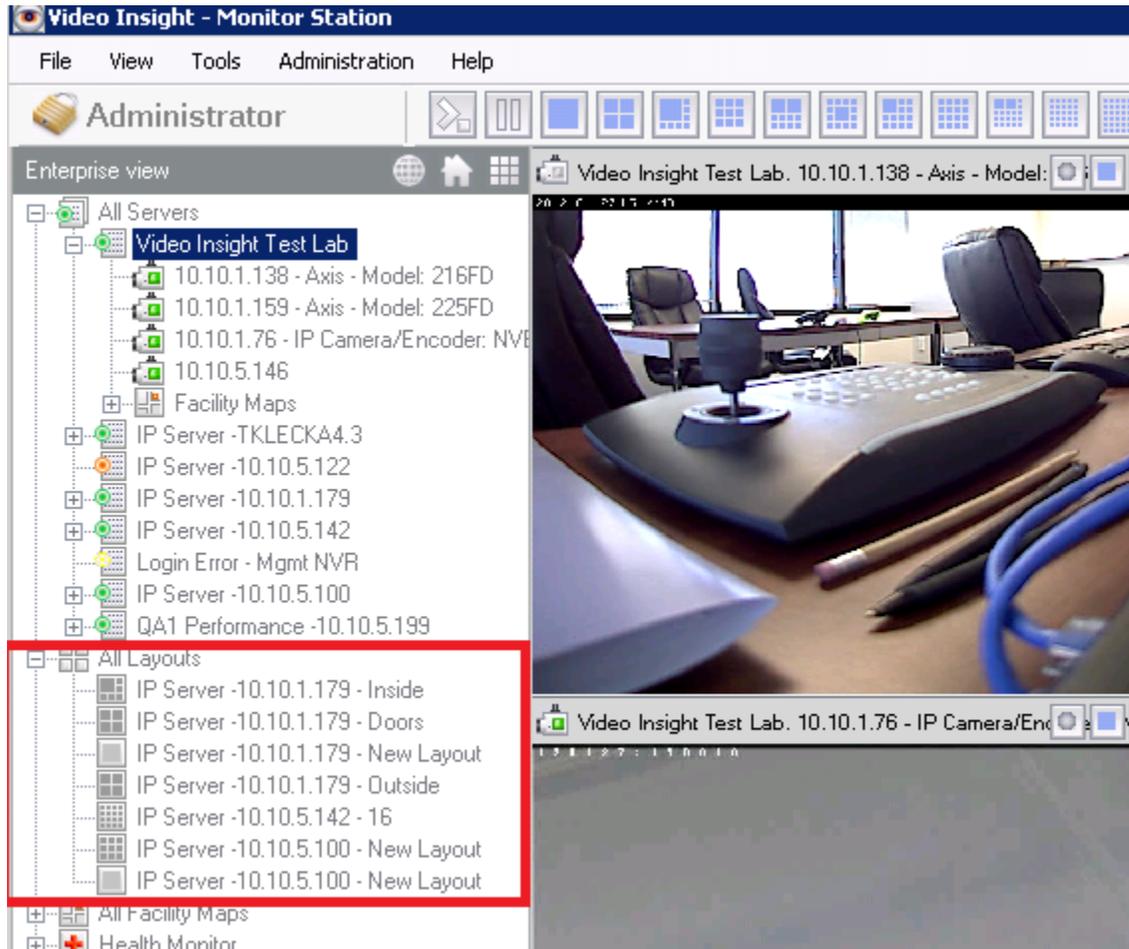
To resume live streaming when closing the live window, click **Pause**.

Include Server Name for All Facility Maps: Facility maps are available in the left navigation tree for quick access, but when multiple servers are added to a single Monitor Station it can be difficult to determine which facility maps belong to which server. You can add the server name to make it easier. If checked, the server name will preface the Facility Map name, as shown in the figure below.



Include Server Name for All Layouts: Layouts are available in the left navigation tree for quick access, but when multiple servers are added to a single Monitor Station it can be difficult to determine which

layouts belong to which server. You can add the server name to make it easier. If checked, the server name will preface the Layout name, as shown in the figure below.



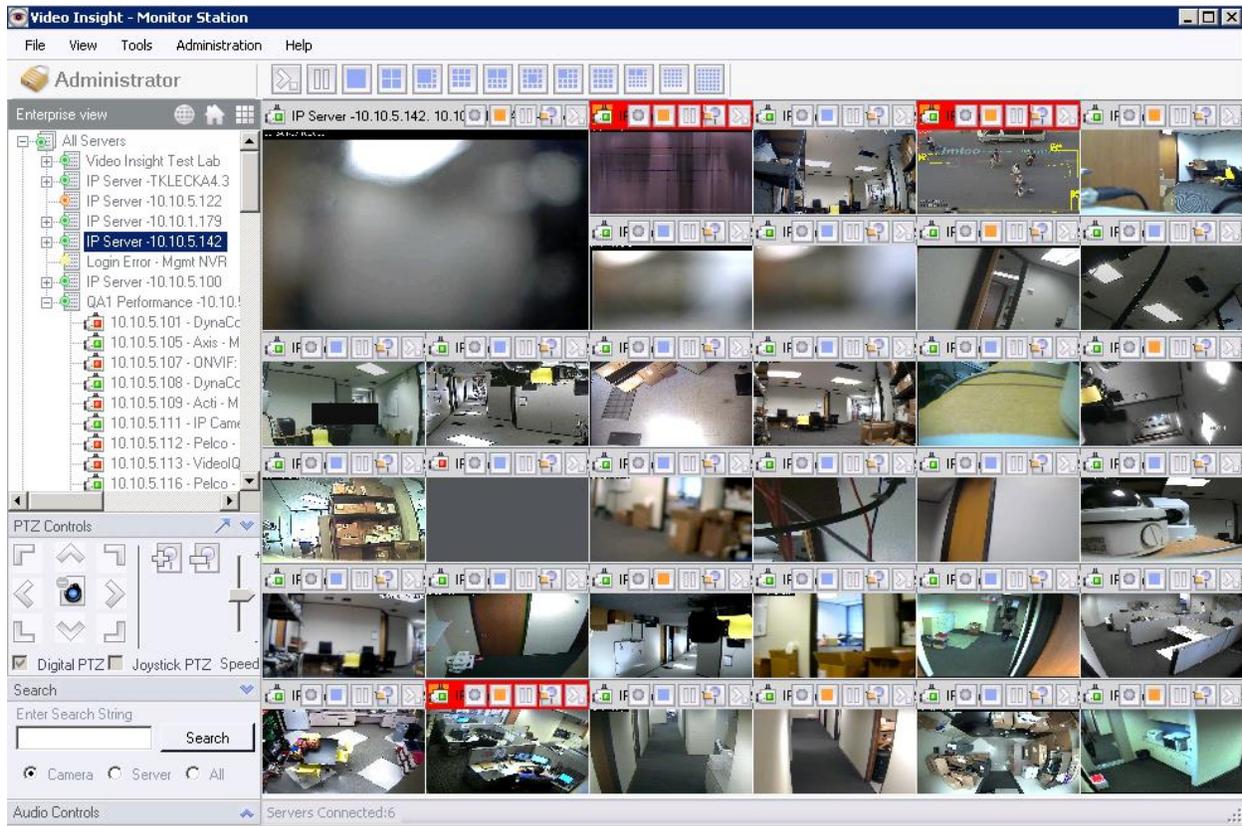
Layout tour cycle time: You can set the time interval between each camera on a tour. The default is five seconds.

Rules Manager Triggered Actions: Creating rules adds flexibility and customization to your software. Rules can include results that send notifications to all Monitor Stations or specific users. You can prevent these dialog boxes from appearing in your Monitor Station by checking the applicable boxes.

Flash Red on Motion: You can select this option to highlight the camera toolbar in red to indicate that motion has been detected on a camera. This is useful when viewing many cameras at once as shown in the figure below.

Note

There is no way to retrieve the messages you would have received once they are blocked.



Use Maintenance view: You can select this option to change the Contact Information tab in Camera Properties to Maintenance tab properties. See Maintenance tab for more information on the difference between the two tabs.

Audio tab



Audio notification on motion: You can select this option to give the user the ability to specify if there will be audio notification when motion is detected on a camera. You have the option of no sound, default system beep or you can load your own notification sound by browsing to a .WAV file.

Audio notification from tasks and alarms: You can create rules that specify that an audio notification will be generated based on a predetermined set of events. You have the option of no sound, default system beep or you can load your own custom notification sound by browsing to a .WAV file.

Startup tab

The screenshot shows the 'Startup' tab of the Video Insight Administrator configuration window. The window has a tabbed interface with 'General', 'Tools Configuration', 'Live Window', 'Audio', and 'Startup' tabs. The 'Startup' tab is active. It contains the following settings:

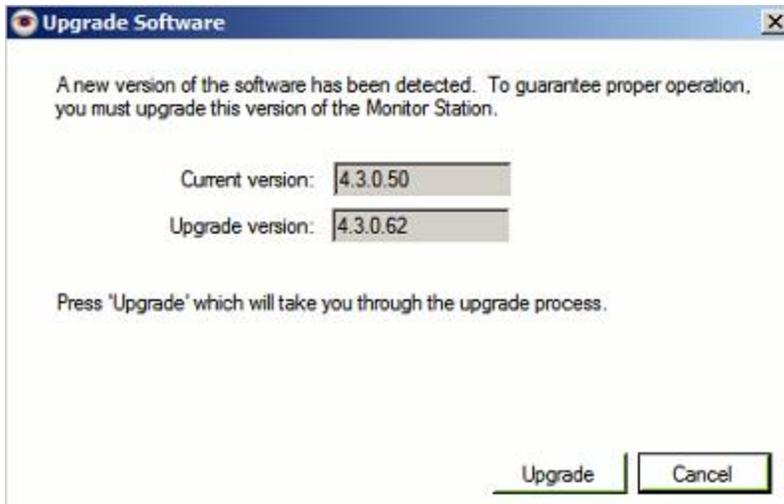
- Starting Layout:** A group box containing two radio buttons and two dropdown menus. The 'First cameras in layout' radio button is selected, and its dropdown menu shows '1 Camera Layout'. The 'Custom layout' radio button is unselected, and its dropdown menu shows 'My Tour (IP Server -TKLECK)'.
 - First cameras in layout
 - Custom layout
- Hide archive tree on startup
- Launch facility map on startup: This option is accompanied by a dropdown menu labeled 'Facility map name'.
- Auto upgrade
- Start in full screen mode
- Verify Active Directory login
- Auto Login:** A group box containing an 'Enable Auto Login' checkbox and two text input fields labeled 'User' and 'Password'.
 - Enable Auto Login
 - User: []
 - Password: []

Starting Layout: The Monitor Station main dashboard display is set by what is selected here. If you want to display a specific camera choose the first camera in layout options and choose 1 Camera Layout from the drop-down menu. You can display a specific customized layout by selecting Custom layout and the correct server and layout option from the drop-down menu.

Hide archive tree on startup: Selecting this option hides the left navigation tree.

Launch facility map on startup: You can select a specific facility map on startup. Check this option and select the desired Facility Map from the drop-down menu. When you launch Monitor Station a separate pop-up window will display the selected Facility Map.

Auto upgrade: Select this option to have the local Monitor Station compare its version to all the servers that are connected to it at the next startup. If a later version is found on a server Monitor Station will be prompted to upgrade, as shown in the figure below.



Click **Upgrade** to upgrade the software on the Monitor Station. Monitor Station will close and the installation will appear on the screen. Start Monitor Station and navigate to Help, then About Video Insight to confirm the upgrade was successful.

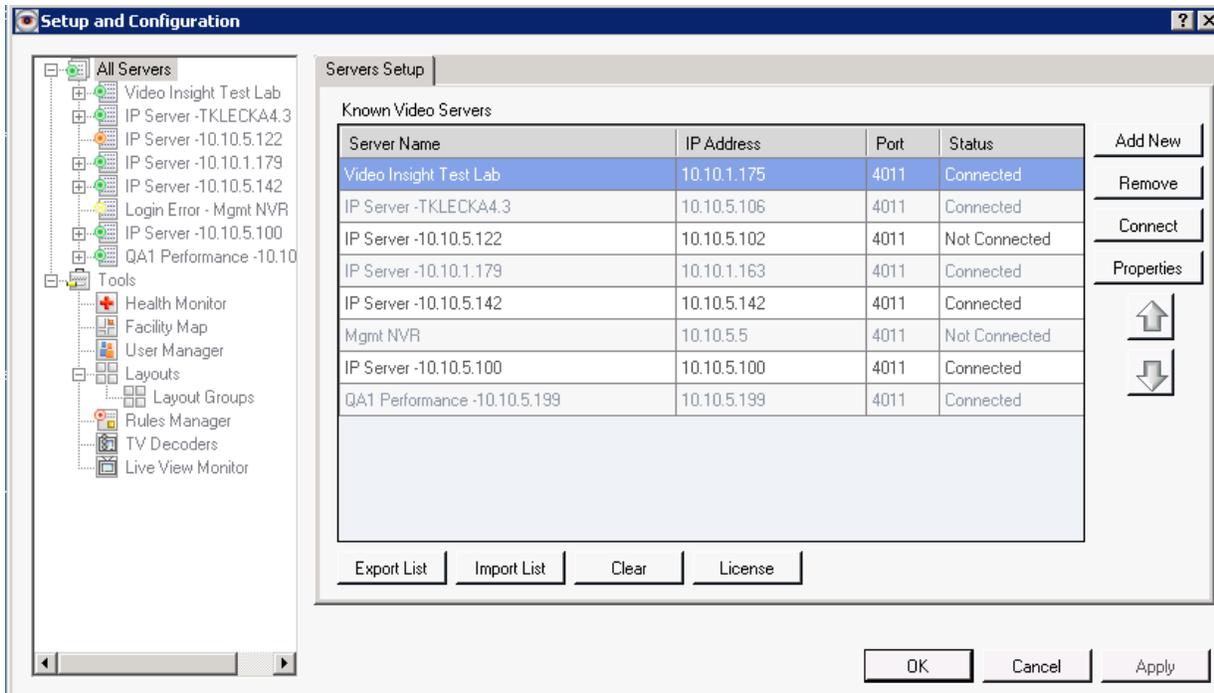
Start in full screen mode: Select this option to have Monitor Station display in full screen the next time it is started.

Verify Active Directory login: Select this option to have authentication of user credentials in Active Directory occur in real-time.

Enable Auto Login: To bypass the login dialog box, enter the user name and password. See [Login](#) for more information on login.

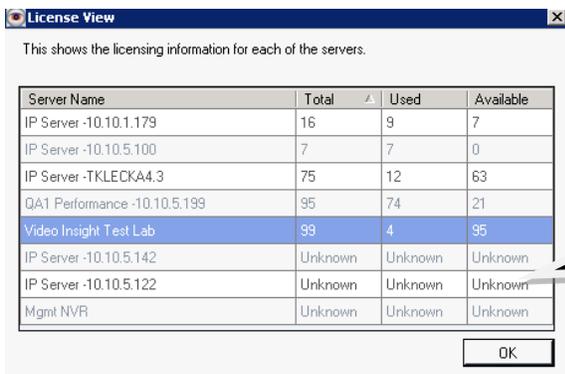
Administration>Setup and Configuration

You can use Setup and Configuration to change many aspects of the video surveillance setup, including changing server properties, user management and application integration with Health Monitor and Live View Monitor. Administrator-level access is required to change most of the options.



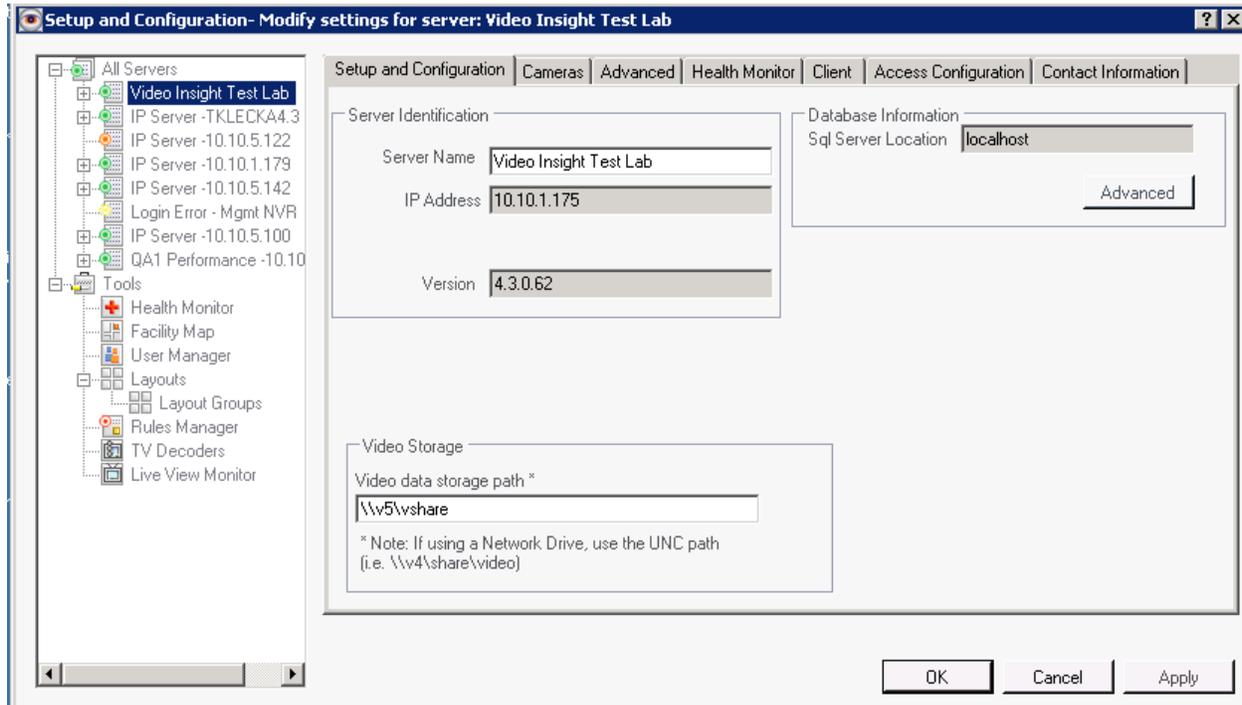
Click the up and down arrow buttons to change the server display order in the left navigation tree.

Click **License** to view the number of each server’s available licenses. Clicking License displays the total number of cameras licensed, the total used and the total available, as shown in the figure below.



Unknown will appear when server is not connected

Setup and Configuration Left Navigation Tree

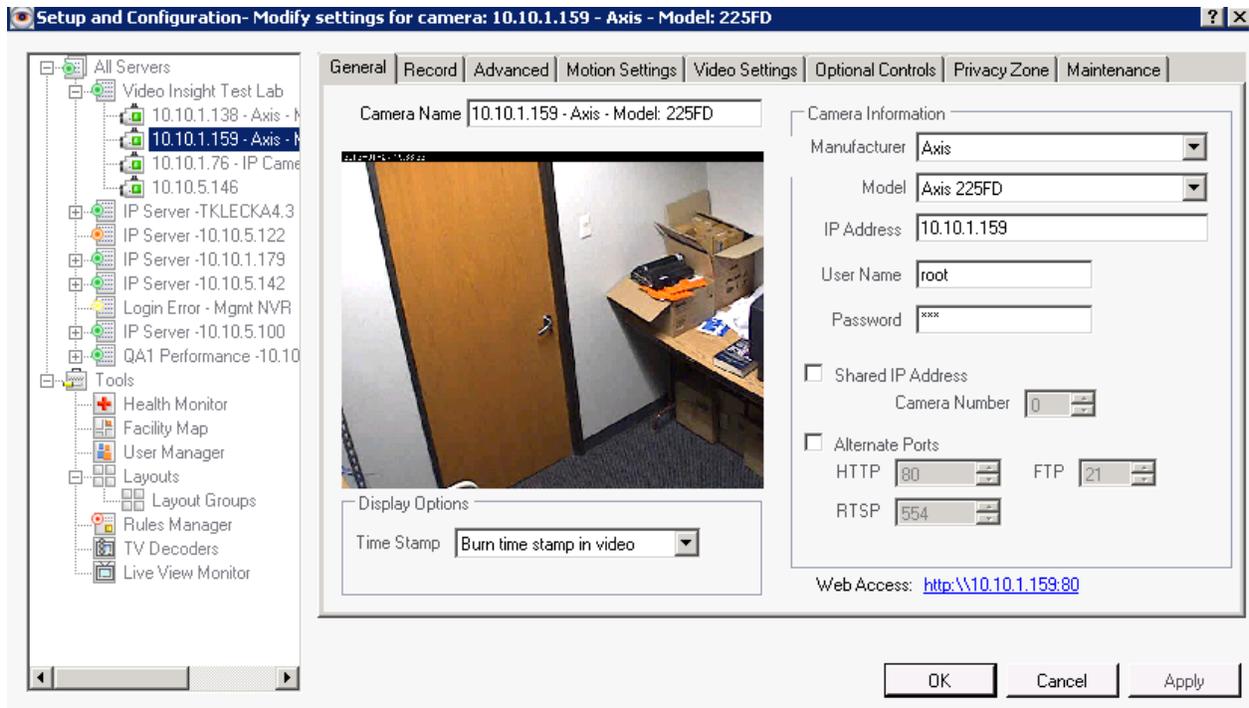


The left navigation tree displays a status color for each server:

-  = Server is connected and settings may be modified.
-  = Server is not connected due to a login error. It will continue to record video to the specified location; however, modifications to settings using MS or IPSM are not allowed.
-  = Server is not connected, possible due to a stopped service or a problem with the connection properties; confirm the IP address and port.

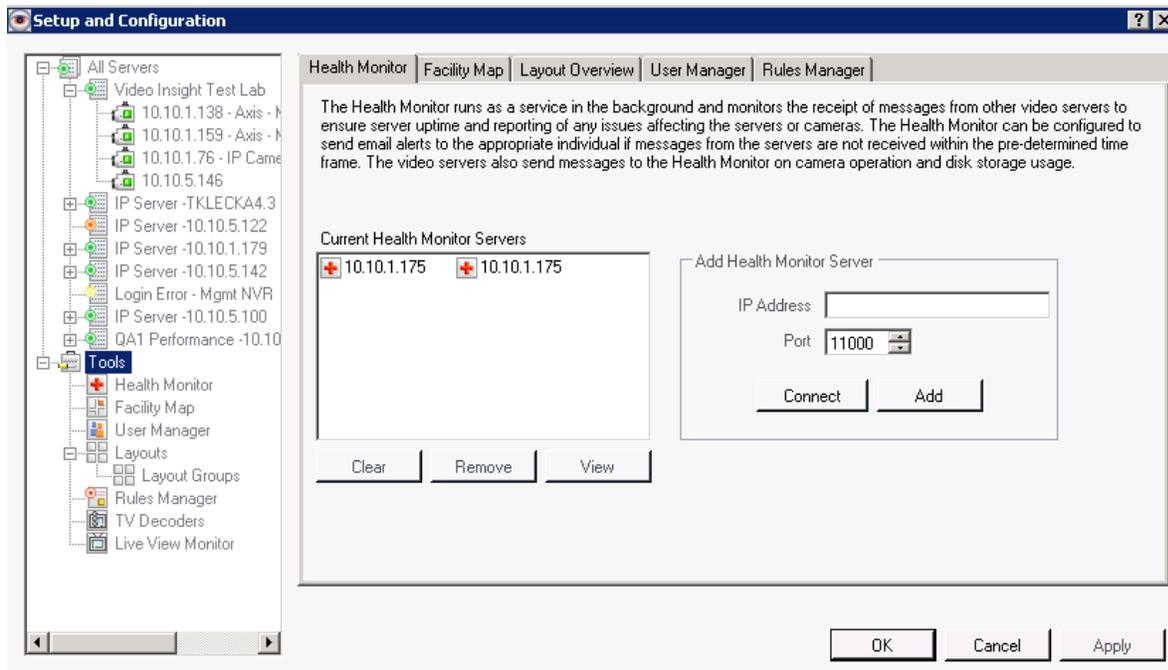
Selecting a server from the left navigation tree displays the server's properties. Administrator rights are required to modify them. See [IP Server customization](#) for more information on each field and tab.

Clicking on a connected server allows quick access to the properties of attached cameras.

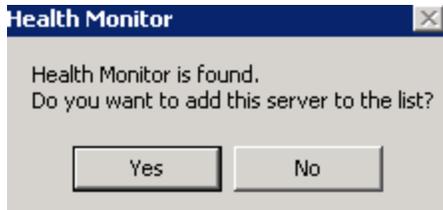


See [Modifying camera details](#), for more information on camera properties.

Setup and Configuration Tools Node

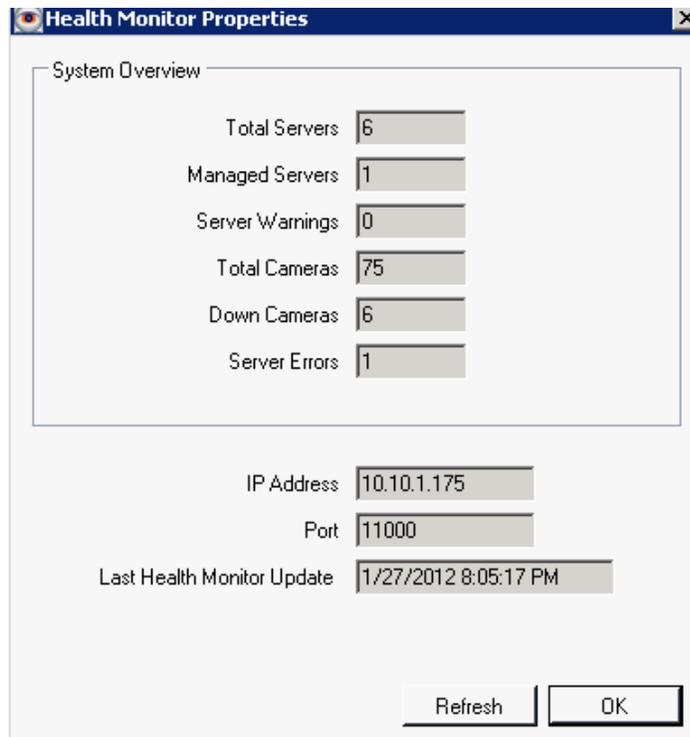


See [Health Monitor](#) for more information on Health Monitor. You can add any installed Health Monitor by entering its IP address and port. Click **Connect** to test the connection parameters as shown in the figure below.



Click **Add** to add the Health Monitor without testing the connection.

You can view the status of a listed Health Monitor by highlighting it.



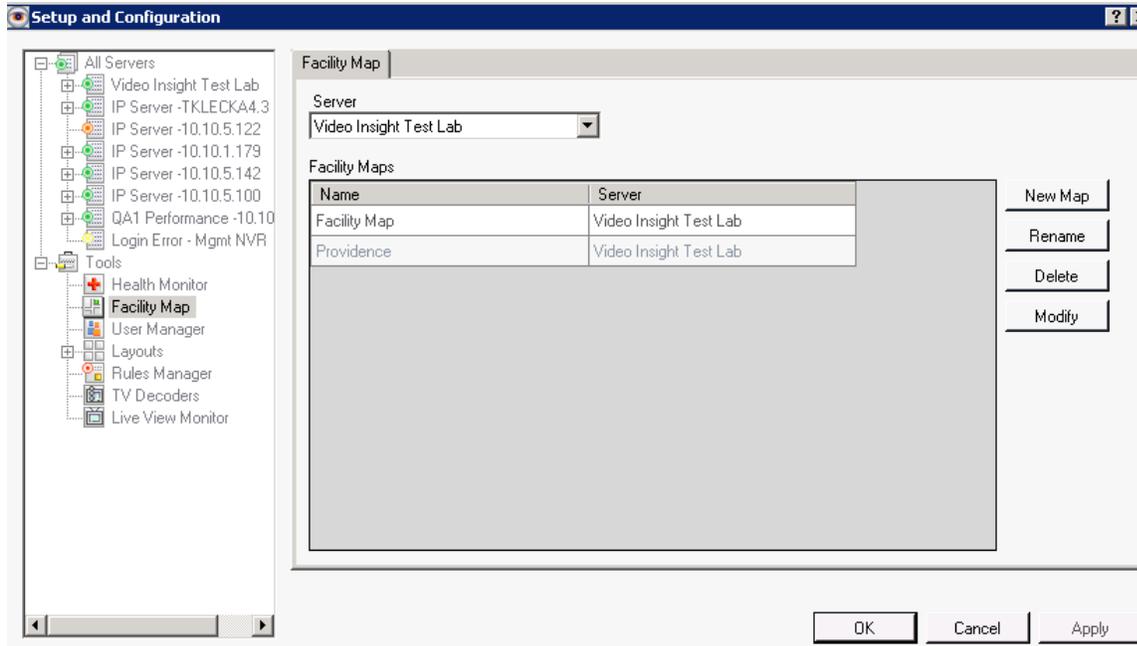
Facility Maps

Camera names may not be descriptive enough to identify a camera. You can use Facility Maps to upload floor plans of your buildings and place cameras on the plans to represent their location. This feature supports multiple layers of maps that can link to one another and supports cameras on each map. Layouts can also be placed on Facility Maps. Once Facility Maps are set up, you can use Monitor Station to view all your cameras by Facility Map views instead of the server and camera tree view.

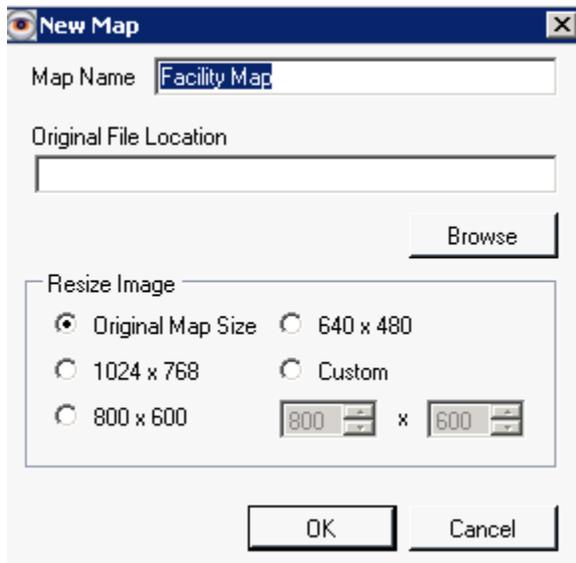
Adding a Map

To add a facility map:

1. Click Facility Map.



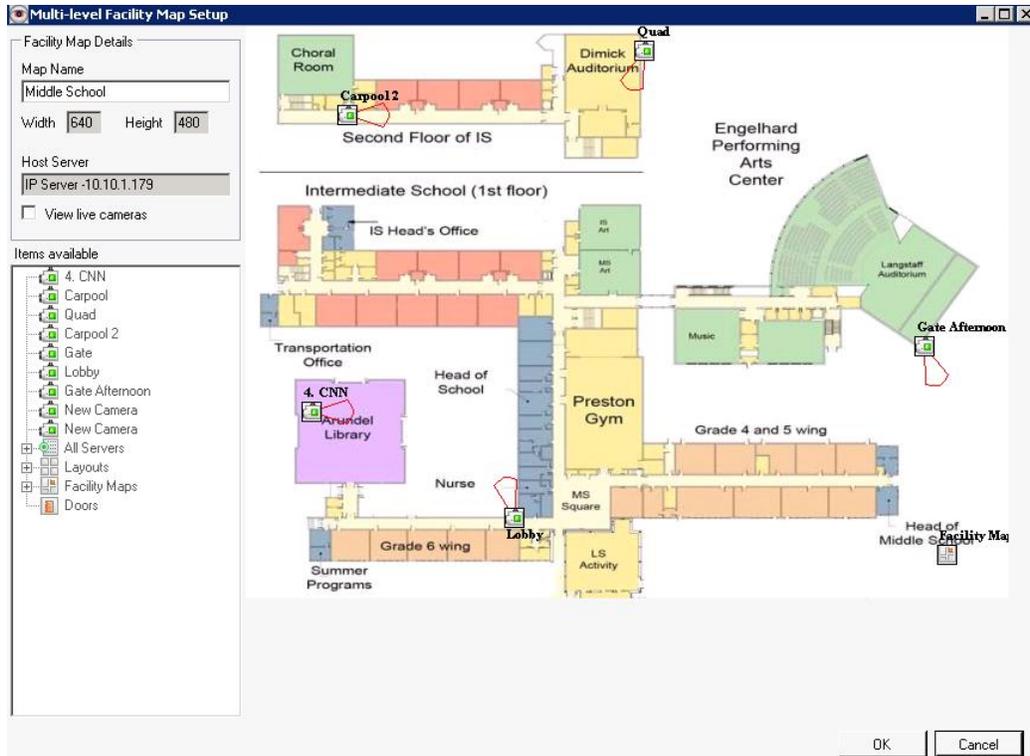
2. Select the server to add a map.
3. Click **New Map**.



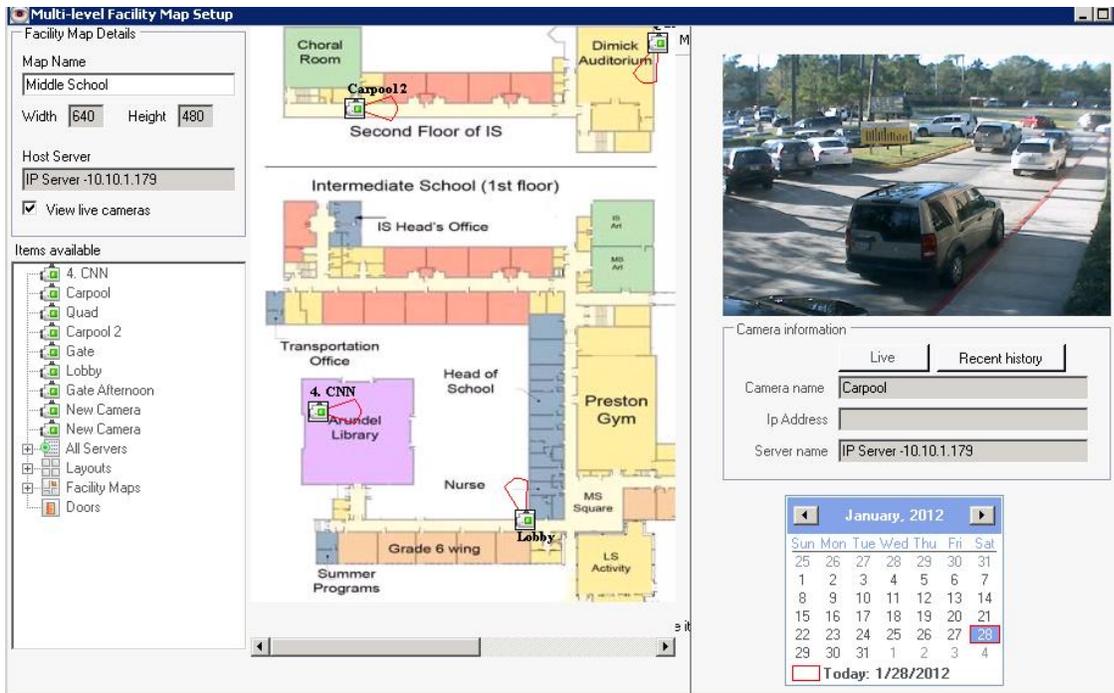
4. Enter the map name.
5. Browse to the location of the map image. JPG- or JPEG-formatted images work best.
6. Keep the original map size or select a new size for it, keeping in mind the average monitor resolution that will be used to view the map in Monitor Station.
7. Click **OK**.

Note

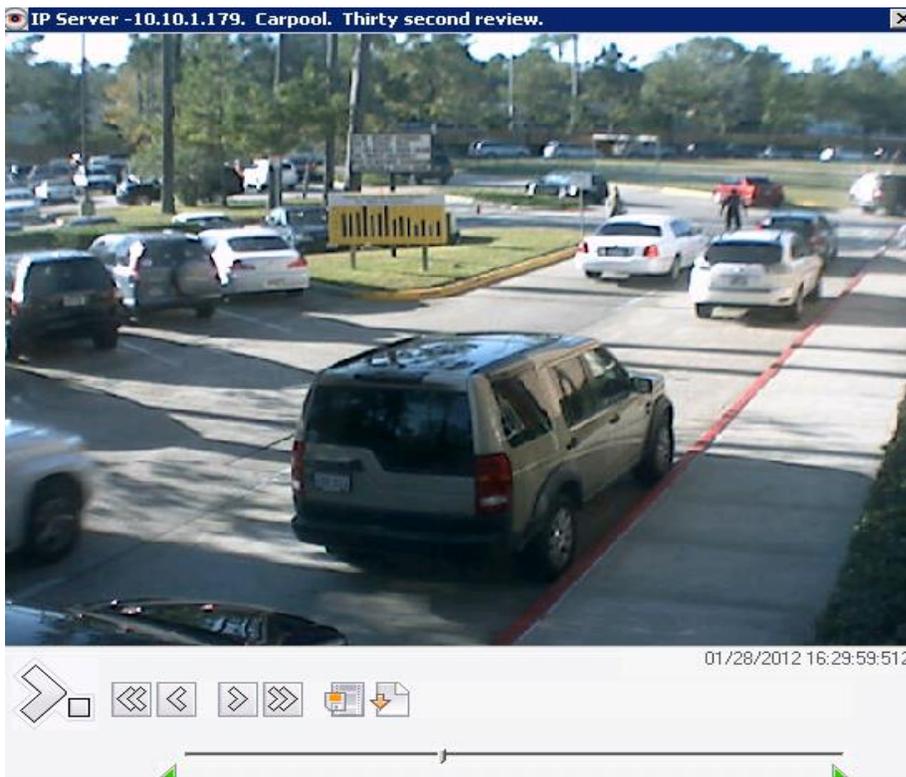
Double-click an existing item to remove it from the map.



8. Drag and drop available items from the left pane on to the map and align them with their view. Items such as cameras, layouts, doors (doors are access points used for Access Control integrations) and other facility maps may be overlaid on the newly created Facility Map.
9. Verify camera placement by checking the box for View live cameras to view live images from the camera.



10. Click **Recent History** to view the last 30 seconds of recorded video.

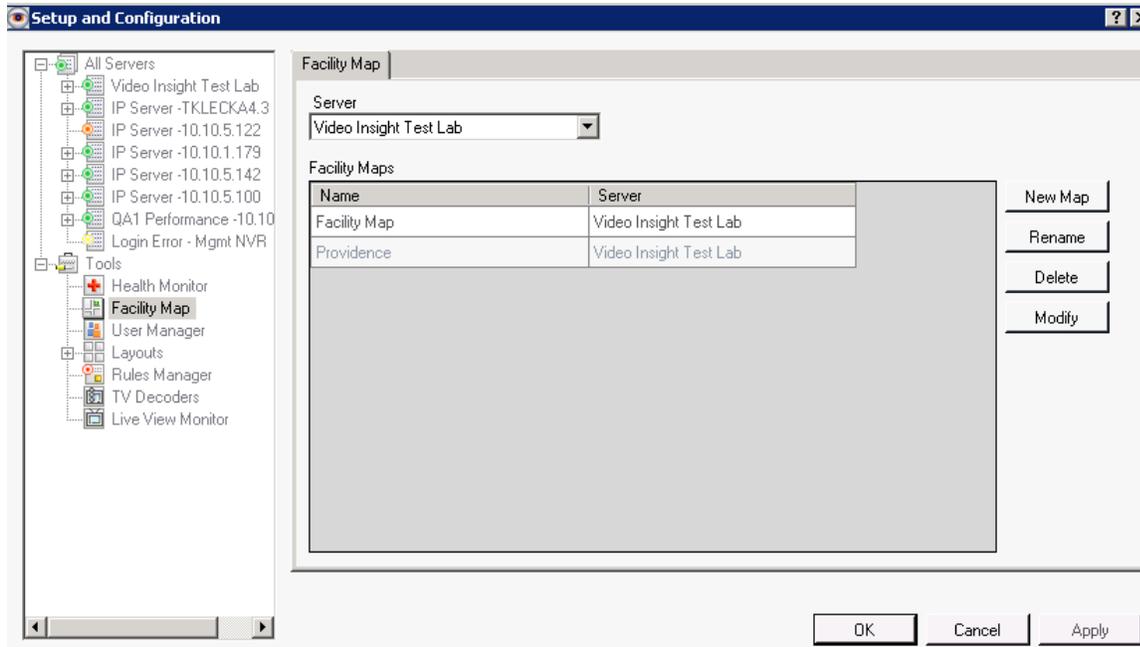


11. When all items have been positioned on the map, click **OK**.

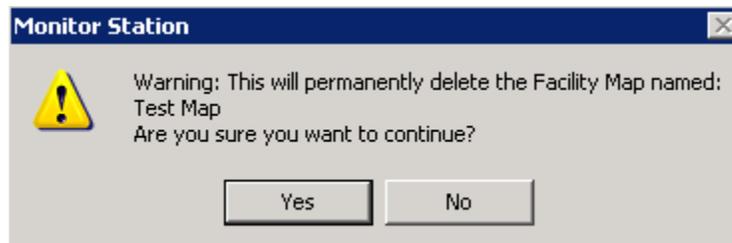
Deleting a Map

To delete a facility map:

1. Click **Facility Map**.



2. Select the server that has the map to delete.
3. Select the map to delete from the Facility Maps list.
4. Click **Delete**.

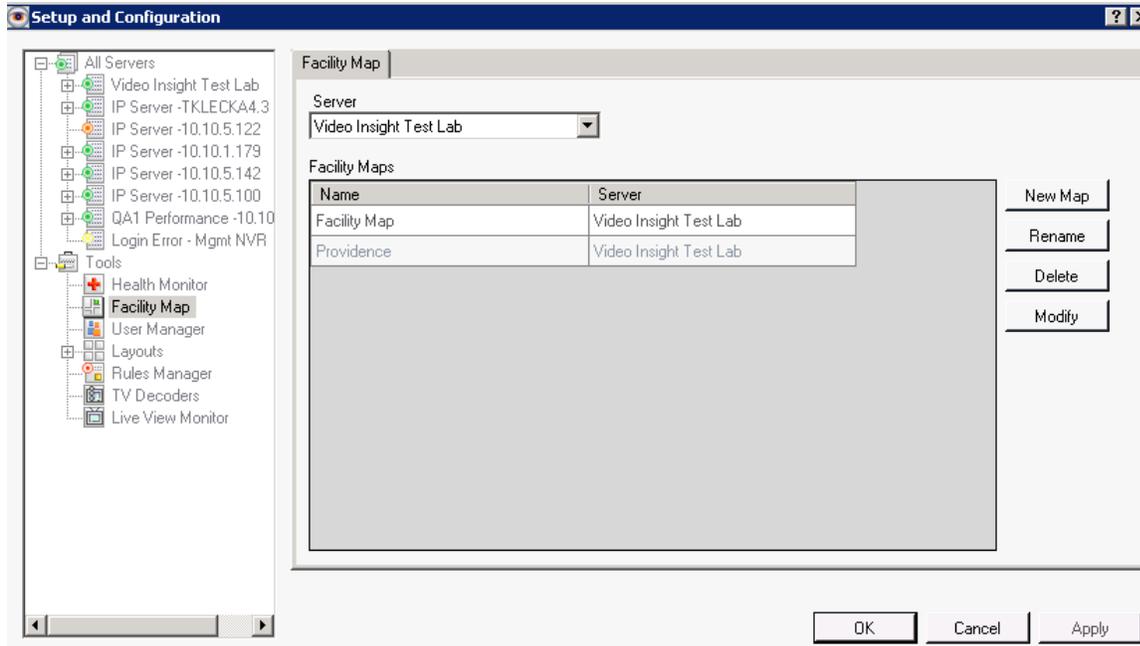


5. Click **Yes** to confirm.
6. Click **Apply** and then **OK**.

Modifying a Map

To modify a facility map:

1. Click **Facility Map**.

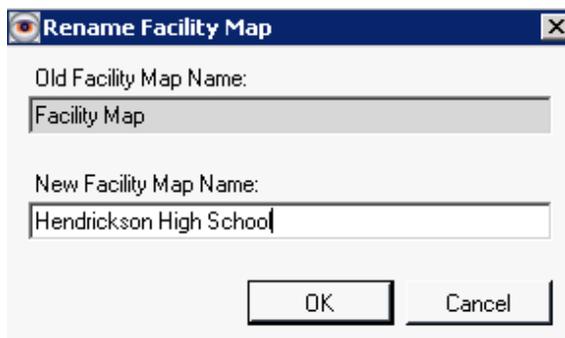


2. Select the server with the map to modify.
3. Select the map to modify from the Facility Maps list.
4. Click **Modify**.
5. Make changes as needed.
6. Click **OK**.

Renaming a Map

To rename a facility map:

1. Click Facility Map.
2. Select the server with the map to rename.
3. Select the map to rename from the Facility Maps list.
4. Click Rename.



5. Enter the new map name.
6. Click **OK**.

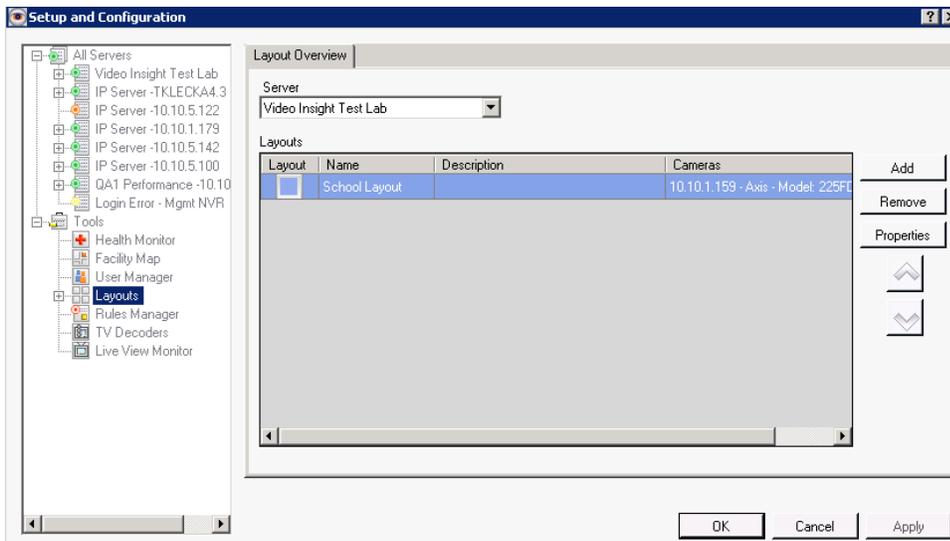
Layouts

You can create custom layouts using cameras from multiple servers. When you add a custom layout to a server it is available to all Monitor Station users that have the necessary rights.

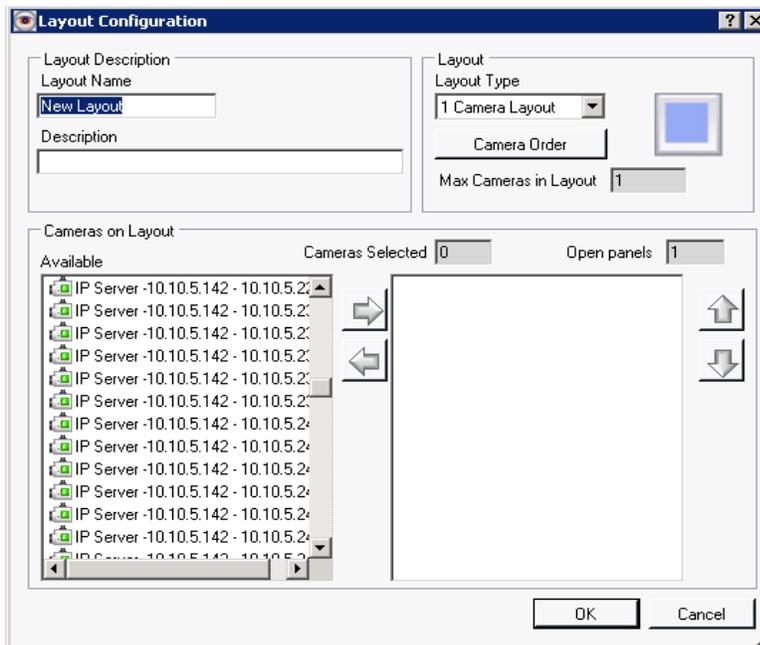
Adding Layouts

To add a layout:

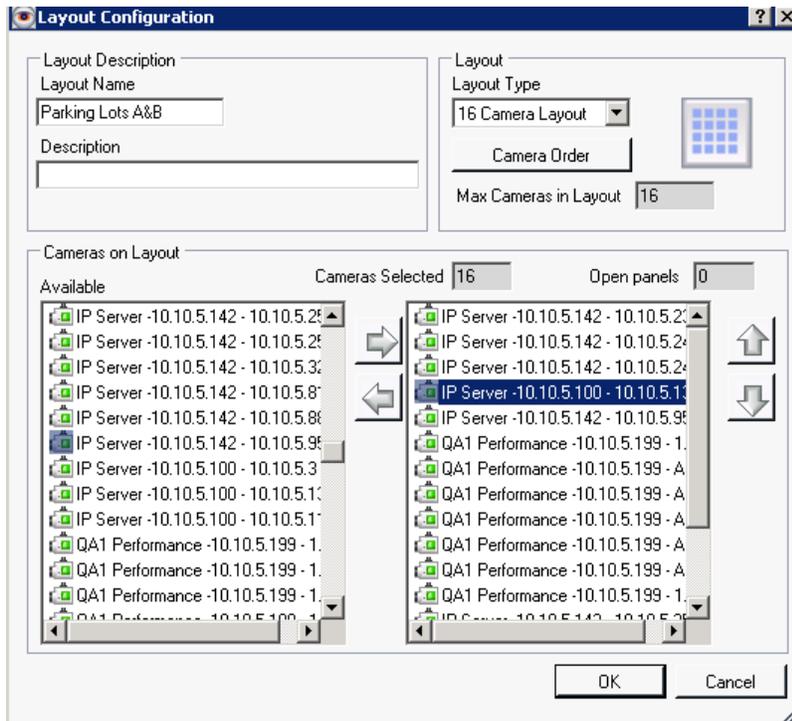
1. Select Layouts.



2. Click Add.



3. Enter the layout name.
4. Adding a description is optional.
5. Select the layout type from the drop-down menu.
6. Select cameras from the left pane and add them by clicking the right arrow. Select cameras from the right pane and remove them by clicking the left arrow.

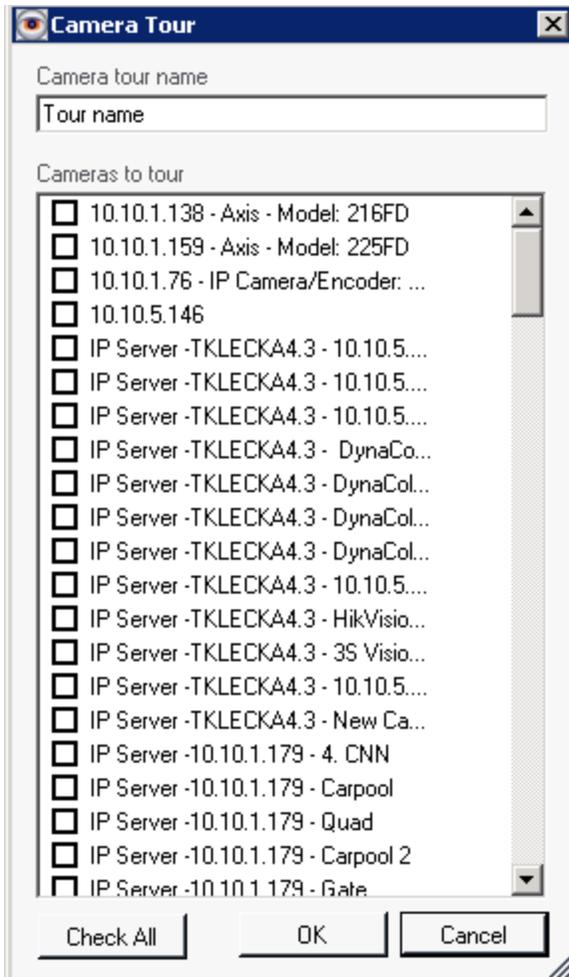


7. You can reorder the cameras in the layout by clicking the up and down arrow buttons.
8. Click **OK**.
9. Click **Apply** and then **OK**.

Adding Layout Tour

To add a layout tour:

1. Repeat steps 1-5 in the Adding Layouts section.
2. When selecting cameras to add to the Layout, select Camera Tour. (This option will appear at bottom of Available pane).

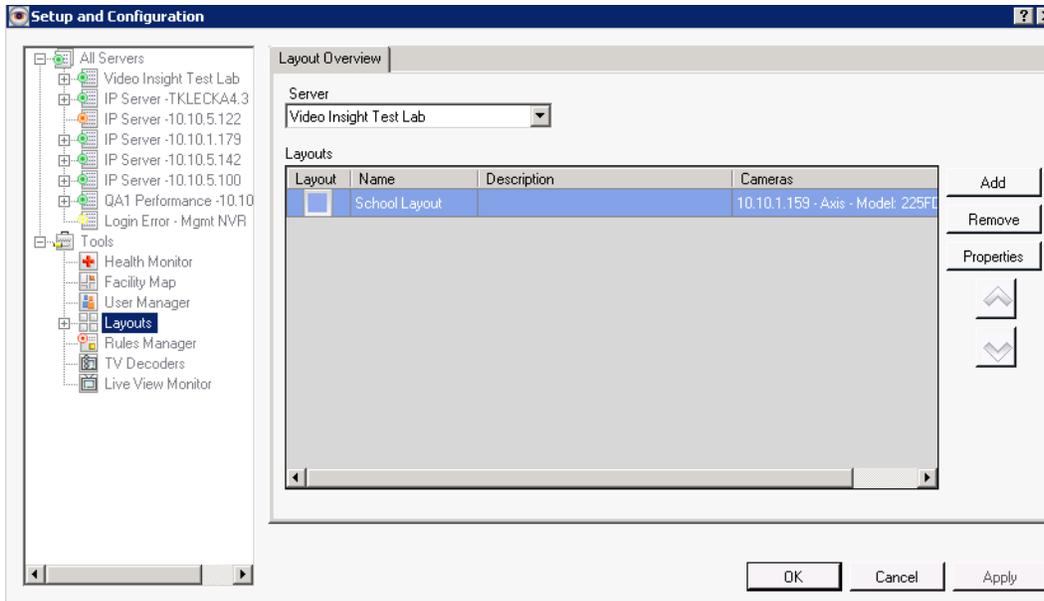


3. Enter the tour name.
4. Select the cameras the tour will cycle through, or click **Check All** to select all of them.
5. Click **OK**.
6. Click **OK**.
7. Click **Apply** and then **OK**.

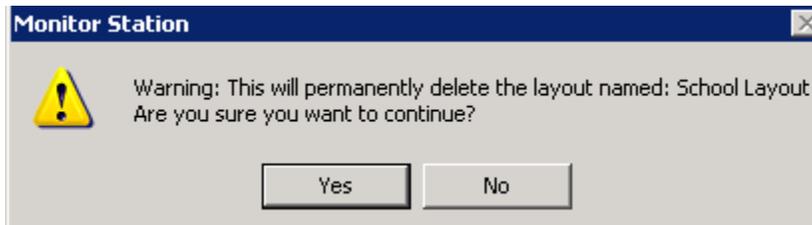
Deleting a Layout

To delete a layout:

1. Select the Layout Overview tab.



2. Select the Layout to remove from the Layouts list.
3. Click **Remove**.

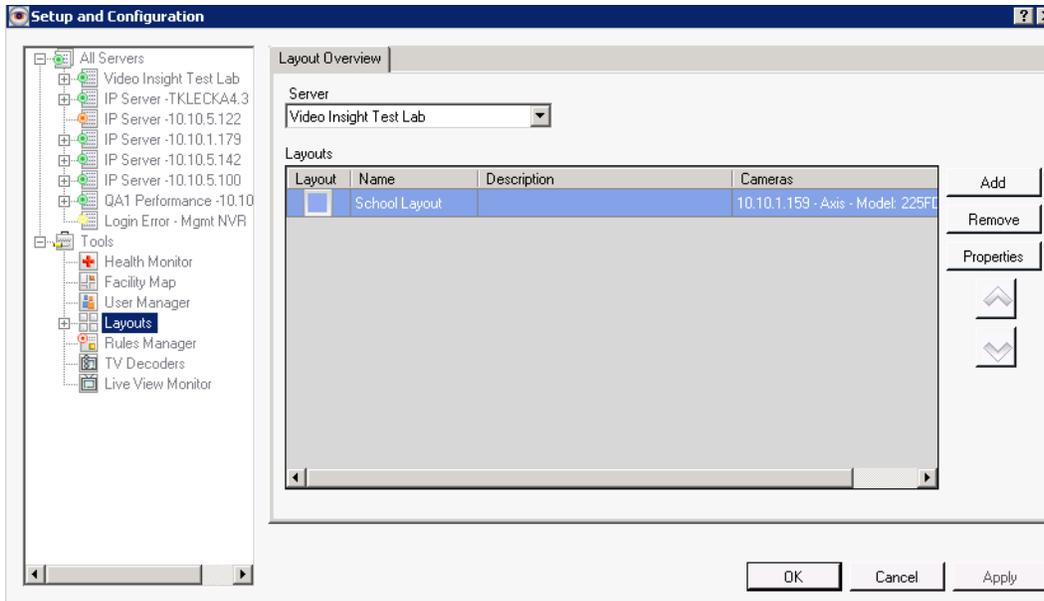


4. Click **Yes** to confirm.
5. Click **Apply** and then **OK**.

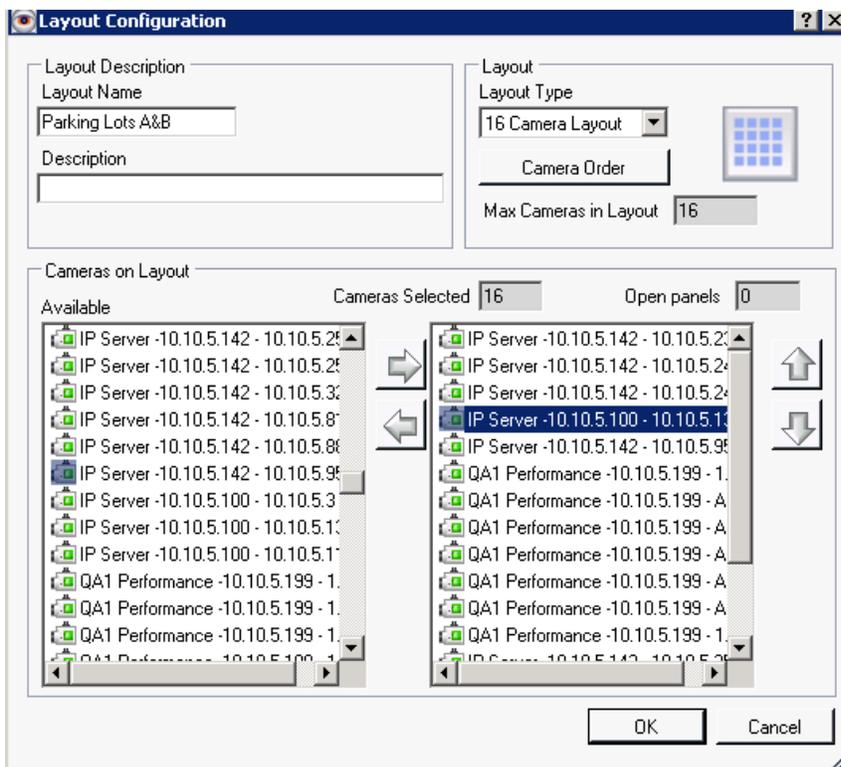
Modifying a Layout

To modify the layout:

1. Select the Layout Overview tab.



2. Select the Layout to modify from the Layouts list.
3. Click **Properties**.



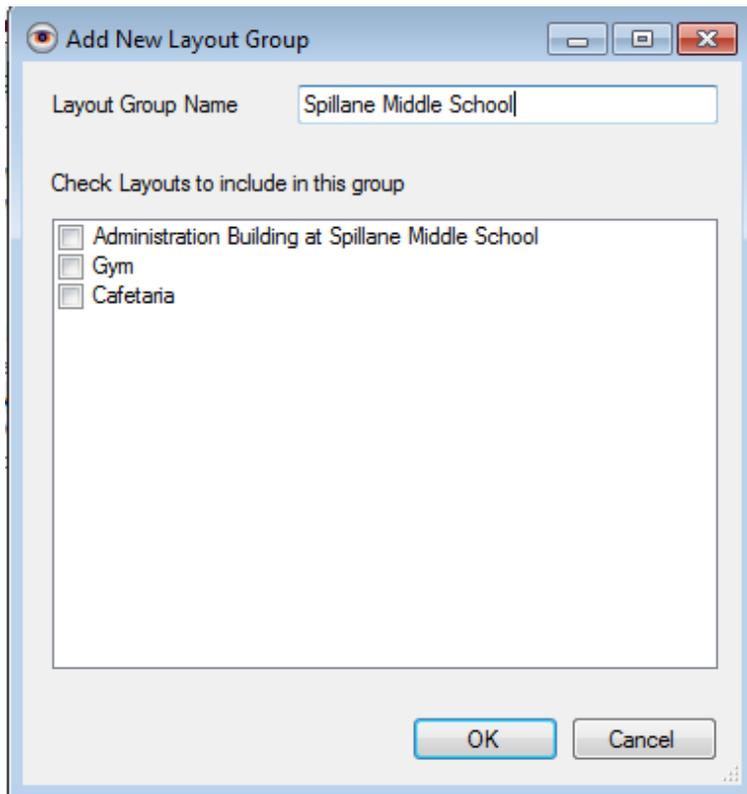
4. Modify the layout as needed.
5. Click **OK**.
6. Click **Apply** and then **OK**.

Adding Layout Groups

Layout Groups is a new feature added to Monitor Station and is visible in the Web Client. You can use Layout Groups to logically group individual layouts. This is useful when a group of sites needs to be grouped by region.

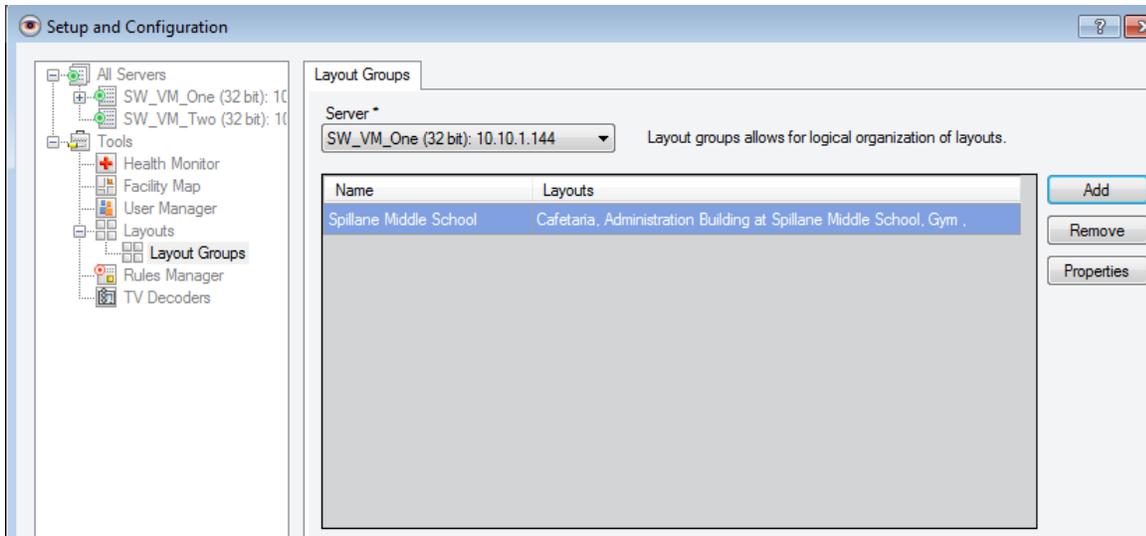
To create a Layout Group you must first have individual Layouts created for the server. See [Adding Layouts](#) for more information on Adding Layouts.

1. Click **Administration** then select Setup and Configuration.
2. Select Layouts and then Layout Groups from the left navigation tree.
3. Select the server you would like to create the Groups for from the server drop-down menu.
4. Click **Add**.
5. Enter the name for the Layout Group.
6. Select the Layouts that will be part of the group. Only Layouts created on this server will appear in the list.

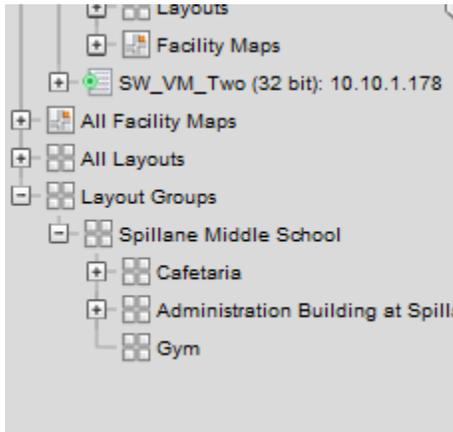


7. Click **OK**.

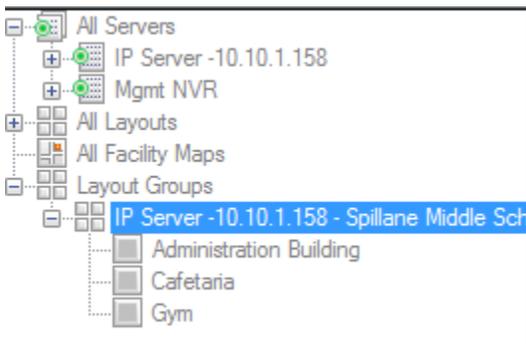
The new Layout Group displays in the Layout Groups list, as shown in the figure below.



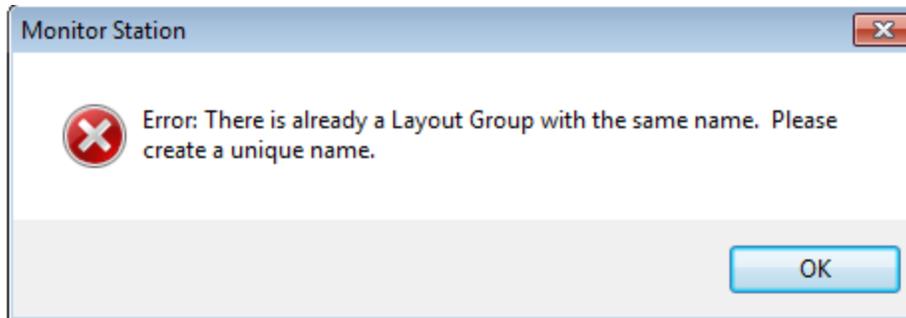
The figure below shows how a user with access to view layouts will see it on the Web Client.



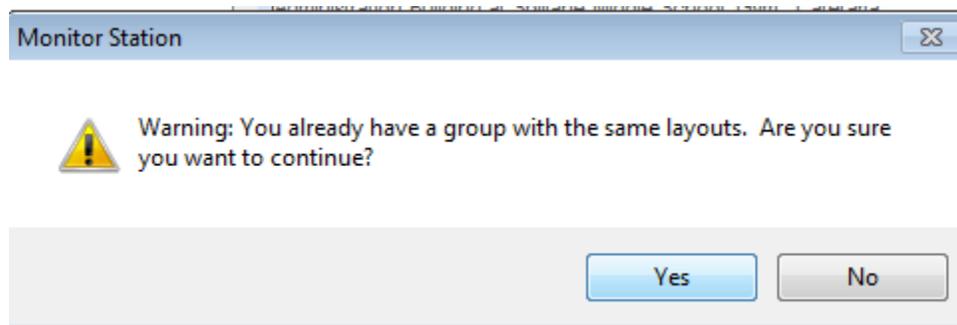
The figure below shows how a user with access to view layouts will see it on the Monitor Station.



The figure below shows the error displayed if you create a Layout Group with the same name.



The figure below shows the error displayed if you create a Layout Group with a unique name but the same layouts of an existing group. You can bypass it and create the group anyway by clicking **Yes**.



Rules Manager

Rules Manager is a configuration wizard for Comprehensive Event Triggers and Actions. You can use it to set up a simple activity such as a recording schedule or complex cause and effect relationships involving Boolean logic.

Triggers can be:

- DIO Input
- Motion Event
- Alert Button
- Scheduled
- Programmed -Remote triggers from the SDK
- LPR - License Plate Recognition
- Access Control Events

Resulting Actions include:

- Create an action event for the Video Player
- Send a digital Output on a specific port
- Audio Alert
- Email custom message
- Email video to a specified user

- Flashback - Email a picture from a specific camera. The flashback function shows thumbnails of key motion movements for that recording. Instead of showing all motion, it analyzes the motion event and shows the most relevant image.
- Live Window – Pops up a window displaying the live feed of a camera.
- Move a PTZ camera to a specific preset
- Record - Set a recording type
- Create a video file with audio
- Audio alert – This will play a sound on the monitor station
- Instant Replay – Plays the last 30 seconds of recorded video.
- Network Decoder – sends Axis camera images to the network decoder
- Record with audio – creates a file with audio included
- Switch camera or switch layout – Configuration allows you to have the monitor station change from the current layout to the one defined by this rule. You can set it up so that only a specific user can make the switch.
- Start time lapse recording
- Copy, Move or Delete Files
- Alarm Window

For example, if motion is detected or a door is opened between 12 AM to 8 AM, move the PTZ camera to a preset position and send an email.

For example, if motion is detected on Sundays, send an email and attach an AVI clip of the motion.

Rules in the Rules Manager can also be specific combinations of trigger events, schedules and resulting actions. For example, you could create a rule named Off-hour. Motion in Boy's Gym 12 AM and 6 AM moves the PTZ camera to a preset position, increases the recording frames per second and sends an email to the security chief.

Rules: Ability to Copy, Move or Delete a File

You can use Rules Manager to back-up files to another location. This new feature takes the daunting task of remembering to back-up important video recordings on a server and automates it. Using Rules Manager and File Manipulation you can also move or delete videos.

Administrator-level access is required to perform these tasks. To configure this new feature:

1. Click **Administration** and then select Setup and Configuration.
2. Select Rules Manager from the left navigation tree.
3. Enter the rule name for the task.
4. Click **Next**.
5. Schedule the time and frequency you want this rule to run.

Steps to complete the rules wizard.

Step 1:
[Enable Rule](#)
 Name and Enable or Disable the rule.

Step 2:
[Schedules \(Optional\)](#)
 Set the Time for the rule to be run.

Step 3:
[Events](#)
 Set Configure the Trigger Events.

Step 4:
[Actions](#)
 Set the list of Actions that will run when the trigger events exist.

Schedules Add a date and time for the rule to be run. It can be set to run once or on a recurring schedule.

Name _____ Type _____

Rules Wizard - Schedule

General Information

Name:

Type:

Weekly Scheduled Days

Monday Thursday Sunday

Tuesday Friday

Wednesday Saturday

Scheduled Time

Start:

End:

OK Cancel

6. Click **Next**.
7. Click **Next** to bypass the type of Event screen this rule should trigger.
8. Double-click File Manipulation from the Available Actions list.

Rules Wizard

Steps to complete the rules wizard.

Step 1:
[Enable Rule](#)
 Name and Enable or Disable the rule.

Step 2:
[Schedules \(Optional\)](#)
 Set the Time for the rule to be run.

Step 3:
[Events](#)
 Set Configure the Trigger Events.

Step 4:
[Actions](#)

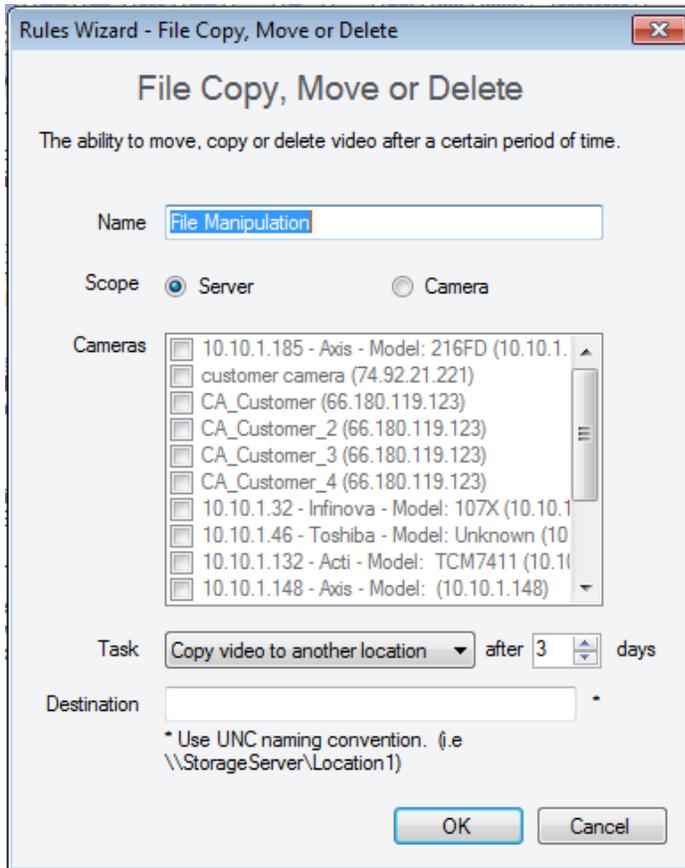
Actions Configure the actions that occur when the condition is triggered.

Available Actions

Type	Description
Digital Output	Send a digital output on a specific port
Email	Email custom message
Email Avi Clip	Email video to a specified user
Email Flashback Image	Email Flashback Image
File Manipulation	Copy, Move or Delete files
Instant Replay	Pop up a 30 second review window of a camera

Add

Selected Actions



9. Enter the rule name.
10. Choose the scope of this rule. If Server is selected, all of the files for all of the cameras will be included. If Camera is selected, only the files for the checked cameras will be included.
11. Select the Task type: Copy, Move or Delete. You can create multiple rules to manage multiple cameras and server configurations. For example, you could create a rule to copy some camera's videos, delete others and move the rest.
12. Select the number of days, with a minimum of one day and a maximum of 999. The number selected reflects the most current days to keep; for example, if three is selected it will move, copy or delete all files older than three days.
13. Select the Destination folder. It can be a local folder or shared location. The folder must already exist for the task to complete successfully.

TV decoders

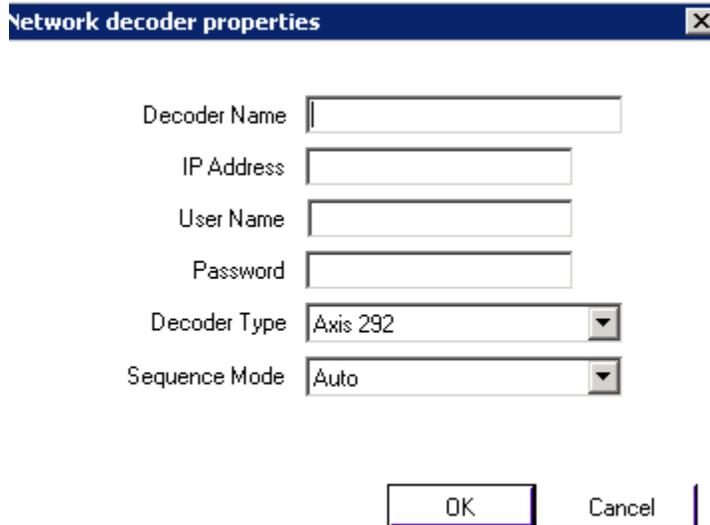
Adding a decoder

You can output system video to a television monitor. To output to a television you must add a TV decoder.

Note

Video Insight supports Axis 292 and P7701 decoders.

1. Click **Administration** and then select Setup and Configuration.
2. Select TV Decoders from the left navigation tree.
3. Select the server to add the decoder to from the drop-down menu.
4. Click **Add**.



Network decoder properties [X]

Decoder Name

IP Address

User Name

Password

Decoder Type

Sequence Mode

5. Enter a decoder name.
6. Enter the IP address of the decoding device.
7. Enter the user name and password for the decoding device.
8. Select the Decoder Type.
9. Select the Sequence mode.
10. Click **OK**.

Deleting a decoder

1. Click **Administration** and then select Setup and Configuration.
2. Select TV Decoders from the left navigation tree.
3. Select the server to delete the decoder from the drop-down menu.
4. Select the Decoder from the list.
5. Click **Remove**.
6. Click **Apply** and then **OK**.

Modifying a decoder

1. Click **Administration** and then select Setup and Configuration.
2. Select TV Decoders from the left navigation tree.

3. Select the server to modify a decoder on from the server drop-down menu.
4. Select the Decoder from the list.
5. Click **Properties**.
6. Make changes as necessary and then click **OK**.
7. Click **Apply** and then **OK**.

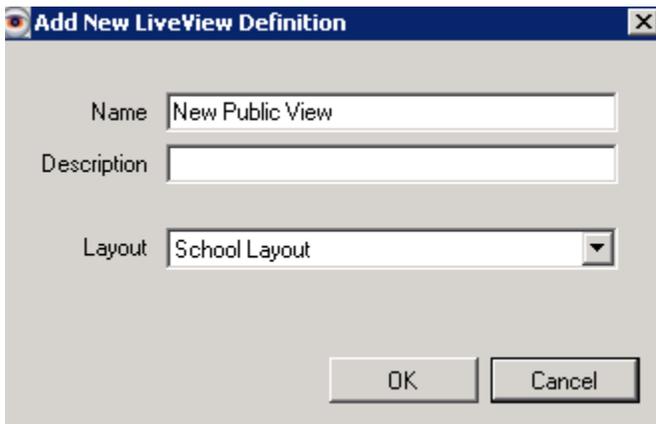
Live View Monitor

Live View Monitor is an extension application used in conjunction with IP Server and Monitor Station to output control of live images displayed on walls of televisions.

You must have existing Layouts on the server before you can configure Live View Monitor.

Adding a Live View

1. Click **Administration** and then select Setup and Configuration.
2. Select Live View Monitor from the left navigation tree.
3. Select the server to add the Live View Layout to from the server drop-down menu.
4. Click **Add**.



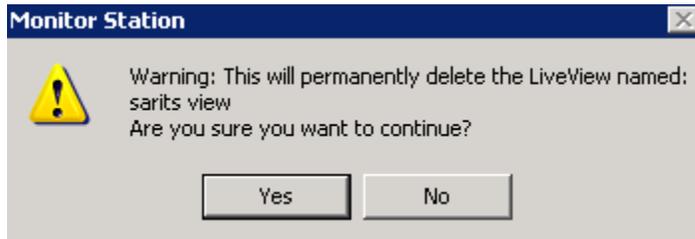
The screenshot shows a dialog box titled "Add New LiveView Definition". It has a standard Windows-style title bar with a close button (X). The dialog contains three input fields: "Name" with the text "New Public View", "Description" which is empty, and "Layout" with a dropdown menu showing "School Layout". At the bottom of the dialog are two buttons: "OK" and "Cancel".

5. Enter a definition name.
6. Add an optional description.
7. Select the layout from the drop-down menu.
8. Click **OK**.
9. Click **Apply** and then **OK**.

Deleting a Live View

1. Click **Administration** and then select Setup and Configuration.
2. Select Live View Monitor from the left navigation tree.
3. Select the server to delete the Live View Layout from the server drop-down menu.

4. Select the layout to delete from the list.
5. Click **Remove**.



6. Click **Yes**.
7. Click **OK**.
8. Click **Apply** and then **OK**.

Modifying a Live View

1. Click **Administration** and then select Setup and Configuration.
2. Select Live View Monitor from the left navigation tree.
3. Select the server to modify the layout from the server drop-down menu.
4. Select the layout to modify.
5. Click **Properties**.
6. Make changes as necessary and then click **OK**.
7. Click **Apply** and then **OK**.

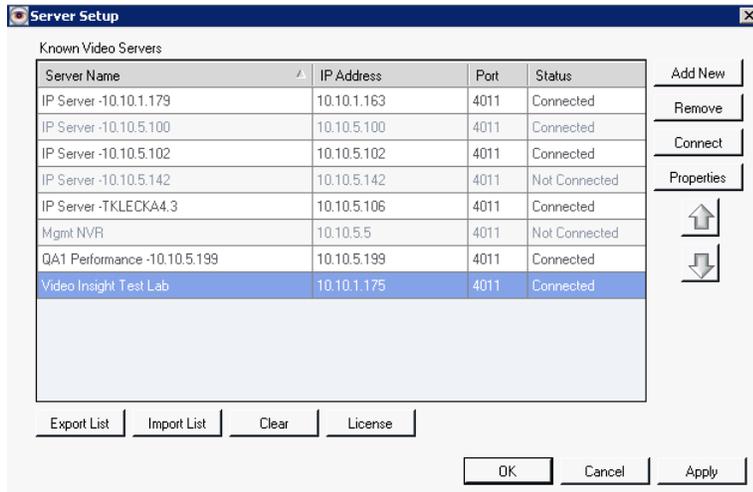
Left navigation tree

The left navigation tree is a core functionality area for most user operations. There are three possible views of the left navigation tree:

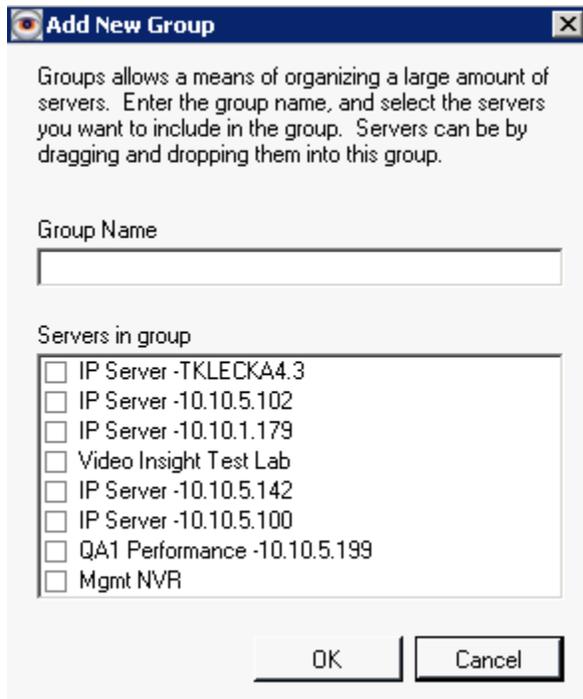
-  [Enterprise View \(default\)](#)
-  [Facility Map View](#)
-  [Layout View](#)

Enterprise View

Add/Remove Server: Select this option to show the Add/Remove Server dialog. See Adding servers manually for more information on adding and removing a server.

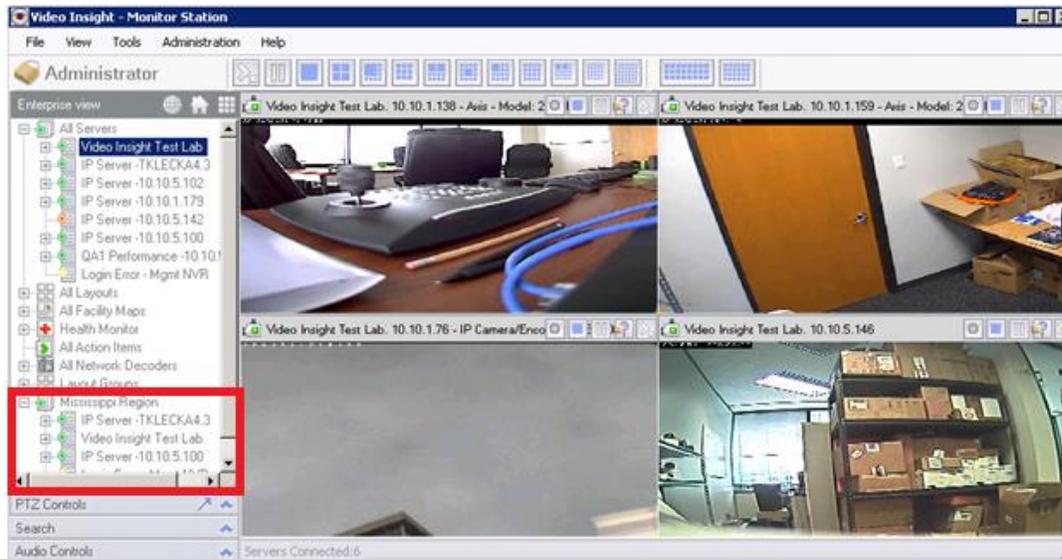


Add Group: Select this option to add server groups. This is useful when organizing server locations by logical groups such as region in Monitor Station.



1. Enter a group name.
2. Check the servers that will be added to the group.
3. Click **OK**.

The figure below shows the newly added group:



There are three possible states for a server in the left navigation tree:

The left navigation tree displays a status color for each server:

-  = Server is connected and settings may be modified
-  = Server is not connected due to a login error. It will continue to record video to the specified location; however, modifications to settings using MS or IPSM are not allowed
-  = Server is not connected, possible due to a stopped service or a problem with the connection properties; confirm the IP address and port

Selecting a server from the left navigation tree displays the server's properties. Administrator rights are required to modify them. See Server Customization for more information on each field and tab.

 = Server is functioning properly: streaming video to clients, recording video and reporting to Health Monitor (if applicable).

 = Server is stopped and is NOT recording or streaming video.

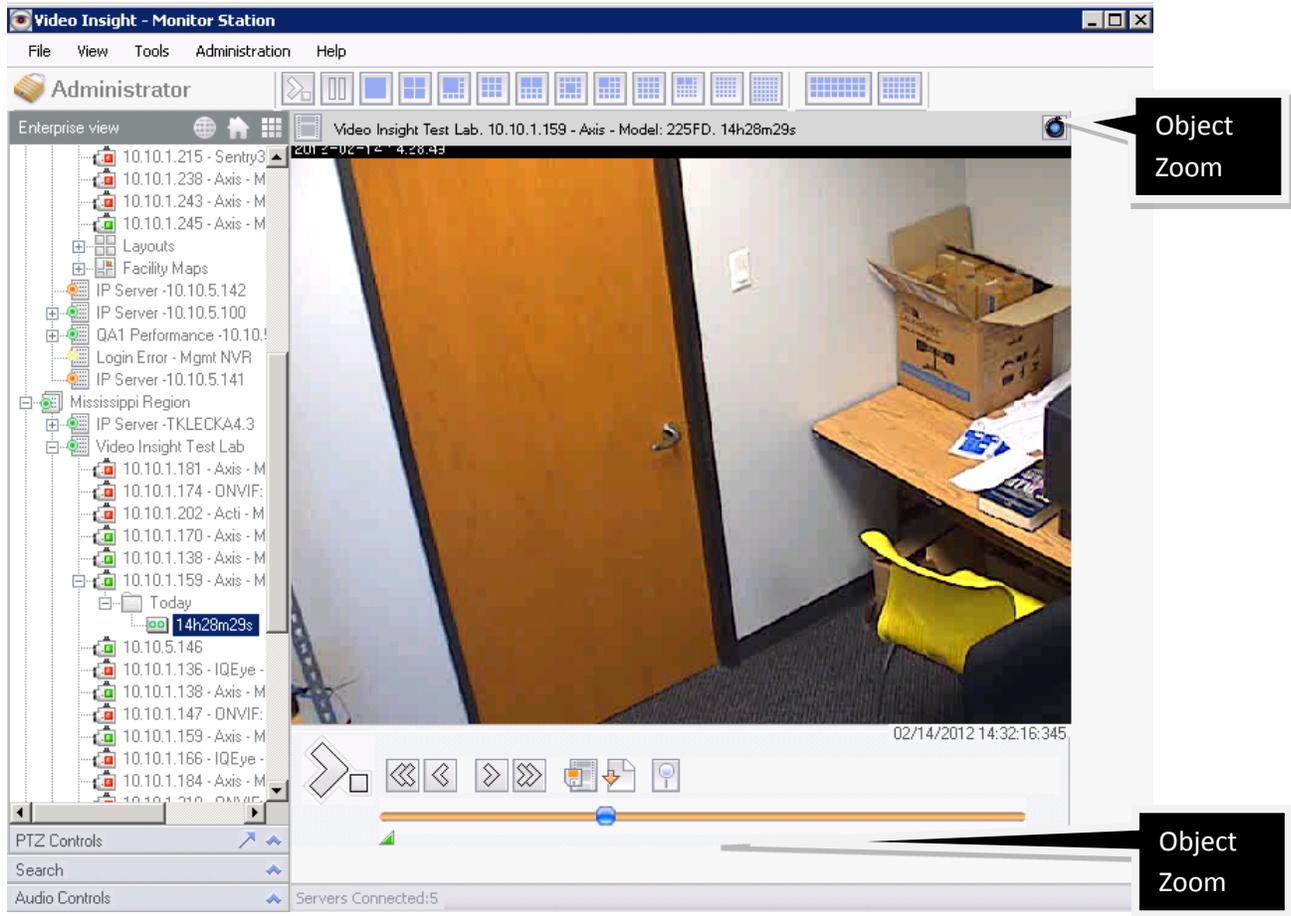
 = Login Error: The server is found but security is on and the server attempted to authenticate with default credentials (Administrator/blank). Log out and log in to Monitor Station with appropriate credentials.

You can use the Enterprise view to view recorded videos if such access has been granted to the user.

To view recorded video double-click a camera in the left navigation tree. You may see several folders depending on the archiving settings configured for the server and the storage reserve space requirements. See [Media Player](#) for more information on accessing video on long-term storage.

You have several options when viewing recorded video from the Enterprise view.

1. Click the camera to list the video folders.



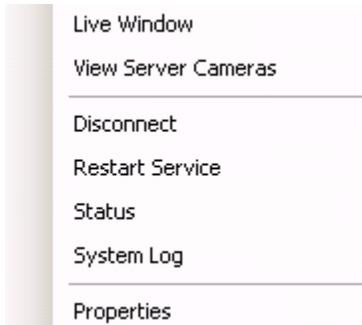
2. Click the file to play.
3. You can pause, stop or fast forwards or backward using the control buttons. You can also move one frame forward or backwards using the control buttons.
4. You can use the slider control to jump to a specific point in the video. The bottom right corner of the playback window displays time and date information.
5. You can also [download a video](#) or [create a clip](#) for distribution.

You can access the properties of any of node by right-clicking it.

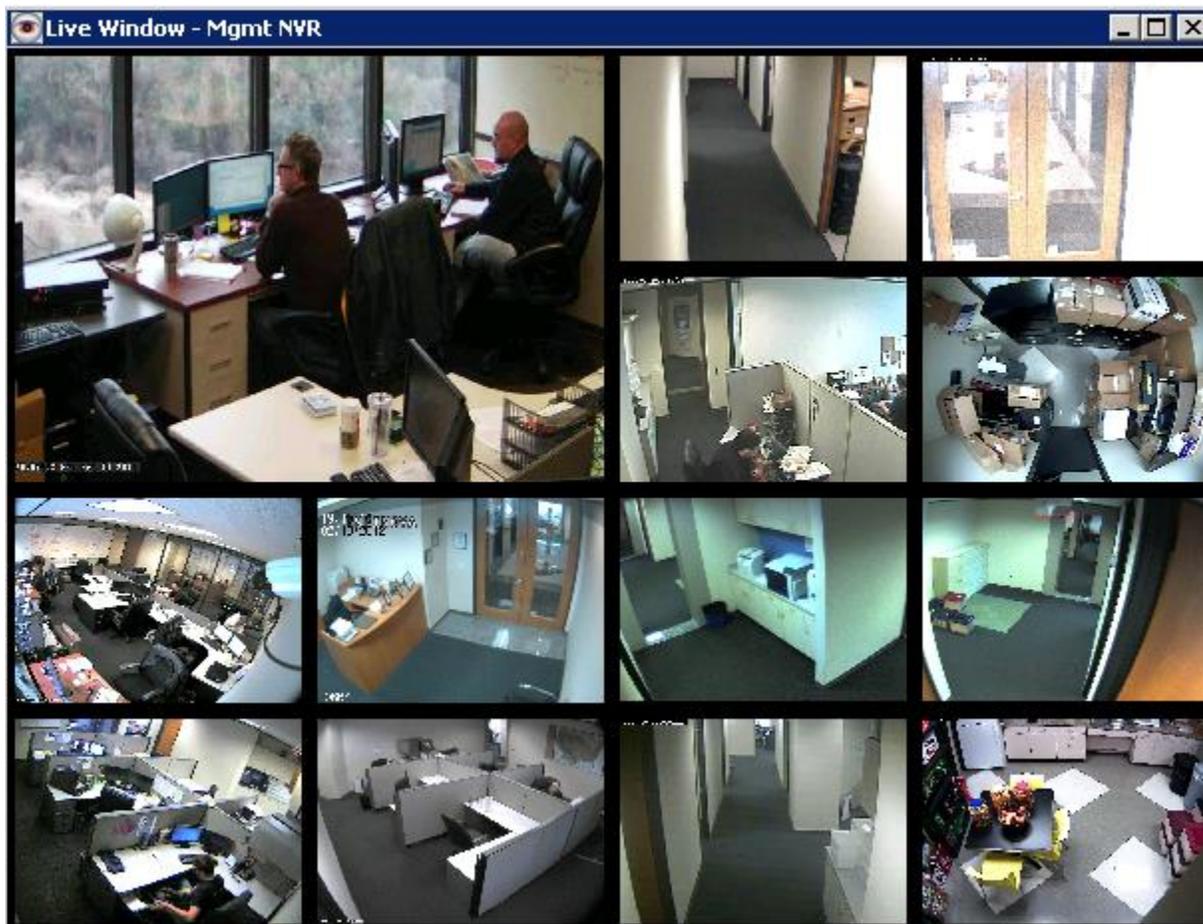
Contextual right-click menu

You can access the contextual menu for Servers and Server Groups by using a right click.

1. Right-click the server node.



Live Window: Selecting Live Window displays a window with all of the server's cameras as shown in the figure below.



View Server Cameras: Selecting this option has the same effect as if clicking the server node. All of the server's cameras will appear in the main viewable area.

Disconnect: Select this option to disconnect the server. Cameras will no longer stream to the local Monitor Station. You can reconnect the server using a right click.

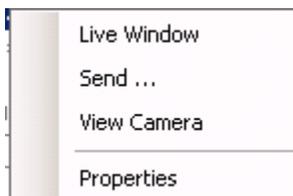
Restart Service: Select this option to restart the server service. IPSM must be running for the server to accept the request from the client. If IPSM is not running at the time of the request it will restart the next time it is launched.

Status: Select this option to bring up the Server Statistics dialog box. See Server statistics for more information on server status.

System Log: Select this option to display the system log. See System log for more information on the system log.

Properties: Selecting this option displays server properties. See IP Server customization for more information on server properties.

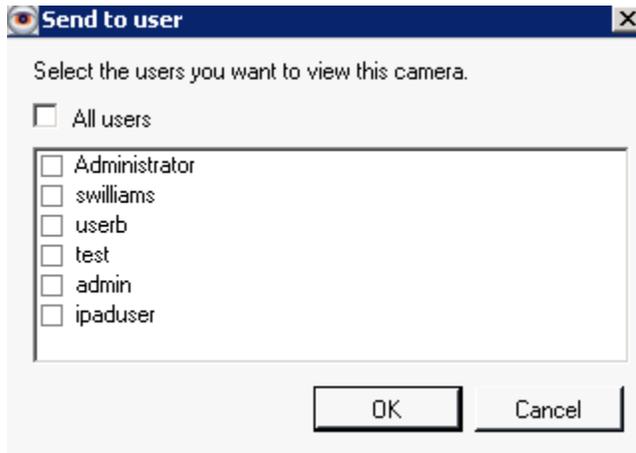
You can access the contextual menu for Cameras by using a right click.



Live Window: Select this option to display a Live Window dialog box with the selected camera's view as shown in the figure below.



Send: Select this option to display a dialog box to select users to send the image to.



Once sent, the same live window will appear on the user's Monitor Station, unless they have pop-ups blocked.

View Camera: Select this option to bring the camera into focus in a one camera layout in the main viewable area.

Properties: Select this option to change camera settings. See Modifying camera details for more information on camera settings.

For Layout:

Right-click the specific Layout node



Live Window: Selecting Live Window will display a pop-up with the using the selected Layout, as shown in the figure below.



View Layout: Select this option to bring the selected Layout into focus in the main viewable area.

Properties: Select this option to change Layout settings, including adding and removing cameras. See [Modifying a Layout](#) for more information on configuring layouts.

For Facility Map

Right-click the specific Facility Map node.

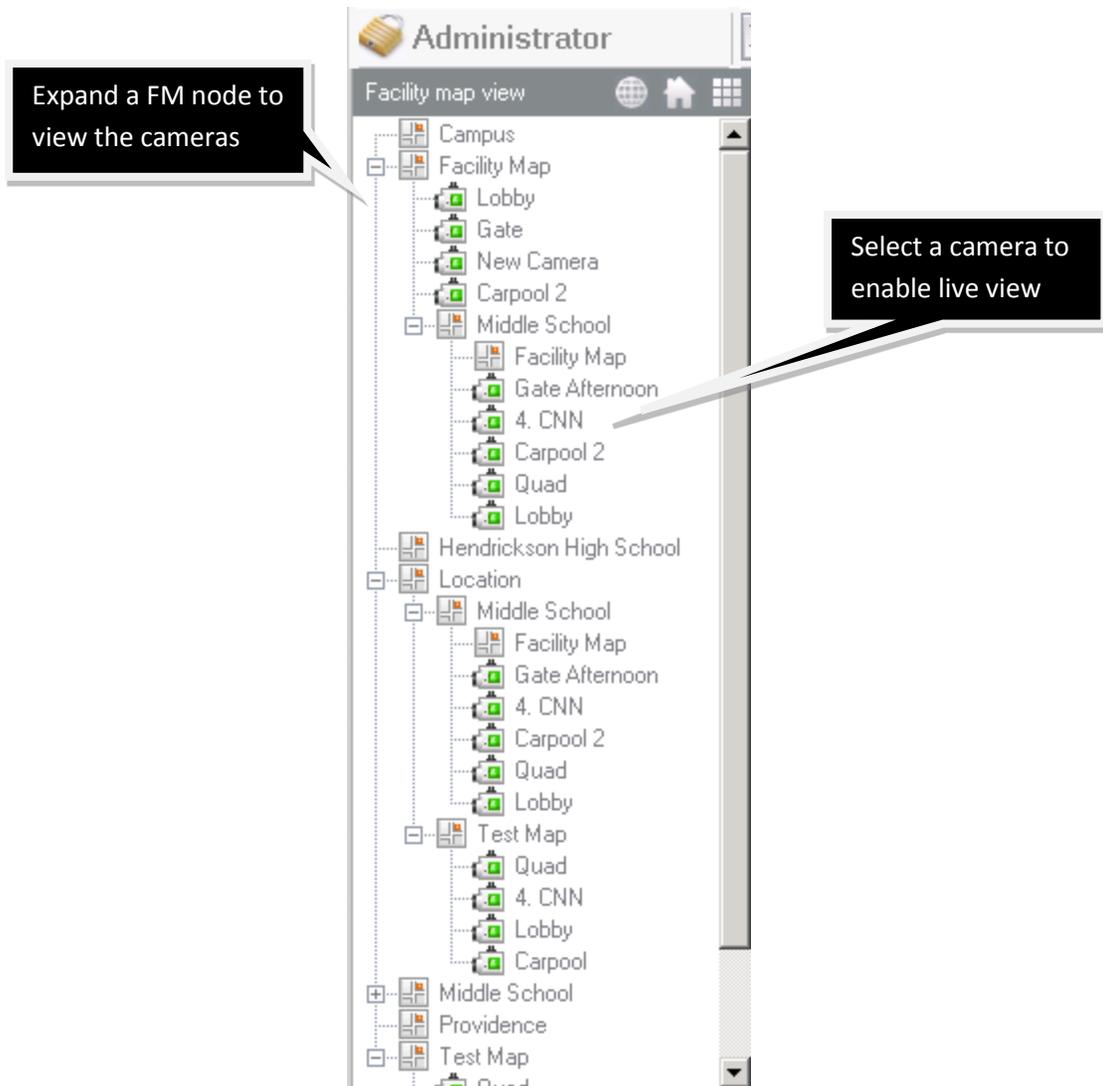


View Map: Selecting this option brings the selected map into focus in the main viewable area as an integrated map (if that option is selected) or as a pop-up.

View cameras: Selecting this option brings the selected cameras overlaid on the map as a layout into focus in the main viewable area.

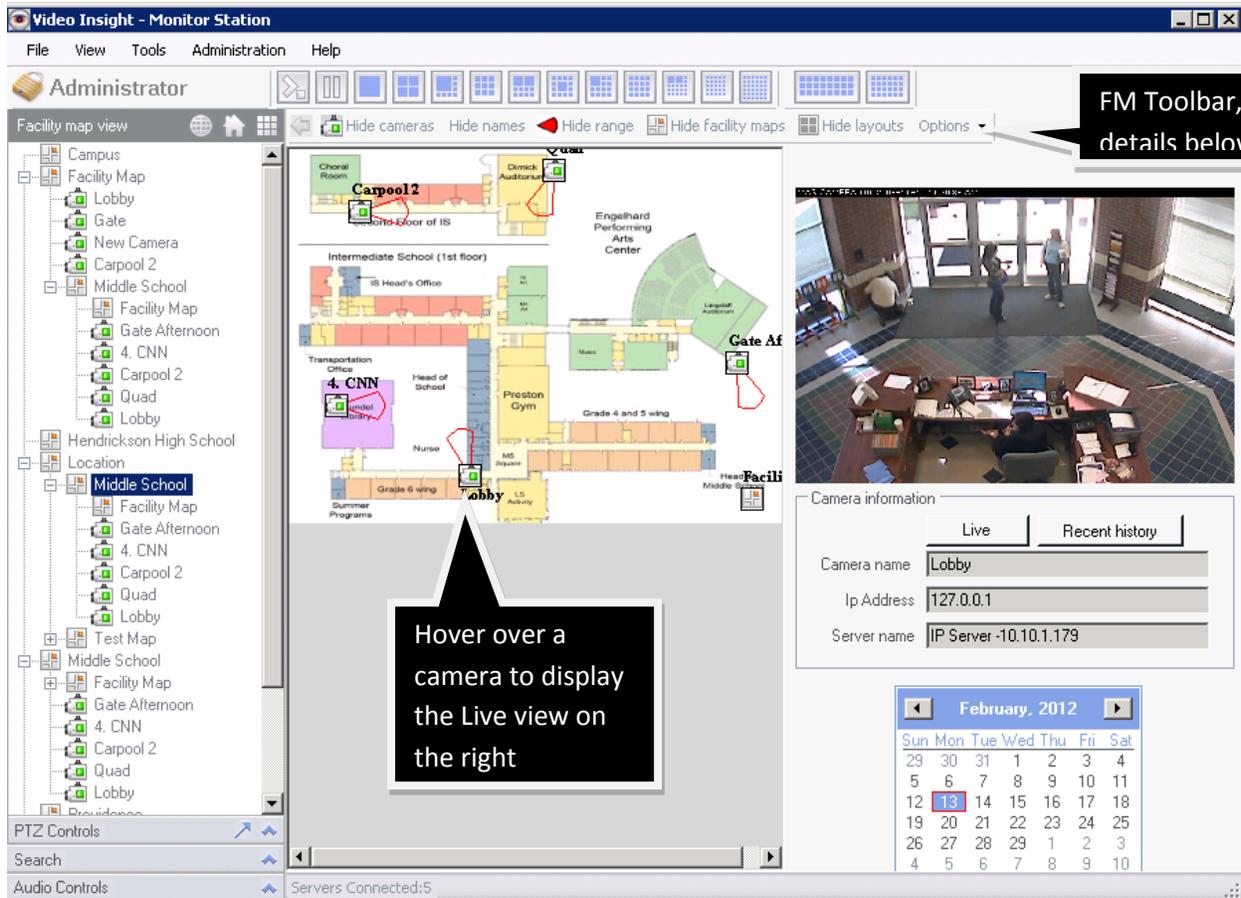
Properties: Selecting this option displays the Facility map setup pop-up to change its settings, including adding and removing cameras. See [Facility Maps](#) for more information on facility maps.

Facility Map View



You can view and manage surveillance operations using the Facility Map view instead of the main live view. This is useful from a tactical stand point as you will know the location of each camera and their viewable area aids security personnel.

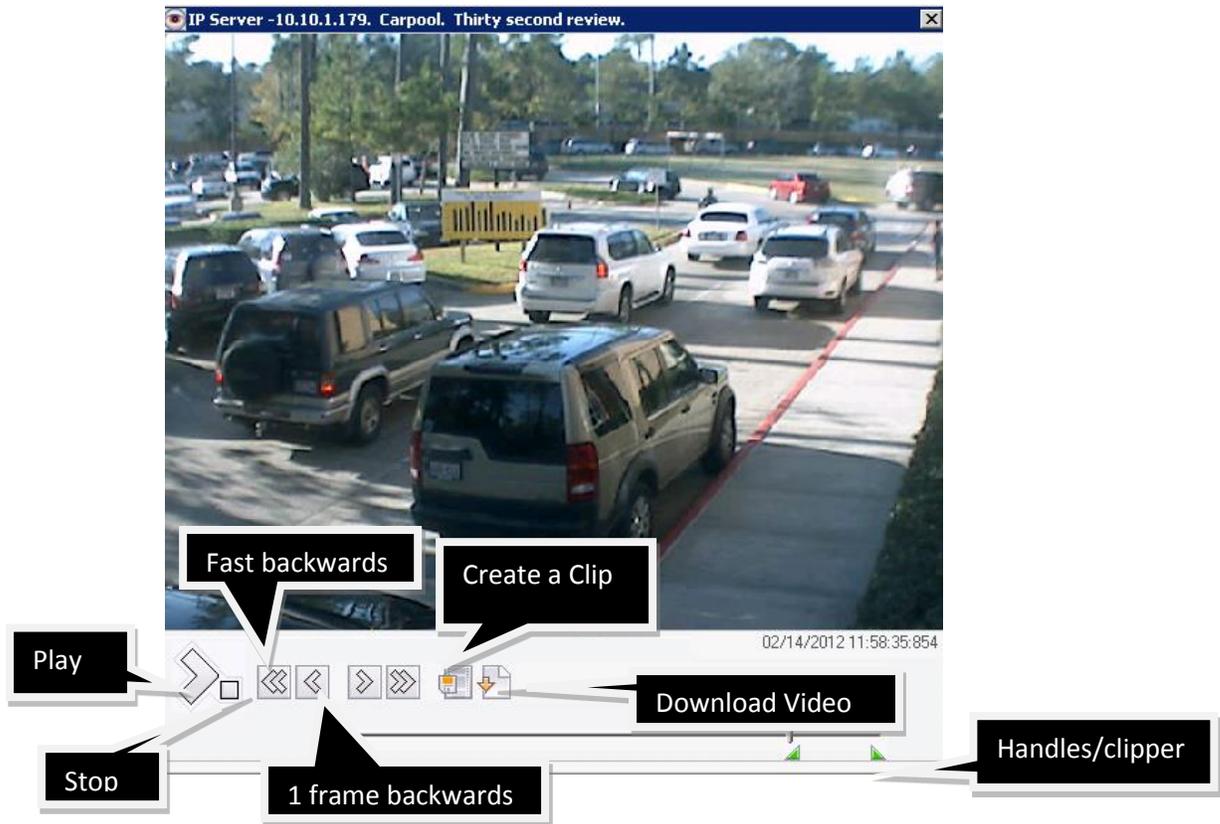
You can view a Facility Map by clicking the desired node, as shown in the figure below.



You can perform several actions on this screen.

Live: Click this button to display a live pop-up window.

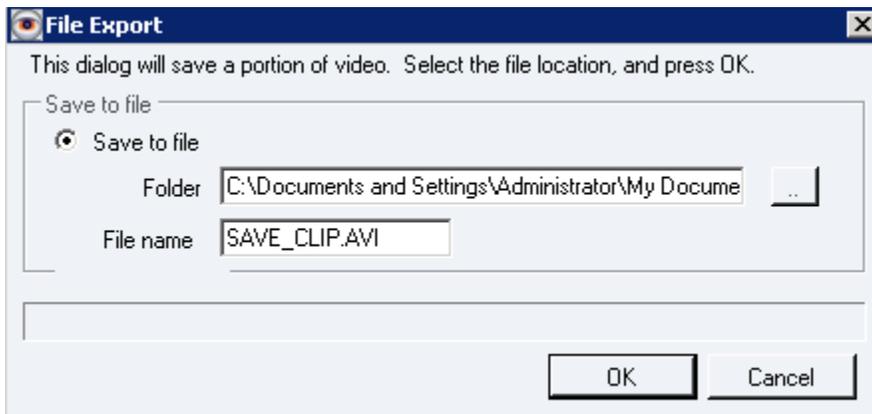
Recent history: Click this button to display a 30 Second Review pop-up with the most recent history from the day selected on the calendar.



You can create a clip from the 30 Second Review pop-up.

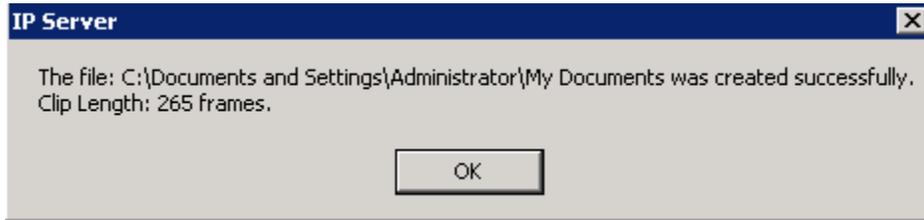
Creating a clip

1. Use the green symbols to bracket the desired clip.
2. Click **Create a Clip**.



3. Browse to the desired save location or enter the path.

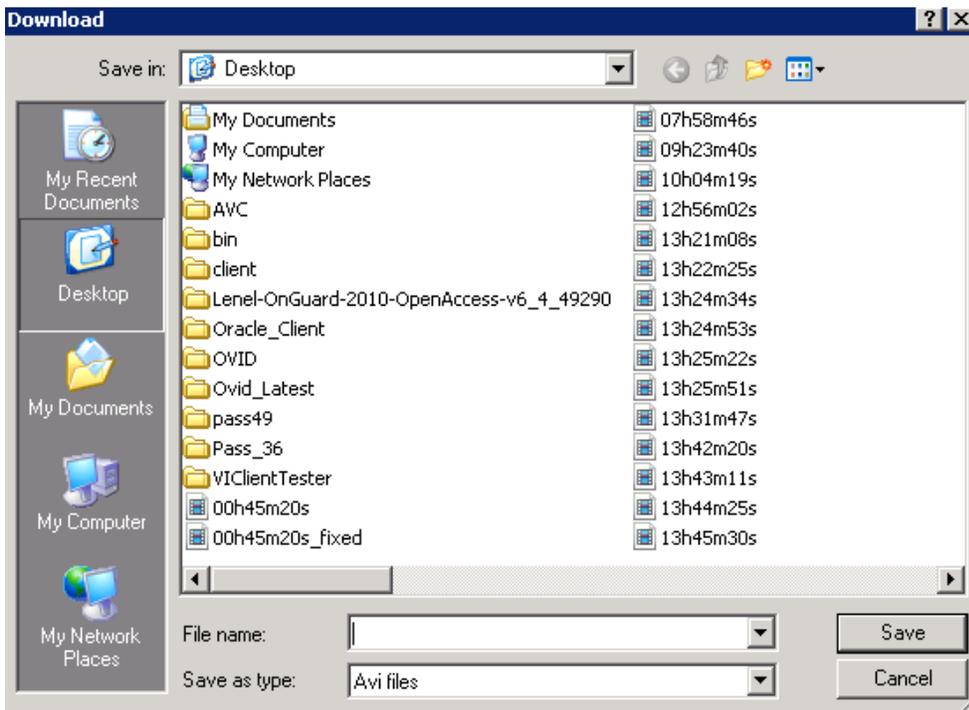
4. Enter the clip name or accept the default and then click **OK**.



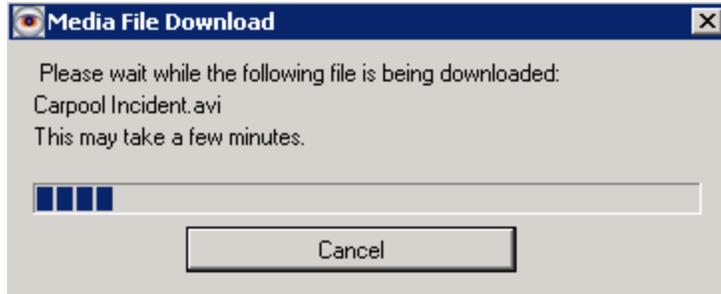
5. After the file is saved a notification pop-up displays the clip length. Click **OK**.

Downloading a recorded file

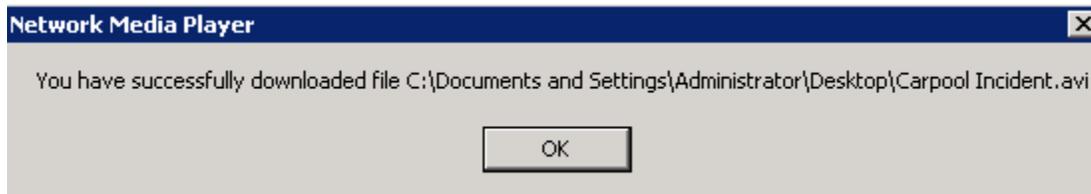
1. To save a recorded file, click **Download Video**.



2. Select the save location and enter the file name.
3. Click **Save**.



4. A notification pop-up displays download progress.



5. Click **OK**.

Facility Map toolbar

You can use the Facility Map Toolbar to further customize the Facility map view and behavior.



 = Facility Maps can have cameras as well as other Facility Maps overlaid additional terrain detail. Use the back button to return from a sub map to the prior view.

 = Clicking this hides the camera icon used to designate a camera on the map.

Hide names = Clicking this hides the camera names that may obstruct the terrain view.

 = Clicking this hides the viewable cone icon on the map.

 = Clicking this hides sub facility maps on the current map.

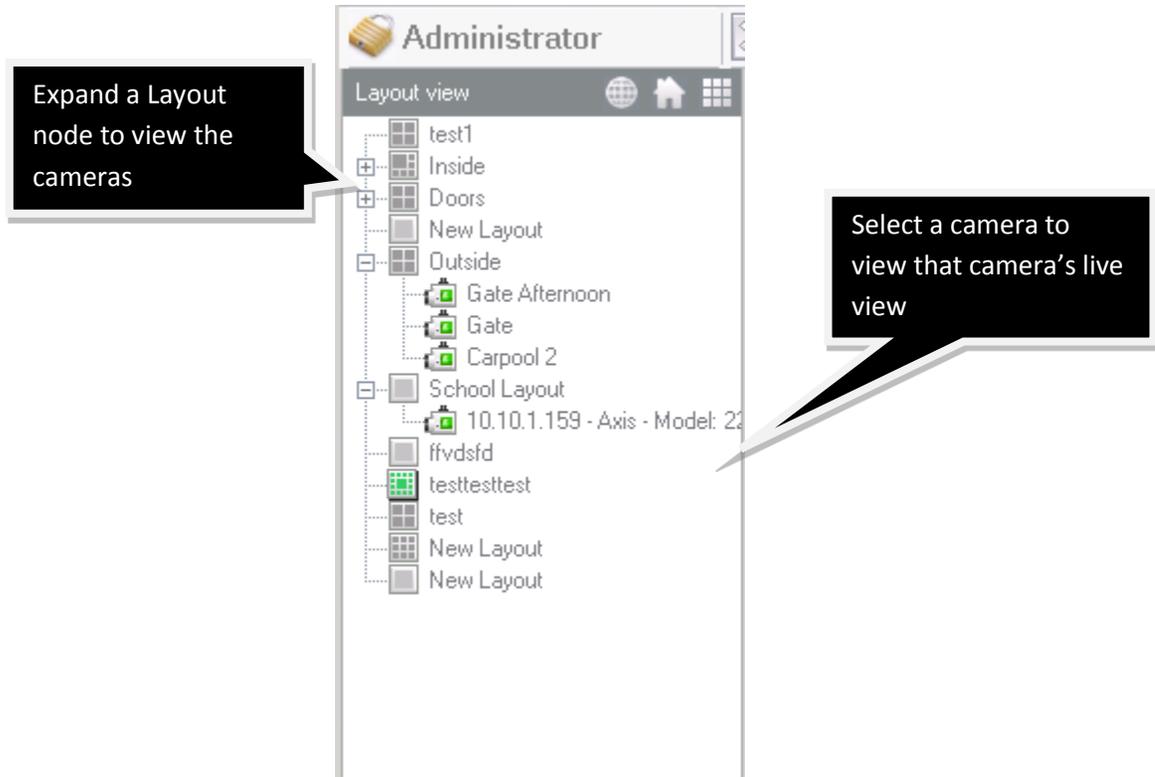
 = Clicking this hides layouts on the current map.

Options ▾ = Clicking this displays the following menu:

Change Font...
Hide Zoom Bar
Change font color

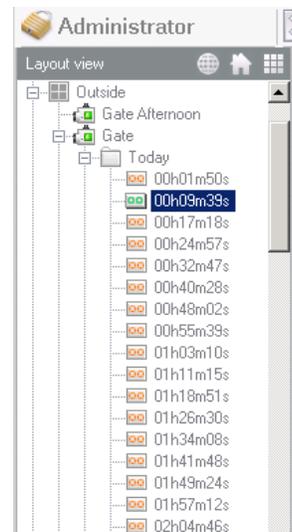
From this menu you can change the camera name font and the font color. You can also hide the Zoom bar that is located at the bottom right of the screen.

Layout View



You can view a Layout by clicking the desired node. The selected layout displays in the main view area. You can also right-click a Layout and display the contextual right-click menu. See Contextual right-click menu for more information on this menu.

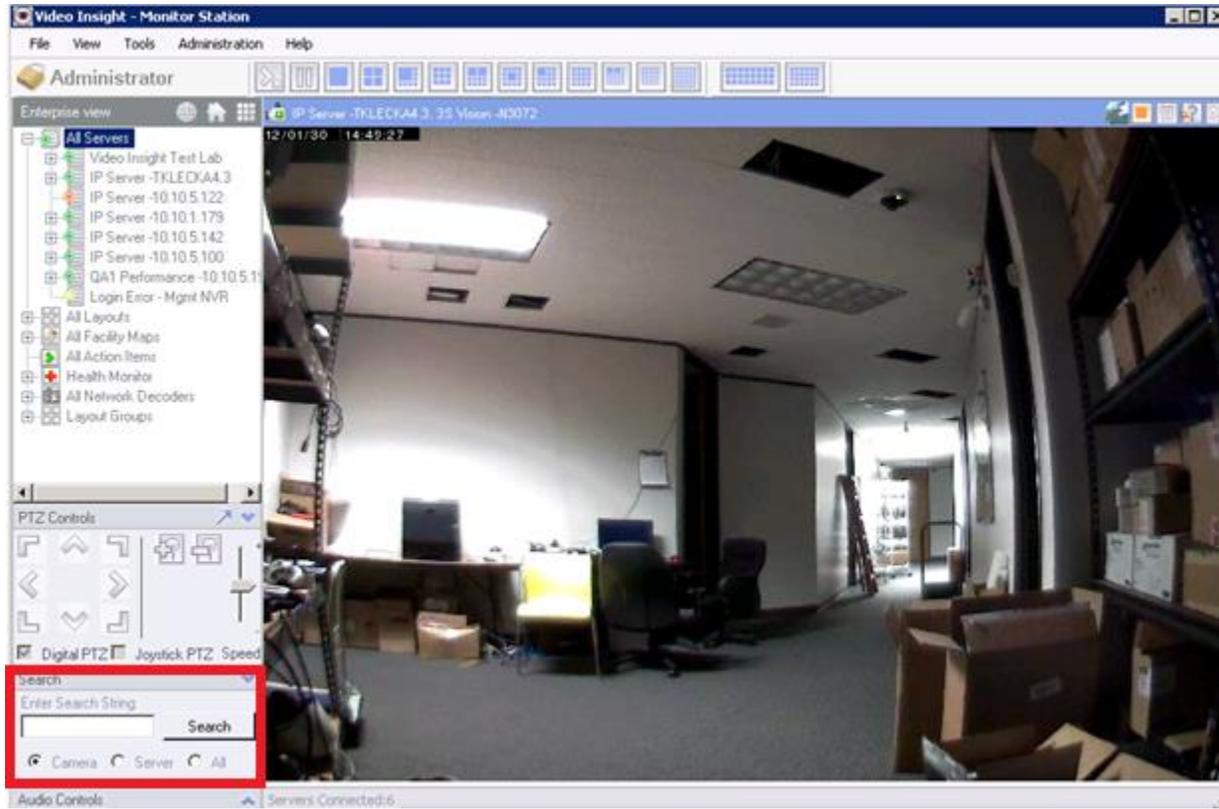
You can view recorded video by double-clicking a camera to expand the recorded video folders.



PTZ Controls pane

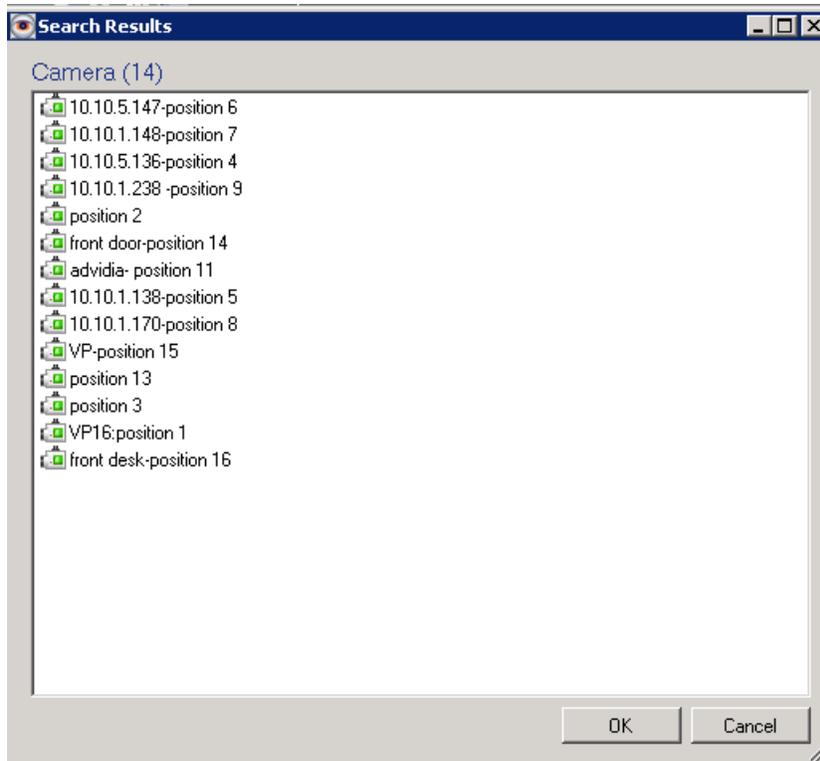
See [PTZ controls](#) for more information.

Search pane



You can use the Search box in the left navigation tree to find a camera, server or anything with a matching string.

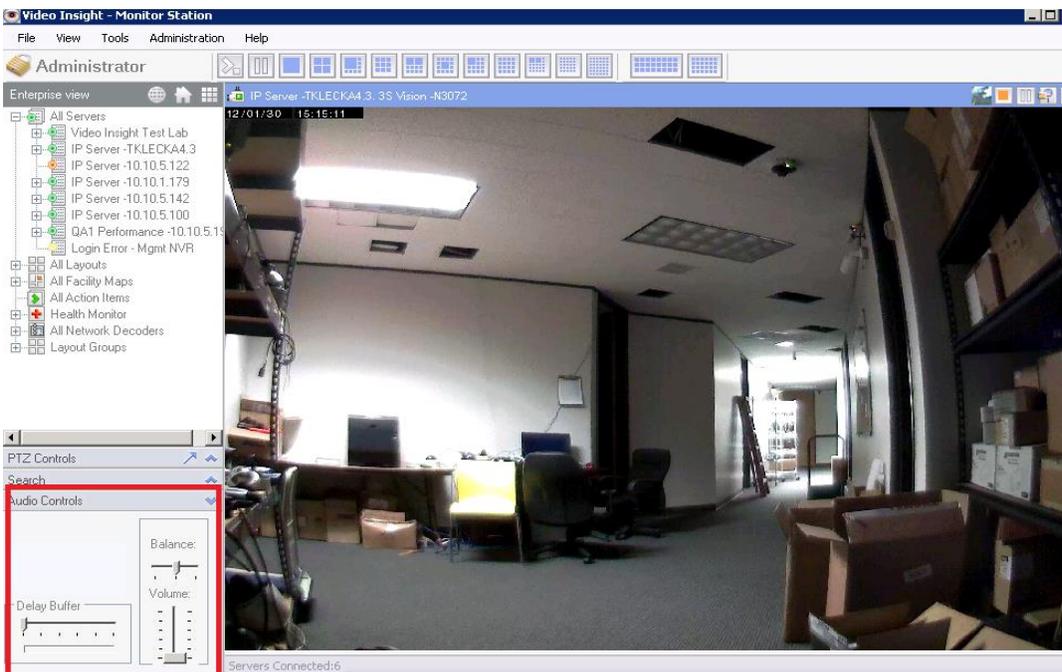
The search result displays all matches. For example, if multiple cameras use “pos” in their name the search result will look like the figure below.



Double-click the camera of your choice or highlight it and then click **OK**. The selected camera is highlighted in the left navigation tree.

Searching for a camera by its IP address searches the IP field instead of the camera name.

Live Audio Controls pane



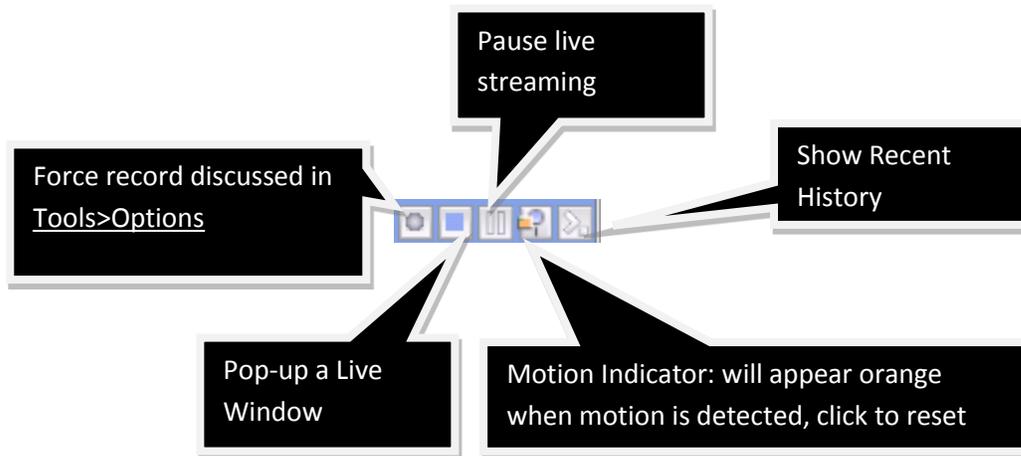
You can use the Audio Controls pane to control the speaker's volume, balance and buffering. Live Audio must be selected and supported by the camera.

Layouts toolbar

See [Cycle Layouts](#) for more information on the layout toolbar.

Quick Access toolbar

The camera's Quick Access toolbar includes display information and several shortcut buttons.

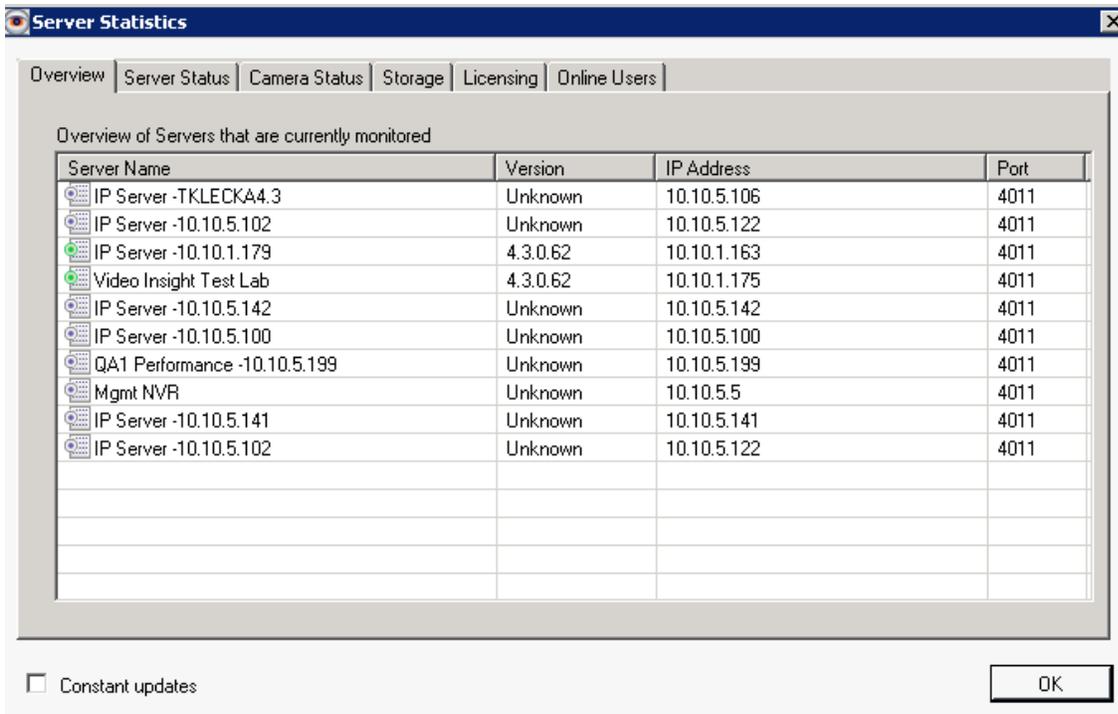


Server statistics

Administrators can use the Server Statistics sub menu to manage all servers, review server and camera status, as well as manage storage, licensing and online users.

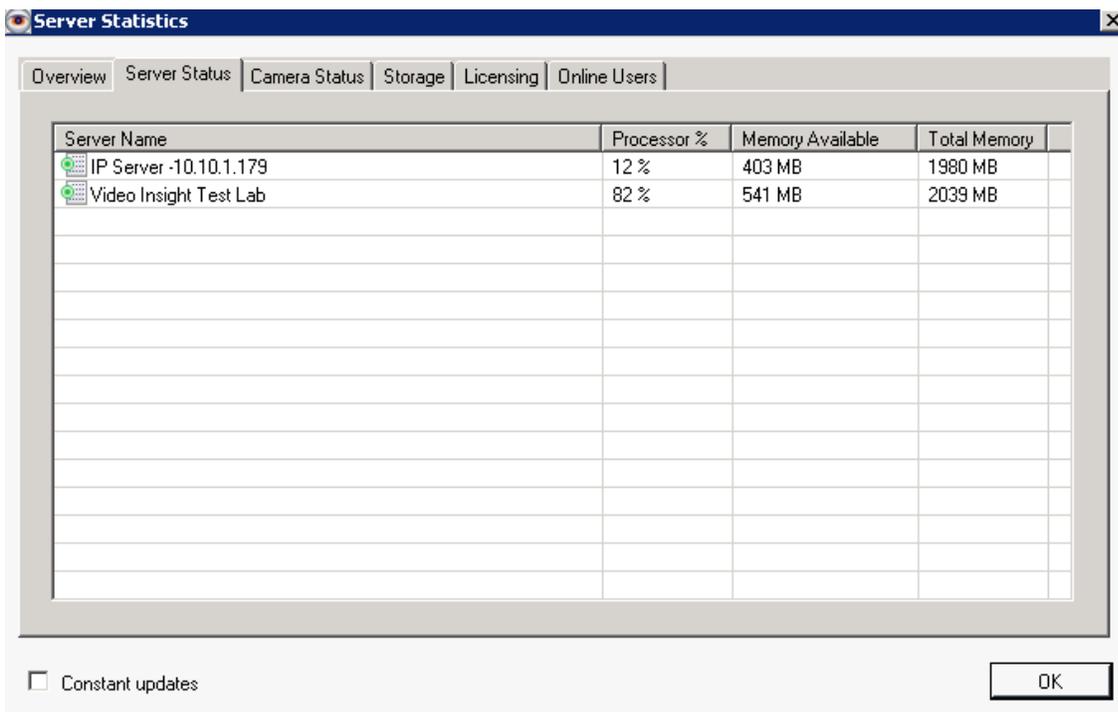
Overview tab

The Overview tab displays all servers that have been added to the Monitor Station. The tab lists the server name, software version, IP address and the port used for that service. If a server is offline or security is on and incorrect credentials have been used the tab displays the software version as Unknown.



Server Status tab

The Server Status tab displays all servers and their current processor usage percentage, memory available to the IP service and total memory available on the server. To have the values automatically refreshed for servers running version 4.3 or later, check the box for Constant updates.

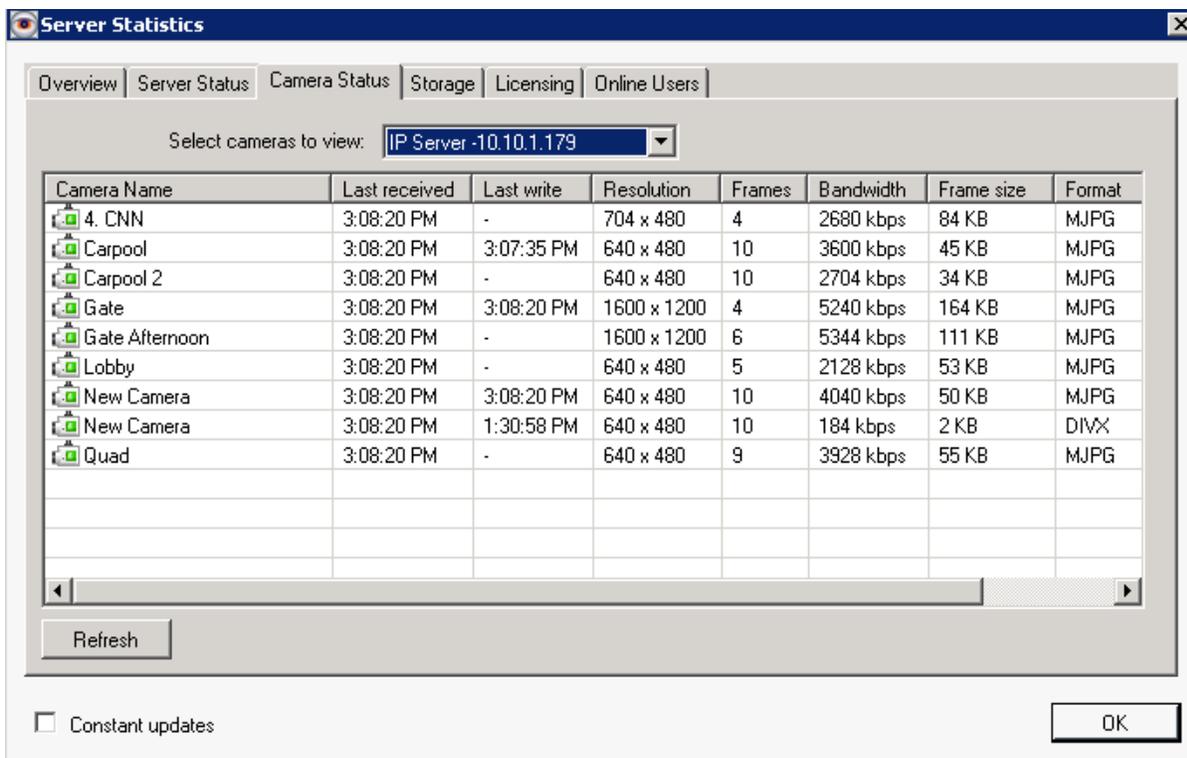


Camera Status tab

The Camera Status tab displays the camera name, the last received communication from the server, the resolution being used, the number of frames per second, the bandwidth, frame size and the format.

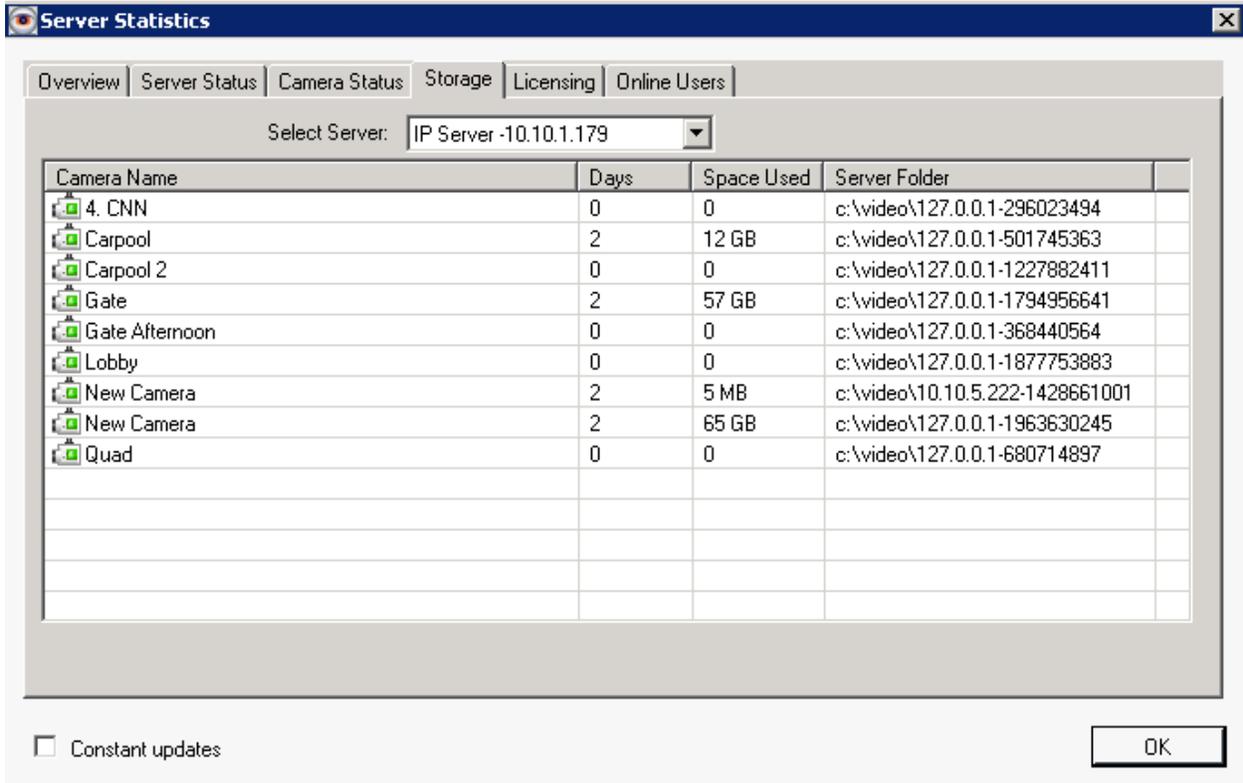
The Format displays unknown if no connection to the camera has been made recently. Cameras attached to a server running Video Insight software earlier than version 4.3 will display most information as 0 or unknown.

You can filter the camera list by server from the drop-down menu, as shown in the figure below.



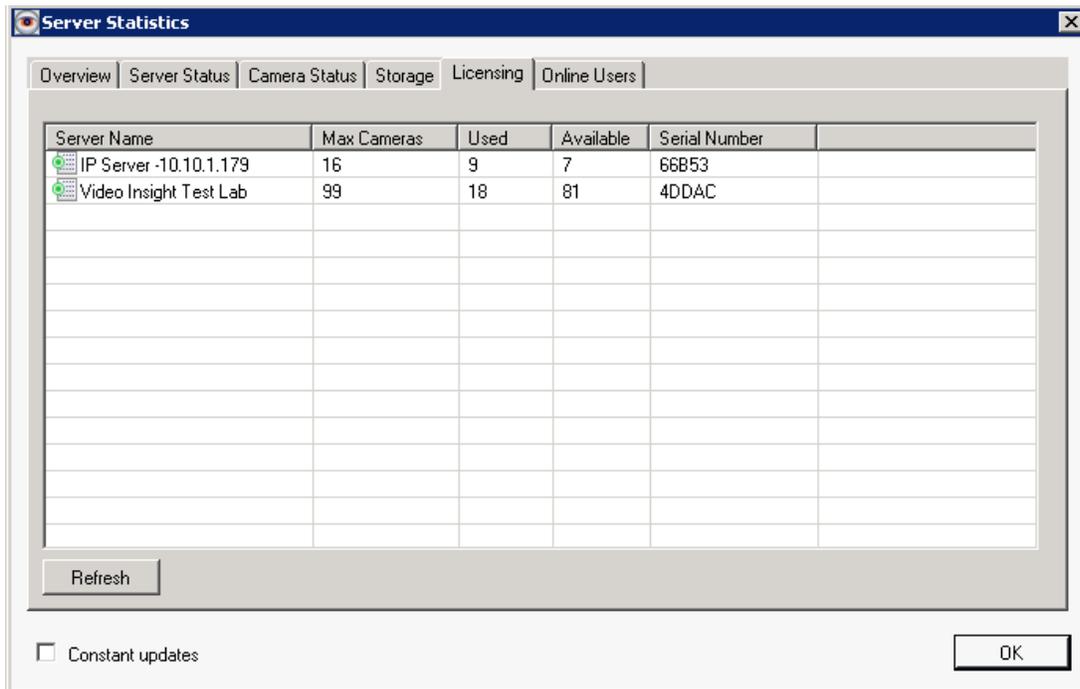
Storage tab

The Storage tab displays all cameras on a selected server and their corresponding storage usage for the displayed number of days.



Licensing tab

The Licensing tab displays all servers, the maximum number of cameras allowed by the license, the number of licenses used by cameras, the number of licenses available and the serial number.



3. Click **OK**.
4. Find the Health Monitor icon (a medical cross) in the System Tray. The health monitor service is running if the icon is green.
5. Right-click on the icon and select Launch Console.
6. Click **Setup** and then User Manager.
7. Click **Add**.

Email Contact Properties

Contact Information

Contact: [New]

Contact Name: Sarit Williams

Email Address: swilliams@video-insight.com

Alternate information

Alternate Contact:

Assistant:

Optional Contact Information

Location:

Phone #:

Office:

Address:

City:

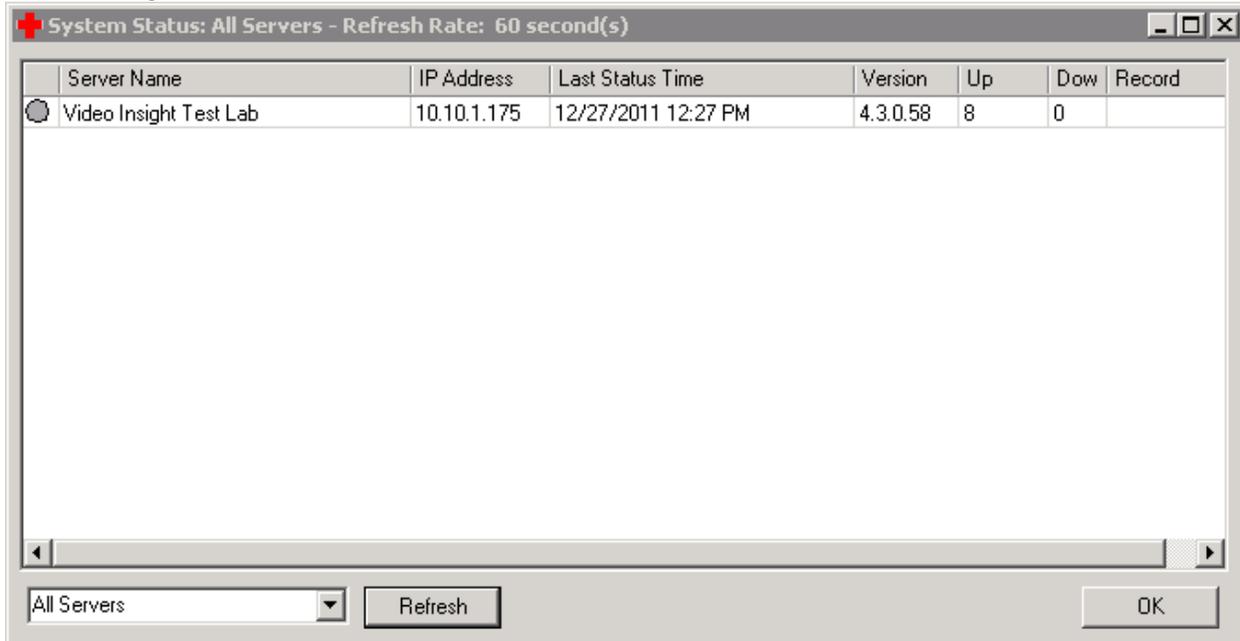
State:

Test OK Cancel

8. Enter contact information. Only Contact Name and Email Address is required.
9. Click **Test** to send a test email to the contact. This is optional.
10. Click **OK**.

Configuration of Health Monitor is complete. Configure each IP Server to point to Health Monitor as described in [Health Monitor tab](#) and in [Health Monitor](#).

Server configuration



The screenshot shows a window titled "System Status: All Servers - Refresh Rate: 60 second(s)". It contains a table with the following data:

Server Name	IP Address	Last Status Time	Version	Up	Dow	Record
Video Insight Test Lab	10.10.1.175	12/27/2011 12:27 PM	4.3.0.58	8	0	

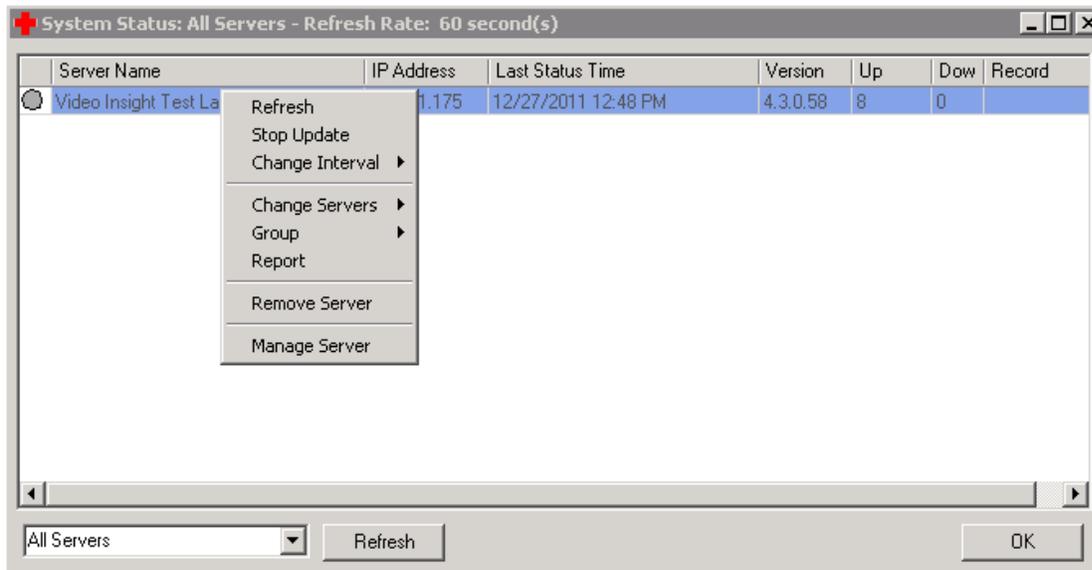
Below the table, there is a dropdown menu set to "All Servers", a "Refresh" button, and an "OK" button.

After an IP Server is configured to report to Health Monitor, it sends the server name, IP address, last contact date and time, IP Server version number as well as the number of cameras up and down. Health Monitor refreshes for any changes every 60 seconds by default. Server status is indicated by a colored circle to the left of the server name. There are four possible states in Health Monitor:

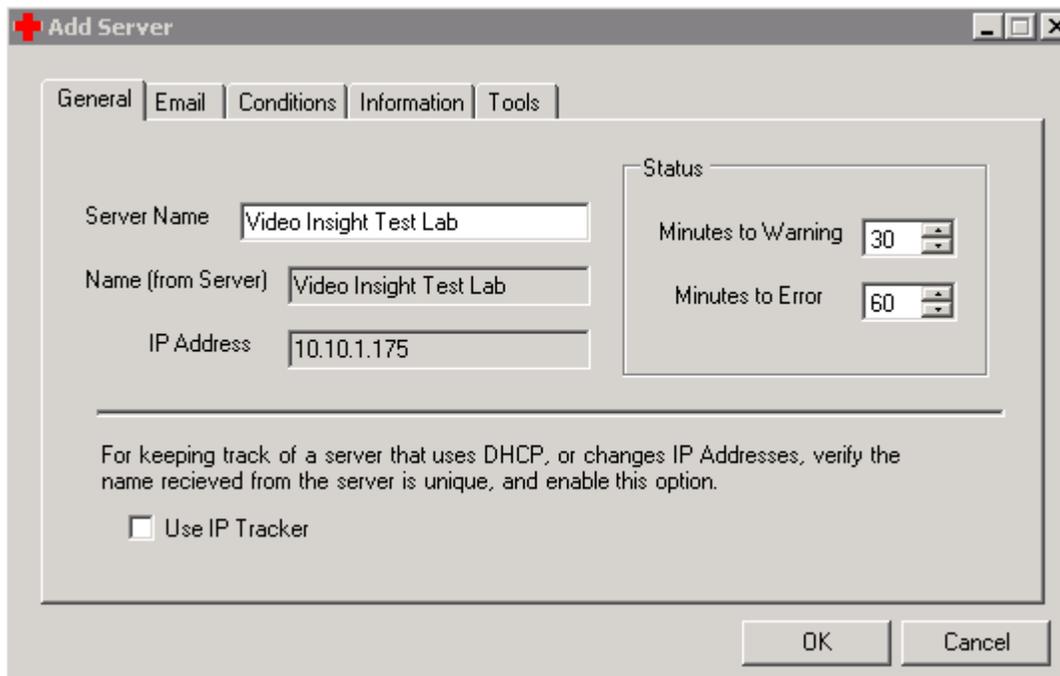
-  = Managed condition: The server has been configured or managed.
-  = Unmanaged condition: The server has reported to Health Monitor, but is not managed.
-  = Warning condition: The server has not reported in the allotted time.
-  = Error condition: The server is down or otherwise offline and attention is required.

To manage an unmanaged server:

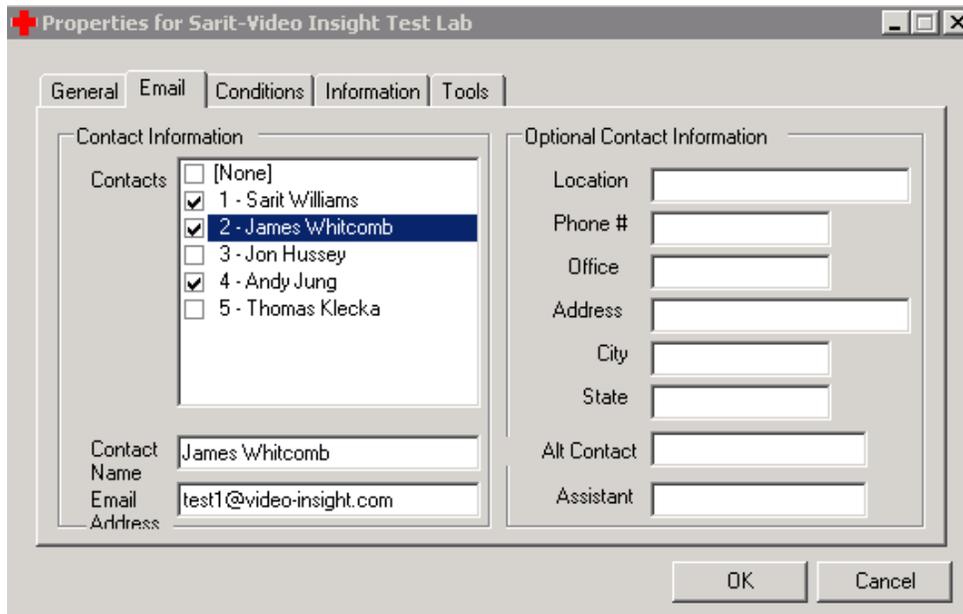
1. Right-click on a server with gray status.



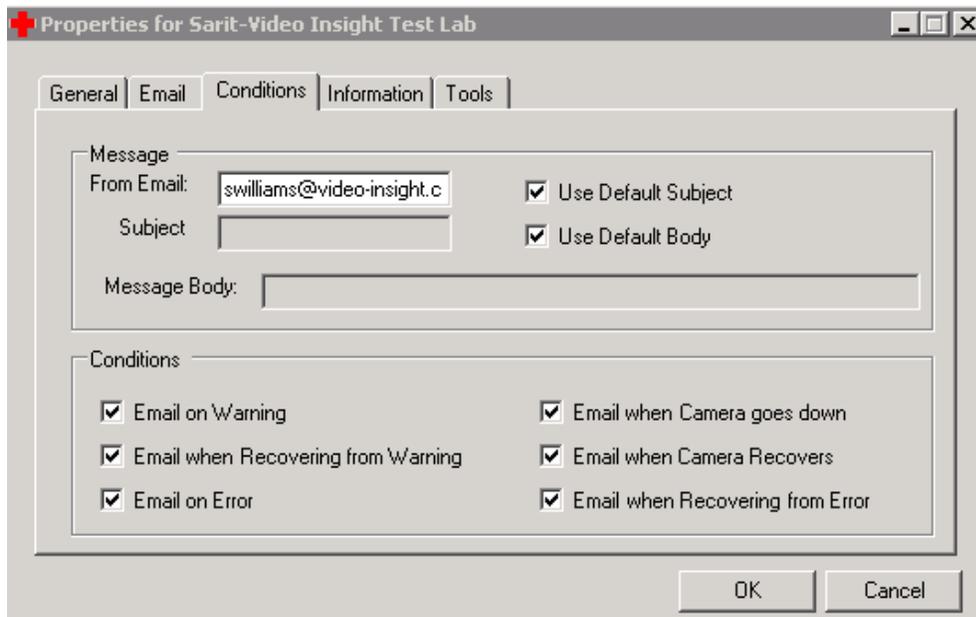
2. Click **Manage Server**.



3. On the General tab you can accept or add to the server's reported name. You cannot completely delete or rename it. You can accept or change the default warning time in minutes before an email is sent to Health Monitor contacts. You can accept or change the default error time in minutes before an email is sent to Health Monitor contacts.
4. Click the Email tab.
5. Check the contact(s) to be notified in the event of a warning or error.



6. Click the Conditions tab.



7. Check the condition(s) that generate an email to the contact when the warning and error time thresholds are met.

Note

Do not set the threshold too low because you may miss important notifications. For example, if a server and camera time threshold is set to 30 minutes and a server is shut down and restarted within five minutes an email will not be generated. In another example, if a server and camera time threshold is set to one minute and it takes the server five minutes to restart an email will be generated and sent to all selected contacts.

Health Monitor may report that it is unable to connect to IP Server. The table below lists possible reasons and potential solutions.

Possible reasons Health Monitor cannot connect to IP Server and potential solutions.

IP address changed	Update the server's IP address.
Server is either manually or automatically restarted	The server or its services may have been restarted to apply changes. Wait a few minutes and refresh Health Monitor.
Diagnostics is running	During Diagnostics the service is stopped for troubleshooting purposes. Wait for Diagnostics to complete or access Diagnostics and start the service.
The time interval set to warning or error is extremely long, server status has not updated in some time and the last known status of a server is down	Check Minutes to Warning and Minutes to Error settings.
Port 11000 is blocked	Access a command line and enter the DOS command <i>netstat</i> to verify the port is available and listening
The checkbox for Enable Health Monitor is unchecked in Server Properties	Check the box to enable management of the server.
Health Monitor information is removed from Setup and Configuration>Health Monitor Section	Add Health Monitor back to this section.
IP service is not started due to an expired	Acquire the proper license and click Update

demonstration version	Activation in Diagnostics .
Network outage	Wait for network service to be restored.
The server's name has changed	Health Monitor displays red status for the old server name. Status for the new server name displays gray (unmanaged). Remove the old server name from Health Monitor and configure the new server name or restore the name of the old server.
Database-related information has changed and the server can no longer access the database	Use Diagnostics to check database connectivity.

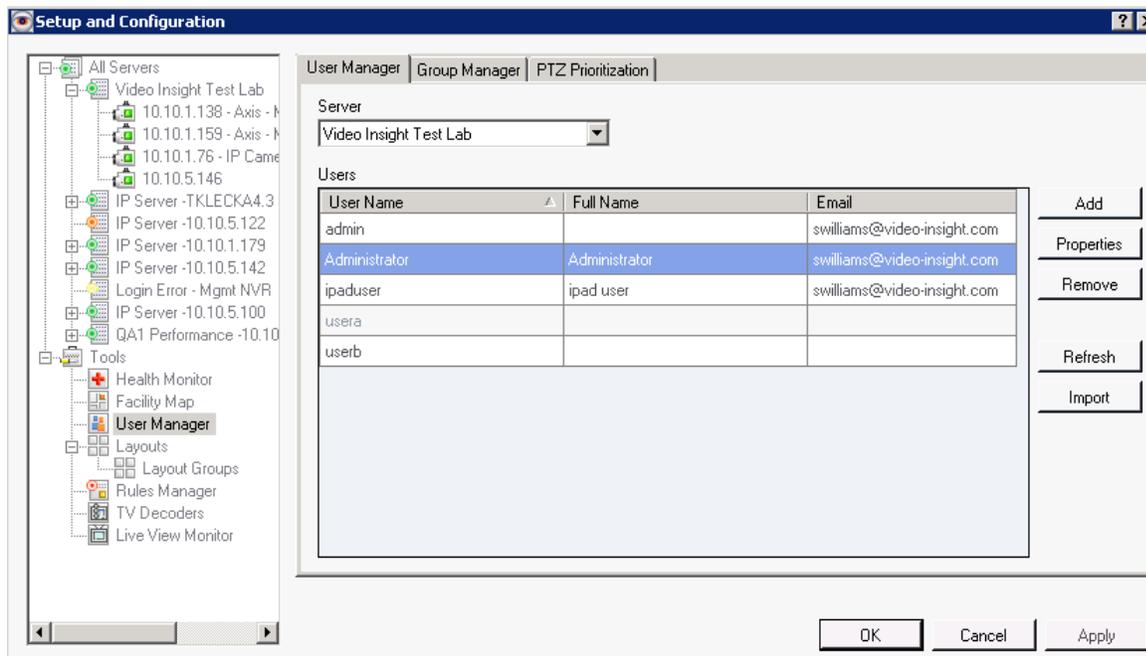
Security

Video surveillance is a pillar of overall security. To secure our products we have implemented secure access to the software, watermarking of recorded video and the ability to quickly know when someone has modified something by using the logs.

User Manager

You can use the User Manager utility to add, modify and delete users. You can also use it to add groups and assign permissions to groups.

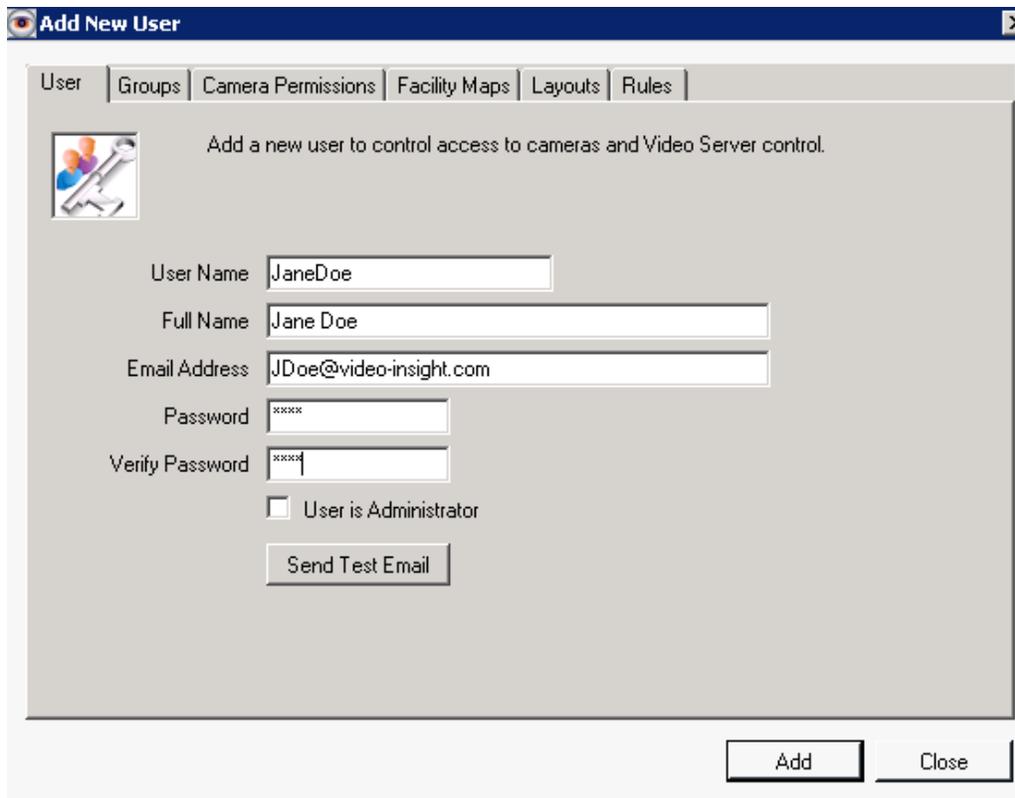
1. Start Monitor Station.
2. Click **Administration** and then Setup and Configuration.
3. Click User Manager in the left navigation tree.



Adding users

To add a user using User Manager:

1. Select the server to add the user to.
2. Click **Add**.



Add New User

User | Groups | Camera Permissions | Facility Maps | Layouts | Rules

Add a new user to control access to cameras and Video Server control.

User Name: JaneDoe

Full Name: Jane Doe

Email Address: JDoe@video-insight.com

Password: xxxx

Verify Password: xxxx

User is Administrator

Send Test Email

Add Close

3. Enter the user's information.
4. Check the box if the user is an Administrator.
5. To send a test email to the user, click **Send Test Email**.
6. Click **Add** if the user is an Administrator. If the user is not an administrator, see [Modifying Users](#) for more information on modifying non-administrator users.

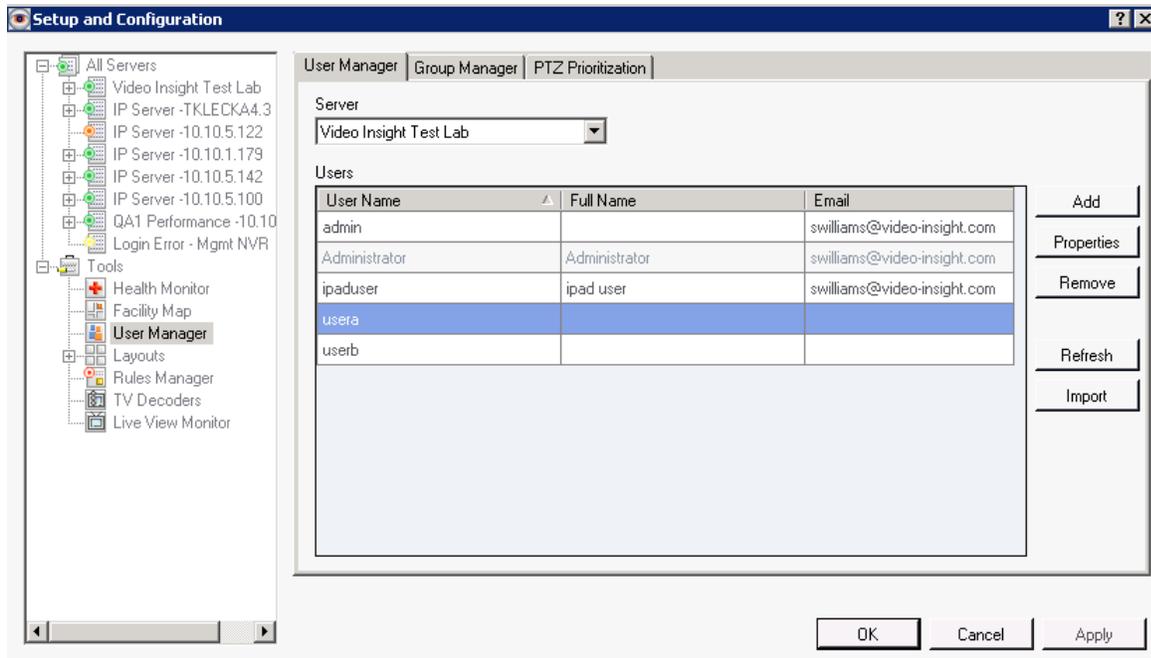
Note

When designating a user as an Administrator, access to all cameras, facility maps and layouts is generated automatically.

Deleting users

To delete a user using User Manager:

1. Select the server to delete the user from.
2. Select the user from the Users list.

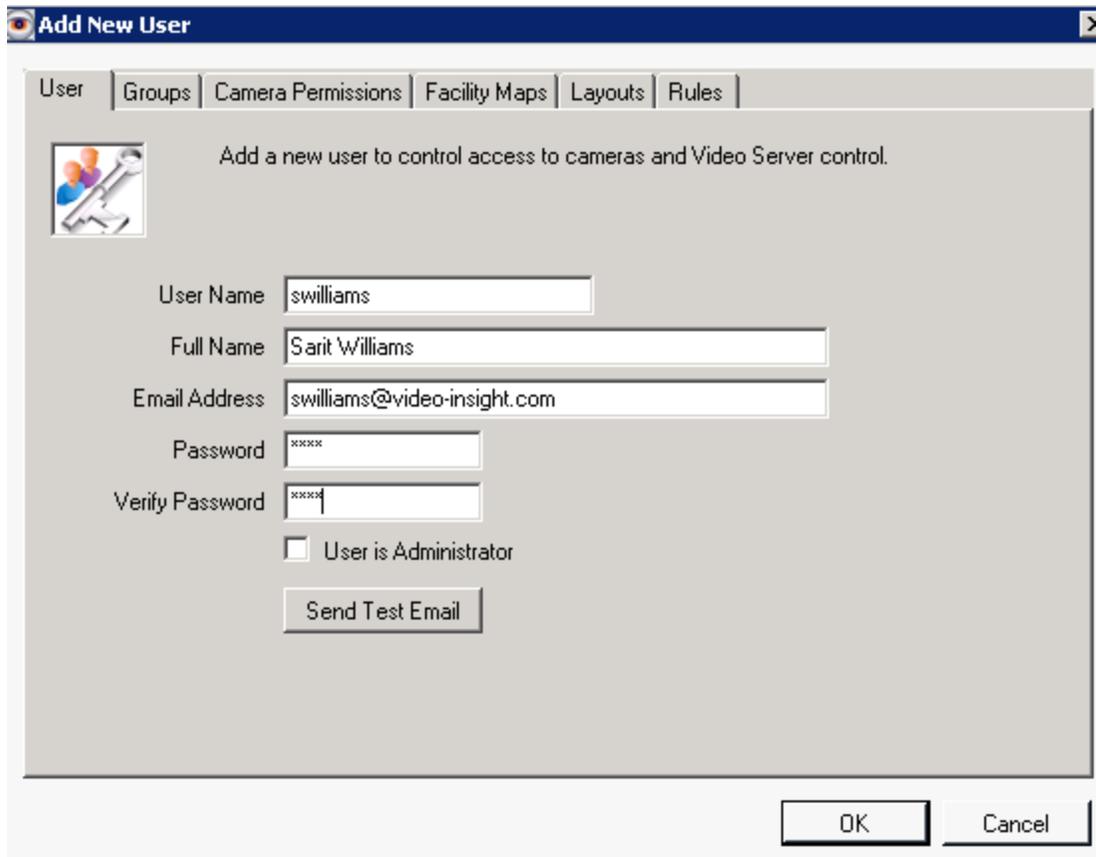


3. Click **Remove**.

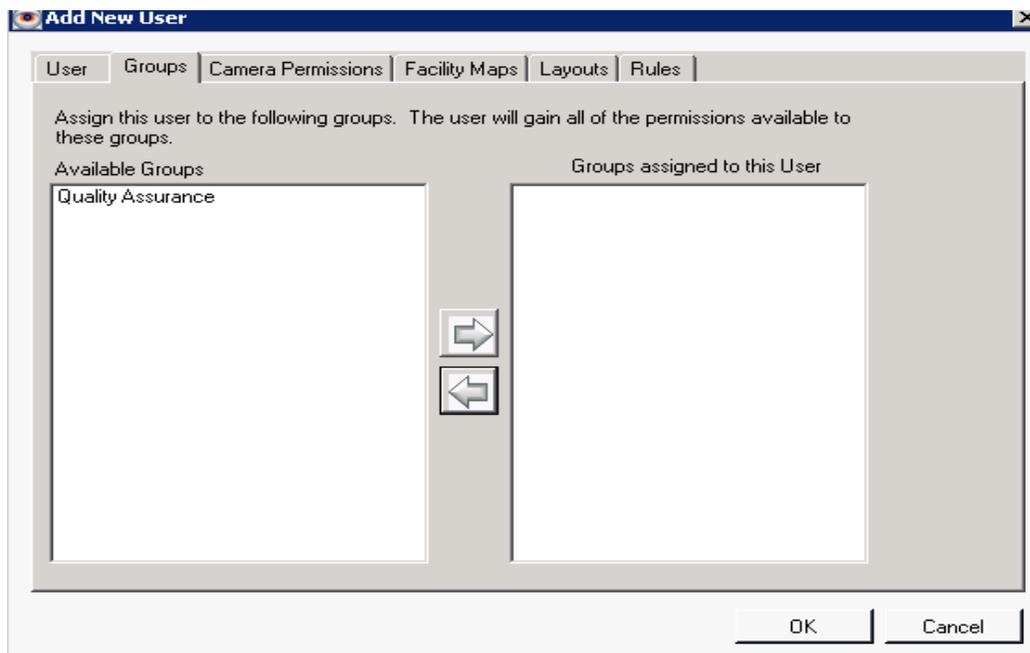
Modifying users

To modify a user using User Manager:

1. Select the server to modify the user on.
2. Select the user from the Users list.
3. Click **Properties**.



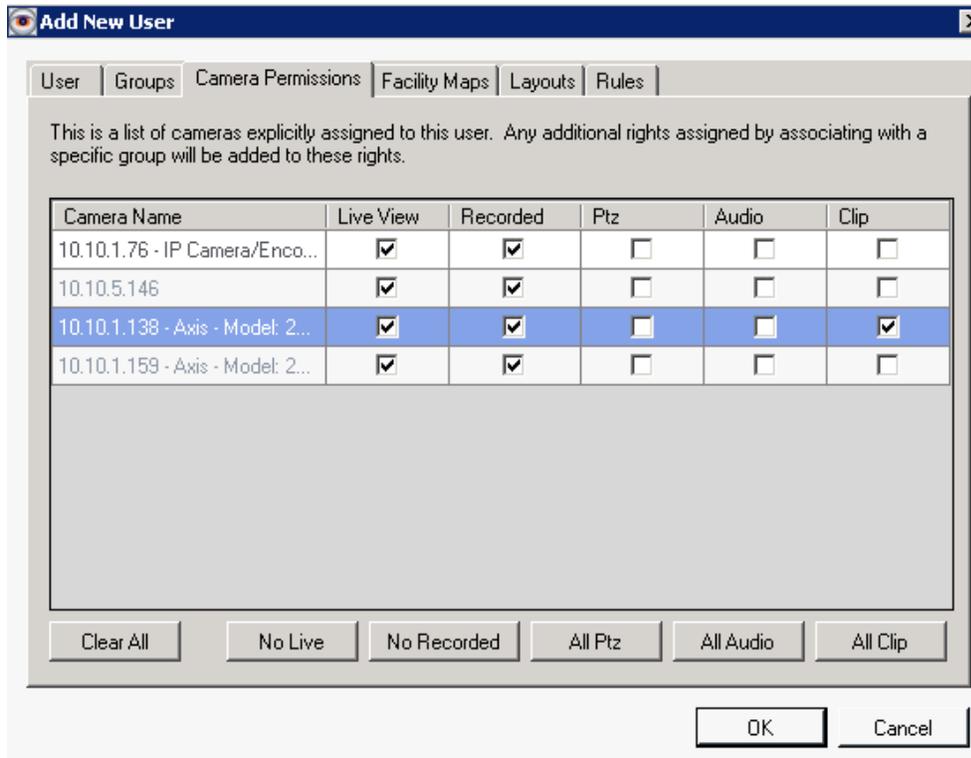
- 4. To modify the user's information, click the User tab.
- 5. To modify the user's group association, click the Groups tab.



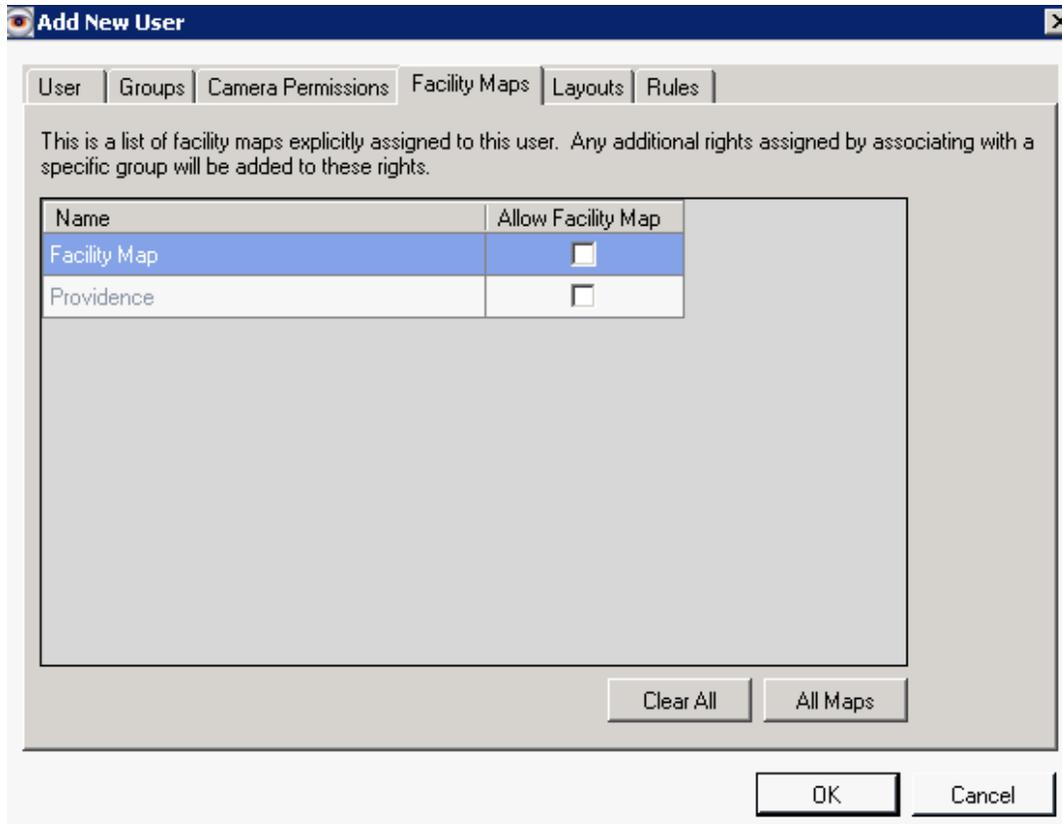
6. To add a group association, select a group from the Available Groups pane and click the right arrow button. To remove a group association, select a group from the Groups assigned to this user pane and click the left arrow button.
7. To modify the user's camera permissions, click the Camera Permissions tab.

Note

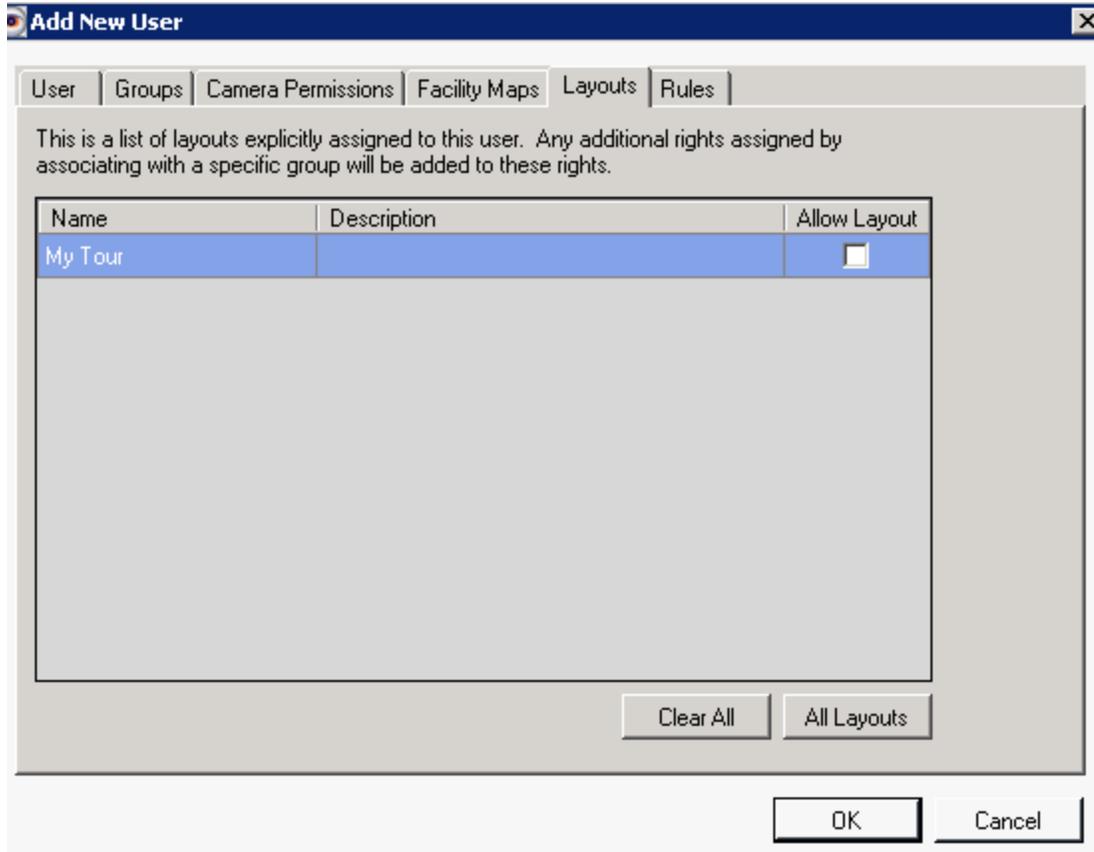
Cameras without audio or PTZ capabilities will remain unchecked regardless of the user.



8. To add camera permissions, check the feature boxes for each camera the user will have access to. To remove camera permissions, uncheck the feature boxes for each camera the user will no longer have access to.
9. To modify the user's map permissions, click the Facility Maps tab.



10. To add map permissions, check the box next to each Facility Map the user will have access to. To remove map permissions, uncheck the box next to each Facility Map the user will no longer have access to.
11. To modify the user's layout permissions, click the Layouts tab.

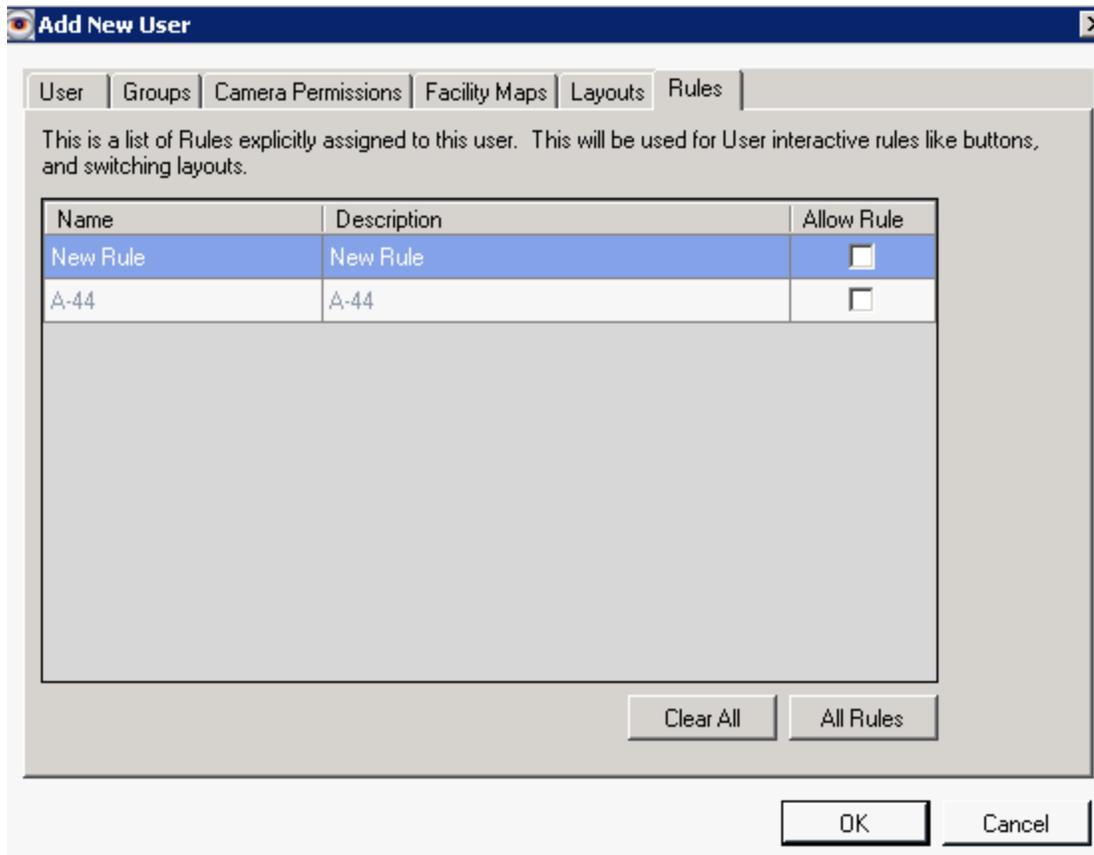


12. To add layout permissions, check the box next to each Layout the user will have access to. To remove layout permissions, uncheck the box next to each Layout the user will no longer have access to.

13. To modify the user's rules permissions, click the Rules tab.

Note

You must repeat the permissions granting process for all users and groups with each added camera, Layout, Facility Map or Rule.



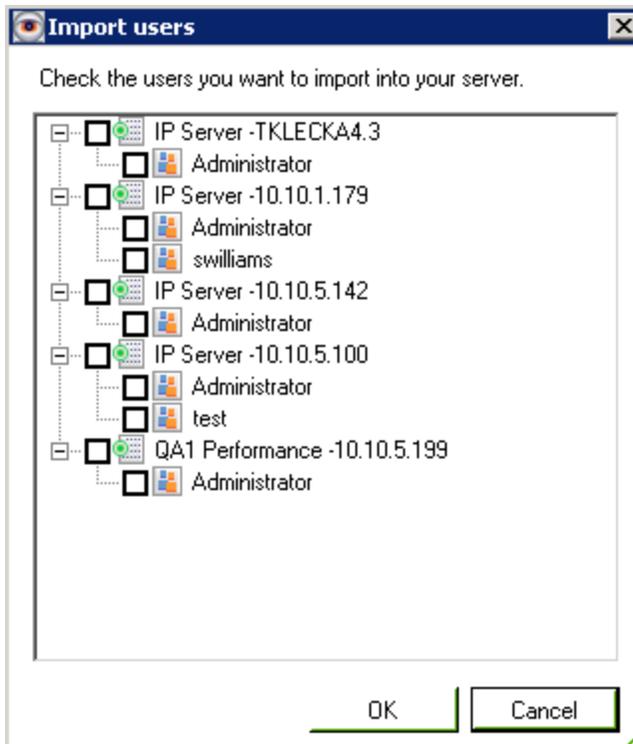
14. To add rules permissions, check the box next to each Rule the user will have access to. To remove rules permissions, uncheck the box next to each rule the user will no longer have access to.
15. Click **OK** if complete.
16. Click **Apply** and then **OK** to exit the Setup and Configuration module.

Importing users

If you have multiple databases and servers used by the same users, you can create the users on one server and then import them to the rest of the servers with a few clicks.

To import users using User Manager:

1. Select the server the users selected will be imported to.
2. Click **Import**.

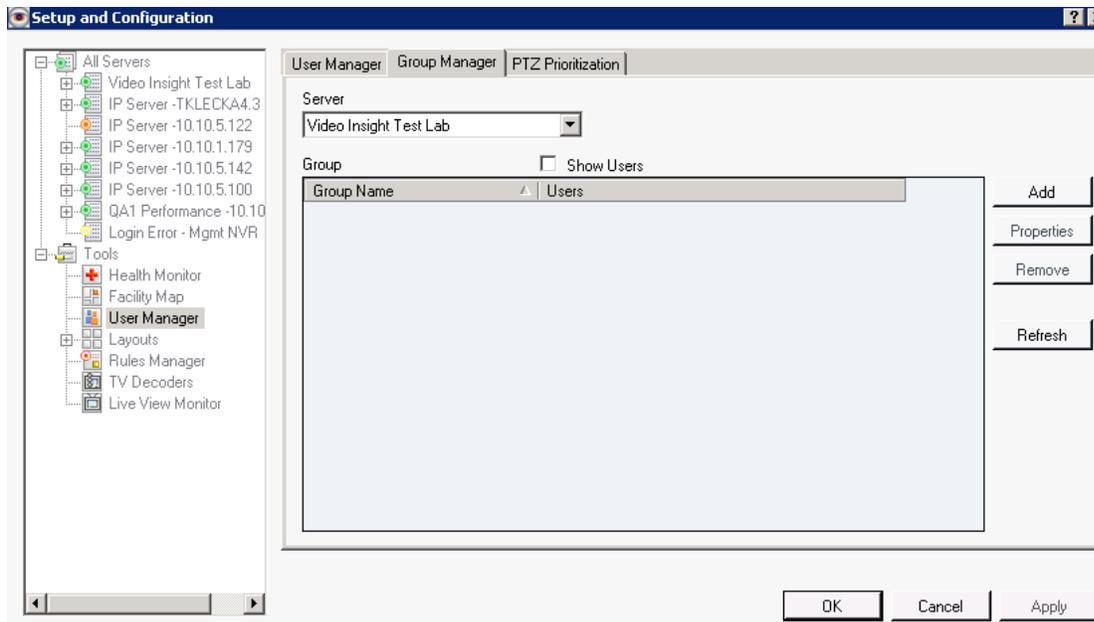


3. Check the users to import.
4. Click **OK**.
5. Click **Refresh**.
6. Repeat the process for all servers to import users to.

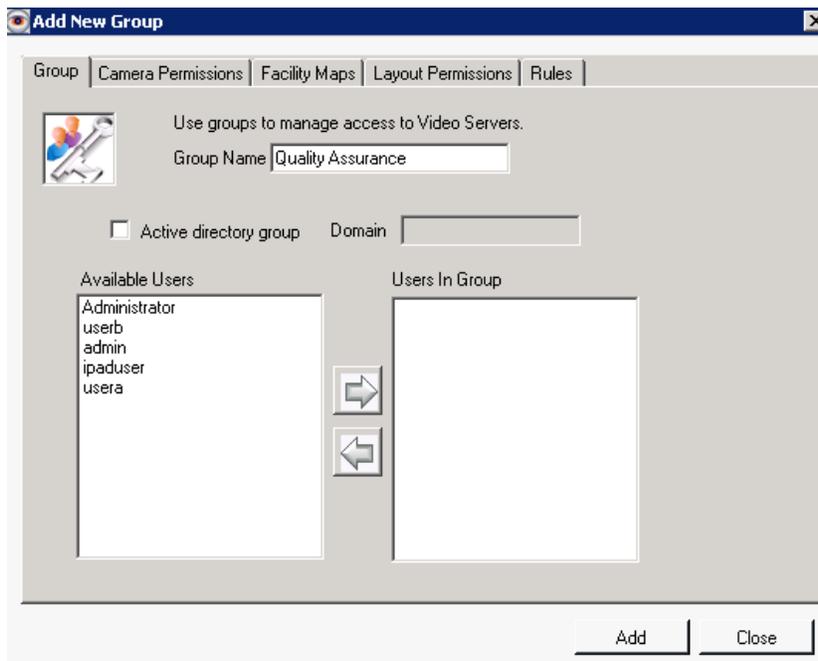
Adding groups

To add groups using User Manager:

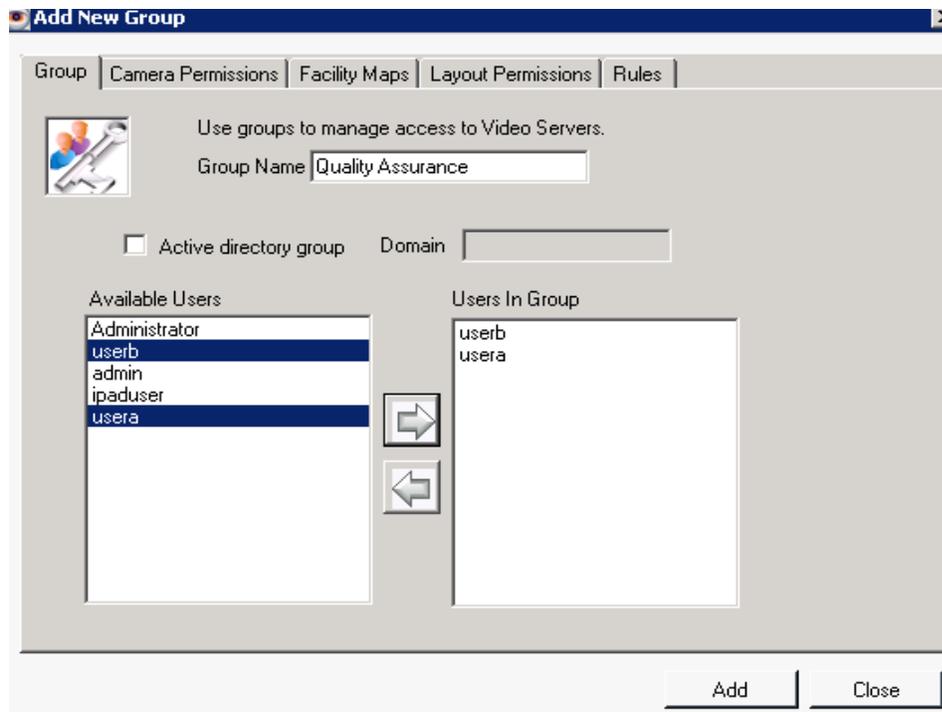
1. Click the Group Manager tab.



2. Select the server.
3. Click **Add**.



4. Enter the group name.
5. Check the box for Active directory group if Active Directory has already been configured.
6. To add a user to the group, select a user from the Available Users pane and then click the right arrow button. To remove a user from the group, select a user from the Users In Group pane and then click the left arrow button.

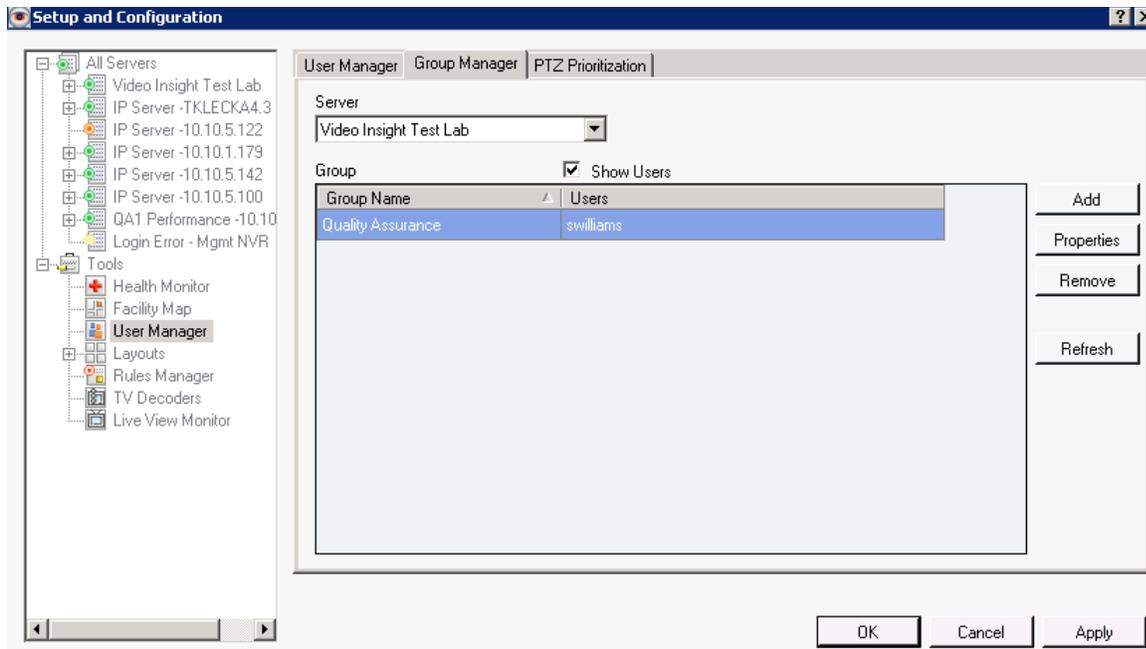


7. Click **Add**.
8. See [Modifying groups](#) for more information on setting permissions.

Deleting groups

To delete a group using User Manager:

1. Select the server from which the group will be removed from.
2. Select the group from the Group list.

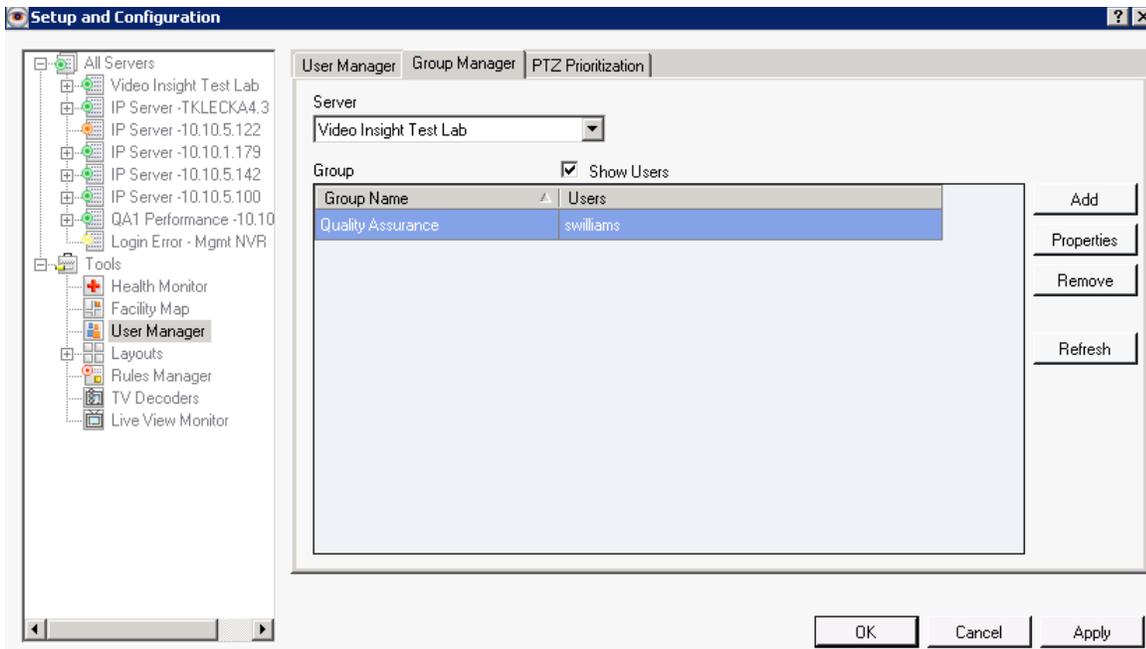


3. Click **Remove**.

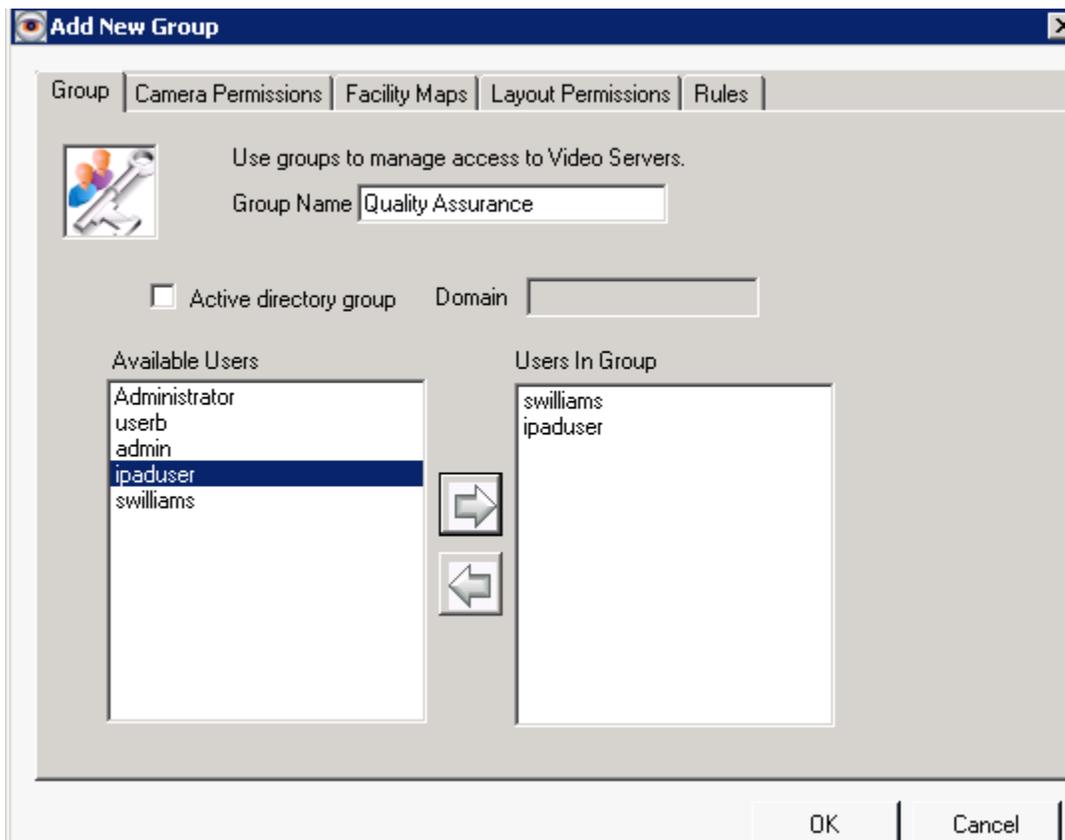
Modifying groups

To modify a group using User Manager:

1. Select the Group Manager tab.
2. Select the server.
3. Select the group from the Group list.

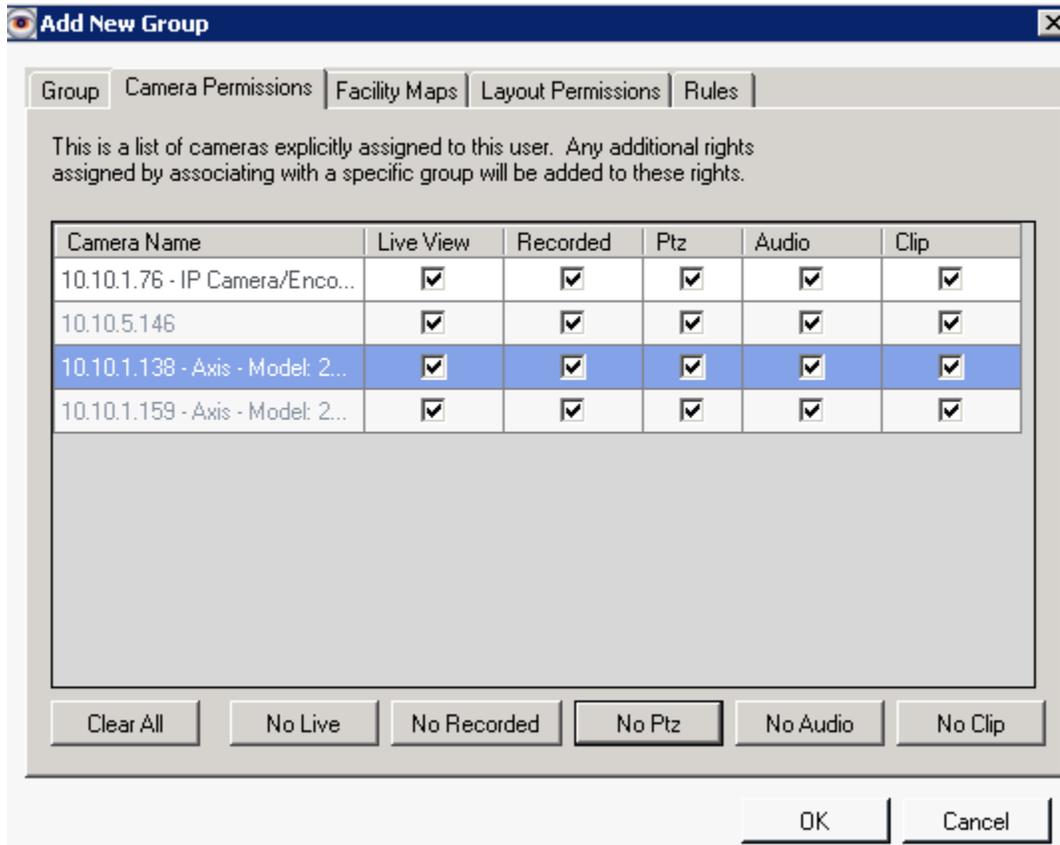


4. Click **Properties**.



5. Modify the group's name if needed.

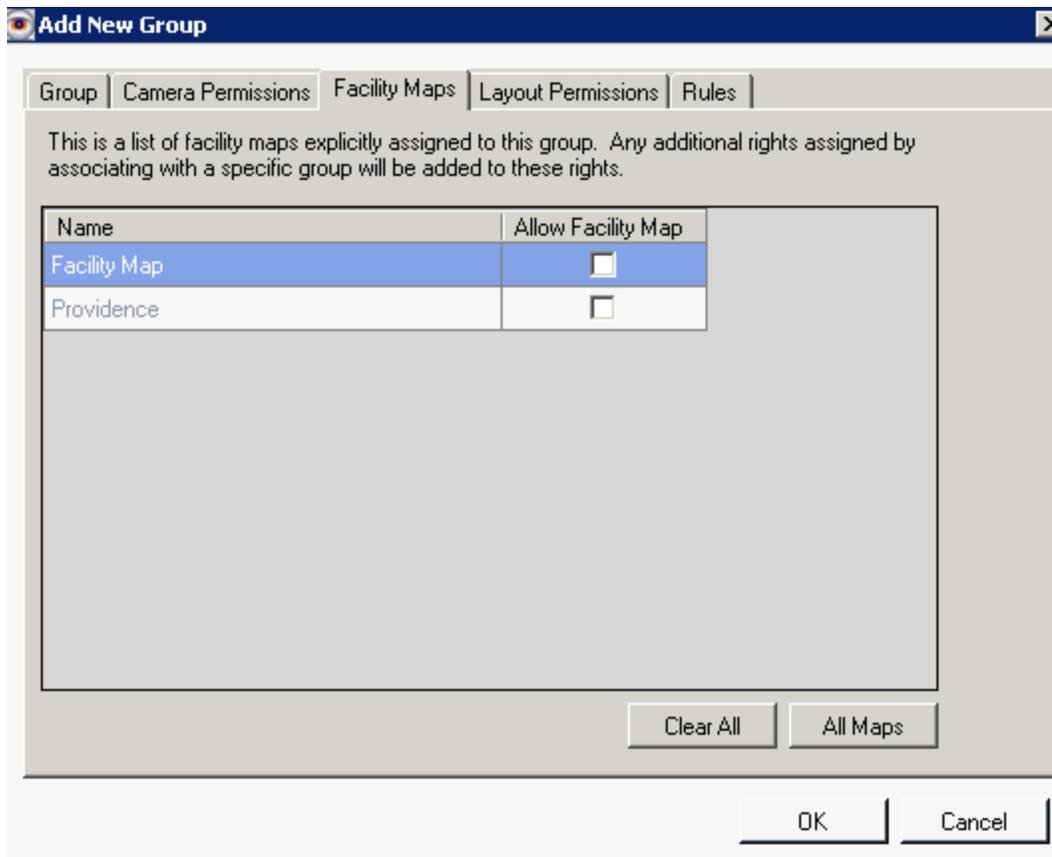
6. To add a user to the group, select a user from the Available Users pane and then click the right arrow button. To remove a user from the group, select a user from the Users In Group pane and then click the left arrow button.
7. To modify a group's camera permissions, click the Camera Permissions tab.



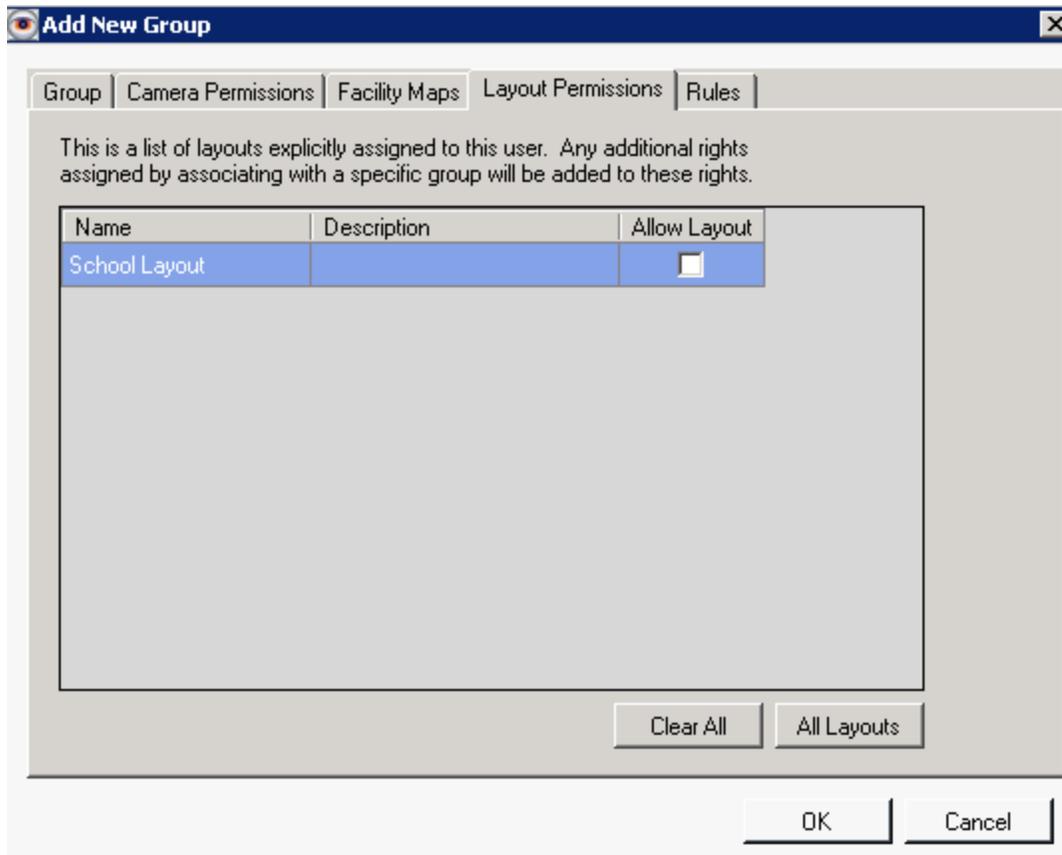
8. To add camera permissions, check the feature boxes next to each camera the group will have access to. To remove camera permissions, uncheck the feature boxes next to each camera the group will no longer have access to.
9. To modify a group's map permissions, click the Facility Maps tab.

Note

Cameras without audio or PTZ capabilities will remain unchecked regardless of the user.



10. To add map permissions, check the box next to each Facility Map the group will have access to. To remove map permissions, uncheck the box next to each Facility Map the group will no longer have access to.
11. To modify a group's layout permissions, click the Layout Permissions tab.

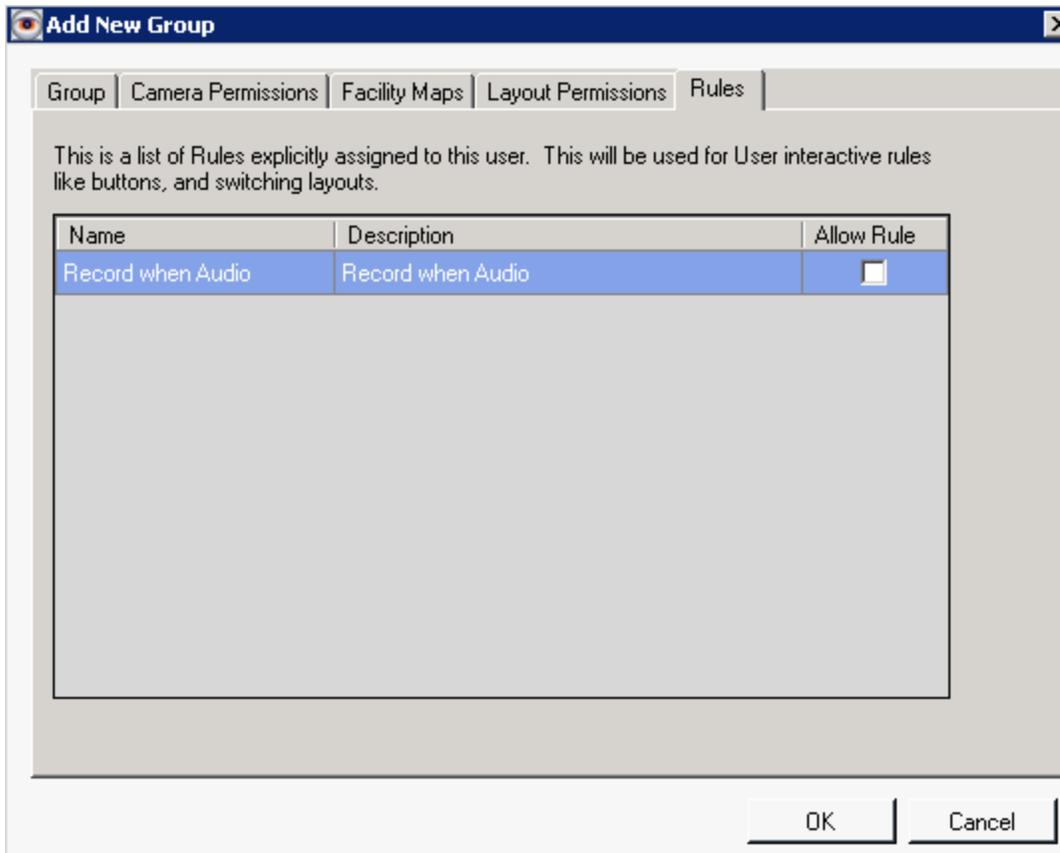


12. To add layout permissions, check the box next to each Layout the group will have access to. To remove permissions, uncheck the box next to each Layout the group will no longer have access to.

13. To modify a group's rules permissions, click the Rules tab.

Note

You must repeat the permissions granting process for all users and groups with each added camera, Layout, Facility Map or Rule.



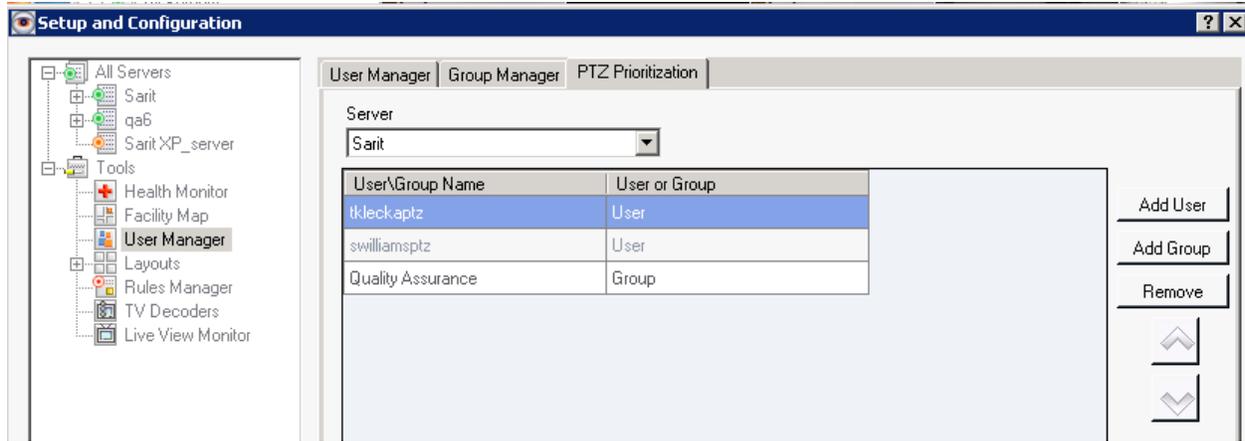
14. To add rules permissions, check the box next to each Rule the group will have access to. To remove rules permissions, uncheck the box next to each Rule the group will no longer have access to.
15. Click **OK** if complete.
16. Click **Apply** and then **OK** to exit the Setup and Configuration module.

PTZ priority

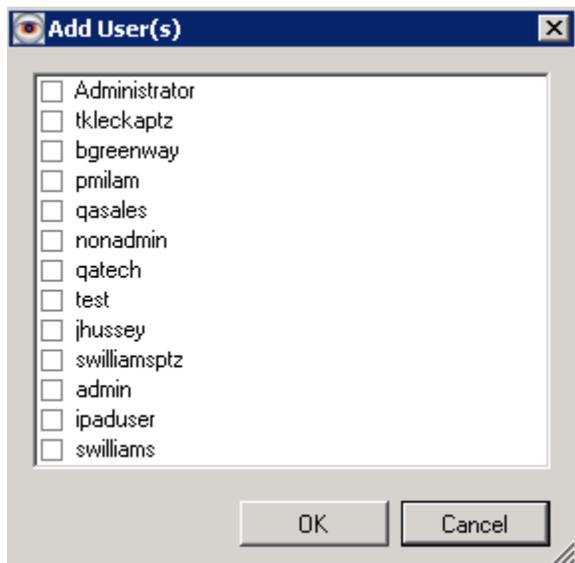
The PTZ Prioritization tab allows administrators to set the priority for users on all PTZ capable cameras. The higher the listed user or group is, the higher their priority.

To configure PTZ priority:

1. Start Monitor Station.
2. Click **Administration** and then Setup and Configuration.
3. Click User Manager from the left navigation tree.
4. Click the PTZ Prioritization tab.
5. Select the server to set the priority on from the Server drop-down menu.

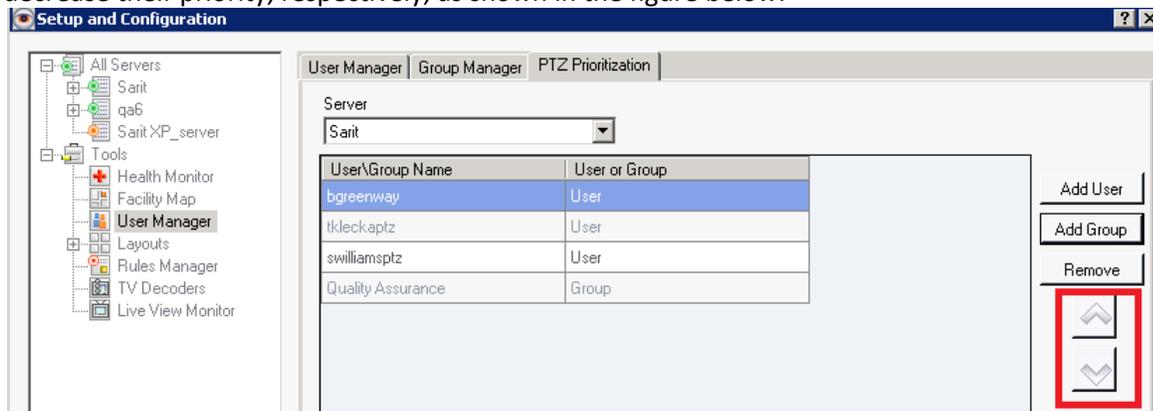


6. Click **Add User** or **Add Group**.



7. Check the user(s) or group(s) and then click **OK**.

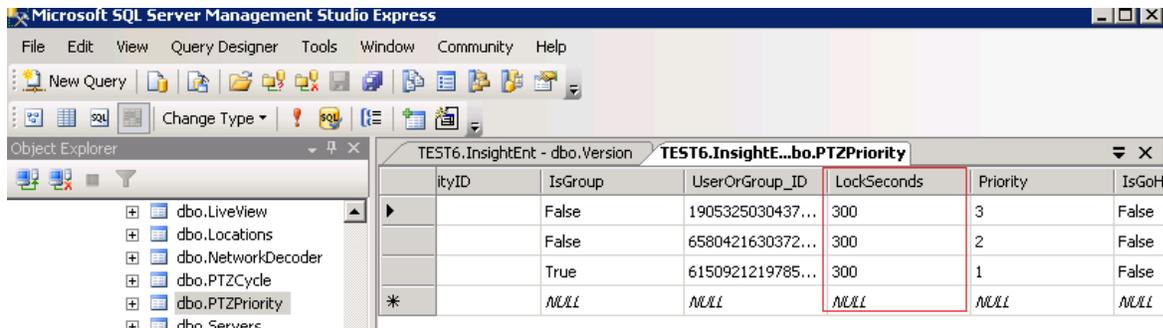
8. Select the user or group to prioritize and click the up or down arrow buttons to increase or decrease their priority, respectively, as shown in the figure below.



If two users or groups want to use the PTZ feature on the camera at the same time, the lower-priority user will have to wait 300 seconds. The default wait time is 5 minutes (300 seconds). The wait time can be changed in the database but is a task recommended only for advanced users.

To increase or decrease the wait time per user:

1. Start Microsoft SQL Server Management Studio Express.
2. Expand the InsightEnt database.
3. Right-click the PTZPriority table and select open.



4. Notice the LockSeconds column.
5. To update the value to something other than 300 seconds run the following query:

```
UPDATE [InsightEnt].[dbo].[PTZPriority]
SET [LockSeconds] = '240'
```

This sample query will change all users in PTZPriority table to a 240 second (3 minutes) delay. You can add additional clauses to further restrict certain users or groups.

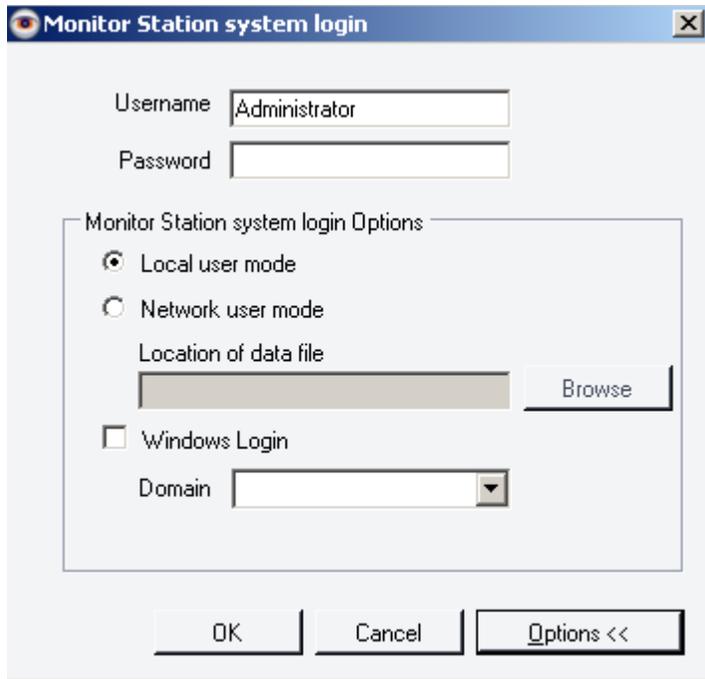
Login

The software is installed with security off enabling login-free access to the Monitor Station and Web Clients. See the Advanced tab of [Server properties](#) for more information on setting server security.

You can choose any one or a combination of login options depending on your company and security needs.

To change Monitor Station login settings:

1. Start Monitor Station.



Local user mode: This option can be used on its own or in combination with the Windows Login checkbox (discussed later). When this option is used on its own it behaves differently depending on other system settings.

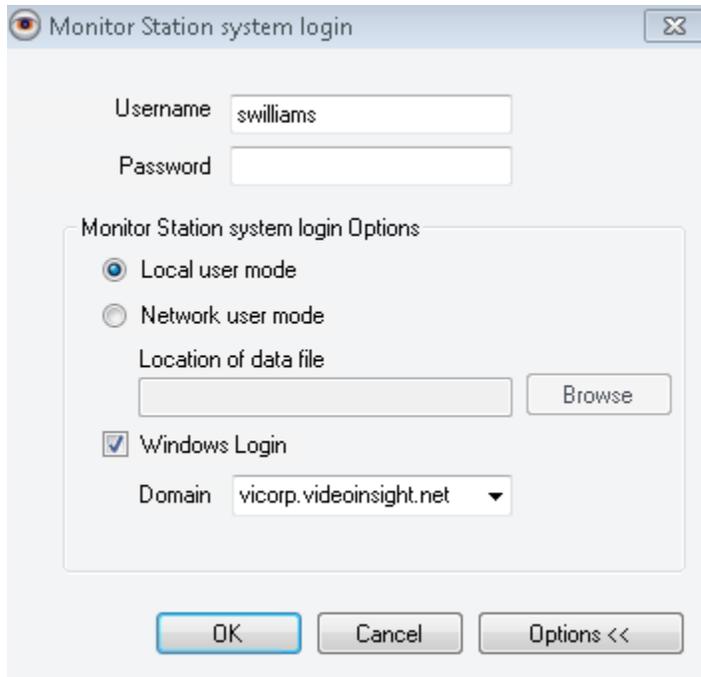
Security On: With Server Security On, the credentials entered will be checked for validity against Monitor Station User Manager. See [Adding users](#) for more information on adding users in User Manager.

Security Off: With Server Security Off, all logins will be accepted.

With Windows Login Check enabled: This case assumes that an Active Directory or LDAP configuration has been implemented and that all users will be authenticated against Active Directory and/or Monitor Station User Manager (because all Active Directory/LDAP users are imported to User Manager) as long as Server Security is turned on.

To login using Active Directory:

1. Start Monitor Station.
2. Click **Options**.



3. Check the box for Windows Login.
4. Select the Domain from the drop-down menu.
5. Enter the user name and password.
6. Click **OK**.

Network user mode: This option is useful in large environments where there are many clients and servers. Instead of adding every server to each client and then having to manage multiple lists when adding or removing servers from Setup and Configuration, you can add all of the servers using one Monitor Station.

To add all servers using one Monitor Station:

1. Navigate to Setup and Configuration.
2. Add all of the servers, one by one, to the Known Video Servers list.
3. Click **Export List** and save the .LSL file to a shared location.

Direct all users to that file. This file gives them the latest server information every time they log in without having to manage hundreds of clients. The administrator has just one file to manage by adding or removing servers at any time without interfering with daily business functions.

This option may also be used with an Active Directory or LDAP configuration using the Windows Login Mode checkbox.

You can also bypass the Login pop-up with or without Server Security being on by setting the Auto Login option:

1. Start Monitor Station.
 2. Navigate to Tools and then Options.
 3. Click the Startup tab.
 4. Check the box for Enable Auto Login.
- a. If Server Security is off credentials are not needed
 - b. If Server Security is on you must provide valid credentials.

Active Directory

Active Directory is a Microsoft Windows Server network directory service that spans the organization. It is used to manage users, groups and their access to applications and file systems. Monitor Station and Web Client integrate with Active Directory to simplify credential management. Users can use their domain user name and password to login to Monitor Station and Web Client. Consult your Microsoft documentation for more information on Active Directory.

Note

When multiple IP Servers are installed and Active Directory configuration is being considered we recommend using a shared database install to avoid importing users and groups multiple times to each database.

Prerequisites

1. Active Directory server with users and groups configured.
2. Active Directory can be configured using a local database for each server or using a shared database environment.
3. Administrator user account with administrator-level credentials in both the domain and on the Active Directory server (do not use an individual account).
4. The IP Server host is part of the domain.
5. IP Server must be able to communicate with all domain controllers via port 389 or 636. Port 389 cannot be changed. Port 636 is used for SSL encryption.
6. IP Server configuration must be done while logged into the domain with a valid domain account. This is required by Windows for security reasons.

We recommend importing users as a group instead of individually. The group must be created in Active Directory before it can be imported. You can create groups to suit your needs and policies.

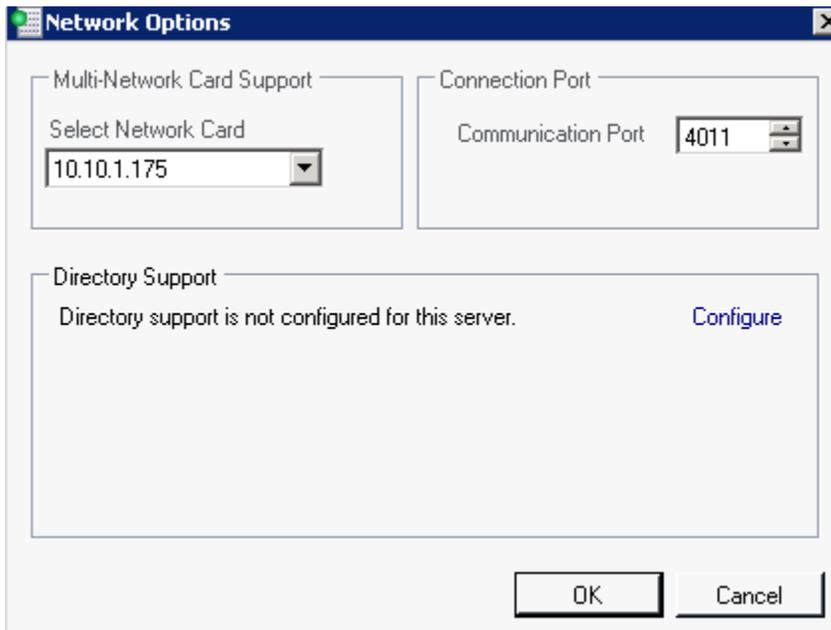
To configure the IP Video Enterprise service to run as an Active Directory account:

1. Click the Start button.
2. Enter *services.msc* and then press Enter.

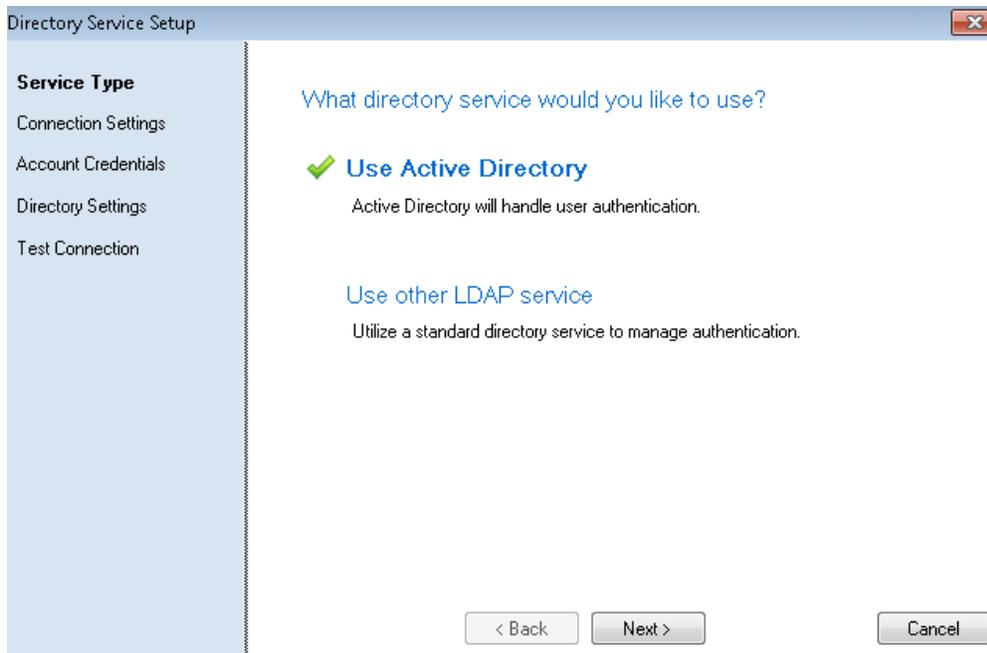
3. Locate the IP Video Enterprise service.
4. Right-click and select Stop.
5. Right-click and select Properties.
6. Select the Log On tab.
7. Select the second option for the account.
8. Provide an Active Directory account with minimal rights. A basic domain user account should be sufficient.
9. Click the General tab and then select Start.
10. Click OK.
11. Restart the IIS Admin service if using Web Client.

Configuring Active Directory

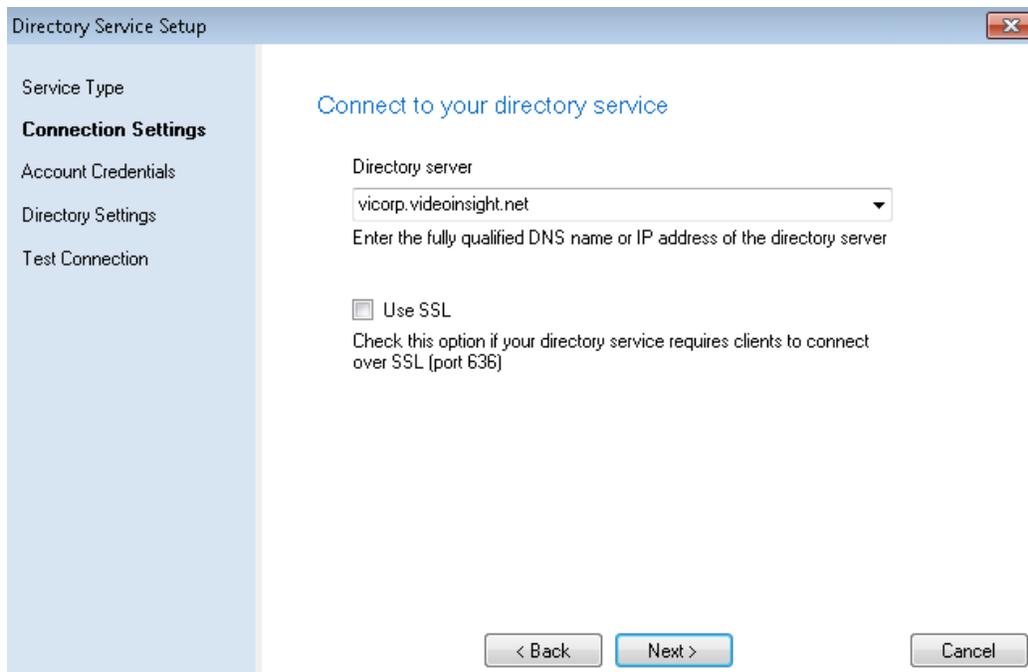
1. Access the IP Server computer.
2. Right-click the IPSM icon in the System Tray.
3. Select Server Configuration.
4. Click **Network Options**.



5. Click **Configure**.

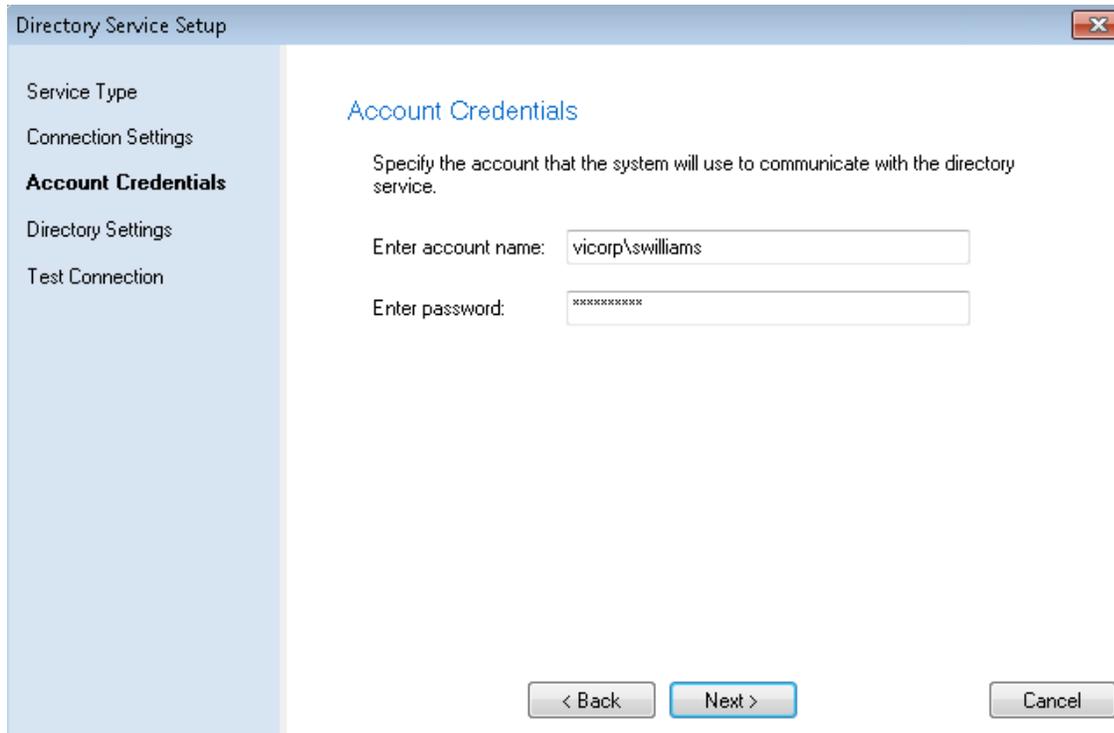


6. Click **Use Active Directory**.
7. Click **Next**.



The domain name automatically populates the Directory server field. If it is blank, check if the prerequisites have been met.

8. Confirm the domain name.
9. Check the box for Use SSL if using SSL for Active Directory configuration.
10. Click **Next**.



The screenshot shows a window titled "Directory Service Setup" with a close button in the top right corner. On the left is a navigation pane with the following items: "Service Type", "Connection Settings", "Account Credentials" (which is highlighted), "Directory Settings", and "Test Connection". The main area of the window is titled "Account Credentials" and contains the following text: "Specify the account that the system will use to communicate with the directory service." Below this text are two input fields: "Enter account name:" with the text "vicorp\swilliams" and "Enter password:" with a masked password "XXXXXXXXXX". At the bottom of the window are three buttons: "< Back", "Next >" (which is highlighted in blue), and "Cancel".

11. Enter the administrator account name and password.
12. Click **Next**.

The screenshot shows a window titled "Directory Service Setup" with a sidebar on the left containing the following menu items: "Service Type", "Connection Settings", "Account Credentials", "Directory Settings" (which is highlighted), and "Test Connection". The main area of the window is titled "Configure directory service settings" and contains the following fields and text:

- Base Distinguished Name (Base DN)**: A text input field containing the value "DC=vicorp,DC=videoinsight,DC=net". Below the field is the text: "This should be the directory service's root container. Directory searches will start here."
- Request timeout**: A spin box containing the value "30". Below the field is the text: "Directory requests will time out after the specified number of seconds have elapsed."
- Limit search results**: A spin box containing the value "1000". Below the field is the text: "Limits the number of users or groups returned from a single search."

At the bottom of the window, there are three buttons: "< Back", "Next >" (which is highlighted in blue), and "Cancel".

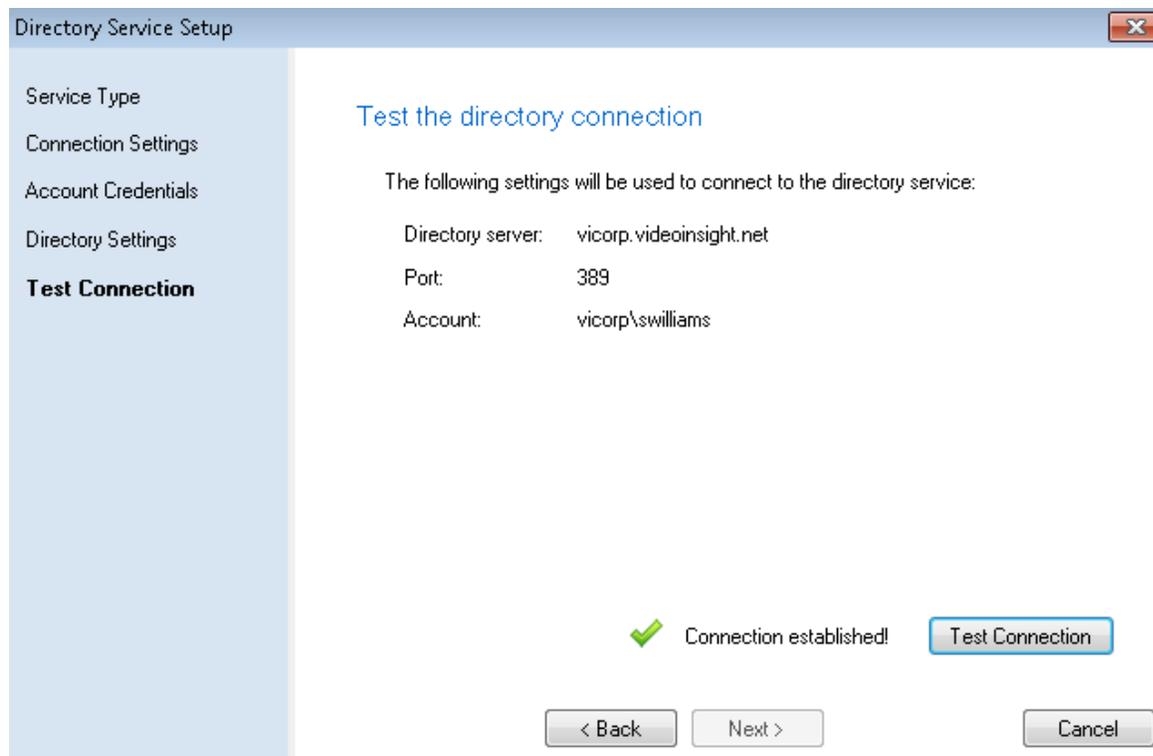
The Base Distinguished Name automatically populates the Base (DN) field. If it is blank, check if the prerequisites have been met. If they have, the Base DN should be the top (root) folder to allow for adding of any user from any group.

If the Base DN is extremely long it could mean the user has access restrictions. This could limit the number of users they will be able to add.

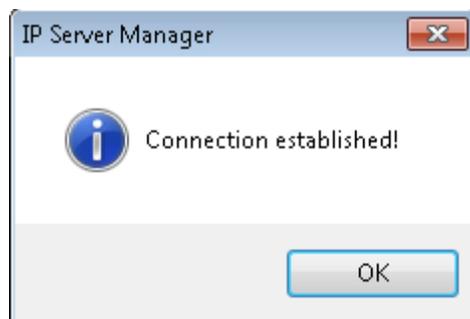
Request timeout: This value reflects the setting on the Active Directory server, and cannot be changed here. Any requests made to the Active Directory server that exceed that time will timeout.

Limit search results: This value reflects the setting on the Active Directory server. This is the maximum number of results returned from the Active Directory server.

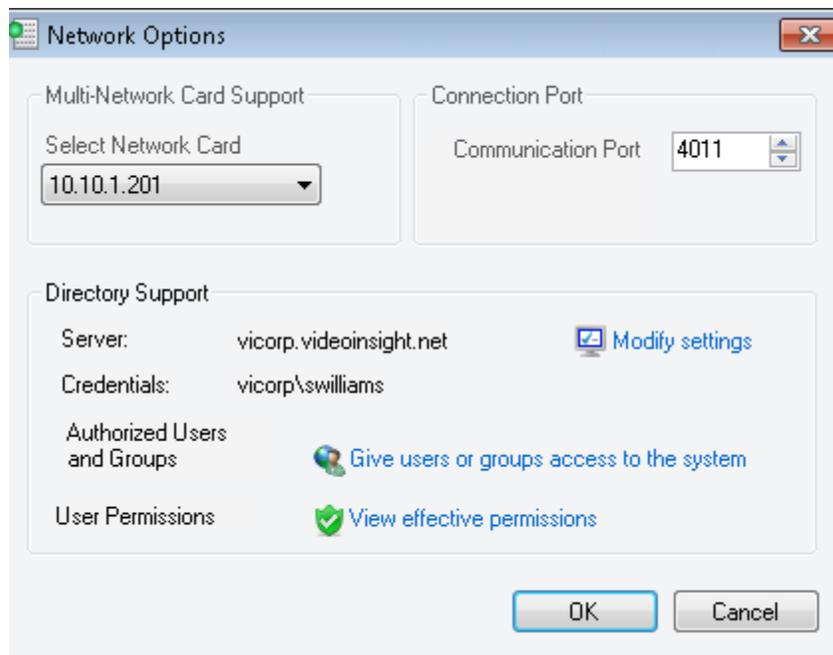
13. Click **Next**.



14. Click **Test Connection**.



15. Click **OK** to dismiss the "Connection established!" message. If the test connection fails, review steps 1-14.
16. Click **Apply**.

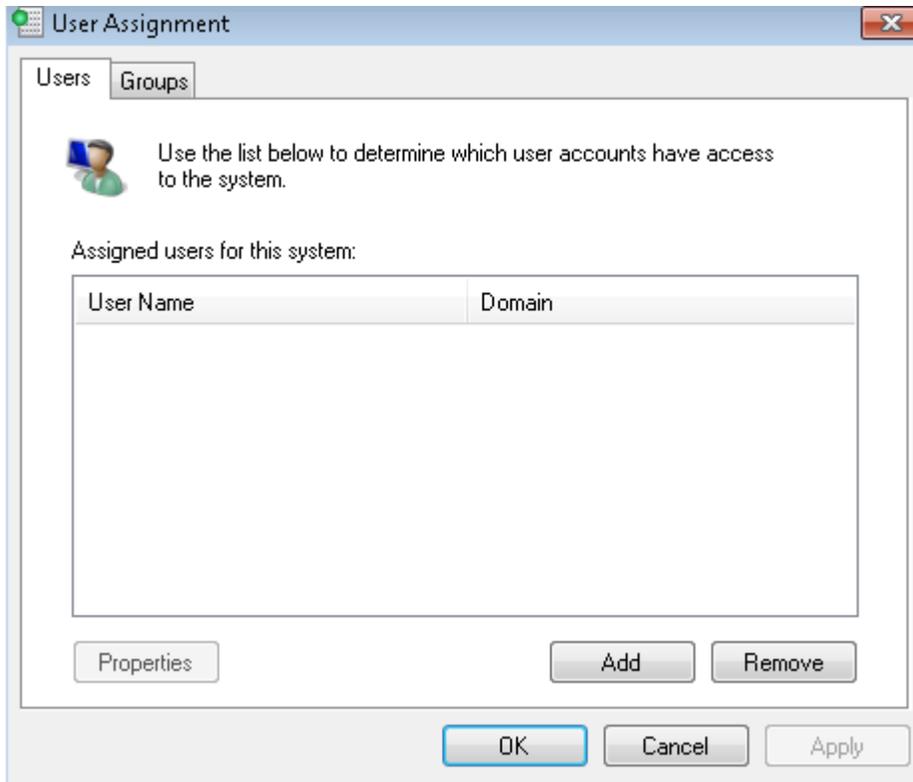


IP Server and Active Directory are now integrated. You will need to add users and groups before users can log in to Monitor Station.

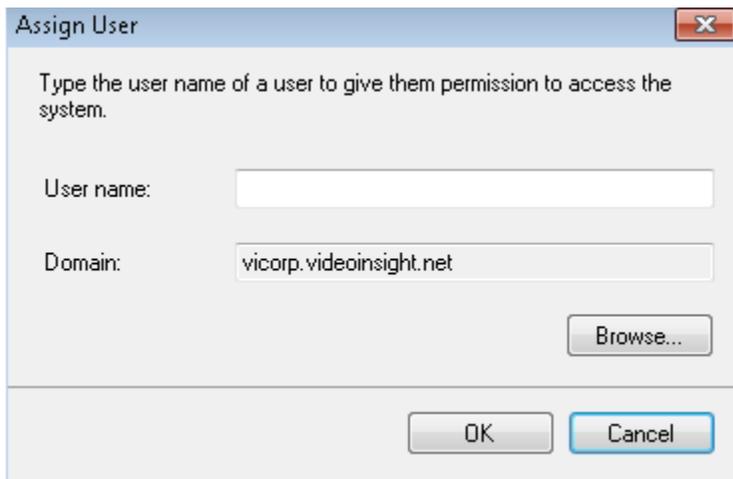
Adding users or groups

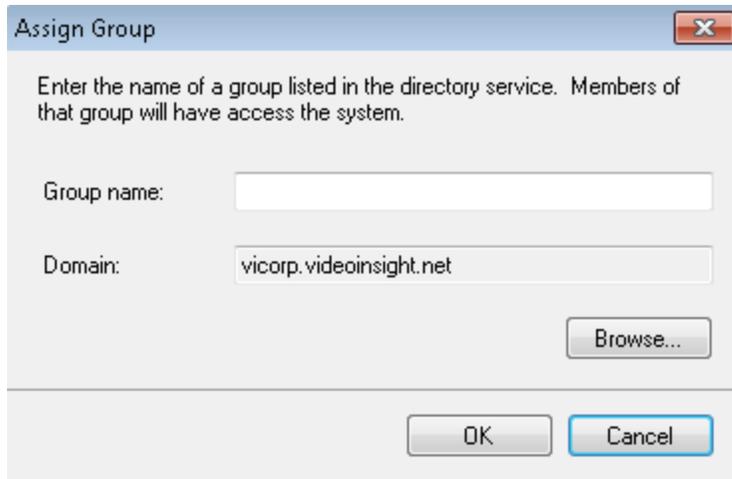
To add Active Directory users and groups:

1. On the Network Options screen click Give users or groups access to the system.

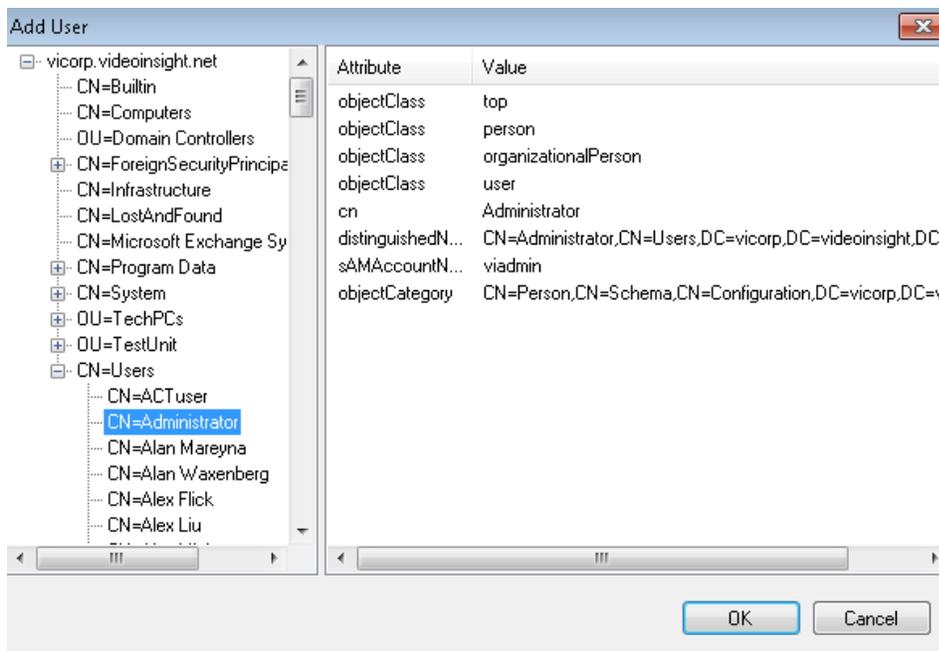


2. Click **Add**.

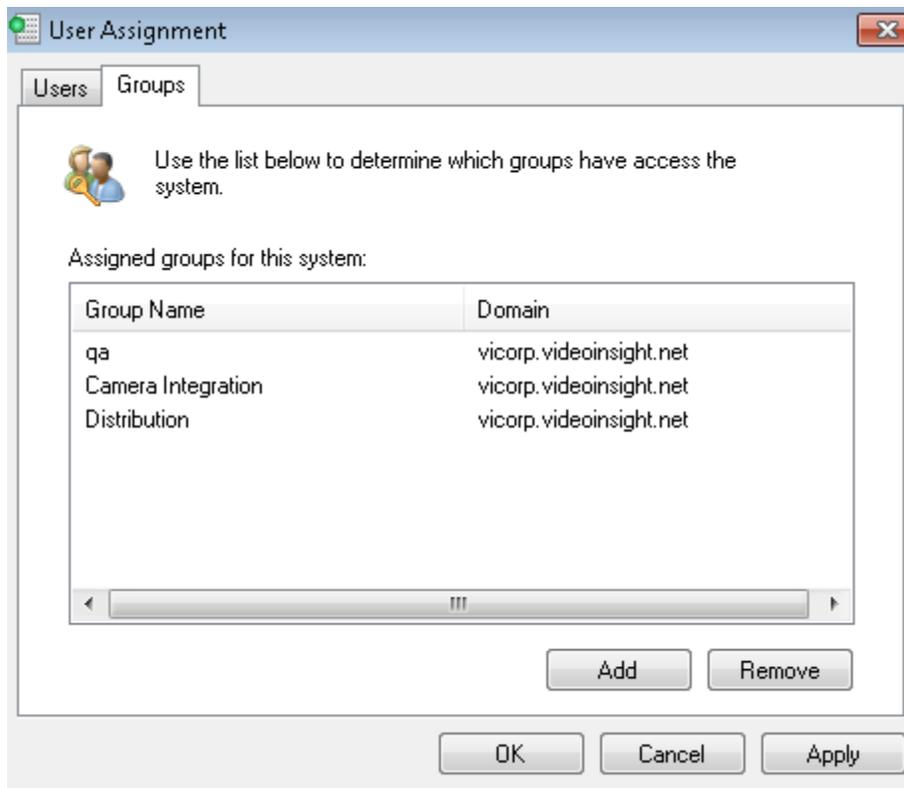
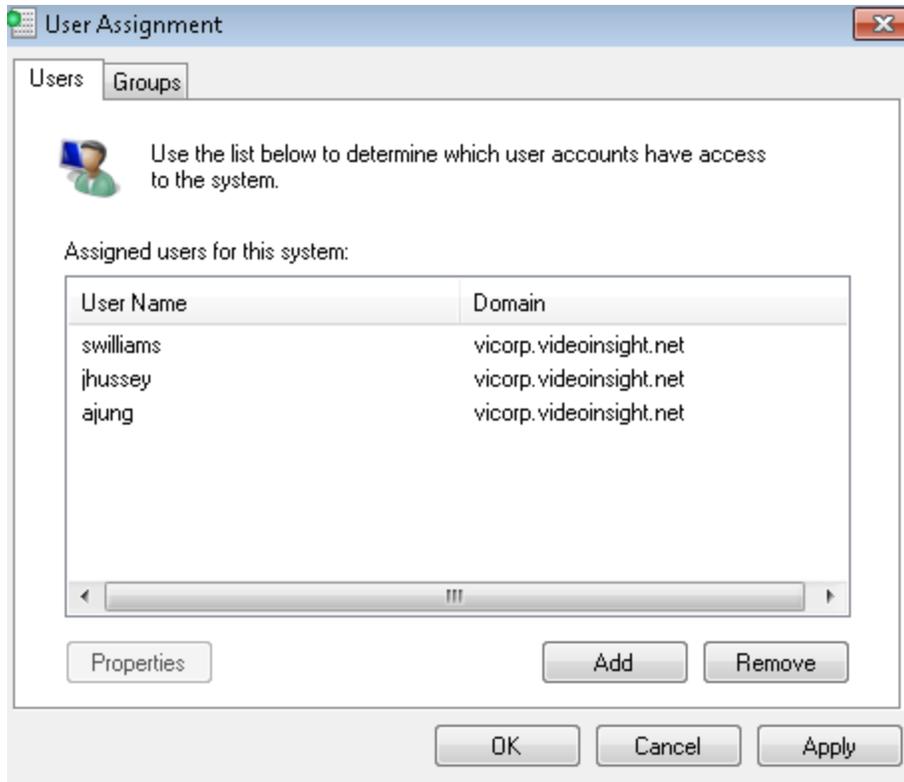




3. Enter the user or group name exactly as it appears in Active Directory and then click **OK**.



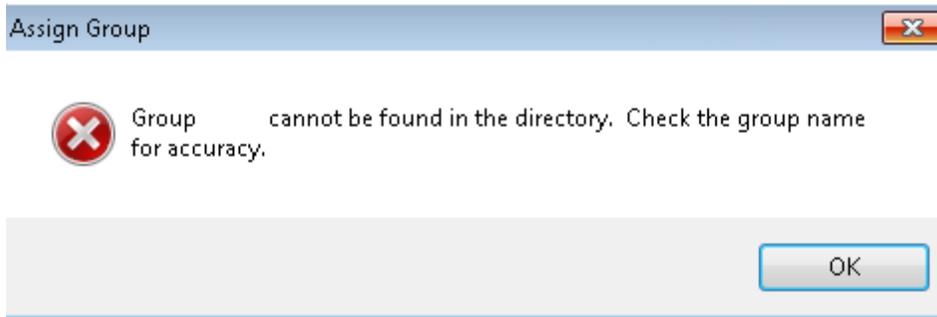
17. Click **Browse** to select a user or group from the list.
18. Select the user or group and then click **OK**.
19. Click **OK** again.



1. Click **Apply** and then click **OK**.
2. See Monitor Station [User Manager](#) for more information on how to import these users and groups.

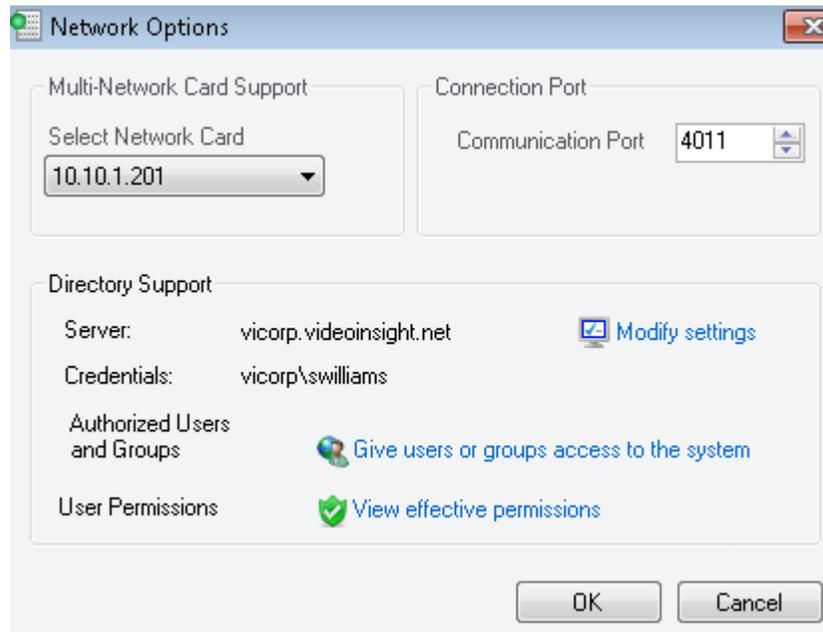
See [Login](#) for more information on how to login.

Entering an invalid user or group name displays an error message as shown in Figure below.

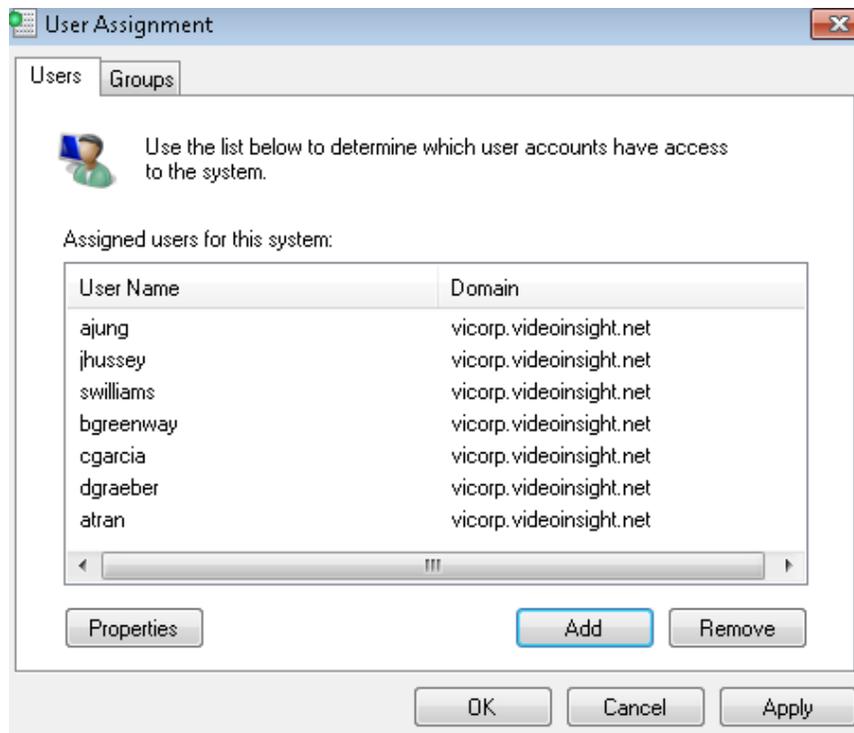


Removing users or groups

To remove Active Directory users and groups:



1. On the Network Options screen click Give users or groups access to the system.

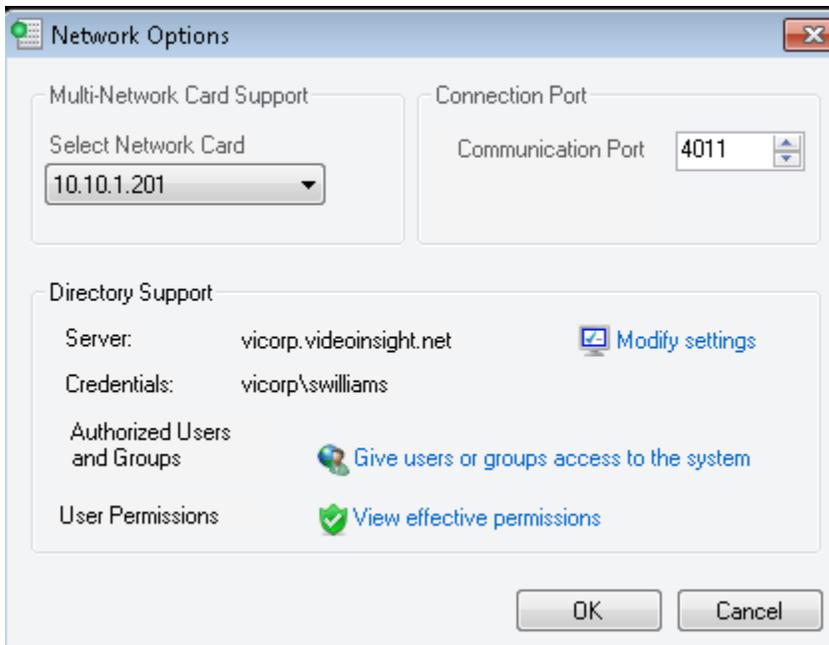


2. Select the user or users to remove and then click **Remove**.
3. Click **Apply**.
4. Click **OK**.

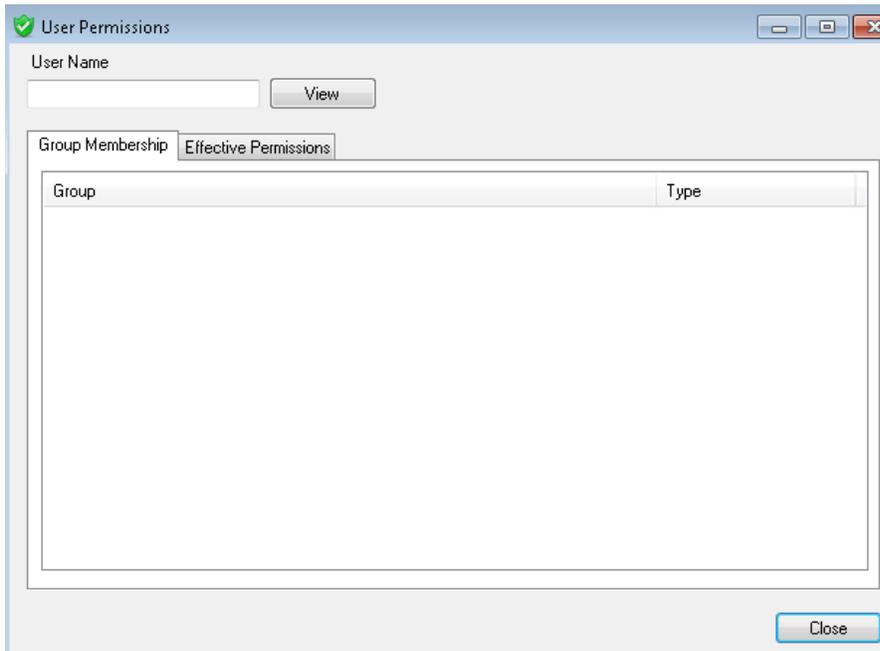
Viewing user permissions

IP Server and Active Directory are highly integrated. You can view the same user permissions using both.

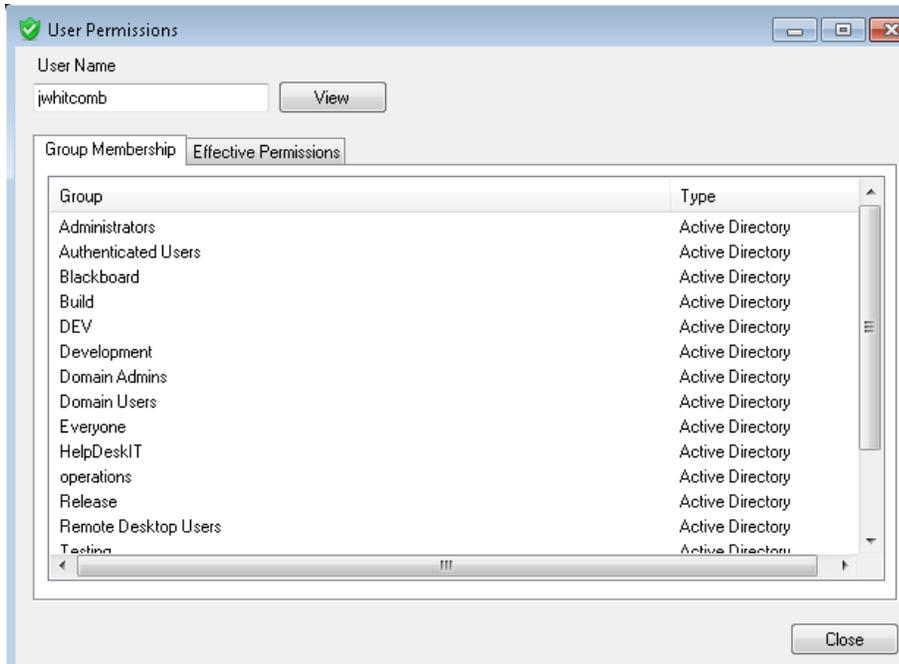
You can view user permissions in several places: Network Options, Add User and Monitor Station [User Manager](#).



1. On the Network Options screen click the View effective permissions.

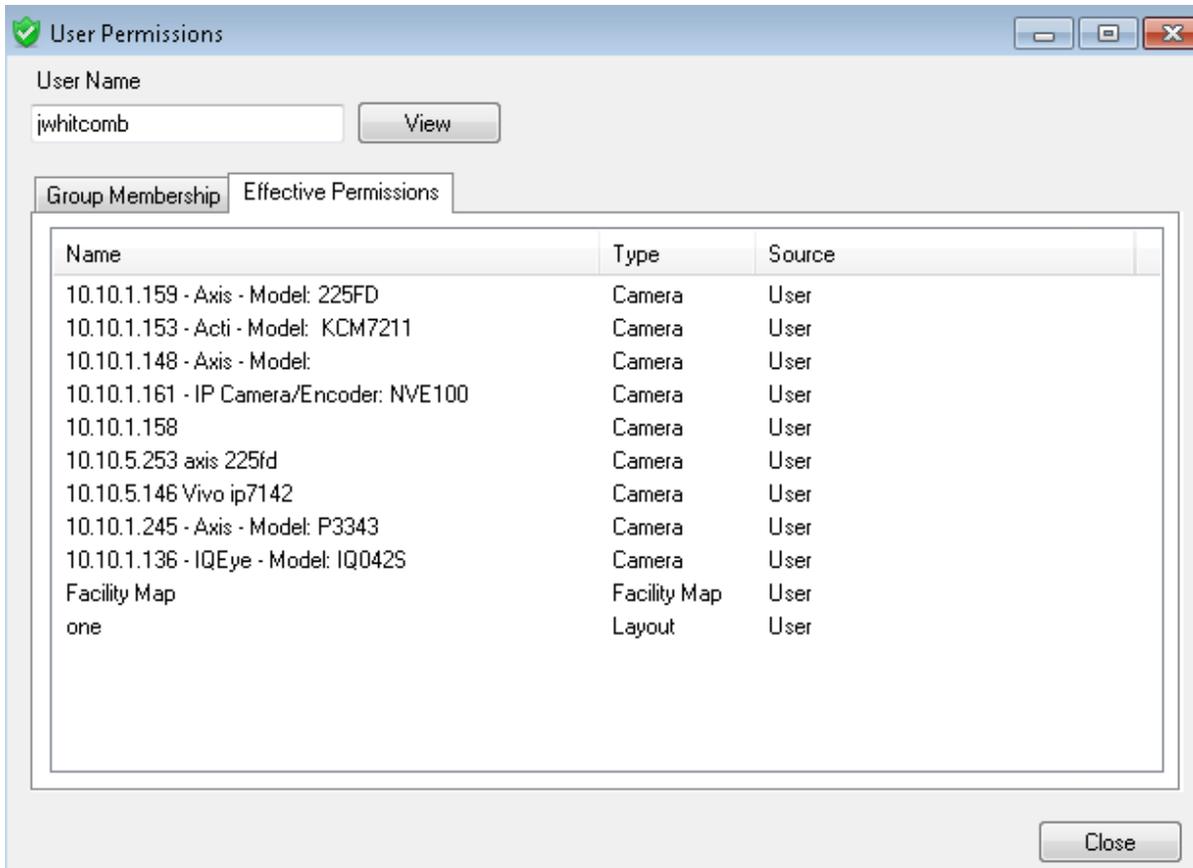


2. Enter the user name and then click **View**.



The Group Membership tab displays all Active Directory groups the user belongs to. You cannot make any changes on this tab.

The Effective Permissions tab displays all IP Server items the user has access to. You cannot make any changes on this tab. See [User Manager](#) for more information on modifying user permissions in Monitor Station.



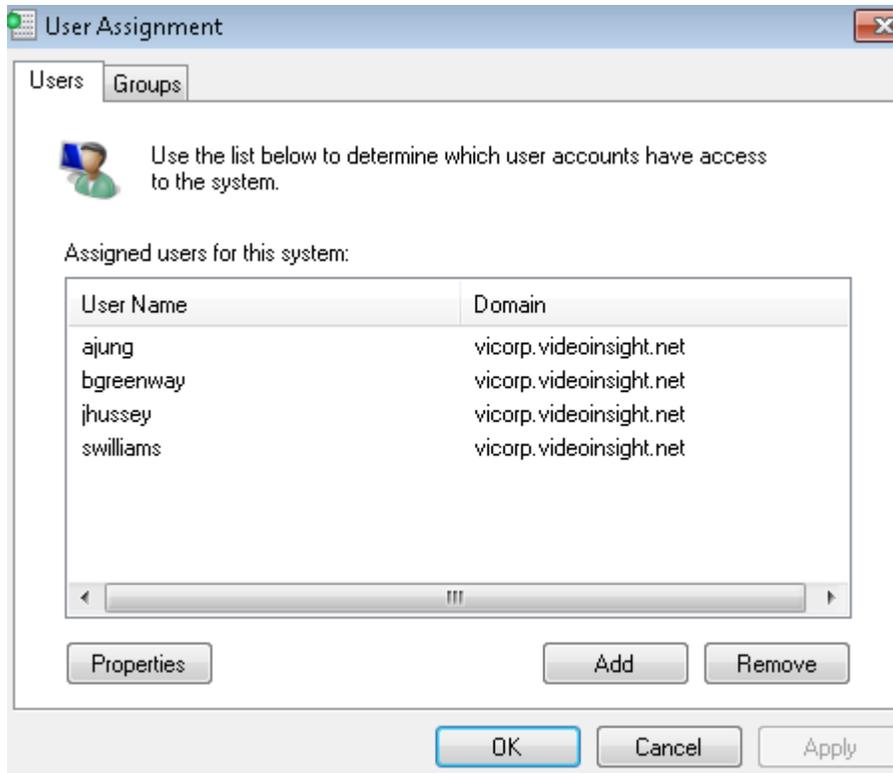
Name: Lists the object names the user has access to.

Type: Lists the object type the user has access to.

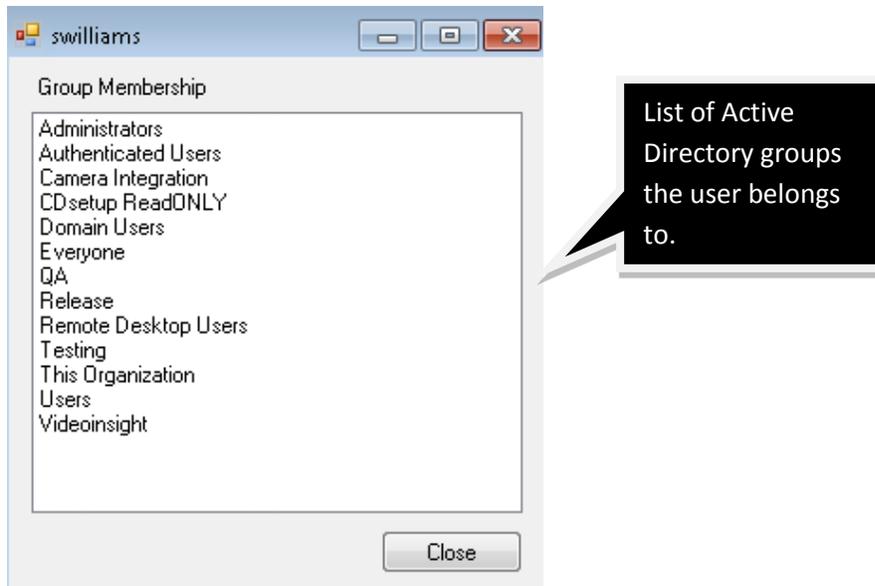
Source: Lists the source of the permission; in this example, the user was created individually and granted permissions exclusively, not as part of a group.

To view permissions from the User Assignment screen:

1. On the Network Options screen click Give users or groups access to the system.



2. Select a user name and then click **Properties**.



3. The Group Membership screen displays a list of Active Directory groups the user belongs to. Click **Close**.

LDAP (Lightweight Directory Access Protocol)

LDAP is the information technology standard way of accessing a directory service over a TCP/IP network. Active Directory is Microsoft's directory service. Some other directory services are Novell eDirectory and OpenLDAP. Directory services store, organize and provide access to information in a directory containing information about users, computers and permissions.

LDAP uses Distinguished Name (DN) as the syntax to identify objects in the directory. The DN is composed of four discrete name parts:

- CN – Common Name – For example, Jane Doe
- OU – Organizational Unit – For example, Sales
- DC – Domain component – For example, mydomain
- Domain component – For example, net

The DN reads from left to right, from the most specific part of the node to the least specific node on the right. The root of the DN is actually the last two parts (for example, mydomain.net).

See [Active Directory](#) for more information on managing users using LDAP. The process to manage users in both systems is the same.

Checksum

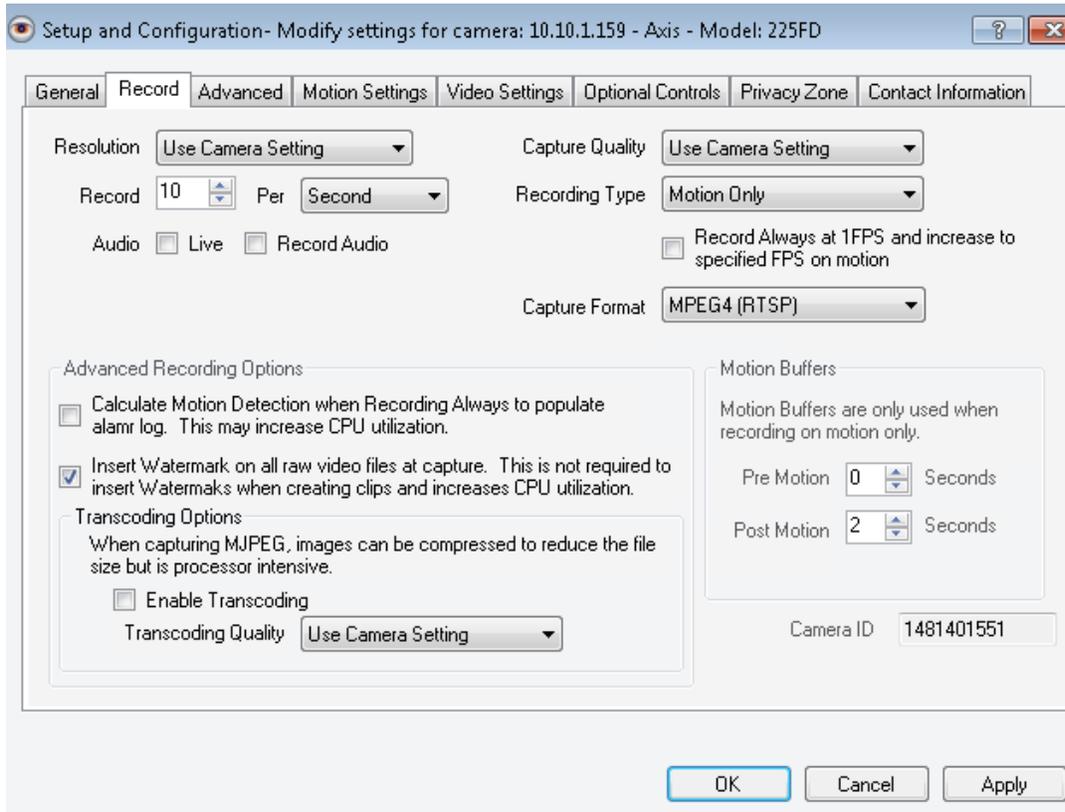
The checksum logic incorporated into Video Insight software prevents modification to recordings that can be made using other software. This feature guarantees the authenticity of the recording and ensures the delivered recording has not been tampered with. This is important when using recordings as evidence in legal proceedings. Video Insight uses MD5 checksum logic.

Enabling this feature is processor intensive because the server decompresses and recompresses each image to interlace the watermark. You can interlace the watermark into clips or full recordings. The watermark is invisible to the naked eye and can only be verified using our Standalone Player utility.

Enabling CheckSum Watermark

1. Start Monitor Station.
2. Select a camera from the left navigation tree.
3. Right-click the camera node and select Properties.
4. Click the Record tab.

5. Click the Advanced tab.



6. Check the box to Insert Watermark on all raw video files at capture.
7. Click **Apply** and then click **OK**.

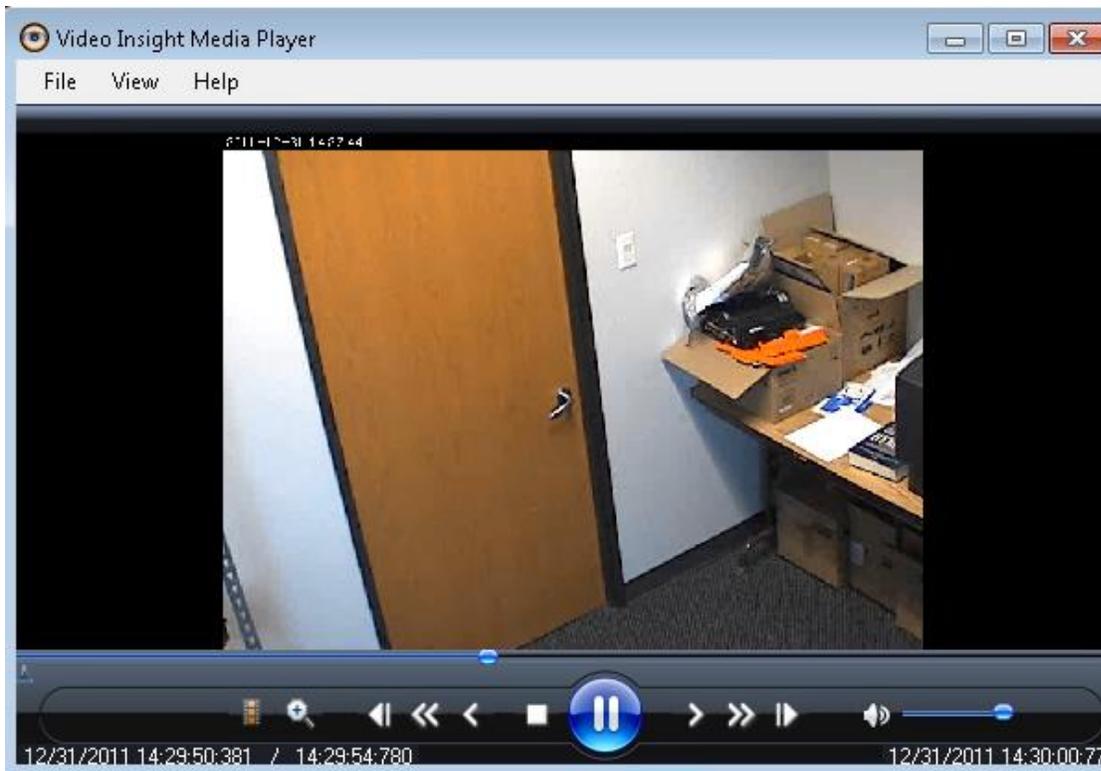
You can verify a video has not been tampered with by using the Standalone Player utility provided in the full DVD download for your operating system type.

Verifying a CheckSum Watermark

1. Start the Standalone Player utility (also called Video Insight Standalone Media Player).



2. Click the File menu and then select Open to navigate to the file that needs verification.
3. Select the file and then click **Open**.



4. Click the File menu and then select Check Water Mark.
5. The player will check the file and if the video is watermarked and has not been tampered with, it will display a verification message. Click **OK**.



6. The player displays a different message if the file does not have a watermark or has been tampered with.

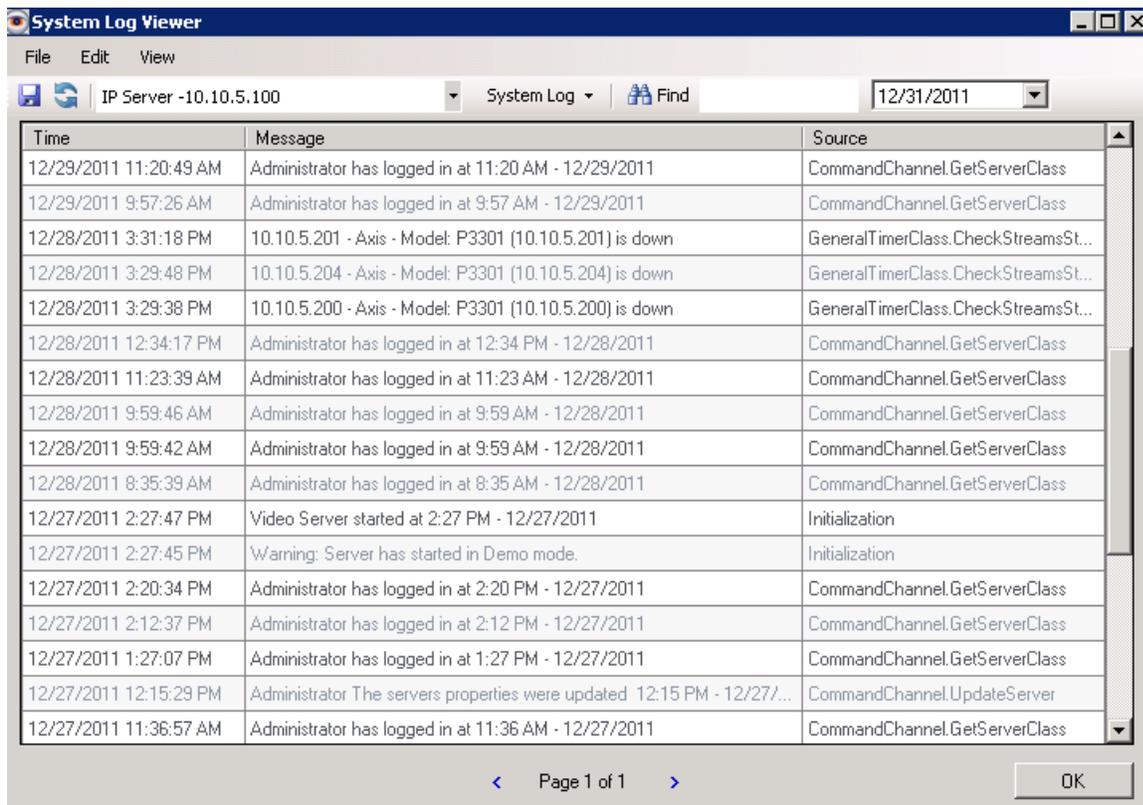


System Log

Reviewing the System Log is a good way to identify user actions, server and camera messages as well as obtain any error logs which can aid in troubleshooting.

You can access the System Log from several areas of the application, but the functionality and available actions are the same.

1. Start the System Log.



Note

The number of pages available and saved in the database depends on the System Log setting. You can change this setting on the Advanced Tab of Server Properties. The default is 30 days and the maximum is 1000 days.

 = The Save icon exports the System Log. Clicking it displays three options:



 = The Refresh icon refreshes the System Log.

 = This drop-down menu selects the server. All servers added to Monitor Station with a status of Connected display here. However, if you are using the [IPSM Diagnostics System Log](#) all servers in a shared database will appear, regardless of their connection status.

 = This drop-down menu selects the type of log to view. System Log is the default.

 = The field next to this icon allows you to search for a specific string.

 = The calendar control selects the “through” date of the logs. For example, when 12/31/2011 is selected all logs available up to and including 12/31/2011 display.

System Log Entry			
Message	Source	Explanation	Resolution
Warning: Server has started in Demo mode.	Initialization	A reminder that this server is in Demo mode	Upgrade to a fully licensed version to avoid this message
Video Server started at 2:45 PM - 12/22/2011	Initialization	Message will appear each time the server is started whether manually or using Auto Restart	Informational message
Administrator has logged in at 2:45 PM - 12/22/2011	CommandChannel.GetServerClass	User logged in to Monitor Station	Informational message
Administrator The servers properties were updated 12:15 PM - 12/27/2011	CommandChannel.UpdateServer	Administrator happens to be the user (security is likely off) that updated server properties	Informational message
ErrCode: 0 -Fail to write file: c:\video\127.0.0.1-1963630245\12.31.2011\18h17m14s.avi	(10:0:8)	Camera failed to write to path listed	Check permissions: could be due to an invalid path, the folder may have been moved or rights to write to that folder have changed
Cannot delete folder:(c:\video\127.0.0.1-1794956641\12.22.2011)	GeneralTimer.CleanDrive()	Deletion routine is unable to delete the folder	If one of the files is currently being viewed or is locked for another reason the folder cannot be deleted. The server deletion routine will now revert to deleting one file at a time in this folder instead

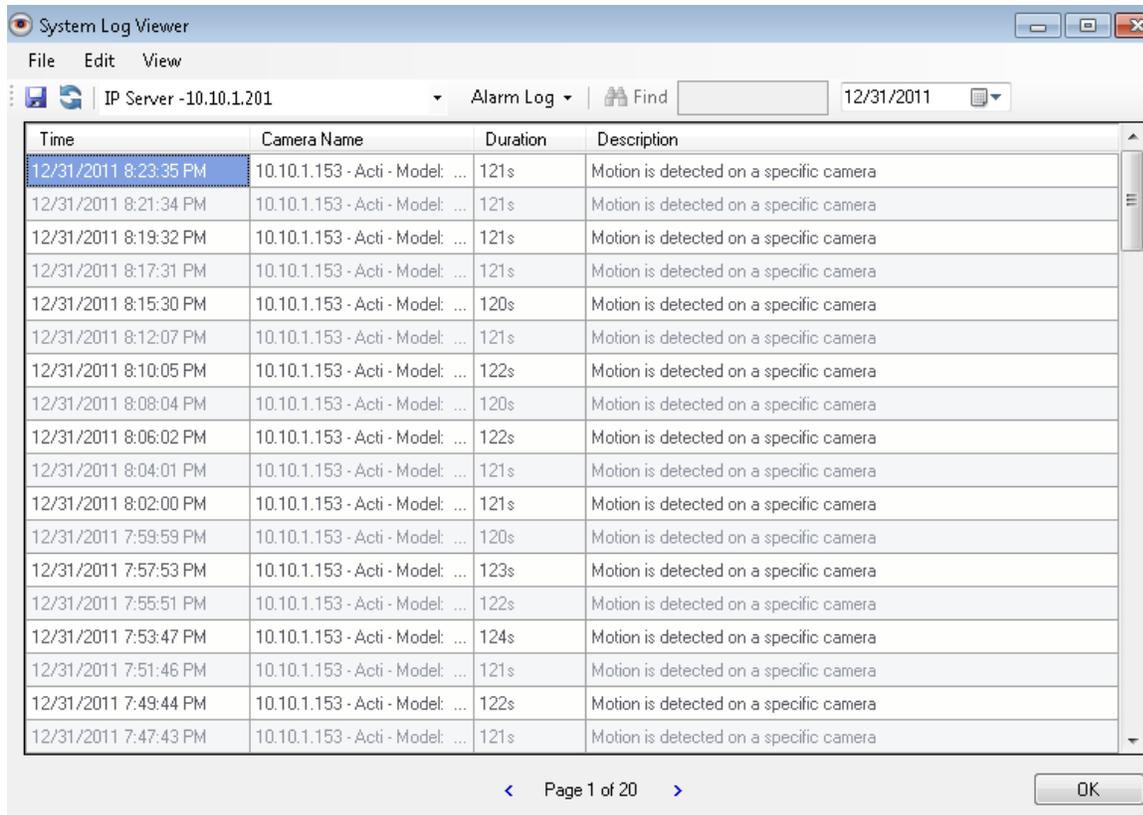
Video Server Task: DIO-Alarm Log	Task Manager	This entry is due to a rule that was just triggered	Informational message
10.10.5.151 - Axis - Model: P3301 (10.10.5.151) is down	GeneralTimerClass.CheckStreamsStatus	Camera streaming is down	The server will continue to attempt to restore connection.
Could not find a part of the path 'c:\video\10.10.5.148-453894083'.	System.IO.__Error.WinIOError(20:0:1)	Unable to find write path	Check the path and that the camera is indeed still added to the server with that Camera Unique ID
Restart Request	CommandChannel.RemoveCamera	A client has requested a server restart	The next time the IPSM is running it will process the request automatically
Video Server was shut down at 2:58 PM - 12/22/2011	Board.Close	The server was properly shutdown	Each time a server is stopped either manually or using Diagnostics this informational message will appear.
10.10.5.212 - Hikvision - Model: Universal (10.10.5.212) is restored	GeneralTimerClass.CheckStreamsStatus	Camera connectivity is restored	The server was able to resume connection.
Object reference not set to an instance of an object.	Videoin sight.LIB.AccessControl_BlackBoard.CheckForNewEvents(200:0:45)	Access Control Blackboard is configured for specific cameras and constantly checks for new alarms. The camera can no longer be found, it was removed from the server.	Change the camera in Blackboard or re-add the original camera to the server.
No Security granted user JWhitcomb permission to map Facility Map (ID:1073740123)	CommandChannel.UserUpdate	Security was off on this server when the JWhitcomb user was	Informational message

10:57 AM - 12/31/2011		granted access to a Facility Map	
vicorp.videoinsight.net\swilliams has logged in at 6:39 PM - 12/31/2011	CommandChannel.GetServerClass	A user logged in with Active Directory or LDAP and security was on	Informational message
vicorp.videoinsight.net\swilliams updated camera properties at 12/31/2011 2:29:22 PM : Camera login,	CommandChannel.UpdateCamera	Specific LDAP or Active Directory user made changes to a camera	Informational message
vicorp.videoinsight.net\swilliams [GetUserGroupMembership]	LDAP Authentication	Prior to actually logging an Active Directory/LDAP user login in the server authenticates the user against Active Directory/LDAP	Informational message
Access to the path 'C:\Program Files\VI Enterprise\Enterprise Service\app\mycamera.bin' is denied.	System.IO.__Error.WinIOError(9:0:1)	The action performed at this time did not have the right access to write to that folder	Check the user logged in, they should have local admin rights
Login successful for User ID administrator User Address : ::1	WebClient	With security enabled Web Client users logins are also captured	Informational message
A New Camera was added at 12:41 PM - 12/2/2011	CommandChannel.AddNewCamera	User added a new camera to this server	Informational message

Alarm Log

The Alarm Log is a list of all motion events for all cameras set to Motion-only recording or Record Always with the Calculate Motion Detection When Recording Always option selected on the Record tab.

1. Start the System Log.
2. Click the View menu and then select Alarm Log.



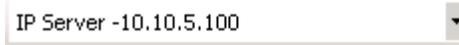
Please Note: The number of pages available and saved in the DB depends on the Alarm Log setting in Server properties, Advanced tab, discussed on page 39; the default is 30 days and the maximum is 1000 days.

The camera name and event duration displays for all motion events. You have several options on this screen.

 = The Save icon exports the Alarm Log. Clicking it displays three options:



 = The Refresh icon refreshes the Alarm Log.

 = This drop-down menu selects the server. All servers added to Monitor Station with a status of connected display here. However, if you are using the [Diagnostics System Log](#) all servers in a shared database will appear, regardless of their connection status.

 = This drop-down menu selects the type of log to view. System Log is the default.

 = Search functionality is disabled in this view.

 = The calendar control selects the “through” date of the logs. For example, when 12/31/2011 is selected all logs available up to and including 12/31/2011 display.

Cameras

IP Server supports over 2300 cameras. Video Insight adds support for new cameras as part of its ongoing development process.

Adding cameras

Note

You can also access Server Properties by right-clicking the server name in the left navigation tree and selecting Properties and then Cameras.

You can add cameras during or after an install or upgrade.

1. Start Monitor Station.
2. Enter the user name and password if Security is enabled or click **OK** to login.
3. From the main dashboard navigate to Administration and then Setup and Configuration.
4. Select your server from the left navigation tree.
5. Click the Camera tab.

Automatically

This wizard searches your current network segment for online IP cameras. When it detects one it examines the MAC address to determine the manufacturer. It then accesses the camera using the user name and password. If the camera responds successfully, the software obtains the camera model.

On the Cameras tab click **Auto Discovery**. The figure below shows a sample result.

Manually

On the Cameras tab click **Manual Add**.

Camera Name: Enter the camera name or IP address. The default is Camera Name.

Note

For PTZ capable cameras a “Disable PTZ” checkbox will also appear. Check it if you need to disable PTZ for users. Disabling PTZ also disables PTZ Presets.

Time Stamp: Use this option to stamp all recorded video with the server time. If you select “Burn Time Stamp on Video” and the camera does not support this feature, the server will do it; however, this uses additional CPU which can affect overall performance.

Manufacturer and Model: Choose the manufacturer and model of the camera here. The software supports a wide variety of camera models from major camera manufacturers. Every camera has its own mechanism for communicating with the server. Selecting the correct model informs the system with specific information about the camera such as communication method, DIO support, compression type and whether it supports audio. If your camera model is not found, try the ONVIF universal protocol offered on most cameras.

IP Address: Enter the camera’s IP address or domain name. If entering a domain name, do not include http:// or www.

Camera Credentials: Enter the camera’s user name and password. Some manufacturers require credentials to view live images and others only when modifying camera settings. Video Insight recommends entering credentials when security is enabled on the camera for proper integration and to configure certain features on the camera such as side motion detection or camera flip.

Shared IP Address: This checkbox should be used with cameras such as those from Arecont. Arecont is a four lens camera available in 180- or 360-degree views that use only one license. Adding it to the system requires entering the camera information four times, selecting a different channel number (1-4) each time. If you are adding a single lens camera leave this box unchecked.

Alternate Ports: If you are adding a camera or encoder that reports to a port other than the standard port of 80, change it under this section. Check the box for Alternate Ports and enter the proper port or ports.

Web Access: The Web Access link becomes active after you add the camera’s information. Click it to verify camera connectivity. Camera manufacturers use different interfaces and setup functionality at the camera level. Clicking the link displays an image of the camera. If no image displays, the most likely reason is an incorrect IP address or credentials.

Removing cameras

Note

Cameras are never truly deleted; they become unassigned. To add a deleted camera to another server sharing the same database click **Load** to view Unassigned Cameras.

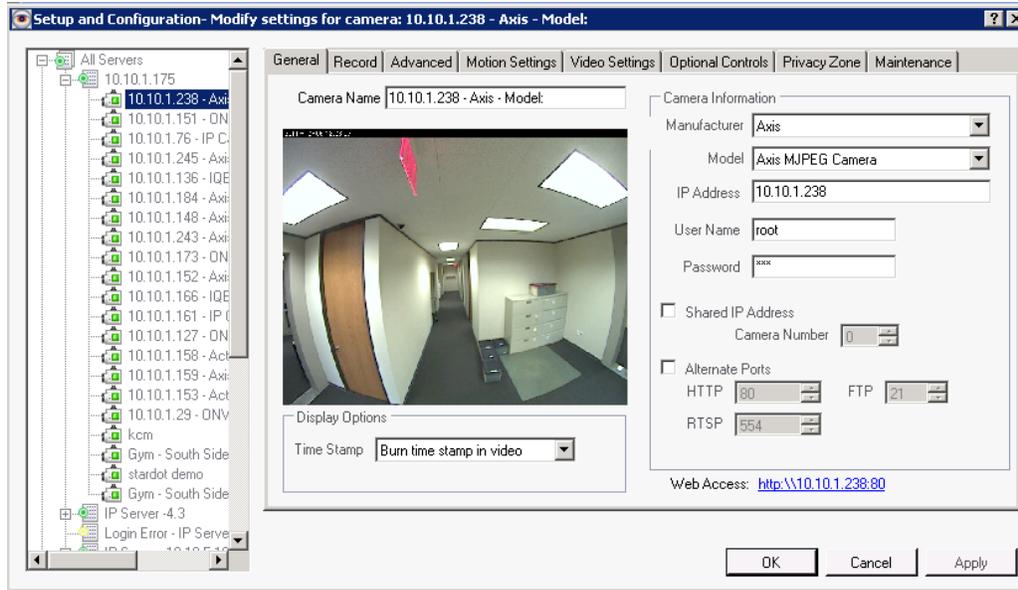
To remove a camera:

1. Start Monitor Station.
2. Enter the user name and password if Security is enabled or click **OK** to login.
3. From the main dashboard navigate to Administration and then Setup and Configuration.
4. Select your server from the left navigation tree.
5. Click the Camera tab.
6. Double-click the camera to be removed from the Cameras to be Monitored pane. The camera now displays in the Unassigned Cameras pane.
7. Click **Apply** and then **OK**.

Modifying camera details

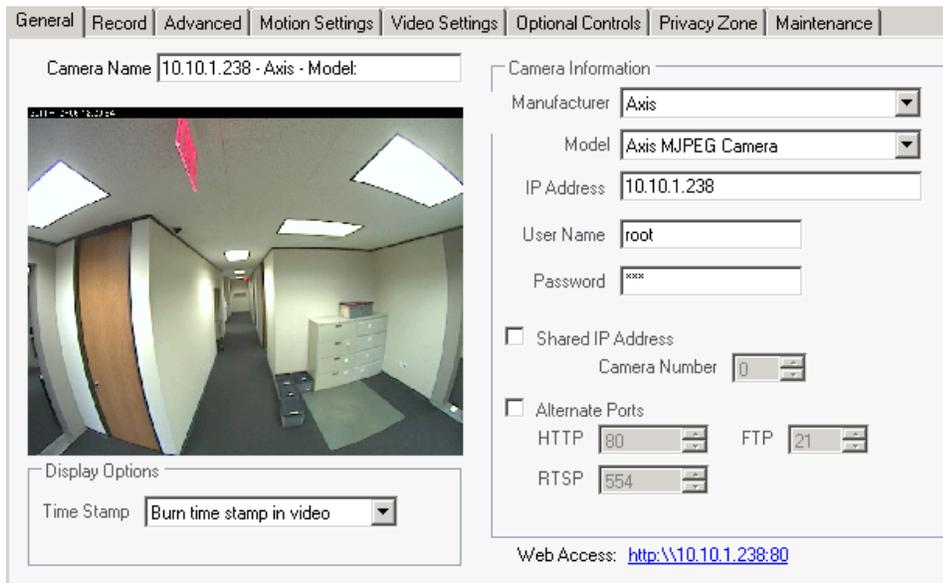
You may need to modify or tweak camera details after installation or as the environment changes. You may also need to apply new camera firmware. To modify camera details:

1. Navigate to Administration and then Setup and Configuration.
2. Expand the All Servers node from the left navigation tree.



Each tab is explained in detail below.

General tab



Camera Name: Enter the camera name or IP address. The default is Camera Name.

NOTE: For PTZ capable cameras a 'Disable PTZ' checkbox will also appear, check it if you'd like to disable PTZ for users. Disabling PTZ will also disable Presets.

Time Stamp: Use this option to stamp all recorded video with the server time. If you select “Burn Time Stamp on Video” and the camera does not support this feature, the server will do it; however, this uses additional CPU which can affect overall performance.

Manufacturer and Model: Choose the manufacturer and model of the camera here. The software supports a wide variety of camera models from major camera manufacturers. Every camera has its own mechanism for communicating with the server. Selecting the correct model informs the system with specific information about the camera such as communication method, DIO support, compression type and whether it supports audio. If your camera model is not found, try the ONVIF universal protocol offered on most cameras.

IP Address: Enter the camera’s IP address or domain name. If entering a domain name, do not include http:// or www.

Camera Credentials: Enter the camera’s user name and password. Some manufacturers require credentials to view live images and others only when modifying camera settings. Video Insight recommends entering credentials when security is enabled on the camera for proper integration and to configure certain features on the camera such as side motion detection or camera flip.

Shared IP Address: This checkbox should be used with cameras such as those from Arecont. Arecont is a four lens camera available in 180- or 360-degree views that use only one license. Adding it to the system requires entering the camera information four times, selecting a different channel number (1-4) each time. If you are adding a single lens camera leave this box unchecked.

Alternate Ports: If you are adding a camera or encoder that reports to a port other than the standard port of 80, change it here. Check the box for Alternate Ports enter the proper port or ports.

Web Access: The Web Access link becomes active after you add the camera’s information. Click it to verify camera connectivity. Camera manufacturers use different interfaces and setup functionality at the camera level. Clicking the link displays an image of the camera. If no image displays, the most likely reason is an incorrect IP address or credentials.

Record tab

The screenshot displays the 'Record' tab configuration window. At the top, there are tabs for 'General', 'Record', 'Advanced', 'Motion Settings', 'Video Settings', 'Optional Controls', 'Privacy Zone', and 'Maintenance'. The 'Record' tab is active.

Key settings visible include:

- Resolution:** Use Camera Setting (dropdown)
- Capture Quality:** Use Camera Setting (dropdown)
- Record:** 10 (spin box) Per Second (dropdown)
- Recording Type:** Motion Only (dropdown)
- Record Always at 1FPS and increase to specified FPS on motion
- Capture Format:** MJPG (dropdown)

Advanced Recording Options (grouped in a box):

- Calculate Motion Detection when Recording Always to populate alarm log. This may increase CPU utilization.
- Insert Watermark on all raw video files at capture. This is not required to insert Watermarks when creating clips and increases CPU utilization.
- Transcoding Options:**
 - When capturing MJPEG, images can be compressed to reduce the file size but is processor intensive.
 - Enable Transcoding
 - Transcoding Quality:** Use Camera Setting (dropdown)

Motion Buffers (grouped in a box):

- Motion Buffers are only used when recording on motion only.
- Pre Motion:** 0 (spin box) Seconds
- Post Motion:** 2 (spin box) Seconds

At the bottom right, the **Camera ID** is displayed as 40996983.

Resolution: Most cameras can support multiple resolutions. You can change camera resolution using the Web Access link. You can also change camera resolution without going to the camera itself. Unfortunately, camera manufacturers have different ways of expressing resolutions. For example, Axis expresses resolution in CIF, 2 CIF, 4 CIF and D1 whereas ACTi expresses resolution in more common terms such as 1280 x 1024 and 640 x 480. Resolution settings in this option are more generic and are mapped to the appropriate resolution based on the camera. You can select from Lowest to Highest, as well as the default setting of Use Camera Setting. Video Insight recommends using the highest setting for high resolution cameras. You cannot change the resolution if this option is not available.

Record and Per: The software can capture images at between 1 and 30 frames per second (FPS). The higher the FPS, the more fluid motion will be. A higher FPS setting requires more storage. Adjusting FPS settings per camera optimizes storage space. These values do not represent what the camera is producing, but what the server is willing to accept. Available bandwidth and camera performance may result in a FPS lower than what is set, but never higher. "Frames Per" defaults to seconds, but you can also choose Minute, Hour or Day. This is useful in time lapse situations.

Capture Quality: If the camera allows it, this setting modifies its capture quality. Settings range from Lowest to Highest. You can also select Use Camera Setting, which defaults to the camera's native setting. The higher the quality the image, the larger the image size. If the camera does not have settings for quality, this option is unavailable.

Note

Audio options will appear if the camera supports audio. Enable Audio – Capture live and listen using Monitor Station. Record Audio – Capture Live and Record with Video. Note that Enable Audio must be set in order Record Audio.

Recording Type: There are four recording type options. The default is Motion-only.

Record Off: Images are not recorded but live images are still available. If the camera offers live audio, it is also available if selected.

Record Always: Images are recorded 24 hours a day, seven days a week. This setting consumes a lot of storage. See [Storage Consideration](#) for more information on storage consumption.

Motion-only: Images are only recorded when motion is detected. Motion sensitivity depends on motion zones, camera environment and sensitivity settings. Camera Pre and Post settings are also taken into account. See the [Motion Settings tab](#) for more information on motion settings.

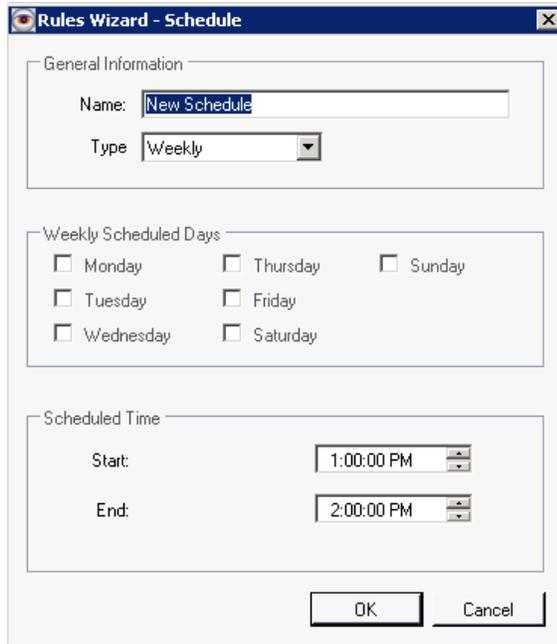
Schedule: Images are recorded per a defined schedule. This setting is useful in reducing storage consumption when combined with Record Always. Selecting Schedule displays a Config button next to Recording Type. To setup a Scheduled Recording Type:

1. Click **Config**.

The screenshot shows a window titled "Camera schedule" with a close button (X) in the top right corner. Inside the window, there is a text box with the following text: "Scheduled recordings are done by starting with the camera in the off position. Then add the scheduled times for recording always, and recording with motion." Below this text box, there are two sections for scheduling. The first section is labeled "Schedule(s) for record always" and contains a table with two columns: "Name" and "Type". Below the table are three buttons: "Modify", "Delete", and "Add". The second section is labeled "Schedule(s) for record motion" and also contains a table with two columns: "Name" and "Type". Below this table are three buttons: "Modify", "Delete", and "Add". At the bottom of the window, there are two buttons: "OK" and "Cancel".

The process to add a schedule to record always and record motion is the same. Record motion takes into account the Pre- and Post-motion settings of the camera.

1. Click **Add**.



The screenshot shows a dialog box titled "Rules Wizard - Schedule". It is divided into three main sections:

- General Information:** Contains a text field for "Name" with the value "New Schedule" and a dropdown menu for "Type" set to "Weekly".
- Weekly Scheduled Days:** A grid of checkboxes for each day of the week: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday. All checkboxes are currently unchecked.
- Scheduled Time:** Two time selection fields. "Start" is set to "1:00:00 PM" and "End" is set to "2:00:00 PM".

At the bottom of the dialog are "OK" and "Cancel" buttons.

2. Enter a schedule name.

3. Select the occurrence type.

- Weekly-** The camera will record weekly on the days selected. Holidays are not taken into account.
- One Time-** The camera will record one time on a scheduled day with beginning and ending at specified times. Should the rule not be able to run due to Server or Network problems, the rule will NOT execute.
- Daily-** The camera will record on a selected day, week day or weekend day. Holidays are not taken into account and the rule will execute as usual.
- Monthly-** The camera will record monthly on a specific date or dates. You can also combine a day with its recurrence, such as the fourth Friday of every month.

4. Enter the start and end time.

You can setup more than one schedule and type for each camera. In effect, the software is actually setting up a rule in Rules Manager. See [Rules Manager](#) for more information on setting up rules.

Capture Format: This option sets the format the camera uses to stream video from it to the server. Cameras vary in the formats they offer, as well as the number of streams allowed per format type.

Note

Drop-down lists, as well as their values, on the Record tab will change depending on the camera type selected due to the available capabilities of that camera.

MJPEG: MJPG format creates the largest file sizes due to the raw images received from the camera. If your camera only supports this format you may want to consider Transcoding for more efficient storage utilization; however, Transcoding is CPU intensive. See [Transcoding](#) for more information on this feature.

MPEG4: MPEG4 format images are slightly more compressed than MJPG format, but still much larger than current formats. MPEG4 absorbed many of the features of MPEG1 and MPEG2 and other related standards as well as AAC standardization for audio compatibility.

H.264: H.264 format is the current standard for streaming images from IP cameras. This format adds video compression used for HDTVs, Blu-Ray and other high quality video. It allows for higher quality with a lower bit rate, lower storage consumption and improved audio capture and playback.

In some cases you may notice a capture format with RTSP appended to it. Where this appears, Video Insight modified the capture format protocol to bridge the gap between the thin support provided by the Software Development Kit (SDK) and our customer's needs. The RTSP class offers tighter integration and avoids some known bugs when using the manufacturer-provided SDK. The RTSP class is not available or needed for all camera models and manufacturers.

Record Always at 1 FPS: This option is best used in conjunction with Motion-only recording. Its purpose is to combine the benefits of Record Always (no missed events) with Motion-only (only events). Recording always at one FPS reduces the storage consumed by Record Always yet still ensures smooth playback by switching to the higher frame rate defined in the Record field.

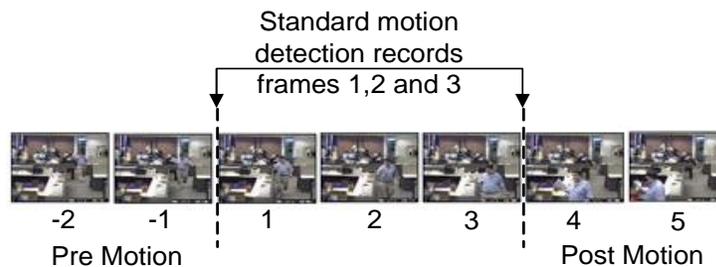
Calculate Motion Detection When Recording Always: Select this option to go with Record Always when you want the server to calculate motion percentages and include them in Timeline view and Media Player as motion events. Doing so increases CPU utilization, but accessing motion events immediately instead of viewing video of non-events may be worthwhile.

Insert Watermark on all raw video files at capture: Select this option to ensure video integrity. The server interlaces all raw images with a checksum that can only be read or verified with Video Insight's CheckSum Utility found in the stand alone Media Player. See [Security](#) for more information on watermarking.

Transcoding: Transcoding was created to mitigate large files created by older cameras utilizing only the MJPEG format. Transcoding is a process performed by our server while the images are received and saved into the AVI container or file. MJPG images are received by the server and converted to WMV format while simultaneously compressing the images. This is a CPU-intensive process.

Many cameras on one server utilizing Transcoding can greatly affect server performance. Transcoding quality also determines CPU usage. The higher the transcoded quality the larger the image and thus the file size.

Motion Buffers: Motion Buffers are used when the camera is using Motion-only and ensures the pre- and post-motion pictures are also captured.



Note

MPEG4 Capture Format does not use motion buffers.

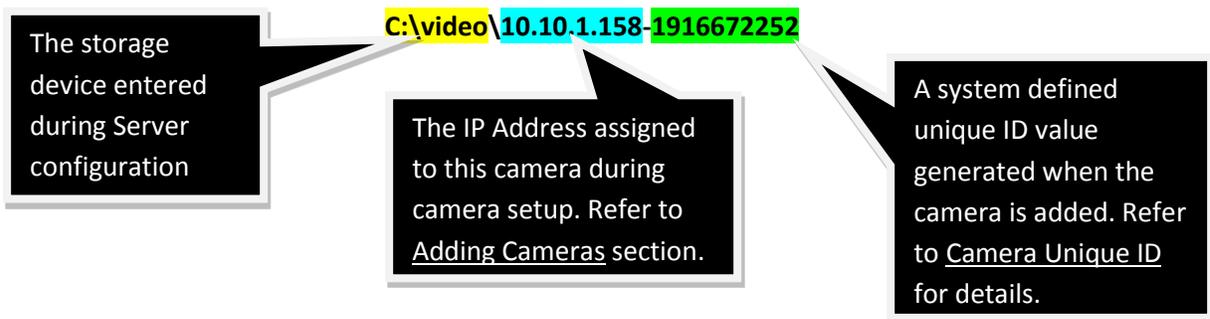
Camera ID: This is for reference only. A unique camera ID is added to each stream to identify it on the server. This ID also correlates to the exact folder where the camera's recordings are saved. Adding the same camera (as opposed to unassigning and reassigning cameras) creates a unique ID for each instance. In the case of a four-stream Arecont camera, adding the same camera IP address four times, once for each stream, creates a different folder of recorded video for each view.

Advanced tab

General	Record	Advanced	Motion Settings	Video Settings	Optional Controls	Privacy Zone	Maintenance
Storage Options Disk Space will be configured for the drive selected by the image location. Multiple cameras associated to the same drive will use the same settings.			Camera transmission preferences				
Max Disk Space <input type="text" value="0"/> (in GB)			Live Maximum Refresh Rate <input type="text" value="5"/> Frames per Second				
Image Location <input type="text" value="C:\video\10.10.1.158-1916672252"/>			Optimize Video Streams				
Max File Size <input type="text" value="200"/> (in MB)			<input checked="" type="radio"/> Use server default				
			<input type="radio"/> Low CPU \ High Bandwidth				
			<input type="radio"/> High CPU \ Low Bandwidth				

Max Disk Space: This option specifies the maximum amount of disk space each camera can use, in gigabytes. If set to zero, camera recordings will defer to the server disk space minimum before the deletion logic triggers to delete the oldest recordings.

Image Location: Recordings for each camera can be stored in different folders and across multiple hard drives. The recording path is a combination of values entered during server and camera setup, and is specific to the configuration. For example:



Max File Size: Each camera records to a unique file that is limited to 200 MB by default. A new file is created when the limit is reached. Different camera settings will create more or less files as a result. For example, if you have a camera set to 3 FPS with motion activation, the system might only use one file for the entire day. In contrast, the same camera set to record always might result in five 200 MB files for the day. The system creates a new file when the file size reaches the specified size. The system automatically creates a new file for each camera at midnight, regardless of the current recording file size.

Note

The record “time” of the 200 MB files varies depending on several factors: Bit-rate, Quality, Resolution, Compression format and Recording type. As a result, some files may contain only two minutes of video and others two hours of video.

Live Maximum Refresh Rate: This option is used to set live refresh frame rates sent to Monitor Station or Web Client. Using lower FPS saves bandwidth. This camera-level setting overrides the server’s settings for this camera.

Optimize Video Streams: This option affects the video streams from the IP Server to Monitor Station and Web Client. There is a tradeoff between bandwidth utilization and CPU utilization.

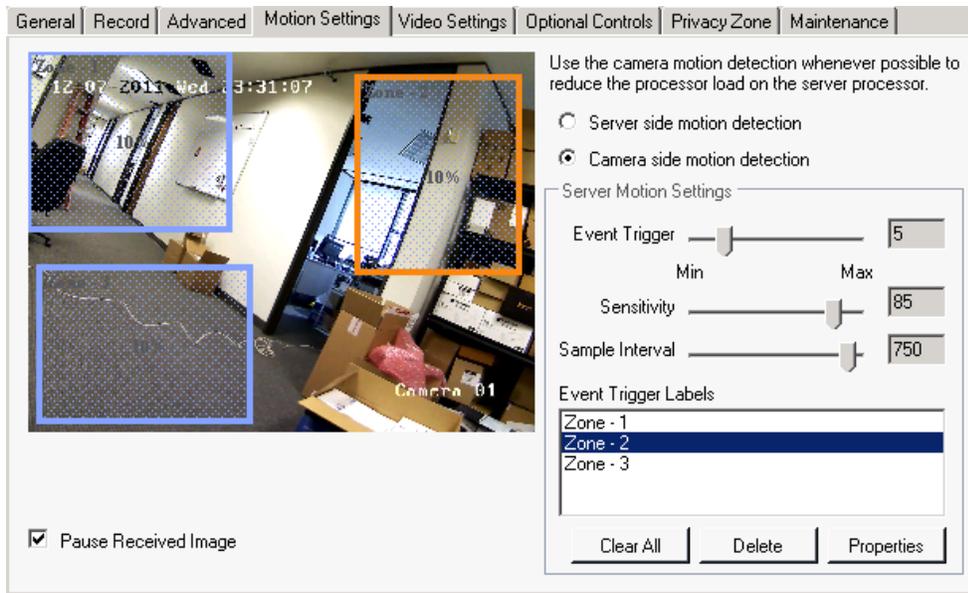
When you optimize for a low bandwidth environment, video compression occurs at the server. The server then sends a compressed MPEG4 image to the Monitor Station and Web Client. When you optimize for a high bandwidth environment, no compression occurs at the server. Uncompressed images are sent to the Monitor Station and Web Client.

User server default- This setting defers to server default options.

Low CPU\High Bandwidth- This setting sends uncompressed images directly to the Monitor Station and Web Client.

High CPU\Low Bandwidth- This setting compresses the image, sends them and then decompresses them. It allows the system to get a much higher frame rate over slower networks.

Motion Settings tab



Note

You can create unlimited Motion Zones when using Server-Side Motion detection.

Camera and encoder motion detection capabilities can differ greatly from model to model. One camera may offer partial motion detection with multiple zones and another only one motion zone which spans the entire image.

Pause Received Image: Check this box to pause the received image while you create a motion zone. Leaving it unchecked can cause the motion zone to flicker while it is being created.

Server side motion detection: Use this setting if the camera does not support side motion detection. The server compresses each image and is **extremely processor intensive**.

Camera side motion detection: Use this setting if the camera supports side motion detection. When camera detection is used, there is no need to decompress the image and server CPU utilization is not affected.

Server Motion Settings: This setting is only enabled if Camera side motion detection is selected.

Event Trigger: The Event Trigger slider determines how large or small an event or object) the motion trigger looks for when determining whether something is considered motion or not. Moving the slider to the right reduces software alertness, causing it to only watch for larger, more distinct changes. Moving the slider to the left raises software alertness, causing it to watch for less distinct changes. Setting the Event Trigger closer to maximum generates more recordings. The camera records more events, but

many can be “false positives.” The sliding bar below the live image shows the current Event Trigger level. The maximum event or object size is 30. This is 100% of the image area, or a very large event or object.

Sensitivity: The Sensitivity slider sets proximity distance thresholds for any changes to be counted in determining motion. At high sensitivity, a random pixel change across the picture from another pixel change would be added to the sum of other changes to determine if motion thresholds have been met. At low sensitivity, the changes must be in close proximity to other changes or they will be ignored. To increase sensitivity, move the slider bar to the right. To decrease sensitivity, move the slider bar to the left.

Sample Interval: This option is only available if Server side motion detection is selected. The Sample Interval slider determines the interval time in milliseconds the server checks for changes. To increase the frequency the server checks for changes, lower the value. To decrease the frequency the server checks for changes, increase the value.

Setting up Motion Zones: Motion Zones are areas created within the image that the camera monitors for motion. Motion Zones allow for more precise motion detection. When combining Motion Zones with Motion-Only recording, the camera will ignore certain areas in its view. You can create a Motion Zone in the Event Trigger Labels section.

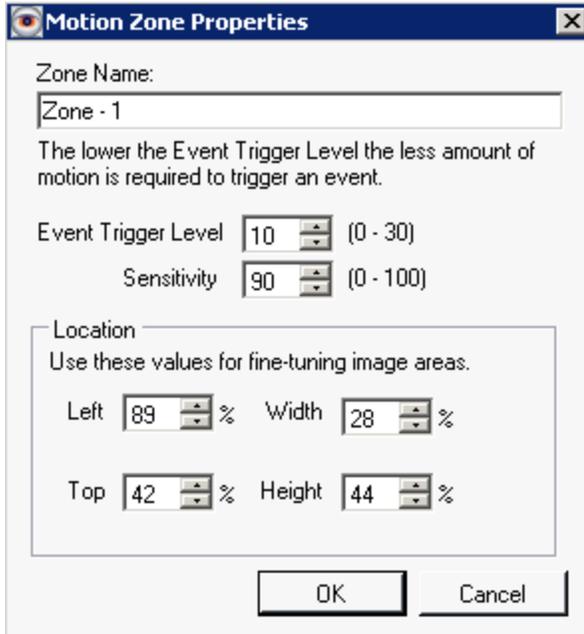
For example, you might have an outdoor camera set to record motion overlooking a playground with many trees. You only want the camera to record substantial movement, like that of vehicles, people and animals, and not when leaves move on a tree. You can create a motion zone in an area that is free of trees, focusing on real movement.

To create a Motion Zone:

1. On a camera’s Motion Settings tab draw a square or rectangular shape over all or part of the live image.
2. After a shape is drawn a zone is added to the Event Trigger Labels section.
3. Create additional shapes for additional zones, up to the cameras maximum. You have reached the maximum when you can no longer create zones.
4. Click **Apply** and then **OK**.
5. You can check the camera’s [Web Access](#) to verify the zone(s) were sent to the camera properly.

To modify a Motion Zone:

1. Select the zone from the Event Trigger Labels list.
2. Click **Properties**.



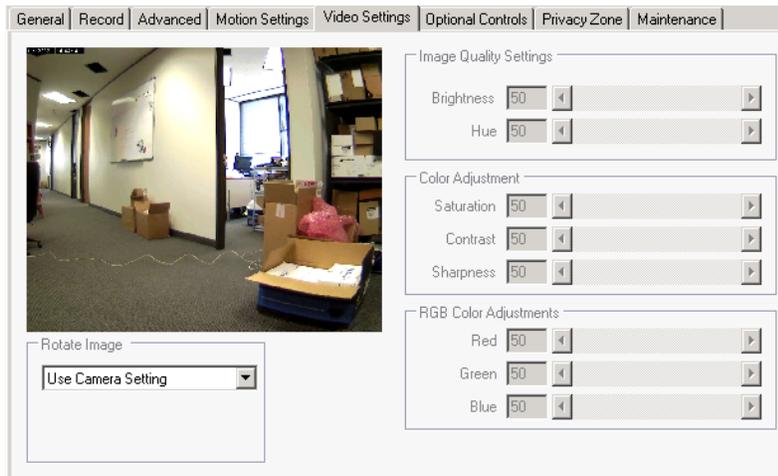
3. Change the zone name or leave it as-is.
4. Select the Event Trigger Level and Sensitivity settings.
5. To fine-tune the image area, change the left, width, top or height settings.

Note

Properly naming zones makes the motion event appear in the Motion Log with the specified name (i.e., Door Open) rather than the default of Zone - 1.

You can make a zone more sensitive than the rest of the camera view by setting its trigger level higher; to reduce a zone's sensitivity, lower the trigger level lower. Setting a zone to zero percent prevents motion detection from operating in that zone. Setting a zone to zero is useful if there is frequent motion in part of the image that you want to ignore. You can also manually move or resize the motion zone using the location settings.

Video Settings tab



You can use the Video Setting tab to modify certain camera settings. The software determines which settings can be modified based on the camera model. Options that are not supported cannot be modified.

Note

Most digital cameras use HSV color scheme rather than RGB.

There are generally two ways to defining color: HSV (hue, saturation, value) or RGB (red, green, blue). Most digital cameras use HSV instead of RGB.

Image Quality Settings:

- **Brightness:** Brightness is the amount of light in the image. You can adjust image brightness by moving the slider control. The higher the brightness, the brighter the image.
- **Hue:** Hue is described with words we normally think of as describing color: red, purple, blue and so on. You can adjust the camera color to make it more “true” by moving the slider control.

Color Adjustment:

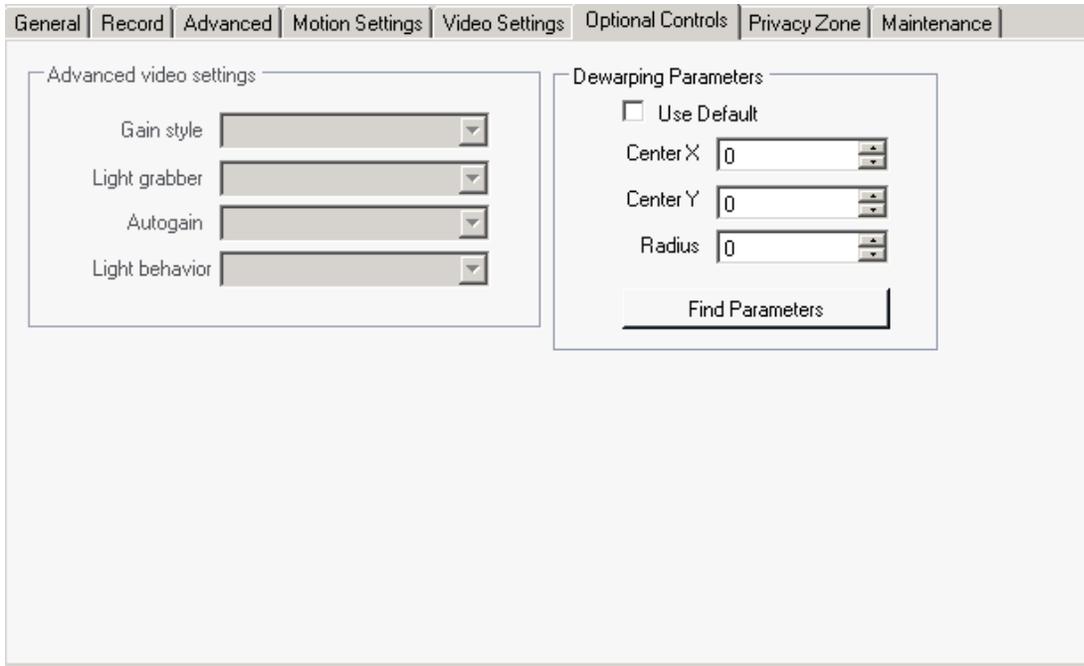
- **Saturation:** Saturation describes the difference of a color from the gray of the same lightness. Increasing saturation deepens image colors, making reds redder and blues bluer. Decreasing saturation brings images closer to a grayscale, making them look more black-and-white.
- **Contrast:** You can adjust image contrast by moving the slider control.
- **Sharpness:** Adjusting image sharpness changes its colors in a way similar to saturation, but reducing sharpness generally makes images look more “flat.”

RGB Color Adjustments: If the camera uses the RGB color model, you can adjust the levels of red, green and blue in your image by moving the slider controls.

Rotate Image: Some cameras display an upside down image by default. You can use this drop-down menu to change how the image displays.

- **Use Camera settings:** Use the image orientation sent from the camera.
- **No rotation:** The image is not rotated. If camera rotates the image, the system rotates it back.
- **Flip:** The image is flipped 180 degrees.

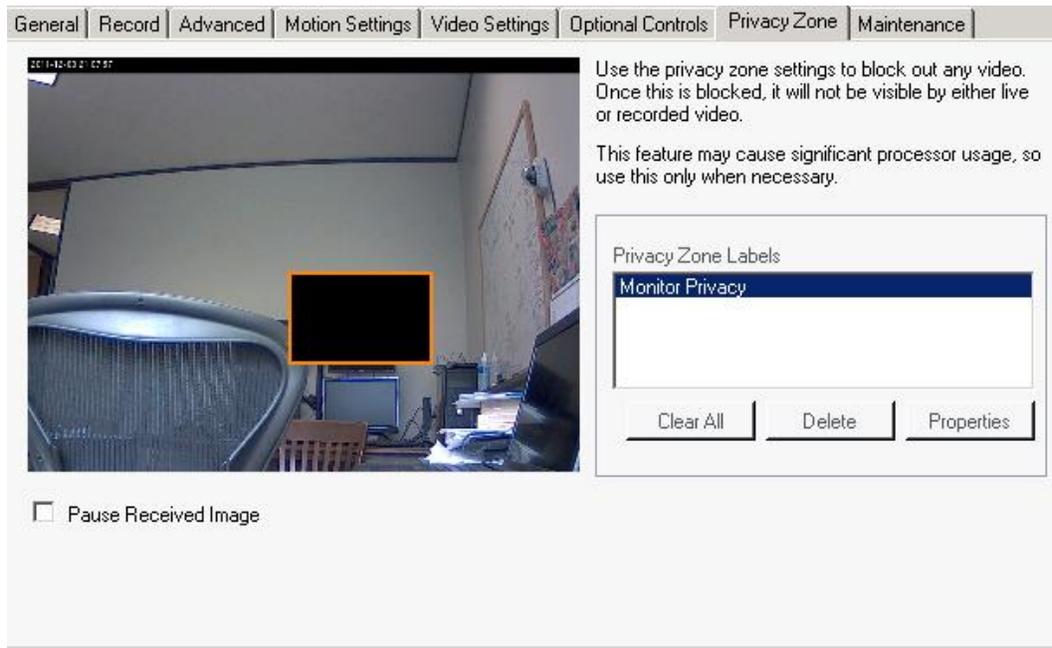
Optional Controls tab



The screenshot shows the 'Optional Controls' tab selected in the interface. The 'Advanced video settings' section contains four dropdown menus: 'Gain style', 'Light grabber', 'Autogain', and 'Light behavior'. The 'Dewarping Parameters' section includes a checkbox for 'Use Default', three numeric input fields for 'Center X', 'Center Y', and 'Radius', and a 'Find Parameters' button.

You can use the Optional Controls tab to manipulate complex features offered by some cameras. For example, the Sentry 360 camera has de-warping capabilities and feature-specific configuration settings. In The figure below, the Optional Controls tab shows the enabled controls for this camera feature. See the appendices for more information on configuring specific camera types.

Privacy Zone tab



You can use the Privacy Zones tab to block live images and recorded video from a specified part of the camera image. Once set, that zone cannot be viewed, recorded or monitored. In addition, if a camera with a Privacy Zone is set to Motion-Only Recording, motion in the zone will not trigger recording.

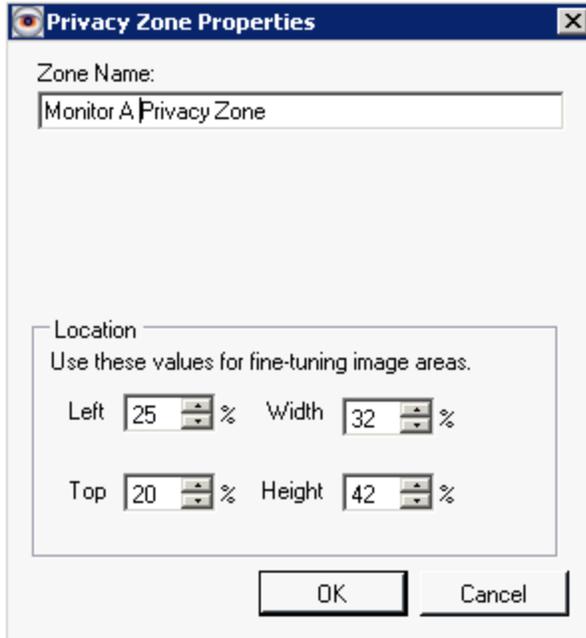
Pause Received Image: Check this box to pause the received image while you create a privacy zone. Leaving it unchecked can cause the privacy zone to flicker while it is being created.

To create a Privacy Zone:

1. From the Privacy Settings tab of a camera start drawing a square shape over the live image on the left.
2. Use the mouse to left-click and draw a box around the area to be blocked. Enter a name for the zone that will be displayed on the Privacy Zone Labels list. You can move the zone on the live image to fine-tune its placement.
3. You can add as many zones as the view field allows.
4. Click **Apply** and then **OK**.
5. You can check the camera's [Web Access](#) to verify the zone(s) were sent to the camera properly.

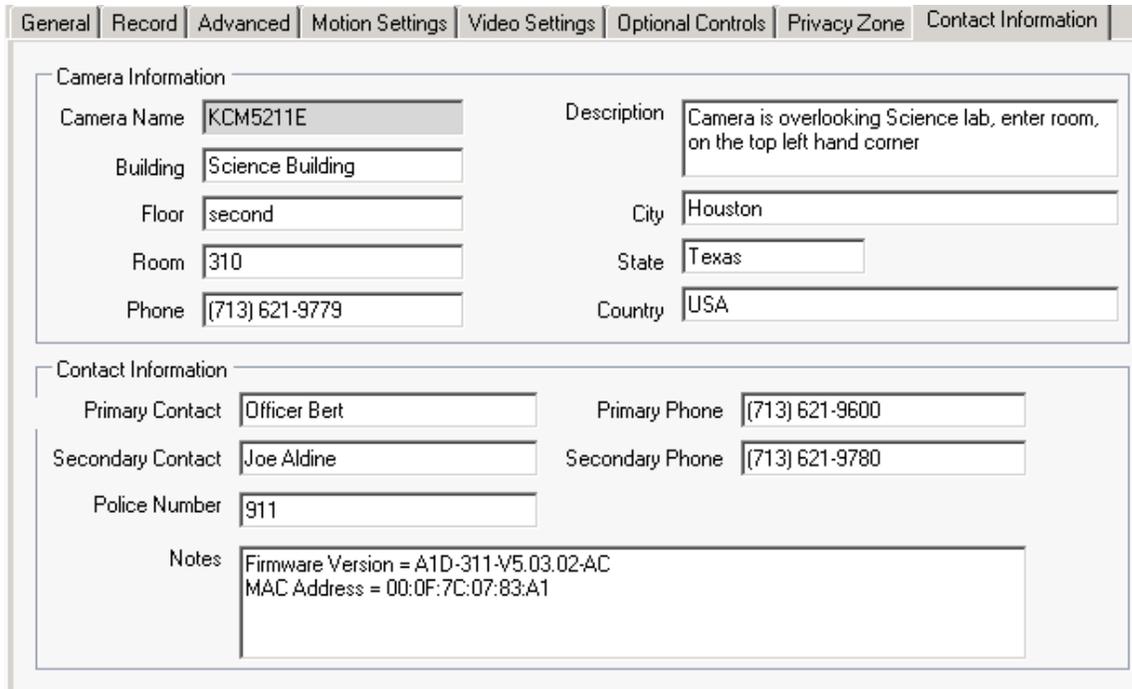
To modify a Privacy Zone:

1. Select the zone from the Privacy Zone Labels list.
2. Click **Properties**.



3. Change the zone name or leave it as-is.
4. To fine-tune the image area, change the left, width, top or height settings.
5. Click **OK**.

Contact Information tab



You can use the Contact Information tab to identify the camera in more detail. The only information displayed by default is the camera name. The server administrator can enter the additional camera information. Click **Apply** and then **OK** to save the information.

Maintenance tab

The screenshot shows the Maintenance tab selected in the Video Insight Administrator interface. The form is divided into several sections:

- Camera Information:**
 - Camera Name: KCM5211E
 - Vendor: ACTi
 - Model: ACTi KCM-5211
 - Installed: 12/01/2011
 - Warranty: 1 year
 - Firmware: A1D-311-V5.03.02-AC
 - Other: Purchased From Video Insight on 11/15/2011
 - IDF/Switch: IDF-E200/10.4.52.103
 - Other: Cable Label: CI-E2 STAIR
- New Service Record:** 12/17/2011<Officer Bert>: Camera was damaged on December 17th by a couple of teenagers, Incident # 15225-DFH. Called Video Insight and spoke to Joan to order a replacement; ETA: 2 days.
- Service History:** 11/15/2011: Camera received by Officer Bert
- Contact Information:**
 - Contact: Officer Bert
 - Phone: 713-621-9779

You can use the Maintenance tab as another option to enter detailed camera information. The only information displayed by default is the camera name and model. The server administrator can enter the additional camera information.

Note

Switching between the two tabs erases all information entered on the other tab.

Information entered in the **New Service Record** field is added to the Service History for later review.

Click **Apply** and then **OK** to save the information.

Dual-streaming capability

The Video Insight VP encoder series (VP 1, 8 and 16) offers a sub-stream for H.264. This is a useful option when bandwidth and CPU utilization are a concern. This feature allows you to add the VP 16

using channels 1-16 in Monitor Station for Live view using one stream of H.264 with lower FPS and resolution, and add channels 17-32 with a much higher FPS and resolution for recording purposes.

Adding the VP Encoder in this method results in a smoother live view that works best with a less-than-ideal environment. It provides great quality and the highest resolution possible for recorded video.

Access controls

Access controls manage entry and exit to monitored facilities. IP Server integrates with a variety of access controls to provide an enhanced security environment.

S2

Video Insight and S2 certification is another offering to customers that would like to use Video Insight as a robust, dependable NVR system on the backend with an S2 user interface. This integration requires Video Insight Server version 4.3.0.40 and higher and S2 version 4.2 and higher. Documentation on how to configure and use S2 can be found by browsing to the following link for the latest OVID installer and an integration manual.

http://downloadvi.com/downloads/Current/OVID_S2_SERVER.zip

RS2

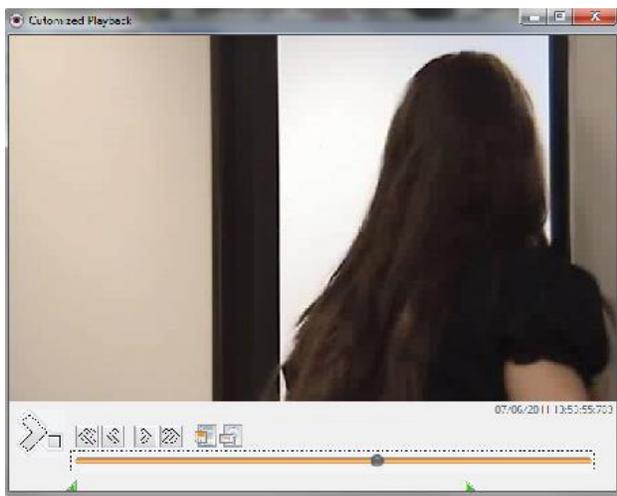
RS2 is a command line integration you can execute using a batch file or a simple command line. RS2 integration offers a live and recorded view of each camera.

To use RS2 to view recorded video:

1. Access a command line.
2. Enter "DVRViewer -sserverip -c1 -ddate -bbegintime -eendtime", where sserverip is the server IP address, ddate is the date in mmddyyyy format, bbegintime is the time point to start the video in 24-hour hh:mm:ssformat and eendtime is the time point to end the video in 24-hour hh:mm:ss format. For example, entering

```
DVRViewer -s10.10.1.213 -c1 -d07062011 -b09:00:00 -e10:00:00
```

Displays video recorded by server 10.10.1.213 from 9 AM to 10 AM on July 6, 2011 in a stand-alone player, as shown in the figure below.

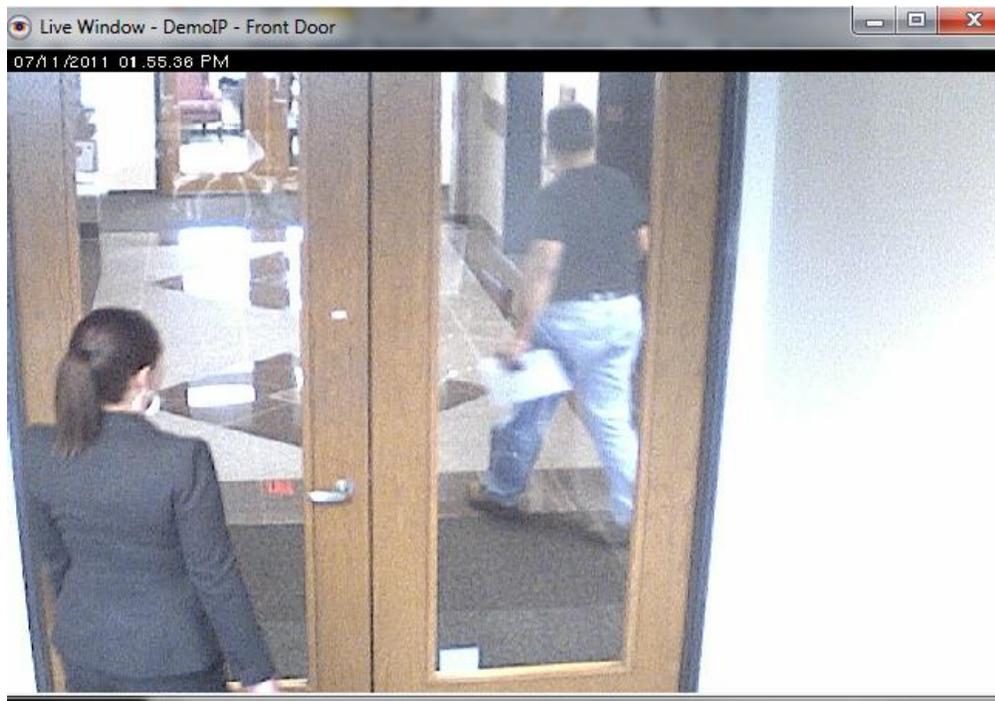


To use RS2 to view live video:

1. Access a command line.
2. Enter “DVRViewer –sserverip:portnumber-c1 –dlive”, where sserverip is the IP address of the server and portnumber is the server port number. For example, entering

```
DVRViewer -s38.100.66.196:4021 -c1 –dlive
```

Displays live video from server 38.100.66.196 through port 4021 in a stand-alone player, as shown in the figure below.



Video Insight does not provide support for RS2. Contact RS2 for more information.

DSX

Video Insight supplies an installer for the required files. You can download it from <http://downloadvi.com/>. Integrating Video Insight with DSX gives you live and recorded video as well as the ability to use your camera's PTZ presets.

Video Insight does not provide support for DSX. Contact DSX for more information.

MonitorCast

Video Insight offers MonitorCast integration. The access control capability, hardware, features and integrations are built into our software. You must have a MonitorCast server running to configure the integration. You can contact Video Insight Technical Support for instructions on installing a MonitorCast server. Video Insight supports MonitorCast version **8.8.61** and higher.

You must add the IP Server IP address to the MonitorCast authorized clients list prior to configuring Monitor Station.

1. Log on to the MonitorCast server.
2. Click the Hardware Manager icon.
3. Click the Lock icon to make changes.
4. Select the Web Service node.

Press the Lock icon to Unlock and make changes

Properties	
Auto Start Web Server	<input checked="" type="checkbox"/> True
Windows Services Manager	(Click here for more options) ▾
Website	(Click Here to Connect) ▾
Website Timer	15
SDK Allowed IP Client(s)	10.10.1.39,10.10.1.202, 10.10.5....
SDK TCP Port	2051

5. Enter the IP Server's IP address into SDK Allowed IP Client(s). Separate all IP addresses with a comma.
6. Note the pre-defined SDK TCP Port number. You will need it when configuring Monitor Station.
7. Click **Save**.
8. Click the Lock icon to secure changes.

To configure MonitorCast using Monitor Station:

1. Login to IP Server directly or through Monitor Station.
2. Start Server Properties by clicking on Administration followed by Setup and Configuration and select the desired server from the left tree.
3. Click the Access Configuration tab.
4. Enter the MonitorCast Server IP address, TCP Port number and Operator user name.

Setup and Configuration | Cameras | Advanced | Health Monitor | Client | Access Configuration | Contact Information

Enable access control support Access Control Type: MonitorCast

MonitorCast Server Connection

Server IP: 10.10.1.91 Port: 2051 Operator: Admin Test

Access Configuration Options

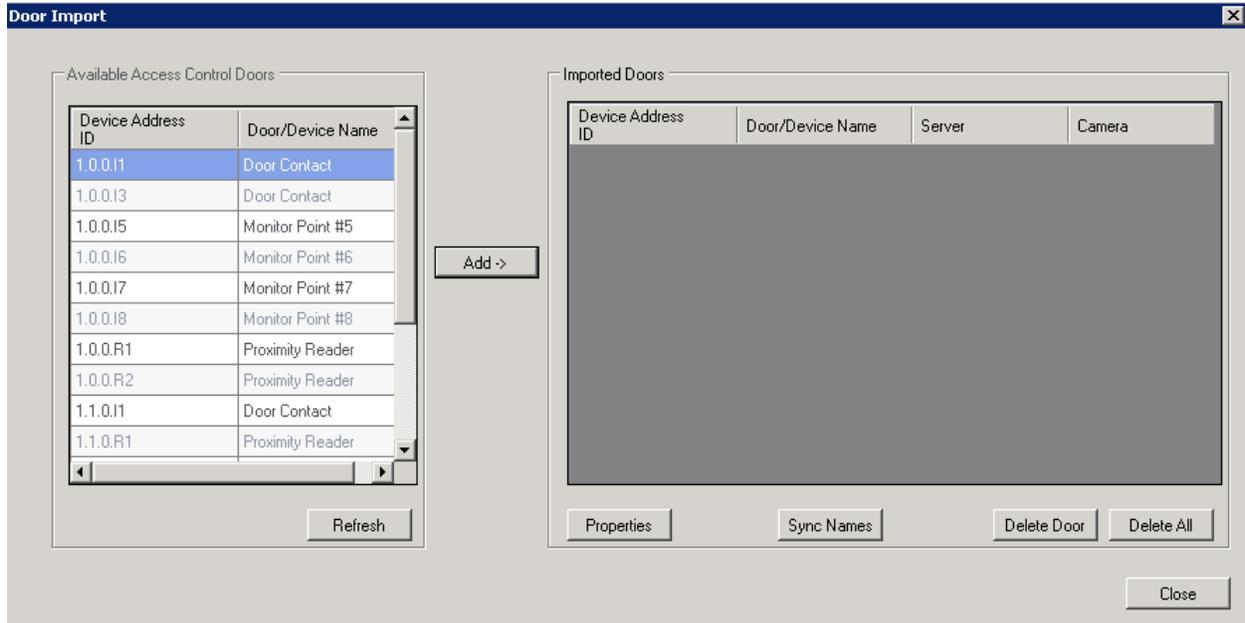
- Log all card events in the event motion log
- Log Alarms in the system log
- Send alarms to Monitor Station

Imported Doors

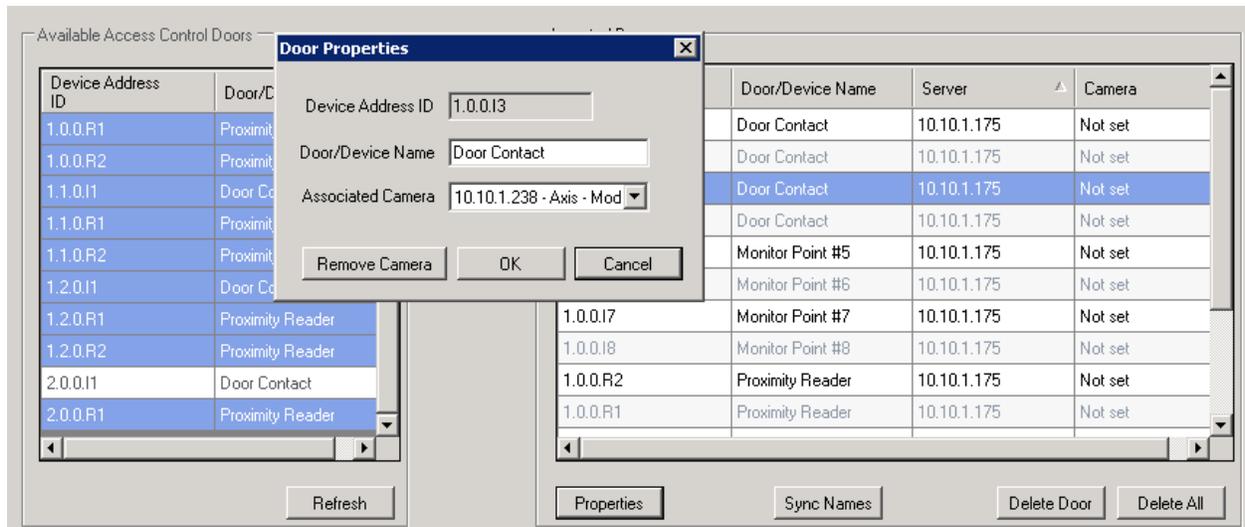
Door/Device Name	Server	Camera
------------------	--------	--------

Import Properties Delete Door Delete All

5. Click **Test**. If successful, the system displays the message “Access control system connection successful.” If unsuccessful, return to step one on the previous page.
6. Click **Import**. All doors and devices configured in MonitorCast are displayed under Available Access Control Doors.
7. Ensure the port is allowed on the firewall or Windows Firewall is disabled.



8. Select the door or device to import and then click **Add**.



9. To associate a camera to the imported door or device, click **Properties**.
10. Enter a door or device name or accept the default.
11. Select the camera from the Associated Camera drop-down menu.
12. Click **OK**.

To modify MonitorCast using Monitor Station:

1. Right-click a server from the left navigation tree and select Properties.
2. Click the Access Configuration tab.

Setup and Configuration | Cameras | Advanced | Health Monitor | Client | Access Configuration | Contact Information

Enable access control support Access Control Type: **MonitorCast**

MonitorCast Server Connection

Host IP: Port: Operator:

Access Configuration Options

Log all card events in the event motion log
 Log Alarms in the system log
 Send alarms to Monitor Station

Photo

User: Password:

Imported Doors

Door/Device Name	Server	Camera
Proximity Reader	10.10.1.175	Not set
Proximity Reader	10.10.1.175	Not set
Proximity Reader	10.10.1.175	Not set
Proximity Reader	10.10.1.175	Not set
Proximity Reader	10.10.1.175	Not set
Sarit Name Test	10.10.1.175	10.10.1.245 -

3. Select an Imported Door and click **Properties**.
4. Change the name and/or the camera.
5. Click **OK**.

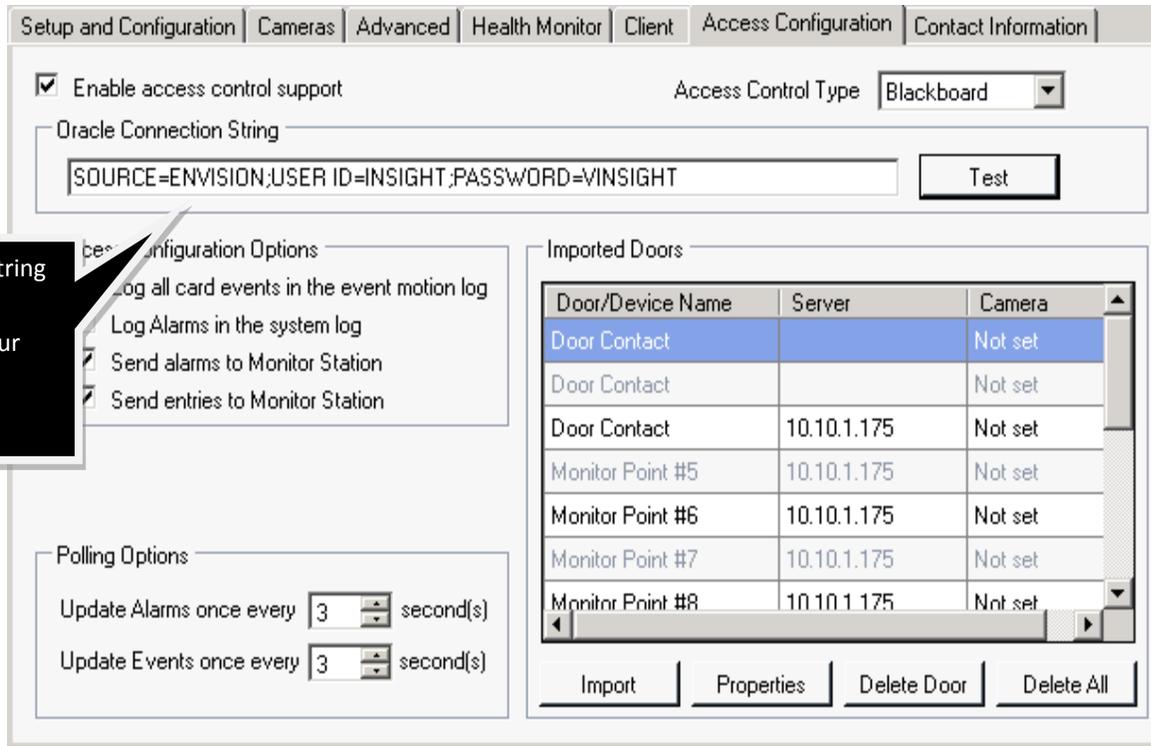
If the name of an Access Point changes on the MonitorCast server, click **Import** on the Access Configuration tab and then click **Sync Names**.

BlackBoard

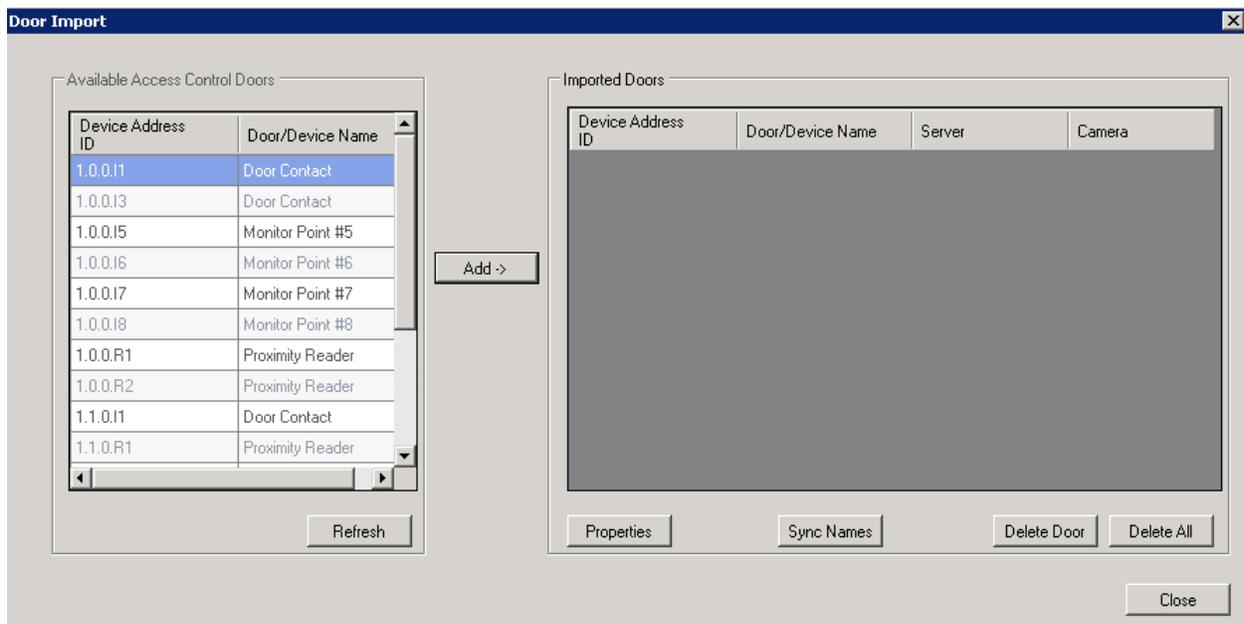
BlackBoard is an integration similar to MonitorCast. BlackBoard requires an ORACLE™ server.

To configure BlackBoard using Monitor Station:

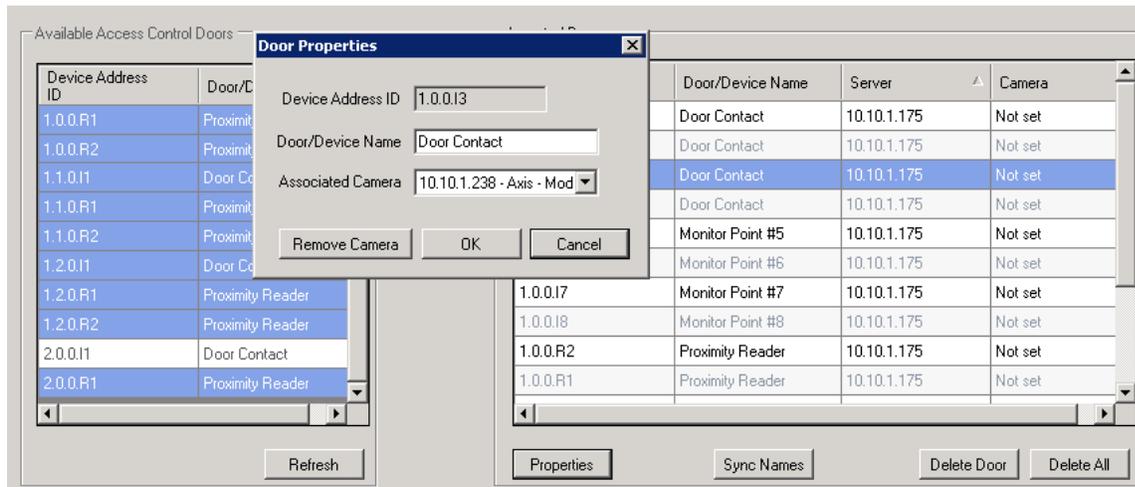
1. Login to IP Server directly or through Monitor Station.
2. Start Server Properties by clicking on Administration, followed by Setup and Configuration.
3. Click the desired server in the left tree navigation.
4. Click the Access Configuration tab.
5. Enter the Oracle Connection String.



- Click **Test**. If successful, the system displays the message “Access control system connection successful.” If unsuccessful, contact your System Administrator to confirm the connection string and whether the ORACLE client is running.
- Click **Import**. All doors and devices configured in BlackBoard are displayed under Available Access Control Doors.



- Select the door or device to import and then click **Add**.



9. To associate a camera to the imported door or device, click **Properties**.
10. Enter a door or device name or accept the default.
11. Select the camera from the Associated Camera drop-down menu.
12. Click **OK**.

Note

Clicking the Delete Door icon removes the door or device from Monitor Station only.

To modify BlackBoard using Monitor Station:

1. Right-click a server from the left navigation tree and select Properties.
2. Click the Access Configuration tab.

Setup and Configuration | Cameras | Advanced | Health Monitor | Client | Access Configuration | Contact Information

Enable access control support Access Control Type: **Blackboard**

Oracle Connection String
 Test

Access Configuration Options

- Log all card events in the event motion log
- Log Alarms in the system log
- Send alarms to Monitor Station
- Send entries to Monitor Station

Imported Doors

Door/Device Name	Server	Camera
Door Contact		Not set
Door Contact		Not set
Door Contact	10.10.1.175	Not set
Monitor Point #5	10.10.1.175	Not set
Monitor Point #6	10.10.1.175	Not set
Monitor Point #7	10.10.1.175	Not set
Monitor Point #8	10.10.1.175	Not set

Import Properties Delete Door Delete All

Polling Options

Update Alarms once every second(s)

Update Events once every second(s)

3. Select an Imported Door and click **Properties**.
4. Change the name and/or the camera.
5. Click **OK**.

If the name of an Access Point changes on the BlackBoard server, click **Import** on the Access Configuration tab and then click **Sync Names**.

There are two additional areas where BlackBoard is used: Lane Viewer and Access View in Facility Maps.

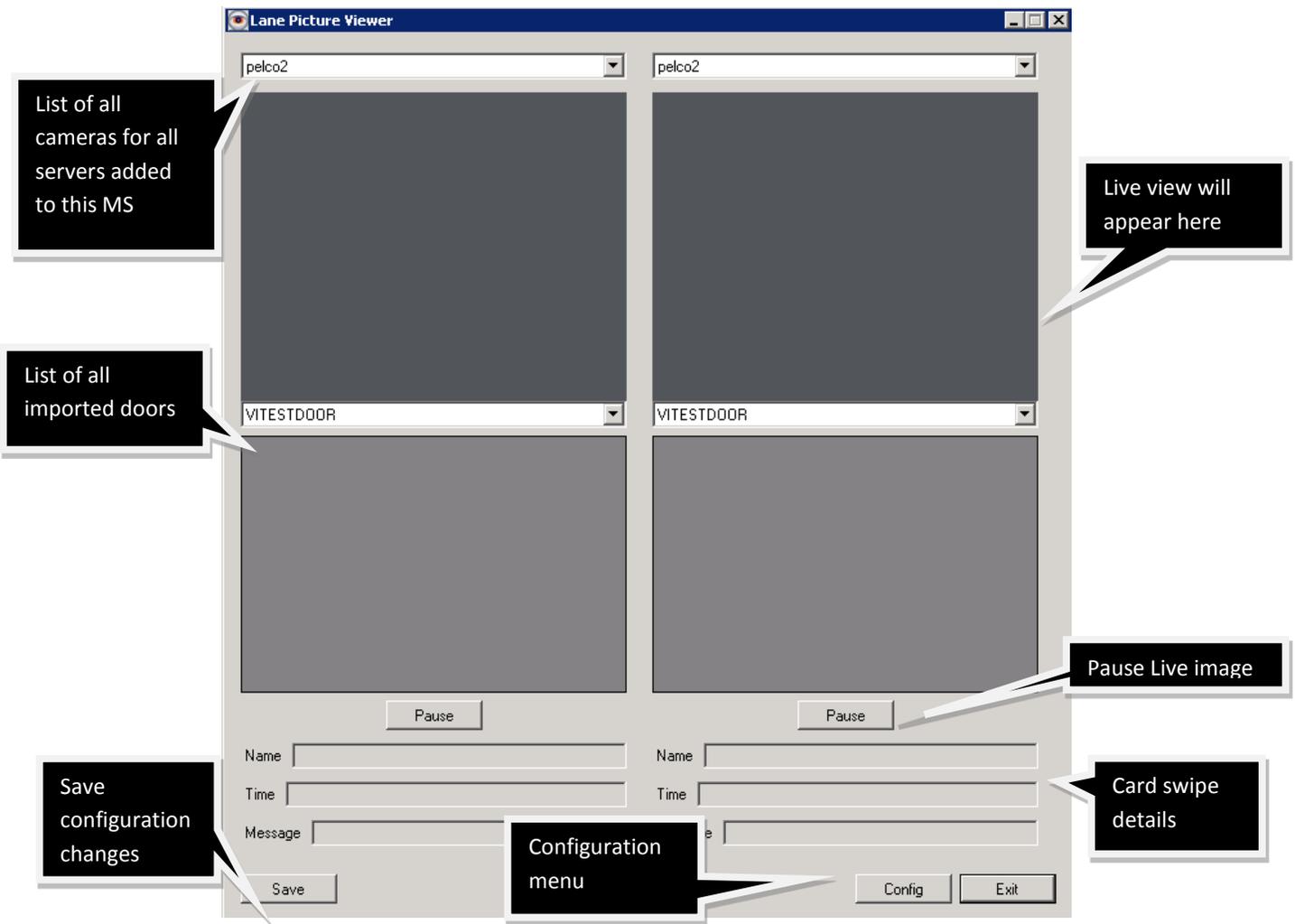
Lane Viewer

Use Lane Viewer when you need to view several cameras and their associated card swipes at the same time.

To enable Lane Viewer:

1. Start Monitor Station.
2. Click the Tools menu and then select Options.
3. Click the Tools Configuration tab.
4. Check the box to Enable Access Control Lane Viewer.
5. Click **Apply**.
6. Click **OK**.

Enabling the access control lane viewer adds it as an option on the Tools menu. Select it.



1. Select the camera from the upper drop-down menu or select the door from the lower drop-down menu. Selecting a door displays the corresponding camera in the live view.
2. When a card is swiped the name, time and message display as shown in the figure below.



If no photo exists for the name, the system displays a *No Photo* message will appear:

You can customize Lane Picture Viewer options by clicking the Config button.

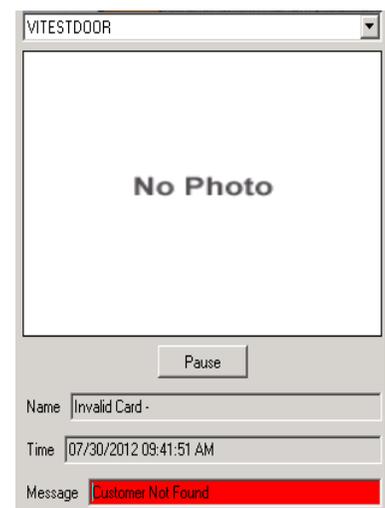
Picture Size:

- **Width/Height:** The sizes entered here determine the lane size. Click Restore to reset the width and height to their default.
- **Always show last entry:** Checking this option displays data from the last card swipe. If unchecked, the data is blacked-out after 30 seconds by default.
- **Keep History:** Checking this option allows you to press Pause and iterate through the preceding 10 images by default.

Viewing options:

Number of Lanes: Select the number of lanes to view at once, up to six.

You can check or uncheck the next five boxes to include or exclude the display of that information.



Live Video: Select these options to show live video. If unchecked, only the card swipe information and photo display.

Access View

Access view is accessible either by the facility map and hovering over a door or from Tools > Access View in the Monitor Station. If the facility map is open and Access View is closed, it will pop up when an alarm or event occurs.

Alarm History

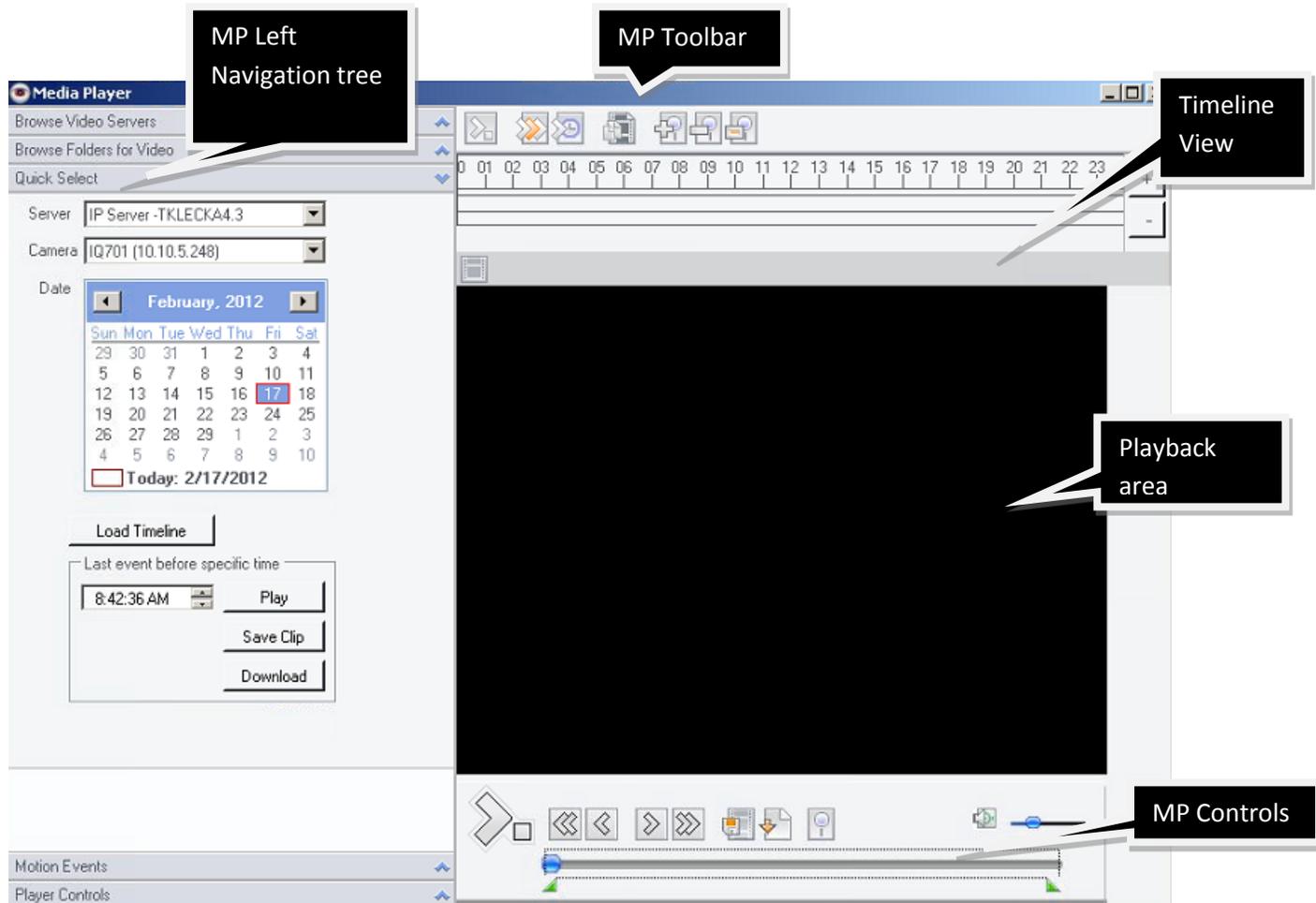
Click this tab to display a complete list of the most recent alarms. Double-click on an alarm in the list to play the recorded video for that event.



User Entry History tab: Click this tab to display a complete list of the most recent card swipe history. Double-click on the entry to display the recorded video for that event.

Media Player

Video Insight’s built-in Media Player offers a slew of filtering options, printing and managing of videos making it fast and easy to find a video or motion event.

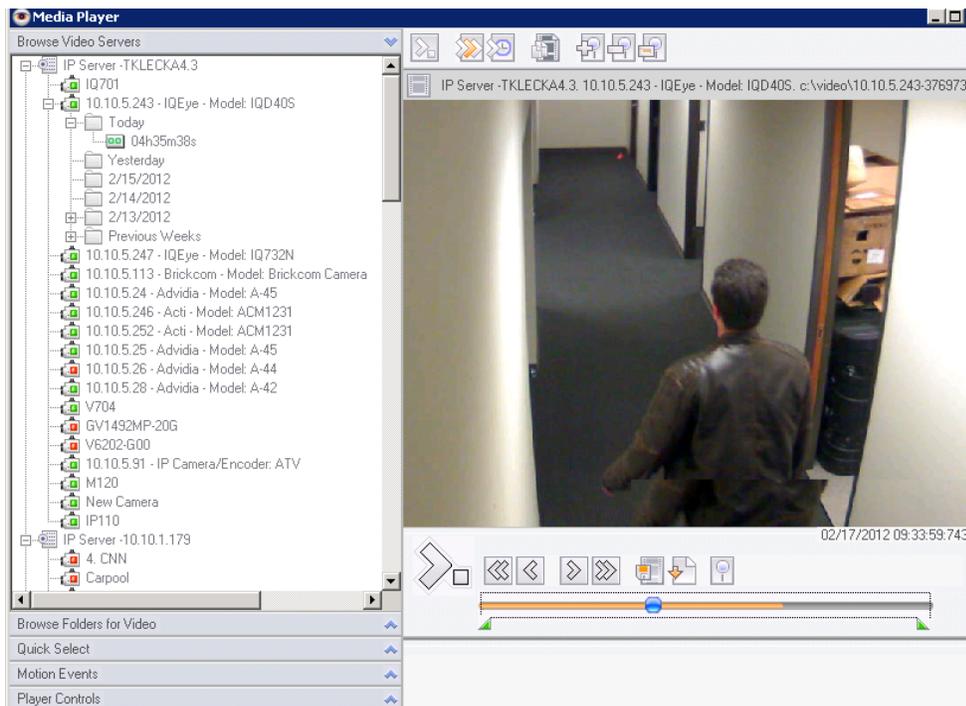


Left navigation tree

The left navigation tree has multiple panes. The Quick Select pane is expanded by default.

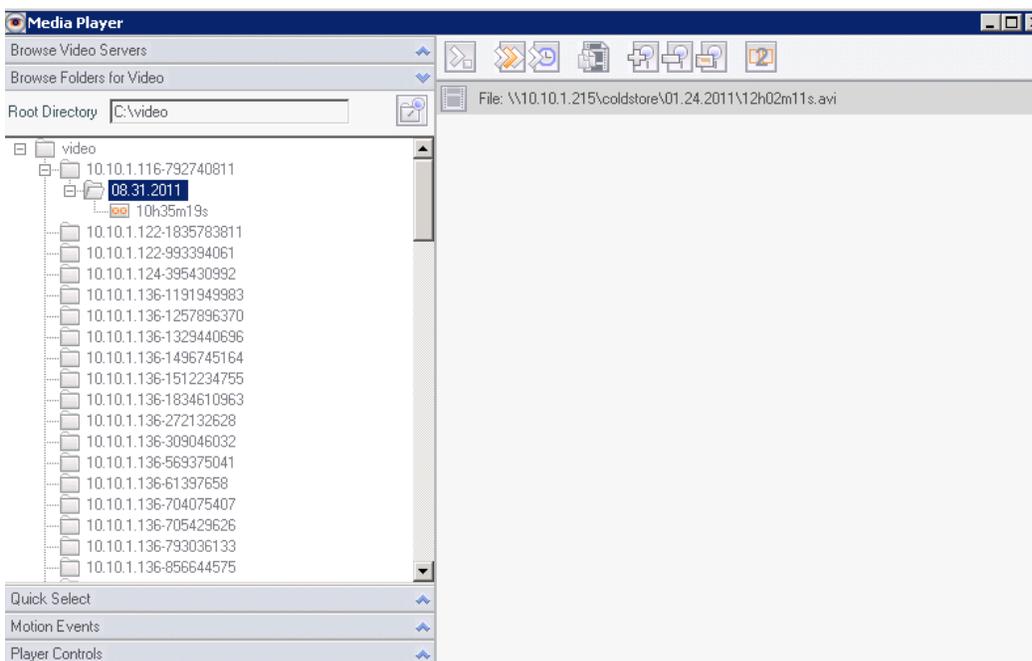
- [Browse Video Servers](#)
- [Browse Folders for Video](#)
- [Quick Select](#)
- [Motion Events](#)
- [Player Controls](#)

Browse Video Servers



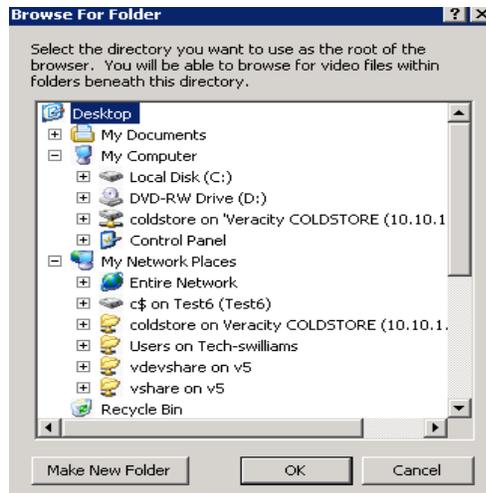
Browsing video servers is done the same as you would from Monitor Station’s left navigation tree. You can browse to the server, camera, day folder and file you want to view. The selected object plays on the right. You can also download a clip, print an image and perform an object search from this view.

Browse Folders for Video



Browsing folders for video is similar to browsing using Windows Explorer.

1. To change the root directory click the  icon.



2. Select a location and all video recordings in that network path display on the left.
3. Select a recorded file to play.

Quick Select



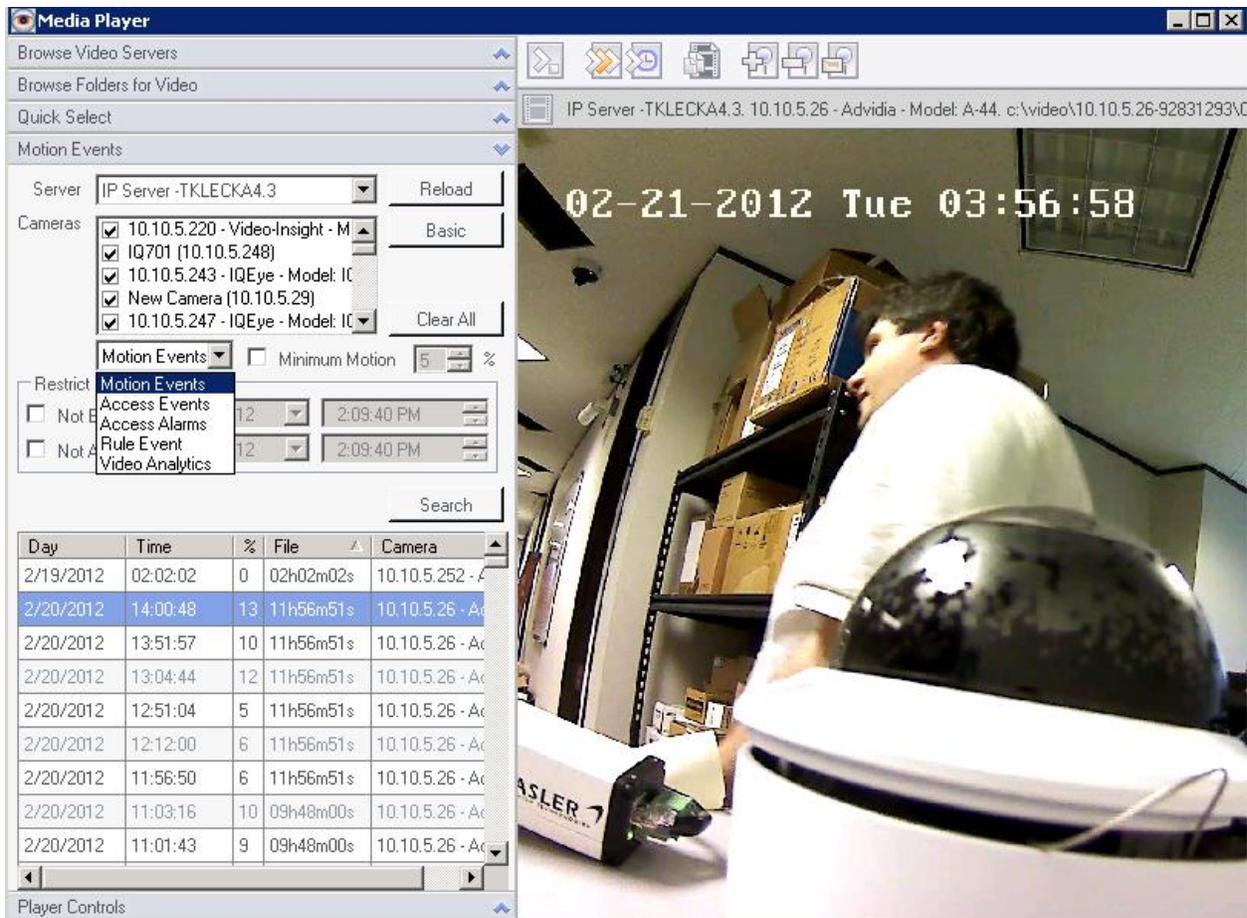
Quick Select is useful when viewing recorded files as motion events in the timeline view. These are shown in the figure below as orange marks.

1. Select the server from the Server drop-down menu.
2. Select the camera from the Camera drop-down menu.
3. Select a date from the calendar.
4. Click **Load Timeline**.
5. Place your cursor on any orange mark on the timeline (motion events). The motion event plays in the view.

You can search for a specific event around a known time using the Last event before specific time option. Enter a time closest but past when the event occurred and then click the Play button.

Motion Events

Added cameras are set to Motion-Only Record type by default. You can use this panel and avoid going through hours of video looking for a specific event if you know the exact camera, server, and time of the event.



1. Select the server from the Server drop-down menu.
2. Select the specific camera that recorded the event or select all.
3. Select a before and after time under Restrict Times or uncheck the boxes for a greater interval.
4. Click **Reload**. Motion events that match the search parameters display.
5. Click the motion event and the file will play on the right.

Motion events can also be filtered to include specific motion types:

Motion Events: Cameras set to Motion-Only Record type display events here.

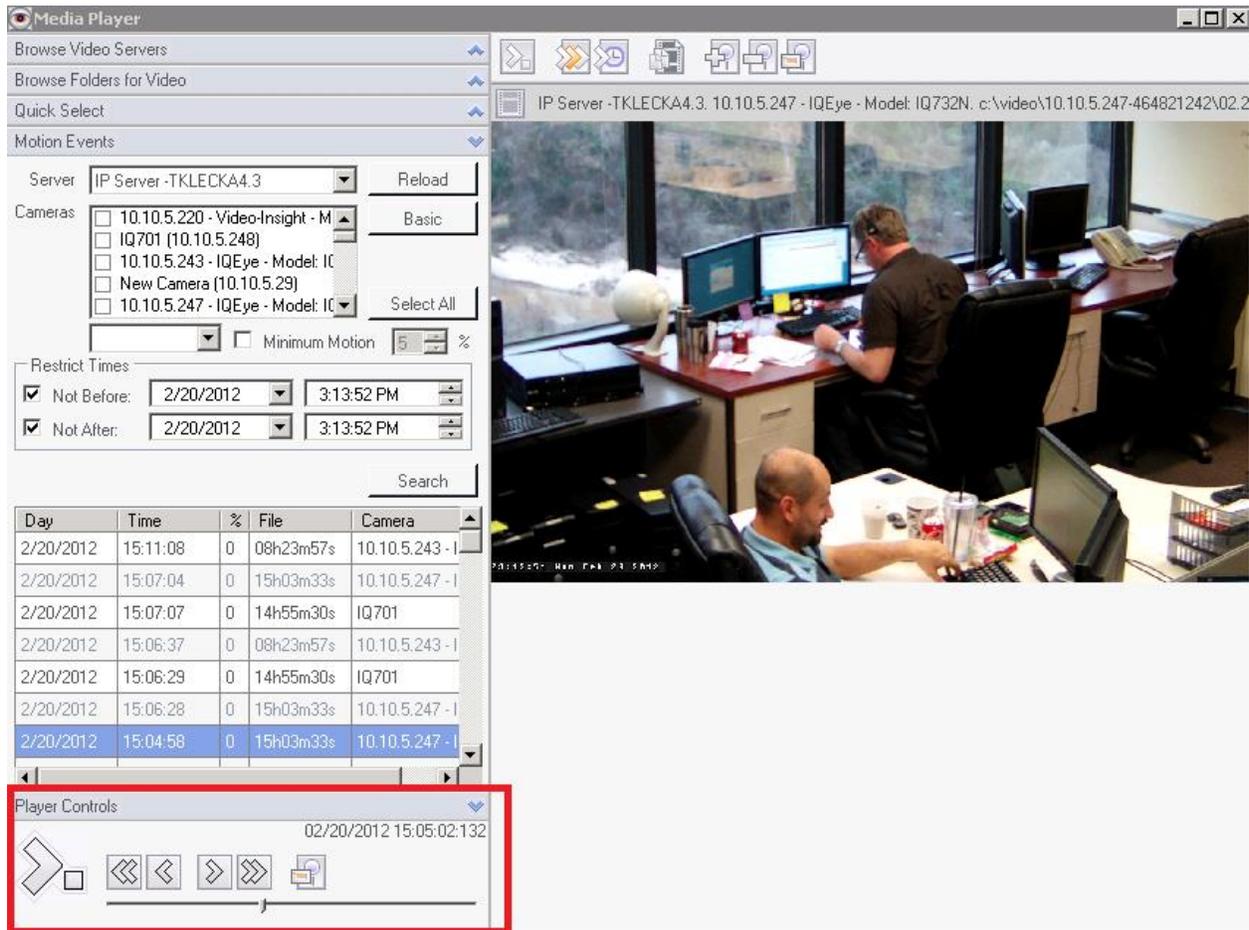
Access Events: Positive alarms of successful access control swipes from integrations such as MonitorCast and BlackBoard display here.

Access Alarms: Negative alarms of failed access control swipes from integrations such as MonitorCast and BlackBoard display here.

Rule Event: Motion events created because of a Rule display here.

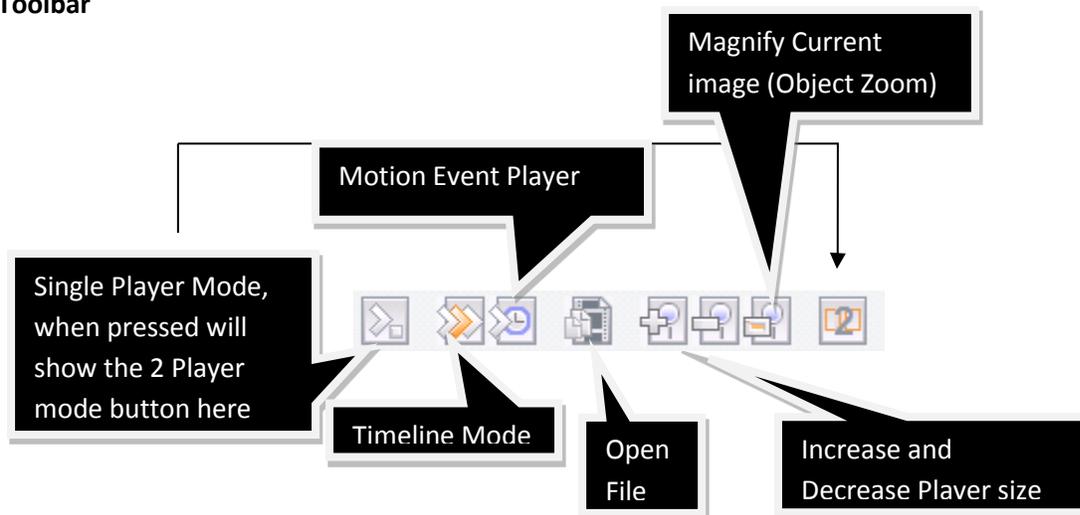
Video Analytics: Motion events created because of VCA Analytics (rules) display here.

Player Controls



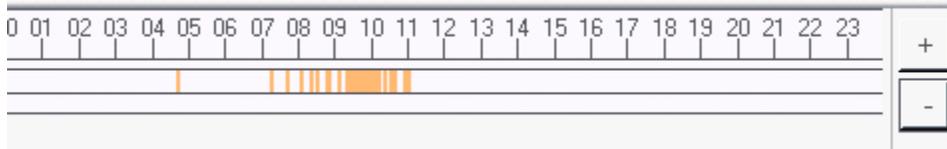
Media Player controls are located below the right view and also in the left pane. The left controls are useful when player size is increased to the point making the right controls disappear or when the size of the monitor coupled with the camera resolution size causes the controls below to disappear.

Toolbar



Single/Dual Player Mode: You can use these buttons to display one or two players and play and control the same video in two different players.

Timeline Mode: Timeline Mode is best used with cameras that are set to Motion-Only Recording type. Clicking the Timeline Mode button displays a timeline as shown in the figure below.



The orange marks indicate recorded motion events. You can use the plus and minus buttons to display whole days, hours or minutes. Place your cursor on any of the orange marks to play that motion event.

Motion Event Player: Clicking this button expands the Motion Events pane. See Motion Events for more information on motion events.

Open File: In some cases browsing to a video's location is not enough you will need to open a specific file. Click this button and browse to the location of the file.

Magnify Current Image (Object Zoom): Each click of the Object Zoom button displays a pop-up that allows printing, zooming in and out as well as saving to a location for later retrieval. The figure below shows an example of an Object Zoom pop-up.



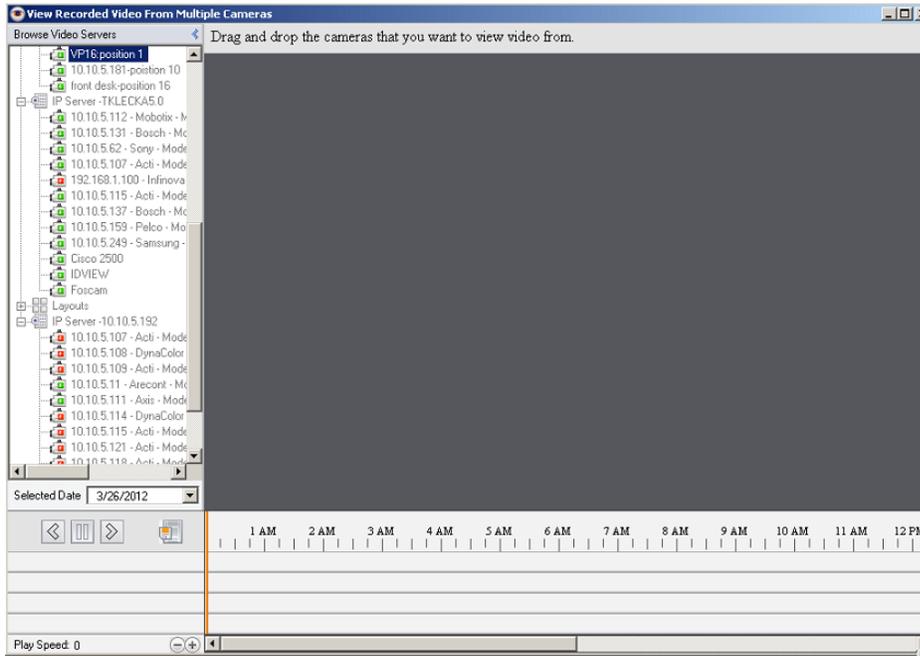
Note

To use cameras in the Sync Player the server the cameras reside on must be running IP Server version 5.0 or later.

Synchronized Player

The Video Insight Synchronized Player is easy to access and use.

1. Start Monitor Station.
2. Click the Tools menu and then select Synchronized Player.



3. Drag-and-drop up to six cameras from the left navigation tree to the viewing area.

Please Note: all of the cameras selected should be from the same server.

The screenshot shows the 'View Recorded Video From Multiple Cameras' window. On the left is a tree view of 'Browse Video Servers' containing a list of cameras with their IP addresses and names. Below this is a 'Selected Date' dropdown set to '3/26/2012'. The main area displays a grid of video playback windows for selected cameras. At the bottom is a timeline from 9 AM to 7 PM with a vertical orange bar indicating the current playback time. A list of camera names is shown below the timeline, and a 'Speed: 1' control is visible.

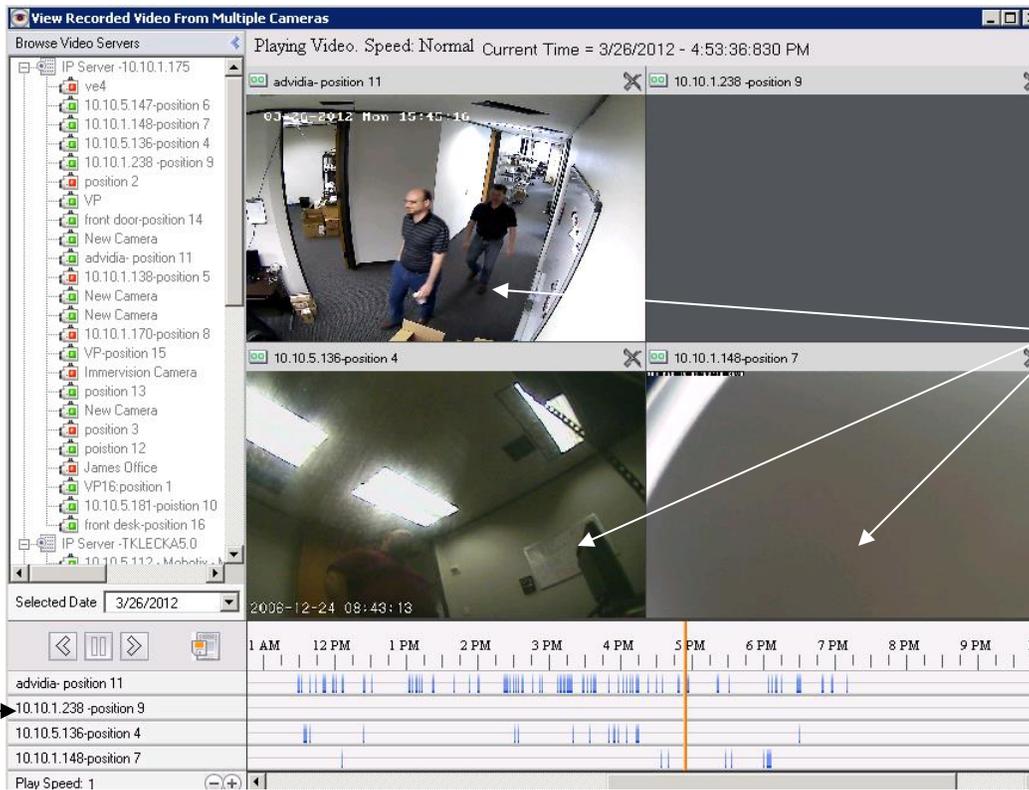
Callouts and their descriptions:

- All connected servers will appear here, you may select up to 6 cameras from any one 5.0**: Points to the 'Browse Video Servers' tree view.
- Playback speed controls**: Points to the 'Speed: Normal' indicator.
- Playback Speed**: Points to the 'Speed: Normal' indicator.
- Current playback date and time**: Points to the 'Current Time = 3/26/2012 - 3:25:031 PM' indicator.
- Camera**: Points to a video window title bar.
- Selected cameras Playback area**: Points to the video grid.
- Click X to remove camera**: Points to an 'X' icon in a video window title bar.
- Date Selection**: Points to the 'Selected Date' dropdown.
- Player Controls**: Points to the playback navigation buttons.
- Correlating camera names and their available**: Points to the camera list below the timeline.
- File Export; Clip creation**: Points to the 'Export' icon in the player controls.

Placing a camera in the playback area loads its available recordings for the selected date (the default is Today).

Recording Types: A solid blue line indicates that a camera uses Record Always Recording. Blue marks indicate that the camera uses Motion-only Recording.

Once the recordings load, the vertical orange bar moves to the earliest recording and begins playing the video for the applicable camera(s). Not all cameras added to Synchronized Player have recordings at the same time and as such the camera(s) without recording pauses or remains gray while the camera(s) with recordings play. When the vertical orange bar reaches a point where all cameras in the viewing area have recordings (i.e., all cameras show a blue mark for the same time) all the recordings play synchronously. The figure below shows an example of synchronized playback.

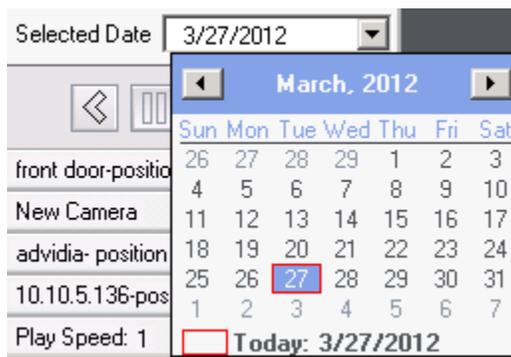


Position 9 camera is gray because there are no motion events or recordings to display

3 cameras are playing: position 11, position 4 and position 7

The vertical orange bar progresses from left to right as video is playing. It progresses along the timeline until the end of the day or the end of the recordings are reached. You can click anywhere in the timeline to replay a motion event.

The Synchronized Player defaults to the current date when started. To view video from a different date click the Selected Date drop-down menu.



The default playback speed is 1. Click the '+' or '-' buttons to increase or decrease video speed. 64 is the fastest forward speed and -64 is the fastest reverse speed.

The player displays three controls at first: Play, Pause and Rewind.



After any of the control buttons is pressed fast forward and fast reverse controls become available.



Synchronized Player clip option

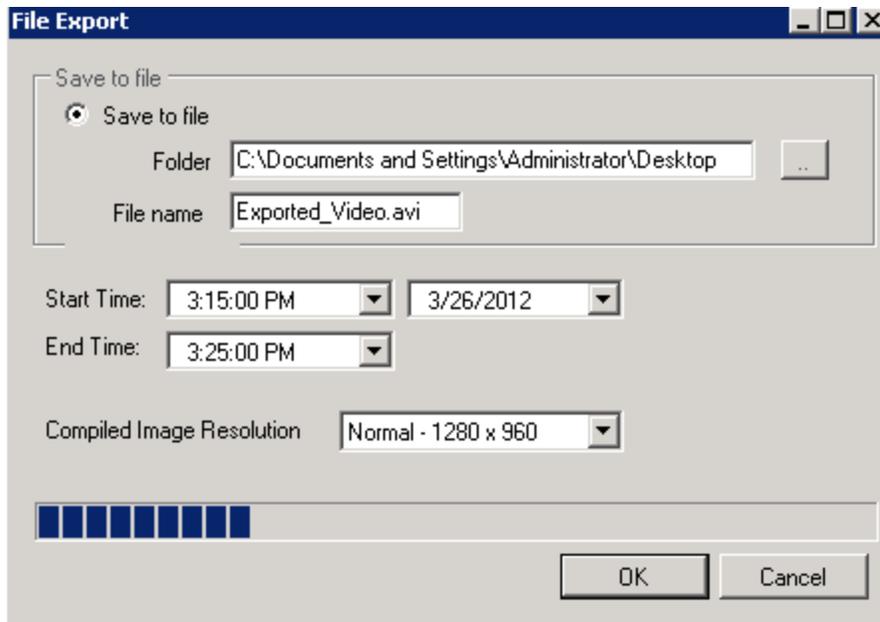
Once Synchronized Player is used with a set number of preselected cameras and the video with the interesting footage is displayed it is possible to create a synchronized clip that will play in all supported media players just as a regular video would; only displaying the synchronized view of the matrix.

To export a file from Synchronized Player:

1. Click the File Export icon.



2. Accept the default save location or enter or browse to another.
3. Accept the default file name or enter another.
4. Change the default time and date and time if different than what is currently playing.
5. Select a compiled image resolution.
6. Click **OK**.



7. Click **Cancel** after the file export is completed.

Troubleshooting

Your registered Video Insight product includes one year software maintenance and a technical support plan that begins on your purchase date. This is verified by the serial number used to activate the software. The one year of software maintenance entitles users to one full year of free software upgrades and unlimited technical support. Video Insight recommends renewing your maintenance before it expires to avoid a lapse in upgrades and support.

Our technical support team is highly skilled in our software and in the world of IP cameras, as well as networking and access control systems. Video Insight technical support works to make sure your issue is resolved as quickly and completely as possible.

Frequently Asked Questions

What types of cameras are supported?

Video Insight supports a most camera manufacturers and models. Camera support includes feature support. You can view the most recent list of supported cameras at: <http://www.video-insight.com/supported-cameras.php>

Why am I seeing skipping in Live View?

Live View performance depends heavily on your server, client and network capabilities. If you are seeing skipping in Live View is could be related to these capabilities and the number of concurrent connections to the camera exhibiting the skipping.

I'm having trouble installing IP Server on my computer.

The Video Insight Application Suite installer takes all pre-requisites into consideration to allow users to install any or all of our applications using one installer. The installer considers which SQL or IIS versions are needed and when and how they should be installed. Due to the many variables involved, it is possible that the Video Insight installer may fail to properly install SQL or IIS, which in turn may cause the Video Insight suite to be installed and configured properly. There are two options to overcome any possible installation issues.

Option I: If the destination server is not in production and can be reformatted we recommend it as the fastest route to a successful install.

Option II: If the destination server is currently in production and cannot be reformatted, you must manually remove the following items:

1. Use the Add/Remove Program applet in Control Panel to uninstall all Video Insight software.

2. Remove the Video Insight IP Enterprise folder from all installed locations, typically C:\Program Files.
3. Remove all registry keys related to Video Insight. These are different for 32- and 64-bit installations.
4. Use the Add/Remove Program applet in Control Panel to uninstall all SQL-related applications, including SQL Server Management studio and SQL Native Client
5. Remove MSSQL folders located in C:\Program Files.
6. Remove all registry keys related to the SQL installation.
7. Restart the computer.
8. Reinstall the Video Insight application suite.

Note

We recommend backing-up your database prior to any database modification and removal.

I can't get Health Monitor and my IP Server to connect.

Verify that Health Monitor information is correct on the [Health Monitor tab](#) of the IP Server's properties. Verify that Health Monitor installation and configuration steps described in [Health Monitor](#) were followed. If this is correct, check that:

1. The IP Server name does not exceed 30 characters. Health Monitor supports a maximum of 30 characters for the IP Server name.
2. Verify that the Health Monitor service is running on the server hosting Health Monitor. The service name is HealthMonitorService.exe.

I just added my servers, so why does it keep asking me to reenter them? It's not saving added servers.

If the Server Setup pop-up appears every time Monitor Station is restarted it means the user logged on to the computer does not have rights to edit the registry. Both Monitor Station and IP Server require Registry access to save specific settings; in this case, the server list. Login to the computer using a local Administrator account.

Another possibility is that Windows User Access Control is still active. A restart of the computer hosting Monitor Station is required after installation. Restart the computer and import the server list again.

Is there a list of all the ports used by IP Server and their purpose?

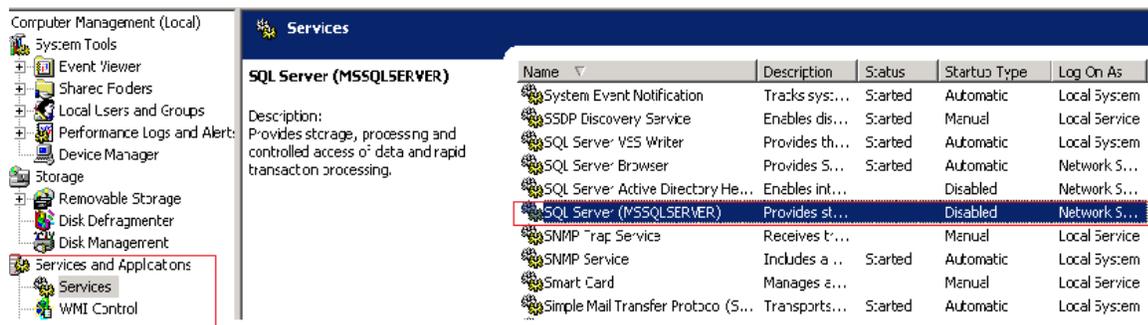
See Appendix A.

What does 'There was a database error, or this version of the database...' mean?

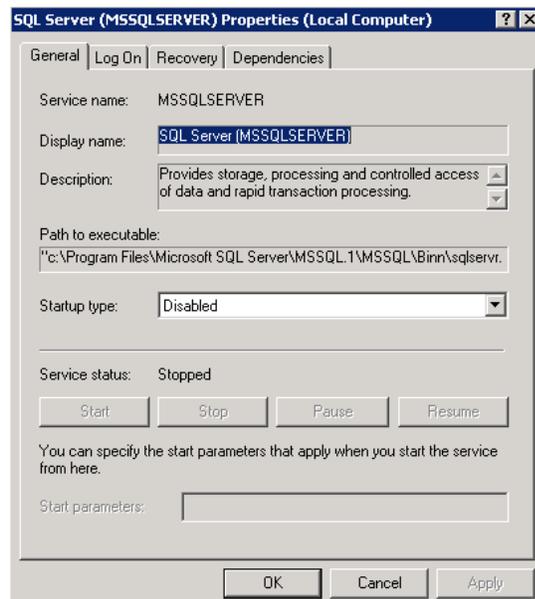
This error may appear in several different areas but is most likely due to a problem with the database. Either Health Monitor or the IP Server is unable to connect to the database to capture current settings and configurations. If you think the problem may be related to an IP address change or credentials you can use [IPSM Diagnostics](#) to check for database connectivity.

This error may also be due to the SQL service not running. To check if the SQL service is running:

1. Start the Administrative Tools applet in Control Panel.
2. Double-click Services.
3. Find the SQL Server (MSSQLSERVER) service.



4. Note the Status and Startup Type values for this service.
5. Right-click the service and select Properties.



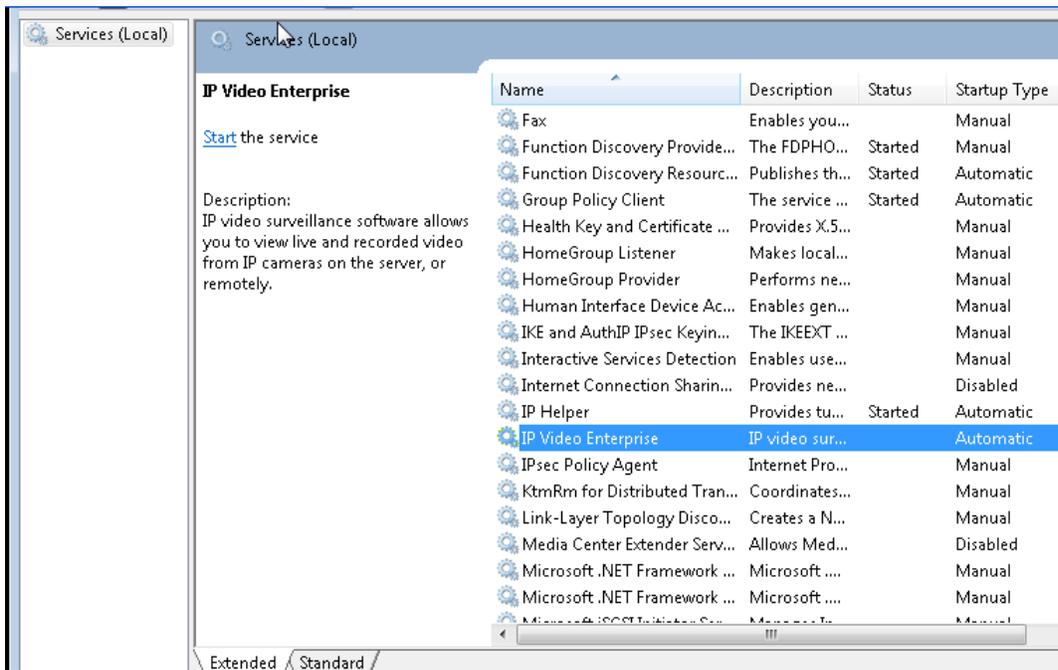
1. Select Automatic from the Startup type drop-down menu.
2. Click **Apply**.
3. Click **Start**.

4. Click **OK**.
5. Restart Health Monitor and the IP Service if necessary to reestablish a connection.

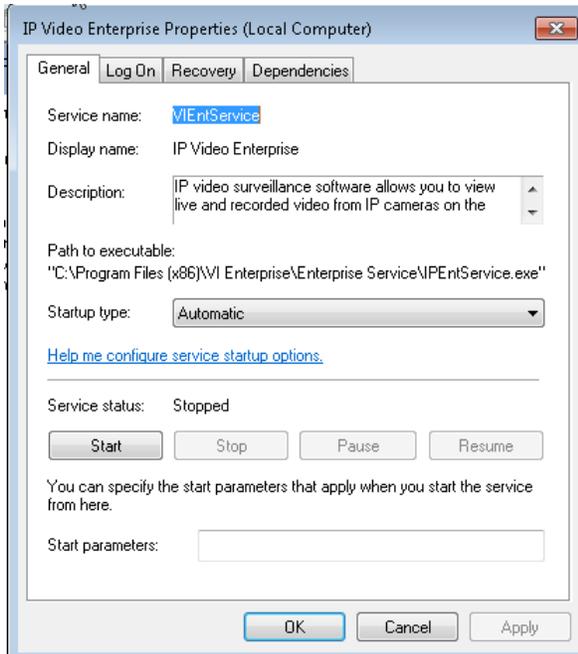
How do I set the IP Service to restart in the event of a crash?

You can set Windows service parameters to automatically restart a service in the case of a crash.

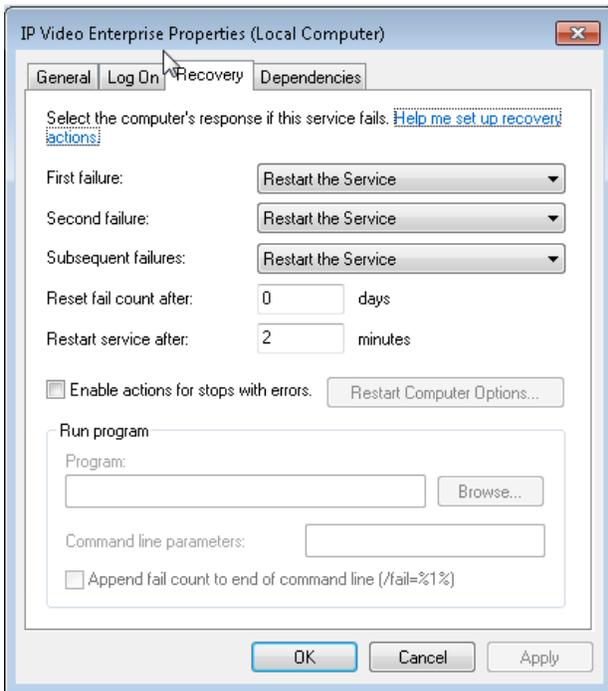
1. Start the Administrative Tools applet in Control Panel.
2. Double-click Services.
3. Find the IP Video Enterprise service.



4. Note the Status and Startup Type values for this service.
5. Right-click the service and select Properties.



Click the Recovery tab.



The installation of IP Server automatically sets this parameter to restart the service on failure.

How do I backup and restore my Video Insight database?

Backing up your database regularly is good IT practice. Regular backups speed disaster recovery.

To back up your database:

1. Click the **Start** button.
2. Enter *services.msc* and then press Enter.
3. Find the SQL Server (MSSQLSERVER) service.
4. Right-click on the service and select Stop.
5. Using Windows Explorer, browse to *C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\DATA*
6. Copy the files *Insightent.mdf* and *Insightent_log.ldf* to a safe location.
7. Click the **Start** button.
8. Enter *regedit* and then press Enter.
9. Browse to *HKLM>Software>Video Insight*.
10. Right-click the Video Insight folder and select Export.
11. Save this file to the same location that you put your database files in.

To restore your database:

1. Click the **Start** button.
2. Enter *services.msc* and then press Enter.
3. Find the SQL Server (MSSQLSERVER) service.
4. Right-click on the service and select Stop.
5. Browse to where you saved *InsightENT.mdf* and *InsightENT_Log.ldf*.
6. Copy the files to *C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\DATA*.
7. Click **OK** to replace the existing files.
8. Return to where you saved your database files and double-click your registry export file (.reg).
Your registry keys are re-installed.
9. Repeat steps 1-3.
10. Right-click on the service and select Start.

I'd like to migrate all of my servers to one centralized database.

Review the [Database considerations](#) and [Storage considerations](#) to choose the proper server to migrate to.

1. Stop the service on all secondary servers.
2. Uninstall SQL from all secondary servers. This is optional.
3. Delete ServerID from the registry on secondary servers by:
 - a. Click the **Start** button.
 - b. Enter *regedit* and then press Enter.
 - c. Browse to *HKLM>Software>Video Insight>IP Server Ent*.
 - d. Right-click on ServerID key.
4. Run [Initialization](#) on secondary servers. See page 25 for more information.

5. Enter the new SQL information.
6. Restart the IP Service.

How do I completely remove Microsoft SQL without reformatting the drive?

Completely removing SQL is a bit more complicated than simply using Add/Remove Programs in Control Panel. Add/Remove Programs does not remove everything and remnants will interfere with a new install of SQL and the Video Insight software. There are three methods of removing SQL manually:

Note

Making changes to your registry can make your Microsoft Windows operating system unusable. We recommend backing up your registry before making any changes.

Method 1

1. Remove SQL using Add/Remove Programs. If you are using MSDE, there is only one entry. If you are using SQL Express, there are four. Remove the top entry first and then proceed to the next.
2. Download MSIINV and MSIZAP from <http://www.downloadvi.com/downloads/ftp>.
3. Extract the files to C:\.
4. Click the **Start** button.
5. Enter '*cmd*' and then press Enter.
6. At the command prompt enter `cd \`.
7. Enter `msiinv >C:\openme.txt`.
8. Using Windows Explorer, browse to C:\ and open the file named openme.txt.
9. Press the CTRL and F keys to open a search box.
10. Enter SQL and click **Find**.
11. After SQL is found locate {product id} and note it. Leave the document open.
12. Return to the command prompt and enter `msizap T {product id}`. Include the brackets with the product ID.
13. Repeat step 12 until all SQL references are removed.
14. To verify that all services have been removed, click the **Start** button.
15. Enter `services.msc` and then press Enter.
16. In the Services list locate any service that starts with Microsoft SQL or SQL.
17. Right-click each of these and select Stop.
18. Click the Start button.
19. Enter `cmd` and press Enter.
20. Return to the command prompt and enter `cd \`.
21. Enter `sc query state= all >c:\openme1.txt`.
22. Return to Windows Explorer and browse to C:\ and open the file named openme1.txt.

23. Press the CTRL and F keys to open a search box.
24. Enter SQL then click **Find**.
25. After SQL is found locate Service Name.
26. Return to the command prompt and enter `sc delete <service name>`.
27. Repeat step 25 until all services are removed.
28. Return to Windows Explorer and browse to `C:\Program Files` and delete the Microsoft SQL Server folder.
29. Click the **Start** button.
30. Enter `regedit` and then press Enter.
31. Browse to `HKLM>software>Microsoft`.
32. Remove any object that has SQL in the name.
33. Browse to `HKLM>Services>Current Control Set`.
34. Remove any object that has SQL in the name.
35. Shutdown and restart the server before attempting another installation.

Method 2

1. Download Microsoft Windows Installer Clean Up Utility from <http://www.support.microsoft.com/kb/290301>.
2. Install the utility.
3. Start the program.
4. Select the product you want to uninstall and then click **Remove**.
5. Using Windows Explorer, browse to `C:\Program Files` and delete the Microsoft SQL Server folder.
6. To verify that all services have been removed, click the **Start** button.
7. Enter `services.msc` and then press Enter.
8. In the Services list locate any service that starts with Microsoft SQL or SQL.
9. Right-click each of these and select Stop.
10. Click the **Start** button.
11. Enter `cmd` and then press Enter.
12. At the command prompt enter `cd \`.
13. Enter `sc query state= all>c:\openme1.txt`.
14. Return to Windows Explorer and browse to `C:\` and open the file named `openme1.txt`.
15. Press the CTRL and F keys to open a search box.
16. After SQL is found locate Service Name.
17. Return to the command prompt and enter `sc delete <service name>`.
18. Repeat step 17 until all services are removed.
19. Click the **Start** button.
20. Enter `regedit` and then press Enter.
21. Browse to `HKLM>software>Microsoft`.
22. Remove any object that has SQL in the name.
23. Browse to `HKLM>Services>Current Control Set`.

24. Remove any object that has SQL in the name.
25. Shutdown and restart the server before attempting another installation.

Method 3

1. Download CCleaner from <http://www.piriform.com/ccleaner/download/standard>.
2. Install the software. Uncheck the option to install the Toolbar.
3. Run the program.
4. Click the Tools menu, select the software and then click **Run Uninstaller**.
5. Using Windows Explorer, browse to C:\Program Files and delete the Microsoft SQL Server folder.
6. To verify that all services have been removed, click the **Start** button.
7. Enter `services.msc` and then press Enter.
8. In the Services list locate any service that starts with Microsoft SQL or SQL.
9. Right-click each of these and select Stop.
10. Click the **Start** button.
11. Enter `cmd` and then press Enter.
12. At the command prompt enter `cd \`.
13. Enter `sc query state= all>c:\openme1.txt`.
14. Return to Windows Explorer and browse to C:\. and open the file named openme1.txt.
15. Press the CTRL and F keys to open a search box.
16. After SQL is found locate Service Name.
17. Return to the command prompt and enter `sc delete <service name>`.
18. Repeat step 17 until all services are removed.
19. Click the **Start** button.
20. Enter `regedit` and then press Enter.
21. Browse to `HKLM>software>Microsoft`.
22. Remove any object that has SQL in the name.
23. Browse to `HKLM>Services>Current Control Set`.
24. Remove any object that has SQL in the name.
25. Shutdown and restart the server before attempting another installation.

I'm getting errors when playing recordings in Windows Media Player and Video Insight's Media Player.

Errors like “unable to play file”, black screen, or “SonyNetwork.dll didn't load” when attempting to play recordings in Windows Media Player or in Video Insight Media Player are usually indicative of codecs missing on that server. Codecs allow video players to decode video files and play them properly. Video Insight recommends downloading and installing the latest codecs package on every server expected to play back videos.

http://download.cnet.com/Windows-7-Codec-Pack/3000-13632_4-10965840.html?tag=mncol;3

How do I add a VP1, VP8, VP16 Encoder or an Arecont-type camera with multi channels?

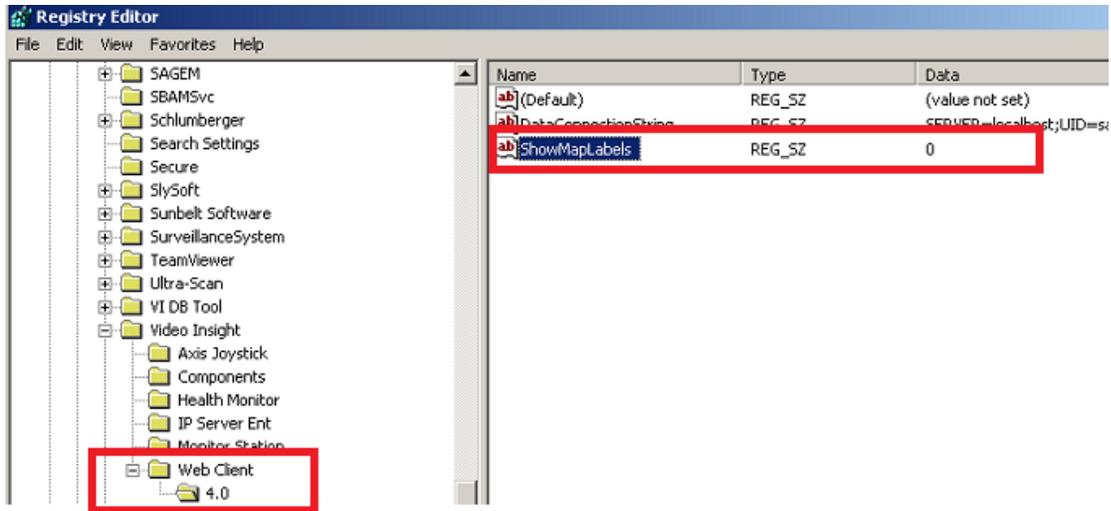
Multi-channel devices are cost effective inclusive devices with either multiple ports such as the Video Insight VP series of encoders or multiple eyes such as Arecont cameras. Adding them to our software is as simple as checking the channel number and assigning it a port number (1-16 for VP encoders) or eye position (1-4 for Areconts).

How do I disable Map Labels for the Web Client?

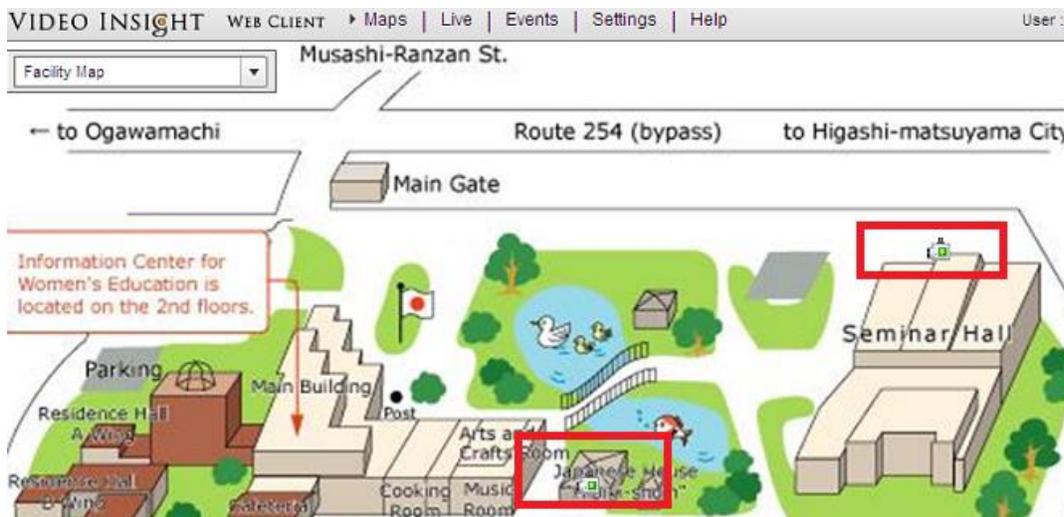
Facility Maps can have lots of cameras and their names can clutter the map. To remove camera names in the Web Client map view you must add a registry key. Figure x shows a Facility Map with camera names.



1. Click the **Start** button.
2. Enter *regedit* and then press Enter.
3. Browse to *HKEY_LOCAL_MACHINE>SOFTWARE>Video Insight>Web Client>4.0* . Note, this path is for a 32-bit system. For 64-bit systems use the Wow64 folder.
4. On the left side pane right-click and select New and then select String Value.
5. Enter ShowMapLabels and then press the Enter key.
6. Right-click the new string value and select Modify.
7. Enter 0 in the Value Data field.



The figure below shows the same Facility Map without camera names.



My C-drive is filling up due to Temp Cache, how do I clear it?

Viewing videos in Web Client adds temporary folders on the local computer while buffering or downloading video. Windows saves a local copy and does this automatically to avoid downloading the same media again. There are two ways to remove these files and create some space:

Automatically:

“First go to Start, then run and type in gpedit.msc

Next select -> Computer Configuration/Administrative Templates/Windows Components/Terminal Services/Temporary Folder. Then right-click "Do Not Delete Temp Folder upon Exit". Go to properties

and click **Disable**. Now next time Windows puts a temp file in that folder it will automatically delete it when it's done! Remember, GPEDIT (Group Policy Editor) is only available in XP Pro." (Source: <http://www.marvswindowstips.com/cleanup.htm>)

Manually:

1. Click the **Start** button.
2. Enter %TEMP% and then press Enter.
3. Sort files by descending date.
4. Select the files you want to remove and press the Delete key.

Online Resources

Youtube Tutorials: <http://www.youtube.com/user/videoinsighttv>

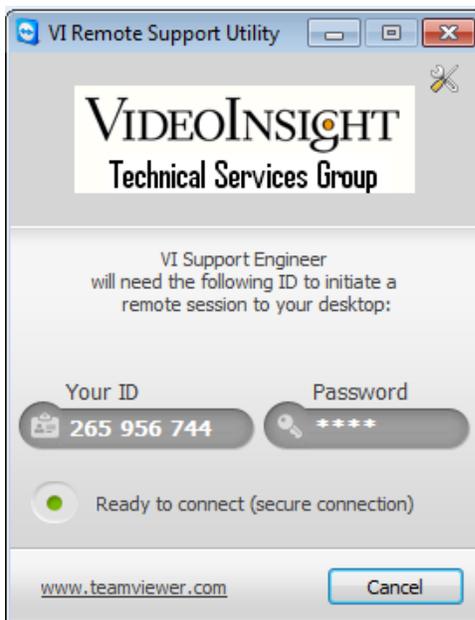
Downloads: <http://downloadvi.com>

Remote Support

If you require personal assistance from one of our Technical Support representatives, please contact us using one of our [contact methods](#). Install the Team Viewer client application prior to requesting remote support.

To install Team Viewer:

1. Browse to <http://www.downloadvi.com>
2. Click the VI Remote Support QS button.
3. Click **Run** at the prompt.
4. Click **Run** again.
5. Call us at Technical Support at 713-621-9779.
6. Give the representative your ID. Your ID is randomly generated every time you request remote support.



7. The representative will log on to your computer and show you how to correct the issue or fix it for you.

Contact Us**In person:**

3 Riverway, Suite 700
Houston, Texas 77056

Hours of Operation:

9:00 AM - 6:00 PM CST, Monday – Friday

By Phone: 713-621-9779

800-513-5417

By Fax: 713-621-7281

Sales Department:

713-621-9779

Technical Support Hours: 8:00 AM - 6:00 PM CST, Monday – Friday

For **Saturdays and Holidays:** 10:00 AM - 2:00 PM

Please call our Answering Service at **877-743-2403** and the support engineer on call will be paged to assist you.

By Email: support@video-insight.com

Feature Request <http://www.questionpro.com/akira/TakeSurvey?id=1028953>

Appendices

Appendix A: IP Server port list

Appendix B: Current Customers Examples

Appendix C: Commonly Used Camera Credentials

Appendix D: Configuring a CNB camera

Appendix E: Configuring Sentry FS1000 and FS2000 cameras

Appendix F: Configuring an IQEye Camera using Optional Controls

Appendix A: IP Server port list

Port Number	Name	Purpose
4010	Data Port	Sends live video streams from IP Server to Monitor Station
4011	Command Port	To get and set system information by Monitor Station
3010	Ovid Server	Communication between S2, IP Server and the Ovid Server for Video Insight and S2 Access Control Configuration
80	HTTP	IIS for serving the Web Client Note: Some ISPs block port 80 access. You may need to configure IIS to use a different port
2051	MonitorCast	Access control communication between Video Insight and MonitorCast
554	RTSP	Specific camera properties
21	FTP	Specific camera properties
11000	N/A	Communication between IP Server and Health Monitor
636	Active Directory SSL	Active Directory configured with Secure Socket Layer (SSL)
389	Active Directory non-SSL	Active Directory configured without Secure Socket Layer (SSL)

Appendix B: Current Customers Examples

Klein ISD – is using HP servers with Dual Xeon E554 2.53GHz processors with 8GB memory and Windows 2003 Server.

1. Server CS21 has (90) 1.3MP H.264 cameras
2. Server 41 has (100) 1.3MP H.264 cameras and (30) D1 cameras running MJPEG

Server Name	Max Cameras	Used	Available	Serial Number	Processor %	Memory Available
CS 21	150	120	30	69247	13 %	6732 MB
CS 23	150	140	10	317DA	15 %	6808 MB
CS 25	200	72	128	12345	10 %	7016 MB
CS 27	150	116	34	C116A	10 %	6898 MB
CS 29	150	89	61	F64A2	11 %	6891 MB
CS 33	150	64	86	552F0	3 %	7011 MB
CS 35	150	105	45	06678	13 %	6822 MB
CS 37	150	86	64	4A4D6	5 %	6960 MB
CS 39	150	63	87	3CDA1	5 %	7096 MB
CS 41	300	130	170	0429B	7 %	6291 MB
CS PD	150	24	126	8451A	34 %	2468 MB
CS-KMS	40	11	29	12345	28 %	1976 MB

Pflugerville ISD – is using Dell R510’s with Dual Xeon E5620 2.4GHz processors, 12GB memory and Windows Server 2008 R2. The servers are running 1,200 2MP H.264 cameras and 400 D1 cameras spread across the servers.

Server Name	Max Cameras	Used	Available	Serial Number	Processor %	Memory Available
VS01 .31	300	141	225	F789F	5 %	4312 MB
VS02 .32	300	147	225	AA475	3 %	3877 MB
VS03 .33	300	148	230	9C205	2 %	2843 MB
VS04 .34	300	246	177	B7347	9 %	3074 MB
VS05 .35	300	169	197	B0554	7 %	3236 MB
VS06 .36	300	218	194	E2528	14 %	2580 MB
VS07 .37	300	191	191	5C790	11 %	3370 MB
VS07 .38	300	208	194	47B84	19 %	2689 MB
VS09 .39	300	156	215	1099A	7 %	3282 MB
VS10 .40	300	117	241	816CA	5 %	3683 MB
IP Server -10.225.187.41	300	0	300	D5292	0 %	10772 MB
VS12 .42	300	0	300	BD600	0 %	10856 MB
VS13 .43	300	15	294	AD283	1 %	7601 MB

Recommendations - the following are general guidelines based on the previous discussion assuming Xeon processors and camera side motion detection:

- a. D1 or 4CIF cameras – 150-200 cameras per OS
- b. 1.3 MP cameras – 90 cameras per OS
- c. 3 MP cameras – 50 cameras per OS

Appendix C: Commonly Used Camera Credentials

Here is a list of the default usernames/passwords for a few of the supported IP camera manufacturers. Should your camera model not appear here please refer to the manual included with your camera.

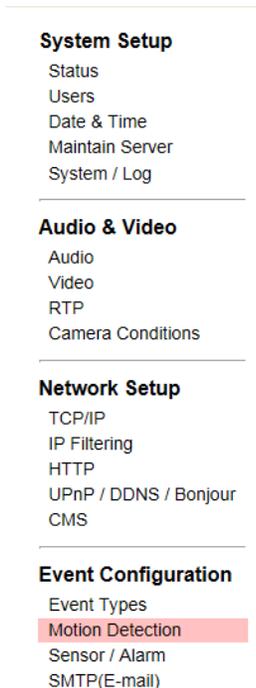
Brand	UserName	Password	Notes
3S	root	root	
Acti	Admin	123456	or 'admin' with lowercase a
Arecont Vision			No credentials needed
Avigilon	admin	admin	
Axis	root	blank or pass	You will be asked to create a root password the first time you go into the cameras interface.
Basler	admin	admin	
Bosch Dinion			No credentials needed
Brickcom	admin	admin	
Cisco			You will be asked to create a root password the first time you go into the cameras interface.
Dlink	root	blank	
Grandstream	admin	admin	
Hikvision	admin	12345	
Honeywell	Administrator	1234	
Huviron	Admin	admin	To change settings
Huviron	root	root	To view images
Infinova	infinova	INFINOVA	
IPX-DDK	root	admin	Also try 'Admin'

IQeye	root	system	
IQinVision	root	system	
Mobotix	admin	meinsm	
Panasonic	admin	12345	
Pelco Sarix	admin	admin	
Pixord	admin	admin	
Samsung Electronics	root	root	or admin/4321
Samsung Techwin (new)	admin	4321	
Samsung Techwin (old)	admin	1111111	
Sanyo	admin	admin	
Scallop	admin	password	
Sony	admin	admin	
Stardot	admin	admin	
Starvedia	admin	leave blank	
Toshiba	root	ikwb	
Toshiba	root	ikwd	
Trendnet	admin	admin	
Ubiquiti	ubnt	ubnt	
VideoIQ	supervisor	supervisor	
Vivotek	root	leave blank	
VP16	admin	12345	
VP16-A	Admin	12345	

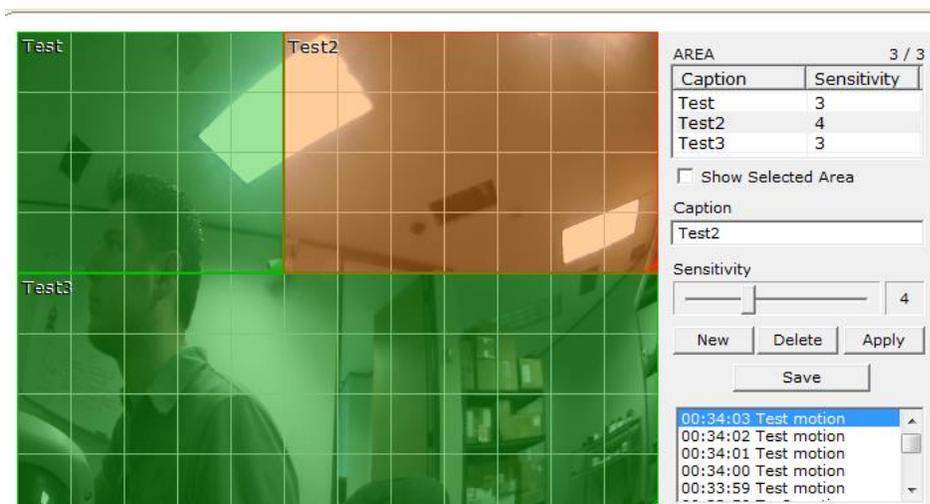
Appendix D: Configuring a CNB camera

Due to the nature of the CNB camera integration and the capabilities of the camera will turn on Motion detection inside the camera, but we cannot draw zones inside the Motion Detection page, all zones must be created inside the CNB web page under Motion Detection as shown below.

1. Access the camera's Web page



2. Click the Motion Detection option



With the CNB cameras the best way for Motion Detection to work is to draw at least two zones; the camera will not detect motion anywhere there is not a zone and allows you to draw up to three zones.

The Sensitivity adjusts the threshold for the amount of motion that needs to occur. The lower the number, the less amount of motion that needs to occur to trigger a motion event, setting the Sensitivity to 10 turns off Motion Detection in that area.

Motion Zones can over lap and it appears the zone with the lower sensitivity takes precedence over the other zone.

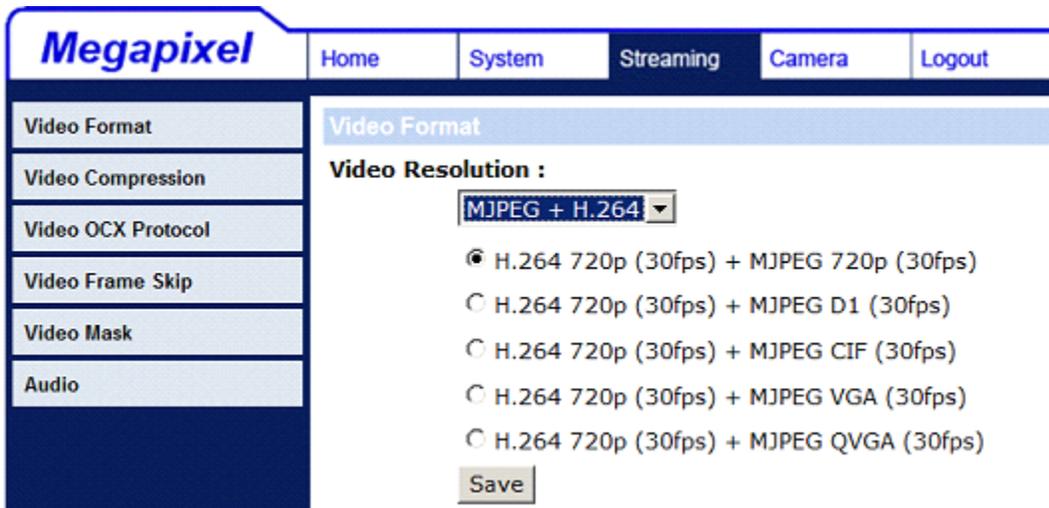
The window is dynamic once you save the changes you have made, but as you can see from the picture, it does not tell you the amount of motion, just that motion has occurred and in which zone.

While testing we discovered that a zone with sensitivity between 3 and 5 work the best, but it will depend on the size of the zone drawn as well. The bigger the zone, the lower the number will need to be.

Appendix E: Configuring Sentry FS1000 and FS2000 cameras

Web client requirement of cameras streaming JPEGs may require specific configuration to ensure these two models are streaming both H.264 and JPEG to properly display in Monitor Station and the Web Client.

If the Sentry cameras you are de-warping have menus that look like this:



Then the correct setting should be H.264 + MJPEG for the web client and the dewarp to work properly.

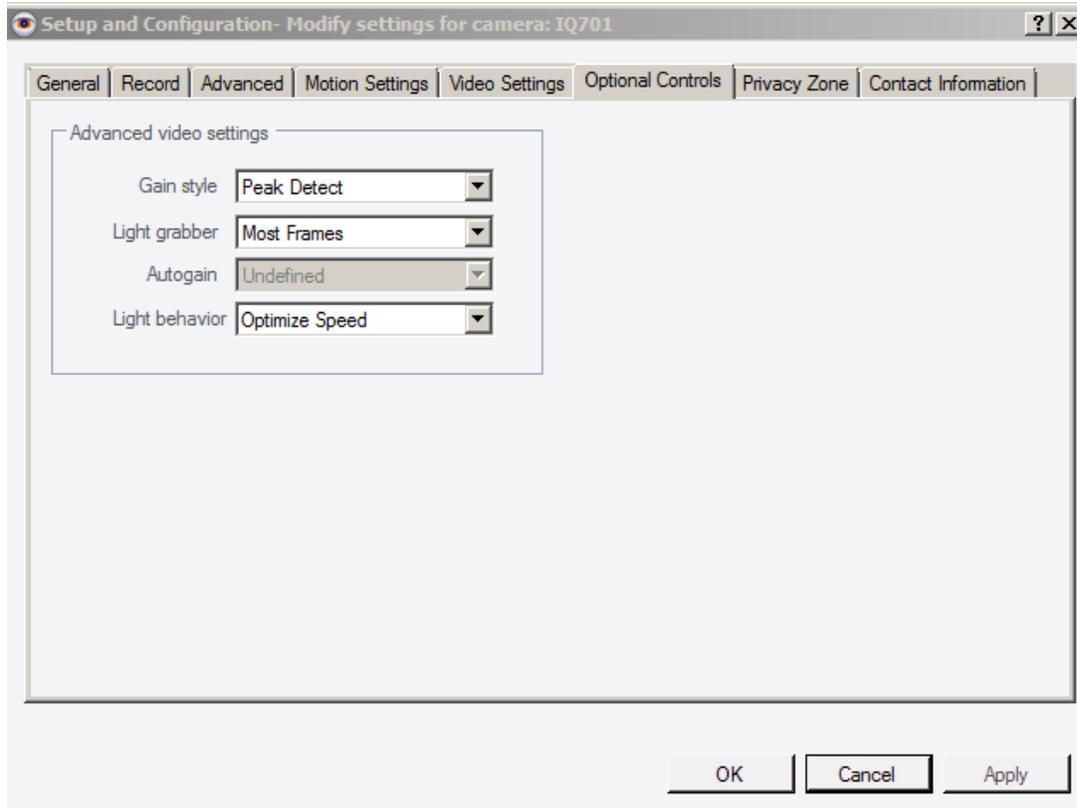
Conversely, if the camera's web interface looks like this:



No changes are needed; the camera streams both h.264 and JPEG as requested, regardless of what the image settings are set to.

Appendix F: Configuring an IQEye Camera using Optional Controls

Once the camera is added to the software, access the Optional Controls tab in the Camera's Properties.



These controls change the way that the IQ Eye cameras handle different light settings and adjust the iris accordingly.

Gain Style- The autogain algorithm of your camera will set brightness to best display. The gain style setting chooses which pixels within the exposure window will be used by the autogain algorithm for setting brightness levels.

- **Peak Detect:** uses only the brightest pixels in the exposure window, making sure they're appropriately-adjusted for bright pixels. This is a good setting for watching bright areas.
- **Backlight:** uses only the darkest pixels in the exposure window, making sure they're appropriately-adjusted for dark pixels. This is a good setting for outdoor scenes where you want to watch a shaded region.
- **Average:** uses **all** of the pixels in the exposure window. This is a good setting for indoor scenes where there are no very bright or very dark areas to skew the gain calculations.

- **Clip Average:** uses all pixels **except** for the very darkest and brightest pixels. This is a good setting for outdoor scenes where you want to ignore both sky and shadows and to watch a region of intermediate brightness levels. This is also a good setting for interior scenes.

- Undefined- This setting turns off Gain Style

Light Grabber- Enables or disables special processing for low-light images. These values can be seen at the camera's web page under Image tab.

- Most Frames- Sets the Light Grabber value to 4x, which specifies "integration" of four frames, twice the lowlight correction as the 2x setting which specifies integration of two frames.

- Medium- Sets the Light Grabber value to 2x.

- Undefined- Sets the Light Grabber value to 4x

- Disabled- Turns Light Grabber off at the camera.

Light Behavior- This setting adjusts the electronic shutter values for the IQeye camera

- **Optimize speed:** Use this setting for fast moving subjects. This setting may cause images to appear grainy in low light conditions.

- **Optimize quality:** Use this setting for high quality images. This setting may cause images to blur in low light conditions.

- **Auto:** This setting is ideal when there is adequate light and objects are not moving too fast.

The other values set a fixed exposure. This is useful for tuning a camera to minimally changing conditions or to capture objects moving at predictable speeds. The list of available exposures may change based on other settings like frame rate, Light Grabber and resolution.

Index

3

30 Second Review pop-up144

A

Adding a Map..... 123, 124, 134

Adding cameras209

Administration>Setup and Configuration111

Auto Restart.....64

C

Cameras16

COLDSTORE.....17

Contextual right click menu

For Cameras139

For Facility Map141

For Layout140

For Servers and Server Groups138

Contextual right-click menu.....138

Creating a clip144

D

Downloading a recorded file145

E

Enterprise View

Left Navigation View Options42, 43, 134, 142, 147

F

Facility Maps115

Adding a Map.....115

Deleting a Map119

Facility Map toolbar.....146

Modifying a Map.....119

Renaming a Map.....120

File Manipulation Rule.....17

File Menu

Exit79

Media Fixer75

H

Health Monitor tab.....58

I

IP Server19

L

Layouts.....121

Adding Layout Tour122

Adding Layouts121

Left navigation tree134

Left Navigation Tree

Enterprise View42, 43, 134

Facility Map View.....142

Layout View147

Licensing16

Live View Monitor.....133

Adding a Live View133

Deleting a Live View.....133

Modifying a Live View.....134

Long Term Storage Application17

M

Maintenance plan.....255

Maintenance tab229

Monitor Station15

N

Network.....13

P

PTZ

Controls pane148

PTZ controls84

PTZ controls84

PTZ Operations

Creating a preset87

R

RAID17

Router configuration16

Rules Manager128

S

Server.....11

Server Group.....135

Server States.....136

Setup and Configuration Left Navigation Tree113

Setup and Configuration Tools Node.....114

SQL Password25

SQL Server.....	25	System Log.....	89
SQL Username:	25	TV decoders	131
Storage considerations	17	Adding a decoder.....	131
<i>T</i>		Deleting a decoder	132
Tools Menu		Modifying a decoder.....	132
Options		<i>V</i>	
Audio tab	109	View Menu	
Live Window tab	103	Cycle Layouts	82
Startup tab.....	110	View Menu	
Tools Configuration tab	98	Archive Tree.....	79
Tools Menu		Full Screen	81
Axis Joystick Control	89	Layout	81
Live Window	91	Mini Toolbars.....	82
Media Player.....	92	View Menu	
Options	92	Toolbars	88
General tab	93	<i>W</i>	
PTZ Operations	92	Web Client	15
Synchronized Player	92		