Panasonic

Video Insight 7.5.1 IP Server Administrative Guide

Last updated: Oct/28/2019

TABLE OF CONTENTS

SOFTWARE LICENSE AGREEMENT

1. **IMPORTANT - READ CAREFULLY BEFORE ACCESSING THIS SOFTWARE**: This license agreement ("License Agreement") is a legal agreement between the user (referred to herein as "You" or "Licensee" and meaning either an individual or a single entity) and Panasonic System Solutions Company of North America, Division of Panasonic Corporation of North America, and its suppliers (collectively, "PSSNA" or "Licensor") for the Software (the "Software"). BY USING OR ACCESSING THE SOFTWARE; LOADING THE SOFTWARE OR ALLOWING THE SOFTWARE TO BE LOADED; OR UTILIZING ANY DEVICE OR OTHERWISE UTILIZING THE SERVICES OR FUNCTIONALITY OF THE SOFTWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE AGREEMENT, YOU MAY RETURN THE SOFTWARE TO YOUR PLACE OF PURCHASE FOR A FULL REFUND.

2. **GRANT OF LICENSE.**

   a. Overview of the License Agreement. This License Agreement describes your rights to use or otherwise utilize the Software. This License Agreement does not entitle You to any ownership rights of the programming code. The Software is licensed, not sold. The Software is protected by copyright and other intellectual property laws and treaties. PSSNA owns the title, copyright and other intellectual property rights in the Software. You may not rent, lease, or lend the Software or transfer the License Agreement to another user.

   b. System Limits. You may use the Software with one unique system identified by its Mac address. Each unique system requires a separate License Agreement.

3. **TERMINATION.** Without prejudice to any other rights, PSSNA may terminate this License Agreement if You do not abide by the terms and conditions herein, in which case you must destroy all copies of the Software and/or return the Software to PSSNA and all its component parts.

4. **TRANSFER.** You may move the Software to a different server.

5. **LIMITATION ON REVERSE ENGINEERING, DECOMPILATION AND DISASSEMBLY.** You may not reverse engineer, decompile, or disassemble the Software.

6. **CONSENT TO USE OF DATA.** You agree that PSSNA and its affiliates may collect and use any technical information You provide as part of support services related to the Software. PSSNA agrees not to use this information in a form that personally identifies You.

7. **LIMITED WARRANTY.** Because of uncertain or unknown conditions and incidental hazards under which the Software is used, PSSNA does not warrant or guarantee that any particular result will be achieved. PSSNA disclaims all liability and responsibility for damages or other loss caused by any independent supplier/installer of the Software or other third-party. The sole and exclusive warranty provided by PSSNA is that (1) the media on which the Software is furnished will be free of defects in materials and workmanship; and (2) the Software substantially conforms to its published specifications (the "Limited Warranty"). The Software is warranted only for its initial installation. This warranty shall survive inspection of, payment for and acceptance of the Software, but in any event, shall expire ninety (90) days after the date you receive the Software, unless prohibited by law. Any supplements or updates to the Software, including without limitation service packs (if any) or hot fixes provided to You after the expiration of the ninety-day Limited Warranty period are not covered by any warranty or condition, express, implied or statutory. **Except for the Limited Warranty as set forth herein, PSSNA provides the Software and support services (if any) "AS IS" AND WITH ALL FAULTS. THERE ARE NO OTHER WARRANTIES (NOR REPRESENTATIONS) HEREUNDER OR ELSEWHERE MADE BY PSSNA, EXPRESS OR IMPLIED, AND ALL OTHER WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, SUITABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OF GOOD AND WORKMANLIKE PERFORMANCE, ALL WITH REGARD TO THE SOFTWARE AND THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT SERVICES, ARE DISCLAIMED BY PSSNA AND EXCLUDED FROM THIS AGREEMENT. ALSO, THERE IS NO WARRANTY OR CONDITION OF TITLE, QUIET ENJOYMENT, QUIET POSSESSION, AND CORRESPONDENCE TO DESCRIPTION OR NON-INFRINGEMENT WITH REGARD TO THE SOFTWARE. NO AFFIRMATION WHETHER BY WORDS OR ACTIONS BY PSSNA, ITS AGENTS, EMPLOYEES OR REPRESENTATIVES SHALL CONSTITUTE A WARRANTY.**

8. **Limited and Exclusive Remedy.** PSSNA's sole responsibility and Your exclusive remedy for any nonconformance or defect in the Software is expressly limited to the replacement of the Software or the refund of the license fees, if any, as determined by PSSNA, in its sole discretion, to the extend PSSNA confirms that the Software possess such a defect. As a condition precedent to any remedy described herein, or otherwise available to You, You shall seek and accept PSSNA's reasonable effort to replace the allegedly defective or nonconforming Software. In furtherance of such undertaking, if You reasonably believe that the Software contains a defect or nonconformity for which PSSNA is responsible, You shall inform PSSNA immediately by telephone at (713) 621-9779 and by providing written notification to PSSNA within forty-eight (48) hours of discovery. All returned Software shall be shipped at customer's expense. This Limited Warranty is void if failure of the Software has resulted from accident, abuse, misapplication, abnormal use, or a virus. Any replacement Software will be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer.

9. **NO CONSEQUENTIAL OR OTHER DAMAGES**. NOTWITHSTANDING ANYTHING TO THE CONTRARY, EXPRESS OR IMPLIED, (1) PSSNA'S LIABILITY FOR ANY CLAIM OR ACTION OF ANY KIND ARISING OUT OF, IN CONNECTION WITH OR RESULTING FROM THE MANUFACTURE, SALE, DELIVERY, RESALE, TRANSFER, USE OR REPAIR OF THE SOFTWARE OR SERVICES RENDERED BY PSSNA

UNDER THIS LICENSE AGREEMENT SHALL NOT EXCEED THE PRICE, IF ANY, YOU PAID FOR THE SOFTWARE OR $5.00, WHICHEVER IS GREATER; AND (2) PSSNA SHALL IN NO EVENT BE LIABLE FOR SPECIAL, INDIRECT, PUNITIVE, INCIDENTAL OR CONSEQUENTIAL DAMAGES OR CONTINGENT LIABILITIES ARISING OUT OF THIS LICENSE AGREEMENT OR THE FAILURE OF THE SOFTWARE TO OPERATE PROPERLY, INCLUDING BUT NOT LIMITED TO ANY DAMAGE OCCASIONED BY DELAY, DOWNTIME, LOST BUSINESS OPPORTUNITY, LOSS OF CONFIDENTIAL INFORMATION, LOSS OF PRIVACY, LOST PROFITS OR OTHERWISE (NOTWITHSTANDING THE CAUSE OF SUCH DAMAGE AND WHETHER OR NOT CAUSED BY PSSNA'S NEGLIGENCE, FAULT OR STRICT LIABILITY). CUSTOMER ASSUMES THE RISK FOR AND INDEMNIFIES PSSNA FROM AND AGAINST ALL LIABILITIES FOR ANY LOSS, DAMAGE OR INJURY TO PERSONS OR PROPERTY ARISING OUT OF, CONNECTED WITH OR RESULTING FROM THE USE OF OR INABILITY TO USE THE SOFTWARE, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT SERVICES, OR THE POSSESSION, USE OR APPLICATION OF THE SOFTWARE, EITHER ALONE OR IN COMBINATION WITH OTHER PRODUCTS. PSSNA ASSUMES NO RESPONSIBILITY OR LIABILITY, WHETHER EXPRESS OR IMPLIED, WHETHER IN TORT OR IN CONTRACT, AS TO THE CAPACITY OF THE SOFTWARE TO SATISFY THE REQUIREMENT OF ANY LAW, RULE, SPECIFICATION, OR CONTRACT PERTAINING THERETO, INCLUDING, BUT NOT LIMITED TO, ANY CONTRACT BETWEEN ANY CUSTOMER OF ITS PRODUCTS AND PARTIES WITH WHOM SUCH CUSTOMER HAS CONTRACTED.

10. INDEMNIFICATION: YOU AGREE TO PROTECT, INDEMNIFY, HOLD HARMLESS AND DEFEND PSSNA FROM AND AGAINST ANY CLAIMS, DEMANDS, LIENS, CAUSES OF ACTION, JUDGMENTS, LOSSES AND LIABILITIES OF ANY NATURE WHATSOEVER ARISING IN ANY MANNER, DIRECTLY OR INDIRECTLY OUT OF OR IN CONNECTION WITH OR IN THE COURSE OF OR INCIDENTAL TO (1) YOUR WORK OR OPERATIONS WITH THE SOFTWARE REGARDLESS OF CAUSE OR OF THE SOLE, CONCURRENT OR CONTINUING FAULT OR NEGLIGENCE OF PSSNA OR ITS EMPLOYEES OR AGENTS; OR (2) ANY BREACH OR FAILURE TO COMPLY WITH ANY OF THE PROVISIONS OF THIS LICENSE AGREEMENT. YOU AGREE TO PROTECT, INDEMNIFY, HOLD HARMLESS AND DEFEND PSSNA FROM AND AGAINST ANY CLAIMS, DEMANDS, LIENS, CAUSES OF ACTION, JUDGMENTS, LOSSES AND LIABILITIES FOR INJURY TO OR DEATH OF YOU, YOUR AGENTS OR EMPLOYEES OR ANY EMPLOYEE OR AGENTS OF ANY CO-VENTURER, CONTRACTOR, SUBCONTRACTOR OR PERSONS AT YOUR WORK LOCATION ARISING IN ANY MANNER, DIRECTLY OR INDIRECTLY, OUT OF OR IN CONNECTION WITH OR IN THE COURSE OF OR INCIDENTAL TO YOUR WORK OR OPERATIONS WITH THE SOFTWARE, REGARDLESS OF CAUSE OR OF ANY FAULT OR NEGLIGENCE OF PSSNA OR ITS EMPLOYEES OR AGENTS.
11. SEVERANCE: Should any provision of this License Agreement, or a portion thereof, be unenforceable or in conflict with the laws of the United States of America or of any state or jurisdiction which governs any transaction between PSSNA and You, then the validity of the remaining provisions, and any portion thereof, shall not be affected by such unenforceability or conflict, and this License Agreement shall be considered as if such provision, or portion thereof, were not contained herein.
12. UNLAWFUL PURPOSE. Use of the Software for any unlawful purpose or in any unlawful manner, use for any improper or unintended use, or use by anyone other than you are strictly prohibited and constitute a material breach of this License Agreement.
13. APPLICABLE LAW. This License Agreement is governed by the laws of the State of New York without regard to its conflict of laws principles. PSSNA and Licensee hereby agree that exclusive jurisdiction of any, controversy, claim, suit or proceeding arising out of or relating in any way to the Software or this License Agreement or the breach, termination or invalidity thereof shall lie within the courts of the State of New York or within the courts of the United States of America located within New York. PSSNA and Licensee consent to venue and jurisdiction within the Courts of New York, New York.
14. NO WAIVER: Failure to enforce any or all of this License Agreement in a particular instance shall not act as a waiver or preclude subsequent enforcement.
15. ENTIRE AGREEMENT. This License Agreement (including any addendum or amendment to this License Agreement which is included with the Software) constitutes the entire agreement between You and PSSNA relating to the Software and any support services, and this License Agreement supersedes all prior or contemporaneous oral or written communications, proposals, and representations with respect to the Software or any other subject matter covered by this License Agreement. To the extent the terms of any PSSNA policies or programs for support services conflict with the terms of the License Agreement, the terms of the License Agreement shall control.
16. This Software is of the U.S. origin and may be subject to the U.S. export control laws, including the U.S. Export Administration Act and its associated regulations. Licensee agrees that it will not export, re-export or import, directly or indirectly, the Software except in compliance with all applicable laws and regulations.

Rev 04/18

1. 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 can intelligently and efficiently monitor security throughout your organization.

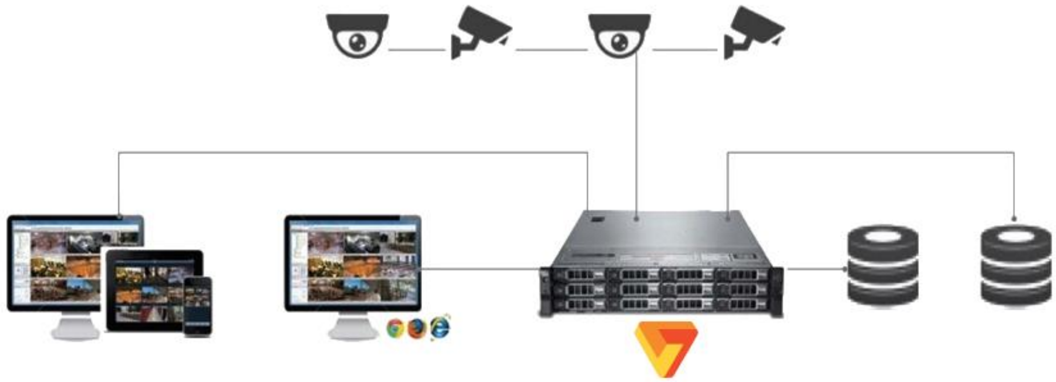
Key features of this version are:

- Updated, easy to use interface
- Support for over 4,100 cameras models
- Alarm Monitoring
- Facility Maps
- Synchronized Playback

This document is intended for use by advanced users and system administrators.

1.1 SYSTEM OVERVIEW

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

There is **no limit** to the number of IP Servers that can be utilized to manage the growing needs of today's IP camera video surveillance needs.

1.2 SOFTWARE COMPONENTS

The Video Insight Enterprise Suite consists in three main components used to monitor live and recorded video: **VI MonitorPlus**, **Web Client** and **VI Mobile**. These three clients can be used to connect to **IP Server** at no additional charge.

1.2.A VI MonitorPlus

VI MonitorPlus is a Thick Client that provides full access to all cameras and access control points within an organization or multiple locations. It features a centralized management and configuration interface for an extended range of video monitoring resources, designed to meet System and Security Administrators' needs.

VI MonitorPlus receives 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.

1.2.B Web Client

Web Client accesses IP Server via Microsoft Internet Information Services (IIS) hosted on the same server as the IP Server. It currently supports HTML5-compatible browsers such as: Google Chrome, Internet Explorer 11+, Mozilla Firefox and Microsoft Edge, among others.

The Web Client can access and manage live and recorded video and Facility Maps; it can also create clips and download recorded video. ***Unlike VI Monitor Plus, Web Client connects directly to the cameras*** to view live video***.***

1.2.C VI Mobile

VI Mobile is a free app available in the App Store for iOS users and Google Play for Android users. VI Mobile gives users access to live and recorded video as well as access to Facility Maps.

1.2.D IP Server

IP Server is the hub of the Video Insight IP Video Management Software (VMS). It supports over 4,100 different camera models from 150 different camera manufacturers. It runs as a Windows service and supports both 32-bit (x86) and 64-bit (x64) Windows environments.

IP Server connects directly to the cameras and can record video locally or write directly to NAS or SAN devices.

2. PLANNING

Getting the most out of the hardware using IP Server software requires planning. Understanding the needs of the environment will help shape the final installation solution. Evaluate and plan the integrations necessary for the most effective installation.

2.1 CONSIDERATIONS BEFORE INSTALLATION

Before beginning the installation process, it is necessary to determine the key system requirements.

Will the system:

- Require multiple-server configuration?
- Utilize a shared SQL environment?
- Utilize a shared network storage solution?
- Be attached to Active Directory or Lightweight Directory Access Protocol (LDAP)?

If the system is going to be a single, standalone installation of IP Server, opting to use the basic installation process is recommended.

If Microsoft SQL Server is already present in your server or environment, then ***only IP Server*** is required to be installed. Otherwise, the downloadable package includes Microsoft SQL Server Express 2012 as the database of choice. Either way, IP Server Enterprise **requires a fully functioning SQL database** as part of its platform

2.1.A IP Server and Accessory Software Installation

Video Insight software supports both **32-bit** and **64-bit** operating systems; some features, however, are limited to use within the 64-bit client only. **Make sure to download the correct version for your operating system**.

NOTE - Administrator-level access to the server is required during the installation and troubleshooting.

Review the following items prior to beginning the installation process:

- Storage Considerations
- Database Considerations
- Network Configuration

The Storage and Bandwidth calculator is available online to gauge your platform's needs: http://www.video-insight.com/storage-and-bandwidth-calculator

(1) IP SERVER ESSENTIAL REQUIREMENTS

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

- Windows Server 2008 R2 Web, R2 Standard, R2 Enterprise and R2 Datacenter.
- Windows Server 2012 and Server 2012 R2.
- Windows Server 2016 Standard.
- Windows 7 Pro, 10 Pro, Enterprise and Education.

IP Server requires Microsoft .NET Framework 4.5+ and Microsoft Internet Information Services (IIS) with "static content" enabled. Because Video Insight hardware and software integrates with the latest Windows updates, the operating system must be updated, with all current Windows updates applied.

Required hardware 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.

(2) GPU SUPPORT

Video Insight software supports NVIDIA graphics cards. Additionally, Intel QSV is supported for displaying video within VI MonitorPlus.

The following GPUs are currently supported:

Intel GPUs	Nvidia Graphics Cards
• Intel QSV • Intel HD Graphics, 3rd or later generation • Intel Core processor-based platforms	• EVGA GeForce GTX 750Ti SC 2GB • EVGA GeForce GTX 950 2GB • EVGA GeForce GTX 1050 2GB • EVGA GeForce GTX 1050Ti 2GB • EVGA GeForce GTX 1060 3GB • EVGA GeForce GTX-1080 8GB
For On-board H.265 support, Intel HD Graphics 4th generation processor or higher is recommended.	For hardware decoding with an additional graphics processor, the Nvidia EVGA GeForce GTX 950 2GB card is the minimum recommendation.

NOTE - Only one GPU is used for hardware decoding with IP Server. If two properly installed GPUs are detected by the operating system, IP Server will only use one.

Activating Intel QSV

If a graphics card is installed in addition to the On-board Intel graphics card, the primary display will be used as hardware decoding. If Intel QSV is used as the primary GPU, please make sure BIOS setting has been configured properly to use this specific GPU.

If the additional graphics card is set as the primary display, change the On-board Intel graphics card to primary by connecting it to the monitor. Check the Intel Download center for the correct On-board Intel graphics card driver.

After the above is configured, VI MonitorPlus will detect the On-board Intel graphics card, verifying that the card supports automatic hardware acceleration and use when available.

If both Intel GPU and Nvidia GPUs are available, VI MonitorPlus will use the fastest GPU as default.

(3) ACTIVE DIRECTORY PREREQUISITES

- Active Directory server with users and groups configured.
- Active Directory can be configured with IP Servers that use a localized, independent, database for each server or within a shared database environment.
- Administrator user account with administrator-level credentials in both the domain and on the Active Directory server (do not use an individual account).

NOTE - Alternatively, an account created with proper read/write access for Active Directory integration would be appropriate if the local Administrator account is used to install and modify IP Server during the initial setup process. This allows modifying the registry of the IP Server, granting other Active Directory user scopes and security objects the necessary permissions for accessing video storage in both read/write modes..

- The IP Server host is part of the Domain.
- IP Server must be able to communicate with all domain controllers via port 389 or 636. Port 389 cannot be modified. Port 636 is used for SSL encryption.
- IP Server configuration must be done while logged into the domain with a valid domain account.

Video Insight recommends importing users as a group instead of adding users individually. The group must be created in Active Directory prior to import. Customizing Groups to suit the individual needs and policies of the organization installing IP Server is done easily.

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

- Click the **Start** button.
- Enter ***services.msc*** and then press Enter.
- Locate the **IP Video Enterprise** service.
- Right-click and select **Stop**.
- Right-click and select **Properties**.
- Select the **Logon** tab.
- Select the second option for the account.

- Provide an Active Directory account with minimal rights. A basic domain user account should be sufficient.
- Click the **General** tab and then select **Start**.
- Click **OK**.

NOTE - Restart the IIS Admin service if using Web Client.

(4) FAILOVER SERVER OPTION

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 SQL Database as part of a cluster, the Failover Server feature minimizes video loss and enables continuous live streaming video.

To use the Failover Server feature, the following criteria are required:

- Complete setup of two identical servers with the same hardware configuration.
- A shared Database installation; see IP Server's "Installation with an existing SQL Database".
- A license and a serial number or activation key for each server.

(5) 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.

IP Server saves all *video recordings* to its local hard drive, SAS/NAS storage device so video recordings are still accessible in the case of a SQL database failure.

The following table can be used to determine whether a local or shared database is required:

Local Database	Shared Database
Small centralized organization with 1-3 servers	Large regional organization with many servers
Use VI MonitorPlus client and built-in User Manager	Use Active Directory/LDAP
Disaster recovery and backup for each server's database	Disaster recovery and backup for one database
Failover server functionality **is not desired**	Failover server functionality **is desired**
Cameras will not move from one server to another	Cameras will move from one server to another at final configuration
Avoids unnecessary exposure of SQL database to the network	Exposure of SQL database to the network in a secured network environment

(6) FACTORS AFFECTING PERFORMANCE

Any system is the sum of its parts. A mismatched sub-system or component can have a negative effect on the entire 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.

2.1.B Web Hosting Configuration for Web Client

Operating system requirements for hosting the Web Client interface vary according to the versionused on the server. As a reference, the following Microsoft Operating systems are currently supported:

- Windows 2008 Server and Server R2
- Windows 7 Professional
- Windows 8 Professional
- Windows Server 2012 and Server 2012 R2
- Windows Server 2016

Operating System Roles and Features that should be available prior to installation are:

- Microsoft .NET Framework version 4.5+ or later
- Microsoft IIS v 6.0 or later

Necessary Microsoft IIS Components for full functionality of Web Client:

- ASP and ASP. NET
- ISAPI Filters
- ISAPI Extensions
- Default Document
- Directory Browsing
- Static Content
- Windows Communication Foundation Non-HTTP Activation
- HTTP Logging
- Basic Authentication

NOTE - Video Insight highly recommends to update each of the above features ***to their latest stable version*** via the Microsoft Update Services, prior to their installation.

2.1.C Network Configuration

Network Configuration is ***extremely important*** when implementing an IP video solution. IP cameras use considerable bandwidth to deliver video data between the camera and the server. Different cameras will require different amounts of bandwidth based on factors such as resolution and frame rate.

Accessing video from VI MonitorPlus, Web Client, VI Mobile and Video WallPlus increases the amount of required bandwidth.

(1) 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 less than 100 Mb/s.

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

- Camera is using a dynamic IP address instead of static IP address
- Another service or network device is running at the same time with the same IP address, causing a conflict.
- Another service or network device is broadcasting substantial amounts of data
- 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 total number of cameras. The power output of a switch must be greater than the sum of the power requirements of the attached cameras. Refer to the relevant equipment manuals or specification sheets for hardware power requirements.

NOTE - Due to potential dead zones, transmission speed and/or outside interference with Wi-Fi signals, Video Insight *does* ***not*** recommend using Wireless Networking to connect video cameras.

If an organization using IP Server has more than one site location or multiple installations, it shall rely on an Internet Service Provider (ISP) for connectivity between the sites. The performance expectation from the ISP will depend on their network infrastructure, its utilization by their customers, and their cost/quality ratio.

For better results, consider creating a link with a 50Mbps +/- connection between the two site locations, with occasional video browsing. Streaming video remotely to a desktop client requires basic broadband. Streaming to a mobile device requires 4G service or Wi-Fi..

(2) EXAMPLE ROUTER CONFIGURATION

Video Insight recommends using a router if the IP Server is connected to the internet.

Small Office/Home Office (SOHO) routers provide a simple hardware firewall that protects the computer, preventing all inbound traffic from accessing the network and computers except for the traffic specifically allowed through the firewall.

Follow these steps to configure IP Server and the router for remote access:

1. Assign a static IP address to the IP Server.
2. SOHO routers typically use DHCP to assign an IP address to devices connected to them. Choose an address outside of the DHCP range.
3. Configure the SOHO router to forward ports 80 and 4011 to the IP Server.
4. To test the IP Servers configuration by accessing the Web Client externally, open any compatible Internet browser and enter <**http://<external> IP**>/**videoinsight** into the address bar (URL).

For help on assigning a static IP address or forwarding ports, review the router's documentation or consult with a Network Administrator.

For more information on configuring most SOHO routers in the market, visit http://www.portforward.com. Video Insight **does not** endorse or support the information found on this website.

NOTE - Many SOHO routers will not allow a connection to the external IP address when the IP Server is behind a firewall.

2.1.D Camera Configuration

Video Insight supports a vast array of cameras from many manufacturers. Additional camera support is included with each software release. Please refer to our website for the latest list of supported cameras.

Video Insight supports the Open Network Video Interface Forum (ONVIF) standard, Version 1.02 and Profile S.

(1) CAMERA AUDIO

IP Server is capable of recording audio along with the capturing of video recording when used with the appropriate and desired peripherals. While configuring audio recording is a possibility, it is often over-looked that necessary and desired changes be made on the camera itself for audio recording to function within IP Server's video recording process.

(2) BODY WORN CAMERAS (BWC) AUDIO

For **Body Worn Cameras**, synchronized audio and video are currently available only for 64-bit Windows OS environments. For 32-bits environments, however, recorded video ***does not*** have audio capabilities.

(3) COMPATIBLE AUDIO CODECS

The following codecs are found to work well with IP Server and are most commonly used by known camera manufacturers:

L8 @ 8K (Uncompressed 8-bit audio)	L16 @ 16K (Uncompressed 16-bit audio)
G711 ULAW and ALAW @ 8K and 16K	G726 40/32/24/16
AAC Low Complexity (*) Bitrate is 128kbps or less	AMR Audio

(4) FACTORS AFFECTING CAMERA IMAGING WITHIN VI MONITORPLUS

- Bit Rate - a higher bit rate usually provides better picture quality.
- Resolution - a higher resolution usually provides better picture quality.
- Format - some picture formats, such as **AVI**, incorporate better algorithms that more accurately represent the video capture. The most basic, but bandwidth heavy **MJPEG**, was industry-standard for many years. Since then, other video codecs have been used, including **H.264** and **H.265**.
- 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.

2.1.E 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.

Video Insight provides flexibility in terms of camera storage options:

Record Always	Requires significantly more storage space because video is constantly recorded.
Motion Only	Requires less storage space than **Record Always** because video is recorded only when motion occurs in the camera's field of view.
Schedule	Allows both **Record Always** and **Motion Only** within specified schedules.

The amount of storage needed is determined by the bit-rate of each camera and how much of that will need to be saved. For example, a 1.3 Megapixel camera set at 10 FPS, can be configured to stream video at 1.5 Mbits/sec and, if the camera is recording motion at 50% of the time, then we can estimate we need 7GB of storage per day.

Access the VI Storage Calculator at http://www.security.us.panasonic.com/storage-and-bandwidth-calculator

Video Insight supports all storage that Windows can address. In addition to the size of the storage, it's necessary to confirm the storage system can handle the amount of video otherwise video can be lost when the storage is overloaded.

To calculate the maximum storage throughput, it is assumed that all cameras will write simultaneously and add up all camera bitrates. Because most storage systems refer to maximum simultaneous write speeds in megabytes, divide the total camera traffic by 8 to convert it to MB. For example:

Assume the IP Server has 100 cameras streaming at 3 Mbits/sec or a total of 300 Mbits and it is expected that they are to record 50% of the time.

The storage system must be able to write 37.5 MB/sec at its maximum. Video Insight has developed a storage speed test application to confirm an IP Server's capability. This is available on the www.downloadvi.com website. Click on Tools. Under the Utilities section, the Hard Drive Speed Test will be found.

Supported types of storage:

- NAS
- SAN & RAID 5
- RAID 6
- RAID 10
- JBOD (with custom camera configuration, per camera)

(1) FILE MANIPULATION RULE (RULES MANAGER)

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

(1A) IP SERVER SAMPLE CONFIGURATIONS

The table below is the sample specification for IP Server based on camera number and configuration. Noted CPU Performance is for IP server while recording video without anyone logged into the system or using Client applications (i.e. VI MonitorPlus):

# of H.264 cameras streaming 1.5 Mbps	Server Hardware Configuration	# of Live Camera Views: CPU Utilization
20	Dell Optiplex 7010 with Intel Core i5 3.30 GHz, with 4GB RAM, 3TB of Storage, Intel HD 2500 Graphics, and Windows 7 Professional	4 Live Windows: CPU utilization at 25% 9 Live Windows: CPU utilization at 35% 16 Live Windows: CPU utilization at 45% 20 Live Windows: CPU utilization at 60%
40	Dell Optiplex 7010 with Intel Core i5 3.30 GHz, with 4GB RAM, 3TB of Storage, Intel HD 2500 Graphics, and Windows 7 Professional	4 Live Windows CPU utilization at 25% 9 Live Windows CPU utilization at 35% 16 Live Windows CPU utilization at 45% 20 Live Windows CPU utilization at 60%
120	Dell PowerEdge R520 2U Rackmount with Dual Intel Xeon E5-2403 1.80GHz, with 8GB RAM, 21TB of RAID5 Storage, Intel HD 2500 Graphics, and Windows Server 2008	4 Live Windows: CPU utilization at 25% 9 Live Windows: CPU utilization at 35% 16 Live Windows: CPU utilization at 45% 20 Live Windows: CPU utilization at 60%
240	Dell PowerEdge R720xd 2U Rackmount with Dual Intel Xeon E5-2403 1.80GHz, with 8GB RAM, 42TB of RAID5 Storage, Intel HD 2500 Graphics, and Windows Server 2008	4 Live Windows: CPU utilization at 25% 9 Live Windows: CPU utilization at 35% 16 Live Windows: CPU utilization at 45% 20 Live Windows: CPU utilization at 60%

NOTE - CPU utilization increases 10% when using camera-side Motion Detection.

2.2 LICENSING

Video Insight's licensing structure is simple: one camera requires one channel license, and one server requires one server license. Our floating licenses mean there is no need to tie a licensing seat, IP address or MAC address to a camera.

Cameras offering multiple camera views only require one channel 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.

2.2.A Panasonic Camera License Activation

Video Insight offers a bundle license for Panasonic iPRO camera made in October 2014 or later. To generate a Panasonic camera license for the Video Insight serial number registration process, please follow the instructions found in Tab: Administration: Panasonic Licensing.

2.3 CLIENT SOFTWARE REQUIREMENTS

2.3.A VI MonitorPlus

VI MonitorPlus is a Client application designed to manage the resources of an IP Server environment within a facility or a geographical location. It runs on industry-standard hardware and **works with 32-bit and 64-bit versions of Microsoft Windows 7 or later**.

(1) H.265 ENCODING

H.265 and its use within IP Server is contingent upon hardware and IP Server version numbering. At the time of this introduction, v6.3.7 is the official base for use of H.265 with IP Server.

H.265 is the latest video compression standard which is based on H.264, driven by ever increasing demand for high definition and the rapid development of imaging technology, UHD standards for ultra-high definition include 4K UHD and 8K UHD to meet the trend in today's television and video surveillance market where 4K UHD equals 3840 x 2160 (8.29 megapixels), and UHD equals 7680 x 4320 (33.18 megapixels).

If the criteria for hardware and software has been met, then the use of approved H.265 IP Cameras should function without any *known* limitations now.

	VI MonitorPlus	Web Client	Video WallPlus	VI Monitor for Mac	VI TV	VI Mobile iOS	VI Mobile Android
Live	Yes	No (*1)	Yes	No	No	No	No
Playback	Yes	No	-	No	No	No	No
Video Clip	Yes	No	-	No	-	No	No
Snapshot	Yes	No	-	No	-	-	-
ROI	Yes (*2)	-	-	-	-	-	-

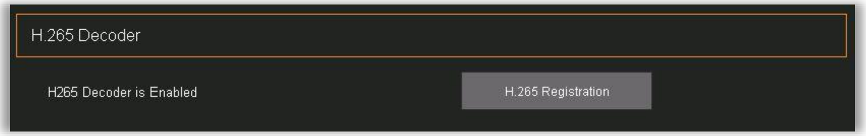
(*1) Live video can be shown in Low mode. (*2) ROI motion search for H.265 is supported by v7.1.1 or later.

✓ **Limitation**: The features that use H.265 decoder in server side, server-side motion detection or LPR etc., are not available for H.265 camera if a server does not support H.265 decoding.

(1A) H.265 DECODER

This section confirms that H.265 registration has been completed.

If the Administrator has not been prompted to register any H.265 cameras placed on the IP Server, selecting H.265 Registration will open a new window.


H.265 Decoder

H265 Decoder is Enabled

2.3.B Web Client

To view the Web Client on the hosted server, the following HTML5-compliant browsers are known to function as needed:

- Microsoft Internet Explorer 11+
- Google Chrome
- Microsoft Edge
- Mozilla Firefox

NOTE - Other HTML5-compliant browsers may work; however, support is currently provided only for the browsers listed above.

2.4 CLIENT HARDWARE REQUIREMENTS

Because video decompression is performed ***on the client*** side, VI MonitorPlus hardware requirements are different from those of IP Server's.

VI MonitorPlus requires additional system memory, video memory and graphic processing capacity where large numbers of cameras are viewed, or while processor-intensive compression protocols are used.

PC Desktops and Laptops

Component	Minimum	Recommended (*H.265 Cameras*)
Processor	Intel Core-based platforms (1 2.4 GHz dual-core); 4th Gen Intel HD Graphics.	6th Generation or later, Intel Core processor (1 3.1 GHz Quad-Core+)
Memory	8GB	8GB+
Video	512 MB	1GB+
Network	100 Mb/s	1GB/s+
Resolution	1600 X 900	1920 X 1080

Small Form Factor computers (Intel NUCs)

Component	Recommended
Processor	Intel Core i5-4250U 1.30GHz
Memory	4GB RAM (Device supports up to 16GB)
Video	HD Intel 5000 Graphics Card
Network	10/100/1000GB NIC

NOTE - Video subsystem must support Microsoft DirectShow 9 or higher.

NOTE - Intel NUCs are **NOT recommended** for IP Server installations.

2.4.A Hardware Decoding

For optimum use of H.265 and H.264 codec capable cameras, the following are the minimum recommended practices:

- 4th generation Intel HD Graphics Intel Core processor-based platforms.
- GPU: Nvidia GTX 750Ti, 950, 1050, 1050Ti and 1060 (750Ti supports only H.264).
- Where a second graphics card is installed alongside the On-board Intel graphics card, it is necessary to configure the system BIOS to force-use the second graphics card as the primary display.
- Separate graphics cards and On-board Intel graphics cards connected to the monitor.
- Verify the correct driver for the On-board Intel graphics card with those found on Intel's website
- IP Server will detect whether the On-board graphics card supports hardware acceleration automatically and use the card when it is available. IP Server only enables it during live and recorded video playback and streaming for 4k or higher resolution.
- For all other instances that use server-side motion detection, thumbnails, snapshots or mobile device connectivity, the use of low speed (JPEG) hardware acceleration is due to asynchronous limitations.

Hardware decoding configuration for H.265 and H.264 is done within VI MonitorPlus. The following items must be selected:

- **Enable hardware decoding** in **Option > Performance** is required. If the CPU does not support the HW codec and the GPU does not exist, it won't display properly within VI MonitorPlus.
- "**Highest Performance**" is for video streaming where the display provides multiple camera views using GPU-heavy codecs such as H.264 and H.265.

3. INSTALLATION AND ADMINISTRATION

The installation process will install the following items:

- IP Server
- VI MonitorPlus
- SQL Server Express
- ASP .NET Framework
- Web Client

The administrator can select and deselect the software components required based on the needs of the system. This includes SQL database location and credentials.

NOTE - IIS, .NET Framework 4.5, and SQL Server Express are all registered trademarks of Microsoft corp. IIS and .NET Framework are installed through the Microsoft Operating system on which they are provided. Not all Microsoft Operating systems offer IIS capabilities, and some older systems are limited in their functional use. It may be necessary to upgrade the operating system completely or install a brand-new operating system entirely if there are any issues during the installation process.

The Video Insight Client Applications connect directly to the IP Server, not to the cameras or the database, requiring the Administrator to forward only three TCP ports for remote access by default. The Client applications can be used to view live and recorded video from a single or multiple IP Servers.

3.1 IP SERVER: INSTALLATION

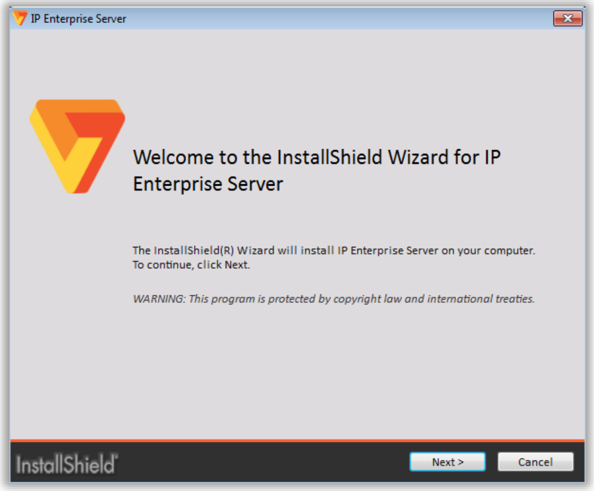
3.1.A Installation without an existing SQL Server Database

Follow the steps below to install IP Server with Microsoft SQL Server for the first time. This option will also install VI MonitorPlus and Web Client as part of VI Enterprise Server.

Download the proper installer (32-bit or 64-bit) from DownloadVI.com.

Launch the executable installer as Administrator, then click **Next.**

Click **Cancel** to exit the process.



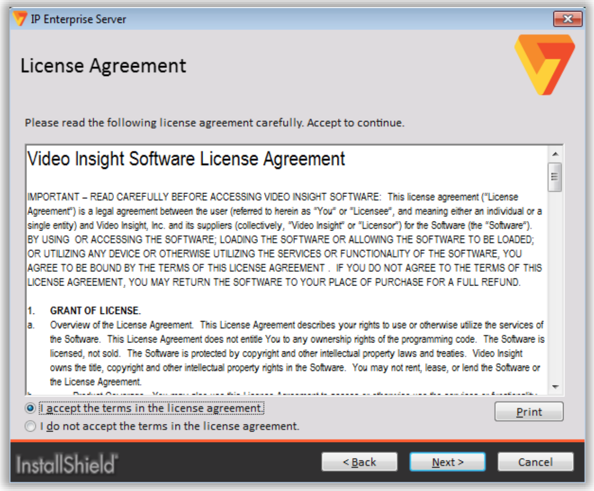
Welcome to the InstallShield Wizard for IP Enterprise Server

The InstallShield(R) Wizard will install IP Enterprise Server on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

Select “**I accept…**” to agree to the terms, then click **Next** to continue.

Click **Back** to return to the previous screen or **Cancel** to exit the process.



License Agreement

Please read the following license agreement carefully. Accept to continue.

Video Insight Software License Agreement

IMPORTANT – READ CAREFULLY BEFORE ACCESSING VIDEO INSIGHT SOFTWARE: This license agreement (“License Agreement”) is a legal agreement between the user (referred to herein as “You” or “Licensee”, and meaning either an individual or a single entity) and Video Insight, Inc. and its suppliers (collectively, “Video Insight” or “Licensor”) for the Software (the “Software”). BY USING OR ACCESSING THE SOFTWARE; LOADING THE SOFTWARE OR ALLOWING THE SOFTWARE TO BE LOADED; OR UTILIZING ANY DEVICE OR OTHERWISE UTILIZING THE SERVICES OR FUNCTIONALITY OF THE SOFTWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE AGREEMENT . IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE AGREEMENT, YOU MAY RETURN THE SOFTWARE TO YOUR PLACE OF PURCHASE FOR A FULL REFUND.

1. GRANT OF LICENSE.

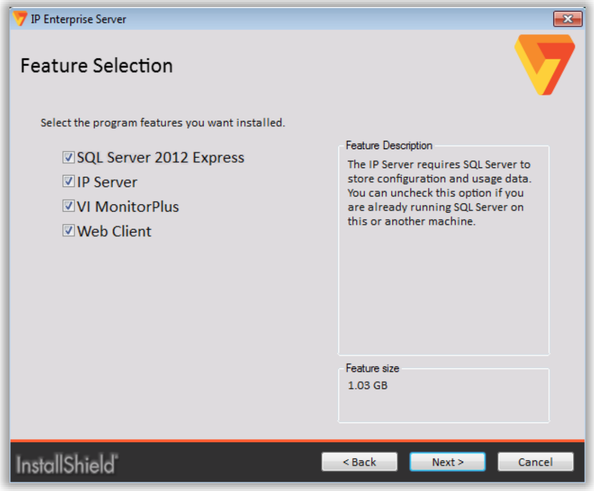
a. Overview of the License Agreement. This License Agreement describes your rights to use or otherwise utilize the services of the Software. This License Agreement does not entitle You to any ownership rights of the programming code. The Software is licensed, not sold. The Software is protected by copyright and other intellectual property laws and treaties. Video Insight owns the title, copyright and other intellectual property rights in the Software. You may not rent, lease, or lend the Software or the License Agreement.

● I accept the terms in the license agreement.

○ I do not accept the terms in the license agreement.

Select **all the components** in the Features Selection list and then click **Next**.

Click **Back** to return to the previous screen or **Cancel** to exit the process.



Feature Selection

Select the program features you want installed.

☑ SQL Server 2012 Express

☑ IP Server

☑ VI MonitorPlus

☑ Web Client

Feature Description

The IP Server requires SQL Server to store configuration and usage data. You can uncheck this option if you are already running SQL Server on this or another machine.

Feature size: 1.03 GB

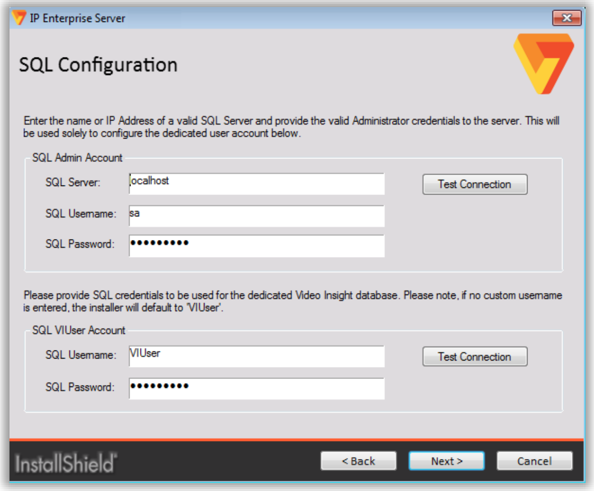
The default credentials are displayed for the SQL installation; these can be changed according to each specific configuration.

Click **Test Connection** to validate the correct SQL configuration.

NOTE - If SQL Server is hosted on another server, the SQL Server field can be modified to match that server’s IP address or DNS hostname.

Click **Next** to continue.

Click **Back** to return to the previous screen or **Cancel** to exit the process.



SQL Configuration

Enter the name or IP Address of a valid SQL Server and provide the valid Administrator credentials to the server. This will be used solely to configure the dedicated user account below.

SQL Admin Account

SQL Server: localhost

SQL Username: sa

SQL Password: •••••••••

Please provide SQL credentials to be used for the dedicated Video Insight database. Please note, if no custom username is entered, the installer will default to 'VIUser'.

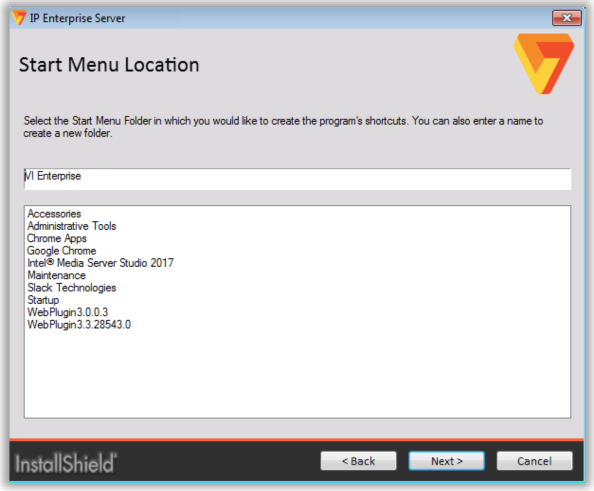
SQL VIUser Account

SQL Username: VIUser

SQL Password: •••••••••

Select the **Start Menu location** to create the program's shortcuts, then click **Next**.

Click **Back** to return to the previous screen or **Cancel** to exit the process.



Start Menu Location

Select the Start Menu Folder in which you would like to create the program's shortcuts. You can also enter a name to create a new folder.

VI Enterprise

Accessories
Administrative Tools
Chrome Apps
Google Chrome
Intel® Media Server Studio 2017
Maintenance
Slack Technologies
Startup
WebPlugin3.0.0.3
WebPlugin3.3.28543.0

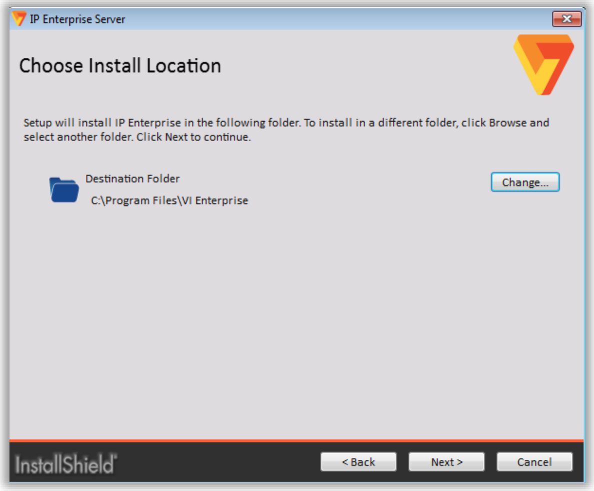
Select the **Install location** where the IP Enterprise software will be installed.

To accept the default destination folder, click **Next**.

To choose another destination, click **Change** and manually locate the desired folder in your hard drive.

Click **Next** to proceed,

Click **Back** to return to the previous screen or **Cancel** to exit the process.



Choose Install Location

Setup will install IP Enterprise in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.

Destination Folder
C:\Program Files\VI Enterprise

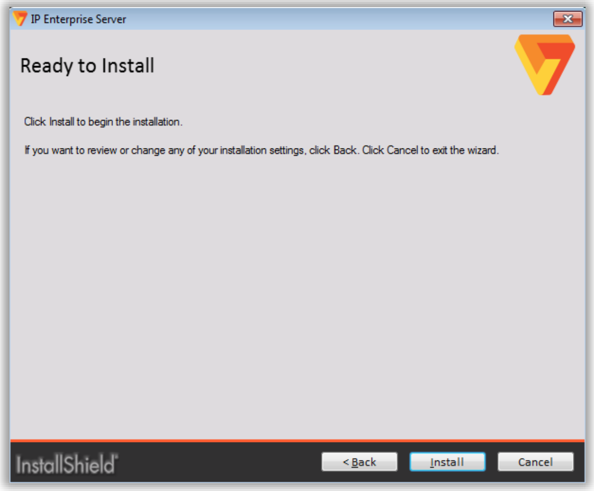
Once all steps have been completed, click **Install** to start the installation process.

During this phase, a series of informational screens will appear to inform that the installation process is underway.

After IP Server has installed itself, the initialization window will appear.

Ensure to have easy access to the Serial number provided by the sales agent for this installation of IP Server.

Click **Back** to return to the previous screen or **Cancel** to exit the process.



Ready to Install

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

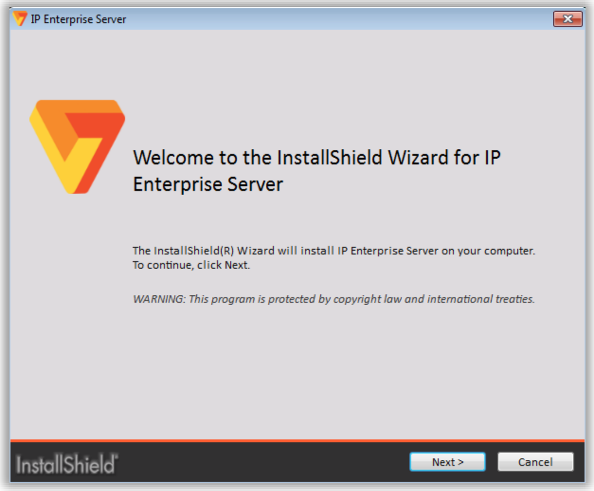
3.1.B Installation with an existing SQL Server Database

Use the following steps to install IP Server for the first time in an environment with a preexisting Microsoft SQL Server instance. This option also installs VI MonitorPlus Client and Web Client.

Download the proper installer (32-bit or 64-bit) from DownloadVI.com.

Launch the executable installer as Administrator, then click **Next.**

Click **Cancel** to exit the process.



IP Enterprise Server

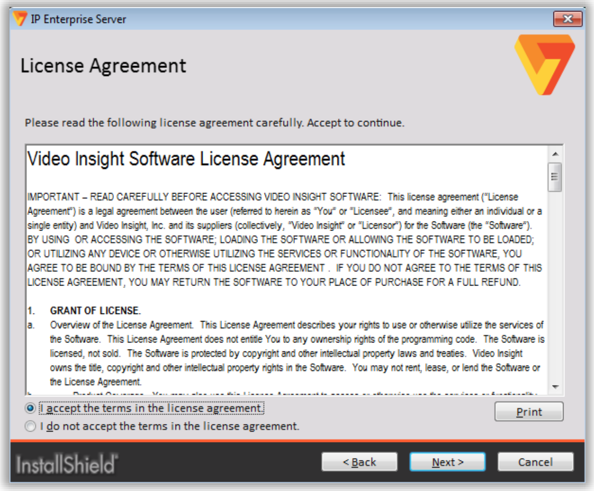
Welcome to the InstallShield Wizard for IP Enterprise Server

The InstallShield(R) Wizard will install IP Enterprise Server on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

Select "**I accept…**" to agree to the terms, then click **Next** to continue.

Click **Back** to return to the previous screen or **Cancel** to exit the process.



IP Enterprise Server

License Agreement

Please read the following license agreement carefully. Accept to continue.

Video Insight Software License Agreement

IMPORTANT – READ CAREFULLY BEFORE ACCESSING VIDEO INSIGHT SOFTWARE: This license agreement ("License Agreement") is a legal agreement between the user (referred to herein as "You" or "Licensee", and meaning either an individual or a single entity) and Video Insight, Inc. and its suppliers (collectively, "Video Insight" or "Licensor") for the Software (the "Software"). BY USING OR ACCESSING THE SOFTWARE; LOADING THE SOFTWARE OR ALLOWING THE SOFTWARE TO BE LOADED; OR UTILIZING ANY DEVICE OR OTHERWISE UTILIZING THE SERVICES OR FUNCTIONALITY OF THE SOFTWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE AGREEMENT . IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE AGREEMENT, YOU MAY RETURN THE SOFTWARE TO YOUR PLACE OF PURCHASE FOR A FULL REFUND.

1. **GRANT OF LICENSE.**

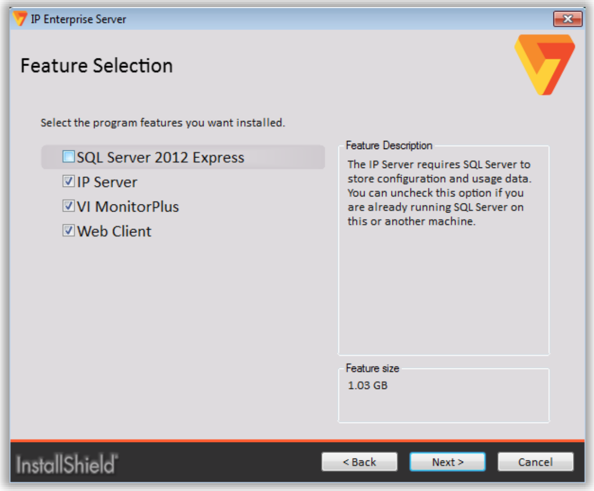
a. Overview of the License Agreement. This License Agreement describes your rights to use or otherwise utilize the services of the Software. This License Agreement does not entitle You to any ownership rights of the programming code. The Software is licensed, not sold. The Software is protected by copyright and other intellectual property laws and treaties. Video Insight owns the title, copyright and other intellectual property rights in the Software. You may not rent, lease, or lend the Software or the License Agreement.

● I accept the terms in the license agreement.

○ I do not accept the terms in the license agreement.

Select all the components in the Feature Selection list **except SQL Server 2012 Express** and then click **Next**.

Click **Back** to return to the previous screen or **Cancel** to exit the process.



IP Enterprise Server

Feature Selection

Select the program features you want installed.

□ SQL Server 2012 Express

☑ IP Server

☑ VI MonitorPlus

☑ Web Client

Feature Description

The IP Server requires SQL Server to store configuration and usage data. You can uncheck this option if you are already running SQL Server on this or another machine.

Feature size

1.03 GB

NOTE - If **TLS protocol** is enabled in your platform, please contact our **Support Team** for assistance during this phase.

See *Contact Us* for more details.

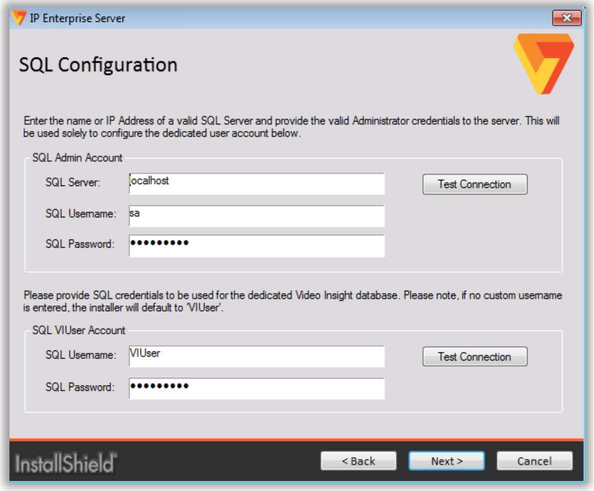
The default credentials are displayed for the SQL installation; these can be changed according to each specific configuration.

Click **Test Connection** to validate the correct SQL configuration.

> **NOTE -** If SQL Server is **hosted on another server**, the **SQL Server field** value shall match it's IP address or DNS hostname.

Click **Next** to continue.

Click **Back** to return to the previous screen or **Cancel** to exit the process.



IP Enterprise Server

SQL Configuration

Enter the name or IP Address of a valid SQL Server and provide the valid Administrator credentials to the server. This will be used solely to configure the dedicated user account below.

SQL Admin Account

SQL Server: localhost

SQL Username: sa

SQL Password: •••••••••

Please provide SQL credentials to be used for the dedicated Video Insight database. Please note, if no custom username is entered, the installer will default to 'VIUser'.

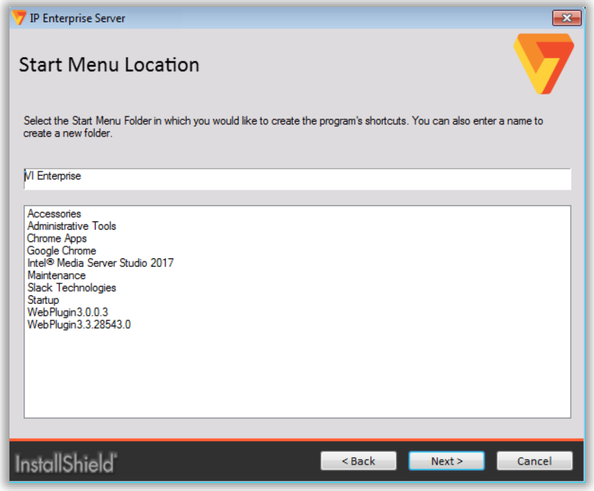
SQL VIUser Account

SQL Username: VIUser

SQL Password: •••••••••

Select the **Start Menu location** to create the program's shortcuts, then click **Next**.

Click **Back** to return to the previous screen or **Cancel** to exit the process.



IP Enterprise Server

Start Menu Location

Select the Start Menu Folder in which you would like to create the program's shortcuts. You can also enter a name to create a new folder.

VI Enterprise

Accessories
Administrative Tools
Chrome Apps
Google Chrome
Intel® Media Server Studio 2017
Maintenance
Slack Technologies
Startup
WebPlugin3.0.0.3
WebPlugin3.3.28543.0

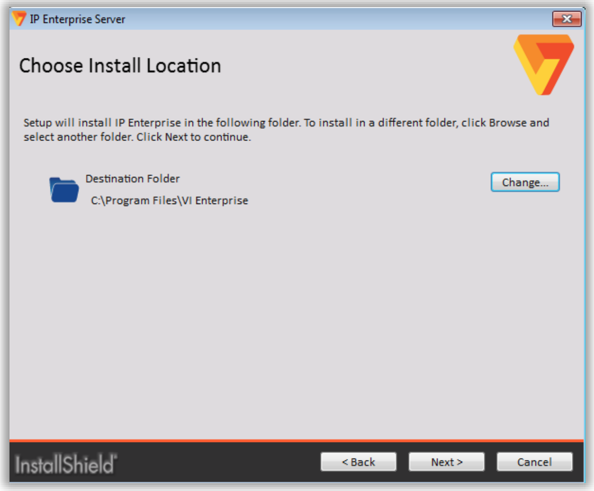
Select the **Install location** where the IP Enterprise software will be installed.

To accept the default destination folder, click **Next**.

To choose another destination, click **Change** and manually locate the desired folder in your hard drive.

Click **Next** to proceed,

Click **Back** to return to the previous screen or **Cancel** to exit the process.



IP Enterprise Server

Choose Install Location

Setup will install IP Enterprise in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.

Destination Folder
C:\Program Files\VI Enterprise

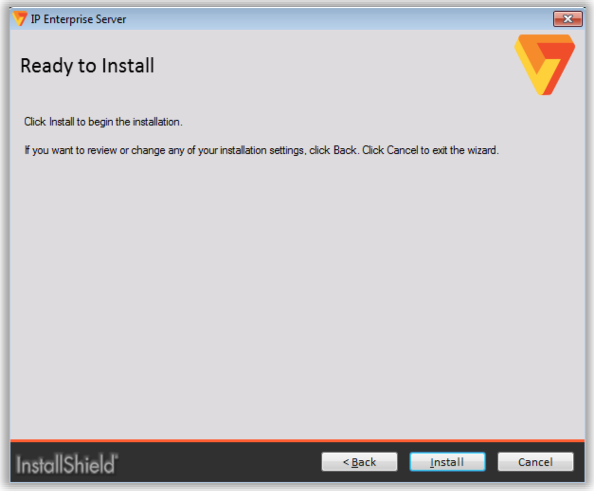
Once all steps have been completed, click **Install** to start the installation process.

During this phase, a series of informational screens will appear to inform that the installation process is underway.

After IP Server has installed itself, the initialization window will appear.

Ensure to have easy access to the Serial number provided by the sales agent for this installation of IP Server.

Click **Back** to return to the previous screen or **Cancel** to exit the process.



Ready to Install

Click Install to begin the installation.

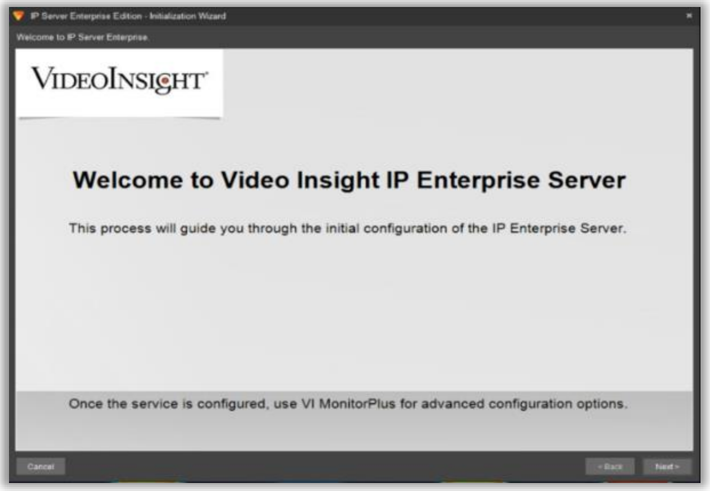
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

3.1.C Initialization

IP Server ***needs to be activated*** to function properly. For this, there are ***three options*** available:

Activate or Upgrade license online	This can be completed on a server with an active internet connection and permission to connect to port 30000. If online activation fails, try the next option: Activate by phone.
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. **NOTE -** Available in the ***United States only***. Please contact the sales agent or vendor where you purchased IP Server Enterprise.
Demo Mode	Grants the user the ability to use a full-featured version for up to 60 days, with a maximum of 99 cameras. Once the 60-day period has expired, the software will no longer record or display live images. IP Server will fail to start until a valid serial number is provided, or activation code is used. Re-installation is not required.

To **initialize IP Server**, follow the steps below:

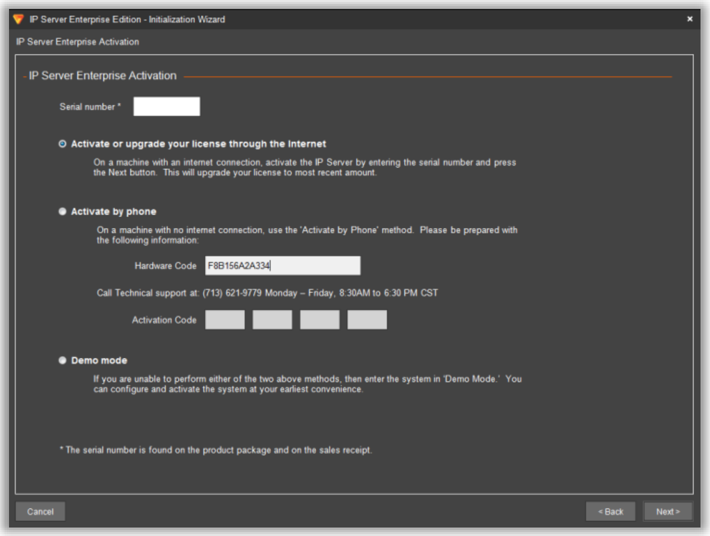

IP Server Enterprise Edition - Initialization Wizard
Welcome to IP Server Enterprise
VIDEOINSIGHT

Welcome to Video Insight IP Enterprise Server

This process will guide you through the initial configuration of the IP Enterprise Server.

Once the service is configured, use VI MonitorPlus for advanced configuration options.

Run the Installation program and click **Next.**



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. Please be prepared with the following information:

Hardware Code: F8B156A2A334

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 and activate the system at your earliest convenience.

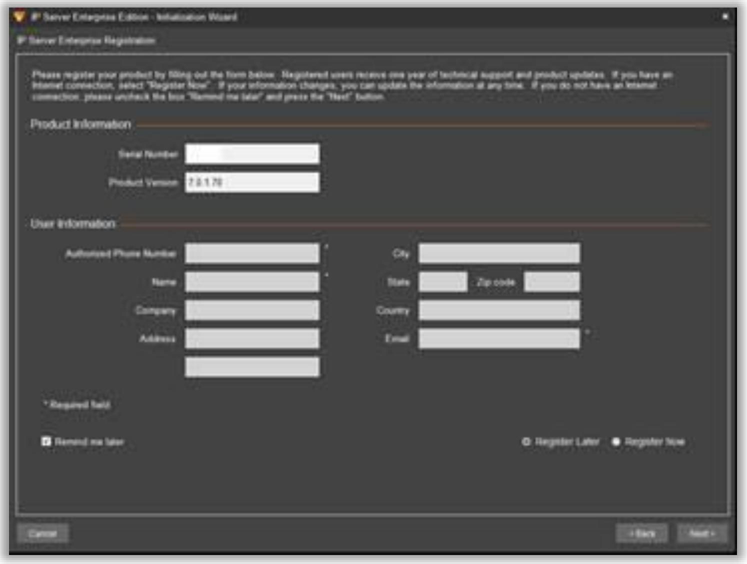
* The serial number is found on the product package and on the sales receipt.

Where prompted, enter the five-character, alpha-numeric serial number provided at the time of purchase.

Click **Next**.

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

Select ***Activate by Phone*** and call +1-713-621-9779 (USA only) if there is a problem activating the software with the provided serial number, or select Demo mode, to start recording immediately. (Toll charges may apply.)



IP Server Enterprise Edition - Initialization Wizard

IP Server Enterprise Registration

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.

Product Information

Serial Number

Product Version: 7.0.1.70

User Information

Authorized Phone Number *

Name *

Company

Address

City

State

Zip code

Country

Email *

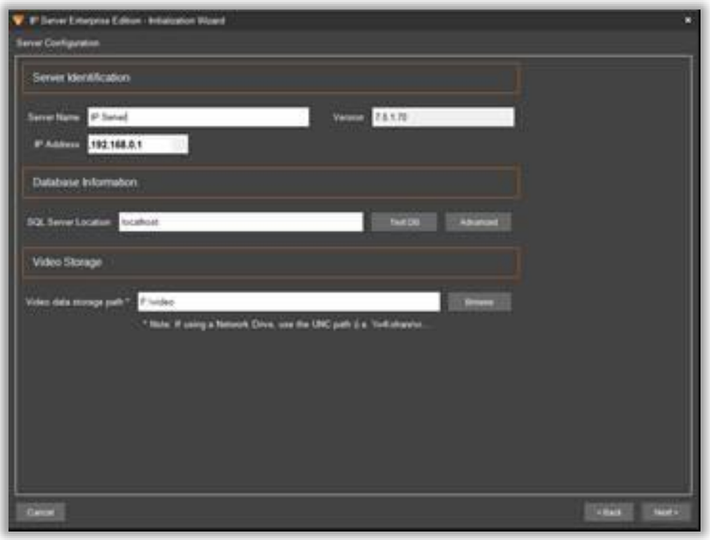
* Required field

☑ Remind me later

○ Register Later ● Register Now

Enter any relevant user information.

The Administrator has the option of registering the product now or waiting until a later date. Select the best option.



IP Server Enterprise Edition - Initialization Wizard

Server Configuration

Server Identification

Server Name: IP Server

Version: 7.0.1.70

IP Address: 192.168.0.1

Database Information

SQL Server Location: localhost

Video Storage

Video data storage path *: F:\video

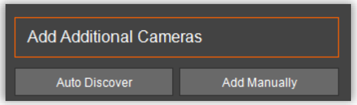
* Note: If using a Network Drive, use the UNC path (i.e. [illegible]

Verify the configuration for IP Server. If there is a need to modify the configuration, select make changes, and click **Next**.

Otherwise, click **Next** to accept the default values.

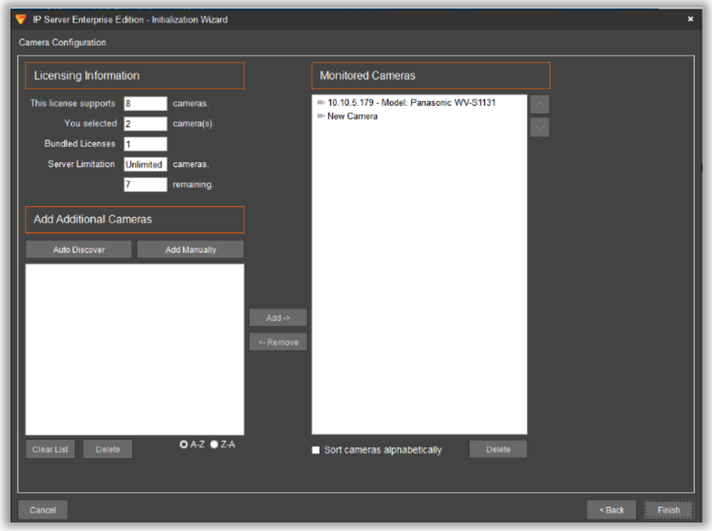
Server Name	The default is “IP Server -“ and the detected IP address of this server. You can change this to a more friendly or meaningful name. Do not use special characters.
IP Address	This is the selected server’s IP address and should not be changed.
Version	The current version of the software.
SQL Server Location	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 hosted 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.
Video Data Storage Path	The location where all the recorded video is saved. The default is the local OS drive (i.e., C). The video folder is created automatically after the server configuration is completed. It is possible to save video to other locations, for example: • Alternate local drive: *For example, D:\video* • Shared drive: For example, \\vShareHost\vshare\HHSvideo

NOTE - . Recording to a shared location requires a User account with write permission to the shared drive, otherwise recordings will not be saved.



Add cameras using Auto Discover if needed.

See Adding Cameras for more information on adding cameras.


IP Server Enterprise Edition - Initialization Wizard

Camera Configuration

Licensing Information

This license supports 8 cameras.

You selected 2 camera(s).

Bundled Licenses 1

Server Limitation Unlimited cameras.

7 remaining.

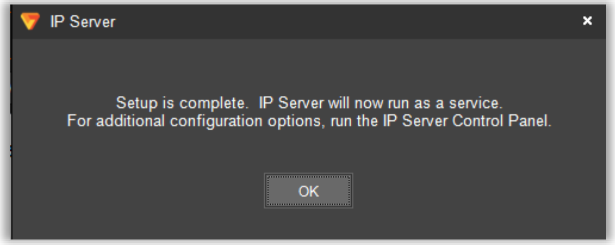
Monitored Cameras

10.10.5.179 - Model: Panasonic WV-S1131

New Camera

Cameras, when initially added through this method, will be at their default values.

Further customization of camera settings is necessary. .


IP Server

Setup is complete. IP Server will now run as a service.
For additional configuration options, run the IP Server Control Panel.

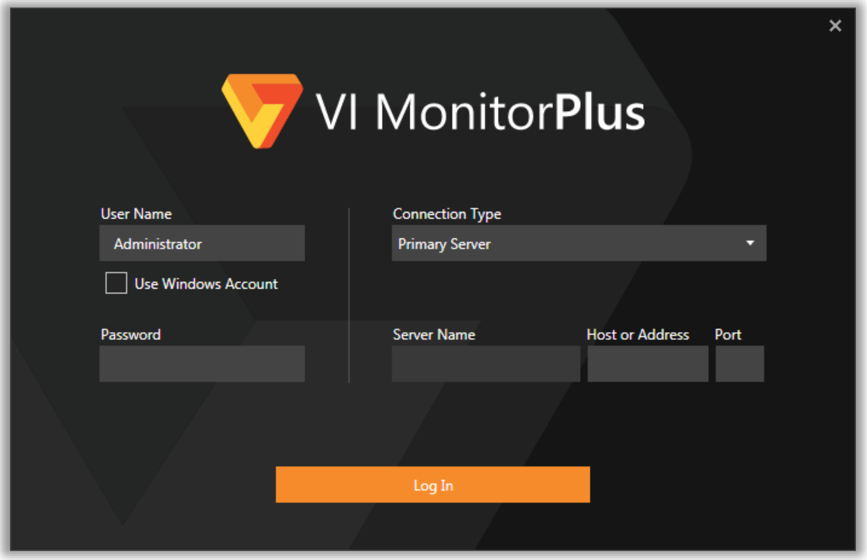
Click **OK**.

IP Server will now run as a service on the operating system. A user desktop can be logged out of, without hampering the video recording capabilities.

3.2 VI MONITORPLUS CLIENT

3.2.A Logging In

Open **VI MonitorPlus** by double-clicking the corresponding **desktop icon** for the application. The **Login window** will be displayed (*see below*).



User Name: Administrator

□ Use Windows Account

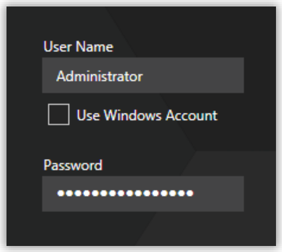
Connection Type: Primary Server

Field	Description
User Name	User Identification for IP Server account.
Use WindowFields Account	Enable/Disable use of Windows account to log in.
Password	Password for IP Server account.
Connection Type	Drop-down list with three options: • Primary Server: access the Main Server on a single connection. • Multiple Servers: simultaneously access a List of Servers after a single login. • Use Configuration File: load login parameters from an external file. NOTE - VI MonitorPlus' Login Interface automatically changes its layout according to the selected Connection Type; the above image shows the interface for **Primary Server**. *See below for more information on all three Connection Types and their respective fields and options.*
Server Name	Name of the Server.
Host or Address	IP Address of the Server.
Port	Port of the Server.

(1) USER NAME, PASSWORD AND USE WINDOWS ACCOUNT

The left side of the Login Interface shows the basic fields for accessing the server(s).

By default, the User Name and Password for the main **IP Server** account is used.

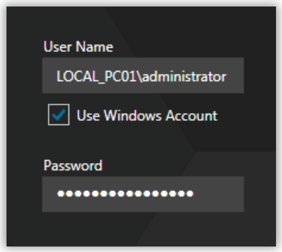


User Name: Administrator

□ Use Windows Account

Password: ••••••••••••••••

When checking the **Use Windows Account** box, the user will be asked to enter the corresponding Windows-based credentials, overriding IP Server’s account.



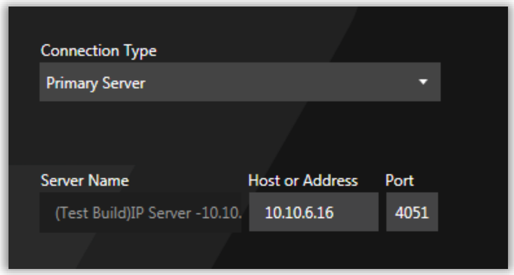
User Name: LOCAL_PC01\administrator

☑ Use Windows Account

Password: ••••••••••••••••

(2) CONNECTION TYPE: PRIMARY SERVER

When **Primary Server** connection is selected, VI MonitorPlus will only display the primary server name on the **Server Name** box, with the ability of modifying both the **Host or Address** and the **Port** fields values.



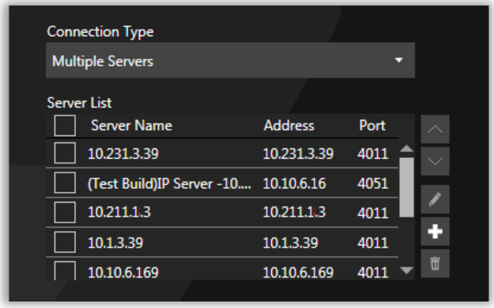
Connection Type: Primary Server

Server Name	Host or Address	Port
(Test Build)IP Server -10.10.	10.10.6.16	4051

(3) CONNECTION TYPE: MULTIPLE SERVERS

The **Multiple Servers** option allows to connect to more than one IP Server instance using ***only one login account***.

The interface shows a list of available servers, with the possibility to select or deselect them individually as needed.



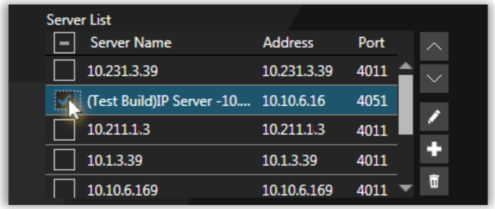
Connection Type: Multiple Servers

Server List

□	Server Name	Address	Port
□	10.231.3.39	10.231.3.39	4011
□	(Test Build)IP Server -10....	10.10.6.16	4051
□	10.211.1.3	10.211.1.3	4011
□	10.1.3.39	10.1.3.39	4011
□	10.10.6.169	10.10.6.169	4011

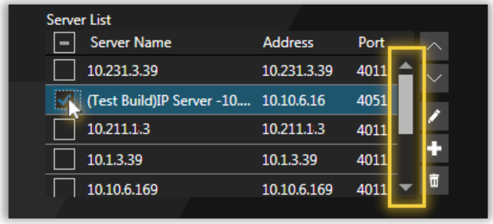
(3A) SELECTING SERVERS FROM THE LIST

Select/Deselect servers ***individually*** by clicking on the corresponding check boxes.


Server List

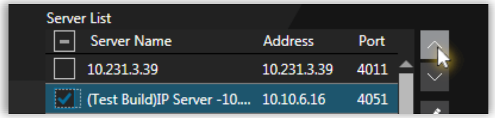
☐	Server Name	Address	Port
☐	10.231.3.39	10.231.3.39	4011
☑	(Test Build)IP Server -10....	10.10.6.16	4051
☐	10.211.1.3	10.211.1.3	4011
☐	10.1.3.39	10.1.3.39	4011
☐	10.10.6.169	10.10.6.169	4011

When the Server List is highly populated, the **Scroll Bar** on the right can be used to find specific servers within the list.


Server List

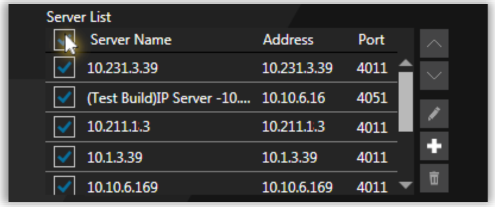
☐	Server Name	Address	Port
☐	10.231.3.39	10.231.3.39	4011
☑	(Test Build)IP Server -10....	10.10.6.16	4051
☐	10.211.1.3	10.211.1.3	4011
☐	10.1.3.39	10.1.3.39	4011
☐	10.10.6.169	10.10.6.169	4011

Use the **Arrow buttons** on the right to reposition the selected server across the list (*Up/Down*).


Server List

☐	Server Name	Address	Port
☐	10.231.3.39	10.231.3.39	4011
☑	(Test Build)IP Server -10....	10.10.6.16	4051

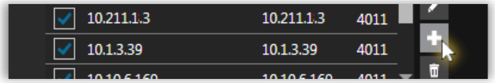
Select/Deselect *all* servers by clicking on the top check box, besides the **Server Name** title.


Server List

☑	Server Name	Address	Port
☑	10.231.3.39	10.231.3.39	4011
☑	(Test Build)IP Server -10....	10.10.6.16	4051
☑	10.211.1.3	10.211.1.3	4011
☑	10.1.3.39	10.1.3.39	4011
☑	10.10.6.169	10.10.6.169	4011

(3B) ADDING A NEW SERVER TO THE SERVERS LIST

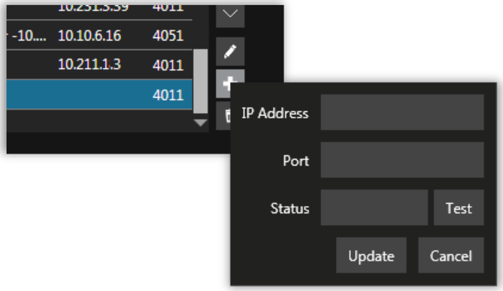
Click on the **plus icon [+]** (*see right*).



☑	10.211.1.3	10.211.1.3	4011
☑	10.1.3.39	10.1.3.39	4011

A **new blank row** (in blue) will be displayed on the Servers List, and a **pop-up window** with the data entry for the new server will open next to the [+] button. Here, enter **the IP Address or Name** and the **Port Number** of the IP Server to connect to.

Click **Update** to add the new server or **Cancel** to exit the operation.



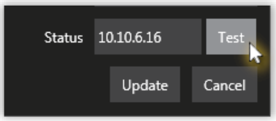
-10....	10.10.6.16	4051
	10.211.1.3	4011
		4011

IP Address

Port

Status

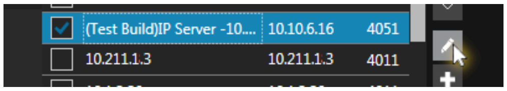
Optionally, click **Test** to confirm the connectivity. If successful, the Status field will display the new server's name.


Status 10.10.6.16

NOTE - If the server cannot be found, an error message will be displayed on the corresponding row.

(3C) MODIFYING A SERVER

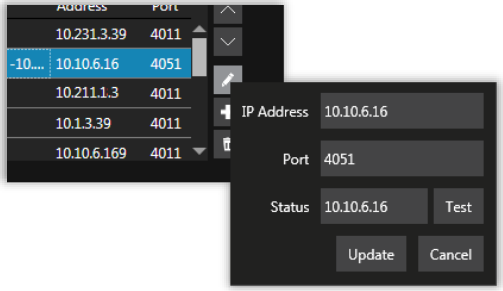
On the Server List, select the row for the server to be modified and click on the **pencil icon** (*see right*) to open the pop-up form containing its data.



☑	(Test Build)IP Server -10....	10.10.6.16	4051
□	10.211.1.3	10.211.1.3	4011

Edit the information where needed and click **Update** to save the changes or **Cancel** to close the window and exit.

Optionally, click **Test** to validate the connection with the server before updating.



	Address	Port
	10.231.3.39	4011
-10...	10.10.6.16	4051
	10.211.1.3	4011
	10.1.3.39	4011
	10.10.6.169	4011

IP Address: 10.10.6.16

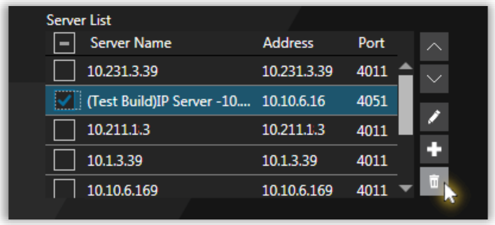
Port: 4051

Status: 10.10.6.16

(3D) DELETING A SERVER

Select the row for the server to be deleted and click on the **[X]** icon on the right to delete it.

NOTE - This operation cannot be undone.



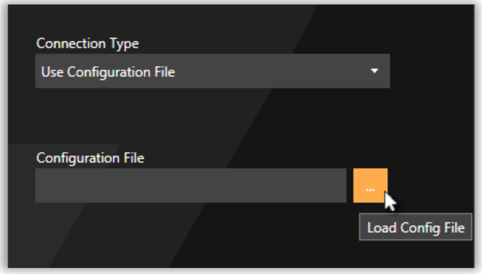
Server List

☐	Server Name	Address	Port
□	10.231.3.39	10.231.3.39	4011
☑	(Test Build)IP Server -10....	10.10.6.16	4051
□	10.211.1.3	10.211.1.3	4011
□	10.1.3.39	10.1.3.39	4011
□	10.10.6.169	10.10.6.169	4011

(4) CONNECTION TYPE: USE CONFIGURATION FILE

The **Use Configuration File** option allows to retrieve and use an external file (***.lsl* format**) containing a specific set of connections to one or many IP Server instances.

After selecting the option from the **Connection Type** drop-down list, click on the **yellow icon […]** next to the **Configuration File** field to open a Windows Explorer session; search for the corresponding file and open it.

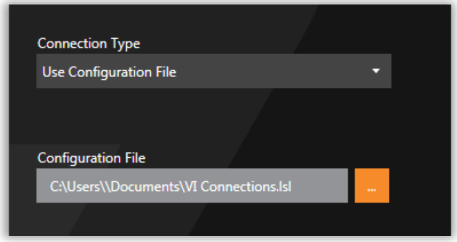


Connection Type: Use Configuration File

Configuration File:

Once the filename has been retrieved, click **Login** to to start using VI MonitorPlus.

NOTE - The *.lsl* file is generated by VI MonitorPlus, using the **Export Profile** option from the **System** > **Options** > **Connections** > **Specify Each Server** interface.



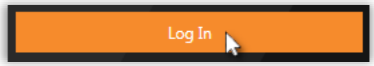
Connection Type: Use Configuration File

Configuration File: C:\Users\\Documents\VI Connections.lsl

NOTE - For more information on creating an Exported Server List, see Use Server Profiles.

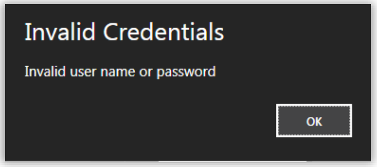
(5) LOG IN

Once the **User Name** and **Password** have been entered, and the **Connection Type** defined, click **Log In** to access VI MonitorPlus.



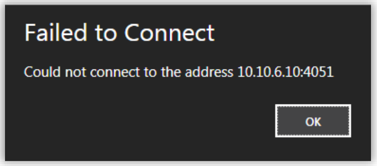
(5A) ERROR MESSAGES

If the User Name and/or Password are incorrect, the application will display an Error Message.


Invalid Credentials

Invalid user name or password

Likewise, if the application is not able to establish a connection with one or more servers, a message will inform the failed attempt indicating the server's IP address and Port number.


Failed to Connect

Could not connect to the address 10.10.6.10:4051

3.2.B Adding IP Servers to VI MonitorPlus

In a large organization, it is possible to utilize more than 20 video surveillance servers across multiple locations.

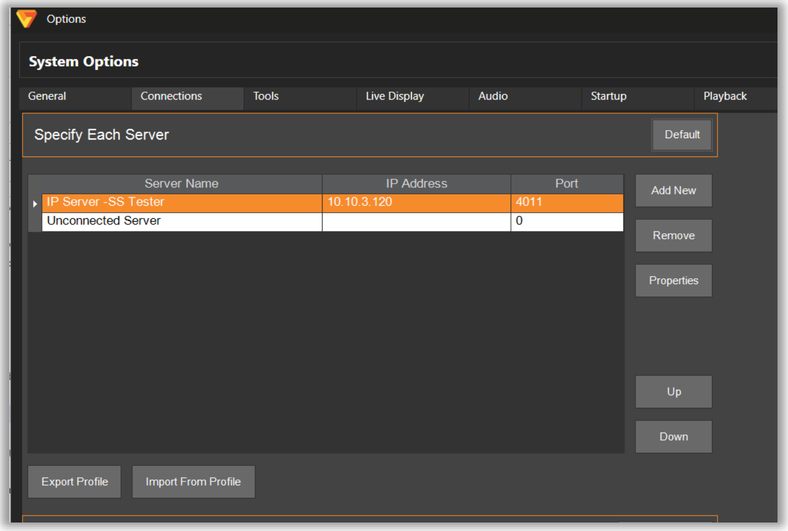
It is also possible to add a lengthy list of servers at one time using the **Import** feature. For this, an exported list of servers is needed prior to importation. The file format used by IP Server is a proprietary "*.lsl*" file.

NOTE - For more information on creating an Exported Server List, see Use Server Profiles:

Select **System** --> **Options** and then click **Connections**.

Select **Import From Profile**.

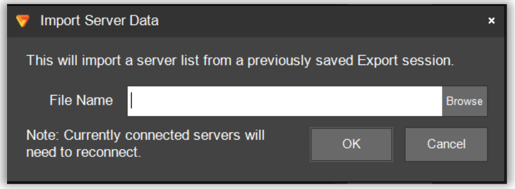
Enter the filename or click **Browse** to go to the location of the saved "*.lsl*" file.



Server Name	IP Address	Port
IP Server -SS Tester	10.10.3.120	4011
Unconnected Server		0

Select the *.lsl* file to use with VI MonitorPlus.

Click **OK**.

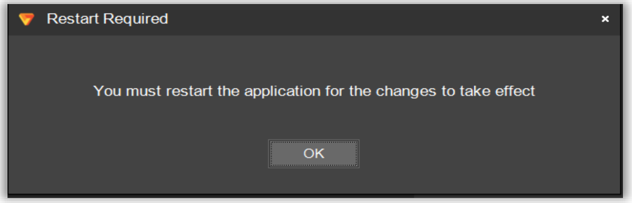


This will import a server list from a previously saved Export session.

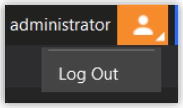
File Name

Note: Currently connected servers will need to reconnect.

NOTE - If the file is unreadable or not found *an error will appear.* If the import is successful, the full list of servers will display in the **Known Video Servers** grid.



You must restart the application for the changes to take effect



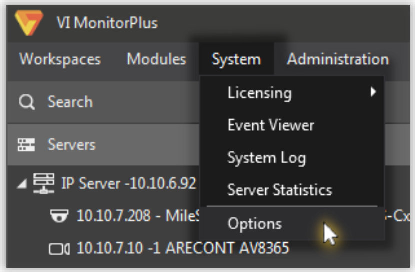
A popup window indicates that VI MonitorPlus needs to be restarted for changes to take effect.

This process is accomplished by clicking the **Logout** icon on the upper left corner of the main dashboard

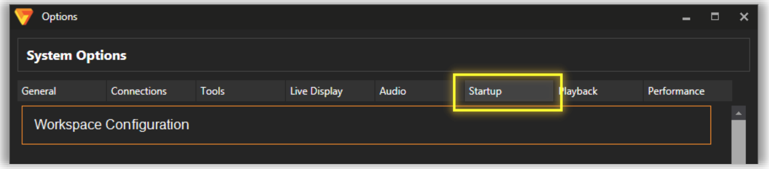
3.2.C Auto Login

The Auto Login option disables the log in window and opens VI MonitorPlus directly using the pre-configured User Account.

To activate it, open the "**System**" option from the Main Menu, then select "**Options**".

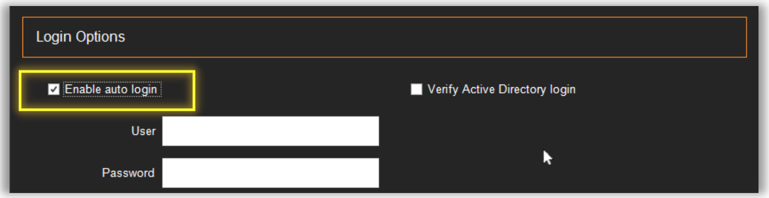


In the **System Options** window, click on the "**Startup**" tab, then go to the "**Login Options**" section.



Check the "**Enable Auto Login"** box and enter the User and Password in the corresponding fields.

You can also check the "**Verify Active Directory login**" box if the User account is associated to a Windows Server profile in your network.



NOTE - Do not Log Off; instead, close all windows and shut VI MonitorPlus down; reopen VI MonitorPlus and the application will go directly to the main view overriding the Log In window.

3.3 ADMINISTRATION

3.3.A IP Server Manager (IPSM)

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. It provides access to many necessary administrative functions of IP Server:

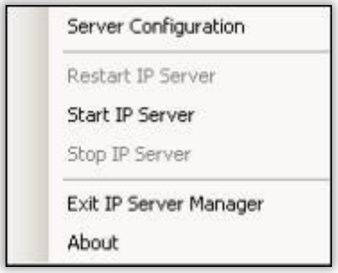
- Monitors the IP Server and presents visual status cues for each server.
- Provides a Diagnostic version of the IP Server Manager for troubleshooting and system optimization.
- Manages IP Server network connections.
- Manages licensing and registration.
- Manages Lightweight Directory Access Protocol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

(1) ACCESSING IPSM

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

🟩	**ON**: IP Server is functioning properly, streaming video to clients, recording video and reporting to Health Monitor Cloud (if configured). Hover the mouse cursor over the icon in the taskbar to view the server's IP Address.
🟥	**OFF**: IP Server is not functioning. No video recording or streaming available.

Right-click on the IPSM icon to open the IP Server options menu:



To manage the IP Server service, configure and utilize the IPSM, select **Server Configuration**.

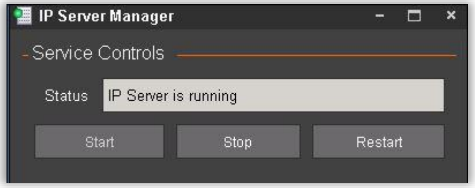
Select **Start IP Server, Stop IP Server** or **Restart IP Server** to start, stop or restart the IP Server service.

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.

(2) CONFIGURING IP SERVER

Right-click on the IPSM icon in the Windows System Tray and select **Server Configuration** to open the **IP Server Manager**.



Status: IP Server is running

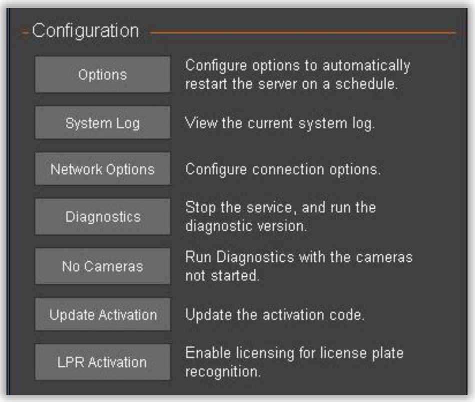
The Service Controls **Status** field displays the IP Server service status.

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

Clicking on **Close** removes the IP Server Manager dialog box; it does not stop the IP Server service from recording video if functioning cameras are connected to the IP Server.

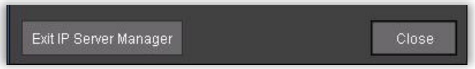
Click a **Configuration** button to perform other functions:

- **Options** - Configure options specific to IP Server.
- **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 IP Server activation for use with the serial license.


Configuration

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 service, and run the diagnostic version.
No Cameras	Run Diagnostics with the cameras not started.
Update Activation	Update the activation code.
LPR Activation	Enable licensing for license plate recognition.

To exit the IPSM application, click **Exit IP Server Manager.** This closes the IP Server Manager in the Windows System tray only, but the IP Server service continues to run in the background, so video capture continues.



NOTE - Stopping the IP Server service prevents clients from remotely restarting the IP Server service.

(2A) IPSM: OPTIONS

Clicking on **Options** will display 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.

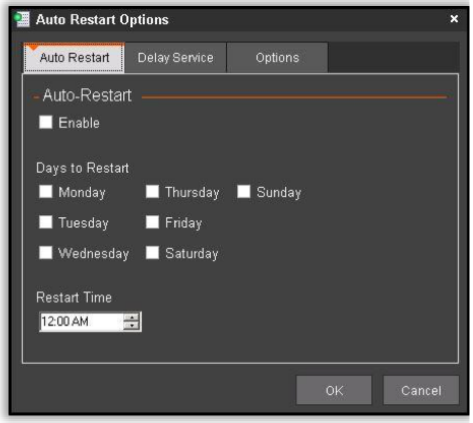
Auto Restart

Restarting the service can refresh camera connections and video streaming and alter CPU performance by releasing used resources, providing the ability to automatically restart the service for a specific day and time.

This flexibility allows the Administrator to schedule IP Server service without impacting business hours recording.

To set an Auto-Restart schedule, follow the steps below:

- Check the **Enable** box.
- Select the Restart Day or days.
- Select a Restart Time.
- Click **OK**.


Auto Restart Options

Auto-Restart

□ Enable

Days to Restart

□ Monday □ Thursday □ Sunday
□ Tuesday □ Friday
□ Wednesday □ Saturday

Restart Time

12:00 AM

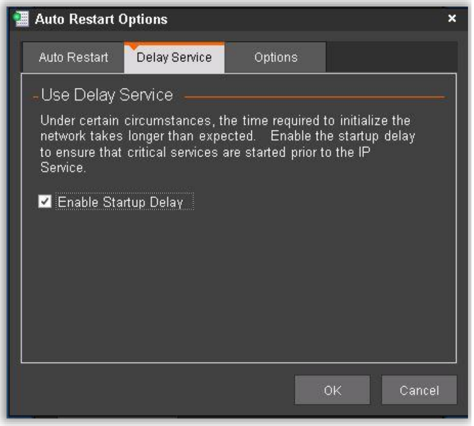
Delay Service

Delaying the IP Server service start is a viable option if the server has many additional services running.

The IP Server service may have trouble initializing without services such as the Microsoft SQL database service already running.

IIS loads the localhost IP Address (http://127.0.0.1) if it is not able to resolve the hostname of the IP Server.

To set a startup delay, check the **Enable Startup Delay** box and click **OK**.


Auto Restart Options

Use Delay Service

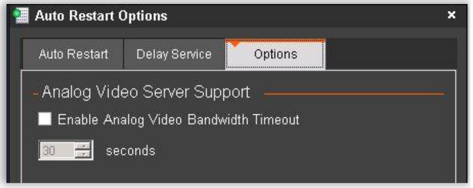
Under certain circumstances, the time required to initialize the network takes longer than expected. Enable the startup delay to ensure that critical services are started prior to the IP Service.

☑ Enable Startup Delay

Options

For environments where both an Analog and an IP Server are installed **on the same server**, with resulting high bandwidth usage, there is an option to restrict the Analog server's resources consumption.

Enabling this feature will stop the communication between Analog and IP servers. As a result, no live streaming or recording will be performed by the IP server when the timeout threshold is reached.



Auto Restart Options

Analog Video Server Support

□ Enable Analog Video Bandwidth Timeout

30 seconds

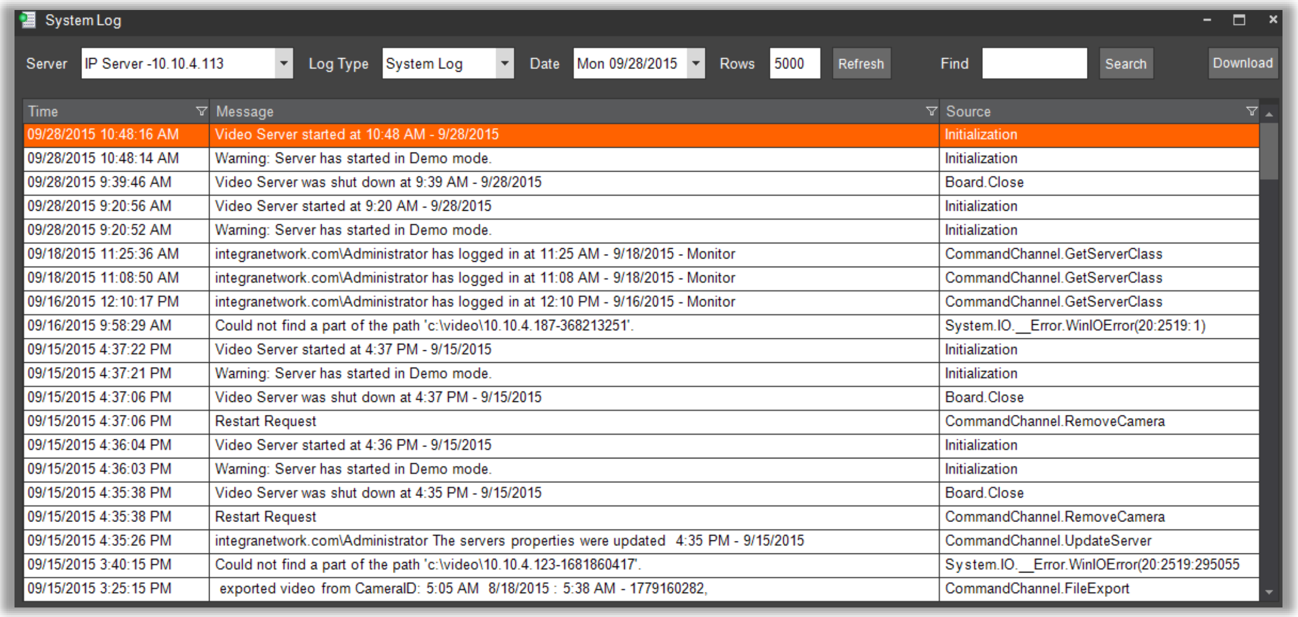
EXAMPLE - in a scenario with the timeout enabled and set to 30 seconds, there is a VI MonitorPlus Client layout comprised of both analog and IP camera images. For 30 seconds, both streaming and recording are managed by the IP Server. When 30 seconds have passed, the analog cameras will stop streaming 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:

- Check the **Enable Analog Video Bandwidth Timeout** box.
- Select the **Timeout** in seconds.
- Click **OK**.

(2B) IPSM: SYSTEM LOG

Clicking on **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.



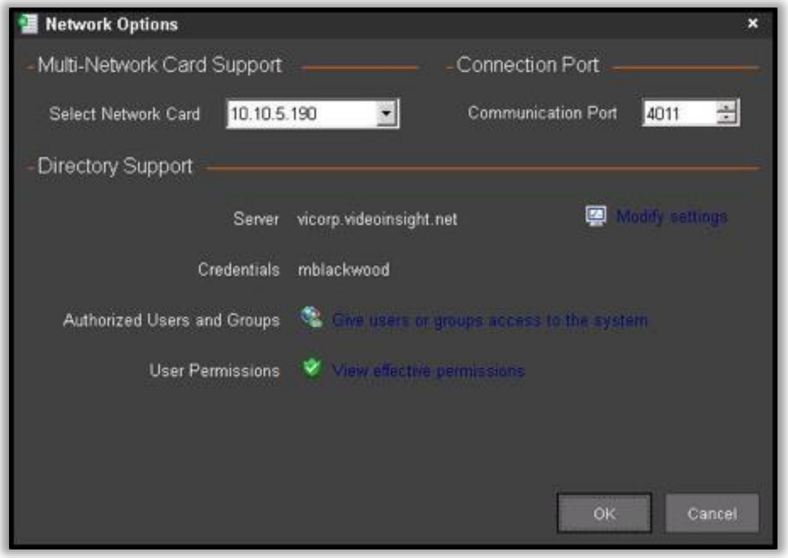
System Log

Server: IP Server -10.10.4.113 | Log Type: System Log | Date: Mon 09/28/2015 | Rows: 5000

Time	Message	Source
09/28/2015 10:48:16 AM	Video Server started at 10:48 AM - 9/28/2015	Initialization
09/28/2015 10:48:14 AM	Warning: Server has started in Demo mode.	Initialization
09/28/2015 9:39:46 AM	Video Server was shut down at 9:39 AM - 9/28/2015	Board.Close
09/28/2015 9:20:56 AM	Video Server started at 9:20 AM - 9/28/2015	Initialization
09/28/2015 9:20:52 AM	Warning: Server has started in Demo mode.	Initialization
09/18/2015 11:25:36 AM	integranetwork.com\Administrator has logged in at 11:25 AM - 9/18/2015 - Monitor	CommandChannel.GetServerClass
09/18/2015 11:08:50 AM	integranetwork.com\Administrator has logged in at 11:08 AM - 9/18/2015 - Monitor	CommandChannel.GetServerClass
09/16/2015 12:10:17 PM	integranetwork.com\Administrator has logged in at 12:10 PM - 9/16/2015 - Monitor	CommandChannel.GetServerClass
09/16/2015 9:58:29 AM	Could not find a part of the path 'c:\video\10.10.4.187-368213251'.	System.IO.__Error.WinIOError(20:2519:1)
09/15/2015 4:37:22 PM	Video Server started at 4:37 PM - 9/15/2015	Initialization
09/15/2015 4:37:21 PM	Warning: Server has started in Demo mode.	Initialization
09/15/2015 4:37:06 PM	Video Server was shut down at 4:37 PM - 9/15/2015	Board.Close
09/15/2015 4:37:06 PM	Restart Request	CommandChannel.RemoveCamera
09/15/2015 4:36:04 PM	Video Server started at 4:36 PM - 9/15/2015	Initialization
09/15/2015 4:36:03 PM	Warning: Server has started in Demo mode.	Initialization
09/15/2015 4:35:38 PM	Video Server was shut down at 4:35 PM - 9/15/2015	Board.Close
09/15/2015 4:35:38 PM	Restart Request	CommandChannel.RemoveCamera
09/15/2015 4:35:26 PM	integranetwork.com\Administrator The servers properties were updated 4:35 PM - 9/15/2015	CommandChannel.UpdateServer
09/15/2015 3:40:15 PM	Could not find a part of the path 'c:\video\10.10.4.123-1681860417'.	System.IO.__Error.WinIOError(20:2519:295055
09/15/2015 3:25:15 PM	exported video from CameraID: 5:05 AM 8/18/2015 : 5:38 AM - 1779160282,	CommandChannel.FileExport

NOTE - Only some messages may appear, depending on User level and Overall Server Configuration.

(2C) IPSM: NETWORK OPTIONS


Network Options
Multi-Network Card Support
Connection Port
Directory Support
Modify settings
Give users or groups access to the system
View effective permissions
OK
Cancel

Select Network Card: 10.10.5.190

Communication Port: 4011

Server: vicorp.videoinsight.net

Credentials: mblackwood

Authorized Users and Groups

User Permissions

Click on **Network Options** to display the Network Options dialog box.

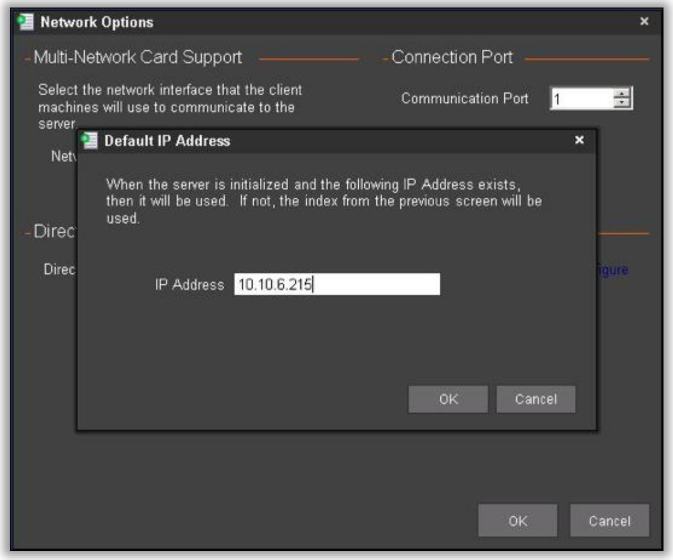
This dialog box is used for selecting the network scheme when a server has dual NIC cards or changing the communication port of the server.

It is also possible to change Active Directory and LDAP settings.

NOTE - If the Communication Port is changed, it must also change the command port in **Server Properties** within VI MonitorPlus.

The **Multi-Network Card Support** feature allows the user to use multiple NIC cards without configuration issues related to how the TCP/IP bindings within Windows server affect the flow of traffic.

To utilize this feature, click the **Advanced** button. A new window appears.



Select the network interface that the client machines will use to communicate to the server.

Communication Port: 1

When the server is initialized and the following IP Address exists, then it will be used. If not, the index from the previous screen will be used.

IP Address: 10.10.6.215

Here, the Administrator selects a specific internal IP address for public-facing (internal network facing) connectivity for the IP Server.

This is the IP address that is viewable from within VI MonitorPlus, as well as the IP Address that will be associated with IIS and the Web Client.

NOTE - This feature is best utilized with virtual environments, or with computers that have multiple NIC cards. It will force the registration of the MAC address that is associated with the IP Address that is provided by the administrator.

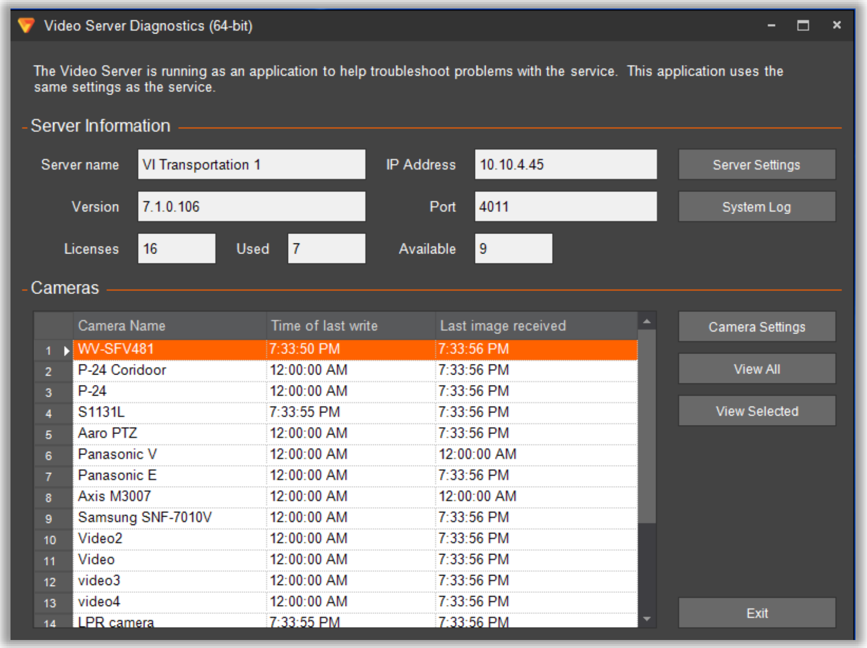
(2D) IPSM: DIAGNOSTICS

Clicking **Diagnostics** displays the **Video Server Diagnostics** interface.

This interface is used for troubleshooting most service related issues.

Server Settings can also be configured within VI MonitorPlus, with exception to testing the SQL database connectivity, and altering the SQL database connectivity.

NOTE - The IP Server service stops when Diagnostics is launched. To reactivate video recording and functionality, ***restart IP Server manually***.



Video Server Diagnostics (64-bit)

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

Server Information

Server name: VI Transportation 1
IP Address: 10.10.4.45
Version: 7.1.0.106
Port: 4011
Licenses: 16
Used: 7
Available: 9

Cameras

	Camera Name	Time of last write	Last image received
1	WV-SFV481	7:33:50 PM	7:33:56 PM
2	P-24 Coridoor	12:00:00 AM	7:33:56 PM
3	P-24	12:00:00 AM	7:33:56 PM
4	S1131L	7:33:55 PM	7:33:56 PM
5	Aaro PTZ	12:00:00 AM	7:33:56 PM
6	Panasonic V	12:00:00 AM	12:00:00 AM
7	Panasonic E	12:00:00 AM	7:33:56 PM
8	Axis M3007	12:00:00 AM	12:00:00 AM
9	Samsung SNF-7010V	12:00:00 AM	7:33:56 PM
10	Video2	12:00:00 AM	7:33:56 PM
11	Video	12:00:00 AM	7:33:56 PM
12	video3	12:00:00 AM	7:33:56 PM
13	video4	12:00:00 AM	7:33:56 PM
14	LPR camera	7:33:55 PM	7:33:56 PM

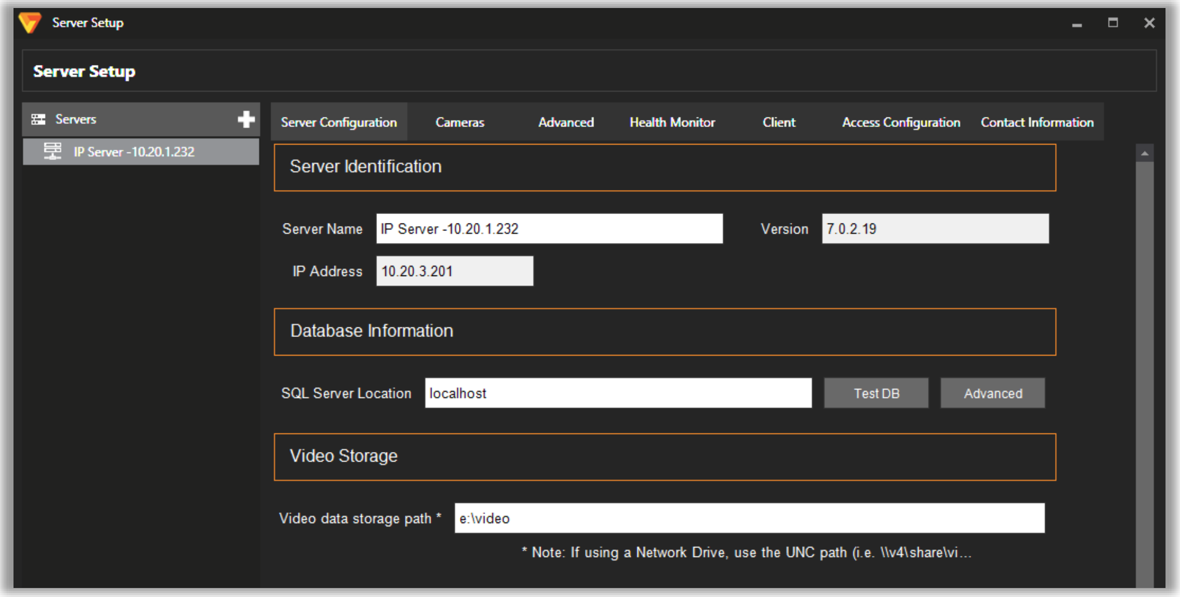
Server name	Server name previously entered. *It is **not** editable*. To change the name of the server, click **Server Settings** and configure in the left pane or from within Server Properties.
IP Address	Server's IP address and should not be changed if multiple clients will connect regularly to the IP Server.
Port	Port used by the VI MonitorPlus to control the IP Server. This port is referred to as the Command Channel Port. See list of ports for more information on ports used by the software.
Version	Software version of the IP Server. It should be the same as VI MonitorPlus to avoid errors.
Licenses	Maximum number of cameras allocated to the IP Server's serial number. Using only Video Insight Encoders, Advidia and / or Panasonic cameras on the system should reflect a value of zero.
Used	Number of cameras used against the license associated with the IP Server. If using Panasonic, Video Insight or Advidia cameras and/or encoders, no license will be used or deducted if other camera manufacturers are used and licensed with IP Server.
Available	Number of camera licenses available to add to the server.
Cameras	Cameras associated with the specific IP Server, including the Camera Name. The grid area of the Diagnostics interface is read-only. It displays all cameras, the last video write-time, the recording status, and the time the last video image was received from a camera.
Time of last write	Last time video was recorded to a file by IP Server. A time of 12:00:00 AM indicates that a camera may have Recording turned Off, or that it is not recording due to a Motion-Only recording type.
Last image received	Last moment in time video was received by the IP Server. A time of 12:00:00 AM is indicative of a camera that may be offline or not accessible. Common connectivity issues can be: incorrect credentials, network, bandwidth or the IP Server service is not running. Visit the online FAQ section for more information on why a camera could be offline.

NOTE - Remember to start the IP Server service after exiting the Diagnostics application.

Testing SQL connectivity and Changing the SQL Database location.

There are two additional features for troubleshooting within IPSM that are not available within VI MonitorPlus. To test the connectivity with SQL Server, select the IP server found on the left-hand side of the screen:

Click **Test DB** to test connectivity to the database.



Server Name: IP Server -10.20.1.232

Version: 7.0.2.19

IP Address: 10.20.3.201

SQL Server Location: localhost

Video data storage path *: e:\video

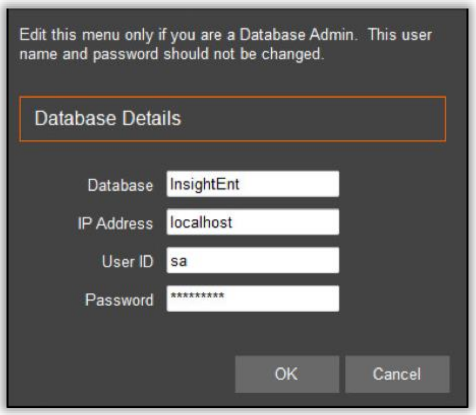
* Note: If using a Network Drive, use the UNC path (i.e. \\v4\share\vi...

The database test passes when the server makes a successful connection to the database. If the IPSM is not able to connect, the test will display: “Error: Database version is not correct.

Either the SQL database did not respond, or the IP Server has an outdated version of the SQL tables. There are several reasons why the database test may have failed. See the online FAQs for reasons for and potential solutions to the failure.

NOTE - Incorrect database information may cause test failure. To update or confirm the information, click **Advanced**.

- **Database:** Enter the database name. The default database name is **InsightEnt**.
- **IP Address:** Enter the IP address *or* the hostname of the SQL (database) server.
- **User ID:** The default user ID for the *InsightEnt* database is “sa” unless opting to use the VIUser credentials entered during the setup process.
- **Password:** The default password for the InsightEnt database is V4in$ight/ if using the default “sa” account in legacy systems. Otherwise, the password will be as selected during the setup process.



Edit this menu only if you are a Database Admin. This user name and password should not be changed.

Database: InsightEnt

IP Address: localhost

User ID: sa

Password: *********

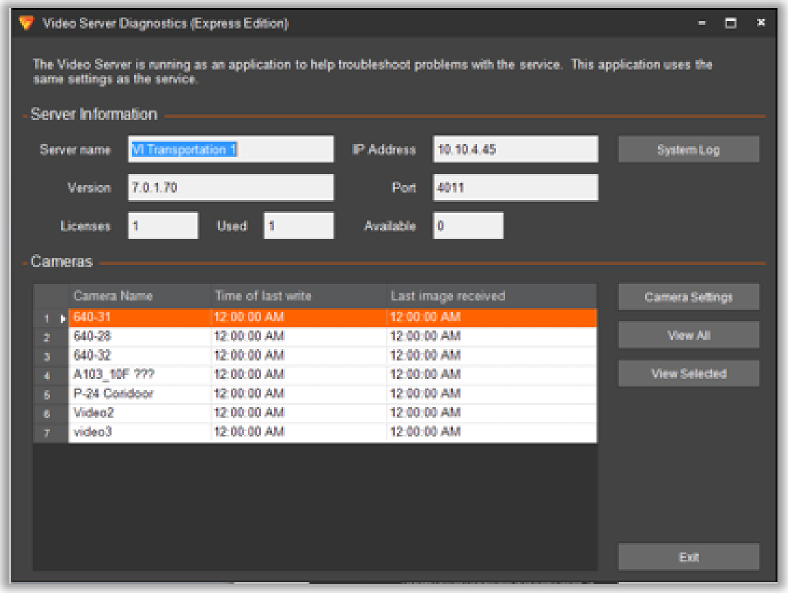
(2E) IPSM: NO CAMERAS

Another troubleshooting option is the use of **Diagnostics** that do not display live-video feeds for cameras associated with the IP Server.

This option does not consume any bandwidth, which might be useful when troubleshooting connectivity issues, or in environments with heavy network latency.

The **No Cameras** option is similar to the alternative **System Log** within VI MonitorPlus. Camera-related features and information such as **Live View** and **Time of Last Write** will not available after this diagnostics version is started.

NOTE - See IPSM Diagnostics for more information on running diagnostics.



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

Server Information

Server name: VI Transportation 1
IP Address: 10.10.4.45
Version: 7.0.1.70
Port: 4011
Licenses: 1
Used: 1
Available: 0

Cameras

	Camera Name	Time of last write	Last image received
1	640-31	12:00:00 AM	12:00:00 AM
2	640-28	12:00:00 AM	12:00:00 AM
3	640-32	12:00:00 AM	12:00:00 AM
4	A103_10F ???	12:00:00 AM	12:00:00 AM
5	P-24 Corridoor	12:00:00 AM	12:00:00 AM
6	Video2	12:00:00 AM	12:00:00 AM
7	video3	12:00:00 AM	12:00:00 AM

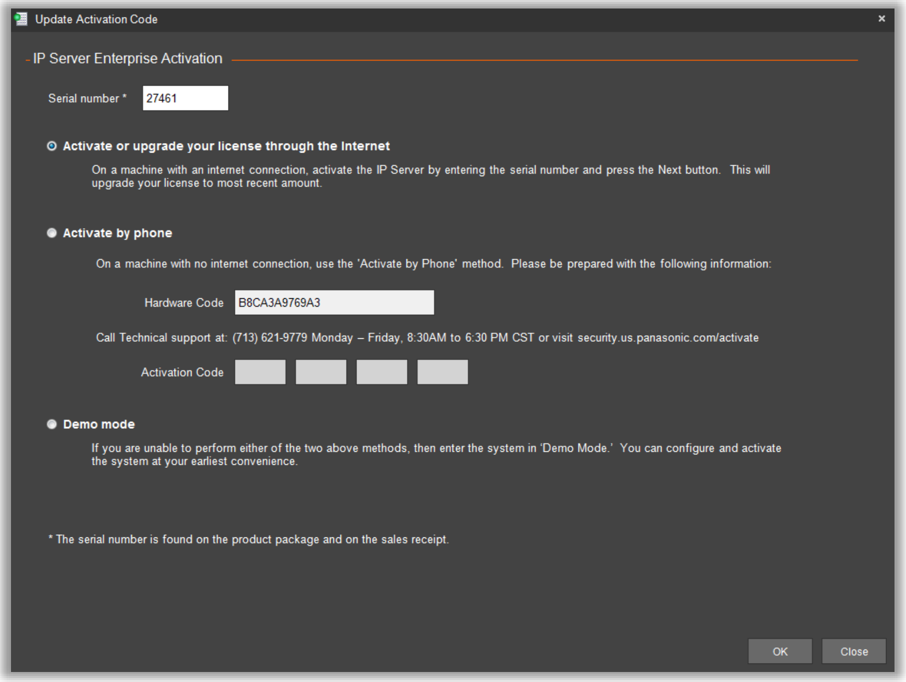
(2F) IPSM: UPDATE ACTIVATION

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.

NOTE - See Installation for more information on changing the activation type.

Click **OK** to confirm the number of licenses currently available.

When upgrading the license type from Express to Enterprise, **Enterprise** tab should be selected. Next, click **OK**.



IP Server Enterprise Activation

Serial number *: 27461

◉ **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. Please be prepared with the following information:

Hardware Code: B8CA3A9769A3

Call Technical support at: (713) 621-9779 Monday – Friday, 8:30AM to 6:30 PM CST or visit security.us.panasonic.com/activate

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 and activate the system at your earliest convenience.

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

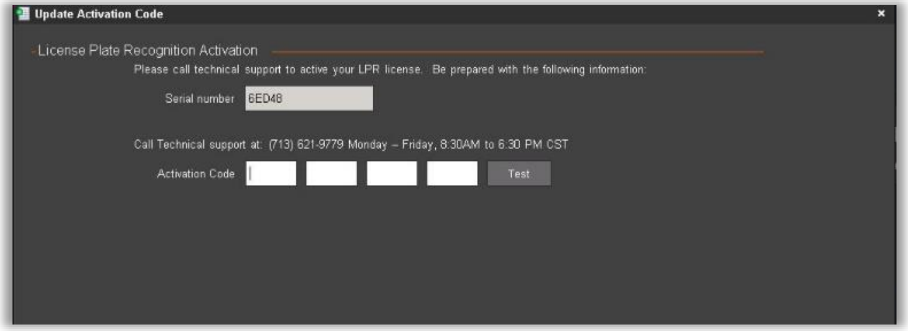
(2G) IPSM: LPR ACTIVATION

The **Update LPR Activation** option is used to update the LPR Activation.

To use the LPR feature, the USB dongle is required.

Enter Activation Code.

To validate the license, click **Test**.



Update Activation Code

License Plate Recognition Activation

Please call technical support to active your LPR license. Be prepared with the following information:

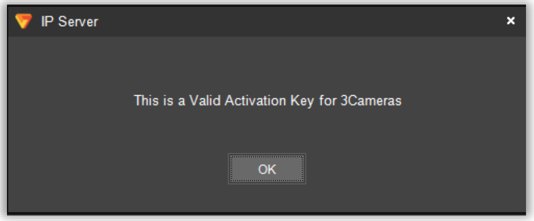
Serial number: 6ED48

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

Activation Code

Once IPSM confirms the provided license information, click **OK**.

Restart IP Server, then the license will be activated.



IP Server

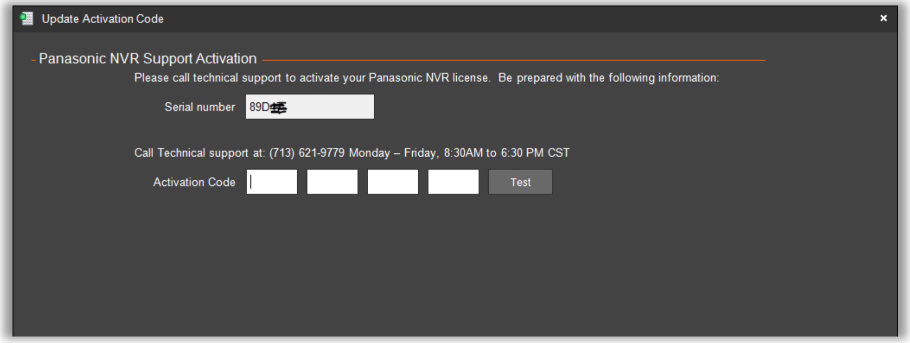
This is a Valid Activation Key for 3Cameras

(2H) IPSM: NVR ACTIVATION

The **Update NVR Activation** option is used to update the NVR Activation.

Enter Activation Code.

To validate the license, click **Test**.



Update Activation Code

Panasonic NVR Support Activation

Please call technical support to activate your Panasonic NVR license. Be prepared with the following information:

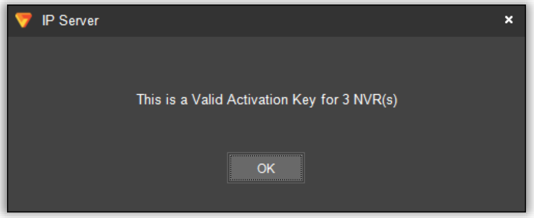
Serial number: 89D[redacted]

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

Activation Code

Once IPSM confirms the provided license information, click **OK**.

Restart IP Server, then the license will be activated.



IP Server

This is a Valid Activation Key for 3 NVR(s)

NOTE - If License type is Express, ***NVR will not be activated***.

3.4 ADVANCED INSTALLATION CONFIGURATION INFORMATION

3.4.A Installer: InstallShield

By default, the Setup_x64.exe installer for IP Server Enterprise places files into the *C:\Program Files\VI Enterprise* folder location and the Setup_x86.exe installer places into the *C:\Program Files(x86)\VI Enterprise* folder location.

NOTE - It is not possible to use a 64-bit installer to install into a 32-bit Operating System.

In instances where it may be necessary to know where packages are installed, they can be found in the local directory: *C:\Users\YourUsername\AppData\Local\Downloaded Installations.*

3.4.B Server Backup and Restore

IP Server can be backed-up manually. It is important to note that the reinstallation of IP Server requires the same version of software for reinstallation from backup due to differences in each database version. Therefore, it is recommended to maintain a backup of the IP Server installation software with the system backup.

If slightly different version is used, there may be a minor error during the installation, which may require Technical Support's assistance. In other cases, where different sub-versions are used, it may not be possible to restore IP server completely without a great deal of work.

With that observation, it is important to note the specific version used at the time of back up, and then any subsequent upgrades from that version to the current download to minimize any potential problems with the restoration process.

(1) BASIC IP SERVER BACKUP PROCESS

The IP Server can be backed-up with a minimum of effort. The steps below are provided with the assumption that SQL is located on the local server. It may be necessary to modify the steps to meet the needs of any custom installation done based on your organization's configuration.

On the host IP Server:

1. Open VI MonitorPlus.
2. Go to **Help** > **About.**
3. Note the version number of VI MonitorPlus /IP Server in use.
4. Go to http://www.downloadvi.com and find the matching version number of IP Server.
5. Download the matching version of IP Server / VI MonitorPlus.
6. Save the downloaded file to a safe location. (i.e.: a USB drive, a NAS device, another server, etc.).
7. Open the system's Start menu and choose Run.
8. Type: services.msc
9. Locate "Microsoft SQL service".
10. Right-Click and choose **Stop**.
11. Browse to My Computer > Local Disk C > Program Files > Microsoft SQL Server > MSSQL.1 > MSSQL > DATA
12. Copy Insightent.mdf and Insightent_log.ldf
13. Save these to a safe location. (i.e.: a USB drive, a NAS device, another server, etc.).
14. Return to the system's Start menu and select **Run**.
15. Type: **regedit**
16. In the new window that appears, browse to **HKLM>Software>Video Insight.**
17. Right-click the Video Insight folder and choose **Export**.
18. Save this file to the same location as the other files listed above.

(2) BASIC IP SERVER RESTORE PROCESS

Restoring an IP server from a backup, when following the procedures above, is an almost effortless process. If the steps above were followed, there should be no issues with a reinstallation of the IP server software, SQL database and/or the registry keys required for reinstallation. If a problem does arise, our Technical Support team is available during the hours listed at the end of this document.

To restore IP server, follow these steps:

1. Go to Start > Run
2. Type: services.msc
3. Find "Microsoft SQL service"
4. Right-Click and choose **Stop**.

5. Locate the files saved during the backup process and copy **InsightENT.mdf** and **InsightENT_Log.ldf**
6. Browse to My Computer > Local Disk C > Program Files > Microsoft SQL Server > MSSQL.1 > MSSQL > DATA
7. Paste **InsightENT.md**f and **InsightENT_Log.ldf** and replace the existing files of the same name (if they exist).
8. Locate saved files and double-click the Registry export file. This will re-install the registry keys.
9. Locate **services.msc** again.
10. Find "Microsoft SQL service"
11. Right-click and choose **Start.**
12. Reinstall the IP Server software with the same version number.
13. Reboot the computer after the installation is completed.

Congratulations. IP Server has been restored.

3.4.C Edge Recording

Failover Edge Recording, sometimes referred to as "Edge Storage," "Local Storage" or "On-Board" camera recording, is a feature of a camera designed to record video directly onto an SD card or other type of memory card physically installed on the camera- instead of a separate NVR or storage device.

Edge Recording, first released in IP Server v6.3.7 is to be used as a temporary bridge between the immediate need to capture video footage in case of a temporary IP server failure and the need to expand to a larger, fully redundant failover system. It is compatible with Panasonic iPRO and Advidia Cameras only at the time of this publication.

NOTE - Edge Recording does ***not*** work in conjunction with the IP Server Failover server.

In other words, If Edge Recording and Failover server are used at the same time, *ALL VIDEO RECORDING FOR NON-EDGE CAMERAS WILL BE LOST*. i.e. **The video recording feature will not work on IP Server**.

(1) OVERVIEW

Fail Over Edge Recording, when used with Video Insight's IP Server, allows for a temporary loss of connection between the IP Server and the camera without losing critical video captured during that time.

The camera will begin recording video after detecting a connection loss with the IP Server.

Once the connectivity between the IP Server and IP Camera is re-established, the IP Server will download the recorded video automatically. After the video is downloaded from the camera's SD Memory Card, then and only then will it be available for playback within VI MonitorPlus.

Necessary Considerations:
Failover Edge Recording was designed in response to the growing demand for reliable access to recorded video during a temporary NVR failure, or temporary loss of network connectivity between the NVR and the IP Camera.

Because of the loss of recorded video during critical times, Failover Edge Recording technologies have developed as a result. Yet, to prevent video loss, it should be stated that it is also necessary to assess the overall network equipment needs in order to achieve the greatest success and results with Failover Edge Recording.

Example:
During a temporary power outage, it is common to supply UPS battery backups for all servers in a server closet that supply power to the NVRs and mission critical computing devices.

However, for Failover Edge Recording to be truly successful, it is necessary to ensure that the total power consumption of any network switch responsible for powering Failover Edge Recording IP Cameras be taken into consideration as well.

Otherwise, without the use of a battery backup system to power IP Cameras using Failover Edge Recording technology, then the capture of Video Recording is negated and lost- even if the NVR remains functional during the power outage.

In the event of an unforeseen power outage, any camera that is not connected to a power source will not provide Failover Edge Recording due to a lack of power to the PoE switch. Thus, a lack of power to the PoE switch means a lack of power to the Edge Recording camera.

It is important to provide a battery backup system to the switch, or alternatively wire the cameras to get power from an alternative power source in the event of a power failure for Edge Recording to function as it is designed.

Configuration Description

The differences between normal IP Camera configuration and Failover Edge Recording configuration are the addition of some type of memory card and the confirmation of changes within the IP Camera for Failover Edge Recording to occur.

A basic outline of the process is as follows, in the necessary order for successful setup of Failover Edge Recording:

- Phase 1: Camera-Side Configuration
- Phase 2: IP Server Configuration
- Phase 3: Verification of communication between IP Camera and IP Server

(2) PREREQUISITES FOR EDGE RECORDING FUNCTIONALITY

The following items are required for the successful deployment of Failover Edge Recording. Any deviation outside that which is described in these prerequisites can cause a failure in Failover Edge Recording and a loss of critical video data.

(2A) REQUIRED HARDWARE

For long-term successful deployment of Failover Edge Recording:

- An appropriately sized SD/SDHC/SDXC memory card to match recording storage needs
- Panaso nic branded IP cameras running firmware v2.50 or later (Subject to change in future releases of IP Server)
- Functioning network equipment
- Necessary battery backup systems to power IP Cameras and/or POE switches in the event of a power outage

(2B) REQUIRED SOFTWARE

Prior to configuration of Failover Edge Recording:

- Video Insight's IP Server running at software version 6.3.6.4 or later
- SD Memory card is installed into the IP Camera

(3) SETUP AND CONFIGURATION

The following steps are to be followed in order. Once the initial setup has been confirmed functioning, other changes within the camera can be made.

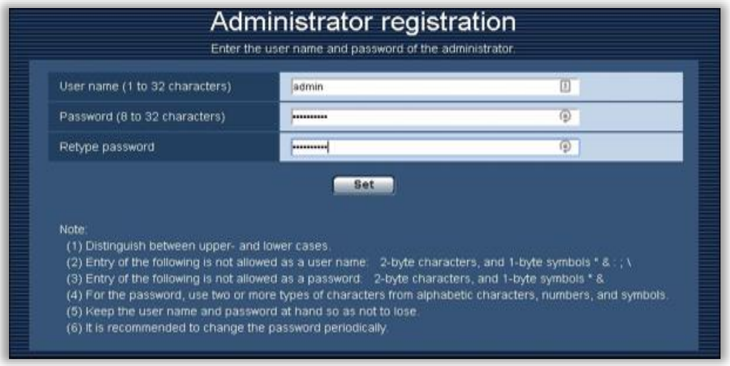
Consideration to the following steps are necessary for ease of installation:

- The camera is connected to the network and powered on
- The camera is set to its default values with firmware v2.50 or later
- The camera has a new SD Card installed and is ready to be formatted

If any of the three criteria are NOT followed, then Failover Edge Recording will **not** successfully be implemented.

(3A) CAMERA CONFIGURATION

With the assumption that the SD Card has been installed, and the camera has been connected to the network, it may be necessary to first access the camera's web page to set the default Administrator account.



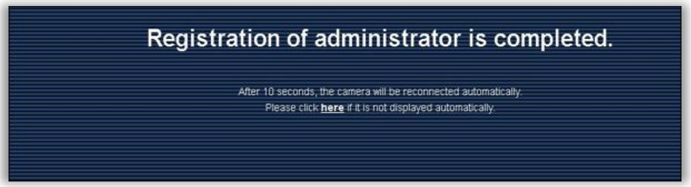
Administrator registration

Enter the user name and password of the administrator.

User name (1 to 32 characters)	admin
Password (8 to 32 characters)	••••••••••
Retype password	••••••••••

Note:
(1) Distinguish between upper- and lower cases.
(2) Entry of the following is not allowed as a user name: 2-byte characters, and 1-byte symbols " & : ; \
(3) Entry of the following is not allowed as a password: 2-byte characters, and 1-byte symbols " &
(4) For the password, use two or more types of characters from alphabetic characters, numbers, and symbols.
(5) Keep the user name and password at hand so as not to lose.
(6) It is recommended to change the password periodically.

Enter a username and password to access the camera being used with Edge Recording. Be sure to remember this information as it will be critical for accessing the camera settings and features in the future.



Registration of administrator is completed.

After 10 seconds, the camera will be reconnected automatically.
Please click **here** if it is not displayed automatically.

A confirmation message will show once the new administrative account password has been set.

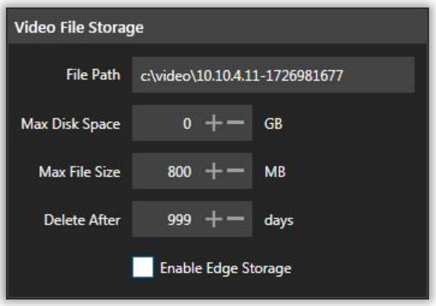
PAUSE HERE. DO NOT REBOOT THE CAMERA.

Next, minimize the browser window for the IP camera.

NOTE - Reopen the browser to confirm the correct configuration and access between IP Server and the Camera.

(3B) IP SERVER CONFIGURATION

Add camera through normal process, as described in the Installation section.



Video File Storage

File Path: c:\video\10.10.4.11-1726981677

Max Disk Space: 0 GB

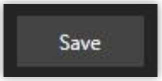
Max File Size: 800 MB

Delete After: 999 days

□ Enable Edge Storage

After a camera is added to IP Server, open **Camera Properties** and select the **Recording** tab.

Select **Enable Edge Storage** found on the bottom right-hand side of the screen, under the **Video File Storage** section.



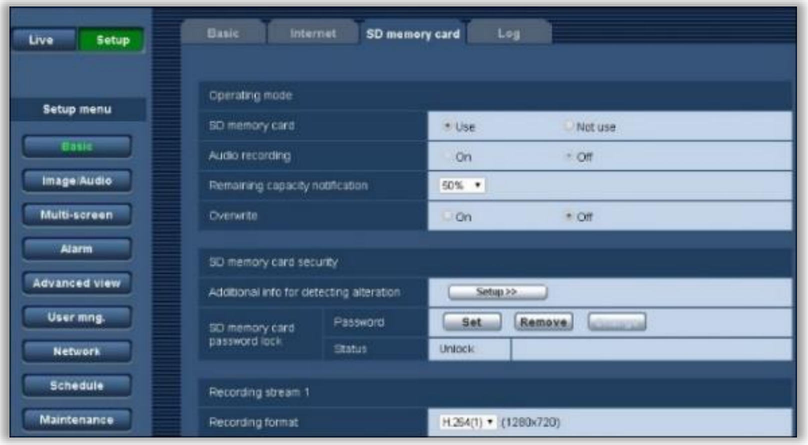
Click on **Save;** Restart VI MonitorPlus AND Video Insight's IP Server.

NOTE - Wait until IP server is running again before proceeding.

(3C) COMMUNICATION VERIFICATION

The process of verification of communication between IP Server and IP Camera is crucial to determining the efficiency of Failover Edge Recording. This step will help make troubleshooting easier in the event of an unlikely Edge Recording failure.

After the IP Server has restarted, open the camera's Management interface within the internet browser window that was minimized at the end of Step 1, and proceed as follows:



Operating mode

SD memory card: ● Use ○ Not use

Audio recording: ○ On ● Off

Remaining capacity notification: 50%

Overwrite: ○ On ● Off

SD memory card security

Additional info for detecting alteration

SD memory card password lock — Password; Status: Unlock

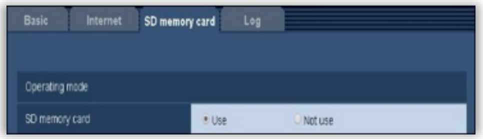
Recording stream 1

Recording format: H.264(1) (1280x720)

On the next page, Select **Setup**.
On the **Setup** page, the green button labelled **Basic** should be highlighted by default.

Select the **SD Memory card** tab at the top of the screen.

On the **SD Memory card** page, verify the following:

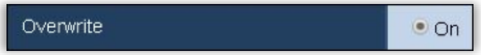


Operating mode

SD memory card: ● Use ○ Not use

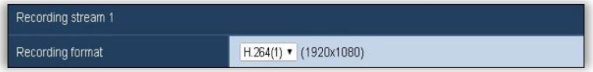
SD Memory card:

USE *must* be selected if it is not already.



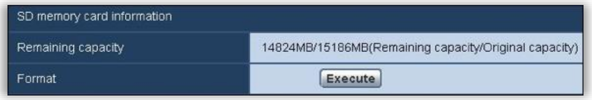
Overwrite: ● On

Overwrite **MUST** be **ON** if it is not already.



Recording stream 1	
Recording format	H.264(1) ▾ (1920x1080)

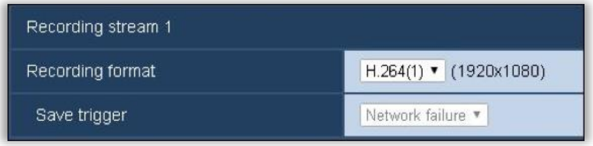
Recording Stream 1:
This is set to H.264 (1) by default.
It is possible to select one of the four available H.264 settings. ** see notes below for more information*



SD memory card information	
Remaining capacity	14824MB/15186MB(Remaining capacity/Original capacity)
Format	Execute

SD memory card information: Format the installed SD Card

*** see notes below*

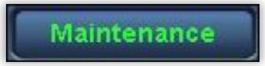


Recording stream 1	
Recording format	H.264(1) ▾ (1920x1080)
Save trigger	Network failure ▾

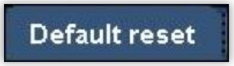
This page provides an easy way to determine if the IP Server has successfully connected to the IP Camera with Failover Edge Recording enabled. Verify that the **Save Trigger** (under Recording Stream 1) is greyed out and displays the phrase *Network failure*.

Network failure *should* appear, as displayed on the left. This is confirmation of a successful connection with the IP Camera and Failover Edge Recording.

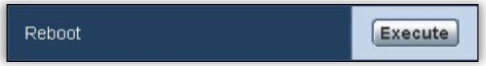
If **Network Failure** IS visible, reboot the camera by doing the following steps:



Select **Maintenance** (on the left)



Select Default reset tab



Find **Reboot** from the list of options presented and then select **Execute**. (The reboot process takes 2 minutes.)

Congratulations! Edge Recording is now configured!

NOTES:
* The image above depicts only the first selection for H.264 configuration settings as an example. It is recommended that the owner's manual be read for the specific camera used with EDGE Recording to better understand how this specific section will affect the captured video recording while implemented by Edge recording.

** If the SD Card has been installed and never formatted, it is recommended that a full formatting of the card be done the first time Edge recording settings are configured to ensure that video is captured.

*** If **Network Failure** is *NOT* visible now, then IP server is not communicating with the camera. It is recommended that the camera be removed from IP server and that the camera be defaulted to original factory condition and the steps above.

3.4.D Rules Manager

Rules Manager provides necessary automation of certain tasks to help the Administrator or any desired features range from sending email to a specific email address after a video camera detects motion, to moving video files from one location to another for the purposes of server maintenance and long-term storage.

Rule Creation Process Cheat Sheet

Basic Steps	Trigger Events	Action Events
1. Open VI MonitorPlus 2. Click the Administration tab 3. Click on the Rules icon 4. Select the + icon for new rule creation 5. Select Add Trigger OR Add Action	1. When the new Trigger selection window appears, select the trigger desired for activation 2. Provide the necessary information for that trigger to become active 3. Click OK 4. Move to Action events section below the Trigger events section 5. Select Add Action	1. After the new Action Events window opens, select the desired resulting action event. 2. Provide the necessary information within the Action being used 3. Click OK 4. Restart IP Server 5. Test rule for verification

These are the most basic steps required for the creation of a rule that will increase the productivity, security and further enhancement of the Video Insight IP Server Enterprise suite.

(1) BASIC CONCEPTS

In most scenarios, a rule is made up of two parts: **Triggers** and **Actions**.

A trigger can be as simple as motion detection on a camera. A subsequent action can be to take a snapshot of the image and to email it to a specific email address. The rule itself, in basic terms would be written as: When there is motion on a specified camera, take a snapshot and send that snapshot to a specific email address.

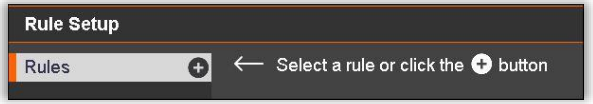
(2) CREATING A RULE

To start the process of rule creation, it is best to open VI MonitorPlus and select the Administration tab at the top of the screen. Then, once the Administration tab has been selected, click on the Rules button in the navigation menu.

Creating a rule takes many considerations, but it can be broken into four specific areas:

- Rule Properties
- Schedule
- Trigger Events
- Action Events

To create a New Rule, click the **+** symbol to the right of the Rules bar.



(3) RULE PROPERTIES

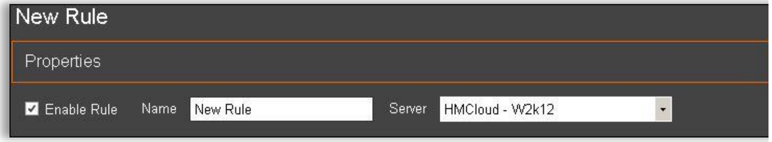
Once the Rule creation process is started, give the new rule a unique name and a description.

During Rule creation, it is important to be mindful of instances where VI MonitorPlus might be connected to more than one IP server. If VI MonitorPlus is connected to multiple IP Servers, it is necessary to verify the name of the server where the rule will be applied so that a newly created rule doesn't inadvertently damage another server.

Enable Rule: Sometimes a rule loses its usefulness or causes a conflict with other rules.

Name: Provide a descriptive name.

Server: Select the server from the drop-down where the rule will apply.



☑ Enable Rule Name: New Rule Server: HMCloud - W2k12

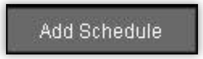
NOTE - To determine which rule might be contributing to a problem, the ability to disable or re-enable a rule manually is available. This allows the Administrator the temporary ability to troubleshoot or configure other items within IP Server.

(4) SCHEDULES

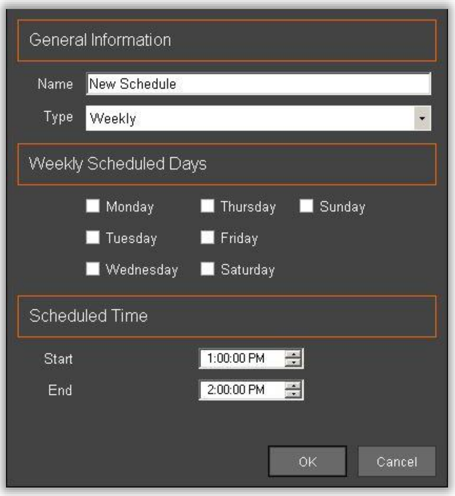
Schedules are a necessary tool provided to perform certain maintenance and functional tasks within the operational use of IP Server.

The default condition for all Rules is to ***run always***. This means that no Schedule is necessary if there is no need for an Action to occur, unless it is to occur at a specific time of day.

(4A) SCHEDULE SETUP



When the Rules manager tool within VI MonitorPlus opens, and the Add Schedule button is selected, a new pop-up window will appear.



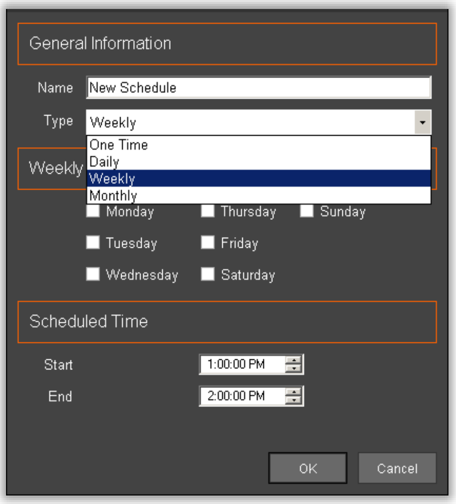
Name: New Schedule
Type: Weekly
Start: 1:00:00 PM
End: 2:00:00 PM

This new pop-up allows the user to provide a name for the schedule, the frequency which it runs, the days that it will run, and the times that it will run.

NOTE - It is recommended that the name of the schedule serve as a reminder for the trigger and action events for later troubleshooting, if necessary.

Please refer to the documentation below regarding use of the scheduled days.

It may be necessary to create multiple schedules for events that overlap the 11:59 pm to 12:00 am threshold.



Name: New Schedule
Type: Weekly
Start: 1:00:00 PM
End: 2:00:00 PM

Select the appropriate number of times the rule will run. This is critical for the long-term success of the rule, without errors.

One Time - The Rule will work only once, and it will not be repeated at any point in time unless manually triggered by the user.

Daily - The Rule will run either every Weekday, every Weekend Day or every Day, at the specific times selected, as long as it is active..

Weekly- The Rule will be executed on a specific set of Days of the Week, during the selected time interval.

Monthly - The Rule will run either Once (by selecting a specific Day), or during a specific occurrence of Days and Weekdays in a Month. within the selected Time interval..

After all the necessary criteria is provided in the fields above, click on **OK**. The schedule is now complete.

(4B) MULTIPLE SCHEDULES

The most common occurrence for multiple schedules is usually tied to tasks that occur on a weekly or monthly basis according to the need of the IP Server Administrator.

If a series of actions is required multiple times per day, multiple schedules can be created within the same rule.

It is important to note that the **Default** for all created rules is for them to run at ***all times***. Adding a schedule to a rule that runs always may prove the rule to be ineffective or result in an undesired effect if added haphazardly.

NOTE - The schedule timer runs on a 12:00 am to 11:59 pm cycle for each day.

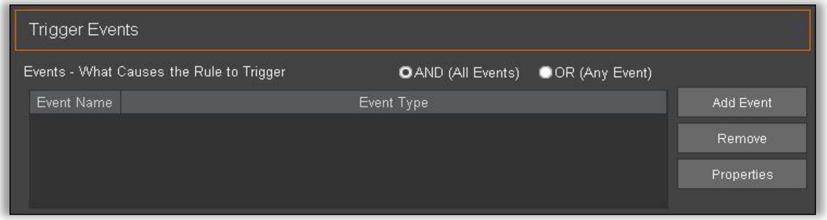
This means that each segment of a scheduled task is limited to the specific day of that task and will not overlap with other tasks. It will not span the course of multiple days, even if it appears that it would, otherwise.

Therefore, it is required that multiple schedules be created if there is to be a repetition of actions based on selected triggers spanning the course of many days where the threshold between any two days is required.

(5) TRIGGER EVENTS

Trigger Events are best thought of as a *cause* for an action. Within VI MonitorPlus, Trigger Events occur as the direct result of something that has happened. Once the event has occurred, it will be followed by an action that is designated below:

Trigger Events can be considered as the "**IF**" in an "If, Then" statement. (***IF Trigger event occurs, THEN do this Action Event***). When creating a rule, the Administrator should first consider what event it is that is occurring that needs to have an action follow it.



Trigger Events

Events - What Causes the Rule to Trigger ◉ AND (All Events) ○ OR (Any Event)

Event Name	Event Type

(5A) TRIGGER EVENT SETUP

It is important to determine whether the event needs to meet multiple criteria or if it requires only one event to occur prior to an action event.

Knowing that information allows the administrator to determine whether the Trigger event will work as desired with the Action Event that follows.

To keep things simple, it is suggested that the first rule created have as few items as possible. Once it is determined that the rule was successfully created, it will be easier to determine if there is a problem down the line.

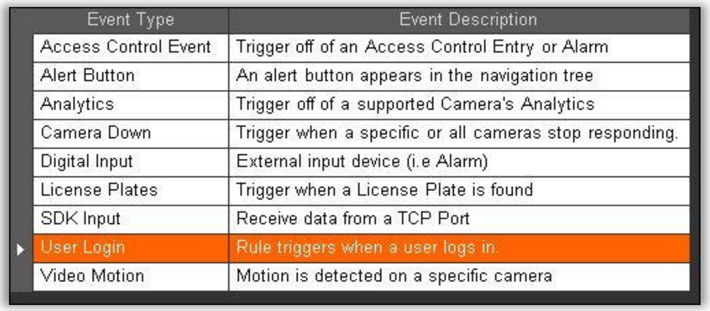
EXAMPLES:

- *Single Event (Any)*

  IF a Camera becomes unresponsive OR a specific user logs in to IP Server.
- *Multiple Events: (AND)*

  IF Camera becomes unresponsive AND specific user logs into the IP Server.

(5B) TRIGGER EVENT OPTIONS



Event Type	Event Description
Access Control Event	Trigger off of an Access Control Entry or Alarm
Alert Button	An alert button appears in the navigation tree
Analytics	Trigger off of a supported Camera's Analytics
Camera Down	Trigger when a specific or all cameras stop responding.
Digital Input	External input device (i.e Alarm)
License Plates	Trigger when a License Plate is found
SDK Input	Receive data from a TCP Port
User Login	Rule triggers when a user logs in.
Video Motion	Motion is detected on a specific camera

Selecting **Add Event** results in a new window appearing within VI MonitorPlus**.** The window offers the following options to select from. A description of what each **Event Type** does is explained in the chart below in a little more detail.

(5C) TRIGGER EVENT DEFINITIONS

Trigger	Description
Access Control Event	Triggers an Access Control Entry or Alarm
Alert Button	Triggers when an alert button appears in the navigation tree
Analytics	Triggers from a supported Camera's Analytics *
Camera Down	Triggers when a specific camera stops responding or all cameras stop responding
Digital Input	Triggers based on external input device *
License Plates	Triggers when a license plate is found *
SDK Input	Triggers based on receiving data from a TCP port *
User Login	Triggers when a user logs into the IP Server
Video Motion	Triggers when motion is detected on a specific camera *

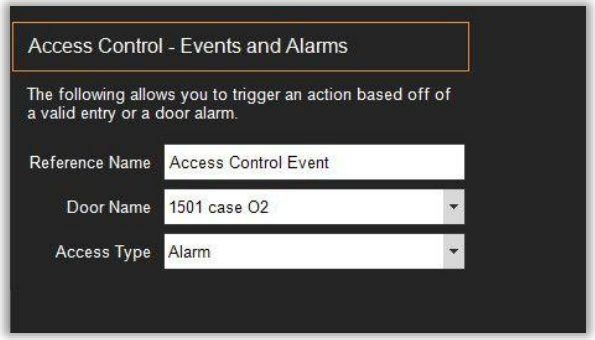
** Items with an asterisk, listed above, require that the device has the capability of the function itself. Please refer to the device manufacturer's user guide for information on how to utilize its functionality for best results.*

(6) TRIGGER INPUT REQUIREMENTS

Access Control Event

Access Control Events allows to trigger an Action based on a valid entry or on a door alarm

Define a unique Reference Name; select a Door from the **Door Name** drop-down list and, for **Access Type**, select either **Alarm** or **Entry**.



Access Control - Events and Alarms

The following allows you to trigger an action based off of a valid entry or a door alarm.

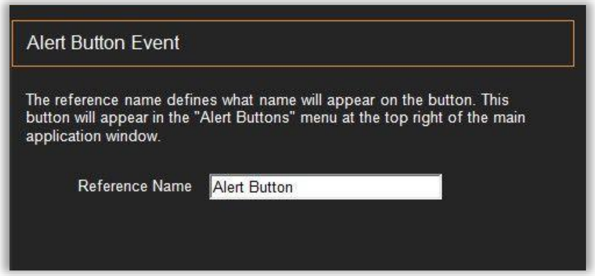
Reference Name: Access Control Event

Door Name: 1501 case O2

Access Type: Alarm

Alert Button

This type of Event only requires a unique **Reference Name**, which will be displayed in the **Alert Buttons menu** at the top right of the main application window.



Alert Button Event

The reference name defines what name will appear on the button. This button will appear in the "Alert Buttons" menu at the top right of the main application window.

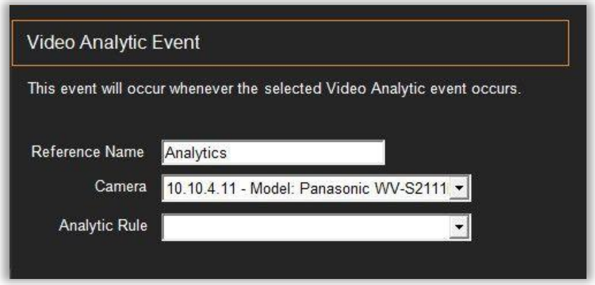
Reference Name: Alert Button

Analytics

Camera Analytics are used for camera "training" in areas that require enhanced security functionality.

Define a unique **Reference Name**, select the **Camera** from the drop-down list and the **Analytic Rule** to be applied, if available.

Cameras that can enhance their capabilities over time may offer a variety of functions based on their set of features.



Video Analytic Event

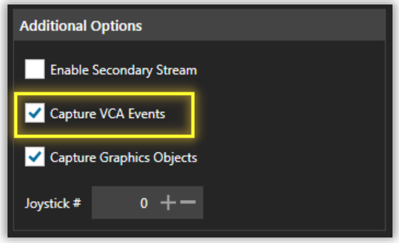
This event will occur whenever the selected Video Analytic event occurs.

Reference Name: Analytics

Camera: 10.10.4.11 - Model: Panasonic WV-S2111

Analytic Rule:

To use this feature, open the **Camera Properties** for the selected camera and check the **"Capture VCA Event"** box in the **"General"** tab, **"Additional Options"** section.



Additional Options

□ Enable Secondary Stream

☑ Capture VCA Events

☑ Capture Graphics Objects

Joystick #: 0

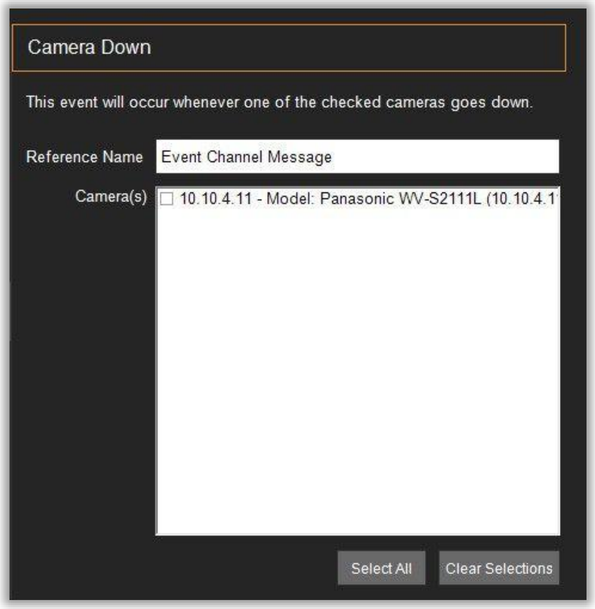
Camera Down

The **Camera Down** Event relies on multiple variables to be triggered.

Most commonly, this trigger becomes active when a camera cannot be logged into by the IP Server or becomes unresponsive due to a network outage.

It is helpful for early detection of issues that might not be immediately noticed by the Administrator.

Define a unique **Reference Name** for the Event and select the **Camera(s)** to be monitored from the list.



Camera Down

This event will occur whenever one of the checked cameras goes down.

Reference Name: Event Channel Message

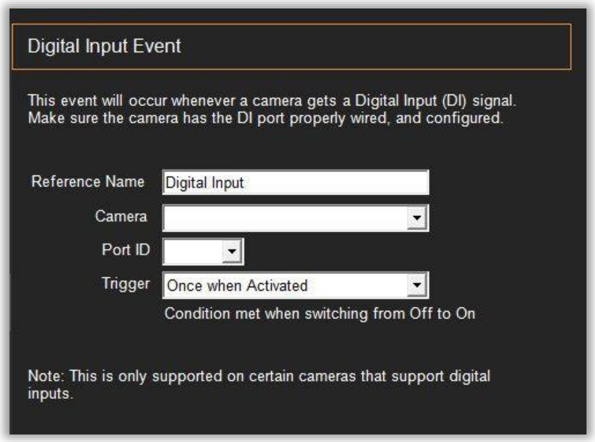
Camera(s): □ 10.10.4.11 - Model: Panasonic WV-S2111L (10.10.4.1

Digital Input

Some manufacturers provide cameras with the ability to enhance their functionality using **Digital Input**/**Output** devices within VI MonitorPlus.

Most commonly, a microphone is used with a camera via **Digital Input/Output** to record conversations within its range.

Define the unique **Reference Name** for the Event, then select the **Camera** from the drop-down list of available devices, its **Port**, and the **Trigger Type**.



Digital Input Event

This event will occur whenever a camera gets a Digital Input (DI) signal. Make sure the camera has the DI port properly wired, and configured.

Reference Name: Digital Input

Camera:

Port ID:

Trigger: Once when Activated

Condition met when switching from Off to On

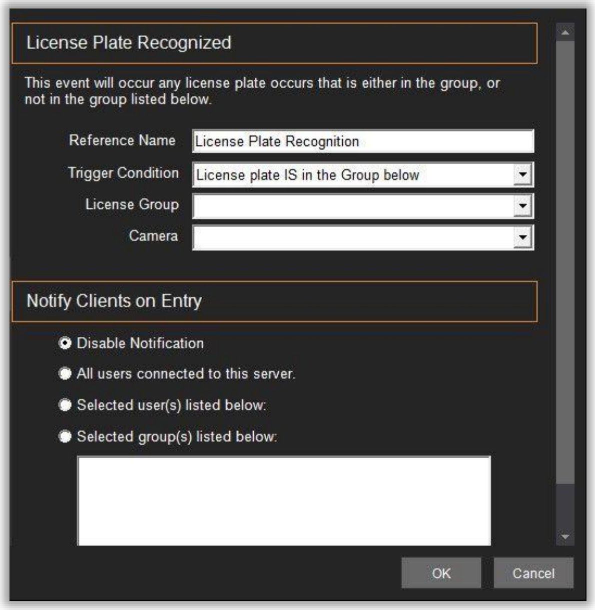
Note: This is only supported on certain cameras that support digital inputs.

License Plates

License Plate Recognition (LPR) Events occur when a license plate that is either **in** or **not in** the Group listed below is detected by a specific camera.

It requires a unique **Reference Name**, a **Trigger Condition** (license plate ***IS*** or ***IS NOT*** in the Group below), the corresponding **License Group** and the **Camera** that will detect the event.

Additionally, when an Entry is detected, a **Notification** message can be sent to All Users connected to the server or to selected User or Groups defined from a list.



License Plate Recognized

This event will occur any license plate occurs that is either in the group, or not in the group listed below.

Reference Name: License Plate Recognition

Trigger Condition: License plate IS in the Group below

License Group:

Camera:

Notify Clients on Entry

● Disable Notification

○ All users connected to this server.

○ Selected user(s) listed below:

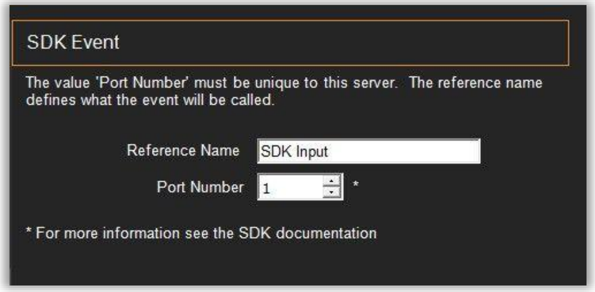
○ Selected group(s) listed below:

SDK Input

SDK Input Events allow the IP Server to interface with other software and hardware manufacturers connected to the same network; they indicate that IP Server is receiving data from the connected SDK device/software.

The value for **Port Number** must be ***unique*** to the server, as well as the **Reference Name**.

This is only used by software and hardware developers and for testing purposes.



SDK Event

The value 'Port Number' must be unique to this server. The reference name defines what the event will be called.

Reference Name: SDK Input

Port Number: 1 *

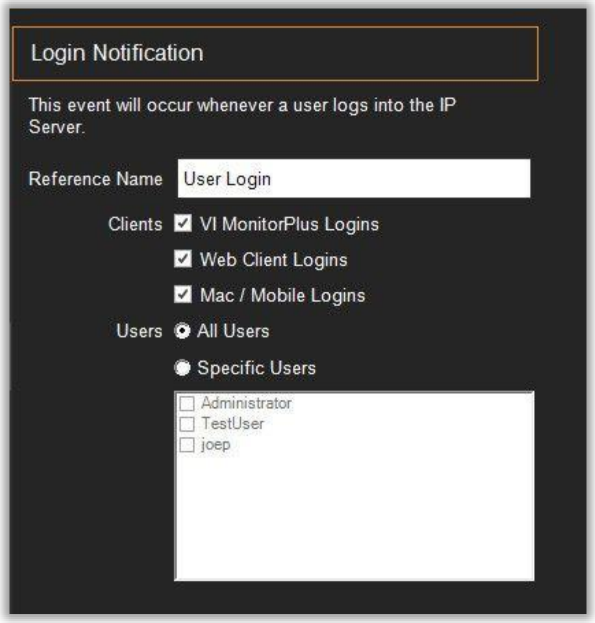
* For more information see the SDK documentation

User Login

User Login is for notifications to groups of Admins or higher-access-level Users who need to monitor a system for unusual access rights, or for routine use of IP server.

A unique Reference Name must be provided, as well as the selection of Clients and Users to be monitored (*see list of options in the image*).

When a User logs into the system, it is recorded into the IP Server System Log files.



Login Notification

This event will occur whenever a user logs into the IP Server.

Reference Name: User Login

Clients: ☑ VI MonitorPlus Logins

☑ Web Client Logins

☑ Mac / Mobile Logins

Users: ● All Users

○ Specific Users

☐ Administrator

☐ TestUser

☐ joep

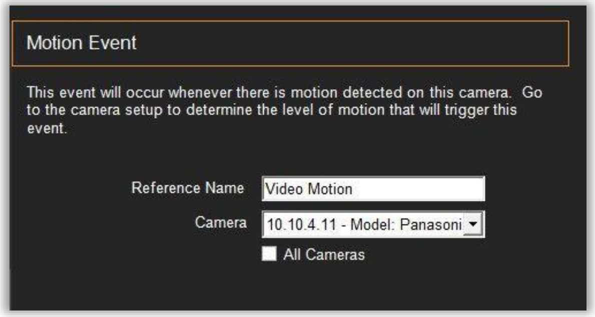
Video Motion

Motion Events occur when there is motion detected on a camera.

NOTE - The level of motion that triggers this event can be configured in the **Camera Setup** module of **VI MonitorPlus**.

This event requires a unique **Reference Name** and to select either a **single** specific Camera or **All** cameras in the network.

Motion Events are recorded in the IP Server System Logs and can be utilized by an Action Event.



Motion Event

This event will occur whenever there is motion detected on this camera. Go to the camera setup to determine the level of motion that will trigger this event.

Reference Name: Video Motion

Camera: 10.10.4.11 - Model: Panasoni

□ All Cameras

(7) ACTION EVENTS

Action Events are operations and actions resulting after a **Trigger Event** occurs, based on their criteria.

Below is a list of available Action Events. Not all action events will function with all trigger events. Refer to the **Functional Relationship Guide** further below this section for a complete reference of **Trigger Event** and **Action Event** interactions.

(7A) ACTION DEFINITIONS

Actionable Input	Description
Door State	Change the state of the door.
Digital Output	Send a digital output on a specific port.
Execute a program	Send a program to a specific user running VI MonitorPlus to execute.
HTTP Command	Send an HTTP command to a specific device.
TCP Message	Send ASCII message to TCP socket.
Email	Email a custom message.
Email AVI clip	Email AVI file to a specific user.
Email Flashback Image	Email Flashback image.
Email Snapshot	Email a snapshot of an image to a specific email address.
Action Event Log	Create an action event for the Media Player.
Alarm Window	Displays alarm window for client within Workspaces and Message Display.
Audio Alert	Audio alert for a specified VI MonitorPlus Client.
File Manipulation	Copy, Move or Delete files.
Instant Replay	Pop up a 30-second review of recorded video on a specific camera.
Live Window	Pop up window for displaying a live camera feed.
Message instruction	Message instruction for the VI MonitorPlus Client.
Move PTZ Camera	Move a PTZ camera to a specific location.
Record	Set a recording type.
Record with Audio	Create a video file with audio included.
Switch Audio	Switch viewing field to a specific camera, capable of audio recording.
Switch Camera	Switch VI MonitorPlus ’s main layout to a camera view.
Switch View	Switch VI MonitorPlus 's main view to a specific view.
Time Lapse Recording	Create time-lapse recordings (very low frame rate).
Monitor Points	Mask / unmask monitor points.

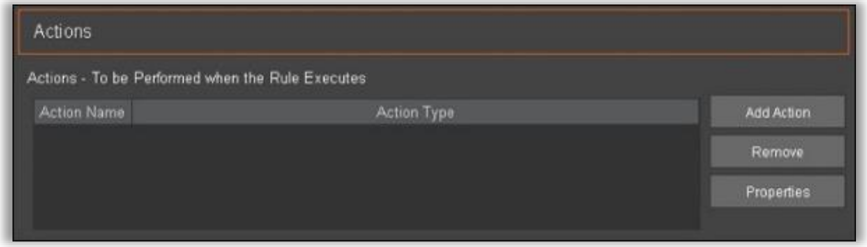
(7B) ACTION EVENT SETUP

On the **Rules Manager Rule Creation** page, the **Actions** section provides the option to customize actions that will take place *AFTER* a trigger is received by the server. Not all actions require a trigger to function, yet all actions will be affected by any triggered schedules. Be very careful when selecting specific time-related triggers as they may have an adverse effect on subsequent Actions.

Action events can be used to further enhance a linear chain of events, which result in the action becoming a trigger for a second action, and so on. Please refer to the definitions for each Action below the Action Event Setup procedures.

Action Event Creation

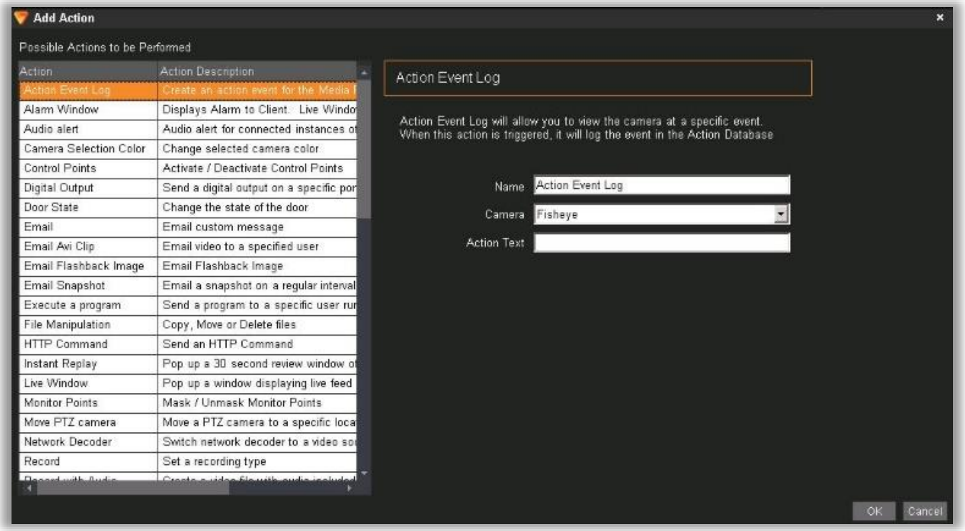
The process of creating an Action comes after a Trigger Event is created. To create an action that is used with a trigger, click the **Add Action** button.



Actions - To be Performed when the Rule Executes

Action Name	Action Type

A larger **Add Action** window appears. This window provides a comprehensive list of the available actions that can be taken.



Possible Actions to be Performed

Action	Action Description
Action Event Log	Create an action event for the Media I
Alarm Window	Displays Alarm to Client. Live Windo
Audio alert	Audio alert for connected instances of
Camera Selection Color	Change selected camera color
Control Points	Activate / Deactivate Control Points
Digital Output	Send a digital output on a specific por
Door State	Change the state of the door
Email	Email custom message
Email Avi Clip	Email video to a specified user
Email Flashback Image	Email Flashback Image
Email Snapshot	Email a snapshot on a regular interval
Execute a program	Send a program to a specific user rur
File Manipulation	Copy, Move or Delete files
HTTP Command	Send an HTTP Command
Instant Replay	Pop up a 30 second review window of
Live Window	Pop up a window displaying live feed
Monitor Points	Mask / Unmask Monitor Points
Move PTZ camera	Move a PTZ camera to a specific loca
Network Decoder	Switch network decoder to a video so
Record	Set a recording type
Record with Audio	Create a video file with audio included

Action Event Log

Action Event Log will allow you to view the camera at a specific event.
When this action is triggered, it will log the event in the Action Database

Name: Action Event Log
Camera: Fisheye
Action Text:

Select the desired **action** to be taken.

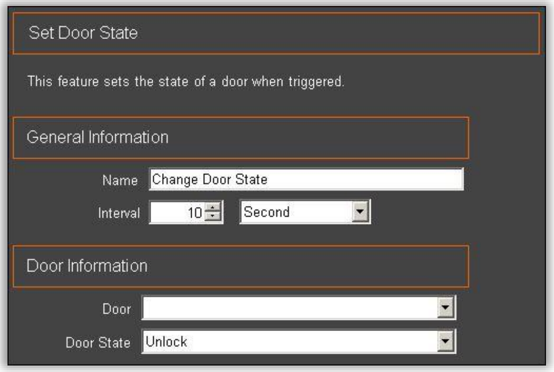
NOTE - Depending on the action it is necessary, in most instances, to provide some additional information for the specific action for it to function properly.

When completed, click **OK**

(7C) ACTION EVENT EXPANDED DEFINITIONS

Door State is a function of Access Control trigger events. Its function as an action is designed to act as a timer for a noticed change in a door status over a period of time.

Additionally, it can be used to automatically change Access Control door status from locked to unlocked or vice versa.



Set Door State

This feature sets the state of a door when triggered.

General Information

Name: Change Door State

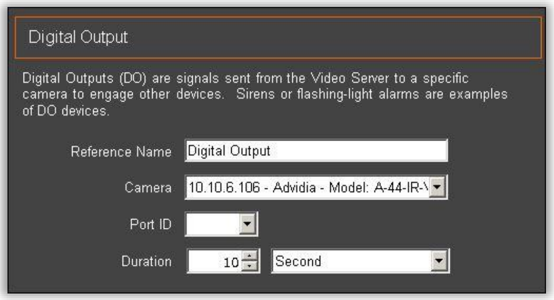
Interval: 10 Second

Door Information

Door:

Door State: Unlock

Digital Output is an Action event which works to aid in the enhancement of a security device with the use of additional input from that device. This is an **Action Event** that relies on a specific trigger and acts as a trigger.



Digital Output

Digital Outputs (DO) are signals sent from the Video Server to a specific camera to engage other devices. Sirens or flashing-light alarms are examples of DO devices.

Reference Name: Digital Output

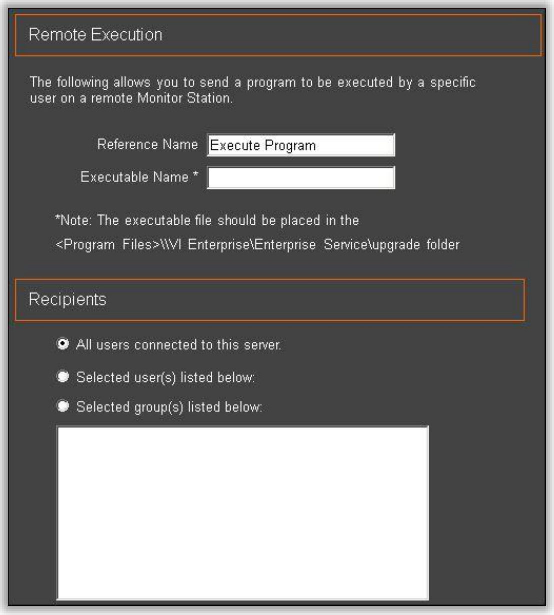
Camera: 10.10.6.106 - Advidia - Model: A-44-IR-\

Port ID:

Duration: 10 Second

Execute a Program is designed to force a program on a computer to also start once the corresponding trigger value is assigned to it.

For example, a program could be started when a specific user login trigger is activated, saving time for the user on their machine.



Remote Execution

The following allows you to send a program to be executed by a specific user on a remote Monitor Station.

Reference Name: Execute Program

Executable Name *:

*Note: The executable file should be placed in the <Program Files>\\VI Enterprise\Enterprise Service\upgrade folder

Recipients

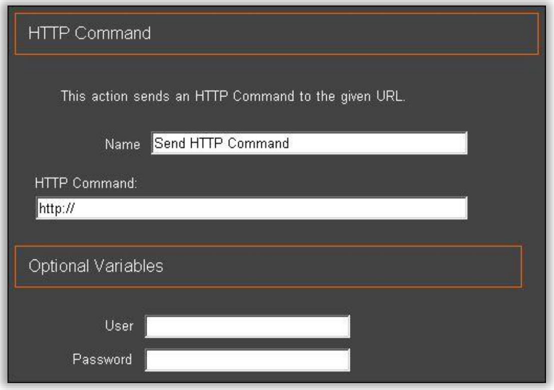
● All users connected to this server.

○ Selected user(s) listed below:

○ Selected group(s) listed below:

HTTP Command is designed to work with certain camera and hardware manufacturers to issue commands to those devices using specific Hypertext Transfer Protocol.

Some of these devices have the capability to receive an HTTP command from remote locations to modify the functional use of different portions of its internal software.



HTTP Command

This action sends an HTTP Command to the given URL.

Name: Send HTTP Command

HTTP Command:

http://

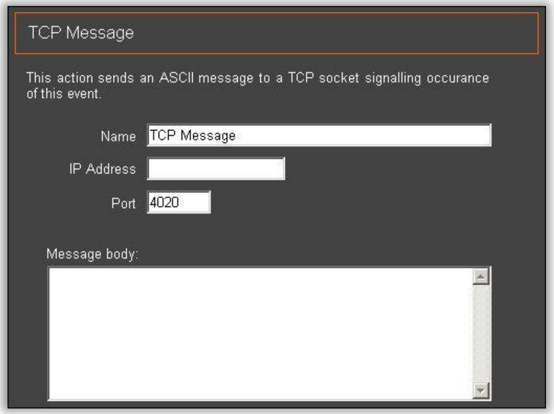
Optional Variables

User:

Password:

TCP Message gives the user the ability to send a pre-written message to a remote computer and specific port where the sent message is intercepted at the remote receiving end.

This can be read by the Administrator of the receiving computer and utilized for enhanced security purposes.



TCP Message

This action sends an ASCII message to a TCP socket signalling occurance of this event.

Name: TCP Message

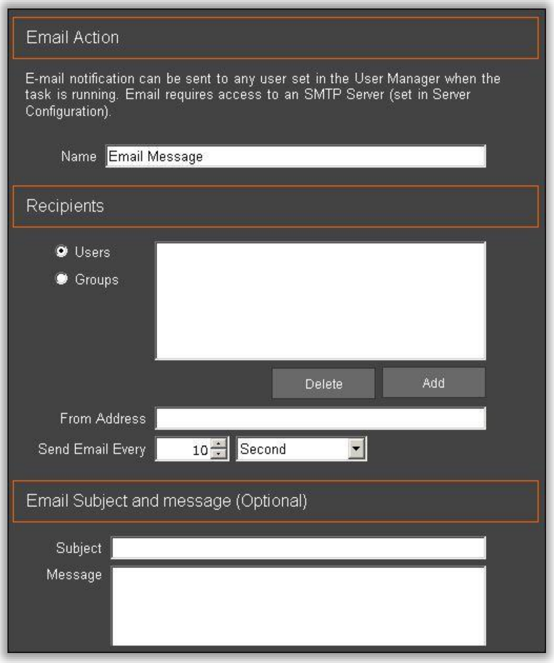
IP Address:

Port: 4020

Message body:

Email messages can be sent after the IP Server has been properly configured for using SMTP Services with an email provider.

This feature will send specific information to a group of users of a specific user. The message and subject line can be customized to accommodate the needs of an email filter, if necessary.



Email Action

E-mail notification can be sent to any user set in the User Manager when the task is running. Email requires access to an SMTP Server (set in Server Configuration).

Name: Email Message

Recipients

● Users
○ Groups

From Address:

Send Email Every: 10 Second

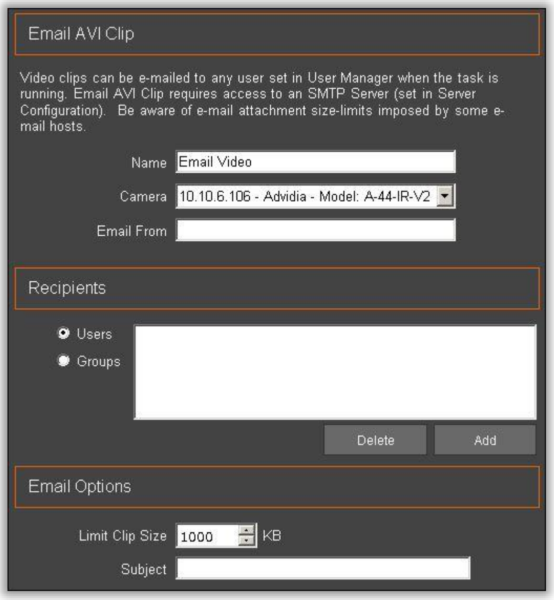
Email Subject and message (Optional)

Subject:

Message:

Email AVI clip allows the IP Server Administrator to capture a certain specified amount of recorded motion and clip it into a file of desired file size chosen by the administrator.

It will then email that file to a user, user group, or all registered users so that the triggered event details can be observed and recorded at a convenient location.



Email AVI Clip

Video clips can be e-mailed to any user set in User Manager when the task is running. Email AVI Clip requires access to an SMTP Server (set in Server Configuration). Be aware of e-mail attachment size-limits imposed by some e-mail hosts.

Name: Email Video

Camera: 10.10.6.106 - Advidia - Model: A-44-IR-V2

Email From:

Recipients

● Users
○ Groups

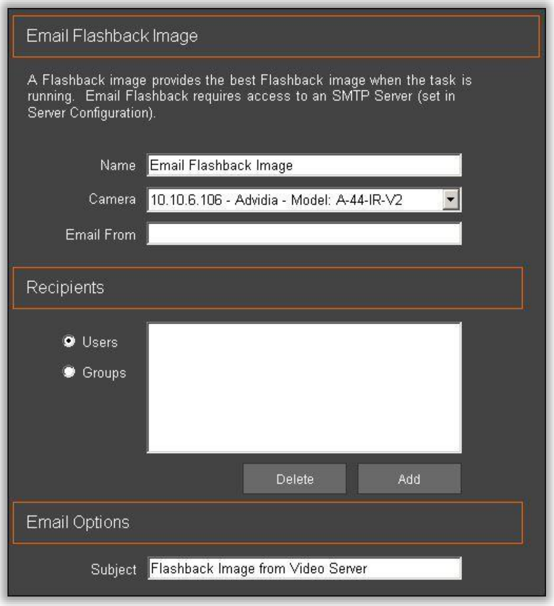
Email Options

Limit Clip Size: 1000 KB

Subject:

Email Flashback Image gives the administrator the ability to send an email with an image at the beginning of a series of motion events which is a series of framed snapshots combined to give a range of motion over time, without the need to review the full video file.

Associate this feature with only a specific camera, as it cannot be used to select multiple cameras. This is most commonly associated with motion event triggers.



Email Flashback Image

A Flashback image provides the best Flashback image when the task is running. Email Flashback requires access to an SMTP Server (set in Server Configuration).

Name: Email Flashback Image

Camera: 10.10.6.106 - Advidia - Model: A-44-IR-V2

Email From:

Recipients

● Users
○ Groups

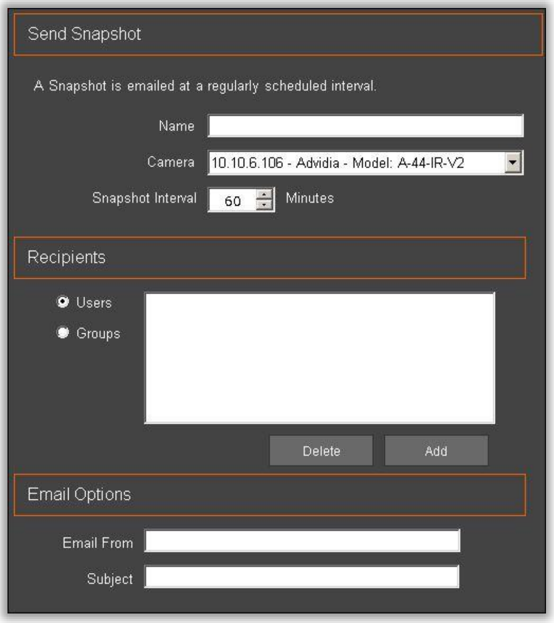
Email Options

Subject: Flashback Image from Video Server

Send Snapshot is used to send a single image file at the start of a motion event to a specific email address.

It can send a single image capture at specific intervals so that it is easy to determine a point in time when something that appears to normally be static, has moved.

This is most commonly used with motion event triggers.



Send Snapshot

A Snapshot is emailed at a regularly scheduled interval.

Name:

Camera: 10.10.6.106 - Advidia - Model: A-44-IR-V2

Snapshot Interval: 60 Minutes

Recipients

● Users
○ Groups

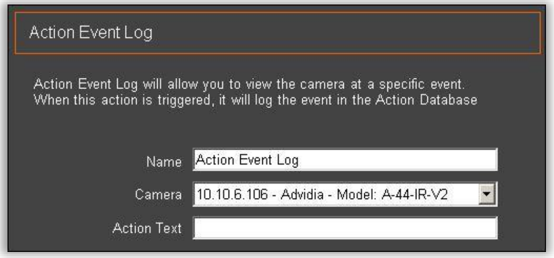
Email Options

Email From:

Subject:

Action Event Log is used with motion event triggers, but it can also be used with any trigger where logging is desired for specific information.

When used, it will place a specific message into the log notes.



Action Event Log

Action Event Log will allow you to view the camera at a specific event. When this action is triggered, it will log the event in the Action Database

Name: Action Event Log

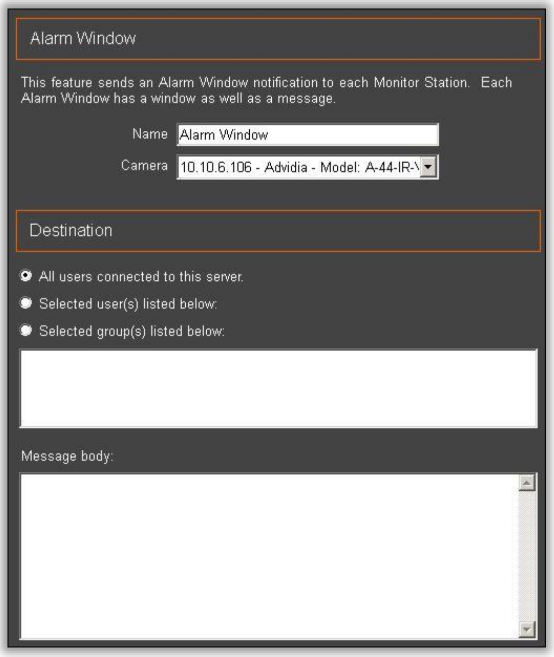
Camera: 10.10.6.106 - Advidia - Model: A-44-IR-V2

Action Text:

Alarm Window sends a notification to each person logged in to VI MonitorPlus and is actively using the client.
Alarm Windows can be used to alert security guards very quickly of any motion in an area, by displaying a specific camera where motion is detected.

The ability to designate specific users or groups is available.

The second criteria are the **Message Body**, which can list the name of the camera, location of where the camera is, or anything desired to be added for the intended purpose of notification and instruction.



Alarm Window

This feature sends an Alarm Window notification to each Monitor Station. Each Alarm Window has a window as well as a message.

Name: Alarm Window

Camera: 10.10.6.106 - Advidia - Model: A-44-IR-\

Destination

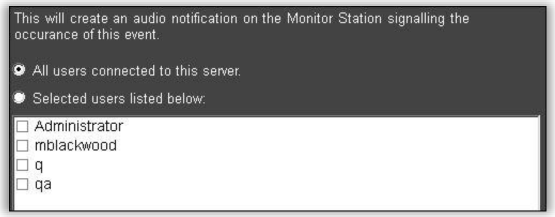
● All users connected to this server.

○ Selected user(s) listed below:

○ Selected group(s) listed below:

Message body:

Audio Alert will cause a chime to sound on ALL VI MonitorPlus clients logged into an IP Server, or the ability to specify a specific end user for administrative purposes. This is most commonly used with the user Login Trigger.



This will create an audio notification on the Monitor Station signalling the occurance of this event.

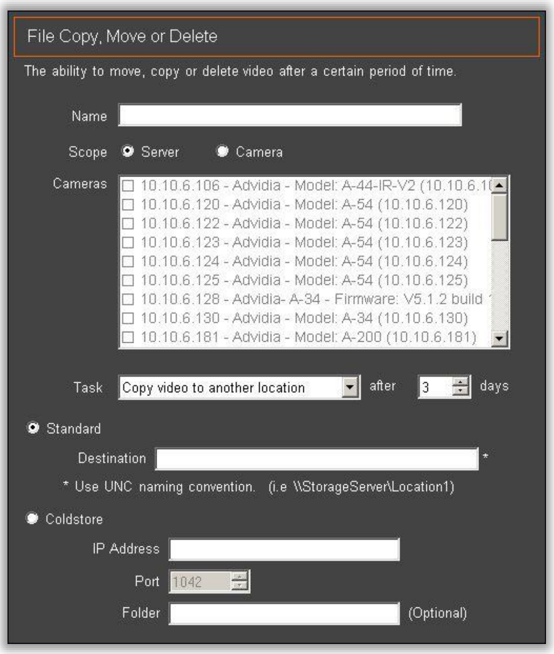
● All users connected to this server.

○ Selected users listed below:

□ Administrator
□ mblackwood
□ q
□ qa

File Manipulation is used to move video files from one location to another after a specific time-period has passed.

This is most useful as a maintenance tool enhancement when used in conjunction with a NAS drive or another backup device.



File Copy, Move or Delete

The ability to move, copy or delete video after a certain period of time.

Name

Scope ● Server ○ Camera

Cameras
□ 10.10.6.106 - Advidia - Model: A-44-IR-V2 (10.10.6.1(
□ 10.10.6.120 - Advidia - Model: A-54 (10.10.6.120)
□ 10.10.6.122 - Advidia - Model: A-54 (10.10.6.122)
□ 10.10.6.123 - Advidia - Model: A-54 (10.10.6.123)
□ 10.10.6.124 - Advidia - Model: A-54 (10.10.6.124)
□ 10.10.6.125 - Advidia - Model: A-54 (10.10.6.125)
□ 10.10.6.128 - Advidia- A-34 - Firmware: V5.1.2 build
□ 10.10.6.130 - Advidia - Model: A-34 (10.10.6.130)
□ 10.10.6.181 - Advidia - Model: A-200 (10.10.6.181)

Task: Copy video to another location after 3 days

● Standard

Destination *

* Use UNC naming convention. (i.e \\StorageServer\Location1)

○ Coldstore

IP Address

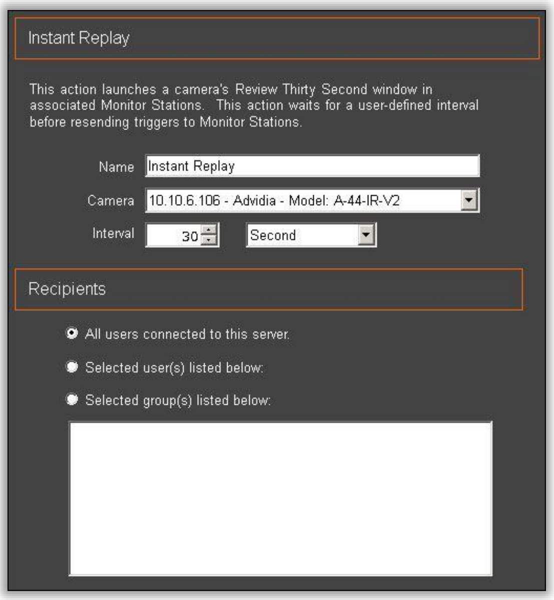
Port 1042

Folder (Optional)

Instant Replay is most commonly used with motion event detection for desired cameras.

It can be used to bring to the immediate attention of security or police officers' motion that is occurring It shows the last 30 seconds of recorded motion event.

It requires that a user, a group of users, or all users be selected.



Instant Replay

This action launches a camera's Review Thirty Second window in associated Monitor Stations. This action waits for a user-defined interval before resending triggers to Monitor Stations.

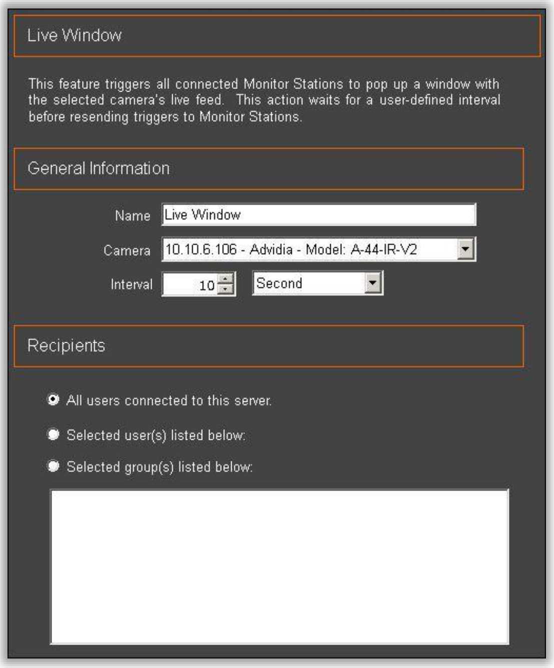
Name: Instant Replay
Camera: 10.10.6.106 - Advidia - Model: A-44-IR-V2
Interval: 30 Second

Recipients

● All users connected to this server.
○ Selected user(s) listed below:
○ Selected group(s) listed below:

Live Window will pop-up a display window containing live camera feed for a specific camera.

It can be used to bring the attention to the center of the VI MonitorPlus window for viewing of an event that may need immediate action taken.



Live Window

This feature triggers all connected Monitor Stations to pop up a window with the selected camera's live feed. This action waits for a user-defined interval before resending triggers to Monitor Stations.

General Information

Name: Live Window
Camera: 10.10.6.106 - Advidia - Model: A-44-IR-V2
Interval: 10 Second

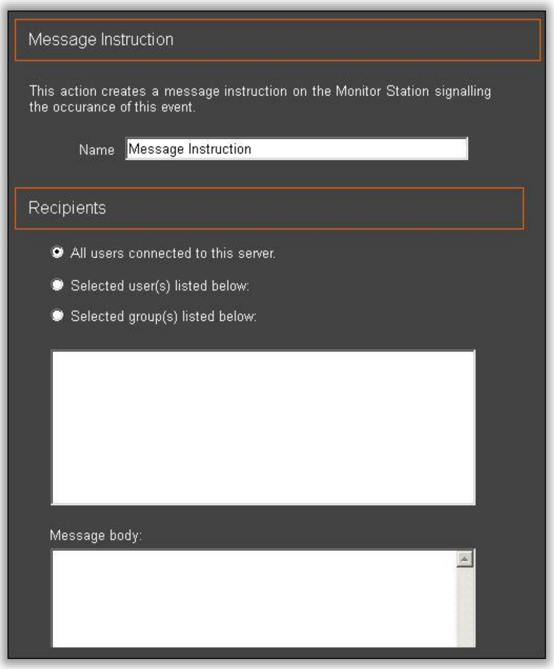
Recipients

● All users connected to this server.
○ Selected user(s) listed below:
○ Selected group(s) listed below:

Message Instruction is used to send specific messages after a trigger event is fired.

It can be used with Access Control, LPR, Motion Events, Camera Outages, or any other trigger.

It appears within VI MonitorPlus as a pop-up window and can be closed by the receiving user.



Message Instruction

This action creates a message instruction on the Monitor Station signalling the occurance of this event.

Name: Message Instruction

Recipients

● All users connected to this server.

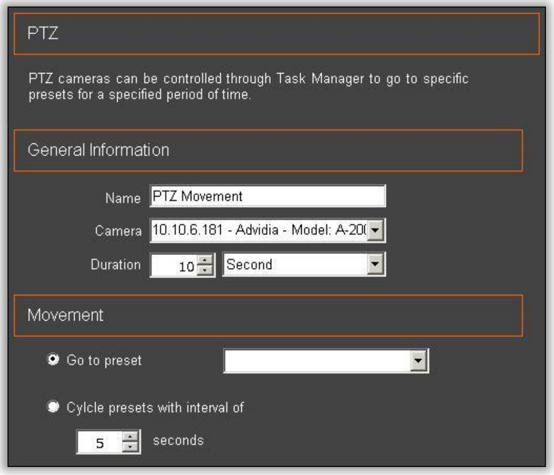
○ Selected user(s) listed below:

○ Selected group(s) listed below:

Message body:

Move PTZ Camera, once triggered, Move PTZ Camera can force a PTZ camera to return to a specific, pre-defined, focal point.

When used with Access Control Door access, a PTZ camera located near that door can be forced to turn and capture a headshot of the individual triggering the door access code.



PTZ

PTZ cameras can be controlled through Task Manager to go to specific presets for a specified period of time.

General Information

Name: PTZ Movement

Camera: 10.10.6.181 - Advidia - Model: A-20(

Duration: 10 Second

Movement

● Go to preset

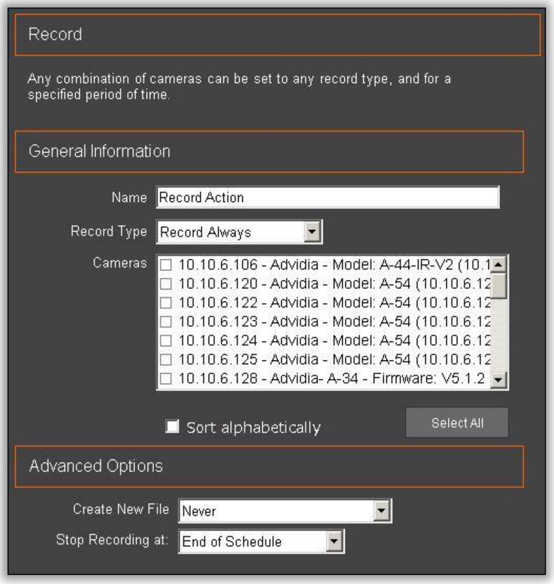
○ Cylcle presets with interval of

5 seconds

Record, when triggered, can force a camera to record if it is normally not set to record anything at all, or has another restriction imposed upon it.

The creation of a new file can be forced, and other limitations can be imposed based on the needs of the rule creator.

This action is used with a wide number of trigger events and can have a variety of results based upon the needs of the rule creator.



Record

Any combination of cameras can be set to any record type, and for a specified period of time.

General Information

Name: Record Action

Record Type: Record Always

Cameras:
- □ 10.10.6.106 - Advidia - Model: A-44-IR-V2 (10.1
- □ 10.10.6.120 - Advidia - Model: A-54 (10.10.6.12
- □ 10.10.6.122 - Advidia - Model: A-54 (10.10.6.12
- □ 10.10.6.123 - Advidia - Model: A-54 (10.10.6.12
- □ 10.10.6.124 - Advidia - Model: A-54 (10.10.6.12
- □ 10.10.6.125 - Advidia - Model: A-54 (10.10.6.12
- □ 10.10.6.128 - Advidia- A-34 - Firmware: V5.1.2

□ Sort alphabetically

Advanced Options

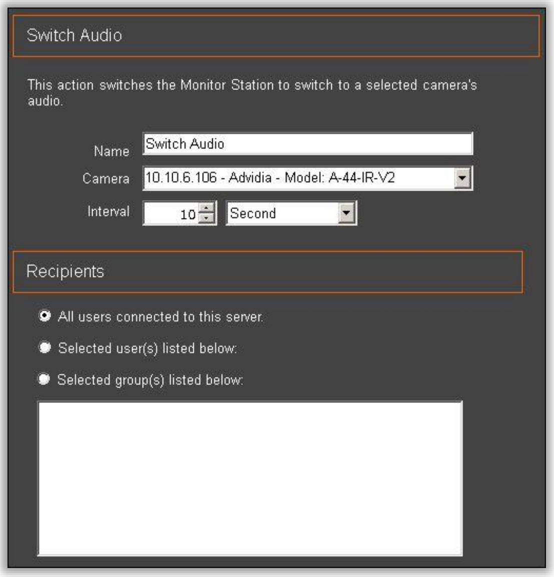
Create New File: Never

Stop Recording at: End of Schedule

Switch Audio allows the user to listen to only a single audio source.

If a pre-configured trigger activates this action, the resulting effect is that a pop-up window appears with the specific camera which is streaming audio and all other audio sources are muted.

This will allow the user to isolate video and audio to a specific source and give cause to action if necessary.



Switch Audio

This action switches the Monitor Station to switch to a selected camera's audio.

Name: Switch Audio
Camera: 10.10.6.106 - Advidia - Model: A-44-IR-V2
Interval: 10 Second

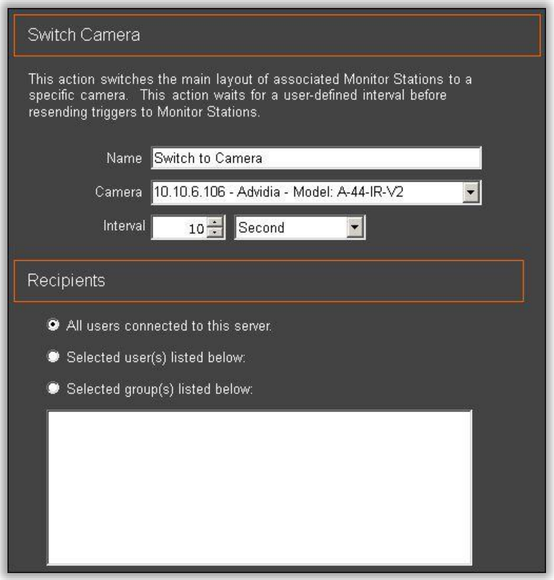
Recipients

◉ All users connected to this server.
○ Selected user(s) listed below:
○ Selected group(s) listed below:

Switch Camera functions in a way that will add another way to bring immediate attention to a specific camera where motion is occurring.

This feature will return to the view of whatever image was in place prior to its injection on the screen.

This is good for random spot checks on various cameras, so that a completely random timing interval can be used based on the trigger of a motion event



Switch Camera

This action switches the main layout of associated Monitor Stations to a specific camera. This action waits for a user-defined interval before resending triggers to Monitor Stations.

Name: Switch to Camera
Camera: 10.10.6.106 - Advidia - Model: A-44-IR-V2
Interval: 10 Second

Recipients

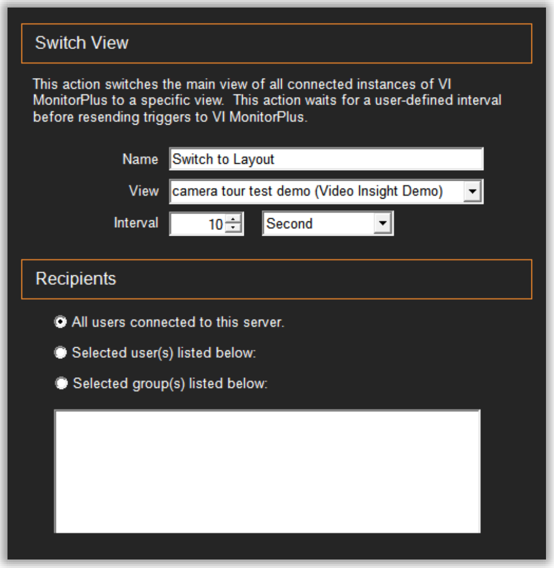
◉ All users connected to this server.
○ Selected user(s) listed below:
○ Selected group(s) listed below:

Switch View can force users that are logged in to use a predefined View**.**

A specific time interval can be assigned to that View.

This is most useful with **Access Control**, **LPR**, and motion event triggers.

No trigger event is required for use with the **Switch View**.



Switch View

This action switches the main view of all connected instances of VI MonitorPlus to a specific view. This action waits for a user-defined interval before resending triggers to VI MonitorPlus.

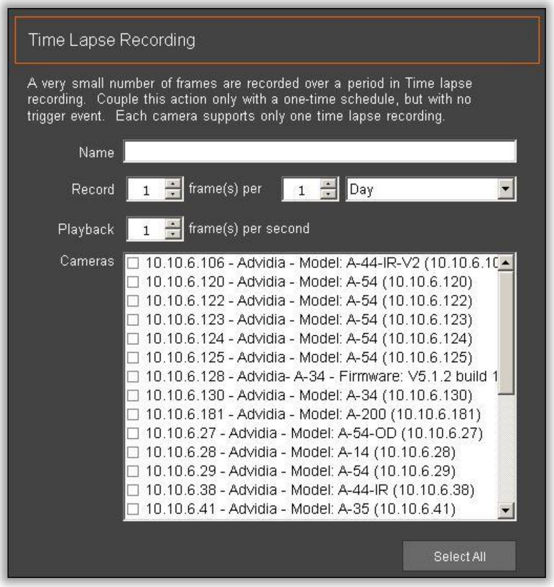
Name: Switch to Layout
View: camera tour test demo (Video Insight Demo)
Interval: 10 Second

Recipients

◉ All users connected to this server.
○ Selected user(s) listed below:
○ Selected group(s) listed below:

Time Lapse Recording causes a camera to take a single-frame snapshot at desired intervals for any designated camera or cameras.

The video output playback frame rate can be adjusted to help manage how quickly playback appears.



A very small number of frames are recorded over a period in Time lapse recording. Couple this action only with a one-time schedule, but with no trigger event. Each camera supports only one time lapse recording.

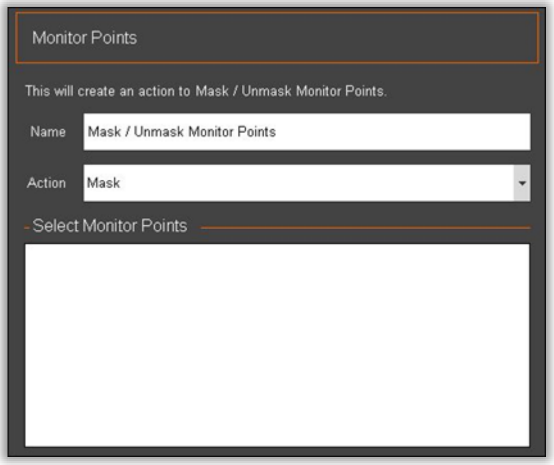
Name

Record 1 frame(s) per 1 Day

Playback 1 frame(s) per second

Cameras
□ 10.10.6.106 - Advidia - Model: A-44-IR-V2 (10.10.6.10
□ 10.10.6.120 - Advidia - Model: A-54 (10.10.6.120)
□ 10.10.6.122 - Advidia - Model: A-54 (10.10.6.122)
□ 10.10.6.123 - Advidia - Model: A-54 (10.10.6.123)
□ 10.10.6.124 - Advidia - Model: A-54 (10.10.6.124)
□ 10.10.6.125 - Advidia - Model: A-54 (10.10.6.125)
□ 10.10.6.128 - Advidia- A-34 - Firmware: V5.1.2 build 1
□ 10.10.6.130 - Advidia - Model: A-34 (10.10.6.130)
□ 10.10.6.181 - Advidia - Model: A-200 (10.10.6.181)
□ 10.10.6.27 - Advidia - Model: A-54-OD (10.10.6.27)
□ 10.10.6.28 - Advidia - Model: A-14 (10.10.6.28)
□ 10.10.6.29 - Advidia - Model: A-54 (10.10.6.29)
□ 10.10.6.38 - Advidia - Model: A-44-IR (10.10.6.38)
□ 10.10.6.41 - Advidia - Model: A-35 (10.10.6.41)

Monitor Points, when used with certain Access Control input devices, can be triggered to Mask or Unmask a specific function of a device.
It is an on-off switch for a two-way input device.
Depending on how the device is configured, Masking the device will force it to do the opposite of whatever configuration it holds.
Unmasking the device will revert it to the original state.
Most commonly used with schedules and Access Control triggers.



This will create an action to Mask / Unmask Monitor Points.

Name Mask / Unmask Monitor Points

Action Mask

(7D) BEST PRACTICES

When using the Rules Manager, keep the following aspects in mind to help achieving the best end results in customizing this software.

The default for rules created within the rules manager is to run **always**. Using the schedule will impact certain rules in a way that may not be intended.

- **Keep it simple** - When creating a new rule, keep things simple so that, in the event of a problem, it can be resolved easily.
- **Document, Document, Document** - When a rule is created, keep notes as to WHY the rule was created, WHICH steps the intended rule is supposed to perform, WHAT software and hardware devices are supposed to be affected, and HOW it is expected to function when it is run.
- **Create only one rule at a time** - During the creation of a rule, let it run a full course to verify that it is working as it is intended to function. Once that rule has successfully run its full course, then add a second rule. Let it runs its course completely. Verify that both rules are still functioning as desired. Remember rules two and three, then add a fourth rule.
- **Multiple simple rules can create a complex outcome** - When viewing rules as a step-by-step process, the creation of very complex rules can result in a variety of desired outcomes. Each rule that is created requires a trigger and an action. Actions can be used as trigger events when used in a sequence of rules.
- **Troubleshooting** - If a rule does not function as desired, disable each rule one-at-a-time to eliminate the possibility of a rule conflict. Sometimes two rules will fail logically, causing a conflict for one or more subsequent rules. Concentrate on the process and flow of the rule and verify that nothing is wrong with the rule syntax due to a maligned.

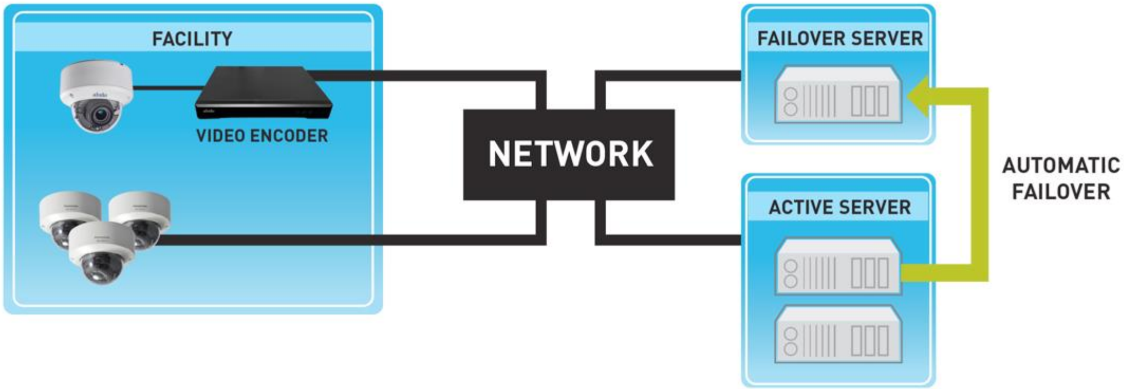
3.4.E Failover Server

(1) INTRODUCTION

VI IP Server supports **Automated Failover** at no additional software cost. When utilizing the **Video Insight Shared Database configuration**, a physical or virtual server can be designated as a Failover. This server will monitor the other servers and inherit the cameras of a failed one.

For example, if there are 5 servers with one designated as Failover, when one of the 4 stops writing information to the SQL database, the Failover Server will assume the role of the failed one and all camera traffic will now be associated with that server. Once the failed server is put back into service, the Failover Server will move the cameras back to their original location.

(2) FAILOVER OVERVIEW



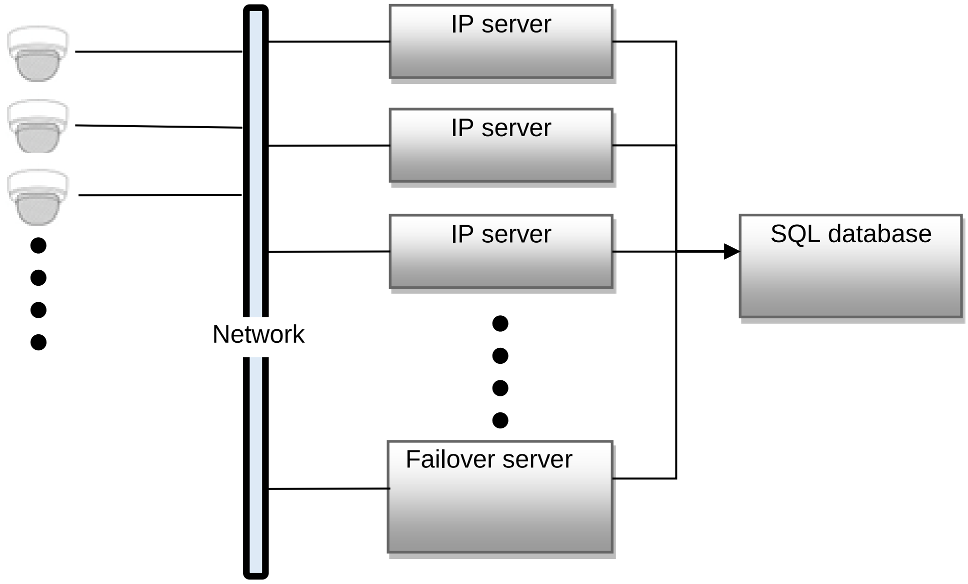
When utilizing a Failover Server, a shared SQL database must be configured. Note that a Failover Server should work only for one server as an alternative. Thus, after activating a Failover Server, a down server will be required to recover promptly so that system can be returned to normal operation.

(3) REQUIREMENTS

To use the Failover Server feature, the following criteria must be met:

- Two functional IP Servers with the same hardware configuration, or a secondary server with greater storage capacity. (Virtualized systems can also be used. It is recommended that the virtualized servers are on two different pieces of hardware.)
- Shared SQL Database installation; see **IP Server installation with an existing SQL installation**.
- At least one license and a serial number or activation key for each server.

(4) SYSTEM STRUCTURE



(4A) RECORDING DURING FAILOVER PROCESS

If a Failover Server has its own storage, a video recorded by it will not be moved to an Active Server after recovering a failed one. Thus, having the same hardware configuration is required since a server cluster feature is used.

In case of using three or more servers, **shared storage is also recommended** so that all recorded videos during Failover can be accessed by VI MonitorPlus after recovering.

(5) ACTIVATION SEQUENCE OF A FAILOVER SERVER

The example below provides a basic sequence for activating a Failover Server. The value of interval for checking whether a server is alive is configurable (See the **Technical Support Knowledge Database** for details).

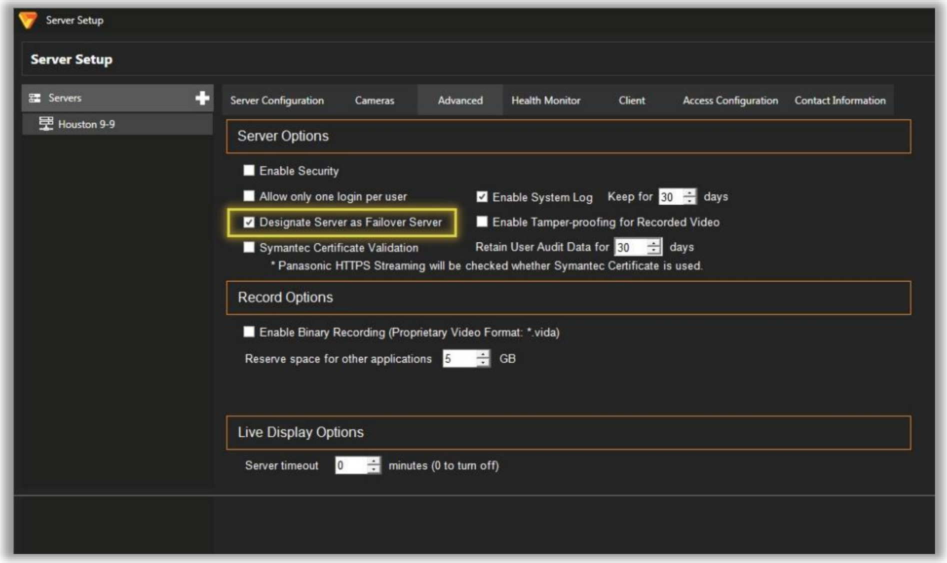
1. The minimum amount of time for switching to the failover server is 11 seconds. During that time, video recording will not occur. This means that there will be a gap in the coverage for recorded video files which will not ever be accessible. The default time for failover to occur is set at 5 minutes by recommendation.
2. **SQL Server data recovery** - is not recovered if a shared SQL DB is not used.

NOTE - If a shared SQL DB is used for multiple IP Servers in a system, recorded data before and after switching over happens can be monitored and managed seamlessly by VI MonitorPlus.

1) A single failover server in a system

2) After an active server recovers, a backup server will transfer control back to the primary IP Server.

(6) DESIGNATE AN IP SERVER AS A FAILOVER SERVER



Server Options

- □ Enable Security
- □ Allow only one login per user
- ☑ Designate Server as Failover Server
- □ Symantec Certificate Validation
- ☑ Enable System Log Keep for 30 days
- □ Enable Tamper-proofing for Recorded Video
- Retain User Audit Data for 30 days

* Panasonic HTTPS Streaming will be checked whether Symantec Certificate is used.

Record Options

- □ Enable Binary Recording (Proprietary Video Format: *.vida)
- Reserve space for other applications 5 GB

Live Display Options

- Server timeout 0 minutes (0 to turn off)

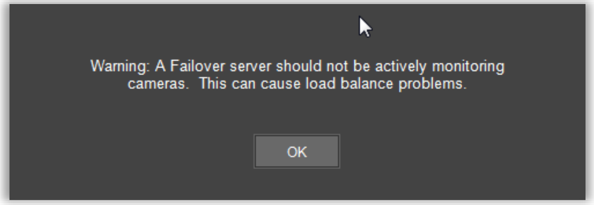
On **VI MonitorPlus**, click **Administration** > **Servers** > **Setup and Configuration** from the Main Menu.

Select the desired Failover Server from the Left Navigation pane.

Select the **Advanced** tab.

Check the **Designate Server as Failover Server** box.

Avoid selecting a server that is actively monitoring cameras.


Warning: A Failover server should not be actively monitoring cameras. This can cause load balance problems.

During an IP Server failure, the transfer of the video recording functionality to the Failover Server will take **5 to10 minutes**.

Upon recovery from the outage, video files recorded on the Failover Server ***will not*** be transferred to the original IP Server.

The Failover Server will be accessed via VI MonitorPlus while the main IP Server is down..

Once the Failover Server is accessed by VI MonitorPlus, it will show all cameras and images from the offline server. Recording will continue onto the Failover Server or a previously configured Network Share location, if available.

NOTE - It is possible to 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.

.

4. VI MONITORPLUS

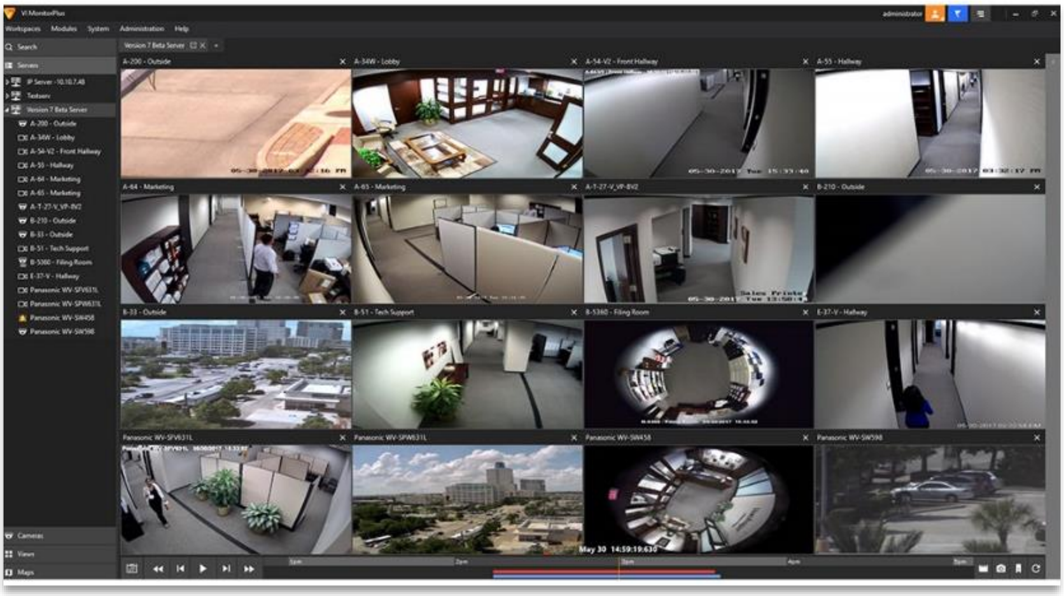
4.1 ACCESS AND LOG IN

Open **VI MonitorPlus** by double-clicking the corresponding **desktop icon** for the application.

The **Login window** will be displayed).

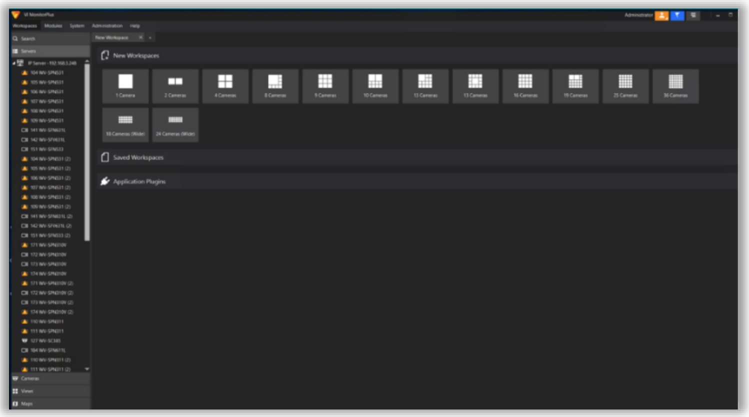
NOTE – For more information and details on ***Logging into VI MonitorPlus***, refer to: Logging In.

VI MonitorPlus is the client VMS Application that has three core functions: Live Monitoring, Viewing History and Centralized Management for configuring and optimization of all IP Servers connected to it.



4.2 F11 - FULL SCREEN MODE

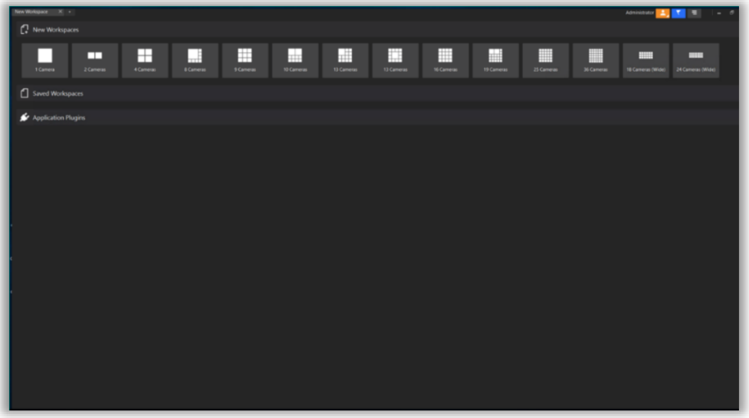
VI MonitorPlus is designed to work in many environments, while following the guidelines for an easily customized viewing arrangement.



Normal view

The use of the **F11** key on most keyboards will force the application into ***Full Screen mode***. To exit Full Screen mode, use the Esc button, or press F11 a second time.

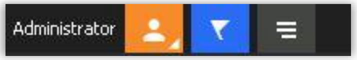
This will force the program window to resize itself and provide the user with quick access to the desktop background.



Full Screen view

4.3 MENU BAR OPTIONS

The new VI MonitorPlus user interface has undergone some major redesign because of important feedback from our favorite clients, industry members, and test groups. As a result, VI MonitorPlus has been reshaped to make navigation and control as simple and fluid as possible.

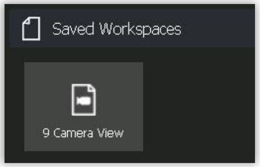
	At the top right-hand side of the screen appears a new Menu Bar.
👤	This icon, when selected, allows the user to logout of VI MonitorPlus.
▼	The flag icon provides the user with quick access to downloaded files, notifications, and recent changes made to the system.
≡	This icon allows quick access to any currently configured rules once they have been configured within **Rules Manager.**

4.4 TAB: WORKSPACES

Workspaces are individual pages, like modern browsers, that allow customizing live and/or recorded video views.

The default Workspace view can optionally be modified to facilitate the access to specific cameras at critical times within large areas to monitor.

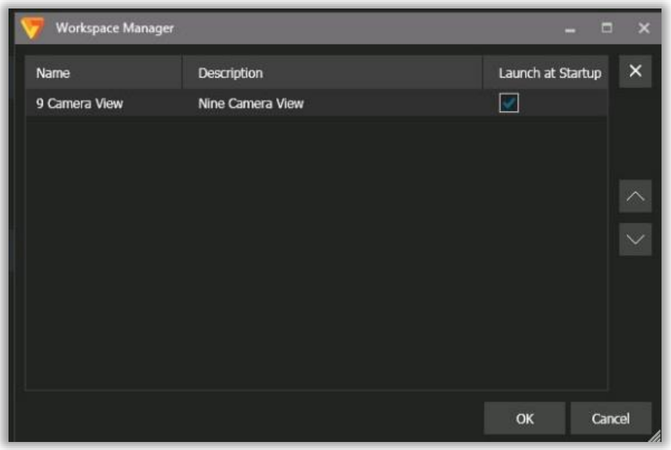
4.4.A Save



Open opens a previously saved Workspace within VI MonitorPlus.

Save will allow the user to arrange a series of camera views and save the workspace for easy access at a later time.

4.4.B Manage



Name	Description	Launch at Startup
9 Camera View	Nine Camera View	☑

Manage - opens a new window, displaying a list of previously saved Workspace views. This feature allows to organize the order of appearance for recently created Workspaces. The user can also optionally select a specific Workspace manager to start at the launch of VI MonitorPlus.

New Workspace - Allows the user to create a new workspace for customization.

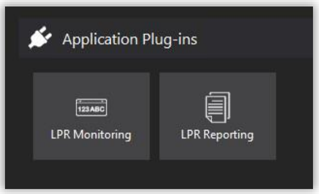
Close All - Closes all opened workspaces.

.

4.4.C Application Plug-ins

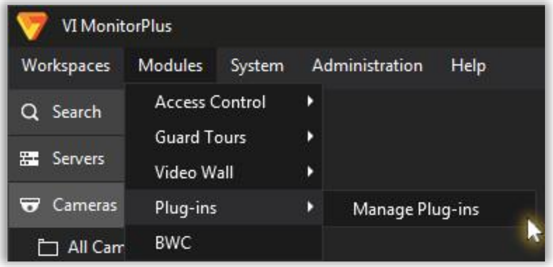
VI MonitorPlus allows functionality to install additional Application Plug-ins. Whenever available, the Plug-ins can be executed from the “Application Plug-ins” section in the new Workspace.

This function ***requires IP Server 7.2 or later***.

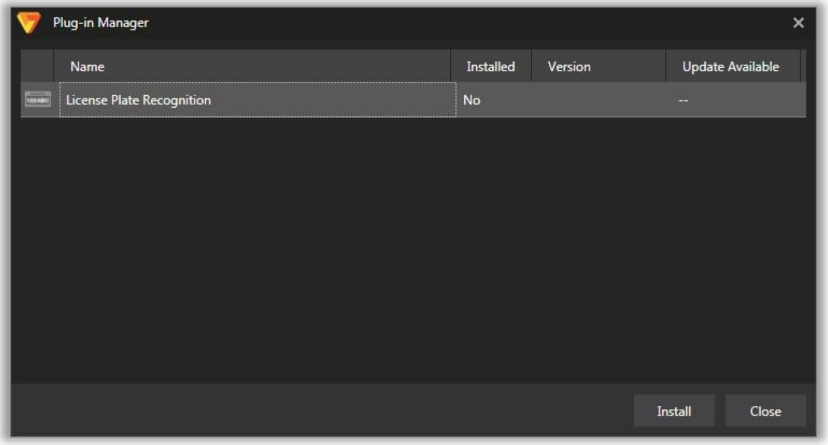


(1) INSTALLING A NEW PLUG-IN

Select **Modules** from the main menu and select **Plug-ins**.



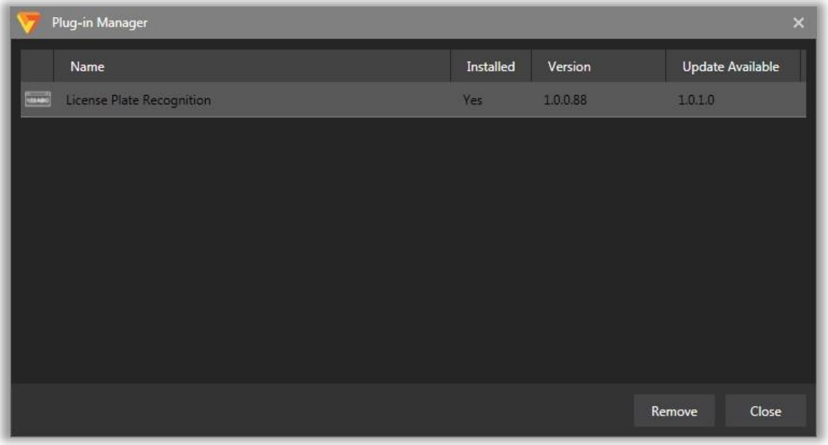
Select the **Plug-in** to add from the list, then click **Install**.



Name	Installed	Version	Update Available
License Plate Recognition	No		--

(2) UNINSTALLING A PLUG-IN

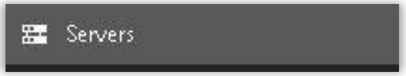
From the Plug-in Manager, select the **Plug-in** to uninstall from the list, then click **Remove**.



Name	Installed	Version	Update Available
License Plate Recognition	Yes	1.0.0.88	1.0.1.0

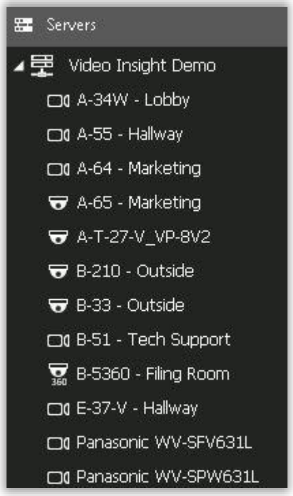
4.5 LEFT HAND MENU ICONS

4.5.A Servers

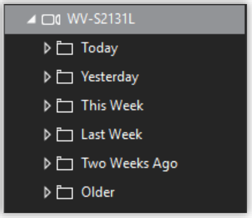


Server View provides the Administrator with the capability to view all configured servers and their corresponding cameras in one convenient scrollable menu bar.

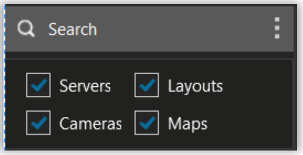
NOTE - To display all servers and cameras upon application launch, you can configure the setting to "***Start with Expanded Servers***" listed under **System** > **Options** > **Startup**. The Server View will also reflect the changes made by the user of Resource Groups, where changes have been made.



- Expand the Server by selecting the triangle shape, found on the left of the server name. This action expands the visible area, displaying the names of all cameras associated and controlled by that specific server.
- Applying a double-click to a camera will display the recorded video folder, by date, for that camera. Where "Show video files folders" has been activated in Application Controls, below.



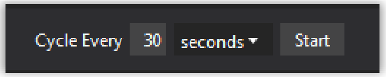
- Selecting the date under the camera view will display all files for the camera when file view has been enabled using Application Controls.
- To collapse the view, click the triangle icon, directly left of the server.



Search

The search option is a reduction filter, which isolates servers to display the camera being searched for on any shared database. Clicking on the three vertical lines exposes four defaulted criteria that a search will search through.

If any of the options is not applicable, unchecking it will help aid in creating a faster search, but may reduce the effectiveness of the search being conducted.

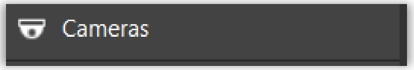


Cycle Views

To cycle or page through cameras in a specific View, select and click the Server in the left tree. Use the Cycle Every option at the base of the workspace to specify a cycle time. This feature will update the cameras, keeping the View count locked. For example, if 8-camera view is selected, you will receive 8 new sets of cameras at the time specified after 30 seconds.

4.5.B Cameras

This view displays all cameras listed on all servers in order grouped by server, or camera groups. Click and drag functionality allows to click a specific camera, add it to a layout or workspace.



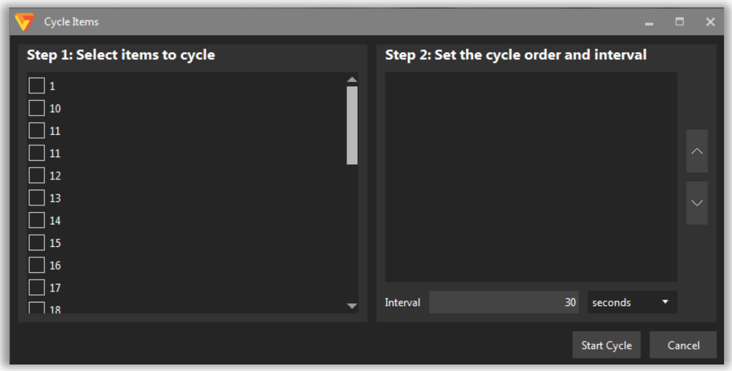
The order by which each of the servers shown on the Desktop View can be changed by clicking on **Administration** > **Servers** > **Cameras** (Add/Remove or discover cameras) and followed by manipulating the cameras into the desired order of appearance.

NOTE - Single server environments will often show the **Camera View** by default. Typing a camera name directly into the search field will conduct a search for a known camera name

4.5.C Views

This option allows the User to see all available Views within each server.

Clicking **Views** will change the current workspace layout to the selected layout. Searching for a view is possible by clicking on the magnifying glass next to the View menu title.



Step 1: Select items to cycle

□ 1
□ 10
□ 11
□ 11
□ 12
□ 13
□ 14
□ 15
□ 16
□ 17
□ 18

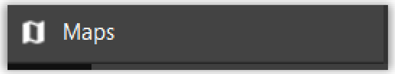
Step 2: Set the cycle order and interval

Interval 30 seconds

Clicking the ellipsis menu icon will allow you to navigate into **Cycle Custom Views** menu. Select the custom View you would like to cycle (rotate in View), set the cycle order by move the Views up and down in the order. You can also choose a time interval in which you wish to update the View in the cycle. The default setting will be selected at 30 seconds. To start the rotating Views, click **Start Cycle**.

4.5.D Maps

Facility Maps can be configured by clicking Maps found at the bottom of the left navigation menu. To find out more about **Facility Maps**, navigate to the Maps section in this document.

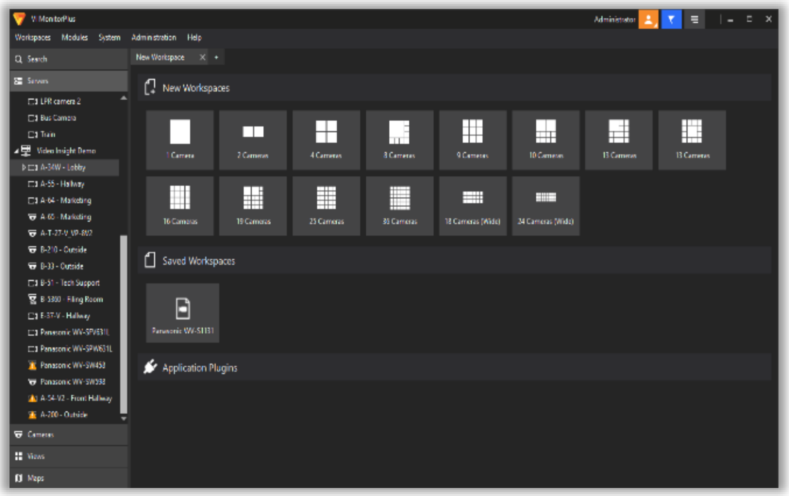


To view a facility map within a Workspace, click the map title and it will display in current workspace. This field is also capable of allowing the user to conduct a search for a saved map, is desired

4.6 LIVE VIDEO

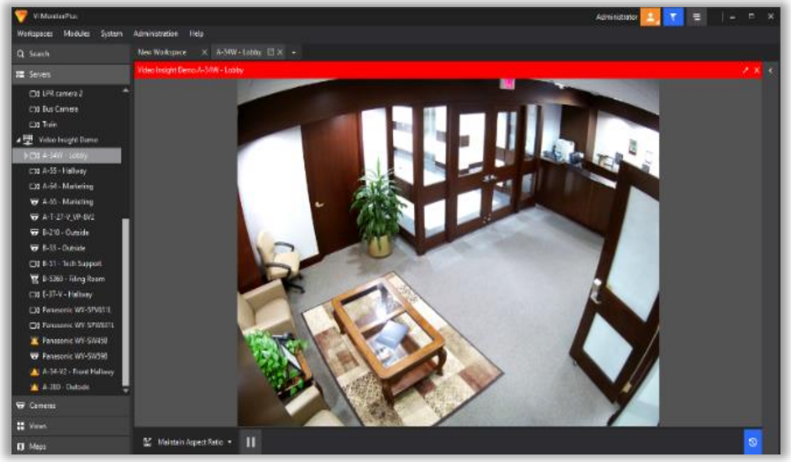
By default, VI MonitorPlus displays a list of cameras in the left navigation tree, under the name of any IP Server that VI MonitorPlus connects to.

To view Live Video, select a camera from the left tree to display a camera view. Drag the camera name into an available workspace to see a live image. To add additional cameras, click and drag a new camera to the Workspace area.

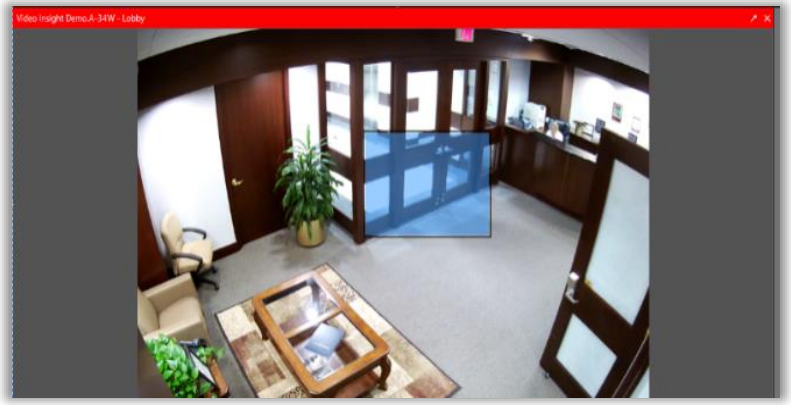


Different views can be displayed automatically by using the Cameras Views icons in the Toolbar.

Expanding the Left tree displays all the cameras connected to a specific IP Server, and that server's name.

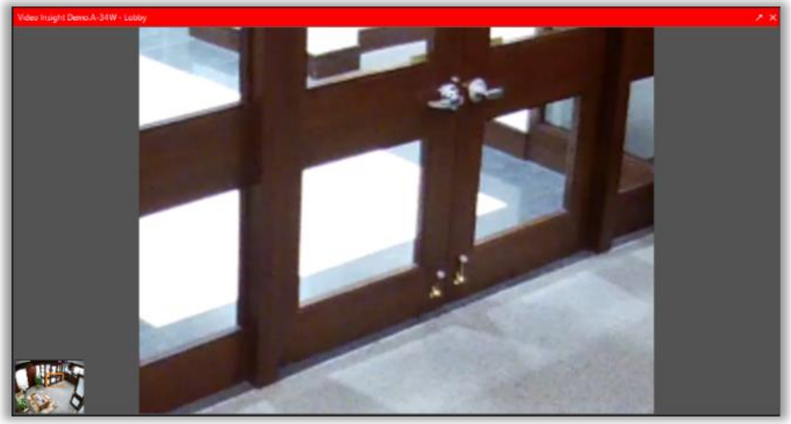


Dragging one of the cameras into a Workspace will change the Main Layout view to that camera (seen left).



While viewing the **Live Video**, applying a click-and-drag (left click and pull) across the screen results in a digital zoom.

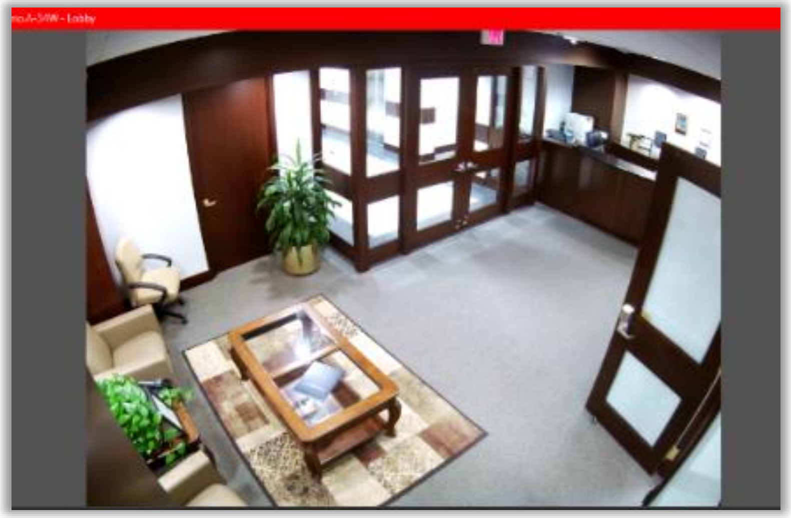
The screen will be expanded to the zoomed area. (example: left)



Alternatively, **Pan-Tilt-Zoom** (PTZ) operations can be performed by using the mouse wheel to scroll in or out of the image being displayed.

This action will zoom in from the center of the live image.

With the digital zoom, navigation around an image is possible by grabbing the orange box in the Preview Window at the bottom left or by using the **PTZ** controls in the Left tree.

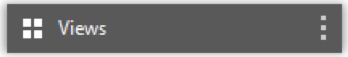


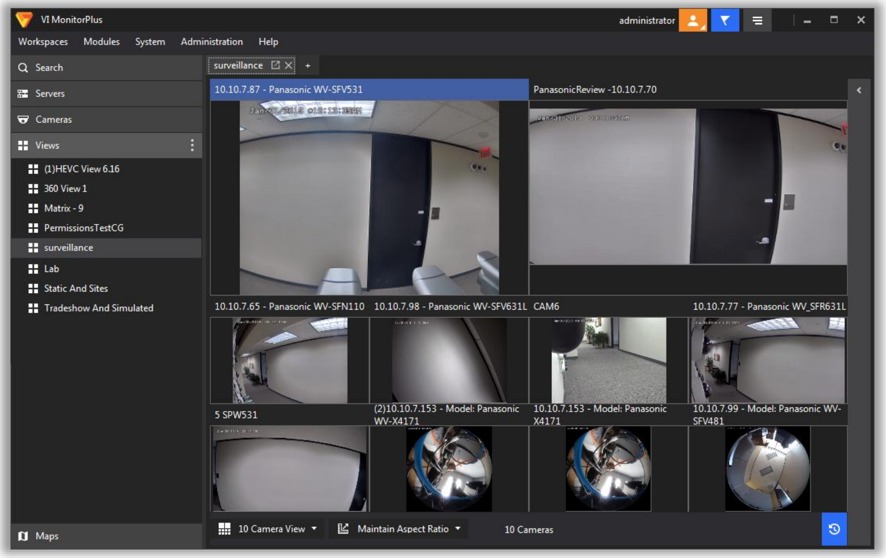
To zoom back out and see the entire image, left click and drag right to left. The digital zoom only affects the VI MonitorPlus application in use. If another user is viewing the same camera on a different computer will not be affected. This does not affect recorded video made during the time of zoom control.

4.6.A Using Views

Views are organized representations of all cameras connected to the IP Server in customizable layouts, allowing to visualize multiple live video streams simultaneously.

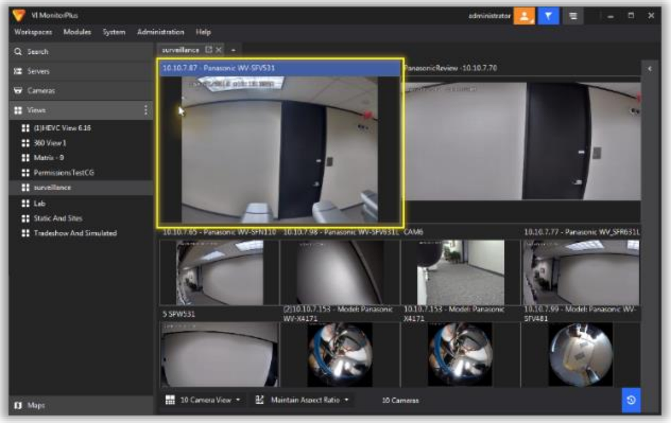
Click on “**Views**” on the Left panel to expand the list of available views; to access any View, click on the corresponding name.



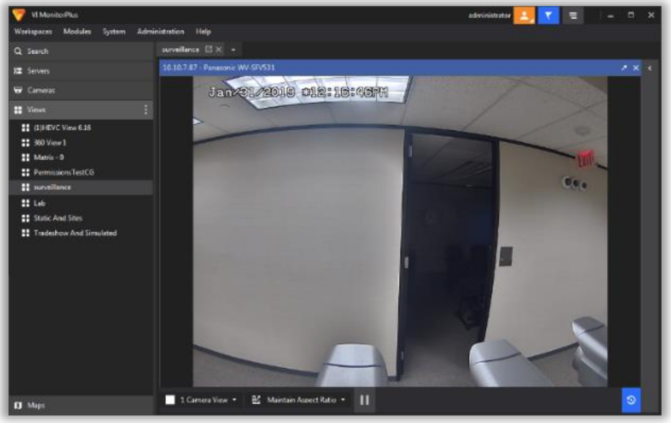

VI MonitorPlus
administrator
Workspaces
Modules
System
Administration
Help
Search
Servers
Cameras
Views
(1)HEVC View 6.16
360 View 1
Matrix - 9
PermissionsTestCG
surveillance
Lab
Static And Sites
Tradeshow And Simulated
Maps
surveillance
10.10.7.87 - Panasonic WV-SFV531
PanasonicReview -10.10.7.70
10.10.7.65 - Panasonic WV-SFN110
10.10.7.98 - Panasonic WV-SFV631L
CAM6
10.10.7.77 - Panasonic WV_SFR631L
5 SPW531
(2)10.10.7.153 - Model: Panasonic WV-X4171
10.10.7.153 - Model: Panasonic X4171
10.10.7.99 - Model: Panasonic WV-SFV481
10 Camera View
Maintain Aspect Ratio
10 Cameras

Expanding Views

To expand a single camera video from a View, **double click** directly on the desired camera frame within the View.

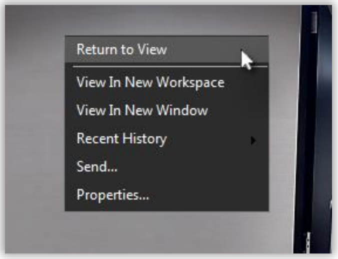


The camera feed will be displayed on top, full-size, covering all the Workspace area.



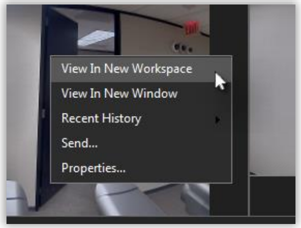
Returning to Views

To return to the View, **right click** on the video output and select “**Return to View**” from the pop-up menu.

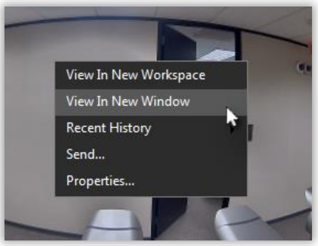


Expanded individual views of cameras can also be invoked from a View by right-clicking on the camera’s area and opening a pop-up menu.

Select “**View in new Workspace**” to create and open a new workspace with only the camera’s current live video output.

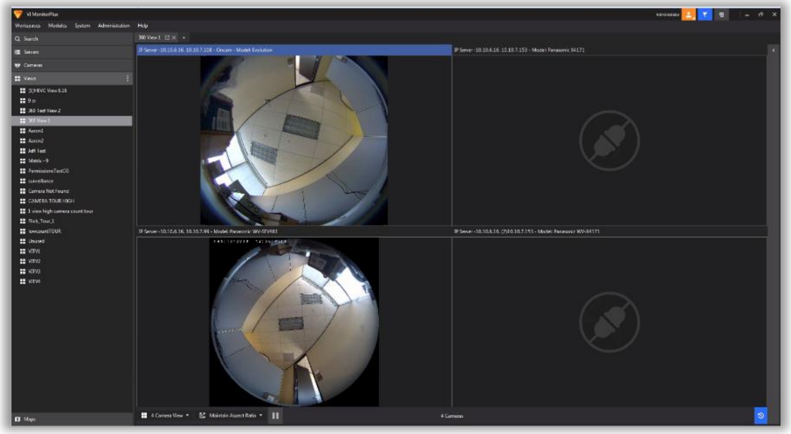


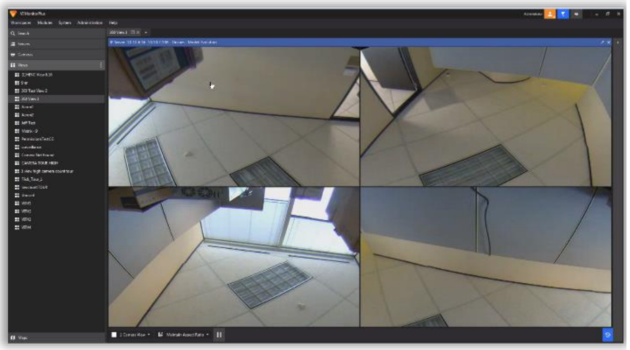
Select “**View in new Window**” to open a new VI MonitorPlus window containing only the camera’s live video.

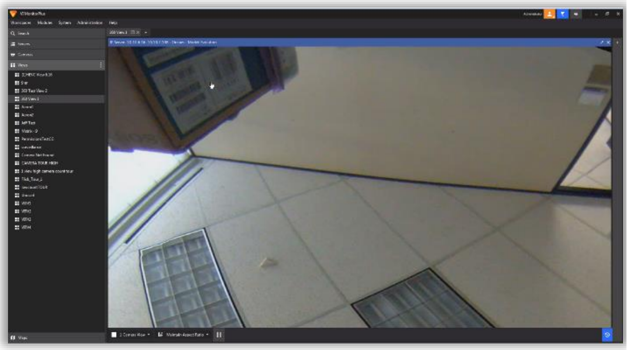


Behavior with 360° /Fisheye cameras

When viewing **360°/Fisheye** cameras from Views, double-clicking on an individual camera display will open a single quadrant view as in a single camera.

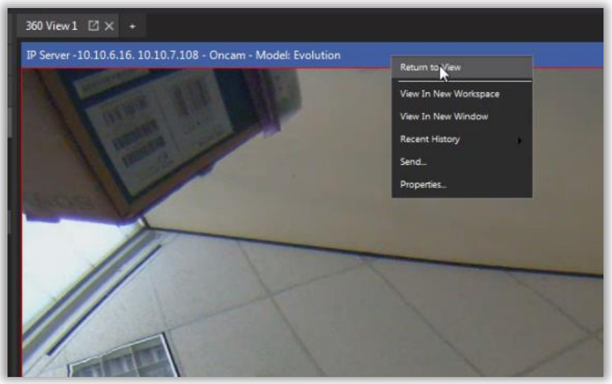






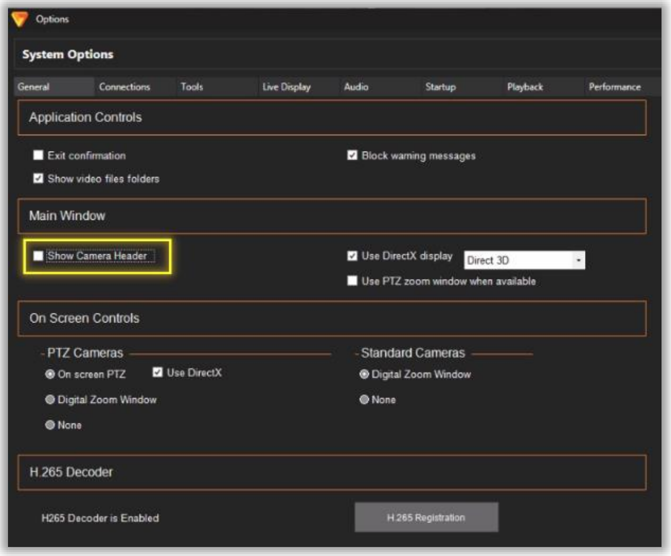
Double-clicking the quadrant again will switch back to Dewarp view.

To avoid this, **right-click** on the view and select "**Return to View**" from the pop-up menu.



Double-clicking on a 360°/Fisheye camera **view header** (the top bar with the camera name and IP address) will return to View as well.

If "**Show Camera Header**" is disabled from **System Options**, thus hiding the camera view header, use the **Right-Click/Return to View** option as explained above.



System Options

Application Controls

- □ Exit confirmation
- ☑ Show video files folders
- ☑ Block warning messages

Main Window

- □ Show Camera Header
- ☑ Use DirectX display: Direct 3D
- □ Use PTZ zoom window when available

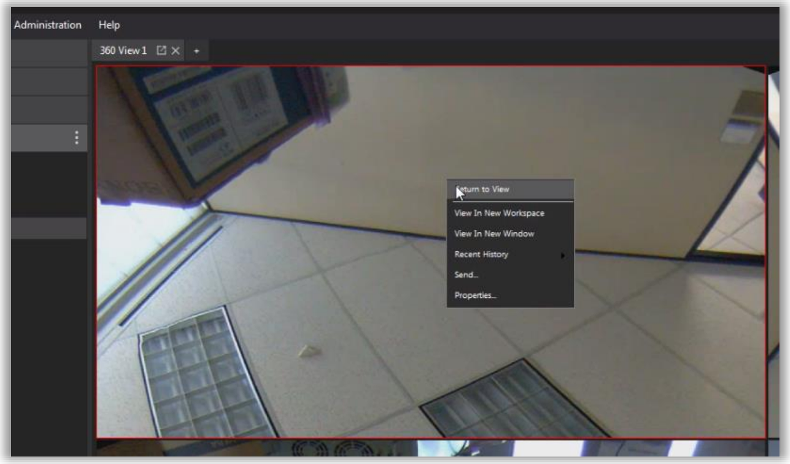
On Screen Controls

PTZ Cameras
- ● On screen PTZ ☑ Use DirectX
- ○ Digital Zoom Window
- ○ None

Standard Cameras
- ● Digital Zoom Window
- ○ None

H.265 Decoder

H265 Decoder is Enabled



4.6.B Details Pane

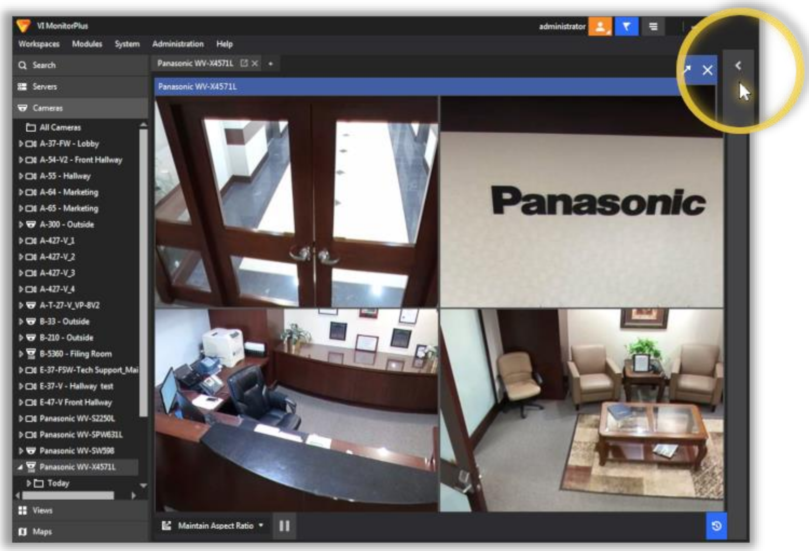
The **Details Pane** provides additional information and options for a specific camera while in Live Video mode.

To access it, click on the Details Pane icon to open a new menu bar on the upper right side of the workspace window.

‹

To close the Details Pane, click again on the same icon (inverted), now located next to the Details title.

›

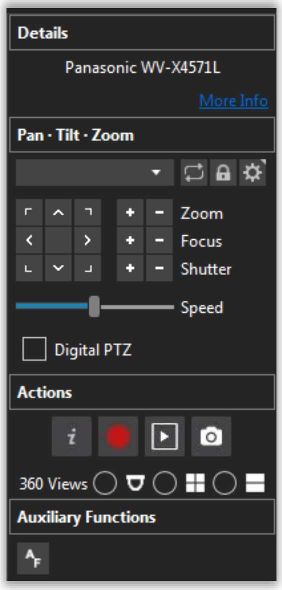


While viewing a specific camera within a workspace in Live Video mode, the **Details Pane** is hidden by default.

Once opened, the Details Pane will display basic information about the selected camera, as well as its corresponding options and controls.

Depending on the type of camera and its features, the available options are:

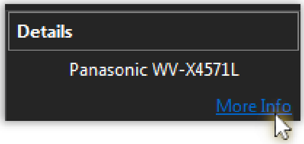
- Details
- Pan-Tilt-Zoom (PTZ) controls
- Actions
- Auxiliary Functions



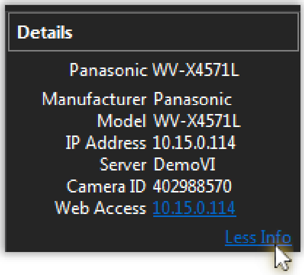
(1) DETAILS

This area displays the camera's specific information as it appears in the IP Server database.

Click on **More Info** or **Less Info** to toggle the Details view option **ON** or **OFF**.



Details OFF



Details

Panasonic WV-X4571L

Manufacturer Panasonic
Model WV-X4571L
IP Address 10.15.0.114
Server DemoVI
Camera ID 402988570
Web Access 10.15.0.114

Less Info

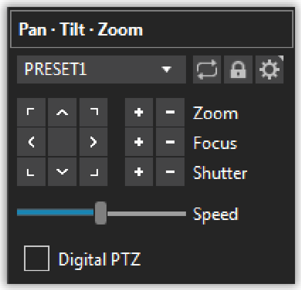
Details ON

Last updated: Oct/28/2019

Camera Details Values

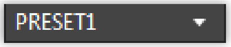
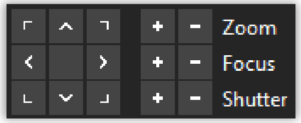
Manufacturer	Name of the manufacturing company for the displayed camera.
Model	Camera model as it appears in the IP Server database.
IP Address	IP Address of the camera.
Server	Name of the IP Server that the camera is associated with.
Camera ID	This Camera ID is unique only to the IP Server database. It can be used for troubleshooting.
Web Access	Web Access is a URL to access the camera's webpage. Clicking on this link will open a web browser window, where the user will be able to provide access credentials for the camera.

(2) PAN-TILT-ZOOM (PTZ)

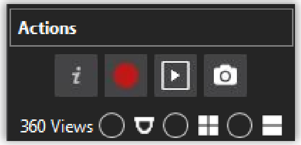


This feature is available only when the Details Pane window is selected on a camera **with PTZ functionality**.

NOTE - Not all 360° Cameras come with PTZ functionality.

	This drop-down menu provides a list of pre-defined and custom camera viewing angles.
⟳	PTZ Preset cycling configuration
🔒	PTZ Prioritization lock
⚙	Customization of Preset PTZ controls: Add a new preset or Delete a preset
	Remote controls for **Zoom**, **Focus** and **Shutter** capabilities, including angles and increase/decrease buttons.
	Adjusts the speed of panning and tilting within the Live Video, using the mouse when Digital PTZ is unchecked
	By checking the **Digital PTZ** box, functionality of PTZ controls becomes limited only to the use of the mouse. This means that panning and tilting the Live Video feed is not functional until the box for Digital PTZ has been unchecked.

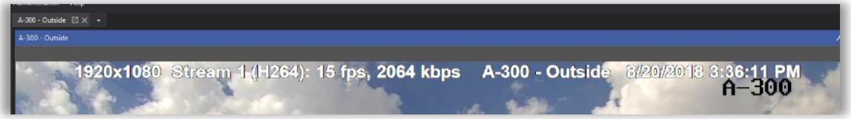
(3) ACTIONS



The **Actions** feature includes a series of additional controls and options for the Live Video.

Some of these options are not available, depending on the type of camera selected.

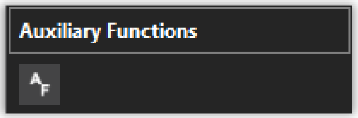
i	Display camera information on Live Video, including: Resolution, Codec, FPS and Timestamp

	 1920x1080 Stream 1 (H264): 15 fps, 2064 kbps A-300 - Outside 8/20/2018 3:36:11 PM A-300
●	Force Video Recording
▶	View recent Video History, opening a new window with recorded video streaming and the Timeline for advanced controls
📷	Capture Image Snapshot

Dewarping View Modes - The following options change the output from a **360° Camera**:

○ ◡	**Fisheye View**: It forces the camera to use fisheye view. If Panomorph (**Dewarping**) is available for the camera, this will represent the dewarped "fisheye" view when activated.
○ ⊞	**Quad View**: It will display **four** individual feeds from a fisheye camera, arranged within a workspace as a single image.
○ ▤	**Panorama View:** It enables an elongated view that spans across the top and bottom half of the workspace view.

(4) AUXILIARY FUNCTIONS



The **Auxiliary Functions** area provides extra features for the selected camera, where available.

AF	Auto Focus activates the camera's autofocus capability

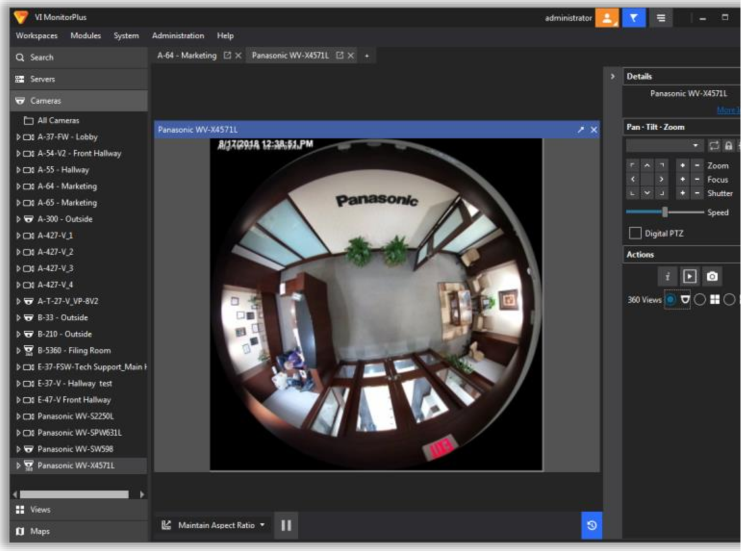
4.6.C Fisheye Cameras

The use of Fisheye Cameras and their features such as viewing Live and Recorded video, Pan-Tilt-Zoom (PTZ) controls and Camera Registration are all possible in VI MonitorPlus.

Fisheye Cameras appear on the Left Navigation Tree under their IP Server, identified by the following icons:

360

To use the Fisheye Cameras advanced view options, click on the corresponding **Details Pane** (*see 4.5.A*).

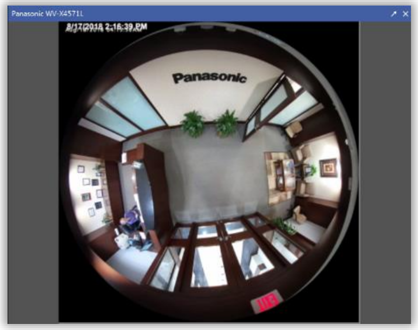


NOTE - Fisheye Cameras with 360° capability support advanced **Dewarp View Modes**.

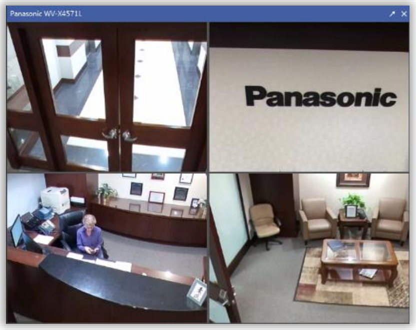
(1) 360° CAMERA DEWARP VIEW MODES

The Details Pane for a Fisheye Camera with 360° capability shows the **360 Views** options under **Actions**, enabling the Dewarp View Modes.

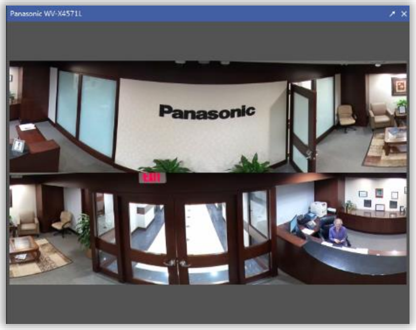
360 Views ○ ○ ○



FISH EYE



QUAD VIEW

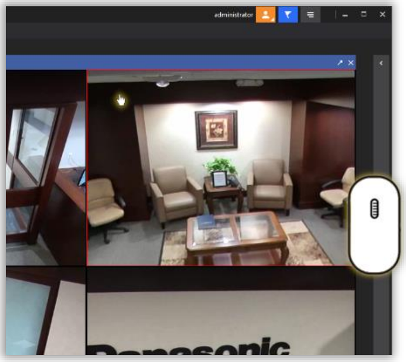


PANORAMA

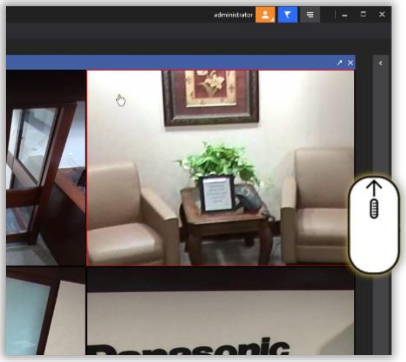
NOTE - When switching between Dewarp Views on a **Panasonic 360 camera**, the ***Aspect Ratio is maintained***, allowing the fisheye image to be fully displayed in the active layout.

(2) ZOOMING WITH MOUSE WHEEL

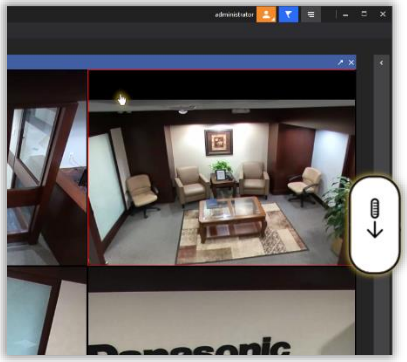
It is possible, with a Panasonic 360° camera, to **zoom in and out** on the live video feed by using the Mouse Wheel when in Fisheye or Quad mode, keeping the cursor within the desired view.



DEFAULT



ZOOM IN



ZOOM OUT

(3) AUTOSAVING LATEST VIEW

When using a Fisheye camera, VI MonitorPlus **will save its latest selected view** automatically.

This operation occurs on the Client's side whenever changes are made on the Workspace for each specific 360° Camera. view settings are stored physically in the local machine's registry.

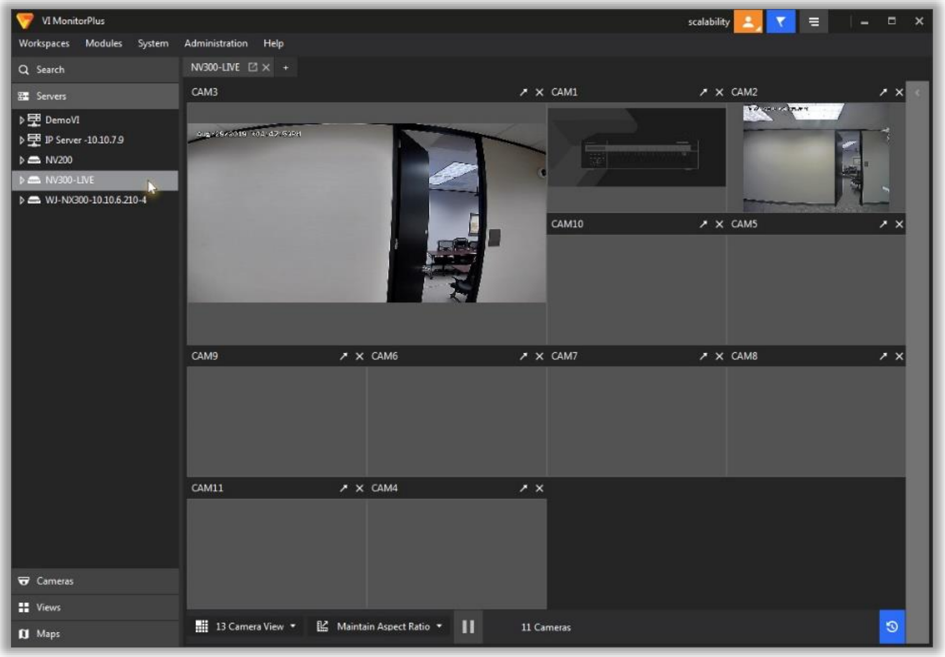
This feature also saves the User's last **Quad View** and **Panorama** positionings for each quadrant.

When the camera is selected again **from any module** of VI MonitorPlus, its latest saved view configuration will be displayed **by default**.

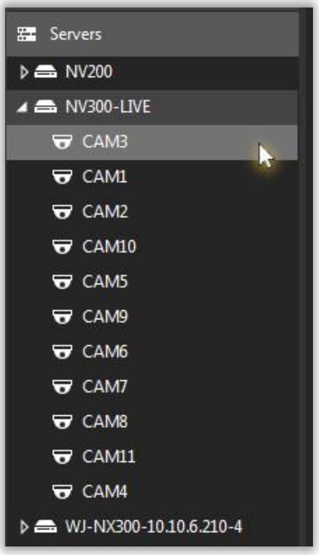
4.6.D NVR Live Video

NVR cameras can be accessed from the left tree, whenever available.

When clicking on any NVR icon, the cameras associated to it will be shown on the Workspace.



To access Live video from a supported NVR model,(*see 4.9.G*) select the camera from the **NVR menu** on the Left tree. Video will be displayed like other supported cameras. Camera Properties will be unavailable for NVR cameras setup.



4.6.E Vehicle Incident Detection feature

The **Vehicle Incident Detection** feature, also known as **VID**, allows users to track a moving object (such as a car, bus or train) and register its trajectory, displaying Metadata with geometric shapes overlaying the Live Video.

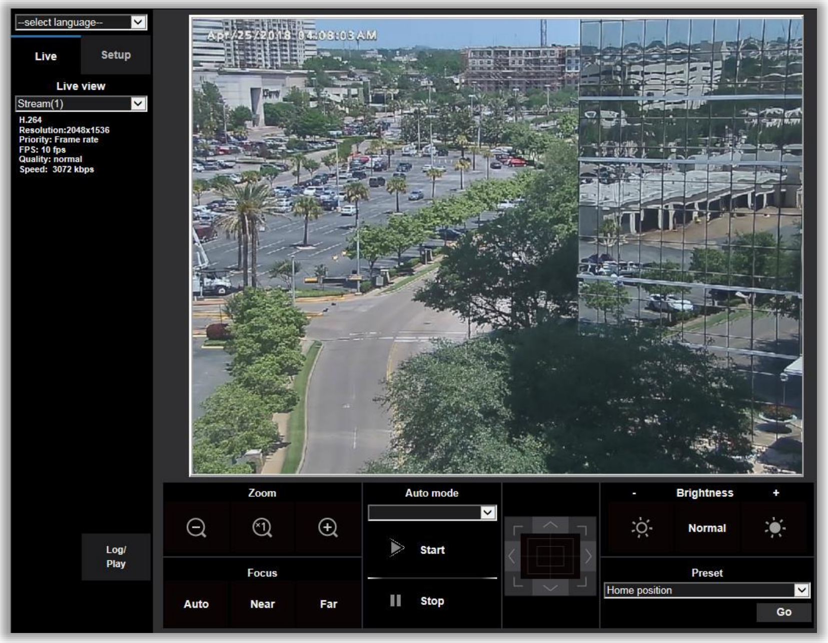
NOTE - Video Incident Detection is supported only by **Panasonic** cameras .

Open Internet Explorer and log into the camera's setup URL or web interface.

This URL can be found on the Camera Properties page, listed as ***Web Access***.

Ensure **your camera is properly positioned** to cover the desired view area.

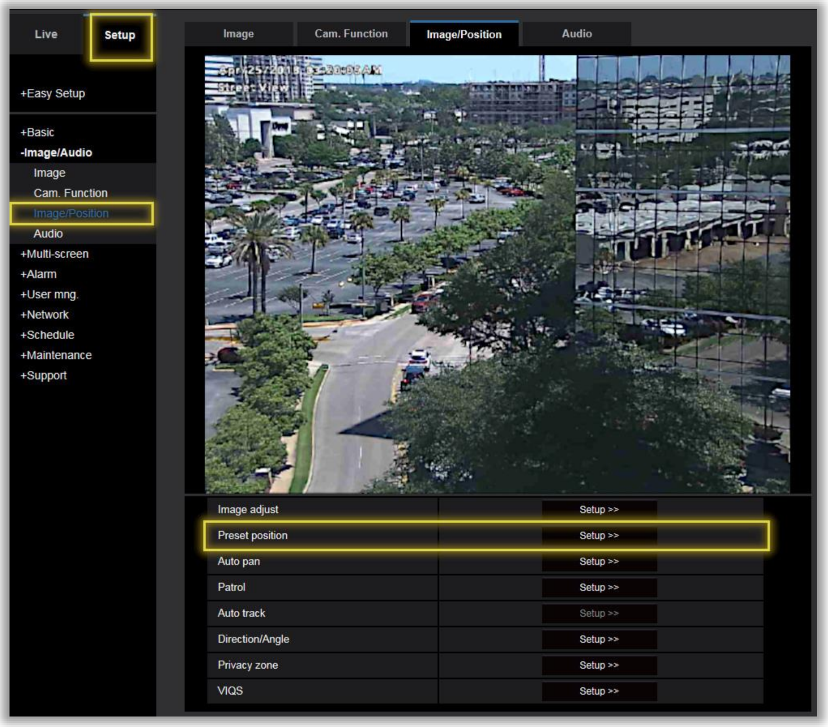
VID supports horizontal lane drawing; align streets and pathways with the view for better results.



H.264
Resolution:2048x1536
Priority: Frame rate
FPS: 10 fps
Quality: normal
Speed: 3072 kbps

To setup a **Basic Preset** for the camera:

- From the Left Tree, click on the **Setup** tab (top).
- Select **Image/Audio** > **Image/Position.**
- In the Main Panel (right), click on **Setup** for **Preset Position.**

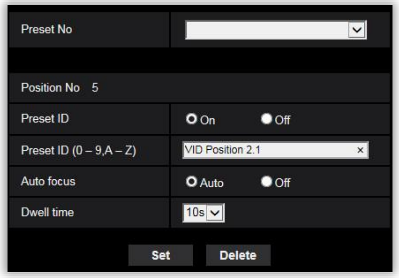


In the **Position Preset** window, click on the **Preset No**. drop down list and select an available option.

Ensure **Preset ID** and **Auto Focus** are both **ON**.

In the **Preset ID** (0-9,A-Z) field, create a valid name.

Click **Set** to create the Preset Position.



Preset No	
Position No 5	
Preset ID	◉ On ○ Off
Preset ID (0 – 9,A – Z)	VID Position 2.1
Auto focus	◉ Auto ○ Off
Dwell time	10s

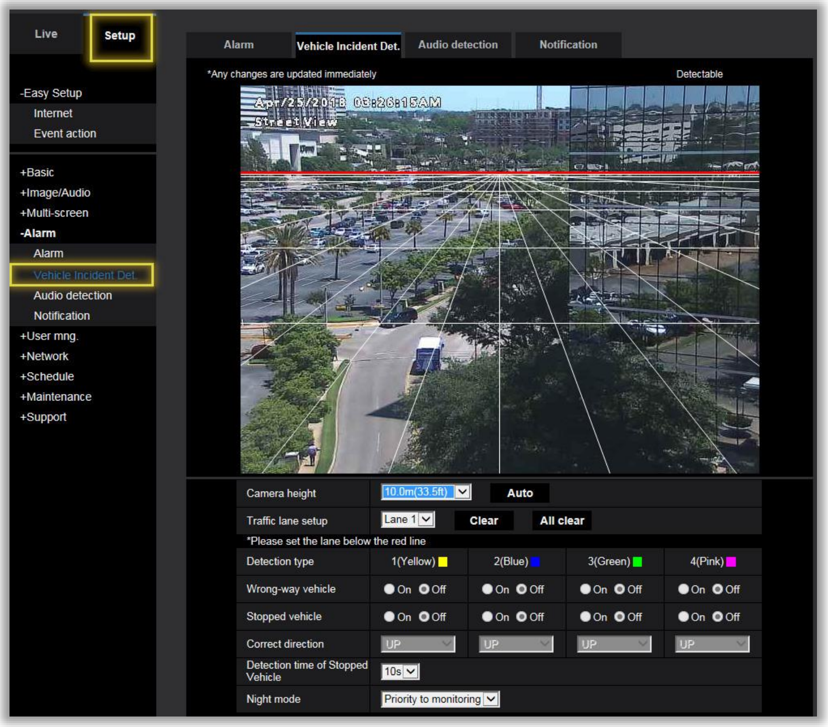
Click **Close** (at the bottom).

To access **Vehicle Incident Detection**:

- From the Left Tree, click on the **Setup** tab (top).
- Select **Alarm** > **Vehicle Incident Detection.**

A Live Video feed image will be shown on the Main Panel (right).

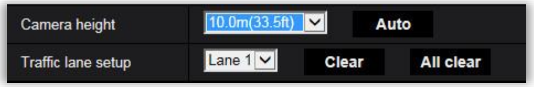
It will show a horizontal red line (Camera Height) and a series of gridlines generated by the camera to be used when defining Lanes.



*Any changes are updated immediately

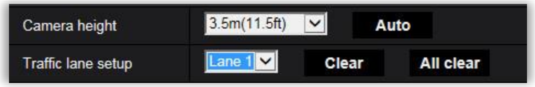
Camera height	10.0m(33.5ft) Auto			
Traffic lane setup	Lane 1 Clear All clear			
*Please set the lane below the red line				
Detection type	1(Yellow) 🟨	2(Blue) 🟦	3(Green) 🟩	4(Pink) 🟪
Wrong-way vehicle	○ On ◉ Off	○ On ◉ Off	○ On ◉ Off	○ On ◉ Off
Stopped vehicle	○ On ◉ Off	○ On ◉ Off	○ On ◉ Off	○ On ◉ Off
Correct direction	UP	UP	UP	UP
Detection time of Stopped Vehicle	10s			
Night mode	Priority to monitoring			

To adjust the grid position, use the **Camera Height** drop-down list and select the desired height.



Camera height	10.0m(33.5ft) Auto
Traffic lane setup	Lane 1 Clear All clear

To setup a new lane, select **Lane 1** from the **Traffic lane setup** drop-down list. Lanes are defined below the horizontal red line on the video.



Camera height	3.5m(11.5ft) Auto
Traffic lane setup	Lane 1 Clear All clear

Using the mouse cursor, click and drag a line on top of the video to define the lane area.

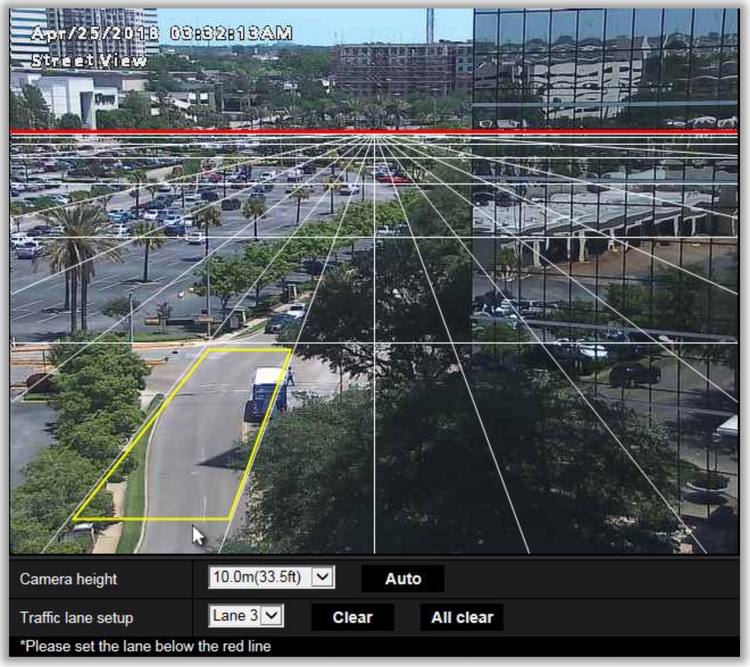
Start by defining the vertical height and next the horizontal width.

Draw a straight line then select the opposite corner to complete the lane.

Click "**Clear**" to delete the current lane.

Click "**All Clear**" to delete ALL the lanes on the view.

Additional segments can be created by drawing connecting boxes (for example to cover a curved area).



Camera height	10.0m(33.5ft)	Auto	
Traffic lane setup	Lane 3	Clear	All clear

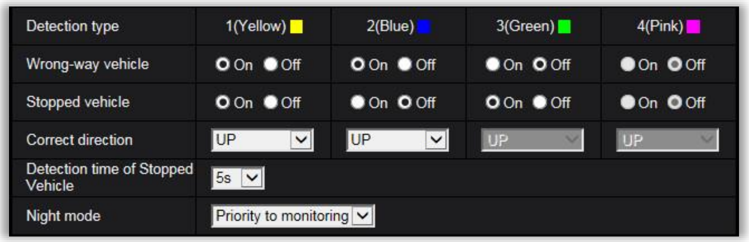
*Please set the lane below the red line

NOTE - Up to **4 Lanes** can be defined on a single view, each one with a distinctive color and specific options.

Set the **Wrong-way vehicle** radio button to **On** to view onscreen objects (tracking lines) when vehicles traveling in the wrong direction are detected.

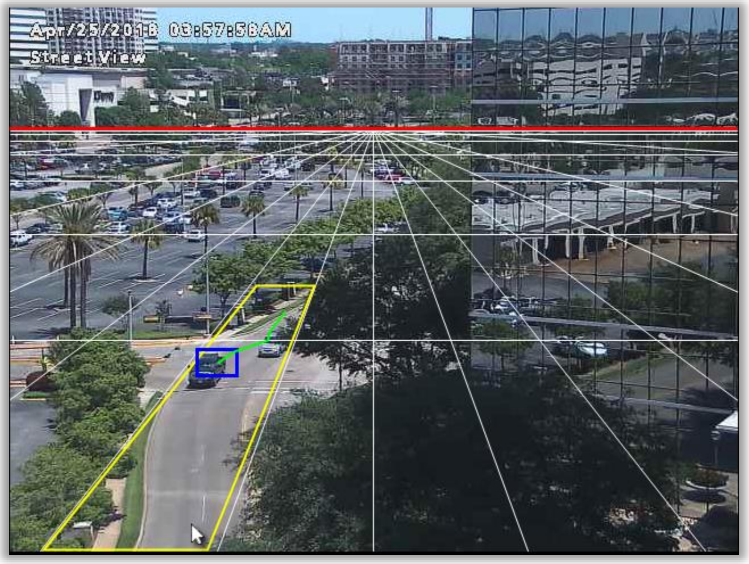
You may also enable **Stopped vehicle** to trigger that event.

Define the **Correct direction** of the traffic by selecting **UP** or **DOWN** on each lane where it applies.



Detection type	1(Yellow) 🟨	2(Blue) 🟦	3(Green) 🟩	4(Pink) 🟪
Wrong-way vehicle	◉ On ○ Off	◉ On ○ Off	○ On ◉ Off	○ On ◉ Off
Stopped vehicle	◉ On ○ Off	○ On ◉ Off	◉ On ○ Off	○ On ◉ Off
Correct direction	UP	UP	UP	UP
Detection time of Stopped Vehicle	5s			
Night mode	Priority to monitoring			

Once configured, any vehicle traveling the wrong direction will be identified by a blue square and a trailing green path line.



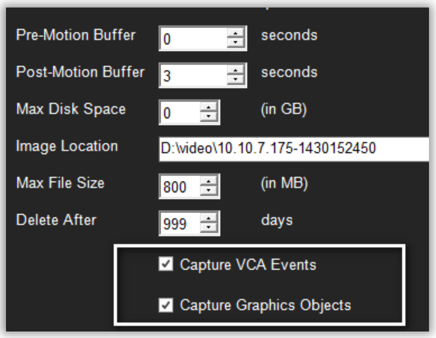
NOTE - VID setup takes 10 to 15 minutes to reflect the changes on the received images. Allow sufficient time for the camera to apply the configuration.

Next, go to the camera's Live Video in VI MonitorPlus.

Access **Camera Properties** by right clicking on the camera in View or right clicking the camera node and selecting Properties.

Enable **Capture VCA Events** and **Capture Graphics Objects** by clicking the corresponding checkboxes from the General tab.

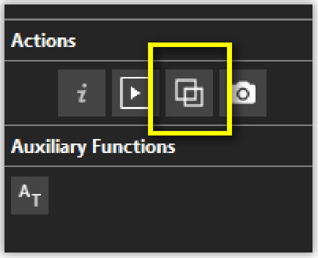
> **NOTE -** If you are receiving overlay objects in your camera web page, but not on VI MonitorPlus, uncheck and re-check **Capture VCA Events** and **Capture Graphics Objects**.



Pre-Motion Buffer 0 seconds
Post-Motion Buffer 3 seconds
Max Disk Space 0 (in GB)
Image Location D:\video\10.10.7.175-1430152450
Max File Size 800 (in MB)
Delete After 999 days

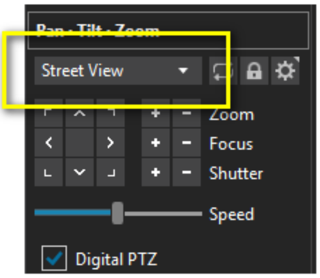
☑ Capture VCA Events
☑ Capture Graphics Objects

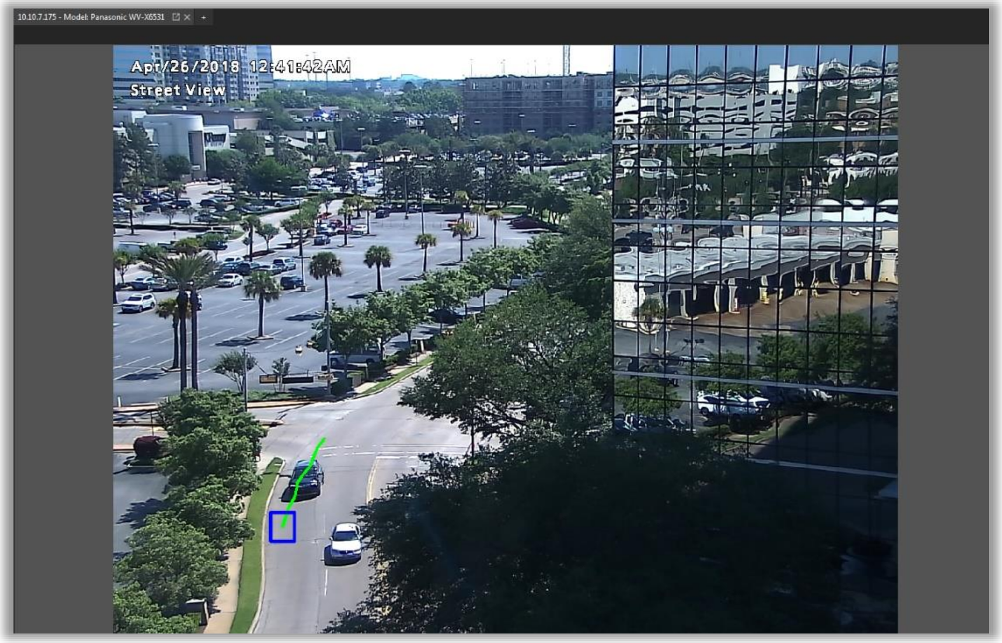
Once in Live mode, expand the Camera Details Panel and select **Show Graphic Object Overlay**.



> **NOTE -** Moving the PTZ camera in any direction will reset all VID camera configurations. Please utilize the PTZ Lock feature to prevent this from moving during VID operation.

To restore the VID feature, select the configured preset in the Camera Details Panel.



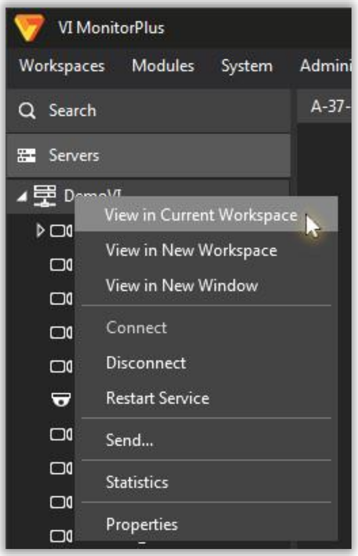


To view the On-screen objects, select the camera in the left tree to view it in Live mode. Any event that triggers the Wrong Direction alarm will be detected and shown instantly.

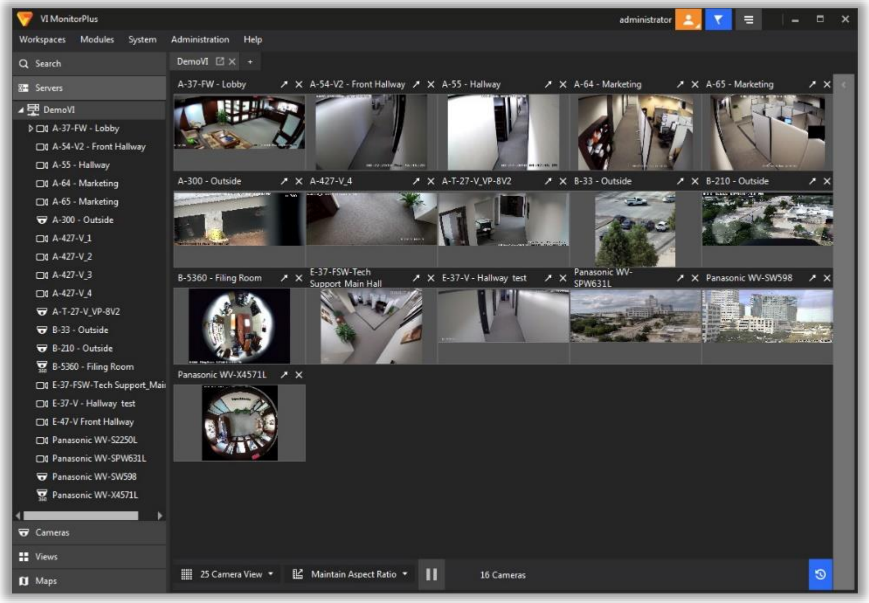
4.6.F Cycle Views feature

VI MonitorPlus comes with a feature to split multiple cameras outputs into self-cycling Views (*Pages*), displayed automatically after a specific time interval. For example, in a 24-cameras server environment, it is possible to configure a set of three 8-cameras views, each one organized as a single page that skips to the next one after 10 seconds, and so on until it goes back to the first one.

To activate the Cycle Views feature, right-click on the server name shown in the left-side panel, under "**Servers**", then click on "**View in Current Workspace**".

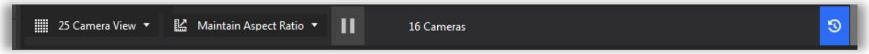


All the cameras in the server will be displayed in a new Workspace, generated automatically.

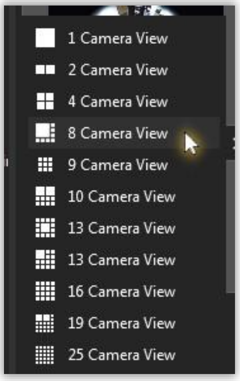


At the bottom of the Workspace, a status bar will show:

- Camera View options
- View size options
- Play/Pause button
- Number of visible cameras
- Recorded Video switch button.

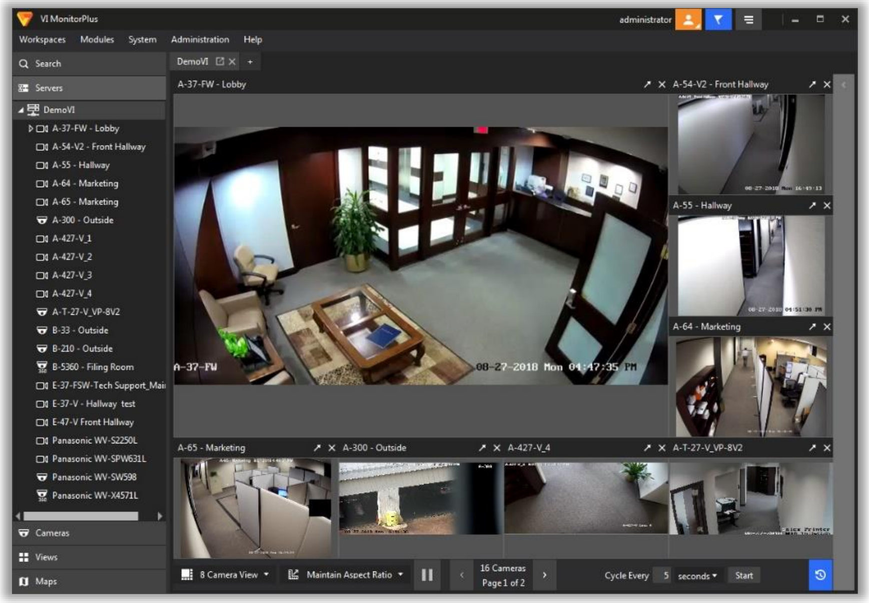


Define the size of each view layout by opening the Camera View list at the bottom left of the Workspace and select the desired View.



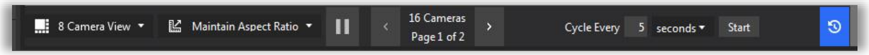
NOTE - Always select a number that is less than the total of cameras displayed.

The first automatically generated View (Page) will be displayed, using the View layout previously selected from the Camera View list.



The status bar now displays the following:

- Camera View options
- View size options
- Play/Pause button
- Cameras, Page number and Next/Previous page buttons
- Cycle interval (time) options, Start button
- Recorded Video switch button.



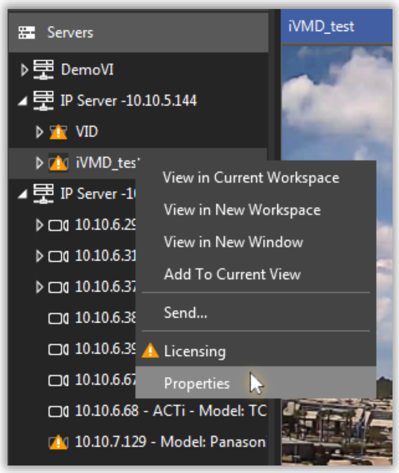
*Set the paging interval value (**Cycle Every** field) and click on **Start** to begin the automatic sequence.*
You can also manually go to the next or previous page by clicking on the left/right arrow buttons.

4.6.G Embedded Analytics support for i-VMD Cameras

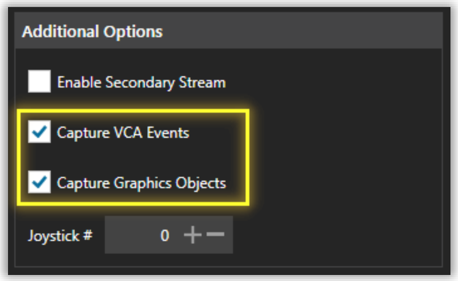
VI MonitorPlus supports **Embedded Analytics** for Panasonic i-VMD (Video Motion Detection) cameras.

To ensure the feature is active, proceed as follow:

Right-click the camera on the left tree, and select "**Properties**"



In the **Camera Setup** window, "**General**" tab, locate the "Additional Options" box on the right side, and check both "**Capture VCA Event**" and "**Capture Graphic Objects**" boxes.



Additional Options

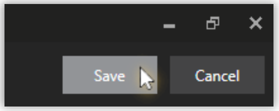
□ Enable Secondary Stream

☑ Capture VCA Events

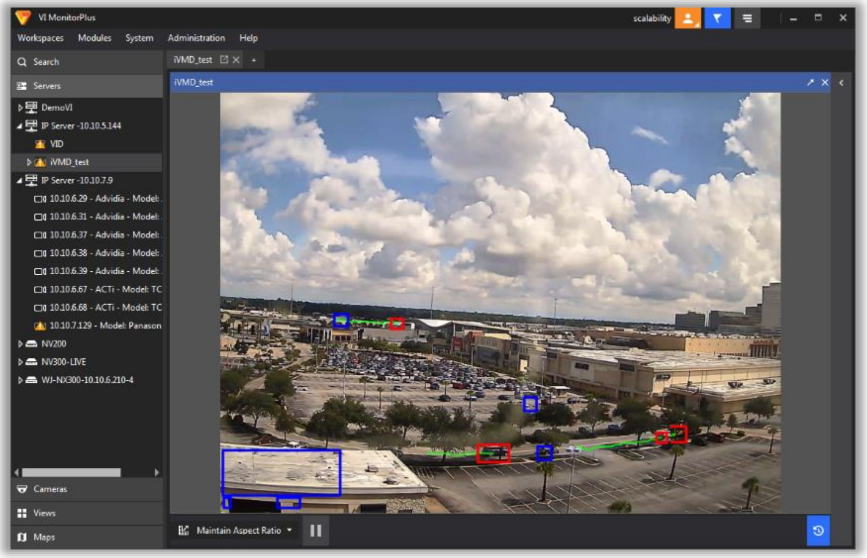
☑ Capture Graphics Objects

Joystick # 0

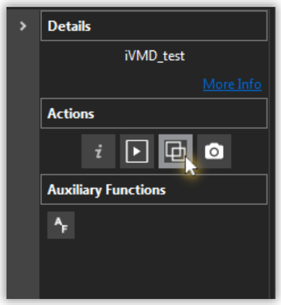
Click on "**Save Now**" (top right button).



Depending on the settings for the camera, the object detection will appear in the live video streaming, with color coded frames and motion lines.

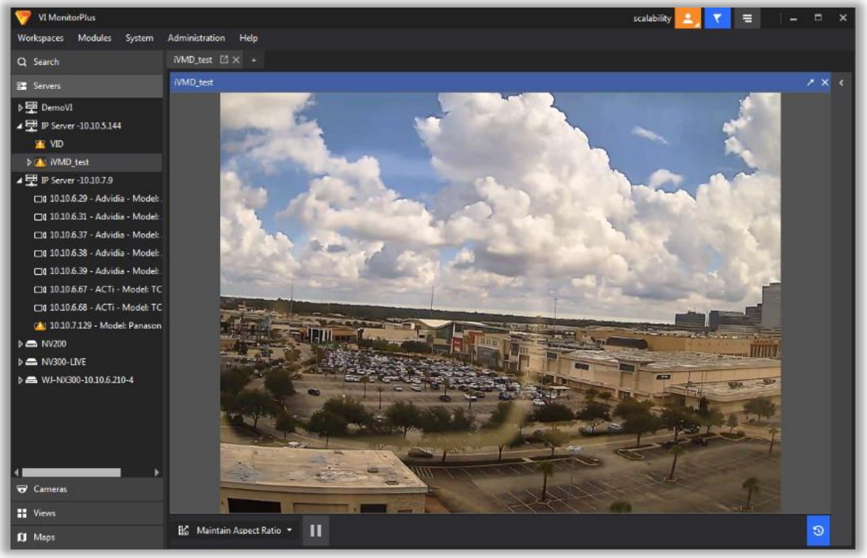

VI MonitorPlus
scalability
Workspaces
Modules
System
Administration
Help
Search
Servers
iVMD_test
DemoVI
IP Server -10.10.5.144
VID
iVMD_test
IP Server -10.10.7.9
10.10.6.29 - Advidia - Model:
10.10.6.31 - Advidia - Model:
10.10.6.37 - Advidia - Model:
10.10.6.38 - Advidia - Model:
10.10.6.39 - Advidia - Model:
10.10.6.67 - ACTi - Model: TC
10.10.6.68 - ACTi - Model: TC
10.10.7.129 - Model: Panason
NV200
NV300-LIVE
WJ-NX300-10.10.6.210-4
Cameras
Views
Maps
Maintain Aspect Ratio

To turn off the live object detection, open the **Details Pane** (upper right arrow) and click on the "**Hide Graphic Objects Overlay**" button.



The live streaming will now appear without the frames and lines.

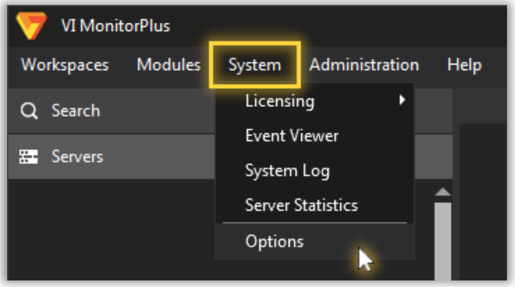
Click on the "**Show Graphic Objects Overlay**" button (in the Details Pane) to reactivate the live detection.


VI MonitorPlus
scalability
Workspaces
Modules
System
Administration
Help
Search
Servers
iVMD_test
DemoVI
IP Server -10.10.5.144
VID
iVMD_test
IP Server -10.10.7.9
10.10.6.29 - Advidia - Model:
10.10.6.31 - Advidia - Model:
10.10.6.37 - Advidia - Model:
10.10.6.38 - Advidia - Model:
10.10.6.39 - Advidia - Model:
10.10.6.67 - ACTi - Model: TC
10.10.6.68 - ACTi - Model: TC
10.10.7.129 - Model: Panason
NV200
NV300-LIVE
WJ-NX300-10.10.6.210-4
Cameras
Views
Maps
Maintain Aspect Ratio

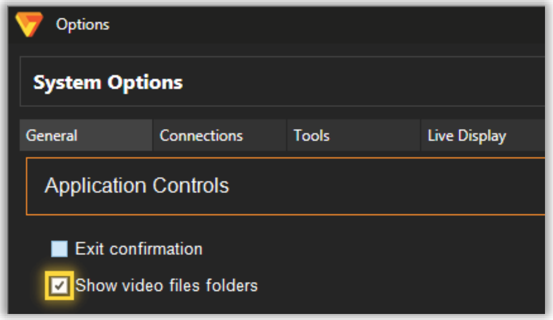
4.7 RECORDED VIDEO

VI MonitorPlus comes with the ability to access Recorded Video directly from the Left Navigation tree. To enable this feature, follow the steps below:

On the Main menu (Top), select "**System**", then "**Options**"



In the **System Options** screen, select the "**General Tab**"; under the **Application Control** section, make sure the "**Show video files folders**" box is checked.



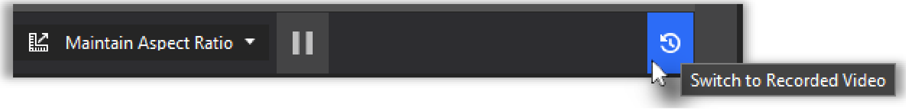
□ Exit confirmation

☑ Show video files folders

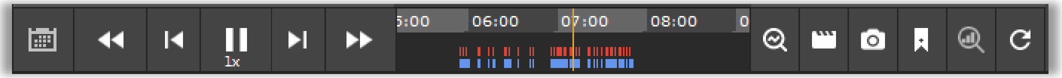
Close the System Options screen and exit VI MonitorPlus. **To use the feature, run VI MonitorPlus again and test it.**

4.7.A Playback

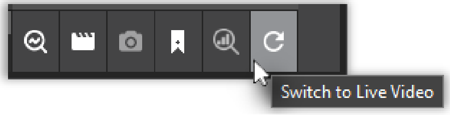
Recorded Video can be accessed and managed using the **Playback bar**, which is located at the bottom of the workspace screen for any camera that supports this feature.



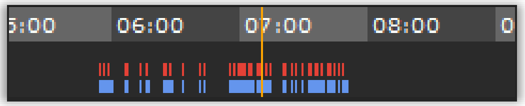
To switch from Live to Recorded Video, click on the **Blue Icon** located at the bottom-right corner of the screen.



The Recorded Video bar will be activated showing the **Calendar** and **Playback** controls on the left side, the **Timeline** on the center, and the **Video Management** controls on the right side.



To switch back to Live Video, click on the **Return icon** at the bottom-right corner of the screen.



In the Timeline, the **Orange vertical bar** (centered) indicates the current position in time of the video. It is also the starting point to begin playing it.

Red areas or spots represent motion detection, and **Blue areas** or spots represent motion video recording available for playback.

4.7.B Analytics

VI MonitorPlus comes with the ability to enable or disable the display of **Recorded Video Analytics** directly from the Timeline bar. This feature is available on cameras that support VCA (Video Content Analysis) events.

(1) ENABLING VIDEO ANALYTICS DISPLAY

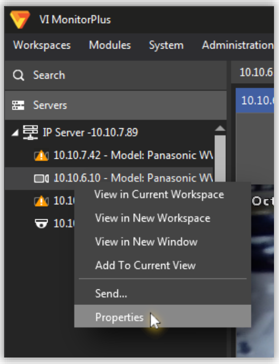
To activate the Analytics Display feature, follow the steps below:

Open the **Properties** page for the camera:

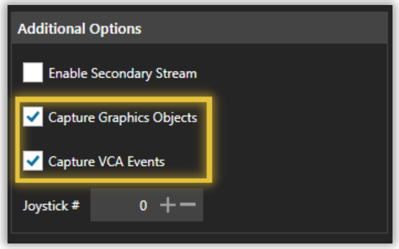
- Right-click the selected camera from the Left Navigation Tree and select **Properties**.

or:

- Open **Main Menu > Administration > Cameras > Configure Properties** and select the camera model from the Left Tree.



In the **Camera Setup** window, **General** tab, make sure the checkboxes for "***Capture Graphics Objects***" and "***Capture VCA Events***" are available and selected, under the "**Additional Options**" section.


Additional Options

☐ Enable Secondary Stream

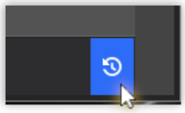
☑ Capture Graphics Objects

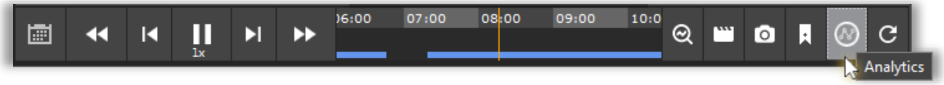
☑ Capture VCA Events

Joystick # 0

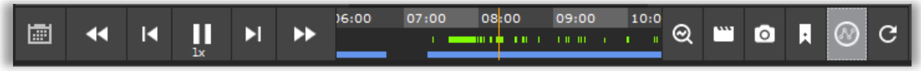
(2) VISUALIZING ANALYTICS

From the Live Video interface, switch to **Recorded Video** to access the Timeline.





From the Timeline bar, click on the **Analytics** icon.



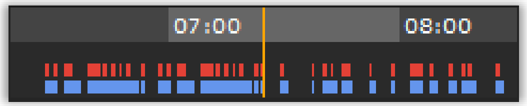
The **green lines** on the Timeline will indicate events captured during the Live video session and processed as **Analytics.**

4.7.C Bookmarks

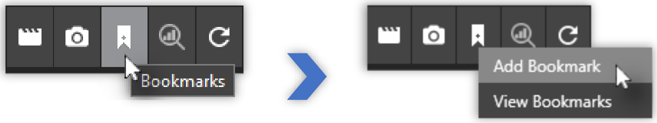
VI MonitorPlus comes with a complete interface to create and manage **Recorded Video Bookmarks**, which can either point to a single frame within the video sequence or include specific time intervals (***start-end***). Bookmarks are used as a reference for further review or analysis.

(1) ADDING A BOOKMARK

In the Timeline, position the starting point of the bookmark aligning it with the Orange indicator.



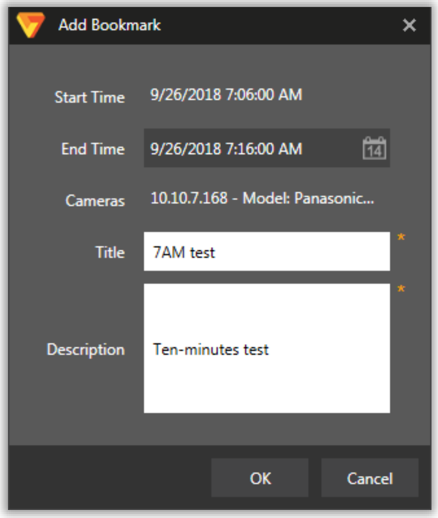
Click on the **Bookmarks icon**, then select "**Add Bookmark**" on the menu.



In the **Add Bookmark** window, enter the **End Time** manually or using the Calendar (see below), and the **Title** and **Description** of the bookmark.

Click **OK** when ready.

All fields must be filled.



Add Bookmark

Start Time 9/26/2018 7:06:00 AM

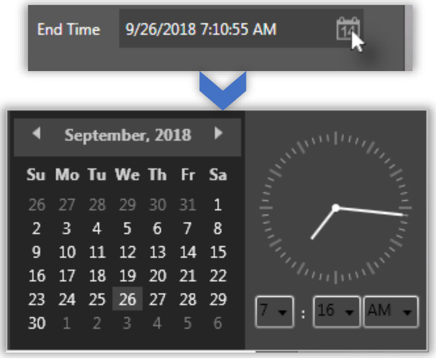
End Time 9/26/2018 7:16:00 AM

Cameras 10.10.7.168 - Model: Panasonic...

Title * 7AM test

Description * Ten-minutes test

When adding a new bookmark, use the **Calendar** clicking on the corresponding icon, and easily select the End Time from its interface.



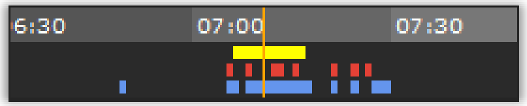
End Time 9/26/2018 7:10:55 AM

September, 2018

Su	Mo	Tu	We	Th	Fr	Sa
26	27	28	29	30	31	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	1	2	3	4	5	6

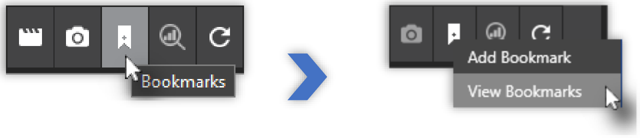
7 : 16 AM

When finished, a thick **Yellow line** will appear on the Timeline indicating the Bookmark interval.



(2) VIEWING BOOKMARKS

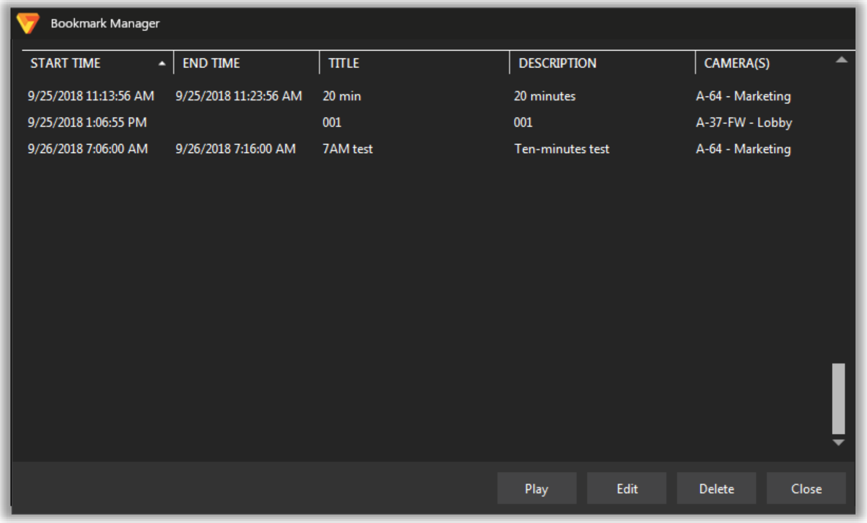
Click on the **Bookmarks icon**, then select "**View Bookmarks**" on the menu.



The **Bookmark Manager** window will show the customizable list of available bookmarks, plus 4 option buttons: **Play**, **Edit**, **Delete** and **Close**.

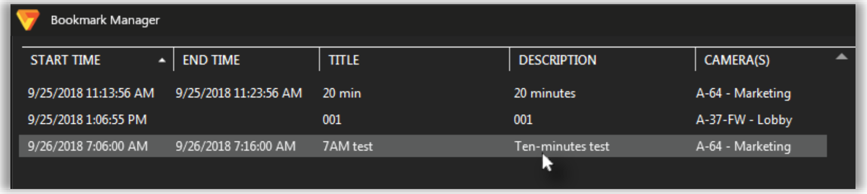
Click on any column title to **sort the list** by its value (descending / ascending).

Adjust any column width by clicking and dragging the vertical separator between column titles to the left or the right.



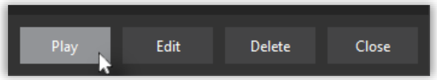
START TIME	END TIME	TITLE	DESCRIPTION	CAMERA(S)
9/25/2018 11:13:56 AM	9/25/2018 11:23:56 AM	20 min	20 minutes	A-64 - Marketing
9/25/2018 1:06:55 PM		001	001	A-37-FW - Lobby
9/26/2018 7:06:00 AM	9/26/2018 7:16:00 AM	7AM test	Ten-minutes test	A-64 - Marketing

To activate any of the options, select the desired bookmark from the list.

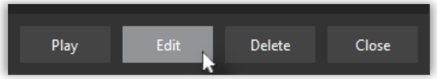


START TIME	END TIME	TITLE	DESCRIPTION	CAMERA(S)
9/25/2018 11:13:56 AM	9/25/2018 11:23:56 AM	20 min	20 minutes	A-64 - Marketing
9/25/2018 1:06:55 PM		001	001	A-37-FW - Lobby
9/26/2018 7:06:00 AM	9/26/2018 7:16:00 AM	7AM test	Ten-minutes test	A-64 - Marketing

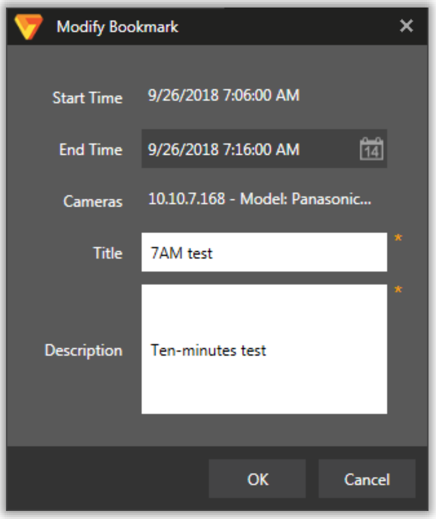
Click **Play** to launch the bookmarked video (close the Bookmark Manager to view it).



Click **Edit** to modify the parameters for the bookmark.



The Modify Bookmark option will allow to change the End Time, Title and/or Description.



Start Time 9/26/2018 7:06:00 AM

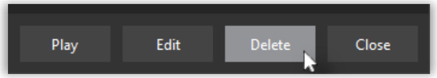
End Time 9/26/2018 7:16:00 AM

Cameras 10.10.7.168 - Model: Panasonic...

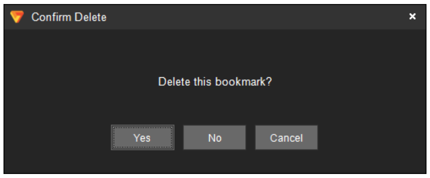
Title 7AM test *

Description Ten-minutes test *

Click **Delete** to remove the bookmark from the list (***confirmation needed***).



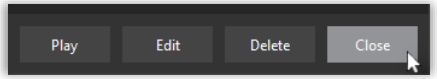
Once the bookmark is deleted, the yellow indicator will disappear from the timeline.


Confirm Delete

Delete this bookmark?

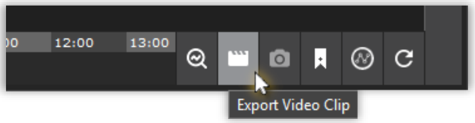
This operation cannot be undone.

Click **Close** to exit the Bookmark Manager and return to the Recorded Video feed.



4.7.D Video Clips

To create and export a recorded video clip from a specific time interval, click the **Export Video Clip** button, located to the right of the timeline bar.



The **Export Video Clip** window will open in the foreground.

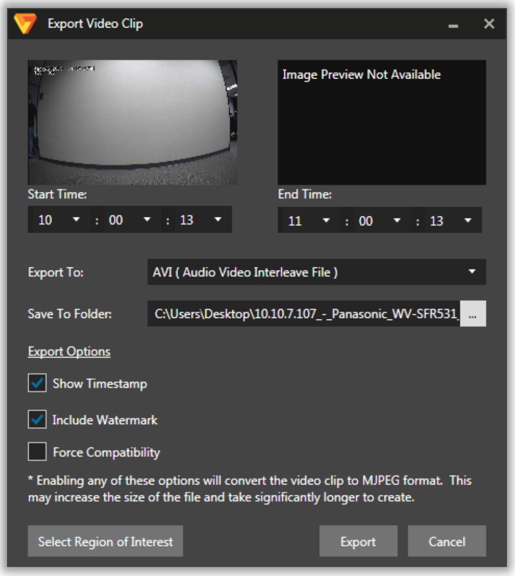

Export Video Clip

Image Preview Not Available

Start Time: 10 : 00 : 13

End Time: 11 : 00 : 13

Export To: AVI (Audio Video Interleave File)

Save To Folder: C:\Users\Desktop\10.10.7.107_-_Panasonic_WV-SFR531_

Export Options

☑ Show Timestamp

☑ Include Watermark

☐ Force Compatibility

* Enabling any of these options will convert the video clip to MJPEG format. This may increase the size of the file and take significantly longer to create.

Specify the **Start Time** and **End Time** for the clip, using the corresponding drop-down lists for each value.

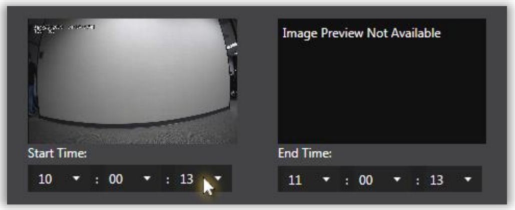


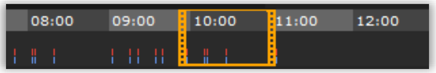
Image Preview Not Available

Start Time: 10 : 00 : 13

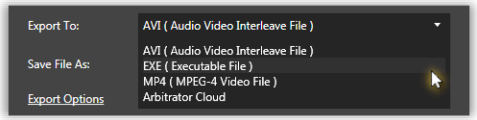
End Time: 11 : 00 : 13

The selected interval will be automatically shown in the timeline within an **orange frame**.

> NOTE - This frame can be adjusted by clicking and dragging it horizontally to manually modify the time interval.



Open the **Export To**: drop-down list to change the video file format.


Export To: AVI (Audio Video Interleave File)

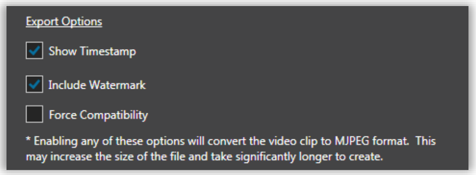
Save File As:

Export Options

AVI (Audio Video Interleave File)
EXE (Executable File)
MP4 (MPEG-4 Video File)
Arbitrator Cloud

When “**AVI**” or “**MPEG**” are selected, the application will display a set of **Export Options**:

- **Show Timestamp:** Embeds the timestamp in to the exported video.
- **Include Watermark**: Creates a watermark and embeds it into the video to prevent video tampering.
- **Force Compatibility**: Forces the video to be exported in MJPEG format.


Export Options

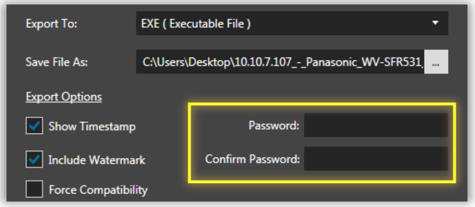
☑ Show Timestamp

☑ Include Watermark

☐ Force Compatibility

* Enabling any of these options will convert the video clip to MJPEG format. This may increase the size of the file and take significantly longer to create.

If “**EXE (Executable file)**” is selected, the application will ask for a Password to protect the exported file. A self-executable file will be produced.



Export To: EXE (Executable File)

Save File As: C:\Users\Desktop\10.10.7.107_-_Panasonic_WV-SFR531

Export Options

☑ Show Timestamp

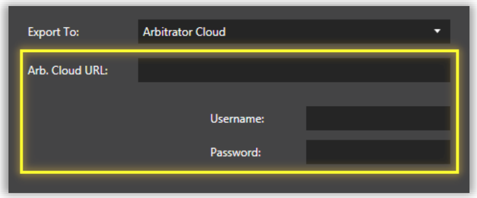
☑ Include Watermark

□ Force Compatibility

Password:

Confirm Password:

If “**Arbitrator Cloud**” is selected, the application will ask for the Arbitrator Cloud’s URL, its Username and Password.



Export To: Arbitrator Cloud

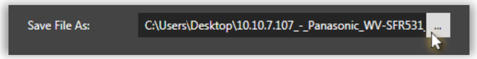
Arb. Cloud URL:

Username:

Password:

“**Save to Folder:**” shows the default destination folder and filename for the clip.

Click on the white icon to the right to open the File Explorer window for more options.

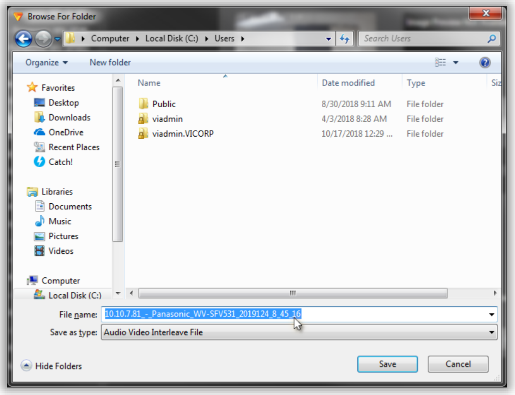


Save File As: C:\Users\Desktop\10.10.7.107_-_Panasonic_WV-SFR531

The File Explorer window allows ***changing both the destination folder and the file name*** for the exported clip.

The “***Save as type***” option will replicate the file type selected from the application’s interface by default.

Click “**Save**” to confirm or “**Cancel**” to return.



Browse For Folder

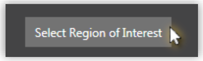
Computer ▸ Local Disk (C:) ▸ Users ▸

Name	Date modified	Type
Public	8/30/2018 9:11 AM	File folder
viadmin	4/3/2018 8:28 AM	File folder
viadmin.VICORP	10/17/2018 12:29 ...	File folder

File name: 10.10.7.81_-_Panasonic_WV-SFV531_2019124_8_45_16

Save as type: Audio Video Interleave File

Click on “**Select Region of Interest**” to define a R.o.I. for the clip.

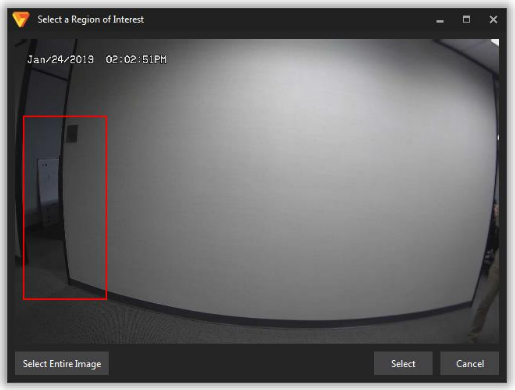


Mark the Region of Interest directly on the corresponding window and click “**Select**” to confirm.

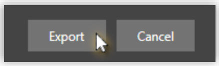
Click “**Select Entire Image**” to expand the Region of Interest to the maximum allowable size.

The Region of Interest will be displayed back in the “**Export Video Clip**” window preview.

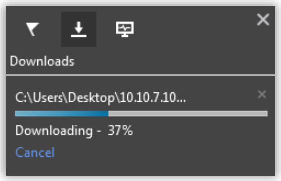
Click “**Cancel**” to return.



Click “**Export**” to start the file exporting process, or “**Cancel**” to exit.



The file will start to be downloaded. Click “**Cancel**” to stop the process.

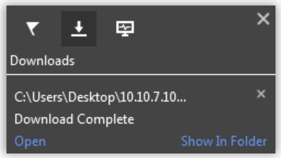

Downloads

C:\Users\Desktop\10.10.7.10...

Downloading - 37%

Cancel

Once finished, the file will be ready to be played (“**Open**”) or to be found on its destination folder (“**Show in Folder**”).


Downloads

C:\Users\Desktop\10.10.7.10...

Download Complete

Open Show In Folder

NOTE - Clipped video files are limited in size to be 1.5GB, while exporting. In some rare instances, the file size may be slightly smaller than 1.5GB.

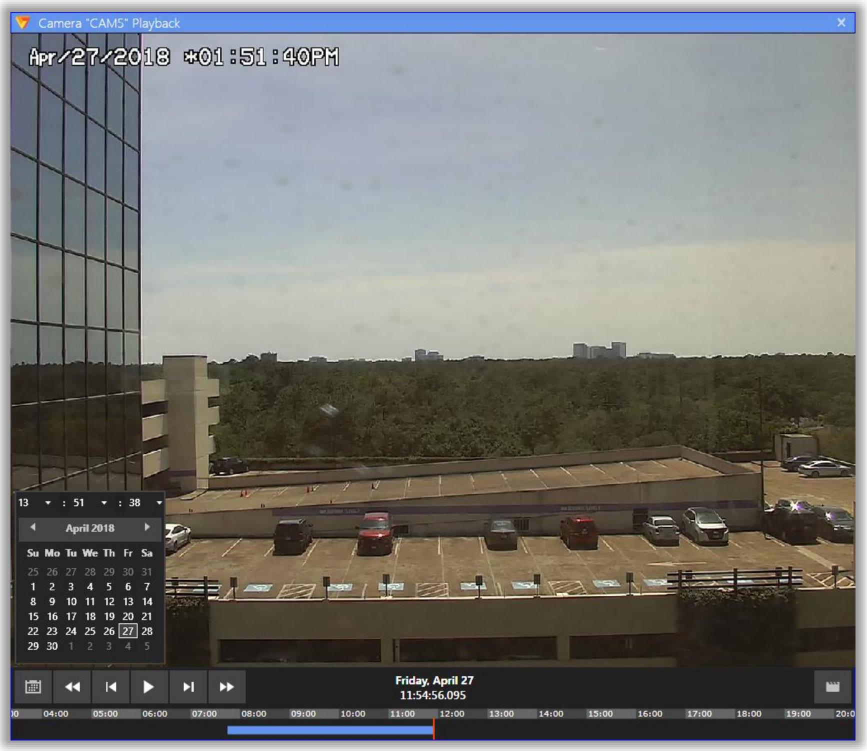
4.7.E Playback support for NVR Cameras

Recorded video for **NVR cameras** listed in the left navigation tree is available through the recorded mode of VI MonitorPlus.

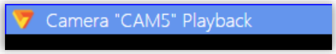
To access recorded video, click on the camera under the enrolled NVR server.

A new **Playback Window** will appear displaying the **Playback bar** along with the **Calendar** picker and the **Export Clip** icon.

The **Timeline** is also visible at the bottom of the window.



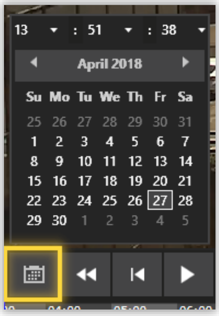
Before utilizing **NVR Cameras** in **recorded mode**, ensure your NVR is properly enrolled.



Before utilizing **NVR Cameras** in **recorded mode**, ensure your NVR is properly enrolled.

To locate recorded video, use the Calendar to select a time and date or use the Forward and Previous File Recording icons on the toolbar.

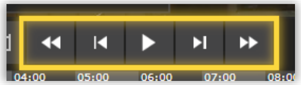
Selecting Previous Recording or Next Recording will jump the playback to the next recorded segment.



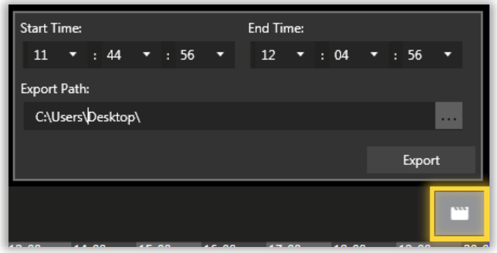
13 : 51 : 38

April 2018

Su	Mo	Tu	We	Th	Fr	Sa
25	26	27	28	29	30	31
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	1	2	3	4	5



The Export Clip option allows the creation of an external AVI video clip after specifying the start-end time and its export path.



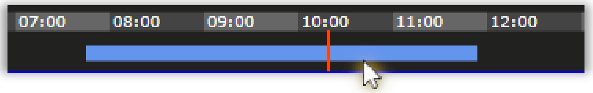
Start Time: 11 : 44 : 56

End Time: 12 : 04 : 56

Export Path: C:\Users\Desktop\

Export

The Timeline can be used to navigate the NVR camera playback within a time interval.

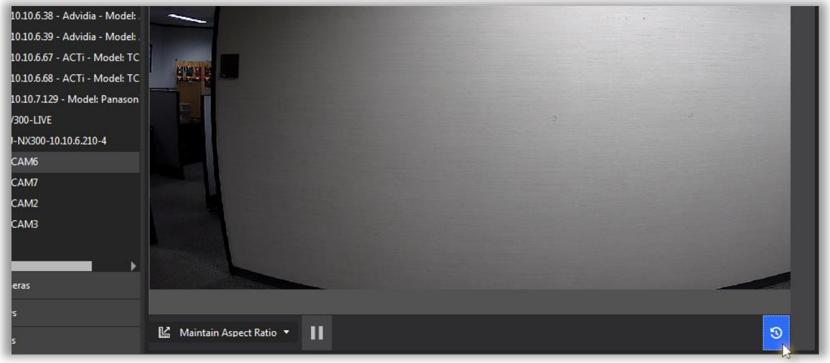


NOTE - NVR Playback support is recommended on a physical client machine, instead of virtual computer environment.

4.7.F Video Clipping support for NVR Cameras

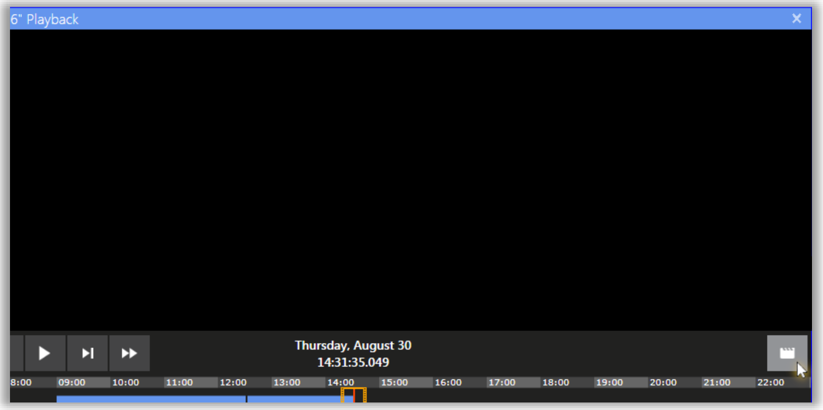
VI MonitorPlus features the option to Export Video clips from NVR Cameras' live streaming.

From the NVR Camera live video view, click on the "**Switch to Recorded Video**" button (bottom-right).

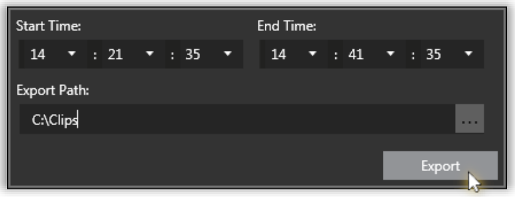

10.10.6.38 - Advidia - Model:
10.10.6.39 - Advidia - Model:
10.10.6.67 - ACTi - Model: TC
10.10.6.68 - ACTi - Model: TC
10.10.7.129 - Model: Panason
/300-LIVE
I-NX300-10.10.6.210-4
CAM6
CAM7
CAM2
CAM3
eras
Maintain Aspect Ratio

The Camera Playback view will open in a new window.

Click on the "**Export Video Clip**" button at the bottom right corner (gray).



Select the Start Time, End Time and file path for the clip, then click on "**Export**" to begin the operation.

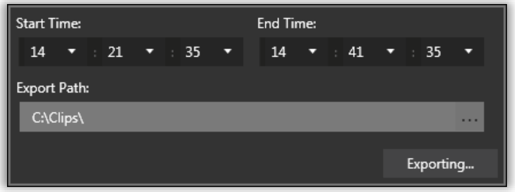


Start Time: 14 : 21 : 35

End Time: 14 : 41 : 35

Export Path: C:\Clips

The export clip sequence will begin. Once completed, the "Exporting" window will disappear, going back to the Camera Playback.



Start Time: 14 : 21 : 35

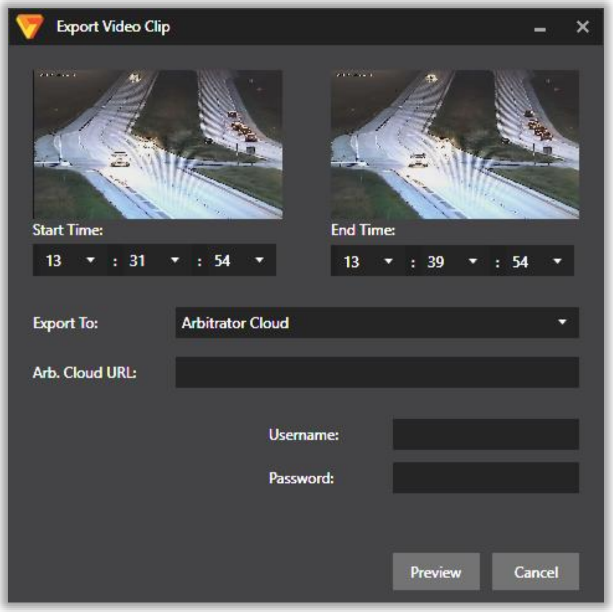
End Time: 14 : 41 : 35

Export Path: C:\Clips\

NOTE - The Video Clip files will be generated in **AVI** format.

4.7.G Panasonic Arbitrator Cloud Export

To export files to **Panasonic Arbitrator Cloud**, use the Export Video Clip menu to send the video clip. First, select the date and time you wish to create a clip. Next, select Arbitrator Cloud from the Export to drop down.



Export Video Clip

Start Time: 13 : 31 : 54

End Time: 13 : 39 : 54

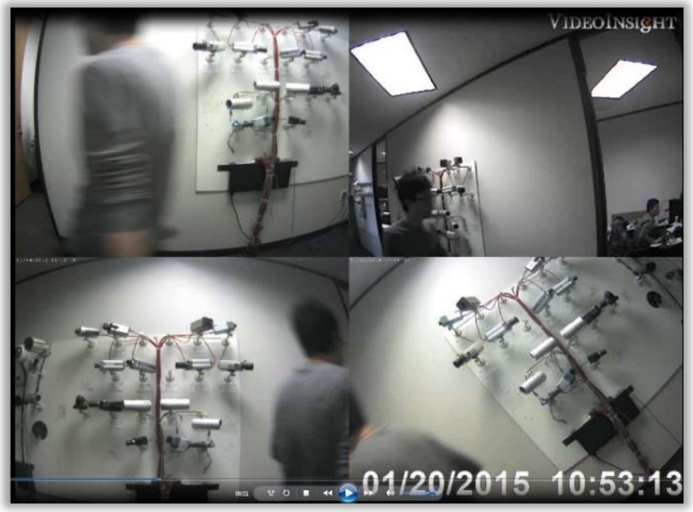
Export To: Arbitrator Cloud

Enter the correct Arbitrator Cloud URL and authenticate with your Arbitrator Cloud username and password. Select Preview to generate the clip preview for verification. Once connected the Arbitrator Cloud server, you will be allowed to enter in case details along with classifications for the case. This video clip will be stored on your Arbitrator Cloud system for future review along with the details supplied for the case.

4.7.H Multiplex Video

While exporting a clip, there is an option to keep all video in the appropriate layout when making a clip. This is done by selecting **Multiplex Video** during the file export.

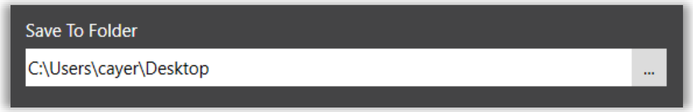
The output will display all involved layouts in a single AVI file and all views will be shown on the playback. See example image below of **AVI** playback.



If **Multiplex Video** is not selected, then the output file will default to the previously selected options located above the Multiplex Video checkbox.

Each recording will be exported individually, until all have completed, before the video is compiled and ready to be presented in this view.

The maximum number of cameras in the viewable area is limited to 16 cameras at the time of publication.


Save To Folder

C:\Users\cayer\Desktop

The **Save to Folder** option can be selected to change the default destination directory for storage.

4.7.I Region of Interest Motion Search (ROI)

Region of Interest Motion Search (ROI) allows the user to draw a box within previously recorded video view and to monitor changes within that specific area over a desired time frame. This feature enables the user to capture the moment that a change occurred within a visible region on the recorded video.

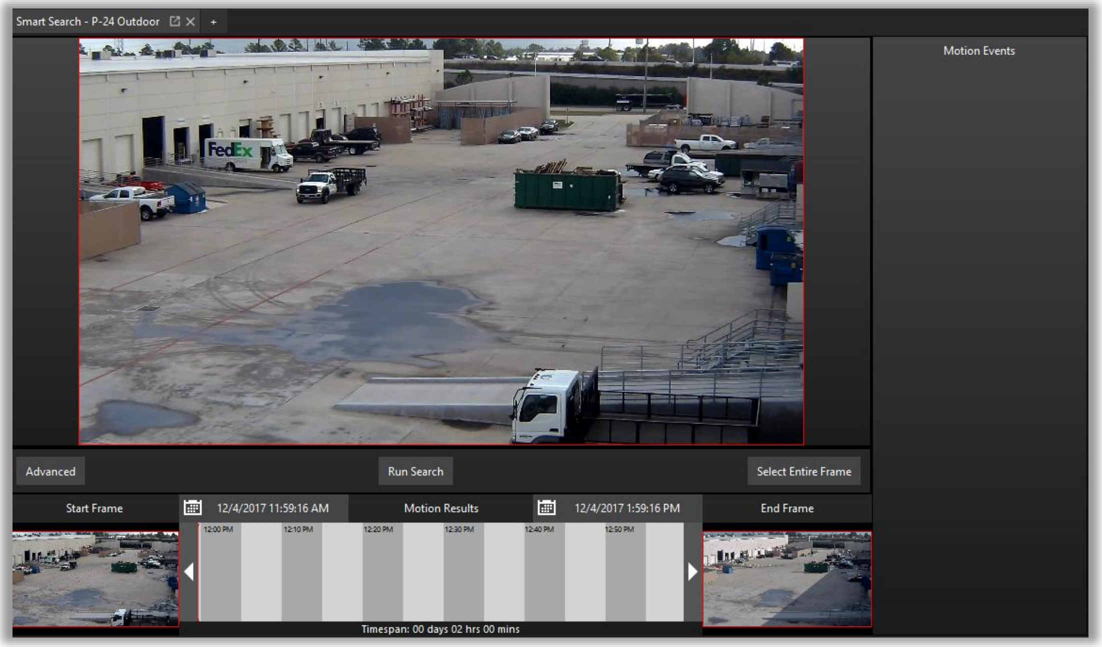
NOTE - The use of ROI Motion Search does not *require* a hardware-based GPU to conduct searches. When ROI Motion Search is not used with a hardware-based GPU, as outlined in the IP Server requirements, the search results will be performed in software-only mode. This can be very slow. It is highly recommended that a graphics processor, as listed in the Requirements for the hardware decoding (Hardware Decoding) is used for best performance output.

The use of ROI requires a 64-bit OS and VI MonitorPlus installation.

The ROI Motion Search feature compares frames within a recorded video to determine that enough pixilation change has occurred. When combined with the Region of Interest specified with the recorded video frame itself, the search conducted within the recorded video become much more glandular, yielding higher positive search results.

NOTE - It is recommended that ROI is used within a single workspace. Opening multiple workspaces to use with ROI will result in performance degradation and undesired results.

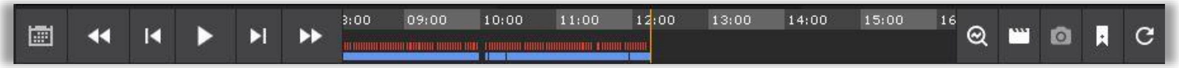
To get started with ROI Motion Search, follow the steps below:



Select a camera with recorded video where an event is thought to have occurred.

Next, select the Recorded Video icon, found in the bottom right-hind side of the screen (see left).

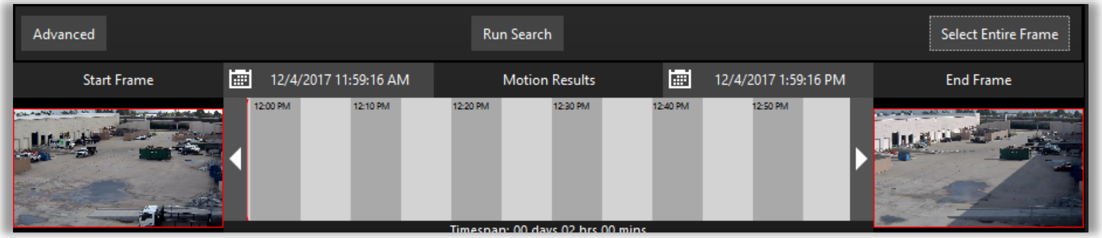
The recorded video timeline appears (see below)



On the right-hand side of the timeline the ROI Motion Search icon appears (see left).

Click on this icon, and the workspace refreshes with a new timespan bar.

In the image below, a Timespan bar appears.



The Timespan bar located between the Start Frame and the End Frame is the timespan in which a search is conducted. The Timespan Bar can be used for quick access to more recent events. To use it, click and drag the time bar to the point in time that the recent event may have occurred.

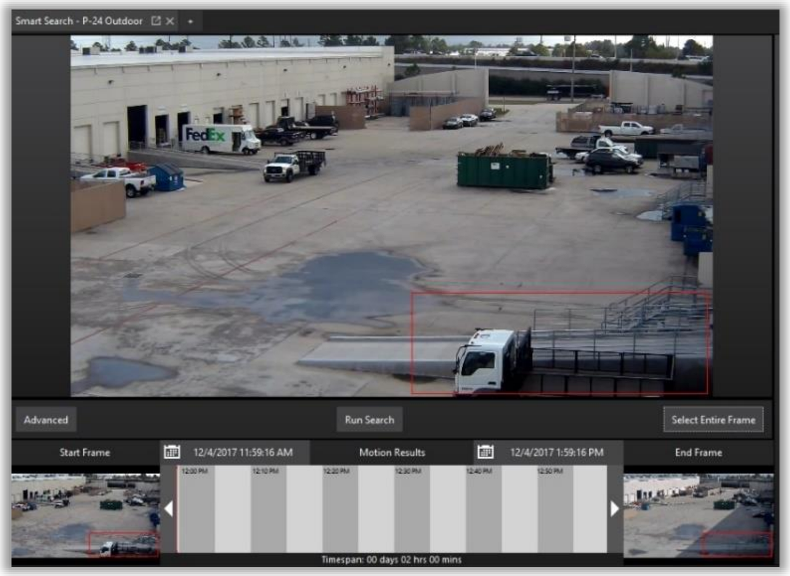
NOTE - The use of ROI with fisheye cameras has a visual playback limitation. Dewarping and Quad-View features are not processed by IP Server while recorded video is displayed on the screen within the ROI search. Video playback for fisheye cameras will appear in fisheye-view only. ROI video clips made from fisheye cameras will play back in fisheye view only.

NOTE - If it is necessary to conduct a search over a greater span of time, it is an option to use the two calendars above the timespan bar to specify exact start and end times across a period of days.

NOTE - The use of network-bandwidth conserving features, such as Panasonic Smart Coding, can negatively impact the ROI search results where bandwidth settings on the camera are maximized for network efficiency. It is recommended that an acceptable balance between these two features be tested to match the preferences of the administrator prior to production use.

At the time of publication, the ROI Motion Search feature is limited to searching previously recorded video that is accessible within VI MonitorPlus and only within a 30-day range. This limitation is due to the possibility that a search is conducted beyond the scope of available video recordings.

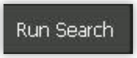
The **Start Frame** acts as a visual point of reference, used for quickly scrolling through the **Timespan Bar**. It displays the very first frame from the video recording for use by ROI Motion Search. The **End Frame** is a visual guide and visual point of reference for quickly scrolling through the **Timespan Bar**. It displays the very last frame from the video recording used for a ROI Motion Search.

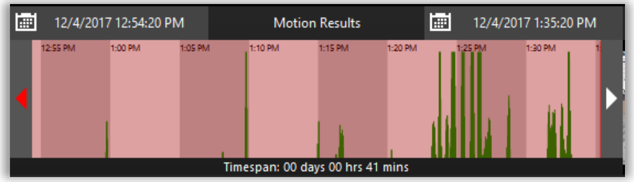


After the selecting the desired start frame, click and drag across the image in an area on the recorded video.

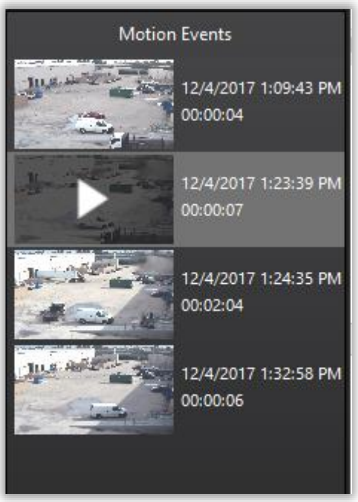
This creates the Region of Interest for searching with the ROI Motion Search feature.

Click on **Run Search**.





During the search process, the Timespan bar will begin to populate potential hits- found within the frame reference. When the green shaded area extends beyond the Timespan bar, the likelihood that some motion has occurred within the Region of Interest.



Motion Events

12/4/2017 1:09:43 PM
00:00:04

12/4/2017 1:23:39 PM
00:00:07

12/4/2017 1:24:35 PM
00:02:04

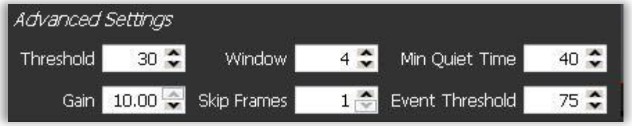
12/4/2017 1:32:58 PM
00:00:06

The Motion Events section, found on the right-hand side of the screen, will begin populating with clippings of motion events- found within the specified Region of Interest.

To view one of the Motion Events, double-click on one of the visible images. A new pop=up window appears.

This window allows the user to view the specific motion event within a stand-alone player. The player is designed to be compatible by default with any of the required operating systems for IP Server.

Advanced Settings



Advanced Settings

Threshold 30 Window 4 Min Quiet Time 40

Gain 10.00 Skip Frames 1 Event Threshold 75

The table below offers a description of the items that appear within Advanced Settings.

Threshold	Threshold represents the minimum deviation of a value within a pixel, for that pixel to be considered "changed" within the recorded video.
Gain	This adjusts the motion detector's sensitivity to change.
Window	Represents the number of overlapped video frames that are used to determine if a pixel has changed.
Skip Frames	Motion analysis is done only on key frames
Min Quiet Time	The number of seconds that must pass where no motion has been detected, before a new motion event is created
Event Threshold	The percentage of pixels that must change within the Region of Interest before a new motion is created

4.8 TAB: MODULES

4.8.A Access Control

(1) ACCESS VIEW

(1A) ACCESS VIEW CONFIGURATION

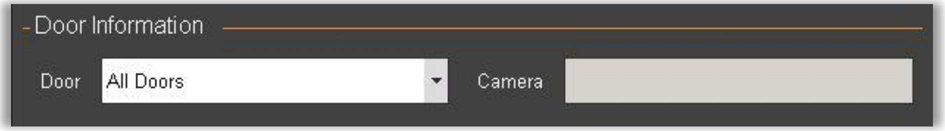
Access View is the user facing interface to Access Control servers that can be implemented into IP Server and VI MonitorPlus. The newly arranged feature set was designed to maximize ease of use and to provide the user with the necessary details of each Access Control event.

This screen will only become relevant when IP Server is integrated with an Access Control server. Otherwise, this screen offers no additional / functional features for the User.

(1B) ACCESS VIEW CONTROLS

Door Information

Door information allows the user to select a specific door, and see which camera is assigned to that door. The default is to show All Doors, which limits the ability to display all doors at the same time in the Live View window below. This is intended to be used as quick access to a specific door where there may be an alarm event that needs to be rectified with human interaction.



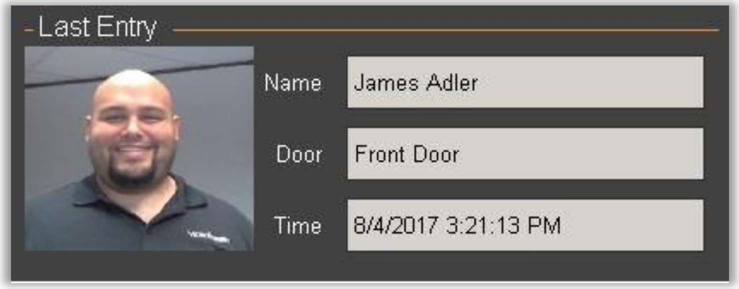
Door Information

Door: All Doors

Camera:

LAST ENTRY

Last Entry displays the information pertinent to an **Access Control** device being accessed. Depending on the depth of Administrative Management used and incorporated into a person's account, the features available here are the display of a photo of the individual that attempted to access the secured area



Last Entry

Name: James Adler

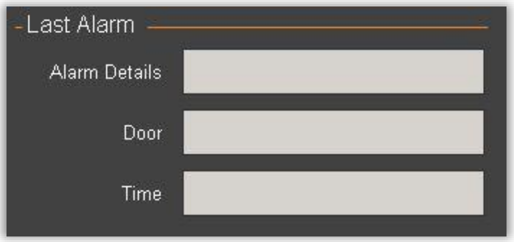
Door: Front Door

Time: 8/4/2017 3:21:13 PM

Seen left, are the person's name, the name of the door that was being accessed (for use with **Door Information,** above), and the **Time** of the last attempted/successful/failed entry.

LAST ALARM

Last Alarm provides the user with the type of alarm that triggered the door, the event that triggered an alarm and provides the time that the alarm was triggered.



Last Alarm

Alarm Details:

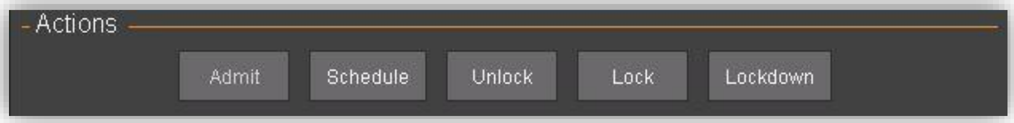
Door:

Time:

This is a live feed provided to the user, in the event there is a need for manual interaction, to easily elect to choose the door from **Door Information** (above) and then select one of the following **Actions** (see *Actions* image, below).

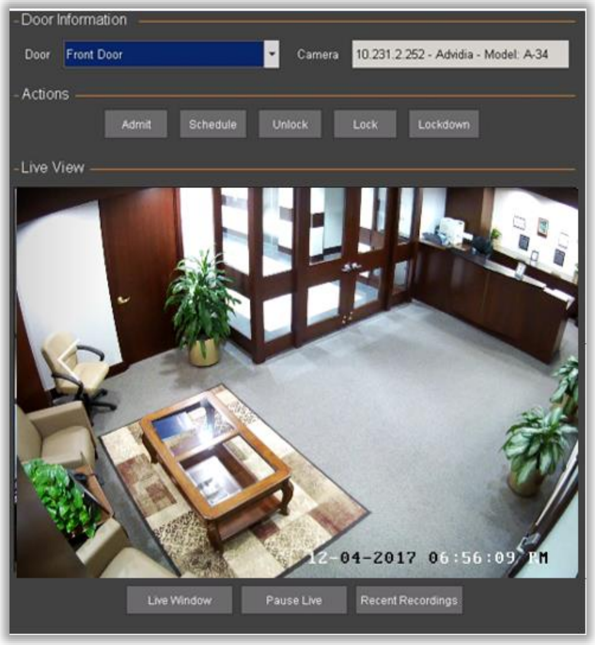
ACTIONS

Actions are a list of functional items available to the user for controlling a single door, if it is being viewed, or ALL DOORS if **All Doors** is selected in the Door Information area, seen above. Use caution with any of these tools while viewing ALL DOORS in the Door Information area, above. If access control permissions have not been properly configured, undesired changes can result in some adverse effects on the IP Server.



Admit	Most commonly used with a live guard and a single door with a camera or a camera with a microphone. The Admit button provides manual authorization for entry. Because it is a manual authorization, the action is tracked within the system logs for IP Server
Schedule	This function, when selected, forces the door being viewed* into one of two states. The first state is to force the door being viewed back onto a previously programmed schedule if one is available. If there is no schedule available for the door, then it will force the door into the default setting on the controller card. Usually, the default on controller cards is for Card swipe/pin access depending on the reader card. ***Important note:*** *This will take any visible door (or ALL doors, if ALL Doors are being viewed) out of Lockdown, scheduled mode if security settings are not properly configured on the access control server.*
Unlock	This feature will unlock a door being viewed, or all doors being viewed if ***All Doors** is selected in the drop-down menu within Door Information. **** Important note:*** *This will take any visible door (or ALL doors if ALL Doors are being viewed) out of Locked or scheduled mode if security settings are not properly configured on the access control server.*
Lock	This button will lock the door being viewed.
Lockdown	Selecting this button will force all doors to lock**.** Pressing this button will lock the door being viewed, or ***ALL DOORS** if viewing All Doors in the drop-down menu above. **** Important note:*** *This will take any visible door (or ALL doors, if ALL Doors are being viewed) out of Lockdown, scheduled mode if security settings are not properly configured on the access control server.*

LIVE VIEW



Door: Front Door

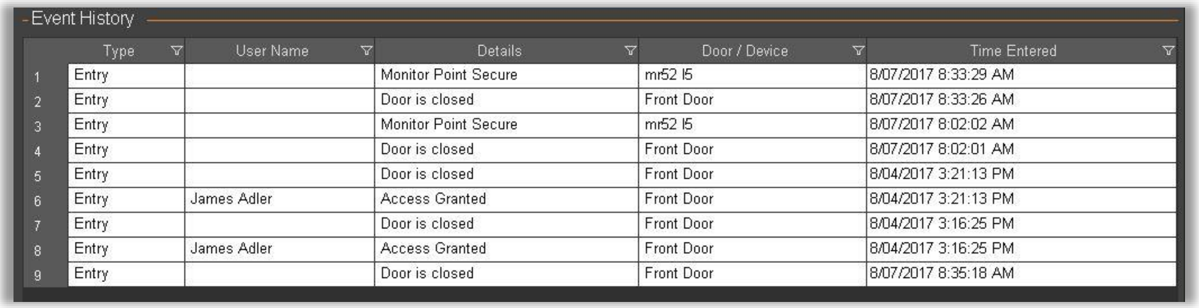
Camera: 10.231.2.252 - Advidia - Model: A-34

Live View displays a live stream of any camera that might be associated to a specific door, and then chosen from the Door Information drop-down menu.

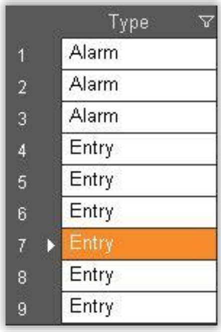
The ability to pause the live stream is available, and access to the Recent Recordings is also available for quick review of any potential or unexpected security violations.

EVENT HISTORY

Event History provides limited information that is pertinent to the Access View Controls, and the doors assigned to the Access Control server. Information made available are as follows:

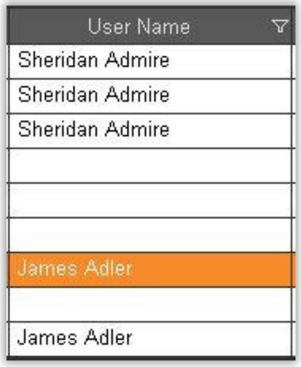


	Type	User Name	Details	Door / Device	Time Entered
1	Entry		Monitor Point Secure	mr52 I5	8/07/2017 8:33:29 AM
2	Entry		Door is closed	Front Door	8/07/2017 8:33:26 AM
3	Entry		Monitor Point Secure	mr52 I5	8/07/2017 8:02:02 AM
4	Entry		Door is closed	Front Door	8/07/2017 8:02:01 AM
5	Entry		Door is closed	Front Door	8/04/2017 3:21:13 PM
6	Entry	James Adler	Access Granted	Front Door	8/04/2017 3:21:13 PM
7	Entry		Door is closed	Front Door	8/04/2017 3:16:25 PM
8	Entry	James Adler	Access Granted	Front Door	8/04/2017 3:16:25 PM
9	Entry		Door is closed	Front Door	8/07/2017 8:35:18 AM



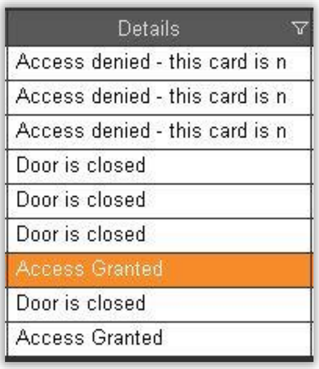
	Type
1	Alarm
2	Alarm
3	Alarm
4	Entry
5	Entry
6	Entry
7	Entry
8	Entry
9	Entry

Type: This list denotes whether the type of access was an entry or exit, if a second card reader is implemented inside of the secured area.



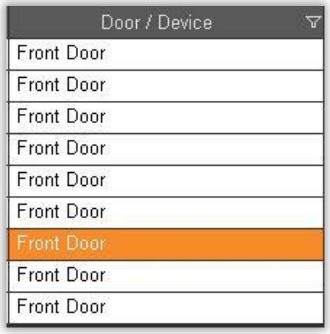
User Name
Sheridan Admire
Sheridan Admire
Sheridan Admire
James Adler
James Adler

User Name: This is the name of the person that is associated with the access control card/pin number/voice recognition device that has been given or denied access to the secured area.



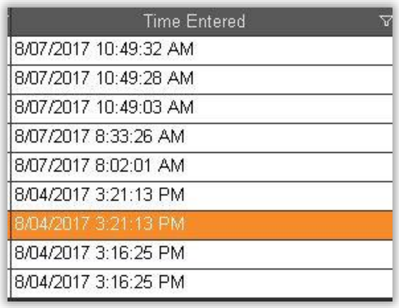
Details
Access denied - this card is n
Access denied - this card is n
Access denied - this card is n
Door is closed
Door is closed
Door is closed
Access Granted
Door is closed
Access Granted

Details: This provides a running list of items that of more specific events that may have occurred. The scope of this detail information provides a quick view of helpful information that affords the user to discern if an actionable task needs to be performed, or if some sort of maintenance needs to be done. In general, it is a running log of devices, controls, users, and times of events.



Door / Device
Front Door
Front Door
Front Door
Front Door
Front Door
Front Door
Front Door
Front Door
Front Door

Door/Device: A list of the specific device where an event has occurred.

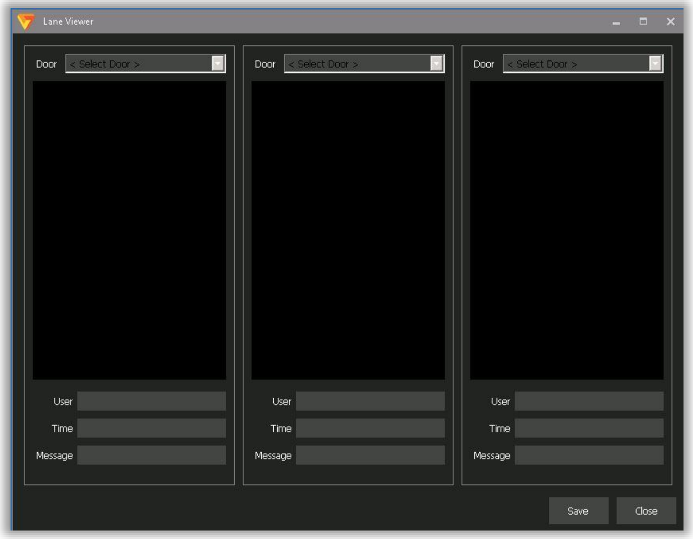


Time Entered
8/07/2017 10:49:32 AM
8/07/2017 10:49:28 AM
8/07/2017 10:49:03 AM
8/07/2017 8:33:26 AM
8/07/2017 8:02:01 AM
8/04/2017 3:21:13 PM
8/04/2017 3:21:13 PM
8/04/2017 3:16:25 PM
8/04/2017 3:16:25 PM

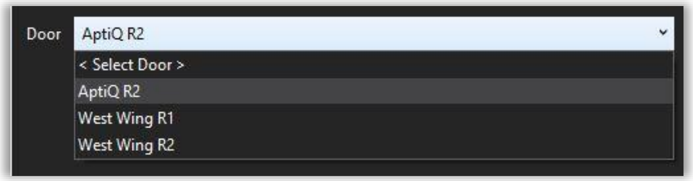
Time Entered: Date and time of recorded event.

(2) LANE VIEWER

Designed to work with MonitorCast, selecting Lane viewer from the Modules Tab opens a window that displays three doors. The purpose of lane viewer is to allow a person (typically security personnel) to monitor for issues that might arise with a specific door or camera. These settings can be modified, in the Administration section for Lane Viewer.



By default, when Lane Viewer is opened, the appearance of three doors/cameras appears.

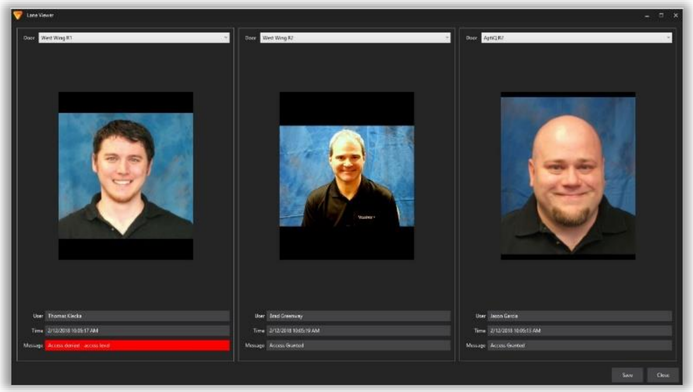


The first step for configuring Lane Viewer, after it is opened, is to assign a door to one of the views.

Do this by selecting the drop-down menu at the top of the lane viewer display.

After the doors have been assigned to each desired Lane Viewer view window, the configuration is complete.

Each time an individual uses an access badge, or key code for entry, the information that has been associated to that person within the MonitorCast database appears.



Door: West Wing R1
User: Thomas Klecka
Time: 2/12/2018 10:05:17 AM
Message: Access denied access level

Door: West Wing R2
User: Brad Greenway
Time: 2/12/2018 10:05:19 AM
Message: Access Granted

Door: AptiQ R2
User: Jason Garcia
Time: 2/12/2018 10:05:13 AM
Message: Access Granted

When pictures are associated with personnel at the site using MonitorCast, the image of that person is displayed on the screen when the access control card/code is used.

Where no image is associated, a default image stating, "No Image" appears.

4.9 TAB: SYSTEM

The System tab provide administrative functions that will have an effect within VI MonitorPlus. These administrative controls and function do not necessarily have a direct impact on the IP Server itself, and are centered around visual enhancements and User-level personalization for the client interface.

4.9.A Licensing

Licensing, within this section is directly related to single-use instances of H.265 licensing. H.265 licensing is done entirely client-side, on a per-installation basis. Panasonic wishes to respect the terms of the license and has implemented this minor adjustment to the licensing feature to comply with the H.265 licensing agreement.

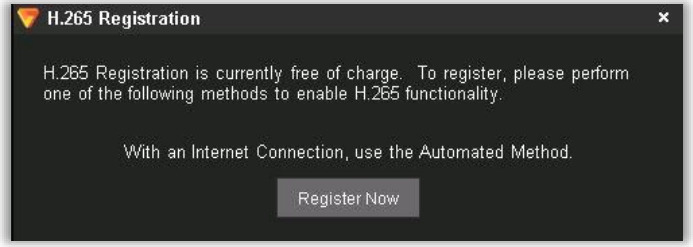
(1) H.265 ON-LINE REGISTRATION

The registration process does not require the collection of any data that will identify a person. Panasonic does not collect a name, address, phone number, email address or other any other personal information.

NOTE - H.265 Cameras that are not registered will record video, however the video playback of H.265 cameras will not permit the user to view the recording without registration. Registration is required on each computer that VI MonitorPlus is installed and used with H.265 cameras.

To register any qualified Panasonic Camera for H.265 Camera Licensing, navigate to **System > Licensing > H.265**.

(1A) AUTOMATED REGISTRATION



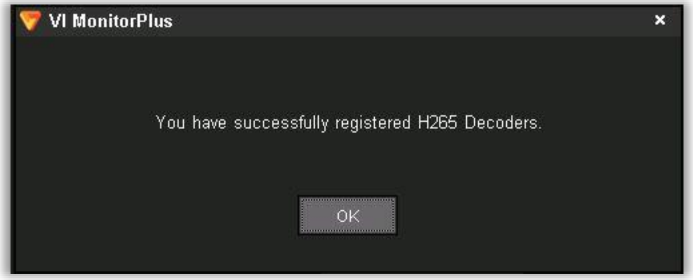
H.265 Registration

H.265 Registration is currently free of charge. To register, please perform one of the following methods to enable H.265 functionality.

With an Internet Connection, use the Automated Method.

If the computer registering H.265 has internet access, the automated method of registering is 2 steps:

Step 1: Select the **Register Now** button.



VI MonitorPlus

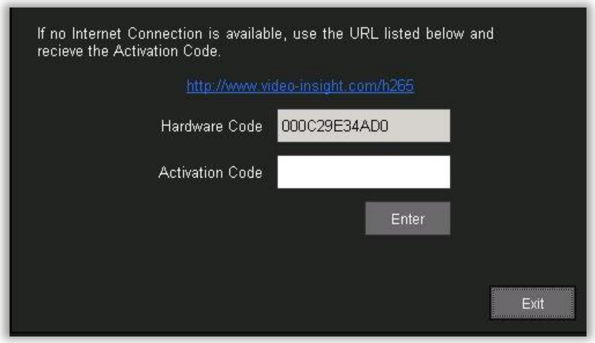
You have successfully registered H265 Decoders.

A new pop-up window appears, confirming that registration of H.265 is complete.

Step 2: Click **OK** to exit the registration process.

(1B) MANUAL REGISTRATION

For computers using VI MonitorPlus on a closed-network environment, without internet access, the process for registering H.265 was made to be as simple as possible. This process can be done on a cell phone, or by calling Technical Support.



If no Internet Connection is available, use the URL listed below and recieve the Activation Code.

http://www.video-insight.com/h265

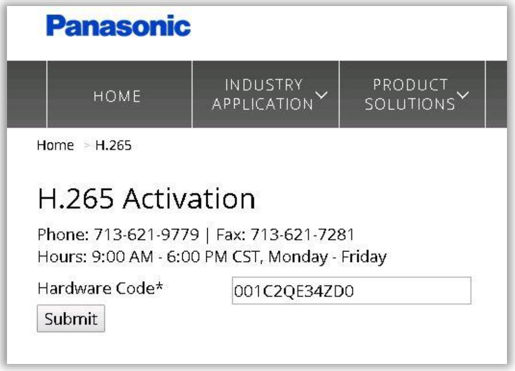
Hardware Code: 000C29E34AD0

Activation Code:

Step 1: Copy the URL for H.265 registration.

Step 2: Copy the hardware code provided.

Step 3: On a device that does have access to the internet, enter the URL and go to the page for registration.



H.265 Activation

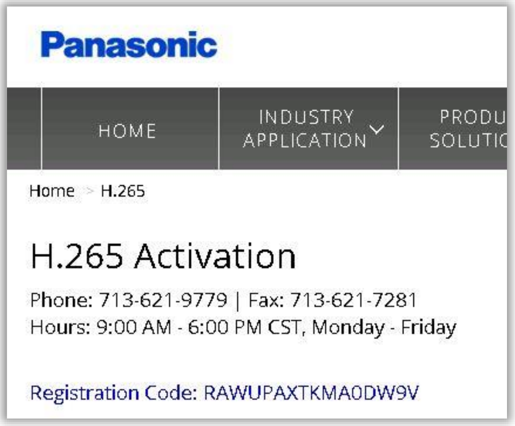
Phone: 713-621-9779 | Fax: 713-621-7281
Hours: 9:00 AM - 6:00 PM CST, Monday - Friday

Hardware Code*: 001C2QE34ZD0

Once the webpage loads, continue with these steps:

Step 4: Enter the hardware code for the computer that will use H.265 video playback within VI MonitorPlus

Step 5: Select **Submit**



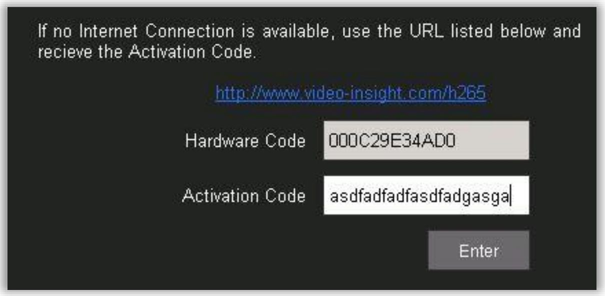
H.265 Activation

Phone: 713-621-9779 | Fax: 713-621-7281
Hours: 9:00 AM - 6:00 PM CST, Monday - Friday

Registration Code: RAWUPAXTKMA0DW9V

The next page appears with the registration code.

Copy this code and take it to the computer without internet access.



If no Internet Connection is available, use the URL listed below and recieve the Activation Code.

http://www.video-insight.com/h265

Hardware Code: 000C29E34AD0

Activation Code: asdfadfadfasdfadgasga

Step 6: Enter the registration code into the Activation Code area.

Step 7: Click **Enter** to complete the registration process.

H.265 is now registered. Video recorded on H.265 cameras will playback without any issues.

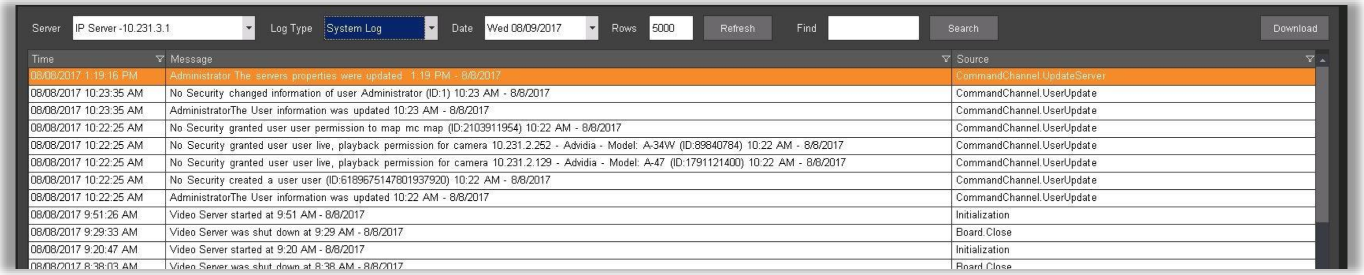
4.9.B Event Viewer Details

Event Type	Description
Access Control Manager	
AccessAlarm	General notification that access has occurred or access has been attempted.
AccessEntry	General notification that an entryway was opened or closed
DoorAlarmed	Denotes that a door alarm was triggered for the time and date specified. Please verify that the door is functioning properly.
DoorLockStatus	Will signify if a door is locked or unlocked
DoorState	Status of a door - on/off/connected/not connected
IP Server Event Messages	
CameraDown	IP Server is reporting that it does not have access to the camera specified. Please check username, password and network connectivity issues.
CameraMotion	Notification of a motion event. Meaning, motion occurred within the field of view on the camera that has been specified.
CameraRestored	IP Server reporting that it can now connect to the previously downed camera.
ClientMessage	A message was sent from one user to another user.
LiveWindow	Live window was activated by a user, or rule.
IP Server Rules Manager output	
AlarmWindow	This will appear when there is a rule setup to trigger a pop-up window for access control.
ExecuteProgram	Within Rules Manager, if the option to execute an additional program outside of IP server is requested, this will appear within the logs.
InstantReplay	This represents a call by a logged in user to perform an instant replay task.
LPRAlarm	This item appears with the use and activation of LPR services.
MessageAlert	This indicates that a message alert pop-up was triggered and displayed.
SwitchToCamera	During the Tour feature, this indicates changing views between cameras.
SwitchToServer	This indicates that that specific server was selected from the main menu.
SwitchToLayout	This indicates a change in the number of visible cameras.
SwitchToAudio	This indicates the activation of Audio with cameras capable of capturing audio.
License Plate Recognition (LPR) related messages	
LPREvent	This denotes any event that may have occurred with the use of LPR software and cameras. If you are not using LPR functionality, then this message can be disregarded.
Video WallPlus	
ChangeMatrix	This indicates a change in the layout of the monitor views, or matrix.
DBDown	SQL Query failure. Most commonly a temporary SQL connection issue. Please verify that the SQL server is not experiencing any issues.
DBRestored	SQL query connection successful. Seen at IP Server startup as well as after a failed query has been triggered.

4.9.C System Log

System log provides data useful to the administrator searching for specific events.

In this log, the Admin will find the option to select a specific server's logs (if multiple servers are connected to VI MonitorPlus), the type of log, the ability to sort by date, the number of rows to display in the log, the ability to search for a specific keyword, and the ability to download the sorted data once it is found.



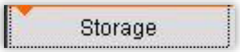
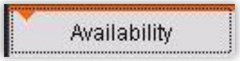
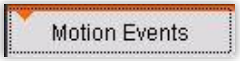
Server: IP Server -10.231.3.1 | Log Type: System Log | Date: Wed 08/09/2017 | Rows: 5000

Time	Message	Source
08/08/2017 1:19:16 PM	Administrator The servers properties were updated 1:19 PM - 8/8/2017	CommandChannel.UpdateServer
08/08/2017 10:23:35 AM	No Security changed information of user Administrator (ID:1) 10:23 AM - 8/8/2017	CommandChannel.UserUpdate
08/08/2017 10:23:35 AM	AdministratorThe User information was updated 10:23 AM - 8/8/2017	CommandChannel.UserUpdate
08/08/2017 10:22:25 AM	No Security granted user user permission to map mc map (ID:2103911954) 10:22 AM - 8/8/2017	CommandChannel.UserUpdate
08/08/2017 10:22:25 AM	No Security granted user user live, playback permission for camera 10.231.2.252 - Advidia - Model: A-34W (ID:89840784) 10:22 AM - 8/8/2017	CommandChannel.UserUpdate
08/08/2017 10:22:25 AM	No Security granted user user live, playback permission for camera 10.231.2.129 - Advidia - Model: A-47 (ID:1791121400) 10:22 AM - 8/8/2017	CommandChannel.UserUpdate
08/08/2017 10:22:25 AM	No Security created a user user (ID:6189675147801937920) 10:22 AM - 8/8/2017	CommandChannel.UserUpdate
08/08/2017 10:22:25 AM	AdministratorThe User information was updated 10:22 AM - 8/8/2017	CommandChannel.UserUpdate
08/08/2017 9:51:26 AM	Video Server started at 9:51 AM - 8/8/2017	Initialization
08/08/2017 9:29:33 AM	Video Server was shut down at 9:29 AM - 8/8/2017	Board.Close
08/08/2017 9:20:47 AM	Video Server started at 9:20 AM - 8/8/2017	Initialization
08/08/2017 8:38:03 AM	Video Server was shut down at 8:38 AM - 8/8/2017	Board.Close

4.9.D Server Statistics

Server Statistics displays the status of their IP Server Enterprise system.

Each of the features below will display a column for Active Servers and a separate column for Inactive Servers. Within each of these two columns, the total number of serves and cameras will be displayed. This is most useful for Administrators of large, multi-server installations.

	Provides a general look at what VI MonitorPlus is connected to. In addition to the **Active** and **Inactive** columns described above, the lower chart provides **Server Name**, **IP Server Version**, **Server IP Address, Serial Number**, **Maximum Number of Cameras** attached to the server, the number of available cameras, the number of cameras being used, and the number of bundled licenses associated with the cameras.
	Provides the **Server Name**, the processor usage on that server, the total amount of memory available and total amount of memory for the server itself, and the OS Bit Type.
	Provides the **Camera Name**, **IP Address**, **Server Name**, **Last Image Received**, **Last Image Written**, **Resolution**, **Frames**, **Frame Size**, **Bandwidth**, **Format**, **Camera MD** (Modified YES/NO), **Manufacturer**, **Model** and **Web Access** (opens a new browser session).
	Allows the Administrator to select a specific server (where multiple servers are connected) and view the amount of storage being used by each functioning camera. The chart displays **Camera Name**, number of days of recorded video, the total amount of space used by the camera and the specific folder where data is being written to.
	Provides the Administrator with the **Server Name**, the percentage of time that the server has been active since installation and activation, the length of time the server has been up, the amount of time the server has been down and the number of failures the server has encountered during the time it has been running.
	Provides the Administrator with a quick view of the system users that are logged in to any of the attached **IP Servers**. The chart provides the User Name, the servers that the user is logged in to, the last task that the user performed, and any available actions that the Administrator might be able to make on that user, if available.
	Provides the Administrator with a variety of breakdown points for viewing and accessing specific dates and times of recorded **Motion Events**. The chart breaks down with the use of actionable buttons, used to display or hide the information in a hierarchal schema, starting at the server level, and working its way down camera by camera.
	Provides the administrator with a chart that displays the **Camera ID**, **Camera Name**, **Start Time** (for edge recording), **End Time** (for same Edge Recording) the status of the recorded video and the **Percentage Complete** of total download of the recorded **Edge Video** in the event of an unexpected network failure.

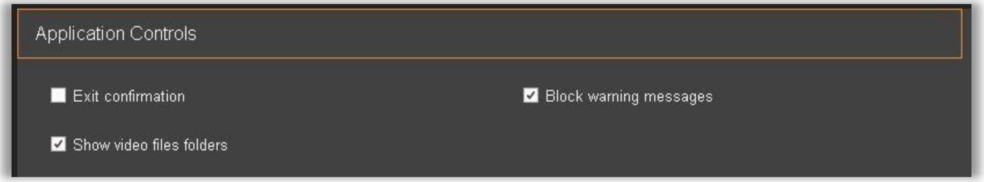
4.9.E Options

The **Options** section provides changes to the way that VI MonitorPlus looks, feels and operates. The changes made here are more for the general functionality of VI MonitorPlus itself, and not IP Server. For IP Server functionality, please refer to **Administration > Servers > Setup and Configuration**

(1) GENERAL

This tab gives the user access to various **Application Controls**, how VI MonitorPlus displays images, how VI MonitorPlus displays **PTZ controls**, and provides access to licensing the user's computer for H.265 camera use, as per the terms and conditions of the End User License Agreement.

(1A) APPLICATION CONTROLS



Application Controls

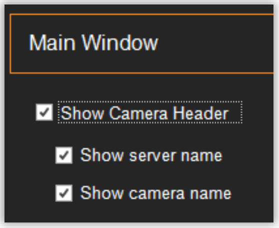
☐ Exit confirmation

☑ Block warning messages

☑ Show video files folders

Exit Confirmation	Selecting this checkbox will force a confirmation window to appear when exiting the menu. During the installation process, it is checked by default.
Show Video Folders	This option is incorporated to replicate the legacy Monitor Station video access folders. When checked, it will display a series of folders under each camera assigned to a server to provide the easiest access to recorded video possible.
Block Warning Messages	This option allows the Administrator to prevent the occasional pop-up warning boxes that may occur during advanced modification of the IP Server settings. This check box is not checked by default.

(1B) MAIN VIEW LAYOUT



Main Window

☑ Show Camera Header

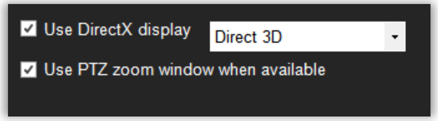
☑ Show server name

☑ Show camera name

In the center of the screen, on the right-hand side, is an area called **Main Window**. The first three options are, by default, checked:

- **Show Camera Header**
- **Show Server Name**
- **Show Camera Name**

If **Show Camera Header** is not selected, this feature will not work. If you must select this button, then VI MonitorPlus must be closed and restarted after steps have been completed.



☑ Use DirectX display Direct 3D

☑ Use PTZ zoom window when available

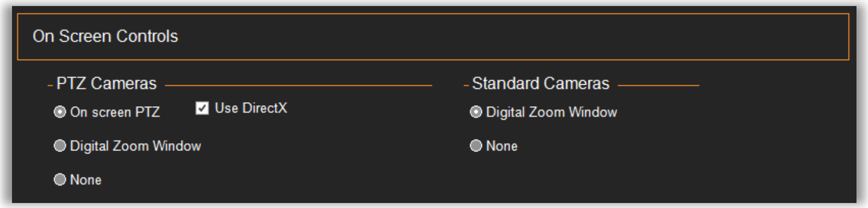
Use DirectX display

Forces the incorporation of the use of **DirectX** for control of certain video controller within the display for cameras that require **DirectX**.

Selecting **Use DirectX** will force VI MonitorPlus to manipulate cameras using a legacy DirectX controller. Please see Microsoft's DirectX support page for more information regarding DirectX and its requirements: https://www.microsoft.com/en-us/download/details.aspx?id=35

(1C) ON SCREEN CONTROLS

On Screen Controls modifies the appearance of PTZ controls and how they are displayed within VI MonitorPlus.



On Screen Controls

PTZ Cameras
- ● On screen PTZ ☑ Use DirectX
- ○ Digital Zoom Window
- ○ None

Standard Cameras
- ● Digital Zoom Window
- ○ None

On Screen PTZ: When selected, this feature enables PTZ controls while hovering over a PTZ camera.

Use Direct X opens a pop-up window that allows the visual use of a PTZ controller with PTZ camera functionality. The visual effect on the screen will appear as Arrows on the edges of the Live View screen, while viewing video on a PTZ camera.

Use PTZ zoom window when available: When this is not selected, there will be no visual controls seen along the edges of the screen. PTZ cameras will need to be moved by use of joystick, or by manipulating the camera with the use of the PTZ controller tools on the left side of the Live View Screen.

Digital Zoom Window: Allow the use of the camera's digital zoom feature, if available. Unchecking this box will disable digital zoom on cameras that may have the option available. This box is checked by default.

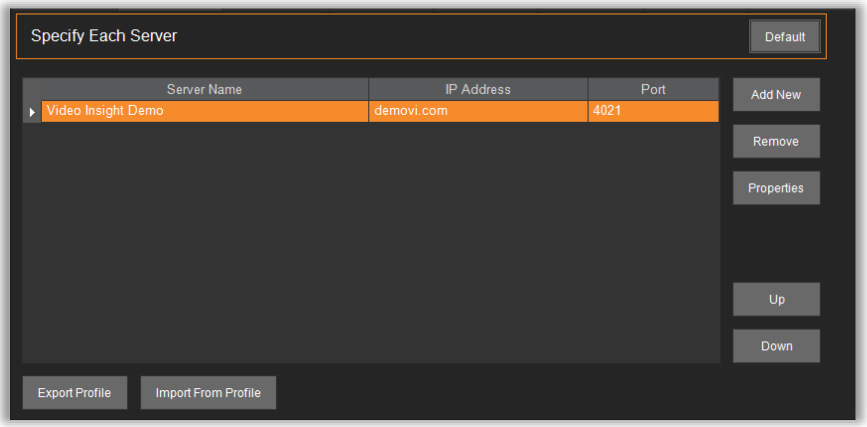
(2) CONNECTIONS

The Connections screen shows a list of all the servers currently added and allows the administrator, or user, to add or remove servers. The user can change the order of appearance for each of the IP Servers listed (above a single server), and to modify the properties of the server. The user can also map an exported profile, as directed by the administrator.

The user and or administrator can specify the location of a previously created **Server Profile**.

(2A) SPECIFY EACH SERVER

Is the interface where the Administrator or User will add, remove and view the properties of the server.



Specify Each Server

Server Name	IP Address	Port
Video Insight Demo	demovi.com	4021

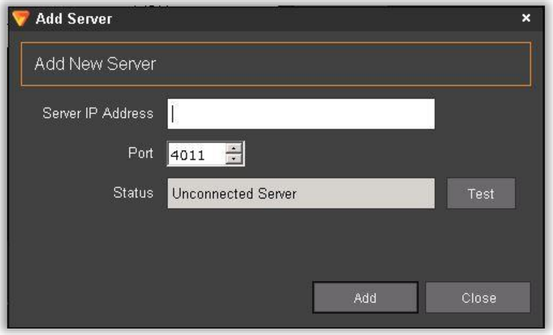
Click **Add New** to add a new server.

In the new window, enter the ***IP Address*** for IP Server.

If necessary, change the Port number to reflect the **Command Port** of the IP Server (Default is 4011).

Click on **Test**.

If the server connects successfully, a confirmation window will appear. Otherwise, verify the IP Address and the Port number.



Add Server

Add New Server

Server IP Address: |

Port: 4011

Status: Unconnected Server

NOTE – Server's IP and Port must be set by the user to successfully add a server. Using the *Set to Default* buttons resets the profile information for the selected server to default values

To Remove a server from the display, select the undesired server, and then click on **Remove**.

(2B) USE SERVER PROFILE

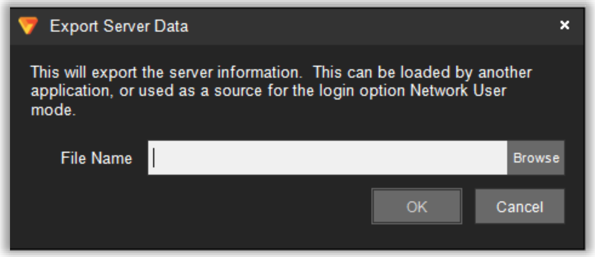
A server profile can be used to share between many installations of VI MonitorPlus where manually entering multiple server connections would prove to be time consuming.

Server information can be ***exported*** and ***imported***.

Click **Browse** to find a previously configured profile.

Click **OK**.

The profile will begin functioning at the next login.


Export Server Data

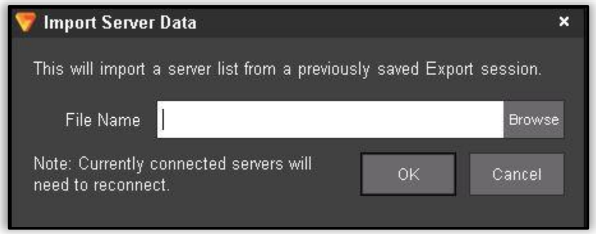
This will export the server information. This can be loaded by another application, or used as a source for the login option Network User mode.

File Name

To ***Export Server Data***, the user must select a server and click on **Export Profile**, which will pop up the Export Server Data window. Here, a file name must be set. Make sure to choose a file name that is easy to remember and still unique to the system.

The inverse process is also available by clicking on **Import From Profile**.

This will result in the displaying of the **Import Server List** window where users can browse and select a previously exported file.


Import Server Data

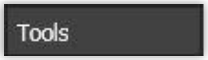
This will import a server list from a previously saved Export session.

File Name

Note: Currently connected servers will need to reconnect.

Any changes made to VI MonitorPlus will require an updated export of recent changes to successfully work across multiple machines. Placing the exported data on a NAS or SAS network share will make the ease of access to these features the easiest for network connected computers.

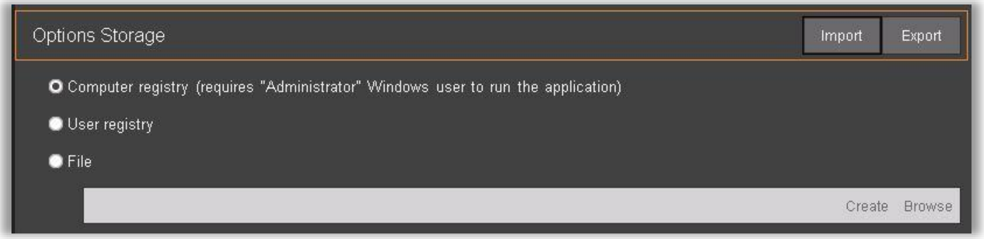
(3) TOOLS



The **Tools** tab allows some various changes such as XML and registry storage options, facility map alarms settings, and Guard Tours setting.

(3A) OPTIONS STORAGE(FOR OPTION CONFIGURATION))

This feature allows the IP Server administrator to customize VI MonitorPlus options and export the modifications that have been made on one machine and export them to another machine for ease of administration.


Options Storage

◉ Computer registry (requires "Administrator" Windows user to run the application)

○ User registry

○ File

The ability to push the settings through GPO (Group Policy Objects) is possible after making all desired changes to the VI MonitorPlus interface, and then exporting the settings to a location accessible by Microsoft GPO within Active Directory. This is considered an advanced feature and is not recommended without proper training in Microsoft Active Directory and GPOs.

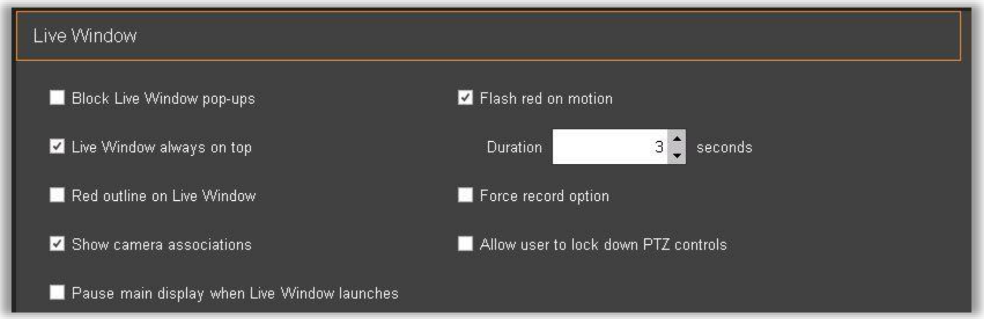
(3B) FACILITY MAP ALARM

Open Facility Map (Default: Checked)	This option, when the use of facility maps is in place and corresponding cameras and/or access control devices is used in conjunction with a facility map, will create a pop-up on the facility map-displaying the live view of the camera on top of the map when triggered.
Launch Live Window (Default: Checked)	When an alarm is triggered on a facility map, a live window will be displayed with a video image of the area where the alarm has been triggered.
Play Sound (Default: Not Checked)	The administrator can choose to use a .wav file to be played each time a facility map alarm has been triggered. The file can be placed on the machine, locally, or on a NAS/SAS storage device.

(4) LIVE DISPLAY

The **Live Display** screen provides settings for the visual appearance of the VI MonitorPlus application windows, display names for facility maps, utilize **Rules Manager** actions, provides access for controlling **Layout Tour** cycle times.

(4A) LIVE WINDOW



Live Window

□ Block Live Window pop-ups

☑ Live Window always on top

□ Red outline on Live Window

☑ Show camera associations

□ Pause main display when Live Window launches

☑ Flash red on motion

Duration 3 seconds

□ Force record option

□ Allow user to lock down PTZ controls

Block Live Window Pop-ups	Selecting this option prevents optionally program rules manager tasks, and / or images sent from other users from being displayed during a critical point in time. This feature can negate other desired settings, so use it with caution.
Live Window Always on top (Default: ON)	In the event a user selects to right-click on a camera and view a single camera display of a specific image, this prevents the live image from being covered by the rest of the VI MonitorPlus application.
Red Outline on Live Window	Selecting this option results in the appearance of a red outline around all motion-sensitive cameras where the server or the camera is reporting motion within the designated video display.
Show Camera Associations (Default: ON)	This feature is a legacy control which, at this point, will not have any effect on any screen. It will be removed in future releases.
Pause main display when live window launches	Prevents the streaming of video at the launch of VI MonitorPlus. It is useful to have this box checked when calling Technical Support as it prevents a spike in network saturation while logged in remotely to the IP Server.
Flash Red on Motion	Selecting this option results in the camera icons flash with a red border when motion is detected by the camera and/or server (dependent upon configuration). This is to enhance the ability to act quickly in camera locations that would otherwise not have much motion and to reduce potential of oversight if not enabled.
Force Record Option	Allows a user or administrator to override “motion only” and other settings and record video as it is being displayed within that moment. it will continue to record video on a selected camera until it has otherwise been turned off.
Allow user to lock down PTZ control:	Enables the hierarchical control of any PTZ camera associated with the IP Server. By enabling this option, an administrator can grant control of any camera to any person. If a subsequent person attempts to take control of the camera during an administrative viewing and use of the PTZ controls, that user will be denied the ability to change camera settings. The default time limit on PTZ camera control is 5 minutes without movement by the higher ranked user. Prioritization of PTZ controls is explained here: PTZ Prioritization

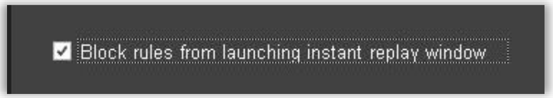
(4B) RULES MANAGER ACTIONS

Rules Manager default values are all ***unchecked***.

These are the available options:

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

> **NOTE -** These rules, when activated, can negate the purpose of alerts and notifications set by the administrator.



☑ Block rules from launching instant replay window

(4C) FACILITY MAP

This feature enables the visible server name for each facility map that has been created.

(4D) OTHER

Here, the user can opt to include a server name for all Layouts by selecting "Include server name for all Layouts."

Additionally, the **Camera Tour Interval** can be modified to suit the needs of the person viewing the camera tour.

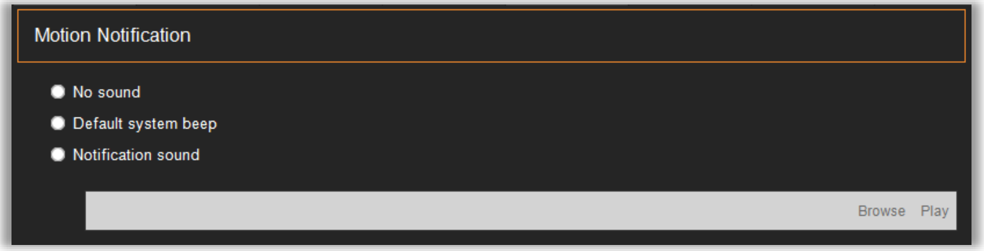
The user can also change the **Cycle Layouts interval**. Default value for these settings is **5** seconds.

(5) AUDIO

This screen allows user to decide if it is desired for audio to play with motion notifications, rules, or LPR alarms.

The options provided her are for Motion Notifications and Rules and Alarms. Each section allows for the option of No sound, Default system beep, and the selection of a custom audio file.

(5A) MOTION NOTIFICATION



Motion Notification

○ No sound

○ Default system beep

○ Notification sound

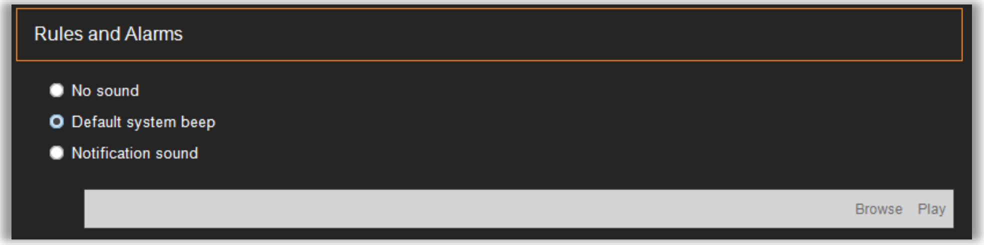
This section applies specifically to **Camera Motion** Settings.

If enabled, and IP Server or camera determines that there is motion occurring, causing a sound to play.

The option to choose a custom file is also available.

Using this feature requires that the computer have some sort of audio processing, and audio playback capability, that the audio playback capability is turned on, and that the user understands what the sound being played means in relation to the Motion Settings. in the computer's directory. The accepted file playback type is .WAV. No other file type has been tested.

(5B) RULES AND ALARMS



Rules and Alarms

○ No sound

● Default system beep

○ Notification sound

This section applies specifically to Rule triggers and for customers that use LPR (License Plate Recognition) with VI MonitorPlus.

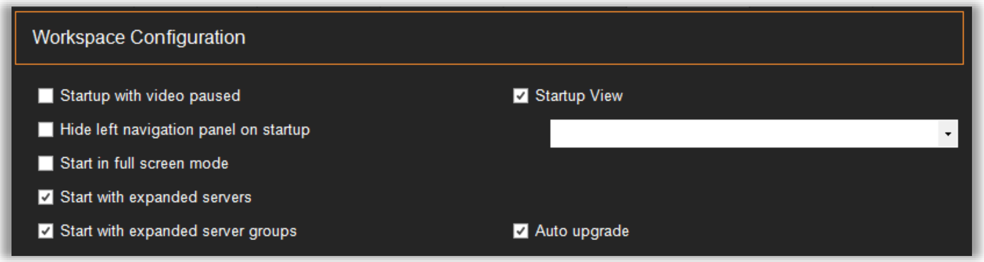
If a **Rule** has been created to produce sound under specific instances, or if LPR is triggered, a default sound will play.
The option to choose a custom file is available, if desired.

Using this feature requires a computer with audio processing and playback capabilities; the audio playback capability is turned on, and the user understands what the sound being played means in relation to the Motion Settings.

(6) STARTUP

(6A) WORKSPACE CONFIGURATION

Workspace configuration allows the user to set some visual defaults for viewing live and recorded video.



Workspace Configuration

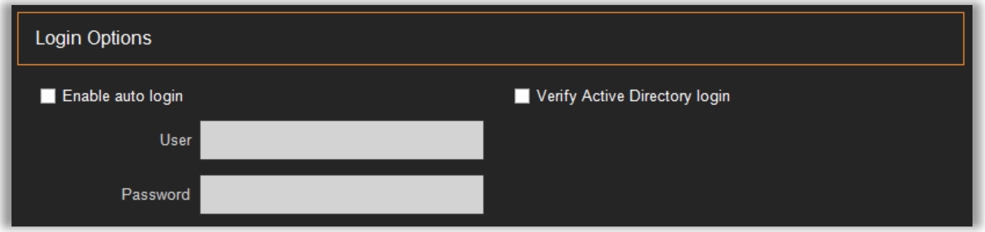
□ Startup with video paused
□ Hide left navigation panel on startup
□ Start in full screen mode
☑ Start with expanded servers
☑ Start with expanded server groups
☑ Startup View
☑ Auto upgrade

Startup with video paused	In some low-bandwidth environments, it may be desired to start VI MonitorPlus with video paused. This can allow the user or the administrator to quickly access various features and controls without waiting for video feeds to begin displaying in the main workspace.
Hide Left Navigation panel on startup	In some cases, it may be desired to hide the left navigation menu from the user. Selecting this feature turns off the ability to view the left navigation menu.
Start in full screen mode	Selecting this feature turns on Full screen mode at startup.
Start with expanded servers	Selecting this feature will expand each of the servers that appear in the left column, to display all associated cameras. **NOTE -** If "Hide left navigation panel on startup" has been selected, this feature may override that setting.
Start with expanded server groups	If the administrator has created Server Groups, the ability to view them at startup is made available here. If there are no previously created Server Groups on any of the servers, selecting this check box will have no effect.
Startup View	When this checkbox is selected, the ability to select a previously created view for startup display is available. If there have been no previously created Views, this feature will not function properly.
Auto upgrade (Default: ON)	When selected, this feature will compare the version of IP Server to the version of VI MonitorPlus that is being used to log into IP Server.

NOTE - It is HIGHLY RECOMMENDED that all versions of VI MonitorPlus and IP Server match, to reduce the possibility of IP Server database corruption.

When there is a mismatch between IP Server and VI MonitorPlus versions, a pop-up window will appear, encouraging the user to upgrade accordingly.

Login Options

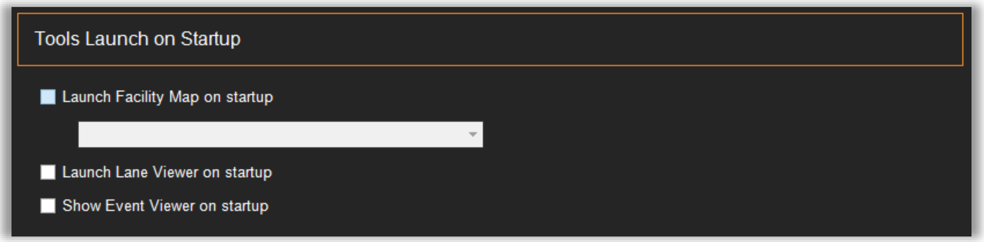


Login Options

□ Enable auto login
User
Password
□ Verify Active Directory login

NOTE - Enabling Auto login is a security risk and should not be enabled without fully understanding the implications and potential results of that action.

Tools Launch on Startup



Tools Launch on Startup

□ Launch Facility Map on startup

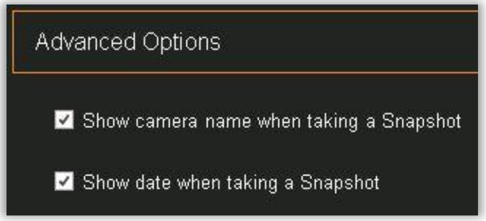
□ Launch Lane Viewer on startup

□ Show Event Viewer on startup

- **Launch Facility Map on startup** allows the user to select a previously configured facility map, and force it to be displayed when VI MonitorPlus is started, after logging in.
- **Launch Lane Viewer on startup** forces any previously configured Lane Viewer view to be displayed after logging in to VI MonitorPlus.
- **Show Event Viewer on startup** forces a separate window displaying the results of any previously configured Access Control configuration that has been previously configured.

(7) PLAYBACK

(7A) ADVANCED OPTIONS



Advanced Options

☑ Show camera name when taking a Snapshot

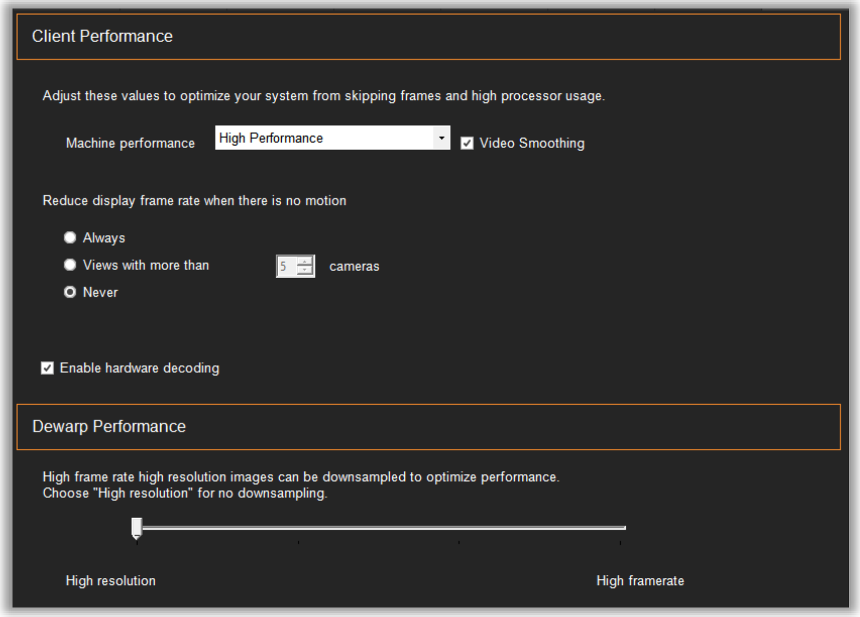
☑ Show date when taking a Snapshot

Show camera name when taking a Snapshot: Forces the VI MonitorPlus screen to display a camera name when taking a Snapshot. The default value is selected.

Show date when taking a Snapshot: Displays the date and time when taking a snapshot. The default value is selected.

(8) PERFORMANCE

This option allows users to alter the performance of their machines by changing a few settings. Additionally, it gives the Administrator the ability to change the capability for de-warping, on servers using 360 cameras, or cameras that have images that require the use of de-warping.



Client Performance

Adjust these values to optimize your system from skipping frames and high processor usage.

Machine performance: High Performance ☑ Video Smoothing

Reduce display frame rate when there is no motion

○ Always

○ Views with more than 5 cameras

● Never

☑ Enable hardware decoding

Dewarp Performance

High frame rate high resolution images can be downsampled to optimize performance.
Choose "High resolution" for no downsampling.

These options give users the possibility of increasing the performance of their machines by changing a few settings:

Reducing frame rate when there's no motion and down-sampling high resolution images (which can be done at different grades) are the options to be changed.

(8A) CLIENT PERFORMANCE

These setting directly affect the client-side VI MonitorPlus plus. They do not have any effect on IP server unless the client is being used on the IP Server itself. Selecting the desired Machine Performance will affect the CPU usage.

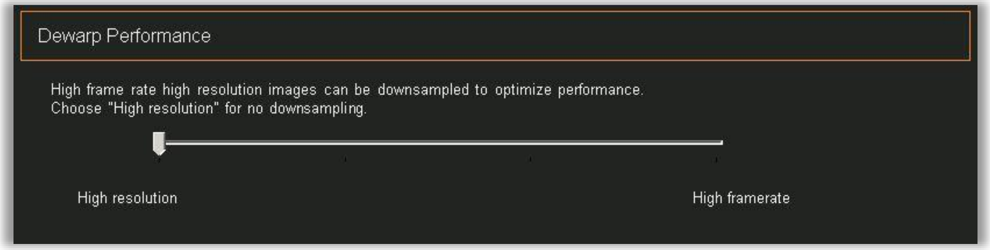
Video Smoothing is expensive for processors and should only be used on machines with significant computing resources.

Reduce frame rate capture can be useful on computers with lower end video cards. The default setting is **Never**. Selecting **Always** will produce a "choppy" view of the video being captured, but does not have any effect on the video recording itself. This is used to minimize resources and bandwidth consumption on older machines and/or over-utilized networks.

Enable hardware decoding: This feature will enable VI MonitorPlus to use hardware decoding. This will have a positive performance effect on H.264 and H.265 video codecs. If there is no Hardware Decoder the checkbox will not appear.

(8B) DEWARP PERFORMANCE

This feature impacts the IP Server performance when combined with 360° and 180° cameras with dewarping capabilities.



Dewarp Performance

High frame rate high resolution images can be downsampled to optimize performance.
Choose "High resolution" for no downsampling.

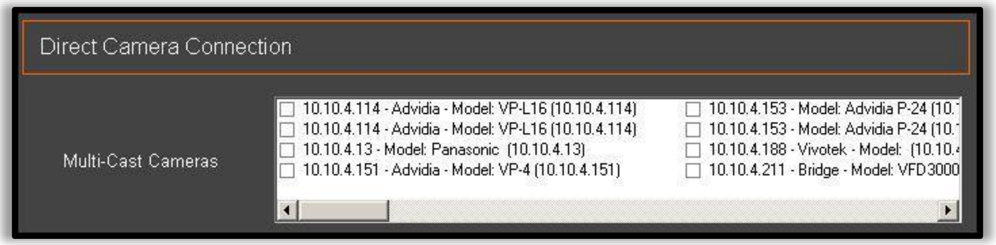
NOTE - If the IP server does not utilize any cameras with dewarped images, this setting will have no effect.

If cameras with dewarping features are available, the user can determine if higher framerates for viewing a steadier playback of live videos are necessary, or if more processing power with a reduction in fluid playback is desired.

(9) DIRECT CAMERA CONNECTION

In some instances, a direct connection to the cameras from a remote VI MonitorPlus on the local Network might be preferable.

Direct Live Video Streaming Support (Multicast) allows to select the cameras to be enabled. It requires a registry key modification ON the specific machine that will be using VI MonitorPlus. It also requires that the camera itself has built-in Multicast capability. (The configuration is in **System** → **Options** → **Performance**).



Direct Camera Connection

Multi-Cast Cameras

☐ 10.10.4.114 - Advidia - Model: VP-L16 (10.10.4.114)
☐ 10.10.4.114 - Advidia - Model: VP-L16 (10.10.4.114)
☐ 10.10.4.13 - Model: Panasonic (10.10.4.13)
☐ 10.10.4.151 - Advidia - Model: VP-4 (10.10.4.151)
☐ 10.10.4.153 - Model: Advidia P-24 (10.1
☐ 10.10.4.153 - Model: Advidia P-24 (10.1
☐ 10.10.4.188 - Vivotek - Model: (10.10.4
☐ 10.10.4.211 - Bridge - Model: VFD3000

There are two locations that can alternately be modified within the System Registry.

NOTE - The following registry keys should be modified prior to launching VI MonitorPlus.

For Windows x64 systems, the string value is to be added under this key:

HKLM\SOFTWARE\Wow6432Node\Video Insight\Monitor Station

For Windows x86 systems, the string value is to be added under this key:

HKLM\SOFTWARE\Video Insight\Monitor Station

The new string value is called **DirectLiveVideoSupport** and the following values can be added depending on the requirements:

- **0 value** = Disable, no UI options will appear
- **1 value** = Multicast cameras only, list will appear in the UI functions. Only those selected clients will engage directly with the camera
- **2 value** = Enable for All cameras

4.10 TAB: ADMINISTRATION

The items found under the administration tab will directly affect the IP Server itself. The controls used here will make changes on the IP Server itself, and will be a functional part of how IP Server is utilized within the organization.

4.10.A Servers Setup

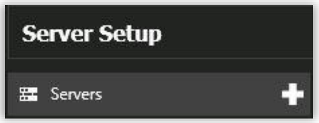
NOTE - All items under this tab will result in the modification of the IP Server configuration.

(1) SETUP AND CONFIGURATION

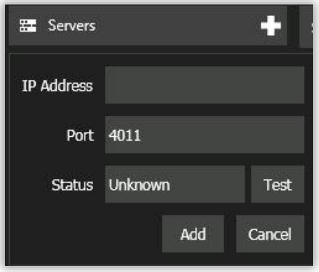
The only exception to this is adding a server to VI MonitorPlus. Without adding an IP Server to VI MonitorPlus, it will not be possible to edit or modify settings with the tools made available within VI MonitorPlus.

(1A) ADD A NEW IP SERVER TO VI MONITORPLUS

To add a new server to VI MonitorPlus, navigate to the **Administration** Tab and select **Server > Setup and Configuration**. A new window appears.



Click on the **+** symbol, and a new screen will appear.



IP Address

Port 4011

Status Unknown

Enter the information requested

- **IP Address**
- **Port Number** (default port number is 4011)

Once the information requested has been provided, click **Test**.

When successfully connected, the Status will change to the name of the server.

Click **Add**, or if the incorrect IP address was provided, click **Cancel** and restart.

Once a server has been added, it will appear in the main startup menu when logging into VI MonitorPlus for the first time.

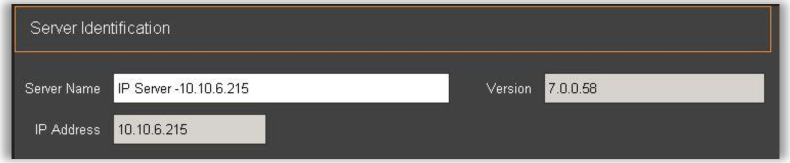
(1B) SERVER CONFIGURATION

Server Configuration

This section provides access to three critical items for ease of management as it applies to the IP Server selected from the left menu window. Those three sections are:

- Server Identification
- Database Information
- Video Storage

Server Identification



Server Name IP Server -10.10.6.215

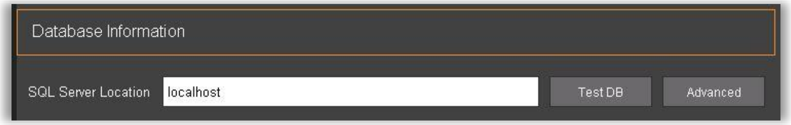
Version 7.0.0.58

IP Address 10.10.6.215

Allows the Administrator to change the default server name, view the version number of the IP Server connected to VI MonitorPlus, and view the IP address of the IP server itself.

Only the name of the IP server can be modified in this section.

Database Information

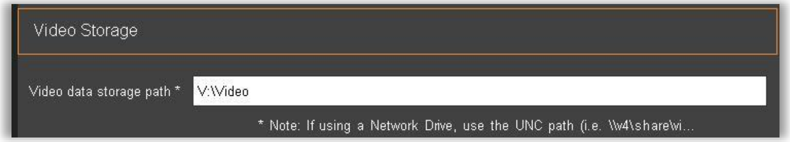

Database Information

SQL Server Location: localhost

Database Information

This section allows the Administrator to test connectivity with the SQL database, as well as alter the database connectivity parameters.

Video Storage

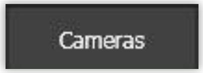

Video Storage

Video data storage path *: V:\Video

* Note: If using a Network Drive, use the UNC path (i.e. \\w4\share\vi...

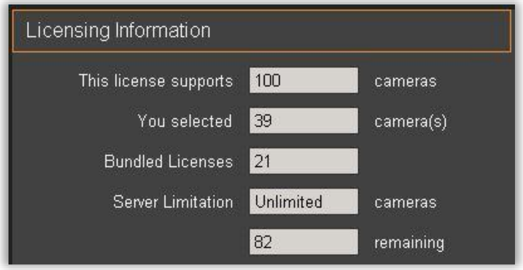
The Administrator can elect to use a new video storage location by modifying this field to reflect the desired landing point for video collection. This will apply to any NEW cameras

(1C) CAMERAS



The cameras section provides access for the administrator to quickly add or remove cameras, view licensing information as it relates to the total number of cameras available through the licenses and move cameras from server to server in a share database environment.

Licensing Information


Licensing Information

This license supports: 100 cameras

You selected: 39 camera(s)

Bundled Licenses: 21

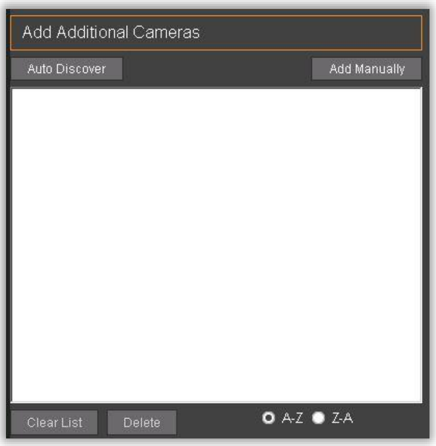
Server Limitation: Unlimited cameras

82 remaining

Number of cameras in total that the license supports

- Number of cameras being used against the license
- Number of cameras being used with a bundled license
- Server limitation for number of cameras
- Total number of cameras that can be used on the server with the current license

Add Additional Cameras

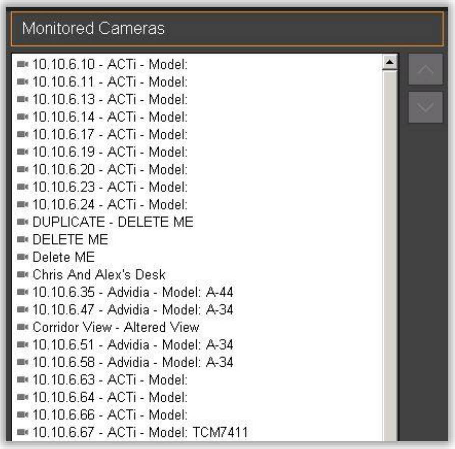


The **Add Additional Cameras** section is the main point for Administrators to add cameras to an IP Server.

Cameras can be added automatically, if their passwords are at default or the password is known.

Additionally, Cameras loaded into this screen in a shared database environment can be move to other servers, for ease of administration of multiple servers and many cameras.

Monitored Cameras



Monitored Cameras

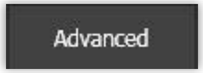
- 10.10.6.10 - ACTi - Model:
- 10.10.6.11 - ACTi - Model:
- 10.10.6.13 - ACTi - Model:
- 10.10.6.14 - ACTi - Model:
- 10.10.6.17 - ACTi - Model:
- 10.10.6.19 - ACTi - Model:
- 10.10.6.20 - ACTi - Model:
- 10.10.6.23 - ACTi - Model:
- 10.10.6.24 - ACTi - Model:
- DUPLICATE - DELETE ME
- DELETE ME
- Delete ME
- Chris And Alex's Desk
- 10.10.6.35 - Advidia - Model: A-44
- 10.10.6.47 - Advidia - Model: A-34
- Corridor View - Altered View
- 10.10.6.51 - Advidia - Model: A-34
- 10.10.6.58 - Advidia - Model: A-34
- 10.10.6.63 - ACTi - Model:
- 10.10.6.64 - ACTi - Model:
- 10.10.6.66 - ACTi - Model:
- 10.10.6.67 - ACTi - Model: TCM7411

The Monitored Cameras section is a tool that displays the cameras that are assigned to the IP Server.

List of functions available to the Administrator are:

- Sort Cameras Automatically
- Move camera up or down in the list
  (Select the camera to be moved up or down in the list, and then use the arrow keys to move it to the desired location on the list.)
- Delete a camera
  Select the camera to be deleted, and then click on the Delete button.)

(1D) ADVANCED



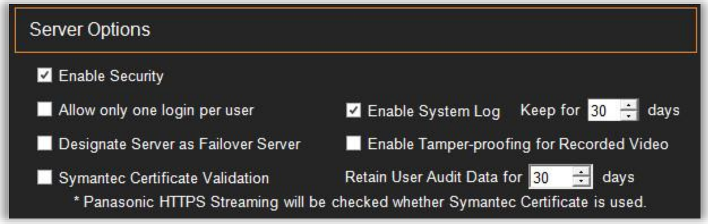
The Advanced tab displays for the Administrator three core components:

- **Server Options** (Basic security and Logging)
- **Record Options** Enable Binary Recording, Reserve Space for other applications
- **Live Display Options** Server Timeout

Server Options

The **Server Options** section provides access to some of the security settings that enhance the overall purpose of having an NVR that can be locked down by feature:

- Enable Security.
- Allow only one login per user.
- Designate Server as a Failover Server.
- Symantec Certificate Validation.
- Enable System Log. (Keep for XX days)
- Enable Tamper-proofing for Recorded Video.
- Retain User Audit Data for XX days.



Server Options

☑ Enable Security

☐ Allow only one login per user ☑ Enable System Log Keep for 30 days

☐ Designate Server as Failover Server ☐ Enable Tamper-proofing for Recorded Video

☐ Symantec Certificate Validation Retain User Audit Data for 30 days

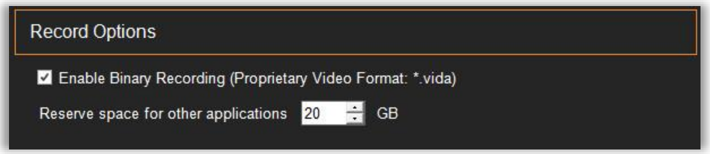
* Panasonic HTTPS Streaming will be checked whether Symantec Certificate is used.

Record Options

Enable Binary Recording: Allows the access to video being recorded on the fly. It's a very resource consuming feature and should only be used when consistent access and review of video are needed.

When enabled, the Proprietary Video Format (**.vida**) will be used instead of the standard **.AVI** file format.

Reserve space for other applications: The maximum amount of space used on any attached storage device used by IP Server. (Default: 5GB)



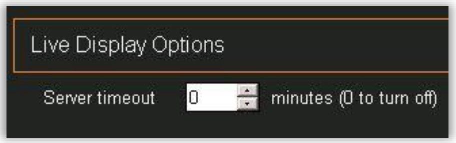
Record Options

☑ Enable Binary Recording (Proprietary Video Format: *.vida)

Reserve space for other applications 20 GB

NOTE - ***Reserve space*** may not reflect the actual available disk space on IP Server.

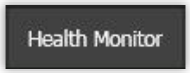
Live Display Options


Live Display Options

Server timeout 0 minutes (0 to turn off)

The Server timeout feature is to prevent unwanted or unintended access to the IP Server through the web client where there is no activity for the desired number of minutes. The default value for this setting is 0, which is powered-off. A recommended value is 20 minutes. After a 20-minute period with no movement in the web client, the user will be automatically logged out.

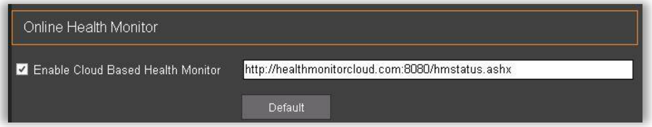
(1E) HEALTH MONITOR



Health Monitor is a web-based client that allows the user to have a record of server and camera uptime stored at an off-site location. It does require Internet access and an account on https://healthmonitorcloud.com to function. If activated without an account, the data sent to the Health Monitor Cloud server will not be retained for any length of time.

NOTE - Video Insight strongly recommends Health monitor cloud managed for environments containing between 1-100 servers or up to 2000 cameras.

Online Health Monitor


Online Health Monitor

☑ Enable Cloud Based Health Monitor http://healthmonitorcloud.com:8080/hmstatus.ashx

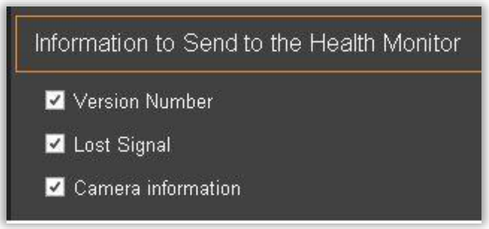
To enable the **Health Monitor Cloud** feature, click in the box next to Enable Cloud-Based Health Monitor.

The default URL that data will be sent to is:

http://healthmonitorcloud.com:8080/hmstatus.ashx

If the administrator determines that the need for an in-house Health Monitor Cloud solution is necessary, please direct inquires to the Video Insight / Panasonic Sales department.

Information to Send to Health Monitor


Information to Send to the Health Monitor

☑ Version Number

☑ Lost Signal

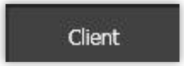
☑ Camera information

Information to Send to the Health Monitor:

It is recommended that each of the three available check boxes is checked for maximized use of the Health Monitor Cloud. The three options available are:

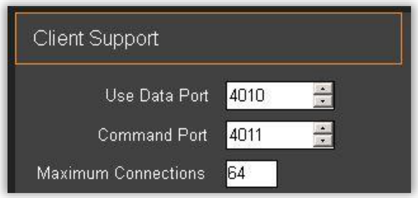
- **Version Number**
  (IP Server Version number)
- **Lost Signal**
  (with either camera or server or both)
- **Camera Information**
  (general statistics about the camera and its performance)

(1F) CLIENT



The **Client** tab gives the administrator access to tools that change port numbers (for enhanced security), provide SMTP configurations for sending messages using rules manager, sending a test email to verify that SMTP configuration settings have been entered correctly, and the ability to launch the Group Policy Editor as it applies to an IP Server on an active Directory Domain, where AD credentials are used for logging into VI MonitorPlus and the IP Server itself.

Client Support



Use Data Port 4010

Command Port 4011

Maximum Connections 64

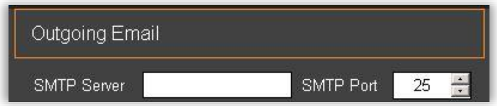
The term **Client Support** refers to the VI MonitorPlus software client itself.

Network Security can be enhanced by changing the default values for Data and Command ports (4010 and 4011 respectively) to better suit the administrator's needs and any customization of the IP Sever.

Maximum Connections is the total number of VI MonitorPlus clients with access to the IP Server. The default value is 64 connections, which is also the maximum recommended value.

NOTE - The Maximum Connections number value can be lowered as a method to slightly increase security on the server. A lower value that matches the exact number of personnel that have access to the server is recommended.

Outgoing Email

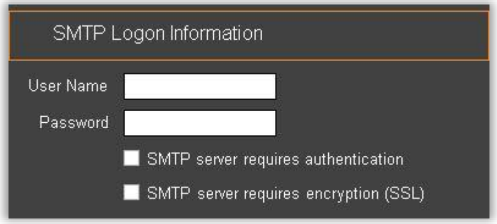


SMTP Port 25

Outgoing Email

This section provides access to the SMTP server and SMTP port values. The default SMTP Server port is 25, but most SMTP port services with advanced security use alternative ports. These values can be customized to suit the needs and requirements of the SMTP server.

SMTP Logon Information

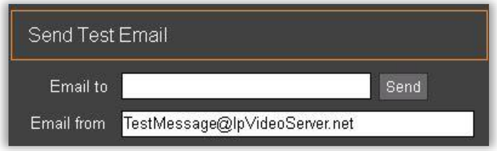

SMTP Logon Information
User Name
Password
☐ SMTP server requires authentication
☐ SMTP server requires encryption (SSL)

SMTP Login Information

This section allows the Administrator to enter the required username and password for the SMTP server entered in the Outgoing Email section listed above.

As part of the enhanced security requirements necessary for connecting to SMTP servers, Server Authentication and SSL encryption have been added.

Send Test Email



Email from TestMessage@IpVideoServer.net

After the Administrator completes the SMTP mail server configuration, a test email will be sent to validate the SMTP connection settings.

If the test email is not received, verify the outgoing email address and password and send a second test message.

If problems persist, verify the correct account settings.

(1G) ACCESS CONFIGURATION

This tab will function only when IP Server is integrated with Access Control devices. Please contact your Video Insight Sales Vendor for more information about Access Control Integration.

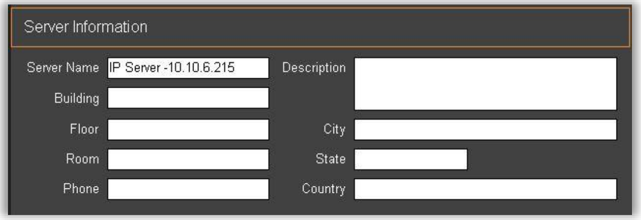
For more information about the Access Control servers that are known to function with IP Server and VI MonitorPlus, please visit http://wwwldownloadvi.com/accesscontrol to find the corresponding product guide.

(1H) CONTACT INFORMATION

The information provided here is not parsed to any Video Insight affiliates, nor is it sent to Health Monitor Cloud. This information is solely for internal documentation purposes of the license holder for IP Server and is ***completely optional***.

Server Information

The server information entered here is solely for the purposes of internal documentation for the Administrator. Information here is not parsed to any organization in any form.


Server Information

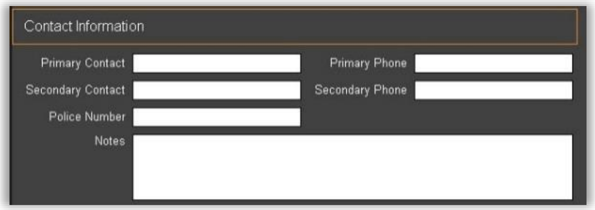
Server Name: IP Server -10.10.6.215

The administrator can enter the following data:

- Server name
- Building
- Floor
- Room
- Phone
- Description
- City
- State
- Country

Contact Information

Also, not parsed to any outside organization, it is the contact information for the server.


Contact Information

The administrator can enter the following values:

- Primary Contact (name)
- Secondary Contact (name)
- Police Number
- Notes
- Primary Phone (number)
- Secondary Phone (number)

(2) RESOURCE GROUPS

This function allows the Administrator of large IP Server installations to create customized viewing groups for quickly organizing assets across multiple IP Servers.

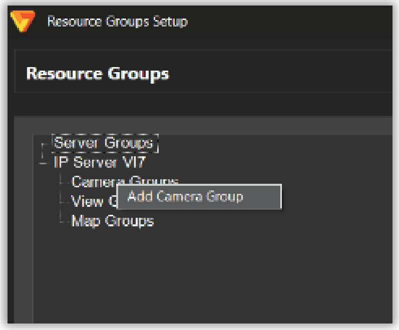
NOTE - This does NOT move Cameras or Layouts or Maps from server to server. Its intentional use is to allow a user to easily define a variety of customized viewing possibilities with the available resources listed on multiple IP Server configurations.

This functionality aids in the elimination of the sorting and grouping substantial amounts of data each time a user is added to IP Server, need to access a specific map within hundreds of maps, or whatever the preferred sorting preference might be and can be used to share resources of one IP Server with another user on another machine.

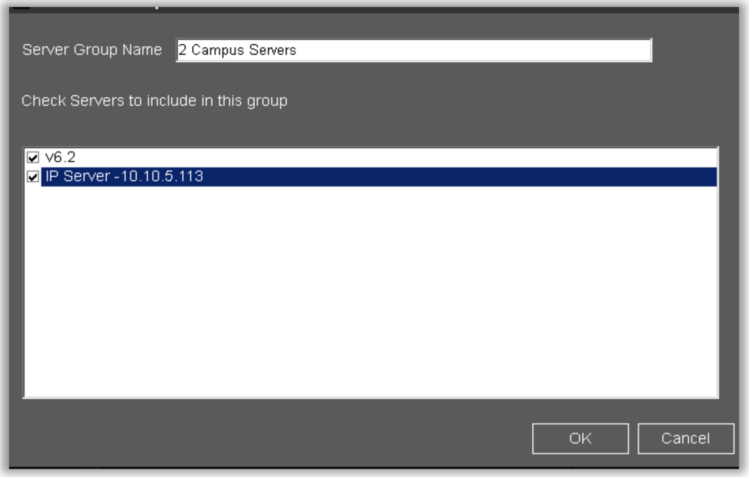
To use a Server Group, the assumption is that there are two or more IP Servers already configured to work within VI MonitorPlus. If VI MonitorPlus has not yet been configured to work with multiple servers, please refer to the section above titled Login Options.

(2A) SERVER GROUPS

Server Groups allow the administrator to group specific IP Servers into categories that are unique to the use and need of the Administrator. This feature was developed with large building campuses in mind, where there may be a need to organize multiple IP Servers for easy visual access.



To create a server group, right-click on the **Server Groups** text, and then select **Add Server Group**

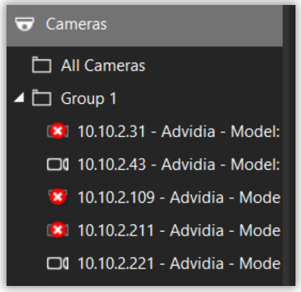

Server Group Name: 2 Campus Servers

Check Servers to include in this group

☑ v6.2
☑ IP Server -10.10.5.113

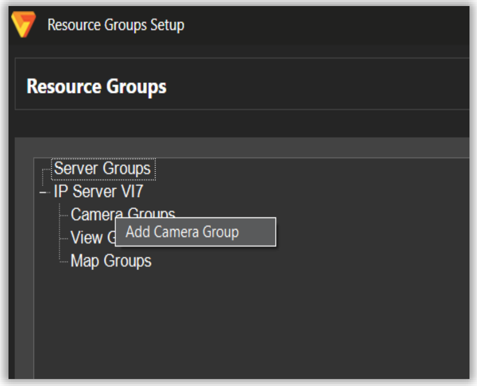
Select the servers desired to form the group and give the group an appropriate name.

Once all IP Servers have been selected for the group, click **OK**.


Cameras
All Cameras
Group 1
10.10.2.31 - Advidia - Model:
10.10.2.43 - Advidia - Model:
10.10.2.109 - Advidia - Mode
10.10.2.211 - Advidia - Mode
10.10.2.221 - Advidia - Mode

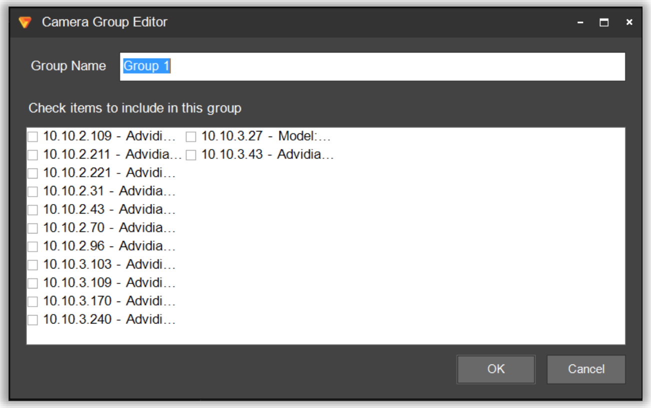
The new **Server Group** will appear in the Enterprise View window of VI MonitorPlus, as seen on the left.

(2B) CAMERA GROUPS



To create a custom **Camera Group**, right click on the Camera Groups title and select **Add Camera Group**.

A pop-up window appears requiring custom input.



Camera Group Editor

Group Name: Group 1

Check items to include in this group

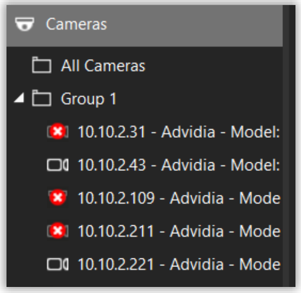
□ 10.10.2.109 - Advidi…
□ 10.10.2.211 - Advidia…
□ 10.10.2.221 - Advidi…
□ 10.10.2.31 - Advidia…
□ 10.10.2.43 - Advidia…
□ 10.10.2.70 - Advidia…
□ 10.10.2.96 - Advidia…
□ 10.10.3.103 - Advidi…
□ 10.10.3.109 - Advidi…
□ 10.10.3.170 - Advidi…
□ 10.10.3.240 - Advidi…
□ 10.10.3.27 - Model:…
□ 10.10.3.43 - Advidia…

OK | Cancel

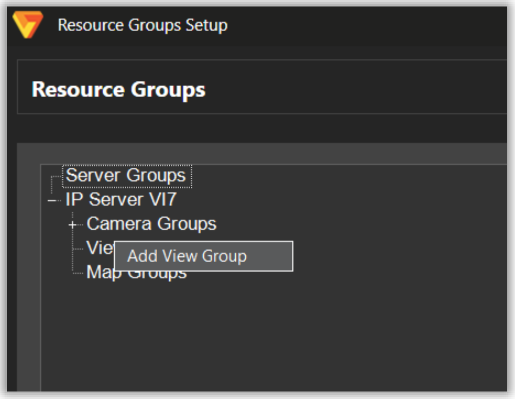
All cameras connected to each IP Server will appear within the window.

Add the desired cameras to the list and give the new Camera Group a name for identification.

The new **Camera Group** will appear in Enterprise View under Camera Groups.

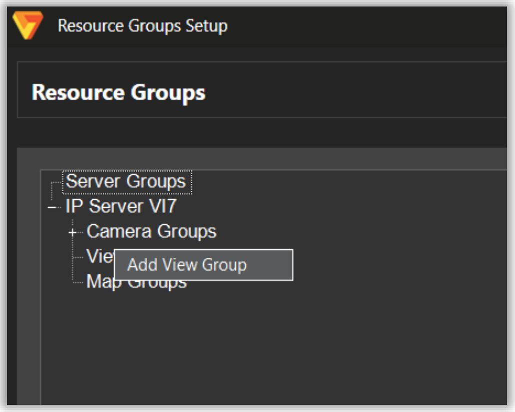

Cameras
All Cameras
Group 1
10.10.2.31 - Advidia - Model:
10.10.2.43 - Advidia - Model:
10.10.2.109 - Advidia - Mode
10.10.2.211 - Advidia - Mode
10.10.2.221 - Advidia - Mode

To create **View Groups** and **Map Groups**, the process is a repeat of the above steps, with exception to the final display of the View Groups and Map Groups. Each of these is available only on the original server where the layouts are created.



For the creation of View Groups, select **View Groups** and then **Right Click** on **Add View Group**.

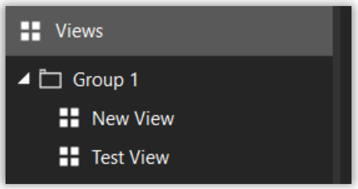
Create a name for the custom view and add the previously created Views to the new **Custom View** grouping.



Next add the desired Views.

Click **OK** when done adding new Views to the new View Group.

When complete, the **New View Group** will appear *BELOW* the Enterprise View box, on the main menu.

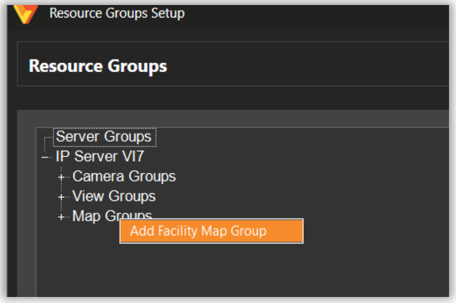


This newly created Group will appear.
Selecting **View Groups** will result in the displaying of the Views that were added to this group.

They will be displayed to the right of the View Group list, as seen left.

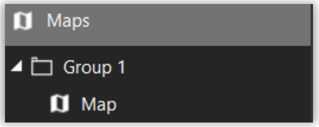
(2C) MAP GROUPS

To create Map Groups, select **Map Groups**, and then Right-click on **Add Facility Map Group**, as seen below.



Give the new Map Group an appropriate name, add the selected maps that were previously created, and then *Click* on **OK** to complete the new Map Group.

The new Map Group is found on the Live Tab, at the bottom of the left-hand column

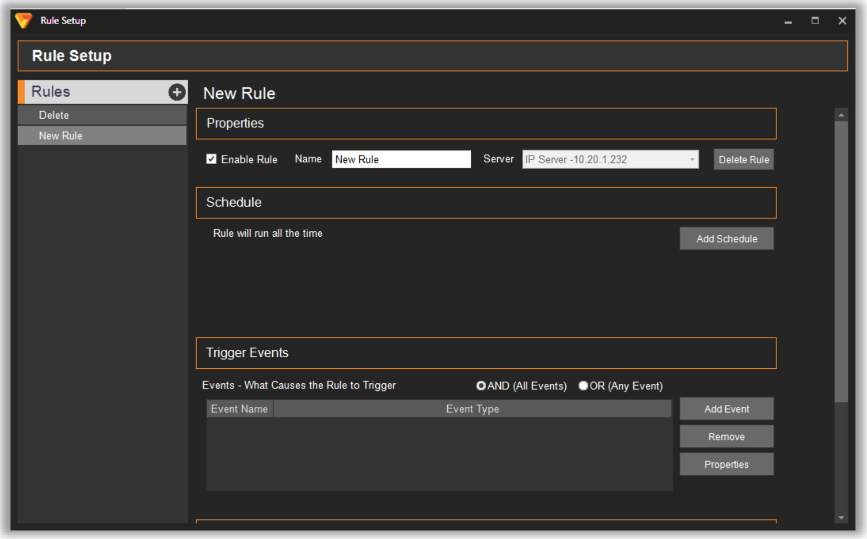


Select the newly created Map Group and you will have successfully completed the creation of new groups.

(3) RULES

Users can add new rules by clicking on the **+** sign next to **Rules** in the left side menu.

NOTE - For more detailed construction of Rules, please refer to the **Supplemental Rules Manager Guide** for a more detailed explanation of each of the rules and features available.



☑ Enable Rule Name New Rule Server IP Server -10.20.1.232

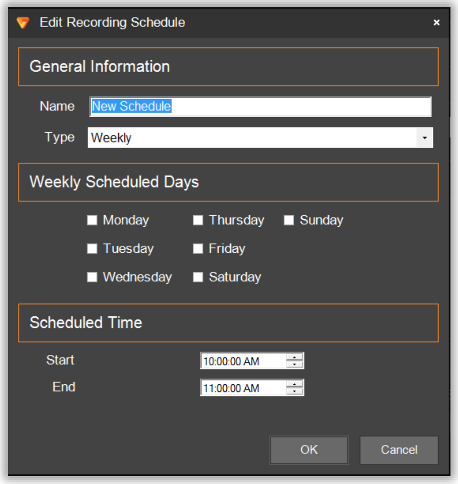
Rule will run all the time

Events - What Causes the Rule to Trigger ○ AND (All Events) ● OR (Any Event)

Once rules have been added, users can select them from the menu and the rules information will appear on the right side of the screen.

If no screen is selected, the screen will look like the image on the left.

As the image on the left demonstrates, Rules can be enabled, given a name and then assigned to a server.



Edit Recording Schedule

General Information

Name: New Schedule

Type: Weekly

Weekly Scheduled Days

□ Monday □ Thursday □ Sunday
□ Tuesday □ Friday
□ Wednesday □ Saturday

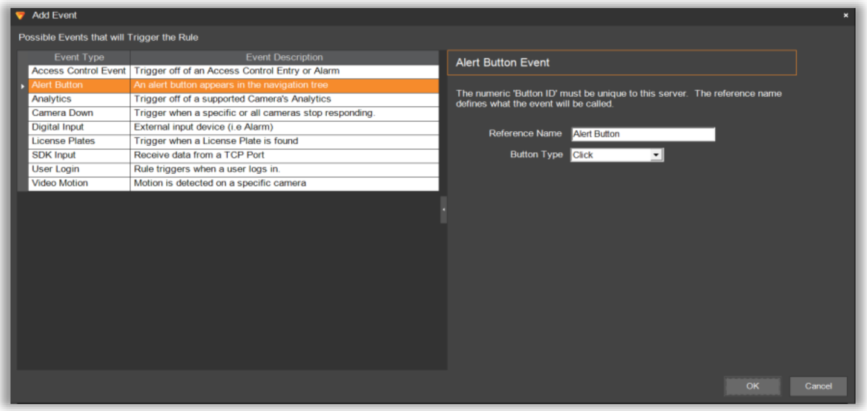
Scheduled Time

Start: 10:00:00 AM

End: 11:00:00 AM

Schedules, events and actions can be added by clicking on the **Add Schedule**, **Add Event** and **Add Action** buttons, respectively.

As a user creates a new schedule, the following popup will appear as seen on the left.



Add Event

Possible Events that will Trigger the Rule

Event Type	Event Description
Access Control Event	Trigger off of an Access Control Entry or Alarm
Alert Button	An alert button appears in the navigation tree
Analytics	Trigger off of a supported Camera's Analytics
Camera Down	Trigger when a specific or all cameras stop responding.
Digital Input	External input device (i.e Alarm)
License Plates	Trigger when a License Plate is found
SDK Input	Receive data from a TCP Port
User Login	Rule triggers when a user logs in.
Video Motion	Motion is detected on a specific camera

Alert Button Event

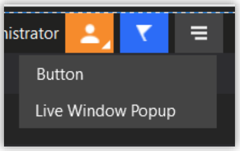
The numeric 'Button ID' must be unique to this server. The reference name defines what the event will be called.

Reference Name: Alert Button

Button Type: Click

Users can set a schedule for the selected rule, choosing the days of the week, specific time and frequency.

When done, **click on OK** to save the changes.



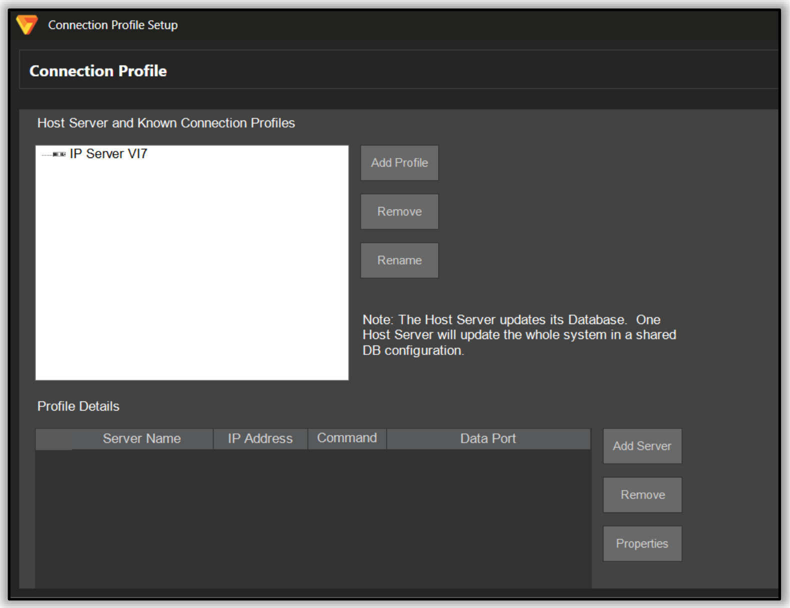
When adding an event, the **Add Event** window will appear.

Users can then select an event among the ones available. All alert buttons will be displayed once configured under the left panel navigation under the header titled Buttons.

(3A) RULES SETUP

This is considered an advanced feature due to its complexity. A more comprehensive guide is available for use in the Advanced Installation section, above. To enable the rule correctly, restart of IP server and VI MonitorPlus is required.

(4) CONNECTION PROFILES

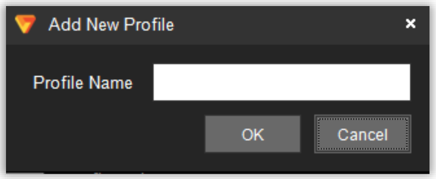


Note: The Host Server updates its Database. One Host Server will update the whole system in a shared DB configuration.

Server Name	IP Address	Command	Data Port

Connection Profiles allows Administrators to manage user profiles and servers based on the profile that has previously been created.

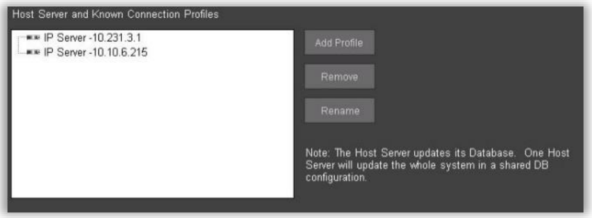
Connection Profiles are similar to the use of **Groups**.



To add a new connection profile, click on '**Add Profile'** and the **Add Connection Profile** will be displayed.

Once set, click **OK** to create a new profile

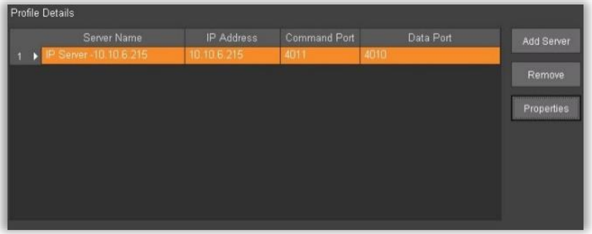
(4A) HOST SERVER AND KNOWN CONNECTION PROFILES



Note: The Host Server updates its Database. One Host Server will update the whole system in a shared DB configuration.

Known Connection Profiles

This list displays only the servers that are available for creation of Host Server Connection Profiles. If a server does not appear in this list, click on Add Profile and provide the information being requested.



	Server Name	IP Address	Command Port	Data Port
1 ▸	IP Server -10.10.6.215	10.10.6.215	4011	4010

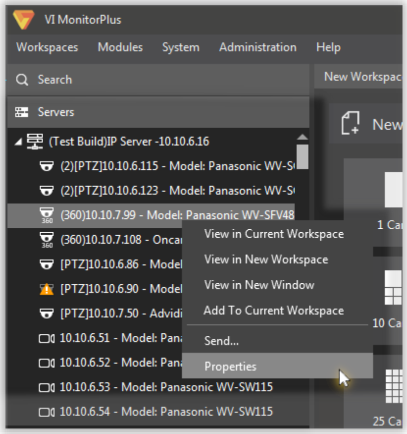
Profile Details

This section allows the Administrator to create a base for server profiles, which can be added to a network share device for easy access from any server that has permissions and access to that share.

4.10.B Camera Properties

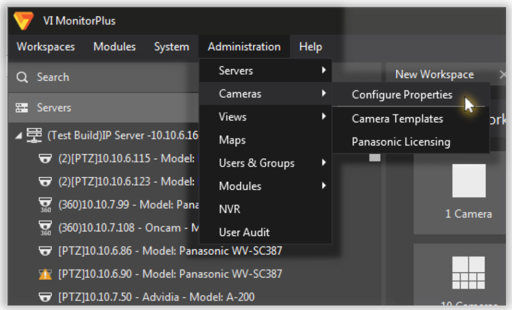
VI Monitor Plus features a complete interface to configure and setup the existing inventory of cameras for an IP Server installation. It can be accessed in 2 different ways:

From the Navigation Tree



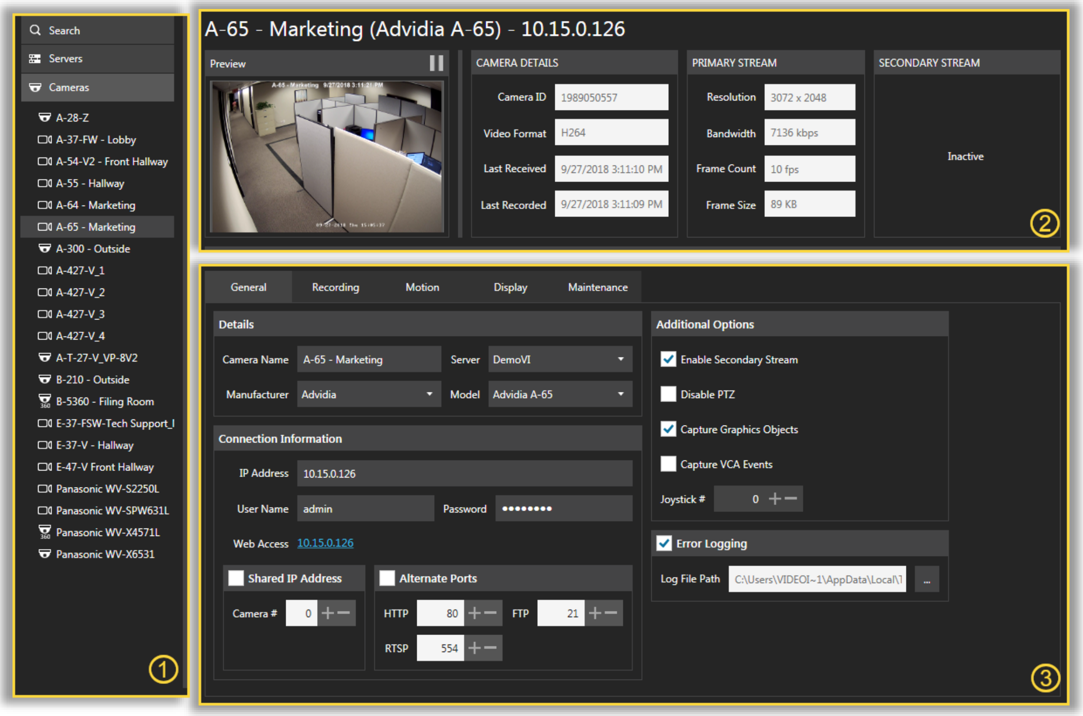
On the left navigation tree, **Right click** on the desired camera name, either under the **Servers** tab or the **Cameras** tab. From the pop-up menu, select “**Properties**”.
The **Camera Properties** window will open with the selected camera’s settings.

From the Administration tab


VI MonitorPlus
Workspaces
Modules
System
Administration
Help
Search
Servers
Servers
Cameras
Views
Maps
Users & Groups
Modules
NVR
User Audit
New Workspace
Configure Properties
Camera Templates
Panasonic Licensing
(Test Build)IP Server -10.10.6.16
(2)[PTZ]10.10.6.115 - Model:
(2)[PTZ]10.10.6.123 - Model:
(360)10.10.7.99 - Model: Pana
(360)10.10.7.108 - Oncam - M
[PTZ]10.10.6.86 - Model: Panasonic WV-SC387
[PTZ]10.10.6.90 - Model: Panasonic WV-SC387
[PTZ]10.10.7.50 - Advidia - Model: A-200
1 Camera

Open the **Administration** tab on the Main Menu, select “**Cameras**” and click on “**Configure Properties**”.
The **Camera Properties** window will open without a selected camera.

The **Camera Properties** interface is divided into **3 main areas**:



A-65 - Marketing (Advidia A-65) - 10.15.0.126

CAMERA DETAILS

- Camera ID: 1989050557
- Video Format: H264
- Last Received: 9/27/2018 3:11:10 PM
- Last Recorded: 9/27/2018 3:11:09 PM

PRIMARY STREAM

- Resolution: 3072 x 2048
- Bandwidth: 7136 kbps
- Frame Count: 10 fps
- Frame Size: 89 KB

SECONDARY STREAM

Inactive

Details

- Camera Name: A-65 - Marketing
- Server: DemoVI
- Manufacturer: Advidia
- Model: Advidia A-65

Connection Information

- IP Address: 10.15.0.126
- User Name: admin
- Password: ••••••••
- Web Access: 10.15.0.126

□ Shared IP Address
- Camera #: 0

□ Alternate Ports
- HTTP: 80
- FTP: 21
- RTSP: 554

Additional Options

☑ Enable Secondary Stream
□ Disable PTZ
☑ Capture Graphics Objects
□ Capture VCA Events
- Joystick #: 0

☑ Error Logging
- Log File Path: C:\Users\VIDEOI~1\AppData\Local\

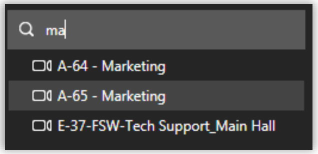
① **Left Panel** - Navigation Tree to access and select the available Servers and Cameras, complete with a Search option.

② **Top Panel** - Live Video preview from the selected camera, its Details and Primary and Secondary streams data.

③ **Control Panel** - Includes 5 Option Tabs for detailed Data and Configuration settings for the selected camera.

(1) LEFT PANEL: NAVIGATION TREE

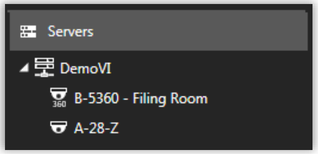
Search - Quickly locates a camera or a group of cameras within the Navigation Tree by typing its name or number in the input box.



ma

- A-64 - Marketing
- A-65 - Marketing
- E-37-FSW-Tech Support_Main Hall

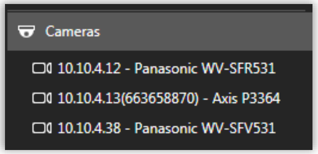
Servers - Displays all servers connected to VI MonitorPlus and provides access to the cameras associated to each server.



Servers

- DemoVI
  - B-5360 - Filing Room
  - A-28-Z

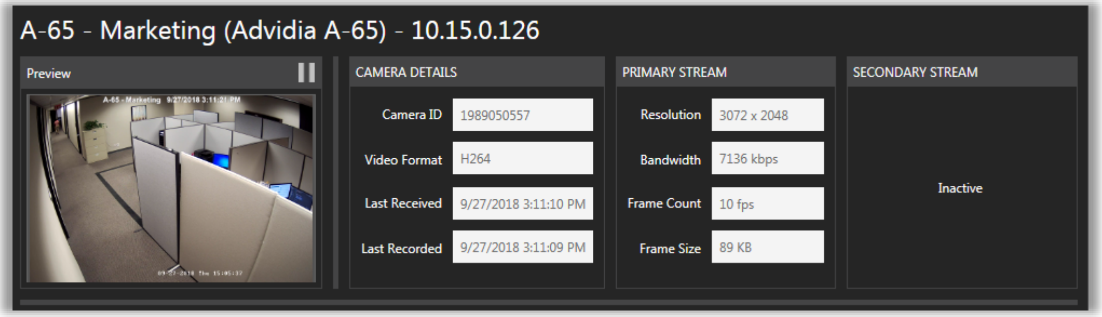
Cameras - Displays all cameras for all servers connected to VI MonitorPlus without separating them by associated servers.



Cameras

- 10.10.4.12 - Panasonic WV-SFR531
- 10.10.4.13(663658870) - Axis P3364
- 10.10.4.38 - Panasonic WV-SFV531

(2) TOP PANEL: STREAMING



A-65 - Marketing (Advidia A-65) - 10.15.0.126

CAMERA DETAILS

Camera ID	1989050557
Video Format	H264
Last Received	9/27/2018 3:11:10 PM
Last Recorded	9/27/2018 3:11:09 PM

PRIMARY STREAM

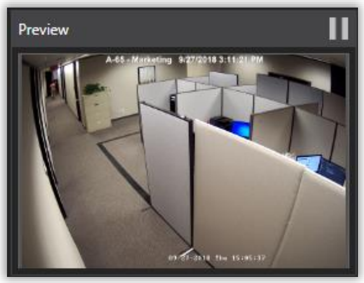
Resolution	3072 x 2048
Bandwidth	7136 kbps
Frame Count	10 fps
Frame Size	89 KB

SECONDARY STREAM

Inactive

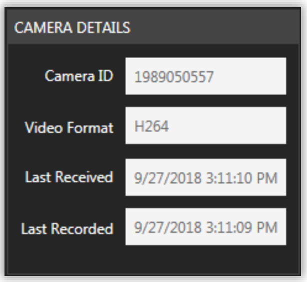
The **Name, Model** and **IP Address** of the selected camera are shown at the top of the window with enlarged characters.

Preview - Shows the live video streaming from the selected camera, which can be paused or continued by clicking on the top-right playback button.



Camera Details

- **Camera ID** - Designated unique identification number of any given camera.
- **Video Format** - Specific codec type used by the selected camera.
- **Last Received** - Most recent time a live image was received by the server from the camera.
- **Last Recorded** - Last time a recorded event took place and wrote to the storage location.

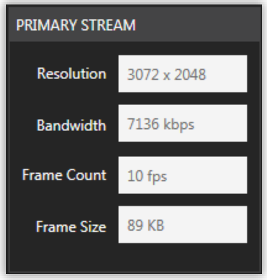


CAMERA DETAILS

Camera ID	1989050557
Video Format	H264
Last Received	9/27/2018 3:11:10 PM
Last Recorded	9/27/2018 3:11:09 PM

Primary Stream

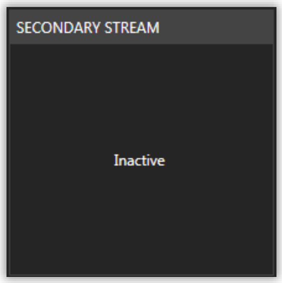
- Resolution - Maximum resolution of the video stream.
- Bandwidth - Camera's Bandwidth usage per second.
- Frame Count - Number of frames per second received from the camera.
- Frame Size - Storage quota for each individual frame received.



PRIMARY STREAM

Resolution: 3072 x 2048
Bandwidth: 7136 kbps
Frame Count: 10 fps
Frame Size: 89 KB

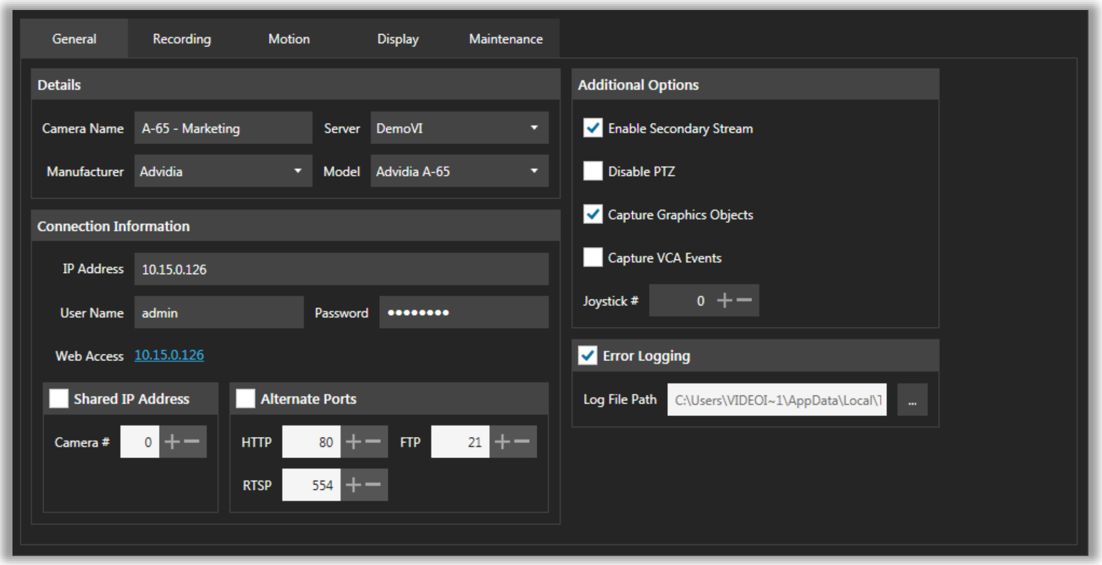
Secondary Stream - Shows the same fields of the Primary Stream window, and it is visible depending on the camera and its availability. When unavailable, the status "*Inactive*" is displayed instead.



SECONDARY STREAM

Inactive

(3) CONTROL PANEL: GENERAL



Details

Camera Name: A-65 - Marketing
Server: DemoVI
Manufacturer: Advidia
Model: Advidia A-65

Connection Information

IP Address: 10.15.0.126
User Name: admin
Password: ••••••••
Web Access: 10.15.0.126

□ Shared IP Address
Camera #: 0

□ Alternate Ports
HTTP: 80
FTP: 21
RTSP: 554

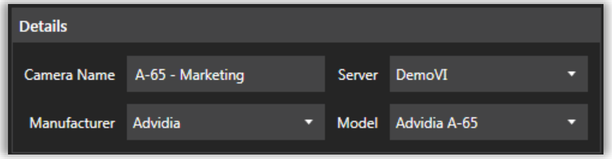
Additional Options

☑ Enable Secondary Stream
□ Disable PTZ
☑ Capture Graphics Objects
□ Capture VCA Events
Joystick #: 0

☑ Error Logging
Log File Path: C:\Users\VIDEOI~1\AppData\Local\

Details

- Camera Name - Unique name to identify the camera throughout the application, briefly specifying its brand, model, location, department, features, etc.
- Server - Drop-down list of the available VI servers.
- Manufacturer - Drop-down list of Camera Manufacturers.
- Model - Drop-down list of Camera Models associated to the selected Manufacturer.



Details

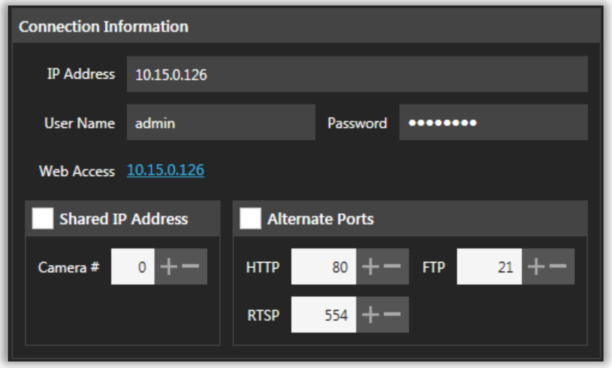
Camera Name: A-65 - Marketing
Server: DemoVI
Manufacturer: Advidia
Model: Advidia A-65

Connection Information

- IP Address - Unique IP address for the camera/encoder.
- User Name/Password - Account data to access the camera settings (where available).
- Web Access - Opens an external web browser session to access the camera.

- Shared IP Address - Check this box to manage specific lenses or cameras attached to an encoder. Some cameras (such as Arecont or Scallop Imaging) have multiple lenses and encoders that connect multiple analog cameras on a single device, such as Advidia VP-16, VP-8, VP-4, etc. Therefore, using this feature will let you specify exactly what to display, whether it be lenses or encoders.
- Camera # - Selects the lens/camera to display on a device that shares an IP address.

- Alternate Ports - Check this box to configure any device connected to the IP Server using custom ports. Default ports are:
  - HTTP: 80
  - FTP: 21
  - RSTP: 554



Connection Information

IP Address 10.15.0.126

User Name admin Password ••••••••

Web Access 10.15.0.126

□ Shared IP Address

Camera # 0

□ Alternate Ports

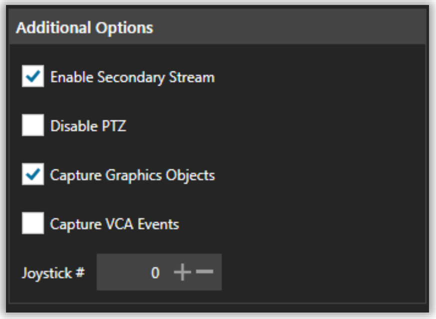
HTTP 80

FTP 21

RTSP 554

Additional Options

- Enable Secondary Stream - Allows the IP Server to extract the secondary stream of a camera when supported.
- Disable PTZ - Disables the camera's Pan/Tilt/Zoom functionality. PTZ functions are accessed via USB by both on-screen and joystick controls. Both are disabled when the option is checked.
- Capture Graphics Objects - Active when VID or iVMD are being used.
- Capture VCA Events - Active when VID, iVMD or camera-side Analytics are being used.
- Joystick # - Used when using a DCZ joystick to designate a specific camera to a specific number on the joystick list, providing the ability to quickly select a camera from the left tree without having to navigate the left tree at all.



Additional Options

☑ Enable Secondary Stream

□ Disable PTZ

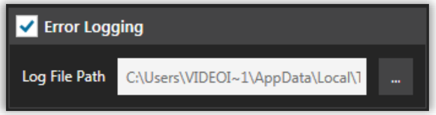
☑ Capture Graphics Objects

□ Capture VCA Events

Joystick # 0

Error Logging - Check this box to enable the capture and save errors messages received from a camera into a log text file. This allows Administrators, Technical Support and Development staff to quickly diagnose possible issues with a specific camera.

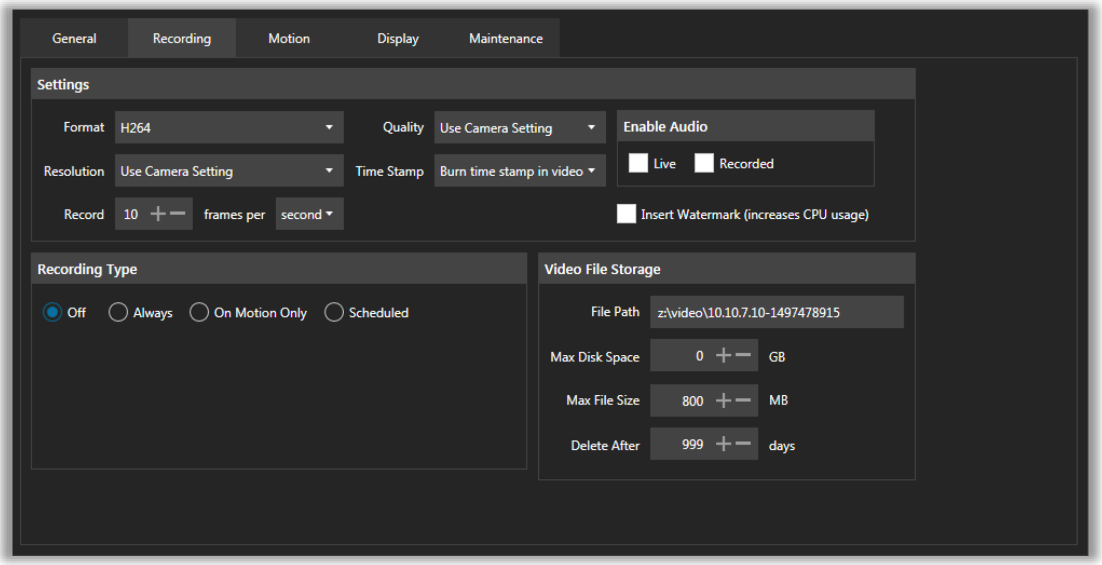
- Log File Path - Specifies the physical folder/file for the Error Log.



☑ Error Logging

Log File Path C:\Users\VIDEOI~1\AppData\Local\

(4) CONTROL PANEL: RECORDING



Settings

Format: H264 | Quality: Use Camera Setting | Enable Audio: □ Live □ Recorded

Resolution: Use Camera Setting | Time Stamp: Burn time stamp in video

Record 10 frames per second | □ Insert Watermark (increases CPU usage)

Recording Type

● Off ○ Always ○ On Motion Only ○ Scheduled

Video File Storage

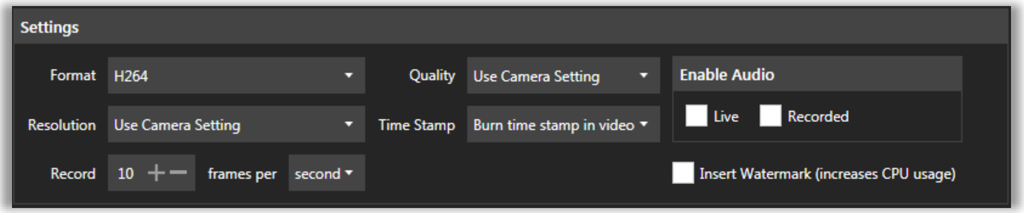
File Path: z:\video\10.10.7.10-1497478915

Max Disk Space: 0 GB

Max File Size: 800 MB

Delete After: 999 days

Settings



Settings

Format: H264 | Quality: Use Camera Setting | Enable Audio: □ Live □ Recorded

Resolution: Use Camera Setting | Time Stamp: Burn time stamp in video

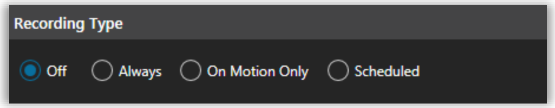
Record 10 frames per second | □ Insert Watermark (increases CPU usage)

- **Format** - Drop-down list of Video Codec types. **H.264/H.265** (default) are recommended for best performance.
- **Resolution** - Drop-down list of resolution levels provided by the camera.
- **Record** - Defines the recorded video frame rate during a specific interval of time, depending on the camera's supported properties.
- **Quality** - Adjusts the camera's bit rate (lower bit rate = lower video quality).
- **Time Stamp** - Enables/disables the on-video time stamp obtained from the camera's date/time feature.
- **Enable Audio**
  - **Live** - Activates audio support during live video streaming.
  - **Recorded** - Enables audio for recorded video viewing.
- **Insert Watermark** – Check this box to enable the on-top display of live/recorded video, including: Codec, FPS, Camera Name/Model, etc. This feature might impact the CPU performance.

Recording Type

- **Off** - No recording enabled.

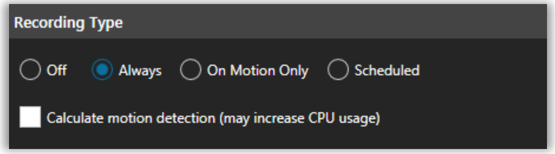
> For audio/video synchronization, it is highly recommended that *Record Always* recording type is used with all audio functions.



Recording Type

● Off ○ Always ○ On Motion Only ○ Scheduled

- **Always** - Always recording, enables ability to use motion detection when recording. Events with no motion are not recorded. Enable "***Calculate motion detection***" by checking the box.

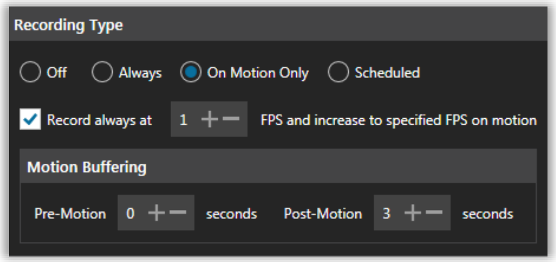


Recording Type

○ Off ● Always ○ On Motion Only ○ Scheduled

□ Calculate motion detection (may increase CPU usage)

- **On Motion Only** - Records on motion only, based on camera-side or server-side settings.
  Check the "***Record Always at***" box to select 1, 2 or 3 FPS "no motion" video recording rate.
  If motion is detected, recording will start at the current FPS setting.
  If a user is recording at 1FPS always, with motion detection set to 10 FPS, the video that contains "no motion" will appear at fast speed.
  Motion is detected at normal speed during playback.

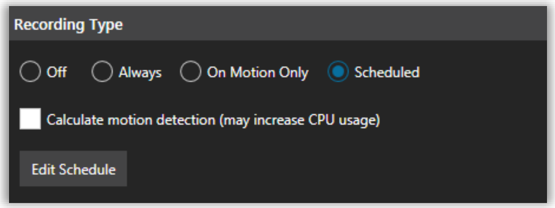

Recording Type
○ Off ○ Always ● On Motion Only ○ Scheduled
☑ Record always at 1 FPS and increase to specified FPS on motion
Motion Buffering
Pre-Motion 0 seconds Post-Motion 3 seconds

Motion Buffering

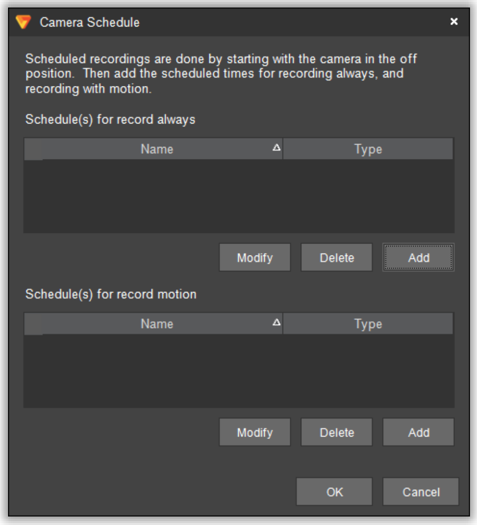
Pre-Motion - Information captured **x seconds** before the motion event occurs. When Binary recording is not used, it is stored on the memory cache. If Binary recording is used, the open file maintains pre-motion values. **Default = 0**.

Post-Motion - Information captured **x seconds** after the motion event occurs. **Default = 3**.

- **Scheduled** - Records using a time schedule. When no schedule is defined, the camera recording is set to ***off***. Enable "***Calculate motion detection***" by checking the corresponding box.


Recording Type
○ Off ○ Always ○ On Motion Only ● Scheduled
□ Calculate motion detection (may increase CPU usage)

Click on "***Edit Schedule***" to open the **Camera Schedule** interface:

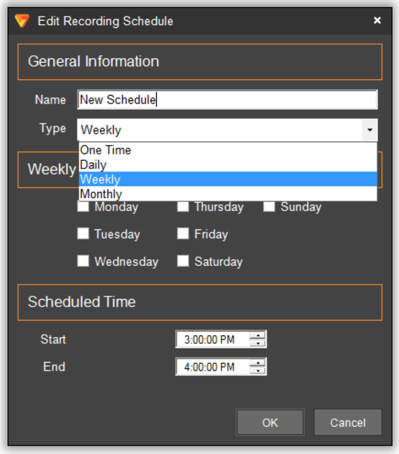

Camera Schedule
Scheduled recordings are done by starting with the camera in the off position. Then add the scheduled times for recording always, and recording with motion.
Schedule(s) for record always

Name	Type

Schedule(s) for record motion

Name	Type

The **Camera Schedule** interface allows ***adding***, ***modifying*** or ***deleting*** scheduled times for **Record Always** and **Record with Motion** times.


Edit Recording Schedule
General Information
Name: New Schedule
Type: Weekly
Weekly
□ Monday □ Thursday □ Sunday
□ Tuesday □ Friday
□ Wednesday □ Saturday
Scheduled Time
Start: 3:00:00 PM
End: 4:00:00 PM

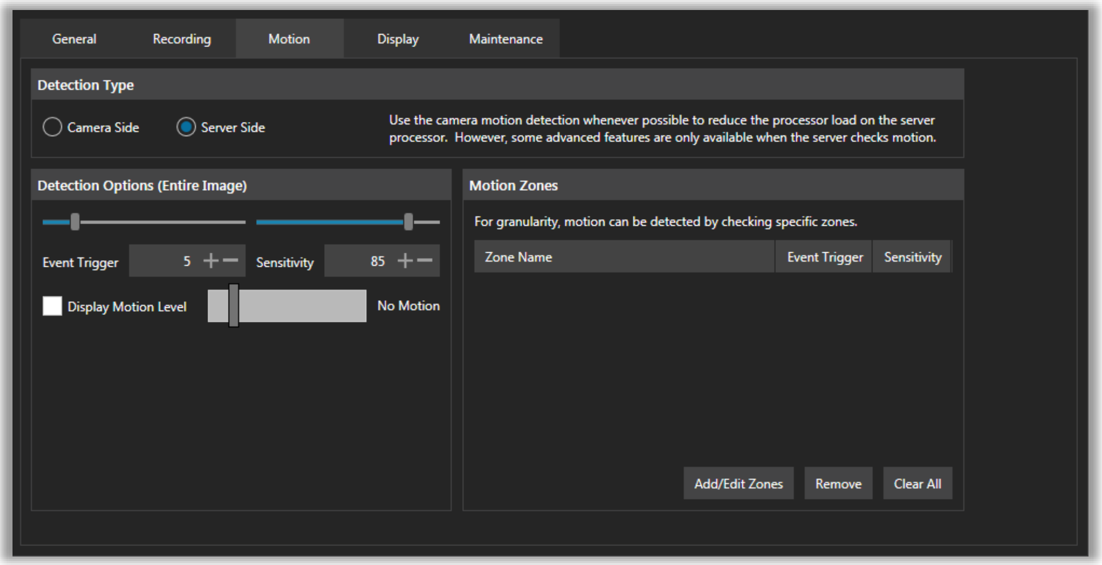
The **Edit Recording Schedule** form is opened by ***adding*** or ***modifying*** a schedule, and it allows defining **one-time**, **daily**, **weekly** or **monthly** recording schedules, as well as the **start and end times** for each event.

Video File Storage

- **File Path** - Physical location where the recorded video will be stored.
- **Max Disk Space** - Limits de maximum space on disk reserved for the camera.
- **Max File Size** - Maximum physical size of each recorded video file.
- **Delete After** - Number of days the video file will be stored before its removal (first in-first out basis).

(5) CONTROL PANEL: MOTION

Motion Zones allow more precise motion detection within captured video recordings. When combining Motion Zone with Motion-Only recording, the camera will ignore certain areas in its line-of-sight.



Use the camera motion detection whenever possible to reduce the processor load on the server processor. However, some advanced features are only available when the server checks motion.

Event Trigger 5; Sensitivity 85

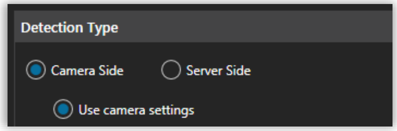
□ Display Motion Level — No Motion

For granularity, motion can be detected by checking specific zones.

Detection Type: Camera Side

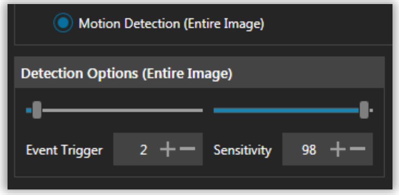
When available, Camera-side Motion Detection is ***recommended to reduce the CPU load*** on the server's processors.

- **Use Camera Settings** - Select this option to use the motion detection settings already configured on the camera.



- **Motion Detection (*Entire Image*)** - Select this option to activate the ***Detection Options (Entire Image)*** for the Camera Side detection. The variables are:
    - **Event Trigger**: Defines the percentage of visual area where change/motion is detected.
    - **Sensitivity**: Near-far gauge, the higher the sensitivity, the better the accuracy.

  Each zone can have its own specific combination of sensitivity and event triggers.

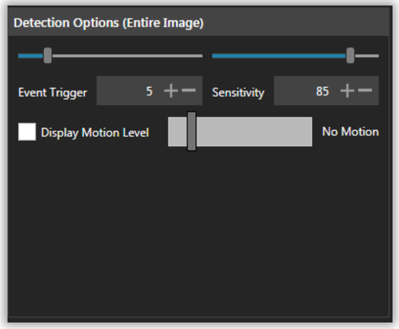

● Motion Detection (Entire Image)
Detection Options (Entire Image)

Event Trigger 2; Sensitivity 98

Detection Type: Camera Side

- **Detection Options (Entire Image)** - This area allows the configuration of **Event Trigger** and **Sensitivity** values for the entire image motion detection.
    - **Event Trigger**: Defines the percentage of visual area where change/motion is detected.
    - **Sensitivity**: Near-far gauge, the higher the sensitivity, the better the accuracy.

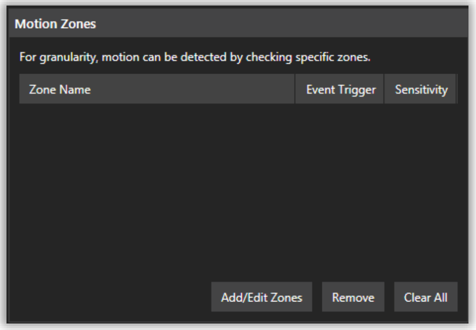
  A **live gauge** shows the occurrence of an event that triggers a motion detection, displaying a "Motion Detected" status message in orange letters when this happens; "***No Motion***" is the default status.



Event Trigger 5; Sensitivity 85

□ Display Motion Level — No Motion

- **Motion Zones** - This section provides an interface to define specific areas within the video feed where motion detection may be considered more critical for event monitoring.



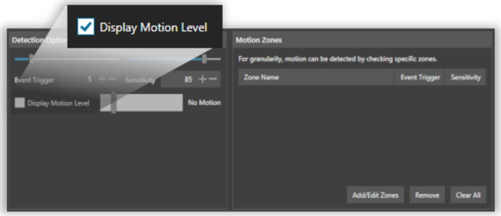
Motion Zones

For granularity, motion can be detected by checking specific zones.

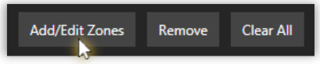
Zone Name	Event Trigger	Sensitivity

Motion Zones are **off** by default, which means the corresponding buttons (Add/Edit/Remove/Clear) are deactivated.

To activate them, check the **"Display Motion Level"** box on the left, under "**Detection Options (Entire Image**)".



To **Add** Motion Zones, click the "**Add/Edit Zones**" button and the **Motion Zone Configuration** screen will open.

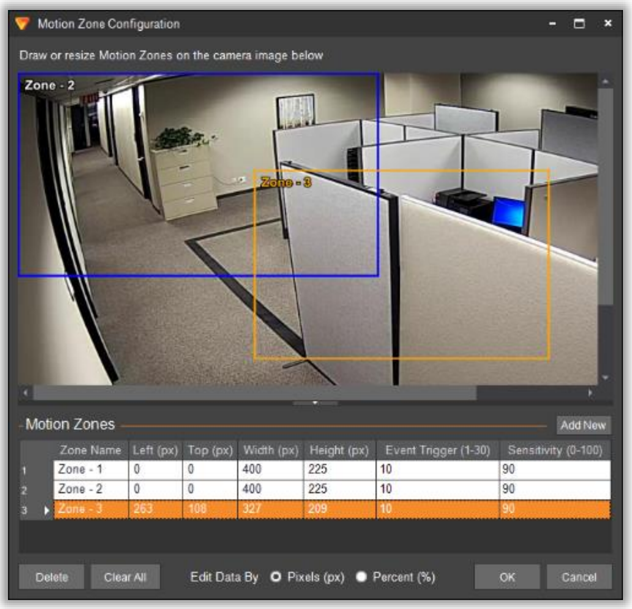


Start adding zones by **drawing or resizing** the desired areas ***directly on the video feed***, or by clicking "**Add New**".

The **Motion Zones table** shows the currently defined zones for the camera, with the corresponding settings and values. The selected one appears with orange background and an orange frame on the image.

Zones can be deleted individually by clicking the "**Delete**" button or cleared from the table by clicking "**Clear All**".

Data can also be edited by **Pixels** or **Percent**.



Motion Zone Configuration

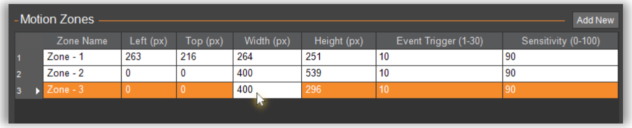
Draw or resize Motion Zones on the camera image below

Motion Zones

	Zone Name	Left (px)	Top (px)	Width (px)	Height (px)	Event Trigger (1-30)	Sensitivity (0-100)
1	Zone - 1	0	0	400	225	10	90
2	Zone - 2	0	0	400	225	10	90
3	Zone - 3	263	108	327	209	10	90

Edit Data By ○ Pixels (px) ● Percent (%)

Cells on the Motion Zones table ***can be directly edited*** by clicking on each cell and entering the desired value.

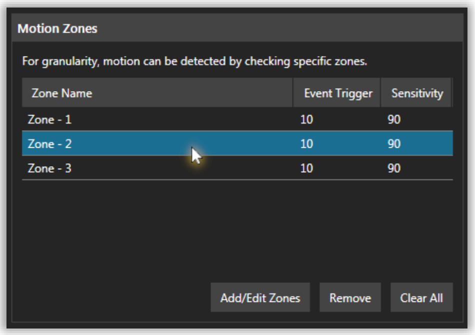


Motion Zones

	Zone Name	Left (px)	Top (px)	Width (px)	Height (px)	Event Trigger (1-30)	Sensitivity (0-100)
1	Zone - 1	263	216	264	251	10	90
2	Zone - 2	0	0	400	539	10	90
3	Zone - 3	0	0	400	296	10	90

Click “**OK**” to save the Motion Zones, and the Configuration window will close.

Now, the Zones previously defined ***will be shown*** on the Camera Properties page.



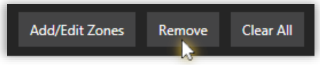
Motion Zones

For granularity, motion can be detected by checking specific zones.

Zone Name	Event Trigger	Sensitivity
Zone - 1	10	90
Zone - 2	10	90
Zone - 3	10	90

To delete a specific zone, highlight it with the cursor and click the “**Remove**” button.

To delete all zones from the table, click the “**Clear All**” button.



(6) CONTROL PANEL: DISPLAY

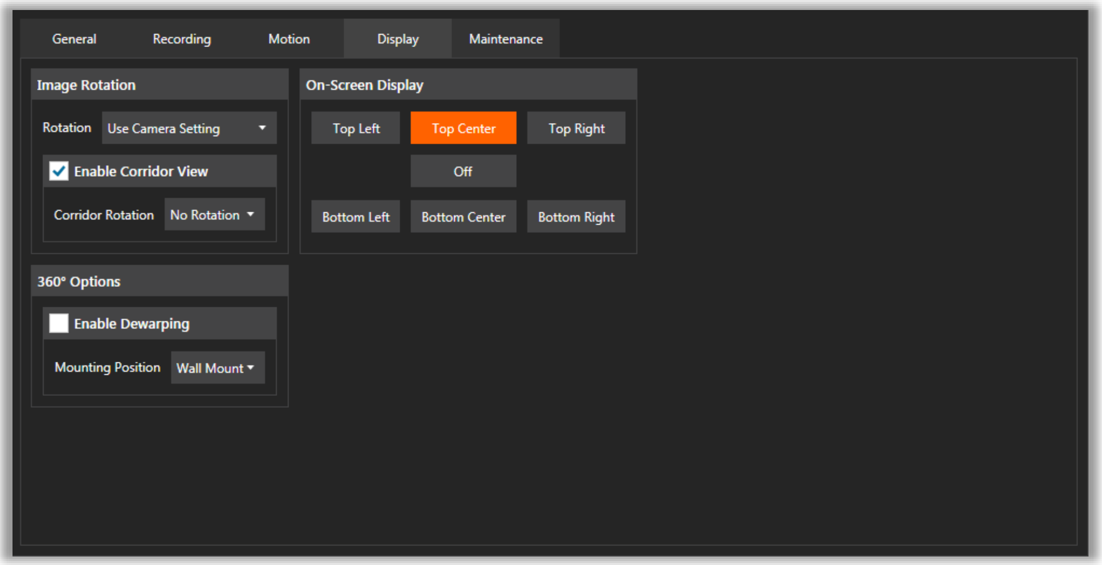
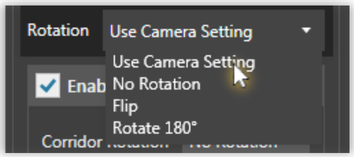
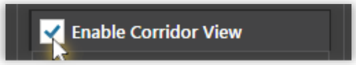


Image Rotation

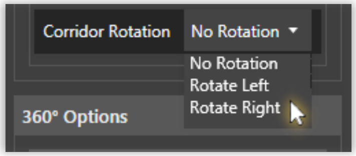
- **Rotation** – Drop-down list of available image rotation options; only for cameras that support this feature.



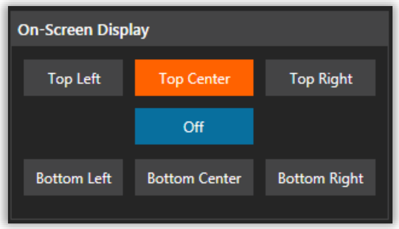
- **Enable Corridor View** – Enables 90° corridor view mode and rotation options below



- **Corridor Rotation** – Select either left or right rotation for Corridor View.

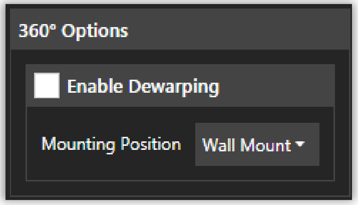


On-Screen Display - Displays and positions a built-in watermark on top of the live video.



360° Option

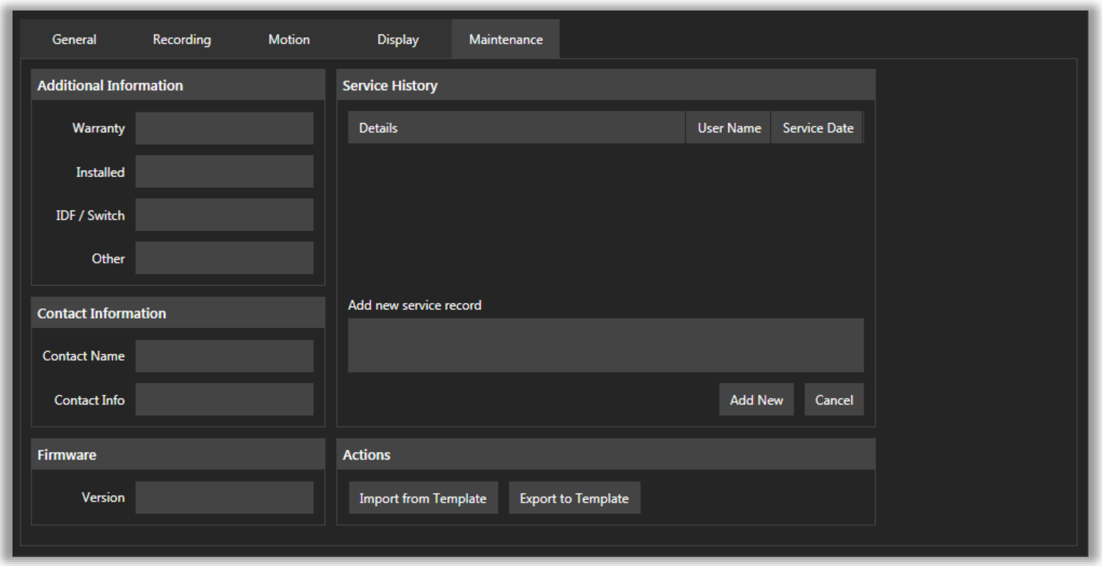
- Enable Dewarping – Check the box to activate Dewarping features on supported cameras.
- Mounting Position – After enabling dewarping, select the view orientation from the drop-down list.


360° Options

☐ Enable Dewarping

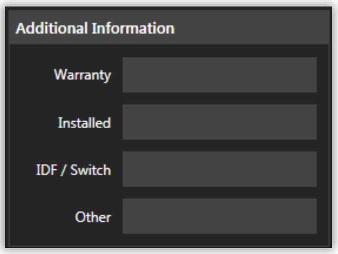
Mounting Position: Wall Mount

(7) CONTROL PANEL: MAINTENANCE



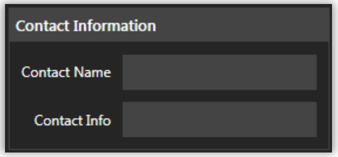
Additional Information

- *Warranty* – Date of expiration of the camera's warranty.
- *Installed*- Installation Date of the camera.
- *IDF/Switch* – Physical location of the switch that the camera is connected to.
- *Other* – Additional information deemed relevant for maintenance purposes.



Contact Information

- *Contact Name* – Name of key person(s) responsible for the camera.
- *Contact Info* - Phone number, email or any information to contact the key person(s).



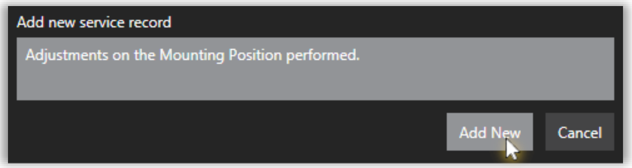
Firmware

- *Version* – Latest Firmware version number / date.

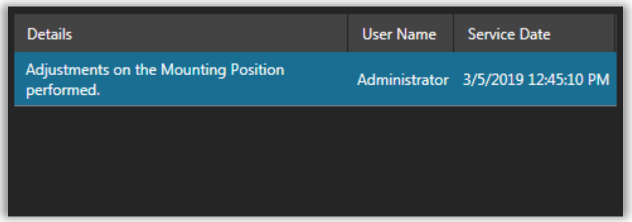
Service History - This area is used to keep a log of each maintenance-related activity for the camera.

To **Add** a new service record, start writing on the "***Add new service record***" box, describing the details of the activity; then, click "**Add**".

The information will be displayed on the **Service History** table, including the *User Name* and the *Service Date*, posted automatically.

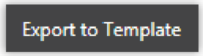


Adjustments on the Mounting Position performed.



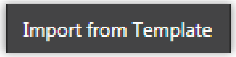
Details	User Name	Service Date
Adjustments on the Mounting Position performed.	Administrator	3/5/2019 12:45:10 PM

Actions



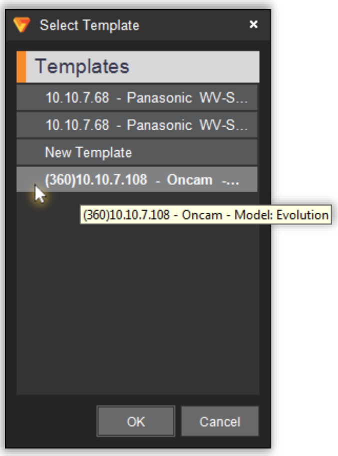
Click on “**Export to Template**” to create an external file with all the basic features and settings of the camera, which might be used to quickly configure similar cameras on separate instances.

VI MonitorPlus will create a new file with the name of the camera by default.



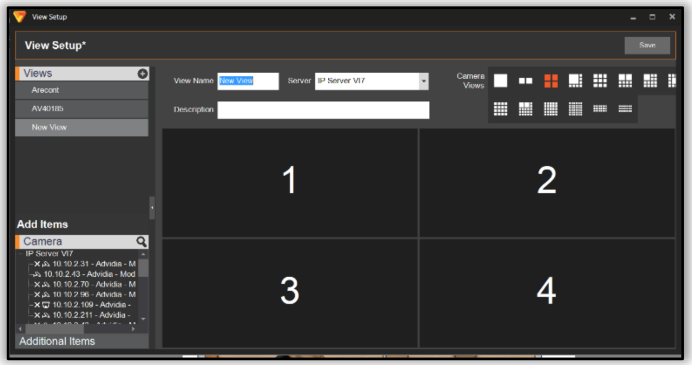
To import settings from a previously configured camera with similar or identical features, click “**Import from Template**” to open the Select Template window.

Select the desired template from the list; click “**OK**” and the Properties fields for the current camera will be automatically populated.


Select Template
×
Templates
10.10.7.68 - Panasonic WV-S...
10.10.7.68 - Panasonic WV-S...
New Template
(360)10.10.7.108 - Oncam -...
(360)10.10.7.108 - Oncam - Model: Evolution
OK
Cancel

4.10.C Views Setup

The left side menu works as in the previous section, with a list of all the existent views and then another with items available to be added to the views.



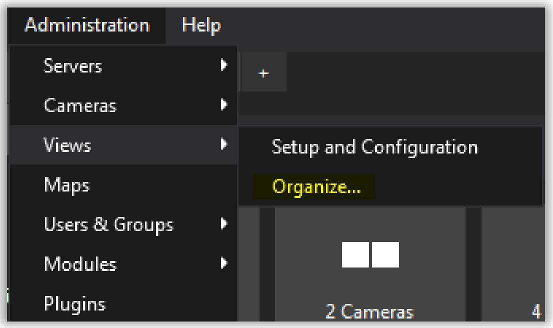
View Name: New View

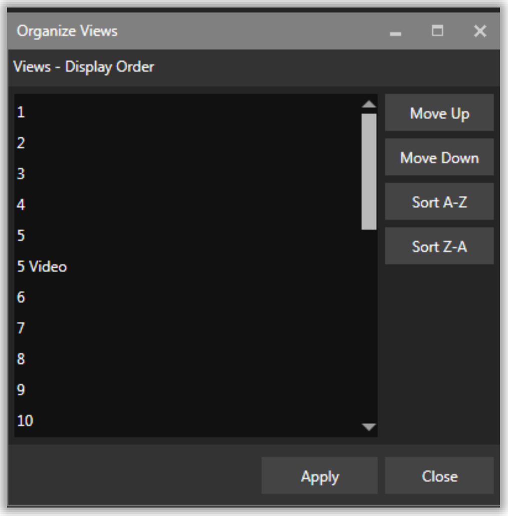
Server: IP Server VI7

Description:

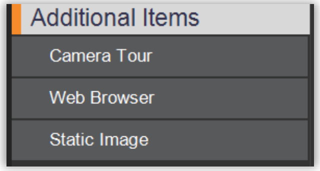
To add a new view, click on the + sign.
When the user selects a view from the list, it will appear on the screen. Drag and drop the desired cameras into place as they are to appear for viewing on the screen.

Fill in the name and description fields and click **Save** to save the view.





To organize the View order, select Administration from the menu ribbon, click **Views** and select **Organize**. Select the View you wish to organize into order and use the Move Up and Move Down buttons to rearrange the order. For organizations that wish to have the Views listed in alphabetical order, use the Sort A- Z button to order. Clicking the Sort Z-A button will reverse the order of the Views into descending order.



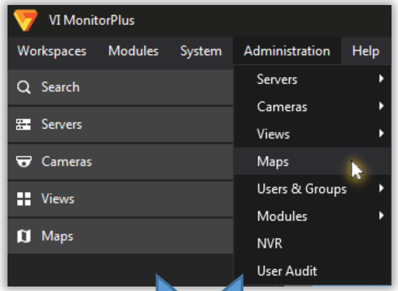
Views can be populated with static images, PDF documents, or URLs to a specific website. To add any of these items, click on the Additional Items link in the bottom left side of the page.

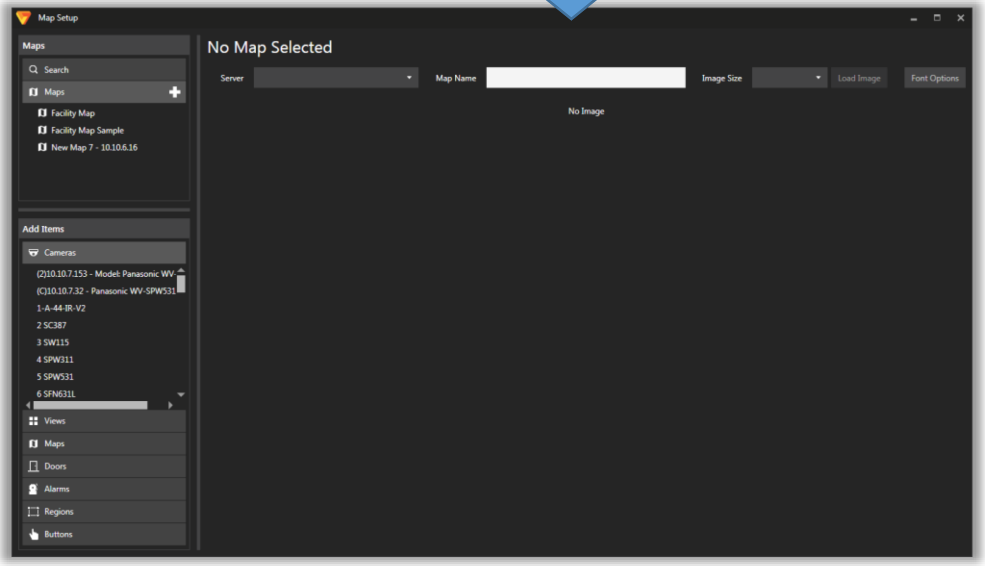
4.10.D Facility Maps Setup

Facility Maps are graphic representations of the facility's assets and their locations inside a building or campus. They may include: cameras, views, doors and alarms, among others, providing real-time access to video feeds, access control and other resources using a user-friendly interface.

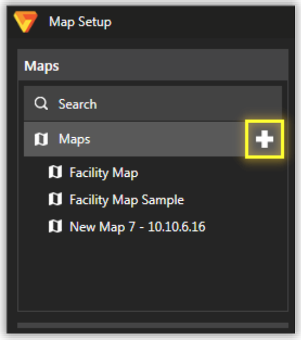
(1) CREATING FACILITY MAPS

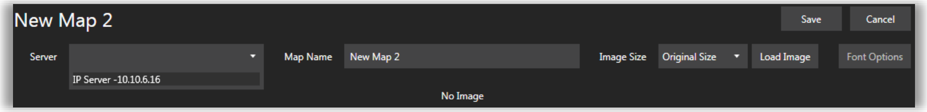
From the Main Menu, select "**Administration**", then "**Maps**". This will open the **Maps Setup** window (*see below*).





Click on the Plus **[+]** sign next to the "**Maps**" header. A **New Map** interface will open on the right side of the window (*see below*).



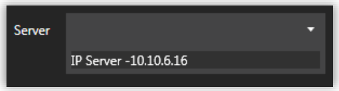


Server: IP Server -10.10.6.16

Map Name: New Map 2

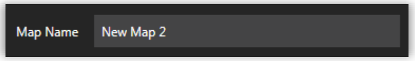
Image Size: Original Size

In the New Map area, select the **Server** in which your Map will appear using the corresponding drop-down list.



Server: IP Server -10.10.6.16

Define a **Name** for your Map.



Map Name: New Map 2

Select the **Image Size** (Original or Custom) from the drop-down list.

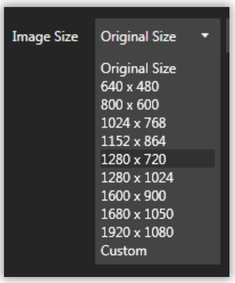
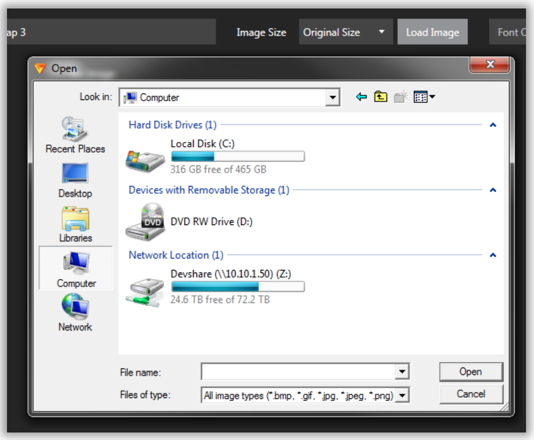
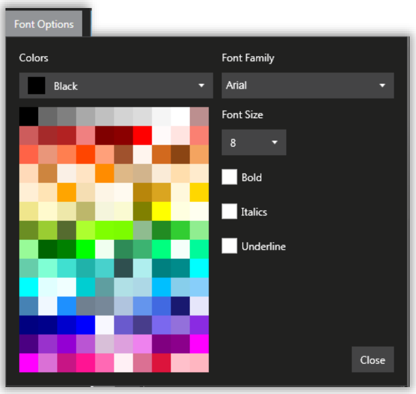


Image Size: Original Size

Click “**Load Image**” to browse and select the image file from your computer.



Click “**Font Options**” to open the corresponding window and select the color, family and size of your Map’s fonts.



Font Options

Colors: Black

Font Family: Arial

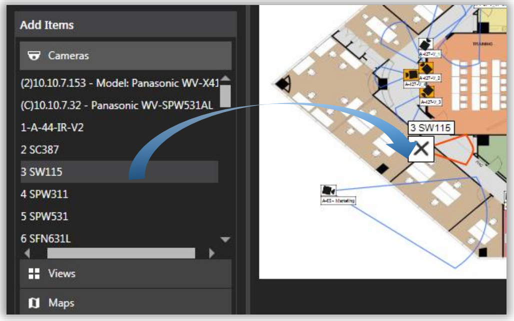
Font Size: 8

□ Bold

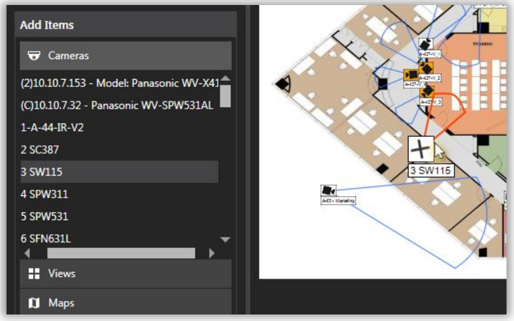
□ Italics

□ Underline

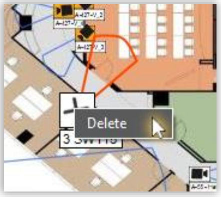
Once the Map image is properly positioned, start adding Cameras and other items to it by dragging and dropping them from the **Add Item** section on the left panel to the map.



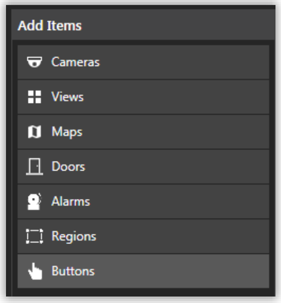
Once positioned on the map, items can be ***moved, rotated*** and ***resized*** using the mouse cursor to replicate their position and range.



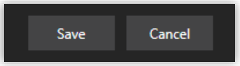
To **Delete** an item on the map, right-click your mouse while pointing to the item and select "**Delete**".



In addition to Cameras, ***Views***, ***Maps***, ***Doors***, ***Alarms***, ***Regions*** and ***Buttons*** can also be added to your Map.



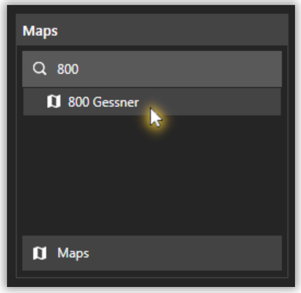
Click "**Save**" to save the new Map on your server, and it will appear on the left panel, under the Maps section.
Press "**Cancel**" if you do not want to save it.



(2) SEARCHING FACILITY MAPS

To search a specific map in your directory, click on "**Search**"from the left panel, then ***type the name of the map*** until it shows on the list.

Click on the map name from the list to open it.

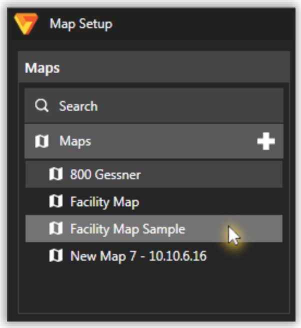


(3) EDITING FACILITY MAPS

To **Edit** or **Modify** a Facility Map, ***click on its name*** from the **Maps** list (left panel) or using the **Search** option.

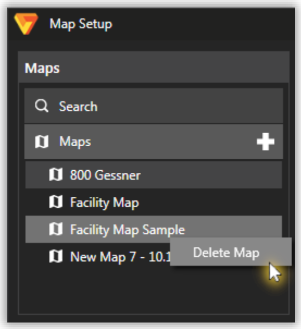
Once the map is open, proceed to make the changes following the instructions as indicated in the **Creating a Facility Map** section (*see above*).

Save your map after finishing.

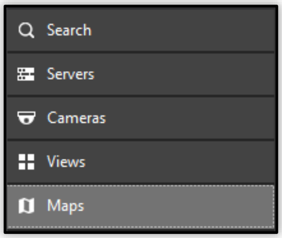


(4) DELETING FACILITY MAPS

To **Delete** a Facility Map, point the cursor on its name from the left panel list, then right-click on, select "**Delete**" and confirm the operation.



(5) VIEWING FACILITY MAPS



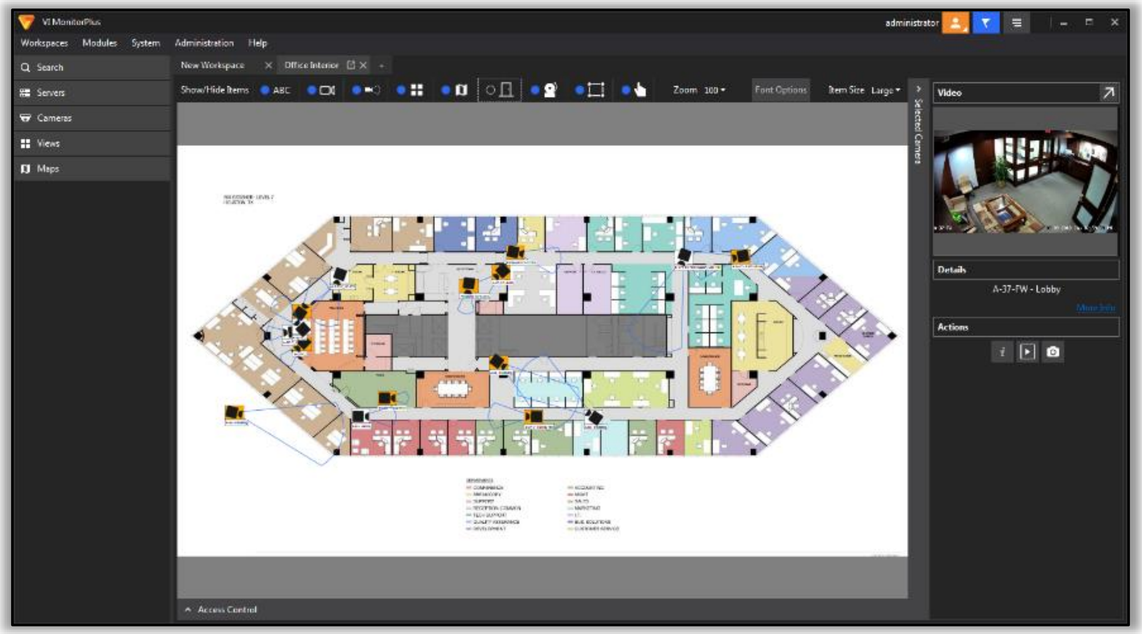
Facility Maps can be created in the VI MonitorPlus by a System Administrator to give a graphical representation of where cameras are located throughout a building or campus.

To view a Map in VI MonitorPlus, click **Maps** on the left navigation bar.

Opening a Map will replace the current workspace from the main view.

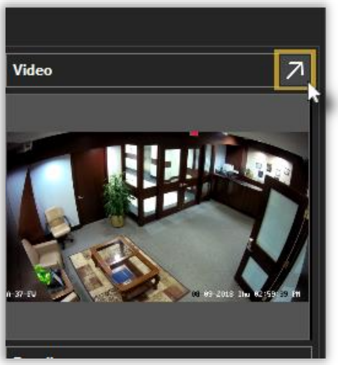
(6) VIEWING LIVE VIDEOS WITHIN FACILITY MAPS

To view live videos from a **Facility Map**, click on ***any Camera icon*** on the map itself, and the right panel will open automatically, displaying the view of selected camera's streaming video and its corresponding Details and Actions.



To **enlarge a live video view**, click on the **diagonal arrow** on the upper right corner of the workspace, above the minimized video view.

A new window will open on top of VI MonitorPlus, displaying the enlarged video streaming from the selected camera.



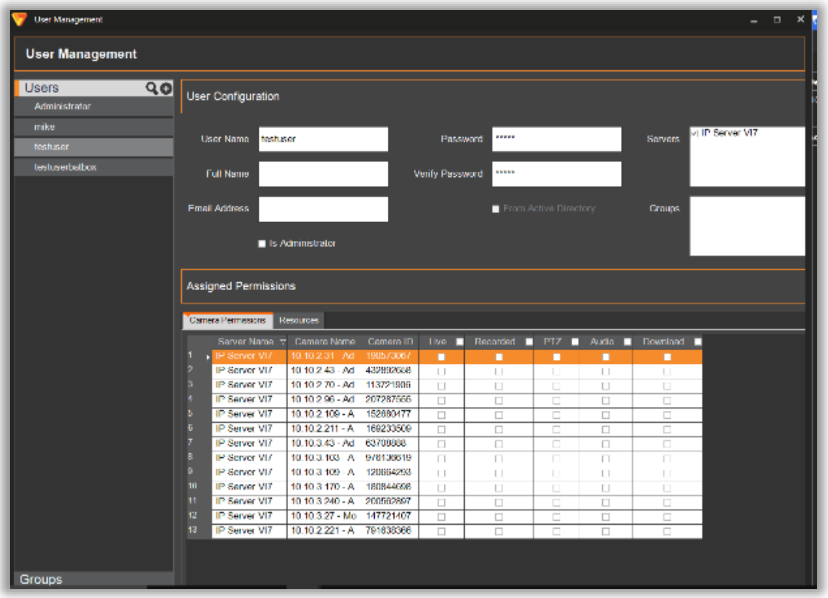
© 2019 – Panasonic System Solutions Company of North America
Last updated: Oct/28/2019

4.10.E Users & Groups

To manage VI MonitorPlus operators and user groups, use the **Users & Groups** button on the menu toolbar. A menu in the left side of the screen will open to select active Users (and in this case, also Groups).

4.10.E Users & Groups

To manage VI MonitorPlus operators and user groups, use the **Users & Groups** button on the menu toolbar. A menu in the left side of the screen will open to select active Users (and in this case, also Groups).



User Name: testuser
Password: *****
Verify Password: *****
Full Name:
Email Address:
Servers: ☑ IP Server VI7
Groups:
■ From Active Directory
■ Is Administrator

	Server Name	Camera Name	Camera ID	Live ■	Recorded ■	PTZ ■	Audio ■	Download ■
1	IP Server VI7	10.10.2.31 - Ad	1905/3067	■	■	■	■	■
2	IP Server VI7	10.10.2.43 - Ad	432892668	□	□	□	□	□
3	IP Server VI7	10.10.2.70 - Ad	113721806	□	□	□	□	□
4	IP Server VI7	10.10.2.96 - Ad	207287566	□	□	□	□	□
5	IP Server VI7	10.10.2.109 - A	152880477	□	□	□	□	□
6	IP Server VI7	10.10.2.211 - A	169233509	□	□	□	□	□
7	IP Server VI7	10.10.3.43 - Ad	63708888	□	□	□	□	□
8	IP Server VI7	10.10.3.103 - A	978136619	□	□	□	□	□
9	IP Server VI7	10.10.3.109 - A	120864293	□	□	□	□	□
10	IP Server VI7	10.10.3.170 - A	180844698	□	□	□	□	□
11	IP Server VI7	10.10.3.240 - A	200562897	□	□	□	□	□
12	IP Server VI7	10.10.3.27 - Mo	147721407	□	□	□	□	□
13	IP Server VI7	10.10.2.221 - A	791838366	□	□	□	□	□

When a user is selected, the loaded user page appears (*see left*).

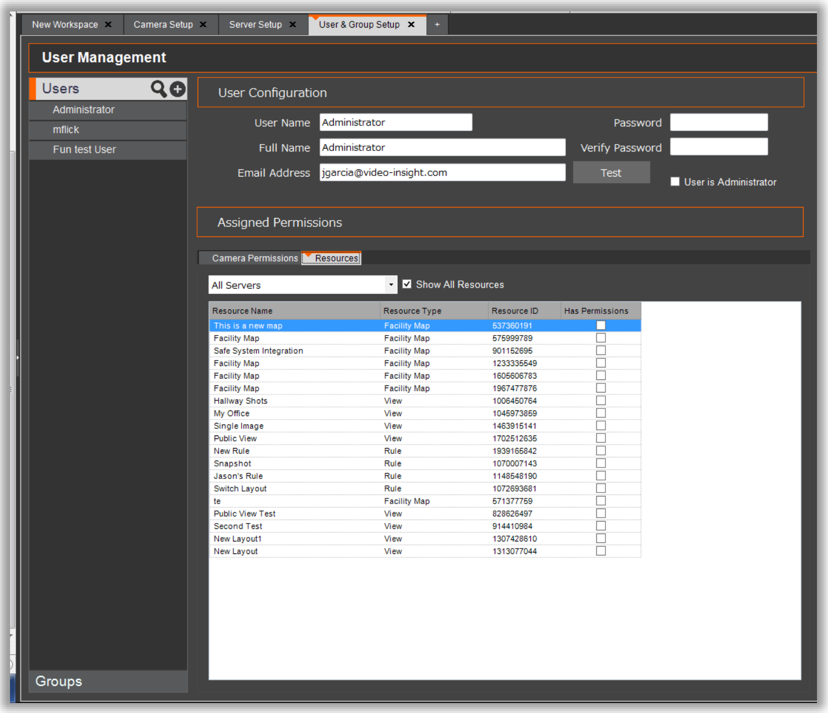
User data such as name, login information and e-mail is displayed and able to be edited.

Permissions are also shown in the bottom grid.

Users can also select the Resources tab, which will show the managed resources (facility maps, views and rules).

(1) GROUPS

Groups can be assigned during creation by selecting the **Group** in the checkbox on the right side of the screen.



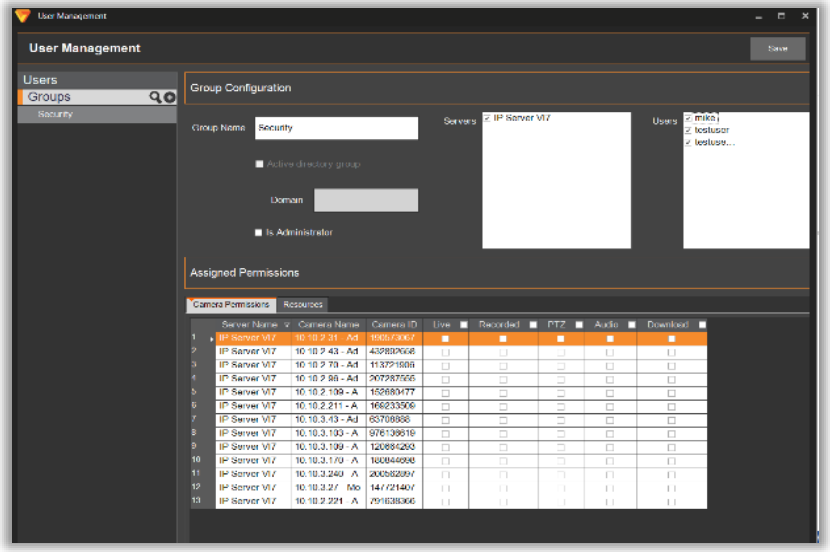
User Name: Administrator
Full Name: Administrator
Email Address: jgarcia@video-insight.com
Password:
Verify Password:
□ User is Administrator

All Servers ☑ Show All Resources

Resource Name	Resource Type	Resource ID	Has Permissions
This is a new map	Facility Map	537360191	□
Facility Map	Facility Map	575999789	□
Safe System Integration	Facility Map	901152695	□
Facility Map	Facility Map	1233335549	□
Facility Map	Facility Map	1605606783	□
Facility Map	Facility Map	1967477876	□
Hallway Shots	View	1006450764	□
My Office	View	1045973859	□
Single Image	View	1463915141	□
Public View	View	1702512635	□
New Rule	Rule	1939165842	□
Snapshot	Rule	1070007143	□
Jason's Rule	Rule	1148548190	□
Switch Layout	Rule	1072693681	□
te	Facility Map	571377759	□
Public View Test	View	828626497	□
Second Test	View	914410984	□
New Layout1	View	1307428610	□
New Layout	View	1313077044	□

Similar to selecting a user, a group can also be selected from the left menu.

To add a user or a group, the Administrator must click on the + sign next to Users or Groups in the left side menu.



Group Configuration

Group Name: Security

Servers: ☑ IP Server VI7

Users: ☑ mike ☑ testuser ☑ testuse...

■ Active directory group

Domain

■ Is Administrator

	Server Name	Camera Name	Camera ID	Live ■	Recorded ■	PTZ ■	Audio ■	Download ■
1	IP Server VI7	10.10.2.31 - Ad	190573067	□	□	□	□	□
2	IP Server VI7	10.10.2.43 - Ad	432892668	□	□	□	□	□
3	IP Server VI7	10.10.2.70 - Ad	113721906	□	□	□	□	□
4	IP Server VI7	10.10.2.98 - Ad	207287566	□	□	□	□	□
5	IP Server VI7	10.10.2.109 - A	152680477	□	□	□	□	□
6	IP Server VI7	10.10.2.211 - A	169233509	□	□	□	□	□
7	IP Server VI7	10.10.3.43 - Ad	63708688	□	□	□	□	□
8	IP Server VI7	10.10.3.103 - A	976138619	□	□	□	□	□
9	IP Server VI7	10.10.3.109 - A	120884293	□	□	□	□	□
10	IP Server VI7	10.10.3.170 - A	180844698	□	□	□	□	□
11	IP Server VI7	10.10.3.240 - A	200562097	□	□	□	□	□
12	IP Server VI7	10.10.3.27 - Mo	147721407	□	□	□	□	□
13	IP Server VI7	10.10.2.221 - A	791638306	□	□	□	□	□

Fill in the blanks for username, full name, email address and password to setup a new user or group.

The roles of the user can be customized by selecting camera specific permissions using the table (seen left).

(2) SETUP AND CONFIGURATION

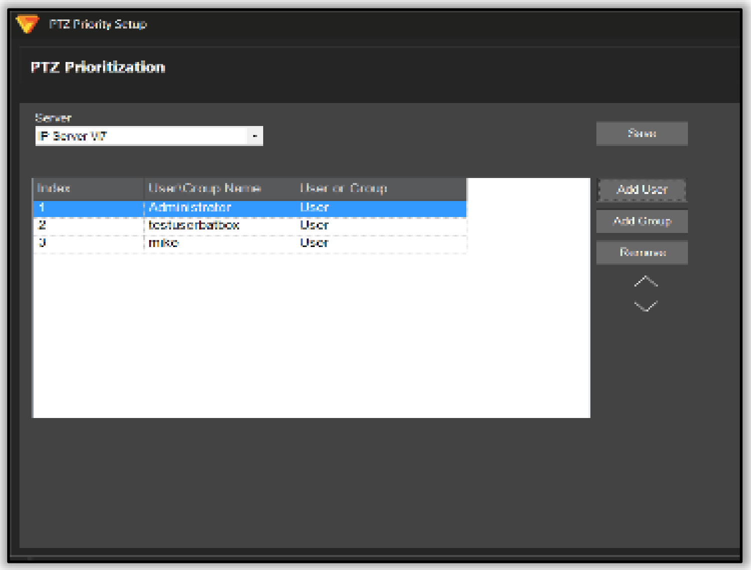
(2A) USER MANAGEMENT

VI MonitorPlus can be used to connect and add Users by way of **Active Directory** or **LDAP**. While the prerequisites vary between the two, we will cover only those associated with Active Directory.

Security will persist on the server only when "Enable Security" has been checked within the **Administration > Servers > Advanced** tab.

(3) PTZ PRIORITIZATION

This legacy PTZ Prioritization function 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.

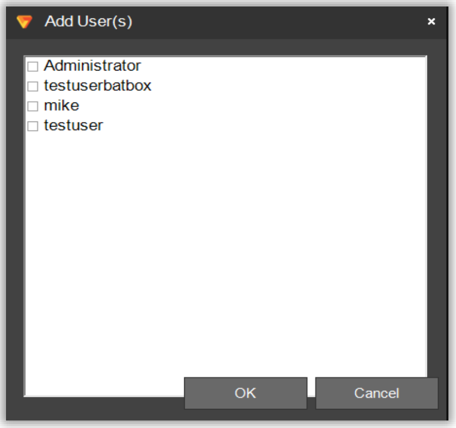


Server: P Server VI7

Index	User/Group Name	User or Group
1	Administrator	User
2	testuserbatbox	User
3	mike	User

To enable, open VI MonitorPlus and navigate to **Administration → Modules**. Select **PTZ Prioritization**.

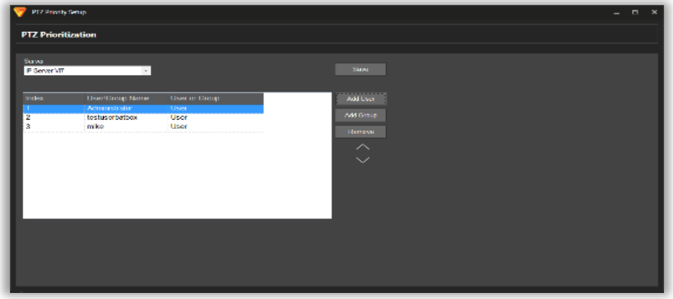
Here, select either **Add User** or **Add Group**, depending on the desired configuration.
A new pop-up window appears.



□ Administrator
□ testuserbatbox
□ mike
□ testuser

Next, select the desired users for PTZ prioritization. Once the desired users have been selected, press **OK**.

If the added users aren't appearing the in correct order, select one user and change its location within the list by using the Up and Down arrows. (pictured below)



Server: IP Server VIT

Index	User/Group Name	User or Group
1	Administrator	User
2	testuserbatbox	User
3	mike	User

To move a second user, click on the user, and again use the up and down arrows on the right to move the users into a Top → Down hierarchical order of PTZ use prioritization. Once all users appear in the desired order, click Save.

NOTE - PTZ Prioritization is now configured. 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 after the higher-ranking member stops using the PTZ controls.

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.

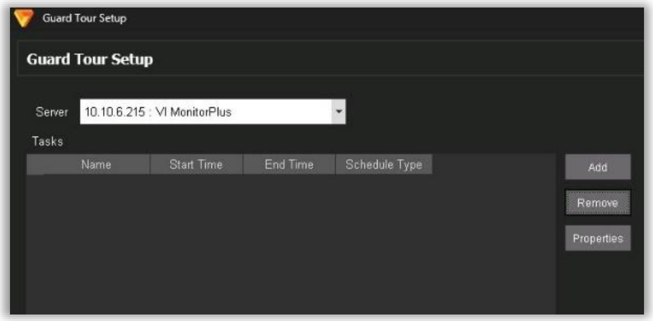
4.10.F Modules

(1) GUARD TOURS

Guard Tours are a select number of cameras and live views that are set to create a pop-up window during a pre-determined period. The Administrator can control who has access to a guard tour, when the pop-ups appear, which cameras are to be monitored, and if manual data entry must be performed to move on to subsequent camera views for accountability purposes. Below are the steps for creating and a new Guard Tour.

Guard Tours Setup

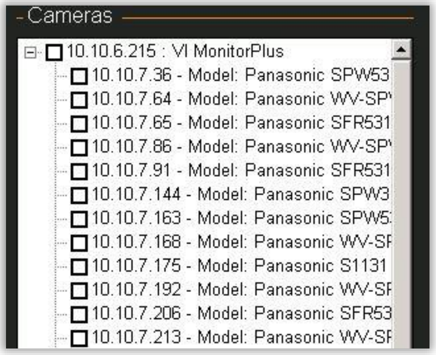
To setup a new Guard Tour, log in as an Administrator. Next, select **Administration > Modules > Guard Tour**.



Server: 10.10.6.215 : VI MonitorPlus

Once the new window appears, select the server with the Users, Groups and Cameras that are going to be used with the new Guard Tour, then click **Add**.

Provide a name for the new Guard Tour.

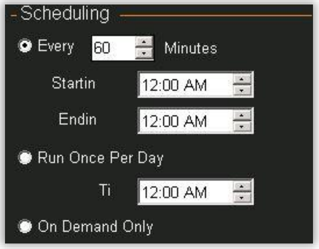


- □ 10.10.6.215 : VI MonitorPlus
  - □ 10.10.7.36 - Model: Panasonic SPW53
  - □ 10.10.7.64 - Model: Panasonic WV-SP'
  - □ 10.10.7.65 - Model: Panasonic SFR531
  - □ 10.10.7.86 - Model: Panasonic WV-SP'
  - □ 10.10.7.91 - Model: Panasonic SFR531
  - □ 10.10.7.144 - Model: Panasonic SPW3
  - □ 10.10.7.163 - Model: Panasonic SPW5
  - □ 10.10.7.168 - Model: Panasonic WV-SF
  - □ 10.10.7.175 - Model: Panasonic S1131
  - □ 10.10.7.192 - Model: Panasonic WV-SF
  - □ 10.10.7.206 - Model: Panasonic SFR53
  - □ 10.10.7.213 - Model: Panasonic WV-SF

Select the cameras to be used on the Guard Tour.

Each Camera must have the check box marked for it to appear within the Guard Tour.

Scheduling



● Every 60 Minutes

Startin 12:00 AM

Endin 12:00 AM

○ Run Once Per Day

Ti 12:00 AM

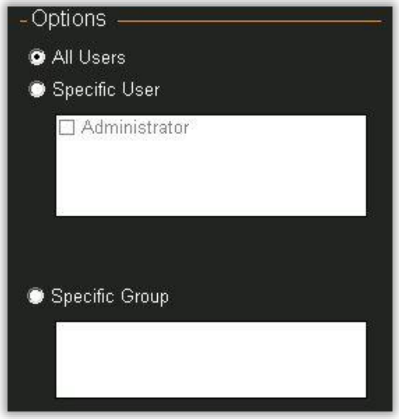
○ On Demand Only

Scheduling the Guard Tour so that it appears several times (within a specific range of time) is possible.

A maximum time limit of 1440 minutes (24 hours) is permitted when electing to populate the Guard Tour window every XXX number of minutes. Default is 60 minutes.

The Guard Tour can be configured to run once a day as a specific time, or Demand Only.

Options:



Options

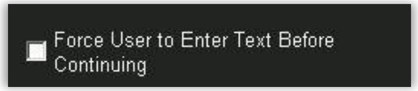
● All Users

○ Specific User

□ Administrator

○ Specific Group

Within the Options section, this allows the admin to select specific users or groups that the guard tour will apply to. Configuring more than one tour for different needs is possible.

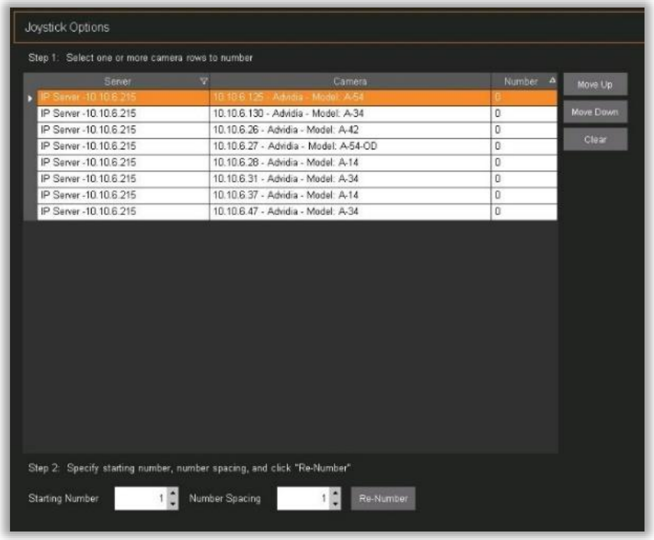


□ Force User to Enter Text Before Continuing

Selecting the check box for this feature forces the user to be required to enter text within the Guard Tour window before dismissing a screen.

Click **OK** to save the guard tour.

(2) JOYSTICK OPTIONS



Joystick Options

Step 1: Select one or more camera rows to number

Server	Camera	Number
IP Server -10.10.6.215	10.10.6.125 - Advidia - Model: A-54	0
IP Server -10.10.6.215	10.10.6.130 - Advidia - Model: A-34	0
IP Server -10.10.6.215	10.10.6.26 - Advidia - Model: A-42	0
IP Server -10.10.6.215	10.10.6.27 - Advidia - Model: A-54-OD	0
IP Server -10.10.6.215	10.10.6.28 - Advidia - Model: A-14	0
IP Server -10.10.6.215	10.10.6.31 - Advidia - Model: A-34	0
IP Server -10.10.6.215	10.10.6.37 - Advidia - Model: A-14	0
IP Server -10.10.6.215	10.10.6.47 - Advidia - Model: A-34	0

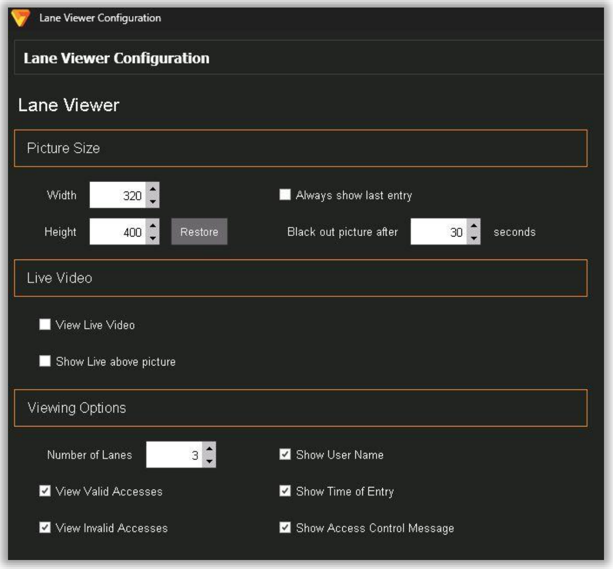
Step 2: Specify starting number, number spacing, and click "Re-Number"

Starting Number 1 Number Spacing 1

Joystick Options allows the administrator to specify a camera to a designated button on the Video Insight joystick.

NOTE - For more information about the Video insight customizable joystick, please contact your **Panasonic Sales** representative.

(3) LANE VIEWER



Lane Viewer Configuration

Lane Viewer

Picture Size

Width 320

Height 400 Restore

□ Always show last entry

Black out picture after 30 seconds

Live Video

□ View Live Video

□ Show Live above picture

Viewing Options

Number of Lanes 3

☑ View Valid Accesses

☑ View Invalid Accesses

☑ Show User Name

☑ Show Time of Entry

☑ Show Access Control Message

The **Lane Viewer Configuration** screen displays all the related settings to Lane Viewer, a function that works with Access Control servers.

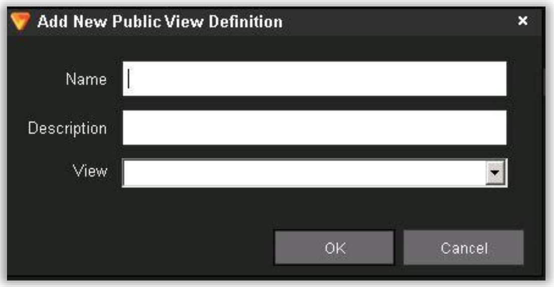
The ability to modify Lane Viewer picture size (width, height and blackout), Lane Viewing options (number of lanes, valid and invalid accesses, show name, time, and message) and live video options (view live video, show live above picture).

(4) PUBLIC VIEW MONITOR

Public View Monitor is obsolete. The functionality has been transferred to **VI Video WallPlus**. For more details, please refer to the VI Video WallPlus documentation.

(4A) CONFIGURATION

After the installation is complete, launch VI MonitorPlus and click on **Administration** > **Views**. Create the layout you want visible in Public View Monitor Application.



Name

Description

View

Once the View is created, click **Administration**> **Modules** and select Public View Monitor in the left tree.

Click **Add**. Create a name and description for your Public View Window and select the View you wish to display.

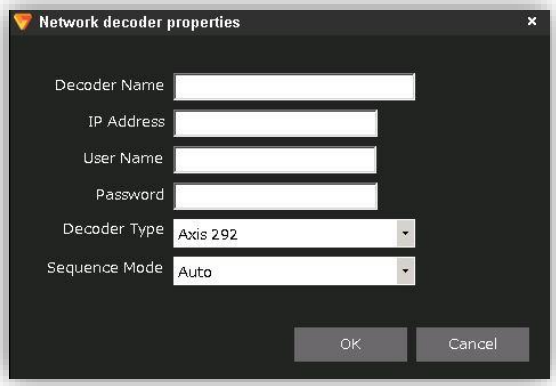
Click **OK** and then **Apply** in the Public View Monitor area to save your changes.

NOTE - The **ONLY** layouts that will appear in the Public View Monitor menu are the layouts specifically created for use in the Public View Monitor layout list, not the VI MonitorPlus layout list.

(5) TV DECODERS

IP Server can record data sent by a **TV Decoder**. Adding a TV Decoder to IP Server within VI MonitorPlus will allow customizing its name, and adding it to the IP Server's cameras list on the left-side of the screen.

Network decoder properties: Configuration



Network decoder properties

Decoder Name

IP Address

User Name

Password

Decoder Type: Axis 292

Sequence Mode: Auto

Enter the IP Address, username and password of the decoder, followed by the model number and camera sequence mode for the workspace used to display the decoder.

(6) VIDEO WALLPLUS

Video WallPlus allows monitoring a large quantity of cameras at one time, controlling the content of several TV monitors from a single console. Video WallPlus allows each TV monitor to display a single camera, a server or a customized layout.

For more information about Video WallPlus, please refer to the supplemental documentation found in Appendix D, below.

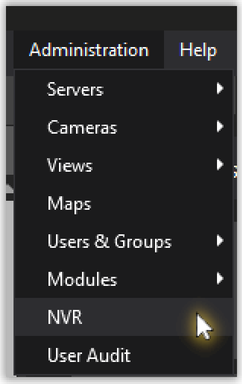
4.10.G NVR Enrollment and Integration

VI MonitorPlus supports the enrollment of the following Panasonic NVR camera models:

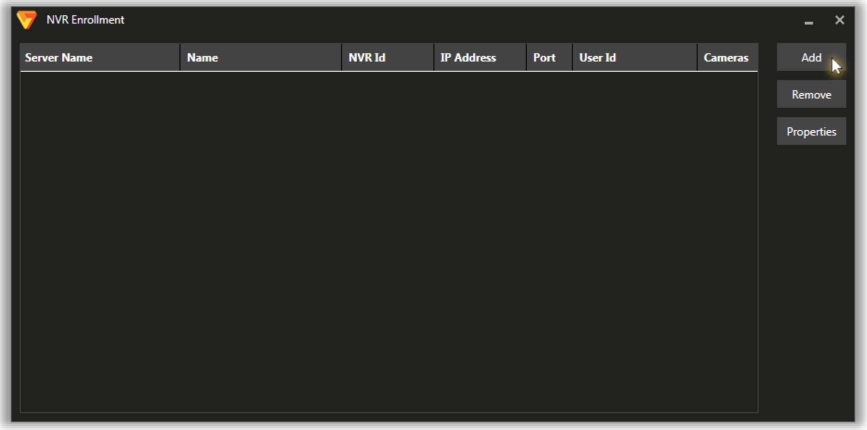
- WJ-NX400
- WJ-NX300
- WJ-NX200
- WJ-ND400
- WJ-NV300
- WJ-NV200

This support allows users to access live and recorded video through the VI MonitorPlus client. To utilize this functionality, Administrators need to follow the following steps for setup and enrollment.

Select **Administration** -> **NVR**.



To add a new NVR device, click **Add**.



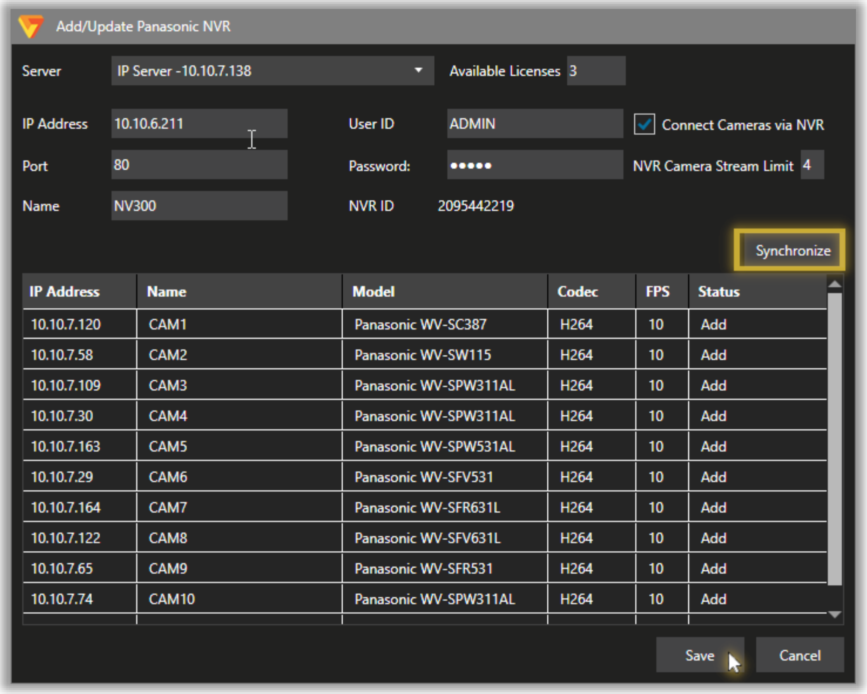
Assign a server to the NVR device by selecting a **Server** in the drop-down box. Next, enter **IP Address** and **Port** of the NVR (default = 80), along with **User ID** and **Password**.

Define a Name for the NVR in the **Name** field.

To complete, click on the **Synchronize** button.

The detected cameras will be displayed in the table below.

Click **Save** to complete the NVR enrollment.



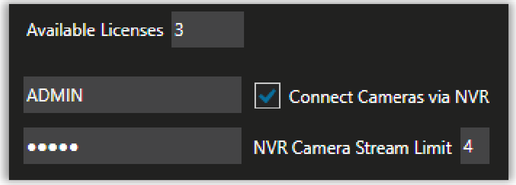
Add/Update Panasonic NVR

Server: IP Server -10.10.7.138
Available Licenses: 3
IP Address: 10.10.6.211
User ID: ADMIN
☑ Connect Cameras via NVR
Port: 80
Password: •••••
NVR Camera Stream Limit: 4
Name: NV300
NVR ID: 2095442219

IP Address	Name	Model	Codec	FPS	Status
10.10.7.120	CAM1	Panasonic WV-SC387	H264	10	Add
10.10.7.58	CAM2	Panasonic WV-SW115	H264	10	Add
10.10.7.109	CAM3	Panasonic WV-SPW311AL	H264	10	Add
10.10.7.30	CAM4	Panasonic WV-SPW311AL	H264	10	Add
10.10.7.163	CAM5	Panasonic WV-SPW531AL	H264	10	Add
10.10.7.29	CAM6	Panasonic WV-SFV531	H264	10	Add
10.10.7.164	CAM7	Panasonic WV-SFR631L	H264	10	Add
10.10.7.122	CAM8	Panasonic WV-SFV631L	H264	10	Add
10.10.7.65	CAM9	Panasonic WV-SFR531	H264	10	Add
10.10.7.74	CAM10	Panasonic WV-SPW311AL	H264	10	Add

The Add/Update Panasonic NVR interface shows:

- Number of available NVR licenses
- Option to connect camera streaming via NVR
- Limit of NVR camera stream (default=4)



Available Licenses 3

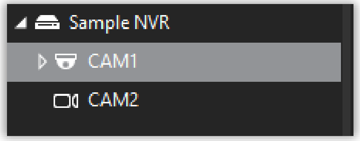
ADMIN

☑ Connect Cameras via NVR

●●●●●

NVR Camera Stream Limit 4

Once enrolled, the left tree will refresh with a new NVR Server icon along with the name of the NVR selected from enrollment.



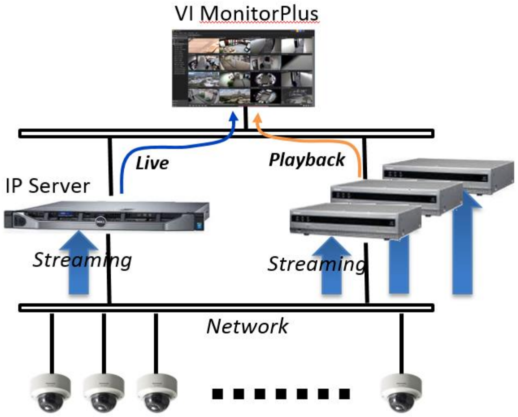
Sample NVR

CAM1

CAM2

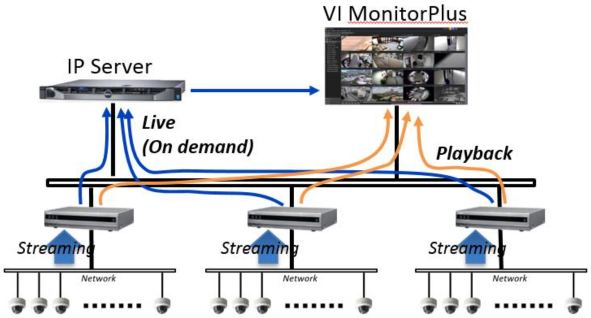
(1) NVR INTEGRATION

NVR ARCHITECTURE UP TO V7.2



- NVR cameras are managed as normal cameras in live video.
- IP Server must be connected to the camera network.
- Dual network bandwidth needed for each camera.

NVR ARCHITECTURE STARTING FROM V7.3



- NVR camera live feed may be restricted due to NVR resources.
- IP Server does not have to be connected to the camera network.
- Single network bandwidth required for each camera.

(2) MAXIMUM NUMBER OF CONCURRENT FTP REQUESTS

The following table shows the maximum number of concurrent FTP request for each model:

Camera model	Max. concurrent FTP requests
WJ-NX400	8
WJ-NX300	8
WJ-NX200	8
WJ-ND400	8
WJ-NV300	2
WJ-NV200	2

(3) ENABLING MEDIA FOUNDATION ON WINDOWS SERVER

For certain NVR cameras (e.g. **ND400**), the ability to view recordings from VI MonitorPlus is not available by default.

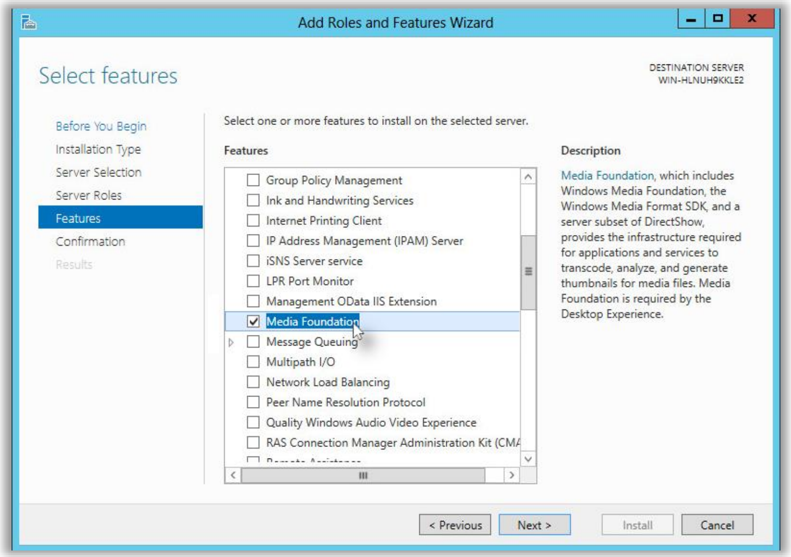
To enable it, the **Media Foundation** feature must be installed on the Windows Server where NVR cameras are currently enrolled.

The procedure is as follows:

1. Execute Server Manager:
   - (**Start** > **Administrative Tools** > **Server Manager**)

   or:

   - Type "**ServerManager**" in the shortcut location box and click "**Next**"
2. Select "**Manage**" and "**Add Roles and Features**"
3. Select "**Features**"
4. Check the "**Media Foundation**" option
5. Click "**Next**"



Add Roles and Features Wizard

Select features

DESTINATION SERVER
WIN-HLNUH9KKLE2

Select one or more features to install on the selected server.

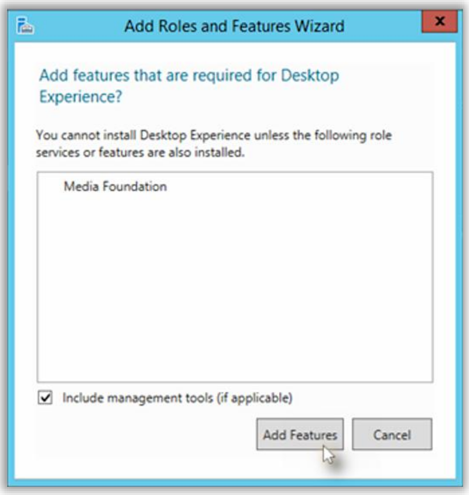
Features

- □ Group Policy Management
- □ Ink and Handwriting Services
- □ Internet Printing Client
- □ IP Address Management (IPAM) Server
- □ iSNS Server service
- □ LPR Port Monitor
- □ Management OData IIS Extension
- ☑ Media Foundation
- □ Message Queuing
- □ Multipath I/O
- □ Network Load Balancing
- □ Peer Name Resolution Protocol
- □ Quality Windows Audio Video Experience
- □ RAS Connection Manager Administration Kit (CMA

Description

Media Foundation, which includes Windows Media Foundation, the Windows Media Format SDK, and a server subset of DirectShow, provides the infrastructure required for applications and services to transcode, analyze, and generate thumbnails for media files. Media Foundation is required by the Desktop Experience.

When asked to install the additional feature, click "**Add Features**", then "**Install**". ***Restart the server***.



Add Roles and Features Wizard

Add features that are required for Desktop Experience?

You cannot install Desktop Experience unless the following role services or features are also installed.

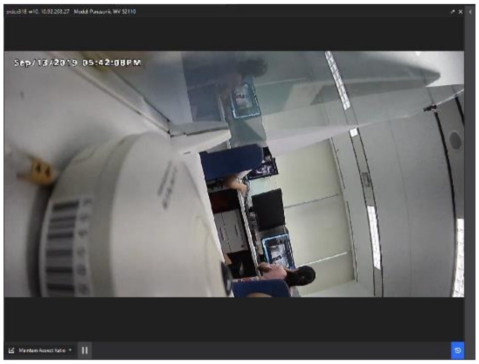
Media Foundation

☑ Include management tools (if applicable)

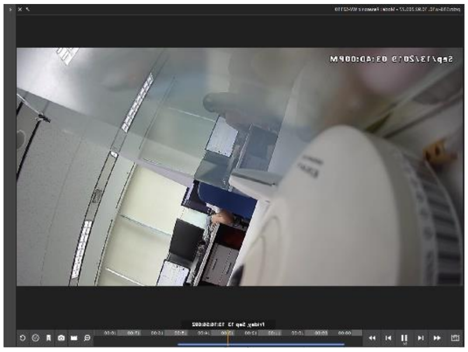
4.10.H User Audit Video Logging

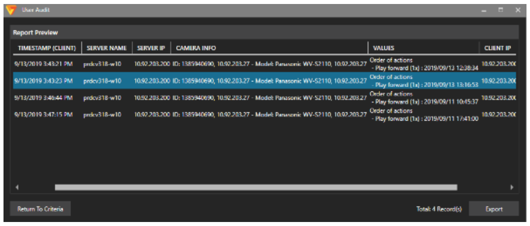
VI Monitor Plus User Audit function now records when users start to playback and save videos. The Audit log can be shown when users exit the playback function. This can be done from a single camera or multiple cameras. The User Audit function is set to off for all users. Users will have to turn the function **ON** to use.

Open in playback mode.



When opened, select the time the playback was executed.





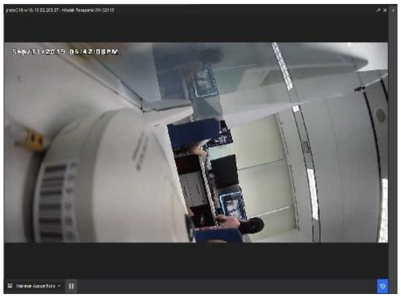
User Audit

Report Preview

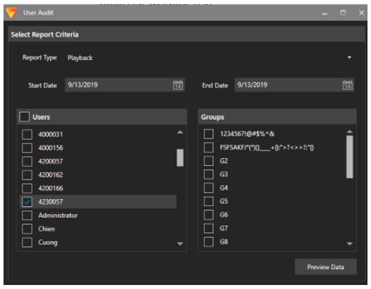
TIMESTAMP (CLIENT)	SERVER NAME	SERVER IP	CAMERA INFO	VALUES	CLIENT IP
9/13/2019 3:43:21 PM	prdcv318-w10	10.92.203.200	ID: 1385940690, 10.92.203.27 - Model: Panasonic WV-S2110, 10.92.203.27	Order of actions - Play forward (1x) : 2019/09/13 12:38:34	10.92.203.20
9/13/2019 3:43:23 PM	prdcv318-w10	10.92.203.200	ID: 1385940690, 10.92.203.27 - Model: Panasonic WV-S2110, 10.92.203.27	Order of actions - Play forward (1x) : 2019/09/13 13:16:53	10.92.203.20
9/13/2019 3:46:44 PM	prdcv318-w10	10.92.203.200	ID: 1385940690, 10.92.203.27 - Model: Panasonic WV-S2110, 10.92.203.27	Order of actions - Play forward (1x) : 2019/09/11 10:45:37	10.92.203.20
9/13/2019 3:47:15 PM	prdcv318-w10	10.92.203.200	ID: 1385940690, 10.92.203.27 - Model: Panasonic WV-S2110, 10.92.203.27	Order of actions - Play forward (1x) : 2019/09/11 17:41:00	10.92.203.20

Return To Criteria   Total: 4 Record(s)   Export

Close play back mode.



Select the user, start date, due date, report type as play back, and preview data.



User Audit

Select Report Criteria

Report Type: Playback

Start Date: 9/13/2019   End Date: 9/13/2019

□ Users
- □ 4000031
- □ 4000156
- □ 4200057
- □ 4200162
- □ 4200166
- ☑ 4230057
- □ Administrator
- □ Chien
- □ Cuong

Groups
- □ 1234567!@#$%^&
- □ FSFSAKFJ"(")()___+{}:">?<>>?:"{}
- □ G2
- □ G3
- □ G4
- □ G5
- □ G6
- □ G7
- □ G8

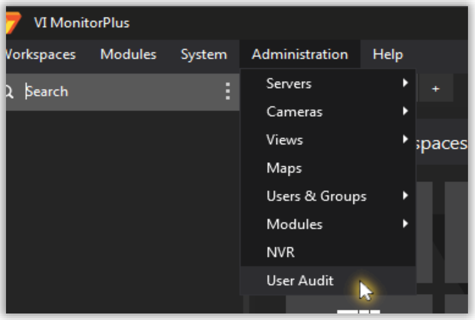
Preview Data

4.10.I User Audit Reports

VI MonitorPlus features the **User Audit** reporting tool, which generates a parametrized report with data about the login sessions of a specific user or a group of users, as well as the resources utilized during said sessions.

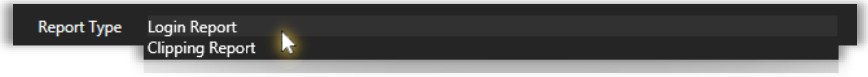
The User Audit data will only be stored for 30 days on a first-in, first-out basis. The oldest records will be overwritten automatically with the newest ones, following the 30-days cycle. The User Audit function is set to off for all users. Users will have to turn the function **ON** to use.

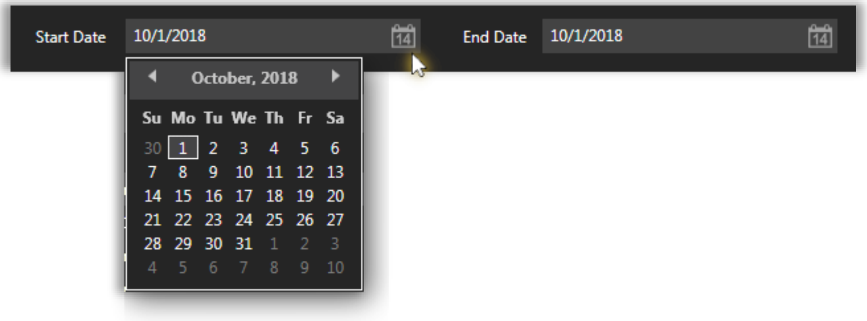
This tool can be accessed selecting the **User Audit** option under the **Administration** tab.



In the **User Audit** window, select the parameters for the report:

- Report Type
- Start and End date





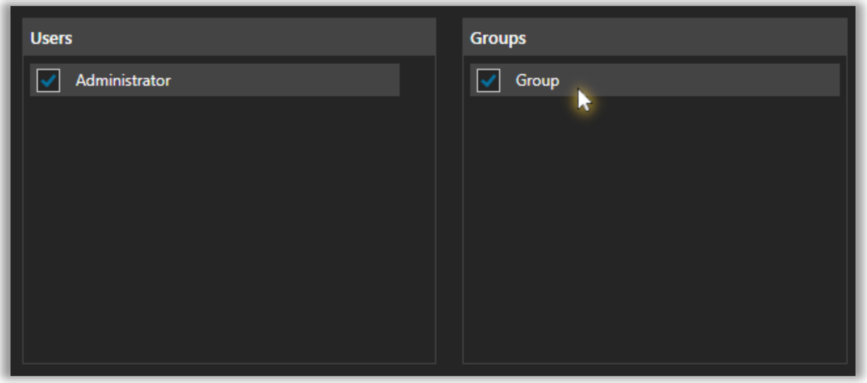
Start Date 10/1/2018

End Date 10/1/2018

October, 2018

Su	Mo	Tu	We	Th	Fr	Sa
30	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	1	2	3
4	5	6	7	8	9	10

- Users and Groups



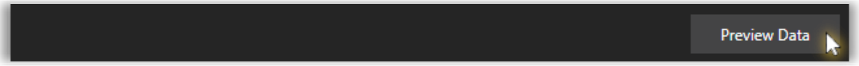
Users

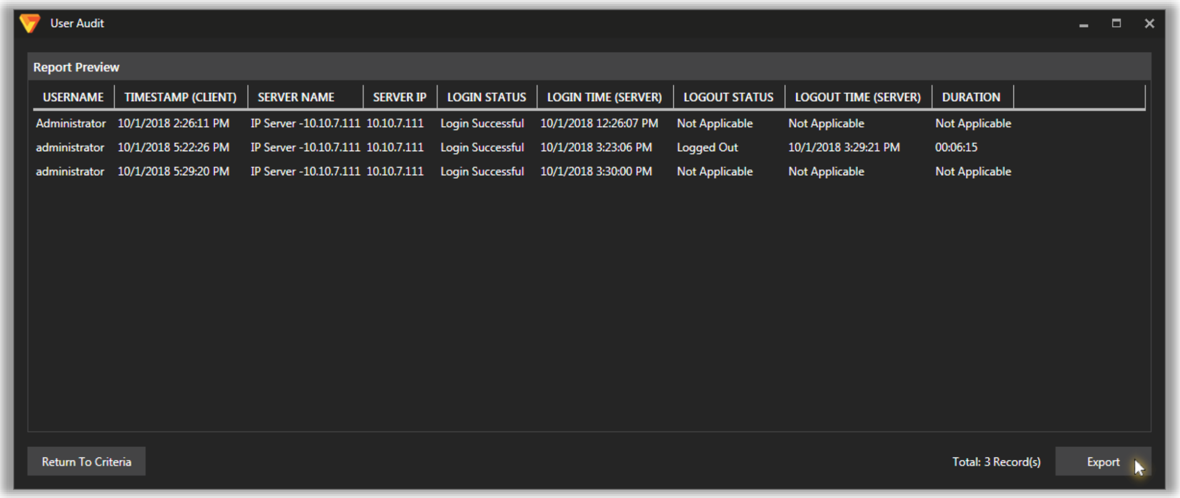
☑ Administrator

Groups

☑ Group

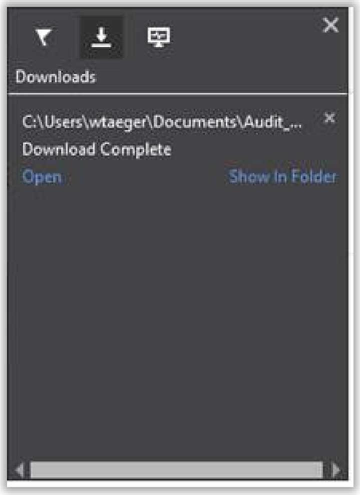
Once the parameters are selected, click on **Preview Data**.





USERNAME	TIMESTAMP (CLIENT)	SERVER NAME	SERVER IP	LOGIN STATUS	LOGIN TIME (SERVER)	LOGOUT STATUS	LOGOUT TIME (SERVER)	DURATION
Administrator	10/1/2018 2:26:11 PM	IP Server -10.10.7.111	10.10.7.111	Login Successful	10/1/2018 12:26:07 PM	Not Applicable	Not Applicable	Not Applicable
administrator	10/1/2018 5:22:26 PM	IP Server -10.10.7.111	10.10.7.111	Login Successful	10/1/2018 3:23:06 PM	Logged Out	10/1/2018 3:29:21 PM	00:06:15
administrator	10/1/2018 5:29:20 PM	IP Server -10.10.7.111	10.10.7.111	Login Successful	10/1/2018 3:30:00 PM	Not Applicable	Not Applicable	Not Applicable

The **Report Preview** will display the output before generating the report itself. When ready, click on **Export** to create the report, or **Return to Criteria** to redefine the parameters.



The Report will be generated and downloaded to a predefined folder, in CSV format.

Click on **Open** to view the report or **Show in Folder** to retrieve the CSV file.

5. WEB CLIENT

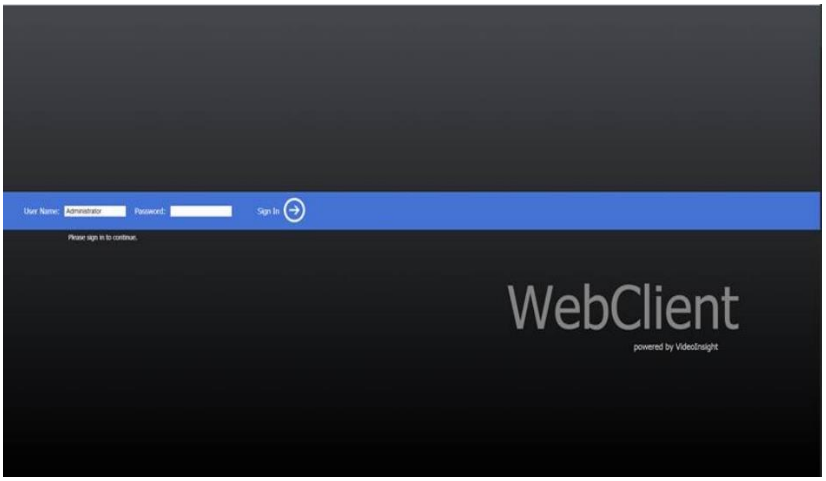
The **Web Client** is a free thin client application that allows the access to live and recorded video from any web browser. An optional ActiveX control can be used when viewing the Web Client in **Internet Explorer**.

The Web Client requires **IIS v 6.0** (or later) to be installed on the **IP Server** machine.

5.1 LOGGING IN

Access the Web Client using **http://<SERVERIP>/videoinsight** or the URL provided by the IP Server Administrator, using the browser of your choice.

Enter the **User Name** and **Password** for your account and click **Login**.



User Name: Administrator

Password:

Please sign in to continue.

5.2 LIVE VIDEO

Once logged in, the **Web Client** will display the first 30 cameras in the Server list (where 30 or more cameras have been added to the IP Server).

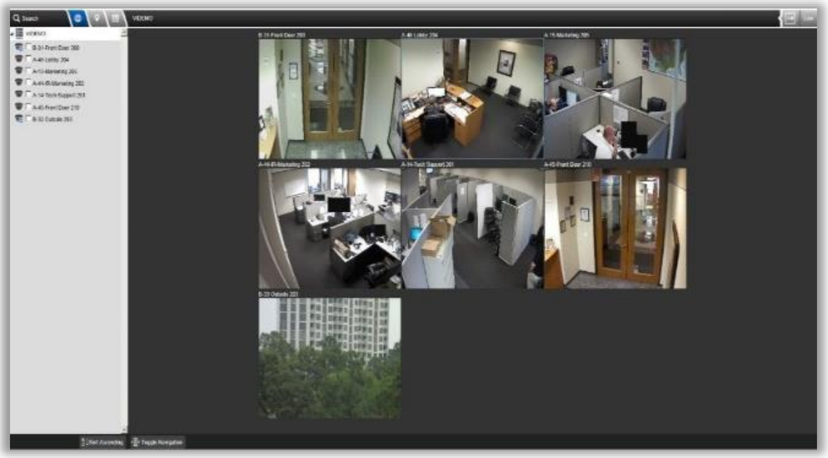
To view the names of the Cameras, expand the **Server Name** in the left tree.

After selecting a camera from the left tree, the Web Client will only display the video for that camera.

There are **2 options** to view a single camera:

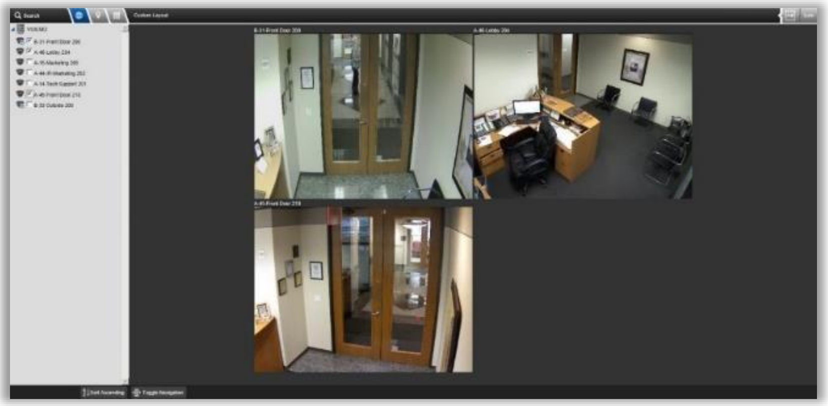
1. Click on the Camera's live image.
2. Click on the Camera's name in the left tree

The image from the selected camera will be displayed over the other cameras in the visible layout.



From this view it is possible to:

- Perform a digital zoom
- Move the camera (PTZ supported cameras)
- Take a snapshot from the live video
- Tiew the video in its true aspect ratio
- View recorded video.



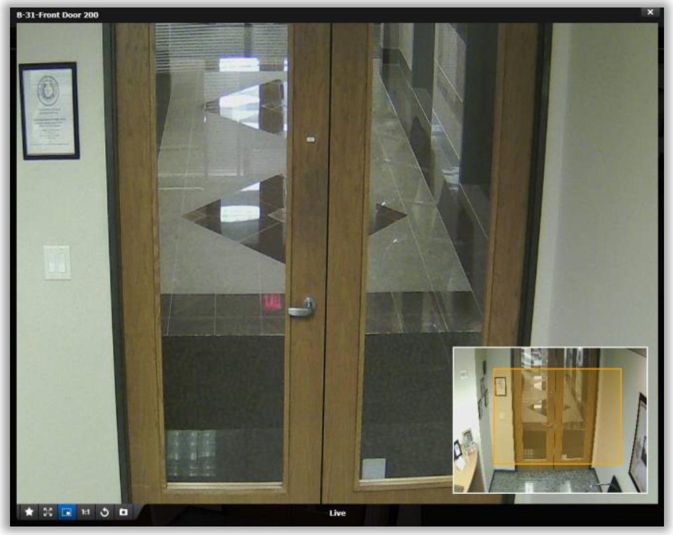
5.2.A Camera Manipulation

(1) DIGITAL ZOOM

To perform a Digital Zoom:

1. Select the **Digital Zoom** button on the video toolbar.

2. Click and drag from left to right in your area of interest.
3. Drawing this zone will enlarge the area to full screen.

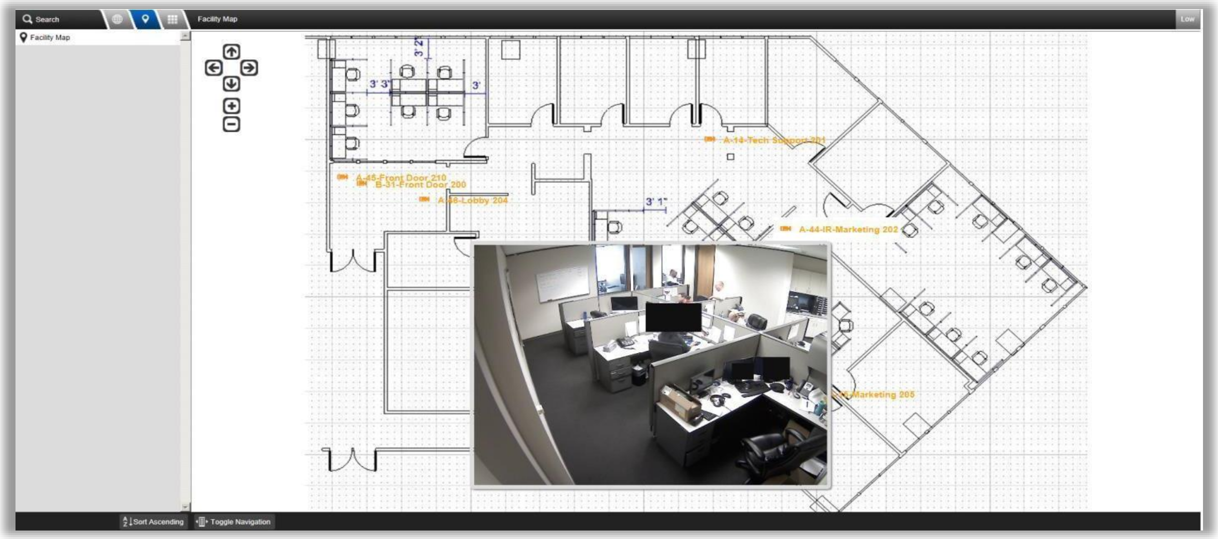


To view the full image once again, click the **Reset** button or double-click on the image.

NOTE - Snapshots of the zoomed image can be taken, but, unlike VI MonitorPlus, it is not possible to move within the zoomed image on the Web Client.

5.3 FACILITY MAPS

To view **Facility Maps** from within the Web Client, click on the **Map** icon found in the left tree.

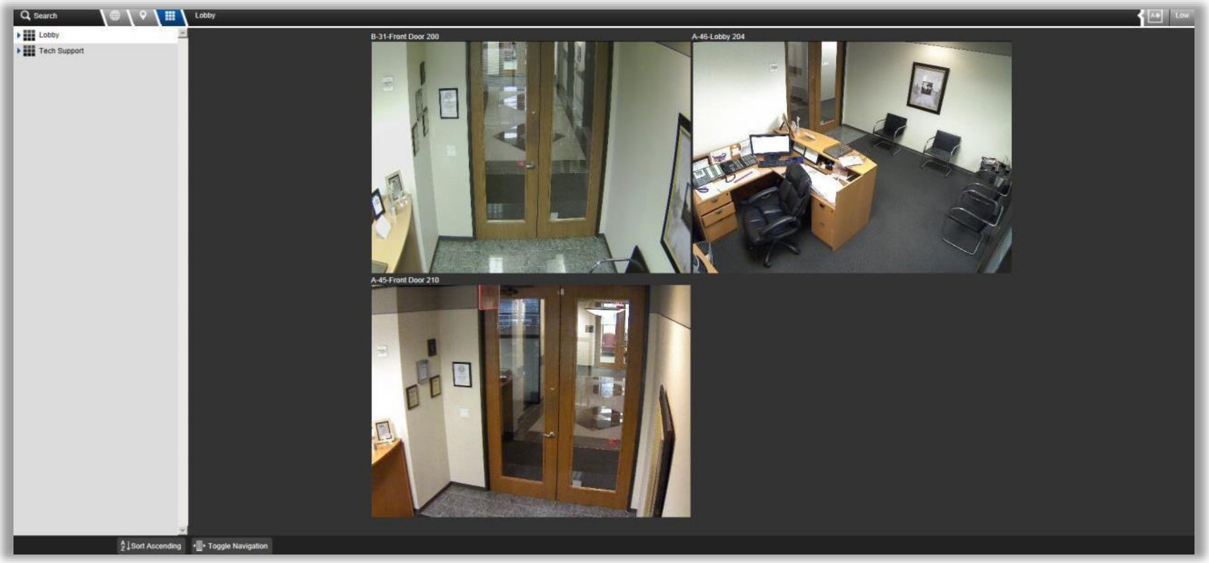


Hover the mouse cursor over a Camera Name/Icon to display its Live Video.

5.4 LAYOUT DIRECTORY

Custom **Views** can be accessed by clicking the **Layouts** button at the top of the left tree.

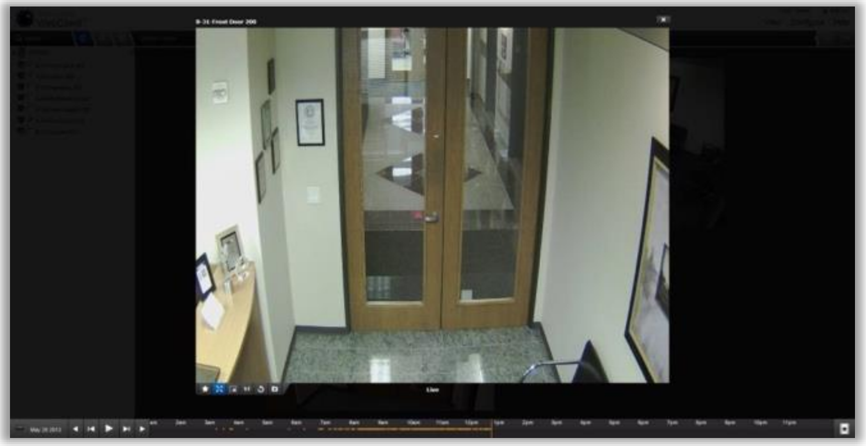
Similar to the default **Enterprise View** that appears after logging into the Web Client, clicking on a single camera view allows the user to customize the Layout.



This is accomplished by expanding the **Layout** camera list and checking off which cameras are desired for viewing.

5.5 RECORDED VIDEO

To access recorded video in the Web Client, click on the camera image of the camera to display the timeline video of available recorded video.



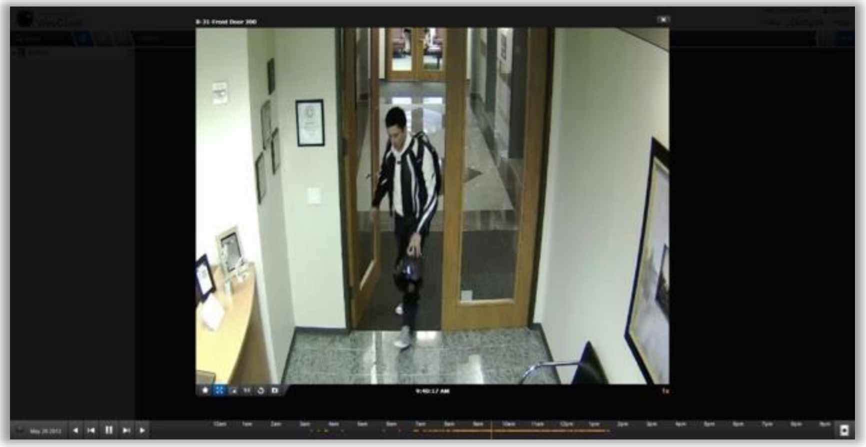
NOTE - Allow initial loading time on the first camera displayed.

The Timeline, displayed across the bottom of the image, can be used to review the footage recorded for that day.

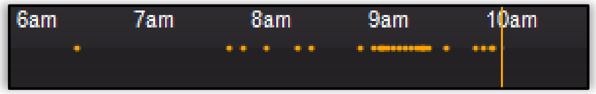
D rag the mouse along the timeline to select the desired timeframe to view.

The Web Client will load the recorded video file for that time and start playing it back.

To view recorded video from previous days, click on the ***date*** in the lower left-hand corner of the image to bring up a calendar.



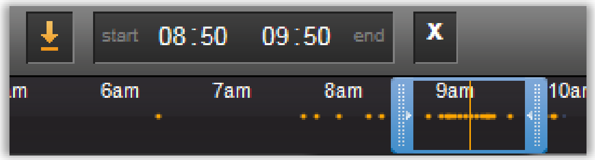
Areas shaded ***Orange*** contain playable recorded video.



5.5.A Creating Clips

To create a clip, click on the film icon at the end of the Timeline, this will display the clip/time selector

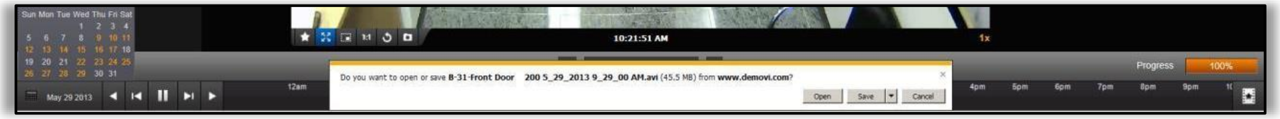
Select the time range by adjusting the blue sliders or typing into the text fields which display the time.



Next, click the Download icon.

NOTE - A progress bar will appear on the right area of the screen while downloading.

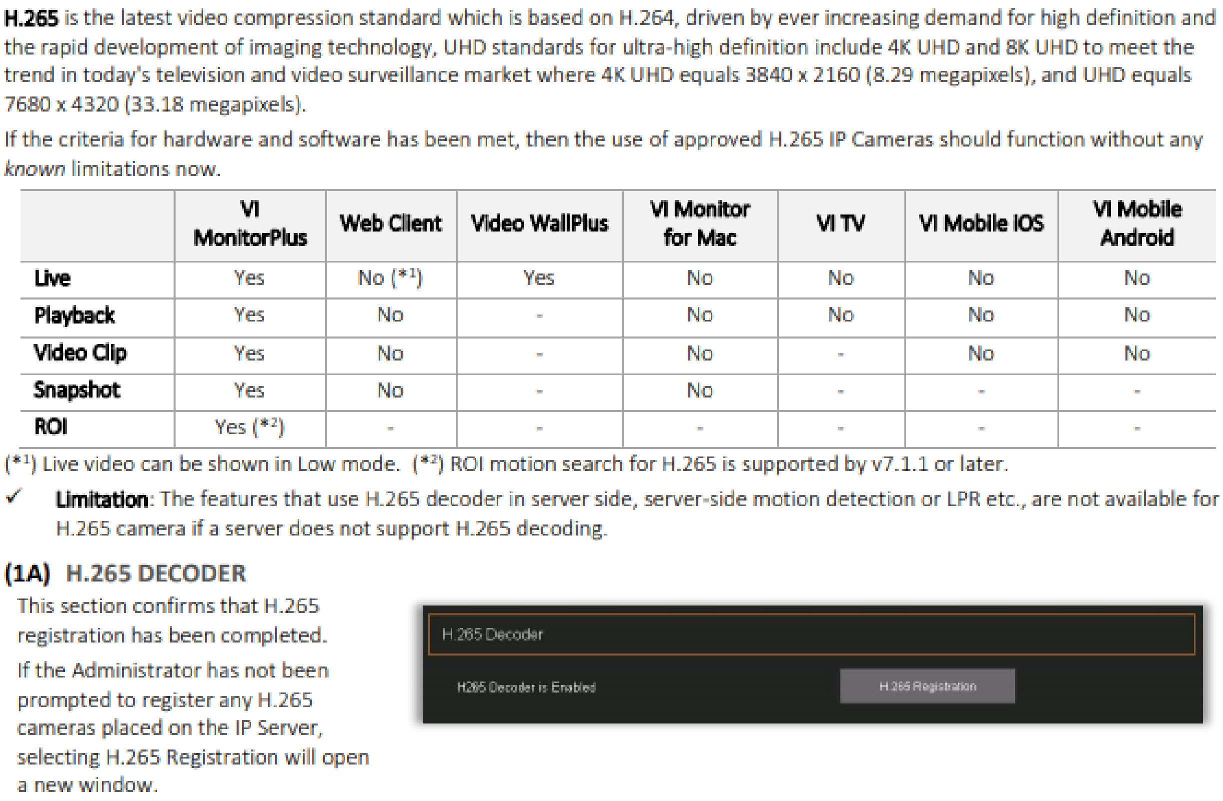
Once the download is complete, you will be asked if you would like to Open or Save the video. Opening the video will immediately start playback on the local media player, while saving will allow the server to save and store the file for review later.



Do you want to open or save **B-31-Front Door 200 5_29_2013 9_29_00 AM.avi** (45.5 MB) from **www.demovi.com**?

Unlike VI MonitorPlus, this video is stored in the compression format which the camera is recording in, so if the camera is recording H.265 video, then the .AVI will require an H.265 codec to play. If you are unable to playback the clips saved through the Web Client, please see your System Administrator to obtain the required codecs needed for your cameras.

While VI Mobile does not directly support H.265 cameras through software or server transcoding, if Hardware coding in both VI iOS and VI Mobile Android are both turned off, H.265 cameras do work.



H.265 is the latest video compression standard which is based on H.264, driven by ever increasing demand for high definition and the rapid development of imaging technology, UHD standards for ultra-high definition include 4K UHD and 8K UHD to meet the trend in today's television and video surveillance market where 4K UHD equals 3840 x 2160 (8.29 megapixels), and UHD equals 7680 x 4320 (33.18 megapixels).

If the criteria for hardware and software has been met, then the use of approved H.265 IP Cameras should function without any *known* limitations now.

	VI MonitorPlus	Web Client	Video WallPlus	VI Monitor for Mac	VI TV	VI Mobile IOS	VI Mobile Android
Live	Yes	No (*1)	Yes	No	No	No	No
Playback	Yes	No	-	No	No	No	No
Video Clip	Yes	No	-	No	-	No	No
Snapshot	Yes	No	-	No	-	-	-
ROI	Yes (*2)	-	-	-	-	-	-

(*1) Live video can be shown in Low mode. (*2) ROI motion search for H.265 is supported by v7.1.1 or later.

✓ **Limitation**: The features that use H.265 decoder in server side, server-side motion detection or LPR etc., are not available for H.265 camera if a server does not support H.265 decoding.

(1A) H.265 DECODER

This section confirms that H.265 registration has been completed.

If the Administrator has not been prompted to register any H.265 cameras placed on the IP Server, selecting H.265 Registration will open a new window.

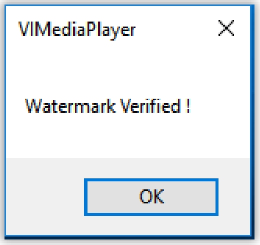
H.265 Decoder

H265 Decoder is Enabled

H.265 Registration

5.5.B Watermark Verification

To verify a **Watermark** for any clip created by the Web Client, follow these steps:



VIMediaPlayer

Watermark Verified !

1. Navigate to the web-client using either IE (high or low speed mode) or Chrome
2. Select any Camera with a recording desired for downloading
3. Click the "**Create Clip**" icon in the lower right-hand side of the window and choose the desired clip length; make sure to check the "Include Watermark" box.
4. Click **Download** to the right of the time display and wait for the download to complete.
5. **Save** the file to a location that is easy to recall.
6. Open **VI Media player** and select the downloaded clip, after pausing the video.
7. Next, select **File** > **Check Watermark.** A verification message will appear (see left)

5.6 HIGH SPEED MODE

High Speed Mode Web Client utilizes the Active X control for Video Insight and requires Internet Explorer to run.

The benefits to using High Speed Mode are that it gives you the exact frame rate, resolution and compression the camera is streaming to the Server. After the Active X control is loaded, the Web Client functions in the exact same manner.

In High Speed mode, you can also DPTZ in both live and recorded video when using the Digital Zoom function of the Web Client.

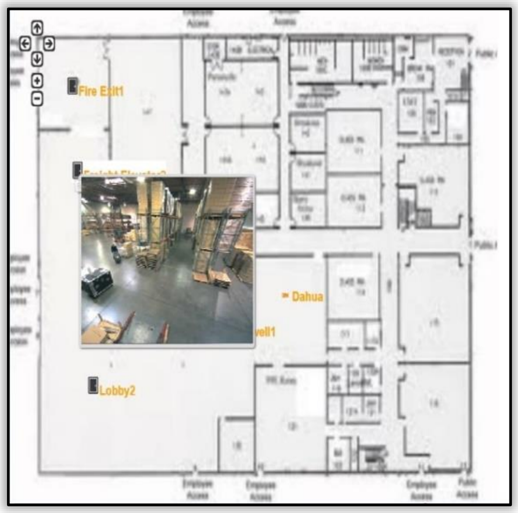
To start using the High-Speed mode, click the **Speed** button on the top right area of your screen. You will be prompted to **download an ActiveX tool** to install. This action usually requires Administrator privileges within your operating system.

5.7 ACCESS CONTROL

Limited Access Control functionality is available via the Web Client, and it is easily accessed by selecting the Custom Layout created for the IP Server.

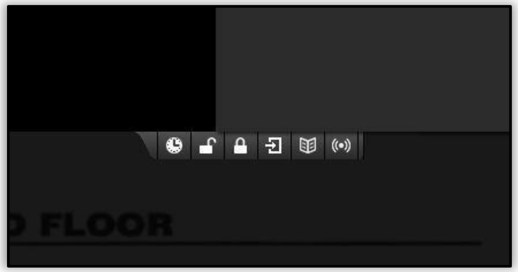
There are 2 primary ways to access the Access Control features in Web Client:

View Camera Layout	Select the View from the **Layout Directory** icon on the left panel.
Facility Map - Door View	Select a Facility Map on the left navigation panel by selecting the **Maps icon**.



Select the desired map to view. If configured in VI MonitorPlus, a visual map of the facility with the doors connected in the correct locations.

Hover over the door to see a live preview of a door with an associated camera.



To access the door controls, double-click the door icon the map. Once selected, a new display menu will appear. In the menu, there are six access control specific functions made available to the user.

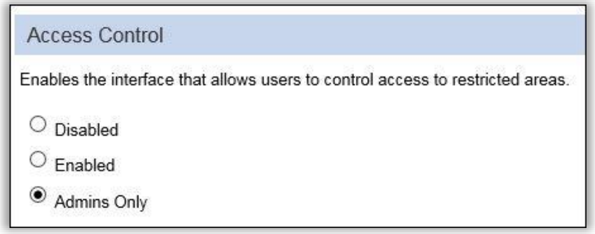
The controls (above) are listed from left to right are:

- Schedule: Forces device to return to any previously configured schedule.
- Unlock: Unlocks device.
- Lock: Lock device.
- Admit Entry: Temporarily unlocks device. Period of temporary unlock is often customizable in the access control application.
- View (Access) History: Views detail list of authorized access names.
- View (Alarm) History: Displays detailed list of door lock violations.

When any of the action-oriented controls (Lock, Unlock, Admit, Schedule) are selected, a confirmation box will appear to prevent an unintentional command from being executed on the device at the wrong time.

Click **OK** on the dialog to continue the action.

Web Client can alter access control settings for minor changes. To do so, select the Interface icon from the menu bar on the left side of the administrator's control screen.



Access Control

Enables the interface that allows users to control access to restricted areas.

○ Disabled
○ Enabled
● Admins Only

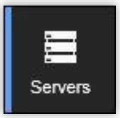
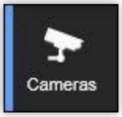
Next, three options appear as choices:

- Disable Access Control features.
- Enable Access Control features.
- Grant access for Administrator level accounts only.

Once the desired choice is selected, be sure to click **Save** at the top of the screen.

5.8 ADMIN FEATURES

Web Client can perform some basic administrative tasks that affect the performance and appearance of IP Server, all within the convenience of a web page. These abilities are a way to quickly administer some of the more basic features of IP Server, without having to use the feature rich VI MonitorPlus.

	The Servers button allows the administrator to modify base configuration settings for the IP server, including adding and removing cameras, enabling Health Monitor reporting, changing port settings for VI MonitorPlus connections, and adding general support information for your own internal purposes.
	The new Cameras button, found in the left navigation bar, allows the admin to apply most of the administrative tasks to specific cameras that can also be done within VI MonitorPlus.
	The Views button allows the admin to create custom layouts of various cameras on the fly. Options are available to add a single camera view all the way up to a 36-camera view. Additionally, the ability to add a static image, create a custom tour of only specific cameras, or add a web page for display within the View area is possible.
	The Interface button allows the admin to create and define the default user experience when logging in to the Web Client.
	The Network button on the left navigation bar allows the user to create custom network profiles for use with servers that may have both a high-speed LAN connection and an open Internet connection and limited bandwidth.

To access the new Admin Features, select Admin located in the top right-hand side of the page.

Once the new page opens, you are presented with many options that will allow you to modify the server on various levels. Those options are described above, and within the following pages.

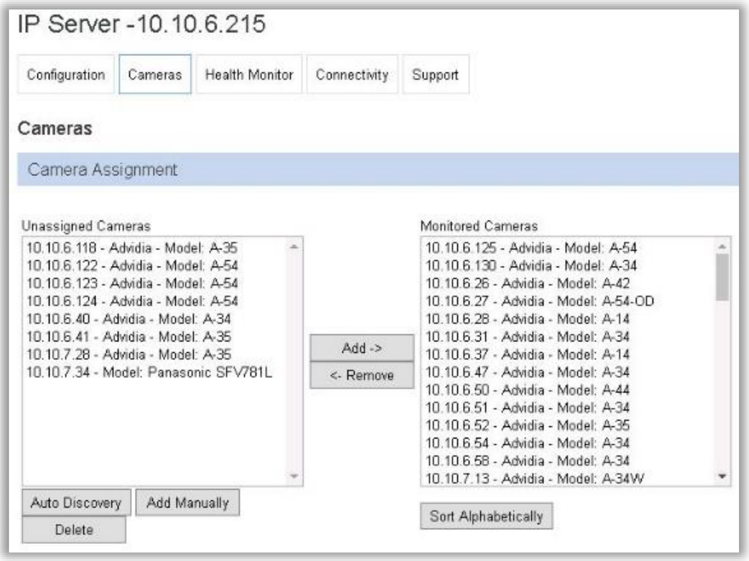
5.8.A Servers

The Servers Section is divided into five separate tabs that cover Configuration, Camera addition/removal, Health Monitor addition, Connectivity to the IP Server and general Support information.

(1) CONFIGURATION TAB

By selecting the **Servers** button found on the left navigation bar, the options made available include the ability to change the name of the server, change the SQL server location, alter the video location path, enable **Binary Recording**, and other advanced options. These functions are also available within VI MonitorPlus in the **Camera Configuration** settings.

(2) CAMERAS TAB



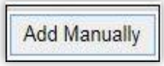
Unassigned Cameras

10.10.6.118 - Advidia - Model: A-35
10.10.6.122 - Advidia - Model: A-54
10.10.6.123 - Advidia - Model: A-54
10.10.6.124 - Advidia - Model: A-54
10.10.6.40 - Advidia - Model: A-34
10.10.6.41 - Advidia - Model: A-35
10.10.7.28 - Advidia - Model: A-35
10.10.7.34 - Model: Panasonic SFV781L

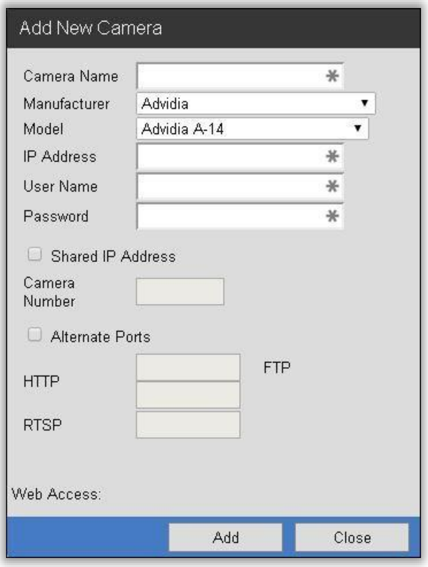
Monitored Cameras

10.10.6.125 - Advidia - Model: A-54
10.10.6.130 - Advidia - Model: A-34
10.10.6.26 - Advidia - Model: A-42
10.10.6.27 - Advidia - Model: A-54-OD
10.10.6.28 - Advidia - Model: A-14
10.10.6.31 - Advidia - Model: A-34
10.10.6.37 - Advidia - Model: A-14
10.10.6.47 - Advidia - Model: A-34
10.10.6.50 - Advidia - Model: A-44
10.10.6.51 - Advidia - Model: A-34
10.10.6.52 - Advidia - Model: A-35
10.10.6.54 - Advidia - Model: A-34
10.10.6.58 - Advidia - Model: A-34
10.10.7.13 - Advidia - Model: A-34W

The Cameras tab allows admins and/or users the ability to search, add, and remove cameras from the IP Server, very similar to the way that adding cameras is done in the initial IP Server configuration, or within VI MonitorPlus.



To add a camera to the IP Server, select the **Add Manually** button. Auto Discovery of a camera is also available and works as described by following this link.



Camera Name
Manufacturer: Advidia
Model: Advidia A-14
IP Address
User Name
Password
Camera Number
HTTP
RTSP
Web Access:

A prompt appears requesting information regarding the specific camera being added.

Once the information has been entered, select **Add**, and the camera information screen will appear in the left column.

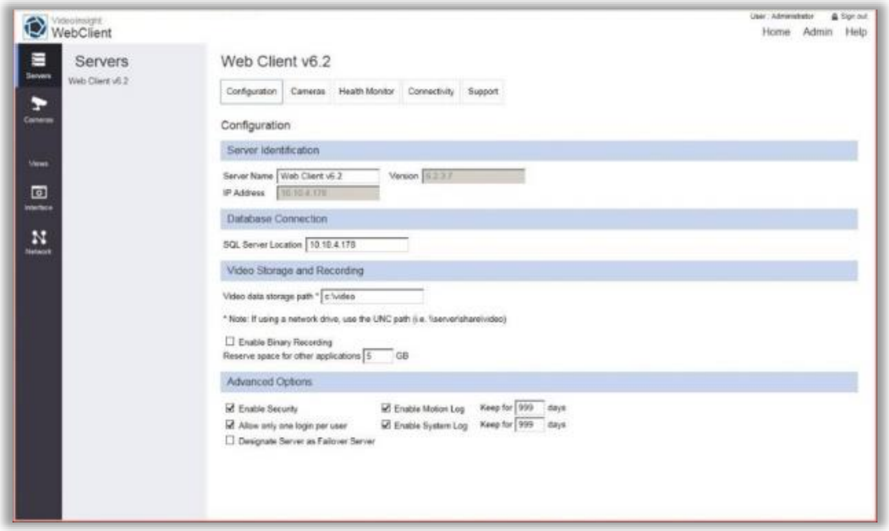
Next, select the camera, then click on the right arrow.

Finally, select **Save**.

IP server has now successfully added a camera with the web client

(3) HEALTH MONITOR TAB

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 sends 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.



Configuration

Server Identification

Server Name: Web Client v6.2 Version: 6.2.3.7
IP Address: 10.10.4.178

Database Connection

SQL Server Location: 10.10.4.178

Video Storage and Recording

Video data storage path *: c:\video

* Note: If using a network drive, use the UNC path (i.e. \\server\share\video)

☐ Enable Binary Recording
Reserve space for other applications: 5 GB

Advanced Options

☑ Enable Security ☑ Enable Motion Log Keep for 999 days
☑ Allow only one login per user ☑ Enable System Log Keep for 999 days
☐ Designate Server as Failover Server

Within the Administration page, a user can manipulate the Health Monitor server location by IP address, Server port (if modified from default), update frequency, and the details sent to the Health Monitor Server, including IP Server version number, a lost signal with configured cameras, camera information, available disk space on IP server, and recording status.

(4) CONNECTIVITY TAB

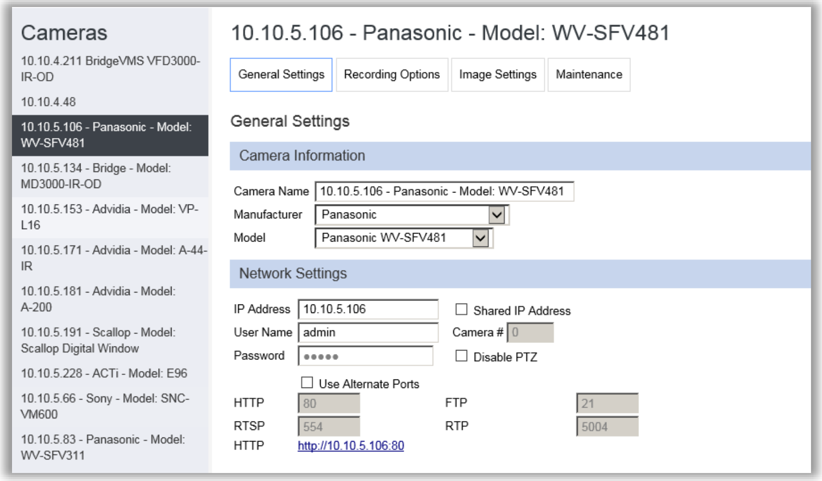
The Connectivity tab displays the ports that both IP Server and VI MonitorPlus use, as well as configure the outgoing SMTP mail server for use with mail services like Gmail, Hotmail, and Yahoo Mail.

(5) SUPPORT INFORMATION

The Support tab allows the user to update specific information about the IP Server. This information is to be updated by the Administrator and used as a guide to provide information that is useful on an as-needed basis.

5.8.B Cameras

This page, within VI MonitorPlus, is divided into four sections including the General Settings tab, Recording Options tab, Image Settings tab, and the Maintenance Tab. The general tab shows basic information such as the camera's name, manufacturer, model, IP address, and network configuration settings.



Cameras

- 10.10.4.211 BridgeVMS VFD3000-IR-OD
- 10.10.4.48
- 10.10.5.106 - Panasonic - Model: WV-SFV481
- 10.10.5.134 - Bridge - Model: MD3000-IR-OD
- 10.10.5.153 - Advidia - Model: VP-L16
- 10.10.5.171 - Advidia - Model: A-44-IR
- 10.10.5.181 - Advidia - Model: A-200
- 10.10.5.191 - Scallop - Model: Scallop Digital Window
- 10.10.5.228 - ACTi - Model: E96
- 10.10.5.66 - Sony - Model: SNC-VM600
- 10.10.5.83 - Panasonic - Model: WV-SFV311

10.10.5.106 - Panasonic - Model: WV-SFV481

General Settings

Camera Information

Camera Name: 10.10.5.106 - Panasonic - Model: WV-SFV481
Manufacturer: Panasonic
Model: Panasonic WV-SFV481

Network Settings

IP Address: 10.10.5.106 | □ Shared IP Address
User Name: admin | Camera #: 0
Password: ●●●●● | □ Disable PTZ

□ Use Alternate Ports

HTTP: 80 | FTP: 21
RTSP: 554 | RTP: 5004
HTTP: http://10.10.5.106:80

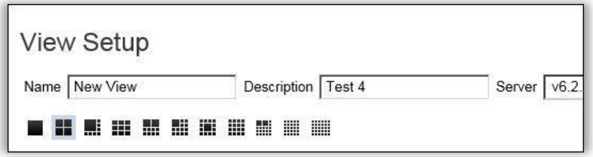
The **Recording Options** tab allows you to modify the Resolution, Frames Per Second, turn On or Off Audio (if camera supports it), Recording Type, Capture Format, Image Location on the server, and set Maximum File size.

The **Image Settings** Tab Allows you to change Image Rotation, Color adjustments (limited to specific cameras), Various Advanced Settings (limited to specific cameras), and modify 360 view camera settings.

The **Maintenance** tab shows the camera's firmware information, service history, and the contact information.

5.8.C Views (formerly known as Layouts)

To create a View, type the name that you would like to use and, optionally, a description of the View. Next, select the number of cameras for the View.

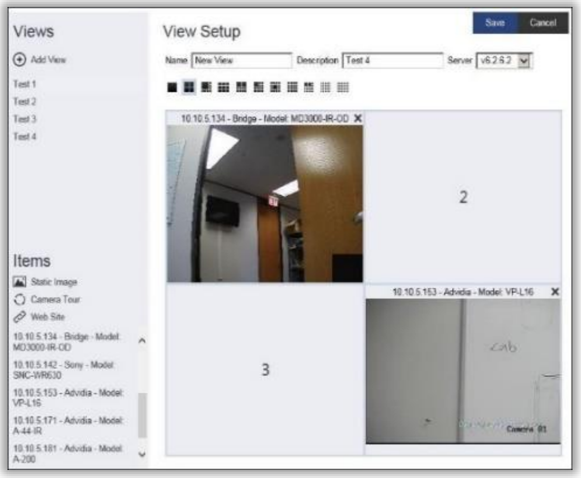


View Setup

Name New View Description Test 4 Server v6.2.

After the initial naming and basic layout is completed, cameras on the left can be dragged and dropped into the desired point on the Layout View on the right.

The number of options for viewing vary, based on the construction of the previously designed custom **View** layout.



Views

Add View

Test 1
Test 2
Test 3
Test 4

View Setup

Name New View Description Test 4 Server v6.2.6.2

10.10.5.134 - Bridge - Model: MD3000-IR-OD

10.10.5.153 - Advidia - Model: VP-L16

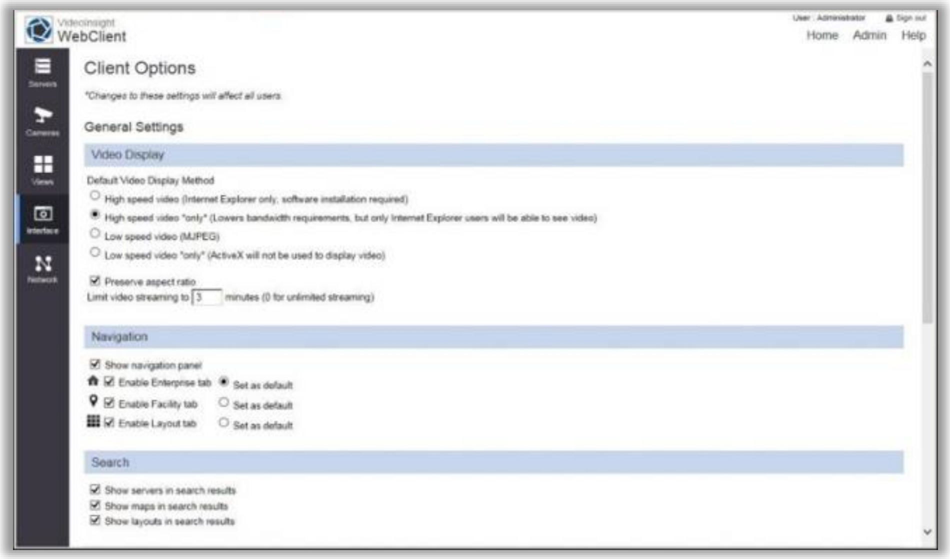
Items

Static Image
Camera Tour
Web Site
10.10.5.134 - Bridge - Model: MD3000-IR-OD
10.10.5.142 - Sony - Model: SNC-WR630
10.10.5.153 - Advidia - Model: VP-L16
10.10.5.171 - Advidia - Model: A-44-IR
10.10.5.181 - Advidia - Model: A-200

Once the settings are customized for the new View, select **Save** at the top right-hand side of the screen. You can now go back to the main page and choose the View that you have just created.

(1) INTERFACE

By accessing the Interface button, it is possible to alter and customize the appearance of the Web Client.



Client Options

*Changes to these settings will affect all users

General Settings

Video Display

Default Video Display Method

○ High speed video (Internet Explorer only, software installation required)
● High speed video "only" (Lowers bandwidth requirements, but only Internet Explorer users will be able to see video)
○ Low speed video (MJPEG)
○ Low speed video "only" (ActiveX will not be used to display video)

☑ Preserve aspect ratio
Limit video streaming to 3 minutes (0 for unlimited streaming)

Navigation

☑ Show navigation panel
☑ Enable Enterprise tab ● Set as default
☑ Enable Facility tab ○ Set as default
☑ Enable Layout tab ○ Set as default

Search

☑ Show servers in search results
☑ Show maps in search results
☑ Show layouts in search results

Some of the items that can be changed are the login screen starting in high-speed or low-speed viewing mode, limiting the number of video streams able to view at one time (saving bandwidth), navigation pages, custom login messages, and event notifications for use with access control devices.

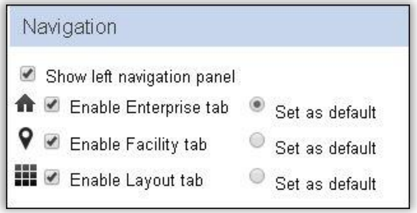
Access Control functionality can also be enabled or disabled by Administrator users in the Interface section.

5.8.D General Settings

(1) VIDEO DISPLAY

Video Display supports changing camera video capture methods. It will require an IP Server restart once any option has been changed.

(2) NAVIGATION



Navigation

☑ Show left navigation panel

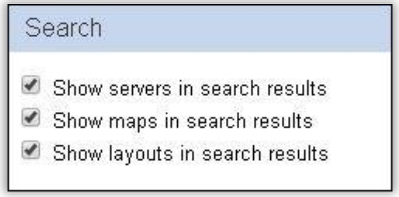
☑ Enable Enterprise tab ● Set as default

☑ Enable Facility tab ○ Set as default

☑ Enable Layout tab ○ Set as default

This feature allows the Administrator to hide a specific feature that is not desired for users to see.

(3) SEARCH



Search

☑ Show servers in search results

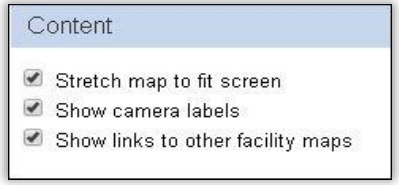
☑ Show maps in search results

☑ Show layouts in search results

Using this feature allows the Administrator to hide other features that would otherwise appear on the default website after logging in.

Often this is done to restrict access to viewing only specific devices across multiple servers.

(4) CONTENT



Content

☑ Stretch map to fit screen

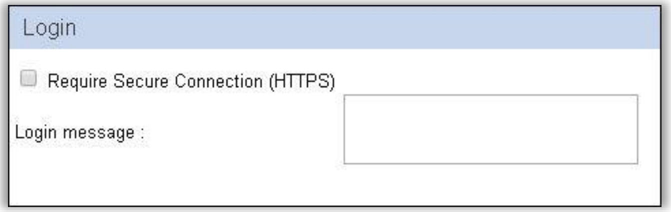
☑ Show camera labels

☑ Show links to other facility maps

Content modification, by default, allows the maps to be stretched across a screen view, show camera labels (names), and copy links to facility maps.

Unchecking these tic-boxes prevents these capabilities from being used or manipulated by non-administrative users.

(5) LOGIN



Login

□ Require Secure Connection (HTTPS)

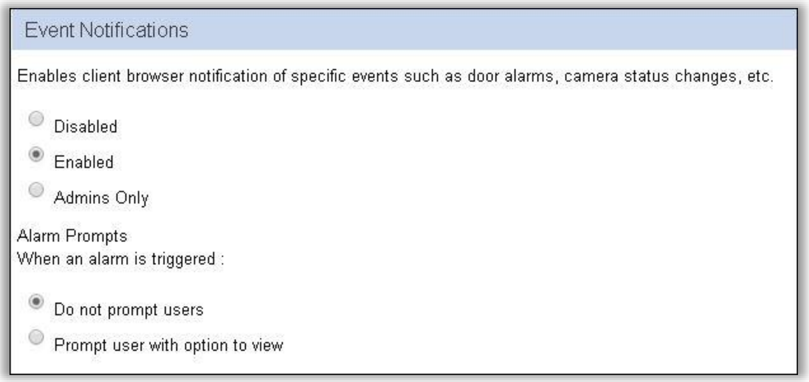
Login message :

The ability to force the HTTPS protocol for login is available.

This is a security enhancement feature and will work only with fully-qualified domain names with registered SSL certificates.

For more information on setting up HTTPS protocol for enhanced security, please contact Microsoft for support. Alternatively, using a self-signed certificate is possible.

(6) EVENT NOTIFICATIONS



Event Notifications

Enables client browser notification of specific events such as door alarms, camera status changes, etc.

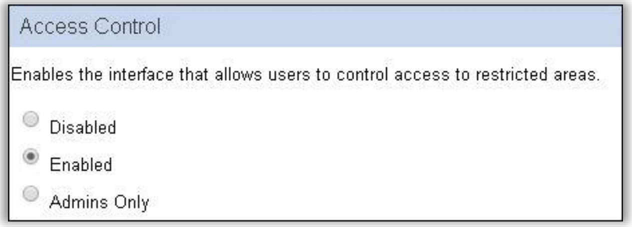
○ Disabled
● Enabled
○ Admins Only

Alarm Prompts
When an alarm is triggered :

● Do not prompt users
○ Prompt user with option to view

Event notifications work with Access Control, as well as motion detection from cameras. This can be limited to administrative use only or blocked altogether.

(7) ACCESS CONTROL



Access Control

Enables the interface that allows users to control access to restricted areas.

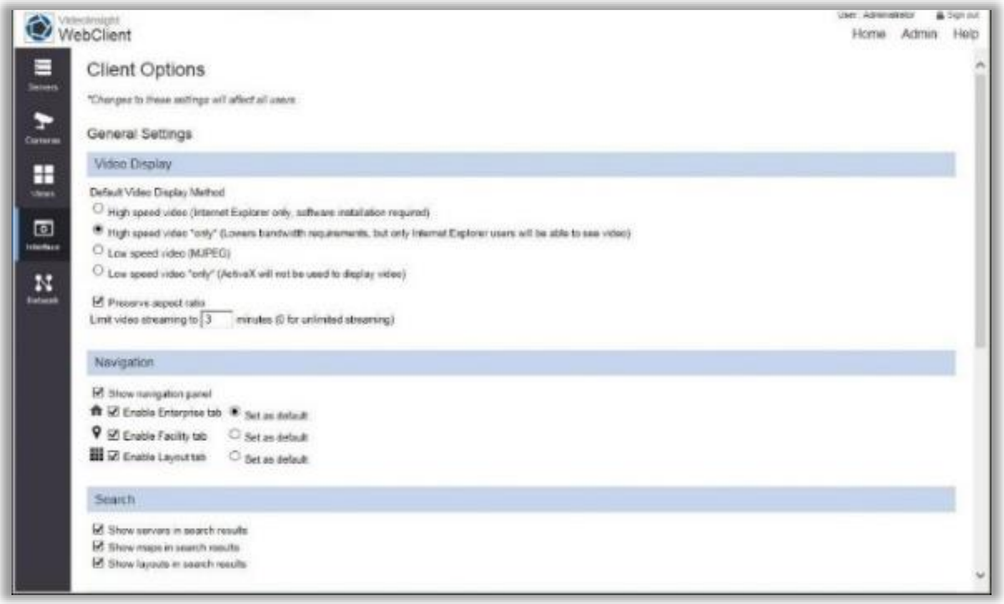
○ Disabled
● Enabled
○ Admins Only

This allows a quick shortcut to access control features for IP Servers that are integrated with Access Control services.

By default, this is enabled. If no Access Control services are being used by the IP Server, then this feature has no effect on the functionality of the Web Client.

(8) NETWORK

By creating a separate profile for use across the Internet on a low-speed connection, the settings can be optimized to limit the number of frames that IP server sends through the Web Client view to minimize the impact on the outgoing Internet connection.



Client Options

*Changes to these settings will affect all users

General Settings

Video Display

Default Video Display Method
○ High speed video (Internet Explorer only, software installation required)
● High speed video "only" (Lowers bandwidth requirements, but only Internet Explorer users will be able to see video)
○ Low speed video (MJPEG)
○ Low speed video "only" (ActiveX will not be used to display video)

☑ Preserve aspect ratio
Limit video streaming to 3 minutes (0 for unlimited streaming)

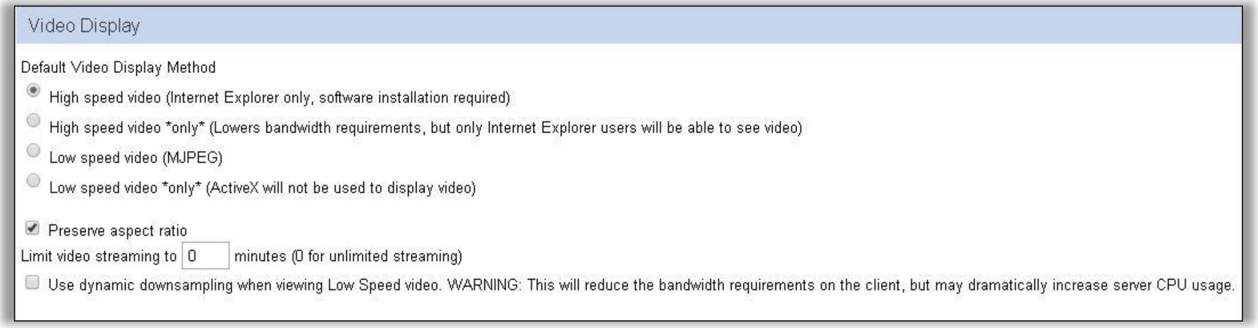
Navigation

☑ Show navigation panel
☑ Enable Enterprise tab ● Set as default
☑ Enable Facility tab ○ Set as default
☑ Enable Layout tab ○ Set as default

Search

☑ Show servers in search results
☑ Show maps in search results
☑ Show layouts in search results

Best used for IP Server Admins that have the need to allow multiple people to connect to the IP Server, but only have a limited bandwidth issue.



Video Display

Default Video Display Method

● High speed video (Internet Explorer only, software installation required)

○ High speed video *only* (Lowers bandwidth requirements, but only Internet Explorer users will be able to see video)

○ Low speed video (MJPEG)

○ Low speed video *only* (ActiveX will not be used to display video)

☑ Preserve aspect ratio

Limit video streaming to 0 minutes (0 for unlimited streaming)

□ Use dynamic downsampling when viewing Low Speed video. WARNING: This will reduce the bandwidth requirements on the client, but may dramatically increase server CPU usage.

This specifically reduces the overall refresh rate for each user so that other necessary services do not come into conflict with not having an internet connection on a bandwidth-laden network.

6. VIDEO INSIGHT SUPPORT RESOURCES

For demonstrations of how to complete various tasks and configurations using IP Server Enterprise Software, Video Insight has made available some YouTube Tutorials: http://www.youtube.com/user/videoinsighttv

To download manuals and software available for use, please visit our Downloads: http://www.downloadvi.com

6.1 REMOTE SUPPORT

If more personal assistance is needed, one of our Technical Support representatives is available to aid with any troubleshooting. *For remote support, Video Insight requests that the user install the TeamViewer client application prior to requesting support.*

To install TeamViewer:

- Browse to http://www.downloadvi.com
- Click the Remote Support link at the bottom of the page.
- Click Run at the prompt.
- Click Run again.
- Call Technical Support at 713-621-9779.
- Give the representative the ID number that appears within the VI Remote Support TeamViewer application window.
- Your ID is randomly generated every time you request remote support.

The representative will log onto your computer and work with you to resolve the issue

6.2 CONTACT US

Main Address	800 Gessner, Suite 700 Houston, Texas 77024
Hours of Operation	Monday to Friday: 9:00am - 6:00pm CST
Phone	713-621-9779
Fax	713-621-7281

Technical Support	
Hours of Operation	Monday to Friday: 7:00am - 7:00pm CST Saturdays and Holidays: 10:00am - 2:00pm CST
Email	support.h@us.panasonic.com
Emergency Support Service #	877-743-2403 (*our Support Engineer on call will be paged to assist you.*)

NOTE - This information is made available for clients only in North America and the United States.
For Support outside of the United States, please contact your sales agent or vendor.

7. APPENDICES

7.1 APPENDIX A: IP SERVER PORT LIST

Service names officially recognized by the Internet Assigned Numbers Authority (IANA) may not appear within the listed items below. Instead, the listed name might reflect the name used throughout this document and within the software.

For more information about the official port names assigned by the IANA, please visit the website located at: https://www.iana.org/

Port Number	Name	Purpose for use of port	Outbound WAN traffic required?
4010	Data Port	Sends live video streams from IP Server to VI MonitorPlus Client	No
4011	Command Port	To get and set system information by VI MonitorPlus Client	No
3010	Ovid Server	Communication between S2, IP Server and the Ovid Server for Video Insight and S2 Access Control Configuration	No
80	HTTP	IIS for serving the Web Client **NOTE -** Some ISPs block port 80 access. Some may need to configure IIS to use a different port than default for internet access	No
2051	MonitorCast	Access control communication between Video Insight and MonitorCast	No
554	RTSP	Specific camera properties	No
21	FTP	Specific camera properties	No
11000	Health Monitor	Communication between IP Server and Health Monitor	No
636	Active Directory SSL	Active Directory configured with Secure Socket Layer (SSL)	No
389	Active Directory non-SSL	Active Directory configured without Secure Socket Layer (SSL	No
8080	HMCloud	TCP port used to receive data on Health Monitor Cloud, located at: http://www.healthmonitorcloud.com.	Yes
4030	POS	Port used for Point of Sale customized software integration	No

7.2 APPENDIX B: .AVI FILES WRITE/MODIFY PERMISSIONS SETTINGS

VI Enterprise uses the Windows File System in order to generate ***.avi*** files directly onto the storage location, and it must follow Windows File Permissions rules to function properly.

When VI Enterprise is installed by default, the service which is created (**IP Video Enterprise**) runs under the **Local System Account** within Windows. Depending on the **Group Policy** or **Security Settings** for an operating system installed on a computer, these permissions are not enough in order to have complete control on files in video storage folders.

> **NOTE -** If you do not have **Write** permission, you cannot create a file and put data into it. Likewise, if you do not have **Modify** permission, you cannot delete the file from the storage location.

One solution from preventing normal video file operations is **to assign a Service Account** to the IP Video Enterprise service.

You need to first create a New Local Account or assign an existing Domain Account to the IP Enterprise service. This is located under **Control Panel**>**Administrative Tools**>**Computer Management.**

Scenario 1: Create a New Local Admin Account

- Within **Computer Management**, go to **System Tools**>**Local Users and Groups**.
- Create a new User and provide a valid password. Check the **Password Never Expires** box.
- Highlight the new user, right click and select **Properties**. Navigate to the **Member Of** tab.
- Click **Add**. Add the **Administrators** group to this user.
- Navigate to the **Services Management Console** located in **Control Panel**>**Administrative Tools**>**Services.**
- Navigate to **IP Video Enterprise** service.
- Right click **on IP Video Enterprise** and select **Properties**. Navigate to the **Log On** tab.
- Select **This Account** and provide your **username** and **password**.
- Go to your **Data Storage Path** for VI, highlight it and right click selecting **Properties**.
- Navigate to the **Security** tab. Verify that **Administrators** is located in the **Group** or **User Names** and that it has **Full Control**.
- **Restart the VI Enterprise** service.

Scenario 2: Add an Existing Domain Account

- Within **Computer Management**, go to **System Tools**>**Local Users and Groups**.
- Double click on **Groups**, then **Administrators**.
- Click **Add**. Navigate to the **Domain Account** that you wish to be an **Administrator** for this computer.
- Navigate to the **Services Management Console** located in **Control Panel**>**Administrative Tools**>**Services.**
- Navigate to the **IP Video Enterprise** service.
- Right click **on IP Video Enterprise** and select **Properties**. Navigate to the **Log On** tab.
- Select **This Account** and provide your **username** and **password**.
- Go to your **Data Storage Path** for VI, highlight it and right click selecting **Properties**.
- Navigate to the **Security** tab. Verify that **Administrators** is located in the **Group** or **User Names** and that it has **Full Control**.
- **Restart the VI Enterprise** service.

7.3 APPENDIX C: 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 are 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 are 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 Graber- 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 low-light correction as the 2x setting which specifies the 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.

7.4 APPENDIX D: SECURE SYSTEM GUIDELINE

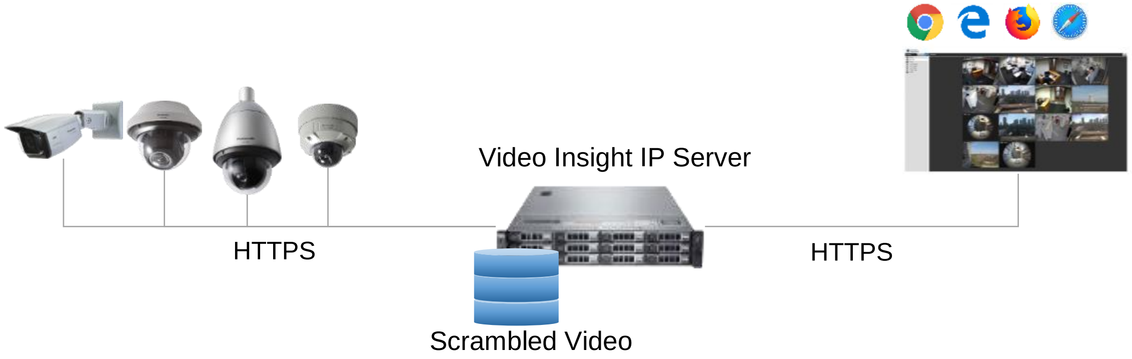
Introduction

Video Insight VMS is an application designed to be easy to use, scalable and flexible. To ensure encrypted communications within critical environments, the **Secure System** has been created as an additional security layer for the application. This document describes how to enable and configure **Secure System** for **Video Insight VMS**.

System Overview

The communication between the cameras **and Video Insight IP Server** can be encrypted over *HTTPS* protocol, and **VI Web Client** can be used over HTTPS to ensure data encryption on the client side. Also, recorded video files will not be readable by other systems after being created with the security layer enabled.

The basic System Structure is shown below:



Use Cases

To enable **Secure System**, a system Integrator must consider all possible scenarios and design specific solutions for each one of them. The following table presents typical use cases and their corresponding solutions:

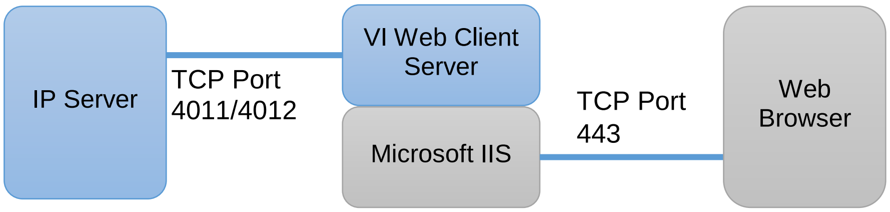
Use Case	Solution	Reference
Video Insight VMS will be accessed via public internet without VPN.	Only **HTTPS** communication can be enabled when using Web Client/Microsoft IIS to encrypt all the data.	Setup HTTPS on Microsoft IIS.
Cameras that are managed by IP Server will be installed on public internet with anonymous access.	**Video Insight** supports **HTTPS** communications for Panasonic cameras, and Panasonic **i-PRO Extreme** series cameras come with pre-installed Symantec server certificate. The option can be easily configured, and IP Server can verify Symantec's certificate before data communication is established.	Setup HTTPS Camera Communication.
A Recorded Video can be leaked even when is stored on the local Server.	Use the **Proprietary Format Video** feature for Server File Storage to scramble the video file output, disabling its access by third-party software.	Setup Proprietary Format Video.

Setting Up HTTPS on Microsoft IIS

This section covers the steps to follow in order to enable HTTPS protocol on IIS Server.

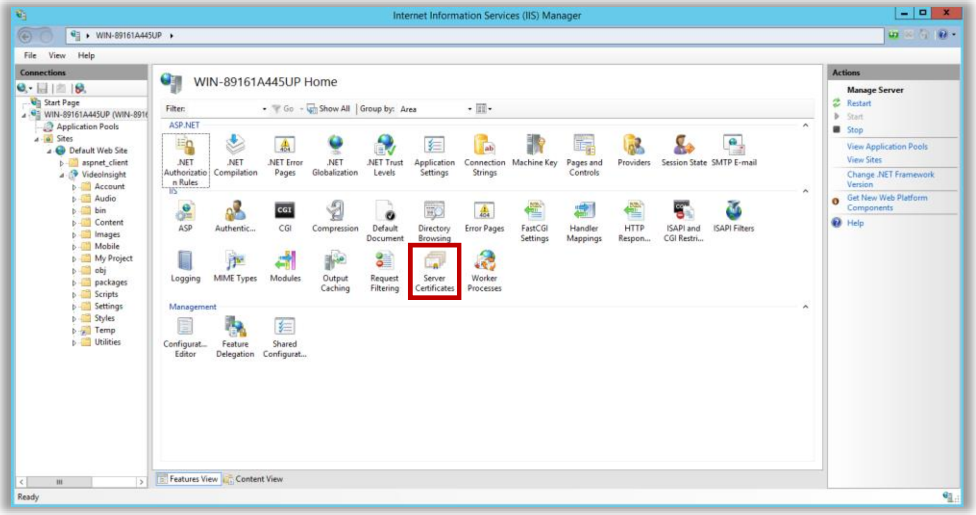
Software Components

VI Web Client is installed over Microsoft IIS. The following is the basic software structure and expected communication interface when HTTPS communication between IP Server and VI Web Client is used by Video Insight VMS.

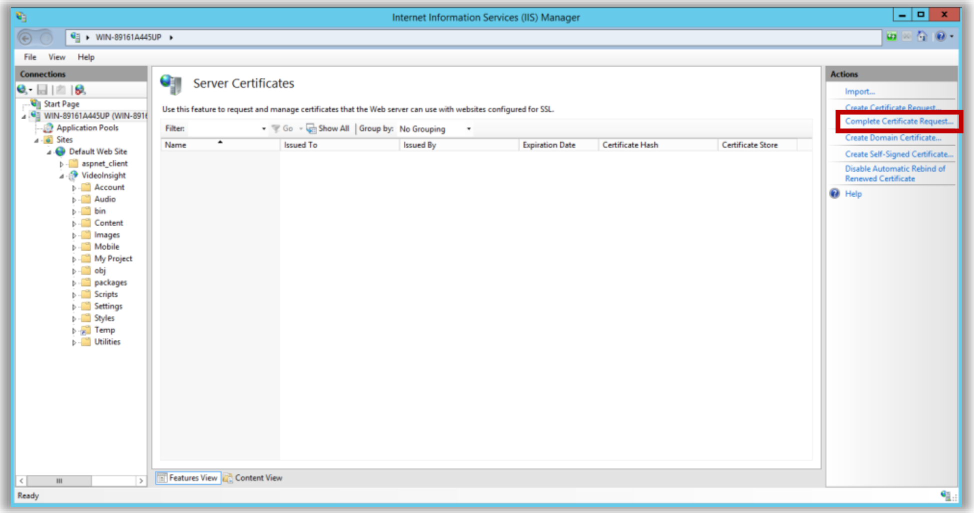


Enabling HTTPS

Create a CSR (Certificate Signing Request)

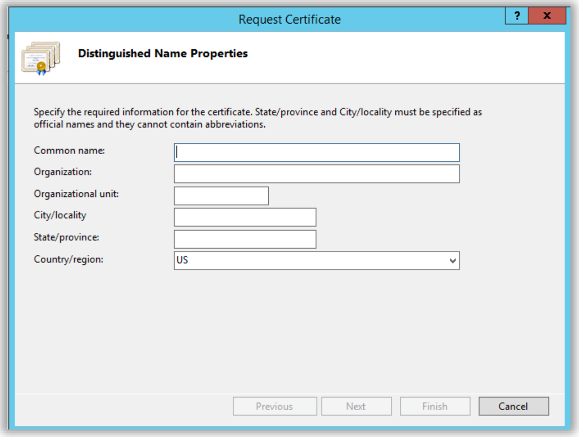


1. Open IIS Manager and select “Server Certificates”.



Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

2. Click on "**Create Certificate Request**".



Distinguished Name Properties

Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name:

Organization:

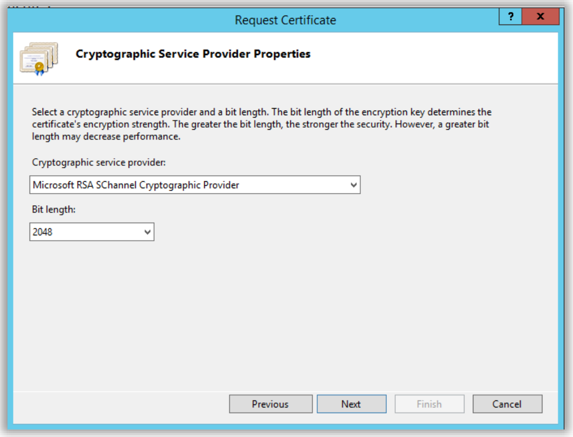
Organizational unit:

City/locality:

State/province:

Country/region: US

3. Fill out the **Request Certificate** form and click "**Next**".



Cryptographic Service Provider Properties

Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

Cryptographic service provider: Microsoft RSA SChannel Cryptographic Provider

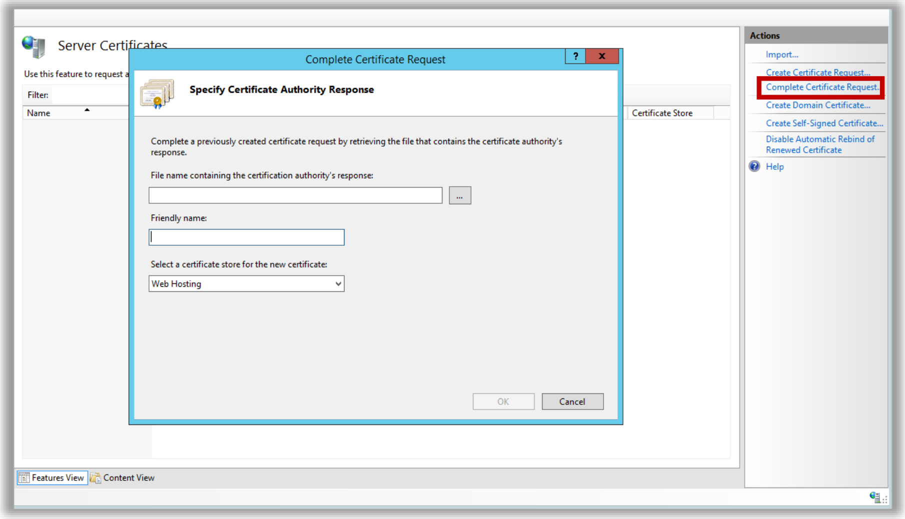
Bit length: 2048

4. Select each parameter for your server's Certificate, then click "**Next**".

Obtain a Signed Server Certificate

After submitting the CSR, you will need to request a CA certificate like DigiCert (Symantec) to issue a Signed Server Certificate based on the newly created CSR.

Complete the Request


Server Certificates
Use this feature to request a
Filter:
Name
Certificate Store
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Disable Automatic Rebind of Renewed Certificate
Help
Features View
Content View
?
✕
OK
Cancel
...

Complete Certificate Request

Specify Certificate Authority Response

Complete a previously created certificate request by retrieving the file that contains the certificate authority's response.

File name containing the certification authority's response:

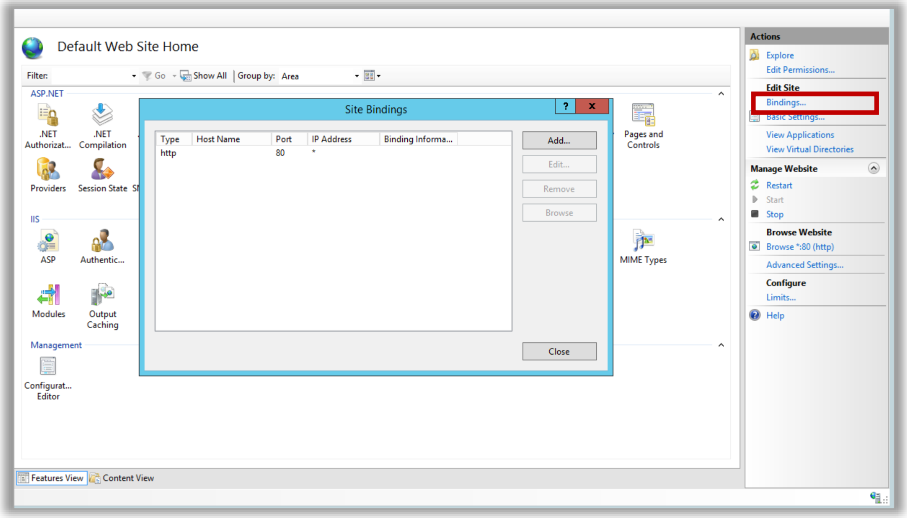
Friendly name:

Select a certificate store for the new certificate: Web Hosting

2.6

Click "**Complete Certificate Request**", then select a Certificate issued by the CA and specify the Friendly Name.

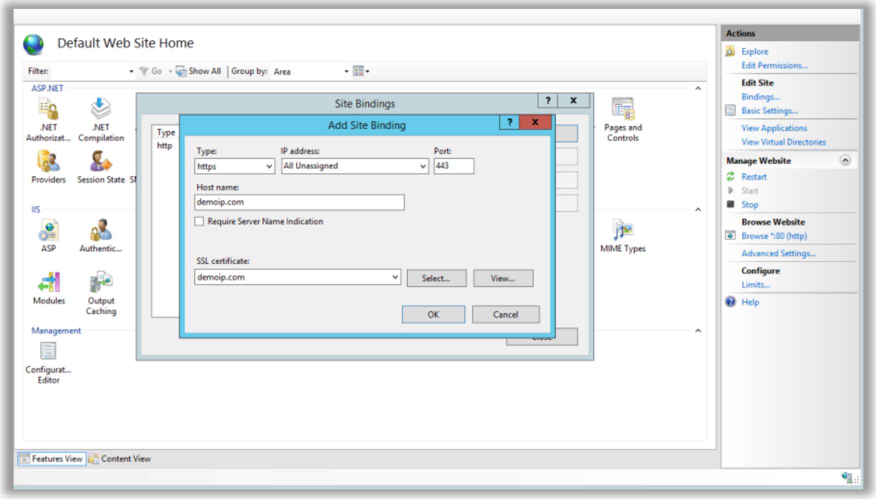
Bind HTTPS Port



Site Bindings

Type	Host Name	Port	IP Address	Binding Informa...
http		80	*	

1. Open the **Default Web Site Home** option and click on "**Bindings**"; in the **Site Bindings** window, click "**Add**".



Add Site Binding

Type: https

IP address: All Unassigned

Port: 443

Host name: demoip.com

□ Require Server Name Indication

SSL certificate: demoip.com

2. In the **Add Site Binding** window:
   - Select “**https**” from the “**Type**” list box;
   - Enter the value for the “**Host name**” field;
   - Select the issued certificate from the ”**SSL certificate**” list box.
   - Click “**OK**” to add the site Binding.

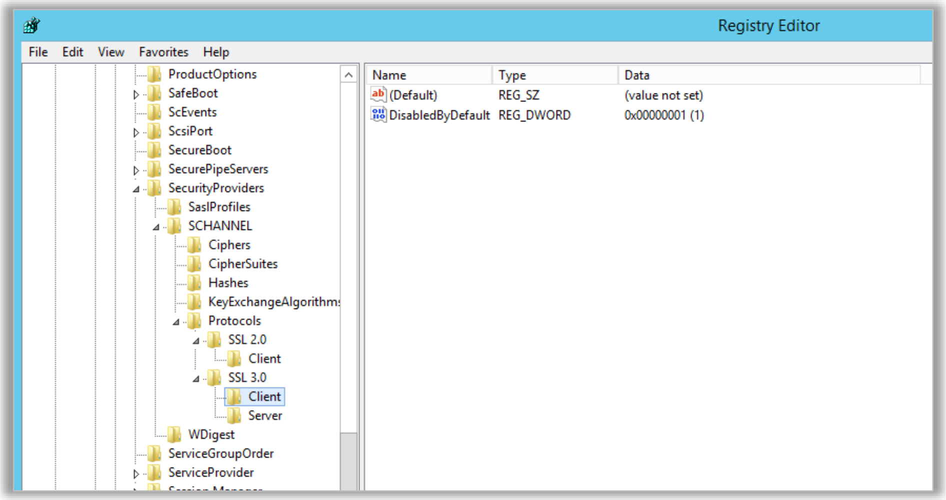
Disable Weak SSL Ciphers

(1) Disable SSL v3.0

- Create “**SSL 3.0**” Key under the following Registry Key:
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0

- Create “**Client**” Key and Value for the following Registry Key:
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Client "DisabledByDefault"=dword:00000001

- Create “**Server**” Key and Value for the following Registry Key:
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server "Enabled"=dword:00000000



Name	Type	Data
(Default)	REG_SZ	(value not set)
DisabledByDefault	REG_DWORD	0x00000001 (1)

Registry Editor – Disable SSL v3.0

(2) Disable RC4 Ciphers

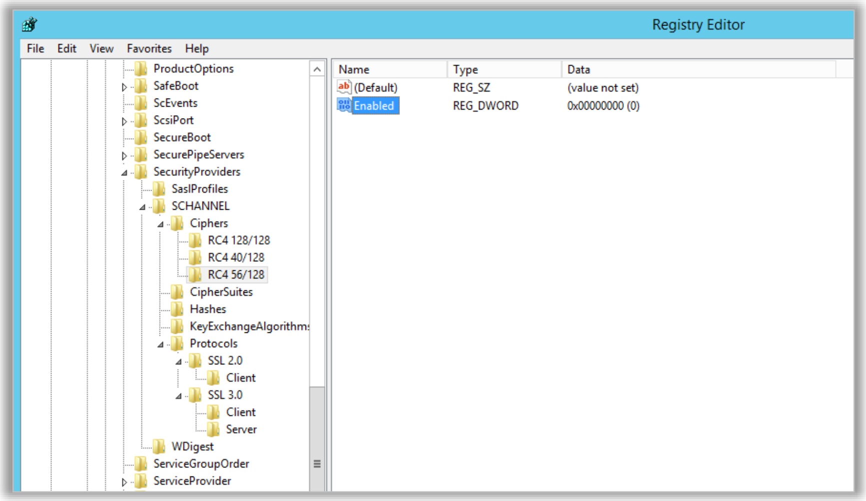
- Create the “**Ciphers**” Key and “**RC4 128/128**”, “**RC4 40/128**” and “**RC4 56/128**” under “**Ciphers**”. Then add the following values:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 128/128
  "Enabled"=dword:00000000

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 40/128
  "Enabled"=dword:00000000

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56/128
  "Enabled"=dword:00000000



Name	Type	Data
(Default)	REG_SZ	(value not set)
Enabled	REG_DWORD	0x00000000 (0)

Registry Editor – Disable RC4 Ciphers

Setting Up HTTPS Camera Communications

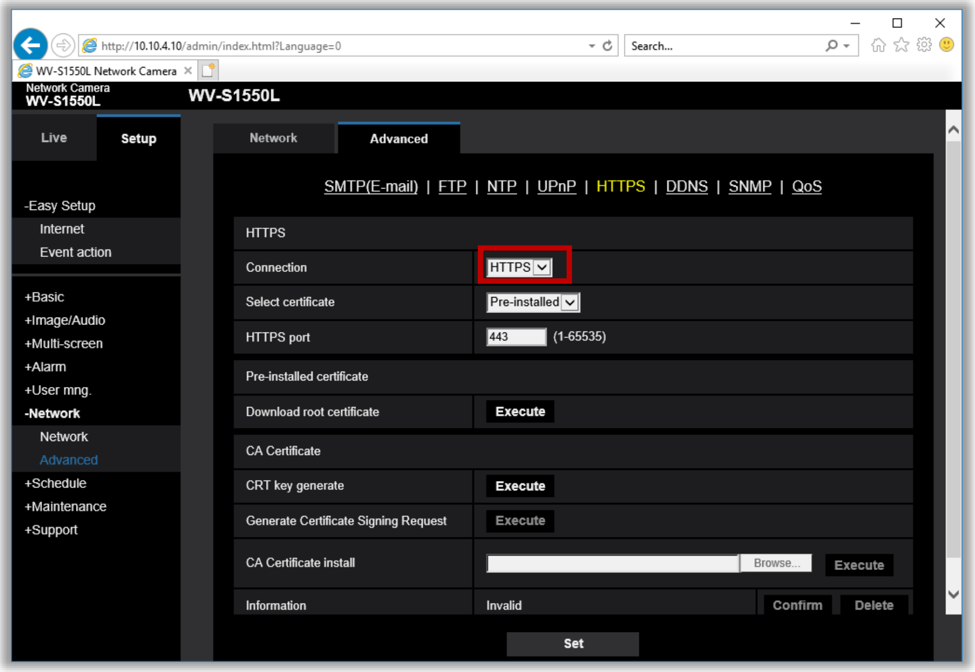
To enable HTTPS for Camera communications, the camera must support HTTPS; if Symantec's certificate is required, the camera must also support it.

> **NOTE -** See https://security.panasonic.com/products/functions/secure_communication/ for further information and supported models.

Camera Setup

Open the camera's **Administrative Console** (*see instructions for each made and model*).

In **Setup** -> **Network** -> **Advanced** -> **HTTPS**, select "**HTTPS**" from the **Connections** list box.



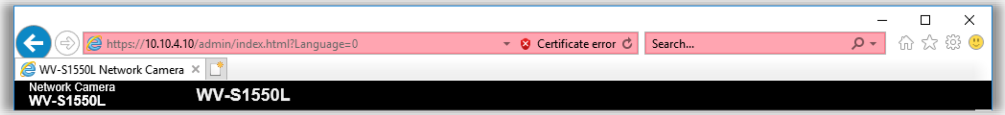
HTTPS

Connection: HTTPS

Select certificate: Pre-installed

HTTPS port: 443 (1-65535)

Information: Invalid

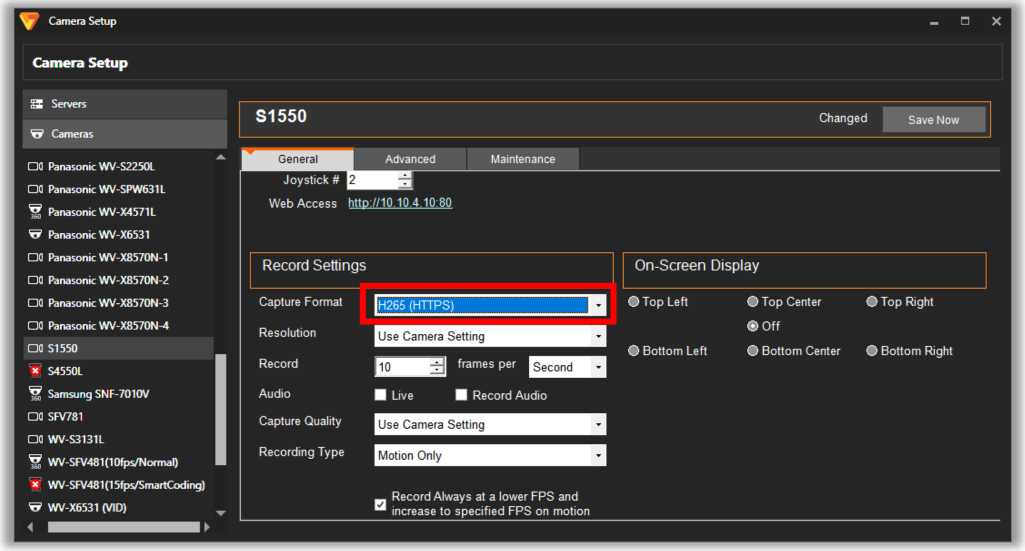
> **NOTE -** If the Symantec Certificate is pre-installed on the camera, a Certificate error message will appear on the browser (*see picture below*).
>
> 
>
>

https://10.10.4.10/admin/index.html?Language=0
> Certificate error
> Search...
> WV-S1550L Network Camera
> Network Camera
> WV-S1550L
> WV-S1550L
>
> This may happen because the pre-installed certificate is not associated to new environment; however, ***this error message can be ignored***.

IP Server Set Up

1. Open **VI MonitorPlus** (*Client app*).

2. In **Camera Setup** -> **General** -> **Recording Settings**, the **Capture Format** value must be set to “**H.265 (HTTPS)”** or “**H.264 (HTTPS)”**.



Joystick # 2

Web Access http://10.10.4.10:80

Record Settings

Capture Format: H265 (HTTPS)

Resolution: Use Camera Setting

Record: 10 frames per Second

Audio: ☐ Live ☐ Record Audio

Capture Quality: Use Camera Setting

Recording Type: Motion Only

☑ Record Always at a lower FPS and increase to specified FPS on motion

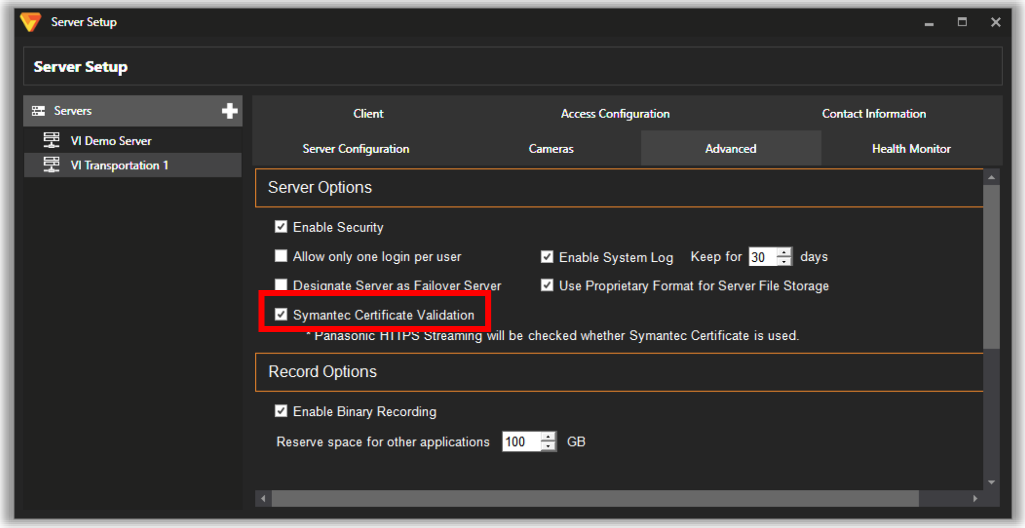
On-Screen Display

○ Top Left ○ Top Center ○ Top Right

● Off

○ Bottom Left ○ Bottom Center ○ Bottom Right

3. In **Server Setup** -> **Advanced** -> **Sever Options**, **“Symantec Certificate Validation”** shall be checked.



Server Options

☑ Enable Security

☐ Allow only one login per user ☑ Enable System Log Keep for 30 days

☐ Designate Server as Failover Server ☑ Use Proprietary Format for Server File Storage

☑ Symantec Certificate Validation

* Panasonic HTTPS Streaming will be checked whether Symantec Certificate is used.

Record Options

☑ Enable Binary Recording

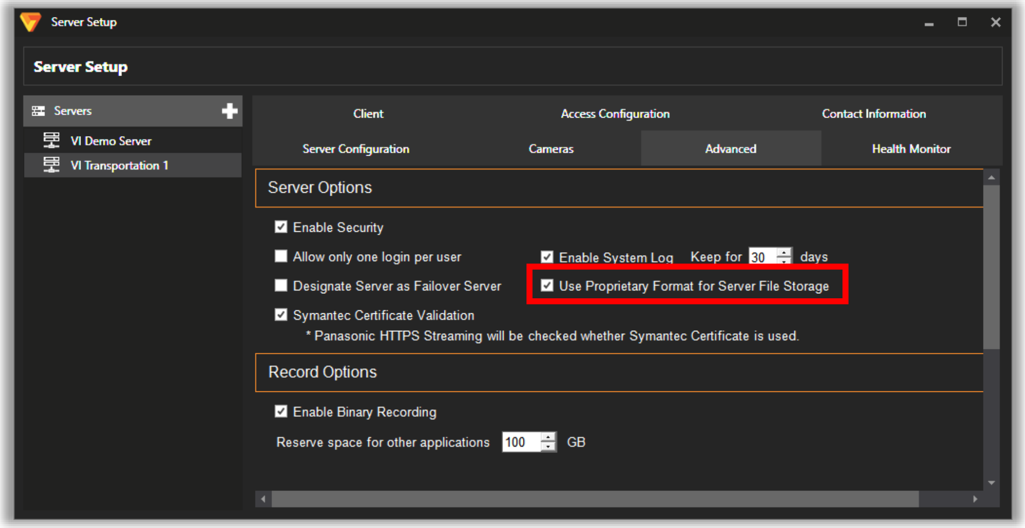
Reserve space for other applications 100 GB

4. Restart **IP Server**.

Setting Up Proprietary Format Video

The **Proprietary Format** feature allows recorded video files to be ***encrypted***, making them unreadable by any standard video player software like Windows Media Player or VLC Media Player. This encryption capability includes ***binary*** level.

In **Server Setup** -> **Advanced** -> **Server Options**, "**Use Proprietary Format for Server File Storage**" option shall be checked.



☑ Enable Security

□ Allow only one login per user

☑ Enable System Log Keep for 30 days

□ Designate Server as Failover Server

☑ Use Proprietary Format for Server File Storage

☑ Symantec Certificate Validation

* Panasonic HTTPS Streaming will be checked whether Symantec Certificate is used.

☑ Enable Binary Recording

Reserve space for other applications 100 GB

7.5 APPENDIX E: THE INDEPENDENT JPEG GROUP'S JPEG SOFTWARE NOTICE

====================================
README for release 6b of 27-Mar-1998
====================================

This distribution contains the sixth public release of the Independent JPEG Group's free JPEG software. You are welcome to redistribute this software and to use it for any purpose, subject to the conditions under LEGAL ISSUES, below.

Serious users of this software (particularly those incorporating it into larger programs) should contact IJG at jpeg-info@uunet.uu.net to be added to our electronic mailing list. Mailing list members are notified of updates and have a chance to participate in technical discussions, etc.

This software is the work of Tom Lane, Philip Gladstone, Jim Boucher, Lee Crocker, Julian Minguillon, Luis Ortiz, George Phillips, Davide Rossi, Guido Vollbeding, Ge' Weijers, and other members of the Independent JPEG Group.

IJG is not affiliated with the official ISO JPEG standards committee.

DOCUMENTATION ROADMAP
=====================

This file contains the following sections:
OVERVIEWGeneral description of JPEG and the IJG software.
LEGAL ISSUES   Copyright, lack of warranty, terms of distribution.
REFERENCES   Where to learn more about JPEG.
ARCHIVE LOCATIONS   Where to find newer versions of this software.
RELATED SOFTWARE Other stuff you should get.
FILE FORMAT WARS Software *not* to get.
TO DO   Plans for future IJG releases.

Other documentation files in the distribution are:
User documentation:
install.doc   How to configure and install the IJG software.
usage.doc   Usage instructions for cjpeg, djpeg, jpegtran, rdjpgcom, and wrjpgcom.
*.1   Unix-style man pages for programs (same info as usage.doc).
wizard.doc   Advanced usage instructions for JPEG wizards only.
change.log   Version-to-version change highlights.

Programmer and internal documentation:
libjpeg.doc   How to use the JPEG library in your own programs.
example.c   Sample code for calling the JPEG library.
structure.doc   Overview of the JPEG library's internal structure.
filelist.doc   Road map of IJG files.
coderules.doc   Coding style rules --- please read if you contribute code.

Please read at least the files install.doc and usage.doc. Useful information can also be found in the JPEG FAQ (Frequently Asked Questions) article. See ARCHIVE LOCATIONS below to find out where to obtain the FAQ article.

If you want to understand how the JPEG code works, we suggest reading one or more of the REFERENCES, then looking at the documentation files (in the order listed) before diving into the code.

OVERVIEW
========

This package contains C software to implement JPEG image compression and decompression. JPEG (pronounced "jay-peg") is a standardized compression method for full-color and gray-scale images. JPEG is intended for compressing "real-world" scenes; line drawings, cartoons and other non-realistic images are not its strong suit. JPEG is lossy, meaning that the output image is not identical to the input image. Hence you must not use JPEG if you have to have identical output bits. However, on typical photographic images, very good compression levels can be obtained with no visible change, and remarkably high compression levels are possible if you can tolerate a low-quality image. For more details, see the references, or just experiment with various compression settings.

This software implements JPEG baseline, extended-sequential, and progressive compression processes. Provision is made for supporting all variants of these processes, although some uncommon parameter settings aren't implemented yet. For legal reasons, we are not distributing code for the arithmetic-coding variants of JPEG; see LEGAL ISSUES. We have made no provision for supporting the hierarchical or lossless processes defined in the standard.

We provide a set of library routines for reading and writing JPEG image files, plus two sample applications "cjpeg" and "djpeg", which use the library to perform conversion between JPEG and some other popular image file formats. The library is intended to be reused in other applications.

In order to support file conversion and viewing software, we have included considerable functionality beyond the bare JPEG coding/decoding capability; for example, the color quantization modules are not strictly part of JPEG decoding, but they are essential for output to colormapped file formats or colormapped displays. These extra functions can be compiled out of the library if not required for a particular application. We have also included "jpegtran", a utility for lossless transcoding between different JPEG processes, and "rdjpgcom" and "wrjpgcom", two simple applications for inserting and extracting textual comments in JFIF files.

The emphasis in designing this software has been on achieving portability and flexibility, while also making it fast enough to be useful. In particular, the software is not intended to be read as a tutorial on JPEG. (See the REFERENCES section for introductory material.) Rather, it is intended to be reliable, portable, industrial-strength code. We do not claim to have achieved that goal in every aspect of the software, but we strive for it.

We welcome the use of this software as a component of commercial products. No royalty is required, but we do ask for an acknowledgement in product documentation, as described under LEGAL ISSUES.

LEGAL ISSUES
============

In plain English:
1. We don't promise that this software works. (But if you find any bugs, please let us know!)
2. You can use this software for whatever you want. You don't have to pay us.
3. You may not pretend that you wrote this software. If you use it in a program, you must acknowledge somewhere in your documentation that you've used the IJG code.

In legalese:
The authors make NO WARRANTY or representation, either express or implied, with respect to this software, its quality, accuracy, merchantability, or fitness for a particular purpose. This software is provided "AS IS", and you, its user, assume the entire risk as to its quality and accuracy.

This software is copyright (C) 1991-1998, Thomas G. Lane.
All Rights Reserved except as specified below.

Permission is hereby granted to use, copy, modify, and distribute this software (or portions thereof) for any purpose, without fee, subject to these conditions:

(1) If any part of the source code for this software is distributed, then this README file must be included, with this copyright and no-warranty notice unaltered; and any additions, deletions, or changes to the original files must be clearly indicated in accompanying documentation.

(2) If only executable code is distributed, then the accompanying documentation must state that "this software is based in part on the work of the Independent JPEG Group".

(3) Permission for use of this software is granted only if the user accepts full responsibility for any undesirable consequences; the authors accept NO LIABILITY for damages of any kind.

These conditions apply to any software derived from or based on the IJG code, not just to the unmodified library. If you use our work, you ought to acknowledge us.

Permission is NOT granted for the use of any IJG author's name or company name in advertising or publicity relating to this software or products derived from it. This software may be referred to only as "the Independent JPEG Group's software".

We specifically permit and encourage the use of this software as the basis of commercial products, provided that all warranty or liability claims are assumed by the product vendor.

ansi2knr.c is included in this distribution by permission of L. Peter Deutsch, sole proprietor of its copyright holder, Aladdin Enterprises of Menlo Park, CA. ansi2knr.c is NOT covered by the above copyright and conditions, but instead by the usual distribution terms of the Free Software Foundation; principally, that you must include source code if you redistribute it. (See the file ansi2knr.c for full details.) However, since ansi2knr.c is not needed as part of any program generated from the IJG code, this does not limit you more than the foregoing paragraphs do.

The Unix configuration script "configure" was produced with GNU Autoconf. It is copyright by the Free Software Foundation but is freely distributable. The same holds for its supporting scripts (config.guess, config.sub, ltconfig, ltmain.sh). Another support script, install-sh, is copyright by M.I.T. but is also freely distributable.

It appears that the arithmetic coding option of the JPEG spec is covered by patents owned by IBM, AT&T, and Mitsubishi. Hence arithmetic coding cannot legally be used without obtaining one or more licenses. For this reason, support for arithmetic coding has been removed from the free JPEG software. (Since arithmetic coding provides only a marginal gain over the unpatented Huffman mode, it is unlikely that very many implementations will support it.)

So far as we are aware, there are no patent restrictions on the remaining code.

The IJG distribution formerly included code to read and write GIF files. To avoid entanglement with the Unisys LZW patent, GIF reading support has been removed altogether, and the GIF writer has been simplified to produce "uncompressed GIFs". This technique does not use the LZW algorithm; the resulting GIF files are larger than usual but are readable by all standard GIF decoders.

We are required to state that "The Graphics Interchange Format(c) is the Copyright property of CompuServe Incorporated. GIF(sm) is a Service Mark property of CompuServe Incorporated."

REFERENCES
==========

We highly recommend reading one or more of these references before trying to understand the innards of the JPEG software.

The best short technical introduction to the JPEG compression algorithm is Wallace, Gregory K. "The JPEG Still Picture Compression Standard", Communications of the ACM, April 1991 (vol. 34 no. 4), pp. 30-44.

(Adjacent articles in that issue discuss MPEG motion picture compression, applications of JPEG, and related topics.) If you don't have the CACM issue handy, a PostScript file containing a revised version of Wallace's article is available at ftp://ftp.uu.net/graphics/jpeg/wallace.ps.gz. The file (actually a preprint for an article that appeared in IEEE Trans. Consumer Electronics) omits the sample images that appeared in CACM, but it includes corrections and some added material. Note: the Wallace article is copyright ACM and IEEE, and it may not be used for commercial purposes.

A somewhat less technical, more leisurely introduction to JPEG can be found in "The Data Compression Book" by Mark Nelson and Jean-Loup Gailly, published by M&T Books (New York), 2nd ed. 1996, ISBN 1-55851-434-1. This book provides good explanations and example C code for a multitude of compression methods including JPEG. It is an excellent source if you are comfortable reading C code but don't know much about data compression in general. The book's JPEG sample code is far from industrial-strength, but when you are ready to look at a full implementation, you've got one here...

The best full description of JPEG is the textbook "JPEG Still Image Data Compression Standard" by William B. Pennebaker and Joan L. Mitchell, published by Van Nostrand Reinhold, 1993, ISBN 0-442-01272-1. Price US$59.95, 638 pp. The book includes the complete text of the ISO JPEG standards (DIS 10918-1 and draft DIS 10918-2). This is by far the most complete exposition of JPEG in existence, and we highly recommend it.

The JPEG standard itself is not available electronically; you must order a paper copy through ISO or ITU. (Unless you feel a need to own a certified official copy, we recommend buying the Pennebaker and Mitchell book instead; it's much cheaper and includes a great deal of useful explanatory material.) In the USA, copies of the standard may be ordered from ANSI Sales at (212) 642-4900, or from Global Engineering Documents at (800) 854-7179. (ANSI does not take credit card orders, but Global does.) It's not cheap: as of 1992, ANSI was charging $95 for Part 1 and $47 for Part 2, plus 7% shipping/handling. The standard is divided into two parts, Part 1 being the actual specification, while Part 2 covers compliance testing methods. Part 1 is titled "Digital Compression and Coding of Continuous-tone Still Images, Part 1: Requirements and guidelines" and has document numbers ISO/IEC IS 10918-1, ITU-T T.81. Part 2 is titled "Digital Compression and Coding of Continuous-tone Still Images, Part 2: Compliance testing" and has document numbers ISO/IEC IS 10918-2, ITU-T T.83.

Some extensions to the original JPEG standard are defined in JPEG Part 3, a newer ISO standard numbered ISO/IEC IS 10918-3 and ITU-T T.84. IJG currently does not support any Part 3 extensions.

The JPEG standard does not specify all details of an interchangeable file format. For the omitted details we follow the "JFIF" conventions, revision 1.02. A copy of the JFIF spec is available from:

Literature Department
C-Cube Microsystems, Inc.
1778 McCarthy Blvd.
Milpitas, CA 95035
phone (408) 944-6300, fax (408) 944-6314

A PostScript version of this document is available by FTP at ftp://ftp.uu.net/graphics/jpeg/jfif.ps.gz. There is also a plain text version at ftp://ftp.uu.net/graphics/jpeg/jfif.txt.gz, but it is missing the figures.

The TIFF 6.0 file format specification can be obtained by FTP from ftp://ftp.sgi.com/graphics/tiff/TIFF6.ps.gz. The JPEG incorporation scheme found in the TIFF 6.0 spec of 3-June-92 has a number of serious problems.

IJG does not recommend use of the TIFF 6.0 design (TIFF Compression tag 6). Instead, we recommend the JPEG design proposed by TIFF Technical Note #2 (Compression tag 7). Copies of this Note can be obtained from ftp.sgi.com or from ftp://ftp.uu.net/graphics/jpeg/. It is expected that the next revision of the TIFF spec will replace the 6.0 JPEG design with the Note's design.

Although IJG's own code does not support TIFF/JPEG, the free libtiff library uses our library to implement TIFF/JPEG per the Note. libtiff is available from ftp://ftp.sgi.com/graphics/tiff/.

ARCHIVE LOCATIONS
=================

The "official" archive site for this software is ftp.uu.net (Internet address 192.48.96.9). The most recent released version can always be found there in directory graphics/jpeg. This particular version will be archived as ftp://ftp.uu.net/graphics/jpeg/jpegsrc.v6b.tar.gz. If you don't have direct Internet access, UUNET's archives are also available via UUCP; contact help@uunet.uu.net for information on retrieving files that way.

Numerous Internet sites maintain copies of the UUNET files. However, only ftp.uu.net is guaranteed to have the latest official version.

You can also obtain this software in DOS-compatible "zip" archive format from the SimTel archives (ftp://ftp.simtel.net/pub/simtelnet/msdos/graphics/), or on CompuServe in the Graphics Support forum (GO CIS:GRAPHSUP), library 12 "JPEG Tools". Again, these versions may sometimes lag behind the ftp.uu.net release.

The JPEG FAQ (Frequently Asked Questions) article is a useful source of general information about JPEG. It is updated constantly and therefore is not included in this distribution. The FAQ is posted every two weeks to Usenet newsgroups comp.graphics.misc, news.answers, and other groups. It is available on the World Wide Web at http://www.faqs.org/faqs/jpeg-faq/ and other news.answers archive sites, including the official news.answers archive at rtfm.mit.edu: ftp://rtfm.mit.edu/pub/usenet/news.answers/jpeg-faq/.

If you don't have Web or FTP access, send e-mail to mail-server@rtfm.mit.edu with body send usenet/news.answers/jpeg-faq/part1 send usenet/news.answers/jpeg-faq/part2

RELATED SOFTWARE
================

Numerous viewing and image manipulation programs now support JPEG. (Quite a few of them use this library to do so.) The JPEG FAQ described above lists some of the more popular free and shareware viewers, and tells where to obtain them on Internet.

If you are on a Unix machine, we highly recommend Jef Poskanzer's free PBMPLUS software, which provides many useful operations on PPM-format image files. In particular, it can convert PPM images to and from a wide range of other formats, thus making cjpeg/djpeg considerably more useful. The latest version is distributed by the NetPBM group, and is available from numerous sites, notably ftp://wuarchive.wustl.edu/graphics/graphics/packages/NetPBM/.

Unfortunately, PBMPLUS/NETPBM is not nearly as portable as the IJG software is; you are likely to have difficulty making it work on any non-Unix machine.

A different free JPEG implementation, written by the PVRG group at Stanford, is available from ftp://havefun.stanford.edu/pub/jpeg/. This program is designed for research and experimentation rather than production use; it is slower, harder to use, and less portable than the IJG code, but it is easier to read and modify. Also, the PVRG code supports lossless JPEG, which we do not. (On the other hand, it does not do progressive JPEG.)

FILE FORMAT WARS
================

Some JPEG programs produce files that are not compatible with our library. The root of the problem is that the ISO JPEG committee failed to specify a concrete file format. Some vendors "filled in the blanks" on their own, creating proprietary formats that no one else could read. (For example, none of the early commercial JPEG implementations for the Macintosh were able to exchange compressed files.)

The file format we have adopted is called JFIF (see REFERENCES). This format has been agreed to by a number of major commercial JPEG vendors, and it has become the de facto standard. JFIF is a minimal or "low end" representation. We recommend the use of TIFF/JPEG (TIFF revision 6.0 as modified by TIFF Technical Note #2) for "high end" applications that need to record a lot of additional data about an image. TIFF/JPEG is fairly new and not yet widely supported, unfortunately.

The upcoming JPEG Part 3 standard defines a file format called SPIFF. SPIFF is interoperable with JFIF, in the sense that most JFIF decoders should be able to read the most common variant of SPIFF. SPIFF has some technical advantages over JFIF, but its major claim to fame is that it is an official standard rather than an informal one. At this point it is unclear whether SPIFF will supersede JFIF or whether JFIF will remain the de-facto standard. IJG intends to support SPIFF once the standard is frozen, but we have not decided whether it should become our default output format or not. (In any case, our decoder will remain capable of reading JFIF indefinitely.) Various proprietary file formats incorporating JPEG compression also exist.

We have little or no sympathy for the existence of these formats. Indeed, one of the original reasons for developing this free software was to help force convergence on common, open format standards for JPEG files. Don't use a proprietary file format!

TO DO
=====

The major thrust for v7 will probably be improvement of visual quality.

The current method for scaling the quantization tables is known not to be very good at low Q values. We also intend to investigate block boundary smoothing, "poor man's variable quantization", and other means of improving quality-vs-file-size performance without sacrificing compatibility.

In future versions, we are considering supporting some of the upcoming JPEG
Part 3 extensions --- principally, variable quantization and the SPIFF file format. As always, speeding things up is of great interest. Please send bug reports, offers of help, etc. to jpeg-info@uunet.uu.net.

INDEX