V7 IP Server Administrative Guide

Copyright 2017 – Panasonic System Communications Company of North America
Last updated: Friday, October 06, 2017
# TABLE OF CONTENTS

**VIDEO INSIGHT SOFTWARE LICENSE AGREEMENT** ................................................................. 5

**CHAPTER I** \**INTRODUCTION**.......................................................................................... 9

**SECTION 1)** \**SYSTEM OVERVIEW** ............................................................................. 9

**SECTION 2)** \**SOFTWARE COMPONENTS** ................................................................. 10

**Part A)** \**VI MonitorPlus** ............................................................................................. 11

**Part B)** \**Web Client** .................................................................................................. 11

**Part C)** \**VI Mobile** ................................................................................................... 12

**CHAPTER II** \**PLANNING** ............................................................................................. 13

**SECTION 1)** \**CONSIDERATIONS BEFORE INSTALLATION** ........................................ 13

**Part A)** \**IP Server and Accessory Software Installation** ........................................... 14

**Part B)** \**Network Configuration** ................................................................................. 17

**Part C)** \**Cameras** ..................................................................................................... 19

**Part D)** \**Storage considerations** ............................................................................... 20

**SECTION 2)** \**LICENSEING** ........................................................................................ 23

**Part A)** \**Panasonic Camera License Activation** .......................................................... 23

**SECTION 3)** \**HARDWARE / SOFTWARE REQUIREMENTS FOR CLIENT** ................... 24

**CHAPTER III** \**INSTALLATION AND ADMINISTRATION** ............................................... 27

**SECTION 1)** \**IP SERVER** ............................................................................................ 28

**Part A)** \**Installation** .................................................................................................. 28

**Part B)** \**Initialization** ............................................................................................... 33

**SECTION 2)** \**VI MONITORPLUS CLIENT** ................................................................. 37

**Part A)** \**Manually Adding Additional Servers to VI MonitorPlus** .............................. 38

**Part B)** \**Adding more than one IP Server to VI MonitorPlus** ................................... 39

**SECTION 3)** \**ADMINISTRATION** ................................................................................ 41

**Part A)** \**IP Server Manager (IPSM)** ......................................................................... 41

**SECTION 4)** \**ADVANCED INSTALLATION CONFIGURATION INFORMATION** .............. 54

**Part A)** \**Installer: Installshield** ................................................................................. 54

**Part B)** \**Server Backup and Restore** ....................................................................... 54

**Part C)** \**Edge Recording** .......................................................................................... 55

**Part D)** \**Rules Manager** ............................................................................................ 61

**Part E)** \**Failover Server** ............................................................................................ 87

**CHAPTER IV** \**VI MONITORPLUS** ................................................................................. 91

**SECTION 1)** \**MENU BAR OPTIONS** ........................................................................... 91

**SECTION 2)** \**TAB: WORKSPACES** .......................................................................... 91

**Part A)** \**Save** .......................................................................................................... 91

**Part B)** \**Manage** ..................................................................................................... 92

**SECTION 3)** \**LEFT HAND MENU ICONS** ................................................................. 92

**Part A)** \**Servers** ....................................................................................................... 92
CHAPTER V WEB CLIENT .................................................................................................................. 148

SECTION 1) LOGGING IN .................................................................................................................. 148

SECTION 2) LIVE VIDEO .................................................................................................................. 148

Part A) Camera Manipulation ........................................................................................................... 149

SECTION 3) FACILITY MAPS ......................................................................................................... 149

SECTION 4) LAYOUT DIRECTORY ................................................................................................. 150

SECTION 5) RECORDED VIDEO ...................................................................................................... 150

Part A) Creating Clips ....................................................................................................................... 151

Part B) Watermark Verification ........................................................................................................ 152

SECTION 6) HIGH SPEED MODE ................................................................................................... 152

SECTION 7) ACCESS CONTROL ..................................................................................................... 153

SECTION 8) ADMIN FEATURES ....................................................................................................... 154

Part A) Servers ............................................................................................................................... 156

Part B) Cameras .............................................................................................................................. 157

Part C) VIEWS (FORMERLY KNOWN AS LAYOUTS) ..................................................................... 158

Part D) General Settings ................................................................................................................ 159

CHAPTER VI PUBLIC VIEW MONITOR ........................................................................................... 162

SECTION 1) DOWNLOAD SETUP ...................................................................................................... 162
VIDEO INSIGHT SOFTWARE LICENSE AGREEMENT

IMPORTANT – READ CAREFULLY BEFORE ACCESSING VIDEO INSIGHT SOFTWARE: This license agreement ("License Agreement") is a legal agreement between the individual, corporate or other entity or governmental entity, as applicable, that is licensing the Software (referred to herein as “You” or “Licensee”) and Video Insight, Inc. and its suppliers (collectively, “Video Insight” or “Licensor”) for the Software (the “Software”).

FEDERAL GOVERNMENT LICENSEEES: “You” or “Licensee” refers to an Ordering Activity, as defined in GSA Order ADM4800.2G and as revised from time to time

USERS OTHER THAN FEDERAL GOVERNMENT LICENSEEES: 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.

FEDERAL GOVERNMENT LICENSEEES: THE AUTHORIZED CONTRACTING OFFICER ACCEPTED THE TERMS OF THIS LICENSE AGREEMENT IN ACCORDANCE WITH FAR 1.601(a).

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.
   b. Product Coverage. You may also use this License Agreement to access or otherwise use the services or functionality of Video Insight Software utilized by other individuals or entities provided that the other individuals or entities obtain a valid license.
   c. System Limits. You may use the Software with one unique system identified by its unique capture board. Each unique system requires a separate License Agreement.

2. TERMINATION (NOT APPLICABLE TO FEDERAL GOVERNMENT LICENSEEES): Without prejudice to any other rights, Video Insight 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 return all component parts.

3. TRANSFER. You may move the Software to a different server.

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

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

6. LIMITED WARRANTY. Because of uncertain or unknown conditions and incidental hazards under which the Software is used, Video Insight does not warrant or guarantee that any particular result will be achieved. You understand and agree that suppliers and/or installers of the Software are independent contractors that are not employed by or under the control of Video Insight. Video Insight disclaims all liability and responsibility for damages or other loss caused by any independent supplier/installer or other third-party. The sole and exclusive warranty provided by Video Insight 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 any event shall expire ninety (90) days after the date you receive the Software, unless prohibited by law. As to any defects discovered after ninety days from receipt, there is no warranty or condition of any kind. Any supplements or updates to the Software, including without limitation any (if any) service packs or hotfixes 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 and to the maximum extent permitted by applicable law, Video Insight 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 VIDEO INSIGHT, 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 VIDEO INSIGHT AND EXCLUDED FROM THIS AGREEMENT. ALSO, THERE IS NO WARRANTY OR CONDITION OF TITLE, QUIET ENJOYMENT, QUIET POSSESSION, CORRESPONDENCE TO DESCRIPTION OR NON-INFRINGEMENT WITH REGARD TO THE SOFTWARE. NO AFFIRMATION WHETHER BY WORDS OR ACTIONS BY VIDEO INSIGHT, ITS AGENTS, EMPLOYEES OR REPRESENTATIVES SHALL constitute a warranty. APPLICABLE TO FEDERAL GOVERNMENT LICENSEES: THIS AGREEMENT DOES NOT LIMIT OR DISCLAIM ANY OF THE WARRANTIES SPECIFIED IN THE GSA SCHEDULE 70 CONTRACT UNDER FAR 52.212-4(O). IN THE EVENT OF A BREACH OF WARRANTY. THE U.S. GOVERNMENT RESERVES ALL RIGHTS AND REMEDIES UNDER THE CONTRACT, THE FEDERAL ACQUISITION REGULATIONS, AND THE CONTRACT DISPUTES ACT, 41 USC 7101-7109.

7. Limited and Exclusive Remedy. Video Insight’s sole responsibility and Your exclusive remedy for any nonconformance or defect is expressly limited to the refund of the purchase price paid, if any, or the replacement of the Software determined by Video Insight, in its sole discretion, to possess such a defect. As a condition precedent to any remedy described herein, or otherwise available to You, You shall seek and accept Video Insight’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 Video Insight is responsible, You shall inform Video Insight immediately by telephone at (713) 621-9779 and by providing written notification to Video Insight 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.

8. NO CONSEQUENTIAL OR OTHER DAMAGES. NOTWITHSTANDING ANYTHING TO THE CONTRARY, EXPRESS OR IMPLIED, (1) VIDEO INSIGHT’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 VIDEO INSIGHT SHALL NOT EXCEED THE PRICE, IF ANY, YOU PAID FOR THE SOFTWARE OR $5.00, WHICHEVER IS GREATER; AND (2) VIDEO INSIGHT SHALL IN NO EVENT BE LIABLE FOR SPECIAL, INDIRECT, 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 VIDEO INSIGHT’S NEGLIGENCE, FAULT OR STRICT LIABILITY). CUSTOMER ASSUMES THE RISK FOR AND INDEMNIFIES VIDEO INSIGHT FROM AND AGAINST ALL LIABILITIES FOR ANY LOSS, DAMAGE OR INJURY TO PERSONS OR PROPERTY ARISING OUT OF, CONNECTED WITH OR RESULTING

Copyright 2017 – Panasonic System Communications Company of North America

Last updated: Friday, October 06, 2017
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. VIDEO INSIGHT 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. APPLICABLE TO FEDERAL GOVERNMENT LICENSEES: THIS CLAUSE SHALL NOT IMPAIR THE U.S. GOVERNMENT’S RIGHT TO RECOVER FOR FRAUD OR CRIMES ARISING OUT OF OR RELATED TO THIS AGREEMENT UNDER ANY FEDERAL FRAUD STATUTE. FURTHERMORE, THIS CLAUSE SHALL NOT IMPAIR NOR PREJUDICE THE U.S. GOVERNMENT’S RIGHT TO EXPRESS REMEDIES PROVIDED IN THE SCHEDULE CONTRACT (I.E. PRICE REDUCTIONS, PATENT INDEMNIFICATION, LIABILITY FOR INJURY OR DAMAGE, PRICE ADJUSTMENT, FAILURE TO PROVIDE ACCURATE INFORMATION.)

9. INDEMNIFICATION (NOT APPLICABLE TO FEDERAL GOVERNMENT LICENSEES): YOU AGREE TO PROTECT, INDEMNIFY, HOLD HARMLESS AND DEFEND VIDEO INSIGHT 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 VIDEO INSIGHT 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 VIDEO INSIGHT 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 VIDEO INSIGHT OR ITS EMPLOYEES OR AGENTS.

10. 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 Video Insight 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.

11. 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 is strictly prohibited and constitutes a material breach of this License Agreement.

12. APPLICABLE LAW.
   a. LICENSEES OTHER THAN FEDERAL GOVERNMENT LICENSEES: This License Agreement is governed by the laws of the State of Texas. Video Insight 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 Texas or within the courts of the United States of America located within the Southern District of Texas. Video Insight and Licensee consent to venue and jurisdiction within the Courts of Harris County, Texas.
   b. FEDERAL GOVERNMENT LICENSEES: This License Agreement is governed by the laws of the United States. Video Insight 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 United States of America.

Copyright 2017 – Panasonic System Communications Company of North America
Last updated: Friday, October 06, 2017
13. **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.

14. **ENTIRE AGREEMENT (NOT APPLICABLE TO FEDERAL GOVERNMENT LICENSEEES)**. 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 Video Insight 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 Video Insight policies or programs for support services conflict with the terms of the License Agreement, the terms of the License Agreement shall control.

15. This software is of U.S. origin and is subject to the Export Administration Regulations. Diversion contrary to U.S. law is prohibited.

HOUSTON 6467133v.3
Chapter I  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 v7 can intelligently and efficiently monitor security throughout your organization. Key advantages of this version are:

- Easy to Use Updated User 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.

SECTION 1)  SYSTEM OVERVIEW

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

The Video Insight application suite runs over an Ethernet network, meaning cameras, security personnel, and servers do not have to be co-located. 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.
SECTION 2) SOFTWARE COMPONENTS

The Video Insight software suite has three main components used to monitor live and recorded video; the VI MonitorPlus, Web Client and VI Mobile. These three clients can be used to connect to the IP Server at no additional charge.

**Thick Clients**
VI MonitorPlus and VI Mobile communicate directly with the server to receive camera feeds. One instance of VI MonitorPlus or VI Mobile can communicate with multiple servers for the same user interface.

**Web Client**
The Web Client connects to the server via Microsoft IIS. IIS can run on each server or a single IIS server can support all Web Clients.

**Server**
The Server is the hub of the Video Insight IP Video Management Software (VMS) product. The Video Insight IP Server communicates directly with the cameras and the Clients, provides storage, and runs the SQL database.

**Storage**
Storage options are limitless as they are customizable depending on the chosen server size or a variety of storage options.

**SQL**
The SQL server database saves all configuration, motion, and system logs.

Copyright 2017 – Panasonic System Communications Company of North America
Last updated: Friday, October 06, 2017
Part A) VI MonitorPlus

VI MonitorPlus is the primary User Interface for the Product Suite. It provides centralized viewing of all live and recorded video from any server to the end user. VI MonitorPlus also provides the camera configuration menus for System and Security Administrators. It is a thick client, allows users full access to all cameras and provides centralized administration for the system. It is used to watch live and recorded video. It runs on industry-standard hardware and works with 32- and 64-bit versions of Microsoft Windows XP or later. Microsoft DirectShow 9 or higher is required. The operating system must be current with all recent updates because Video Insight’s IP Server software integrates with the latest updates from Microsoft.

VI MonitorPlus pulls video from the server in the camera’s native format. Transferring video in the camera’s native format is a file server operation that does not burden the IP Server CPU as a video decompression operation would. Because video decompression is performed on the client and not the server, the hardware requirements for VI MonitorPlus are different from those of IP Server.

Part B) Web Client

The Web Client accesses IP Server via Microsoft Internet Information Services (IIS). It can be accessed from any browser application and has an optional Active X control for Internet Explorer. The Web Client has access to live and recorded video and can access Facility Maps. The Web Client can also create clips and download recorded video Web Client, allows users remote access to cameras. Web Client is distinct from the Video Insight mobile device application. Web Client utilizes Microsoft IIS services hosted on the same server as IP Server. To support cross-platform compatibility, IP Server sends MJPEG images to clients that are unable to decompress MPEG4 or H.264 streams. These images are normally provided as a dual stream from the camera. IP Server can create an MJPEG but this increases the load on the CPU. Web Client connects directly to the cameras to view live video, unlike VI MonitorPlus Client. Web Client currently supports Internet Explorer 11+ or Chrome (for low speed only). Note: Other HTML5 compatible browsers may work.
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.

In this document, we will explain and focus on the VI MonitorPlus component exclusively, for more information on the VI Mobile client software, please reference the VI Mobile User Guides available on the www.downloadvi.com website.
Chapter II  PLANNING

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

SECTION 1) CONSIDERATIONS BEFORE INSTALLATION

Before beginning the installation process, it is necessary to determine key system requirements, for example, will the system:

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

If the system is going to be a single, stand-alone installation of IP Server, opting to use the basic installation process is recommended. Follow the installation instructions for “Installation without an existing SQL Installation” to achieve success.

If Microsoft SQL Server is not already present in your environment you can choose to install the SQL-EXPRESS version included in the complete download. The package includes Microsoft SQL Server 2012.

If the installation server/environment already has Microsoft SQL Server installed, then the only necessary item to install is the IP Server itself. This does not mean that SQL is not necessary for proper IP Server configuration and functionality, as the SQL database is a required element of IP Server Enterprise.
Part A) IP Server and Accessory Software Installation

Video Insight software supports both 32-bit and 64-bit operating systems. Download and install the correct installation for your version. Review the following list prior to beginning the installation process:

- Storage Considerations
- SQL Considerations
- Network Considerations


Administrator-level access on server during Installation and Troubleshooting is required.

(1) IP SERVER PREREQUISITES

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 these Microsoft operating systems.

- Windows Server 2008 R2
- Windows Server 2008 Enterprise, Standard and Web editions
- Windows 7 Pro and Enterprise editions
- Windows Server 2012
- Windows 8 Pro and Enterprise editions
- Windows 10 Pro, Enterprise and Education editions

IP Server also requires Microsoft .NET Framework 4.5+ and Microsoft Internet Information Services (IIS) with “static content” enabled. As Video Insight hardware and software is designed to integrate with the latest Windows updates, the operating system must be updated with all current Windows updates applied.

The hardware required for installation of IP Server is determined by a variety of factors including the number of cameras, the resolution of those cameras, the number of frames per second, as well as the number of days of required video storage.

(2) ACTIVE DIRECTORY PREREQUISITES

- Active Directory server with users and groups configured.
- Active Directory can be configured using a local database for each server or using 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 which allows modifying the registry of the IP Server, and granting other Active Directory user-scopes and security-objects the necessary permissions for accessing video storage in both read/write would be appropriate if the local Administrator account is used to install and modify IP Server during the initial setup process.

- 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 changed. Port 636 is used for SSL encryption.
- IP Server configuration must be done while logged into the domain with a valid domain account. This is required by Windows for security reasons.
- Video Insight recommends importing users as a group instead of individually. The group must be created in Active Directory before it can be imported. You can create groups to suit the individual needs and policies of the organization installing IP Server.

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.

Restart the IIS Admin service if using Web Client

---

(3) **FAILOVER SERVER**

In the event a network outage or hardware failure prevents a server from recording camera video, the IP Server Failover Server feature will enable another server to take over the recording capabilities of the offline server. When configured with a shared 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 must be met:

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

---

(4) **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:

<table>
<thead>
<tr>
<th>Local Database</th>
<th>Shared Database</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small centralized organization with 1-3 servers</td>
<td>Large regional organization with many servers</td>
</tr>
<tr>
<td>Use VI MonitorPlus Client and built-in User Manager</td>
<td>Use Active Directory/LDAP</td>
</tr>
<tr>
<td>Disaster recovery and backup for each server’s database</td>
<td>Disaster recovery and backup for one database</td>
</tr>
<tr>
<td>Failover server functionality is not desired</td>
<td>Failover server functionality is desired</td>
</tr>
<tr>
<td>Cameras will not move from one server to another</td>
<td>Cameras will move from one server to another at final configuration</td>
</tr>
<tr>
<td>Avoids unnecessary exposure of SQL database to the network</td>
<td>Exposure of SQL database to the network in a secured network environment</td>
</tr>
</tbody>
</table>
(5) 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.

Part B) 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, mobile device client and Video Wall increases the 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, outside interference and weather conditions, 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, then it will likely rely on an Internet provider for connectivity between the two site locations. The performance expectation from the internet service provider will depend on their network infrastructure, customer utilization of that network and what can be afforded.

For best results, consider creating link between the two remote sites with nothing less than 50Mbps up/down for connecting between 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 WIFI.

(2) EXAMPLE ROUTER CONFIGURATION
Video Insight recommends using some type of router if the IP Server is connected to the internet. Small Office/Home Office (SOHO) routers provide a simple hardware firewall that protect the computer. SOHO routers connect to a DSL or cable modem and then connect to the server with them. The SOHO router prevents all inbound traffic from accessing the network and computers except for the traffic that are specifically allowed through the firewall.

How to configure the IP Server and router for remote access:

1. Assign a static IP address to the IP Server.
2. NOTE: SOHO routers typically use DHCP to assign an IP address from a range of addresses to devices connected to the router. Choose an address outside of this range but within the subnet to assign to the server. For help on assigning a static IP address, review your SOHO router user guide or consult with a network administrator.
3. Configure your SOHO router to forward ports 80 and 4011 to IP Server.
4. For help on forwarding ports, review manual that came with the router consult with a network administrator.
5. [http://www.portfoward.com](http://www.portfoward.com) provides information on how to configure most SOHO routers. Video Insight does not endorse or support the information found on this website.
6. Test the IP Servers configuration by trying to access the Web Client externally.
7. Start an Internet browser.
8. Enter: http://<external IP>/videoinsight into the address bar of the Internet browser.

Note, many SOHO routers will not allow a connection to the external IP address when the IP Server is behind the firewall. Testing will need to be conducted outside of the local area network (LAN).
Part C) Cameras

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

Video Insight supports the Open Network Video Interface Forum (ONVIF) standard. We support version 1.02 and Profile S.

The following factors can affect camera imaging as it is seen within VI MonitorPlus, connected to an IP Server:

- Bit Rate – a higher bit rate usually gives better picture quality
- Resolution – a higher resolution usually gives better picture quality
- Format – some picture formats such as 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, but not limited to: H.264, 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

(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 in order for audio recording to function within IP Server’s video recording process.

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

<table>
<thead>
<tr>
<th>L8 @ 8K (Uncompressed 8-bit audio)</th>
<th>L16 @ 16K (Uncompressed 16-bit audio)</th>
</tr>
</thead>
<tbody>
<tr>
<td>G711 ULA\W and ALAW @ 8K and 16K</td>
<td>G726 40/32/24/16</td>
</tr>
<tr>
<td>AAC Low Complexity (*) Bitrate is 128kbps or less</td>
<td>AMR Audio</td>
</tr>
</tbody>
</table>

Copyright 2017 – Panasonic System Communications Company of North America

Last updated: Friday, October 06, 2017
Part D) Storage considerations

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

<table>
<thead>
<tr>
<th>Storage Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Record Always</td>
<td>This requires significantly more storage space because video is constantly recorded.</td>
</tr>
<tr>
<td>Motion Only</td>
<td>This requires less storage space than Record Always because video is recorded only when motion occurs in the camera’s field of view.</td>
</tr>
<tr>
<td>Schedule</td>
<td>This configuration allows both Record Always and Motion Only in specified schedule.</td>
</tr>
</tbody>
</table>

IP Server supports the following types of storage:

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

(1) SERVER AND STORAGE

IP Server

IP Server 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 the video locally or write directly to NAS or SAN devices.

Storage

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 7 GB of storage per day.


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.

Since most storage systems refer to their 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 3Mbits/sec or a total of 300Mbits 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](http://www.downloadvi.com) website. Click on Tools. Under the Utilities section, the Hard Drive Speed Test will be found.

(2) **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.

(A) **IP SERVER SAMPLE CONFIGURATIONS**

The below is the sample specification for IP Server based on camera number and configuration

<table>
<thead>
<tr>
<th>20 H.264 cameras streaming 1.5Mbps</th>
<th>40 H.264 cameras streaming 1.5Mbps</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server Hardware Configuration:</strong></td>
<td><strong>Server Hardware Configuration:</strong></td>
</tr>
<tr>
<td>Dell Optiplex 7010 with Intel Core i5 3.30 GHz, with 4GB, 3TB of Storage, Intel HD 2500 Graphics, and Windows 7 Professional</td>
<td>Dell Optiplex 7010 with Intel Core i5 3.30 GHz, with 4GB, 3TB of Storage, Intel HD 2500 Graphics, and Windows 7 Professional</td>
</tr>
<tr>
<td>CPU Performance of server while recording video without anyone logged into the system.: 10% utilization while using Camera-Side Motion Detection.</td>
<td></td>
</tr>
<tr>
<td><strong>Number of Live Camera Views: CPU Utilization</strong></td>
<td><strong>Number of Live Camera Views: CPU Utilization</strong></td>
</tr>
<tr>
<td>4 Live Windows: CPU utilization at 25%</td>
<td>4 Live Windows CPU utilization at 25%</td>
</tr>
<tr>
<td>9 Live Windows: CPU utilization at 35%</td>
<td>9 Live Windows CPU utilization at 35%</td>
</tr>
<tr>
<td>16 Live Windows: CPU utilization at 45%</td>
<td>16 Live Windows CPU utilization at 45%</td>
</tr>
<tr>
<td>20 Live Windows: CPU utilization at 60%</td>
<td>20 Live Windows CPU utilization at 60%</td>
</tr>
<tr>
<td>120 H.264 cameras streaming 1.5Mbps</td>
<td>240 H.264 cameras streaming 1.5Mbps</td>
</tr>
</tbody>
</table>
**Server Hardware Configuration:**
Dell PowerEdge R520 2U Rackmount with Dual Intel Xeon E5-2403 1.80GHz, with 8GB, 21TB of RAID5 Storage, Intel HD 2500 Graphics, and Windows Server 2008

**Server Hardware Configuration:**
Dell PowerEdge R720xd 2U Rackmount with Dual Intel Xeon E5-2403 1.80GHz, with 8GB, 42TB of RAID5 Storage, Intel HD 2500 Graphics, and Windows Server 2008

CPU Performance of server while recording video without anyone logged into the system:
10% utilization while using Camera-Side Motion Detection.

**Number of Live Camera Views: CPU Utilization**

<table>
<thead>
<tr>
<th>Number of Live Windows</th>
<th>CPU Utilization</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 Live Windows</td>
<td>25%</td>
</tr>
<tr>
<td>9 Live Windows</td>
<td>35%</td>
</tr>
<tr>
<td>16 Live Windows</td>
<td>45%</td>
</tr>
<tr>
<td>20 Live Windows</td>
<td>60%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Number of Live Windows</th>
<th>CPU Utilization</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 Live Windows</td>
<td>25%</td>
</tr>
<tr>
<td>9 Live Windows</td>
<td>35%</td>
</tr>
<tr>
<td>16 Live Windows</td>
<td>45%</td>
</tr>
<tr>
<td>20 Live Windows</td>
<td>60%</td>
</tr>
</tbody>
</table>
SECTION 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 means there is no need to tie a licensing seat, IP address or MAC address to a particular camera.

Cameras offering multiple camera views only require one 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.

Part A) Panasonic Camera License Activation

Video Insight offers a bundle license for Panasonic i-PRO camera that was made in October 2014 or later. To generate a Panasonic camera license for the Video Insight serial number registration process, please follow the directions found on the chapter of “PANASONIC LICENSING Error! Reference source not found.”.
SECTION 3) HARDWARE / SOFTWARE REQUIREMENTS FOR CLIENT

(1) VI MONITORPLUS

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

VI MonitorPlus runs on industry-standard hardware and works with 32-bit and 64-bit versions of Microsoft Windows XP or later. Microsoft DirectShow 9 or higher is required.

VI MonitorPlus streams video from the server in the camera’s native format. Transferring video in the camera’s native format is a file server operation that does not burden the IP Server CPU as a video decompression operation would. Because video decompression is performed on the client and not the server, the hardware requirements for VI MonitorPlus are different from those of IP Server.

**VI MonitorPlus Client Hardware requirements**

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum</th>
<th>Recommended (for use with H.265 Cameras)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>Intel HD Graphics 4th generation or better Intel Core processor based platforms (1.2 GHz dual-core)</td>
<td>6th Generation or better Intel Core processor (1.3 GHz quad-core+)</td>
</tr>
<tr>
<td>Memory</td>
<td>8 GB</td>
<td>8 GB+</td>
</tr>
<tr>
<td>Video</td>
<td>512 MB</td>
<td>1 GB+</td>
</tr>
<tr>
<td>Network</td>
<td>100 Mb/s</td>
<td>1 Gb/s+</td>
</tr>
<tr>
<td>Display Resolution</td>
<td>1600 X 900</td>
<td>1920 X 1080</td>
</tr>
</tbody>
</table>

**Note** The video subsystem must support Microsoft DirectShow.

VI MonitorPlus will require additional system memory, video memory and processor when more cameras are viewed or while processor-intensive compression protocols are used.

Dual streaming (model specific) on the client is also available for the ability to monitor more cameras at once.
(A) HARDWARE REQUIREMENT FOR H.265 CAMERAS

For optimal use of H.265 codec capable cameras, it is highly recommended that a minimum of these hardware practices is implemented although the software decoding is also available:

- Intel HD Graphics 4th or upper generation Intel Core processor-based platforms, as per the specification table above.
- GPU (NVIDIA GTX 950, 1050, 1050Ti and 1060)
- If a separate graphics card (not the above models) is installed alongside the on-board intel graphics card, go to BIOS to set the separate graphics card as primary display. Separate graphics card (except HDMI connections) and on-board intel graphics card (except VGA connections) connected to the monitor. Check with Intel download center to get the right driver for the on-board Intel graphics card.
- IP Server will detect whether the on-board graphics card supports hardware acceleration automatically and use it when it is available. But IP Server only enables it during live and playback streaming for 4k or larger resolution. For all other cases, server-side motion detection, thumbnail, snapshot and mobile device low speed (jpeg conversion), hardware acceleration is not used because of asynchronous limitations.

Configuration of the hardware decoding for H.265 is quite simple. Within VI MonitorPlus the following items must be selected / altered:

Enable hardware decoding in Option → Configuration is required. If the CPU does not support the HW codec, it won’t display properly within VI MonitorPlus.

“Highest Performance” is for video streaming where the display provides multiple cameras at the same time. If a requirement for use of high framerates and high bitrates for multiple cameras, it is suggested to enable the “Highest Performance” setting. However, for simpler, single camera layouts, “Normal mode” is acceptable since the current Intel based hardware codecs are capable of handling approximately two 4k cameras with 30 fps.
Operating system requirements for hosting the Web Client interface vary according to the Operating System used. For reference the following Microsoft Operating systems are supported:

- Windows 2008 Server
- Windows Vista Professional
- Windows 7 Professional
- Windows 8 Professional
- Windows Server 2012

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

- Microsoft .NET Framework version 4.5+ (or better)
- Microsoft IIS v6.0 (or better)

Necessary Microsoft IIS Components for full functionality of Web Client:

- ASP.NET
- ASP
- 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 that each of the above system prerequisites should be updated to reflect the most recent stable version offered by the Microsoft Update Services, prior to installation.

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

- Internet Explorer version 11
- Google Chrome

*Other HTML5 compliant browsers may work, however, we will only provide support using the browsers listed above.*
Chapter III  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 to 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.

**NOTE:** 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.
SECTION 1) IP SERVER

Part A) Installation

(1) INSTALLATION WITH SQL DATABASE

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

Step 1:
Download the proper installer (32-bit or 64-bit) for the server environment from DownloadVI.com.

Step 2:
Launch the executable installer as Administrator. Then click Next.

Step 3:
Click Next, then Chose “I accept...” to agree to the terms and continue the installation. If you do not agree or do not want to continue the installation, click Cancel.
Step 4:
Select all desired components desired for installation and then click Next.

Step 5:
The default credentials are entered for the SQL installation. If you would like to change the credentials please enter them now and click Next.

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

Step 6:
Select the start menu folder that you would like the installation to be created, click Next.
Step 7:
To accept the default destination folder, click Next.
To choose another destination, enter the destination path or click Browse to search.

Step 8:
To begin the installation process, click Next.

(2) INSTALLATION WITH AN EXISTING SQL DATABASE

Use the following steps to install IP Server for the first time in an environment with Microsoft SQL Server. This option will also install VI MonitorPlus Client and Web Client.
Step 1:
Select all the components that you would like to install excluding “SQL Server 2012 Express” then click Next.

Step 2:
The default credentials are entered for the SQL installation, as seen in the figure, below.
Optional: If there is a need to change the credentials, please enter them now and click Next.

Step 3:
Select the start menu folder that you would like the installation to be created, click Next.
Step 4:

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

**Optional:**

To choose another destination, enter the destination path or click **Browse** to search.

---

Step 5:

To start installing, click **Install**.

Once these steps have been taken, a series of screens appear. These screens can largely be ignored as they are mere informational and demonstrate that the process of installation is underway.

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

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

---

Now that IP Server is installed, the next series of steps will guide the administrator to the end of the entire setup process.
Part B) Initialization

In order for IP server to function properly, it should be installed and initialized with a serial key. However, if a serial key is not available, Demo mode can be used until 60 days and 99 cameras. To activate IP Server at initialization, the following is Options:

**Option 1**: “Activate or Upgrade your license through the internet”

This can be completed on a server with an active internet connection. This has to be allowed to connect the port 30000. If online activation fails, try Option 2.

**Option 2**: “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**: This is available in the United States only. Please contact the sales agent or vendor where you purchased IP Server Enterprise.

**Option 3**: “Demo Mode”

Selecting Demo mode will allow IP Server to operate normally for up to 60 days using up to 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 initialization is completed with a valid serial number or activation code. Reinstallation is not required.

**Step 1**: To activate and initialize IP Server, click **Next**
Step 2:
Where prompted, enter the five-character, alpha-numeric, serial number provided at the time of purchase.

Step 3:
Click Next.

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

Select **Activate by Phone** and call 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.)

Step 4:
Next, enter the user information in the event there is a desire to be notified of updates.

Step 5: Now, click Next.

Step 6:
Alternatively, if this information is to be entered later, select **Register Later** and then click Next.
Step 7:
Verify the configuration for IP Server. If you want to change the configuration, then make changes, and click Next.

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

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

**Version:** The current version of the software.

**SQL Server Location:** This is the location or IP address of the database server. ‘Localhost’ indicates that the database and Microsoft SQL server are local to the host computer.

An IP address in this field indicates the Microsoft SQL Server is located on another computer.

To test the connection, click **Test DB**. Click **Advanced** to modify the database connection string values: Database Name, IP Address, SQL Server User ID and Password.
**Video Data Storage Path:** This is the location where all the recorded video will be saved. The default is the local OS drive (i.e., C). The video folder is created automatically once server configuration is completed. 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 with write permission to that share or recordings will not be saved.

**Step 8:**

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

Cameras, when initially added through this method, will be at their default values. Further customization will be required. Please refer to **Part C of Section 2**, below.

**Step 9:**

Click **OK**. Then IP Server will run as a service.
SECTION 2) VI MONITORPLUS CLIENT

The VI MonitorPlus client is installed automatically with either IP Server installation process, or by choosing to install the client itself.

The default is intended to provide the Administrator with a VI MonitorPlus client, easily accessible from the server.

After VI MonitorPlus Client is installed, it is ready to be initialized, then configured.

**Step 1:**
Open VI MonitorPlus Client by double-clicking the icon on the desktop.

**Step 2:**
Enter login credentials or accept the default login, and click **SUBMIT** to continue.

At least one server must be entered into the Server Setup prior to using VI MonitorPlus client.
Optional:
For additional connection option, Click Connection Type.

Part A) Manually Adding Additional Servers to VI MonitorPlus

To add a server manually, in the Connection Type, Select Multiple Servers

Enter the IP address or name of the server to connect to, and the port (4011 is the default to input here)

There are three possible outcomes testing a connection to an IP Server

- **Login Error:** The server is found but security is on.
  The server attempted to authenticate the login with the initial credentials used to login to VI MonitorPlus. The server default login is Administrator/blank for the password). You can still add the server. Then logout of VI MonitorPlus login again with the correct credentials. *This should not happen with a default installation where IP server is being installed for the first time.*

- **No Server Found:** Confirm that the IP address, server name, server port or any of the three are incorrect. Enter the correct values and then click Test again.
Server Found: The server is found and a successful connection was made using the current credentials (Administrator/blank). The server’s name is displayed in the Status field.

Part B) Adding more than one IP Server to VI MonitorPlus

In a large organization, it is possible to have upwards of 20 video surveillance servers across multiple locations. It is possible to add a lengthy list of servers at one time using the import feature. In order to accomplish this task, an exported list of servers is required prior to importation. The file format is “.LSL.”

For more information on creating an exported server list, please see Use Server Profiles, below.

Step 1:
In the System> Options and click Connections.

Step 2:
Select Import From Profile.

Step 3:
Enter the filename or click Browse to go to the location of the saved “.LSL” file.

Step 4:
Next, click OK.

Note: If the file is unreadable or not found an error will display.
If the import is successful the full list of servers will display in the Known Video Servers grid.
A popup window will indicate that VI MonitorPlus needs to be restarted for changes to take effect.

Client can be restarted by clicking the **Logout** icon on the upper left of the main dashboard.

**Login:**

Enter the credentials to login to the desired server(s) or click **Log in** to bypass the Login dialog box without any credentials.
SECTION 3)  ADMINISTRATION

Part 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, and allows access to a number of necessary administrative functions for the proper use of IP Server and various aspects of Troubleshooting.

The IPSM (IP Server Manager)

- Monitors the IP Server and presents visual status cues for each server
- Provides a Diagnostics version of the IP Server Manager for troubleshooting and system optimization
- Manages IP Server network connections
- Manages licensing and registration
- Manages Lightweight Directory Access Protocol (LDAP) and Active Directory configuration
- Options available in IPSM vary slightly depending on the installation type.

(1) ACCESSING IPSM

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

- Server is functioning properly; streaming video to clients, recording video and reporting to Health Monitor (if configured). While mousing over the icon in the taskbar, the IP Address of the server will appear.
- Server is stopped. No video recording or video streaming is occurring on the IP Server, or with IP Server software on the machine that this icon appears on.

IP Server can be configured, managed, and used to exit the application and see information about Video Insight by right-clicking on the IPSM icon

- To manage the IP Server service, configure and terminate 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

Managing service controls and configuring IP Server is done by right-clicking the IPSM icon in the Windows System Tray, then selecting Server Configuration.

![IP Server Manager](image)

The Service Controls Status field displays IP Server service status.

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

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

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.

Click a configuration button to perform other functions:

- **Options** – This allows for the configuration of options for IP Server specifically.
- **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.
(A) IPSM: OPTIONS

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

(1) **Auto Restart**

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

![Auto Restart Options dialog box]

To set an auto-restart schedule:

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

(2) **Delay Service**

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

Check the Enable Startup Delay box.

Select the startup delay time (in seconds).

Click OK.

(3) Options

In environments where both an Analog and an IP server are installed on the same server, and where bandwidth resources will likely be very highly utilized as a result, there is an option to restrict the Analog server’s bandwidth consumption.
Enabling this option will terminate communication between the Analog and the IP server. As a result, no live streaming or recording will be done by the IP server when the timeout threshold has been reached.

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

To set an analog video timeout:

- Check the Enable Analog Video Bandwidth Timeout box.
- Select the timeout in seconds.
- Click OK.
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. Only some messages may appear, depending on User level and Overall Server Configuration.

**C**  **IPSM: NETWORK OPTIONS**

Clicking **Network Options** will 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 modify 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, select the Advanced button.

A new window appears, allowing the administrator to select a specific IP address for public-facing (internal network facing) connectivity for the IP Server.

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

This feature was created for the purposes of avoiding licensing conflicts that might arise where multiple NICs are used in a system.

(A) IPSM: DIAGNOSTICS
Clicking **Diagnostics** brings up the Video Server Diagnostics interface.

This interface is used for troubleshooting any service related issues.

The IP Server service is stopped when Diagnostics is launched.

Server Settings can be configured within VI MonitorPlus, with exception to testing the SQL database connectivity, and altering the SQL database connectivity. Those two features are explained below.

<table>
<thead>
<tr>
<th><strong>Server name</strong></th>
<th>This field displays the server name previously entered. <em>It is not editable.</em> To change the name of the server, click <strong>Server Settings</strong> and configure in the left pane or from Server Properties.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP Address</strong></td>
<td>This field displays the server’s IP address and should not be changed.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>This field displays the port used by the VI MonitorPlus to get and set system information. This port is also referred to as the Command Channel Port. See <a href="#">list of ports</a> for more information on ports used by the software.</td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>This field displays the software version of the IP Server.</td>
</tr>
<tr>
<td><strong>Licenses</strong></td>
<td>This field displays the maximum number of cameras allocated to the serial number assigned to the server. Using only Video Insight Encoders, Advidia and / or Panasonic cameras on the system should reflect a value of zero due to there not being a need for annual</td>
</tr>
<tr>
<td>Used</td>
<td>Licensing for these items. Please speak to your Video Insight or Panasonic sales person for more details.</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>This field displays the number of cameras used that have taken away from the overall license value listed above. If using Panasonic, Video Insight or Advidia cameras/encoders, no license will be used or deducted if additional brands are used and licensed.</td>
<td></td>
</tr>
<tr>
<td>Available</td>
<td>This field displays the number of licenses available to add to the server.</td>
</tr>
<tr>
<td>Cameras</td>
<td>This section displays the cameras that are associated with the specific IP Server, including the Camera Name. The grid area of the Diagnostics interface is read-only and displays all cameras, the last video write-time, if it is recording and the time the last image was received, or the last time a live image was received from the camera.</td>
</tr>
<tr>
<td>Time of last write</td>
<td>This column displays the last time the camera’s images were recorded to a file. A time of 12:00:00 AM is indicative of a camera that is set to Recording Off or not recording due to a Motion-Only recording type.</td>
</tr>
<tr>
<td>Last image received</td>
<td>This column displays the last time the camera’s live images were streamed. A time of 12:00:00 AM is indicative of a camera that is offline. The camera could be offline for several reasons: incorrect credentials, network, bandwidth or the IP Server service not running. See the FAQ section for more information on why a camera could be offline.</td>
</tr>
</tbody>
</table>

**Note:** Remember to start the service when exiting the Diagnostics application.
SECTION 1  TESTING SQL CONNECTIVITY AND CHANGING THE SQL DATABASE LOCATION.

Two additional features for troubleshooting are available that are not available in VI MonitorPlus Client, by highlighting the Server Configuration in the left pane:

Click Test DB to test connectivity to the database.

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

Either the database did not respond, nor has an outdated version.” There are several reasons why the database test failed. See the online FAQs for possible reasons for and potential solutions to the failure.

Incorrect database information may be one cause of test failure. To update or confirm the information click Advanced.
Database: Enter the database name. The default database name is InsightEnt.

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

User ID: The default user ID for the InsightEnt database is “sa” 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.
Another troubleshooting option is a diagnostics version that can run the application without starting any cameras. This option does not consume any bandwidth, which might be useful if troubleshooting connectivity issues, or environments with heavy network latency due to a large number of cameras.

This version functions the same as the alternative System Log within VI MonitorPlus, with the exception that camera-related features and information such as Live View and Time of last write are not available after this diagnostics version is started.

Note: See IPSM Diagnostics for more information on running diagnostics.
(F) IPSM: UPDATE ACTIVATION

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

See Installation for more information on changing the activation type. Click OK to confirm the number of licenses currently available.

When you upgrade the license type from Express to Enterprise, Enterprise tab should be selected. Then click OK.

(G) 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, then, to make sure the license is valid, click Test.

After confirming the license as valid, click OK.
SECTION 4) ADVANCED INSTALLATION CONFIGURATION INFORMATION

Part 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.

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

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

Part B) Server Backup and Restore

IP Server can be backed up manually. It is important to note that the reinstallation of IP Server does require the same version of software for reinstallation from backup.

If slightly different version is used, there may be a minor error during the installation, which may involve 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 do any subsequent upgrades from that version to the current download in an effort to minimize any potential problems.

(1) BASIC IP SERVER BACKUP PROCESS

The IP Server can easily 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 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.mdf** and **InsightENT_Log.ldf** and replace the existing if they exist.
8. Locate saved files and double-click your 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**.

---

**Part C) Edge Recording**

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

Edge Recording, in release 6.3.7 is made available to be used as a temporary bridge between the immediate need to capture video footage in the event of a temporary IP server failure and the need to expand to a larger, full redundant failover system. It is compatible with Panasonic iPRO and Advidia Cameras only at the time of this publication.

**IMPORTANT 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, **YOU WILL LOSE ALL VIDEO RECORDING FOR NON-EDGE CAMERAS**, 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 has been 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 in the event of 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. But, in an effort 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 results with Failover Edge Recording.

---

**Example:**

In the event of a temporary power outage, it is common to supply UPS battery backups for all servers in a server room that supply power to the NVRs and mission critical computing devices. However, in order for Failover Edge Recording to be truly successful, it is necessary to ensure that the total power consumption of any network switch responsible for providing power to 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 a power outage, any camera that is provided power by use of a PoE switch will not provide Failover Edge Recording due to a lack of power to the switch. Thus, a lack of power to the 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 in order 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

---

**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.
(A) REQUIRED HARDWARE

For long-term successful deployment of Failover Edge Recording:

- An appropriately sized SD/SDHC/SDXC memory card to match recording storage needs
- Panasonic branded IP cameras running firmware v2.50 or better
  (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

(B) REQUIRED SOFTWARE

Prior to configuration of Failover Edge Recording:

- Video Insight’s IP Server running at software version 6.3.6.4 (or better)
- 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 better)
- 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 with the use of the IP Server.

(A) PART 1: CAMERA CONFIGURATION

<table>
<thead>
<tr>
<th>Camera Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>
Simply enter a username and password that will be used to access the camera. Be sure to remember this information as it will be critical for accessing the camera settings and features in the future.

Once the password has been set for the new administrative account, a confirmation message appears.

**PAUSE HERE. DO NOT REBOOT THE CAMERA**

Simply minimize the browser window for the IP camera at this time. It will be necessary to re-open the browser window in order to conduct confirmation of configuration and access between IP Server and Camera has been established.

**B) PART 2: IP SERVER CONFIGURATION**

Add camera through normal process, described in the installation process.

Once a camera is added, go to the camera properties and select the **Advanced** tab.

Select Enable Failover Edge Recording located on the bottom right-hand side of the screen
(C) PART 3: COMMUNICATION VERIFICATION

Verification of communication between IP Server and IP Camera

The process of verification is crucial to determining if the IP Server has successfully connected with the IP Camera in a manner that will provide the desired effect of Failover Edge Recording. Verifying this information during the setup process will help make troubleshooting easier in the event of an unlikely Edge Recording failure.

Once the IP Server has restarted, open the camera’s management interface within the browser window that was minimized at the end of Part 1, above and proceed with the following steps.

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:

Click on Save Now

Now, restart VI MonitorPlus AND Video Insight’s IP Server.

Note: Wait until IP server is up and running again before proceeding.
SD Memory card:

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

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

**Recording Stream 1:**
Will be set to **H.264 (1)** by default.  
It is possible to select one of the four available H.264 settings

*see notes below

**SD memory card information:** Format the installed SD Card

**see notes below

On this page, a way to determine if the IP Server has successfully connected to the IP Camera with Failover Edge Recording enabled is to verify that the **Save Trigger** (under Recording Stream 1) is greyed out and displays the phrase **Network failure**.

**Network failure should** appear, as displayed above, as successful confirmation of connectivity with the IP Camera and Failover Edge Recording.

If **Network Failure** **IS** visible... then simply reboot the camera by doing the following steps:

1. Select **Maintenance** (on the left)
2. Select Default reset tab
Find **Reboot** from the list of options presented and then select **Execute**.

(Reboot process takes approximately 2 minutes.)

Congratulations! You have successfully configured the camera to work with Failover Edge Recording!

**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 in order 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.

---

**Part D) Rules Manager**

**Rules Manager** was created to provide some 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 simply moving video files from one location to another for the purposes of server maintenance and long-term storage.

**RULE CREATION PROCESS CHEATSHEET**

**Basic Steps:**

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. After 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

Simply put, the steps listed above 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 suit.

If it is determined that there is more information needed on the specifics of what each item does in the Trigger Events and Action events sections, then please continue reading.

(1) BASIC CONCEPTS

The various concepts are explained below for ease of use.

(2) CREATING A RULE

To start the process of rule creation, it is best to open VI MonitorPlus and then select Administration in the 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 can be broken into four specific areas.

<table>
<thead>
<tr>
<th>Trigger Events</th>
<th>Action Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. After the new Trigger selection window appears, select the trigger desired for activation</td>
<td>1. After the new Action Events window opens, select the desired resulting action event.</td>
</tr>
<tr>
<td>2. Provide the necessary information for that trigger to become active</td>
<td>2. Provide the necessary information within the Action being used</td>
</tr>
<tr>
<td>3. Click OK</td>
<td>3. Click OK</td>
</tr>
<tr>
<td>4. Move to Action events section below the Trigger events section</td>
<td>4. Restart IP Server</td>
</tr>
<tr>
<td>5. Select Add Action</td>
<td>5. Test rule for verification</td>
</tr>
</tbody>
</table>

Four Properties of a Rule
- 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. It is recommended that it is named with a description. If connected to more than one IP server, verify the name of the server where the rule will be applied by using the drop-down menu to the right of the name.

<table>
<thead>
<tr>
<th>New Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Properties</td>
</tr>
<tr>
<td>Enable Rule</td>
</tr>
</tbody>
</table>

Enabling Rule

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

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.

Name

Give the rule a name that loosely describes its function.

Server

If using more than one IP Server, use the drop-down menu to select the server where the rule will apply.

(4) SCHEDULES

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

The default for all rules is to run at all times. This means that no schedule is necessary. In the event that there is not a need for an action to occur unless it is to occur at a specific time of day.

(A) SCHEDULE SETUP
When the Rules manager tool within VI MonitorPlus is opened, and the Add Schedule button is selected, a new pop-up window appears.

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 the proper use of the scheduled days. It may be necessary to create multiple schedules for events that overlap the 11:59pm to 12:00am threshold.
Selecting the appropriate number of times the rule will run is critical for long-term success of the rule.

Selecting **One Time** will cause the rule to work only once, and it will not be repeated again.

**Daily** causes the rule to run on the specified days, at the specific times selected.

**Weekly** causes the rule to run on a specific day, or specific days, once a week, at the time selected.

**Monthly** will run the rule only a single time, during the designated days and times within a one-month period.

After all of the necessary criteria is provided in the fields above, click on **OK**.

The schedule is now complete.

(B) **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 at all times may prove the rule to be ineffective, or result in an undesired effect.

**Note**: The only caveat to the schedule timer at this point in time is that it 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 action. Within VI MonitorPlus, Trigger Events occur as the direct result of something that has occurred. Once the event has occurred, it will be followed by an action that is designated below.

Trigger Events occur in the present moment, and give cause to a log event. They can be considered as the “IF” in an “If, Then” statement. (IF Trigger event occurs, THEN do this Action Event.)

To create a rule using the Rules Manager, the administrator should first consider what event it is that is occurring that needs to have an action follow it.

(A) TRIGGER EVENT SETUP

Next, determine whether the event needs to meet multiple criteria or if it requires only one event to occur prior to an action event. This is necessary to determine whether or not the Trigger event will work as desired with the Action Event that follows.

Examples:

Single Event (Any):

IF a Camera becomes unresponsive OR a specific user logs in to IP Server.

Multiple Events: (AND)

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

To keep things simple, it is suggested that the first rule created be as simple as possible. That way, it will be easier to determine if there is a problem down the line.

When only a single item acts as the trigger, select OR and the rules manager moves through each of the Rules generated subsequently after the first rule completes.

(B) TRIGGER EVENT OPTIONS
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.

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control Event</td>
<td>Trigger off of an Access Control Entry or Alarm</td>
</tr>
<tr>
<td>Alert Button</td>
<td>An alert button appears in the navigation tree</td>
</tr>
<tr>
<td>Analytics</td>
<td>Trigger off of a supported Camera’s Analytics</td>
</tr>
<tr>
<td>Camera Down</td>
<td>Trigger when a specific or all cameras stop responding</td>
</tr>
<tr>
<td>Digital Input</td>
<td>Trigger based on external input device *</td>
</tr>
<tr>
<td>License Plates</td>
<td>Trigger when a License Plate is found</td>
</tr>
<tr>
<td>SDK Input</td>
<td>Trigger based on receiving data from a TCP port *</td>
</tr>
<tr>
<td>User Login</td>
<td>Trigger when a user logs into the IP Server</td>
</tr>
<tr>
<td>Video Motion</td>
<td>Trigger when motion is detected on a specific camera *</td>
</tr>
<tr>
<td>Alert Button</td>
<td>Trigger when an alert button appears in the navigation tree</td>
</tr>
</tbody>
</table>

(C) TRIGGER EVENT DEFINITIONS

Before selecting the Trigger, which will result in an Action, the simple definition of each trigger is made available here.

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

* 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
When creating a Trigger Event for Access Control Events, the Administrator will give the Event a Reference Name. Select the door from the drop-down menu titled Door Name, and for alarm type, select from either Alarm or Entry for the options.

Analytics
Camera analytics are commonly used for camera “training” in areas that require enhanced security functionality. Cameras that have the ability to enhance their capabilities over time, while focused on a specific area of interest, can offer a variety of functions based on the available feature set provided from the camera’s hardware manufacturer. Please refer to the camera’s user guide from the manufacturer in order to determine the capabilities provided from analytic use. To use this action, “Capture VCA Event” in camera setup has to be enabled.

Digital Input
Some camera manufacturers provide cameras with the ability to enhance the performance and functionality of a camera with the use of Digital Input/output devices. This trigger is designed to enhance the capabilities of those cameras within VI MonitorPlus for a seamless number of possibilities. Most commonly, a microphone is used with a camera by way of the Digital Input/output for recording conversations within range of said device.
SDK Input
SDK input allows for the IP Server to interface with other software and hardware manufacturers who are connected to the same network with the IP Server. These SDK Input events indicate whether or not the IP Server is receiving the data from the connected SDK device/software. This is generally only used by software and hardware developers and for testing purposes.

Camera Down
The Camera Down trigger relies on multiple variables in order for it to be triggered. Most commonly, this trigger becomes active when a camera cannot be logged into by the IP Server, when it becomes unresponsive due to a network outage and is helpful in early detection of possible issues that might not be fully realized by the Administrator.

User Login
User Login is for notifications to groups of Admins or higher-access-level individuals who need to monitor a system for unusual access rights, or routine use of the IP server. When a User logs into the system, it is recorded into the IP Server system log files.
License Plates

License Plate Recognition (LPR) requires a reference name, Trigger Condition, License Group and Camera specification. Additionally, the option to notify a specific Group, individual or all users logged in to the IP Server System Logs.

Video Motion

Motion Event creation requires that a reference name is provided. Additionally, the option to choose a single camera or All Cameras is available. These motion events are recorded in the IP Server system logs and can be referenced there, or utilized by an Action Event.

---

(7) ACTION EVENTS

Action Events are the resulting operations that take place after a Trigger Event occurs. They are actions that will take place, based on the criteria selected in the Trigger Event.

Below is a list of Action events that are available for use. Not all action events will function with all trigger events. Please refer to the Functional Relationship Guide further below this section for a reference of which Trigger Event will function with an appropriate Action Event.

---

(A) ACTION DEFINITIONS

<table>
<thead>
<tr>
<th>Actionable Input</th>
<th>Description</th>
</tr>
</thead>
</table>

Copyright 2017 – Panasonic System Communications Company of North America

Last updated: Friday, October 06, 2017
<table>
<thead>
<tr>
<th>Action Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Door State</td>
<td>Change the state of the door</td>
</tr>
<tr>
<td>Digital Output</td>
<td>Send a digital output on a specific port</td>
</tr>
<tr>
<td>Execute a program</td>
<td>Send a program to a specific user running VI MonitorPlus to execute.</td>
</tr>
<tr>
<td>HTTP Command</td>
<td>Send an HTTP command to a specific device</td>
</tr>
<tr>
<td>Network Decoder</td>
<td>Switch network decoder to a video source</td>
</tr>
<tr>
<td>TCP Message</td>
<td>Send ASCII message to TCP socket</td>
</tr>
<tr>
<td>Email</td>
<td>Email a custom message</td>
</tr>
<tr>
<td>Email AVI clip</td>
<td>Email AVI file to a specific user</td>
</tr>
<tr>
<td>Email Flashback Image</td>
<td>Email Flashback image.</td>
</tr>
<tr>
<td>Email Snapshot</td>
<td>Email a snapshot of an image to a specific email address</td>
</tr>
<tr>
<td>Action Event Log</td>
<td>Create an action event for the Media Player</td>
</tr>
<tr>
<td>Alarm Window</td>
<td>Displays alarm window for client within Workspaces and Message Display</td>
</tr>
<tr>
<td>Audio Alert</td>
<td>Audio alert for a specified VI MonitorPlus Client</td>
</tr>
<tr>
<td>File Manipulation</td>
<td>Copy, Move or Delete files</td>
</tr>
<tr>
<td>Instant Replay</td>
<td>Pop up a 30-second review of recorded video on a specific camera</td>
</tr>
<tr>
<td><strong>Live Window</strong></td>
<td>Pop up window for displaying a live camera feed</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td><strong>Message instruction</strong></td>
<td>Message instruction for the VI MonitorPlus Client</td>
</tr>
<tr>
<td><strong>Move PTZ Camera</strong></td>
<td>Move a PTZ camera to a specific location.</td>
</tr>
<tr>
<td><strong>Record</strong></td>
<td>Set a recording type</td>
</tr>
<tr>
<td><strong>Record with Audio</strong></td>
<td>Create a video file with audio included</td>
</tr>
<tr>
<td><strong>Switch Audio</strong></td>
<td>Switch viewing field to a specific camera</td>
</tr>
<tr>
<td><strong>Switch Camera</strong></td>
<td>Switch VI MonitorPlus ’s main layout to a camera view</td>
</tr>
<tr>
<td><strong>Switch View</strong></td>
<td>Switch VI MonitorPlus ’s main view to a specific view</td>
</tr>
<tr>
<td><strong>Time Lapse Recording</strong></td>
<td>Create time-lapse recordings (very low frame rate)</td>
</tr>
<tr>
<td><strong>Monitor Points</strong></td>
<td>Mask / unmask monitor points</td>
</tr>
</tbody>
</table>

**B) ACTION EVENTS**

On the Rules Manager Rule Creation Page, the Actions section provides a large number of customizable actions that will take place AFTER a trigger is received. The only exception to this process is the time-lapse image control.

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 Setup

Add Action

The process of creating an Action comes after a Trigger Event is created. Simply click the **Add Action** button and a new window will appear.

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

Simply select the desired action to be taken.

Depending on the action, it will be necessary, in most instances, to provide additional information for that specific action in order for it to function.

When completed, click **OK**.
**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.

**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.

**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.
HTTP Command is designed to work with certain camera and hardware manufacturers in an effort 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 in order to modify the functional use of different portions of its internal software.

To use this Trigger Event, please refer to the manufacturer's administrative guide for proper commands as each may have its own format requirement unique to its capabilities.

This feature is being phased out at the time of publication.

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.
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 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 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 Snapshot is most commonly 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.
**Action Event Log** is most commonly 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.
**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 is 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.

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

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

**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.
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.

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.
Move PTZ Camera, once triggered, 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.

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

In the event that 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 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 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.

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.
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, in essence, 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.

Best Practices

Below are a few things to keep in mind when using the Rules Manager that will help assist any IP Server Administrator achieve 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 the problem can be resolved easily.

Document, Document, Document
When a rule is created, keep notes as to WHY the rule was created, WHAT 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 desire 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
(1) INTRODUCTION

The Video Insight 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 server.

For example, if there are five servers with one designated as a Failover, if one of the four stops writing information to the SQL database, the Failover Server will assume the role of the failed server 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.

This section describes an overview of the failover feature and how it operates.

(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.
- Shared SQL Database installation; see IP Server installation with an existing SQL installation. (http://www.video-insight.com/support/FAQ/sql-install-upgrade-connection-issues.php)
- At least one license and a serial number or activation key for each server.
(A) RECORDING DURING FAILOVER PROCESS

A recorded video by a failover server will not be moved to an active server after recovering a failed server if a failover server has its own storage. Thus, having the same hardware configuration is required since a server cluster feature is used. In case of using three servers or more, a shared storage is also recommended so that all recorded videos during failover can be shown also by VI MonitorPlus after recovering.
(5) ACTIVATION SEQUENCE OF A FAILOVER SERVER

The example below provides a basic display of the 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 of recorded video files which will not ever be accessible.

2) SQL Server data recovery – is not recovered if you do not use a shared SQL DB

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

3) A single failover server in a system

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

(6) TO DESIGNATE AN IP SERVER AS A FAILOVER SERVER:

Click Administration -> Servers on 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.

The image below shows the warning that appears if a server with existing cameras is selected as a Failover Server

During an IP Server failure, the transfer of the video recording functionality to the Failover Server will take approximately 5-10 minutes.

Upon recovery from the outage, Video files recorded on the Failover are not transferred to the original IP Server.

During the time that the main IP Server is down, the Failover Server can be accessed via VI MonitorPlus Client.
Once the Failover Server is accessed by VI MonitorPlus, the Failover server 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.
Chapter IV  VI MONITORPLUS

The VI MonitorPlus has three core functions; live monitoring, viewing past history, and to act as a centralized management point for configuring and optimization of all IP Servers connected to it.

SECTION 1) MENU BAR OPTIONS

The new VI MonitorPlus user interface has undergone some major redesign as a result of important feedback from our favorite clients, industry members, and test groups. As a result, VI MonitorPlus has been reshaped in order 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 (left).

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>This icon, when selected, provides the user with the Logout function.</td>
</tr>
<tr>
<td></td>
<td>This icon provides quick access to downloaded files, notifications, and recent changes made to the system.</td>
</tr>
<tr>
<td></td>
<td>This icon allows quick access to any currently configured rules, once they have been configured within Rules Manager.</td>
</tr>
</tbody>
</table>

SECTION 2) TAB: WORKSPACES

Workspace are individual pages, similar to modern browsers, that allow a user or administrator to customize viewing of live and/or recorded video.
**Part B) Manage**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Open</td>
<td>Using this option opens a previously saved Workspace within VI MonitorPlus</td>
</tr>
<tr>
<td>Save</td>
<td>will allow the user to arrange a series of camera views, and save the workspace for easy access at a later time.</td>
</tr>
</tbody>
</table>

---

**SECTION 3) LEFT HAND MENU ICONS**

**Part A) Servers**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Servers" /></td>
<td>Server View provides the Administrator with the capability to view all configured servers and their corresponding cameras in one convenient scrollable menu bar.</td>
</tr>
</tbody>
</table>

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, if any have been made.
- Expand the Server by selecting the Triangle on the left of the server name. This action will expand the area, displaying the names of all cameras associated and controlled by that specific server.
- Selecting a camera will display the recorded video, by date, for that camera. Where “View Recorded Video Files” has been activated in Application Controls, below.
- Selecting the date under the camera view will display all files for that specific 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 in order 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.

---

**Part 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. Single server environments will often show the Camera View by default.

**Note:** Typing a camera name directly into the search field will conduct a search for a known camera name.

---

**Part C) Views**

This option allows the User to see all available Views within each server. Clicking the view 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. To create a new View, follow the instructions in the Views section, below.

---

**Part D) Maps**

Copyright 2017 – Panasonic System Communications Company of North America

Last updated: Friday, October 06, 2017
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 area 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.

SECTION 4) LIVE VIDEO

After the server(s) have been added, the VI MonitorPlus application will display selected cameras in the left tree navigation menu under Servers.

To view Live Video, select a camera from the left panel 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 of the cameras attached to a particular IP Server.

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, a **Digital Zoom** can also be performed by use of the mouse wheel.

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 also does not affect recorded video.

---

**SECTION 5) RECORDED VIDEO**

**Part A) Recorded Video Playback**
Recorded video files can be viewed with the use of the playback bar at the bottom of the workspace screen as seen in the image below.

Selecting the blue icon in the bottom right-hand side of the screen reveals a timeline bar with the current date.

To move the timeline back to an earlier point in video recording, click and drag the blue and red timeline to an earlier point in the recording history. Use the Orange line as the meter for the point in time which is desired to begin viewing recorded video.

**Note:** Red spots on the timeline bar indicate motion detection. Blue spots on the timeline bar indicate video recording of motion that is available for playback.

---

**Part B) Exporting Recorded Video**

To select a period of time for exporting recorded video, click the Export Video button, located immediately to the right of the timeline bar.

[Export Video Clip Icon.]
A new window appears. Select the desired start time and end time.

Optional:

Show Time Stamp: This will embed the timestamp in to the exported video.

Include Watermark: This feature will create a watermark for verification purposes and embed it into the video to prevent video tampering.

Force Compatibility: This feature forces the exported video to download in MJPEG format.

Select a folder to download the file to when it is exported.

The default exported video is in AVI file format, commonly recognized by most operating systems.

Creating a Self-Running Executable file allows the user to create a password protected video for additional security precautions.

Selecting the orange bar in the middle of the timeline bar will also allow the user to visually select the first and last frames of the recorded video, to be exported.

Part C) Accessing Recorded Video

The ability to enable the legacy viewing structure for the fastest access to previously recorded video has been added again by popular demand. By default, this feature must be manually activated.

Select the Administration tab at the top of VI MonitorPlus

Next, select Options
Within the System Options find the General menu settings

On the right-hand side of the screen, under the Application Controls label, select Show Video File Folders

Restart the VI MonitorPlus application

Log back in to VI MonitorPlus.

The default view should now allow the user to select a specific camera and see the previously stored video recordings for each specific camera as seen on the left.

Part D) Multiplex Video

While exporting a clip, there is an option to keep all video in the appropriate layout during your clip. This is done by simply 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 particular view.
SECTION 6) TAB: MODULES

Part A) Access Control

(1) ACCESS VIEW

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 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.

(2) 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**
  
<table>
<thead>
<tr>
<th>Door</th>
<th>Camera</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Doors</td>
<td></td>
</tr>
</tbody>
</table>

**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. Also displayed 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 Entry**
  
<table>
<thead>
<tr>
<th>Name</th>
<th>Door</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>James Adler</td>
<td>Front Door</td>
<td>8/4/2017 3:21:13 PM</td>
</tr>
</tbody>
</table>

**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.

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**
  
  | Acmit | Schedule | Unlock | Lock | Lockdown |

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 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:** 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**

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**: 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**: 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:** 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 whether or not 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.

<table>
<thead>
<tr>
<th>Door/Device</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access denied - this card is n</td>
<td>Access granted</td>
</tr>
<tr>
<td>Access denied - this card is n</td>
<td>Door is closed</td>
</tr>
<tr>
<td>Door is closed</td>
<td>Door is closed</td>
</tr>
<tr>
<td>Door is closed</td>
<td>Access granted</td>
</tr>
</tbody>
</table>

**Door/Device:** A list of the specific device where an event has occurred.

<table>
<thead>
<tr>
<th>Time Entered</th>
</tr>
</thead>
<tbody>
<tr>
<td>08/07/2017 10:49:22 AM</td>
</tr>
<tr>
<td>08/07/2017 10:49:26 AM</td>
</tr>
<tr>
<td>08/07/2017 10:49:03 AM</td>
</tr>
<tr>
<td>08/07/2017 8:33:25 AM</td>
</tr>
<tr>
<td>08/07/2017 8:02:31 AM</td>
</tr>
<tr>
<td>08/04/2017 3:21:13 PM</td>
</tr>
<tr>
<td>08/04/2017 3:21:15 PM</td>
</tr>
<tr>
<td>08/04/2017 3:16:25 PM</td>
</tr>
<tr>
<td>08/04/2017 3:16:25 PM</td>
</tr>
</tbody>
</table>

**Time Entered:** Date and time of recorded event.

---

**Part B) Lane Viewer**
The Lane Viewer Configuration screen displays all the related settings to Lane Viewer, a function that works with Access Control servers.

Here, the ability to modify the Lane Viewer picture size (width, height and possible 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).

SECTION 7) TAB: SYSTEM

The System tab holds controls and 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 largely centered around visual enhancements and User-level personalization for the client interface.

Part 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 at this time. Panasonic USA 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

To register any qualified Panasonic Camera for H.265 Camera Licensing, simply click on H.265 Online Registration. A confirmation window will appear when completed. H.265 Manual Registration

For Manual Registration, select the H.265 Manual registration button and follow the steps required on a computer that has access to the Internet. Be sure to write down the code that is provided in order to ensure a successful registration.

Part B) Event Viewer Details
### Access Control Messages

<table>
<thead>
<tr>
<th>AccessAlarm</th>
<th>General notification that access has occurred or access has been attempted.</th>
</tr>
</thead>
<tbody>
<tr>
<td>AccessEntry</td>
<td>General notification that an entryway was opened or closed.</td>
</tr>
<tr>
<td>DoorAlarmed</td>
<td>Denotes that a door alarm was triggered for the time and date specified.</td>
</tr>
<tr>
<td></td>
<td>Please verify that the door is functioning properly.</td>
</tr>
<tr>
<td>DoorLockStatuss</td>
<td>Will signify if a door is locked or unlocked.</td>
</tr>
<tr>
<td>DoorState</td>
<td>Status of a door - on/off/connected/not connected.</td>
</tr>
</tbody>
</table>

### IP Server Event Messages

<table>
<thead>
<tr>
<th>CameraDown</th>
<th>IP Server is reporting that it does not have access to the camera specified.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Please check username, password and network connectivity issues.</td>
</tr>
<tr>
<td>CameraMotion</td>
<td>Notification of a motion event. Meaning, motion occurred within the field of</td>
</tr>
<tr>
<td></td>
<td>view on the camera that has been specified.</td>
</tr>
<tr>
<td>CameraRestored</td>
<td>IP Server reporting that it can now connect to the previously downed camera.</td>
</tr>
<tr>
<td>ClientMessage</td>
<td>A message was sent from one user to another user.</td>
</tr>
<tr>
<td>LiveWindow</td>
<td>Live window was activated by a user, or rule.</td>
</tr>
</tbody>
</table>

### IP Server Rules Manager output

<table>
<thead>
<tr>
<th>AlarmWindow</th>
<th>This will appear when there is a rule setup to trigger a pop-up window for access control.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ExecuteProgram</td>
<td>Within Rules Manager, if the option to execute an additional program outside of IP server is requested, this will appear within the logs.</td>
</tr>
<tr>
<td>InstantReplay</td>
<td>This represents a call by a logged in user to perform an instant replay task.</td>
</tr>
<tr>
<td>LPRAlarm</td>
<td>This item appears with the use and activation of LPR services.</td>
</tr>
<tr>
<td>MessageAlert</td>
<td>This indicates that a message alert pop-up was triggered and displayed.</td>
</tr>
<tr>
<td>SwitchToCamera</td>
<td>During the Tour feature, this indicates changing views between cameras.</td>
</tr>
<tr>
<td>SwitchToServer</td>
<td>This indicates that that specific server was selected from the main menu.</td>
</tr>
</tbody>
</table>
### 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 Wall

#### 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.

---

### Part 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.

<table>
<thead>
<tr>
<th>Time</th>
<th>Server</th>
<th>Log Type</th>
<th>Event</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-11-15</td>
<td>10:20:31</td>
<td>SystemLog</td>
<td>Date</td>
<td>06/06/2017</td>
</tr>
<tr>
<td>2017-11-15</td>
<td>10:20:31</td>
<td>SystemLog</td>
<td>Time</td>
<td>05:00:07</td>
</tr>
<tr>
<td>2017-11-15</td>
<td>10:20:31</td>
<td>SystemLog</td>
<td>Size</td>
<td>05:00:07</td>
</tr>
<tr>
<td>2017-11-15</td>
<td>10:20:31</td>
<td>SystemLog</td>
<td>Status</td>
<td>05:00:07</td>
</tr>
<tr>
<td>2017-11-15</td>
<td>10:20:31</td>
<td>SystemLog</td>
<td>Download</td>
<td>05:00:07</td>
</tr>
</tbody>
</table>

---

### Part D) Server Statistics

Server Statistics displays to the administrator 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.

---

Copyright 2017 – Panasonic System Communications Company of North America

Last updated: Friday, October 06, 2017
Overview 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.

Server Status 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.

Camera Status provides the Camera Name, IP Address, Server Name, Last Image Received, Last Image Written, Resolution, Frames, Frame Size, Bandwidth, Format and “camera MD” which answers the question “Was the camera modified?” with a Yes or a No.

Storage 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.

Availability 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.

Online Users 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.

Motion Events 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.

Edge Recording 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.

Part 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

Copyright 2017 – Panasonic System Communications Company of North America
Last updated: Friday, October 06, 2017
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.

(A) APPLICATION CONTROLS

Application controls Provides the user with the ability to turn on or off Exit Confirmations and Block warning messages, and provides the user with the ability to make video file folders available under each camera listed in the left-hand column under the server it is attached to.

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. This box is NOT check marked by default in v6.3 or later versions.

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.
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 Layout
- Show Server Name
- Show Camera Name

If Show Layout is not selected, this feature will not work. If you must select this button, then VI MonitorPlus must be closed and restarted for the result to occur each of these steps has been completed.

**Use Direct X display**

This forces the incorporation of the use of **Direct X** for control of certain video controller within the display for cameras that require **Direct X**.

Selecting Use Direct X will force VI MonitorPlus to manipulate cameras using a legacy direct X controller. Please see Microsoft’s Direct X support page for more information regarding Direct X and its requirements. It can be downloaded by following this url: [https://www.microsoft.com/en-us/download/details.aspx?id=35](https://www.microsoft.com/en-us/download/details.aspx?id=35)

---

**On Screen Controls**

On Screen controls is more specifically about the appearance of PTZ controls and how they are displayed within VI MonitorPlus.

**On Screen PTZ**

When selected, this feature enables PTZ controls while hovering over a PTZ camera.

The use of Direct X provides a pop-up window within the display that allows for 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**

Selecting this option will allow the user to use the camera’s digital zoom feature, if available. Unchecking this box will result in the absence of 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.

**Add a Server:**

Users and Administrators can add a new server by clicking on **Add New**

- A new window appears
- Enter the **IP Address** of the IP Server.
- Note: If necessary, change the Port number to reflect the **Command Port** of the IP Server. (Default is 4011)
- 1. Click on **Test**.
  - If the server has successfully connected, a confirmation window will appear.
  - If the server does not make a successful connection, please verify the IP Address of the server and the port number.

**Note:** Server 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, simply select the undesired server, and then click on **Remove**.

(A) **SPECIFY EACH SERVER**

Specify Each Server is the location where the Administrator or User will add, remove and view the properties of the server.
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 on **Browse** to find a previously configured profile. Click OK. And the profile will begin functioning at the next login.

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.

Any changes made to VI MonitorPlus will require an updated export of recent changes in order 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.

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.

---

**3) TOOLS**

The **Tools** tab allows some various changes such as facility map alarms settings, whether created clips have watermarks enabled, MJPEG is forced onto them, and XML and registry storage options.
(A) OPTIONS STORAGE

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.

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.

(B) FACILITY MAP ALARM

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.

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.

The administrator can elect 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.
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.

(A) **LIVE WINDOW**

**Live Window default values:**

- **Live Window always on top**
- **Show Camera Associations**
- **No other boxes are selected by default within this section.**

<table>
<thead>
<tr>
<th>Live Window</th>
<th>Block Live Window Pop-ups</th>
<th>Flash Red on Motion</th>
<th>Duration</th>
<th>Force Second Option</th>
<th>Allow user to lock down PTZ controls</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Live Window always on top</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Red outline on Live Window</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Show camera associations</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Pause main display when Live Window launches</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Live Window Always on top:**

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.

**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.

**Red Outline on Live Window**

Selecting this option results in the appearance of a red outline around any and all motion-sensitive cameras where the server or the camera is reporting motion within the designated video display.

**Show Camera Associations**

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**

This 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**

By selecting this option, the effect will result 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 reduce potential of oversight if not otherwise enabled.

**Allow user to lock down PTZ control:**

This is an option that enables the hierarchal 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](#)

**Force Record** Option:
The 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.

---

**B) 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.

---

**C) FACILITY MAP**

This feature enables the visible server name for each facility map that has been created.

---

**D) 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 values for these to 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 here 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.

(A) MOTION NOTIFICATION

This section applies specifically to Camera Motion Settings.

If enabled, and IP Server or camera determines that there is motion occurring, enabling this feature will cause a sound to play.

The option to choose a custom file is available, if desired.

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. The accepted file playback type is .WAV. No other file type has been tested.

(B) RULES AND ALARMS

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 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.

(6) STARTUP

(A) WORKSPACE CONFIGURATION

Workspace configuration allows the user to set some visual defaults for viewing live and recorded video.

The options made available here are:

- Start with video paused
- Hide Left Navigation panel on startup
- Start in full screen mode
- Start with expanded servers
- Start with expanded server groups
- Start 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, in order 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 check box 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:**
(Defaulterd 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, in an effort to reduce 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.

**B) LOGIN OPTIONS**

Login Options allows the User to elect to login automatically, or specific if the need to use an active directory login is required. *Note: Enabling Auto login is a security risk and should not be enabled without fully understanding the implications and potential results of that action.*

<table>
<thead>
<tr>
<th>Login Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable auto login</td>
</tr>
<tr>
<td>User Admin</td>
</tr>
<tr>
<td>Password ****</td>
</tr>
</tbody>
</table>

Copyright 2017 – Panasonic System Communications Company of North America
Last updated: Friday, October 06, 2017

116 | Page
(C) TOOLS LAUNCH ON STARTUP

Tools launch on Startup provides the options to:

- 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

(A) ADVANCED OPTIONS

Show camera name when taking a Snapshot.
This 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
This gives a visual display of 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.

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.

(A) CLIENT PERFORMANCE

These setting directly affect the client-side VI MonitorPlus plus. They do not have any effect on IP server itself, unless the client is being used on the IP Server itself. Selecting the desired Machine Performance will alter how the computer utilizes its processor.

Video Smoothing is relatively expensive for processors, and should only be used with machines that have significant computing resources.

Reducing frame rate capture can sometimes be desired where computers with lower end video cards might otherwise be overwhelmed.

The default setting is Never, and can be changed to suit the user’s preferences.

Selecting Always will give the user a slightly “choppy” view of the video being captured, but does not have any effect on the video recording itself. This is used to minimize bandwidth consumption and computing resources on older machines and 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.

(B) DEWARP PERFORMANCE

This feature has a direct impact on the IP Server performance when combined with 360 and 180-degree cameras that have de-warping capabilities. If the IP server does not utilize any cameras with de-warped images, this setting will have no effect.

If cameras with de-warping features are available, the user can determine if using higher framerates for viewing a steadier playback of live video is displayed, or if more processing power with a reduction in fluid playback is desired. This feature is completely optional and based on user preference and need.

(9) DIRECT CAMERA CONNECTION

In some very rare and advanced instances, it may be desired to have a direct connection to the cameras from a remote VI MonitorPlus on the local Network.

Direct Live Video Streaming Support (multicast) allows the user to select the cameras they wish to enable. It requires a registry key modification ON the specific machine that will be using VI MonitorPlus. It also requires that the camera itself to have the Multicast capability built into its firmware. (The configuration is in System → Options → Performance)

There are two locations that can alternately be modified within the system registry.

Important 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 to it for various intentional purposes depending on the needs required:

- 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
SECTION 8) 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.

Part A) Administration: Servers

All items under this tab will result in modification of the IP Server configuration.

(1) SETUP AND CONFIGURATION

Server Setup

<table>
<thead>
<tr>
<th>Server Setup</th>
</tr>
</thead>
<tbody>
<tr>
<td>To setup a new server within VI MonitorPlus, simply click on the + symbol, and a new screen will appear.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the information being requested</td>
</tr>
<tr>
<td>- IP Address</td>
</tr>
<tr>
<td>- Port Number (default port number is 4011)</td>
</tr>
</tbody>
</table>

Once the information requested has been provided, click the Test button. When successfully connected, the Status will change to the name of the server. Click that Add button, or if the incorrect IP address was provided, click on the Cancel Button and start again.

Once a server has been added to VI monitor through this means, it will appear in the main startup menu when logging in to VI MonitorPlus for the first time.
(A) SERVER CONFIGURATION

Server Configuration:
This section provides the Administrator with the ability to access 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

i. Server Identification

Server Identification
This section allows the administrator to alter the name of the server from the default name, view the version number of the IP Server that VI Monitor is connected to, and view the IP address of the IP server itself.
Only the name of the IP server can be modified in this section.

ii. Database Information

Database Information
This section allows the Administrator to test connectivity with the SQL database, as well as alter the database connectivity parameters.

iii. Video Storage

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.

(B) 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.

i. Licensing Information
This screen provides the Administrator with the following information:

- 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

ii. 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 a large number of cameras.

iii. Monitored Cameras
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.)

(C) 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

i. **Server Options**

The Server Options section give the administrator access to some of the security settings that enhance the overall purpose of having an NVR that can be locked down by feature.

Available options:

- **Enable Security**
- **Allow only one login per user**
- **Designate Server as a Failover Server**
- **Symantec Certificate Validation**
- **Enable System Log**
- **Use Proprietary Format for Server File Storage**
- **Increase number of days that logs are kept in the system**
ii. Record Options

Enable Binary Recording. Default is not checked.
This feature allows for the accessing of video being recorded on the fly. It is a feature that is very resource intensive, and should only be used in situations where consistent access to video and review of the video is needed.

Reserve space for other applications: Default 5GB
This feature allows the administrator to configure the maximum amount of space used on any attached storage device used by IP Server. This may not reflect the actual amount of disk space available to IP Server.

iii. Live Display Options

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 turned off. A recommended value is 20 minutes, so that after a 20-minute period passes that has no movement within web client, the user will be automatically logged out.

(D) 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 in order 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.

i. Online Health Monitor

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 inquiries to the Video Insight / Panasonic Sales department.

ii. Information to send to Health Monitor
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)

(E) 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.

i. **Client Support**

The term “Client Support” refers to the VI MonitorPlus software client.

In this section, the Administrator has the capability of enhancing security on the network by changing the default Data and Command ports from their default values (4010 for Data and 4011 for Command Port) to something that better suits the needs of the Admin.

The **Maximum Connections** field refers to the total number of VI MonitorPlus clients that will be allowed to access the IP Server itself. The default value is 64 connections, which is also the maximum recommended value. To increase security on the server, selecting a value that matches the exact number of personnel that have access to the server is recommended.

ii. **Outgoing Email**

This section is provided to the administrator so that the entry of an SMTP server and the required SMTP port number can be set. The default SMTP server port shown is 25, but
iii. SMTP Logon Information

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, the addition of Server Authentication and SSL encryption has been added.

iv. Send test Email

Once the Administrator has completed the SMTP mail server configuration, a test email can be sent in order to validate that everything is working as desired with SMTP. In the event that an email message is not received, verify that the outgoing email address is correct when sending a second test message. If problems continue to occur with receiving messages, then verify the account settings are correct.

(F) CONTACT INFORMATION

The Contact Information tab is for organizational purposes only. The information provided here is not parsed to any Video Insight affiliates, and is not sent to Health Monitor Cloud. This information is solely for internal documentation purposes of the license holder for IP Server, and is completely optional.

i. 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.
Here, the administrator can enter the following information:

- Server name
- Building
- Floor
- Room
- Phone
- Description
- City
- State
- Country

### ii. Contact Information

Also, not parsed to any outside organization, it is the contact information for the server.

Here, an 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. It is intended to allow you to easily define a variety of customized viewing possibilities with the available resources listed on multiple IP Server configurations.

This functionality aids in eliminating the hassle of sorting and grouping substantial amounts of data every 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 you have not configured VI MonitorPlus to work with multiple servers, please refer to the section above titled Logging In.

### (A) SERVER GROUPS
To create a server group, right-click on the Server Groups text, and then select Add Server Group.

Select the servers that you wish to form the group, and give the group an appropriate name.

The new Server group will appear in the Enterprise View window of VI MonitorPlus, as seen on the left.
(B) CAMERA GROUPS

To create a custom camera group, simply right click on the Camera Groups text and then select Add Camera Group.

Another pop-up window appears requiring your custom input.

All cameras connected to each IP Server will appear here.

This will require some knowledge of which cameras are being searched for specifically.

Add the desired cameras to the list, and give the new Camera Group an appropriate name for their intended purposes.

The new Camera Group will appear in Enterprise View under Camera Groups.

For creating 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, simply 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.
MAP GROUPS

The creation of Map Groups is similar to the above steps. Simply 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.

RULES

Users can add new rules by clicking on the + sign next to Rules in the left side menu.

For more detailed construction of Rules, please refer to the Supplemental Rules Manager Guide for a more expanded explanation of each of the rules and features available.

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, the enabling of Rules can be enabled, given a name and then assigned to a server.
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.

Users can set a schedule for the selected rule, choosing the days of the week, specific time and also frequency. When done, click on OK to save the changes.

If trying to add an event, the Add Event window will appear as it does, below.

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.

(A) 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.

(4) CONNECTION PROFILES
Connection Profiles allows Administrators to manage user profiles and servers based on the profile that has been created. They 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, users must click on ‘OK’ to create a new profile.

(A) HOST SERVER AND KNOWN CONNECTION PROFILES

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, simply click on Add Profile and provide the information being requested.

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.
Part B) Administration: Cameras

(1) CONFIGURATION PROPERTIES

(A) GENERAL

i. Camera Information

The menu displays a tree list with the active servers and their respective cameras.

This area displays the camera’s live video and some useful statistics below the image.

The live video can be paused during configuration by clicking on the Pause icon on the bottom right.

It is possible to update all the settings on the selected camera.

![Image of Camera Information](image)

The general tab shows basic information such as the camera’s name, manufacturer, model, IP address, and some motion, record and display settings.

The Advanced tab shows advanced settings, such as advanced recording, transcoding, quality, lens, high resolution association, and motion buffer options. The ability to enable the secondary stream for various supported cameras is also supported.

ii. Motion Settings

**Motion Zones** are areas created within the image that the camera monitors for motion. Motion Zones allow for more precise motion detection within captured video recordings. When combining Motion Zones with Motion-Only recording, the camera will ignore certain areas in its line-of-sight. A Motion Zone can be created in the Event Trigger Labels section.

*For example:* A user might have an outdoor camera set to record motion overlooking a playground with many trees. They only want the camera to record substantial movement, like that of vehicles, people or animals, and not when leaves move on a tree. A motion zone can be created in an area that is free of trees, focusing on real movement within the desired area.

To create a Motion Zone using VI MonitorPlus, select Administration → Cameras.

A new tab appears.
Choose the desired camera to configure motion zones with by dragging it into the workspace on the right-hand side of the screen.

Click on the Motion tab within the camera settings. On the right side of the screen, a box will be presented to allow the modification of Motion Settings for the camera.

Video Insight recommends the use of Camera side motion detection, if the camera is capable of measuring motion events.

Next, select Add/Edit Zones, and a new window appears.

Within the camera image, simply click and drag across the screen, to draw the first zone.

To use more than one zone, click Add New located at the bottom right hand side of the displayed camera image.

Next, drag across the displayed image to create a second zone.
An example of the creation of a second zone is on the left, in yellow

To change the sensitivity or the percentage of pixel change for a zone to report as motion, the options are found immediately below the displayed image.

To change the Event Trigger (percentage of pixel change in a recording for a motion zone) select the zone to be changed, and then alter the percentage number accordingly.

To change the Sensitivity for a zone, simply select the zone you wish to change and change the setting to reflect the desired value.

Once the desired values are found to be adequate for the intended purpose, click OK at the bottom right-hand side of the screen.

Note: While this feature is very useful for cameras with views that may have trees that move often, the reduction of sensitivity and event trigger values should be used.

For camera views with long range capture angles (such as a long hallway) it will be best to configure multiple zones for these types of recordings.

The zone that covers the farthest portion of the image (the end of the hallway, farthest from the camera) will use higher Event Trigger and Sensitivity values.

The midsection of the same shot will use values slightly lower than the zone used for the far end of the hallway.

The section closest to the camera can use the defaults, as this will show the greatest number of pixel changes with the least amount of movement necessary to trigger a motion event recording.
The Advanced tab gives the Administrator more control and access to camera specific options available within various camera models. Not all features in this tab are applicable to all camera manufacturers and models. If a feature appears to be greyed out, or not available for the specific model the administrator has added to the IP Server, then the setting will not allow the Administrator to make the changes.

i. **Image Rotation**

Image Rotation is the control available in many cameras to alter the appearance of how the image is displayed within VI MonitorPlus - based on how the camera is mounted on the wall, and whether or not an adjustment needs to be made.

1. **CORRIDOR VIEW**

Corridor view is unique to some cameras. Some manufacturers like Panasonic, Advidia, and a few others offer a multi-lens camera that allows a user to view a single image view of an entire hallway.

To enable Corridor view for your camera, select the check-box next to Corridor view to enable it. Next, click the Corridor Rotation drop-down menu and select the direction (Left or Right) for desired directional focal point. Select No Rotation if you do not wish for the focal point to move at all.

Once the desired camera direction is selected for Corridor view, click on Save, and select the next camera to enable.

ii. **Advanced Recording Options**

Advanced Recording options become available for specific camera makes and models designed to allow the administrator to customize the options listed. Many camera makes and models do not allow for the configuration of these settings.

A description of each of the four available features is made clear in the manual that is provided with the camera.
The four available features in this section are:

- Gain style
- Light Grabber
- Autogain
- Light Behavior

**Note:** The image displayed here does not show the feature that enables **EDGE recording** unless the specific camera model being configured has been tested and proven to work within VI MonitorPlus.

### iii. Secondary Stream

Secondary Stream is a feature that allows for a viewing of any camera that is configured and capable of offering more than a single video stream.

<table>
<thead>
<tr>
<th>Secondary Stream (Verify 2nd Stream is Enabled)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Dual Streaming</td>
</tr>
<tr>
<td>Capture Frame Rate</td>
</tr>
<tr>
<td>Resolution</td>
</tr>
<tr>
<td>Capture Quality</td>
</tr>
<tr>
<td>Capture Format</td>
</tr>
</tbody>
</table>

The view provided from this setting is dependent on the **Capture Frame Rate**, **Resolution**, **Capture Quality** and **Capture Format** that the camera may or may not be able to provide as a secondary stream.

This feature allows the availability of capturing a secondary recording stream.

In order to utilize this functionality, please refer to the Camera Manufacturer’s Product Manual that dual streaming capability is available and enabled within the camera. Selecting **Enable Dual Streaming** does not always activate the secondary streaming capability within the camera itself.

- **Capture Frame Rate:**
  
  This feature allows the administrator to increase or decrease the visible frame rate when viewing secondary streams from a camera.

- **Resolution:**
  
  This feature allows the administrator to change the visible resolution to a higher or lower quality-dependent on the needs of the Administrator or user.

- **Capture Quality:**
  
  This feature directly affects the recording value of the secondary stream provided by the camera.
iv. **Color Adjustments**

<table>
<thead>
<tr>
<th>RGB Color Adjustments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red</td>
</tr>
<tr>
<td>Green</td>
</tr>
<tr>
<td>Blue</td>
</tr>
</tbody>
</table>

*Color Adjustments* options become available for specific camera makes and models designed to allow the administrator to customize the options listed. Many camera makes and models do not allow for the configuration of these settings.

A description of each of the three available features is made clear in the manual provided with the camera, by the camera manufacturer. The three available options in this section are:
- Red
- Green
- Blue

**Note:** When these settings are greyed out, the feature is not available for modification within VI MonitorPlus due to limitations imposed by the camera manufacturer for that specific camera.

(C) **MAINTENANCE**

**Maintenance** To view the properties of a camera, or several cameras, drag all of the cameras to view into a workspace and then select the Info button. It will turn the information on for all cameras.
The **Maintenance** tab displays three main sections:

**Camera info (general)**
- Camera Name
- IP Address
- Firmware Version
- IDF/Switch
- Vendor
- Model
- Install Date
- Warranty Date
- Other Information

**Service Information**
- New Service Record
- Service History

**Contact information**
- Contact Name
- Contact Phone Number

---

**(D) 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 (approximately 8.29 megapixels), and UHD equals 7680 x 4320 (approximately 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 at this time.

<table>
<thead>
<tr>
<th>VI MonitorPlus</th>
<th>Web Client</th>
<th>Video Wall</th>
<th>VI Monitor for Mac</th>
<th>VI TV</th>
<th>VI Mobile iOS</th>
<th>VI Mobile Android</th>
</tr>
</thead>
<tbody>
<tr>
<td>Live</td>
<td>Yes</td>
<td>No (1)</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

---

Copyright 2017 – Panasonic System Communications Company of North America

Last updated: Friday, October 06, 2017
(A) CREATING a Template

Camera templates are used to create a set of camera properties that can be used to set-up new cameras.

Commonly, these are used while configuring cameras to prevent the need to adjust each camera individually.

To create a template, click Templates under Administration tab. Next, click the + icon next to Templates sub header.

Next, select Create a template from an existing camera or Create blank template.

The option to import from existing camera will copy all camera properties including model, record settings, motion settings and extended properties. The IP address will not be copied into the template, and should be supplied after applying the template to the desired camera.

If it is desired to start from a blank template and customizing specific settings, select Blank Template. Click OK to save the template and name.

Verify that all settings have been modified as desired and click Save to finish creating a template.

(B) EDITING / DELETING A TEMPLATE
To edit a template, select the desired template to edit and make the changes needed. Be sure to click Save to finalize the changes. To delete a template, right click on the left templates menu, and click Delete.

All cameras with that template assigned will continue to be assigned those properties.

To apply a template to a camera, click the camera desired by selecting Administration > Cameras from the main menu. Click on the specific camera from the left navigational tree.

Scroll to the General tab and locate the Templates section.
In this area, there are two options: Import settings from Template, or Export Camera to Template.

To apply an existing template to a camera, select Import Settings.

A short menu will display to allow for the selection of the desired Template from the list.

Click OK to continue.

The menu options will take a second to reload and a SAVE button will appear.

Ensure all the settings are applied successfully and make any last-minute changes before clicking SAVE to finish. Exporting Camera to Template setting will save all properties to a new template file. The template will be named the camera name within the Templates area.

To see which template is currently applied, or changes made, refer to the Service History field on the Maintenance tab.

---

(3) ADMINISTRATION: PANASONIC LICENSING

Video Insight’s licensing structure is simple: one camera requires one license. Our floating licenses means there is no need to tie a licensing seat, IP address or MAC address to a particular camera.

Copyright 2017 – Panasonic System Communications Company of North America

Last updated: Friday, October 06, 2017
Cameras offering multiple camera views only require one license. Separate video streams from the same camera do not require a separate license. Video Insight offers encoders, such as the VP16, that allow up to 16 analog cameras with only one license. Please contact us for more information on specific licensing requirements.

Note: Some cameras include a license for use with Video Insight / Panasonic USA’s software.

Before attempting to activate Panasonic Licensing, add any new Panasonic cameras to the system if they haven’t already been added. Once done with adding the new cameras, Restart IP Server.

To activate your Panasonic Cameras, click on:

Administration → Cameras → Panasonic Licensing.

A new window appears with the Panasonic Cameras that you are to have registered. The details listed for each Panasonic Camera are: Camera Name, Camera Model, Status. The cameras listed should have “Register by (date)” which tells you that activation has not yet been completed.

Once the information has been verified for each camera, and if the IP Server is able to reach the internet, click the button labeled Activate.

Cameras should update and now read “Registered.”

**Note:** Cameras that are not registered after 60 days will no longer display a live view within the software.

Restart VI MonitorPlus and IP Server.

If VI MonitorPlus does not have access to the internet, please take offline process.

---

**Part C) Administration: View 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.
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.

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.

**Part D) Administration: Maps**

This section provides information about managing Facility Maps.

There is a left menu similar to the previous section where the user can select a facility map or search for one.

However, this one differs as there are also several other menu entries that have the capability of being drag and dropped on the facility map *itself* as items, such as cameras, views, doors or alarms. Additional information regarding facility maps can be found in the **Facility Map** section, below.

---

**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 the building.

To view a Maps in VI MonitorPlus, click on Maps, found on the left navigation bar.

Opening a Map will replace the current workspace from the main view.

---

**Part E) Administration: Users & Groups**

To manage VI MonitorPlus operators and user groups, use the Users & Groups button on the menu toolbar. As seen in previous sections, a menu in the left side of the screen where the user can choose between active users (and in this case, also groups).

When a user is selected, the loaded user page appears as the image on the 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 resources (facility maps, views and rules) managed by the user.
**GROUPS** can also be assigned during the time of creation by selecting the Group in the checkbox on the right side of the screen.

Similar to selecting a user, a group can also be selected from the left menu.

In order to add a user or a group, the Administrator must click on the + sign next to Users or Groups in the left side menu.

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).

---

**(1) SETUP AND CONFIGURATION**

**(A) 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.

**(2) ADMINISTRATION: 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.
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.

Next, select the desired users for PTZ prioritization. Once the desired users have been selected, press OK.

In the event that the added users aren’t appearing in the correct order, select one user and change its location within the list by using the Up and Down arrows. (pictured below)

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.

Now, PTZ Prioritization is 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.
Chapter V  WEB CLIENT

The web client is a free thin client that allows you to access live and recorded video from any web browser. There is an optional Active X control that can be used when viewing the Web Client in Internet Explorer. The Web Client requires IIS v6.0 (or later) to be installed on the IP Server machine. For details on configuring the Web Client, please see the Administrative Guide.

SECTION 1) LOGGING IN

Access the Web Client using http://<SERVERIP>/videoinsight or the URL provided by IP Server Administrator, using the browser of your choice.

If security is enabled, it will be necessary to enter the User Name and Password.

**Note:** If Security is not enabled on the IP Server, then the Web Client will allow users to log in without any password using Administrator as the username.

Please refer to this video for instructions on how to enable security on the IP Server.

SECTION 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 camera names, expand the Server Name in the left tree.

When selecting a camera’s name in the left tree, the Web Client will only display the video of the cameras selected.

To view a single camera, click on the live image of the camera or click on the camera name in the left tree, the image from the camera you selected will display over the other cameras in the layout.
From this view it is possible to perform a digital zoom, move the camera (PTZ support cameras), take a snapshot from the live video, view the video in its true aspect ratio, or view recorded video.

### Part A) Camera Manipulation

#### (1) DIGITAL ZOOM

To perform a digital zoom, select the Digital Zoom button on the video toolbar and click and drag from left to right in your area of interest.

Drawing this zone will enlarge the area to full screen.

Snapshots can be taken of the zoomed image, but unlike VI MonitorPlus, it is not possible to move around in the zoomed image.

To view the full image once again, click the **Reset** button or double click to return back to full normal screen.

### SECTION 3) FACILITY MAPS

To view Facility Maps in the Web Client, click on the Map icon in the left tree. This will display your map(s).

Hover the mouse pointer over a camera name/icon to display the live video from that camera.
SECTION 4) LAYOUT DIRECTORY

If custom Views have been implemented on the IP Server, they can be viewed by clicking the **Layouts** button at the top of the left tree.

Similar, to the default **Enterprise View** that appears when at first login to the Web Client, clicking on a single camera 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.

SECTION 5) RECORDED VIDEO
To access recorded video in the Web Client, simply click on the camera image of the camera to display the timeline video of available recorded video.

Please 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.

Drag 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.

**Part 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, seen left.

*(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 your local media player, while saving will allow you to save and store the file for review at a later time.

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.

**Part B) Watermark Verification**

To verify a watermark for any clip created by the Web Client, follow these steps:

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 and make sure to place a checkmark in "Include Watermark" tic 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

8. A pop-up appears with verification (see above)

**SECTION 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.

SECTION 7) ACCESS CONTROL

Limited Access Control functionality is available via the Web Client and is easily accessed by selecting the custom layout that you created for the IP Server.

There are two primary ways to access the Access Control features in Web Client:

- View Camera Layout
- Facility Map – Door View

To use the View Layout method, select the view from the Layout Directory icon on the left panel (seen left).

To use the Facility Map – Door View, select a Facility Map on the left navigation panel by selecting the Maps icon (seen left).

Select the map you wish to launch. If configured in VI MonitorPlus, you will see a visual map of your facility with the doors connected in the correct locations. Hover over the door to see a live preview of the door.
To access the door controls, double-click the door icon on 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. Time period of temporary unlock is often customizable in your 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. The purpose of this box is to prevent an unintentional command from being executed on the device at the wrong time. Click OK on the dialog to continue the action.

New for Web Client 6.3 is the ability to alter access control settings for minor changes. To do so, simply select the Interface icon from the menu bar on the left side of the administrator’s control screen.

<table>
<thead>
<tr>
<th>Access Control</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Enables the interface that allows users to control access to restricted areas.</td>
<td></td>
</tr>
<tr>
<td>□ Disabled</td>
<td>□ Enabled</td>
</tr>
</tbody>
</table>

Next, three options appear as choices.
1) Disable Access Control features.
2) Enable Access Control features.
3) Grant access for Administrator level accounts only.

Once the desired choice is selected, be sure to click **Save** at the top of the screen.

**SECTION 8) ADMIN FEATURES**

New to v6.3 Web Client is the ability to 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.
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, simply select Admin located in the top right-hand side of the page.

Once the new page opens, you are presented with a number of options that will allow you to modify the server on various levels. Those options are described above, and within the following pages.
Part 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

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 your system, simply select the Add Manually button.

Next, a prompt appears requesting information regarding the specific camera to be added.

Once the information has been entered, select Add, and the camera will appear in the left column.

Select the camera, then click on the right arrow.

Finally, select Save.

IP server has now successfully added a camera through the web client.

(3) HEALTH MONITOR TAB

Copyright 2017 – Panasonic System Communications Company of North America

Last updated: Friday, October 06, 2017
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.

Within the Administration page, you 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 you to update specific information about a given IP Server. This information is to be updated by the Administrator and used as a guide to provide information that is useful only to you and your IP Server Administrators or IT Personnel.

Part B) Cameras

This page 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.
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.

Part 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.

After the initial naming and basic layout is completed, you can easily drag and drop cameras found on the left into the desired point on the layout View.

The number of options for viewing vary, based on the construction of the previously designed custom View layout.
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. 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.

---

### Part 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
This feature allows the Administrator user to control the icons available on the main page, once a user is logged in. It can be used to “force” a user to see a specific page at login, or hide a specific feature that is not desired for users to see.

(3) SEARCH

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 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 tick-boxes prevents these capabilities from being used or manipulated by non-administrative users.

(5) LOGIN

A new feature available as of v6.3 is the ability to force the HTTPS protocol for login. 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, creating a self-signed certificate is an option.

(6) EVENT NOTIFICATIONS
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, you can optimize the settings to limit the number of frames that your IP server sends through the Web Client view in an effort to minimize the impact on the outgoing Internet connection.

Best used for IP Server Admins that have the need to allow multiple people to connect to the IP Server, but have a somewhat limited bandwidth issue.

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.
SECTION 1) DOWNLOAD SETUP

Download the Public View Monitor Application by navigating to DownloadVI.com and downloading the latest version of Public View. Be sure to save it to an accessible location to be used to upload to the Server you will use to host public view.

<table>
<thead>
<tr>
<th>Name</th>
<th>Date modified</th>
<th>Type</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>PublicViewSetup</td>
<td>1/27/2016 9:53 AM</td>
<td>Application</td>
<td>54,760 KB</td>
</tr>
</tbody>
</table>

SECTION 2) INSTALLATION PROCESS

Once the file is saved and transferred it to the server that will be used to run Public View Monitor, double click the file to start the installation process.

Click Next on the Welcome Setup Wizard screen.

Select I Agree from the License Agreement page

Choose the Installation location.

The setup will install the application to the default location of C:\Program Files\VI Enterprise. This location should match the location of all IP Server installation files.

To change this location, click Browse. Click Next when completed.

Click Install to save the Public View Setup to the Start Menu.
Click **Finish** to complete the installation.

![Public View Setup](image)

**Part A) Setup**

Upon initial launch, you will need to configure database information. Public View Monitor can be integrated with your Video Insight system (Database Configuration), stand-alone configuration, or set up by file import configuration.

**STAND ALONE CONFIGURATION:**

This method allows the Public View Monitor to discover, attach, and display cameras independently of the Video Insight IP Server.

To begin, Click Auto Discovery to auto locate your cameras on your network, or manually add your camera by selecting the Manual Entry button. You can also import selected cameras from a Video Insight database on the network by choosing the Import button.

Once you have selected the cameras to view, click **Next** to choose a layout grid that will determine the order in which the cameras are visible. Once you have selected the appropriate layout, click **Finish**.

(1) **DATABASE METHOD:**
Note: Ensure all required ports are opened on the firewall and router if connecting outside of the network.

Enter in all required information for database configuration.

Enter the IP address of the server’s database you wish to locate the layouts for Public View Monitor form.

Once the database information is submitted, click **Load** and select your Public View Layout created that was in VI MonitorPlus.
(2) FILE IMPORT METHOD:

This method allows the Video Insight Administrator to create a simple configuration file that can be imported into Public View Monitor.

Anytime the client computer boots up or Public View Monitor is launched, it will go directly to the selected layout under the Public View Layouts.

Note: It is possible to install Public View Monitor on multiple machines and just change the SQL Server Location IP address to whichever server you want it to look at. One way that you are able to get all layouts from all locations is to share the SQL Database between all client computers. There may be some problems in getting the communication to work outside of the network, but for internal use, this method works well.

SECTION 3) 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.

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.

ACCESSING PUBLIC VIEW MONITOR

On the client computer, where public View will be used, be certain that the same installation files used during the server setup are utilized. Once the install is complete, locate the public view Monitor icon on the desktop.

Double click to run Public View Monitor application and observe the screen(s) that have been attached to it.

SECTION 4) PUBLIC VIEW OPTIONS:
Right clicking on the Public View Option will display a few different configuration options. These options are detailed in the table below.

<table>
<thead>
<tr>
<th>Setup and Configuration</th>
<th>Allows the user to enter Setup mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Options</td>
<td>This setting allows the user to display options to cycle layouts, and display headers.</td>
</tr>
<tr>
<td>Export Configuration</td>
<td>This setting allows the user to export the configuration file used for Public View Monitor. This file can be shared and used during the import file method of set up on separate client machines.</td>
</tr>
<tr>
<td>Full screen</td>
<td>When toggled, this setting is used to enter/exit full screen mode.</td>
</tr>
<tr>
<td>Restart</td>
<td>When used, the application will restart.</td>
</tr>
<tr>
<td>Exit</td>
<td>This setting is used to exit the application.</td>
</tr>
</tbody>
</table>
Chapter VII  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](http://www.youtube.com/user/videoinsighttv)

To download manuals and software available for use, please visit our Downloads: [http://www.downloadvi.com](http://www.downloadvi.com)

**SECTION 1) REMOTE SUPPORT**

If more personal assistance is required, one of our Technical Support representatives is available to assist 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](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.

**SECTION 2) CONTACT US**

**In Person**
800 Gessner, Suite 700  
Houston, Texas 77024

**Sales Department:** 713-621-9779

**Technical Support Hours:**
Monday – Friday 7:00 AM - 7:00 PM CST,  
Saturdays and Holidays: 10:00 AM - 2:00 PM CST

**Hours of Operation**
9:00 AM - 6:00 PM CST, Monday – Friday

**By Phone:** 713-621-9779

**By Fax:** 713-621-7281

**By Email:** [support@video-insight.com](mailto:support@video-insight.com)

**NOTE:** This information is made available for clients only in North America and the United States. For Support information outside of the United States, please contact your sales agent or vendor for more information.
### 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/](https://www.iana.org/)

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Name</th>
<th>Purpose for use of port</th>
<th>Outbound WAN traffic required?</th>
</tr>
</thead>
<tbody>
<tr>
<td>4010</td>
<td>Data Port</td>
<td>Sends live video streams from IP Server to VI MonitorPlus Client</td>
<td>No</td>
</tr>
<tr>
<td>4011</td>
<td>Command Port</td>
<td>To get and set system information by VI MonitorPlus Client</td>
<td>No</td>
</tr>
<tr>
<td>3010</td>
<td>Ovid Server</td>
<td>Communication between S2, IP Server and the Ovid Server for Video Insight and S2 Access Control Configuration</td>
<td>No</td>
</tr>
<tr>
<td>80</td>
<td>HTTP</td>
<td>IIS for serving the Web Client&lt;br&gt;Note: Some ISPs block port 80 access. Some may need to configure IIS to use a different port than default for internet access</td>
<td>No</td>
</tr>
<tr>
<td>2051</td>
<td>MonitorCast</td>
<td>Access control communication between Video Insight and MonitorCast</td>
<td>No</td>
</tr>
<tr>
<td>554</td>
<td>RTSP</td>
<td>Specific camera properties</td>
<td>No</td>
</tr>
<tr>
<td>21</td>
<td>FTP</td>
<td>Specific camera properties</td>
<td>No</td>
</tr>
<tr>
<td>11000</td>
<td>HealthMonitor</td>
<td>Communication between IP Server and Health Monitor</td>
<td>No</td>
</tr>
<tr>
<td>636</td>
<td>Active Directory SSL</td>
<td>Active Directory configured with Secure Socket Layer (SSL)</td>
<td>No</td>
</tr>
</tbody>
</table>
Active Directory configured without Secure Socket Layer (SSL)

TCP port used to receive data on Health Monitor Cloud, located at: http://www.healthmonitorcloud.com.

Port used for Point of Sale customized software integration

Appendix B: The Independent JPEG Group's JPEG Software Notice

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.

This file contains the following sections:

OVERVIEW General 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.
exmple.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 roughly 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 exactly 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.

Copyright 2017 – Panasonic System Communications Company of North America

Last updated: Friday, October 06, 2017
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.

Copyright 2017 – Panasonic System Communications Company of North America
Last updated: Friday, October 06, 2017
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.


(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 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

Some 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 the 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 simply 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.

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.
Enable Binary Recording, 128, See Record Options
Enable Cloud Based Health Monitor, 129
Enable Security, 128
Enable System Log, 128
**Event History:** Live Event Stream. See Access View
Event Notifications: Web Client, 165
Event Trigger: Motion Zones, 141; ref, 139
Event Type: EVENT VIEWER DETAILS, 106
Event Viewer Details. See System Tab
Examples, 18; Router configuration, 18
Execute Program: IP Server Rules Manager output, 108
Exit Confirmation: VI MonitorPlus, 111
export server data: VI MonitorPlus, 115
Exporting Recorded Video. See Recorded Video
Facility Map. See Live Display
Facility Map Alarm, 116; Launch Live Window, 116; Open Facility
Map, 116; **Play Sound**, 116
Facility Maps: Maps, 150, See; Web Client, 154
Failover Server: Web Client, 89
File Import Method: PUBLIC VIEW MONITOR, 170
General Settings: Web Client, 164
Google Chrome, 26
Groups: Users and Groups, 151
H.265, 24, 25, 145, 146
**H.265 Manual Registration, 106**
**H.265 Online Registration, 106**
Hardware / Software Requirements: VI MonitorPlus, 24
Health Monitor, 128
Health Monitor Tab: Web Client, 161
Hide Left Navigation panel on startup. See Workspace Configuration
High Speed Mode: Web Client, 157
Import From Profile: Configuration, 115
Increase number of days that logs are kept in the system., 128
Information to send to Health Monitor, 129
Information to Send to the Health Monitor: Health Monitor, 129
Initialization: IP Server, 33; VI Monitor, 33
Installation, 27, See IP Server Installation
Installation Process: Public View Monitor, 167
Instant Replay: IP Server Rules Manager output, 108
Interface: Web Client, 164
Internet Explorer, 26
Introduction, 9
IP Address: Networking, 49
IP Server, 14, 21; (1) INSTALLATION WITH AN EXISTING SQL DATABASE, 28, 30; Activate by Phone, 34; Installation, 28
IP Server and Accessory Software Installation: IP Server, 14
IP Server Event Messages, 107
IP Server Manager: (IPSM), 41
IP Server Manager (IPSM): Auto Restart, 44
IP Server Prerequisites, 14
IP Server Rules Manager output, 108
IPSM, 41, 42, 44, 47, 48, 53, 54, See IP Server Manager; functionality, 41; IP Server Manager, 41
ISAPI Extensions, 26
Lane Viewer: Access Control. See Modules
**Last Alarm:** Informational. See Access View
**Last Entry:** Informational. See Access View
Launch Facility Map on startup, 121, See Tools Launch on Startup
Launch Lane Viewer on startup, 121, See Tools Launch on Startup
Layout Configuration: Views, 148
Layouts. See VIEWS
License Agreement, 5
License Plate Recognition (LPR) related messages, 109
Licenses, 49
Licensing, 23, See System Tab
Licensing Information, 125
Live Display, 117, See Tools; Allow user to lock down PTZ control,
118; Flash Red on Motion, 117; Force Record, 118; Pause main
display when live window launches, 117; Red Outline on Live
Window, 117; Show Camera Associations, 117
Live Display Options, 128
Live Video, 97; Viewing, 96
**Live View.** See Access View; Visual Display. See Access View
Live Window, 117, See Live Display
Live Window Always on top, 117
LiveWindow: IP Server Event Messages, 108
Local and Wide Area Network, 17
Local Database, 16
**Lock.** See Access View
Logging In: Web Client, 153
Login Options. See Startup
LPREvent: License Plate Recognition (LPR) related messages, 109
Main Window: Configuration - VI MonitorPlus, 113
Manage. See Workspaces
Map Groups: creation, 134
Maps. See Facility Maps
Maximum Connections: VI MonitorPlus Client, 130
Message Alert: IP Server Rules Manager output, 108
Modules: Access Control and Plug-in s, 101
Monitored Cameras, 126, See Cameras
Motion Zone: Configuration, 139
Motion Zones, 139
Move camera up or down: Visual representation, 127
**Multi-Network Card Support:** Networking. See
Multiplex Video: Recorded Video, 100
Navigation: Web Client, 164
Network, 17; Network Options. See Networking; Web Client, 166
Network Configuration, 17
New Workspace. See Workspaces
**Note:** Error, 39; Reboot, 50; Shared Storage location, 36
Number of cameras: License Use, 126
On Screen Controls: General. See Options
On Screen PTZ, 113, See On Screen Controls
Online Health Monitor, 129
Options, 111; IPSM, 44, 45; Resource Groups. Resource Groups
Options Storage. See Tools
Other, 118
Outgoing Email, 130; SMTP Server Entry, 130
Panasonic Camera License Activation: Licensing, 23
Panasonic Licensing, 147
performance, 17
Performance, 122, See Options
Planning, 13
Playback, 122, See Startup
Prerequisites, 14; Active Directory, 14
Prolamin Server Rules Manager output, 108
PTZ: Live Video, 97
PTZ zoom window: Configuration, 113
Public View Monitor, 167
Public View Options: PUBLIC VIEW MONITOR, 170
Record Always: Recording, 20
Motion Only: Recording, 20
Record Options, 128
Recorded Video: Web Client, 155
Remote Support: VI Insight Support Resources, 172
Remove Server from List, 114
Requirements. See PreRequisites; Hardware, 24; Software, 24
Resource Groups, 132
Resources: VI MonitorPlus, 150
Rules: Configuration, 136
Rules Manager: Supplemental Rules Manager Guide, 136
RULES MANAGER, 21
Rules Manager Actions. See Live Display
Rules Setup, 137
Save. See Workspaces
Schedule. See Access View; Recording, 20
Search. See Left Side server options; Web Client, 165
Secondary Stream, 143
Self-Running Executable, 99
Send test Email, 130
Sending a test email: SMTP configuration, 131
Server Configuration, 125
Server Identification, 125
Server Information, 131; (not parsed), 131
Server limitation: Number of Cameras, 126
Server Options, 127
Server Performance Server, 122
Server Profile. See System Options, See Connections
Server Setup, 124
Server Statistics. See System
Server timeout: Web Client, 128
Server Timeout:
Servers, 124; Configuration, 124; Web Client, 161
Setup: PUBLIC VIEW MONITOR, 168
Shared Database, 16
Shared Database Environment: Advanced Configurations. See
Advanced Configurations
Show camera name when taking a Snapshot. See Playback
Show date when taking a Snapshot. See Playback
Show Event viewer on startup. See Tools Launch on Startup
Show Event Viewer on startup, 121
Show Layout: Configuration, 113
Show Video Folders: VI MonitorPlus, 111
SMTP Login Information: SMTP configuration, 130
SMTP Logon Information, 130
Software Components, 10
Software Suite: Installation Process, 27
Sort Cameras Automatically, 127
Specify each server, 115
SQL: Database, 51, See Database; Databases, 51
Stand Alone Configuration: PUBLIC VIEW MONITOR, 168
Start in full screen mode. See Workspace Configuration
Start View. See Workspace Configuration
Start with expanded server groups. See Workspace Configuration
Start with expanded servers. See Workspace Configuration
Startup, 119
Startup with video paused. See Workspace Configuration
Storage, 20; NAS, SAS Drives, 20
Support Information: Web Client, 162
SwitchToAudio: IP Server Rules Manager output, 109
SwitchToCamera: IP Server Rules Manager output, 108
SwitchToLayout: IP Server Rules Manager output, 109
SwitchToServer: IP Server Rules Manager output, 108
Symantec Certificate Validation, 128
System Log: IPSM, 47
System Overview, 9
System Tab, 106
Templates: Editing / Deleting a Template, 146
Time of last write: System Log, 50
Tools, 115, See Options; Facility Map Alarm, 116
Tools Launch on Startup. See Startup
Unlock. See Access View
Update Activation: IP Server, 54, See Activation, See Activation
Use Direct X display: Configuration, 113
Use Proprietary Format for Server File Storage, 128
Use Server Profile. See Connections
User Management, 151, See Post-Installation; Users and Groups, 151
Users & Groups: Configurations, 150
VI Mobile, 12
VI Monitor: Client, 37

Copyright 2017 – Panasonic System Communications Company of North America
Last updated: Friday, October 06, 2017

179 | Page
VI Monitor Client. See VI Monitor
VI MonitorPlus, 11
VI MonitorPlus Client Hardware requirements. See VI Monitor
VI MonitorPlus VI Monitor Plus Client Hardware requirements, 24
Video Display: Web Client, 164
VIDEO Insight Support Resources, 172
Video Storage, 125
Video Wall, 109
View Groups: creation, 134
Views: (Layouts), 96; Layouts, 96; Web Client. See Layouts
Watermark Verification: Web Client, 157

Web Client, 11, 15, 26, 152; .NET Framework, 26; ASP, 26; ASP.NET, 26; HTML5, 26; IIS, 26, 48; ISAPI Extensions, 26; ISAPI Filters, 26
Web Client System Requirements, 26
Wide Area Network: Networking, 17
Windows 10 Pro, Enterprise and Education, 14
Windows 7 Pro and Enterprise editions, 14
Windows 8 Pro and Enterprise editions, 14
Windows Server 2008 Enterprise, Standard and Web editions, 14
Windows Server 2008 R2, 14
Workspaces, 94