



## DV-IP Server Advanced Setup Guide





## Contents

Introduction to Networks	5
What is a Network?	6
Equipment and Protocols	7
Introduction	16
How this Manual has been Constructed	17
Features of the DV-IP Server	18
MPEG4 Compression	21
Installing the DV-IP Server	22
DV-IP Server Connections and LED's	22
Rear Panel Connection	22
Front Panel LED's	24
Unpacking the DV-IP Server	25
Safety Notes	25
Location	25
Servicing	26
Lightning Strike	26
Regulatory Notes FCC and DOC Information	26
CE Mark	26
Simple Installation	27
Tools Required	27
Recommended PC Specification	28
Step 1 Connecting the Rack Mounting Brackets	29
Step 2 Connecting Video Sources	30
Step 3 Connecting to the Network	30
Step 4 Connecting the Spot Monitor	30
Step 5 Connecting serial devices	31
Step 6 Termination Dip Switches	32
Step 7 Connecting Power	32
Step 7a Allocating an IP Address	33
Step 8 Locating the DHCP Allocated IP Address	35

Advanced Installation	36
Tools Required	36
Step 9 Looping Cameras	37
Step 10 Connecting Alarm Inputs	37
Step 11 Connecting Relays	40
Step 12 Connecting 485 Bus Devices	40
Step 13 Connecting Audio Equipment	41
Step 14 Connecting External Storage (JBOD / RAID)	41
Step 15 Setting and Enabling Passwords	44
Configuring the DV-IP Server	47
Web Page Icons	47
Accessing the Configuration Web Pages	48
Simple Configuration	49
How to Configure Global Parameters	49
How to Enable System Features	51
Advanced Alarm Features	53
How to Configure Camera Inputs	54
Advanced Camera Setup	59
Configuring the Network Settings of the DV-IP Server	61
How to Select and Enable Coaxial Telemetry	64
Telemetry Setup Page	65
How to Enable Serial Telemetry	66
Telemetry Setup Page	68
Supported Modems/TA's	68
How to Configure Matrix Control	69
Advanced Configuration	72
How to Adjust Camera Settings	72
How to Configure Variable Recording	72
RAM Disk	74
How to Enable Audio Recording	75
How to Configure the Video Inputs for VMD	77
Walk Test	85
How to Enable and Configure Alarms	84
How to Configure the Relay Connections	96
How to Configure Alarm Presets	97
How to Configure Connect/ Dial, FTP, SMS and Email on Alarm	98
How to Configure Connect/Dial on Alarm	98
How to Configure FTP Settings for Archiving Images	104
How to Configure SMS Text messaging	107
How to Configure Email Settings	111

How to Protect or Un-protect Images	113
How to Configure the Alarm Database	115
How to Configure an Alarm Schedule	116
How to Configure Text in Image Functionality	119
How to Enable and Configure the On-board Firewall	121
IP Address Range and Subnet	125
How to Enable System Logs	126
How to Enable and Configure Watermarking	127
How to Enable and Configure the Webcamera functionality	129
DV-IP Server Tools	133
Video Scope	133
Audio Trace	134
Relay Test Page	135
Watermarking	136
System Variable	136
Reset	137
Reviewing the DV-IP Server Logs	138
Connection Log	138
Anonymous FTP Log	139
Security Log	139
E-mail Log	140
Sent Message Log	141
FTP Download Log	141
Logfile	141
Logfile Backup	142
Appendix A - Resetting the DV-IP Server	143
Reset using Telnet	143
Appendix B – DV-IP Server .ini Files	144
Updating the Bootloader	145
Editing the ini Files using FTP Client Application	145
Structure of the Files	148
hosts	148
modems.ini	148
paths.ini	149
USER.ini	151
vidcfg.ini	151
WEBUSER.ini	153

Appendix C – Port Assignment on the DV-IP Server	154
Port Allocation	154
Appendix D – DV-IP Server Serial and Network Cables	156
DM RS232 Debug Cable (supplied)	156
Straight-through Network Cable	157
DM 485 Bus Cable (supplied)	158
Cross Over Network Cable	159
DM RS232 Null Modem Cable	160
Nokia 30 Cable	161
Appendix E – IP Address Range and Subnets	162
IP address and Subnet Masks	162
Classes of Networks	163
Class A	163
Class B	163
Class C	164
Calculating IP Address Range	165
Class A table	165
Class B table	166
Class C table	166
Appendix F – SMS Message Format	167
Command Format	167
SMS Commands	167
Callback	167
SMS Reports	168
Startup	168
Alarm	168
VMD	169
Camfail	170
Additional Information	171
Command Reference List	171

## Introduction to Networks

The following will give you an entry level introduction to protocols used with Ethernet networks, equipment that makes up the network and how these work together.

It should help you when installing the DV-IP Server within a Local Area Network (LAN), or Wide Area Network (WAN). First we will identify some of the terminology we will use in this section;

**Server** – This is used in many ways in networking, a central server where we retrieve and save all our documents, an e-mail server that receives all e-mails and then forwards them to the relevant recipient, or a video server that serves video (live and playback) onto a network so a single or multiple users can access it.

**Host** – Host are any device that is connected to a network via a Network Interface Card; e.g. printers, PC's, web cameras.

**Client Application** – This is the application that is used to receive and translate the information from the server, Microsoft Word, Internet Explorer, Dedicated Micros DV-IP Viewer software.

**Ethernet** – Ethernet is a network that allows multiple applications to share the same 'piece of string'. Ethernet is the largest installed network technology in the world.

**NIC** – Network Interface Card. This is the interface that enables a device to connect to the network. These are available for any network; Asynchronous Transfer Mode, token ring, Ethernet and can range in sophistication and speed (more capability more cost). The DV-IP Server has a 10/100Mbps auto-detecting NIC.

**LAN** – Local Area Network. A LAN has specific characteristics; there is a geographical limitation that means more often than not a LAN is within the same building, it is usually owned and managed by the Company and more commonly the speed (how quickly information is transmitted from one place to another) is 100Mbps +.

**WAN** – Wide Area Network. A WAN is a network that links two LAN's together. There are numerous WAN links available (ISDN, DSL) and are usually supplied by telecommunication providers. It is important to remember that the speeds of WAN links are usually much slower than the LAN, this can result in the video stream slowing down, and however the video quality will remain the same.

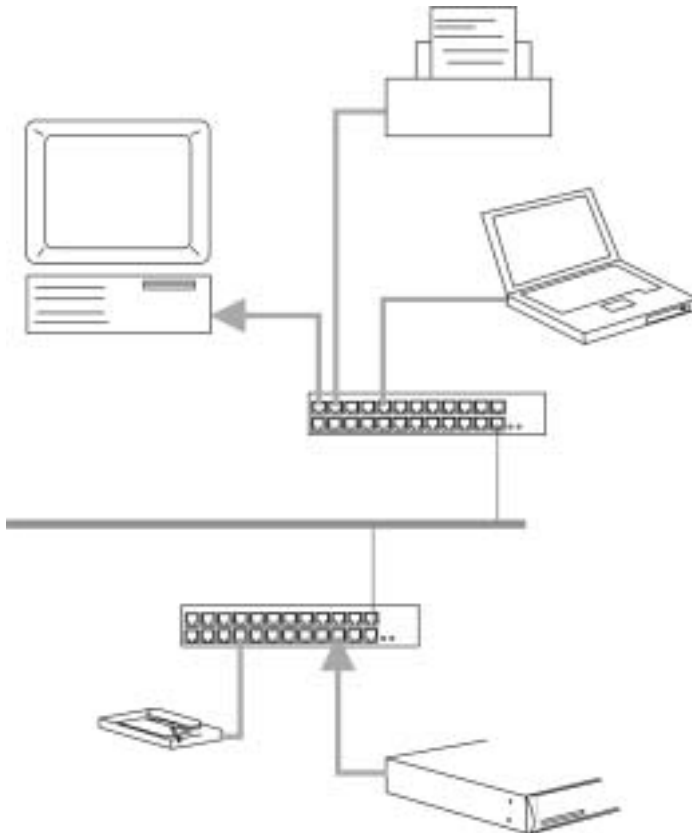
**VPN** – Virtual Private Network. A VPN is an alternative to transmitting information over a distance. These can be provided by Internet Service Providers and it acts as a tunnel through their network infrastructure to transport your data from one location to another. The link is private and secure and gives a seamless link, i.e. a virtual network that is part of your own network.

## What is a Network?

A network is a communication path allowing two or more devices to share/transmit data; e.g. telephone to telephone exchange, camera to matrix, server to host.

If we look at this in terms of the DV-IP System solution the devices are the DV-IP Server and the Client Applications, the communication path is the Ethernet network (LAN or WAN).

Today's networks have the capability to support multiple applications running across the same hardware and cabling infrastructure; IP telephony, Door Access, CCTV.



This is bringing the ability to have a single network for whole of the Building Management requirements; IT, Security, lighting and telephone systems, offering us a converged solution.

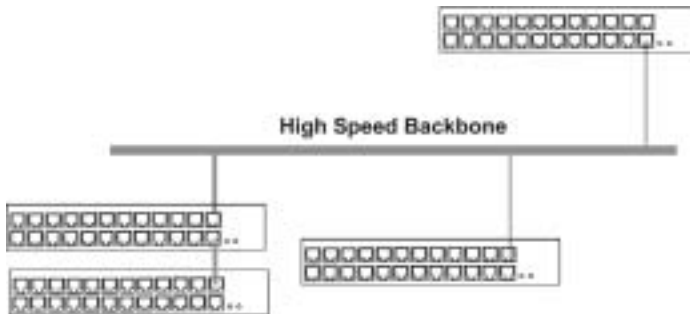
The DV-IP Server sits on an Ethernet network and allows video (Live and Recorded) to be transmitted across the network (LAN or WAN) for a single or multiple user to access. Therefore the rest of this section will detail the equipment and protocols within an Ethernet network.



## Equipment and Protocols

A network consists of hardware, cabling and protocols, the following describes the most common devices and protocols that you will be introduced to when installing a DV-IP Solution.

A network infrastructure generally consists of a high speed 'bus' backbone that connects to hardware to introduce a 'star' topology at the edge of the network.



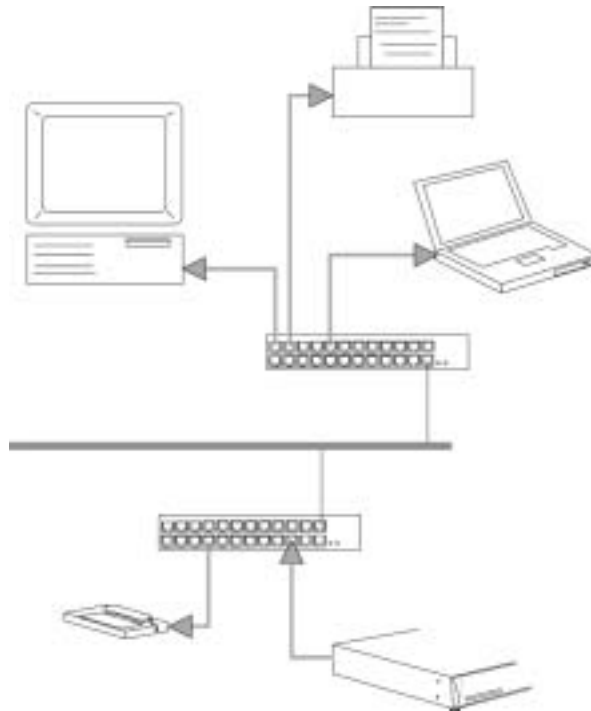
A bus network has the advantage of speed, i.e. no hardware to slow down the data being transmitted, but the disadvantage is the whole network is a point of failure. If a cable is cut the whole network will no longer function, and it is also very difficult to find the area on the cable that has the problem.

A star network introduces hardware, therefore reducing the point of failure to a single device. Identifying this failure is extremely easy and quick as there are software applications that run on these devices allowing for feedback on packet loss, usage (capacity), failure, etc. The disadvantage is the introduction of hardware adds time to the transmission of the information; however the advantages are far more significant.

A combination (described above) of bus and star gives speed at the centre of the network where it is required (route of most of the network data) while adding security and single points of failure with the introduction of hardware.

# Hub

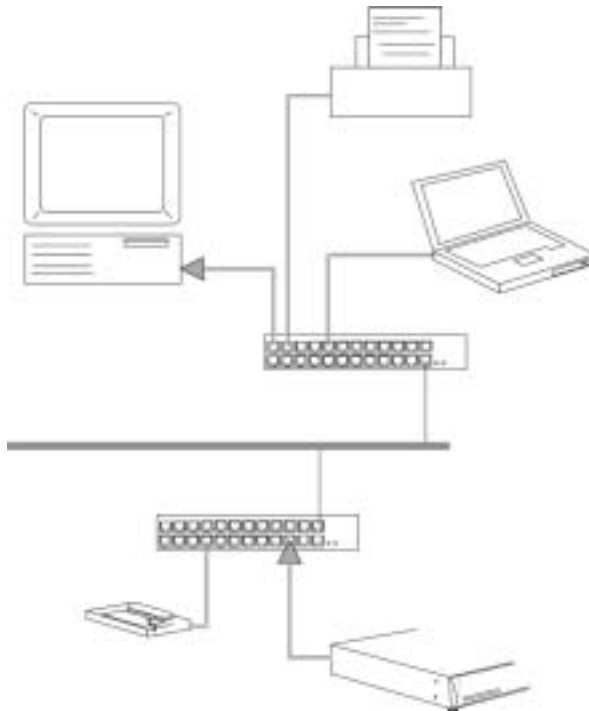
A hub is an unintelligent device and in simple terms acts as an electrical repeater, i.e. what comes in is re-amplified and transmitted onwards out of **every** port on the hub. The disadvantage of this is data is distributed to every host on the network even if they have not requested the data. This can have an affect on the efficiency of a network especially when transmitting large files such as video. Not recommended in real time (voice, video) application.



# Switch

There are many Ethernet switches available this section will not highlight any specific switches but explain how they work within a network.

A switch enables a star topology for a network. A switch is an intelligent device and uses information (that is found in the Header of the data being transmitted) to identify where the transmit host and the destination host is located on the network. From this information the switch will begin to build up information on its network.



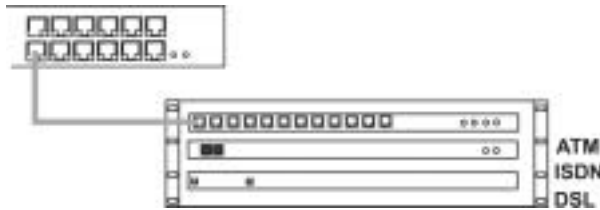
There are different types of Ethernet switches available and depending on the protocols you are using will depend which switch would be more appropriate.

Protocols such as UDP multicast would require a more sophisticated switch (Layer 3 Switch) that has the ability to analyse, in more detail, the information held in the packet Header and identify the IP address as well as the hardware address of the transmit host and destination host.

# Router

A Router or more commonly known as a 'Gateway' is the device that acts as a filter for transmission of information from one network to another.

The router looks at the data and identifies if it is for a host on the LAN or if it is to be transmitted across the WAN, what is the priority of the information (optimum path = high priority), is it time critical and what speed is it being transmitted.



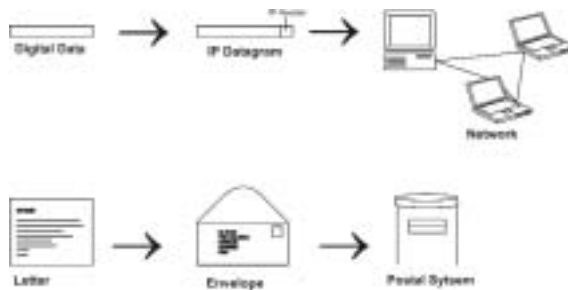
A router also has the capabilities of converting one medium to another, e.g. Ethernet to ISDN and buffers the data to slow high speed information transfer is successful over slower speed links, 10Mbps to 128kbps.

A simple router can have a single LAN and WAN connection, where more sophisticated routers have a LAN and multiple WAN connections (ISDN as a back up route, DSL, E1 as the main transmission paths) and will identify the optimum route for the data to be transmitted.

## IP Internet Protocol

The World Wide Web protocol, IP sits on top of the network hardware (described above) and is responsible for transmission of Ethernet (or other networks such as Token Ring) packets to be sent from host to host across the LANs, WANs and the WWW.

Any device connected to a network must have a unique address to identify who and where it is, this address is an IP address, see below for more information on IP Addresses.



The hardware in a network (switches and routers) use the information in the Header to identify the IP addresses of transmitter and destination host to ensure the information reaches the correct destination in a timely manner. The analogy above shows how the information that you transmit across the network can be associated with how we send a letter; the data is the letter, the IP packet is the addressed envelope and finally the network is the postal service taking the letter from the sorting office to our door.

## What is an IP address?

Every host that is connected to a network is allocated a unique address, an IP address. This ensures the network hardware can differentiate between hosts and ensures that data reaches the correct destination. The current network infrastructure's support IP V4 where a 32 bit address is allocated to each host in a decimal format, e.g. 192.168.3.6.

When assigning an IP address it is very important to assign the subnet mask of the network the host is connected to, e.g. 192.168.3.6, 255.255.255.0 (where 255.255.255.0 is the subnet) this gives additional information to the network hardware when routing data to the correct destination.

If you are connecting the DV-IP Server to a network then the unit must be allocated an IP address and subnet mask. If the video is to be transmitted via a router (Gateway) then the default gateway information must also be configured. You can obtain an IP address in two ways via automatic allocation; Dynamic Host Configuration Protocol (DHCP) or from the Network Administrator.

DHCP networks have a DHCP Server that receives a 'hand shake' from any host that is connected to the network, this will then search it's database for a free IP address and configure the host with this address. The disadvantage of this technique is that if the DV-IP Server loses power for any reason when it comes back on line it will request an IP address from the DHCP server; this address may not be the same as it was previously allocated. This could lead to a remote monitoring station not being able to connect to the DV-IP Server.



**Note:** Although the DV-IP Server supports DHCP it is recommended that a fixed IP address is allocated to the unit.

## DHCP Dynamic Host Control Protocol

This is a protocol for dynamically assigning IP addresses to hosts on the network. When a network is configured for DHCP this allows any host that is connected to the network to be automatically assigned an IP address from the DHCP Server. The advantage of this protocol is that it simplifies network administration; however if for any reason the host is disconnected or loses power then on re-connection a new IP address will be assigned.

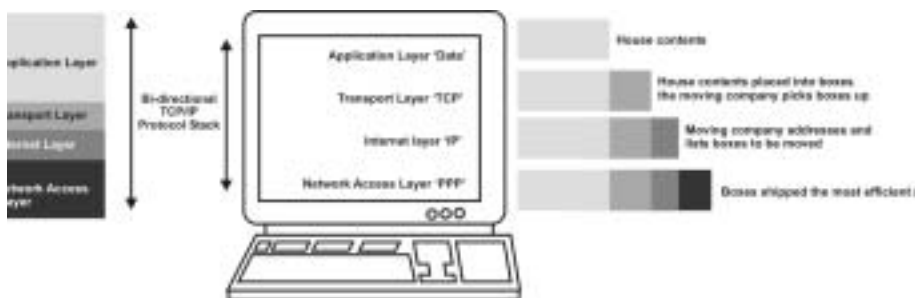
## TCP Transmission Control Protocol

We more commonly refer to this as TCP/IP however TCP is a protocol that sits on top of the IP protocol and adds reliability to the data being transmitted. TCP is a point to point protocol (one – to – one).

TCP is a secure protocol and adds error checking which checks to see if all the data is sent and received. There are many applications that sit under the TCP umbrella such as File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP – e-mail) where receipt of the information is very important but the time it may take to get that information is not as important; we don't care how long it takes as long as we get it.

The majority of networks will by default support TCP as this is the most commonly used protocol for transmission of data. The DV-IP Server uses TCP/IP for transmission of Video. The Network Administrator will have information on supported protocols on the network.

The diagram shows an analogy of how important it is to receive the information from and how TCP works; we are moving house and we have the contents of our house to move. We place the contents into boxes for the removal men to take, these are numbered and we have also identify the total number of boxes; Box 1 of 10 (TCP, error checking).



The company addresses the boxes (IP address) and then sends them by the most efficient route. If there is an accident then they may take a different route. When we get to our new house we look at the boxes and see if they are all there, if we find some missing then the removal company will speak to the Office and find out where they are and ask them to be sent again (TCP), finally we get all our boxes possibly not as fast as we would have expected but they are all there.

## UDP User Datagram Protocol

Not as commonly known as TCP, UDP can also sit on top of IP and offers great value to real time applications such as voice and video. These are time critical applications that are transmitting real time data. UDP does not have any error checking therefore removes any overhead required to perform this task which slows the transmission down, therefore ensuring the data is transmitted at real time, in the case of video 25pps.

UDP can be a point to point (unicast) or point to multi-point (multicast) protocol, the DV-IP Server uses UDP unicast protocol for the transmission of audio and telemetry control data.

You will need to check with the Network Administrator that the network supports the UDP protocol if you intend to implement audio and control data in your system.

## SMTP Simple Mail Transfer Protocol

This is the method of transmitting e-mails between servers. The DV-IP Server has the facility to transmit and e-mail to an SMTP Server for forwarding onto a Client application.

## FTP File Transfer Protocol

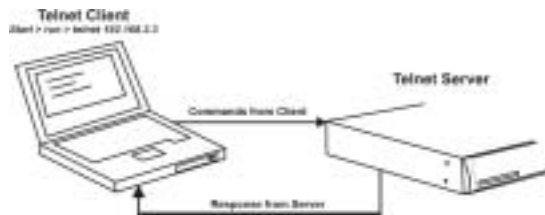
Part of the TCP/IP suite of protocols, FTP is a protocol for transferring data (files) from one location to another over the Internet. You are able to download files from FTP Servers; the DV-IP Server can send files using FTP to an FTP Server which will then send this on for notification of an event.

## HTTP Hyper Text Transfer Protocol

This is the underlying protocol used for the World Wide Web. HTTP defines how messages are formatted & transferred and what action the web server (browser) should take, i.e. typing the IP address of the DV-IP Server tells it to 'get' the information from the Server.

## Telnet – Terminal Network

This is a terminal emulation that allows a PC to be connected to a Server via the network. Commands can then be entered in the Telnet application on the PC for configuration, download of files, etc. The DV-IP Server supports Telnet communication and has usernames and passwords to protect from unauthorised users.



## ICMP Internet Control Message Protocol

The ICMP messages typically report errors in the processing of datagram's, this protocol has the ability to detect when datagram's (Ethernet packets) have not reached their destination and can send an error message giving details of the error. IP as a protocol is not reliable, however with the introduction of this (and other) protocol means that feedback can now be provided about problems in the communication environment, it does not make IP reliable but gives us information so we can act and resolve the problem. Usually used by Internet Managers.

## ARP Address Resolution Protocol

This is a network layer protocol and can be used to convert/relate an IP address to a physical address (hardware address of the host), this information is then stored within the DV-IP Server.

## DNS Domain Name Server (or Service, System)

This is a process that allows a unit to be allocated a Domain Name; this name can then be used when a client wants to connect to the server rather than entering the IP address of the Server. An example of this is how we connect to the World Wide Web; we do not enter the IP address of the web server but the Domain Name of the website we want to connect to, e.g. [www.dedicatedmicros.com](http://www.dedicatedmicros.com).

## How does DNS (Domain Name Server/Service/System) work?

The DV-IP Server, depending on the network configuration, can support DNS (Domain Name Server). It is possible to enter the Serial Number of the unit or the System Name (if this has been configured) to connect to the Server rather than having to remember the IP address of the unit. This could be very useful in applications where a single operator is monitoring multiple locations.



**Note:** The DNS functionality is not supported when the DV-IP Server is connected to a WINS (Windows Internet Naming Service) network, you would need to enter the IP address of the unit in this situation.

## Bits and Bytes

How do we identify the difference between a bit and a byte?

A bit is computer information that is transmitted across a network between network devices; it can have the value 1 or 0. When we talk about bits we add a speed reference to identify the number of bits that are transmitted within this time period, 512bits/s tells us that 512 bits are being transmitted every second.



In addition we have units of thousand (Kilo), million (Mega) and thousand million (Giga). When we write these terms we use the following:

- bps – bits per second
- kbps – kilobits per second
- Mbps – Megabits per second
- Gbps – Gigabits per second

We also refer to bandwidth in bits per second; a Gigabit Ethernet network has the properties to transmit thousand million bits per second, we say an ISDN link has a bandwidth of 64k, which means it has the property of 64kbps and can transfer 64000 bits per second.

A byte is a 'group' of bits, there are eight bits in every byte. We use the term byte to identify the files size or how much storage is required to save these files.

Again bytes come in multiples of thousand, million and thousand million; when we write these we use the following:

- B – Bytes
- kB – kilobytes
- MB – MegaBytes
- GB – GigaBytes

## Examples

If we had a 100kB file that is saved at 50kbps/s, we can calculate the time it would take for the information to be transferred:

100kBytes is equivalent 800000 bits (100k = 100000 x 8 – 8bits in each byte) being at 50000 (50 x 1000) bits per second.

Which means  $800000/50000 = 16$  seconds to transfer the information

Alternatively if we were streaming video at 512kbps/s for 60 seconds we would need;

$512000\text{bits} \times 60 = 30720\text{kbps}$  or information in total

$30720 / 8$  (8 bits in a byte) = 3840kBytes of storage would be required



**Note:** In networking terms the real value of a Kilo is 1024 rather than 1000. To get an accurate result you should use value 1024 for kilobits and kiloBytes

## Introduction

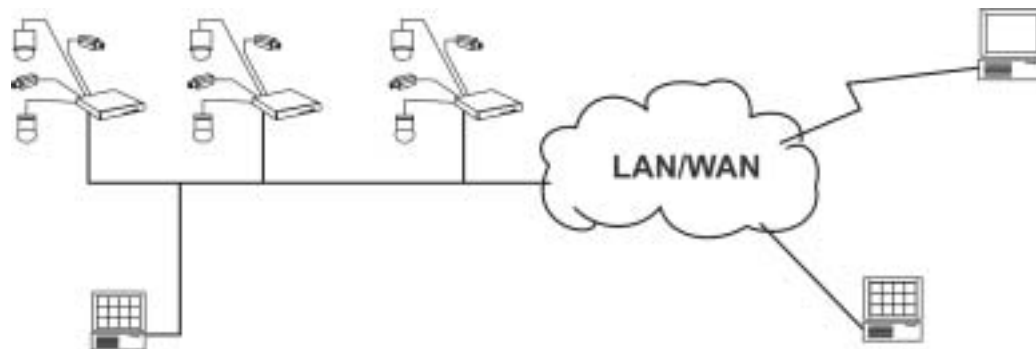
The Dedicated Micros DV-IP range has been designed to offer distributed monitoring and recording of multiple inputs. Combining advanced hardware technology with numerous sophisticated viewing applications makes the product range the ideal solution for many applications.

The DV-IP Video Server performs the task of a concentrator for analogue video, digitises, compresses, stores and distributes these signals across an Ethernet network infrastructure. Supporting alarm handling, on-board firewall for security, web configuration and monitoring, video motion detection and much more making the Server a fully featured solution.

Remote monitoring of any site can be achieved via the Internet or a more sophisticated viewing application can open up the extra features (remote alarm verification) supported on the Server.

Incorporating audio into the system allows a live bi-directional audio connection to be made between the Server and a Client application, as well as recording the audio along with the video on the Server hard drive.

The DV-IP Server is available as 6, 10 or 16 channel units, supporting JPEG and MPEG4 compression ensures high quality video performance is maintained, and with the modular codec architecture within the Server it is possible to achieve up to 120pps (NTSC) recording across all inputs.



The local recording achieved with the DV-IP Server removes the issues found in many applications where there are high bandwidth requirements for centralised recording. Supporting numerous network protocols (IP, TCP, UDP, DHCP, FTP, TELNET, ICMP, HTTP, ARP) the DV-IP Server is an ideal choice for a true converged network ensuring compatibility with new and existing network infrastructure's.

To further enhance the recording and monitoring capabilities external alarms and video motion detection can be built-in to the system configuration to enable event recording and (with an unlock code) remote alarm monitoring; an ideal scenario for Central Monitoring Stations.

The integration of numerous dome/PTZ protocols ensures that the DV-IP Server can be retrofitted into an existing system and offers no limitations for selecting compatible cameras when incorporating into a new installation.

One of the unique features of the DV-IP Server is the On-board firewall supporting IP filtering and TCP and UDP port allocation enhancing the security already achieved with the network firewall and ensuring the unit can not be targeted when connected to a public network.

## **How this Manual has been Constructed**

The DV-IP Server manual is divided into section to allow ease of installation and configuration. The system works in a two tier scenario; simple and advanced features. This allows the manual to follow the same format, therefore offering:

- **Simple installation**
- **Advanced installation**
- **Simple configuration**
- **Advanced configuration**

In addition there is reference material to assist with the advanced features, explaining how the function operates and the advantage of this to any installation.

The configuration section is designed to demonstrate typical scenarios and will guide you through the configuration for all aspects of that scenario; How to allocate and IP address, How to enable the Firewall feature, etc.

The operation and control of the System is detailed in the DV-IP Server User Guide.

First let's take a look at what the DV-IP System can offer you, what features can be enabled, what functionality the unit supports that you didn't know about.

# Features of the DV-IP Server

## What does the DV-IP System offer you?

Below is a list of the features that the DV-IP System supports, take a look at this and see which of these features is what your application needs, maybe this will highlight some features that you hadn't thought of but may be of value to the system you are installing, then using the How to....? documents select the scenario to configure the unit.

- **NetVu Connected**

The DV-IP Server is part of the NetVu Connected family of DVR's, Servers and software offered by Dedicated Micros. This allows the DV-IP Server to be easily integrated into any NetVu Connected system providing a system that can operate as a single unit or as part of a system providing central monitoring capabilities for numerous sites.

- **TransCoding Support**

The DV-IP Server supports the option to record and view JPEG video images alternatively it is possible to take the recorded JPEG and view this in MPEG4 format, this features ensures applications with bandwidth restrictions can still maintain the highest quality video recordings but transmit at much lower bit rates maintaining network efficiency.

- **Multi Compression Support**

The DV-IP Server supports the option to record and view JPEG video images or record JPEG but view MPEG4 images, this features ensures applications with bandwidth restrictions can still maintain the highest quality video recordings but transmit at much lower bit rates maintaining network efficiency.

- **Multi-camera Recording Server**

Up to 16 cameras can be digitally recorded simultaneously. Using JPEG video compression the high video quality is maintained.

- **Internal Hard disk for Local Storage**

The DV-IP Server can support up to 600GB of internal storage ensuring download of the video for archiving needs to occur less frequently – less man power for archiving.

- **Multi Site Video Distributor**

With the introduction of the Ethernet connection the DV-IP Server can distribute video to any location on the LAN or WAN.

- **Audio Control and Recording**

The integration of bi-directional audio means that potential situations can be diverted, help points can be incorporated into the overall solution.

Recording of the audio along side the video allows simultaneous playback showing and hearing what happened during the incident.

- **Multiple PTZ and Matrix Protocols**

Allows the DV-IP System to fit into any application, retrofit existing analogue systems; incorporate a network connection by adding a DV-IP Server. This ensures that nothing needs to be removed and discarded to achieve the functionality supported on the unit.

- **Local Spot Monitor Support**

The DV-IP Server supports a local spot monitor allowing any of the video inputs to be displayed on the monitor as part of a sequence, this can be used as a deterrent for potential criminals and can be placed in a strategic position to inform people that the area is monitored by a CCTV system.

- **Alarms and Relays**

Integration of all Building Management means a single interface for monitoring the area; door access alarm can trigger a camera to be recorded and transmitted to a monitoring station.

Relays can be used to automatically trigger devices; lift barriers, open doors again emphasises the possibilities of integration.

- **Web Interface for Viewing and Configuration**

No need to install dedicated software to connect to the Server, all configurations can be carried out with a common interface for ease of use. Viewing is dependant on the functionality required but simple viewing and control can be achieved via the web interface.

- **Demo pages**

Additional demo pages have been provided with the web interface demonstrating how the user can adapt the system to meet customers needs – DuoView, Multisite and Maps.

- **'Webcam' option**

Designed to offer the facility to enable video inputs on the DV-IP Server to transfer images to a web server allowing these images to be viewed over an Intranet or Internet.

- **Bandwidth restrictions client and server**

Where bandwidth limitations are a consideration then the DV-IP portfolio will ensure this limit is not exceeded. With the facility to configure both the DV-IP Server and the DV-IP Viewer software to prevent the problem occurring.

- **Support of Numerous Network Protocols**

Ensures the DV-IP Server can be incorporated into any network infrastructure without any disruption.

- **Integral Firewall**

Added security to ensure no unauthorised user can access the DV-IP Server when connected to the public network.....No way in!

- **FTP, SMTP**

Ability to transfer images to an FTP Server and E-mail server on receipt of alarm enhance the remote alarm support of the system

- **Telnet**

These protocols provide a route for Remote Alarm Monitoring, alarms received on the DV-IP Server which sends the message/file to notify the Central Monitoring Station of an incident.

- **Video Motion Detection**

Each video input can be enabled for VMD which can enhance the alarm support of the unit. No need to add a PIR, external VMD unit this sophisticated software VMD will ensure no incident goes un-noticed.

- **Multilingual Support**

The DV-IP Server supports many languages which ensures the product can be distributed anywhere in the world. The installation and configuration will be in the native tongue making the easy installation of the unit even easier.

- **MD5 Fingerprinting**

Making sure the video follows the Standards and can demonstrate that the evidence has not been tampered with.

- **Schedule Function**

Further enhance the remote monitoring feature, no need for Operator intervention for recording, alarms, etc. simply incorporate the Schedule function to set and unset these features.

## **MPEG4 Compression**

The DV-IP Server has been updated to include MPEG4 image transmission capabilities. This technology ensures that users over bandwidth constrained networks have the ability to view video in real time. Features are provided to ensure the user can configure the DV-IP Server's image resolution, bit rate and also how many pictures will be transmit. The DV-IP Server is truly a multi-tasking machine, able to simultaneously serve JPEG images across a LAN, transmit MPEG4 over a wide area connection, and record high quality JPEG images to disk.

# Installing the DV-IP Server

The Installation of the DV-IP Server can be carried out in simple steps as described in the Quick Start Guide; this section will elaborate on this information and the connectivity required for the Advanced features supported on the DV-IP Server.

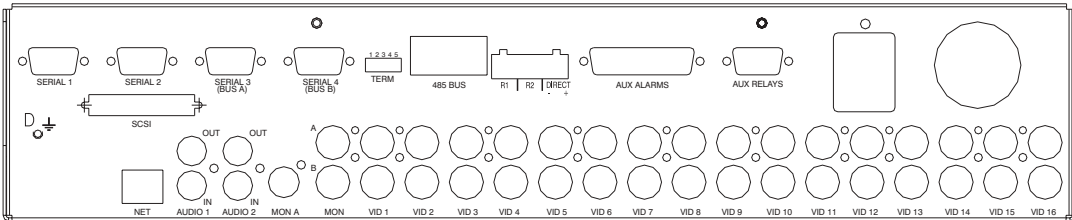
In addition to detailing the physical connectivity this section also describes some aspects of configuration that are required to be carried out at installation stage, these are all the serially configured parameters of the Server.

The installation of the DV-IP Server can be separated into:

- Simple installation - essential components required for the unit to operate
- Advanced installation - project based requirements such as alarms, external storage, and audio

## DV-IP Server Connections and LED's

### Rear Panel Connection



### Video

VID1 to VID16 75Ohms BNC composite camera connections, 1V pk-pk with loop through, DV-IP Server is available as a 6, 9 or 16 channel unit

### Monitor Output

- MON A Not currently used, available for future expansion
- MON B 75 Ohms BNC composite monitor output, 1V pk-pk
- MON A Not currently used available for future expansion



## Audio

Audio 1 IN	RCA (phono) socket, 8KHZ sampling 47KOhms input impedance
Audio 1 OUT	RCA (phono) socket
Audio 2 IN	Not currently used, available for future expansion
Audio 2 OUT	Not currently used, available for future expansion

## Data

SCSI	50 pin high density SCSI-2 connection
NET	RJ45 10/100BaseT Ethernet connection
485 BUS	2 x MMJ ports for DM 485-BUS accessories (additional alarm inputs / relays)
SERIAL 1 - 2	9 way (male) D Type RS-232 serial port (PPP, general purpose, debug, text in image)
SERIAL 3 - 4	9 way (male) D Type RS-232 (3 wire), RS-422, RS-485 serial port (Telemetry, debug, general purpose, text in image)
TERM	Dip switches for correct termination of SERIAL 3 and SERIAL 4 for RS422 and RS485 serial data

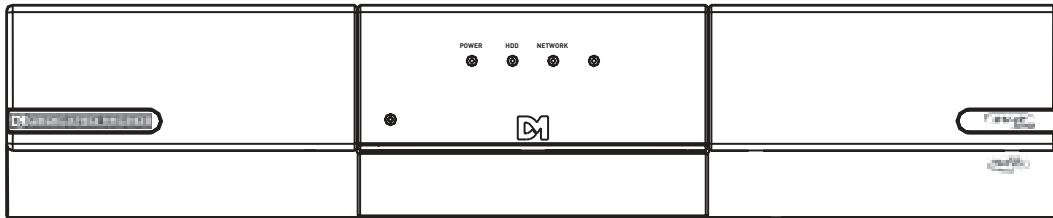
## Alarms and Relays

R1	Screw terminal, dry contact relay, NO/NC, user configurable
R2	Screw terminal, dry contact relay, NO/NC, user configurable
AUX RELAYS	9-way (female) D-type, user configurable
DIRECT	Screw terminal, direct auxiliary input, NO/NC
AUX ALARMS	25-way (female) D-type programmable alarms, NO/NC

## Power

POWER	Mains powered, internal power supply
-------	--------------------------------------

## Front Panel LED's



- |         |   |
|---------|---|
| Power   | The power LED will be green to indicate power is connected to the Server  |
| HDD     | <b>Hard Disk Drive</b> – this will flash when images are being stored to the hard disk                                      |
| Network | The Network LED will light when the unit is connected to the network, the LED will be off if there is no network connection |
| IR      | Not currently used available for future expansion   |

# Unpacking the DV-IP Server

Remove all the items from the packaging and check you have the items listed below.

- DV-IP Server
- External Power Supply and Power Leads – one US and one Generic (without a plug)
- CD ROM
- DV-IP Server Quick Start Guide - Supplied on the CD ROM
- DV-IP Server User Guide – Supplied on the CD ROM
- DV-IP Server Advanced Setup Guide - Supplied on the CD ROM
- RS232 Cross-over Communication cable
- RS485-bus cable with ferrite clamp filter
- Front and rear rack mounting brackets

If any of these items are missing please contact the Dedicated Micros Technical Support team.



**Important Note:** Before installing the DV-IP Server you must carefully read all Safety Instructions and the following information on where the unit should be located.

## Safety Notes

All the safety and operating instructions should be read before the unit is operated.

## Location

The DV-IP Server is designed to be rack or desk mounted. The following precautions must be taken when installing the unit:

- The rear supports must be used when rack mounting the unit, failure to use these may cause damage to the unit.
- If the unit is to be installed in a closed or multi-unit rack assembly, the maximum operating ambient temperature must not exceed 104°F (40°C).
- Ensure there is a 1" (2.54cm) gap on either side of the unit.
- Openings in the unit's case are provided for ventilation and to prevent overheating, these openings should not be blocked or covered.
- When stacking units, ensure there is at least a 1/2" (1.3 cm) gap between each unit.
- Ensure the unit is not located in an area where it is likely to be subjected to mechanical shocks.
- The unit should be located in an area with low humidity and a minimum of dust. Avoid places like damp basements or dusty hallways.
- Ensure there is reliable earthing of the mains outlet when fitted to supply connections other than direct connection to the branch circuit.
- When connecting the unit to a branch circuit this must be rated 15 Amps.
- If using external storage, refer to the relevant JBOD or RAID instructions for placement details.
- It is recommended that a UPS (Uninterruptible Power Supply) be connected to the unit in case of power failure, this will ensure continuous operation.

## Electrical Connections

Please ensure the following are available and have been tested prior to the installation:

Mains point

Network point

Network cable

Active video signals, that is, at least one working camera feed

Desk / Laptop PC with CD ROM drive and connection to the same network as the DV-IP Server

## Servicing

Do not attempt to service this unit yourself as opening or removing covers may expose you to dangerous voltage or other hazards.

Refer all servicing to qualified service personnel.

## Lightning Strike

The DV-IP Server has some in-built protection for lightening strike, however it is recommended that isolation transformers be fitted to the system in areas where lightening is a common occurrence.

## Regulatory Notes FCC and DOC Information

### (US and Canadian models Only)

**Warning:** This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at their own expense.

If necessary, the user should consult the dealer or an experienced radio/television technician for corrective action. The user may find the following booklet prepared by the Federal Communications Commission helpful: "How to Identify and Resolve Radio-TV Interference Problems".

This booklet is available from the US Government Printing Office, Washington, DC20402, Stock No. 004-000-00345-4.

This reminder is provided to call the CCTV system installer's attention to Art.

820-40 of the NEC that provides guidelines for proper grounding and, in particular, specifies that the cable ground shall be connected to the grounding system of the building, as close to the point of cable entry as practical.

## CE Mark



This product is marked with the CE symbol and indicates compliance with all applicable directives.

Directive 89/336/EEC.

A "Declaration of Conformity" is held at Dedicated Micros Ltd.,  
11 Oak Street, Swinton, Manchester M27 4FL.

## Simple Installation

Simple Installation is the minimum installation required for the DV-IP Server for the unit to operate; we will look at:

Installing the DV-IP Server into a Rack/Shelf

Connecting Analogue video sources

Connecting a Spot Monitor

Connecting the unit to the Network

Applying Power to the system

### Tools Required

The tools required to install the DV-IP Server to this stage are:

Item	Description
1	Suitable screw driver for or Allen key connecting the rack mounting kit and installing in the rack  <b>Note:</b> The rack screws are not supplied by Dedicated Micros.
2	Rack mounting brackets (supplied)
3	Laptop running a terminal application, for example HyperTerminal™, see below for full PC specification
4	RS232 cross-over communication cable (supplied)
5	Power Supply (supplied)
6	Mains cable (supplied)
7	Ethernet cable
8	Ethernet cross-over cable

## Recommended PC Specification

The following is the recommended PC specification to allow configuration and viewing of the DV-IP Server using a browser interface and also viewing and control from the NetVu ObserVer application:

	<b>Minimum</b>	<b>Recommended</b>
Operating System	Window XP Pro	Windows XP Pro
	Processor 1GHz Intel Pentium 3 or equivalent	2GHz Intel Pentium 4 or equivalent
System RAM	512MB	1024MB
Screen Resolution	800 x 600*	1024x 768 or higher*
Colour Depth	24bit*	24bit or 32bit*

Internet Explorer 6

Netscape Navigator 7.1

Firefox 1.5

Although the system will operate on lower specification computers the above is recommended to provide high performance video quality and update rates. If lower specification processors are used this will affect the overall performance of the computer.



**WARNING:** For a web browser to correctly operate with DV-IP Server, Java Virtual Machine (JVM) must be installed on each PC that will be used to access DV-IP Server. The JVM enables Java components in web pages to operate as intended by Dedicated Micros. A version of Java Virtual Machine may be downloaded from [www.java.com](http://www.java.com).

## Step 1 Connecting the Rack Mounting Brackets

Please note the DV-IP Server is heavy. Always follow health and safety guidelines when lifting the unit from the box or installing the DV-IP Server unit. When rack mounting the unit it is important that both the front and rear brackets are installed to correctly support the unit in the rack, failure to do this may result in damage of the unit.

A rack mounting kit is supplied with this product, it is important to install this correctly. The kit comprises of:

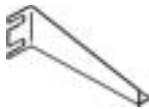
4 x Rack mount screws



2 x Front Rack mount ears



2 x Rear supports



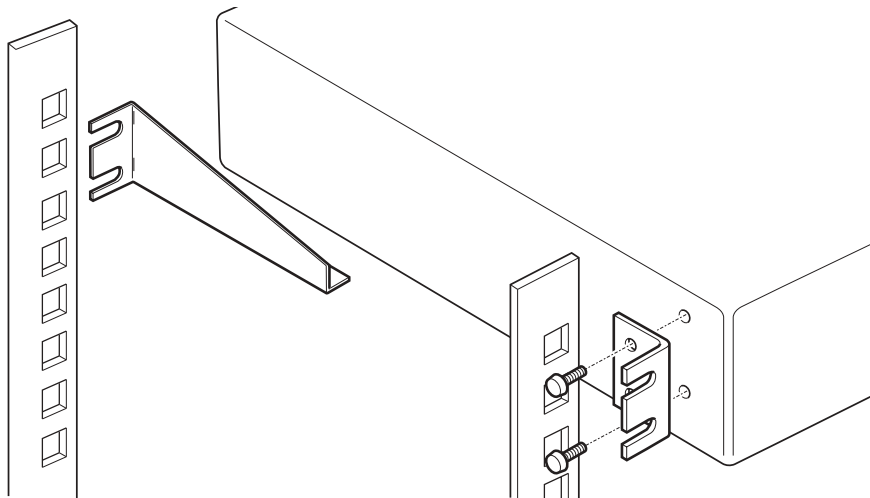
Before connecting any cables to the DV-IP Server connect the rack mounting kit:

Attach the rear supports to the rack that the DV-IP Server will sit in, these will support the weight of the unit.

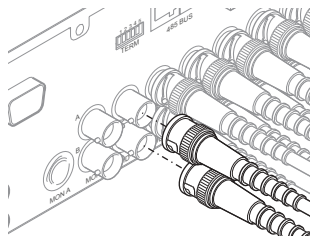
Using the supplied screws, attach the rack mount ears to each side of the unit.

Position the unit on the rear supports.

Attach the rack mount ears to the front of the rack.



## Step 2 Connecting Video Sources



The DV-IP Server is available as 4, 6, 10 or 16 channel units; the rear panel at the start of this section shows a 16 channel unit, the changes for the available units are the number of video inputs all other connections are the same.

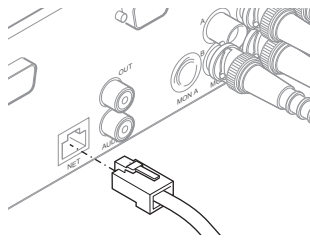
The Video inputs are 75 ohm BNC connector's and require a 1 Volt peak-to-peak video signal.

There are two rows of connector which provide video input and loop through support it is possible to connect the video input to either the top row or bottom row of BNC's. However it is important to ensure connection consistency for quality of installation by selecting one of the rows as the video input and the other as the loop through connection.



**Note:** It is recommended that you connect the cameras from the lowest number first; however it is possible to disable inputs in the DV-IP Server configuration pages.

## Step 3 Connecting to the Network



The DV-IP Server supports a 10/100Mbps auto detecting Ethernet Network Interface Card. The purpose of the network interface is to support the remote configuration, monitoring and control of the unit over a network connection.

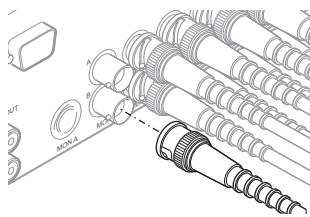
Using a straight through network cable (Appendix A) connect to the NET connector on the units and a port on the network.

The DV-IP Server is shipped enabled for DHCP network. An IP Address will automatically allocated when the unit is powered up.



**Note:** Although the DV-IP Server is automatically allocated and IP address it is recommended that a static IP address be configured on the unit.

## Step 4 Connecting the Spot monitor



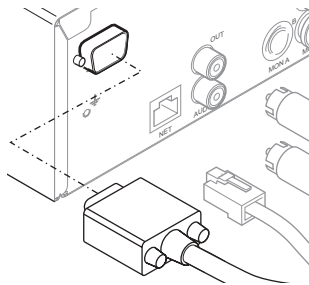
The DV-IP Server supports a Spot monitor (MON B) output which allows a single or a sequence of cameras to be displayed full screen.

This monitor output can be used as a deterrent to a potential criminal to show that the premises is being monitored, for example a point of sale monitor, Reception monitor.

The Spot monitor output is a 75 Ohm BNC connector.



## Step 5 Connecting serial devices



The DV-IP Server supports four serial (communication) ports. Each port can be configured to support various peripheral devices.

By default Serial 1 is the only port enabled and is set for Debug (Engineering mode) allowing you to connect and configure the unit.

All COM ports are 9 Way D-type connector's with the following pin connections for RS232, RS422 and RS485.

### RS422 Connectivity

Pin	SERIAL 3	SERIAL 4
1	Transmit Data (TX+)	Transmit Data (TX+)
4	Receive Data (RX-)	Receive Data (RX-)
6	Receive Data (RX+)	Receive Data (RX+)
9	Transmit Data (TX-)	Transmit Data (TX-)

### RS485 Connectivity

Pin	SERIAL 3	SERIAL 4
1	Transmit Data (TX+)	Transmit Data (TX+)
9	Transmit Data (TX-)	Transmit Data (TX-)

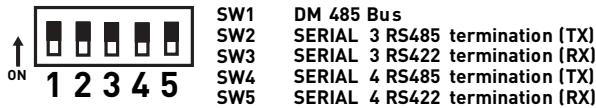
### RS232 Connectivity

Pin	Description	SERIAL 1	SERIAL 2	SERIAL 3	SERIAL 4
1	Data Carrier Detect	DCD	DCD		
2	Receive Data	RX	RX	RX	RX
3	Transmit Data	TX	TX	TX	TX
4	Data Terminal Ready	DTR	DTR		
5	Ground	GND	GND	GND	GND
6	Data Set Ready	DSR	DSR		
7	Ready to Send	RTS	RTS	RTS	RTS
8	Clear to Send	CTS	CTS	CTS	CTS
9	Ring Indicate	RI	RI		

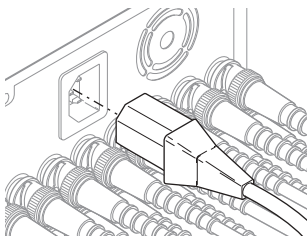
## Step 6 Termination Dip Switches

Part of the installation process for the communication ports is to ensure the termination is correctly set on each port.

The communication ports support RS232, RS422 or RS485 serial data. When connecting to RS422 or RS485 devices the corresponding DIP switches on the rear of the DV-IP Server must be set for termination, the following details the correct configuration.



## Step 7 Connecting Power



If there are no further installation requirements (audio, alarms, etc) you can connect power to the unit at this stage.

The DV-IP Server is configured for DHCP and will be automatically allocated and IP Address if connected to a DHCP network. If a static IP Address is required refer to Step 6a before applying power.

To connect power to the DV-IP Server:

1. The mains connector on the DV-IP Server is an 8 pin DIN connector. To power up the unit:
2. Ensure the mains is switched off at the socket
3. Connect the power supply (supplied in the packing kit) to the POWER connector on the unit; this is the 8 pin Din connector shown above
4. Connect the mains lead (supplied in the packing kit) to the power supply, the European lead requires the relevant mains plug be attached to the lead, ensure you follow Health and Safety procedures
5. Switch the mains on at the socket
6. Check the Green LED on the front panel of the DV-IP Server lights to show the unit has powered up successfully.

## Step 7a Allocating an IP Address

This section is separated into:

- Setting a static IP address
- Enabling DHCP

### Setting a static IP address

The following describes how a preferred static IP address can be allocated and divided into:

- static IP address
- subnet mask
- and if required default gateway

1. Ask your Network Administrator to complete the following with the information that will be configured on the DV-IP Server.

IP address

for example 172.16.0.100

Subnet mask

for example 255.255.0.0

Gateway  
(if required)

for example 172.16.0.254

2. With the mains power OFF, connect the PSU to the power input on the rear of the unit.
3. If the RS232 communication cable is not connected to the unit, connect this between the COM port on your PC and COM1 on the rear of the unit.
4. On your PC, from the **Start** menu, select **Programs> Accessories> Communications> HyperTerminal** and create a new connection using the COM port and the following settings:

Bits per second	38400
Data bits	8
Parity	None
Stop bits	1
Flow control	None

5. Apply mains power to the DV-IP Server. The green power LED should light on the front panel of the DV-IP Server and some debug information should appear in HyperTerminal as the DV-IP Server starts up, wait for this debug information to finish.

6. In HyperTerminal, log on to the DV-IP Server by typing **+++** and pressing enter.

7. At the **DV-IP>** command prompt, type the following commands, replacing <aaa.bbb.ccc.ddd> with the values issued by the Network Administrator.

**<ESC>** denotes the Escape button on your keyboard, **<ENTER>** denotes the enter key on your keyboard.

**<ESC>m\ether\_ip\aaa.bbb.ccc.ddd <ENTER>**

**<ESC>m\subnet\aaa.bbb.ccc.ddd <ENTER>**

**<ESC>m\gateway\aaa.bbb.ccc.ddd <ENTER>**

**<ESC>m\save <ENTER>**

**reset** (to restart the DV-IP Server) - you must reset the DV-IP Server for the settings to be applied.

### Enabling DHCP

The DV-IP Server is set for DHCP by default; the following details how to enable DHCP if this setting has been changed so that the DV-IP Server is automatically allocated an IP address:

1. With the mains power OFF, connect the PSU to the power input on the rear of the unit.

2. If the RS232 communication cable is not connected to the unit, connect this between the COM port on your PC and COM1 on the rear of the unit.

3. On your PC, from the **Start** menu, select **Programs> Accessories> Communications> HyperTerminal** and create a new connection using the COM port and the following settings:

Bits per second	38400
Data bits	8
Parity	None
Stop bits	1
Flow control	None

4. Apply mains power to the DV-IP Server. The green power LED should light on the front panel of the DV-IP Server and some debug information should appear in HyperTerminal as the DV-IP Server starts up, wait for this debug information to finish.

5. In HyperTerminal, log on to the DV-IP Server by typing **+++** and pressing enter.

6. At the **DV-IP>** command prompt, type the following commands, replacing <aaa.bbb.ccc.ddd> with the values issued by the Network Administrator.

<ESC> denotes the Escape button on your keyboard, <ENTER> denotes the enter key on your keyboard.

<ESC>m\ether\_ip\000.000.000.000 <ENTER>

<ESC>m\subnet\000.000.000.000 <ENTER>

<ESC>m\gateway\000.000.000.000<ENTER>

<ESC>m\save <ENTER>

**reset** (to restart the DV-IP Server) - you must reset the DV-IP Server for the settings to be applied.

The DV-IP Server will automatically be allocated an IP address from the DHCP server.

## Step 8 Locating the DHCP Allocated IP Address

If the unit has been left at default setting then the unit will be automatically allocated an IP address, it is important to find this information before the configuration of the unit can be carried out.

The DV-IP Server must be connected to the DHCP network during this procedure.



**Note:** Although this configuration provides an IP address for the DV-IP Server unit using the DHCP protocol, the IP address is only temporary, so it is advised that a permanent IP address is provided manually at a later date.

1. Connect to DV-IP Server using Hyper Terminal as described in Allocating and IP Address above.

2. At the DV-IP> prompt in HyperTerminal, run the IP configuration tool, type: **ipcfg<ENTER>** - the DHCP IP address assigned is displayed.

Make a note of the IP address for testing the network configuration.

IP address                     

for example 172.16.0.100

Subnet mask                     

for example 255.255.0.0

Gateway  
(if required)                     

for example 172.16.0.254

## Advanced Installation

The unit now has been installed for simple operation; the remaining installation would be applicable to the requirements of the projects.

The remaining installation covers the connectivity for:

Loop through

Alarms and Relays

485 bus devices

Audio devices

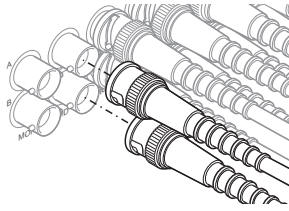
External Storage (JBOD / RAID)

### Tools Required

The tools required to carry out the remaining installation are as previously detailed plus:

Item	Description
9	485-bus cable with ferrite clamp filter (supplied)

## Step 9 Looping Cameras



The DV-IP Server supports loop through of all camera inputs, this allows the video source to be looped onto other pieces of equipment for example Monitors and Matrices.

Loop through connections can be connected to the top or bottom row of BNC connectors, for consistency ensure the connections are either one or the other not a mixture of both.



**Important Note:** Remember the last piece of equipment in line must be terminated.

If loop through is connected it is necessary to remove termination for the corresponding input on the DV-IP Server, this is achieved within the Configuration pages of the Server, *Refer to Configuring the DV-IP Server section of this manual.*

Double termination (not removing termination from the DV-IP Server) will result in the 1V peak to peak video signal being crushed. This can reduce the colour rendition of the video source and may cause the video signal not to be detected by the last piece of equipment, i.e. the signal is no longer 1V peak-to-peak.



**Terminated 75 ohm**

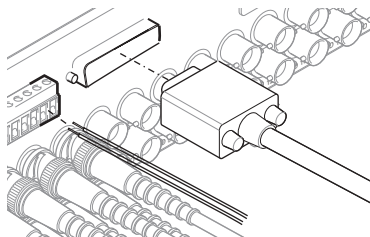


**Unterminated**



**Double terminated**

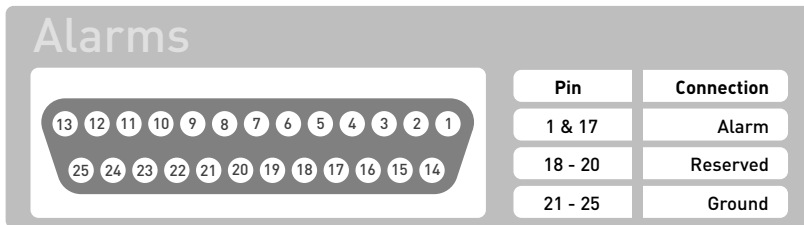
## Step 10 Connecting Alarm Inputs



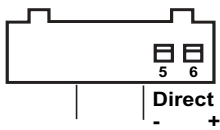
The DV-IP Server supports multiple alarm inputs allowing for third party devices to be connected to the unit to trigger alarms on the Server.

There are 18 on-board alarm connections. By default inputs 1 to 16 are configured to trigger event recording on cameras 1 to 16 of a sixteen channel unit.

The AUX ALARMS (alarms 1 to 17) are connected to the 25 Way D-Type Female Connector, the pin out and associated functionality are:



There is an additional alarm contact on a screw terminal labeled Direct - / +, which is used in conjunction with the schedule functionality of the system. It acts as the trigger for the keyswitch and can be used to trigger an alarm preset.



Both the AUX ALARMS and Direct alarm can replace or used in conjunction with external alarm modules (DM/CI01) via the 485-Bus. The DV-IP Server can support multiple alarm modules.

To add alarms:

1. Connect the corresponding alarm contact to the alarm input, i.e. Alarm 2 would be connected between ground (GND) and A2.
2. If multiple alarm modules are required then each will need to be addressed; consult the alarm module documentation for details.
3. Connect the 485-bus cable from the alarm module to one of the 485-bus sockets on the unit.
4. The polarity of the alarms (normally open/closed) is set in the 'Alarms Inputs' web page.



**Note:** The alarm contacts do not have to correspond to the equivalent camera number, for example alarm 2 could trigger camera 1, 2 and 3 into alarm mode.



## End Of Line Alarms

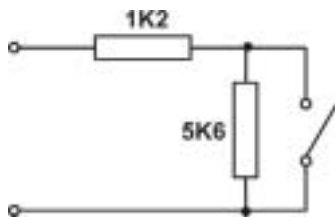
Any of the on-board alarms can be configured as End Of Line, the following describes the EOL tamper alarms circuitry needed when EOL has been enabled.

There should be two resistive values within the tamper alarm circuitry; these **must** be located inside the alarm device (furthest point from the DV-IP Server).

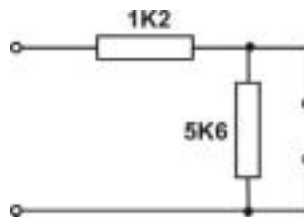
The alarm state could be Normally Open or Normally closed however the tamper state is the same for both settings.



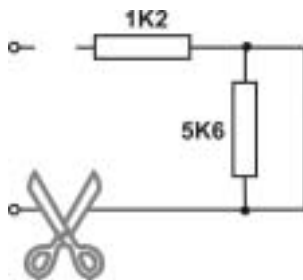
**Note:** Although the unit is shipped with resistive alarm inputs these need to be enabled in the Alarm Input Setup page, refer to the Configuring the DV-IP Server.



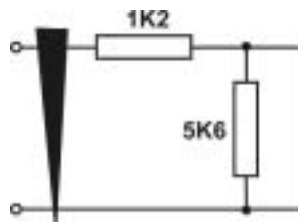
Open, the resistive value is 6.8K ohms (1.2K + 5.6K)



Closed, the resistive value is 1.2K ohms, as the circuit does not see the 5.6K ohm resistor.

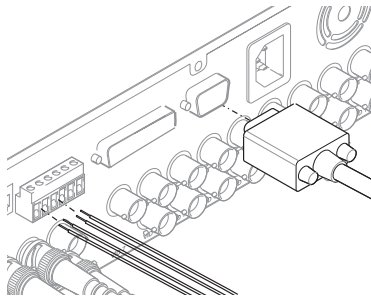


Open Circuit Tamper, the resistive value is infinity as the circuit has been cut and therefore is 'open'.



Short Circuit Tamper, the resistive value is 0 Ohms.

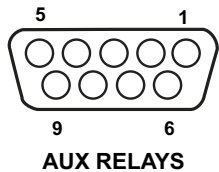
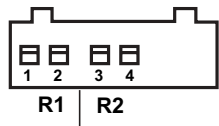
## Step 11 Connecting Relays



The DV-IP Server supports six auxiliary relays in total. These are divided between the 9 Way D-Type (AUX RELAYS) and the screw terminal (R1 / R2).

All of the relays are configurable within the web menus. There are six default options that allow any of the on-board or additional alarm modules to be selected for automatically triggering, refer to the configuration section for more details.

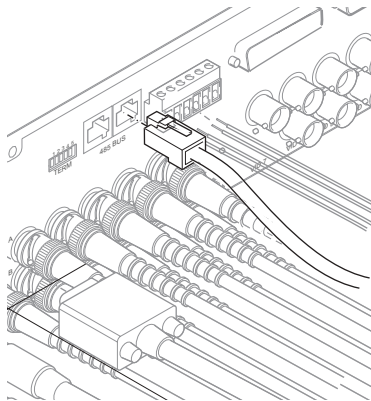
The following details the relay pin connections:



RELAYS	
Relay	Pin
R1	1 & 2
R2	3 & 4
R3 (AUX RELAYS)	1 & 6
R4 (AUX RELAYS)	2 & 7
R5 (AUX RELAYS)	3 & 8
R6 (AUX RELAYS)	4 & 9

The maximum rating of all the relays is 500mA @ 48V, exceeding this load will cause damage to the relays.

## Step 12 Connecting 485 Bus Devices



The DV-IP Server can support additional alarm inputs and relays via the 485-bus.

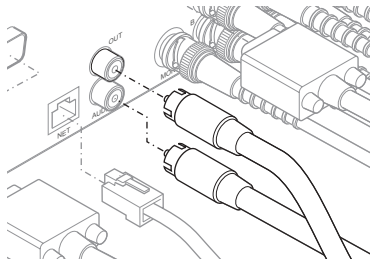
The DV-IP Server can support a single Alarm Input Module (DM/CC01) and two additional Relay Modules (DM/CI02) giving a possible total of 32 alarms inputs and 38 relays creating extensive integration capability for a single control of building management devices.

The DV-IP Server has two MMJ connections for 485-bus. Using the RS485 bus cable supplied connect to either of the MMJ connector's on the rear of the DV-IP Server and to the Alarm or Relay module.



**Note:** Ensure the ferrite clamped end of the DM485 bus cable is connected to the DV-IP Server. These modules can be daisy chained and therefore it is essential that the units are correctly addressed and termination set, please refer to the relevant installation manual supplied with your accessory for this information.

## Step 13 Connecting Audio Equipment



There are two audio channels on the DV-IP Server at the present time only Audio channel 1 is enabled. This allows audio to be recorded along side the video, as the audio is independently handled it is not linked to a specific video input.

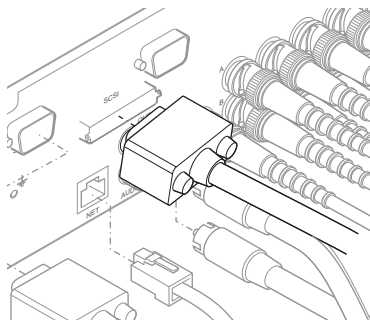
The DV-IP Server receives the audio digitises and compresses this and records it to hard disk alongside the video; the audio compression technique is ADPCM 8K.

The audio input and output connector's are phone sockets (RCA) and are line level (1 Volt peak to peak) therefore the peripheral audio devices require amplification. The audio phono sockets have the following attributes:

Audio In      47 KOhms input impedance, 1V peak to peak

Audio Out     1V peak to peak

## Step 14 Connecting External Storage (JBOD / RAID)



Although the DV-IP Server supports internal hard drives it is also possible to introduce additional storage by connecting an external storage device via the SCSI connector on the rear of the unit. The SCSI II connector is a 50 pin Micro 'D' connector; this is an industry standard connector.

The DV-IP Server is compatible with the Dedicated Micros JBOD and RAID storage devices and can support up to seven of these devices simultaneously which calculates up to 14Tbytes of storage per Server.



**Note:** Ensure if multiple storage devices are connected to the DV-IP Server these are correctly addressed, refer to the relevant Installation manual for the storage device.

## Step 15 Setting and Enabling Passwords

There are a number of features supported on the DV-IP Server that can be password protected to prevent any unauthorised user accessing the unit, these are:

- Viewing live and recorded video
- Webpage Configuration
- Telnet
- FTP

These are configured within the relevant .ini files using a terminal application, the following details how this is done.

### Default Passwords

The DV-IP Server has the following default user names and passwords; it is recommended that these default settings be changed as soon as possible to ensure security.

File Name	Function	Username	Password	Default Status
etc/webuser.ini	Web Configuration	dm	web	Enabled
	Live & Playback	- -	- -	Disabled
etc/users.ini	FTP	dm	ftp	Enabled
	Telnet	dm	telnet	Enabled
	Serial	dm	serial	Disabled



**Note:** Ensure you make note of the new user names and passwords that you set as loss of any of these may result in the unit being returned to Dedicated Micros.

The passwords are held within two of the .ini files on the Server; USERS.ini and the WEBUSER.ini files, these are located in the /etc directory on the unit.

### USER.ini File

The USER.ini file contains the user names and passwords for FTP, telnet and serial access, to change the username and password. Locate and edit this file.

To edit the .ini files you will need an FTP client, note an FTP client such as Cute FTP or Filezilla (<http://sourceforge.net/projects/filezilla>) can be downloaded free from the internet.

1. Using FTP software connect to the DV-IP Server;

To connect to the DV-IP Server type the IP address of the unit in the FTP software, you will be prompted for a user name and password, the default settings for these are **dm** and **ftp** respectively. Locate the file within the DV-IP/etc folder. Open the file with a text editor.



2. Change the **password** for the relevant function, here is an example of the original settings; note that the Serial user name and password are commented (#) out as this is not enabled by default.



3. **Save** the changes and then **upload** the file to the unit.

Multiple user names and passwords can be allocated to each function, simple add the information under the relevant heading, e.g.

```

[FTP]
dm=ftp
psmith=manager
jjones=admin

```

This will give three usernames and passwords for accessing the FTP function.

4. **Reset** the unit for the new Username(s) to take affect

## WEBUSER.ini

The WEBUSER.ini file contains the usernames and passwords for accessing the web configuration (step 4) accessing the live and playback modes (step 5) on the DV-IP Server.

To edit the .ini files you will need an FTP client, note an FTP client such as Cute FTP or Filezilla (<http://sourceforge.net/projects/filezilla>) can be downloaded free from the internet.

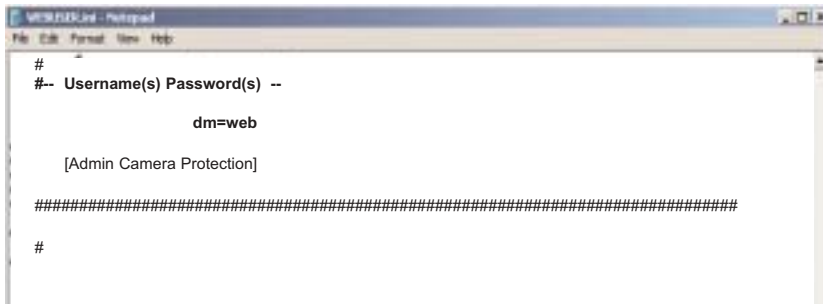
1. To connect to the DV-IP Server type the IP address of the unit in the FTP software, you will be prompted for a user name and password, the default settings for these are **dm** and **ftp** respectively.
2. Locate the WEBUSER.ini file within the DV-IP/etc folder.



3. Open the files with a text editor.

## Web Configuration

4. To change the web configuration passwords locate the Username(s) Password(s) section of the WEBUSER.ini file and change the default settings.



## Viewing (Live and Playback)

5. It is possible to allocate additional users to any of the pre-defined realms.

This example shows how two users may be allocated access to all cameras in live mode but will **not** have access to playback.

```
[User1 Camera Protection]
#####
#
# Provides Live access to cameras 1 - 16 in live for John Smith & Fred Bloggs.
# Playback is not permitted.
#
#####
object=cgi
live_cams=1-16
replay_cams=0
# -- Username(s) Password(s) --
john=smith
fred=bloggs
```

This example shows how a single user can be allocated access to all cameras in live and playback.

```
[User2 Camera Protection]
#####
#
# Provides access to cameras 1-16 in live and playback mode for John Green
#
#####
object=cgi
live_cams=1-16
replay_cams=1-16
# -- Username(s) Password(s) --
john=green
```



**Note:** It is possible to give access to specific cameras by entering the associated camera numbers, e.g. 1,5,8-10 will allow access to cameras 1, 5 and 8 through to 10.

3. **Save** the changes and then **upload** the file back to the etc directory, overwrite the file on the unit when prompted.

4. **Reset** the unit for the new Password(s) to take affect.



**NOTE: IT IS NECESSARY TO RESET THE UNIT WHEN ANY PASSWORDS ARE CHANGED!**

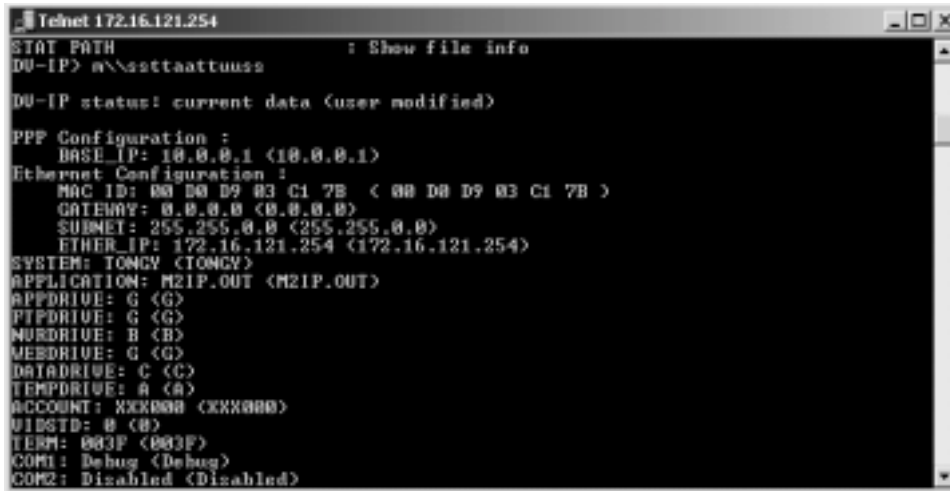


**Note:** The '#' is a comment and is placed in front of text that is to be ignored by the DV-IP Server.

Although passwords have been configured, if the security is not enabled on the system then the passwords will not be relevant. To check the status of the security settings, using FTP or telnet, enter:

**<ESC> m\status**

This will display the following information



```
Telnet 172.16.121.254
STAT PATH          : Show file info
DU-IP> m\\ssttaattuuss

DU-IP status: current data (user modified)

PPP Configuration :
  BASE_IP: 10.0.0.1 (10.0.0.1)
Ethernet Configuration :
  MAC ID: 00 D0 D9 03 C1 7B < 00 D0 D9 03 C1 7B >
  GATEWAY: 0.0.0.0 (0.0.0.0)
  SUBNET: 255.255.0.0 (255.255.0.0)
  ETHER_IP: 172.16.121.254 (172.16.121.254)
SYSTEM: TONGV (TONGV)
APPLICATION: M2IP.OUT (M2IP.OUT)
APPDRIVE: G (G)
PTPDRIVE: G (G)
MURDRIVE: B (B)
MEEDRIVE: G (G)
DATADRIVE: C (C)
TEMPDRIVE: A (A)
ACCOUNT: XXXXXX (XXXXXX)
UIDSTD: 0 (0)
TERM: 003F (003F)
COM1: Debug (Debug)
COM2: Disabled (Disabled)
```

Check that the security setting are both set to Pass, this means security is enabled for the Engineering and Debug modes.

To set the security up using telnet or FTP application enter

**<ESC> m\security\eng\pass**

The options available are; Pass – default, Open, Off

For Debug security, enter:

**<ESC> m\security\debug\pass**

The options available are; Pass – default, Open, Off



**WARNING: DEDICATED MICROS STRONGLY RECOMMEND THAT THE DEFAULT PASSWORDS BE CHANGED AS SOON AS POSSIBLE. CHANGING THE PASSWORDS WILL ENSURE THAT NO UNAUTHORISED USERS GAIN ACCESS TO THE UNIT.**



## Configuring the DV-IP Server

To assist you with the configuration of the DV-IP Server, this section is constructed in a tutorial manner and will make use of typical scenarios describing how to ..... allocate an IP address, set up VMD, etc. Select the sections that are relevant to the functionality required for your application and follow the step by step instructions.

As with the Installation of the unit this section will be divided into:

Simple Configuration – required to get the unit up and running

Advanced Configuration – project specific requirements



**Note:** It is presumed that configuration steps detailed in the DV-IP Server Quick Start Guide have been followed and therefore the cameras inputs have been enabled and the standard record rate has been set, although these features are detailed within this section.

## Web Page Icons

Each of the DV-IP Server configuration web pages has the following buttons:



**Reset to Defaults** – this will return the associated page to factory defaults.



**Display Help** – this will display the Help pages for the associated configuration page. This is a good starting point if you are having problems or do not understand the configuration parameters.



**Save Settings** – this will save a changes that has been made to the configuration page - remember to save the changes selecting a new page before saving the changes will result in all changes will be lost!



**Reset** – this will be displayed on the configuration pages for functionality that requires the unit to be reset to initiate the function, always save the settings before resetting the unit.

For each How to.... section the Tab name and Function name will be shown allowing you to easily locate the correct configuration page.

## Accessing the Configuration Web Pages

The configuration of the DV-IP Server is achieved via on the on board web pages, to access these:

1. Launch Internet Explorer (or Netscape Navigator)
2. Type the **IP address** of the DV-IP Server into the address bar



3. You will be presented with the Main Menu page



4. Select Configuration Options, you will be prompted for a username and password, if these have not been previously changed in the .ini file the default settings are dm and web respectively.



**Note:** The user name and password are case sensitive; it is recommended that you change the default username and password. Please keep this information as mislaid usernames and passwords could result in the unit being returned to Dedicated Micros.

## Simple Configuration

### How to Configure Global Parameters



There are some parameters that can be set that will affect the overall system; video standard for the video inputs, browser format for the web interface, language that the menus will be displayed in and the DST (daylight saving time) settings.

To configure these parameters:

1. Select **Home -> Main Set-up**
2. Select the **video format** from the drop down list; this will be the standard for all the video inputs on the DV-IP Server



**Note:** If the video format is changed it is necessary to carry out a system reset before saving the settings. This allows the unit to activate the change.

3. Select the **date format** from the drop down list
4. The DV-IP Server web pages can be viewed in two formats; **Active X** (default) or **Java**, select the relevant option from the drop down list
5. The web configuration pages for the DV-IP Server can be displayed in a selection of languages, **select the language** which is most appropriate to your installation from the drop down list



**Note:** Ensure the PC being used for the configuration is set to the correct time zone and that DST is enabled before continuing.

6. Select the **time zone** for the application from the drop down list
7. If the settings are incorrect reset the Server by selecting the **reset** button
8. If the DV-IP Server time is to be synchronised to the PC that is being used to configure the system then select **sync DV-IP** time from PC. Note this only synchronises the time when the button is selected this will not maintain synchronisation permanently.
9. Remember to save the configuration by selecting **Save Settings!**



Function	Description
Video Standard	<p>This is a global setting for all the video inputs on the DV-IP Server. The video format can be configured as PAL or NTSC.</p> <p>When the video standard is changed the DV-IP Server <b>must</b> be reset. Click on the Reset button</p>
Date Format	<p>It is possible to identify the format in which the date will be displayed; the default setting is Day Day, Month Month, Year Year.</p>
Browser Settings	<p>The browser interface on the DV-IP Server supports Active X or Java, the most appropriate for your application can be selected from a drop down list. Again this is a global settings and therefore any user connecting to the system will be presented with the same interface</p>
Language	<p>The DV-IP Server web configuration pages can be displayed in the language that is most suitable to the country of installation.</p> <p>The currently languages supported are; English, Spanish, French, Czech, Italian, Russian, Dutch, Portuguese, German, Turkish, Croatian, Danish, Finnish, Norwegian, Hungarian, Swedish, Polish</p>
DST	<p>Daylight Saving Time. This is the time zone that the DV-IP Server is installed in, select from the list for the most appropriate time</p>
Reset	<p>This will reset the DV-IP Server</p>
Sync Unit time from PC	<p>The DV-IP Server can be synchronised with the PC that is being used to configure the unit. If the PC is synchronised with the network clock then this time will be reflected in the DV-IP Server.</p> <p>The synchronisation is not a persistent and will only synchronise the DV-IP Server and the PC at the time the button is pressed</p>

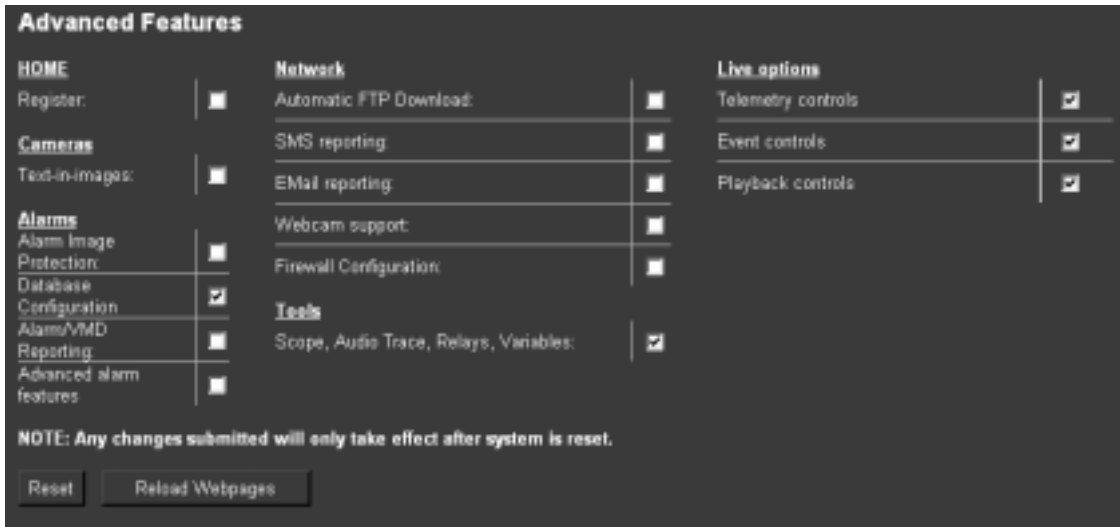
# How to Enable System Features



There are a number of features supported on the DV-IP Server that can be enabled or disabled depending on your system requirements.

When these features are enabled, the relevant configuration web pages will be displayed; if these are disabled then these pages will be omitted.

1. To enable the features select the **System -> Advanced Features**
2. By default the **Alarm/VMD Reporting** feature is enabled, to enable the other features **tick** the box next to the feature
3. Remember to select **Save Settings!**
4. You will now need to select **Reload Webpages** for the relevant configuration pages for the enabled features to be displayed
5. **Reset** the unit will initiate the functions and also re-load the additional web pages



Section	Feature	Description
Home	Register	<b>Note:</b> Configuration and registration of the DV-IP Server is carried out at the factory, therefore this screen is for fault diagnostics only and it is recommended that the page is not enabled unless advised by Dedicated Micros Technical Support

Section	Feature	Description
Cameras	Text in image	It is possible to integrate the DV-IP Server into an application where receipt of specific text can be used to trigger an alarm. This will enable the configuration page to be included in the <b>Cameras</b> tab
Alarms	Alarm image protection	It is possible to configure the DV-IP Server to protect images within parameters set by the operator (time and date, etc). This will enable the configuration page to be included in the <b>Alarms/VMD</b> tab
Alarms	Database configuration	The database can be set to have a maximum number of entries to ensure efficient management of the information. This will enable the configuration page to be included in the <b>Alarms/VMD</b> tab
Alarms	Alarm/VMD reporting	It is possible for the DV-IP Server to send information to a remote monitoring station under certain conditions (camera fail, alarm, etc). This will enable the configuration page to be included in the <b>Alarms/VMD</b> tab
Alarms	Advanced alarm features	This allows you to enable the advanced alarm support on the DV-IP Server. This will affect how the alarms operate in conjunction and supports features of the British Standard BS8418
Network	Automatic FTP download	The DV-IP Server can be configured to automatically download information using FTP, This will enable the configuration page to be included in the <b>Network</b> tab
Network	SMS reporting	The DV-IP Server can be configured to send data to an SMS server This will enable the configuration page to be included in the <b>Network</b> tab
Network	E-mail reporting	The DV-IP Server supports e-mail of data under certain conditions (alarm, start up, etc). This will enable the configuration page to be included in the <b>Network</b> tab
Network	Webcam support	The DV-IP Server can make any of the video inputs available to a web server for use within a web page. This function uses FTP to upload the images to the web server. This will enable the configuration page to be included in the <b>Network</b> tab
Network	Firewall configuration	The DV-IP Server supports an on board firewall to ensure no unauthorised users can access the unit. This will enable the configuration page to be included in the <b>Network</b> tab
Tools	Scope, Audio Trace, Relays, Variables	There are a number of tools that can be used to obtain information on the system performance, enabling this options will display the relevant pages in the <b>Tools</b> tab

Section	Feature	Description
Live options	Telemetry controls	This option allows the live pages to be tailored to the Operators requirements, disabling the option will remove all telemetry controls from the Live viewing pages.
Live options	Event controls	The unit supports an event database which can be accessed from the Live page, disabling this option will remove all event controls and will not allow the Operator to analyse the event database.
Live options	Playback controls	It is possible from the Live page to review any recorded images stored on the Digital Sprite, disabling this option will remove all playback controls from the Live viewing page.

## Advanced Alarm Features

These advanced alarm features are for detector activated CCTV systems and ensures that mandatory requirements for remote video installations that are requiring a level one, i.e. effectively immediately Police response are met. Such requirements are outlined in the British Standard BS8418 and makes the DV-IP Server respond to alarms in a specific way.

### Features

The following lists the additional features which are enabled when the Advanced Alarm option is enabled: Entry / Exit routes, Entry time, Alarm logic, Tamper proof alarm inputs, Automatic management of nuisance detectors and cameras, Relay outputs, System logs and Watch dog



**Note:** The advanced alarm features option is disabled by default; this can be enabled in the Advanced Features Web Configuration pages.

### Relay Settings with Advanced Alarms Enabled

When the Advanced Alarm Feature is enabled the Relay outputs on the Server have the following settings:

Description	Allocated Function
Relay 4	Set/Unset notification (default)
Relay 5	Set/Unset notification (default) User programmable for Primary signalling failure notification

# How to Configure Camera Inputs



Each video input can be individually configured.

How to enable each input and set the standard record settings has been briefly described in the Quick Start Guide, this section will detail the full configuration process; camera resolution and file size, camera titles, termination, video colour and camera fail notification, standard recording settings.

The enabled cameras can also be included on in a sequence that will be displayed on the DV-IP Server Spot monitor, how this is configured is also covered in this section.

This section is divided into:

- Enabling and configure the camera inputs settings
- Configuring the standard record settings
- Enabling cameras for display on the spot monitor.

To enable/configure camera input settings:

1. Select **Cameras -> Camera Set-up**
2. It is possible to identify the global **camera resolution** (common to all video input) for the images that are viewed and recorded, select the correct resolution from the drop down list
3. To ensure the files sizes are maintained when viewing high, medium or low quality video enter the global **maximum file size** (common to all video inputs) for these viewing options.



**Note:** It is recommended that the DV-IP Server record images at the High resolution settings to ensure best video performance on recorded images, refer to the *Advanced Camera Setup* section for full details.

4. **Enable** the **video inputs** that have a video source connected by placing a **tick** in the corresponding box
5. In the corresponding title box enter the **camera name** for the video source connected to that input
6. If the final destination that the video source is to be connected is the DV-IP Server then this input must be **terminated**, however if the **loop through** connections on the Server are to be used then the corresponding input must be un-terminated. To select termination place a tick in the box adjacent to the video input, to un-terminate remove the tick from the box
7. By default the DV-IP Server presumes all enabled inputs are **colour video sources**. If you are connecting a **monochrome** signal to the Server it is recommended that the input be set for **mono**, place a tick in the corresponding video input



8. To enable the Server to send notification that the video input does not detect a 1V peak to peak signal place a tick in the box adjacent to the video input, this will give a **camera fail** alarm
9. Save the configuration by select **Save Settings!**

To configure the standard record settings

10. The **record duration** and **standard record rate** are inter-connected; changing one of these settings will automatically update the other.



**Note:** The **alarm record rate** is **not** taken into account.

11. Enter the information in either the record duration or standard record rate, these are global settings
12. Enter the **alarm record rate** for when the DV-IP Server is in an alarm situation, this is a global setting
13. Enter the **video expiry period** in days

The DV-IP Server supports three operating modes (default Day, Night and Weekend), if these have been enabled within the **Cameras>Schedule** function then it is possible to identify the alarm record rate in all modes of operation.

14. If **all operating modes** are enabled each cameras must be selected for recording depending on the mode they are to be available for alarm recording. The default modes of operation are Deay, Night and Weekend.

15. Enter the **record rate** for the operating modes, this applies to all cameras enabled within these modes.

16. Select the **alarm record mode** for each operating mode, the options are Unchanged, interleave or exclusive.

17. Save the configuration by select **Save Settings!**

**Camera Set-up** -  Pictures Per Second (pps)  Milliseconds (ms) [Click here to see thumbnail images](#)

Live/Record Resolution:

High:  KB Jpeg Image Size

Medium:  KB Jpeg Image Size

Low:  KB Jpeg Image Size  
Image Sizes 5KB-45KB

Image Sizes 5KB-45KB

Video Expiry Period:  Days

	DAY		NIGHT	
	DD	HH	DD	HH
Record Duration	<input type="text" value="17"/>	<input type="text" value="13.4"/>	<input type="text" value="17"/>	<input type="text" value="13.4"/>
Standard Record Rate	<input type="text" value="6"/> pps		<input type="text" value="6"/> pps	
Alarm Record Rate	<input type="text" value="6"/> pps		<input type="text" value="6"/> pps	
Alarm Record Mode	<input type="text" value="Unchanged"/>		<input type="text" value="Unchanged"/>	


Connected	Title	DAY	NIGHT	Terminated	Mono	Telemetry	Cam-Fail Reporting
<input checked="" type="checkbox"/>	Camera 1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	None	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Camera 2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	None	<input checked="" type="checkbox"/>

Function	Description
----------	-------------

Pictures Per Second (pps) / milliseconds (ms)	This allows the record settings to be configured as either Pictures Per Second or Milliseconds
Live/Record Resolution	This is the resolution of the live and recorded images (JPEG only) that will be transmitted from the DV-IP Server and recorded to hard disk. <b>JPEG</b> PAL Fields 640 x 256, 720 x 256, 768 x 288 Frame 640 x 576, 768 x 576 NTSC Fields 640 x 240, 720 x 240 Frame 640 x 480, 720 x 480 <b>Note:</b> Frame recording will reduce the image record rate performance by half.
High	This is the maximum file size for the images when high quality video has been selected to be recorded or viewed.
Medium	This is the maximum file size for the images when medium quality video has been selected to be viewed
Low	This is the maximum file size for the images when low quality video has been selected to be viewed



**Note:** The smaller the file size the more data can be transmitted but the more compression applied and therefore the lower the quality. Images sizes can be set between 5 and 45KB

Advanced Setup	This allows the alias configuration for the MPEG4 option, refer to the Advanced Setup section below.
Video Expiry Period	This indicates the maximum time any images can be stored on the hard disk, if the record duration is less than the video expiry period the images will automatically be overwritten
Connected	It is necessary to enable the video inputs that have a video source connected. By default only video input 1 is enabled (refer to the Quick Start Guide for more information)
Camera Title	It is possible to allocate an ASCII camera title to each of the enabled inputs, this along with the camera number will be displayed on the screen to identify the camera selected
Operating modes	Each camera can be individually selected to be enabled or disabled in each of the operating modes, e.g. within the Night mode cameras would be enabled that are to be triggered during out of office hours.
Terminated	As the DV-IP Server supports loop through it is necessary to remove the termination of any inputs that are 'looped', by default all inputs are terminated at 75 ohms
Mono	<p>If the video input on the DV-IP Server has a black and white (monochrome) source connected then enable the corresponding camera.</p> <p><b>Note:</b> The Server will try and compress the colour contents of the image if this box is not enabled, ticking this box will remove unnecessary overhead on the compression process</p>
Telemetry	<p>The DV-IP Server supports Dennard, Pelco and BBV protocols for coaxial telemetry cameras, this allows the relevant protocol to be applied to the corresponding video input (see below for more information)</p> <p><b>Note:</b> Refer to How to Enable Serial Telemetry for RS232/RS422/RS485 telemetry</p>
	<p><b>Note:</b> This will only be active when one of the video inputs on the DV-IP Server has been configured for coaxial telemetry. When any of the inputs have been set for coaxial telemetry this allows the telemetry functions to be configured (see below for more detailed information)</p>
Camera Fail Reporting	If the video input on the DV-IP Server does not identify a 1V peak-to-peak signal then the unit can transmit an alarm notification for camera failure on the corresponding video input
Record Duration	<p>The total record time available in (DD) Days and (HH) Hours. This indicates the storage capacity of the system without any alarm recording. This is estimated from size of video storage, the standard record rate and the requested target size of the recorded images. Note: Changing the Record Duration will automatically update the Standard Record Rate. Changing the Standard Record Rate will likewise update the Record Rate</p>

Function	Description
Standard Record Rate	<p>This is global setting and identifies the 'common pictures per second' for all enabled video inputs on the unit. This will remain unless otherwise actioned (Alarm or Variable Record Rate)</p> <p>This can be set in milliseconds or the number of pictures per second.</p> <p>The delay between consecutive images from any one camera is the Standard Record Rate multiplied by the number of cameras being recorded. Changing the Standard Record Rate will automatically update the Record Duration. Changing the Record Duration will likewise change the Standard Record Rate</p> <p>Example Record Rates show the pps and the equivalent ms:</p> <p>100 picture per second or 40ms  50 pictures per second or 20ms  25pps or 40ms  20pps or 50ms  10 pps or 100ms  8pps or 125ms  5 pps or 200ms  2pps or 500ms  1pps or 1000ms</p> <p><b>WARNING:</b> When running the unit at maximum Record Rate (50pps or 20ms in Standard Record Settings), this will affect viewing and network transmission, as the video codecs will be running close to capacity - the unit's priority is to record the footage to the internal HDD, so transmission performance will be reduced. This is exhibited by slow connection to the html pages and reduced viewing frame rates. Multi-user viewing will also be affected. It is not recommended to set the Standard Record rate to 20ms for everyday usage, but rather only for specific situations where this rate is necessary.</p>
Alarm Record Rate	<p>This identifies the global alarm recording rate which will be activated if an alarm is triggered on the unit. For example, the unit may be configured to increase the recording rate when a door contact is triggered.</p>
Alarm Record Mode	<p>This option allows exclusive or interleave recording to be selected within any of the operating modes (Day, Night, Weekend) to adjust the record sequence when an alarm is received. The options for event recording are:</p> <p><b>Unchanged</b> – This sets the record sequence to remain the same whether an alarm is present or not.</p> <p><b>Exclusive</b> – The unit will only record the alarm cameras.</p> <p><b>Interleaved</b> – This will set the unit to record the alarm cameras more frequently than non-alarm cameras, by interleaving the two i.e. if camera 1 is in alarm the interleave recording would be 1213141516...</p>
Click here to see thumbnail images	<p>This will display a thumbnail view of video connected to the unit. Place the cursor in the camera title box to view the corresponding video input</p>

## Advanced Camera Setup

The DV-IP Server supports JPEG and MPEG4 compression, this section allows the two compression and associated settings (resolution, image size, pps, etc) to be configured so that the User Interface allows dynamic switching between viewing JPEG or MPEG4 images.

To configure the Advanced JPEG-MPEG4 settings:

1. Select **Cameras -> Camera Set-up -> Advanced Setup**
2. **Enter** the **JPEG** file size in **Kbytes** for the various image resolutions; 2CIFHI, 2CIFMED, 2CIFLO, CIF, QCIF.
3. **Enter** the **bit rate** for the equivalent **MPEG4** images for the same image resolution.
4. **Enter** the number of **pictures per second** required with the **MPEG4** compression.

Advanced Jpeg-Mpeg4 Setup			
System Resolution (640 x 512)			
Resolution codes	Jpeg (Kbytes)	Mpeg4 Bitrates (Kb/sec)	Mpeg4 Framerate(pps)
2CIFHI (640 x 256)	20	512	25
2CIFMED (640 x 256)	10	256	12
2CIFLO (640 x 256)	5	64	6
CIF (320 x 256)	20	256	25
QCIF (160 x 128)	5	32	12

Function	Description
System Resolution	This reflects the resolution set within the Camera Setup page and will apply this setting to all resolution configuration within this page
Resolution codes	There are a number of resolution codes that identify the size of the image that will be transmitted when this resolution is selected. These figures will be dependant on the System Resolution setting. <b>Note:</b> The image sizes are shown within the brackets.
JPEG (Kbytes)	This is the maximum JPEG file size for each of the resolution options, the settings is in Kilobytes
MPEG4 Bit rates (Kb/sec)	This is the maximum bit rate for each of the resolution options and is configured in the number of kilobits to be transmitted per second
MPEG4 Frame rate (pps)	This identifies the number of frames per second that DV-IP Server will transmit for the equivalent bit rate

5. Select the **resolution** of the **recorded images** from the drop down list, the settings configured in steps 1 to 3 will be used for recorded video.



**Note:** The DV-IP Server records JPEG images while simultaneously supporting the option to transmit JPEG and MPEG4 images for viewing.

6. Select the **resolution** for the images that will be transmitted when the **high resolution** option is selected in the viewing application.

7. Select the **resolution** for the images that will be transmitted when the **medium resolution** option is selected in the viewing application.

8. Select the **resolution** for the images that will be transmitted when the **low resolution** option is selected in the viewing application.

9 Remember to save the configuration by selecting **Save Settings!**

Resolution alias	Resolution code
Rec	2CIFHI
High	2CIFHI
Medium	2CFMED
Low	2CIFLO

Function	Description
Resolution alias	This identifies the functions available on the DV-IP Server when utilising one of the viewing applications. It identifies the record resolution on the JPEG images and the options for viewing live and playback images in high, medium or low resolution
Resolution codes	This is a drop down list and allows any of the configured resolution to be selected, the example shows that the record alias is 2CIFHI, selecting the low resolution option in the viewer will force the DV-IP Server to transmit 2CIFLO images

# Configuring the Network Settings of the DV-IP Server



The Quick Start Guide gives details of how an IP address can be allocated to the network port on the DV-IP Server to allow you to communicate via a LAN or WAN from a web interface.

This section details these additional configuration parameters.

To configure the network information

1. Select **Network -> Network Settings**
2. The **IP address**, **subnet mask** and **default gateway** (if set) that has already been configured in the .ini file will be displayed on this page, these can be changed by entering the new information in the relevant areas
3. The DV-IP Server supports **Domain Name Server** allowing the DV-IP Server to reference other hosts by their name rather than their IP address, enter the **IP address** of the **primary DNS** and **secondary DNS** server
4. The default **unit name** for the DV-IP Server is DV-IP, this can be changed to a more appropriate name by entering the information in this section
5. If the Server is to use **PPP** then the corresponding **IP address** needs to be entered



**Note:** The PPP IP address must be in a different range to the local IP address range.

Description	Command	IP Address
PPP IP	Ethernet_IP\PPP_IP	10.0.0.1
Ethernet IP	Base_IP	172.16.1.2

6. As the DV-IP Server can be connected to a LAN or WAN network it is possible to identify the **maximum bit rate** for the network connection. There are **default settings** for **LAN**, **WAN** and **ISDN** if these defaults are accept select the corresponding button for your network link
7. If the default settings are not as you require enter the information in the sections that are incorrect
8. Remember to save the configuration by selecting **Save Settings!**




**Note:** It is possible to limit the bandwidth for remote monitoring. The limitation is for HTTP connections only (configuration and viewing via the web interface), FTP and Telnet connections are not included in this limitation these connections may use bandwidth.

**Network Settings**

IP Address: 172 16 254 74  
 Subnet Mask: 255 255 0 0  
 Default Gateway: 172 16 60 60  
 Primary DNS: 0 0 0 0  
 Secondary DNS: 0 0 0 0  
 System Name: ANDYS\_C2D\_DVP  
 Base PPP IP: 10 0 0 1  
 PPP IP: Link1 10.0.0.1  
 PPP IP: Link2 10.0.0.2  
 DHCP IP: 0.0.0.0  
 DHCP Subnet: 0.0.0.0  
 DHCP Gateway: 0.0.0.0  
 DHCP Name:  
 Serial Number: DEV51836N004

Please choose one of the pre-set buttons for your Ethernet bandwidth settings, or manually enter your preferred settings.  
 LAN WAN ISDN

Force 10BaseT operation:   
 Maximum Trans Rate: 100000 Kilobits/second (100 KBytes)  
 Transmit Image Buffers: 3 (1 to 3 buffers)  
 Ethernet MTU: 1500 Bytes  
 TCP Re-Transmit Timeout: 250 Milliseconds  
 PPP Idle Line Timeout: 180 Seconds  
 PPP Link Down Timer: 2 Minutes  
 Packet Size: 0 Bytes  
 Secondary Web Server Port: 0

Function	Description
IP Address, Subnet Mask, Default Gateway	These are the settings that have already been configured via the Serial port configuration. This is the static IP address and subnet mask, and if applicable default gateway
Primary DNS	This is the primary DNS server IP address for applications that are utilising domain names
Secondary DNS	This is the IP address of the secondary DNS server in case of failure of the primary server
System Name	This is the name that is allocated to the DV-IP Server, this will be used when transmitting alarm information to a Remote Monitoring Station
Base PPP IP	This is the base IP address allocated to the DV-IP Server. The PPP Link 1 and PPP Link 2 are automatically generate from the allocated base IP. PPP Link 1 takes the base IP and PPP Link 2 will take the next sequential IP address.
DHCP IP	If the DV-IP Server was installed on a DHCP network this would be the IP address the DHCP server allocated on power up of the unit
DHCP Subnet	If the DV-IP Server was installed on a DHCP network this would be the subnet of the network the unit is connected and would be automatically allocated by the DHCP server on power up



Function	Description
DHCP Gateway	This is the IP address of the default gateway (router) that the DV-IP Server would be automatically assigned to by the DHCP server
DHCP Name	This would be the name of the DV-IP Server that is automatically allocated by the DHCP server
Serial Number	This is the serial number of the DV-IP Server, this is a read only section
LAN, WAN, ISDN	These have default settings for the following information, selecting these will automatically allocate values to these settings LAN – 10000 Kilobits/second WAN – 256 Kilobits/second ISDN – 64 Kilobits/second
Force 10BaseT operation	The DV-IP Server supports 10 or 100BaseT half duplex transmission, this will force the unit to operate at a 10BaseT connection
Transmit Image Buffers	This is used in order to improve the picture delivery over Ethernet when using a slow connection, i.e. 256Kbps. Options available are 1, 2 or 3 buffers
Ethernet MTU	This is the maximum transmit unit for the Ethernet packet. By default this figure is set to 1514bytes
TCP Re-Transmit Timeout	This is the time the DV-IP Server will wait to re-send a packet if an acknowledgement is not received. When making a connection across a WAN link this figure should be increased and should match the timeout figure for the router
PPP Idle Line Timeout	This is the time the DV-IP Server will wait before dropping the PPP link if data has not been transmitted
PPP Link Down Timer	If for any reason the connection is lost then this is the time period before the DV-IP Server will be forced to drop the PPP connection
Packet Size	This is the maximum packet size that will be transmitted from the DV-IP Server. This figure is identified in Bytes
Secondary Web Server Port	If the default port setting for web serving has already been allocated it is possible to configure a second port number. Eg. If the secondary web port is set for 8000 because the default (80) web port is blocked by the network or firewall. To obtain images from the DV-IP Server enter the IP address plus the secondary web port in the address section of Internet Explorer or in the DV-IP Viewer; <a href="http://172.16.1.2:8000">http://172.16.1.2:8000</a> (<IP address><:><secondary port number>)

# How to Select and Enable Coaxial Telemetry



The DV-IP Server supports numerous coaxial telemetry protocols allowing these cameras to be connected directly to the Server and controlled using their native control protocol.

Simple selection of manufacturer/model within the configuration pages and these cameras can be controlled. Common telemetry operations such as pan, tilt, zoom, presets can be controlled via the Live page of the web interface or via the DV-IP Viewer software.



**Note:** Priorities are not allocated to the PTZ control; this works on the initial connection and request having the control. Any subsequent connections will allow viewing but no control until the initial connection is relinquished or after a set period (5 seconds) where control commands have not been issued to the PTZ/dome camera

Any of the video inputs on the Server can be configured for coaxial telemetry; this is achieved in the Camera Set-up page.

1. Select **Cameras -> Camera Set-up** to configure the individual cameras
2. The protocols currently supported on the DV-IP Server are: BBV, Pelco and Dennard. Using the **drop down list**, select the relevant manufacturer for the associated video input
3. Remember to save the changes you have made by selecting **Save Settings!**


Once you have selected the telemetry protocol it is possible to; review the image from the video input, test the control, configure the features of the camera that are required for you application (such as presets), and access the dome/PTZ camera menus to configure the more enhanced features supported on the dome, refer to the manufactures manual for the camera for these features.

## Important Information

It is possible to use VMD (Video Motion Detection) on moveable cameras, however to ensure that moving the camera does not trigger false alarms the VMD will only be active when the dome is in preset position 1 (home position). This ensures that VMD is only active when the camera is viewing the field of view that the VMD mask corresponds to, moving the camera away from preset 1 will automatically inhibit VMD detection on the camera. As soon as the camera receives the command to 'return to home' the VMD will be automatically re-enabled.



**Note:** It is necessary for the 'return to home' command to be issued so that the DV-IP Server is aware the camera is back at preset position 1, leaving the camera to return to preset 1 after a dwell time will not be sufficient to re-enable the VMD functionality.

Function	Description
Telemetry	The DV-IP Server supports numerous protocols for telemetry cameras, this allows the corresponding video input to be configured for the relevant protocol (see below for more information)
	If any of the inputs have been set for coaxial telemetry this option allows the telemetry functions to be configured (see below for more detailed information)

## Telemetry Setup Page

1. To access the set up parameters of the camera select the **Telemetry Setup** button on the **Camera Set-up** page



**Note:** When you select the Telemetry Setup button, it may take a few seconds for the page and video to be downloaded, during this time do not press any buttons as this will slow the process down.

2. The video from any of the cameras on the unit along with the telemetry control buttons for testing will be displayed

This allows you to view any of the enabled inputs on the DV-IP Server, control the telemetry connected to the system and set up any features that are required for your application; such as presets. You can also access the camera menus from this page allowing you to configure parameters that are only programmable from the camera menu.



**Note:** Review the relevant documentation for the camera to see how you navigate the camera menus. Remember to save any configuration settings in the dome menu!

## How to Enable Serial Telemetry



The DV-IP Server supports numerous serial telemetry protocols, any of the video inputs on the DV-IP Server can be configured as a functional camera.

Common telemetry operations such as pan, tilt, zoom, presets can be controlled via the Live page of the web interface or via the NetVu Observer software.

Serial 1 and 2 can be enabled for RS232 Telemetry, Serial 3 and 4 can be enabled for RS232/485 Telemetry.

The current serial protocols supported on the Server are:

DM-Serial	Kalatel	Philips	Vantage
Dennard	Mark Mercer	Samsung	VCL
Ernitec	Panasonic	Sensormatic	Vista
JVC	Pelco	Ultrak	

1. Connect the camera and serial cables to the DV-IP Server before configuring the Server:
2. Select **System -> Serial Ports & Telemetry**
3. Using the drop down list on the associated communication port (**SERIAL 3** or **SERIAL 4**) select **RS232/485 Telemetry**
4. Select the relevant **telemetry type** from the list of supported protocols.
5. Enter the dome/PTZ **standard settings** for:  
Baud rate, Parity, Data bits, Stop bits, Flow control
6. Ensure the **address** of the dome/PTZ camera is the same as the **video input** number on the DV-IP Server, e.g. Video input 15 would equate to the dome/PTZ camera being address 15
7. Remember to save the changes you have made by selecting **Save Settings!**
8. It is necessary to Reset the unit after configuring this page, press the **Reset** button.

Once you have selected the telemetry protocol and addressed the dome/PTZ camera it is possible to; review the image from the video input, test the control, configure the features of the camera that are required for you application (such as presets) and access the dome/PTZ camera menus to configure the more enhanced features supported on the dome, refer to the manufactures manual for the camera for these features.

## Important Information

It is possible to use VMD (Video Motion Detection) on moveable cameras, however to ensure that moving the camera does not trigger false alarms the VMD will only be active when the dome is in preset position 1 (home position). This ensures that VMD is only active when the camera is viewing the field of view that the VMD mask corresponds to, moving the camera away from preset 1 will automatically inhibit VMD detection on the camera. As soon as the camera receives the command to 'return to home' the VMD will be automatically re-enabled.



**Note:** It is necessary for the 'return to home' command to be issued so that the DV-IP Server is aware the camera is back at preset position 1, leaving the camera to return to preset 1 after a dwell time will not be sufficient to re-enable the VMD functionality.



Function	Description
Serial 1 and 2	Serial port configuration, the port usage that can be assigned is; off, debug, general purpose, text in image, PPP (PPP_Link 2) and RS232 telemetry
Modem/TA	When the serial port has been configured for PPP it is necessary to select from one of the supported modems to identify the device connected to the unit, refer to table below for supported modems/TA's
Telemetry type	This is the list of RS232 serial telemetry protocols that are supported on the DV-IP Server
Serial 3 and 4	Serial port configuration, the port usage that can be assigned is; off, debug, general purpose, text in image and RS232/485 telemetry
Telemetry type	This is the list of RS232/485 serial telemetry protocols that are supported on the DV-IP Server
Baud rate, parity, data bits, stop bits, flow control	These are the default settings of the selected serial device. Refer to the relevant manufacturer manual for the peripheral serial device for this information

## Telemetry Setup Page

1. To access the set up parameters of the camera select the **Telemetry Setup** button on the **Serial Ports & Telemetry** page



**Note:** When you select the Telemetry Setup button, it may take a few seconds for the page and video to be downloaded, during this time do not continually press any buttons as this will slow the process down.

2. The video from any of the cameras on the unit along with the telemetry control buttons for testing will be displayed

This allows you to view any of the enabled inputs on the DV-IP Server, control the telemetry connected to the system and set up any features that are required for your application; such as presets. You can also access the camera menus from this page allowing you to configure parameters that are only programmable from the camera menu.



**Note:** Review the relevant documentation for the camera to see how you navigate the camera menus. Remember to save any configuration settings in the dome menu!

## Supported Modems/TA's

Generic AT Modem

3ComImpact II

KTX 33600 – Modem

PSL - ISDN TA

Nokia30 HSCSD V.110

SHIVA LanRover

Spider 4 CDPD Modem

3Com US Robotics 56K Modem

Falcom GSM Phone / Modem

PLANET Smart IP

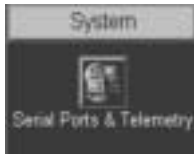
Nokia30 GSM

Nokia30 HSCSD V.120

Siemens TC35GPS / MC35 GPRS

Zyxel Omni-net.D - ISDN TA

# How to Configure Matrix Control



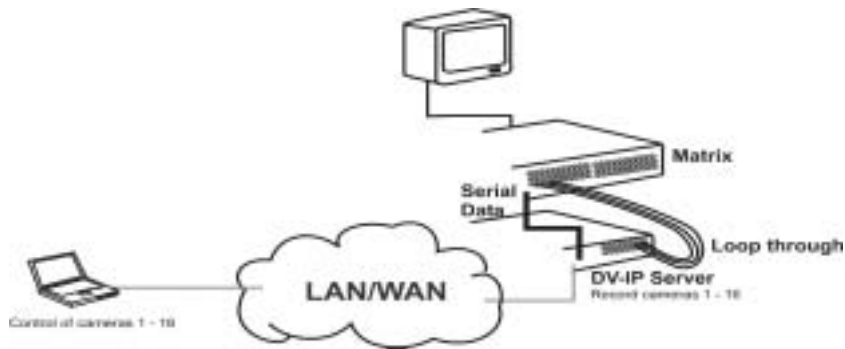
The DV-IP Server can be incorporated into an existing analogue matrix installation and offers control of the matrix via the Live web page or the DV-IP Viewer software.

This ensures that any existing installation does not need to be removed to over network control, simply integrate the DV-IP Server into the system a network output.

The Server supports connectivity to the matrix on serial ports COM3 or COM4, the following matrix protocols are currently integrated into the Server software:

- American Dynamics (AD) RS232 Matrix
- AD168 RS232 Matrix
- BBV TX1000, TX1500 and BBus-Interface Matrices
- VCL/Ademco Maxcom Matrix

Connect the all video inputs to the matrix and the DV-IP Server (loop through) as shown below, then carry out the following:



1. Select **System -> Serial Ports & Telemetry**
2. Using the drop down list on the associated **communication port** (Serial 1 to 4) select **RS232 Telemetry**
3. Select the relevant **matrix** from the list of supported protocols.  
The serial standard settings for the selected matrix will automatically be allocated, however if this is incorrect you can change these for:
  - Baud rate, Parity, Data bits, Stop bits, Flow control
4. Enter the **Matrix Monitor** number of the matrix that the DV-IP Server is connected to and that you will be controlling
5. Enter the **Matrix Offset** address

6. Save the configuration by selecting the **Save Settings!**



Function	Description
----------	-------------

Serial 1 and 2	Serial port configuration, the port usage that can be assigned is; off, debug, general purpose, text in image, PPP (PPP_Link 2) and RS232 telemetry
----------------	---

Serial 3 and 4	Serial port configuration, the port usage that can be assigned is; off, debug, general purpose, text in image and RS232/485 telemetry
----------------	---

Telemetry type	This is the list of serial telemetry protocols that are supported on the DV-IP Server, select the correct protocol for the connected matrix
----------------	---

Telemetry Matrix Monitor	Matrices support many monitor outputs, this is the monitor output that has been allocated for connection to the DV-IP Server
--------------------------	--

Telemetry Matrix Offset	This is the matrix offset to allow any camera input on the matrix to be set as input 1 for the DV-IP Server. An example of this is in large systems where multiple operators are allocated groups of cameras, for ease of use each camera can be configured to start at camera 1. However they could actually be connected to any input on the matrix but we would select camera 1 which could be controlling input 32 on the matrix.
-------------------------	---

Baud rate, parity, data bits, stop bits, flow control	These are the default settings of the selected serial device. Refer to the relevant manufacturer manual for the peripheral serial device for this information
---	---



This completes the Simple Configuration of the DV-IP Server. The unit can operate at the basic level and the remaining configuration would include functionality that is specific to the customer requirements.

The following parameters have been configured:

- Global settings

- Video inputs

- Cameras parameters

- Record rates

- Remote connectivity

## Advanced Configuration

### How to Adjust Camera Settings

This allows the camera colour and contrast to be adjusted on each of the camera inputs.



**Note:** It is recommended that these settings be checked at various times of the day when the light levels change to ensure optimum performance.

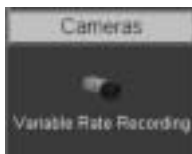
Camera Adjustments			
Camera	Title	Colour Level	Contrast Level
1	Camera 1	0	0
2	Camera 2	0	0
3	Camera 3	0	0

#### Function

#### Description

Camera	This identifies the video input number on the unit, this will be dependant on which unit you are installing, i.e. 6, 9, 16 channel version.
Title	This identifies the corresponding camera title allocated to the video input.
Colour	Select a value from the drop down list to select the colour level for the video input.
Contrast	Select a value from the drop down list to select the contrast level for the video input.

### How to Configure Variable Recording



The DV-IP Server by default will record all enabled inputs at the standard record rate.

Standard recording sets a record rate that is evenly distributed across all the enabled inputs. Alternatively it is possible to identify individual record rates for each of the video inputs; this will allow you to have cameras with higher importance recorded at a higher frame rate.



**Note:** You can set Standard or Variable Record Rate only; you are not able to configure the same cameras for both settings.

The following details how the Variable Record Rate can be set for; normal recording, in the event of an alarm and when VMD has been identified on an input. These setting would be used in an alarm situation where an increased frame rate may be required.



**Note:** Remember that although each video input can be individually configured the DV-IP Server supports up to 100pps (PAL)/120pps (NTSC) across all inputs, do not exceed this quantity.

To set up Variable Recording on the Server:

1. If the relevant camera has already been enabled in the **Standard Record** menu then you must **de-select** the **camera** from this menu and **save** the configuration before setting Variable Rate Recording
2. Select **Cameras -> Variable Rate Recording** to configure individual cameras
3. Select between **Pictures Per Second (PPS)** or **Milliseconds (ms)**
4. By default the cameras are disabled, to enable the relevant cameras **tick** the box associated with that camera
5. There are three record rate settings that can be configured within this page; Variable Record Rate, Alarm/VMD Record Rate, Pre-alarm Record Rate. In addition you can also identify the number of pre-alarm pictures that you want to be stored along with the alarm recording. Enter the **record rate** in the relevant setting alongside the camera input.

If the record rates you enter exceed the **total** record rate that the DV-IP Server supports the following prompt will be displayed.



6. Remember to save the configuration you have entered by selecting **Save Settings!**

Variable Record Setup - <input checked="" type="radio"/> Pictures Per Second (pps) <input type="radio"/> Milliseconds (ms)		Variable record			Variable record rate			Alarm/VMD record rate			Pre alarm record rate			Number of pre-alarm pictures		
Camera	Title	DAY	NIGHT	WEEKEND	DAY	NIGHT	WEEKEND	DAY	NIGHT	WEEKEND	DAY	NIGHT	WEEKEND	DAY	NIGHT	WEEKEND
1	Camera 1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0	0	0	0	0	0	0	0	0	0	0	0
2	Camera 2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0	0	0	0	0	0	0	0	0	0	0	0
3	Camera 3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0	0	0	0	0	0	0	0	0	0	0	0

Function	Description
Pictures Per Second - Milliseconds	The variable record rate can be configured as pps or ms. Ensure the information entered is in the correct format
Variable record (Day / Night / Weekend)	By default all the video inputs are disabled, this allows you to enable all or select individual inputs - in either of both recording modes if dual mode operation is enabled
Variable record rate (Day / Night / Weekend)	This is the pictures per second or milliseconds that the unit will record in normal operation, if the camera is only to be recording in an alarm situation leave the setting at 0. If dual mode operation is enabled the variable record rate can be set in either or both modes
Alarm/VMD record rate (Day / Night / Weekend)	This is the pictures per second or milliseconds that the unit will record when the corresponding video input has identified VMD or has been triggered by an external alarm If dual mode operation is enabled the alarm/VMD record rate can be set in either or both modes
Pre-alarm record rate (Day / Night / Weekend)	This is the pre-alarm pictures per second or milliseconds that will be recorded along with the alarm images If dual mode operation is enabled the pre-alarm pps or ms can be set in either or both modes
Number or pre-alarm pictures (Day / Night / Weekend)	Although the pre-alarm record rate is set it is also necessary to identify the number of pre-alarm pictures If dual mode operation is enabled the pre-alarm record rate can be set in either or both modes

## RAMDisk

This indicates how much RAMDisk is available for pre-alarm images. This allows the operator to monitor the RAMDisk allocation and ensure as you configure your variable record settings you have sufficient RAMDisk to accommodate the number of images required on alarm; i.e. variable record rate, alarm/VMD record rate, pre-alarm record rate and number of pre-alarm cameras.

The screen shows the settings for camera 1 and camera 2 and how much of the RAMDisk would be required for these settings.

Camera	Title	Variable record		Variable record rate		Alarm/VMD record rate		Pre-alarm record rate		Number of pre-alarm pictures	
		DAY	NIGHT	DAY	NIGHT	DAY	NIGHT	DAY	NIGHT	DAY	NIGHT
1	Camera 1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	2	0	4	0	2	0	6	0
2	Camera 2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	0	4	0	3	0	6	0

DAY	RAM disk requirement:	343	KBytes
NIGHT	RAM disk requirement:	0	KBytes
	RAM disk available:	16384	KBytes
	RAMDISK (A)	<input type="text" value="16384"/>	KBytes (16 Kb - 16384 Kb) <input type="button" value="Max"/>

Note: - The system must be reset after changing the value to RAMDisk (A)

Function	Description
----------	-------------

RAMDisk requirement (Day / Night / Weekend)	This is a read only section and is automatically calculated from; the [number of cameras with pre-alarm recording selected] and the [requested record size]. This will show how much of the allocated RAM disk has been taken for these settings If dual mode operation is enabled the values will be displayed for both modes
---	---

Function	Description
----------	-------------

RAM disk available	This identifies the size of the RAMDisk that is available for capturing images, this read only
RAMDISK (A)	This area is user definable and allows a portion of the RAMDisk to be allocated for alarm recording, the range is between 16KB and 2048KB

## How to Enable Audio Recording



The DV-IP Server supports two audio inputs which can allow for external audio equipment to be connected to the Server. This allows the Operator to communicate via the DV-IP Viewer software across the network to the camera location.

The audio is independent of the video inputs which means any camera can have associated audio equipment, e.g. Intercom system. The audio can also be recorded along side the video to allow review of both simultaneously. This section is divided into:

Audio setup  
Variable Rate Audio Setup

To configure and enable the audio to be recorded:

1. Select **System -> Audio Recording**
2. Enter the **title** for **Audio channel 1**
3. **Tick** the box to enable **recording** of audio **channel 1**
4. Select the **camera** that is to be **associated** with the audio channel
5. Enter the **title** for **Audio channel 2**
6. **Tick** the box to enable **recording** of audio **channel 2**
7. Select the **camera** that is to be **associated** with the audio channel



**Note:** Audio is available in Live monitoring at all times, the audio will only start recording after the Record Audio option has been enabled.

Audio Set-up		
Audio Channel	Title	Record Audio
1	Audio in	<input checked="" type="checkbox"/>
2	Audio out	<input checked="" type="checkbox"/>

Function	Description
Audio Channel	Audio equipment can be connected to the DV-IP Server to allow bi-directional audio to be integrated into the system. There are two audio channels this identifies the channel being configured
Title	This title will be saved alongside the recorded audio, ensure this has significance to the system

Function	Description
Record Audio	This option must be enabled for the audio to be recorded with the video, audio is continuously available in live mode but this option <b>must</b> be enabled for audio in record mode

## How to Configure the Video Inputs for VMD / Activity



The DV-IP Server supports VMD (Video Motion Detection) and Activity Detection on all video inputs and allows cameras to automatically detect if there is any movement/changes within the video scene.

This can then trigger a number of operations such as FTP alarm notification and increase camera recording rate for the corresponding video input.



**Note:** It is recommended that you utilise the Walk test function to ensure the settings are correct for each input enabled, if the settings are too low this will mean VMD will not be identified to high and false alarms will occur.

Configuration of VMD / Activity will be separated into three sections:

- Enabling video inputs and display options
- Configuring action on notification of motion
- Setting up the VMD / Activity area

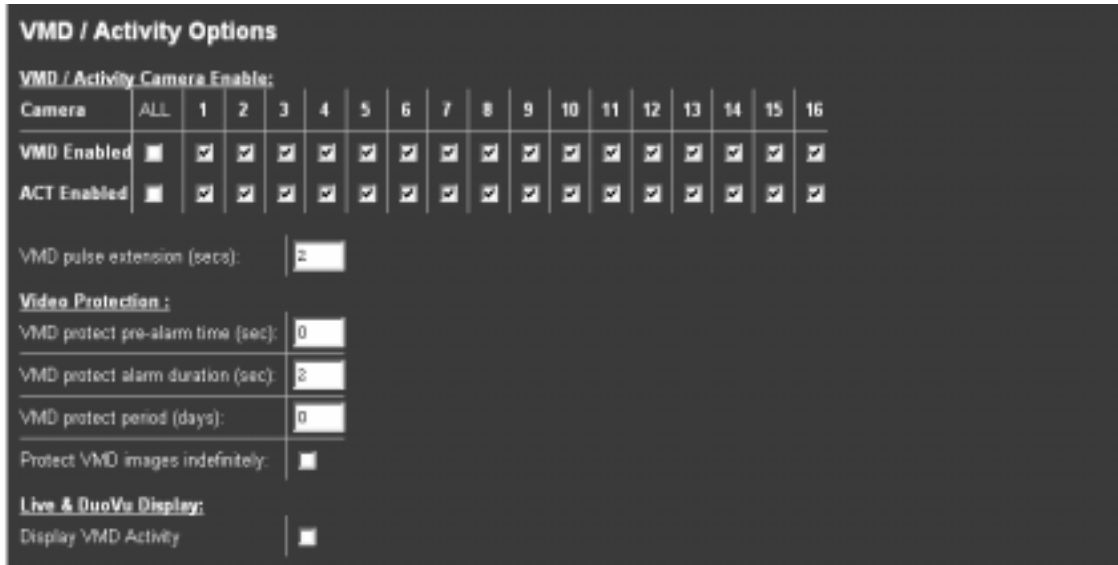
To enable individual video inputs on the DV-IP Server:

1. Select **Alarms/VMD -> VMD**
2. **Enable** the **video inputs** that require identification of movement by putting a tick next to the corresponding camera input for either VMD, Activity or both
3. Enter the **time period** with regard to the VMD settings for **pulse extension** in seconds; this is the time the alarm will last if the alarm occurrence is only for an instance, i.e. if it lasts for a second the VMD pulse extension will extend this by the time allocated to ensure all video is recorded
4. Enter the **pre-alarm** time settings in seconds, this is the time prior to the VMD trigger that is to be saved and protected from being overwritten along with the actual incident, enter the time period you require
5. The **alarm duration** is the period of time you want the VMD trigger to be active and therefore the VMD actions will occur for this period, e.g. increased recording, enter the time period in seconds

6. If **VMD actions** are to be **saved and protected** it is possible to allocate the **time period** these are to be maintained or select indefinitely. Enter the time period in days for protecting the files or tick **indefinitely**

7. It is possible to monitor the video from the **Live** and **DuoView** web pages on the server, if you want to view **VMD triggers** on these page **enable** the function by placing a tick in the box

8. Remember to save the configuration by selecting **Save Settings!**



Function	Description
VMD Activity / Camera Enable	This option allows for both VMD and Activity display to be enabled on individual or all video inputs. Tick the VMD, Activity of both boxes that correspond to the input that is to display VMD and/or Activity
VMD pulse extension	This allows you to extend the time that an alarm is valid, If there is an occurrence of VMD identified on one of the inputs and the duration is only one second in length then the pulse extension will increase this time period, this will ensure the recording contains sufficient information. <b>Note:</b> If VMD occurs again within this pulse extension it will only be acknowledged as a single trigger
VMD protect pre-alarm time	This is the time period prior to the VMD trigger where the images will be saved and protected along with the trigger itself



Function	Description
VMD protect alarm duration	This is the period of time that the VMD alarm will be in alarm mode, i.e. the period of time the alarm action allocated will be active, e.g. increased recording
VMD protect period	Any VMD entry in the database can be protected from being overwritten, this is the period of time the files will be saved and protected. After this time the files will be automatically overwritten unless specified
Protect VMD images indefinitely	It is possible to protect VMD images indefinitely to ensure any incidents are saved and protected for review at a later date. These files will remain protected until specified differently
Live & DuoView Display	It is possible to utilise the web interface to monitor live and recorded video, if the Live or DuoView are to be used it is possible to identify when VMD and/or Activity has been triggered, squares will appear over the area where there is movement

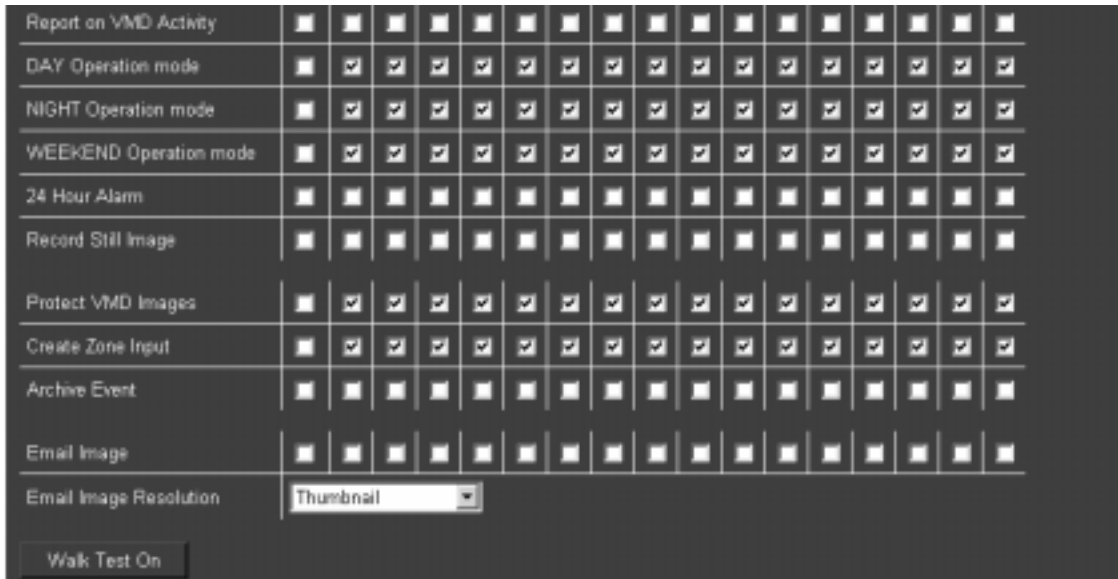
To configuring the alarm action on identification of VMD:

9. There are a number of actions that can be initiated when VMD has been triggered, each camera can be individually configured. Place a tick in the boxes of the **VMD action** that is to occur against the relevant video input

10. If an **e-mail** is to be sent on identification of an alarm it is possible to configure what information will be contained in the e-mail, using the drop down box select the **resolution** of the image to be sent

11. Don't forget to save the configuration of the alarm actions by selecting **Save Settings!**

VMD Actions:	VMD Cameras															
	ALL	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Create Database Entry	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Change Standard Record Rate	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Change Variable Record Rate	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>



Function	Description
Create Database Entry	This will record an event in the database using the VMD Zone number (refer to Alarm Zone below for more information)
Change Standard Record Rate	This will set the alarm record rate across ALL cameras that are enabled in the record sequence
Change Variable Record Rate	This will change the record rate of the corresponding camera ONLY, make sure the camera is enabled in the Camera Input page (Refer to the Quick Start Guide for enabling video inputs)
Report on VMD Activity	This will automatically send a telnet alarm message to an allocated DV-IP Viewer, when the PC receives and accepts the alarm video is then requested, refer to Alarm/VMD Reporting below for more detailed information
DAY Operation Mode	This will enable the VMD zone when the unit is in Day operation mode only.
NIGHT Operation Mode	This will enable the VMD zone when the unit is in Night operation mode only.
WEEKEND Operation Mode	This will enable the VMD zone when the unit is in Weekend operation mode only.

Function	Description
24 Hour Alarm	This will ensure that VMD is permanently enabled on the corresponding input (24/7)
Record Still Image	This will record (and mark the image by stating the word 'ALARM' in the title) still of the corresponding video input alongside the recording of the event, access to the still is via the Live Page
Protect VMD Images	This will protect the whole recorded 50 Mbyte block of video regardless of which camera(s) are recorded.
Create Zone Input	This turns the VMD camera into an alarm input when used with the Alarm Zones page, Select VMD1 instead of an alarm input to trigger the event
Archive Event	This will mark the VMD event for automatic FTP download to the FTP Server identified, refer to FTP Events Download page for more information
Email Image	This will automatically e-mail a snapshot of the VMD incident to the SMTP server identified, refer to Email configuration page for more information
Email Image Resolution	This identifies the resolution of the snapshot that will be attached to the e-mail; the options available are thumbnail, low resolution, medium resolution and high resolution

To set up each camera with a VMD / Activity grid:

12. Click on the area where **Click here to VMD applet** is located to display the video image and VMD grid, by default video input 1 will be displayed and the grid is divided into 16 zones



15. Select the **video input** you are configuring from the drop down menu

16. Select **zone** you are configuring from the drop down box.

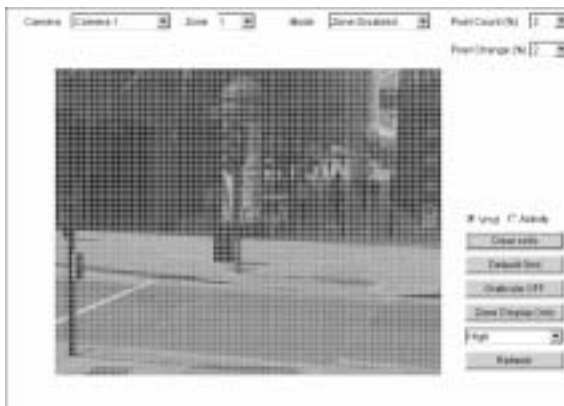


**Note:** Any configuration carried out at this stage is for the selected video input and zone, you will need to save the settings and then select another zone to configure the whole area.

17. If the default zones are not positioned over the areas you intend to allocate motion detection there is an option to **clear all cells**, you will be presented with a prompt to check you want them cells deleting, select **Yes**

18. To set a zone **click at the edge of the area** where you want to place the zone, move to the **opposite corner** where the zone will sit and click again, a zone area will be displayed over the area

19. It is possible to have a grid overlay displayed over the image to assist you in placing the zone areas, select **graticule on**



20. Select the **next zone** from the drop down box to create another zone area



**Note:** If this is incorrect then you can click again and the zone will move to the new area.

21. If you want to use the default zone settings you can select the **default grid** option, this will place 16 zones over the image. You will be presented with a prompt, select **Yes**

22. Select the **zone mode** from the drop down box that will apply to the zone you have selected in the zone drop down option

23. Set the **pixel count (%)** by selecting from the drop down box the range is between 2 and 100%, this will apply to the zone you are configuring

24. Set the **pixel change (%)** by selecting a value from the drop down box the range is between 2 and 100%, this will apply to the zone you are configuring

An example of VMD operation:

Select the zone area for monitoring activity. Set the pixel count to 20%. This determines that the unit will look at 20% of the greyscale pixels evenly distributed over the zone area.

Set the pixel change to 10%. This means if 10% of the **monitored** pixels change video motion detection will be triggered and the unit will go into VMD alarm.

25. To check you have covered the areas that you want to monitor for motion you can select to view the zone areas only, select **zone display only** and you will be presented with the areas you have highlighted



26. Selecting **full display** will show the whole image

27. Remember to save the configuration by select **Save Settings!**

### Setting Activity Detection

1. Select the **Activity** option in the Applet to display the activity grid. A 16 x 16 (16 x 14 for NTSC) grid will be displayed over the image

2. Select the camera from the drop down list which is to be configured
3. Select the Sensitivity to be applied to the setting
4. Cells can be individually added / removed or the Clear cells option will remove all cells.
5. Click on the area where a cell is to be displayed / removed or use the Default grid option to add the 16 x 16 grid.



Function	Description
Camera	This is a drop down list of the video inputs on the DV-IP Server, selecting one of the inputs will display the corresponding video source
Zone	Up to 16 VMD zones can be configured, this is a list of the VMD zones
Mode	<p>The zone mode identifies when the reference image is taken for triggering VMD. The options are:</p> <p><b>Normal</b> - the reference image is updated approx. 1/second so this will only allow small changes in the scene without triggering</p> <p><b>Last trigger</b> - the reference image is only updated when the VMD is triggered and would be used under controlled lighting, i.e. so there are no false triggers due to ambient light changes</p> <p><b>Static</b> - the reference image is collected on startup and is never updated. This would be used in 'sterile' areas where there are no changes expected</p> <p><b>Zone disabled</b> - this will disable the zone mode.</p>
Pixel Count (%)	This value is set as a percentage and equates to the percentage of pixels in the selected zone that must change for the VMD event to be triggered.
Pixel Change (%)	This setting is a percentage value of the overall change required in the greyscale to be included in the pixel count. The percentage change is defined over the complete range of black to white, a 100% pixel change would be from black to peak white.

Function	Description
Clear cells	Removes all defined zones from the image
Default Grid	Displays the default grid of 16 VMD zones over the whole image
Graticular ON	Displays a grid to assist in identifying and creating zone areas
Zone Display Only	This will display the areas of the image that are covered by a zone only and will assist you in ensuring the necessary areas are covered
Resolution	This is the resolution of the reference VMD image being displayed
Refresh	This will update the reference image to the latest view during set up
Sensitivity	This will be displayed when the Activity option is selected. This allows the Sensitivity to be selected the options are: Indoor high, Indoor low, Outdoor high, Outdoor low, Very low

## Walk Test



This is part of the configuration process and will provide you with a low resolution image to check that the settings made for VMD or activity cover the required area(s).

A thumbnail will be shown and any triggers will be displayed on this screen this will enable you to add zones if all areas are not covered increase or decrease the sensitivity, etc.

Using the Walk test will ensure that you are satisfied with the configuration and remove the need to revisit the site.



**Note:** A VMD Zone can be used to trigger an Alarm Zone, refer to How to Enable and Configure Alarms for more information.

# How to Enable and Configure Alarms



The DV-IP Server supports 17 alarm inputs which are individually configurable.

This section will be divided into:

- Enabling and configuring the alarm inputs
- Enabling and configuring the alarm actions

By default the 16 alarm inputs are disabled, these need to be enabled so that external alarm devices can be connected to the unit.

1. Select **Alarms/VMD -> Alarm Inputs**
2. Place a tick in the box under the **Enabled** option to select all the alarm inputs or individually tick the required alarm(s).



**Note:** There are 16 alarm inputs on board the unit and the option for an additional 16 alarm inputs (17 to 32) by connecting a DM alarm module to the DV-IP Server. Ensure the additional alarm module is connected to the Server before powering up the unit.

3. Select the **input** that the alarm will be triggered on from the drop down menu, select the **contact** number.
  4. Select whether the input is **Normally Open** or **Normally Closed** by default.
  5. Select whether the alarm is to be enabled as a tamper alarm (**EOL**).
  6. Set the **nuisance count**, **stuck time** and **pulse extension** for the relevant alarm input (if applicable).
  7. Remember to save the configuration by selecting **Save Settings!**
- Once the alarm inputs have been enabled it is necessary to configure what actions will be taken when an alarm is triggered.



Alarm Input Configuration								
Input	Enabled <input type="checkbox"/>	Module	Contact	Normally Closed Contact <input type="checkbox"/>	EOL Contact <input type="checkbox"/>	Nuisance Count	Stuck Time (minutes)	Pulse extension (secs)
1	<input type="checkbox"/>	AUX	Contact 1	<input type="checkbox"/>	<input type="checkbox"/>	5	10	0
2	<input type="checkbox"/>	AUX	Contact 2	<input type="checkbox"/>	<input type="checkbox"/>	5	10	0
3	<input type="checkbox"/>	AUX	Contact 3	<input type="checkbox"/>	<input type="checkbox"/>	5	10	0
4	<input type="checkbox"/>	AUX	Contact 4	<input type="checkbox"/>	<input type="checkbox"/>	5	10	0
5	<input type="checkbox"/>	AUX	Contact 5	<input type="checkbox"/>	<input type="checkbox"/>	5	10	0

Function	Description
Input	This identifies which input is being configured. The unit supports 16 on-board alarms and 16 virtual alarms plus the unit can also have an additional alarm modules connected each supporting 16 alarm inputs.
Enabled	Each input must be enabled for it to be functional; if the input is not enabled and an alarm is received the Digital Sprite 2 will not acknowledge the alarm. By default none of the alarm inputs are enabled.
Module	This identifies whether the alarm is from the onboard alarms or one of the additional alarm modules. The options are Aux, Direct, Module 1 to 16.
Contact	Identify the contact that is associated with the selected module. This option allows you to select from contact 1 to 20 for Aux, Contact 1 for Direct and Contact 1 to 16 for additional modules.
Normally Closed	This applies to both the on-board alarms and the additional alarm module, that can be connected to the Digital Sprite 2 via the 485-bus. When an input is enabled then by default it will be normally closed, removing the tick in the normally closed box makes the corresponding input normally open going closed for alarm.
EOL	The End Of Line (EOL) option enables the inputs to detect any changes in the input electronic resistance. A change outside the expected values will result in a Tamper Alarm (short circuit or open circuit) being detected as well as the system switching to alarm mode. By default the EOL contacts are disabled for each input.
Nuisance Count	This is a repetitive detector value. When an alarm is received on the unit it will store the alarm time and will monitor the number of times the same detector is triggered within an hour period. If the detector is triggered the number of times that has been set for the nuisance count then the unit will de-activate this detector from triggering an alarm on the system for an hour.  The unit will continue to monitor the detector and check how many times it is triggered during this hour, if it is triggered the same number as the nuisance counter it will remain de-activated for another hour, this will continue until the trigger value goes below the nuisance count setting.

Function	Description
Stuck Time	If any of the alarms/detectors are active for a period longer than specified in the stuck time setting then these detectors will automatically be omitted.
Pulse extension	This identifies the minimum duration of the alarm event. This time period is set in seconds



Numerous actions can be allocated to each alarm zone; this zone is a virtual zone and can encompass a single or multiple cameras. This allows a single alarm trigger to carry out any actions such as increase record cameras 1-4, send notification via FTP, etc.

It is possible to allocate up to 32 alarm zones to carry out a combination of actions.

Enabling and configuration of the alarm zones will be separated into:

- Enabling and configuring the alarm zone
- Allocating alarm actions

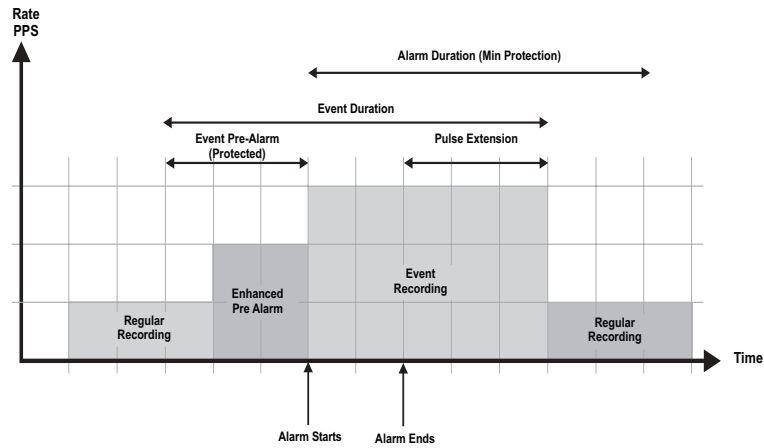
To enable and configure the alarm zone:

1. Select **Alarms/VMD -> Alarm Zone**
2. Alarms can be protected from being overwritten for a set **period of time** or **indefinitely**. Enter the time period in days that you want the alarms to be protected or place a tick in the box alongside indefinitely
3. If the **Advanced Alarm Feature** has been enabled in the Advanced Features option then you will have additional configuration information; **alarm entry time** and **alarm exit time**. Enter the time in seconds that you require for these features
4. Select the **alarm zone** you are going to configure from the drop down option (Zone 1 to Zone 32)
5. Enter an appropriate **title** to the **alarm zone**, this will be stored in the database (if enabled)
6. Enter the **time period prior** to the **alarm** that you wish to save along with the incident for review with the incident, this time is in seconds
7. Enter the number of seconds for the **alarm duration** (this includes the pre-alarm period); this is the time period that will be protected from being overwritten

8. The **zone alarm input** can be an of the external alarms (direct or 485) or any of the configured VMD zones, select the appropriate alarm input from the drop down list
9. The **Zone OR** input allows you to configure a situation where an alarm received on either of the **zone alarm input** or the **zone OR** input will force the DV-IP Server go into alarm mode and initiate pre-defined alarm actions, select the appropriate option from the drop down list
10. The **zone AND input** allows you to configure a situation where an alarm must be received on both the **zone alarm input** and the **zone AND input** to force the DV-IP Server to go into alarm mode, select the appropriate option from the **drop down list**
11. The **zone NOT input** allows you to configure a situation where if an alarm is received on the **zone alarm input** then an alarm must **not** be received on the **zone NOT input** to force the DV-IP Server into alarm mode which will initiate the alarm actions configured, select the appropriate option from the **drop down list**
12. Remember to save the configuration by selecting **Save Settings!**

Function	Description
Alarm image protect period	This is the time period in days that the alarm images will be protected from being overwritten, when this time period elapses the images will be automatically overwritten <b>Note:</b> When protecting an image it is important to remember that the DV-IP Server saves files in 50 Megabyte blocks, the whole block that contains the image will be protected. If the image overlaps into another block the all associated blocks will be protected this can start to reduce the hard disk capacity available for storing images. To unprotect images refer to System>Protect/Unprotect Images

Function	Description
Protect alarm images indefinitely	Protecting the alarm images indefinitely will ensure the alarm images are never overwritten <b>Note:</b> This section must be used in conjunction with System>Protect/Unprotect Images.
Alarm entry timer (seconds)	This is the number of seconds set for the user to disable the alarms. If the alarm is not disabled within this period then the alarm will be triggered
Alarm exit timer (seconds)	This is the number of seconds from the alarm being set to allow the user to exit the set zones. If the user is still within the set zones after this time period the alarm will be triggered
Select Alarm Zone	This is a virtual zone that can encompass a single or multiple cameras. Alarm actions to be triggered on receipt of an alarm will affect the cameras selected within this zone
Zone Title	This information is stored along with the images in the database, ensure this has relevance to the alarm trigger
Pre-Alarm Time	This is the time period in seconds prior to the alarm trigger that will be stored alongside the actual incident
Alarm Duration	This is the minimum time period in seconds from the start of the alarm that will be protected from being overwritten. This time will include the alarm trigger, the pulse extension and any post alarm recording, it will not include the pre-alarm images.



Function	Description
Zone Alarm Input	This determines which input or system function will trigger the zone alarm, the options are; Contacts 1 to 32, VMD 1 to 16, Presets 1 to 16, Keyword 1 to 16 and no contact.
Zone OR Input	The Zone OR Input identifies an alternative input that can also be used to trigger the zone alarm. This means an alarm trigger can be received on the Zone Alarm Input or the Zone OR Input for the trigger to be activated, the options available are the same as the Zone Alarm Input.
Zone AND Input	The Zone AND Input identifies that an alarm trigger needs to be received on both the Zone Alarm Input and the Zone AND Input for the trigger to be activated and the alarm action to be automatically initiated. The options available are the same as the Zone Alarm Input.
Zone NOT Input	The unit will only issue the alarm actions if the trigger is received on the zone alarm input and not on the Zone NOT input. The allocated alarm triggers available are the same as the Zone Alarm Input.

To allocate the cameras and actions that will be carried out when an alarm is received:

13. Select the cameras from the select zone **camera list**; these will correspond to the video inputs on the Server you are configuring. To select a camera **click the mouse over** the cameras these will then be highlighted. At least one camera must be highlighted at all times.

14. All of the **alarm zone actions** can be allocated to each of the zones, to select all cameras, place a **tick** in the **select all** box

15. To select individual actions place a **tick** alongside the **relevant action**, see the table below for more information on the actions listed

16. If the Advanced Alarm Features has been enabled in the Advanced Features option then additional alarm actions will be displayed, these will allow the DV-IP Server to be enabled for; **zone on entry route**, **zone on exit route**, **entry initiator** and **exit terminator**. Place a **tick** against the appropriate action(s)

17. If multiple cameras have been selected a **primary camera** must be allocated to the zone, select the corresponding camera from the **drop down list**. The primary camera is the camera that will be sent to a preset position (if selected) and a still image will be taken from this camera for e-mailing on alarm. The record still image function will add ALARM text to the title when the alarm occurs

18. It is possible to send a camera to a **preset position** on receipt of an alarm, identify the **preset number** and the corresponding **camera** that is to be switched

19. It is possible to close a **relay output** module (DM/CI02/16) which can be connected to an external device; door entry system, loudspeaker announcement system which means the system can function automatically without user intervention. Select the **relay** that is to be actioned on receipt of an alarm

20. An **e-mail** can be automatically sent to an e-mail server on alarm, identify the **resolution** of the image that will be attached to the e-mail

21. Save the information configured by selecting **Save Settings!**



Function	Description
Select Zone Cameras	This allows you to select one or more cameras that will be associated with the Alarm Zone being configured. Each camera will become part of the 'alarm sequence' when this alarm zone is triggered
Alarm Zone Actions (select all)	These are the actions that can be allocated to each alarm zone. The Select All options will tick all the boxes corresponding to the actions in the list

Function	Description
Zone on entry route	<p>This is part of the Advanced Alarms Feature and will create deferred alarms while the entry time is active.</p> <p>There will be specific alarm areas associated with the entry route, if someone enters the specified alarm areas during the entry count down process the alarm will not be triggered allowing the operator to reach the keyswitch to switch the system into an operating mode where the deferred alarms are disabled. Diverting from the entry route during the count down will result in the alarm being triggered immediately.</p>
Zone on exit route	<p>This feature is similar to a zone on entry route option, but works in the reverse, this allocates an exit route from the keyswitch to the exit allowing an operator to enable the alarm system for the premises and allow them to pass through the specified alarm areas without triggering the alarm. Diversion from the exit route will result in an alarm being triggered immediately.</p> <p>This feature is only available when Advanced Alarms are enabled.</p>
Entry Initiator	<p>This is part of the Advanced Alarms Feature. This is the count down timer that will automatically start when an entry initiator is triggered (e.g. front door) and works in conjunction with the entry route to ensure the alarm system is not activated by other alarm triggers on the entry route for this set time.</p>
Exit terminator	<p>Once the keyswitch is switched on the alarm system will wait for the exit timer to expire to ensure everyone has exited the building via the exit routes. This timer can be terminated earlier by triggering an exit terminator, e.g. closing the front door.</p>
Text Only Alarm	<p>A text message, without any image attachments, will be transmitted when the alarm zone is triggered. This may be used in situation where a camera is not associated with an alarm zone</p>
Switch System into NIGHT / WEEKEND operation mode	<p>This will switch the unit to night operation mode and assign the night operation settings to the recorded video.</p>
Create Database Entry	<p>An alarm entry will be added to the database, the zone title will be used as part of the entry information</p>
Change Standard Record Rate	<p>This will change the record rate of the cameras that have been identified in the Standard Record Rate page (refer to Camera Set-up for information on how to configure standard record rate). The cameras will switch to the alarm record rate specified</p>
Change Variable Record Rate	<p>This changes the record rate of the cameras that are selected in the alarm zone to the variable record rate previously specified (refer to How to Configure Variable Record Rate in this section of the manual). Each of the cameras must have an alarm record rate specified</p>
Connect/Dial on Alarm	<p>The DV-IP Server will automatically connect to the remote alarm monitoring station (defined). Note the DV-IP Viewer application requires an unlock code for this function to operate.</p>

Function	Description
Alarm Enabled in Day operation mode	Each alarm can be configured to be active when the unit is in a specific operation mode, enable this for the alarm to be active in Day operation mode.
Alarm Enabled in Night operation mode	Each alarm can be configured to be active when the unit is in a specific operation mode, enable this for the alarm to be active in Night operation mode.
Alarm Enabled in Weekend operation mode	Each alarm can be configured to be active when the unit is in a specific operation mode, enable this for the alarm to be active in Weekend operation mode.
24 Hour Alarm	This will force the alarm zone to be permanently active (24/7)
Record still image	This will record a still image of the trigger along with the standard recording. Still images are accessible through the Live page of the web interface. This will also add the word 'alarm' to the title header
Protect Alarm Images	Alarm images can be automatically protected from being overwritten.
Archive Alarms	This will force the alarm images to be automatically sent via FTP to a central FTP server, refer to How to Set up Connect on Alarm in this section of the manual
Primary Camera	This is the primary camera and will be the image displayed when the event is triggered, it is also the input the snap-shot will be taken from if e-mail image is selected
Goto Preset	It is possible to action one of the selected cameras to go to a preset position when an alarm zone is triggered
Close Relay	Any of the On-board or external relays can be configured to automatically close on receipt of an alarm, the options are On-board relays 1 to 4 (if not pre-defined within the System -> Relay Set-up page) relays R5 and R6 and Module 1 Relays 1 to 16
Email Image	When e-mail on alarm is enabled it is possible to attach an image to the e-mail, the resolution of the image must be defined. It is important to consider the speed of the link between the DV-IP Server and the SMTP Server that the e-mail will be sent to. The resolution options available are; thumbnail, high resolution, medium resolution and low resolution



# How to Configure Alarm Presets

The DV-IP Server supports the ability to automatically send a camera to a preset position on the receipt of an alarm.

Within this web page it also possible to identify if the alarm is to be available as a trigger for an alarm zone. To enable and configure alarm presets:

1. Select **Alarms/VMD -> Alarm Presets**
2. Select the **camera** that will be sent to the preset position from the drop down list.
3. Enter the **pulse extension** in seconds.
4. Select **Aux, Direct** or the **Module** number from the drop down list that the input will be triggered from.
5. Select the **contact** number for the Aux input or the Module. Direct will default to contact 1.
6. Identify if the input is **normally open** (not ticked) or **normally closed** (ticked).
7. Enter the **preset position** that the camera is to move to when the alarm is triggered.
8. Select whether the alarm is to be available as a **zone trigger**.
9. Remember to save the configuration by selecting **Save Settings!**



Function	Description
----------	-------------

Select Camera	Select the camera that is to be configured.
---------------	---

Pulse extension	The pulse extension extends the trigger to avoid double triggers of alarms from occurring, i.e. if a second incident is received, after the first alarm has finished but within this time period, the unit will not create a new event.
-----------------	---

Function	Description
Module Number	This identifies the alarm input that will be the trigger for the camera being configured, the options available are the Auxiliary input and Module 1 to 16 for the additional alarm modules that can be connected to the Digital Sprite 2.
Contact Number	The Auxiliary input and the additional alarm modules support sixteen input contacts any of these can be allocated as the alarm input trigger.
Normally Closed Contact	The alarm trigger can be configured as normally open (default) or normally closed.
Preset	The preset position is the position the camera will move to when the alarm is triggered.
Zone Trigger	It is possible for a camera specific alarm to also trigger an alarm zone. If the input is to trigger a zone as well as send a camera to a preset position this option must be enabled.

## How to Configure the Relay Connections



The DV-IP Server supports a number of On-board relay connections and can also integrate additional relay modules via the 485 bus connection.

These relays can be triggered under specific conditions; on receipt of an alarm, notification of VMD, etc or they can be permanently allocated for set functions.

This section details how to enable the default actions for a number of on-board relays. If the defaults are not set this allows the onboard relays to be available to be automatically triggered on alarm, this is configured within the **Alarm/VMD -> Alarm Zone** option.

To enable the default relay settings

1. Select **System -> Relay Setup**. There are five default settings that can be enabled which are directly linked to a relay connection
2. Select the associated **input** that will trigger when the system to identifies: a global alarm, global VMD, camera failure, schedule notification, primary signalling failure, weekend notification. The input options are Aux and Module 1, Module 2.



**Note:** The Schedule Notification, Primary Signalling Failure and Weekend Notification are only available when the Advanced Alarms option is enabled.



**Note:** If any relays are enabled for the default settings the corresponding relay test option will be removed from the Close Relay list in the Alarm Zone page, refer to the previous section for more information.

Relay Set-up		
Global Alarm:	AUX	Relay 1
Global VMD:	AUX	Relay 2
Global Camera Fail:	AUX	Relay 3
Schedule Notification	AUX	Relay 4
Primary signalling failure	AUX	Relay 5
Weekend Notification	AUX	Relay 6

Function	Description
Global Alarm	If an alarm trigger is received on any of the alarm inputs on the DV-IP Server then it is possible to allocate the relay connection to close, this in turn will trigger the peripheral device that is connected to the relay. The default relay is Relay 1
Global VMD	If VMD is activated on any of the enabled video inputs on the DV-IP Server then it is possible to allocate the relay connection to close, this in turn will trigger the peripheral device that is connected to the relay. The default relay is Relay 2
Global Camera Fail	If any of the enabled video inputs detect that their video signal has gone below 1 volt peak-to-peak then it is possible to allocate the relay connection to close, this in turn will trigger the peripheral device that is connected to the relay. The default relay is Relay 3
Schedule Notification	The unit can identify a switch between operating modes (Day, Night, and Weekend). The schedule notification relay is closed when the unit is switched out of Day operation mode. Any of the AUX relays or the additional relay modules can be selected.
Primary signalling failure	The unit can be configured to transmit alarm notification to a remote monitoring station. This notification normally will go via the primary route as configured. If for any reason this fails it is possible to configure the unit to automatically trigger this relay to give notification of this failure. Any of the AUX relays or the additional relay modules can be selected.
Weekend Notification	This option allows the Digital Sprite 2 to notify the Operator that the unit has been switched into weekend operation mode by automatically closing the relay output when this occurs. Any of the AUX relays or the additional relay modules can be selected.

## How to Configure Connect/ Dial, FTP, SMS and Email on Alarm

As described in the Alarm Zone section above there are a number of actions that can be initiated when the DV-IP Server is receipt of an alarm trigger.

For these actions to operate correctly there are additional configuration requirements; address of the DV-IP Viewer, FTP server address, SMS and GPS settings and SMTP Server address. Without this information the DV-IP Server would not have a route to transmit images on receipt of an alarm/VMD.

This section will be separated into the configuration processes required to enable these functions to operate.

### How to Configure Connect/Dial on Alarm



It is possible to force the DV-IP Server to transmit a message to an allocated DV-IP Viewer on receipt of an alarm; this connection can be via the Ethernet port of the Server or via a dial up connection via the serial port of the Server.

The message will be transmitted to the remote station to notify them of an alarm on the system. The operator can then make a connection to the unit to verify and action the alarm response.

There are two modes of configuration depending on the route of the alarm message. For Ethernet the system can be configured wholly using the web interface pages when using the modem link, also referred to as PPP (Point to Point Protocol) then it is necessary to edit the 'profile' file within the \etc directory of the Server.

At this stage it is presumed that the DV-IP Server, is installed with a modem connected to a serial port and/or is connected to the Ethernet network and has been allocated an IP address but the serial port has not been enabled for PPP.

This section will be separated into:

- Enabling PPP for dial into the Server
- Enabling PPP and identifying specific modems for dial up
- Configuring Alarm/VMD Reporting via the web and editing the profile.ini file

### How to Enable and Configure PPP via Serial Port



The DV-IP Server supports PPP via serial connectivity and also over the network connection. The following identifies the parameters that require configuration to allow a PPP connection to be made via the serial interface.

To enable PPP and allocate a modem:

1. Select **System -> Serial Ports & Telemetry**
2. Using the drop down list on the associated serial port (**Serial 1 or 2**) select **PPP**



**Note:** PPP Link 1 is allocated to Serial 2 for dial out on alarm and PPP Link 2 is allocated to Serial 1 for dial in.

3. Select the relevant **modem** from the **Modem/TA** drop down list, if your modem is not supported select **generic**



**Note:** Auto detect will only auto detect the modems the Server recognises.

### Supported Modems

Generic AT Modem	3Com US Robotics 56K Modem
3ComImpact II	Falcom GSM Phone / Modem
KTX 33600 – Modem	PLANET Smart IP
PSL - ISDN TA	Nokia30 GSM
Nokia30 HSCSD V.110	Nokia30 HSCSD V.120
SHIVA LanRover	Siemens TC35GPS / MC35 GPRS
Spider 4 CDPD Modem	Zyxel Omni-net.D - ISDN TA

4. The **serial standard settings** for the selected modem will automatically be allocated, however if this is incorrect you can change these for:

- Baud rate, Parity, Data bits, Stop bits, Flow control  
115200, 0, 8, 1, HARDWARE

5. Remember to save the configuration by selecting **Save Settings!**
6. **Reset** the DV-IP Server for the unit to initialise the modem.



**Note:** For Connect on Alarm to function the Remote Alarm Monitoring function of the DV-IP Viewer must be unlocked, contact Dedicated Micros Customers Services for more information.

## How to Configure the Remote Alarm Host Information web Interface

When an alarm is triggered the DV-IP Server will send a message via the serial port or over the network using PPP.

This section identifies the details of the receiving station and the route the message will take.

When using the Ethernet network to transmit the alarm message all configuration for the remote receiving station can be carried out using the web interface, to enable PPP via a modem the 'profiles' (etc/profiles) file will need to be edited.

To configure the 'profiles' file:

1. Using an **FTP client** application connect to the DV-IP Server
2. Locate the **etc** directory and expand
3. Locate the **profiles** file
4. Highlight and press the **right mouse button**, select **view**
5. The profile information will be displayed, enter the information regarding the **modem link; Username** (& Profile Label), **Password, Port, Phone No, IP Address Range, Subnet Mask.**

The port options available are

PPP\_Link1 = Serial 2  
PPP\_Link2 = Serial 1  
Ether = Ethernet



**Note:** The port option is case sensitive, entering the information incorrectly will result in the function not operating. It is recommended that Serial 2 be used for PPP for the serial options as Serial 1 is by default set as Debug and this would still enable serial communication with the unit.

An example of the profiles file is shown below:

```
#-----  
#Profiles Table List  
#-----
```

<Username>	<Password>	<Port>	<Phone No>	<IP Address Range>	<Subnet Mask>
dm	password	PPP_Link2	1234567890	10.0.0.1	255.255.255.0
username	password	PPP_Link1	1234567890	10.0.0.1	255.255.255.0
test	password	PPP_Link1	1234	10.0.0.1	255.255.255.0

The username will also be the profile information that will be entered in the web interface page.



**Note:** The username and password must be unique and they will both be case sensitive.

6. **Save** the file and **upload** back onto the DV-IP Server. You will now need to add this information to the **Alarm/VMD Reporting** page via the web interface

7. **Reset** the DV-IP Server.



**Note:** It is possible to identify the host information, as displayed on the web page, within the hosts file in the \etc directory.

To configure the remote alarm station information using the web interface:

1. Select **Alarms/VMD -> Alarm/VMD Reporting**
2. Enter the **IP address** of the **primary remote host**, this is require for connections via the network and via the serial ports
3. When making a connection via the Ethernet network enter **Ethernet** to identify the medium by which the connection will be made. Alternatively for dial up connections via the modem enter the **username** previously configured in the '**profiles**' file, the example above would result in the profile entry being dm
4. Enter the **IP address** of the **secondary host**; this is in case the primary host can not be contacted
5. Enter the medium how the DV-IP Server will connect to the host; **Ethernet** or the **username** as identified in the 'profiles' file
6. When using **NAT** enter the IP address that will be used for the public address
7. Enter the **video server port** number when port forwarding is required
8. Identify the **Unit Alarm name**; this is the name that will be presented to the remote alarm station and must match the name that has been allocated in their site tree
9. For the system to **dial on alarm, camera fail, tamper alarm** and **system startup** these functions must be enabled, place a tick in the box associated with the function
10. Enter the **time delay** between the Digital Sprite 2 trying to connect to the remote monitoring station after a failed connection.
11. Enter the number of times the DV-IP Server is to **re-try** to connect to the remote monitoring station, a value of 0 means no limit is set and therefore the unit will continue to re-try until a connection is made, this should be taken into account when using a dial up connection

12. This **telnet server port** is the port that the receiving station will have allocated to list for alarm message from the DV-IP Server, if these port address do not match the function will not operate

13. Save the configuration by selecting **Save Settings!**



**Note:** It is necessary to have a 'telservers' application enabled when using NetVu ObserVer or have the telservers function on the DV-IP Viewer software enabled, of the PC that will be utilised for remote alarm monitoring, refer to the Viewer manuals for more detailed information.

14. It is necessary to configure the PPP settings on the unit, select **Network -> Network Settings**, enter the **PPP IP address**.



**Note:** The PPP IP address must be in the same network range as the Alarm Receiving Centre.

15. Enter the **PPP Idles Line Timeout** and the **PPP Link Down Timer** to determine how the unit will transmit information via PPP, these settings should be discussed with the Network Manager.

The screenshot shows the 'Alarm Connection Settings' interface. It features a table for host and profile configuration, followed by various input fields and checkboxes for additional settings.

	HOST	PROFILE
Primary:	172.16.80.5	etelnet
Secondary:	172.16.80.10	etelnet

Public (NAT) IP Address: [ ]

Video Server Port (Port forwarding): [0]

Unit Alarm Name: [09]

Remote Alarm Reporting:

Remote Callfail Reporting:

Remote Tamper Reporting:

Remote Startup Reporting:

Dial Retry Time: [1] (minutes)

Dial Limit: [0]

Alarm Telnet Server Port: [23]



Function	Description
Primary Host	This is the IP address or name of the initial host that the DV-IP Server will transmit an alarm message to
Secondary Host	If the DV-IP Server is unable to contact the primary host then it is possible to identify an alternative route and a secondary host If there is only one alarm receiving IP address, you must enter the details in both the primary and secondary connection settings
Profile	This is the medium that the DV-IP Server will use to make the connection to the primary or secondary host. <b>Note:</b> If the connection is via the serial port the profile will be the username configured in the 'profiles' file in the /etc directory on the DV-IP Server.
Public (NAT) IP Address	This is public IP (or domain name) for a unit connected to the Internet via a NAT Router or Firewall. This field should be left blank if NAT is not used e.g. on a private network.
Video Server Port (port forwarding)	This field allows the ARC to connect to the unit through a router that is using port forwarding e.g. if the video server does not appear on port 80 (HTTP) to the external network.
Unit Alarm Name	This is the name that will be presented to the remote alarm viewing application and therefore should have some significance to the Operator. This name <b>must</b> match the defined folder name in the DV-IP Viewer PC folder tree
Remote Alarm Reporting	This must be enabled for the DV-IP Server is to automatically connect on alarm, it must also be enabled in the Alarm Zone option
Remote Camfail Reporting	If the DV-IP Server identifies camera failure on any of the inputs enabling this option will force the Server to connect to the remote alarm station
Remote Tamper Reporting	This is part of the Advanced Alarm Features and will send an alarm report when the DV-IP Server has identified a tamper alarm
Remote Startup Reporting	This is part of the Advanced Alarm Features and will send an alarm report when the DV-IP Server starts up, this will identify any system resets
Dial Retry Time	If the initial connection attempt fails then the DV-IP Server will wait for the specified time period before attempting to re-connect

Function	Description
Dial Limit	This identifies the number of times the DV-IP Server will attempt to connect to the remote alarm monitoring station after a failed attempt, a setting of 0 identifies no limit and the Server will continue to try and connect until it is successful
Alarm telnet Server Port	This specifies the network port number to use for reporting to the alarm server. This is normally left at the default value.

## How to Configure FTP Settings for Archiving Images



The DV-IP Server can transmit images via FTP (File Transfer Protocol); this can be on receipt of an alarm or VMD using a scheduled time to backup the video.

In a multi-unit application this will ensure that one central location stores all the files from each of the DV-IP Servers, offering efficient file management and easier review capabilities.

To configure the FTP information:

1. Select **Network -> FTP Events Download**
2. Enter the information on the **FTP Server**; this can be an IP address, full URL or name of the server
3. It is possible to identify the **FTP control port**, the default for networks is usually port 21 however if this port number is not supported on the network, then this option allows you allocate an unused port number
4. Enter the **directory information** where the images are to be stored, this should be a name associated with the DV-IP Server name for ease of retrieval
5. For files to be saved to the FTP Server it is necessary to go through an **authentication process** to gain access to the server, enter the **username** and **password**
6. It is possible to enable the DV-IP Server to **start an FTP download** when an **active Ethernet** connection is detected.



**Note:** As the DV-IP Server always has a permanent network connection the Active Ethernet option means when the Network port identifies a change in state of the Ethernet link (down to up), for example when the DV-IP Server is reset or the network cable is unplugged then re-connected.

7. If the FTP download is to happen **automatically** at a **set time** each day, enter the required time in the **scheduled time** option or

8. It is possible to enable an FTP download and more regular intervals by enabling the **polled** option, once enabled identify the **time period** between the end of one FTP download to the start of the next or
9. If the FTP download is only to be initiated by the **Operator** then enable the **manual download** option. The FTP download will only commence when the **Start Download** button is selected
10. To automatically **remove the image protection** from files that are **downloaded** then enable the **clear video protection after download** option. If this is not enabled the images would require un-protecting manually via the Alarm Image Protect/Un-Protect page
11. It is possible to allocate a **watermark** for each video partition; this watermark information is logged in the **log file**. Enable this function by selecting **watermark each partition download** option
12. The server directory is a fixed directory structure, all FTP downloads will be saved in the directory name you have identified under this main directory. This a read only section
13. Remember to save the configuration by selecting **Save Settings!**

**FTP Events Download Settings**

FTP Server (IP, URL or name):

FTP Control Port (Default 21):

FTP Root Drive/Directory:  e.g. C:/images/

Username:

Password:

**Download options**

On Connection:

Scheduled:   Schedule time (hh:mm)

Polled:   Poll time (Minutes)

Manual only:

Clear video protection after download:

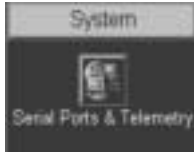
Watermark each partition after download:

Server Directory: "/>

Download video on demand:

Function	Description
FTP Server	This is the IP address, URL or name of the FTP server the DV-IP Server will connect to for FTP download of images
FTP Control Port	The default port for FTP is port 21, if this port has already been allocated on the network it is possible to identify and alternative port number
FTP Root Drive/Directory	This is the directory where the images are to be stored, it is recommended that a name associated with the unit name be used for ease of retrieval
Username	To access an FTP Server it is necessary to go through an authentication process, this is the username for you to gain access to the FTP Server
Password	To access an FTP Server it is necessary to go through an authentication process, this is the password for you to gain access to the FTP Server
On Connection	This will automatically start the FTP download when the unit detects a change in state of the Network port (down to up)
Scheduled and Schedule time	It is possible to force the DV-IP Server to FTP images at a scheduled time. The time entered will be the time each day that this function will be activated
Polled and Poll time	This will set the DV-IP Server to activate FTP download at regular intervals, the time period is in minutes and is the time between the end of one FTP download to the start of the next
Manual only	The FTP action will only commence when the User initiates the action by pressing the FTP download option
Clear video protection after download	This automatically clears the image protect from the images that are successfully downloaded
Watermark each partition after download	This enables a watermark to be generated and stored in a text file downloaded with the video to the FTP server for each image partition, this watermark is logged in the log file
Server Directory	This is the main directory on the FTP server where the images will be stored. The Root Drive/Directory will be created under this main directory. This is read only
Start Download	This allows the user to manually initiate an FTP download

## How to Configure SMS Text messaging



The DV-IP Server supports the function to send an SMS text message to a SMS Server for forwarding to a mobile phone.

This gives the ability to automatically or manually action the DV-IP Server to send a text to inform a Guard of incident when they are away from the monitoring station, i.e. Security check of the site, mobile security units, making sure the site is monitored 24/7 whether the Guard is at the site or mobile.



**Note:** Delivery of an SMS message can not be guaranteed. This is a limitation of the communications network providers not with the Dedicated Micros DV-IP Server.

The typical process for SMS messaging is:

The DV-IP Server will send a message to the mobile phone. This can be on receipt of an alarm or manually initiated.

The operator then has the option to send a message back to the Server or log onto the unit using the web interface or DV-IP Viewer software.

If the Operator is remote they can send a message back to the DV-IP Server to action the Server to send an alarm message to a remote viewing application. The DV-IP Server will send a message to the remote monitoring station which includes the information in the text it has received

The remote station can then access the DV-IP Server to acknowledge and action the alarm.

To enable the serial port for the SMS feature:

1. Select **System -> Serial Ports & Telemetry**
2. Using the drop down list on the associated Communication port (**Serial 1** if dial on alarm is enabled) select **PPP**
3. Select the relevant modem from the **Modem/TA** drop down list, if your modem is not supported then you will need to add the modem to the **modem.ini** file
4. The **serial standard settings** for the selected modem will automatically be allocated, however if this is incorrect you can change these for:
  - Baud rate, Parity, Data bits, Stop bits, Flow control

5. Remember to save the configuration by selecting **Save Settings!**

To edit the modem.ini file for **modems which are not identified in the dropdown list** of supported modems:

1. Using an **FTP client** application connect to the DV-IP Server
2. Locate the **letc** directory and expand
3. Locate the **modem.ini** file
4. Highlight and press the **right mouse button**, select **edit**
5. Enter the information for the GSM Modem being used, an example of the information is shown below:

```
[N30HSCSD]
name=Nokia30HSCSD
reset=AT&F
init=ATE0&C1&D2S0=1+CMGF=1;+CBST=16,0,1
save=AT&W
negate_dtr=0
```

To configure the SMS information to allow a text message to be transmitted on receipt of an alarm:

1. Select **Network -> SMS-Setup**
2. Enter the **GSM destination number** of the mobile phone, this should be entered in international format including the country code
3. It is possible to make the DV-IP Server into an **SMS Server** by enabling the SMS Server option. If this has been enabled then you need to enter the **destination URL** or **IP address** of the DV-IP Server. This will allow the message to be sent from a DV-IP Server to a DV-IP Server
4. Enable the operations that are applicable to your application; **Report startup, alarm, camera fail, and VMD activation**
5. **Verbose messages** must be enabled to ensure the text message is in a human readable format. Tick the box adjacent to the relevant function
6. Enter the **callback profile** in 0 and 1, this is the route the text message from the Operator will take when sending a message back to the DV-IP Server
7. Enter the **password** to enable **SMS commands** to be initiated. This password will be included in the text message from the Operator
8. Select the **advanced setup** button to enter details on the **GSM module** that will be used in the system

9. Enter the **service centre number**, this is the network service centre number of the mobile phone, this information can usually be found on the phone in **Messages -> Message Settings -> Profile -> Message Centre Number** based on a Nokia phone menu
10. Enter the **pin number** for the **SIM card** (if applicable)



**Note:** If a pin has been set the number must be entered each time changes are made to this page and is submitted (Save Settings).

11. Enter the **GSM/SMS port number** that will be used for this function to operate on
12. Remember to save the configuration by selecting **Save Settings!**

Function	Description
----------	-------------

Destination Number	This is the GSM number for the SMS server. The format should be entered in international format including the country code and local area code
Destination URL	This can be the URL or the IP address of the SMS Server when utilising SMS over TCP/IP. The messages will be sent over an Ethernet link if present, alternatively it will be sent over the GSM network

Function	Description
SMS Server	This will enable the DV-IP Server to accept and log SMS messages. <b>Note:</b> The Verbose option must not be enabled when this option is selected
Report startup	This will enable the DV-IP Server to transmit a message on power up of the unit
Report alarms	Sends a text message on receipt of an alarm via the On-board or additional alarm inputs
Report camera fail	If any of the enabled video inputs on the DV-IP Server does not detect a 1 volt peak-to-peak signal then the unit will send a SMS message
Report VMD activation	If VMD is identified on any of the enabled video inputs the unit will send a SMS message
Verbose messages	This will send a SMS message in a readable format to a mobile devices (e.g. mobile phone). <b>Note:</b> This format is not supported in standard SMS Servers
Callback profile	This identifies the route the return message, from the Operator mobile device, will take. The return message must contain the SMS command password, callback IP address (IP address of the remote PC with the DV-IP Viewer application) and the command to action the DV-IP Server to call the remote station
SMS command password	This is the password to enable the SMS commands to be initiated and will be included in the return text from the Operator
Last signal strength	This is a read only section and identifies the signal strength of the GSM module
Last bit error rate	This is a read only section and will detail the error rate of the GSM module

**GSM Module Administration**

Service Centre Number

GSM PIN number  [See Note 1](#)

GSM/SMS port

**NOTE 1:** If the SIM requires a PIN, it must be re-entered everytime this page is submitted

[Return to SMS Setup](#)



Function	Description
Service Centre Number	This page is specific to the GSM module connected to the DV-IP Server, this is the number for the service centre that will be responsible for the SMS message
GSM PIN Number	This is the pin code for the SIM card in the mobile device that will receive the SMS message. If any changes are made to this page the Pin number must be re-entered each time
GSM/SMS Port	This is the port address that will be used for the SMS message to be transmitted/received

### SMS Message Format

There is a specific format for the text message that is returned to the DV-IP Server, the format is detailed within this section. It is important that the message format be strictly adhered to for this function to operate. Further message formats can be found in Appendix F along with information that can be obtained from the DV-IP Server.

CALLBACK?<password>&<destination>&<profile>&<text>

password	This is the SMS password that has been identified in the SMS Set-up page and enables the command to be executed
destination	This is the IP address or DNS name of the Viewing application that has telserve/DV-IP Viewer (Telnet listener) enabled to receive the message
profile	This can be a number or name that has been configured on the SMS Set-up page, this will be via the serial port or Ethernet connection
text	This is the text message that will be sent to the remote viewer informing the Operator of an incident and therefore should be meaningful

## How to Configure Email Settings



The DV-IP Server can automatically transmit and e-mail to an SMTP Server under numerous conditions; on start up of the DV-IP Server, on receipt of an alarm, camera failure and notification of VMD.

This allows the DV-IP Server to be installed in unmanned applications where a Remote Monitoring Station (or Manager, etc) would be notified, by e-mail, if any of the above conditions occur.

To configure the settings to allow e-mails to be transmitted:

1. Select **Network -> Email**
2. Enter the **connection profile**; this can be Ethernet if the e-mail is to be transmitted over the LAN or WAN or named profile if using a dial up connection

3. Enter the **IP address** or the **DNS name** of the **SMTP Server** the e-mail will be sent to
4. Enter the **e-mail address** that the **SMTP server** should **forward** the e-mail to
5. If applicable **enter the display name** for the e-mail address
6. Enter the **e-mail address** that the recipient is to **reply to**, this is only applicable if a reply is required and must be filled in for this to happen
7. If applicable enter the **display name** of the reply e-mail address



**Note:** The DV-IP Server can not receive e-mail replies this must be a valid e-mail address.

8. It is possible to identify where the **e-mail** has be **sent from**, this is optional if this are is left empty the video server will use the system name & DNS name to create a sender name
9. The DV-IP Server can be forced to send an e-mail under numerous conditions; **start up** of the Server, on **alarm** (this must also be enabled in Alarm Zone page), **camera failure** and **VMD activation** (this must also be enabled in the Alarms/VMD page). Place a **tick** against the actions that are applicable to your systems functional requirements
10. Place a **tick** in the **e-mail log** box to ensure ever e-mail transaction is added to the system logs
11. Save your configuration by selecting **Save Settings!**

**Email Logging**

Connection Profile

Mail Server

	Email Address	Display Name
Recipient	<input type="text"/>	<input type="text"/>
Reply to	<input type="text"/>	<input type="text"/>
Sender	<input type="text"/>	<input type="text"/>

**Email Reports**

Startup

Alarms

Camera fail

VMD activation

Email Logging

Function	Description
Connection Profile	It is possible for the e-mail to be transmitted via the Ethernet network or dial up connection. This setting presumes that a modem has been connected and configured and the DV-IP Server is connected to a LAN or WAN and allocated a valid IP address
Mail Server	This is the IP address or DNS name of the SMTP Server that the e-mail from the DV-IP Server will be sent to. The SMTP server will then forward this onto the recipient <b>Note:</b> You must ensure the DNS Server address in the Network Settings is correctly configured to be able to use DNS instead of the IP address.
Recipient	This is the e-mail address and display name of the intended recipient of the e-mailed image
Reply to	This field must be configured if the recipient is to reply to an e-mail. The DV-IP Server does not accept e-mails so this must be a valid e-mail address
Sender	These optional fields indicate the source of the e-mail notification. If the fields are left blank the DV-IP Server will use the system name & DNS name to create a sender name
Email reports	These are the conditions under which the DV-IP Server will transmit an e-mail; when the DV-IP Server has been reset, when an alarm zone has been triggered, if any of the video inputs has detected camera failure, if VMD has been identified on any of the enabled video inputs
Email Logging	A log can be created for every e-mail transaction that the DV-IP Server issues

## How to Protect or Un-protect Images



Images stored on receipt of an alarm can be automatically protected within the corresponding alarm configuration page.

In addition it is possible to protect images that are stored on the hard disk and have not been protected, or increase the time period allocated for protecting the image.

Alternatively it is also possible to highlight protected recordings and un-protect these so they can be overwritten.

To protect existing recorded images

1. Select **Alarms/VMD – Alarm Image Protect/Unprotect**

2. If there are any existing protected images these will be displayed within the **protect image partition summary**, enter the **start** and **end time** and **date** to display the corresponding recordings

3. **Highlight** the **recorded file** in the **protect image partition summary**

4. Enter the **time period** that images are to be protected in the **protect image** option or select **protect images indefinitely** for these never to be overwritten

To unprotect existing protected images

1. Select **Alarms/VMD – Alarm Image Protect/Unprotect**

2. Highlight the **recorded file** in the **protect image partition summary**

3. Select **un-protect images**, this will remove the protection from the files, release the hard disk space these files where stored in and the files will now be overwritten

Function	Description
----------	-------------

Start Date and time

This allows you to enter the start time and date for the period you wish to search for recorded images

Function	Description
End Date and time	This allows you to enter the end time and date for the period you wish to search for recorded images
Protect Image Partition Summary	The recorded files will be displayed within the area. These are then selected to either unprotect or protect
Unprotect Images	Any images that have been previously protected and are selected in the protect image partition summary section will be unprotected, these files will then be overwritten
Protect Images	Any images that have not been protected or require the protect period extending can be selected in the protect image partition summary and then the time the images are to be protected can be identified in days
Protect Images Indefinitely	If images are never to be overwritten they can be protected indefinitely

## How to Configure the Alarm Database



The DV-IP Server supports numerous logs which will store information on the actions and processes the DV-IP Server carries out.

As we have identified the alarms and enabled these to function it is necessary to ensure the database can support and register all the configured alarms.

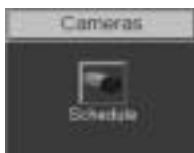
To configure the database parameters:

1. Select **Alarms/VMD -> Database Configuration**
2. The **last database reset time** will be displayed; this is a **read only** section
3. The **current number of entries** in the database will be displayed; this is a **read only** section
4. Enter the **maximum number of entries** for the database file, once this figure has been reached the database will 'wrap round' and start entering over the top of entry 1
5. To **reset the database** select **Save Settings**, you will then be prompted to reset the database, select **OK** to reset or **cancel**

Database Configuration	
Last database reset time:	08 February 2005 10:48:55
Current number of entries:	155
Maximum number of entries:	<input type="text" value="1000"/>

Function	Description
Last database reset time	This is a read only section and is generated by the DV-IP Server, it identifies the last time that the database was reset
Current number of entries	This is a read only section and is generate by the DV-IP Server, it identifies the current number of entries in the database
Maximum number of entries	This is the maximum number of events that will be logged in the database. When this figure is reached the database will start overwriting the entries starting at entry 1.

## How to Configure an Alarm Schedule



Now that all the alarm settings have been configured we need to identify when the alarms are to be active.

It's possible to utilise the On-board schedule function of the DV-IP Server to enable and disable alarm triggers and VMD activation. This can reduce unnecessary alarm triggers, e.g. during office hours it would be unnecessary to have VMD active.

To Set the Schedule function we will use a typical example,

- Monday to Friday – Alarms/VMD are not active from 08:30
- Monday to Friday – Alarms/VMD become active from 18:30
- Weekend – Alarms/VMD are active all weekend

1. Enter **24:00** in the **Set** box adjacent to **Sunday** and **Saturday**
2. Enter **24:00** in the **Unset** box adjacent to **Sunday** and **Saturday**
3. Enter **18:30** in the **Set** box adjacent to **Monday, Tuesday, Wednesday, Thursday and Friday**
4. Enter **08:30** in the **Unset** box adjacent to **Monday, Tuesday, Wednesday, Thursday and Friday**

5. Save the information configured by selecting **Save Settings!**

The example on the menu page shows how the schedule option can be configured.



**Note:** 24:00 -24:00 = Alarms/VMD 24 hour enabled, 00:00 – 00:00 = Alarms/VMD disabled.

**Schedule**

E.g - Mon - Fri Alarms/VMD not active at 08:30  
 Mon - Fri Alarms/VMD active at 18:30  
 Alarms active all weekend.

NIGHT Time		DAY Time		NIGHT Time		DAY Time	
Sunday	00:00	Sunday	00:00	Sunday	24:00	Sunday	24:00
Monday	00:00	Monday	00:00	Monday	18:30	Monday	08:30
Tuesday	00:00	Tuesday	00:00	Tuesday	18:30	Tuesday	08:30
Wednesday	00:00	Wednesday	00:00	Wednesday	18:30	Wednesday	08:30
Thursday	00:00	Thursday	00:00	Thursday	18:30	Thursday	08:30
Friday	00:00	Friday	00:00	Friday	18:30	Friday	08:30
Saturday	00:00	Saturday	00:00	Saturday	24:00	Saturday	24:00

Function	Description
----------	-------------

Schedule	This is a seven day schedule that allows alarms and VMD to be enabled or disabled at times during the day
----------	---

DAYTime	This identifies the time when the Digital Sprite 2 will switch to Day operation mode.
---------	---

NIGHTTime	This identifies the time when the Digital Sprite 2 will switch to Night operation mode.
-----------	---

6. If **Weekend** operation is to be active, **enable** the option and configure the **start** and **end** times, weekend settings will be applied to the recorded video during this time period.

WEEKEND Enabled

WEEKEND Start Sunday 00:00

WEEKEND End Sunday 00:00

24:00 - 24:00 = Alarms/VMD 24 hour enabled  
 00:00 - 00:00 = Alarms/VMD Disables

Reset \*Please reset after updating times

Function	Description
----------	-------------

Weekend Enabled	Enabling this option will switch the unit to weekend mode settings at the time and date selected.
-----------------	---

Function	Description
----------	-------------

Weekend Start / End	This identifies the time when the Digital Sprite 2 will switch to Day operation mode.
---------------------	---

7. Select the **schedule type** from the drop down list.
8. Disabling the **record schedule rates** would result in the day, night and weekend record settings being replaced by a single 'Rate' record setting.
9. Enter the **titles** that will be associated with the **dual mode** operation
10. If the **keyswitch** is to be functional, enable the option.
11. Select the **input** that will be used to trigger the keyswitch.
12. Select whether the keyswitch is **normally open** (default) or **normally closed**.
13. Save the configuration by selecting **Save Settings!**

It is possible to use a combination of the keyswitch and the schedule option. If an operator forgets to unset the alarms when the keyswitch is disabled the schedule will override the keyswitch at the next set time.

Function	Description
----------	-------------

Schedule Type	This identifies the how the schedule will operate, the options available are: <b>Timed</b> - allows settings to be configured for set times during the day, night and weekend operation modes. <b>Zone Control</b> - This enables or disables Night Zone or Weekend Zone settings.
Schedule Record Rates	If this option is disabled then the record settings for day, night and weekend operation mode will be replaced by a single Rate option in the Standard record menus.
Operation Mode 1 Title	This title identifies the mode of operation for Mode 1 (DAY default)



Function	Description
Operation Mode 2 Title	This title identifies the mode of operation for Mode 2 (NIGHT default)
Operation Mode 3 Title	This title identifies the mode of operation for Mode 2 (WEEKEND Default)
Keyswitch Enable	When the keyswitch option is enabled it is necessary to identify the input that will be used to trigger the keyswitch, the options are Direct, Aux and Module 1 to 16.
Keyswitch – Normally closed	The keyswitch by default will be configured as normally open, however it is possible to change this to normally closed operation.

## How to Configure Text in Image Functionality



It is possible to integrate the DV-IP Server into a system where text information can be stored with the relevant images for review at a later date, e.g. Retail, Finance.

The DV-IP Server can be configured to search for specific text information, allowing for fast retrieval and review of images.

This section is divided into:

- Enable text in image on the serial port
- Configuring the paths.ini file to specify the communication port and text information
- Enabling and configuring the function using the web pages

To enable the serial port for text in image

1. Select **System -> Serial Ports & Telemetry**
2. Using the **drop down list** associated with the **serial port** that will be connected to the peripheral equipment select **TEXT in Image**
3. Configure the **serial parameters** for the device connected to the DV-IP Server: Baud rate, Parity, Data bits, Stop bits, Flow control
4. Save configuration by selecting **Save Settings!**
5. **Reset** the unit for the settings to be applied

## Default Settings

- Camera 1 – Serial 1
- Camera 2 – Serial 2
- Camera 3 – Serial 3 (Bus A)
- Camera 4 – Serial 4 (Bus B)

To configure the communication port

1. Using an **FTP client** application connect to the DV-IP Server
2. Locate the **letc** directory and expand
3. Locate the **paths.ini** file
4. Highlight and press the **right mouse button**, select **edit**
5. Enter the text information in the .ini file, the example details how the file is configured and shows an example configuration for COM1:

```
# COM1 = tty
# COM2 = term
# COM3 = aux1 or if input_path set to pic0 GPS stored on Port 3
# COM4 = aux2
# TEXT00 = camera 1
# TEXT01 = camera 2
# TEXT15 = camera 16
# input_path - the ports COM1 to COM4 that will receive text
# output_path - the command that will associate text to a camera
# buffer_size - the total number of character stored per line
# prefix      - this strips off leading characters received from EPOS
# =====
# COM1 will store text with Camera-1
# =====
[PATH0]
input_path=\tty
output_path=\pipe\TEXT00
buffer_size=80
# prefix=J
```

This example shows that text in image is set up on COM1 which means text is inserted in Camera 1 using 80 characters per line with no text filtering.

6. **Save** the configuration and **upload** to the DV-IP Server
7. **Reset** the unit for the settings to be applied

To enable and configure text in image feature via the web page:

1. Select **Camera -> Text -in-Images**
2. Identify the **number of lines in the image** that will be stored with the image

3. Identify the **length** (in characters) of these lines of information; 80 lines in generally full screen width and is the default setting
4. It is also possible to view the text as well as storing this information. Enter the information on the **number of lines** that will be displayed **below the image** in the live page, this will determine the area that the text will be displayed
5. Remember to save the configuration information by selecting **Save Settings!**
6. **Reset** the unit for the settings to be applied



Function	Description
Number of lines in Image	This is the number of lines that will be displayed in live and replay (via the web pages) along with the relevant images. The default setting is 10 lines.
Line length	This identifies the length of the lines that will be stored with the image. The default setting is 80 characters which is generally the full screen
Number of visible lines	To enable the text information to be viewed in the Live page it is necessary to identify the number of visible lines



**Note:** When viewing video in Live view (Active X only) it is possible to left mouse click over the image and the text information is superimposed over the image.

## How to Enable and Configure the On-board Firewall



The DV-IP Server supports an on-board Firewall to add to the security of the unit. The Firewall can be enabled and work in conjunction with the security applications that are already present in the network.

This feature ensures that unauthorised users can not gain access to the DV-IP Server and therefore have any affect of the operation of the system. With IP address and port filtering the firewall has been designed to let the authorised people access and keep everyone else out.



**Note:** The Firewall function is always enabled on the Digital Sprite 2.

To configure the firewall functionality:

1. If not already enabled, enable the Firewall function within **System -> Advanced Features** and **Reset** the unit for the settings to take affect
2. Select **Network -> Firewall**
3. Enable the **PING response** option by placing a tick in the adjacent box. Disabling this feature will make the DV-IP Server less visible on the network
4. Enter the **IP addresses** that can have access to the unit, these can be a range of addresses or a single IP address

If there is a range of address then enter the first IP address in the sequence followed by /nn where nn is the last IP address in the range. *Refer to IP Address and Subnet Calculation below*

5. Enter the **subnet** of the network, if a subnet has been specified in the IP address then that will take precedence over this subnet
6. Identify the **TCP ports** that are **enabled** and available on the DV-IP Server, enter the same number in the To and From values if a single port is required



**Note:** If you attempt to use a port that is not in the list, even if you have a valid IP address you will not gain access to the unit.

7. Enter the **UDP ports** on the system that are **available**, enter the same number in the To and From values if a single port is require



**Note:** If you attempt to use a port that is not in the list, even if you have a valid IP address you will not gain access to the unit.

8. Save the configuration by selecting **Save Settings!**

### Firewall Options

Enable PING response from server

**Allowed IP Addresses**

IP Table Entry: 1

IP Address	Subnet
0.0.0.0	255.255.255.255

**Open TCP ports**

TCP Table Entry: 1

From:	To:
0	0

**Open UDP ports**

UDP Table Entry: 1

From:	To:
0	0

Function	Description
----------	-------------

Enable PING response from server	By default this option is enabled and allows the DV-IP Server to be pinged. Disabling this option will make the Server less visible on the network
----------------------------------	--

Allowed IP address	These are the IP addresses and subnets that the server will allow connections from, i.e. the IP address of the host PC's that will connect to the DV-IP Server to; review video, download information.
--------------------	--



**Note:** If you enable this function ensure the IP address of the PC you are using to configure the system is also in the list. If the address is not added then you will be unable to communicate with the Server via the network, it is important to take this feature into account when the Server is on a DHCP network where IP addresses are allocated automatically.

If no IP addresses are specified than any IP address can connect to the sever

Function	Description
----------	-------------

Open TCP ports	This list identifies the TCP ports that are on the system and available. If a host tries to communicate with the DV-IP Server using a TCP port that is not in the list, even with a valid IP address, the host will not gain access to the unit. The enabled ports can be a range or single port address, if a single port is needed then enter the same port number in the to and from section
----------------	--

Open UDP ports	This is the list of UDP ports that are available on the DV-IP Server. If a host tries to communicate with the Server using a UDP port that is not specified in the list, even with a valid IP address, the host will not gain access to the unit. The enabled ports can be a range or single port address, if a single port is needed then enter the same port number in the to and from section
----------------	---

Function	Description
----------	-------------

Port, Type, Application, Use                      This identifies the default ports and their functionality that is supported on the unit.

The following are the default port settings supported on the DV-IP Server; this is shown on the Firewall page menu.

PORT	TYPE	APPLICATION	USE
21	TCP	File Transfer Port - (FTP) Connection	Used for manual/auto archiving video & audio to a remote server or PC
23	TCP	Terminal (Telnet) Connection	Remote terminal application, allows engineering function to be carried out
80	TCP	HTTP - Web Server Connection	This port is used when streaming video from a Unit or when accessing the WebPages
1025	UDP	Telemetry Control	PTZ commands are passed from the PC to the Unit
2074	UDP	Audio Port	Outgoing and incoming audio is passed over this link
2075	UDP	Audio Port	This port provides the control for audio outgoing and incoming
5201	TCP	Engineering Debug	Click start, RUN, type - telnet 5201

Alternatively it is possible to identify the supported ports and also determine who is connected to the DV-IP Server via a telnet session.

At the DV-IP prompt enter:

**TCP Ports**

The following is an example of the information that is displayed

```

DV-IP> ttccpp ppoorttes
Entry 0: socket no 0, myport 2074, (UDP) Daemon
Entry 1: socket no 1, myport 1025, (UDP) Telemetry listener
Entry 2: socket no 2, myport 21, (TCP) FTP Server Daemon
Entry 3: socket no 3, myport 5201, (TCP) Engineering Debug Daemon
Entry 4: socket no 4, myport 23, (TCP) Telnet Daemon
Entry 5: socket no 5, myport 80, (TCP) Web Server Daemon
Entry 6: socket no 7, myport 82, (TCP) SMC Server Daemon
Entry 7: socket no 8, myport 5202, (TCP) Daemon
Entry 8: socket no 9, myport 8080, (TCP) Daemon
Entry 53: socket no 53 (2), myport 23, hisport 1711 foreign IP 172.16.100.8
DV-IP>

```

## IP Address Range and Subnet

When entering a range of IP addresses in the Firewall it is necessary to calculate the relevant subnet that does not mask out the first IP address to the last IP address in the range. The following shows the figures that are entered in the IP address field and/or the subnet mask.



**Note:** For details on how these figures are calculated please refer to Appendix E.

The address can be written in two ways:

IP address/number of bits no subnet mask – 192.168.3.1/24

IP address and subnet mask – 192.168.3.1 255.255.255.0

If you wanted to add an address range to include IP address 1 to 12, then you would need to find the nearest IP address and subnet that would encompass this requirement, use the table below to assist you with configuring this function.

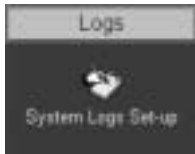
The table shows the address range including the number of bits allocated to the network address, the equivalent subnet mask for this range of addresses and the IP address that will be included in the range, (we will use the IP address of 192.168.3.1 for the example).

IP address	Network address	Included IP Address Range
192.168.3.1/24	255.255.255.0	0 - 255
192.168.3.1/25	255.255.255.128	0 - 127
192.168.3.1/26	255.255.255.192	0 - 63
192.168.3.1/27	255.255.255.224	0 – 31
192.168.3.1/28	255.255.255.240	0 – 15
192.168.3.1/29	255.255.255.248	0 – 7
192.168.3.1/30	255.255.255.252	0 – 3
192.168.3.1/31	255.255.255.254	0 - 1



**Important Note:** A host cannot be allocated an IP address of 0 or 255, which means there are really only up to 254 host addresses available in the example.

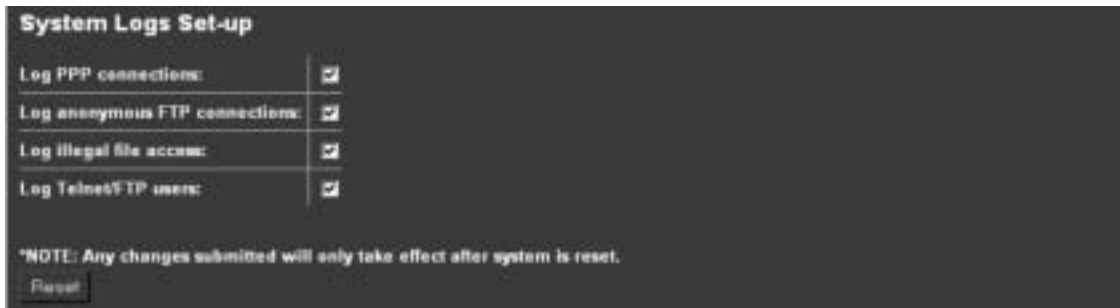
# How to Enable System Logs



There are numerous actions that the DV-IP Server can be configured to automatically carry out on receipt of; an alarm, VMD activation, Schedule function, etc. When these triggers are received and the actions initiated then it is possible to log this information within the DV-IP Server System Logs.

By default the DV-IP Server will log illegal file access and telnet/FTP users, to enable the other functions:

1. Select **Logs -> System Logs Set-up**
2. If connect/dial using **PPP** has been configured within the alarm and VMD pages enabling this option will **log** all the PPP actions
3. If the DV-IP Server has been configured to transmit file to an **FTP** server enabling this function will log all FTP transactions
4. Save the configuration by selecting **Save Settings!**



Function	Description
Log PPP connections	This enabled logging of WAN connections using the PPP ports and records the IP address, the profile used and the local time of the attempted connection
Log anonymous FTP connections	This identifies when an unauthorised user tries to access the DV-IP Server by entering anonymous in the username or password.
Log illegal file access	Any web access to a CGI protected directory or non-existent file will be logged with an IP address, time and type of action
Log Telnet/FTP users	This will log users that are trying to gain access to the DV-IP Server using an FTP or telnet session



# How to Enable and Configure Watermarking



The DV-IP Server supports the facility to watermark recorded images. It is also possible to produce a watermark certificate which proves that an image has not been altered or tampered with; this is achieved with the allocation of a unique MD5 signature which will change if the image files are changed.

This process can assist with the audit trail process for digital recorded video. The MD5 signature is a unique signature that is automatically allocated by the Server by using file information and generating the unique signature.

To configure and produce a watermark certificate

1. Select **Tools -> Watermark**
2. Enter the **start time** and **date** for the period that is to be reviewed
3. Enter the **finish time** and **date** for the period that is to be reviewed
4. Select **partition information** button, the recorded files within the specified time period will be displayed within the partition information summary
5. Highlight the **files** (partition) that your intend to allocate a **watermark**
6. It is possible to view the **index information** by selecting the **get index info button**, the video index information will be displayed

Video Index Information

Video partition: c:\index\DIR00019\VID01226.VID

Beam number: 0

File number: 1226

Entry	Channel	Attributes	Time	Offset in File
0	3	VID	Thu 24 Mar 2005 15:25:16.169	0
1	0	VID	Thu 24 Mar 2005 15:25:16.233	20580
2	1	VID	Thu 24 Mar 2005 15:25:16.237	40692
3	3	VID	Thu 24 Mar 2005 15:25:16.273	60952
4	2	VID	Thu 24 Mar 2005 15:25:16.276	81124
5	1	VID	Thu 24 Mar 2005 15:25:16.359	102732
6	3	VID	Thu 24 Mar 2005 15:25:16.393	123044
7	0	VID	Thu 24 Mar 2005 15:25:16.411	143528
8	2	VID	Thu 24 Mar 2005 15:25:16.435	164124
9	1	VID	Thu 24 Mar 2005 15:25:16.477	185668

7. If the Operator that is generating the watermark certificates is to be logged, enter the **report author** information, this will be added to the certificate
8. Enter the **step size** information; this identifies the 'skip' distance between bytes used in the watermark calculations, default 256 bytes

9. To generate the watermark codes that will be linked to the partition selected press the **watermark** button



**Note:** The smaller the step size the longer the calculation process, do not press any buttons while the Server is calculating, the progress of the process is displayed in the status bar.

10. When the watermark codes have been generated a **certificate** must be created by pressing the **create certificate** button, this certificate should then be printed and archived. This should form part of the customer security procedure regarding incidents.



Function	Description
Start Date and time	This is the start time and date for the time period of interest
End Date and time	This is the end time and date for the time period of interest
Report author	This will identify the Operator or Administrator responsible for generating the watermark certificate and can be used as part of the audit trail
Watermark step size	This is the step size in bytes used when calculating the watermark, if the step size is set to 1 then every byte in the in the video partition will be part of the watermark calculation. <b>Note:</b> The smaller the step size the more information that is to be processed. The process time will increase, this is displayed in the status bar
Partition Information Summary	This is the area when the partition information within the set time and date will be displayed. Each partition can be selected by highlighting the file

Function	Description
Partition Info	This button is selected for the DV-IP Server to search for the partition information within the set time and date. The partitions are then displayed in the partition information summary area
Get Index info	This allows you to obtain the index information of the selecting partition
Watermark	This will generate the unique MD5 signature for the selected partition. This watermark can be used as part of the audit trail to identify that the images have not been changed or tampered with
Create Certificate	Once the watermark has been generated this allows a certificate with all the information on the watermark to be created, it is possible to print this certificate

## How to Enable and Configure the Webcamera functionality



Any of the video inputs on the DV-IP Server can be made available to be transmitted to a webserver via FTP. These images can then be incorporated into a web page and accessed via a standard web browser.

This function gives users the opportunity to incorporate video images into their Corporate web site.

Examples of where this can be incorporated are:

Company that utilise the DV-IP Server for their building security but also route some strategically placed cameras to their intranet allowing employees access to the video, possible to view the car park

Theme Parks that again use the DV-IP Sever for their site security but link some of the cameras to the Internet site to allow potential visitors to gauge how busy the Park is and when they should visit.

This section has been divided into:

- Enabling the feature, identifying server information and enabling the cameras
- Configuring the FTP session details

To enable and configure the webcamera feature:

1. Select **Network -> Webcam Set-up**
2. Enter the **FTP Server** details; this can be the IP address, URL or domain name of the Server that will forward the images to the web pages. This link is usually provided by the Internet Service Provider (ISP)

3. Enter the **root directory** on the FTP server where the files will be saved
4. Enter the **image directory** information; this is the path within the root drive that will store the images that are being FTP'd to the Server
5. Enter the **prefix** information that will precede the image file when uploaded to the FTP Server, an example is 'cam\_' which would create a file name of cam\_01.jpg
6. Enter the **username** and **password** to allow the files to be uploaded to the FTP Server, this will be given to you by the Network Administrator
7. Enter the **update interval** in seconds, this identifies the time between updated files being transmitted from the DV-IP Server to the FTP Server. The speed and cost of the network connection being used should be taken into account when setting this time period
8. Enable the **video input(s)** that are to be made available for webcam functionality. Images from these inputs will be transmitted to the FTP Server for integration into web pages
9. Save the configuration information by selecting **Save Settings!**

**Webcam Configuration**

**Webcam Upload Settings**

Ftp Server (IP, URL or name)

Ftp Root Drive/Directory

Ftp Image Directory

Image Filename Prefix

Username

Password

Update Interval (Seconds)

**Camera Selection**

Camera:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Selected:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Function	Description
FTP Server	This is the IP address, URL or Domain Name of the FTP Server. Images will be uploaded from the DV-IP Server to this FTP server as time intervals specified
FTP Root Drive/Directory	This is the main/root directory on the FTP server where the image directory will be located
FTP Image Directory	This directory will be created when the initial image is uploaded to the FTP Server, it is the directory where all images will be saved on the server

Function	Description
Image Filename Prefix	This is an identifier for images sent from this DV-IP Server and will be stored as a prefix to the file name
Username	To gain access to the FTP server it is necessary to go through an authentication process this is the <b>username</b> that will allow the images from the DV-IP Server to be uploaded to the FTP Server
Password	To gain access to the FTP server it is necessary to go through an authentication process this is the <b>password</b> that will allow the images from the DV-IP Server to be uploaded to the FTP Server
Update interval	This is the minimum update interval between each image that is transmitted from the DV-IP Server.
Camera selection	This allows you to enable the video inputs that will be accessible for upload to the FTP Server

To enable the webcam connection information:

1. Enable the **single FTP session** so the FTP link from the DV-IP Server to the FTP server is **permanently up**. If this is not enabled then an FTP session will need to be established every time the DV-IP Server needs to transmit images

2. Enable **batch transfer** and images will be transmitted to the FTP Server in a **'batch'**, e.g. the DV-IP Server will take 'snap shots' from video inputs 1, 2, 4 and send these in a single batch to the FTP Server. If this is **disabled** then the DV-IP Server will transmit files **individually**.

The delay between batch files being transmitted is the **update interval**, e.g. every 10 seconds the DV-IP Server will send images from video inputs 1, 2, 3.

If batch is disabled then the update interval is the time between the DV-IP Server sampling an image from one input to the next, e.g. the DV-IP Server will transmit an image from input 1, 10 seconds later it will transmit and image from input 2, etc.

3. Select the **resolution** of the image that will be transmitted to the FTP Server, the files sizes that are applicable to this resolution are displayed. The file size should be taken into account with reference to the speed and type of network link

4. Enable the **Webcam** functionality for this feature to operate, **tick** the box which is appropriate to your application; **disabled, enabled when system SET, enabled when system UNSET** or **always enabled**

5. Remember to save the configuration by selecting **Save Settings!**



**Note:** When Developers are utilising the JPEG images that are provide from the webcam mode, the destination web page must have a video window with a 4:3 aspect ration to allow the video image to be displayed correctly.



Function	Description
Single FTP session	This avoids login/logout procedure for each image that is transmitted to the FTP Server. The DV-IP Server will remain connected and logged in to the ISP until the connection is disabled
Batch transfer	This will transfer all camera images in one batch. If this is selected then the update interval is the delay between all images being updated
Webcam Resolution	This is the resolution of the images, defined in the Camera Setup Page, that are transferred to the FTP Server. Take into account the speed and type of network connection being used when selecting the resolution.
Webcam Enabled	The webcam functionality can be enabled at specific times (SET or UNSET mode), always enabled or disabled. If the webcam functionality is to be disabled it is recommended that the option also be disabled in the Advanced Features option, refer to How to Enabled System Features above

## DV-IP Server Tools

There are a number of tools that are supported on-board the DV-IP Server itself. These can be accessed through the web interface and are available for testing system parameters and obtaining information for fault finding.

To access the Tools option:

1. Select the **Configuration** option on the **web interface**
2. Enter the **username** and **password** (default setting **dm** and **web**)
3. Select the **Tools** tab, the tools available are:

- Video Scope
- Audio Trace
- Relay Test Page
- Watermarking
- System Variables
- Reset

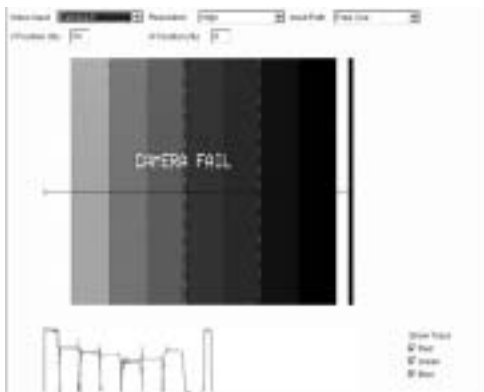
### Video Scope



The Video Scope page shows a trace of the video content (RGB) of the overall image. It will give the RGB values of the selected image.

It is possible to select any of the video inputs on the DV-IP Server to view the video contents. It is also possible to select the resolution of the image and compare the RGB levels.

Clicking within the video image will select a line of video and identify the value for that line rather than the overall image.



Function	Description
Video Input	This is a drop down list of the available video inputs on the DV-IP Server
Resolution	This is a drop down list allowing selection of the resolution being viewed/traced (high, medium and low)
Input Path	This is a drop down list allowing selection between free use or preselector 1 – 4
V and H Position	When a line of video is selected this identifies the vertical and horizontal position. For the overall image these values will be 0
Show Trace	This allows the R, G, B trace to be enabled or disabled
RGB	These are the calculated values for the RGB contents within the whole image or the selected line

## Audio Trace



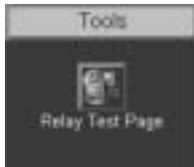
It is possible to use the audio trace option to identify if audio is being transmitted or received by the DV-IP Server.

To view the audio select the line in or line out buttons, the corresponding audio signal will be traced.

Function	Description
Audio Line Out	This will produce a trace of the audio out line on the DV-IP Server. This is represented by a red line
Audio Line In	This will produce a trace of the audio in line on the DV-IP Server. This is represented by a blue line



# Relay Test Page



The relay test page allows you to test the On-board relays and the additional relay modules. The DV-IP Server supports four On-board relays and up to two additional relay modules, these modules have sixteen relay connections each.

To test the relay select the tick box adjacent to the relay number, save the configuration. Press the OK button and this will trigger the corresponding relay.



**Note:** If the On-board relays have been configured to have the default settings it will not be possible to test these, the corresponding text box will be disabled.



Function	Description
Global Alarm	This identifies which of the relays has been enabled for global alarm. Note this relay will be disabled for test
Global VMD	This identifies which of the relays has been enabled for global VMD. Note this relay will be disabled for test
Global Camera Fail	This identifies which of the relays has been enabled for global camera fail. Note this relay will be disabled for test
Schedule Notification	This identifies which of the relays has been enabled for schedule notification. Note this relay will be disabled for test

Function	Description
Primary Signalling Failure	This identifies which of the relays has been enabled for primary signalling failure. Note this relay will be disabled for test
Weekend Notification	This identifies which of the relays has been enabled for weekend notification. Note this relay will be disabled for test
On-board Relays	There are six On-board relays, enabling the corresponding relay will close the output
Module 1	If an additional relay module has been connected to the 485 bus, this allows the relevant relays to be tested <b>Note:</b> The relay will only be initiated when the Save option has been selected
Module 2	If a second additional relay module has been connected to the 485 bus, this allows the relevant relays to be tested <b>Note:</b> The relay will only be initiated when the Save option has been selected

## Watermarking



This option has already been covered in the Configuration section of this manual; please refer to How to Enable and Configure Watermarking for details of this option.

## System Variable



This page can be used for system diagnostics as it provides a readable overview of the configuration parameters of the DV-IP Server. Any information that has been configured and stored on the Server will be shown on the file. Typical information is; camera titles, alarm title. It identifies the Value, Variable Name and the Description.



**Note:** This information may be useful when contacting Dedicated Micros for system analysis.

## Reset



This will reset the unit. Remember to save all configuration settings before resetting the unit as information not saved will be lost.

## Reviewing the DV-IP Server Logs

The DV-IP Server can be configured to produce a number of log files, these are for:

- PPP connections
- Anonymous FTP connections
- Illegal file access attempts
- FTP and telnet users



Configuration of these logs is detailed in the Configuration section of this manual. The logs that are generated can be viewed via the web interface on the DV-IP Server.

To access the logs:

1. Select **Logs**, to enable the logs select **System Log Set-up** enable the logs that are required and select **Save**.
2. The logs can now be accessed these are:

- Connection Log
- Anonymous FTP Log
- Security Log
- e-mail Log
- Sent Message Log
- FTP Download Log
- Logfile
- Logfile Backup

3. To **review** the files select the corresponding option, the information will be displayed on screen

### Connection Log



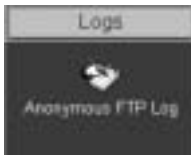
This log details all FTP and telnet connections made to the DV-IP Server.

Telnet and FTP can be allocated a username and password by enabling and configuring the option within the **USER.ini** file, this file registers all the information on the User name, IP address of the remote PC, time of transaction.

Having this log containing the above information ensures ease of identification of Operators/Administrators that have logged into the system, the following shows typical log information;

```
Wed Jun 02 10:49:16 2004 (+0100): FTP User [dm1] logged in
Wed Jun 02 10:49:16 2004 (+0100): Foreign IP 172.16.100.65
Wed Jun 02 10:49:16 2004 (+0100): Socket no 15, myport 21, hisport 1083
Wed Jun 02 10:53:20 2004 (+0100): Telnet User [dm1] logged in
Wed Jun 02 10:53:20 2004 (+0100): Foreign IP 172.16.100.65
Wed Jun 02 10:53:20 2004 (+0100): Socket no 24, myport 23, hisport 1199
Wed Jun 02 10:53:53 2004 (+0100): FTP User [dm1] logged in
Wed Jun 02 10:53:53 2004 (+0100): Foreign IP 172.16.100.65
Wed Jun 02 10:53:53 2004 (+0100): Socket no 18, myport 21, hisport 1235
```

## Anonymous FTP Log



The FTP function on the DV-IP Server is password protected, however it is possible to disable the password allowing any user access to the Server via FTP.

If the password is disabled then any user accessing the DV-IP Server will be logged in the Anonymous FTP log.

A typical example of the log is shown:

```
Wed Jun 02 10:56:45 2004 (+0100): FTP User [anonymous] logged in
Wed Jun 02 10:56:45 2004 (+0100): Foreign IP 173.16.85.25
Wed Jun 02 10:56:45 2004 (+0100): Socket no 18, myport 21, hisport 1235
```

## Security Log



The Security Log identifies the users that have attempted to access the Configuration pages or any password protected page on the DV-IP Server Web interface and have entered an incorrect password.

The information logged is:

- The action requested and status
- Time and date
- IP address
- Port information

This information can be used to monitor the connections to the DV-IP Server and identify unauthorised actions.

The following shows typical log information;

*Attempt to access to frmpages\index.html at Tue Jun 08 12:43:04 2004 +0100, action GET Authentication fail  
Foreign IP 172.16.50.60  
Socket no 22, myport 80, hisport 12226*

*Attempt to access to scripts\root.exe at Tue Jun 08 13:50:35 2004 +0100, action GET file does not exist  
Foreign IP 172.16.50.60  
Socket no 23, myport 80, hisport 1049*

## E-mail Log



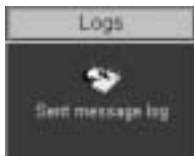
This log holds information on the e-mails sent from the DV-IP Server on receipt of an alarm.

It follows the complete transaction from receipt of alarm to acknowledgement that the e-mail has been sent and the SMTP link has been dropped.

The following shows a typical e-mail log, it contains the sending address, the recipient address, the mail server information (IP address or name) and the reason for the mail, in this example Camera 3 has failed:

```
Sending message to jsmith@dmicros.com at Wed Jun 30 14:21:26 2004 +0200  
220 heron.jbloggs ESMTP Server (Microsoft Exchange Internet Mail Service 5.7.2653.13) ready  
HELO DV-IP  
250 OK  
MAIL FROM:<DV-IP@DV-IP>  
250 OK - mail from <DV-IP@DV-IP>  
RCPT TO: <jsmith@jbloggs.com>  
250 OK - Recipient <jsmith@jbloggs.com>  
DATA  
354 Send data. End with CRLF.CRLF  
Date: Wed, 30 Jun 2004 14:21:32 +0200  
X-Mailer: ADH SendMail V1.0  
MIME-Version: 1.0  
To: jsmith@jbloggs.com (John Smith)  
From: DV-IP@DV-IP  
Subject: System Exception  
Content-Type: text/html; charset=us-ascii;  
Content-Transfer-Encoding: 7bit  
<!doctype html public "-//w3c//dtd html 4.0 transitional//en">  
<html>  
Site-Id: DV-IP<br>  
System-Exception: Camera fail 3 at Wed Jun 30 14:21:26 2004 +0200<br>  
</html>  
250 OK  
QUIT 221 closing connection
```

## Sent Message Log



This logs all the SMS message information. There are various options that can be configured to allow an SMS message to be sent; start up, alarms, etc.

The Sent Message Log, logs the information on the message sent including; the time and date, sender and receiver details and the message that was sent.

The following shows a typical SMS message log for when the system starts up after power down or reset.

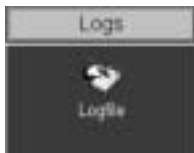
```
Fri Mar 12 12:05:26 2004 +0000
SMS to: 07970972823
SMS message: STARTUP, TVDEMO, Fri Mar 12 11:15:06 2004 +0000, 0.0.0.0
SMS response: STARTUP, TVDEMO, FRI MAR 12 11:15:06 2004 +0000, 0.0.0.0
```

## FTP Download Log



The DV-IP Server can be configured to manual or automatically trigger and FTP download of images. These downloads are logged and stored with the FTP Download Log for future analysis.

## Logfile



The Logfile stores all information on every action that is carried out by the DV-IP Server; when alarms are received and actioned, resets, failed outward bound alarm connections, etc.

This is the current file and will continue to store data until it reaches its maximum size limit (typically 1Mb). This file then writes over the top of the Logfile Backup and becomes the backup file and a new logfile is created.

This ensures current and recent information is always available.

The information detailed is; Time and date, Reset Code and Reason, Connection-status, Site and ARC ID.

The following is typical log information:

```
#
System-Start : at 15:11:39 on 24-06-2004 UTC
System-Halt : at 15:11:28 on 24-06-2004 UTC
Restart code : 100
Restart reason : Controlled user RESET from Telnet or the webpages
Alarm-Log : Alarm initiated : Zone 1 at 15:11:59 on 24-06-2004 +0100
Connection-Status: request connection for Alarm Reporting at 15:11:59 on 24-06-2004 +0100
Connection-Status : Connection to 172.16.100.12\Ethernet at 15:11:59 on 24-06-2004 +0100
Site-Id: DV-IP-50
Arc-ID: DV-IP-50
System-Status:
Local-IP: 172.16.89.50
Activating-Channel: 3
Response-Images: 1
Response-Area: Zone 1
Response-Level: GREEN
Alarm-Time: 15:11:59 on 24-06-2004
Rec-Index: 14:11:59 on 24-06-2004
Connection-Status : Connection closed at 15:11:59 on 24-06-2004 +0100
#
```

## Logfile Backup



This file is updated every time the Logfile reaches its maximum capacity. The Logfile will automatically write over the top of the existing Logfile Backup to create a file containing information that occurred recently.

Along with the Logfile this ensures the current information and most recent information is available for analysis.

The following is a typical example of the information held within the Logfile Backup.

```
System-Start : at 15:47:41 on 04-06-2004 UTC
System-Halt : at 15:47:30 on 04-06-2004 UTC
Restart code : 100
Restart reason : Controlled user RESET from Telnet or the webpages
System-Status : Standard UNSET recording selected by timer at 15:47:42 on 04-06-2004 +0100
System-Status : Standard UNSET recording selected by timer at 15:47:42 on 04-06-2004 +0100
System-Status : Standard UNSET recording selected by timer at 15:47:42 on 04-06-2004 +0100
System-Status : Standard UNSET recording selected by timer at 15:47:42 on 04-06-2004 +0100
System-Status : Standard UNSET recording selected by timer at 15:47:43 on 04-06-2004 +0100
System-Status : Standard UNSET recording selected by timer at 15:47:43 on 04-06-2004 +0100
```



This is an example of the details that are contained in the logs; this shows an unauthorised user trying to access the DV-IP Server using an FTP connection.

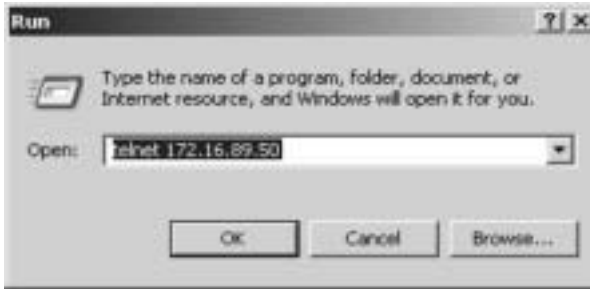
*Sat Apr 24 05:53:50 2004 (+0100): FTP FAILED LOGIN User: [test] Password: [test]  
Sat Apr 24 05:53:50 2004 (+0100): Foreign IP 62.214.19.65  
Sat Apr 24 05:53:50 2004 (+0100): Socket no 82, myport 21, hisport 4953  
Sat Apr 24 05:53:50 2004 (+0100): FTP FAILED LOGIN User: [test] Password: [test12]  
Sat Apr 24 05:53:50 2004 (+0100): Foreign IP 62.214.19.65  
Sat Apr 24 05:53:50 2004 (+0100): Socket no 83, myport 21, hisport 4999  
Sat Apr 24 05:53:50 2004 (+0100): FTP FAILED LOGIN User: [test] Password: [test123]  
Sat Apr 24 05:53:50 2004 (+0100): Foreign IP 62.214.19.65  
Sat Apr 24 05:53:50 2004 (+0100): Socket no 84, myport 21, hisport 1049  
Sat Apr 24 05:53:50 2004 (+0100): FTP FAILED LOGIN User: [test] Password: [123]  
Sat Apr 24 05:53:50 2004 (+0100): Foreign IP 62.214.19.65  
Sat Apr 24 05:53:50 2004 (+0100): Socket no 85, myport 21, hisport 1071*

## Appendix A - Resetting the DV-IP Server

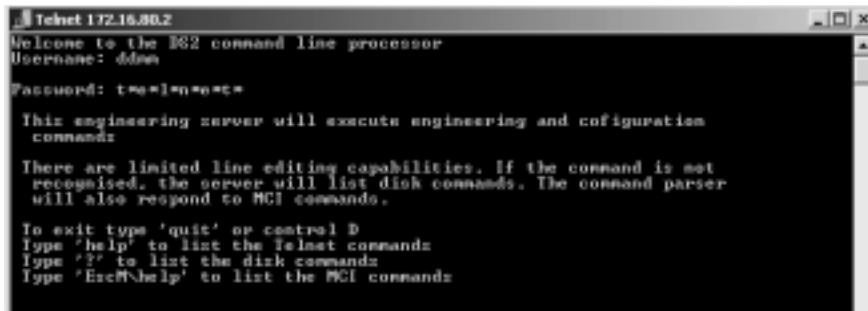
### Reset using Telnet

An alternative option for resetting the DV-IP Server is to connect to the unit using telnet.

1. Go to **Start -> Run**
2. Enter **<telnet <IP address of Server>>**



3. You will be prompted for a **username** and **password** (default **dm** and **telnet**) and press return



**Note:** Echo is enabled on the DV-IP Server for telnet.

4. Type **<reset>**, the Server will reset itself and will not be available for a few minutes

## Appendix B – DV-IP Server .ini Files

### Updating the Bootloader

If any updates are required to the DV-IP Server bootloader it is necessary for the DV-IP Server to be in Engineering Mode. To put the unit into Engineering mode carry out the following steps:

1. Using Telnet connect to the DV-IP Server.
2. Enter the username and password (default **dm** and **telnet**).

At the DV-IP> prompt type **engmode**.

4. Press <**return**>, the telnet connection will be automatically dropped while the DV-IP Server reboots into engineering mode.

5. Wait approximately 60 seconds before re-connecting to the unit for updating the bootloader, when you re-connect you will be prompted with a warning that the machine is in bootloader mode.

### Editing the ini Files using FTP Client Application

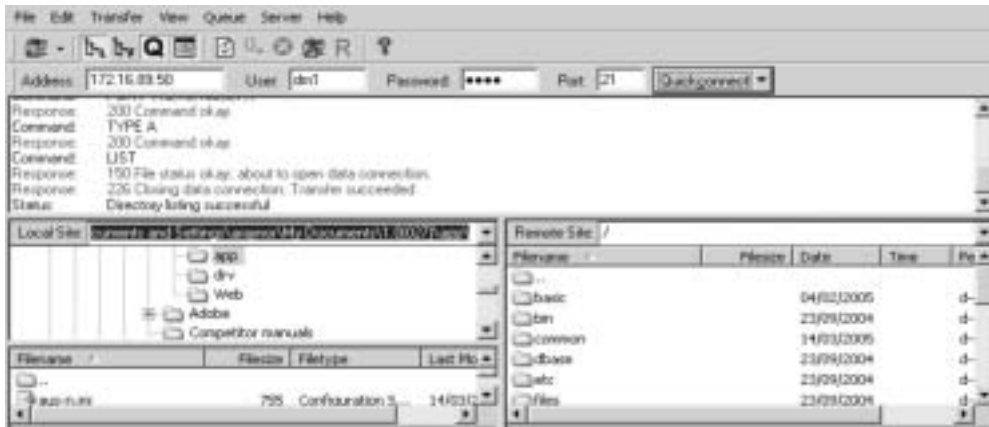
There are a number of parameters that can be configured within the ini files on the DV-IP Server. This section details the files, their function and how these are configured.

To edit and configure these files on the DV-IP Server you will require:

- FTP communication to be enabled on the DV-IP Server
- Valid FTP username and password
- FTP Client software application
- Connection via the Ethernet network to the DV-IP Server

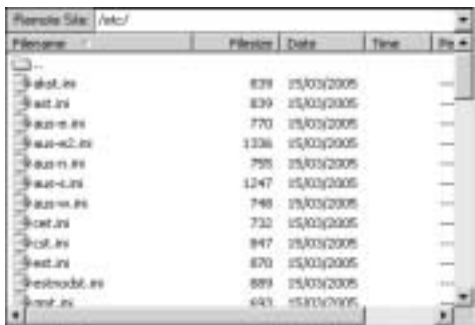
The following steps give an example of how to create an FTP session with the DV-IP Server to configure these files, take note this may differ from the process of the FTP software you are utilising.

1. Launch the **FTP client** software
2. You will need to **create a site** for the FTP link, enter the **IP address** of the DV-IP Server, enter the **FTP username** and **password**

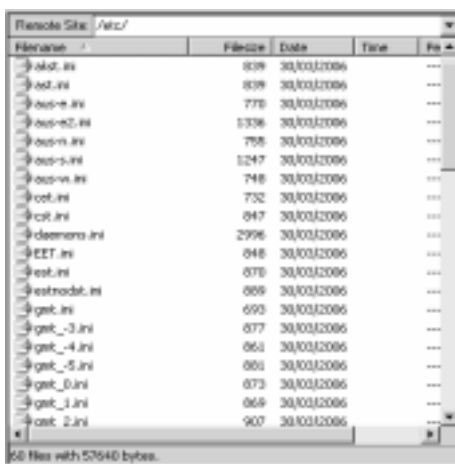


3. Select the **Connect** button to make the connection

4. You will be presented with the directory structure on the DV-IP Server, locate and select the **etc** directory in the root drive



5. The following files are all stored in the etc directory.



6. There are two ways of opening and editing these files, depending on the file that is selected

### hosts and profiles

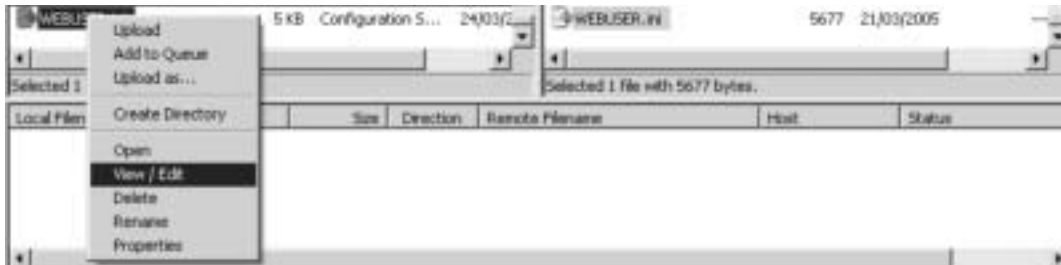
**Highlight** the file, click the **right mouse key** and select **Download (or View)**

The file will be downloaded, highlight and right mouse click and select **Open**, you can edit the information

### modems.ini, USER.ini, Vidcfg.ini, WEBUSER.ini

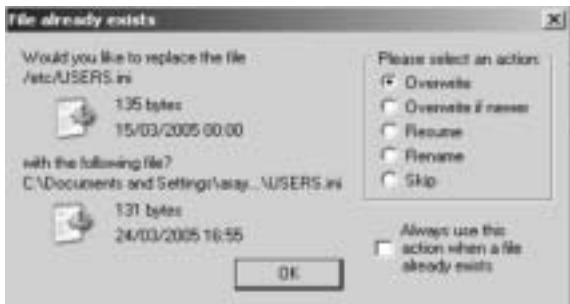
**Highlight** the file, click the **right mouse key** and select **Edit**

The file will be opened and you can edit the information



9. Once you have completed the configuration **Save** the file

10. When you close the file you will be prompted to upload the file to the DV-IP Server, select **Upload**



**Note:** If you are not prompted ensure you upload the file to the DV-IP Server for the configuration to take affect.

## Structure of the Files

Each of the following files usually has an explanation at the beginning of the file describing what the feature command set is and how they can be edit.

If any of the configuration commands have a comment (#) at the beginning of the line then this has been disabled, remove the comment (#) enables the feature and allows you to configure the settings.

Headings will be included when more that one feature can be configured within the file to identify the command string within that section, e.g. [unlock], [watermarking].

### hosts

This file contains the IP address of the remote monitoring PC that is the point of contact when an alarm is received on the DV-IP Server.

The file allows you to identify the name and IP address of the PC



**Note:** There is a corresponding web page that is the usual interface for configuring this information; however this file has also be supplied.

An example of the information contained in this file is shown

```
# DV-IP Hosts Table 23-January-2004
# The Host is the IP address of the PC the DV-IP connects to on alarm.
# <Label/Remote PC Description><IP Address of Alarm Receiving PC>
# The label is used as the description in the Alarm Connection Page on the DV-IP.
# i.e. the label location1 would be entered in the primary & secondary host name.
# Note:- You must fill in both the primary & secondary host options in the
# Alarm Connection Settings page.
# The Host label/username & password listed in the Hosts Table are "Case Sensitive".
# Hosts Table List
# _____
# <Label/PC Description><IP Address of remote PC>
JohnSmith 10.0.0.50
ARC1      10.0.0.51
Location1 192.168.2.3
NULL      0.0.0.0
```

### modems.ini

The DV-IP Server supports a number of modems that can be configured in the Serial Port & Telemetry web page, however if a modem is not supported then the configuration and operational information for the modem can be added to the modems.ini file.

An example of the information stored in this .ini file is shown:

```
# modem description file
# These modem strings will be installed prior to the fixed strings and can therefore be
# used to update the initialisation strings
# format:
# [code]
# name=descriptive text name
# reset=string to reset device to factory defaults
# init=initialisation string
# save=string to save current settings
# negate_dtr=0 assert DTR line during modem initialisation
# negate_dtr=1 negate DTR line during modem initialisation
# type=0,1,2 type of PPP device
# 0 - modem / terminal adaptor (default)
# 1 - router
# 2 - always on eg GPRS, CDPD
# code is the product code as returned by AT! (if appropriate)
# name is the descriptive text name (including spaces if required)
# initialisation string is the complete AT string sent to the TA/modem on detection of DTR
# The negate_dtr line allows control over DTR during initialisation. Some modems will
# not respond if DTR is negated whilst others will answer calls unless DTR is negated
# Initialisation requirements - brackets indicate usual settings
# echo off (E0), DCD follows carrier (&C1), DTR causes hangup (&D2)
# useful settings - hardware handshaking, autobaud
[FALCOM_A2]
name=Falcom GSM Phone/Modem
reset=AT&F
init=ATE0&C1&D2&S0S0=1
save=AT&W
negate_dtr=0
[ENFORA]
name=Spider 4 CDPD Modem
reset=AT&F
init=ATE0&C1&D2+WS45=4
save=AT&W
negate_dtr=0
type=2
```

## paths.ini

This file is part of the Text in Image configuration and identifies the communication port on the DV-IP Server that will be connected to the peripheral equipment and also the text information.

Once the associated serial port has been enabled for text in image (refer to the Configuration Section of this manual) it is necessary to enter the relevant information in the paths.ini file so the DV-IP Server is aware of the route (path) of the text information that will be stored with the associated image.

This is an example of the information that is stored within the paths.ini file.

```
# DV-IP 17-07-03
# -----
# Example ini file to add text for COM1 to COM4
# COM1 = tty
# COM2 = term
# COM3 = aux1 or if input_path set to pic0 GPS stored on Port 3
# COM4 = aux2
# TEXT00 = camera 1
# TEXT01 = camera 2
# TEXT15 = camera 16
# input_path - the ports COM1 to COM4 that will receive text
# output_path - the command that will associate text to a camera
# buffer_size - the total number of character stored per line
# prefix - this strips off leading characters received from EPOS
# =====
# COM1 will store text with Camera-1
# =====
[PATH0]
input_path=\tty
output_path=|pipe\TEXT00
buffer_size=80
# prefix=J
# =====
# COM2 will store text with Camera-2
# =====
[PATH1]
input_path=\term
output_path=|pipe\TEXT01
buffer_size=80
# prefix=J
profiles
```

When utilising the Connect/Dial on alarm function of the DV-IP Server, it is necessary to identify the receiving station information – profile – so the DV-IP Server is aware of the route the alarm is to take. For Ethernet connectivity this can be carried out using the web interface, for connection via a serial port it is necessary to enter the information in the 'profiles' file.



**Note:** Ethernet profiles can also be entered in the profiles file instead of using the web interface page.

```
# DV-IP Profiles Table 23-January-2004
# Profile list
# PPP_Link1 = COM2 - Default alarm dial communication port.
# PPP_Link2 = COM1 - Default dial in communication port.
# Ether1 = Alarm connection across an Ethernet Port (Entering Ethernet as the Profile
# will connect over Ethernet)
# Rules
# 1) The IP address range is that of the remote network the DV-IP is connecting to.
# 2) IF you set the IP range to 10.0.0.50 with a subnet of 255.255.255.0, the HOST PC
# IP address range will be 10.0.0.51 to 10.0.0.254
# 3) If you only wish to dialling into the DV-IP, the Phone No.
# 4) The first field <Username & Profile Label> is the description you will use in the
```



```
# Alarm Connection Page as the Profile description for the primary & secondary call.
# The Profile label/username & password listed in the Profiles Table are "Case
  Sensitive".
# _____
# Profiles Table List
# _____
```

#<Username>	<Password>	<Port>	<Phone No>	<Address Range>	<Subnet Mask>
Dm	password	PPP_Link2	1234567890	10.0.0.1	255.255.255.0
username	password	PPP_Link1	1234567890	10.0.0.1	255.255.255.0
Test	password	PPP_Link1	1234	10.0.0.1	255.255.255.0

## USER.ini

A number of features on the DV-IP Server are password protected; these have default usernames and passwords. The features that can be enabled for authentication are FTP, telnet and serial communication.

The user.ini file contains the username and password information for these features and is also the interface to enable or disable password protection.

The example shows the default usernames and passwords and which of these features are enabled on the DV-IP Server when shipped from the factory.

```
[FTP]
dm=ftp

[Telnet]
dm=telnet

[Serial]
# dm=serial
# serial=password
```

## vidcfg.ini

The DV-IP Server can support up to 600Gb of internal storage, however in applications that require large storage capacities it is possible to integrate the Dedicated Micros RAID or JBOD storage units into the application.

If the DV-IP Server has additional storage connected to the SCSI port of the unit it is necessary to enter the configuration information for this unit in the vidcfg.ini file so the DV-IP Server is aware that an external storage device is attached and also the drive structure of the storage unit.

```

# =====
# DV-IP03-03-2004
# =====
# Entries are as follows
# [Partition name]
# path = <pathname>
# file_size = <file_size>
# max_blocks = <max_blocks>
# disk_offset = <day_mask>
# write_type =
# The meanings of the parameters are as follows
# Partition Name: Any ascii name for this partition. Does not perform any other function
# path :The effective MSDOS style root of the partition directory structure
#     default 3.5" = c:\video
# file_size :The size in bytes of each partition file - default = 50Mbyte (52428800)
# max_blocks : The number of files in this partition. A value of -1 makes the system use the maximum available
# space on the disk specified in path
# default = -1
# disk_offset : The offset into the disk for the WebPages, Application, Form Files etc; start making video
partitions
# specified in 64 KiloBytes blocks default=3200 (Equal to 200 MegaBytes)
# write_type : unbuffered - writes data straight to the hard disk drive. Useful to speed up height images sizes
# written at fast to the HDD.
#     NOTE:- This can be wasteful when writing images to HDD i.e. 256 bytes per image on average. buffered -
#     Default setting - Buffers data to a fixed 20 KiloByte
#     buffer prior to a HDD write. More efficient when writing
#     images to the HDD.
# -----
# Drive Definitions A – Z
# -----
# Drive a = 4096 KB Ram
# Drive b = 16 KB RAM
# Drive c = MASTER 3.5"
# Drive d = SLAVE 3.5"
# Drive e = Master 3.5"
# Drive f = Slave 3.5"
# Drive g = Flash Drive
# Drive h to K not used
# Drive l to Z = SCSI Drive ID-0 to 7 LUN-0 to LUN-7
# DV-IP will support up to Drive letter Z
# Note:- If multiple logical unit numbers (LUN) are used within the SCSI ID, the DV-IP will automatically offset
the logical drives between drive letters L to Z.
# e.g. SCSI ID-0 LUN-0 = Drive L
# SCSI ID-0 LUN-1 = DRive M
# SCSI ID-0 LUN-2 = DRive N
# SCSI ID-1 LUN-0 = DRive O
# SCSI ID-1 LUN-1 = DRive P
# SCSI ID-2 LUN-0 = DRive Q
# -----
# Drive Partition Options
# -----
# 10 MegaByte Partition - 10485760 - For hard disk sizes 160 GB or less
# 50 MegaByte Partition - 52428800 - Default in Bootloader & upto 600 GB
# 100 MegaByte Partition - 104857600 - For hard disk blocks larger that 600 GB
# 200 MegaByte Partition - 209715200 - For hard disk blocks larger than 2000 GB
# -----

```

```

# Use the following settings to format Addresses 0 to 6 for drives l: to r: external SCSI drives.
#
# [Partition 5]
# path=l:\video
# max_blocks=-1
# file_size=104857600
# disk_offset=3200
# [Partition 6]
# path=m:\video
# max_blocks=-1
# file_size=104857600

```

## WEBUSER.ini

The WEBUSER.ini file contains the username and passwords for accessing the web configuration pages on the DV-IP Server.

It also contains the username and password for the DV-IP Viewer software and the ability to identify which mode of operation can be accessed by a user (live or replay) and which cameras the user can access.

The first example shows the default username and password for accessing the web configuration pages on the DV-IP Server.

```

#####
#
# DV-IP Webuser.ini Version 18th May 2004
#
#####
#
# Note: This file requires a blank line at the end of this file.
# Note: Line with #— are comments. i.e. #— Username(s) Password(s)
#
# [WebPage Configuration]
# — Username(s) Password(s) —
    dm=web

```

This example shows the command string for enabling John Smith to have access to cameras 1 to 16 in live mode, cameras 1 to 8 in replay and the username and password for this Operator when logging in using the DV-IP Viewer software

```

#####
#
# Provides access for cameras 1 to 16 in live and cameras 1 to 8 in playback
# for John Smith
#
#####
# object=cgi
live_cams=1-16
replay_cams=1-8
#— Username(s) Password(s) —
john=smith

```

## Appendix C – Port Assignment on the DV-IP Server

### Port Allocation

It is possible to identify specific ports that will be used for functionality supported on the DV-IP Server.

These functions are:

FTP  
Telnet  
HTTP  
Telemetry Control  
Audio  
Debug

Some of these ports have default settings that will link to the default settings of a standard network infrastructure, e.g. port 21 default port for FTP, port 80 default port for HTTP.

However if these default port numbers have already been allocated to other devices on the network then it is possible to identify alternative port numbers.



**Important Note:** It's important to ensure all devices that are part of the system configuration are all allocated the same port number otherwise communication between the devices will not be successful.

To view the ports that have been enabled and configured on the DV-IP Server, select **Network -> Firewall Options**. This details the port numbers, type of connection, application and use.

The screen shot shows the default settings for each of the features that utilises a port number as part of its communication path.

PORT	TYPE	APPLICATION	USE
21	TCP	File Transfer Port - (FTP) Connection	Used for manual/auto archiving video & audio to a remote server or PC
23	TCP	Terminal (Telnet) Connection	Remote terminal application, allows engineering function to be carried out
80	TCP	HTTP - Web Server Connection	This port is used when streaming video from a Unit or when accessing the WebPages
1025	UDP	Telemetry Control	PTZ commands are passed from the PC to the Unit
2074	UDP	Audio Port	Outgoing and incoming audio is passed over this link
2075	UDP	Audio Port	This port provides the control for audio outgoing and incoming
5201	TCP	Engineering Debug	Click start, RUN, type: telnet 5201

It is possible to redefine the port allocation for FTP, telnet and HTTP, how this is achieved is detailed in the Configuration section of this manual.

The telemetry control, audio port and engineering debug are default settings and are not configurable; these port numbers must be given to the Network Manager to ensure there are no other devices on the network using these ports.

Using a telnet session it is possible to telnet to a specific port to obtain debug information, for example at the DV-IP prompt enter:

Telnet <IP address or DV-IP Server> 5201

This will download debug information on the Engineering port, the following is an example of the information obtained:

```

Telnet 172.16.89.50
RECORD: 360 pix written at 6 pix per sec, reqs = 0
RECORD: 359 pix written at 6 pix per sec, reqs = 0
RECORD: 359 pix written at 6 pix per sec, reqs = 0
RECORD: 359 pix written at 6 pix per sec, reqs = 0
RECORD: 360 pix written at 6 pix per sec, reqs = 0
RECORD: 359 pix written at 6 pix per sec, reqs = 0
RECORD: 359 pix written at 6 pix per sec, reqs = 0
RECORD: 360 pix written at 6 pix per sec, reqs = 0
RECORD: 359 pix written at 6 pix per sec, reqs = 0
RECORD: 359 pix written at 6 pix per sec, reqs = 0
RECORD: 359 pix written at 6 pix per sec, reqs = 0
TN_DRU: attempting to open a specified socket (<telnet\54, Thu Mar 24 17:40:57 2005 +0100>)
TN_DRU: creating new link count for socket 54
TN_DRU: attempting to open a specified socket (<telnet\54, Thu Mar 24 17:40:57 2005 +0100>)
DEMON: Telnet server on socket 54
TN_CMD: process telnet requests
ERRLOG: connection logfile size 59744
ERRLOG: connection logfile size 59806
ERRLOG: connection logfile size 59864
TN_CMD: exit process_telnet_requests
DEMON: launching debug server
RECORD: 360 pix written at 6 pix per sec, reqs = 0

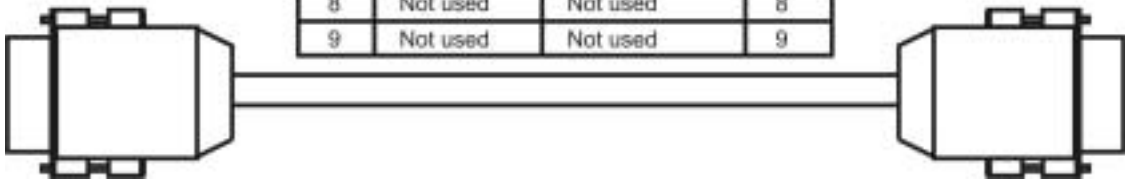
```

## Appendix D – DV-IP Server Serial and Network Cables

### DM RS232 Debug Cable (supplied)

The RS232 Debug cable can be used to connect the PC serially to the DV-IP Server for configuration using a terminal application (such as HyperTerminal™).

Pin	Colour Code	Pin Assignment	Pin
1	Not used	Not used	1
2	Red	TX	3
3	Blue	RX	2
4	Not used	Not used	4
5	Green	Ground	5
6	Not used	Not used	6
7	Not used	Not used	7
8	Not used	Not used	8
9	Not used	Not used	9

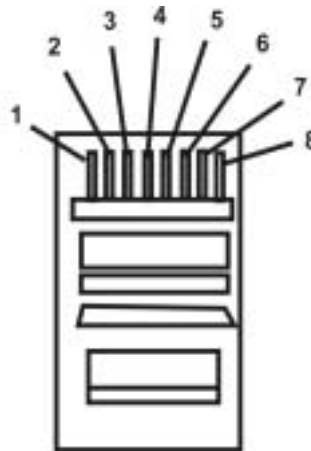


## Straight-through Network Cable

A straight through network cable connects hosts to network devices; PC to switch, DV-IP Server to Switch.

Coloured wires may be a solid colour without the white stripe.

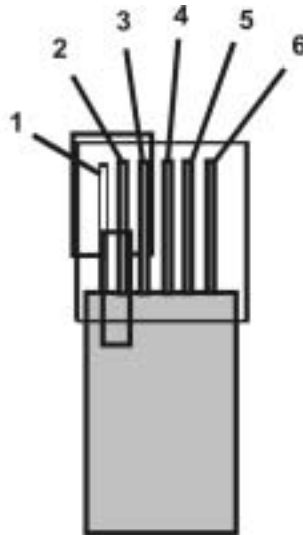
Pin	Colour Code	Pin Assignment	Pin
1	White/Orange	Transmit (+)	1
2	Orange/White	Transmit (-)	2
3	White/Green	Receive (+)	3
4	Blue/White	Not used	4
5	White/Blue	Not used	5
6	Green/White	Receive (-)	6
7	White/Brown	Not used	7
8	Brown/White	Not used	8



## DM 485 Bus Cable (supplied)

The DM 485 Bus cable is supplied for connectivity to peripheral DM devices such as Alarm Modules and Relay Modules.

Pin	Colour Code	Pin Assignment	Pin
1	White	Not used	1
2	Black	Ground	2
3	Red	485 bus data A	3
4	Green	485 bus data B	4
5	Yellow	Ground	5
6	Blue	+8V d.c. Supply	6



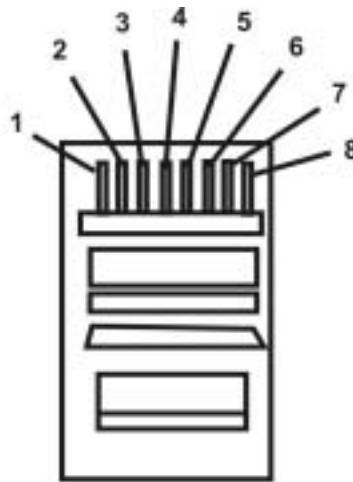


## Cross Over Network Cable

A cross over network cable is used to connect hosts to hosts or network equipment to network equipment, switch to router, PC to DV-IP Server.

Coloured wires may be a solid colour without the white stripe.

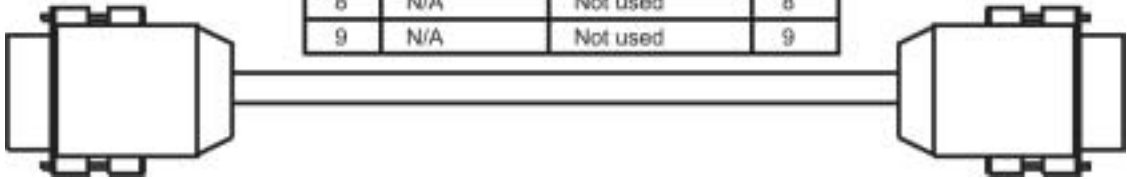
Pin	Colour Code	Pin Assignment	Pin
1	White/Orange	Transmit (+)	3
2	Orange/White	Transmit (-)	6
3	White/Green	Receive (+)	1
4	Blue/White	Not used	4
5	White/Blue	Not used	5
6	Green/White	Receive (-)	2
7	White/Brown	Not used	7
8	Brown/White	Not used	8



## DM RS232 Null Modem Cable

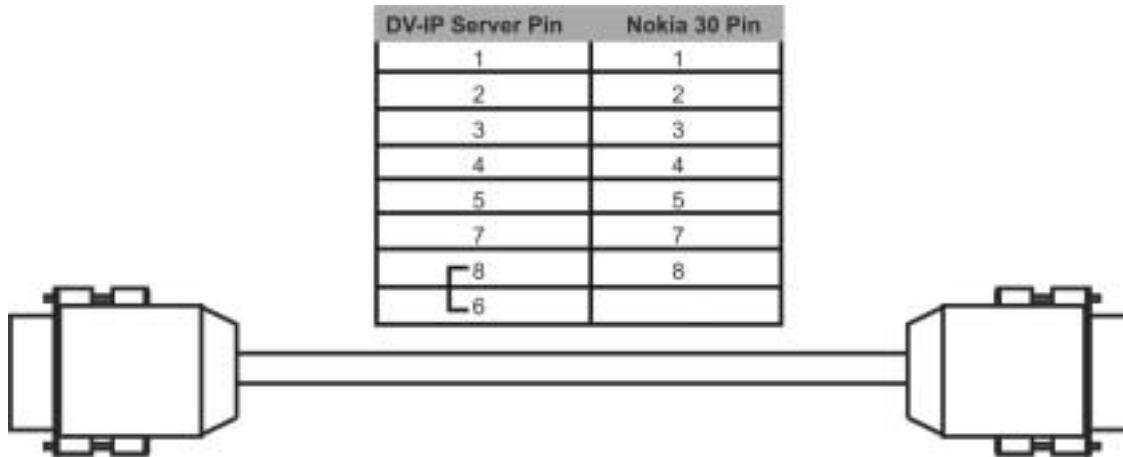
The null modem cable can be used to connect ancillary devices that require 'handshaking' such as modems, GSM, etc.

Pin	Colour Code	Pin Assignment	Pin
1	N/A	Not used	1
2	N/A	TX	2
3	N/A	RX	3
4	N/A	Not used	4
5	N/A	Ground	5
6	N/A	Not used	6
7	N/A	Not used	7
8	N/A	Not used	8
9	N/A	Not used	9



## Nokia 30 Cable

This cable is for use from the Server to the modem only.



## Appendix E – IP Address Range and Subnets

It is possible to set a range of IP address within the Firewall that will have access to the DV-IP Server. The following details how the address range and subsequent subnet is calculated and can be used in conjunction with the Configuration section of this manual.

### IP address and Subnet Masks

An IP address is a 32 bit address that is read by the network devices (switches, hubs, routers) in a binary format, however to make life simpler for Network Administrator, IP addresses are displayed in a decimal format.

The same applies to subnet masks, these too are 32 bit addresses and are identified by the network devices in binary format, but for written in a decimal format.

The 32 bits are grouped in to four 8 bits (an Octet) to give us the IP address format we are used to:

Binary Format	Decimal Equivalent
11000000.10101000.00000011.00000001	192.168.3.1
11111111.11111111.11111111.00000000	255.255.255.0

The binary format of the IP address uses 1's and 0's and within an octet it is possible to identify 256 decimal numbers from 0 to 255.

128	64	32	16	8	4	2	1	Decimal
1	1	1	1	1	1	1	1	255
0	0	0	0	0	0	0	0	0

An IP address along with its subnet mask is made up of two parts; Network ID and Host ID. If we use our example IP address, 192.168.3.1 we can see the network ID and the host ID;

IP Address	Network ID	Host ID
192.168.3.1	192.168.3	.1
255.255.255.0	255.255.255	.0

Wherever the subnet gives a value of 255 (all 1's) it 'masks' out the IP address octet and therefore represent the Network part of the overall IP address. Hence the reason the above example takes the first three octets as the network ID and the last octet as the host ID.

# Classes of Networks

There are three 'available' classes of networks. There other classes of networks that are reserved and therefore are not 'available' to the general public.

## Class A

The Class A network allocates the first octet to the Network ID and the remaining three octets are the Host ID's. There is also an address range that has been defined for a Class A network. As we use the first octet as the Network ID, we can see from the subnet mask that a Class A subnet 'masks' out the network portion of the address.

Class A Address Range	Subnet Mask	Alternative Format
0.x.x.x	255.0.0.0	0.x.x.x/8
126.x.x.x	255.0.0.0	126.x.x.x/8

### Class A Address Range

This identifies the range of network address that are within the Class A address range; 0 – 126.

### Subnet Mask

This shows that the first octet masked by the subnet which identifies the Network ID and the remaining 3 octets are the Host ID's. Which means that we can have 127 (0 to 126) networks each with up to 16,777,216 hosts.

### Alternative Format

There are two ways an IP address can be written;

10.1.1.23 255.0.0.0

10.1.1.23/8 - which identifies that the first 8 bits (octet) is the Network ID

Both addresses are the same they are just written in a different format.

## Class B

A Class B network can be seen as being a medium sized network offering more network ID's than a Class A but less host ID's, we can see that the subnet 'masks' out the network portion of the IP address.

Class B Address Range	Subnet Mask	Alternative Format
128.1.x.x	255.255.0.0	128.1.x.x/16
191.255.x.x	255.255.0.0	191.255.x.x/16

### Class B Address Range

This identifies the range of network address that are within the Class B address range; 128.1 – 191.255.

### Subnet Mask

This shows that the first two octets are masked by the subnet which identifies the Network ID and the remaining 2 octets are the Host ID's.

### Alternative Format

There are two ways an IP address can be written;

132.1.1.23 255.255.0.0

132.1.1.23/16 - which identifies that the first 16 bits (2 octets) are the Network ID

Both addresses are the same they are just written in a different format.

### Class C

A Class C network is the most commonly used class, and is available for small to medium sized business. The allocated network portion is the first three octets, with the remaining octet being the host address.

Class C Address Range	Subnet Mask	Alternative Format
192.0.1.x	255.255.255.0	192.0.1.x/24
223.255.255.x	255.255.255.0	223.255.255.x/24

### Class C Address Range

This identifies the range of network address that are within the Class C address range; 192.0.0 – 223.255.255.

### Subnet Mask

This shows that the first three octets are masked by the subnet which identifies the Network ID and the remaining octet is the Host ID's.

## Alternative Format

There are two ways an IP address can be written;

192.168.3.55 255.255.255.0

192.168.3.55/24 - which identifies that the first 24 bits (3 octets) are the Network ID

Both addresses are the same they are just written in a different format.

## Calculating IP Address Range

If we are to include an address range within the Firewall option, it is necessary to:

Identify the IP address range

Calculate the subnet mask

The following tables show the format for each Class (A, B, C), they include the IP address and number of bits allocated to the network address, equivalent subnet mask, IP address range and number of hosts.

Use these tables to assist you in entering the correct information.

### Class A table

The table below shows the address ranges for a Class A network. To identify the correct information, locate the Host address that best fits your requirements and enter the IP address and subnet or the IP address and number of bits in the Firewall option (10.1.1.1/10).

Example IP address	Equivalent Network address	Host Addresses
10.1.1.1/8	255.0.0.0	10.1.1.0 – 10.255.255.255
10.1.1.1/9	255.128.0.0	10.1.1.0 – 10.127.255.255
10.1.1.1/10	255.192.0.0	10.1.1.0 – 10.63.255.255
10.1.1.1/11	255.224.0.0	10.1.1.0 – 10.31.255.255
10.1.1.1/12	255.240.0.0	10.1.1.0 – 10.15.255.255
10.1.1.1/13	255.248.0.0	10.1.1.0 – 10.7.255.255
10.1.1.1/14	255.252.0.0	10.1.1.0 – 10.3.255.255
10.1.1.1/15	255.254.0.0	10.1.1.0 – 10.1.255.255

## Class B table

The table below shows the address ranges for a Class B network. To identify the correct information, locate the Host address that best fits your requirements and enter the IP address and subnet or the IP address and number of bits in the Firewall option (128.1.1.1/15).

Example IP address	Equivalent Network address	Host Addresses
128.1.1.1/8	255.255.0.0	128.1.1.0 – 128.1.255.255
128.1.1.1/9	255.255.128.0	128.1.1.0 – 128.1.127.255
128.1.1.1/10	255.255.192.0	128.1.1.0 – 128.1.63.255
128.1.1.1/11	255.255.224.0	128.1.1.0 – 128.1.31.255
128.1.1.1/12	255.255.240.0	128.1.1.0 – 128.1.15.255
128.1.1.1/13	255.255.248.0	128.1.1.0 – 128.1.7.255
128.1.1.1/14	255.255.252.0	128.1.1.0 – 128.1.3.255
128.1.1.1/15	255.255.254.0	128.1.1.0 – 128.1.1.255

## Class C table

The table below shows the address ranges for a Class C network. To identify the correct information, locate the Host address that best fits your requirements and enter the IP address and subnet or the IP address and number of bits in the Firewall option (192.168.3.1/27).

Example IP address	Equivalent Network address	Host Addresses
192.168.3.1/24	255.255.255.0	192.168.3.0 – 192.168.3.255
192.168.3.1/25	255.255.255.128	192.168.3.0 – 192.168.3.127
192.168.3.1/26	255.255.255.192	192.168.3.0 – 192.168.3.63
192.168.3.1/27	255.255.255.224	192.168.3.0 – 192.168.3.31
192.168.3.1/28	255.255.255.240	192.168.3.0 – 192.168.3.15
192.168.3.1/29	255.255.255.248	192.168.3.0 – 192.168.3.7
192.168.3.1/30	255.255.255.252	192.168.3.0 – 192.168.3.3
192.168.3.1/31	255.255.255.254	192.168.3.0 – 192.168.3.1



## Appendix F – SMS Message Format

The DV-IP Server supports GSM communications and SMS messaging. This allows the DV-IP Server to report events via SMS and to receive SMS messages in order to create events on the system.

### Command Format

The commands consist of a descriptor followed by a variable parameter list. The order in which the parameters appear must follow the format detailed below.

### SMS Commands

These are messages that are sent to the DV-IP Server to force an event to be triggered on the Server. These messages can be sent from a mobile phone or an Internet Service Provider (ISP) supporting SMS messaging.

#### Callback

This command is used to force the DV-IP Server to make a connection to an Alarm Receiving Centre where the telnet listener (telserve) application is running.

***CALLBACK?<password>&<destination>&<profile>&<text>***

password	This is the SMS password that has been identified in the SMS Set-up page and enables the command to be executed
destination	This is the IP address or DNS name of the Viewing application that has telserve (Telnet listener) enabled to receive the message
profile	This can be a number or name that has been configured on the SMS Set-up page, this will be via the serial port or Ethernet connection
text	This is the text message that will be sent to the remote viewer informing the Operator of an incident and therefore should be meaningful

## SMS Reports

These are messages sent from the DV-IP Server to a pre-defined SMS Server when an event occurs. The 'events' that will initiate this function are configured within the DV-IP Server configuration web pages.

### Startup

An SMS message will be sent from the DV-IP Server to the receiving station when the DV-IP Server 'starts up'.

**STARTUP?<name>&<time>&<IP address>&<latitude>&<longitude>&<zone>**

name	This is the system name configured on the DV-IP Server
time	This is the local julian time of the message. The julian time is the number of seconds since 00:00:01 hour on January 1st 1970. If the Verbose message option has been enabled on the DV-IP Server this message will be in a human readable format
IP address	This is the Ethernet IP address of the DV-IP Server
latitude	This parameter is not relevant to the DV-IP Server and included to support other Dedicated Micros platforms
longitude	This parameter is not relevant to the DV-IP Server and included to support other Dedicated Micros platforms
zone	This parameter is not relevant to the DV-IP Server and included to support other Dedicated Micros platforms

### Alarm

This report is generated when an alarm is received on the DV-IP Server.

**ALARM?<name>&<time>&<lat>&<long>&<speed>&<course>&<zone>&<camera>&<title>**

name	This is the system name configured on the DV-IP Server
time	This is the local julian time of the message. The julian time is the number of seconds since 00:00:01 hour on January 1st 1970. If the Verbose message option has been enabled on the DV-IP Server this message will be in a human readable format
lat	This parameter is not relevant to the DV-IP Server and included to support other Dedicated Micros platforms

long	This parameter is not relevant to the DV-IP Server and included to support other Dedicated Micros platforms
Speed	This parameter is not relevant to the DV-IP Server and included to support other Dedicated Micros platforms
course	This parameter is not relevant to the DV-IP Server and included to support other Dedicated Micros platforms
zone	This parameter is not relevant to the DV-IP Server and included to support other Dedicated Micros platforms
camera	This is the video input number that is directly associated with the alarm on the DV-IP Server
title	This is the alarm title allocated to the alarm that forced the SMS message

## VMD

This report is generated when activity has been identified on the DV-IP Server.

**VMD?<name>&<time>&<lat>&<long>&<speed>&<course>&<zone>&<camera>&<vmd zone>**

name	This is the system name configured on the DV-IP Server
time	This is the local julian time of the message. The julian time is the number of seconds since 00:00:01 hour on January 1st 1970. If the Verbose message option has been enabled on the DV-IP Server this message will be in a human readable format
lat	This parameter is not relevant to the DV-IP Server and included to support other Dedicated Micros platforms
long	This parameter is not relevant to the DV-IP Server and included to support other Dedicated Micros platforms
speed	This parameter is not relevant to the DV-IP Server and included to support other Dedicated Micros platforms
course	This parameter is not relevant to the DV-IP Server and included to support other Dedicated Micros platforms
zone	This parameter is not relevant to the DV-IP Server and included to support other Dedicated Micros platforms

camera	This is the video input number that is directly associated with the alarm on the DV-IP Server
vmd zone	VMD zones are configured on the DV-IP Server, this identifies the zone that has been activated to initiate the SMS message

## Camfail

This report will be generated if the DV-IP Server identifies that any of the video inputs does not have a 1V peak-to-peak signal.

**CAMFAIL?<name>&<time>&<lat>&<long>&<speed>&<course>&<zone>&<upper>&<lower>**

name	This is the system name configured on the DV-IP Server
time	This is the local julian time of the message. The julian time is the number of seconds since 00:00:01 hour on January 1st 1970. If the Verbose message option has been enabled on the DV-IP Server this message will be in a human readable format
lat	This parameter is not relevant to the DV-IP Server and included to support other Dedicated Micros platforms
long	This parameter is not relevant to the DV-IP Server and included to support other Dedicated Micros platforms
speed	This parameter is not relevant to the DV-IP Server and included to support other Dedicated Micros platforms
course	This parameter is not relevant to the DV-IP Server and included to support other Dedicated Micros platforms
zone	This parameter is not relevant to the DV-IP Server and included to support other Dedicated Micros platforms
upper	This identifies the bitmask of failed cameras 33 – 64
lower	This identifies the bitmask of failed cameras 1 - 32

## Additional Information

### Command Reference List

DV-IP command line – DV-IP>

Command	Description
<ESC> m\Ether_IP\xxx.xxx.xxx.xxx	Set IP address of the DV-IP Server
<ESC> m\subnet\xxx.xxx.xxx.xxx	Set subnet of the DV-IP Server
<ESC> m\gateway\xxx.xxx.xxx.xxx	Set gateway of the DV-IP Server
<ESC> m\status	Displays the status information or the DV-IP Server; drive information, comm. Ports information, enabled telemetry, etc.
<ESC> m\serial_mode\comx\disabled  Debug  PPP Text Telem	This command will allow any of the serial ports to be set for a specific function.  Replace the x with the port number and select from the list the option available (refer to the serial port section of this manual for allocated functionality for each port)
<ESC> m\security\Eng\Open Off Pass	Allows the security password for debug mode to be enabled (pass)or disable (off) on the DV-IP Server
<ESC> m\security\debug\Open Off Pass	Allows the security password for debug mode to be enabled (pass)or disable (off) on the DV-IP Server
<ESC> m\set\bs8418\on Off	Allows the Advanced Alarm Features on the DV-IP Server to be enabled via the command line.  <b>Note:</b> This is usually enabled within the web configuration pages
ipcfg	Shows the IP address, subnet mask and gateway set on the DV-IP Server
TCP Ports	Displays the active TCP ports supported on the DV-IP Server





**Dedicated Micros Ltd.**

11 Oak Street, Swinton,  
Manchester. M27 4FL, UK  
Tel: +44 (0) 161 727 3200  
Fax: +44 (0) 161 727 3300

**Dedicated Micros Europe**

Neckarstraße 15,  
41836 Hückelhoven, Germany  
Tel: +49 2433 5258-0  
Fax: +49 2433 5258-10

**Dedicated Micros France**

9-13 rue du Moulinet  
75013 Paris, France  
Tel : +33 (0) 1 45 81 99 99  
Fax : +33 (0) 1 45 81 99 89

**Dedicated Micros, Australia PTY.**

5/3 Packard Avenue, Castle Hill,  
NSW 2154, Australia  
Tel: +612 9634 4211  
Fax: +612 9634 4811

**Dedicated Micros, Asia PTY**

16 New Industrial Road,  
#03-03 Hudson Techno Centre,  
Singapore 536204  
Tel: +65 62858982  
Fax: +65 62858646

**Dedicated Micros Slovenia**

Delavska cesta 26,  
4208 Sencure, Slovenia  
Tel: +386 4279 1890  
Fax: +386 4279 1891

**Dedicated Micros Benelux**

Joseph Chantraineplantsoen 1,  
3070 Kortenberg  
Belgium  
Tel: +32 2751 3480  
Fax: +32 2751 3481

**Dedicated Micros Middle East**

Building 12, Suite 302,  
P.O. Box 500291, Dubai Internet City,  
Dubai, United Arab Emirates  
Tel: +971 (4) 390 1015  
Fax: +971 (4) 390 8655

**Dedicated Micros (Malta) Ltd.**

UB2 San Gwann Industrial Estate,  
San Gwann SGN 09 Malta  
Tel: +356 21483 673  
Fax: +356 21449 170

**Dedicated Micros USA.**

14434 Albemarle Point Place, Suite  
100,  
Chantilly, Virginia 20151 USA  
Freephone: 800 864 7539  
Tel: +1 703 904 7738  
Fax: +1 703 904 7743

23456 Hawthorne Blvd. Suite 100,  
Torrance, CA 90505, USA  
Tel: +1 310 791-8666  
Fax: +1 310 791-9877